

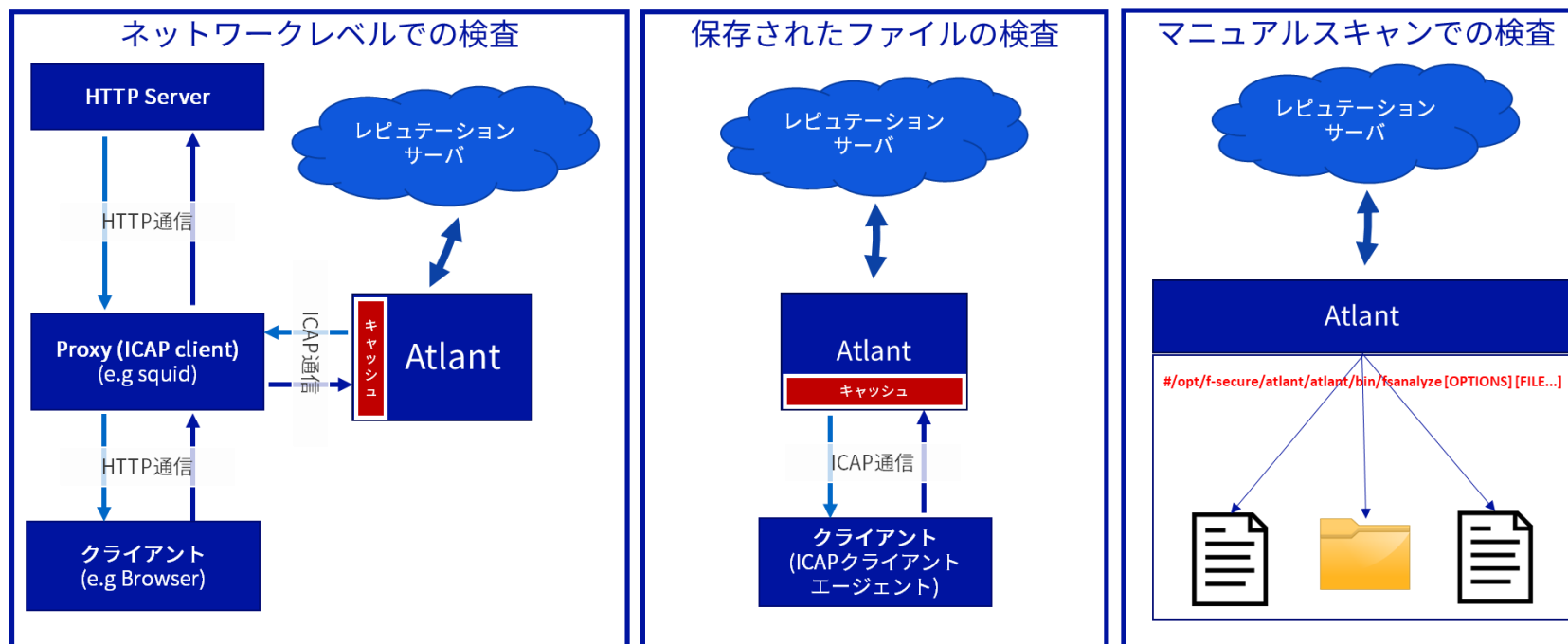


ATLANT WITH POLICY MANAGER

作成日：2021年5月12日

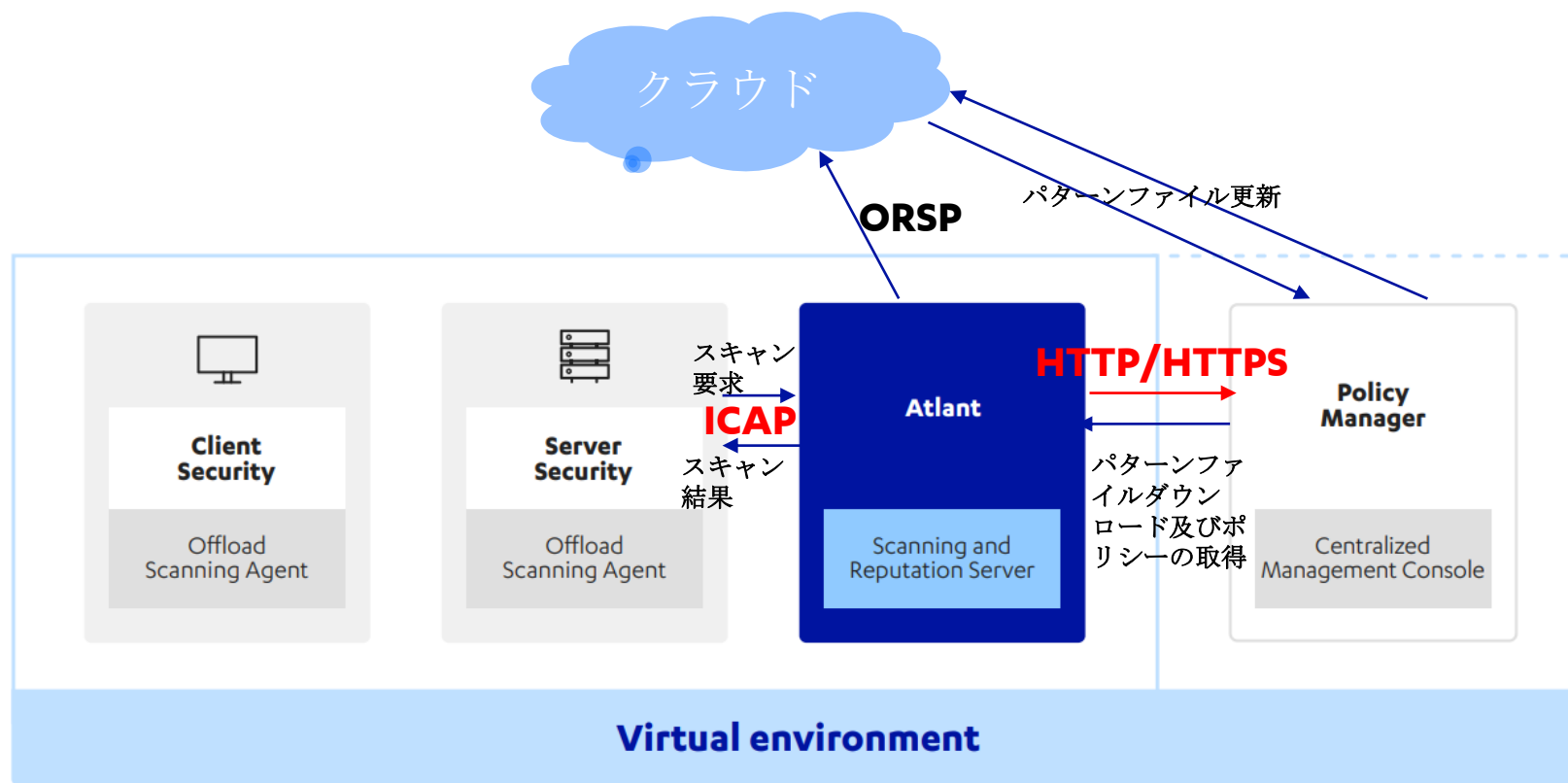
ATLANTとは - 1

Atlantは悪意あるファイルをスキャンする為のシステム構築用プラットフォームです。製品設定及びファイルスキャンはREST API経由で提供されます。また、ウィルスやその他の有害なファイル、エクスプロイト、ネットワークベースの攻撃及びその他のセキュリティ脅威からエンドポイントやネットワークを保護するため、ICAPプロトコル要求に基づいたスキャンサービスを提供します。



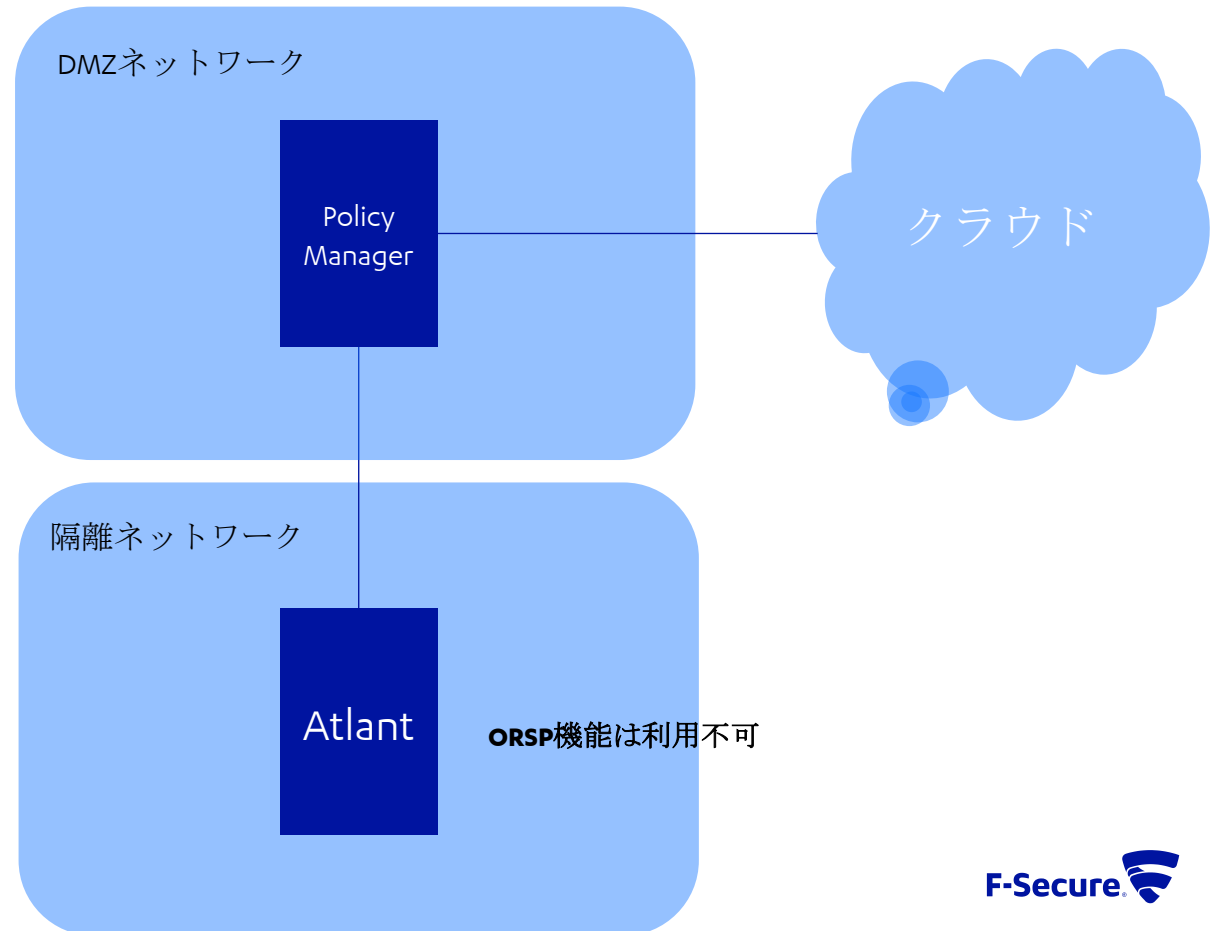
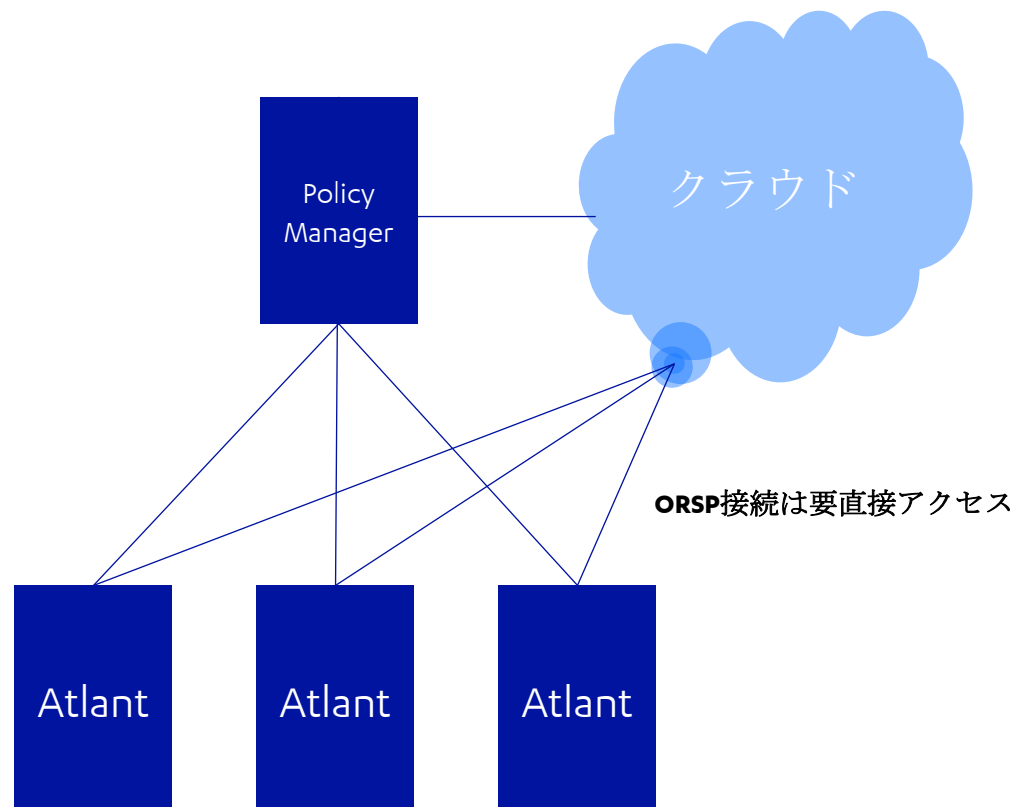
ATLANTとは - 2

Atlantは仮想環境でのスキャンングプラットフォームとしてご利用いただけます。F-Secureエンドポイント製品からのオフロードスキャンリクエストをAtlantにICAP経由で集約し、クライアント側にスキャン結果を提供します。エンドポイントでのスキャン負荷(CPU/メモリ/etc)が軽減されます。F-Secure Scanning and Reputation Server 12.20.5 virtual appliance(仮想スキャンサーバ)の後継として導入いただけます。クライアント側(Client Security / Server Security)は現行のエンドポイント製品(EOL前製品)のオフロードスキャン機能を使用します。

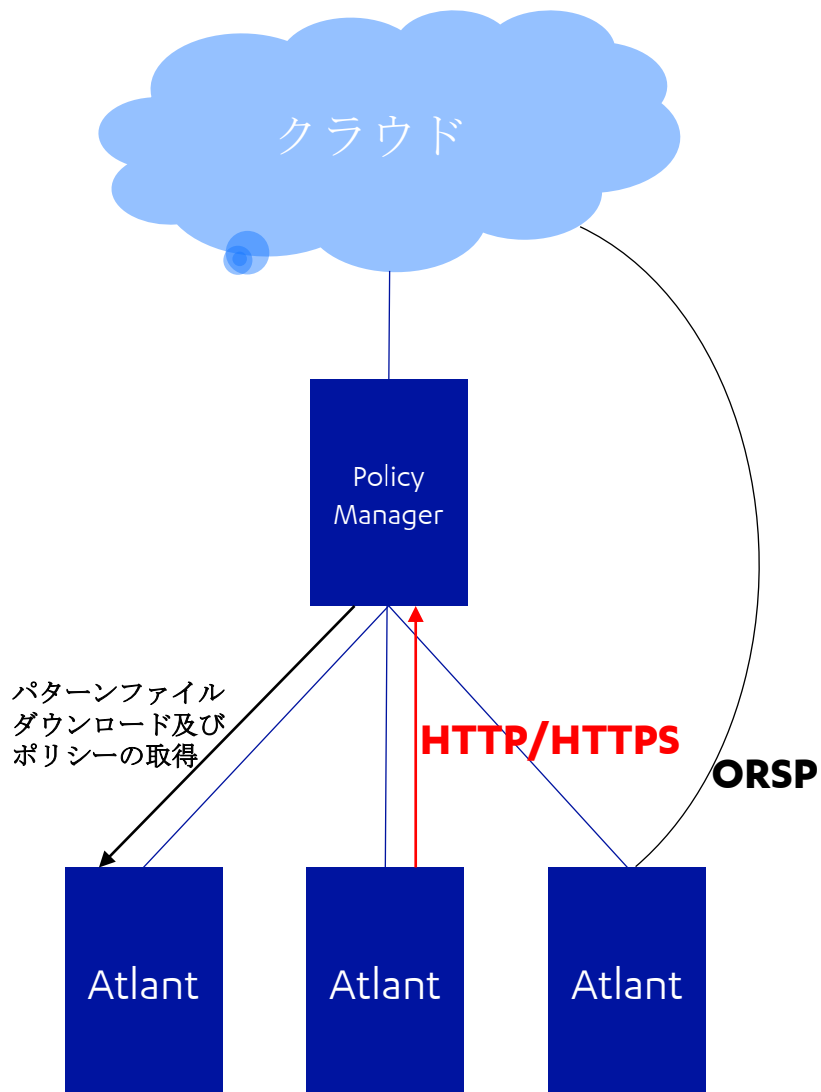


ATLANT の管理

- Atlantは直接クラウドへの接続を行います。複数台のAtlantサーバーを管理したい場合は、Policy Manager を使用します。@複数台のAtlantを1台のPolicyManagerで管理
- Atlantが直接外部のインターネット環境に接続できない場合、Policy Managerを使用してパターンファイルダウンロード等の中継を行います。@Atlantを隔離ネットワーク環境で運用

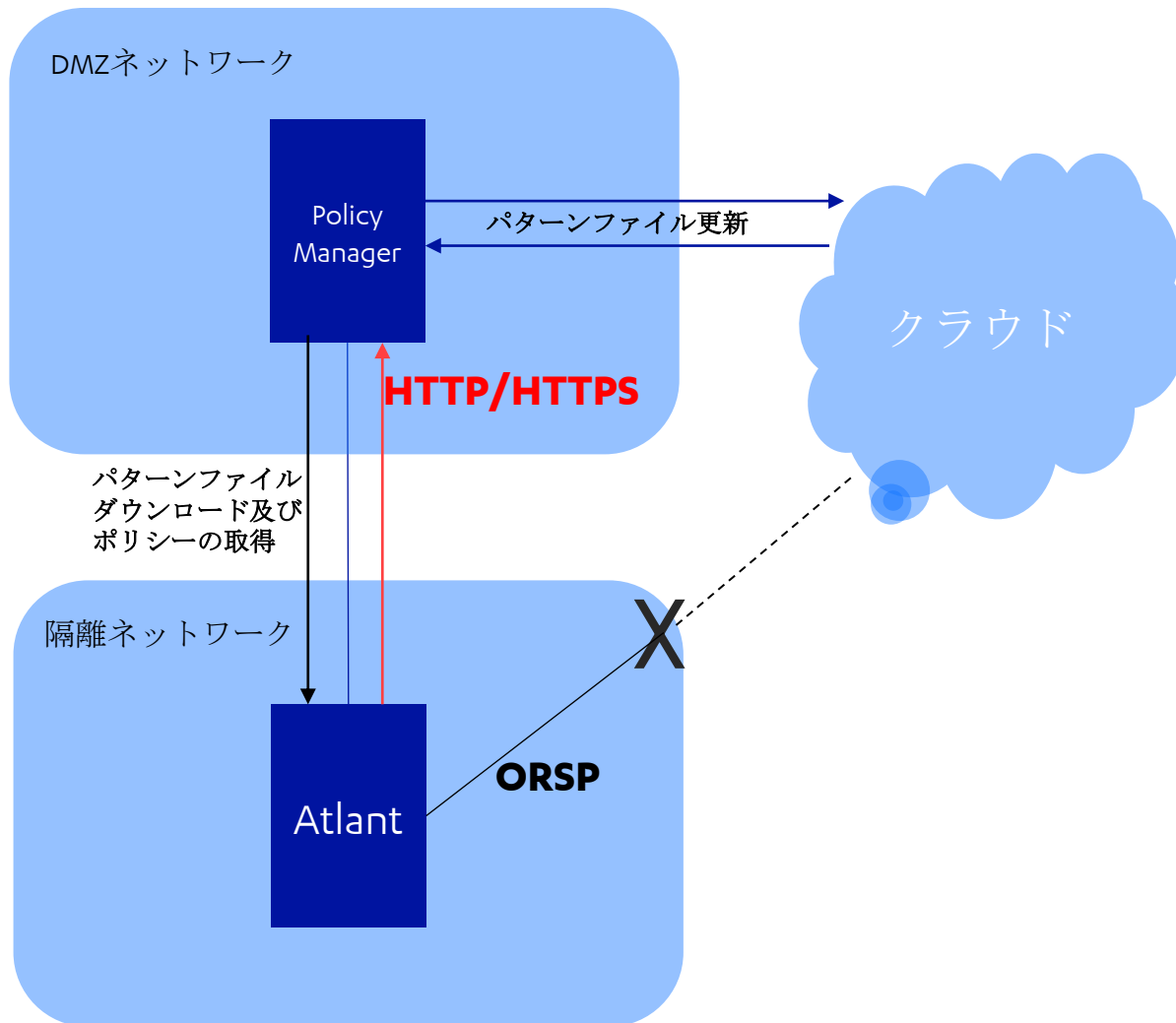


ATLANT の管理 @複数台のATLANTを1台のPOLICYMANAGERで管理



- ✓ Atlantへの設定はPolicyManagerからポリシー配信を行うことで設定することができます。
- ✓ すべてのAtlantはパターンファイル更新をPolicyManager経由で行うため、ネットワーク負荷が軽減されます。（クラウドへ最新のパターンファイルを取得しに行くのはPolicyManagerのみです。）
- ✓ PolicyManagerはAtlantからHTTP/HTTPSの通信を受け付けられるようにする必要があります。

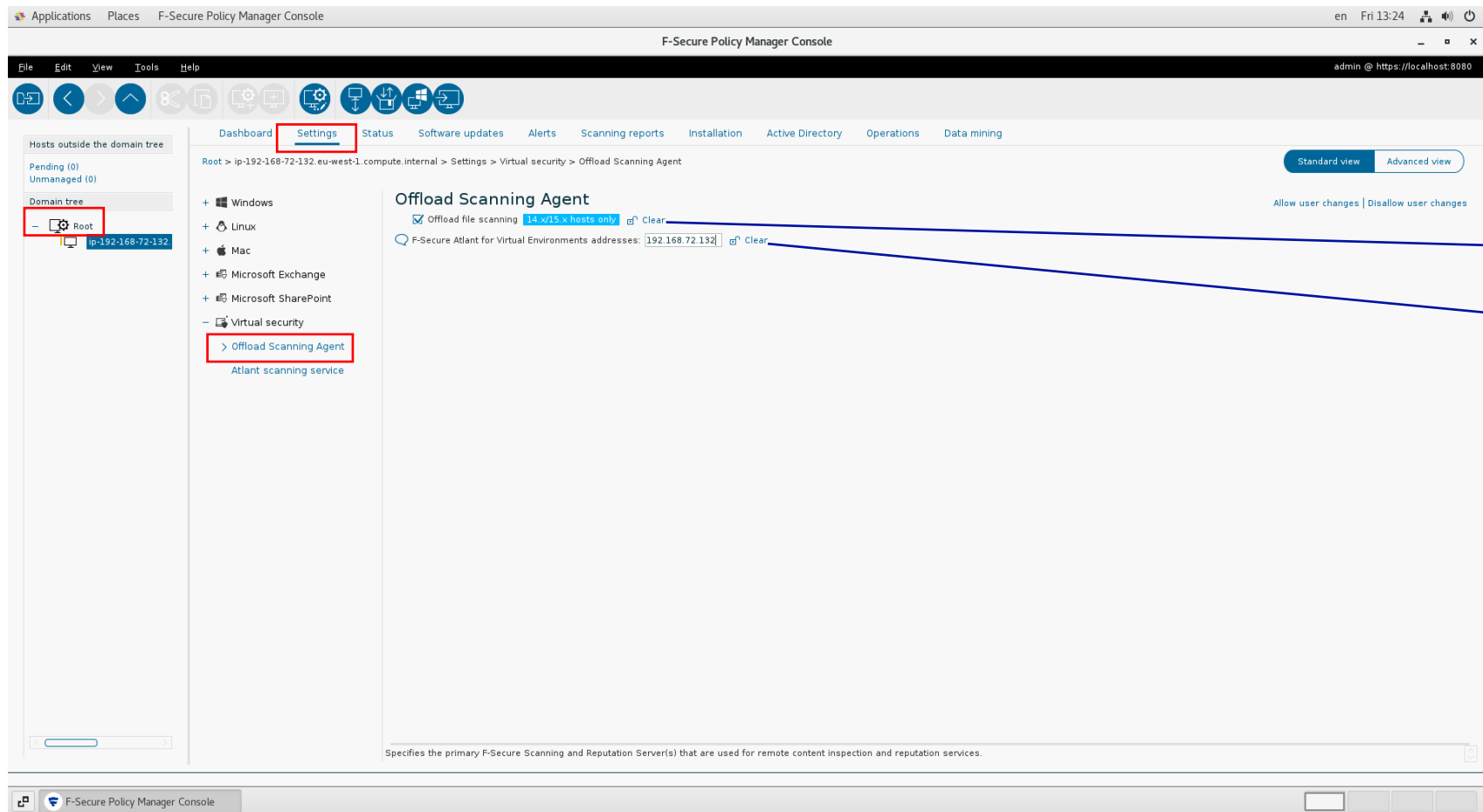
ATLANT の管理 @ATLANTを隔離ネットワーク環境で運用



- ✓ Atlantへの設定はPolicyManagerからポリシー配信を行うことで設定することができます。
- ✓ AtlantはDMZ環境にあるPolicyManagerからパターンファイル更新を行います。
- ✓ PolicyManagerはAtlantからHTTP/HTTPSの通信を受け付けられるようにする必要があります。
- ✓ Atlantは直接インターネットへ接続できないため、ORSPの機能は利用できません。

POLICYMANAGER (15.10) の管理画面-1

- ✓ スキャンレピュテーションサーバーとして利用する場合、「Root」ドメインを選択し下記設定を有効、及びAtlantのIPアドレスを指定してポリシーを配布する必要があります。



Offload file scanning設定のON/OFF

Atlantホストのアドレスを設定

本設定はWindowsクライアントに対して、オフロードスキャンを使用するかどうか、及びAtlantへの接続に使用するアドレスを通知します。

設定の詳細は下記URLを参照してください。
https://help.f-secure.com/product.html#business/atlant/latest/en/task_9446E84598264D58957A27FE19B5664D-latest-en

POLICYMANAGER (15.10) の管理画面-2

✓ 下記の設定について、Policy Manager Consoleから設定を変更することができます。

The screenshot displays the F-Secure Policy Manager Console interface. The left sidebar shows a domain tree with 'Root' and 'ip-192-168-72-137'. The main content area is titled 'Atlant scanning service' and contains the following sections:

- Atlant subscription:** Includes a 'Subscription key' input field and a note: 'Note: The subscription key is optional. It is needed to enable advanced features not covered by the Business Suite license.'
- General:** Includes checkboxes for 'Check file reputation' and 'Check URL reputation', and input fields for 'Timeout for reputation requests', 'Maximum scanning time', 'Keep client connections alive', and 'Scan archives up to nesting level'.
- Endpoints:** A table with columns 'Active', 'Address', and 'Port'. It contains one entry with 'Active' checked, 'Address' '0.0.0.0', and 'Port' '1944'. Buttons for 'Add', 'Edit', 'Force table', and 'Clear table' are visible.

Blue arrows point from the following Japanese text labels to the corresponding UI elements in the screenshot:

- プレミアムサブスクリプションキーを入力 (サンドボックススキャン機能を利用する場合) → Subscription key input field
- ファイルレピュテーション設定のON/OFF → Check file reputation checkbox
- URLレピュテーション設定のON/OFF → Check URL reputation checkbox
- レピュテーションリクエストのタイムアウト時間 → Timeout for reputation requests input field
- 最大スキャン時間 → Maximum scanning time input field
- クライアントとの接続時間 → Keep client connections alive input field
- スキャンを行うアーカイブファイルの階層レベル → Scan archives up to nesting level input field
- ICAPの接続元アドレス及び待ち受けポート番号 → Address and Port input fields in the Endpoints table

ATLANT側の設定

- ✓ Policy Managerから変更できる設定は、`#/opt/f-secure/atlant/atlant/bin/atlantctl get` コマンドで表示される下記の設定に該当します。（※これらの設定はfsanalyzeコマンドでのスキャン設定に該当するものではありません。）

```
{,
  "scanning": {
    "archive_max_nested": 5,
    .
    .
    .
  },
  "https_endpoints": [],
  "icap_endpoints": [
    {
      "address": "0.0.0.0",
      "port": 1344
    }
  ],
  "keepalive_time": 600,
  "max_scan_time": 90,
  "reputation": {
    "file_check": true,
    "timeout": 5,
    "url_check": true
  }
},
```

スキャンを行うアーカイブファイルの階層レベル

接続元アドレス

待ち受けポート番号

クライアントとの接続時間

最大スキャン時間

ファイルレピュテーション設定のON/OFF

レピュテーションリクエストのタイムアウト時間

URLレピュテーション設定のON/OFF

インストールレーションガイド-1

インストールの流れ

- Policy Manager Server上にインストールパッケージ作成用のJarファイルをダウンロードします。

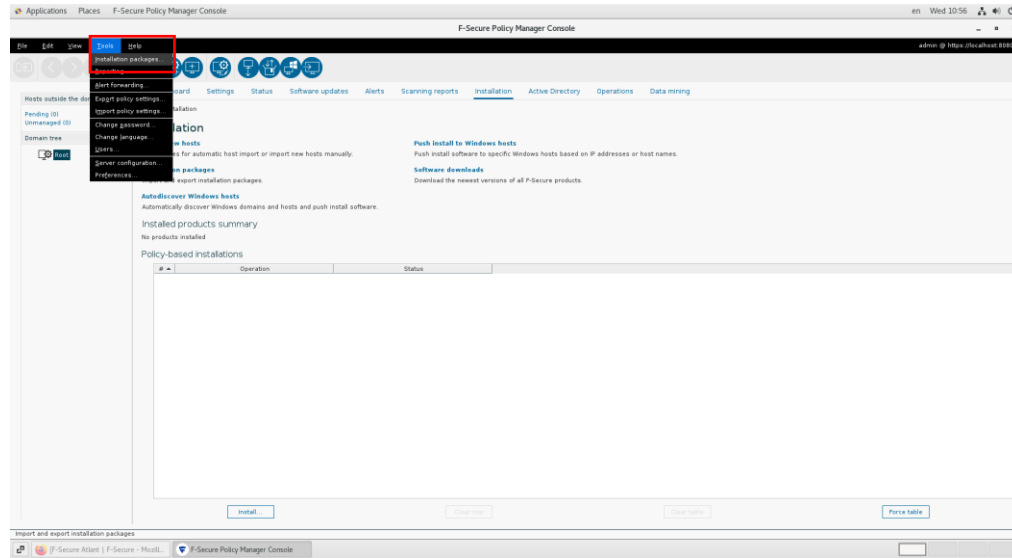
※Jarファイルは下記URLからダウンロードすることができます。

<https://www.f-secure.com/jp-ja/business/downloads/atlant>

※Policy Manager Ver15.00以降で運用する必要があります。

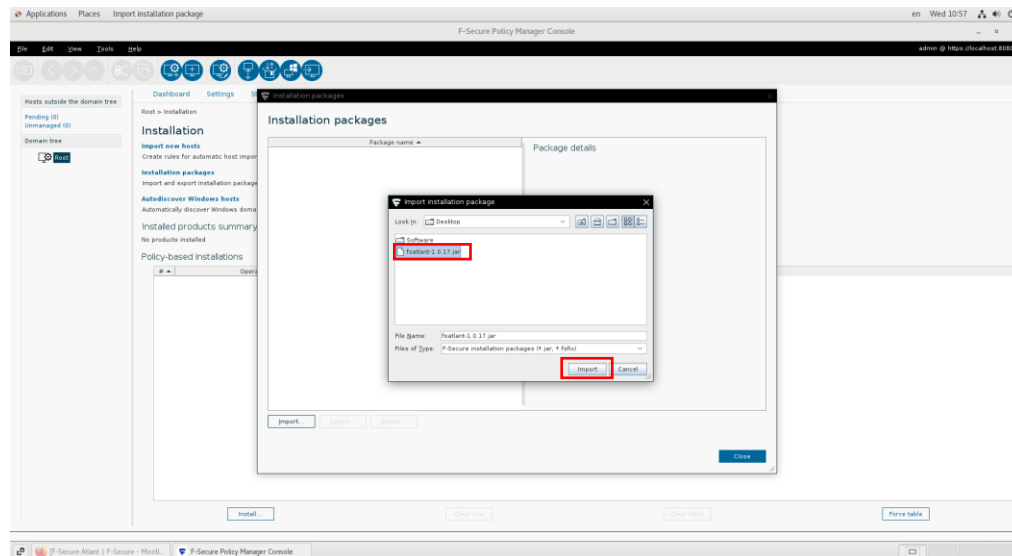
- ダウンロードしたJarファイルをPolicy Manager Consoleからインポートして、手順に従いインストールパッケージを作成します
- Policy Manager上で作成したインストールパッケージを、Atlantをインストールするサーバー上へ持っていきインストールします。

POLICY MANAGERでのインストールパッケージ作成-1



1. Toolメニューの[Installation packages...]を開きます。

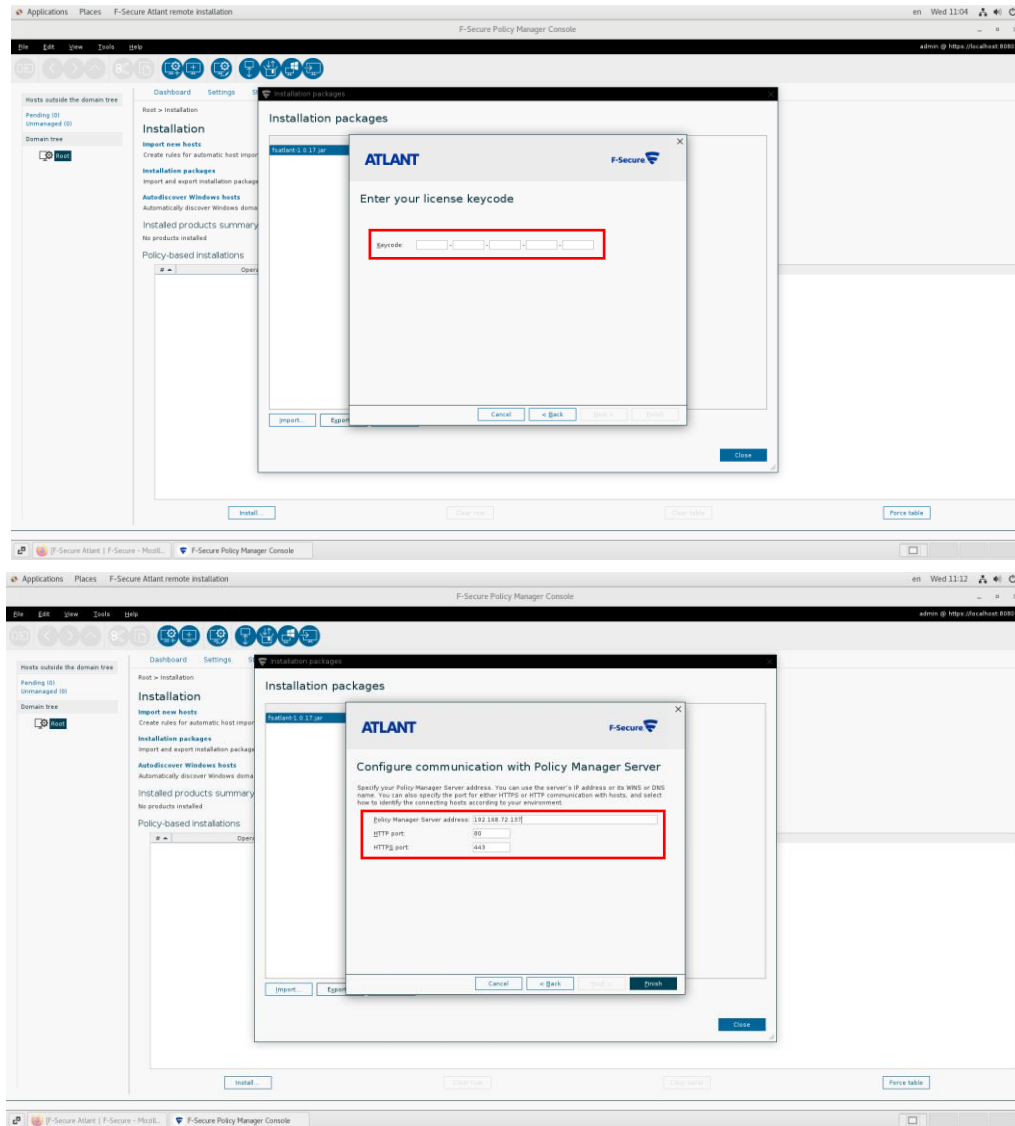
2. [Import]をクリックしてダウンロードしたJarファイル（fsatlant-x.x.xx.jar）を指定してインポートします。



3. Package nameの一覧にインポートした上記Jarファイルが表示されるので、それを選択して[Export]をクリックします。

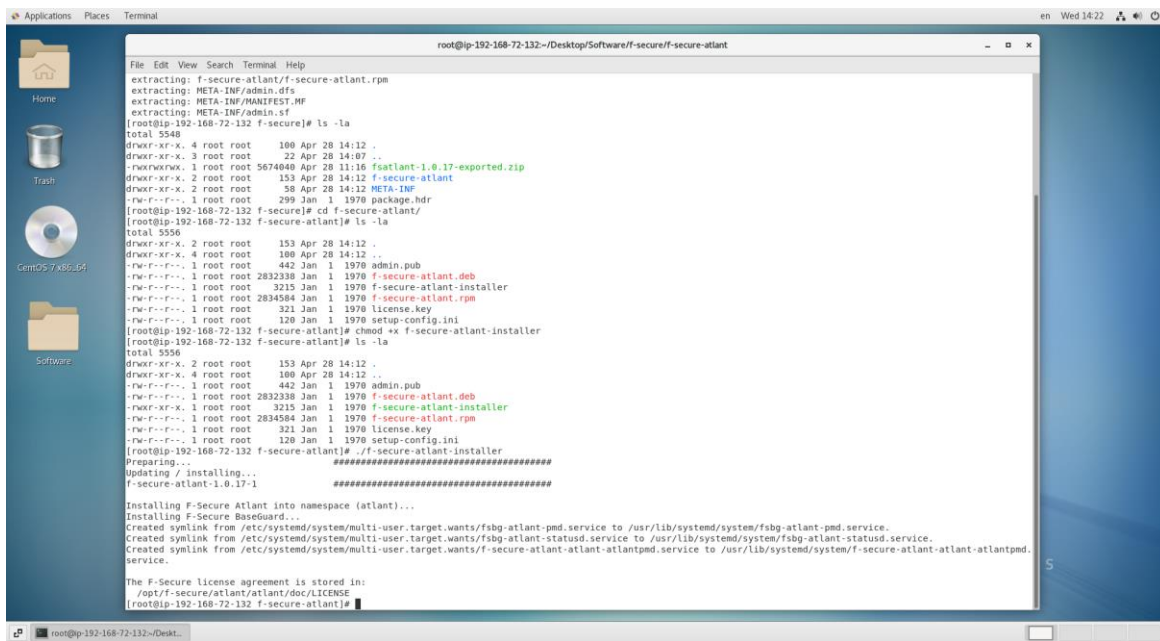
4. Atlantインストールパッケージのエクスポート先のパスを指定します。

POLICY MANAGERでのインストールパッケージ作成-2



5. ウィザードが開くので[Next]を押下します。
6. キーコードを入力して[Next]を押下します。
7. ポリシーマネージャサーバーのIPアドレス、HTTP/HTTPSの待ち受けポート番号を入力して[Finish]を押下します。
8. 前頁4.で指定した場所にインストーラが作成されます。
(ファイル名 : fsatlant-x.x.xx-exported.zip)

ATLATNのインストール (CENTOS7へのインストール例)

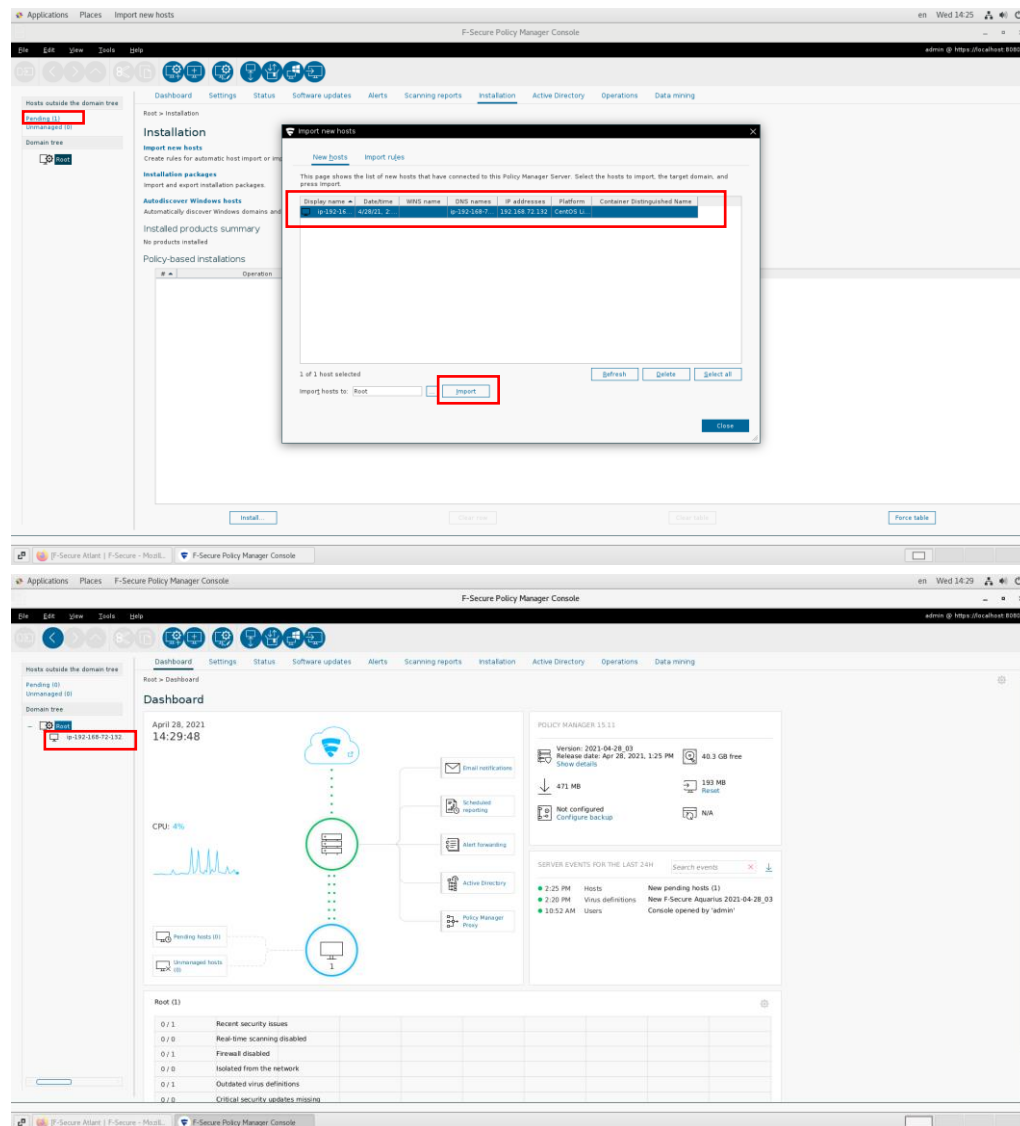


```
root@ip-192-168-72-132:~/Desktop/Software/f-secure/f-secure-atlant
extracting: f-secure-atlant/f-secure-atlant.rpm
extracting: META-INF/admin.dfs
extracting: META-INF/MANIFEST.MF
extracting: META-INF/admin.sf
[root@ip-192-168-72-132 f-secure]# ls -la
total 5548
drwxr-xr-x. 4 root root   100 Apr 28 14:12 .
drwxr-xr-x. 3 root root    22 Apr 28 14:07 ..
-rw-r--r--. 1 root root 5674040 Apr 28 11:16 fsatlant-1.0.17-exported.zip
drwxr-xr-x. 2 root root   153 Apr 28 14:12 f-secure-atlant
drwxr-xr-x. 2 root root    58 Apr 28 14:12 META-INF
-rw-r--r--. 1 root root   290 Jan 1 1970 package.hdr
[root@ip-192-168-72-132 f-secure]# cd f-secure-atlant/
[root@ip-192-168-72-132 f-secure-atlant]# ls -la
total 5556
drwxr-xr-x. 2 root root   153 Apr 28 14:12 .
drwxr-xr-x. 4 root root   100 Apr 28 14:12 ..
-rw-r--r--. 1 root root   442 Jan 1 1970 admin.pub
-rw-r--r--. 1 root root 2832338 Jan 1 1970 f-secure-atlant.deb
-rw-r--r--. 1 root root 3215 Jan 1 1970 f-secure-atlant-installer
-rw-r--r--. 1 root root 2834584 Jan 1 1970 f-secure-atlant.rpm
-rw-r--r--. 1 root root   321 Jan 1 1970 license.key
-rw-r--r--. 1 root root   120 Jan 1 1970 setup-config.ini
[root@ip-192-168-72-132 f-secure-atlant]# chmod +x f-secure-atlant-installer
[root@ip-192-168-72-132 f-secure-atlant]# ls -la
total 5556
drwxr-xr-x. 2 root root   153 Apr 28 14:12 .
drwxr-xr-x. 4 root root   100 Apr 28 14:12 ..
-rw-r--r--. 1 root root   442 Jan 1 1970 admin.pub
-rw-r--r--. 1 root root 2832338 Jan 1 1970 f-secure-atlant.deb
-rw-r--r--. 1 root root 3215 Jan 1 1970 f-secure-atlant-installer
-rw-r--r--. 1 root root 2834584 Jan 1 1970 f-secure-atlant.rpm
-rw-r--r--. 1 root root   321 Jan 1 1970 license.key
-rw-r--r--. 1 root root   120 Jan 1 1970 setup-config.ini
[root@ip-192-168-72-132 f-secure-atlant]# ./f-secure-atlant-installer
Preparing...
Updating / Installing...
f-secure-atlant-1.0.17-1
*****
Installing F-Secure Atlant into namespace (atlant)...
Installing F-Secure BaseGuard...
Created symlink from /etc/systemd/system/multi-user.target.wants/fsbg-atlant-pmd.service to /usr/lib/systemd/system/fsbg-atlant-pmd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/fsbg-atlant-statusd.service to /usr/lib/systemd/system/fsbg-atlant-statusd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/f-secure-atlant-atlant-atlantpmd.service to /usr/lib/systemd/system/f-secure-atlant-atlant-atlantpmd.service.
The F-Secure license agreement is stored in:
/opt/f-secure/atlant/atlant/doc/LICENSE
[root@ip-192-168-72-132 f-secure-atlant]#
```

1. Atlantをインストールするサーバーにパッケージ（fuse-libs, libcurl,python）がインストールされているか確認します。
2. ポリシーマネージャサーバー上で作成したインストーラー（fsatlant-x.x.xx-exported.zip）をAtlantをインストールするサーバー上の任意のディレクトリにコピーします。
3. Zipファイルを展開し、f-secure-atlant-installerに実行権限を付与します。
4. root権限でインストールコマンドを実行してインストールします。

コマンド実行例：# ./f-secure-atlant-installer

POLICY MANAGERへのインポート



1. インストール完了後、ポリシーマネージャーコンソールの[Pending]にホスト情報が確認できます。
2. 新しいホストを選択して[Import]を押下することでRootドメイン配下にAtlant端末が追加されます。

インストールレーションガイド-2

Atlant VAの場合

インストールの流れ

- Policy Manager Server上にインストールパッケージ作成用のJarファイルをダウンロードします。

※Jarファイルは下記URLからダウンロードすることができます。

<https://www.f-secure.com/jp-ja/business/downloads/atlant>

※Policy Manager Ver15.00以降で運用する必要があります。

- ダウンロードしたJarファイルをPolicy Manager Consoleからインポートして、手順に従いインストールパッケージを作成します。

- .ovaファイルをダウンロードし仮想化環境上にデプロイします。

※.ovaファイルは下記URLからダウンロードすることができます。

<https://www.f-secure.com/jp-ja/business/downloads/atlant>

- Atlant VAの初期セットアップの中で、上記で作成したインストーラーをscpコマンドにてAtlant VA上へコピーを行いインストールを実行する。

ATLANT VAのインストール①

- Policy Managerでのインストーラーの作成手順については、前項「インストレーションガイド-1」をご参照ください。

```
F-Secure Atlant Virtual Appliance 1.0.13 Installation

Choose the keymap group from the list

1.  Belgian (be-latin1) .. Dutch
2.  Estonian .. Italian
3.  Japanese .. Russian
4.  Serbian .. Ukrainian
5.  United Kingdom .. United States

Enter a menu number: 5

Choose the keymap group from the list (United Kingdom .. United States)

1.  United Kingdom
2.  United States
0.  Go back

Enter a menu number [0]: 2

United States keymaps

1.  U.S. International
2.  U.S. English
0.  Go back

Enter a menu number [0]: 2

Set the keymap to us? y/n [n]: y
```

1. ダウンロードした.ovaファイル (atlant-va-x.x.xx-vmware.ova) を仮想環境上にインポートします。
2. インポートした仮想イメージを起動すると初期セットアップが始まります。
3. 環境に合わせてキーボードを設定します。

※左図はキーボードをU.S.Englishに設定した場合の例になります。

ATLANT VAのインストール②

```
The keymap us was set successfully

Choose the timezone group from the list

1. Africa .. Australia
2. Europe .. UTC

Enter a menu number: 1

Choose the timezone group from the list (Africa .. Australia)

1. Africa
2. America/Adak .. Iqaluit
3. America/Jamaica .. Yellowknife
4. Antarctica
5. Arctic
6. Asia/Aden .. Krasnoyarsk
7. Asia/Kuala_Lumpur .. Yerevan
8. Atlantic
9. Australia

0. Go back

Enter a menu number [0]: 7

Asia/Kuala_Lumpur .. Yerevan

1. Kuala_Lumpur .. Nicosia
2. Novokuznetsk .. Qostanay
3. Qyzylorda .. Taipei
4. Tashkent .. Ust-Nera
5. Vientiane .. Yerevan

0. Go back

Enter a menu number [0]: 4

Asia/Kuala_Lumpur .. Yerevan (Tashkent .. Ust-Nera)

1. Tashkent
2. Tbilisi
3. Tehran
4. Thimphu
5. Tokyo
6. Tomsk
7. Ulaanbaatar
8. Urumqi
9. Ust-Nera

0. Go back

Enter a menu number [0]: 5

Set the timezone to Asia/Tokyo? y/n [n]: y

Timezone Asia/Tokyo set successfully

Changing password for user admin.
New password:
Retype new password:
```

4. タイムゾーンを任意の地域に設定します。

※左図はタイムゾーンをTokyoに設定した例になります。

5. 管理者パスワードを設定します。

ATLANT VAのインストール③

```
Setting up the network
Please choose the network type
1.  Configure using DHCP
2.  Configure manual IP
Enter a menu number: 1
The network has been set up successfully!

Select if you want to use HTTP proxy during activation
1.  Activate using HTTP proxy
2.  Activate without using HTTP proxy
Enter a menu number: 2

Select the appliance management mode
1.  Policy Manager
2.  Standalone
Enter a menu number: 1
You need to upload the exported zip bundle to the appliance.
The bundle file will be used to activate the product and will
be deleted by the installer.
Please upload the exported zip bundle using the command:

scp <path-to-zip-bundle> admin@192.168.72.147:/tmp/atlant-exported.zip

Press Ctrl-C to cancel.
Press enter when the archive is uploaded...
```

6. ネットワークを設定します。

※左図はDHCPを選択した例になります。

7. 必要に応じてHTTPプロキシを設定します。

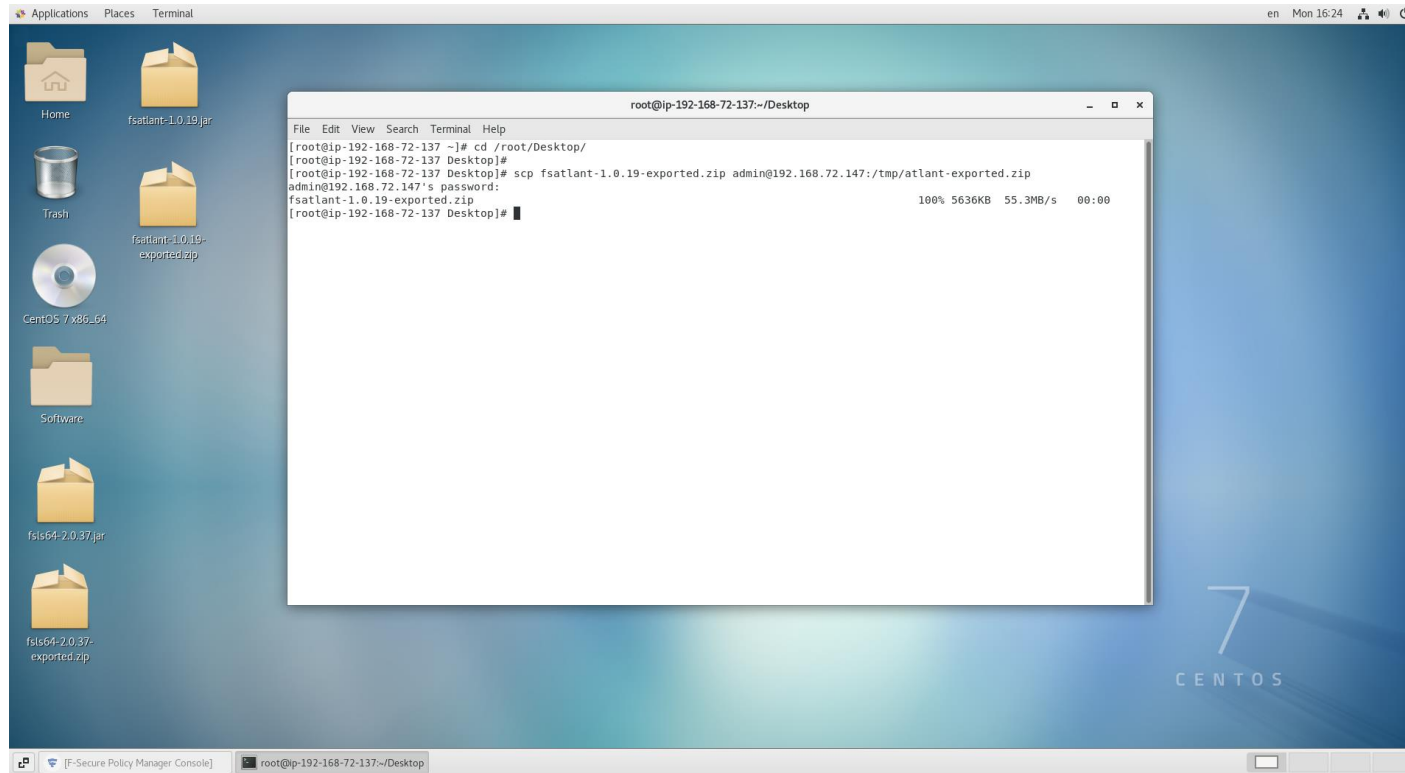
※左図はHTTPプロキシを設定しない場合の例になります。

8. PolicyManager連携するかStandaloneで使用するかを選択します。

※左図はPolicyManager連携を選択した例になります。

PolicyManager側で実行するscpコマンドの例

ATLANT VAのインストール④



9. PolicyManager側でscpコマンドを実行し、atlantのインストーラをコピーします。
10. パスワードは先ほど「5.」で設定した管理者パスワードを入力します。

※インストールパッケージの作成手順については、本ドキュメントの「インストレーションガイド-1」を参照してください。

ATLANT VAのインストール⑤

```
1. Policy Manager
2. Standalone

Enter a menu number: 1
You need to upload the exported zip bundle to the appliance.
The bundle file will be used to activate the product and will
be deleted by the installer.
Please upload the exported zip bundle using the command:

    scp <path-to-zip-bundle> admin@192.168.72.147:/tmp/atlant-exported.zip

Press Ctrl-C to cancel.

Press enter when the archive is uploaded...

Found the file!
Verifying... #####
Preparing... #####
Updating / installing...
f-secure-atlant-1.0.20-1 #####

Installing F-Secure Atlant into namespace (atlant)...
Installing F-Secure BaseGuard...
Created symlink /etc/systemd/system/multi-user.target.wants/fsbg-atlant-pmd.service → /usr/lib/systemd/system/fsbg-atlant-pmd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/fsbg-atlant-statusd.service → /usr/lib/systemd/system/fsbg-atlant-statusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/f-secure-atlant-atlant-atlantpmd.service → /usr/lib/systemd/system/f-secure-atlant-atlant-atlantpmd.service.

The F-Secure license agreement is stored in:
/opt/f-secure/atlant/atlant/doc/LICENSE

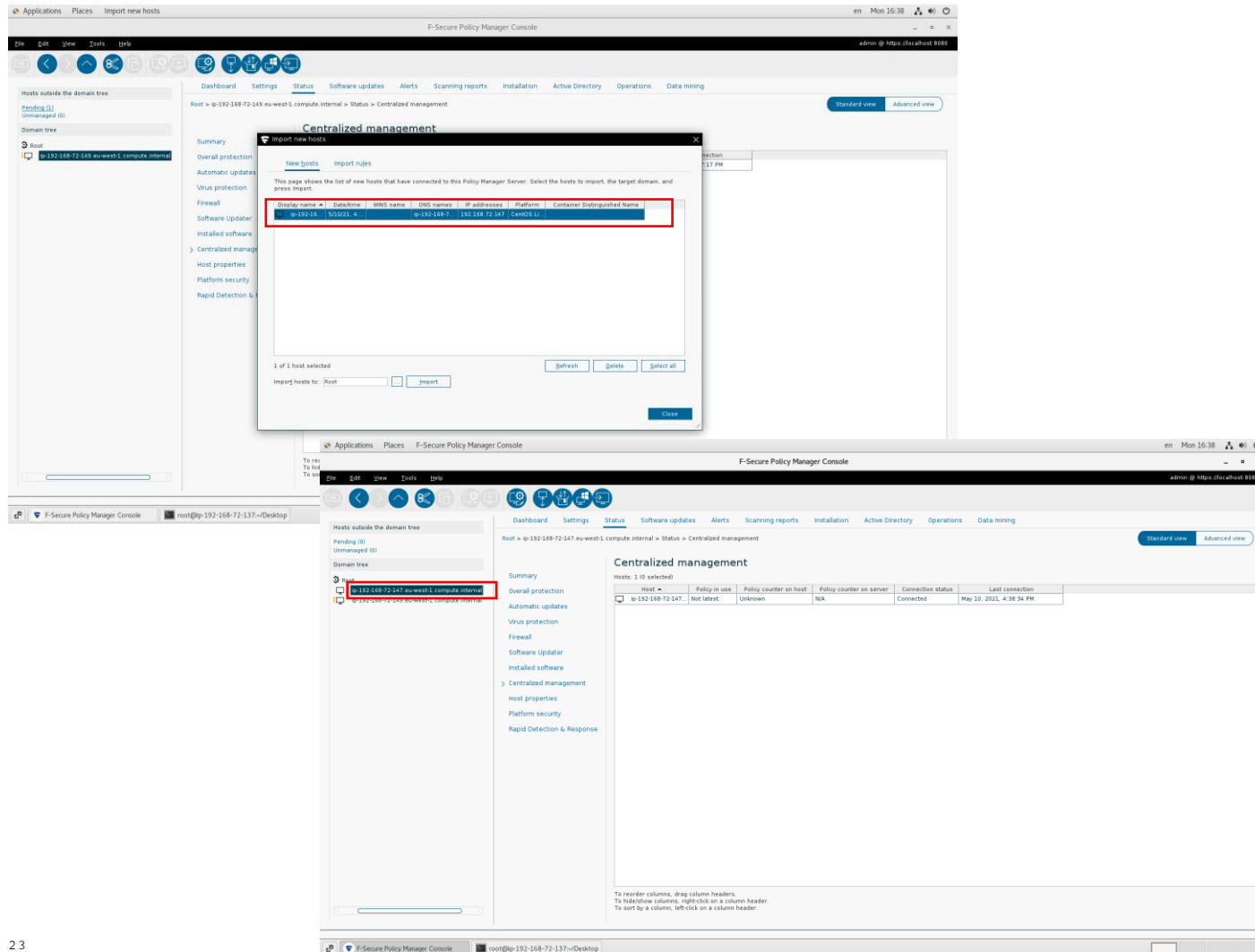
Weekly OS update check with possible reboot scheduled for Sunday at 04:06.

Installation completed!
Press enter to finish the installation..._
```

11. インストーラーのコピー完了後、Atlant VEの画面にて「Enter」を押下するとインストールが行われます。

12. 再度「Enter」を押下すると、インストールが完了します。

POLICYMANAGERへ端末のインポート



13. PolicyManager Consoleの「New hosts」に先ほどインストールしたAtlant VAの端末が表示されるので、選択してインポートします。