



FFRI Enterprise Management Console ネットワーク必要要件と設定ガイド

FFRI Security, Inc.
株式会社 FFRIセキュリティ
<https://www.ffri.jp>

前提

本ネットワーク必要要件と設定ガイドは、FFRI Enterprise Management Console における構成要件ガイドである。

用語解説

次ページ以後に記載している用語・略語を以下に記載する。

用語	説明
管理コンソール サーバー	FFRI Enterprise Management Console がインストールされたサーバー。
レポジトリサーバー	帯域負荷分散のために管理コンソールサーバーとは別に配布データを保持するレポジトリ機能がインストールされたサーバー。
AD	Microsoft社提供のActive Directoryの略。ネットワーク上のオブジェクトについての情報を格納し、この情報をユーザーとネットワーク管理者が使用できるようにするディレクトリサービス。
DC	Microsoft社提供のDomain Controllerの略。Active Directoryのディレクトリ・データベースを管理するサーバーを「ドメイン・コントローラ (Domain Controller)」と呼ぶ。
FW	Firewallの略。あるネットワークのリソースを他のネットワークのユーザーから保護するプログラム。
WINS Server	Microsoft社提供のWindows インターネット ネーム サービス (WINS) サーバーは、コンピュータ名 (NetBIOS 名) に動的に IP アドレスをマッピングします。これにより、ユーザーは IP アドレスではなくコンピュータ名でリソースにアクセスできるようになります。

管理コンソールサーバーネットワーク要件

- ・ 管理コンソールサーバーから以下のネットワーク到達性を確保する必要がある
 - － クライアントとの通信
 - ・ NAT環境の制約
 - ・ 管理コンソールの通信量
 - － データベースサーバーとの通信
 - － インターネットへの接続
- ・ プッシュ型インストールのネットワーク要件
 - － コンピューターブラウジングの設定と確認方法
 - － Active Directoryの設定と確認方法
 - － リモート管理とファイル共有の設定と確認方法
 - － リモート管理とファイル共有に関するその他の情報

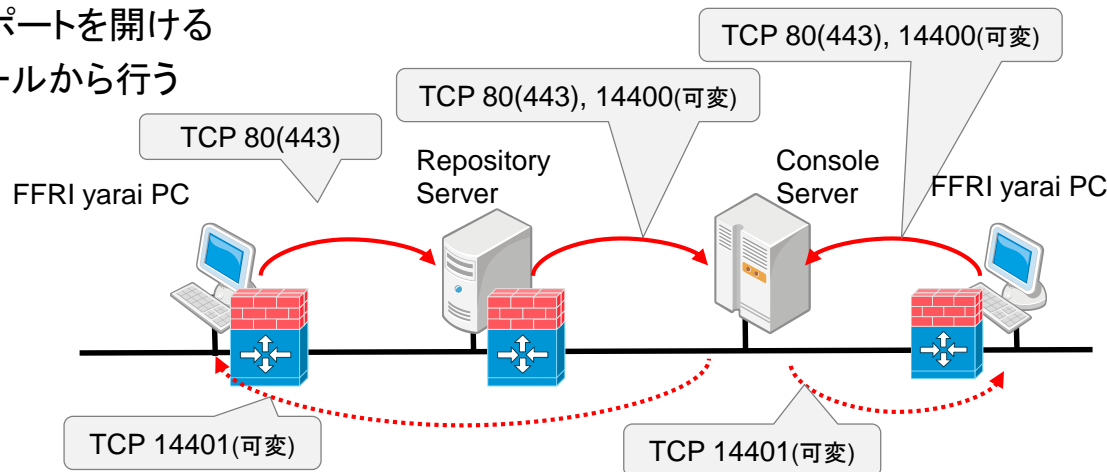
クライアントとの通信

設定方法

- ・ ファイアウォール越しのFFRI yaraiまたはレポジトリサーバーの管理（ポート番号は設定により変更可能）
 - 管理コンソールサーバーのTCP 14400ポートを開ける
 - シリアルナンバーによるアクティベーションを行う場合のみクライアントのTCP14401ポートを開ける
- ※ 管理コンソール-FFRI yarai間にNATが存在し、クライアントからのポーリングのみ行う場合は、サーバー側のポート設定だけでよい
- ※ 管理コンソール-レポジトリサーバー間はNATをサポートしていない
- ・ FFRI yaraiまたはレポジトリサーバーが管理コンソールサーバーから更新ファイルをダウンロード
 - 管理コンソールサーバーのTCP 80(443)ポートを開ける
- ・ FFRI yaraiがレポジトリサーバーから更新ファイルをダウンロード
 - レポジトリサーバーのTCP 80(443)ポートを開ける
- ・ クライアントのProxy設定は、管理コンソールから行う

確認方法

- ・ それぞれtelnetで疎通を確認



NAT環境の制約

使用不可機能

1. シリアルナンバーによるアクティベーション
2. リモートインストール
3. レポジトリサーバーとの連携
4. 旧バージョンのクライアント管理 (FFRI yarai 1.2.572以前、FFRI yarai 脆弱性攻撃防御機能 1.2.610以前)
5. 連携サーバー機能

その他の制約

1. 上記使用不可機能以外の管理コンソールの命令はクライアントから管理コンソールのポーリング時に処理が行われる為最大で15分(デフォルト値の場合)かかる
 - ※ 管理コンソールに結果が返ってくるまでさらに15分かかる
2. SSL-VPN未サポート
3. VPNを利用している場合であっても管理コンソールとクライアントが通信可能であれば管理可能
 - ※ 弊社の把握している範囲で「SecureClient」は動作実績あり(弊社未検証)
 - ※ VPNソフトの種類によってはMACアドレスが各クライアント共通となるソフトがあるため、この場合は管理不可

管理コンソールの通信量

・通信量の目安は下記となります(v2.14の場合)

■管理コンソール <-> クライアント

イベント種類	通信量
スタートアップ(*1)	約2KB
シャットダウン	約1KB
検出(*2)	約1-3KB
ポーリング	約1KB
ポリシー配布	約2KB
アップデート	アップデートファイルの容量参照
オフラインアクティベート	約3KB
オンラインアクティベート	約5KB
検体/ログ収集 (*2)	不定

*1 クライアントが起動して初めて行う通信です。

*2 検体、検出エンジンによって通信量が異なります。

■管理コンソール <-> 弊社アップデートサーバー

イベント種類	通信量
ダウンロード	アップデートファイルの容量参照
ライセンス認証	約5KB

■アップデートファイル(v2.14)の容量

イベント種類	通信量
FFRI yarai	約49.5MB

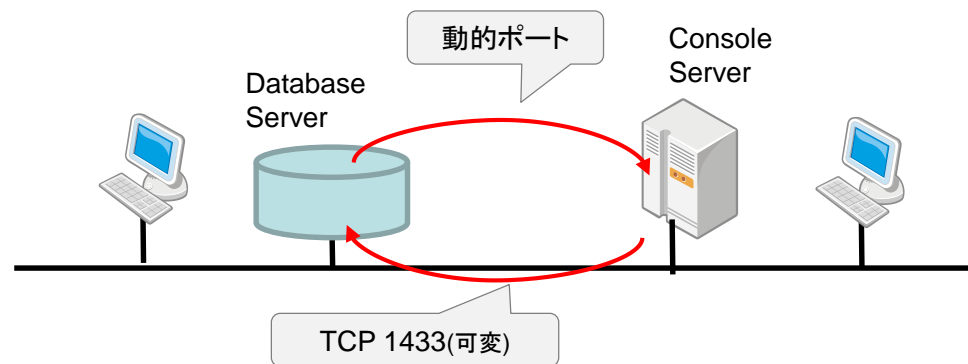
データベースサーバーとの通信

設定方法

- ・ Microsoft SQL Server を構築し、SQL認証による接続を許可する
- ・ インストール時にデータベースサーバーの情報を入力する
- ・ 管理コンソールに付属のDB Connection String Updaterによっても変更可能

確認方法

- ・ Microsoft SQL Management Studioやsqlcmdコマンドなどの管理ツールによって接続を確認



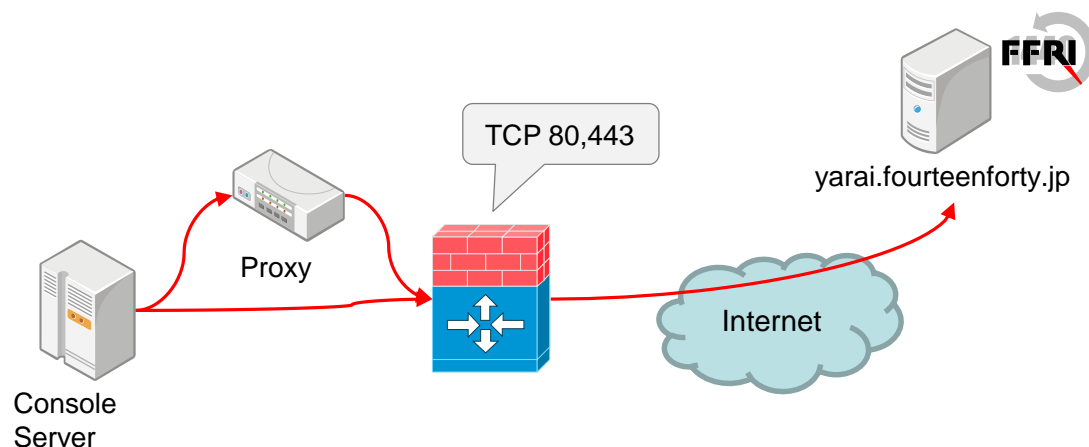
インターネットへの接続

設定方法

- ・ 管理コンソールが直接インターネットにアクセスできる場合は特に設定不要
- ・ Proxyを経由する必要がある場合は、管理コンソール上で設定を行う

確認方法

- ・ IE等でProxyが使用可能か調べた上で管理コンソール上で操作を行う
- ・ 管理コンソール上でFFRI yaraiのライセンス登録を行い、エラーが出ないことを確認



プッシュ型リモートインストールのネットワーク要件

コンピューターブラウザーによる参照

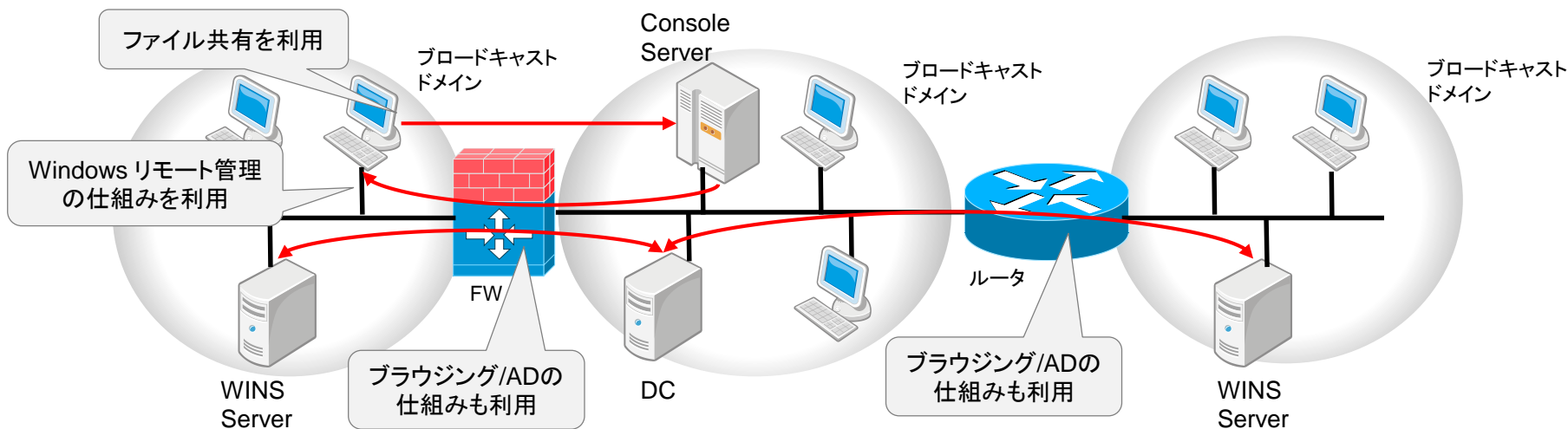
- ・ 別ネットワークのマシンはWINS等によるブラウジングを有効にする

Active Directoryによる参照

- ・ ADによるドメイン管理を有効にする

Windows リモート管理とファイル共有

- ・ Windowsファイアウォールでリモート管理とファイル共有を使用できる設定が必要
- ・ ただし、NAT環境でのプッシュ型リモートインストールはサポートされていない



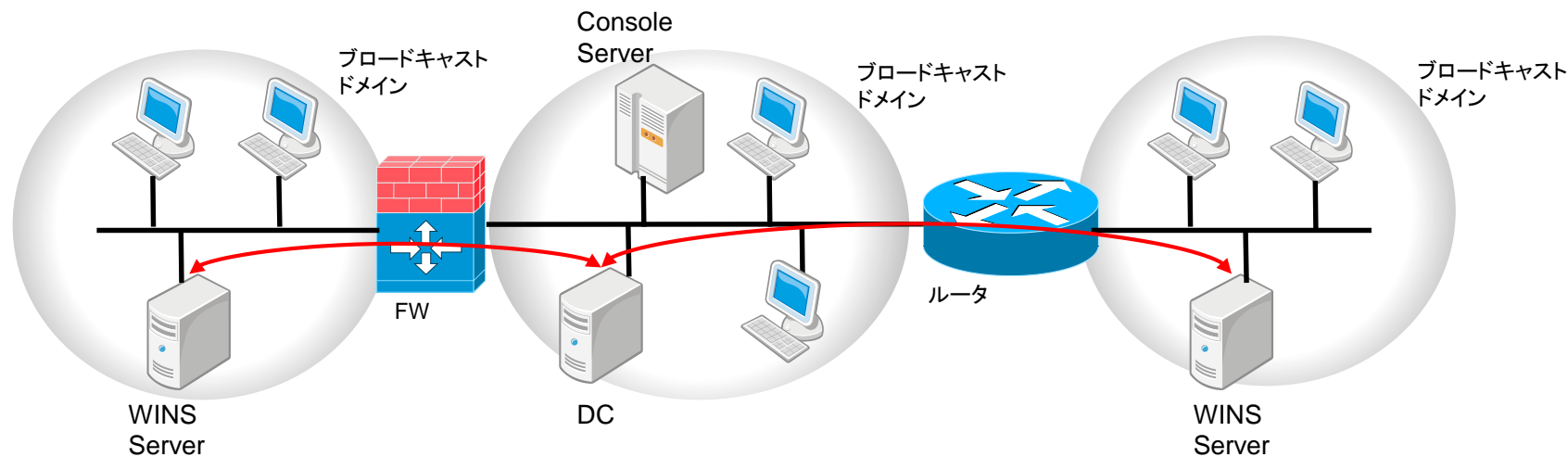
コンピューターブラウジングの設定と確認方法

設定方法

- ・ 別ブロードキャストドメイン内のマシンを管理コンソール上で列挙するには、一般的にそのセグメントに WINS サーバーを設置する

確認方法

- ・ 管理コンソールのリモートインストールの画面で、「Windows Networkからの取得」を選択し、対象マシンが表示されるか確認



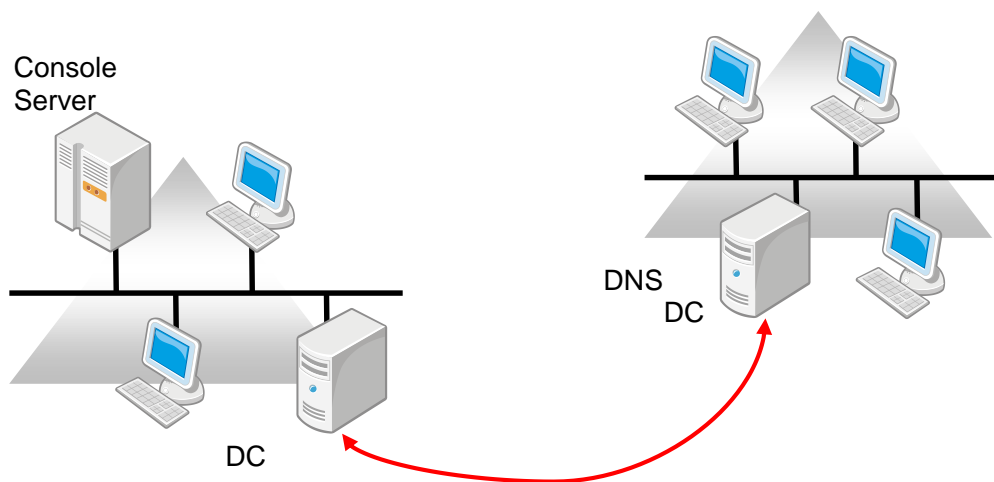
Active Directoryの設定と確認方法

設定方法

- ・ ドメインコントローラーを設置し、適宜ドメインを構成する

確認方法

- ・ 管理コンソールのリモートインストールの画面で、「Active Directoryからの取得」を選択し、必要なドメインの情報を入力して対象マシンが表示されるか確認



リモート管理とファイル共有の設定と確認方法

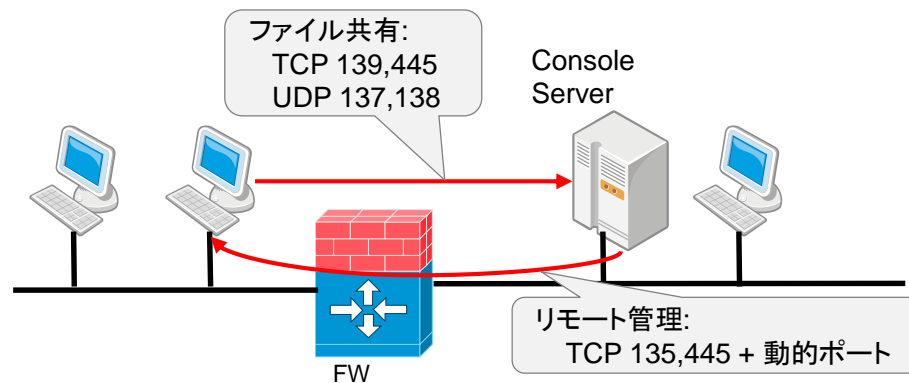
設定方法

- ・ ファイアウォール越しのプッシュ型インストールをするには、少なくとも以下のポートを開ける必要がある(「ファイルとプリンタの共有」と「Windowsリモート管理」)
 - TCP: 135,139,445 UDP: 137,138
- ・ リモート管理については、WMIにより動的に割り当てられるポートも開ける必要がある

確認方法

- ・ 以下のWMICコマンドで応答があれば、リモート管理が可能な状態であることを確認

```
C:¥> WMIC /NODE:"MACHINENAME" /user:"MACHINENAME¥admin"  
/password:"PASSWORD" OS GET Caption
```



リモート管理とファイル共有に関するその他の情報

- ・ Windows サーバー システムのサービス概要およびネットワーク ポート要件
<http://support.microsoft.com/kb/832017/ja>