S-7491-01U
S-7491-05P

不正持込み PC 監視＆強制排除システム

NX　NetMonitor

S-7491-01U
S-7491-05P

本製品を輸出される場合には，外国為替及び外国貿易法の規制並びに米国の輸出管理関連法規など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

第１版　　２００４年　２月
第２版　　２００４年　４月
第３版　　２００４年　６月
第４版　　２００４年　９月
第５版　　２００５年　３月
第６版　　２００５年　６月
第７版　　２００５年　８月
第８版　　２００５年１０月
第９版　　２００５年１２月
第１０版　２００６年１１月
第１１版　２００７年０３月
第１２版　２００７年０５月
第１３版　２００７年０８月
第１４版　２００８年０５月
第１５版　２００８年１０月

－目次－

ご注意

はじめに

本書は、登録されていないPCがネットワークに接続されたら、それを検知し、強制的に排除するNX NetMonitorについて、機能や構築方法について記述したものです。

ご注意

・システムの構築やプログラムの作成などの操作を行う前には、このマニュアルの記載内容をよく読み、書かれている指示や注意を十分理解してください。誤った操作により、システムの故障が発生することがあります。
・このマニュアルは、必要なときすぐに参照できるよう、手近な所に保管してください。このマニュアルの記載内容について理解できない内容、疑問点または不明点がございましたら、最寄りの当社営業もしくは SE までお知らせください。
・お客様の誤った操作に起因する事故発生や損害につきましては、当社は責任を負いかねますのでご了承ください。
・当社提供ソフトウェアを改変して使用した場合には、発生した事故や損害につきましては、当社は責任を負いかねますのでご了承ください。
・ネットワークへの接続を許可するための許可機器一覧、環境設定ファイル、ログファイルなどのバックアップ作業を日常業務に組み入れてください。ファイル装置の障害、ファイルアクセス中の停電、誤操作、その他何らかの原因によりファイルの内容を消失することがあります。このような事態に備え、計画的にファイルをバックアップしてください。

他社商標に関する表示

Linux は、Linus Torvalds 氏 の登録商標です。
Red Hat は、Red Hat Software,Inc.の登録商標です。
Microsoft Windows, Internet Explorer, Excel は米国 Microsoft Corporation の米国およびその他の国における登録商標です。
その他の社名、製品名はそれぞれの会社の商標または登録商標です。
なお、本文中では (R) の記号は使用していない場合もあります。

WinPcap

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.
This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.
This product includes software developed by Yen Yen Lim and North Dakota State University.

一般用語

略称	名称
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
ICMP	Internet Control Message Protocol
IPX	Internetwork Packet eXchange
MAC	Media Access Control
MIB	Management Information Base
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input Output System
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
MIME	MultiPurpose Internet Mail Extensions

＜記憶容量の計算値についての注意＞

- 2^n 計算値の場合（メモリ容量・所要量、ファイル容量・所要量など）
  1KB（キロバイト）＝1,024 バイトの計算値です。
  1MB（メガバイト）＝1,048,576 バイトの計算値です。
  1GB（ギガバイト）＝1,073,741,824 バイトの計算値です。
- 10n 計算値の場合（ディスク容量など）
  1KB（キロバイト）＝1,000 バイトの計算値です。
  1MB（メガバイト）＝$1,000^2$ バイトの計算値です。
  1GB（ギガバイト）＝$1,000^3$ バイトの計算値です。

用語の定義

統合管理ツール NX NetMonitor/Manager を搭載した計算機を統合管理装置と呼びます。統合管理ツールの GUI を統合管理画面といいます。
ネットワーク毎に監視する計算機を配置して、監視や不正 PC の排除を行うソフトウェアを NX NetMonitor といいます。NX NetMonitor を搭載した計算機を監視装置といいます。
中央のセンタなどに配置された計算機から、各拠点の監視を行うソフトウェアを NX NetMonitor /Detector といいます。NX NetMonitor/Detector を搭載した計算機を集中監視サーバといいます。
NX NetMonitor や NX NetMonitor/Detector で監視するネットワークを監視ネットワークといいます。ネットワークを監視する処理を監視処理といいます。

1. 概要

この章では、不正持込 PC 監視＆強制排除システムの機能について説明します。

1.1 背景

近年、無線 LAN やモバイル PC の普及に伴い利便性が向上してきたことで、社員や社外の人が意図すれば個人的に使用している PC を持ち込み、容易に企業内 LAN に接続することができるような状況にあります。そのため、これらからウィルス感染や、コピーによる情報の不正持ち出しといった問題も発生するようになり、それらの対策を求められるようになっています。

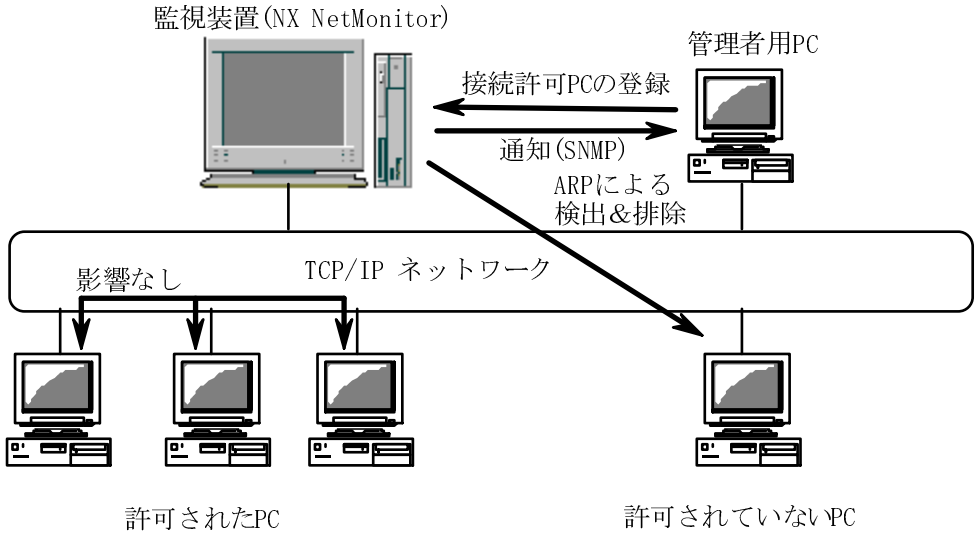
本システムを導入することにより、許可されていない持ち込み PC の企業内 LAN（TCP/IP ネットワーク）への接続を排除(*1)し、企業のネットワークを保護することができます。

(*1) 排除とは、論理的にネットワークから切り離すことを指します。
許可されていない PC に対して、下記の状態となる機能を提供します。
① ネットワーク機能を使用できない状態。
② TCP/IP 通信を使用できない状態。

1.2 概要

NX NetMonitor は、許可されていない PC の企業内 LAN（TCP/IP ネットワーク）への接続を検出し、ネットワークからの切り離すことで、企業のネットワークを保護するシステムです。ネットワーク管理者が管理していない PC を排除し、ウィルス感染や情報漏洩など、セキュリティ上の問題発生を防止します。

- クライアントソフトは不要です。
- 接続が許可されていない PC を自動的に LAN から切り離します。
- 指定した期限を越えた PC を自動的に LAN から切り離します。
- 一定期間、接続されなかった PC を自動的に LAN から切り離します。
- LAN から切り離された PC の物理的な位置を特定します。
  → PC が接続されているスイッチ、リピータの MAC アドレス、IP アドレス、ポート番号をログファイルに出力します。
- 不正 PC を LAN から切り離しますが、検疫のための通信のみを可能にします。(検疫支援通信)
- 不正接続件数や機器の稼動状況を日、週、月単位で表示します。



1.3 機能

(1) ネットワーク接続機器の管理

企業内 LAN へのネットワーク接続を許可する機器を、MAC アドレスと IP アドレスで管理します。DHCP により IP アドレスを管理しているネットワークの場合、ひとつの MAC アドレスに対して割り付ける IP アドレスの範囲を指定することができます。

(2) 許可されていない PC の検出と強制排除

ネットワーク接続が許可されていない PC がネットワークに接続されたことを検出すると、当該 PC を論理的に強制排除します。

(3) 統合システム管理ツールとの連携

運用時に監視処理が検出および強制排除した PC の情報を、統合管理装置(NX NetMonitor /Manager)に通知することができます。また、SNMP トラップ(SNMP v1 または v2)で通知することができます。通知を受信するには、管理者用 PC に SNMP トラップを受信できる SNMP マネージャツールをインストールする必要があります。

(4) GUI によるメンテナンス機能

NX NetMonitor は、監視状況の確認やネットワーク接続を許可する機器一覧のメンテナンスを、Web ブラウザによりネットワーク経由で行える機能を提供します。これにより、管理者は、メンテナンス時に、管理者用 PC から、NX NetMonitor が監視する複数の監視ネットワークに対して集中管理を行うことができます。

(5) 許可機器一覧／排除機器一覧と管理機能

以下に、許可機器一覧／排除機器一覧と管理機能の概要を示します。

＜許可機器一覧／排除機器一覧と管理機能概要の一覧 1/2＞

分類	機能	概要	備考
許可機器一覧 排除機器一覧	MAC アドレス	MAC アドレスと IP アドレスを組み合わせ、より厳密にネットワーク接続を許可する機器を定義することが可能。	DHCP により IP アドレスを管理しているネットワークの場合、IP アドレスの範囲を指定します。
	IP アドレス		
	停止期間監視	指定した期間起動されなかった機器が起動されたときに、排除するかどうか指定する機能。	有効にするときには“Y”を指定します。期間指定は、環境設定の許容停止期間で設定します。 排除機器一覧の場合無効です。
	有効期限	ネットワーク接続を許可する有効期限。	YYYY.MM.DD の形式で指定します。排除機器一覧を使用する場合は無効です。
	コメント	監視対象の PC に対するコメントを入力することが可能。	32 バイトまで入力できます。
管理機能	不正接続機器 検出/排除機能	許可されていない機器を検出し、論理的に排除する機能。	検疫支援モード時には、監視装置とだけ、または指定した特定のサーバとのみ通信を可能にします。特定サーバとの通信機能は Linux 版監視措置の機能です。
	接続機器一覧 表示機能	対象のサブネットに接続されている機器の一覧を表示する機能。	Windows(R)マシンの機器名やワークグループ名も取得します。

＜許可機器一覧／排除機器一覧と管理機能概要の一覧 2/2＞

分類	機能	概要	備考
管理機能	ログ機能	ログを記録する機能。	許可されていない機器が SNMP の MIB 情報を実装した機器（インテリジェントスイッチなど）に接続された場合、MIB 情報を利用して、接続したスイッチやポートの物理的位置を特定するための情報もログに記録します。
	トラップ通知機能	許可されていない機器の検出や排除を、トラップにて通知する機能。	トラップ通知は、統合管理装置(NX NetMonitor/Manager) と SNMP マネージャへの通知への 2 種類を使用可能です。
	許可機器一覧 固定機器一覧 排除機器一覧 登録機能	Web ブラウザで許可機器一覧等を登録、修正する機能。	メンテナンス作業時には、管理者用 PC が必要です。
	環境設定機能	各種設定を行う機能。	
	操作権限機能	全ての操作が可能な管理者ユーザと、情報参照のみを行うユーザを設定可能。	NX NetMonitor インストール時にユーザを作成します。
	統計情報表示	不正接続を検出した回数、各機器の稼動情報を、日、週、月単位に表示する機能。	稼働時間は接続機器一覧/拒否機器一覧の時刻付をダウンロードする、または統合管理装置(NX NetMonitor/Manager)で、参照可能です。

(6) 検疫支援機能

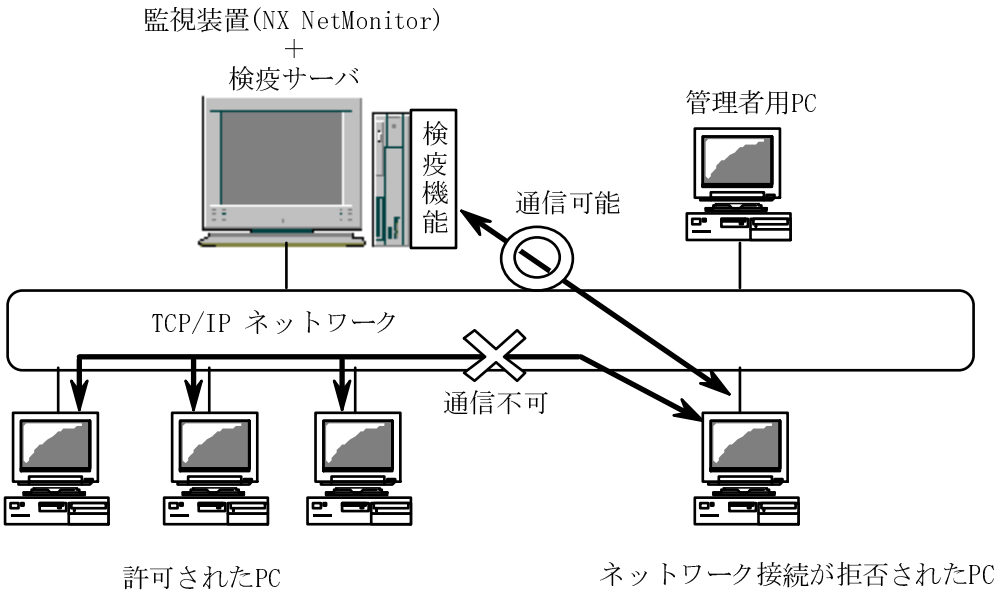
NX NetMonitor では、許可機器/固定機器として登録されている PC 以外、または、排除機器として登録された PC は、ネットワークへの接続が拒否されます。また、連携するソフトウェアや管理者によって、ウィルス感染・ウィルスパターンファイルが最新でない等のセキュリティポリシーに違反した PC のネットワーク接続を拒否することが可能です。その他、許可機器として登録されている PC が起動された時に、強制的に排除し、連携するソフトウェア等にて該当 PC がセキュリティポリシーに違反していないことが確認された場合にネットワーク接続を許可する機能をサポートしています（「６．16 環境設定」の「検疫支援機能」の「許可機器起動時の対処」を参照)。連携するソフトウェアに関しましては、連携製品のマニュアル等を参照ください。

ネットワーク接続が拒否された PC でも､他の PC との通信を遮断しつつ､自席(通常の企業内 LAN)からウィルスパターンファイルやパッチ更新(検疫)を行うための通信を可能にする機能（検疫支援通信）をサポートします。設定方法は、「６．16 環境設定」を参照ください。

なお、通常(検疫支援機能を無効とした場合)、不正 PC を起動すると、ネットワークインタフェースが無効となり、システムエラー等が発生しますが、検疫支援機能を有効にすると、検疫のための通信を行うために、ネットワークインタフェース自体は有効になります（固定 IP の場合)。
また、DHCP により IP アドレスを管理している場合には、検疫支援機能の有効/無効に関わらず、ネットワークインタフェースは有効となるケースがあります。

ネットワーク接続が拒否された PC は、他の機器との通信を遮断しつつ、検疫機能を搭載するマシンとの通信のみを許可することにより、検疫を行うことを可能としています。

Windows 版監視装置では、NX NetMonitor の監視機能と検疫機能を同じマシンにインストールする形態をサポートします。
Linux 版監視装置では、NX NetMonitor の監視機能と検疫機能を同じマシンにインストールする形態に加え、NX NetMonitor の監視機能と検疫機能を別マシンにする形態もサポートします。ネットワーク接続が拒否された PC と検疫機能を搭載するマシン（検疫サーバ等）を通信させるための設定や構成は、本書の「７．特定機器との通信サポート」を参照してください。

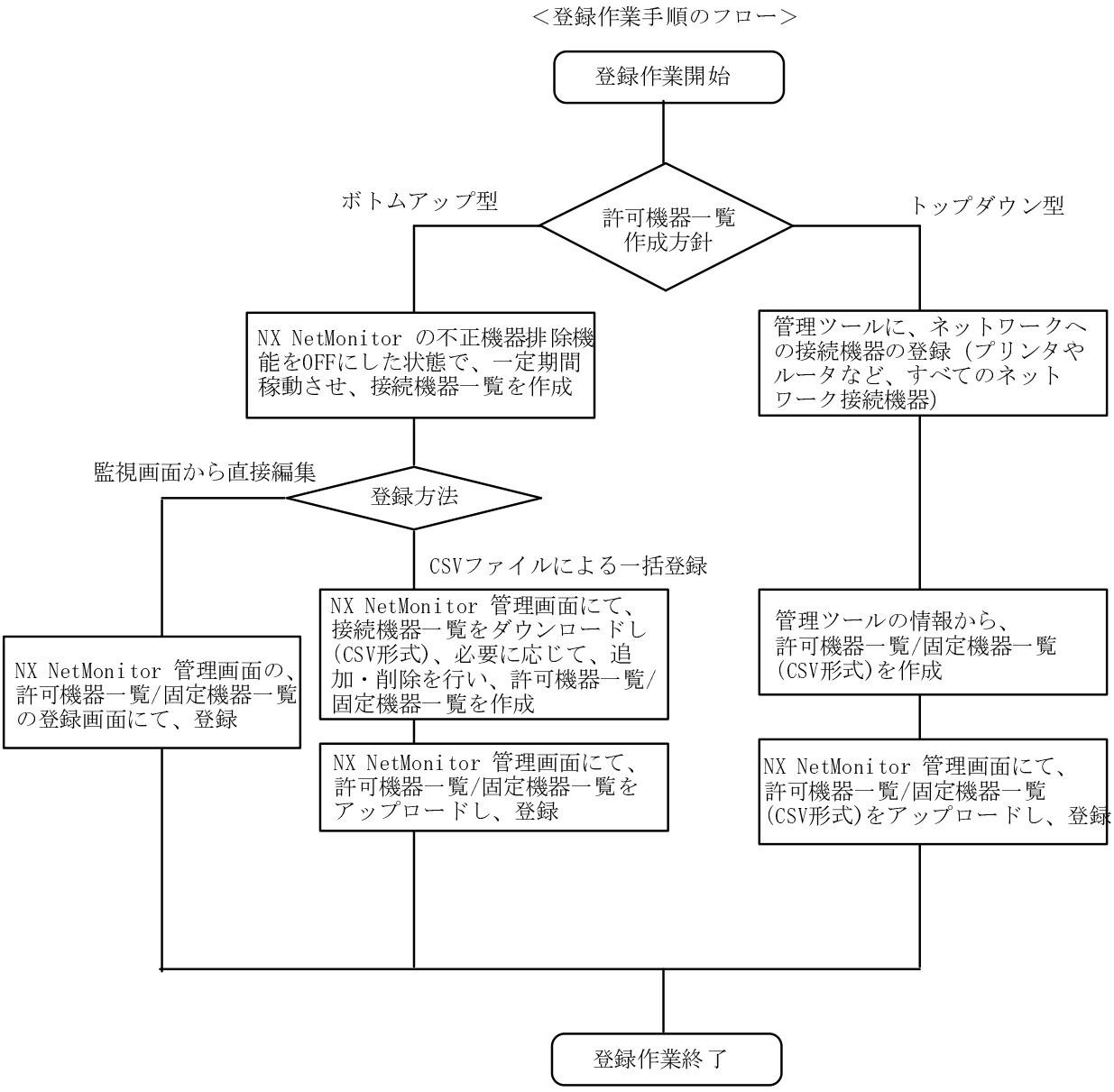


1.4　適用例

以下に、NX NetMonitor での管理情報の登録の適用例を示します。

ブロードキャストが届くサブネット単位に、NX NetMonitor をインストールした監視装置を接続し、管理情報として、許可された機器のアドレス一覧(許可機器一覧/固定機器一覧)を登録します。
許可機器一覧は、下記２つの方法で登録することができます。

ボトムアップ型 ： 監視処理で検出した現状のネットワーク接続機器、管理者が追加登録した機器の一覧を使用
トップダウン型 ： ご利用中のネットワーク接続機器の管理ツールから出力した CSV 形式の一覧を使用

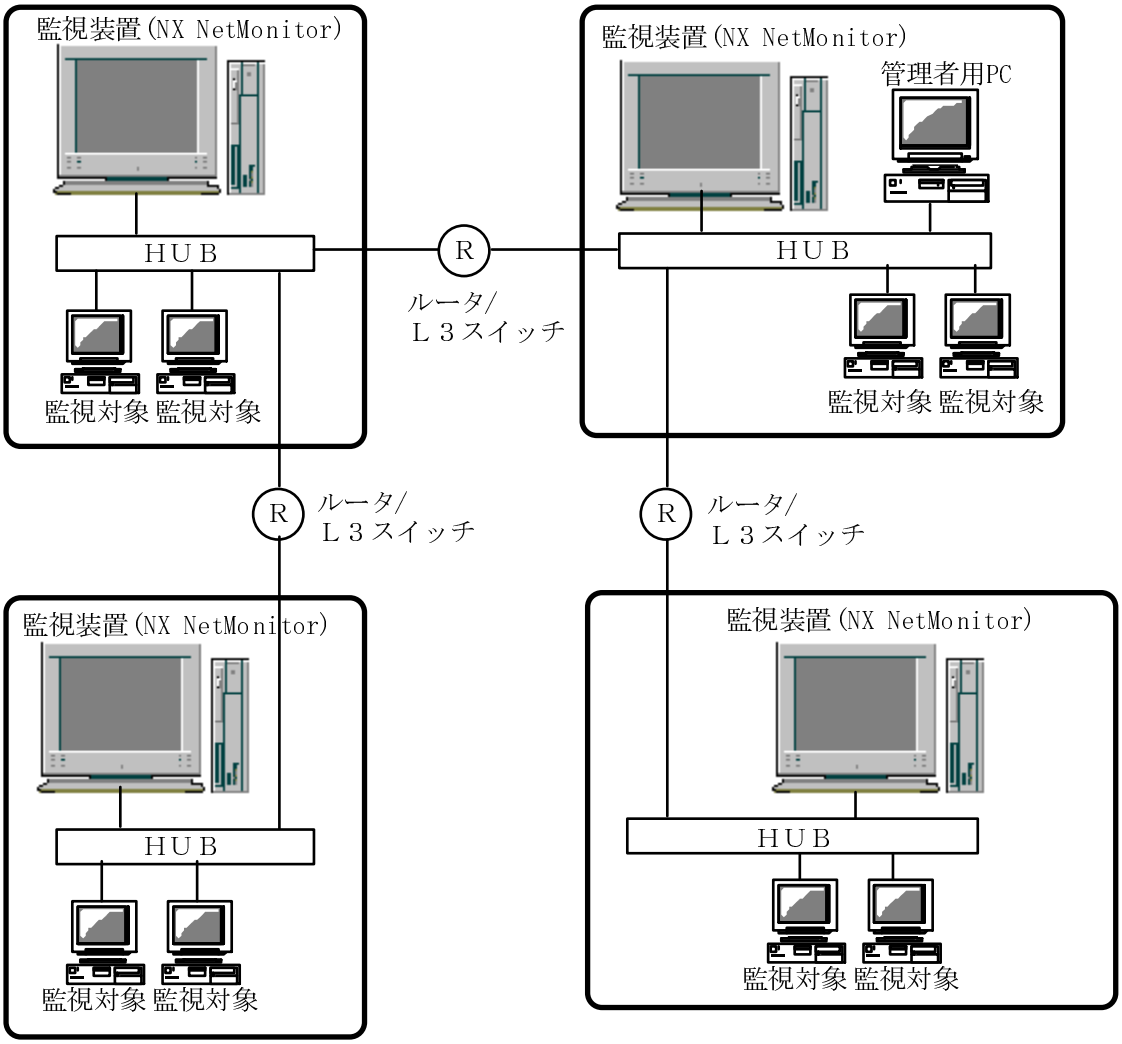


2. システム構成

この章では、不正持込み PC 監視＆強制排除システムの代表的な構成について説明します。

2.1 基本構成

ルータやＬ３スイッチで区切ったサブネットワーク単位（ブロードキャストが届く範囲）に、監視装置(NX NetMonitor)を用意してください。一つのサブネットワークには、監視装置の CPU 性能やメモリ搭載量にもよりますが、監視装置１台(CPU800MHz)で、監視対象の PC などが約５００台程度監視可能です。また、監視可能なアドレス管理体系として、固定 IP アドレス、DHCP による自動 IP アドレス割り当てをサポートします。

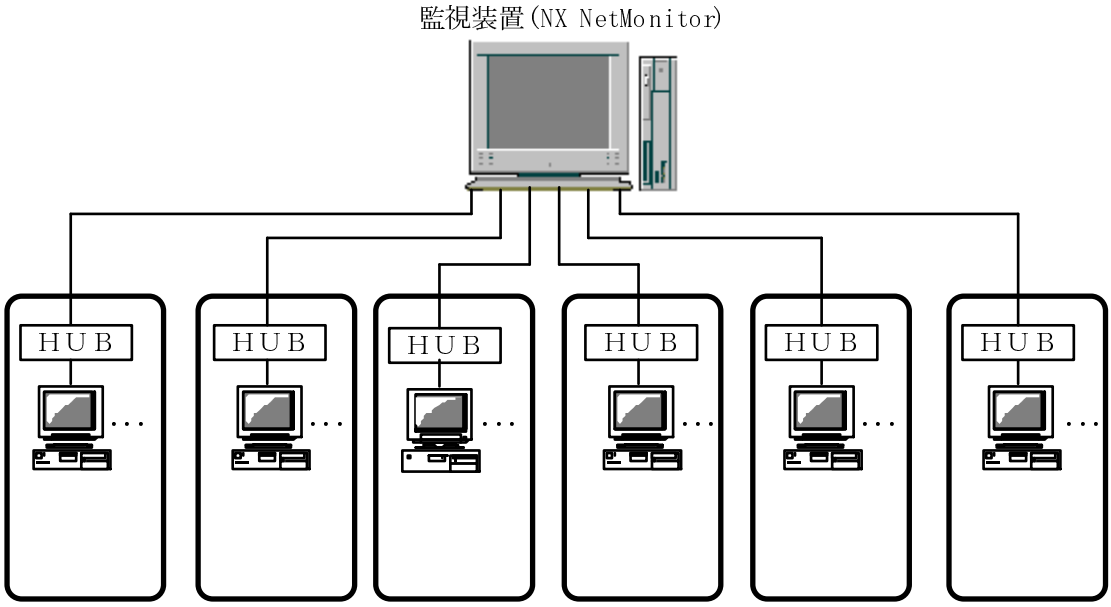


＜システム構成要素一覧＞

構成要素	説明
NX NetMonitor	サブネットワークの監視を行うソフトウェアです。監視装置にインストールします。 接続されたサブネットワークを監視し、不正持込み PC の検出や強制排除を行います。不正持込み PC の検出をログファイルに記録し、統合管理装置(NX NetMonitor/Manager)、または、SNMP にて管理者用 PC に通知します。
監視装置	NX NetMontior を搭載した装置です。
管理者用 PC	NX NetMonitor を集中管理するための PC です。管理者は、ネットワークへの接続を許可する PC の一覧の登録や検出状況の確認を Web ブラウザにて行うことができます。 また、統合管理ツール(NX NetMonitor/Manager)をインストールすることにより、統合管理ツールの画面で複数の監視ネットワークの情報参照、許可機器一覧の一括更新をおこなうことが可能です。
監視対象	監視対象となる機器です。Windows(R) 95, Windows(R) 98, Windows(R) Me, Windows(R) XP, Windows(R) NT 3.51 および 4.0, Windows(R) 2000, Windows(R) 2003 , Windows(R) Vista, Windows(R) 2008 を搭載している PC とします。上記以外の Macintosh や UNIX、組込み OS などの機器については、標準 TCP/IP を使用している場合に限り、監視対象となります。

2.2 複数サブネットワークを監視する際の構成

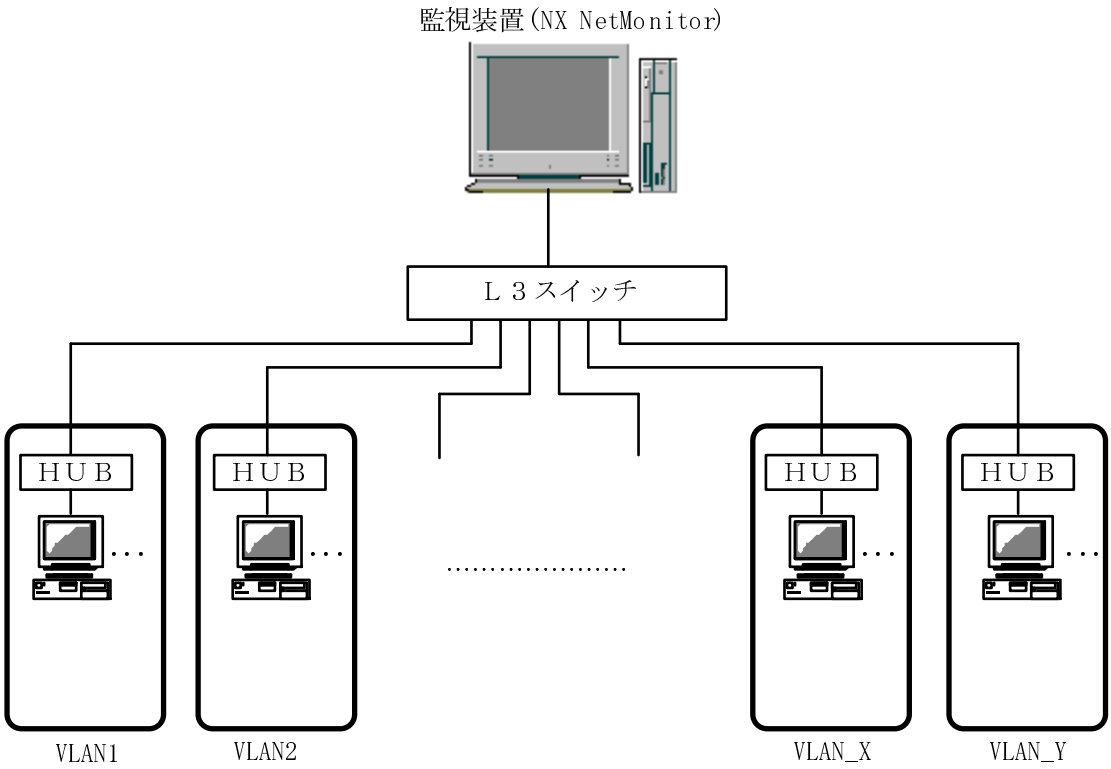
基本システム構成としては、サブネット単位に 1 台の監視装置を配置する構成ですが、ネットワークインターフェースを複数に拡張することにより、1 台の監視装置にて、複数のサブネットワークを監視することができます。



また、VLAN(Virtual LAN)のトランク接続機能を使用して、複数の VLAN を束ねることにより、1 台の監視装置（一つのネットワークカード）で、複数のサブネットワーク(VLAN)を監視することが可能です。

ただし、前提条件として、下記があります。

- 監視装置のネットワークカード
  IEEE 802.1Q (VLAN) に対応していること
- 監視装置を接続するスイッチのポート
  ① タグ VLAN の設定が可能なこと
  ② トランク接続（複数の VLAN を通過させる）が可能なこと



3. ご用意していただくもの

この章では、不正持込み PC 監視&強制排除システムを使用する際に、用意するべきものについて説明しています。

3.1 監視装置（NX NetMonitor を搭載するマシン）

＜監視装置の前提ハードウェア/ソフトウェア一覧＞

項目	仕様
CPU	Intel PentiumⅢ　800MHz 以上
メモリ	512 MB 以上
ディスク	空き容量が　１ＧＢ以上
OS	<Linux> ・Red Hat Linux 7.2 （日本語） ・Red Hat Enterprise Linux 3 （日本語） ・Red Hat Enterprise Linux 4 （日本語） ・Red Hat Enterprise Linux 5 （日本語） <Windows> ・Windows(R) 2000 Professional SP4 （日本語） ・Windows(R) 2000 Server SP4 （日本語） ・Windows(R) 2000 Advanced Server SP4 （日本語） ・Windows(R) XP Professional SP2,SP3 （日本語） ・Windows(R) Server 2003 Standard Edition　SP1,SP2（日本語） ・Windows(R) Server 2003 Enterprise Edition　SP1,SP2（日本語） ・Windows(R) Server 2003 R2 Standard Edition SP2（日本語） ・Windows(R) Server 2003 R2 Enterprise Edition SP2（日本語） (注) 検疫支援機能は、Windows(R) 2000 Professional, Server, Advanced Server が非サポートとなります。
前提ソフトウェア	<Linux> Red Hat Linux 7.2 の場合 ・Web サーバ：apache Red Hat Enterprise Linux 3/4/5 の場合 ・Web サーバ：httpd <Windows> Windows(R) 2000, Windows(R) XP の場合 ・Web サーバ：IIS 5.X Windows(R) Server 2003 の場合 ・Web サーバ：IIS 6.0
ネットワーク	監視装置 1 台につき、1 つのサブネットを基本とします。 監視装置にネットワークインタフェースを増設・拡張する場合、インタフェースに接続したサブネット単位で監視可能とします。 また、VLAN のトランク接続機能を利用することにより、複数のサブネットを監視可能とします。

※1. NX NetMonitor を動作させる監視装置は、監視処理の遅れを防止するため、他の用途(NX NetMonitor と連携動作するソフトウェア以外)と併用せずに専用の PC をご用意することを推奨します。このとき、ARP(Address Resolution Protocol)データのブロードキャストが届く範囲のサブネット単位に監視装置を設置してください。

※2. 上記は、1 台の監視装置で 500 台のネットワーク接続機器を監視するスペックです。 1 台の監視装置で監視できる機器数は、CPU 性能や各サブネットワークの接続機器台数などに依存します。

※3. 本製品は、クラスタ環境未サポートです。

※　4. VLAN 環境で使用する場合には、
・監視装置のＯＳが Linux の場合、Red Hat Enterprise Linux 3 または 4 が前提
・IEEE 802.1Q (VLAN) に対応したネットワークカードが前提(Intel(R) PRO/1000 など)です。
その場合、ネットワークカードがタグ VLAN(IEEE 802.1Q)に対応していることをカタログなどで事前にご確認ください。

※ 5. Red Hat Enterprise Linux 3 の対応アーキテクチャは X86 システム(32 ビット)、
Red Hat Enterprise Linux 4／5 の対応アーキテクチャは X86 システム(32 ビット)
および AMD64/EM64T システム(64 ビット)です。
Windows では 64 ビットマシンをサポートしていません。

3.2 管理者用 PC（NX NetMonitor の操作を行うマシン）

＜管理者用 PC 前提ハードウェア/ソフトウェア一覧＞

項目	仕様
CPU	Intel PentiumⅢ 500MHz 以上
メモリ	推奨：255 MB 以上 最小：128 MB 以上
ディスク	空き容量が 100 M バイト以上
OS	Windows(R) 2000, Windows(R) XP, Windows(R) Server 2003, Windows Vista,Windows(R) Server 2008
前提ソフトウェア	Microsoft(R) Internet Explorer 6.0 以降

※1. 管理者用 PC に、NX NetMonitor はインストール不要です。
Web ブラウザ、または統合管理ツールを使用して、監視ネットワークの操作・表示を行います。
※2. 不正機器の検出の通知を行う場合には、監視処理の独自トラップ機能を使用して、統合管理装置(NX NetMonitor/Manager)へ通知します。または、SNMP トラップを受信可能なツールをインストールしたマシンに通知します。なお、使用する SNMP のバージョンは 、ｖ1, ｖ2 です。
※3.Internet Explorer 7 を使用して監視ネットワークの Web 画面を参照する場合、Internet Explorer 7 の機能である、ズーム機能を使用した場合に画面表示が乱れる場合があります。ズームは 100%表示でご使用ください。
※4. 上記管理者用 PC は、他のソフトウエアと共存させない場合のスペックです。

3.3　ネットワークへの接続を許可する機器一覧

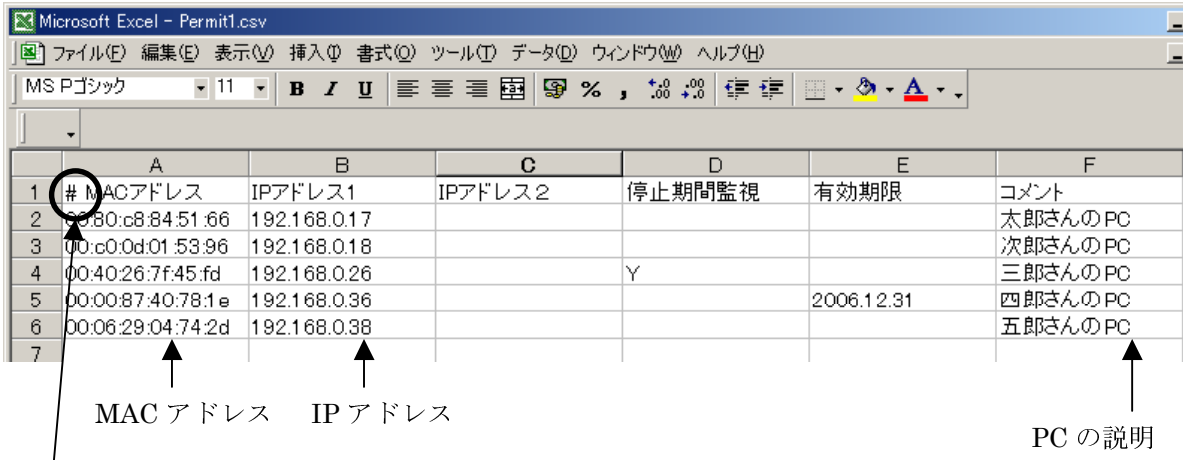
許可するＰＣの一覧表を作成してください。フォーマットは、以下の通りで、許可する PC の MAC アドレス、IP アドレス、そして、その PC の説明を、Microsoft(R) Excel(R) などを使用し、CSV 形式で記述します。詳細は、「６．１０ アップロード」を参照ください。
このファイルを、管理者用 PC から、Web ブラウザを使用してアップロードすることにより、監視ネットワークに登録します。

登録の方法として、以下の４種類があります。

- MAC アドレスと IP アドレス　　：固定 IP アドレスを割り付けた機器
- MAC アドレスと IP アドレスの範囲　：DHCP による IP アドレス自動割当てを行う機器
- IP アドレスのみ　　：仮想 IP アドレスを用いて多重化されたサーバなど
- MAC アドレスのみ　　：持ち運んで使用するモバイル機器など

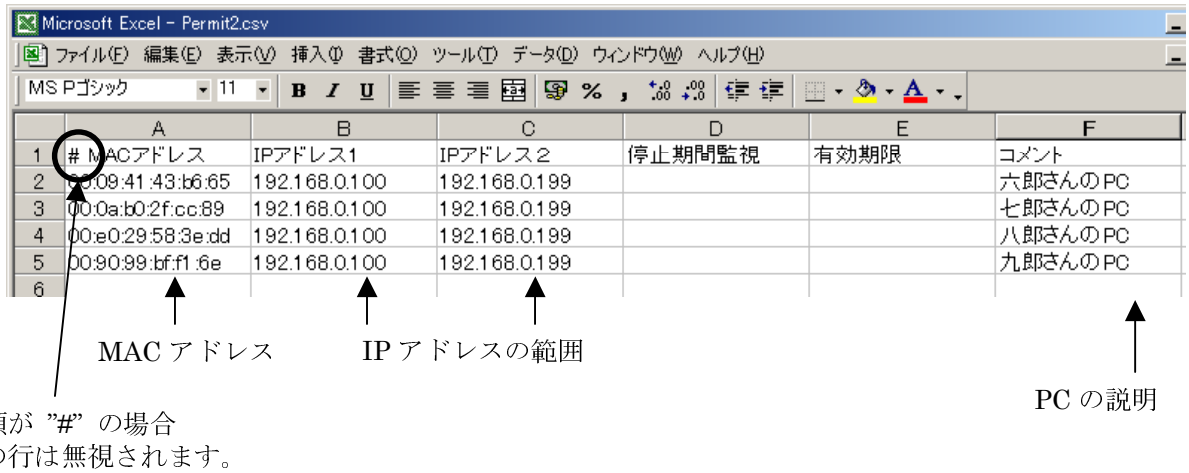
設定例を以下に示します。

・固定 IP アドレスの場合の設定例



先頭が ”#” の場合
その行は無視されます。

・DHCP による IP アドレス自動割当の場合の設定例



先頭が ”#” の場合
その行は無視されます。

4. 注意事項

この章では、不正持込 PC 監視＆強制排除システムを使用する際の注意事項について説明します。

4.1 機能全般

(1) ネットワーク接続機器に対して，下記の状態となる機能を提供します。
・Windows(R)を搭載し，許可されていない PC が LAN 接続された場合、当該 PC のネットワーク機能(TCP/IP 通信)を使用できない状態にします。
・Windows(R)以外の OS を搭載した機器の場合、または、監視処理が一時的に停止している間に LAN 接続され，その後，監視処理が監視を再開した場合。TCP 通信を使用できない状態にします。
・DHCP により IP アドレス管理している場合、DHCP サーバが IP アドレスをリース後，TCP 通信を使用できない状態にします。

(2) 許可機器一覧/固定機器一覧には，監視対象とするクライアント PC のほか，ネットワークに接続されるプリンタやルータなどを含むすべてのネットワーク接続機器のアドレスを登録してください。

(3) ネットワークカードの交換など，許可機器一覧/固定機器一覧に登録したネットワーク接続機器の MAC アドレスが変更になる場合は，登録してある MAC アドレス情報も更新してください。
「MAC アドレスのベンダ指定」を有効とし、MAC アドレスの下位３バイトを０で指定すると、ベンダ ID(上位３バイト)のみ一致すると許可されます。詳細は、「６．１６ 環境設定」を参照してください。

(4) MAC アドレスが変更されても許可機器一覧の更新が早急に行えないが，ネットワーク接続機器として継続利用できたほうがよい場合は，許可機器一覧に IP アドレスのみ登録することを推奨します。
例えば，下記のネットワーク接続機器が該当します。
・24 時間稼働が前提となっているサーバやルータ
・仮想 IP アドレスを用いて多重化されたサーバ

(5) 仮想 IP アドレスを定義した機器については，許可機器一覧に IP アドレスのみ登録してください。

(6) 本製品の機能により論理的に排除した後は，対象の機器がどのような用途で使用されているかを確認して不要なものであれば、ネットワークに接続させないような対応を取ってください

(7) 本製品は，排除機能によってウィルスの蔓延防止効果が期待できますが，ウィルスの蔓延防止を保証するものではありません。

(8) スイッチングハブなどのネットワーク装置の稼働状態によっては，不正接続の検出に時間がかかる場合があります。

(9) ネットワークの状況や，同時に多量のトラップが発生した場合などに，監視処理からの独自のトラップ情報や SNMP による通知が管理者用 PC に届かない場合があります。ただし，通知内容のログは監視装置内で保存していますので，Web ブラウザにて参照してください。

(10) 不正機器の接続位置を特定するために、HUB の情報(MIB 情報)を、SNMP にて取得しています。そのため、該当情報(MIB)が存在しない機器が存在する場合や、ネットワーク機器の状態、その他の要因により、特定ができない場合があります。また、直接接続している HUB(MIB 情報を持った HUB)を特定できなければ、その上位に接続されている HUB の情報を出力する場合があります。

4.2 監視装置

(1) 監視処理の遅れを防止するため，監視装置は専用の PC を用意し，他の用途（NX NetMonitor と連携動作するソフト以外）と共用しないことを推奨します。

(2) 監視装置が停止，または監視対象ネットワークの機能が停止している場合，監視はできません。
この状態で不正に LAN 接続が行われ，その後，監視処理が監視を再開した場合は，TCP 通信を利用できない状態にすることで排除を行います。

(3) 監視装置は，ケーブルによる有線の LAN 接続としてください。無線 LAN で接続した場合，通信環境が劣化した際に不正な PC の LAN 接続の検出や排除ができないことがあります。

(4) 監視装置の OS の保守やセキュリティパッチの適用は，PC 購入元で提供しているセキュリティ情報などを入手して，顧客の責任で運用してください。

4.3 監視対象のネットワーク

(1) 本製品は，ルータや L3 スイッチで区切られたブロードキャストが届くサブネットワーク単位に監視を行います。

(2) 監視処理が DHCP サーバを用いて動的に IP アドレスを割り当てるネットワークを監視した場合，DHCP サーバは不正接続 PC にリースしようとした IP アドレスを，一定時間使用中として管理します。したがって，監視処理がその時間内に多数の不正接続 PC を排除した場合は，管理している使用可能な IP アドレスが少なくなることがありますので，排除した PC は速やかにネットワークから取り除いてください。

(3) VLAN を用いたネットワークの場合、タグ VLAN(IEEE 802.1Q)のトランク機能を使用することにより、複数のサブネットワークを監視することができます。その場合、監視装置のネットワークカードがタグ VLAN(IEEE 802.1Q)に対応していることをカタログなどで事前にご確認ください。

(4) IPv6 のネットワークは、未サポートです。

(5) 1 つのセグメントに複数のネットワークが存在する場合、監視装置の NIC に割り当てたエイリアス IP アドレスでの監視も可能ですが、複数のネットワークを監視するため、監視装置の CPU 負荷やメモリ負荷が増加します。エイリアス IP アドレスでの監視も行う場合には、監視装置の性能を事前に評価して下さい。1 つのセグメントに複数のネットワークが存在する場合には、監視装置も複数台用意することを推奨します。

4.4 監視対象とする機器

(1) 監視対象とするクライアント PC の OS は下記とします。下記以外の Macintosh や UNIX、組込み OS などの機器については、標準 TCP/IP を使用している場合に限り、監視対象となります。
- Windows(R) 95
- Windows(R) 98
- Windows(R) Me
- Windows(R) XP
- Windows NT(R) 3.51　および 4.0
- Windows(R) 2000
- Windows(R) Server 2003
- Windows(R) Vista
- Windows(R) Server 2008

(2) 監視対象となるプロトコルは TCP/IP のネットワークです。NetBEUI や IPX などは対応していません。

(3) 無線 LAN に接続したネットワーク接続機器を監視する場合は，MAC アドレスの情報を中継するアクセスポイントとしてください。MAC アドレスの情報を中継しない場合、不正接続の検出はできません。

4.5 その他

(1) 許可機器一覧/固定機器一覧/排除機器一覧は、 それは Windows(R) で作成したものを前提としています。文字コードは ASCII および Shift-JIS、改行コードは CRLF です。

(2) 許可機器一覧から削除しても、すぐに切り離されない場合があります。すぐに切り離したい場合には、まず監視画面から手動で「拒否」を行い、その後、許可機器一覧から削除してください。

(3) 許可機器一覧に追加、または手動で許可しても、すぐに接続できない場合があります。

(4) 登録されていない機器の接続を許可する場合、接続許可作業完了後に該当機器を再起動することを推奨します。再起動しなくても通信可能となることがありますが、接続許可操作は、その機器の再起動なしに通信を可能とすることを保証するものではありません。

(5) 環境設定の監視周期（「６．16 環境設定」参照）で指定した間隔で、監視パケットが送信されます（以降、パトロール機能と呼びます)。これは、定周期でネットワークに接続されている機器を検出するためのポーリングです。この監視パケットの送信間隔、対象 IP アドレスの範囲を調整することにより、ネットワーク負荷を調整できます。

(6) パトロール機能は、環境設定にて停止させることが可能です。停止させても、不正接続の監視は行われます。ただし、他の PC と通信を行わない PC は検出されません。そのような PC も検出したい場合には、パトロール機能を有効にしてください。

(7) パトロール機能は、クラス A（ネットマスクが 16 ビット未満）のネットワークを監視する場合、無効となります。クラス A のネットワークでパトロール機能を有効にするには、環境設定にて対象 IP アドレスの範囲を指定してください。

5. インストール手順

この章では、NX NetMonitor のインストール手順について説明しています。

5.1 Linux 版のインストール

（1）ＯＳのインストール

RedHat Linux をインストール画面の指示に従い、インストールします。
下記項目を選択します。

・パッケージのインストール：Web サーバ

次に、root でログインし、下記設定を確認します。
下記設定は、ARP キャッシュに保存するエントリ数です。

```
# cd /proc/sys/net/ipv4/neigh/default
# cat gc_thresh1
128
# cat gc_thresh2
512
# cat gc_thresh3
1024
```

これが監視する機器の台数より大きいことを確認します。
(デフォルトは、1024)

監視する機器の台数より小さい場合には、定義ファイル(/etc/sysctl.conf)の設定を変更します。

本項目は、デフォルトでは定義されていませんので、本項目がない場合には追加します。

・net.ipv4.neigh.default.gc_thresh1：gc_thresh2 の 1/4 とします。
・net.ipv4.neigh.default.gc_thresh2：gc_thresh3 の 1/2 とします。
・net.ipv4.neigh.default.gc_thresh3： 監視対象機器の台数より大きくします。

以下に、監視台数 4000 台程度の場合の設定例を示します。

ファイル /etc/sysctl.conf

```
net.ipv4.neigh.default.gc_thresh1 = 512
net.ipv4.neigh.default.gc_thresh2 = 2048
net.ipv4.neigh.default.gc_thresh3 = 4096
```

設定内容は、マシンの再起動後反映されます。再起動後、変更されたことを確認してください。

```
# cd /proc/sys/net/ipv4/neigh/default
# cat gc_thresh1
512
# cat gc_thresh2
2048
# cat gc_thresh3
4096
```

以上で、完了です。

（2）前提ソフトウェアの確認とインストール

root でログインして下記のコマンドを実行し、前提ソフトウェアがインストールされていることを確認ください(X,Y,Z,V はバージョン番号)。下記のようにコマンドの実行結果が表示されればインストール済みです。

・RedHat　Linux 7.2 の場合

```
# rpm -q apache
apache-X.Y.Z-V
```

← 表示されればインストール済みです。

・RedHat Enterprise Linux ES 3 または 4 の場合

```
# rpm -q httpd
httpd-X.Y.Z-V.ent
```

← 表示されればインストール済みです。

インストールされていなければ、RedHat Lunux のインストール CD の /RedHat/RPMS の下にソフトウェアパッケージが格納されていますので、インストールしてください。例えば、httpd の場合、以下の通りです。

```
# rpm -ivh /mnt/cdrom/RedHat/RPMS/httpd-X.Y.Z-V.i386.rpm
```

また、Web サーバの文字コードの設定を確認してください。正しく設定されていないと、管理者用 PC から監視画面を見たときに、文字化けする可能性があります。

/etc/httpd/conf/httpd.conf

```
AddDefaultCharset XXXXX
```

という項目です。
この設定がない、none、EUC-JP の場合は、問題ありません。但し、Red Hat Enterprise Linux 4 の場合は、デフォルトが UTF-8 になっているため、明確に EUC-JP と定義してください。
EUC-JP 以外の場合には、エディタにて、

```
AddDefaultCharset EUC-JP
```

と変更してください。

次に、Web サーバの格納ディレクトリを確認してください。下記と異なる場合には、下記のとおりに変更してください。

/etc/httpd/conf/httpd.conf

```
DocumentRoot     "/var/www/html"
```

なお、Red Hat Enterprise Linux 4 の場合は、SELinux の設定を確認してください。
SELinux の設定を有効にしていると、HTTP でのアクセスに制限が加わるため、Network Monitor の管理操作（環境設定、監視の起動など）を行うことができません。

/etc/selinux/config

```
SELINUX=XXXXX
```

この設定が、Permissive、disabled の場合は、問題ありませんが、enforcing　となっている場合はエディタにて、

```
SELINUX=disabled
```

と変更してください。

（3）不要サービスの停止処理について

NX NetMonitor をインストールすると、xinetd 関連のサービス(telnet, FTP など)は強制的に停止します。これを回避する場合には、以下のディレクトリを作成し、

```
/usr/etc/nxnetmonitor/limit/xinetd.d/able
```

その下に、telnet など、停止を除外したいサービスに対応する名称のファイルを作成してください。ファイルの内容は問いません。サービス名に対応した名称のファイルがあれば、そのサービスは停止しません。各サービスのファイル名は、/etc/xinetd.d の下を参照ください。

（4）NX NetMonitor のインストール

root でログインし、下記手順でNX NetMonitorをインストールします。
なお、Red Hat Enterprise Linux 4 の場合は、マウントポイントが /mntではなく、/mediaとなりますので、/mntを/mediaに読替えてください。
また、/mnt や /media の下に cdrom という名称のディレクトリが存在しない場合、mkdir コマンドで cdromディレクトリを作成してください。

① CD-ROM ドライブに、NX NetMonitor の提供媒体をセットします。
② CD-ROM ドライブをマウントします。

```
# mount -r -o mode=0544 /dev/cdrom /mnt/cdrom
```

③ CD-ROM ドライブへ移動します。

```
# cd /mnt/cdrom/S749101U
```

④ インストールコマンドを起動します。

```
# ./nxnm.install user
  ++ NX NetMonitor install start ++
        :
        :
  New password: password
  Retype new password: password
        :
        :
  ++ NX NetMonitor install completed ++
```

NX NetMonitorへのログイン名を指定(※1)
NX NetMonitorへのパスワードを入力
NX NetMonitorへのパスワードを再入力

※1　NX NetMonitorのWeb画面へアクセスする管理者ユーザを登録する必要があります。
参照限定ユーザを作成する場合は、「（8）参照限定ユーザの登録」を参照してください。

⑤ CD-ROM ドライブ外へ移動します。

```
# cd /
```

⑥ CD-ROM ドライブをアンマウントします。

```
# umount /mnt/cdrom
```

⑦ CD-ROM ドライブから、NX NetMonitor の提供媒体を取り出します。
⑧ マシンを再起動します。

```
# shutdown -r 0
```

以上で完了です。

（5）NX NetMonitor の再インストール

root でログインし、下記手順でNX NetMonitorを再インストールします。
再インストールはNX NetMonitorのバージョンアップ時などに行います。

① ～ ③ は、インストールと同様です。
④ インストールコマンドを起動します。

```
# ./nxnm.install
  ++ NX NetMonitor install start ++
        :
        :
  ++ NX NetMonitor install completed ++
```

ログイン名は不要です。

⑤ ～ ⑧ は、インストールと同様です。

以上で完了です。
また、再インストール時には、NX NetMonitor は、自動的に停止しますのでマシンを再起動してください。

（6）NX NetMonitor のログイン／パスワードの変更

root でログインし、下記コマンドでログイン名とパスワードを変更します。

```
# /usr/etc/nxnetmonitor/bin/nxnm.setup -pwd user
  ++ NX NetMonitor setup start ++
        :
        :
  New password: password
  Retype new password: password
        :
        :
  ++ NX NetMonitor setup completed ++
```

NX NetMonitor へのログイン名を指定
NX NetMonitor へのパスワードを入力
NX NetMonitor へのパスワードを再入力

※1 参照限定ユーザのログイン／パスワードの変更は、「（8）参照限定ユーザの登録」を参照してください。

（7）NX NetMonitor の起動・停止・状態表示

root でログインし、下記コマンドで NX NetMonitor の起動、停止、状態表示を実行します。

・管理プログラム

Web ブラウザからのネットワーク監視プログラムの起動／停止／状態表示の要求を実行するものです（「６．２２ その他メニュー」参照)。管理プログラムが起動されていないと、Web ブラウザからの要求はエラーとなります。また、監視装置の起動時には、管理プログラムが自動的に起動されます。

① 起動

```
# /etc/rc.d/init.d/nxnmmngd start
```

② 再起動

```
# /etc/rc.d/init.d/nxnmmngd restart
```

③ 停止

```
# /etc/rc.d/init.d/nxnmmngd stop
```

④ 状態表示

```
# /etc/rc.d/init.d/nxnmmngd status
```

・ネットワーク監視プログラム

不正な機器の検出・強制排除を行うプログラムです。ネットワーク監視プログラムが起動され ていないと、不正な機器の検出・強制排除は行われません。また、Web ブラウザからも、実行 できます（「６．２２ その他メニュー」参照)。
また、監視装置の起動時には、ネットワーク監視プログラムが自動的に起動されます。

① 起動

```
# /etc/rc.d/init.d/nxnmd start
```

② 再起動

```
# /etc/rc.d/init.d/nxnmd restart
```

③ 停止

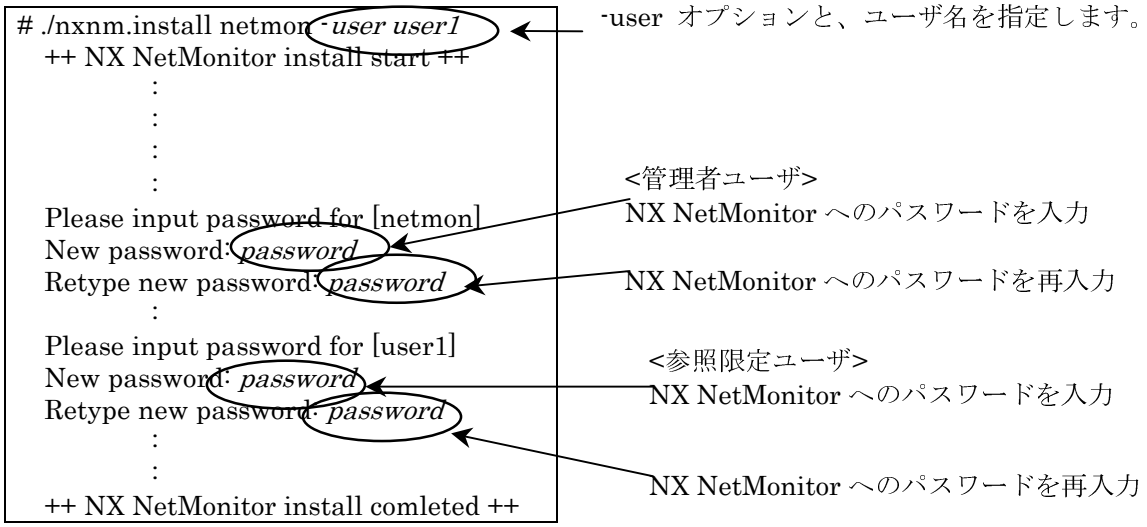
```
# /etc/rc.d/init.d/nxnmd stop
```

④ 状態表示

```
# /etc/rc.d/init.d/nxnmd status
```

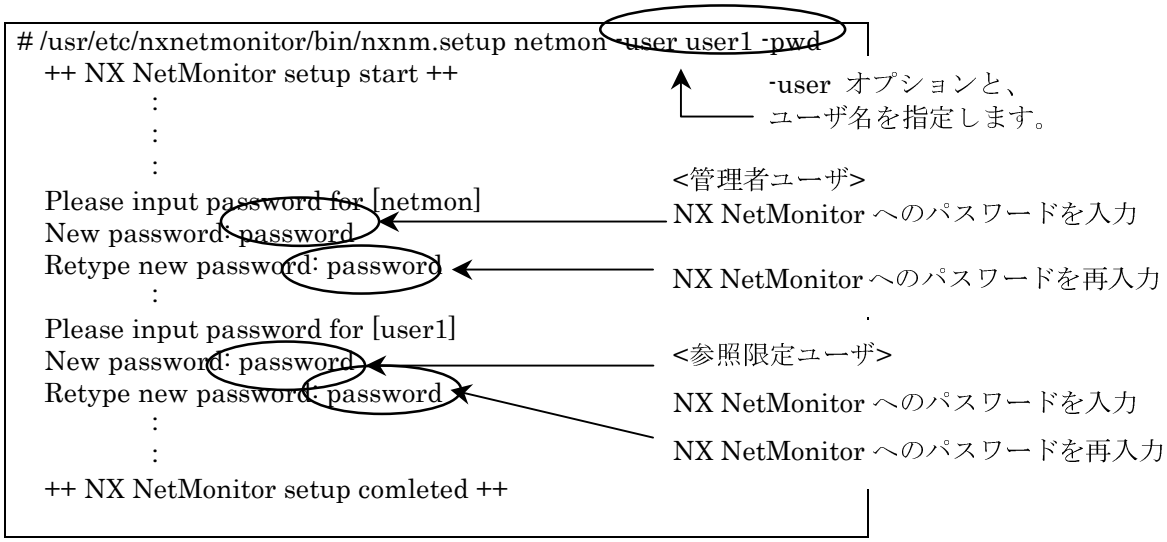
（8）参照限定ユーザの登録

参照限定ユーザを作成する場合は、インストールコマンドで -userオプションを指定します。
root でログインしてオペレーションを行ってください。
以下、管理者ユーザ netmonと user1 というユーザを作成する例を示します。



・ 参照限定ユーザのパスワード変更
root でログインしてオペレーションを行ってください。
参照限定ユーザを作成する場合は、セットアップコマンドの -userオプションを指定します。
また、現在、管理者ユーザのみを作成していて、参照限定ユーザも作成したい場合にも、本手順を行ってください。

以下、管理者ユーザ netmonと user1 というユーザを作成する例を示します。



参照限定ユーザの場合の監視画面は「６．２１　ユーザ権限の付与」を参照してください。

NX NetMonitorのWeb監視画面にアクセスするためには、nxnm.installコマンドまたは、nxnm.setupコマンドで登録したユーザのみアクセスが可能です。それ以外のユーザはWeb画面のログイン時にエラーとなります。

5.2　Windows 版のインストール

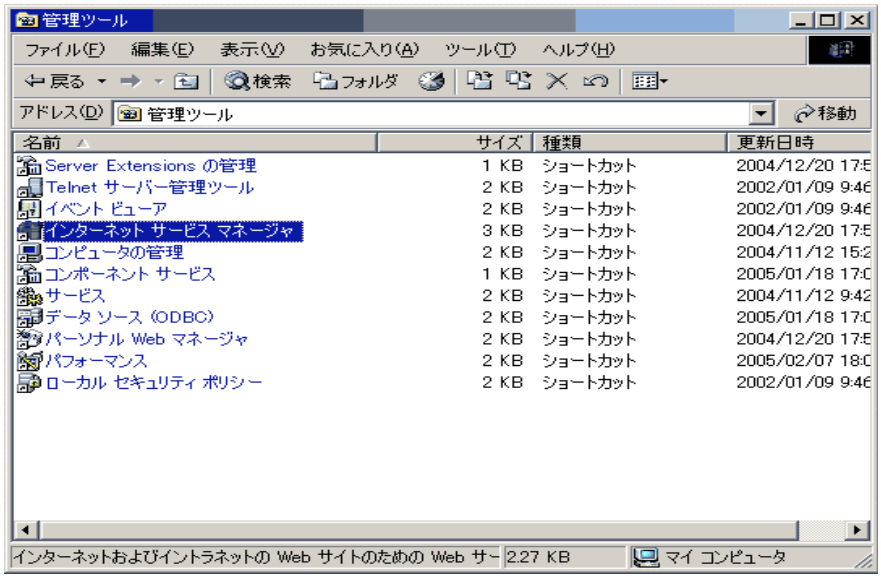
（1）ＯＳのインストール

インストール画面の指示に従い、Windows をインストールします。

（2）前提ソフトウェアの確認とインストール

＜Web サーバ＞

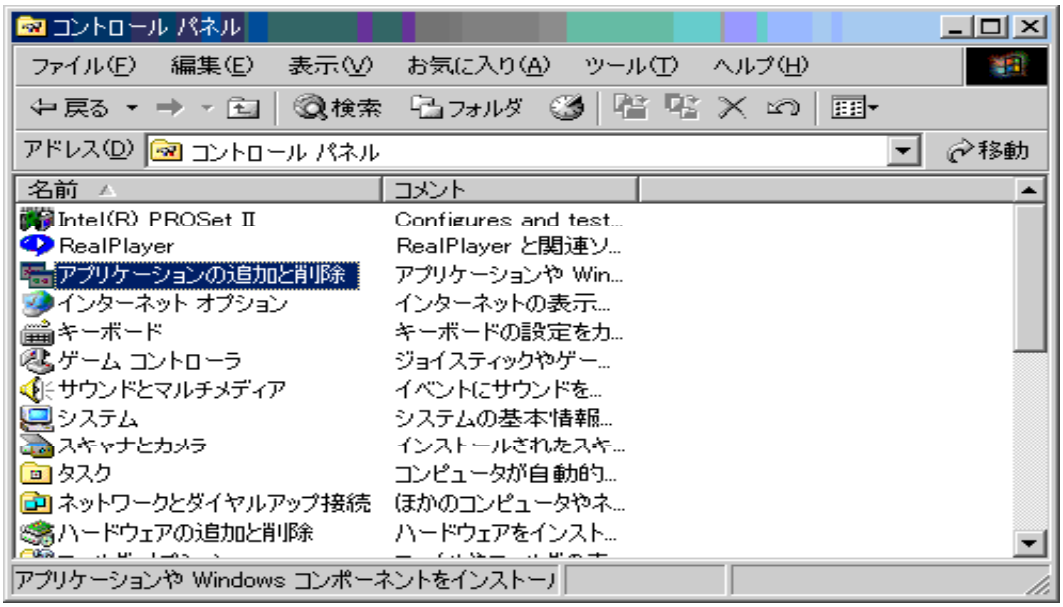
Administrator でログインし、エクスプローラから、「マイコンピュータ」→「コントロールパネル」→「管理ツール」を実行します。



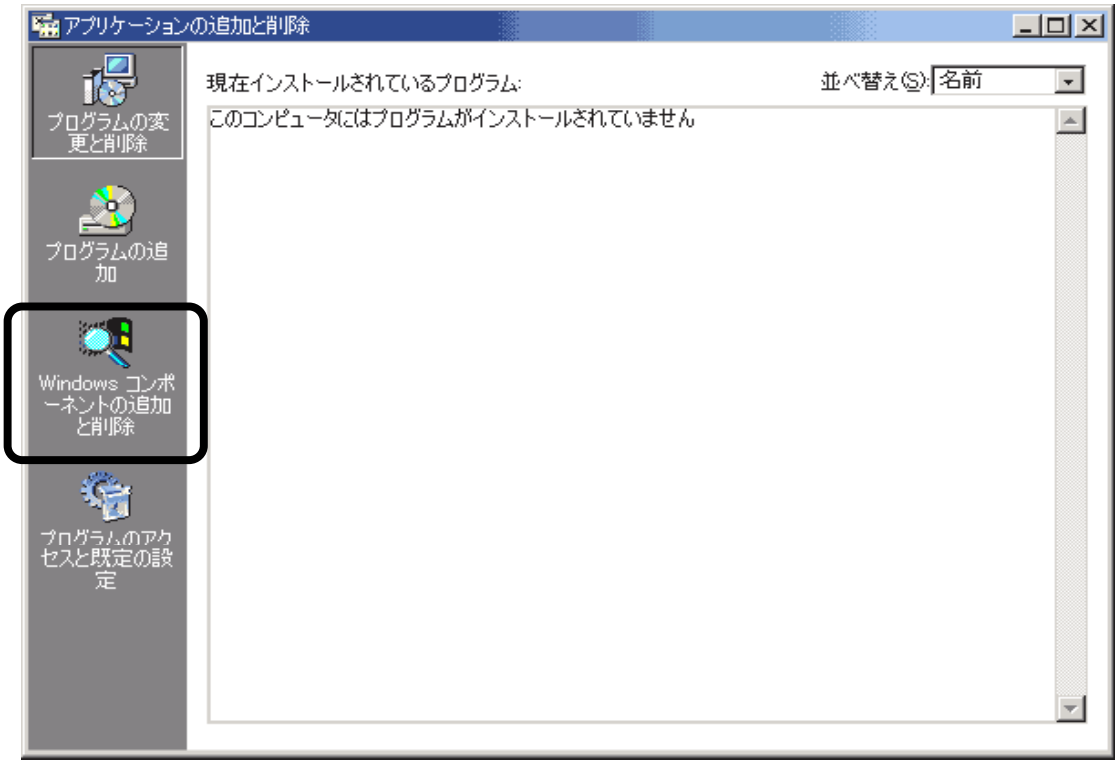
「インターネットサービスマネージャ」が表示されていれば、IIS はインストール済みです。
インストールされていなければ、Windows のインストール CD に格納されていますので、インストールしてください。

・Windows 2000 の場合

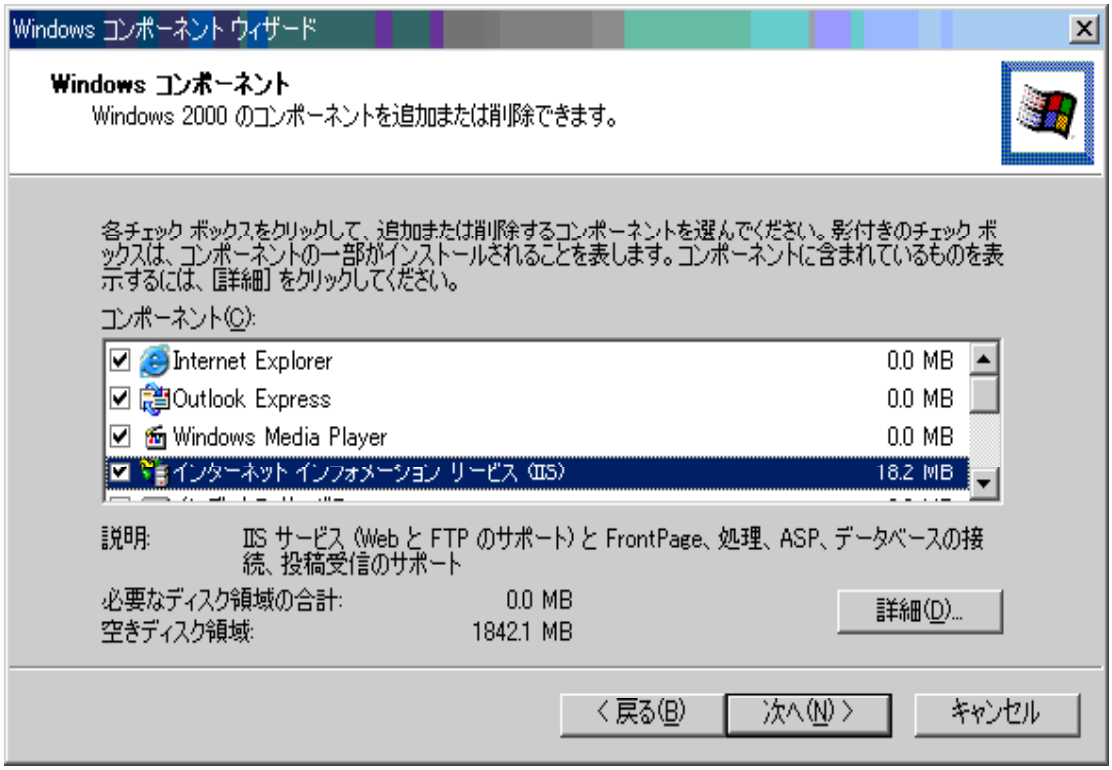
エクスプローラから、「マイコンピュータ」→「コントロールパネル」を実行し、「アプリケーションの追加と削除」を実行してください。（Windows XP、2003 の場合は「プログラムの追加と削除」）



次に、左のメニューから、「Windows コンポーネントの追加と削除」をクリックします。

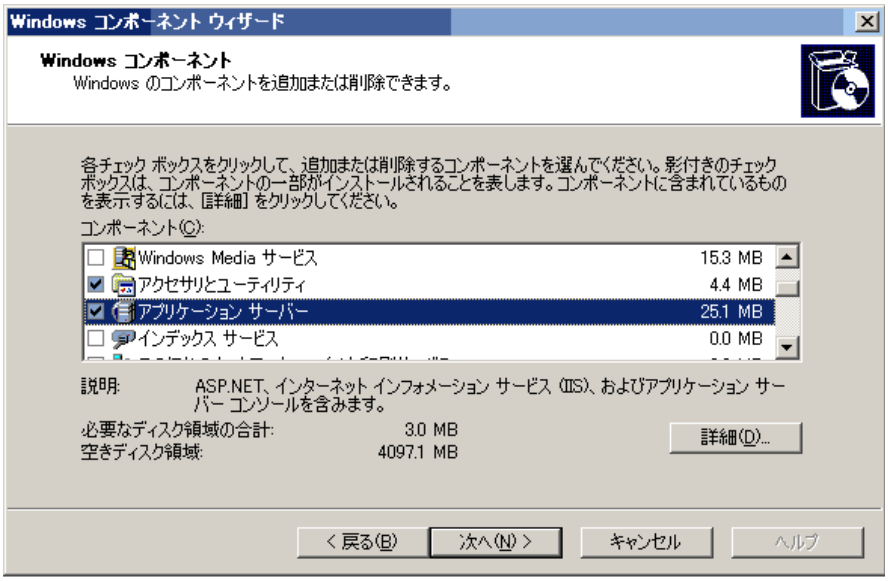


「Windows コンポーネントウィザード」が表示されますので、「インターネットインフォメーションサービス(IIS)」にチェックを入れ、「次へ」をクリックしてください。
これで IIS がインストールされます。

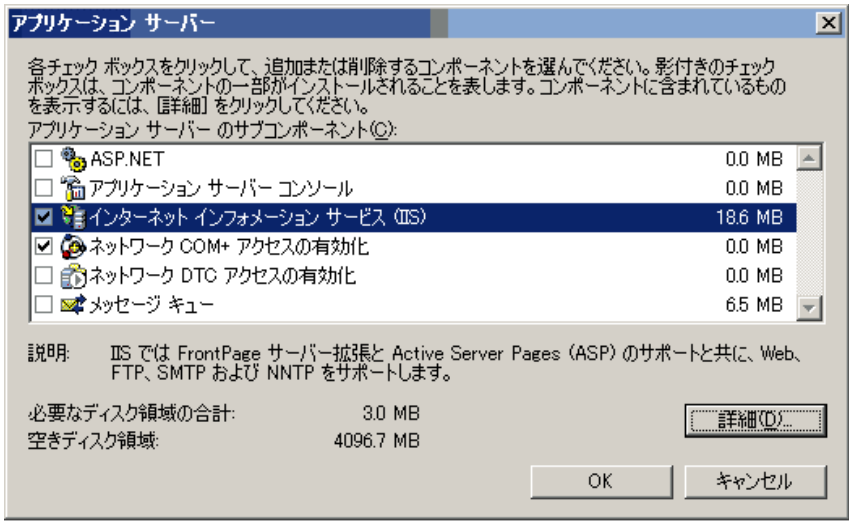


・Windows Server 2003 の場合

Windows 2000、Windows XP の場合と同様に、コントロールパネルから「プログラムの追加と削除」を実行し、「Windows コンポーネントの追加と削除」をクリックします。「Windows コンポーネントウィザード」が表示されますので、「アプリケーションサーバー」を選択し、「詳細」ボタンをクリックします。



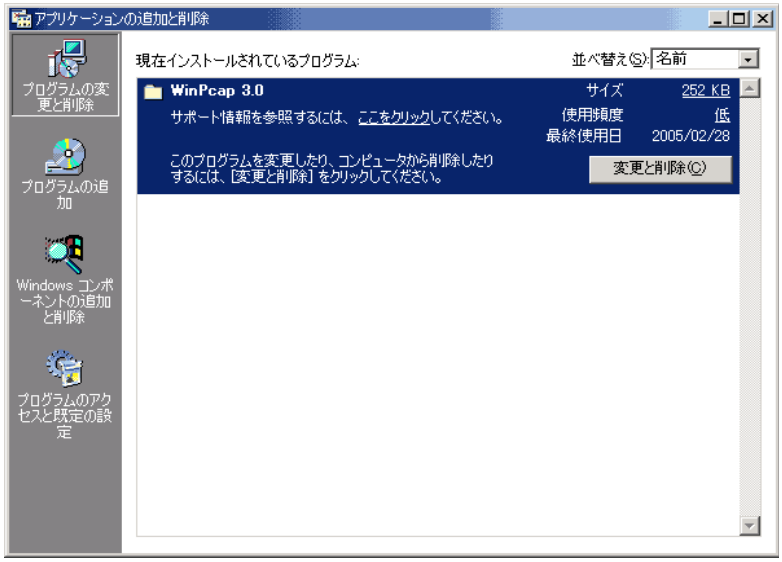
次に、アプリケーションサーバーのサブコンポーネントが表示されますので、「インターネットインフォメーションサービス(IIS)」にチェックを入れ、「OK」をクリックします。



その後、「Windows コンポーネントウィザード」の「次へ」をクリックすると、IIS のインストールが開始されます。

＜WinPcap＞

「スタート」→「設定」→「コントロールパネル」からコントロールパネルをクリックし、Windows 2000 の場合は「アプリケーションの追加と削除」、Windows XP、Windows Server 2003 の場合は「プログラムの追加と削除」を実行します。



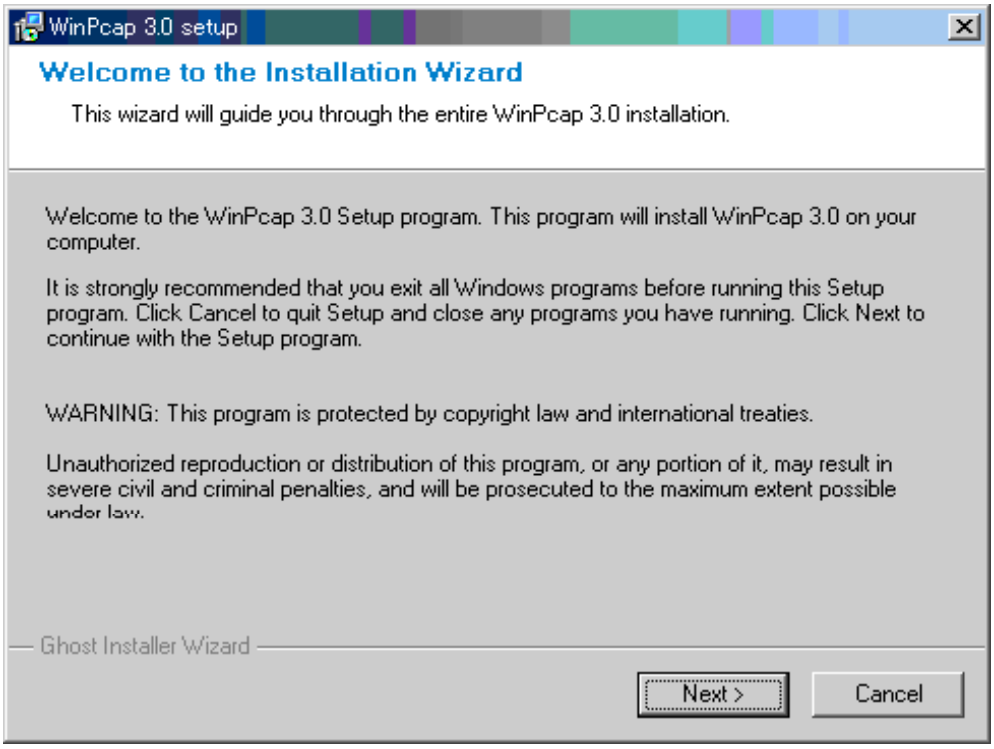
ここで、「WinPcap 3.0」と表示されていれば、WinPcap はインストール済みです。

インストールされていなければ、NX NetMonitor の提供媒体に格納されていますので、以降の手順に従い、インストールしてください。

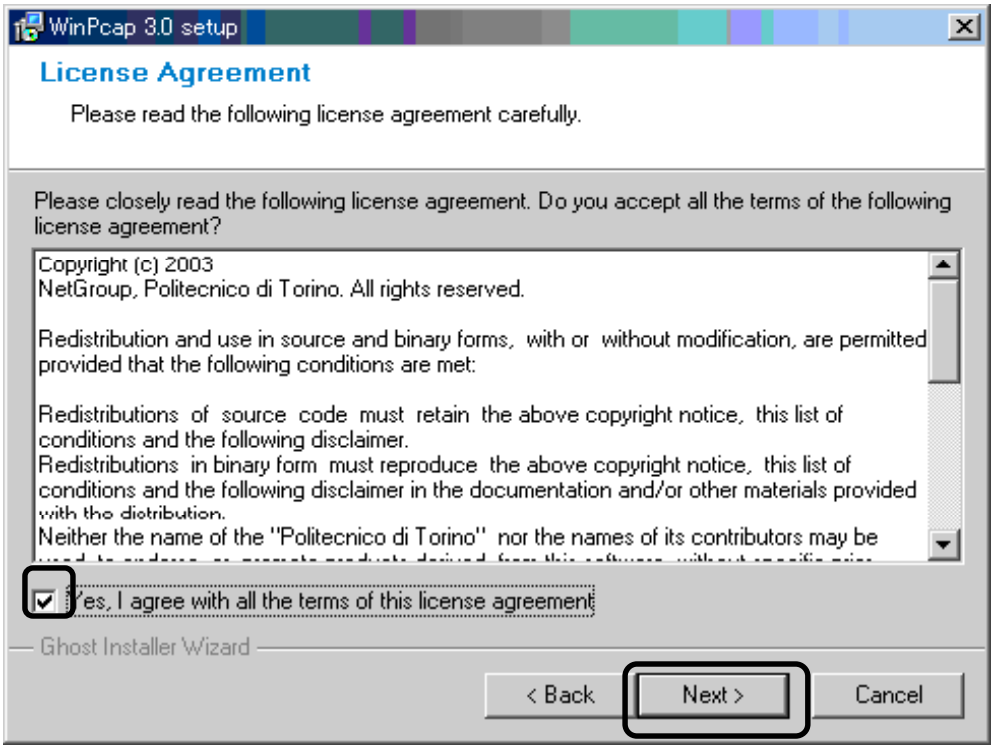
・WinPcap のインストール手順

NX NetMonitor の提供媒体を CD ドライブにセットし、エクスプローラから提供媒体内の S749105P 下にある WinPcap_3_0.exe を実行します。

WinPcap_3_0.exe を実行すると、WinPcap のインストーラが起動しますので、「Next」をクリックします。



次に、ライセンスの同意を求められますので、「Yes, I agree with all the terms of this license agreement」にチェックを入れ、「Next」をクリックすると、WinPcap のインストールが開始されます。



（3）NX NetMonitor のインストールと再インストール

Administratorでログインし、下記手順に従い、インストールしてください。
以下の例では、システムドライブをC、CD-ROMドライブをDとします。

① CD-ROMドライブにNX NetMonitor の提供媒体をセットします。

② コマンドプロンプトからCD-ROMドライブに移動します。

```
C:¥> d:
```

③ 提供媒体内の「S749105P」フォルダに移動します。

```
D:¥> cd S749105P
```

④ インストールコマンドを起動します。

```
D:￥S749105p＞ nxnminstall
     ++ NX NetMonitor install start ++
                                :
                                :
                                :
  ++ NX NetMonitor install completed ++
```

上記の例ではC:¥nx¥netmonitor¥agent下にインストールされます。
インストールディレクトリを指定する場合には、nxnminstallコマンドのパラメタにインストールディレクトリを指定してください。
（例：nxnminstall C:¥nx¥netmonitor¥agent）
なお、インストールディレクトリには、スペースが含まれていないディレクトリを指定してください。

⑤ マシンを再起動します。
以上で完了です。

なお、インストールが失敗した場合、以下のように表示されますので、再インストールしてください。

```
D:¥S749105P> nxnminstall
++ NX NetMonitor install start ++
                                :
                                :
++ NX NetMonitor install abnormal end ++
```

NX NetMonitorの再インストールはインストールと同様の手順を行ってください。

「インストール時の注意事項」

・複数 VLAN 構成時、Windows の起動に時間がかかることがあり、起動が全て完了する前にインストールを行うと、NX NetMonitor の登録が失敗することが有ります。登録に失敗した場合、しばらく待って再度インストールを行ってください。
・再インストール時にはネットワーク監視処理が自動的に停止しますのでマシンの再起動をを行ってください。

（4）NX NetMonitor のアンインストール

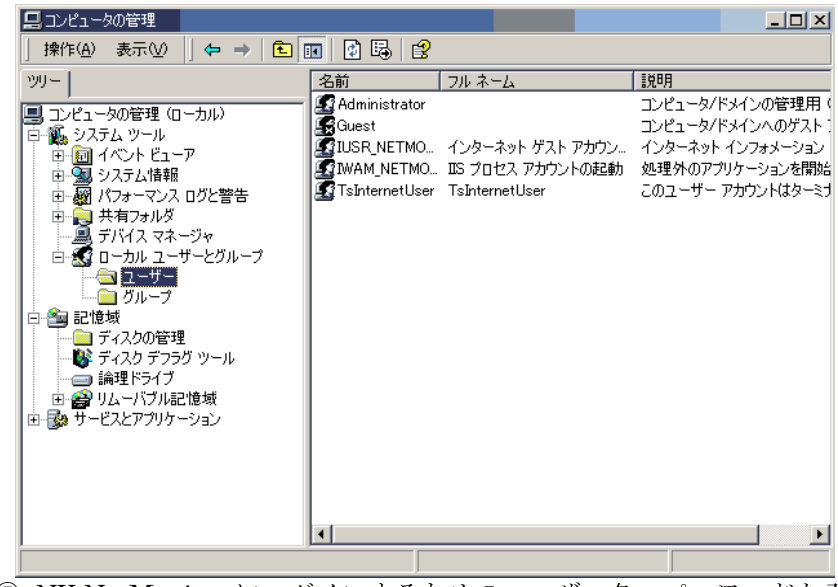
① コマンドプロンプトを起動して以下のオペレーションを行ってください。

```
C:¥ >cd c:¥nx¥netmonitor¥agent¥bin
C:¥nx¥netmonitor¥agent¥bin >nxnmuninstall.bat
++ NX NetMonitor uninstall start ++
                    :
                    :
++ NX NetMonitor uninstall completed ++
```

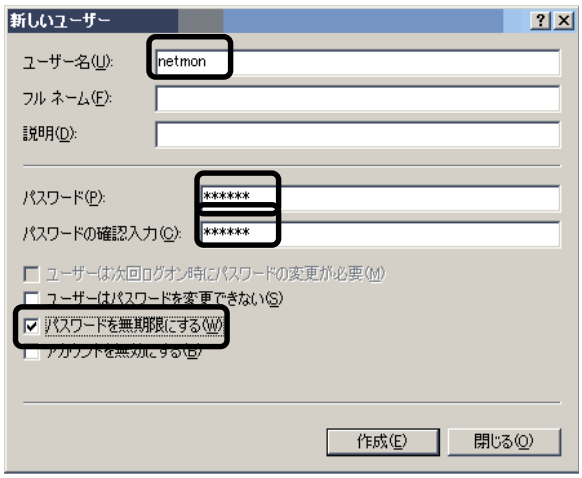
（5）ユーザーの作成

Web ブラウザで NX NetMonitor にアクセスする際のユーザーを作成します。
以下の手順に従い、設定を行ってください。

① エクスプローラから、「マイコンピュータ」→「コントロールパネル」を起動します。
② コントロールパネル内の「管理ツール」を起動します。
③ 管理ツール内の「コンピュータの管理」を起動します。
④ 「システムツール」→「ローカルユーザーとグループ」→「ユーザー」を選択し、「操作」メニューから「新しいユーザー」をクリックします。



⑤ NX NetMonitor にログインするためのユーザー名、パスワードを入力します。また、「ユーザーは次回ログオン時にパスワードの変更が必要」のチェックをはずし、「パスワードを無期限にする」のチェックを入れ、「作成」ボタンをクリックします。
（下のウィンドウでは、ユーザ：netmon を作成）



⑥ NX NetMonitor へのユーザ登録

Web 監視画面にアクセスする管理者ユーザを NX NetMonitor に登録してください。
管理者ユーザ以外に参照限定ユーザも登録することが出来ます。
NX NetMonitor のバージョン 07-04 以前では、nxnmsetup.bat で NX NetMonitor のユーザを登録した場合でも、Windows へログインできるユーザは NX NetMonitor の Web 監視画面にアクセスすることが可能でした。NX NetMonitor のバージョン 07-04 以降から、セキュリティを強化し、NX NetMonitor のユーザとして登録したユーザ以外は、Web 監視画面にアクセスできないように制限する機能をサポートしてます。

・登録方法

nxnmsetup.bat を実行して、ユーザーの登録を行います。管理者ユーザと参照限定ユーザをそれぞれ 1 つだけ登録することができます。

(1) 管理者ユーザ netmon を登録する例を示します。

```
prompt> cd c:¥nx¥netmonitor¥agent¥bin
prompt> nxnmsetup.bat netmon
++ setup user[netmon]
++ NX NetMonitor setup comleted ++
```

(2) 管理者ユーザ netmon と参照限定ユーザ user1 というユーザーを登録する例を示します。
参照限定ユーザは –user オプションの後に指定します。
参照限定ユーザも、「(５) ユーザーの作成」の ④、⑤の操作を行い、Windows ユーザを作成しておいてください。

```
prompt> cd c:¥nx¥netmonitor¥agent¥bin
prompt> nxnmsetup.bat netmon –user user1
++ setup user[netmon]
++ setup user[user1]
++ NX NetMonitor setup comleted ++
```

(3) 管理者ユーザ netmon と参照限定ユーザー user1 を netmon2 と user2 に変更する例を示します。
ユーザを変更する時には、-pwd オプションを指定します。

```
prompt> cd c:¥nx¥netmonitor¥agent¥bin
prompt> nxnmsetup.bat netmon2 –user user2 -pwd
++ NX NetMonitor setup comleted ++
```

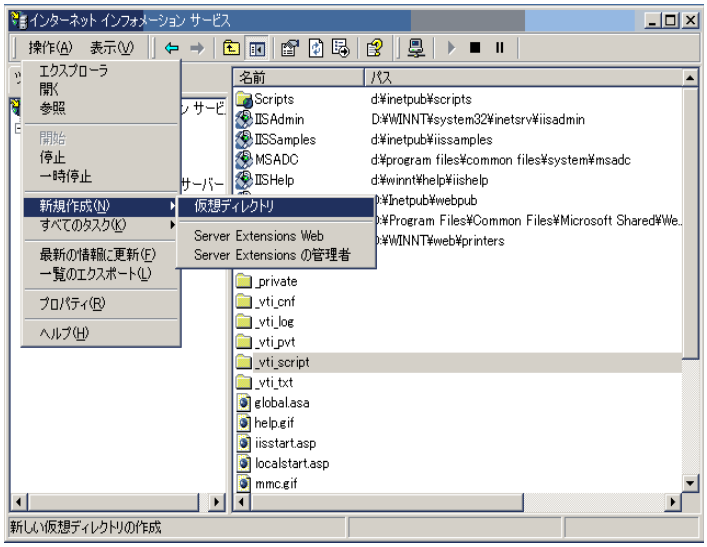
nxnmsetup.bat コマンドでユーザ登録を行わなかった場合、Windows のログインユーザは NX NetMonitor の Web 監視画面にアクセスすることが出来ます。

参照限定ユーザの場合の監視画面は「６．２１　ユーザー権限の付与」を参照してください。

（6）IIS の設定

Web ブラウザから NX NetMonitor にアクセスするには、IIS の設定を行う必要があります。以下の手順に従い、IIS の設定を行ってください。

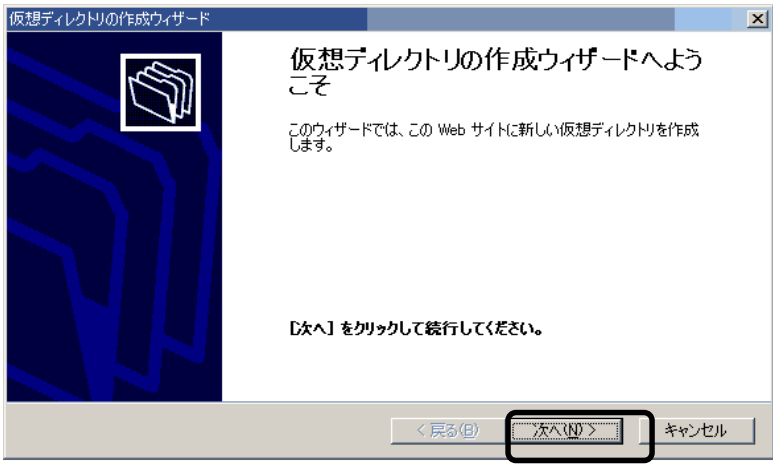
① エクスプローラから、「マイコンピュータ」→「コントロールパネル」を起動します。
② コントロールパネル内の「管理ツール」を起動します。
③ 管理ツール内の「インターネットサービスマネージャ」を起動します。
（IIS 5.X の場合は「インターネットインフォメーションサービス」、
IIS 6.0 の場合は「インターネットインフォメーションサービス(IIS)マネージャ」）



上図のウィンドウが表示されたら、左のツリーの「PC 名称」→「既定の Web サイト」を選択します。（IIS 6.0 の場合は「PC 名称」→「Web サイト」→「既定の Web サイト」）

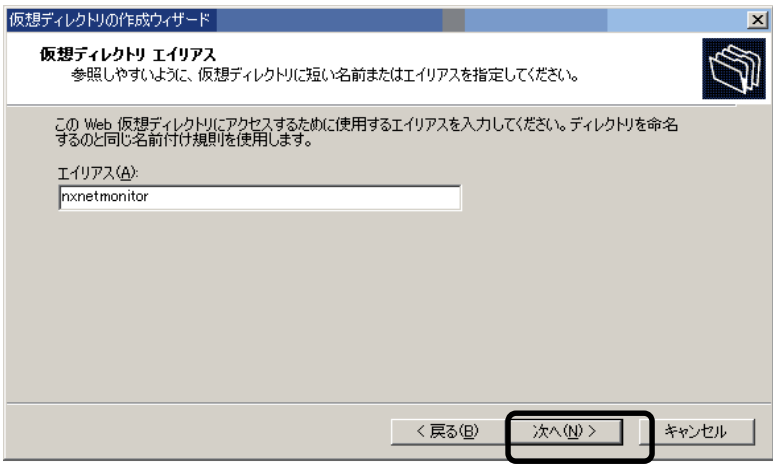
次に、「操作」メニューをクリックし、「新規作成」→「仮想ディレクトリ」を選択します。

④ その後、仮想ディレクトリの作成ウィザードが起動しますので、ウィザードの指示に従い、仮想ディレクトリの設定を行います。

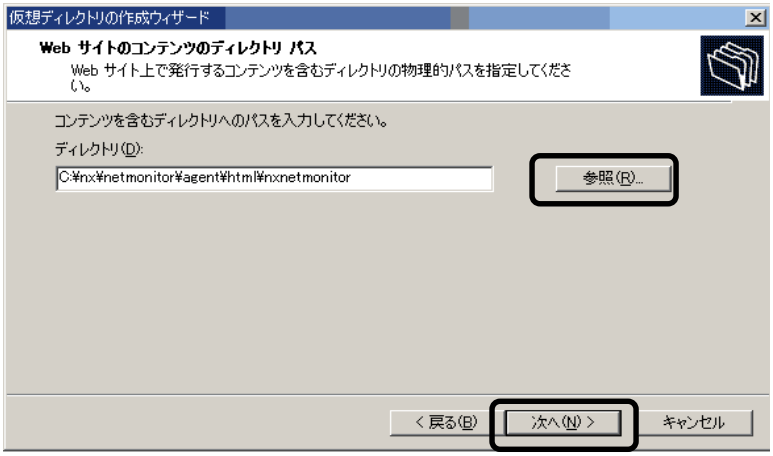


「次へ」をクリックします。

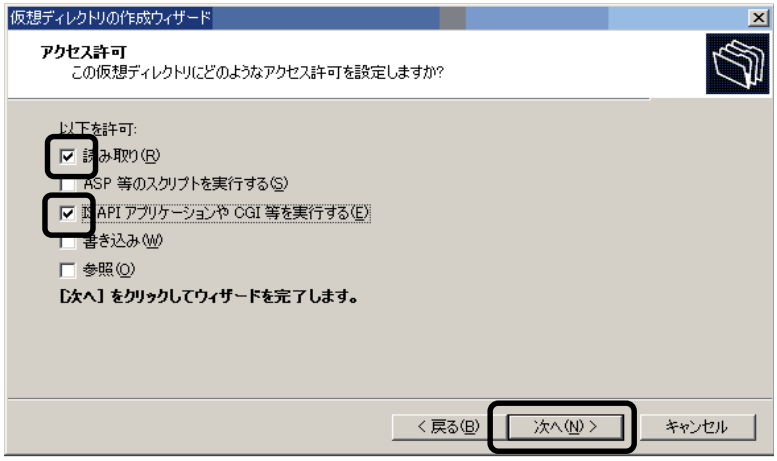
⑤ 仮想ディレクトリのエイリアスを入力します。エイリアスに nxnetmonitor と入力し、「次へ」をクリックします。



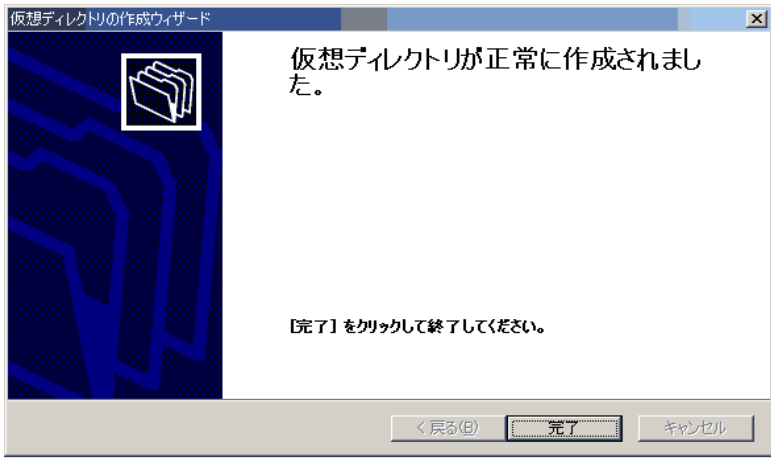
⑥ ⑤で入力した仮想ディレクトリに関連付ける物理パスを指定します。ディレクトリは、「参照」ボタンから インストールディレクトリ¥html¥nxnetmonitor を選択し、「次へ」をクリックします。
（下のウィンドウのインストールディレクトリは C:¥nx¥netmonitor¥agent）



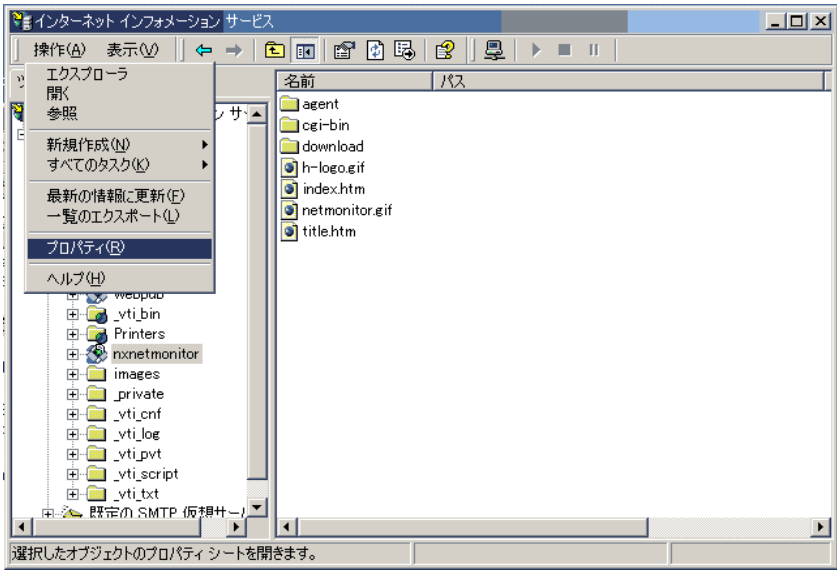
⑦ 次に、設定する仮想ディレクトリのアクセス権を指定します。「読み取り」と「ISAPI アプリケーションや CGI 等を実行する」にチェックを入れます。



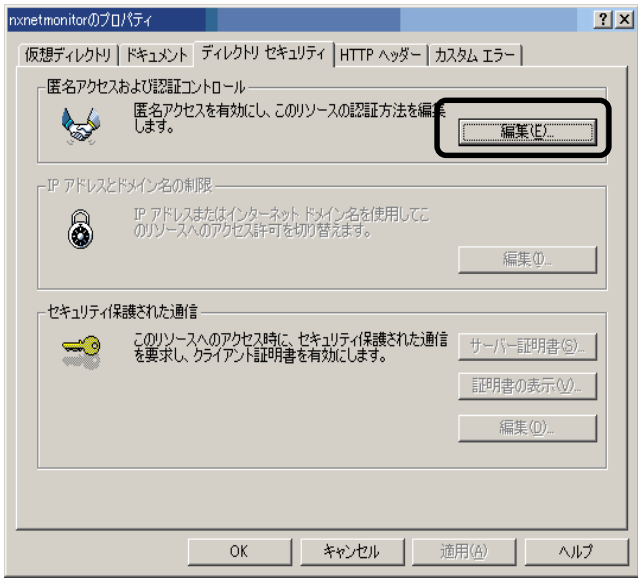
⑧ 以下のウィンドウが表示されれば、仮想ディレクトリの設定は終了です。



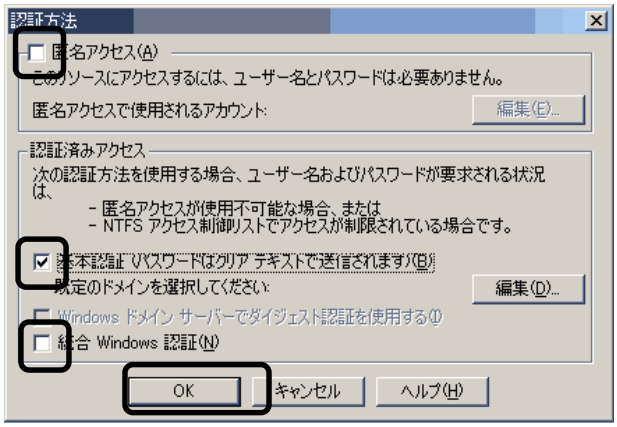
⑨ 次に、認証の設定を行います。インターネットサービスマネージャ内の「既定の Web サイト」→「nxnetmonitor」を選択し、「操作」メニューの「プロパティ」をクリックします。



⑩ 「ディレクトリセキュリティ」タブをクリックし、「匿名アクセスおよび認証コントロール」内の「編集」ボタンをクリックします。



⑪ 「匿名アクセス」、「統合 Windows 認証」のチェックをはずし、「基本認証」にチェックを入れ、「OK」ボタンをクリックします。



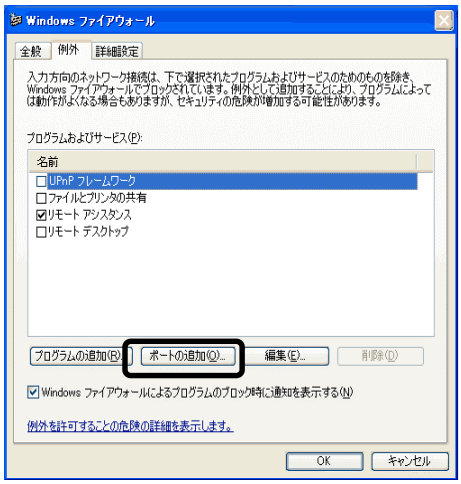
（7）その他の設定

・Windows XP SP2 および Windows 2003 Server SP1 の場合

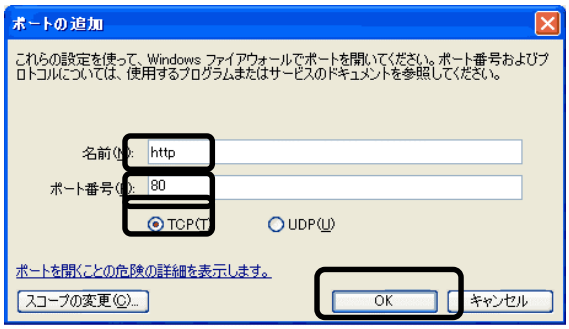
＜Windows ファイアウォールの設定＞

Windows XP SP2 および Windows 2003 Server SP1 以降では、Web アクセスを行うため、ファイアウォールの設定が必要となります。
以下の手順に従い、ファイアウォールの設定を行ってください。

① エクスプローラから、「マイコンピュータ」→「コントロールパネル」を起動します。
② コントロールパネル内の「Windows ファイアウォール」を起動します。
③ Windows ファイアウォール ダイアログボックスの「例外」タブをクリックします。
④ 「ポートの追加」ボタンをクリックします。



⑤ 名前に任意の名称(下のウィンドウでは http)、ポート番号に 80、プロトコルに TCP を指定し、「OK」ボタンをクリックします。



以上で、Windows ファイアウォールの設定は終了です。

・IIS 6.0 の場合

＜Web サービス拡張、MIME の設定＞

IIS6.0 では、NX NetMonitor にアクセスするため、Web サービス拡張、MIME(MultiPurpose Internet Mail Extensions)の設定が必要となります。

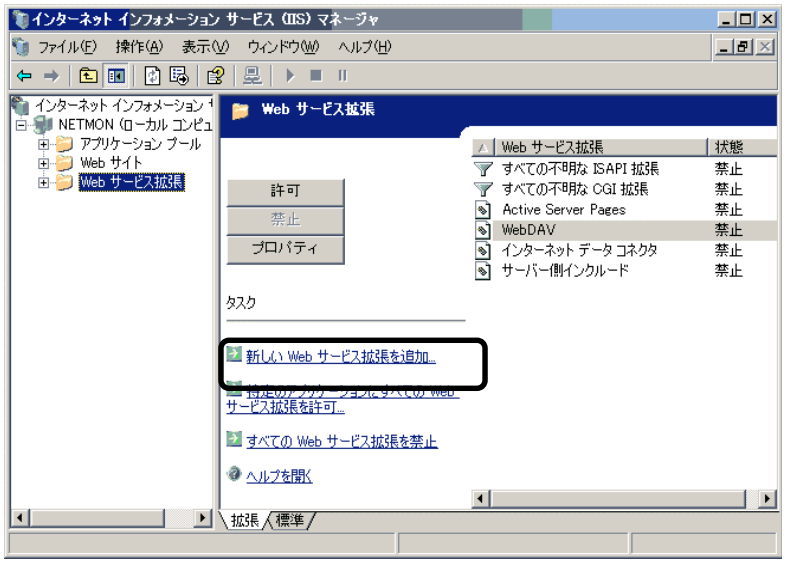
以下の手順に従い、設定を行ってください。

・Web サービス拡張の設定

① エクスプローラから、「マイコンピュータ」→「コントロールパネル」→「管理ツール」を起動します。

② 管理ツール内の「インターネットインフォメーションサービス(IIS)マネージャ」を起動します。

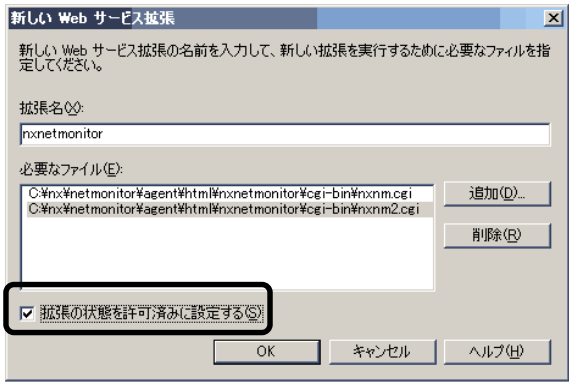
③ 「Web サービス拡張」を選択し、「新しい Web サービス拡張を追加」をクリックします。



④ 新しく登録する Web サービス拡張名と必要なファイルを入力します。

拡張名には nxnetmonitor と入力し、必要なファイルには「追加」ボタンをクリックし、以下のファイルを選択してください。

インストールディレクトリ¥html¥nxnetmonitor¥cgi-bin¥nxnm.cgi
インストールディレクトリ¥html¥nxnetmonitor¥cgi-bin¥nxnm2.cgi



以上を入力し、「拡張の状態を許可済みに設定する」にチェックを入れ、「OK」ボタンをクリックします。

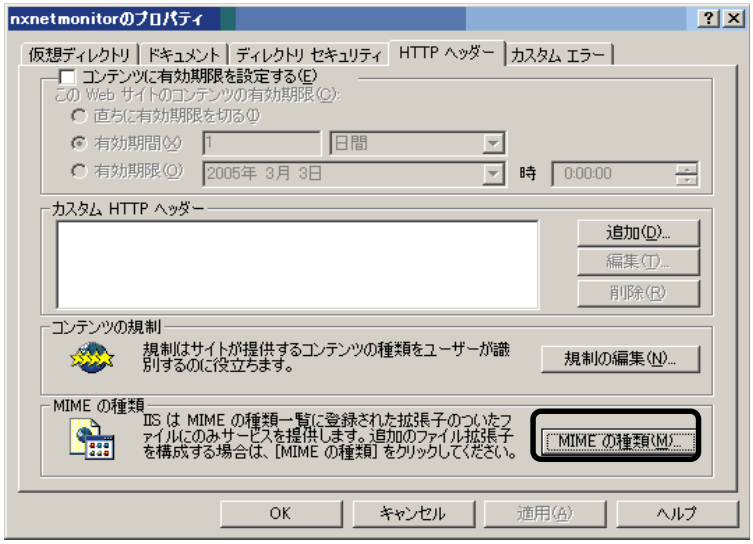
・MIME の設定

① エクスプローラから、「マイコンピュータ」→「コントロールパネル」→「管理ツール」を起動します。

② 管理ツール内の「インターネットインフォメーションサービス(IIS)マネージャ」を起動します。

③ 「Web サイト」→「既定の Web サイト」→「nxnetmonitor」を選択し、「操作」メニューから「プロパティ」をクリックします。

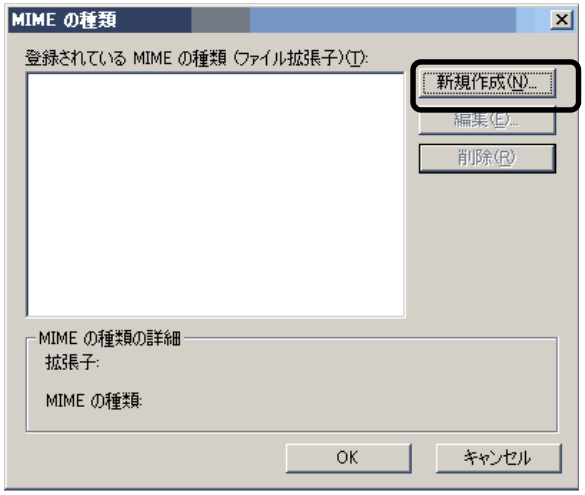
④ 「HTTP ヘッダー」タブの「MIME の種類」内の「MIME の種類」ボタンをクリックします。

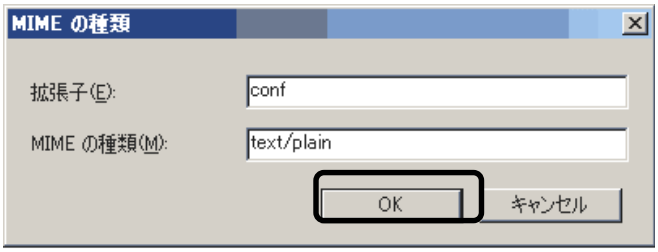


⑤ 新しく表示されたウィンドウの「新規作成」ボタンをクリックします。
新しく登録する MIME の種類を入力するウィンドウが表示されますので、

拡張子　：conf
MIME の種類：text/plain

と入力し、「OK」ボタンをクリックします。





以上で Web サービス拡張、MIME の設定は終了です。

6. 操作方法

この章では、不正持込み＆強制排除システムの監視画面の操作方法について説明しています。

6.1 操作手順一覧

操作手順は、以下の通りです。
＜操作手順一覧 (1/3)＞

No	項目	操作内容
1	Web ブラウザから監視装置へ接続	「６．３ 監視装置への接続」または「６．６ 監視装置への接続２」を参照してください。
2	監視装置、監視ネットワークの登録	「６．４ 監視装置の登録」または「６．７ 監視対象ネットワークの登録」を参照してください。 なお、統合管理ツール(NX NetMonitor/Manager)を使用する場合には、監視装置や監視対象ネットワークを登録する必要はありません。その場合には、統合管理ツールに監視装置やネットワークを登録してください。
3	監視画面の表示	「６．５ 監視画面の表示」または「６．１０ 監視対象ネットワークの表示」を参照してください。
4	監視の設定	「６．１６ 環境設定」で下記を設定してください。 以下の①、②および③の設定は、必須です。 ①監視モードで「ネットワークの監視を行う」選択する。 ②動作モードで「通常(許可機器一覧を使用する)」または「簡易(排除機器一覧を使用する)」を選択してください。 ③排除モードで「検出のみ行う」または「検出・排除ともに行わない」を選択してください。 次の ④および⑤は、必要に応じて設定してください。 ④トラップ情報(独自)で、「送信先 IP アドレス」および「送信先ポート番号」を設定してください。 ⑤トラップ情報(SNMP)で、「送信先 IP アドレス」および「コミュニティ名」を設定してください。 その他の設定は「６．１６ 環境設定」を参照してください。 その後、すぐに監視処理を動作させたい場合、「変更＆監視処理起動」をチェックして「更新」ボタンをクリックしてください。また、「変更のみ」をチェックして「更新」ボタンをクリックすると、ネットワークの監視を行う設定ができます。だたし、この時点では、監視処理は開始されていません。 なお、「変更&再読み込み」をチェックした場合、エラーとなりますが、監視処理が起動されていないためで、問題ありません。
5	監視処理の起動	「６．２１ その他メニュー」の「監視処理の起動」をチェックして、「実行」ボタンクリックすると監視処理が手動にて起動できます。

＜操作手順一覧 (2/3)＞

No	項目		操作内容
6	スイッチ情報の設定		位置特定を行わない場合には、設定不要です。 「６．１４　スイッチ情報の表示」を参照して設定してください。 スイッチ情報が設定されていなくても「環境設定」の「不正機器特定情報」の「コミュニティ名」が指定されていると、NX NetMonitor は、不正機器位置情報を自動で検出します。NX NetMonitor が自動で検出できるスイッチは、監視対象ネットワークの IP アドレスを持ち（接続機器一覧の表示されている)、「環境設定」の「不正機器特定情報」の「コミュニティ名」で MIB 情報を収集できるスイッチです。 NX NetMonitor がスイッチ情報を検出できない場合には、不正接続された PC の位置特定情報を表示できません。スイッチを検出していても、情報を表示できない場合には、位置特定できていないか、上位のスイッチと認識されている場合があります。 スイッチを定義するためのメニューは、環境設定画面で、「不正機器特定情報」にコミュニティ名を設定している時に表示されます。 NX NetMonitor が認識しているスイッチの情報は「その他」メニューのスイッチ情報から確認することができます。
7	ネットワーク接続の許可・拒否の設定		動作モードで「通常(許可機器一覧を使用する)」を選択した場合は、”許可機器の登録方法”を参照してください。 動作モードで「簡易(排除機器一覧を使用する)」を選択した場合は、”排除機器の登録方法”を参照してください。また簡易モードでの操作は「６．２０　簡易モード」を参照してください。
8	不正機器強制排除の設定		「６．１６ 環境設定」で、監視モードを「不正機器を検出したら排除する」選択して、「更新」ボタンをクリックすると、強制排除が開始されます。
9	手動による接続許可・拒否	手動による拒否	「６．１１ 接続機器一覧の表示」にて、拒否したい機器をチェックして、「拒否」ボタンをクリックすると、ネットワークから一時的に切り離されます。
10		手動による許可	「６．１２ 拒否機器一覧の表示」にて、許可したい機器をチェックして、「許可」ボタンをクリックすると、ネットワークへの接続が一時的に可能になります。
11	ネットワーク接続の許可・拒否の設定の変更		動作モードで「通常(許可機器一覧を使用する)」を選択した場合は、”許可機器の登録方法”を参照してください。 動作モードで「簡易(排除機器一覧を使用する)」を選択した場合は、”排除機器の登録方法”を参照してください。また簡易モードでの操作は「６．２０　簡易モード」を参照してください。
12	接続機器の確認		「６．１１ 接続機器一覧の表示」により、現在ネットワークに接続している機器の一覧が表示されます。
13	拒否機器の確認		「６．１２ 拒否機器一覧の表示」により、現在ネットワークへの接続が拒否されている機器の一覧が表示されます。

＜操作手順一覧 (3/3)＞

No	項目	操作内容
14	ネットワーク接続の許可・拒否の設定の参照	動作モードで「通常(許可機器一覧を使用する)」を選択した場合は、「６．１３ 許可機器/固定機器の表示」により、現在の、許可機器の一覧、固定機器の一覧が表示されます。 動作モードで「簡易(排除機器一覧を使用する)」を選択した場合は、「６．２０ 簡易モード」の排除機器一覧により、現在の、排除機器一覧が表示されます。
15	ログの確認	「６．１５ ログ表示」にて、不正機器の検出、切り離し、許可などのログが表示されます。
16	スイッチ情報の確認	「６．２２ その他メニュー」の「スイッチ情報」で NX NetMonitor が認識しているスイッチ情報の一覧が表示されます。「UNKNOWN」と表示されているものがあれば、定義が誤っている可能性がありますので、スイッチ一覧の定義情報を見直してください。 スイッチ情報を参照するための「スイッチ情報」は、、環境設定画面で、「不正機器特定情報」にコミュニティ名を設定している時に表示されます。
17	不正接続統計情報の確認	「６．２２ その他メニュー」の「不正接続統計」で NX NetMonitor が検出した不正接続 PC の検出回数を日、週、月単位に表示します。
18	バージョン情報の確認	「６．２２ その他メニュー」を参照してください。

6.2 機器の登録

＜許可機器の登録方法＞

許可機器一覧の登録方法は以下の４つがあります。いずれかの方法で許可機器一覧を登録してください。

なお、許可機器とは、固定機器以外のクライアント PC などを意味します。
固定機器とは、ルータ、プリンタ、サーバ等の機器を意味します。固定機器一覧の登録は、必須ではありません。固定機器一覧を作成せず、固定機器と許可機器を１つのファイルにまとめて、許可機器一覧として登録しても問題ありません。

No	登録方法	操作内容
1	Web ブラウザから許可機器一覧、および固定機器一覧を編集	「６．１９ ブラウザからの直接編集機能」にて Web ブラウザから直接、許可機器一覧または、固定機器一覧を編集します。
2	手動で許可機器一覧ファイルおよび固定機器一覧ファイルを登録	「６．１８ アップロード」にて、作成した許可機器一覧、または固定機器一覧のファイル名を指定して、「アップロード」ボタンをクリックすると、登録されます。
3	現在ネットワークに接続している PC から自動的に、許可機器一覧を作成	「６．１１ 接続機器一覧の表示」にて、「許可機器一覧の新規作成」ボタンをクリックすると、現在、ネットワークに接続している機器が全て許可機器一覧に登録されます。
4	統合管理ツールから許可機器一覧、および固定機器一覧を編集登録	統合管理ツールの接続機器、拒否機器、許可機器、固定機器画面を右クリックして編集登録が可能です。 詳細は「統合管理機能 NX NetMonitor/Manager」のマニュアルを参照してください。

＜排除機器の登録方法＞

排除機器一覧の登録方法は以下の３つがあります。いずれかの方法で排除機器一覧を登録してください。なお、排除機器とは、排除すべき PC を意味します。

No	登録方法	操作内容
1	Web ブラウザから排除機器一覧を登録	「６．１９ ブラウザからの直接編集機能」にて Web ブラウザから直接、排除機器一覧を作成します。
2	手動で排除機器一覧を登録	「６．１８ アップロード」にて、作成した排除可機器一覧のファイル名を指定して、「アップロード」ボタンをクリックすると、登録されます。
3	統合管理ツールから排除機器一覧を編集登録	統合管理ツールの接続機器、拒否機器、排除機器画面を右クリックして編集登録が可能です。 詳細は「統合管理機能 NX NetMonitor/Manager」のマニュアルを参照してください。

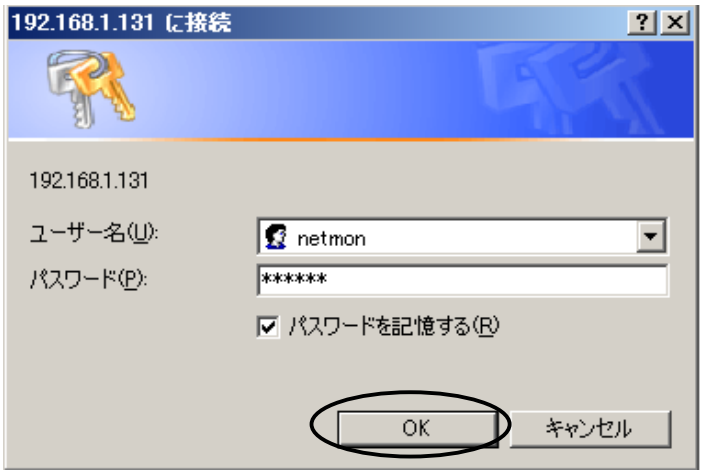
6.3　監視装置への接続

監視装置への接続は、Web ブラウザから、下記 URL にアクセスしてください。

URL：http://**監視装置の IP アドレス**/nxnetmonitor/index.htm

1）Web ブラウザを開き、URL を入力します。
監視装置の IP アドレスが、192.168.1.131 の場合、下記のように入力します。

2）URL を入力すると、ログイン画面が表示されます。
ユーザー名、パスワードを入力し、「OK」ボタンをクリックします。



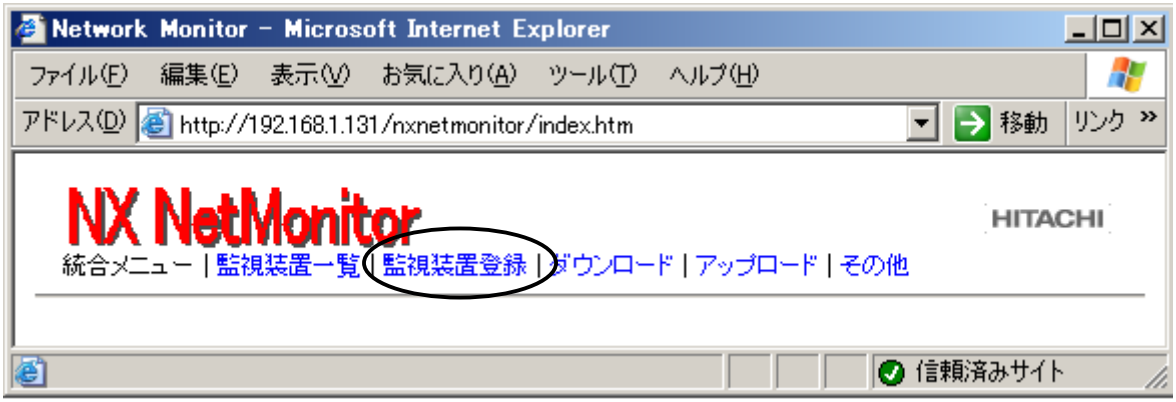
3）統合メニュー画面が表示されます。

管理者用 PC から監視装置が監視しているネットワークの IP アドレスに直接アクセスできない場合には、「６．６監視装置への接続２」を参照してください。

6.4　監視装置の登録

監視装置登録画面にて、登録を行います。

1）「監視装置登録」をクリックし、登録画面を表示します。



2）監視装置の IP アドレス、説明を入力して、「登録」ボタンをクリックします。

3）監視装置が監視する監視装置の IP アドレスが登録されます。

なお、登録した監視装置の情報はダウンロード、アップロードも可能です。
CSV 形式で、

IP アドレス, コメント

となります。
また、ファイルは Microsoft(R) Windows(R) の搭載された PC での参照・編集を前提としています。
（文字コードは Shift-JIS、改行コードは CRLF）
監視装置一覧で、説明や IP アドレスを修正する場合には、CSV 形式のファイルを一旦ダウンロードし、変更点を修正してからアップロードしてください。

6.5　監視装置の表示

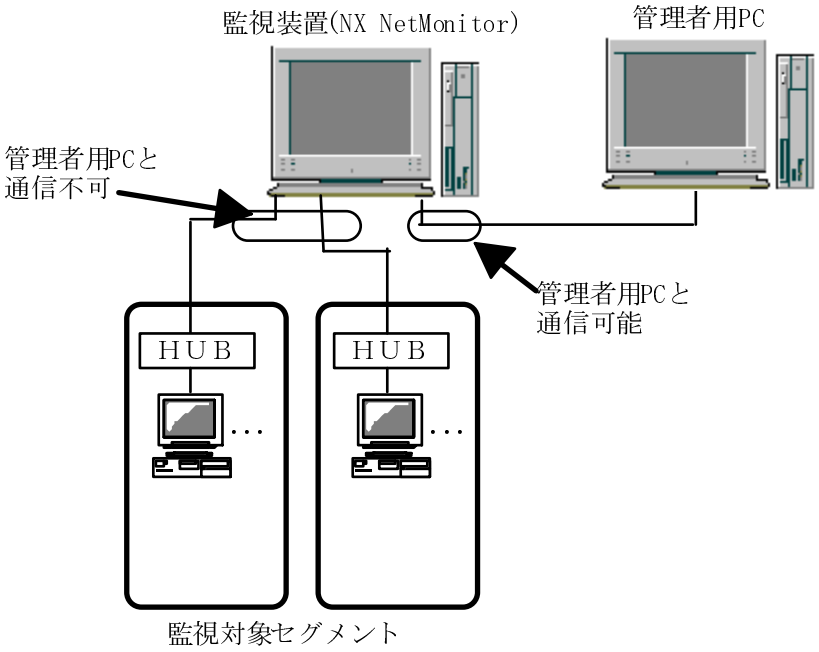
監視装置一覧から、参照したい監視装置の IP アドレスをクリックすると、監視画面が別ウィンドウで開きます。

1）説明欄の監視ネットワーク名称をクリックします。

2）監視ネットワークの監視画面が表示されます。

6.6　監視装置への接続２

管理者用 PC から監視装置が監視しているネットワークと直接通信ができずに、NX NetMonitor が監視しているネットワークの監視画面をひらくことができない場合があります。監視装置に複数のネットワークがあり、そのうちの１つが、管理者用 PC と通信できる場合には、以下のように URL を指定することで、監視対象ネットワークの監視画面をひらくことが出来ます。



Web ブラウザから、下記 URL にアクセスしてください。
URL：http://**管理者用 PC と通信可能な監視装置の IP アドレス**/nxnetmonitor/**index2.htm**

１）Web ブラウザを開き、URL を入力します。
　管理者用 PC と通信可能な監視装置の IP アドレスが 192.168.2.131 の場合、下記のように入力します。

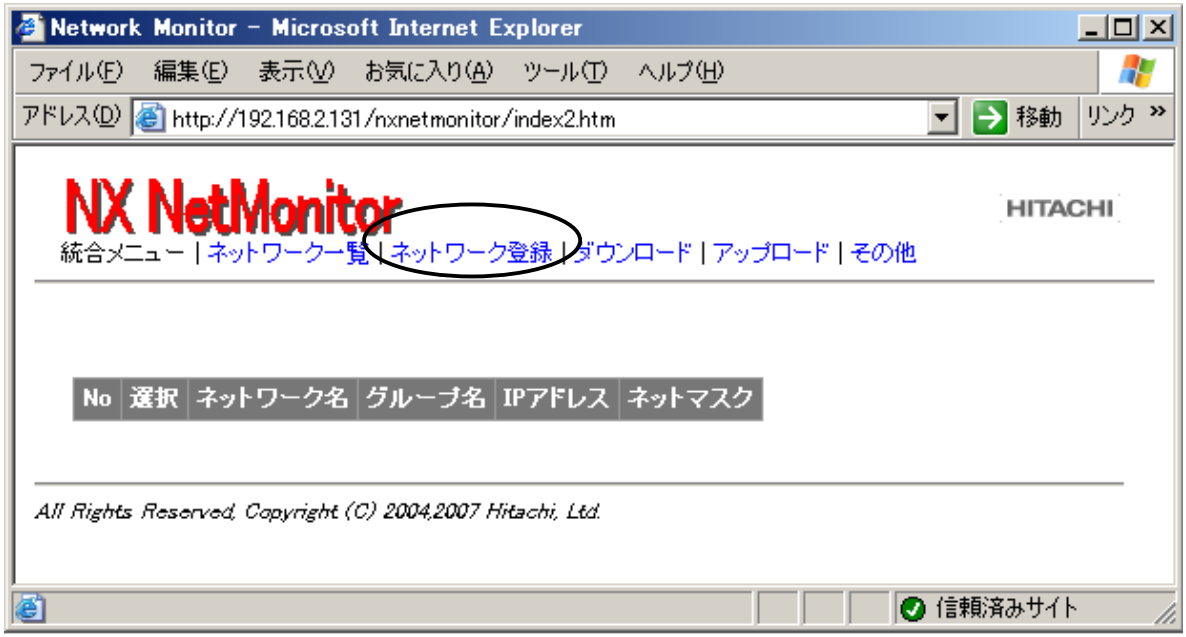
2）URL を入力すると、ログイン画面が表示されます。
ユーザー名、パスワードを入力し、「ＯＫ」ボタンをクリックします。

3）統合メニューの管理画面が表示されます。

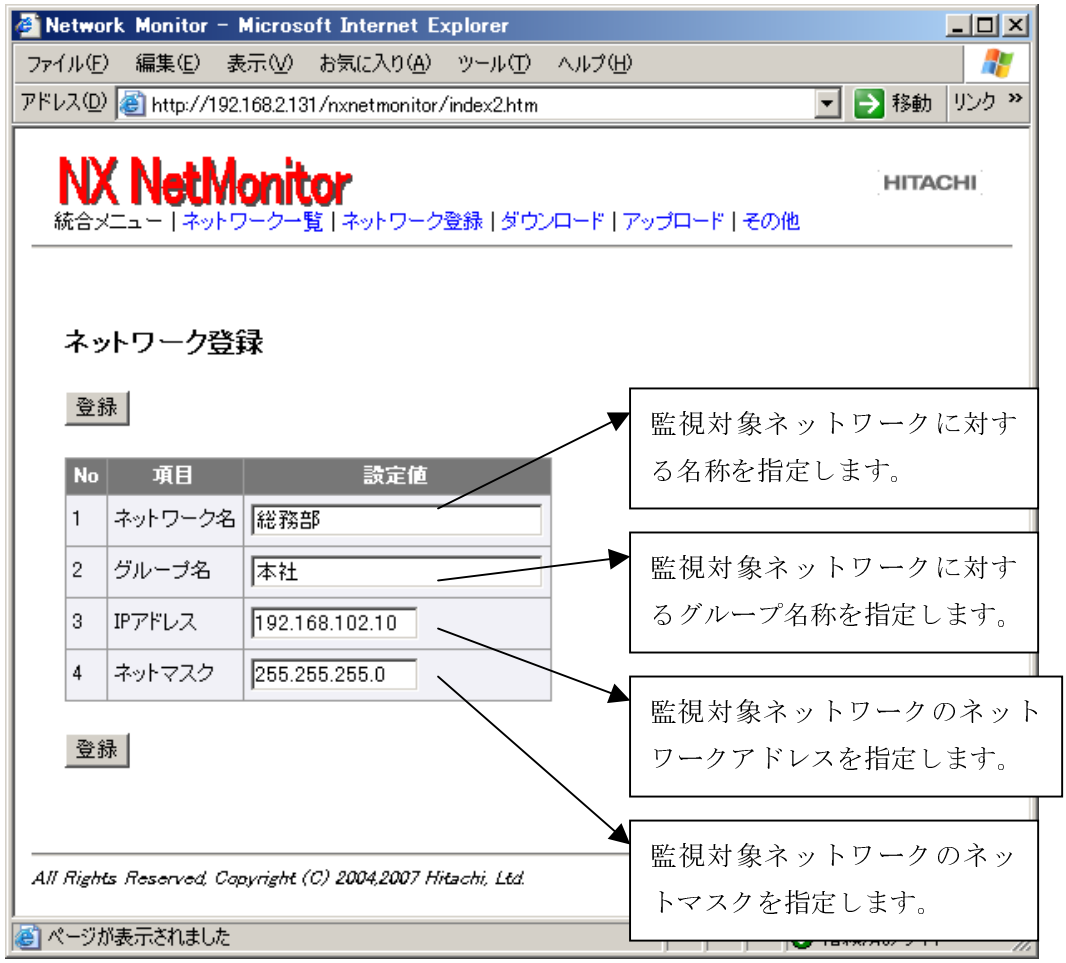
6.7　監視対象ネットワークの登録

ネットワーク登録画面にて、監視対象ネットワークの登録を行います。

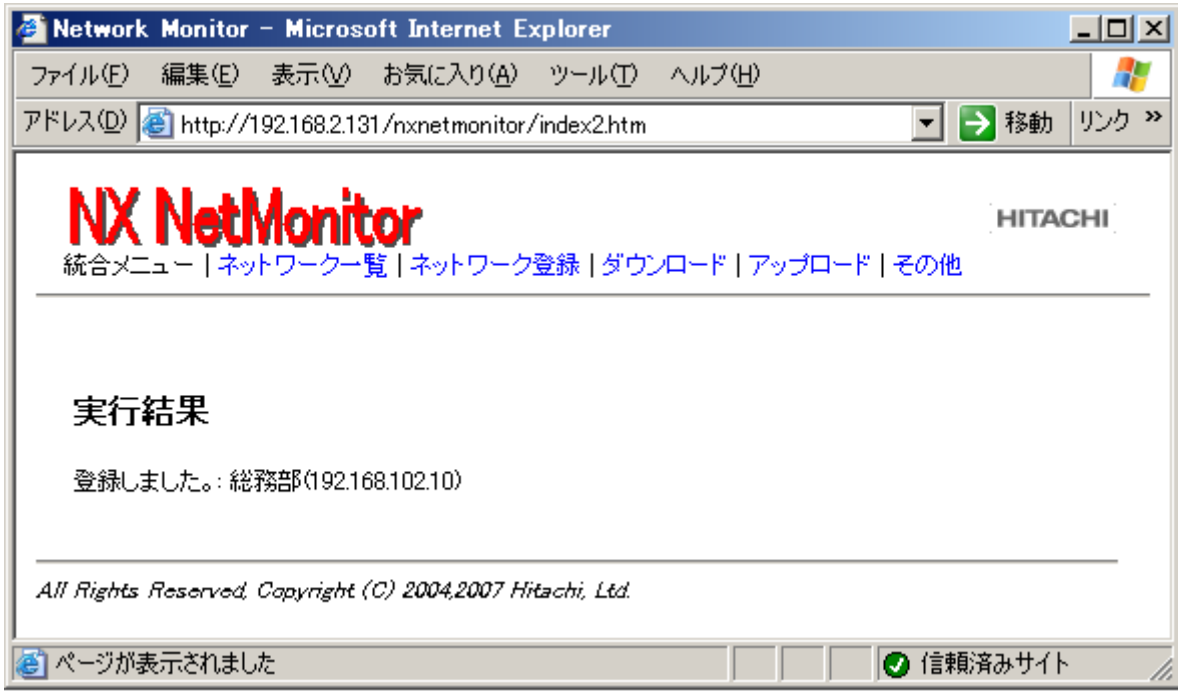
1）「ネットワーク登録」をクリックして、登録画面を表示します。



2）ネットワーク名、グループ名、監視装置の IP アドレス、ネットマスクを入力して「登録」ボタンをクリックします。



3）監視対象のネットワークが登録されます。

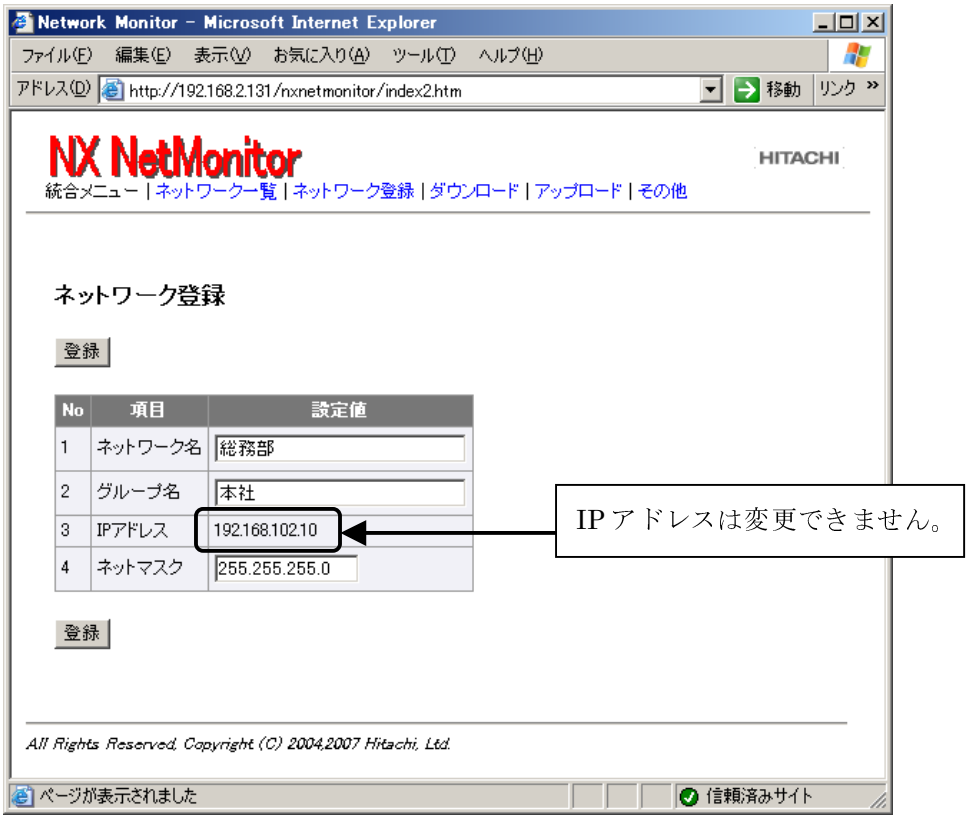


4）「ネットワーク一覧」を開くと、登録したネットワークを参照することができます。

6.8　監視対象ネットワークの削除と修正

ネットワーク一覧画面から、監視対象ネットワークの設定内容の修正および削除を行うことができます。監視対象ネットワークの設定内容を修正する場合には、修正するネットワークの「選択」項目にチェックマークをつけて、「修正」ボタンをクリックします。複数のネットワークをチェックした場合には、最初に見つけたネットワークを修正します。

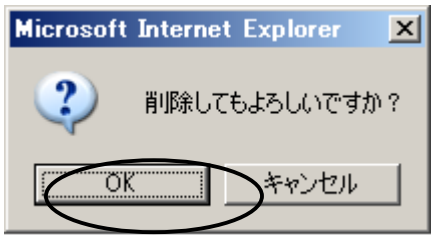
ネットワークの修正では、ネットワーク名、グループ名、ネットマスクの修正ができます。IP アドレスの修正をすることはできません。IP アドレスを修正する場合には、一旦削除してから、再登録を行ってください。



ネットワークの削除は、ネットワークの監視をやめる場合や、監視するネットワークアドレスが変更になり、それまでの監視情報を削除する場合などの時に使用します。

ネットワークの削除は「選択」ボタンに削除するネットワークをチェックして、「削除」ボタンをクリックします。ネットワーク一覧から削除すると、対象のネットワークの環境設定ファイルや許可機器一覧、接続一覧など関連するファイルが全て削除されます。関連ファイルを削除時は、監視処理を一旦停止します。ファイル削除時に、監視処理を再起動する場合には、「削除&監視処理再起動」にチェックをつけて「削除」ボタンをクリックしてください。対象のネットワークの監視処理を停止したままにする場合には、「削除のみ」ボタンにチェックをつけて「削除」ボタンをクリックしてください。

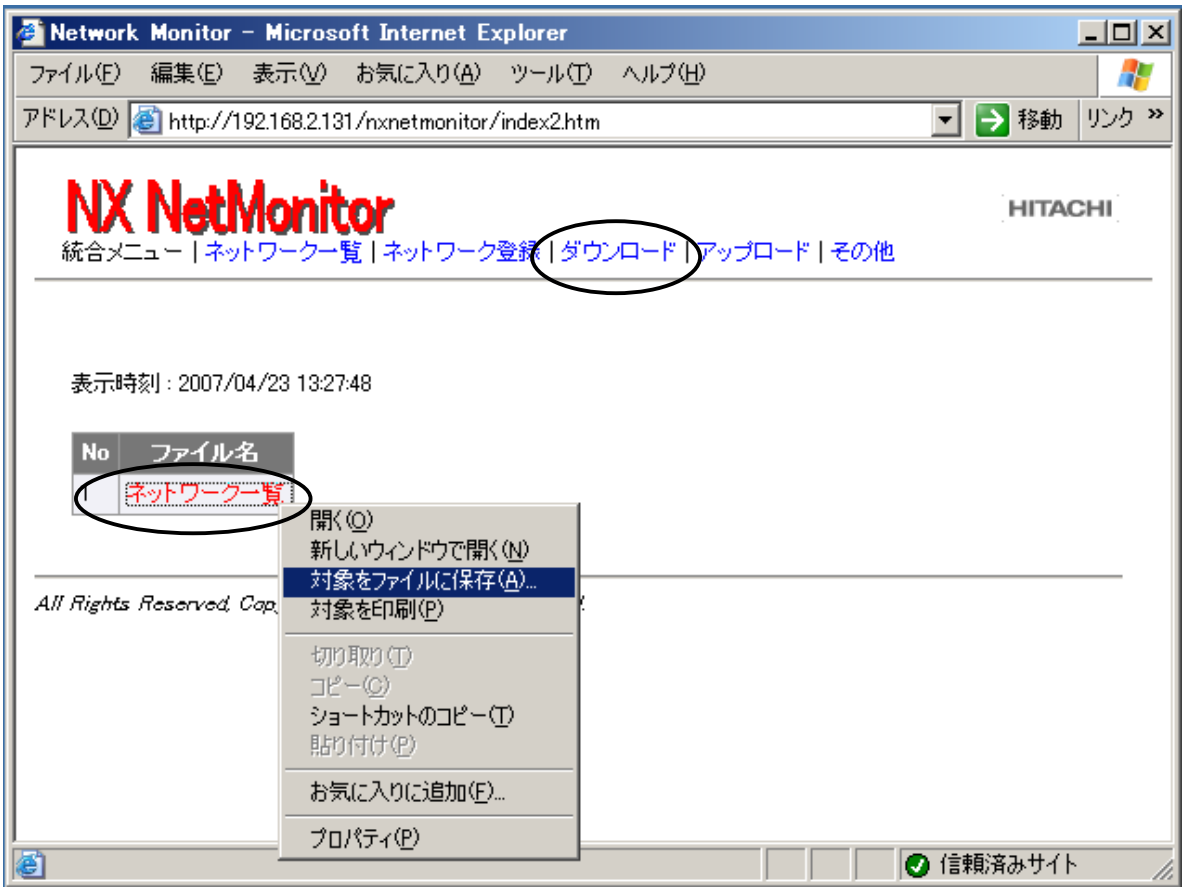
「削除」ボタンをクリックすると、以下のダイアログが表示されて、「OK」ボタンをクリックすると、チェックしたネットワークが削除されます。



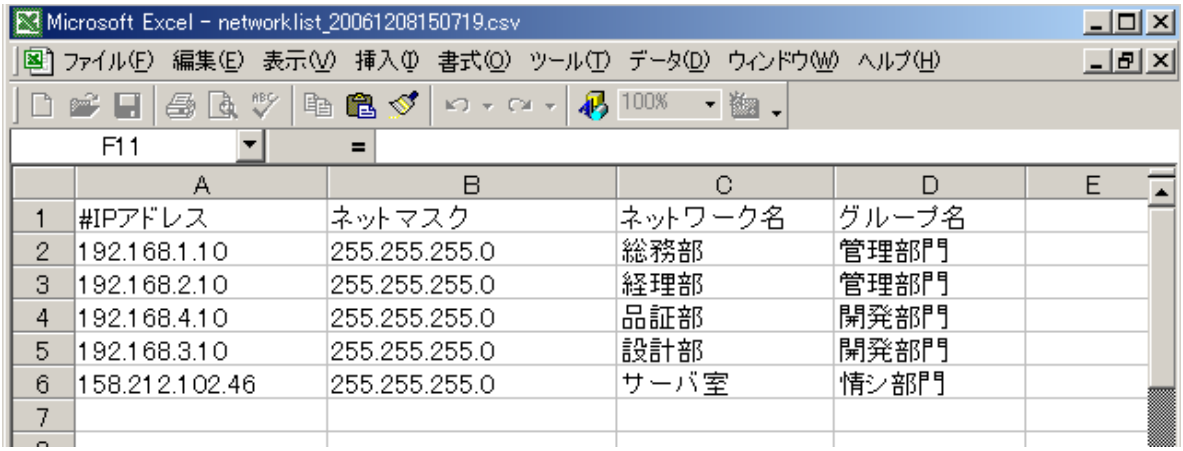
6.9　監視対象ネットワーク一覧のダウンロードとアップロード

監視対象ネットワークの一覧は CSV 形式のファイルにダウンロードすることが可能です。また、CSV 形式のファイルを修正して、アップロードすることが可能です。

監視対象ネットワーク一覧のダウンロードは、「ダウンロード」メニューをクリックします。
ダウンロードできるファイルの一覧が表示されますので、「ネットワーク一覧」を右クリックして。「対象をファイルに保存」を実行します。

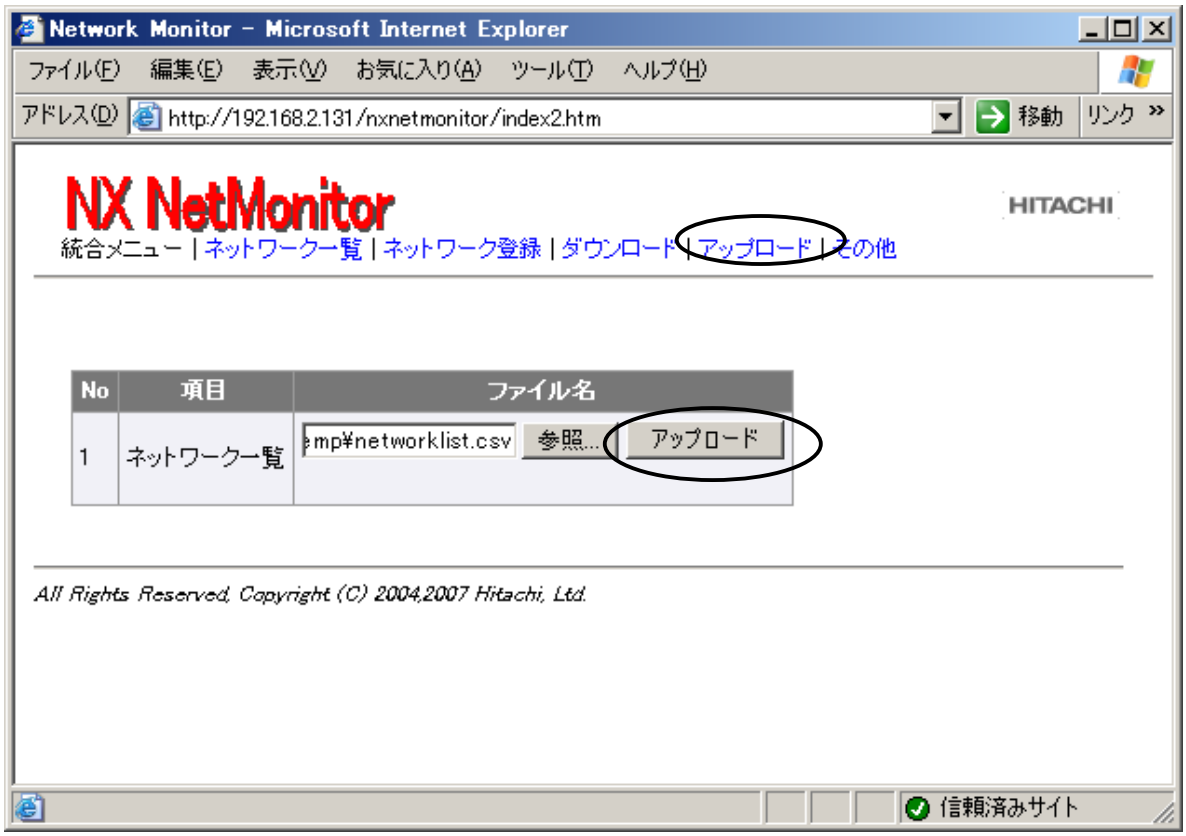


以下のような、内容のファイルがダウンロードされます。



※　1 ダウンロードされるファイルは Microsoft(R) Windows(R) の搭載された PC で見ることを前提としています（文字コードは Shift-JIS、改行コードは CRLF）

ダウンロードしたファイルを修正し、アップロード画面で修正したファイルを指定して、アップロードを行います。



「ダウンロード」ボタンで作成されるネットワーク一覧は、以下の通りとなります。
先頭に “# “がついた行はコメントになります。

フォーマット(CSV 形式)

ネットワークアドレス, ネットマスク, ネットワーク名, グループ名

・ネットワークアドレス、ネットマスクは、ドット形式です。
・行の先頭に # があれば、その行はコメント行として無視されます。
・ファイルは Microsoft(R) Windows(R) の搭載された PC で作成されたものを前提としています。
（文字コードは Shift-JIS、改行コードは CRLF）
・ネットワーク名、グループ名は任意の名称をつけることが出来ます。名称は日本語文字も可能です。

6.10 監視対象ネットワークの表示

ネットワーク一覧から表示させたいネットワーク名をクリックすると、対象ネットワークの監視画面を表示することができます。

6.11 接続機器一覧の表示

「接続機器」メニューを選択すると、現在ネットワークに接続されている機器の一覧を表示します。また、タイトル部をクリックすると、状態、MAC アドレス、IP アドレス、検出時刻、最終確認時刻にて並べ替えを行います。再度クリックすると、表示順番が昇順／降順で切り替わります。また、状態により、色が変わります。

・「削除」ボタン
　選択した機器をリスト上から削除することができます。
　使用されていないと思われる機器の情報は、削除してください。
・「拒否」ボタン
　選択した機器をネットワークから切り離すことができます。
　「６．１６　環境設定」で、「不正機器を検出しても排除しない」を指定している場合にはエラーとなり、実行できません。
・「許可機器一覧の新規作成」ボタン
　現在表示している機器の全ての接続を許可します。
　ここで、接続するための条件として、「MAC＋IP」、「MAC のみ」、「IP のみ」が指定可能です。

「修正」ボタン、「許可機器登録」ボタンおよび、「固定機器登録」ボタンの使用方法は、
「６．１９ ブラウザからの直接編集機能」を参照してください。

※ 状態について、以下に示します。
「動作中」 ：現在動作中の許可された機器
「動作中*」: 現在動作中の手動で許可された機器、または現在動作中で許可されていない機器(青)
「停止」 ：現在停止中の許可された機器
「停止*」 ：現在停止中で許可されていない機器（青）
「切断」 ：接続が許可されていない機器（赤）
「切断*」 ：手動で切り離された機器（青）
「期限切」：指定された停止期間以上起動されなかったため切り離された機器（緑）
「無効」 ：指定された接続許可の有効期限を越えたため切り離された機器（緑）
「対象外」：監視対象ネットワークアドレス以外の IP アドレスが割当てられている機器

ここで、「動作中*」、「切断*」状態の機器(青)は、ブラウザの監視画面から許可、または拒否の操作が行われたものです。継続的に使用・排除を行う場合には、許可機器一覧を更新してください。

※ 「許可機器一覧の新規作成」ボタンで作成される許可機器一覧は、以下の通りとなります。
IP アドレス 2、停止期間監視、有効期限は、指定されません（空欄)。
コメントは、"Permitted_Entry"となります。

フォーマット(CSV 形式)

```
MAC アドレス,IP アドレス 1,IP アドレス 2,停止期間監視,有効期限,コメント
```

例

・「MAC+IP」を選択した場合

```
00:80:c8:84:51:66,192.168.0.123,,,,Permitted_Entry
```

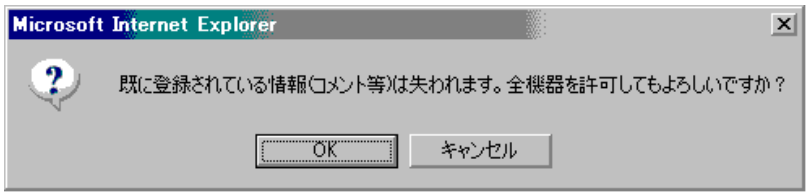
・「MAC のみ」を選択した場合

```
00:80:c8:84:51:66,,,,,Permitted_Entry
```

・「IP のみ」を選択した場合

```
,192.168.0.123,,,,Permitted_Entry
```

また、「許可機器一覧の新規作成」ボタンで、許可機器一覧を作成する場合には、下記画面が表示され、すでに登録されている情報は全て失われて、新規に許可機器一覧が作成されます。
なお、すでに登録されている情報を変更する場合には、「６．１９ ブラウザからの直接編集機能」を参照ください。



6.12 拒否機器一覧の表示

「拒否機器」メニューを選択すると、現在ネットワークへの接続が拒否されている機器の一覧を表示します。また、タイトル部をクリックすると、状態、MAC アドレス、IP アドレス、検出時刻、最終確認時刻にて並べ替えを行います。再度クリックすると、表示順番が昇順／降順で切り替われます。また、状態により、色が変わります。

・「許可」ボタン
選択した PC をネットワークへの接続を許可することができます。
「６．１６　環境設定」で、「不正機器を検出しても排除しない」を指定している場合にはエラーとなり、実行できません。

「修正」ボタン、「許可機器登録」ボタンおよび、「固定機器登録」ボタンの使用方法は、「６．１９ ブラウザからの直接編集機能」を参照してください。

※1 状態について、以下に示します。

(1) 環境設定で、排除モードが「不正機器を検出したら排除する」、
または「不正機器を検出しても排除しない（検出のみおこなう）」の場合
「切断」　：接続が許可されていない機器（赤）
「切断*」　：手動で切り離された機器（青）
「期限切」：指定された停止期間以上起動されなかったため切り離された機器（緑）
「無効」　：指定された接続許可の有効期限を越えたため切り離された機器（緑）
ここで、「切断*」状態の機器(青)は、ブラウザの監視画面などから拒否の操作が行われたものです。継続的に排除を行う場合には、許可機器一覧/固定機器一覧から削除してください。
排除モードが「不正機器を検出しても排除しない（検出のみ行う）」では、拒否機器一覧に表示されている機器は、実際には切断されていません。

(2) 環境設定で、排除モードが「不正機器を検出しても排除しない（検出･排除ともに行わない）」の場合
「動作中*」：現在、接続を許可されていない動作中の機器（青）
「停止*」　：現在、接続を許可されていない停止中の機器（青）
これらの機器(青)は許可機器一覧に登録されていない機器です。そのため「不正機器を検出したら排除する」に変更すると、これらの機器はネットワークから切り離されます。
継続的に接続する場合は、許可機器一覧/固定機器一覧に追加してください。

※　2 「期限切」状態の機器を、ネットワークへ接続させるには、機器をチェックして、「許可」ボタンをクリックしてください。

6.13 許可機器/固定機器一覧の表示

ネットワークへの接続が許可された機器の一覧を表示します。

「登録」ボタンおよび、「修正」ボタンの使用方法は、以下の章を参照してください。
「６．１９ ブラウザからの直接編集機能」
(許可機器一覧／固定機器一覧共通)

(1) 許可機器一覧

許可機器一覧では、ネットワークへの接続が許可された許可機器の一覧を表示します。
なお、許可機器とは、クライアント PC などを意味します。

また、「検索」ボタンをクリックすると、検索画面が表示されます。
許可機器検索画面にて、MAC アドレスや IP アドレス、その両方を入力してチェック後、「検索」ボタンをクリックします。

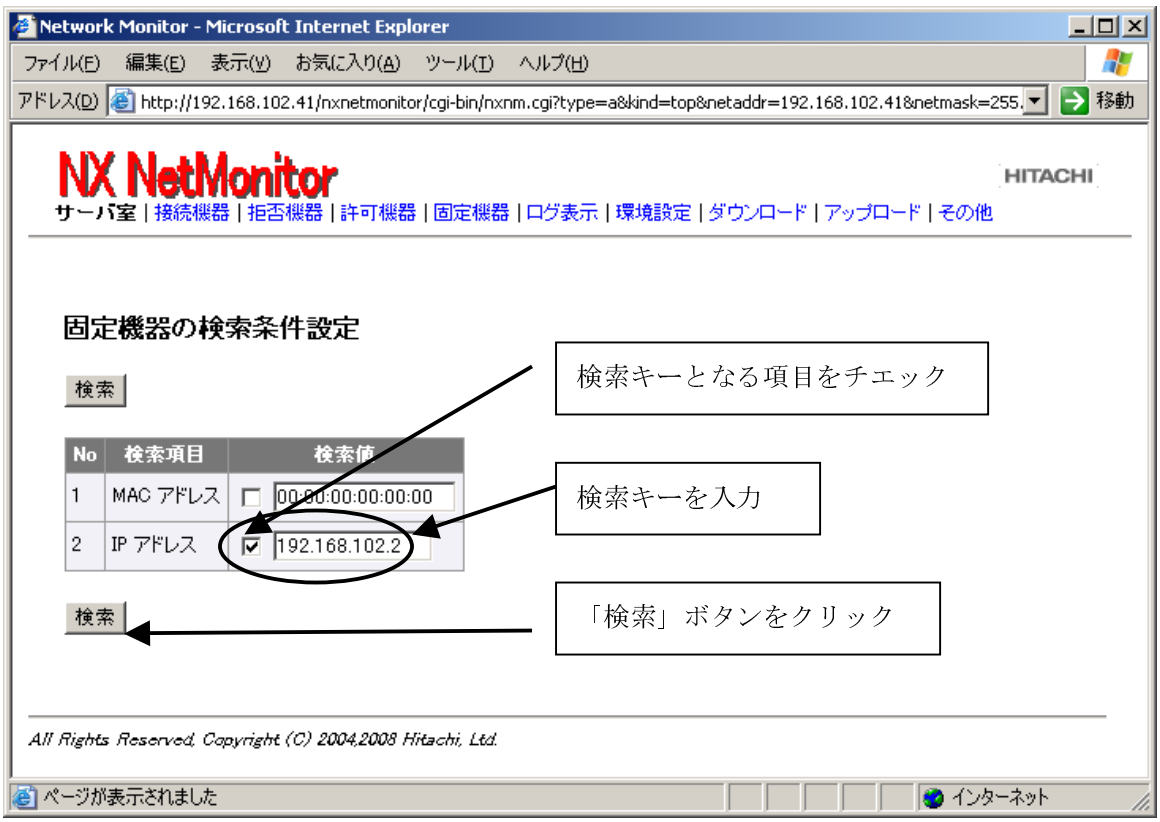
検索結果が表示されます。

※ MAC アドレス、IP アドレスのどちらも選択されていない場合には検索されません。「検索条件が指定されていません。」と表示されます。

(2) 固定機器一覧

固定機器一覧では、ネットワークへの接続が許可された固定機器の一覧を表示します。
なお、固定機器とは、ルータ、プリンタ、サーバ等の機器です。

また、「固定機器検索」をクリックすると、検索画面が表示されます。
固定機器検索画面にて、MACアドレス、IPアドレス、その両方を入力してチェック後、「検索」ボタンをクリックすると、検索結果が表示されます。



検索結果が表示されます。

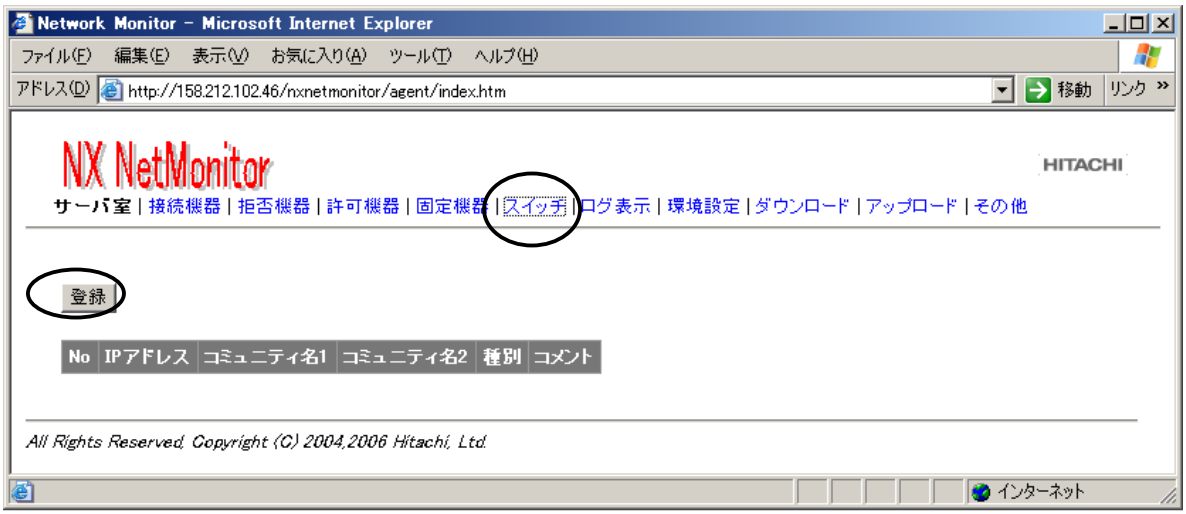
※ MAC アドレス、IP アドレスのどちらも選択されていない場合には検索されません。「検索条件が指定されていません。」と表示されます。

6.14 スイッチ情報の表示

スイッチメニューは、環境設定画面で、「不正機器特定情報」にコミュニティ名を設定している時に表示されます。 「スイッチ」メニューを選択すると、登録されているスイッチ情報の一覧を表示します。スイッチ一覧の画面からスイッチ情報の登録、修正を行うことができます。
環境設定画面で「不正機器特定情報」にコミュニティ名を設定すると、スイッチ情報を設定していなくても、監視対象の監視ネットワークに接続されているスイッチを自動的に検出します。

1）スイッチ情報の登録

「登録」ボタンをクリックして、登録画面を開きます。



スイッチ登録画面で、スイッチ情報を入力します。

＜スイッチ登録画面の入力項目＞

No	項目	説明
1	IP アドレス	MIB 情報を収集する器機（スイッチ等）の IP アドレス
2	コミュニティ名 1	MIB 情報を取得するためコミュニティ名（例：public）
3	コミュニティ名 2	将来用（指定しないでください）
4	種別	将来用（指定しないでください）
5	コメント	コメントを 32 バイトまで指定可能

（注 1）Cisco 社製のスイッチで、VLAN を指定している場合は、コミュニティ名に VLAN 番号を付加して指定してください。（コミュニティ名@VLAN 番号　例：public@100）

（注 2）スイッチを登録する場合は、監視ネットワークの全てのスイッチをコアスイッチからエッジスイッチのように上位のスイッチから順番に登録してください。

設定例

IP アドレス	コミュニティ名 1	コミュニティ名 2	種別	コメント
192.168.0.1	public	－	－	SW1（コアスイッチ）
192.168.0.11	public	－	－	SW2（フロアスイッチ）
192.168.0.12	public	－	－	SW3（フロアスイッチ）
192.168.0.101	public	－	－	SW4（エッジスイッチ）
192.168.0.102	public	－	－	SW5（エッジスイッチ）

（注 3）スイッチの登録は、監視しているネットワークとは別ネットワークのスイッチの IP アドレスは登録してないで下さい。

「実行」ボタンをクリックすると、確認のダイアログが出力されます。

「OK」ボタンをクリックすると、スイッチ情報が登録されます。

（注）JP1/NETM/Network Monitor が参照するスイッチの MIB 情報

JP1/NETM/Network Monitor は、スイッチに接続された不正機器の接続位置を特定するために、以下の MIB 情報を参照します。不正機器の位置特定を行うためには、JP1/NETM/Network Monitor に登録するスイッチで以下の標準 MIB 情報を RFC 準拠でサポートしている必要があります。

JP1/NETM/Network Monitor が参照するスイッチの MIB 情報

No	グループ名	オブジェクト識別子	説明
1	dot1dBase グループ	dot1dBaseBridgeAddress	ブリッジの MAC アドレス
2		dot1dBasePortIfIndex	このポートに対応するインタフェースが MIB-II に定義されたオブジェクトのインスタンスの値。
3	dot1dTp グループ	dot1dTpFdbEntry	フィルタリング情報を持つユニキャスト MAC アドレス情報
4	interfaces グループ	ifTable	インタフェースの管理テーブル。
5	ipAddrTable グループ	ipAddrTable	このエンティティの IP アドレスに関連するアドレッシング情報のテーブル(IP アドレス別のアドレス情報テーブル)。

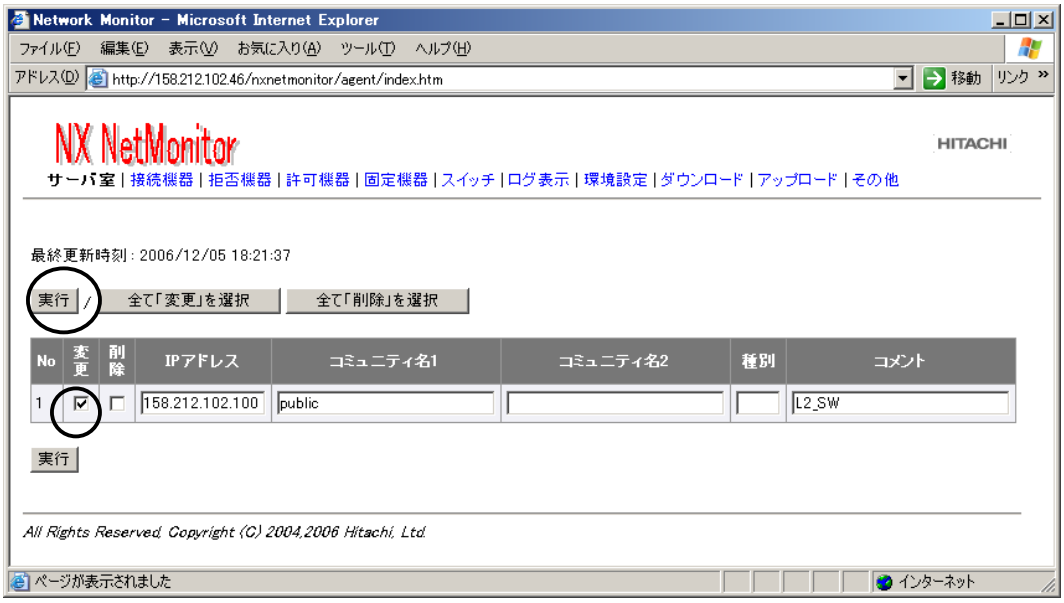
2）スイッチ情報の指定例

Cisco 社製以外のスイッチ、または Cisco 社製で VLAN 未使用時の指定例

3）スイッチ情報の更新

スイッチ一覧の修正は、「スイッチ」メニューから行います。修正したいスイッチをチェックして、修正画面を表示します。

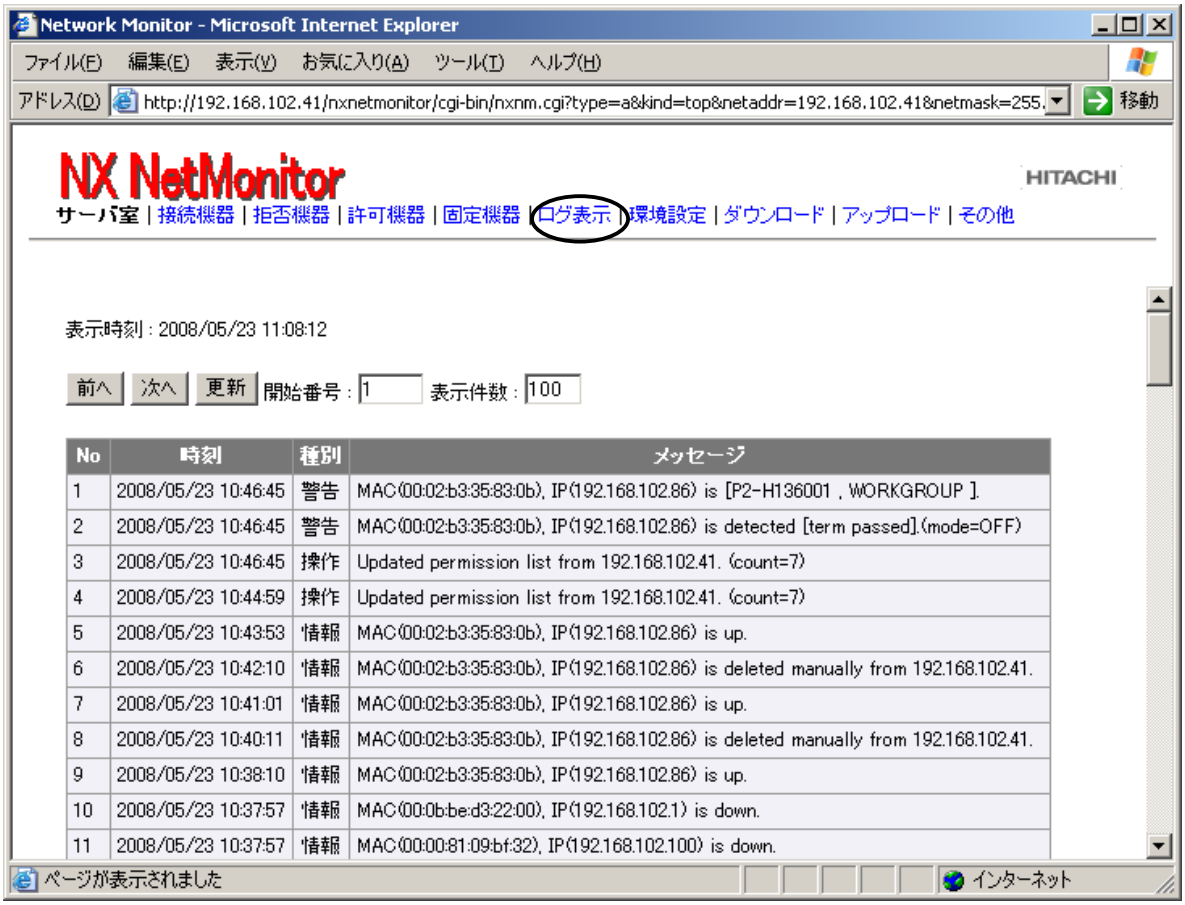
設定内容を修正し、変更項目にチェックを付けます。



「実行」ボタンをクリックすると、スイッチ情報が更新されます。

6.15 ログ表示

不正機器接続の検知・排除や、手動による接続拒否・許可などのログを新しい順に表示します。
メッセージの一覧は、「８．１　ログ／トラップ一覧」を参照してください。



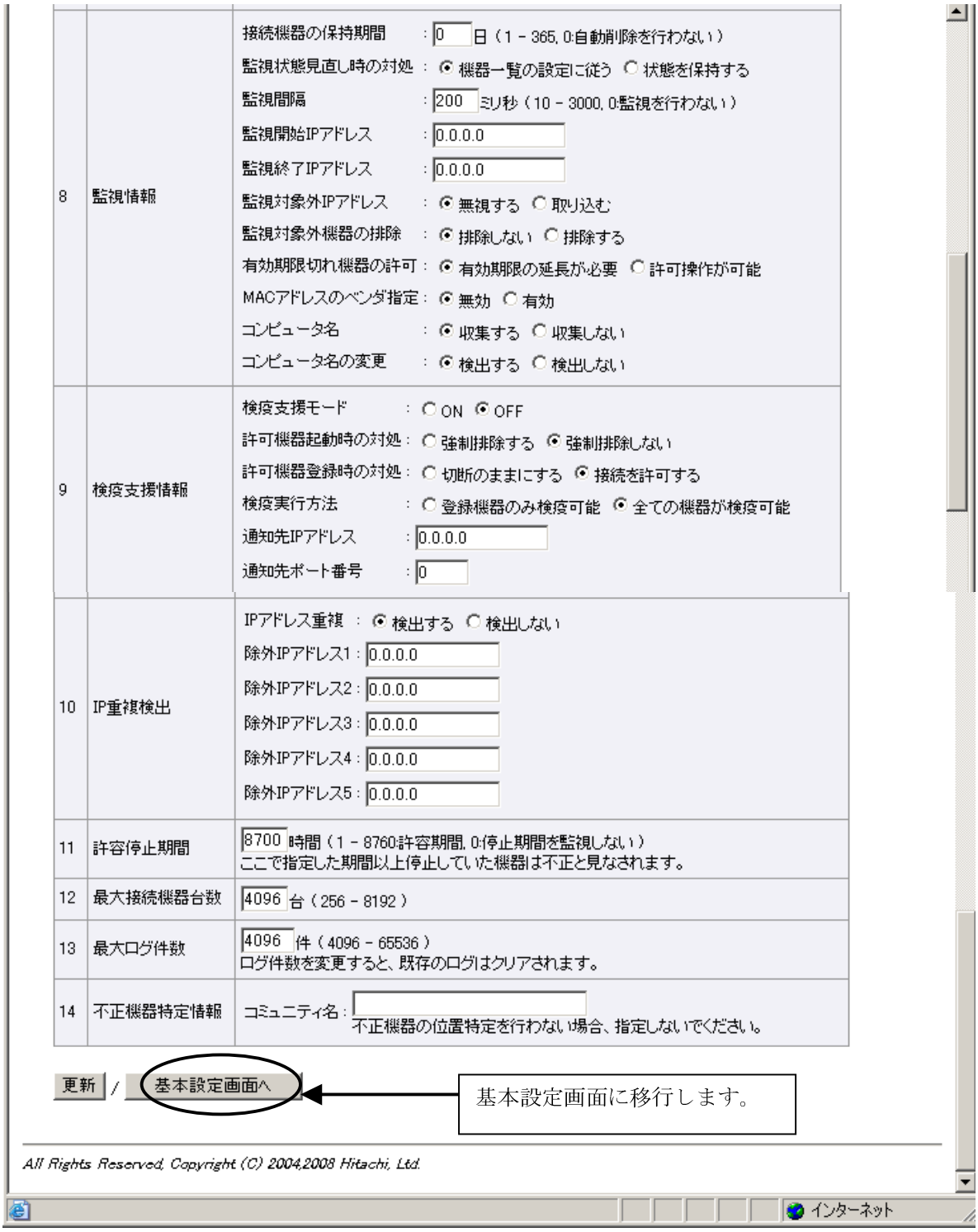
※　最大ログ件数は、デフォルトで 4096 件です。最大ログ件数を変更する場合には「環境設定」の「最大ログ件数」で設定します。「最大ログ件数」は 4096～65536 の範囲で指定することができます。
「最大ログ件数」を変更した場合、それまでのログはクリアされます。既存のログが必要な場合には、統合管理装置などのダウンロードして保存してください。
また、最大ログ件数を超えた場合には、古いものから上書きされます。

6.16 環境設定

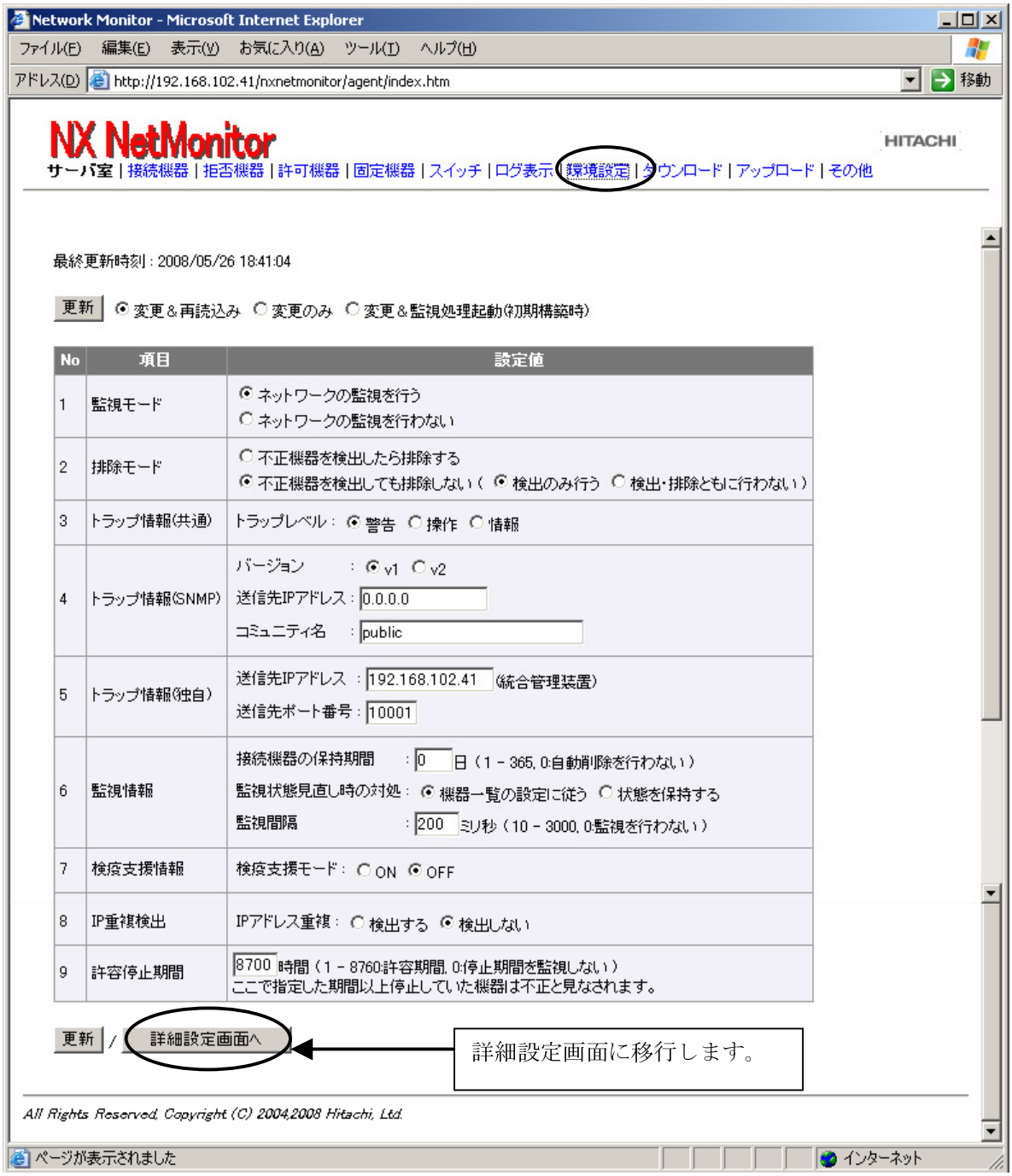
ネットワークの監視、不正機器の排除、など、ネットワーク監視に関する設定を行います。
環境設定画面は、ネットワーク監視を行うために設定が必要な項目を表示する「基本設定画面」と、デフォルトから設定を変更する必要がない項目を表示する「詳細設定画面」があります。「基本設定画面」は、ネットワークを監視するための基本的な項目です。「詳細設定画面」は、連携製品を使用する場合や、きめ細かい設定を行うために使用し通常は設定の変更は不要です。「基本設定画面」と「詳細設定画面」の切替は、下部に表示されている「基本設定画面」、「詳細設定画面」のボタンを押すと切り替わります。デフォルトでは「基本設定画面」が表示されます。

各種モードや情報を変更した後、「更新」ボタンを押すと環境設定が行われます。
「変更＆再読込み」は変更情報が監視処理に即時反映されます。
「変更のみ」は環境設定ファイルを更新するだけで、監視処理には反映されません。次の監視処理起動時に反映されます。
「変更＆監視処理起動」は環境ファイルを更新後、監視処理を起動します。初期構築時（監視処理が停止している場合）にチェックします。

「詳細設定画面」


8 監視情報
接続機器の保持期間 : 0 日（1 - 365, 0:自動削除を行わない）
監視状態見直し時の対処 : 機器一覧の設定に従う 状態を保持する
監視間隔 : 200 ミリ秒（10 - 3000, 0:監視を行わない）
監視開始IPアドレス : 0.0.0.0
監視終了IPアドレス : 0.0.0.0
監視対象外IPアドレス : 無視する 取り込む
監視対象外機器の排除 : 排除しない 排除する
有効期限切れ機器の許可 : 有効期限の延長が必要 許可操作が可能
MACアドレスのベンダ指定 : 無効 有効
コンピュータ名 : 収集する 収集しない
コンピュータ名の変更 : 検出する 検出しない
9 検疫支援情報
検疫支援モード : ON OFF
許可機器起動時の対処 : 強制排除する 強制排除しない
許可機器登録時の対処 : 切断のままにする 接続を許可する
検疫実行方法 : 登録機器のみ検疫可能 全ての機器が検疫可能
通知先IPアドレス : 0.0.0.0
通知先ポート番号 : 0
10 IP重複検出
IPアドレス重複 : 検出する 検出しない
除外IPアドレス1 : 0.0.0.0
除外IPアドレス2 : 0.0.0.0
除外IPアドレス3 : 0.0.0.0
除外IPアドレス4 : 0.0.0.0
除外IPアドレス5 : 0.0.0.0
11 許容停止期間
8700 時間（1 - 8760:許容期間, 0:停止期間を監視しない）
ここで指定した期間以上停止していた機器は不正と見なされます。
12 最大接続機器台数
4096 台（256 - 8192）
13 最大ログ件数
4096 件（4096 - 65536）
ログ件数を変更すると、既存のログはクリアされます。
14 不正機器特定情報
コミュニティ名 :
不正機器の位置特定を行わない場合、指定しないでください。
更新 / 基本設定画面へ
基本設定画面に移行します。
All Rights Reserved, Copyright (C) 2004,2008 Hitachi, Ltd.
インターネット

「基本設定画面」



※１　検疫支援モードが「ON」の時には、基本設定画面でも検疫支援情報の詳細設定項目が表示されます。

※２　IP アドレス重複が「検出する」の時には、基本設定画面でも除外 IP アドレスの設定項目が表示されます。

以下に「環境設定」で設定する内容を記述します。
＜環境設定内容一覧（1/7)＞

No	項目	設定値	デフォルト
1	監視モード	「ネットワークの監視を行う」をチェックすると、監視処理を行います。「ネットワークの監視を行わない」をチェックすると、監視処理を行いません。 「監視モード」の変更は NX NetMonitor の次回起動時から有効になります。	ネットワークの監視を行わない
2	排除モード	「不正機器を検出したら排除する」をチェックすると、許可機器一覧/固定機器一覧、または排除機器一覧にしたがって、不正機器を検出・排除します。 「不正機器を検出しても排除しない」をチェックし、かつ、「検出のみを行う」にした場合、不正機器を検出すると排除は行いませんが、ログへの出力、トラップによる通知を行います。 「検出・排除とも行わない」にした場合、ログへの出力、トラップによる通知を行いません。 なお、「不正機器を検出したら排除する」をチェックした場合には、「検出のみを行う」や「検出・排除とも行わない」を選択しても無効となります。	「不正機器を検出しても排除しない」 「検出・排除とも行わない」
3	排除レベル	NX NetMonitor が不正機器を排除するための処理のレベルを設定します。 一部の LinuxOS では、NetMonitor が排除レベル(中)で排除を行なった場合でも、許可機器から排除された Linux マシンへの通信が行えるタイミングが発生することがあります。この場合「高」に設定します。 また、不正な機器に対して排除するためのパケットを許可機器（一部の無線アクセスポイント）が取り込んでしまうケースがあり、許可機器が通信できなくなる場合があります。この場合「低」に設定します。 通常は「中」としてください。	「中」
4	動作モード	「通常(許可機器一覧を使用する)」をチェックすると、許可機器一覧に従って不正機器を検出します。 「簡易(排除機器一覧を使用する)」をチェックすると、排除機器一覧に従って不正機器を検出します。	通常(許可機器一覧を使用する)
5	トラップ情報(共通)	「警告」の場合は警告のみ、「操作」の場合は警告と操作、「情報」の場合は警告と操作と情報が出力されます。 通常は、「警告」をチェックします。 (注) 同時に大量のトラップが発生した時に、全てのトラップが送信できない場合があるため、「警告」に設定することを推奨します。	警告

＜環境設定内容一覧 (2/7)＞

No	項目	設定値	デフォルト
6	トラップ情報(SNMP)	SNMP マネージャにトラップ情報を通知するための、情報を設定します。 「バージョン」は SNMP マネージャが受信する SNMP のバージョンを「V1」または「V2」で設定します。 「送信先 IP アドレス」は SNMP マネージャがインストールされている管理者用 PC の IP アドレスを設定します。 「コミュニティ名」は SNMP マネージャと通信を行なう際のコミュニティ名を 32 バイト以内で指定します。(注 1)	・バージョン「V1」 ・送信先 IP アドレス「0.0.0.0」 ・コミュニティ名「public」
7	トラップ情報(独自)	統合管理装置(NX NetMonitor/Manager)にトラップ情報を通知するための、情報を設定します。 「送信先 IP アドレス」は統合管理装置の IP アドレスを設定します。「送信先ポート番号」は、統合管理装置(NX NetMonitor/Manager)で設定した受信ポート番号とあわせてください。(注 1)	・送信先 IP アドレス「0.0.0.0」 ・送信先ポート番号「0」
8	監視情報	●接続機器の保持期間 1～365 の値(日)を指定した場合、指定期間停止していた機器を接続機器一覧のエントリから自動削除します。保持期間に 0 を指定した場合は自動削除を行いません。	「0」(日)
		●監視状態見直し時の対処 「機器一覧の設定に従う」をチェックすると、手動による接続許可、拒否を行った機器は監視処理を再起動後に現在登録されている許可機器一覧、または排除機器一覧の設定に従います。「状態を保持する」にチェックすると、監視状態見直し時も同じ状態を保持します。なお、監視状態見直しは、監視処理の再起動、環境設定の変更、許可機器一覧/固定機器一覧/排除機器一覧の更新した場合に行われます。 ただし、排除モードを OFF にした場合、有効期限が過ぎたため排除された機器に関しては、「状態を保持する」を設定した場合でも、状態は保持されません。	機器一覧の設定に従う
		●監視間隔 監視間隔は、不正機器を監視するためのポーリング間隔です。10～3000 ミリ秒の範囲で指定します。 監視間隔を 0 とすると、ポーリングによる監視処理を行いません。この場合、不正な機器の検出に時間がかかる場合があります。	200 (ms)

(注 1) 不正機器のコンピュータ名検出のログ（ログ/トラップ一覧の No9）は、SNMP トラップ、独自トラップのいずれか、または両方を定義したときに出力されます。

＜環境設定内容一覧 (3/7)＞

No	項目	設定値	デフォルト
8	監視情報	●「監視開始 IP アドレス」と「監視終了 IP アドレス」 ポーリングによる監視処理を行う IP アドレスの範囲を指定します。監視 IP アドレスの範囲（開始 IP アドレスから終了 IP アドレス、開始より終了が小さいと監視しません）を指定することにより、ネットワーク負荷を調整することができます。 また、"0.0.0.0" （デフォルト）を指定した場合は、監視対象ネットワーク内の全機器が対象となります。	･監視開始 IP アドレス 「0.0.0.0」 ･監視終了 IP アドレス 「0.0.0.0」
		●監視対象外 IP アドレス 「無視する」をチェックすると、監視対象ネットワークと異なるネットワークの IP アドレスを持つ機器の情報を取り込みません（接続機器一覧にも表示されません)。 「取り込む」をチェックした場合、異なるネットワークの IP アドレスを持つ機器の情報を取り込んで、接続機器一覧に表示を行います。異なるネットワークの IP アドレスを持つ機器を排除するかどうかは、「監視対象外機器の排除」の設定に従います。	無視する
		●監視対象外機器の排除 「排除しない」をチェックすると、監視対象ネットワークと異なるネットワークの IP アドレスを持つ機器を排除しません。 「排除する」をチェックすると、監視対象ネットワークと異なるネットワークの IP アドレスを持つ機器を排除します。「監視対象外 IP アドレス」を「無視する」に設定してある場合には、排除はおこなわれません。	「排除しない」
		●有効期限切れ機器の許可 「有効期限の延長が必要」をチェックすると、有効期限を過ぎた機器に対して手動操作で許可操作を行うことができません。 「許可操作が可能」をチェックすると有効期限を過ぎた機器に対しても、手動で許可操作を行うことが出来ます。	有効期限の延長が必要
		●MAC アドレスのベンダ指定 「有効」をチェックし、許可機器一覧や固定機器一覧で指定する MAC アドレスの下位 3 バイトを全て 0 を指定した場合、上位 3 バイトのベンダ ID のみでチェックします。これにより、ルータなど同じメーカの機器に交換した場合に、許可機器一覧や固定機器一覧の MAC アドレスを修正する必要がない場合があります。	無効

＜環境設定内容一覧（4/7)＞

No	項目	設定値	デフォルト
8	監視情報	●コンピュータ名 コンピュータ名を「収集する」に選択すると、監視対象機器が立ち上がった時にコンピュータ名とワークグループ名(ドメイン名)を取得します。収集する対象の機器はWidnows のみ(Windows NT, Windows 2000, Windows XP, Windows Server 2003)です。取得した情報は接続機器一覧などに表示されます。 「収集しない」にチェックすると、コンピュータ名とワークグループ名(ドメイン名)の取得を行いません。 なお、パーソナルファイアウォール機能が有効になっている機器に対しては情報を収集することができません。	収集する
		●コンピュータ名の変更 「検出する」をチェックすると、コンピュータ名の変更を検出時ログを出力します。「検出しない」をチェックすると、コンピュータ名の変更を検出しません。	「検出する」
9	検疫支援情報	●検疫支援モード 検疫支援機能を有効にする場合には、「ON」を指定します。検疫支援機能を有効にした場合、ネットワークから排除された機器は、他の機器との通信を遮断しつつ、監視装置または指定した特定のサーバとの通信のみ可能となります。(注 2)	・検疫支援モード「OFF」
		●許可機器起動時の対処 動作モードが、通常(許可機器一覧使用)の場合のみ有効です。長期出張等で、しばらく使用していない機器を起動した時に、パッチやウィルス定義ファイルなどが更新されていない可能性があるため、まず、検疫処理を行い問題ないことが確認されてから接続を許可するために使用します。起動時に排除したくない機器は、固定機器一覧に登録してください。また、簡易モードの場合は、許可機器は登録できないため、「強制排除する」を指定しても排除されません。(設定は無効)	・許可機器起動時の対処「強制排除しない」

(注 2) 検疫支援機能で、指定した特定のサーバとの通信は監視装置が Linux 版のときのみ有効です。
構成や設定方法は「７　特定機器との通信サポート」を参照してください。

＜環境設定内容一覧（6/7)＞

No	項目	設定値	デフォルト
9	検疫支援情報	●許可機器登録時の対処 許可機器登録直後は、パッチやウィルス定義ファイルなどが、最新に更新されていない可能性があるため、まず、検疫処理を行い問題ないことが確認されてから接続を許可するために使用します。検疫処理を受けて、パッチ/ウィルスパターンファイルなどが最新となった場合に、初めてネットワークに接続許可する場合に、「切断のままにする」を指定します。許可機器登録時すぐにネットワークに接続する場合は「接続を許可する」を指定してください。 また、「許可機器登録時の対処」動作モードが、通常(許可機器一覧使用)の場合のみ有効です。 「許可機器登録時の対処」で、「切断のままにする」を設定時は、検疫支援モードが「ON」でかつ、監視情報の監視状態見直し時の対処が「状態を保持する」のときに有効になります。	・許可機器登録時の対処「接続を許可する」
		●検疫実行方法 「登録機器のみ検疫可能」を有効にした場合、「排除モードが ON」かつ「検疫支援モードが ON」のときに、接続拒否された機器の内、許可機器一覧や固定機器一覧に登録した機器のみが監視装置または指定した特定のサーバと検疫通信できるようになります。「登録機器のみ検疫可能」を有効にすると、許可(固定)機器一覧に登録されていない接続拒否機器は、「検疫支援モード ON」であっても、監視装置または指定した特定のサーバと検疫通信ができません。(検疫モード OFF のように動作します)	
		●通知先 IP アドレス 検疫モジュールがインストールされている機器の IP アドレスを指定します。	・通知先 IP アドレス「0.0.0.0」
		●通知先ポート 検疫モジュールが NX NetMonitor 監視処理からの情報を受信するポート番号を指定します。検疫モジュールの詳細は、連携製品のマニュアル等を参照ください。	・通知先ポート番号「0」

＜環境設定内容一覧 (6/7)＞

No	項目	設定値	デフォルト
10	IP 重複検出	二重化システムなどで使用されるチーミング機能を持つ機器を IP 重複と誤検出しないように IP アドレス重複を「検出しない」に設定します。IP アドレス重複を検出する場合には、「検出する」を設定します。「検出する」に設定した場合でも、「除外 IP アドレス」を設定することにより、指定された IP アドレスは IP アドレス重複として検出しません。「除外 IP アドレス」は 5 つまで登録できます。「除外 IP アドレス」が 5 つ以上ある場合には、「検出しない」に設定してください。	・「検出する」 ・除外 IP アドレス「0.0.0.0」
11	許容停止期間	許容停止期間は、指定した時間以上起動されなかった機器が立ち上がった場合にネットワークへの接続を拒否するものです。 1～8760 時間の範囲で指定します。時間に 0 を指定すると、排除処理を行いません。 許可機器一覧/固定機器一覧の「停止期間監視対象」に Y が指定されている機器が排除の対象となります（設定方法は、「６．１８　アップロード」を参照ください)。	0 (時間)
12	最大接続台数	現在ネットワークに接続しているかどうかに関わらず、監視するサブネットワークに接続する可能性のある機器の最大数を指定します。256 から 8192 台の範囲で指定します。	4096 (台)
13	最大ログ件数	ログを保存する最大ケース数を指定します。4096 から 65536 の範囲で指定します。最大ログ件数を変更するとそれまで保存されていたログはクリアされます。	4096

＜環境設定内容一覧（7/7）＞

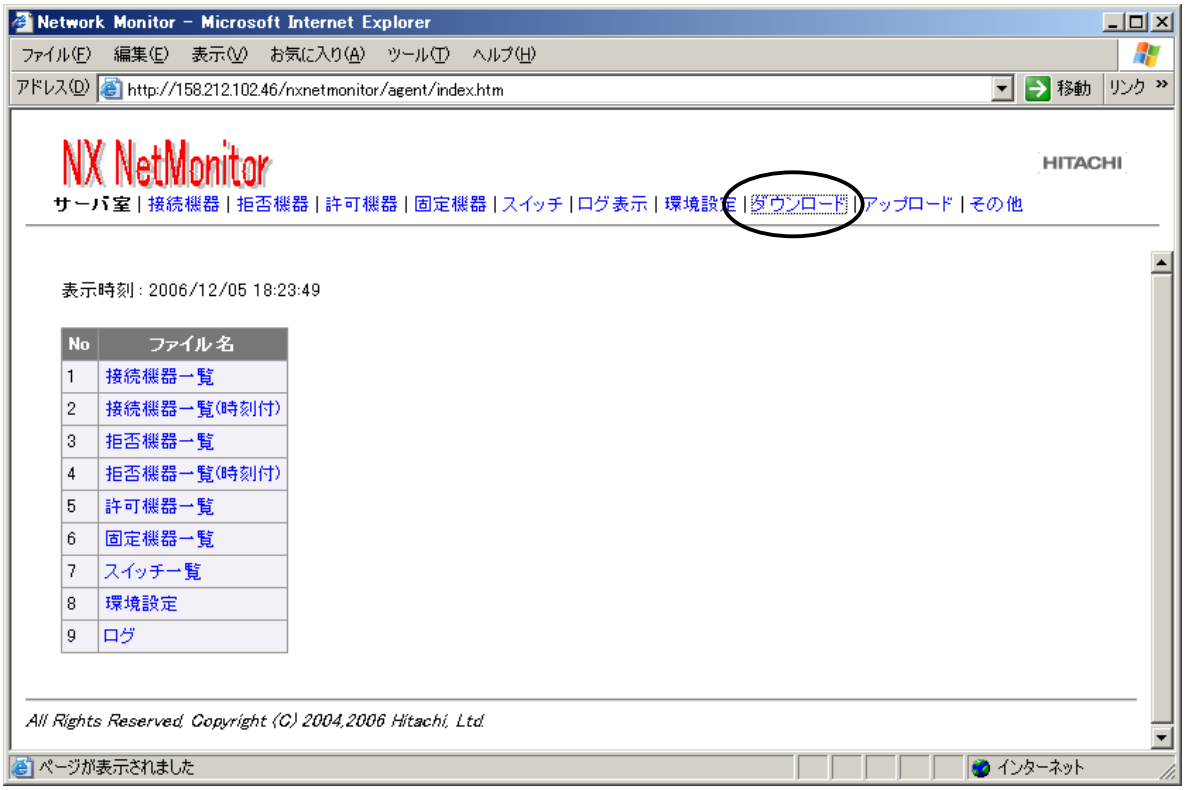
No	項目	設定値	デフォルト
14	不正機器特定情報	不正機器の位置(接続スイッチの IP アドレスを接続ポート番号)特定機能を有効にする場合、コミュニティ名を指定します。コミュニティ名の指定がない場合には、位置特定を行いません。 不正機器特定機能では、 ・スイッチ情報が登録されていない場合、監視ネットワーク内の接続機器から、ここに登録されているコミュニティ名を使用してスイッチの MIB 情報を収集することで、スイッチを自動検出します。 ・スイッチ情報が登録されている場合、スイッチ情報に登録されている情報（コミュニティ名１）を使用して、スイッチの MIB 情報を収集し、登録されている機器がスイッチが判断します。 NX NetMonitor が認識しているスイッチは、「６．２２その他メニュー」のスイッチ情報」で確認することが出来ます。 コミュニティ名を指定すると、画面表示を切り替えるメニュー一覧にスイッチ情報を設定するための「スイッチ」メニューを表示します。また「その他」メニューに「スイッチ情報」を表示します。（注３）	なし

（注３）SNMP コミュニティ名を設定し、「更新」ボタンを押した後、Web ブラウザの再表示ボタンで画面を再表示させて下さい。「スイッチ」メニューが表示されます。

6.17 ダウンロード

各種ファイルのダウンロードが可能です。ダウンロードしたいファイルを右クリックし、表示されるメニューの「対象をファイルに保存」を選択して、ダウンロードを行います。

・「接続機器一覧」、「接続機器一覧(時刻付)」
　現在ネットワークに接続されている機器の一覧です。
・「拒否機器一覧」、「拒否機器一覧(時刻付)」
　現在ネットワークへの接続が拒否されている機器の一覧です。
・「許可機器一覧」、「固定機器一覧」
　現在ネットワークへの接続が許可されている機器の一覧です。
・「排除機器一覧」(「６．２０　簡易モード」を参照してください。)
　現在ネットワークへの接続を拒否する機器の一覧です。
・「環境設定」
　「６．１６　環境設定」で設定した内容です。
・「スイッチ一覧」
　「６．１４　スイッチ情報の表示」で表示される内容です。
　「スイッチ一覧」は環境設定画面で、「不正機器特定情報」にコミュニティ名を設定している時に表示されます。
・「ログ」
　「６．１５　ログ表示」で表示される内容です。



※　ダウンロードされるファイルは Microsoft(R) Windows(R) の搭載された PC で見ることを前提としています（文字コードは Shift-JIS、改行コードは CRLF)。

ダウンロードされるファイルのフォーマットは、以下の通りです。

・「接続機器一覧」
・「拒否機器一覧」
・「許可機器一覧」
・「固定機器一覧」
・「排除機器一覧」（「６．２０　簡易モード」を参照してください。）
　フォーマットは、「６．１８　アップロード」の「許可機器一覧」を参照してください。
　なお、「接続機器一覧」,「拒否機器一覧」の場合、IP アドレス 2,停止期間監視,有効期限は空欄となります。
　コメントは、「接続機器一覧」の場合は "Connected_Entry",
　「拒否機器一覧」の場合は、"Isolated_Entry"となります。

　「許可機器一覧」は、アップロードしたファイル、監視画面から編集した直接編集したファイルまたは、「接続機器」メニューから、「許可機器一覧の新規作成」で自動生成したファイルとなります。
・「接続機器一覧(時刻付)」
・「拒否機器一覧(時刻付)」
　フォーマット(CSV 形式)：接続機器一覧画面に表示されるフォーマット（1 行で表示されます）

```
状態,MAC アドレス,IP アドレス,検出時刻,最終確認時刻日,月,火,水,木,金,土,
　　今週,先週,2 週,3 週,4 週,5 週,1 月,2 月,3 月,4 月,5 月,6 月,7 月,8 月,9 月,10 月,11 月,12 月
```

例

```
#STATUS,MAC,IP,FIND_TIME,LAST_TIME,COMMENT,VALID,PCNAME,WGNAME,MACVNDR,Su,Mo,Tu,We,Th,Fr,Sa,
　　ThisW,LastW,2W,3W,4W,5W,Jan,Feb,Mar,Apr,May,Jun,Jul,Aug,Sep,Oct,Nov,Dec
#
停止 ,00:e0:2b:5d:9a:00,158.212.102.1,2006/11/23 11:20:46,2006/11/27 14:52:31,"L3SW",,
　"-","-","EXTREME NETWORKS",0,0,0,0,0,0,0,0,1,4,0,0,0,0,0,0,0,0,0,0,0,0,5,0
動作中　,00:0d:0b:51:8f:3f,158.212.102.205,2006/12/05 13:53:00,2006/12/08 15:20:42,"許可 PC"
　　,,"-","-","Buffalo Inc.",0,0,3,1,0,1,0,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3
```

（注）ここで示される各機器の稼働時間は、監視装置の時刻を変更した当日の情報は。正しく表示されていません。また、稼動時間は日単位の合計が、週の集計値、週の合計が月の集計値より大きくなる可能性があります。稼動時間は目安として扱ってください。

・「環境設定」
　フォーマットは、「６．１８　アップロード」を参照してください。

・「ログ」
　フォーマット(CSV 形式)

```
No,時刻,レベル,メッセージ
```

例

```
# No,Time,Level,Message
1,2004/02/14 21:00:03,情報,"MAC(00:80:c8:84:51:66), IP(192.168.0.123) is up."
2,2004/02/14 21:30:19,情報,"MAC(00:80:c8:84:51:66), IP(192.168.0.123) is down."
```

・「スイッチ一覧」
　フォーマット(CSV 形式)

```
IP アドレス,コミュニティ名 1,コミュニティ名 2,種別,予備 1(空白),予備 2(空白),コメント
```

例

```
# IP addr,name1,name2,flag, , ,Comment
192.168.102.1,public@102,,1,,,L3_SW(ルータ)
192.168.102.100,public,,,,,リピータ HUB
192.168.102.254,public,,1,,,_
```

6.18　アップロード

各種ファイルのアップロードを行います。「参照」ボタンで、アップロードしたいファイル名を指定して、「アップロード」ボタンをクリックすると、以下のファイルのアップロードが行われます。

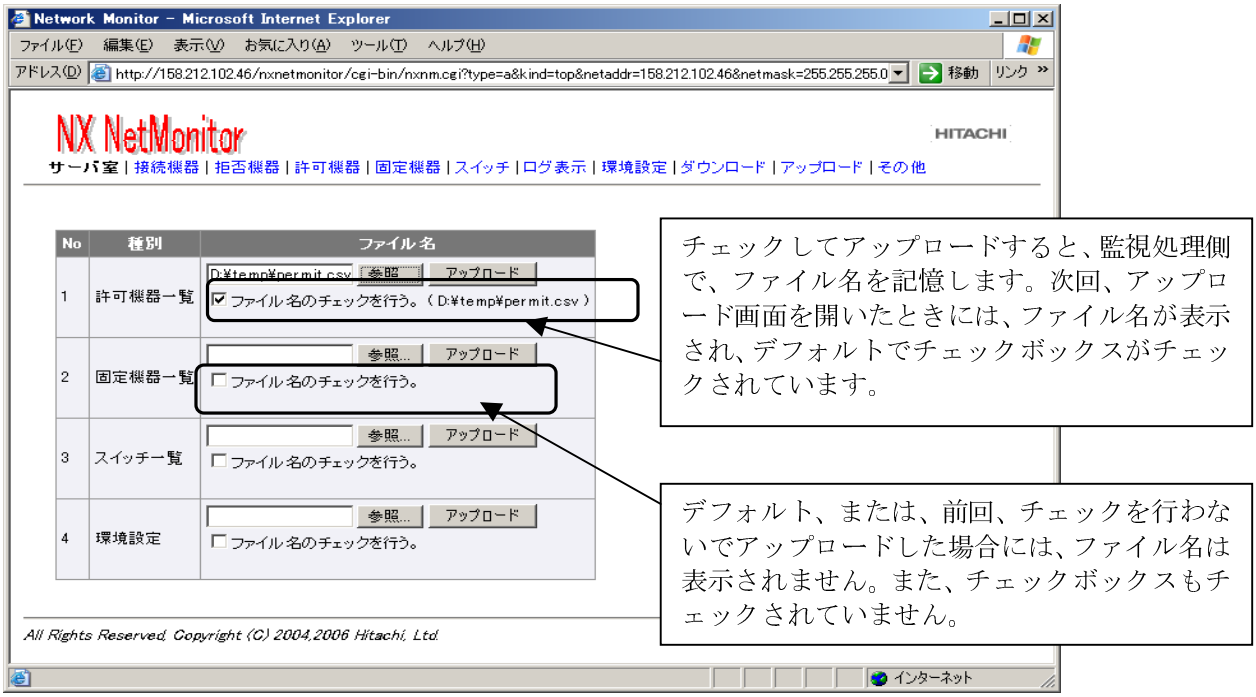
・「許可機器一覧」
現在ネットワークへの接続が許可されている機器の一覧です。許可機器とは、固定機器以外のクライアント PC などのことです。拡張子が csv のファイル以外は、アップロードは拒否されます。
登録可能な機器は、許可機器と固定機器合わせて、262140 台までです(262140=65535×4)。

・「固定機器一覧」
現在ネットワークへの接続が許可されている機器の一覧です。固定機器とは、ルータ、プリンタ、サーバ等の機器のことです。拡張子が csv のファイル以外は、アップロードで拒否されます。
登録可能な機器は、許可機器と固定機器合わせて、262140 台までです(262140=65535×4)。
なお、固定機器一覧の登録は、必須ではありません。固定機器一覧を作成せず、固定機器と許可機器を 1 つのファイルにまとめて、許可機器一覧として登録しても問題ありません。

・「排除機器一覧」
現在ネットワークへの接続を拒否する機器の一覧です。
拡張子が csv のファイル以外は、アップロードは拒否されます。登録可能な機器は、262140 台までです(262140=65535×4)。「６．２０　簡易モード」を参照してください。

・「スイッチ一覧」
スイッチ情報定義ファイルです。
「スイッチ一覧」は環境設定画面で、「不正機器特定情報」にコミュニティ名を設定している時に表示されます。

・「環境設定」
環境設定ファイルです。
拡張子が conf のファイル以外は、アップロードは拒否されます。



（注）空の許可機器一覧および固定機器一覧がアップロード（有効な許可機器・固定機器の合計の件数が０）された場合、全ての機器が排除され、通信できなくなることを防止するために、監視装置では排除処理を行いません。この時、監視装置は有効な許可機器、固定機器一覧が登録されるまで、定期的にこの旨のメッセージをログに出力します。

アップロードするファイルのフォーマットは、以下の通りです。

・許可機器一覧
・固定機器一覧
・排除機器一覧（「６．２０　簡易モード」を参照してください。）

フォーマット(CSV 形式)

MAC アドレス, IP アドレス 1, IP アドレス 2, 停止期間監視, 有効期限, コメント

・MAC アドレスはの区切り文字は':'または'-'です。
・IP アドレスは、ドット形式です。
・IP アドレスを指定する場合は、IP アドレス 1 に指定し、IP アドレス 2 は空欄にします。
・IP アドレスの範囲を指定する場合には、IP アドレス 1 に開始アドレス、IP アドレス 2 に終了アドレスを指定します。
・環境設定で指定した期間起動されなかった機器が起動された時に、ネットワークから切り離す場合には、停止期間監視に'Y'を指定します。切り離しを行わない場合には、空欄とします。簡易モード(排除機器一覧)の場合には、停止期間監視は空欄としてください(指定しても無視されます)。
・有効期限は、日単位で指定します。指定した日の次の日の０時０分０秒以降に、ネットワークから排除されます。指定フォーマットは、"年.月.日"(例：2004.04.30)です。無期限の場合には、空欄としてください。簡易モード(排除機器一覧)の場合には、有効期限は空欄としてください（指定しても無視されます)。
・コメントは３２バイト以内、半角英数、'_'、または日本語が指定可能です。
・行の先頭に "#" があればその行は無視します。
・アップロードするファイルは Microsoft(R) Windows(R) の搭載された PC で作成したものを前提としています（文字コードは Shift-JIS、改行コードは CRLF)。
・MAC ベンダを指定して許可する場合には、MAC アドレスの上位３バイトにベンダ ID を指定し、下位３バイトには０を設定します。

例

```
# MAC, IP1, IP2, UNUSED, TERM, COMMENT
#
00:80:c8:84:51:01,192.168.0.1,,,,MAC と IP で指定
00:80:c8:84:51:02,192.168.0.2,,Y,,停止期間監視を指定
00:80:c8:84:51:03,192.168.0.10,192.168.0.20,,,MAC と IP の範囲で指定
00:80:c8:84:51:04,,,,2004.04.30,MAC のみと有効期限の指定
,192.168.0.5,,,,IP のみで指定
00:80:c8:00:00:00,,,,,MAC ベンダ指定
```

・スイッチ一覧

フォーマット(CSV 形式)

```
IP アドレス, コミュニティ名 1 , コミュニティ名 2 , 種別, 予備 1(空白), 予備 2(空白), コメント
```

詳細は「６．１４　スイッチ情報の表示」を参照してください。

例

```
# IP addr,name1,name2,flag, , ,Comment
192.168.102.1,public@102,,1,,,L3_SW(ルータ)
192.168.102.100,public,,,,,リピータ HUB
192.168.102.254,public,,1,,,_
```

・環境設定

フォーマット(テキストファイル)

omit	: 排除モード(Y または N)
trap_ver	: SNMP TRAP バージョン(1 または 2)
trap_addr	: SNMP トラップ送信先 IP アドレス
community	: SNMP コミュニティ名(32 バイト)
trap_level	: SNMP トラップレベル(W,O,I : W=警告,O=操作,I=情報)
max_ent_cnt	: 最大接続機器台数(256 - 8192)
ptrl_interval	: 監視間隔 (60 - 3000, または、0)
ptrl_addr1	: 監視開始 IP アドレス
ptrl_addr2	: 監視終了 IP アドレス
netout	: 監視対象ネットワーク外は無視する(Y または N)
unused_period	: 許容停止期間(1 - 8760、または、0)
det_community	: 不正機器の位置を特定する時に、MIB 収集のための SNMP コミュニティ名(32 バイト)
k_keneki	: 検疫支援モード(Y または N)
notice_ipaddr	: 許可機器起動の通知先 IP アドレス
notice_portno	: 許可機器起動の通知先ポート番号(0 - 65535)
keep_manu_ope	: 手動操作(許可/拒否)保持フラグ(Y または N)
termout_manu_ope	: 無効状態機器の手動操作フラグ(Y または N)
startup_force_omit	: 許可機器起動時の強制排除フラグ(Y または N)
easy_mode	: 動作モード(Y または N)(N:通常, Y:簡易)
detect_mode	: 検出モード(Y または N)
event_ipaddr	: 独自トラップ送信先 IP アドレス
event_portno	: 独自トラップ送信先ポート番号(0 - 65535)
pc_name	: コンピュータ名の収集フラグ(Y または N)
mac_vender	: MAC アドレスのベンダ指定可否フラグ(Y または N)
omit_level	: 排除レベル (H(高), M(中), L(低))
max_log_case	: 最大ログ件数(4096 - 65536)
keep_refusal	: 許可機器登録時、接続を許可する(Y または N)
isolate_netout	: 対象外 IP アドレスの機器を排除する(Y または N)
ipdup_log	: IP アドレス重複を検出する(Y または N)
name_change_log	: コンピュータ名変更を検出
ipdup_exclusion1	: 重複検出除外 IP アドレス 1(0.0.0.0 なら除外 IP ｱﾄﾞﾚｽなし)
ipdup_exclusion2	: 重複検出除外 IP アドレス 2(0.0.0.0 なら除外 IP ｱﾄﾞﾚｽなし)
ipdup_exclusion3	: 重複検出除外 IP アドレス 3(0.0.0.0 なら除外 IP ｱﾄﾞﾚｽなし)
ipdup_exclusion4	: 重複検出除外 IP アドレス 4(0.0.0.0 なら除外 IP ｱﾄﾞﾚｽなし)
ipdup_exclusion5	: 重複検出除外 IP アドレス 5(0.0.0.0 なら除外 IP ｱﾄﾞﾚｽなし)
device_save_limit	: 接続機器保持期間(日) (1 - 365, または、0)
quarantine_permit	: 登録機器のみ検疫可フラグ(Y または N)

・設定内容は「６．16　環境設定」を参照してください。

・各項目の設定がない場合、設定に誤りがある場合には、デフォルト値として動作します。
デフォルト値は、「６．16　環境設定」を参照してください。

例

```
#
omit                :       Y
trap_ver            :       1
trap_addr           :       158.212.102.46
community           :       public
trap_level          :       I
max_ent_cnt         :       4096
ptrl_interval       :       200
ptrl_addr1          :       0.0.0.0
ptrl_addr2          :       0.0.0.0
netout              :       Y
unused_period       :       0
det_community       :       public
k_keneki            :       N
notice_ipaddr       :       0.0.0.0
notice_portno       :       0
keep_manu_ope       :       N
termout_manu_ope:           N
startup_force_omit:         N
easy_mode           :       N
detect_mode         :       Y
event_ipaddr        :       158.212.102.46
event_portno        :       12345
pc_name             :       Y
mac_vendor          :       N
omit_level          :       M
max_log_case        :       4096
ipdup_log           :       Y
keep_refusal        :       N
isolate_netout      :       N
name_change_log:            Y
ipdup_exclusion1 :          0.0.0.0
ipdup_exclusion2 :          0.0.0.0
ipdup_exclusion3 :          0.0.0.0
ipdup_exclusion4 :          0.0.0.0
ipdup_exclusion5 :          0.0.0.0
device_save_limit:          90
quarantine_permit:          Y
```

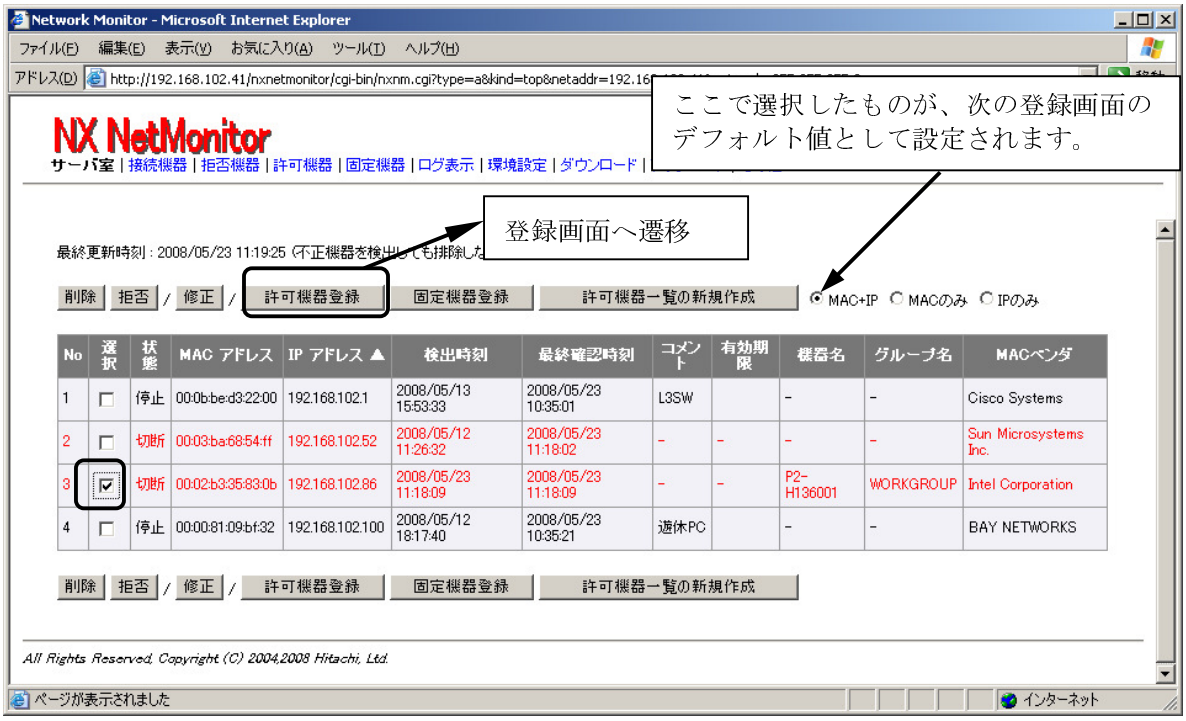
6.19 ブラウザからの直接編集機能

許可機器・固定機器の変更は、CSV 形式のファイルを作成し、それをアップロードすることにより行う方法と、以下に説明する「ブラウザからの直接編集機能」を利用する方法があります。
「ブラウザからの直接編集機能」では、監視装置内の許可機器一覧等を編集します。許可機器一覧等を編集後は、統合管理装置でダウンロードを実行し、編集した許可機器一覧等のバックアップを取る運用としてください。

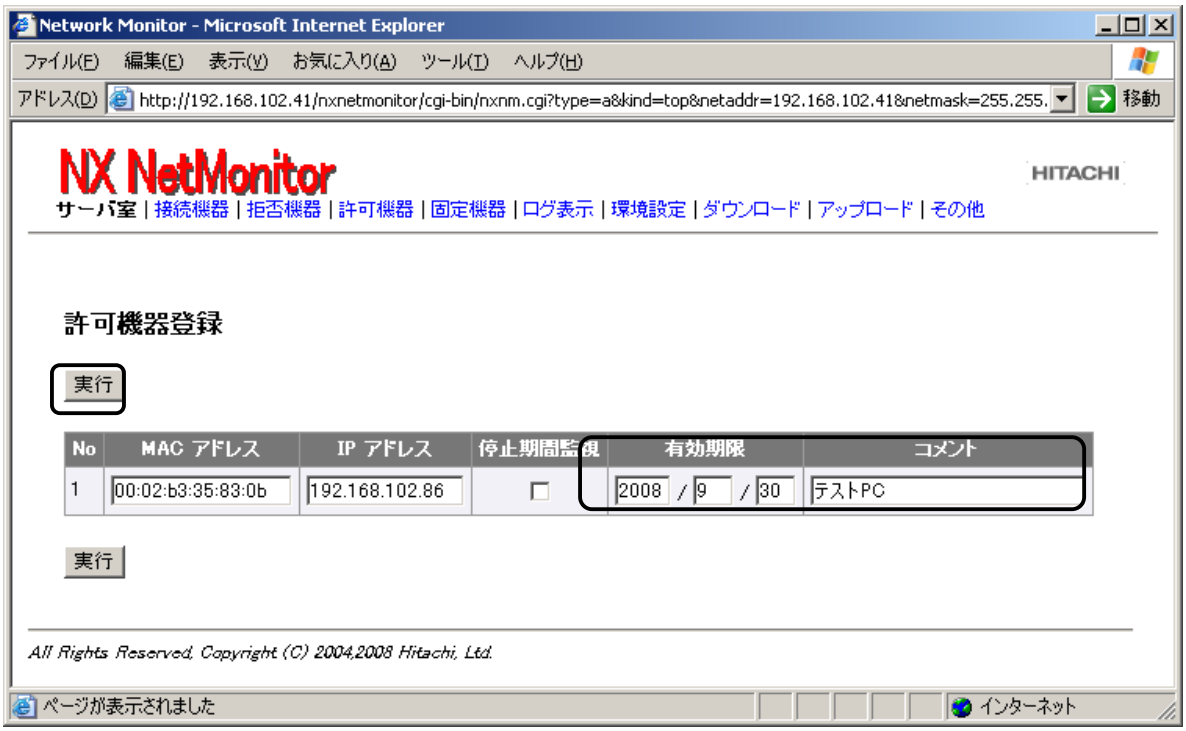
6.19.1 拒否された機器の許可

接続機器一覧、または、拒否機器一覧から、拒否された機器を選択して、許可機器一覧/固定機器一覧に追加することが可能です。以下に、操作手順を示します。
（例は、許可機器の登録手順ですが、固定機器も同様の操作で登録できます。）

1）許可機器一覧に追加する機器をチェックし、「許可機器登録」ボタンをクリックします。

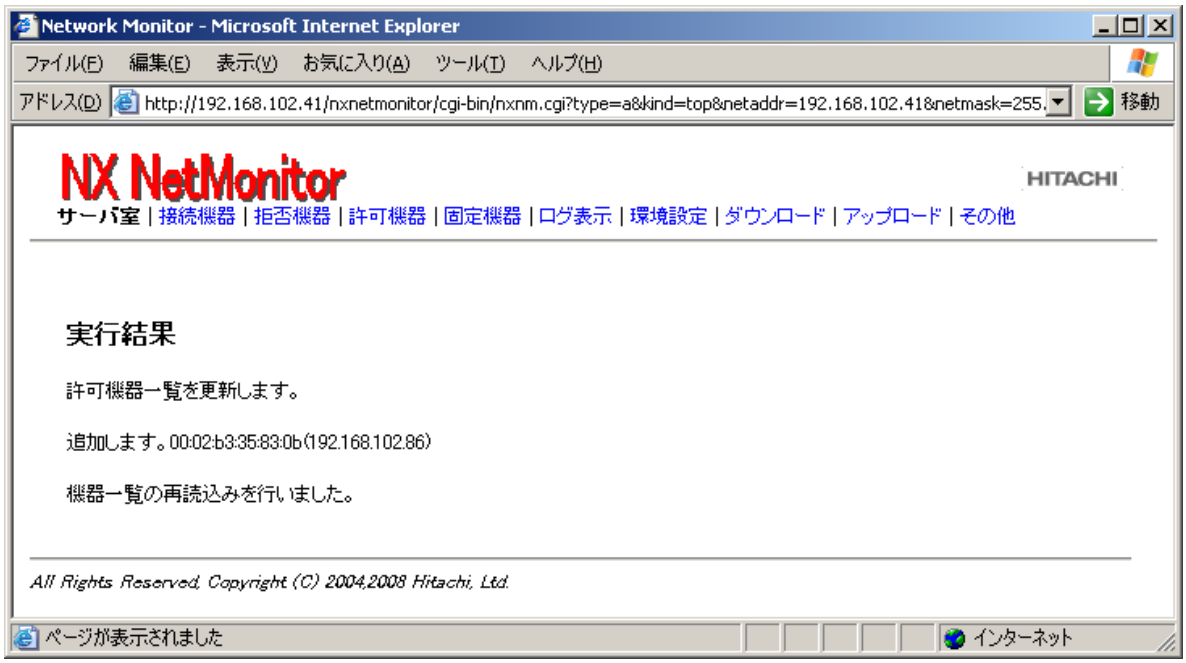


2）許可機器登録画面が表示されます。
必要な情報を入力して、「実行」ボタンをクリックします。



3）確認のメッセージが出力されますので、「OK」ボタンをクリックします。

4）許可機器一覧が更新されます。

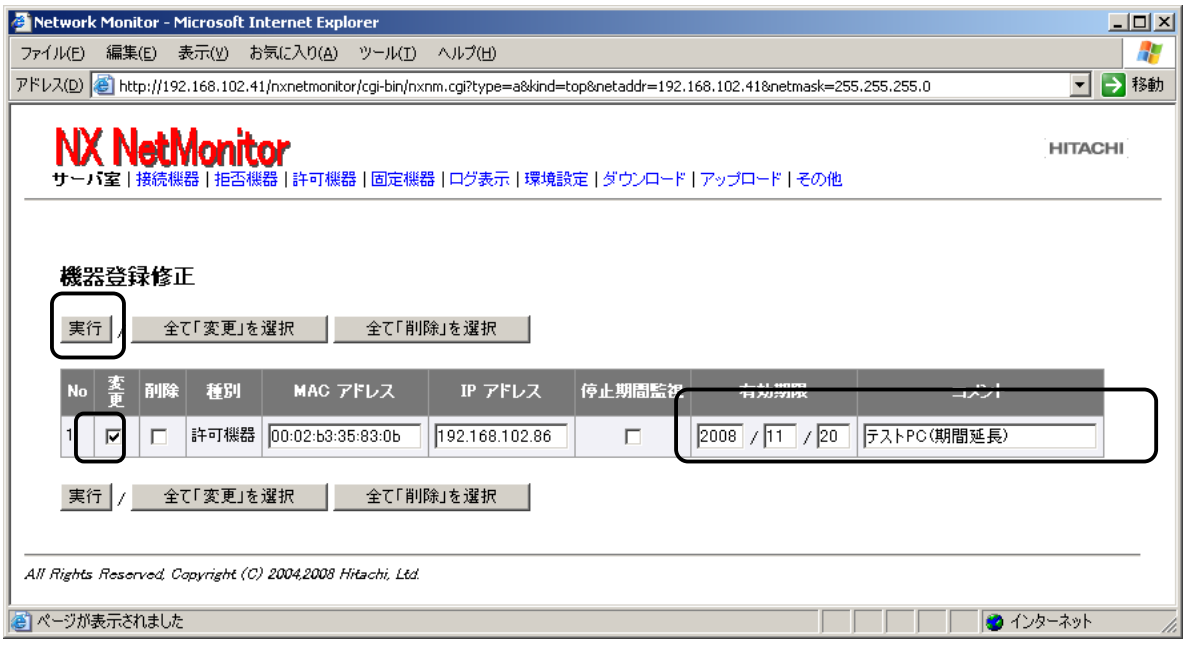


6.19.2 接続機器・拒否機器一覧からの修正

接続機器一覧、または、拒否機器一覧から、許可された機器を選択して、許可機器一覧/固定機器一覧を修正することが可能です。以下に、操作手順を示します。
（例は、許可機器一覧を修正する手順ですが、固定機器でも同様の操作で修正できます。）

1）許可機器一覧を修正する機器をチェックし、「修正」ボタンをクリックします。

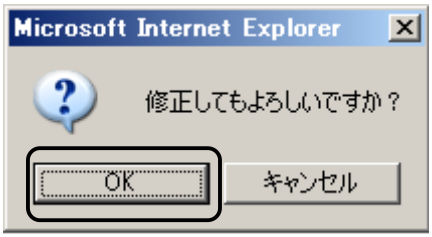
2）機器登録修正画面が開きます。設定内容を修正します。
「変更」または「削除」にチェックして、[実行]ボタンをクリックします。



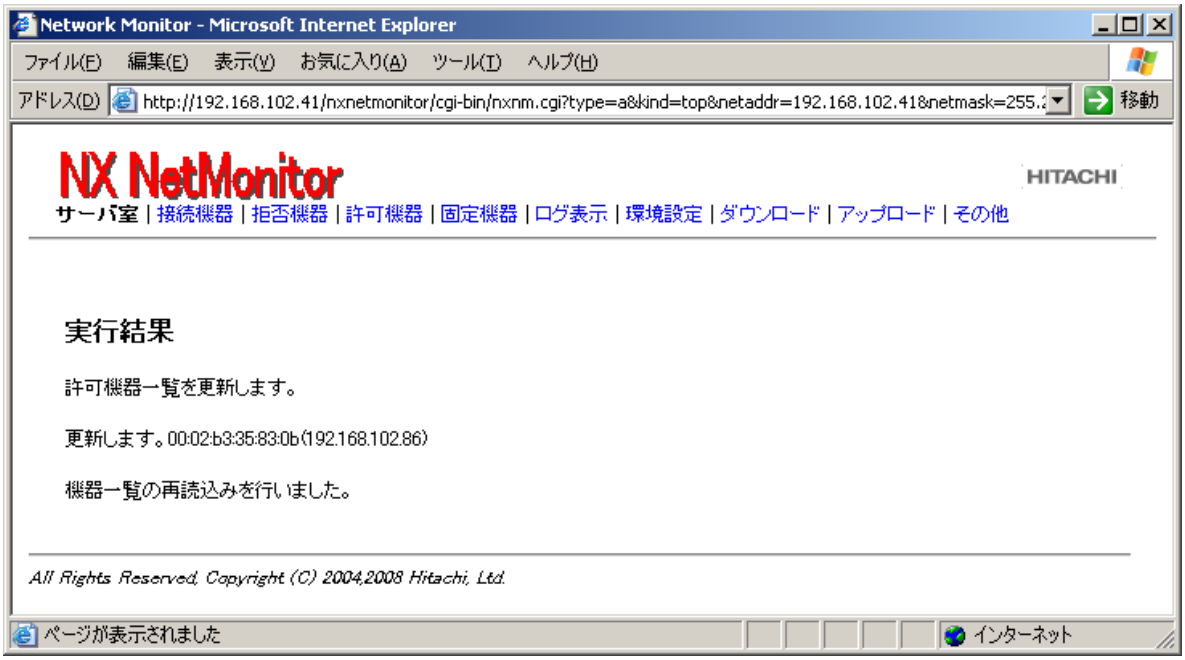
※1　MAC アドレス、IP アドレスを重複して定義することはできません。すでに CSV ファイルをアップロードして登録されている場合に修正を行うと、MAC アドレス、IP アドレスが一致する機器の情報は、修正した内容に更新されることがあります。

※2　IP アドレスの範囲指定で定義している場合には、修正できません（表示もされません）。CSV ファイルを編集して、アップロードしてください。なお、IP アドレスの範囲が混在している場合は、本機能で修正しても、その定義は変更なく、そのまま保持されます。本機能で修正すると、IP アドレスの範囲指定の部分が削除されてしまうことはありません。

3）確認のメッセージが出力されますので、「OK」ボタンをクリックしてください。



4）許可機器一覧が更新されます。



6.19.3 許可機器・固定機器一覧からの修正

許可機器一覧、または、固定機器一覧から、機器を選択して、許可機器一覧/固定機器一覧を修正することが可能です。以下に、操作手順を示します。
（例は、許可機器一覧ですが、固定機器でも同様の操作で修正できます。）

１）許可機器一覧を修正する機器をチェックし、「修正」ボタンをクリックします。

２）機器登録修正画面が開きます。
以降は、「６．１９．２．接続機器・拒否機器一覧からの修正」と同様の操作となります

6.19.4 新規追加

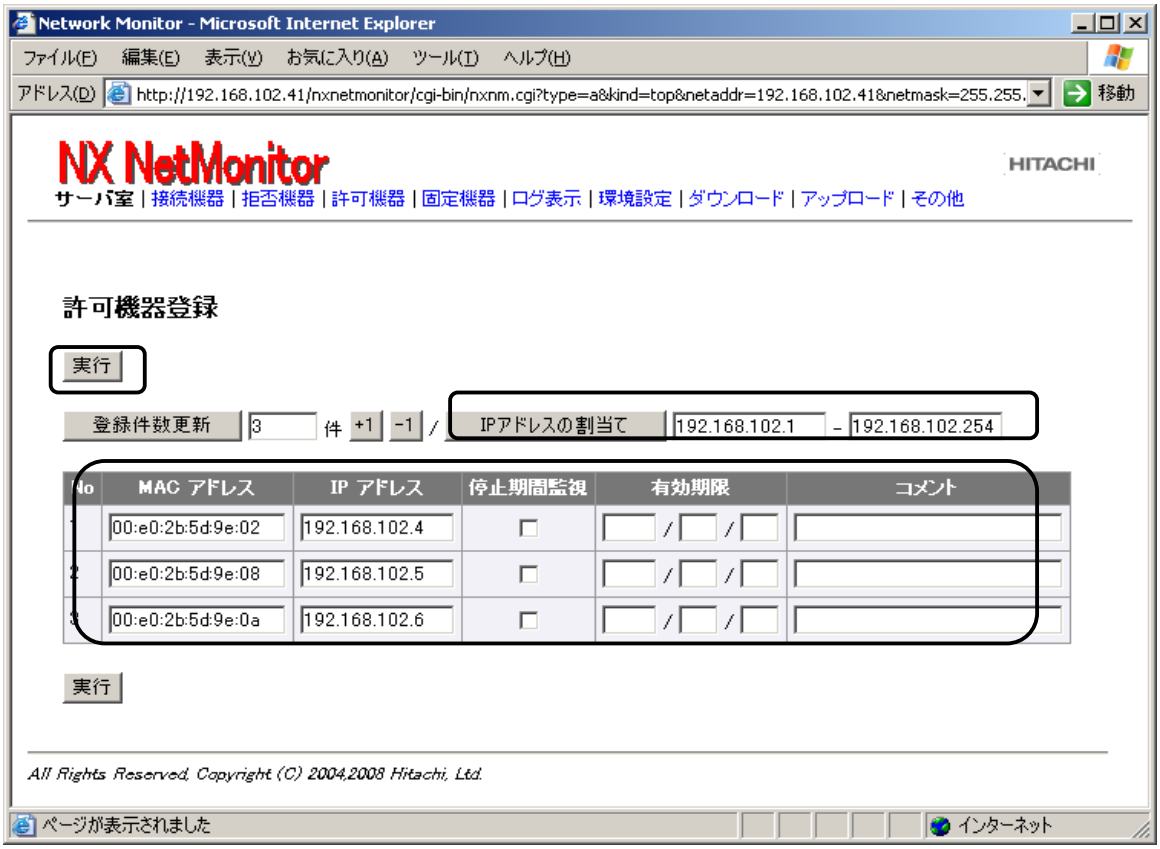
許可機器一覧、または、固定機器一覧から、新規に機器を登録することが可能です。
以下に、操作手順を示します。
（例は、許可機器一覧ですが、該当機器が固定機器でも同様の操作で登録できます。）

１）「登録」ボタンをクリックします。

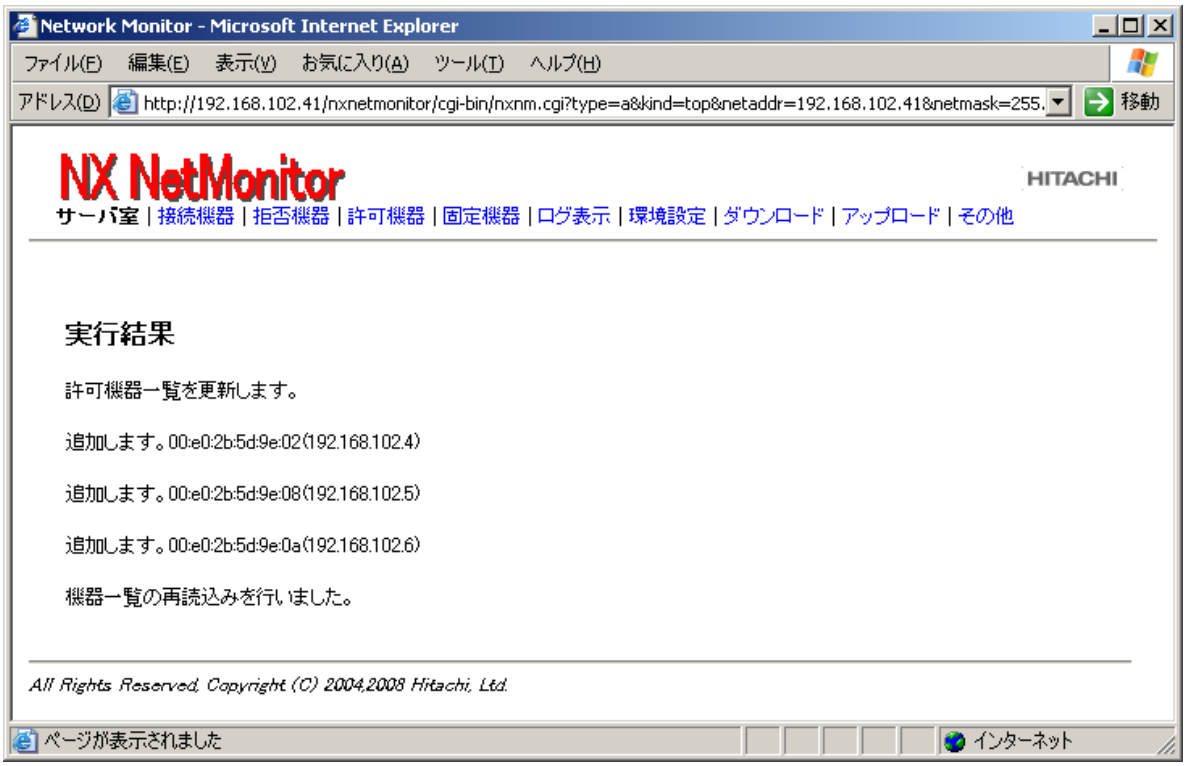
２）許可機器登録画面が開きます。
[登録件数更新]、もしくは、[+1][-1]ボタンをクリックして、登録する機器の数を調整します。
１回で、最大 100 件まで登録可能です。100 件以上登録する時には、登録作業を複数回に分けて行ってください。

(注) IP アドレスの範囲指定はできません。範囲指定を行いたい場合には、CSV 形式のファイルをアップロードしてください。

3）許可機器登録画面では、IP アドレスの割当てを行うことが可能です。
許可機器・固定機器に存在しない IP アドレスを割り当てます。
割り当て可能な IP アドレスの範囲を指定して、「IP アドレスの割当て」ボタンをクリックすると割り当てられます。未使用の IP アドレスがない場合には、IP アドレスは表示されません。
必要な情報を入力して、「実行」ボタンをクリックします。



4）許可機器一覧が更新されます。



6.20 簡易モード

簡易モードとは、ネットワークへの接続を許可する機器を登録する運用(通常モード)とは逆に、デフォルトで全ての機器の接続を許可し、排除したい機器の情報を登録すると（排除機器一覧)、指定された機器のネットワーク接続を拒否します。なお、許可/固定機器一覧との共存はできません。
動作モードは、環境設定の「基本設定画面」では表示されません。「詳細設定画面」を表示させて設定してください。

動作モードの項目
・通常モード：許可/固定機器一覧を使用
・簡易モード：排除機器一覧を使用
のどちらかを選択する必要があります。

なお、排除機器一覧のファイル形式は、許可機器一覧と同じです。（停止期間監視、有効期限の指定は無効となります。)

＜ 簡易モード(排除機器一覧を使用)の設定方法 ＞
環境設定画面の「動作モード」で、簡易(排除機器一覧を使用する)を選択します。

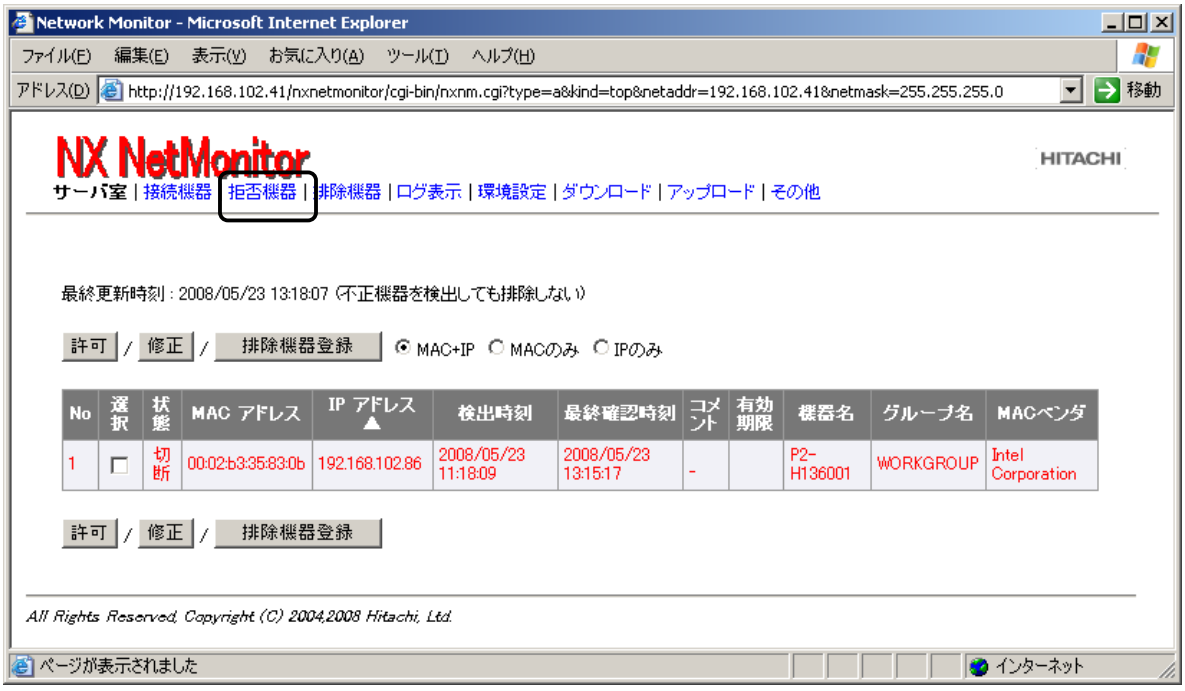
また、排除機器一覧を使用する場合、ブラウザの監視画面が通常モード(許可/固定機器一覧を使用)と一部異なります。次に，監視画面を示します.

＜接続機器一覧＞

簡易モードでは、メニューに排除機器一覧が表示されます。
「排除機器登録」ボタンをクリックすると、排除機器を登録することができます。
対象の機器にチェックをつけて、「修正」ボタンをクリックすると、排除機器一覧を修正することができます。

＜拒否機器一覧＞

「排除機器登録」ボタンをクリックすると、排除機器を登録することができます。
対象の機器にチェックをつけて、「修正」ボタンをクリックすると、排除機器一覧を修正することができます。



＜排除機器一覧＞

排除機器一覧画面では、「登録」ボタンで、機器を排除機器一覧に登録することが出来ます。
「修正」ボタンで、登録済の排除機器を修正することができます。
「検索」ボタンで排除機器一覧に登録されている機器を検索することができます。

＜ログ表示＞

通常モード(許可機器一覧を使用する)と同じです。

＜環境設定＞

通常モード(許可機器一覧を使用する)と同じです。

＜その他＞

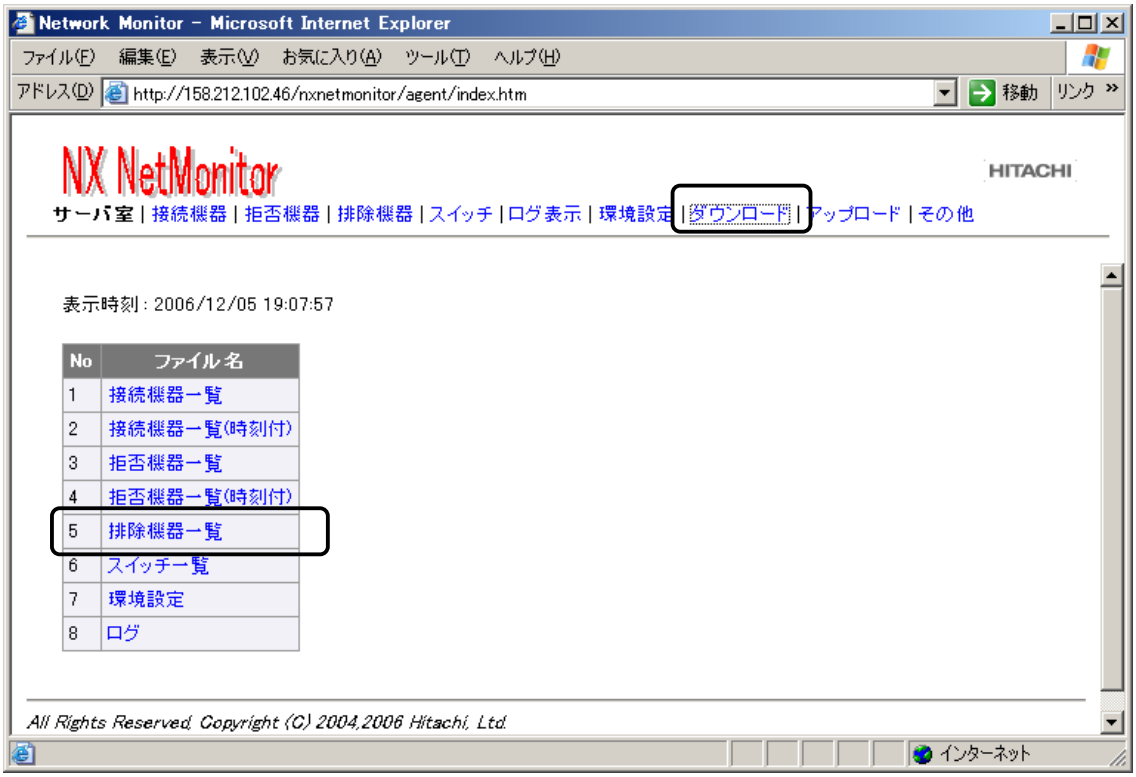
通常モード(許可機器一覧を使用する)と同じです。

＜スイッチ＞

スイッチメニューは、環境設定画面の不正機器特定情報に「コミュニティ名」が設定されている時に表示されます。設定内容は、通常モード(許可機器一覧を使用する)と同じです。

＜ダウンロード＞

通常モードの許可機器一覧ではなく、排除機器一覧がダウンロードできます。
操作方法は通常モードと同じです。
スイッチ一覧は、環境設定画面の不正機器特定情報に「コミュニティ名」が設定されている時に表示されます。



＜アップロード＞

通常モードの許可機器一覧ではなく、排除機器一覧をアップロードします。
操作方法は通常モードと同じです。種別のスイッチ一覧は、環境設定画面の不正機器特定情報に「コミュニティ名」が設定されている時に表示されます。

6.21 ユーザ権限の付与

ブラウザから監視画面を参照する時のログイン名により、

・管理者ユーザ　　：全操作可能
・参照限定ユーザ　：参照のみ

と、画面操作を制限することを可能です。
参照限定ユーザの設定方法は、「５．インストール手順」を参照ください。
また、参照限定ユーザ場合、ブラウザの監視画面が管理者ユーザと一部異なります。以下に、監視画面を示します。

＜接続機器一覧＞
画面上部のメニューにアップロードやダウンロードが表示されません。
「拒否」や「登録」ボタンが表示されずに、参照のみが可能です。

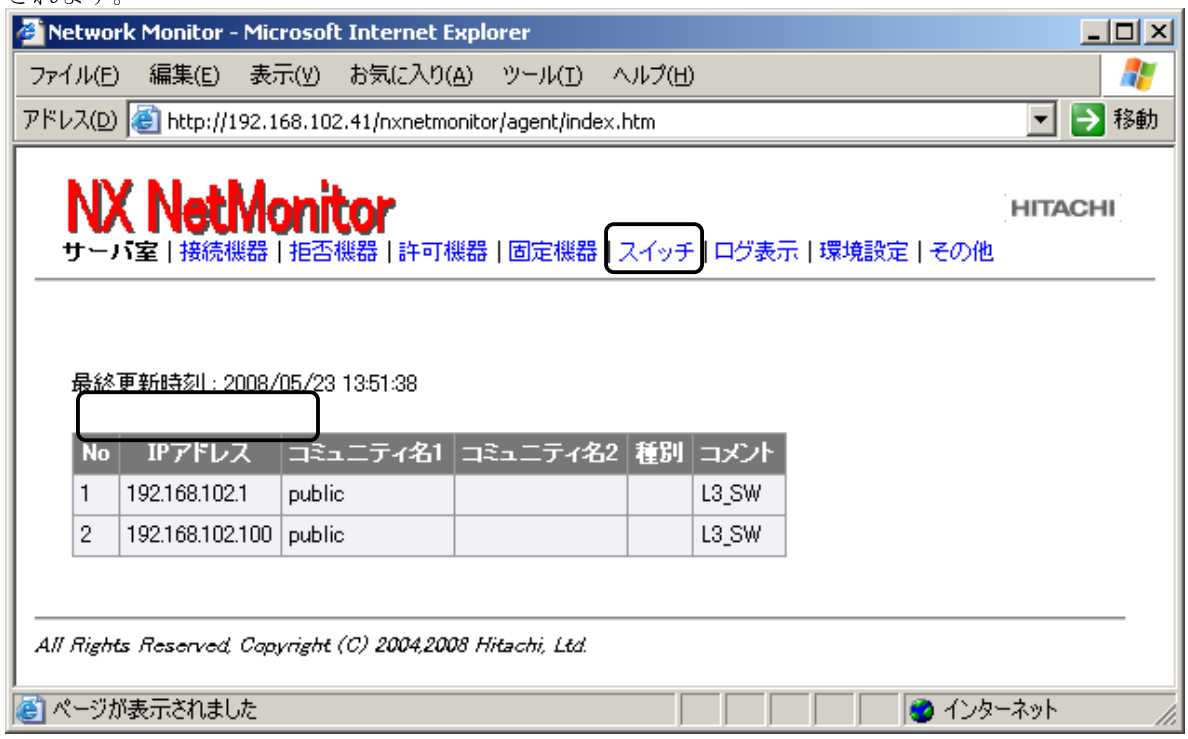
＜拒否機器一覧＞
画面上部のメニューにアップロードやダウンロードが表示されません。
[許可]や[登録]ボタンが表示されず、参照のみが可能です。

＜許可機器一覧、固定機器一覧、排除機器一覧＞

画面上部のメニューにアップロードやダウンロードが表示されません。
登録、修正ボタンが表示されないため、機器の追加・更新はできません。検索は可能です。

＜スイッチ＞

登録、修正ボタンが表示されないため、スイッチ情報の追加・更新はできません
スイッチメニューは、環境設定の不正機器特定情報に「コミュニティ名」が設定されている時に表示されます。

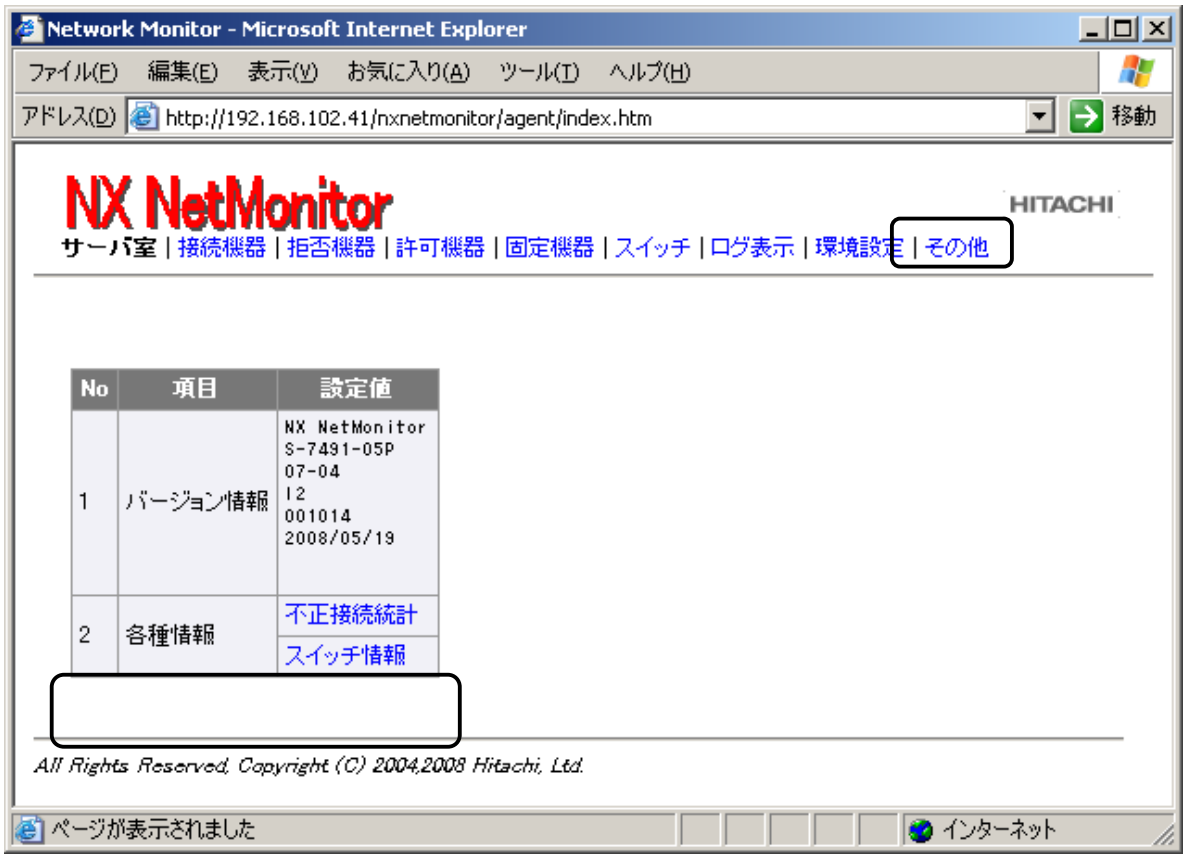


＜ログ表示＞
ログは参照のみのため、管理者ユーザと同じ画面になります。

＜環境設定＞
「更新」ボタンが表示されないため、参照のみが可能です。

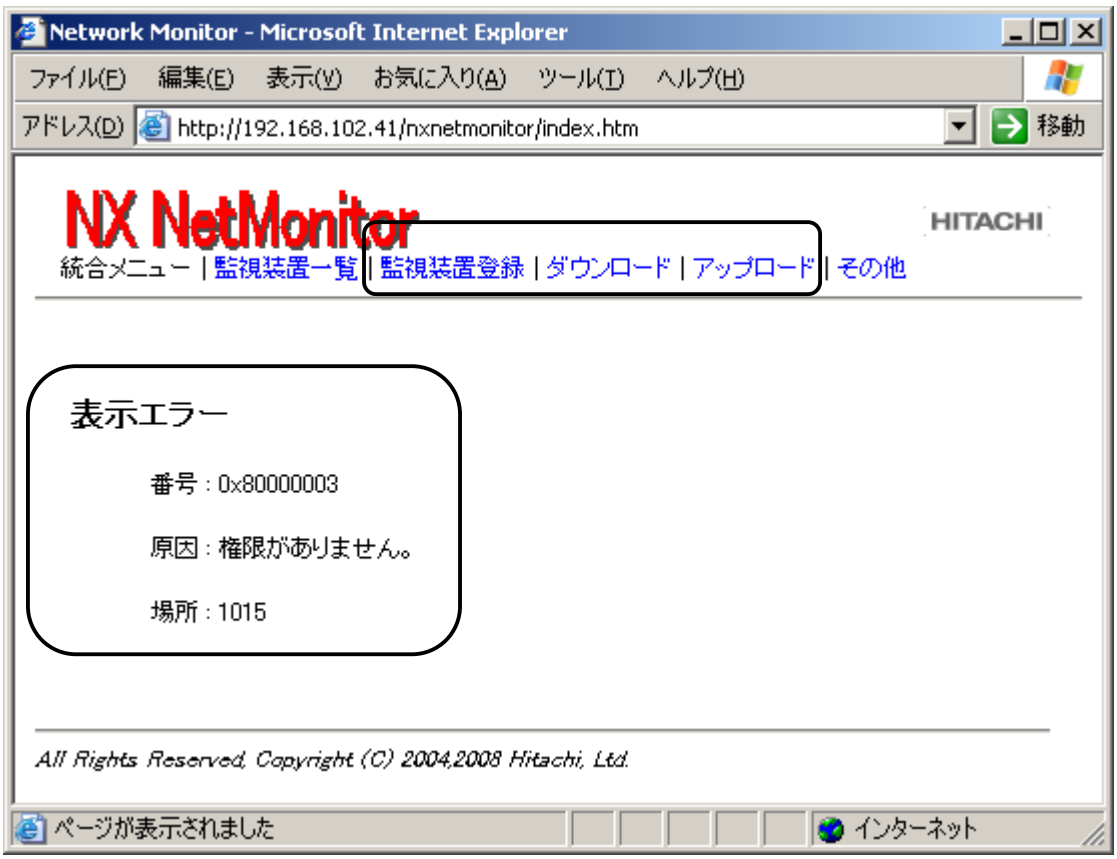
＜その他＞

No 3 の起動/停止項目がないため、NX NetMonitor の起動/停止ができません。
各種情報の「スイッチ情報」は、環境設定の不正機器特定情報に「コミュニティ名」が設定されている時に表示されます。



＜統合メニュー＞

統合メニューは、「監視装置一覧」、「ネットワーク一覧」、「その他」以外のメニューは、権限がないため、エラーとなります



6.22　その他メニュー

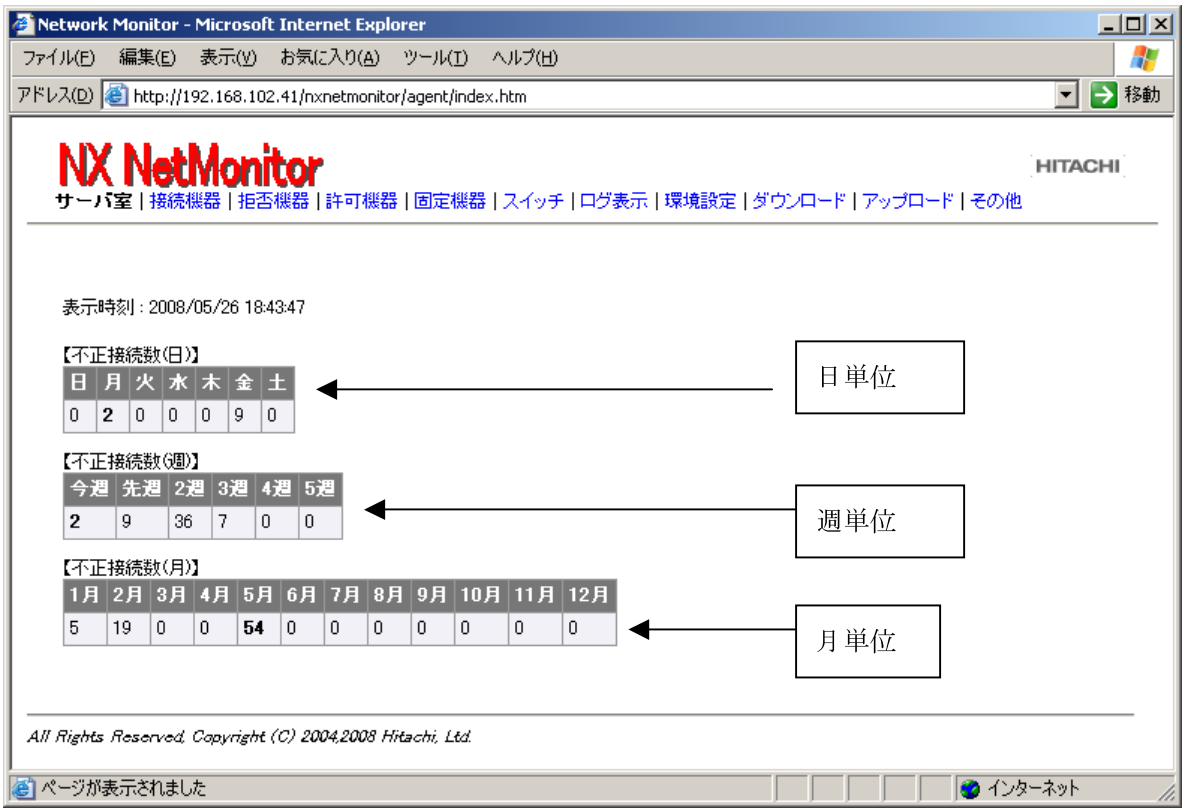
NX NetMonitor のバージョン情報を表示します。
また、NX NetMonitor の起動、停止および状態の表示が、ブラウザ上からも行えます。
各種情報情報の「スイッチ情報」は、環境設定の不正機器特定情報に「コミュニティ名」が設定されている時に表示されます。

※　No. 3　「起動／停止」にある「ログ表示」は、メニューの「ログ表示」とは異なり、
開発元がトラブル解析に使用するための情報ですので、通常の運用で参照する必要はありません。

1）バージョン番号
バージョン番号は、監視対象のネットワークで動作している、NX NetMonitor の PP 型式、バージョン番号などを表示します。

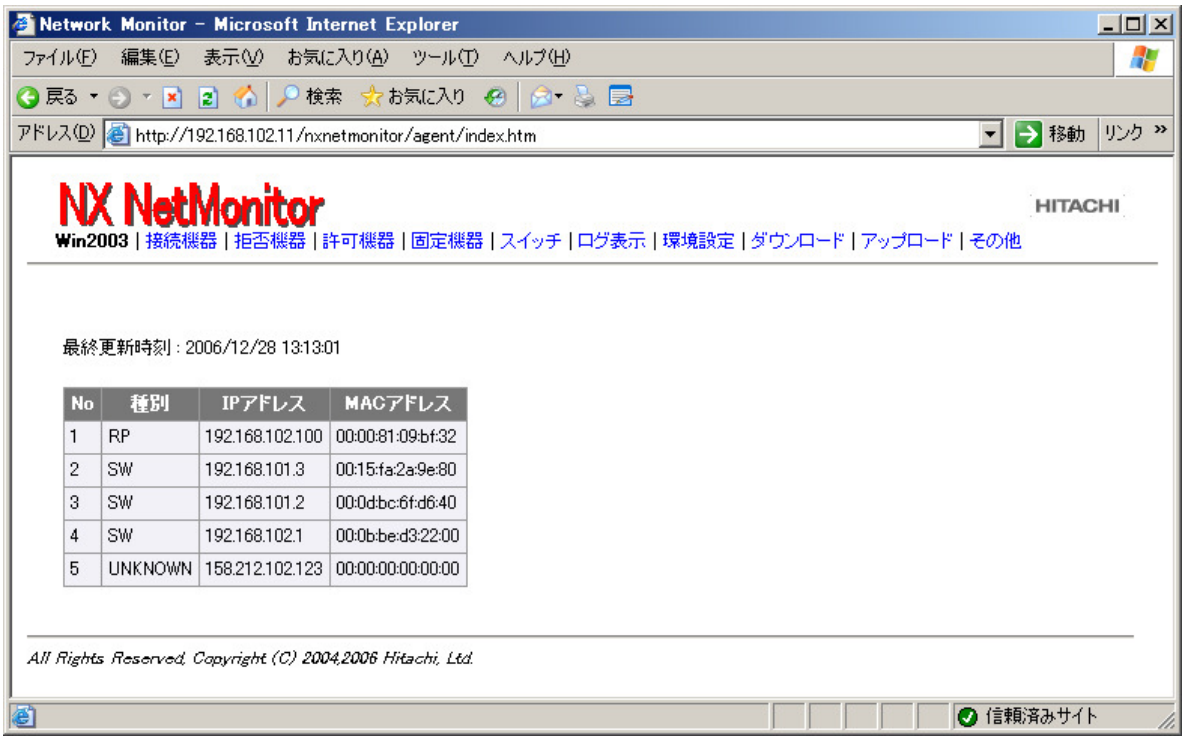
2）各種情報情報

・不正接続統計表示
不正接続統計は、日、週、月単位に不正な機器(未登録の機器や有効期限切れの機器など)が何回ネットワークに接続されたかを表示します。この数字は、不正な機器の台数ではありませんので注意してください。不正な機器が何台接続されているかは、拒否機器一覧を参照してください。
不正接続統計を表示した当日は太字で表示します。当日より後に表示されている情報は過去の情報になります。例えば、当日が水曜日であった場合、木曜日から土曜日の情報はその前の週の情報になります。



・スイッチ情報表示

スイッチ情報は、不正機器を検出したときに、不正機器が接続されているスイッチのアドレスやポートの位置を特定するため、NX　NetMonitor が認識しているスイッチの一覧を表示します。



スイッチ情報は以下のように表示されます。

No	種別	意味
1	SW	スイッチ
2	RP	リピータ
3	UNKOWN	指定された IP アドレスが見つからないか、スイッチの定義情報が誤っている。 MAC アドレスは 0 で表示されます。

SW,RP の機器は、NX NetMonitor が MIB を収集する機器と認識したものです。

3）起動／停止

NX NetMonitor の起動、停止、状態表示をおこないます。

NX NetMonitor の起動・停止を実行した場合は、下記のように表示されます。

・NX NetMonitor の状態表示

```
実行結果

nxnmd (pid 1504) is running...
nxnmptrl (pid 1503) is running...
nxnmtmr (pid 1502) is running...
nxnmdetc (pid 1501) is running...
nxnminit (pid 1500) is running...

起動指定

192.168.0.31
```

監視プロセスの PID です。1 台の監視装置で複数のサブネットワークを監視している場合、複数起動されます。

監視対象ネットワークでの監視装置の IP アドレスです。1 台の監視装置で複数のサブネットワークを監視している場合、複数起動されます。

・NX NetMonitor の起動

```
実行結果

Stopping NetworkMonitor services
Stopping NetworkMonitor services end
Starting NetworkMonitor services
NetworkMonitor start [192.168.0.31] : start up OK
Starting NetworkMonitor services end
```

すでに起動されていても一度停止してから、起動します。再起動となります。

1 台の監視装置で複数のサブネットワークを監視している場合、複数起動されます。

・NX NetMonitor の停止

```
実行結果

Stopping NetworkMonitor services
Stopping NetworkMonitor services end
```

6.23 監視画面のカスタマイズ

NX NetMonitor の監視画面ではカスタマイズにより、以下のボタンやメニューの表示/非表示を選択することができます。
具体的には、custom.txt ファイルに表示/非表示にする項目を設定します。
custom.txt はインストールディレクトリの conf の下に作成します。custom.txt ファイルはデフォルトでは提供されませんので、表示をカスタマイズする場合には、custom.txt ファイルを作成してください。

1）設定ファイルのパス

Windows 版
c:¥nx¥netmonitor¥agent¥conf¥custom.txt　(c:¥nx¥netmonitor¥agent にインストール時)

Linux 版
/usr/etc/nxnetmonitor/conf/custom.txt

設定内容

No	表示/非表示項目	設定項目	設定値	備考
1	許可ボタン	permit	N or Y	拒否機器画面の項目です。
2	拒否ボタン	refuse	N or Y	接続機器画面の項目です。
3	許可機器一覧の新規作成ボタン	allpermit	N or Y	接続機器画面の項目です。
4	IP アドレスの自動割当ボタン	allocip	N or Y	許可/固定機器の登録画面の項目です。
5	検疫通信情報メニュー	quarantine	N or Y	その他メニューの項目です。 Linux 版のみ有効です。

項目を表示する場合は「Y」、非表示にする場合は「N」を設定します。

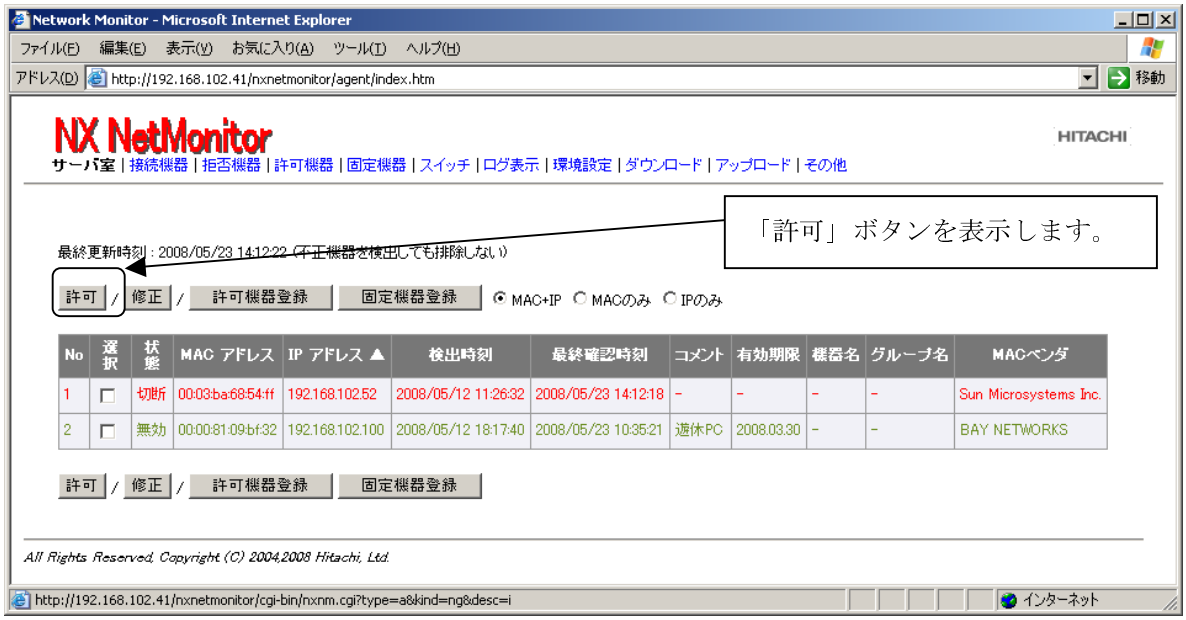
2）設定例

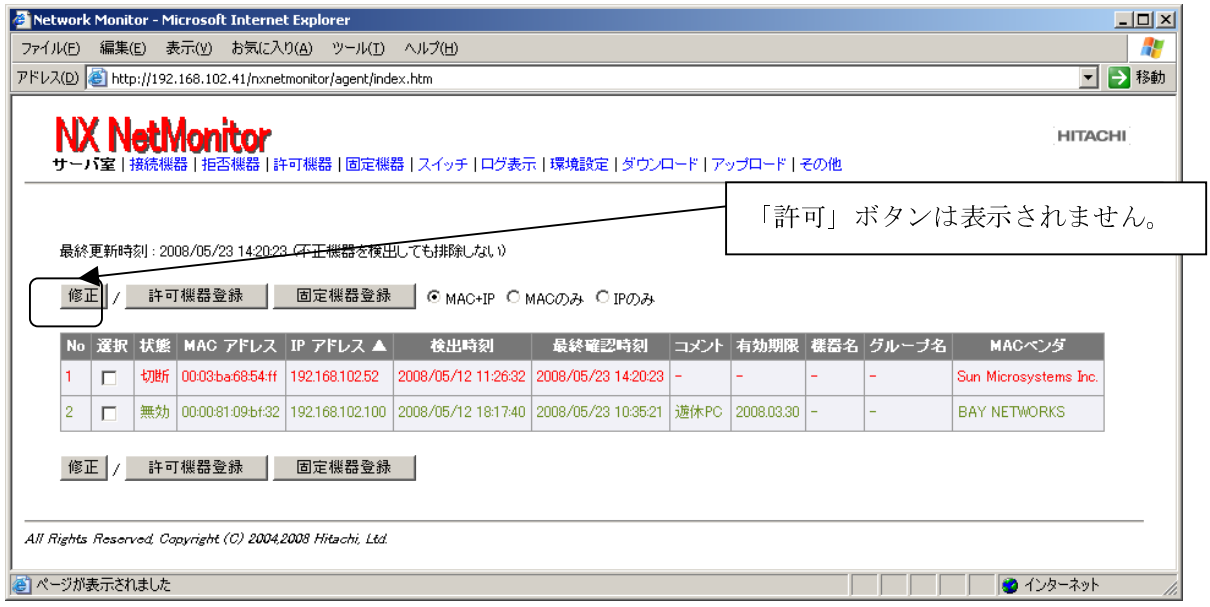
custom.txt

```
permit：N
refuse：N
allpermit：N
allocip：N
quarantine：N
```

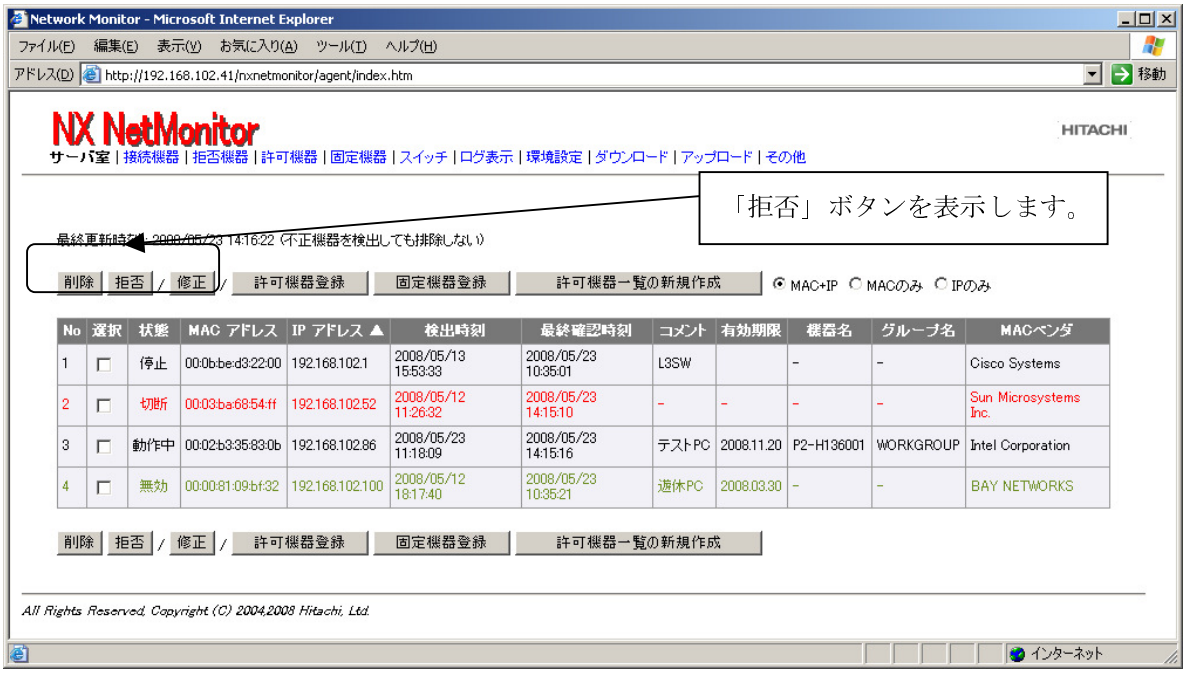
3）表示例

3-1) 許可ボタンの表示/非表示（拒否機器一覧）

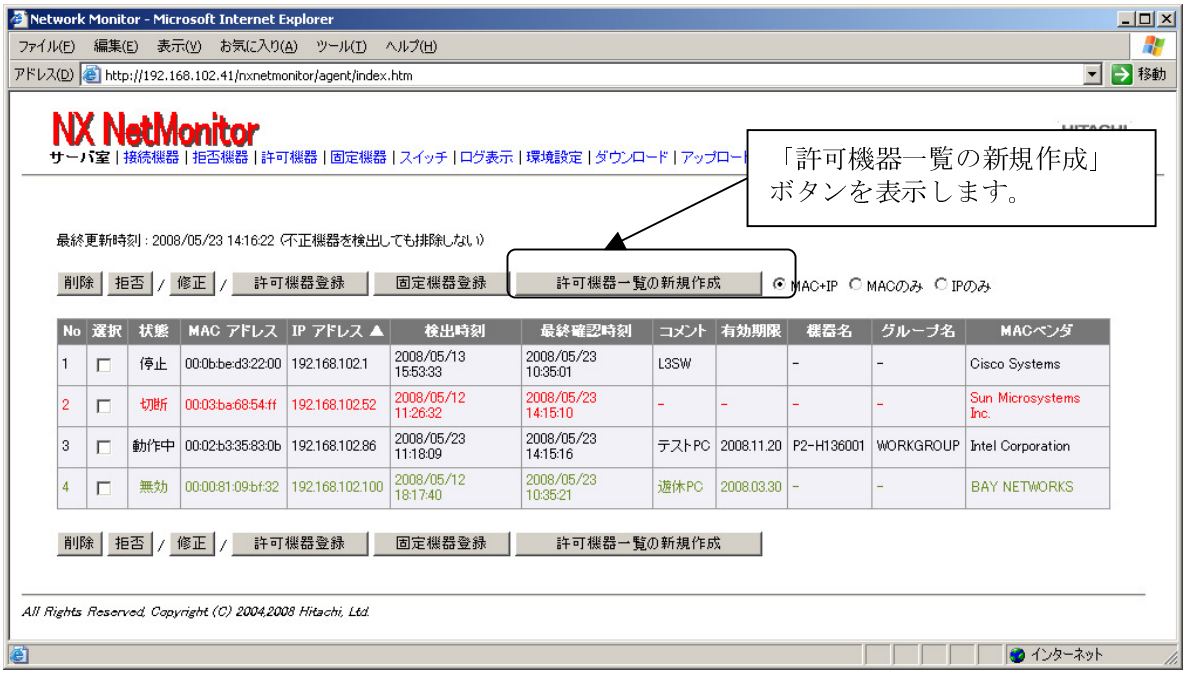


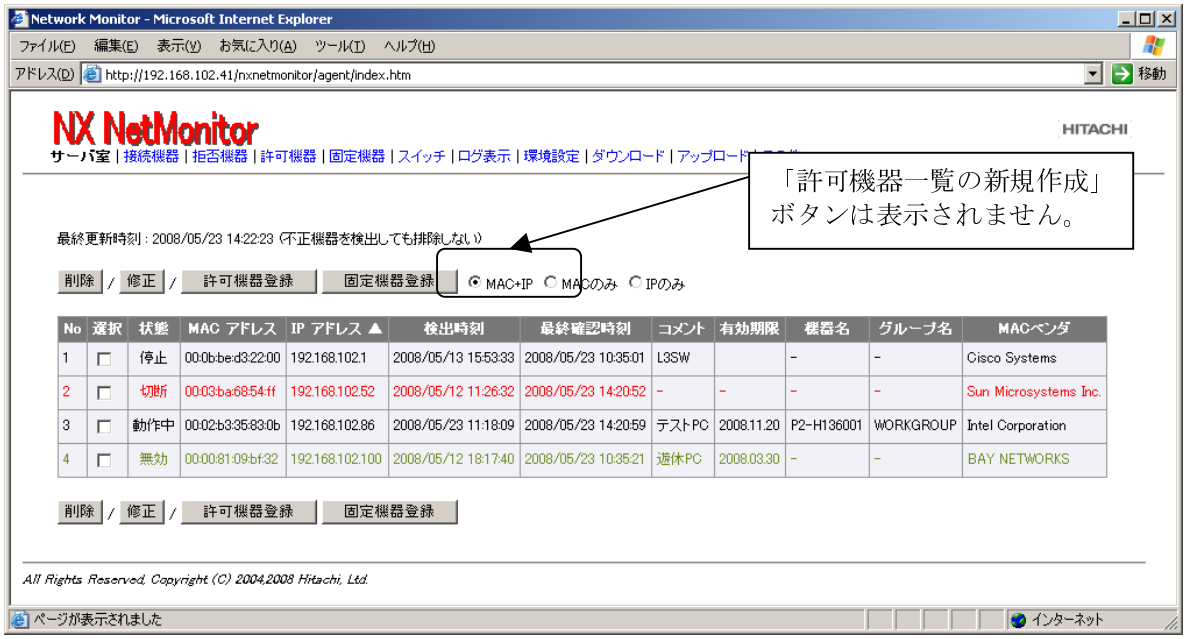


3-2) 拒否ボタンの表示/非表示（許可機器一覧）



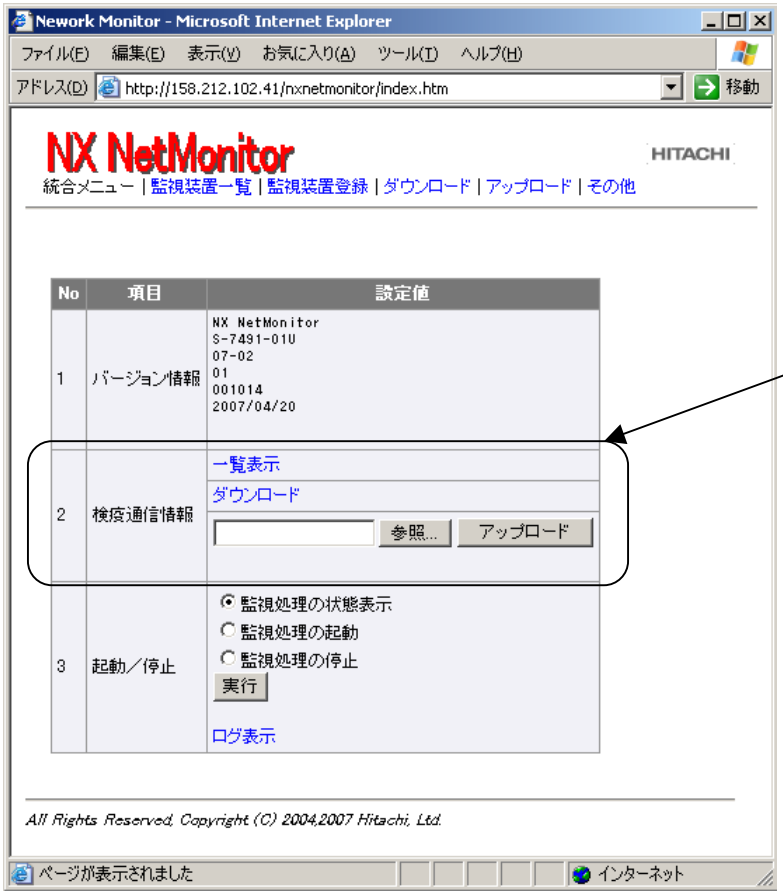
3-3) 接続機器一覧の新規作成ボタンの表示/非表示（接続機器一覧）





3-4) IP アドレスの自動割当ボタンの表示/非表示

3-5) 検疫通信情報メニューの表示/非表示(Linux 版のみ)



「検疫支援情報メニュー」を表示します。

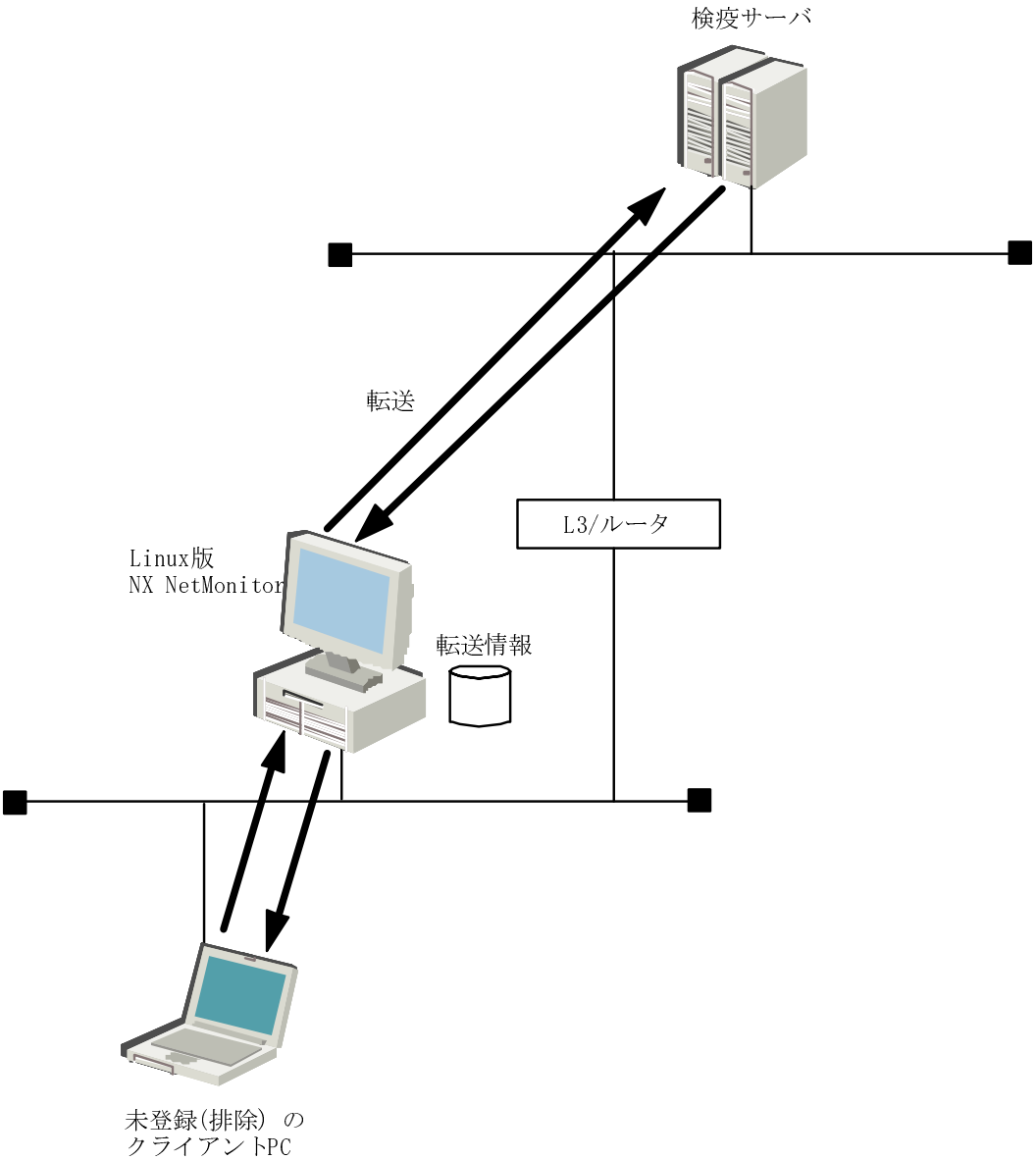
「検疫支援情報メニュー」は表示されません。

7. 特定機器との通信サポート

この章では、NX NetMonitor で排除された機器が、NX NetMontior に設定した特定の機器との通信を可能にするための機能について説明しています。

7.1 機能概要

本機能では、排除された機器でも、監視装置(NX NetMonitor)自身が中継することで、NX NetMonitor に設定した特定機器との通信を許可する機能をサポートします。
検疫モードが ON の時には、監視装置とだけ通信を許可していますが、本機能を使用することで、NX NetMonitor で排除された機器が、監視装置以外の機器とでも通信が可能になります。
この機能を使用すると、パッチなどが古くて検疫システムにより不適合 PC として排除されたクライアント PC でも、特定の機器と通信が可能となるため、検疫サーバからの治療（パッチのインストール）を行うことが可能となります。
この機能は、Linux 版の監視装置のみサポートします。
管理者は、通信を許可するサーバの IP アドレスやポート番号などを登録する必要があります。



7.2　設定方法

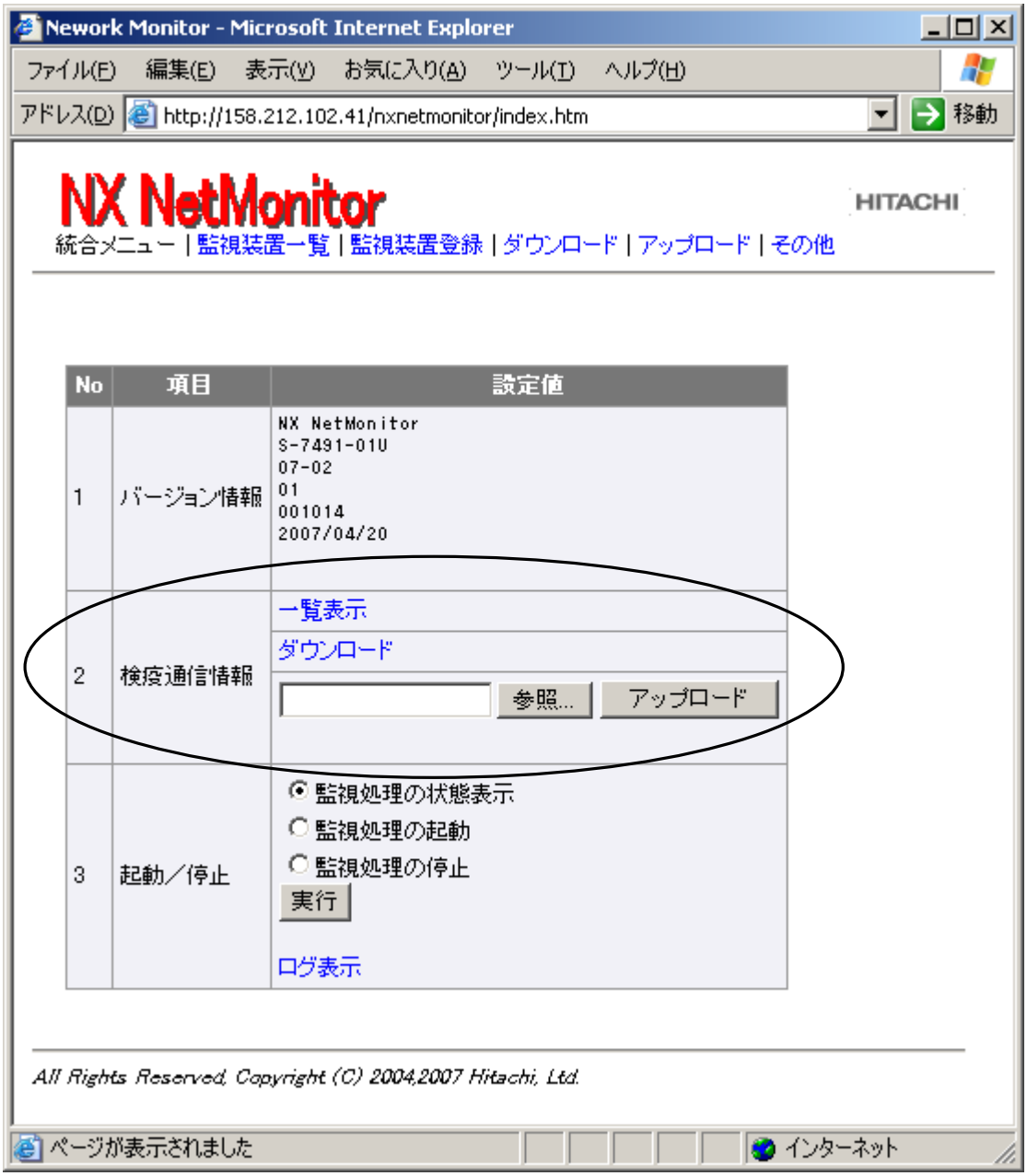
１）設定画面の表示

NX NetMonitor の統合メニュー画面の「その他」から、通信を許可する機器（サーバ）を設定します。統合メニューの「その他」は、監視装置一覧(index.htm)またはネットワーク一覧(index2.htm)の画面から開くことができます。

「監視装置一覧」

「ネットワーク一覧」

「検疫サーバ情報」
　検疫サーバ情報は、NX NetMonitor により排除された機器が特定の機器と通信を行うための設定を行うためのものです。検疫サーバ情報は Windows 版では表示されません。



検疫サーバ情報は「一覧表示」からブラウザの Web 画面から設定する方法と、CSV 形式のファイルをアップロードする方法の 2 つがあります。
また、設定されている内容は、CSV 形式でダウンロードすることも可能です。

２）設定項目と内容

検疫サーバ情報の設定では、一覧表示画面により通信を許可するサーバ（機器）の情報を設定します。設定項目は以下のものになります。検疫サーバ情報の設定は環境設定の「排除モード」が「不正機器を検出したら排除する」でかつ、「検疫支援情報」の「検疫支援モード」が ON の時に有効になります。

＜設定項目と内容＞

No	項目	内容
1	サーバアドレス	通信を許可するサーバの IP アドレスを指定します。 省略時は通信を拒否する設定となります。
2	クライアントアドレス	クライアントの IP アドレス、またはネットワークアドレスを指定します。ネットワークアドレスは、CIDR 形式で指定します。例えば、ネットマスクが、255.255.255.0 の場合、“192.168.1.0/24 “と指定します。省略時は、すべてのクライアントが許可されます。
3	プロトコル	通信を許可するプロトコルを指定します。tcp、udp、icmp が指定可能です。省略時は、すべてのプロトコルが対象になります。
4	サーバポート番号	通信を許可するサーバ側のポート番号を 0～65535 の範囲で指定します。プロトコルが、tcp、udp　の場合のみ指定可能です。 省略時は、すべてのポート番号が対象になります。 　なお、ポート番号が 0 というのは、ワイルドカード(すべてのポート番号が対象)ではありません。すべてのポート番号を対象としたい場合には、ポート番号を省略（空欄）してください。
5	クライアントポート番号	通信を許可するクライアント側のポート番号を 0～65535 の範囲で指定します。プロトコルが、tcp、udp　の場合のみ指定可能です。 省略時は、すべてのポート番号が対象になります。 　なお、ポート番号が 0 というのは、ワイルドカード(すべてのポート番号が対象)ではありません。すべてのポート番号を対象としたい場合には、ポート番号を省略（空欄）してください。
6	コメント	任意の３２バイトまでの文字列を指定することが出来ます。

＜CSV 形式での指定方法＞

フォーマット(CSV 形式)

サーバアドレス, クライアントアドレス, プロトコル, サーバ側ポート番号, クライアント側ポート番号, コメント

指定内容については、＜設定項目と内容＞を参照してください。

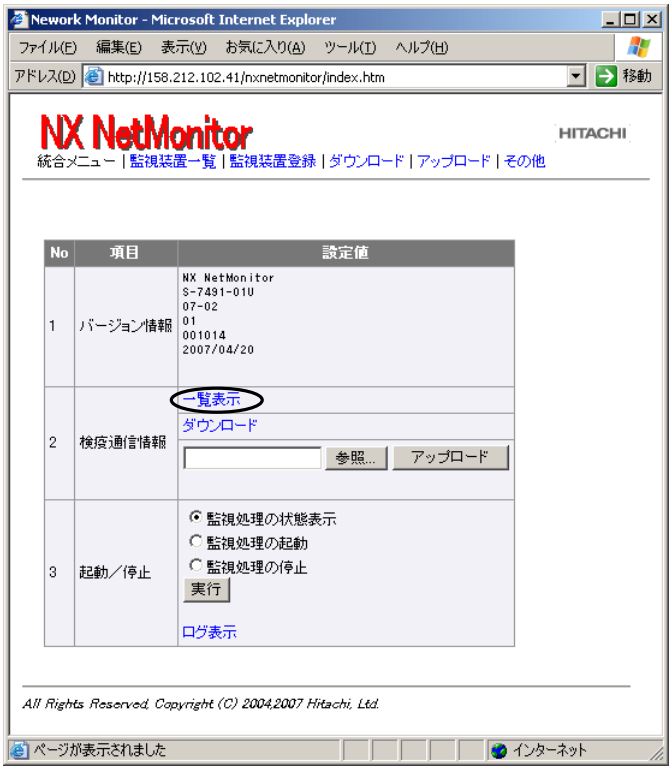
＜設定例＞

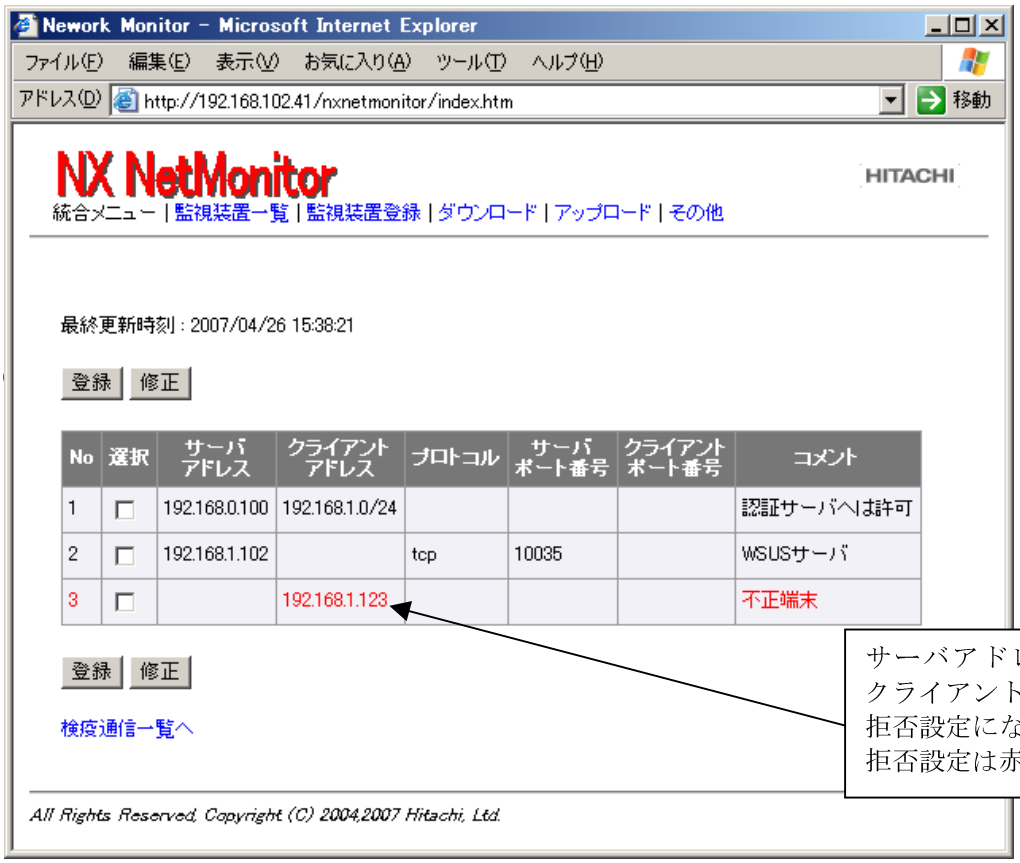
No	#サーバ アドレス	クライアント アドレス	プロトコル	サーバ側ポート	クライアント側ポート	コメント
1		192.168.1.0/24	udp			特定ネットワークの UDP 通信拒否
2		192.168.1.123				特定 IP の通信を拒否
3	192.168.0.100					サーバとの通信を許可
4	192.168.0.100	192.168.1.123				サーバと特定 IP との通信許可
5	192.168.0.100	192.168.1.0/24				サーバと特定ネットワークの通信許可
6	192.168.0.100		icmp			サーバとの ICMP 通信を許可
7	192.168.0.100		tcp			サーバとの TCP 通信を許可
8	192.168.0.100		tcp	80		サーバへの http 通信(ポート 80)を許可
9	192.168.0.100		tcp		137	サーバからの NetBIOS 通信(ポート 137)許可

(注) 通信の内容が複数の定義に合致する場合は，最も上に設定されている定義が有効になります。

3）Web 画面からの設定方法

「その他」メニュー、No2「検疫サーバ情報」項目の「一覧表示」から検疫サーバの定義情報を開きます。そこで、「登録」ボタンをクリックする、または、選択項目のチェックボックスにチェックを入れて「修正」ボタンをクリックすることにより、検疫サーバ情報を編集することができます。





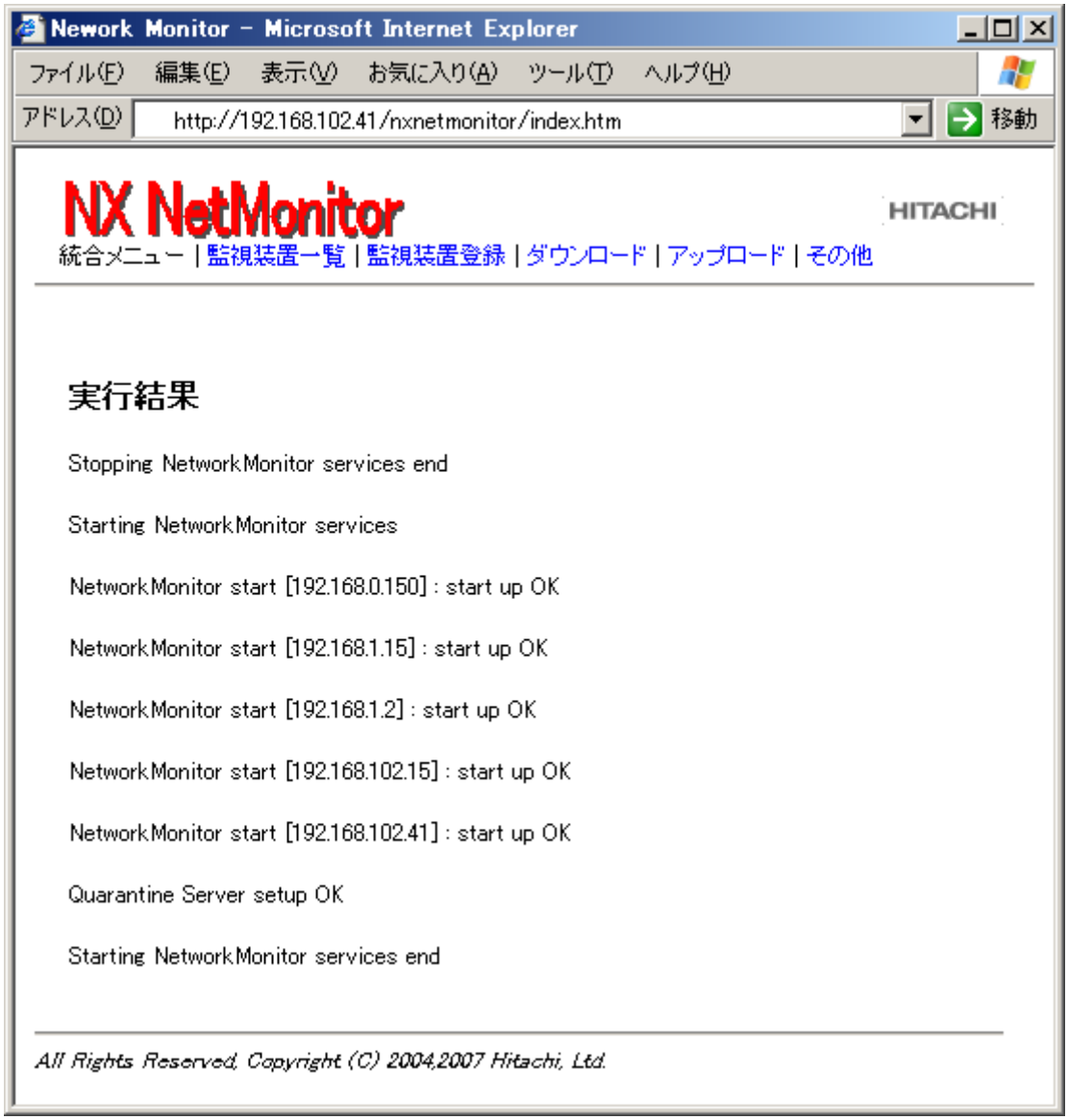
サーバアドレス未指定時はクライアントアドレス PC の拒否設定になります。
拒否設定は赤で表示します。

「登録」ボタンをクリックすると以下の検疫通信定義画面が開きます。
必要な情報を入力して、「実行」ボタンをクリックしてください。

設定内容が登録されると以下の実行結果のメッセージを出力します。以下の画面に表示されている「監視処理の再起動」ボタンを押すと、監視処理が再起動され、検疫通信定義が設定されます。「監視処理の再起動」ボタンを押さない場合には、「その他」メニューの「起動/停止」から別途「監視処理の再起動」を実施してください。監視処理の再起動後に、設定した情報が有効になります。

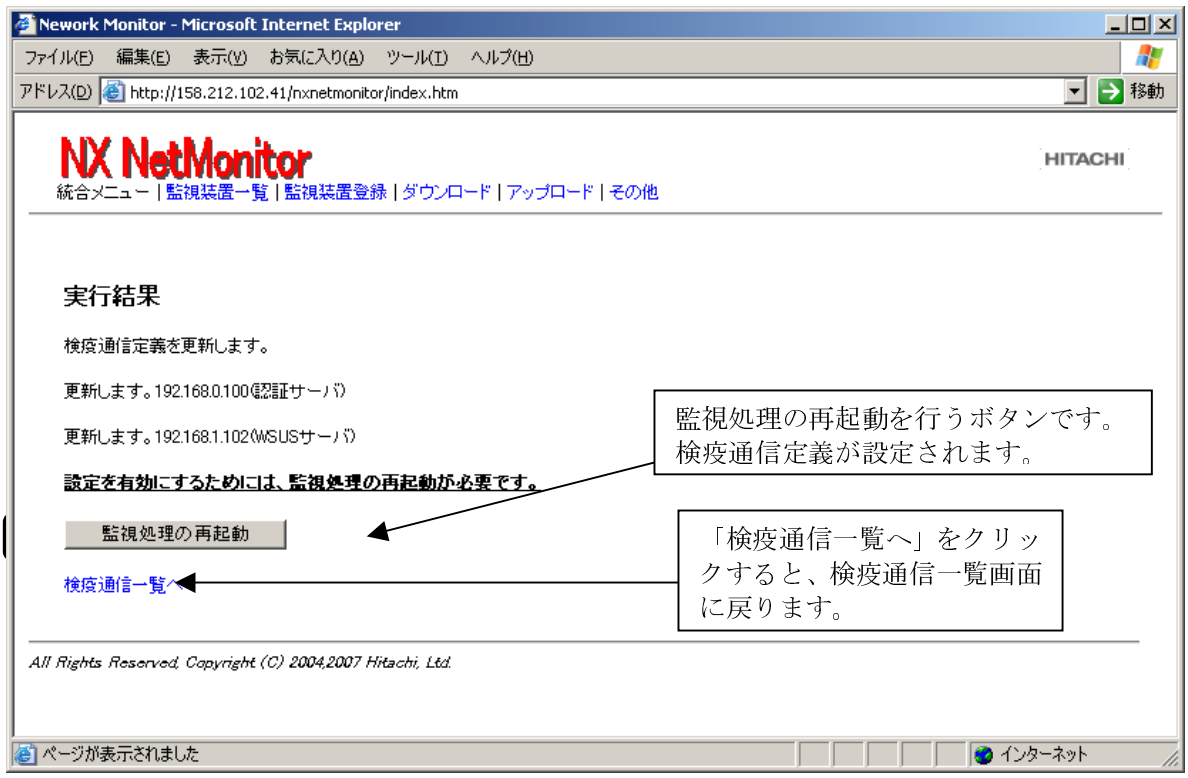
「監視処理の再起動」ボタンを押すと「監視処理を再起動してもよろしいですか」のメッセージが出力されますので、「OK」ボタンを押してください。「キャンセル」ボタンを押した場合は「その他」画面の「起動/停止」メニューから「監視処理の再起動」を別途行ってください。

監視処理の再起動「実行結果」が表示されます。



検疫通信一覧画面から、修正したい項目をチェックして、「修正」ボタンをクリックすると以下の修正画面が開きます。設定の「変更」または「削除」をチェックし、必要な情報を入力し、「実行」ボタンをクリックしてください。

設定内容が登録されると以下の実行結果のメッセージを出力します。修正した場合も、検疫通信定義時と同様に、監視処理の再起動後に、検疫通信定義が設定されます。



4）CSV ファイルへのダウンロード

検疫サーバ通信定義は、CSV 形式のファイルでダウンロードすることも可能です。
CSV ファイルでの登録フォーマットは２）設定項目と内容を参照してください。
「ダウンロード」ボタンを選択し、右クリックしてメニューから「対象をファイルに保存」を実行してください。quarantine_XXXXXXXX.csv の名称でファイルをダウンロードします。
XXXXXXXX はダウンロードした年月日時分になります。

5）CSV ファイルからのアップロード

検疫サーバ通信定義は、CSV 形式のファイルに記述してアップロードすることも可能です。CSV ファイルでの登録フォーマットは２）設定項目と内容を参照してください。

「アップロード」ボタンをクリックすると、「アップロードしてよろしいですか」のメッセージを表示しますので、「OK」ボタンを押してください。

アップロードが行われると実行結果画面が表示され、アップロードしたファイル名が表示されます。「その他」メニューの「起動/停止」から「監視処理の再起動」を実施してください。監視処理の再起動後に、設定した情報が有効になります。

6）監視処理の再起動

検疫サーバ情報に設定した内容を有効にするためには、監視処理の再起動を行ってください。
「監視処理の起動」をチェックして、「実行」ボタンを押します。

監視処理の起動をチェックして、「実行」ボタンをクリックすると、監視処理が再起動されます。

8. メッセージ

この章では、不正持込み PC 監視＆強制排除システムの監視処理で出力されるログやトラップ、監視画面で出力されるメッセージについて説明しています。

8.1 ログ・トラップ一覧

不正機器接続の検知・排除や、手動による接続拒否・許可などのログメッセージを以下に示します。
以下のメッセージは集中監視サーバ(NX NetMonitor/Dtector)が出力するものも含まれています。従って NX NetMonitor で以下全てのメッセージを出力するわけではありません。
ログ/トラップ一覧でレベル、トラップ識別番号の（ ）内の情報は JP1 イベントでの重大度、イベント ID を示します。

＜ログ/トラップ一覧（1/3）＞

No	レベル (重大度)	トラップ 識別番号 (イベント ID)	メッセージ	内容
1	警告 (Alert)	1001 (00005D00)	MAC(00:11:22:33:44:55), IP(192.168.0.10) is detected [not permitted].(*6)	不許可機器を検出しました。(*9)
2	警告 (Warning)	1002 (00005D01)	MAC(00:11:22:33:44:55), IP(192.168.0.10) is detected [not used].(*6)	許容停止期間を過ぎた機器を検出しました。
3	警告 (Warning)	1003 (00005D02)	The number of PC connected to the network will exceed the maximum number.	現在接続 PC 台数が、最大接続 PC 台数の９０％に達しました。(最大数を超えそうです)
4	警告 (Warning)	1004 (00005D03)	The number of PC connected to the network exceeded the maximum number.	最大接続 PC 台数を超えました。
5	警告 (Warning)	1005 (00005D04)	MAC(00:11:22:33:44:55), IP(192.168.0.10) is detected [term passed].(*6)	接続許可の有効期限が過ぎた機器を検出しました。
6	警告 (Warning)	1006 (00005D05)	MAC(00:11:22:33:44:55), IP(192.168.0.1) is connected YY[MAC(AA:BB:CC:DD:EE:FF), IP(192.168.0.2), PORT(1)].(*2)	不正機器の接続されているスイッチ(リピータ)のアドレス、ポートを検出しました。
7	警告 (Warning)	1007 (00005D06)	MAC(00:11:22:33:44:55), IP(192.168.0.1) is IP duplicated(MAC(55:44:33:22:11:00)).	IP アドレスが重複しました。
8	警告 (Warning)	1008 (00005D07)	Permission list is not effective.	許可機器一覧と固定機器一覧の件数が 0 件のため、排除機能を無効にしました。 (*5)
9	警告 (Warning)	1009 (00005D08)	MAC(00:11:22:33:44:55), IP(192.168.0.1) is [PCNAME, GRPNAME].	不正機器のコンピュータ名を検出しました。(*8)
10	警告 (Warning)	1010 (00005D09)	MAC(00:11:22:33:44:55), IP(192.168.0.1) is changed AFTER_NAME from BEFOR_NAME	コンピュータ名称が変更されたことを検出しました。

＜ログ/トラップ一覧（2/3）＞

No	レベル（重大度）	トラップ識別番号（イベントID）	メッセージ	内容
11	警告（Alert）	1011（00005D0A）	MAC(00:11:22:33:44:55), IP(192.168.0.1)is detected [not permitted]. (by detecotor)	不許可機器を検出しました（集中監視による検出）(*9)
12	警告（Warning）	1012（00005D0B）	MAC(00:11:22:33:44:55), IP(192.168.0.1) is detected [not used]. (by detecotor)	許容停止期間を過ぎた機器を検出しました。(集中監視による検出)
13	警告（Warning）	1013（00005D0C）	MAC(00:11:22:33:44:55), IP(192.168.0.1) is detected [term passed]. (by detecotor)	接続許可の有効期限が過ぎた機器を検出しました。(集中監視による検出)
14	警告（Warning）	1997（00005D0D）	Monitor is up.　(*7)	監視処理が起動しました。
15	警告（Warning）	1998（00005D0E）	Monitor is stop. (*7)	監視処理が停止しました。
16	警告（Warning）	1999（00005D0F）	Monitor is down. (*7)	監視装置が停止しました。(監視装置と統合管理装置の通信不可)
17	操作(Information)	2001（00005D55）	MAC(00:11:22:33:44:55), IP(192.168.0.10) is permitted manually from XXX.(*1)	手動による許可を行いました。
18	操作(Information)	2002（00005D56）	MAC(00:11:22:33:44:55), IP(192.168.0.10) is isolated manually from XXX.(*1)	手動による拒否を行いました。
19	操作(Information)	2003（00005D57）	Updated permission list from XXX.(count=CCC) (*1)(*4)	許可機器一覧の更新を行いました。(許可機器/固定機器の総数)
20	操作(Information)	2004（00005D58）	Updated configuration(mode=ON or OFF) from XXX.(*1)	環境設定の更新(排除モード)を行いました。
21	操作(Information)	2005（00005D59）	MAC(00:11:22:33:44:55), IP(192.168.0.1) is permitted by VVVV(*3) from XXX.(*1)	パートナー連携機能による許可を行いました。
22	操作(Information)	2006（00005D5A）	MAC(00:11:22:33:44:55), IP(192.168.0.1) is isolated by VVVV(*3) from XXX.(*1)	パートナー連携機能による拒否を行いました。
23	操作(Information)	2007（00005D5B）	Updated blocked list from XXX. (count=CCC) (*1)(*4)	排除機器一覧の更新を行いました。
24	操作(Information)	2008（00005D5C）	Updated switch list from XXX.(*1)	スイッチ一覧の更新を行いました。
25	情報(Information)	3001（00005DAA）	Start NetworkMonitor(mode=ON or OFF).	監視の開始(排除モード)を行いました。

＜ログ/トラップ一覧（3/3）＞

No	レベル (重大度)	トラップ 識別番号 (イベント ID)	メッセージ	内容
26	情報(Information)	3002 (00005DAB)	MAC(00:11:22:33:44:55), IP(192.168.0.10) is up.	機器が起動しました。
27	情報(Information)	3003 (00005DAC)	MAC(00:11:22:33:44:55), IP(192.168.0.10) is down.	機器が停止しました。
28	情報(Information)	3004 (00005DAD)	MAC(00:11:22:33:44:55), IP(192.168.0.10) is permitted.	許可機器一覧に追加されました。
29	情報(Information)	3005 (00005DAE)	MAC(00:11:22:33:44:55), IP(192.168.0.10) is deleted manually from XXX.(*1)	機器が接続機器一覧から削除されました。
30	情報(Information)	3006 (00005DAF)	MAC(00:11:22:33:44:55), IP(192.168.0.1) cannot detect connection position.	不正機器の接続されているスイッチ(リピータ)のアドレス、ポートが検出できませんでした。
31	情報(Information)	3007 (00005DB0)	MAC(00:11:22:33:44:55), IP(192.168.0.1) is permitted automatically [fixed].	固定機器のため、起動時に強制排除を行いませんでした。
32	情報(Information)	3008 (00005DB1)	MAC(00:11:22:33:44:55), IP(192.168.0.1) is deleted automatically.(xxx days)	接続一覧から自動削除されました。
33	情報(Information)	3009 (00005DB2)	Deleted connected list from XXX.(*1)	接続一覧の情報を全て削除しました。

(*1) XXX:操作した PC の IP アドレス。

(*2) YY :スイッチの場合は "SW"、リピータの場合は "RP" 。

(*3) VVVV ： 要求元のベンダ略称（ベンダ ID、ソフト ID は、非公開情報のため直接出力しません)

(*4) CCC:登録した許可機器、固定機器、排除機器の件数。

(*5) 許可機器/固定機器一覧の合計が 0 件の場合、定期的(2 分程度)に、本ログが出力されます。
許可機器/固定機器一覧を登録してください。

(*6) 環境設定で、排除モードが「不正機器を検出しても排除しない」、かつ「検出のみ行う」を指定した場合、排除モードで「不正機器を検出したら排除する」 の場合と区別するため "(mode=OFF)"と出力します。
(例) MAC(00:11:22:33:44:55), IP(192.168.0.1)is detected [not permitted]. (mode=OFF)

(*7) No14, 15, 16 は、監視装置側で出力されるログではありません。
統合管理装置側(NX NetMonitor/Manager)で監視を行い、出力します。

(*8) 不正機器のコンピュータ名検出のログは、SNMP トラップ、独自トラップのいずれか、または両方を定義したときに出力されます。

(*9)トラップ識別番号 1001,1011 のログは JP1 イベント時には、Alert のレベルになります。

＜SNMP トラップメッセージについて＞

SNMP トラップにて通知されるメッセージの内容は、先頭に

"Network Monitor(監視対象ネットワークのネットワークアドレス) : "

が付加されます。

例) Network Monitor(192.168.0.10) : MAC(00:80:c8:84:51:66), IP(192.168.0.123) is up.

<SNMP トラップ定義ファイルについて＞

NX NetMonitor および NX NetMonitor – Detector では検出したイベント情報を JP1/Cm2/NNM などの SNMP マネージャにトラップ送信することが出来ます。SNMP マネージャがトラップ受信時にイベント内容を表示するために必要なトラップ定義ファイル「nxnmtrapd.conf」を NX NetMonitor/Manager をインストールしたディレクトリ下にに格納しています。必要に応じて SNMP マネージャにロードしてください。

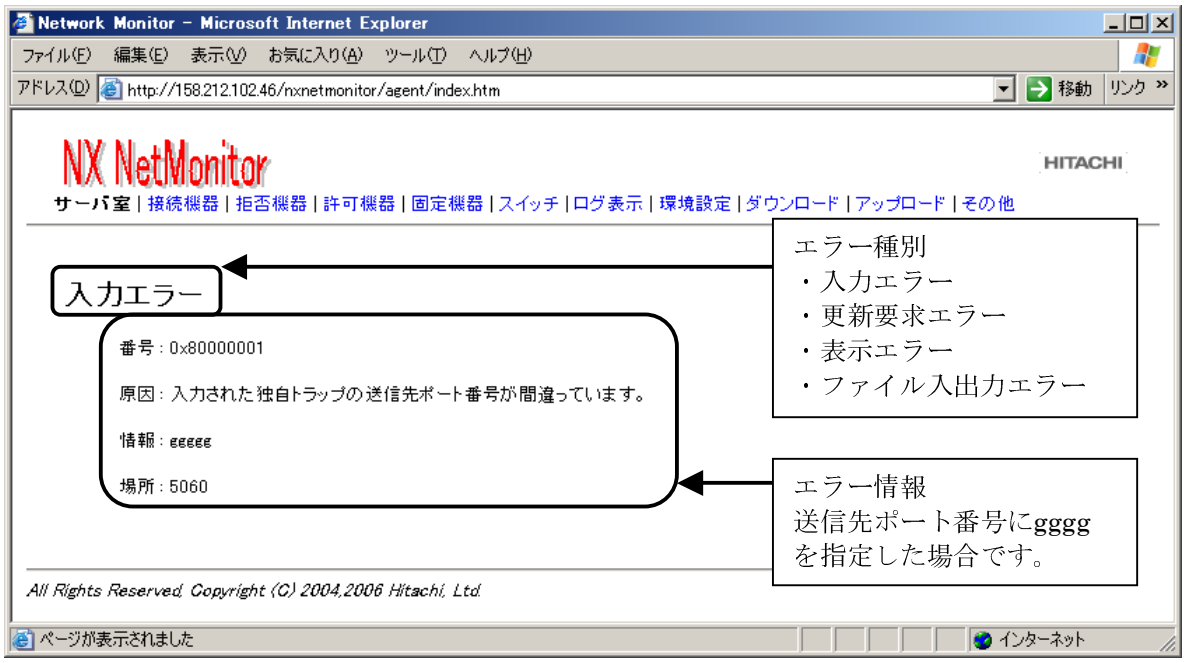
「nxnmtrapd.conf」ファイル格納場所

C:¥nx¥netmonitor¥sample

「nxnmtrapd.conf」は、NX NetMonitor および NX NetMonitor – Detector で共通です。

8.2　監視画面のエラーメッセージ一覧

画面操作にてエラーが発生すると下記のように、エラー内容が表示されます。



以下に、表示されるエラー番号の一覧を示します。

＜表示エラー番号一覧＞

No	エラー番号	エラー種別	対処法
1	0x80000001	入力エラー	入力値を見直してください。
2	0x80000002	アップロードエラー	アップロードするファイルを見直してください。
3	0x80000003	操作エラー	操作できません。
4	0x80000004	タイムアウト	しばらく経ってから再試行してください。
5	0x80000005	ロックエラー	しばらく経ってから再試行してください。
6	0x80000006	メモリエラー	メモリの使用状況を確認してください。
7	0x80000007	システムコールエラー (*1)	出力されたエラーメッセージを記録すると共に、「８．１障害時の対応」の手順でログを収集し、製造元に連絡してください。
8	0x80000008	フォーマットエラー	
9	0x80000009	FORM エラー/表示エラー	

(*1) エラー種別が、「更新要求エラー」で、システムコールエラーが発生した場合、監視処理が起動されていない可能性があります。
「６．１１　その他」の監視処理の状態表示にて、起動されているかを確認してください。

以下のメッセージは NX NetMonitor で全てを出力するわけではありません。
集中監視サーバ(NX NetMonitor/Detector)が出力するものも含まれています。
＜エラーメッセージ一覧　（１／３）＞

No	内容	メッセージ（原因）
1	入力エラー	IP アドレスが入力されていません。
2		コメント(説明)は 32 バイト以内です。
3		カンマがありません。（フォーマット異常）
4		IP アドレスの指定が間違っています。
5		MAC アドレスの指定が間違っています。
6		IP アドレス 1 の指定が間違っています。
7		IP アドレス 2 の指定が間違っています。
8		停止期間監視対象の指定が間違っています。
9		有効期限の指定が間違っています。
10		最大数を超えて許可機器/固定機器を登録しました。
11		１００個以上のエラーが発生しました。以降のエラーは表示されません。
12		入力された排除モードが間違っています。
13		入力された最大接続機器台数が間違っています。
14		入力された SNMP トラップ送信先 IP アドレスが間違っています。
15		入力されたコミュニティ名が間違っています。
16		入力されたトラップレベルが間違っています。
17		入力された監視間隔が間違っています。
18		入力された監視開始 IP アドレスが間違っています。
19		入力された監視終了 IP アドレスが間違っています。
20		入力された許容停止期間が間違っています。
21		入力されたトラップバージョンが間違っています。
22		入力された監視対象外 IP アドレスの対処法が間違っています。
23		入力された検疫支援モードが間違っています。
24		入力された検疫の通知先 IP アドレスが間違っています。
25		入力された検疫の通知先ポート番号が間違っています。
26		入力された監視状態見直し時の対処が間違っています。
27		入力された有効期限切れ機器の許可が間違っています。
28		入力された許可機器起動時の対処が間違っています。
29		入力された動作モードが間違っています。
30		入力された検出モードが間違っています。
31		入力された独自トラップ送信先 IP アドレスが間違っています。
32		入力された独自トラップ送信先ポート番号が間違っています。
33		MAC アドレス、IP アドレスの指定がありません。
34		コメントの指定がありません。
35		すでに登録されています。

＜エラーメッセージ一覧　（２／３）＞

No	内容	メッセージ（原因）
36	入力エラー	「変更」または「削除」を選択してください。
37		MAC アドレスが重複指定されています。
38		IP アドレスが重複指定されています。
39		MAC/IP アドレスが重複指定されています。
40		入力された監視モードが間違っています。
41		入力された許可機器登録時の対処が間違っています。
42		入力されたコンピュータ名(NetBIOS 情報)収集が間違っています。
43		入力された MAC アドレスのベンダ指定が間違っています。
44		入力された排除レベルが間違っています。
45		入力された最大ログ件数が間違っています。
46		入力された IP アドレス重複検出が間違っています。
47		入力された監視対象外機器の排除が間違っています。
48		入力された許可リスト管理単位が間違っています。
49		入力された IP 重複時の除外 IP アドレスが間違っています。
50		入力されたコンピュータ名変更検出が間違っています。
51		入力された SNMP エージェント IP アドレスが間違っています。
52		入力された NetBIOS 情報収集間隔が間違っています。
53		入力された ICMP 送信が間違っています。
54		入力された ICMP 送信間隔が間違っています。
55		入力された ARP 情報収集が間違っています。
56		入力された ARP 情報収集周期が間違っています。
57		入力された不正機器位置特定が間違っています。
58		入力されたスイッチ種別が間違っています。
59		ネットワーク名が入力されていません。
60		ネットワーク名は 32 バイト以内です。
61		グループ名が入力されていません。
62		グループ名は 32 バイト以内です。
63		ネットマスクが入力されていません。
64		入力されたネットマスクが間違っています。
65		すでに、該当ネットワークが定義されています。
66		該当ネットワークの監視処理は起動されていません。「変更のみ」を選択してください。

＜エラーメッセージ一覧　（３／３）＞

No	内容	メッセージ（原因）
67	入力エラー	サーバアドレス、クライアントアドレスの指定がありません。
68		サーバアドレスの指定が間違っています。
69		クライアントアドレスの指定が間違っています。
70		ネットマスクの指定が間違っています。
71		プロトコルの指定が間違っています。
72		サーバポート番号の指定が間違っています。
73		クライアントポート番号の指定が間違っています。
74		ポート番号は指定できません。
75		入力された検疫実行方法が間違っています。
76		入力された接続機器の保持期間が間違っています。
77	アップロードエラー	ファイルサイズが０またはファイルが存在しないためアップロードできません。
78		拡張子が異なるため、アップロードが拒否されました。
79		ファイル名が指定されていません。
80		ファイル名が一致しません。
81		空白行がありません。
82	操作エラー	指定された機器は接続されていません。
83		指定された機器は監視対象外のネットワークのため操作できません
84		排除モードが OFF のため操作できません。
85		現在接続している機器がないため操作できません。
86		有効期限切れのため許可できません。
87		権限がありません。
88	タイムアウト	要求がタイムアウトしました。再試行してください。
89	ロックエラー	他のユーザが操作中です。しばらくして再試行してください。
90	メモリエラー	メモリが確保できません。
91	システムコールエラー	(システムコールのエラーメッセージが表示されます)
92	フォーマットエラー	アドレステーブルのサイズが異常です。
93		ログファイルのフォーマットが異常です。
94		要求メッセージが異常です。
95	FORM エラー	環境変数(REQUEST_METHOD)がありません。
96		環境変数(QUERY_STRING)がありません。
97		環境変数(CONTENT_LENGTH)が不正です。
98		ページ種別がありません。
99		ページ区分がありません。
100		ページ種別が不正です。
101		ページ区分が不正です。
102		入力フォームの内容が異常です。

9. 付録

9.1 障害時の対応

（1）ログの保存

＜Linux 版の場合＞

root でログインし、下記を実行して、ログ情報を保存します。

```
# cd /usr/etc/nxnetmonitor/log          ←ログディレクトリへ移動
# mkdir -p /tmp/bkup                      ←保存用ディレクトリ作成
# cp log* /tmp/bkup/                      ←保存
# ls /tmp/bkup -l                          ←確認
合計     1040
-rw-r--r--  1  root root 524304  9 月 2 15:08 log_c0a8001f
-rw-r--r--  1  root root 524304  9 月 2 15:08 log_mng
```

＜Windows 版の場合＞

Administrator でログインし、コマンドプロンプトから下記を実行して、ログ情報を保存します。

```
C:¥> cd C:¥nx¥netmonitor¥agent¥log                          ←ログディレクトリへ移動
C:¥nx¥netmonitor¥agent¥log> mkdir c:¥bkup                   ←保存用ディレクトリ作成
C:¥nx¥netmonitor¥agent¥log> copy log* c:¥bkup                  ←保存
C:¥nx¥netmonitor¥agent¥log> dir c:¥bkup                        ←確認

 F:¥nx¥netmonitor¥agent¥log¥bkup のディレクトリ
2005/02/28  10:37       <DIR>          .
2005/02/28  10:37       <DIR>          ..
2005/02/22  14:20               524,304 log_c0a800ae
2005/02/22  14:20               524,304 log_mng
               2 個のファイル             1,048,608 バイト
               2 個のディレクトリ    1,806,950,400 バイトの空き領域
```

（2）共有メモリの保存

Administrator でログインし、コマンドプロンプトから下記を実行して、共有メモリの情報を保存します。

```
C:¥> cd C:¥nx¥netmonitor¥agent¥bin                          ←bin ディレクトリへ移動
C:¥nx¥netmonitor¥agent¥bin>  mkdir c:¥bkup                  ←保存用ディレクトリ作成
C:¥nx¥netmonitor¥agent¥bin> nxnmagtdump > c:¥bkup¥shmdump.txt       ←保存
C:¥nx¥netmonitor¥agent¥bin> type c:¥bkup¥shmdump.txt          ←確認

[HEADER]
shmsize         = 8192(0x0002000)
init_time       = 2005/02/28 10:22:23
dmninfo_offset  = 0x60000020
network_cnt     = 1(0x00000001)
dmninfo_cnt     = 128(0x00000080)
port_mng        = 1065(0x00000429)

[DMNINFO]
  *** MONITOR IPADDRESS : 0xc0a800ae ***
        NXNMD      PTRL       TMR        DETC       INIT
  ------------------------------------------------------------
  PID  : 0x00000318 0x0000054c 0x000003c0 0x000004dc 0x000002f8
  PORT : 0x0000042b 0x0000042a 0x0000042c 0x0000042d 0x0000042e
```

9.2 使用するポート番号

NX NetMonitor は以下のポート番号を使用して、統合管理装置や SNMP マネージャと通信を行います。統合管理装置や SNMP マネージャとの通信経路にファイアウォールなどがある場合、以下のポート番号を通過するように設定してください。

＜使用ポート一覧＞

No	ポート番号	プロトコル	発信元	接続先	備考
1	80	TCP	統合管理装置 (NX NetMonitor)	監視装置 (NX NetMonitor)	許可機器一覧の配布、ログの収集など (http による通信)
2	162	UDP	監視装置 (NX NetMonitor)	SNMP マネージャ (JP1 の NNM など)	SNMP トラップ情報
3	ユーザ設定値 (*)	UDP	監視装置 (NX NetMonitor)	統合管理装置 (NX NetMonitor / Manager)	独自トラップ情報
4	137	UDP	監視装置 (NX NetMonitor)	監視対象端末	機器名の取り出し
5	161	UDP	監視装置 (NX NetMonitor)	監視対象ネットワーク内スイッチ等	MIB 情報の取り出し

(*) 設定値の内容は「６．１６ 環境設定」を参照してください。

9.3 MAC ベンダ表示の追加修正方法

NX NetMonitor の接続機器一覧、拒否機器一覧に機器の MAC ベンダ名を表示しています。MAC アドレスは、ネットワークカードに割当られる世界に一つしかない固有な番号です。最初の２４ビットがベンダ固有の番号になります。このベンダ固有の番号は IEEE が割当て、管理を行っています。

NX NetMonitor では、MAC アドレスのベンダ名と値を以下のファイルにデータベースとして保持しており、接続機器から検出した MAC アドレスと対応させてベンダ名を表示しています。接続機器一覧の MAC ベンダ表示が、”―“で表示されている場合、NX NetMonitor が保持しているデータベースの情報より、MAC ベンダが新しいことが考えられます。このような場合には、NX NetMonitor の MAC ベンダのデータベースを修正して対応ください。なお、下記の MAC アドレスのベンダ名のデータベースは、NX NetMonitor を再インストールすると、上書きされますので必要に応じてバックアップを行ってください。

NX NetMonitor の MAC ベンダデータベースは以下の場所にあります。

Linux 版 : /usr/etc/nxnetmonitor/conf/macvendor.txt

Windows 版 : [インストールディレクトリ]¥conf¥macvendor.txt

(インストールディレクトリのデフォルトは C:¥nx¥netmonitor¥agent です)

フォーマット

```
MAC ベンダアドレス　　ベンダ名称
```

MAC ベンダアドレスを先頭３バイト、後ろ３バイトは０を指定します。MAC ベンダアドレスと　ベンダ名称は「タブ」で区切ってください。

ベンダ名称は、対応するベンダ名称を英語で指定します。

例

```
00:00:87:00:00:00　　HITACHI, LTD.
```

なお、MAC ベンダを管理する IEEE　Standards Association のページは以下になります。このページで最新の MAC アドレスのベンダ名を検索することができます。

http://standards.ieee.org/regauth/oui/index.shtml

9.4 バックアップとリストア

ディスク障害などが発生してシステムが動作しなくなった場合，NX NetMonitor で使用する各種のデータが回復できなくなることがあります。このような不測の事態に備えて，定期的に各種のファイルをバックアップしておく必要があります。
バックアップが必要なファイルを次の表に示します。

バックアップが必要なファイル

種別	フォルダ名
定義情報	インストール先フォルダ¥conf

（凡例）
インストール先フォルダ：NX NetMonitor をインストールしたフォルダです。
NX NetMonitor のデフォルトのインストール先フォルダは，次のとおりです。
Windows の場合：
C:¥nx¥netmonitor¥agent
Linux の場合：
/usr/etc/nxnetmonitor
障害が発生した場合は，バックアップファイルを元の場所にリストアしてください。