

# **Innominate** **mGuard**

## Innominate mGuard Security Appliance 設定事例 – Logging

平成19年1月  
アルテック・エーディエス株式会社  
オプト&ネットワーク事業部

## Logging/ 設定

Logging の項目では、mGuard の Log 関係を設定します。

以下の設定の説明をします。

設定(システムログサーバの設定)

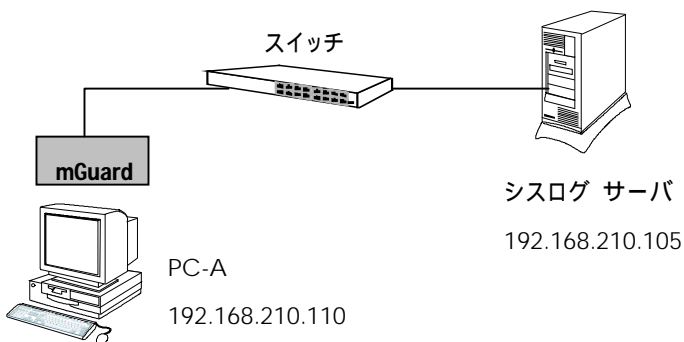
ローカルログの閲覧

mGuard メニューから Logging >> 設定



### リモート Logging

mGuard のログ・エントリーは全て mGuard の一時メモリーに記録されます。ログ用に使用可能なメモリーが一杯になると、古い順にログ・エントリーが上書きされます。更に mGuard の電源を切ると全てのログ・エントリーが削除されます。ログを保存するには、ログ・エントリーを外部のシステムログサーバへ送信することができます。この機能は、ログを集中管理したい場合に非常に便利です。



#### 設定

リモートUDP Loggingを有効にする	はい
ログサーバのIPアドレス	192.168.210.105
ログサーバのポート(通常は 514)	514

Logging >> ローカルログの閲覧



ローカルログの閲覧

以下の機能のログが mGuard のローカルログとして記録されます。

必要な機能にチェックをして、「Reload」をする事でローカルログが参照できます。

<input type="checkbox"/> 共通	<input type="checkbox"/> Blade	<input type="checkbox"/> DHCP Server/Relay	<input type="checkbox"/> SNMP/LLDP
<input type="checkbox"/> ネットワークセキュリティ	<input type="checkbox"/> アンチウイルス	<input type="checkbox"/> AntiVirus Update	<input type="checkbox"/> IPsec VPN
<input type="button" value="Reload"/>			

Logging >> ローカルログの閲覧

```
uptime 0 days 00:00:36.98223 pluto[2422]: listening for IKE messages
uptime 0 days 00:00:36.98401 pluto[2422]: adding interface ipsec0/br0 192.168.210.105
uptime 0 days 00:00:36.98549 pluto[2422]: adding interface ipsec0/br0 192.168.210.105:4500
uptime 0 days 00:00:36.98727 pluto[2422]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:37.04571 pluto[2422]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:37.04811 pluto[2422]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:37.05035 pluto[2422]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:11:15.56438 pluto[2422]: | from whack: got --esp=3des!
uptime 0 days 00:11:15.56449 pluto[2422]: | from whack: got --ike=3des!
uptime 0 days 00:11:15.56458 pluto[2422]: added connection description "aaaaaaaa"
uptime 0 days 00:11:15.58103 pluto[2422]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:11:15.58124 pluto[2422]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:11:15.58140 pluto[2422]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:12:24.50150 firestarter: 002 "aaaaaaaa" #1: initiating Main Mode
uptime 0 days 00:12:24.50213 pluto[2422]: "aaaaaaaa" #1: initiating Main Mode
uptime 0 days 00:12:24.50461 firestarter: 104 "aaaaaaaa" #1: STATE_MAIN_I1: initiate
uptime 0 days 00:12:24.53091 pluto[2422]: "aaaaaaaa" #1: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
uptime 0 days 00:12:24.53193 pluto[2422]: "aaaaaaaa" #1: received Vendor ID payload [Dead Peer Detection]
uptime 0 days 00:12:24.59301 pluto[2422]: "aaaaaaaa" #1: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
uptime 0 days 00:12:24.78385 pluto[2422]: "aaaaaaaa" #1: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike-02/03: no NAT detected
uptime 0 days 00:12:24.78538 pluto[2422]: "aaaaaaaa" #1: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
uptime 0 days 00:12:24.79305 pluto[2422]: "aaaaaaaa" #1: Main mode peer ID is ID_IPV4_ADDR: '192.168.210.102'
uptime 0 days 00:12:24.79430 pluto[2422]: "aaaaaaaa" #1: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4
uptime 0 days 00:12:24.79547 pluto[2422]: "aaaaaaaa" #1: ISAKMP SA established
uptime 0 days 00:12:24.79700 pluto[2422]: "aaaaaaaa" #2: initiating Quick Mode PSK+ENCRYPT+PFS
uptime 0 days 00:12:25.19850 pluto[2422]: "aaaaaaaa" #2: Dead Peer Detection (RFC3706) enabled
uptime 0 days 00:12:25.19863 pluto[2422]: "aaaaaaaa" #2: transition from state STATE_QUICK_I1 to state STATE_QUICK_I2
uptime 0 days 00:12:25.19873 pluto[2422]: "aaaaaaaa" #2: sent QI2, IPsec SA established
uptime 0 days 00:12:33.42298 pluto[2422]: "aaaaaaaa" #3: responding to Quick Mode
uptime 0 days 00:12:33.42317 pluto[2422]: "aaaaaaaa" #3: transition from state (null) to state STATE_QUICK_R1
uptime 0 days 00:12:33.49812 pluto[2422]: "aaaaaaaa" #3: Dead Peer Detection (RFC3706) enabled
uptime 0 days 00:12:33.49915 pluto[2422]: "aaaaaaaa" #3: transition from state STATE_QUICK_R1 to state STATE_QUICK_R2
uptime 0 days 00:12:33.50016 pluto[2422]: "aaaaaaaa" #3: IPsec SA established
uptime 0 days 00:31:08.65956 pluto[2422]: "aaaaaaaa" #1: received Delete SA payload: replace IPSEC State #3 in 10 seconds
uptime 0 days 00:31:08.65971 pluto[2422]: "aaaaaaaa" #1: received and ignored informational message
uptime 0 days 00:31:08.75854 pluto[2422]: "aaaaaaaa" #1: received Delete SA payload: deleting IPSEC State #2
uptime 0 days 00:31:08.75867 pluto[2422]: "aaaaaaaa" #1: received and ignored informational message
uptime 0 days 00:31:08.76223 pluto[2422]: "aaaaaaaa" #1: received Delete SA payload: deleting ISAKMP State #1
uptime 0 days 00:31:08.76235 pluto[2422]: packet from 192.168.210.102:500: received and ignored informational message
uptime 0 days 00:31:16.79508 pluto[2422]: "aaaaaaaa": deleting connection
uptime 0 days 00:31:16.79522 pluto[2422]: "aaaaaaaa" #3: deleting state (STATE_QUICK_R2)
```

<input type="checkbox"/> 共通	<input type="checkbox"/> Blade	<input type="checkbox"/> DHCP Server/Relay	<input type="checkbox"/> SNMP/LLDP
<input type="checkbox"/> ネットワークセキュリティ	<input type="checkbox"/> アンチウイルス	<input type="checkbox"/> AntiVirus Update	<input type="checkbox"/> IPsec VPN
<input type="button" value="Reload"/>			