XR 検疫管理サービス

ユーザーズガイド

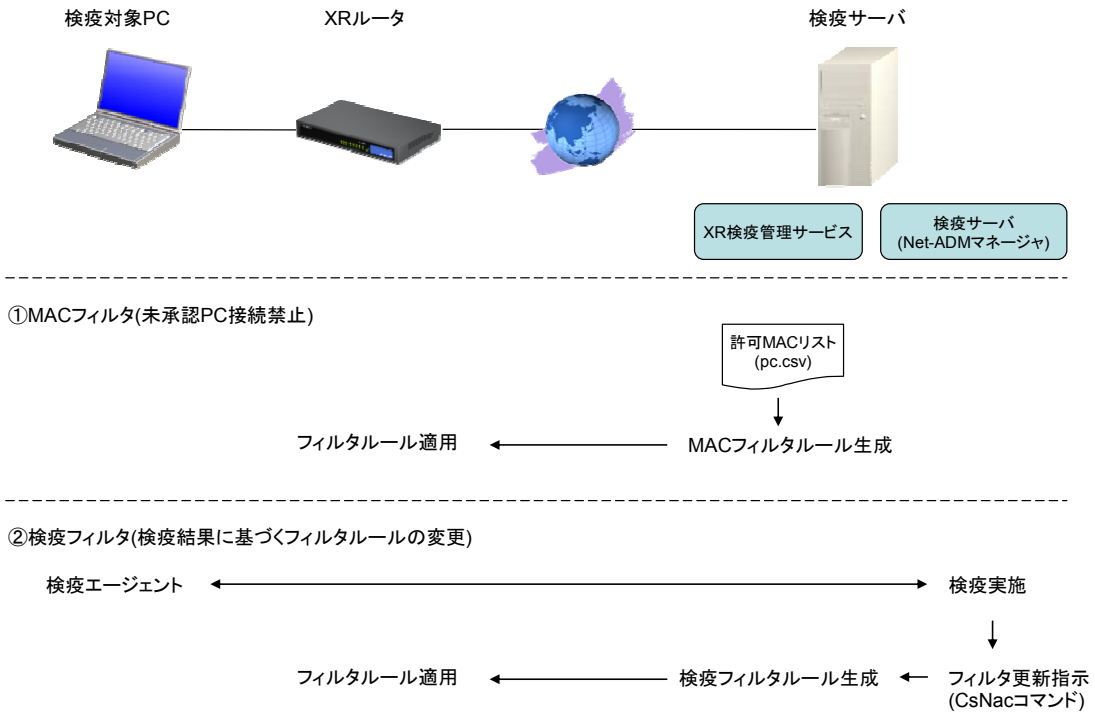
1.0 版

センチュリー・システムズ 株式会社

目次

1. 概要

本マニュアルでは XR 検疫管理サービスソフトのインストールおよび使用方法について説明します。
XR 検疫管理サービスは、検疫フィルタ機能を持つ XR シリーズルータに対して外部からフィルタ設定に関する指示をおこなうソフトウェアです。検疫サーバ機能を提供する製品と組み合わせることで、検疫結果に基づいたフィルタルールの設定変更を動的におこなうことができるようになります。



2. 動作環境

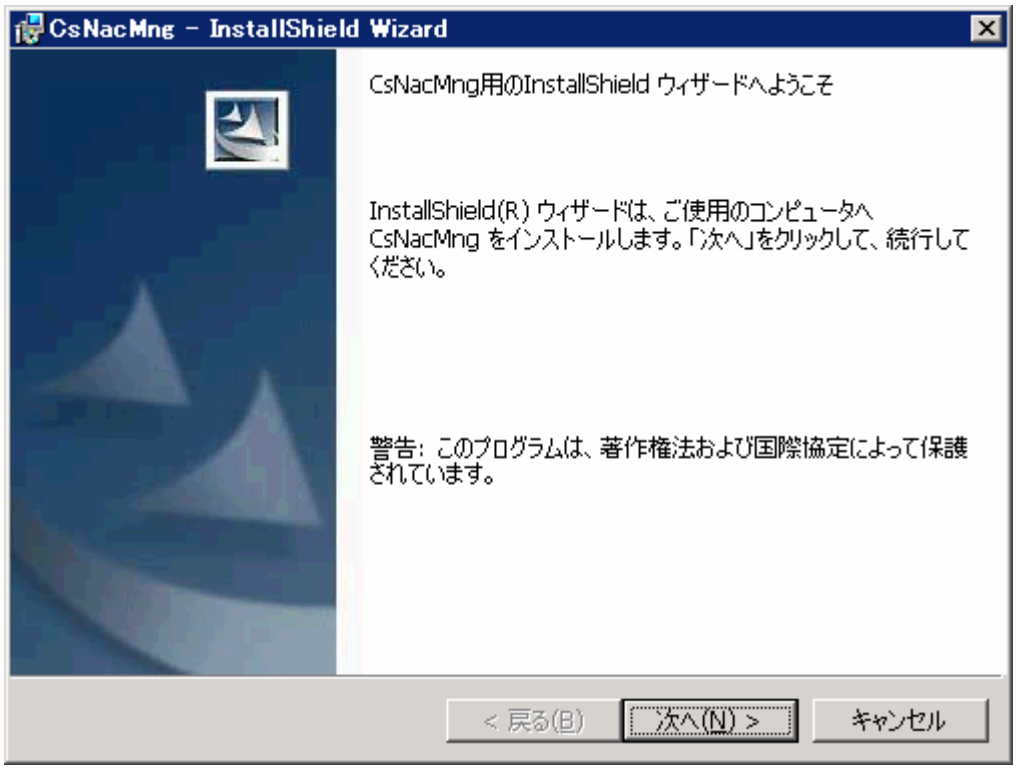
対象 OS ： Windows 2003 Server
対応する検疫サーバ: ヌリテレコム社製 Net-ADM V2.4.2 以降

3. インストール

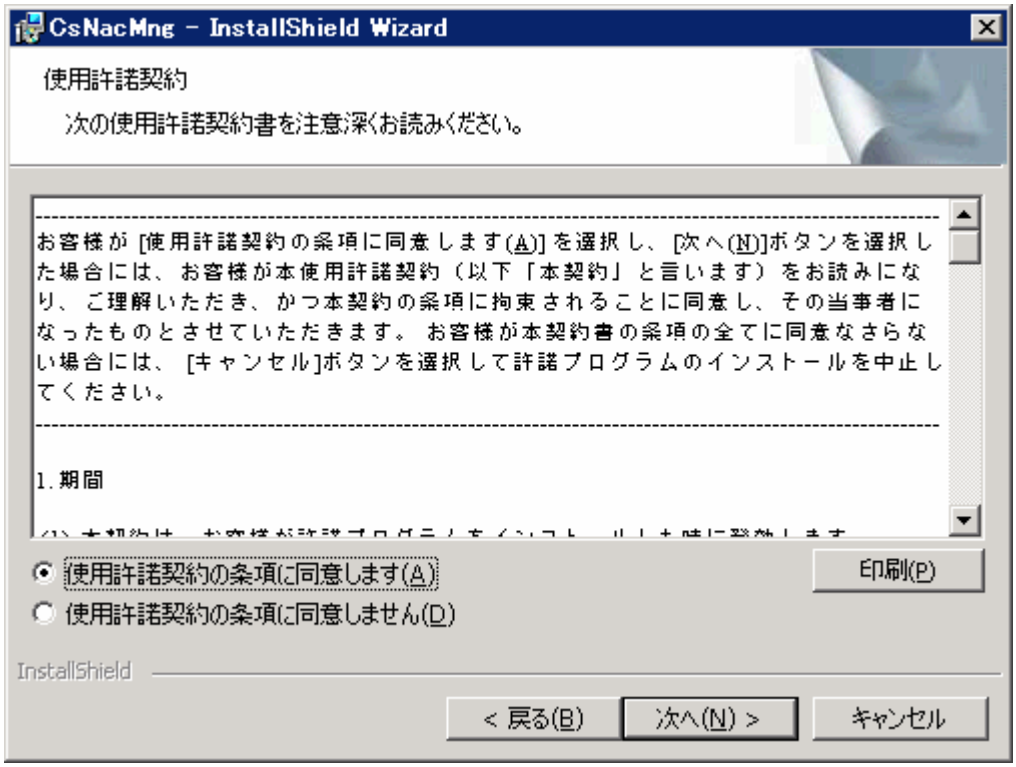
導入マシン上に Administrator 権限のユーザでログインし、以下の操作をおこなってください。

以前のバージョンの XR 管理サービスがインストールされている場合には、先にアンインストールをおこなってください。

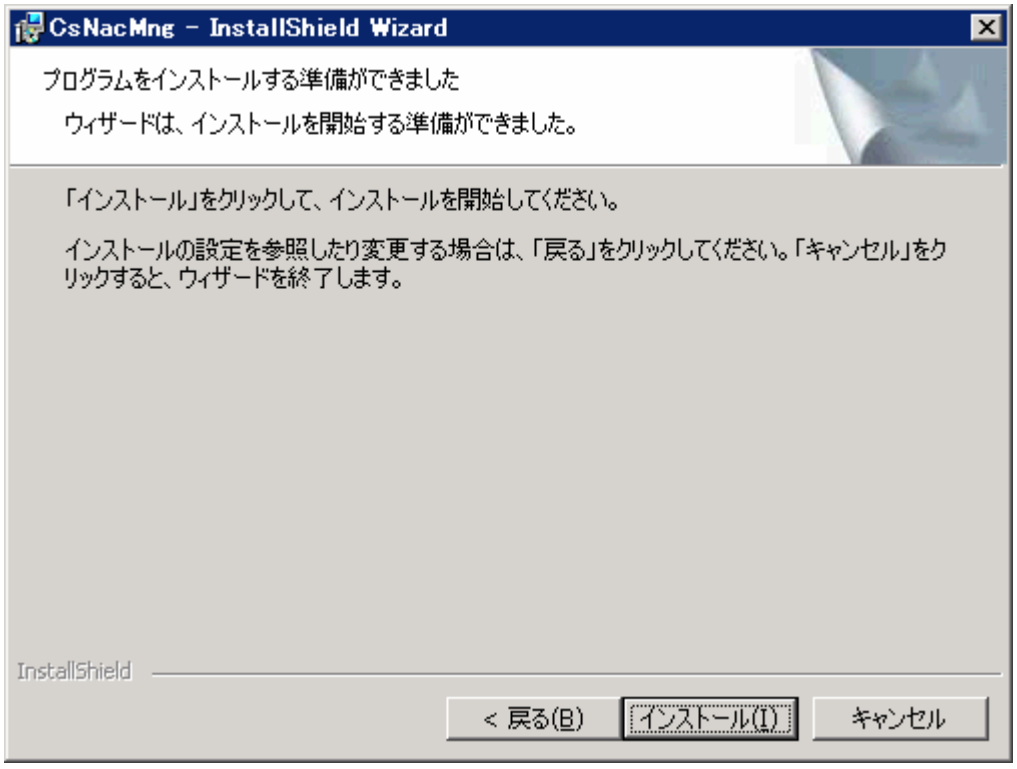
配布パッケージである CsNacSetup.exe を実行するとインストールが開始されます。



「次へ」ボタンを押すと使用許諾契約の画面が表示されますので、内容を確認してください。使用許諾契約の条項に同意されない場合には本ソフトウェアはインストールできません。

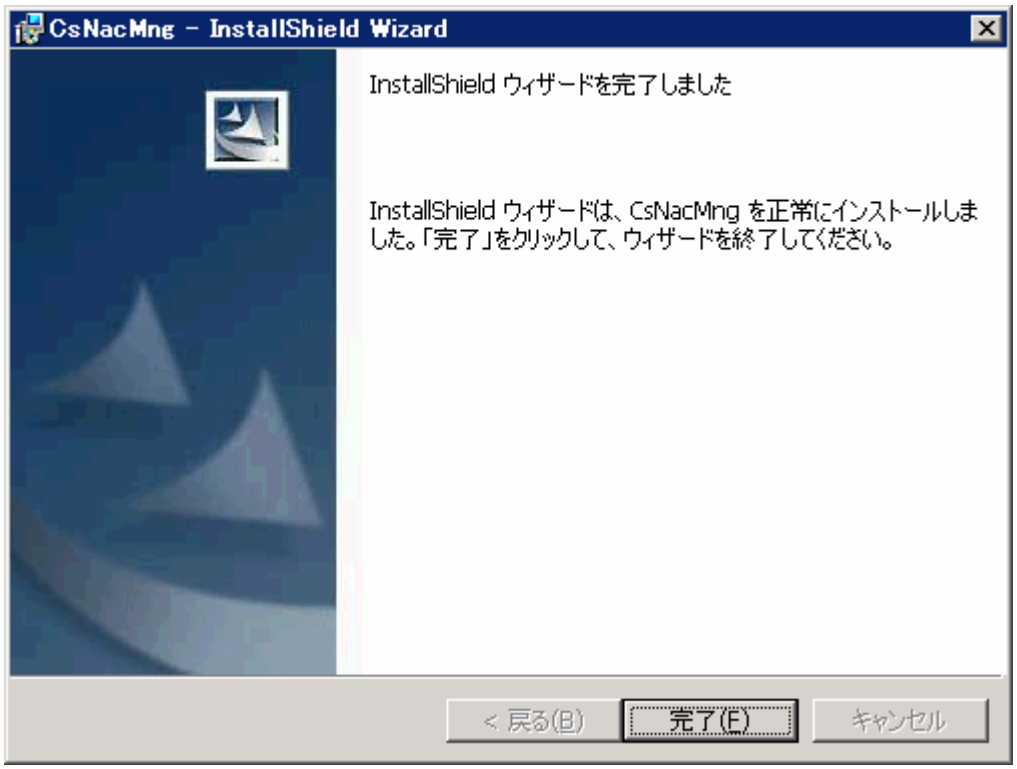


インストール先のフォルダを選択します。インストール先をデフォルトの設定から変更したい場合には「変更」ボタンを押してインストール先を選択してください。



「インストール」ボタンを押してインストールを開始します。

正常にインストールが終了すると次の画面が表示されます。



3.1. syslog の出力先の設定

本ソフトウェアはデフォルトでログ情報をローカルホスト(127.0.0.1)に syslog で出力するように設定されています。またログの出力レベルは info レベルになっています。

syslog に関する設定を変更する場合は以下の ini ファイルを作成するようにします。

フォルダ: Windows システムフォルダ(例: C:¥WINDOWS)

ファイル名: syslog.ini

内容:

[SYSLOG]

DESTINATION=(転送先ホストの IP アドレス)

PRIORITYMASK=(ログレベル)

ログレベルには高いものから順に以下のものが指定可能です。指定されたレベル以上のログが送信されます。

emerg / alert / crit / err / warning / notice / info / debug

設定例)ログレベルが notice 以上であるログを IP アドレスが 192.168.0.1 であるホストに送信します。

ファイル: C:¥WINDOWS¥syslog.ini

```
[SYSLOG]
DESTINATION=192.168.0.1
PRIORITYMASK=notice
```

設定を変更した場合、Windows の「コントロールパネル」-「管理ツール」-「サービス」で CsNacMng のサービスの再起動をおこなってください。

4. アンインストール

本ソフトウェアをアンインストールする場合には「コントロールパネル」の「プログラムの追加と削除」から、「CSNacMng」を選択して削除ボタンを押してください。なお、以下のファイルは削除されませんので、不要な場合は個別に削除してください。

・インストール先のフォルダ

・フォルダ “C:¥Windows¥system32” 配下の以下のファイル （一度も設定の保存をしていない場合には存在しません。）

xr.csv, xroute.csv, quarantine.csv, pc.csv

・フォルダ “C:¥Windows” 配下の以下のファイル。(設定していない場合には存在しません。)

syslog.ini

5. 設定コマンド

本ソフトウェアの設定はコマンドプロンプトからインストール先のフォルダ(デフォルトでは” C:¥Program Files¥Century Systems¥Nac Service”) 配下の設定コマンドを使っておこないます。設定内容は CSV ファイルに保存することができ、設定コマンドを実行する代わりに CSV ファイルを直接編集して読み込ませることでも設定することができます。(CsNac を除く。)

コマンドの種類

コマンド名	説明
CsXr	検疫フィルタをおこなう XR ルータの IP アドレス、パスワード等を設定します。
CsXroute	PC の IP アドレスに基づいて、検疫フィルタルールを送信する XR ルータを設定します。
CsQuarantine	検疫サーバの IP アドレス、ポート番号の設定をおこないます。
CsPc	検疫対象 PC の MAC アドレスと IP アドレスを設定します。(未承認 PC フィルタ)
CsNac	検疫に成功した場合、およびユーザがログアウトした場合に、XR の検疫フィルタルールを更新します。

以下、各コマンドについて説明します。

5.1. CsXr

検疫フィルタをおこなう XR ルータの IP アドレス、パスワード等を設定します。

【形式】

```
CsXr OPERATION [TARGET] [sport SRC PORT] [user ID] [pass PW]
```

【利用例】

```
> CsXr add 172.18.1.250 sport 880 user demo pass demo
```

【指定オプション】

(1) OPERATION

以下のいずれかを指定します。

add	OPERATION以降の設定内容を現在の設定に追加します。
del	OPERATION以降の設定内容を現在の設定から削除します。
save	現在の設定を設定ファイルに保存します。 保存場所: Windows システムフォルダ(例: C:¥WINDOWS¥system32) ファイル名: xr.csv
load	設定ファイルの内容を読み込み、現在の設定に追加します。設定ファイルは上記 save の保存場所になります。
clear	現在の設定内容が消去されます。
show	現在の設定内容を一覧表示します。

以降のオプションは add または del の場合にのみ指定します。save/load/clear/show の場合には指定しないでください。

(2) TARGET

検疫フィルタ機能を動かす XR ルータの IP アドレスを指定します。

(3) sport SRC_PORT

検疫フィルタ機能を動かす XR ルータのポート番号を文字列”sport”に続けて指定します。ここで指定するポート番号は、XR 側の設定内容と同じにします。

(4) user ID

検疫フィルタ機能を動かす XR ルータへのアクセス時に用いるユーザ名を文字列”user”に続けて指定します。ここで指定するユーザ名は、XR 側の設定内容と同じにします。

(5) pass PW

検疫フィルタ機能を動かす XR ルータへのアクセス時に用いるパスワードを文字列”pass”に続けて指定します。ここで指定するパスワードは、XR 側の設定内容と同じにします。

5.2. CsXroute

PC の IP アドレスに基づいて、検疫フィルタルールを送信する XR ルータを設定します。

【形式】

```
CsXroute OPERATION [TARGET] [network NW] [netmask NM] [dev IF]
```

【利用例】

```
> CsXroute add 172.16.0.1 network 192.168.0.0 dev eth0
```

【指定オプション】

(1) OPERATION

以下のいずれかを指定します。

add	OPERATION以降の設定内容を現在の設定に追加します。
del	OPERATION以降の設定内容を現在の設定から削除します。
save	現在の設定を設定ファイルに保存します。 保存場所: Windows システムフォルダ(例: C:¥WINDOWS¥system32) ファイル名: xroute.csv
load	設定ファイルの内容を読み込み、現在の設定に追加します。設定ファイルは上記 save の保存場所になります。
clear	現在の設定内容が消去されます。
show	現在の設定内容を一覧表示します。

以降のオプションは add または del の場合にのみ指定します。save/load/clear/show の場合には指定しないでください。

(2) TARGET

検疫フィルタ情報を送る XR ルータの IP アドレスを指定します。

(3) network NW

検疫対象のPCが属するネットワークアドレスを”network”に続けて指定します。このnetowrokと次のnetmaskの組で指定されたIPアドレスの範囲に属する検疫結果のフィルタルールが、TARGETで指定されたXRルータに対して送られます。

(4) netmask NM

検疫対象のPCが属するネットワークのネットマスクを”netmask”に続けて指定します。上のnetowrokとこのnetmaskの組で指定されたIPアドレスの範囲に属する検疫結果のフィルタルールが、TARGETで指定されたXRルータに対して送られます。

(5) dev IF

検疫対象のPCが属するネットワークが接続されているXRルータのインタフェース名を、文字列”dev“に続けて指定します。検疫結果のフィルタルールがTARGETで指定されたXRルータのうち、指定されたインタフェースに対して適用されます。

5.3. CsQuarantine

検疫サーバの IP アドレス、ポート番号の設定をおこないます。CsPc コマンドで登録された PC から、この設定コマンドで設定された検疫サーバのポートへの通信を許可するフィルタルールが XR ルータに追加されます。

【形式】

```
CsQuarantine OPERATION [source SRC_IP] [protocol PROTO] [sport SRC_PORT]
```

【利用例】

```
> CsQuarantine add source 172.17.254.254 protocol tcp sport 4208
```

【指定オプション】

(1) OPERATION

以下のいずれかを指定します。

add	OPERATION以降の設定内容を現在の設定に追加します。
del	OPERATION以降の設定内容を現在の設定から削除します。
save	現在の設定を設定ファイルに保存します。 保存場所: Windows システムフォルダ(例: C:¥WINDOWS¥system32) ファイル名: quarantine.csv
load	設定ファイルの内容を読み込み、現在の設定に追加します。設定ファイルは上記 save の保存場所になります。
clear	現在の設定内容が消去されます。
show	現在の設定内容を一覧表示します。

以降のオプションは add または del の場合にのみ指定します。save/load/clear/show の場合には指定しないでください。

(2) source SRC_IP

検疫サーバが動いているマシンの IP アドレスを”source”に続けて指定します。

(3) protocol PROTO

検疫サーバが使用するプロトコルを”protocol”に続けて指定します。

(4) sport SRC_PORT

検疫サーバが使用するポートを”sport”に続けて指定します。

5.4. CsPc

検疫対象 PC の MAC アドレスと IP アドレスを設定します。このコマンドで登録された PC から Quarantine コマンドで設定された検疫サーバへの通信を許可するフィルタルールが、XR ルータに対して送られます。

【形式】

```
CsPc OPERATION [source-mac SRC_MAC [source SRC_IP]] [network NW [netmask NM]]
```

”[source-mac SRC_MAC [source SRC_IP]]”は個々のPCのMACアドレスを指定してフィルタをおこないたい場合に指定します。”network NW [netmask NM]”は一定範囲のIPアドレスに対してはMACアドレスによるフィルタをおこなわずに検疫サーバへの通信を許可したい場合に指定します。” [source SRC_IP]”と” [netmask NM]”はどちらか一方を指定します。両方同時には指定できません。

【利用例】

```
> CsPc add source-mac 00:00:00:00:00:01 source 192.168.0.1
```

【指定オプション】

(1) OPERATION

以下のいずれかを指定します。

add	OPERATION以降の設定内容を現在の設定に追加します。
del	OPERATION以降の設定内容を現在の設定から削除します。
save	現在の設定を設定ファイルに保存します。設定変更後は必ず保存してください。XR 管理サービスを再開した時にはこの保存ファイルから設定が読み込まれます。 保存場所: Windows システムフォルダ(例: C:¥WINDOWS¥system32) ファイル名: pc.csv
load	設定ファイルの内容を読み込み、現在の設定に追加します。設定ファイルは上記 save の保存場所になります。
clear	現在の設定内容が消去されます。
show	現在の設定内容を一覧表示します。

以降のオプションは add または del の場合にのみ指定します。save/load/clear/show の場合には指定しないでください。

(2) source-mac SRC_MAC

検疫対象 PC の MAC アドレスを”source-mac”に続けて指定します。この PC から検疫対象サーバへの接続が許可されます。

(3) source SRC_IP

検疫対象 PC の IP アドレスを”source”に続けて指定します。

(4) network NW

MAC アドレスの値によらず検疫サーバへの接続を許可するネットワークアドレスを”network”に続けて指定します。

(5) netmask NM

MAC アドレスの値によらず検疫サーバへの接続を許可するネットワークアドレスのマスク値を”netmask”に続けて指定します。”netmask 255.255.255.0”のように指定します。

5.5. CsNac

検疫に成功した場合、およびユーザがログアウトした場合に、XR の検疫フィルタルールを更新します。検疫に合格した場合に検疫サーバがこのコマンドを実行するように設定してください。

【形式】

```
CsNac OPERATION [TARGET] [source SRC_IP] [source-mac SRC_MAC]
```

【利用例】

```
> CsNac add accept source 172.16.0.1 source-mac 00:00:00:00:00:01
```

【指定オプション】

(1) OPERATION

以下のいずれかを指定します。

add	OPERATION以降の設定内容を現在の設定に追加します。
del	OPERATION以降の設定内容を現在の設定から削除します。
show	現在の設定内容を一覧表示します。

以降のオプションは add または del の場合にのみ指定します。show の場合には指定しないでください。

(2) TARGET

設定するフィルタルールに応じて accept または drop を指定します。検疫に通った時のルールを追加/削除する場合には通常 accept を指定します。

(3) source SRC_IP

検疫に合格した PC の IP アドレスを”source”に続けて指定します。

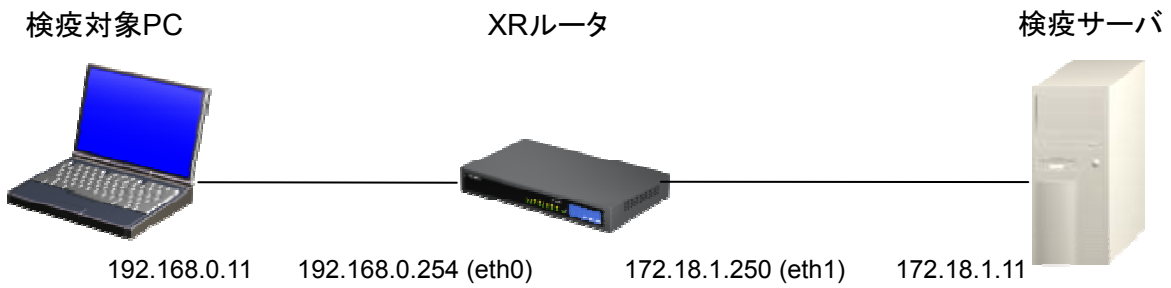
(4) source-mac SRC_MAC

検疫に合格した PC の MAC アドレスを”source-mac”に続けて指定します。

6. 設定例

6.1. ネットワーク環境

本設定例では以下のネットワーク構成を前提に説明します。検疫サーバにはヌリテレコム社製「Net-ADM」がインストールされているものとします。



PC(WindwosXP):192.168.0.11
XR: eth0 192.168.0.254
eth1 172.18.1.250
検疫サーバ(Windows2003 Server): 172.18.1.11

6.2. XR ルータ側の設定

(1)転送フィルタの設定

フィルタの成否に関わらず通す必要がある通信を事前にフィルタ設定で許可するようにします。
XR ルータのフィルタ設定メニューの「転送フィルタ」で以下のフィルタルールを追加します。
操作の詳細については XR のマニュアルを参照してください。

インタフェース	方向	動作	プロトコル	送信元	送信ポート	あて先アドレス	あて先ポート
eth1	受信時	許可	tcp	172.18.1.11		192.168.0.0/24	7500

eth0	受信時 許可	tcp	192.168.0.0/24	7500	172.18.1.11
eth1	受信時 許可	icmp	172.18.1.11		192.168.0.0/24
eth0	受信時 許可	icmp	192.168.0.0/24		172.18.1.11

上記は「Net-ADM マネージャ」から PC の管理をおこなうために必要な通信ポートになります。

(2)検疫フィルタメニューの設定

XR ルータの検疫フィルタ設定メニューで検疫フィルタを「使用する」に変更します。また外部から検疫フィルタ設定をおこなうためのユーザ名、パスワードを設定します。この設定により検疫フィルタが適用され、各種フィルタにより明示的に許可されていない通信は全て遮断されるようになります。
操作の詳細については XR のマニュアルを参照してください。

6.3. XR 管理サービスの設定

コマンドプロンプトを開き、設定コマンドを使って設定をおこないます。事前にインストール先のフォルダ(デフォルト “C:¥Program Files¥Century Systems¥Nac Service”)に移動するか、パスを通した上で以下を実施します。

(1) CsXr コマンドで検疫フィルタ機能を持つ XR の IP アドレス、ポート、ユーザ名、パスワードを設定します。XR 側の設定と一致している必要があります。

```
> CsXr add 172.18.1.250 sport 880 user example pass example
```

(2) CsXroute コマンドで 192.168.0.0/24 のネットワーク上の PC の検疫結果に基づいて、検疫情報を 172.18.1.250 に送る設定をします。

```
> CsXroute add 172.18.1.250 network 192.168.0.0 netmask 255.255.255.0 dev
eth0
```

(3) CsQuarantine コマンドで Net-ADM マネージャが動作しているマシンの IP アドレスとポート番号を設定します。

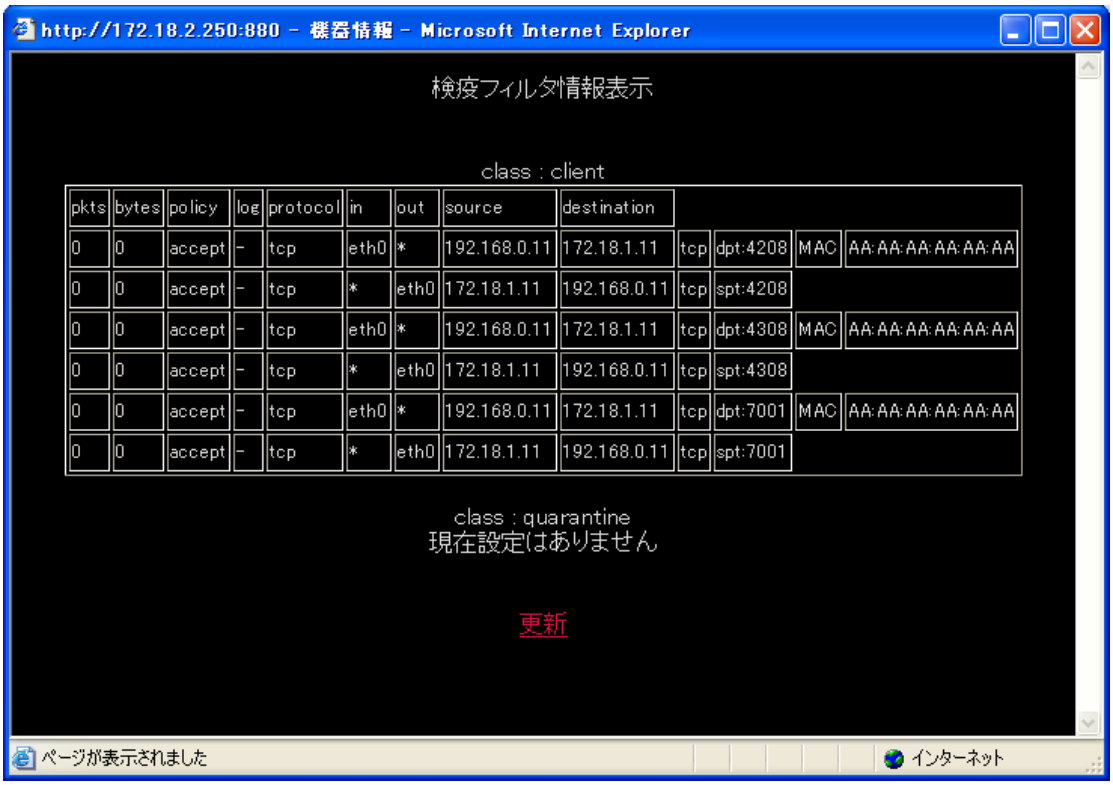
```
> CsQuarantine add source 172.18.1.11 protocol tcp sport 4208
> CsQuarantine add source 172.18.1.11 protocol tcp sport 4308
> CsQuarantine add source 172.18.1.11 protocol tcp sport 7001
```

(4) 検疫対象の PC を登録します。

```
> CsPc add source-mac aa:aa:aa:aa:aa:aa source 192.168.0.11
```

aa:aa:aa:aa:aa:aa には PC の MAC アドレスを指定します。

この時点で XR ルータが、指定された PC から検疫サーバへの監査要求の通信を通すようになります。設定されたフィルタの内容は XR ルータの管理メニューの検疫フィルタ設定メニューで確認できます。(class:client として表示されます。)



(5) 設定を保存しておきます。

```
> CsXr save
> CsXroute save
> CsQuarantine save
> CsPc save
```

6.4. Net-ADM マネージャの設定

以下に設定例を示します。Net-ADM の操作の詳細については Net-ADM のマニュアルを参照してください。

(1) アドミッションポリシーの設定

アドミッションサービスの監査状況に応じて CsNac.exe コマンドにより XR のフィルタを更新するように設定します。監査の条件や監査後のアクションは Net-ADM のアドミッションポリシーファイル(policy.csv)を作成し、その中で規定します。

監査に成功した場合に XR ルータの検疫フィルタを追加するために、policy.csv ファイルの中

の”OKAction3”の項目に以下のように CaNac コマンドを指定します。

```
"""C:¥Program Files¥Century Systems¥Nac Service¥CsNac.exe"" add accept source %agtip%
source-mac %mac%"
```

※コマンドパス中に空白文字が含まれているため、コマンド部分をクォーテーションマーク(”)2つで囲っています。クォーテーションマークが二つ必要なのは、csv ファイル中でクォーテーションマークはフィールドの区切りの意味になるため、二つ続けることで一つのクォーテーションマークとして扱うようにするためです。また、%agtip%, %mac% 部分はそれぞれ監査要求をおこなった PC の IP アドレスと MAC アドレスが渡されるようになります。

監査終了時に XR ルータの検疫フィルタルールを解除するために、policy.csv ファイルの中の”FinAction3”の項目に以下のように CsNac コマンドを指定します。

```
"""C:¥Program Files¥Century Systems¥Nac Service¥CsNac.exe"" del accept source %agtip%
source-mac %mac%"
```

ポリシーファイルの作成後、以下のコマンドでポリシーファイルを読み込ませます。ユーザ名、パスワードは Net-ADM マネージャの設定に合わせて変更してください。

```
> C:¥NASCenter¥Manager¥NasPolImpm.exe -u root -p 1 -i policy.csv
```

(2) 監査終了ノード検知機能の設定

一定時間以上稼動状態が確認できなかったノードに対し監査終了処理をおこなうための設定をおこないます。Net-ADM マネージャを導入したディレクトリの NASCenter.ini ファイルの NasPolicy セクションに AliveTime 行を追加します。

設定例) NASCenter.ini

```
[NasPolisy]
AliveTime=30
```

この設定により、ユーザが PC をネットワークから外すなどした場合に、XR ルータの検疫フィルタからその PC の通信を許可する設定が削除されます。

6.5. Net-ADM エージェントの設定

以下に設定例を示します。Net-ADM の操作の詳細については Net-ADM のマニュアルを参照してください。

検疫対象 PC で以下のコマンドを実行すると監査要求が Net-ADM マネージャに送信されます。

```
> C:¥NASCenter¥Agent¥NasAdsa.exe -t HW -t SW
```

また、検疫対象 PC で以下のコマンドを実行すると監査終了要求が Net-ADM マネージャに送信されます。

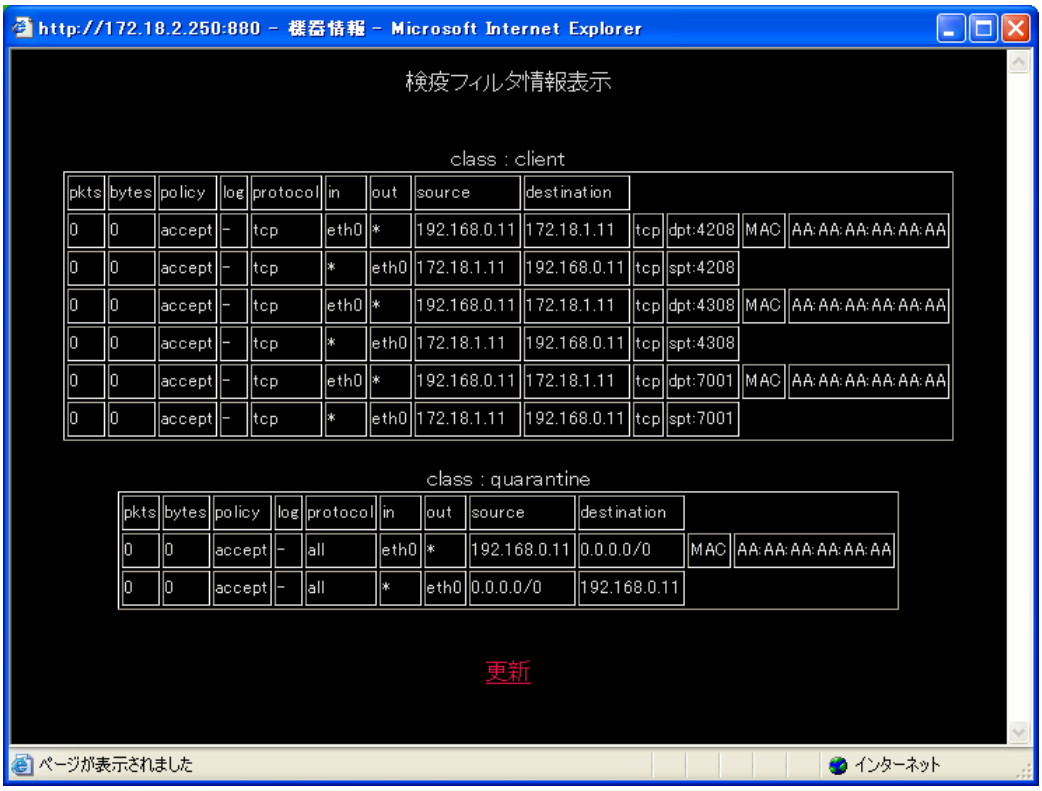
```
> C:¥NASCenter¥Agent¥NasAdsa.exe  --fin
```

ユーザログイン/ログアウト時に自動的に監査要求、監査終了要求を送るためには、エージェントを導入したディレクトリの RMSAGENT.ini ファイルの Admission セクションに以下の行を追加します。

設定例） RMSAGENT.ini

```
[Admission]
LogonRequest=1
LogoffRequest=1
FinRequest=1
RequestInterval=30
InvType=HW, SW
AliveInterval=5
```

監査に合格すると検疫対象 PC から XR ルータを越えた通信が許可されます。設定されたフィルタの内容は XR ルータの管理メニューの検疫フィルタ設定メニューで確認できます。(class:quarantine として表示されます。)



XR 検疫管理サービス

2006 年 6 月版

発行　センチュリー・システムズ株式会社