FFRI AMC
ネットワーク要件の補足資料

株式会社ＦＦＲＩセキュリティ
https://www.ffri.jp/

Ver 1.0.9.00

目次

はじめに

本ドキュメントは、FFRI AMC におけるネットワーク要件の補足資料である。

関連資料

- FFRI AMC セットアップマニュアル
- FFRI AMC オペレーションマニュアル

用語解説

次ページ以後に使用されている用語・略語を以下に記載する。

用語	説明
クライアント	FFRI yarai が「管理されたクライアント」としてインストールされた端末。
管理コンソール サーバー	FFRI AMC がインストールされた端末。
データベース サーバー	管理コンソールサーバーとは別の筐体に、FFRI AMC で使用するデータベース PostgreSQL をセットアップしている端末。
FW	ファイアウォール （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。

管理コンソールサーバーのネットワーク要件

- 管理コンソールサーバーから以下のネットワークへの到達性を確保する必要がある
  - クライアントとの通信
  - インターネットへの通信
  - SMTP (メール送信) サーバーとの通信
  - データベースサーバーとの通信（※）

※データベースを管理コンソールサーバーに同居させる場合は設定不要

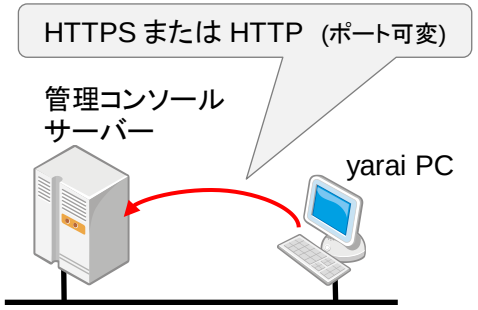
クライアントとの通信 (1/2)

前提

- FFRI AMC では、クライアントとの通信は HTTPS（443） または HTTP（80） のみを使用してクライアントとのすべての通信が行われる
  ※括弧内のデフォルトポート番号は、変更可能
- クライアントとのすべての通信は、クライアント側から管理コンソール側へ接続され、管理コンソールからクライアントへ接続することはない

設定方法

- 管理コンソールサーバーの HTTPS または HTTP のポートを開放



クライアントとの通信 (2/2)

確認方法

- 管理コンソールサーバーでの確認
  - オペレーションマニュアル「トラブルシューティング-> Apacheのアクセスログ出力」の項を参照
- クライアントからの確認
  - 管理コンソールサーバーにてあらかじめ、以下の作業を実施
    - [管理コンソールインストールディレクトリ]¥public¥index.htmlを
      [管理コンソールインストールディレクトリ]¥public¥func¥background¥index.html
      として、コピー
  - クライアントのブラウザにて以下URLを閲覧して、画面に「FFRI AMC」と表示されれば問題なし
    - http[s]://[管理コンソールのホスト名またはIPアドレス]/func/background/index.html

※クライアントと管理コンソールの間にプロキシを導入している場合

一部制約があり、クライアント側でWinHTTPのプロキシ設定が必要となる
（詳細は次ページ「クライアント-管理コンソール間でプロキシを導入する場合」に後述）

クライアント-管理コンソール間でプロキシを導入する場合

- クライアント端末側にてコマンドプロンプトより WinHTTP のプロキシ設定を行う必要がある。セットアップマニュアル「事前準備(プロキシサーバーの設定確認)」項を参照のこと
- WinHTTP のプロキシ設定は認証付きプロキシに対応していない。認証付きプロキシを利用する場合は、管理コンソールへのアクセスのみ、認証なしでアクセスできるように事前にシステム管理者にて対応の必要あり

クライアントとの通信のセキュリティ

HTTPS による TLS 通信の利用を推奨

- 管理コンソールサーバーとクライアントとの通信に TLS を利用可能
  - TLS を利用することで、通信内容が暗号化され、情報漏えいのリスクが低下
- 特別な理由がない限り、TLS を用いた接続を推奨
  - TLS を使用しない場合、通信が暗号化されないことにより、クライアントと管理コンソールサーバー間でやり取りする通信情報を傍受される可能性あり
  - 自己署名証明書も利用可能、ただし、通信先の真正性は確認されない
- TLS 1.1, TLS 1.2 のみ利用可能

FFRI AMC からインターネットへの通信（1/6）

前提

- FFRI AMC からインターネットへの通信は、オンラインライセンスの認証、アップデートモジュールの取得、過検出判定システムとの連携時に発生する
- 通信は HTTPS または HTTP のみを使用しており、ポートも 443 または 80 （変更不可）のみを使用してすべての通信が行われる
- 通信は、 FFRI AMC 側からインターネットへ接続され、インターネットから FFRI AMC へ接続することはない
- HTTPSでインターネット上のＦＦＲＩセキュリティの提供するサーバーと通信を行うにあたって、デフォルトでは証明書が本物であるかどうかの検証を行う設定となっている。この証明書をAMC側で検証を行う過程で、認証局であるAmazonの下記URLにFFRI AMCがアクセスできる必要がある。

  http://crl.r2m02.amazontrust.com/r2m02.crl

  ※URLは2023年03月時点のものであり、変更の可能性あり

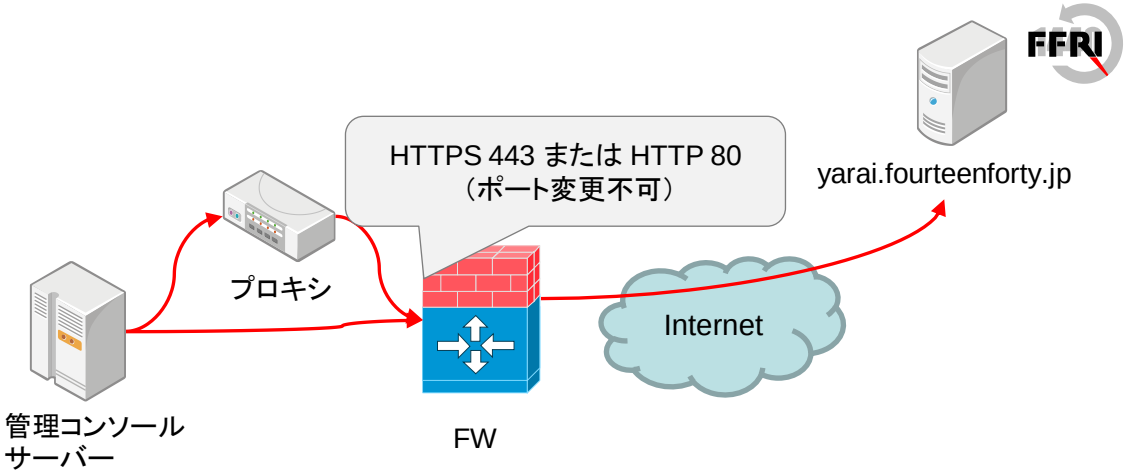
設定方法

- 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
- プロキシ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 (WebUI「ネットワーク設定」画面)

FFRI AMC からインターネットへの通信（2/6）

確認方法 (yarai.fourteenforty.jp)

- プロキシを使用する場合は、 Internet Explorer にプロキシの設定をした上で、 URL 欄に「 https://yarai.fourteenforty.jp/ 」を入力して、アクセスできるか確認
  - 画面に 「yarai.fourteenforty.jp」という文字が表示されれば問題なし
- オンラインライセンスを使用する場合、管理コンソール上でクライアントのライセンス登録を行い、エラーが出ないことを確認 （エラーになった場合は次のシートについても確認）



FFRI AMC からインターネットへの通信（3/6）

オンラインライセンスサーバーとの通信が上手く行かない場合の注意(Amazon証明書認証局へのアクセス) (1/2)

- オンラインライセンスを使用する場合、サーバー証明書の検証のために認証局サーバーから失効リストを取得するため、下記のURLにFFRI AMCがアクセスできる環境である必要がある。

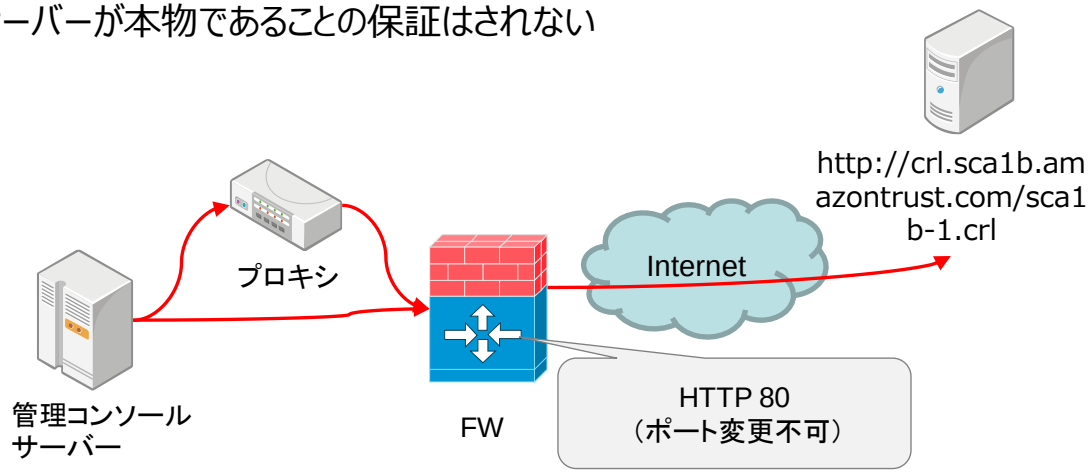
  http://crl.r2m02.amazontrust.com/r2m02.crl

  ※URLは2023年03月時点のものであり、変更の可能性あり
- プロキシを使用する環境下であれば、プロキシによって上記のURLがブロックされていないかを確認する。
- AmazonへのアクセスはWinHTTPのプロキシ設定に従ってアクセスが行われる。（WebUIのプロキシ設定はAmazonへのアクセス時には適用されないので注意が必要）
- ブロックを解除することが困難であるなど、上記URLアクセスが困難である場合においては、FFRI AMC側での証明書検証処理をスキップする設定を行うことで回避することが可能。

FFRI AMC からインターネットへの通信（4/6）

オンラインライセンスサーバーとの通信が上手く行かない場合の注意(Amazon証明書認証局へのアクセス) (2/2)

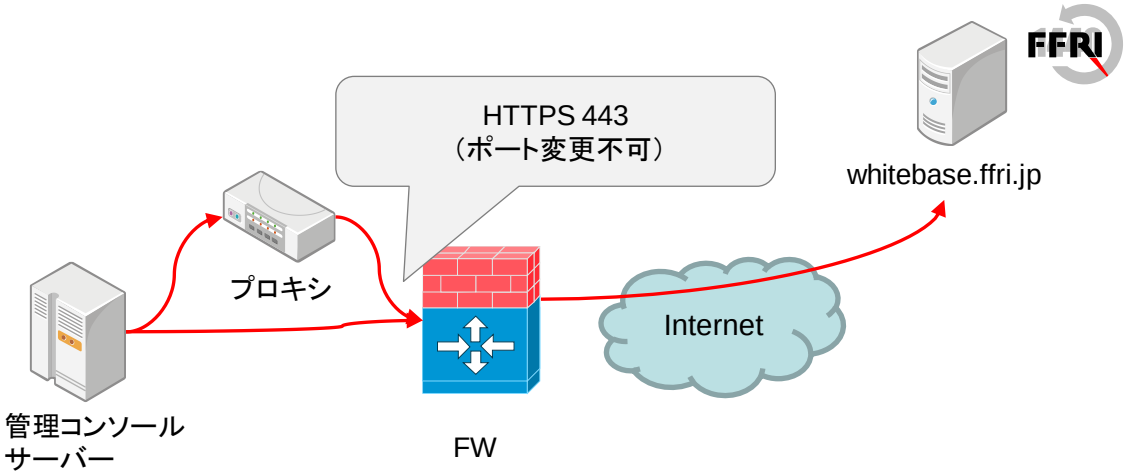
- スキップする場合には、管理コンソールサーバーのレジストリに以下のエントリを追加する。(再起動不要)
  [HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥FFR¥LicenseManager]
  "InternetOptionSecurityFlags"=dword:00000000
  - この設定を行った場合は、通信先サーバーが本物であることの保証はされない
  - HTTPSによる暗号化は行われる



FFRI AMC からインターネットへの通信（5/6）

確認方法 (whitebase.ffri.jp)

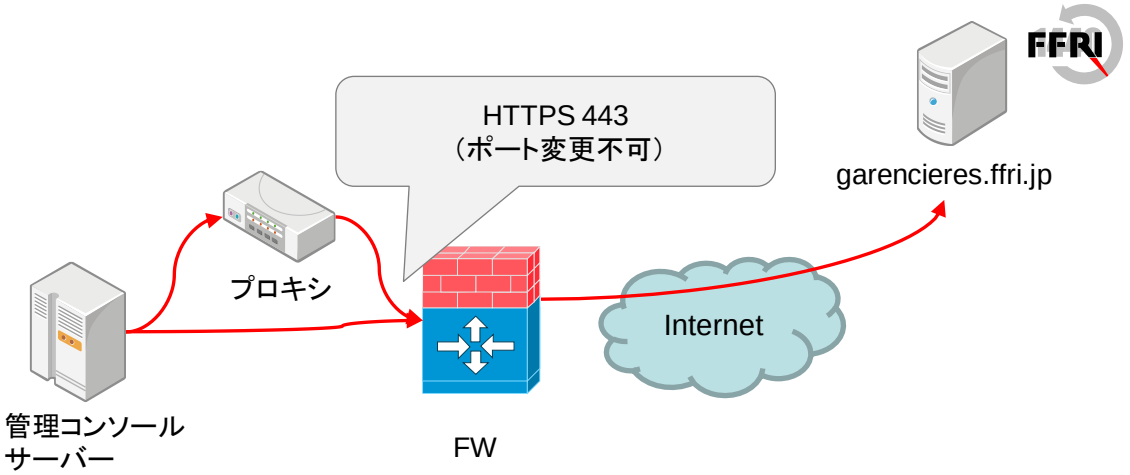
- プロキシを使用する場合は、 Internet Explorer にプロキシの設定をした上で、URL 欄に「 https://whitebase.ffri.jp/ 」を入力して、アクセスできるか確認
  - 画面に「whitebase.ffri.jp」という文字が表示されれば問題なし



FFRI AMC からインターネットへの通信（6/6）

確認方法 (garencieres.ffri.jp)

- プロキシを使用する場合は、 Internet Explorer にプロキシの設定をした上で、URL 欄に「 https://garencieres.ffri.jp/」を入力して、アクセスできるか確認
  - 画面に「garencieres.ffri.jp」という文字が表示されれば問題なし



ＦＦＲＩセキュリティがインターネットに公開しているサーバー

- ライセンスサーバー
  - ホスト名： yarai.fourteenforty.jp
  - IPアドレス： 変動します
  - ポート： 443
- アップデートサーバー
  - ホスト名： yarai.fourteenforty.jp
  - IPアドレス： 変動します
  - ポート： 443 または 80
- 過検出判定システムサーバー
  - ホスト名： whitebase.ffri.jp
  - IPアドレス： 変動します
  - ポート： 443
- クラウド連携サーバー
  - ホスト名： garencieres.ffri.jp
  - IPアドレス： 変動します
  - ポート： 443

SMTPサーバーとの通信

設定方法

- 管理コンソール上で SMTP サーバーの設定を行う (WebUI「ネットワーク設定」画面)

確認方法

- 管理コンソール WebUI ログイン画面のリンク「パスワードを忘れた場合はこちら」より、パスワードリセットメール送信にて確認可能

データベースサーバーとの通信

設定方法

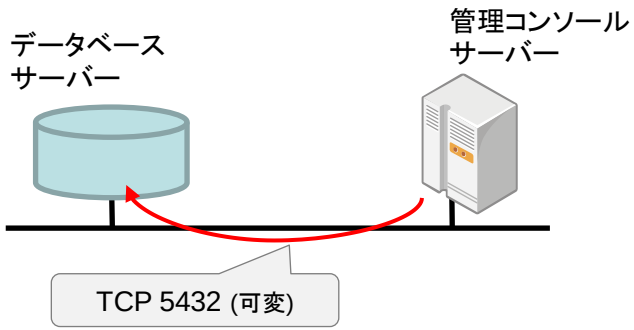
- セットアップマニュアル参照の上、データベースサーバー上のPostgreSQLの設定ファイルにて管理コンソールサーバーのホスト名/IPアドレスからの接続を許可後、 FW設定でポート開放する
- FFRI AMC インストール時にデータベースサーバーの情報を入力する
- FFRI AMC インストール後のデータベース設定情報変更についてはオペレーションマニュアル「保守」の項を参照する

確認方法

- [管理コンソールインストールディレクトリ]¥pgsql¥bin¥psql コマンドによって接続を確認可能
  例： psql -h hostname –p 5432 -U postgres

※実行するには PostgreSQL セットアップ時に指定したパスワードの入力が必要です。

オプション	入力値
-h	データベースサーバーのホスト名/IPアドレス
-p	データベースサーバーのポート番号 ※デフォルトであれば5432
-U	PostgreSQLのスーパーユーザー名 「postgres」



通信量の目安（1/9）

・v3.5.3 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	備考
ポーリング	約5.9KB	クライアントから管理コンソールへ定期的（デフォルト15分毎）に発生する通信。この通信により、管理コンソールからの命令を受け渡しする。
ポーリング	約6.2KB	Windows Defender 連携が有効の場合。
ポーリング	約7.1KB	ポリシー項目「検出エンジンのレジストリ情報をすべて収集」が有効の場合。
シャットダウン	約3.8KB	
ポリシー配布	約10.6KB	最低値の目安であり、例外リストなどの数によって増加。
ポリシー配布	約3.25MB	※計測時は英字例外パス1万件（サポート対象となる最大数）を含んだポリシーを配布して計測。
アクティベート配布	約11.1KB	年額版のみの通信。適用完了通知を含む。
ディアクティベート配布	約6.9KB	年額版のみの通信。適用完了通知を含む。
ライセンスチェックポーリング	約4.0KB	月額版のみの通信。クライアントから管理コンソールへ定期的（30分毎[変更不可]）に発生する通信。
デフォルト配布	約24.7KB	グループ名、ポリシー（例外リストなし）、ライセンスファイル、即時フルスキャン、ハッシュ計算をデフォルト配布設定して計測。 最低値の目安であり、例外リストなどの数によって増加。

通信量の目安（2/9）

・v3.5.3 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	備考
検出通知	約8.60KB	
検出通知 + 検体収集	約195.2KB	検体サイズ、検出エンジンによって変動。 ※計測時に収集したzipファイルサイズは180KB。
駆除（成功時）	約9.1KB	適用完了通知を含む。駆除ファイル数によって増加。 ※計測時に駆除を命令したファイルは1ファイル。
駆除（失敗時）	約586.5KB	「駆除失敗の詳細」適用完了通知を含む。「駆除失敗の詳細」画面に表示される一覧のファイル数によって増加。 ※計測時の「駆除失敗の詳細」に表示される内訳はレジストリ257件、ファイル3件。
「駆除失敗の詳細」削除	約12.2KB	適用完了通知を含む。駆除ファイル数によって増加。 ※計測時に削除を命令したファイルは1ファイル。
即時スキャン配布	約12.1KB	適用完了通知を含む。
スケジュールスキャン配布	約8.4KB	
Windows Defender コマンド配布	約9.3KB	※計測時の命令は「シグネチャーアップデート後にスキャン」。管理コンソールからクライアントへの命令の通信量であり、Windows Defender が実施する通信の量ではありません。

通信量の目安（3/9）

・v3.5.3 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	備考
アップデート配布	約51.1MB	アップデートモジュールサイズによって増加。適用完了通知を含む。 ※計測時に使用したアップデートモジュールサイズは49.5MB。
グループ配布	約6.7KB	
組織名更新	約6.7KB	
過検出抑制パッチ配布	約7.4KB	
プロキシ設定配布	約5.9KB	「プロキシサーバーを直接指定する」を設定し配布。
通信設定配布	約6.0KB	
アンインストール配布	約10.9KB	適用完了通知を含む。
初回計算完了通知	約5.9KB	
ハッシュ計算配布	約6.9KB	配布受信応答を含む。
ハッシュ計算停止配布	約6.9KB	配布受信応答を含む。

通信量の目安（4/9）

・v3.5.3 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	備考
ハッシュ検索配布	約2.0MB	※計測時は検索対象のハッシュを4万件配布。そのうち一度のポーリングで配布できる上限（デフォルト3万件）が配布された時点で計測。
ポーリング（ハッシュ検索中）	約696.2KB	配布している検索対象のハッシュの数によって変動。 ※上記「ハッシュ検索配布」に続くポーリングの応答にて残りの1万件を配布。その際の計測値。
ハッシュ検出通知	約4.5KB	
ハッシュ検出通知＋検出ログ収集	約6.5KB	収集するログファイルのサイズによって変動。 ※計測時に収集したzipファイルサイズは168B。
ハッシュ検索完了通知	約4.2KB	
ハッシュ検索停止配布	約10.3KB	適用完了通知を含む。
隔離命令配布	約7.3KB	適用完了通知を含む。
隔離解除配布	約6.9KB	適用完了通知を含む。

通信量の目安（5/9）

- v3.5.3 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	備考
クライアントのログ収集命令	約5.3KB	
クライアントのログ収集	約4.4MB	収集するログのzipファイルサイズによって通信量は変動。 ※計測時に収集したzipファイルサイズは4.35MB。 ログサイズは、配布ウィザード（ログ収集コマンド）における、収集オプションの有無やPC、yaraiの使用状況によって、数GBになる可能性がある。
クラウド連携	約2.1KB	年額版のみの通信。
ホワイトリスト連携	約3.2KB	年額版のみの通信。

通信量の目安（6/9）

- v3.5.3 の場合

■管理コンソール <－> アップデート&ライセンスサーバー（yarai.fourteenforty.jp）

イベント種類	通信量	備考
アップデートモジュール登録	約51.1MB	アップデートモジュールサイズによって増加。
オンラインライセンス認証	約5.0KB	

■管理コンソール <－> 過検出判定システムサーバー（whitebase.ffri.jp）

イベント種類	通信量	備考
過検出判定の問合せ	約4.2KB	1件あたりの目安。問合せ検出数によって増加。 ※計測時の参考値。 10件 6.7KB 70件 30.0KB 検体のアップロード時には検体サイズによって増加。

通信量の目安（7/9）

・v3.5.3 の場合

■管理コンソール ＜－＞ ネットワーク設定画面で設定するSMTPサーバー

イベント種類	通信量	備考
メール送信	約10.7KB	※計測は「通知設定」画面の「検出」の通知で確認。

■管理コンソール ＜－＞ ネットワーク設定画面で設定するファイルサーバー

イベント種類	通信量	備考
ファイルサーバーへの検体ファイル保存	約103KB	ファイルのサイズによって変動。 ※計測はテストマルウェア「yarai_StaticTest.exe(76KB)」の検体収集時。

■管理コンソール ＜－＞ネットワーク設定画面で設定するSyslogサーバー

イベント種類	通信量	備考
Syslog通知	約4.5KB	※計測は「通知設定」画面の「検出」のCEFフォーマットの通知、プロトコルはTCP(暗号化あり)で確認。

通信量の目安（8/9）

- v3.5.3 の場合

■管理コンソール <－> EDR自動化基本設定画面で設定するTAXIIサーバー

イベント種類	通信量	備考
TAXIIサーバーからのハッシュ情報取得	約8.8KB	配信情報が空であった時の計測値。
TAXIIサーバーからのハッシュ情報取得	約220KB	ハッシュ情報100件のみ取得した場合の計測値。 ハッシュ以外にもIPアドレスやホスト名等が配信される場合があり、それらの配信量によって通信量が都度変動。

通信量の目安（9/9）

・v3.5.3 の場合

■管理コンソール <－> クラウド連携サーバー（garencieres.ffri.jp）

イベント種類	通信量	備考
クラウド連携	約2.1KB	年額版のみの通信。
ホワイトリスト連携	約3.2KB	年額版のみの通信。

■クライアント <－> クラウド連携サーバー（garencieres.ffri.jp）

イベント種類	通信量	備考
クラウド連携	約2.1KB	
ホワイトリスト連携	約3.2KB	

※TLS 有効の状態で計測しています。
※通信状況によって、通信量は変化します。
※Wireshark での計測結果です。

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
  https://support.microsoft.com/ja-jp/help/832017/service-overview-and-network-port-requirements-for-windows

- FFRI AMC が採用しているWebサーバー（Apache）のアクセス制限機能（.htaccess）
  ※公式サイト（英語）
  https://httpd.apache.org/docs/2.4/mod/mod_authz_host.html#requiredirectives

- FFRI AMC に同梱されているOSSのバージョン（FFRI yarai システム要件ガイド）
  https://yarai.fourteenforty.jp/clients/common_documents/FFRI_yarai_System_requirements.pdf
  ※アクセスには認証が必要です。