855-900604-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：Windows 編＞

開示および用途制限資料

DD-400-1000-D

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 gzip(GNU GENERAL PUBLIC LICENSE Version 2)を ソースコードを改変せずに利用しております。GNU GENERAL PUBLIC LICENSE Version 2 のライセンス条文につきましては、付録　GNU GENERAL PUBLIC LICENSE Version 2 ライセンス条文　をご参照下さい。

目次

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 Windows マシンで実現する「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。

本ドキュメントにおいて使用しているウインドウの画像や記述で「R X.X」と表記されている部分は、適宜読み替えてください。

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

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	10.5 版
R5.4	10.41 版
R5.3	10.3 版
R5.2	10.2 版
R5.1	10.1 版
R4.81	9.9 版
R4.8	9.7 版
R4.5	9.5 版
R4.4	9.4 版
R4.1	9.2 版
R4.0	9.1 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。

HP-UX マシンの監視では、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 または https 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

HP-UX マシンを監視する場合、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。Manger 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

定期通報（１回／日）

- Manager の稼動ステータス情報

Agent の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、7.2.1 章(2)(1)③以降を参考に、ユーザ宛通報メッセージの 100001 番 alive check alert のレポートアドレスを dummy@com(初期値: OFF)にしてください。

2.3.2. 通報抑止

通報の抑止機能には以下の種類があります。

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３０分間抑止
(70xxM/70xxH/80xxM/80xxH の場合は１５分間抑止)
② 個々のメッセージに対して通報許可レベル設定を変更することによる抑止
③ 個々のメッセージに対して通報許可を×にすることによる抑止
④ repctrl コマンドによる抑止（全メッセージが対象）
⑤ 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から④の抑止は対象外となります。
※②、③は保守員のみ実施可能です。

2.3.3. 通報手段

NX リモート通報は、保守センター（NEC フィールディング）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 4.3.13 参照。

被監視サーバ

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 4.4.8 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 MCOperations および WebSAM System Navigator と連携が可能です。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

3.1.1. サーバを監視する場合の動作要件

（1） 監視サーバと被監視サーバの動作要件

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/50xxM/50xxH/70xxM/70xxH/80xxM/80xxH『以外』の場合）→図 3-1 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）
・ 被監視サーバ（30xxM/30xxH の場合）→図 3-2 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)
・ 被監視サーバ（50xxM/50xxH の場合）→図 3-3,3-4 参照
　－システムコンソールが利用可能なこと。当該システムコンソールが監視サーバとなる。
　－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（70xxM/70xxH/80xxM/80xxH の場合）→図 3-5,3-6 参照
　－システムコンソールが利用可能なこと。
　－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
　－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（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。
・ 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。
　　（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。
Windows 版は下記必要容量の合計がインストールするドライブに確保可能であること。

監視サーバ	被監視サーバ
－インストールディレクトリ配下 100MB 以上	－/opt の空き容量 100 MB 以上（プログラム格納用） －/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）

・ 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。
・ 監視サーバはタスクスケジューラが使用できること。
・ 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（WindowsPC 版）の OS は以下のものであること。
Windows Server2008(x86)、Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016
・Windows Server は Server Core インストールではなくフルインストールを行うこと。
・監視サーバのインストールには Administrators 権限が必要。
・被監視サーバのインストールには root 権限が必要。
・監視サーバが監視できる被監視サーバの台数は、最大 150 台となります。
また、監視サーバが監視できる SNMP Trap 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、インストールディレクトリ配下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で必要です。

被監視サーバの台数×1MB

・監視サーバ（WindowsPC 版）をインストールする OS では、ショートネーム（8.3 形式）を無効にしないでください。
ショートネームが有効であるかを確認するには、以下のコマンドを実行してください。

a) Windows Server2008(x86)の場合
Administrators 権限を持つアカウントでログインします。コマンドプロンプトを開いて fsutil コマンドを以下のオプションで実行し、disable8dot3 が 0 であることを確認します。

```
C:¥WINDOWS¥system32>fsutil behavior query disable8dot3
disable8dot3 = 0
```

b) Windows Server 2008 R2／2012 R2／2016 の場合
Administrators 権限を持つアカウントでログインします。コマンドプロンプトを開いて fsutil コマンドを以下のオプションで実行し、インストールドライブの「C:」が「有効」であることを確認します。
※監視サーバを C ドライブへインストールする場合の実行例です。

```
C:¥Windows¥system32>fsutil 8dot3name query C:
Disable8dot3 のボリュームの状態は 0 です (8dot3 名の作成は有効です)。
NtfsDisable8dot3NameCreation のレジストリの状態は既定値の 2 です (ボリューム単位で設定します)。
上の 2 つの設定に基づいて、8dot3 名の作成は C: で有効です。
```

・［通報メッセージ管理］と［SG バックアップ/リストア処理］を使用するためには、.NET Framework 3.5 が必要です。監視サーバ(WindowsPC 版)の OS が Windows Server 2012 R2／2016 の場合は、NET Framework 3.5 を有効にしてください。
・ただし、Windows Server 2012R2 において、下記の問題が発生した場合は、対処方法により問題を回避することが可能です。

No.	問題内容	対処方法
1	・下記のエラーが発生する 1 つ以上の役割、役割サービス、または機能のインストールに失敗しました。 ソースファイルが見つかりませんでした。 役割と機能の追加ウィザードの新しいセッションで役割、役割サービス、または機能のインストールを再実行し、ウィザードの［確認］ページで［代替ソースパスの指定］をクリックして、インストールに必要なソースファイルの有効な場所を指定してください。接続先のサーバーのコンピューターアカウントを使用してアクセスできる場所を指定する必要があります。	●左記のエラーが発生した時、Windows Server 2012 R2 の OS メディアを DVD ドライブにセットし、メッセージに従って、［代替ソースパスの指定］で『(メディアドライブ)¥ sources¥sxs』を指定する。
2	・.NET Framework 3.5 用のセキュリティ更新プログラム 2966827 または 2966828 をインストール済みのため、.NET Framework 3.5 が有効にならない。	●更新プログラム 3005628 をインストールする。更新プログラムの詳細は以下の URL を参照してください。 https://support.microsoft.com/ja-jp/kb/3005628/ja

（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。(保守センター宛の通報手段は https にすることができます。) 必要なメール環境は以下の通りです。

- 保守センターへ 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 3.3.2 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 / iSP	22 / 23 / 5001	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

HP-UX マシンの監視では、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、保守センター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保守センターの 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. サーバを監視する場合の接続例 （30xxM/30xxH/50xxM/50xxH/70xxM/70xxH/80xxM/80xxH 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、保守センター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。

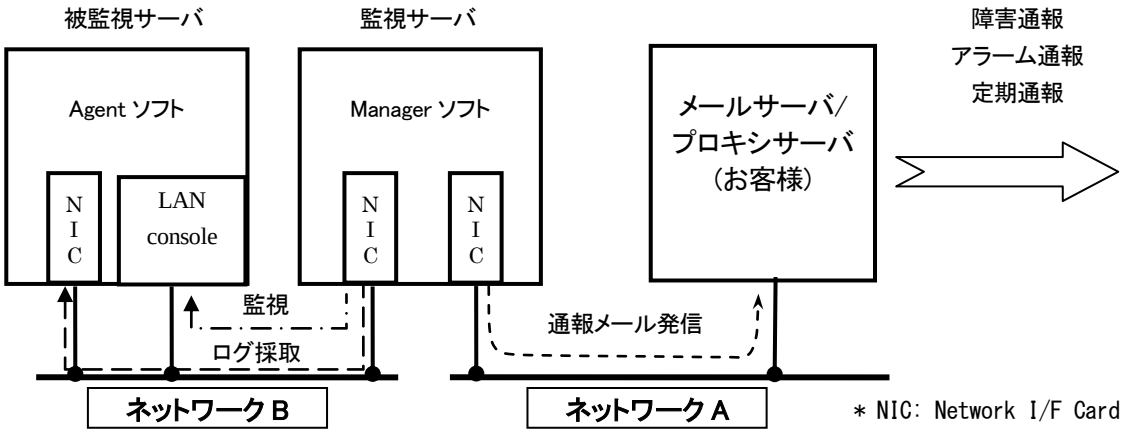


図 3-1

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。

3.2.2. サーバを監視する場合の接続例（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、保守センター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 3-2）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。

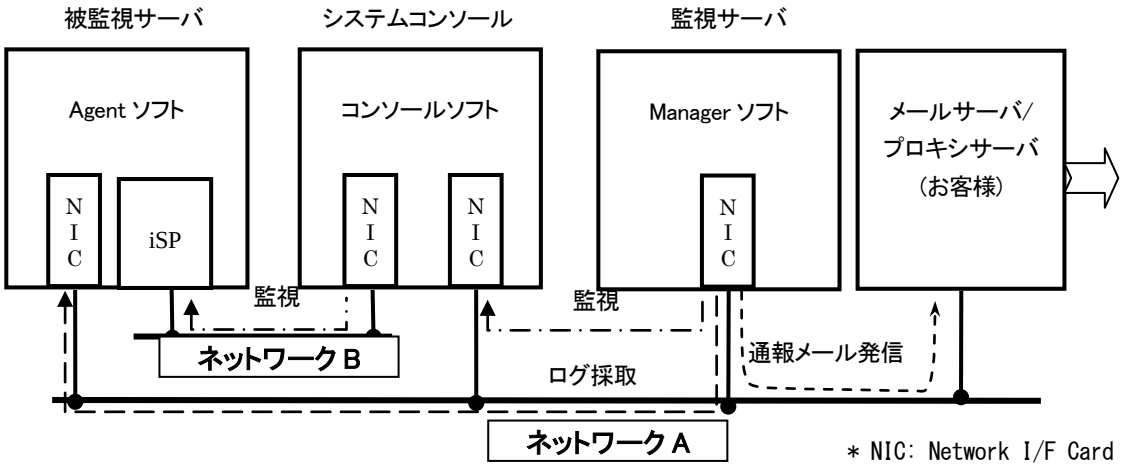


図 3-2

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. サーバを監視する場合の接続例（50xxM/50xxH）

被監視サーバが 50xxM/50xxH の場合、システムコンソールを必ず監視サーバにします。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 iSP 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、保守センター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。

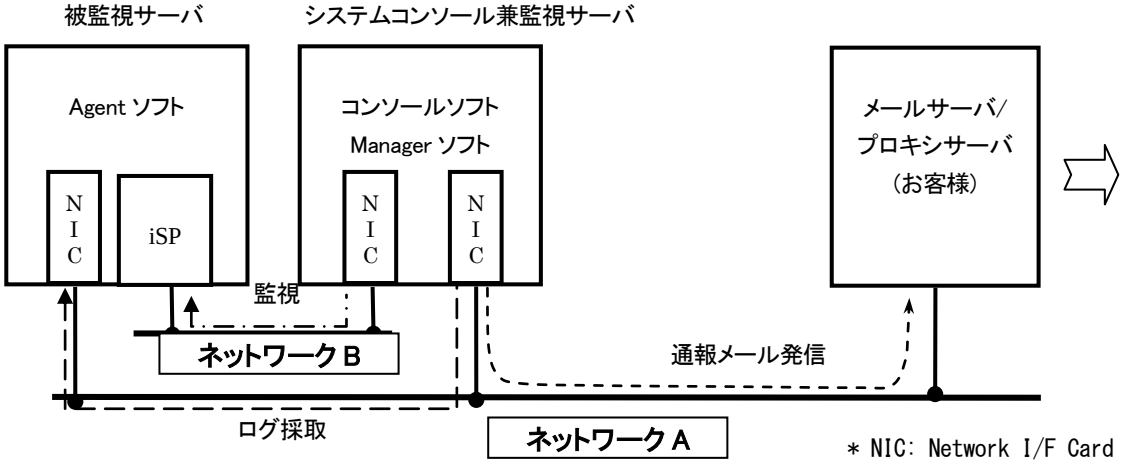


図 3-3

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。
- 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 3-4 を参照。

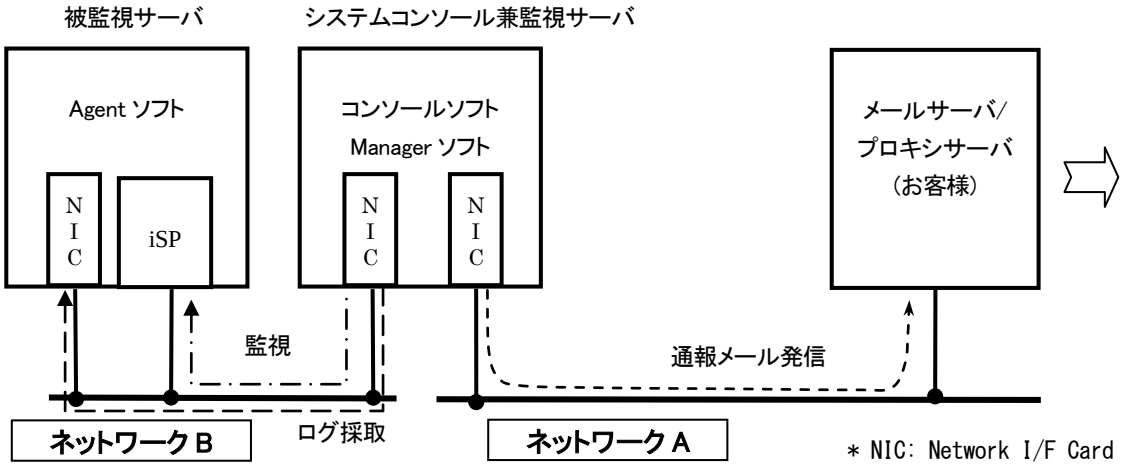


図 3-4

3.2.4. 接続例（70xxM/70xxH/80xxM/80xxH）

被監視サーバが 70xxM/70xxH/80xxM/80xxH の場合、システムコンソールを監視サーバにすることもできます。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、保守センター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 3-5）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。

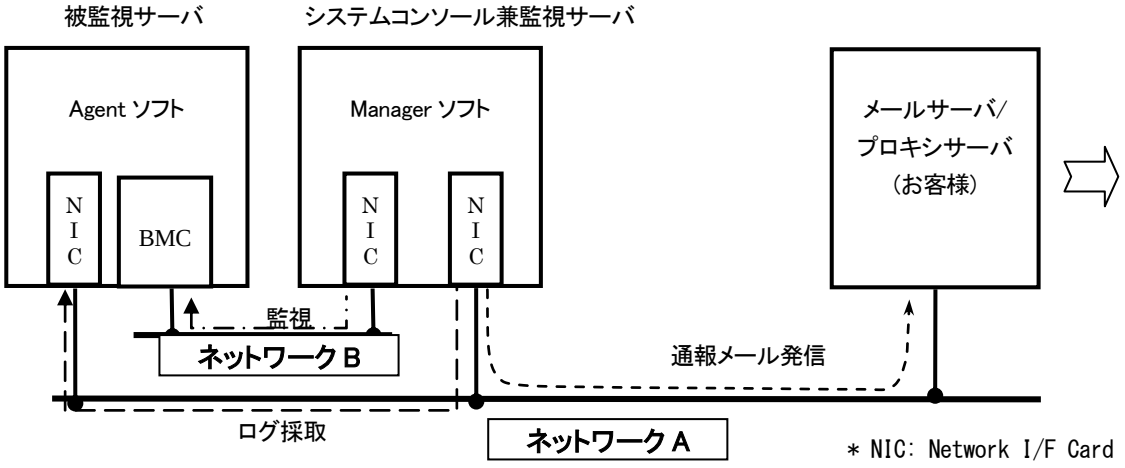


図 3-5

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 3-6 を参照。

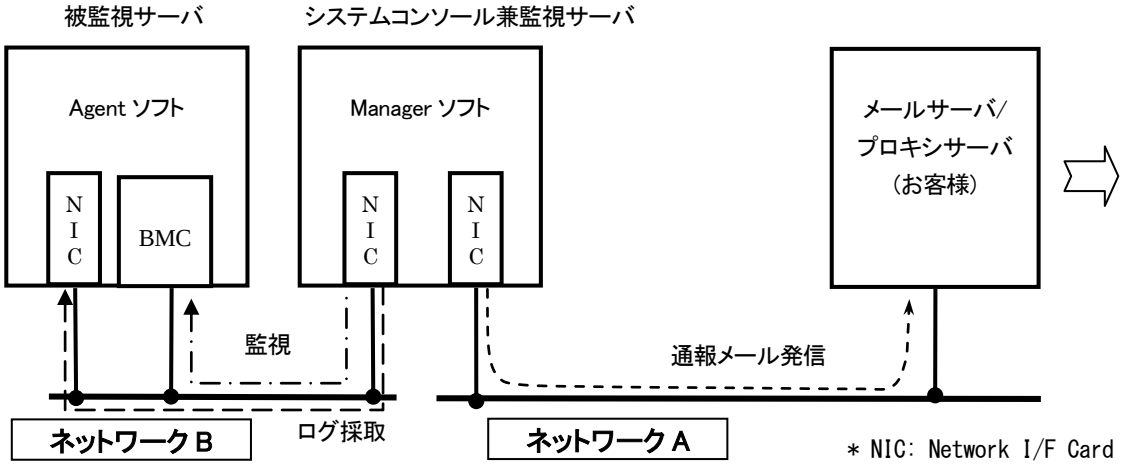


図 3-6

3.3. 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」に記入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。

3.3.1. 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は、マスタを 0 番、スレーブを 1 番とします。

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

3.3.2. メールサーバ

e-mail にて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入します。

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。

記入項目（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。

記入項目（メールサーバ毎）

IP アドレス	マネージャサーバの IP アドレス
From アドレス	root@上記 IP アドレス
※e-mail 通報には使用しません。	
認証	SMTP 認証を行わない(off)

3.3.3. 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
プロキシサーバポート番号	プロキシサーバのポート番号

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。メールサーバの設定については 3.3.2 を参照ください

3.3.4. 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。この通報時刻を記入します。既定値は「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。
　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。

3.3.5. 被監視サーバ

被監視サーバの情報を記入します。

記入項目（サーバ毎）

システム管理コード	装置のシステム管理コード
シリアル No.	装置号機（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
Node No.	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 Version	OS バージョン指定 HP-UX の例：11iv3
マシン名	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）
機種	rp3410 や 3010L-2 などの型式名
システム IP アドレス	OS が使用する LAN ポートの IP アドレス
GSP/MP IP アドレス	GSP/MP の IP アドレス
iSP　IP アドレス	iSP の IP アドレス
接続方法	telnet/ssh いずれかを選択してください
iSP/MP Login	iSP/MP/GSP のログイン名
iSP/MP Passwd	iSP/MP/GSP のログインパスワード

3.3.6. 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
ラック番号	エンクロージャーの識別名
機種	BE600／BE1000
システム IP アドレス	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、4.4.7 章を参照してください。
接続方法	telnet/ssh いずれかを選択してください
Login	接続時のログイン名（OA ログイン名）
Passwd	接続時のログインパスワード（OA ログインパスワード）

3.3.7. BMC の SNMP Trap 監視（70xxM/70xxH/80xxM/80xxH）

SNMP Trap 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

3.3.8. 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 4.3.9 を参照ください

3.4. 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保守センター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、お客さま負担となります。

詳細はご担当の保守センター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。

3.5. 通報受信側準備完了の確認

障害通報を受信する保守センター側のサーバに、お客様の機器管理情報を登録しておく必要が有ります。

保守センター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。

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。Web からダウンロードした物件を使用する場合の注意事項は、10 章を参照してください。

4.1.2. ライセンスコード

監視対象がサーバの場合、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。

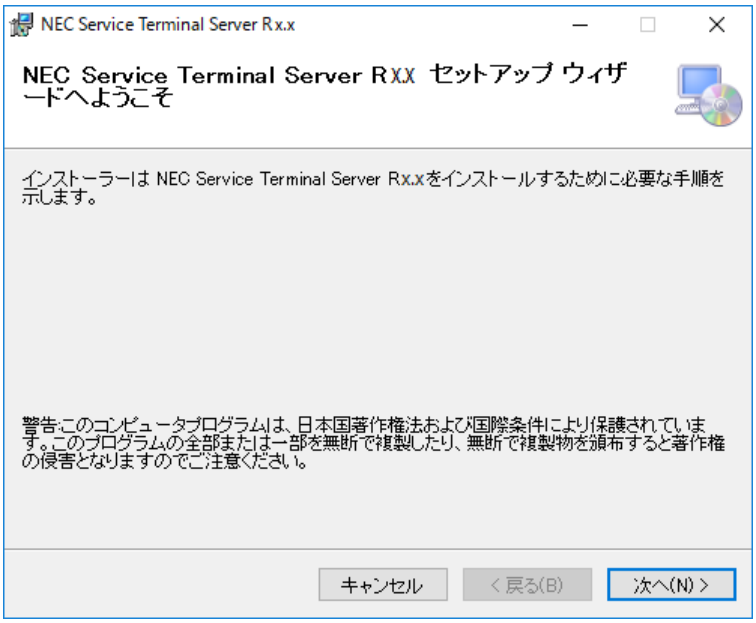
4.2. Manager ソフトのインストール

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。

－注意事項－
他目的で使用したパソコン等を転用する際は、BIOS の設定を初期状態に戻し、OS ディスクをフォーマット後、OS のインストールを行い、初期出荷状態に戻してください。

(1) Administrators の権限をもつアカウントでログインします。
(2) CD-ROM をドライブに挿入します。
(3) Windows の［スタート］の［ファイル名を指定して実行］にてインストールプログラムを指定します。インストールプログラムは、以下の場所の setup.exe になります。
CD-ROM ドライブ：¥NX¥windows¥
(4) ［OK］ボタンをクリックすると、本ソフトのインストールが開始され、下記のセットアップウィザードのダイアログボックスが表示されます。インストールを継続する場合は[次へ]ボタンをクリックしてください。[キャンセル]ボタンをクリックした場合は、本ソフトのインストール自体がキャンセルされインストールが中断します。



(5) インストールフォルダの選択のダイアログボックスが表示されます。インストール先のフォルダとして、推奨フォルダが表示されます。

推奨フォルダ：(システムドライブ)¥Program Files (x86)¥STS¥

インストール先のフォルダを変更する場合は、[参照]ボタンをクリックし、インストール先のフォルダを変更してください。

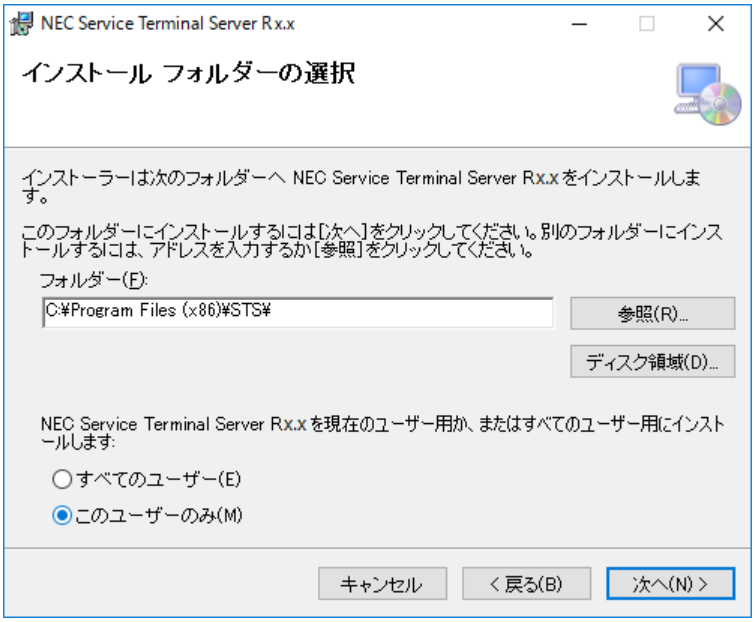
※32 ビット版 OS の場合は「(システムドライブ)¥Program Files¥STS¥」が推奨フォルダとして表示されます。以下、64 ビット版 OS へのインストールを前提として説明しますが、32 ビット版 OS へのインストールを行う場合、適宜、読み替えてください。

※インストール先フォルダパスの最下位は¥STS¥となるようにしてください。

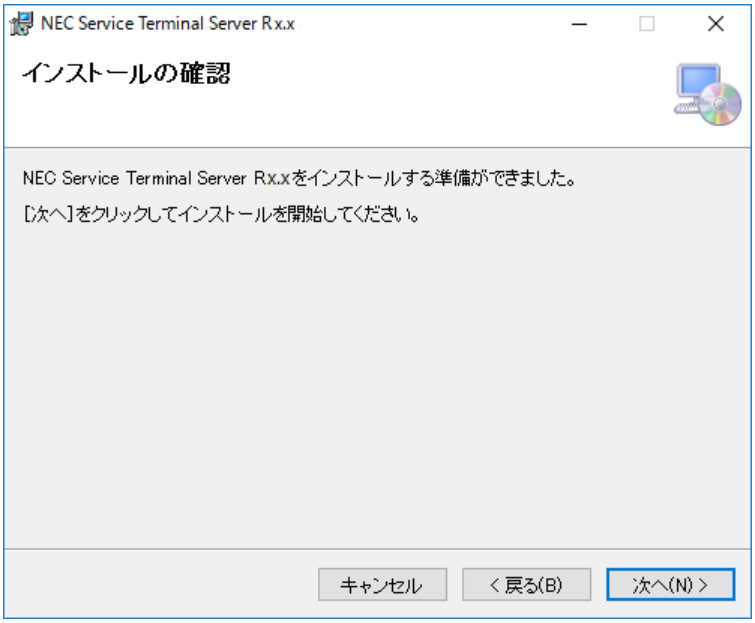
次にユーザの選択をしてください。監視サーバの設定（4.3、7.2）、および手動によるサービスの登録/削除/開始/停止（5.1）をインストールしたユーザのみ(自分のみ)可能とする場合は「このユーザのみ」、他のユーザも可能とする場合は「すべてのユーザ」を選択してください。

その後、[次へ]ボタンをクリックしてください。

[キャンセル]ボタンをクリックした場合は、本ソフトのインストール自体がキャンセルされインストールが中断します。

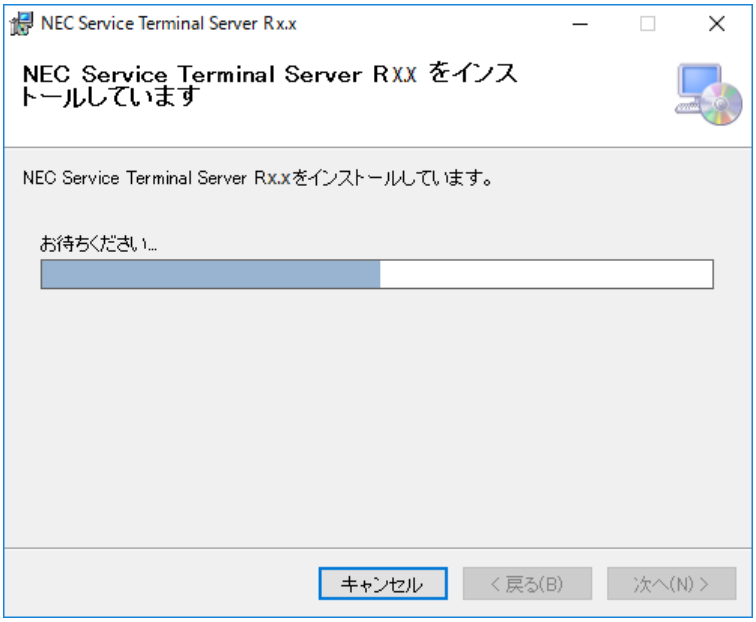


(6) インストールの確認のダイアログボックスが表示されますので、[次へ]ボタンをクリックしてください。
[キャンセル]ボタンをクリックした場合は、本ソフトのインストール自体がキャンセルされインストールが中断します。

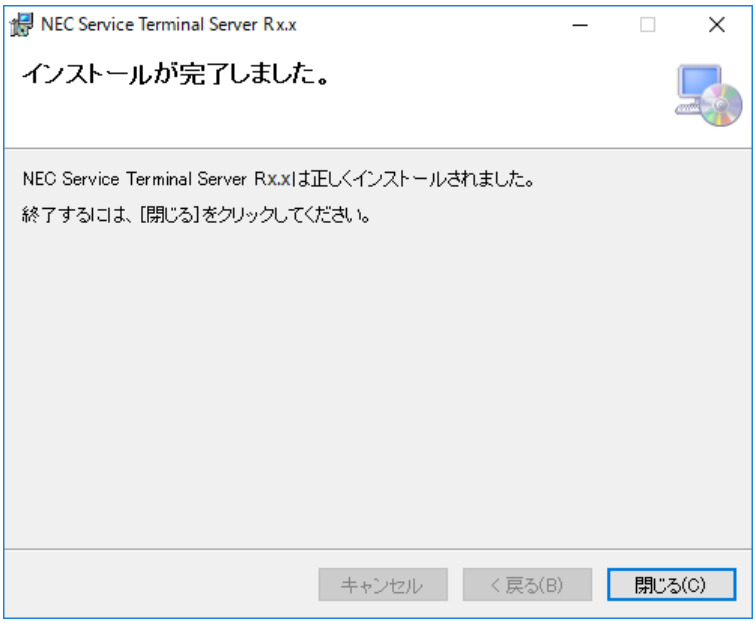


(7) ユーザアカウント制御ダイアログが表示された場合は、[はい]ボタンをクリックしてください。
[いいえ]ボタンをクリックした場合は、本ソフトのインストール自体がキャンセルされインストールが中断します。

(8) インストール中、ダイアログボックスが表示されます。インストール終了のダイアログが表示されるまでお待ちください。
[キャンセル]ボタンをクリックした場合は、本ソフトのインストール自体がキャンセルされインストールが中断します。



(9) インストールが終了すると、以下のダイアログボックスが表示されます。[閉じる]ボタンをクリックしてください。



(10) これでインストールは完了です。
もし、Windows の再起動のダイアログボックスが表示された場合は、Windows を再起動してください。

4.3. 監視サーバの設定

4.3.1. 設定ツールの起動

監視サーバの設定は、設定ツールから行います。
次の手順で設定ツールを起動してください。

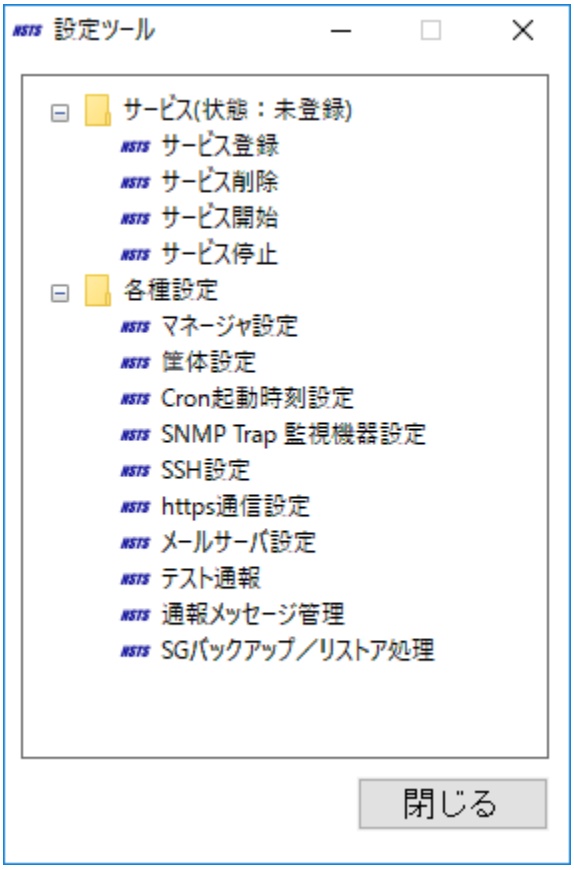
(1) Windows Server2008／2008 R2／2016 の場合
[スタート]→[プログラム]→[NEC Service Terminal Server]→[設定ツール]を選択します。

(2) Windows Server 2012 R2 の場合

- キーボードの「Windows ロゴ」キーを押下するか、デスクトップ画面で左下隅の「Windows ロゴ」をクリックしてスタートメニューを表示します。
- スタートメニューにおいて左下隅の下向きの矢印をクリックし、すべてのアプリケーションを表示させます。
- 一覧から NEC Service Terminal Server の 設定ツールを選択します。

ユーザアカウント制御ダイアログが表示された場合は、[はい]ボタンをクリックしてください。

設定ツールが起動します。

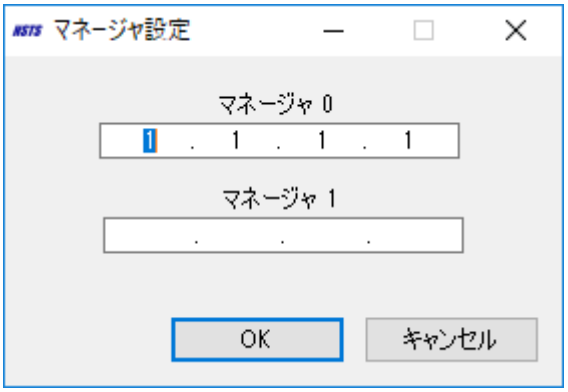


4.3.2. マネージャ情報の設定方法

マネージャ情報として設定するものは、監視サーバの IP アドレスです。
HP-UX 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。本設定画面では、HP-UX 版のマネージャの IP アドレスを設定しないでください。

(1) ツールの起動方法
設定ツール画面の[各種設定]→[マネージャ設定]を選択すると、マネージャ設定画面が表示されます。

(2) 設定画面と設定内容



表示/設定項目		表示/設定内容
マネージャ 0	必須	マネージャの IP アドレスを設定してください。 マネージャ 1 台構成の場合は、監視サーバの自 IP アドレスを設定してください。 監視サーバを 2 重化する場合、本アドレスの監視サーバをマスタと判断します。 【デフォルト値】"1.1.1.1" 【入力条件】 半角数字。入力形式は 10 進数入力で‘0’～‘255’まで。 [例] 133.203.40.22 134.203.4.123
マネージャ 1	－	マネージャの IP アドレスを設定してください。 監視サーバを 2 重化する場合、本アドレスの監視サーバをスレーブと判断します。 入力条件はマネージャ 0 と同じです。

ボタン名	機能
OK	設定内容を登録後、本画面を閉じます。
キャンセル	設定内容を登録せずに、本画面を閉じます。

4.3.3. 監視対象マシン（被監視サーバ）情報の設定方法

筐体、ノード/パーティション情報は設定ツールを用いて設定します。
監視サーバが監視できる監視対象マシン(被監視サーバ)の最大数は150台となります。

－注意事項１－
監視対象毎に筐体情報、ノード/パーティション情報の順番で登録してください。
筐体情報を登録後、機種名を変更する際は、ノード/パーティション情報の設定も再度やり直す必要があります。

－注意事項２－
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。

{*インストールフォルダ*}¥sg¥chassis.sg
{*インストールフォルダ*}¥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３－
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 4.3.8 章を参照してください。

－注意事項４－
被監視サーバの台数が多い場合、NX リモート通報サービスの開始直後に、イベントビューアの Windows ログ→システムに以下のメッセージが記録されることがあります。

アプリケーション ポップアップ: plink.exe - アプリケーション エラー : アプリケーションを正しく起動できませんでした (0xc0000142)。
[OK] をクリックしてアプリケーションを閉じてください。

この場合、デスクトップヒープが枯渇していますので、レジストリを変更して拡張する必要があります。
以下のレジストリ値を変更して OS を再起動してください。

レジストリキー：
HKEY_LOCAL_MACHINE¥SYSTEM
¥CurrentControlSet¥Control¥Session Manager¥SubSystems
名前：Windows
値：(変更前)
%SystemRoot%¥system32¥csrss.exe
ObjectDirectory=¥Windows SharedSection=1024,20480,768
Windows=On
：
（実際には１行に表示される）

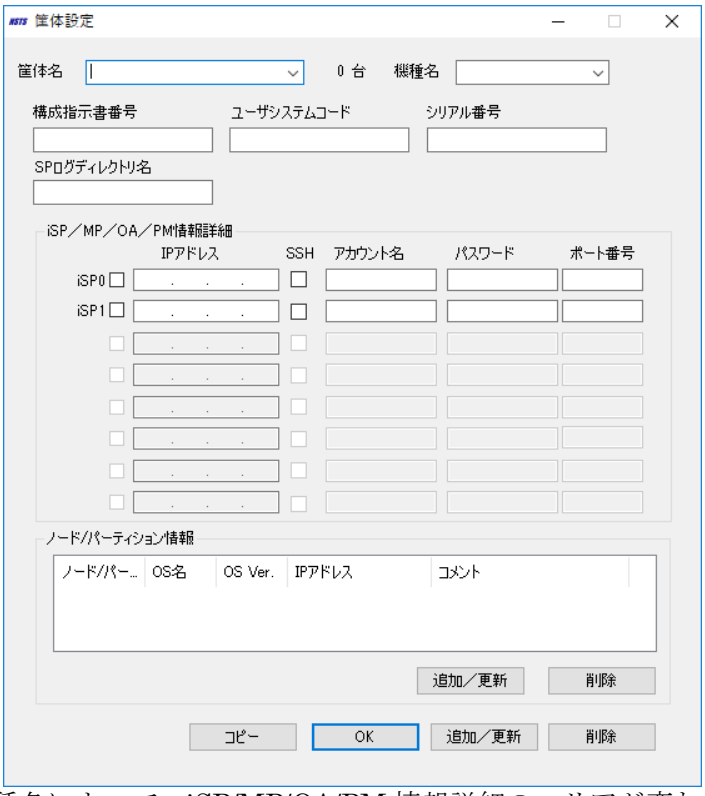
↓ SharedSection の 3 番目のパラメータを 2048 に変更する

(変更後)
%SystemRoot%¥system32¥csrss.exe
ObjectDirectory=¥Windows SharedSection=1024,20480,2048
Windows=On
：

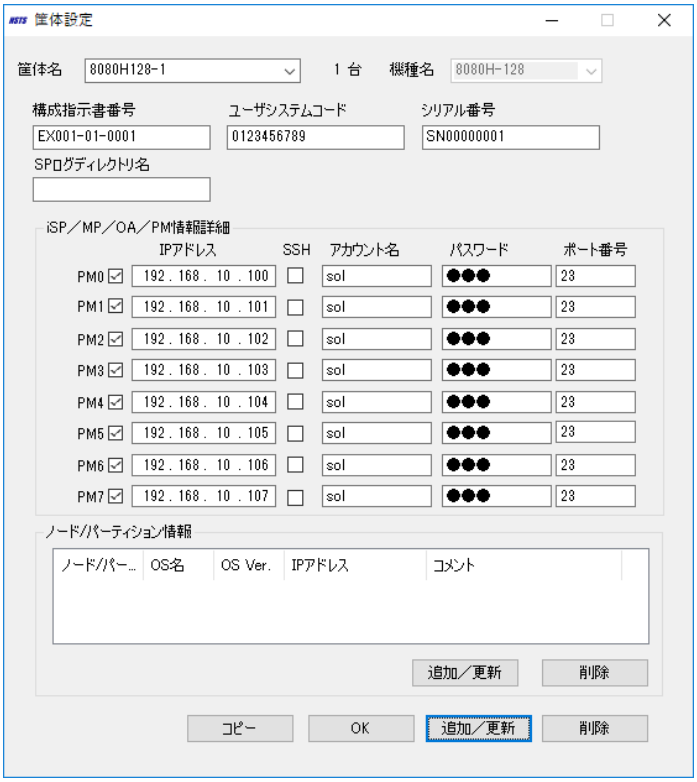
監視サーバの利用状況によりますが、ひとつの目安として、被監視サーバが 100 台を超える場合は、本設定変更が必要になります。

(1) ツールの起動方法
設定ツール画面にて[各種設定]→[筐体設定]を選択すると、筐体設定画面が表示されます。ノード/パーティション情報の設定ツールは筐体設定画面から起動させることができます。

(2) 設定画面と設定内容



選択した機種名によって、iSP/MP/OA/PM 情報詳細のエリアが変わる場合があります。

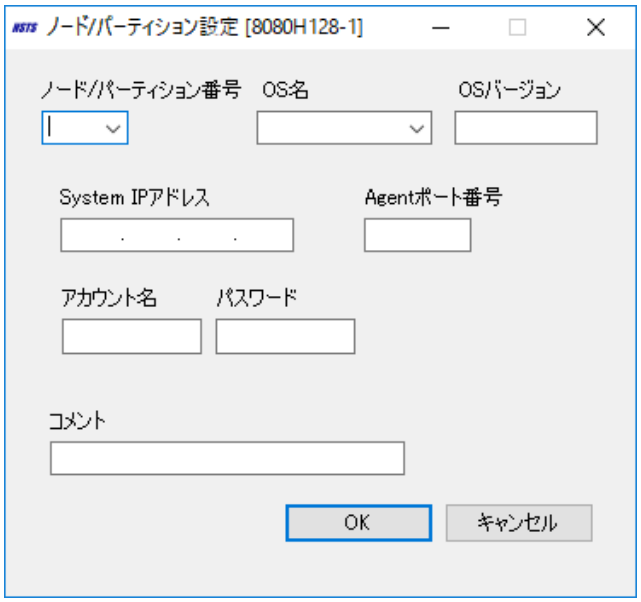


表示/設定項目			表示/設定内容
筐体名		必須	新規に筐体（7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 の場合は筐体設定画面でパーティションの設定をします。以下、筐体→パーティションと読み替えてください。）を登録する場合は、筐体名を設定してください。 筐体名は、お客さま任意の装置管理名称を登録してください。 既に登録されている筐体情報を更新する場合は、既登録の筐体情報がドロップダウンリストに表示されますので、該当する筐体を選択してください。筐体を選択することにより、登録内容が本画面に表示されます。 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)、スペースは使用できません。
登録台数		―	登録済みの筐体台数が表示されます。 【デフォルト値】"0"
機種名		必須	ドロップダウンリストに機種名が表示されます。該当する機種名を選択してください。
構成指示書番号		任意	構成指示書番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。
ユーザシステムコード		必須	システム管理コードを設定してください。 【入力条件】 半角英数字。最大 10 桁まで。","(カンマ)は使用できません。
シリアル番号		任意	装置の銘板に記載されている番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。
SP ログディレクトリ名		機種により、入力必須	機種が下記の場合、SP から転送されるログの格納場所ディレクトリを設定してください。下記以外の機種の場合は、入力不要です。 【入力必須の機種】 NX7700i シリーズの 5080H-64、5040H-32、5020M-16、i9610 【入力条件】 半角英数字。","(カンマ)は使用できません。
iSP／MP／OA／PM情報詳細	50xxH/50xxM: iSP0/iSP1 30xxH/30xxM: CSL PC/iSP 70xxM/70xxH/ 80xxM/80xxH: PM x その他: MP	必須	チェックボックスにチェック(レ印)してください。チェックボックスにチェックすると、IP アドレス、アカウント名、パスワード、ポート番号が設定できるようになります。 【デフォルト値】チェックなし
	IP アドレス	必須	iSP/MP/GSP/CSL PC/PM の IP アドレスを設定してください。チェックボックスにチェック時、自動でデフォルト値"0.0.0.0"が設定されます。 【入力条件】 半角英数字。入力形式は 10 進数入力で‘0’～‘255’まで。

	SSH	－	MP,PM,OA に接続する際、ssh プロトコルを用いる場合はチェックしてください。チェックしない場合は telnet プロトコルを使用します。 ssh 接続を使用する場合は、本設定の前に SSH 設定を完了させてください。SSH 接続に関する説明と注意事項は、「4.3.9 SSH の設定」を参照してください。
	アカウント名	必須（※）	iSP/MP/GSP/CSL PC/PMに接続する時に使用するアカウント名を設定してください。(※)MP/GSP時は任意 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)は使用できません。 【注意事項】 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 の場合は、PM のログインアカウントではなく、SMASH/CLP コンソールへ接続する時に使用するアカウント名を設定してください。
	パスワード	必須（※）	iSP/MP/GSP/CSL PC/PM に接続する時に使用するパスワードを設定してください。(※)MP/GSP 時は任意 尚、設定したパスワードは暗号化して管理します。 【入力条件】 半角英数字。最大 16 桁まで。","(カンマ)は使用できません。 【注意事項】 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 の場合は、PM の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時に使用するパスワードを設定してください。
	ポート番号	必須	iSP/MP/GSP/CSL PC/PM に接続する時に使用するポート番号を設定してください。チェックボックスにチェック時、自動でデフォルト値が設定されます。ポート番号を変更する場合は、他で使用しているポート番号と重複しないよう注意して設定してください。 【デフォルト値】 50xxH/50xxM=”5001”、30xxH/30xxM=”12011”、その他=”23” 【入力条件】 半角数字。最大 5 文まで。入力形式は 10 進数入力で‘1’～‘65535’まで。
ノード／パーティション情報	ノード/パーティション番号	－	登録済みのノード/パーティションのノード/パーティション番号が表示されます。
	OS 名	－	登録済みのノード/パーティションの OS 名が表示されます。
	OS Ver	－	登録済みのノード/パーティションの OS バージョンが表示されます。
	IP アドレス	－	登録済みのノード/パーティションの IP アドレスが表示されます。
	コメント	－	登録済みのノード/パーティションのコメントが表示されます。

ボタン名		機能
ノード／パーティション情報	追加/更新	ノード/パーティション情報を登録または更新します。押下するとノード/パーティション設定画面が表示されます。更新の場合、ノード/パーティションリストから更新したいノード/パーティションを選択し、本ボタンを押下してください。ノード/パーティション設定画面が表示されている間、本ボタンは透かし表示で無効となります。
	削除	ノード/パーティション情報を削除します。ノード/パーティションリストから削除したいノード/パーティションを選択し、本ボタンを押下してください。
コピー		NCM（NEC Console Manager）をインストール済みの場合、NCM で設定した筐体情報をコピーします。本機能は 50xxH/50xxM でのみ有効です。
OK		筐体情報の設定内容が未登録または更新されている場合、登録または更新を行うか否かの確認画面が表示されます。登録または更新を指示した場合は、登録または更新後、本画面を閉じます。登録または更新を指示しない場合は、設定内容を無効にし、本画面を閉じます。
追加/更新		筐体名に表示されている筐体の情報を登録または更新します。指示した筐体名が既に存在する場合は当該筐体情報を更新し、存在しない場合は追加登録します。
削除		筐体名に表示されている筐体の情報を削除します。

ノード/パーティション情報の[追加／更新]ボタンを押すと、ノードパーティション設定ダイアログが表示されます。

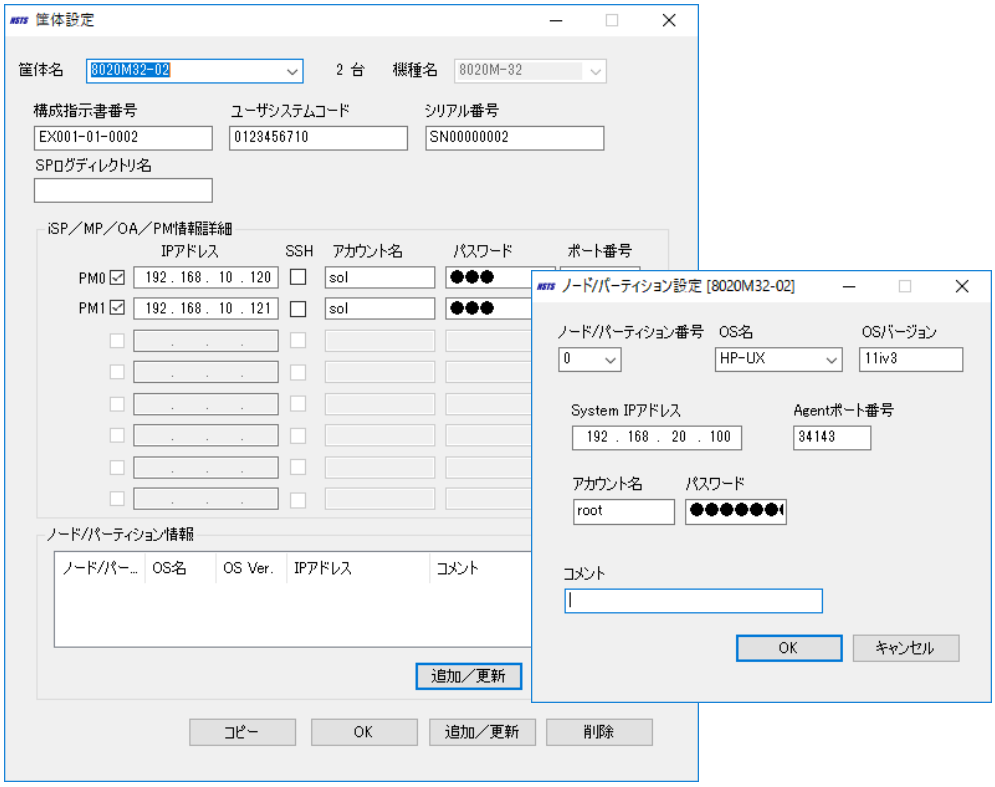


表示/設定項目		表示/設定内容
ウィンドウタイトル	ー	画面名の右横に当該ノード/パーティションの筐体名を表示します。[ ]内が筐体名になります。
ノード/パーティション番号	必須	筐体設定画面で表示対象ノード/パーティションを選択(反転)した場合は、当該ノード/パーティションのノード/パーティション番号が表示されます。表示対象を選択していない場合は、空欄が表示されます。ドロップダウンリストにノード/パーティション番号が表示されますので、ノード/パーティション番号を選択してください。 HW パーティション非対応のサーバの場合は、‘0’を入力してください。 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 の場合は、筐体設定画面で設定した PM 番号とパーティション番号が対となる設定を行なってください。
OS 名	必須	筐体設定画面で表示対象ノード/パーティションを選択(反転)した場合は、当該ノード/パーティションの OS 名が表示されます。表示対象を選択していない場合は、空欄が表示されます。ドロップダウンリストに OS 名が表示されますので、OS 名を選択してください。
OS バージョン	任意	筐体設定画面で表示対象ノード/パーティションを選択(反転)した場合は、当該ノード/パーティションの OS バージョンが表示されます。表示対象を選択していない場合は、空欄が表示されます。OS バージョン(例： 11iv3)を設定してください。 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)は使用できません。
System IP アドレス	必須	筐体設定画面で表示対象ノード/パーティションを選択(反転)した場合は、当該ノード/パーティションの IP アドレスが表示されます。表示対象を選択していない場合は、空欄が表示されます。OS の IP アドレスを設定してください。 尚、ノード/パーティション番号を入力時、自動で"0.0.0.0"が設定されます。 【入力条件】 半角数字。入力形式は 10 進数入力で‘0’～‘255’まで。
アカウント名	機種により、入力必須	機種が下記の場合、PM のログインアカウントを設定してください。下記以外の機種の場合は、入力不要です。 【入力必須の機種】 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)は使用できません。
パスワード	機種により、入力必須	機種が下記の場合、PM のログインパスワードを設定してください。下記以外の機種の場合は、入力不要です。 【入力必須の機種】 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 【入力条件】 半角英数字。最大 16 桁まで。","(カンマ)は使用できません。

nPar no	機種により、入力必須	機種が下記の場合、nPar 番号を設定してください。下記以外の機種の場合は、入力不要です。 【入力必須の機種】 7320H-256/8160H-256/9160H-256 【入力条件】 半角数字。最大 6 桁まで。","(カンマ)は使用できません。
Agent ポート番号	必須	筐体設定画面で表示対象ノード/パーティションを選択(反転)した場合は、当該ノード/パーティションの Agent ポート番号が表示されます。表示対象を選択していない場合は、空欄が表示されます。ノード/パーティション番号を入力時、自動で"34143"が設定されます。ポート番号を変更する場合は、他で使用しているポート番号と重複しないよう注意して設定してください。 ※"34143"以外を設定した場合は、非監視サーバ側の設定も変更する必要があります。 【デフォルト値】"34143" 【入力条件】 半角数字。最大 5 文まで。入力形式は 10 進数入力で '1' ～ '65535' まで。
コメント	任意	筐体設定画面で表示対象ノード/パーティションを選択(反転)した場合は、当該ノード/パーティションのコメントが表示されます。表示対象を選択していない場合は、空欄が表示されます。 マシン名を識別するホスト名（hostname コマンドで表示される値）を設定してください。 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)は使用できません。

ボタン名	機能
OK	設定内容を登録後、本画面を閉じます。
キャンセル	設定内容を登録せずに、本画面を閉じます。

7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 のパーティションの設定例を以下に示します。



4.3.4. 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。

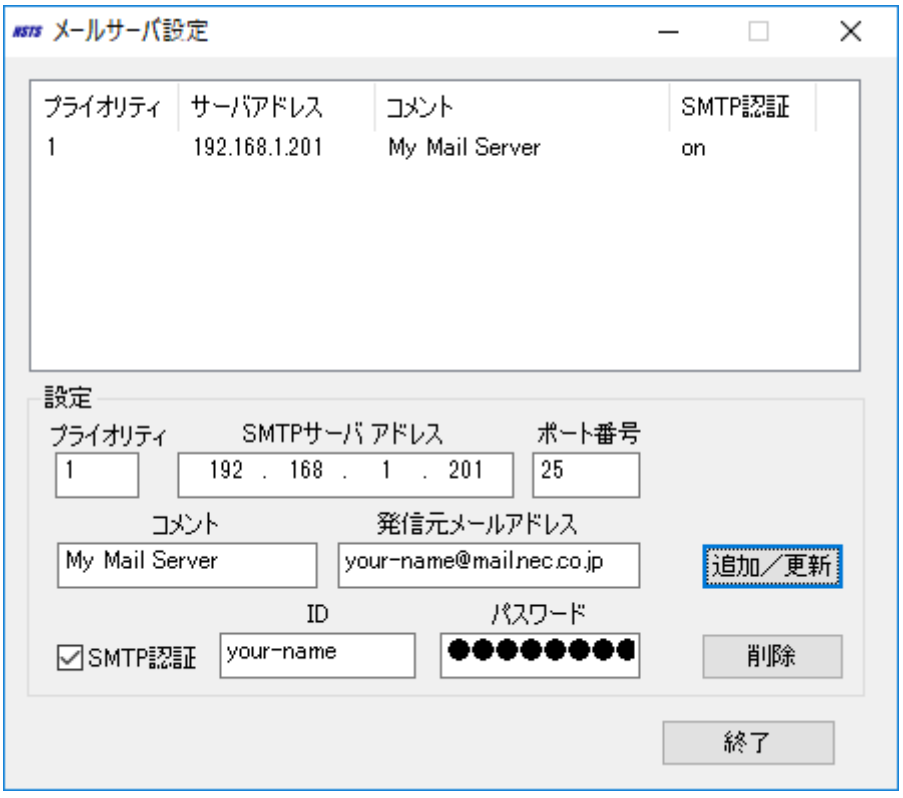
メールサーバは複数登録することが可能です。プライオリティの数値が小さい方が優先度"高"となります。プライオリティの数値が小さい(優先度"高")メールサーバに対し通報を行い、通報できなかった場合は、次のプライオリティのメールサーバに対し通報を行い、通報が成功するまで、または、登録されている全メールサーバに対して通報するまで、順次通報を行います。

－注意事項－ 登録済みのメールサーバのプライオリティを変更する場合は、既登録のメールサーバを削除してから新たに登録してください。削除せずにプライオリティを変更した場合、同一のメールサーバが複数登録されてしまいます。

(1) ツールの起動方法

設定ツール画面にて[各種設定]→[メールサーバ設定]を選択すると、メールサーバ設定画面が表示されます。

(2) 設定画面と設定内容



表示/設定項目			表示/設定内容
メールサーバリスト	プライオリティ	―	メールサーバの プライオリティが表示されます。 【デフォルト値】"1"
	サーバアドレス	―	メールサーバの IP アドレスが表示されます。 【デフォルト値】"1.1.1.1"
	コメント	―	メールサーバに関するコメントが設定されている場合、その設定内容が表示されます。
	SMTP認証	―	メールサーバの SMTP 認証を行うか否かが表示されます。 "on"表示： SMTP 認証を行う "off"表示： SMTP 認証は行わない(デフォルト値) 【デフォルト値】off
設定	プライオリティ	必須	メールサーバのプライオリティを設定してください。 【入力条件】 半角数字。入力形式は 10 進数入力で‘1’～‘99’まで。 数値 1 が最も優先度"高"とし、数値が大きくなるにつれ優先度が低くなる。
	SMTPサーバアドレス	必須	メールサーバの IP アドレスを設定してください。 【入力条件】 半角数字。入力形式は 10 進数入力で‘0’～‘255’まで。
	ポート番号	必須	メール発信に使用するポート番号を設定してください。[プライオリティ]を入力時、自動でデフォルト値"25"が設定されます。ポート番号を変更する場合は、他で使用しているポート番号と重複しないよう注意して設定してください。 【デフォルト値】"25"（SMTP のデフォルト値） 【入力条件】 半角数字。最大 5 文字まで。入力形式は 10 進数入力で‘1’～‘65535’まで。
	コメント	任意	メールサーバ名等、マシンを識別するための文字列を設定してください。 【入力条件】 半角英数字。最大 20 文字まで。
	発信元メールアドレス	必須	メールサーバから発信するメールの発信元(From)のメールアドレスを設定してください。 【入力条件】 半角英数字。最大 40 文字まで。
	SMTP認証	必須	メールサーバの SMTP 認証を行う場合は、チェックボックスにチェック(レ印)してください。 SMTP 認証を行わない場合は、チェックボックスはチェック(レ印)しないでください。 【デフォルト値】チェックなしの状態
	ID	SMTP認証の設定内容による	[SMTP 認証]がチェックされている場合、本項目は入力可能になります。認証に用いるアカウント名を設定してください。 【入力条件】 半角英数字。最大 40 文字まで。
	パスワード		[SMTP 認証]がチェックされている場合、本項目は入力可能になります。認証に用いるパスワードを設定してください。 尚、設定したパスワードは暗号化して管理します。 【入力条件】 半角英数字。最大 16 文字まで。

ボタン名		機能
メールサーバリスト設定	追加/更新	設定内容を追加/更新します。追加の場合は、[設定]欄に情報を設定してから本ボタンを押下してください。更新の場合は、対象メールサーバを選択(反転)させて、登録内容を[設定]欄に表示させ、情報を更新してから本ボタンを押下してください。 追加/更新対象のメールサーバ情報は[メールサーバリスト]欄に追加/更新され、[設定]欄にも表示されたままです。追加/更新が完了すると完了画面が表示されます。
	削除	設定内容を削除します。対象メールサーバを選択(反転)させて、登録内容を[設定]欄に表示させてから本ボタンを押下してください。 削除対象のメールサーバ情報は[メールサーバリスト]欄から削除されますが、[設定]欄には表示されたままです。削除が完了すると完了画面が表示されます。
終了		本画面を閉じます。

－注意事項－
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。

4.3.5. https 通信情報の設定方法

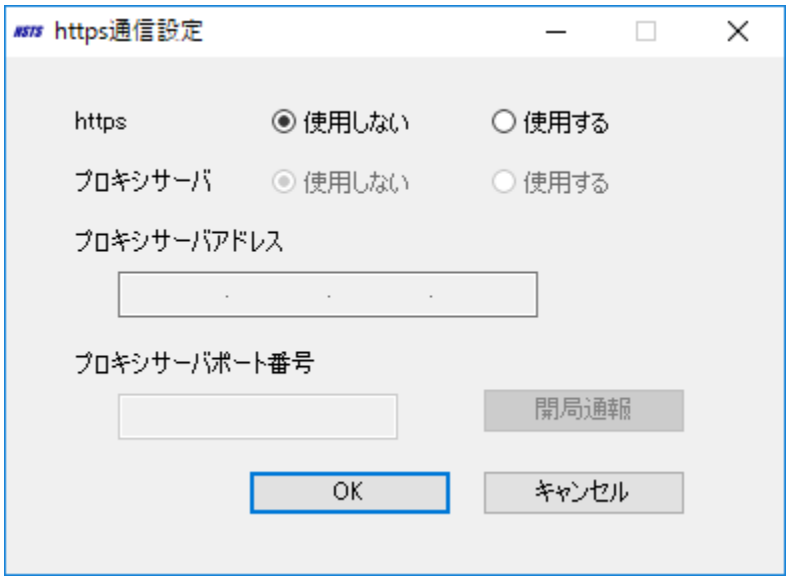
通報には、保守センター宛の通報とお客さま宛ての通報があります。このうち保守センター宛の通報は、https による通報と e-mail による通報のどちらかを選択できます。保守センター宛の通報は、採取したログを添付しますが、ログのサイズが大きくなる場合がありますのでファイルサイズの制限のない https による通報を推奨します。https にて通報を行う場合は、次の設定を行なってください。https 通報を選択しユーザ通報を利用しない場合もメールサーバの設定が必要となります。メールサーバの設定については 3.3.2 を参照ください

設定項目は、https を使用して通報するかどうか、https を使用して通報する場合にプロキシサーバを使用するかどうか、プロキシサーバを使用する場合はその IP アドレスとポート番号です。

(1)ツールの起動方法

設定ツール画面にて[各種設定]→[https 通信設定]を選択すると、https 通信設定画面が表示されます。

(2)設定画面と設定内容



表示/設定項目		表示/設定内容
https	必須	https 通信を用いた通報を使用するかどうかを設定してください。 使用しない場合は、以降の設定は不要(設定できません)です。 使用しない場合は、保守センター宛の通報は e-mail にて通報されます。
プロキシサーバ	―	プロキシサーバの使用有無を設定します。使用しない場合は、以降の設定は不要(設定できません)です。
プロキシサーバアドレス	―	プロキシサーバの IP アドレスを設定します。プロキシサーバを「使用する」に設定し、本設定を行なわなかった場合は、「0.0.0.0」が設定されます。
プロキシサーバポート番号	―	プロキシサーバのポート番号を設定します。プロキシサーバを「使用する」に設定し、本設定を行なわなかった場合は、「8080」が設定されます。

ボタン名	機能
OK	設定内容を登録後、本画面を閉じます。
キャンセル	設定内容を登録せずに、本画面を閉じます。
開局通報	「https」が「使用する」に設定されている状態で、設定画面を表示したときのみ有効となります。 「保守センター宛」に、開局通報を行います。 **必ず１回以上の開局通報を行なってください。**

4.3.6. cron 定期実行時刻情報の設定方法

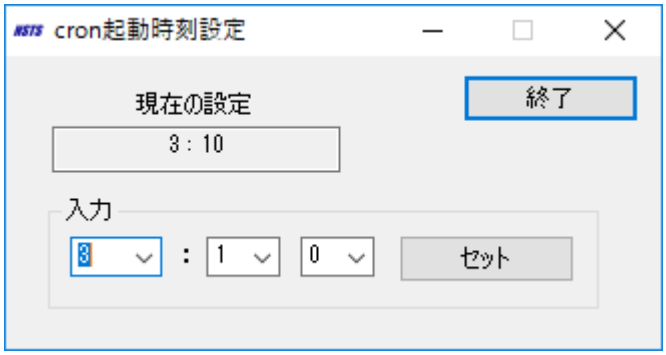
cron 定期実行時刻情報として設定するのは、毎日行う定期処理の処理開始時刻です。

定期処理は本画面で設定した時刻を元に、Manager ソフト起動時にタスク(Windows の[コントロールパネル]→[タスク])に登録され、スケジュールされます。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。

(1) ツールの起動方法

設定ツール画面にて[各種設定]→[cron 定期実行時刻設定]を選択すると、cron 起動時刻設定画面が表示されます。

(2) 設定画面と設定内容



表示/設定項目			表示/設定内容
現在の設定		―	現在の設定時刻(HH:MM)が表示されます。 【デフォルト値】"3:10"
入力	時間	必須	ドロップダウンリストに時刻"時(HH)"が表示されます。該当する時刻を選択してください。 【デフォルト値】】"3"
	分(10 の位)	必須	ドロップダウンリストに時刻"分(MM)"の 10 の位が表示されます。該当する時刻を選択してください。 【デフォルト値】"1"
	分(1 の位)	必須	ドロップダウンリストに時刻"分(MM)"の 1 の位が表示されます。該当する時刻を選択してください。 【デフォルト値】"0"

ボタン名		機能
入力	セット	設定内容を登録します。
終了		本画面を閉じます。

4.3.7. アラーム通報先の設定

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します。設定方法は　7.2.1 章⑤を参照してください。ユーザ定義辞書の定義済みメッセージであるメッセージ番号 100001～100050 のメッセージが対象となります。

4.3.8. SNMP Trap 監視機器の設定

SNMP Trap 監視機器の設定では、以下の機器が扱えます。

- ブレードエンクロージャー(BE600/BE1000)
- 7320H-256/8160H-256/9160H-256
- BMC(7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128)

監視サーバが監視できる SNMP Trap 監視機器の最大数は 50 台となります。

SNMP Trap 監視対象の設定を行います。
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。)

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、4.4.7 章を参照してください。

SNMP Trap 監視機器の設定では、「4.3.2 マネージャ情報の設定方法」で設定したマネージャの IP アドレスを利用しています。先にマネージャ設定を完了してください。

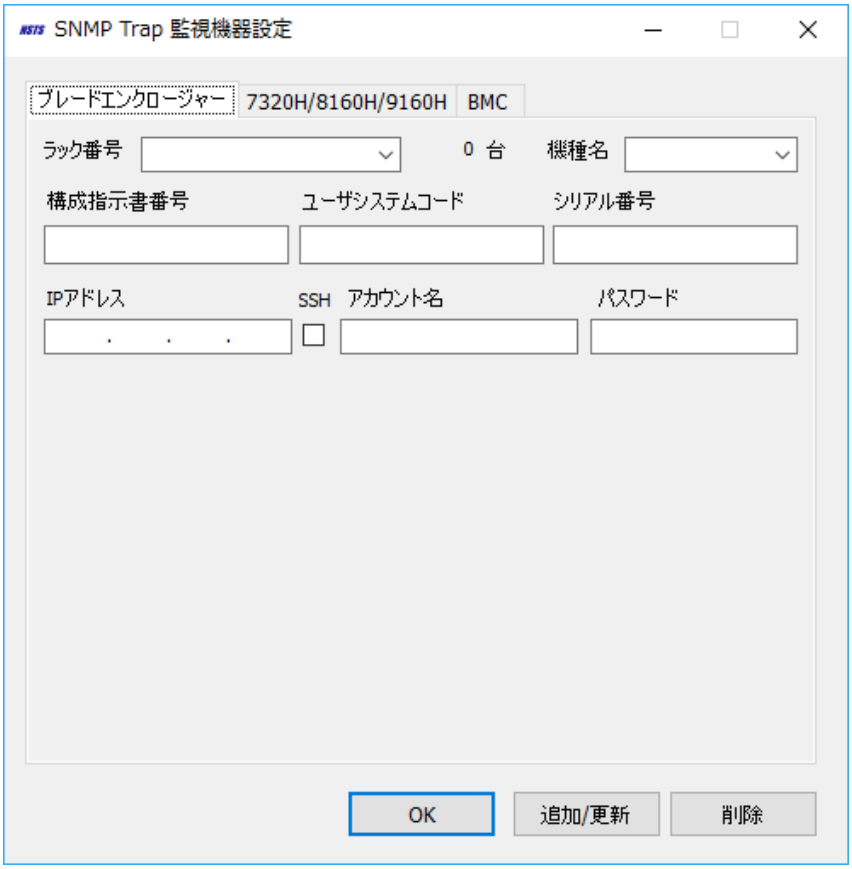
マスタ・スレーブ構成をとっている場合は、SG ファイルの登録順を厳密に一致させる必要があります。
そのため、マスタ・スレーブ構成の場合は スレーブ側での SG 設定はせず、マスタで設定した以下の SG ファイルをスレーブにコピーしてください。

{*インストールフォルダ*}¥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。

(1) ツールの起動方法
設定ツール画面にて[各種設定]→[SNMP Trap 監視機器設定]を選択すると、SNMP 設定画面が表示されます。

(2) ブレードエンクロージャーの設定画面と設定内容



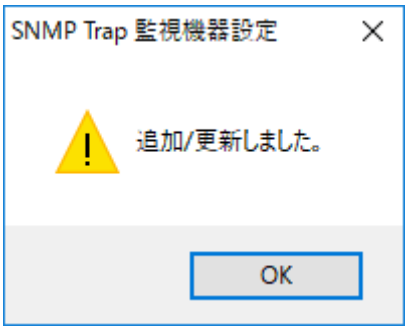
OA 設定は 4.4.7 章を参照ください。

表示/設定項目		表示/設定内容
ラック番号	必須	新規にブレードエンクロージャーを登録する場合は、筐体のラック番号を設定してください。ラック番号は、お客さま任意のラック管理名称を登録してください。 既に登録されている筐体情報を更新する場合は、既登録のラック番号がドロップダウンリストに表示されますので、該当するラック番号を選択してください。ラック番号を選択することにより、登録内容が本画面に表示されます。 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)、スペースは使用できません。
登録台数	－	登録済みの筐体台数が表示されます。 【デフォルト値】"0"
機種名	必須	ドロップダウンリストに機種名が表示されます。該当する機種名を選択してください。
構成指示書番号	任意	構成指示書番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。
ユーザシステムコード	必須	システム管理コードを設定してください。 【入力条件】 半角英数字。最大 10 桁まで。","(カンマ)は使用できません。
シリアル番号	任意	装置の銘板に記載されている番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。
IP アドレス	必須	IP アドレスを設定してください。（OA 設定 IP アドレス） 【入力条件】 半角英数字。入力形式は 10 進数入力で‘0’～‘255’まで。
SSH	－	OA に接続する際、ssh プロトコルを用いる場合はチェックしてください。チェックしない場合は telnet プロトコルを使用します。 ssh 接続を使用する場合は、本設定の前に SSH 設定を完了させてください。SSH 接続に関する説明と注意事項は、「4.3.9 SSH の設定」を参照してください。
アカウント名	必須	ブレードエンクロージャーのアカウント名を設定してください。（OA へのログインアカウント名） 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)は使用できません。
パスワード	必須	ブレードエンクロージャーのパスワードを設定してください。（OA へのログインパスワード） 尚、設定したパスワードは暗号化して管理します。 【入力条件】 半角英数字。最大 16 桁まで。","(カンマ)は使用できません。

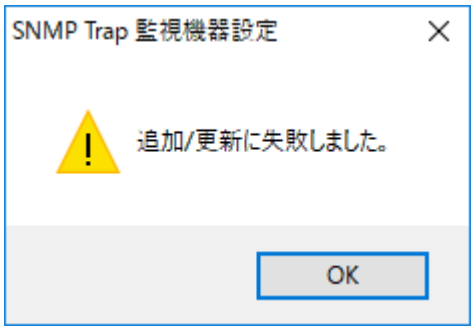
ボタン名	機能
OK	筐体情報の設定内容が未登録または更新されている場合、登録または更新を行うか否かの確認画面が表示されます。登録または更新を指示した場合は、登録または更新後、本画面を閉じます。登録または更新を指示しない場合は、設定内容を無効にし、本画面を閉じます。

追加/更新	ラック番号に表示されている筐体の情報を登録します。また、SNMP 障害通報受信のために自ホストの IP アドレスを OA に登録します。指示したラック番号が既に存在する場合は当該筐体情報を更新し、存在しない場合は追加登録します。
削除	ラック番号に表示されている筐体の情報を削除します。

各項目を入力後、「追加/更新」ボタンを押下するとブレードエンクロージャーに接続して、自ホストの IP アドレスを登録します。登録が完了（ボタン押下時から 30 秒程度）すると以下のメッセージが表示されます。

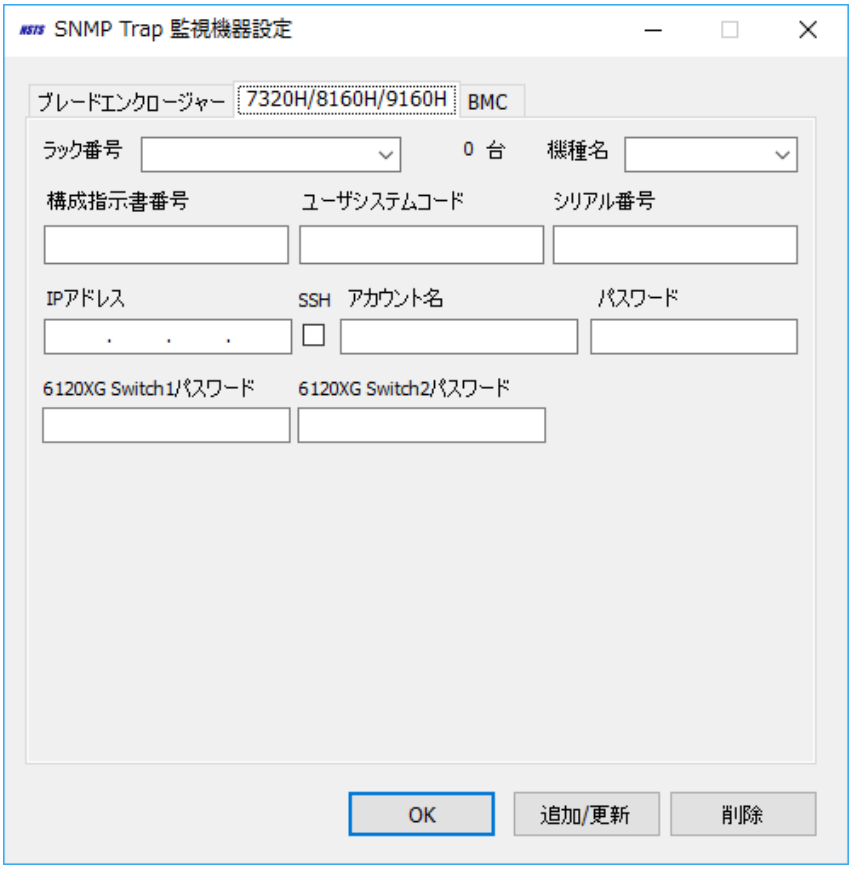


以下のメッセージが表示された場合、入力内容（IP アドレス、アカウント、パスワード）およびブレードエンクロージャーの SNMP 設定の確認を行ってください。
注）設定情報が正しくてもブレードエンクロージャー依存の登録可能数の上限に登録台数が達した場合も、同様のメッセージが表示されます。



「OK」ボタン押下時はブレードエンクロージャーには接続せず、設定内容を登録して画面を終了します。

(3)　7320H-256/8160H-256/9160H-256 の設定画面と設定内容

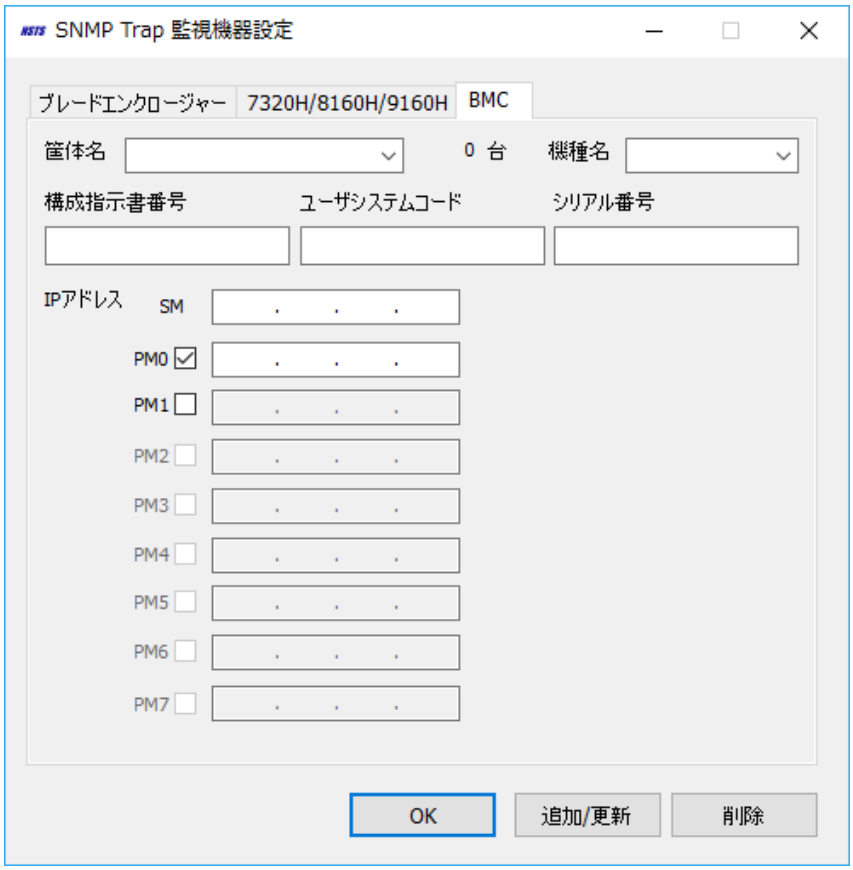


表示/設定項目		表示/設定内容
ラック番号	必須	新規に 7320H-256, 8160H-256, 9160H-256 を登録する場合は、筐体の登録名を設定してください。登録名は、お客さま任意の管理名称を登録してください。 既に登録されている筐体情報を更新する場合は、既登録の登録名がドロップダウンリストに表示されますので、該当する登録名を選択してください。ラック番号を選択することにより、登録内容が本画面に表示されます。 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)、スペースは使用できません。
登録台数	―	登録済みの筐体台数が表示されます。 【デフォルト値】"0"
機種名	必須	ドロップダウンリストに機種名が表示されます。該当する機種名を選択してください。
構成指示書番号	任意	構成指示書番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。
ユーザシステムコード	必須	システム管理コードを設定してください。 【入力条件】 半角英数字。最大 10 桁まで。","(カンマ)は使用できません。
シリアル番号	任意	装置の銘板に記載されている番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。

IP アドレス	必須	IP アドレスを設定してください。（OA 設定 IP アドレス） 【入力条件】 半角英数字。入力形式は 10 進数入力で‘0’～‘255’まで。
SSH	－	OA に接続する際、ssh プロトコルを用いる場合はチェックしてください。チェックしない場合は telnet プロトコルを使用します。 ssh 接続を使用する場合は、本設定の前に SSH 設定を完了させてください。SSH 接続に関する説明と注意事項は、「4.3.9 SSH の設定」を参照してください。
アカウント名	必須	7320H-256, 8160H-256, 9160H-256 のアカウント名を設定してください。（OA へのログインアカウント名） 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)は使用できません。
パスワード	－	7320H-256, 8160H-256, 9160H-256 のパスワードを設定してください。（OA へのログインパスワード） 公開鍵認証方式を使用する場合は、空欄で構いませんが、公開鍵認証に失敗したのち、パスワードが設定されていた場合は、パスワード認証を試みます。 尚、設定したパスワードは暗号化して管理します。 【入力条件】 半角英数字。最大 16 桁まで。","(カンマ)は使用できません。
6120XG Switch1 パスワード	必須	7320H-256, 8160H-256 の 6120XG Switch1 のパスワードを設定してください。9160H-256 を選択した場合、本フィールドは表示されません。 尚、設定したパスワードは暗号化して管理します。 【入力条件】 半角英数字。最大 16 桁まで。","(カンマ)は使用できません。
6120XG Switch2 パスワード	搭載されている場合は必須	7320H-256, 8160H-256 の 6120XG Switch2 のパスワードを設定してください。9160H-256 を選択した場合、本フィールドは表示されません。 尚、設定したパスワードは暗号化して管理します。 【入力条件】 半角英数字。最大 16 桁まで。","(カンマ)は使用できません。

ボタン名	機能
OK	筐体情報の設定内容が未登録または更新されている場合、登録または更新を行うか否かの確認画面が表示されます。登録または更新を指示した場合は、登録または更新後、本画面を閉じます。登録または更新を指示しない場合は、設定内容を無効にし、本画面を閉じます。
追加/更新	ラック名に表示されている筐体の情報を登録します。SNMP 障害通報受信のために自ホストの IP アドレスを OA に登録します。指示したラック名が既に存在する場合は当該筐体情報を更新し、存在しない場合は追加登録します。
削除	ラック名に表示されている筐体の情報を削除します。

(4) BMC(7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128)の設定画面と設定内容



表示/設定項目		表示/設定内容
筐体名	必須	新規に 7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128 を登録する場合は、筐体名を設定してください。 既に登録されている筐体情報を更新する場合は、既登録の筐体名がドロップダウンリストに表示されますので、該当する筐体名を選択してください。筐体名を選択することにより、登録内容が本画面に表示されます。 【入力条件】 半角英数字。最大 20 桁まで。","(カンマ)、スペースは使用できません。
登録台数	―	登録済みの筐体台数が表示されます。 【デフォルト値】"0"
機種名	必須	ドロップダウンリストに機種名が表示されます。該当する機種名を選択してください。機種名により IP アドレス入力可能エリアが設定されます。
構成指示書番号	任意	構成指示書番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。
ユーザシステムコード	必須	システム管理コードを設定してください。 【入力条件】 半角英数字。最大 10 桁まで。","(カンマ)は使用できません。

シリアル番号	任意	装置の銘板に記載されている番号を設定してください。 【入力条件】 半角英数字。最大 23 桁まで。","(カンマ)は使用できません。
IP アドレス(SM)	必須	SM の IP アドレスを設定してください。 【入力条件】 半角英数字。入力形式は 10 進数入力で‘0’～‘255’まで。
IP アドレス (PM0-PM7)	必須	装置構成にあわせ、チェックボックスを ON し、PM の IP アドレスを設定してください。 【入力条件】 半角英数字。入力形式は 10 進数入力で‘0’～‘255’まで。

ボタン名	機能
OK	筐体情報の設定内容が未登録または更新されている場合、登録または更新を行うか否かの確認画面が表示されます。登録または更新を指示した場合は、登録または更新後、本画面を閉じます。登録または更新を指示しない場合は、設定内容を無効にし、本画面を閉じます。
追加/更新	筐体名に表示されている筐体の情報を登録します。指示した筐体名が既に存在する場合は当該筐体情報を更新し、存在しない場合は追加登録します。
削除	筐体名に表示されている筐体の情報を削除します。

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。

4.3.9. SSH の設定

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、PuTTY に含まれる plink.exe を使用して ssh 接続を実現しています。
ssh 接続を利用するためには、別途 PuTTY のインストールが必要です。
PuTTY をインストールできない環境では、telnet を使用して接続してください。

PuTTY については、<http://www.putty.org/>を参照してください。

PuTTY 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(GUI の putty.exe からの確認でも可)。
NX リモート通報の評価は PuTTY 0.68 で実施しました。

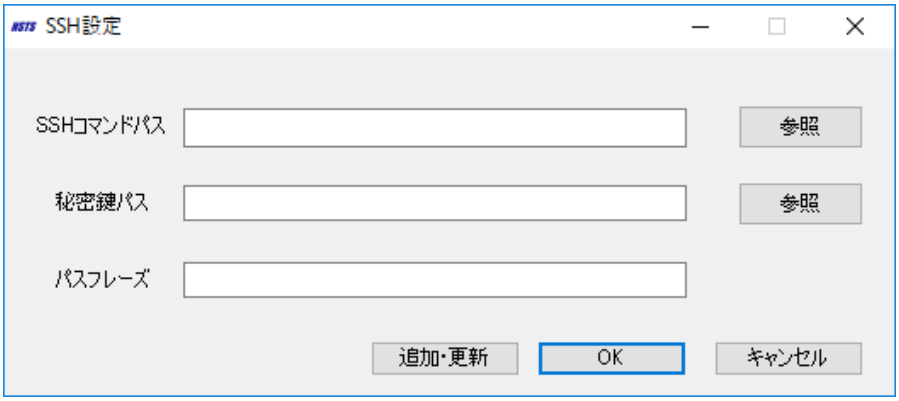
ssh 接続の対象となるサーバと認証方式は以下のとおりです。

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。

(1) ツールの起動方法
設定ツール画面にて[各種設定]→[SSH 設定]を選択すると、SSH 設定画面が表示されます。

(2) 設定画面と設定内容



表示/設定項目		表示/設定内容
SSH コマンドパス	必須	plink コマンドのフルパス名を入力してください。[参照]ボタンを押して、フォルダを選択しながら plink コマンドを指定することもできます。 「4.3.3 監視対象マシン（被監視サーバ）情報の設定方法」および、「4.3.8 SNMP Trap 監視機器の設定」において、ssh を使用すると設定した場合、本項目の設定は必須となります。
秘密鍵	―	公開鍵認証を使用する場合の秘密鍵のフルパス名を入力してください。[参照]ボタンを押して、フォルダを選択しながら plink コマンドを指定することもできます。
パスフレーズ	―	秘密鍵のパスフレーズを入力してください。秘密鍵にパスフレーズを設定していない場合は、入力を省略してください。 なお、パスフレーズにカンマは使用しないでください。

4.3.10. ウィルス対策ソフト(VirusScan 等)とファイアウォールの設定

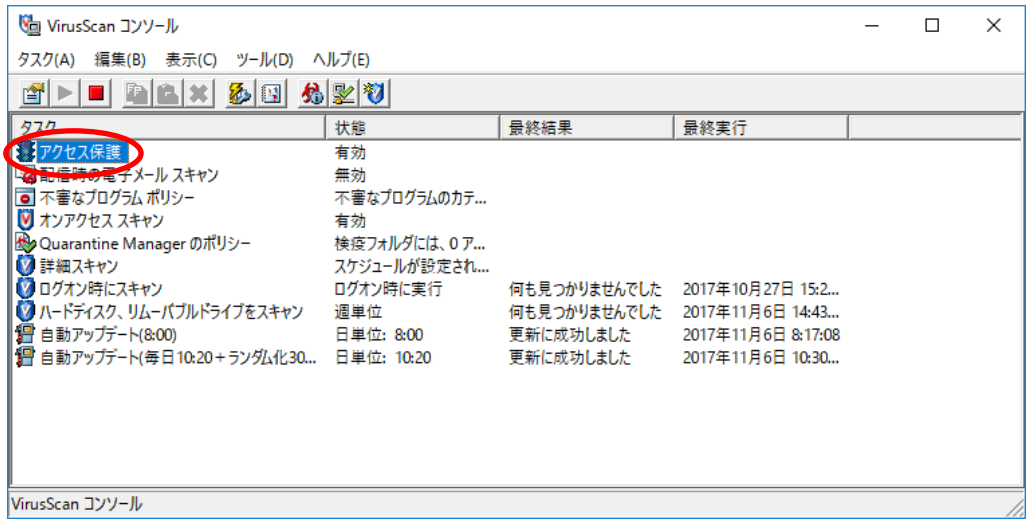
(1) メール送信プログラムの設定　(VirusScan Enterprise 8.8 の場合)

当該サービスでは、通報をメールで行ないます。通報メールがブロックされないようウィルス対策ソフトの設定でメール送信プログラムを除外登録する必要があります。また、ウィルス対策ソフトをバージョンアップした際は、再登録が必要となる場合があります。

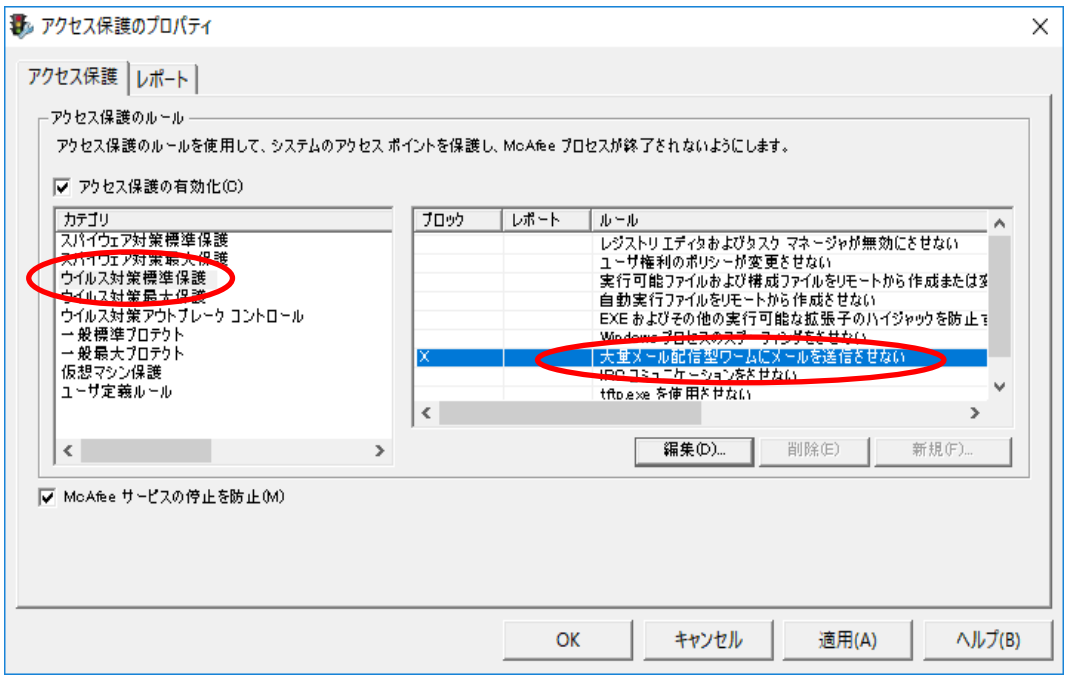
ここでは、ウィルス対策ソフトとして VirusScan を例に示します。

なお、以下の画面は Windows Server 2016 で操作したときの画面になります。

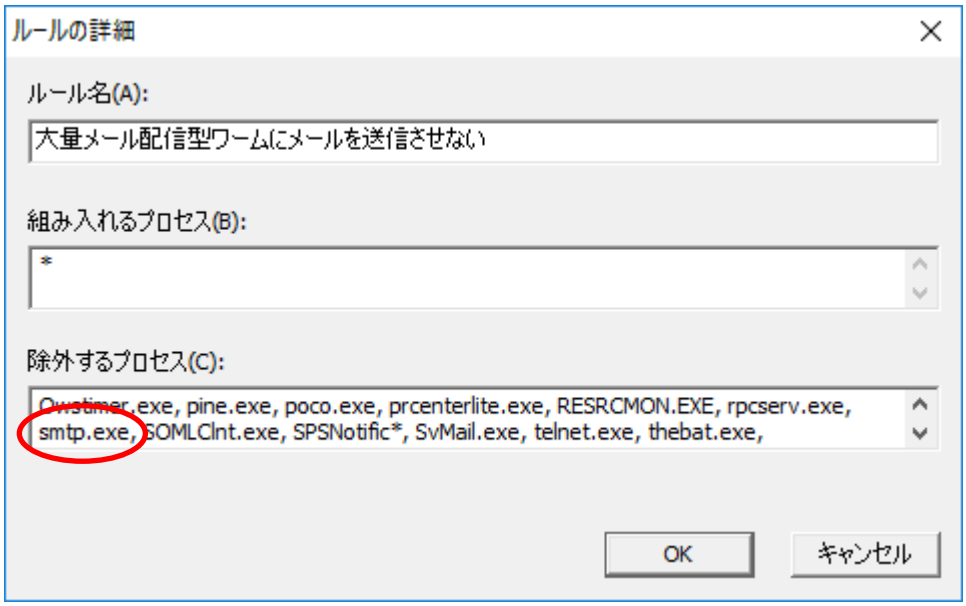
VirusScan のコンソールを開き、アクセス保護を選択します。



アクセス保護タブで、カテゴリは「ウィルス対策標準保護」、ルールは「大量メール配信型ワームメールを送信させない」を選択し、[編集]を選択します。



以下の画面で、除外するプロセスにメール送信プログラムの smtp.exe をカンマで区切って追加した後、OK を押してください。



(2) Windows ファイアウォールの設定

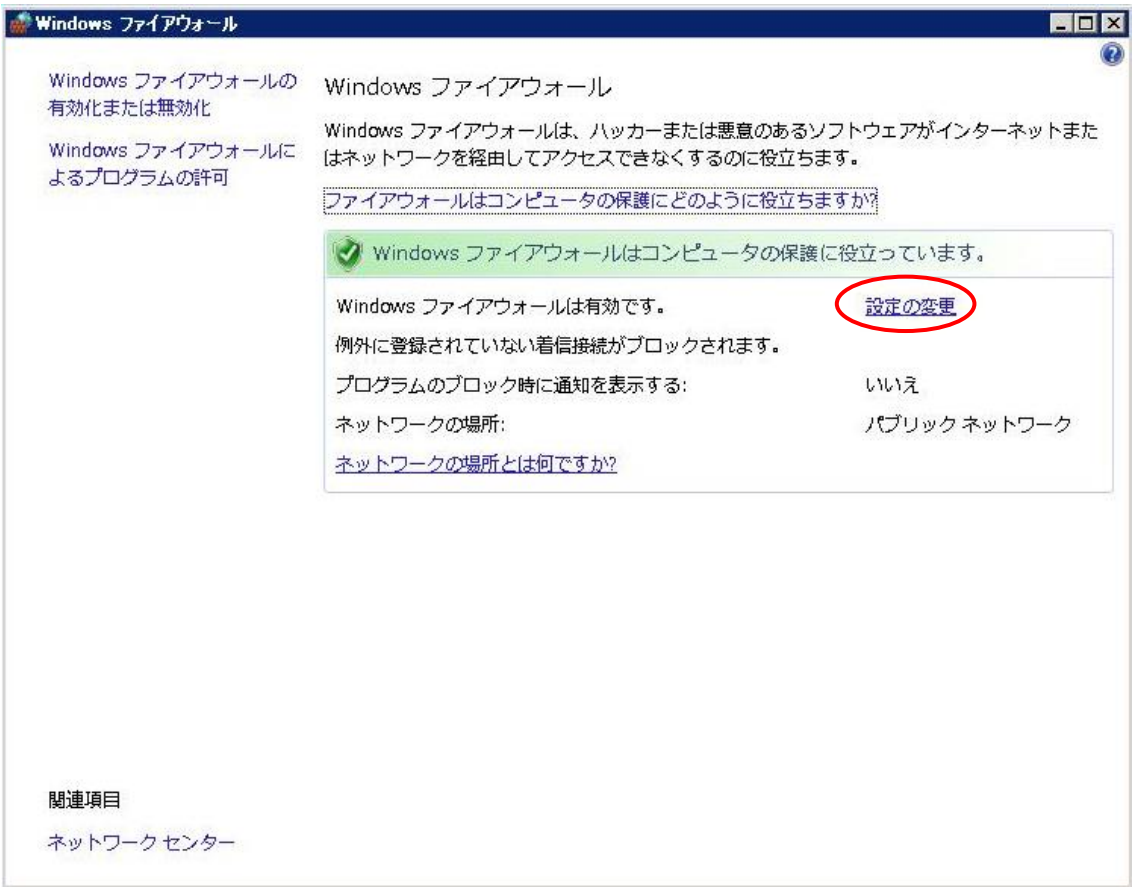
当該サービスでは､プロセス間の通信にポート番号 34145 と 34146 を使用しています。このため、Windows のファイアウォールの例外にマネージャプログラム sts.exe を登録して、通信を許可します。また、SNMP Trap 機器の監視を行なう場合、SNMP Trap を受信するために、snmptrap.exe を登録します。

以下に Windows ファイアウォールの例外でプログラムを追加する手順を示します。

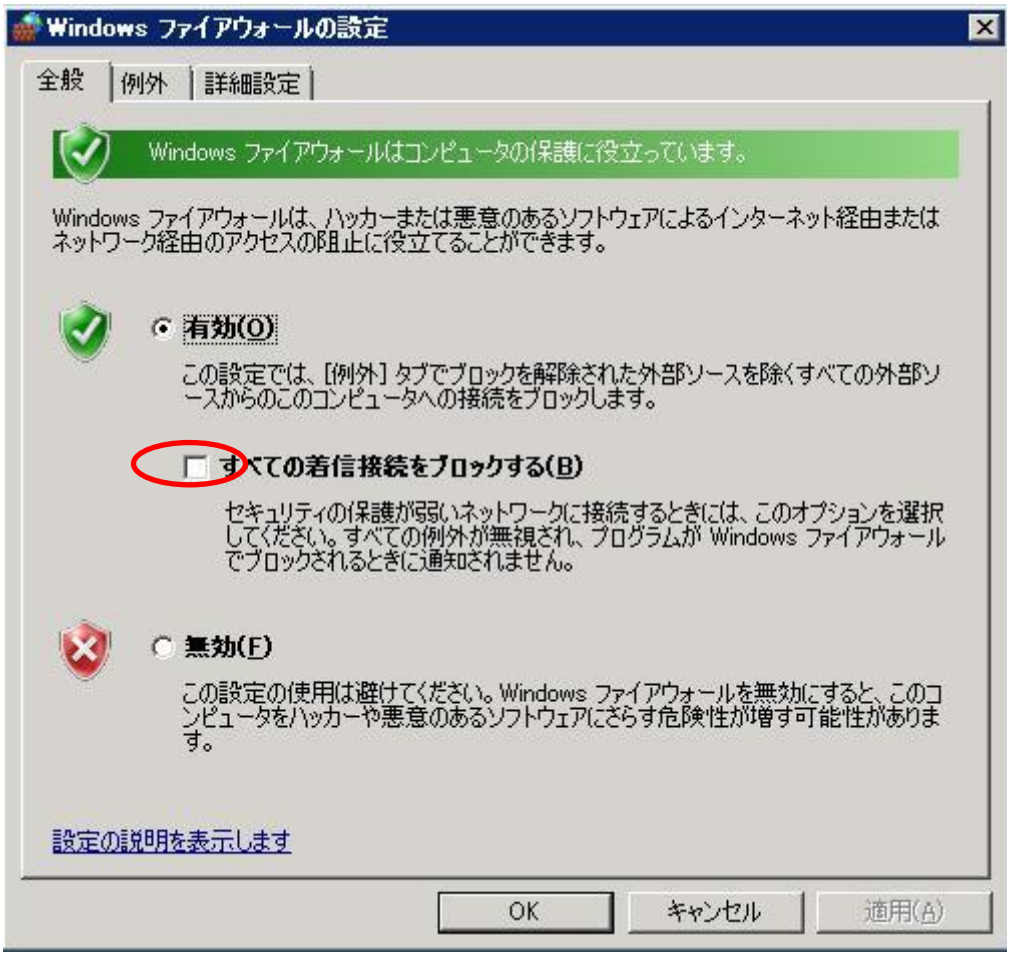
a) Server 2008 の場合

[コントロールパネル]→[Windows ファイアウォール]のパネルを開きます。

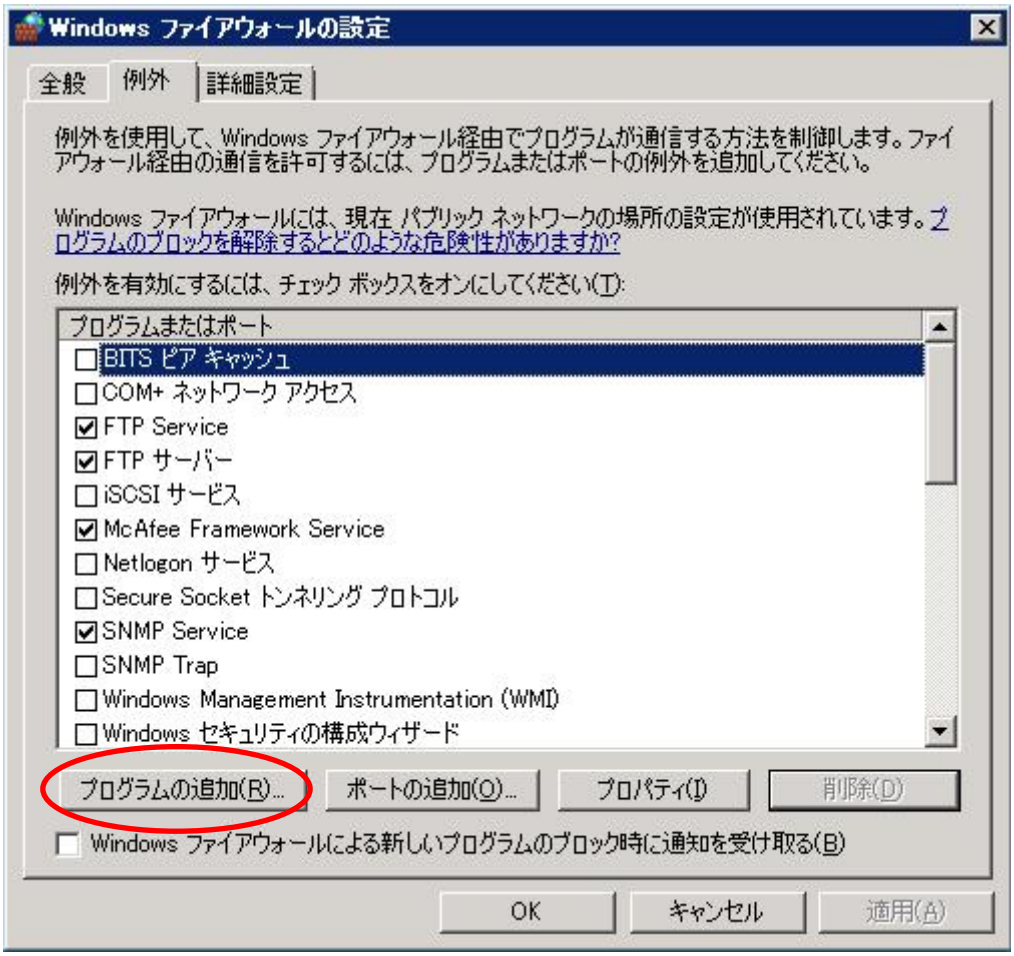
設定の変更を選択します。



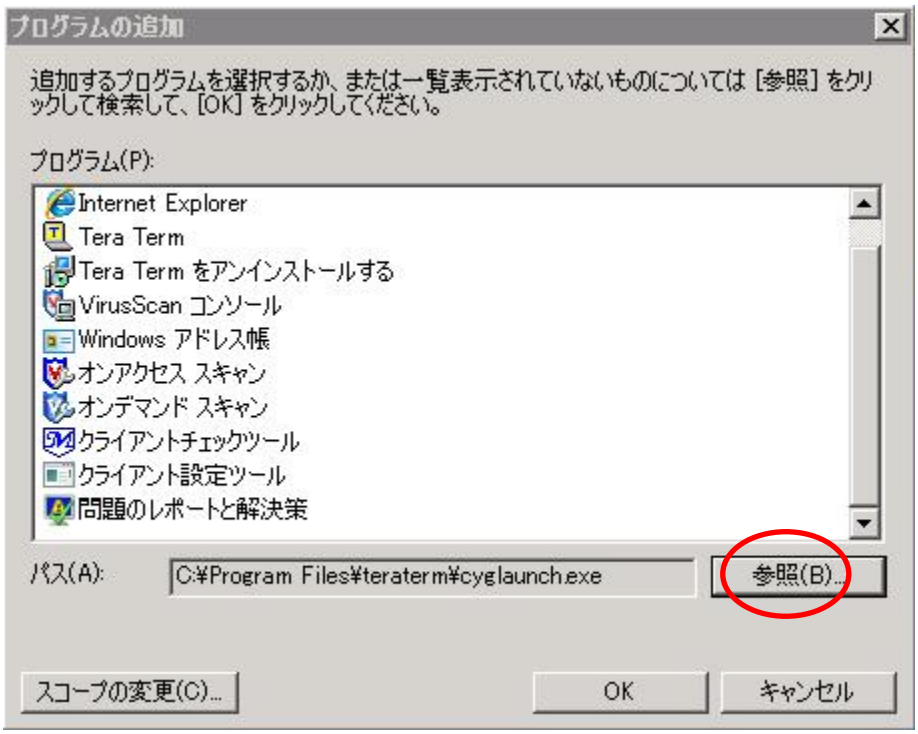
[全般]タブを選択します。
“有効”が選択されている場合： ”例外を許可しない”のチェックを外してください。



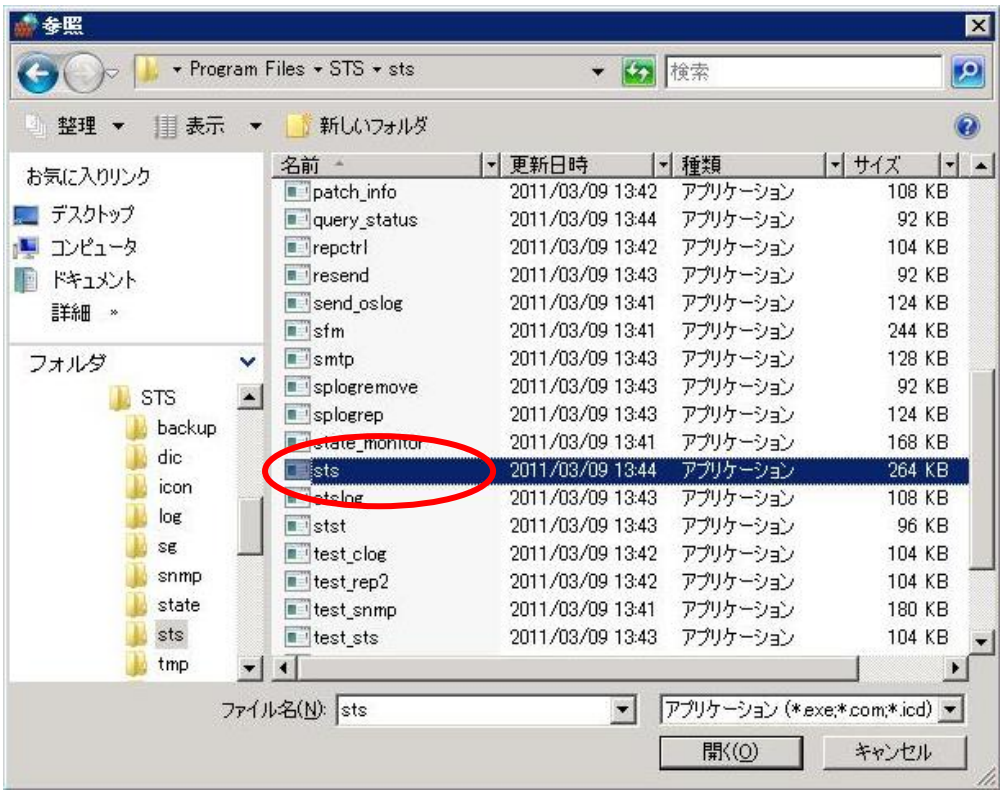
・sts.exe の追加
[例外]タブを選択し、マネージャプログラム(sts.exe)を追加します。
最初に、[プログラムの追加]を押し、プログラムの追加画面を出します。



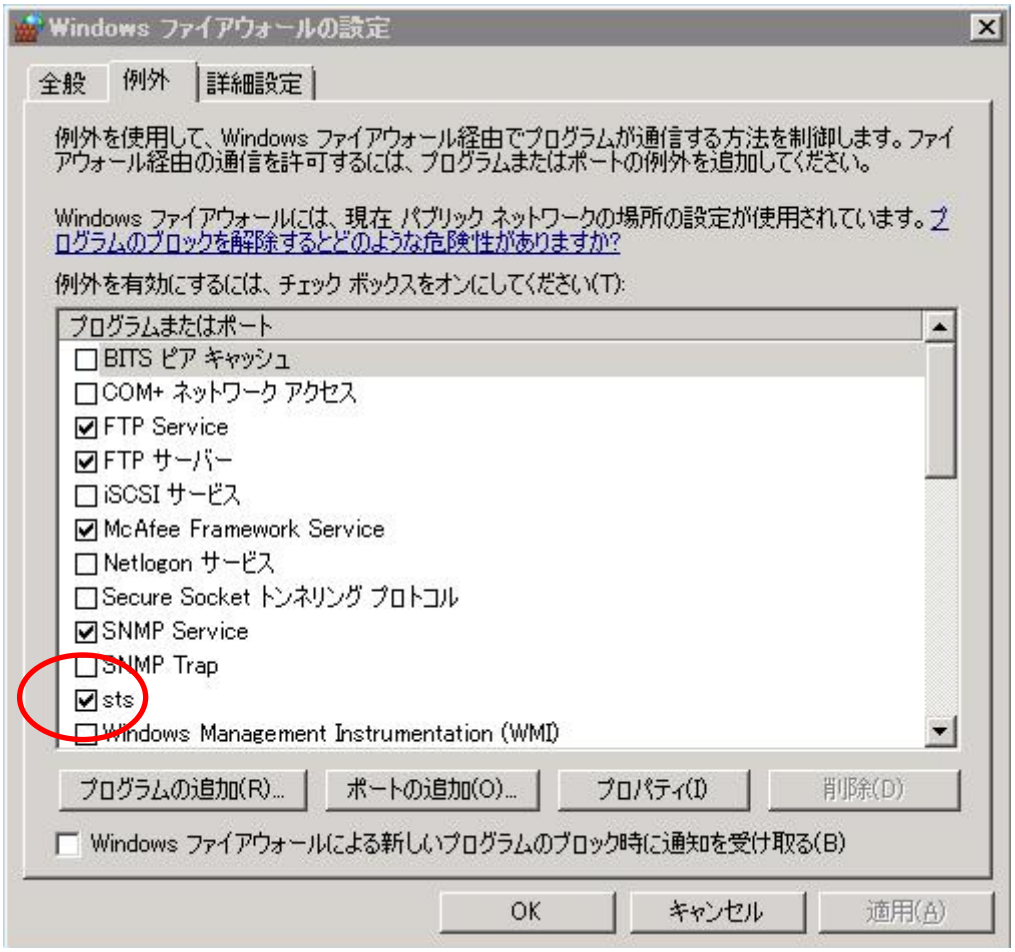
次に参照ボタンを押下します。



[参照]画面で、当該サービスをインストールしたパス（規定値の場合：C:¥Program Files (x86)¥STS¥）の sts フォルダを選択し、マネージャプログラム sts.exe を[開く]で選択してください。



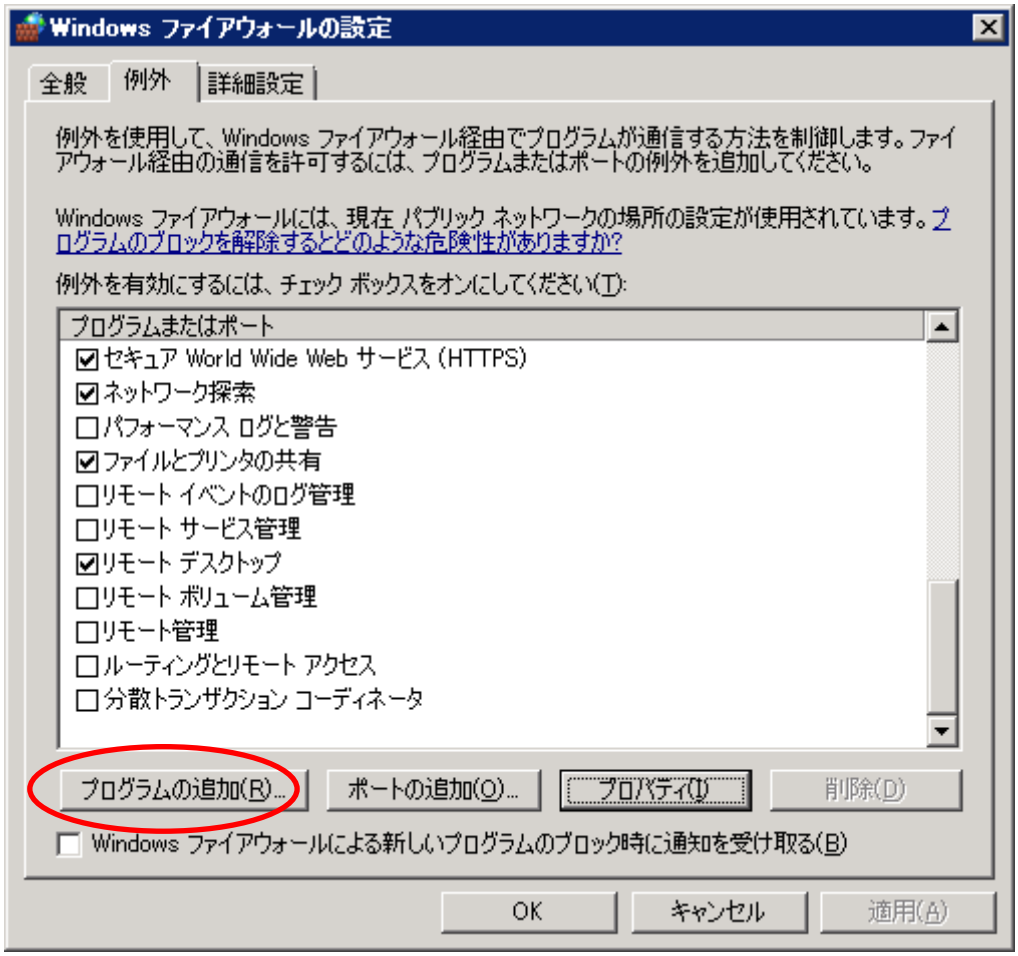
sts.exe を追加した後、[OK]を押すと、下のようになります。sts がチェックされていることを確認して、[OK]を押して、終了してください。
※SNMP Trap 機器の監視を行なう場合は、[OK]を押す前に次のページ以降の設定を行なってください。



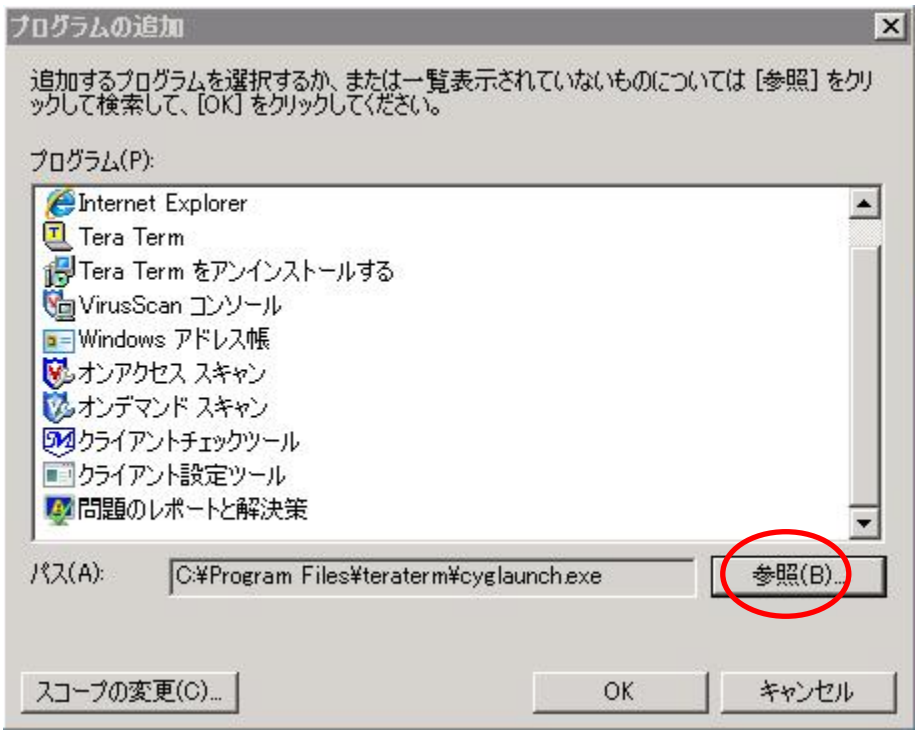
・snmptrap.exe の例外登録

[例外]タブを選択し、SNMP Trap 受信プログラム(snmptrap.exe)を追加します。

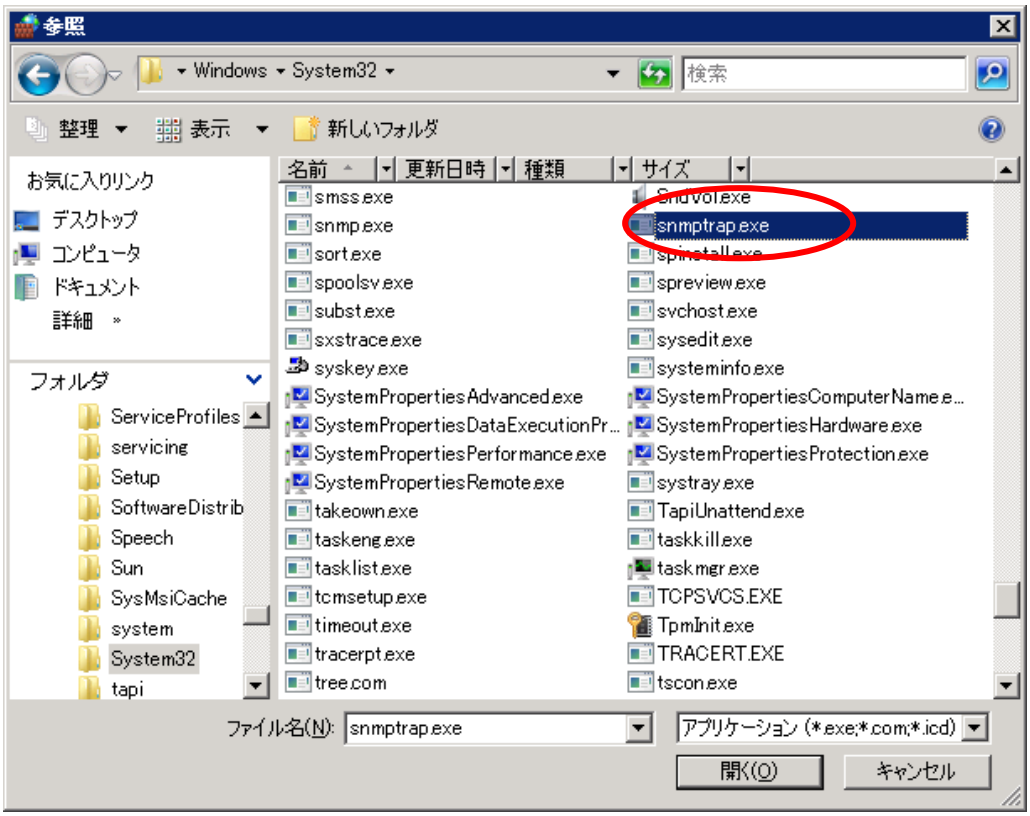
最初に、[プログラムの追加]を押し、プログラムの追加画面を出します。



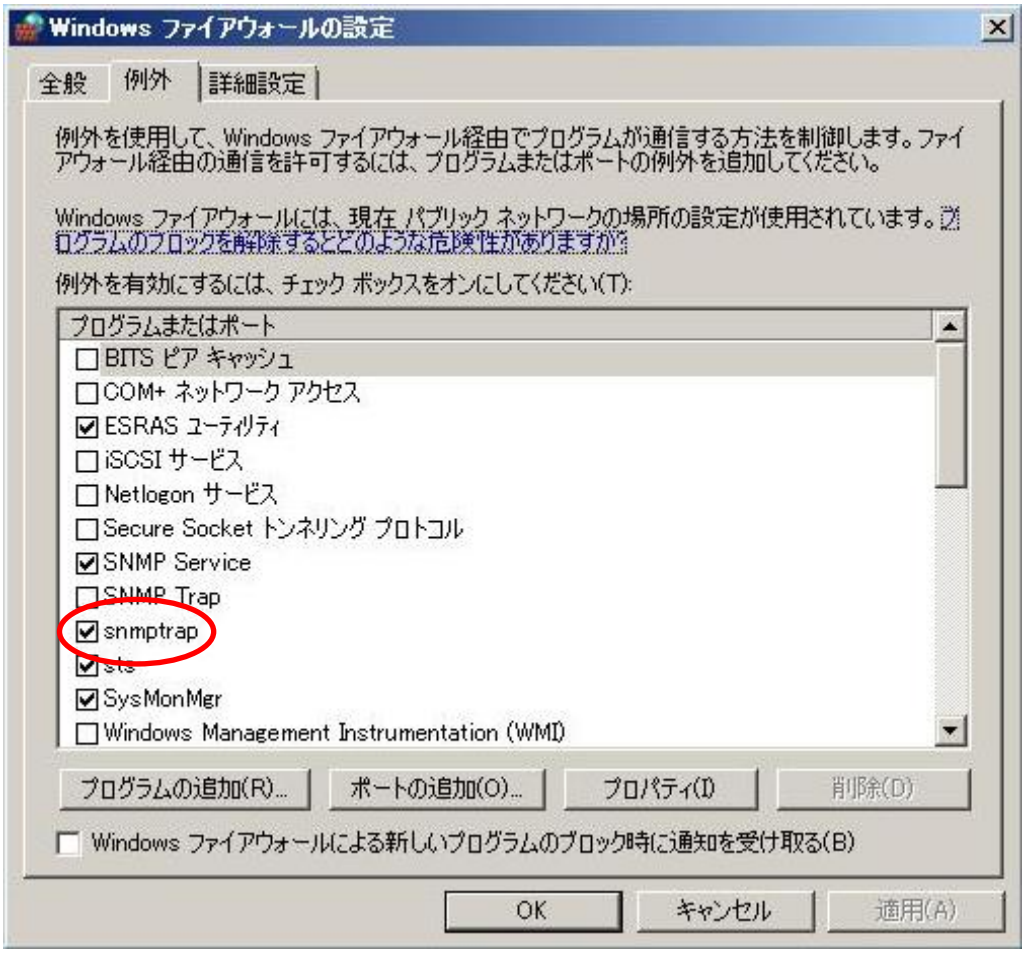
次に参照ボタンを押下します。



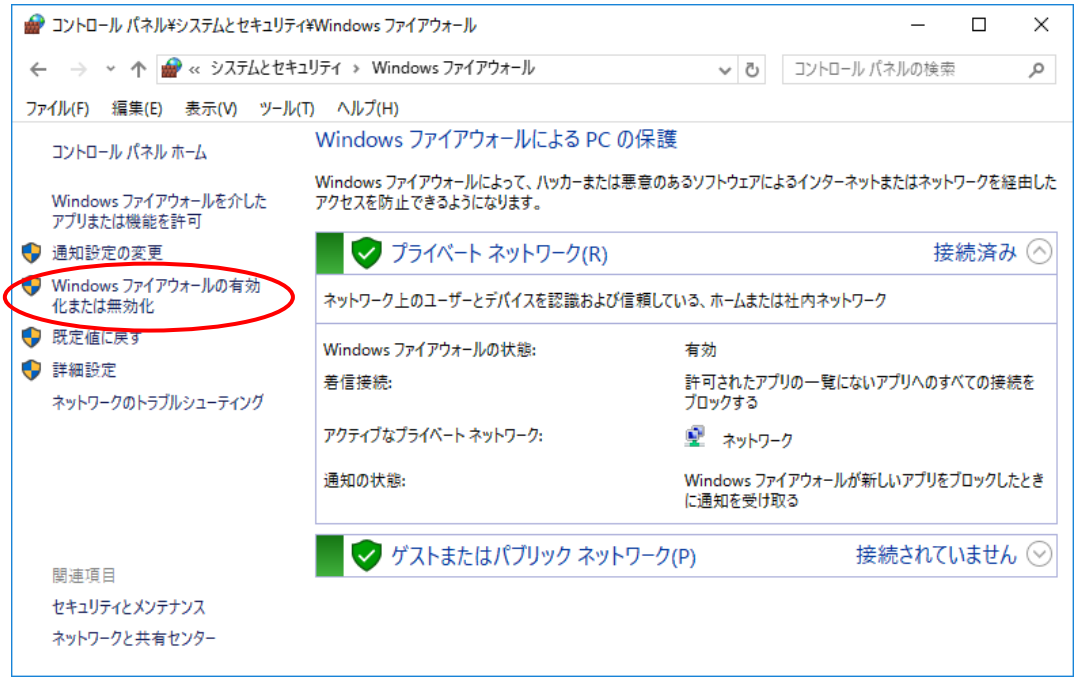
[参照]画面で、当該サービスをインストールしたパス（規定値の場合：C:¥Windows¥System32¥）を選択し、snmptrap.exe を[開く]で選択してください。



snmptrap.exe を追加した後、[OK]を押すと、下のようになります。snmptrap がチェックされていることを確認して、[OK]を押して、終了してください。

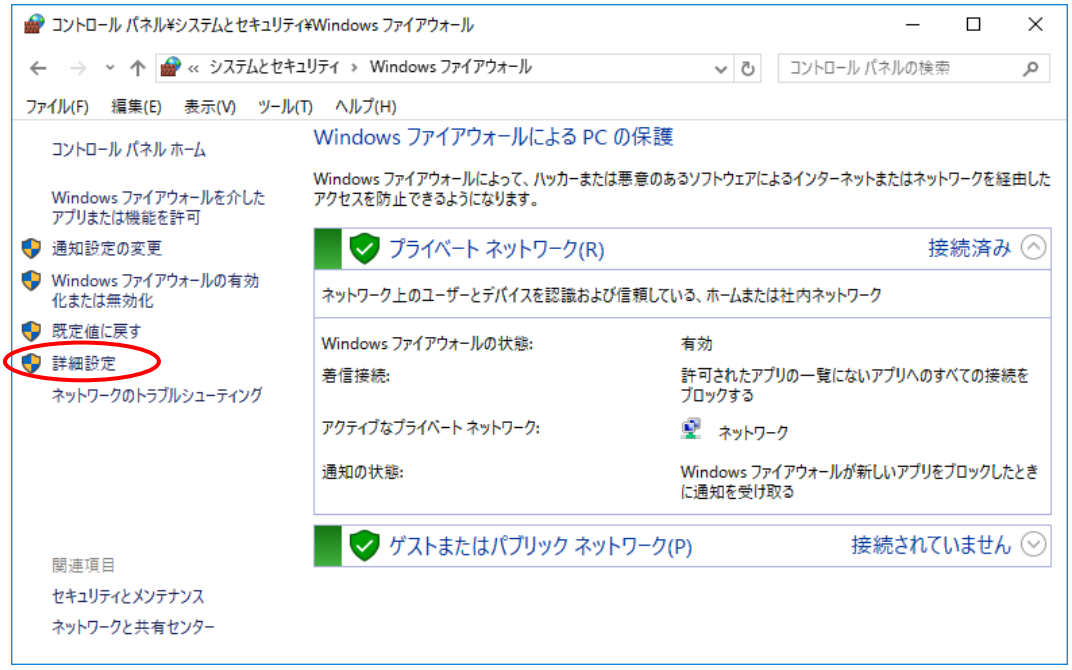


b)　Windows Server 2008 R2／2012 R2／2016 の場合
[コントロールパネル]→[システムとセキュリティ]→[Windows ファイアウォール]のパネルを開きます。
[Windows ファイアウォールの有効化または無効化]を選択します。

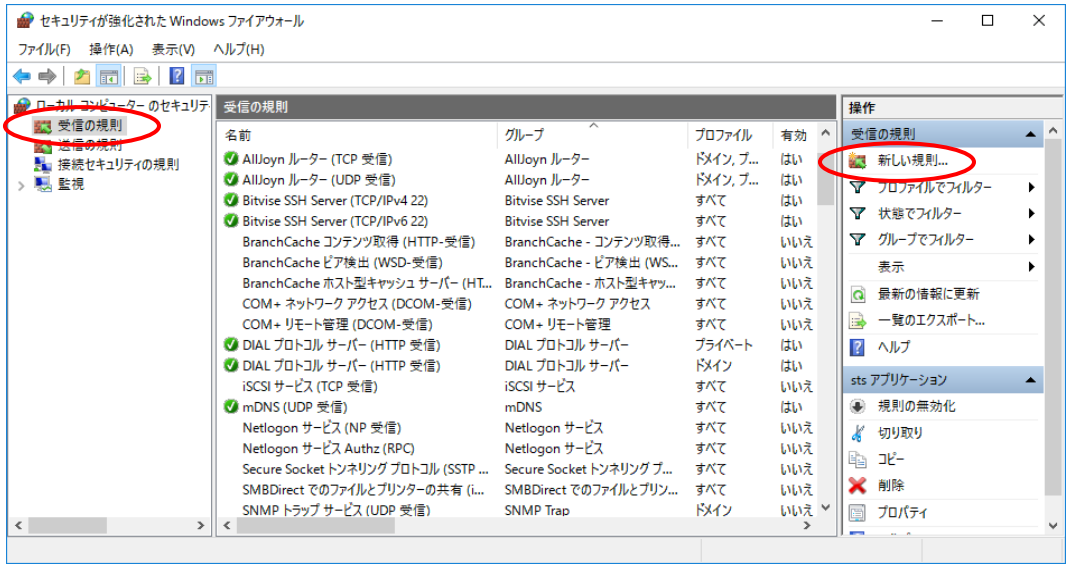


各種類のネットワーク設定で[Windows ファイアウォールを有効にする]が選択されている場合、[許可されたアプリの一覧にあるアプリも含め、すべての着信接続をブロックする]のチェックを外してください。
設定を変更した後、[OK]ボタンを押してください。

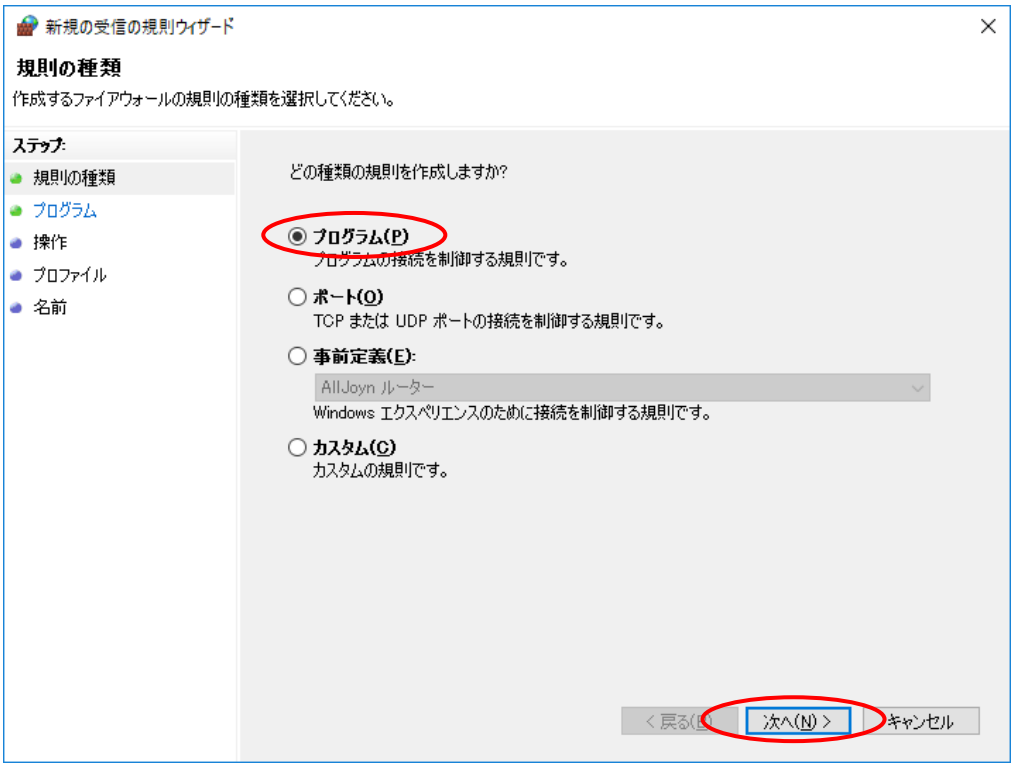
・マネージャプログラム（sts.exe）の追加
[Windows ファイアウォール]のパネルから[詳細設定]を選択します。



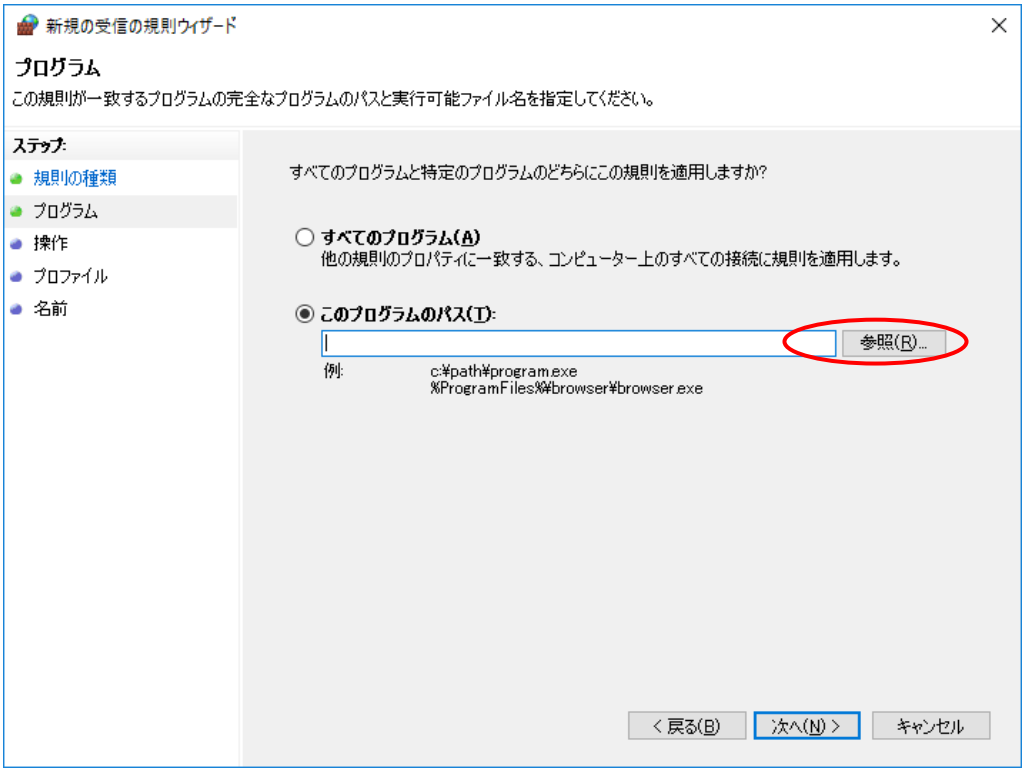
[セキュリティが強化された Windows ファイアウォール]の画面から左側ツリーの[受信の規則]を選択して、右側メニューから[新しい規則]を選択します。



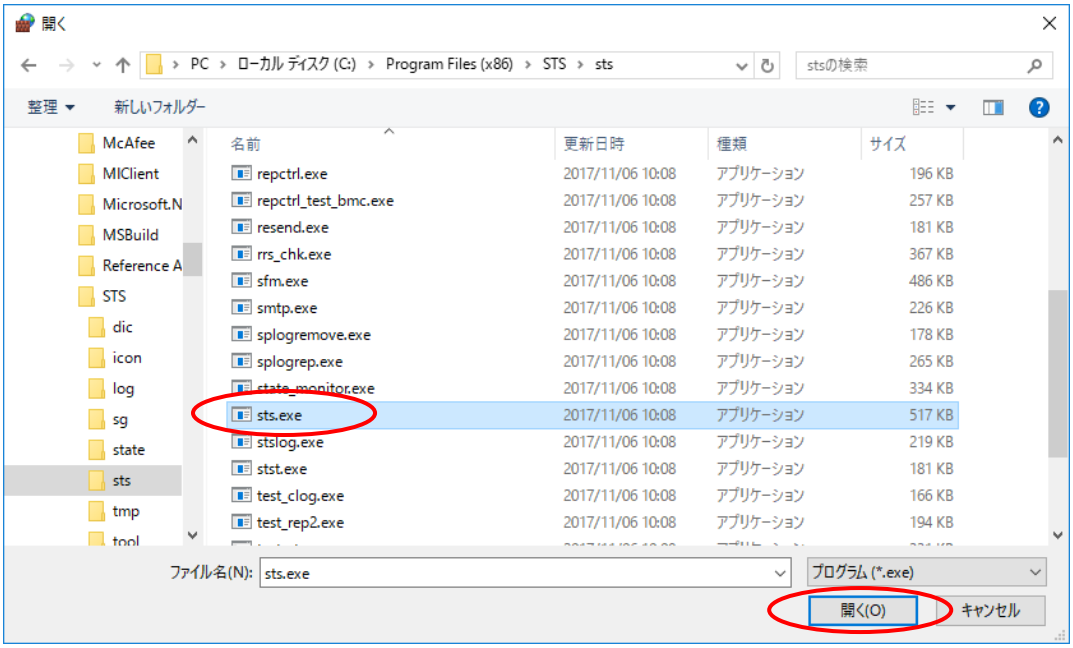
[新規の受信の規則ウィザード]の[規則の種類]では、[プログラム]を選択します。
選択した後、[次へ]ボタンを押してください。



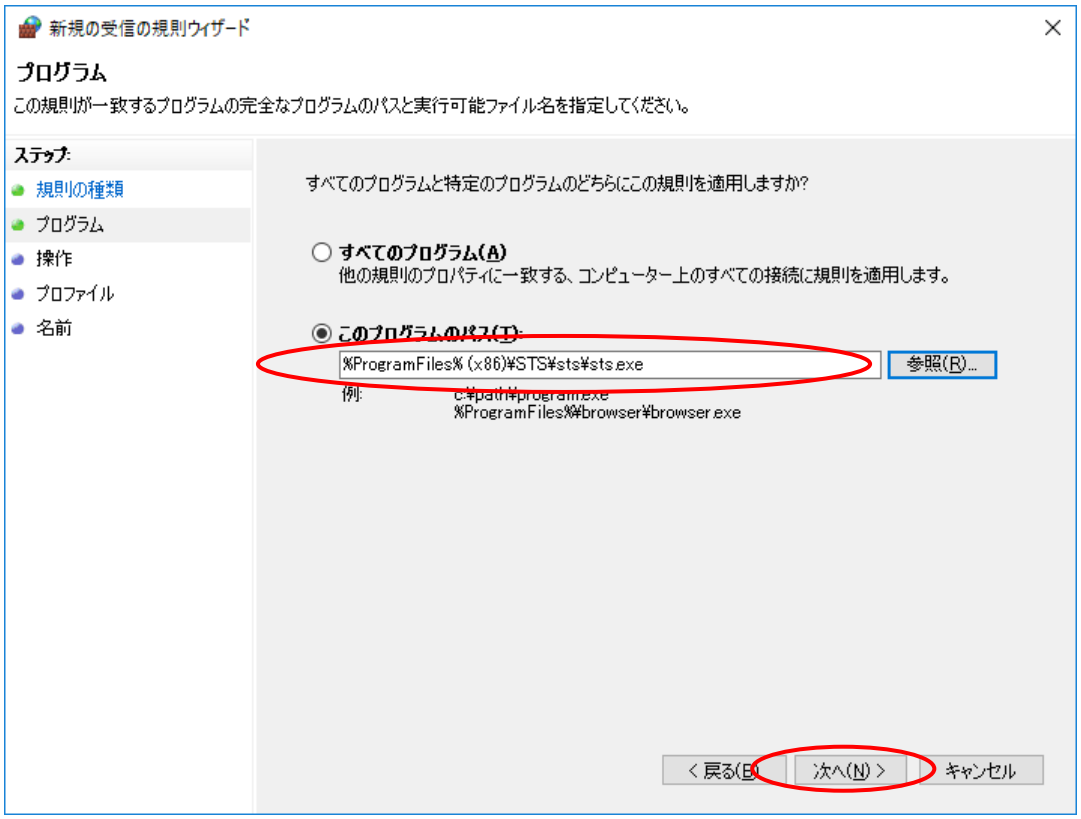
[プログラム]では、マネージャプログラム（sts.exe）を追加します。
最初に、[このプログラムのパス]を選択後、[参照]ボタンを押し、[開く]画面を出します。



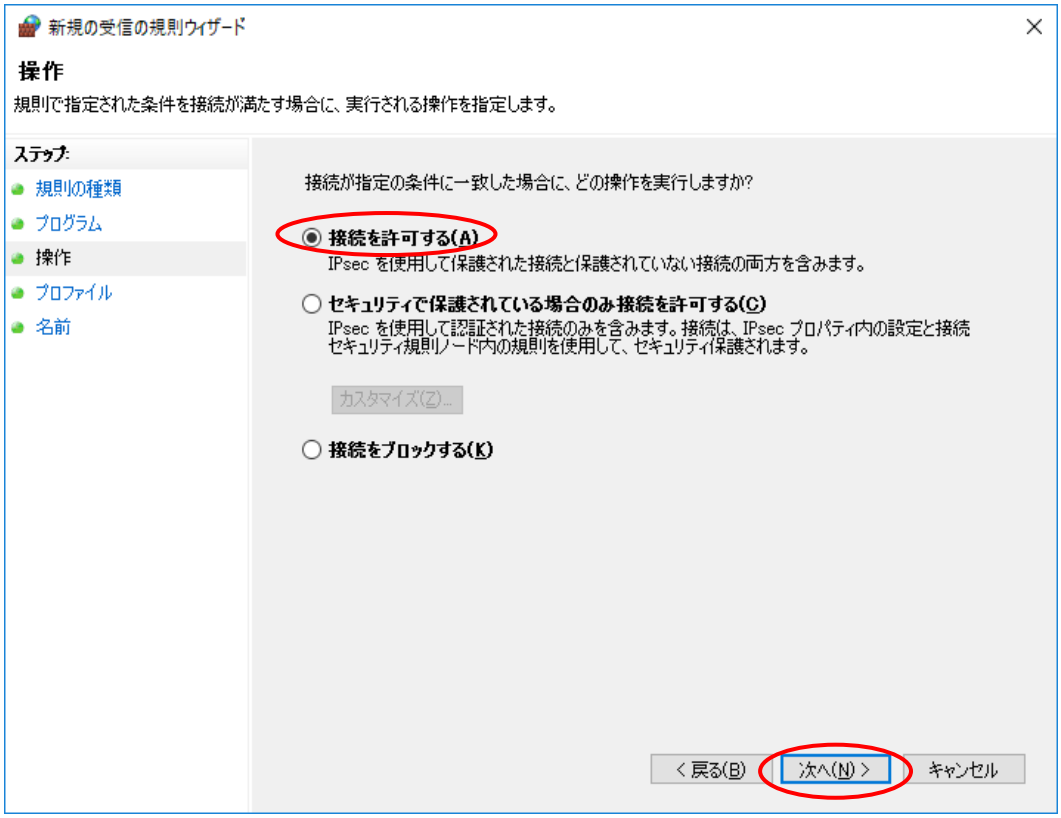
[開く]画面では、当該サービスをインストールしたパス（規定値の場合：C:¥Program Files（x86)¥STS¥）の sts フォルダを選択し、マネージャプログラム（sts.exe）を選択後、[開く]ボタンを押してください。



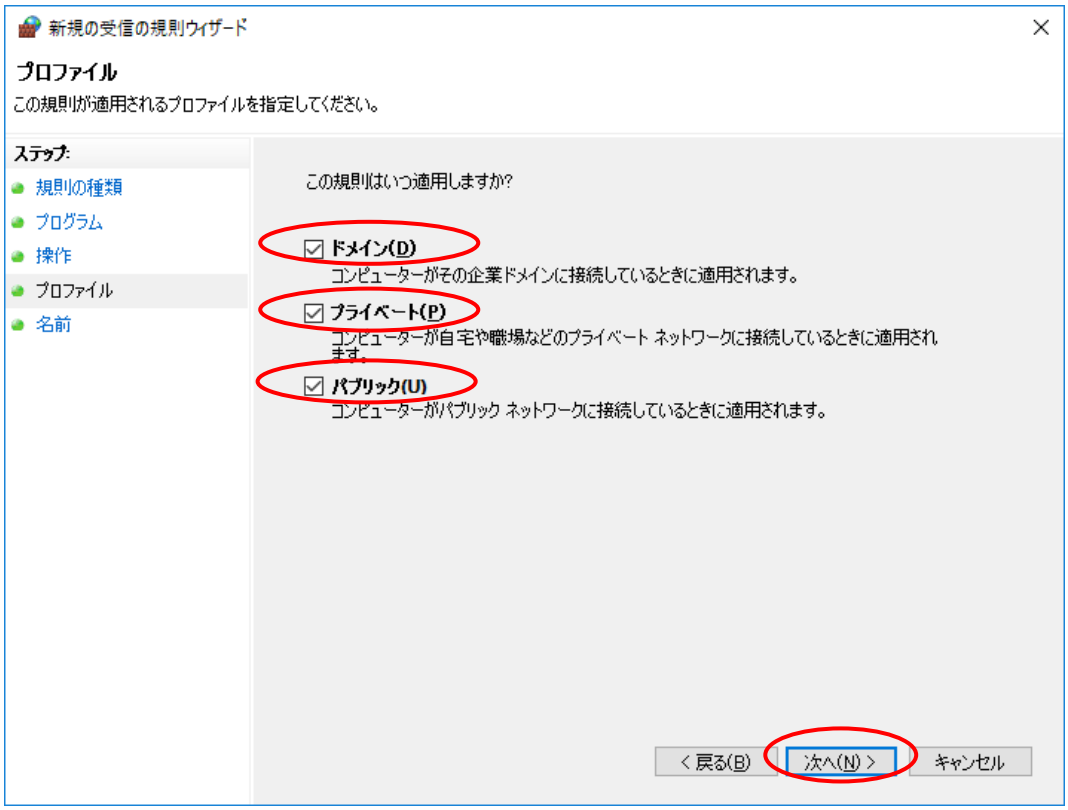
マネージャプログラム（sts.exe）を追加した後、[このプログラムのパス]に sts.exe のパスが設定されます。
sts.exe へのパスが正しく設定されていることを確認した後、[次へ]ボタンを押してください。



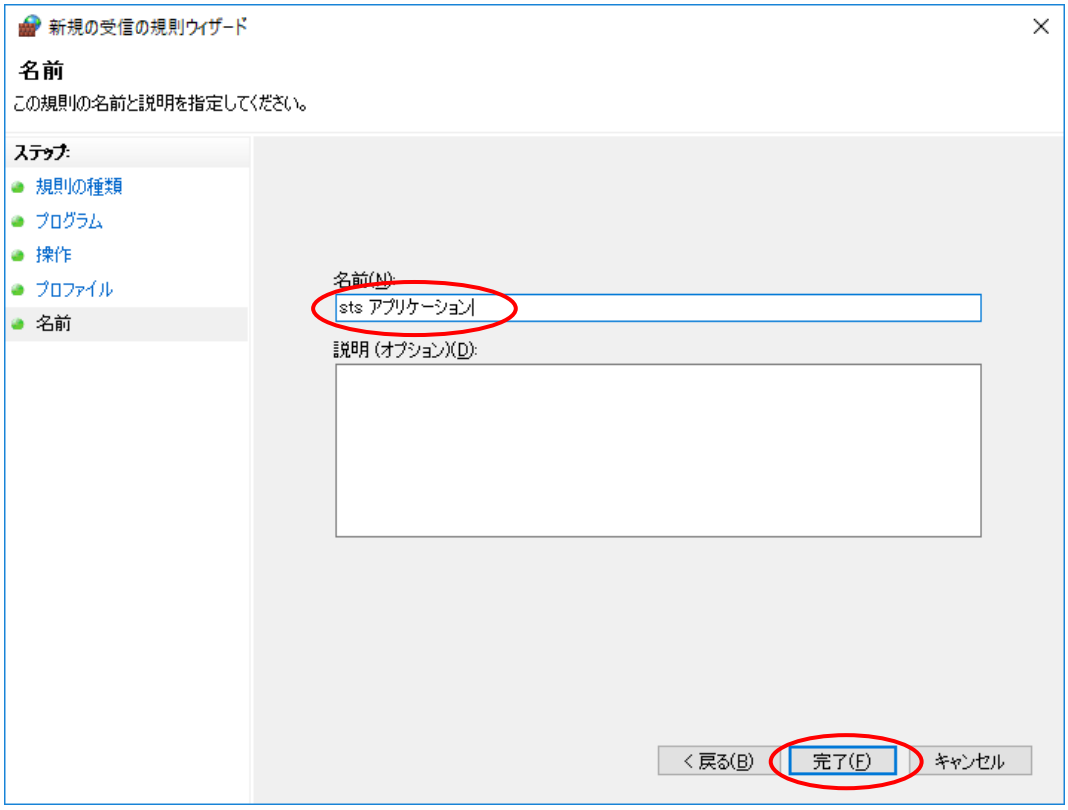
[操作]では、[接続を許可する]を選択します。
選択した後、[次へ]ボタンを押してください。



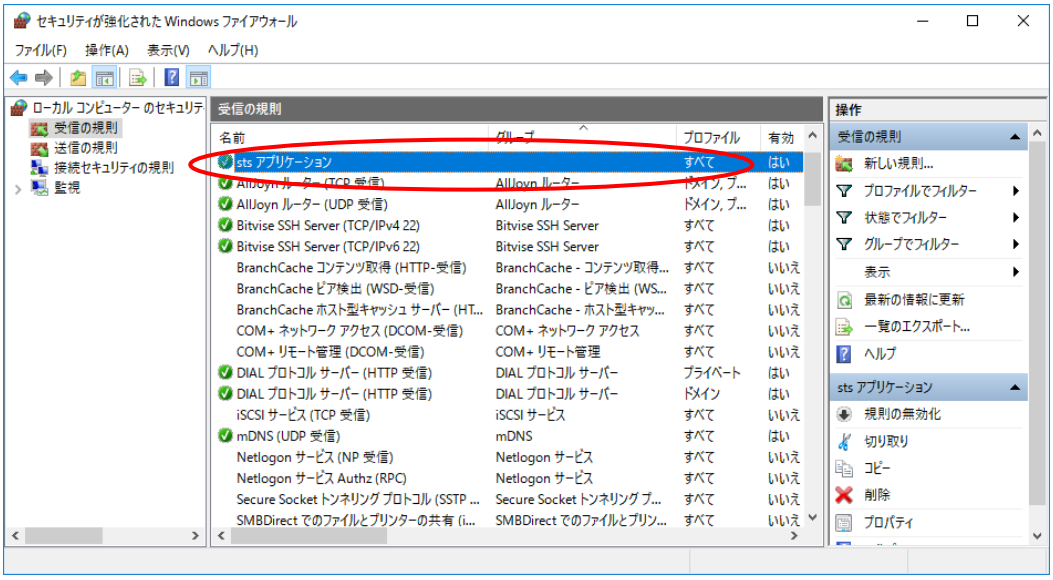
[プロファイル]では、[ドメイン]、[プライベート]、[パブリック]の 3 つ全てをチェックします。
チェックした後、[次へ]ボタンを押してください。



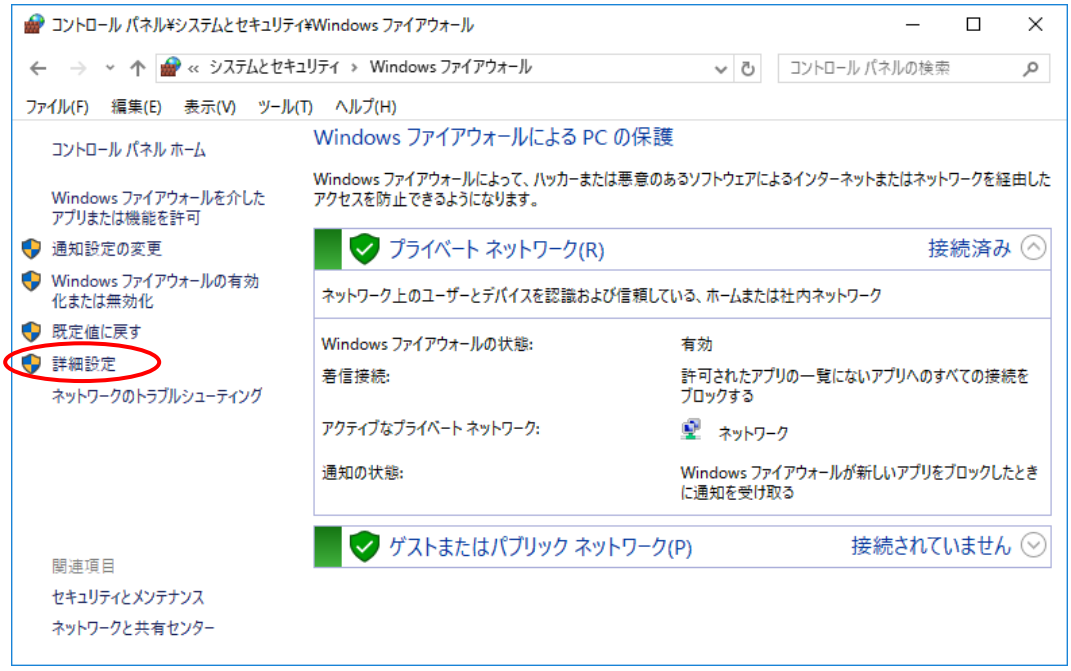
[名前]では、[名前]の入力欄に『sts アプリケーション』(”sts”＋半角空白＋”アプリケーション”) と入力します。
入力した後、[完了]ボタンを押してください。



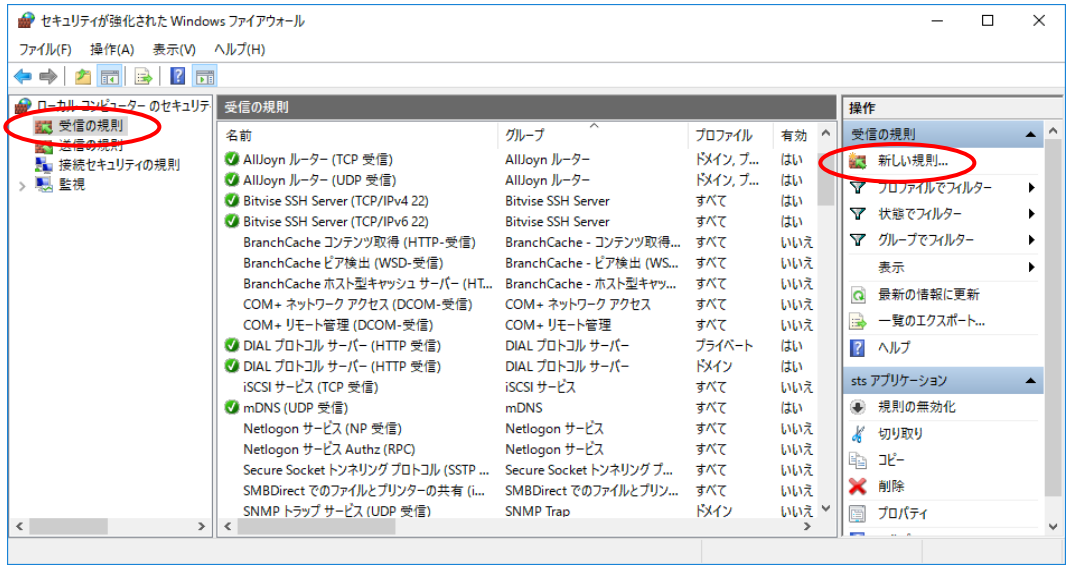
[新規の受信の規則ウィザード]の[完了]ボタンを押すと、下図の様に[セキュリティが強化された Windows ファイアウォール]の画面の中央リストに『sts アプリケーション』が追加されます。
※SNMP Trap 機器の監視を行なう場合は、次ページ以降の設定も行なってください。



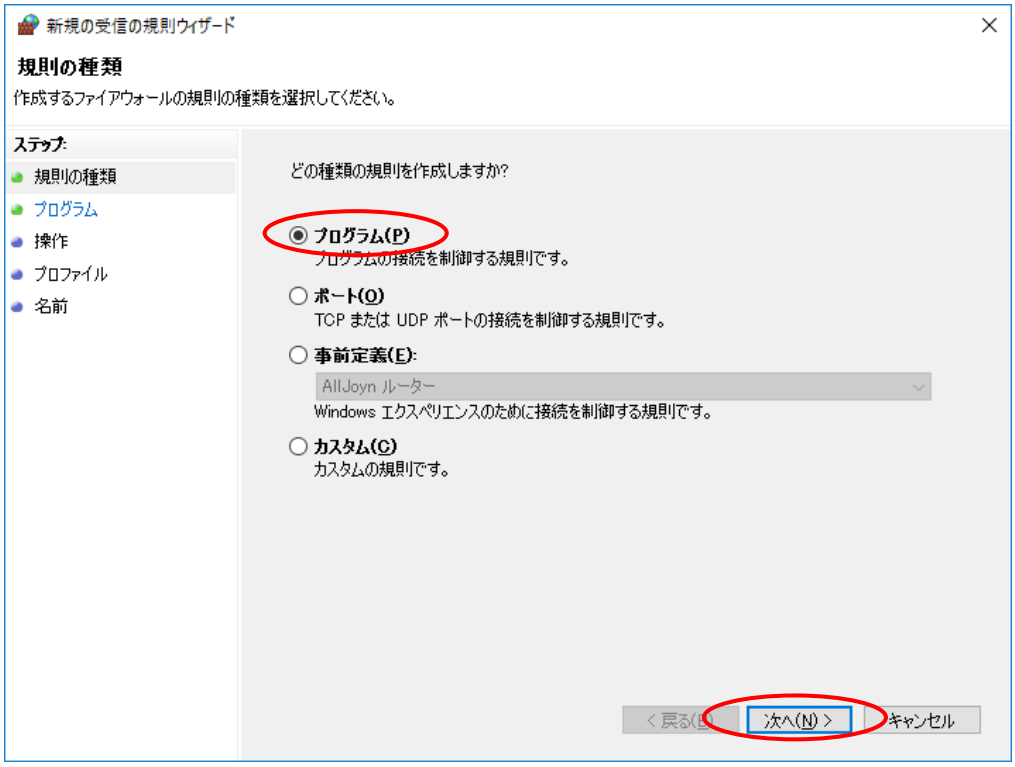
・SNMP Trap 受信プログラム（snmptrap.exe）の追加
[Windows ファイアウォール]のパネルから[詳細設定]を選択します。



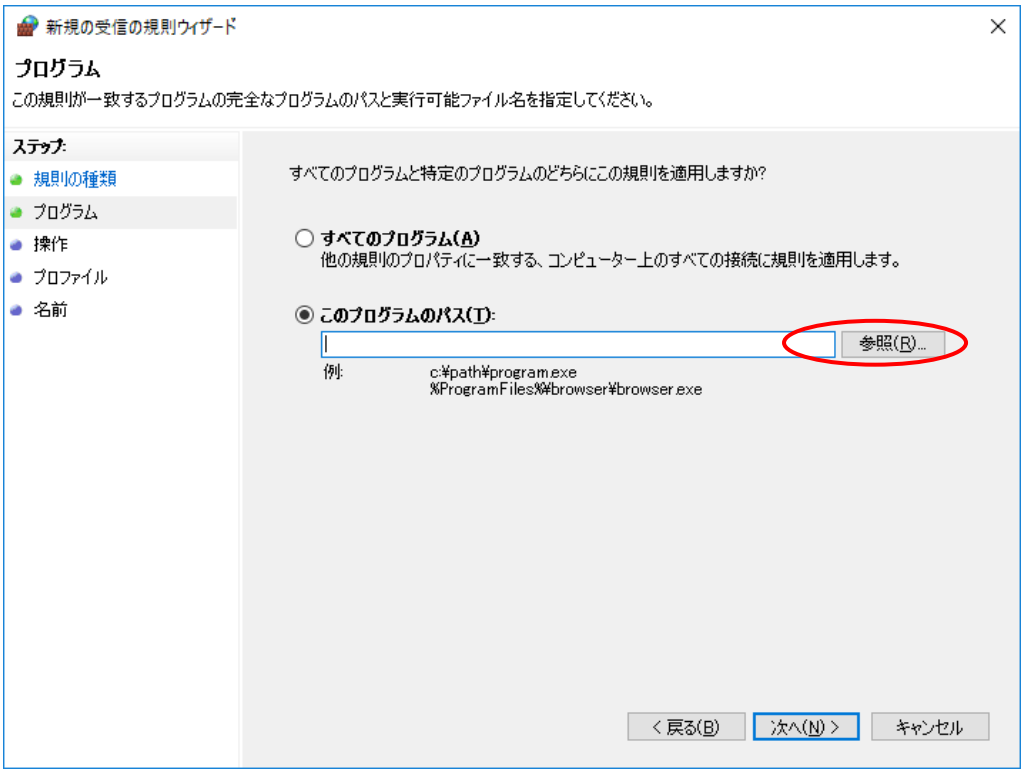
[セキュリティが強化された Windows ファイアウォール]の画面から左側ツリーの[受信の規則]を選択して、右側メニューから[新しい規則]を選択します。



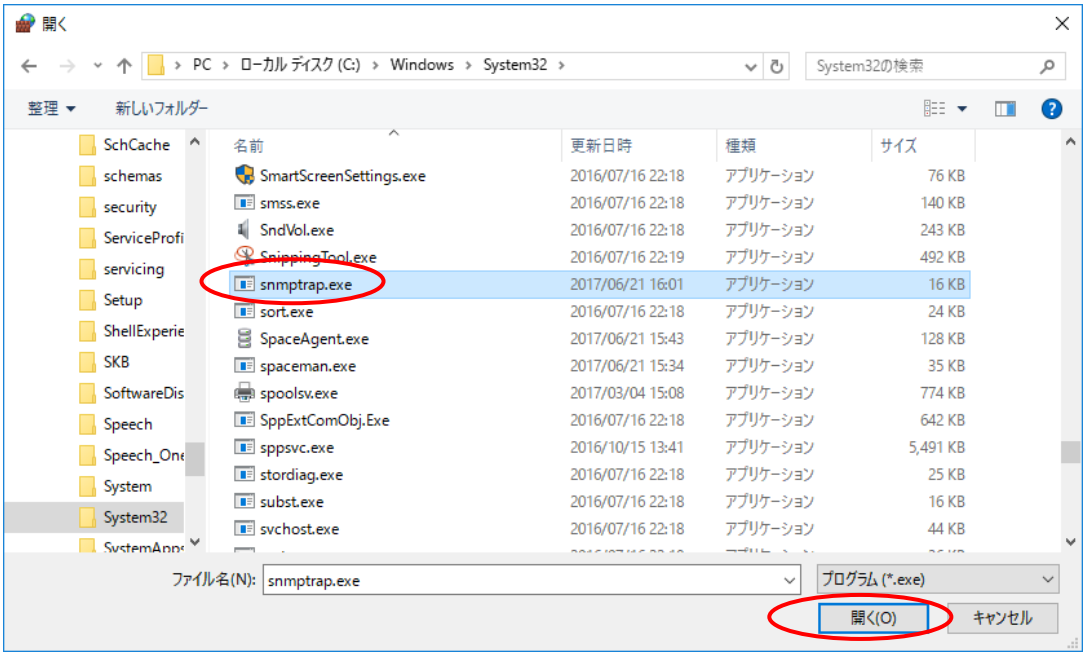
[新規の受信の規則ウィザード]の[規則の種類]では、[プログラム]を選択します。
選択した後、[次へ]ボタンを押してください。



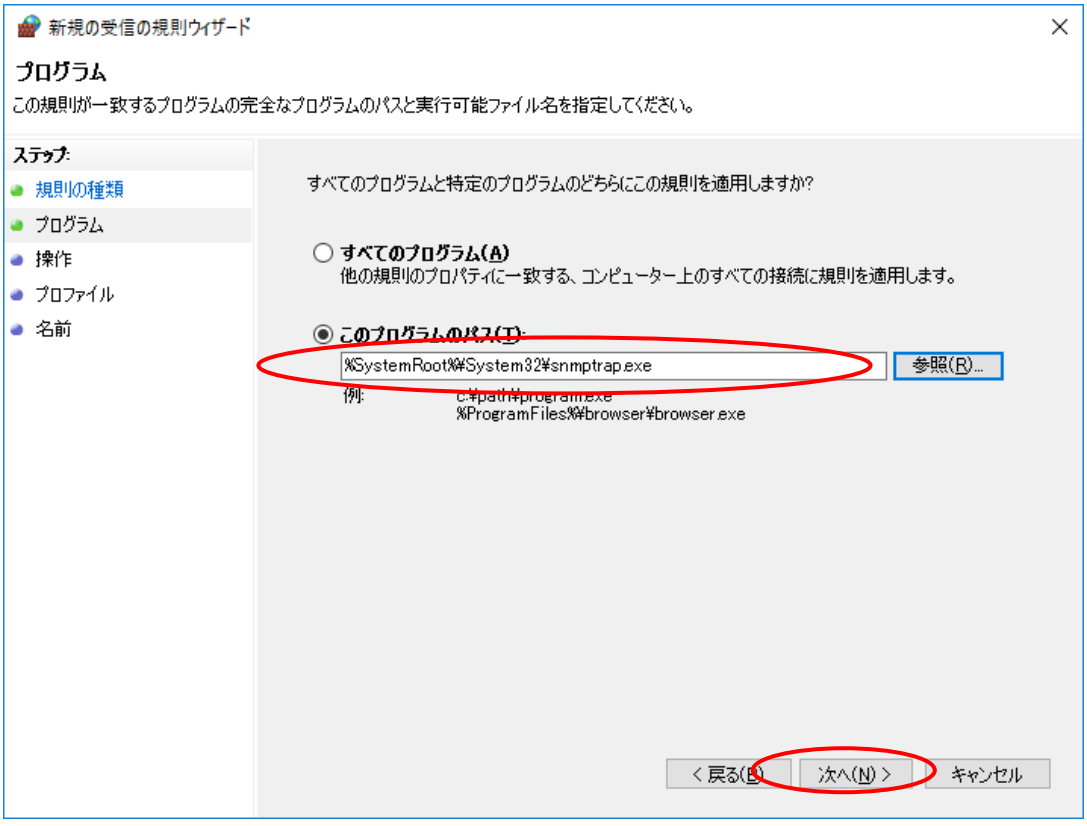
[プログラム]では、SNMP Trap 受信プログラム（snmptrap.exe）を追加します。
最初に、[このプログラムのパス]を選択後、[参照]ボタンを押し、[開く]画面を出します。



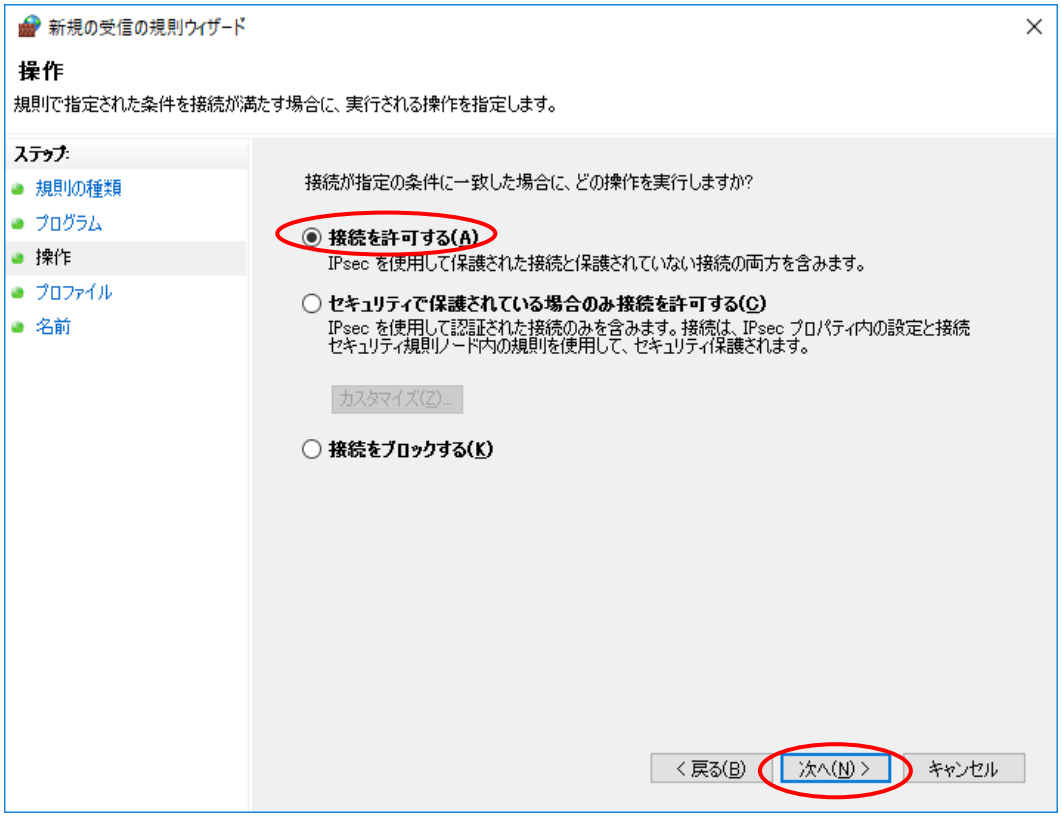
[開く]画面では、Windows のシステムディレクトリ（規定値の場合：C:¥Windows¥System32¥）の SNMP Trap 受信プログラム（snmptrap.exe）を選択後、[開く]ボタンを押してください。



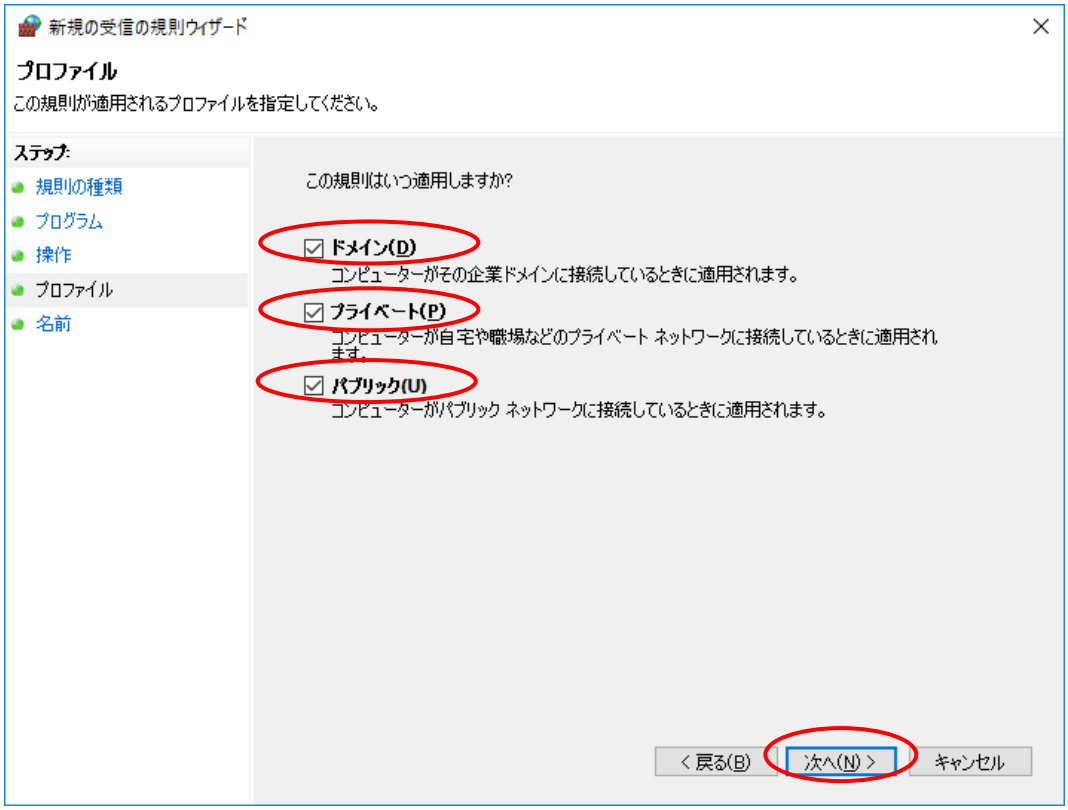
SNMP Trap 受信プログラム（snmptrap.exe）を追加した後、[このプログラムのパス]に snmptrap.exe のパスが設定されます。
snmptrap.exe へのパスが正しく設定されていることを確認した後、[次へ]ボタンを押してください。



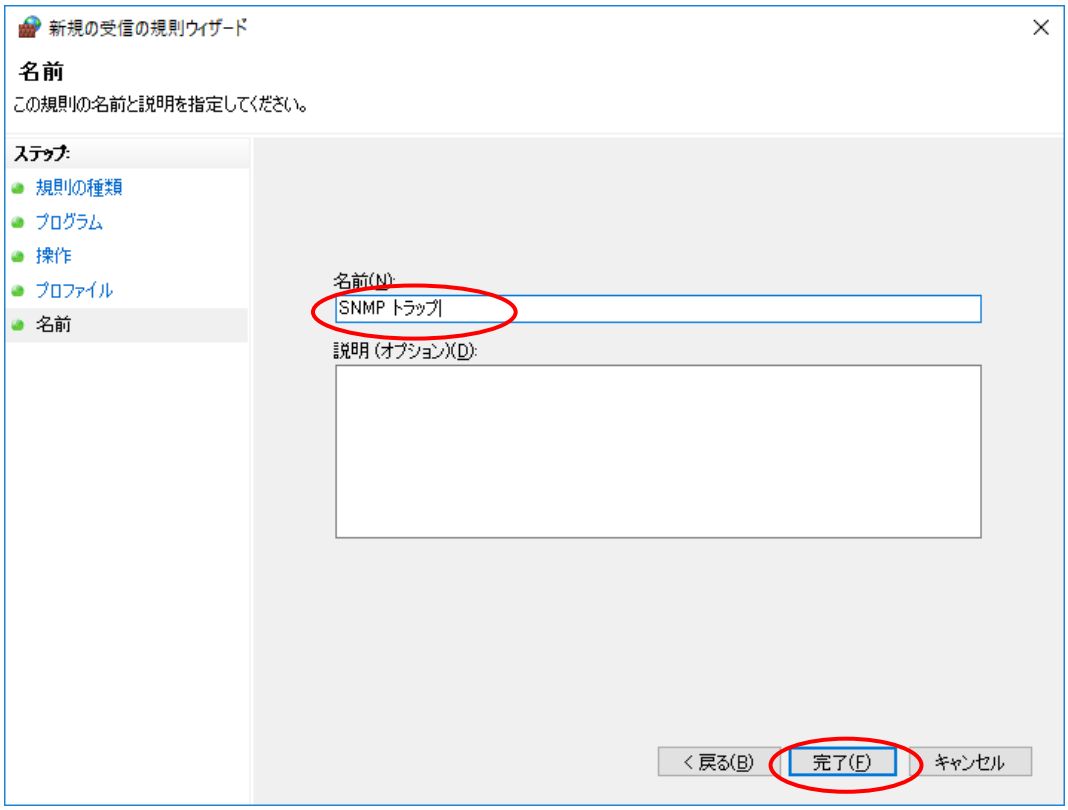
[操作]では、[接続を許可する]を選択します。
選択した後、[次へ]ボタンを押してください。



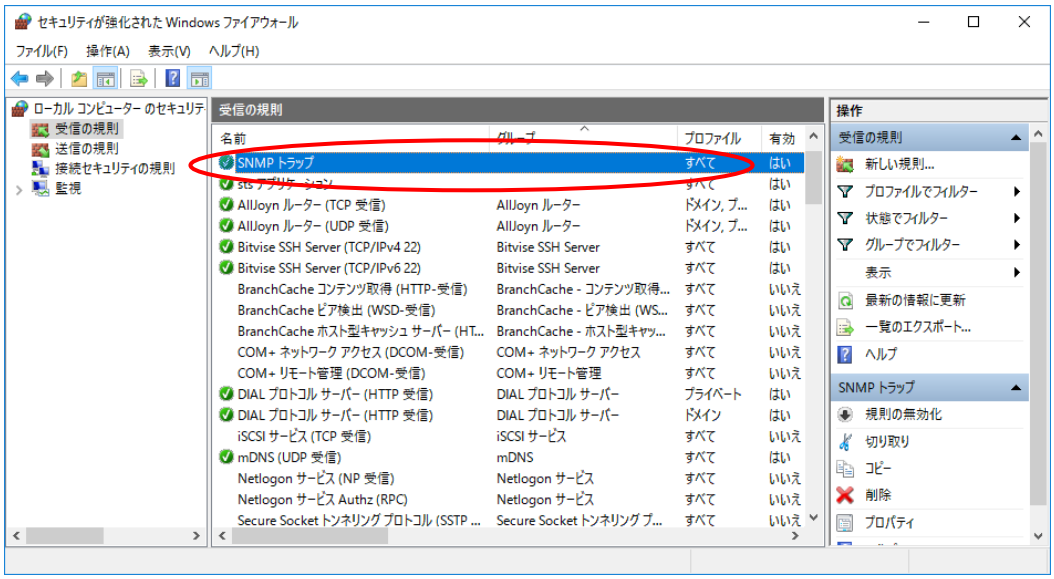
[プロファイル]では、[ドメイン]、[プライベート]、[パブリック]の 3 つ全てをチェックします。
チェックした後、[次へ]ボタンを押してください。



[名前]では、[名前]の入力欄に『SNMP トラップ』(”SNMP”＋半角空白＋”トラップ”)と入力します。
入力した後、[完了]ボタンを押してください。



[新規の受信の規則ウィザード]の[完了]ボタンを押すと、下図の様に[セキュリティが強化された Windows ファイアウォール]の画面の中央リストに『SNMP トラップ』が追加されます。



4.3.11. WebSAM との連携方法

WebSAM MCOperations および WebSAM System Navigator との連携方法は、「WebSAM MCOperations WebSAM System Navigator NX リモート通報 連携機能ガイド」を参照してください。

4.3.12. ESMPRO ServerManager と共存する場合の注意点

ESMPRO ServerManager と共存する場合は、ESMPRO ServerManager のアラートビューアの「SNMP トラップ受信設定」において、SNMP トラップ受信方式が「SNMP トラップサービスを使用する」を選択してください。「独自方法を使用する」を選択されていると NX リモート通報で SNMP Trap の受信ができません。

また、ESMPRO ServerManager 以外にも、Windows 標準の SNMP Trap サービスではなく、独自の方法で SNMP Trap を受信するソフトウェアが共存する場合は、NX リモート通報で SNMP Trap の受信ができません。

4.3.13. 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。

4.4. Agent ソフトのインストールと被監視サーバの設定

4.4.1. 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。

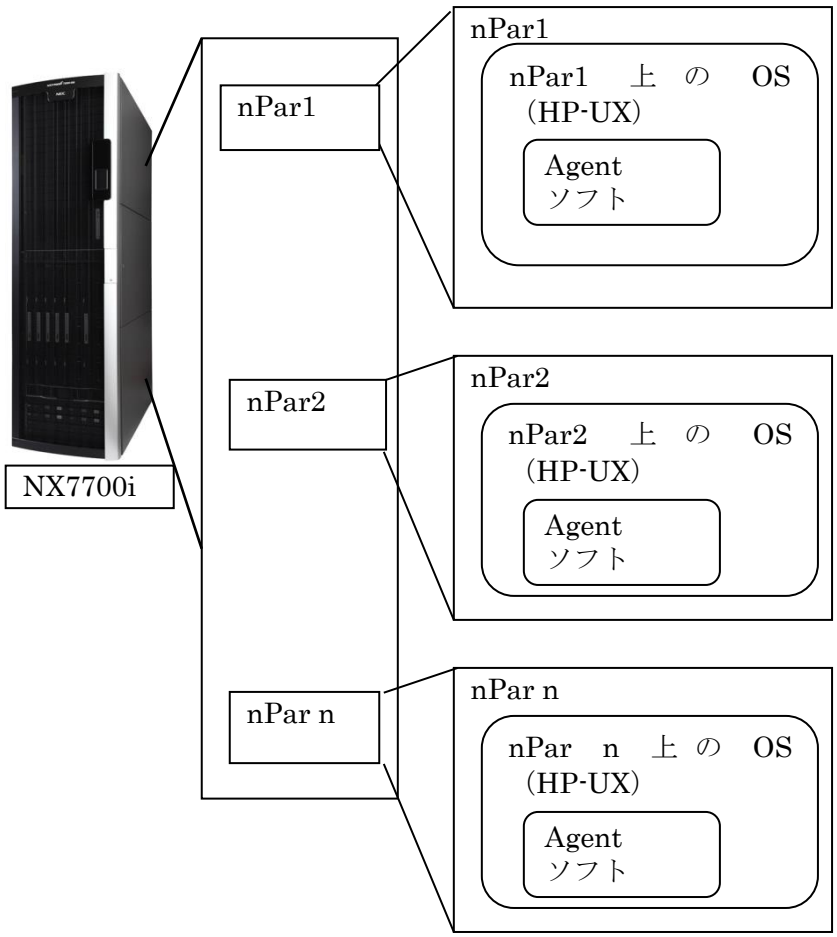


図 4-1 nPartitions 環境へのインストール対応図

4.4.2. Agent ソフトのインストール

－注意事項－
インストールは root 権限で実施願います。
root 権限以外の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.

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。Web サイトからダウンロードした物件を CD-ROM に格納する方法は、「10 ダウンロード物件の取り扱い方」の章を参照してください。

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は、/CDROM をファイル一式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ください。

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。

また、途中で SFM か EMS モードの選択メニューが表示されるので、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。但し SFM がインストールされていない場合、モード選択メニューを表示せず EMS モードでインストールを行います。

```
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
```

【中略：インストールプログラムのメッセージ】

【R3.5 以降の場合、以下のモード選択が表示されます。SFM が必須の機種では必ず 1 を選択してください。】
*** select SFM/EMS mode.
1. SFM mode
2. EMS mode

Enter selection:[1] 1　　←メニュー番号を入力

【中略】

[press return to continue]

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 により以下の設定を変更し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。

4.4.3. 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。
※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 は、EMS を選択しないで下さい。

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
```

4.4.4. 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、” [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。

4.4.5. 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ないます。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: 2010/12/31
License flag: 0000000000
codeID is OK.

All install programs are successfully completed.
```

4.4.6. 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。登録を行なわない場合は、任意の IP アドレスからの接続を受け付けます。

監視に使用する IP アドレスが複数ある場合は、すべてを登録するようにしてください。

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。

4.4.7. 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、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。

4.4.8. 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
syslog	ARCHIVE_SYSLOG	YES： 採取する(デフォルト値) NO ： 採取しない
dmesg の結果	ARCHIVE_DMESG	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/停止

Managerの起動及び停止はサービスで行うため、予めサービスを登録しておく必要があります。
起動方法には、以下の２通りがありますが、通常運用では、”PC 起動に連動した自動プログラム起動”を推奨します。

[ＰＣ起動に連動した自動プログラム起動を行う場合(推奨)]
- PC起動に連動してサービスが自動的に開始し、これによりManagerが起動する方法です。[サービス]の[スタートアップ]の起動方法を[自動]に設定しておく必要があります。

[ユーザが任意の時点でプログラム起動を行う場合]
- サービスを手動で開始させることにより、Managerが起動する方法です。[サービス]の[スタートアップ]の起動方法を[手動]に設定しておく必要があります。

また、停止方法には、以下の２通りがありますが、通常運用では、”PC シャットダウンに連動した自動プログラム停止”を推奨します。

[ＰＣシャットダウンに連動した自動プログラム停止を行う場合(推奨)]
- PCのシャットダウンに連動してサービスが自動的に停止し、Managerが停止する方法です。

[ユーザが任意の時点でプログラム停止を行う場合]
- サービスを手動で停止させることにより、Managerを停止させる方法です。

サービスの登録/削除及び手動でManagerの起動/停止(サービスの開始/停止)を行う場合、Administratorsの権限が必要になります。Administratorsの権限があるユーザでログインしてから行ってください。

本ソフトは、本ソフトのアンインストール、バージョンアップを実行する目的以外には終了させないでください。これらの作業を行う場合のみ、"ユーザが任意の時点でプログラム停止を行う場合"にて本ソフトを停止し、作業実施後はすみやかにPCの再立ち上げを実行し本ソフトを起動してください。また、サービスの登録、削除、開始、停止を行なう際は、リモートデスクトップは使用せずに監視サーバを直接、操作してください。

本ソフト停止中は障害監視及び通報機能が停止します。停止中に障害が発生した場合、障害検出できませんので、ご留意ください。

以下にサービスの登録、削除、開始、停止の手順を示しますので、手順にしたがって行ってください。

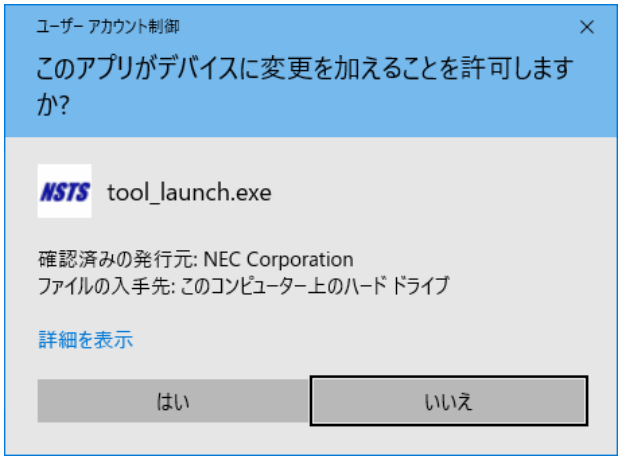
5.1.1. 設定ツールの起動

サービスの操作は、設定ツールから行います。
次の手順で設定ツールを起動してください。

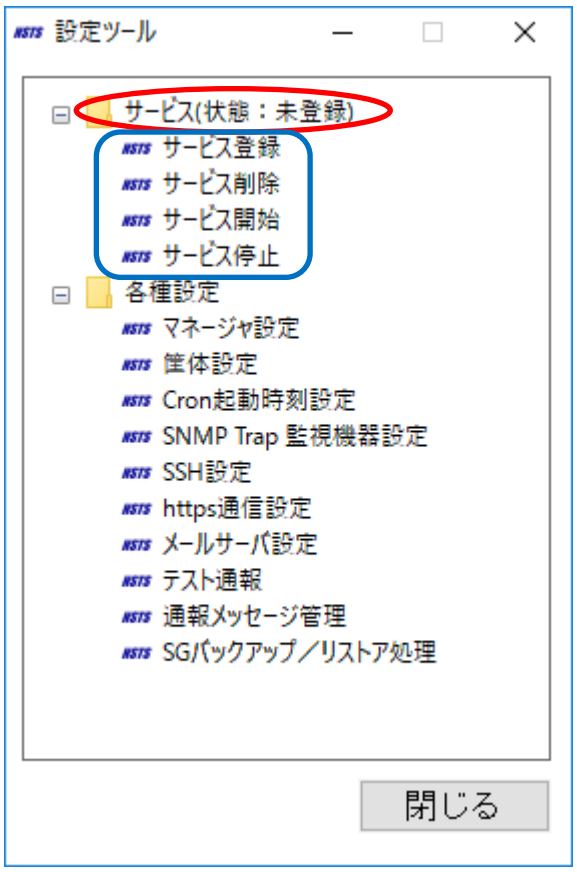
(1) Windows Server2008／2008 R2／2016 の場合
[スタート]→[プログラム]→[NEC Service Terminal Server]→[設定ツール]を選択します。

(2) Windows Server 2012 R2 の場合
- キーボードの「Windows ロゴ」キーを押下するか、デスクトップ画面で左下隅の「Windows ロゴ」をクリックしてスタートメニューを表示します。
- スタートメニューにおいて左下隅の下向きの矢印をクリックし、すべてのアプリケーションを表示させます。
- 一覧から NEC Service Terminal Server の 設定ツールを選択します。

ユーザアカウント制御ダイアログが表示された場合は、[はい]ボタンをクリックしてください。

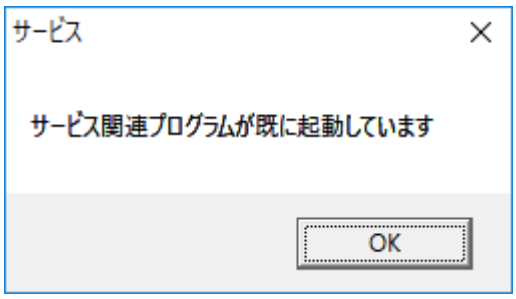


設定ツールが起動します。



サービスは、青枠で囲った箇所を選択して操作します。
図中の赤丸の部分に現在のサービスの状態が表示されます。

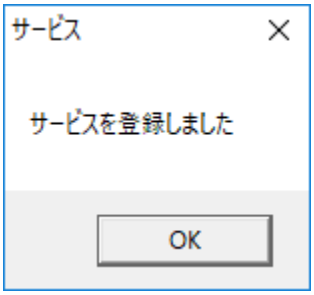
サービスの操作を行うと、操作に対するダイアログがポップアップされます。
このダイアログを消さずに他のサービスに関する操作を行うと下記のエラーダイアログが表示されます。

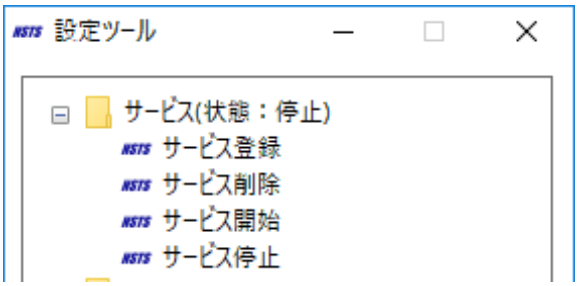


このダイアログが表示された場合は、サービス操作に対するダイアログが表示されていないか、確認してください。

5.1.2. サービスの登録

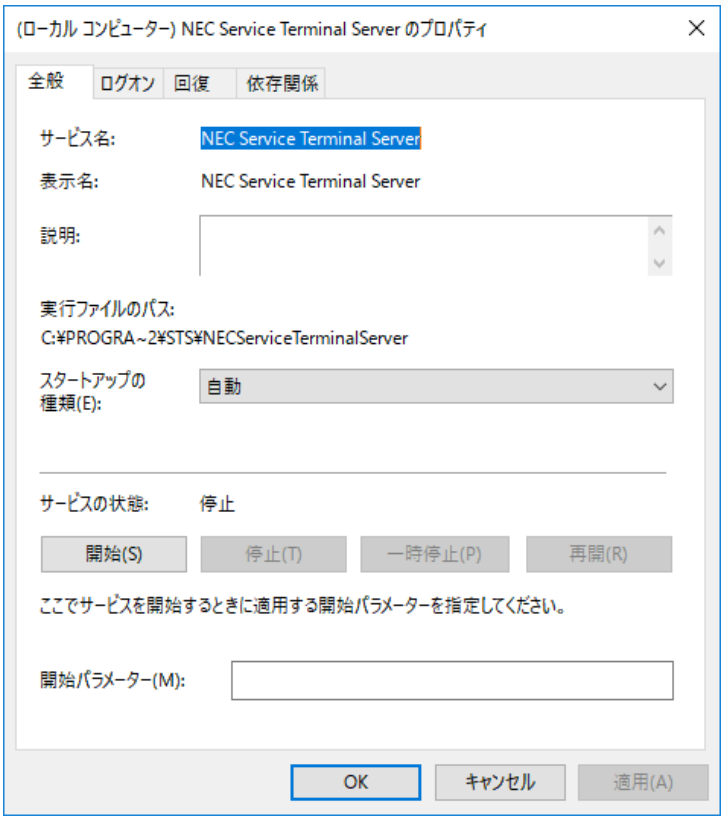
設定ツール画面のサービス状態の表示が「未登録」であることを確認してください。
設定ツール画面にて[サービス]から[サービス登録]を選択してください。サービスの登録処理が動作します。
サービスが登録されると以下のダイアログが表示され、設定ツール画面のサービスの状態表示が、「停止」になります。





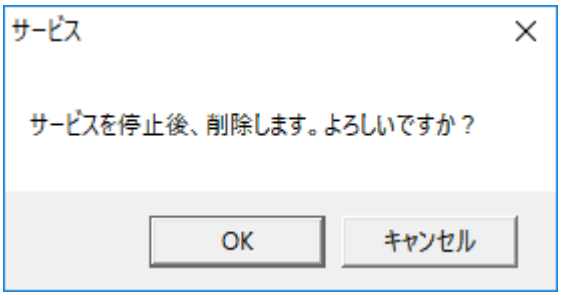
登録されたサービスの設定内容は以下の通りです。
サービス名　NEC Service Terminal Server
スタートアップの種類　自動

スタートアップの種類は、PC の起動と連動してサービスが自動起動する[自動]を推奨します。([コントロールパネル]→[管理ツール]→[サービス]でサービス制御ツールが立ち上がります。「NEC Service Terminal Server」を選択し、右ボタンでプロパティを選択すると下図が表示されます)

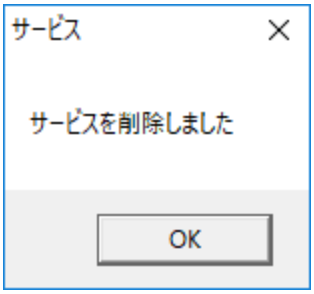


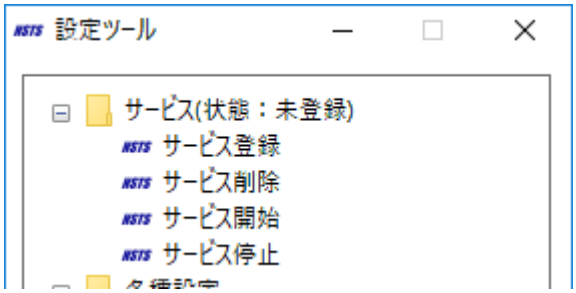
5.1.3. サービスの削除

設定ツール画面のサービス状態の表示が「停止」または「実行中」であることを確認してください。
設定ツール画面にて[サービス]から[サービス削除]を選択してください。サービスの削除処理が動作します。サービスの削除処理が動作すると、以下のダイアログが表示されます。削除を行う場合は、[OK]をクリックしてください。削除を取り消す場合は、[キャンセル]をクリックしてください。



サービスが削除されると以下のダイアログが表示され、設定ツール画面のサービスの状態表示が、「未登録」になります。





5.1.4. サービスの開始

(1) [スタート]→[プログラム]からのサービス開始方法

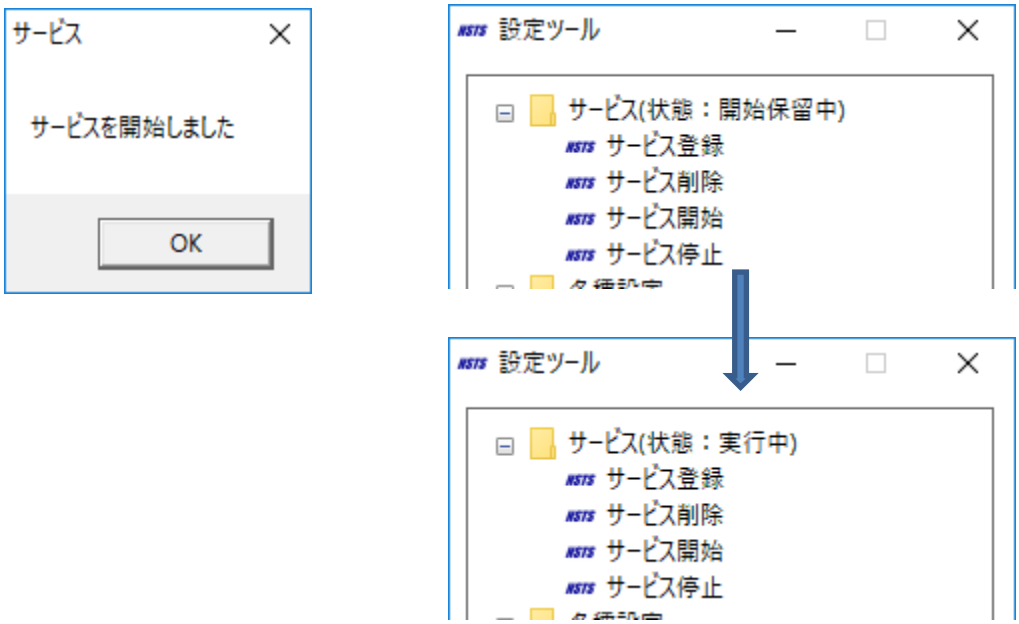
設定ツール画面のサービス状態の表示が「停止」であることを確認してください。

設定ツール画面にて[サービス]から[サービス開始]を選択してください。サービスの開始処理が動作します。

サービスが開始すると以下のダイアログが表示され、設定ツール画面のサービスの状態表示が、「開始保留中」を経て「実行中」になります。

「開始保留中」状態は、NX リモート通報の監視処理の準備中です。この状態のときは、他の操作はできません。

環境や設定に問題が無ければ、30 秒ほどで「実行中」に遷移します。



起動に失敗した場合は、「停止」に戻ります。

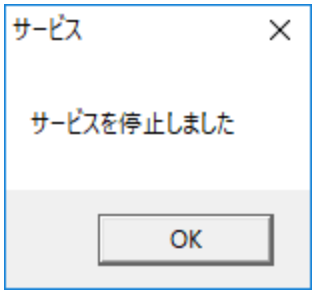
(2)管理ツールからのサービス開始方法

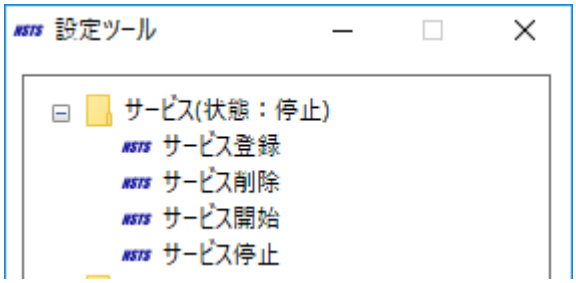
［コントロールパネル］→［管理ツール］から［サービス］を選択し起動してください。サービスの一覧が表示されますので、サービス NEC Service Terminal Server を選択し開始させてください。開始すると状態欄に[開始]が表示されます。

5.1.5. サービスの停止

(1) [スタート]→[プログラム]からのサービス停止方法

設定ツール画面のサービス状態の表示が「実行中」であることを確認してください。設定ツール画面にて[サービス]から[サービス停止]を選択してください。サービスの停止処理が動作します。サービスが停止すると以下のダイアログが表示され、設定ツール画面のサービスの状態表示が、「停止」になります。





(2)管理ツールからのサービス停止方法

［コントロールパネル］→［管理ツール］から［サービス］を選択し起動してください。サービスの一覧が表示されますので、サービス NEC Service Terminal Server を選択し停止させてください。停止すると状態欄から[開始]の文字が消えます。

5.1.6. サービスの設定内容の確認及び/変更方法

サービスの設定内容や稼動状態の確認、設定内容の変更を行う場合は、［管理ツール］の［サービス］で行うことができます。サービスの起動方法（自動/手動）を変更する場合は、以下の手順で行ってください。

(1)［コントロールパネル］→［管理ツール］から［サービス］を選択し起動してください。

(2)サービスの一覧が表示されますので、サービス NEC Service Terminal Server を選択し、設定内容や稼動状態の確認、設定内容の変更をしてください。

6 テスト通報

6.1. テスト通報

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。

なお、テスト通報における「アラーム通報先」とは、

設定ツール → 通報メッセージ管理 → [ユーザ宛通報メッセージ]タブ
番号： 100008
通報メッセージ：test message for sts setup.

に設定されたレポートアドレスを指します。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。編集方法は、7.2.1 章(2)③および④ を参照してください。

保守センタ宛の通報に https を選択しても、アラーム通報先に対しては、e-mail で通報されます。

(1) 監視サーバからテストを行う。(Manager テスト通報)
監視サーバと保守センター（NEC フィールディング）間の導通確認を行います。Manager から保守センターとユーザ定義辞書に設定されている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 フィールディング）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 ログ採取用 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通報されます。アラーム通報先には通報されません。

(注1) ユーザ定義辞書の「test message for sts setup.」のレポートアドレスが "dummy@com"(デフォルト値)の場合は、アラーム通報先へは通報されません。

(注2) https を使用する設定の場合は、保守センターへの通報は、https 通信を用いて行なわれます。

(注3) 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テスト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 ソフトを停止します。
＊ スレーブ側の Manager ソフトを起動します。マスタが起動していないため、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

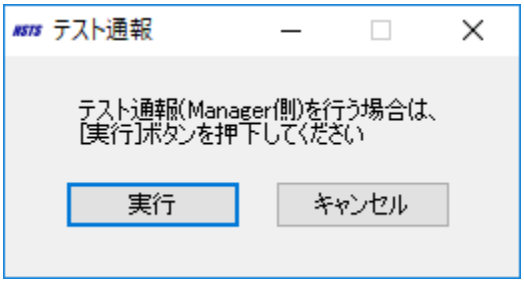
Manager 側のテスト通報はツールを用いて行います。

テスト通報のメールは保守センターとユーザ定義辞書に設定されているアラーム通報先に通報されます。

（1） ツールの起動方法

設定ツール画面にて[各種設定]→[テスト通報]を選択すると、テスト通報画面が表示されます。

（2） 指示画面と指示内容



ボタン名	機能
実行	Manager 側のテスト通報を行います。
キャンセル	テスト通報を行わず、本画面を閉じます。

（3） 通報結果の確認

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、（4）および（5）をご確認ください。

メール送信および https 通信できなかった通報データは、
C:¥Program Files (x86)¥STS¥tmp¥failed.mail*.*.*
にファイル出力され残ります (C:¥Program Files (x86)¥STS の部分はインストールしたディレクトリであり、この限りではありません)。このファイルは、次回にメール送信および https 通信が正常に行われた場合に再送信された後、削除されます。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去されます。

（4） 保守センターおよびアラーム通報先に通報状況の確認

保守センターおよびアラーム通報先に通報されない場合は、メール送信および https 通信の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、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 ディレクトリ配下に作成されます（通常は C:¥Program Files (x86)¥STS¥log)。なお、https 通信の場合も同じファイルに出力されます。

・メール送信が成功した場合

「result: succeeded in sending email.」と出力されている場合は正常です。

・メール送信に失敗した場合
「result: failed to send email.」と出力されている場合は異常です。
※メール送信が異常であった場合の詳細は(５)を参照してください。

・https 通信が成功した場合
「https_report_main() End(0)」と出力されている場合は正常です。

・https 通信が失敗した場合
「https_report_main() End(1)」と出力されている場合は異常です。
※https 通信が異常であった場合の詳細は(５)を参照してください。

（５） 保守センターおよびアラーム通報先に通報されない原因の確認
メール送信および https 通信で異常となった場合は、以下の内容がログに出力されていないか確認し、原因を確認してください。

・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

・ メールサーバでの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 PDMyMzAwMjMzMjcuMTEzNjk2MzQ2NUBtYWlsLmpwLm5lYy5jb20+
MDAwMaAxMtEy1jg3NiA3ZTFmYzcxZjZhOWY1NTI1YwRiZjk2NjQyzDcxYjc4
ZQ==
501 Unauthorized

・ メール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

・ https 通信が End(1)で失敗した場合、以下のようなエラーをログに出力します。
ERROR：CreateFile failed!
ERROR：write_read_thread returned
プロキシサーバの設定に問題がないか確認してください。問題ない場合は、サーバ側の問題または、一時的な失敗の可能性が高いので、時間を置いて再度実行してください。

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 4.4 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ユーザ定義辞書に設定されている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。

テスト通報結果の確認方法は、6.1.1（３）と同じです。

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 4.4 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ユーザ定義辞書に設定されている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。

テスト通報結果の確認方法は、6.1.1（３）と同じです。

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。PC 上でコマンドプロンプト(cmd.exe)を起動して、以下のようにコマンドを実行してください。

```
> cd “C:¥Program Files (x86)¥STS¥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ユーザ定義辞書に設定されている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。

テスト通報結果の確認方法は、6.1.1（3）と同じです。

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 4.4 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。

テスト通報結果の確認方法は、6.1.1（3）と同じです。

【通報されない場合】"7020M-16/7040M-32/7080H-64/8020M-32/8040M-64/8080H-128"

は、除く。

- 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
```

テスト通報結果の確認方法は、6.1.1（3）と同じです。

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 のコマンドに関しての詳細は、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。

監視サーバにおいて Windows のコマンドプロンプトを起動して、Manager ソフトをインストールしたディレクトリ（通常は C:¥Program Files (x86)¥STS）配下の sts ディレクトリに移動します。

```
>cd “C:¥Program Files (x86)¥STS¥sts”
```

通常監視モードからテストモードへは、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 の簡単な使用方法は、-h オプション付きで実行すると表示されます。

```
> repctrl_test_bmc.exe -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。

テスト通報結果の確認方法は、6.1.1（３）と同じです。

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 テストモードの終了
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 の簡単な使用方法は、-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

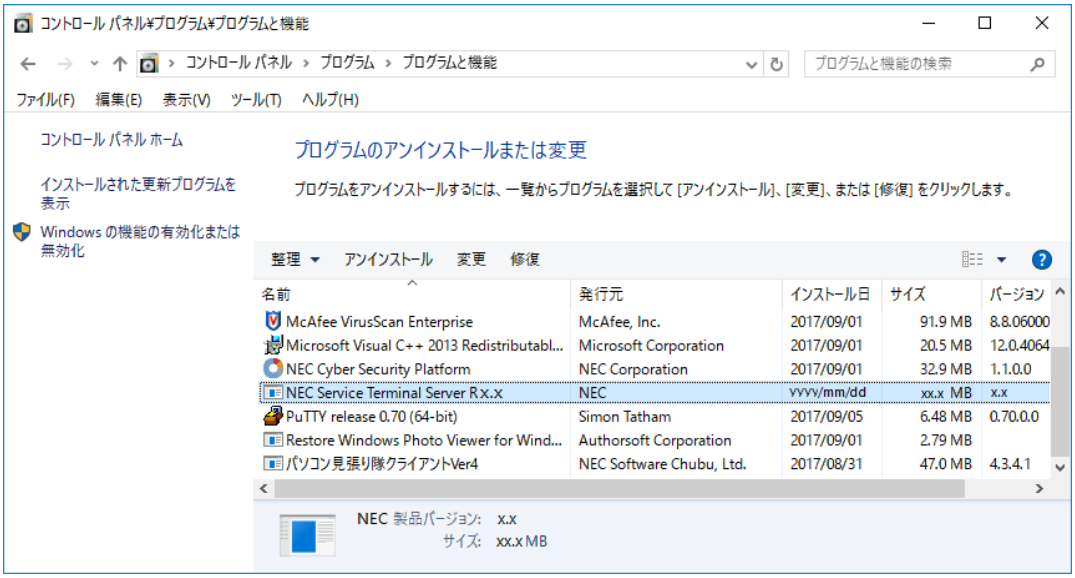
7.1.1. Manager ソフトのアンインストール

以下の手順にしたがって、監視サーバ用の Manager ソフトをアンインストールしてください。なお、以下の画面は Windows Server 2016 で操作したときの画面になります。

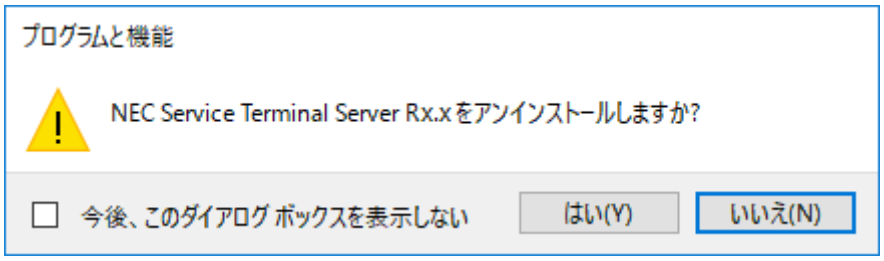
(1) Administrators の権限をもつアカウントでログインします。

(2) Manager ソフトを停止（5.1.5 章を参照）後、サービスを削除（5.1.3 章を参照）します。

(3) Windows の[コントロールパネル] →[プログラム]→[プログラムと機能] により、アンインストールするソフトウェア NEC Service Terminal Server Rx.x を選択し、[削除]ボタンをクリックしてください。



(4) 以下のダイアログボックスが表示されますので、アンインストールする場合は、[はい]ボタンをクリックしてください。アンインストールを中断する場合は、[いいえ]ボタンをクリックしてください。



(5) アンインストールが完了すると、Windows の［コントロールパネル］の［プログラムと機能］上から、NEC Service Terminal Server Rx.x の表示がなくなります。
もし、Windows の再起動のダイアログボックスが表示された場合は、Windows を再起動してください。

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 # NX remote communicator agent

(7) /etc/inetd.conf より以下の行を削除

NX remote communicator agent
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

注意：上記の行を削除すると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、削除は不要です。

(10)　EMS の設定変更

(R3.0 以前、または R3.1 以降のインストール時に EMS モードを選択した場合)

```
# /etc/opt/resmon/lbin/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

ここでは、NX リモート通報のメンテナンス機能について説明します。

7.2.1. 通報メッセージ情報（辞書）の編集方法

通報メッセージ情報として設定するのは、通報許可レベル、追加登録の通報メッセージです。共に設定ツールを用いて設定します。その他に既登録済みの通報メッセージの登録内容の確認や設定内容の変更も本設定ツールで行うことができます。

設定内容は次回 Manager ソフトが起動時に反映されます。Manager ソフトが起動中に設定を変更した場合は、サービスを再起動してください。

(1) ツールの起動方法

設定ツール画面にて[各種設定]→[通報メッセージ管理]を選択すると、通報メッセージ管理画面が表示されます。

(2) 設定画面と設定内容

設定ツールが起動すると本画面が表示されます。本画面以外にもいくつかの設定画面があります。画面毎に項目及びボタンの説明を示しますので、下記を参照してください。

① 通報メッセージ管理　トップ画面－保守センター宛通報メッセージ

本画面では以下の事項を行うことができます。

- 通報許可レベル設定
- 定義済みの通報メッセージの設定内容確認
  (通報メッセージ種別及びユーザ宛通報メッセージへの切り替え含む)
- 定義済みの通報メッセージに対する通報許可設定

・ 保守員設定の通報メッセージの追加登録/更新/削除指示
追加登録できる通報メッセージは最大 128 件です。

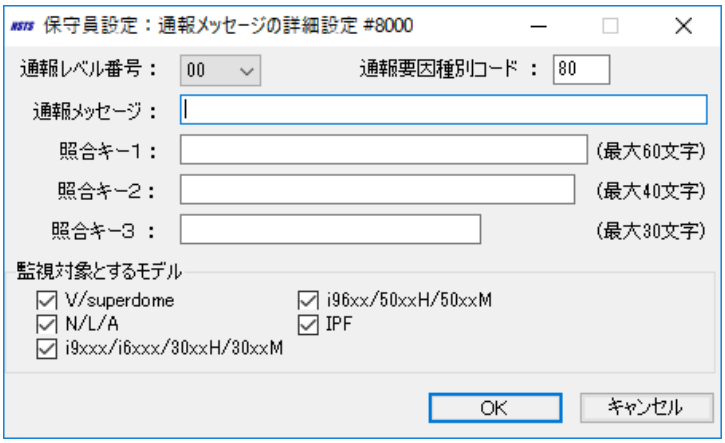
－注意事項－
保守センター宛通報メッセージの編集は保守センターとの同期が必要です。
従って、編集操作は保守員のみが行ってください。

表示/設定項目			表示/設定内容
OS Select		任意	現在表示されている定義済みの通報メッセージの種別が表示されます。ドロップダウンリストに OS 種別が表示されます。通報メッセージに切り替える場合は、表示したい OS 種別を選択してください。 尚、SP 検出の通報メッセージは OS 検出の通報メッセージの後に続けて表示されます。 【デフォルト値】"HP-UX"
定義済みの通報メッセージリスト	番号	－	通報メッセージのメッセージ番号が表示されます。
	通報許可	必須	通報メッセージの通報許可が表示されます。設定内容を変更する場合は、変更対象の通報許可に位置づけクリックし、"○"→"×"または"×"→"○"に変更してください。 "○"印：通報対象　"×"印：通報対象外
	通報レベル	－	通報メッセージの通報レベルが表示されます。項目の内容は 7.3 項を参照してください。
	通報要因	－	通報メッセージの通報要因が表示されます。項目の内容は 7.3 項を参照してください。
	モデル	－	通報メッセージの監視対象モデルの略称が表示されます。 モデルと略称の対応は 7.3 項を参照してください。
	通報メッセージ	－	通報時に送られるメッセージが表示されます。
	全登録件数	－	通報メッセージの総登録件数が表示されます。
保守員設定の通報メッセージリスト	番号	－	新規登録した通報メッセージのメッセージ番号が表示されます。新規登録した通報メッセージが存在しない場合は表示されません。
	通報許可	必須	新規登録した通報メッセージの通報許可が表示されます。設定内容を変更する場合は、変更対象の通報許可に位置づけクリックし、"○"→"×"または"×"→"○"に変更してください。 "○"印：通報対象　"×"印：通報対象外 新規登録した通報メッセージが存在しない場合本リストは表示されません。
	通報レベル	－	新規登録した通報メッセージの通報レベルが表示されます。 新規登録した通報メッセージが存在しない場合本リストは表示されません。項目の内容は 7.3 項を参照してください。
	通報要因	－	新規登録した通報メッセージの通報要因が表示されます。 新規登録した通報メッセージが存在しない場合本リストは表示されません。項目の内容は 7.3 項を参照してください。
	モデル	－	新規登録した通報メッセージの監視対象モデルの略称が表示されます。モデルと略称の対応は 7.3 項を参照してください。

			新規登録した通報メッセージが存在しない場合本リストは表示されません。
	通報メッセージ	ー	通報時に送られるメッセージが表示されます。 新規登録した通報メッセージが存在しない場合本リストは表示されません。
	全登録件数	ー	新規登録した通報メッセージの総登録件数が表示されます。
通報許可レベル		必須	通報許可レベルで通報を抑止します。現在の設定レベルが表示されます。ドロップダウンリストに通報許可レベルが表示されます。他の通報許可レベルに切り替える場合は、変更後の通報許可レベルを選択してください。 通報許可レベルに関する詳細は 7.3 項を参照してください。 【デフォルト値】"全レベル許可"
辞書ファイルセット Version		ー	通報メッセージの辞書ファイルのバージョンが表示されます。

ボタン名	機能
保守センター宛通報メッセージ　タブ	タブの上部をクリックすると、保守センター宛通報メッセージが表示さます。
ユーザ宛通報メッセージ　タブ	タブの上部をクリックすると、ユーザ宛通報メッセージが表示さます。使用できません。
新規追加	保守員設定の通報メッセージを新規登録するために、詳細設定画面を表示させます。
削除	新規登録した保守員設定の通報メッセージを削除します。
編集	新規登録した保守員設定の通報メッセージの設定内容を更新するために、詳細設定画面を表示させます。
コピー	NCM（NEC Console Manager）がインストール済みの場合、NCM で設定したメッセージ情報をコピーします。本機能は 50xxH/50xxM のみで有効です。
設定保存	設定内容が更新されている場合は更新を行うか否かの確認画面が表示されます。更新を指示した場合は、更新後、Manager ソフトが稼動中で即時変更内容が反映できる場合は反映させ、本画面を閉じます。Manager ソフトが停止中の場合は次回 Manager ソフトが起動時に変更内容を反映させます。
終了	設定内容が更新されている場合は更新を行うか否かの確認画面が表示されます。更新を指示した場合は、更新後、Manager ソフトが稼動中で即時変更内容が反映できる場合は反映させ、本画面を閉じます。Manager ソフトが停止中の場合は次回 Manager ソフトが起動時に変更内容を反映させます。

② 保守員設定　通報メッセージの詳細設定画面
本画面では以下の事項を行うことができます。
・ 保守員設定の通報メッセージの詳細内容設定/更新



表示/設定項目		表示/設定内容
ウィンドウタイトル	―	画面名の右横に当該通報メッセージのメッセージ番号を表示します。"＃"の後ろの数値がメッセージ番号になります。
通報レベル番号	必須	通報レベルを設定してください。ドロップダウンリストに通報レベル番号が表示されます。該当する通報レベル番号を選択してください。項目の内容は 7.3 項を参照してください。 【デフォルト値】"00"
通報要因種別コード	必須	通報要因種別コードを設定してください。項目の内容は 7.3 項を参照してください。 【デフォルト値】"80"
通報メッセージ	任意	通報時に使用する障害内容の概要を示すメッセージを設定してください。このメッセージは障害内容が一意に判別できるものを設定することを推奨します。 【入力条件】 半角英数字。最大 72 文字まで。
照合キー1	必須 照合キー1～3いずれか必ず設定のこと	コンソールの出力メッセージが通報要因かどうかを識別するためのキー文字列を設定してください。照合キー1～3 の全てのキー文字列が一致した時、通報要因とみなします。 【入力条件】 半角英数字。最大 60 文字まで。スペースのみは不可。
照合キー2		コンソールの出力メッセージが通報要因かどうかを識別するためのキー文字列を設定してください。照合キー1～3 の全てのキー文字列が一致した時、通報要因とみなします。 【入力条件】 半角英数字。最大 40 文字まで。スペースのみは不可。
照合キー3		コンソールの出力メッセージが通報要因かどうかを識別するためのキー文字列を設定してください。照合キー1～3 の全てのキー文字列が一致した時、通報要因とみなします。 【入力条件】 半角英数字。最大 30 文字まで。スペースのみは不可。
監視対象とするモデル	必須	モデルの略称が表示されています。通報メッセージの監視対象モデルを設定してください。監視対象モデルに設定する場合はチェック

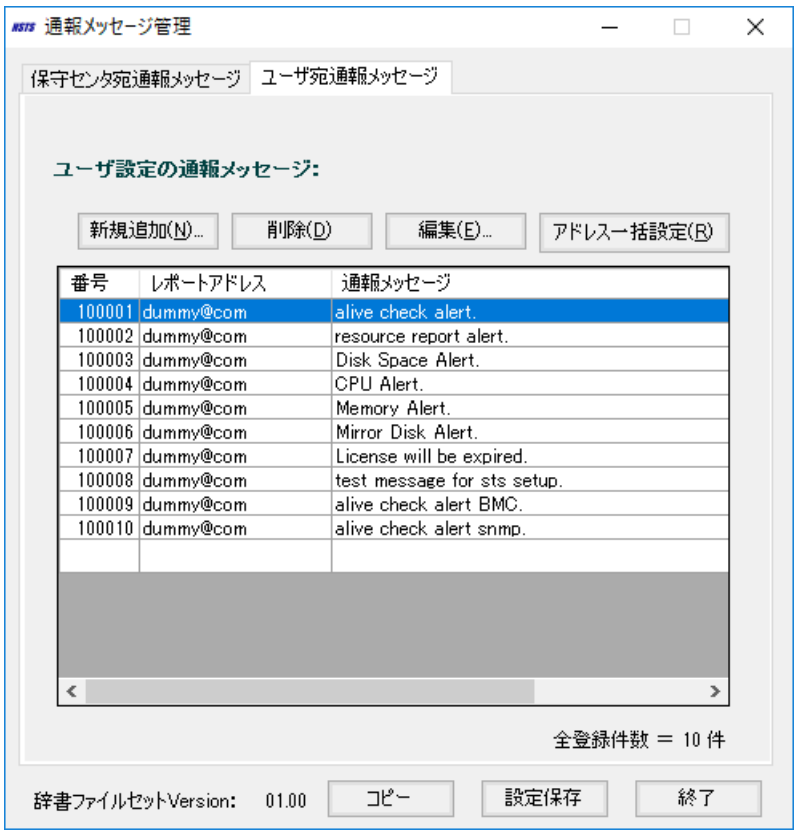
		ボックスにチェック(レ印)してください。未チェックの場合、その通報メッセージは監視対象外とみなします。 モデルの略称については、7.3 項を参照してください。 【デフォルト値】全モデル監視対象 (チェックボックスにチェック(レ印)あり)

ボタン名	機能
ＯＫ	設定内容を登録後、本画面を閉じます。
キャンセル	設定内容を登録せずに、本画面を閉じます。

③ 通報メッセージ管理　トップ画面－ユーザ宛通報メッセージ
本画面では以下の次項を行うことができます。

- 定義済みの通報メッセージの設定内容確認
  (保守センター宛通報メッセージへの切り替え含む)
- 定義済みの通報メッセージに対するメールアドレス設定
  (通報メッセージ毎または一括のメールアドレス設定)
- ユーザ設定の通報メッセージの追加登録/更新/削除指示

定義済みの通報メッセージと追加登録した通報メッセージの判別はメッセージ番号で行います。メッセージ番号"100001"～"100050"は定義済みの通報メッセージ、メッセージ番号"100051"以降は追加登録した通報メッセージになります。
両者を合わせ最大 128 件の通報メッセージを設定することができます。

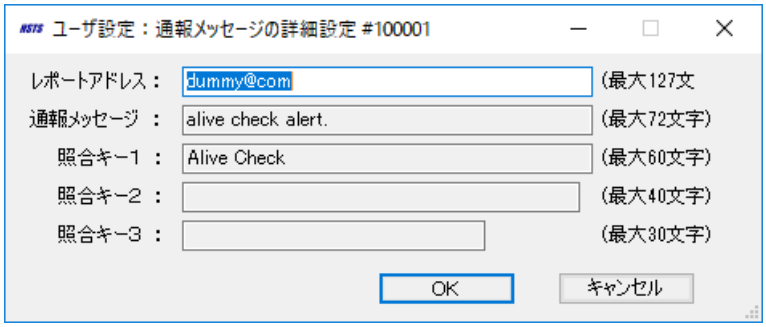


表示/設定項目			表示/設定内容
ユーザ設定の通報メッセージリスト	番号	－	通報メッセージのメッセージ番号が表示されます。
	レポートアドレス	－	通報メッセージの通報先であるレポートアドレスが表示されます。 【デフォルト値】"dummy@com"
	通報メッセージ	－	通報メッセージの通報時に送られるメッセージが表示されます。
	全登録件数	－	ユーザ宛通報メッセージの総登録件数が表示されます。既定義の通報メッセージと新規登録の通報メッセージの総件数です。
辞書ファイルセット Version		－	通報メッセージの辞書ファイルのバージョンが表示されます。

ボタン名	機能
保守センター宛通報メッセージ　タブ	タブの上部をクリックすると、保守センター宛通報メッセージが表示さます。
ユーザ宛通報メッセージ　タブ	タブの上部をクリックすると、ユーザ宛通報メッセージが表示さます。
新規追加	ユーザ設定の通報メッセージを新規登録するために、詳細設定画面を表示させます。
削除	新規登録したユーザ設定の通報メッセージを削除します。
編集	新規登録したユーザ設定の通報メッセージの設定内容を更新するために、詳細設定画面を表示させます。
アドレス一括設定	通報先のメールアドレスを一括変更するために、一括設定画面を表示させます。
設定保存	設定内容が更新されている場合は更新を行うか否かの確認画面が表示されます。更新を指示した場合は、更新後、Manager ソフトが稼動中で即時変更内容が反映できる場合は反映させ、本画面を閉じます。Manager ソフトが停止中の場合は次回 Manager ソフトが起動時に変更内容を反映させます。 尚、通報先のメールアドレスに"dummy@com″が設定されている場合は設定の可否を確認する画面が表示されます。
終了	設定内容が更新されている場合は更新を行うか否かの確認画面が表示されます。更新を指示した場合は、更新後、Manager ソフトが稼動中で即時変更内容が反映できる場合は反映させ、本画面を閉じます。Manager ソフトが停止中の場合は次回 Manager ソフトが起動時に変更内容を反映させます。 尚、通報先のメールアドレスに"dummy@com″が設定されている場合は設定の可否を確認する画面が表示されます。

④ ユーザ設定　通報メッセージの詳細設定画面
本画面では以下の次項を行うことができます。
・ 定義済みの通報メッセージに対するメールアドレス設定
・ ユーザ設定の通報メッセージの詳細内容設定/更新

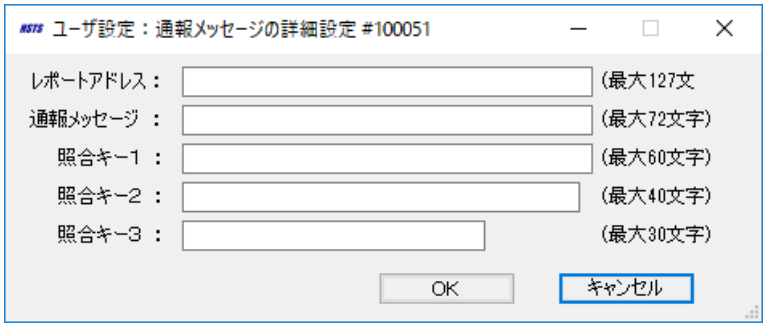
－定義済みの通報メッセージの詳細設定画面の場合
(メッセージ番号"100001"～"100050")－



表示/設定項目		表示/設定内容
ウィンドウタイトル	－	画面名の右横に当該通報メッセージのメッセージ番号を表示します。"＃"の後ろの数値がメッセージ番号になります。
レポートアドレス	必須	メールアドレスを設定してください。複数のメールアドレスを設定する場合は","(カンマ)で続けて設定してください。 【デフォルト値】"dummy@com" 【入力条件】 半角英数字。最大 127 文字まで。"<"," >"(カッコ)は入力できません。 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。
通報メッセージ	－	当該通報メッセージが表示されます。変更はできません。
照合キー1	－	当該通報メッセージの照合キー1 が表示されます。変更はできません。
照合キー2	－	当該通報メッセージの照合キー2 が表示されます。変更はできません。
照合キー3	－	当該通報メッセージの照合キー3 が表示されます。変更はできません。

ボタン名	機能
ＯＫ	設定内容を登録後、本画面を閉じます。
キャンセル	設定内容を登録せずに、本画面を閉じます。

－ユーザ設定の通報メッセージの詳細設定画面の場合
(メッセージ番号"100051"以降)－



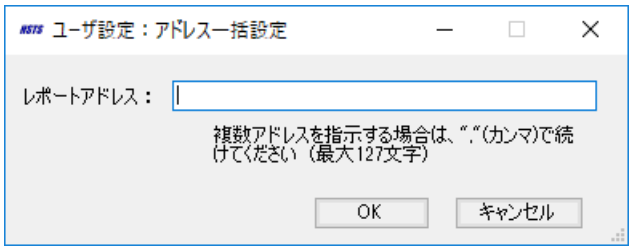
表示/設定項目		表示/設定内容
ウィンドウタイトル	－	画面名の右横に当該通報メッセージのメッセージ番号を表示します。"＃"の後ろの数値がメッセージ番号になります。
レポートアドレス	必須	メールアドレスを設定してください。複数のメールアドレスを設定する場合は","(カンマ)で続けて設定してください。 【入力条件】 半角英数字。最大 127 文字まで。"<",">"(カッコ)は入力できません。 なお、当該通報メッセージを通報しない場合、レポートアドレスへ空白を設定せずに"dummy@com"を入力してください。
通報メッセージ	任意	通報時に使用する障害内容の概要を示すメッセージを設定してください。このメッセージは障害内容が一意に判別できるものを設定することを推奨します。 【入力条件】 半角英数字。最大 72 文字まで。"<",">"(カッコ)は入力できません。
照合キー1	必須 照合キー1～3いずれか必ず設定のこと	コンソールの出力メッセージが通報要因かどうかを識別するためのキー文字列を設定してください。照合キー1～3 の全てのキー文字列が一致した時、通報要因とみなします。 【入力条件】 半角英数字。最大 60 文字まで。スペースのみは不可。"<",">"(カッコ)は入力できません。
照合キー2		コンソールの出力メッセージが通報要因かどうかを識別するためのキー文字列を設定してください。照合キー1～3 の全てのキー文字列が一致した時、通報要因とみなします。 【入力条件】 半角英数字。最大 40 文字まで。スペースのみは不可。"<",">"(カッコ)は入力できません。
照合キー3		コンソールの出力メッセージが通報要因かどうかを識別するためのキー文字列を設定してください。照合キー1～3 の全てのキー文字列が一致した時、通報要因とみなします。 【入力条件】 半角英数字。最大 30 文字まで。スペースのみは不可。"<",">"(カッコ)は入力できません。

ボタン名	機能
ＯＫ	設定内容を登録後、本画面を閉じます。
キャンセル	設定内容を登録せずに、本画面を閉じます。

⑤ ユーザ設定　アドレス一括設定画面

本画面では以下の次項を行うことができます。

・ 定義済み及び追加登録のユーザ宛通報メッセージの一括メールアドレス設定



表示/設定項目		表示/設定内容
レポートアドレス	必須	メールアドレスを設定してください。複数のメールアドレスを設定する場合は","(カンマ)で続けて設定してください。 【入力条件】 半角英数字。最大 127 文字まで。"<","<"(カッコ)は入力できません。 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。

ボタン名	機能
ＯＫ	設定内容を登録後、本画面を閉じます。"dummy@com″が設定されている場合は設定の可否を確認する画面が表示されます。
キャンセル	設定内容を登録せずに、本画面を閉じます。

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: 2012/7/1               <=== 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. 障害通報の一時抑止方法

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。監視制御ツール(repctrl)による抑止機能は、SNMP Trap による通報には作用しません。

(1) 実行環境

監視制御ツールは、監視サーバにおいて、Manager ソフトをインストールしたディレクトリ（通常は C:¥Program Files (x86)¥STS）配下の sts ディレクトリ下で動作します。

Windows のコマンドプロンプトを起動して、ディレクトリを移動します。

```
>cd “C:¥Program Files (x86)¥STS¥sts”
```

監視制御ツールの簡単な使用方法は、-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、現在の状態を表示します。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：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 番のサーバは監視中、2 番のサーバは指定された日時まで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

7.2.5. 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。

7.2.6. 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。

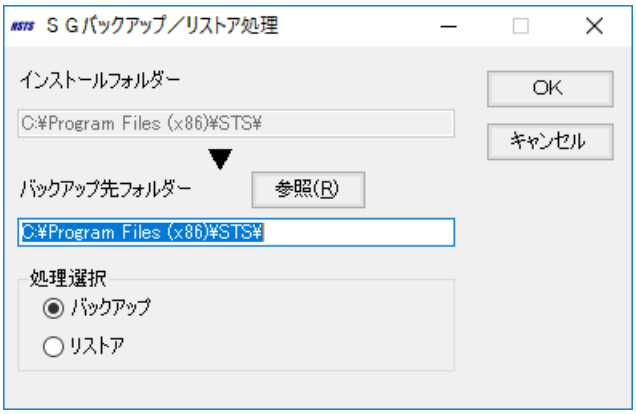
7.2.7. 辞書/SG ファイルのバックアップ/リストア方法

NX リモート通報の辞書/SG ファイルをバックアップ及びリストアすることができます。共にツールを用いて行います。

(1) ツールの起動方法

設定ツール画面にて[各種設定]→[SG バックアップ/リストア処理]を選択すると、SG バックアップ/リストア処理画面が表示されます。

(2) 設定画面と設定内容



表示/設定項目		表示/設定内容
インストールフォルダ	―	NX リモート通報のインストールフォルダが表示されます。 【デフォルト値】 (システムドライブ)¥Program Files (x86)¥STS¥ ※上図は 64 ビット版 OS へインストールした場合の設定例です。
バックアップ先フォルダ	必須	辞書/SG ファイルの一時的な格納場所を設定してください。
処理選択	必須	オプションボタンにチェック(●印)してください。オプションボタンをバックアップにチェックすると、上記画面のように「インストールフォルダ」、「バックアップ先フォルダ」の順に表示されます。リストアにチェックすると、「インストールフォルダ」と「バックアップ先フォルダ」の表示位置が逆転して表示されます。 【デフォルト値】 バックアップ(オプションボタンにチェック(●印)あり)

ボタン名	機能
参照	フォルダの参照画面が表示されます。この参照画面からバックアップ先フォルダを設定することができます。
ＯＫ	バックアップを指示した場合は設定した格納場所にバックアップを、リストアを指示した場合は設定した格納場所からリストアを開始するために処理開始の確認画面が表示されます。ＯＫボタンを押下することにより処理を開始します。
キャンセル	処理せずに、本画面を閉じます。

[注意事項]
NX リモート通報のパラメータファイル sts_parameter.sg はリストア対象となりません。お客様の運用によりこれらのパラメータを変更してお使いの場合は、バックアップ先フォルダに格納されているパラメータファイル sts_parameter.sg を参照しながら手動で変更してください。
[参照データ(旧バージョンのパラメータファイル)]
バックアップ先フォルダ¥sg¥sts_parameter.sg
[更新対象データ(新バージョンのパラメータファイル)]
(システムドライブ)¥Program Files (x86)¥STS¥sg¥sts_parameter.sg
尚、他のパラメータは変更しないでください。他のパラメータを変更した場合、NX リモート通報が正常動作しなくなることがあります。ご注意ください。

7.2.8. マネージャプログラム起動状況のイベントログ出力

マネージャプログラムが異常終了した場合、異常終了時にメッセージを Windows のイベントログへ出力します。

(1) ログ出力内容

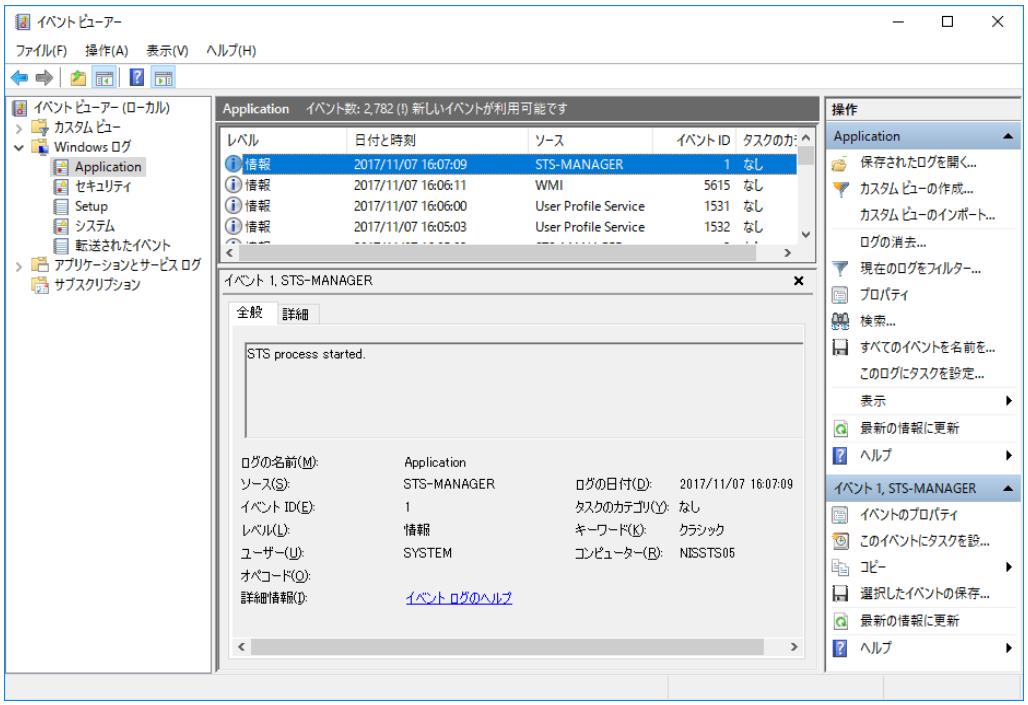
マネージャプログラムが異常終了した場合、異常終了時に Windows のイベントビューアー（[コントロールパネル]→[システムとセキュリティ]→[管理ツール]→[イベント ビューアー]）へ下記内容のメッセージが出力されます。
マネージャプログラム起動時のメッセージは、障害復旧時の確認用に使用してください。もし復旧しない場合は開発元に問い合わせてください。

項目名	設定値
ログの名前	APPLICATION
ソース	STS-MANAGER

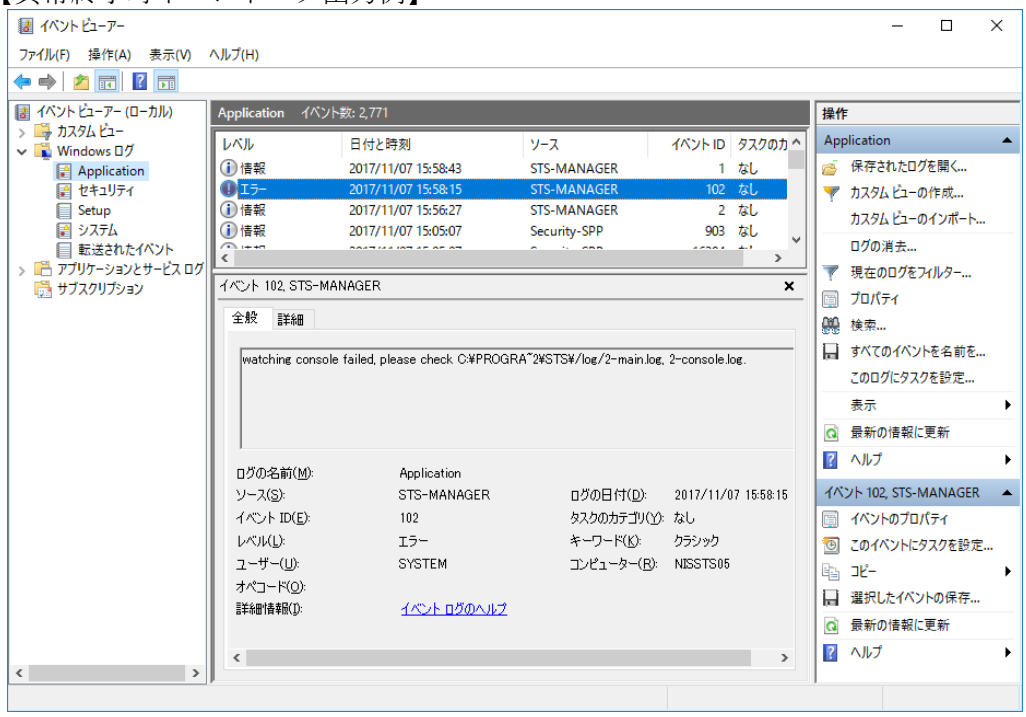
ID	レベル	メッセージ	説明
001	Information	sts process started.	sts プロセスの開始
002	Information	sts process stopped.	sts プロセスの停止
102	Error	watching console failed, please check *log_dir*/*id*-main.log, *id*-console.log.	被監視サーバのコンソールが監視できませんでした。SG 誤りの可能性があります。該当のログファイルを確認してください。
207	Error	Failed to send to manager of service control.	Window の状態が異常になっている可能性があります。OS の再起動を実施してください。
208	Error	Failed to get execute path.	
209	Error	Failed to read parameter file.	
210	Error	Failed to create event.	
211	Error	Failed to allocate memory.	メモリが不足しています。空きメモリを増やしてから再度実行してください。

212	Error	Failed to remove *filename*.	*filename* が削除できませんでした。 *filename* を削除してから再度実行してください。
213	Error	Failed to start process %s.	プロセスの生成に失敗しました。空きメモリを増やして再度実行してください。改善しない場合は OS の再起動を実施してください。
214	Error	Opening of a registry key failed.	Window の状態が異常になっている可能性があります。OS の再起動を実施してください。
215	Error	Reading of data of a registry key failed.	
216	Error	Close of a registry key failed.	
217	Error	Failed to initialize security descriptor.	
218	Error	Failed to set security descriptor.	

【マネージャプログラム起動時イベントログ出力例】



【異常終了時イベントログ出力例】



7.3. 通報メッセージ管理におけるコードの説明

通報メッセージ管理 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。

<table>
<tr><td>項目</td><td colspan="3">説明</td></tr>
<tr><td>通報許可レベル</td><td colspan="3">通報レベルのどのレベル以上のメッセージに対して、通報を行うかを示します。以下の選択肢から選択できます。
「全レベル許可」：全レベルのメッセージの通報を許可にする。
「レベル６以上」：通報レベルが 0～6 のメッセージの通報を許可する
「レベル５以上」：通報レベルが 0～5 のメッセージの通報を許可する
「レベル４以上」：通報レベルが 0～4 のメッセージの通報を許可する
「レベル３以上」：通報レベルが 0～3 のメッセージの通報を許可する
「レベル２以上」：通報レベルが 0～2 のメッセージの通報を許可する
「レベル１以上」：通報レベルが 0～1 のメッセージの通報を許可する
「レベル０」　：通報レベルが 0 のメッセージの通報を許可する
「全レベル不許可」：全レベルのメッセージの通報を不許可にする。

尚、ユーザ宛通報メッセージ、テスト通報の通報メッセージ、定期通報の通報メッセージは本設定の影響は受けません。</td></tr>
<tr><td>通報レベル番号</td><td colspan="3">発生した障害の内容を 0～7 の 8 段階にランク付けしています。リモート保守センターで受信した通報を通報要因別にフィルタリングする場合に使用します。</td></tr>
<tr><td>通報要因種別コード</td><td colspan="3">発生した障害の内容をその要因毎に割り当てた 16 進数 2 桁のコードです。リモート保守センターで受信した通報を通報要因別に分類するために使用します。</td></tr>
<tr><td rowspan="4">モデル略称</td><td colspan="3">モデルと略称の対応は下記の通りです。</td></tr>
<tr><td>通報メッセージ管理画面での表示モデル</td><td>通報メッセージ詳細設定画面での表示モデル</td><td>当該モデル</td></tr>
<tr><td>V</td><td>V/superdome</td><td>NX7000/ rp74xx
rp84xx
Superdome</td></tr>
<tr><td>N/L/A</td><td>N/L/A</td><td>NX7000/ rp24xx
rp34xx
rp44xx
rp54xx
rp74xx
rp84xx</td></tr>
<tr><td>I</td><td>IPF</td><td>NX7700i/i4510
rx7620
rx7640
rx8620
rx8640
301xE-2
301xL-2/4/8
3160H-64
5010B-4
5012B-4
5012B-8
5010E-4
501xL-4/8</td></tr>
</table>

			5160H-128 7010B-8 7010B-16 7010B-32 7010E-8 7020M-16 7040M-32 7080H-64 7320H-256 8010E-16 8010B-16 8020B-32 8040B-64 8020M-32 8040M-64 8080H-128 8160H-256 9010E-16 9160H-256
	W	i9xxx/i6xxx/30xxH/30xxM	NX7700i/3020M-8 3040M-16 3040H-16 3080H-32 TX7/i6010 i6510 i9010 i9510 i-PX9000　A/S モデル （オープンＯＳ搭載機構必須）
	M	i96xx/50xxH/50xxM	Nx7700i/5020M-16 5040H-32 5080H-64 TX7/i9610

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

ユーザ定義辞書は、システム管理者(SE)が定義内容を編集可能な辞書です。

Manager が監視しているコンソール(/dev/console)に、ユーザ定義辞書に登録されている特定の文字列が出力された時、システム管理者にアラーム通報を行います。ユーザ定義辞書にメッセージ文字列を登録することより、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。

ユーザ定義辞書の編集方法については、7.2.1 を参照して下さい。

9 ログ

NX リモート通報は以下の 10 種類のログを生成します。

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 受信した SNMP Trap 情報	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の動作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。⑤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

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
※既定のフォルダであれば、C:¥Program Files (x86)¥STS¥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。

・ HW ログを受け取ったとき
SP LOG TRANSMISSION SUCCESS

・ １時間の通報抑止で抑止されたとき
(---) inhibit in 1H.

・ 通報許可レベル設定により抑止されたとき
(---) suppress by level.

・ 通報許可を×にして抑止されたとき
(---) suppress by disallow.

・ 機種が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 8.2.2 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に出力します（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（ディフォルト 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】
Manager 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
※既定のフォルダであれば、C:¥Program Files (x86)¥STS¥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 からダウンロードした物件を 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。
ダウンロードしたインストール物件(NXremote_Win_Rxx.zip)を展開(※)し、以下のファイルを CD-R に書き込んで下さい。

・instNECServiceTerminalServerRxx.msi
・setup.exe

※インストール物件は、エクスプローラまたは市販の ZIP ファイル解凍ソフトで展開してください。

11　インストール設定表

記入方法は「3.3 設定項目の確認」の章を参照してください。

■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	

■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	
									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			
						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	
						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

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. GNU GENERAL PUBLIC LICENSE Version 2 ライセンス条文

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION
0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)
These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)
The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS
How to Apply These Terms to Your New Programs
If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.
Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.
Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'. This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.
The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.