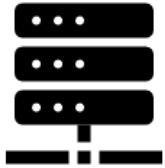


Linux Security 64(LS64)のオフライン環境へのインストール

Linux Security 64(LS64)はスタンドアロンインストールパッケージ、アップデートアーカイブを利用し、完全オフライン環境で運用する事が可能です。LS64 インストーラ/アーカイブ準備作業には Policy Manager が必要ですが、アップデートアーカイブ更新作業はオンラインクライアントで実施可能です。この例ではすべて Linux 端末での作業を実施しています。

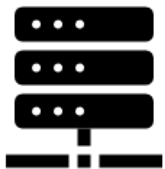
[運用イメージ]



Online PM

[パターンファイルアーカイブ準備作業]

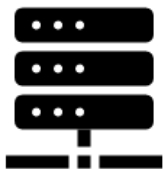
1. prepare-fspm-definitions-update-tool を実行 (初回のみ)
2. channels.json を編集 (初回のみ)



Any online machine

[パターンファイルアーカイブ更新作業]

3. fspm-definitions-update-tool を実行
※f-secure-updates.zip が作成される



Offline LS64

[パターンファイルアーカイブインポート作業]

4. f-secure-updates.zip をコピーして配置
5. fspm-definitions-update-tool でインポート

[Linux Security 64(LS64)のオフライン環境へのインストール手順]

1. スタンドアロンインストーラの作成

https://www.withsecure.com/userguides/product.html#business/linux-security-64/latest/ja/task_5C570986E91C4FDEAE621040DF5080B3-latest-ja

※0.0.0.0 を Policy Manager として指定し、インストールパッケージを作成。

※最新のインストーラファイル(jar)をダウンロードして作成(2020年11月2日時点 /fsls64-2.0.15.jar が最新)

2. コンテンツパッケージ(パターンファイルアーカイブ)の作成
https://www.withsecure.com/userguides/product.html#business/linux-security-64/latest/ja/task_DB7A3BA35BE747168B9F05499160F552-latest-ja
※f-secure-updates.zip がコンテンツパッケージとなります。
3. 「コンテンツパッケージ(パターンファイルアーカイブ)」を指定してインストール。
https://www.withsecure.com/userguides/product.html#business/linux-security-64/latest/ja/task_4F943A13730B43AE90CE85B32019825B-latest-ja
※通常版のインストールコマンドとは異なり、下記のコマンドでオプション指定が必要。

```
bash f-secure-linuxsecurity/f-secure-linuxsecurity-installer --package=/tmp/f-secure-updates.zip --automatic-updates=none
```

※この例では、f-secure-updates.zip を/tmp に配置しています。

[パターンファイルアーカイブ準備作業]

1. PolicyManager(PM)サーバがインストールされているコンピュータでコマンドラインを開きます。このコンピュータは、F-Secure サーバに接続できるようにネットワークに接続している必要があります。
2. ポリシーマネージャ定義更新ツール(fspm-definitions-update-tool)を展開するディレクトリを作成し、カレントディレクトリとして移動します。
3. 次のコマンドを実行して、パターンファイルアーカイブ更新ツールを抽出します。
/opt/f-secure/fspm/bin/prepare-fspm-definitions-update-tool
4. 以下のファイルをテキストエディタで開きます。
/fspm-definitions-update-tool/conf/channels.json.
5. 次の内容が含まれるようにファイルを編集します。
["fsbspamd-100-linux-x86_64", "aqualnx64", "fmlibunix64", "hydra-linux64",
"baseguard-100-linux-x86_64", "fsbg-100-linux-x86_64", "linuxsecurity-1200-linux-x86_64"]

[パターンファイルアーカイブ更新作業]

1. オンライン状態の端末(PM/Win/Linux)に"/fspm-definitions-update-tool/"フォルダをコピーします。
2. /fspm-definitions-update-tool/data/ ディレクトリが存在しないか、空である事(なにかある場合は削除)を確認し、以下のコマンドを実行してパターンファイルアーカイブ(f-secure-updates.zip)を作成します。

```
/fspm-definitions-update-tool/fspm-definitions-update-tool
```

コマンドの実行が終了すると、パターンファイルアーカイブ"f-secure-updates.zip" が作成されます。

[パターンファイルアーカイブインポート作業]

1. f-secure-updates.zip ファイルを LS64 の任意の場所にコピーし、root ユーザとして次のコマンドを実行し、製品のパターンファイルを適用(※)します。
/opt/f-secure/fsbg/bin/offline-update <任意>/f-secure-updates.zip

※正確には、f-secure-updates.zip からアップデートを抽出してインストール予定リストに登録を行います。登録されたチャンネル名が表示され、下記がこのコマンドの出力例です。

```
Preparing channel updates...
baseguard-100-linux-x86_64.1585583363
fsbg-100-linux-x86_64.1585581843
linuxsecurity-1200-linux-x86_64.1585581846
aqualnx64.1585581033
fsbspamd-100-linux-x86_64.1582614359
fmlibunix64.1580813614
hydra-linux64.1585289384
Registering updates...
```

※登録されたアップデートは、製品構成 (lsctl で変更可能) で定義された更新スケジュールを無視して即座にインストールされます。

2. 次回以降は [パターンファイルアーカイブ更新作業] から同じ作業を繰り返してください。

[補足事項]

・ [パターンファイルアーカイブ更新作業] を Windows 端末で実施する場合、[パターンファイルアーカイブ準備作業] を Windows 端末で実施する必要があります。もし Windows 端末を用意できない場合、下記手順で java 実行環境を入れ替える事で Window 用ツールへの切り替えが可能です。(Window32bit 版の動作は確認されていません。)

<https://community.withsecure.com/ja/kb/articles/29496-how-to-switch-fspm-definitions-update-tools-platform-from-linux-to-windows-vice-versa-in-policy-manager>

・ LS64 はローカル GUI を持ちません。PM との常時接続が無いスタンドアロンインストール LS64 の設定は lsctl ユーティリティを使用して行います。

#lsctl ユーティリティを使用して設定を構成する

https://www.withsecure.com/userguides/product.html#business/linux-security-64/latest/ja/task_57B4371465924825B36469EA081CD0A5-latest-ja

・ この作業に Policy Manger の「隔離モード(isolate)への切り替え」は不要です。隔離モードへの切り替えは、PM 自体がオフライン環境に存在している際に利用します。

※LS64 で直接アップデートアーカイブをインポートできる機能が追加された為、PM と LS64 との直接アクセス(http_proxy 不可)は不要となりました。(2020 年 9 月 23 日更新)