



Kiwi Syslog Daemon

A Freeware Syslog Daemon for Windows

訳：ジュピターテクノロジー株式会社

平成20年9月17日

Program copyright 1998 - 2007 by Kiwi Enterprises.

最新版の入手先: www.kiwisyslog.com

サポート: <http://www.kiwisyslog.com/support>

- * 本日本語マニュアルはできる限り忠実に実際のプログラムに沿うよう書き換えてありますが、検証が取れない部分等は原文のまま翻訳してあります。参照先のリンク切れ等が含まれておりますが、ご了承ください。
- * 製品版を弊社よりご購入された方は文中のサポート窓口として示されているKiwi社の連絡先ではなく、下記の弊社サポート受付窓口までご連絡ください。Eメール: tech-support1@jtc-i.co.jp TEL:042-358-1251

目次

1. Kiwi Syslog Daemon.....	8
1.1 フリーウェア版の機能.....	8
1.2 正規登録版の機能.....	9
1.3 正規登録版の購入.....	10
1.4 Kiwi Syslog Daemonの初期設定.....	10
1.4.1 インストール時の設定.....	10
1.5 フィードバック – コメントやバグ.....	10
1.6 ソフトウェアライセンス条項.....	10
1.7 免責条項.....	11
1.8 謝 辞.....	12
2 メイン表示ウィンドウ.....	12
2.1 メイン表示ウィンドウ.....	12
2.2 Fileメニュー.....	12
2.2.1 Setup ([Ctrl]+[P]、 設定).....	12
2.2.2 Send Test message to local host ([Ctrl]+[T]、 テストメッセージ送信).....	13
2.2.3 Purge (パージ).....	13
2.2.4 Debug options (デバッグ オプション).....	13
2.2.4.1 Create Tech-Support File (Zip) (サポートファイルの作成).....	13
2.2.5 Export settings to INI file (設定情報をINIファイルにエクスポート).....	13
2.2.6 Exit (終了).....	14
2.3 Edit (編集)メニュー.....	14
2.3.1 Select All (全て選択).....	14
2.3.2 Copy selected items to the clipboard (選択した項目をクリップボードにコピー).....	14
2.4 View (ビュー)メニュー.....	14
2.4.1 View syslog statistics (syslog統計の表示).....	14
2.4.2 View e-mail log file (Eメールログファイルの表示).....	14
2.4.3 View error log file (エラーログファイルを表示).....	14
2.4.4 Adjust width to fit screen (画面幅の自動調節).....	15
2.4.5 Clear display (画面消去).....	15
2.4.6 Highlighting Options (ハイライト表示オプション).....	15
2.4.7 Choose font (表示フォント選択).....	16
2.5 Manage (管理)メニュー.....	16
2.5.1 Manage (管理)メニュー.....	16
2.5.2 Install the Syslogd service (Syslogdサービスのインストール).....	17
2.5.3 Uninstall the Syslogd service (Syslogdサービスのアンインストール).....	17
2.5.4 Start the Syslogd service (Syslogdサービスの開始).....	17
2.5.5 Stop the Syslogd service (Syslogdサービスの停止).....	17
2.5.6 Ping the Syslogd service (SyslogdサービスにPing).....	17
2.5.7 Show the Syslogd service state (Syslogdサービス状態の表示).....	17
2.5.8 Debug options(デバッグオプション)メニュー.....	17
2.5.8.1 Display the Service version (サービスのバージョン表示).....	18
2.5.8.2 Get diagnostic information (診断情報の入手).....	18
2.5.8.3 Reset the Syslogd service (Syslogdサービスリセット).....	18
2.5.8.4 Clear the service DNS Cache (DNSキャッシュのクリア).....	18
2.5.8.5 Apply new settings to Syslogd service (新しい設定の適用).....	18
2.5.8.6 Retrieve last messages (最終メッセージの取得).....	18
2.5.8.7 Send keep alive (キープアライブメッセージの送信).....	18
2.6 Help (ヘルプ)メニュー.....	19
2.6.1 Kiwi Syslog Help (ヘルプ、 F1).....	19
2.6.2 Help Topics (ヘルプトピックス).....	19
2.6.3 Online FAQ (オンラインFAQ).....	19
2.6.4 Request a 30 day trial key (30日間トライアルキーの申請).....	19
2.6.5 Purchase the registered version (正規登録版の購入).....	19
2.6.6 Enter the registration details (ライセンスの登録、 F2).....	19
2.6.7 Make a suggestion or report a bug (バグレポート作成).....	19

2.6.8	Join the mailing list (メーリングリストへの参加).....	19
2.6.9	About Kiwi Syslog (Kiwi Syslog Daemonについて).....	19
3	Syslogプロパティの設定.....	20
3.1	Syslog Daemon初期設定ガイド.....	20
3.2	キーボードの使用法.....	20
3.3	Rules / Filters / Actions (ルール/フィルター/アクション).....	20
3.3.1	ルールエンジンの動作.....	20
3.3.2	Filter Type (フィルタータイプ).....	21
3.3.2.1	Simple filter (シンプルフィルター).....	21
3.3.2.2	Complex filter (複合フィルター).....	21
3.3.2.3	Regular Expression filter (正規表現フィルター).....	22
3.3.2.4	IP Address Range filter (アドレス範囲フィルター).....	25
3.3.2.5	IP Subnet Mask filter (IP サブネットマスクフィルター).....	26
3.3.2.6	Priority filter (プライオリティフィルター).....	27
3.3.2.7	Time of Day filter (時刻フィルター).....	28
3.3.2.8	Time interval filter (タイムインターバルフィルター).....	29
3.3.2.9	Threshold filter (閾値フィルター).....	30
3.3.2.10	Timeout filter (タイムアウトフィルター).....	31
3.3.2.11	フィルター定義のインポートとエクスポート.....	32
3.3.2.12	Input source (入力ソース).....	32
3.3.3	Action - Display (アクション - 表示).....	32
3.3.4	Action - Log to file (アクション - ファイル記録).....	32
3.3.4.1	Action - Log to file (アクション - ファイル記録).....	32
3.3.4.2	AutoSplit values (自動分割値).....	32
3.3.4.3	Log file formats (ログファイルフォーマット).....	36
3.3.4.4	Log File Rotation (ログファイルローテーション).....	38
3.3.5	Action - Forward to another host (アクション - 他のホストへ転送).....	39
3.3.6	Action - Play a sound (アクション - 音を鳴らす).....	40
3.3.7	Action - Run external program (アクション - 外部プログラム実行).....	40
3.3.8	Action - E-mail message (アクション - Eメールメッセージ送信).....	41
3.3.8.1	Insert message content or counter (メッセージ内容/カウンターの挿入).....	42
3.3.9	Action - Send Syslog message (アクション - Syslogメッセージ送信).....	44
3.3.10	Action - Log to database (アクション - データベース記録).....	45
3.3.10.1	Action - Log to database (アクション - データベース記録).....	45
3.3.10.2	To configure an ODBC database DSN (ODBCデータベースDSNの構築).....	47
3.3.10.3	Problems logging when running as a Service (サービス版実行時の記録エラー).....	48
3.3.11	Action - Log to NT Event log (アクション - NT Event logへの記録).....	48
3.3.11.1	Action - Log to NT Event log (アクション - NT Event log記録).....	48
3.3.11.2	ログ挿入タイプの設定.....	48
3.3.12	Action - Send pager or SMS message via NotePage Pro (アクション - NotePage Pro経由でポケットベル/SMSにメッセージ送信).....	49
3.3.13	Action - Send ICQ instant message (アクション - ICQインスタントメッセージ送信).....	50
3.3.14	Action - Send SNMP Trap (アクション - SNMPトラップ送信).....	51
3.3.15	Action - Stop processing message (アクション - メッセージ処理終了).....	52
3.3.16	Action - Run Script (アクション - スクリプト実行).....	52
3.3.16.1	練習 - 初めてのスクリプト作成.....	54
3.3.16.2	スクリプト変数.....	56
3.3.16.3	スクリプト関数.....	59
3.3.16.4	スクリプト記述辞書.....	66
3.3.16.5	スクリプト例.....	68
3.4	Setup - Schedules (設定 - スケジュール).....	71
3.4.1	スケジューラーの動作.....	72
3.4.2	On a schedule (スケジュールに従って実行).....	74
3.4.3	On application/service startup (アプリケーション/サービスの起動時に実行).....	78
3.4.4	On application/service shutdown (アプリケーション/サービスの終了時に実行).....	78
3.4.5	Archive (アーカイブ) タスク.....	78
3.4.6	Clean-up (クリーンアップ) タスク.....	84

3.4.7	Run Program (プログラム実行) タスク	86
3.4.8	Run Script (スクリプト実行) タスク	88
3.4.9	Schedule Report (スケジュールレポート)	90
3.5	Setup – Formatting (設定 – フォーマット)	91
3.5.1	Custom file formats (カスタムファイルフォーマット)	91
3.5.2	Custom DB formats (カスタムDBフォーマット)	92
3.6	Setup - DNS Resolution (設定 – DNSの解決)	93
3.6.1	Resolve the address of the sending device (送信デバイスのアドレス解決)	93
3.6.2	Remove the domain name (show only the host name) (ドメイン名を消去- ホスト名のみ表示)	93
3.6.3	Resolve IP addresses within the message text (SyslogメッセージテキストのIPアドレス解決)	93
3.6.4	DNS query timeout (DNSクエリーのタイムアウト)	94
3.6.5	Setup - DNS Setup (設定 – DNS設定)	94
3.6.5.1	Internal IP address – Name Resolution (内部IPアドレス - 名前解決)	94
3.6.5.2	External IP address – Name Resolution (外部IPアドレス - 名前解決)	95
3.6.6	Setup - DNS Cache (設定 – DNSキャッシュ)	95
3.6.6.1	ローカルのDNSキャッシュ	95
3.6.6.2	Cache settings (キャッシュ設定)	96
3.7	Setup – Modifiers (設定 – 修正)	96
3.7.1	Syslog message modifiers (Syslogメッセージモディファイアー)	97
3.8	Setup – Scripting (設定 – スクリプト作成)	97
3.9	Setup – Appearance (設定 – 外観)	98
3.9.1	Wallpaper (壁紙)	98
3.10	Setup - E-mail options (設定 – Eメールオプション)	98
3.10.1	E-mail setup options (設定 – Eメール設定オプション)	98
3.10.2	アラームメッセージの例	99
3.10.3	統計メッセージの例	100
3.11	Setup - Alarm thresholds (設定 – アラーム閾値)	100
3.11.1	Notify by Mail (メールで通知)	100
3.11.2	Audible Alarm (音で通知)	101
3.11.3	Run Program (プログラム実行)	101
3.12	Setup - Input options (設定 – 入力オプション)	101
3.12.1	Setup - Input options (設定 – 入力オプション)	101
3.12.2	Inputs – UDP (入力 - UDP)	101
3.12.3	Inputs – TCP (入力 – TCP)	102
3.12.4	Inputs – SNMP (入力 - SNMP)	103
3.12.5	Beep on every message received (メッセージ受信時ピーブ音)	105
3.12.6	Cisco PIX ファイアーウォール(TCP)	105
3.12.7	Inputs - Keep-alive (入力 – キープアライブ)	106
3.13	Setup – Display (設定 – 表示)	107
3.13.1	Display window is always on top of others (常に最前面に表示)	107
3.13.2	Number of display rows (表示行数)	107
3.13.3	Minimize to System Tray on start-up (起動時にシステムトレイに最小化)	107
3.13.4	Use 3D text in display heddings (3Dタイトルを使用)	107
3.13.5	Use MM/DD/YYYY date format (日付をMM/DD/YYで表示)	107
3.13.6	Show messages per hour in title bar (タイトルバーに1時間の受信メッセージ数を表示)	108
3.13.7	Blink System Tray Icon when receiving messages (メッセージ受信時にアイコンを点滅)	108
3.13.8	Word wrap long message text(長いテキストを折り返す)	108
3.13.9	Adjust column widths automatically (列幅の自動調整)	108
3.14	テストボタンの動作	108
4	Syslog statistics window (syslog統計ウィンドウ)	108
4.1	Syslog statistics window (Syslog 統計ウィンドウ)	108
4.2	History [1hr] (1時間の受信履歴)	109
4.3	History [24hr] (24時間の受信履歴)	109
4.4	Severity (重要度)	109
4.5	Top 20 Hosts (上位20ホスト)	109
4.6	Counters (カウンター)	110
5	Kiwi Syslog Daemon サービス版	110

5.1	Kiwi Syslog Daemon サービス版のシステム要件.....	110
5.2	Installing the Service edition (サービス版をインストールする).....	111
5.3	サービス版を管理する.....	111
5.4	サービス版の問題を解決する.....	112
5.5	Kiwi Syslog Daemon NT Service のアップグレード.....	112
5.5.1	Kiwi Syslog Daemon NT Service のアップグレード.....	112
5.5.2	現在インストールされているプログラムを削除する.....	112
5.5.3	新バージョンをインストールする.....	112
6	syslog 送信デバイスの設定.....	113
6.1	SNARE でWindowsイベントログを取得する.....	113
6.2	3Com NetServer の設定.....	114
6.3	3Com Total Control Chassis の設定.....	114
6.4	Alliant Cellular Gateway の設定.....	115
6.5	Allied Telesyn ルーターの設定.....	116
6.6	Arris Cable Modem Termination System の設定.....	116
6.7	Extreme Summit スイッチの設定.....	116
6.8	Barracuda Spam Firewall の設定.....	117
6.9	Bay Networks デバイスの設定.....	117
6.10	Bintech アクセスルーターの設定.....	120
6.11	Buffalo エアステーションルーターの設定.....	120
6.12	Checkpoint FW-1 ファイアーウォールの設定.....	121
6.13	Cisco 3000 シリーズVPNコンセントレータの設定.....	121
6.14	Cisco Catalyst スイッチの設定.....	121
6.15	Cisco PIX の設定.....	122
6.16	Cisco ルーターの設定.....	122
6.17	Cisco ワイヤレスデバイス(Aironet)の設定.....	122
6.18	D-Link DFL-700 ファイアーウォールの設定.....	123
6.19	DLINK DL-840V ルーターの設定.....	123
6.20	FortiGate アンチウイルスファイアーウォールの設定.....	123
6.21	FREESCO ルーター/ファイアーウォールの設定.....	124
6.22	HP JetDirect プリンタの設定.....	124
6.23	Intertex ADSL ルーターの設定.....	125
6.24	Linksys ファイアーウォールの設定.....	125
6.25	Linksys ワイヤレスVPNルーターの設定.....	125
6.26	Lucent ルーターの設定.....	126
6.27	Meinberg タイムサーバーの設定.....	126
6.28	Netgear / ZyXEL RT311/RT314.....	127
6.29	Netgear ADSL ファイアーウォールルーター DG834.....	128
6.30	Netgear FVS318 VPN ファイアーウォール.....	128
6.31	Netgear RP114 ルーター.....	128
6.32	NetScreen ファイアーウォールの設定.....	129
6.33	Nortel Networks ルーターの設定.....	129
6.34	Pack X IDScenterの設定.....	130
6.35	SnapGear SOHO+ の設定.....	130
6.36	SonicWall ファイアーウォールの設定.....	130
6.37	Symantec ファイアーウォール/VPN 200.....	131
6.38	Unix マシンの設定.....	131
6.39	VegaStream テレフォニーゲートウェイの設定.....	132
6.40	Watchguard Firebox と Dshieldの連携設定.....	133
6.41	WatchGuard SOHO ファイアーウォールの設定.....	133
6.42	W-Linx MB ブロードバンドルーターの設定.....	133
6.43	ZyXEL ZyWALL 10の設定.....	133
7	SNMPトラップ送信デバイスの設定.....	134
7.1	Cisco IOS SNMP トラップのサポート設定.....	134
8	SyslogdエラーとEメールログ.....	134
8.1	エラーログ.....	134
8.2	エラーログファイルの表示.....	134

8.3	SMTPメールログ	134
8.4	Eメールログファイルの表示	135
9	Syslog プロトコル	135
9.1	Syslog ファシリティ	135
9.2	Syslog レベル	135
9.3	Syslog プライオリティ	136
9.4	転送	137
9.5	Syslog RFC 3164 ヘッダーフォーマット	137
9.6	Kiwi Reliable Delivery Protocol (KRDP)	137
9.6.1	KRDP エラーメッセージ	139
10	問題の解決	140
10.1	問題を解決するには	140
10.2	Windows XP SP2 / Windows 2003 Server SP1上で使用する場合の注意事項	140
10.3	Windows 95上で使用する場合の注意事項	141
11	開発者向けの情報	141
11.1	Kiwi Syslog Daemonのレジストリ設定	141
11.1.1	表示 - 有効列	141
11.1.2	表示 - デフォルトの行の高さ	142
11.1.3	統計メール配信時刻	142
11.1.4	サービス - 開始/停止 タイムアウト	142
11.1.5	サービス - プロパティ更新タイムアウト	143
11.1.6	サービス - アプリケーション間通信ポート	143
11.1.7	サービス - 依存性	143
11.1.8	サービス - デバッグ開始	144
11.1.9	DNS - ビジー時に待機を無効にする	144
11.1.10	DNS - 最大キャッシュサイズ	145
11.1.11	DNSキャッシュの参照失敗	145
11.1.12	DNS 設定- DNS/NetBIOS キューバッファバースト係数	145
11.1.13	DNS 設定 - DNS/NetBIOS キューバッファクリア率	145
11.1.14	DNS 設定 - DNS/NetBIOS キュー制限	146
11.1.15	DNS 設定 - デバッグモード	146
11.1.16	メッセージバッファサイズ	146
11.1.17	Eメール - 件名追加テキスト	147
11.1.18	Eメール - 本文追加テキスト	147
11.1.19	Eメール - 送信メッセージの制限	148
11.1.20	ファイル書き込みキャッシュ	148
11.1.21	ファイルへの記録 - 日付区切り文字	150
11.1.22	ファイルへの記録 - 時間区切り文字	151
11.1.23	ファイルへの記録 - エンコード形式	151
11.1.24	スクリプトエディター	152
11.1.25	スクリプトのタイムアウト	152
11.1.26	データベースコマンドのタイムアウト	152
11.1.27	アーカイブ - 置き換え文字	153
11.1.28	アーカイブ - 区切り文字	153
11.1.29	アーカイピング - 古いアーカイブ名規則を使用する	153
11.1.30	アーカイピング - アーカイブ処理時Tempフォルダのパス指定	154
11.1.31	アーカイピング - Tempファイルを有効にする	154
11.1.32	エラーログフォルダ	154
11.1.33	メールログフォルダ	154
11.1.34	KRDP - ACKタイマー	155
11.1.35	KRDP - キープアライブタイマー	155
11.1.36	KRDP - ディスクキャッシュフォルダ	155
11.1.37	KRDP - Rx デバッグ	155
11.1.38	KRDP - Tx デバッグ	156
11.1.39	KRDP - キューサイズ	156
11.1.40	KRDP - キューの最大サイズ(MB)	156
11.1.41	KRDP - 自動接続	156

11.1.42	KRDP - 接続時間	157
11.1.43	KRDP - 送信スピード	157
11.1.44	KRDP - アイドルタイムアウト	157
11.1.45	KRDP - SeqNumの追加	157
11.1.46	Syslogd プロセスのプライオリティ	158
11.1.47	送信元アドレス - カスタムの開始 / 終了タグ	159
11.1.48	ルール - 最大ルール数	159
11.1.49	データベースロガー - キャッシュクリアの頻度	160
11.1.50	データベースロガー - キャッシュのタイムアウト	160
11.1.51	データベースロガー - データベースキャッシュを無効にする	160
11.2	コマンドライン引数	160
11.2.1	起動時デバッグ	160
11.2.2	サービス版のインストール	161
11.2.3	サービス版のアンインストール	161
11.3	Kiwi Syslog Daemon の自動インストール	161
11.4	設定にINI ファイルを使用	162
12	Kiwi社のソフトウェア製品	162
12.1	Kiwi CatTools	162
12.2	Kiwi SyslogGen	163
12.3	Kiwi Logfile Viewer	163
12.4	Kiwi Secure Tunnel	163

1. Kiwi Syslog Daemon

Kiwi Syslog Daemonはsyslogメッセージをネットワークデバイスから受け取り、それらをリアルタイムに表示します。

さらに、syslogメッセージに対し下記のようなイベント処理を行います。

- メッセージをスクロールウィンドウに表示
- メッセージをテキストファイルに記録
- 他のsyslogサーバーへのメッセージ転送
- ODBCデータベースへの記録
- NTアプリケーションイベントログへの書き込み
- SMTP経由でメッセージをEメール送信
- 音によるアラーム発生
- ポケットベルシステムなどの外部プログラムの実行
- SNMPトラップメッセージの送信
- NotePager Proによる通知

受信メッセージに対してアクションを実行します。メッセージはホスト名、ホストのIPアドレス、プライオリティ、本文あるいは時刻でフィルター可能です。

インストール用パッケージのインストール方法:

- Windows NT4/2K/XP/2K3用にWindowsサービスとして
- Windows 95/98/ME/NT4/2K/XP/2K3用の標準的な対話式アプリケーションとして

標準アプリケーション版は対話方式で実行され、ユーザーがログインしている間だけ操作できます。

サービス版はNTサービスとして自動的に実行されます。操作のためにログオンする必要はありません。

Kiwi Syslog Service ManagerプログラムにはWindows NTサービスの設定・管理を行うためのインターフェイスが付属しています。

BSD SyslogプロトコルはRFC3164で定義されています。

<http://community.roxen.com/developers/idoocs/rfc/rfc3164.html>

syslogプロトコルについては次のWebページを参照してください。

<http://www.sans.org/infosecFAQ/unix/syslog.htm>

1.1 フリーウェア版の機能

Kiwi Syslog Daemonフリーウェア版の有する機能および特長は以下のとおりです。

- GUIベースによるsyslogマネージャ
- 受信時にメッセージをリアルタイム表示
- 10種類のバーチャルディスプレイ
- すべてあるいはプライオリティ、日時フィルター後のメッセージを記録もしくは転送
- プライオリティ、日時によりログファイルを自動分割
- UDP、TCPまたはSNMP経由でメッセージを受信
- UDPあるいはTCP経由でメッセージの転送
- 指定したスケジュールによるログファイルの自動アーカイビング
- 1時間内に受信したメッセージ数の音やEメールによるアラーム通知
- ログファイル容量の音やEメールによるアラーム通知
- syslogトラフィック統計を毎日Eメールで送信
- システムトレイの最小化
- 他のsyslogホストへの転送時に送信元アドレスを保持
- syslogトレンドグラフ機能 (直近24時間/1時間)
- 高負荷時でもメッセージ喪失の無いバッファリング機能
- 送信元ホストIPの名前解決と任意でのドメイン消去
- 最大100エントリーのDNSキャッシング
- 最大10スレッドのプリエンティブDNSルックアップ
- プログラム外観を変更する5種類のスキンが付属
- 表示フォント、表示色、背景の選択
- NTサービスとして実行

- RFC3164送受信オプション
- コンテキストベースのヘルプ
- 無料（再販禁止）

正規登録版には、フリーウェア版のすべての機能に加え、多数の追加機能が付属しています。

変更点やバグ、新バージョンのリリースをお知らせするメーリングリストがあります。
登録は以下のページから行ってください。

<http://www.kiwisyslog.com/feedback.htm>

1.2 正規登録版の機能

フリーウェア版の機能/特長に加え、柔軟性に富んだ多くの機能が追加されています。

追加ログファイル自動分割機能

- ホスト名
- ホストIPアドレス
- ドメイン名
- WELFフォーマットタグサポート

追加フィルターオプション

- IPアドレス、ホスト名、テキスト本文によるフィルター
- 不要なホストメッセージの除去あるいはホスト名によって異なるロギングアクション
- 特定キーワードを含むメッセージの処理

追加アクション

- フィルタリング、文脈解析、カスタム統計およびそれらに引き続いて実行するアクションなどを実現する強力なスクリプトエンジン
- ODBCデータベース(Access/SQL/Oracle/MySQL/Informix等)へのロギング
- WindowsNTアプリケーションイベントログへの書き込み
- フィルター条件に合致したときの任意の音声ファイルによるアラーム
- Eメールによるsyslogメッセージ転送
- フィルター条件に合致したときのsyslogメッセージの他ホストへの転送
- SNMPトラップ送信 (Version 1/Version 2)
- ICQインスタントメッセージ送信
- NotePager ProによるポケットベルやSMSメッセージの送信
- フィルター条件に合致したときの外部プログラムの指定・実行
- 下記の受信syslogメッセージの値を外部プログラム、Eメールメッセージまたはsyslogメッセージへ渡す
 - メッセージテキスト
 - メッセージ時刻
 - メッセージ日付
 - ホスト名
 - ファシリティ
 - レベル
 - アラーム閾値
 - 現在のSyslog統計

追加バッファリング機能

- 20,000のsyslogメッセージバッファにより高負荷時でのメッセージ喪失がありません。
- 1,000のEメールメッセージバッファにより高負荷時やメールサーバーの一時的な停止でのEメールメッセージロスがありません。

追加DNS機能

- メッセージテキストのIPアドレスをホスト名解決
- IPアドレスをホスト名で置き換え、またはIPアドレスの後にホスト名を追加
- 20,000エントリーのDNSキャッシュ
- 200スレッドの先行DNS ルックアップ

追加アラームオプション

- アラーム時に任意の音声ファイルの実行
- アラーム時に任意の外部プログラムの実行。ポケットベルやSMS など

正規登録版におけるその他の特長

- Kiwi Syslog Daemonで作成したログファイルの管理や調査の柔軟性が高められています。特に大規模なネットワークを管理している管理者にとって最新のステータスとイベント情報をタイムリーに得られるという点は非常に大きな魅力です。拡張されたログファイルの自動分割(Auto Split)機能を使用すれば、受信メッセージを容易に分類しそれぞれのログファイルに記録することができます。その後、これらのログファイルを基に特定のデバイス、イベント、条件、あるいは興味に従ったレポートを作成することができます。
- 拡張されたフィルター機能で必要なアクションコントロールを完全にかつ容易に行えます。多数の拡張アクションは受信メッセージ、フィルター、ルールで自動的に実行されます。特に多くのアラート機能はモバイル環境の増加に適しています。
- 大容量バッファ機能。大規模なネットワークに対応でき、一時的なメッセージの大量発生時などでも信頼できるメッセージ処理が可能です。
- Eメールの優先処理サポート

1.3 正規登録版の購入

フリーウェア版は無償で無期限に使用できます。日本語資料、代理店による日本語サポート、追加機能が必要な場合は正規登録版を購入してください。

Kiwi Syslog Daemon正規登録版の購入はジュピターテクノロジー株式会社までご連絡ください。

<http://www.jtc-i.co.jp>

1.4 Kiwi Syslog Daemonの初期設定

Kiwi Syslog Daemonは可能な限り柔軟に、容易に使用できるように設計されています。そのため初期設定は非常に簡単です。

Kiwi Syslog Daemonの設定に必要なことはアプリケーションをシステムの希望の場所にインストールすることだけです。デフォルトではUDP/514でsyslogメッセージを受信します。

基本構成ではこれ以上必要ありません。

Kiwi Syslog Daemonがsyslogメッセージを受信するためには送信ネットワークデバイス側で、その情報をKiwi Syslog DaemonがインストールされたシステムのIPアドレスに送信するように設定します。

多くのデバイスの設定手順については[後述](#)します。

本書に記載されていないsyslogメッセージ送信可能デバイスについての情報をお持ちでしたら、下記までお知らせください。次回マニュアル更新時に情報を追加させていただきます。

<http://www.kiwisyslog.com/support>

1.4.1 インストール時の設定

Kiwi Syslog Daemonのインストール直後は、フィルターなしのルールが1つだけ定義されており、受信するすべてのsyslogメッセージに対しこのルールで定義されているアクションが適用されます。ルールには Display アクションと Log to file アクションの2つが定義されています。Display アクションによって受信した全情報がリアルタイムで表示され、Log to file アクションによって SyslogCatchall.txt というファイルにその情報が記録されます。このファイルはKiwi Syslog Daemonをインストールしたフォルダの \Logs ディレクトリにあります。

これは、ごく基本的な初期設定です。このルールがオフにされていたり、削除された場合には、メッセージの表示もファイルへの記録も行われません。

syslogメッセージを管理するためのフィルターやアクションは、これ以外にも必要に応じて作成し、追加することができます。

1.5 フィードバック – コメントやバグ

プログラムについてのコメントや改良提案は下記までEメールにてお知らせください。

<http://www.kiwisyslog.com/support>

1.6 ソフトウェアライセンス条項

[使用許諾契約書](#)

お客様はフリーウェア版のKiwi Syslog Daemonを、登録せずに無期限で使用できるものとします。その場合、Kiwi Softwareメーリングリストに参加されることをお勧めします。本メーリングリストではバグレポート、使用方法のヒント、新バージョンの発行などを順次お知らせしております。

フリーウェア版のKiwi Syslog Daemon(以下「ソフトウェア製品」と表示)は、登録することによってフリーウェア版では使用できない機能や特長を使用できるようにすることが可能です。1台のPCにインストールされているソフトウェア製品1つに対して1つの登録キーが必要です。登録キーには重複しない固有のシリアル番号と登録コードが含まれ、フル機能で使用するプログラム1つに対して1組のシリアル番号と登録コードが必要となります。

本ソフトウェア製品をインストールし、使用するためには以下の禁止条項に同意していただく必要があります。

- (a) ソフトウェア本体ならびに付属文書の全部および一部を元にした逆コンパイル、リバースエンジニアリング、逆アセンブル、改変、派生物の生成などの行為を禁じます。
- (b) 著作権またはKiwi Enterpriseの所有権表示を削除する行為を禁じます。
- (c) ソフトウェア製品の登録キーを正式に登録されたエンドユーザー以外の第三者に配布する行為を禁じます。
- (d) ソフトウェア製品を第三者に貸し出す行為を禁じます。
- (e) Kiwi Enterpriseから直接発行されたものでない登録キー/シリアル番号の使用を禁じます。

ライセンス契約の解除

本ライセンス契約書に記載されている使用許諾条項に違反した場合、他のいかなる権利に影響を与えることなく、Kiwi Enterpriseは本ライセンス契約を解除することができます。その場合、本ソフトウェアおよび登録キーを含むすべての付属物およびその複製を破棄するものとします。

所有権

本ソフトウェア製品およびKiwi Enterprises社のWebサイトにて公開しているすべての情報は著作権によって保護され、その所有権はKiwi Enterprise社に帰属するものとします。よって、Kiwi Enterprises社の書面による事前の承認を得ず、いかなる形式においても複製、再生産、改変、発行、アップロード、投稿、転送、配布などの行為はできません。

承認を得たい場合は、Kiwi EnterpriseのWebサイトのサポートページに記載されている連絡先までご連絡ください。

ソフトウェア製品ライセンス

本ソフトウェア製品は著作権法ならびに著作権に関する国際条約、その他知的財産法および関連条約による保護を受けています。本ソフトウェアはライセンス許諾による使用許可を与えるものであり、製品そのものが販売されるわけではありません。

免責事項

本ソフトウェア製品は、市場性、特定目的との適合性、権利侵害がないことなどの点を含む(ただし、必ずしもこれらに限定されない)明示または暗示の保証をすることなく、現状で提供するものとします。明示保証の例外範囲を認めていない、あるいは適用しない一部の国や地域では、上記の例外事項すべてが適用されないことがあります。

本ソフトウェアには技術上の間違いや誤字・脱字が含まれている可能性があり、これらの修正・変更・更新などは予告なく行うものとします。

また、Kiwi Enterprisesは本ソフトウェアに関わる改良やその他の変更を随時予告なく行います。

危険度の高い活動での使用禁止

本ソフトウェアは障害対策が施されておらず、フェールセーフ機構を要するような危険な環境での使用や再販を想定して設計、生産されていません。核施設での稼働、航空機航行/通信システム、航空管制システム、直接的な人命救助装置、武器システム等がこれに該当します。また、本ソフトウェアが使用できないことによって直接・間接に人命を脅かし、傷害に繋がる危険がある、あるいは重大な肉体的環境的ダメージを与えるおそれのある、いかなる環境およびシステムが含まれます。

Kiwi Enterpriseでは、危険度の高い活動における本ソフトウェアの使用に関していかなる明示的暗示的保証をしないことを明言します。

派生的損害に対する免責

適用される法律が許容する最大範囲において、いかなる場合においてもKiwi Enterprise社またはソフトウェアの制作者が、本ソフトウェアの使用または使用できないことによって生じる(商業上の損失、中断、商情報の喪失、その他いかなる金銭的損失を含むが制御できない)損害に対して、たとえKiwi Enterprise社がそのような損害の可能性について言及していた場合であっても、いかなる責任を負うことはないものとします。

1.7 免責条項

本プログラムは無償で提供されるフリーウェアであり、その動作・効果・結果等に対する何の保証もいたしません。製品自体の不具合ならびに使用や使用方法の誤りによって生じたいかなる問題に対し、ソフトウェア著作者に責任はないものとします。

本ソフトウェアの著作権は1998 – 2006までKiwi Enterprises社が有しております。

本プログラム(Kiwi Syslog Daemon) の使用にあたっては、上記の免責条項に同意するものとします。

1.8 謝 辞

Kiwi Syslog Daemonの前バージョンのユーザーの方から多数の激励のメールをいただき、真にありがとうございます。お寄せいただいたフィードバックやご提案に感謝し、これからもユーザーのニーズに合う改良を行っていきます。

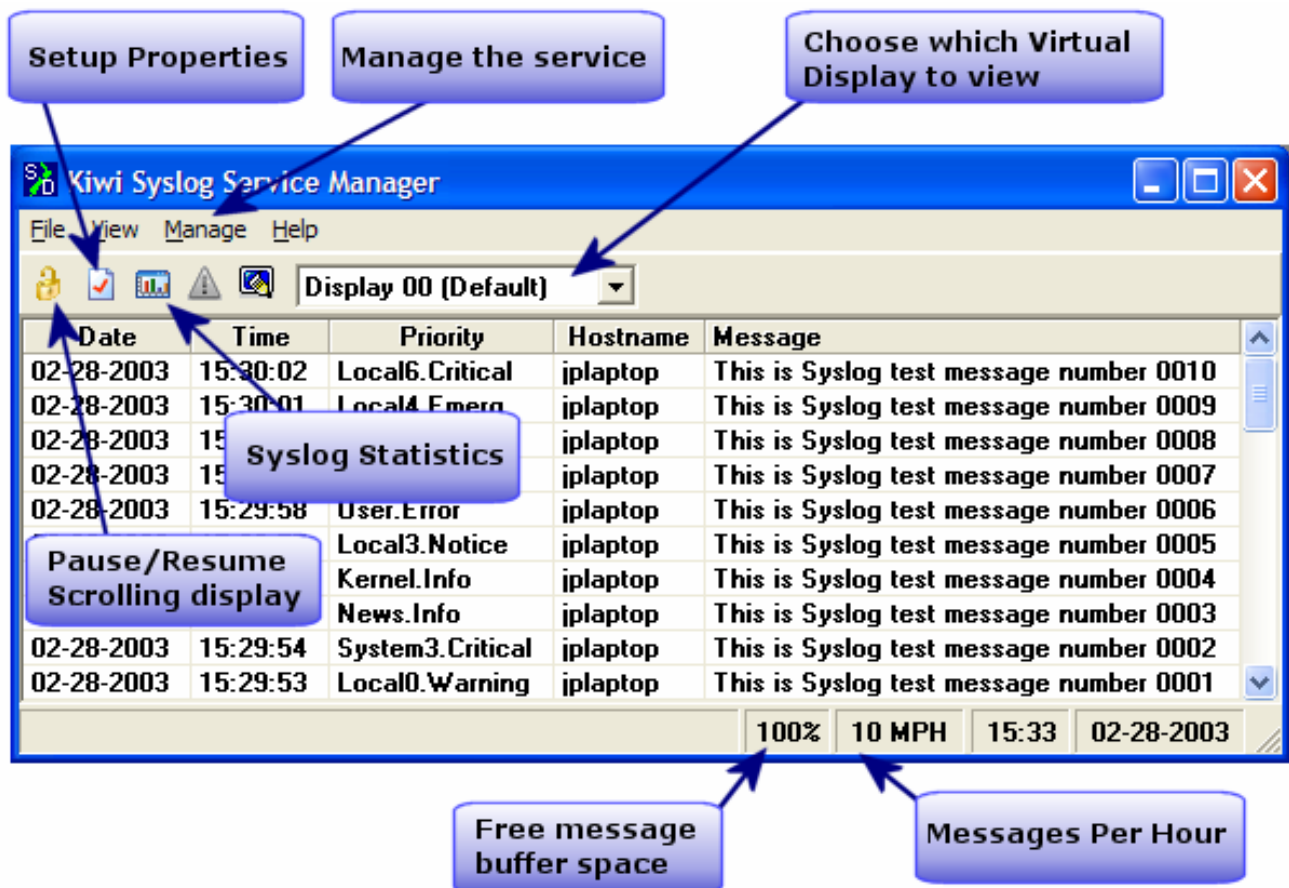
正規登録版を購入していただき製品の改良をサポートしていただいたすべてのユーザーに感謝いたします。

*Kiwi Enterprises*チーム

2 メイン表示ウィンドウ

2.1 メイン表示ウィンドウ

Kiwi Syslog Daemonを起動して最初に表示されるメイン表示ウィンドウ:



2.2 Fileメニュー

2.2.1 Setup ([Ctrl]+[P]、設定)

Kiwi Syslog Daemon Setup 画面が開きます。この画面からsyslogコンフィグレーションの設定を行います。

2.2.2 Send Test message to local host ([Ctrl]+[T]、テストメッセージ送信)

ローカルホスト(127.0.0.1)にUDP syslog メッセージを送信し、プログラムが機能的に正常であることを確認します。このときメッセージはSyslogの受信を待機しているポートに向けて送られます。プログラムのTCP設定の確認にはKiwi SyslogGenをお使いください。次のWebサイトから入手できます。

<http://www.kiwisyslog.com>

次のようなテストメッセージが送信されます。

Kiwi Syslog Daemon - Test message number 0001

末尾の番号はテストが実行されるたびに1ずつ増加します。

2.2.3 Purge (パージ)

次の内容をクリアします：

- Eメールログ(InstallPath\SendMailLog.txt)
- エラーログ(InstallPath\Errorlog.txt)
- 内部syslogメッセージキュー(1000メッセージまで)
- 内部Eメールキュー(1000メッセージまで)
- 失敗したルックアップファイル(InstallPath\MIBs\UnknownIODs.txt)

2.2.4 Debug options (デバッグ オプション)

下記のオプションを選択できます。

- Enable Syslog Debug (全受信データをInstallPath\Syslogd-debug.txtに記録します)
- Reset Syslog socket (待ち受けソケットをクローズし、データをクリアし再びソケットをオープンします)
- View the message buffer (キューのメッセージを表示します)
- View mail buffer (キューのメッセージを表示します)

2.2.4.1 Create Tech-Support File (Zip) (サポートファイルの作成)

問題の診断をするために必要な情報を取得するためのファイルを作成します。

作成されるファイル(C:\Program Files\Syslogd\Syslogd_TechSupport.zip)には次に挙げるどれか、あるいはすべてのファイルが圧縮されています。

- **ErrorLog.txt** - Syslog Daemonのエラーログ(このファイルはエラーログの数だけ作成されるため、総サイズが1MBを超える可能性があります。)
- **Syslog_Daemon_Settings.ini** - Syslog Daemonの設定ファイル
- **DNS-debug.txt** - Syslog DNS/NetBIOS詳細デバッグファイル
- **Syslogd-debug.txt** - Syslog受信メッセージのデバッグファイル
- **Syslogd_Startup.txt** - Syslogの起動デバッグファイル(スタンダード版)
- **Syslogd_Service_Startup.txt** - Syslog Serviceの起動デバッグファイル(サービス版)
- **Syslogd_Manager_Startup.txt** - Syslog Managerの起動デバッグファイル(サービス版)
- **KRDP_Sessions.ini** - Kiwi Reliable Delivery Protocol (KRDP)セッションファイル
- **CacheSettings.ini** - Kiwi Reliable Delivery Protocol (KRDP)キャッシュ設定ファイル
- **install.log** - Kiwi Syslog Daemonインストーラーログファイル(スタンダード/サービス版共通)
- **StaticHosts.txt** - DNS名前解決固定ホストファイル
- **Unknown_OID_list.txt** - MIBルックアップの不明または未解決OIDリスト
- **Standard-YYYYMMDDHHNNS-DebugLogN.txt** - Syslog Debugバージョンのみ: スタンダード版の詳細デバッグファイル
- **Manager-YYYYMMDDHHNNS-DebugLogN.txt** - Syslog Debugバージョンのみ: サービス版(Manager)の詳細デバッグファイル
- **Service-YYYYMMDDHHNNS-DebugLogN.txt** - Syslog Debugバージョンのみ: サービス版(Service)の詳細デバッグファイル

2.2.5 Export settings to INI file (設定情報をINIファイルにエクスポート)

INIファイルにプログラムの構成を保存します。

このファイルを他のシステムに転送し、その設定を | File | Setup | Defaults/Import/Export オプションで取り込むことができます。

Kiwi Enterpriseのサポートスタッフに報告したい問題がある場合は、詳細を下記のページからアクセスできるサポートフォームに記入し、エクスポートしたINIファイルを添付して送信してください。

<http://www.kiwisyslog.com/support/>

2.2.6 Exit (終了)

プログラムを終了します。スタンダード版ではプログラムを終了するとメッセージの受信もロギングも停止します。システムをログオフしてから受信、ロギング、メッセージ処理を継続する必要がある場合はサービスとしてインストールしてください。

WindowsNTサービスとしてインストールできるのはWindows NT4, 2000, XP Profesisonal, 2003のみです。

上記以外のOS上にKiwi Syslog Daemonをインストールしようとする、インストール時に表示される Install Kiwi Syslog Daemon as a Service というメニューは使用できません。

Display オプションの **Minimize to system tray on [X] button** がチェックされていると、フォーム右上にある [X] ボタンでプログラムを閉じることができなくなります。その場合は、システムトレイポップアップメニューの **File** から **Exit** を選択してプログラムを閉じてください。

2.3 Edit (編集)メニュー

2.3.1 Select All (全て選択)

このオプションは現在表示されているすべてのsyslogメッセージを選択します。

このオプションを使った後、選択したメッセージを Copy selected items to the clipboard メニューまたは[Ctrl] + [C]を押してクリップボードにコピーできます。

2.3.2 Copy selected items to the clipboard (選択した項目をクリップボードにコピー)

現在選択されているsyslogメッセージをクリップボードにコピーします。

選択するためには、表示を中断し、コピーしたいメッセージのセルをクリックして反転表示状態にし [Ctrl] + [C] を押します。

2.4 View (ビュー)メニュー

2.4.1 View syslog statistics (syslog統計の表示)

メッセージカウンターとトレンドグラフを含むsyslog統計ウィンドウを表示します。

2.4.2 View e-mail log file (Eメールログファイルの表示)

メモ帳で送信済みメールメッセージのログファイルを表示します。

メールログファイルの名前と場所は次のとおりです。

Kiwi Syslog Daemonをインストールしたフォルダ\SendMailLog.txt

2.4.3 View error log file (エラーログファイルを表示)

メモ帳でロギングエラーを記録したエラーログファイルを表示します。

エラーログファイルの名前と場所は次のとおりです。
Kiwi Syslog Daemonをインストールしたフォルダ\Errorlog.txt

2.4.4 Adjust width to fit screen (画面幅の自動調節)

Kiwi Syslog Daemonのメインウィンドウをディスプレイ幅いっぱいに広げて表示します。

2.4.5 Clear display (画面消去)

選択した Display に表示されている全メッセージを削除します。

2.4.6 Highlighting Options (ハイライト表示オプション)

正規登録版でのみ使用できます。

画面内に表示されるメッセージごとに適用されるハイライト表示ルールを作成できます。このルールは上から順に適用され、ルールにマッチするsyslogメッセージに指定したハイライト表示が適用されます。

Highlight Items:

表示されるsyslogメッセージごとに適用されるハイライト表示ルール、検索対象のsyslogメッセージフィールド、検索対象の文字列パターン、適用される効果のリストです。ルールはリストの左端にあるチェックボックスをオン/オフすることによって有効/無効を切り替えることができます。[Field]列のドロップダウンリストに表示されるフィールド名はメイン表示ウィンドウの列名(例: Date, Time, Priority, Hostname, Message)に該当します。ハイライト表示ルールはリストの右側にあるツールバーのボタンをクリックして追加/削除できます。ルールの適用順序はこのツールバーの上矢印と下矢印を使って変更できます。

注：このオプションを初めて表示しようとする時、"No highlighting rules have been found. Do you want to create some default rules based on Syslog Priorities?"(ハイライト表示ルールがありません。syslogの優先度に基づいたデフォルトのルールを作成しますか?) というメッセージが表示されることがあります。[Yes]をクリックするとsyslogの優先度に基づいたデフォルトのルールが作成され、表示されます。図1を参照してください。

String to match:

選択したsyslogメッセージフィールド内で検索する文字列パターンを指定します。

[Regular Expression]	検索対象の文字列が正規表現である場合チェックします。 (Regular Expression(正規表現)に関する項を参照)
[Invert Match]	文字列が見つからない場合に効果を適用する場合チェックします。
[Ignore Case]	検索パターン(マッチする文字列)の大文字小文字を区別しない場合チェックします。

Highlight Effects:

[Apply Foreground Color]	選択した文字色を適用する場合チェックします。 チェックされていない場合、現在の文字色が使用されます。
[Apply Background Color]	選択した背景色を適用する場合チェックします。 チェックされていない場合、現在の背景色が使用されます。
[Bold Font]	太字にする場合チェックします
[Italic Font]	イタリックにする場合チェックします。
[Underline Font]	下線を引く場合チェックします。
[Selected Icon]	現在のsyslogメッセージに効果が適用される場合に表示されるアイコンです。

Icons:

図1のアイコンは(デフォルトで) Kiwi Syslogに内蔵されているアイコンです。 <Program Files>\Syslogd\Iconsディレクトリに入れておけば他のアイコンも使用できるようになります。アイコンリストはプログラムの起動時にロードされます。そのため新しいアイコンを追加した場合はKiwi Syslogを再起動する必要があります。再起動後に新しいアイコンがこのリストに表示されません。

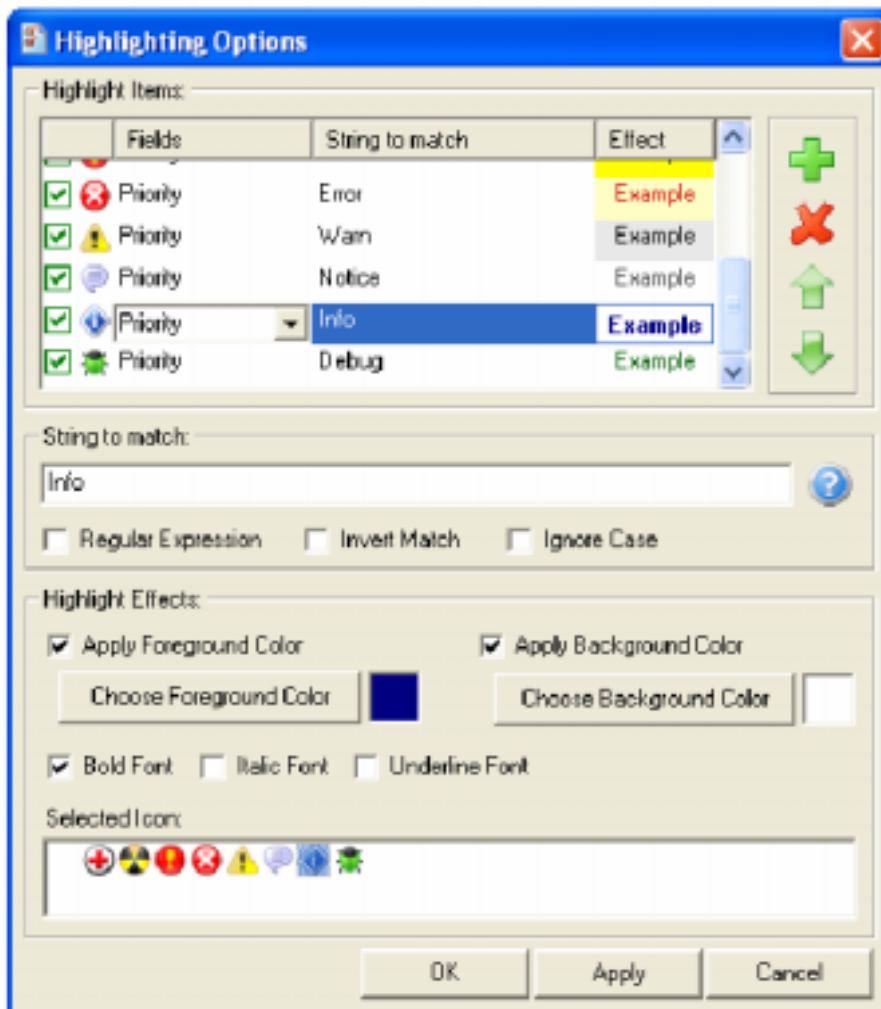


図1 - Kiwi Syslog Daemon Highlighting Options

2.4.7 Choose font (表示フォント選択)

メッセージ表示のフォント名、スタイル、カラー等を選択します。

ASCII文字以外は空白あるいは で表示されますが、これはフォントが必要なユニコード文字を含んでいないことをあらわします。

MS OfficeはArial MS Unicodeになっています。このフォントは希望するすべてのユニコード字体を含んでいます。残念ですがこのフォントは再配布されず、MS Office所有者だけが利用可能です。

代案としていくつかの無料ユニコードフォントが以下のリンクより入手できます。

<http://www.unicode.org>

http://www.travelphrases.info/gallery/all_fonts.html

ほとんどの無料フォントは字体のサブセットです。表示したい言語の字体を含む最適なフォントを選択してください。

2.5 Manage (管理)メニュー

2.5.1 Manage (管理)メニュー

サービス版でのみ表示されます。

Kiwi Syslog Daemonサービスマネージャからプログラムのサービス部分の管理とコントロールができます。

2.5.2 Install the Syslogd service (Syslogdサービスのインストール)

Kiwi Syslog DaemonをWindows NT4/2000/XP/2003のサービスとしてインストールします。

サービス版は一回インストールするだけで他の作業をする必要はありません。

インストール後、**Manage** の **Start the syslogd Service** メニューオプションを選択してサービスを開始してください。

2.5.3 Uninstall the Syslogd service (Syslogdサービスのアンインストール)

Kiwi Syslog Daemonサービスをアンインストールします。

アンインストールを行う前に必ずサービスを停止してください。

サービスをアンインストールしたら、**[コントロールパネル]**の**[アプリケーションの追加と削除]**でアプリケーションを削除します。

2.5.4 Start the Syslogd service (Syslogdサービスの開始)

Syslogdサービスを開始します。

サービスが開始(実行)されると、メッセージの受信、記録、転送が開始されます。

サービスが実行中かどうかは **Manage** の **Ping the Syslog service** メニューで確認できます。

2.5.5 Stop the Syslogd service (Syslogdサービスの停止)

Syslogdサービスを停止します。

サービスを停止するとプログラムの実行は止まります。メッセージの記録は止まり、表示もされません。

サービスは **Manager** からの **Ping** またはどのような通信にも応答しません。

注：サービス停止まで20秒くらいかかります。

2.5.6 Ping the Syslogd service (SyslogdサービスにPing)

Syslogdサービスにテストメッセージを送り応答を待ちます。5秒以内に応答が無い場合、サービスが停止中かインストールされていないことを示します。

結果はメインウィンドウ下部のステータスバーに表示されます。

Ping応答があれば "The Syslogd Service is Alive!" と表示されます。

2.5.7 Show the Syslogd service state (Syslogdサービス状態の表示)

現在のサービスの状態をチェックします。

Uninstalled(インストールされていない)、Running(実行中)、Stopping(停止中)、Not Responding(無応答)のいずれかが結果として表示されます。

2.5.8 Debug options(デバッグオプション)メニュー

2.5.8.1 Display the Service version (サービスのバージョン表示)

バージョンがService Managerのバージョンと同じか確認します。サービスのバージョン番号を表示させることができます。

バージョン番号はステータスパーウィンドウに表示されます。

2.5.8.2 Get diagnostic information (診断情報の入手)

サービスの障害回復が必要ないろいろな段階で、Service Managerに全情報を送ります。

データはクリップボードにコピーされますのでEメールやメモ帳に貼り付けることができます。

Kiwi Syslog Daemonのサービスに問題があったら、このオプションで得られる診断情報を確認してください。

2.5.8.3 Reset the Syslogd service (Syslogdサービスリセット)

プログラムやOSに問題は無いがサービスが停止し、理由の分からない問題が発生することがあります。このオプションでサービスを再起動し、初期状態に戻すことができます。

このオプションが問題を起こすことはありませんが、サービスリスタート時に2,3のメッセージ喪失が発生する可能性があるので注意してください。

このオプションが完了するまでに3秒かかります。

受信ソケット、つまりサービスのWinsockがリセットされます。

2.5.8.4 Clear the service DNS Cache (DNSキャッシュのクリア)

サービスはIPアドレスのホスト名への名前解決を行いますので、DNSキャッシュはネットワークトラフィックを減少させます。

Service ManagerのDNSキャッシュをクリアすると、サービスのキャッシュもクリアされます。

このオプションは手動で強制的にサービスキャッシュをクリアする際に使用します。

2.5.8.5 Apply new settings to Syslogd service (新しい設定の適用)

レジストリから現在のSyslogd設定を読み込み、その設定でサービスを開始します。

新しい設定を適用したことを確認したい場合にこのオプションを使用してください。

サービスが新しい設定を使用しているかどうかはステータスバーに表示されます。

2.5.8.6 Retrieve last messages (最終メッセージの取得)

バーチャルディスプレイの現在の全メッセージを送信するよう要求します。これはService Managerが起動したとき自動的に実行されます。

2.5.8.7 Send keep alive (キープアライブメッセージの送信)

Service Managerは1分ごとに「現在動作中である」ことを示すメッセージ(キープアライブメッセージ)をサービスに送っています。これにより、サービスはメッセージを実行中のService Managerに送るか否かを判別します。サービスが3分間キープアライブメッセージを受信しない場合、Service Managerへのメッセージ送信を停止します。こうすることによってService Managerが実行されていない時のCPU使用率とネットワークトラフィックを抑えています。

このオプションを使用すると、サービスにキープアライブメッセージが送信されます。この機能はデバッグ目的でのみ使用してください。

2.6 Help (ヘルプ)メニュー

2.6.1 Kiwi Syslog Help (ヘルプ、F1)

ヘルプファイルが開きます。

2.6.2 Help Topics (ヘルプトピックス)

ヘルプファイルの目次が開きます。

2.6.3 Online FAQ (オンラインFAQ)

Webブラウザで <http://www.kiwisyslog.com> のFAQが開きます。

2.6.4 Request a 30 day trial key (30日間トライアルキーの申請)

<http://www.kiwisyslog.com/trial> が開きます。このページまたは <http://www.jtc-i.co.jp> から30日間有効なトライアルキーを申請できます。

トライアルキーを使用すれば正規登録版のすべての機能を評価できます。

2.6.5 Purchase the registered version (正規登録版の購入)

<http://www.kiwisyslog.com/register.htm> が開きます。このページまたは <http://www.jtc-i.co.jp> から正規登録版のプログラムを購入できます。

2.6.6 Enter the registration details (ライセンスの登録、F2)

現在の登録状況を表示し、ライセンスコードを登録します。この操作をすることによってフリーウェア版のプログラムが正規登録版に自動的にアップグレードされます。

2.6.7 Make a suggestion or report a bug (バグレポート作成)

Kiwi社へのご要望や障害報告を行うためのサポートページが開きます。ここから必要なフォームにアクセスしてください。
<http://www.kiwisyslog.com/support/>

フォームに必要事項を記入して(英語)、Submit Enquiry ボタンを押すとEメールが弊社まで送信されます。

2.6.8 Join the mailing list (メーリングリストへの参加)

メーリングリストに参加するためのフィードバックフォームが開きます。
<http://www.kiwisyslog.com/support/>

2.6.9 About Kiwi Syslog (Kiwi Syslog Daemonについて)

About Kiwi Syslog Daemon ウィンドウが開きます。

著作権情報、バージョン、ライセンス登録内容、Kiwi社のWebサイトへのリンクなどが表示されます。

3 Syslogプロパティの設定

3.1 Syslog Daemon初期設定ガイド

Kiwi Syslog Daemonを初めて起動したときはデフォルト設定が使用されます。デフォルトでは、すべてのメッセージがウィンドウに表示され、SyslogCatchAll.txt というログファイルに記録されます。このログファイルはKiwi Syslog Daemonをインストールしたディレクトリの \Logs ディレクトリにあります。

File の Setup メニューあるいは[Ctrl] + [P]でこれらの設定を変更できます。

File の Setup から Defaults/Import/Export メニューオプションの Load default Rules and Settings ボタンをクリックすれば、いつでもデフォルト設定に戻すことができます。

3.2 キーボードの使用方法

[Delete]	選択したルール、フィルター、アクション、アーカイブスケジュールの削除
[Insert]	新しいルール、フィルター、アクション、アーカイブスケジュールの追加 (選択アイテムはルール、フィルター、アクション、アーカイブのみ)
[Ctrl-V]	ルール、フィルター、アクション、アーカイブスケジュールの貼り付け (選択アイテムはルール、フィルター、アクション、アーカイブのみ)
[Ctrl-C]	選択したルール、フィルター、アクション、アーカイブスケジュールのコピー
[F2]	選択したルール、フィルター、アクション、アーカイブスケジュールの名前変更
[F4]	フィルター、アクション、アーカイブスケジュールに対する自動命名
[Home]	ツリー先頭にカーソル移動
[End]	ツリー末尾にカーソル移動
[Enter]	現在の選択位置でツリーを展開/折り畳み(マウスのダブルクリックと同じ)
[スペース]	選択したルール、フィルター、アクション、アーカイブスケジュールの有効/無効切り替え
[Shift +]	選択したルール、フィルター、アクション、アーカイブスケジュールを上移動
[Shift + [選択したルール、フィルター、アクション、アーカイブスケジュールを下移動

3.3 Rules / Filters / Actions (ルール/フィルター/アクション)

3.3.1 ルールエンジンの動作

最大100のルールを定義できます。各ルールは最大100のフィルターと100のアクションを定義することができます。

受信したsyslogメッセージはルールで処理されます。ルールは上から順に適用されていきます。ルールの順序はツールバーに表示されている上下の矢印ボタンを使って調整できます。

ルールが適用されるたびに、メッセージに指定したフィルターがかけられます。フィルターは上から順にかけられていきます。どのフィルターにも合致するメッセージが見つからなかった場合、そのルール処理をストップし次のルールに移ります。フィルター条件に合致するメッセージが見つかったら、指定した1つもしくは複数のアクションが上から順に実行されます。

ルールに含まれているすべてのアクションが完了すると、リストの次のルール処理を開始します。すべてのルール処理を終了すると次のsyslogメッセージの受信を待ち、新しいメッセージの処理を最上位のルールから行います。

各ルール、フィルター、アクションには分かり易い名前を付けておいてください。名前を編集するには、F2をクリックするかメニューを右クリックします。名前は重複しても構いませんが、どのような動作をするのかを表すような名前を付けておくといでしょう。名前は25文字までです。

ルールにフィルターが定義されていない場合はすべてのメッセージが通されます。

デフォルトでは、初期設定で「Default」という名前のルールが一つ定義されています。フィルターは定義されていません。そのためすべてのメッセージが通されます。受信した全メッセージに対して2つのデフォルトアクション「Display」および「Log to file」が実行されます。すべてのメッセージが表示され、Kiwi Syslog Daemonをインストールしたフォルダの下にある\Logsディレクトリ内のSyslogCatchAll.txtファイルに記録されます。

ルール、フィルター、アクションの追加/削除/名前変更については、「キーボードの使用方法」の項を参照してください。

3.3.2 Filter Type (フィルタータイプ)

3.3.2.1 Simple filter (シンプルフィルター)

概要

簡単な1行のフィルターです。メッセージに含まれている1つまたは複数のテキストやIPアドレスのマッチングに有効です。複数の検索文字列を " " で囲んで指定すると、文字列Aまたは文字列Bのどちらかに一致するメッセージの検索が可能です。

Include : "link up" "link down"

上記のように指定すると link up もしくは link down に対するマッチングが行われます。

詳細

シンプルフィルターでは検索対象の文字列を1行で指定します。複数の文字列を指定する場合、各検索文字列を " " で区切り1行内に並べて指定します。フィルターは指定された文字のいずれかのマッチングを行います。指定文字列の関係はORになります。

[C]ボタンにより大文字小文字を区別するかどうかを指定します。

[S]ボタンにより部分一致検索か完全一致検索かを指定します。

例:



メッセージテキストのどこかにいずれかの文字列が含まれていれば、フィルター結果は真となります。

注: [S]ボタンが押下げられている場合、部分一致検索になります。テキストのどこかに検索文字列が含まれているものすべてが対象となります。

すべての文字列は二重引用符(" ")で囲み、1行に並べて指定します。各文字列の関係はORになります。

上記のようにフィルターを指定した場合、大文字/小文字を問わずPOP3、SMTP、MAPIという文字列のいずれかがメッセージテキストに含まれていればフィルターは真となります。



メッセージテキストが指定文字と完全に一致していれば、フィルター結果は真となります。

注: [S]ボタンが押下げられていない場合、検索文字列とメッセージテキストは一文字ごとに完全に一致している必要があります。[C]ボタンが押下げられている場合は、大文字小文字も完全に同じでなければなりません。

上記のようにフィルターを指定した場合、The link is down というメッセージテキストがあればフィルターは真となります。

3.3.2.2 Complex filter (複合フィルター)

概要

複数行にわたる複雑なフィルターです。メッセージ内に指定したテキストやIPアドレスが含まれているか含まれていないかを複雑に組み合わせて検索したいときに使用します。複数の検索文字列をそれぞれ引用符(" ")で囲んで指定し、ブール演算処理を行います。

AND、OR、NOT-OR、NOT-AND演算と含まない文字列の指定 (Exclude) が可能です。

詳細

複合フィルターでは複数の検索文字列を指定できます。検索文字列は[(A または B) および (C または D)]しかし[(E または F) および(GまたはH)]のように互いに組み合わせることで複雑なマッチング処理を実行できます。

各検索文字列は" "で囲み、1行に並べて指定します。フィルターは指定された文字列のマッチングを行います。各文字列の関係はORになります。

[C]ボタンにより大文字小文字を区別するかどうかを指定します。
[S]ボタンにより部分一致検索か完全一致検索かを指定します。

フィルターマッチングでは空白のフィールドは無視されます。

最初の2つのフィールドが空白で、3,4番目でテキストを指定すると指定した文字列を含まないテキストの検索を実行します。一致するテキストが見つからなかった場合に結果は真となります。

例：

Include:	<input type="text" value='"fox" "quick" "hello"'/>	<input type="button" value="C"/>	<input type="button" value="S"/>
And:	<input type="text" value='"over" "the"'/>	<input type="button" value="C"/>	<input type="button" value="S"/>
Exclude:	<input type="text" value='"hello"'/>	<input type="button" value="C"/>	<input type="button" value="S"/>
And:	<input type="text" value='"brown"'/>	<input type="button" value="C"/>	<input type="button" value="S"/>

注 [S]ボタンが押下げられていると部分一致検索になります。テキストのどこかに検索文字列が含まれているものすべてが対象となります。

すべての文字列は二重引用符(" ")で囲み、1行に並べて指定します。各文字列の関係はORになります。

上記のようにフィルターを指定した場合、大文字小文字を問わず fox、quick、hell oのいずれかの文字列がメッセージテキストに含まれ、さらに over あるいは the を含むが hello および brown を含まないメッセージテキストがあれば、フィルターは真となります。

Include:	<input type="text"/>	<input type="button" value="C"/>	<input type="button" value="S"/>
And:	<input type="text"/>	<input type="button" value="C"/>	<input type="button" value="S"/>
Exclude:	<input type="text" value='"chicken" "duck"'/>	<input type="button" value="C"/>	<input type="button" value="S"/>
And:	<input type="text"/>	<input type="button" value="C"/>	<input type="button" value="S"/>

上記は含まない文字列を指定する場合の例です。

chickenあるいはduckが含まれていないメッセージテキストがあれば、結果は真となります。最初の2つのフィールドが空白(空白)であることに注意してください。これらのフィールドはフィルター処理で無視されます。

注:

[And:]フィールドは指定する必要がなければ空白のまま構いません。

[And:]フィールドに文字列を指定した場合はその上のフィールドにも何らかの文字列を入力する必要があります。

3.3.2.3 Regular Expression filter (正規表現フィルター)

概要

Unixタイプの標準表現一致を使います。テキストの数字の範囲、文字やシンボルで合致条件を作るのに有効です。テキスト中の位置の指定なども可能で、最も自由度の高いテキスト検索方法です。

AND、OR、NOT-OR、NOT-AND演算と含まない文字列の指定 (Exclude) が可能です。

詳細

正規表現フィルターではUnixタイプの正規表現引数を用いて “どこ” で “どんな” テキストを検索するのかを厳密にコントロールできます。

各検索文字列は" "で囲み、1行に並べて指定します。フィルターは指定文字列のいずれかに合致するかを検索します。各文字列の関係はORになります。

[C]ボタンにより大文字小文字を区別するかどうかを指定します。

フィルターによるマッチ処理では空白フィールドは無視されます。

最初の2つのフィールドが空白で、3,4番目でテキストを指定すると指定した文字列を含まないテキストの検索を実行します。一致するテキストが見つからなかった場合に真となります。

例:

Include:	"^The"	C
And:	"dog\$"	C
Exclude:	"chicken"	C
And:	"duck"	C

すべての文字列は二重引用符(" ")で囲み、1行に並べて指定します。各文字列の関係はORになります。

上記のように指定した場合、Theで始まり(大文字小文字の区別あり)dogで終わるメッセージテキストでchickenやduckを含まないものがあれば、結果は真となります。

Include:		C
And:		C
Exclude:	"^The"	C
And:	"dog\$"	C

上記は含まない文字列を指定する場合の例です。

先頭がTheで始まらずdogで終わらないメッセージテキストがあれば、フィルターは真を返します。最初の2つのフィールドが空白(空白)であることに注意してください。これらのフィールドはフィルター処理で無視されます。

注:

[And:]フィールドは指定する必要がなければ空白のまま構いません。

[And:]フィールドに文字列を指定した場合はその上のフィールドにも何らかの文字列を入力する必要があります。

正規表現構文:

フィルターで認識される正規表現構文に使用できる特殊文字および文字列を以下に挙げます。

文字	説明
^	文字列の始まり
\$	文字列の終わり
.	任意の文字
?	直前の文字を0回あるいは1回使った文字列。例: 10? は 1 と 10 をマッチする。

*	直前の文字を 0 回あるいは1回以上繰り返した文字列。例：10* は1、10、1000 などをマッチする。
+	直前の文字を1回以上繰り返す。例：10+ は10、1000 などをマッチする。
\	次の文字をエスケープ。構文に特殊文字を含める場合に必須。例：*+\\ は .*+\\ にマッチする。特殊印字不能文字(タブなど)をエンコードする際にも必要。
x y	x か y のどちらかにマッチ。例：z wood は z または wood にマッチする。(z w)oo は zoo または wood にマッチする。
{n}	n は非負整数。直前の文字をn回繰り返している文字列をマッチする。例：o{2} はBobの o にマッチしないが、fooooood の最初の2つの o にマッチする。
{n,}	n は非負整数。直前の文字を最低n回繰り返している文字列にマッチする。例：o{2,} は Bob の o にマッチしないが、fooooood のすべての o にマッチする。o{1,} は o+、o{0,} は o* と同等
{n,m}	m と n は非負整数。直前の文字を最低n回、最高 m 回繰り返している文字列にマッチする。例：o{1,3} は fooooood の最初の3つの o にマッチする。o{0,1} は o? と同等
[xyz]	文字セット。括弧内の文字が含まれているものすべてにマッチ。例：[abc] は plain の a にマッチ
[^xyz]	否定文字セット。括弧内以外の文字が含まれているものすべてにマッチ。例：[^abc] は plain の p にマッチ
[a-z]	文字の範囲。指定した範囲に含まれる文字にマッチ。例：[a-z] はアルファベット小文字の a から z までの文字にマッチ
[^m-z]	否定文字の範囲。指定した範囲に含まれない文字にマッチ。例：[m-z] は m から z 以外の任意の文字にマッチ
\b	語句の境界 すなわち語句の区切り位置やスペース(空白)にマッチ。例：er\b は never の er にマッチするが verb の er にマッチしない
\B	語句の境界以外にマッチ。例：ea*\rB は never early の ear にマッチ
\d	数字にマッチ。[0-9] と同等
\D	数字以外の文字にマッチ。[^0-9] と同等
\f	改ページにマッチ
\n	改行にマッチ
\q	引用符または ASCII 34
\r	キャリッジリターンにマッチ
\s	スペース、タブ、改ページ等空白類文字にマッチ。[\f\n\r\t\v] と同等
\S	非空白類文字にマッチ。[^ \f\n\r\t\v] と同等
\t	タブにマッチ
\v	垂直タブにマッチ
\w	下線付きの文字にマッチ。[A-Za-z0-9_] と同等
\W	文字以外の記号にマッチ。[^A-Za-z0-9_] と同等
\num	正の整数にマッチ。記憶済みマッチに戻って参照。例："(.)\1 は2つの連続した同一文字にマッチ
\n	8進エスケープ値である n にマッチ。8進エスケープ値は 1 桁、2 桁または 3 桁の値。例：\11 および \011 は両方ともタブ文字にマッチ。\0011 は \001 および 1 と同等。8進エスケープ値は256以下の値を指定すること。これを超える値を指定すると最初の2桁のみが対象となる。正規表現ではASCIIコードを使用可能

\xn 16進エスケープ値である n にマッチ。16進エスケープ値は2桁。例：\x41 は A にマッチ。 \x041 は \x04 および 1 と同等。正規表現ではASCIIコードを使用可能

例:

"^stuff"	stuff で始まる任意の文字列"
"stuff\$"	stuff で終わる任意の文字列"
"o.d"	old, odd, ord 等
"o[l]d"	old または odd のみ
"o[^l]d"	odd, ord, ではあるが old ではない
"od?"	o 又は od
"od*"	o, od, odd
"od+ "	od, odd 等
"\."	小数点(エスケープ文字が必要)
"[A-Z][a-z]*"	任意の大文字語句
"[0-9]+ "	任意の数字列
"[1-9]+ [1-9]*"	0で始まらない任意の数字列
"[+ -]?[0-9]* [\.]?[0-9]*"	符号と小数点付きの任意の数字 (2つのエスケープ文字が必要)
"dst=\qLOCAL MACHINE\q"	dst="LOCAL MACHINE" を検索
"dst=\x22LOCAL MACHINE\x22"	dst="LOCAL MACHINE" を検索 Hex(22) = ASCII 34 または ("
"(z w)oo"	zoo または woo を検索

3.3.2.4 IP Address Range filter (アドレス範囲フィルター)

概要

IPアドレス範囲の一致を見ます。ホストアドレスの範囲を含むか含まないかを判断します。

詳細

含むあるいは含まないIPアドレスの範囲を指定できます。

IncludeあるいはExcludeの範囲はどちらかがブランク(空白)でも構いませんが、両方をブランク(空白)にすることはできません。

Include範囲がブランクであればフィルターはエクスクルージョンモードになります。IPアドレスがExclude値の範囲内であれば結果は真となります。

例:

The image shows a configuration interface for an IP Address Range filter. It consists of four rows of input fields, each with a label and four numeric boxes separated by dots. The first row is labeled 'Include range start:' and contains the values 203, 185, 100, and 0. The second row is labeled 'Include range end:' and contains the values 203, 185, 100, and 255. The third row is labeled 'Exclude range start:' and contains the values 203, 185, 100, and 10. The fourth row is labeled 'Exclude range end:' and contains the values 203, 185, 100, and 20.

上記のように指定した場合、IPアドレスが 203.185.100.0 ~ 203.185.100.255 の範囲内にあり、203.185.100.10 ~ 203.185.100.20 の範囲内でなければ結果は真となります。

Include range start:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>
Include range end:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>
Exclude range start:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="10"/>
Exclude range end:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="20"/>

上記は含まない範囲を指定する場合の例です。

IPアドレスが 203.185.100.10 ~ 203.185.100.20 の範囲内になれば結果は真となります。

3.3.2.5 IP Subnet Mask filter (IP サブネットマスクフィルター)

概要

ホストアドレスの含む/含まないの定義にサブネットマスクを使用できます。

詳細

IP サブネットマスクフィルターはマスクマッチングに基づいて、含むあるいは含まないIPアドレスの範囲を指定できます。

IncludeあるいはExcludeのフィールドはどちらかがブランク(空白)でも構いませんが、両方をブランク(空白)にすることはできません。

Include 範囲がブランクであればフィルターはエクスクルージョンモードになります。IPアドレスがExclude値の範囲内であれば結果は真となります。

例：

Include IP Address:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="0"/>
Mask:	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="0"/>
Exclude IP Address:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>
Mask:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>

指定したIPアドレスがMask: に指定した値とAND演算され、メッセージのホストIPと比較されます。2つのアドレスが同一サブネットであれば結果は真です。

上記のように指定すると、IPアドレスが 203.185.100.0 ~ 203.185.100.255 の範囲内であれば結果は真となります。

Include IP Address:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Mask:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Exclude IP Address:	<input type="text" value="203"/>	<input type="text" value="185"/>	<input type="text" value="100"/>	<input type="text" value="0"/>
Mask:	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>

上記は含まない範囲を指定する場合の例です。

IPアドレスが 203.185.100.0 ~ 203.185.100.255 の範囲内になれば結果は真となります。

3.3.2.6 Priority filter (プライオリティフィルター)

概要

受信メッセージのプライオリティと比較するプライオリティ値を設定できます。

詳細

各受信メッセージにはプライオリティ値が含まれています。この値はファシリティとレベルで構成されています。どのプライオリティでフィルター結果を真にするかを指定できます。

プライオリティを選択するにはファシリティとレベルの交点にあるセルをダブルクリックします。緑の球が設定され、そのプライオリティにマッチするメッセージに対するフィルター結果が真になります。

セルを選択し右クリックするとポップアップメニューオプションが表示されます。

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Mail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Daemon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Auth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Syslog	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Lpr								
News								
UUCP								

Toggle to ON
 Toggle to OFF
 Select All
 Inverse

すべてのプライオリティに緑の球を設定すると、プライオリティ値に関わらずすべてのメッセージがマッチすることになります。すべてのプライオリティをマッチさせたいのであれば、フィルターを指定する必要はありません。プライオリティフィルターが指定されていないければ、すべてのプライオリティのメッセージを通過させます。

Inverse は現在有効になっているボックスを空白にしたり、逆に空白のボックスに緑の球を追加するときに使います（有効ボックスを Inverse すると基本的に含まないプライオリティを指定するフィルターが作成されます）。

Select All ですべてのセルが選択されます。次に Toggle to OFF または Toggle to ON をクリックして緑の球の設定をオン/オフします。

例：

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Mail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Daemon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Auth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Syslog	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

上記のように設定すると、Warnig より高いレベルのすべてのファシリティのメッセージに対して真の結果となります。

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel								
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mail								
Daemon								
Auth								
Syslog								

上記のように設定すると、User ファシリティを持つすべてのメッセージに対して真の結果となります。

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User								
Mail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Daemon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Auth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Syslog	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

上記は含まないプライオリティを指定する場合の例です。

このように指定すると User ファシリティ以外のすべてのメッセージに対して真の結果となります。

3.3.2.7 Time of Day filter (時刻フィルター)

概要

現在の時刻と表内に設定された時刻を比較し、アクションの許可/拒否が判断されます。

詳細

含むあるいは含まない時刻を指定できます。

時刻（15分単位）を選択するには、時刻と曜日の交点にあるセルをダブルクリックします。緑の球が設定され、その時刻にマッチするメッセージに対するフィルター結果が真になります。

セルを選択し右クリックするとポップアップメニューオプションが表示されます。

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00:00	✓	✓	✓	✓			
00:15	✓	✓	✓	✓			
00:30	✓	✓	✓	✓			
00:45	✓	✓	✓	✓			
01:00	✓	✓	✓	✓			
01:15							
01:30							

Toggle to ON
 Toggle to OFF
 Select All
 Inverse

すべての時刻に緑の球を設定すると、メッセージの受信時刻に関わらずすべてのメッセージがマッチします。時刻フィルターが指定されていないければ、すべての時刻のメッセージを通過させます。

Inverse は現在有効になっているボックスを空白にしたり、逆に空白のボックスに緑の球を追加するときに使います（有効ボックスを Inverse すると基本的に含まない時刻を指定するフィルターが作成されます）。

Select All ですべてのセルが選択されます。次に Toggle to OFF または Toggle to ON をクリックして緑の球の設定をオン/オフします。

例：

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
07:45							
08:00		✓	✓	✓	✓	✓	
08:15		✓	✓	✓	✓	✓	
08:30		✓	✓	✓	✓	✓	
08:45		✓	✓	✓	✓	✓	
09:00		✓	✓	✓	✓	✓	
09:15		✓	✓	✓	✓	✓	

上記のように指定すると、月曜日から金曜日までの午前8時から午前9時15分までの全メッセージに対する結果は真となります。

月曜日から金曜日の午前8時から午後5時までを選択すれば、就業時間フィルターを作成できます。設定済みのセルに対して Inverse オプションを適用するとその時刻は除外するフィルターになります。例えば、月曜から金曜の午前8時から午後5時以外を指定するときに使用します。

3.3.2.8 Time interval filter (タイムインターバルフィルター)

概要

1回のトリガーから次のトリガーまで設定した時間待ちます。

ルールに定義した全フィルターの後にFlags/Countersフィルターを配値する必要があります。他のフィルターが先に処理されます。

詳細

タイムインターバルフィルターは、特定のメッセージテキスト（例えば"link down"）が見つかった時に実行される send e-mail message のような通知アクションに定義すると効果的です。1分間に接続と切断が何度も繰り返されると、通常ではそのたびに回線切断メッセージを受信します。タイムインターバルフィルターを設定すると、通知アクションが1回実行されるとX分間待ってから次のアクションが実行されるようになります。

タイムインターバルフィルターを使用した回線切断の通知例：

Rule: Link down notify
 Filters

Filter: Field=Hostname, Type=Simple.
Include: **"central-router.company.com" [S]**
Filter: Field=Msg Text, Type=Simple.
Include: **"link down" [S]**
Filter: Field=Flags/Counters, Type=Time interval
Fire this event once, then wait for **15** minutes before firing again.

Actions

Action: Send E-mail message
E-mail body: **The link has gone down, please call the helpdesk.**
Alert - %MsgText

ホスト central-router.company.com から、テキストに link down を含むメッセージを受信すると最初のフィルター (Message text) は真になります。次にタイムインターバルフィルターが処理されます。最初のタイムインターバルフィルターは真となり、指定されている次のアクションが実行されます。指定された時間のカウントダウンが始まります。上の例では15分です。同じホストから link down を含むメッセージを受信すると最初のフィルター (Message text) は再び真になります。カウントダウンタイマーがまだゼロになっていなければタイムインターバルフィルターは偽になり、次のアクションは実行されません。

このフィルターはアタックを受けたときに受信する通知Eメールの量を少なくする目的で使用することもできます。例えば、port scan detected というテキストを受信したことを知りたいが、毎回ではなく1時間に1回で良いような場合です。タイムインターバルフィルターを使用して1回実行したら次の実行まで60分間待つように設定すればよいのです。

3.3.2.9 Threshold filter (閾値フィルター)

概要

このフィルターは前のフィルターがY秒にX回の条件を満たすと実行されます。

ルールに定義した全フィルターの後にFlags/Countersフィルターを配値する必要があります。他のフィルターが先に処理されます。

詳細

Threshold フィルターはあるレベルに達したイベントについてのみ知りたい場合に有効です。例えば、port scan detected を含むメッセージを1分間に5回以上受信した時だけアラートが必要な場合などです。このことは誰かが継続的にネットワークをスキャンしていることを示している可能性があります。

ログイン試行の失敗を監視するときにも有効です。30秒に5回以上テキストに login failed が含まれるようなメッセージを受信している場合、総当りログインアタックの可能性がります。

タイムインターバルフィルターを使用した link down 通知例：

Rule: Failed login
Filters
Filter: Field=Hostname, Type=Simple.
Include: **"unixhost.company.com" [S]**
Filter: Field=Msg Text, Type=Simple.
Include: **"login failed" [S]**
Filter: Field=Flags/Counters, Type=Threshold
Filter is true if event occurs **10** times in **120** seconds.
Actions
Action: Send E-mail message
E-mail body: **Intruder Alert – Login failed 10 times in 2 minutes.**
Alert - %MsgText

ホスト central-router.company.com から、120秒に10回テキストに login failed を含むメッセージを受信するとフィルターは真になり、以降のアクションが実行されます。

このフィルターは送信される通知Eメールの量を少なくする目的で使用することもできます。Threshold フィルターを使って通知を受けるための閾値を設定すればよいのです。

Maintain individual threshold counts for each host address

チェックすると Kiwi Syslog Daemon の内部でメッセージを送信するホストごとに個別の閾値カウントが保存されます。つまり、Y秒にX回送信されたメッセージに対して標準閾値カウントを適用するのではなくホストZからY秒にX回送信されたメッセージの回数が記録されます。

以下はこの設定を利用した好例です。あるデバイス上で一定の閾値を超える portflapping が検出されると管理者にEメールで通知されます。Eメールは閾値を超えるデバイスごとに1通送信されます。閾値イベントを起動する原因となったホストまたはデバイスは %MsgHost を使ってレポート可能です。

Rule: Link Up

Filters

Filter: Field=Msg Text, Type=Simple

Include: "Link Up" [S]

Filter: Fields=Flags/counters, Type=Threshold

Filter is true is event occurs 10 times in 120 seconds,
maintain individual threshold counts for each host address.

Actions

Action: Send E-mail message

E-mail body: Port Flapping Detected - Link Up message on device '%MsgHost'
received 10 times in 2 minutes.

Device - %MsgHost

Alert - %MsgText

3.3.2.10 Timeout filter (タイムアウトフィルター)

概要

このフィルターは前のフィルターがY分にX回の条件を満たさないと実行されます。

ルール中の他の全タイプのフィルターの後にFlags/Counters フィルターが必要です。他のフィルターが先に処理されます。

詳細

タイムアウトフィルターは監視中のSyslogデバイスに何も問題が起きていないことを知りたいときに有効です。例えば、ファイアーウォールは通常1時間に200メッセージ以上を生成します。メッセージ量が突然1時間に10メッセージ以下になった時、あるいはメッセージがなくなった時にEメールで通知されます。

このフィルターは他の flags/counters のように受信メッセージにより起動されるものとは異なります。メッセージが無くなると開始されるカウントダウンタイマーにより起動されます。したがって、このフィルターが起動される時はイベントにはメッセージが関連付けられていません。その代わりにフィルター以降のアクションに渡す通知メッセージが生成されます。このメッセージは次のようなものになります。

Priority: Local7.Debug (191)

HostIP: 127.0.0.1 (localhost)

MsgText: The rule 'Rule name here' has only been matched X times in Y minutes. The threshold was set for Z times.

Rule: Firewall Monitor

Filters

Filter: Field=Hostname, Type=Simple.

Include: "firewall.company.com" [S]

Filter: Field=Flags/Counters, Type=Timeout

Filter is true if event doesn't occur 1 times in 5 minutes.

Filter: Field=Time of Day, Type= Time of Day

Monday to Friday 8:00 a.m. to 6:00 p.m.

Actions

Action: Send E-mail message

E-mail body: Firewall is not alive

Alert - %MsgText

%MsgText は次のようなテキストになります。

The rule 'Firewall Monitor' has only been matched 0 times in 5 minutes. The threshold was set for 1 times.

firewall.company.com から5分間メッセージを受信しないしていると、カウントダウンタイマーが起動します。Timeout フィルターの次に定義されているフィルターを通過すると (8:00 a.m. ~ 6:00 p.m の時間)、定義されているアクションが実行されます。このフィルターは他のフィルターのように特定のメッセージがトリガーにはなりません。カウントダウンタイマーが終わったときに限られます。現在のメッセージとして通知メッセージが生成されます。この通知メッセージはアクションとして定義されているアラートテキストなどで使用されます。

3.3.2.11 フィルター定義のインポートとエクスポート

フィルター定義は後で再利用したり、他のユーザーと共有するためにファイルにエクスポートすることができます。Import および Export ボタンを使います。

フィルターをインポートするには Import ボタンを選択します。KSDファイルをインポートするダイアログが聞かれます。

選択したフィルターをファイルに保存するにはExportボタンを選択します。フィルターファイルの拡張子は **.KSR** です。

他のユーザーにとっても有効なフィルター定義を作成したらファイルにエクスポートして support@kiwisyslog.com までEメールで送ってください。Kiwi社のWebサイトにて公開します。

3.3.2.12 Input source (入力ソース)

概要

このフィルターは現在のメッセージの入力ソースが以下のフィルターの入力ソースに一致するとトリガーされます。

選択可能な入力ソース

- UDP
- TCP
- SNMP

詳細

UDPメッセージのみをフィルターする場合：

UDPチェックボックスをチェックしTCPとSNMPチェックボックスがチェックされていないことを確認します。

TCPメッセージのみをフィルターする場合：

TCPチェックボックスをチェックしUDPとSNMPチェックボックスがチェックされていないことを確認します。

SNMPメッセージのみをフィルターする場合：

SNMPチェックボックスをチェックしUDPとTCPチェックボックスがチェックされていないことを確認します。

3.3.3 Action - Display (アクション - 表示)

メッセージを画面に表示します。

メッセージ送信先として10個の仮想画面の一つを選びます。Kiwi Syslog Daemonのメイン表示ウィンドウのドロップダウンリストからどの画面を表示するかを選びます。

File | Setup | Display メニューオプションの Modify display names ドロップダウンリストからディスプレイを選択し、フィールドに名前を入力します。その後 Update ボタンを押します。

3.3.4 Action - Log to file (アクション - ファイル記録)

3.3.4.1 Action - Log to file (アクション - ファイル記録)

選択したファイルフォーマットに従いメッセージを指定のファイルに記録します。

Log file name フィールドにログファイルのフルパスとファイル名を入力するか[...]ボタンで保存先を参照してファイルを選択します。

デフォルトのログファイル名は SyslogCatchAll.txt です。

デフォルトのパスは InstallPath\Log\ です。InstallPath にはKiwi Syslog Daemonをインストールしたフォルダのパスが入ります。

3.3.4.2 AutoSplit values (自動分割値)

AutoSplit値を使用すれば受信メッセージを複数のログファイルに分割する際にフィルターやアクションを実行する必要がなくなります。

AutoSplit値を使うには、カーソルを新しい値を挿入したい場所に置き [Insert AutoSplit value](#) リンクをクリックします。表示されるメニュー項目の中から選択します。新しい変数が現在のカーソルの位置に挿入されます。

メッセージを受信すると変数はメッセージの値に置き換えられます。例えば、%PriLevAA はメッセージのプライオリティレベルに置き換えられます。

AutoSplit値は結果が正しいファイル名になるのであれば、パスやログファイル名のどこでも使用可能です。

例：

メッセージを日付で分割する場合：

C:\Logs\MyLogFile%DateD2.txt

%DateD2 は現在の日付に置き換わります。23日であれば次のファイルに記録されます。

C:\Logs\MyLogFile23.txt

パスおよびファイル名にはAutoSplit値がいくつ含まれていても構いません。

プライオリティレベルと現在の日付に基づいてメッセージを分割する場合：

C:\Logs\%PriLevAA\MyLogFile-%DateISO.txt

パスおよびファイル名の結果例

C:\Logs\Debug\MyLogFile-2002-04-09.txt

送信ホストに基づいてメッセージを分割し、次にホストごとにプライオリティレベルで分割する場合：

C:\Logs\%HostName.%HostDomain\MyLogFile-%PriLevAA.txt

パスおよびファイル名の結果例

C:\Logs\myhost.mycompany.com\MyLogFile-Debug.txt

Run Scriptアクションを使えば、任意のVarCustomまたはVarGlobalフィールドを自動分割アイテムとして使用できます。

各%変数名は覚えなくてもメニューアイテムから選択すれば自動で値を挿入することができます。

以下に現在使用可能なAutoSplit値の全リストを掲載します。

Date値

メニュー名: ISO Date (YYYY-MM-DD)

パラメータ: %DateISO

説明: 国際日付形式 YYYY-MM-DD。先行ゼロ付き、常に10文字。

例: 2002-10-15

メニュー名: Year (YYYY)

パラメータ: %DateY4

説明: 4桁の年、常に4文字

例: 2002

メニュー名: Year (YY)

パラメータ: %DateY2

説明: 2桁の年、常に2文字

例: 02

メニュー名: Month (MM) with leading zero

パラメータ: %DateM2

説明: 先行ゼロ付きの2桁の月、常に2文字。

例: 12

メニュー名: Month (MMM) in English

パラメータ: %DateM3

説明: 英語3文字の月名、常に3文字。先頭は大文字(Jan, Feb, Mar, Apr...)

例: Nov

メニュー名: Date (DD) with leading zero

パラメータ: %DateD2
説明: 先行ゼロ付きの2桁の日、常に2文字。
例: 05

メニュー名: Day (DDD) in English
パラメータ: %DateD3
説明: 英語3文字の曜日、常に3文字。先頭は大文字(Sun, Mon, Tue...)
例: Fri

Time値

メニュー名: Hour (HH) with leading zero
パラメータ: %TimeHH
説明: 2桁の時間、常に2文字。24時間表示。3 p.m. = 15
例: 14

メニュー名: Minute (MM) with leading zero
パラメータ: %TimeMM
説明: 2桁の分、常に2文字。
例: 59

メニュー名: AM/PM indicator (AM or PM)
パラメータ: "%TimeAMP
説明: 2文字の時刻、常に2文字。00:00 ~ 11:59 = AM. 12:00 ~ 23:59 = PM
例: AM

Priority値

メニュー名: Level (Alpha)
パラメータ: %PriLevAA
説明: 語句によるプライオリティレベル。Debug, Notice, Info等...
例: Critical

メニュー名: Facility (Alpha)
パラメータ: %PriFacAA
説明: facilityの語句によるプライオリティ。Local1, News, Cron...
例: User

メニュー名: Level (2 digit numeric)
パラメータ: %PriLev00
説明: 2桁の数字によるプライオリティレベル。00~07
例: 05

メニュー名: Facility (2 digit numeric)
パラメータ: %PriFac00
説明: 2桁の数字によるfacilityプライオリティレベル。00~23
例: 23

メニュー名: Priority (3 digit numeric)
パラメータ: %Pri000
説明: 3桁の数字によるメッセージプライオリティ。000~191
例: 016

IP Address値 (正規登録版のみ)

メニュー名: IP Address (4桁8進数, ゼロパディング)
パラメータ: %IPAdd4
説明: メッセージ送信デバイスのIPアドレス。各桁はゼロ埋め。常に15文字
例: 192.168.001.024

メニュー名: IP Address (3桁8進数, ゼロパディング)
パラメータ: %IPAdd3
説明: メッセージ送信デバイスのIPアドレスの先頭3桁。各桁はゼロ埋め。常に11文字。
例: 192.168.001

メニュー名: IP Address (2桁8進数, ゼロパディング)
パラメータ: %IPAdd2
説明: メッセージ送信デバイスのIPアドレスの先頭2桁。各桁はゼロ埋め。常に7文字。
例: 203.056

Host name値(正規登録版のみ)

メニュー名: Hostname (no domain)
パラメータ: %HostName
説明: メッセージ送信デバイスのホスト名。ドメイン名は含まない。
例: sales-router

メニュー名: Domain (no host)
パラメータ: %HostDomain
説明: メッセージ送信デバイスのドメイン名。ホスト名は含まない。
例: mycompany.co.nz

メニュー名: Reversed domain (no host)
パラメータ: %HostDomRev
説明: メッセージ送信デバイスのドメイン名の逆順序。ホスト名は含まない。
例: nz.co.mycompany

Message Text - WELF フォーマット (登録正規版のみ)

WELF フォーマットとはWebTrends拡張ロギングフォーマットです。このフォーマットはGNATBox, SonicWall, CyberWallPlus, NetScreen 等を含む多くのファイアーウォールで使われています。メッセージテキストの各フィールドには先頭にタグが付けられています。例えばfw=ファイアーウォール名、src=パケット送信元などです。将来はより多くのフィールドがAutoSplitリストに追加されます。追加が必要な場合は <http://www.kiwisyslog.com/support> まで連絡してください。

メニュー名: Firewall name (WELF format)
パラメータ: %TextFW
説明: メッセージを生成したファイアーウォール名
例: protector

メニュー名: Source address (WELF format)
パラメータ: %TextSrc
説明: ファイアーウォールでロギングされたパケットの送信元IPアドレス(すでにファイアーウォールで処理されていない限りゼロパディング無し)
例: 192.168.1.6

メニュー名: Destination address (WELF format)
パラメータ: %TextDst
説明: ファイアーウォールでロギングされたパケットの宛先IPアドレス(すでにファイアーウォールで処理されていない限りゼロパディング無し)
例: 203.57.12.1

メニュー名: Protocol (WELF format)
パラメータ: %TextProto
説明: ファイアーウォールでロギングされたパケットのプロトコル。
例: http

Input Source値(正規登録版のみ)

メニュー名: Input Source (UDP/TCP/SNMP)
パラメータ: %InpSrc
説明: メッセージの入力ソース(メッセージ受信待機方式)
例: UDP

Custom/Global script fields(正規登録版のみ)

メニュー名: VarCustom01 ~ VarCustom16
パラメータ: %VarCustom01 ~ %VarCustom16

説明: Run Script アクションで変更可能なカスタムフィールドは16個あります。これらのフィールドがスクリプトで変更されていない場合、空白になります。空白の autosplit 値が挿入されるとファイル名が不正であるというエラーが出る可能性があります。新しいメッセージを受信するとカスタムフィールドの値はクリアされます。カスタムフィールド値は現在のメッセージに対してのみ有効です。1つのメッセージより長い値を保存するときは VarGlobal フィールドを使用します。

例: スクリプトが生成する任意の値

メニュー名: VarGlobal01 ~ VarGlobal16
パラメータ: %VarGlobal01 ~ %VarGlobal16
説明: Run Script アクションで変更可能なグローバルフィールドは16個あります。これらのフィールドがスクリプトで変更されていない場合、空白になります。空白の autosplit 値が挿入されるとファイル名が不正であるというエラーが出る可能性があります。グローバルフィールドにはメッセージ間の値が入っています。

例: スクリプトが生成する任意の値

3.3.4.3 Log file formats (ログファイルフォーマット)

指定のファイルに記録するフィールドとメッセージの内容を変更するための種々の標準フォーマットをドロップダウンリストから選択します。使いたいファイルフォーマットがない場合自分のフォーマットを作成できます。Formatting オプションの下の Custom File Formatで新しいフォーマットを追加し、各フィールドを適宜設定します。次に Log to file アクションでこの新しいフィールドフォーマットをドロップダウンリストから選びます (カスタムフォーマットはリストの最後に表示されます)。

プログラムに付属の標準ファイルフォーマットは以下のとおりです。

Kiwi format ISO yyyy-mm-dd (Tab delimited)

フォーマット: 日付時刻 (YYYY-MM-DD HH:MM:SS) [TAB] プライオリティ (ファシリティ.レベル) [TAB] ホスト名 [TAB] メッセージテキスト

例: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format ISO UTC yyyy-mm-dd (Tab delimited)

フォーマット: UTC 日付時刻 (YYYY-MM-DD HH:MM:SS) [TAB] プライオリティ (ファシリティ.レベル) [TAB] ホスト名 [TAB] メッセージテキスト

例: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format mm-dd-yyyy (Tab delimited)

フォーマット: 日付 (MM-DD-YYYY) [TAB] 時刻 (HH:MM:SS) [TAB] プライオリティ (ファシリティ.レベル) [TAB] ホスト名 [TAB] メッセージテキスト

例: 07-22-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format dd-mm-yyyy (Tab delimited)

フォーマット: 日付 (DD-MM-YYYY) [TAB] 時刻 (HH:MM:SS) [TAB] プライオリティ (ファシリティ.レベル) [TAB] ホスト名 [TAB] メッセージテキスト

例: 22-07-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format UTC mm-dd-yyyy (Tab delimited)

フォーマット: UTC 日付 (MM-DD-YYYY) [TAB] UTC 時刻 (HH:MM:SS) [TAB] プライオリティ (ファシリティ.レベル) [TAB] ホスト名 [TAB] メッセージテキスト

例: 07-22-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format UTC dd-mm-yyyy (Tab delimited)

フォーマット: UTC 日付 (DD-MM-YYYY) [TAB] UTC 時刻 (HH:MM:SS) [TAB] プライオリティ (ファシリティ.レベル) [TAB] ホスト名 [TAB] メッセージテキスト

例: 22-07-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Comma Separated Values yyyy-mm-dd (CSV)

フォーマット：日付時刻 (YYYY-MM-DD HH:MM:SS),プライオリティ (ファシリティ.レベル),ホスト名,メッセージテキスト

例: 2002-07-22 12:34:56,Local5.Debug,firewall-inside,"prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64"

Comma Separated Values UTC yyyy-mm-dd (CSV)

フォーマット：UTC 日付時刻 (YYYY-MM-DD HH:MM:SS),プライオリティ (ファシリティ.レベル),ホスト名,メッセージテキスト

例: 2002-07-22 12:34:56,Local5.Debug,firewall-inside,"prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64"

BSD Unix syslog format

フォーマット：日付時刻 (Mmm DD HH:MM:SS) [SPACE] ホスト名 [SPACE] メッセージテキスト (先頭PIDタグ付き)

例: Jul 22 12:34:56 [SPACE] firewall-inside [SPACE] amd[308]: key sys: No value component in "rw,intr"

XML tagged format

フォーマット：<Message><DateTime> 日付(YYYY-MM-DD HH:MM:SS) </DateTime><Priority> プライオリティ (Facility.レベル) </Priority><Source_Host> ホスト名 </Source_Host><MessageText> メッセージテキスト </MessageText></Message>

例: <Message><DateTime>2002-07-23 21:53:35</DateTime><Priority>Local7.Debug</Priority><Source_Host>firewall-inside</Source_Host><MessageText> prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64</MessageText></Message>

RnRsoft ReportGen format

フォーマット：rnrsoft [TAB] 日付 (YYYY-MM-DD) [TAB] 時刻 (HH:MM:SS) [TAB] ホスト名 [TAB] レベル (0-7の数字) [TAB] Message text

例: rnrsoft [TAB] 2002-07-23 [TAB] 22:02:51 [TAB] firewall-inside [TAB] 7 [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

SonicWall, PIX, GNATbox および Netscreen 用 ReportGen に関しては次のWebページを参照してください。

<http://www.reportgen.com>

WebTrends format

フォーマット：WTsyslog[2001-11-12 12:44:45 ip=192.168.168.1 pri=6] <134>id=firewall time="2001-11-15 08:43:42" fw=192.168.1.1 pri=6 src=192.168.1.34 proto=http

例: WTsyslog[2001-11-12 12:44:45 ip=192.168.168.1 pri=6] <134>id=firewall time="2001-11-15 08:43:42" fw=192.168.1.1 pri=6 src=192.168.1.34 proto=http

Webtrends firewall suite に関しては次のWebページを参照してください。

<http://www.netiq.com/products/fwr>

Cisco PIX PFSS format (Raw logging)

フォーマット：<Priority value (0-191)>メッセージテキスト

例: <191>Built outbound TCP connection 12004 for faddr grc.com/80 gaddr 192.168.2.2/4120 laddr 192.168.1.1/4391

3Com 3CDeamon format (BSD space delimited)

フォーマット：日付時刻 (Mmm DD HH:MM:SS) [SPACE] ホストアドレス [SPACE] メッセージテキスト

例: Jul 22 12:34:56 [SPACE] 192.168.1.1 [SPACE] key sys: No value component in "rw,intr"

Raw - Message text only (no priority)

フォーマット：メッセージテキストのみ

例: Built outbound TCP connection 12004 for faddr grc.com/80 gaddr 192.168.2.2/4120 laddr 192.168.1.1/4391

Sawmill format ISO yyyy-mm-dd (Tab delimited)

フォーマット： 日付 (YYYY-MM-DD HH:MM:SS) [TAB] プライオリティ (ファシリティ.レベル) [TAB] ホスト名 [TAB] メッセージテキスト

例： 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Sawmill ログ処理ソフトウェアに関しては次のWebページを参照してください。

<http://www.sawmill.net>

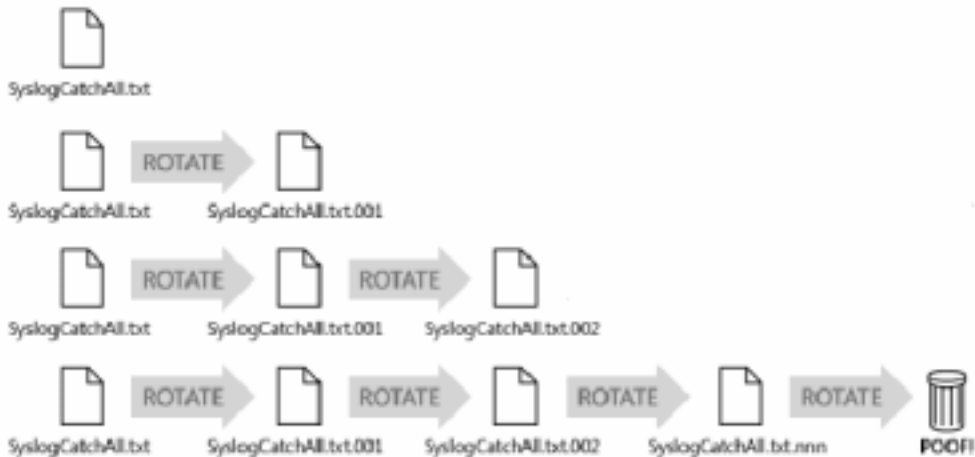
3.3.4.4 Log File Rotation (ログファイルローテーション)

この機能は正規登録版でのみ使用できます。

ログファイルローテーションを使用することによってログファイルが無制限に肥大することを防ぎ、ログデータとして適切なサイズに保つことができます。

ディスクの空き領域が少ない等何らかの理由で制限されている場合は特にこの機能を使うことを検討する必要があります。ファイルローテーションはディスク容量の問題を解決する有効な手立てとなります。

ログファイルが一定のサイズや経過時間に達すると、現在のログファイルに別の名前(例:logfile.txt.001)が付けられて移動されます。ログ処理は空のファイルに対して継続されます。このファイルも所定のサイズや経過時間に達すると同じ処理が実行されます。このとき logfile.txt.001 は logfile.txt.002 に、現在のログファイルは logfile.txt.001 に移動されます。この処理はローテーションによって作成されたログファイルが設定した数になるまで繰り返されます。それ以降は一番古いファイルが削除されます(下図参照)。



Log to file アクションでのログファイルローテーションオプション

Enable Log File Rotation

このオプションにチェックすると上記のようにログファイルがローテートされます。

チェックをしないとログファイルはローテートされず通常どおりデータはファイルに記録され続けます。

Total number of log files

ローテートするログファイルの総数を指定します。ファイルローテーション処理中に作成されるログファイルの数は指定値を超えることはありません。

例：4 に設定すると、<logfile>, <logfile.001>, <logfile.002> および <logfile.003> という名前の4つまでのログファイルが作成されます。

Maximum log file size

ローテートするログファイルのサイズが一定のサイズを超えないようにしたいときに設定します。各ログファイルのサイズはバイト、キロバイト、メガバイト、ギガバイトのどれかで指定します。

Maximum log file age

ローテートするログファイルの経過時間が一定の値を超えないようにしたいときに設定します。各ログファイルの経過時間は分、時間、日、営業日、週、月、四半期のどれかで指定します。

3.3.5 Action - Forward to another host (アクション - 他のホストへ転送)

他のSyslogホストにUDPまたはTCP syslogプロトコルを使って受信メッセージを転送します。

Destination IP address or hostname

メッセージの転送先ホストのホスト名かIPアドレスを指定します。

複数のホストにメッセージを送信するには、ホスト名やIPアドレスをカンマで区切って指定します。

例 : I.e. Myhost.com, SecondHost.net, 203.75.21.3

Protocol

SyslogメッセージはUDP(デフォルト)、TCPあるいはKRDPで送信します。

Kiwi Reliable Delivery Protocol (KRDP)は2台のKiwi Syslog Daemonn間をTCPで転送する信頼性の高い送信です。

New Port

メッセージを送信するポート番号を指定します。

推奨値 :

UDP: 514

TCP: 1468または601

KDRP: 1468

New Facility / New Level

すべての送信メッセージに対し指定したファシリティおよびレベルの値を強制的に適用します。多くの場合、このオプションは -No change- に設定して構いません。これは受信したファシリティとレベルのまま転送することを意味します。

KDRP connection identifier

KDRP接続に対する重複しない固有の名前を指定します。送信元と宛先間の接続が試行されるたびにsyslog daemonは識別されなければなりません。接続が途切れ、再確立されるとシーケンス番号が交換され、送信されなかったメッセージが再送されます。メッセージシーケンス番号は接続IDごとに割り当てられます。

例 : Source: RemoteOffice1またはSyslogDaemon1

テキストは送信元から宛先のsyslog daemonへの接続を個別に識別します。

複数の Forward to another host アクションを作成している場合、同一の接続IDをすべてのアクションに使用することができます。これは送信元と宛先間でのKRDP接続は1回のみ確立されることを意味しています。異なる接続IDを指定すると複数のKRDPセッションが生成されます。

IDが重複しない固有な値であることを確実にするために %MACAddress 変数を使用することを推奨します。この変数はマシンの最初のMACアドレスで置き換えられます。

例 : Source: RemoteOffice1-%MACAddress

実行時のIDは次のようになります。

Source: RemoteOffice1-AA-BB-CC-DD-EE-FF-00

MACアドレスは各マシンのネットワークカードに対してグローバルに固有な値が割り当てられています。

Send with RFC3164 header information

これは送信メッセージにRFC3164ヘッダーを追加します。次のようなフォーマットで指定します。

<Priority>Date Hostname PID Message text

Priority は0-191の値を指定します。

Date は Mmm DD HH:NN:SS(July 4 12:44:39)の形式で指定します。年を指定することはできません。

PID は最大32文字のプログラム識別子を指定します。

Retain the original source address of the message

通常 syslog プロトコルは syslog をフォワード/リレーする場合には本来の送信元アドレスを保持できません。なぜならば送信元アドレスはUDPまたはTCPパケットで受信するからです。

Kiwi Syslog Daemon はメッセージテキストに本来の送信元アドレスを含むタグを埋めることでこの問題を解決しました。タグはOriginal Address=192.168.1.1 のようになります。すなわち Original Address= タグの後にIPアドレス、その後スペースが来ます。

このタグは Retain the original source address of the message オプションをチェックした場合だけ挿入されます。

また、このタグは OriginalAddressStartTag および OriginalAddressEndTag という2つのレジストリ設定によって上書きされます。

デフォルトの送信元アドレスの開始/終了タグを変更する方法については[関連項目](#)を参照してください。

注：Spoof Network Packet オプションにチェックすると、Original Address= タグは使用されません。syslog パケットは宛先アドレスにあたかも本来の送信元IPアドレスから送信されたように転送されます。

Use a fixed source IP address

このオプションは Original Address= タグに固定IPアドレスを使います。すべての送信メッセージが特定のホストから送信されている場合にそれらを識別するのに有効です。たとえば多くのリモート syslog daemon から1台の syslog daemon に集中して送信するような場合です。各リモートsyslogが10.0.0.xというアドレス範囲を使っているとすると、すべての受信メッセージは同一ホストから送信されているように見えます。リモートsyslogごとに異なる送信元IPアドレスを指定することによって受信メッセージの識別が容易になります。

注：Spoof Network Packet オプションにチェックすると、Original Address= タグは使用されません。syslog パケットは宛先アドレスにあたかも指定した固定IPアドレスから送信されたように転送されます。

Spoof Network Packet

この機能は正規登録版でのみ使用できます。

WinPcap 3.0+ がインストールされている Windows 2000/XP/2003 上のみで動作します。

このオプションはUDPプロトコル経由で転送されたsyslogメッセージにのみ適用されます。ネットワークパケットは転送メッセージがあたかもSyslog Serverのアドレスではなく本来の送信元デバイスのIPアドレスから直接受信したかのように見えます。Kiwi Syslog Daemonはこの見せかけのUDP/IPパケットを送信する際 Selected Network Adapter に指定したネットワークアダプタを使用します。

重要:

Kiwi Syslog Daemonでこのネットワークパケットのスプーフィング機能をサポートするのは次のプラットフォームのみです。

Windows 2000/XP/2003 (Window 95/98/Me/Vista はサポート対象外)。また、WinPcap バージョン3.0以上がインストールされていなければなりません。WinPcap (Windows Packet Capture library)は<http://www.winpcap.org/>からダウンロードできます。

Test ボタン

Test ボタンをクリックすると指定ホストへのSyslogメッセージの送信テストが実行されます。

3.3.6 Action - Play a sound (アクション - 音を鳴らす)

この機能は正規登録版でのみ使用できます。

上記で設定したフィルターにメッセージがマッチした場合、指定の音を鳴らすことが出来ます。

Filename of wav. sound file フィールドに音声ファイル名を入力するか、[...] ボタンでファイルを選択してください。

\\sounds フォルダにサンプルの音声ファイルがあります。Test ボタンで音を聞いてください。

3.3.7 Action - Run external program (アクション - 外部プログラム実行)

この機能は正規登録版でのみ使用できます。

上記で設定したフィルターにメッセージがマッチした場合、外部プログラムが実行されます。コマンドライン引数としてメッセージとSyslog統計の詳細を外部プログラムに渡すことが出来ます。Program file name フィールドに外部プログラムのファイル名を入力するか、[...] ボタンでファイルを選択してください。

Command line options フィールドでプログラムに渡すコマンドラインオプションを指定してください。外部プログラムへ渡すメッセージの詳細やSyslog統計の構文については [?] ボタンをクリックしてヘルプページを参照してください。

Insert message content or counter

外部プログラムにプログラム変数、カウンター、スクリプトフィールド、統計を渡すには Insert message content or counter リンクをクリックし、ポップアップメニューからオプションを選びます。値の詳細については[関連項目](#)参照してください。

変数をポップアップメニューから選択します。変数はメッセージの送信前に現在の値に置き換えられます。例えば %MsgText は現在のSyslogメッセージに置き換えられます。カーソルを件名かメッセージテキストの行内に置き Insert message content or counter リンクをクリックしてください。ポップアップメニューが表示されますので変数を選びます。

Command line options の例:

"555-1234", "Syslog - A link has gone down - %MsgAll"

または: "Warning, message received from host %MsgHost at %MsgTime"

Process Priority

生成されたWindowsプロセスのプライオリティを指定します。

指定可能な値:

LOW_PRIORITY

BELOW_NORMAL_PRIORITY

NORMAL_PRIORITY(デフォルト)

ABOVE_NORMAL_PRIORITY

HIGH_PRIORITY

REALTIME_PRIORITY (注: この値に設定するとシステムがロックアップする可能性があります)

AboveNormal

Normal 以上 High 以下のプライオリティのプロセスに対して指定します。

BelowNormal

Idle 以上 Normal 以下のプライオリティのプロセスに対して指定します。

High

直ぐに実行する必要がある緊急度の高いタスクを実行するプロセスに対して指定します。Normal や Idle のプロセススレッドよりも先に処理されます。例えば、Task List などOSにかかる負荷を無視してでもユーザーに呼び出されたらすぐに応答する必要のあるプロセスに対して設定します。この値を適用すると、使用可能なほぼすべてのCPU時間が消費されるため使用するときには特に注意が必要です。

Low

システムがアイドルのときのみ実行されるスレッドのプロセスに対して指定します。この値の設定されたプロセススレッドは Low 以上のプライオリティクラスが設定されているプロセスの実行後に実行されます。スクリーンセーバーなどが該当します。プライオリティクラスが Idle のプロセスは子プロセスに引き継がれます。

Normal

特にスケジュールする必要のないプロセスに対して指定します。

Realtime

最優先のプロセスに対して指定します。この値の設定されたプロセススレッドは他のすべてのプロセスよりも先に実行されます。重要なタスクを実行するOSのプロセスなどがこれに該当します。例えば、非常に短い間隔でアルタイムプロセスが繰り返し実行されると、ディスクキャッシュへの書き込みが不能になったり、マウスが応答しなくなることがあります。

Window Mode

プロセスがユーザーインターフェイスを有するときに Window Mode にします。ユーザーインターフェイスの無いプロセスには無効です。Syslog Daemonをサービスで実行するときは使えません。

指定可能な値:

Hide

Normal

Minimized

Maximized

Wait for program initialization to complete before continuing

チェックすると、Syslogは新たなプロセスが初期化されるまで待ちます。すなわち新たなプロセスがアイドルになるまで待ちます。

注: これはブロック操作です。プロセスから InputIdle シグナルを受信するまで Kiwi Syslog によるメッセージ処理は実行されません。そのため、どのくらいSyslogがプロセスの初期化を待つかを次のオプションで指定する必要があります。この時間が過ぎると、Syslogはプロセスが正常に開始されたとみなします。

この設定は後にプロセスと相互連携するためプロセスが開始したことを確認するのに有効です。

3.3.8 Action - E-mail message (アクション - Eメールメッセージ送信)

この機能は正規登録版でのみ使用できます。

設定したフィルターにマッチしたSyslogメッセージを受信すると、Eメールメッセージが送信されます。

受信したSyslogメッセージの詳細やSyslog統計をEメールの件名やメッセージ本文に挿入することができます。事実上SyslogからEメールへのコンバータとして使うことができます。

最初に E-mail オプションでSMTPサーバーオプションの設定が必要です。

E-mail recipient フィールドに受信者アドレスを指定します。複数のアドレスを指定できます。各アドレスはカンマで区切ります。

E-mail subject フィールドに件名を指定します（1行のみ）。件名の送信文字数は **Max subject length** オプションで指定した文字数までです。

E-mail message フィールドにメッセージを指定します（複数行可能）。このメッセージをポケットベルに送るのであればメッセージ本文を指定しないほうが良いでしょう。このような場合は空白のままにしております。ポケットベルシステムの多くはディスク領域が限られているため、件名のみを指定してください。メッセージ本体の送信データ文字数を制限するには **Max message length** オプションを使用します。メッセージ本文に変数 %MsgText が含まれており、このようなときに大きなSyslogメッセージを受信してしまうと、Eメールで送信するには大きすぎて送れなくなる可能性があります。このオプションを指定することによって、メッセージ本文を扱いやすい長さに制限することが可能です。

[Test] ボタンをクリックすると指定受信者へEメールでテストメッセージが送信されます。テストメッセージの内容は**Test Setup** ボタンで変更できます。

Insert message content or counter

プログラム変数、カウンター、スクリプトフィールド、統計をメッセージや件名に渡すには Insert message content or counter リンクをクリックしポップアップメニューからオプションを選びます。値の詳細については[関連項目](#)を参照してください。

ポップアップメニューから変数を選択します。変数はメッセージ送信前に現在の値に置き換えられます。例えば %MsgText は現在のSyslogメッセージテキストに置き換えられます。カーソルを件名やメッセージテキストを指定するフィールド内に置き、Insert message content or counter リンクをクリックします。ポップアップメニューが表示されますので変数を選択してください。

例

E-mail Subject: Syslog Alert from %MsgHost

E-mail Message: Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

Kiwi Syslog Daemon を、SyslogメッセージをEメールに変換するコンバータとして使うには、メッセージ本文テキストに %MsgAll キーワードを挿入し受信したすべてのSyslogメッセージ情報をEメールメッセージに渡します。

大量のメッセージを受け取ると、Eメールサーバーに輻輳が発生する可能性があるため注意が必要です。Eメールバッファは最大1,000メッセージまでしか保持できず、それ以降のメッセージは失われます。大量のSyslogメッセージを一度に受信しメールサーバーがビジーになったときに有効な機能です

Eメール送信前1分になるとキューが発行されます。メッセージ送信の都度メールサーバーに接続するよりもこの方が効率的です。キューに入ったメッセージは一分後にバッチに送信されます。

E-mail Delivery Options

このオプションを使用してEメールメッセージにImportance(重要度)、Priority(プライオリティ)、Sensitivity(種類)のフラグを設定できます。Eメール受信者には適宜これらのレベルが付けられたメッセージが届きます。

Importance: Unspecified (デフォルト) / High / Normal / Low

Priority: Unspecified (デフォルト) / Normal / Urgent / Non-Urgent

Sensitivity: Unspecified (デフォルト) / Personal / Private / Confidential

Expand <013> <010> in message

<013> および <010> に事前に置き換えられたCRおよびLFを元に戻します。

replace non printable characters with ASCII value オプションがチェックされているとSyslogメッセージに含まれているCR、LFは置き換えられます。Eメールで転送する時に元の文字に戻すようにするとテキストが読み易くなり便利です。

3.3.8.1 Insert message content or counter (メッセージ内容/カウンターの挿入)

変数やカウンターをポップアップメニューから選べます。変数はメッセージ送信前に現在の値に置き換えられます。例えば %MsgText は現在のSyslogメッセージに置き換えられます。ポップアップメニューの中から項目を適宜クリックすると現在のカーソル位置に %変数 が挿入されます。

例

E-mail Subject : Syslog Alert from %MsgHost

変数および機能一覧

メニュー名:	All of the message
パラメータ:	%MsgAll
説明:	画面に表示されるとおりのメッセージ全体。時刻、日付、プライオリティ、メッセージテキスト等。各フィールドはスペースで区切られる。
例:	2002-10-10 11:28:04 Local7.Debug host.company.com This is a test message
メニュー名:	Date
パラメータ:	%MsgDate
説明:	メッセージ受信日。フォーマットはYYYY-MM-DD
例:	2002-02-18
メニュー名:	Time
パラメータ:	%MsgTime
説明:	メッセージ受信時刻。フォーマットはHH:MM:SS
例:	22:30:16
メニュー名:	Facility
パラメータ:	%MsgFacility
説明:	メッセージのファシリティ。テキスト。
例:	Local7, Mail
メニュー名:	Level
パラメータ:	%MsgLevel
説明:	メッセージのlevel。テキスト。
例:	Debug, Info
メニュー名:	Host address of sender
パラメータ:	%MsgHost
説明:	送信デバイスのホストIPアドレス
例:	192.168.1.1
メニュー名:	The message text
パラメータ:	%MsgText
説明:	syslogメッセージに含まれるテキスト部分
例:	This is a test message
メニュー名:	Alarm min msg threshold
パラメータ:	%MsgAlarmMin
説明:	アラームを鳴らす最小メッセージ数として設定されている閾値レベル
例:	100 (1時間あたりに受信する最小メッセージ数)
メニュー名:	Alarm max msg threshold
パラメータ:	%MsgAlarmMax
説明:	アラームを鳴らす最大メッセージ数として設定されている閾値レベル
例:	5000 (1時間あたりに受信する最大メッセージ数)
メニュー名:	Alarm disk space threshold
パラメータ:	%MsgAlarmDisk
説明:	MB単位のディスク残量の最小閾値レベル設定
例:	90 (MB)
メニュー名:	Message count this hour
パラメータ:	%MsgThisHour
説明:	この時間での受信メッセージ数
例:	254
メニュー名:	Message count last hour
パラメータ:	%MsgLastHour
説明:	直前1時間の受信メッセージ数
例:	254

メニュー名: Machine Mac address
パラメータ: %MACAddress
説明: 最初に見つかったネットワークアダプタのMACアドレス
例: AA-BB-CC-DD-EE-FF-00

Custom/Global/Statistics フィールド (正規登録版でのみ有効)

メニュー名: VarCustom01 ~ VarCustom16
パラメータ: %VarCustom01 ~ %VarCustom16
説明: Run Script アクションで変更可能なカスタムフィールドは16個あります。これらのフィールドがスクリプトで変更されていない場合、空白になります。空白の autosplit 値が挿入されるとファイル名が不正であるというエラーが出る可能性があります。新しいメッセージを受信するとカスタムフィールドの値はクリアされます。カスタムフィールド値は現在のメッセージに対してのみ有効です。1つのメッセージより長い値を保存するときは VarGlobal フィールドを使用します。
例: スクリプトが生成する任意の値

メニュー名: VarGlobal01 ~ VarGlobal16
パラメータ: %VarGlobal01 ~ %VarGlobal16
説明: Run Script アクションで変更可能なグローバルフィールドは16個あります。これらのフィールドがスクリプトで変更されていない場合、空白になります。空白の autosplit 値が挿入されるとファイル名が不正であるというエラーが出る可能性があります。グローバルフィールドにはメッセージ間の値が入っています。
例: スクリプトが生成する任意の値

メニュー名: VarStats01 ~ VarStats16
パラメータ: %VarStats01 ~ %VarStats16
説明: Run Script アクションで変更可能な統計フィールドは16個あります。統計フィールドにはフィールドにはメッセージ間の値が入っています。統計フィールドに関連付けられている名前とその初期値は設定ウィンドウの Script options で変更できます。カスタム統計値は統計表示や日別の統計Eメールで確認できます。
例: スクリプトが生成する任意の値

3.3.9 Action - Send Syslog message (アクション - Syslogメッセージ送信)

この機能は正規登録版でのみ使用できます。

メッセージを受信し、フィルターを通過したSyslogメッセージを指定したホストに送ります。

受信メッセージの詳細とSyslog統計を送信Syslogメッセージに含ませることができます。

選択したSyslogメッセージを他のホストに追加情報とともにあるいはオリジナルのテキストを追加してリレーできます。

IP address or Hostname フィールドに宛先IPアドレスまたはホスト名を指定します。

ホスト名の構文については構文については [?] ボタンをクリックしてヘルプページを参照してください。

複数のホストで転送メッセージを受信できます。

複数のホストを指定するときはホスト名またはIPアドレスをカンマで区切ります。

例. Myhost.com, SecondHost.net, 203.75.21.3

転送するメッセージに新しいファシリティとレベルを適用するには、New facility および New level リストから選択します (デフォルトでは受信したファシリティとレベルのまま転送されますが、適宜変更できます)。

[Test] ボタンをクリックすると指定アドレスへSyslogテストメッセージが送信されます。

Insert message content or counter

新しいSyslogメッセージにプログラム変数、カウンター、スクリプトフィールドを渡すには Insert message content or counter link をクリックしポップアップメニューからオプションを選びます。値の詳細については[関連項目](#)を参照してください。

ポップアップメニューから変数を選ぶことが出来ます。変数はメッセージ送信前に現在の値に置き換えられます。例えば %MsgText は現在のsyslogメッセージテキストで置き換えられます。カーソルを Syslog message text: のフィールド内に置き、ハイパーリンクをクリックします。ポップアップメニューが表示されますので変数を選びます。

例

Syslog message text: : Syslog Alert from %MsgHost

または

Syslog message text: Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

3.3.10 Action - Log to database (アクション - データベース記録)

3.3.10.1 Action - Log to database (アクション - データベース記録)

この機能は正規登録版でのみ使用できます。

メッセージをODBC Data Source Name (DSN)で指定したテーブルに記録します。

Datalink connection string

Datalink connection string フィールドにデータベースのDSN、ユーザーID、パスワードを入力します。

あるいは、[...] ボタンでマシンに構成されているODBC DSNから選びます。

Datalink connection string は次の要素で構成されています。

Data Source Name

システムに構成されている ODBC DSN を参照します。[...]ボタンを押してシステムのODBC Data Source Names リストから選びます。

UID=UserID; データベースがパスワードで保護されている時に限り必要です。データベースのユーザー名を入力します。

PWD=Password; データベースがパスワードで保護されている時に限り必要です。データベースのパスワードを入力します。

例

DSN=Syslogd;UID=Admin;PWD=Password;

各要素はセミコロンで区切ります。UserID や Password が不要の時、接続文字列はDSNのみで構成されます。

デフォルトの接続文字列は DSN=Syslogdです;

多くの場合DSN名の前に DSN= と指定しなければなりません。

Database table name

有効なデータベーステーブル名を指定します。指定したテーブルには選択したデータベースフォーマットに合致するフィールド名が設定されていなければなりません。フィールドサイズが短かすぎると、データがデータベースに記録される時に切り詰められてしまいます。

デフォルトのテーブル名は Syslogd です。

ODBCデータベースのログアクションをテストするには [Test] ボタンを押します。アクションの成功/失敗およびエラーの詳細を示すメッセージが表示されます。

Database type/field format

デフォルトのデータベースタイプリストから選ぶか、[Edit custom format] ボタンをクリックしてオリジナルのフォーマットを作成します。

デフォルトのデータベースタイプ:

- Access
- SQL
- MySQL
- Oracle

デフォルトのデータベーステーブルは以下のように設計されています。

Microsoft Access database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	Text	30
Hostname	MSGHOSTNAME	Text	255
Message text	MSGTEXT	Memo	1024

SQL database (Microsoft SQL とgeneric SQL)

Field	Name	Type	Size
Date	MSGDATE	DateTime	10
Time	MSGTIME	DateTime	8
Priority	MSGPRIORITY	VarChar	30
Hostname	MSGHOSTNAME	VarChar	255
Message text	MSGTEXT	VarChar	1024

MySQL database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	VarChar	30
Hostname	MSGHOSTNAME	VarChar	255
Message text	MSGTEXT	Text	1024

Oracle database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	VarChar2	30
Hostname	MSGHOSTNAME	VarChar2	255
Message text	MSGTEXT	VarChar2	1024

注：

ODBC データソースに記録するには MDAC (Microsoft Data Access Components) ドライバーが必要です。バージョン2.50以上をお奨めします。このパッケージは次のページからダウンロードできます。

<http://www.microsoft.com/data/>

データベースが他のプロセスで排他的に開かれている間は Kiwi Syslog Daemon はデータベースへの新しいレコードの記録ができません。

ODBC データベースのサンプルを次のページからダウンロードできます。

http://www.kiwitools.com/downloads/Syslog_ODBC_Samples.zip

Zipファイルには情報とサンプルデータベースが含まれており、ご使用のシステムで ODBC ログイン設定を行う際役立ちます。

ODBC Control Panel ボタン

[コントロールパネル] の [ODBC] アプレットが開き、システムDSNの構築や使用可能なODBCオプションを確認することができます。

Create table ボタン

DSNで参照されたデータベースに指定されたテーブルを作成します。既存のテーブルは削除され内容が失われます。選択したデータベースタイプで指定したフィールド名とタイプの新しいテーブルが作成されます。すべてうまく行き、新しいテーブルが作成されると確認メッセージが表示されます。テーブル作成中に問題が生じると、エラーメッセージが表示されます。問題を修正してください。

Query table ボタン

指定したテーブルの最終5エントリーを取得します。ダイナミックアクセスができるようDSNタイプを指定します。Forward only databases はデータベースに対して Move previous コマンドが発行されていますので正しく読めません。

得られたデータはメモ帳で読めます。最後の5フィールドのテーブル構造とデータから情報を得ることが出来ます。

クエリーで得られた情報の例：

Field name	Type	Size	Data
MsgDate	adDBTimeStamp	16	28/07/2002
MsgTime	adDBTimeStamp	16	14:45:16
MsgPriority	adVarChar	30	Local7.Debug
MsgHostname	adVarChar	255	host.company.com
MsgTex	adLongVarChar	1024	This is a test message from Kiwi Syslog Daemon

Edit custom format ボタン

Database type/field format のドロップダウンリストからカスタムフォーマットを選んで、このボタンを押すと選択したカスタムフォーマットが表示されます。カスタムフォーマットを選択しなかった場合、Custom DB formats オプションで新しいフォーマットを作成できます。

Show SQL commands ボタン

選択したテーブルに挿入するデータを作成するためのSQLコマンドを生成します。生成されるコマンドは選択されたデータベースによって異なります。これらのコマンドを使ってご使用のデータベースアプリケーションで使用できるデータベーステーブルスキーマが生成されます。あるいは、Create table ボタンを使って Kiwi Syslog Daemonでテーブルを生成することも可能です。

生成されたSQLコマンドの例：

Database type: Access database
Database name: Kiwi Access format ISO yyyy-mm-dd

テーブル生成のSQLコマンド：

```
CREATE TABLE Syslogd (MsgDate DATE,MsgTime TIME,MsgPriority TEXT(30),MsgHostname TEXT(255),MsgText MEMO)
```

SQL INSERT コマンドの例：

```
INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText) VALUES ('2002-07-28','14:58:04','Local7.Debug','host.company.com','This is a test message from Kiwi Syslog Daemon')
```

Connection Inactivity timeout

最終メッセージの送信からどのくらいデータベース接続をオープンしているかを指定します。接続のオープンとクローズはデータベースのロギングにおいて最も時間のかかる処理です。データのロギング中は継続してオープンにします。タイムアウト前にログデータが無くなった場合、データベース接続はクローズされます。新しいメッセージが到着すると再び接続がオープンされます。デフォルト値は 600 秒 (10分)です。0 を指定すると接続がタイムアウトしなくなります。最大値は 86400 秒 (1日)です。

Run debug command ボタン

データベースへのロギング中に問題が発生した場合このボタンで診断できます。データベースで実行するSQLコマンドを入力するための別のウィンドウが開きます。コマンドが失敗すると結果フィールドに詳細なエラーメッセージが表示されます。デフォルトでは選択したデータベースタイプの現在のINSERT文が query フィールドに表示されます。この文を少し変更してテストを試みることができます。

このオプションを実行してもデータベース上でクエリーが実行されるわけではありません。エラー情報だけが結果フィールドに返されます。例えば Select From 文を実行し結果を得ることはできません。わかるのはその文が正しく実行されたか否かだけです。

Show SQL commands ボタンをクリックすればデバッグテストで使用する正しい構文を確認できます。

カスタムフィールド

カスタムフィールドは Run script アクションで使います。構文解析スクリプトを作成すると、syslog メッセージテキストをいくつかのサブフィールドに分離できます。値は16個のカスタムフィールドに割り当てられデータベースに記録されます。syslog メッセージはデバイスメーカーごとに異なるフォーマットで生成されますので、メッセージテキストを別々のフィールドに分離する汎用の構文解析プログラム(パーサー)を作成することはできません。メッセージテキストを解析し、カスタムデータベースフィールドに挿入するカスタムスクリプトを作成しなければなりません。Scripts サブフォルダに構文解析スクリプトのサンプルがありますので参考にしてください。

3.3.10.2 To configure an ODBC database DSN (ODBCデータベースDSNの構築)

[コントロールパネル] を開き [データソース(ODBC)] アプレット(32ビット) を開きます。

[システム DSN] タブの [追加] ボタンをクリックします(サービスとしてKiwi Syslog Daemonを実行する場合は、システム DSN の作成が必要です)。

使用するドライバーを選びます (サンプルデータベースの場合 Microsoft Access Driver を選択します)。

[データソース名] フィールドに重複しない固有の名前を入力します (Syslogd で始まる名前にすると良いでしょう)。

[選択] ボタンをクリックし、フォルダを参照して使用するデータベースファイル名を探します。

[OK] をクリックしデータソース名のリストに作成したDSNが追加されているか確認します。

Log to Database アクションの設定時に Data link connection string フィールドにこの新しいDSN名を入力します。

3.3.10.3 Problems logging when running as a Service (サービス版実行時の記録エラー)

Service Manager からODBC記録テストを実行する際プログラムは現在のユーザーで実行されています (通常Administrator)。

サービスがログをODBCデータベースに記録する時、デフォルトでは Local System ユーザーとして実行します。

テストメッセージは正しく送信されるが、サービスでエラーが発生する場合、サービスのログオン名を Local System ではなく Administrator に変更してみてください。

ログオン名は [コントロールパネル] の [サービス] アプレットで変更できます。

プログラムをデスクトップから操作できるようにするためのチェックボックスもありますので必要であればオンにしてください。

3.3.11 Action - Log to NT Event log (アクション - NT Event logへの記録)

3.3.11.1 Action - Log to NT Event log (アクション - NT Event log記録)

この機能は正規登録版でのみ使用できます。

メッセージを受信し設定したフィルターにマッチした時syslogメッセージをNTイベントログに記録します。

NTイベントログには Error, Warning, Information, Success Audit および Failure Audit の5種類のログレベルがあります

ドロップダウンリストからログレベルを選びます。メッセージにはこのレベルが付加されてNTイベントログに記録されます。

3.3.11.2 ログ挿入タイプの設定

メッセージのイベントログへの挿入方法は3つあります。

メッセージは次のように記録されます。

Single insertion string

%1 は次のように置き換えられます。

日付 - Tab - 時刻 - プライオリティ - Tab - ホスト名 - Tab - メッセージ

5 Tab delimited insertion strings

%1 Tab %2 Tab %3 Tab %4 Tab %5

%1 = 日付

%2 = 時刻

%3 = プライオリティ

%4 = ホスト名

%5 = メッセージ

5 Space delimited insertion strings

%1 Space %2 Space %3 Space %4 Space %5

%1 = 日付

%2 = 時刻

%3 = プライオリティ

%4 = ホスト名

%5 = メッセージ

[Test] ボタンをクリックするとNTイベントログのテストが実行されます。Windows 95/98のようなNT以外のシステムではメッセージは書き込まれずエラーメッセージが表示されます。

注: デフォルトではNTイベントログビューワーでNTイベントログを表示するとログタイプはSystemイベントを表示するように設定されています。アプリケーションイベントを表示するにはNTイベントビューワーのログメニューでアプリケーションをチェックしてください。

3.3.12 Action - Send pager or SMS message via NotePage Pro (アクション - NotePage Pro 経由でポケットベル/SMSにメッセージ送信)

この機能は正規登録版でのみ使用できます。

このアクションは NotePagerPro アプリケーション経由でポケットベル、SMSあるいはEメールメッセージを送信します。この機能を使用するにはまず、<http://www.notepager.com> から NotePager を購入しインストールする必要があります。NotePager Pro は低価格ですが非常に高機能なポケットベルおよびSMSゲートウェイのアプリケーションです。

NotePager Proを使用するメリット

- グループメッセージ送信機能
 - 携帯電話、ポケットベルなどの複数のキャリアをサポート
 - SNPP, WCTP, SMTPなどのインターネットポケットベルプロトコルをサポート
 - メッセージ送受信のスケジュール化、メッセージ再送/再受信、メッセージ送受信のプログラム化のサポート
- 今すぐ NotePager Pro をダウンロードするには以下のページにアクセスしてください。

<http://www.notepager.com>

メッセージは NotePager Pro に渡されると送信キューに入れられます。NotePager Pro は周期的にキューをチェックし、指定の方法でそれらを送信します。SNPP、電子メール、モデム、TAPI、構成済みのポケットベルインターフェイスなどを経由して送信できます。

Insert message content or counter リンクをクリックすると、送信されるポケットベルメッセージに含まれる受信Syslog メッセージとSyslog 統計の詳細が表示されます。

Send Page To:

ドロップダウンリストから受信者を選択します。このリストは NotePager Pro の Recipients and Groups データベースから自動的に読み込まれます。ドロップダウンリストに名前がない場合は、NotePager Pro が正しくインストールされていません。受信者1人を選択するか、受信者グループを選択します。

例:

Send to: Joe

あるいは

Send To: All-Network-Staff.

Message From:

任意の名前を入力できます。NotePager Pro で受信者がEメール経由でメッセージを受信するように指定されている場合、ここに入力した名前が設定済みのデフォルトドメインの前に追加されます。例えば、NotePager Pro でデフォルトドメインとして "company.com" が設定されている場合、「Syslog」という送信者からメッセージを送信すると Syslog@company.com からメッセージが送られたように表示されます。

Message:

ポケットベルやSMSメッセージに送るメッセージを指定します。通常これは %MsgText と入力します。%MsgText は本来の syslogメッセージのメッセージテキストで置き換えられます。

他の変数を挿入することもできます。Insert message content or counter リンクをクリックすると指定可能な変数のポップアップメニューが表示されます。Max message length オプションを指定すれば送信するメッセージの長さを制限できます。メッセージ本文に変数 %MsgText が含まれており、このようなときに大きなSyslogメッセージを受信してしまうと、ポケットベルに送信するには大きすぎて送れなくなる可能性があります。このオプションを指定することによって、メッセージ本文を扱いやすい長さに制限することが可能です。

ポケットベルが数字メッセージのみを受信するのであれば、%MsgText の代わりに Message フィールドに数字を指定します。各数字が対応するコードを決めておく必要があります。

例: 1=link up, 2=link down, 9=Router unreachable

Test ボタン

[Test] ボタンをクリックすると指定した受信者にポケットベルメッセージがテスト送信されます。[Test Setup] ボタンをクリックすればテストメッセージの設定を変更できます。

Insert message content or counter

プログラム変数、カウンター、スクリプトフィールド、統計などをポケットベルメッセージに渡すには、Insert message content or counter リンクをクリックしてポップアップメニューからオプションを選択します。値の詳細については[関連項目](#)を参照してください。

このオプションではポップアップメニューから変数を選択します。変数はメッセージ送信前に現在の値で置き換えられます。例えば、%MsgText は現在のsyslogメッセージで置き換えられます。カーソルをフィールド内に置きハイパーリンクをクリックします。ポップアップメニューが表示されますので変数を選びます。

例

Message: Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

3.3.13 Action - Send ICQ instant message (アクション - ICQインスタントメッセージ送信)

この機能は正規登録版でのみ使用できます。

*****この機能はICQ WWWページングシステムへの変更中であり無効になっています。まもなく変更が完了します。*****

フィルターにマッチしたSyslogメッセージを受信すると指定したICQ番号にICQインスタントメッセージを送信します。

WWPagerメッセージを受信するとICQにアラームメッセージ表示されます。ICQアラームメッセージは読んだ後閉じることができます。

メッセージはICQ Webベースインターフェイス経由で送信されます。現在は無料のサービスです。ICQクライアントは<http://www.icq.com> から無料でダウンロードできます。

メッセージの配信は保証されず最大の努力をして配信するという条件で実行されます。ICQはポケットベルメッセージを2秒に1回に制限します。これより早いメッセージは失われます。

この機能を使うには標準httpでICQ Webサーバーのポート80に接続しなければなりません。透過プロキシは問題になりません。この機能はポート80への直接アクセスをブロックするファイアーウォール経由では動作しません。宛先Webサイトアドレスは<http://www.icq.com> です。このアドレスをファイアーウォールの直接アクセスリストに追加します。

メッセージの件名あるいは本文に受信したSyslogメッセージやSyslog統計の詳細を含めることができます。

ICQ number:

有効なICQ番号を入れてください。

From name:

任意の名前を入力できます。ICQメッセージのニックネームとして表示されます。

From e-mail address:

有効な返送アドレスを入力してください。ICQメッセージのEメールアドレスフィールドに表示されます。

Subject:

メッセージの件名を指定します。通常は %MsgHost と入力します。本来の syslogメッセージを送信したデバイスのホスト名に置き換えられます。

Insert message content or counter リンクをクリックすると指定可能な変数のポップアップメニューが表示されます。**Max message length** オプションを指定すれば送信する件名の文字数を制限できます。

Message:

ICQメッセージに送るメッセージを指定します。通常これは %MsgText と入力します。%MsgText は本来のsyslogメッセージのメッセージテキストで置き換えられます。

他の変数を挿入することもできます。Insert message content or counter リンクをクリックすると指定可能な変数のポップアップメニューが表示されます。**Max message length** オプションを指定すれば送信するメッセージの長さを制限できます。メッセージ本文に変数 %MsgText が含まれており、このようなときに大きなSyslogメッセージを受信してしまうと、ICQに送信するには大きすぎて送れなくなる可能性があります。このオプションを指定することによって、メッセージ本文を扱いやすい長さに制限することが可能です。

Expand <013><010> in message

<013> および <010> に事前に置き換えられたCRおよびLFを元に戻します。replace non printable characters with ASCII value オプションがチェックされているとSyslogメッセージに含まれているCR、LFは置き換えられます。ICQで転送する時に元の文字に戻すようにするとテキストが読み易くなり便利です。

例

下記はICQポケットベルメッセージの表示例です。

```
Nickname: Syslog Daemon
E-mail: syslog@company.com
Sender IP: xxx.xxx.xxx.xxx
Subject: firewall.company.com
Firewall Alert - Unauthorized login attempt: User=Administrator
```

[Test] ボタンをクリックすると指定したICQ番号にICQポケットベルメッセージがテスト送信されます。[Test Setup] ボタンをクリックすればテストメッセージの設定を変更できます。

Insert message content or counter

プログラム変数、カウンター、スクリプトフィールド、統計などをICQポケットベルメッセージに渡すには、Insert message content or counter リンクをクリックしてポップアップメニューからオプションを選択します。値の詳細については[関連項目](#)を参照してください。

このオプションではポップアップメニューから変数を選択します。変数はメッセージ送信前に現在の値で置き換えられます。例えば、%MsgText は現在のsyslogメッセージで置き換えられます。カーソルをフィールド内に置きハイパーリンクをクリックします。ポップアップメニューが表示されますので変数を選びます

例

```
subject: Syslog Alert from %MsgHost
message: Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText
```

3.3.14 Action - Send SNMP Trap (アクション – SNMPトラップ送信)

この機能は正規登録版でのみ使用できます。

フィルターにマッチしたSyslogメッセージを受信すると指定したIPアドレスにSNMPトラップを送信します。

File | Setup | Action を右クリックするか選択し Add New item をクリックすると新しいアクションを作成することができます。

次のパラメータを Send SNMP trap オプションで設定します。

Destination host

SNMPトラップを受信するシステムのIPアドレスを入力します。

Message text

転送するSNMPトラップの内容を入力します。このフィールドにはすべての標準メッセージ変数を挿入できます。これらの変数は Insert message content or counters リンク(Message text フィールドのすぐ上)をクリックして選択できます。

Agent IP address

SNMPトラップ送信元として表示されるIPアドレスです。デフォルトは From original sender ですが From this machine (つまりKiwi Syslog Daemonを実行しているマシンのアドレス)に設定することもできます。

Generic type

送信されるトラップタイプを示す0～6の値を指定します。version 1トラップに対してのみ適用されます。

値：

- 0 Cold Start
- 1 Warm Start
- 2 Link Down
- 3 Link Up
- 4 Authentication Failure
- 5 EGP Neighbor Loss
- 6 Enterprise Specific

上記の値はドロップダウンメニューから選択できます。

Version

Kiwi Syslog DaemonからSNMPトラップを受信するシステムがサポートするSNMPバージョン(v1あるいはv2)を選択します。

Enterprise OID

SNMPトラップのMIBエンタープライズを表す値(例: 1.3.6.1.x.x.x.x)を指定します。バージョン1トラップ専用のフィールドです。バージョン2トラップのエンタープライズ値はメッセージに2番目の変数としてバインドされています。

Generic Type を6に設定するとエンタープライズタイプトラップとなります。この場合特定のトラップ値を指定することを考慮しなければなりません。

Variable OID

バージョン2 SNMPトラップのMIB変数を表す値(例: 1.3.6.1.x.x.x.x)を指定します。

Community

トラップメッセージのパスワードのようなものです。通常この値は public, private または monitor に設定します。

Specific type

トラップ送信の原因を示す値を指定します。バージョン2トラップでは、この値は特定のトラップ(またはsyslogメッセージ)を送信するデバイスに定義されたMIBに固有の条件となります。

Remote port

SNMPトラップを送信するポートを指定します。デフォルトでは162に指定されています。

この設定を変更すると、SNMPトラップ受信デバイスの受信待機ポートも同じ番号にする必要があります。

3.3.15 Action – Stop processing message (アクション – メッセージ処理終了)

メッセージ処理を終了します。

このメッセージは他のルールでこれ以上評価されません。

3.3.16 Action - Run Script (アクション – スクリプト実行)

この機能は正規登録版でのみ使用できます。

(フリーウェア版はアクションのテストだけが可能です)

指定のスクリプトを実行し現在のメッセージに対するフィルターや解析処理を行います。

スクリプトの作成手順および使用方法については後述します。

スクリプトファイルの規則

スクリプトには必ず関数 **Main()** が含まれていなければなりません。パラメータは関数に渡されませんが、スクリプトの実行が成功したことを示す **OK** を返します。OK 以外が戻ってきた場合はスクリプトにエラーがあると判断され、エラーログに記録されます。スクリプト関数から返された値も診断用にエラーログに記録されます。

例(VBスクリプト):

```
Function Main()
```

```
' Your code goes here
```

```
' Set the return value
```

```
Main = "OK"
```

```
End Function
```

使用可能なスクリプト変数については[関連項目](#)を参照してください。

Script file name

スクリプトファイルはスクリプトコマンドが書かれた標準テキストファイルです。ファイルの拡張子は任意ですがデフォルトはメモ帳で編集しやすいよう .txt になっています。

Script description

任意の説明文を入力できます。スクリプトの機能を簡単に説明してください。

Script Language

Windows Script では Visual Basic® Scripting Edition と Microsoft Jscript® 2つのスクリプトエンジンがサポートされています。

VBScript - MS Word と Excel で使われる Visual Basic や VBA (Visual Basic for Applications)の一種です。学習しやすい上に豊富な機能セットがあります。

Jscript - Webで使われるJavaスクリプトの一種です。Javaスクリプトに精通している場合はこれを選択してください。

どちらの言語も機能面でも処理速度の面でも同等です。どちらを選択しても構いません。お好みで選んでください。Kiwi社でのテストでは、スクリプトが主に文字列操作である場合ほとんどのケースでJscriptの方が処理速度が速かったという結果が出ました。

VBScript に関しては以下のWebページを参照してください。

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/vtoriVBScript.asp>

J Script に関しては以下のWebページを参照してください。

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/js56jsoriJScript.asp>

他に Perl, Python, Ruby などのスクリプト言語も選択できます。

ただし、これらを選択した場合には対応するスクリプティングエンジンをインストールする必要があります。

PerlScript については次のWebページを参照してください。

<http://www.activestate.com/Products/ActivePerl>

Python については次のWebページを参照してください。

<http://www.activestate.com/Products/ActivePython>

ActiveScriptRuby については次のWebページを参照してください。

<http://arton.hp.infoseek.co.jp/index.html>

Edit script ボタン

メモ帳でスクリプトファイルを開きコードの確認/変更ができます。コードを変更したら必ずファイルを保存してください。[Test] ボタンでテストできます。

Test ボタン

指定のスクリプトを実行します。スクリプトには関数 **Main()** が含まれていなければなりません。Syslog Daemon から呼び出される唯一の関数です。Main() 関数から OK が返されるとスクリプトは成功したことになります。

スクリプト実行中にエラーが起こるとメッセージボックスにエラーの説明とその行番号が表示されます。スクリプト実行が成功し show test results オプションがチェックされていると実行前と実行後の変数が表示されます。スクリプトにより変数が変化することがわかります。

Setup 画面からスクリプトをテストすると([Test] ボタンを押す) キャッシュに保存されません。各スクリプトは実行前に新しくロードされます。

Show test results オプション

スクリプトが正しく実行され show test results オプションがチェックされていると実行前と実行後の変数が表示されます。スクリプトにより変数が変化することがわかります。

スクリプトファイルのキャッシュ

通常のオペレーションではスクリプトファイルがディスクから読まれるとキャッシュに入ります。プログラム実行速度が上がり余分なディスクアクセスが減ります。スクリプトを変更しディスクに保存してもプログラムを再起動しなければ効果はありません。

Kiwi Syslog Daemonを標準アプリケーションとして実行している場合は、File | Debug options | Clear the script file script file cache メニューでスクリプトファイルキャッシュをクリアし、ディスクからファイルをリロードすることが出来ます。あるいはメインウィンドウから [Ctrl]+[F8] を押しても同じことができます。

Kiwi Syslog Daemonをサービスとして実行している場合この機能は使用できません。スクリプトファイルキャッシュをクリアするには Manage メニューからサービスを停止し、再起動する必要があります。

ディスクから新しいスクリプトファイルを読み込もうと思ったら、キャッシュをクリアすることを忘れないでください。

Field Read/Write permissions

セキュリティと速度を確保するという理由で、メッセージおよびスクリプト変数に対するアクセスを制限することができます。スクリプトが実行されるたびに、メッセージフィールドがスクリプト変数にコピーされ、スクリプトが完了すると元に戻されます。コピーは時間とCPUサイクルを消費しますので、Read/Writeアクセスを使用したい変数のみに制限すると、実行速度が上がります。

フィールドグループの Read アクセスを有効にすると、値がスクリプト変数にコピーされますのでスクリプト内で読むことができます。

フィールドグループの Write アクセスを有効にすると、値がスクリプト変数からコピーされ対応するプログラムフィールドがその値で置換されます。

フィールドはスクリプト中で使用方法が似ているもの同士をグループ化できます。

フィールドの詳細については[関連項目](#)を参照してください。

共通フィールド

VarFacility
VarLevel
VarInputSource
VarPeerAddress
VarPeerName
VarPeerDomain
VarCleanMessageText

その他のフィールド

VarDate
VarTime
VarMilliSeconds
VarSocketPeerAddress
VarPeerAddressHex
VarPeerPort
VarLocalAddress
VarLocalPort
VarPriority
VarRawMessageText

カスタムフィールド

VarCustom01 から VarCustom16

下記のスクリプト変数はスクリプトからの Read/Write アクセスが常に可能です。

Inter-script フィールド

VarGlobal01 から VarGlobal16

Custom Statistics フィールド

VarStats01 から VarStats16

Control フィールドおよび Counter フィールド

ActionQuit
SecondsSinceMidnight
SecondsSinceStartup

定期的にスクリプトを起動する

Keep-alive input 関数を有効にすると、メッセージが定期的に挿入されます。このメッセージをスクリプトアクションのトリガーとして使えます。

3.3.16.1 練習 – 初めてのスクリプト作成

ここではどのように関数を作成し、それを使ってSyslogメッセージのテキストを検索し置き換えるかを説明します。

スクリプトアクションは正規登録版でのみ使用できます。フリーウェア版ではスクリプトアクションのテストはできますが、通常に使用することはできません。フル機能で使用できる30日間有効なトライアルキーを提供しております。次のWebページより入手してお試しください。

<http://www.kiwisyslog.com/trial>

ステップ1. スクリプトアクションの作成

Replace Text というルールを新規作成します。

Run Script アクションを新規作成します。

Script file name でファイル名を ReplaceText.txt にします。

Script description に Replaces occurrences of "cat" with "dog" と入力します。

Script language で VBScript を選択します。

Field Read/Write permissionsを以下のように設定します。

Common fields: Read=Yes, Write=Yes

Other fields: Read=No, Write=No

Custom fields: Read=No, Write=No

[Edit Script] ボタンを押してメモ帳でファイルを開いてください。ファイルが存在しないため新しいファイルを作成することを確認するメッセージが表示されます。[はい] を選択するとメモ帳で新しいファイルが作成されます。

メモ帳に以下のスクリプトをコピー&ペーストし、ファイル | 上書き保存をクリックします。

```
Function Main()
```

```
' Replace cat with dog within the message text field
```

```
Fields.VarCleanMessageText = Replace(Fields.VarCleanMessageText, "cat", "dog")
```

```
' Return OK to tell syslog that the script ran correctly.
```

```
Main = "OK"
```

```
End Function
```

ステップ 2. アクションの作成

Log to file アクションを新規作成します。

Path and file name of log file に任意のフォルダの下にファイル名 MyCustomLog.txt と入力します。

Log file format はデフォルトのままにします。

左枠の New action をクリックし [F4] キーを押すと自動的に Log to file という名前に変更されます。

Display アクションを新規作成します。

Display number はデフォルトのままにします。

左枠の New action をクリックし [F4] キーを押すと自動的に Display という名前に変更されます。

Run script アクションは Display および Log to file アクションの上にします。そうならない場合は Run script アクションを選択し、ツールバーにある ボタンで上へ動かします。

左枠に新しいルールが次のように追加されているはずです。

Rules

Rule: Replace Text

Filters

Actions

Run Script

Display

Log to file

ステップ3. スクリプトのテスト

Run Script アクションを選択します。

[Test Setup] ボタンをクリックします。

message text を The cat sat on the mat に変更します。

[Show action] ボタンをクリックします。

[Show test results] チェックボックスをチェックします。

[Test] ボタンをクリックします。

スクリプトを実行すると結果がメモ帳で表示されます。すべてのスクリプト変数が表示されています。VarCleanMessageText フィールドを見ると cat が dog に代わっていることがわかります。

ステップ 4. SyslogGen でスクリプトをテスト

Kiwi Syslog Daemon Setup 画面の [OK] ボタンをクリックし新しく作成したルールの変更を適用します。メイン画面に戻ります。

Kiwi SyslogGen を www.kiwisyslog.com からダウンロードします。
Kiwi Syslog Daemon をインストールしたのと同じマシンにインストールします。
Send オプションを send message once に設定します。
Destination を localhost (127.0.0.1) に設定します。
Message text を This is a test. The cat sat on the mat にします。
[Send] ボタンをクリックします。
画面に This is a test. The dog sat on the mat .と表示されます。

3.3.16.2 スクリプト変数

スクリプト間で受け渡される変数は多種多様です。アクションの Read/Write permissions 設定に従い、変数は変更されSyslogプログラムに返され使用されます。

変数および関数はグローバルにアクセスできる Fields というオブジェクト経由で渡されます。変数および関数にアクセスするには変数/関数名の前に Fields.を付けます。

共通フィールド

Fields.VarFacility

詳細: メッセージのファシリティ値

タイプ: 整数 (0-32767)

範囲: 0 ~ 23 ファシリティの一覧については[関連項目](#)を参照してください。

Fields.VarLevel

詳細: メッセージのレベル値

タイプ: 整数 (0-32767)

範囲: 0 ~ 7 レベルの一覧については[関連項目](#)を参照してください。

Fields.VarInputSource

詳細: メッセージの入力元

タイプ: 整数 (0-32767)

範囲: 0 to 2. 0=UDP, 1=TCP, 2=SNMP, 3 = KeepAlive, 4 = NT Event Log, 5 = Log file, 6 = Comm port
(4, 5, 6 は未使用)

Fields.VarPeerAddress

詳細:

送信デバイスのIPアドレス(フォーマットは nnn.nnn.nnn.nnn)。メッセージが他のSyslogコレクタから転送されても、この値は本来の送信元アドレスとなります。

ケース A.

ファイアーウォールデバイス (192.168.1.1) ---> 最初のSyslogコレクタ (192.168.1.2) ---> このSyslogコレクタ (192.168.1.3)
フィールドの値は 192.168.1.1です。

ケース B.

ファイアーウォールデバイス (192.168.1.1) ---> このSyslogコレクタ (192.168.1.3)
フィールドの値は 192.168.1.1です。

タイプ: 文字列

フォーマット: nnn.nnn.nnn.nnn ゼロパディングなし

例: 192.168.1.67

Fields.VarPeerName

詳細:

送信デバイスのホスト名。DNSルックアップオプションが有効でルックアップが成功した時に限り解決されたホスト名が入る。それ以外は VarPeerAddress と同じの値。フォーマットは nnn.nnn.nnn.nnn。FQDNのホスト名部分のみが入りドメインの接尾語は含まれない。

タイプ: 文字列

フォーマット: myhost

Fields.VarPeerDomain

詳細:

解決されている FQDNのドメイン名部分。ドメインの接尾語のみでが入りホスト名は含まれない。DNSルックアップオプションが有効でルックアップが成功した時に限り値が入る。それ以外は空白。

タイプ: 文字列

フォーマット: mydomain.com

Fields.VarCleanMessageText

詳細:

(ヘッダー削除, DNS ルックアップ, 元のアドレス削除, Cisco 日付削除など)変更後の文字列。

タイプ: 文字列

例:

%SEC-6-IPACCESSLOGP: list 101 denied udp 10.0.0.3 (firewall) (137) -> 216.7.14.105 (webservers.company.com) (137), 1 packet

その他のフィールド

Fields.VarDate

詳細: メッセージ受信日付

タイプ: 文字列(10バイト)

フォーマット: YYYY-MM-DD

例: 2002-03-17

Fields.VarTime

詳細: メッセージ受信時刻

タイプ: 文字列(8バイト)

フォーマット: HH:MM:SS

例: 23:10:04

Fields.VarMilliSeconds

詳細: 1/1000秒単位のメッセージ受信時刻

タイプ: 文字列 (3バイト)

範囲: 000 ~ 999

フォーマット: nnn (3バイト, ゼロパディング)

Fields.VarSocketPeerAddress

詳細: メッセージ送信デバイスまたは最も近いコレクタのIPアドレス

ケース A.

ファイアウォールデバイス (192.168.1.1) ---> 最初のSyslogコレクタ (192.168.1.2) ---> このsyslogコレクタ (192.168.1.3)

値は 192.168.1.2.

ケース B.

ファイアウォールデバイス (192.168.1.1) ---> このsyslog コレクタ (192.168.1.3)

値は 192.168.1.3.

タイプ: 文字列

フォーマット: nnn.nnn.nnn.nnn.ゼロパディングなし

例: 192.168.1.67

Fields.VarPeerAddressHex

詳細:

メッセージを送信したIPアドレスを8桁16進数に変換。

16進アドレスはIPマスクとIPレンジフィルターに使用。VarPeerIPAddress を変更しIPマスクやIPレンジフィルターを使うには VarPeerAddressHex フィールドも変更します。

タイプ: 文字列 (8バイト)

範囲: 00000000 から FFFFFFFF

例: COA80102 (192.168.1.2 を2バイト16進数に変換。ゼロパディング)

Fields.VarPeerPort

詳細: メッセージを送信した UDP/TCP ポート

タイプ: 整数 (0-65535)

範囲: 0 から 65535

通常使用する値: 1023以上の値

Fields.VarLocalAddress

詳細: このマシンにメッセージを送信したIPアドレス

タイプ: 文字列

例: 127.0.0.1, 192.168.1.2

Fields.VarLocalPort

詳細: メッセージを受信したローカルマシンのUDP/TCP ポート

タイプ: 整数 (0-65535)

範囲: 0 から 65535

通常使用する値: UDP では514, TCPでは1468, SNMPでは162

Fields.VarPriority

詳細: メッセージプライオリティ値

タイプ: 整数 (0-32767)

範囲: 0 から191

Fields.VarRawMessageText

詳細:

変更前の受信メッセージ (<pri> タグ, 元のアドレスなどを含む)。

このフィールドは読み取り専用です。スクリプトのフィールドを変更しても対応するプログラム変数は変更されません。

カスタムフィールド

これらのフィールドは動的に変更され、新しいメッセージを受信するたびにクリアされます。これらのフィールドにはスクリプトの結果が入るため Log to file や Log to Database アクションに使われます。このフィールドの値は %VarCustom01 **Insert message content or counter** オプションか AutoSplit 文を使ってアクションにパラメータとして渡すこともできます。メッセージをスクリプトでいくつかのフィールドに分割し、ファイルやデータベースの対応するフィールドに記録するのに適しています。

カスタムフィールドは16個あります。1 ~ 9 まではゼロパディングされます(VarCustom1ではなくVarCustom01となります)。

Fields.VarCustom01 から Fields.VarCustom16

スクリプト間フィールド

固定されておりメッセージを受信しても変化しません。他のスクリプトへの値の受け渡し、同一スクリプトで後に利用するために値を維持するためのものです。%VarGlobal01 **Insert message content or counter** オプションか AutoSplit 文を使って値をパラメータとしてアクションに渡すこともできます。

グローバルフィールドは16個あります。1 ~ 9 まではゼロパディングされます(VarCustom1ではなくVarCustom01となります)。

Fields.VarGlobal01 から Fields.VarGlobal16

カスタムスクリプトフィールド

固定されておりメッセージを受信しても変化しません。自身のカスタム統計とカウンター用に使われます。%VarStats01 **Insert message content or counter** オプションを使って値をパラメータとしてアクションに渡すこともできます。

Syslog Statistics ウィンドウの Counters タブで現在のフィールド値を見ることができます。カスタム統計は日別統計Eメールにも記載されています。

統計フィールドの名前と初期値は Scripting オプションから設定します。

カスタム統計フィールドは16個あります。1 ~ 9 まではゼロパディングされます(VarStats1ではなくVarStats01となります)。

Fields.VarStats01 から Fields.VarStats16

コントロールとタイミングフィールド

Fields.ActionQuit

詳細:

スクリプト実行後に何をするかを設定します。0 はルール次のアクションを続けます。1 ~ 99はルール内でスキップするアクション数です(1=次の1アクションをスキップ、3=次の3アクションをスキップ)。100 は次のルールへのジャンプです。1000 はすべてのルールをスキップしメッセージ処理を終了します。値が指定されていないときは 0 とみなされます。

タイプ: 整数 (0-32767)

範囲: 0 から 1000

指示: 0=スキップしない, 1-99=スキップするアクション数, 100=次のルールまでスキップ, 1000=メッセージ処理終了

Fields.SecondsSinceMidnight

詳細: 深夜0時からの経過時間 (秒)

タイプ: ロング (0-20億)

範囲: 0 ~ 86400

Fields.SecondsSinceStartup

詳細: プログラム起動からの経過時間 (秒)

タイプ: ロング (0-20億)

3.3.16.3 スクリプト関数

Fields オブジェクトから利用できる組み込み関数は多数あります。今後のリリースではさらに追加され、スクリプティングエンジンの機能強化を図る予定です。

組み込み関数は Fields オブジェクトの前に実行したい関数名を付けるだけで使用できます。必要なパラメータが渡され、結果が返されます。

Fields オブジェクトの組み込み関数

Fields.IsValidIPAddress(IPAddress as string) as Boolean

機能: 渡された文字列をチェックし正しいIPアドレスフォーマットであれば true を返す

入力パラメータ: IPアドレス文字列

結果: ブール値 (true/false)

使用例:

```
If Fields.IsValidIPAddress(Fields.VarPeerAddress) = True then
    Fields.VarCustom01 = Fields.VarPeerAddress
End if
```

Fields.ConvertIPtoHex(IPAddress As String) As String

機能: IPアドレスを8バイトの16進数に変換

入力パラメータ: IPアドレス文字列

結果: 8 バイト16進数

使用例:

```
If Fields.IsValidIPAddress(Fields.VarPeerAddress) = True then
    Fields.VarCustom01 = Fields.ConvertIPToHex(Fields.VarPeerAddress)
End if
```

Fields.GetDailyStatistics() As String

機能: CRLF区切りで日別統計を返す

入力パラメータ: なし

結果: 文字列

使用例:

```
MyStats = Fields.GetDailyStatistics()
```

結果はファイルやEメール等へ書き出されます。

Fields.ConvertPriorityToText(PriorityValue)

機能: メッセージプライオリティ値をファシリティ レベルによるテキスト表現に変換

入力パラメータ: プライオリティ値

範囲: 0 ~ 191

結果: ファシリティ レベル文字列

例: 191 は Local7.Debug を返す

使用例 :

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
```

```
' Use the date and time from the current message
```

```
With Fields
```

```
MsgDate = .VarDate & " " & .VarTime
```

```
MsgText = "This is a test message from the scripting action"
```

```
Data = MsgDate & vtab & .ConvertPriorityToText(.VarPriority) & vtab & _  
.VarPeerAddress & vtab & MsgText
```

```
Call .ActionLogToFile(Filename, Data)
```

```
End with
```

Fields.ActionPlaySound(SoundFilename As String, RepeatCount as Long)

機能: 音を鳴らす、あるいは指定したwavファイルを実行。X 回もしくはキャンセルされるまで繰り返す。

入力パラメータ: サウンドファイル名文字列, ロング値で繰り返し回数

結果: なし

サウンドファイル名が空白の場合はシステムビープ音を鳴らす。

RepeatCount オプション:

0 = キャンセルされるまで繰り返し(メイン表示ウィンドウで点滅するベルを押してキャンセルします)

1 ~ 100 = 繰り返し数

繰り返し数が1以上の時、5秒間隔でサウンドまたはビープ音が鳴ります。

使用例:

```
' Play the squeak sound 5 times
```

```
Call Fields.ActionPlaySound("C:\Program Files\Syslogd\Sounds\Squeak.wav", 5)
```

```
' Play the squeak sound until cancelled
```

```
Call Fields.ActionPlaySound("C:\Program Files\Syslogd\Sounds\Squeak.wav", 0)
```

```
' Play the system beep sound 10 times
```

```
Call Fields.ActionPlaySound("", 10)
```

```
' Play the system beep sound until cancelled
```

```
Call Fields.ActionPlaySound("", 0)
```

Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage , [MailImportance] , [MailPriority] , [MailSensitivity])

機能: 指定のアドレスにEメールを送信

結果: なし

E-mail Delivery Options(Importance、Priority、Sensitivity)の指定は任意です。

Eメール送信オプション

以下のパラメータを使用してEメールメッセージに Importance(重要度)、Priority(プライオリティ)、Sensitivity(種類)のフラグを設定できます。Eメール受信者には適宜これらのレベルが付けられたメッセージが届きます。

MailImportance: 0 - Unspecified (デフォルト)

1 - High

2 - Normal

3 - Low

MailPriority: 0 - Unspecified (デフォルト)

1 - Normal

2 - Urgent

3 - Non-Urgent

MailSensitivity: 0 - Unspecified (デフォルト)

1 - Personal

2 - Private

3 - Confidential

複数のアドレスにメッセージを送信する場合は各アドレスをカンマで区切ります。

例

```
MailTo = "user1@company.com,user2@company.com,user3@company.com"
```

使用例: Eメール送信オプションをデフォルト値で joe@company.com にEメール送信
MailTo = "joe@company.com"
MailFrom = "server@company.com"
MailSubject = "This is a test of the scripting action"
MailMessage = "This is a test mail message" & vbCrLf & "Multiple lines."

Call Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage)

使用例: Eメール送信オプションを Importance = High、Priority = Urgent、Sensitivity = Confidential で
joe@company.com にEメール送信
MailTo = "joe@company.com"
MailFrom = "server@company.com"
MailSubject = "This is a test of the scripting action"
MailMessage = "This is a test mail message" & vbCrLf & "Multiple lines."
MailImportance = 1
MailPriority = 2
MailSensitivity = 3
Call Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage, MailImportance,
MailPriority, MailSensitivity)

**Fields.ActionLogToFile(Filename, Data, [RotateLogFile] , [RotationType] , [NumLogFiles] ,
[Amount] , [Unit])**

機能: 指定のログファイルの終わりにデータを追加
結果: なし

メッセージログをファイルに独自のフォーマットで記録します。

ファイル名に AutoSplit 値が使えます。
ファイル名に現在の時刻を含めるには %TimeHH を使います。

例: Filename = "C:\Program files\Syslogd\Logs\TestLog%TimeHH.txt"

使用例:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"  
MsgPriority = "Local7.Info"  
MsgHostAddress = Fields.VarPeerAddress  
' Use the date and time from the current message  
MsgDate = Fields.VarDate & " " & Fields.VarTime  
MsgText = "This is a test message from the scripting action"  
Data = MsgDate & vtab & MsgPriority & vtab & MsgHostAddress & vtab & MsgText
```

Call Fields.ActionLogToFile(Filename, Data)

注: この例では Other fields の Read 権限が有効になっていなければなりません。VarDate とVarTime 変数がスクリプトを読むことができるようにするためです。

ログファイルローテーション:

Kiwi Syslog Daemon のログファイルローテーション機能についての詳細は[関連項目](#)を参照してください。

パラメータ RotateLogFile, RotationType, NumLogFiles, Amount および Unit の指定は任意ですが、ローテートされるログファイルに記録する場合は必須です。

RotateLogFile: 0 = ローテートしない
1 = ローテートする

RotationType: 0 = **ログファイルサイズ**が Amount や Unit の指定値を超えた場合にローテートする
1 = **ログファイルの経過時間**が Amount や Unit の指定値を超えた場合にローテートする

NumLogFiles: ローテーションで使用するログファイルの数

Amount: For RotationType=0 : Amount はファイルサイズ
For RotationType=1 : Amount はファイルの経過時間

Unit For RotationType=0 : ファイルサイズを示す単位。Amount の単位としてバイト、キロバイト、メガバイト…
のどれが適用されるかを指定
0 = バイト
1 = キロバイト
2 = メガバイト
3 = ギガバイト

For RotationType=1: ファイルの経過時間を示す単位。Amount の単位として分、日、週...のどれが適用されるかを指定
0 = 分
1 = 時
2 = 日
3 = 曜日
4 = 週
5 = 月
6 = 四半期
7 = 年

使用例:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"  
MsgPriority = "Local7.Info"  
MsgHostAddress = Fields.VarPeerAddress  
' Use the date and time from the current message  
MsgDate = Fields.VarDate & " " & Fields.VarTime  
MsgText = "This is a test message from the scripting action"  
Data = MsgDate & vtab & MsgPriority & vtab & MsgHostAddress & vtab & MsgText  
RotateLogFile = 1 'Rotate this log  
RotationType = 0 'Using File size rotation -  
NumLogFiles = 4 'Use up to 4 log files  
Amount = 1000 'Each log file no more than 1000  
Unit = 0 'bytes in length
```

Call Fields.ActionLogToFile(Filename, Data, RotateLogFile, RotationType, NumLogFiles, Amount, Unit)

使用例 (2):

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"  
MsgPriority = "Local7.Info"  
MsgHostAddress = Fields.VarPeerAddress  
' Use the date and time from the current message  
MsgDate = Fields.VarDate & " " & Fields.VarTime  
MsgText = "This is a test message from the scripting action"  
Data = MsgDate & vtab & MsgPriority & vtab & MsgHostAddress & vtab & MsgText  
RotateLogFile = 1 'Rotate this log  
RotationType = 1 'Using File age rotation -  
NumLogFiles = 12 'Use up to 12 log files  
Amount = 1 'Each log file no more than 1  
Unit = 5 'month old
```

Call Fields.ActionLogToFile(Filename, Data, RotateLogFile, RotationType, NumLogFiles, Amount, Unit)

Fields.ActionSendSyslog(Hostname, Message, Port, Protocol)

機能: syslogメッセージをホスト名の Protocol で指定したポートに送信
結果: なし

Hostname: リモートホストのホスト名またはIPアドレス
Message: プライオリティタグとsyslogメッセージ文を含むテキスト
Port: 1 ~ 65535の整数 (514 が標準syslogポート)
Protocol: 0 または 1 (0=UDP, 1=TCP)

他のホストにUDPまたはTCPでsyslogメッセージを送信する関数です。

使用例:

```
Hostname = "10.0.0.1" ' Remote syslog host  
Priority = 191 ' Local7.Debug  
Port = 514 ' Use the standard syslog port  
Protocol = 0 ' 0=UDP, 1=TCP  
' Construct the syslog message by adding <PRI> value to the front of the text  
Message = "<" + Cstr(Priority) + ">" + "This is an example of a syslog message"
```

Call Fields.ActionSendSyslog(Hostname, Message, Port, Protocol)

Fields.ActionSpoofSyslog(AdapterAddress, SrcAddress, DstAddress, DstPort, Message)

機能: 見せかけのSyslogメッセージ(UDPのみ)を DstAddress の DstPort ポート宛に送信

結果: なし

AdapterAddress: メッセージ送信元のネットワークアダプタのIPまたはMACアドレス(例: IPアドレス 192.168.0.1、MACアドレス 00:50:56:C0:00:08)

SrcAddress: メッセージ送信元のホスト名またはIPアドレス(メッセージは現物でも見せかけでも構わない)

DstAddress: リモートホスト(受信用)のホスト名またはIPアドレス

DstPort: 1 ~ 65535の整数 (514 が標準syslogポート)

Message: プライオリティタグとsyslogメッセージ文を含むテキスト

他のホストにUDPでsyslogメッセージを送信する関数です。

使用例:

```
AdapterAddress = "192.168.1.100"    ' Adapter Address (Can be IP Address- ie "192.168.0.1", or MAC address - ie. "00:50:56:C0:00:08")
SrcAddress = "192.10.10.1"         ' Source of message
DstAddress = "10.0.0.1"           ' Destination of message
DstPort = 514                      ' Use the standard syslog port
Priority = 191                      ' Local7.Debug
```

```
' Construct the syslog message by adding <PRI> value to the front of the text
Message = "<" + Cstr(Priority) + ">" + "This is an example of a syslog message"
```

Call Fields.ActionSpoofSyslog(AdapterAddress, SrcAddress, DstAddress, DstPort, Message)

重要:

Kiwi Syslog Daemonでこのネットワークパケットのスプーフィング機能をサポートするのは次のプラットフォームのみです。

Windows 2000/XP/2003 (Window 95/98/Me/Vista はサポート対象外)。また、WinPcap バージョン3.0以上がインストールされていなければなりません。WinPcap (Windows Packet Capture library)は<http://www.winpcap.org/>からダウンロードできます。

Fields.ActionLogToFileWithCache(Filename, Data, [RotateLogFile] , [RotationType] , [NumLogFiles], [Amount] , [Unit])

機能: 指定のログファイルにデータを書きます。キャッシュは100メッセージまたは5秒ごとにクリアされます。キャッシュの設定はレジストリで行います。この関数は書き込みキャッシュを使うこと以外は ActionLogToFile と同じです。毎秒10メッセージ以上を受信する場合は書き込みキャッシュ関数を使ってください。

結果: なし

メッセージログをファイルに独自のフォーマットで記録します。

ファイル名に AutoSplit 値が使えます。

ファイル名に現在の時刻を含めるには %TimeHH を使います。

例: Filename = "C:\Program files\Syslogd\Logs\TestLog%TimeHH.txt"

使用例:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
MsgPriority = "Local7.Info"
MsgHostAddress = Fields.VarPeerAddress
' Use the date and time from the current message
MsgDate = Fields.VarDate & " " & Fields.VarTime
MsgText = "This is a test message from the scripting action"
Data = MsgDate & vbtab & MsgPriority & vbtab & MsgHostAddress & vbtab & MsgText
```

Call Fields.ActionLogToFileWithCache(Filename, Data)

注:この例では Other fields の Read 権限が有効になっていなければなりません。VarDate とVarTime 変数がスクリプトを読むことができるようにするためです。

ログファイルローテーション:

Kiwi Syslog Daemon のログファイルローテーション機能についての詳細は[関連項目](#)を参照してください。

パラメータ RotateLogFile, RotationType, NumLogFiles, Amount および Unit の指定は任意ですが、ローテートされるログファイルに記録する場合は必須です。

RotateLogFile: 0 = ローテートしない

1 = ローテートする

RotationType: 0 = **ログファイルサイズ**が Amount や Unit の指定値を超えた場合にローテートする

1 = **ログファイルの経過時間**が Amount や Unit の指定値を超えた場合にローテートする

NumLogFiles: ローテーションで使用するログファイルの数

Amount: For RotationType=0 : Amount はファイルサイズ

For RotationType=1 : Amount はファイルの経過時間

Unit For RotationType=0 : ファイルサイズを示す単位。Amount の単位としてバイト、キロバイト、メガバイト…のどれが適用されるかを指定

0 = バイト

1 = キロバイト

2 = メガバイト

3 = ギガバイト

For RotationType=1: ファイルの経過時間を示す単位。Amount の単位として分、日、週…のどれが適用されるかを指定

0 = 分

1 = 時

2 = 日

3 = 曜日

4 = 週

5 = 月

6 = 四半期

7 = 年

使用例:

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
```

```
MsgPriority = "Local7.Info"
```

```
MsgHostAddress = Fields.VarPeerAddress
```

```
' Use the date and time from the current message
```

```
MsgDate = Fields.VarDate & " " & Fields.VarTime
```

```
MsgText = "This is a test message from the scripting action"
```

```
Data = MsgDate & vtab & MsgPriority & vtab & MsgHostAddress & vtab & MsgText
```

```
RotateLogFile = 1 'Rotate this log
```

```
RotationType = 0 'Using File size rotation -
```

```
NumLogFiles = 4 'Use up to 4 log files
```

```
Amount = 1000 'Each log file no more than 1000
```

```
Unit = 0 'bytes in length
```

```
Call Fields.ActionLogToFileWithCache(Filename, Data, RotateLogFile, RotationType, NumLogFiles, Amount, Unit)
```

使用例 (2):

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"
```

```
MsgPriority = "Local7.Info"
```

```
MsgHostAddress = Fields.VarPeerAddress
```

```
' Use the date and time from the current message
```

```
MsgDate = Fields.VarDate & " " & Fields.VarTime
```

```
MsgText = "This is a test message from the scripting action"
```

```
Data = MsgDate & vtab & MsgPriority & vtab & MsgHostAddress & vtab & MsgText
```

```
RotateLogFile = 1 'Rotate this log
```

```
RotationType = 1 'Using File age rotation -
```

```
NumLogFiles = 12 'Use up to 12 log files
```

```
Amount = 1 'Each log file no more than 1
```

```
Unit = 5 'month old
```

```
Call Fields.ActionLogToFileWithCache(Filename, Data, RotateLogFile, RotationType, NumLogFiles, Amount, Unit)
```

Fields.ActionDeleteFile(Filename)

機能: 指定ファイルを削除

結果: なし

ログファイルを削除し完全なスタート状態にします。

ワイルドカードを使用できませんので、完全なファイル名を指定する必要があります。確認メッセージが表示されないため、慎重に使用してください。

使用例：

```
Filename = "C:\Program files\Syslogd\Logs\TestLog.txt"  
Call Fields.ActionDeleteFile(Filename)
```

Fields.ActionDisplay(DisplayNumber, TabDelimitedMessage)

機能：指定したバーチャルディスプレイ番号にメッセージを表示

結果：なし

画面に独自フォーマットのメッセージを表示するための関数です。

TabDelimitedMessage には5個のタブ区切りフィールドを指定します。各フィールドの内容は何でもかまいません。標準の表示フィールド：日付 [TAB] 時刻 [TAB] プライオリティ [TAB] ホスト名 [TAB] メッセージ

使用例：

With Fields

```
MsgPriority = ConvertPriorityToText(.VarPriority)  
MsgHostAddress = .VarPeerAddress  
' Use the date and time from the current message  
MsgDate = .VarDate & " " & .VarTime  
MsgText = "This is a test message from the scripting action"  
Display = MsgDate & vbtab & MsgTime & vbtab & MsgPriority & vbtab &  
MsgHostAddress & vbtab & MsgText  
Call .ActionDisplay(0, Display)
```

End with

Fields.ActionLogToODBC(DSNString, TableName, InsertStatement, Timeout)

機能：DSNString とTableNameで指定したデータベースに InsertStatement を渡す。

Timeout はデータベース接続を待つ時間（秒）です。

結果：成功ではブランク。その他の場合は文字列。

この関数はメッセージをデータベースに独自フォーマットで記録するためのものです。データベース接続はプログラム内で開かれます。データを送信するたびに接続の生成と切断を行うことによるオーバーヘッドを防ぐためです。データベースへの送信データがなくなり、タイムアウト時間が過ぎると接続が遮断されます。次にデータ送信されるときに再接続されます。

使用例：

"KiwiSyslog" というSystem DSNが生成されており、MS Access データベースをポイントするコードです。書き込むデータベースタイプによりSQL挿入文の構文は若干異なります。以下の例は MS Access 97 および2000で実証済みです。

必要なフィールドすべてが設定された "Syslogd" というテーブルが作成済みであることを前提とします。

```
MyDSN = "DSN=KiwiSyslog;"  
MyTable = "Syslogd"  
MyFields = "MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText"
```

```
' MS Access DB SQL INSERT command example:  
' INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText)  
' VALUES ('2004-08-08','13:26:26','Local7.Debug','host.company.com',  
' This is a test message from Kiwi Syslog Daemon')
```

With Fields

```
' Construct the insert statement  
SQLcmd = "INSERT INTO " & MyTable & " (" & MyFields & ") VALUES (" & _  
Quote(.VarDate) & "," & Quote(.VarTime) & "," & _  
Quote(.ConvertPriorityToText(.VarPriority)) & "," & _  
Quote(.VarPeerAddress) & "," & Quote(.VarCleanMessageText) & ")"  
' Log the data to database using DSN, Table, SQLcmd and Timeout of 30 seconds  
.VarCustom01 = .ActionLogToODBC(MyDSN, MyTable, SQLcmd, 30)  
' VarCustom01 now holds the return value from the function.
```

End with

Function Quote(Data)

' Replace all occurrences of ' with '' to escape existing quotes

' Wrap data with single quotes

= '''' & Replace(Data, ''', ''''') & ''''

End Function

注:この例では Other fields の Read 権限が有効になっていなければなりません。VarDate とVarTime 変数がスクリプトを読むことができるようにするためです。

注:\Scripts サブフォルダにはサンプルコードが他にもいくつか用意されています。

3.3.16.4 スクリプト記述辞書

Kiwi Syslog Daemon バージョン8.1 に新しく付け加えられた辞書機能を使えばデータキーとアイテムを対応させる(名前付き)辞書を作成できます。辞書に登録されたデータは永続データでありアプリケーションが使用されている限り消えることはありません。辞書の範囲は基本的に Fields ネームスペースの VarGlobal 変数と同じです。

名前付き辞書は PERL 連想配列と同等です。アイテムはデータ形式を問わず配列内に格納されます。アイテムごとに固有のキーが関連付けられています。キーは個々のアイテムを取得する際に使用され、通常は整数または文字列ですが配列以外であれば何でも構いません。

すべての辞書のメソッドおよびプロパティには dictionaries ネームスペースからアクセスできます。

Dictionaries オブジェクトの組み込み関数

StoreItem(dicName As String, dicKey As String, dicItem As Variant)

StoreItem メソッドはキーとアイテムを組み合わせて名前付き辞書に保存します。

dicName 必須。辞書の名前。指定した名前の辞書が存在しない場合は新規作成される
dicKey 必須。保存するアイテムに関連付けられているキー。指定したキーが存在しない場合は新規作成される
dicItem 必須。保存するキーに関連付けられているアイテム

例: Call Dictionaries.StoreItem("MyDictionary", "MyKeyName", "MyItemValue")

.AddItem() と .UpdateItem() は Kiwi Syslog Daemon のバージョン8.1.4から .StoreItem() メソッドに変更されました。旧バージョンとの互換性を維持するために .AddItem() と .UpdateItem() は今後も継続して使用できます。

AddItem(dicName As String, dicKey As String, dicItem As Variant)

AddItem メソッドはキーとアイテムの組み合わせを名前付き辞書に追加します。キー **dicKey** が **dicName** に既に登録されている場合エラーとなります。

dicName 必須。辞書の名前。指定した名前の辞書が存在しない場合は新規作成される
dicKey 必須。追加するアイテムに関連付けられているキー
dicItem 必須。追加するキーに関連付けられているアイテム

例: Call Dictionaries.AddItem("MyDictionary", "MyKeyName", "MyItemValue")

UpdateItem(dicName As String, dicKey As String, dicItem As Variant)

UpdateItem メソッドは **dicKey** と関連付けられているアイテムを **dicItem** の値で更新します。**dicName** の辞書にのみ適用されます。**dicName** の辞書あるいは **dicKey** のキーが存在しない場合エラーとなります。

dicName 必須。辞書の名前。
dicKey 必須。更新されるアイテムに関連付けられているキー
dicItem 必須。更新後の新しいアイテム

例: Call Dictionaries.UpdateItem("MyDictionary", "MyKeyName", "MyNewItemValue")

RemoveItem(dicName As String, dicKey As String)

RemoveItem メソッドは **dicName** の辞書からキーとアイテムの組み合わせを削除します。**dicName** の辞書あるいは **dicKey** のキーが存在しない場合エラーとなります。

dicName 必須。辞書の名前
dicKey 必須。削除されるアイテムに関連付けられているキー

例： Call Dictionaries.RemoveItem("MyDictionary", "MyKeyName")

RemoveAll(dicName As String)

RemoveAll メソッドは **dicName** の辞書に登録されているすべてのキーとアイテムの組み合わせを削除します。**dicName** の辞書が存在しない場合エラーとなります。

dicName 必須。辞書の名前

例： Call Dictionaries.RemoveAll("MyDictionary")

Delete(dicName As String)

Delete メソッドは **dicName** の辞書全体を削除します。**dicName** の辞書が存在しない場合エラーとなります。

dicName 必須。削除される辞書の名前

例： Call Dictionaries.RemoveItem("MyDictionary", "MyKeyName")

DeleteAll()

DeleteAll メソッドはすべての辞書を削除します。

例： Call Dictionaries.DeleteAll()

GetItemCount(dicName As String) As Long

GetItemCount プロパティは **dicName** の辞書に登録されているアイテムの数を返します。**dicName** の辞書が存在しない場合エラーとなります。

dicName 必須。辞書の名前

例： itemCount = Dictionaries.GetItemCount("MyDictionary")

GetItem(dicName As String, dicKey As String) As Variant

GetItem プロパティは **dicName** の辞書に登録されている **dicKey** のキーに対応するアイテムを返します。**dicName** の辞書あるいは **dicKey** のキーが存在しない場合エラーとなります。

dicName 必須。辞書の名前
dicKey 必須。フェッチされるアイテムに関連付けられているキー

例： MyItem = Dictionaries.GetItem("MyDictionary", "MyKeyName")

ItemExists(dicName As String, dicKey As String) As Boolean

ItemExists プロパティは **dicKey** に指定したキーが **dicName** の辞書に存在する場合 **True** を返します。**dicName** の辞書が存在しない場合エラーとなります。

dicName 必須。辞書の名前

dicKey 必須。フェッチされるアイテムに関連付けられているキー

```
例： If Dictionaries.ItemExists("MyDictionary", "MyKeyName") Then
...
End If
```

GetKeys(dicName As String) As Variant

GetKeys プロパティは **dicName** の辞書に登録されているすべてのキーを含む配列を返します。**dicName** の辞書が存在しない場合エラーとなります。

dicName 必須。辞書の名前

```
例： MyKeyArray = Dictionaries.GetKeys("MyDictionary")
For i = 0 to UBound(MyKeyArray)
ThisKey = MyKeyArray(i)
...
Next
```

GetItems(dicName As String) As Variant

GetItems プロパティは **dicName** の辞書に登録されているすべてのアイテムを含む配列を返します。**dicName** の辞書が存在しない場合エラーとなります。

dicName 必須。辞書の名前

```
例： MyItemArray = Dictionaries.GetItems("MyDictionary")
For i = 0 to UBound(MyItemArray)
ThisItem = MyItemArray(i)
...
Next
```

エラーリファレンス

関数名	エラー
GetName()	Script Error executing .GetName() - Dictionary does not exist
Delete()	Script Error executing .Delete() - Dictionary [x] does not exist
AddItem() [y]	Script Error executing .AddItem() - Dictionary Key [x] already exists in dictionary
UpdateItem()	Script Error executing .UpdateItem() - Dictionary Key [x] does not exist in dictionary [y] Script Error executing .UpdateItem() - Dictionary [x] does not exist
RemoveItem()	Script Error executing .RemoveItem() - Dictionary Key [x] does not exist in dictionary [y] Script Error executing .RemoveItem() - Dictionary [x] does not exist
RemoveAllItems()	Script Error executing .RemoveAllItems() - Dictionary [x] does not exist
GetItemCount()	Script Error executing .GetItemCount() - Dictionary [x] does not exist
GetItems()	Script Error executing .GetItems() - Dictionary [x] does not exist
GetKeys()	Script Error executing .GetKeys() - Dictionary [x] does not exist
GetItem()	Script Error executing .GetItem() - Dictionary Key [x] does not exist in dictionary [y] Script Error executing .GetItem() - Dictionary [x] does not exist
ItemExists()	Script Error executing .ItemExists() - Dictionary [x] does not exist

3.3.16.5 スクリプト例

手始めにヘルプファイルに書かれているスクリプトで練習してください。今後もより多彩なサンプルスクリプトやチュートリアルをWebサイト <http://www.kiwisyslog.com> で公開する予定でいます。

プログラムに付属のサンプルスクリプトには音を鳴らす、Eメール送信、ファイルへのログ記録等を実行するためのスクリプトを用意しています。これらのサンプルは Kiwi Syslog Daemonをインストールしたフォルダの\Scripts サブフォルダの下にあります。

他のユーザーにとっても有効なスクリプトを作成したら support@kiwisyslog.com までEメールで送ってください。Kiwi社のWebサイトにて公開します。

3.3.16.5.1 PIX メッセージの検査

下記の関数は特定のPIXメッセージ数を調べカスタムメッセージフィールドに説明を送ります。カスタムフィールドはSend e-mail アクションで使います。

このスクリプトの値はCisco Webサイトで見る事が出来ます :

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/pixmsgs.htm

スクリプトアクション設定

Common fields: Read=yes

Custom fields: Write=yes

ルール設定

Rules

Rule: Lookup PIX msg

Filters

Filter: Host IP address: Simple: Match PIX firewall address

Actions

Action: Run Script: Lookup PIX msg

Action: Send e-mail

To: helpdesk@company.com:

Subject: Problem with PIX

Body: %MsgText%

Explanation: %VarCustom01

Action to take: %VarCustom02

Function Main()

' Set the return value to OK

Main = "OK"

' By default, skip to the next rule, don't take the actions that follow

' If we exit the function before we get to the end, the default 'skip to next rule'

' will be used.

Fields.ActionQuit = 100

' Example of a PIX message

' %PIX-4-209004: Invalid IP fragment...

Dim M ' Message

Dim E ' Explanation

Dim A ' Action

' Copy message to local variable for speed

M = Fields.VarCleanMessageText

' If message length is too short, exit function

If Len(M) < 15 then exit function

' Grab the first 15 chrs

M = Left(M,15)

' Check the message is a valid PIX message

If Mid(M,1,5) <> "%PIX-" then exit function

' Add any additional checks you want to perform here

' Grab the important part ("4-209004")

M = Mid(M,6,8)

E = ""

A = ""

' Now lookup the values and create an explanation and action for each match

Select Case M

Case "4-209004"

E = "An IP fragment is malformed. The total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes"

A = "A possible intrusion event may be in progress. If this message persists, contact the remote peer's administrator or upstream provider."

Case "2-106012"

E = "This is a connection-related message. A IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded."

A = "A security breach was probably attempted. Check the local site for loose source or strict source routing."

' Insert other values to lookup here

End Select

' Exit if we don't have any values to pass

If len(E) = 0 then exit function

If len(A) = 0 then exit function

' Pass the Explanation and Action to take to the custom variables

Fields.VarCustom01 = E

Fields.VarCustom02 = A

' Since we have a valid match, we want to execute the send e-mail action which follows.

' Setting ActionQuit to 0 means we won't skip any actions.

Fields.ActionQuit = 0

End function

3.16.5.2 全ての変数 (Info関数)

下記の関数は全フィールドの変数を表示します。参考として作成したスクリプトにコピー&ペーストしておくとい良いでしょう。

注: スクリプトにコピー&ペーストした変数はすべてコメントです。関数を呼び出しても実行されません。

Function Info()

' // Common fields

' VarFacility

' VarLevel

' VarInputSource

' VarPeerAddress

' VarPeerName

' VarPeerDomain

' VarCleanMessageText

' // Other fields

' VarDate

' VarTime

' VarMilliSeconds

' VarSocketPeerAddress

' VarPeerAddressHex

' VarPeerPort

' VarLocalAddress

' VarLocalPort

' VarPriority

' VarRawMessageText (Read only)

' // Custom fields

' VarCustom01 to VarCustom16

' // Inter-Script fields

' VarGlobal01 to VarGlobal16

' // Custom Stats fields

```
' VarStats01 to VarStats16

' // Control and timing fields
' ActionQuit
'   0=No skip, 1-99=skip next n actions within rule,
'   100=skip to next rule, 1000=stop processing message
'
' SecondsSinceMidnight
' SecondsSinceStartup

' // Functions and Actions
' IsValidIPAddress(IPAddress as string) as boolean
' ConvertIPtoHex(IPAddress as string) as string

' ActionPlaySound(SoundFilename as string, RepeatCount as long)
'   RepeatCount 0=until cancelled, 1-100=repeat x times
'   Soundfilename ""=system beep, "wav file name"=play wav file

' ActionSendEmail(MailTo as String, MailFrom as string, MailSubject as string, MailMessage as string)
'   Sends an e-mail message to the addresses specified in MailTo

End function
```

3.3.16.5.3 Jscriptエスケープ文字

Jscriptにはエスケープシーケンスが用意されており、直接入力できない文字を文字列として使用できます。エスケープシーケンスはバックスラッシュ(\)で始まります。バックスラッシュは次の文字が特殊文字であることをJscriptのインタープリタに知らせるエスケープ文字です。

エスケープシーケンス	説明
\b	バックスペース
\f	フォームフィード (あまり使用されません)
\n	ラインフィード (改行)
\r	キャリッジリターン。ラインフィードと組み合わせて(\r\n)出力の書式を指定します。
\t	水平タブ
\v	垂直タブ (あまり使用されません)
\'	単一引用符 (')
\"	二重引用符 (")
\\	バックスラッシュ (\)
\n	8進数の n で表されるASCII文字。*
\xhh	2桁の16進数 hh で表されるASCII文字
\uhhhh	4桁の16進数 hhhh で表されるUnicode文字

* n の範囲は 0 ~ 377 (8進数)

上記以外のエスケープシーケンスは、単にエスケープシーケンスのバックスラッシュに続く文字を表します。たとえば \a は a と解釈されます。

バックスラッシュ自体はエスケープシーケンスの開始を表しますので、スクリプトに直接文字として入力することはできません。

バックスラッシュを文字として入力するには2つ続けて(\\)入力する必要があります。

例: 'The log file path is c:\Program Files\Syslogd\SyslogCatchAll.txt'

単一引用符と二重引用符のエスケープシーケンスを使用すると、リテラル文字列で引用符を使用できます。

例: 'The caption reads, \"This is a test message from \Kiwi SyslogGen\.'\"'

3.4 Setup – Schedules (設定 – スケジュール)

ログのアーカイブを有効にするには **Schedules** オプションを右クリックし **add new schedule** をクリックします。もしくは **Schedules** オプションをクリックしツールバーの **New** ボタンをクリックします。

リストには最大100のカスタムスケジュールを登録できます。個々のスケジュールは順次実行されます。同じ時刻に複数のスケジュールが登録されている場合リストの上にあるスケジュールが先に実行されます。

スケジュール名の左のチェックボックスでいつでもスケジュールの有効/無効を切り替えることができます。

カスタムスケジュールの名前は任意です。重複していても構いませんが、内容あるいは実行時間がわかるような名前を付けてください。

3.4.1 スケジューラーの動作

Kiwi Syslog Daemon の内蔵スケジューラーを使えば指定した時刻または間隔で様々なタスクを実行したり、Kiwi Syslog Daemon 自体を起動/終了させることができます。

スケジューリングツールとして必要な機能はすべて揃えており、Kiwi Syslog Daemon 特有のタスク(ログアーカイブ、ログクリーンアップ、Kiwi Syslog Script アクション等)はもちろん Windows プロセスや外部プログラムを実行することができます。

スケジュール実行頻度は1回限りから年単位まで、分、日、週、月など見分けさえ付けばどんな間隔でも細かく設定できます。祝祭日やネットワークの停止期間など特定の日付を除外する例外スケジュールも付加することができます。

図3はアーカイブタスクのスケジュールの例です。

実行可能なタスクタイプは4つです。

- ・ Archive
- ・ Clean-up
- ・ Run Program
- ・ Run Script



図1 - Schedule の Task Type。スケジュールオプション画面の上部ドロップダウンリストで選択可能

上記タスクの実行タイミング(タスクタイプによって異なります)

- ・ スケジュールに従って実行
- ・ アプリケーション/サービスの起動時
- ・ アプリケーション/サービスの終了時



図2 - Schedule の Task Trigger。スケジュールオプション画面の上部ドロップダウンリストで選択可能

Task Type: Archive Task Trigger: On a schedule

Schedule | Source | Destination | Archive Options | Archive Notifications

Schedule Start
 Date: 08 Aug 2007 Time: 12:00 UTC Never

Schedule Frequency
 Once Minute Hour Day Week Month Year
 Run at: 00 minutes after the hour, Every: 4 hour(s) UTC

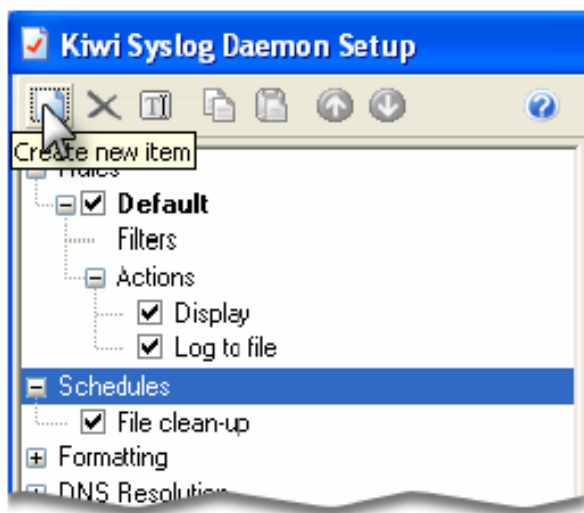
Schedule Exceptions
 Weekends
 Daily 00:00 to 23:59 UTC
 Weekly S M T W T F S
 Selected date: 13 August UTC
 All day Between 00:00 and 23:59 UTC

Schedule Finish
 Date: 19 Jul 2007 Time: 10:37 UTC Never Run Now

図3 - Archive タスクのスケジュール。土日以外の平日4時間おきに実行

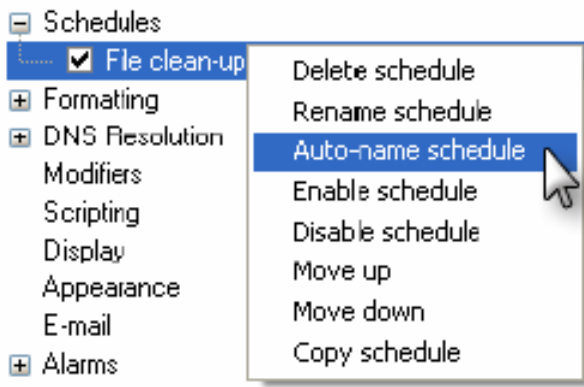
スケジュールの追加

新しいスケジュールを作成するには、Kiwi Syslog Daemonの Setup 画面の左枠に表示されるプロパティツリーから Schedule を選択しツールバーの [Create new item] ボタンをクリックします。



その他のスケジュール選択オプション

スケジュールを選択すると、コンテキストメニュー(あるいは Setup 画面の上部左側のツールバー)から様々なオプションを選択できます。



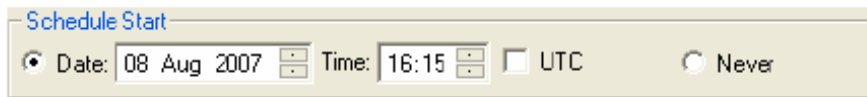
スケジュールのコンテキストメニューはスケジュールを選択し右クリックすると表示されます。

3.4.2 On a schedule (スケジュールに従って実行)

新しいスケジュールを作成したら、以下のオプションを設定します。

- ・ スケジュール化するタスクの開始日時
- ・ スケジュール化するタスクの実行頻度
- ・ スケジュール化するタスクの終了日時
- ・ スケジュール化するタスクの例外処理(必要時)

Schedule Start:



スケジュール化するタスクを起動する日時をここで設定します。未来の日付を設定しても全く問題ありませんが、設定した日付になるまでこのスケジュールは非アクティブとなります。

同様に、Never に設定するとそのタスクはずっと非アクティブな状態となります(事実上無効になります)。

スケジュールオプションを設定するとき、日付時刻はUTC(Coordinated Universal Time = 協定世界時)でも指定可能です。

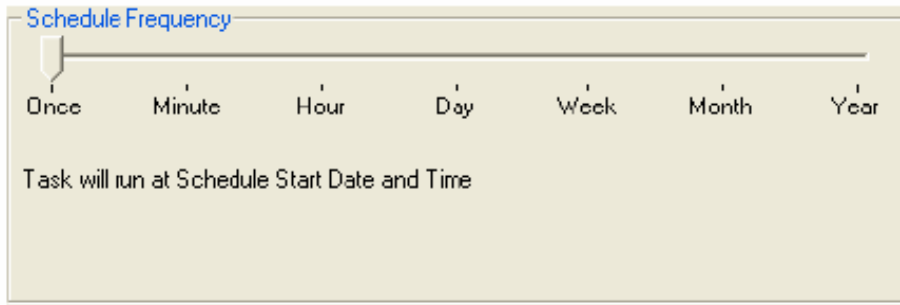
Schedule Frequency:

スケジュールの頻度として指定可能なオプションは以下の7つです。

- ・ Once
- ・ Minute
- ・ Hour
- ・ Day
- ・ Week
- ・ Month
- ・ Year

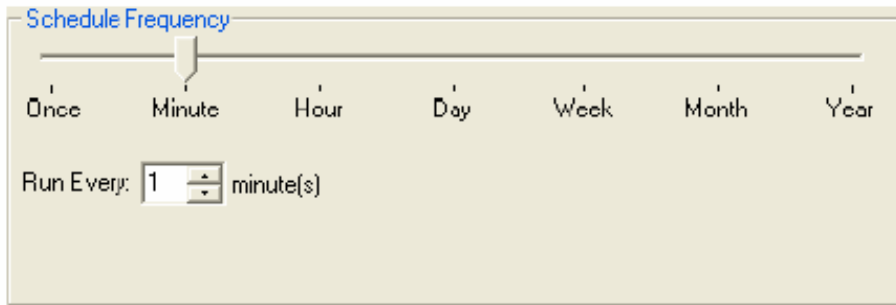
各オプションには独自の設定オプションがあります。次に、それぞれのオプションの概要について説明します。

Schedule Frequency - Once:



タスクは Schedule Start オプションで設定した日付時刻に1回のみ実行されます。

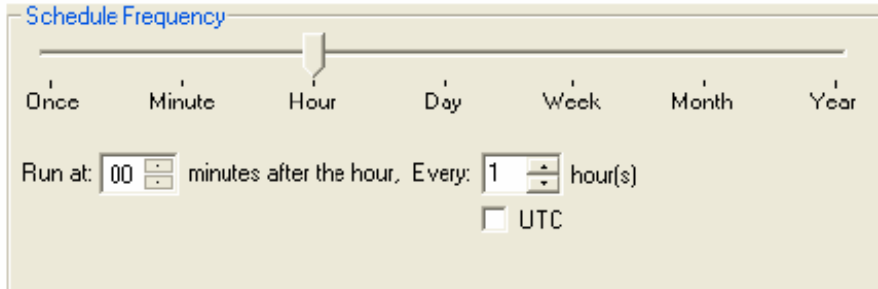
Schedule Frequency - Minute:



タスクは N 分おきに実行されます。

上図ではタスクは1分おきに実行されるよう設定されています(つまり00:00, 00:01, 00:02, 00:03, ... , 23:59にタスクが実行されます)。

Schedule Frequency - Hour:

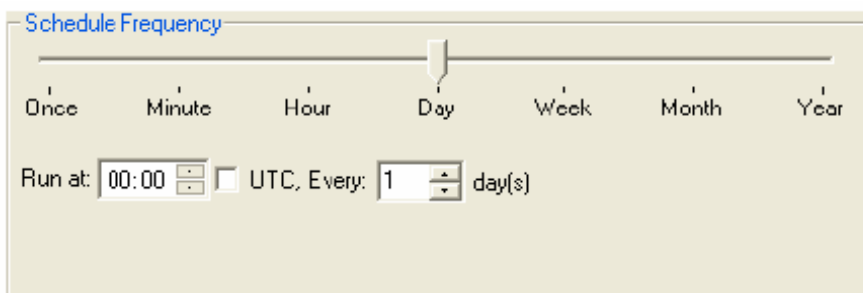


タスクは X 時間おきに正時を N 分過ぎると実行されます。

上図ではタスクは1時間おきに正時きっかりに実行されるよう設定されています(つまり00:00, 01:00, 02:00, 03:00, ... , 23:00にタスクが実行されます)。

スケジュールオプションを設定するとき、日付時刻はUTC(Coordinated Universal Time = 協定世界時)でも指定可能です。

Schedule Frequency - Day



タスクは X 日おきに HH:MM に実行されます。

上図ではタスクは毎日深夜00:00に実行されるよう設定されています(つまり2007-08-30 00:00, 2007-08-31 00:00,

2007-09-01 00:00, ...にタスクが実行されます)。

スケジュールオプションを設定するとき、日付時刻はUTC(Coordinated Universal Time = 協定世界時)でも指定可能です。

Schedule Frequency - Week:

Schedule Frequency

Once Minute Hour Day Week Month Year

Run at: 00:00 UTC

on: Sun Mon Tue Wed Thu Fri Sat

Every: 1 week(s)

タスクは X 週おきに指定した曜日の HH:MM に実行されます。

上図ではタスクは毎週毎日深夜0:00に実行されるよう設定されています(つまり日曜00:00, 月曜00:00, 火曜00:00, ...にタスクが実行されます)。

スケジュールオプションを設定するとき、日付時刻はUTC(Coordinated Universal Time = 協定世界時)でも指定可能です。

Schedule Frequency - Month

Schedule Frequency

Once Minute Hour Day Week Month Year

Run On: 1st day of the month, at: 00:00 UTC

Every: 1 month(s)

On these months: Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

タスクは指定した月の N 日の HH:MM に実行されます。実行月は次のいずれかで指定します。

- ・ N 月おき
- ・ 指定した月のみ

上図ではタスクは毎月1日の深夜に実行されるよう設定されています(つまり1月1日00:00, 2月1日00:00, 3月1日00:00 ... ,12月1日00:00にタスクが実行されます)。

スケジュールオプションを設定するとき、日付時刻はUTC(Coordinated Universal Time = 協定世界時)でも指定可能です。

Schedule Frequency - Year:

Schedule Frequency

Once Minute Hour Day Week Month Year

Run On: 18 January at: 00:00 UTC, Every: 1 year(s)

タスクは N 年おきに X 月 N 日の HH:MM に実行されます。

上図ではタスクは毎年1月18日の深夜に実行されるよう設定されています(つまり2008年1月18日00:00, 2009年1月18日00:00, 2010年1月18日00:00, ... にタスクが実行されます)。

Schedule Finish:

スケジュール化したタスクはアクティブになっているときのみ実行されます。アクティブか非アクティブかは開始日と終了日の指定によって変わります。

スケジュール終了日時を基準にすると、スケジュール化したタスクは指定した終了日まで実行されます。
Never に設定すると、スケジュールは永久にアクティブとなります。

Schedule Exceptions:

スケジュールの例外指定の方法は3種類あります。

Daily :

毎日指定した時間帯が除外されます。

スケジュールオプションを設定するとき、日付時刻はUTC(Coordinated Universal Time = 協定世界時)でも指定可能です。

例: 下図は毎日 00:00 ~ 23:59 の間(つまり全日)除外する例外指定を表しています。

スケジュール化したタスクは指定した時間帯の間実行されません。

The screenshot shows the 'Schedule Exceptions' dialog box. The 'Daily' radio button is selected. The time range is set to 00:00 to 23:59, and the 'UTC' checkbox is checked. The 'Weekly' and 'Selected date' options are unselected.

Weekly :

1つ以上の指定した曜日が除外されます。

例: 下図は毎週土曜日と日曜日を除外する例外指定を表しています。

スケジュール化したタスクは指定した曜日には実行されません。

The screenshot shows the 'Schedule Exceptions' dialog box. The 'Weekly' radio button is selected. The days of the week are set to S (Sunday) and S (Saturday), and the 'UTC' checkbox is checked. The 'Daily' and 'Selected date' options are unselected.

Selected Date :

指定した日付の全日または指定時間帯が除外されます。

スケジュールオプションを設定するとき、日付時刻はUTC(Coordinated Universal Time = 協定世界時)でも指定可能です。

例: 下図は8月13日の00:00 ~ 23:59 の間を除外する例外指定を表しています。

スケジュール化したタスクは8月13日の指定時間帯には実行されません。

The screenshot shows the 'Schedule Exceptions' dialog box. The 'Selected date' radio button is selected. The date is set to 13 August, and the time range is set to 00:00 to 23:59. The 'UTC' checkbox is checked. The 'Daily' and 'Weekly' options are unselected.

3.4.3 On application/service startup (アプリケーション/サービスの起動時に実行)

選択したタイプのタスクはKiwi Syslog Daemonを起動するとすぐに実行されます。

この実行オプションをサポートしているタスクタイプは次の4つです。

- ・ Archive
- ・ Clean-up
- ・ Run-Program
- ・ Run-Script

3.4.4 On application/service shutdown (アプリケーション/サービスの終了時に実行)

選択したタイプのタスクはKiwi Syslog Daemonの終了プロセスの一部として実行されます。

この実行オプションをサポートしているタスクタイプは次のとおりです。

- ・ Run-Script

3.4.5 Archive (アーカイブ) タスク

アーカイブタスクはv.8.3.0以前のKiwi Syslog Daemon の旧アーカイブ機能を強化/拡張したものです。あるフォルダに保存されているログを別のフォルダにコピーまたは移動させ、ファイルを個別にあるいはまとめて1つのアーカイブに圧縮することができます。アーカイブの暗号化、複数ファイルへの分割、ファイル/アーカイブハッシュの作成、外部プログラムの実行などが可能です。アーカイブタスクの完了時にEメールで通知したり、Webベースのレポートをディスク上に作成することもできます。


アーカイブタスクは任意の間隔/日付、あるいはアプリケーション/サービスの起動時に実行されるようスケジュール化することが可能です。

スケジュール化されているか否かに関わらず、アーカイブタスクは次の4つの部分で構成されています。

- ・ Source
- ・ Destination
- ・ Archive Options
- ・ Archive Notification

Source:

Source Location:



移動/コピーするファイルが保存されているルートフォルダを指定します。Include sub-folders オプションをチェックすると、指定したルートフォルダの下にあるすべてのサブフォルダがファイル処理の対象になります。チェックしない場合、指定したルートフォルダの直下にあるファイルのみが処理対象となります。

Source Files:

Source Files

File Mask: *.txt

File Size: Any Size

At Least 500 MB (Megabytes)

At Most 1 KB (Kiobytes)

Between 1 and 500 KB (Kilobytes)

File Age: Any Age

At Least 6 Month(s) old

At Most 24 Month(s) old

Between 6 and 24 Month(s) old

タスク処理の対象にするファイルについて定義します。
 ファイルマスク、サイズ、経過時間の指定条件に一致したファイルのみが処理対象となり、一致しないものは除外されます。
 例: 上図では500MB以上で6ヶ月以上経過している*.txtファイルが処理されます。

Destination:

Destination Location:

Destination Location

C:\Program Files\Syslogd\Dated Logs

Create sub-folders (preserve source directory structure)

ファイル条件に一致したファイルを移動/コピーするフォルダを指定します。Create sub-folders (preserve source directory structure) オプションをチェックすると、元ファイルが保存されている場所のディレクトリ構造がコピーされます。チェックしない場合、ファイルパスは「平準化」され、元ファイルがある場所のディレクトリ構造は無視されます。

Destination files

Move files from source to destination Copy files from source to destination

Use a dated folder name YYYY-MM-DD 2008-01-29

Use dated file names YYYY-MM-DD 2008-01-29

Insert the formatted date before the beginning of file name

Insert the formatted date before the end of file name

Adjust file/folder date(s) to that of the previous Day(s)

元の場所から移動/コピー先へファイルを転送させるときの方法等を指定します。

Move/Copy files from source to destination:

Copy Files from Source to Destination を選択すると、元ファイルはそのまま元のフォルダに残されます。Move Files from Source to Destination を選択すると、移動先フォルダにファイルがコピーされると元ファイルは元の場所から削除されます。

元のフォルダから移動/コピー先フォルダにファイルを移動/コピーするときにオプションで日付スタンプを追加することができます。

Use dated file name:

チェックすると日付スタンプが(指定フォーマットで)移動/コピーされるファイルのファイル名に追加されます。指定のフォルダに移動/コピー後のファイル名に所定のフォーマットの日付スタンプが次のいずれかの方法で挿入されます。

- ・ ファイル名の先頭。すなわち、日付スタンプ-ファイル名.log
- ・ ファイル名の末尾。すなわち、ファイル名-日付スタンプ.log

Use a dated folder names:

チェックすると、日付スタンプが条件に一致するすべてのファイルが移動/コピーされるルートフォルダの名前に追加されます。

Adjust file/folder date(s) to that of the previous ... :

日付スタンプのオプションを設定すると、移動/コピー後のファイル/フォルダの日付を前の日、週、月、年のいずれかに合わせるすることができます。

この設定を利用すれば、スケジュール化したアーカイブタスクが新しい期間の初めに実行されアーカイブ後のログにその前の期間の情報が記録されるようになるため、ログ管理の利便性を高めることができます。

例えば、アーカイブタスクが毎日深夜に実行されるようスケジュール化したとします。このオプションを指定することによって日付が調整され移動/コピー後のファイル名には前日の日付が追加されます。アーカイブ後のログには前日からのデータが記録されます。

Archive Options:

Zip Options:

Zip options

Zip files after moving/copying

Compression level: Medium

Compression method: Deflate

All files into a single zip

Multipart zip (.zip, .z01, .z02, .z03, etc.)

Split size: 0 KB (Kilobytes)

Encrypt zip file

Password:

Encryption type: Compatible

Encryption strength: 192 bit

Preserve Paths in Zip file(s)

Zip files after moving/copying:

チェックすると移動/コピー後のファイルの含まれたzipファイルが作成されます。

Compression Level:

None

圧縮されません。zipファイル内のファイルは生データです。

Low

最小限の圧縮を行います。データ圧縮時間が最短で済みます。Deflate圧縮方式の場合、Medium に比べて圧縮時間は著しく短縮されますが圧縮後のファイルサイズは1%~15%程度大きくなります。

Medium

通常の圧縮を行います。データ圧縮にかかる時間と圧縮率が最もバランスの取れたオプションです(圧縮方式がDeflateであってもBurrowsWheeler (BWT)であっても同じです)。

High

最大限の圧縮を行います。圧縮アルゴリズムが生成しうる最大の圧縮率でファイルを圧縮します。Deflate圧縮方式の場合、Mediumに比べて圧縮後のファイルサイズが大して変わらないにも関わらず圧縮にかかる時間は非常に長くなります。圧縮後のファイルサイズをできる限り小さくしたい場合で圧縮時間はさほど重要でないときに限り、このオプションを使用するようにしてください。

Compression Method:

Stored

圧縮/解凍は全く行われません。

Deflate

Deflate圧縮方式で圧縮されます。このアルゴリズムは圧縮/解凍速度が速くちょうど良い圧縮率で結果を得ることができます。

Deflate 64

Deflate64™圧縮方式で圧縮されます。Deflateよりも時間はかかりますが、圧縮率は良くなります。

BurrowsWheeler

BWT圧縮方式で圧縮されます。このアルゴリズムはデータベース、画像、テキスト、実行ファイル等多くの標準的なファイルタイプに対応しており優れた圧縮率で結果を得ることができます。標準的なDeflateアルゴリズムと比較すると圧縮/解凍に要する時間は長くなります。

All files into a single Zip:

チェックすると移動/コピー先のフォルダにあるすべてのファイルが1つのzipファイルにまとめてアーカイブされます。チェックしないと移動/コピー先フォルダにあるファイルごとにzipファイルが作成されます。

Multi-part Zip (.zip, .z01, .z02, .z03, etc.) / Split size:

これは複数のファイルに分割されたzipファイルを作成するオプションです。すべてのファイルは同じフォルダ内に作成されます。通常、分割されたファイルは同じファイル名がつけられますがそれぞれ拡張子が異なります。このオプションをチェックした場合、Split size に指定したサイズで分割された複数のファイルが作成されます。

Encrypt Zip file:

チェックすると作成されるすべてのzipファイルが暗号化されます。パスワード、暗号化タイプ、暗号化の強度も指定します。

Encryption password:

ファイルの暗号化/複合化するとき使用するパスワードを指定します。大文字小文字が区別されます。指定したパスワードはzipされたすべてのファイルに適用されます。このオプションが空白 - すなわちパスワードを指定しない場合、zipされたファイルは暗号化されません。パスワードは79文字まで使用できます。

Encryption Type:

Compatible

通常のzip暗号 (弱)

WinZip AES

WinZip 9.0 の AES 暗号 (強)

Encryption Strength:

暗号化の強度を指定します(ビット単位)。暗号タイプが Compatible の場合には適用されません。

Preserve Paths in Zip file(s):

作成されるzipファイルに移動/コピー後のファイルのパス情報を含めるかどうかを指定します。

Archive Options:

Run External Program:

Run External Program

Run program after each file is moved/copied [Variable options](#)

File: ... Command-line:

Wait for program completion

Maximum time to wait: seconds

Run program after all files are moved/copied [Variable options](#)

File: ... Command-line:

Wait for program completion

Maximum time to wait: seconds

Run program after each file is moved/copied:

選択したWindowsプログラムがファイルの移動/コピーが行われる度に実行されます。
指定したコマンドラインパラメータが選択したプログラムに渡されます。

Wait for program completion:

プログラムの終了待ち時間を指定します。指定した時間が経過すると、その時点でまだ実行中のプログラムや処理は終了されます。

Run program after all files are moved/copied:

選択したWindowsプログラムがすべてのファイルの移動/コピーが終わった後に実行されます。
指定したコマンドラインパラメータが選択したプログラムに渡されます。

Wait for program completion:

プログラムの終了待ち時間を指定します。指定した時間が経過すると、その時点でまだ実行中のプログラムや処理は終了されます。

Archive Notification:

E-mail notification

HTML format Plain text format

Send report by e-mail

Recipient(s):

Include file hashes in report

Generate hash before zip

Generate hash after zip

Hashing method:

Send report to disk [Variable options](#)

...

Use absolute paths in report (don't use relative paths)

Eメールの形式：

アーカイブレポートはHTML形式かテキスト形式のどちらかで作成され、送信されます。

Send Report by e-mail:

チェックするとアーカイブレポートがEメールで送信されます。送信先のアドレスは Recipient(s) フィールドで指定します。

Recipient(s):

アーカイブレポートを複数のアドレスに送信するときは各アドレスをコンマまたはセミコロンで区切って指定します。

Include file hashes in report:

チェックするとファイルハッシュ値がファイル処理の度に生成されます。

Generate Hash before zip:

元のファイルからzip前にハッシュ値が生成されます。ハッシュ値は作成されるレポートに記載されます。

Generate Hash after zip:

アーカイブ処理の途中で作成されたすべてのzipファイルからハッシュ値が生成されます。ハッシュ値は作成されるレポートに記載されます。

Hashing Method:

ファイルから生成されるハッシュのタイプを指定します。

MD5

MD5 (Message Digest Algorithm 5)は安全なハッシュアルゴリズムで1991年に RSA Data Security, Inc の R. Rivest によって開発されました。このアルゴリズムは任意の長さのメッセージから128ビット長のメッセージダイジェストを生成します。MD5 は使用されることの多いハッシュアルゴリズムであり安全性も確保されているとされています。しかし、一部には潜在的な弱点があることも報告されています。また、指定したハッシュ値と一致するプレーンテキストを数週間内に検索するような特殊目的のマシンをビルドすることも可能であることが報告されています。

SHA1

SHA-1 (Secure Hash Algorithm 1)はアメリカ国立標準技術研究所(NIST)によっていくつかの米国連邦政府の適用業務向けに提案されました。このアルゴリズムは任意の長さのメッセージから160ビット長のメッセージダイジェストを生成します。128ビットのハッシュ関数に比べSHA-1が生成する160ビットのハッシュ値は総当たり攻撃に対する耐性が高められており、MD5よりも安全とされています。

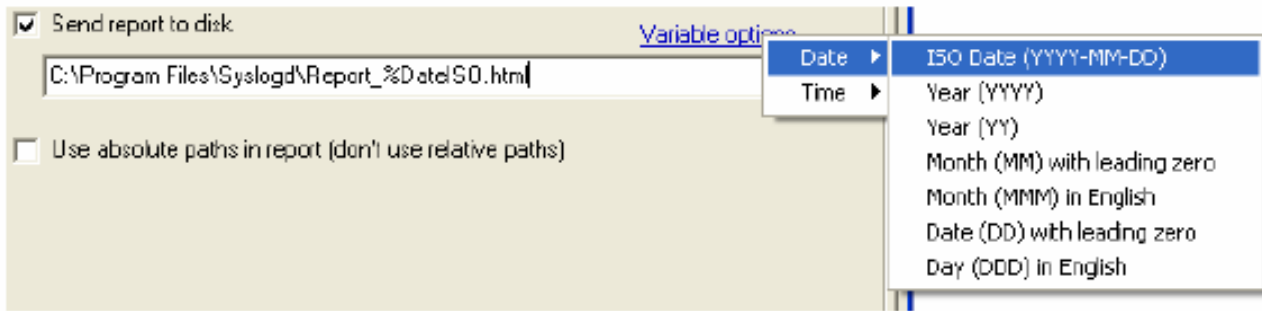
SHA256

SHA256 (または SHA-2 = Secure Hash Algorithm 2 (256)) はアメリカ国立標準技術研究所(NIST)によっていくつかの米国連邦政府の適用業務向けに提案されました。このアルゴリズムは任意の長さのメッセージから256ビット長のメッセージダイジェストを生成します。SHA-2(256)アルゴリズムによって生成される出力は新暗号規格(AES)に見合うセキュリティが実現されています。

Send Report to disk:

チェックするとアーカイブレポートのファイルが指定したパスとファイル名でディスクに保存されます。

Variable options:



選択した変数がファイルパスに挿入されます。変数を利用すれば日付や時刻スタンプ付きのレポートファイルが作成されるため、アーカイブタスクが実行されるたびに同じレポートファイルが上書きされる心配がありません。

Use absolute paths in report (don't use relative paths):

チェックすると作成されるレポート(ディスク上でもEメールでも)にはデフォルトの相対パスではなくフルパスが表示されます。

3.4.6 Clean-up (クリーンアップ) タスク

指定条件に一致したファイルを元の場所から削除します。

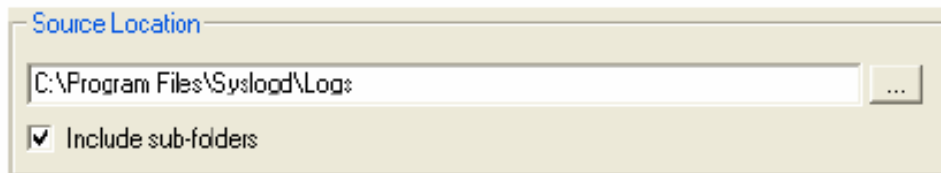
クリーンアップタスクは任意の間隔/日付、あるいはアプリケーション/サービスの起動時に実行されるようスケジュール化することが可能です。

スケジュール化されているか否かに関わらず、クリーンアップタスクは次の3つの部分で構成されています。

- ・ Source
- ・ Clean-up Options
- ・ Clean-up Notification

Source:

Source Location:



削除するファイルが保存されているルートフォルダを指定します。Include sub-folders オプションをチェックすると、指定したルートフォルダの下にあるすべてのサブフォルダがファイル処理の対象になります。チェックしない場合、指定したルートフォルダの直下にあるファイルのみが処理対象となります。

Source Files:

Source Files

File Mask: *.txt

File Size: Any Size
 At Least 500 MB (Megabytes)
 At Most 1 KB (Kilobytes)
 Between 1 and 500 KB (Kilobytes)

File Age: Any Age
 At Least 6 Month(s) old
 At Most 24 Month(s) old
 Between 6 and 24 Month(s) old

タスク処理の対象にするファイルについて定義します。ファイルマスク、サイズ、経過時間の指定条件に一致したファイルのみが処理対象となり、一致しないものは除外されます。例: 上図では500MB以上で6ヶ月以上経過している*.txtファイルが処理されます。

Clean-up Options:

Remove empty folders:

チェックすると空になったフォルダも元の場所から削除します。

Clean-up Notification:

Clean-up notification

HTML format Plain text format

Send clean-up notification report by e-mail
 Recipient(s): joe@company.com; jane@company.com

Send clean-up notification report to disk [Variable options](#)
 C:\code\Syslog\8\CleanUpReport_%Date%.html

Use absolute paths in report (don't use relative paths)

Eメールの形式

クリーンアップレポートはHTML形式かテキスト形式のどちらかで作成され、送信されます。

Send Clean-up Notification Report by e-mail:

チェックするとクリーンアップレポートがEメールで送信されます。送信先のアドレスは Recipient(s) フィールドで指定します。

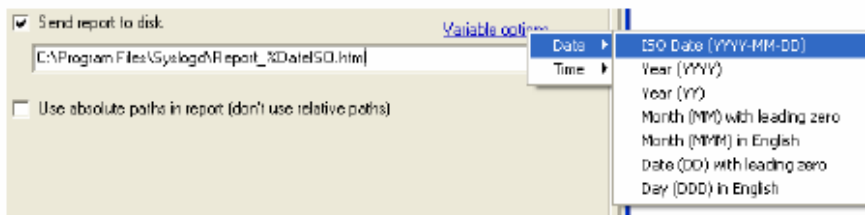
Recipient(s):

クリーンアップレポートを複数のアドレスに送信するときは各アドレスをコンマまたはセミコロンで区切って指定します。

Send Clean-up Notification Report to disk:

チェックするとクリーンアップレポートのファイルが指定したパスとファイル名でディスクに保存されます。

Variable options:



選択した変数がファイルパスに挿入されます。変数を利用すれば日付や時刻スタンプ付きのレポートファイルが作成されるため、クリーンアップタスクが実行されるたびに同じレポートファイルが上書きされる心配がありません。

Use absolute paths in report (don't use relative paths):

チェックすると作成されるレポート(ディスク上でもEメールでも)にはデフォルトの相対パスではなくフルパスが表示されます。

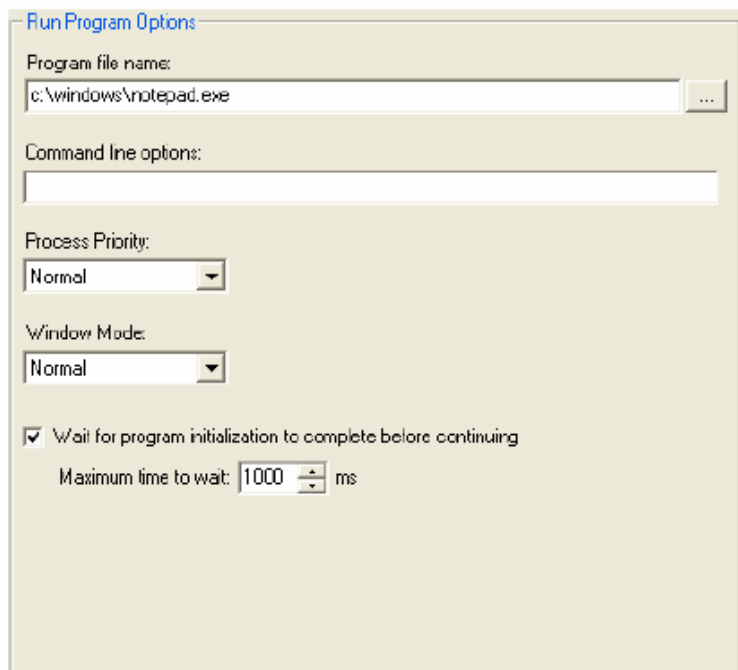
3.4.7 Run Program (プログラム実行) タスク

Windowsプログラム、プロセス、バッチファイルなどを実行します。Run Program (プログラム実行)タスクは任意の間隔/日付、あるいはアプリケーション/サービスの起動時に実行されるようスケジュール化することが可能です。

スケジュール化されているか否かに関わらず、Run Program (プログラム実行)タスクは次の2つの部分で構成されています。

- ・ Run Program Options
- ・ Run Program Notification

Run Program Options:



Program file name:

Windowsによって実行されるプログラムまたはプロセスを指定します。

Command line options:

実行ファイルに渡すコマンドラインパラメータを指定します。

Process Priority:

作成される新しいWindowsプロセスのプライオリティを設定します。

選択可能な値:

- ・ Low
- ・ Below_Normal
- ・ Normal (デフォルト)
- ・ Above_Normal
- ・ High
- ・ Realtime (注: この値に設定するとシステムがロックアップする可能性があります)

AboveNormal

Normal以上High以下のプライオリティのプロセスに対して指定します。

BelowNormal

Idle以上Normal以下のプライオリティのプロセスに対して指定します。

High

直ぐに実行する必要がある緊急度の高いタスクを実行するプロセスに対して指定します。Normal や Idle のプロセススレッドよりも先に処理されます。例えば、Task List などOSにかかる負荷を無視してでもユーザーに呼び出されたらすぐに応答する必要のあるプロセスに対して設定します。この値を適用すると、使用可能なほぼすべてのCPU時間が消費されるため使用するときは特に注意が必要です。

Low

システムがアイドルのときのみ実行されるスレッドのプロセスに対して指定します。この値の設定されたプロセススレッドはLow以上のプライオリティクラスが設定されているプロセスの実行後に実行されます。スクリーンセーバーなどが該当します。プライオリティクラスがIdleのプロセスは子プロセスに引き継がれます。

Normal

特にスケジュールする必要のないプロセスに対して指定します。

RealTime

最優先のプロセスに対して指定します。この値の設定されたプロセススレッドは他のすべてのプロセスよりも先に実行されます。重要なタスクを実行するOSのプロセスなどがこれに該当します。例えば、非常に短い間隔でアルタイムプロセスが繰り返し実行されるとディスクキャッシュがクリアされなくなったりマウスが応答しなくなることがあります。

Window Mode:

プロセスがユーザーインターフェイスを有するときに Window Mode にします。ユーザーインターフェイスの無いプロセスには無効です。

選択可能な値:

- ・ Hide
- ・ Normal
- ・ Minimized
- ・ Maximized

Wait for program initialization to complete before continuing

チェックすると、Syslogは新たなプロセスが初期化されるまで待ちます。すなわち新たなプロセスがアイドルになるまで待ちます。この設定は後にプロセスと相互連携するためプロセスが開始したことを確認するのに有効です。

Run Program Notification:

The screenshot shows a dialog box titled "Run Program Notification". At the top, there are two radio buttons: "HTML format" (selected) and "Plain text format". Below this, there are two checked checkboxes: "Send Run-Program Notification Report by e-mail" and "Send Run-Program Notification Report to disk". The "e-mail" checkbox has a text input field with "joe@company.com" entered. The "to disk" checkbox has a text input field with "C:\Program Files\Syslogd\RunProgramReport.html" entered and a "Variable options" link to its right. A "..." button is visible at the end of the disk path input field.

Eメールの形式:

Run ProgramレポートはHTML形式かテキスト形式のどちらかで作成され、送信されます。

Send Run Program Notification Report by e-mail:

チェックするとRun ProgramレポートがEメールで送信されます。送信先のアドレスは Recipient(s) フィールドで指定します。

Recipient(s):

Run Programレポートを複数のアドレスに送信するときは各アドレスをコンマまたはセミコロンで区切って指定します。

Send Run Program Notification Report to disk:

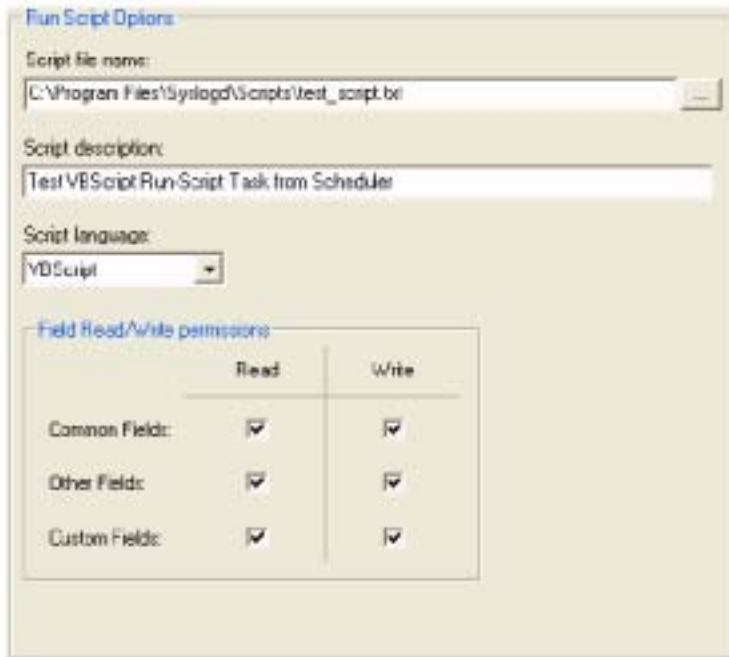
チェックするとRun Programレポートのファイルが指定したパスとファイル名でディスクに保存されます。

3.4.8 Run Script (スクリプト実行) タスク

Kiwi Syslog Daemonの Run-Script を実行します。Run Script (スクリプト実行)タスクは任意の間隔/日付、あるいはアプリケーション/サービスの起動時/終了時に実行されるようスケジュール化することが可能です。スケジュール化されているか否かに関わらず、Run Script (スクリプト実行)タスクは次の2つの部分で構成されています。

- ・ Run Script Options
- ・ Run Script Notification

Run Script Options:



Script file name

スクリプトファイルはスクリプトコマンドが書かれた標準テキストファイルです。ファイルの拡張子は任意ですがデフォルトはメモ帳で編集しやすいよう .txt になっています。

Script description

任意の説明文を入力できます。スクリプトの機能を簡単に説明してください。

Script Language

Windows Script では Visual Basic® Scripting Edition と Microsoft Jscript® 2つのスクリプトエンジンがサポートされています。

VBScript - MS Word と Excel で使われる Visual Basic や VBA (Visual Basic for Applications)の一種です。学習しやすい上に豊富な機能セットがあります。

Jscript - Webで使われるJavaスクリプトの一種です。Javaスクリプトに精通している場合はこれを選択してください。

どちらの言語も機能面でも処理速度の面でも同等です。どちらを選択しても構いません。お好みで選んでください。Kiwi社でのテストでは、スクリプトが主に文字列操作である場合ほとんどのケースでJscriptの方が処理速度が速かったという結果が出ました。

VBScript に関しては以下のWebページを参照してください。

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/vtoriVBScript.asp>

J Script に関しては以下のWebページを参照してください。

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/js56jsoriJScript.asp>

他に Perl, Python, Ruby などのスクリプト言語も選択できます。

ただし、これらを選択した場合には対応するスクリプティングエンジンをインストールする必要があります。

PerlScript については次のWebページを参照してください。

<http://www.activestate.com/Products/ActivePerl>

Python については次のWebページを参照してください。

<http://www.activestate.com/Products/ActivePython>

ActiveScriptRuby については次のWebページを参照してください。

<http://arton.hp.infoseek.co.jp/index.html>

Field Read/Write permissions

セキュリティと速度を確保するという理由で、メッセージおよびスクリプト変数に対するアクセスを制限することができます。スクリプトが実行されるたびに、メッセージフィールドがスクリプト変数にコピーされ、スクリプトが完了すると元に戻されます。コピーは時間とCPUサイクルを消費しますので、Read/Writeアクセスを使用したい変数のみに制限すると、実行速度が上がります。

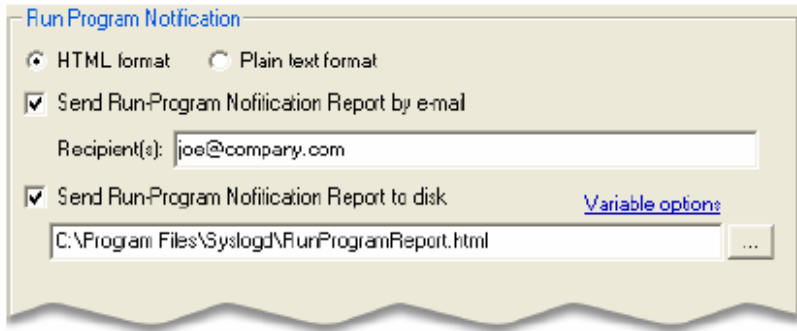
フィールドグループの Read アクセスを有効にすると、値がスクリプト変数にコピーされますのでスクリプト内で読むことができます。

フィールドグループの Write アクセスを有効にすると、値がスクリプト変数からコピーされ対応するプログラムフィールドがその値で置換されます。

フィールドはスクリプト中で使用方法が似ているもの同士をグループ化できます。

フィールドの詳細については[関連項目](#)を参照してください。

Run Script Notification:



E-mail format:

Run ScriptレポートはHTML形式かテキスト形式のどちらかで作成され、送信されます。

Send Run Script Notification Report by e-mail:

チェックするとRun ScriptレポートがEメールで送信されます。送信先のアドレスは Recipient(s) フィールドで指定します。

Recipient(s):

Run Scriptレポートを複数のアドレスに送信するときは各アドレスをコンマまたはセミコロンで区切って指定します。

Send Run Script Notification Report to disk:

チェックするとRun Scriptレポートのファイルが指定したパスとファイル名でディスクに保存されます。

3.4.9 Schedule Report (スケジュールレポート)

HTML形式レポートの例:

Kiwi Syslog Daemon - Scheduled Archive Task Report - New Schedule

Archive Task, performed: Tuesday, 28 August 2007 at 10:10:32

Source location: C:\PROGRAM FILES\SYSLOGD\Logs\

Destination location: C:\PROGRAM FILES\SYSLOGD\Dated Logs\

Source file	Copied/Moved to	File size (bytes)	Date created	Hash (SHA-256)
SyslogCatchAll.txt	SyslogCatchAll(2).txt	1,350	28/08/07 10:10:29	33E585044A17C9811E4ED71589686LCEE400005C491FC3D30C798039EF203257

テキスト形式レポートの例:

Kiwi Syslog Daemon - Scheduled Archive Task Report - Archive on a schedule

Archive Task, performed: Friday, 24 August 2007 at 16:10:01

Source location: C:\Program Files\Syslogd\Logs\

Destination location: C:\Program Files\Syslogd\Dated logs\

File 1:

Source file: SyslogCatchAll.txt

Copied/Moved to: 2007-08-24\SyslogCatchAll2007-08-24(2).txt

File size (bytes): 259,509,414

Date created: 24/

3.5 Setup – Formatting (設定 – フォーマット)

3.5.1 Custom file formats (カスタムファイルフォーマット)

データを標準フォーマットと異なるフォーマットで記録するには、このオプションで独自のファイル記録フォーマットをフィールドから作成します。

新しいカスタムフォーマットを作成する

新しいカスタムフォーマットを作成するには Custom file formats オプションを右クリックし add new custom file format を選択します。もしくは Custom file formats オプションをクリックしツールバーの New ボタンをクリックします。

カスタムファイルフォーマットを作成すると、Log to File アクションの Log File Format ドロップダウンリストから選択できるようになります。カスタムファイルフォーマットはリストの一番下に表示されます。

フィールド順を変更する

ファイルに書き込むフィールドの順序を変更するにはフィールドチェックボックスをドラッグします。マウスをチェックボックス上に置くと、マウスカーソルがドラッグアンドドロップカーソルに変わります。任意の項目をクリックし、変更したい位置までドラッグアンドドロップすることで順序を変更することができます。表示された順序でログファイルエントリーが作成されます。

フィールドを有効にする

使用可能なフィールドは Log file fields に表示されています。ログファイルに書き込みたいフィールドのみチェックしてください。

日付と時刻のフォーマット

Date、Time および Date-Time フィールドのフォーマットは画面右側のドロップダウンリストで選択できます。ご使用の環境に応じて最適なフォーマットを選択するようにしてください。

Field delimiter

通常、各フィールドは重複しない特定の文字で区切ります。タブはsyslogファイルでもっとも一般的に使用されている区切り文字です。

Qualifier

各フィールドを引用符もしくは二重引用符等で括ることができます。これは区切り文字としてカンマ(,)を使うように設定したときに特に効果的です。

Adjust time to UTC (-9hrs)

ログファイルの日付時刻スタンプをUTC(GMT)時間に合わせたい場合にチェックします。UTCとの時差(1時間単位)が括弧内に表示されています。

カスタムフィールド

カスタムフィールドは Run Script アクションで使います。構文解析スクリプトを作成すると、syslog メッセージテキストをいくつかのサブフィールドに分離できます。値は16個のカスタムフィールドに割り当てられファイルに記録されます。syslogメッセージはデバイスメーカーごとに異なるフォーマットで生成されますので、メッセージテキストを別々のフィールドに分離する汎用の構文解析プログラム(パーサー)を作成することはできません。メッセージテキストを解析し、カスタムデータベースフィールドに挿入するカスタムスクリプトを作成しなければなりません。Scripts サブフォルダに構文解析スクリプトのサンプルがありますので参考にしてください。Custom fieldチェックボックスをチェックすると16個すべてのフィールドがログファイルに記録されます。各カスタムフィールドは選択した区切り文字で分離されます。

フィールドと値の例

Field name	Example
Date	28/01/2005
Time	16:12:54
Date-Time	28/01/2005 16:12:54
Milliseconds	123
TimeZone	-13 hrs
Facility	Local7
Level	Debug
Priority	Local7.Debug
HostAddress	192.168.0.1
Hostname	host.company.com

```

InputSource      UDP
Message Text    This is a test message from Kiwi Syslog Daemon
Custom          Custom01 Custom02 Custom03 etc

```

3.5.2 Custom DB formats (カスタムDBフォーマット)

新しいカスタムフォーマットを作成する

新しいカスタムフォーマットを作成するには Custom DB formats オプションを右クリックし add new custom DB format を選択します。もしくは Custom DB formats オプションをクリックしツールバーの New ボタンをクリックします。最初にデータベースタイプ Access database が表示されますので、Type ドロップダウンリストから使用したいデータベースタイプを選びます。使用したいものがないときは Unknown format を選び、希望するデータベースタイプに合うようフィールドを変更します。

フィールド順を変更する

データベースに作成されたフィールドの順序を変更するには Function セルを他のセルの上または下にドラッグアンドドロップします。マウスを灰色の Function セルの上に置くと、マウスカーソルがドラッグアンドドロップカーソルに変わります。任意の項目をクリックし、変更したい位置までドラッグアンドドロップすることで順序を変更することができます。表示された順序でデータベーステーブルが作成されテーブルにデータが挿入されます。

フィールド Function

一番左側の列にデータベースの Function フィールドが表示されています。次の列はフィールドの有効/無効を切り替えるチェックボックスです。チェックされていないフィールドは、データベースの INSERT 文から除外される、あるいはデータベーステーブルの作成時に使用されません。

フィールド名

Field name 列は編集可能です。適切な名前を付けてください。デフォルトフィールド名はすべてのデータベースに対して問題を起こさないことが確認されています。例えば日付フィールドの名前をDATEに変更すると、一部のデータベースタイプでエラーを引き起こす可能性があります。そのようなデータベースタイプでは DATE が予約語であるためです。フィールド名の先頭に MSG を追加すれば予約語との衝突を避けることができます。

フィールドサイズ

データベースの作成にあたり、フィールドに最大のデータが入るようにサイズを指定することが重要です。いくつかのフィールドではフィールドタイプでサイズが決まりますので指定する必要がありません。たとえば Time は常に8バイトとみなされます。サイズはプログラムでログをデータベースに書く時にも必要となります。データは INSERT 文で渡されますので、指定されたフィールドサイズに切り詰められます。フィールドに大きすぎるデータが入ることによるエラーを避けるためです。例えば、メッセージテキストフィールドに255バイトを指定しているときに300バイトのメッセージを受信したとします。データは255バイトに切り詰められてからログファイルに記録されます。

フィールドタイプ

フィールドタイプはログデータのタイプに一致しなければなりません。正しいデータタイプが不明な時は、VarChar を選択しておけば大抵の場合大丈夫です。データタイプを編集するときは各セルのドロップダウンリストに候補が表示されますので選択してください。リストから選ぶ代わりに、セルに直接入力することもできます。リストのデータタイプは選択したデータベースタイプに応じて変わります。例えば Access で Text となるフィールドのデータタイプは SQL では VarChar となります。

カスタムフィールド

カスタムフィールドは Run Script アクションで使います。構文解析スクリプトを作成すると、syslog メッセージテキストをいくつかのサブフィールドに分離できます。値は16個のカスタムフィールドに割り当てられデータベースに記録されます。syslog メッセージはデバイスメーカーごとに異なるフォーマットで生成されますので、メッセージテキストを別々のフィールドに分離する汎用の構文解析プログラム(パーサー)を作成することはできません。メッセージテキストを解析し、カスタムデータベースフィールドに挿入するカスタムスクリプトを作成しなければなりません。Scripts サブフォルダに構文解析スクリプトのサンプルがありますので参考にしてください。

記録されたデータフォーマットの例

Field name	Type	Size	Data
MsgUnique	adInteger	4	1
MsgDate	adDBTimeStamp	16	28/01/2005
MsgTime	adDBTimeStamp	16	16:12:54
MsgDateTime	adDBTimeStamp	16	28/01/2005 16:12:54
MsgUTCDate	adDBTimeStamp	16	28/01/2005
MsgUTCtime	adDBTimeStamp	16	04:12:54
MsgUTCDateTime	adDBTimeStamp	16	28/01/2005 04:12:54
MsgTimeMS	adInteger	4	0
MsgPriorityNum	adInteger	4	191
MsgFacilityNum	adInteger	4	23
MsgLevelNum	adInteger	4	7
MsgPriority	adVarChar	30	Local7.Debug

MsgFacility	adVarWChar	15	Local7
MsgLevel	adVarWChar	15	Debug
MsgHostAddress	adVarWChar	15	192.168.0.1
MsgHostname	adVarWChar	255	host.company.com
MsgInputSource	adVarWChar	10	UDP
MsgText	adLongVarWChar	1024	This is a test message from Kiwi Syslog Daemon

フィールドフォーマット

データフォーマットをデータフィールドごとに指定できます。ほとんどのフィールドで指定不要です。日付フィールドでは多くのフォーマットがサポートされており、データベースに書き込まれるときに独自の内部フォーマットに変換されます。クエリー時にはログが記録されたときとは異なるフォーマットで表示されることがあります。

HostAddress フィールドのフォーマット形式によってアドレスは0埋めされるため、表示されると先頭に0が現れます。これによりアドレスは常に15バイト長となり、IPアドレスでソートしやすくなります。

Format セルをブランクにすると、データは変更されず、受信したとおり追加されます。

Show SQL commands ボタン

このボタンを押すとテーブルを作成し、データを挿入するために使われるコマンドリストが表示されます。これらのコマンドを使って、使用しているデータベースアプリケーション内に独自のテーブルを作成できます。コマンドを送信する時のデフォルトのテーブル名は Syslogd です。

SQL コマンド例:

```
Database type: MySQL database
Database name: New Format
SQL command to create the table:
CREATE TABLE Syslogd (MsgDate DATE,MsgTime TIME,MsgPriority VARCHAR(30),MsgHostname
VARCHAR(255),MsgText TEXT)
SQL INSERT command example:
INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText) VALUES ('2005-01-
28','16:22:44','Local7.Debug','host.company.com','This is a test message from Kiwi Syslog
Daemon')
```

3.6 Setup - DNS Resolution (設定 - DNSの解決)

3.6.1 Resolve the address of the sending device (送信デバイスのアドレス解決)

送信デバイスのIPアドレスをホスト名に変換します。203.50.23.4 に代えて sales-router.company.com のような表示になります。

解決されたホスト名は表示やその他のアクションで使用されます。

また、Hostname タイプフィルターでもホスト名が使用されます。

希望するなら、Remove the domain name オプションにより表示からドメイン名の部分を削除することが可能です。

3.6.2 Remove the domain name (show only the host name) (ドメイン名を消去- ホスト名のみ表示)

Resolve the IP address of the sending device オプションをチェックすると、解決したホスト名の後ろのドメイン名を削除できます。すなわち sales-router.company.com ではなく sales-route rとなります。

同一ドメインからのみメッセージを受信する場合や、ホスト名を表示するときにできるだけスクロールしないで済むようにしたいときに有効です。

このオプションはすべてのロギングアクションで使用されるホスト名フィールドに対して適用されます。

3.6.3 Resolve IP addresses within the message text (SyslogメッセージテキストのIPアドレス解決)

この機能は正規登録版でのみ使用できます。

Webブラウザやファイアウォール等からのデータをロギングするとき、メッセージテキストにIPアドレスが含まれている場合があります。このオプションを有効にすれば、これらのIPアドレスはホスト名やWebサイトアドレスに変換されます。プログラムはメッセージテキストに含まれているIPアドレスを検索します。解決された名前の表示方法も指定できます。IPアドレスを名前に置き換えたりIPアドレスの後に名前を追加することができます。

*NetBIOS名の解決は通常のDNSエントリ解決より時間がかかります。NetBIOS名を解決する時はDNSタイムアウト値を20～30秒にしてください。

例:

Replace IP address with host name オプションを選択した場合、Webサイト `http://192.168.1.2/index.html`、`src=192.168.5.100 rxbytes=64`に接続した Test ユーザーのメッセージは以下のようになります。

Test user connected to website `http://website.company.com/index.html`. `src=userpc.company.com rxbytes=64`

Place host name next to IP address オプションを選択した場合は以下のようになります。

Test user connected to website `http://192.168.1.2 (website.company.com) /index.html`. `src=192.168.5.100 (userpc.company.com) rxbytes=64`

Remove the domain name オプションにチェックすると解決した名前からドメイン名が削除されます。

フィルター一致条件から選択的にドメイン名を含めたり、削除したりするには **If domain name contains** チェックボックスをチェックしてください。

削除するドメイン名を引用符で囲んで入力します。複数のドメインをフィルターするには引用符で囲んだ文字列をスペースかカンマで区切ってください。

`".companyabc.com"`, `".companyxyz.co.uk"`

`mypc.company.co.uk` と解決されたIPアドレスは `mypc` になります。

Host name tagging

Place host name next to IP address オプションを選択すると通常ホスト名には [] とスペースのタグが付けられます。このオプションで解決したホスト名に任意のタグを付けることができます。例えば、ホスト名の前に `hostname=[`、後ろに `]` を付けるように指定することも可能です。メッセージのフォーマットに合わせて任意のタグ文字を指定してください。

WELFフォーマットメッセージでの推奨タグフォーマットは、`resolved_host=` とスペースです。

3.6.4 DNS query timeout (DNSクエリーのタイムアウト)

ルックアップクエリーに対するDNSサーバーの応答タイムアウトを指定します。デフォルトは8秒です。遅いDNSサーバーやネットワークリンクが低速であれば大きな値に変更できます。

この値を大きくするのはNetBIOS (Windowsを実行しているコンピュータのマシン名) 経由でアドレス解決をする場合に限りください。ユニキャストルックアップによるNetBIOS名の解決には最大20秒かかることがあります。

DNSサーバーがローカルで内部アドレス変換だけの場合は3秒以下にしても大丈夫です。

タイムアウト時間を大きくしすぎると名前解決が終了するまでメッセージがキューに入って待ち状態になることに気づくことがあります。この場合キューが1,000以上になるとメッセージが失われます。メッセージバッファの空き領域がどれくらいあるかはSyslogメイン画面で分かります。

3.6.5 Setup - DNS Setup (設定 – DNS設定)

3.6.5.1 Internal IP address – Name Resolution (内部IPアドレス - 名前解決)

Internal IP address range(s):

内部ネットワークアドレス空間を識別するマスク済みIPアドレスのリストです。

このリストにはRFC1918/3330/3927で確認された標準内部(プライベート)ネットワークアドレス空間がデフォルト値として表示されています。リストにはIANAによる予約プライベートインターネットアドレス空間およびリンクローカルアドレス範囲が含まれています。

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
169.254.0.0 - 169.254.255.255 (link-local)

内部IPアドレス範囲の追加：

Internal IP address range リストの下にあるテキストボックスに直接マスク済みIPアドレスを入力し [Add] ボタンをクリックします。IPアドレスは X でマスクされていなければなりません。X はその範囲(0-255)のどの値も可能であることを表します。

例：
内部アドレススペースが 10.0.0.0 – 10.255.255.255 の場合マスク済みIPアドレスとして 10.x.x.x と入力します。

重要：

これらのアドレス範囲に含まれるsyslogホストIPアドレスは Internal IP Address – Name Resolution の設定にのみ従って名前解決が行われます。内部アドレス範囲に含まれないホストIPアドレスは External IP Address – Name Resolution の設定に従って名前解決が行われます。この違いは重要です。アドレス範囲リストはフィルターのように動作します。このフィルターはローカルDNSサーバーやNetBIOSを使って内部ネットワーク上のIPアドレスを解決するか、外部DNSサーバー等でIPアドレスを解決するかを決定します。内部アドレス空間を正しく設定されているかどうか名前解決クエリーの応答時間に直接影響します。

Resolve internal addresses using NetBIOS

チェックするとKiwi Syslog DaemonはローカルサブネットにNetBIOSブロードキャストクエリーを送信して内部名前解決を行います。

Resolve internal addresses using DNS server

チェックするとKiwi Syslog DaemonはDNSサーバーにDNSクエリーを送信して内部名前解決を行います。

Preferred / Alternate internal DNS server addresses

DNSクエリーを送信する内部ネットワークアドレスを入力します。デフォルトではこれらのアドレスはKiwi Syslog Daemonによって自動検出されます。ネットワーク構成によってはデフォルト値を変更する必要があります。

もし優先DNSサーバーが使用できなければ、あるいはリクエストに対応できなければ、同じクエリーが代替DNSサーバーに送られます。

代替DNSサーバーが使用できなければ、このアドレスは何も入力しないでください。

3.6.5.2 External IP address – Name Resolution (外部IPアドレス - 名前解決)

Resolve external address using NetBIOS

チェックするとKiwi Syslog DaemonはNetBIOSを使って外部IPアドレスの名前解決を行います。

Resolve external addresses using DNS server

チェックするとKiwi Syslog DaemonはDNSサーバーにDNSクエリーを送信して外部IPアドレスの名前解決を行います。

Preferred / Alternate external DNS server addresses

DNSクエリーを送信する外部ネットワークアドレスを入力します。デフォルトではこれらのアドレスはKiwi Syslog Daemonによって自動検出されます。ネットワーク構成によってはデフォルト値を変更する必要があります。

もし優先DNSサーバーが使用できなければ、あるいはリクエストに対応できなければ、同じクエリーが代替DNSサーバーに送られます。

代替DNSサーバーが使用できなければ、このアドレスは何も入力しないでください。

3.6.6 Setup - DNS Cache (設定 – DNSキャッシュ)

3.6.6.1 ローカルのDNSキャッシュ

IPアドレスのホスト名への解決要求の都度DNSサーバーへの問合せが発生します。このことによりプログラム、ネットワーク、DNSサーバーへのオーバーヘッドが増え、特に大量のメッセージを受信した時に大きな負荷がかかる場合があります。

DNSトラフィックを減少させ、名前解決時間を短縮するためにDNS キャッシュが使われます。一度ホスト名が解決されるとその結果がローカルに保存されます。次回同じアドレスを解決する必要があるときは別のDNS要求を発行せずにキャッシュから結果を引き出します。

フリーウェアライセンスではローカルのDNSキャッシュに保存可能なのは100エントリー、正規登録版では20,000エントリーまでです。

[View] ボタン:

現在のキャッシュエントリーをファイルに出力し、メモ帳を開いてその内容を表示します。キャッシュのパフォーマンス情報も表示されます。

[Refresh] ボタン:

現在キャッシュ内にある有効なエントリー数を計算します。

[Clear] ボタン:

すべての変動エントリー(DNSルックアップの結果)をクリアします。ファイルからロードされた固定エントリーは対象外です。

[Clear All] ボタン:

(変動と固定の両方を含む)すべてのエントリーのDNSキャッシュをクリアします。固定エントリーファイルを再度読み込むにはプログラムを再起動する必要があります。

3.6.6.2 Cache settings (キャッシュ設定)

Flush entries after X seconds:

指定時間後キャッシュから古いエントリーを消去します。デフォルト値は1440分(1日)です。エントリーは1日の間はキャッシュに残りますが、その後キャッシュから消去されルックアップを経て再作成されます。

Enable pre-emptive lookup of IP addresses:

各アドレスを順番に解決するのではなく、メッセージをプロセスキューに追加する前にIPアドレスを抽出します。アドレス解決を非同期に実行し、結果をキャッシュに保存します。メッセージが処理される時にはアドレスはすでにキャッシュに存在します。DNS解決はマルチスレッドルックアップシステムで同時に100個(フリーウェアモードでは10個)実行します。大量の受信メッセージがあり、IPアドレスの解決を速やかに行いたいときは、このオプションを有効にしてください。

Pre-load the cache with static entries from a hosts file:

プログラムの起動時に固定ホストエントリーのリストをロードします。リストにはタブで区切ったIPアドレスとホスト名が書かれていなければなりません。アドレスはキャッシュにロードされ、固定マークがつけられます。これは期限の無いことを意味し、変動エントリーのようにクリアされません。

サンプルのホストファイルがインストールフォルダにあります。名前はStaticHosts.txtです。

Hostファイルの例

```
# Static DNS host file
# Each entry must consist of an IP address, a tab, then a host name
# The IP address is in the format aaa.bbb.ccc.ddd
# The host name can be any text value that you like up to 63 characters in length
#
# Comments can be on a separate line and must start with a # character
#
# Example:
# 192.168.1.1 myhost.mycompany.com
#
# NOTE: The IP address and host name MUST be separated with a tab (ASCII chr 9)
# Spaces will not be recognised as a valid separator
# Default value for localhost
127.0.0.1 localhost
# local machines
192.168.1.2 myfunny.valentine.com
192.168.1.5 flyme2.themoon.com
```

3.7 Setup – Modifiers (設定 – 修正)

メッセージを受信すると、指定した各種の修正が行われます。メッセージの長さを短縮したり、不正なプライオリティを変更したり、余分なCR/LFコードを削除するといった処理が可能です。

3.7.1 Syslog message modifiers (Syslogメッセージモディファイア)

Remove imbedded date and time from Cisco messages

Ciscoデバイスはsyslogメッセージに時刻スタンプを追加します。これらの余分な時刻スタンプを削除することによって、領域を節約したりログファイルを読みやすくすることができます。

このオプションは特定のCiscoメッセージフォーマットに対して機能します。将来はCisco PIXファイアウォールのメッセージを含むCisco製品に採用されているすべての日付時刻フォーマットに対応する予定です。

Allow messages with no priority (use default priority)

ルーターやホストから発せられるメッセージにはプライオリティコードが書かれていない場合があります。このような場合にメッセージにデフォルトのプライオリティを適用することができます。このボックスをチェックし、ドロップダウンリストから適用したいデフォルトプライオリティを選択してください。

正常なSyslogメッセージテキストには先頭にプライオリティコードが書かれています。

例： <100>This is a test message

標準Unixプライオリティコードでのプライオリティは0~191です。

Maximum message length (bytes)

受信メッセージの最大メッセージサイズを制限します。小さいメッセージのみ受信したいときはデフォルトの4096より小さい値を指定してください。

このオプションでメッセージサイズを制限することによって、ハッカーから送信されてきた、あるいは転送エラーで戻ってきたサイズの大きいメッセージを受信拒否することができます。

一部のSyslog Daemonは大きなパケットを受信するとクラッシュすることがあります。このオプションでプログラムが受信し処理しうるパケットのサイズに制限してください。

Syslog RFC 3164 は正常なメッセージ長は(パケットヘッダーを除いて)1024バイトを以下であると定義しています

Allow messages with priority > 191 (use default priority)

Syslogメッセージの先頭にはプライオリティコードが書かれています。通常Unixシステムやルータでは0~191です。デバイスから送信されてくるメッセージに191以上の値が付いていることも時々あります。プライオリティの値は191以上のこともあります。191以上のプライオリティまたはファシリティのレベルを定義する標準は存在しません。

このオプションを有効にすると、191以上のプライオリティの付いた受信メッセージにデフォルトプライオリティの設定で指定したプライオリティが適用されます。

Remove CR/LF from end of messages

一部のルーターやホストはメッセージの送出時に末尾にCR/LFを追加します。そのため、ログファイルに2行の空白行ができます。

このオプションをチェックするとメッセージの末尾にあるすべてのCR/LF文字が削除されます。

Replace non-printable characters with <ASCII value>

一部のルーターやホストは制御文字を含むメッセージを送出します。例えば、複数行のメッセージにはCRおよびLFが含まれています。このオプションを有効にすると、制御文字の代わりに同等のASCII文字が表示されます。

例えば、CRを受信すると<013>で置き換えます。

3.8 Setup – Scripting (設定 – スクリプト作成)

スクリプトファイルおよび統計レポートで使用するカスタム統計フィールドの名前と初期値を設定します。

スクリプト用に16のカスタム統計フィールドがあります。これらの値は固定されており他のスクリプトフィールドのように削除できません。

カスタム統計の値は Syslog Statistics ウィンドウの Counters タブで見ることができます。指定したフィールド名はStatistics ウィンドウおよび日別統計Eメールに使用されます。

統計カウンターの初期値は任意の値に設定できます。デフォルトは 0 です。例えば降順カウンターとして初期値を1000にし Run Script アクションが実行されるたびにカウンターの値を1ずつ減少させることができます。

名前と初期値はプログラムの起動時に適用されます。プログラムでフィールドをこれらの値で強制的に再初期化するには、**File | Debug options | Initialize custom statistics** メニューを使います。あるいはメインsyslogウィンドウで [Ctrl]+[F9] を押します。

スクリプト作成については[関連項目](#)を参照してください。

3.9 Setup – Appearance (設定 – 外観)

3.9.1 Wallpaper (壁紙)

ウィンドウに適用される背景画像を選択します。サンプルとしてペーパースタイルの画像が付属しています。

3.10 Setup - E-mail options (設定 – Eメールオプション)

3.10.1 E-mail setup options (設定 – Eメール設定オプション)

Send syslogd alarm messages to:

アラーム閾値を超えるとEメールでアラームメッセージが送信されます(アラーム閾値は Alarms で設定します)。

アラームが発生した場合に通知するEメールアドレスを入力します。複数のアドレスを指定するときはカンマで区切ります。

例 noc@company.com,helpdesk@company.com,pager123@company.com

テキストボックスの左側にあるチェックボックスでアラームEメール送信の有効/無効を切り替えます。

アラームEメールメッセージの例は[関連項目](#)を参照してください。

Send syslog statistics to:

毎晩深夜0:00に日別統計情報がEメールで送信されます。送信されるEメールメッセージにはログファイルのサイズ、アーカイブドライブの空き容量、メッセージ総数、メッセージ送信元の概要、FacilityとLevelなどが記載されます。

Courier new などの固定フォントで表示するのが最も望ましく、一行に全列を表示できます。

日別統計Eメールメッセージの例は[関連項目](#)を参照してください。

Short alarm messages (for pagers)

チェックすると、件名だけが送信されます。メッセージ本文は送信されません。メッセージをポケットベルに転送するときや表示スペースが限られているときに使用すると便利です。

Keep a log file of e-mail activity

Eメールでアラームや統計を送信する場合、どのメッセージを誰に送ったかというログを残すことができます。

このログファイルの名前は SendMailLog.txt で、プログラムのインストールディレクトリに作成されます。

[View log] ボタンをクリックすると、メモ帳が開き内容を確認できます。

既存のログファイルを破棄し、新しいログファイルを作成するには [delete log] ボタンをクリックします。

Enable verbose logging

メールが正常に送信されないときに非常に有効です。プログラムからメールサーバーへ送信された全情報がログファイルとして残ります(メッセージの内容は記録されません)。

注: 送信メッセージが大量にあるときにこのオプションをチェックすると、多くのディスクスペースが使用されます。

Hostname or IP address of SMTP mail server:

SMTPサーバーのホスト名かIPアドレスを入力します。ローカルサーバーもしくはISPによって提供されたサーバーのアドレスを指定します。

メールサーバーのホスト名は通常 mail.company.com あるいは smtp.company.com のような形となります。

ローカルSMTPサーバーが無い場合は Mail Direct などを使うことをお勧めします。

Mail Direct の入手先 : <http://www.ocloudsoft.com>

Valid 'from' e-mail address on SMTP server:

このフィールドには有効な返信用アドレスを入力してください。メールの送信エラー時SMTPサーバーはこのアドレスにメッセージを転送します。

SMTPサーバーによってドメイン名を記述する必要があるものとなないものがあります。

指定するアドレスは受信Eメールのmessage from (送信者)フィールドに表示されている名前と同一でなければなりません。

アドレスの後に続けて(xxxxx)のように括弧で括って分かりやすい表示名を任意で指定することができます。xxxxxはメールクライアントの From (送信者)フィールドに表示されます。

例 noc@company.com (Syslog Server)

上の例で名前の Syslog Server は受信メッセージの From(送信者)フィールドに表示されます。SMTPサーバーによってはこの形式で from(送信者)アドレスを表示する機能をサポートしていません。その場合はEメールアドレスのみを指定してください。

SMTP port:

ご使用のSMTPサーバーが待機用として標準ポート以外のポートを使用している場合は、ここにそのポート番号を指定します。通常SMTPサーバーの受信待機ポートは25番です。企業によってはセキュリティ上の理由からこの値を変更しています。指定可能な値は1~65535までです。

Timeout:

プログラムがSMTPサーバーの応答待ち時間を指定します。SMTPがダイヤルアップ経由で接続している場合やビジー状態であることが多いときは、デフォルトの30秒より大きくします。指定可能な値は1~240までです。

SMTP Username and Password:

SMTPサーバーがEメールを受信する前に認証が必要な場合に限り指定する必要があります。ほとんどのSMTPサーバーでは指定しなくても構いません。

左のチェックボックスをチェックし、SMTPサーバーのユーザー名とパスワードを入力すると認証が可能になります。指定する場合はネットワーク管理者、SMTPサーバーのプロバイダ、ISPにお問合せください。

認証で POP before SMTP オプションを使わなければならない時、フリーウェアのPOPメールボックスチェッカーをダウンロードし使ってください。新しいメッセージを5分ごとにチェックしその後SMTPメールが送られます。POP before SMTP authentication は今後のバージョンに追加する予定で開発が進められています。

3.10.2 アラームメッセージの例

```
Syslog Alarm: 2198 messages received this hour.
The current maximum threshold is set at 3 messages per hour.
This could indicate a problem, please check the log files and syslog statistics below.
/// Kiwi Syslog Daemon Statistics ///
```

```
-----
24 hour period ending on: Fri, 26 Jan 2005 15:39:16 +1200
Syslog Daemon started on: Wed, 17 Jan 2005 11:39:53
Syslog Daemon uptime: 9 days, 3 hours, 59 minutes
-----
```

```
+ Messages received - Total:          361965
+ Messages received - Last 24 hours:   37964
+ Messages received - Since Midnight:  26530
+ Messages received - Last hour:       2821
+ Messages received - This hour:       2198
+ Messages per hour - Average:         1582
+ Messages forwarded:                  3063
+ Messages logged to disk:              26530
+ Errors - Logging to disk:              0
+ Errors - Invalid priority tag:         0
+ Errors - No priority tag:              0
+ Errors - Oversize message:             0
+ Disk space remaining on drive C:      59505 MB
-----
```

Breakdown of Syslog messages by sending host

```
+-----+-----+-----+
| Top 20 Hosts | Messages | Percentage |
+-----+-----+-----+
| pix_firewall_inside | 26530 | 100.00% |
+-----+-----+-----+
```

Breakdown of Syslog messages by severity

Message Level	Messages	Percentage
0 - Emerg	0	0.00%
1 - Alert	0	0.00%
2 - Critical	0	0.00%
3 - Error	123	0.46%
4 - Warning	0	0.00%
5 - Notice	715	2.70%
6 - Info	25692	96.84%
7 - Debug	0	0.00%

End of Report.

3.10.3 統計メッセージの例

```
/// Kiwi Syslog Daemon Statistics ///
```

```
-----  
24 hour period ending on: Fri, 26 Jan 2005 00:00:01 +1200  
Syslog Daemon started on: Wed, 17 Jan 2005 11:39:53  
Syslog Daemon uptime: 8 days, 12 hours, 19 minutes  
-----
```

```
+ Messages received - Total:          335435  
+ Messages received - Last 24 hours:  35206  
+ Messages received - Since Midnight:  35967  
+ Messages received - Last hour:      1149  
+ Messages received - This hour:      366  
+ Messages per hour - Average:        1467  
+ Messages forwarded:                  0  
+ Messages logged to disk:             35967  
+ Errors - Logging to disk:             0  
+ Errors - Invalid priority tag:        0  
+ Errors - No priority tag:             0  
+ Errors - Oversize message:           0  
+ Disk space remaining on drive C:     59573 MB  
-----
```

Breakdown of Syslog messages by sending host

Top 20 Hosts	Messages	Percentage
pix_firewall_inside	35967	100.00%

Breakdown of Syslog messages by severity

Message Level	Messages	Percentage
0 - Emerg	0	0.00%
1 - Alert	0	0.00%
2 - Critical	0	0.00%
3 - Error	69	0.19%
4 - Warnin	0	0.00%
5 - Notice	731	2.03%
6 - Info	35167	97.78%
7 - Debug	0	0.00%

End of Report.

3.11 Setup - Alarm thresholds (設定 - アラーム閾値)

3.11.1 Notify by Mail (メールで通知)

最低または最高の閾値として設定した値を超えると E-mail オプションで設定したアラーム通知の受信者すべてにEメールが送られます。

このとき送信されるメッセージにはアラームメッセージであることと閾値を超えたこと、および現在の閾値などが記載されています。

参照用として直近の統計も記されています。

アラームEメールの例については[関連項目](#)を参照してください。

3.11.2 Audible Alarm (音で通知)

この機能は正規登録版でのみ使用できます。

最低または最高の閾値として設定した値を超えるとKiwi Syslog Daemonのメインウィンドウのステータスバーに赤い警告ベルが表示され、点滅しながら1秒1回の割合でピープ音が鳴り始めます。鳴動を止めるにはアラームアイコンをダブルクリックしてキャンセルしてください。

Play sound file が有効になっているときはキャンセルされるまで指定されたサウンドファイルが5秒おきに再生されます。

アラーム音をキャンセルするには点滅している赤の警告ベルアイコンをダブルクリックしてください。

3.11.3 Run Program (プログラム実行)

この機能は正規登録版でのみ使用できます。

最低または最高の閾値として設定した値を超えると指定した外部プログラムを実行します。コマンドラインパラメータとして実行するプログラムに情報を渡すことができます。

コマンドラインに置き換え可能な値の詳細については[関連項目](#)を参照してください。

例：

Pager.exe "555-1234" ,"Syslog - Warning, lots of messages received, Max set at %MsgAlarmMax but received %MsgThisHour so far this hour."

[Test] ボタンを押して外部プログラムが期待通りに実行されるかどうか確認してください。

スペースを含むファイル名やパスは引用符(")で囲んでください。

3.12 Setup - Input options (設定 - 入力オプション)

3.12.1 Setup - Input options (設定 - 入力オプション)

UDPまたはTCPポートでsyslogメッセージを受信するだけでなく、SNMP Version1/2c トラップの受信もできます。

デフォルトではUDP 514ポートが受信ポートとして有効になっています。syslog受信ポートとして最も一般的に使用されているポートです。

一部のファイウォール (Cisco PIX) やsyslogデーモンではTCPでsyslogを送信可能です。Cisco PIXはTCP 1468ポートからメッセージを送信します。デフォルトではTCPポートでの受信が無効になっています

SNMP Version1/2c トラップの受信およびデコーディングはサポートされていますが、デフォルトでは無効になっています。通常のSNMPトラップ受信ポートはUDP 162です。

受信ソケットとしてUDP、TCPおよびSNMPの3種類が使用可能です。

また、キーブアライブメッセージを受信ストリームに挿入することによって、トラフィックの同期を取ることが可能です。

3.12.2 Inputs – UDP (入力 - UDP)

通常、Kiwi Syslog DaemonはUDPポート 514でUDP syslogメッセージを受信します。他のポートでsyslogメッセージを受信したい場合は1～65535の任意の数値を入力してください。ポートを514以外に変更した場合はsyslogメッセージを送信するデバイスのポート番号も変える必要があります。

Kiwi Syslog DaemonでUDP syslogメッセージの受信を停止するには、**Listen for UDP Syslog messages** チェックボックスのチェックを外してください。Kiwi Syslog Daemonでは一度に一つのUDPポートでのみ受信します。将来は複数のUDPポートでの同時受信が可能になるよう開発を進めています。

Bind to Address:

デフォルトではUDPソケットは接続されているすべてのインターフェイスのメッセージを受けます。特定のインターフェイスに限定するときは **Bind to address** フィールドにIPアドレスを指定することができます。その必要がない場合はこのフィールドは空白のままにしておいてください(**Bind to address** フィールドを空白にすると、すべてのインターフェイスから受信します。多くの場合これが最適です)。

例えば、コンピュータにルーティングされていない二つのインターフェイス192.168.1.1 と192.168.2.1が存在する場合、192.168.1.1 インターフェイスのみバインドすることができます。この場合もう一方のインターフェイスへ送信されたsyslogメッセージは無視されます。

Data Encoding:

異なるエンコード形式の複数のシステムからメッセージを受信している場合、受信データに適用するデコード形式を指定することができます。デフォルトではシステムコードページを使用するように設定されています。ドロップダウンリストにある代表的なエンコード形式から選択してください。これ以外のエンコードを指定するには、Other--> を選択しコードページ番号を右側のフィールドに入力します。

ほとんどのWindowsシステムで使用可能なコードページは数多くあります。次のWebページを参照してください。

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/act/html/actml_ref_scpq.asp

使用可能なコードページの例

名前	コードページ番号	説明
System	1	System Code Page
ANSI	0	ANSI
UTF-8	65001	Unicode Transformation Format 8
Shift-JIS	932	Japanese
EUC-JP	51932	Japanese Extended Unix Code
BIG5	950	Traditional Chinese
Chinese	936	Simplified Chinese

注: ご使用のシステムのコードページで有効になっていない番号を指定すると、受信データは正常にデコードされず失われます。自信がない場合はすべてのUnicode文字を処理可能なUTF-8を指定してください。

UTF-8については次のWebページを参照してください。

<http://en.wikipedia.org/wiki/UTF-8>

3.12.3 Inputs – TCP (入力 – TCP)

Syslog ロギングは伝統的にUDPポート514でおこなわれています。

UDPはコネクションレスプロトコルであり、不確実性が内在します。UDPでは応答、エラー検出、シーケンス管理、消失パケットの再送などは行いません。

Cisco PIX などではTCPによるsyslogプロトコルをサポートしています。TCPはコネクション志向型のプロトコルです。あて先ホストが存在することが保証されます。送信デバイスが初期化される、あるいは最初のsyslogメッセージが送信される前に接続が確立されます。最初に3ウェイハンドシェイクを行い、すべてのパケットはサーバーが受信し次の送信前に応答が返されますので、TCPを使うと遅くなります。TCPプロトコルは信頼性とエラー補正を提供します。メッセージをsyslogサーバーに確実に送信したいときはこちらを使用してください。

[PIX ファイアウォール](#)および[Cisco PIX](#)の関連項目を参照してください。

Bind to Address:

デフォルトではTCPソケットは接続されているすべてのインターフェイスのメッセージを受けます。特定のインターフェイスに限定するときは **Bind to address** フィールドにIPアドレスを指定することができます。その必要がない場合はこのフィールドは空白のままにしておいてください。(**Bind to address** フィールドを空白にすると、すべてのインターフェイスから受信します。多くの場合これが最適です)。

例えば、コンピュータにルーティングされていない二つのインターフェイス192.168.1.1 と192.168.2.1が存在する場合、192.168.1.1 インターフェイスのみバインドすることができます。この場合もう一方のインターフェイスへ送信されたsyslogメッセージは無視されます。

Cisco PIX はポート1468を使います。デフォルト動作は、syslog サーバーへの接続ができなかった場合すべてのネットワークトラフィックがブロックされます。

Cisco Pix Firewallの詳細については次のWebページを参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix>

Data Encoding:

異なるエンコード形式の複数のシステムからメッセージを受信している場合、受信データに適用するデコード形式を指定することができます。デフォルトではシステムコードページを使用するように設定されています。

ドロップダウンリストにある代表的なエンコード形式から選択してください。これ以外のエンコードを指定するには、Other--> を選択しコードページ番号を右側のフィールドに入力します。

大半のWindowsシステムで使用可能なコードページについては、次のWebページで確認してください。

<http://msdn.microsoft.com/ja-jp/library/aa288104.aspx>

使用可能なコードページの例

名前	コードページ番号	説明
System	1	システムコードページ
ANSI	0	ANSI
UTF-8	65001	Unicode Transformation Format 8
Shift-JIS	932	日本語
EUC-JP	51932	日本語(EUC)
BIG5	950	繁体字中国語
Chinese	936	簡体字中国語

注: ご使用のシステムのコードページで有効になっていない番号を指定すると、受信データは正常にデコードされず失われます。自信がない場合はすべてのUnicode文字を処理可能なUTF-8を指定してください。

UTF-8については次のWebページを参照してください。

<http://ja.wikipedia.org/wiki/UTF-8>

Message Delimiters:

TCPで送信されるsyslogメッセージは必ずしも1つのTCPパケットに含まれているわけではありません。Kiwi Syslog Daemonには連続して送信されるTCPパケットを内部に蓄積するバッファリング機能が付属しています。そのため、1つのTCPストリームの中に含まれているsyslogメッセージを個別に特定する必要があります。それにはメッセージ区切り文字を使います。各区切り文字は文字(または連続した文字)を表し、ストリームを分割して個別のsyslogメッセージに変換します。使用する区切り文字の種類はTCPでsyslogを送信するクライアントまたはデバイスによって全く違います。

区切り文字の例:

CRLF (ASCII 13, ASCII 10)
CR (ASCII 13)
LF (ASCII 10)
Null (ASCII 00)

3.12.4 Inputs – SNMP (入力 - SNMP)

Kiwi Syslog Daemon はSNMP v1/2c トラップを受信可能です。受信したトラップはデコードされ正規のsyslogメッセージと同様に処理されます。

Listen for SNMP traps:

デフォルトでは無効になっています。チェックボックスをオンにするとSNMPトラップ受信が有効になります。

UDP port:

SNMPトラップを受信するUDPポートです。通常トラップは162ポートに送信されます。1~65535までの値を入力できます。162以外の値を入力した場合は、トラップ送信デバイスでも送信先として同じポートを指定します。

Bind to Address:

デフォルトではSNMPとラップレシーバーは接続されているすべてのインターフェイスのメッセージを受けます。特定のインターフェイスに限定するときは **Bind to address** フィールドにIPアドレスを指定することができます。その必要がない場合はこのフィールドは空白のままにしておいてください。(Bind to address フィールドを空白にすると、すべてのインターフェイスから受信します。多くの場合これが最適です)。

例えば、コンピュータにルーティングされていない二つのインターフェイス192.168.1.1 と192.168.2.1が存在する場合、192.168.1.1 インターフェイスのみバインドすることができます。この場合もう一方のインターフェイスへ送信されたsyslogメッセージは無視されます。

SNMP fields:

どのSNMPフィールドをデコードし入力メッセージに追加するかを選択します。フィールド横のボックスをチェックし有効にします。フィールド名をドラッグアンドドロップすることによってメッセージのデコード順を変更できます。

Community:

トラップメッセージに含まれているパスワードのようなものです。通常この値は"public", "private" あるいは"monitor"に設定されています。

Enterprise:

SNMPトラップのMIBエンタープライズを表すドット区切りの値(1.3.6.1.x.x.x.x) です。このフィールドはv1トラップにのみ適用されます。v2トラップではエンタープライズ値は2番目の変数としてメッセージにバインドされています。

Uptime:

メッセージ送信デバイスのシステムアップタイムです。値は時間単位で表示されデバイスがリスタートされると0にリセットされます。小さい値は最近デバイスがウォームあるいはコールドスタートされたことを示します。このフィールドはv1トラップにのみ適用されます。v2トラップではシステムアップタイムは最初の変数としてメッセージにバインドされています。

Agent address:

送信デバイスのIPアドレスです。

Trap type:

Generic Type、Specific Trap-Type、Specific Trap-Name の3種類のトラップタイプフィールドが有効になります。これらのフィールドはv1トラップにのみ適用されます。6種類のGeneric Type のトラップが定義されています。Generic Type が6に設定されていると Enterprise タイプのトラップであることを示します。この場合 Specific Type トラップの値を考慮しなければなりません。

Version:

受信トラップのバージョンです。現在では v1 と 2c がサポートされています。

Message:

バインドされているすべての変数で構成されるフィールドです。トラップには1つ以上の変数がバインドされることもあります。変数が8進文字タイプであれば、プレーンテキストとして表示されます。カウンターや整数値で表される変数もあります。この場合MIB構文に対する値としてチェックしてください。

Syslog priority to use:

受信したSNMPメッセージは内部で標準syslogメッセージに変換されます。標準syslogメッセージと同じように、ここのオプションで受信したSNMPメッセージに対してフィルターをかけることができます。SNMPトラップにはメッセージの facility や level が設定されていない為デフォルト値を適用する必要があります。この値をルールエンジンで使用することができます。例えば、すべてのトラップに Local0.Debug というタグを付けることができます。タグ付け後、この facility とlevel の設定されたメッセージを検索するプライオリティフィルターを作成し、特定のアクションを実行することができます。

SNMP field tagging:

このドロップダウンリストでデコードされたフィールドをどのようにメッセージに変換するかを指定します。デフォルトは fieldname=value が選択されています。この値を選択しておけば、後のログ解析が容易になります。これ以外に選択可能なオプションとしてXML、カンマ区切り、[] 区切りなどがあります。

fieldname=value オプションによってタグ付けされたメッセージの例 :

```
community=public enterprise=1.3.6.1.2.1.1.1 enterprise_mib_name=sysDescr uptime=15161
agent_ip=192.168.0.1 generic_num=6 specific_num=0 version=Ver1 generic_name="Enterprise specific"
var_count=01 var01_oid=1.3.6.1.2.1.1.1 var01_value="This is a test message from Kiwi Syslog Daemon"
var01_mib_name=sysDescr
```

スペースを含む値は引用符 ("") で囲まれます。

Use LinkSys Display filter:

LinkSys Display フィルターは表示からすべてのPPPメッセージを消去します。PPPメッセージは通常通りファイルには記録されています。

この機能はLinkSysネットワークデバイスからのメッセージを記録するときのみ有効です。

Perform MIB lookups:

Kiwi Syslog Daemonの内蔵データベースには既知のオブジェクトID値とそのテキスト名が登録されています。Cisco, 3Com, Allied Telesyn, SonicWall, Nokia, Checkpoint, BreezeCom, Nortel, SNMP MIB-II等の最も一般的なトラップを処理します。

MIBデータベースファイルはKiwi Syslog Daemonをインストールしたフォルダの下の MIBs フォルダにKiwiMIBDB.dat というファイル名で保存されています。このデータベースは60,000件以上のMIB定義からコンパイルされた独自のデータベースファイルです。多くのMIBファイルには使用できるトラップ情報が5%以下しか含まれていないため、このプレコンパイル方式を採用したことによって標準的なMIBコンパイラ/パーサーを使用する際のルックアップ時間、ディスクスペース、ハッシュテーブルメモリが大幅に節約されています。

追加したいMIBルックアップ値があればご連絡ください。zip圧縮したMIBファイルを下記まで送信してください。
http://www.kiwisyslog.com/option.com_enquiry/Itemid,459/

新しいデータベースファイルをコンパイルし更新結果を返送します。
すべてのOIDを参照できるよう Unknown_OID_list.txt ファイルもzipに入れてください。

MIBデータベースを作成するとき、MIBファイルからすべてのトラップ、通知、参照変数が読み込まれ解析されます。オブジェクトを正しく参照できないときは追加されません。この場合、知るべきことはOID値であり、それが含まれることを確認できます。詳細は次のセクションを参照してください。

Log failed lookups to debug file:

OID値がデータベースに登録されておらず、このオプションがオンになっていればOID値はデバッグファイルに記録されます。デバッグファイルは Kiwi Syslog Daemon をインストールしたフォルダの下の MIBs フォルダにUnknown_OID_list.txt というファイル名で保存されています。このファイルをzip圧縮し下記まで送信してください。

http://www.kiwisyslog.com/option.com_enquiry/Itemid,459/

次のデータベースリリース時に未登録の値を追加します。

Show additional OID suffix info:

デバイスが送信する情報にはメインのOID番号の後にエンコード済みの追加情報が付けられていることがあります。この情報にはインターフェイスのインデックス、送信元と送信先のアドレス、ポート番号等を含めることができます。MIB名に対する接尾語として表示されます。

例えば、Ciscoスイッチが変数 1.3.6.1.2.1.2.2.1.2.3 を含む Link up トラップを送信するとします。OID番号の最後の 3 はインターフェイスインデックスを参照し、それ以外はMIB名である ifDescr に解決されます。

このオプションをオンにすると、MIB名に .3 の情報が追加されて表示されます。例えば、IfDescr.3=SlowEthernet0/3 の場合、オプションをオフにすると次のように表示されます。

ifDescr=SlowEthernet0/3

3.12.5 Beep on every message received (メッセージ受信時ビーブ音)

このオプションをオンにするとsyslogメッセージやSNMPトラップを受信するたびにビーブ音が鳴ります。フィルターで表示やロギングをブロックしている場合でもビーブ音は鳴ります。デバッグ時にメッセージを受信したことを知るのに有効です。

* このオプションがオフになっているときにメッセージ受信時にビーブ音が鳴った場合は、メッセージをディスクに記録しようとしてエラーが生じたことを意味しています。エラーの詳細についてはエラーログを確認してください(Viewメニューより表示できます)。メッセージを指定されたログファイルに書き込めないときにビーブ音が鳴ってエラーが発生していることを知らせます。

3.12.6 Cisco PIX ファイアウォール(TCP)

Cisco PIX ファイアウォールはUDPの代わりにセキュアコネクション志向のTCPでメッセージを記録します。PIXのデフォルトTCPポートは1468です。このポート番号は1~65535までの任意の番号を使用できます。デフォルト以外の値に変更したときはPIXのポートもそれに応じて設定を変更する必要があります。

TCPはコネクション志向であるため、ロギングデバイス(Kiwi Syslog Daemon)がディスクの空きがなくなっている等の理由でメッセージ受信不能になったときにそのことをPIX側で知ることができます。PIXにフィードバックするには、Kiwi Syslog Daemon は接続をクローズしメッセージの受信ができないようにします。Kiwi Syslog Daemon はログを保存しているドライブのディスクスペースをチェックし、空きエリアの割合が閾値より低ければPIXに対するTCP接続を切断します。Kiwi Syslog DaemonがPIXからの接続要求を再度受け付けるようになるまで、PIXはこれ以上トラフィックを送れなくなります。空きディスクの割合が閾値を越えればすぐにPIXからのログメッセージを受け付け、トラフィックは再び流れ始めます。

警告: ディスクチェックを有効にし、ディスク使用量が閾値に達すると、すべてのPIXトラフィックがストップします。すなわちユーザーのインターネットアクセスができなくなります。インターネットアクセスよりログの整合性が重要な場合だけこのオプションを有効にしてください。

3.12.7 Inputs - Keep-alive (入力 - キープアライブ)

キープアライブメッセージの動作

キープアライブメッセージは等間隔でsyslog受信ストリームに挿入されます。これらはスクリプトアクションのトリガーとして、または等間隔でログファイルにスタンプするために使われます。

キープアライブメッセージは他の受信メッセージと同等に扱われ rule エンジンで処理されます。Rule 設定によりますが、メッセージはディスクに書かれ、表示され、他のsyslogサーバーに転送されます。

キープアライブメッセージが他のsyslogサーバーに転送される時、“I am still alive and well” メッセージとして他のサーバーにすべて順調であることを知らせます。リモートサーバーではキープアライブメッセージの喪失を検出し必要に応じてアラームを送信するフィルターを設定することができます。

挿入されるメッセージのプロパティは Facility、Level、ホストIPアドレス、メッセージテキストを指定することによって変更できます。

キープアライブメッセージはスクリプトで varInputSource フィールドをチェックし検出することができます。キープアライブメッセージは “3” を使用します。

Enable keep-alive messages:

デフォルトは無効です。キープアライブメッセージを挿入するにはチェックボックスをオンにしてください。

Frequency:

入力ストリームに挿入するキープアライブメッセージの頻度を設定します。デフォルトは60秒に1回ですが1 ~ 86400秒 (1日) の範囲で任意の値を指定できます。

Syslog facility:

キープアライブメッセージのファシリティを設定します。このファシリティのみで動作するようルールのパライオリティフィルターを設定することができます。通常このオプションはSyslogプログラムがメッセージを生成していることを示す Syslog に設定します。

Syslog level:

キープアライブメッセージのレベルを設定します。このファシリティ/レベルの組み合わせでのみ動作するようルールのパライオリティフィルターを設定することができます。通常このオプションは情報メッセージであることを示す info に設定します。

From IP Address:

キープアライブメッセージの送信元IPアドレスを設定します。1.1.1.1 ~ 255.255.255.255 の範囲で任意の値を設定できます。デフォルトは 127.0.0.1 にしてください。指定したアドレスはルール設定のフィルター対象となります。

Message text:

キープアライブメッセージのテキストを入力します。任意の文字列が可能です。デフォルトはKeep-alive message です。

キープアライブメッセージの使用方法:

スクリプト目的での利用

通常Rules/Filters アクションはメッセージが到着した時とルールエンジンが処理する時だけ実行されます。時間でアクションを実行する時はキープアライブメッセージをルールエンジンのトリガーとして使えます。

Rules

Rule: MyScript

Filters

Priority: Match Syslog.Info only

Actions

Action: Run script

Action: Stop processing (Exits the rule engine here)

Other Rules here...

キープアライブメッセージはスクリプトで varInputSource フィールドをチェックし検出することができます。キープアライブメッセージは “3” を使用します。

ビーコンとして他のホストに転送

キープアライブメッセージは他のホストにすべて順調であることを知らせるために、転送することができます。

Rules

Rule: Send keep alive message

Filters

Priority: Match Syslog.Info only

Actions

Action: Forward to host (send to another host via a syslog message)

Action: Stop processing (Exits the rule engine here)

Other Rules here...

Stop processing アクションを使用していますので、キープアライブメッセージはこれ以降のルールには見えません。プライオリティフィルターは Syslog.info に一致したらアクション(forward message)を実行、次に rule エンジンがメッセージを破棄し次のメッセージの受信を待ちます。

3.13 Setup – Display (設定 – 表示)

3.13.1 Display window is always on top of others (常に最前面に表示)

Kiwi Syslog Daemon が常に最前面のウィンドウとして表示されます。

3.13.2 Number of display rows (表示行数)

スクロールして表示する行数を設定します。

通常は40行に設定します(メッセージが全画面表示されます)。

フリーウェア版では10～50行の範囲で指定できます。

正規登録版では5～1000行の範囲で指定できます。

注: スクロール行数を多くすると画面を更新するときに時間がかかります。

新しいメッセージが表示されると、すべての表示メッセージの並べ替えが行われ最終行のメッセージが切り捨てられます。この動作はCPUを消費するため、並べ替える行が多ければ多いほど多くのCPUが使われるため長い時間がかかります。

3.13.3 Minimize to System Tray on start-up (起動時にシステムトレイに最小化)

Kiwi Syslog Daemon の起動時にシステムトレイにアイコンを最小化します。

Kiwi Syslog Daemon をWindowsのスタートアップと同時に起動し邪魔にならないようシステムトレイに置いておきたいときに有効です。

3.13.4 Use 3D text in display heddings (3Dタイトルを使用)

Kiwi Syslog Daemonのメイン画面と Setup 画面のタイトルに3Dテキスト(影付き)を使います。

3.13.5 Use MM/DD/YYYY date format (日付をMM/DD/YYで表示)

US日付フォーマットmm-dd-yyyyを使用します。

ここで指定した日付フォーマットは表示するときのみ適用されます。ログファイルに記録されている日付フォーマットはロギングフォーマットで設定した形式となります。

3.13.6 Show messages per hour in title bar (タイトルバーに1時間の受信メッセージ数を表示)

アクティブであるときに1時間のうちに受信したメッセージ数をタイトルバーに表示します。

3.13.7 Blink System Tray Icon when receiving messages (メッセージ受信時にアイコンを点滅)

システムトレイにアイコンで最小化している場合でもメッセージの受信が目で見えて分かるようにします。

メッセージを受信すると最小化したシステムトレイアイコンが青と緑で点滅します。

3.13.8 Word wrap long message text(長いテキストを折り返す)

Kiwi Syslog Daemonのウィンドウサイズを超えるような長いメッセージを受信したときにテキストを折り返してスクロールせずに読めるようにします。

3.13.9 Adjust column widths automatically (列幅の自動調整)

メッセージを受信するとテキストに合わせて列幅を自動的に調節します。

テキストが読み易くなります。多くのテキストを読みたいときはフォントサイズを小さくできます。View メニューの Choose font オプションで設定してください。

3.14 テストボタンの動作

Test ボタンを押すと、Test Setup ページの各フィールドに設定されている値を使ってsyslogメッセージがフィルタあるいはアクションに渡されます。

フィルターのテストを行うとき、フィルター対象のフィールドの値にマッチするものがない場合は[Test]ボタンの隣に赤のチェックマークが表示されます。

これを修正するには Test ボタンの隣の Test Setup ボタンを押します。Test message ページが開き、Test ボタンを押したときにフィルターまたはアクションに渡される値がすべて表示されます。

Test ボタンに緑色のチェックマークを表示するには、テスト対象のフィールドの値をフィルターが true を返すよう変更する必要があります。Test message ページでマッチ対象のフィールドに入力されている値をフィルターでマッチする値に変更します。変更後は Test ボタンが押せるようになっており、緑色のチェックマークが表示されているはずですが。

アクションのテストを行うときは Test message ページのフィールドに入力されている値はすべてsyslogメッセージの形式で送信されます。アクションが成功すると緑色のチェックマークが表示されます。何らかの問題が起きて失敗したときは赤のチェックマークが表示されます。

作成したフィルターやアクションの設定をテストするには下記のWebページからKiwi SyslogGenをダウンロードしてください。このプログラムはKiwi Syslog Daemonにテスト用のsyslogメッセージを送ることができます。この方法がルールのテストには最も適しています。

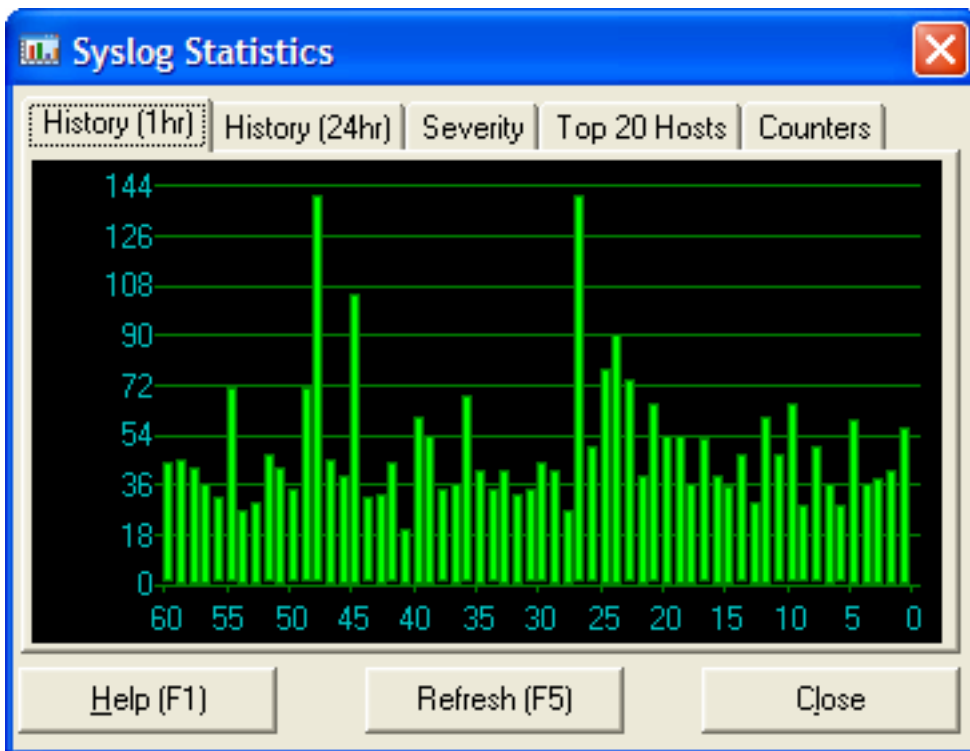
<http://www.kiwisyslog.com/downloads>

4 Syslog statistics window (syslog統計ウィンドウ)

4.1 Syslog statistics window (Syslog 統計ウィンドウ)

Kiwi Syslog Daemonのメイン画面の View メニューから View Syslog Statistics を選択する、もしくは [Ctrl] + [S] を押します。

下図のような Syslog Statistics ウィンドウが開きます。



syslog統計は10秒ごとに更新されます。Refresh ボタンまたは [F5] キーを押すとすぐに更新されます。

4.2 History [1hr] (1時間の受信履歴)

直近60分間のトラフィックを棒グラフで表示します。各々の棒が示しているのは1分間の受信メッセージ数です。グラフは右から左に進みます。すなわち、チャートの左端に1時間前のトラフィックが表示され、右端の棒は現在のトラフィックを示しています。

4.3 History [24hr] (24時間の受信履歴)

直近24時間のトラフィックを棒グラフで表示します。各々の棒が示しているのは1時間ごとの受信メッセージ数です。グラフは右から左に進みます。すなわち、チャートの左端に24時間前のトラフィックが表示され、右端の棒は現在のトラフィックを示しています。

4.4 Severity (重要度)

プライオリティレベル別のメッセージ分析結果を表示します。最も緊急を要するレベルである0-Emergency から問題解決用の7-Debug まで重要度の高い順に上から下へ列記されています。

テーブルにはメッセージ数と全トラフィックに対する割合が示されています。

任意の列のヘッダーをクリックするとその列を軸として並べ替えられます。もう一度クリックすると元に戻ります。

4.5 Top 20 Hosts (上位20ホスト)

送信ホスト別のメッセージ分析結果を表示します。テーブルにはホストごとのメッセージ数と全体に対する割合が示されています。

任意の列のヘッダーをクリックするとその列を軸として並べ替えられます。もう一度クリックすると元に戻ります。

特定ホストから大量のトラフィックが発生している、あるいはパターンが変化している場合、そのデバイスに問題があることを示しています。

4.6 Counters (カウンター)

トラフィックとエラーの統計を表示します。Messages-Average (平均メッセージ数)カウンターはアラーム通知の閾値を設定するときや、どのくらいのsyslogがあるのかを予測するのに役立ちます。

カウンターは(現在の時刻からの)直近24時間の値を表示するものと深夜(0:00)からの値を表示するものがあります。

1時間はプログラム起動時を0とし、実際のHH:MM:SSフォーマットの時刻とは関係ありません。プログラム実行時間はProgram up-time カウンターに示されています

Messages - Total:

プログラムスタート時からの受信メッセージ数です。この値はプログラムがサービスのリスタートでリセットされます。

Messages - Last hour:

直近1時間の受信メッセージ数です。時間はプログラムスタート時からカウントされます。プログラム実行が60分以内であればこの値は0となります。1時間経過していれば、最終の1時間経過後の受信メッセージ総数が表示されます。この値は次の1時間が経過するまで更新されません。

Messages - This hour:

直近1時間以内に受信したメッセージ数です。時間はプログラムスタート時からカウントされます。この値は1時間経過するたびに0にリセットされ、新しいメッセージを受信すると更新されます。

Messages - Last 24 hours:

直近24時間(現在を基準に)の受信メッセージ数です。この値は直近23時間の受信メッセージの合計と直近1時間内に受信したメッセージの総数です。時間が切り替わると、それまでの23時間の値が再計算され既存の値は捨てられます。この値は直近1時間以内にメッセージを受信するたびに再計算されます。計算式は次のようになります。

LastHours(1 ~ 23) + messages this hour

Messages - Average:

直近24時間における1時間あたりの平均受信メッセージ数です。時間が切り替わるたびに再計算されます。最初の1時間が経過した後、1時間おきに更新されます。

Messages - Forwarded:

Forward message アクションで他のsyslogコレクタに転送/リレーされたメッセージの数です。このカウンターは日別統計が送信されるとすぐにリセットされます。日別統計は通常深夜に送信されるため、値は深夜0:00からのカウントになります。

Messages - logged to disk:

Log to file アクションでディスクに記録されたメッセージ数です。このカウンターは日別統計の送信後すぐにリセットされます。日別統計は通常深夜に送信されるため、値は深夜0:00からのカウントになります。

Errors - logged to disk:

ディスクに記録されたプログラム内部のエラー数です。エラーの原因はログファイルへのアクセス不能あるいはプログラム内部エラーにあります。このカウンターは日別統計の送信後すぐにリセットされます。日別統計は通常深夜に送信されるため、値は深夜0:00からのカウントになります。0以外の値が表示されている場合はエラーログ(View | Error log メニュー)を参照してください。

Disk space remaining:

ディスクスペースの残量をMBで示します。監視するドライブは Alarms の Disk space monitor 設定オプションで設定できます。デフォルト設定は C ドライブです。

CustomStats:

カスタム統計値は Counters タブに表示されています。これらの値は Run Script アクションで変更できます。これらのカスタム統計カウンターを利用することで、任意の値をカウントし表示することが可能です。

カウンター名を分かりやすい名前にするには、Setup 画面の Scripting オプションでカウンター名と初期値を設定できます。

5 Kiwi Syslog Daemon サービス版

5.1 Kiwi Syslog Daemon サービス版のシステム要件

Kiwi Syslog DaemonをWindows NTのサービスとしてインストールする場合の推奨要件は以下のとおりです。

- Windows NT4 (SP4以上) / Windows 2000 / Windows XP Professional / Windows 2003 Server
- Microsoft Internet Explorer Version 5.x 以上
- RAM 128MB 以上
- 解像度 800 x 600, 256 色以上のディスプレイ

5.2 Installing the Service edition (サービス版をインストールする)

NTサービスとしてKiwi Syslog Daemonをインストールするには注意が必要です。

新しいバージョンをインストールする前に、必ず既にインストールされているKiwi Syslog Daemonを停止しアンインストールしてください。

インストールは installation .exe をダブルクリックして開始します。

セットアッププログラムによりKiwi Syslog Daemon Service Managerがインストールされます。

インストール完了後、[スタート]メニューからプログラムを起動します。Kiwi Syslog Daemonのメイン画面が表示されます。

Manage メニューでNTサービスを管理します。

サービスのインストールは Manage から Install the Syslogd Service を選択して実行します。

インストールが成功したか失敗したかを示すメッセージが表示されます。

失敗した場合、すでに他のバージョンのKiwi Syslog Daemonがインストールされていた可能性があります。

サービスを手動でインストールするには、[スタート]メニューから [ファイル名を指定して実行] またはコマンドプロンプトを呼び出し、次のように入力します。

C:\Program files\Syslogd\Syslogd_Service.exe -install

サービスをアンインストールするには -uninstall スイッチを使って次のように入力します。

C:\Program files\Syslogd\Syslogd_Service.exe -uninstall

サービスがインストールされたら、それを開始する必要があります。

NTを再起動するとサービスは自動的に開始されます。手動で開始させるには Manage から Start the Syslogd service を選択するか [Ctrl]+[F3] を押します。

コマンドラインを使ってサービスを手動で開始するには、次のように入力します。

C:\>net start "Kiwi Syslog daemon"

次のように表示されます。

The Kiwi Syslog Daemon service is starting.

The Kiwi Syslog Daemon service was started successfully.

コマンドラインを使ってサービスを手動で停止するには、次のように入力します。

C:\>net stop "Kiwi Syslog Daemon"

次のように表示されます。

The Kiwi Syslog Daemon service is stopping.

The Kiwi Syslog Daemon service was stopped successfully.

注: サービスが停止するまで約20秒かかります。

[コントロールパネル] の [サービス] でNTサービスの管理と設定ができます。

サービスをインストールし、開始したら、Pingでオペレーションのテストが可能です。

Manage の Ping the Syslogd service を選択します。

サービスがSyslogメッセージを受信しているかどうかテストするには、[Ctrl]+[T] を押します。localhost にテストメッセージが送信されます。

次のように表示されます。

Kiwi Syslog Daemon - Test message number 0001

上記のメッセージが表示されないときは、File の Properties から Display で確認します。

5.3 サービス版を管理する

Kiwi Syslog Daemon Service Manager から Syslogd サービスの管理とコントロールができます。

Manage メニューの項を参照してください。

5.4 サービス版の問題を解決する

うまく動作しないときは次のことを確認してください。 -

1). サービスにPingできるか？

Manage の Ping Syslogd service を選択します。

2). 自分自身へのテストメッセージ送信と受信はOKか？

Syslog Service Manager から [Ctrl]+[T] を押してテストメッセージを localhost に送信してください。

3). ローカルマシンからメッセージを送信してみる。

テストメッセージの送信には、次のWebページから Kiwi SyslogGen をダウンロードご利用ください。

<http://www.kiwisyslog.com/>

5.5 Kiwi Syslog Daemon NT Service のアップグレード

5.5.1 Kiwi Syslog Daemon NT Service のアップグレード

Kiwi Syslog Daemon の新バージョンがリリースされたときは、最新機能やバグの修正が含まれているため、できるだけアップグレードしてください。

最新バージョンのKiwi Syslog Daemonは次のWebページから入手できます。

<http://www.jtc-i.co.jp>

<http://www.kiwisyslog.com/>

アップグレードを実行する前に、必ず現在インストールされているバージョンのプログラムを削除してください。

5.5.2 現在インストールされているプログラムを削除する

1). Service Manager からサービスを停止します。

Manage の Stop the Syslogd service を選択します。

2). Service Manager でサービスをアンインストールします。

Manage の Uninstall the Syslogd service メニューを選択します。

3). Service Manager プログラムを終了させます。

4). [コントロールパネル] の [アプリケーションの追加と削除] からアプリケーションをアンインストールします。

5.5.3 新バージョンをインストールする

1). Kiwi Syslog Daemon NTサービス版の最新バージョンをダウンロードします。

2). 新バージョンをインストールします。

3). [スタート] メニューから Syslogd Service Manager を起動します。

[スタート]、[プログラム]、[Kiwi Syslog Daemon]、[Kiwi Syslog Daemon Service Manager] を選択します。

4). デフォルトのアクション設定を使用するかどうかの確認画面で [Yes] または [No] を選びます。

以前の設定をそのまま使う時は [No] を選びます。

5). Syslogd Service をインストールします。

Manage の Install the Syslogd service を選択します。

6). Syslogd Service を開始します

Manage の Start the Syslogd service を選択します。

7). サービスにpingを送って新しいサービスがきちんとインストールされているかどうかチェックします。
Manage の Ping the Syslog service を選択します。

8). メッセージ受信が正常かチェックします。
[Ctrl]+[T] を押して localhost にテストメッセージを送信します。

6 syslog 送信デバイスの設定

本章ではsyslogメッセージ送信機能を使用するためのネットワーク機器の設定について個別に解説します。

本書に記載されていないsyslogメッセージ送信可能デバイスについての情報をお持ちでしたら、下記までお知らせください。次回のマニュアル更新時に情報を追加させていただきます。
<http://www.kiwisyslog.com/support/>

6.1 SNARE でWindowsイベントログを取得する

Kiwi Syslog Daemon はそのままではWindowsのイベントログを読むことができません。

Windowsイベントログを収集したいときはサードパーティ製アプリケーションを利用する必要があります。お勧めのWindowsイベントログ収集アプリケーションは Snare Agent for Windows です。次のWebページから無料でダウンロードできます。
<http://www.intersectalliance.com/projects/SnareWindows/index.html>

Snare はWindowsのイベントログをsyslogメッセージに変換し Kiwi Syslog Daemon に送信します。この時点でメッセージをテキストファイルやデータベースに書き出すといった通常の方法で処理可能です。

Windows ユーザーのログオン/ログオフイベントを収集するには次のWebページを参照してください。ログオン/ログオフイベントを有効にする方法の例が記載されています。
<http://support.microsoft.com/kb/300549>

Snare Agent for Windows をダウンロードしインストールしたら設定を行う必要があります。デフォルトのウィンドウから Network Configuration を選択します。

1. Destination Snare Server address フィールドにKiwi Syslog DaemonをインストールしたシステムのIPアドレスを入力します。
2. Destination Port はKiwi Syslog Daemonのsyslogメッセージ受信ポートと同じ 514 にします。

下図は Snare Network Configuration の例です。

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	<input type="text"/>
Destination Snare Server address	192.168.1.20
Destination Port	514
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input checked="" type="checkbox"/>
Export Snare Log data to a file?	<input type="checkbox"/>
Enable SYSLOG Header?	<input checked="" type="checkbox"/>
SYSLOG Facility	User
SYSLOG Priority	DYNAMIC

Change Configuration

ResetForm

[Change Configuration] ボタンを押したらWindowsの [コントロールパネル] の [サービス] で Snare サービスを再起動してください。変更が正しく読み込まれます。

Kiwi Syslog Daemonのsyslog受信ポート(514)がWindowsファイアウォールによってブロックされていないことを確認してください。

syslogメッセージの受信に関し問題があるときは次のWebページを参照してください。

<http://www.kiwisyslog.com/kb/info:-kiwi-syslog-daemon-is-not-receiving-messages/>

6.2 3Com NetServer の設定

NetServer 8/16 からSyslogメッセージを送信するための手順

NetServerにTelnetかコンソールケーブルで接続します。
次のように Add Syslog コマンドを入力します。

ADD SYSLOG <IP Address> LOGLEVEL <logging level>

IP address にはKiwi Syslog Daemonを実行しているPCのIPアドレスを入力します。

logging level には次のいずれかを入力します。

COMMON
CRITICAL
DEBUG
UNUSUAL
VERBOSE

例

ADD SYSLOG 10.0.10.23 LOGLEVEL VERBOSE

LIST SYSLOGS コマンドでエントリを表示しsyslogエントリが追加されていることを確認します。

次のように表示されます。

```
Console Prompt>LIST SYSLOGS
SYSLOG SINKS
SysLog          Log Level   Msg Count
192.168.203.203 COMMON     507
192.168.203.230 COMMON     4551
```

必ず **SAVE ALL** コマンドを実行し、詳細をNVRAMに記憶させてください。

6.3 3Com Total Control Chassis の設定

Total Control Chassis からSyslog メッセージを送信するための手順

HiPer Access Router Card (HiPer ARC) にTelnet かコンソールケーブルで接続します。
次のように Add Syslog コマンドを入力します。

ADD SYSLOG <IP Address> FACILITY <Facility> LOGLEVEL <logging level>

IP address にはKiwi Syslog Daemonを実行しているPCのIPアドレスを入力します。

Facility には次のいずれかを入力します。

LOG_AUTH
LOG_LOCAL0
LOG_LOCAL1
LOG_LOCAL2
LOG_LOCAL3
LOG_LOCAL4
LOG_LOCAL5

LOG_LOCAL6
LOG_LOCAL7

Logging level には次のいずれかを入力します。

COMMON
CRITICAL
UNUSUAL
VERBOSE

例

ADD SYSLOG 10.0.10.23 FACILITY LOG_LOCAL7 LOGLEVEL VERBOSE

LIST SYSLOGS コマンドでエントリーを表示しsyslogエントリーが追加されていることを確認します。

次のように表示されます。

```
Console Prompt>LIST SYSLOGS
SYSLOG SINKS
SysLog      Log Level  Msg Count  Facility
192.168.203.203 COMMON    507        LOG_LOCAL7
192.168.203.230 COMMON    4551       LOG_AUTH
```

必ず **SAVE ALL** コマンドを実行し、詳細をNVRAMに記憶させてください。

6.4 Alliant Cellular Gateway の設定

以下の情報を提供してくださった Mark Hamilton 氏に謝意を表明いたします。

Alliant Cellular Gateway の詳細については次のWebページを参照してください。

<http://www.alliantnetworks.com/>

SYSLOG メッセージを有効にしフィルタするための手順

デフォルトではSYSLOGメッセージ送信は無効になっています。SYSLOGサーバーの設定作業が終わったら、SYSLOGメッセージを有効にしなければなりません。メッセージのフィルタリングを設定して出力するメッセージタイプを制限することもできます。

必要な情報

- SYSLOGサーバーのIPアドレス
- ゲートウェイの管理者パスワード(デフォルトのパスワードは: public)
- Telnet CLIを使うのであれば、ゲートウェイのIPアドレス
- シリアルCLIを使うのであれば、ゲートウェイに接続するためのシリアルケーブル

次の手順でSYSLOGメッセージを有効にしフィルターします。

1. シリアルまたはTelnetでCLIにアクセスします。
2. 次のコマンドを入力してください。

```
CG> login <password>
CG# configure system
CG(sys)# configure syslog
CG(sys-sys)# set status on
```

3. コマンドの効果は、show log コマンドで表示して確認します。

出力例:

```
SYSLOG messages are enabled
First SYSLOG server's IP address: 10.0.1.2
Second SYSLOG server's IP address: 0.0.0.0
Severity threshold 6
CG(sys)#
```

4. severity でメッセージをフィルターすると有効です。下記は error 以下のレベルのメッセージはすべて除外し、errorイベント(severity は3) と error 以上のイベントを出力する場合の例です。

```
CG> login <password>
```

```
CG# configure system
Maintenance Onboard logging
CG(sys)# configure syslog
CG(sys-sys)# set status on
CG(sys-sys)# set severity 3
```

6.5 Allied Telesyn ルーターの設定

以下の情報を提供して下さった Allied Telesyn New Zealand の Taylor Wilkens 氏に謝意を表明いたします。

syslog daemon にログ出力を送信するための定義を作成できます。次のコマンドを入力してください。

```
create log output=1 destination=syslog server=address
```

address にはKiwi Syslog Daemonを実行しているホストのIPアドレスを入力します。

この出力定義を作成したら、どんな種類のログメッセージを送信するかを決めるフィルターを追加します。例えば、IPトラフィックフィルターで生成されたメッセージを送信する場合、次のコマンドを入力します。

```
add log output=1 type=IPFILT
```

ISDNコールの時間を記録するコマンド:

```
add log output=1 mod=ICC type=CALL subtype=DOWN
```

すべてのイベントを表示するフィルターを追加するコマンド:

```
add log output=1 filter=1 all
```

フレームアップ/ダウンやlmiのステータス等のインターフェイスイベントのみを記録するコマンド:

```
add log output=1 filter=1 type=vint
add log output=1 filter=1 type=dlink
```

使用可能なログコマンドの詳細については、次のWeb公開資料を参照してください。

<http://www.alliedtelesyn.co.nz/documentation/arrouter/241/pdf/log.pdf>

6.6 Arris Cable Modem Termination System の設定

以下の情報を提供して下さったDale Hutchinson氏に謝意を表明いたします。

Kiwi Syslog daemon を Arris CMTS1000 DOCSIS 1.0 Cable Modem Termination System とCMTS1500 DOCSIS 1.1 Cable Modem Termination Systemで使うコンソールコマンドは以下のとおりです。

```
manage
event-level
syslog-ip-addr xxx.xxx.xxx.xxx // Kiwi Syslog Daemon サーバーのIPアドレス
admin-status-of-throttle unconstrained
```

6.7 Extreme Summit スイッチの設定

スイッチにTelnetあるいはコンソールケーブルで接続し、管理者(admin)レベルユーザーでログインします。

configにsyslogサーバーエントリーを追加するには次のように入力します。

```
Configure syslog add <IP address of syslog server> <Facility name>
```

例: Configure syslog add 192.168.1.1 local0

configからsyslogサーバーエントリーを削除するには次のように入力します。

```
Configure syslog delete <IP address of syslog server> <Facility name>
```

例: Configure syslog delete 192.168.1.1 local0

CLI コンフィグレーションコマンドのロギングを有効にするには次のように入力します。

```
enable cli-config-logging
```

6.8 Barracuda Spam Firewall の設定

以下の情報は Barracuda Spam Firewall マニュアルの概要です。

詳細については次のWebページを参照してください。

<http://www.barracudanetworks.com/ns/support/documentation.php>

Barracudaのsyslogとその抽出方法

Barracudaではsyslogメッセージを Barracuda Spam Firewall がメッセージを処理するたびにその内容を記録する手段として利用しています。syslogメッセージはSpam Firewallに送られテキストファイルとして保存されます。同時にBarracuda管理者が管理可能なリモートサーバーにも送られます。この送られてきたsyslogメッセージを管理者は解析を実行してレポートを作成したり、Barracuda Spam Firewallが行った処理内容をより深く理解することができます。

syslogを有効にするには Web GUI の Advanced から Syslog を選択し、メッセージ転送先のsyslogサーバーのIPアドレスを入力します。

注: Web GUI の画面上にはsyslog通知に関する項目がありますが、本書では解説しておりません。

syslogメッセージは標準syslogポートであるUDP 514ポートに送信されます。Barracudaとsyslogメッセージの受信サーバー間にファイアウォールが設置されている場合には、必ずファイアウォールのポート514が開いていることを確認してください。受信時のsyslogメッセージのファシリティはmail、プライオリティレベルはdebugです。Barracuda製品内部ではsyslogメッセージを独自の方式でロギングするため、ファシリティやプライオリティレベルを変更することはできません。

BarracudaのSyslogフォーマット

Barracuda Spam Firewall は以下に挙げるような形式でsyslogメッセージを送信します。メッセージに対して何らかのアクションが起こるとsyslogに記録されます。複数の受信者にメッセージを送信している場合は受信者ごとに個別のログファイルが作成されます。syslogの実装方法は様々ですがそのすべてが以下と全く同じ形式で表示されるわけではありません。しかし、syslogメッセージの行には表示されていない項目も含まれています。ここで挙げる例はsyslogメッセージ行のメイン部分です。

```
Timestamp Host Barracuda Process Client IP Message ID Start End Service Info
Sep 8 17:38:48 dev1 inbound/pass1[27564]: XX.XX.XX.XX 1126226282-27564-2-0 1126226286
1126226328 RECV [ . . . . ]
```

6.9 Bay Networks デバイスの設定

以下の情報はBay Networks社のWebページからの抜粋です。

詳細については次のWebページを参照してください。

<http://support.baynetworks.com/library/tpubs/html/switches/bstream/115412A/MARKER-2-455>

ルーターのSyslog設定

Technician Interface コマンドを使ってルーターのsyslog設定を行うことができます。syslogは一連のタスクとして設定し、そのタスクの一部には1つまたは複数の番号が振られたステップが含まれています。

ルーターでsyslogを設定するのに必要な作業の概要は以下のとおりです。

1. ルーターに接続したコンソールから、あるいはルーターにTelnetで接続し、Technician Interface セッションを開く。
2. ルーターにSyslogをロードするためのスロットマスク(スロットマップ)を定義する。
3. ルーターにsyslogエンティティを生成する。
4. syslogグローバル属性を設定する。
5. syslogホストテーブルにリモートホストを追加する。
6. syslogエンティティフィルターテーブルにエンティティフィルターを追加する。
7. 5、6の手順を繰り返してリモートホストとエンティティフィルターを追加する。追加するリモートホストもエンティティフィルターもない場合は8へ進みます。
8. 設定に加えられた変更をNVFSボリューム上にあるファイルに保存する。
9. Technician Interface セッションを終了する。

syslog設定手順の詳細について以下で(作業ごとに順番に)解説します。設定手順の後にsyslog設定の例とsyslog属性の定義例を記載します。

作業1: ルーターに接続したコンソールから、あるいはルーターにTelnetで接続し、Technician Interface セッションを開く。
Bay Networksルーターの Technician Interface セッションのオープンの詳細は第1章を参照してください。

作業2: ルーターにsyslogをロードするためのスロットマスク(スロットマップ)を定義する。

ルーターにsyslogエンティティを生成する前にsyslogスロットマスクを定義します。スロットマスクはシステムがsyslogエンティティをロードし実行するスロットを特定します。Technician Interface プロンプトで、下記のように入力します。

```
$: set wfProtocols.wfSYSSLoad.0 0x7FFE0000;commit
```

このコマンドはルーターモデルに関係なくすべてのスロット上でのsyslog実行を有効にします。

次に、ルーターのsyslog エンティティを作成します。

作業3: ルーターにsyslogエンティティを生成する。

次のようにルーター設定でsyslog エンティティを生成します。

```
set wfSyslog.wfSyslogDelete.0 1;commit
```

これはルーターのsyslogも有効にします(システムはsyslogベースレコードの属性wfSyslogDisable, OID = 1.3.6.1.4.1.18.3.3.2.15.1.2 を1にします)。

次に、syslog グローバル属性を設定します。

作業4: syslog グローバル属性を設定する。

ルーター上でのsyslog生成を有効にすると、wfSyslogMaxHosts と wfSyslogPollTimer 属性に対するデフォルト値をそのまま使うことも、カスタマイズすることもできます。syslogグローバル属性のデフォルト値をそのまま使用する場合は、作業5へ進みます。それ以外は次の手順を実行してください。

1. ルーターのsyslogでサポートするアクティブホストの最大数を設定します。

```
$: set wfSyslog.wfSyslogMaxHosts.0 <1 - 10>;commit
```

wfSyslogMaxHosts のデフォルト設定は5です。設定されている最大数を超過してsyslogホストテーブルにエントリを追加することは可能ですが、syslogメッセージは最初の n 個のアクティブホストに対してのみ転送されます。n = wfSyslogMaxHostsの値です。

2. ルーターのsyslogポーリングサイクルの間隔(秒)を設定します

```
$: set wfSyslog.wfSyslogPollTimer.0 <5 - 610000>;commit
```

wfSyslogPollTimer のデフォルト値は5 秒です。

次に、syslogホストテーブルにリモートホストを追加します。

作業5: syslog ホストテーブルにリモートホストを追加する。

ネットワーク内に設置されているルーター上でsyslog(イベント)メッセージを受信するリモートホストを定義します。

syslogホストテーブルへの初めての登録の場合は下記の手順1へ進みます。初めてではない場合はまず、ルーターで設定済みのホストの一覧を表示できます。syslogホストテーブルへ登録済みのエントリを表示するには、Technician Interface プロンプトで次のコマンドを入力します。

```
list -i wfSyslogHostEntry
```

リストには、現在syslogホストテーブルに定義されているすべてのインスタンスID(この場合はIPアドレス)が記載されています。

1. 次のように入力してsyslogホストテーブルに新しいホストエントリを追加します。

```
$: set wfSyslogHostTable.wfSyslogHostDelete.<host_IP_address> 1 $: commit
```

送信先として指定したIPアドレスのリモートホストにsyslog情報を送信します。

ホスト属性wfSyslogHostLogFacility (184 = Local7)と wfSyslogHostTimeSeqEnable(2 = disabled) のデフォルト設定を使用する場合は作業6へ進みます。それ以外は2に進んでこれらの属性をカスタマイズします。

2. ルーターからsyslogメッセージを受信するUNIXシステムのファシリティを定義するには、次のコマンドを入力します。

```
$: set wfSyslogHostTable.wfSyslogHostLogFacility.<host_IP_address>  
<128|136|144|152|160|168|176|184>;commit
```

128 = local0 160 = local4

136 = local1 168 = local5

144 = local2 176 = local6

152 = local3 184 = local7

3. リモートホストのsyslogメッセージタイムシーケンシングを有効にするには、次のように入力します(任意)。

```
$: set wfSyslogHostTable.wfSyslogHostTimeSeqEnable.  
<host_IP_address> 1;commit
```

注: エントリが有効で(wfSyslogHostDisable = 1)アクティブ(wfSyslogHostOperState = 1)なりリモートホストのみがルーターのsyslogからメッセージを受信します。

次に、追加したホストエントリに対するエンティティフィルターを追加します。

作業6: リモートホストにエンティティフィルターを追加する。

syslogホストテーブルにホストを定義したら、ホストにエンティティ固有のメッセージフィルターを追加(定義)します。

エンティティとリモートホストの組み合わせに対して初めてフィルターを適用する場合以外は、まず、次のように入力してフィルターインスタンスリストを表示してください。

```
list -i wfSyslogEntFiltrEntry
```

表示されたインスタンスIDリスト(フォーマットは<host_IP_address>.<entity_code>.<filter_index>)から、追加した<host_IP_address>と<entity_code>の組み合わせに適用する新しいフィルターに割り当てる< filter_index>番号を決定します。新しいフィルターに割り当てる番号はリストに記載されている<filter_index>の最大値に1を加えた値となります。新しいフィルター番号を確認したら、1に進みます。

1. 任意のエンティティとリモートホストの組み合わせに適用する新しいフィルターを作成します。次のように入力して、まず syslog エンティティフィルターテーブルにエントリを作成します。
\$: set WfSyslogEntityFilterTable.WfSyslogEntFltrDelete.
<host_IP_address>.<entity_code>.<filter_index> 1;commit
<host_IP_address>にはリモートホスト(管理用ワークステーション)のIPアドレスを入力します。
<entity_code>には<host_IP_address>のリモートホストへイベントメッセージを転送するソフトウェアエンティティを入力します。
<filter_index>には選択したエンティティとリモートホストの組み合わせにフィルターをアサインするための番号を入力します。
2. 特定のホストのエンティティフィルターを作成したら、次について定義します。
 - イベント番号(または範囲)とスロット番号(または範囲)または
 - セベリティマスクとスロット番号(または範囲)

注: フィルターはイベントとスロット番号、またはセベリティマスクとスロット番号を定義するまで動作しません。次の手順に従ってエンティティフィルター属性の設定を行います。

- a. **イベント番号別に定義**して、イベントメッセージをsyslogで選択し特定のリモートホストに送信するには、次のように入力します。
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtLowBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 255>
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtUppBnd
<host_IP_address>.<entity_code>.<filter_index> <0 - 255>
\$: commit
イベント番号によるフィルタリングを定義したくない場合は、イベント番号の下限と上限のデフォルト値である 0 と255を使用してください(2bへ進みます)。デフォルト値を使用する場合、メッセージの選択と転送を行うときの条件としてセベリティとスロットマスクのみが適用されます。
- b. イベント番号(または範囲)が未定義のときに限りセベリティマスクを定義します。イベント番号や範囲が定義済みである場合、syslogはこのフィルターのセベリティマスクを無視します。
セベリティレベル別に定義して、イベントメッセージをsyslogで選択し特定のリモートホストに送信するには、次のように入力します
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSevMask.
<host_IP_address>.<entity_code>.<filter_index> "<fwitd>"
\$: commit
- c. **スロット番号別に定義**して、イベントメッセージをsyslogで選択し特定のリモートホストに送信するには、次のように入力します。
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowUpp.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>
\$: commit

注: 有効なスロット番号の下限と上限はそれぞれ0と14ですが、設定しようとしているルーターモデルの実際のスロット番号の範囲の値を指定してください。実際の値以外の値を設定すると、フィルターは実行状態になりません。

3. ルーターイベントメッセージのセベリティレベルとUNIXシステムのエラーレベルをマッピングします。
ほとんどの場合、デフォルト設定を使用して作業7へ進んで構いません。設定を変更する場合は、次の手順に従ってメッセージマッピングをカスタマイズします。
Technician Interface プロンプトで、変更するメッセージマッピングのためのコマンドを入力します。
- a. 次のように入力してルーターの FAULT メッセージのマッピングを変更します。
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrFaultMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
wfSyslogEntFltrFaultMap のデフォルト値は3であり、ルーターの FAULT レベルメッセージをUNIXシステムレベルが CRIT のメッセージにマッピングします。
- b. 次のように入力してルーターの WARNING メッセージのマッピングを変更します。
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
wfSyslogEntFltrWarningMap のデフォルト値は5であり、ルーターの WARNING レベルメッセージをUNIXシステムレベルが WARNING のメッセージにマッピングします。
例:
\$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap 5

このコマンドは Warning レベルのルーターイベントメッセージをそれぞれ Warning レベルのUNIXシステムエラーメッセージにマッピングします。

- c. 次のように入力してルーターの INFO メッセージのマッピングを変更します。

```
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrInfoMap.
```

```
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

wfSyslogEntFiltrInfoMap のデフォルト値は7であり、ルーターの INFO レベルメッセージをUNIXシステムレベルがINFO のメッセージにマッピングします。

- d. 次のように入力してルーターの TRACE メッセージのマッピングを変更します。

```
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrTraceMap.
```

```
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

wfSyslogEntFiltrTraceMap のデフォルト値は3であり、ルーターの TRACE レベルメッセージをUNIXシステムレベルがCRIT のメッセージにマッピングします。

- e. 次のように入力してルーターの DEBUG メッセージのマッピングを変更します。

```
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrDebugMap.
```

```
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

wfSyslogEntFiltrDebugMap のデフォルト値は8であり、ルーターの DEBUG レベルメッセージをUNIX システムレベルがDEBUG のメッセージにマッピングします。

作業7: ホストまたはエンティティフィルターの追加を続ける。

syslog設定にホストやエンティティフィルターをさらに追加する場合は次の手順に従ってください。

1. このリモートホストへのエンティティフィルターの追加を完了し別のリモートホストを追加しない場合は作業8へ進みます。追加する場合は2へ進みます。
2. **今までと同じリモートホストへもう一つエンティティフィルターを追加したい場合は作業6に戻ります。**別のリモートホストを追加する場合は3へ進みます。
3. ルーターからsyslogメッセージを受信する別のリモートホストを追加するには作業5へ戻ります。

作業8: ルーターのSyslog設定を保存する。

次のように入力してsyslog設定に加えられた変更をNVFSボリューム上にあるファイルに保存します。

```
save config <vol>:<filename>
```

作業9: Technician Interface からログアウトする。

Technician Interface コマンドラインインターフェイスから次のコマンドを入力します

```
$: logout
```

6.10 Bintech アクセスルーターの設定

以下の情報を提供して下さったTorsten Richter氏に謝意を表明いたします。

詳細についてはBintech社のWebページを参照してください。

<http://www.bintec.net/en/index.php>

コマンドラインインターフェイス設定:

- ルーターにTelnetで接続
- ゴール - (input / action)
- このセッションのタイムアウトをオフにする- (t 0 と入力)
- setup を開く - (setup と入力)
- 選択 - (SYSTEM を選択)
- 選択 - (External System Logging を選択)
- 選択- (ADD を選択)
- フィールド: Log Host - (Kiwi Syslog Daemonマシンの [IPアドレスまたはホスト名])
- フィールド: Level - (スペースとタブで選択)
- フィールド: facility - (スペースとタブで選択)
- フィールド: Type - (スペースとタブで選択)
- フィールド: Timestamp - (スペースとタブで選択)
- セーブ- (save)
- setup tool/systemを終了 - (exit)
- setup tool を終了- (save)
- 保存して終了 - (Save as boot configuration and exit を選択)

6.11 Buffalo エアステーションルーターの設定

以下の情報はBuffalo エアステーションのユーザーマニュアルからの抜粋です。

詳細は次のWebページで公開されているオンラインマニュアルで確認してください。

<http://buffalo.jp/download/manual/>

設定ガイド

- CDからエアステーションセットアップソフトウェア AirNavigator をインストールします。
- 管理するエアステーションに接続します。
- 左のメニューリストから、Management を選択します。
- ツリーから Syslog Transmitting をクリックします。
- Use を選択してsyslogメッセージ送信を有効にします。
- Kiwi Syslog Daemonを実行するマシンのIPアドレスを入力します。
- Error か Notify を選択しリモートのsyslog daemonに記録するメッセージレベルを指定します。
- Log information からsyslog daemonに送信する特定のレポートを選択します。

6.12 Checkpoint FW-1 ファイアウォールの設定

以下の情報はLogAnalysis フォーラムの投稿を引用しました。

詳細については次のWebページを参照してください。

<http://lists.jammed.com/loganalysis/2001/09/0006.html>

この情報はFirewall-1のUNIXバージョンを前提としています。

Checkpoint コマンド \$FWDIR/bin/fw log -f でCheckpointの固有フォーマットからプレーンテキストに変換できます。次にUNIX の logger ユーティリティでプレーンテキストをsyslogに変換します。fw log -f はすべてのネットワーク接続ログをテキストに変換しますので、ファイアウォールの停止と再起動の度にすべての接続ログがsyslogに変換されます。重複を避けるため、システムの再起動時には毎回ネットワーク接続ログをローテーションしてください。

また、これによって得られるsyslogには、ネットワーク接続ログやホストのOSの標準syslogには含まれていないファイアウォールの稼働状態等の価値ある情報がたくさん含まれています。特に、ファイアウォール管理にGUIを使うと管理者のGUIへのログイン/ログアウト、ファイアウォールへの新しいポリシーの発行などを見ることができます。集中ログサーバーにこれらの情報を記録するには、ファイル\$FWDIR/log/cpmgmt.aud を使って上記の logger を実行する必要があります。

6.13 Cisco 3000 シリーズVPNコンセントレータの設定

Cisco VPN 3000シリーズコンセントレータはsyslogメッセージおよびSNMPトラップの送信をサポートしています。Kiwi Syslog Daemonはどちらも受信できます。

設定手順についてはCisco社のWebサイトを参照してください。

http://www.cisco.com/web/JP/product/hs/security/vpn3000con/prod_literature.html

6.14 Cisco Catalyst スイッチの設定

set コマンドタイプCLIを使うCisco Catalystスイッチで動作します。旧タイプである2900シリーズや5000シリーズのスイッチも対象です。

スイッチへTelnetあるいはコンソールケーブルで接続しイネーブルモードにします。

スイッチのイネーブルプロンプトから次のコマンドを入力します。

Set logging enable

Set logging level all 7 default (すべてのファシリティにdebugレベルが適用されます)

Set logging [Kiwi Syslog Daemon実行マシンのIPアドレスまたはホスト名]

IOSタイプCLIを使う新しいCatalystスイッチの場合は次のコマンドを入力します。

Logging on

logging trap warnings (任意のレベル)

Logging Facility Local7 (またはこのルーターに割り当てる、その他のファシリティ)

Logging <Kiwi Syslog Daemon実行マシンのIPアドレスまたはホスト名>

Catalyst 6000 のロギングについては次のWebページを参照してください。

http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/sw/cat60/65scg2/chapter28/8978_01_28.shtml

および

http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guide_chapter09186a008007e784.html

6.15 Cisco PIX の設定

Cisco PIX ファイアウォールのSyslog メッセージ送信を有効にする

Cisco社の次のWebページを参照してください。

<http://www.cisco.com/JP/support/public/mt/tac/100/1002233/pixsyslog.shtml>

PIXのログメッセージについては下記のWebページを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/63syslog/pixmsgs.htm

http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/sec/pix/slm/chapter02/pixmsgs.html

<http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl>

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>

注:

TCPプロトコルを使ってPIXからsyslogメッセージを送信する場合は、次のコマンドも追加してください。

```
logging permit-hostdown
```

このコマンドにより、シスログサーバーが停止してもトラフィック転送は続けられるようになります。このコマンドを指定しない場合、シスログサーバーのTCP接続が切れると直ちにPIXはトラフィック転送を停止します。

[TCP入力](#)およびKiwi Syslog Daemonでの[PIX使用](#)についての詳細は関連項目を参照してください。

セキュアVPNトンネル経由のPIX SNMPトラップまたはsyslogメッセージ送信については次のWebページを参照してください。

http://www.cisco.com/JP/support/public/mt/tac/100/1000172/pix_vpn_4094.shtml

6.16 Cisco ルーターの設定

ルーターにTelnetあるいはコンソール経由で接続し、イネーブルモードにします。

ルーターのイネーブルプロンプトから次のコマンドを入力します。

Config term

Logging on

```
Logging Facility Local7 (またはこのルーターに割り当てる、その他のファシリティ)
```

```
Logging [Kiwi Syslog Daemon実行マシンのIPアドレスまたはホスト名]
```

```
End
```

この他にIOS v11.2で初めて登場した `logging source-interface` も有用なコマンドです。Cisco社によれば、syslogメッセージにはルーターの出力側インターフェイスのIPアドレスが含まれています。logging source-interface コマンドで、パケットがルーターから送出されるときに使用されたインターフェイスに関わらず、特定のインターフェイスのIPアドレスを含むsyslogパケットを指定することができます。

*一部のIOSバージョンにはバグが存在しますので、必ず `logging source-interface` コマンドを使用してください。このコマンドを使わないと、送信されるsyslogメッセージのUDPチェックサムは不正となり、Kiwi Syslog Daemon が受け取る前にWinsockで廃棄されます。

Cisco ロギングコマンドの詳細については次のWebページを参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/cs/csprtf/csprtf4/cstroubl.htm>

6.17 Cisco ワイヤレスデバイス(Aironet)の設定

ワイヤレスアクセスポイントにTelnetあるいはコンソール経由で接続し、イネーブルモードにします。

デバイスのイネーブルプロンプトから次のコマンドを入力します。

Config terminal

Logging on

Logging Facility Local7 (またはこのデバイスに割り当てる、その他のファシリティ)

Logging [Kiwi Syslog Daemon実行マシンのIPアドレスまたはホスト名]

End

この他にIOS v11.2で初めて登場した logging source-interface も有用なコマンドです。Cisco社によれば、syslogメッセージにはルーターの出力側インターフェイスのIPアドレスが含まれています。logging source-interface コマンドで、パケットがルーターから送出されるときに使用されたインターフェイスに関わらず、特定のインターフェイスのIPアドレスを含むsyslogパケットを指定することができます。

*一部のIOSバージョンにはバグが存在しますので、必ず logging source-interface コマンドを使用してください。このコマンドを使わないと、送信されるsyslogメッセージのUDPチェックサムは不正となり、Kiwi Syslog Daemon が受け取る前にWinsockで廃棄されます。

Cisco ログインコマンドの詳細については次のWebページを参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/cs/csprtf/csprtf4/cstroubl.htm>

6.18 D-Link DFL-700 ファイアウォールの設定

以下の情報を提供して下さったGeir Aasmoe氏に謝意を表明いたします。

詳細については次のWebページを参照してください。

<http://support.dlink.com/products/view.asp?productid=DFL%2D700>

DFL-700 でsyslogメッセージを送信するための設定

- 1). ファイアウォールがインストールされ動作していることを確認します。
- 2). Webブラウザを立ち上げ、コンフィグレーションパネルを開きます(<http://192.168.1.1>)。上部のナビゲーションバーにある System タブをクリックします。
- 3). 左側のナビゲーションバーにある Logging を選択します。
- 4). Syslog チェックボックスをオンにします。
- 5). Syslog Server 1 ボックスにKiwi Syslog DaemonをインストールしたマシンのIPアドレスを入力します。
- 6). 使用するsyslogのファシリティを選択します(推奨値: Local7)。

6.19 DLink DL-840V ルーターの設定

以下の情報はDShield社のWebサイト(<http://www.dshield.org/>) で公開されているセットアップガイドからの抜粋です。詳細については次のWebページを参照してください。

<http://www.dshield.org/clients/dlinkhelp>

- 1). ルーターがインストールされ動作していることを確認します。
- 2). Webブラウザを立ち上げ、コンフィグレーションパネルを開きます(<http://192.168.1.1>)。上部のナビゲーションバーにある Advanced Settings タブをクリックします。
- 3). 左側のナビゲーションバーにある Administration Settings を選択します。
- 4). SYSTEM Log の下の Enable System Log Function をクリックし、Kiwi Syslog DaemonをインストールしたマシンのIPアドレスを入力します。

6.20 FortiGate アンチウイルスファイアウォールの設定

以下の情報はFortiGate 60 設定マニュアルからの抜粋です。

詳細については次のWebページを参照してください。

http://docs.forticare.com/fgt/admin/01-28008-0002-20050909_FortiGate-60_Administration_Guide.pdf

FortiGateユニットからsyslogサーバーを実行しているリモートコンピュータへログを送信するための設定は、CLIまたはWebインターフェイスから行います。

コマンド構文

```
config log syslogd setting
  set <keyword> <variable>
```

```
config log syslogd setting
  unset <keyword>
get log syslogd setting
```

```
show log syslogd setting
```

注: Webベースの管理ツールに表示されないsyslog設定のコマンドキーワードのみがファシリティキーワードとなります。

例:
以下のコマンドを入力して、リモートsyslogサーバーへのロギングを有効にし、サーバーのIPアドレスとポートおよびユーザーのファシリティタイプを設定します。

```
config log syslogd setting
  set status enable
  set server 220.210.200.190
  set port 514
  set facility user
end
```

以下のコマンドを入力して、リモートsyslogサーバーに対するロギングの設定を表示します。

```
get log syslogd setting
```

以下のコマンドを入力して、リモートsyslogサーバーに対するロギングのコンフィグレーションを表示します。

```
show log syslogd setting
```

showコマンドを入力したときにプロンプトが返されたときは設定がデフォルトのままであることを示しています。

FortiOS V 2.8を実行しているFortiGateデバイスの設定に関する詳細は次のWebページを参照してください。

<http://kc.forticare.com/default.asp?id=1580&Lang=1&SID=>

6.21 FREESCO ルーター/ファイアーウォールの設定

以下の情報を提供してくださったBill Hely氏に謝意を表明いたします。

Freesco (<http://www.freesco.org/>) は優れたフロッピーベースのLinuxファイアーウォール/ルーター O/S です。8Mb RAMを搭載した386sx以上(486以上推奨)のハードウェア上で動作します。オプションのHDDインストールではさらに広範な機能を有しアドオンも充実しています。Freescoはsyslog出力が可能であり、Kiwi Syslog Daemonで使用するには小さなファイルを1つだけ編集する必要があります。

- Freesco PC にrootでログインします。
- [Linux]プロンプトで、edit /boot/etc/syslog.cfg と入力します。
(既存のsyslog.cfgファイルが表示されます。このファイルでは[TAB] が大文字の I のような垂直線として表示されますので注意が必要です)。
- 既存のファイルの末尾行に、次のエントリーを追加します。
.[press the TAB key]@192.168.1.20
(IPアドレスはKiwi Syslog Daemonの実行コンピュータのアドレスです。IPアドレスの直前に @ を付けます。)
- [Enter] キーを押してファイルの最後に空白行を挿入します。
- {Alt} + [S] で変更したファイルを保存します。次に[Alt] + [X] でエディタを終了します。
- [F1] を押すと、その他の使用可能コマンドキーのリストが表示されます。
- Freesco コンピュータを再起動すると変更が有効になります。

6.22 HP JetDirect プリンタの設定

HP JetDirect のsyslog設定は HP JetAdmin プログラムまたは内蔵のWebインターフェイスから行います。

Webインターフェイスに接続するには、ブラウザでhttp://print_server_address:8000/と入力します。

- HPロゴをクリックしてメインメニューを表示します。
- 使用可能なデバイスの一覧から設定するプリンタを選択します。
- Configuration リンクをクリックします。

- 左側のメニューから Network リンクをクリックします。
- System Log Server にカーソルを移動します。
- Kiwi Syslog Daemon実行マシンのアドレスを入力します。
- [Apply]ボタンを押します。

6.23 Intertex ADSL ルーターの設定

以下の情報は IG ADSL ルーターのマニュアルからの抜粋です。

外部のsyslogサーバーへのシステムログのエクスポート

本製品のsyslogクライアントは、システムログおよびセキュリティログを接続されているコンピュータ上で実行中のRFC 3164準拠syslogサーバーに送信できます。syslogを有効にするにはコンピュータ上でsyslogサーバーが稼動していなければなりません。多くのシェアウェアあるいはフリーウェアのsyslogサーバーがあります。Kiwi Syslog Daemon(<http://www.kiwisyslog.com>)はフリーウェアのWindows用syslogサーバーであり製品CDにバンドルされています。

syslogを開始するには

1. Webブラウザで Internet Gate Webページを開きます(デフォルトIPアドレス: 192.168.0.1.)。
2. ログインします。
3. **Administration** をクリックします。
4. **Syslog server** フィールドでKiwi Syslog サーバー実行マシンのIPアドレスを入力します。
5. **Save** をクリックします。

システムログに記録された新しいイベントもすべて指定したKiwi Syslog Daemonサーバーに送られるようになります。

6.24 Linksys ファイアーウォールの設定

Linksys ファイアーウォールはSNMP経由でメッセージを送信します。Kiwi Syslog Daemonでポート162でのSNMPトラップ受信を有効にする必要があります。

- Kiwi Syslog Daemonのメイン画面で **File** の **Setup** を選択します。
- Setup 画面で **Inputs** の **SNMP** オプションを表示します。
- **Listen for SNMP traps** チェックボックスをオンにします(デフォルトポートは162です)。

Use Linksys Display Filter... をオンにすることもできます。このオプションをオンにするとPPPとPPPoEメッセージが表示されなくなりますが、ログファイルには残ります。Linksysファイアーウォールは大量のメッセージを送信する傾向があるため、極めて効果的です。

設定の変更が終わったらシステムを再起動してください。Kiwi Syslog Daemonの設定が正しく更新されます。

Linksysファイアーウォールの吐き出すメッセージはSNMPトラップにエンコードされたテキストメッセージです。OID値に対するMIB参照が実行されますが、有用な情報の多くはテキストに既に含まれています。

6.25 Linksys ワイヤレスVPNルーターの設定

新しいLinksys Wireless-G VPN ブロードバンドルーターでsyslogメッセージ送信が可能になりました。以前のLinksys ファームウェアではアラート送信にSNMPトラップを経由していました。SNMPトラップの設定については前項を参照してください。

- WebブラウザからLinksysルーターへログインします。
- Administration タブをクリックします。
- Log タブをクリックします。
- Syslog notification を表示します。
- オプションを Enabled にします。
- Device name にログメッセージを識別するための固有名を入力します。Linksys のままでも構いません。
- Kiwi Syslog Daemon実行マシンのIPアドレス(例: 192.168.1.100)を入力します。
- 送信するsyslogメッセージのタイプを設定します。デフォルト Informational です。すべてのメッセージのプライオリティが debug となります。
- Alert Log では通知を受信したいアラートに関係するボックスを選択します。
- General Log では通知を受信したいメッセージに関係するボックスを選択します。
- ページ下部の Save Settings リンクをクリックして変更を保存します。

6.26 Lucent ルーターの設定

Ethernet -> Mod Config --> Log...

```
Syslog=Yes
Log Host=10.23.45.111
Log Facility=Local5
```

MAX が Syslog daemon にメッセージ送信するように設定するには、Ethernet Profile (Mod Config メニュー)の Logサブメニューを開き、次の作業を行います。

Syslog をYesにする

ホストがMAXと同じサブネット上にない場合、Kiwi Syslog Daemonの実行ホストのIPアドレスを指定します。

MAX にはホストに対してRIP経由でのルートもしくはスタティックルートが確立されていなければなりません。

Table 12-3を参照 "System configuration and administration parameters."
"Location Parameters via RIP or a static route."
Chapter 10を参照. "Configuring the MAX as an IP Router."

注：ダイヤルアップ接続しかできないSyslogホストにレポートを送るような設定はしないでください。そのように設定してしまうと、MAX はログアクションの度にログホストにダイヤルしハングアップ等を引き起こす可能性があります。

Log Facility パラメータはMAXからのメッセージを識別するために使われます。ログファシリティ番号を設定したら、Kiwi Syslog Daemonでそのファシリティ番号の含まれたすべてのメッセージを指定したログファイル(MAXログファイル)へ書き込むよう設定します。

Actions タブでファシリティ別にログファイルを設定します(あるいは all.debug ですべてのファシリティを取得します)。

パラメータの詳細については、MAX Reference Guide またはLucent社のWebサイトを参照してください。

6.27 Meinberg タイムサーバーの設定

以下の情報を提供して下さったMeinberg Funkhrehn社のHeiko Gerstung氏に謝意を表明いたします。

詳細については次のWebページを参照してください。

<http://www.meinberg.de/english/products/time-server.htm>

Meinberg LANTIME タイムサーバー

<http://www.meinberg.de/english/products/time-server.htm>

Meinberg Linuxベースタイムサーバーはローカルで生成したsyslogエントリを最大2つのリモートsyslogサーバー(例: WindowsベースのPCとKiwi Syslog Daemon実行サーバー)に転送することができます。設定はシステムに搭載されているWeb管理インターフェイスを使って行います。

- LANTIMEのWebインターフェイスにログオンします。
- メインページで Ethernet を選択します。
- Syslog Server 1 フィールドにKiwi Syslog Daemon実行システムのホスト名かIPアドレスを入力します(もう1台別のsyslogサーバーを運用している場合は Syslog Server 2 フィールドに2代目のsyslog受信マシンのIPアドレス/ホスト名を入力します)。
- Save Settings をクリックして設定を保存します。すぐにKiwi Syslog Daemonで最初のsyslogメッセージの受信を確認できるはずです。

Webベースの設定インターフェイスは次のWebページでオンラインデモとして公開されています。

<http://www.meinberg.de/cgi-bin/main.cgi>

(このデモではログオン処理がスキップされています。最初に表示される画面は上記のメインページです)

LAN-XPTモジュール搭載 Meinberg GPS 受信機

<http://www.meinberg.de/english/products/lanxpt.htm>

Meinberg GPS電波時計の代表モデルであるGPS167シリーズは多くの増設用ネットワーク管理モジュールに搭載可能であり、SNMPを使用したGPS電波時計のステータス値の問い合わせができるようになります。

(GPS167シリーズについては、<http://www.meinberg.de/english/products/gps167.htm> を参照)
また、これらのモジュールからはsyslogメッセージを1台のsyslogサーバーに送信し、SNMPトラップを最大3台のSNMPトラップ受信機に送信することができます。

モジュールの設定は次の手順で行います。

- Telnetでモジュールのポート9999に接続し、ログオンします。
*** Meinberg XPT Setup V1.5 ***
MAC address 00204A82B8B8
- Software version V0160 (050127) CPK_580_XPTEX
[] XPT Password: *****
- Setup メニューでオプション4 (syslog configuration) を選択します。4 と入力して[RETURN]を押します。
Change Setup:
1 Network configuration
2 Clock port configuration
3 SNMP configuration
4 SYSLOG configuration
7 factory defaults
8 exit without save (no reboot)
9 save and exit

90 Change password
Your choice ?
- Use SYSLOG logging? という質問に対し Y(=yes) と答えます。
電波時計のマニュアルに書かれているとおりにKiwi Syslog Daemon実行システムのIPアドレスを入力します。

```
***** SYSLOG Configuration *****  
Use SYSLOG logging? (Y) ? Y
```

```
Enter IP address for SYSLOG server: (172) .(016) .(003) .(042)
```

9 と入力して[RETURN]を押し、設定を保存します。モジュール(電波時計全体ではない)が再起動されsyslogサーバーへのステータスメッセージの送信が開始されます。

Meinberg Redundant GPS電波時計 (SCU-XPTネットワーク管理モジュールに搭載)

http://www.meinberg.de/english/products/scu_xpt.htm

SCU-XPTモジュールは冗長GPS電波時計システムに採用されており、2つのGPS電波時計が動作してSCU-XPTモジュールが出力信号の送信元をこの2つの時計のステータスに応じて切り替えます。このユニットはsyslogおよびSNMPトラップの機能と処理手順という意味ではLAN-XPTモジュールと非常に似通っており、LAN-XPTモジュールの設定を変更無しでそのまま使用できます。

6.28 Netgear / ZyXEL RT311/RT314

以下の情報は次のNetgear非公式サポートページからの抜粋です。

<http://www.netgear.org>

Webインターフェイスはsyslog設定をサポートしていません。Telnetコマンドから実行してください。

Menu 24.3.2 - System Maintenance - UNIX Syslog

Syslog:

Active= Yes

Syslog IP Address= xxx.xxx.xxx.xxx <---- syslogサーバーのIPアドレス

Log Facility= Local 1 <----- syslogでも同じグループが設定されていることを確認

Types:

CDR= Yes

Packet triggered= Yes

Filter log= Yes

PPP log= Yes

6.29 Netgear ADSL ファイアーウォールルーター DG834

詳細については次のWebページを参照してください。

<http://www.netgear.com/products/details/DG834.php>

syslogメッセージの送信設定

- WebインターフェイスからNetgearルーターにログインします。
- 左側の SECURITY の下にある Security logs を選択します。
- Security logs 画面の Syslog の下にある Send to this syslog server IP address チェックボックスをオンにします。
- Send syslog to this address フィールドにKiwi Syslog Daemon実行サーバーのIPアドレスを入力します。
- Include in Log では送信したいログアイテムを選択できます(任意)。

6.30 Netgear FVS318 VPN ファイアーウォール

以下の情報を提供して下さったMount Sterling OhioのPaul Bohn氏に謝意を表明いたします。

詳細については次のWebページを参照してください。

<http://www.netgear.com/products/details/FVS318.php>

必要なファームウェアレベル: NETGEAR FVS318 FIRMWARE 1.01j beta 2002年8月7日以降

syslogメッセージの送信設定

- Netgearルーターにサインオンします。
- 左側の SECURITY の下にある Security logs を選択します。
- Security logs 画面の SYSLOG チェックボックスをオンにします。
- Send syslog to this address フィールドにKiwi Syslog Daemon実行サーバーのIPアドレスを入力します。

6.31 Netgear RP114 ルーター

以下の情報はNetgear RP114の資料からの抜粋です。

詳細については次のWebページを参照してください。

<http://www.netgear.jp/products/details/RP114.html>

Webインターフェイスはsyslog設定をサポートしていません。Telnetコマンドから実行してください。

Menu 24.3.2 の System Maintenance の下の UNIX Syslog でsyslogの設定を行うことができます。Menu 24.3.2 ではルーターがUnixシステムログを他のマシンに送信するよう設定します。パラメータを変更してsyslogを有効にしてください。

フィールド: Active

コマンド: スペースバーでyes / noを切り替え

説明: syslogオプションのオン/オフが切り替わる

フィールド: Syslog IP Address

コマンド: a.b.c.d のように小数点付き4桁のアドレスを入力。a,b,c,d は0~255までの数字

説明: syslog送信先のIPアドレス

フィールド: Log Facility

コマンド: Facility値を入力

説明: 7個のローカルオプションから選択。メッセージをサーバーの異なるファイルに記録できる。

フィールド: Types: CDR, Packet triggered, Filter log, PPP log

コマンド: すべてスペースバーでyes/noを切り替え

説明: Call detail record (CDR), Packet trigger, Filter event (match or not match), PPP event.の記録を有効にする

ローカルホスト上のsyslogdプログラムを使ってロギングするためのルーター設定

1. Menu 24.3.2 の System Maintenance の下の UNIX Syslog を表示します。
2. Active を Yes にします。
3. Syslog IP Address フィールドにsyslogホストPCのIPアドレスを入力します。

4. Log Facility 番号を選択します。
5. 記録するアクティビティのタイプを選択します。

ルーターから送信可能なsyslogメッセージ

- Call detail record (CDR)
- Packet trigger
- Filter event log
- PPP event log

6. 設定を保存してメニュー画面を閉じます。

6.32 NetScreen ファイアウォールの設定

以下の情報を提供してくださったGeorge McCashin氏に謝意を表明いたします。

Webインターフェイスによる設定手順

- 1). admin ユーザーでWebインターフェイスにログオンします。
- 2). Configuration の Report Settings の下の Syslog を表示します。
- 3). Enable Syslog をクリックします。
- 4). すべてのトラフィックをログ出力させたい場合は Include Traffic Log をクリックします。
- 5). ログホストアドレスとポート番号を入力します(Kiwi Syslog Daemon実行マシンのアドレスとUDPポート514)

Kevin Branchによる追加情報

すべてのタイプのNetscreenポリシー(permit/deny/tunnel)から受信する全トラフィックを、デフォルトで許可されているログトラフィックと同様にログ出力します(Netscreenが特に拒否指定されていないセッションを許可するように設定されている場合)。

Log Packets Terminated to Self オプションはNetscreen全体のセッションとは関係ありませんが、Netscreen自身にセッションをログ出力します (Netscreen管理トラフィックだけですが、インターネットからのプローブを表示します)。

代わりに、CLIからNetScreenを設定することができます。

コマンドラインインターフェイス設定:

syslogサーバーの設定に必要なコマンドは以下のとおりです。

```
set syslog config ip_address security_facility
local_facility
set syslog enable
set syslog traffic
set log module system level level destination syslog
```

注: set syslog config コマンドでは security_facility と local_facility を定義することが必要です。syslogコマンドの security_facility とlocal_facility のオプション一覧については、NetScreen CLI Reference Guide を参照してください。

注:メッセージレベルごとに set log コマンドを入力する必要があります。レベルのオプションは以下のとおりです:

```
emergency
alert
critical
error
warning
notification
information
```

6.33 Nortel Networks ルーターの設定

以下の情報を提供してくださったFlavio Ramos氏に謝意を表明いたします。

Bay Command Console (BCC)から、次のコマンドを入力してください。

```
stack# syslog
  syslog
    log-poll-timer 10
  log-host address <Kiwi Syslog Daemon実行PCのIPアドレス>
  filter name WILDCARD entity all
    severity-mask {fault warning}
    slot-lower-bound 1
    slot-upper-bound 14
  back
back
back
back
```

6.34 Pack X IDScenterの設定

IDScenterはWindowsプラットフォーム用Snort IDSの設定管理ツールです。

次のサイトからダウンロードできます:

<http://www.packx.net/packx/html/en/index-en.htm>

outputプラグインを使えばアラートをKiwi Syslog Daemonに送信できます。

設定:

IDScenter メインウィンドウから、左側の IDS Rules タブを選択します
左側の Output プラグインアイコンを押します。
すべての設定済みoutputプラグインのリストが表示されます。

新しいプラグインの追加は、-> Add ボタンを押し、ポップアップメニューから Syslog Alert Plugin を選択します。

ウィンドウの下部にプラグインの設定画面が表示されます。

アラートメッセージを送信する facility と priority (level) を選択します。

Facility: LOG_LOCAL7

Priority: LOG_ALERT

通知されるエラー状態をすべてをチェックします。

LOG_CONS, LOG_PERROR, LOG_NDELAY, LOG_PID

次に右下の **Add** ボタンを押します。設定したばかりのsyslogアラートoutputプラグインがリストの一番上に表示されます。

6.35 SnapGear SOHO+ の設定

Webブラウザで、SOHO+の管理コンソールに接続します。

左側の **SYSTEM** セクションの下にある **Advanced** リンクをクリックします。

System Log セクションの下にある **System Log** リンクをクリックします。

Address of remote machine フィールドにKiwi Syslog Daemon実行マシンのIPアドレスまたはホスト名を入力します。

Enable remote logging チェックボックスをオンにしてメッセージの送信を有効にします。

Submit ボタンを押して変更を適用します。

これでシステムログに記録される新しいイベントはすべてKiwi Syslog Daemonサーバーに送信されるようになります。

6.36 SonicWall ファイアウォールの設定

SonicWALLファイアウォールアプライアンスはリモートのsyslog daemonへのsyslogメッセージ送信をサポートします。2台のサーバーまで構成できます。

SonicWALLの管理インターフェイスにWebブラウザで接続し、ユーザー名とパスワードを入力してログインします。

左側のメニューにある **Log** ボタンをクリックします。

メインディスプレイにタブ付きウィンドウが表示されます。

Log Settings タブをクリックします。

Sending the Log の Syslog Server 1 フィールドにKiwi Syslog Daemon実行マシンのIPアドレスを入力します。受信ポートとして514以外のポートを使用している場合は、Syslog server port 1 に実際に使用しているポート番号を入力します。

Automation で **Syslog Format** を **Webtrends** を選択してください。

Categories の Log でsyslogメッセージとして受信したいイベントタイプをすべてチェックしてください。

update ボタンを押します。

新しい設定を有効にするにはSonicWALLを再起動する必要があります。

SonicWALL が出力するsyslogメッセージのレポートを作成するには、RnRSoft ReportGen for SonicWALL をご利用ください。次のWebページからトライアル版がダウンロードできます。

<http://www.reportgen.com>

6.37 Symantec ファイアウォール/VPN 200

以下の情報を提供してくださったDavid Masilott氏に謝意を表明いたします。

Webブラウザで管理コンソールに接続します。

左側の **Advanced** の下にある **Log Settings** リンクをクリックします。

Syslog Server フィールドにKiwi Syslog Daemon実行マシンのIPアドレスまたはホスト名を入力します。

必要に応じて**System**、**Debug**、**Blocked**、**Dropped** および **Attack** の中から送信したいメッセージタイプのチェックボックスをオンにして送信を有効にします。はじめはすべてのメッセージタイプを有効にし、記録する情報が多すぎる場合はチェックを減らしてください。

Save ボタンを押して変更を適用します。

これでシステムログに記録される新しいイベントはすべてKiwi Syslog Daemonサーバーに送信されるようになります。

6.38 Unix マシンの設定

以下の情報を提供してくださったAntonino Iannella氏に謝意を表明いたします。

Unixホストでファイルを変更するにはsuper user権のあるユーザーでログインする必要があります。 -

```
/etc/syslog.conf  
/etc/hosts
```

Unixボックス上のKiwi Syslog Daemonを再起動(HUP)します。

Vi あるいはご使用のテキストエディターで/etc/hostsファイルを編集します。

hostsファイルの例

```
#  
# Internet host table  
#  
127.0.0.1    localhost  
192.168.230.23  loghost
```

loghostというホスト名のホストにメッセージが転送されます。
LoghostのIPアドレスはKiwi Syslog Daemonを実行しているWindowsマシンまたはUnixボックスのアドレスです。

Vi あるいはご使用のテキストエディターで/etc/syslog.conf ファイルを編集します。

syslog.confファイルの例

```
# Syslog configuration file.
#
*.err;kern.notice;auth.notice          /dev/console
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages

*.alert;kern.err;daemon.err            operator
*.alert                                 root

*.emerg                                 @loghost
mail.debug                              @loghost
```

上記の例では、**emerg** レベルのすべてのファシリティがlocalhost (hostsファイルで定義したホスト) に転送され、**debug** レベルのメールアラートも同様に転送されることに注目してください。

一般的には **ファシリティ.レベル <TAB> @loghost** と指定します。

編集が終わったら、このファイルを保存します。Unixボックス上のKiwi Syslog Daemonを再起動することによって変更が有効になります。syslog daemonのプロセスIDを確認し、SIGHUP シグナルを送ります。**logger** コマンドを使ってsyslogサーバーがメッセージを書き出しているかどうかテストしてください。

コマンド例：**logger -p user.emerg Unix test message**

正しく動作しているかどうか疑わしいときは man syslog を再ソートしてみてください。

6.39 VegaStream テレフォニーゲートウェイの設定

以下の情報はVegaStreamの技術マニュアルからの抜粋です。

オリジナルは次のWebページからダウンロードできます。

http://www.vegaassist.com/documentation/3-Technical%20Documentation/IN_21-Syslog_01.pdf

Vegaでのsyslog設定

Vegaゲートウェイは次にあげる4種のsyslog情報をサポートしています。

1. Log データ(ログとして表示されるデータと同じ)
2. Billing / CDR データ(料金として表示されるデータと同じ)
3. Console audit (全コンソールに対するシリアル、Web、Telnetコマンドすべてのログ)
4. Debug 情報(デバッグとして表示されるデータと同じ)

Vegaゲートウェイでは最大5つのsyslogセッションをサポートしています。1つのsyslogセッションでこれらの情報のうち1つ、あるいは複数の情報を組み合わせて送信するよう設定できます。

Vegaがsyslog送信するときに使用するポートはUDPです。

syslogセッションの設定を行うには、Webブラウザで左側のメニューから Logging を選択し SYSLOG Configuration の下の SYSLOG を選択します。

syslogサーバーのリストから適宜 Add、Delete、Modify を選択します。

Name フィールドには自分でわかりやすい名前を入力し、Host にはメッセージ送信先syslogサーバーのIPアドレスを入力します。

Port にはメッセージの出力用UDPポート番号を入力します(通常は514)。

このサーバーに送信する情報のタイプを Logging、Billing、Console、Debug の中から選択し定義します。

Submit ボタンを押し、Apply Changes ボタンを押すと変更が適用されて新しい設定が有効になります。

注:syslogによってかなり大量のデータトラフィックが発生する可能性があります。複数のsyslogロギングオプションが選択され受信先サーバーを複数設定されている場合は特にこの傾向が顕著となります。その結果、LAN帯域やゲートウェイのパフォーマンスに影響が及ぶことがあります。

6.40 Watchguard Firebox と Dshieldの連携設定

詳細については、次のWebページを参照してください。

http://live.dshield.org/clients/watchguard_kiwi_setup.php

6.41 WatchGuard SOHO ファイアウォールの設定

以下の情報はWatchGuard Knowledgebaseからの抜粋です。

SOHO 2.4.0以上ではネットワーク経由でのsyslogサーバーに対するログ送信がサポートされています。syslogはSolaris、CO Unix、BSD、Linux およびその他の*nix形式のオペレーティングシステムからログデータを取得する共通サービスです。SOHOでは標準ログと同時にsyslog機能が実行され、バックアップ手段として活用可能です。

しかし、若干の制約があります。syslogサービスではUDP 514ポートでネットワークデータを送ります。SOHOやsyslogホストからはログデータが正確に配信されたかどうか確認できません。syslog仕様によればデータの暗号化はされません。

設定は簡単です。次の手順に従ってください。

SOHOのsyslog設定

SOHOの設定インターフェイスを開きます。

System Administration をクリックします。

Syslog Logging をクリックします。

Enable Syslog output チェックボックスをオンにします。

Kiwi Syslog Daemon実行ホストのIPアドレスを入力します。

syslogはログデータの暗号化を行いません。syslogを悪意のあるネットワーク経由で送信しないよう設定時には十分気を付けてください。

Submit をクリックします。

SOHO を再起動します。

6.42 W-Linx MB ブロードバンドルーターの設定

以下の情報を提供して下さったPhilipp Beckers氏に謝意を表明いたします。

詳細については次のWebページを参照してください。

http://www.w-linx.com.tw/products/multifunction/soho_mate.htm

1. Webブラウザで W-Linx ボックス(<http://192.168.1.254>)に接続し、adminでログインします。
2. Advanced Setting をクリックし、System Log を表示します。
3. IP Adress for Syslog フィールドにKiwi Syslog Daemon実行PCのIPアドレスを入力します。
4. enable チェックボックスがオンになっていることを確認し、save をクリックします。
5. ルーターを再起動するとsyslogが使用可能になります。

6.43 ZyXEL ZyWALL 10の設定

以下の情報を提供して下さったKillian McCourt氏に謝意を表明いたします。

詳細については次のWebページを参照してください。

<http://www.netgear.org>

Webインターフェイスからはsyslog設定は行えません。Telnetコマンドラインインターフェイスもしくはコンソールポート経由でのみ設定可能です。

Menu 24.3.2 - System Maintenance - UNIX Syslog

Syslog:
Active= Yes
Syslog IP Address= xxx.xxx.xxx.xxx (IP address of the syslog)
Log Facility= Local 1 (Send messages with a facility of Local1)

Types:
CDR= No
Packet triggered= No
Filter log= No
PPP log= No
Firewall log= Yes
VPN log= No

上記の設定方法はNetgear/Zyxel RT311/RT314とほとんど変わりません。

7 SNMPトラップ送信デバイスの設定

本章ではSNMPトラップ送信可能なネットワーク機器の設定について説明します。
本書に記載されていないSNMPとラップ送信可能デバイスについての情報をお持ちでしたら、下記までお知らせください。次回のマニュアル更新時に情報を追加させていただきます。
<http://www.kiwisyslog.com/support/>

7.1 Cisco IOS SNMP トラップのサポート設定

Cisco標準IOSソフトウェアを実行するCiscoデバイス(各種ルーター、ATMスイッチ、リモートアクセスサーバー)は多くのSNMPトラップを送信できます。
サポート対象Cisco IOS SNMPトラップおよび設定手順については次のWebページを参照してください。
http://www.cisco.com/JP/support/public/mt/tac/100/1001716/snmp_traps.shtml

8 SyslogdエラーとEメールログ

8.1 エラーログ

Kiwi Syslog Daemonがログファイルにメッセージを書き込めない時や、ログファイルのアーカイビングに問題がある時、エラーログテキストファイルにエラーが記録されます。

ファイル名は Errorlog.txt で、Kiwi Syslog Daemonをインストールしたフォルダの直下にあります。

Kiwi Syslog Daemonで発生したその他のエラーもこのファイルに記録されます。

8.2 エラーログファイルの表示

Kiwi Syslog Daemonのメイン画面から次の操作を行います。

View の View Error log file を選択する、もしくは [Ctrl]+[R] を押します。

エラーログが記録されている場合はメモ帳でエラーログテキストファイルが開きます。

8.3 SMTPメールログ

アラーム通知メールや、日別統計がEメールで送られると詳細が送信メールログファイルに記録されます。

ファイル名は SendmailLog.txt で、Kiwi Syslog Daemonをインストールしたフォルダの直下にあります。

<PRI>HEADER MESSAGE

プライオリティは0～191の値です。スペースを挿入したり、先頭桁を0埋めしないでください。
syslogメッセージフォーマットの詳細については、RFC文書を参照してください。

ファシリティは、マシンのどのプロセスによって生成されたメッセージであるかを示しています。syslogプロトコルは当初BSD Unix用に開発されたものであるため、ファシリティはUnixのプロセスやデーモンの名前が反映されています。
プライオリティは次の式で計算されます。
Priority = Facility * 8 + Level

セベリティレベルの一覧

- 0 Emergency: システム使用不可
- 1 Alert: 対応至急必要
- 2 Critical: 危険な状態
- 3 Error: エラー発生
- 4 Warning: 警報発生
- 5 Notice: 正常だが重大な事態
- 6 Informational: 情報
- 7 Debug: デバッグレベルメッセージ

通常のメッセージには Notice または Informational レベルを指定してください。

セベリティレベルの詳細

DEBUG:

アプリケーションのデバッグ用で開発者にとっては有用だが、オペレーターには有用でない情報

INFORMATIONAL:

通常の実行で発生するメッセージ - レポート作成やスループット測定等に活用される場合がある。対応不要

NOTICE:

異常ではあるがエラーではないイベント - 緊急な対応は不要だが問題が発生する可能性があるため概要を開発者や管理者にEメールで連絡してもよい。

WARNING:

警告メッセージ - エラーではないが、何らかの対応を怠るとエラーが発生する可能性を示す。例: file system 85% full - 一定時間内での対応が必要

ERROR:

緊急ではないが障害が発生していることを示す - 開発者が管理者に連絡する必要がある。一定時間内に解決する必要がある。

ALERT:

至急に解決する必要がある障害が発生していることを示す - 問題解決できるメンバーに連絡 - 例: 予備のISP接続の切断

CRITICAL:

至急に解決する必要がある障害が発生しており、主要システムに問題があることを示す - ALERTよりも優先して対応する必要がある。 - 例: ISPとの再接続の切断

EMERGENCY:

緊急対応を要するパニック状態が発生していることを示す - 多くのアプリケーション、サーバー、サイト等に影響を及ぼすような状況(地震/竜巻など)であるため、技術スタッフ全員に通知する必要があるかもしれない。

9.3 Syslog プライオリティ

各syslogメッセージにはテキストの先頭にプライオリティ値が付けられています。プライオリティは0～191までの値であり、ファシリティ値とレベル値で構成されます。プライオリティは<>で括弧で囲われています。

以下はBSD Unixのsyslogメッセージの一例です。

<PRI>HEADER MESSAGE

プライオリティは0～191の値です。スペースを挿入したり、先頭桁を0埋めしないでください。
syslogメッセージフォーマットの詳細については、RFC文書を参照してください。

プライオリティは次の式で計算されます。
Priority = Facility * 8 + Level

手動で特定のプライオリティを設定するには Priority フィールドに数字を入力し Use this value チェックボックスをオンにします。入力した値はsyslogメッセージの <PRI> フィールドに送られます。191～255まで使用できます。191以上は不正な値であり不測の結果を引き起こす可能性があります。

9.4 転送

Kiwi Syslog DaemonはUDPメッセージもTCPメッセージも受信します。通常syslogメッセージはUDPで送信されます。Cisco PIX ファイアウォール等一部のネットワークデバイスは、TCPでメッセージを送信しKiwi Syslog Daemonからの受信応答を待ってパケットが確実に届いたかどうか確認します。

UDPを使ってメッセージを送信する際の受信ポートは通常514です。

TCPを使ってメッセージを送信する際の受信ポートは通常1468です。

9.5 Syslog RFC 3164 ヘッダーフォーマット

HEADER 部分には時刻とデバイスのホスト名またはIPアドレスが入ります。
HEADER には TIMESTAMP と HOSTNAME というフィールドがあります。
PRIの > の直後に TIMESTAMP が入り、1つスペースを空けて HOSTNAME フィールドが入ります。TIMESTAMP と HOSTNAME の間には必ず1文字分のスペースが入ります。
HOSTNAME にはその名のとおりホスト名が入ります。ホスト名が指定されていない場合はIPアドレスが入ります。
TIMESTAMP には現地時刻が入りそのフォーマットは Mmm dd hh:mm:ss です。

MSG 部分には TAG と CONTENT というフィールドがあります。TAG フィールドにはメッセージを生成したプログラム名またはプロセス名が入ります。CONTENT にはメッセージの詳細が入ります。イベント情報などを自由に書けるフリーフォームのメッセージです。TAG にはABNF英数字で32文字以内の文字列が入ります。英数字以外の文字を入力すると、そこがTAGフィールドの終点で CONTENT フィールドの始点とみなされます。通常、CONTENT フィールドの開始文字は [、:またはスペースであり、これは同時に TAG フィールドの終点を意味します。

Kiwi SyslogGen によって生成されるメッセージのフォーマットは次のとおりです。
<PRI>Jul 10 12:00:00 192.168.1.1 SyslogGen MESSAGE TEXT

BSD Syslog プロトコルについてはRFC 3164で議論されています
<http://community.roxen.com/developers/idocs/rfc/rfc3164.html>

syslogプロトコル全般については次のWebページを参照してください。
<http://www.sans.org/infosecFAQ/unix/syslog.htm>

9.6 Kiwi Reliable Delivery Protocol (KRDP)

背景:

Kiwi Reliable Delivery Protocol はネットワーク障害でTCP接続が切断されたときにデータが喪失する問題を解決するために設計されました。

KRDPはTCPプロトコルを利用しています。送信パケットに番号が付けられ受信すると応答があるため各パケットが順番に確実に送信されます。受信システムのTCPプロトコルはパケット順に処理し、失われたパケットが再送されていることを確認します。

問題点:

TCPは接続の開閉に問題がないときには信頼できる転送を行います。TCPハンドシェイクが閉じられるあいだ、通常、転送途中のパケットの受信が済み、応答があってから接続が閉じられます。。

しかし、メッセージ送信中にネットワークが切断されると、送信者はTCPウィンドウサイズまでパケット送信を続けます。タイムアウトを過ぎても応答がないとWinsockスタックはタイムアウトイベントを実行します。この場合どのメッセージまで(あるいはメッセージのどの部分まで)正確に受信しリモートホストから応答があったかを正確に知ることは不可能です。Winsockスタックバッファのデータは失われます。TCPウィンドウサイズとデータ送信速度にもよりますが、失われるメッセージは数100に達すると思われます。

解決策:

KRDPはTCP転送の上に別の応答とシーケンスレイヤーを追加します。KRDPは各syslogメッセージを固有のシーケンス番号を含むヘッダーでラップします。KRDP送信者は送信した各メッセージのローカルコピーを保存します。KRDP受信者は最後に受信したKRDPラップ済みsyslogメッセージに対して定期的に応答を返します。応答を受信したら、KRDP送信者は応答済みの最終シーケンス番号までのローカル保存メッセージを削除しても構いません。接続が切れ、再接続されたときには、受信者はどのメッセージの再送が必要かを送信者に連絡します。

各KRDP送信者は固有の接続名で識別されます。このため送信者と受信者は同じセッションとシーケンス番号で再接続ができます。DHCPなどにより送信者のIPアドレスや送信ポートなどが変更されても大丈夫です。

固有のメッセージシーケンス：

各KRDPメッセージは固有のシーケンス番号で識別されます。シーケンスは1から始まり2147483647(20億)まで1ずつ増加し、2147483647に到達したら1に戻ります。メッセージ番号 0 は、システムで最終番号を認識できないことを示し、新たに番号を振り直す必要がある場合に使用されます。このような場合、送信者側と受信者側の双方でメッセージが喪失したことを示すエラーが記録されます。

外国文字の処理：

Unicodeはすべての外国文字を既知のバイトシーケンスにマッピングします。非US-ASCII文字は1文字あたりに複数バイト使用します。TCPでこれらの複数バイト文字を送信するときに最も多く使用されているのは、UTF-8エンコーディングを利用する方法です。KRDP送信者はsyslogメッセージをUTF-8でエンコードし、KRDP受信者はUnicodeにデコードします。

KRDPメッセージのフォーマット：

Sender (S)
Receiver (R)

メッセージタイプ (MsgType)：

00 = SenderID
01 = ReceiverResponse
02 = Sequenced message
03 = Message acknowledgement
04 = Receiver KeepAlive
99 = Error message

メッセージフォーマット：

KRDP AA 0000000000 Message<CR>
KRDP = Unique tag
Space (ASCII 32)
AA = Msg type (as above)
Space (ASCII 32)
0000000000 = Sequence number 0 to 2147483647
Space (ASCII 32)
Message = UTF-8 encoded message text
<CR> = Carriage return character ASCII 13 to indicate end of message stream

イベントのシーケンス：

S connects via TCP
S sends first ID packet (MsgType 00)
R responds with ReceiverResponse message (MsgType 01)
S sends sequenced messages (MsgType 02)

ルール：

1. If the first message R receives is not a ID message (MsgType 00), R disconnects. (Any data received is ignored).
2. If R does not receive ID message after 60 seconds, R disconnects.
3. After S sends the ID message, S will wait up to 60 seconds for a ReceiverResponse message. If there is no response, S will disconnect session.
4. R sends ACK messages to S with the next expected message sequence
5. ACK messages are sent no more frequently than once every 200ms

メッセージフォーマット：

MsgType 00 (Version and SenderID)

KRDP 00 PV UniqueKey<CR>

The unique key identifies the channel and is used to synchronise the message numbers

PV = Protocol Version to use. 01 = KRDP Reliable/Acknowledged

Unique key format is free form.

An example would be: "IP=192.168.1.1, Host=myhost.com, ID=Instance1"

Or, just: "Instance1"

Since the receiver might already have an "Instance1" name from another source, the first UniqueKey would be better. Use as much information to uniquely describe the source of the messages

MsgType 01 (ReceiverResponse message)

KRDP 01 0000000000 Listener ID<CR>

Message number is 10 digit number 0000000000 to 2147483647

MsgType 02 (Sender Message content)

KRDP 02 0000000000 Message content<CR>

Message number is 10 digit number 0000000000 to 2147483647

MsgType 03 (Receiver ACK)

KRDP 03 0000000000 ACK<CR>

Message number is 10 digit number 0000000000 to 2147483647

Message number indicates the next sequence number it expects to receive

ACK messages are sent at a maximum rate of once every 200ms

MsgType 04 (Keep alive)

KRDP 04 0000000000 KeepAlive<CR>

Message number is 10 digit number 0000000000 to 2147483647

Message number = Next expected message number

If being sent by Sender, MsgSeq should be set to 0

If being sent by Receiver, MsgSeq should be set to next expected message number

MsgType 99 (Error)

KRDP 99 0000000000 0000 Error message here<CR>

Message number is 10 digit number 0000000000 to 2147483647

Message number indicates which message caused the error if any. Set to zero (0) if not related to a message number

0000 = Error number (0000 to 9999)

Error message can be any text

9.6.1 KRDP エラーメッセージ

Error 1000 - Unable to decode the following message: <不正メッセージ>

正しくエンコードされなかった、あるいは破損したメッセージを受信しました。メッセージを参照してデバッグしてください。

Error 1001 - Sender is unable to supply message number: <NextMsgSeq>. Starting again from 0. Sender

ID: <UniqueSenderId>

シーケンス番号1以上のメッセージを受信するはずでしたが送信者がメッセージを送信できなかったため、0から再スタートする必要があります。受信者は送信者と同期を取りなおします。

Error 1002 - Missed message number: <NextMsgSeq>. Received: <ActualMsgSeq> on ID: <UniqueSenderId>

受信するはずだったメッセージ番号のメッセージを受信できませんでした。受信者は送信者と同期を取りなおします。

Error 1003 - Received unexpected message data. Message ignored. Sender ID: <UniqueSenderId>

予期しないメッセージを受信しました。このデータは無視されます。

Error 1004 - First message did not contain Sender ID. Connection closed.

接続確立後に最初に受信したメッセージに送信者IDが含まれていませんでした。受信者側でその接続を閉じました。

Error 1005 - Unable to send Expected message number reply. Connection closed.

受信者側から確立されている接続を通じて応答メッセージを送信できませんでした。受信者側でその接続を閉じました。

Error 1006 - Unable to send error message.

受信側から確立されている接続を通じてエラーメッセージを送信できませんでした。

Error 1007 - Unable to send KeepAlive message. Connection closed.

受信側から確立されている接続を通じてキープアライブメッセージを送信できませんでした。受信者側でその接続を閉じました。

Error 1008 - Unable to send KeepAlive to connection: <UniqueSenderId>

受信側から確立されている接続を通じてキープアライブメッセージを送信できませんでした。

Error 1009 - Unable to send ACK to connection: <UniqueSenderId>

受信側から確立されている接続を通じてACKメッセージを送信できませんでした。

Error 1099 - <送信者からのメッセージ>

1099エラーを発信することによって送信者から受信者にエラー発生を通知できます。メッセージは送信者からのものです。

Error 1010 - Unexpected message received. Type: <MsgType>. Message content: <Message Content>
予期しないタイプのメッセージを受信しました。メッセージを参照してでバグしてください。

10 問題の解決

10.1 問題を解決するには

メッセージが表示されない、あるいはログが記録されない

- 送信デバイスからKiwi Syslog DaemonマシンにPingしてネットワーク接続に問題がないか確認してください。
- 複数のKiwi Syslog Daemonインスタンスが稼動していないか確認してください([Ctrl] + [Alt] + [Del]でタスクリストを表示できます)。
- ZoneAlarm や BlackIce のようなパーソナルファイアウォールを無効にしてください。
- コマンドプロンプトからホスト名でPingし、DNSが正しく解決されているか確認して下さい。
- 受信したいメッセージのファシリティとレベルに対し Display アクションの設定がされていないことを確認してください。
- [Ctrl] + [T]**でテストメッセージを送信してください。
次のWebページから無料のSyslog Daemon Message Generator (SyslogGen)をダウンロードしてください。
<http://www.kiwisyslog.com/downloads>
- Kiwi SyslogGenをインストールし、127.0.0.1 (ローカルホスト)に1秒ごとにメッセージを送ってください。
メッセージが表示されれば、問題はルーター、スイッチ、Unixボックス等Syslogメッセージ送信側デバイスにあります。
- 他のマシンからKiwi SyslogGenでKiwi Syslog Daemon実行ホストにメッセージを送信してください。
- メッセージ送信デバイスから送られてくるメッセージにプライオリティ値が含まれていない可能性があります。Kiwi Syslog Daemonの Setup 画面の Modifiers オプションでデフォルトのプライオリティ値を設定してください。Setup 画面を表示するにはKiwi Syslog Daemonのメイン画面から **File | Setup** を選択します。
- Ciscoルーターからのメッセージを受信できていない場合、Logging source-interface コマンドで送信元のインターフェイスを指定してください。Cisco IOSのバグにより、このコマンドで指定しないとUDPチェックサムが不正になります。

まだKiwi Syslog Daemonにメッセージが表示されない

- コンピュータを再起動してください(可能ならば電源を切ってください)。
- IPアドレス解決を行わないよう、DNS設定を無効にしてください。
- Alarm と Statistics 通知オプションのチェックをはずしEメール送信を無効にしてください。
- Defaults/Import/Export** の [Load default Rules and Settings] ボタンを押してください。次に [OK] を押して変更を適用してください。
- Kiwi Syslog Daemonのエラーログファイルを表示して、役に立ちそうな情報がないか確認してください。
エラーログファイルの名前は Errorlog.txt でKiwi Syslog Daemonをインストールしたフォルダの直下にあります。
- エラーログファイルの中にKiwi Syslog Daemonが特定のポートをバインドできないことを示すメッセージを見つけたら、そのポートを使用しているアプリケーションを閉じてからKiwi Syslog Daemonをもう一度再起動してください。詳細については次のWebページにあるFAQを参照してください。
<http://www.kiwisyslog.com/support>

まだKiwi Syslog Daemonにメッセージが表示されない

上記の作業を行ってもまだ問題が解決しない場合は、次のWebページからアクセスできるサポートフォームに記入して詳細をお知らせください。その際は問題の早期解決のため、できるだけ詳細な技術情報をご記入ください。

<http://www.kiwisyslog.com/support>

10.2 Windows XP SP2 / Windows 2003 Server SP1上で使用する場合の注意事項

Windows XP Service Pack 2/Windows 2003 Server Service Pack 1をインストールすると、デフォルトでWindowsのファイアウォール機能がオンになります。このままだとKiwi Syslog Daemonへのトラフィック転送がすべてブロックされてしまいます。

この問題を解決するにはWindows のファイアウォールの設定で例外を作成する必要があります。

次の手順に従ってください。

- Windowsの [コントロールパネル] の [Windows ファイアウォール] を開きます。
- [例外] タブを選択します。

- [ポートの追加] ボタンを押します。
- [名前] と [ポート番号] にそれぞれ指定し、[TCP] と [UDP] のどちらかを選択します。
(デフォルトではKiwi Syslog DaemonはUDPポート514を使用します)

Kiwi Syslog Daemon側で受信用として違うポートを指定した場合は、指定したポートごとに例外を作成する必要があります。例えば、SNMPトラップを受信するよう設定してある場合はUDPポート162を許可する例外を作成する必要があります。

上記の設定を行ってもまだ問題が解決しない場合は、次のWebページからアクセスできるサポートフォームに記入して詳細をお知らせください。

<http://www.kiwisyslog.com/support>

また、前項の「問題を解決するには」も参照してください。

10.3 Windows 95上で使用する場合の注意事項

Windows 95上でKiwi Syslog Daemonを実行するにはMicrosoft社からリリースされている以下の更新を適用する必要があります。

DCOM for Windows 95:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=d7a4de78-81a9-4db7-beb6-84ff99342172&displaylang=en>

Winsock2 for Windows 95:

<http://support.microsoft.com/kb/177719/ja>

Windows Common Controls update:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=6f94d31a-d1e0-4658-a566-93af0d8d4a1e&DisplayLang=en>

場合によってはInternet Explorer 4以上をインストールする必要があるかもしれません。

次のリンクをクリックするとWindows 95の更新ファイルを1つのzipファイルでまとめてダウンロードできます。

<http://www.kiwitools.com/downloads/Windows95Updates.zip>

更新を適用したら、システムを再起動しKiwi Syslog Daemonを再インストールしてください。

上記の作業を行ってもまだプログラムが起動しない場合は、次のWebページからアクセスできるサポートフォームに記入して詳細をお知らせください。

<http://www.kiwisyslog.com/support>

11 開発者向けの情報

11.1 Kiwi Syslog Daemonのレジストリ設定

以下ではKiwi Syslog daemonに影響を与えるレジストリ値について解説します。

レジストリ変更にあたってはKiwi Syslog Daemonが起動していないことを確認してください。サービス版であればService Manager の Manage メニューからサービスを停止してください。

レジストリ値を表示し、変更するには RegEdit を使用します。

変更後Kiwi Syslog Daemonを再起動することによって新しい値が読み込まれます。

11.1.1 表示 - 有効列

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DisplayColumnsEnabled

最小値: 0

最大値: 31

デフォルト値: 31

タイプ: 0-31までの十進数

この値はディスプレイに表示される列数を指定します。通常はすべての列が表示されます。指定する値を調整することで表示列を有効にしたり無効にしたりすることができます。

各列は0または1に設定されるバイナリービット値で表されます。

ビット数	十進数	列名
0	1	Date
1	2	Time
2	4	Priority
3	8	Hostname
4	16	Message text

全列を表示するには31に設定します。

Message text (16) および Hostname (8)列を表示するには24 (16 + 8 = 24)に設定します。

Message text (16) および Time (2)列を表示するには18 (16 + 2 = 18)に設定します。

Message text 列のみを表示するには16に設定します。

11.1.2 表示 – デフォルトの行の高さ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DisplayRowHeight

最小値: 5

最大値: 50

デフォルト値: 15

タイプ: 行の高さ(ピクセル)

この値はディスプレイに表示されるデフォルトの行の高さを指定します。指定した高さよりも表示されるフォントの高さが高い場合はテキストに合わせて自動調整されます。

11.1.3 統計メール配信時刻

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: MailStatsDeliveryTime

最小値: 00:00

最大値: 23:59

デフォルト値: 00:00

タイプ: HH:MM

この値は日別統計Eメールの送信時刻を指定します。デフォルトでは真夜中(00:00)に送信されます。統計メールを午後6時に送信するには18:00と設定します。

11.1.4 サービス – 開始/停止 タイムアウト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ServiceStartTimeout

最小値: 1

最大値: 120

デフォルト値: 30

タイプ: 秒

どのくらいの時間 Service Manager が Service Start あるいは Service Stop を待つかを指定します。設定済みのアクションが10以上ある場合、あるいは300Mhz以下のCPUを搭載したマシン上で実行している場合は、適宜この値を大きくしてください。

11.1.5 サービス – プロパティ更新タイムアウト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ServiceUpdateTimeout

最小値: 1
最大値: 120
デフォルト値: 5
タイプ: 秒

どのくらいの時間 Service Manager が Properties Update の完了を待つかを指定します。設定済みのアクションが10以上ある場合、あるいは300Mhz以下のCPUを搭載したマシン上で実行している場合は、適宜この値を大きくしてください。

11.1.6 サービス – アプリケーション間通信ポート

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: NTServiceSocket

最小値: 1
最大値: 65535
デフォルト値: 3300
タイプ: TCPポート番号

Kiwi Syslog Daemonの Manager はサービスとTCP3300ポートを使って通信を行います。2つのアプリケーションとの通信が可能です。サービスは表示するメッセージ、警告、統計情報を Manager に送り、受信したらすぐに表示できるようにします。他のプロセスが同じポートを使用している場合は、値を変更してください。

11.1.7 サービス – 依存性

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: NTServiceDependencies

デフォルト値: ブランク
タイプ: サービス名のテキスト 複数指定する際はセミコロン(;)で区切る
例: ServiceName1;ServiceName2;ServiceName3

サービスの依存性

大半のオペレーティングシステムでは、サービスは問題なく開始されます。Windows 2000 Serverシステムの一部には他のいくつかのシステムサービスの開始を待ってからでないと開始できないものもあります。そうしないと再起動後にコンソールの画面上に One or more system services failed to start (1つ以上のシステムサービスが開始されませんでした) というエラーメッセージが表示されます。

必要なサービスが確実に開始されてからKiwi Syslog Daemonが開始されるようにするには、上記のレジストリ設定を変更する必要があります。

サービスの依存性を追加する手順

- Manage メニューからサービスをアンインストールします。
- RegEdit を起動します。
- HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties セクションを表示します。
- NTServiceDependencies という文字列値を新規作成します。
- 最初に開始するサービスのリストが含まれるよう値を変更します。
- 例: LanmanWorkstation;TCPIP;WMI
- Manage メニューからサービスをインストールします。

上記の例では、Workstation、WMI (Windows Management Interface)およびTCP/IPの各スタックサービスが実行中であることを確認してからKiwi Syslog Daemonサービスの起動試行を行います。

11.1.8 サービス – デバッグ開始

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Options

キー: DebugStart

デバッグ有効: 1

デバッグ無効: 0

タイプ: 文字列

この値を1に設定するとサービスと Manager の両方が有効になります。

コマンドラインの値: DEBUGSTART

適用: Syslogd.exe、Syslogd_Service.exe、Syslogd_Manager.exe

効果:

レジスト値を1に設定してプログラムを実行すると、Kiwi Syslog Daemonをインストールしたフォルダの直下にデバッグファイルが作成されます。ファイル名は実行ファイルの名前によって異なります(下記参照)。デバッグファイルにはプログラムの起動とソケット初期化ルーチンの結果が記録されます。

作成されるファイル:

SyslogNormal = Syslogd_Startup.txt

SyslogService = Syslogd_Service_Startup.txt

SyslogManager = Syslogd_Manager_Startup.txt

使用タイミング:

プログラムが Input 設定オプションで指定したポートのメッセージを受信していないように見えるときは、起動デバッグファイルをチェックしてソケットの初期化が正常に行われたかどうか確認してください。

起動時にプログラムがクラッシュしているような場合に問題のありかを探す手助けになります。

コマンドラインオプションについては[関連項目](#)を参照してください。

11.1.9 DNS – ビジー時に待機を無効にする

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DNSDisableWaitWhenBusy

最小値: 0

最大値: 100

デフォルト値: 10

タイプ: パーセンテージ

ビジー時に待機を無効にする

通常、DNSキャッシュ内にIPアドレスが見つからない場合、プログラムはIPアドレスが解決されるまで一定時間待機します。負荷が高い環境下では、この遅延がメッセージ入力バッファを満杯にしまい、新しいメッセージを取りこぼす結果になることがあります。

このオプションは、入力メッセージバッファの最大容量を指定してそれを超えたらDNSの解決待機を無効にすることができます。デフォルトでは、入力バッファが10%に達するとKiwi Syslog Daemon はIPアドレスの解決待機を止めるようになっています。

プリアンプティブルックアップを有効にしていると、バックグラウンドでIPアドレス解決が続行され結果がキャッシュに入ります。このオプションはバッファに負荷がかかっている間のみ DNS timeout の待ち時間を無効にします。解決されるまで待たずにバッファに入ったメッセージを処理することができるようプログラムを開放します。

入力バッファレベルが設定値を下回ると、通常の解決待機タイムアウトが再び有効になります。

11.1.10 DNS – 最大キャッシュサイズ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DNSCacheMaxSize

フリーウェア版:

最小値: 50

最大値: 100

デフォルト値: 100

タイプ: キャッシュエントリーの最大数

正規登録版:

最小値: 50

最大値: 20000

デフォルト値: 5000

タイプ: キャッシュエントリーの最大数

キャッシュエントリーの最大数:

キャッシュバッファメモリーサイズを制限します。フリーウェア版は100エントリーまで、正規登録版では20,000エントリーまで可能です。キャッシュに保存したいIPアドレスの数を設定します。

11.1.11 DNSキャッシュの参照失敗

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DNSCacheFailedLookups

最小値: 0

最大値: 1

デフォルト値: 1

タイプ: 1=DNSキャッシュ参照失敗, 0=DNSキャッシュ参照成功

DNSキャッシュの失敗参照

失敗した参照をキャッシュに溜めることによってDNS名前解決をスピードアップします。DNSサーバーが有効な応答を返しているがその中に解決済みの名前が含まれていないようなとき、Kiwi Syslog Daemonはその応答をキャッシュに保存して同様の問合せがDNSサーバーに繰り返し送信されないようにします。このような処理は、DNSサーバー自体が未知のIPアドレスやホスト名をそのDNSサーバーに対して問い合わせるようなときに行われます。タイムアウトするのではなく、DNSサーバーからは NAME NOT FOUND という有効な応答が返されます。このような応答がキャッシュに溜められて検索できない名前の問合せが繰り返しDNSサーバーに送信されるのを防ぎます。失敗参照は Flush entries after X minutes で定義した間隔で消去されます。

11.1.12 DNS 設定- DNS/NetBIOS キューバッファバースト係数

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DNSSetupQueueBufferBurstCoefficient

最小値: 1

最大値: 50

デフォルト値: 10

タイプ: 内部キューバファから即待機解除されるDNS/NetBIOS要求の数

11.1.13 DNS 設定 - DNS/NetBIOS キューバッファクリア率

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DNSSetupQueueBufferClearRate

最小値: 1

最大値: 100
デフォルト値: 10
タイプ: DNS/NetBios内部キューバッファをクリアする割合

11.1.14 DNS 設定 - DNS/NetBIOS キュー制限

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties
キー: DNSSetupQueueLimit

最小値: 100
最大値: 30000
デフォルト値: 1000
タイプ: DNS/NetBIOS内部キューバッファのサイズ

11.1.15 DNS 設定 - デバッグモード

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties
キー: DNSSetupDebugModeOn

最小値: 0
最大値: 1
デフォルト値: 0
タイプ: DNS/NetBIOS詳細デバッグモード(on/off)

(1) に設定した場合、DNS/NetBIOSの詳細デバッグ要求と応答は {プログラムファイル}/Syslogd/DNS-debug.txt からアンロードされます。

11.1.16 メッセージバッファサイズ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: MsgBufferSize

フリーウェア版:
最小値: 100
最大値: 500
デフォルト値: 500
タイプ: メッセージバッファエントリーの最大数

登録正規版:
最小値: 100
最大値: 10,000,000 (1000万)
デフォルト値: 20,000
タイプ: メッセージバッファエントリーの最大数

メッセージバッファエントリーの最大数:

受信したメッセージ(UDP, TCP, SNMP, Keep Alive)は内部キューに入ります。次に、メッセージはキューから取り出され到着順(FIFO)に処理されます。処理エンジンがビジー状態のとき大量のメッセージを受信すると、メッセージはキューに入ります。そのため負荷が高い場合でもメッセージは失われません。

キューに入ったメッセージが消費するメモリーはわずかです。多くの場合、最大20,000 メッセージ分のバッファがあれば十分です。メッセージを大量に受信する場合は、バッファサイズを増やすことができます。バッファ処理はメッセージの流れをスムーズにし、処理エンジンがすべてのメッセージを処理しきれるようにします。

メッセージは1文字あたり2バイト使用するUnicodeで保存されます。つまり、100文字のメッセージであれば200バイトのメモリーが消費されます。メッセージは内容によりサイズが異なりますが、1件100文字あるとして20,000件のメッセージを保存するのに4,000,000バイト(4MB)のメモリーを使います。1件が200文字ならば8MBのメモリーを使うことになります。メモリーはメッセージがキューに入るときのみ使われます。通常量のトラフィックを処理する場合、処理エンジンはメッセージフローに十分追いつくため、メッセージがキューに入ることはありません。

11.1.17 Eメール – 件名追加テキスト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: MailAdditionalSubjectText

デフォルト値: ブランク

タイプ: テキスト

Eメール件名の前に追加するテキスト

日別統計およびアラームEメールの件名の先頭にテキストを追加します。日別統計とアラームEメールを多数のシスログデーモンから受信する場合、どのシスログデーモンから送信されたか識別するための情報を挿入する手段として利用できます。

シスログデーモンの名前やロケーションを簡潔に説明するテキストを指定してください。テキストはEメールの件名の先頭に追加されます。

例:

最大メッセージアラームEメールに通常使用される件名は次のとおりです。

Syslog Alarm: 16000 messages received this hour.

MailAdditionalSubjectText に [London] と設定すると、上記Eメールの件名は次のようになります。

[London] Syslog Alarm: 16000 messages received this hour.

件名と追加されるテキストの間には自動的にスペースが挿入されます。

次項も参照してください。

11.1.18 Eメール – 本文追加テキスト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: MailAdditionalBodyText

デフォルト値: ブランク

タイプ: テキスト

Eメール本文に追加するテキスト

ここでは日別統計およびアラームEメールに挿入する追加テキストを指定します。日別統計とアラームEメールを多数のシスログデーモンから受信する場合、どのシスログデーモンから送信されたか識別するための情報を挿入する手段として利用できます。

シスログデーモンの名前やロケーションを簡潔に説明するテキストを指定してください。テキストはEメールの本文の先頭に追加されます。

例:

通常送信される統計Eメールは次のようなものです。

```
///      Kiwi Syslog Daemon Statistics      ///
```

```
24 hour period ending on: Fri, 06 Feb 2004 13:04:55 +1300
Syslog Daemon started on: Fri, 06 Feb 2004 13:03:54
Syslog Daemon uptime:    24 hours, 0 minutes
-----
```

+ Messages received - Total: 20000
+ Messages received - Last 24 hours: 20000

MailAdditionalBodyText に London - Firewall Monitoring Syslog Daemon と設定すると、上記の日別統計Eメールは次のようになります:

```
///      Kiwi Syslog Daemon Statistics      ///
```

24 hour period ending on: Fri, 06 Feb 2004 13:04:55 +1300
Syslog Daemon started on: Fri, 06 Feb 2004 13:03:54
Syslog Daemon uptime: 24 hours, 0 minutes

+ Messages received - Total: 20000
+ Messages received - Last 24 hours: 20000

テキストの前後にはCRLFが追加され見やすくなっています。

前項も参照してください。

11.1.19 Eメール – 送信メッセージの制限

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: MailMaxMessageSend

最小値: 1
最大値: 1000
デフォルト値: 50
タイプ: メッセージ数

Eメールメッセージは一時的に内部キューに入り、それからまとめて送信されます。これはSMTP サーバー接続は1回でよいことを意味しています。各メッセージは別々に送られ、サーバーへの接続がクローズされます。

MailMaxMessageSend には1分間に送信されるメッセージの最大数を指定します。送信されなかったメッセージは再びキューに入り、1分後に再送信されます。

このオプションはメッセージ送信に制限があるSMSゲートウェイ経由で大量のEメールを送信する場合に有効です。メールサーバーの負荷を減少させ、数回に分けて送信することによってメッセージ負荷を分散させることも可能です。

11.1.20 ファイル書き込みキャッシュ

大量のメッセージを受信するとき、ファイル書き込みキャッシュにより Log to file アクションのパフォーマンスは大幅に向上します。

この機能を有効にすると、Log to File アクションはファイル書き込み前に指定した時間(秒)、または指定した数のメッセージをキャッシュに保存します。データはログファイルが更新されるまでメモリーのキャッシュに溜められます。これはメッセージ受信の都度ファイルに書くのに比べ効率的です。

出力ファイルごとにメモリーキャッシュが作成されます。通常の場合出力ファイルは一つですが、AutoSplit やフィルターを使ってメッセージを複数のファイルに分割しているときは複数の出力ファイルが生成されることもあります。

出力ファイルキャッシュが指定した時間の間使用されないと、リソース節約のためキャッシュは破棄されます。

プログラムが終了されると、キャッシュに溜められていたすべてのデータが該当するファイルに書き込まれるため、データが喪失されることはありません。

ファイル書き込みキャッシュを有効にするには

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: FileWriteCacheEnabled

最小値: 0
最大値: 1
デフォルト値: 1
タイプ: 有効 = 1, 無効 = 0

有効にすると、Log to File アクションはファイル書き込み前のデータを指定した時間、あるいは指定したメッセージ数に到達するまでキャッシュに保存します。データはログファイルが更新されるまでメモリーのキャッシュに溜められます。これはメッセージ受信の都度ファイルに書くのに比べ効率的です。

キャッシュのタイムアウト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: FileWriteCacheTimeout

最小値: 1
最大値: 120
デフォルト値: 5
タイプ: 秒

タイムアウト後キャッシュの内容はディスクに書き込まれます。タイマーは最初のメッセージがキャッシュに入った時点でスタートします。キャッシュがフルにならず、タイムアウトになるまで消去されずに残っている場合、キャッシュに溜まっているデータはディスクに書き込んだ後に消去されます。この設定ではメッセージをディスクに書き込むまでのキャッシュに溜める最大時間を指定します。ディスク書き込み回数が少ないほど、ファイルへのロギング処理の効率は高まります。

最大キャッシュエントリー数

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: FileWriteCacheEntries

最小値: 10
最大値: 100,000
デフォルト値: 1000
タイプ: キャッシュエントリーの最大数(メッセージ)

各出力ファイルに対して、ファイル書き込み前にキャッシュに保存するメッセージの最大数を指定します。

最大数に達するまで、あるいはタイムアウトになるまでメッセージはキャッシュに溜められます。ディスク書き込み回数が少ないほど、ファイルへのロギング処理の効率は高まります。メッセージは1文字あたり2バイト使用するUnicodeで保存されます。つまり、100文字のメッセージであれば200バイトのメモリーが消費されます。

1つのキャッシュに対する最大メモリーサイズ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: FileWriteCacheMaxSizeKB

最小値: 1
最大値: 2,000
デフォルト値: 50
タイプ: 最大サイズ/キャッシュ(KB)

最大キャッシュサイズ(KB)を設定します。キャッシュがこのサイズに達するとファイルに書き込まれます。

最大メモリーサイズに達するまで、あるいはタイムアウトになるまでメッセージはキャッシュに溜められます。ディスク書き込み回数が少ないほど、ファイルへのロギング処理の効率は高まります。メッセージは1文字あたり2バイト使用するUnicodeで保存されます。つまり、100文字のメッセージであれば200バイトのメモリーが消費されます。Out of Memory エラーが表示されたときは、この値を小さくするかファイル書き込みキャッシュを無効にしてください。

キャッシュクリーンアップ時間

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: FileWriteCacheCleanup

最小値: 10
最大値: 1440

デフォルト値: 10

タイプ: キャッシュを破棄する前に無効にする時間(分)

キャッシュが無効になりメッセージ受信をストップすると、クリーンアッププロセスによってキャッシュを破棄しリソースを開放します。クリーンアッププロセスはすでにファイルに書き出されている無効キャッシュのみを破棄しますので、データが喪失されることはありません。

ログファイルのロック

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: FileWriteCacheFileLock

最小値: 0

最大値: 1

デフォルト値: 0

タイプ: 有効 = 1, 無効 = 0

効率性を高めることとセキュリティ上の理由から、ログファイルは append shared モードで開くことができます。キャッシュへの書き込みが行われるたびにファイルを開閉する必要がないので効率的です。ファイルが開かれている間は、他のアプリケーションを起動して中身を変更したり、削除することはできません。新しいエントリーの追加のみが可能で、ファイルは読み取り専用で開くことができますが、変更はできません。

大量のsyslogメッセージを受信するとき、このオプションを有効にすることによってパフォーマンスを改善することができます。唯一の難点は、ファイルが新しいログエントリーをすぐには反映しないことです。OSは内部バッファがフルになるまでデータをキャッシュに溜め、それからファイルに書き出します。メッセージが多いときは、すぐにこの状態になりますが、少ないときはバッファがフルになりデータが書き出されるまでに時間がかかります。FileWriteCacheCleanup に指定した時間(分)の間キャッシュが無効になると、ログファイルは自動的に更新され閉じられます。

開いているログファイルの最大数

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: FileWriteCacheOpenFiles

最小値: 1

最大値: 250

デフォルト値: 100

タイプ: 最大数

FileWriteCacheFileLock が1(有効)のとき、各ログファイルは append shared モードで開いています。プログラムは同時に最大255ファイルまで開くことができます。ここでは同時に開くファイルの最大数を指定します。指定した数に達すると、現在のキャッシュの **FileWriteCacheFileLock** 値が無効になり、キャッシュへの書き込みが行われるたびにファイルが開閉されます。Log to File アクションで AutoSplit を使ってログホストごとに独立したファイルを作成するように設定されている場合、同時に255以上のファイルが開かれる可能性があります(255以上の有効な送信ホストがある場合)。適切なレベルでシステムリソースを利用するため、この値は100ファイルに設定することをお勧めします。

11.1.21 ファイルへの記録 – 日付区切り文字

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: LogFileDateSeparator

デフォルト値: "-" (ダッシュ)

タイプ: 文字または文字列

通常、現在の日付は YYYY-MM-DD 形式で表され、区切り文字としてダッシュ記号(-)が使用されています。区切り文字は自由に変更できます。例えば、スラッシュ(/)を用いる国もあります。

日付区切り文字を変更すると、使用する構文解析プログラム(パーサー)やレポート作成ツール(レポーター)によってはログファイルが読めなくなる可能性があるので注意してください。レポート作成ソフトウェアはダッシュ記号(-)を検索するものもあるので、見つからないとエラーを発生させることになるかもしれません。

この設定は次のフォーマットに対してのみ適用されます。

- Kiwi フォーマット ISO yyyy-mm-dd (タブ区切り)
- Kiwi フォーマット ISO UTC yyyy-mm-dd (タブ区切り)

使用例:

通常の Kiwi ISO ログファイルフォーマットのメッセージ:

```
2004-05-27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message
```

区切り文字をスラッシュ(/)に変更した場合:

```
2004/05/27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message
```

次項も参照してください。

11.1.22 ファイルへの記録 – 時間区切り文字

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: LogFileTimeSeparator

デフォルト値: ":" (コロン)

タイプ: 文字または文字列

通常、現在の日付は HH:MM:SS 形式で表され、区切り文字としてコロン記号(:)が使用されています。区切り文字は自由に変更できます。例えば、ドット(.)を用いる国もあります。

時間区切り文字を変更すると、使用する構文解析プログラム(パーサー)やレポート作成ツール(レポーター)によってはログファイルが読めなくなる可能性があるので注意してください。レポート作成ソフトウェアはコロン記号(:)を検索するものもあるので、見つからないとエラーを発生させることになるかもしれません。

この設定は次のフォーマットに対してのみ適用されます。

- Kiwi フォーマット ISO yyyy-mm-dd (タブ区切り)
- Kiwi フォーマット ISO UTC yyyy-mm-dd (タブ区切り)

使用例:

通常の Kiwi ISO ログファイルフォーマットのメッセージ:

```
2004-05-27 10:58:22 Kernel.Warning 192.168.0.1 kernel: This is a test message
```

区切り文字をドット(.)に変更した場合:

```
2004-05-27 10.58.22 Kernel.Warning 192.168.0.1 kernel: This is a test message
```

前項も参照してください。

11.1.23 ファイルへの記録 – エンコード形式

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: LogFileEncodingFormat

最小値: 0

最大値: 65535

デフォルト値: 1 (System)

タイプ: コードページ番号

通常、メッセージがログファイルに書き込まれるときはシステムのデフォルトエンコード形式(コードページ)が使用されます。デフォルトコードページの異なるシステムからメッセージを受信する場合の最良の対策は、UTF-8にエンコードして送受信することです。Kiwi Syslog Daemonには受信メッセージを内部でUnicodeに変換する機能があります。Unicodeメッセージをログファイルに書き込む際にはUTF-8(コードページ 65001)エンコードの使用をお勧めします。UTF-8は全Unicode文字セットを表すことができます。

大半のWindowsシステムで使用可能なコードページについては、次のWebページで確認してください。

<http://msdn.microsoft.com/ja-jp/library/aa288104.aspx>

以下は使用可能な標準コードページ番号です。

名前	コードページ番号	説明
System	1	システムコードページ
ANSI	0	ANSI
UTF-8	65001	Unicode Transformation Format 8
Shift-JIS	932	日本語
EUC-JP	51932	日本語(EUC)apanese Extended Unix Code
BIG5	950	繁体字中国語
Chinese	936	簡体字中国語

注：指定した番号がご使用のシステムで有効なコードページではない場合ファイルへのデータ書き込みは行われません。

不安があるときはUTF-8エンコードを使用してください。UTF-8はすべてのUnicode文字を処理できます。

UnicodeおよびUTF-8の詳細については次のWebページを参照してください。

<http://ja.wikipedia.org/wiki/UTF-8>

11.1.24 スクリプトエディター

この設定により、Edit Script ボタンが押されたときに起動するスクリプトエディターを変更することができます。デフォルトではスクリプトの編集にはメモ帳が起動します。この設定は Run Script アクションの設定ページに対してのみ適用されます。

スクリプトエディター

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ScriptEditor

デフォルト値: Notepad.exe

タイプ: スクリプトエディターのパスおよびファイル名

例: C:\Program files\MetaPad\MetaPad.exe

11.1.25 スクリプトのタイムアウト

スクリプトによっては他よりも実行時間が長くなるものがあります。スクリプトによってタイムアウトエラーが引き起こされるような場合、スクリプト実行のタイムアウト値を大きくしたい場合があります。スクリプトはリアルタイムで処理されるため、長いスクリプトを実行中にメッセージが喪失したり、キューに入った他のメッセージの処理に遅延が生じる可能性があります。複雑な長いスクリプトを実行するときは後処理として実行することをお勧めします。これを行うにはKiwi Syslog Daemonが作成するログファイルに対してWindows Scripting Hostを使用してスクリプトを実行します。リアルタイムで長いスクリプトを実行するのはできるだけ避けてください。

スクリプトのタイムアウト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ScriptTimeout

最小値: 0 (タイムアウトなし – 非推奨)

最大値: 60000

デフォルト値: 10000

タイプ: タイムアウト(ミリ秒 10000ミリ秒 = 10秒)

デフォルトではスクリプトの実行時間は最大10秒で、10秒経過するとタイムアウトします。スクリプトがリアルタイムでデータ処理を行うのに10秒以上かかる場合は、タイムアウト値を最大60秒まで大きくすることができます。タイムアウト値を0に設定するとスクリプトがタイムアウトしなくなります(スクリプトが無限ループ状態になったときにプログラムが落ちる可能性があるため、このように設定することはお勧めできません)。

11.1.26 データベースコマンドのタイムアウト

Log to Database アクションは指定したデータベースにレコードを挿入する際にADOを使用します。デフォルトではADOデータベースコマンドはデータベースがビジー状態のときや応答がない場合に30秒待ってからタイムアウトするようになっています。

エラーログにSDOコマンドのタイムアウトエラーが表示されている場合タイムアウト値を大きくすることができます。データベースレコードはリアルタイムに挿入されるため、タイムアウト値を大きくするとメッセージが喪失したり、キューに入った他のメッセージの処理に遅延が生じる可能性があります。この値を大きくするのはタイムアウトエラーが発生しているときのみに限ってください。

データベースコマンドのタイムアウト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DBCommandTimeout

最小値: 0 (No timeout - not recommended)
最大値: 120
デフォルト値: 30
タイプ: タイムアウト(秒)

デフォルトではデータベース挿入コマンドの実行時間は最大30秒で、30秒経過するとタイムアウトします。ご使用のデータベースが低速で、リアルタイムでデータ処理を行うのに30秒以降かかる場合は、タイムアウト値を最大120秒まで大きくすることができます。タイムアウト値を0に設定するとスクリプトがタイムアウトしなくなります(データベースが無応答になったときにプログラムが落ちる可能性があるため、このように設定することはお勧めできません)。

11.1.27 アーカイブ – 置き換え文字

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ArchiveFileReplacementChr

デフォルト値: "-" (ダッシュ)
タイプ: 文字、文字列

アーカイピングプロセスは現在のシステム日時を使ってアーカイブ後のファイルやフォルダ名に日時を追加します。

日付フォーマットはユーザーが選択できるため、ファイル名に使用できない文字が含まれていることがあります。アーカイピングプロセスはこのような不正文字 (& * + = : ; , / \ | ? < > 等) を有効な文字 (- 等) に置き換えて正しい名前の付いたファイルやフォルダを作成します。

例えば、システム日時が 2004/12/25 12:45:00 であれば、アーカイピングプロセスにより名前が 2004-12-25 12-45-00 に変換されます。この文字列がアーカイピングプロセスのファイルやフォルダ名となります。- ではなく他の文字を指定することもできます。不正な文字を指定すると、アーカイピングプロセスによって不正なファイルやフォルダが作成されてしまう可能性があるため注意してください。

11.1.28 アーカイブ – 区切り文字

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ArchiveFileSeparator

デフォルト値: "-" (ダッシュ)
タイプ: 文字、文字列

アーカイブスケジュールを Use dated file names に設定すると、既存のファイル名と現在のシステム日時の間に区切り文字が挿入されます。通常この文字はダッシュ(-)です。ダッシュ以外の文字を使用したいときは、このレジストリ設定を変更してください。

11.1.29 アーカイピング – 古いアーカイブ名規則を使用する

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: UseOldArchiveNaming

最小値: 0
最大値: 1
デフォルト値: 0 (無効)
タイプ: 数値

この設定はアーカイブタスクで1つのzipアーカイブを作成する際に適用されるデフォルトの命名規則を変更します。この値を (1) に設定するとKiwi Syslog Daemon 8.3.x以前のバージョンで使用されていたアーカイブ名規則が使用されるようになります。この設定の影響を受けるのは、1つのzipファイルに圧縮するアーカイブタスクのみです。

11.1.30 アーカイピング – アーカイブ処理時Tempフォルダのパス指定

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ArchiveTempPath

デフォルト値: (なし)
タイプ: 文字列

この設定はKiwi Syslog Daemonのアーカイバが使用するデフォルトの一時フォルダを変更します。デフォルトではWindowsの一時フォルダが使用されます(通常は C:\Windows\Temp または C:\Documents and Settings\\Local Settings\Temp)。

注:この設定は EnableArchiveTempFile が有効になっている場合のみ適用されます(次項参照)。

11.1.31 アーカイピング – Tempファイルを有効にする

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: EnableArchiveTempFile

最小値: 0
最大値: 1
デフォルト値: 0 (無効)
タイプ: 数値

この設定はデフォルトのアーカイブスケジューラタスクのデフォルトの振る舞いを変更します。

(1) に設定するとKiwi Syslog Daemonはアーカイブファイルの作成時に一時ファイルを生成するようになります。一時ファイルは1回のみ書き込み可能なメディア(CD-WORM)やネットワーク上にあるzipファイルに書き込む際に使用すると便利です。zipファイルは一時ファイルとして(通常はローカルドライブ上に)作成され、圧縮処理が終わると指定したドライブやネットワーク上に書き込むためです。

11.1.32 エラーログフォルダ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ErrorLogFolder

デフォルト値: プログラムのインストール先パス
タイプ: フォルダのパス (C:\My Logs\)

errorlog.txt ファイルには操作上生じたすべてのエラーが記録されます。通常このファイルはプログラムをインストールしたフォルダの下に作成されます。この値を変更するとerrorlog.txtファイルは指定した場所に作成され、そこにエラーが書き込まれるようになります。

11.1.33 メールログフォルダ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: MailLogFolder

デフォルト値: プログラムのインストール先パス
タイプ: フォルダのパス (C:\My Mail Logs\)

SendMailLog.txtファイルにはすべてのメールアクティビティが記録されます。通常このファイルはプログラムをインストールしたフォルダの下に作成されます。この値を変更するとSendMailLog.txtファイルは指定した場所に作成され、そこにメールアクティビティが書き込まれるようになります。

11.1.34 KRDP - ACKタイマー

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPACKTimer

最小値: 10
最大値: 65535
デフォルト値: 200
タイプ: ミリ秒

この設定はTCP_ACKプロトコルの確認タイマーの間隔を指定します。デフォルトではプロトコルは200ミリ秒ごとに受信パケットの確認(ACK)を行っています。

11.1.35 KRDP - キープアライブタイマー

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPKeepAliveTimer

最小値: 1
最大値: 65535
デフォルト値: 25
タイプ: ACKタイマーの間隔

この設定は接続済みセッションのキープアライブメッセージを送信する間隔を指定します。このカウンタはKRDPACKTimer の倍数となります。例えば、KRDPACKTimer が 200ms に設定されており5秒おきにキープアライブを送信したいときはこの値を25(25 x 200ms = 5秒)に指定する必要があります。

11.1.36 KRDP - ディスクキャッシュフォルダ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPCacheFolder

デフォルト値: InstallFolder\Cache\
タイプ: キャッシュフォルダのパス

この設定はディスクキャッシュファイルの保存先を指定します。ディスクキャッシュファイルはリモートホストがダウンしているとき、およびメモリキャッシュがフルになったときにのみ作成されます。

11.1.37 KRDP - Rx デバッグ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDP Rx Debug

最小値: 0

最大値: 1
デフォルト値: 0
タイプ: 有効/無効

この設定はKRDP受信イベントのデバッグログファイルの有効/無効を指定します。KRDP TCP受信機に関するすべてのイベントが対象となります。ログファイルはプログラムをインストールしたフォルダの下に KRDP RxDebug.txt という名前で作成されます。

KRDP受信機は Inputs の TCP オプションを有効にすることで作成されます。

11.1.38 KRDP - Tx デバッグ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDP TxDebug

最小値: 0
最大値: 1
デフォルト値: 0
タイプ: 有効/無効

この設定はKRDP送信イベントのデバッグログファイルの有効/無効を指定します。KRDP送信機に関するすべてのイベントが対象となります。ログファイルはプログラムをインストールしたフォルダの下に KRDP TxDebug.txt という名前で作成されます。

KRDP送信機は Forward to another host アクションを使って作成されます。

11.1.39 KRDP – キューサイズ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPQueueSize

最小値: 50
最大値: 200000
デフォルト値: 10000
タイプ: キューに入れるメッセージ数

この設定はKRDPおよびTCPメッセージのバッファリング時に使用されるメッセージキューのサイズを指定します。キューがフルになると、キューに溜まっていたデータはキャッシュファイルとして書き出されます。

11.1.40 KRDP – キューの最大サイズ(MB)

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPQueueMaxMBSize

最小値: 1
最大値: 100
デフォルト値: 20
タイプ: メモリーキューおよびキャッシュファイルの最大サイズ(MB)

バッファに入ったメッセージは個別にメモリーキューに追加され、メモリーキューのサイズは常に監視されています。キューの総サイズが KRDPQueueMaxMBSize の設定値に達すると、キューに溜まっているメッセージはキャッシュファイルに書き出されます。通常よりも大きなメッセージを受信したときにシステムメモリーを使い切らないようにするための対策です。

11.1.41 KRDP – 自動接続

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPAutoConnect

最小値: 0
最大値: 1
デフォルト値: 1
タイプ: 有効/無効

この値が1に設定されていると、KRDPおよびTCPメッセージの送信機はリモートホストへの自動接続を試みます。0に設定されていると、送信メッセージがキューに入った場合のみ接続されます。

11.1.42 KRDP - 接続時間

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPConnectTime

最小値: 5
最大値: 65535
デフォルト値: 5
タイプ: 秒

接続を再試行する間隔を指定します。リモートピアに対する接続が確立できないとき、KRDPConnectTime で指定した間隔(秒)で接続を試みます。

11.1.43 KRDP - 送信スピード

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPSENDspeed

最小値: 10
最大値: 10000
デフォルト値: 2000
タイプ: 送信メッセージ数/秒

1秒間に送信可能なメッセージの最大数を指定します。リモートピアに最速でメッセージを送信し受信機やネットワークリンクの過負荷を回避することができます。

11.1.44 KRDP - アイドルタイムアウト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPIdleTimeout

最小値: 0 (オフ)
最大値: 65535
デフォルト値: 60
タイプ: 秒

最終メッセージの送信後に送信ソケットを開けたままにする時間を指定します。TCPは接続時および切断時にオーバーヘッドが生じるため、TCPコネクションは一定時間新しい接続を開かずに次の送信メッセージが来るまでポートを開いたままにします。アイドル時間のカウンタはメッセージ送信直後から始まります。KRDPIdleTimeout で指定した時間内に送信メッセージが来なかった場合、接続ポートは閉じられます。

11.1.45 KRDP - SeqNumの追加

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: KRDPAddSeqToMsgText

最小値: 0
最大値: 1
デフォルト値: 0
タイプ: 有効/無効

この値が1に設定されていると、KRDP受信機は受信したシーケンス番号をメッセージテキストの末尾に追加します。シーケンス番号はコネクションIDごとに0~2147483647までの重複しない番号が割り当てられます。

追加されるタグの例: KRDP_Seq=1234

例

The quick brown fox jumped over the lazy dogs back KRDP_Seq=5742
The quick brown fox jumped over the lazy dogs back KRDP_Seq=5743
The quick brown fox jumped over the lazy dogs back KRDP_Seq=5744
The quick brown fox jumped over the lazy dogs back KRDP_Seq=5745

11.1.46 Syslogd プロセスのプライオリティ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: ProcessPriority

最小値: 0
最大値: 3
デフォルト値: 0
タイプ: Syslogプロセスのプライオリティ

このレジストリ設定が存在している場合、この値を指定することによってsyslogdのWindowsプライオリティを変更できます。

指定可能な値:

- 0 - LOW_PRIORITY
- 1 - BELOW_NORMAL_PRIORITY
- 2 - NORMAL_PRIORITY (default)
- 3 - ABOVE_NORMAL_PRIORITY
- 4 - HIGH_PRIORITY
- 5 - REALTIME_PRIORITY (注: この値に設定するとシステムがロックアップする可能性があります)

AboveNormal

Normal 以上 High 以下のプライオリティのプロセスに対して指定します。

BelowNormal

Idle 以上 Normal 以下のプライオリティのプロセスに対して指定します。

High

直ぐに実行する必要がある緊急度の高いタスクを実行するプロセスに対して指定します。Normal や Idle のプロセススレッドよりも先に処理されます。例えば、Task List などOSにかかる負荷を無視してでもユーザーに呼び出されたらすぐに応答する必要のあるプロセスに対して設定します。この値を適用すると、使用可能なほぼすべてのCPU時間が消費されるため使用するときには特に注意が必要です。

Low

システムがアイドルのときのみ実行されるスレッドのプロセスに対して指定します。この値の設定されたプロセススレッドはLow 以上のプライオリティクラスが設定されているプロセスの実行後に実行されます。スクリーンセーバーなどが該当します。プライオリティクラスが Idle のプロセスは子プロセスに引き継がれます。

Normal

特にスケジュールする必要のないプロセスに対して指定します。

Realtime

最優先のプロセスに対して指定します。この値の設定されたプロセススレッドは他のすべてのプロセスよりも先に実行されます。重要なタスクを実行するOSのプロセスなどがこれに該当します。例えば、非常に短い間隔でアルタイムプロセスが繰り返し実行されると、ディスクキャッシュへの書き込みが不能になったり、マウスが応答しなくなることがあります。

11.1.47 送信元アドレス - カスタムの開始 / 終了タグ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: OriginalAddressStartTag

デフォルト値: "Original Address="

タイプ: 送信元アドレスの開始タグ

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: OriginalAddressEndTag

デフォルト値: " " (空白)

タイプ: 送信元アドレスの終了タグ

通常syslogプロトコルはsyslogメッセージを転送/リレーしてしまうと送信元のアドレスを保持できません。送信者アドレスは受信したUDP/TCPパケットから取得されるためです。

Kiwi Syslog Daemonでは送信元アドレスを含むメッセージテキストにタグを付けることによってこの問題に対応できます。デフォルトでは Original Address=192.168.1.1 というタグが付けられます。すなわち Original Address= の後にIPアドレスと空白が来ます。

これらのタグは Forward to another host アクションで Retain the original source address of the message がチェックされているときのみ挿入されます。

[関連項目](#)を参照してください。

上記2つのレジストリキーを指定することによってデフォルトの開始タグおよび終了タグを変更できます。

例:

デフォルトの送信元アドレスタグ:

OriginalAddressStartTag = "Original Address="

OriginalAddressEndTag = " " (空白)

- 結果は Original Address=nnn.nnn.nnn.nnn となる。nnn.nnn.nnn.nnn には送信元のIPアドレスが入る。

新しい(カスタムの)送信元アドレスタグ:

OriginalAddressStartTag = "<ORIGIN>"

OriginalAddressEndTag = "</ORIGIN>"

- 結果は <ORIGIN>nnn.nnn.nnn.nnn</ORIGIN> となる。nnn.nnn.nnn.nnn には送信元のIPアドレスが入る。

新しい(カスタムの)送信元アドレスタグ:

OriginalAddressStartTag = "F="

OriginalAddressEndTag = " " (空白)

- 結果は F=nnn.nnn.nnn.nnn となる。nnn.nnn.nnn.nnn には送信元のIPアドレスが入る。

11.1.48 ルール - 最大ルール数

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Options

キー: MaxRuleCount

最小値: 10

最大値: 999

デフォルト値: 100

タイプ: Kiwi Syslog Daemonで設定可能なルールの上限数

注:

最大ルール数として100を超える値を設定しないでください。この値を大きくしすぎるとKiwi Syslog Daemonの実行速度が遅くなり、メモリ消費量が急激に増えます。ルール数の上限である100に近づいている場合は別の方法をとることをお勧めします。考えられる方法としてファイルロギングの autosplit 機能の利用が挙げられます。詳細については[関連項目](#)を参照してください。

11.1.49 データベースロガー - キャッシュクリアの頻度

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DBLoggerCacheClearRate

最小値: 10
最大値: 1000
デフォルト値: 1000 (ms)
タイプ: 数値

データベースキャッシュをチェックして未実行のSQLデータを確認する頻度(ミリ秒)を指定します。

11.1.50 データベースロガー - キャッシュのタイムアウト

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DBLoggerCacheTimeout

最小値: 1
最大値: 30
デフォルト値: 3 (日)
タイプ: 数値

未変更のキャッシュファイルの最大経過時間(日)を指定します。この値に達したデータベースキャッシュファイルはすべてシステムにより削除されます。

11.1.51 データベースロガー - データベースキャッシュを無効にする

セクション: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd\Properties

キー: DBLoggerCacheDisable

最小値: 0
最大値: 1
デフォルト値: 0 (有効)
タイプ: 数値

上記の設定はデータベースのデフォルトの振る舞いを変更します。

11.2 コマンドライン引数

Syslogd実行ファイル Syslog.exe、Syslogd_Manager.exe、Syslogd_Service.exe のいずれかの起動時には以下の項で挙げるコマンドラインパラメータが使用できます。パラメータは大文字、小文字を区別しません。複数のパラメータを指定する時はスペースで区切ってください。

11.2.1 起動時デバッグ

コマンドラインの値: DEBUGSTART

適用: Syslogd.exe, Syslogd_Service.exe & Syslogd_Manager.exe

効果:
上記のコマンドでプログラムを実行すると、Kiwi Syslog Daemonをインストールしたフォルダの直下にデバッグファイルが作成されます。ファイル名は実行ファイルの名前によって異なります(下記参照)。デバッグファイルにはプログラムの起動とソケット初期化ルーチンの結果が記録されます。

作成されるファイル:

SyslogNormal = Syslogd_Startup.txt
SyslogService = Syslogd_Service_Startup.txt
SyslogManager = Syslogd_Manager_Startup.txt

使用タイミング:

プログラムが Input 設定オプションで指定したポートのメッセージを受信していないように見えるときは、起動デバッグファイルをチェックしてソケットの初期化が正常に行われたかどうか確認してください。

起動時にプログラムがクラッシュしているような場合に問題のありかを探す手助けになります。

サービス版のデバッグ

サービス版ではコマンドライン引数を使用できません。レジストリでエントリを設定する必要があります。レジストリの設定については[関連項目](#)を参照してください。

11.2.2 サービス版のインストール

コマンドラインの値: -INSTALL

適用: Syslogd_Service.exe

効果:

Windows NT/2000マシンでKiwi Syslog Daemonをサービスとしてインストールします。成功/失敗を示すメッセージが表示されます。

使用タイミング:

Kiwi Syslog Daemon Service Managerの Manage メニューでインストールエラーが生じたとき、あるいはバッチファイルからサービス版の自動インストールを行う必要があるときにこの方法をお試しください。

Silent オプション:

コマンドの末尾に `-silent` を付けて実行するとインストールの成否を示すメッセージが表示されなくなります。

例: `-install-silent`

11.2.3 サービス版のアンインストール

コマンドラインの値: -UNINSTALL

適用: Syslogd_Service.exe

効果:

Windows NT/2000マシンからKiwi Syslog Daemon サービス版をアンインストールします。成功/失敗を示すメッセージが表示されます。

使用タイミング:

Kiwi Syslog Daemon Service Managerの Manage メニューでアンインストールエラーが生じたとき、あるいはバッチファイルからサービス版の自動インストール/アンインストールを行う必要があるときにこの方法をお試しください。

アンインストールを始める前にサービスが停止していることを確認してください。

コマンドラインから `net stop` コマンドを実行しても同じことができます。

例: `net stop "Kiwi Syslog Daemon"`

Silent オプション:

コマンドの末尾に `-silent` を付けて実行するとアンインストールの成否を示すメッセージが表示されなくなります。

例: `-uninstall-silent`

11.3 Kiwi Syslog Daemon の自動インストール

Kiwi Syslog Daemonでは一切人の手を煩わせずにインストールと設定作業を自動的に行うことができます。

標準の対話式アプリケーションとしてKiwi Syslog Daemonをインストールし、使用するにはバッチファイルを作成する必要があります。バッチファイルには以下の情報が記述されている必要があります。

```
"AppPath\Kiwi_Syslogd_X.X.X.setup.exe" /S INSTALL=APP /D=InstallPath  
"InstallPath\Syslogd.exe"
```

Windows NTのサービスとしてKiwi Syslog Daemonをインストールし、使用するにはバッチファイルを作成する必要があります。バッチファイルには以下の情報が記述されている必要があります。

```
"AppPath\Kiwi_Syslogd_X.X.X.setup.exe" /S INSTALL=SERVICE /D= InstallPath
```

インストーラからライセンスキーを適用するには、次のように入力してライセンス登録内容をプログラムに渡してください。

```
"AppPath\Kiwi_Syslogd_X.X.X.setup.exe REGKEY="Name|Company|E-mail|Serial|Key"
```

インストールが完了すると自動的にソフトウェアのライセンスが登録されます。

/Dスイッチを確実に最後の変数として使用する必要がある場合はすべてのスイッチを結合することができます。

```
"AppPath\Kiwi_Syslogd_X.X.X.setup.exe REGKEY="..." / S INSTALL=SERVICE /D="InstallPath"
```

また、Kiwi Syslog Daemonに自動的に定義済みのコンフィグレーション設定を適用し、アプリケーションやサービスの初回起動時にロードすることも可能です。

詳細については、[関連項目](#)を参照してください。

- * AppPath の部分にはインストール用パッケージ(Kiwi_Syslogd_X.X.X.setup.exe)が実際に置かれているパスを入力します。
- * 二重引用符は AppPath 等に空白が含まれている場合には付ける必要があります。例："C:\ProgramFiles\"

11.4 設定にINI ファイルを使用

通常、プログラムの設定値は起動時にレジストリから読み込まれます。リモートマシンから設定を変更したい場合は、特別なINI ファイルをインストール先のフォルダに置き、そこから設定をロードしてください。このINIファイルはリモートマシンのフォルダにコピーできます。次にプログラムを起動する際にはそのINIファイルから設定が読み込まれ、レジストリに書き出されます。次の起動からはこのレジストリ値が読み込まれます。いったん設定が読み込まれると、INIファイルは削除されます。INIファイルが削除されないようにするには、ファイル属性を読み取り専用に変更します。

プログラムは起動時にインストール先フォルダ(通常はC:\Program files\Syslogd)にある LoadNewSettings.ini を検索します。ファイルが見つかったところから設定が読み込まれ、通常のSyslogdレジストリキー: HKEY_LOCAL_MACHINE\SOFTWARE\Kiwi Enterprises\Syslogd の下のレジストリに置かれます。いったんファイルが読み込まれると削除されるため、再度同じファイルが読み込まれることはありません。プログラムはレジストリから設定を読み込み通常どおり起動します。INIファイルに記述されている設定は既存のレジストリ設定を上書きします。

INIファイルはKiwi Syslog Daemon のINIファイルとして有効であればどんなものでもかまいません。File の Export メニューまたは Setup 画面の Defaults/Import/Export で設定のエクスポートができます

INIファイルは手動で変更するものではありません。ルール、アクション、フィルターの設定の多くはエンコードされているためです。しかし、ドライブ文字を変更(D:をC:に変更する等)する目的でやむなく手動で設定変更する場合には、メモ帳の検索と置換機能を使って変更してください。エンコードされている文字列は変更しないよう注意してください。INIファイルを読み込む際に予期せぬエラーが発生することがあります。

心配なときは下記までお問合せください。
<http://www.kiwisyslog.com/support/>

12 Kiwi社のソフトウェア製品

12.1 Kiwi CatTools

Kiwi CatToolsはルーター、スイッチ、ファイアウォールなどのデバイスのコンフィグレーションを自動管理する目的で開発されたフリーウェアです。

Cisco / 3Com / Extreme / Foundry / HP / Netscreen / Multicom 製デバイス、その他多くの機器に対応しています。

Kiwi CatToolsが実行する多くのタスクの中でも次の機能・特長は日々の管理業務の効率化に大いに貢献します。

- コンフィグレーションの自動バックアップと変更が加えられたときにすぐさま電子メールで管理者に連絡が入るEメール通知機能。
- 多数のデバイスに対しTelnetやSSHを通じてコマンドを同時に実行
- スケジュールに従いコンフィグレーションを自動的に変更
- すべてのネットワークデバイスのパスワードを一括変更

本製品はスクリプトに完全対応したコンフィグレーション管理ツールでもあり、Telnet、SSHなどをサポートするTFTPサーバーが内蔵されています。

Kiwi CatToolsの詳細については弊社Webサイトを参照してください。プログラムのダウンロードもできます。

<http://www.kiwisyslog.com/>

12.2 Kiwi SyslogGen

Windows 95/98/ME/NT4/2000/XP用のsyslogメッセージジェネレータです。

Kiwi SyslogGenはGUIからUnixタイプのsyslogメッセージを生成しKiwi Syslog Daemon実行ホストに送信します。

Kiwi SyslogGenはKiwi Syslog Daemonの設定と通信に問題がないかどうかをテストする目的で使用することもできます。

機能・特長:

- ランダムに Facility と Level を組み合わせてプライオリティを設定可能
- 既成またはユーザー入力によるメッセージ生成
- 配信頻度(1回のみ、毎秒、毎分、連続、バーストモードから選択)
- Kiwi Syslog Daemonに互換性のあるメッセージをプロキシ送信*
- ランダムに不正パケットを発生させてKiwi Syslog Daemonサーバーの耐障害性能をテスト

* プロキシ送信すると、Kiwi Syslog Daemonサーバーから他のサーバーにホスト名フィールドに書かれている送信元のIPアドレスを保持した状態でメッセージを送ることができます。

Kiwi SyslogGenの詳細については弊社Webサイトを参照してください。プログラムのダウンロードもできます。

<http://www.kiwisyslog.com/>

12.3 Kiwi Logfile Viewer

Kiwi Logfile ViewerはWindows 95/98/ME/NT4/2000/XP用のフリーウェアです。

Kiwi Syslog Daemonによって生成されたタブ区切りログファイルを簡単に、読み易く表示します。

機能・特長:

- 列ソート
- ドラッグ&ドロップで列の並び替え
- タブ区切りファイルフォーマットで出力
- カンマ区切りファイルフォーマットで出力
- ブラウザ用にHTMLテーブルで出力.
- タブ区切りファイルの読み込み
- カンマ区切りファイルの読み込み
- コマンドラインオプションとスイッチ
- ヘッダーに標準syslogフィールドのタイトルを使用可能
- デフォルトの振る舞いを設定可能

Kiwi Logfile Viewerの詳細については弊社Webサイトを参照してください。プログラムのダウンロードもできます。

<http://www.kiwisyslog.com/>

12.4 Kiwi Secure Tunnel

Kiwi Secure TunnelはKiwi Syslog Daemon(あるいは互換性のあるシスログデーモン)と併用するWindows用セキュアトンネルサービスを提供するフリーウェアです。ネットワーク上に分散している各種デバイスから送信されたsisylogメッセージを受信し、圧縮・暗号化して安全にKiwi Syslog Daemonに転送します。

Kiwi Secure Tunnelはサービス版のみで、Windows NT4/2000/XP/2003をサポートしています。Kiwi Secure Tunnel ManagerプログラムにはWindows NTサービスの設定・管理を行うためのインターフェイスが付属しています。

Kiwi Secure Tunnelはクライアント1台とサーバー1台で構成されます。

トンネルとなるクライアントはネットワーク上に設置されている1台以上のデバイスから送信されたメッセージを収集し、安全なリンクを通じてトンネルサーバーに転送します。

トンネルサーバーは受信したメッセージを1台以上のKiwi Syslog Daemonサーバーに転送します。

また、選択したファイルの内容を監視し、これらのファイルから送信されたデータをsyslogメッセージとしてKiwi Syslog Daemonに送信することができます。

Kiwi Secure Tunnelの詳細については弊社Webサイトを参照してください。プログラムのダウンロードもできます。

<http://www.kiwisyslog.com/>

1 Hour history, 111
 24 Hour history, 111
 3com, 116
 3Com, 117
 About Kiwi Syslog, 17
 Action - Display, 30
 Action - E-mail message, 39
 Action - Forward to another host, 36
 Action - Log to file, 30
 Action - Log to NT Event log, 46
 Action - Log to ODBC database, 43
 Action - Play a sound, 38
 Action - Run external program, 38
 Action - Run Script, 50
 Action - Send ICQ instant message, 48
 Action - Send SMS or pager message via NotePager Pro, 47
 Action - Send Syslog message, 42
 Additional text or message to be added to the e-mail body, 150
 Additional text or message to be added to the e-mail subject, 150
 Adjust column widths automatically, 110
 Adjust width to fit screen, 13
 ADSL, 127
 allied telesyn, 118
 Always on top, 109
 An example alarm message, 101
 An example Syslog Statistics message, 102
 Archive time options, 72
 Arris, 118
 Arris Cable Modem, 118
 AT, 118
 Audible Alarm, 102
 AutoSplit values, 30
 bay networks, 120
 Bay Networks, 132
 BCC, 132
 Beep on every message received, 107
 Bintech, 123
 Blink System Tray Icon when receiving messages, 110
 catalyst, 124
 Choose font, 14
 cisco, 124, 125
 Cisco, 124
 Cisco PIX Firewall (TCP), 107
 Clear display, 13
 Complex filter, 19
 Configuring a 3Com NetServer, 116
 Configuring a 3Com Total Control Chassis, 117
 Configuring a Bay Networks router, 120
 Configuring a Cisco Catalyst switch, 124
 Configuring a Cisco PIX to send syslog messages, 124
 configuring a cisco router to send syslog, 125
 Configuring a DLink840V, 126
 Configuring a HP JetDirect Printer, 127
 Configuring a Lucent Router, 128
 Configuring a Netgear / ZyXEL RT311/RT314, 130
 Configuring a Netgear FVS318 VPN Firewall, 130
 Configuring a Netgear RP114 Router, 131
 Configuring a WatchGuard SOHO firewall, 135
 Configuring a W-Linx MB Broadband router, 136
 Configuring a Zyxel ZyWALL 10, 136
 Configuring an Arris Cable Modem Termination System, 118
 Copy display to clipboard, 11
 Counters, 112
 Custom DB formats, 93
 Custom file formats, 92
 Debug options, 11
 Debug options - Apply new settings to Syslogd service, 16
 Debug options - Clear the service DNS Cache, 16
 Debug options - Display the Service version, 15
 Debug options - Get diagnostic information, 15
 Debug options - Reset the Syslogd service, 16
 Debug options - Retrieve last messages, 16
 Debug options - Send keep alive, 16
 Disclaimer, 8, 9
 dlink, 126
 DLINK 840V, 126
 DNS - Max cache size, 147, 148
 DNS query timeout, 96
 DShield.org, 135
 E-mail alarm and statistics options, 99
 Enter the registration details (F2), 17
 Exit, 12
 Export settings to INI file, 11
 Features in the free version, 6
 Features in the registered version, 7
 Feedback - Comments or Bugs, 8
 Firebox, 135
 firewall, 127, 128, 130, 134, 135, 136
 Freesco, 127
 FVS318, 130
 Guide to initial Syslog Daemon Setup, 17
 Help Topics, 16
 How the log file archiving works, 70
 How the rule engine works, 18
 How to navigate using the keyboard, 17, 18
 How to purchase the registered version., 8
 HP, 127
 IDScenter, 132
 Importing and Exporting a filter definition, 29, 30
 Install the Syslogd service, 15
 Installing the Service edition, 113
 InternetGate, 127
 IP Address Range filter, 23
 IP Subnet Mask filter, 24
 jetdirect, 127
 Join the mailing list, 17
 keep alive, 107
 keepalive, 107
 keep-alive, 107
 Kiwi Logfile Viewer, 166
 Kiwi Syslog Daemon Service Edition, 113
 Kiwi Syslog FAQ, 16
 Kiwi Syslog Help (F1), 16
 Kiwi SyslogGen, 166
 linksys, 127, 128

- LinkSys firewall, 127, 128
- Log file formats, 34
- lucent, 128
- Lucent, 128
- Make a suggestion or report a bug, 17
- Manage menu, 14
- Managing the service edition, 114
- maximum e-mail messages sent per minute, 151
- MB-401X, 136
- Message buffer size, 149
- Minimize to System Tray on start-up, 109
- netgear, 130, 131
- Netscreen firewall, 131
- Netscreen25, 131
- netserver, 116
- Normal Syslog (UDP port 514), 103
- nortel, 120
- Nortel, 132
- Notify by Mail, 102
- Pack X, 132
- Paging, 47
- Ping the Syslogd service, 15
- PIX, 124
- printer, 127
- Priority filter, 24
- Problems logging when running as a Service, 46
- Properties, 10, 12
- Purchase the registered version, 17
- Purge, 11
- Registry settings for Kiwi Syslog Daemon, 144
- Regular Expression filter, 20
- Resolve IP addresses found within the syslog message text, 95
- router, 125, 127, 128, 131
- Router, 132
- Rows of scrolling display, 109
- RP114, 131
- RT311, 130
- RT314, 130
- Run Program, 103
- Scripting
 - VBScript
 - JScript
 - Initial script, 99
- Send Test message to local host (Ctrl-T), 11
- Service - Install Service, 164
- Service - Inter-App communication port, 146
- Service - Properties Update Timeout, 146
- Service - Start/Stop Timeout, 145
- Service - Uninstall Service, 164
- Setting the log insertion type, 46
- Setup - Archiving, 70
- Setup - Input options, 103
- Setup - Inputs - Keep-alive, 107
- Setup - SNMP logging, 105
- Severity, 111
- Show Hostname instead of IP number (resolve to Hostname), 95
- Show messages per hour in title bar, 109
- Show the hostname only (remove the domain name), 95
- Show the Syslogd service state, 15
- Simple filter, 18
- SMS message, 47
- snapgear, 133
- SnapGear SOHO+, 133
- SNORT, 132
- Software License Agreement, 8
- soho, 133
- SOHO, 135
- soho plus, 133
- sonicwall, 133
- SonicWall, 133
- Start the Syslogd service, 15
- Start-up Debug, 147
- Statistics delivery time, 145
- Steps to installing the new version, 114
- Steps to remove existing version, 114
- Stop the Syslogd service, 15
- support@kiwisyslog.com, 165
- symantec, 134
- Symantec Firewall/VPN 200, 134
- Syslog Facilities, 137
- Syslog Levels, 138
- Syslog Priority values, 139
- Syslog RFC 3164 header format, 140
- sysloggen, 166
- TCP vs. UDP logging, 104
- Thanks, 10
- The error log, 137
- The main display window, 10
- The SMTP mail log, 137
- Threshold filter, 28
- Time Interval filter, 27
- Time of Day filter, 26
- Timeout filter, 29
- To configure an ODBC database DSN, 46
- To view the e-mail log file, 137
- To view the error log file, 137
- Top 20 Hosts, 111
- total control, 117
- Transport, 139
- Troubleshooting, 143
- Troubleshooting the Service edition, 114
- TXT message, 47
- Uninstall the Syslogd service, 15
- Upgrading to a new version of Kiwi Syslog Daemon NT Service, 114
- Use 3D titles, 109
- Use a local DNS cache (improves speed), 96, 97
- Use dd-mm-yyyy date format (non US format), 109
- View e-mail log file, 12
- View error log file, 12
- View syslog statistics, 12
- vpn, 130
- VPN, 128
- vpn 200, 134
- VPN3000, 124
- Wallpaper, 99
- watchguard, 135
- Watchguard, 135
- Word wrap, 110

zywall, 136
Zyxel, 130

zyzel, 136