InterSec/NQ30
V5.2

ユーザーズマニュアル

1版

日本電気株式会社

目次

1　はじめに

1.1　用語説明

本書中の説明で使用する略語は、以下の通りです。

略語	意味
NA	NetworkAgent を指します。文中にて左記の略語が指示された場合、NetworkAgent のみ該当します。
NQ30a	InterSec/NQ30a を指します。文中にて左記の略語が指示された場合、InterSec/NQ30a のみ該当します。
NQ30b	InterSec/NQ30b を指します。文中にて左記の略語が指示された場合、InterSec/NQ30b のみ該当します。
NQ30c	InterSec/NQ30c を指します。文中にて左記の略語が指示された場合、InterSec/NQ30c のみ該当します。
NQ30d	InterSec/NQ30d を指します。文中にて左記の略語が指示された場合、InterSec/NQ30d のみ該当します。
NQ	InterSec/NQ30a、InterSec/NQ30b、InterSec/NQ30c、InterSec/NQ30d を指します。文中にて左記の略語が指示された場合、InterSec/NQ30a、InterSec/NQ30b、InterSec/NQ30c、InterSec/NQ30d 共通となります。
SiteManager	InfoCage 不正接続防止 SiteManager を指します。
DomainManager	InfoCage 不正接続防止 DomainManager を指します。
Lite	InfoCage 不正接続防止 Lite を指します。
eth0	InterSec/NQ30a、InterSec/NQ30b、InterSec/NQ30c の LAN コネクタを指します。また、InterSec/NQ30d の LAN コネクタ 1 を指します。
eth1	InterSec/NQ30d の LAN コネクタ 2 を指します。

1.2　特記事項

パラメータの既定値変更および機能の変更により一部機能の挙動が変更となります。下記の変更内容を確認の上、設定の再確認をお願いします。

概要	バージョン	詳細
パラメータの既定値変更	3.9	JamMacAddressMode の既定値を『0』から『1』に変更しました。 V3.8 以前のバージョンからアップデートした場合に既定値を変更します。 本変更にともない、以下の挙動が変更となります。 ・不正接続防止時の偽装 ARP の MAC アドレスが

		88:88:88:88:88:88 から NQ の MAC アドレスへ変更となります。
パラメータの既定値変更	3.9	DisableBroadCastJamArp の既定値を『0』から『1』に変更しました。 V3.8 以前のバージョンからアップデートした場合に既定値を変更します。 本変更にともない、以下の挙動が変更となります。 ・不正接続防止時の偽装 ARP のパケット送信方法がブロードキャストからユニキャストへ変更となります。 DisableUniCastJamArp との併用はできません。 DisableUniCastJamArp の設定を確認してください。

1.3 関連マニュアル

NQ の導入にあたり、以下のマニュアル類を参照してください。

「InterSec/NQ30a スタートアップガイド」(NQ30a ユーザの場合)
「InterSec/NQ30b スタートアップガイド」(NQ30b ユーザの場合)
「InterSec/NQ30c スタートアップガイド」(NQ30c ユーザの場合)
「InterSec/NQ30d スタートアップガイド」(NQ30d ユーザの場合)
「InfoCage 不正接続防止 SiteManager インストールマニュアル」
「InfoCage 不正接続防止 DomainManager インストールマニュアル」
「InfoCage 不正接続防止集中管理機能運用マニュアル」
「InfoCage 不正接続防止注意制限事項」

※ バージョンアップを行った場合は、お手持ちのスタートアップガイドに記載されている設定手順と異なる場合がありますので、本書の各設定方法を確認してください。なお、バージョンアップ方法は、SiteManager オンラインヘルプの目次より、[InfoCage 不正接続防止]->[InfoCage 不正接続防止その他の機能]->[エージェントの自動バージョンアップ機能]を参照してください。

1.4　共有ネットワーク環境での使用方法

NQ は通常、設定されたネットワークアドレスと同一のセグメントを監視対象としますが、「共有ネットワーク対応機能」を設定することにより、NQ が設置された環境に設定されたネットワークアドレスと異なるセグメントからのパケットが流れる場合も、監視対象とすることが可能となります。設定については、7.5 章の「MultiNetwork」の項目を参照の上、USB メモリを使用した設定ファイルの反映や、telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続によるコマンド入力で行ってください。なお、「共有ネットワーク対応機能」を利用する場合、ネットワーク環境によって「InterSec/NQ30 1VLAN 追加ライセンス」の購入が必要となることがあります。以降の内容を確認し、必要に応じて追加ライセンスを購入してください。

［共有ネットワーク対応機能］

「共有ネットワーク対応機能」には以下の 2 つのモードがあります。

- 全体指定モード
  エージェントが所属する VLAN 上を流れる全てのホストについて、取得した全情報を表示します。設定方法は 7.5 章の「MultiNetwork」の項目を参照してください。
- 個別指定モード
  エージェントの所属する VLAN に設定されたサブネットのうち、監視対象ネットワークリストに設定されたサブネットに所属するホストについて、取得した全情報を表示します。設定方法は 7.5 章の「NetworkList」の項目を参照してください。InterSec/NQ30 利用時の注意事項
  - このモードを使用する場合は、属性値 MultiNetwork の値を 0 に設定し、サービスを再起動してください。
  - 管理対象ネットワークリストからエージェントと同一のネットワークを除外したい場合は、属性値 DisableWatchMyNetwork の値を 1 に設定し、サービスを再起動してください。

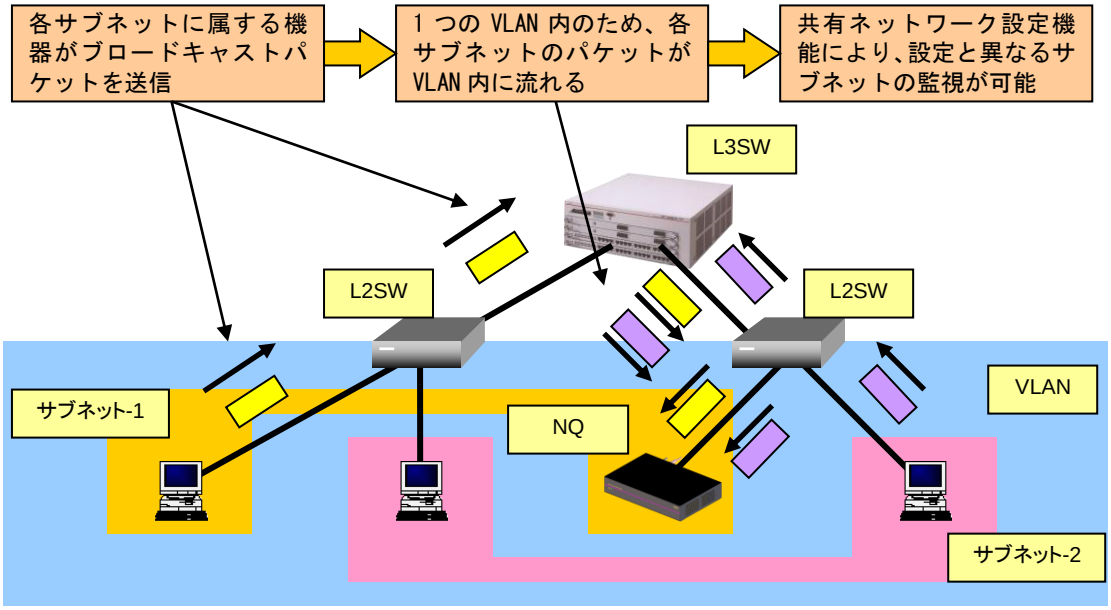
［本機能使用時の注意事項］

- 1 台の NQ で管理できるホスト台数は、2,000 件（NQ30c の場合は約 4,000 件、NQ30d の場合は約 8,000 件）（※）までとなります。
- InfoCage セキュリティリスク管理(CapsSuite) を利用している場合、[共有ネットワーク対応機能の全体指定モード]を利用することはできません。
- 分散管理モードでワーム感染ホストの接続防止機能を使用する場合、サイトコンソールのエージェント設定ダイアログに表示される監視対象ネットワークリストに属さないホストを防止することはできません。

（※）エージェントが一日に検出した MAC アドレス数（目安としてホスト一覧の最終検出日がその日になっているものの件数）

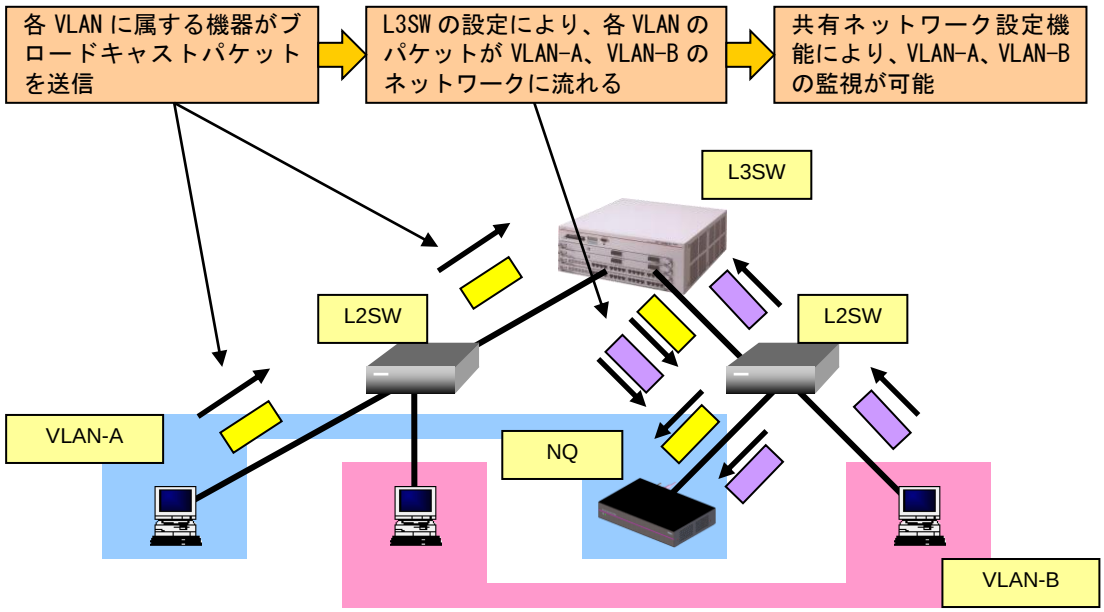
1.4.1　共有ネットワーク環境の場合

1 つの VLAN 内に複数のサブネットが存在する環境（共有ネットワーク環境）を監視する場合は、「InterSec/NQ30 1VLAN 追加ライセンス」は不要です。



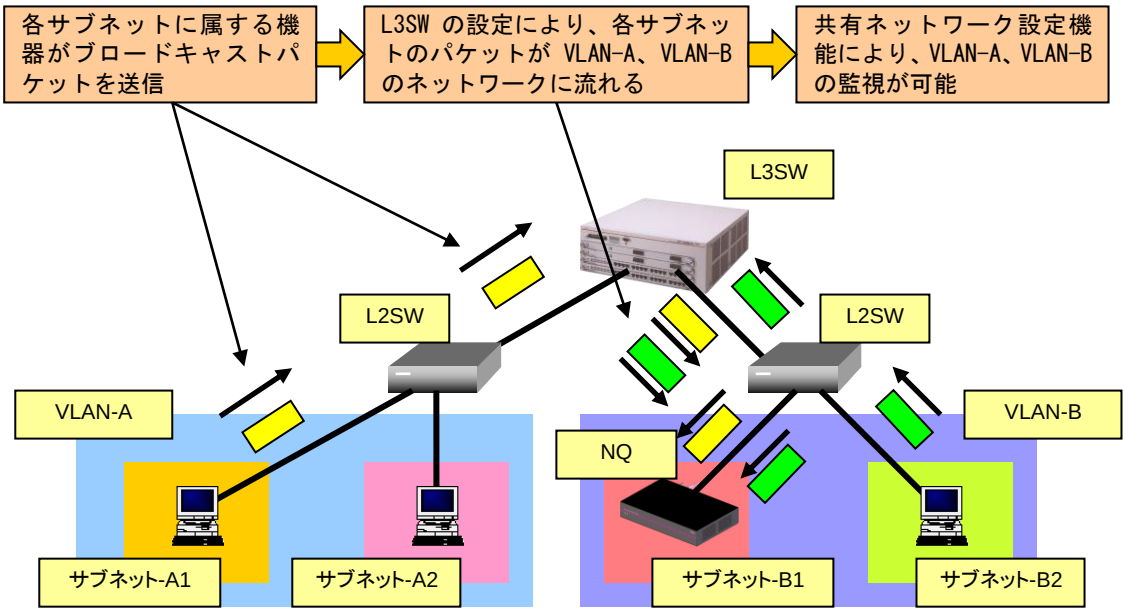
1.4.2　複数 VLAN 環境の場合

複数 VLAN の環境（非タグ VLAN 環境＝マルチ VLAN 環境）において、1 台の NetworkAgent（NQ）で複数の VLAN を監視する場合、“VLAN の数 － 1”の「InterSec/NQ30 1VLAN 追加ライセンス」が必要です。



1.4.3　共有ネットワーク＋複数 VLAN 環境の場合

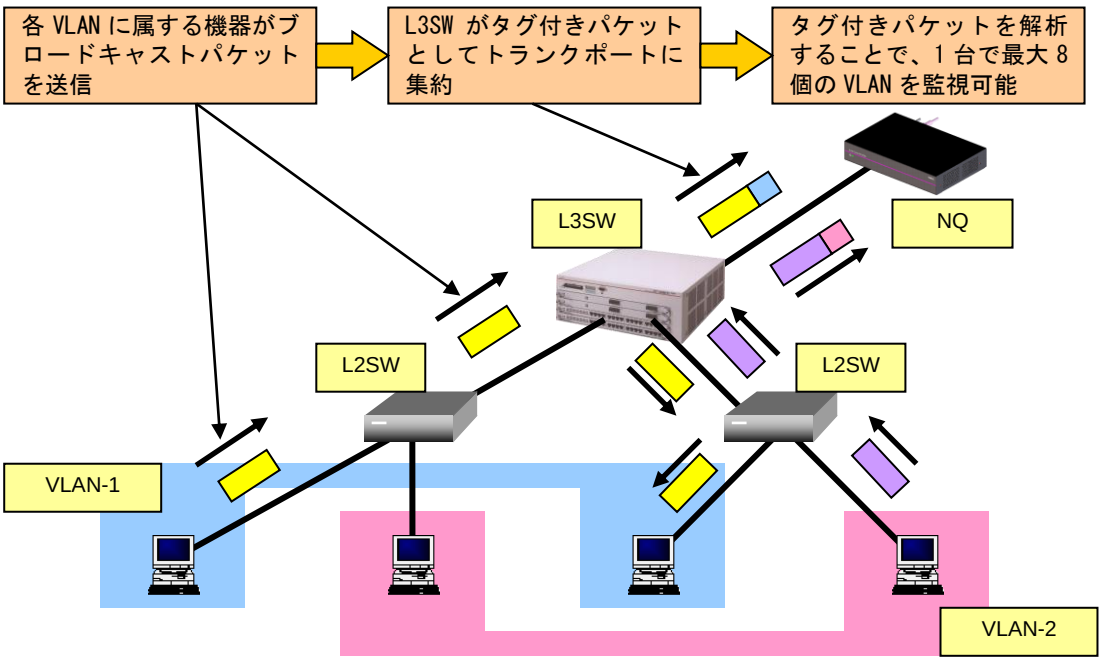
複数 VLAN（非タグ VLAN 環境＝マルチ VLAN 環境）で、各 VLAN 内に複数のサブネットが存在する環境を 1 台の NetworkAgent（NQ）で監視する場合、「1.4.2 複数 VLAN 環境の場合」と同様に、“VLAN の数 － 1”の「InterSec/NQ30 1VLAN 追加ライセンス」が必要です。



1.5　タグ VLAN（IEEE802.1Q）環境での使用方法

NQ は、タグ VLAN（IEEE802.1Q）環境（※1）での動作をサポートしています。L3 スイッチにタグ付きパケットの送受信を可能とするトランクポートを設定し、NQ をトランクポートに接続してデータ収集を行います。これにより、1 台の NQ で最大 8 個(NQ30c の場合、16 個、NQ30d の場合、32 個)の VLAN を監視できます。設定については、2.2.4 章のタグ VLAN 環境での設定パラメータ例、あるいは 2.3.2 章のタグ VLAN 環境設置時の実行例を参照の上、USB メモリを使用した設定ファイルの反映や、telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続によるコマンド入力で行ってください。

なお、タグ VLAN 環境において、1 台の NQ で複数の VLAN を監視する場合、“VLAN の数 － 1”の「InterSec/NQ30 1VLAN 追加ライセンス」が必要です。



［本機能使用時の注意事項］

- 1 台の NQ で管理できるホスト台数は、約 2,000 件（NQ30c の場合は約 4,000 件、NQ30d の場合は約 8,000 件）（※2）までとなります。
- 「共有ネットワーク対応機能」との併用は未サポートです。
- 分散管理モードでワーム感染ホストの接続防止機能を使用する場合、サイトコンソールのエージェント設定ダイアログに表示される監視対象ネットワークリストに属さないホストを防止することはできません。
- NQ への telnet もしくは SSH 接続(NQ30c、NQ30d のみ)は、VLAN インターフェースで設定している IP アドレスに対して接続を行ってください。
- デフォルトゲートウェイの設定は、VLAN インターフェースに属するゲートウェイを指定してください。

(※1) サポート対象のタグ VLAN（IEEE802.1Q）環境は、IP サブネット ベース VLAN、ポート ベース VLAN です。

(※2) エージェントが一日に検出した MAC アドレス数（目安としてホスト一覧の最終検出日がそ

の日になっているものの件数）

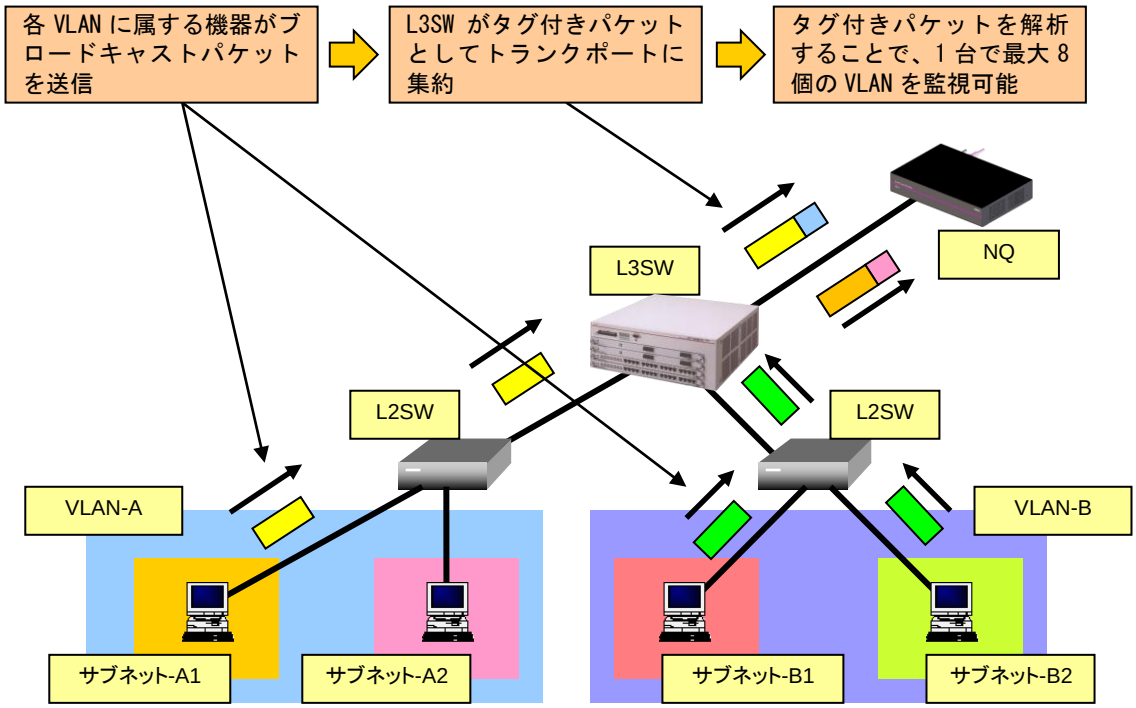
1.6　共有ネットワーク＋タグ VLAN（IEEE802.1Q）環境の場合

「共有ネットワーク対応機能」と「タグ VLAN 対応機能」の併用は以下を満たした場合のみサポートします。

- NQ で管理する全ての VLAN、サブネットの ARP リクエストパケットが NQ で検知できること
- NQ で管理する全ての VLAN、サブネットに NQ から ARP パケットが送信できること

評価機などを用いて実際にパケットのやり取りが可能なことを確認したうえで導入してください。

なお、「共有ネットワーク対応機能」と「タグ VLAN 対応機能」を併用し 1 台の NQ で複数のサブネットを持つ VLAN を複数監視する場合、“VLAN の数 － 1”の「InterSec/NQ30 1VLAN 追加ライセンス」が必要です。



1.7　InterSec/NQ30b、NQ30c、NQ30d の初期化方法について

V3.6 以降、NQ の設定内容を初期化することが可能です。NQ30c、NQ30d はバージョンに関係なく初期化可能です。初期化内容は、パスワードやネットワーク情報など一部の情報を初期化する方法と、V3.1g（NQ30b の場合）、V2.2（NQ30c、NQ30d の場合）にダウングレードする方法があります。なお、NQ30a、および V3.6 未満の NQ30b では本機能は未サポートです。

1.7.1　初期化内容

初期化される内容は以下の通りです。

・パスワードやネットワーク情報などを初期化する場合

初期化内容	パラメータ	初期値
パスワード	Password	admin
IP アドレス	IpAddress	192.168.250.250(eth0) 192.168.251.251(eth1)
ネットワークマスク	NetworkMask	255.255.255.0
ネットワークアドレス	NetworkAddress	192.168.250.0
デフォルトゲートウェイアドレス	DefaultGateway	192.168.250.1
マネージャアドレス	ManagerIpAddress	192.168.250.251
ドメイン名	DomainName	isnq.dom
DNS サーバアドレス	DNSServer	未設定
エージェント名・ホスト名	AgentName	isnq30
タグ VLAN 設定情報	VLAN1～VLAN8 （NQ30c の場合は VLAN1～VLAN16） （NQ30d の場合は VLAN1～VLAN32）	未設定
通信速度	ifSpeed	auto
共有ネットワーク機能設定状態	MultiNetwork	Off
監視対象ネットワークリスト	NetworkList	未設定
不正接続防止設定状態	JamStatus	Off
データ収集設定状態	CollectOfPacket	Off
新規ホストの状態(色)	NewHostStatus	0

監視用インターフェース	MonitoringIf	eth0
データ収集専用インターフェース	InfoCollectIf	未設定
ハードウェア VLAN ID	IfVlanId	1,2

・ダウングレードして初期化する場合

NQ30b は V3.1g、NQ30c と NQ30d は V2.2 へダウングレードし、「パスワードやネットワーク情報などを初期化する場合」の内容に加え、以下のエージェント設定の項目も初期化されます。

初期化内容	パラメータ	初期値
設置場所	AgentLocation	未設定
管理者氏名	AdminName	未設定
管理者電話番号	AdminTelephoneNumber	未設定
管理者メールアドレス	AdminMailAddress	未設定
マネージャポート	ManagerPort	23490
DHCP スコープ	DhcpScope	未設定

1.7.2　初期化方法

・NQ30b、NQ30d の場合

電源を投入した直後から STATUS ランプが橙に点灯するまでの間 STATUS スイッチ(※1)を押下し続けると初期化を行います。

・NQ30c の場合

①電源を投入した直後から STATUS ランプが橙に点灯します（約 5 秒）。

②STATUS ランプが消灯します（約 25 秒）。消灯中に STATUS スイッチ(※1)の押下を始めてください。

③STATUS ランプが下記の状態になるまで STATUS スイッチ(※1)を押下し続けると初期化を行います。

赤に点灯（約 25 秒）⇒消灯（約 1 秒）⇒橙に点灯

初期化内容	使用する STATUS スイッチ
パスワードやネットワーク情報などを初期化する場合	SW1
ダウングレードして初期化する場合	SW1 と SW2

STATUS ランプが赤に点灯すると初期化が完了(※2)します。その後、NetworkAgent サービスを起動し、定常状態になると、STATUS ランプは緑色に点灯します。

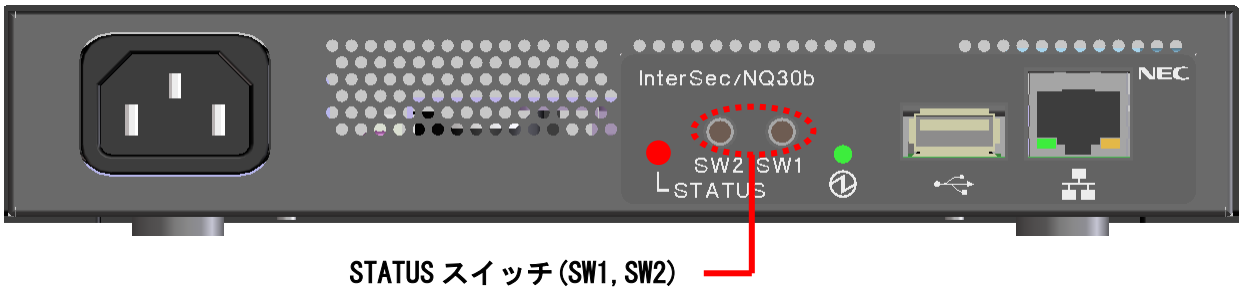
(※1)ダウングレード中に電源断などにより初期化が失敗した場合、次の NQ 起動時に再度初期化

を行います。

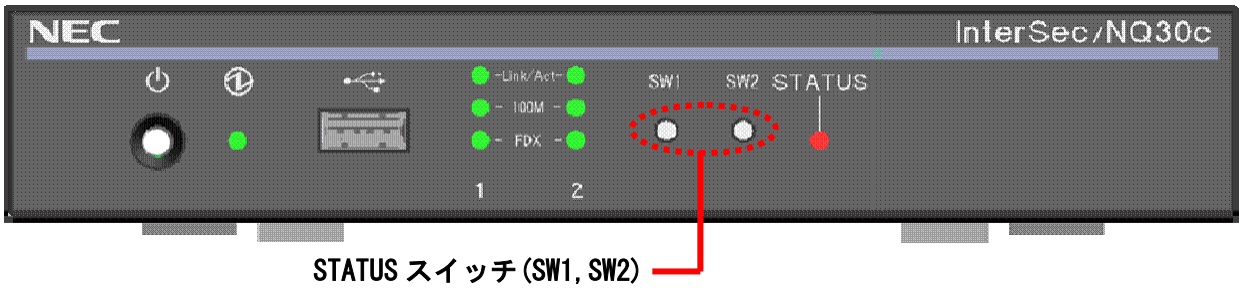
(※2)NQ30b を「ダウングレードして初期化」した場合、初期化完了後に STATUS ランプが赤にならず消灯したままとなります。

(※)NQ30b、NQ30c の STATUS スイッチ

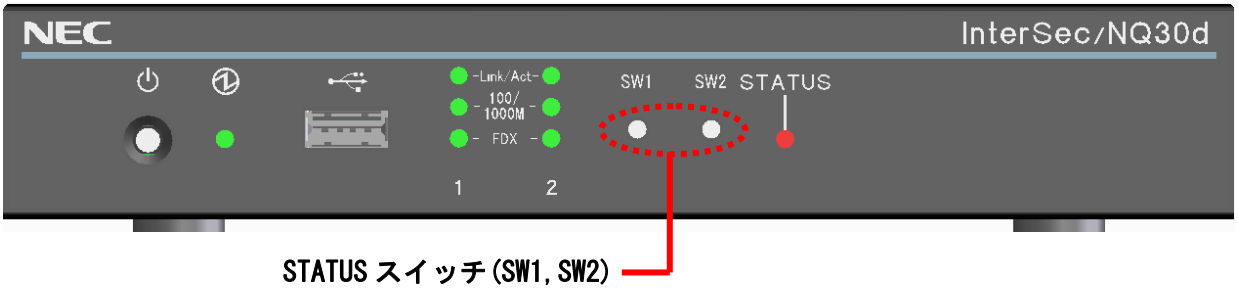
■NQ30b 背面パネルイメージ



■NQ30c 前面パネルイメージ



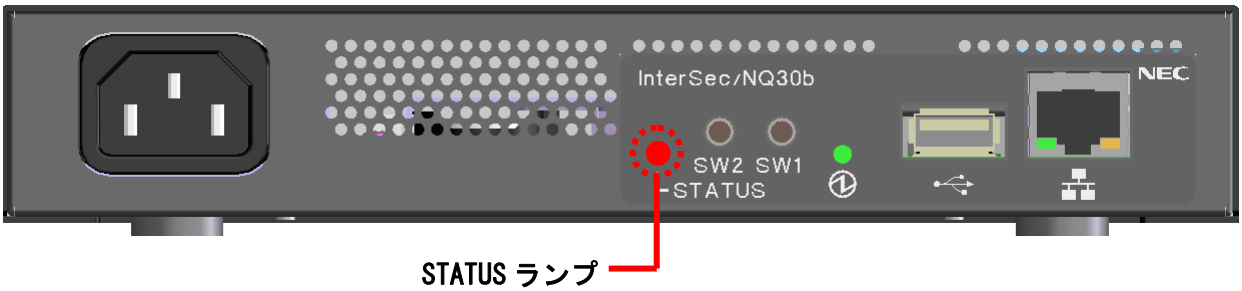
■NQ30d 前面パネルイメージ



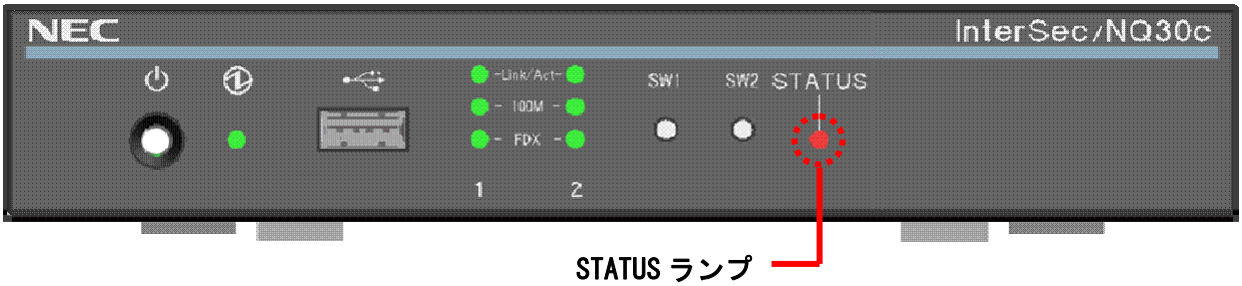
1.8　InterSec/NQ30b、NQ30c、NQ30d の動作状況確認方法について

V3.6 以降の NQ30b、NQ30c、NQ30d の STATUS ランプで NetworkAgent、OS の動作状況を確認することが可能となりました。STATUS ランプは、NQ30c と NQ30d は前面と背面、NQ30b は背面にあります。なお、工場出荷時の NQ30b および、NQ30a では本機能は未サポートです。

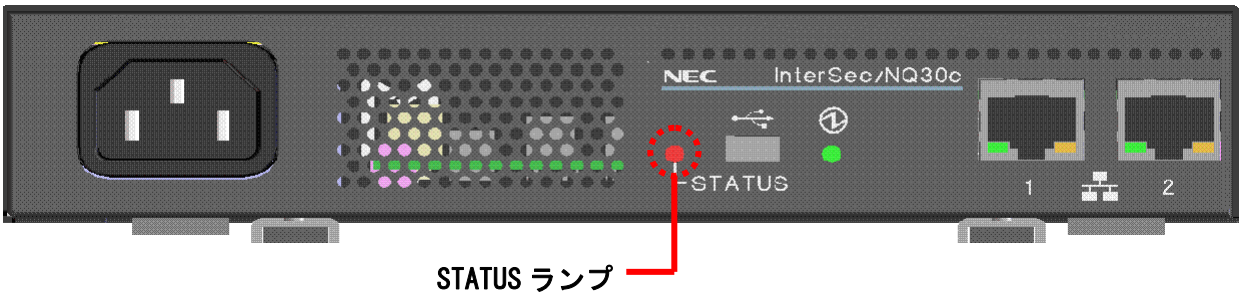
■NQ30b 背面パネルイメージ



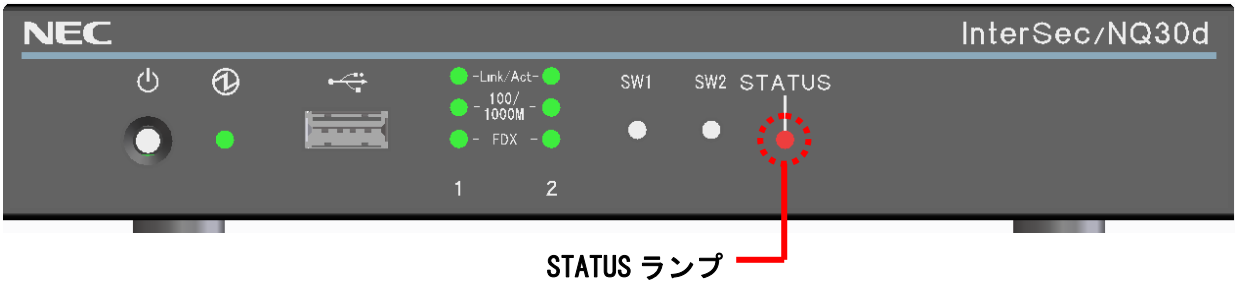
■NQ30c 前面パネルイメージ



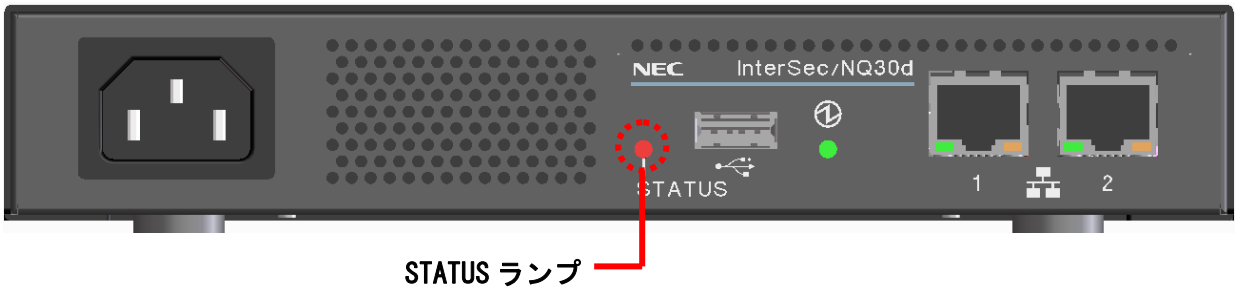
■NQ30c 背面パネルイメージ



■NQ30d 前面パネルイメージ



■NQ30d 背面パネルイメージ



STATUS ランプ

STATUS ランプの状態	InterSec/NQ30b NQ30c NQ30d の状態
消灯（※）	電源 OFF の状態
赤の点灯	OS 起動中で NetworkAgent サービス停止中の状態
緑の点灯	OS、NetworkAgent サービス起動中の状態(定常状態)
橙の点灯	以下の何れかの動作の状態 ・NQ30c 起動直後 ・自動バージョンアップ中 ・STATUS ボタン押下による初期化中の状態 （注意）この状態で電源 OFF しないでください。

（※）状態遷移の間に一時的（２秒～３０秒程度）に消灯します。

起動時、及び各種メンテナンス作業時の STATUS ランプの状態遷移(時系列)は以下の通りです。

１）電源投入時の STATUS ランプの状態遷移

STATUS ランプの状態	InterSec/NQ30b、NQ30d の状態	InterSec/NQ30c の状態
消灯	電源 OFF の状態	電源 OFF の状態
橙の点灯	なし	電源を ON し、NQ を起動中 （橙点灯後、一時消灯）
赤の点灯	電源 ON し、OS を起動中	OS を起動中
緑の点灯	NetworkAgent サービスを起動し、定常状態	NetworkAgent サービスを起動し、定常状態

２）自動バージョンアップ時の STATUS ランプの状態遷移

STATUS ランプの状態	InterSec/NQ30b の状態	InterSec/NQ30c の状態	InterSec/NQ30d の状態
緑の点灯	定常状態	定常状態	定常状態
赤の点灯	SiteManager よりバージョンアップモジュールをダウンロードし、NetworkAgent サービスを停止	SiteManager よりバージョンアップモジュールをダウンロードし、NetworkAgent サービスを停止	SiteManager よりバージョンアップモジュールをダウンロードし、NetworkAgent サービスを停止（橙点灯後）
橙の点灯	バージョンアップ中	バージョンアップ中	なし
消灯	バージョンアップ完了後､本体をリブートするため一旦、電源 OFF	バージョンアップ完了後、本体をリブートするため一旦、電源 OFF	バージョンアップ完了後、本体をリブートするため一旦、電源 OFF
橙の点灯	なし	電源を ON され､NQ を起動中	なし
赤の点灯	電源 ON され、OS を起動	OS を起動中	電源 ON され､OS を起動
緑の点灯	NetworkAgent サービスを起動し､定常状態に戻る	NetworkAgent サービスを起動し、定常状態に戻る	NetworkAgent サービスを起動し、定常状態に戻る

3）STATUS ボタン押下による「パスワード／ネットワーク情報初期化」時の STATUS ランプの状態遷移

STATUS ランプの状態	InterSec/NQ30b の状態	InterSec/NQ30c の状態	InterSec/NQ30d の状態
消灯	電源 OFF の状態	電源 OFF の状態	電源 OFF の状態
橙の点灯	なし	電源 ON し、NQ を起動中（橙点灯後、一時消灯）	電源 ON し、NQ を起動中
赤の点灯	電源 ON し、OS を起動中	OS を起動中	OS を起動中
橙の点灯	STATUS ボタン押下による初期化処理中	STATUS ボタン押下による初期化処理中	なし
赤の点灯	初期化処理完了	初期化処理完了	初期化処理完了（一時消灯後）
緑の点灯	NetworkAgent サービスを起動し、定常状態に戻る	NetworkAgent サービスを起動し、定常状態に戻る	NetworkAgent サービスを起動し、定常状態に戻る

4）STATUS ボタン押下による「ダウングレード初期化」時の STATUS ランプの状態遷移

STATUS ランプの状態	InterSec/NQ30b の状態	InterSec/NQ30c の状態	InterSec/NQ30d の状態
消灯	電源 OFF の状態	電源 OFF の状態	電源 OFF の状態
橙の点灯	なし	電源 ON し、NQ を起動中（橙点灯後、一時消灯）	電源 ON し、NQ を起動中
赤の点灯	電源 ON し、OS を起動中	OS を起動中	OS を起動中
橙の点灯	STATUS ボタン押下による初期化処理中	STATUS ボタン押下による初期化処理中	なし
消灯	ダウングレード完了後、本体をリブートするため一旦、電源 OFF	ダウングレード完了後、本体をリブートするため一旦、電源 OFF	ダウングレード完了後、本体をリブートするため一旦、電源 OFF
橙の点灯	なし（※）	電源を ON され、NQ を起動中	なし
赤の点灯	なし（※）	初期化処理完了	初期化処理完了
緑の点灯	なし（※）	NetworkAgent サービスを起動し、定常状態に戻る	NetworkAgent サービスを起動し、定常状態に戻る

（※）NQ30b を「ダウングレードして初期化」した場合、初期化完了後に STATUS ランプが赤にならず消灯したままとなります。

1.9　使用ポート一覧

NQ と通信する際に必要なポートは以下の通りです。

送信元	送信先	説明
SiteManager (ANY/TCP)	NetworkAgent (23491/TCP)	SiteManager －NetworkAgent 間通信(必須)
NetworkAgent (ANY/TCP)	SiteManager (23490/TCP)	
監視対象サブネット内の PC(ANY/UDP)	NetworkAgent (23499/UDP)	InfoCage 不正接続防止と連携可能な PC 管理製品(パソコン見張り隊など)からの存在通知(任意)
NetworkAgent (ANY/UDP)	監視対象サブネット内の PC(11039/UDP)	監視 LAN 内の PC への状態(色)通知(任意)
NetworkAgent (ANY/UDP)	監視対象サブネット内の PC(137/UDP)	PC のコンピュータ名とユーザ情報を取得する(任意)
NetworkAgent (ANY/TCP)	監視対象サブネット内の PC(139/TCP)	OS 種別を取得(OS デテクト機能)で利用(任意)
DomainManager (ANY/TCP)	NetworkAgent (23491/TCP)	集中管理画面より NetworkAgent の動作ログ即時取得をする際に利用（任意）
クライアント (ANY/TCP)	NetworkAgent (23496/TCP)	コマンドラインインターフェースにより設定変更を行うための telnet ポート（必須）
NetworkAgent (514/UDP)	任意の送信先 (514/UDP)	syslog 転送機能を使用する場合に利用（任意）

(※)ANY は任意のポート番号です。

(※)検知した PC のコンピュータ名などを取得するためには、137/UDP、139/TCP を許可する必要がありますが、この作業を行うと、ウイルスやワームに感染する危険性が高くなるため、推奨ではありません。

2　セットアップ

工場出荷時の NQ は以下の通り、暫定的なバージョンの NetworkAgent がプリインストールされています。

製品名	製品型番	バージョン
InterSec/NQ30a	N8100-1110Q	2.2g
InterSec/NQ30b	N8100-1200Q	2.2h
	N8100-1300Q	3.1g
InterSec/NQ30c	N8100-1400Q	2.2-3.8(※1)
InterSec/NQ30d	N8100-1500Q	2.2-5.2(※2)

(※1) バージョン 2.2 から 3.8 に対応するモジュールがプリインストールされています。
(※2) バージョン 2.2 から 5.2 に対応するモジュールがプリインストールされています。

従いまして、初期導入時に下記の手順によるバージョンアップ手続きが必要です。なお、バージョンアップについての説明、注意事項に関しては、SiteManager オンラインヘルプの、[InfoCage 不正接続防止]->[InfoCage 不正接続防止その他の機能]->[エージェントの自動バージョンアップ機能]を参照してください。V3.7 以降、SiteManager のバージョンアップ後、特定の NQ のみ手動で更新することも可能です。

【バージョンアップ手順】

① NQ に対して､SiteManager と通信するために必要な初期設定(2.2 章または 2.3 章を参照)を行い、ネットワークに接続します。

② NQ が SiteManager へ接続し、自動バージョンアップを行います。(SiteManager から本バージョンの内部ソフトウェアをダウンロードし、インストールを自動的に行います)。

③ バージョンアップ後、本バージョンに対する必要な設定を行います。
設定可能なパラメータについては下記章を参照してください。
・7 NQ のパラメータ詳細

Apple 社製端末、Linux 系 OS 端末、携帯端末を監視対象に含める場合に必要な設定がありますので下記章を参照してください。
・8.5 Apple 社製端末を監視対象にする場合の設定必須パラメータ
・8.6 Linux 系 OS 端末を監視対象にする場合の設定必須パラメータ
・8.7 携帯端末を監視対象にする場合の設定必須パラメータ

④ 運用開始する。

2.1　セットアップ方法

NQ のセットアップは、以下の 2 つの方法があります。

・USB メモリを使用して設定ファイルを反映させる　→　2.2 章参照
・telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続によりコマンドを入力する　→　2.3 章参照

2.2　USB メモリを使用したセットアップ

2.2.1　USB メモリを使用したセットアップ手順

USB メモリを使用したセットアップ手順は以下の通りです。

① SiteManager をインストールする

「InfoCage 不正接続防止 SiteManager インストールマニュアル」を参照し、管理サーバに SiteManager をインストールしてください。

② USB メモリに設定ファイルを作成する

USB メモリのルートフォルダに設定ファイルを作成してください。設定ファイルの作成方法は、2.2.2 章～2.2.4 章を参照してください。NQ は、USB メモリのルートフォルダに保存された設定ファイルのみ認識することができます。

③ USB メモリを差込み、NQ を起動する

NQ 筐体へ設定ファイルを保存した USB メモリ､ネットワークに接続された LAN ケーブル、電源ケーブルを接続してください。接続完了後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。

【注意事項】
・NQ30c の背面パネルにある mini USB ポートは使用できません。
・NQ30c、NQ30d は USB2.0 の USB メモリのみ使用できます。
・USB メモリから設定ファイルを認識させることができるのは、起動時のみです。NQ の起動後に筐体へ USB メモリを接続しても、設定ファイルを認識させることはできませんので注意してください。
・NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

④ USB メモリの認識状態を確認する

NQ が USB メモリを正常に認識したことを確認するため、起動から約 1 分経過後、NQ 筐体から USB メモリを取り外し、USB メモリを PC に接続してください。NQ が USB メモリを正常に認識できた場合は､USB メモリのルートフォルダにテキストファイル(svconflog.txt)が作成されます。テキストファイルが作成されない場合､NQ と USB メモリの相性が悪い、NQ が暗号化 USB メモリに対応していないなどが原因で、認識できていない可能性があります。テキストファイルの詳細は、6.2 章を参照してください。

⑤ パスワードの認証結果を確認する

NQ が USB メモリ内の設定ファイルから認証パスワードを確認する際に認証エラーとなった場合、④で作成されたテキストファイルにエラーログが出力されます。エラーログが出力された場合は 2.2.2 章を参照し、設定ファイルの記述フォーマットに問題がないか確認してください。また、7.1 章の「Password」の項目を参照し、認証パスワードの記述方法に問題がないか確認してください。なお、エラーログの詳細は、6.2 章を参照してください。

⑥ パラメータの設定状況を確認する

NQ が USB メモリ内の設定ファイルから実行したパラメータの設定状況は、パスワードの認証結果と同様、④で作成されたテキストファイルに出力されます。エラーログが出力された場合は 2.2.2 章、3.7 章を参照し、設定ファイルの記述フォーマット、パラメータ、設定値に問題がないか、確認してください。

設定ファイルの例とログの出力イメージは以下の通りです。

[設定ファイル]

```
password:admin
MultiNetwork:On
DisablePreventionAutoIPAddr:On
```

[出力イメージ]

```
2009/12/04 14:07:55 JST: mount ok
+ Welcome to SvNaConsole.
set if auto on
+ Command succeeded.
set na MultiNetwork On
+ Command succeeded.
set na DisablePreventionAutoIPAddr On
+ Command succeeded.
+ Goodbye.
```

⑦ NQ の設定状態を確認する

NQ の起動時に、設定ファイルで接続先として指定した SiteManager インストール PC と正常に通信可能で、SiteManager サービスが起動している場合は、設定ファイルにて指定したエージェント名のアイコンが SiteManager インストール PC 上のサイトコンソールに表示されます。

サイトコンソールに表示されない場合や SiteManager サービスが起動していない場合は、6.3 章を参照して NQ の設定状態を確認してください。

⑧ VLAN インターフェースの設定状態を確認する

非タグ VLAN 環境で使用する場合、VLAN インターフェースが設定されていると、正常にデータ収集ができません。ネットワークインターフェース確認コマンド（3.7.3 章参照）で設定状態を確認し、VLAN インターフェースが設定されていれば 7.5 章の「Vlan(-)」の項目、または VLAN インターフェース削除コマンド（3.7.20 章参照）を参照の上、USB メモリを使用した設定ファイルの反映や、telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続によるコマンド入力で設定の削除を行ってください。

タグ VLAN 環境で使用する場合、VLAN インターフェースの設定数は、最大で 8 個（NQ30c の場合は 16 個、NQ30d の場合は 32 個）までのサポートとなります。不要な VLAN インターフェースが設定されている場合、削除して使用してください。

2.2.2　設定ファイル作成方法

［ファイル名］

svconfig.txt　（全て半角小文字）

［注意事項］

・設定ファイルで使用可能な文字コードは、Shift_JIS、および日本語 EUC(EUC-JP)です。また、使用可能な改行コードは、<CR>+<LF>、および<LF>です。使用するテキストエディタの設定を確認の上、作成してください。なお、Windows 標準のメモ帳は Shift_JIS、<CR>+<LF>で作成されます。設定ファイルの文字コードに日本語 EUC を使用する場合、設定ファイル内での文字コード指定が必須となります。

・設定ファイルは、同一のパラメータを複数行記述しないでください。同一パラメータが複数行記述されている場合、後に記述されたパラメータの内容が設定されます。

・設定ファイルは、1 行につき 1 個のパラメータを記述してください。複数のパラメータを記述する場合は、改行してください。

・パラメータと設定値の間は、コロン（:）で区切ってください。

・パラメータと設定値は、1 行で記述してください。記述行には、不要な改行や半角スペースなどを記述しないでください。

・設定必須パラメータは、パラメータに対する設定値を必ず設定してください。

・設定可能パラメータは、設定値がなければ設定ファイルへ記述しないでください。

・設定ファイルへ設定パラメータを記述しない場合、設定済の値（工場出荷時は既定値）が使用されます。

・設定ファイル内に、設定削除のパラメータと設定反映のパラメータを記述する場合、設定削除パラメータ以降に設定反映パラメータを記述してください。設定削除のパラメータは、パラメータの末尾に「(-)」が記述されたものが該当します。

・設定ファイルは、最後のパラメータ記述後、改行してください。

［設定項目］

設定ファイルの記述例は、非タグ VLAN 環境への初期設定時は 2.2.3 章、タグ VLAN 環境への初期設定時は 2.2.4 章を参照してください。設定パラメータの詳細は、7 章 を参照してください。記述例に記述されていない設定可能パラメータは、必要に応じて設定ファイルに追記して使用してください。

2.2.3　非タグ VLAN 環境への初期設定時の設定パラメータ例

以下に非タグ VLAN 環境へ導入する際の初期設定例を示します。設定パラメータを変更、または追記する場合、7 章 を参照して適切な設定を記述してください。

［設定例］

Password:admin	認証パスワード
AgentName:isnq30	エージェント名
IpAddress:192.168.250.250	エージェントの IP アドレス
NetworkMask:255.255.255.0	サブネットマスク
ManagerAddress:192.168.250.249	サイトマネージャアドレス
DNSServer:192.168.250.2 192.168.250.3	DNS サーバアドレス
DomainName:isnq.dom	ドメイン名
DefaultGateway:192.168.250.1	デフォルトゲートウェイアドレス

2.2.4　タグ VLAN 環境への初期設定時の設定パラメータ例

以下にタグ VLAN 環境へ導入する際の初期設定例を示します。設定パラメータを変更、または追記する場合、7 章 を参照して適切な設定を記述してください。

［設定例］

Password:admin	認証パスワード
AgentName:isnq30	エージェント名
IpAddress:127.0.0.1	NQ の IP アドレス
ManagerAddress:192.168.250.249	サイトマネージャアドレス
Vlan1:192.168.10.250 24 111	VLAN ID 111 の設定
Vlan2:192.168.20.250 24 112	VLAN ID 112 の設定
Vlan3:192.168.30.250 24 113	VLAN ID 113 の設定
Vlan4:192.168.40.250 24 114	VLAN ID 114 の設定
Vlan5:192.168.50.250 24 115	VLAN ID 115 の設定
Vlan6:192.168.60.250 24 116	VLAN ID 116 の設定
Vlan7:192.168.70.250 24 117	VLAN ID 117 の設定
Vlan8:192.168.80.250 24 118	VLAN ID 118 の設定
DNSServer:192.168.10.2 192.168.10.3	DNS サーバアドレス
DomainName:isnq.dom	ドメイン名
DefaultGateway:192.168.10.254	デフォルトゲートウェイアドレス

2.3　ネットワーク接続を使用したセットアップ

2.3.1　ネットワーク接続を使用したセットアップ手順

telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続を使用したセットアップ手順は以下の通りです。

① SiteManager をインストールする

「InfoCage 不正接続防止 SiteManager インストールマニュアル」を参照し、管理サーバに SiteManager をインストールしてください。

② NQ を起動する

NQ 筐体へ、ネットワークに接続された LAN ケーブル（※)、電源ケーブルを接続してください。接続完了後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

（※）タグ VLAN 環境で使用する場合、工場出荷時の状態では L3SW のタグ付きパケットの送受信を可能とするトランクポートに接続しても通信できません。非タグ VLAN 環境に接続して設定を行い、NQ の再起動後、トランクポートに接続してください。

③ telnet(SSH)クライアント PC を用意する

NQ の初期ネットワーク設定は以下の通りです。

IP アドレス	: 192.168.250.250
サブネットマスク	: 255.255.255.0
デフォルトゲートウェイアドレス	: 192.168.250.1
DNS サーバアドレス	: 設定なし

PC に NQ と同じネットワークの IP アドレス(例えば 192.168.250.111)を設定し、NQ と同じ LAN に接続してください。接続後、ping コマンドなどを使用して NQ との通信状態を確認してください。

[実行例]

```
C:¥> ping 192.168.250.250 (※)
```

(※)斜体部分は、NQ に設定されている IP アドレス、あるいは IP アドレスに割り当てられているホスト名を設定してください。実行例の IP アドレスは、工場出荷時の設定で

す。

NQ と通信できない場合は、NQ に設定されているネットワークと接続できるよう、telnet(SSH)クライアント PC のネットワーク設定を確認してください。

④ ネットワーク接続を使用してセットアップする

telnet(SSH)クライアント PC で、telnet もしくは SSH(NQ30c、NQ30d のみ)を介して NQ に接続し、セットアップを行ってください。Windows PC のコマンドプロンプトを使用したセットアップ方法の例を 2.3.2 章に記載していますので確認してください。セットアップ完了後は、設定内容を反映させるため、必ず NQ の再起動を行ってください。なお、各コマンドの詳細は、3 章、7 章を参照してください。

⑤ NQ の設定状態を確認する

NQ の起動時に、接続先として設定した SiteManager インストール PC と正常に通信可能で、SiteManager サービスが起動している場合は、NQ に設定されているエージェント名のアイコンが SiteManager インストール PC 上のサイトコンソールに表示されます。

サイトコンソールに表示されない場合や SiteManager サービスが起動していない場合は、6.3 章を参照して NQ の設定状態を確認してください。

2.3.2　ネットワーク接続を使用したセットアップの実行例

［注意］

・設定しない属性については、該当のコマンドを実行する必要はありません。

・非タグ VLAN 環境で使用する場合、VLAN インターフェースが設定されていると、正常にデータ収集ができません。ネットワークインターフェース確認コマンド（3.7.3 章参照）で設定状態を確認し、VLAN インターフェースが設定されていれば 7.5 章の「Vlan(-)」の項目、または VLAN インターフェース削除コマンド（3.7.20 章参照）を参照の上、USB メモリを使用した設定ファイルの反映や、telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続によるコマンド入力で設定の削除を行ってください。

・タグ VLAN 環境で使用する場合、VLAN インターフェースの設定数は、最大で 8 個（NQ30c の場合は 16 個、NQ30d の場合は 32 個）までのサポートとなります。不要な VLAN インターフェースが設定されている場合、削除して使用してください。

［実行例］

■非タグ VLAN 環境設置時の実行例

```
C:¥>telnet 192.168.250.250 23496
- 400 require authentication
svna> pass admin
+ Welcome to SvNaConsole.
svna> set us admin xxxxxxxx
+ Command succeeded.
svna> set if auto off
+ Command succeeded.
svna> set ns nameserver 10.1.2.6 10.1.2.7
+ Command succeeded.
svna> set ns domain isnq30.dom
+ Command succeeded.
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:172.16.171.255
        UP  BROCAST  RUNNING  MULTICAST
eth0.100        inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.10.255
        Default Gateway:192.168.10.254
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> remove vlan eth0.100
+ Command Succeeded.
svna> set if eth0 address 10.1.2.252 mask 255.255.255.0
+ Command succeeded.
svna> set gw 10.1.2.254
+ Command succeeded.
svna> set na stop
+ Command succeeded.
svna> set hn isnq30
+ Command succeeded.
svna> set sm 10.1.2.253
+ Command succeeded.
svna> reboot
 + Command succeeded.
```

→ telnet によるネットワーク接続の詳細は 3.2 章参照

→ 認証コマンドの詳細は 3.7.1 章参照

→ パスワード変更コマンドの詳細は 3.7.2 章参照

→ ネットワークインターフェース設定の反映タイミング変更コマンドの詳細は 3.7.6 章参照

→ DNS サーバアドレス設定コマンドの詳細は 3.7.9 章参照

→ ドメイン名設定コマンドの詳細は 3.7.10 章参照

→ネットワークインターフェース確認コマンドの詳細は 3.7.3 章参照

→VLAN インターフェースが設定されている場合、必ず削除してください
なお、工場出荷時は実行不要です

→VLAN インターフェース削除コマンドの詳細は 3.7.20 章参照

→ ネットワークインターフェース設定コマンドの詳細は 3.7.7 章参照

→ デフォルトゲートウェイアドレス設定コマンドの詳細は 3.7.21 章参照

→ エージェント停止コマンドの詳細は 3.7.24 章参照

→ エージェント名設定コマンドの詳細は 3.7.15 章参照

→ マネージャ設定コマンドの詳細は 3.7.14 章参照

→ 再起動コマンドの詳細は 3.7.13 章参照

■タグ VLAN 環境設置時の実行例

```
C:¥>telnet 192.168.250.250 23496
- 400 require authentication
svna> pass admin
+ Welcome to SvNaConsole.
svna> set us admin xxxxxxxx
+ Command succeeded.
svna> set if auto off
+ Command succeeded.
svna> set ns nameserver 10.1.2.6 10.1.2.7
+ Command succeeded.
svna> set ns domain isnq30.dom
+ Command succeeded.
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:172.16.171.255
        UP  BROCAST  RUNNING  MULTICAST
eth0.100        inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.10.255
        Default Gateway:192.168.10.254
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> remove vlan eth0.100
+ Command Succeeded.
svna> add vlan eth0 111
+ Command succeeded.
svna> set if eth0.111 address 10.1.2.252 mask 255.255.255.0
+ Command succeeded.
svna> set if eth0 address 127.0.0.1
+ Command succeeded.
svna> set gw 10.1.2.254
+ Command succeeded.
svna> set na stop
+ Command succeeded.
svna> set hn isnq30
+ Command succeeded.
svna> set sm 10.1.2.253
+ Command succeeded.
svna> reboot
 + Command succeeded.
```

→ telnet によるネットワーク接続の詳細は 3.2 章参照

→ 認証コマンドの詳細は 3.7.1 章参照

→ パスワード変更コマンドの詳細は 3.7.2 章参照

→ ネットワークインターフェース設定の反映タイミング変更コマンドの詳細は 3.7.6 章参照

→ DNS サーバアドレス設定コマンドの詳細は 3.7.9 章参照

→ ドメイン名設定コマンドの詳細は 3.7.10 章参照

→ネットワークインターフェース確認コマンドの詳細は 3.7.3 章参照

→不要な VLAN インターフェースが設定されている場合、削除してください
なお、工場出荷時は実行不要です

→VLAN インターフェース削除コマンドの詳細は 3.7.20 章参照

→ VLAN インターフェース追加コマンドの詳細は 3.7.19 章参照

→ ネットワークインターフェース設定コマンドの詳細は 3.7.7 章参照

→ デフォルトゲートウェイアドレス設定コマンドの詳細は 3.7.21 章参照

→ エージェント停止コマンドの詳細は 3.7.24 章参照

→ エージェント名設定コマンドの詳細は 3.7.15 章参照

→ マネージャ設定コマンドの詳細は 3.7.14 章参照

→ 再起動コマンドの詳細は 3.7.13 章参照

3　コマンドラインインターフェース

3.1　コマンドラインインターフェース概要

NQ では、コマンドラインインターフェースによって、NQ の設定を参照／変更することができます。コマンドラインインターフェースは、telnet もしくは SSH(NQ30c、NQ30d のみ)を利用したネットワーク接続を介して NQ にアクセスすることで使用可能です。なお、NQ の設定を参照／変更する場合、認証コマンド（3.7.1 章参照）を使用して各コマンドを実行可能な状態に遷移させる必要があります。

なお、本書の実行例は Windows PC のコマンドプロンプトを使用した場合として記載しています。その他のターミナルソフトを使用する場合は、実行例を参考に利用してください。

3.2　telnet によるネットワーク接続

telnet を介した NQ へのネットワーク接続方法を以下に説明します。

[書式]

```
telnet 〈host〉 23496
```

[説明]

NQ の 23496 番ポートへ telnet を介してネットワーク接続を行います。なお、使用ポートを変更することはできません。コマンドは、全て半角英数字で入力してください。
Tera Term を使用する場合、ツールバーから[File]→[New connection]を選択し、以下の設定を行ってください。

通信種別　　: TCP/IP
Host　　: NQ の IP アドレス、またはホスト名
Service　: Telnet
TCP Port#　: 23496

その他のターミナルソフトを使用する場合は、上記の内容を参考に接続先を指定してください。

[引数]

引数	説明
〈host〉	NQ の IP アドレスまたはホスト名

[実行例]

```
C:¥> telnet 192.168.250.250 23496
- 400 require authentication
svna>
```

[注意]

telnet を介した NQ へのネットワーク接続後、画面上にメッセージが出力されない、入力文字が表示されない、Enter キー入力による実行ができない場合の対処方法は、6.1 章を参照してください。

3.3　SSHによるネットワーク接続

NQ30c、NQ30dでは、V5.1以降、SSHを介してNQへのネットワーク接続ができるようになりました。
NQ30c、NQ30dのSSHポート(22)へSSHを介してネットワーク接続を行います。なお、使用ポートを変更することはできません。
Tera Termを使用する場合、ツールバーから[File]→[New connection]を選択し、以下の設定を行ってください。

通信種別　　：TCP/IP
Host　　：NQ30c、NQ30dのIPアドレス、またはホスト名
Service　　：SSH
TCP Port#　：22
SSH version：SSH2

SSH Authentication
User name　：admin
Passphrase　：なし
“Use plain password to log in”を選択

その他のターミナルソフトを使用する場合は、上記の内容を参考に接続先を指定してください。
SSHで接続した後は、telnetでの接続と同様に認証コマンド(pass)を使用して認証パスワードを入力してください。

3.4　認証前のネットワーク接続終了方法

[書式]

```
exit
```

[説明]

telnet もしくは SSH(NQ30c、NQ30d のみ)を介して NQ へネットワーク接続した際に、認証コマンド（3.7.1 章参照）実行前に接続を終了する場合は、以下のコマンドを実行してください。
なお、終了コマンド（3.7.12 章参照）とは異なり、quit コマンドは使用できません。

[実行例]

```
C:¥> telnet 192.168.250.250 23496          ネットワーク接続を行う
- 400 require authentication
svna> exit                                 ネットワーク接続を終了する
+ Goodbye.

ホストとの接続が切断されました。
C:¥>
```

3.5　コマンド一覧

NQ でサポートするコマンドの一覧を以下に示します。本書で説明されていないコマンドはサポート対象外です。

説明	コマンド	参照
認証コマンド	pass	3.7.1 章
認証パスワード変更コマンド	set us	3.7.2 章
ネットワークインターフェース確認コマンド	list if	3.7.3 章
DNS サーバアドレス、ドメイン名確認コマンド	list ns	3.7.4 章
エージェント設定確認コマンド	list na	3.7.5 章
ネットワークインターフェース設定の反映タイミング変更コマンド	set if auto	3.7.6 章
ネットワークインターフェース設定コマンド	set if	3.7.7 章
エージェント設定コマンド	set na	3.7.8 章
DNS サーバアドレス設定コマンド	set ns nameserver	3.7.9 章
ドメイン名設定コマンド	set ns domain	3.7.10 章
ヘルプコマンド	help	3.7.11 章
終了コマンド	exit quit	3.7.12 章
再起動コマンド	reboot set na reboot	3.7.13 章
マネージャ設定コマンド	set sm	3.7.14 章
エージェント名設定コマンド	set hn	3.7.15 章
初期化コマンド	init all	3.7.16 章
シャットダウンコマンド	shutdown set na shutdown	3.7.17 章
ネットワークインターフェースのネゴシエーション設定変更コマンド	set ifspeed	3.7.18 章
VLAN インターフェース追加コマンド	add vlan eth0	3.7.19 章
VLAN インターフェース削除コマンド	remove vlan	3.7.20 章
デフォルトゲートウェイアドレス設定コマンド	set gw	3.7.21 章
DNS サーバアドレス削除コマンド	remove ns nameserver	3.7.22 章
エージェント開始コマンド	set na start	3.7.23 章
エージェント停止コマンド	set na stop	3.7.24 章
エージェント再起動コマンド	set na restart	3.7.25 章
ドメイン名削除コマンド	remove ns domain	3.7.26 章
デフォルトゲートウェイアドレス削除コマンド	remove gw *	3.7.27 章
文字コード指定コマンド	charset	3.7.28 章
ネットワークリスト追加コマンド	add networklist	3.7.29 章
ネットワークリスト削除コマンド	remove networklist	3.7.30 章

3.6　コマンド入力時の注意・制限事項

- コマンド入力は、一部の引数の入力以外は半角文字を使用してください。エージェント設定コマンド(3.7.8 章参照)を使用して、「AgentLocation」、「AdminName」、「AdminTelephoneNumber」の各項目（7.5 章の該当項目を参照）を設定する場合のみ、引数に全角文字を入力することができます。
- 全角文字は、Shift_JIS、日本語 EUC（EUC-JP）の文字コードが利用できます。telnet クライアント PC の設定を確認の上、文字コード指定コマンド（3.7.28 章参照）を使用して NQ の文字コード設定を一致させてください。
- 入力文字が表示されない、Enter キー入力による実行ができない場合の対処方法は、6.1 章を参照してください。
- 使用する telnet クライアント PC によっては、コマンド入力時に、[back space]、[delete]、方向キー等による入力文字の編集ができない場合があります。
- コマンド実行時に表示されるメッセージから、成功、およびエラーを確認してください。下記に主な表示メッセージを示します。

メッセージ	内容
Welcome to SvNaConsole.	認証成功
Goodbye.	telnet を介したネットワーク接続終了
Invalid command.	コマンド実行エラー（コマンド入力ミスなど）
Command succeeded.	コマンド実行成功
400 require authentication.	telnet を介したネットワーク接続成功
403 bad pass phrase.	認証エラー
404 maximum retries.	認証パスワード入力 3 回失敗時の接続切断通知
500 generic error.	一般エラー
501 system error.	システムエラー
502 no data.	データ（情報詳細）なし
503 invalid data.	不正なデータが設定
504 no record.	設定項目が見つからない

3.7　コマンドリファレンス

3.7.1　認証コマンド（pass）

[書式]

pass *〈password〉*

[説明]

認証コマンドを使用してログインすることで、NQ に対して全てのコマンドを実行可能な状態へ遷移します。telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続後は、本コマンドによって認証しなければ以降に説明するコマンドを利用できません。

〈password〉 には認証パスワードを入力してください。

なお、認証パスワードはセキュリティ対策として既定値から変更することを推奨します。認証パスワードの変更方法は 3.7.2 章を参照してください。

[引数]

引数	説明
〈password〉	設定されている認証パスワード。 パスワードに使用可能な文字は、1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、半角記号、半角スペースからなる文字列です。大文字、小文字を区別します。8 バイト(文字)より長い場合は、以降の文字列は認識されません。引数は、4.2.1 章の注意事項を参照の上、入力してください。工場出荷時の認証パスワードの既定値は『admin』です。

[実行例]

```
svna> pass admin
+ Welcome to SvNaConsole.
svna>
```

[注意]

設定とは異なる認証パスワードを入力してコマンドを実行した場合、認証エラーが合計 3 回に達した時点で NQ へのネットワーク接続が切断されます。認証パスワードを入力せず、pass コマンドのみでコマンドを実行した場合は、認証エラーのメッセージが表示されますが、認証エラーとしてカウントされません。

3.7.2　認証パスワード変更コマンド（set us）

［書式］

set us *〈user〉〈password〉*

［説明］

認証パスワードを変更します。

［引数］

引数	説明
〈user〉	ユーザ名。admin 固定です。
〈password〉	設定変更後に使用する認証パスワード。 パスワードに登録可能な文字は､1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、半角記号、半角スペースからなる文字列です。大文字、小文字を区別します。8 バイト(文字)より長い場合は、以降の文字列は認識されません。引数は、4.2.1 章の注意事項を参照の上、入力してください。

［実行例］

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

認証パスワードを『abcxyz』に変更する

認証パスワードは、変更したパスワードが正しく設定されたことを確認する必要があります。以降の［確認手順］を参照し、確実に設定を行ってください。

[確認手順]

コマンド入力時に[back space]、[delete]、方向キー等による入力文字の編集ができない telnet クライアント PC を使用する場合、認証パスワード入力時に方向キーなどを押下すると、画面上に反映されなくても文字列として認識してしまうことがあります。

そのため、認証パスワードの変更時は、以下の手順で正常にログインできることを確認することを推奨します。手順は、コマンドプロンプトを使用した場合となります。

① 認証パスワードを変更する

telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続を行い、認証コマンドでログインした後、認証パスワード変更コマンドを使用して認証パスワードを変更してください。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

認証パスワードを変更する

② 新たにネットワーク接続を行う

①で接続中のコマンドプロンプトのネットワーク接続を終了させず、新たにコマンドプロンプトを起動させ、NQ へネットワーク接続を行ってください。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
C:¥> telnet 192.168.250.250 23496
- 400 require authentication
svna>
```

別のコマンドプロンプトから接続する

③ 新規接続から認証コマンドを実行する

②で NQ へ接続したコマンドプロンプトから認証コマンドを使用して、①で設定したパスワードでログイン可能か確認してください。パスワードが異なる場合は、認証エラーとなります。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
- 400 require authentication
svna> pass abc
- 403 bad pass phrase.
```

認証コマンドでログインできない場合

パスワードが正しい場合、正常にログインできます。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
svna> pass abcxyz
+ Welcome to SvNaConsole.
svna>
```

認証コマンドでログインできた場合

④ 新規接続から認証コマンドでログインできない場合

①で設定したパスワードを使用しても正常にログインできない場合、変更コマンド使用時に方向キー押下などによる不正な文字入力が含まれた可能性があります。①でログイン中のコマンドプロンプトより、認証パスワードを再設定し、③の確認手順を行ってください。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
svna> pass abcxyz
- 403 bad pass phrase.
svna>
```

認証エラーとなった場合

↓

```
svna> set us admin abcxyz
+ Command succeeded.
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

認証パスワードを再設定する

```
svna> pass abcxyz
- 403 bad pass phrase.
svna> pass abcxyz
+ Welcome to SvNaConsole.
svna>
```

認証コマンドでログインできる

3.7.3　ネットワークインターフェース確認コマンド（list if）

[書式]

```
list if
```

[説明]

ネットワークインターフェースの設定状態を表示します。

[実行例]

■非タグ VLAN 環境設置時の実行例

```
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.250.255
        Default Gateway:192.168.250.1
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna>
```

■タグ VLAN 環境設置時の実行例

```
svna> list if
= Command succeeded.
eth0    inet addr:127.0.0.1 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:127.0.0.255
        UP  BROCAST  RUNNING  MULTICAST
eth0.111        inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.10.255
        Default Gateway:192.168.10.254
        UP  BROCAST  RUNNING  MULTICAST
eth0.112        inet addr:192.168.20.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.20.255
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna>
```

[表示項目]

項目	説明
eth0 eth1	ネットワークインターフェース
eth0.＊	VLAN インターフェース（左記項目のアスタリスク（*）は VLAN ID）
inet addr	IP アドレス
HWaddr	MAC アドレス
Mask	サブネットマスク
Bcast	ブロードキャストアドレス
Default Gateway	デフォルトゲートウェイアドレス

3.7.4　DNS サーバアドレス、ドメイン名確認コマンド（list ns）

[書式]

```
list ns
```

[説明]

DNS サーバの IP アドレス、ドメイン名を表示します。

[実行例]

```
svna> list ns
= Command succeeded.
nameserver 192.168.0.6
nameserver 192.168.0.7
domain isnq.dom
+ Done.
svna>
```

[表示項目]

項目	説明
nameserver	DNS サーバの IP アドレス
domain	NQ が属するドメイン名

3.7.5　エージェント設定確認コマンド（list na）

[書式]

```
list na
```

[説明]

エージェント設定を表示します。確認可能な項目については、7章を参照してください。

[表示形式]

本コマンドを実行した場合、属性名と属性値が同一行に表示されます。
属性名は、アルファベット順にソートされた状態で表示されます。
属性名と属性値は、以下の形式で表示されます。

```
属性名: 属性値
```

[実行例]

```
svna> list na
= Command succeeded.
AdminMailAddress: admin@securevisor.dom
...
+ Done.
svna>
```

[注意]

本コマンドを実行した後に表示される、「PreventIPv6TempAddr」は予約パラメータです。設定を変更しないでください。

3.7.6　ネットワークインターフェース設定の反映タイミング変更コマンド（set if auto）

[書式]

```
set if auto { on | off }
```

[説明]

ネットワークインターフェース設定コマンド（3.7.7 章参照）を実行した時に、設定内容が反映されるタイミングを変更します。設定が有効（*on* ）の場合、ネットワークインターフェース設定コマンドによる設定内容は、コマンド実行直後に反映されます。設定が無効（*off* ）の場合は、NQ の再起動時に反映されます。初期状態では無効が設定されています。

本設定が有効の場合、ネットワークインターフェース設定コマンドを使用して IP アドレスなどを変更すると、コマンド実行直後に反映され、NQ へのネットワーク接続が切断されることがありますので注意してください。

[実行例]

```
svna> set if auto off
+ Command succeeded.
svna>
```

3.7.7　ネットワークインターフェース設定コマンド（set if）

［書式］

set if 〈*nic*〉［address 〈*address*〉］［mask 〈*mask*〉］

［説明］

ネットワークインターフェース設定を行います。set if、または set if 〈*nic*〉のみを実行した場合は、エラーとなります。

［引数］

引数	説明
〈*nic*〉	設定対象のインターフェース。 非タグ VLAN 環境設置時は『eth0（※1)』を指定してください。 VLAN インターフェース設定時は『eth0.〈*vid*〉（※2)』を指定してください。
〈*address*〉	インターフェースに設定する IP アドレス。引数は、4.1 章の注意事項を参照の上、入力してください。設定可能な範囲は、『1.0.0.1』～『223.255.255.254』までとなります。 NQ をタグ VLAN 環境に設置する場合、ネットワークインターフェースである『eth0（※1)』と VLAN インターフェースである『eth0.〈*vid*〉（※2)』に設定する IP アドレスの重複を避けるため、『eth0』に『127.0.0.1』を設定してください。
〈*mask*〉	インターフェースに設定するサブネットマスク。引数は、4.1 章の注意事項を参照の上、入力してください。設定可能な範囲は、『255.0.0.0』の 8 ビットから『255.255.255.252』の 30 ビットまでとなります。 NQ をタグ VLAN 環境に設置する場合、ネットワークインターフェースである『eth0（※1)』に対してサブネットマスクを設定する必要はありません。

(※1) NQ30d の場合は使用するインターフェースに合わせて『eth0』または『eth1』を指定してください

(※2) 〈*vid*〉は VLAN 設定インターフェース追加コマンド（3.7.19 章参照）で指定した VLAN ID

［注意］

『eth0』と『eth1』には異なるネットワークアドレスとなる IP アドレスとサブネットマスクの組み合わせを設定してください。同じネットワークアドレスになる値を設定すると、エラーとなります。

[実行例]

■非タグ VLAN 環境設置時

```
svna> set if auto off                    →ネットワークインターフェース設定の反映タイミング
                                           変更コマンドの詳細は 3.7.6 章参照
+ Command succeeded.

svna> set if eth0 address 192.168.250.250 mask 255.255.255.0
                                         →ネットワークインターフェース設定コマンドの詳細は
+ Command succeeded.                       本章参照

svna> reboot                             →ネットワークインターフェース設定の反映タイミング
                                           変更コマンドを無効に設定した場合は再起動コマンド
+ Command succeeded.                       （3.7.13 章参照）が必須となります
```

■タグ VLAN 環境設置時

```
svna> set if auto off                    →ネットワークインターフェース設定の反映タイミング
                                           変更コマンドの詳細は 3.7.6 章参照
+ Command succeeded.

svna> add vlan eth0 111                  →VLAN インターフェース追加コマンドの詳細は
                                           3.7.19 章参照
+ Command succeeded.

svna> set if eth0 address 127.0.0.1
                                         →ネットワークインターフェース設定コマンドの
+ Command succeeded.                       詳細は本章参照

svna> set if eth0.111 address 211.10.10.200 mask 255.255.255.0

+ Command succeeded.

svna> reboot                             →VLAN インターフェースの設定を反映させるには、
                                           再起動コマンド（3.7.13 章参照）が必須となります
+ Command succeeded.
```

[注意]

NQ をタグ VLAN 環境に設置する場合、VLAN インターフェース追加コマンド（3.7.19 章参照）を実行後､VLAN インターフェースに指定した VLAN ID を使用して本コマンドを実行してください。また、ネットワークインターフェースと VLAN インターフェースの IP アドレスの重複を避けるため､『eth0』(NQ30d の場合は『eth0』と『eth1』)の address の設定値に『127.0.0.1』を設定してください。VLAN インターフェースの設定を行った場合、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（3.7.13 章）を実行してください。

非タグ VLAN 環境設置時に、本コマンドで IP アドレス変更後、NQ の再起動を実施した場合、エージェント設定（4 章参照）の IpAddress、CollectIpAddress、NetworkAddress、NetworkMask の各属性値は、自動的に本コマンドの設定値が反映されます。

なお、ネットワークインターフェース設定の反映タイミング変更コマンド（3.7.6 章参照）を無効に設定していない場合、本コマンド実行直後に IP アドレスなどの変更が反映され、NQ へのネットワーク接続が切断されることがあります。本コマンド実行時は、ネットワークインターフェース設定の反映タイミング変更コマンドは無効に設定し、全ての設定を変更後、NQ を再起動させる手順を強く推奨します。

3.7.8　エージェント設定コマンド（set na）

[書式]

set na *〈attribute〉〈value〉*

[説明]

エージェントの属性を設定します。設定可能な属性は 7 章を参照してください。

[引数]

引数	説明
〈attribute〉	属性名
〈value〉	属性値

[実行例]

```
svna> set na stop
+ Command succeeded.
svna> set na MultiNetwork On
+ Command succeeded.
svna> set na start
+ Command succeeded.
```

→エージェント停止コマンドの詳細は 3.7.24 章参照

→エージェント開始コマンドの詳細は 3.7.23 章参照

[注意]

本コマンドを使用する前に、エージェント停止コマンド（3.7.24 章参照）を使用して NetworkAgent サービスを停止してください。

本コマンドを使用してエージェント属性を変更した場合、設定内容を反映させるため、エージェント開始コマンド（3.7.23 章参照）、あるいは再起動コマンド（3.7.13 章参照）を実行してください。（※）

（※） VLAN インターフェースの追加など、設定内容の反映に NQ の再起動が必要となる操作を併せて実施している場合は、必ず再起動を行ってください。

3.7.9　DNS サーバアドレス設定コマンド（set ns nameserver）

[書式]

set ns nameserver *<server1>* [*<server2>*...]

[説明]

DNS サーバの設定を行います。DNS サーバの設定を行った場合、収集したホストの IP アドレスから DNS 名の逆引きが可能となり、取得した DNS 名を SiteManager へ通知することができます。

[引数]

引数	説明
<server1>...	DNS サーバの IP アドレス。最大 3 個まで設定可能。引数は、4.1 章の注意事項を参照の上、入力してください。複数の DNS サーバアドレスを設定する場合は、引数の間に半角スペースを入れてください。

[実行例]

```
svna> set ns nameserver 192.168.250.6 192.168.250.7
+ Command succeeded.
svna>
```

3.7.10　ドメイン名設定コマンド（set ns domain）

[書式]

set ns domain *<domain1>* [*<domain2>*...]

[説明]

ドメイン名の設定を行います。

[引数]

引数	説明
<domain1>...	DNS のドメイン名。複数のドメイン名を設定する場合は、引数の間に半角スペースを入れてください。

[実行例]

```
svna> set ns domain isnq.dom
+ Command succeeded.
svna>
```

[注意]

本コマンドは、パラメータに設定可能な文字数は 2,000 文字です。文字数制限には、複数設定時に引数の間に設定する半角スペースも含まれますので注意してください。

3.7.11　ヘルプコマンド（help）

[書式]

help [*<command>*]

[説明]

コマンドのヘルプ情報を表示します。help のみを実行した場合はコマンド一覧を表示します。help で表示されるコマンドであっても、本書で説明されていないコマンドの使用はサポート対象外となりますので注意してください。

[引数]

引数	説明
<command>	使用方法を確認したいコマンド名

[実行例]

```
svna> help set
= Usage of set command:
set if <nic> [address <address>] [mask <mask>]
set if <nic> [on|off]
set na <attribute> <value>
set na [start|stop|restart|reboot|shutdown]
set ns nameserver <server1> [<server2>...]
set ns domain <domain1> [<domain2>...]
set ns local <hostname>
set us <user> <password>
set ifspeed [1000fd|1000hd|100fd|100hd|10fd|10hd|auto] <nic>
set gw <defaultgateway>
+ Done.
svna>
```

3.7.12 終了コマンド (exit, quit)

[書式]

```
exit
または
quit
```

[説明]

telnet もしくは SSH(NQ30c、NQ30d のみ)を介したネットワーク接続を終了します。認証コマンド(3.7.1 章参照)による認証後は、exit コマンドと quit コマンドに動作の差異はありません。

[実行例]

```
svna> exit
+ Goodbye.


ホストとの接続が切断されました。
```

3.7.13 再起動コマンド（reboot, set na reboot）

[書式]

```
reboot
または
set na reboot
```

[説明]

NQ を再起動します。reboot コマンドと set na reboot コマンドに動作の差異はありません。

[実行例]

```
svna> reboot
```

3.7.14　マネージャ設定コマンド（set sm）

[書式]

```
set sm 〈address〉
```

[説明]

SiteManager をインストールしている PC の IP アドレスを設定します。

[引数]

引数	説明
〈address〉	NQ の管理／操作を行う SiteManager インストール PC の IP アドレスを設定します。引数は、4.1 章の注意事項を参照の上、入力してください。ホスト名で設定することはできません。

[実行例]

```
svna> set na stop                    →エージェント停止コマンドの詳細は
+ Command succeeded.                   3.7.24 章参照
svna> set sm 192.168.250.251
+ Command succeeded.
svna> set na start                   →エージェント開始コマンドの詳細は
+ Command succeeded.                   3.7.23 章参照
```

[注意]

本コマンドを使用する前に、エージェント停止コマンド（3.7.24 章参照）を使用して NetworkAgent サービスを停止してください。

本コマンドを使用して SiteManager インストール PC の IP アドレスを変更した場合、設定内容を反映させるため、エージェント開始コマンド（3.7.23 章参照）、あるいは再起動コマンド（3.7.13 章参照）を実行してください。（※）

（※） VLAN インターフェースの追加など、設定内容の反映に NQ の再起動が必要となる操作を併せて実施している場合は、必ず再起動を行ってください。

3.7.15　エージェント名設定コマンド（set hn）

[書式]

```
set hn 〈agentname〉
```

[説明]

エージェント名を設定します。

[引数]

引数	説明
〈agentname〉	サイトコンソールに表示するエージェント名を設定します。 引数は、4.3 章の注意事項を参照の上、入力してください。

[実行例]

```
svna> set na stop                    →エージェント停止コマンドの詳細は
+ Command succeeded.                   3.7.24 章参照
svna> set hn isnq30
+ Command succeeded.
+ Command succeeded.
svna> reboot                         → 再起動コマンドの詳細は
+ Command succeeded.                   3.7.13 章参照
```

[注意]

〈agentname〉へ登録可能な文字は、半角英数字、ハイフン(-)、アンダーバー(_)、ドット(.)、小括弧((,))からなる 1 バイト(文字)以上 32 バイト(文字)以下の文字列で、大文字、小文字は区別されません。また、以下に該当する文字列を設定した場合は、SiteManager に登録することができません。

●Windows 予約デバイス名(AUX、CON、NUL、PRN、COM0～COM9、LPT0～LPT9)
●エージェント名の先頭、あるいは末尾がドット(.)である

『isnq30(1)』のように文字列の末尾に小括弧で囲んだ半角数字を記述する場合、SiteManager オンラインヘルプを参照し、サイトコンソールのエージェント設定ダイアログから行ってください。

本コマンドを使用する前に、エージェント停止コマンド（3.7.24 章参照）を使用して NetworkAgent サービスを停止してください。

また､本コマンドを使用してエージェント名を設定した場合は､NQ の再起動が必要となります。

全ての設定を登録後、再起動コマンド（3.7.13 章参照）を実行してください。

3.7.16　初期化コマンド（init all）

［書式］

```
init all
```

［説明］

エージェントのネットワーク設定を工場出荷時の値（初期値）に戻します。ただし、現在は制限事項（5 章参照）があります。工場出荷時の値については 7 章を参照してください。

初期化される項目については「1.7.1 初期化内容」を参照してください。

[実行例]

```
svna> set na stop
+ Command succeeded.
svna> init all
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
svna> reboot
+ Command succeeded.
```

→エージェント停止コマンドの詳細は
3.7.24 章参照

→再起動コマンドの詳細は
3.7.13 章参照

[注意]

本コマンドを使用する前に、エージェント停止コマンド（3.7.24 章参照）を使用して NetworkAgent サービスを停止してください。

本コマンドを使用して工場出荷時に戻した場合は、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（3.7.13 章参照）を実行してください。

3.7.17　シャットダウンコマンド（shutdown、set na shutdown）

[書式]

```
shutdown
または
set na shutdown
```

[説明]

NQ を停止させます。shutdown コマンドと set na shutdown コマンドに動作の差異はありません。
NQ 停止後、再度起動させる場合は電源ケーブルの抜き差しを行ってください。NQ30a、NQ30c、NQ30d の場合は、電源スイッチ押下でも起動可能です。

[実行例]

```
svna> shutdown
```

3.7.18　ネットワークインターフェースのネゴシエーション設定変更コマンド（set ifspeed）

[書式]

・NQ30a、NQ30b、NQ30c の場合

```
set ifspeed { auto | 100FD  | 100HD  | 10FD  | 10HD }
```

・NQ30d の場合

```
set ifspeed { auto | 1000FD | 1000HD | 100FD  | 100HD  | 10FD  | 10HD } [nic]
```

[説明]

NQ のネットワークインターフェースのネゴシエーション設定を変更します。

[引数]

引数	説明
auto	オートネゴシエーションを設定します。工場出荷時は、既定値としてオートネゴシエーションが設定されています。 本引数が指定された場合、オートネゴシエーションのリスタートが実行されます。
1000FD	1000baseT 全二重通信を設定します。
1000HD	1000baseT 半二重通信を設定します。
100FD	100baseTx 全二重通信を設定します。
100HD	100baseTx 半二重通信を設定します。
10FD	10baseT 全二重通信を設定します。
10HD	10baseT 半二重通信を設定します。
nic	設定するインターフェース(eth0 または eth1)を指定します。 省略した場合は『eth0』に設定されます。

[実行例]

```
svna> set ifspeed auto
resetting the transceiver...
+ Command Succeeded.
svna>
```

[注意]

ネットワークインターフェースのネゴシエーション設定を変更する場合、接続先ポートと異なる設定を実施すると、正常に接続できなくなる可能性があります。変更時は、接続先の設定を確認して実施してください。

なお、NQ のネットワークインターフェースのネゴシエーション設定は、NQ の再起動後も設定内容が継続されます。

3.7.19 VLANインターフェース追加コマンド（add vlan）

[書式]

```
add vlan eth0 <vid>
```

[説明]

NQのVLANインターフェースを追加します。NQにVLAN IDを割り当てたVLANインターフェースを作成することで、該当の VLAN ID のタグ付きパケットを収集することができます。VLAN IDには、実際にネットワークで使用しているVLAN IDを設定してください。

[引数]

引数	説明
<vid>	VLAN IDを設定します。VLANインターフェースは、設定されたVLAN IDによって作成されます。 VLAN IDは、10進数で下記の値が設定可能です。 『1』～『4094』

[実行例]

```
svna> add vlan eth0 111
+ Command Succeeded.
svna> set if eth0.111 address 211.10.10.200 mask 255.255.255.0
+ Command Succeeded.        →ネットワークインターフェース設定コマンドの詳細は
                              3.7.7章参照
svna>
svna> add vlan eth0 111     →登録済みのVLAN IDを追加した場合はエラーとなります
 vlan interface already exist
+ Command failed.
svna> reboot
+ Command succeeded.        →VLANインターフェースの設定を反映させるには、
                              再起動コマンド（3.7.13章参照）が必須となります
```

[注意]

追加するVLAN IDが既にNQに登録済みの場合、エラーメッセージが表示され、登録することができません。

なお、本コマンドを実行後、設定を反映させるには、NQの再起動が必要となります。全ての設定を登録後、再起動コマンド（3.7.13章参照）を実行してください。

再起動後、ネットワークインターフェース確認コマンド（3.7.3章参照）で設定を確認してください。

VLANインターフェースはeth0にのみ設定可能です。eth1には設定できません。

MonitoringIfにeth0以外を設定している状態で本コマンドを実行すると、MonitoringIfは自

動的に eth0 に変更されます。
InfoCollectIf に eth0 を設定している状態で本コマンドを実行すると、InfoCollectIf の設定値は自動的に削除されます。

3.7.20 VLAN インターフェース削除コマンド（remove vlan）

[書式]

```
remove vlan 〈nic〉
```

[説明]

NQ の VLAN インターフェースを削除します。VLAN インターフェース単位、または一括での削除が指定可能です。

[引数]

引数	説明
〈*nic*〉	NQ の VLAN インターフェース単位で削除する場合は eth0.〈*vid*〉(※) を設定してください。 全ての VLAN インターフェースを削除する場合、アスタリスク（*）を設定してください。 (※)〈*vid*〉は VLAN インターフェース追加コマンド（3.7.19 章参照）で指定した VLAN ID

[実行例]

```
svna> list if
= Command succeeded.
eth0     inet addr:127.0.0.1 HWaddr 00:00:4c:11:22:33
         Mask:255.0.0.0  Bcast:127.255.255.255
         UP  BROCAST  RUNNING  MULTICAST
eth0.111         inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
         Mask:255.255.255.0  Bcast:192.168.10.255
         Default Gateway:192.168.10.254
         UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> remove vlan eth0.111
+ Command Succeeded.
svna> reboot
+ Command succeeded.
```

→ネットワークインターフェース確認コマンドの詳細は 3.7.3 章参照

→不要な VLAN インターフェースが設定されている場合、削除してください

→VLAN インターフェースの設定を反映させるには、再起動コマンド（3.7.13 章参照）が必須となります

[注意]

本コマンドを実行後、設定を反映させるには、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（3.7.13 章参照）を実行してください。

再起動後、ネットワークインターフェース確認コマンド（3.7.3 章参照）で設定を確認してください。

3.7.21　デフォルトゲートウェイアドレス設定コマンド（set gw）

[書式]

set gw *〈gateway〉*

[説明]

デフォルトゲートウェイアドレスを設定します。

[引数]

引数	説明
〈gateway〉	デフォルトゲートウェイアドレスを設定。 4.1 章を参照して、デフォルトゲートウェイアドレスを入力してください。

[実行例]

```
svna> set gw 10.1.2.254
+ Command Succeeded.
svna> reboot
+ Command succeeded.
```

→デフォルトゲートウェイアドレスの設定を反映させるには、再起動コマンド（3.7.13 章参照）が必須となります

[注意]

本コマンドを実行後、設定を反映させるには、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（3.7.13 章参照）を実行してください。

3.7.22 DNS サーバアドレス削除コマンド（remove ns nameserver）

[書式]

```
remove ns nameserver <server1> [<server2>...]
```

[説明]

DNS サーバの設定を削除します。DNS サーバの IP アドレス単位、または一括での削除が指定可能です。

[引数]

引数	説明
<server1>...	DNS サーバの IP アドレスを指定して削除する場合は、4.1 章の注意事項を参照の上、入力してください。最大 3 個まで設定可能です。複数の DNS サーバアドレスを入力する場合は、引数の間に半角スペースを入れてください。 一括で削除する場合はアスタリスク（*）を入力してください。 なお、引数に IP アドレスとアスタリスクを併用して入力した場合、削除処理が行われません。

[実行例]

```
svna> list ns
= Command succeeded.
nameserver 192.168.0.6
nameserver 192.168.0.7
domain isnq.dom
+ Done.
svna> remove ns nameserver 192.168.0.6 192.168.0.7
+ Command succeeded.
svna> list ns
= Command succeeded.
domain isnq.dom
+ Done.
svna>
```

→DNS サーバ、ドメイン名確認コマンドの詳細は 3.7.4 章参照

→DNS サーバアドレス削除コマンドによって設定値が削除される

3.7.23　エージェント開始コマンド（set na start）

[書式]

```
set na start
```

[説明]

NetworkAgent サービスを開始します。

[実行例]

```
svna> set na start
+ Command succeeded.
svna> set na start
- 501 サービスはすでに開始しています。
svna>
```

→NetworkAgent サービスを多重起動させることはできません。

[注意]

NetworkAgent サービスは、NQ 起動時に開始されます。本コマンドは、エージェント停止コマンド（3.7.24 章参照）を使用して NetworkAgent サービスを停止した時に使用してください。

3.7.24　エージェント停止コマンド（set na stop）

[書式]

```
set na stop
```

[説明]

NetworkAgent サービスを停止します。

[実行例]

```
svna> set na stop
+ Command succeeded.
svna> set na stop
- 501 サービスはすでに停止しています。
svna>
```

→NetworkAgent サービスが停止していれば
エラーとなります。

[注意]

NetworkAgent サービスは、NQ 起動から 1 分以内、あるいはエージェント開始コマンド（3.7.23 章参照）やエージェント再起動コマンド(3.7.25 参照）実行から 30 秒以内は正常に停止できない場合があります。

本コマンドは、前述の時間を目安として一定時間経過後、使用してください。

3.7.25　エージェント再起動コマンド（set na restart）

[書式]

```
set na restart
```

[説明]

NetworkAgent サービスが起動している場合は、一旦停止した後に再起動します。
NetworkAgent サービスが停止している場合は、エージェント開始コマンド（3.7.23 章参照）と同様に NetworkAgent サービスを開始します。

[実行例]

```
svna> set na restart
+ Command succeeded.
svna>
```

[注意]

NetworkAgent サービスは、NQ 起動から 1 分以内、あるいはエージェント開始コマンド（3.7.23 章参照）や本コマンド実行から 30 秒以内は正常に停止できない場合があります。
本コマンドは、前述の時間を目安として一定時間経過後、使用してください。

3.7.26　ドメイン名削除コマンド（remove ns domain）

[書式]

remove ns domain *<domain1>* [*<domain2>*...]

[説明]

ドメイン名の設定を削除します。ドメイン名単位、または一括での削除が指定可能です。

[引数]

引数	説明
<domain1>...	ドメイン名単位で削除する場合は、ドメイン名を指定してください。複数のドメイン名を入力する場合は、引数の間に半角スペースを入れてください。設定可能な文字数の合計は 2,000 文字です。文字数制限には、複数設定時に引数の間に設定する半角スペースも含まれます。 一括で削除する場合はアスタリスク（*）を設定してください。なお、引数にドメイン名とアスタリスクを併用して入力した場合、削除処理が行われません。

[実行例]

```
svna> list ns                          →DNS サーバ、ドメイン名確認コマンドの詳細は
= Command succeeded.                     3.7.4 章参照
nameserver 192.168.0.6
domain isnq.dom
+ Done.
svna> remove ns domain isnq.dom
+ Command succeeded.
svna> list ns
= Command succeeded.                   →ドメイン名削除コマンドによって設定値が
nameserver 192.168.0.6                   削除される
+ Done.
svna>
```

3.7.27　デフォルトゲートウェイアドレス削除コマンド（remove gw）

[書式]

```
remove gw *
```

[説明]

デフォルトゲートウェイアドレスの設定を削除します。

[実行例]

```
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.250.255
        Default Gateway:192.168.250.1
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> remove gw *
+ Command Succeeded.
svna> reboot
+ Command succeeded.
```

→ネットワークインターフェース確認コマンドの詳細は
3.7.3 章参照

→デフォルトゲートウェイアドレスの削除を反映させるには、
再起動コマンド（3.7.13 章参照）が必須となります

3.7.28　文字コード指定コマンド（charset）

［書式］

charset { *sjis* | *eucjp* }

［説明］

NQ の文字コード指定を設定します。「AgentLocation」、「AdminName」、「AdminTelephoneNumber」の各項目（7.5 章の該当項目を参照）で全角文字を入力する前に、telnet(SSH)クライアント PC が使用する文字コードに合わせて変更してください。本コマンドを実行しない場合、文字コードは Shift_JIS として処理されます。

［引数］

引数	説明
sjis	Shift_JIS を設定します。
eucjp	日本語 EUC（EUC-JP）を設定します。

［実行例］

```
svna> charset eucjp
+ Command succeeded.
svna> set na stop          →エージェント停止コマンドの詳細は 3.7.24 章参照
+ Command succeeded.
svna> set na AgentLocation ”○×ビル 4F”
+ Command succeeded.       →エージェント設定コマンドの詳細は 3.7.8 章参照
                             「AgentLocation」の詳細は、7.5 章参照
svna> set na start
+ Command Succeeded.       →エージェント開始コマンドの詳細は 3.7.23 章参照
```

［注意］

NQ に指定された文字コードと、telnet(SSH)クライアント PC が使用する文字コードが異なる場合、全角文字を反映させることができません。telnet(SSH)クライアント PC の設定を確認の上、NQ の文字コード設定を一致させてください。なお、Windows のコマンドプロンプトの場合、既定値で Shift_JIS が設定されています。

3.7.29　ネットワークリスト追加コマンド（add networklist）

[書式]

add networklist <*address*>/<*mask*>

[説明]

監視対象ネットワークリストにネットワークを追加します。共有ネットワーク対応機能の個別指定モード(※)を使用する場合、本コマンドで監視するネットワークを追加します。
現在設定されているネットワークリストを参照する場合､3.7.5章のlist naコマンドを実行し、NetworkListの項目を参照してください。

(※)エージェントの所属するVLANに設定されたサブネットのうち、本コマンドでネットワークリストに追加されたサブネットについて、収集した情報の全てをホスト一覧に表示します。ネットワークリストに追加されていないサブネットについては､MACアドレスのみをホスト一覧に表示します。詳細は、SiteManagerオンラインヘルプの[その他の機能]－[共有ネットワーク対応機能]を参照してください。

[引数]

引数	説明
Address	監視対象とするネットワークのアドレス。
Mask	監視対象ネットワークのサブネットマスク。8～30まで指定可能です。

[実行例]

```
svna> add networklist 192.168.10.0/24
+ Command succeeded.
```

3.7.30　ネットワークリスト削除コマンド（remove networklist）

[書式]

```
remove networklist <address>/<mask>
```

[説明]

ネットワークリスト追加コマンドで追加したネットワークを、監視対象ネットワークリストから削除します。すべてのネットワークを削除する場合は「<*address*>/<*mask*>」の代わりにアスタリスク（*）を指定します。

現在設定されているネットワークリストを参照する場合、3.7.5章のlist naコマンドを実行し、NetworkListの項目を参照してください。

[引数]

引数	説明
address	ネットワークリストから削除するネットワークのアドレス。
mask	監視対象ネットワークのサブネットマスク。8～30まで指定可能です。

[実行例]

```
svna> remove networklist 192.168.10.0/24        →特定のネットワークを監視対象ネットワークリストから削除
+ Command succeeded.
svna> remove networklist *                      →すべての監視対象ネットワークを削除
+ Command succeeded.
```

3.7.31 ハードウェア VLAN ID 変更コマンド（set ifvlanid）

[書式]

```
set ifvlanid nn nn
```

[説明]

NQ30d が内部で使用する VLAN ID を設定します。
VLAN インターフェースとして割り当てる VLAN ID"以外"の値を 2 つ設定してください。
2 つの値の間はスペースで区切って指定してください。
初期状態では『1』と『2』が設定されています。
VLAN インターフェースとして『1』と『2』を使用しない場合は本コマンドによる変更は不要です。

[引数]

引数	説明
nn	内部で使用する VLAN ID を 2 つ指定します。 10 進数で下記の値が設定可能です。 『1』～『4094』

[実行例]

```
svna> set ifvlanid 3000 3001
+ Command succeeded.
svna>
```

→ VLAN ID『3000』と『3001』をハードウェア VLAN ID に設定。

3.7.32 ハードウェア VLAN ID 確認コマンド（list ifvlanid）

[書式]

```
list ifvlanid
```

[説明]

NQ30d が内部で使用する VLAN ID を確認します。
VLAN インターフェースとして割り当てる VLAN ID がハードウェア VLAN ID として使用されているか確認します。
初期状態では『1』と『2』が設定されています。

[実行例]

```
svna> list ifvlanid
3500
3501
+ Command succeeded.
svna>
```

→ ハードウェア VLAN ID として『3500』と『3501』が設定されている。

4　設定値の記述、入力に関する注意事項

4.1　IP アドレス、サブネットマスク、デフォルトゲートウェイアドレス記述時の注意事項

InfoCage 不正接続防止では、各設定に使用する IP アドレス、サブネットマスク、デフォルトゲートウェイアドレスは、IPv4 のみサポートしています。設定値は、10 進数で記述した 4 つのオクテットをドット（.）で繋いだ形式で記述してください。各オクテットとドットの間にスペースを記述する、またはオクテットの先頭桁に 0 を記述する場合、設定が正常に反映されません。

192.168.10.250　→ 正常に反映されます
192.168.△10.250 → 第 3 オクテットにスペース(△)があるため、不正となります
192.168.010.250 → 第 3 オクテットの先頭桁に『0』があるため、不正となります

4.2　文字列記述時の注意事項

4.2.1　認証パスワードに関する注意事項

対象パラメータ		注意事項
設定方法	パラメータ	
設定ファイル	Password →7.1 章参照	設定値に半角スペースが存在する場合、『″aaa bbb″』のように設定値をダブルクォート（″）、あるいはシングルクォート（'）で囲んでください。 ダブルクォート、またはシングルクォートで設定値を囲んでいる際に、設定値にダブルクォート、シングルクォート、円マーク（¥）の半角記号文字が含まれている場合、『″aaa ¥″bbb″』のように該当文字の前に Escape 文字として円マークを記述してください。 文字列を囲むためのダブルクォート、シングルクォート、および Escape 文字は、文字数制限に含まれません。
ネットワーク接続	認証コマンド →3.7.1 章参照 認証パスワード変更コマンド →3.7.2 章参照	

[注意]

通常は、半角スペースを認証パスワードの文字列として認識しません。文字列中に半角スペースがある場合、半角スペースより前の文字列のみ認識します。

■設定ファイルの場合

```
Password:pass wd
```

■コマンド入力の場合

```
svna> pass pass wd
または
svna> set us admin pass wd
```

→ 上記の場合、『pass wd』は『pass』として認識します。

認証パスワードに半角スペースを含める場合、ダブルクォート（"）、またはシングルクォート（'）で文字列を囲んでください。文字列を囲むためのダブルクォート、シングルクォートは、文字数制限に含まれません。

■設定ファイルの場合

```
Password:”pass wd”
```

■コマンド入力の場合

```
svna> pass ”pass wd”
または
svna> set us admin ’pass wd’
```

→ 上記の場合、『”pass wd”』、または『’pass wd’』は『pass wd』として認識します。

文字列の先頭にダブルクォート、またはシングルクォートがある場合、次にダブルクォート、シングルクォートが現れる位置までを認証パスワードと見なします。

■設定ファイルの場合

```
Password:”pass”wd”
```

■コマンド入力の場合

```
svna> pass ”pass”wd”
または
svna> set us admin ’pass’wd’
```

→ 上記の場合、『”pass”wd”』、または『’pass’wd’』は『pass』として認識します。

ダブルクォート、またはシングルクォートで文字列を囲む際に、文字列中に円マーク（¥)、ダブルクォート、シングルクォートを使用する場合は、該当文字の前に Escape 文字として円マークを設定することで認証パスワードと見なします。文字列を囲むためのダブルクォート、および Escape 文字は、文字数制限に含まれません。

■設定ファイルの場合

```
Password:”pass¥”wd”
```

■コマンド入力の場合

```
svna> pass ”pass¥”wd”
または
svna> set us admin ’pass¥”wd’
```

→ 上記の場合、『”pass¥”wd”』、または『’pass¥”wd’』は『pass”wd』として認識します。

ダブルクォート、またはシングルクォートで文字列を囲んだ場合も、1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、および半角記号のみ登録できます。8 バイト(文字)より長い場合、以降の文字列は認識されません。

■設定ファイルの場合

```
Password:”passwd12345”
```

■コマンド入力の場合

```
svna> pass ”passwd12345”
または
svna> set us admin ‘passwd12345’
```

→ 上記の場合、『”passwd12345”』、または『’passwd12345’』は『passwd12』として認識します。

ダブルクォート、シングルクォートが文字列の先頭に設定されているが、以降の文字列にダブルクォート、シングルクォートが含まれていない場合、あるいは文字列の先頭以降にダブルクォート、シングルクォートが設定されている場合は、ダブルクォート、シングルクォートを認証パスワードの文字列の一部として設定します。

■設定ファイルの場合

```
Password:”passwd
```

■コマンド入力の場合

```
svna> pass pass”wd”
または
svna> set us admin pass’wd’
```

→ 上記の場合、『”passwd』は『”passwd』、『pass”wd”』は『pass”wd”』、『pass’wd’』は『pass’wd’』として認識します。

4.2.2　認証パスワード以外の文字列に関する注意事項

対象パラメータ		注意事項
設定方法	パラメータ	
設定ファイル	AgentLocation AdminName AdminTelephoneNumber →7.5 章参照	文字列中に円マーク（¥）、ダブルクォート（″）、シングルクォート（'）の半角記号文字が存在する場合、『aaa ¥″bb』のように該当文字の前にEscape 文字として円マークを記述してください。Escape 文字は、文字数制限に含まれません。 なお、設定値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。
ネットワーク接続	AgentLocation AdminName AdminTelephoneNumber →7.5 章参照	文字列中に半角スペースが存在する場合、ダブルクォート（″）、またはシングルクォート（'）で文字列を囲んでください。ダブルクォート、またはシングルクォートで文字列を囲んでいる際に、文字列中に円マーク（¥）、ダブルクォート（″）、シングルクォート（'）の半角記号文字が存在する場合、『″aaa ¥″bb″』のように該当文字の前にEscape 文字として円マークを記述してください。Escape 文字は、文字数制限に含まれません。 なお、設定値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。

4.3　エージェント名記述時の注意事項

AgentName（エージェント名）は、このエージェントが登録されている SiteManager が管理する他のエージェントと重複しないように設定してください。SiteManager に既に同名のエージェントが登録されている場合は、「AgentName(1)」のような括弧数字付きの名前となりますので、別の名前に変更してください。

5　注意・制限事項

・ NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合は、電源スイッチを押下してください。機器を停止させる場合は、以下のいずれかを実行してください。

●シャットダウンコマンド（3.7.17 章参照）を実行する（推奨）
●電源スイッチを 5 秒以上押し続ける
●電源ケーブルを抜く

・ NQ30b は、電源スイッチがありません。電源ケーブルの接続により、自動起動します。機器を停止させる場合は、以下のいずれかを実行してください。

●シャットダウンコマンド（3.7.17 章参照）を実行する（推奨）
●電源ケーブルを抜く

・ NQ30c、NQ30d を停止させる場合は、以下のいずれかを実行してください。

●シャットダウンコマンド（3.7.17 参照）を実行する（推奨）
●電源スイッチを 5 秒以上押し続ける（推奨）
●電源ケーブルを抜く(※)
(※)上記 2 つの方法で停止できない場合のみ実行してください。

・ 初期化コマンド(3.7.16 章参照)では一部のネットワーク設定が工場出荷状態に戻りません。全てのネットワーク設定を変更する場合、下記の項目を参照し、設定値の変更、または 1.7 章を参照して初期化を行ってください。

項目	使用コマンド	参照	初期設定値
認証パスワード	set us	3.7.2 章	admin
DNS サーバアドレス	remove ns nameserver	3.7.22 章	なし
ドメイン名	set ns domain	3.7.10 章	isnq.dom
VLAN インターフェース	remove vlan	3.7.20 章	なし

・ NQ では、NetBEUI プロトコルのパケットを解析できません。そのため、SiteManager のホスト一覧上で、NetBEUI フラグのチェックがつきません。また、NetBEUI しか利用しない端末の検知、防止ができません。

・ USB メモリを使用したセットアップ方法によってタグ VLAN 環境から非タグ VLAN 環境での使用に切り替える場合、NQ の電源再起動などで設定ファイルを認識させる前に、ネットワークインターフェース設定コマンド（3.7.7 章参照）を使用し、『eth0』(NQ30d の場合は『eth0』または『eth1』)の IP アドレスを設定する必要があります。前述の手順を行わずに設定ファイルを認識させた場合、NQ 起動後にもう一度 NQ の再起動が必要となることがあります。

・ V3.3 未満のバージョンからバージョンアップした場合、list if コマンドで表示される、Bcast の値が、Mask から求められる値と異なる値で表示されます。NQ はこの値を用いて通信することはありませんので、そのまま利用していただいて問題ありません。また、ネットワークマスクを再度設定すれば、不正な表示は解消されます。

・ V3.9 以降、「JamMacAddressMode」、「DisableBroadCastJamArp」パラメータの既定値が変更（0 から 1 へ変更）となりました。
3.8 以前のバージョンから 3.9 以降にバージョンアップする場合、上記パラメータは自動的に既定値である『1』となります。
3.9 から 3.9 以降にバージョンアップする場合、設定値は変更されません。

・ 【IDS への影響】InfoCollectIf に指定した NIC はプロミスキャスモードで利用しますので、プロミスキャスモードの NIC を探知する IDS（侵入検出システム）で検出される可能性があります。

・ 【NQ30d のインターフェース設定の組み合わせ】NQ30d のインターフェースの設定には下記の制限があります。

✓ VLAN インターフェースを設定できるのは eth0 のみ。
✓ eth0 に VLAN インターフェースを設定した場合、eth1 をデータ収集、不正接続防止を実行するインターフェース(MonitoringIf)に指定することはできない。

上記の制限により、設定可能なインターフェースの組み合わせは下記のようになります。

eth1 / eth0	タグ VLAN	非タグ VLAN	データ収集専用	使用しない
タグ VLAN	×	×	○	○
非タグ VLAN	×	○	○	○
データ収集専用	×	○	×	×
使用しない	×	○	×	×

・ 【V5.2 未満の環境で NQ30d を利用する場合の制限事項】V5.2 未満の SiteManager に NQ30d を登録して利用する場合、2 ポートによる監視を行うことはできません。

6　トラブルシューティング

6.1　NQ へのネットワーク接続時に文字が正常に表示されない

telnet を介して NQ に接続した時に、出力文字が正常に表示されない、入力文字が表示できない場合、以下を確認してください。

■NQ に対して単一のネットワーク接続を行っている場合

NQ に対して単一のネットワーク接続を行った際に文字が正常に表示されない場合、ターミナルソフトのローカルエコー設定、改行文字の変換設定が関与している可能性があります。以下は、コマンドプロンプト、および Tera Term での設定方法となります。他のターミナルソフトを使用する場合は、Tera Term の設定方法を参照し、設定内容を確認してください。

◆ コマンドプロンプトの場合

コマンドプロンプトの場合、ローカルエコー設定が関与している可能性があります。以下の手順で telnet クライアント PC の設定を確認／変更してください。

① コマンドプロンプトを起動し、telnet コマンドを入力します。

```
C:¥> telnet
Microsoft (R) Windows 2000 (TM) Version 5.00 (Build 2195)
Microsoft Telnet クライアントへようこそ
Telnet Client Build 5.00.99206.1

エスケープ文字は 'CTRL+]' です

Microsoft Telnet>
```

引数は設定しない

② display コマンドを使用し、設定を確認します。

```
Microsoft Telnet> display
エスケープ文字は 'CTRL+]' です
自動認証 (NTLM 認証) を使う
ローカルエコーを使わない
CR と LF を送信します
使用する端末の種類をネゴシエートする
```

優先する端末の種類は ANSI です Microsoft Telnet>	設定確認を行う

③ 入力文字が表示されていない場合は、ローカルエコーをオンにします。

Microsoft Telnet> set local_echo Microsoft Telnet> display エスケープ文字は 'CTRL+]' です 自動認証 (NTLM 認証) を使う ローカルエコーを使う CR と LF を送信します 使用する端末の種類をネゴシエートする 優先する端末の種類は ANSI です Microsoft Telnet>	ローカルエコーを設定 設定確認を行う

※ 上記の設定を行った場合、PC の再起動後も設定が保存されています。

※ ローカルエコーの設定を戻す場合は、以下のコマンドを入力してください。

```
Microsoft Telnet> unset local_echo
```

④ telnet を終了します。

```
Microsoft Telnet> quit
```

◆ Tera Term の場合

Tera Term の場合、ローカルエコー設定、改行文字の変換設定が関与している可能性があります。以下の手順で telnet クライアント PC の設定を確認／変更してください。

[Setup] → [Terminal]

Receive	: CR	受信改行文字の変換設定
Transmit	: CR+LF	送信改行文字の変換設定
Local echo	: ON	ローカルエコー設定
Kanji(receive)	: SJIS	受信文字コード設定 (EUC でも可)
Kanji(transmit)	: SJIS	送信文字コード設定

6.2 USB メモリを使用したセットアップに失敗する

USB メモリを使用したセットアップを行っても SiteManager-NQ 間の通信が正常に行えない場合、NQ が USB メモリを認識できていない、あるいは設定ファイルに記載された内容が間違っている可能性があります。USB メモリの認識状態、および設定エラーを判断するには、以下を確認してください。

NQ 起動時に USB メモリを認識した場合は、USB メモリのルートフォルダに以下のファイルが作成されます。

［ファイル名］

svconflog.txt （全て半角小文字）

［ファイル内詳細］

YYYY/MM/DD hh:mm:ss JST: mount ok

［内容］

引数	説明
YYYY/MM/DD	svconflog.txt を作成した日付
hh:mm:ss	svconflog.txt を作成した時刻
JST:	日本時間であることを示す（固定）
mount ok	認識できたことを示す（固定）

［注意］

USB メモリ内に同一ファイル名があった場合は既存ファイルを削除し、新規作成します。

本ファイルが存在しない場合、もしくはファイル内の日付や時刻が古い場合、NQ と USB メモリの相性によって USB メモリが認識できていない可能性があります。また、NQ30c、NQ30d は USB2.0 の USB メモリのみ使用できます。2.2.1 章のセットアップ手順を実行しても認識できない場合は、USB メモリを変更して実施してください。

USB メモリの設定ファイル読み込み時にエラーが発生した場合、本ファイルに以下のエラーログを出力します。エラーログに出力される内容は、設定ファイルに記載した内容を設定するコマンドと、その実行結果（コマンド入力時の注意・制限事項参照）です。エラーログ出力時は、2.2.3 章、2.2.4 章の設定例、あるいは 7.1 章の「Password」の項目を参照し、設定ファイルの確認を行ってください。

［認証パスワード未記入］

YYYY/MM/DD hh:mm:ss JST: no password

[認証パスワードによる認証失敗]

```
YYYY/MM/DD hh:mm:ss JST: password error
```

[不正なパラメータ指定による設定失敗]

例：以下のような設定ファイルを用いて設定した場合：(DisableWatchMyNetwork:0 が不正なパラメータ)

```
password:admin
DisableWatchMyNetwork:0
DisableOtherNetworkHostPrevent:1
```

svconflog.txt に以下の内容を出力します。

```
2009/09/08 00:30:09 JST: mount ok
+ Welcome to SvNaConsole.
set na DisableWatchMyNetwork 0
- 503 invalid data.
set na DisableOtherNetworkHostPrevent 1
+ Command succeeded.
+ Goodbye.
```

6.3　NQ にネットワーク設定が正常に反映されたか確認できない

2 章を参照して NQ の設定を行った場合、SiteManager インストール PC と正常に通信可能で、SiteManager サービスが起動していれば、SiteManager インストール PC 上のサイトコンソールにエージェントアイコンが表示されます。
サイトコンソールに表示されない場合や SiteManager サービスが起動していない場合、下記の例を参照して NQ の設定状態を確認してください。

※ 以下の手順は、NQ に設定されている IP アドレスを把握していることを前提としています。
NQ の IP アドレスが分からない場合はネットワーク接続を行うことができないため、2.2 章を参照して USB メモリによる設定変更を行ってください。

① NQ を起動する

NQ 筐体へ、ネットワークに接続された LAN ケーブル、電源ケーブルを接続してください。
接続完了後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。
但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下して起動してください。起動状態は、電源ランプの点灯状態から確認してください。

② telnet クライアント PC を用意する

NQ へ telnet を介してネットワーク接続を行う PC を用意し、ping コマンドなどを使用して NQ との通信状態を確認してください。

［実行例］

```
C:¥> ping 192.168.250.250 (※)
```

（※）斜体部分は NQ に設定されている IP アドレス、あるいは IP アドレスに割り当てられているホスト名を設定してください。

NQ と通信できない場合、NQ に設定されているネットワークと接続できるよう、telnet クライアント PC のネットワーク設定を変更してください。

③ NQ にネットワーク接続する

3.2 章を参照し、telnet クライアント PC から NQ へネットワーク接続を行ってください。

④ 各種設定を確認する

NQ へ接続後、下記の例を参考に設定状態を確認してください。

[実行例]

```
svna> pass admin          →認証コマンドの詳細は 3.7.1 章参照
```

```
+ Welcome to SvNaConsole.
svna> list if                                    →ネットワークインターフェース確認
                                                   コマンドの詳細は 3.7.3 章参照
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.250.255
        Default Gateway:192.168.250.1
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> list ns                                    →DNS ネームサーバ、ドメイン名確認
                                                   コマンドの詳細は、3.7.4 章参照
= Command succeeded.
nameserver 192.168.250.6
nameserver 192.168.250.7
domain isnq.dom
+ Done.
svna> list na                                    →エージェント設定確認コマンドの詳細は
                                                   3.7.5 章参照、エージェント設定の
                                                   各属性の詳細は 7 章参照
= Command succeeded.
AdminMailAddress: admin@securevisor.dom
...
+ Done.
svna>
```

6.4　SiteManager インストール PC を不正接続防止してしまった

SiteManager インストール PC を不正接続防止した場合は、SiteManager-NQ 間の通信が正常に行えなくなり、各種操作が行えなくなります。不正接続防止機能を強制的に停止させたい場合は、下記の手順を実施してください。

① NQ を停止する

5 章の停止手順にしたがって NQ を停止してください。

② SiteManager サービスを停止する

NQ の接続先に設定されている SiteManager サービスを停止してください。サービスの停止手順は以下の通りです。

Windows の[スタート]ボタン → コントロール パネル → 管理ツール → サービス → [InfoCage 不正接続防止 SiteManager]を選択し、サービスを停止する。

③ SiteManager の管理するエージェント設定を変更する

SiteManager が保持している NQ の属性ファイルを編集し、不正接続防止機能が無効となるよう設定します。

NQ の属性ファイルは下記の場所にあります。

C:¥Program Files¥SecureVisor¥SiteManager¥Data¥AgentList¥***xxxx***¥attribute.dat ※SiteManager を "C:¥Program Files¥SecureVisor" にインストールした場合

※ ***xxxx*** は、NQ のエージェント名を示します。

attribute.dat ファイルをメモ帳などのエディタで開き、不正接続防止機能（JamStatus）の属性を以下のように変更してください。

JamStatus: On

↓

JamStatus: Off

※ SiteManager の属性ファイルは、文字コードを Shift-JIS、改行コードを<CR>+<LF>で作成されています。使用するテキストエディタの設定を確認の上、編集、保存を行ってください。なお、Windows 標準のメモ帳は前述の設定を満たしているため、問題なく使用できます。

④ SiteManager のサービスを開始する

NQ の接続先に設定されている SiteManager サービスを開始してください。サービスの開始手順は以下の通りです。

Windows の[スタート]ボタン → コントロール パネル → 管理ツール → サービス → [SecureVisor SiteManager]を選択し、サービスを開始する。

⑤ NQ の設定ファイルを作成する

NQ に設定されている不正接続防止機能を停止させるため、2.2.2 章、および 2.2.3 章を参照し、USB メモリのルートフォルダに設定ファイルを作成します。

［ファイル名］

svconfig.txt （全て半角小文字）

［設定内容］

Password:admin	→ 認証パスワードを記述してください。
JamStatus:Off	→ 不正接続防止機能を Off に設定します。

⑥ NQ を起動する

NQ 筐体へ、設定ファイルを保存した USB メモリ、ネットワークに接続された LAN ケーブル、電源ケーブルが接続されていることを確認してください。接続確認後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。

但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

上記手順実行後、NQ は起動時に SiteManager へ接続することで設定内容が同期され、不正接続防止機能が無効となります。

不正接続防止機能を再度有効とする場合、ホスト一覧を使用し、ネットワークへの接続を許可する機器が全て接続許可状態になっていることを確認してから設定してください。

6.5　現在の NQ のバージョンが分からない

NQ のバージョンは、SiteManager インストール PC から確認することができます。確認手順は、下記の通りです。

■NQ 単位で確認する場合

1. SiteManager インストール PC で、サイトコンソールを起動します。サイトコンソールの起動方法は、以下を参照してください。

Windows の[スタート]ボタン → (すべての)プログラム → SecureVisor →サイトコンソール

2. サイトコンソールでエージェントのプロパティを選択し、エージェント設定ダイアログを起動させ、[バージョン情報]を確認してください。エージェントのプロパティ選択方法は、以下のいずれかを参照してください。

・バージョン確認対象の NQ のエージェントアイコン上で、マウスの左ボタンをクリックして選択する。選択後は、以下のいずれかを実行してください。

●メニューバーより[ファイル(F)] → [エージェントのプロパティ(P)...]を選択する

●ツールバーの左から 2 番目の[プロパティ]ボタンをクリックする

●エージェントアイコン上でマウスの左ボタンをダブルクリックする

●エージェントアイコン上で、マウスの右ボタンをクリックしてポップアップメニューを表示させ、[プロパティ(P)...]を選択する。

■複数の NQ をまとめて確認する場合

（１）サイトコンソールのメインダイアログから確認する

1. SiteManager インストール PC で、サイトコンソールを起動します。サイトコンソールの起動方法は、上記の「■NQ 単位で確認する場合」の 1. を参照してください。
2. サイトコンソールのツールバーで[表示形式の変更]ボタンをクリックする。エージェントの表示を詳細形式に切り替えると、SiteManager が管理しているエージェントの IP アドレス、バージョン情報などを一括で確認することができます。

（２）サイトコンソールのエージェント情報一覧ダイアログから確認する

1. SiteManager インストール PC で、サイトコンソールを起動します。サイトコンソールの起動方法は、上記の「■NQ 単位で確認する場合」の 1. を参照してください。
2. サイトコンソールのメニューバーより[ツール(T)] → [エージェント情報一覧(T)...]を選択する。エージェント情報一覧ダイアログが表示され、SiteManager が管理しているエージェントの IP アドレス、バージョン情報などを一括で確認することができます。

6.6　タグ VLAN 環境で NQ が使用できない

NQ の「タグ VLAN 対応機能」を使用してトランクポートに接続しても、スイッチの設定によっては正常に動作しないことがあります。例として、Cisco Catalyst シリーズのスイッチで構築したタグ VLAN 環境で NQ を使用する場合の注意点を以下に示します。

■トランクポートにネイティブ VLAN が含まれないこと

Cisco Catalyst シリーズでは、IEEE802.1Q トランクにおいてネイティブ VLAN（Catalyst3550 では VLAN 1 が既定）を定義しています。ネイティブ VLAN は、トランクポートに設定してもタグ付けされずに転送するため、NQ にネイティブ VLAN の VLAN ID を収集対象として追加しても、タグ付きパケットでないため収集できません。

また、トランクポートにネイティブ VLAN が含まれている場合、トランクポートに接続した機器のネイティブ VLAN を一致させる必要があるため、設定によっては NQ を接続した際にエラーとなる場合があります。

Cisco Catalyst シリーズでトランクポートを設定する際は、ネイティブ VLAN を外して利用してください。

上記以外にも、使用されているスイッチ固有の設定により、正常に動作しない場合があります。使用されるスイッチのマニュアルを参照の上、適切な設定を実施して利用してください。

7　NQ のパラメータ詳細

パラメータ（属性名）は、設定必須パラメータ、設定可能パラメータがあります。また、「タグ VLAN 対応機能」の設定の有無及び NQ の種類によって、使用できるパラメータが異なります。以降の説明を参照の上、必要に応じて各パラメータを設定してください。

コマンドラインインターフェースによるパラメータ値変更を行う場合、エージェント停止コマンド（3.7.24 章）実行後に実施してください。設定後はエージェント開始コマンド（3.7.23 章）、あるいは再起動コマンド（3.7.13 章）を実施してください。

※ 設定情報を確認するには、エージェント設定確認コマンド（3.7.5 章）を参照してください。
※ VLAN インターフェースの設定状態によっては、エージェント設定確認コマンドを実行した際に、「IpAddress」、「CollectIpAddress」、「NetworkMask」、「NetworkAddress」、「NetworkList」が表示されません。
※ 値が未設定のパラメータは、エージェント設定確認コマンドを実行した際に表示されません。
※ 設定情報を変更するには、エージェント設定コマンド（3.7.8 章）、および本章の各パラメータに対する説明欄の入力例を参照してください。

7.1　設定必須パラメータ

設定必須パラメータを以下に示します。

パラメータ（属性名）	説明	既定値	備考
AgentName	NQ のエージェント名を設定します。設定値は、1 個のみ記述可能です。 設定値を変更する際は、4.3 章の注意事項を参照の上入力してください。 設定値に使用可能な文字は、半角英数字、ハイフン（-）、アンダーバー（_）、ドット（.）小括弧（(,)）からなる 1 バイト(文字)以上 32 バイト(文字)以下の文字列で、大文	isnq30	

	字、小文字は区別されません。また、以下に該当する文字列を設定した場合は、SiteManager に登録することができません。 ●Windows 予約デバイス名（AUX、CON、NUL、PRN、COM0～COM9、LPT0～LPT9） ●エージェント名の先頭、あるいは末尾がドット（.）である 『isnq30(1)』のように文字列の末尾に小括弧で囲んだ半角数字を記述する場合、SiteManager オンラインヘルプを参照し、サイトコンソールのエージェント設定ダイアログから行ってください。 ■記述例（USB メモリ） AgentName:isnq30 ■入力例（コマンド） 3.7.15 エージェント名設定コマンド（set hn）		
IpAddress	ネットワークインターフェースが使用する IP アドレスを設定します。設定値は、1 個のみ記述可能です。 VLAN インターフェースが設定されている場合、本属性は非表示となります。 設定値は、4.1 章の注意事項を参照の上、記述してください。設定可能な範囲は、『1.0.0.1』～『223.255.255.254』までとなります。 NQ をタグ VLAN 環境に設置する場合、本パラメータと VLAN インターフェースに設定する IP アドレスの重複を避けるため、『127.0.0.1』を設定してください。 NQ30d の場合は設定するインターフェースを指定します。USB メモリで設定する場合は省略可能で、省略した場合は『eth0』に設定されます。 NQ30d の場合、『eth0』と『eth1』には異なるネットワークアドレスとなる IP アドレスとサブネットマスクの組み合わせを設定してください。同じネットワークアドレスにな	eth0: 192.168.250.250 eth1: 192.168.251.251	

	る値を設定すると、エラーとなります。 ■記述例（USB メモリ） IpAddress:192.168.250.250 ■記述例（USB メモリ）※NQ30d のみ IpAddress:192.168.250.250 eth1 ■入力例（コマンド） 3.7.7 ネットワークインターフェース設定コマンド（set if）		
ManagerAddress	NQ の管理/操作を行う SiteManager インストール PC の IP アドレスを設定します。設定値は、1 個のみ記述可能です。 設定値は、4.1 章の注意事項を参照の上、記述してください。 ■記述例（USB メモリ） ManagerAddress:192.168.250.251 ■入力例（コマンド） 3.7.14 マネージャ設定コマンド（set sm）	192.168.250.251	
Password	USB メモリを使用したセットアップ実施時に認証を行うための認証パスワードとなります。認証パスワードはネットワーク接続で使用する認証パスワードと共通です。値は、1 個のみ記述可能です。 なお、認証パスワードはセキュリティ対策として既定値から変更することを推奨します。 認証パスワードの変更方法は、AdminPassword パラメータを参照してください。	admin	

	本パラメータは必ず設定ファイルの 1 行目に記述してください。1 行目以外の行に記載された場合は認証エラーとなり各パラメータが反映されません。 ■記述例（USB メモリ） Password:admin ■入力例（コマンド） 3.7.1 認証コマンド（pass）		

7.2　設定不可パラメータ

NQ のコマンドからの設定不可パラメータを以下に示します。NewHostStatus は DomainManager および SiteManager から設定をするパラメータです。
CollectIpAddress、NetworkAddress はネットワークインターフェースの設定から自動で設定されるパラメータです。

パラメータ（属性名）	説明	既定値	備考
CollectIpAddress	SiteManager との通信に使用する IP アドレスです。 VLAN インターフェースが設定されている場合、本属性は非表示となります。 属性値は、ネットワークインターフェース設定コマンドで設定した内容となります。	192.168.250.250	
NewHostStatus	NQ が新規に発見したホストをどの状態(色)で SiteManager に登録するかを示す値です。 0：新規ホストの状態(色)を「青」として登録します。 1：新規ホストの状態(色)を「黄」として登録します。 2：新規ホストの状態(色)を「赤」として登録します。	0	
NetworkAddress	ネットワークインターフェースに設定されているネットワークアドレスです。 VLAN インターフェースが設定されている場合、本属性は非表示となります。 属性値は、ネットワークインターフェース設定コマンドで設定した内容となります。	192.168.250.0	
VlanCollectOfPacket	VLAN グループ管理における各 VLAN のデータ収集設定状態です。 各 VLAN 設定状態は”VLANID/設定値”の形式で設定されます。 ■設定値の例		

	100/Off 200/On		
VlanDhcpScope	VLAN グループ管理における各 VLAN の DHCP スコープ設定範囲です。 各 VLAN 設定状態は”VLANID/設定値”の形式で設定されます。 ■設定値の例 100/192.168.1.1-192.168.1.10 100/192.168.1.101-192.168.1.110		
VlanJamStatus	VLAN グループ管理における各 VLAN の不正接続防止設定状態です。 各 VLAN 設定状態は”VLANID/設定値”の形式で設定されます。 ■設定値の例 100/Off 200/On		
VlanNewHostStatus	VLAN グループ管理における各 VLAN で発見したホストをどの状態(色)で SiteManager に通知するかを示す値です。 0：新規ホストの状態(色)を「青」として登録します。 1：新規ホストの状態(色)を「黄」として登録します。 2：新規ホストの状態(色)を「赤」として登録します 各 VLAN 設定状態は”VLANID/設定値”の形式で設定されます。 ■設定値の例 100/0 200/2		

7.3　非タグ VLAN 環境の設定必須パラメータ

非タグ VLAN 環境の設定必須パラメータを以下に示します。

パラメータ	説明	既定値	備考
NetworkMask	ネットワークのサブネットマスクを設定します。設定値は、1 個のみ記述可能です。 VLAN インターフェースが設定されている場合、本属性は非表示となります。 設定値は、4.1 章の注意事項を参照の上、記述してください。設定可能な範囲は、『255.0.0.0』の 8 ビットから『255.255.255.252』の 30 ビットまでとなります。 NQ30d の場合は設定するインターフェースを指定します。USB メモリで設定する場合は省略可能で、省略した場合は『eth0』に設定されます。 NQ30d の場合、『eth0』と『eth1』には異なるネットワークアドレスとなる IP アドレスとサブネットマスクの組み合わせを設定してください。同じネットワークアドレスになる値を設定すると、エラーとなります。 ■記述例（USB メモリ） NetworkMask:255.255.255.0 ■記述例（USB メモリ）※NQ30d のみ NetworkMask:255.255.255.0 eth1 ■入力例（コマンド） 3.7.7 ネットワークインターフェース設定コマンド（set if）	255.255.255.0	

7.4　タグ VLAN 環境の設定必須パラメータ

タグ VLAN 環境の設定必須パラメータを以下に示します。

パラメータ	説明	既定値	備考
Vlan1～Vlan64	「タグ VLAN 対応機能」で使用する VLAN インターフェースの設定を追加/更新します。VLAN インターフェースには、各 VLAN 内で使用可能な IP アドレスを割り当てる必要があります。各パラメータに対して、設定値を 1 組のみ記述可能です。Vlan1～Vlan8（NQ30c の場合は Vlan1～Vlan16、NQ30d の場合は Vlan1～Vlan32）のパラメータを、必要数に応じて使用してください。NQ を冗長化構成で使用する場合は、Vlan1～Vlan16（NQ30c の場合は Vlan1～Vlan32、NQ30d の場合は Vlan1～Vlan64）のパラメータを設定可能です。 設定値は、以下の定義に従って順に記述してください。各設定値は、半角スペースで繋いだ形式で記述してください。全ての設定値が記述されていない場合、設定が反映されません。 ●IP アドレス → 4.1 章の注意事項を参照し、『1.0.0.1』～『223.255.255.254』の範囲で設定 ●サブネットマスクの有効ビット数 → 10 進数で『8』～『30』の範囲で設定 ●VLAN ID → 10 進数で『1』～『4094』の範囲で設定 設定時は、以下の点に注意してください。 ●VLAN インターフェースの設定数は、最大で 8 個（NQ30c の場合は 16 個、NQ30d の場合は 32 個）までのサポートとなります。 ●パラメータは、1 行目から順番に読み込まれます。VLAN ID が重複したパラメータが存在する場合、後に記述された内容に上書きされます。	未設定	

	●NQ に同一 VLAN ID が設定済の場合、設定ファイルの内容に更新します。 ●MonitoringIf に eth0 以外を設定している状態で VLAN インターフェースを設定すると、MonitoringIf は自動的に eth0 に変更されます。 ●InfoCollectIf に eth0 を設定している状態で VLAN インターフェースを設定すると、InfoCollectIf の設定値は自動的に削除されます。 ■記述例（USB メモリ） Vlan1:192.168.250.251 24 1001 Vlan2:172.16.180.15 23 2001 ■入力例（コマンド） 3.7.19VLAN インターフェース追加コマンド（add vlan） 3.7.7 ネットワークインターフェース設定コマンド（set if）		

7.5　各環境共通の設定可能パラメータ

非タグ VLAN 環境、タグ VLAN 環境共通の設定可能パラメータを以下に示します。

※「説明」に記載のないパラメータは集中(小規模)管理モードおよび分散管理モードで利用可能です。

パラメータ	説明	既定値	備考
ActiveNic	「NQ 冗長化機能」利用時に設定します。管理対象の VLAN ID を指定します。最大 8 個(NQ30c の場合は 16 個、NQ30d の場合は 32 個）まで設定可能です。設定値が指定されていない場合、管理範囲は VLAN インターフェース追加コマンドで設定しているすべての VLAN となります。「NQ 冗長化機能」の詳細は、「InfoCage 不正接続防止 集中管理運用マニュアル」を参照してください。 集中(小規模)管理モードのみ利用可能です。 ■記述例（USB メモリ） ◆設定時 ActiveNic:eth0.2,eth0.3,eth0.4,eth0.5,eth0.6,eth0.7 ◆削除時 ActiveNic:"" ■入力例（コマンド） ◆設定時 set na ActiveNic eth0.2,eth0.3,eth0.4,eth0.5,eth0.6,eth0.7 ◆削除時 set na ActiveNic ""	未設定	

AdminMailAddress	NQ の管理者メールアドレスを設定します。本パラメータを設定した場合、該当の NQ に関するアラートが発生し、メール送信が行われる際に、設定値がメール送信先として追加されます。設定値は、複数記述可能です。 設定値に使用可能な文字は、半角英数字、ハイフン（-）、アンダーバー（_）、ドット（.）からなる 0 バイト以上 1024 バイト以下の文字列で、文字列中にアットマーク（@）をひとつ含み、アットマークの前後に 1 文字以上あるものを、正しいメールアドレスとして扱っています。また、カンマ（,）で区切ることで複数指定可能ですが、カンマの前後に空白は入力できません。なお、設定値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例（USB メモリ） ◆設定時 AdminMailAddress:user@securevisor.dom,admin@securevisor.dom ◆削除時 AdminMailAddress:″″ ■入力例（コマンド） ◆設定時 set na AdminMailAddress user@securevisor.dom,admin@securevisor.dom ◆削除時 set na AdminMailAddress ″″	未設定	
AdminName	NQ の管理者氏名を設定します。本パラメータを設定した場合、SiteManager のアラート通知機能を使用する際に、メール送信、コマンド起動（SNMP トラップ送信機能含む）の通知内容に管理者氏名を含めることができます。設定値は、1 個のみ記述可能です。	未設定	

	設定値に使用可能な文字は、半角英数字、半角記号文字、2バイト文字、半角スペースからなる0バイト以上40バイト以下の文字列で、大文字、小文字は区別されます。4.2.2章の注意事項を参照の上、記述してください。 コマンドにより設定する場合、telnetクライアントの文字コードに合わせて、文字コード指定コマンド（3.7.28章参照）を使用してください。 ■記述例（USBメモリ） ◆設定時 AdminName:ネットワーク管理者 ◆削除時 AdminName:"" ■入力例（コマンド） ◆設定時 set na AdminName ネットワーク管理者 ◆削除時 set na AdminName ""		
AdminPassword	認証パスワードを変更します。認証パスワードは、ネットワーク接続で使用する認証パスワードと共通です。設定値は、1個のみ記述可能です。 設定値に使用可能な文字は、1バイト(文字)以上8バイト(文字)以下の半角英数字、半角記号、半角スペースからなる文字列です。大文字、小文字を区別します。8バイト(文字)より長い場合は、以降の文字列は認識されません。4.2.1章の注意事項を参照の上、記述してください。 ■記述例（USBメモリ）	ー	

	AdminPassword:passwd ■入力例（コマンド） 3.7.2 認証パスワード変更コマンド（set us）		
AdminTelephoneNumber	NQ の管理者電話番号を設定します。本パラメータを設定した場合、SiteManager のアラート通知機能を使用する際に、メール送信、コマンド起動（SNMP トラップ送信機能含む）の通知内容に管理者電話番号を含めることができます。設定値は、1 個のみ記述可能です。設定値に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 100 バイト以下の文字列で、大文字、小文字は区別されます。4.2.2 章の注意事項を参照の上、記述してください。 コマンドにより設定する場合、telnet クライアントの文字コードに合わせて、文字コード指定コマンド（3.7.28 章参照）を使用してください。 ■記述例（USB メモリ） ◆設定時 AdminTelephoneNumber:000-111-2222 ◆削除時 AdminTelephoneNumber:"" ■入力例（コマンド） ◆設定時 set na AdminTelephoneNumber 000-111-2222 ◆削除時 set na AdminTelephoneNumber ""	未設定	
AgentLocation	NQ の設置場所を設定します。本パラメータを設定した場合、SiteManager のアラート通知機能を使用する際に、メール送信、コマンド起動（SNMP トラップ送信機能含む）の通	未設定	

	知内容に設置場所を含めることができます。設定値は、1 個のみ記述可能です。 設定値に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 255 バイト以下の文字列で、大文字、小文字は区別されます。4.2.2 章の注意事項を参照の上、記述してください。 コマンドにより設定する場合、telnet クライアントの文字コードに合わせて、文字コード指定コマンド（3.7.28 章参照）を使用してください。 ■記述例（USB メモリ） ◆設定時 AgentLocation:〇×ビル 4F ◆削除時 AgentLocation:"" ■入力例（コマンド） ◆設定時 set na AgentLocation "〇×ビル 4F" ◆削除時 set na AgentLocation ""		
AgentPort	NQ が SiteManager からの通信を受信するポート番号を設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『1』～『65535』の範囲で記述してください。但し、telnet を介したネットワーク接続の使用ポートである『23496』は設定しないでください。 本パラメータは Port パラメータとして表示します。	23491	

	■記述例（USB メモリ） AgentPort:23491 ■入力例（コマンド） Port パラメータを参照してください。		
AutoRecoveryFromPrev	「防止ホスト自動復帰機能」を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。 「防止ホスト自動復帰機能」の詳細は、SiteManager オンラインヘルプの HowTo 集を参照してください。 ■記述例（USB メモリ） AutoRecoveryFromPrev:On ■入力例（コマンド） set na AutoRecoveryFromPrev On	On	V4.0 で追加
Charset	設定ファイルの文字コード指定を設定します。設定値は、1 個のみ記述可能です。本パラメータ使用時は、必ず設定ファイルの 2 行目に記述してください。 設定値は、Shift_JIS を指定する場合は『sjis』、日本語 EUC(EUC-JP)を指定する場合は『eucjp』を記述してください。本パラメータがない場合、設定ファイルの文字コードは Shift_JIS として処理されます。 本パラメータで指定された文字コードと、設定ファイルの文字コードが異なる場合、全角文字を反映させることができません。 ■記述例（USB メモリ） Charset:eucjp	sjis	

	■入力例（コマンド） 3.7.28 文字コード指定コマンド（charset）		
CheckHttpPort	「承認申請機能」または「防止メッセージ機能」利用時に設定します。不正接続防止された端末から HTTP アクセスによる承認申請要求を許可する TCP ポート番号を指定します。最大 32 個まで設定可能です。設定値は、10 進数で『1』～『65535』の範囲で記述してください。複数のポート番号を記述する場合、カンマ（,）で区切って記述してください。 「承認申請機能」の詳細は、「InfoCage 不正接続防止 集中管理運用マニュアル」を、「防止メッセージ機能」の詳細は「InfoCage 不正接続防止 集中管理運用マニュアル」および「InfoCage 不正接続防止 分散管理運用マニュアル」を参照してください。 ■記述例（USB メモリ） CheckHttpPort:80,8080,8081,8082,8031 ■入力例（コマンド） set na CheckHttpPort 80,8080,8081,8082,8031	80	
CollectOfPacket	データ収集の有効/無効を設定します。設定値は、1 個のみ記述可能です。設定値は、収集を有効にする場合は『On』、無効にする場合は『Off』を記述してください。 なお、NQ を SiteManager へ新規登録した場合は、サイトコンソール、あるいは集中管理画面より収集開始を行わなければ SiteManager と正常に通信できません。新規登録時は本コマンドから設定を変更しないでください。 ■記述例（USB メモリ） CollectOfPacket:On ■入力例（コマンド）	Off	

	set na CollectOfPacket Off		
ContinuePrevention	「Gratuitous ARP 非準拠機器対応機能」を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。 「Gratuitous ARP 非準拠機器対応機能」については、8.2 章を参照してください。 ■記述例（USB メモリ） ContinuePrevention:On ■入力例（コマンド） set na ContinuePrevention On	Off	
ContinueYellowHostPrev	「黄色ホストの防止継続機能」を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。 「黄色ホストの防止継続機能」の詳細は、SiteManager オンラインヘルプの HowTo 集を参照してください。 ■記述例（USB メモリ） ContinueYellowHostPrev:On ■入力例（コマンド） set na ContinueYellowHostPrev On	Off	V4.0 で追加
DefaultGateway	NQ を設置するネットワークのデフォルトゲートウェイアドレスを設定します。設定値は、1 個のみ記述可能です。 設定値は、4.1 章の注意事項を参照の上、記述してください。	192.168.250.1	

	■記述例（USB メモリ） DefaultGateway:192.168.250.1 ■入力例（コマンド） 3.7.21 デフォルトゲートウェイアドレス設定コマンド（set gw）		
DefaultGateway(-)	NQ に設定されているネットワークのデフォルトゲートウェイアドレスを削除します。設定値は 1 個のみ記述可能です。 設定値は、アスタリスク（*）を記述してください。 ■記述例（USB メモリ） DefaultGateway(-):* ■入力例（コマンド） 3.7.27 デフォルトゲートウェイアドレス削除コマンド（remove gw）	ー	
DelayPreventionAlert	不正接続防止実施後からアラートが通知されるまでの猶予期間を設定します。設定した期間内に防止が解除された場合はアラートが通知されません。 設定値は、分単位で、1 個のみ記述可能です。 設定値は、10 進数で『0』～『60』の範囲で記述してください。 『0』を設定した場合、本機能は無効になります。 ■記述例（USB メモリ） DelayPreventionAlert:10 ■入力例（コマンド） set na DelayPreventionAlert 10	0	V5.0 で追加
DhcpScope	NQ が監視するネットワークで設定されている DHCP スコープの範囲を設定します。設定値	未設定	

	は、32 個まで記述可能です。 本パラメータは、NQ が管理しているホストの IP アドレスが固定 IP アドレス、DHCP クライアントのどちらかを判断する場合に利用します。 ここで指定した範囲内の IP アドレスを検知した場合、"DHCP クライアント"と判断します。なお、サイトコンソールの[ホスト一覧設定ダイアログ]で設定する同一ホストとみなす条件で「プロトコルアドレス」を選択している場合、発見したホストの IP アドレスが DHCP スコープの範囲内であれば 新規ホストではなく既存ホストの更新となる場合があります。 設定値は、『10.0.0.2-10.0.0.9』のように、開始と終了の IP アドレスは 4.1 章の注意事項を参照の上、記述してください。開始アドレスと終了アドレスの間は、ハイフン（-）で繋いだ形式で記述してください。複数の DHCP スコープを入力する場合、ダブルクォート（"）、またはシングルクォート（'）で入力値を囲み、各 DHCP スコープの間を半角スペースで繋いだ形式で入力してください。 本パラメータを使用した場合、以前の設定内容を破棄して設定値を反映させます。設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例（USB メモリ） ◆設定時 DhcpScope:10.0.0.1-10.0.0.5 10.0.0.7-10.0.0.9 ◆削除時 DhcpScope:"" ■入力例（コマンド） ◆設定時 set na DhcpScope "10.0.0.1-10.0.0.2 10.0.0.3-10.0.0.4"		

	◆削除時 set na DhcpScope ””		
DisableAutoReboot	InterSec/NQ30a、InterSec/NQ30b はシステムのリフレッシュのため、毎月一日の 0:00:00～0:49:59 の間のランダムな時間に自動で再起動を行っています。本機能はこの再起動の有効/無効を設定します。設定値は、『0』あるいは『1』を記述してください。『0』の場合は再起動が有効、『1』の場合は再起動が無効となります。 なお、本機能は InterSec/NQ30a と InterSec/NQ30b のみ有効です。 ■記述例（USB メモリ） DisableAutoReboot:1 ■入力例（コマンド） set na DisableAutoReboot 1	0	
DisableBroadCastJamArp	偽装 ARP パケットの送信方式を指定します。設定値は、1 個のみ記述可能です。設定値は、『0』あるいは『1』を記述してください。『0』の場合はブロードキャスト、『1』の場合はユニキャストとなります。 設定値が『1』の場合、以下の現象の回避策が有効になります。 ・DHCP クライアントの MacOS 端末を不正接続防止すると、Mac OS 端末が IP アドレスの取得を繰り返し DHCP サーバのアドレスプールが枯渇する。 ・承認済みの Windows Vista 以降の端末と未承認の端末との間の通信が防止されない。 なお、本機能の設定値が『1』の場合、DisableUnicastJamArp の設定値『1』と併用することはできません。 ■記述例（USB メモリ） DisableBroadCastJamArp:1	1	V3.9 より既定値を 1 に変更

	■入力例（コマンド） set na DisableBroadCastJamArp 1		
DisableOtherNetworkHostPrevent	監視対象ネットワークリストに属さないホストを防止しないようにする機能の設定状態です。設定値は『0』あるいは『1』を記述してください。 0：監視対象ネットワークに属さないホストを防止しない機能が無効 1：監視対象ネットワークに属さないホストを防止しない機能が有効 ■記述例（USB メモリ） DisableOtherNetworkHostPrevent:1 ■入力例（コマンド） set na DisableOtherNetworkHostPrevent 1 [注意事項] ・MultiNetwork が On の場合は本属性を On に設定しても機能しません。	0	
DisablePreventionAutoIPAddr	固定 IP アドレスを設定している Windows Vista などを不正接続防止すると APIPA により自動的に新しいアドレスが割り振られ、さらにその IP アドレスを不正接続防止するということを繰り返し、大量のホスト情報の表示および、防止通知が行われる場合があります。本機能は、APIPA などに代表される AutoIP アドレスとして割り振られる LINKLOCAL アドレス（169.254.0.0/16）を持つホストを不正接続防止から除外する機能です。 On：AutoIP アドレス防止除外機能が有効 Off：AutoIP アドレス防止除外機能が無効 ■記述例（USB メモリ） DisablePreventionAutoIPAddr:On	Off	

	■入力例（コマンド） set na DisablePreventionAutoIPAddr On		
DisablePreventionWhenNotConnectSM	SiteManager と通信できない場合に、不正接続防止機能を有効/無効にする機能を設定します。設定値は、1 個のみ記述可能です。 設定値は、通信不可時も不正接続防止機能を有効とする場合は『0』、無効とする場合は『1』を設定してください。 ただし、NQ を再起動した場合はメモリ内の承認ポリシーが消去されるため、設定値が『0』の場合でも、SiteManager から承認ポリシーを取得できるまで不正接続防止機能は有効になりません。 なお、冗長化機能利用時は、必ず本設定を『1』にしてください。 ■記述例（USB メモリ） DisablePreventionWhenNotConnectSM:0 ■入力例（コマンド） set na DisablePreventionWhenNotConnectSM 0	1	
DisableUnicastJamArp	特定条件において承認済みの Windows Vista 以降の端末のネットワークインターフェースが無効になる現象を回避させる機能の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『0』、有効にする場合は『1』を設定してください。 詳細は、「InfoCage 不正接続防止注意制限事項」を参照してください。 なお、本機能の設定値が『1』の場合、DisableBroadCastJamArp の設定値『1』と併用することはできません。 ■記述例（USB メモリ）	0	

	DisableUnicastJamArp:0 ■入力例（コマンド） set na DisableUnicastJamArp 0		
DisableWatchMyNetwork	監視対象ネットワークリストの InterSec/NQ30 と同一のネットワークを無視する機能の設定状態です。On に設定した場合、同一ネットワークを監視対象外のネットワークとして扱います。属性値は、1 個のみ入力可能です。 ■記述例（USB メモリ） DisableWatchMyNetwork:On ■入力例（コマンド） set na DisableWatchMyNetwork On [注意事項] ・MultiNetwork が On の場合、及びタグ VLAN 対応機能を使用している場合は本属性を On に設定しても機能しません。 ・分散管理モードでワーム感染ホストの接続防止機能を使用する場合、本属性を On に設定しても InterSec/NQ30 と同一のネットワークでワームに感染したホストに対して不正接続防止が行われます。	Off	
DNSServer	NQ を設置するネットワークで使用されている DNS サーバの IP アドレスを設定します。設定値は、3 個まで記述可能です。 設定値に IP アドレスを記述する場合、4.1 章の注意事項を参照の上、記述してください。 また、設定値を 2～3 個記述する場合、半角スペースで繋いだ形式で記述してください。 本パラメータを使用した場合、以前の設定内容を破棄して設定値を反映させるため、DNS サーバの削除パラメータ（DNSServer(-)）の設定は不要です。	未設定	

	■記述例（USB メモリ） DNSServer:192.168.250.6 192.168.250.7 ■入力例（コマンド） 3.7.9 DNS サーバアドレス設定コマンド（set ns nameserver）		
DNSServer(-)	NQ に設定されている DNS サーバの IP アドレスを削除します。設定値は、3 個まで記述可能です。 設定値に IP アドレスを記述する場合、4.1 章の注意事項を参照の上、記述してください。 IP アドレスが記述された場合、一致する設定のみ削除します。また、設定値を 2～3 個記述する場合、各 IP アドレスを半角スペースで繋いだ形式で記述してください。 設定値にアスタリスク（*）のみ記述した場合、全ての設定を削除します。 本パラメータが設定されていない場合、ホストの DNS 名が取得できません。 なお、設定値に IP アドレスとアスタリスクを併用して記述されている場合、削除処理が行われません。 ■記述例（USB メモリ） ◆指定削除時 DNSServer(-):192.168.250.6 192.168.250.7 ◆一括削除時 DNSServer(-):* ■入力例（コマンド） 3.7.22 DNS サーバアドレス削除コマンド（remove ns nameserver）	―	
DomainName	NQ を設置するネットワークのドメイン名を設定します。設定値は、複数記述可能です。	isnq.dom	

	設定値は、ネットワークのドメイン名を記述してください。複数のドメイン名を記述する場合、半角スペースで繋いだ形式で記述してください。設定可能な文字数の合計は2,000文字です。文字数制限には、複数設定時に引数の間に設定する半角スペースも含まれます。 ■記述例（USBメモリ） DomainName:isnq.dom test.dom ■入力例（コマンド） 3.7.10 ドメイン名設定コマンド（set ns domain）		
DomainName(-)	NQに設定されているネットワークのドメイン名を削除します。設定値は、複数記述可能です。 設定値をドメイン名で記述した場合、一致する設定のみ削除します。複数のドメイン名を記述する場合、半角スペースで繋いだ形式で記述してください。設定可能な文字数の合計は 2,000 文字です。文字数制限には、複数設定時に引数の間に設定する半角スペースも含まれます。 設定値をアスタリスク（*）のみで記述した場合、全ての設定を削除します。 本パラメータが設定されていない場合、ホストの逆引きが取得できません。 なお、設定値にドメイン名とアスタリスクを併用して記述されている場合、削除処理が行われません。 ■記述例（USBメモリ） ◆指定削除時 DomainName(-):isnq.dom test.dom ◆一括削除時	－	

	DomainName(-):* ■入力例（コマンド） 3.7.26 ドメイン名削除コマンド（remove ns domain）		
DontNotifyMacOnlyEntry	MAC アドレスしか収集できないホスト情報をホスト一覧に表示させないよう設定します。 設定値は、1 個のみ記述可能です。 設定値は、MAC アドレスのみのホスト情報を表示させる場合は『0』、表示させない場合は『1』を設定してください。 ■記述例（USB メモリ） DontNotifyMacOnlyEntry:1 ■入力例（コマンド） set na DontNotifyMacOnlyEntry 0	0	
ExceptMacVendor	特定ベンダの MAC アドレスを不正接続防止対象から除外する機能の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『0』、有効にする場合は『1』を設定してください。 本バージョンでは、Apple 社の MAC アドレス(IEEE-SA にて 2016 年 4 月に登録が確認されたもの)が不正接続防止対象から除外されるよう定義されています。 ■記述例（USB メモリ） ExceptMacVendor:0 ■入力例（コマンド） set na ExceptMacVendor 0	0	
FailOverMode	「NQ 冗長化機能」利用時に設定します。NQ の「冗長化モード」を設定します。設定値は、1 個のみ記述可能です。『On』の場合は「アクティブ」、『Off』の場合は「スタンバイ」	On	

	になります。 「NQ 冗長化機能」の詳細は、「InfoCage 不正接続防止集中管理運用マニュアル」を参照してください。 集中(小規模)管理モードのみ利用可能です。 ■記述例（USB メモリ） FailOverMode:On ■入力例（コマンド） set na FailOverMode On		
Ifspeed	NQ のネットワークインターフェースのネゴシエーション設定を変更します。設定値は、1個のみ記述可能です。 設定値は、オートネゴシエーションは『auto』、1000base-T 全二重通信は『1000FD』、100base-T 半二重通信は『1000HD』、100base-Tx 全二重通信は『100FD』、100base-Tx 半二重通信は『100HD』、10base-T 全二重通信は『10FD』、10base-T 半二重通信は『10HD』を記述してください。 『1000FD』、『1000HD』は NQ30d のみ設定可能です。 NQ30d の場合は設定するインターフェースを指定します。省略した場合は『eth0』に設定されます。 ■記述例（USB メモリ） Ifspeed:100FD ■記述例（USB メモリ）※NQ30d のみ Ifspeed:1000FD eth1 ■入力例（コマンド）	auto	

	3.7.18 ネットワークインターフェースのネゴシエーション設定変更コマンド（set ifspeed）		
IgnoreMISignalIpAddr	PC 管理製品(パソコン見張り隊など)から通知された IP アドレスの有効／無効を設定します。設定値は、1 個のみ記述可能です。『0』あるいは『1』を記述してください。 『0』の場合は PC 管理製品(パソコン見張り隊など)から通知された MAC アドレスと IP アドレスの組み合わせに一致するホストにPC管理製品(パソコン見張り隊など)が導入されていると判断します。 『1』の場合は PC 管理製品(パソコン見張り隊など)から通知された MAC アドレスに一致するすべてのホストにPC管理製品(パソコン見張り隊など)が導入されていると判断します。 IPv4/IPv6 のデュアルスタック環境でホストの状態（色）を”黄”で管理する運用をする場合は、本設定を有効にしてください。 ■記述例（USB メモリ） IgnoreMISignalIpAddr:1 ■入力例（コマンド） set na IgnoreMISignalIpAddr 1	0	V3.9 で追加
IgnoreOsInfo	本設定はホストの状態（色）を”黄”で管理する場合に利用できるパラメータです。 OS 種別に関わらず PC 管理製品(パソコン見張り隊など)からの存在通知を受信していないホストを防止する設定をします。設定値は、1 個のみ記述可能です。『On』あるいは『Off』を記述してください。 『On』の場合は OS デテクトの結果によらず PC 管理製品(パソコン見張り隊など)が導入されていないホストとして防止します。 『Off』の場合は OS デテクトにより Windows と判断されたホストのみ PC 管理製品(パソ	Off	V3.9 で追加

	コン見張り隊など)が導入されていないホストとして防止します。 IPv4/IPv6 のデュアルスタック環境でホストの状態（色）を”黄”で管理する運用をする場合は、本設定を有効にしてください。 ■記述例（USB メモリ） IgnoreOsInfo:On ■入力例（コマンド） set na IgnoreOsInfo On		
JamMacAddressMode	偽装 ARP パケットのアドレスモードを指定します。設定値は、1 個のみ記述可能です。設定値は、『0』あるいは『1』を記述してください。『1』の場合は以下の機能を有効にするモードとなります。 ・承認申請機能 ・承認済みの Windows Vista 以降の端末と未承認の端末との間の通信が防止されない現象の回避策 「承認申請機能」の詳細は、「InfoCage 不正接続防止集中管理運用マニュアル」を参照してください。 ■記述例（USB メモリ） JamMacAddressMode:1 ■入力例（コマンド） set na JamMacAddressMode 1	1	V3.9 より既定値を 1 に変更
JamStatus	NQ の不正接続防止機能を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。サイトコンソールに新規登録した際は、必ず『Off』が設定されます。	Off	

	不正接続防止機能は、NQ の設定内容より SiteManager、あるいは集中管理画面の設定が優先されます。通常時の設定変更は、本パラメータを使用せず、サイトコンソール、または集中管理画面から行ってください。 ■記述例（USB メモリ） JamStatus:Off ■入力例（コマンド） set na JamStatus Off		
ManagerPort	NQ が SiteManager への通信を送信するポート番号を設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『1』～『65535』の範囲で記述してください。設定値が SiteManager に設定されている受信ポート番号と異なる場合は、SiteManager と通信できなくなるため、注意してください。なお、SiteManager の受信ポート番号の変更方法は、SiteManager インストールマニュアルを参照してください。 ■記述例（USB メモリ） ManagerPort:23490 ■入力例（コマンド） set na ManagerPort 23490	23490	
MultiNetwork	「共有ネットワーク対応機能」を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。なお、VLAN 環境設置時は、必ず本設定を無効にしてください。 ■記述例（USB メモリ）	Off	

	MultiNetwork:On ■入力例（コマンド） set na MultiNetwork On [注意事項] 分散管理モードでワーム感染ホストの接続防止機能を使用する場合、本属性を On に設定してもサイトコンソールのエージェント設定ダイアログに表示される監視対象ネットワークリストに属さないワーム感染ホストを防止することはできません。		
NetworkList NetworkList1 ～ NetworkList31	共有ネットワーク対応機能の個別指定モード(※)で、監視対象とするネットワークのアドレスとサブネットマスクを設定します。最大 31 個まで設定可能です。設定値は、ネットワークアドレスとサブネットマスクをスラッシュ(/)で区切って記述してください。サブネットマスクは 8 から 30 まで指定可能です。 VLAN インターフェースが設定されている場合、本属性は非表示となります。 (※)SiteManager オンラインヘルプの[その他の機能]－[共有ネットワーク対応機能]を参照してください。 ■記述例（USB メモリ） NetworkList:192.168.10.0/24 NetworkList1:192.168.20.0/24 NetworkList2:192.168.30.0/24 ■入力例（コマンド） 3.7.29 ネットワークリスト追加コマンド（add networklist）	未設定	

NetworkList(-)	共有ネットワーク対応機能の個別指定モードで、監視対象とするネットワークをネットワークリストから削除します。設定値は、特定のネットワークを削除する場合は、ネットワークアドレスとサブネットマスクをスラッシュ(/)で区切って記述してください。サブネットマスクは 8 から 30 まで指定可能です。監視対象ネットワークリストを空にする場合はアスタリスク（*）を指定してください。 なお、特定のネットワークを複数同時に削除することはできません。この設定値を設定ファイルに複数記述した場合、最後に記述したもののみ有効になります。 ■記述例（USB メモリ） ◆特定のネットワークを削除する場合 NetworkList(-):192.168.10.0/24 ◆全ネットワークを削除する場合 NetworkList(-):* ■入力例（コマンド） 3.7.30 ネットワークリスト削除コマンド（remove networklist）	ー	
NoUpdArpReply	ホストが生存していると判断する条件から、下記パケットを外す場合に設定します。 ・NQ からの ARP リクエストに応答し返ってきた ARP リプライ このパラメータの詳細については「8.14 スリープ中の黄色のホストが防止される場合の対応」を参照してください。 ■記述例（USB メモリ） NoUpdArpReply:On ■入力例（コマンド） set na NoUpdArpReply On	Off	V5.2 で追加

NotifyInterval	NQ が SiteManager にホスト情報の通知を行うインターバルを秒単位で設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『30』～『3600』の範囲で記述してください。 ■記述例（USB メモリ） NotifyInterval:30 ■入力例（コマンド） set na NotifyInterval 30	60	
OsDetect	「OS デテクト機能」の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『0』、有効にする場合は『1』を設定してください。 「OS デテクト機能」を無効にすると、NetBIOS パケットと DNS 名前解決パケットの送信も停止します。 「OS デテクト機能」の詳細は、SiteManager オンラインヘルプを参照してください。 ■記述例（USB メモリ） OsDetect:0 ■入力例（コマンド） set na OsDetect 0	1	
Port	NQ が SiteManager からの通信を受信するポート番号を設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『1』～『65535』の範囲で記述してください。但し、telnet を介したネットワーク接続の使用ポートである『23496』は設定しないでください。 ■記述例（USB メモリ）	23491	

	AgentPort パラメータを参照してください。 ■入力例（コマンド） set na Port 23491		
PreventionTimeForYellowHost	黄で Windows と判断されたホストを発見後、接続防止を開始するまでの時間を秒単位で設定します。設定した時間、PC 管理製品からの存在通知パケットを収集できなければ、接続防止をします。設定値は、1 個のみ記述可能です。（※） （※）IgnoreOsInfo が”On”の場合は、OS 種別に関わらず本パラメータで設定した時間、PC 管理製品からの存在通知パケットを収集できなければ、接続防止をします。 設定値は、10 進数で『1800』～『2678400』の範囲で記述してください。 ■記述例（USB メモリ） PreventionTimeForYellowHost:3600 ■入力例（コマンド） set na PreventionTimeForYellowHost 3600	3600	
ProtectHost	Gratuitous ARP 非準拠機器の IP アドレスを設定します。設定値は、32 個まで記述可能です。 設定値の IP アドレスは、4.1 章の注意事項を参照の上、記述してください。複数の IP アドレスを記述する場合、カンマ（,）で区切って記述してください。設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 「Gratuitous ARP 非準拠機器対応機能」については、8.2 章を参照してください。 ■記述例（USB メモリ）	未設定	

	◆設定時 ProtectHost:192.168.250.252,192.168.250.253 ◆削除時 ProtectHost:"" ■入力例（コマンド） ◆設定時 set na ProtectHost 192.168.250.252,192.168.250.253 ◆削除時 set na ProtectHost ""		
SendArp	ARP パケットを送信することの少ないホストを検知するために定期的に ARP リクエストを送信する機能の有効/無効を設定します。設定値は、1 個のみ記述可能です。機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。 ARP リクエストは、以下のネットワークの IP アドレスの範囲に対して送信します。 ・NetworkList に設定したネットワークのうちサブネットマスクが 16 ビット以上のもの。 また、ARP リクエストは、NetworkAgent サービス起動の 1 分後および毎日午前 1 時に送信します。 ■記述例（USB メモリ） SendArp:On ■入力例（コマンド） set na SendArp On	On	V5.0 で追加
SendArpDelay	不正アクセスの検知後に偽装 ARP パケットを送信してから再送するまでの秒数を指定します。設定値は、1 個のみ記述可能です。設定値は、10 進数で『0』～『60』の範囲で記述してください。設定値が 0 もしくは指定されない場合、本機能は無効になります。	0	

	Linux 系 OS 等、ARP エントリ更新のロックタイムが設定されている OS において、ARP エントリの偽装を有効にするために本機能を使用します。本パラメータの設定値を OS のロックタイムより長い秒数にすることで ARP エントリの偽装が有効になります。 ■記述例（USB メモリ） SendArpDelay:1 ■入力例（コマンド） set na SendArpDelay 1		
SendArpInterval	NQ が当日検知した機器に対してネットワークへの接続を確認するために ARP リクエストを送信する時間間隔を分単位で設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『0』または『3』～『480』の範囲で記述してください。 『0』を設定した場合は、ARP リクエストの送信は行いません。 ■記述例（USB メモリ） SendArpInterval:20 ■入力例（コマンド） set na SendArpInterval 20	20	V5.1 で追加
TimeOut	通信処理時のタイムアウト時間を秒単位で設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『10』～『360』の範囲で記述してください。 通常は既定値で問題ありませんが、SiteManager-NQ 間の通信速度が遅い場合や、SiteManager インストール PC のマシンスペックが低い場合は、本パラメータの設定値を大きくすることで通信エラーが改善されることがあります。 ■記述例（USB メモリ）	20	

	TimeOut:20 ■入力例（コマンド） set na TimeOut 20		
Vlan(-)	設定されている VLAN インターフェースを削除します。設定値は、1 個のみ記述可能です。 VLAN インターフェースを指定して削除する場合、該当の VLAN インターフェースに設定されている VLAN ID を 10 進数で記述してください。全ての VLAN インターフェースを削除する場合、アスタリスク（*）を記述してください。 本パラメータを使用してタグ VLAN 環境から非タグ VLAN 環境での使用に切り替える場合、５章の制限事項を参照してください。 ■記述例（USB メモリ） Vlan(-):101 ■入力例（コマンド） 3.7.20 VLAN インターフェース削除コマンド（remove vlan）	ー	

7.6　NQ30c、NQ30d のみに有効な設定可能パラメータ

NQ30c、NQ30d のみに有効な設定可能パラメータを以下に示します。

パラメータ	説明	既定値	備考
AutoPermitConnPort	通信を検知した場合に自動的に接続を許可するポート番号を設定します。設定値は、32個まで記述可能です。また、設定値を 2～32 個記述する場合、ダブルクォート(")、またはシングルクォート(')で設定値を囲み、各設定値の間を半角スペースで繋いだ形式で記述してください。なお、設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例（USB メモリ） ◆設定例 AutoPermitConnPort:111 AutoPermitConnPort:111 222 333 ◆削除例 AutoPermitConnPort:"" ■入力例（コマンド） ◆設定例 set na AutoPermitConnPort 111 set na AutoPermitConnPort "111 222 333" ◆削除例 set na AutoPermitConnPort ""	未設定	V4.0 で追加
ConsoleTelnet	NQ30c、NQ30d に対する telnet 接続の有効/無効を設定します。設定値は、1 個のみ記述	1	V5.1 で追加

	可能です。 設定値は、telnet 接続を無効にする場合は『0』、有効にする場合は『1』を設定してください。 telnet 接続を無効にした場合は、SSH で接続してください。SSH での接続については「3.3 SSH によるネットワーク接続」を参照してください。 ■記述例（USB メモリ） ConsoleTelnet:1 ■入力例（コマンド） set na ConsoleTelnet 1		
DisablePreventIPv6AddrAlert	IPv6 アドレスの不正接続防止時のアラート通知を設定します。設定値は 1 個のみ記述可能です。 設定値は、全ての IPv6 アドレスの防止を通知する場合は『0』（※）、IPv6 アドレスの防止を通知しない場合は『1』を設定してください。 PreventIPv6AllAddr:1 の場合のみ本パラメータは設定可能です。 EnableIPv6:On の場合は、本設定値に関わらず不正接続防止された IPv6 アドレスの数だけアラートが通知されます。 （※）IPv6 アドレスの防止通知は 1 日 1 回、初回に防止した場合にのみ出力します。 ■記述例（USB メモリ） DisablePreventIPv6AddrAlert:1 ■入力例（コマンド） set na DisablePreventIPv6AddrAlert 1	0	V3.9 で追加
DontJamServer	防止されているホストから NQ を介して接続可能なサーバとポートとプロトコル	未設定	V4.0 で追加

	(TCP/UDP)の一覧を設定します。設定値は、32 個まで記述可能です。この設定は、TCP および UDP プロトコルに対してのみ有効で、ICMP などのプロトコルは対象外です。 IP アドレスの代わりに DNS 名の指定も可能です。 「IP アドレス」の場合は、指定の IP アドレスの任意のポートへの TCP/UDP 接続を許可します。 「IP アドレス:ポート番号」の場合は、指定の IP アドレス:ポート番号への TCP/UDP 接続を許可します。 設定値に IP アドレスを記述する場合、4.1 章の注意事項を参照の上、記述してください。 また、設定値を 2～32 個記述する場合、ダブルクォート(")、またはシングルクォート(‘)で設定値を囲み、各設定値の間を半角スペースで繋いだ形式で記述してください。なお、設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 このパラメータを設定した場合、[DNSServer](DNS サーバアドレス)の設定が必要です。 ■記述例（USB メモリ） ◆設定例 DontJamServer:192.168.0.1 DontJamServer:dl.aaa.co.jp:80 DontJamServer:dl.aaa.co.jp:80/TCP DontJamServer:dl1.aaa.co.jp dl2.aaa.co.jp ◆削除例 DontJamServer:"" ■入力例（コマンド） ◆設定例		

	set na DontJamServer 192.168.0.1 set na DontJamServer dl.aaa.co.jp:80 set na DontJamServer dl.aaa.co.jp:80/TCP set na DontJamServer "dl1.aaa.co.jp dl2.aaa.co.jp" ◆削除例 set na DontJamServer ""		
EnableIPv6	IPv6 対応機能の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『Off』、有効にする場合は『On』を設定してください。 「PreventIPv6AllAddr」との関係は「8.8 IPv6 アドレスを防止するには？」を参照してください。 ■記述例（USB メモリ） EnableIPv6:On ■入力例（コマンド） set na EnableIPv6 On	Off	V3.9 で追加
HttpProxyServer	防止されているホストから NQ を介して HTTP セッションを中継する HTTP Proxy サーバとポートの一覧を設定します。設定値は、32 個まで記述可能です。 各サーバは「IP アドレス」「IP アドレス:ポート番号」のいずれかの形式で指定します。 IP アドレスの代わりに DNS 名の指定も可能です。 「IP アドレス」の場合は、指定の IP アドレスの http(80)のポートへ HTTP セッションを中継します。 「IP アドレス:ポート番号」の場合は、指定の IP アドレス:ポート番号へ HTTP セッションを中継します。	未設定	V4.0 で追加

	設定値に IP アドレスを記述する場合、4.1 章の注意事項を参照の上、記述してください。 また、設定値を 2～4 個記述する場合、ダブルクォート(")、またはシングルクォート(')で設定値を囲み、各設定値の間を半角スペースで繋いだ形式で記述してください。なお、設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 このパラメータで DNS 名を設定した場合、[DNSServer](DNS サーバアドレス)の設定が必要です。 ■記述例（USB メモリ） ◆設定例 HttpProxyServer:192.168.0.1 HttpProxyServer:dl.aaa.co.jp:8080 HttpProxyServer:dl1.aaa.co.jp dl2.aaa.co.jp:8080 ◆削除例 HttpProxyServer:"" ■入力例（コマンド） ◆設定例 set na HttpProxyServer 192.168.0.1 set na HttpProxyServer dl.aaa.co.jp:8080 set na HttpProxyServer "dl1.aaa.co.jp dl2.aaa.co.jp:8080" ◆削除例 set na HttpProxyServer ""		
PreventIPv6AllAddr	全ての IPv6 アドレス接続を防止する設定の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『0』、有効にする場合は『1』を設定してください。	0	V3.9 で追加

	「EnableIPv6」との関係は「8.8 IPv6 アドレスを防止するには？」を参照してください。 ■記述例（USB メモリ） PreventIPv6AllAddr:1 ■入力例（コマンド） set na PreventIPv6AllAddr 1		
SendNdpWaitTime	IPv6 アドレスの不正アクセスを検知してから、偽装 ICMPv6 応答パケット(Neighbor Advertisement)を送信するまでの時間（ミリ秒）を指定します。設定値は、1 個のみ記述可能です。設定値は、10 進数で『0』～『50』の範囲で記述してください。設定値が 0 もしくは指定されない場合、本機能は無効になります。 「PreventIPv6AllAddr」が有効な場合は、設定値に関わらず本機能は無効となります。 ■記述例（USB メモリ） SendNdpWaitTime:1 ■入力例（コマンド） set na SendNdpWaitTime 1	未設定	V4.0 で追加
SshHostKey	NQ30c、NQ30d に対する SSH 接続で使用する SSH ホスト鍵を更新します。SSH ホスト鍵の更新には 1 分程度の時間を要します。 本コマンドを入力すると SSH ホスト鍵が更新されるため、SSH 接続時には SSH クライアントソフトで再度ホスト鍵の受け入れが必要となります。 本コマンドで設定した場合、NetworkAgent サービスの再起動は不要です。 ■入力（コマンド） set na SshHostKey	－	V5.1 で追加

7.7　NQ30d のみに有効な設定可能パラメータ

NQ30d のみに有効な設定可能パラメータを以下に示します。

パラメータ	説明	既定値	備考
MonitoringIf	データ収集、不正接続防止を実行するインターフェースを指定します。 eth0 のみ、eth1 のみ、または eth0 と eth1 の両方を指定します。 eth0 と eth1 の両方を指定する場合はカンマ区切りで指定します。 InfoCollectIf に設定されているインターフェースを MonitoringIf に指定することはできません。MonitoringIf に設定するインターフェースは、あらかじめ InfoCollectIf に設定されていない状態にしておく必要があります。 また、VLAN インターフェースを設定している場合、MonitoringIf は eth0 固定になります。MonitoringIf に eth0 以外を設定している状態で VLAN インターフェースを設定すると、MonitoringIf は自動的に eth0 に変更されます。 ■記述例（USB メモリ） MonitoringIf:eth0 MonitoringIf:eth0,eth1 ■入力例（コマンド） set na MonitoringIf eth0 set na MonitoringIf eth0,eth1	eth0	V5.2 で追加
InfoCollectIf	【本機能は NetworkAgent(Linux)のみ使用可能です】 ミラーポートに接続しホストのデータ情報の収集に使用するインターフェースを指定します。	未設定	V5.2 で追加

	eth0 または eth1 のいずれかを指定します。 MonitoringIf に設定されているインターフェースを InfoCollectIf に指定することはできません。InfoCollectIf に設定するインターフェースは、あらかじめ MonitoringIf に設定されていない状態にしておく必要があります。 設定値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例（USB メモリ） ◆設定例 InfoCollectIf:eth1 ◆削除例 InfoCollectIf: ″″ ■入力例（コマンド） ◆設定例 set na InfoCollectIf eth1 ◆削除例 set na InfoCollectIf ″″		
AccessLog	アクセスログ収集機能の有効/無効を設定します。また、アクセスログを削除します。 無効にする場合は『Off』、有効にする場合は『On』を設定してください。 また、NQ 内に出力されているアクセスログを削除する場合は『Del』を設定してください。 なお、『Del』はコマンドでのみ設定可能で、USB メモリでは設定できません。 ■記述例（USB メモリ） AccessLog:On ■入力例（コマンド）	Off	V5.2 で追加

	set na AccessLog On		
AccessLogType	出力するアクセスログの種類を設定します。 出力するログの種類に応じて下記を指定してください。 ARP: ARP ログ HTTP: HTTP ログ SMB: SMB ログ UDP: UDP ログ TCP: TCP ログ 複数指定する場合は、カンマ区切りで指定します。 設定値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例（USB メモリ） ◆設定例 AccessLogType:HTTP,SMB ◆削除例 AccessLogType: ″″ ■入力例（コマンド） ◆設定例 set na AccessLogType HTTP,SMB ◆削除例 set na AccessLogType ″″	未設定	V5.2 で追加
RestAccessLog	アクセスログ抑制機能の有効/無効を設定します。 無効にする場合は『Off』、有効にする場合は『On』を設定してください。	On	V5.2 で追加

	詳細は「8.13.5 ログ出力の抑制」を参照してください。 ■記述例（USB メモリ） RestAccessLog:On ■入力例（コマンド） set na RestAccessLog On		
AccessLogMaxCnt	アクセスログ抑制機能有効時に保持したアクセスログ抑制データを初期化する閾値を設定します。 「設定値×10,000」を超えるアクセスログを出力するタイミングで、古い方から順に 1/5 のアクセスログ抑制データを削除します。 設定可能な範囲は『1』～『100』です。 詳細は「8.13.5 ログ出力の抑制」を参照してください。 ■記述例（USB メモリ） AccessLogMaxCnt:50 ■入力例（コマンド） set na AccessLogMaxCnt 50	50	V5.2 で追加
AccessLogSize	アクセスログ 1 ファイル毎のサイズ(MB)を設定します。 アクセスログは最大 10 ファイル作成され、それ以上作成する場合は古いアクセスログから順に削除されます。 設定可能な範囲は『1』～『20』です。 ※ NetworkAgent(Linux)の設定可能な範囲は『1』～『1000』です。 ■記述例（USB メモリ） AccessLogSize:20	20	V5.2 で追加

	■入力例（コマンド） 　set na AccessLogSize 20		
Syslog	アクセスログの syslog 出力機能の有効/無効と出力する際の facility を設定します。 無効にする場合は『Off』、有効にする場合は出力する facility の値として『local0』『local1』『local2』『local3』『local4』『local5』『local6』のいずれかを設定してください。 ■記述例（USB メモリ） 　Syslog:local0 ■入力例（コマンド） 　set na Syslog local0	Off	V5.2 で追加
SyslogRemoteHost	syslog に出力したアクセスログの転送先を設定します。 転送先の IP アドレスまたは DNS 名を設定します。転送先に DNS 名を指定する場合は DNS サーバの設定が必要です。 設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例（USB メモリ） 　SyslogRemoteHost:192.168.250.200 ■入力例（コマンド） 　set na SyslogRemoteHost 192.168.250.200	未設定	V5.2 で追加
SyslogOutMsg	監視メッセージの syslog 出力機能の有効/無効を設定します。 無効にする場合は『Off』、有効にする場合は『On』を設定してください。 本機能の詳細については「8.15 監視メッセージを syslog に出力するには」を参照してください。	Off	V5.2 で追加

	■記述例（USB メモリ） SyslogOutMsg:On ■入力例（コマンド） set na SyslogOutMsg On		
SyslogFwdMsgHost	syslog に出力した監視メッセージの転送先を設定します。 転送先の IP アドレスまたは DNS 名を設定してください。転送先に DNS 名を指定する場合は DNS サーバの設定が必要です。 設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例（USB メモリ） SyslogFwdMsgHost:192.168.250.200 ■入力例（コマンド） set na SyslogFwdMsgHost 192.168.250.200	Off	V5.2 で追加
IfVlanId	NQ30d が内部で使用する VLAN ID を設定します。 VLAN インターフェースとして割り当てる VLAN ID”以外”の値を 2 つ設定してください。 2 つの値の間はスペースで区切って指定してください。 初期状態では『1』と『2』が設定されています。 VLAN インターフェースとして『1』と『2』を使用しない場合は本コマンドによる変更は不要です。 ■記述例（USB メモリ） IfVlanId:3000 3001 ■入力例（コマンド）	1 2	V5.2 で追加

	set ifvlanid 3000 3001		

7.8　Lite のみで有効な設定可能パラメータ

Lite のみで有効な設定可能パラメータを以下に示します。

パラメータ	説明	既定値	備考
CoordinatePCMan	特定通信検知による接続許可機能を利用する/しないを設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を利用しない場合は『0』、利用する場合は『1』を設定してください。 ■記述例（USB メモリ） CoordinatePCMan:1 ■入力例（コマンド） set na CoordinatePCMan 1	0	
DisableBlueHostAlert	新規ホスト発見時に状態(色)が青のホストのアラートを通知する/しないを設定します。 設定値は、1 個のみ記述可能です。 設定値は、通知する場合は『0』、通知しない場合は『1』を設定してください。 ■記述例（USB メモリ） DisableBlueHostAlert:1 ■入力例（コマンド） set na DisableBlueHostAlert 1	0	

SmtpPort	メール送信時に使用する SMTP サーバのポートを設定します。設定値は、1 個のみ記述可能です。設定値は、10 進数で『1』～『65535』の範囲で記述してください。設定値が範囲外の場合、既定値が設定されたものとして動作します。 ■記述例（USB メモリ） SmtpPort:25 ■入力例（コマンド） set na SmtpPort 25	25	

8　HowTo 集

8.1　NQ の時刻を SiteManager と同期させるには？

8.1.1　通常版の場合

NQ は SiteManager との同期の際に自動的に、SiteManager 側の OS の時刻と同期を行っているため、時刻同期コマンド（SvNqSetTime.exe）を使用して時刻同期を行う必要はありません。
NQ と SiteManager との同期は以下のタイミングで行います。

- NQ 起動時
- NQ 起動後１時間毎
- サイトコンソール上での操作（データ収集の開始/停止、新規ホストの状態（色）の設定、エージェント設定ダイアログで[OK]ボタンクリック時、不正接続防止機能の有効/無効）の１分後
- DomainManager から NQ のデータ収集の開始/停止、不正接続防止機能の有効/無効の操作の１分後（集中管理モードの場合）

8.1.2　Lite 版の場合

RemoteConsole インストール PC から Lite 版の NQ の時刻を設定します。
詳細は「InfoCage 不正接続防止 Lite 時刻同期コマンドマニュアル」を参照してください。

8.2　不正接続端末から監視対象セグメント外への通信を防止できない場合は？

ルータやスイッチなど、LAN 内の接続対象が Gratuitous ARP(※)に対応していない場合、不正接続端末の通信を防止できない場合があります。ルータやスイッチを経由した通信などが防止できない場合、「Gratuitous ARP 非準拠機器対応機能」を有効に設定し、ルータなどの IP アドレスを登録後、防止できるか確認してください。なお、本機能を有効にしている場合、特定条件において承認済みの Windows Vista 以降の端末のネットワークインターフェースが無効になる現象の回避策を有効にすることができません。現象の詳細は、「InfoCage 不正接続防止注意制限事項」を参照してください。

(※)Gratuitous ARP については SiteManager オンラインヘルプの[InfoCage 不正接続防止]->[その他]->[用語集]->[Gratuitous ARP]を参照してください。

■USB メモリ・telnet もしくは SSH(NQ30c、NQ30d のみ)を使用して設定する場合
7.5 章の「ContinuePrevention」、および「ProtectHost」の内容を参照し、設定を行ってください。

■SiteManager インストール PC 上からコマンドによる設定を行う場合
SiteManager オンラインヘルプの目次より、[InfoCage 不正接続防止]->[その他]->[HowTo 集]を選択し、「■Gratuitous ARP 非準拠機器へ対応するには？」を参照してください。

8.3　使用中の NQ のエージェント名、IP アドレスを変更する方法

エージェント名や IP アドレスを変更する手順は、運用モードにより異なります。以下を参照し、利用する運用モードに応じた手順で変更してください。

8.3.1　分散管理モードの場合

8.3.1.1 エージェント名を変更する手順

エージェント名設定コマンド（3.7.15 章）を参照し、エージェント名を変更する。
※エージェント名設定後、NQ の再起動が必要です。

8.3.1.2 IP アドレスを変更する手順

(1) IP アドレスを変更する
ネットワークインターフェース設定コマンド（3.7.7 章）を参照し、該当 NQ の IP アドレスを変更する。

(2) NQ を再起動する

再起動コマンド（3.7.13 章）を参照し、NQ を再起動する。

8.3.2　集中管理モードの場合

8.3.2.1 エージェント名を変更する手順

【ドメイン・サイト・エージェント管理の場合】

(1) 不正接続防止、データ収集を停止する

DomainManager の集中管理画面の「コンポーネント管理」->「エージェント」より該当 NQ の不正接続防止、データ収集を停止する。

(2) ホストデータをバックアップする

ホストエクスポートコマンドを使用し、ホストデータをバックアップする。

※ホストエクスポートコマンドについては、ドメインマネージャオンラインヘルプの「ホスト情報のエクスポートコマンドについて」を参照してください。

(3) エージェント名を変更する

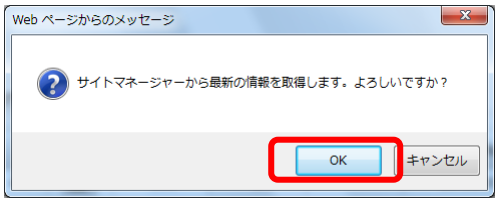
エージェント名設定コマンド（3.7.15 章）を参照し、エージェント名を変更する。

※エージェント名設定後、NQ の再起動が必要です。

(4) SiteManager の最新情報を取得する

NQ が起動したら、DomainManager 集中管理画面の「コンポーネント管理」->「サイトマネージャ」より SiteManager の最新情報を取得する。

このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



(5) エージェントの詳細設定を入力する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」にエージェント名変更後のエージェント情報が表示されたら、「エージェント管理詳細画面」よりエージェント名

変更前の情報を入力してください。

(6) ホストデータをリストアする

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」にエージェント名変更後のエージェント情報が表示されたら、ホストインポートコマンドを使用してホストデータをリストアする。

※ホスト情報をインポートする際は、(2)でエクスポートしたホスト情報ファイルの「エージェント名」カラムのエージェント名を、変更前の名前から変更後の名前に修正してください。

ホストインポートコマンドについては、ドメインマネージャオンラインヘルプの「ホスト情報のインポートコマンドについて」を参照してください。

(7) データ収集を開始する

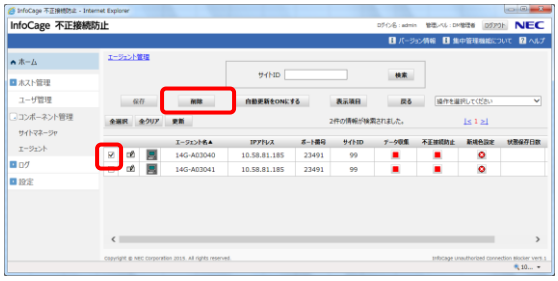
DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」にエージェント名変更後のエージェント情報が表示されたらデータ収集を開始する。

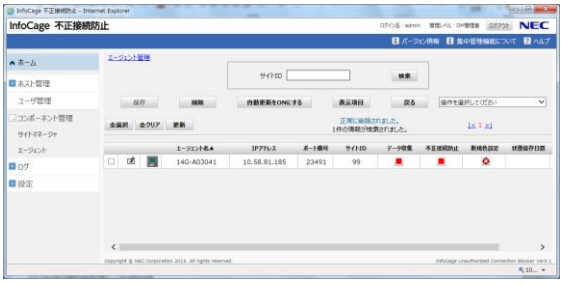
(8) 不正接続防止を開始する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」より該当 NQ の不正接続防止を開始する。

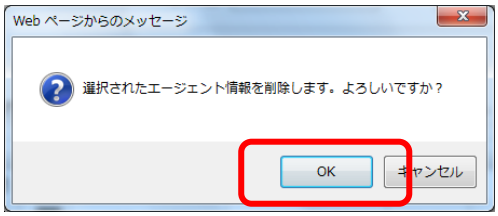
(9) 古いエージェントを削除する

DomainManager 集中管理の「コンポーネント管理」->「エージェント」より変更前のエージェント情報を削除する。





このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



【VLAN グループ管理の場合】

(1) 不正接続防止、データ収集を停止する

DomainManager の集中管理画面の「グループ管理」->「VLAN グループ」より該当 NQ の不正接続防止、データ収集を停止する。

(2) エージェント名を変更する

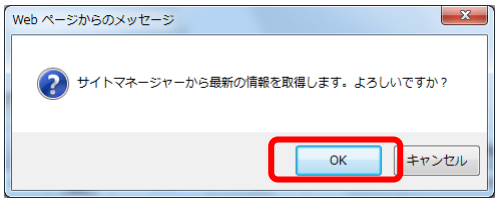
エージェント名設定コマンド（3.7.15 章）を参照し、エージェント名を変更する。

※エージェント名設定後、NQ の再起動が必要です。

(3) SiteManager の最新情報を取得する

NQ が起動したら、DomainManager 集中管理画面の「コンポーネント管理」->「サイトマネージャ」より SiteManager の最新情報を取得する。

このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



(4) エージェントをグループに登録する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」にエージェント名変更後のエージェント情報が表示されたら、「グループ管理」->「VLAN グループ」よりエージェント名変更後のエージェントを既定のグループから削除して、変更前のグループに登録してください。

(5) データ収集を開始する

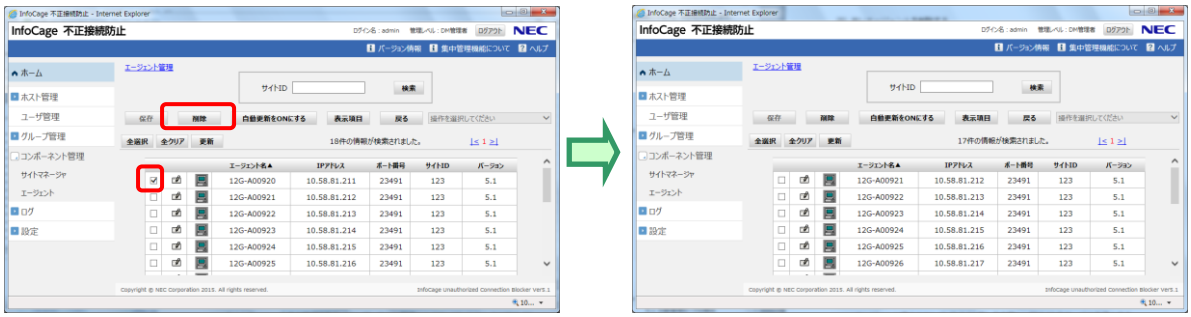
DomainManager 集中管理画面の「グループ管理」->「VLAN グループ」にエージェント名変更後のエージェント情報が表示されたらデータ収集を開始する。

(6) 不正接続防止を開始する

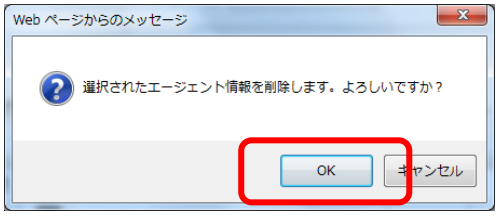
DomainManager 集中管理画面の「グループ管理」->「VLAN グループ」より該当 NQ の不正接続防止を開始する。

(7) 古いエージェントを削除する

DomainManager 集中管理の「コンポーネント管理」->「エージェント」より変更前のエージェント情報を削除する。



このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



8.3.2.2 IP アドレスを変更する手順

(1) 不正接続防止、データ収集を停止する

DomainManager の集中管理画面の「コンポーネント管理」->「エージェント」より該当 NQ の不正接続防止、データ収集を停止する。

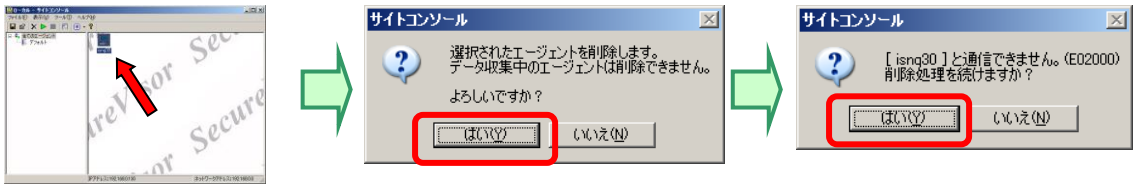
(2) NQ を停止する

エージェント停止コマンド（3.7.24 章）を参照し、該当 NQ のサービスを停止する。

(3) エージェントを削除する

サイトコンソールを起動し、該当 NQ を削除する。

※NQ と通信できない旨のメッセージが表示されますが、そのまま削除してください。



(4) RCV ファイルを Backup フォルダへ移動する

DomainManager より該当 NQ を管理する SiteManager の最新 RCV ファイルを Backup フォルダへ移動する。

【RCV ファイル保存場所】

C:¥Program Files¥SecureVisor¥DomainManager¥RecvData¥AAA_BBB_YYYYMMDDHHMMSS.RCV

※DomainManager を "C:¥Program Files¥SecureVisor" にインストールした場合

※ AAA は、SiteManager の IP アドレス。

BBB は、サイト ID

YYYYMMDDHHMMSS は、日時

例：「192.168.0.100_001_20080824.RCV」

【移動先フォルダの場所】

C:¥Program Files¥SecureVisor¥DomainManager¥Backup¥AAA_BBB

※DomainManager を "C:¥Program Files¥SecureVisor" にインストールした場合

※ AAA は、SiteManager の IP アドレス。

BBB は、サイト ID

例：「192.168.0.100_001」

(5) IP アドレスを変更する

ネットワークインターフェース設定コマンド（3.7.7 章）を参照し、該当 NQ の IP アドレスを変更する。

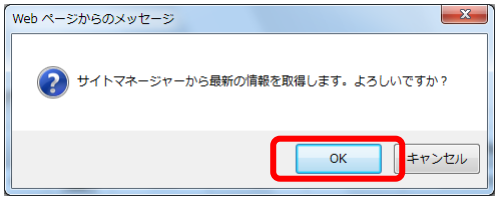
(6) NQ を再起動する

再起動コマンド（3.7.13 章）を参照し、NQ を再起動する。

(7) SiteManager の最新情報を取得する

NQ が起動したら、DomainManager 集中管理画面の「コンポーネント管理」->「サイトマネージャ」より SiteManager の最新情報を取得する。

このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



(8) データ収集を開始する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」に IP アドレス変更後のエージェント情報が表示されたらデータ収集を開始する。

(9) 不正接続防止を開始する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」より該当 NQ の不正接続防止を開始する。

8.4 USB メモリを使用した NQ の設定内容の確認方法

(1) USB メモリに設定ファイルを作成する

USB メモリのルートフォルダに設定ファイルを作成してください。設定ファイルの作成方法は、2.2.2 章～2.2.4 章を参照してください。

(2) USB メモリを差込み、NQ を起動する

設定ファイルを保存した USB メモリを NQ 筐体へ接続してください。接続完了後、電源ケーブルを NQ 筐体およびコンセントへ差し込むことにより、自動起動します。

但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

なお、USB メモリから設定ファイルを認識させることができるのは、起動時のみです。NQ の起動後に筐体へ USB メモリを接続しても、設定ファイルを認識させることはできませんので注意してください。

(3) USB メモリに作成されたテキストファイルで NQ の設定状態を確認する

起動から約 1 分経過後、NQ 筐体から USB メモリを取り外し、USB メモリを PC に接続してください。NQ が USB メモリを正常に認識できた場合(※1)は、USB メモリのルートフォルダにテキストファイル（svconflog.txt）が作成されます。このテキストファイルに NQ の設定状態が出力(※2)されていますので確認してください。

(※1)テキストファイルが作成されない場合、NQ と USB メモリの相性が悪い、NQ が暗号化 USB メモリに対応していない、NQ30c、NQ30d に USB2.0 以外の USB メモリが使用されているなどが原因で、認識できていない可能性があります。

(※2)エージェント設定確認コマンド（list na）(3.7.5 章参照)、ネットワークインターフェース確認コマンド（list if）(3.7.3 章参照)、ネットワークインターフェースのネゴシエーション設定確認コマンド（list ifspeed)、「DNS サーバアドレス、ドメイン名確認コマンド（list ns）(3.7.4 章参照）の実行結果が出力されます。

8.5 Apple 社製端末を監視対象にする場合の設定必須パラメータ

DHCP クライアントの Apple 社製端末が不正接続防止された場合、Apple 社製端末が DHCP の

IP アドレスを繰り返し要求してしまうため、DHCP のアドレスプールが枯渇してしまうことがあります。本現象を回避するためには、「DisableBroadCastJamArp」を「1」に設定してください。「DisableBroadCastJamArp」については、「7.5 各環境共通の設定可能パラメータ」を参照してください。

8.6 Linux 系 OS 端末を監視対象にする場合の設定必須パラメータ

Linux 系 OS 等、ARP エントリ更新のロックタイムが設定されている OS の場合、NQ からの偽装 ARP を受け付けないように動作し、不正接続防止が正常に行なわれないことがあります。ARP エントリの偽装を有効にするために「SendArpDelay」を設定してください。このパラメータの設定値を OS のロックタイムより長い秒数にすることで ARP エントリの偽装が有効になります。 「SendArpDelay」については、「7.5 各環境共通の設定可能パラメータ」を参照してください。

8.7 携帯端末を監視対象にする場合の設定必須パラメータ

・Apple 社製の携帯端末の場合
「8.5 Apple 社製端末を監視対象にする場合の設定必須パラメータ」に記載している設定を行なってください。

・Android 系の携帯端末の場合
「8.6 Linux 系 OS 端末を監視対象にする場合の設定必須パラメータ」に記載している設定を行なってください。

8.8 IPv6 アドレスを防止するには？

IPv6 での通信を防止するためには以下の設定を行ってください。
また、設定変更後はサービスの再起動を行ってください。

・無条件に IPv6 通信を防止したい
IPv6 での通信を防止したい場合には「PreventIPv6AllAddr」を「1」に設定してください。
本設定を行うことにより、IPv6 での通信を無条件に防止します。
IPv4 での通信は承認ポリシーに従い防止しますので承認ポリシー変更などの作業は必要ありません。

・承認リストを設定して IPv6 通信を防止したい
承認リストを設定して IPv6 通信を防止したい場合には「EnableIPv6」を「On」に設定してください。本設定を行うことにより、承認リストに従って IPv6 での通信を防止することができます。

承認リストの設定方法については「InfoCage 不正接続防止 集中管理運用マニュアル」および「InfoCage 不正接続防止 分散管理運用マニュアル」を参照してください。

設定の組み合わせによる挙動を以下に記載します。

PreventIPv6AllAddr	EnableIPv6	挙動
0	Off	IPv6 での通信は防止しません。
1	Off	IPv6 での通信を無条件で防止します。
0	On	承認ポリシーに従い IPv6 での通信を防止します。

(※) PreventIPv6AllAddr:1、EnableIPv6:On を同時に利用することはできません。

・IPv6 アドレス通信が正常に不正接続防止出来ないケース

NQ30c、NQ30d が送信する偽装 ICMPv6 応答パケット(Neighbor Advertisement)が、不正端末の通信先端末からの ICMPv6 応答パケットより先に届くことにより、不正端末が正常に防止されないことがあります。

ホスト台数が少ない環境で、この現象が発生する場合は、「SendNdpWaitTime」を設定してください。

8.9　NA から NQ への移行手順

NA から NQ への移行手順は以下の通りです。

【前提条件】

・NA と NQ のバージョンは同一バージョン

・エージェント名と IP アドレスが異なる場合のみ対応可能

エージェント名及び IP アドレスの変更を行う場合は本手順実施後に[8.3 使用中の NQ のエージェント名、IP アドレスを変更する方法]を参照して変更作業を行ってください。

・ホスト情報の移行のみ可能

エージェントに対する設定はデータ移行後に実施してください。

8.9.1　分散管理モードの場合

(1) 不正接続防止、データ収集を停止する

サイトコンソール画面より不正接続防止、データ収集を停止します。

(2) NA のサービスを停止する

NetworkAgent サービスを以下の手順で停止する。

Windows の[スタート]ボタン→（設定→）コントロールパネル→管理ツール→サービス →[SecureVisor NetworkAgent]を選択し、サービスを停止。

(3) NQ をネットワークに接続し、電源を入れる

NQ がサイトマネージャと通信不可能な場合は 2.2 章又は 2.3 章を参照してネットワークの設定を行ってください。

(4) サイトコンソールに NQ が登録されたらサイトマネージャのサービスを停止する

NQ の接続先に設定されている SiteManager サービスを以下の手順で停止する。

Windows の[スタート]ボタン→（設定→）コントロールパネル→管理ツール→サービス →[SecureVisor SiteManager]を選択し、サービスを停止。

(5) データを移行する

サイトマネージャが保持するデータを移行します。

移行元 NA から移行先 NQ へデータをコピーします。

【移行元 NA】

・{SiteManager インストールフォルダ}¥Data¥AgentList¥{NA 名}¥DailyData

・{SiteManager インストールフォルダ}¥Data¥AgentList¥{NA 名}¥HostList

【移行先 NQ】

・{SiteManager インストールフォルダ}¥Data¥AgentList¥{NQ 名}¥DailyData

・{SiteManager インストールフォルダ}¥Data¥AgentList¥{NQ 名}¥HostList

(6) サイトマネージャのサービスを開始する

NQ の接続先に設定されている SiteManager サービスを以下の手順で開始する。

Windows の[スタート]ボタン→（設定→）コントロールパネル→管理ツール→サービス → [SecureVisor SiteManager]を選択し、サービスを開始。

(7) サイトコンソールから NA を削除する

サイトコンソール画面より古い NA を削除します。削除する時に「[{NA 名}]と通信できません。(E02000)削除処理を続けますか？」というメッセージが表示された場合は、[はい]を選択してください。

(8) サイトコンソールからホスト一覧を保存する

サイトコンソール画面より移行先エージェントを選択してホスト一覧を表示します。ホスト一覧表示後に[保存]を実行してください。

(9) NQ の設定を変更する

2.2 章又は 2.3 章を参照して NQ の設定を行ってください。

除外アドレスを設定している場合は、サイトコンソールのホスト一覧から再度除外アドレスを設定してください。

(10) データ収集を開始する

サイトコンソール画面より「新規ホストの状態（色）設定」を確認してください。設定が問題ない場合はデータ収集を開始してください。

(11) 不正接続防止を有効にする

サイトコンソール画面より移行先エージェントを選択してホスト一覧を表示します。ホスト一覧の状態（赤/黄/青）を確認してください。特に SM の状態が（青）になっていることを確認してください。確認できましたら、不正接続防止を有効にしてください。

8.9.2　集中管理モードの場合

(1) 不正接続防止、データ収集を停止する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」より不正接続防止、データ収集を停止します。

(2) ホストデータのバックアップを取得する

ホストエクスポートコマンドを使用してホストデータをバックアップします。

※ホストエクスポートコマンドについてはドメインマネージャオンラインヘルプの「ホス

ト情報のエクスポートコマンドについて」を参照してください。

(3) NA のサービスを停止する

NetworkAgent サービスを以下の手順で停止する。

Windows の[スタート]ボタン→(設定→)コントロールパネル→管理ツール→サービス →[SecureVisor NetworkAgent]を選択し、サービスを停止。

(4) NQ をネットワークに接続し、電源を入れる

NQ がサイトマネージャと通信不可能な場合は 2.2 章又は 2.3 章を参照してネットワークの設定を行ってください。

(5) サイトコンソールから NA を削除する

サイトコンソール画面より古い NA を削除します。削除する時に「[{NA 名}]と通信できません。(E02000)削除処理を続けますか？」というメッセージが表示された場合は、[はい]を選択してください。

(6) RCV ファイルを Backup フォルダへ移動する

DomainManager より NA を管理する SiteManager の最新 RCV ファイルを Backup フォルダへ移動します。

【RCV ファイル保存場所】

{DomainManager インストールフォルダ}¥RecvData¥AAA_BB_YYYYMMDDHHMMSS.RCV

【移動先フォルダの場所】

{DomainManager インストールフォルダ}¥Backup¥AAA_BBB

※ AAA は、SiteManager の IP アドレス。
BBB は、サイト ID
YYYYMMDDHHMMSS は、日時
例：「192.168.0.100_001_20080824.RCV」

(7) SiteManager の最新情報を取得する

DomainManager 集中管理画面の「コンポーネント管理」->「サイトマネージャ」より SiteManager の最新情報を取得します。

「サイトマネージャーから最新の情報を取得します。よろしいですか？」というダイアログが表示された場合は[OK]ボタンを押してください。

(8) NQ の設定を変更する

2.2 章又は 2.3 章を参照して NQ の設定を行ってください。

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」より NQ の設定を行ってください。

※特に「新規ホストの状態（色）設定」を確認してください。

(9) ホストデータを編集する

(2)でバックアップしたホストデータを編集します。ホストデータファイルを開き、エージェント名列の{NA 名}を{NQ 名}に変更します。変更後は保存してください。

※ホストデータファイルについては「ホスト情報のインポートコマンドについて」を参照してください。

(10) ホストデータをリストアする

ホストインポートコマンドを使用して(9)で編集したホストデータをリストアします。

※ホストインポートコマンドについてはドメインマネージャオンラインヘルプの「ホスト情報のインポートコマンドについて」を参照してください。

(11) データ収集を開始する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」よりデータ収集を開始してください。

(12) 不正接続防止を有効にする

DomainManager 集中管理画面の「ホスト管理」->「ホスト検索」->「ホスト情報一覧画面」にてホスト一覧の状態（赤/黄/青）を確認してください。特に SM の状態が（青）になっていることを確認してください。確認できましたら、不正接続防止を有効にしてください。

(13) 古い NA を削除する

DomainManager 集中管理画面の「コンポーネント管理」->「エージェント」より古い NA を削除します。削除する時に「選択されたエージェント情報を削除します。よろしいですか？」というメッセージが表示された場合は、[OK]を選択してください。

8.10 バージョンアップ後のパラメータ設定を事前に実施する手順

NQ30c では、V3.8(工場出荷状態)の時点で USB メモリによる V3.9 以降に追加されたパラメータの設定が可能です。

(1) USB メモリに設定ファイルを作成する
USB メモリに作成する設定ファイルに V3.8 に対するパラメータ及び V3.9 以降に追加された対するパラメータを記述します。
本バージョンに自動バージョンアップ後に設定するパラメータは V3.9 以降に追加されたパラメータのみとなります。V3.9 以降に追加されたパラメータは「7 NQ のパラメータ詳細」の備考欄を参照してください。

(2) USB メモリを差込み、NQ を起動する
V3.8 に対するパラメータ設定が行われます。

(3) USB メモリを NQ から抜く

(4) 自動バージョンアップする

(5) 自動パラメータ設定
V3.9 以降に対するパラメータが自動で設定されます。

[注意]
- (2)-(5)の作業が完了するまでの間、NQ を再起動しないでください。
- パスワードの変更は(1)の作業の前か(5)の作業の後に行ってください。
- NQ30d の場合は V5.2(工場出荷状態)の時点で全てのパラメータが設定可能のため、本機能は動作しません。

8.11 NQ が送信するパケットを抑制するには？

NQ はホストの情報を取得するため、監視しているホストに対して下記のパケットを送信します。

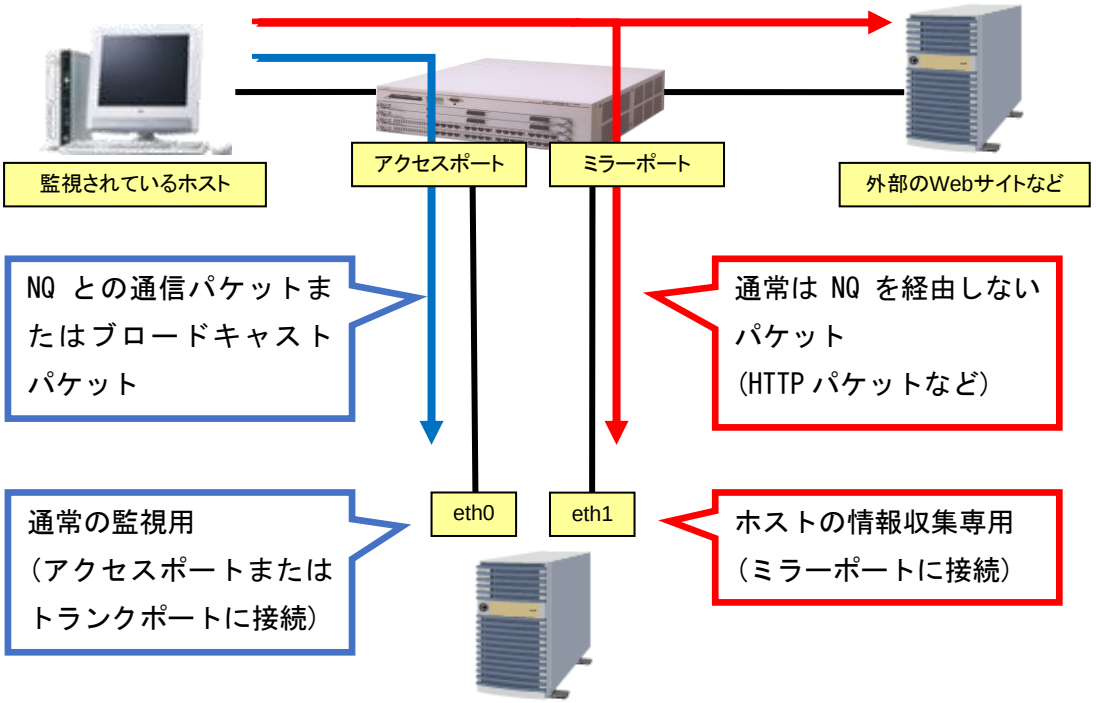
- NetBIOS パケット
  ホスト名やログイン名を取得するために送信します。
- DNS パケット
  ホストの DNS 名解決のために送信します。
- SMB パケット
  ホストの OS 種別を判別するために送信します。
- TCP パケット
  ホストの OS 種別を判別するために送信します。

「OS デテクト機能」を無効にすることで、上記のパケット送信を抑制することができます。
「OS デテクト機能」の無効化については「7.5 各環境共通の設定可能パラメータ」の「OsDetect」の項を参照してください。

なお、「OS デテクト機能」を無効にした場合でも、ミラーポートを使用してホスト情報を収集することで、ユーザーエージェント情報からホストの OS 種別を判別することが可能になります。
ミラーポートを使用したホスト情報の収集については「8.12 ミラーポートを使用してホスト情報を収集するには？」を参照してください。

8.12 ミラーポートを使用してホスト情報を収集するには？

NetworkAgent(Linux)は 2 つのネットワークインターフェースのうち片方を通常の監視用(MonitoringIf)に設定し、もう片方をミラーポートに接続してホストの通信パケットを監視することで、通常の監視時には取得できない NetworkAgent(Linux)を経由しないパケットも監視することが可能になります。



ミラーポートを使用することで下記が可能になります。

- ユーザーエージェント情報の取得
  ユーザーエージェント情報によりホストの OS 種別を判別することができます。
  ※ ミラーポートを使用しない場合は不正接続防止されたホストしかユーザーエージェント情報を取得できません。

- アクセスログの出力
  ホストの通信を監視し、アクセスログを出力することが可能になります。
  ※ ミラーポートを使用しない場合は NQ を経由しない通信(Web アクセスなどほとんどの通信)のアクセスログを出力することができません。

ミラーポートを使用してホスト情報を収集するには、下記を実施してください。

(1) スイッチにミラーポートを設定する。
スイッチにミラーポートを設定し、NQ が監視する端末の通信パケットが送受信されるポートのパケットが送信されるように設定してください。

(2) NetworkAgent(Linux)に、ミラーポートに接続するインターフェースを設定する。
「7.7 NQ30d のみに有効な設定可能パラメータ」の「InfoCollectIf」の項を参照してミラーポートに接続するインターフェースを NetworkAgent(Linux)に設定します。

(3) NetworkAgent(Linux)をアクセスポートとミラーポートに接続する。
通常の監視用インターフェースをアクセスポート(タグ VLAN 環境の場合はトランクポート)に接続、InfoCollectIf に指定したポートをスイッチのミラーポートに接続し、NetworkAgent(Linux)サービスを起動します。

8.13 アクセスログを取得するには？

8.13.1 概要

NQ30d は監視しているホストが送信するパケットをもとにアクセスログを出力できます。

またNetworkAgent(Linux)の場合は､2つあるネットワークインターフェースのうち片方を通常の監視用、もう片方をミラーポートに接続し監視しているホストの通信パケットをNetworkAgent(Linux)で監視することで､通常の監視時には取得できないブロードキャスト以外の通信パケットについてもアクセスログを出力することが可能になります。
ミラーポートを使用しない場合は通常の監視用ネットワークインターフェースで取得できるパケット(主にARPリクエストパケット)のみアクセスログを出力することができます。

8.13.2 ログの種類と出力内容

8.13.2.1 ARPログ

ARPリクエストパケットの情報を出力します。
このログにより、監視対象のホストが同じセグメント内のどのホストと通信しようとしたかを記録することができます。

出力フォーマット

```
検出日時 ARP Host=送信元ホスト名 Src=送信元IP(送信元MAC) Dst=送信先IP
```

検出日時:検出したパケットの受信時刻(YYYY/MM/DD hh:mm:ss形式)
送信元ホスト名:送信元ホストのホスト名
送信元MAC：送信元ホストのMACアドレス
送信元IP：送信元ホストのIPアドレス
送信先IP：送信先ホストのIPアドレス

出力例

```
2015/10/07 12:02:45 ARP Host=TestHost Src=192.168.1.1(00:11:22:33:44:55)
Dst=192.168.1.2
```

8.13.2.2 HTTP ログ

HTTP リクエストパケット(GET)の情報を出力します。
このログにより､監視対象のホストがどの URL に接続しようとしたかを記録することができます。

出力フォーマット

検出日時 HTTP Host=送信元ホスト名 Src=送信元 IP:送信元ポート番号 Dst=送信先 IP:送信先ポート番号 URL=URL

検出日時:検出したパケットの受信時刻(YYYY/MM/DD hh:mm:ss 形式)
送信元ホスト名:送信元ホストのホスト名
送信元 IP:送信元ホストの IP アドレス
送信元ポート番号:送信元ホストのポート番号
送信先 IP:送信先ホストの IP アドレス
送信元ポート番号 : 送信先ホストのポート番号
URL:ホストがアクセスしようとした URL

出力例

2015/10/07 12:02:45 HTTP Host=TestHost Src=192.168.1.1:65432 Dst=118.215.181.189:80 URL=http://jpn.nec.com/infocage/prevention/

8.13.2.3 SMB ログ

SMB(Windows ファイル共有)パケットの情報を出力します。
このログにより、監視対象のホストがどのファイルにアクセスしようとしたかを記録することができます。

出力フォーマット

検出日時 SMB Host=送信元ホスト名 Src=送信元 IP:送信元ポート番号 Dst=送信先 IP:送信先ポート番号 File=ファイル名

検出日時:検出したパケットの受信時刻(YYYY/MM/DD hh:mm:ss 形式)
送信元ホスト名:送信元ホストのホスト名
送信元 IP:送信元ホストの IP アドレス
送信元ポート番号:送信元ホストのポート番号
送信先 IP:送信先ホストの IP アドレス
送信先ポート番号 : 送信先ホストのポート番号

File:ホストがアクセスしようとしたファイル名

出力例

```
2015/10/07 12:02:45 SMB Host=TestHost Src=192.168.1.1:65432 Dst=192.168.10.1:445
File=test.txt
```

8.13.2.4 UDP

UDP パケットの情報を出力します。
このログにより、監視対象のホストがどのホストとデータを送受信したかを記録することができます。

出力フォーマット

```
検出日時 UDP Src=送信元 IP:送信元ポート番号 Dst=送信先 IP:送信先ポート番号
```

検出日時:検出したパケットの受信時刻(YYYY/MM/DD hh:mm:ss 形式)
送信元 IP:送信元ホストの IP アドレス
送信元ポート番号:送信元ホストのポート番号
送信先 IP:送信先ホストの IP アドレス
送信先ポート番号：送信先ホストのポート番号

出力例

```
2015/10/07 12:02:45 UDP Src=192.168.1.1:65432 Dst=192.168.10.5:55544
```

8.13.2.5 TCP

TCP コネクションの開始と終了を記録します。
このログにより、監視対象のホストがどのホストと接続したか(接続された場合も含む)を記録することができます。

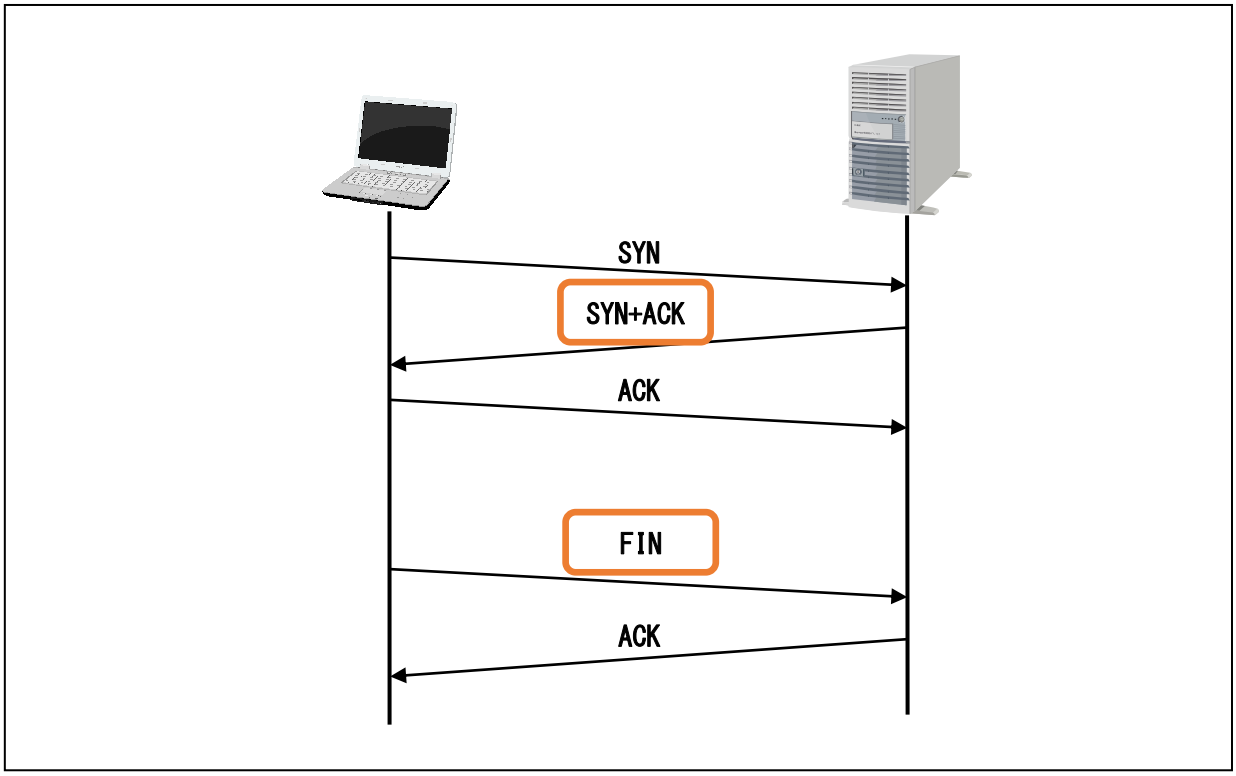
出力フォーマット

```
検出日時 UDP Src=送信元 IP:送信元ポート番号 Dst=送信先 IP:送信先ポート番号
```

検出日時:検出したパケットの受信時刻(YYYY/MM/DD hh:mm:ss 形式)
Status: SYN+ACK の場合は Connect、FIN の場合は DisConnect を出力

送信元 IP:送信元ホストの IP アドレス
送信元ポート番号:送信元ホストのポート番号
送信先 IP:送信先ホストの IP アドレス
送信先ポート番号：送信先ホストのポート番号

※ 送信元と送信先について
TCP コネクションを開始したホストを「送信元」、接続先のホストを「送信先」として IP アドレスとポート番号を出力します。



そのため、Status が Connect(SYN+ACK)の場合は送信元と送信先を実際のパケットとは入れ替えて出力します。

- Status が Connect(SYN+ACK)の場合

接続元 IP とポート番号: **送信先**の IpAddress とポート番号
接続先 IP とポート番号: **送信元**の IpAddress とポート番号

- Status が DisConnect(Fin)の場合

接続元 IP とポート番号: 送信元の IpAddress とポート番号
接続先 IP とポート番号: 送信先の IpAddress とポート番号

出力例

```
2015/10/07 12:02:45 TCP[Connect] Src=192.168.1.1:65432 Dst=192.168.10.5:55544
```

8.13.3　設定

アクセスログを取得するには下記手順を実施してください。

(1) 「8.12 ミラーポートを使用してホスト情報を収集するには？」を参照し、ミラーポートからホストの通信パケットを収集できるように設定してください。

(2) 「7.7 NQ30d のみに有効な設定可能パラメータ」の「AccessLog」「AccessLogType」の項を参照し、アクセスログ収集機能を有効化してください。

(3) 必要に応じて「7.7 NQ30d のみに有効な設定可能パラメータ」の「RestAccessLog」「AccessLogMaxCnt」「AccessLogSize」の項を参照し、各パラメータの設定値を変更してください。

8.13.4　ログ取得方法

NQ 内に出力されているアクセスログを取得するには、下記手順を実施してください。

(1) コマンドプロンプトを起動し、下記いずれかのフォルダに移動してください。
- {DomainManager インストールフォルダ}¥Bin
- {SiteManager インストールフォルダ}¥Bin
- {リモートコンソールインストールフォルダ}¥Bin
- {SvTools インストールフォルダ}

(2) SvGetLogFile.exe コマンドを実行して、アクセスログファイルをコマンドの実行 PC 上に保存してください。
下記オプションを指定して SvGetLogFile.exe コマンドを実行してください。

“-g Log/AccessLog/* -t rp”
実行例) SvGetLogFile.exe -i 192.168.250.250 -p 23491 -g Log/AccessLog/* -t rp

8.13.5　ログ出力の抑制

8.13.5.1 概要

ネットワーク上に多数のホストがある環境で全てのアクセスログを出力すると、短期間でアクセスログの最大保持数に達してしまい必要なアクセスログが保持できなくなる可能性があります。そのような場合はログ出力の抑制機能を使用して、同じアクセスログの出力を行わないようにすることで、出力数を削減し長期間アクセスログを保持することが可能になります。

8.13.5.2 設定

アクセスログの抑制機能を使用するには、「7.7 NQ30d のみに有効な設定可能パラメータ」の「RestAccessLog」項を参照してアクセスログの抑制機能を有効化してください。

8.13.5.3 動作説明

アクセスログの種類ごとに、下記の条件が一致するアクセスログは同じログとみなし、2 回目以降は出力を行わなくなります。

ログの種類	一致条件
ARP ログ	送信元 IP、送信先 IP
HTTP ログ	送信元 IP、送信先 IP、URL
SMB ログ	送信元 IP、送信先 IP、ファイル名
UDP ログ	送信元 IP、送信先 IP、
TCP ログ	送信元 IP、送信先 IP

上記の条件が一致しない異なるアクセスログ件数がアクセスログ抑制データ件数の閾値(初期値 50 万件)を超過すると、古いアクセスログ抑制データから順に 1/5 が削除されます。
その場合、削除されたアクセスログ抑制データに該当するパケットを受信したタイミングで再度同じアクセスログが出力されます。

8.13.6　目的別の設定方法

目的に応じて下記のような設定を行ってください。

- ファイルサーバーやWebへのアクセスを記録する

Windows ファイル共有によるファイルサーバーへのアクセスと任意の Web へのアクセスを記録する場合は、SMB ログと HTTP ログの記録を有効にします。

- 実際に接続した通信のみ記録する

接続できなかった通信については記録不要で、実際に接続が成功した通信のみ記録する場合は、TCP ログの記録を有効にします。

- ホストの全ての通信をネットワークレベル(TCP/UDP)で記録する

TCP/IP またはUDP/IP の全ての通信を記録する場合は、TCP ログと UDP ログの記録を有効にします。また、ARP ログを有効にすることで、同じセグメント内に閉じた通信であっても、どのホストに接続しようとしたかを出力できます。

- セグメント内の通信のみ記録する

L3 スイッチ/ルータを経由する通信は L3 スイッチ/ルータで記録しており、セグメント内通信の記録のみが必要な場合は、ARP ログの記録を有効にします。
この場合、エージェントをミラーポートに接続する必要はありません。

8.14 スリープ中の黄色のホストが防止される場合の対応

OS/ドライバの設定によっては、スリープ中のホストが NQ からの ARP リクエストに応答し、ARP リプライを返す場合があります。その場合、スリープ中のため PC 管理製品からの存在通知パケットが送信されないにもかかわらず、ホストはネットワーク上に接続し続けていると判断されます。そのため、接続防止猶予時間以上スリープ状態が続くと、そのホストはスリープ中にもかかわらず防止されます。

この問題を回避するには「7.7 NQ30d のみに有効な設定可能パラメータ」の「NoUpdArpReply」の項を参照して NQ 宛の ARP 応答パケットを無視するように設定してください。

8.15 監視メッセージを syslog に出力するには？

NQ30d では以下のアラートを発行するタイミングで該当アラートのログを syslog に出力することが可能です。

8.15.1 出力するログの種類

- 不正接続防止

NQ がホストの接続防止を実行したタイミングで出力します。
不正接続防止が継続している場合、1 時間ごとに出力します。

出力例）

```
2016/03/01 10:10:10 M10008 不正接続を防止しました。00:11:22:33:44:55, 192.168.1.1, eth0
```

- 不正接続防止終了

NQ がホストの接続防止を終了したタイミングで出力します。

出力例）

```
2016/03/01 10:10:10 M10008 不正接続防止を終了しました。 00:11:22:33:44:55, 192.168.1.1,
```

- 承認申請許可

NQ がホストの承認申請を許可したタイミングで出力します。

出力例）

```
2016/03/01 10:10:10 M10008 申請許可により不正接続防止を解除しました。
00:11:22:33:44:55, 192.168.1.1, eth0
```

- 新規ホスト発見

NQ が各ホストを、その日最初に検知したタイミングで出力します。
通常のアラートと異なり、日付が変わると前日検知したホストであっても再度出力します。

出力例）

```
2016/03/01 10:10:10 M10001 新規ホストを発見しました。00:11:22:33:44:55, 192.168.1.1,
```

8.15.2 設定

監視メッセージの syslog 出力機能を使用するには、「7.7 NQ30d のみに有効な設定可能パラメータ」の「SyslogOutMsg」の項を参照して機能を有効化してください。

また、syslog の転送を行う場合は、「SyslogFwdMsgHost」の項を参照して設定してください。

8.15.3 仕様

- 出力するメッセージの facility は user、serverity は info 固定です。
- syslog 転送先のポート番号は 514/UDP 固定です。

9　NQ の交換手順

工場出荷時の NQ は以下の通り、暫定的なバージョンの NetworkAgent がプリインストールされています。

製品名	製品型番	バージョン
InterSec/NQ30a	N8100-1110Q	2.2g
InterSec/NQ30b	N8100-1200Q	2.2h
	N8100-1300Q	3.1g
InterSec/NQ30c	N8100-1400Q	2.2-3.8(※1)
InterSec/NQ30d	N8100-1500Q	2.2-5.2(※2)

（※1）バージョン 2.2 から 3.8 に対応するモジュールがプリインストールされています。
（※2）バージョン 2.2 から 5.2 に対応するモジュールがプリインストールされています。

NQ 交換後、新しい NQ にインストールされている NetworkAgent のバージョンが古い場合は、SiteManager オンラインヘルプの、[InfoCage 不正接続防止]->[InfoCage 不正接続防止その他の機能]->[エージェントの自動バージョンアップ機能]を参照してバージョンアップを行ってください。(※)
（※）InterSec/NQ30d の場合、工場出荷時の状態でも V5.2 に対する必要な設定が可能ですので、初期設定時に SiteManager と通信するために必要な設定と、V5.2 に対する必要な設定を実施するだけで、運用が開始できます。

NQ 交換時は、必ずエージェント名は同一のままで実施してください。また、運用モードにより手順が異なりますので、以下を参照し、利用する運用モードに応じた手順で実施してください。

なお、NQ 交換後のエージェント名を変更したい場合は 8.3 章を参照してください。

9.1　分散管理モードの場合

(1) 故障した NQ をネットワークから切り離す

(2) 故障した NQ の情報をバックアップする

以下のマニュアルを参照し、故障した NQ の情報をバックアップ(※)する。

「分散管理運用マニュアル」

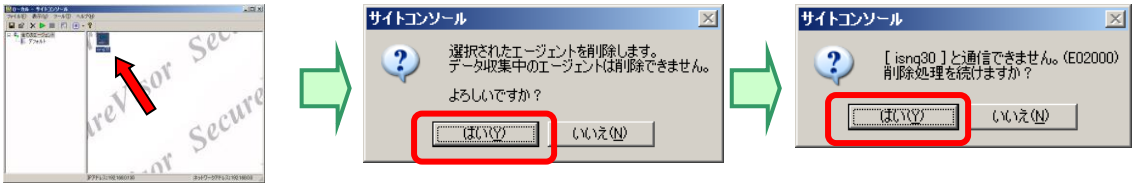
「エージェント情報のバックアップ」

(※)バックアップコマンド実行時、[-a]オプションを指定して実行し、故障した NQ の情報をバックアップしてください。

(3) 故障した NQ のアイコンを削除する

サイトコンソールを起動し、故障した NQ のアイコンを削除する。

※NQ と通信できない旨のメッセージが表示されますが、そのまま削除してください。



(4) NQ をネットワークに接続する

新しい NQ に初期設定(※)を行った後、ネットワークに接続する。

(※)エージェント名を交換前と同一のエージェント名を設定してください。

「CollectOfPacket」に「Off」を設定してください。

「JamStatus」に「Off」を設定してください。

(5) NQ が登録されたことを確認する

サイトコンソールを起動し、該当 NQ のエージェントが灰色の状態で登録されていることを確認する。

(6) 故障した NQ の情報をリストアする

サイトコンソールを起動し、該当 NQ のエージェントが灰色の状態で登録されていることを確認する。

以下のマニュアルを参照し、故障した NQ の情報をリストア(※)する。

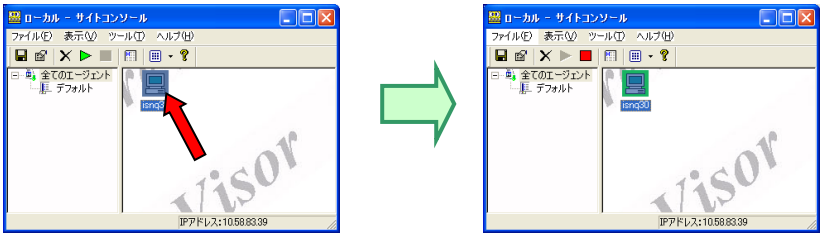
「分散管理運用マニュアル」

「エージェント情報のリストア」

(※)リストアコマンド実行時、[-stop]オプションを指定して実行し、「データ収集」、「不正接続防止」が停止した状態でリストアしてください。

(7) データ収集を開始する

リストア後 NQ の再起動が完了したら、サイトコンソールを起動し、該当 NQ のデータ収集を開始する。

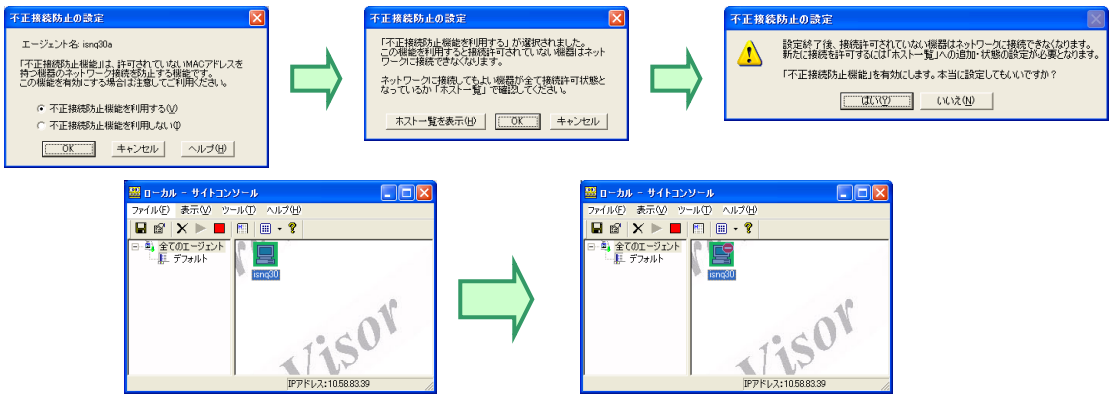


(8) 新 NQ が検知され、接続許可として登録されていることを確認する

ホストー覧を起動し、新 NQ が「青」として登録されていない場合は、「青」に変更して保存する。

(9) 不正接続防止機能を開始する

サイトコンソールを起動し、[ファイル]-[不正接続防止の設定]から該当 NQ の不正接続防止機能を開始する。



9.2　集中管理モードの場合

(1) 故障した NQ をネットワークから切り離す

(2) 不正接続防止機能、データ収集を停止する

DomainManager の集中管理画面から該当 NQ の不正接続防止機能、データ収集を停止する。

(a) 不正接続防止、およびデータ収集を停止する権限のあるユーザで集中管理機能にログインする。

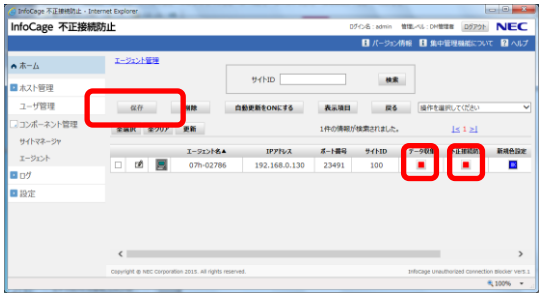
(b) [メニュー画面]で[コンポーネント管理]->[エージェント]ボタンをクリックする。
（ドメイン・サイト・エージェント管理の場合）
[メニュー画面]で[グループ管理]->[VLAN グループ]ボタンをクリックする。
（VLAN グループ管理の場合）

(c) 表示された［メニュー ＞ コンポーネント管理 ＞ エージェント］画面で［検索］ボタンをクリックする。
（ドメイン・サイト・エージェント管理の場合）

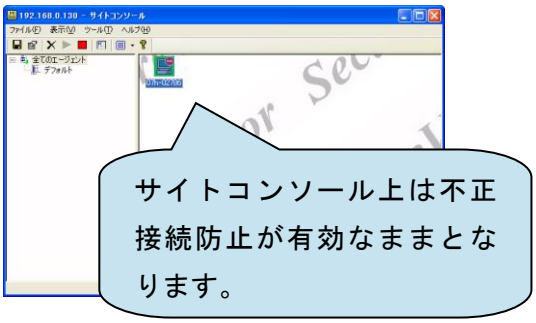
(d) 該当 NQ の［不正接続防止］の  アイコンを２回クリックする。

(e) 該当 NQ の［データ収集］の  アイコンをクリックする
（(d)(e)それぞれのアイコンが  に変わる）。

(f) 設定を反映させるため、[保存]ボタンをクリックする。



このとき、SiteManager のコンソール画面では、右図のような状態となります。



(3) 故障した NQ の情報をバックアップする

以下のマニュアルを参照し、故障した NQ の情報をバックアップ(※)する。

「集中管理運用マニュアル」

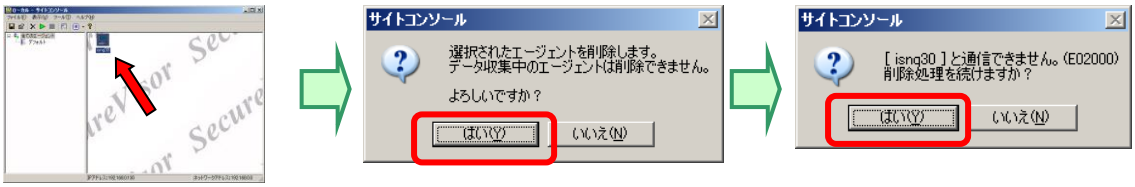
「エージェント情報をバックアップする」

(※)バックアップコマンド実行時、[-a]オプションを指定して実行し、故障した NQ の情報をバックアップしてください。

(4) 故障した NQ のアイコンを削除する

サイトコンソールを起動し、故障した NQ のアイコンを削除する。

※NQ と通信できない旨のメッセージが表示されますが、そのまま削除してください。



(5) NQ をネットワークに接続する

新しい NQ に初期設定(※)を行った後、ネットワークに接続する。

(※)エージェント名を交換前と同一のエージェント名を設定してください。

「CollectOfPacket」に「Off」を設定してください。

「JamStatus」に「Off」を設定してください。

(6) NQ が登録されたことを確認する

サイトコンソールを起動し、該当 NQ のエージェントが灰色の状態で登録されていることを確認する。

(7) 故障した NQ の情報をリストアする

サイトコンソールを起動し、該当 NQ のエージェントが灰色の状態で登録されていることを確認する。

以下のマニュアルを参照し、故障したエージェントの情報をリストア(※)する。

「集中管理運用マニュアル」

「エージェント情報をリストアする」

(※)リストアコマンド実行時、[-stop]オプションを指定して実行し、「データ収集」、「不正接続防止」が停止した状態でリストアしてください。

(8) データ収集を開始する

DomainManager の集中管理画面から該当 NQ のデータ収集を開始する。

(a) データ収集を開始する権限のあるユーザで集中管理機能にログインする。

(b) [メニュー画面] で[コンポーネント管理]->[エージェント]ボタンをクリックする。

(ドメイン・サイト・エージェント管理の場合)

[メニュー画面]で[グループ管理]->[VLAN グループ]ボタンをクリックする。

(VLAN グループ管理の場合)

(c) 表示された [メニュー > コンポーネント管理 > エージェント] 画面で [検索] ボタンをクリックする。

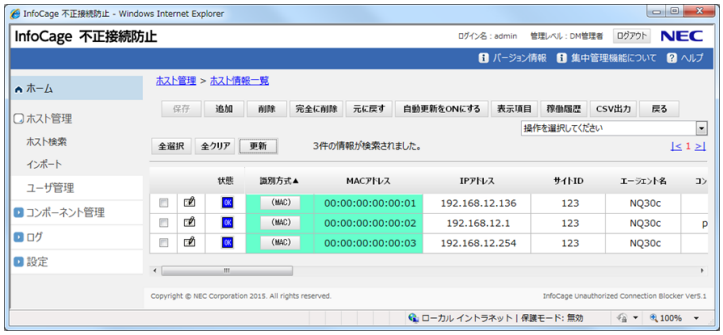
（ドメイン・サイト・エージェント管理の場合）

(d) 復旧した NQ［データ収集］の ■ アイコンをクリックする
（アイコンが ▶ に変わる）。

(e) 設定を反映させるため、[保存]ボタンをクリックする。

(9) 新 NQ が検知され、接続許可として登録されていることを確認する

ホスト情報一覧を起動し、新 NQ が「青」として登録されていない場合は、「青」に変更して保存する。



(10) 不正接続防止機能を開始する

DomainManager の集中管理画面から該当 NQ の不正接続防止機能を開始する。

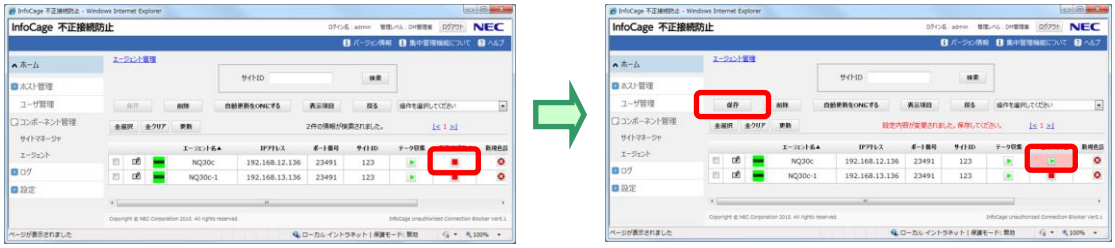
(a) 不正接続防止を開始する権限のあるユーザで集中管理機能にログインする。

(b) ［メニュー画面］で[コンポーネント管理]->[エージェント]ボタンをクリックする。
（ドメイン・サイト・エージェント管理の場合）
[メニュー画面]で[グループ管理]->[VLAN グループ]ボタンをクリックする。
（VLAN グループ管理の場合）

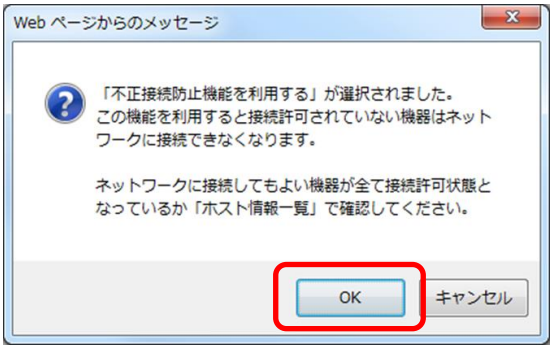
(c) 表示された［メニュー ＞ コンポーネント管理 ＞ エージェント］画面で［検索］ボタンをクリックする。
（ドメイン・サイト・エージェント管理の場合）

(d) 該当 NQ の［不正接続防止］の ■ アイコンをクリックする
（アイコンが ▶ に変わる）。

(e) 設定を反映させるため、[保存]ボタンをクリックする。



このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



10 その他

10.1 InfoCage 不正接続防止の最新情報

InfoCage 不正接続防止に関する最新情報は、下記のウェブサイトを参照してください。

http://www.nec.co.jp/cced/infocage/n_prevention/index.html

～以上～