

BA8000 Pro
ログ機能利用ガイド

BA8000 Pro

株式会社NTT-ME

はじめに

・本ガイドはBA8000 Proのログ機能の利用方法を説明したものです。

更新履歴	初版 2002 年 12 月 25 日
------	---------------------

BA8000 Proのログ機能について

BA8000Proにおいては

syslog機能
メールによるログ配信機能
設定画面でのログ表示

の3種類のログ機能により本体の動作状態の確認を行うことができます。

syslog機能

syslogとは、syslogメッセージ(ログ)を、ネットワーク上に存在するsyslogデーモン(サーバ)に出力する機能です。syslogデーモン側でファイル保存しておくことができ、長期間のログ収集に適しています。本製品のsyslog機能を利用するためには、ネットワーク上にsyslogデーモン(サーバ)を用意する必要があります。

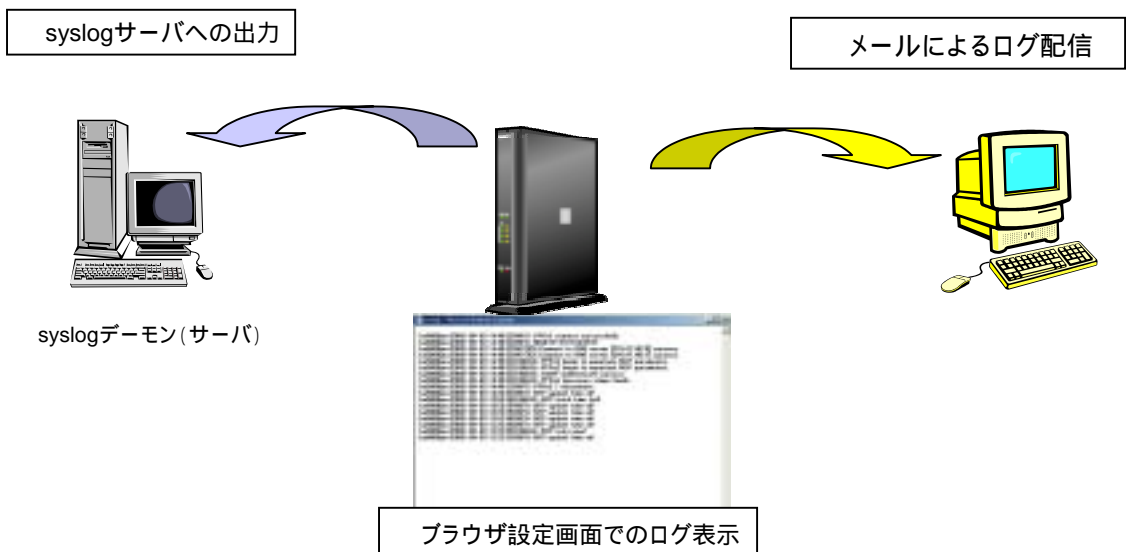
メールによるログ配信機能

BA8000 Proでは指定したアドレスにメールによるログ配信も可能です。ログ配信は毎日決まった時間に行う、DoS攻撃検出時、メモリー一杯時に配信する、から選択することが可能です。

設定画面でのログ表示

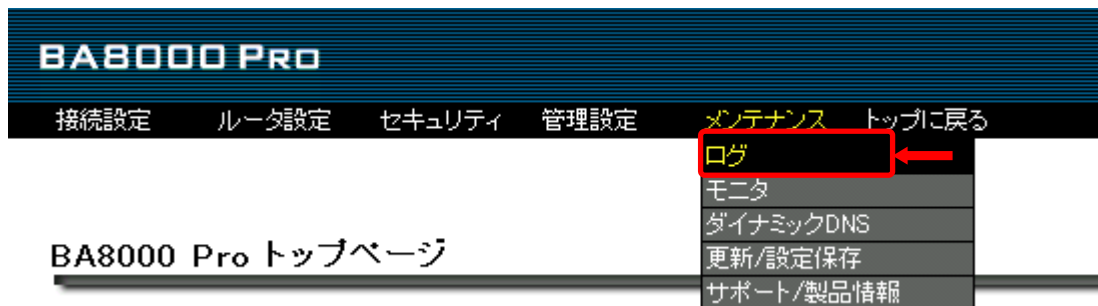
ブラウザ設定画面上でログを確認することができます。

BA8000Proのログ機能



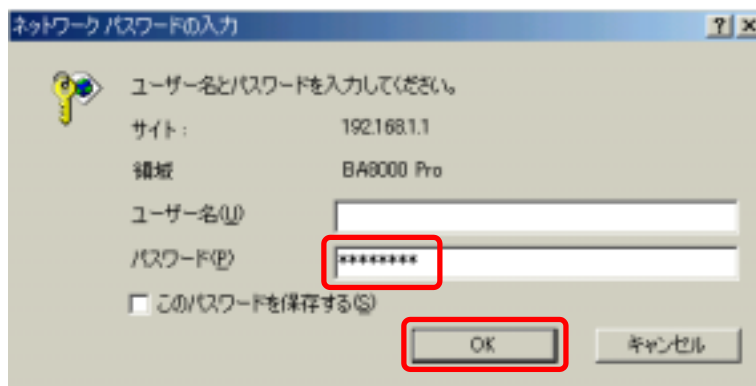
静的フィルタ設定手順

1. WebブラウザのURL欄に「http://192.168.1.1/」と入力し「Enter」キーを押します。
BA8000 Pro設定画面のトップページが表示されますので**[メンテナンス]**の**[ログ]**を選択して下さい。



ユーザ名/パスワード入力画面が表示されます。パスワード欄に「password」を入力し**[OK]**ボタンをクリックします。

上記は工場出荷時のパスワードです。パスワードを変更している場合は設定してあるパスワードを入力してください。



3. 各パラメータの設定を行ってください。
最後に**[設定]**ボタンを押して**[再起動]**してください。

ログ

本製品の状態を記録するログの設定を行います。

ログ方法	<input checked="" type="checkbox"/> syslog <input checked="" type="checkbox"/> E-mail <input checked="" type="checkbox"/> WWW設定画面
syslogレベル	<input checked="" type="checkbox"/> info <input checked="" type="checkbox"/> notice <input checked="" type="checkbox"/> Debug
syslogサーバIPアドレス	192 . 168 . 1 . 20
SMTPサーバIPアドレス	210 . 153 . 1 . 199
送信先メールアドレス	ba8000@ntt-me.co.jp
送信元メールアドレス	ba8000@pluto.plala.or.jp
ログメールの件名	Log report
メール送信トリガ	<input checked="" type="checkbox"/> DoS攻撃検出時 <input type="checkbox"/> メモリー一杯時
	<input checked="" type="checkbox"/> 毎日 12 時 00 分

設定

やり直し

ログ方法

syslog:

ここにチェックを入れると、syslogパケットを利用して本製品の状態をsyslogサーバに送信します。以下の**[syslogサーバIPアドレス]**も設定してください。

E-mail:

ここにチェックを入れると、本製品の状態をインターネットメールで送信します。以下の**[SMTPサーバIPアドレス]**、**[送信先メールアドレス]**、**[送信元メールアドレス]**、**[ログメールの件名]**、**[メール送信トリガ]**も設定してください。

WWW設定画面:

ここにチェックを入れると、本製品の状態をこのページで確認することができます。確認する場合は**[ログ表示]**ボタンをクリックしてください。

syslogレベル

syslogメッセージとして出力する情報の種類を選択します。

- infoレベル : 通常の情報ログします。
- noticeレベル : Port Scan攻撃やDos攻撃を検知した場合、攻撃情報をログします。
エラーが発生した場合、エラー情報をログします。
- debugレベル : 障害解析等のために、PPPoE接続シーケンス等のデバッグ情報をログします。

「debug」レベルにチェックを入れると、場合によっては大量のログが生成されることがあります。
無駄なトラフィックが発生したり本製品の動作が遅くなるなどの弊害が発生しますのでご注意ください。

syslogサーバIPアドレス

syslogメッセージの送信先になる、syslogデーモン(サーバ)のIPアドレスを入力します。

syslogデーモンの一例(フリーウェアソフト等)

- ・Unix系OSの場合: syslogdをご使用ください。
- ・Windows系OSの場合: 以下のフリーウェアソフトがあります。
 - syslogd
<http://www.winsite.com/info/pc/win3/winsock/syslogd.zip/>
 - 3CDaemon
http://infodeli.3com.com/software/utilities_for_windows_32_bit.htm
- ・MAC OSの場合: 以下のフリーウェアソフトがあります。
 - Mac NetLogger
<http://www.laffeycomputer.com/netlogger.html>

SMTPサーバIPアドレス

本製品はメールによるログ配信も可能です。メールによるログ配信を行う場合は、メールサーバ(SMTP)のIPアドレスを入力してください。ただしホスト名入力できません。

プロバイダのメールサーバを指定する場合、SMTPサーバのIPアドレスはご利用のプロバイダに確認いただくかnslookupでご確認ください。
ここで入力したSMTPサーバは『新ファーム公開お知らせ機能』でも利用されます。

宛先メールアドレス

メールによるログ配信を行う場合、宛先メールアドレス(To:)を入力してください。このメールアドレスにログメールが送信されます。

例: infoba@ntt-me.co.jp

ここで入力した宛先メールアドレスは『新ファーム公開お知らせ機能』でも利用されます。

送信元メールアドレス

メールによるログ配信を行う場合、そのメールの送信元メールアドレス(From:)を入力してください。ネットワーク管理者のメールアドレスなどを推奨します。

ここで入力した送信元メールアドレスは『新ファーム公開お知らせ機能』でも利用されます。

ログメールの件名

メールによるログ配信を行う場合、そのメールの件名 (Subject:) を入力してください。

設定可能な文字: 半角英数字 例: Log report

ログメール送信トリガ

どのタイミングでログメールを送信するか設定します。以下のオプションから選択してください。

DoS攻撃検出時:

本製品がDoS攻撃を検出した時に、ログメールを送信します。

メモリー一杯時:

ログ情報は本製品のメモリー上に記憶されます。ログが溜まりメモリーに余裕が無くなった時にログメール送信します。

毎日:

毎日決まった時間に、ログメールを送信します。送信時刻も入力してください

4. ログ内容をブラウザ設定画面で確認する場合は[ログ内容表示]ボタンを、ログメールを手動で送信する場合は[ログメール送信]ボタンを押してください。

毎日 時 分



ログ内容表示 : 現在のログ内容を表示します。

ログ内容消去 : 現在本製品のメモリーに記憶されているログを消去します。

ログメール送信 : メールログを手動で送信します。

ログ出力の一例

・PPPoE関連

レベル	出力	内容
Info	Start connecting to remote PPPoE server.	PPPoE接続開始時
Info	PPP/PAP authentication failure. Name:*** Password:***.	PAP認証失敗
Info	PPP/CHAP authentication failure. Name:*** Password:***.	CHAP認証失敗
Info	PPPoE server IP is:***.	PPPoE接続成功でIPCP開始時、 PPPoEサーバIP
Info	PPPoE server assign IP address is:***.	IPCP成功時、取得IP
Info	Get Primary DNS:*** Secondary DNS:***.	IPCP成功時、取得DNS

・DHCP関連

レベル	出力	内容
Info	DHCP server allocate IP *** to client pc ,which MAC is ***.	DHCPクライアントによるIP取得時
Notice	No more available address in the DHCP server pool.	スコープ一杯時
Debug	Unknown DHCP message type.	unknown DHCPメッセージ受信時
Debug	Receive the invalid DHCPRELEASE.	不正なDHCP release受信時
Debug	Receive DHCPRELEASE, but can't find binding for such client.	不明なDHCP release受信時

・NTP関連

レベル	出力	内容
Info	NTP get time success.Now is ***.	NTP時刻取得時
Notice	NTP get time failed.	NTP時刻取得失敗時
Info	User set time manually.Now is ***.	手動時刻設定

・DNS関連

レベル	出力	内容
Info	DHCP client get DNS.Primary DNS is *** secondary DNS is *** third DNS is ***.	DHCPクライアントによるDNSアドレス取得
Debug	DNS query from IP: ***, Match policy, (Policy info).	DNSルート一致かつ転送時、()内は下記参照。
Debug	DNS query from IP: ***, Match policy, (Policy info), Rejected.	DNSルート一致かつ破棄時、()内は下記参照。

・フィルタリング関連

レベル	出力	内容
Debug	Packet (Packet info) Match routing policy. Rule ID ***, Destination interface ***	ポリシールート一致時、()内は下記参照。
Debug	Packet (Packet info) Match static filter, PASS. Rule (Rule info)	静的フィルタpassルール一致時、()内は下記参照。
Debug	Packet (Packet info) Match static filter, DISCARD. Rule (Rule info)	静的フィルタdiscardルール一致時、()内は下記参照。
Debug	Packet (Packet info) Match dynamic filter trigger, Rule (Rule info)	動的フィルタTriggerルール一致時、()内は下記参照。
Debug	Packet (Packet info) Match dynamic filter action, Rule (Rule info)	動的フィルタActionルール一致時、()内は下記参照。
Debug	HTTP Packet Match web restrict, (Block info), Request from ***	WWW制限一致時、()内は下記参照

- (Packet Info) Direction : ***, ID : ***, Protocol ***, source IP ***, destination IP ***, source port ***, destination IP ***
- (Rule Info) Direction : ***, ID : ***
- (Policy Info) 転送時: Policy ID: ***, URL: ***, DNS server IP: ***, Interface ***
- (Policy Info) 破棄時: Policy ID: ***, URL: ***
- (Block Info) ActiveX: ActiveX filtered, File name: ***
- Java: Java filtered, File name: ***
- Cookie: Cookie blocked
- Proxy: Proxy blocked

ログ機能のご利用上の注意

- ・syslogレベルとして「debug」レベルにチェックを入れると、場合によっては大量のログが生成されることがあり、無駄なトラフィックの発生や本製品の動作が遅くなるなどの弊害が発生しますのでご注意ください。
- ・『TCP session FIN Wait timeout.』は、TCPコネクションを張っている両端のホストのどちらかがFinを送出しから指定した時間が過ぎたらログ出力されるものです。アプリケーションによってはFinパケットを出さないものがあり、そのためBA8000 Proでは一定時間経過後timeoutとしてセッションを終了する仕様になっています。これは正常な動作であり、問題はありません。