

WatchGuard Firebox ファームウェア アップグレード手順書

最新のセキュリティ機能を維持するために、最短の手順で
アップグレードする方法をご案内いたします！



2021年3月19日

対象のUTM製品とバージョン



アップグレードが必要かどうかご確認ください

対象製品とバージョンは？

- Fireware v12.5.3以下 のFireboxデバイス ※XTMモデルは対象外です。
- spamBlocker（スパムメール対策機能）をご利用のデバイス



どのバージョンにアップグレードしますか？

- Fireware v12.5.4以上のバージョン（推奨：v12.5.7 ※2021年3月時点最新Ver）

WatchGuard UTM製品 IPアドレスの確認方法



WatchGuardのUTM製品に接続するにあたり、
製品のIPアドレスを知る必要があります。
このセクションでは接続の前に、IPアドレスを確認する方法を説明します。

※ IPアドレスをご存知の場合、スライド 7 からのアップグレード手順に進んでください。

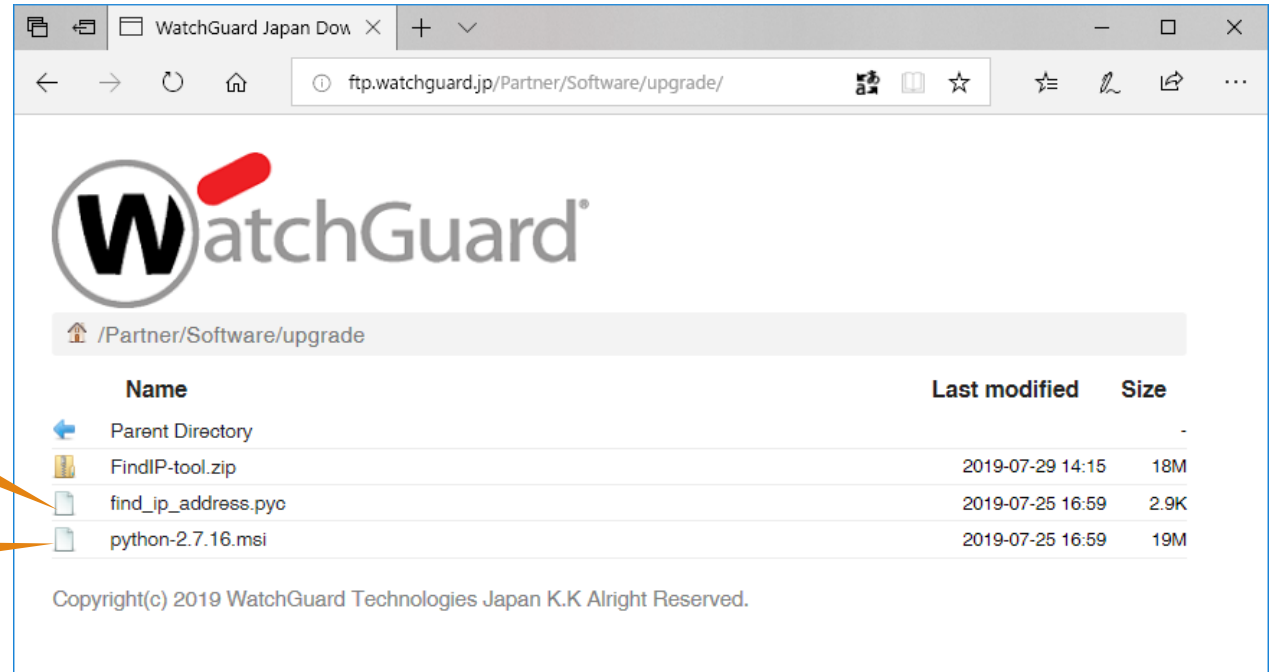
1. ツールのダウンロード

下記のサイトから2つのファイルをダウンロードしてください

- <http://ftp.watchguard.jp/Partner/Software/upgrade/>
- find_ip_address.pyc
- python-2.7.16

IPアドレス検索ツール

ツールの実行環境『Python』

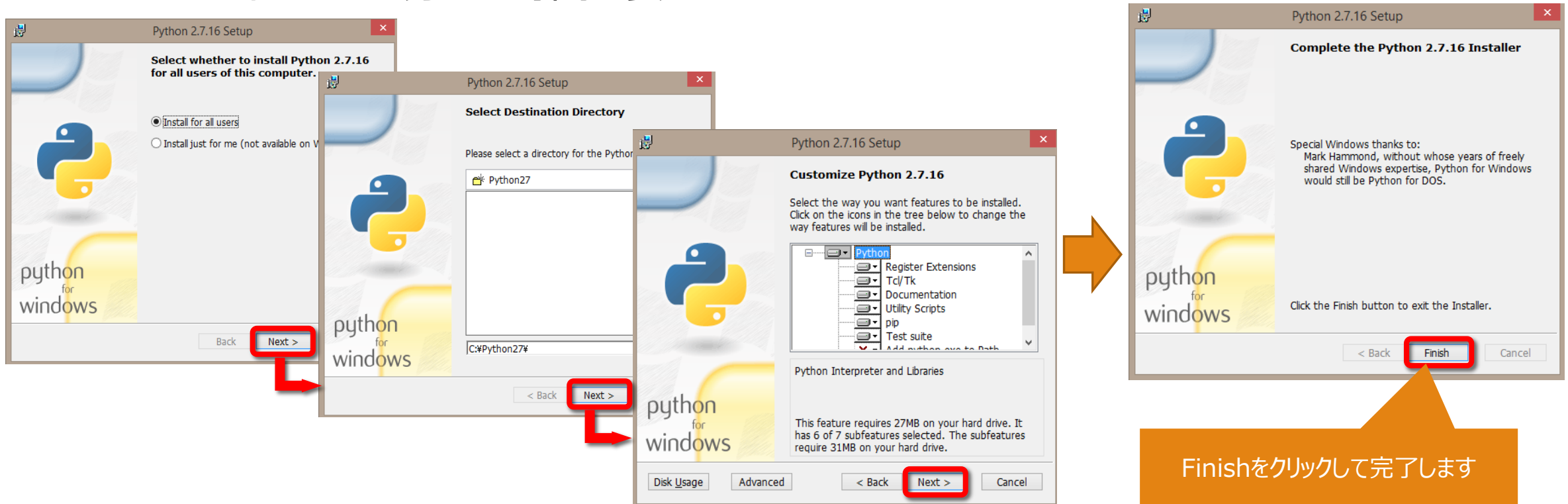


※ 万が一うまくダウンロードできない場合はFindIP-tool.zipをダウンロードし、デスクトップ上などの分かりやすい場所に解凍してください

2. Pythonのインストール

ダウンロードした“python-2.7.16.msi”を実行します。

- インストールに1分ほど時間を要します



Finishをクリックして完了します

3. IP検索ツールの実行

実行！

- ダウンロードしたもう一つのファイル find_ip_address.pyc を実行します。
- 実行後、以下のような画面が表示されます（約40秒）。

```
WatchGuard Technologies [ v1.0.3
(c) 2017, WatchGuard Technologies. All rights reserved.
```

```
Please waiting for about 40 seconds...
```

```
*****
```

```
Found following IP addresses:
```

```
10.0.1.1
```

```
Press any key to exit:
```

この欄に表示されたIPアドレスが UTM (Firebox) のIPアドレスになります。必ずメモしてください。

このIPアドレスをもとにWebブラウザでデバイスにアクセスします。

WatchGuard UTM製品 アップグレードの方法



WatchGuardのUTM製品のIPアドレスが分かりましたら
実際に製品に接続し、アップグレードを実行します。

アップグレード手順① UTM製品に接続



Webブラウザを使って接続します

URLは https://製品のIPアドレス:8080/

- 接続を試みると警告画面になりますが、問題ないのでそのままアクセスを続けてください



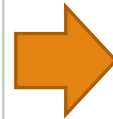
このサイトは安全ではありません

だれかがユーザーを騙そうとしているか、サーバーに送信されたデータを盗み取ろうとしている可能性があります。このサイトをすぐに閉じてください。

[スタートページに移動](#)

[詳細](#)

クリック！



詳細

お使いの PC はこの Web サイトのセキュリティ証明書を信頼しません。
Web サイトのセキュリティ証明書のホスト名が、参照しようとしている Web サイトと異なります。

エラー コード: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

[Web ページへ移動 \(非推奨\)](#)

クリック！

※ブラウザの警告画面が例と違い、進み方が分からない場合は、スライド17からの 付録 をご覧ください

アップグレード手順② Fireboxにログイン



管理者ユーザー『admin』でログインします

- ユーザー名 : admin
- パスフレーズ : 22222222

※このアカウントでログインできない場合は、担当者または販売店様にログイン情報をご確認ください。

アップグレード手順③ バージョンの確認



Web UIの画面右側にあるシステム情報で確認します

クリック！

左側メニュー フロントパネル をクリック

Fireware Web UI

ユーザー: admin

システム

名前	T15
モデル	T15
バージョン	12.5.3 xxxxx
シリアル番号	D0FE02950B3A0
システム時間	11:54 Asia/Tokyo

サービスは 30日以内に期限が切れます。
機能キーの更新

システム

名前	T15
バージョン	12.5.3 xxxxx
シリアル番号	D0FE02950B3A0
システム時間	11:54 Asia/Tokyo
システム日付	2019-07-22
稼働時間	0 days 01:37

バージョン表記が12.5.4以上であればアップグレードは不要です。
この図の例ではアップグレードが必要という判断になります。

アップグレード手順④ アップグレードの実行



Fireware Web UI

ユーザー: admin

OSのアップグレード

現行バージョン: 12.5.5 (Build 627719)
最新バージョン 12.5.7 (Build 635636) 新しいバージョン

watchguard.com から直接アップグレードをダウンロードおよびインストールする (推奨)

12.5.7 (Build 635636) アップグレード

12.5.7 (Build 635636)
12.5.6 (Build 633773)
12.5.5 (Build 630561)

ファイルの選択 ファイルが選択されていません アップグレード

OS アップグレード ファイルをダウンロードするには、次に移動します <http://software.watchguard.com>
EXE ファイルを実行してコンピュータに OS アップグレード ファイルをインストールするか、ZIP ファイルからファイルを抽出します。
インストーラを実行すると、ファイルはここに保存されます:

- 32-bit Windows - Program Files\Common Files\WatchGuard\resources\FirewareXTM\
- 64-bit Windows - Program Files (x86)\Common Files\WatchGuard\resources\FirewareXTM\

The OS upgrade files appear as either:

- T30_T50.sysa-dl
- *.wgpkg-dl (コンポーネント パッケージ)

左側メニュー
システム - OSアップグレード
をクリック

1
クリック!

実行!

2
バージョン12.5.7を選択

1. プルダウンメニューから目的のバージョンを選択
- 12.5.7 (Build xxxxxx)を選択
2. 選択したら、[アップグレード]をクリックして実行!

アップグレード手順⑤ 実行後の再起動



画面推移を確認し、製品を再起動します

処理が完了すると再起動を促すポップアップ画面が表示されますので、YESをクリックして再起動を実行します。

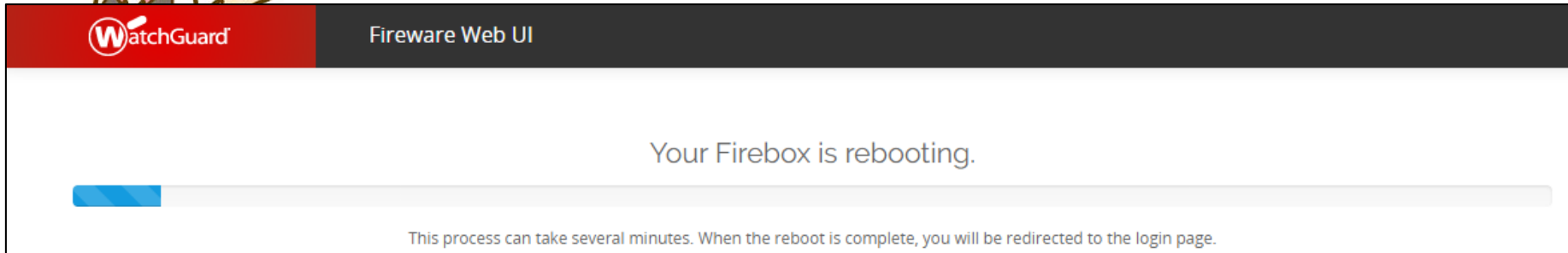
約30秒から1分程度、インジケータが全て青くなるまでお待ちください。

YESをクリック！

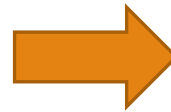
アップグレード手順⑥ 再起動中の画面推移



再起動には3～5分かかります



途中、エラーが表示される可能性がありますが無視していただいて結構です



再起動後、再びログインしてください

アップグレード手順⑦ アップグレード完了確認



アップグレード後のバージョンと動作を確認します

- 再起動実施後、起動までに3～5分かかります
- 目的のバージョンにアップグレードされているか確認
- Web閲覧やメール送受信などの動作確認

Fireware Web UI ユーザー : admin

フロントパネル

トップクライアント すべて表示

名前	レート	バイト	ヒット
192.168.1.8	1 Mbps	3 MB	70
192.168.1.9	1 Kbps	58 KB	1
192.168.1.250	bps	468	9

システム

名前	T30-W-Okawa-Home
モデル	T30-W
バージョン	12.5.7.B635636
シリアル番号	70AD0687D27F7
システム時間	17:51 Asia/Tokyo
システム日付	2021-03-18
稼働時間	0 days 00:07
サーバー	

12.5.7になっていればOKです。

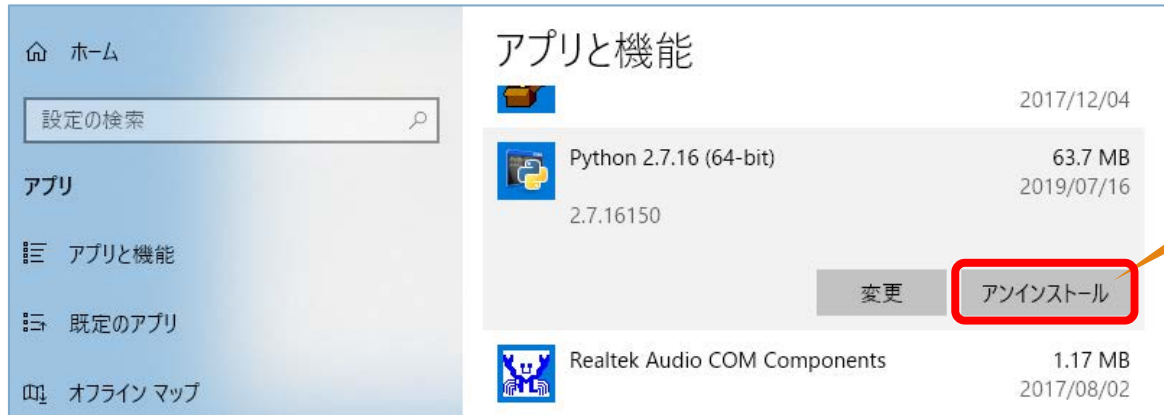
IPアドレス検索ツールの削除



アップグレード作業が完了したら、IPアドレス検索ツールは不要となります。
製品のIPアドレスを調べるためにツールをご使用の場合、
作業後にアンインストールおよびファイルを削除します。

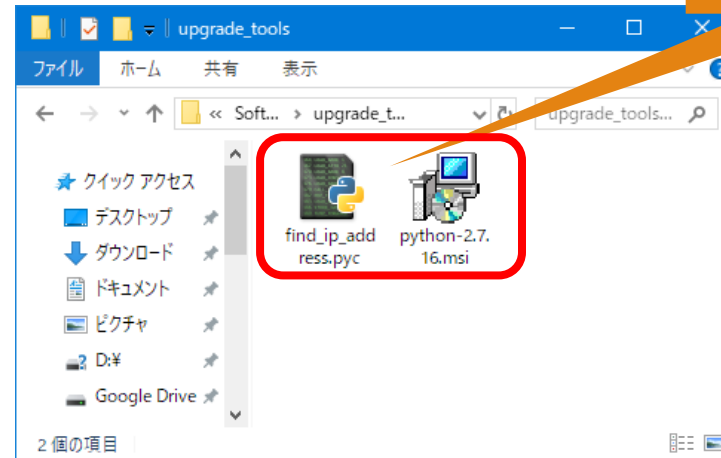
インストールしたPythonと検索ツールを削除

- アプリと機能の一覧から、Python 2.7.16 をアンインストールする



クリック！

- ダウンロードしたファイルを削除する



どちらも削除

付録：ブラウザのセキュリティ警告画面



Web UIで接続した際のセキュリティ警告表示が、ブラウザごとに違いがあります。
警告画面の先に進み方が分からない場合にご覧ください。

セキュリティ警告画面の例 (Edge / Internet Explorer)

Edge

このサイトは安全ではありません

だれかがユーザーを騙そうとしているか、サーバーに送信されたデータを盗み取ろうとしている可能性があります。このサイトをすぐに閉じてください。

[スタートページに移動](#)

詳細

クリック!

詳細

お使いの PC はこの Web サイトのセキュリティ証明書を信頼しません。
Web サイトのセキュリティ証明書のホスト名が、参照しようとしている Web サイトと異なります。

エラー コード: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

Web ページへ移動 (非推奨)

クリック!

Internet Explorer

このサイトは安全ではありません

だれかが利用者を騙そうとしているか、サーバーに送信されたデータを盗み取ろうとしている可能性があります。このサイトをすぐに閉じてください。

[このタブを閉じる](#)

詳細情報

クリック!

詳細情報

お使いの PC はこの Web サイトのセキュリティ証明書を信頼しません。
Web サイトのセキュリティ証明書のホスト名が、参照しようとしている Web サイトと異なります。

エラー コード: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

Web ページに移動 (非推奨)

クリック!

セキュリティ警告画面の例 (Chrome / Firefox)

Chrome

この接続ではプライバシーが保護されません

192.168.150.1 では、悪意のあるユーザーによって、パスワード、メッセージ、クレジットカードなどの情報が盗まれる可能性があります。詳細

NET::ERR_CERT_AUTHORITY_INVALID

一部のシステム情報とページのコンテンツを Google に送信して、セーフ ブラウジングの改善にご協力ください。 [プライバシー ポリシー](#)

クリック!

詳細設定

セキュリティで保護されたページに戻る

詳細情報を表示しない

セキュリティで保護されたページに戻る

このサーバーが **192.168.150.1** であることを確認できませんでした。このサーバーのセキュリティ証明書は、ご使用のパソコンのオペレーティング システムによって信頼されているものではありません。原因としては、不適切な設定や、悪意のあるユーザーによる接続妨害が考えられます。

クリック!

192.168.150.1 にアクセスする (安全ではありません)

Firefox

警告: 潜在的なセキュリティリスクあり

Firefox はセキュリティ上の潜在的な脅威を検知したため、10.0.55.1 への接続を中止しました。このサイトに訪問すると、攻撃者がパスワードやメールアドレス、クレジットカードの詳細な情報を盗み取ろうとする恐れがあります。

[詳細...](#)

クリック!

エラーを報告すると、悪意のあるサイトの特定とブロックに役立ちます

ウェブサイトは証明書で同一性を証明します。10.0.55.1:8080 は無効な証明書を使用しているため、Firefox はこのサイトを信頼しません。

エラーコード: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

[証明書を確認](#)

クリック!

戻る (推奨)

危険性を承知で続行