

855-900612-A

第 12.3 版

NX リモート通報

インストール手順書

<監視サーバ : HP-UX 編>

開示および用途制限資料

この資料にかかわるすべての権利は日本電気株式会社にあります。提供された目的以外にこの資料を使用することはできません。また、日本電気株式会社の許可なく、この資料の複製・改変・第三者への開示など行うことはできません

日本電気株式会社

<商標および登録商標>

- * HP-UX は、米国 Hewlett-Packard 社の登録商標です。
- * その他の会社名、製品名は各社の登録商標または商標です。
- * 本製品の一部の機能においては、オープンソースソフトウェアである RSA Message-Digest のライブラリを使用しております。RSA Message-Digest のライセンス条文につきましては、付録 RSA Message-Digest ライセンス条文 をご参照下さい。
- * 本製品の R 3.1 以降のバージョンにおいては、一部の機能においてオープンソースソフトウェアである net-snmp のライブラリを使用しております。net-snmp のライセンス条文につきましては、付録 net-snmp ライセンス条文 をご参照下さい。
- * 本製品の R 4.8 以降のバージョンにおいては、一部の機能においてオープンソースソフトウェアである OpenSSL のライブラリを使用しております。OpenSSL のライセンス条文につきましては、付録 OpenSSL ライセンス条文 をご参照下さい。

目次

NX リモート通報	1
1. はじめに	5
1.1 この文書について	5
2. 概要	6
2.1 サービス概要.....	6
2.2 Manager と Agent の連携	6
2.3 通報	6
2.3.1 通報種類	6
2.3.2 通報抑止	6
2.3.3 通報手段	7
2.3.4 マイナンバーを扱うサーバを監視する場合	7
2.4 WebSAM との連携.....	8
3. インストール事前準備	9
3.1 システム要件の確認（必須！）	9
3.2 ハードウェア構成	12
3.2.1 接続例（30xxM/30xxH/70xxM/70xxH/80xxM/80xxH を除く）	12
3.2.2 接続例（30xxM/30xxH）	13
3.2.3 接続例（70xxM/70xxH/80xxM/80xxH）	14
3.3 カーネルパラメータの確認.....	15
3.4 設定項目の確認	17
3.4.1 監視サーバ.....	17
3.4.2 メールサーバ	17
3.4.3 プロキシサーバ（https 通報時）	17
3.4.4 定期通報時刻	18
3.4.5 被監視サーバ	18
3.4.6 被監視ブレードエンクロージャー.....	18
3.4.7 BMC の SNMPTrap 監視（70xxM/70xxH/80xxM/80xxH）	19
3.4.8 SSH	19
3.5 ブロードバンドルータによる通報の設定	19
3.6 通報受信側準備完了の確認	19
3.7 OpenSSL について	20
4. インストール	21
4.1 インストール前の準備	21
4.1.1 インストール媒体.....	21
4.1.2 ライセンスコード	21
4.1.3 nPartitions 環境へインストールする際の注意事項	21
4.2 Manager ソフトのインストール	22
4.2.1 インストール手順.....	22
4.3 インストール時の設定ミスの修正方法.....	23
4.4 監視サーバの設定	24
4.4.1 マネージャ情報の設定方法	24
4.4.2 監視対象マシン(被監視サーバ)情報の設定方法	25
4.4.3 メールサーバ情報の設定方法.....	30
4.4.4 https 通信情報の設定方法.....	32
4.4.5 cron 定期実行時刻情報の設定登録.....	34

4.4.6	アラーム通報先のメールアドレス登録	34
4.4.7	SNMP の設定	35
4.4.8	SSH の設定	37
4.4.9	データディレクトリの設定	40
4.4.10	TFTP サーバの設定	43
4.4.11	定期通報抑止の設定方法	44
4.5	Agent ソフトのインストールと被監視サーバの設定	45
4.5.1	Agent ソフトのインストール	45
4.5.2	SFM の設定	47
4.5.3	EMS の設定	48
4.5.4	ライセンスコードの入力	49
4.5.5	マネージャ(監視サーバ)の IP アドレス登録	50
4.5.6	冗長 OA 搭載エンクロージャー(BE600/BE1000) および 7320H-256/8160H-256/9160H-256 の設定	50
4.5.7	ログ採取の設定	51
5.	MANAGER の起動/停止	52
5.1	Manager の起動	52
5.2	Manager の停止	52
5.3	Manager の再起動	53
5.4	Manager のステータス表示	54
6.	テスト通報	55
6.1	テスト通報	55
	【テスト通報の種類】	55
	【テスト通報確認方法】	56
6.1.1	Manager テスト通報	57
6.1.2	Ioscan テスト通報	58
6.1.3	OS ログテスト通報 (1)	58
6.1.4	OS ログテスト通報 (2)	59
6.1.5	SFM テスト通報	59
6.1.6	SNMP Trap テスト通報	61
7.	アンインストール方法及びメンテナンス	63
7.1	アンインストール	63
7.1.1	Manager ソフトのアンインストールと監視サーバの設定変更	63
7.1.2	Agent ソフトのアンインストールと被監視サーバの設定変更	63
7.2	メンテナンス	66
7.2.1	通報サービスの一時抑止方法	66
7.2.2	ライセンスコードの更新	67
7.2.3	ライセンス期限の確認	68
7.2.4	MP 交換時の注意事項	68
7.2.5	iStorageManager のメッセージ iSM07454/iSM07459 を通報させる方法	68
7.2.6	マネージャプログラム起動状況の syslog 出力	69
7.3	コードの説明	71
8.	リソース監視とユーザ辞書の設定	72
8.1	リソースの閾値の設定	72
8.2	ユーザ定義辞書によるユーザ定義メッセージ監視の設定	72
8.2.1	編集ツールの起動	73
8.2.2	監視メッセージの追加	73

8.2.3	既存 ID 項目の編集	74
8.2.4	編集の終了	74
8.2.5	マスタ・スレーブのユーザ定義辞書	75
9.	ログ	76
9.1	動作履歴ログ	76
9.2	WebSAM 連携用ログ	77
10.	ダウンロード物件の取り扱い方	79
10.1	CD-R へ書き込む時の注意事項	79
10.2	物件の展開方法	79
11.	インストール設定表	80
12.	付録.....	85
12.1	RSA Message-Digest ライセンス条文.....	85
12.2	net-snmp ライセンス条文	85
12.3	OpenSSL ライセンス条文	91

1. はじめに

1.1 この文書について

本ドキュメントは監視サーバを HP-UX サーバで実現する「NX リモート通報(R6.0)のインストール手順を示す説明書です。

過去のバージョンのインストールを行う場合は、表 1.1 に記載されているインストール手順書を参照してください。

尚、被監視サーバに NX7700i/50xxM,50xxH が含まれる場合、Windows 版の監視サーバが必須のため＜監視サーバ：Windows 編＞を参照下さい。

表 1.1 インストール手順書対応バージョン一覧

バージョン	インストール手順書の版
R5.5	11.0 版
R5.41	9.5 版
R5.4	9.41 版
R5.3	9.3 版
R5.2	9.2 版
R5.1	9.1 版
R4.8	8.9 版
R3.8	8.7 版
R3.7	8.5 版
R3.6 以前	8.3 版

2.概要

2.1 サービス概要

NX リモート通報は HP-UX マシンの監視と通報の機能を提供するシステムです。NX リモート通報は、監視を行うプログラム(Manager)をインストールした監視サーバから LAN Console port 経由で、被監視サーバのコンソール出力 (/dev/console) を監視し、障害辞書またはユーザ定義辞書に該当するメッセージがコンソールに出力された場合や、アラームが上がった場合、e-mail にて通報を行います。被監視サーバには、Manager と連携して処理を行う Agent プログラムをインストールします。

2.2 Manager と Agent の連携

NX リモート通報の Manager は、被監視サーバにインストールした Agent と連携して動作します。被監視サーバにおいて通報事象が発生した場合や、cron による定期実行の際には Manager が Agent をリモートで起動し、Agent が収集したログ等を Manager に転送します。Manager は、メールにこのログを添付して通報します。

2.3 通報

2.3.1 通報種類

NX リモート通報が通報する事象の一覧は以下の通りです。

随時通報 (保守センター宛)

- 障害通報
- コンソールアクセス障害の通報(コンソールへの接続不可：6 時間経過後)

随時通報 (お客さまメールアドレス宛：ブロードバンドルータ接続時は通報不可)

- リソース監視のアラーム通報
- 死活監視のアラーム通報
- ユーザ定義辞書のアラーム通報
- ライセンス有効期限残存日数通知(R2.7 以降)

定期通報 (1 回/日)

- Manager の稼動ステータス情報

死活監視を有効にすると、コンソール出力の正常性を確認するために、以下のメッセージを定期的にコンソールに出力します。

THIS-IS-A-KEY-MESSAGE-FOR-MONITORING-CHECK-OF-STS

コンソールに他のメッセージが定期的に出力される場合は、本メッセージは出力されません。

このメッセージを出力さないためには、4.4.6 章を参考に、アラーム通報先のメールアドレスを dummy@com(初期値: OFF)にしてください。

2.3.2 通報抑止

以下のメッセージは通報要因ですが通報が抑止されます。

- ① 同一要因のメッセージは 1 時間抑止 (EMS/SFM により検出された障害は対象外)
SNMPTrap 監視の同一要因のメッセージは 3 0 分間抑止
(70xxM/70xxH/80xxM/80xxH の場合は 1 5 分間抑止)
- ② repctrl コマンドで抑止指示されたとき (全メッセージが対象)

③ Agent、Manager、BMC の死活監視メッセージは 24 時間抑止

※SNMP Trap 監視による通報において②の抑止は対象外となります。

2.3.3 通報手段

NX リモート通報は、保守センター（NEC フィールドイング）宛の通報（随時通報と定期通報）手段は e-mail と https から選べます。お客さま宛の通報手段は e-mail のみとなります。

2.3.4 マイナンバーを扱うサーバを監視する場合

通報にはコンソールログや syslog、カーネルバッファが含まれます。マイナンバーを扱うサーバを監視する場合で、これらのログにマイナンバー情報が含まれる可能性がある場合は、これらのログが送信されないように設定を変更してください。

但し、本設定を行うと保守センターにおける障害解析に影響を与える可能性がありますのでマイナンバーを扱わない場合は設定を変更しないで下さい。

監視サーバ

被監視サーバのコンソールログが含まれる定期通報を抑止することが可能です。詳細は 4.4.11 参照。

被監視サーバ

障害通報に含まれるログから以下の内容を除外することが可能です。詳細は 4.5.7 参照。

- syslog
- dmesg の結果

テスト通報

ioscan テスト通報にはコンソールログが含まれます。マイナンバーを扱うサーバを監視する場合は実施しないでください。詳細は 6.1.2 参照。

2.4 WebSAM との連携

NX リモート通報は WebSAM System Navigator と連携しています。これにより、WebSAM でハードウェア障害とソフトウェア障害の一元管理が可能になります。

3. インストール事前準備

3.1 システム要件の確認（必須！）

(1) 動作要件

NX リモート通報の動作要件を以下に示します。

対象が明記されていない項目は、監視サーバ・被監視サーバ共通の要件です。

- ・被監視サーバ (30xxM/30xxH『以外』の場合) →図 3-1,3-2 参照
 - －サーバの LAN コンソールが利用可能なこと (サーバ標準装備の LAN コンソールポートを使用)。
 - ※MP にログインし、EL コマンドで確認出来る (All enabled or Telnet only であること)
 - －サーバは Manager-Agent の通信用に OS で認識できる (lanscan コマンドで表示される) LAN ポートを利用可能なこと。
- ・被監視サーバ (30xxM/30xxH の場合) →図 3-3 参照
 - －システムコンソールが利用可能なこと (サーバ標準装備のコンソールソフト(NEC Console Software)を使用)。
 - －サーバは Manager-Agent の通信用に OS で認識できる (lanscan コマンドで表示される) LAN ポートを利用可能なこと。
 - －システムコンソールは iSP 接続用の LAN ポートとは別に監視サーバとの接続用に LAN ポートを利用可能なこと。(最低でも LAN ポートが 2 つ必要)
- ・被監視筐体(NX7700i/NXBL エンクロージャーの場合)
 - －SNMP Trap 通信(port 162/UDP)が利用可能なこと。
- ・監視サーバ →図 3-1,3-2,3-3,3-4,3-5 参照
 - －サーバは以下の LAN ポートを利用可能なこと。
 - 30xxM/30xxH : ①システムコンソール、Agent およびメールサーバ接続用
 - その他 : ①LAN コンソール/iSP および Agent 接続用、②メールサーバ接続用、③マスタ/スレーブの相互監視用 (マスタ/スレーブ構成でない場合または①でマスタ/スレーブ間の通信が出来る場合は不要)
- ・監視サーバの LAN ポートが、被監視サーバの LAN コンソールポートおよび OS で認識できる (lanscan コマンドで表示される) LAN ポートと、ネットワーク (LAN ケーブル/HUB 等) を介して常時接続されていること。

また、被監視サーバが監視サーバを兼ねる場合は、監視サーバ自身の OS で認識できる (lanscan コマンドで表示される) LAN ポートが、自分自身の LAN コンソールポートと、ネットワーク (LAN ケーブル/HUB 等) を介して常時接続されていること。
- ・監視サーバに、グループ users が作成されていること。

未作成の場合は users の作成が可能であること (Manager ソフトのインストール時に作成します)。

バージョン R3.7 以降からは necsts の代わりに既存ユーザで起動することができます。既存ユーザで起動するは users の作成が可能でなくてもインストールできます。
- ・監視サーバに、専用アカウント necsts の作成が可能であること。
 - －Manager ソフトは、/home/necsts 以下を使用する。
 - バージョン R3.7 以降からは necsts の代わりに既存ユーザを選択できるため、専用アカウント necsts の作成可能は必須ではありません。
 - 但し専用アカウント necsts を推奨します。
- ・被監視サーバでリソース監視を利用する場合、専用アカウント necsts の作成が可能であること。
- ・Agent ソフトは、リソース監視ありの場合 /home/necsts/rrs 以下を使用する。

- ー（リソース監視の有無はインストール時のオプションで選択可能）

- ・監視サーバ／被監視サーバは以下のディスク空き容量が確保可能であること。

監視サーバ	被監視サーバ
ー/home の空き容量 100MB 以上（リソース監視なし）	ー/opt の空き容量 100 MB 以上（プログラム格納用） ー/home の空き容量 不要（リソース監視なし） 200MB 以上（リソース監視あり）

- ・監視サーバが監視できる被監視サーバの台数は、最大 500 台となります。
また監視サーバが監視できる SNMPTrap 監視機器の台数は、最大 50 台となります。

- ・監視サーバの場合、/home の空き容量は上記に加えて被監視サーバの台数分、下記のサイズが追加が必要です。

被監視サーバの台数 × 1MB

- ・データディレクトリ設定（4.4.8 章）を行う場合、設定ディレクトリにも同程度の空き容量が必要です。
- ・監視サーバ／被監視サーバにおいて、swinstall コマンドによるインストールが可能なこと。
- ・監視サーバは cron が使用できること。また/var/adm/cron/cron.allow に専用アカウント necsts を登録可能なこと。
- ・監視モードに SFM を選択される場合、被監視サーバは cron が使用できること。また /var/adm/cron/cron.allow に root ユーザを登録可能なこと。
- ・リソース監視を利用する場合、被監視サーバは cron が使用できること。また /var/adm/cron/cron.allow に専用アカウント necsts を登録可能なこと。
- ・被監視サーバは TCP/IP 通信の port 34143 & 34144 の2つを専用ポートとして登録できること。
- ・監視サーバは TCP/IP 通信の port 34145 & 34146 の2つを専用ポートとして登録できること。
- ・監視サーバ／被監視サーバのインストールに root 権限が必要。
- ・監視サーバは、OpenSSL がインストール済みであること。（詳細は 3.7 章参照）

（2）メール環境

NX リモート通報は通報に e-mail を使用します。必要なメール環境は以下の通りです。

- ・ NEC フィールドディングへ e-mail を送信できるメールサーバがあり、監視サーバとネットワーク(LAN ケーブル/HUB 等)を介して常時接続されていること。
- ・メールサーバが最大 5MB 程度のメールを発信できること。
- ・メールサーバがユーザ認証を行う場合は、ユーザ名とパスワードを使用して認証を行えること（SMTP 認証（CRAM-MD5、PLAIN））。ただし、先に受信が必要な認証方式(POP before SMTP)には対応しない。

（3）https 環境

NX リモート通報は保守センター宛の通報に https を使用することも可能です。ただしユーザ通報は e-mail を使用します。ユーザ通報を利用しない場合もメールサーバの設定が

必要となります。メールサーバの設定については 3.4.2 を参照ください。

必要な https 環境は以下の通りです。

- ・ 保守センターへ https で通信できる環境があり、監視サーバとネットワーク (LAN ケーブル/HUB 等) を介して常時接続されていること。
- ・ 直接保守センターへ https で接続できない場合は、プロキシサーバを用意すること。

また通報先 URL は以下の通りです。URL フィルタリングを行っている場合はフィルタリング対象から除外して下さい。

URL
https://htreptky.red.fielding.co.jp/cgi-bin/htNxRcvRep
https://htreposk.red.fielding.co.jp/cgi-bin/htNxRcvRep

(4) 通信ポート

NX リモート通報は、以下のポート番号を使用して通信を行ないます。ファイアウォール等の設定が必要な場合は、以下のポートを通すようにしてください。

クライアント側	サーバ側	ポート番号	説明
マネージャ	エージェント	34143	エージェントの通信ポート
マネージャ	エージェント	34144	エージェントのデータ送受信ポート
マネージャ	マネージャ	34145	マネージャの通信ポート
マネージャ	マネージャ	34146	マネージャの内部通信ポート
マネージャ	MP	22 / 23	コンソールの監視 (ssh / telnet)
マネージャ	被監視筐体	22 / 23	SNMP 設定・ログ取得
マネージャ	メールサーバ	25	メールの送信 (SMTP) 注 1
被監視筐体	マネージャ	162	SNMP Trap 受信 注 2
マネージャ	https	443	https 通信 注 3
マネージャ	被監視筐体	69	tftp 通信 注 4

注 1. SNMP Trap により障害を監視する機器がない場合、設定は不要です。

注 2. メールによる通報を行なわない場合、設定は不要です。

注 3. https による通報を行なわない場合、設定は不要です。

注 4. 6120XG Blade Switch のログの一部を取得しない場合は不要です。

3.2 ハードウェア構成

NX リモート通報は、ネットワーク経由で各サーバを監視します。そのため、Manager をインストールしたマシンから、監視対象となる全てのマシンのコンソール出力が監視できるようなネットワークの構成をとる必要があります。

NX リモート通報は、通報を e-mail または https で行います。

通報を e-mail で行う場合は、Manager ソフトを導入した監視サーバからアクセス可能で、NEC フィールディング宛にメール発信できるメールサーバを事前に用意していただく必要があります。

通報を https で行う場合は、Manager ソフトを導入した監視サーバから NEC フィールディングの https サーバにアクセスできる環境が必要です。直接インターネットにアクセスできない場合は、プロキシサーバを事前に用意していただく必要があります。以降接続例にプロキシサーバも記載されていますが、環境により無視してください。

3.2.1 接続例（30xxM/30xxH/70xxM/70xxH/80xxM/80xxH を除く）

監視サーバはネットワーク B を介して、被監視サーバの通常の LAN ポート（Core I/O 或は増設 NIC）と管理用の LAN コンソールポートの 2 つのポートと接続します。NX リモート通報では、障害等の通報を e-mail または https で行います。このため、Manager ソフトを導入した監視サーバからアクセス可能で、NEC フィールディング宛にメール発信できるメールサーバまたは https 通信環境を事前にお客様に用意していただく必要があります。下記の例（図 3-1）では、通報用のネットワーク A を介して監視サーバとメールサーバまたはプロキシサーバが接続されています。

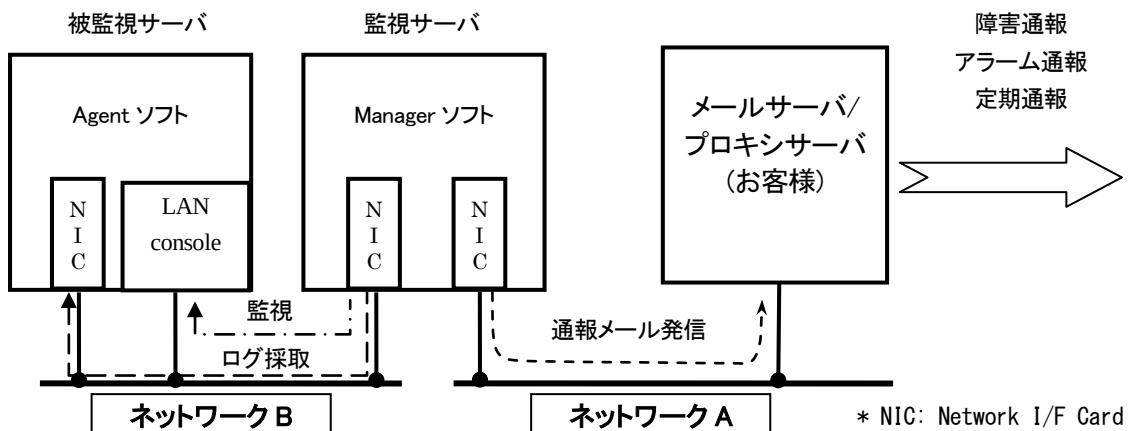


図. 3-1

補足事項

- 図 3-1 では通報用のネットワーク A と監視用のネットワーク B を分離しているが、分離せずにネットワークを共通化した構成も可能。
- 図 3-1 では増設 NIC に接続しているが、Core I/O の LAN ポートに接続することも可能。
- nPartitions（HW パーティション）構成時は、各パーティションに LAN ポートが必要となる。
- 被監視サーバが監視サーバを兼ねる場合、自身を監視するため、当該サーバは Manager ソフトと Agent ソフトを双方インストールし、また、自身のネットワーク B を介して、自身の LAN コンソールポートと接続する。次頁図 3-2 を参照。

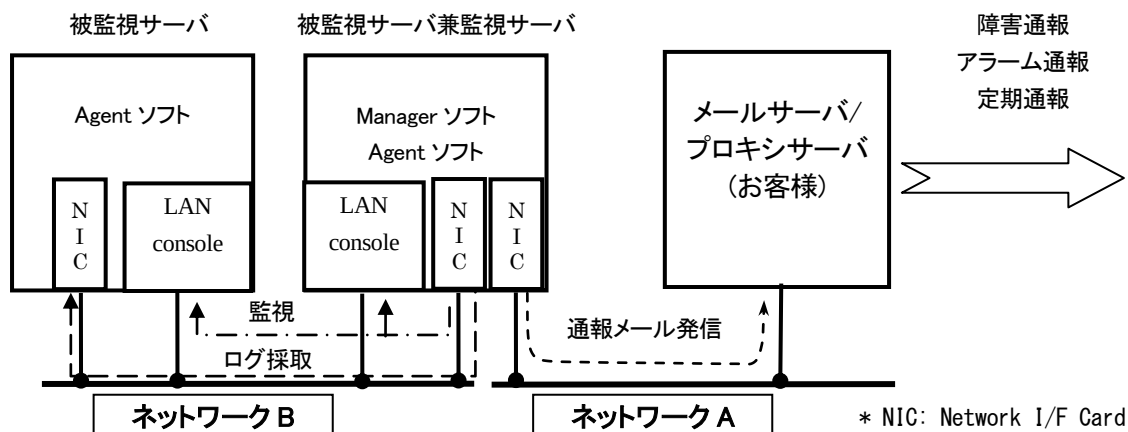


図. 3-2

3.2.2 接続例 (30xxM/30xxH)

監視サーバはネットワーク A を介して、システムコンソールと被監視サーバの通常の LAN ポート (増設 NIC) の 2 つのポートと接続します。また、システムコンソールはネットワーク B を介して被監視サーバの iSP と接続します。NX リモート通報では、障害等の通報を e-mail または https で行います。このため、Manager ソフトを導入した監視サーバからアクセス可能で、NEC フィールディング宛にメール発信できるメールサーバまたは https 通信環境を事前にお客様に用意していただく必要があります。下記の例 (図 3-3) では、通報用のネットワーク A を介して監視サーバとメールサーバまたはプロキシサーバが接続されています。

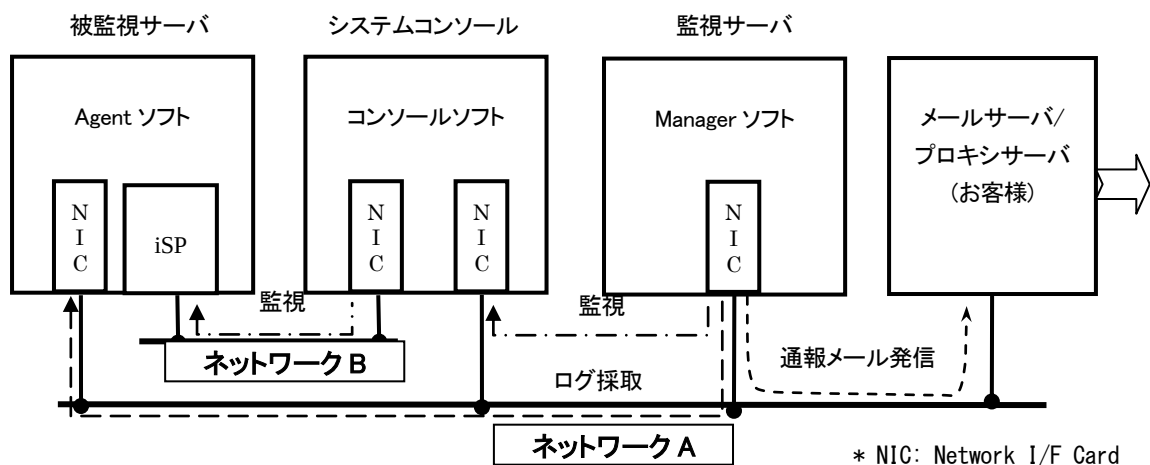


図. 3-3

補足事項

- ・ ネットワーク A とネットワーク B は**共通化不可**。
- ・ nPartitions (HW パーティション) 構成時は、各パーティションに LAN ポートが必要となる。

3.2.3 接続例（70xxM/70xxH/80xxM/80xxH）

ネットワーク A を介して、被監視サーバの通常の LAN ポート（増設 NIC）と接続します。また、ネットワーク B を介して被監視サーバの BMC と接続します。NX リモート通報では、通報を e-mail または https で行います。このため、Manager ソフトを導入した監視サーバからアクセス可能で、NEC フィールドイング宛にメール発信できるメールサーバまたは https 通信環境を事前にお客様に用意していただく必要があります。下記の例（図 3-4）では、通報用のネットワーク A を介して監視サーバとメールサーバまたはプロキシサーバが接続されています。

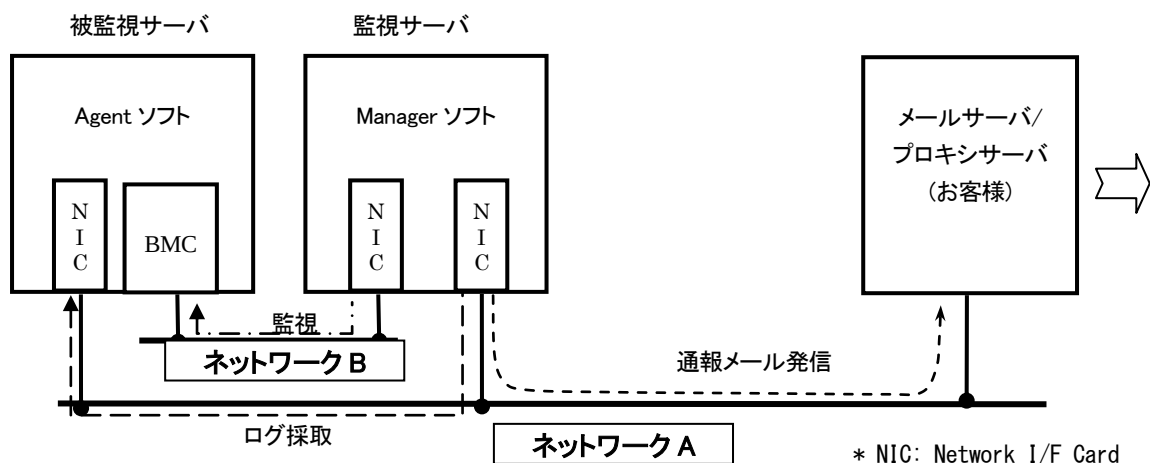


図 3-4

補足事項

- ・ ネットワーク A とネットワーク B は共通化不可。
- ・ nPartitions（HW パーティション）構成時は、各パーティションに LAN ポートが必要となる。
- ・ ネットワーク B を他の目的で利用しなければ、被監視サーバの NIC との接続もネットワークを介して行うことが可。図 3-5 を参照。

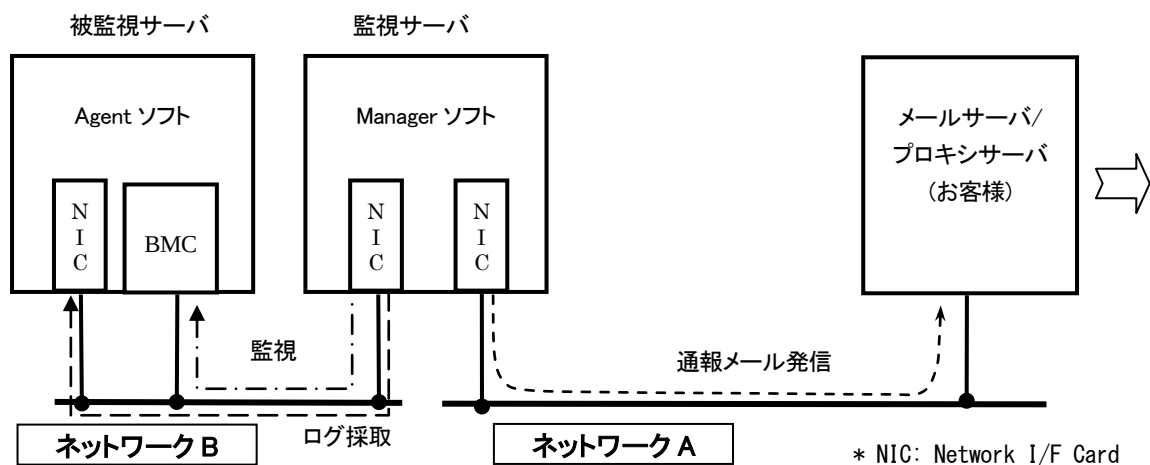


図 3-5

3.3 カーネルパラメータの確認

Manager をインストールする監視サーバでは、監視対象のサーバ数(監視サーバ自身を含む)に応じてカーネルパラメータの変更が必要です。監視対象サーバ数が8台を超える場合は、以下の算出式により計算した値にカーネルパラメータを変更してください。

カーネルパラメータの変更後は、サーバのリブートが必要です。

- ・カーネルパラメータの変更方法

[HP-UX 11i v3 の場合]

root でログインして `kctune` コマンドで以下のパラメータを設定します。

※`kcweb`(Web ベース)でも設定できます。

パラメータ名	意味
<code>maxuprc</code>	ユーザ当たり最大プロセス数
<code>nproc</code>	システム最大プロセス
<code>maxdsiz</code>	プロセス当たりの最大データセグメントサイズ

監視サーバのカーネルパラメータを変更する際は、各項目の設定値を下記の表に示す値にしてください。

- ・監視数 8 以下の場合

パラメータ名	設定値
<code>maxuprc</code>	デフォルト値
<code>nproc</code>	デフォルト値
<code>maxdsiz</code>	デフォルト値

- ・監視数 9 以上の場合

パラメータ名	設定値
<code>maxuprc</code>	監視数+40 を現在値に加算する
<code>nproc</code>	1024 以上
<code>maxdsiz</code>	0x10000000 以上
<code>nstrpty</code>	ssh で該当サーバから他サーバに接続する数+監視数

また、下表のパラメータが最低値未満の場合は、変更することをお勧めします。

パラメータ名	意味	最低値
<code>maxfiles_lim</code>	1 つのプロセスが同時にオープンするファイルの数に対する物理制限値	1024

バージョン R3.7 以降から **Manager** は OS の共有メモリを使用します。使用する共有メモリセグメント数は1、メモリサイズは約 2Mbyte です。

カーネルパラメータの設定を確認し、必要であれば変更してください。

Manager はデフォルトの設定で動作しますが、他のアプリケーションで共有メモリを使用している場合は、変更が必要な可能性があります。

パラメータ名	意味	設定可能な値
shmem	共有メモリのサポートを有効/無効にします	最小値 0 共有メモリを使用不可 最大値 1 共有メモリを使用可 デフォルト値 1
shmmax	システム全体で適用される共有メモリセグメントの最大サイズを指定します。	最小値 2048 (2KB) 最大値 1 GB(32 ビット) 4 TB(64 ビット) デフォルト値 64 MB
shmmni	システム全体で利用できる共有メモリセグメントの最大数を指定します (セグメント識別子の数を制限)。	最小値 3 最大値 メモリサイズに依存 デフォルト値 200
shmseg	1 つのプロセスに同時にアタッチされる共有メモリセグメントの最大許容数。	最小値 1 最大値 shmmni デフォルト値 120

3.4 設定項目の確認

Manager ソフトをインストールした後、監視サーバ上で各種設定が必要となります。予め必要となる設定項目を最終ページの「インストール設定表」に記載して準備しておくことを推奨します。以下にインストール設定表の各項目について説明します。

3.4.1 監視サーバ

NX リモート通報の監視サーバを 2 台 1 組で運用する場合、監視サーバのマスタとスレーブを決定します。インストール設定表にサーバの IP アドレスを記入するときに、マスタを 0 番、スレーブを 1 番に設定します。

監視サーバが 1 台のみの場合は、0 番に IP アドレスを設定してください。

ー注意事項ー

監視サーバが複数の IP アドレスを持っている場合は、自分のホスト名から名前解決で検索できる IP アドレスを指定してください。

ホスト名から名前解決により検索できる IP アドレスは、nslookup コマンドで確認してください。

```
# nslookup `hostname`
```

IP アドレスを名前解決できるように、/etc/hosts へのエントリの追加、あるいは DNS への登録など、環境にあった適切な対処をしてください。

3.4.2 メールサーバ

通報を行う場合に利用するメールサーバに関する情報を記載します。

メールサーバは複数指定できます。最初のメールサーバへの送信が行えなかった場合は、2 番目以降のメールサーバを順番に使用してメール送信を行います。

記載項目（メールサーバ毎）

IP アドレス	メールサーバの IP アドレス
From アドレス	通報メールで使用する From アドレス
※必ず有効なメールアドレスを指定願います。	
認証	SMTP 認証を行う(on)・行わない(off)
認証ユーザ	認証するアカウント名
認証パスワード	認証するパスワード

https 通報を選択しユーザ通報無しを選択された場合でも、次の通りメールサーバ設定を行ってください。

※上記のメールサーバの設定をされている場合は不要です。

記載項目

IP アドレス	マネージャサーバの IP アドレス
※e-mail 通報には使用しません	
From アドレス	root@上記 IP アドレス
※無効なメールアドレスで構いません	
認証	SMTP 認証を行わない(off)

3.4.3 プロキシサーバ (https 通報時)

https にて通報を行う場合に利用するプロキシサーバに関する情報を記入します。

記入項目

プロキシサーバ IP アドレス プロキシサーバの IP アドレス：ポート番号
https 通報を選択しユーザ通報を利用しない場合もメールサーバの設定が必要となります。
す。メールサーバの設定については 3.4.2 を参照ください

3.4.4 定期通報時刻

当該サービスは、1 日 1 回監視サーバ内のログを保守センターに通報します。この通報時刻を記載します。既定値は R2.7 未満の場合は「1：10」、R2.7 以降の場合は「3：10」です。通報の集中を防ぐため、可能な限り既定値から変更願います。

3.4.5 被監視サーバ

被監視サーバの情報を記載します。

記載項目（サーバ毎）

システム管理コード

シリアル No.

構成指示書番号

Node No.

OS Version

装置名

機種

システム IP アドレス

GSP/MP IP アドレス

iSP IP アドレス

接続方法

iSP/MP Login

iSP/MP Passwd

装置のシステム管理コード

装置号機（装置記載のシリアル番号）

構成指示書番号

パーティション作成時のノード番号

パーティション未対応のマシンでは'0'固定。

OS バージョン指定

HP-UX の例： 11iv3

装置のホスト名など、装置を識別するための文字列（ホスト名入力必須）

rp3410 や 3010L-2 などの型式名

OS が使用する LAN ポートの IP アドレス

GSP/MP の IP アドレス

iSP の IP アドレス

telnet/ssh いずれかを選択してください

iSP/MP/GSP のログイン名

iSP/MP/GSP のログインパスワード

3.4.6 被監視ブレードエンクロージャー

エンクロージャーの情報を記載します。

記入項目（筐体毎）

システム管理コード

シリアル No.

構成指示書番号

ラック番号

機種

システム IP アドレス

筐体のシステム管理コード

筐体号機（装置記載のシリアル番号）

構成指示書番号

エンクロージャーの識別名

BE600/BE1000

接続する IP アドレス（OA 設定の IP アドレス）

尚、冗長 OA（Onboard Administrator）を搭載したエンクロージャーを監視する場合は、エンクロージャーの OA の設定” Enclosure IP Mode” を enable にする必要があります。

設定方法は、4.5.6 章を参照してください。

接続方法

Login

Passwd

telnet/ssh いずれかを選択してください

接続時のログイン名（OA ログイン名）

接続時のログインパスワード（OA ログインパスワード）

3.4.7 BMC の SNMPTrap 監視 (70xxM/70xxH/80xxM/80xxH)

SNMPTrap にて監視を行なう BMC の情報を記入します。

記入項目 (筐体毎)

システム管理コード	筐体のシステム管理コード
シリアル No.	筐体号機 (装置記載のシリアル番号)
構成指示書番号	構成指示書番号
筐体名	BMC 装置を識別するための文字列
機種名	7020M-16/7040M-32/7080H-64 8020M-32/8040M-64/8080H-128
SM IP アドレス	SNMP Trap を送信する SM の IP アドレス
PM IP アドレス	SNMP Trap を送信する PM の IP アドレス

3.4.8 SSH

被監視サーバや OA に接続するプロトコルに SSH プロトコルを用いて監視を行う場合に必要な情報を記入します。

記入項目

SSH コマンドパス	SSH 接続する際の ssh クライアントコマンドのフルパス名
秘密鍵パス	公開鍵認証方式を使用する際の秘密鍵のフルパス名
パスフレーズ	秘密鍵に対するパスフレーズ

SSH 設定については 4.4.8 を参照ください

3.5 ブロードバンドルータによる通報の設定

メールサーバが用意できない場合、ブロードバンドを用いて NEC フィールドインギングのメールサーバに直接接続し、メールを送信することも可能です。

ただし、この場合、ADSL/ISDN 回線をお客さまで準備していただき、ブロードバンドルータを接続して運用する形式になります。

※ADSL/ISDN 契約料・回線工事料・回線使用料・ブロードバンドルータの購入費・現調費用などは、お客様負担となります。

詳細はご担当の NEC フィールドインギング保守員にご相談願います。

－注意事項－

ブロードバンドルータを使用する場合、お客様宛に通報ができないため、障害通報以外のサービスは利用できません。

3.6 通報受信側準備完了の確認

障害通報を受信する NEC フィールドインギング側のサーバに、お客様の機器管理情報を登録しておく必要が有ります。

NEC フィールドインギング保守員にお客様機器管理情報 (ALIVE(アライブ)設置連絡票) の登録が完了していることをご確認願います。

3.7 OpenSSL について

監視サーバは OpenSSL の共有ライブラリを通信の暗号化等に使用しています。そのため OpenSSL がインストールされていることが必須となります。

監視サーバが 11iv3 であれば、OpenSSL はインストール済です。

4. インストール

4.1 インストール前の準備

4.1.1 インストール媒体

媒体 (CD-ROM)、もしくは、Web サイトからダウンロードした物件を使用します。

－注意事項－

インストールは root 権限を持ったユーザで実施願います。

root 権限を持たないユーザで作業を行った場合、以下のエラーが表示されます。

ERROR: you have to be root to run this program.

4.1.2 ライセンスコード

NX リモート通報のライセンスを購入すると、インストール対象サーバに対応したライセンスコード(codeID)が納入されます。ライセンスは必要な台数分購入してください。

4.1.3 nPartitions 環境へインストールする際の注意事項

Agent を nPartitions 環境へインストールする場合、監視するパーティションすべての OS にインストールする必要があります。

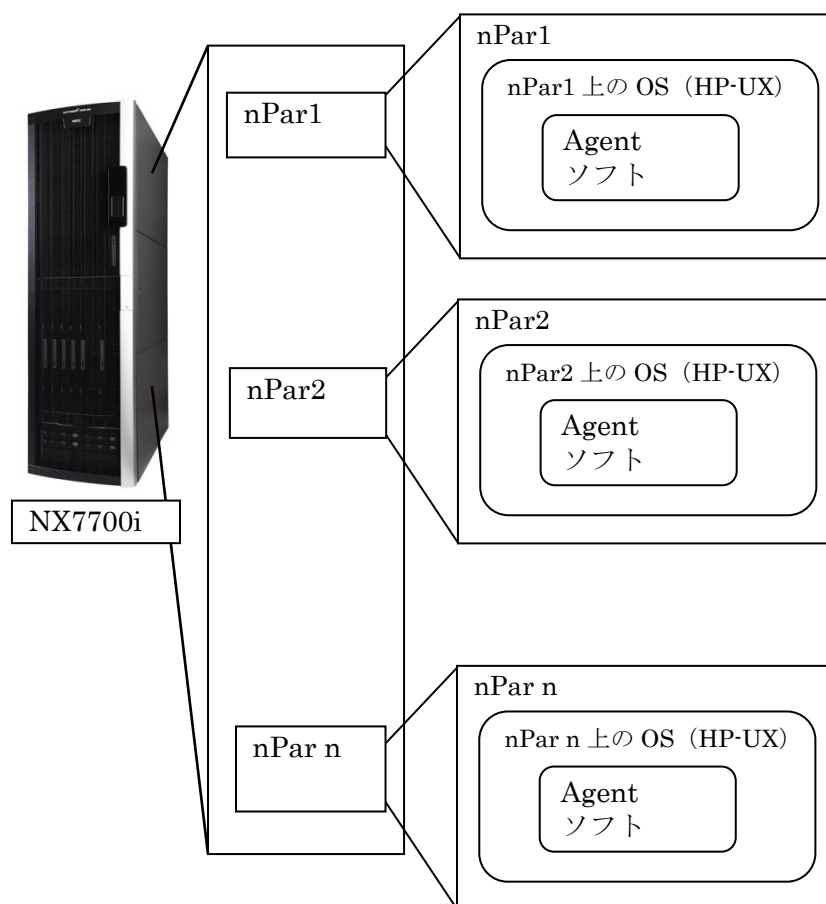


図 4-1 nPartitions 環境への sts インストール対応図

4.2 Manager ソフトのインストール

4.2.1 インストール手順

以下の手順にしたがって、Manager ソフトをインストールしてください。

root でマシンにログインし、インストール CD をマウントして、インストールコマンドを実行します。以下の説明は、CD を /CDROM ディレクトリにマウントした際の例です。また、Web よりダウンロードしたファイルの場合、/CDROM はファイル一式を置いたディレクトリ名に適宜読み替えてください。

```
# mount -F cdfs -r -o cdcase /dev/dsk/c0t0d0 /CDROM
```

※ftp 転送時、mount コマンドは実施不要

```
# /sbin/sh /CDROM/hpux/install.sh
```

注) デバイス名(例: /dev/dsk/c0t0d0)は、マシンにより異なります。

事前に `ioscan -fnkC disk` コマンド等で CD/DVD ドライブのデバイス名を確認願います。

以下のようなプロンプトが表示された場合、パッケージ `sts.dep` を `install.sh` が見つけられないことを示しています。`sts.dep` のある場所を絶対パスで設定してください。

```
input package (sts.dep) path : /CDROM/hpux/sts.dep
```

注) パッケージ名は小文字で指示して下さい。

以下のようにメニューが表示されるので、Manager をインストールする場合は 1 を入力してください。

```
NX remote communicator install program.
```

```
Copyright (c) 2014 NEC Corporation
```

1. install Manager
2. install Agent
3. install Resource_watch
- Q. QUIT

* Resource_watch : This program is the Resource watch feature set.

```
Enter selection:[1] 1
```

←メニュー番号を入力

以下のようなメッセージが表示された場合、/home/necsts/sg/startup_user.sg を削除してから再度実行してください。

```
ERROR: /home/necsts/sg/startup_user.sg exists
```

以下のように **Manager** を起動するユーザを選択するメッセージが表示されます。
専用アカウント **necsts** を使用する場合は、1 を選択してください。既存ユーザを使用する場合は 2 を選択してください。（推奨は専用アカウント **necsts** です。）

```
*** select startup user
    1. necsts
    2. others user

Enter selection:[1] 1
```

←メニュー番号を入力

【注意事項】

既にリソース監視ツールをインストールしてある場合は、**necsts** 以外のユーザを選択しないでください。

上記で 2 を選択した場合、以下のようにユーザ名の入力メッセージが表示されます。
既存のユーザアカウントを入力してください。但し **root** は使用できません。

```
*** input startup user
Enter user:[]
```

←既存のユーザアカウントを入力

install.sh は **swinstall** を呼び出してインストールを実施します。画面には **swinstall** によるインストールの経過が表示されるので、エラーがないこと（“* Selection succeeded.” および “* Analysis and Execution succeeded.” と表示されること）を確認してください。

正常に終了すると、以下のように表示されます。

```
All install programs are successfully completed.
```

swinstallによって以下のファイルセットが/home/necstsディレクトリ配下にインストールされます。

STS.STS (Manager プログラム)
STS.dic (辞書ファイル)

また、この **swinstall** により、以下の設定も自動的に反映します。

- ・グループの登録 [グループ名 **users**] (未登録時)
- ・ユーザアカウントの登録 [ユーザ名 **necsts** グループ名 **users**]
- ・cron 実行権の設定 [/var/adm/cron/cron.allow]
（上記のグループ登録とユーザアカウントの登録は、専用アカウント **necsts** を選択した場合のみです。）

4.3 インストール時の設定ミスの修正方法

インストール時に誤って違うメニューを選択した場合は、7.1 章に従ってアンインストールした後、再インストールしてください。

4.4 監視サーバの設定

監視サーバの設定は、設定ツール `config` によって行います。このツールを `root` で実行することで、設定ファイルを作成します。

通常は、(1)の方法で全ての設定を順番に行って下さい。

設定後に、誤りの修正などで個別項目毎に設定を行う場合は、(2)に示す、それぞれの項目に対応したオプションを使います。

運用開始後に設定を変更した場合は、`Manager` の再起動が必要です。再起動方法については、5.3 章を参照してください。

① 全項目の設定

以下のように、`--set` オプションをつけて `config` を実行します。

```
# /home/necsts/tool/config --set
```

② 個別項目毎の設定

各項目を示す、ハイフン 2 個 `--` を前につけたオプションをつけて実行します。詳細については、()の各章を参照してください。

# /home/necsts/tool/config --ststd_conf	(4.4.1 章)
# /home/necsts/tool/config --sts_hosts	(4.4.2 章)
# /home/necsts/tool/config --mailadd	(4.4.3 章)
# /home/necsts/tool/config --https	(4.4.4 章)
# /home/necsts/tool/config --crontab	(4.4.5 章)
# /home/necsts/tool/config --user_mail	(4.4.6 章)
# /home/necsts/tool/config --snmp	(4.4.7 章)
# /home/necsts/tool/config --ssh	(4.4.8 章)
# /home/necsts/tool/config --data_dir	(4.4.9 章)

－注意事項－ `config` では行わない設定

以下の項目は特別な対応が必要なため、`config` では取り扱いません。

- ・ `sts_parameter.sg` (パラメータ設定ファイル)の設定変更

4.4.1 マネージャ情報の設定方法

監視サーバの IP アドレスを登録します。ここで登録したサーバの順番が、マスタ・スレーブを決める優先順位となります。マスタサーバは、表示されるリストの 0 番、スレーブサーバは、リストの 1 番です。

Windows 版のマネージャと Master-Slave 構成を構築することはできません。本設定では、Windows 版のマネージャの IP アドレスを設定しないでください。

以下のプロンプトに対して、[新規]の場合は `'a'`、[修正]の場合は `'m'`、[削除]の場合は `'d'` を入力してください。

```
*** configure server list & ststd.conf
Manager server host IP list:
input command ([a]dd / [m]odify / [d]elete / [q]uit) >
```

[修正]・[削除]の場合は、修正や削除を行うホスト IP のリストの番号を入力します。[追加]・[修正]の場合は、次に新しい IP アドレスを入力します。

```
command: add IP address.  
input IP address > 10.0.0.1
```

更新後のホスト IP リストが表示されるので、さらに追加する場合は、‘a’ を入力して操作を繰り返してください。

‘q’ によって設定を終了し、設定ファイル `manager.sg` を作成します。

```
Manager server host IP list:  
0: 10.0.0.1  
1: 10.0.0.2  
input command ([a]dd / [m]odify / [d]elete / [q]uit) > q  
command: quit.  
writing /home/necsts/sg/manager.sg ... OK
```

上記のメッセージで、ファイルが正常に作成されたことを確認してください。

4.4.2 監視対象マシン(被監視サーバ)情報の設定方法

1) 概要

監視先の情報を、筐体情報と OS 情報(パーティション情報)の組み合わせで登録します。監視先に登録できる監視対象マシン(被監視サーバ)の台数は、最大 500 台となります。

－注意事項 1－

マスタ・スレーブ構成をとっている場合は、SG ファイルの監視番号(登録順)を厳密に一致させる必要があります。
そのため、マスタ・スレーブ構成の場合は スレーブ側での SG 設定はせず、マスタで設定した以下の SG ファイルをスレーブにコピーしてください。

```
{インストールディレクトリ}/sg/chassis.sg  
{インストールディレクトリ}/sg/partition.sg
```

マスタで筐体、ノード/パーティション情報を変更した場合は、その都度スレーブに上記ファイルをコピーしてください。

－注意事項 2－

被監視サーバが 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 の場合、本設定に加え「SNMP Trap 監視機器の設定」を行うことを推奨します。設定方法は 4.4.7 章を参照してください。

2) 筐体情報設定

まず始めに筐体設定を行います。筐体を[追加]する場合は ‘a’、[修正]する場合は ‘m’、[削除]する場合は ‘d’ を以下のプロンプトに対して入力します。新規の場合は[追加]を選択してください。

```

*** configure sts hosts

configure sts chassis entries
  id: Name          System      Serial      Kousei      Type      Connection
  =====
input command ([a]dd / [m]odify / [d]elete / [p]artition SG / <id> print chassis
data / [q]uit) >

```

ここで、[修正]・[削除]の場合は、その対象となるリストの筐体番号(id)を入力します。[追加]の場合、および[修正]でリスト番号を選択した場合は、次に各項目を以下のように入力します。プロンプトの前にある大カッコ[]内の値をそのまま使用する場合は、リターンキーだけの入力でその内容が使用されます。

```

Command: add entry.
input Chassis Name [] > Name0001          ←筐体名（任意）
input User System Code [] > 123ABC0005    ←システム管理コード
input Serial Number [] > USR00001        ←サーバのシリアル番号
input Kousei-Shijisho Number [] > NXL_-0001 ←構成指示書番号
input Machine Type [] > 9010E-16

```

- 機種(Machine Type)には、NX7000/NX7700iの機種名（例: rp8420）を入力して下さい。以降の入力は機種毎に異なります。

① 機種が通常の機種(MP/GSPがLANコンソールの機種)の場合

```

input LAN Console IP address [] > 10.0.0.1
Use ssh instead of telnet OK? y/[N] > ←sshを使用する場合は y を入力
input USERNAME for MP/GSP Login <> > (例)Admin
input PASSWD for MP/GSP Login >

```

- 「input LAN Console IP address」には、MP/GSP の IP アドレスを入力してください。この場合、この場合、ポート番号はデフォルトの 23(telnet)に設定されます。
- MPへの接続にsshを利用する場合は、「Use ssh instead of telnet OK? y/[N] >」プロンプトに y を入力してください。入力を省略したり、n を入力した場合はtelnetで接続されます。

② 機種が（NX7700i/30xxM,30xxH）の場合

```

input LAN Console IP address [] > 10.0.0.1:12011
input iSP IP address [] > 10.1.1.100

```

- 「input LAN Console IP address」には、LANコンソールのポート番号が、PCにインストールしたコンソールソフト（NEC Console Software）の、LAN consoleの欄で指定したtelnet用のポート番号(規定値:12011)になります。この場合は、LAN console IP address は 10.0.0.1:12011 のように、コロン：の後にポート番号を追加して設定して下さい。
- 「input iSP IP address」には、iSPのIPアドレスを入力して下さい。

- ③ 機種が (7020M-16/ 7040M-32/ 7080H-64/ 8020M-32/ 8040M-64/ 8080H-128) の場合

```
input PM[0] IP address [] > 10.0.0.1
Use ssh instead of telnet OK? y/[N] >
input USERNAME for PM[0] Login <> >
input PASSWD for PM[0] Login >
do you validate PM[1] [Y]/n >y
input PM[1] IP address [] > 10.0.0.2
Use ssh instead of telnet OK? y/[N] >
input USERNAME for PM[1] Login <> >
input PASSWD for PM[1] Login >
do you validate PM[2] [Y]/n >n
```

- 「input PM[0] IP address [] >」には1番目のPMのIPアドレスを入力します。ポート番号はデフォルトの23(telnet)に設定されます。
- 各PMへの接続にsshを利用する場合は、「Use ssh instead of telnet OK? y/[N] >」プロンプトに y を入力してください。入力を省略したり、 n を入力した場合はtelnetで接続されます。
- 「input USERNAME for PM[0] Login」及び「input PASSWD for PM[0] Login」には、PMのログインアカウントとログインパスワードではなく、SMASH/CLPコンソールへ接続する際に使用するアカウント名とパスワードを入力します。
- 「do you validate PM[1] [Y]/n >」には2番目のPMを監視する場合はyを、監視しない場合はnを入力します。nを入力した時点で入力は終了します。yを入力すると、IPアドレス、ユーザ名、パスワードの入力へと続きます。PMは最大で8個まで設定が可能です。

- ④ 機種が (7320H-256/8160H-256/9160H-256) の場合

```
input OA IP address [] >10.0.0.1
Use ssh instead of telnet OK? y/[N] >
input USERNAME for OA Login <> >
input PASSWD for OA Login >
```

- 「input OA IP address [] >」には凡長OAのIPアドレスを入力します。ポート番号はデフォルトの23(telnet)に設定されます。
- OAへの接続にsshを利用する場合は、「Use ssh instead of telnet OK? y/[N] >」プロンプトに y を入力してください。入力を省略したり、 n を入力した場合はtelnetで接続されます。

全ての入力が終わると、この筐体の設定が正しいか否かを確認してきます。正しい場合は 'y' を、間違っている場合は 'n' を入力してください。(図は通常機種の場合)

```

Chassis Data :
id = 1
  Chassis Name           : Name0001
  User System Code       : 123ABC0005
  Serial Number          : USR00001
  Kousei-Shijisho Number : NXL_-001
  Machine Type           : rx1600
  LAN Console IP address : 10.10.10.10
  Connection Method      : TELNET
  USERNAME for MP/GSP Login : aaaa
  PASSWD for MP/GSP Login  : *****
This entry is OK? [Y]/n >

```

1つの筐体の設定が終了すると、また、コマンドの入力画面に戻ります。さらにホストを追加する場合は、‘a’を入力して登録作業を繰り返してください。

【補足】 MP/GSP、iSP ログインのパスワードは、セキュリティ確保のために暗号化して登録されます。入力した値と異なりますが、正常な動作です。

【注意事項】

機種名（Machine Type）は更新時には変更できません。機種名を変更したい場合削除後に新規登録を行ってください。

筐体の詳細情報を表示するには、筐体番号(id)をプロンプトに入力します。

```

input command ([a]dd / [m]odify / [d]elete / [p]artition SG / <id> print chassis
data / [q]uit) > 1      ←筐体番号(id)を入力

Chassis Data :
id = 1
  Chassis Name           : Name0001
  User System Code       : 123ABC0005
  Serial Number          : USR00001
  Kousei-Shijisho Number : NXL_-001
  Machine Type           : i9510
  LAN Console IP address : 10.0.0.1
  Connection Method      : TELNET
  USERNAME for MP/GSP Login : (例)Admin
  PASSWD for MP/GSP Login  : *****

```

設定を終了する場合は‘q’を入力します。OS 情報（パーティション情報）が一つも設定されていない場合、以下のエラーを返します。この際は、メニューに戻り OS 設定（パーティション設定）を行って下さい。

※HW パーティション非対応のサーバについても、OS 情報の設定は必要となります。
この際は、パーティション番号は‘0’を入力願います。

```
input command ([a]dd / [m]odify / [d]elete / [p]artition SG / <id> print
chassis data / [q]uit) > q
command: quit.
Warning: empty partition lists. retry please.
```

3) OS 情報設定

OS 情報設定（パーティション情報設定）を行うには、プロンプトに対し‘p’を入力してください。次に OS 情報（パーティション情報）を設定する筐体番号(id)を入力して下さい。

```
input command ([a]dd / [m]odify / [d]elete / [p]artition SG / <id> print
chassis data / [q]uit) > p
command: partition sg.
input chassis id. (def=quit) > /
```

OS 情報（パーティション情報）を[追加]する場合は ‘a’、[修正]する場合は ‘m’、[削除]する場合は ‘d’ をプロンプトに対して入力します。新規の場合は[追加]を選択してください。

```
configure os_partition entries
chassis name:Name0001
No.: OS      Version      IP      Comment
=====

input command ([a]dd / [m]odify / [d]elete / [q]uit) >
```

ここで、[修正]・[削除]の場合は、その対象となるリストのパーティション番号(No.)を入力します。

[追加]および[修正]でパーティション番号を選択した場合、次に項目を以下のように入力します。プロンプトの前にある大カッコ[]内の値をそのまま使用する場合は、リターンキーのみ入力することで[]内の値が使用されます。

- ※ パーティション番号について、HW パーティション非対応のサーバは ‘0’ を入力願います。
- ※ HW パーティション対応のサーバは、監視対象の OS がインストールされているパーティション全てに対して情報を入力願います。

```

command: add entry.
      input add partition No. (def=quit) > 0  ←パーティション番号
                                              HW パーティション無しの場合は '0'
input OS [HP-UX] >                               ←OS 名 (Enter キーを押下)
input OS Version [] > 11iv3                       ←OS バージョン
input System LAN IP address [] > 0.0.0.0
input Comment [] > COM00  ←コメント (ホスト名の入力必須)

Chassis Name : Name0001
  Partition No.      : 0
    OS               : HP-UX
    OS Version       : 11iv3
    System LAN IP address : 10.0.0.200
    Comment          : COM00
This entry is OK?[Y]/n > y

```

1 つのパーティション設定が終了すると、また、コマンドの入力画面に戻ります。さらにパーティションを追加する場合は、'a' を入力して登録作業を繰り返してください。設定を終了する場合は 'q' を入力し、パーティション設定を終了して下さい。

■機種(Machine Type)が 7020M-16/ 7040M-32/ 7080H-64/ 8020M-32/ 8040M-64/ 8080H-128 の場合

コメント入力の後に、PM のログイン名及びパスワードを入力する必要があります。
PM のログインアカウント及びログインパスワードを入力します。

```

input OS [HP-UX] > HP-UX
input OS Version [] > 11iv3
input System LAN IP address [] > 10.11.12.13
input Comment [] > come
input USERNAME for PM Login <> > admin
input PASSWD for PM Login > passwd

```

■機種(Machine Type)が 7320H-256/ 8160H-256/9160H-256 の場合

コメント入力の後に、nPar 番号を入力する必要があります。
1 以上のパーティション番号を入力してください。

```

input OS [HP-UX] > HP-UX
input OS Version [] > 11iv3
input System LAN IP address [] > 10.11.12.13
input Comment [] > come
input nParNo [] > 1

```

4.4.3 メールサーバ情報の設定方法

メールサーバ情報として設定するのは、通報時に使用するメールサーバの IP アドレス、SMTP 認証の有無です。

メールサーバは複数登録することが可能です。プライオリティの数値が小さい方が優先度"高"となります。プライオリティの数値が小さい(優先度"高")メールサーバに対し通報を行い、通報できなかった場合は、次のプライオリティのメールサーバに対し通報を行い、通報が成功するまで、または、登録されている全メールサーバに対して通報するまで、順

次通報を行います。

まず、現在登録されている通報先のリストと、コマンドプロンプトが出力されます。最初はリストが空なので、何もありません。

[priority]	comment	address	auth

[Q]uit/[R]eread/[Number]/[Help]: ?			

コマンドプロンプトに対して、1 番目の通報先を登録するために ‘1’ を入力します。1 番は登録されていないので追加する旨を問い合わせてくるので、 ‘y’ を入力してください。

there is no such ID number: 1 do you want to add an entry id 1? [Y]/n? y

次に、この通報先の情報を入力します。

input address IP address[] 10. 1. 1. 1	← SMTP サーバのアドレス
comment[] mailserver1	← コメント (通信には使用しない)
from[] xxxxx@xxxxx. co. jp	← 発信元メールアドレス

発信元メールアドレスは、適切なアドレス(システム管理者など)を設定してください。

次に、メールサーバの SMTP 認証の設定を行います。SMTP 認証が不要な場合は、‘off’ で終了です。

smtpauth (on / off) [] off	← SMTP 認証の設定 (off / on)
----------------------------	-------------------------

SMTP 認証が必要な場合は、認証を‘on’にして、認証ユーザ名とパスワードを登録します。

smtpauth (on / off) [] on	← SMTP 認証の設定 (off / on)
userid[] abcdef	← 認証ユーザ名
password[] mai/1234	← 認証パスワード

【補足】 パスワードは、セキュリティ確保のために暗号化して登録されます。入力した値と異なりますが、正常な動作です。

【注意】 設定変更時、” password[] “ プロンプトで何も入力せず、[Enter]キーのみを押下しても、変更前のパスワードは引き継がれません。パスワードに変更が無い場合も、必ず再度入力してください。

全ての設定が終了すると以下のプロンプトを表示するので、良ければ‘y’を入力してください。

is it OK to save it? [y]/n ? y	← ‘y’を入力
--------------------------------	----------

入力が終了すると、サブメニュープロンプトが表示されます。特に修正がなければ、‘q’ で

このエントリの作業を終了します。

```
SUB MENU:1::[Q]uit/[E]dit/[D]elete/[C]opy: ? q
```

先ほど追加したエントリが表示されます。作業を終了する場合は、‘q’を入力してください。エントリを追加する場合は、次の番号となる‘2’を入力して作業を繰り返してください。

[priority]	comment	address	auth
[1]	mailserver1	10.1.1.1	off
[Q]uit/[R]eread/[Number]/[Help]: ? q			

終了すると、設定ファイル /home/necsts/sg/mail_server.sg に設定が保存されます。

ー注意事項ー

メールサーバの設定を誤ると、メール送信時に 10 回再送（約 20 分）が行われます。この間に、設定を修正しても、再送が完了するまで設定が反映されません。

4.4.4 https 通信情報の設定方法

通報には、保守センター宛の通報とお客さま宛での通報があります。このうち保守センター宛の通報は、https による通報と e-mail による通報のどちらかを選択できます。保守センター宛の通報を https にて行う場合は、次の設定を行なってください。

https 通報を選択しユーザ通報を利用しない場合もメールサーバの設定が必要となります。メールサーバの設定については 3.4.2 を参照ください

*** configure https

https report: NO ←現在の設定状態を表示します。(NO は https 通報を使用しない)
proxy server: NO ←現在の設定状態を表示します。(NO はプロキシを使用しない)
proxy address:0.0.0.0:8080 ←現在の設定状態を表示します。
entry is edit OK?[Y]/n > y ←現在の設定状態を変更する場合は y を入力します。

上記で y を入力すると以下のメッセージが表示されます。
https 通報を使用する場合 y を、使用しない場合は n を入力します。

```
https reported uses?y/[N] >y ←https 通報を使用する場合は y を入力します。
```

上記で y を入力すると以下のメッセージが表示されます。
プロキシサーバを使用する場合 y を、使用しない場合は n を入力します。

```
proxy server uses ? y/[N] > y ←プロキシサーバを使用する場合は y を入力します。
```

上記で y を入力すると以下のメッセージが表示されます。
プロキシサーバの IP アドレスとポート番号を入力します。
ポート番号を入力しないと 8080 が自動的に設定されます。

```
input proxy server IP address [0.0.0.0] > 10.10.10.10:8080
```

最後に入力内容の確認が表示されます。内容を確認し間違いなければ **y** を入力します。

https report: YES

proxy server: YES

proxy address: 10.10.10.10:8080

this entry is OK?[Y]/n >y ←内容を確認し、保存する場合は **y** を入力する

4.4.5 cron 定期実行時刻情報の設定登録

cron 定期実行時刻情報として設定するのは、毎日行う定期処理の処理開始時刻です。

最初に、現在の設定時刻が表示されます。変更の必要がなければ'y'を、変更する場合は'n'を入力してください。通報の集中を防ぐため、可能な限り既定値から変更してください。

また、被監視サーバからの情報取得が集中するのを防ぐため、マスタ・スレーブ構成の場合は、マスタ・スレーブ間で定期通報の実行時刻を 1 分以上ずらすことを推奨します。

```
*** configure crontab.  
crontab daily report time is 1:10  
OK? [Y]/n > n
```

次に、設定する時刻を入力します。この時、二通りの入力方法が可能です。

a) の入力方法は、「開始時-終了時 (例 6-23)」を指定して、ランダムな時刻を設定します。この例では、6:00~23:00 の間でランダムな時刻を設定します。

b) の入力方法は、設定する時刻を「時:分(例 12:45)」の 24 時間表記で入力します。

a) input time (start_hour-e_hour / hh:mm) > 6-23
b) input time (start_hour-e_hour / hh:mm) > 12:45

入力すると、ランダムに発生した時刻、または設定した時刻が表示されます。入力が必要な場合は、再度、正しい値を入力してください。設定が正しければ、'y'で終了します。

```
crontab daily report time is 12:45  
OK? [Y]/n > y  
writing /home/necsts/sg/cron.sg ... OK.
```

上記のメッセージで、設定ファイル/home/necsts/sg/cron.sg が作成されます。設定が終わると、以下の注意事項が表示されます。

```
NOTE: If Manager is running, please restart Manager.
```

これは、Manager を既に起動している場合、Manager を再起動しないと cron に設定が反映されないためです。インストール時の設定の場合は、Manager を起動した時に cron に設定が反映されるので、再起動は不要です。

4.4.6 アラーム通報先のメールアドレス登録

リソース監視や死活監視のアラーム通報、ライセンス有効期限残存日数通知等の通報先メールアドレスを設定します。監視しているサーバのダウンや障害の検出機能の異常をお客様の管理者に通報したり、ライセンスの期限切れを防ぐために、メールアドレスを設定することを強く推奨いたします。

以下のプロンプトが表示されるので、メールアドレスを設定してください。

```
*** configure e-mail address of user. (to send Alarm)
input e-mail address [dummy@com] > user@user.domain
OK? [Y]/n > y
```

メールを受け取る方が複数の場合は、`user1@user.domain,user1@user.domain` のように、空白をあげずにカンマで区切って登録してください。このとき、メールアドレスの文字列の長さは 127 文字以下にしてください。メールアドレスに誤りがあると、誤送信や通報が不達などの元になりますのでご注意ください。

また、デフォルト値の `dummy@com` に設定すると、アラーム通報そのものが送信されません。この場合でも、障害通報は保守会社宛に送信されます。

設定したメールアドレスでよければ、`y` を入力して終了します。

アラーム通報の宛先は、ユーザ定義辞書 `/home/necsts/dic/user.dic` の中に設定されます。

4.4.7 SNMP の設定

ブレードエンクロージャー (BE600/BE1000)、BMC (7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128)、7320H-256/8160H-256/9160H-256 の SNMPTrap による障害通報設定を行います。

監視サーバが監視できる SNMPTrap 監視機器の台数は、最大 50 台となります。

ブレードエンクロージャーを除く SNMP Trap 監視対象機器については、監視対象側においても Manager に対して Trap を送信する設定が必要となります。

Master/Slave 構成で監視を行なう場合は、Master および Slave に対して、監視対象機器から Trap を送信する設定にしてください。(詳しくは各装置のオペレーションマニュアルを参照してください。)

冗長 OA (Onboard Administrator) を搭載したエンクロージャーを監視する場合は、エンクロージャーの OA の設定” Enclosure IP Mode” を enable にする必要があります。設定方法は、4.5.6 章を参照してください。

マスタ・スレーブ構成をとっている場合は、SG ファイルの登録順を厳密に一致させる必要があります。

そのため、マスタ・スレーブ構成の場合は スレーブ側での SG 設定はせず、マスタで設定した以下の SG ファイルをスレーブにコピーしてください。

```
{インストールディレクトリ}/sg/snmptrap.sg
```

マスタで SNMP Trap 監視機器の設定を変更した場合は、その都度スレーブに上記ファイルをコピーしてください。

SNMPTrap 監視機器一覧が下記のように表示されます。追加する場合は[a]、編集する場合は[m]、削除する場合は[d]、終了する場合は[q]を押下します。

```
*** configure sts snmptrap
id:ip          RackType  UserSystem  Serial  Kousei  Racknum
=====
0: 10.32.179.181 7020M-16 123 543 666 1
input command ([a]dd / [m]odify / [d]elete / [s]how / [q]uit) >
```

注意事項

追加、編集、削除した内容は、[q]を押下して終了しないとファイルに反映されません。

追加 (a) を押下して、必要な項目を入力します。

```
input command ([a]dd / [m]odify / [d]elete / [s]how / [q]uit) > a
input Snmp machine_type > BE600 ←機種名を入力します。登録できる機種名は表 4.4.8
OK? [Y]/n > y                  を参照
```

表 4.4.8 SNMPTrap 設定可能機種名一覧

BE600	BE1000	7320H-256
7020M-16	7040M-32	7080H-64
8020M-32	8040M-64	8080H-128
8160H-256	9160H-256	

機種名以降の入力内容は、入力した機種名によって異なります。

1) BE600/BE1000 を入力した場合

```
input Snmp IP > 10.10.12.11      ←エンクロージャーの IP アドレスを入力
OK? [Y]/n >
Use ssh instead of telnet
OK? y/[N] >                     ←監視機器に ssh で接続する場合は y を入力
input Snmp UserSystemCode > 123ABC0005
OK? [Y]/n > y
input Snmp Serial-Number > USR001
OK? [Y]/n > y
input Snmp Kousei-Number > NXL-100
OK? [Y]/n >
input Snmp Rack-Number > Rack001
OK? [Y]/n > y
input Snmp Telnet-User or Ssh-User > BE600-Admin ←エンクロージャーにログインする
OK? [Y]/n >                      ユーザを入力
input Snmp Telnet-Passwd or Ssh-Passwd > BE600-passwd ←エンクロージャーにログインする
OK? [Y]/n > y                  パスワードを入力する
```

2) 7320H-256/8160H-256/9160H-256 を入力した場合

```
input Snmp IP > 10.10.12.11      ←OA の IP アドレスを入力
OK? [Y]/n >
Use ssh instead of telnet
OK? y/[N] >                     ←監視機器に ssh で接続する場合は y を入力
input Snmp UserSystemCode > 123ABC0005
OK? [Y]/n > y
input Snmp Serial-Number > USR001
OK? [Y]/n > y
input Snmp Kousei-Number > NXL-100
OK? [Y]/n >
input Snmp Rack-Number > Rack001
OK? [Y]/n > y
input Snmp Telnet-User or Ssh-User > User      ←OA にログインするユーザを入力
OK? [Y]/n >
input Snmp Telnet-Passwd or Ssh-Passwd > Passwd ←OA にログインするパスワード
```

```

を入力
OK? [Y]/n >
input 6120XG Switch1 Passwd > passwd0 ←6120XG Switch1 のパスワードを入力(※)
OK? [Y]/n >
input 6120XG Switch2 Passwd > passwd1 ←6120XG Switch2 のパスワードを入力(※)
OK? [Y]/n >

```

(※)9160H-256 の場合、6120XG Switch のパスワード入力プロンプトは表示されません。

3) 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 を入力した場合

```

input Snmp IP > 10.10.12.11 ←SM の IP アドレスを入力
OK? [Y]/n >
input Snmp UserSystemCode > 123ABC0005
OK? [Y]/n > y
input Snmp Serial-Number > USR001
OK? [Y]/n > y
input Snmp Kousei-Number > NXL-100
OK? [Y]/n >
input Snmp Rack-Number > Rack001
OK? [Y]/n > y
input PM[0] IP address > 10.10.20.21 ←PM0 の IP アドレスを入力
OK? [Y]/n > y
do you validate PM[1]?[Y]/n > y ←PM 1 を監視する場合は y を入力
input PM[1] IP address > 10.10.20.22 ←PM1 の IP アドレスを入力
OK? [Y]/n > y
do you validate PM[2]?[Y]/n > n ←PM2 以降を監視しない場合は n を入力

```

また「NX7700i/7020M-16、7040M-32、7080H-64 メンテナンスマニュアル」の「5.2 Out-of-bound 通報の設定」に従い通報先の設定を行ってください。

NX7700i/8020M-32、8040M-64 8080H-128 も同様の設定を行ってください。

4.4.8 SSH の設定

1) 概要

筐体の MP や BMC の SM/PM、ブレードエンクロージャーおよび 8160H-256/9160H-256 の OA に接続する際に ssh を選択した場合に使用する、ssh コマンドと秘密鍵の設定を行います。

NX リモート通報は、HP-UX 標準の ssh コマンド(OpenSSH)を使用して ssh 接続を実現しています。ssh コマンドが無い環境では、telnet を使用して接続してください。

ssh と MP や SM/PM、OA のバージョンの組み合わせでは、ssh ログインできない場合があります。対象のサーバに対して、事前にログインできることを確認してから利用してください。

接続できない場合、鍵交換アルゴリズム diffie-hellman-group1-sha1 を ssh コマンドが使用しないことが原因である場合があります。この場合は、ssh の設定 (/opt/ssh/etc/ssh_config)を変更することで diffie-hellman-group1-sha1 を使用するように変更できますが、脆弱性の問題があることを十分ご理解の上、ご使用ください。

ssh の設定変更方法については、OpenSSH のマニュアル等をご参照ください。

ssh 接続の対象となるサーバと認証方式は以下のとおりです。

機種名	接続先	認証方式	備考
8010E-16 9010E-16	MP	パスワード認証	
8020B-32 8040B-64	MP	パスワード認証	
	OA	パスワード認証	
8020M-32 8040M-64 8080H-128	PM	パスワード認証	
8160H-256 9160H-256	MP	パスワード認証	
	OA	パスワード認証 公開鍵認証	公開鍵認証方式は Administrator のみ 設定可能

各サーバの ssh 接続設定については、各サーバのマニュアルを参照してください。

2) 手順

2-1) 新規登録

*** configure OpenSSH command info.

OpenSSH command path: "" ←現在の設定状態（初期値は未設定）
 Passphrase: "" ←現在の設定状態（初期値は未設定）
 entry is edit OK?[Y]/n > y ←現在の設定状態を変更する場合は y を入力する

ssh を利用する場合は、y を入力して ssh コマンドを登録します。

上記で y を入力すると以下のメッセージが表示されます。

ssh コマンドのフルパスのファイル名(最大 255 文字)を入力してください。

Input OpenSSH command path <> /usr/bin/ssh ←ssh コマンドのパスを入力する

次に秘密鍵のパスフレーズ(最大 64 文字)を入力します。ただし、パスフレーズにカンマは使用しないでください。

公開鍵認証方式を使わない場合や秘密鍵にパスフレーズを設定していない場合は入力せずに、[Enter]キーのみ入力してください。

パスフレーズは入力した文字がエコーバックされますので、周囲にご注意ください。

なお、SG ファイルには暗号化して保存されます。

Input Passphrase > passphrase ←秘密鍵のパスフレーズを入力する

入力が完了すると設定値を出力します。

OpenSSH command info :
 OpenSSH command path: /usr/bin/ssh
 Passphrase: *****
 this entry is OK?[Y]/n > y

2-2) 登録の修正

既に設定した状態で ssh 設定を実行すると、現在の設定状態を表示します。

```
*** configure OpenSSH command info.  
  
OpenSSH command path: /usr/bin/ssh ←現在の設定状態  
Passphrase: *****(*) ←現在の設定状態  
entry is edit OK?[Y]/n > ←設定状態を変更する場合は y を入力する
```

秘密鍵のパスフレーズを設定されている場合は、"****(*)"が表示され、設定されていない場合は、何も表示されません。

現在の設定を変更する場合は、y を入力します。

上記で y を入力すると以下のメッセージが表示されます。
ssh コマンドのフルパスのファイル名を入力してください。

```
Input OpenSSH command path </usr/bin/ssh> > /opt/ssh/hpux64/bin/ssh
```

ここで入力を省略した場合、以前のパス情報(例では /usr/bin/ssh)はセットされません。同じパスを登録する場合でも必ず入力してください。

次に秘密鍵のパスフレーズを入力します。公開鍵認証方式を使わない場合や秘密鍵にパスフレーズを設定していない場合は入力せずに、[Enter]キーのみ入力してください。

以前の設定時にパスフレーズが登録されていた状態で、[Enter]キーのみ入力した場合は、以前登録したパスフレーズは消去されます。必要な場合は再度入力してください。

パスフレーズは入力した文字がエコーバックされますので、周囲にご注意ください。なお、SG ファイルには暗号化して保存されます。

```
Input Passphrase > passphrase ←秘密鍵のパスフレーズを入力する
```

入力が完了すると設定値を出力します。

```
OpenSSH command info :  
OpenSSH command path: /opt/ssh/hpux64/bin/ssh  
Passphrase: *****(*)  
this entry is OK?[Y]/n >
```

この設定でよければ y を入力して終了してください。設定をやり直す場合は、n を入力してください。

2-3) 登録の削除

ssh 設定を削除する場合は、OpenSSH command path: および、Passphrase: プロンプトにおいて、[Enter]キーのみ入力してください。

```

*** configure OpenSSH command info.

OpenSSH command path: /usr/bin/ssh
Passphrase: ****
entry is edit OK?[Y]/n > y
Input OpenSSH command path </usr/bin/ssh> >

OpenSSH command info :
OpenSSH command path: ""
Passphrase: ""
this entry is OK?[Y]/n > y

```

4.4.9 データディレクトリの設定

1) 概要

NX リモート通報は/home/necsts にインストールされ、設定ファイルやログファイルもインストールディレクトリ下に出力されます。本設定を行うことで、設定ファイルやログファイルを別のディレクトリに格納することができます(以下設定したディレクトリをデータディレクトリと呼称)。

データディレクトリ設定のメリットは以下となります。

- ・ /home に容量の余裕がない場合、ログの出力先を変更できる。
- ・ バージョンアップ時の設定ファイルのバックアップができる。

本設定によりデータディレクトリに格納対象となる NX リモート通報のファイル（以下データファイルと呼称）は以下の通りです。

```

/home/necsts/sg の全ファイル
/home/necsts/log の全ファイル
/home/necsts/tmp の全ファイル
/home/necsts/dic/user.dic

```

また、データディレクトリ設定後の設定ツールによる設定変更はデータディレクトリ下のファイルに対して行われます。

【注意】

SNMP の設定（4.4.7 章）を有効にし、かつ WebSAM と連携する場合は、データディレクトリ設定は使用しないでください。

2) 手順

2-1)以下のメッセージが表示されます。

- ・ データディレクトリを使用する場合は **y** を入力してください。
- ・ データディレクトリを使用しない場合は **n** または **Enter** を入力してください。

```

*** configure Data Directory uses?
y/[N] >

```

既にデータディレクトリを設定している場合は、以下のメッセージが表示されます。

```

*** configure Data Directory uses?
Y/[n] >

```

- ・ データディレクトリの変更、確認を行う場合は **y** または **Enter** を入力してください。
- ・ データディレクトリ設定の取り消しを行う場合は、**n** を入力してください。

2-2)以下のメッセージが表示されます。

- ・ データディレクトリに使用するディレクトリの絶対パスで入力してください。

```
y/[N] > y
input data directory path [/DATA/necsts] ←存在するディレクトリの絶対パスを
入力
```

【注意】

指定するディレクトリにネットワークディレクトリ（NFS）は指定できません。

既にデータディレクトリの設定を行っている場合は、以下のメッセージが表示されます。

- ・ データディレクトリを変更する場合は、新しいパスを入力してください。
- ・ データディレクトリを変更しない場合は、**Enter**を入力してください。

```
Y/[n] > y
input data directory path [/DATA/necsts]
```

データディレクトリに存在しないディレクトリを入力すると以下のメッセージが表示されます。

```
input directory doesn't exist.
Do you keep setting it?[Y]/n >
```

入力した内容を確認し、内容が間違っていない場合は **Y** を入力してください。ディレクトリが存在しなくても、次の 2-3)のファイルコピー処理時にディレクトリが作成されます。入力した内容が間違っている場合は **N** を入力して入力をやり直してください。

2-3)データディレクトリの新規設定や変更、取り消しを行うと以下のメッセージが表示されます。

```
do you copy data files?[Y]/n >
```

Y または Enter キーを入力するとデータファイルを設定したデータディレクトリにコピーします。

コピー元とコピー先の関係は下表となります。コピーの必要はない場合は n を入力してください。(コピー必要の有無は後述の補足参照)

データディレクトリ設定コピー条件表

No.	設定条件	コピー元	コピー先
1	新規設定時	/home/necsts	設定したデータディレクトリ
2	設定変更時	変更前データディレクトリ	変更後データディレクトリ
3	設定取消時	設定していたデータディレクトリ	/home/necsts

【注意】

データディレクトリ下にデータファイルが存在しない場合は、Manager の起動や設定ツールの起動が失敗します。データディレクトリ下にデータファイルが存在しない場合は、必ずコピーを実行してください。

コピーが成功すると以下のメッセージが表示されます。

```
copy /home/necsts/sg /DATA/necsts/sg
copy /home/necsts/log /DATA/necsts/log
copy /home/necsts/tmp /DATA/necsts/tmp
copy /home/necsts/dic/user.dic /DATA/necsts/user.dic
copy complet
```

【補足】コピーの必要がない場合

既にデータディレクトリ下にデータファイルが存在し、そのデータファイルを継続して使用する場合はコピーの必要はありません。

例)

データディレクトリを使用している状態で Manager ソフトをバージョンアップし、同じデータディレクトリを再設定した場合。

ここまでで、config --set による設定が終了します。

4.4.10 TFTP サーバの設定

7320H-256/8160H-256 を被監視エンクロージャーとして障害監視を行う場合、tftp サーバ機能を設定する必要があります。設定しない場合、6120XG Blade Switch のログの一部が取得できませんが、他のログ取得に支障はありません。

9160H-256 では、TFTP の設定は不要です。

1) TFTP サーバ設定手順

以下の作業は root ユーザにて行います。

①/etc/inetd.conf をエディタで開き、以下の内容が記載されていることを確認します。

記載されていない又はコメント化されている場合は、記載してください。

```
# Before uncommenting the "tftp" entry below, please make sure
# that you have a "tftp" user in /etc/passwd. If you don't
# have one, please consult the tftpd(1M) manual entry for
# information about setting up this service.

tftp          dgram  udp  wait   root /usr/sbin/tftpd    tftpd¥
              /opt/ignite¥
              /var/opt/ignite
```

②以下の**太字アンダーバー**の内容を追記します。

```
# Before uncommenting the "tftp" entry below, please make sure
# that you have a "tftp" user in /etc/passwd. If you don't
# have one, please consult the tftpd(1M) manual entry for
# information about setting up this service.

tftp          dgram  udp  wait   root /usr/sbin/tftpd    tftpd¥
              /opt/ignite¥
              /home/necsts/tmp¥
              /var/opt/ignite
```

この際、4.4.9 章でデータディレクトリの設定を行っている場合は、「/home/necsts」を設定したディレクトリとして記載してください。

③/etc/services をエディタで開き、以下の内容が記載されていることを確認します。

記載されていない又はコメント化されている場合は、記載してください。

```
tftp          69/udp          # Trivial File Transfer Protocol
```

④以下のコマンドを実行して/etc/inetd.conf を再読み込みします。

```
>inetd -c
```

2) TFTP サーバ設定の動作確認

①/home/necsts/tmp にサイズが 0 のファイル「tftptest.txt」を作成します。

作成したファイルのパーミッションを確認し、書き込み可能であることを確認してください。

なお、4.4.9 章でデータディレクトリの設定を行っている場合は、/home/necsts/tmpではなく、「設定ディレクトリ/tmp」になります。

```
# ls -l
total 0
-rw-rw-rw-  1 necsts  users          0 Aug 30 10:38 tftpptest.txt
```

作成したファイルのパーミッションを確認します。

②以下のコマンドを実行します。

```
# tftp localhost
tftp> put /tmp/ntlc.9830 /home/necsts/tmp/tftpptest.txt
                ※1                ※2

Sent 12474 bytes in 0.0 seconds
tftp> quit
```

※1 存在している任意のファイルを指定します。

※2 データディレクトリの設定を行っている場合は、/home/necsts は
設定ディレクトリになります。

③/home/necsts/tmp/tftpptest.txt が上記※1 で指定したファイルと同じサイズになっていることを確認します。

④確認が終了したら、/home/necsts/tmp/tftpptest.txt を削除します。

4.4.11 定期通報抑止の設定方法

マネージャの定期通報には被監視サーバのコンソールログが含まれます。マイナンバーを扱うサーバを監視する場合は以下の設定で定期通報を停止し、コンソールログが送信されないようにしてください。

sg/sts_parameter.sg の「STSLOG_MAIL_FLAG」の値を 1 から 0 に変更しマネージャを再起動してください。

但し、本設定を行うと保守センターにおける障害解析に影響を与える可能性がありますのでマイナンバーを扱わない場合は設定を変更しないで下さい。

4.5 Agent ソフトのインストールと被監視サーバの設定

4.5.1 Agent ソフトのインストール

－注意事項－

インストールは root 権限を持ったユーザで実施願います。

root 権限を持たないユーザで作業を行った場合、以下のエラーが表示されます。

ERROR: you have to be root to run this program.

Agent をインストールすると、/etc/syslog.conf に以下の行が追加されます。

kern,daemon.warning /dev/console

これによって syslog.log に出力される Warning レベル以上のメッセージが /dev/console に出力されます。Warning、Critical、Error レベルのメッセージを出力したくない場合は、7.1.2 章(9)及び(10)の作業を行ってください。但し Warning、Critical、Error レベルの障害通報が行われません。

媒体 (CD-ROM)、もしくは、Web サイトからダウンロードした物件を格納した CD-ROM を使用します。

root でマシンにログインし、インストール CD をマウントして、インストールコマンドを実行します。以下の説明は、CD を /CDROM ディレクトリにマウントした際の例です。また、Web よりダウンロードしたファイルの場合、/CDROM はファイル一式を置いたディレクトリ名に適宜読み替えてください。

```
# mount -F cdfs -r -o cdcase /dev/dsk/c0t0d0 /CDROM
```

※ftp 転送時、mount コマンドは実施不要

```
# /sbin/sh /CDROM/hpux/install.sh
```

注) デバイス名(例: /dev/dsk/c0t0d0)は、マシンにより異なります。

事前に `ioscan -fnkC disk` コマンド等で CD/DVD ドライブのデバイス名を確認願います。

以下のようなプロンプトが表示された場合、パッケージ sts.dep を install.sh が見つけられないことを示しています。sts.dep のある場所を絶対パスで設定してください。

```
input package (sts.dep) path : /CDROM/hpux/sts.dep
```

注) パッケージ名は小文字で指示して下さい。

以下のようにメニューが表示されるので、Agent をインストールする場合は 2 を入力してください。

```
NX remote communicator install program.  
Copyright (c) 2014 NEC Corporation
```

1. install Manager
2. install Agent
3. install Resource_watch
- Q. QUIT

* Resource_watch : This program is the Resource watch feature set.

Enter selection:[1] 2

←メニュー番号を入力

途中で以下の SFM/EMS モードの選択メニューが表示された場合、運用状況に合わせてどちらかのモードを選択してください。選択メニューが表示されない場合は、EMS モードでのインストールになります。

```
*** select SFM/EMS mode.
```

1. SFM mode
2. EMS mode

Enter selection:[1] 1

←メニュー番号を入力

【注意】被監視サーバが以下の機種の場合は、EMS モードは選択しないでください。

7010B-8/7010B-16/7010B-32、7010E-8、70xxM/70xxH、7320H-256、8010B-16 / 8020B-32 / 8040B-64、8010E-16、80xxM / 80xxH、8160H-256/9160H-256、9010E-16

install.sh は swinstall を呼び出してインストールを実施します。画面には swinstall によるインストールの経過が表示されるので、エラーがないこと (“* Selection succeeded.” および “* Analysis and Execution succeeded.” と表示されること)を確認してください。

正常に終了すると、以下のように表示されます。

```
All install programs are successfully completed.
```

swinstallによって以下のファイルセットが/opt/necstsディレクトリ配下にインストールされます。

STS.STSTD	(Agent プログラム)
STS.PATCH_SVC	(パッチ診断用プログラム)
STS.config	(設定ツール)
STS.perl	(perl コマンドとライブラリ)

また、この swinstall により、以下の設定も自動的に反映します。

- ・ inetd の設定変更 [/etc/inetd.conf, /etc/services]
- ・ syslog.conf の設定変更 [/etc/syslog.conf]

リソース監視機能を使用する場合は、Agent ソフトのインストール後、再度インストールプログラムを起動し、3 (install Resource_watch)を選択してください。

4.5.2 SFM の設定

Agent ソフトのインストール中に SFM か EMS モードの選択メニューで 1 を入力した場合、SFM モードの設定を開始します。SFM モードの設定は自動で行われます。

```
EMS hardware monitors are disabled & SysFaultMgmt is monitoring devices.  
SFM mode OK.  
[press return to continue]
```

【被監視サーバを夜間停止する運用を行う場合の注意事項】

SFM モードでは、夜間に 2 つのバッチ処理が実行されます。インストール時には各々深夜 1 時と深夜 1 時 30 分に実行されるように設定されます。そのため、上記時間に被監視サーバを停止する運用を行われる場合、以下の手順で、バッチ処理実行時間を変更してください。（変更は Agent のインストール完了後に行ってください。）

- (1) 被監視サーバに root でログインし、以下のコマンドを実行します。

```
# cp /var/spool/cron/crontabs/root /opt/necsts/set_cron
```

- (2) /opt/necsts/set_cron をエディタで開き、以下の行を変更し保存します。
（変更例はバッチ実行時間を各々 1:00 から 12:00 と 1:30 から 12:30 に変更しています。）

変更例—変更前

```
# Entry for STS_SFM_MONITORING  
* * * * * /opt/necsts/getEvent  
0 1 * * * /opt/necsts/deleteEvent  
30 1 * * * /opt/necsts/sts_daily.sh
```

変更例—変更後

```
# Entry for STS_SFM_MONITORING  
* * * * * /opt/necsts/getEvent  
0 12 * * * /opt/necsts/deleteEvent  
30 12 * * * /opt/necsts/sts_daily.sh
```

- (3) 以下のコマンドを実行し、実行時間の変更を設定します。

```
# crontab /opt/necsts/set_cron  
# rm /opt/necsts/set_cron
```

- (4) 以下のコマンドを実行し、実行時間の変更が反映されていることを確認します。

```
# crontab -l  
  
# Entry for STS_SFM_MONITORING  
* * * * * /opt/necsts/getEvent  
0 12 * * * /opt/necsts/deleteEvent  
30 12 * * * /opt/necsts/sts_daily.sh
```

4.5.3 EMS の設定

Agent ソフトのインストール中に SFM か EMS モードの選択メニューで 2 を入力した場合、または選択メニューが表示されなかった場合、” [press return to continue]” というメッセージを出して停止します。ここでリターンキーを押すと、EMS の設定ツールが自動的に起動します。設定ファイルを変更した後、再び停止するので、リターンキーを押して EMS モニタの設定を継続します。

```
EMS hardware monitors are enabled & SysFaultMgmt is not monitoring devices.  
EMS mode OK.
```

```
config EMS monitor.
```

```
modify /var/stm/config/tools/monitor/default_disk_em.clcfg file...done.
```

```
[press return to continue]
```

```
restarting EMS monitor...
```

【中略：EMS 設定ツールのメッセージ】

```
Done.
```

```
[press return to continue]
```

【注意】 Agent ソフトを EMS モードでインストールする場合、SFM モードを ON (EMS モードを OFF) にしないでください。

【注意】 EMS モードを選択し、エラーメッセージ「**ERROR: sfmconfig error. please check /opt/sfm/bin/sfmconfig.**」が表示された場合は、EMS モードではインストールできません。SFM モードでインストールをやり直してください。

4.5.4 ライセンスコードの入力

SFM または EMS の設定が完了すると、次にライセンスコードの入力を行います。リターンキーを押して継続してください。

ライセンスコードの入力画面が表示されるので、ライセンスコードを入力してください。コードの入力が終わると確認の表示が行なわれるので、正しい場合は y を入力してください。入力が終わると、コードのチェックが行なわれます。正しいコードが入力されると、インストールは終了します。

【注意】 ライセンスコードの数字の 0(ゼロ)と英大文字の O (オー)／数字の 1(イチ)と英小文字の l (エル)の入力間違いにご注意ください。

```
*** configure codeID. (/opt/necsts/codeID)
input codeID value for this machine > ABCDEFGHIJKLMNOPQRS
codeID( ABCDEFGHIJKLMNOPQRS ) is OK? [Y]/n > y
current machine ID: 1234567890
licensed machine ID: 1234567890
License period: 2011/12/31
License flag: 0000000000
codeID is OK.
```

```
All install programs are successfully completed.
```

4.5.5 マネージャ(監視サーバ)の IP アドレス登録

インストールが終了したら、次に、マネージャの IP アドレスの登録を行ないます。

登録を行なうと、登録したマネージャからの接続のみを許可します。登録を行わない場合は、任意の IP アドレスからの接続を受け付けます。

以下のプロンプトに対して、[追加]の場合は ‘a’、[修正]の場合は ‘m’、[削除]の場合は ‘d’ を入力してください。

```
# /opt/necsts/config/config.pl --ststd_conf
*** configure ststd.conf
Manager server host IP list:
input command ([a]dd / [m]odify / [d]elete / [q]uit) >
```

[修正]・[削除]の場合は、修正や削除を行う IP アドレスのリストの番号を入力します。

[追加]・[修正]の場合は、次に新しい IP アドレスを入力します。

```
command: add IP address.
input IP address > 10.0.0.1
```

更新後の IP アドレスのリストが表示されるので、さらに追加する場合は、‘a’ を入力して操作を繰り返してください。

‘q’ によって設定を終了し、設定ファイル ststd.conf を作成します。

```
Manager server host IP list:
0: 10.0.0.1
1: 10.0.0.2
input command ([a]dd / [m]odify / [d]elete / [q]uit) > q
command: quit.
writing /opt/necsts/ststd.conf ... OK
```

上記のメッセージで、ファイルが正常に作成されたことを確認してください。

4.5.6 冗長 OA 搭載エンクロージャー(BE600/BE1000) および 7320H-256/8160H-256/9160H-256 の設定

冗長 OA (Onboard Administrator) を搭載のエンクロージャー(BE600/BE1000) および 7320H-256/8160H-256/9160H-256 を監視する場合は、エンクロージャーの OA の設定 “Enclosure IP Mode” を enable にする必要があります。

設定時の OA ログイン後の操作例を、以下に示します。

```
>enable enclosure_ip_mode
Enclosure IP Mode is enabled.
```

また、7320H-256/8160H-256/9160H-256 を監視する場合は、OA のコマンドプロンプトには “OA-1>”、“OA-2>” のように “OA-” で始まる値を設定するようにして下さい。

OA にログインした際、“OA>” などになる場合には、SET OA NAME コマンドで上記のように変更してください。詳細は、「HP Integrity Superdome 2 Onboard Administrator Command Line Interface User Guide」を参照してください。

4.5.7 ログ採取の設定

障害通報には `syslog` やカーネルバッファの内容が含まれます。マイナンバーを扱うサーバを監視する場合は、設定を変更して、これらのログが送信されないようにしてください。

但し、本設定を行うと保守センターにおける障害解析に影響を与える可能性がありますのでマイナンバーを扱わない場合は設定を変更しないで下さい。

採取対象のログ	制御フラグ	フラグ値
<code>syslog</code>	<code>ARCHIVE_SYSLOG</code>	YES : 採取する(デフォルト値) NO : 採取しない
<code>dmesg</code> の結果	<code>ARCHIVE_DMESG</code>	YES : 採取する(デフォルト値) NO : 採取しない

変更手順は以下の通りです。
`root` ユーザで作業してください。

設定ファイル「`LogCollector.conf`」を作成します。

※本ファイルはエージェントをインストールしても生成されません。

```
# mkdir -p /var/opt/ACTIVE/etc
# vi /var/opt/ACTIVE/etc /LogCollector.conf
```

以下の設定を記載します。

```
ARCHIVE_SYSLOG=NO
ARCHIVE_DMESG= NO
```

5. Manager の起動/停止

5.1 Manager の起動

まず、監視サーバに root でログインし /home/necsts/sts に移動した後、ユーザを necsts に切り替え、-start オプションをつけて ./stscrtl を実行します。

但しインストール時に既存ユーザを選択した場合はインストール時に指定したユーザに切り替えてから実行します。

```
# cd /home/necsts/sts
# su necsts
$ ./stscrtl -start
```

起動時に下のような Manager の状態が表示されます。

```
$ ./stscrtl -start
sts is not running.  ←Manager の起動状態表示
starting sts.
waiting sts is coming up...
:
sts main:
 20111 pts/ta    0:00 sts  ←Manager メインプロセスのプロセス番号
sts co-process:
[1] 20113 pts/ta    0:00 sts  ←コンソール出力メッセージ監視プロセスのプロセス番号
adding crontab entry for sts scheduled reporting...
10 1 * * * /home/necsts/sts/sts_cron.bat  ←定期処理自動実行設定
* * * * * /home/necsts/sts/stschk          ←Manager 動作確認設定
done.
```

起動に成功したかどうかは、テスト通報(6章)を実施して確認してください。

また cron.sg が正しく設定されたかどうか確認してください。adding crontab entry...のあと正しく cron.sg の内容が表示されていれば正常です。crontab -l コマンドを実行することでも確認できます。

起動した後、Manager は常駐プロセスとなります。以後、監視サーバをリブートした場合でも Manager は cron.sg の設定により自動的に起動します。

なお、以下のファイルにプロセス番号が記録されます。

/home/necsts/sts/sts.pid

稼動中かどうかの確認を、常駐プロセスの存在で判断する場合、上記ファイルに記載されているプロセスが生きているか、ps コマンド等で確認願います。

5.2 Manager の停止

監視サーバに root でログインし /home/necsts/sts に移動した後、ユーザを necsts に切り替え、-stop オプションをつけて ./stscrtl を実行します。

但しインストール時に既存ユーザを選択した場合はインストール時に指定したユーザに切り替えてから実行します。

```
# cd /home/necsts/sts
# su necsts
$ ./stsctrl -stop
```

上記のコマンドにより Manager が停止します。

```
(実行例)
$ ./stsctrl -stop
sts is running.
deleting crontab entry for sts scheduled reporting...
done.
sts has stopped.
delete socketfile
```

5.3 Manager の再起動

監視サーバに root でログインし /home/necsts/sts に移動した後、ユーザを necsts に切り替え、-restart オプションをつけて ./stsctrl を実行します。

但しインストール時に既存ユーザを選択した場合はインストール時に指定したユーザに切り替えてから実行します。

設定ファイルを変更した際には、再起動する事で新しい設定が有効になります

```
# cd /home/necsts/sts
# su necsts
$ ./stsctrl -restart
```

上記のコマンドにより Manager が停止した後、再起動します。Manager が動作していない場合には Manager を起動します。

```
(実行例)
$ ./stsctrl -restart
sts is running.
deleting crontab entry for sts scheduled reporting...
done.
sts has stopped.
delete socketfile
starting sts.
waiting sts is coming up...

sts main:
 20248 pts/ta    0:00 sts
sts co-process:
[1] 20250 pts/ta    0:00 sts
adding crontab entry for sts scheduled reporting...
10 1 * * * /home/necsts/sts/sts_cron.bat
* * * * * /home/necsts/sts/stschk
done.
```

5.4 Manager のステータス表示

監視サーバにログインし /home/necsts/sts に移動して、ユーザを necsts に切り替え、オプションをつけずに ./stsctrl を実行します。

但しインストール時に既存ユーザを選択した場合はインストール時に指定したユーザに切り替えてから実行します。

```
# cd /home/necsts/sts
# su necsts
$ ./stsctrl
```

以下のように Manager のステータスが表示されます。

```
$ ./stsctrl
sts is running.
sts main:
    8616 pts/ta    0:00 sts
sts co-process:
[1]  8618 pts/ta    0:00 sts
crontab setting for sts is:
10 1 * * * /home/necsts/sts/sts_cron.bat
    * * * * * /home/necsts/sts/stschk
```

6. テスト通報

6.1 テスト通報

【テスト通報の種類】

当該サービスには6種類のテスト通報機能があります。

まず、メールサーバ設定が正しいことを確認するために(1)を実施してください。

その後、被監視サーバの監視モードが SFM の場合は(5)、EMS の場合は(3)を実施してください。

SNMP Trap 対象機器を監視する場合は、(6)についても実施してください。

アラーム通報先とは 4.4.6 章で設定する“e-mail address”を指します。

初期状態(dummy@com)の場合、アラーム通報先には通報されません。

(1) 監視サーバからテスト通報を行う。(Manager テスト通報)

監視サーバと保守センター（NEC フィールドイング）間の導通確認を行います。

Manager から保守センターとアラーム通報先にテストメッセージが e-mail 又は https で通報されます。(アラーム通報先は e-mail のみ)

(2) 被監視サーバからテスト通報を行う。(ioscan テスト通報)

監視サーバと保守センター（NEC フィールドイング）間、および監視サーバと被監視サーバの間のコンソール出力メッセージ監視用 I/F の導通確認を行います。また、通報に先駆けて、被監視サーバ上で ioscan コマンドが実行され、Manager から保守センターにテストメッセージおよび ioscan 結果を含むコンソールログが e-mail 又は https で通報されます。また、Manager からアラーム通報先にはテストメッセージのみが通報されます。(アラーム通報先は e-mail のみ)

【注意】

ioscan テスト通報にはコンソールログが含まれます。マイナンバーを扱うサーバを監視する場合は実施しないでください。

(3) 被監視サーバからテスト通報を行う。(OS ログテスト通報 1)

監視サーバと保守センターの間の I/F と、監視サーバと被監視サーバの間のコンソールメッセージ監視用 I/F、および OS ログ収集用 I/F の導通確認を行います。Manager から保守センターのテストメッセージに OS ログが添付されて通報され、アラーム通報先にはテストメッセージのみが通報されます。

(4) 監視サーバからテスト通報を行う。(OS ログテスト通報 2)

監視サーバと保守センターの間の I/F と、監視サーバと被監視サーバの間のコンソールメッセージ監視用 I/F、および OS ログ収集用 I/F の導通確認を行います。Manager から保守センターのテストメッセージに OS ログが添付されて通報され、アラーム通報先にはテストメッセージのみが通報されます。

(5) 被監視サーバからテスト通報を行う。(SFM テスト通報)

監視サーバと保守センターの間の I/F と、監視サーバと被監視サーバの間の SFM イベント監視用 I/F の導通確認を行います。Manager から保守センターに OS ログが添付されたテストメッセージが e-mail 又は https で通報されます。アラーム通報先には通報されません。

(6) 被監視サーバからテスト通報を行う。(SNMP Trap テスト通報)

監視サーバと保守センターの間の I/F と、監視サーバと被監視サーバの間の HW ログ採収用 I/F の導通確認を行います。Manager から保守センターに HW ログが添付されたテストメッセージが e-mail 又は https で通報されます。アラーム通報先には通報されません。

【テスト通報確認方法】

アラーム通報先が設定されている場合は、テスト通報が成功すると、保守センタから自動応答メールが届きますので、内容を確認してください。

この場合、通報メールと合わせて 計 2 通のメールがアラーム通報先に届きます。

自動応答メールで確認できない場合は、保守センター・担当保守拠点の保守員にテスト通報の有無をご確認下さい（確認の際にユーザシステムコードが必要になります）。

テスト通報の成功が確認できない場合は、以下を参考にしてください。

テスト通報が行われたかどうかを確認する方法として、メール送信ログの内容を確認してください。メール送信ログは、ID-mail.log というファイル名（ID は監視サーバのリスト番号）で、/home/necsts/log ディレクトリ下に作成されています。

（データディレクトリ設定を行っている場合は、「設定したデータディレクトリ/log」ディレクトリ下です。）

・メール送信が成功した場合

```
2006/08/02 16:39:10 [INFO] starting sending a mail...
2006/08/02 16:39:10 [INFO] subject: sts alert mail
2006/08/02 16:39:10 [INFO] trying send email via server xxxxxxxx(*.*.*.*:25).
2006/08/02 16:39:10 [INFO] to:xxxxxx@fielding.nec.co.jp from:xxx@xxx.com
2006/08/02 16:39:10 [INFO] result: succeeded in sending email.
```

・メール送信に失敗した場合

```
2006/08/02 17:15:21 [INFO] trying send email via server xxxxxxxx(*.*.*.*:25).
2006/08/02 17:15:21 [INFO] to:xxxxxx@fielding.nec.co.jp from:xxxxxx@xxxx.com
2006/08/02 17:15:21 [INFO] result: failed to send email.
2006/08/02 17:15:21 [INFO] detailed smtp log is:
[[メールの送信ログの詳細を表示します]]
2006/08/02 17:15:23 [WARNING] failed to send e-mail.
2006/08/02 17:15:23 [WARNING] retry 120 secs later.
```

・https 送信が成功した場合

```
2011/11/08 17:18:06 [nec193] [INFO] trying send https to:xxx.co.jp/cgi-bin/Rep
2011/11/08 17:18:06 [nec193] [INFO] proxy server [xxx.xxx.xxx.xxx]:[8080]
2011/11/08 17:18:07 [nec193] [INFO] result: succeeded in sending https.
```

・https 送信が失敗した場合

```
2011/11/08 17:18:06 [nec193] [INFO] trying send https to:xxx.co.jp/cgi-bin/Rep
2011/11/08 17:18:06 [nec193] [INFO] proxy server [xxx.xxx.xxx.xxx]:[8080]
[[https の送信ログの詳細を表示します]]
2011/11/08 17:18:07 [nec193] [WARNING] failed to send e-mail.
2011/11/08 17:18:07 [nec193] [WARNING] retry 120 secs later.
```

- メールサーバの設定で SMTP 認証を on にしていない場合、以下のようなエラーを返します。
MAIL FROM:nxsts@fielding.nec.co.jp]
505 Authentication required
- 認証に失敗した場合、以下のようなエラーを返します。

AUTH CRAM-MD5

334 PDMYmZAwMjMjcUMTEzNjk2MzQ2NUBtYWIsLmpwLm5lYy5jb20+

MDAwMaAxMTEy1jg3NiA3ZTFmYzcxZjZhOWY1NTI1YWRiZjk2NjQyzDcxYjc4ZQ==

501 Unauthorized

- 認証ユーザ名に対応したメールアドレス以外からの送信を拒否した場合、以下のようなエラーを返します。

MAIL FROM:nxsts@fielding.nec.co.jp]

554 MAIL FROM does not match AUTH user

- プロキシサーバとの接続に失敗した場合、以下のようなエラーを返します。
(send_https_data) It failed connect. [プロキシサーバの IP アドレス]
- https サーバとの接続に失敗した場合、以下のようなエラーを返します。
(send_https_data) gethostbyname err [https サーバ URL]
- https サーバからエラーが返された場合、以下のようなエラーを返します。
(send_https_data) server err. host[https サーバ URL] status[エラーコード]
- OpenSSL の共有ライブラリのリンクに失敗した場合、以下のようなエラーを返します。
この場合は、Manager 起動ユーザ (necsts 又はインストール時に指定したユーザ) の環境変数 SHLIB_PATH に OpenSSL のライブラリのパスを指定してください。

/usr/lib/dld.sl: Can't open shared library: /usr/local/lib/libcrypto.sl

/usr/lib/dld.sl: No such file or directory

これらのエラーで送信できなかったメールは、

/home/necsts/tmp/failed.mail*.*.*

となって残ります。このメールは、次回にメールが正常送信できた場合に再送信されて、消えます。正常に送信できない場合は、3 日以上経つと定期実行プロセスにより消されます。

【マスタ・スレーブ構成の場合】

マスタ・スレーブ構成を取っている場合は、マスタとスレーブそれぞれからメールの通報が行われることをテストします。この場合、次のように実行してください。

- * マスタ側・スレーブ側の両方の Manager を停止します。
- * スレーブ側の Manager を起動します。マスタが起動していないので、この時、マスタモードとなって起動されます。
- * テスト通報を行います。スレーブ側の Manager から、メールが発信されることを確認してください。
- * 通報結果を確認した後、マスタ側の Manager を起動します。マスタが起動すると、自動的にスレーブ側がスレーブモードに変更されます。

6.1.1 Manager テスト通報

監視サーバ上で /home/necsts/sts/test_rep2 を実行することでテスト通報を行うことができます。テスト通報のメールは保守センターとアラーム通報先に通報されます。

```
(書式)
./test_rep2 1    ← 引数は 1 を指定する
```

```
(実行例)
# cd /home/necsts/sts
# su necsts
$ ./test_rep2 1
```

6.1.2 ioscan テスト通報

【注意】

ioscan テスト通報にはコンソールログが含まれます。マイナンバーを扱うサーバを監視する場合は実施しないでください。

被監視サーバ上でコマンドを実行することでテスト通報を行うことができます。コマンドは 4.5 でインストール済みです。

```
# /opt/necsts/test_mail.sh -ioscan
(ioscan が実行され結果がシステムコンソールに表示されます)
(テスト通報メッセージがシステムコンソールに表示されます)
Done.
```

上記コマンドを実行することにより、テスト通報のメールが保守センターとアラーム通報先に通報されます。保守センターへの通報メールには **ioscan** の実行結果が含まれる OS コンソールログが添付されますが、アラーム通報先にはテストメッセージのみが通報されます。

6.1.3 OS ログテスト通報 (1)

被監視サーバ上でコマンドを実行することでテスト通報を行うことができます。コマンドは 4.5 でインストール済みです。

```
# /opt/necsts/test_mail.sh -os
(テスト通報メッセージがシステムコンソールに表示されます)
Done.
```

上記コマンドを実行することにより、テスト通報のメールが保守センターとアラーム通報先に通報されます。保守センターへの通報メールには OS ログが添付されますが、アラーム通報先にはテストメッセージのみが通報されます。

一度ログ収集を行うと、その後 30 分間ログ収集は抑制されます。テスト通報を行う際には事前に **ps** コマンドで **LogCollector.sh** が起動していない事を確認した上で、ログ収集の管理ファイル **NEC_LOGCOLLECTOR_LOCK** を削除しておいてください。本削除により 30 分抑制がリセットされます。

ps コマンドで **LogCollector.sh** が残っている場合は前回のテスト通報が完了していないので完了するまで待ってください。

```
# ps -ef | grep LogCollector.sh
# rm /var/tmp/.NEC_LOGCOLLECTOR_LOCK
```

6.1.4 OS ログテスト通報 (2)

監視サーバから、被監視サーバのエージェントに対してコマンドを発行して、テスト通報を行なう方法です。

```
# cd /home/necsts/sts
# ./testrep 被監視サーバの IP アドレス
  (テスト通報メッセージが被監視サーバのシステムコンソールに表示されます)
#
```

上記コマンドを実行することにより、テスト通報のメールが保守センターとアラーム通報先に通報されます。保守センターへの通報メールには OS ログが添付されますが、アラーム通報先にはテストメッセージのみが通報されます。

テスト通報を行う際には事前にエージェントのサーバにログインし **ps** コマンドで **LogCollector.sh** が起動していない事を確認した上で、ログ収集の管理ファイル、**NEC_LOGCOLLECTOR_LOCK** を削除しておいてください。

削除方法は、[6.1.3](#)と同じです。

6.1.5 SFM テスト通報

被監視サーバ上でコマンドを実行することでテスト通報を行うことができます。コマンドは 4.5 でインストール済みです。

このテストは **Agent** を **SFM** モードでインストールした被監視サーバでのみ実行できます。また、コマンド実行は **root** ユーザで行う必要があります。

```
# /opt/necsts/test_mail.sh -sfm
Sending test event for memory monitor.
Done.
```

上記コマンドを実行することにより、OS ログが添付されたテスト通報のメールが保守センターに通報されます。

但し被監視サーバが 7020M-16,7040M-32,7080H-64,8020M-32,8040M-64,8080H-128 の場合は、上記コマンドは使用できません。代わりに下記のコマンドを実行してください。

```
#/opt/sfm/bin/nec_provider_test -t -m
Sending test event for NEC_Memory_IndicationProviderIA.
```

これらのテスト通報を行うコマンドを実行した時、下記のエラーメッセージが出力されていないことを確認してください。

下記のエラーメッセージが出力された場合、**SFM** が正常に動作していることを確認してください。

```
SysFaultMgmt is not running.
Please use the command 'cimprovider -ls' to check the state of SFMProviderModule.
```

テスト通報を行う際には事前に **ps** コマンドで **LogCollector.sh** が起動していない事を確認した上で、ログ収集の管理ファイル、**NEC_LOGCOLLECTOR_LOCK** を削除しておいてください。

削除方法は、[6.1.3](#)と同じです。

【メールログに出力されない場合】

- SFM モードで運用されていない

以下のコマンド実行し、表示されたメッセージを確認してください。

```
/opt/sfm/bin/sfmconfig -w -q
```

以下のいずれかが表示された場合は、SFM モード運用されています。

EMS hardware monitors are disabled & SysFaultMgmt is monitoring devices.

または

EMS hardware monitors are disabled & SysFaultMgmt is the current monitoring mode.

- 辞書と一致していない

辞書と一致していない場合、通報されません。Manager のバージョンを確認してください。

6.1.6 SNMP Trap テスト通報

- (1) ブレードエンクロージャーおよび 7320H-256/8160H-256/9160H-256 の場合
OA にログインして、下記のテスト用 SNMP Trap を送信してください。

```
enable snmp
test snmp
```

テスト通報結果は、6.1 【テスト通報確認方法】を参照して確認してください。

送信できない場合は、OA 上で **show snmp** コマンドを実行してレシーバの設定を確認してください。**Manager** のアドレスが設定されていない場合は追加してください。

OA のコマンドに関する詳細は、筐体のマニュアルを参照してください。

- (2) 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 の場合

① テストモードに遷移する

BMC から送信される SNMP Trap には障害種別が含まれていません。NX リモート通報は、一定期間内に同じ送信元から受信した SNMP Trap は保守センタに通報しないため、テスト中に発生した実際の障害が通報されなくなる恐れがあります。このため、以下の手順で BMC の通報抑止を解除してからテストを実行してください。

この作業は、ブレードエンクロージャーおよび 7320H-256 / 8160H-256 / 9160H-256 では不要です。

以下では、BMC の通報抑止を解除した状態を「テストモード中」と記載します。

監視サーバに root でログインし、インストールディレクトリに移動した後で、necsts ユーザに切り替えてから、BMC の通報抑止解除コマンドを実行します。

監視サーバ上で、/home/necsts/sts ディレクトリに移動して、necsts ユーザに切り替えます。

```
# cd /home/necsts/sts
# su necsts
$
```

BMC の通報抑止解除コマンドの簡単な使用法は、**-h** オプション付きで実行すると表示されます。

```
$ repctrl_test_bmc -h
usage: start test mode or non test mode.
    repctrl_test_bmc -h                : print help.
    repctrl_test_bmc                  : print status.
    repctrl_test_bmc -status           : print status.
    repctrl_test_bmc -start all        : start test mode to 30 minutes (all)
    repctrl_test_bmc -start 1          : start test mode to 30 minutes (ID==1)
    repctrl_test_bmc -start 10.0.0.1   : start test mode to 30 minutes (10.0.0.1)
    repctrl_test_bmc -start all 06:00  : start test mode to 06:00
    repctrl_test_bmc -start all 12/01 06:00 : start test mode to 12/01 06:00
    repctrl_test_bmc -stop all         : stop test mode (all)
    repctrl_test_bmc -stop 1           : stop test mode (ID==1)
    repctrl_test_bmc -stop 10.0.0.1    : stop test mode (10.0.0.1)
```

repctrl_test_bmc は、BMC 単位でテストモードに設定することができます。
BMC 単位で設定するためには、repctrl_test_bmc -status を実行した出力結果から ID や IP アドレスを確認して、-start の引数に設定してください。
-start の引数に “all” を指定した場合は、全ての BMC がテストモードに設定されます。

テストモード中の時間はデフォルトで 30 分間です。時間がかかることが予想される場合は、-start オプションに続けて、日付や時刻を指定することも可能です。

② テストの実施と確認

Web コンソールから対象となる全ての SM, PM にテスト用 SNMP Trap を送信してください。

HW ログが添付されたテスト通報のメールが保守センターに通報されます。
通報が送信されない場合は、Web コンソール上で SNMP Trap の送信先 IP アドレスを確認してください。

Web コンソールの使用方法については、筐体のマニュアル等を参照してください。

③ テストモードの解除

テストモードから通常監視モードへは sts ディレクトリの repctrl_test_bmc コマンドを用いて遷移します。

repctrl_test_bmc の簡単な使用法は、-h オプション付きで実行すると表示されます。

repctrl_test_bmc は BMC 単位でテストモードを終了できます。

BMC 単位でテストモードを終了させるためには、repctrl_test_bmc -status を実行した出力結果からテストモード中の ID や IP アドレスを確認して、-stop の引数に設定してください。

-stop の引数に “all” を指定した場合は、全ての BMC のテストモードが終了します。

7. アンインストール方法及びメンテナンス

7.1 アンインストール

==注意事項==

Manager と Agent を同じサーバにインストールしている場合、パッケージのアンインストールを実行すると、Manager と Agent の両方がアンインストールされます。

7.1.1 Manager ソフトのアンインストールと監視サーバの設定変更

以下の手順にしたがって、監視サーバ上で Manager ソフトをアンインストールしてください。

(1) Manager の停止

```
# cd /home/necsts/sts
# su necsts
$ ./stscrtl -stop
$ ^D          ←Ctrl-D で su から抜ける
#
```

以降は、root で実施してください。

(2) パッケージのアンインストール

```
# swremove STS
```

必要であれば作成したアカウント necsts を消去し、設定した cron 使用権なども消去してください。

(3) ユーザ necsts の削除

```
# userdel -r necsts
```

(4) /var/adm/cron/cron.allow から necsts を削除

7.1.2 Agent ソフトのアンインストールと被監視サーバの設定変更

以下の手順にしたがって、被監視サーバ上で Agent ソフトをアンインストールしてください。

(1) リソース監視のための cron 指定を解除(リソース監視ありの場合)

```
# su necsts
$ crontab -r
$ ^D          ←Ctrl-D で su から抜ける。
```

以降は、root で実施してください。

(2) SFM 監視のための cron 設定を解除(インストール時に SFM モードを選択した場合)

```
# cp /var/spool/cron/crontabs/root /opt/necsts/set_cron

/opt/necsts/set_cron から以下の行を削除
# Entry for STS_SFM_MONITORING
* * * * * /opt/necsts/getEvent
0 1 * * * /opt/necsts/deleteEvent
30 1 * * * /opt/necsts/sts_daily.sh

# crontab /opt/necsts/set_cron
```

```
# rm /opt/necsts/set_cron
```

- (3) パッケージのアンインストール

```
# swremove STS
```

- (4) ユーザ necsts の削除 (リソース監視ありの場合)

```
# userdel -r necsts
```

- (5) /var/adm/cron/cron.allow から necsts を削除 (リソース監視ありの場合)

- (6) /etc/services より以下の行を削除
stst 34143/tcp # nec sts service

- (7) /etc/inetd.conf より以下の行を削除
stst stream tcp nowait root /opt/necsts/ststd ststd

- (8) inetd デーモンに SIGHUP シグナルを送って更新した inetd.conf を再読み込み

```
# ps -e | grep inetd
677 ?          4:10 inetd      <=== プロセス番号(677)確認
# kill -HUP 677      <=== SIGHUP シグナル送信
```

- (9) /etc/syslog.conf より以下の行を削除
kern,daemon.warning /dev/console

- (10) Syslogd デーモンに SIGHUP シグナルを送って更新した syslog.conf を再読み込み

```
# ps -e | grep syslogd
781 ?          4:10 syslogd    <=== プロセス番号(781)確認
# kill -HUP 781      <=== SIGHUP シグナル送信
```

注意：上記の (9) 及び (10) 行を削除すると syslog.log の内容がコンソールに出力されなくなります。お客様自身で上記の設定を行っていて、コンソールで syslog.log の監視等を行っている場合、(9) 及び (10) の作業は不要です。

- (11) EMS の設定変更
(EMS モードを選択した場合)

```
# /etc/opt/resmon/sbin/monconfig <== 設定メニュー起動
:
Enter selection: [s] d          <== デリート

表示されるリストから、以下の内容のリスト番号(この例では 4)を確認

    4) Send events generated by all monitors
       with severity >= MAJOR WARNING to TEXTLOG /var/opt/resmon/log/console

確認した番号を、削除対象として入力(この例では 4)
Enter number of monitoring request to delete {(Q)uit, (H)elp} 4

Yes で削除
```

Are you sure you want to delete this entry?
{(Y)es, (N)o, (H)elp} [n] y

Check を行う

Enter selection: [s] c

チェック完了までしばらく時間が掛かります
チェックリストが表示される

終了する

Enter selection: [s] q

#

コンソールへのシンボリックリンクを削除する

rm -f /var/opt/resmon/log/console

7.2 メンテナンス

7.2.1 通報サービスの一時抑止方法

ここでは、監視をコントロールするツール(以下、本ツールを監視制御ツール(repctrl)と呼ぶ)の使用方法について説明します。

(1) 実行環境

監視制御ツール(repctrl)は、監視サーバ上の /home/necsts/sts ディレクトリ配下にインストールされています。

コンソールに root でログインし、監視制御ツール(repctrl)インストールディレクトリへ移動した後、necsts ユーザに切り替えます。

但しインストール時に既存ユーザを選択した場合はインストール時に指定したユーザに切り替えてから実行します。

```
# cd /home/necsts/sts
# su necsts
```

監視制御ツールの簡単な使用法は、-h オプション付きで実行すると表示されます。

```
$ repctrl -h
```

(2) 現在の状態の確認

監視制御ツールをオプションなしで実行すると、被監視サーバの現在のメッセージ監視状態を表示します。また、-status オプション付きでも同様の表示を行います。

```
$ repctrl
または
$ repctrl -status
```

実行すると以下のように、ID 番号：被監視サーバの OS 側 IP アドレス：状態 の順で表示されます。

```
1 : 10.1.1.1 : watching
2 : 10.1.1.2 : stop to 06/01/01 12:00:00
```

上記の例では、1 番のサーバはメッセージ監視中、2 番のサーバは指定された日時までメッセージ監視を停止中であることを示しています。

(3) 監視の停止

監視制御ツールを -stop オプション付きで実行することで、監視の停止を指示できます。

```
$ repctrl -stop サーバ 指定日時
```

サーバの指定は、ID 番号、または IP アドレスで行なえます。また、all を指定した場合は、全サーバを指定したことになります。

日時指定を省略した場合、デフォルト値として現時刻から 6 時間後が指定されます。

<実行例>

➤ 10.1.1.1 のサーバの監視を、23:00 まで停止する場合

```
$ repctrl -stop 10.1.1.1 23:00
```

➤ 1 番のサーバの監視を、1 月 6 日の 06:00 まで停止する場合

```
$ repctrl -stop 1 2006/1/6 6:00
```

- 全てのサーバの監視を、 1:00 まで停止する場合
\$ repctrl -stop all 1:00

(4) 監視の再開

監視を再開する場合には、監視制御ツールを `-start` オプション付きで実行してください。

```
$ repctrl -start サーバ
```

停止と同様、サーバの指定は、ID 番号、または IP アドレスで、all を指定することで全サーバを指定が可能です。

<実行例>

- 1 番のサーバの監視を再開する場合
\$ repctrl -start 1
- 10.1.1.1 のサーバの監視を再開する場合
\$ repctrl -start 10.1.1.1
- 全てのサーバの監視を再開する場合
\$ repctrl -start all

7.2.2 ライセンスコードの更新

ライセンスコードの更新は、次の手順に従って行なってください。

root で login または su で root になり、config.pl を以下のオプションで実行します。

```
# /opt/necsts/config/config.pl --codeid
```

次のようなプロンプトが表示されるので、N を入力後、新しいライセンスコードを入力して下さい。

```
*** configure codeID. (/opt/necsts/codeID)
The codeID file is already exist in /opt/necsts
codeID( ABCDEFGHIJKLMNOPQRST ) is OK? [Y]/n > n
input codeID value for this machine > 1234567890ABCDEFGHIJ
codeID( 1234567890ABCDEFGHIJ ) is OK? [Y]/n > y
```

更新したライセンスコードのチェックが以下のように行なわれます。OK が出れば終了です。ライセンスコードのチェックはエージェントが呼ばれるときに行なわれるので、マネージャの再起動は不要です。

```
current machine ID: 1126039678
licensed machine ID: 1126039678
License period: 2010/12/31
License flag: 0000000000
codeID is OK.
```

7.2.3 ライセンス期限の確認

現在登録されているライセンス期限の確認は、次の手順に従って行なってください。

被監視サーバに root でログインします。次に、 /opt/necsts ディレクトリに移動して、check コマンドを実行します。

```
# cd /opt/necsts
# ./check
current machine ID: 1234567890
licensed machine ID: 1234567890    <== ライセンスされたマシン識別番号
License period: 2013/7/1          <== 有効期限
License flag: 0000000000
```

※期限なしライセンスの場合、License period に"2038/1/1"と表示されます。

※ライセンス有効期限の残存日数が 30 日以下になった場合、License period の下部に下記メッセージが出力されます。

- ・残存日数が 0 日～30 日の場合 : License code will be expired after XX days.
XX: 残日数
- ・失効(ライセンス有効期限切れ)の場合 : License code is expired!

7.2.4 MP 交換時の注意事項

MP 交換を実施するとパスワードが初期設定になるため、監視が停止します。MP 交換等の保守作業後は、テスト通報等で監視が正常に動作していることを確認してください。

7.2.5 iStorageManager のメッセージ iSM07454/iSM07459 を通報させる方法

iStorageManager Ver5.3 以降、iSM07454/iSM07459 はメッセージ種別を Notification から Warning に変更することにより、NX リモート通報で通報することが可能です。メッセージ種別は、iSM サーバ(HP-UX 版)の環境定義ファイルの log セクションに modify_remote_notification_msg_to_warning パラメータを設定することにより Warning に変更されます。詳細は「WebSAM iStorageManager インストールガイド」を参照してください。

尚、メッセージ種別を変更しない場合、iSM07454/iSM07459 はコンソールに出力されても通報されません。

7.2.6 マネージャプログラム起動状況の syslog 出力

マネージャプログラムが異常終了した場合、異常終了時、および、障害復旧時にメッセージを syslog へ出力します。

syslog への出力レベルは err

(1) ログ出力内容

マネージャプログラムが異常終了した場合、異常終了時と障害復旧時に syslog へ下記内容のメッセージが出力されます。

なお、メッセージは、一部を除き、①異常終了時、②障害復旧時の順番で出力されます。もし復旧しない場合は開発元に問い合わせてください。

異常発生と障害復旧がペアになっていないメッセージに関しては、対処方法に従って、対処してください。

項目名	設定値	備考
facility	LOG_USER	
level	LOG_ERR	異常終了時
	LOG_INFO	障害復旧時
メッセージ ※一覧参照	sts failed starting/making xxx	異常終了時、xxx は任意のメッセージ
	sts succeeded starting/making xxx	障害復旧時、xxx は任意のメッセージ
	その他	異常終了と障害復旧がペアになっていないもの

【異常終了時 syslog 出力例 1】

```
Oct 26 16:34:50 hostname STS-MANAGER[pid]: sts failed starting SNMPTrapReceiveProcess
```

【障害復旧時 syslog 出力例 1】

```
Oct 26 16:35:14 hostname STS-MANAGER[pid]: sts succeeded starting SNMPTrapReceiveProcess
```

【異常終了時 syslog 出力例 2】

```
Oct 26 16:36:03 hostname STS-MANAGER[pid]: sts failed making a new process (sfm get_event_detail).
```

【障害復旧時 syslog 出力例 2】

```
Oct 26 16:36:25 hostname STS-MANAGER[pid]: sts succeeded making a new process (sfm get_event_detail).
```

【メッセージ一覧】

異常発生と障害復旧がペアになっているメッセージ

No.	メッセージ
1	sts failed starting SNMPTrapReceiveProcess
2	sts succeeded starting SNMPTrapReceiveProcess
3	sts failed starting SNMPTrapReceiveMonitorProcess
4	sts succeeded starting SNMPTrapReceiveMonitorProcess
5	sts failed making a new process (sfm get_event_detail).
6	sts succeeded making a new process (sfm get_event_detail).
7	sts failed making a new process (Reboot SnmpTrapReceive).
8	sts succeeded making a new process (Reboot SnmpTrapReceive).
9	sts failed starting SNMPTrapReceiveProcess (repmodule)
10	sts succeeded starting SNMPTrapReceiveProcess (repmodule)
11	sts failed making a new process (statemonitor_start).
12	sts succeeded making a new process (statemonitor_start).
13	sts failed making a new process (statemonitor_stop)
14	sts succeeded making a new process (statemonitor_stop)
15	sts failed making a new process (sts_main).
16	sts succeeded making a new process (sts_main).
17	sts failed making a new process (MTYPE_MP_MP).
18	sts succeeded making a new process (MTYPE_MP_MP)
19	sts failed making a new process (MTYPE_MP_ISP).
20	sts succeeded making a new process (MTYPE_MP_ISP).
21	sts failed making a new process (MTYPE_MP_ISP2).
22	sts succeeded making a new process (MTYPE_MP_ISP2).
23	sts failed making a new process (SnmpTrapReceiver).
24	sts succeeded making a new process (SnmpTrapReceiver).
25	sts failed making a new process (SnmpTrapDiv).
26	sts succeeded making a new process (SnmpTrapDiv).
27	sts failed making a new process (SnmpGetLog).
28	sts succeeded making a new process (SnmpGetLog).
29	sts failed making a new process (stscore_reboot).
30	sts succeeded making a new process (stscore_reboot).

その他のメッセージ

No.	メッセージ	対処方法
1	watching console failed, please check {log_dir}/{id}-main.log, {id}-console.log.	被監視サーバのコンソールが監視で きませんでした。 SG 誤りの可能性があります。該当の ログファイルを確認してください。

7.3 コードの説明

設定ツールで表示/設定するコードについて説明します。内容を確認の上、正しい内容を設定してください。

項目	説明	
機種 (Machine Type)	シリーズ名	監視対象マシン (被監視サーバ) 情報の設定内容
	NX7000/	Superdome rp24xx、rp34xx、rp44xx、rp54xx、rp74xx、rp84xx
	NX7700/	i4510
	NX7700i/	rx7620 rx7640 rx8620 rx8640 301xE-2 301xL-2/4/8 3160H-64 5010B-4、5012B-4、5012B-8 5010E-4 501xL-4/8 5160H-128 3020M-8、3040M-16 3040H-16 3080H-32 7010B-8、7010B-16、7010B-32 7010E-8 NXBL エンクロージャー (6U/10U) 7320H-256 7020M-16、7040M-32 7080H-64 8010E-16 8010B-16、8020B-32、8040B-64 8020M-32、8040M-64 8080H-128 8160H-256 9010E-16 9160H-256
	TX7/	i6010 i6510 i9010 i9510 i9610

注 1) i-PX9000 A/S モデルは、NX-7700i シリーズの機種を設定してください。

注 2) 上記には、機種名の一部を省略して記載しているものもありますが、正式名称を設定してください。

ex. rp8420-32

ex. 5012L-8

8. リソース監視とユーザ辞書の設定

8.1 リソースの閾値の設定

NX リモート通報では、サーバのリソース使用量が設定した値(閾値)を超えた場合に、システム管理者(SE)に対してアラーム通報を行う機能を提供しています。

閾値が設定できるリソースには、ディスク空き容量・CPU 負荷・空きメモリ容量の 3 種類があります。この 3 種類の閾値を設定するためのパラメータファイルが、インストールディレクトリ /home/necsts/rrs/ の下にある param, cpuparam, memparam の 3 つのファイルです。

閾値設定の詳細に関しては、「運用マニュアル」を参照して下さい。

8.2 ユーザ定義辞書によるユーザ定義メッセージ監視の設定

お客様が作成されたアプリケーションや他のソフトウェアがコンソールに出力されたメッセージを捕らえて通報したい場合には、メッセージをユーザ登録辞書に事前に登録していただき、ソフトウェアを再起動する必要があります。

その特徴は、次の通りです。

- (1) ユーザ定義辞書とは、特定の文字列がコンソール(/dev/console)に出力されたときに、**Manager** がシステム管理者に通報するための、システム管理者が編集可能な辞書です。システム管理者がユーザ定義辞書にメッセージ文字列を登録することにより、ミドルウェアやアプリケーションが出力するコンソールメッセージを監視することができます。
- (2) **Manager** は常にコンソールを監視しており、辞書に登録されている特定の文字列が検出された場合にアクションを起こします。ユーザ定義辞書に登録されている文字列が検出された場合は、ユーザ定義辞書に登録している e-mail アドレスに対してアラーム通報を行います。
- (3) ユーザ定義辞書には、1 行のコンソールメッセージに対してマッチするキー文字列を 3 個まで登録できます。キー文字列にはワイルドカードや正規表現などは使用できません。
 - メッセージ文字列が一意に固定している場合は、キー文字列 1 にそのメッセージを登録します。キー文字列 2,3 は空にして下さい。
 - メッセージの途中で HW パスやバージョン番号等の不確定要素の文字列が含まれる場合は、その前後で固定しているメッセージ文字列をキー文字列 1,2,3 に登録することでメッセージの検出を行います。

(例) 次のようなメッセージを登録する場合、キー文字列 1 に [WARNING: Master] を、キー文字列 2 に [is corrupted.] を登録します。

WARNING: Master *** is corrupted.

- 【注 1】 ユーザ定義辞書では、ID 番号の 1~50 番をシステムの予約番号として使用します。
1~50 番の内容は変更しないで下さい。ただし、通報先のメールアドレスは変更できます。
- 【注 2】 ユーザ定義辞書を変更した場合、**Manager** の再起動が必要です。

【注 3】 お客様環境で利用可能なメールサーバがない場合には、本機能は利用できませんので、ご注意願います。

この機能を有効にする為には、次のような操作が必要になります。

8.2.1 編集ツールの起動

ユーザ定義辞書は、`/home/necsts/dic/user.dic` です。編集ツールを起動する際は、監視サービスのユーザ名 `necsts` にて作業を行ってください。以下のようにして、編集ツールを起動します。

但しデータディレクトリ設定を行っている場合は、ユーザ定義辞書は、設定したデータディレクトリ/`dic/user.dic` となります。

またインストール時に既存ユーザを選択した場合はインストール時に指定したユーザに切り替えてから実行します。

```
# su necsts
$ cd /home/necsts
$ tool/dbedit dic/user.dic
```

起動すると、以下のように定義済みの項目が ID 番号と共に一覧形式で表示されます。ユーザ定義辞書では、ID 番号の 1～50 番についてはシステムの予約番号として使用します。新たに辞書内容を追加する場合は、ID 番号 51 番以降を使用してください。

```
(1st page/1 pages)
[1] alive check alert.
[2] resource report alert.
[3] Disk Space Alert.
[4] CPU Alert.
[5] Memory Alert.
[6] Mirror Disk Alert.
[7] License will be expired.
[8] test message for sts setup.

[Q]uit/[R]eread/[P]rev/[N]ext/[Number]: ?
```

8.2.2 監視メッセージの追加

監視メッセージをユーザ定義辞書に追加する場合は、コマンド入力のプロンプトに対して新規の ID 番号を入力します。次に、追加を確認するプロンプトが出力されるので、`'y'` を入力します。

```
[Q]uit/[R]eread/[P]rev/[N]ext/[Number]: ? 51
there is no such ID number: 51
do you want to add an entry id 51? [Y]/n? y
```

次に、項目の内容を入力します。コメント(定義項目がわかる内容)、通報先の **e-mail** アドレス、そしてマッチさせるコンソール出力のキー文字列を登録します。キー文字列は全部で 3 個指定でき、1 行のコンソールメッセージに対して **AND** でマッチを取ります。キー文字列はそのままコンソール出力メッセージと比較されます。キー文字列にはワイルドカードや正規表現は使用できません。

```
comment[] user-defined message 1.  
reportaddress[] user@user.domain  
key_string[0] [] key message  
key_string[1] []  
key_string[2] []
```

なお、当該通報メッセージを通報しない場合、レポートアドレスへ空白を設定せずに "dummy@com" を入力してください。

各項目の入力が終わると、設定内容を再表示した後にこの内容を辞書にセーブするか否かを尋ねてくるので、OK ならば 'y' を入力してください。

```
is it ok to save it? [Y]/n? y
```

セーブが終わると、辞書内容を表示した後で再びメインメニューのプロンプトが表示されます。

8.2.3 既存 ID 項目の編集

既存 ID 項目を編集する場合は、コマンド入力のプロンプトに対してその ID 番号を入力します。現在の設定内容が表示され、サブメニュープロンプトが表示されるので、'e' で編集モードに入ります。

```
[Q]uit/[R]eread/[P]rev/[N]ext/[Number]: ?51  
  
[51]  
comment: user-defined message 1.  
reportaddress: user@user.domain  
key_string[0]: key message  
  
SUB MENU:11::[Q]uit/[E]dit/[D]elete/[C]opy: ? e  
do you want to edit this entry? [Y]/n? y
```

各項目が順番に表示されるので、変更したい項目の内容を修正します。

修正が終わると、設定した内容が表示され、セーブ要求のプロンプトが表示されるので、OK ならば 'y' を入力してください。

```
is it ok to save it? [Y]/n? y
```

セーブが終わると、辞書内容を表示した後で再びメインメニューのプロンプトが表示されます。

8.2.4 編集の終了

編集を終了する場合は、メインメニューから 'q' で終了してください。

```
[Q]uit/[R]eread/[P]rev/[N]ext/[Number]: ? q
```

8.2.5 マスタ・スレーブのユーザ定義辞書

マスタ・スレーブ構成のユーザ定義辞書を変更した場合は、両方のユーザ定義辞書の内容を一致させるために、同じものを登録してください。

もし、ユーザ定義辞書の内容がマスタとスレーブで異なる場合は、マスタ・スレーブ間の同期が取れないため、スレーブ側からマスタと異なる内容の通報メールが発信されることがあります。

9. ログ

NX リモート通報は以下の 6 種類のログを収集します。

① 動作履歴ログ	alert.log	
② コンソールログ	ID-console.log	※ID は監視サーバのリスト番号
③ 動作ログ	ID-main.log	※同上
④ メール送信ログ	ID-mail.log	※同上
⑤ SNMP Trap 受信ログ	snmpAll.log	
⑥ SNMP Trap check ログ	snmp.log	
⑦ ライセンス情報取得処理のログ	get_license.log	
⑧ SNMP Trap 受信処理のログ	snmpTrapMain.log	
⑨ 通報メール作成処理のログ	createSnmpMail.log	
⑩ WebSAM 連携用ログ	websam.log	

以下に①および⑩の履歴ログの詳細について説明します。②③については開発部門が参照する情報のため説明を割愛します。また、④も主に開発部門が参照する情報ですが、テスト通報の結果確認にも使用できます。確認方法については、6.1.1 章を参照してください。⑤⑥についても主に開発部門が参照する情報ですが、SNMP Trap 受信の試験通報の結果確認や受信状態の確認にも使用できます。⑦から⑨についても主に開発部門が参照する情報です。

※注意

これらのログには保守センターに通報された障害の概要が記載されますが、通報された全ての事象に対して保守センターが対処する訳ではありません。
通報された事象であっても対処不要の場合もあります。
ログファイルを監視する場合は、予めご承知おきください。

9.1 動作履歴ログ

通報の要因となったメッセージ情報を記録します。また、通報が抑止された場合はその理由を記録します。

通報が行われた際の要因の確認、保守において過去に遡って要因の履歴を確認することが可能です。

(1) ファイル名

ファイル名 : alert.log

格納位置 : NX リモート通報をインストールしたディレクトリ配下の log ディレクトリ下

※通常は、/home/necsts/log/

データディレクトリ設定を行った場合は、
設定したデータディレクトリ/log/

(2) フォーマット

2006/09/11 16:57:25[name01(logID=1)]No.9011(FG) xxxx...xxxx

① ② ③ ④ ⑤ ⑥ ⑦

① 日付

② 時間

③ 筐体名

- ④ ログの ID 番号 ※動作ログ/コンソールログファイル名の ID 番号
- ⑤ メッセージ番号 ※障害辞書中のメッセージ番号
- ⑥ 要因コード ※受信側で識別に使用
- ⑦ 検出メッセージ ※障害辞書中の登録メッセージ

(3) 特殊メッセージ

通報を抑止した場合は、⑦のメッセージエリアに通報メッセージではなく、その理由を記載して、ファイルに出力します。

以下のメッセージ例では⑦の部分のみを示します。

- ・ 1 時間の同一要因障害通報抑止機能で抑止されたとき
(---) inhibit in 1H.
- ・ マシンタイプが通報対象機種と異なるため通報しなかったとき
(---) suppress by mismatch Machine type.
- ・ repctrl コマンドで抑止されたとき (repctrl コマンドの詳細は 7.2.1 を参照)
(---) suppress by report-control.
- ・ その他の理由で抑止されたとき
(---) suppress dialog.

(4) 容量制御

当日発生した要因は全てログします (容量に制限なし)。

但し、定期通報で通報後は、最新のログから制限値 (デフォルト 500 行) までを残し、古いログを削除します。

9.2 WebSAM 連携用ログ

保守センターに通報された障害情報を記録します。

WebSAM とは、本ログファイルを介して連携します。

(1) ファイル

ファイル名 : websam.log1, websam.log2, websam.log3

ファイルサイズが 1M バイトを超えると、ファイル名末尾の数字を 1→2→3→1→2→3→・・・とローテーションしながら出力先ファイルを変更します。

格納位置 :

【SNMP Trap により検出した障害】

監視サーバの /home/necsts/log

【SNMP Trap 以外で検出した障害】

Agent サーバの /opt/necsts/log

(2) フォーマット

【SNMP Trap により検出した障害】

2017-11-13 16:54:23 <SGH503914S> 10.34.60.104 [22041] ErrorMessage.

① ② ③ ④ ⑤ ⑥

- ① 日付
- ② 時間
- ③ 筐体名
- ④ 監視機器 IP アドレス
- ⑤ 障害番号
- ⑥ 検出メッセージ

【SNMP Trap 以外で検出した障害】

2017/10/23 16:11:21 [OS] ErrorMessage.

① ② ③ ④

- ① 日付
- ② 時間
- ③ 監視種別(OS: システムコンソール、SP: iSP コンソールのどちらかを出力)
- ④ 検出メッセージ

10. ダウンロード物件の取り扱い方

10.1 CD-R へ書き込む時の注意事項

web からダウンロード物件を CD-R に書き込む場合、フォーマットは Joliet を指定してください。

10.2 物件の展開方法

展開方法の例を示します。

(1) tar ファイルのまま CD-R 書き込んだ場合

(例)

```
# mount -F cdfs -r -o cdcase /dev/dsk/cXtXdX /CDROM ←マウント処理
# ls /CDROM ←CD-ROM 内容の確認
  NXremote_HPUX_RXX.tgz
# mkdir /tmp/wrk ←ワークディレクトリの作成
# cd /tmp/wrk ←ディレクトリの移動
# /usr/contrib/bin/gzcat /CDROM/NXremote_HPUX_RXX.tgz | tar xf -
                                     ←ファイルの解凍
```

(2) ftp で転送した場合の展開方法

(例)

```
# ls /tmp/sts ←ダウンロードしたファイルの確認
  NXremote_HPUX_RXX.tgz
# mkdir /tmp/wrk ←ワークディレクトリの作成
# cd /tmp/wrk ←ディレクトリの移動
# /usr/contrib/bin/gzcat /tmp/sts/NXremote_HPUX_RXX.tgz | tar xf -
                                     ←ファイルの解凍
```

11. インストール設定表

■マネージャ						
マスタ/スレーブ	IP アドレス					
マネージャ0 (マスタ)						
マネージャ1 (スレーブ)						
■メールサーバ						
プライオリティ	IP アドレス	From アドレス	ポート番号 (規定値:25)	認証	認証ユーザ (認証する場合必須)	認証パスワード (認証する場合必須)
1				する/しない		
2				する/しない		
■https通信情報						
https	プロキシサーバ	IP アドレス	ポート番号(デフォルト:8080)			
使用しない/使用する	使用しない/使用する					
■SSH						
SSH コマンドパス		秘密鍵パス		パスフレーズ		
■定期通報時刻の指定						
指定時刻						
時 分						
■アラーム通報先の指定						
e-mail アドレス						
■データディレクトリ設定						
データディレクトリパス						

■ 監視対象マシン(被監視サーバ)										
No.	システム 管理コード	シリアルNo.	構成指示書 番号	Node No.	OS Version	筐体名	機種名	System IP アドレス	iSP/MP/GSP	
									IP アドレス	
									接続方法	☐ Telnet ☐ SSH
									アカウント	
									パスワード	
									IP アドレス	
									接続方法	☐ Telnet ☐ SSH
									アカウント	
									パスワード	
									IP アドレス	
									接続方法	☐ Telnet ☐ SSH
									アカウント	
									パスワード	
									IP アドレス	
									接続方法	☐ Telnet ☐ SSH
									アカウント	
									パスワード	
									IP アドレス	
									接続方法	☐ Telnet ☐ SSH
									アカウント	
									パスワード	

■監視対象マシン(7320H-256/8160H-256/9160H-256)									
No.	システム 管理コード	シリアルNo.	構成指示書 番号	ラック番号	機種名	OA		6120XG Switch パスワード	
						IP アドレス		Switch1	
						接続方法	☐ Telnet ☐ SSH	Switch2	
						アカウント			
						パスワード			
						IP アドレス		Switch1	
						接続方法	☐ Telnet ☐ SSH	Switch2	
						アカウント			
						パスワード			
						IP アドレス		Switch1	
						接続方法	☐ Telnet ☐ SSH	Switch2	
						アカウント			
						パスワード			
						IP アドレス		Switch1	
						接続方法	☐ Telnet ☐ SSH	Switch2	
						アカウント			
						パスワード			
						IP アドレス		Switch1	
						接続方法	☐ Telnet ☐ SSH	Switch2	
						アカウント			
						パスワード			

■監視対象マシン(ブレードエンクロージャー)							
No.	システム 管理コード	シリアルNo.	構成指示書 番号	ラック番号	機種名	OA	
						IP アドレス	
						接続方法	☐ Telnet ☐ SSH
						アカウント	
						パスワード	
						IP アドレス	
						接続方法	☐ Telnet ☐ SSH
						アカウント	
						パスワード	
						IP アドレス	
						接続方法	☐ Telnet ☐ SSH
						アカウント	
						パスワード	
						IP アドレス	
						接続方法	☐ Telnet ☐ SSH
						アカウント	
						パスワード	
						IP アドレス	
						接続方法	☐ Telnet ☐ SSH
						アカウント	
						パスワード	

■監視対象マシン(BMC)										
No.	システム 管理コード	シリアルNo.	構成指示書 番号	筐体名	機種名	IP アドレス				
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7
						SM		PM2		PM5
						PM0		PM3		PM6
						PM1		PM4		PM7

12. 付録

12.1 RSA Message-Digest ライセンス条文

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

12.2 net-snmp ライセンス条文

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright c 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2009, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS

OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
- * The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries,
brand or product names may not be used to endorse or promote products
derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) ----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above
copyright notice, this list of conditions and the following
disclaimer in the documentation and/or other materials provided

with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
COPYRIGHT
HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS
OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

12.3 OpenSSL ライセンス条文

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

OpenSSL License

```
/* =====
 * Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * =====
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com). This product includes software written by Tim
```

* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```