

オンプレミス製品からElements製品への移行について

2025年8月4日

WithSecure Elements全体イメージ

専用管理サーバー導入不要



管理者

どこからでも
アクセス



WithSecure Elements Security Center
(ブラウザベース)



自動適応(OSによって、機能が異なります)
パターンファイル、プロファイル、EPPソフトウェアバージョンアップ、セキュリティパッチ



社内LAN

マルチプラットフォーム対応



支社/海外

多拠点も一元管理

Elementsの利点

- ◆Elements Security Centerで管理を行うため、ローカルネットワークに管理サーバが不要になります。
- ◆EPPのインストーラはElements Security Centerからダウンロードできます。
 - ※BusinessSuite製品についてはWithSecureウェブサイトからjarファイルをダウンロード後PolicyManagerでインストーラを作成する必要がありました。
- ◆Elements Security Centerでライセンスの有効期限や使用状況を確認することができます。
- ◆EDR機能を追加利用したい場合、ライセンス購入後、自動的にEDR機能が追加されます。
 - ※クライアントの再インストールは不要です。

移行前の動作要件/環境の確認について

移行前に動作要件を満たしているか確認をお願いします。

1. 各Agentの動作要件

[WithSecure Elements Endpoint Protection for Computers]

<https://www.withsecure.com/userguides/product.html#business/computer-protection-windows/latest/ja>

[WithSecure Elements Endpoint Protection for Servers]

<https://www.withsecure.com/userguides/product.html#business/server-protection/latest/ja>

[WithSecure Elements Linux Protection]

<https://www.withsecure.com/userguides/product.html#business/linux-protection/latest/ja>

[WithSecure Elements Endpoint Protection for Computers (Mac)]

<https://www.withsecure.com/userguides/product.html#business/psb-cp-mac/latest/ja>

[Elements Connector]

<https://www.withsecure.com/userguides/product.html#business/connector/latest/ja>

[Elements Endpoint Protection]

<https://www.withsecure.com/userguides/product.html#business/psb-portal/latest/ja>

2. 通信環境

[Community: Network addresses for WithSecure Elements (cloud-managed products)]

<https://community.withsecure.com/en/kb/articles/31217-network-addresses-for-withsecure-elements-cloud-managed-products>

※これまでのPolicy ManagerまたはAgentが通信を行っていたOutbound通信先とは異なります為、制限なく通信が可能か確認ください。

※Policy Managerのバージョンが、16.03 またはそれ以降のバージョンとなっている事を確認ください。

以前のバージョンの場合には、前もってバージョンアップをお願いします。

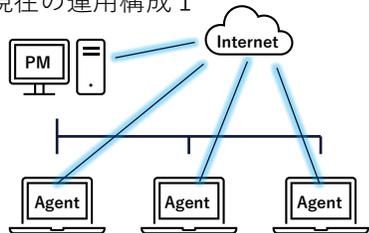
ダウンロード：<https://www.withsecure.com/jp-ja/support/product-support/business-suite/policy-manager#download>

これは、移行時にPolicy Managerを一時的にProxyとして動作させる為で、Policy Managerが稼働しているサーバ機にConnectorを導入する場合に限りです。

Policy Managerが稼働するサーバ機とは異なるサーバ機にConnectorを導入する場合にはこの限りではありません。

現在の運用構成から移行後の運用構成について

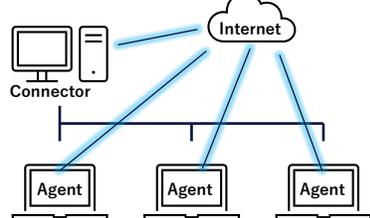
現在の運用構成 1



PM/AgentがInternetへ通信できる環境



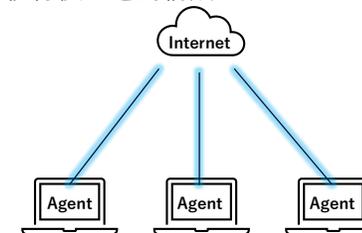
移行後の運用構成 1 - 1



PMの代わりにConnectorを設置

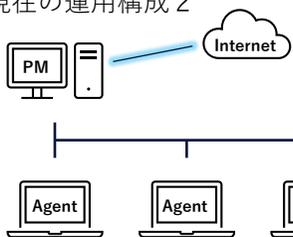
OR

移行後の運用構成 1 - 2



Clientの台数が少ない場合には上記構成が標準構成となります

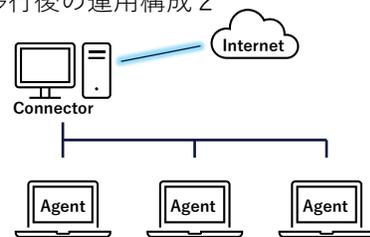
現在の運用構成 2



PMのみがInternetへ通信できる環境

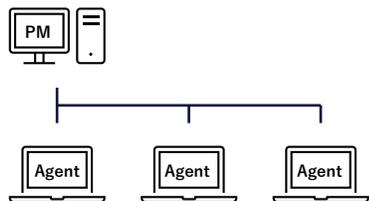


移行後の運用構成 2



PMの代わりにConnectorを設置

現在の運用構成 3



閉域網環境

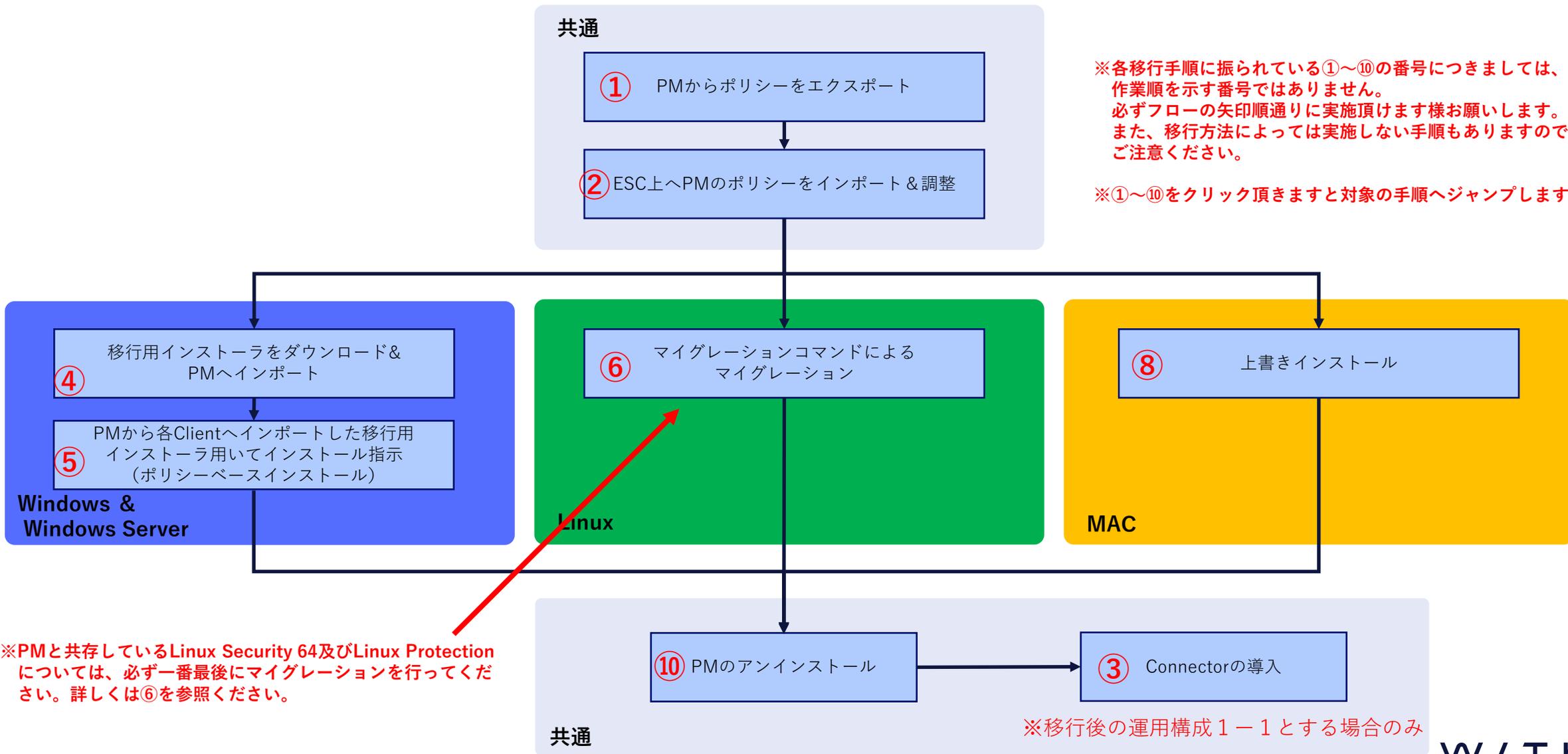


閉域網環境ではご利用いただけません
移行後の運用構成②をご検討ください

移行フロー概要

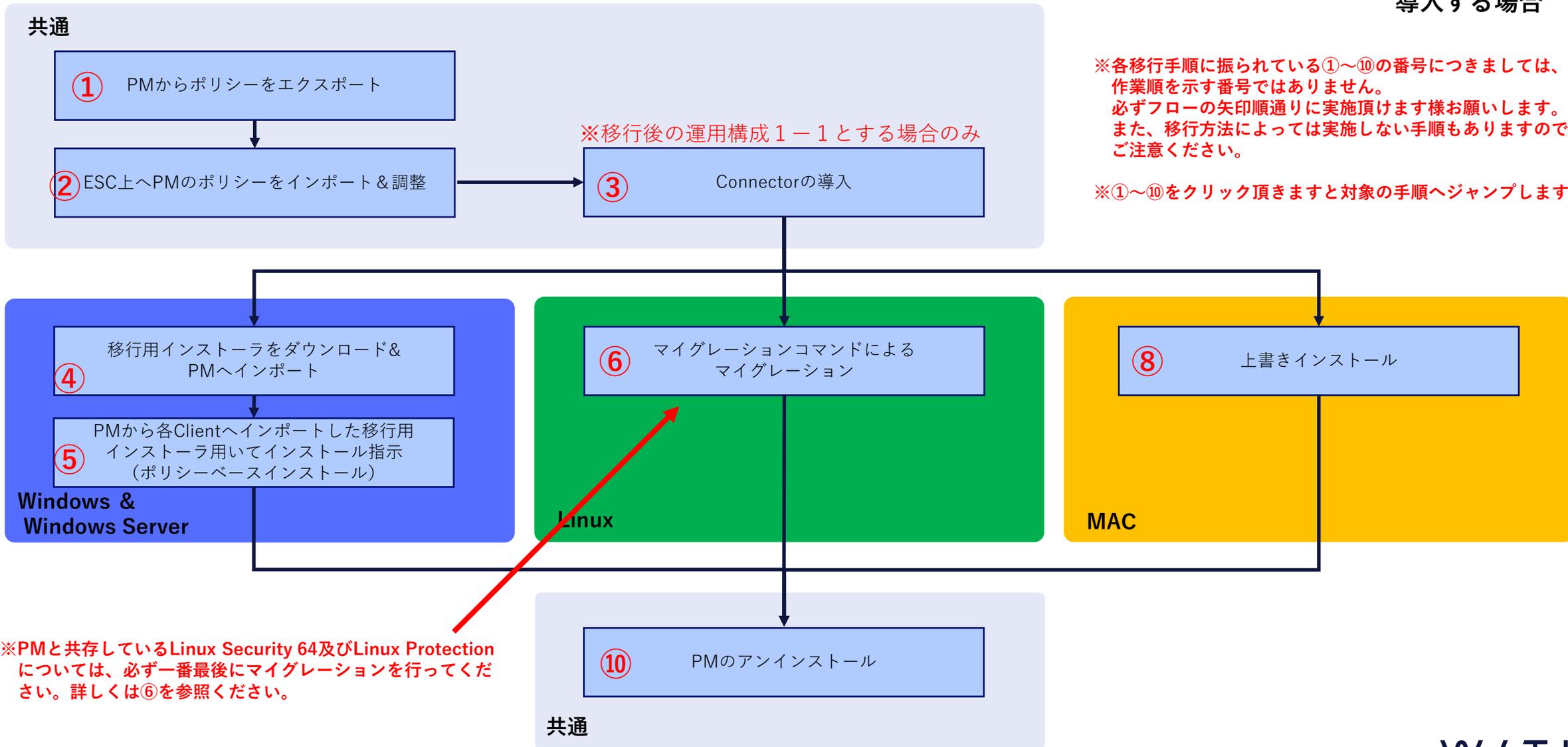
・現在の運用構成 1 ⇒ 移行後の運用構成 1 - 1 / 移行後の運用構成 1 - 2

※PMが稼働するサーバ機にConnectorを導入する場合



移行フロー概要

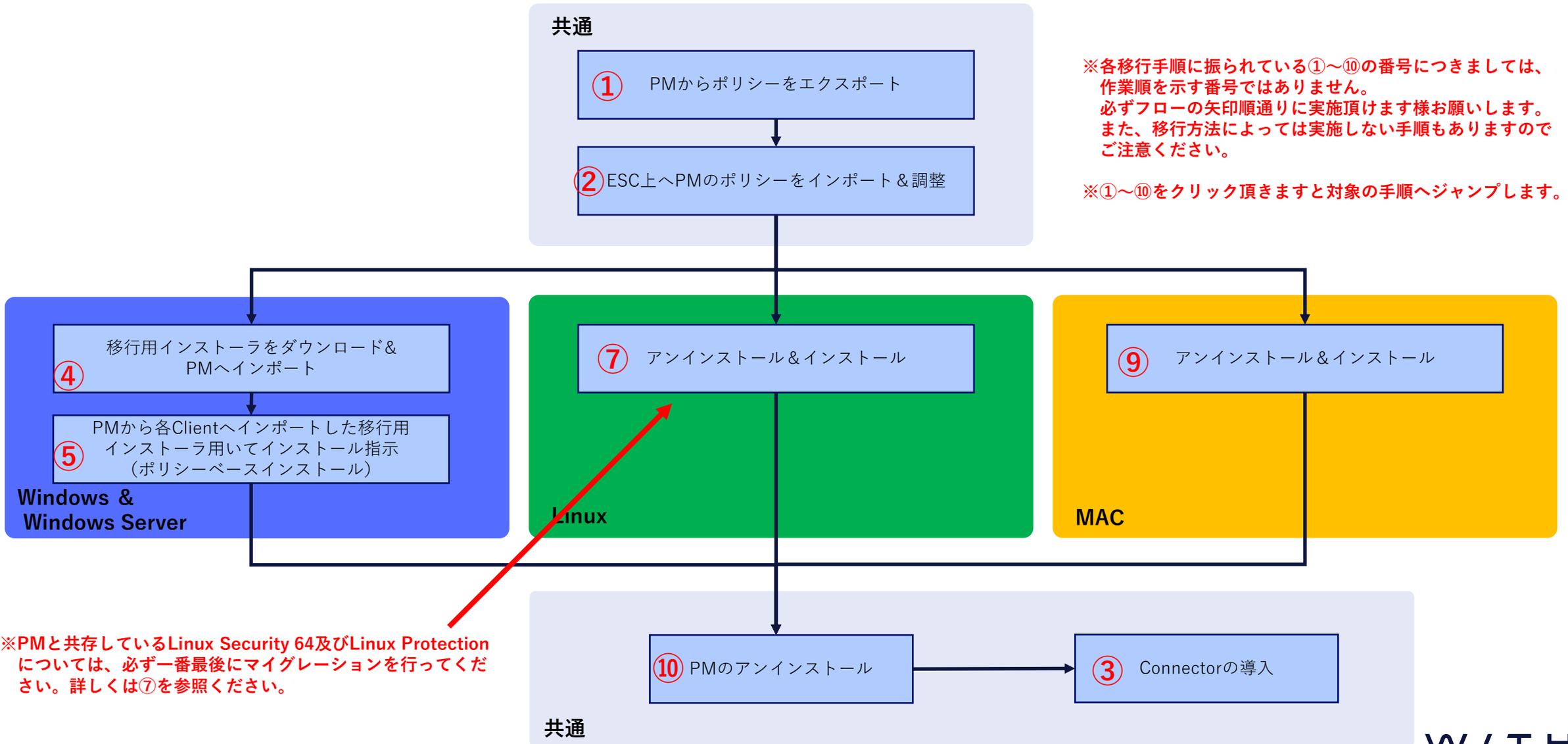
・現在の運用構成 1 ⇒ 移行後の運用構成 1 - 1 / 移行後の運用構成 1 - 2 ※PMが稼働するサーバ機とは別のサーバ機にConnectorを導入する場合



移行フロー概要

・現在の運用構成 2 ⇒ 移行後の運用構成 2

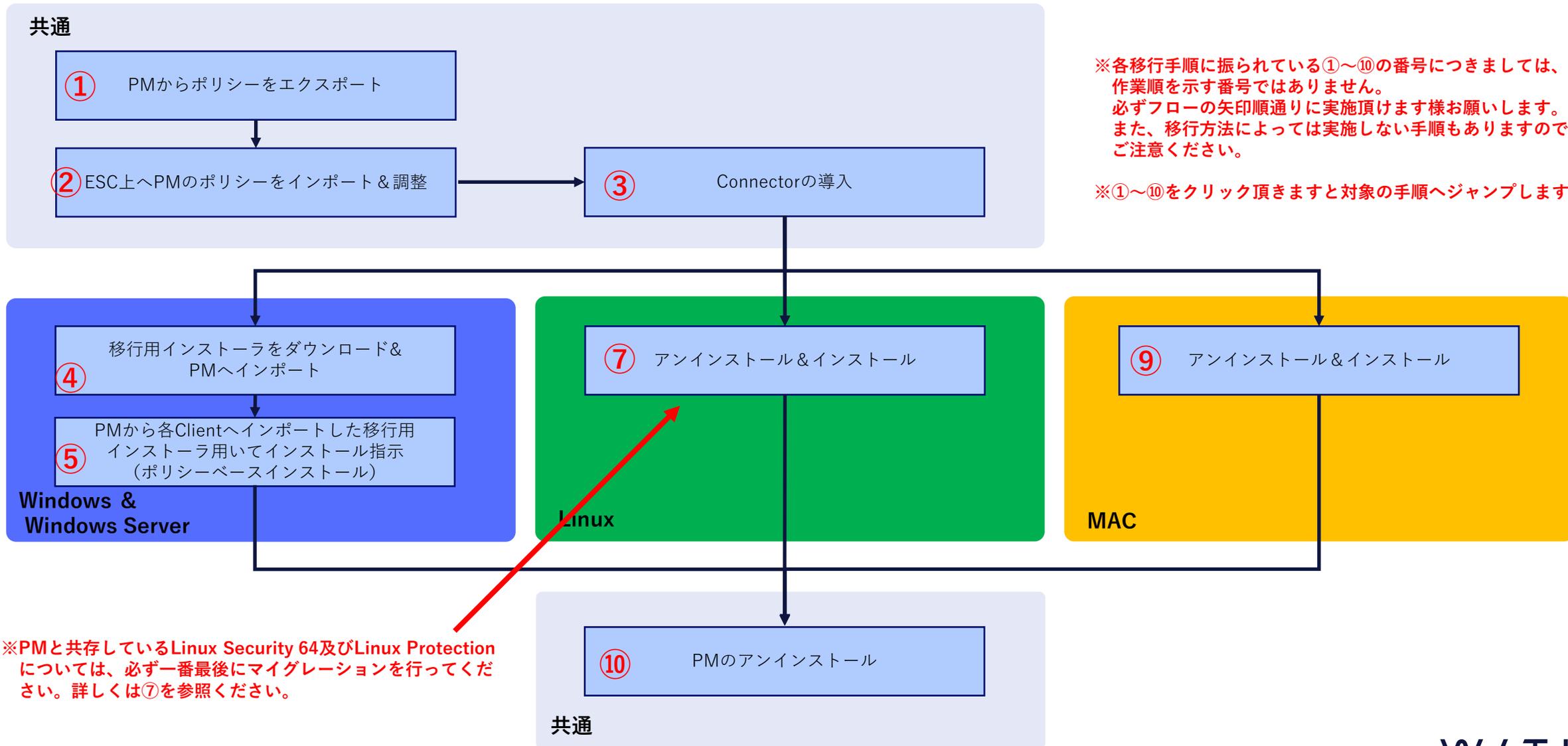
※PMが稼働するサーバ機にConnectorを導入する場合



移行フロー概要

・現在の運用構成 2 ⇒ 移行後の運用構成 2

※PMが稼働するサーバ機とは別のサーバ機にConnectorを導入する場合



①PMからポリシーをエクスポート

ポリシーとプロファイルについて

ポリシーは、PM上でのAgentの設定であり、ルート・ポリシードメイングループ・ホスト単位での設定が可能です。



プロファイルは、ESC上でのAgentの設定であり、ポリシー＝プロファイルとなります。ただし、プロファイルがポリシーと異なる部分としては、プロファイルはルート・ポリシードメイングループでの設定として作成するもので、Agent単位に作成する場合、Agent数分のプロファイルが必要となります。

セキュリティ構成 / プロファイル

プロファイル [プロファイルを作成する](#)

Windows Windows Server : Mac Linux モバイルデバイス Connector : プロファイルの指定ルール Policy Managerから移行 (PILOT)

プロファイル名	タイプ	説明	所有者	指定されているコンピュータ	アクション
20250327			Konary_L3	1	...
202505013			Konary_L3	2	...
test		111	Konary_L3	4	...
test20210112			Konary_L3	2	...
WithSecure™ Laptop (locked) (読み取り専用)		A laptop profile that is locked to prevent users from changing any settings.	システム	5	...
WithSecure™ Laptop (open) (読み取り専用)		A laptop profile that is open for users to change any settings.	システム	1	...
WithSecure™ Office (locked) (読み取り専用)		Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	システム	0	...
WithSecure™ Office (open) (読み取り専用)		Office open for accessing the Internet from a fixed location such as office premises. End users are allowed to change security settings.	システム	1	...

①PMからポリシーをエクスポート

移行前にPMからポリシーをエクスポートします。※ESC側でプロファイル(ポリシー)を手動で設定する場合には必要ありません。

ポリシーのエクスポートは2種類の方法があります。

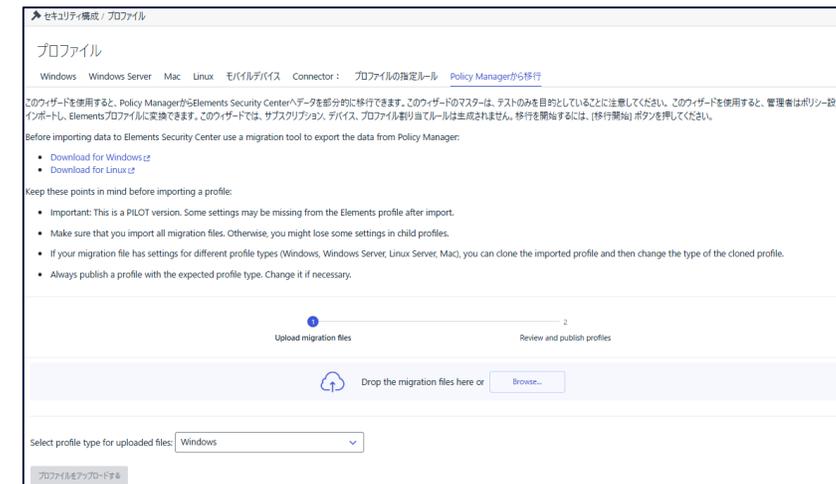
①-1：PMのポリシードメインのホスト毎にポリシーをエクスポート

- ・メリット：ホスト毎に異なる設定をされている場合に個別にエクスポートできます。
- ・デメリット：多数のポリシーをエクスポートしなければならない場合があります。



①-2：ポリシーエクスポートツールを用いたエクスポート

- ・メリット：ポリシードメイン単位での設定をエクスポートできる為作業時間が比較的短時間で完了します。
- ・デメリット：ホスト毎に個別設定がある場合には利用できません。



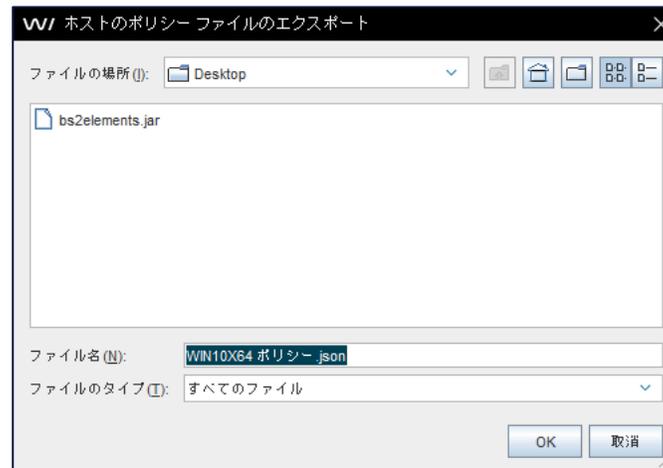
①PMからポリシーをエクスポート

[①-1 : PMのポリシードメインのホスト毎にポリシーをエクスポート]

必要分のホスト毎のポリシーを以下の手順でエクスポートしてください。

Step1 : 対象ホストを右クリックし「ポリシーファイルをエクスポートする」をクリックします。

Step2 : 任意の場所へエクスポートしてください。



※このホスト毎にエクスポートしたポリシーを移行できるプラットフォームは、Windows/Windows Server のみとなります。

MAC/Linuxについては、ポリシーエクスポートツールを用いたエクスポートしたポリシーを利用するかESC側で新規に手動で作成が必要になります。

①PMからポリシーをエクスポート

[①-2：ポリシーエクスポートツールを用いたエクスポート]

ポリシーを以下の手順でエクスポートしてください。

[Windows PMの場合]

Step1：ポリシーエクスポートツールをダウンロードし、PMS稼働するサーバ機上のデスクトップ等に配置します。

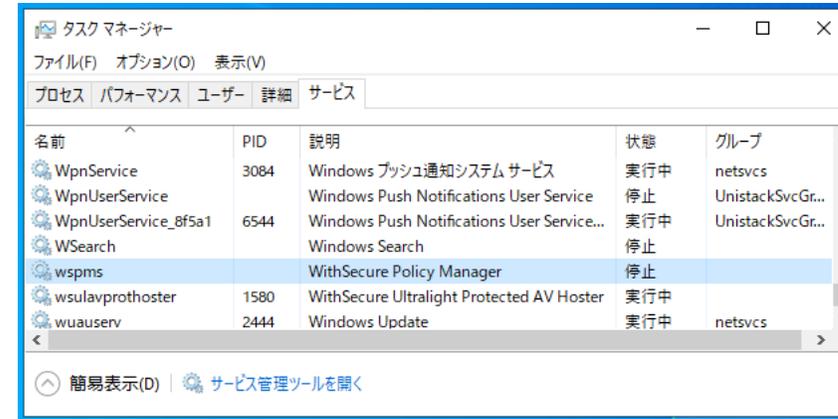
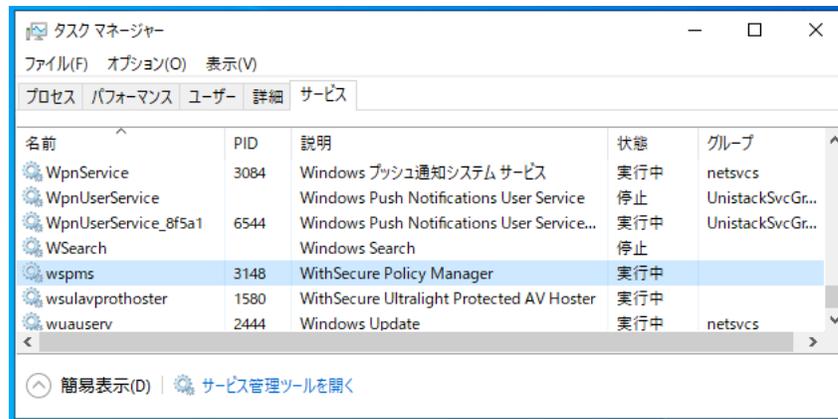
<https://download.withsecure.com/PSB/bs2cp/migration-tool.zip>



Step2：ダウンロードしたポリシーエクスポートツールを解凍します。



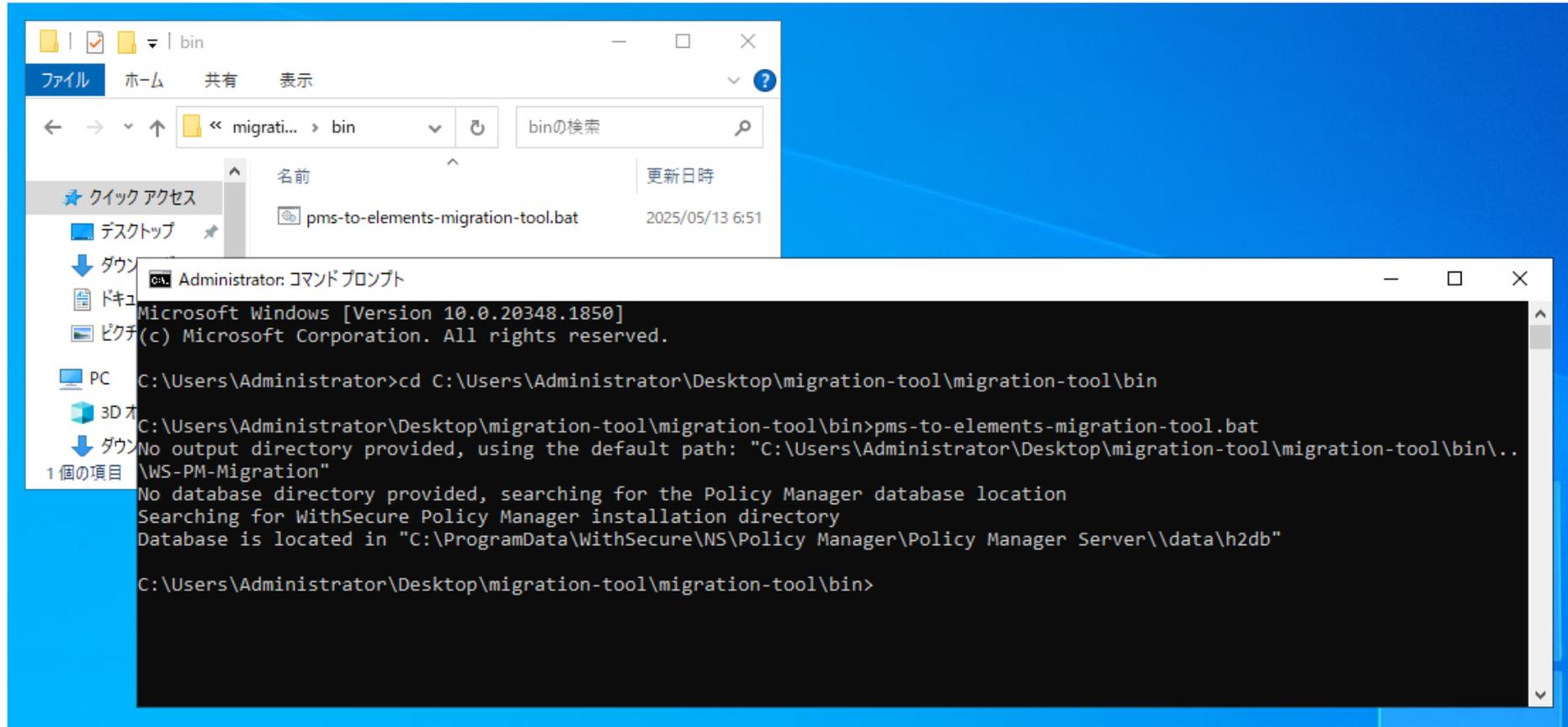
Step3：PMのサービス“wspms”を停止します。



①PMからポリシーをエクスポート

[①-2 : ポリシーエクスポートツールを用いたエクスポート]

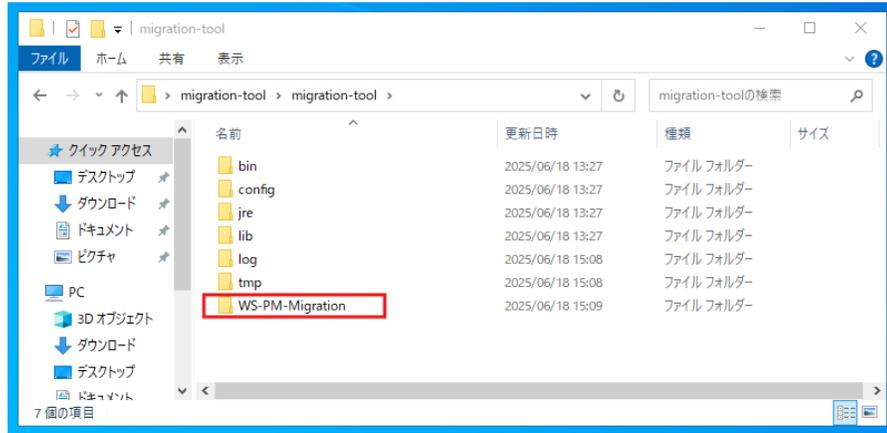
Step4 : 管理者権限でコマンドプロンプトを開き、Step2で解凍したフォルダ>binフォルダ内の pms-to-elements-migration-tool.bat を実行します。



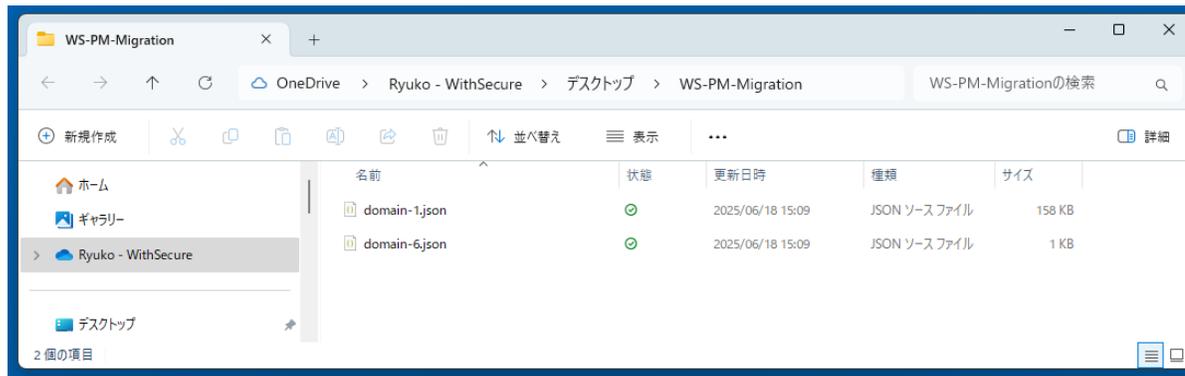
①PMからポリシーをエクスポート

[①-2：ポリシーエクスポートツールを用いたエクスポート]

Step5： Step2で解凍したフォルダ内に WS-PM-Migration フォルダが作成されていますのでこのフォルダごと採取してください。



採取頂いたWS-PM-Migration フォルダを開くとルートやポリシードメイングループ単位のポリシーファイル(JSON)が格納されています。



※ルートやポリシードメイングループに対して設定変更されていないものについてはエクスポートされません。

①PMからポリシーをエクスポート

[①ー2：ポリシーエクスポートツールを用いたエクスポート]

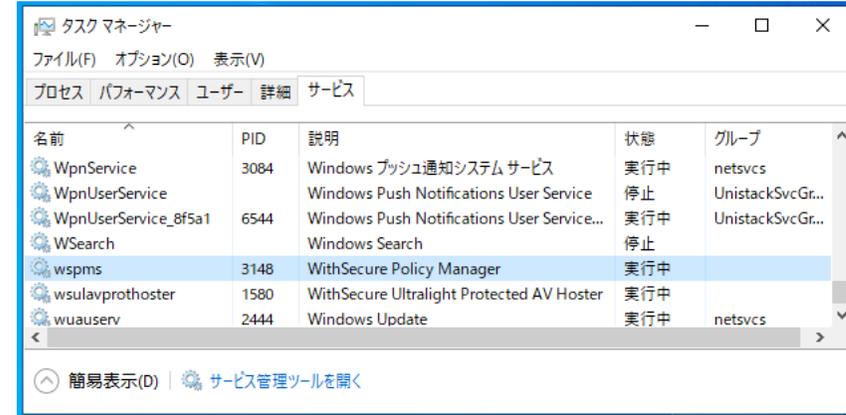
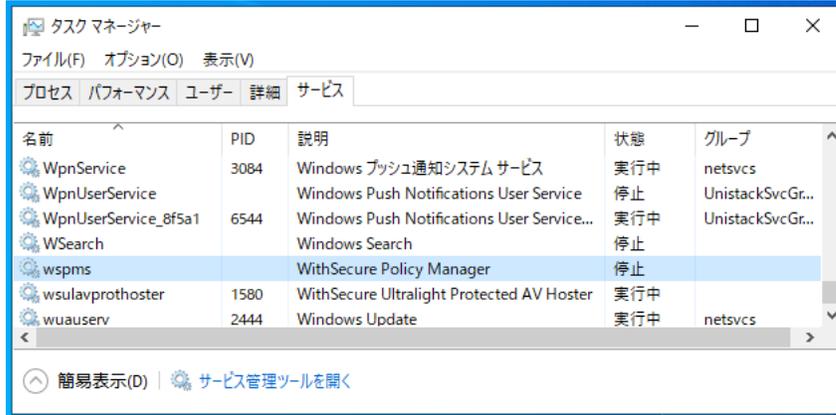
ファイル名からはどのポリシードメイングループか確認できませんが、メモ帳等で開いて頂くと、“domain_id”から内部IDを、“name”の値からポリシードメイングループ名称を確認いただけます。

```
1  {
2    "data": {
3      "domain_id": 6,
4      "name": "linux",
5      "node_path": "1/6/",
6      "settings": {
7        "windows.policy_manager.override_address.host": {
8          "value": "192.168.213.190",
9          "type": "string"
10       },
11       "windows.policy_manager.override_address.http_port": {
12         "value": 80,
13         "type": "integer"
14       }
15     }
16   }
17 }
```

①PMからポリシーをエクスポート

[①-2 : ポリシーエクスポートツールを用いたエクスポート]

Step6 : PMのサービス“wspms”を開始し、実行中に戻しておきます。



②ESC上へPMのポリシーをインポート & 調整

[PMからエクスポートしたポリシーをESC上でインポート]

ポリシーのインポートにつきましては、

“①-1：PMのポリシードメインのホスト毎にポリシーをエクスポート”した場合と“①-2：ポリシーエクスポートツールを用いたエクスポート”した場合によりインポート方法が異なります。

“①-1：PMのポリシードメインのホスト毎にポリシーをエクスポート”した場合

通常のインポート機能を用いてポリシーをインポートします。

セキュリティ構成 / プロファイル

プロファイル [プロファイルを作成する](#)

Windows Windows Server Mac Linux モバイルデバイス Connector: プロファイルの指定ルール Policy Managerから移行 (PILOT)

プロファイル名	タイプ	説明	所有者	指定されているコンピュータ	アクション
20250327			Konary_L3	1	...
202505013			Konary_L3	3	...
test		111	Konary_L3	3	...
test20210112			Konary_L3	2	...
WithSecure™ Laptop (locked) (読み取り専用)		A laptop profile that is locked to prevent users from changing any settings.	システム	5	...
WithSecure™ Laptop (open) (読み取り専用)		A laptop profile that is open for users to change any settings.	システム	1	...
WithSecure™ Office (locked) (読み取り専用)		Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	システム	0	...
WithSecure™ Office (open) (読み取り専用)		Office open for accessing the Internet from a fixed location such as office premises. End users are allowed to change security settings.	システム	1	...

“①-2：ポリシーエクスポートツールを用いたエクスポート”した場合

Policy Manager からの移行ウィザードを用いてポリシーをインポートします。

セキュリティ構成 / プロファイル

プロファイル

Windows Windows Server Mac Linux モバイルデバイス Connector: プロファイルの指定ルール [Policy Managerから移行](#)

このウィザードを使用すると、Policy ManagerからElements Security Centerへデータを部分的に移行できます。このウィザードのマスターは、テストのみを目的としていることに注意してください。このウィザードを使用すると、管理者はポリシー設定をインポートし、Elementsプロファイルに変換できます。このウィザードでは、サブスクリプション、デバイス、プロファイル割り当てルールは生成されません。移行を開始するには、[移行開始] ボタンを押してください。

Before importing data to Elements Security Center use a migration tool to export the data from Policy Manager:

- [Download for Windows](#)
- [Download for Linux](#)

Keep these points in mind before importing a profile:

- Important: This is a PILOT version. Some settings may be missing from the Elements profile after import.
- Make sure that you import all migration files. Otherwise, you might lose some settings in child profiles.
- If your migration file has settings for different profile types (Windows, Windows Server, Linux Server, Mac), you can clone the imported profile and then change the type of the cloned profile.
- Always publish a profile with the expected profile type. Change it if necessary.

1 Upload migration files 2 Review and publish profiles

Drop the migration files here or [Browse...](#)

Select profile type for uploaded files:

[プロファイルモックアップロードする](#)

② ESC上へPMのポリシーをインポート & 調整

[②-1 : PMからエクスポートしたポリシーをESC上でインポート]

“①-1 : PMのポリシードメインのホスト毎にポリシーをエクスポート”したポリシーのインポート

Step1 : ESCにログイン頂き、セキュリティ構成 > プロファイルを開きます。

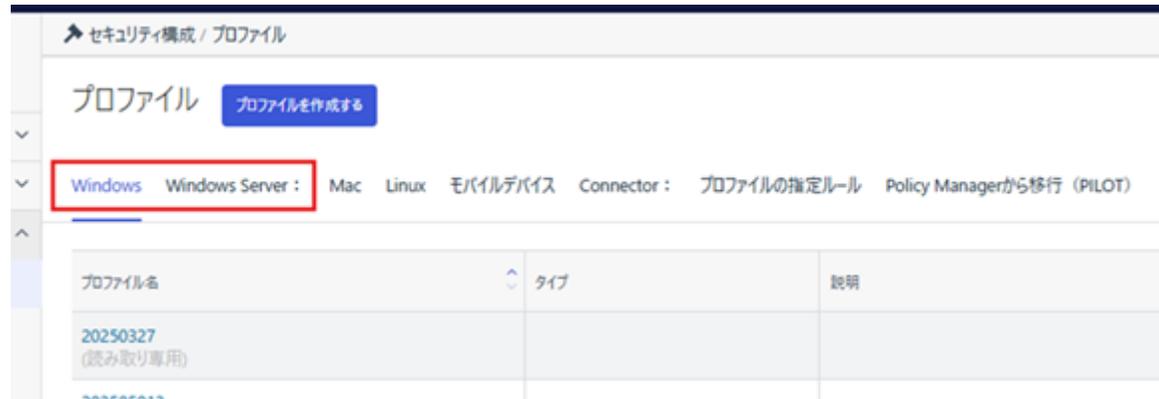
プロファイル名	タイプ	説明
20250327 (読み取り専用)		
202505013 (読み取り専用)		
test (読み取り専用)		111
test20210112 (読み取り専用)		
ToL2 (読み取り専用)		
WithSecure™ Laptop (locked) (読み取り専用)		A laptop profile that is locked to prevent users from
WithSecure™ Laptop (open) (読み取り専用)		A laptop profile that is open for users to change ar
WithSecure™ Office (locked) (読み取り専用)		Office locked for accessing the Internet from a fixe settings.
WithSecure™ Office (open) (読み取り専用)		Office open for accessing the Internet from a fixed settings.

② ESC上へPMのポリシーをインポート & 調整

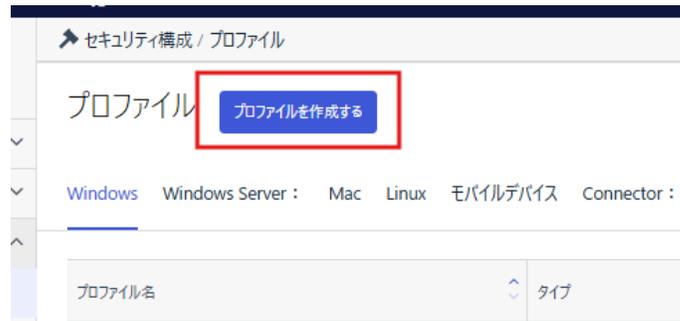
[②-1 : PMからエクスポートしたポリシーをESC上でインポート]

“①-1 : PMのポリシードメインのホスト毎にポリシーをエクスポート”したポリシーのインポート

Step2 : インポート先のプラットフォームをクリックして選択します。(以下の例の場合、Windowsが選択されています)



Step3 : [プロファイルを作成する]をクリックします。



②ESC上へPMのポリシーをインポート & 調整

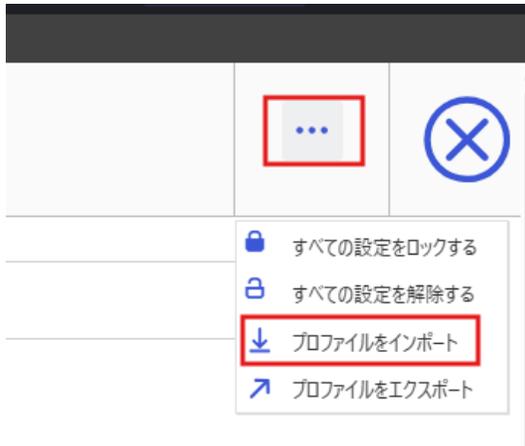
[②-1 : PMからエクスポートしたポリシーをESC上でインポート]

“①-1 : PMのポリシードメインのホスト毎にポリシーをエクスポート”したポリシーのインポート

Step4 : プロファイル名に任意の名称をお決め頂き入力します。



Step5 : ”...”をクリックし、アクションメニューから”プロファイルをインポート”をクリックします。

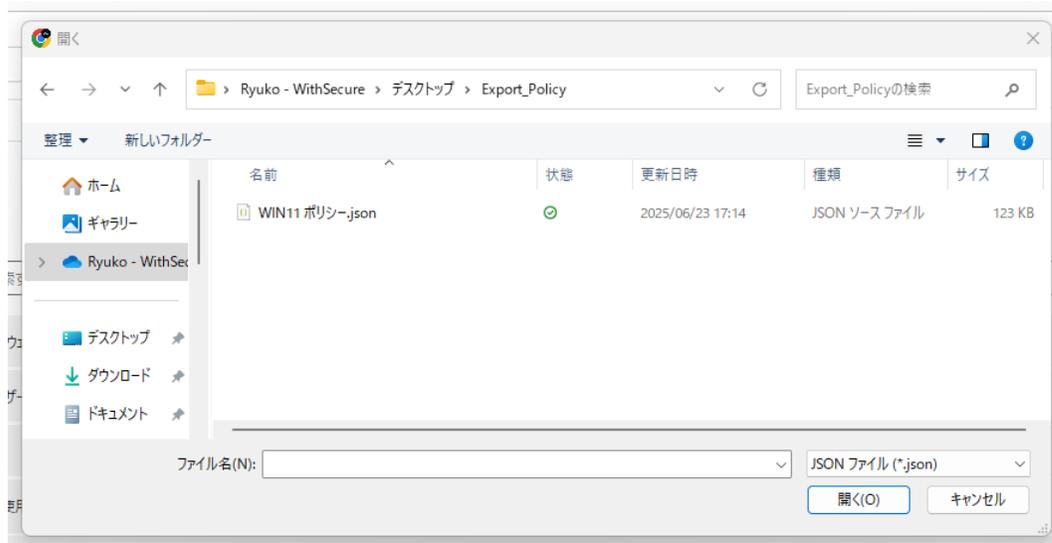


② ESC上へPMのポリシーをインポート & 調整

[②-1 : PMからエクスポートしたポリシーをESC上でインポート]

“①-1 : PMのポリシードメインのホスト毎にポリシーをエクスポート”したポリシーのインポート

Step6 : インポートしたいポリシーファイルを選択し[開く]ボタンを押します。



②ESC上へPMのポリシーをインポート & 調整

[②-1 : PMからエクスポートしたポリシーをESC上でインポート]

“①-1 : PMのポリシードメインのホスト毎にポリシーをエクスポート”したポリシーのインポート

Step7 : ポリシーが反映した箇所が黄色で表示されます。必要に応じて設定を更に変更頂き設定が間違い無い事を確認頂いてから[保存して発行]を押します。保存後は引き続き[OK]を押して頂くとインポートされたプロファイル(ポリシー)を一覧で確認できます。

Windowsのプロファイル
Konary_L18

プロファイル名 Profile1_forWindows 説明

タイプ

一般設定
このタブには、WithSecure™ Elements Agentのセキュリティ機能で共有される設定が含まれています。

すべてのプロファイル設定
特定の設定を検索するには、ここに入力してください...

設定項目	状態	ロック
クライアントソフトウェアを速くも早く利用する	オフ	無
クライアントにユーザーインターフェースを表示する	オン	無
自動更新	オン	無
HTTP プロキシを使用	ユーザーブラウザの設定を検出	無
手動で定義されたプロキシアドレス		有
プロキシ経由の接続を優先	オフ	有
プロキシの設定を隠す	オフ	有

保存して発行

プロファイル [プロファイルを作成する](#)

Windows Windows Server : Mac Linux モバイルデバイス Connector : プロ

プロファイル名	タイプ	説明
20250327 (読み取り専用)		
202505013 (読み取り専用)		
Profile1_forWindows		
test (読み取り専用)		111
test20210112 (読み取り専用)		

② ESC上へPMのポリシーをインポート & 調整

[②-2 : PMからエクスポートしたポリシーをESC上でインポート]

“①-2 : ポリシーエクスポートツールを用いたエクスポート”したポリシーのインポート

Step1 : ESCにログイン頂き、セキュリティ構成 > プロファイルを開きます。

The screenshot shows the 'Profiles' page in the Elements Security Center. The page title is 'プロファイル' (Profiles) and there is a button 'プロファイルを作成する' (Create Profile). Below the title, there are tabs for 'Windows', 'Windows Server', 'Mac', 'Linux', 'モバイルデバイス', and 'Connector'. The 'Windows' tab is selected. The main content area shows a table of profiles:

プロファイル名	タイプ	説明
20250327 (読み取り専用)		
202505013 (読み取り専用)		
test (読み取り専用)		111
test20210112 (読み取り専用)		
ToL2 (読み取り専用)		
WithSecure™ Laptop (locked) (読み取り専用)		A laptop profile that is locked to prevent users from
WithSecure™ Laptop (open) (読み取り専用)		A laptop profile that is open for users to change a
WithSecure™ Office (locked) (読み取り専用)		Office locked for accessing the Internet from a fixed settings.
WithSecure™ Office (open) (読み取り専用)		Office open for accessing the Internet from a fixed settings.

② ESC上へPMのポリシーをインポート & 調整

[②-2 : PMからエクスポートしたポリシーをESC上でインポート]

“①-2 : ポリシーエクスポートツールを用いたエクスポート” したポリシーのインポート

Step2 : 上部タブ > Policy Managerから移行をクリックします。

The screenshot shows the 'Profile' page in the Elements Security Center. The breadcrumb trail is 'セキュリティ構成 / プロファイル'. The main heading is 'プロファイル'. Below it, there are tabs for 'Windows', 'Windows Server', 'Mac', 'Linux', 'モバイルデバイス', and 'Connector'. The 'Connector' tab is active, and the sub-tab is 'プロファイルの指定ルール'. A link 'Policy Managerから移行' is visible. The page contains the following text and elements:

このウィザードを使用すると、Policy ManagerからElements Security Centerへデータを部分的に移行できます。このウィザードのマスターは、テストのみを目的としていることに注意してください。このウィザードを使用すると、管理者はポリシー設定をインポートし、Elementsプロファイルに変換できます。このウィザードでは、サブスクリプション、デバイス、プロファイル割り当てルールは生成されません。移行を開始するには、[移行開始] ボタンを押してください。

Before importing data to Elements Security Center use a migration tool to export the data from Policy Manager:

- [Download for Windows](#)
- [Download for Linux](#)

Keep these points in mind before importing a profile:

- Important: This is a PILOT version. Some settings may be missing from the Elements profile after import.
- Make sure that you import all migration files. Otherwise, you might lose some settings in child profiles.
- If your migration file has settings for different profile types (Windows, Windows Server, Linux Server, Mac), you can clone the imported profile and then change the type of the cloned profile.
- Always publish a profile with the expected profile type. Change it if necessary.

A progress bar shows two steps: 1. Upload migration files (active) and 2. Review and publish profiles.

Drop the migration files here or [Browse...](#)

Select profile type for uploaded files:

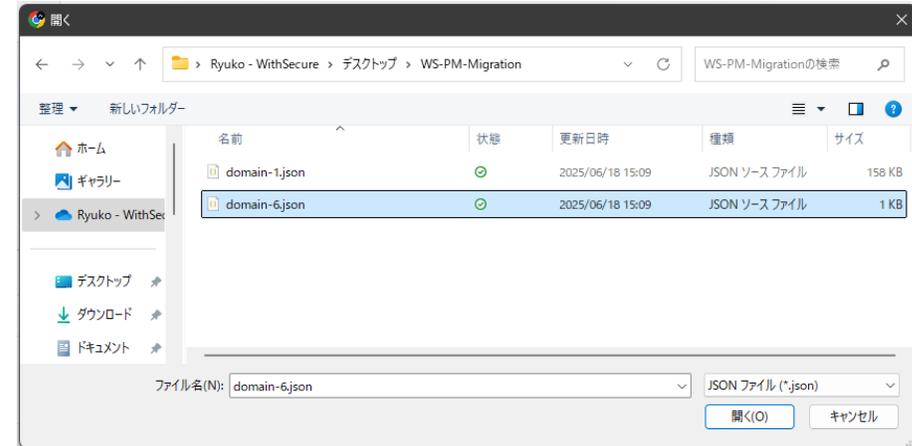
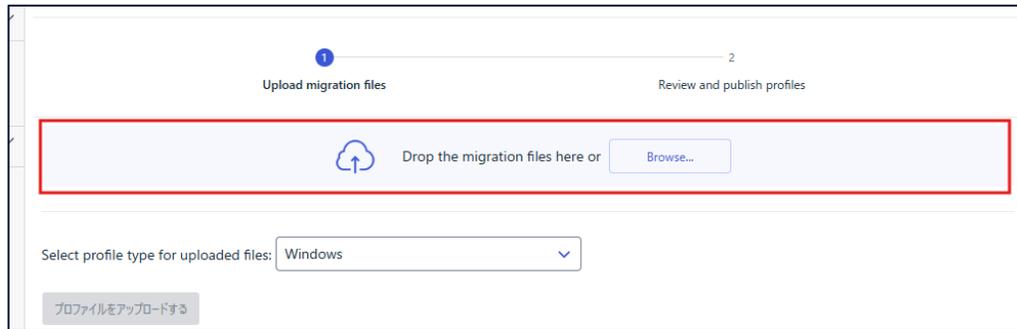
[プロファイルをアップロードする](#)

② ESC上へPMのポリシーをインポート & 調整

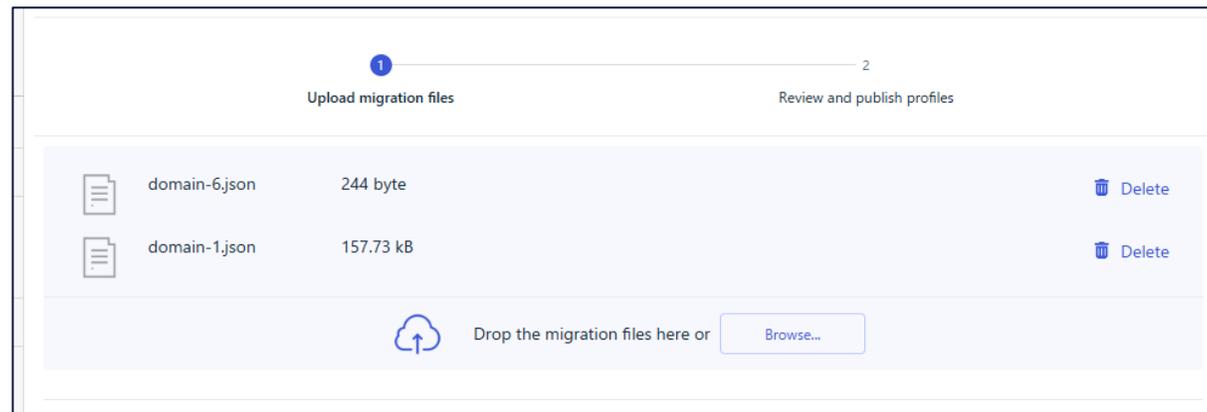
[②-2 : PMからエクスポートしたポリシーをESC上でインポート]

“①-2 : ポリシーエクスポートツールを用いたエクスポート” したポリシーのインポート

Step3 : 以下の部分へインポートしたいポリシーファイルをドロップ頂くか[Browse...]から選択し[開く]を押してください。



※複数のポリシーを指定できます。



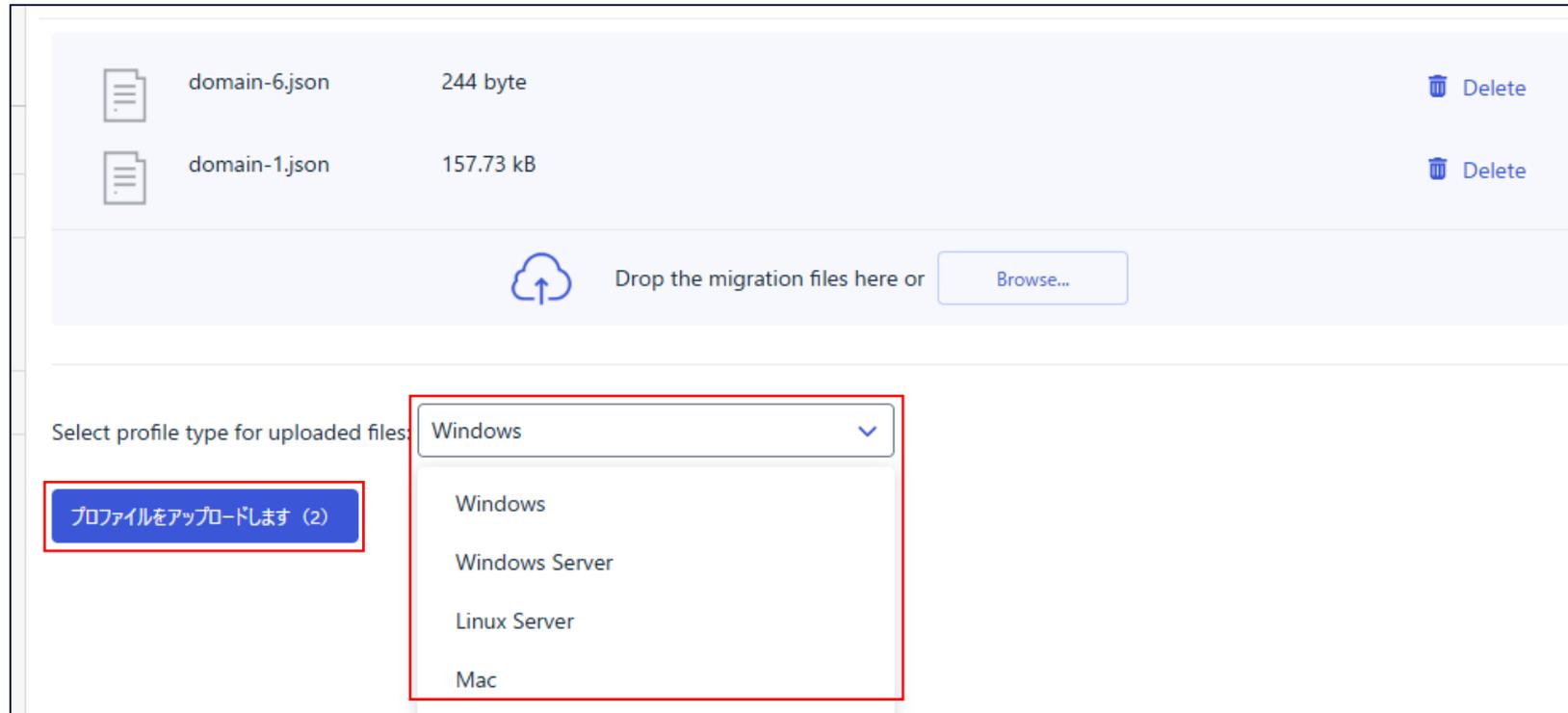
②ESC上へPMのポリシーをインポート & 調整

Top ^

[②ー2 : PMからエクスポートしたポリシーをESC上でインポート]

“①ー2 : ポリシーエクスポートツールを用いたエクスポート”したポリシーのインポート

Step4 : アップロード先プロファイルタイプ(プラットフォーム)を選択し[プロフィールをアップロードします]を押します。。



② ESC上へPMのポリシーをインポート & 調整

[②-2 : PMからエクスポートしたポリシーをESC上でインポート]

“①-2 : ポリシーエクスポートツールを用いたエクスポート” したポリシーのインポート

Step5 : アップロードが完了しますと以下の表示となります。プロファイル名等の変更をされる場合には右端の“...”から変更ください。
アップロードしたプロファイルを利用可能な状態にするには[プロファイルを公開する]を押します。

Upload migration files 2 Review and publish profiles

1 - 2 of 2 < > 1 of 1 < >

<input type="checkbox"/>	Id	タ...	名前	説明		
<input type="checkbox"/>	1	Windows	root		−	...
<input type="checkbox"/>	6	Windows	Windows Client 用プロファイル		−	...

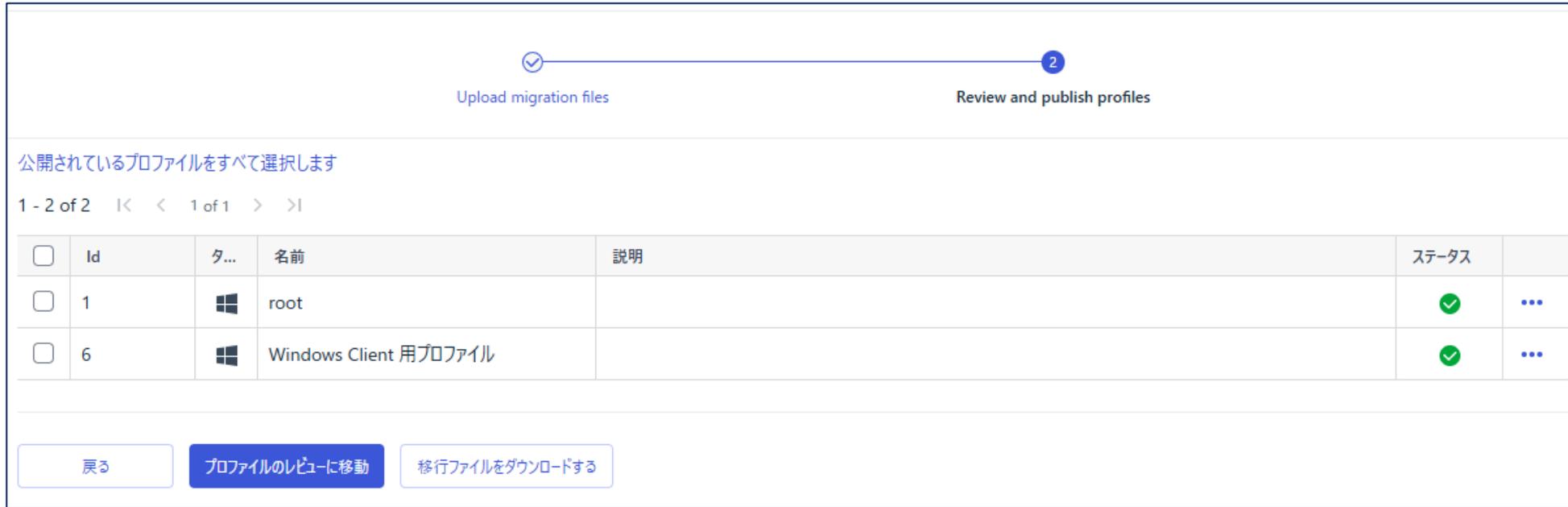
戻る **プロフィールを公開する** 移行ファイルをダウンロードする

②ESC上へPMのポリシーをインポート & 調整

[②-2 : PMからエクスポートしたポリシーをESC上でインポート]

“①-2 : ポリシーエクスポートツールを用いたエクスポート”したポリシーのインポート

Step6 : プロファイルの公開が完了しますと以下の表示となります。
ステータスが  となっていれば正常に公開完了しています。



公開されているプロファイルをすべて選択します

1 - 2 of 2 |< < 1 of 1 > >|

<input type="checkbox"/>	Id	タ...	名前	説明	ステータス	
<input type="checkbox"/>	1		root			...
<input type="checkbox"/>	6		Windows Client 用プロファイル			...

[戻る](#) [プロフィールのレビューに移動](#) [移行ファイルをダウンロードする](#)

② ESC上へPMのポリシーをインポート & 調整

[②-2 : PMからエクスポートしたポリシーをESC上でインポート]

“①-2 : ポリシーエクスポートツールを用いたエクスポート” したポリシーのインポート

Step7 : プロファイル > 対象のプロファイルタイプ(プラットフォーム)を開きアップロードしたプロファイルが登録され利用可能になっている事を確認します。

以下の例では2つのプロファイルが公開され利用可能となっています。

プロファイル [プロファイルを作成する](#)

Windows Windows Server : Mac Linux モバイルデバイス Connector : プロファイルの指定ルール Policy Managerから移行 (PILOT)

プロファイル名	タイプ	説明	所有者	指定されているコンピュータ	アクション
20250327			Konary_L3	1	...
202505013			Konary_L3	3	...
root			Konary_L3	0	...
test		111	Konary_L3	3	...
test20210112			Konary_L3	2	...
Windows Client 用プロファイル			Konary_L3	0	...
WithSecure™ Laptop (locked) (読み取り専用)		A laptop profile that is locked to prevent users from changing any settings.	システム	5	...
WithSecure™ Laptop (open) (読み取り専用)		A laptop profile that is open for users to change any settings.	システム	1	...
WithSecure™ Office (locked) (読み取り専用)		Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	システム	0	...
WithSecure™ Office (open) (読み取り専用)		Office open for accessing the Internet from a fixed location such as office premises. End users are allowed to change security settings.	システム	1	...

②ESC上へPMのポリシーをインポート & 調整

[②- 1 / 2 : Connectorを利用する場合のプロファイル設定について]

Connectorを利用するには、作成したプロファイル内に以下の通りProxy設定 & Connector指定を必ず行ってください。

[Windows & Windows Server の場合の設定例] ※プロキシアドレスとConnectorアドレスの双方にConnectorのIPアドレスを指定してください。

Windowsのプロファイル
Konary_L3

指定されているコンピュータ: 1
更新日: 2025/03/28 1:00
プロファイルID: 51610093

すべてのプロファイル設定

一般設定
このタブには、WithSecure™ Elements Agentのセキュリティ機能で共有される設定が含まれています。

特定の設定を検索するには、ここに入力してください...

クライアント ソフトウェアを誰よりも早く利用する	<input type="checkbox"/>	
クライアントにユーザー インターフェースを表示する	<input checked="" type="checkbox"/>	
自動更新	<input checked="" type="checkbox"/>	
HTTP プロキシを使用	リモート管理	🔒
手動で定義されたプロキシアドレス	192.168.213.200	🔒
プロキシ経由の接続を優先	<input type="checkbox"/>	🔒
プロキシの設定を隠す	<input type="checkbox"/>	🔒
HTTPSを使用してアップデートをダウンロードする	<input type="checkbox"/>	🔒
WithSecure™ Elements Connector	192.168.213.200	🔒

② ESC上へPMのポリシーをインポート & 調整

[②- 1 / 2 : Connectorを利用する場合のプロファイル設定について]

Connectorを利用する場合には、作成したプロファイル内に以下の通りProxy設定 & Connector指定を必ず行ってください。

[MAC の場合の設定例] ※プロキシアドレスとConnectorアドレスの双方にConnectorのIPアドレスを指定してください。

プロファイル所有者: Konary_L3 | プロファイルタイプ: mac | 指定したデバイス: 0 | プロファイルID: 24701952 | 更新日: Jun 8, 2020, 5:34:58 PM

一般

WithSecure Elements AgentをMac OSユーザーに表示する

自動更新 ⓘ

プロキシオプション リモート管理のHTTPプロキシを使用する ▼

リモート管理されているプロキシアドレス 192.168.213.200

WithSecure Elements Connector 192.168.213.200

グローバルWithSecureアップデートサーバーへのフォールバック

HTTPSを使用してアップデートをダウンロードする

連携 ⓘ

② ESC上へPMのポリシーをインポート & 調整

[②- 1 / 2 : Connectorを利用する場合のプロファイル設定について]

Connectorを利用する場合には、作成したプロファイル内に以下の通りProxy設定 & Connector指定を必ず行ってください。

[Linux の場合の設定例] ※プロキシアドレスにConnectorのIPアドレスを指定してください。(ポートは80を指定してください)

プロファイル所有者: Konary_L3 | プロファイルタイプ: linux | 指定したデバイス: 0 | プロファイルID: 51684155 | 更新日: Apr 24, 2025, 4:39:11 PM

🔍 プロファイルを検索

一般

このタブには、WithSecure Elements Agentのセキュリティ機能で共有される設定が含まれています。

インターネット接続 ⓘ

HTTP プロキシを使用	<input checked="" type="checkbox"/>
HTTPプロキシホスト	<input type="text" value="http://192.168.213.200"/>
HTTPプロキシポート	<input type="text" value="80"/>
HTTPプロキシユーザー名	<input type="text"/>

②ESC上へPMのポリシーをインポート & 調整

Top へ

[②- 1 / 2 : Connectorを利用する場合のプロファイル設定について]

Connectorを利用するには、必要に応じてConnector用カスタムプロファイルを作成してください。
(通常はデフォルトプロファイルで問題ありませんが、環境や利用機能に応じて設定変更が必要な場合があります)

[Connectorの設定例]

プロファイル所有者: Konary_L3 | プロファイルタイプ: connector | 指定したデバイス: 0 | プロファイルID: 48031646 | 更新日: Apr 18, 2023, 1:59:52 PM

🔍 プロファイルを検索

一般

このタブには、WithSecure Elements Connectorのセキュリティ機能で共有される設定が含まれています。

通信設定 ⓘ

ポーリング間隔

ソフトウェアアップdaterの設定 ⓘ

最大ディスク容量 (MB)

一般 ⓘ

データベースが古くなっている日数

インターネット接続 ⓘ

HTTP プロキシ

🔍 プロキシアドレスによる手動管理HTTP

② ESC上へPMのポリシーをインポート & 調整

[②- 1 / 2 : プロファイルIDについて]

複数のプロファイルを作成されておりClientへのインストール時にプロファイルを指定される場合には、以下の通りプロファイルにて対象プロファイルをクリックして開いて頂き“プロファイルID”をメモしてください。(必要分のすべてのプロファイルIDの値をメモください)

※用意したプロファイルがプロファイルタイプ(プラットフォーム)毎に1つでデフォルトプロファイルに指定されている場合はこの手順は不要です。

Security Structure / Profiles

Profiles [Create Profile]

Windows Windows Server : Mac Linux Mobile Device Connector :

Profile Name
11111
20250327
202505013
root
test
test20210112
Windows Client 用プロファイル
WithSecure™ Laptop (locked) 読み取り専用
WithSecure™ Laptop (open) 読み取り専用
WithSecure™ Office (locked)



Windows Client 用プロファイル [More]

Profile Owner: Konary_L3 | Profile Type: windows | Designated Device: 0 | Profile ID: 51830354 | Last Updated: Jun 24, 2025, 10:35:49 AM

Search Profiles

General

説明

説明 ①

説明	プロファイル名
エンドユーザーの権利	
タイプ	
説明	

Basic

- 一般
- スキャンの設定
- ウイルスのリアルタイムスキャン
- マニュアル スキャン
- ブラウザ保護
- ファイアウォール
- ソフトウェア アップデータ

②ESC上へPMのポリシーをインポート & 調整

[②-1/2 : プロファイルの指定ルールについて]

各プロファイルタイプ(プラットフォーム)毎に利用するプロファイルが一つの場合、プロファイル>対象のプロファイル指定ルールにてデフォルトルールにインポートしたプロファイルを指定しておく事によりインストール時のプロファイル指定を省略できます。

Connectorをご利用の場合には、必要に応じてカスタマイズされたプロファイルを指定してください。

プロファイル

Windows Windows Server Mac Linux モバイルデバイス Connector : [プロファイルの指定ルール](#) Policy Managerから移行 (PILOT)

アウトブレイクルール ⓘ

順序	条件	クライアントタイプ	プロファイルを指定する	アセットグループを割り当てる ⓘ	ラベルを追加する	説明	アクション
↑	アウトブレイクルール ⓘ	ルールがありません					

プロファイルの指定ルール ⓘ

順序	条件	クライアントタイプ	プロファイルを指定する	アセットグループを割り当てる ⓘ	ラベルを追加する	説明	アクション
↑	カスタムルール ⓘ	ルールがありません					
↑	デフォルトルール ⓘ						
1	すべて デフォルト	Windowsワークステーション	Windows Client 用プロファイル				⋮
2	すべて デフォルト	Windowsサーバー	WithSecure™ Server				⋮
3	すべて デフォルト	Linux	WithSecure™ for Linux				⋮
4	すべて デフォルト	Mac	WithSecure™ Office for Mac (open)				⋮
5	すべて デフォルト	モバイル デバイス	WithSecure™ mobile (open)				⋮
6	すべて デフォルト	Connector	WithSecure™ Elements Connector				⋮

← “⋮”からプロファイル指定が行えます

Connectorについて

Connectorは、3つの目的を果たす製品です。

- Connectorは、ソフトウェアアップデーター、マルウェア定義のアップデート、プログラムのアップグレードをキャッシュすることで、環境内の管理対象エンドポイントとWithSecureサービスとの間のトラフィックを最適化します。これらのアップデートをすべてインターネットから直接ダウンロードした場合、デバイスは膨大な量の外部トラフィックを消費してしまいます。コストを削減するには、要求されたファイルを一度だけダウンロードし、ネットワーク内のデバイスに配布するWithSecureキャッシングエンドポイントを使用することができます。
- Connector Ultimateプロキシは、WithSecureエンドポイントとクラウドサービス間のすべてのトラフィックのプロキシとして機能し、ファイアウォール設定を簡素化してセミクローズド（半閉鎖）環境でのWithSecure製品の利用を可能にします。
- Splunkなどのセキュリティ監視サービスを利用している企業向けに、ConnectorはWithSecureクラウドサービスからセキュリティ情報およびイベント管理（SIEM）へのセキュリティイベント転送を提供します。

プロキシとしての役割を担うConnectorは、WithSecure Policy Manager Proxyを置き換えるものです。従来製品からの最も重要な改善点は、自動アップグレードとWithSecure Elements Security Centerからの集中管理性のサポートです。

※Connectorを正常に動作させるには、動作要件を満たしているネットワーク環境・サーバ機が必要となります。事前に必ずご確認ください。

Connector:

<https://www.withsecure.com/userguides/product.html#business/connector/latest/ja>

通信環境:

[Community: Network addresses for WithSecure Elements (cloud-managed products)]

<https://community.withsecure.com/en/kb/articles/31217-network-addresses-for-withsecure-elements-cloud-managed-products>

③Connectorの導入

[Windows版の導入]

Step1：ESCにログイン頂き、管理>ダウンロードを開きます。Connectorダウンロード部にて[サブスクリプションキーを作成する]が表示されている場合に押しingて頂きますとダウンロードボタンに変わりますので、[ダウンロード.msi]を押してインストーラをダウンロードします。



※Connectorインストーラはパブリックダウンロードページから入手できます。
<https://www.withsecure.com/en/support/download>



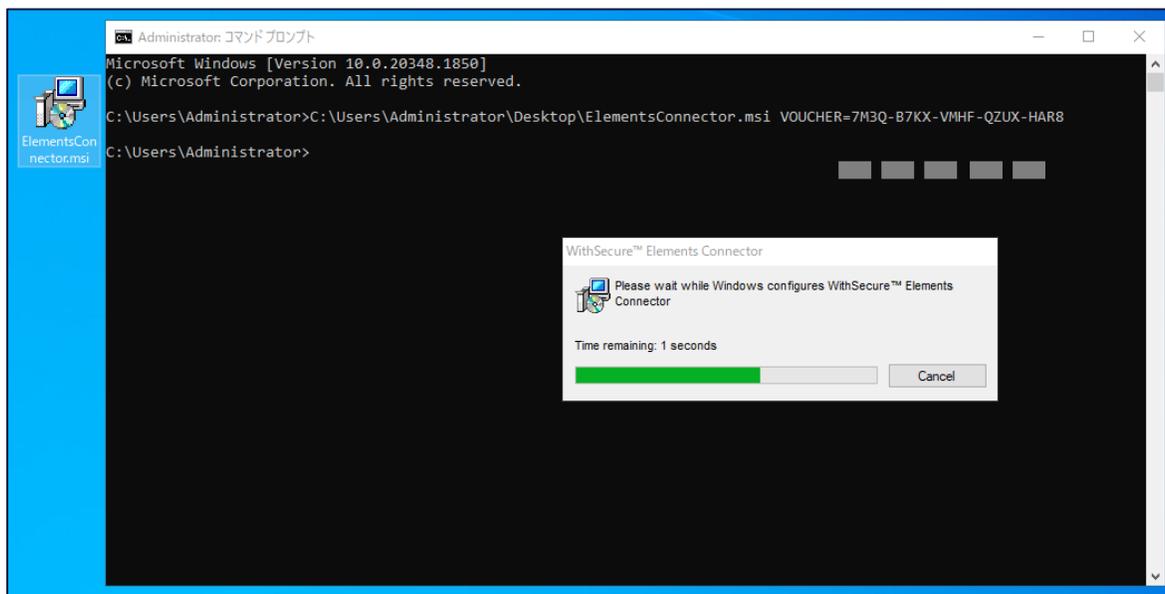
Step2：ダウンロード頂いたインストーラをConnectorを導入するサーバ機のデスクトップ等任意の場所へ配置します。

③Connectorの導入

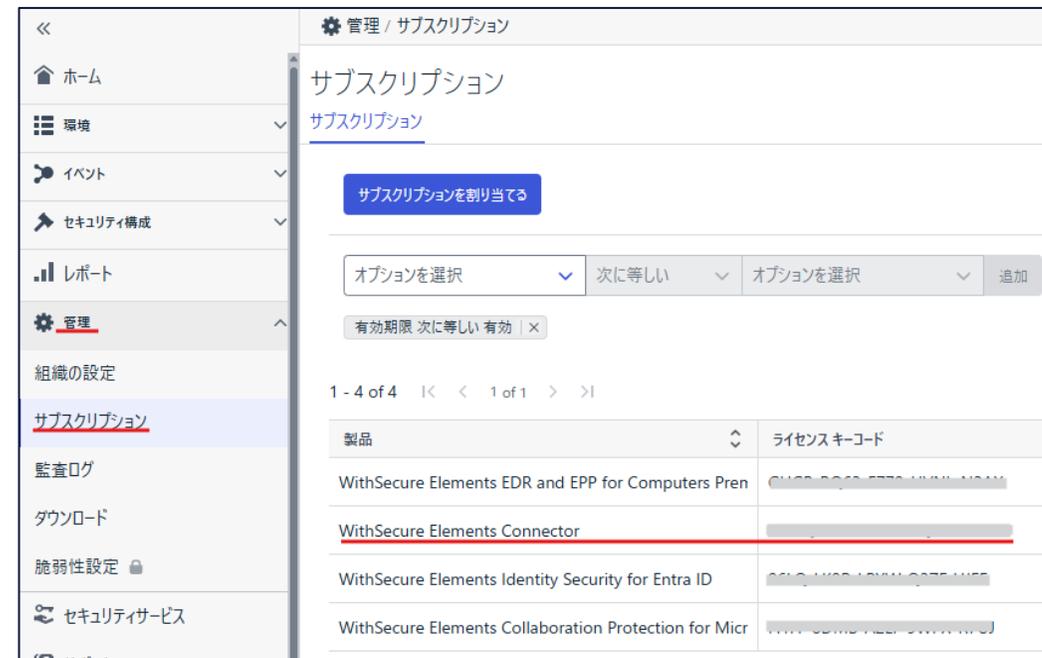
[Windows版の導入]

Step3： 管理者権限でコマンドプロンプトを起動し、配置されたインストーラを実行してインストールを行います。
インストールの際にConnectorのサブスクリプションキーの指定が必要で、必要に応じてProxy Serverの指定も行います。
Connectorのサブスクリプションキーは、管理>サブスクリプションをクリック頂けますとConnectorのサブスクリプションキーを確認できます。

インストールコマンドの実行：



Connector用サブスクリプションキー：



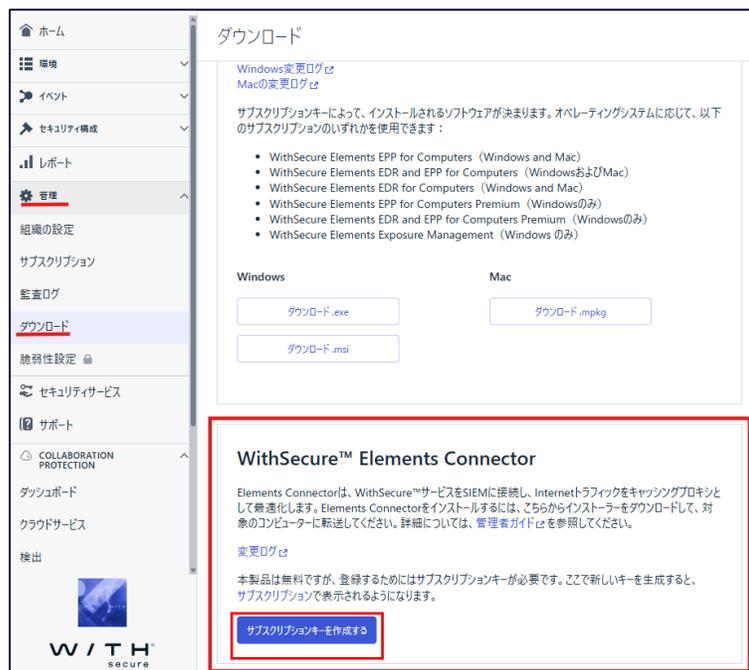
インストールの詳細につきましては、
以下のURLへアクセス頂き「12 Elements ConnectorをWindowsにインストールする」を参照ください。

https://www.withsecure.com/userguides/product.html#business/connector/latest/ja/task_0CC32864F2F54405AED18E54FD2BBDCC-latest-ja

③Connectorの導入

[Linux版の導入]

Step1: ESCにログイン頂き、管理>ダウンロードを開きます。Connectorダウンロード部にて[サブスクリプションキーを作成する]が表示されている場合に押しingて頂きますとダウンロードボタンに変わりますので、お使いのプラットフォームに応じて[ダウンロード.deb]または[ダウンロード.rpm]を押しingてインストーラをダウンロードします。



※Connectorインストーラはパブリックダウンロードページからも入手できます。

<https://www.withsecure.com/en/support/download>



Step2: ダウンロード頂いたインストーラをConnectorを導入するサーバ機のデスクトップ等任意の場所へ配置します。

③Connectorの導入

[Linux版の導入]

Step3： 配置されたインストーラをコマンドから実行してインストールを行います。

Connectorのサブスクリプションキーは、ESC>管理>サブスクリプションをクリック頂けますとConnectorのサブスクリプションキーを確認できます。

インストールコマンドの実行：

- Debian、Ubuntu：

```
# dpkg -i elements-connector.deb
```

- Red Hat、CentOS、SuSE、Oracle Linux：

```
# rpm -i elements-connector.rpm
```

Connector用サブスクリプションキー：

製品	ライセンスコード
WithSecure Elements EDR and EPP for Computers Pren	CWSD-0000-0770-111111-111111
WithSecure Elements Connector	CWSD-0000-0770-111111-111111
WithSecure Elements Identity Security for Entra ID	CWSD-0000-0770-111111-111111
WithSecure Elements Collaboration Protection for Micr	CWSD-0000-0770-111111-111111

③Connectorの導入

[Linux版の導入]

Step4： rootユーザとして以下のスクリプトを実行し、Connectorを設定、起動します。

```
# /opt/f-secure/fspms/bin/fspms-config
```

インストール・設定の詳細につきましては、
以下のURLへアクセス頂き「14 Installing Elements Connector on Linux」を参照ください。

https://www.withsecure.com/userguides/product.html#business/connector/latest/ja/task_2BD1FB5B0D364F39A14E52BBC56BEC74-latest-ja

③Connectorの導入

Top へ

[Windows版/Linux版]

Connectorのインストール完了後、ブラウザから <https://localhost> へアクセス頂き以下の画面が表示されましたら正常動作している事を確認頂けます。
ESC側では、環境>デバイス>コネクタにてインストールしたConnectorが存在しており、且つステータスの更新日時が直近の値となっていて、プロファイルの指定ステータスも最新となっていれば正常に動作しております。

The image shows two overlapping screenshots. The background screenshot is a web browser window displaying the 'Elements Connector' installation confirmation page. The page features the 'W / T H secure' logo and a green checkmark icon with a cloud and server symbol. The text on the page reads: 'Elements Connectorがインストールされ、正常に動作しています。バージョン: 25.17.99283'. The browser's address bar shows 'https://localhost'.

The foreground screenshot is a screenshot of the 'Konary_XDR' console interface. The left sidebar shows a navigation menu with 'デバイス' (Devices) selected. The main content area displays the 'デバイス' (Devices) page, which includes a table of installed connectors. The table has columns for 'タイプ' (Type), '名前' (Name), '企業名' (Company Name), '登録日' (Registration Date), 'ステータスの更新日時' (Status Update Date), 'ラベル' (Label), and 'コメン' (Comments). A single device is listed with the name 'WINSRV2022' and a status update time of 'Jun 30, 2025, 5:23:42 PM'.

※想定されているConnectorプロファイルが適用されている事を必ず確認
頂き、異なる場合には適用したいプロファイルへ変更してください。

W / T H
secure

④ 移行用インストーラをダウンロード&PMへインポート

[Windows/Windows Server 用インストーラのダウンロードからPMへのインポート]

Step1：以下のファイルをダウンロードします。

<https://download.withsecure.com/PSB/bs2cp/bs2elements.jar>

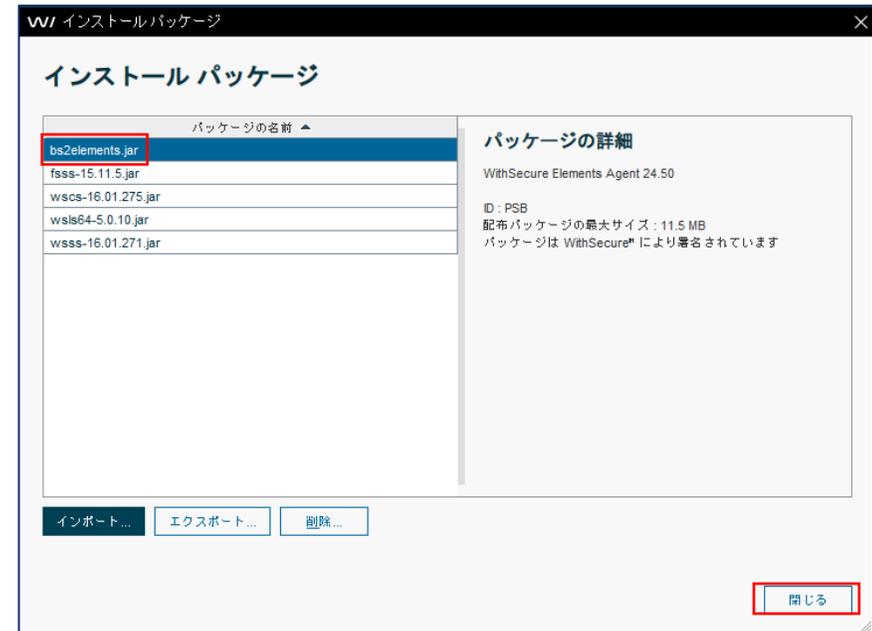
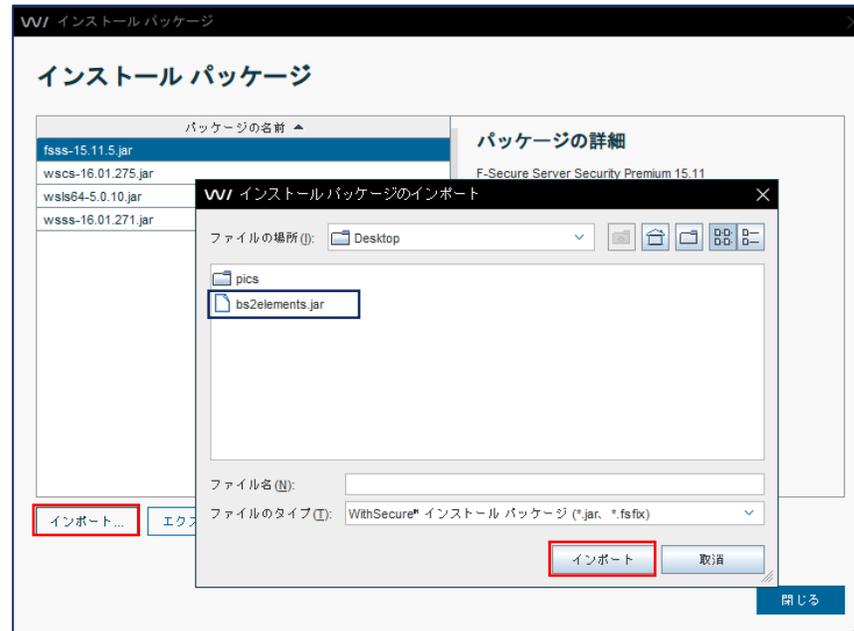
Step2：PMにログイン頂き、インストール>インストールパッケージを開きます。



④ 移行用インストーラをダウンロード&PMへインポート

[Windows/Windows Server 用インストーラのダウンロードからPMへのインポート]

Step3 : [インポート]を押してStep1でダウンロードしたインストーラ“bs2elements.jar” を選択し[インポート]を押してインポートします。
インストールパッケージ一覧に“bs2elements.jar” が存在する事を確認し[閉じる]を押します。



⑤ PMから各Clientへインポートした移行用インストーラを用いてインストール指示 (ポリシーベースインストール) [Top](#) >

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step1: PMにログイン頂き、ドメインツリーからインストール対象端末または対象ドメイングループを選択します。
(以下の例では、Windows Server 端末を選択しています)



※尚、Windows ClientとWindows Server への同時インストールできません。
これは、サブスクリプションキとプロファイルIDを一度に指定する事ができない為です。

⑤ PMから各Clientへインポートした移行用インストーラを用いてインストール指示 (ポリシーベースインストール) [Top](#) Top へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step2: インストールタブを開き下部の[インストール...]を押します。

WithSecure™ ポリシーマネージャコンソール

ファイル 編集 表示 ツール ヘルプ

ダッシュボード 設定 ステータス ソフトウェアアップデート 警告 スキャンレポート **インストール** Active Dir

ルート > WS2022AGENT > インストール

インストール

新しいホストをインポート
ホストを自動インストールするためのルールを作成する、またはホストを手動でインポートします。

インストールパッケージ
インストールパッケージのインポートとエクスポートを行います。

Windows ホストを自動検出
Windows ドメインとホストを自動的に検出してソフトウェアをリモートインストールします。

インストールされている製品

製品	バージョン	カウント	処理
WithSecure® Server Security	16.01	1	アップグレード アンインストール
WithSecure™ Server Security	合計	1	

ポリシーベース インストール

#	処理	ステータス
---	----	-------

インストール... 行を消去 テーブルを消去

⑤ PMから各Clientへインポートした移行用インストーラ用いてインストール指示 (ポリシーベースインストール) [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step3：インストールパッケージ一覧から“bs2elements.jar”を選択し[OK]を押します。



⑤ PMから各Clientへインポートした移行用インストーラを用いてインストール指示（ポリシーベースインストール） [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step4：対象端末のプラットフォームに対応したサブスクリプションキーを入力し[次へ]を押します。

W/ Elements Agent™

W / T H secure

サブスクリプションキー

製品のサブスクリプションキーを指定します。

間違ったサブスクリプションキーを入力すると、インストールが失敗して、気付くまでに数分かかる場合がありますので、正しいキーを入力したかどうか確認してください。

キーコード: - - - -

キャンセル < 戻る **次へ >** 完了

※サブスクリプションキーは、管理>サブスクリプションから確認できます。

W/ Elements™

管理 / サブスクリプション

サブスクリプション

サブスクリプション

サブスクリプションを移行する

オプションを選択 下に等しい オプションを選択 追加 すべてのフィルターをクリア

有効期限 次に等しい 有効

1 - 11 of 11 < < 1 of 1 > >

製品	ライセンスキーコード	組織	タイプ
WithSecure Elements EDR Business Suite for Servers		Konary_L1	評価
WithSecure Elements EDR Business Suite for Computers		Konary_L1	評価
WithSecure Elements EDR Business Suite for Computers		Konary_L1	評価
WithSecure Elements Collaboration Protection for Microsoft 365		Konary_L1	商業
WithSecure Elements EPP for Mobiles		Konary_L1	評価
WithSecure Elements Connector		Konary_L1	商業
WithSecure Elements EDR and EPP for Computers Premium		Konary_L1	評価
WithSecure Elements EPP for Computers		Konary_L1	評価
WithSecure Elements EDR and EPP for Computers Premium		Konary_L1	商業
WithSecure Elements EDR and EPP for Servers Premium		Konary_L1	商業
WithSecure Elements EPP for Servers		Konary_L1	商業

⑤ PMから各Clientへインポートした移行用インストーラ用いてインストール指示 (ポリシーベースインストール) [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step5：使用言語を選択し[次へ]を押します。



⑤ PMから各Clientへインポートした移行用インストーラ用いてインストール指示 (ポリシーベースインストール) [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step6 : 再起動オプションを選択し[次へ]を押します。

W/ Elements Agent™ W / T H secure

再起動オプション

PSBへの移行には再起動が必要な場合があります。コンピュータを再起動するタイミングかを指定できます。

再起動する前にユーザに確認する

次の時間が経過したら再起動する: 0 時間 5 分

キャンセル <戻る **次へ>** 完了

⑤PMから各Clientへインポートした移行用インストーラ用いてインストール指示（ポリシーベースインストール） [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step7：必要に応じてインストールタグ(ラベル)を入力し[次へ]を押します。

W/ Elements Agent™

W / T H
secure

インストールタグ

exeインストーラの--installation-tagsパラメータと同じです。バックエンドポータル（PSB）に報告するインストールタグです（例：PSB=psb-tag1:psb-tag2:psb-tag3,department=accounting,role=secretary）。

現在、PSBは「PSB=psb-tag1:psb-tag2:psb-tag3」から「label」フィールドまでのこれらのタグをカンマ区切りの値として格納しています。文字列の最大長は255文字です。これらのタグはカンマやコロンを含めることはできません。

インストールタグを設定しない

インストールタグ：

キャンセル <戻る **次へ>** 完了

※インストールタグ(ラベル)は後からでもESCから設定できます。

⑤ PMから各Clientへインポートした移行用インストーラ用いてインストール指示（ポリシーベースインストール） [Top](#) ^へ

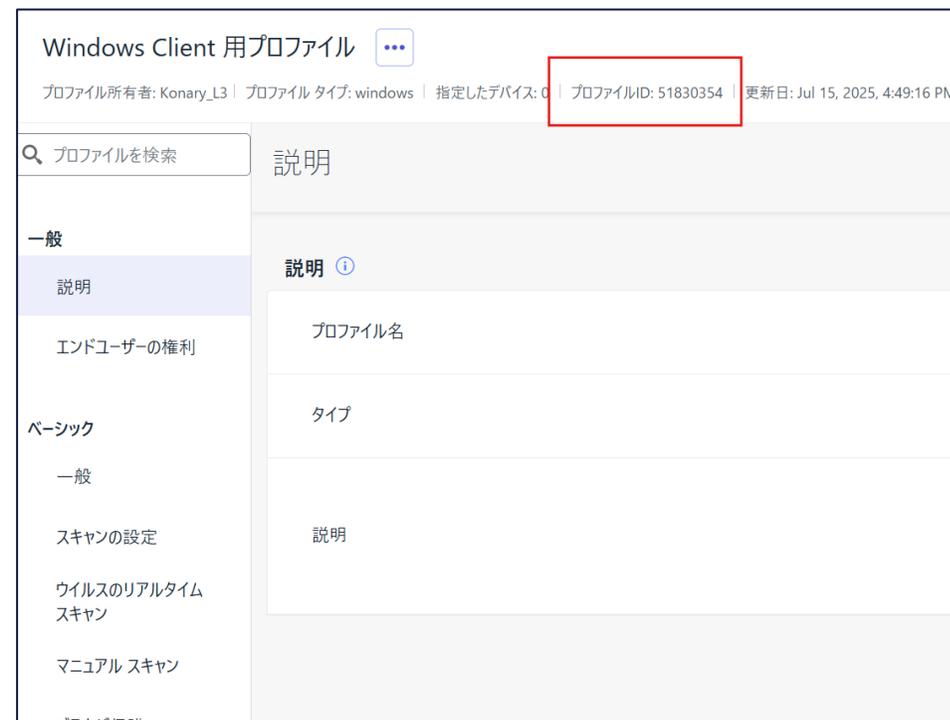
[Windows/Windows Server 端末への移行インストーラによるインストール]

Step8：必要に応じてインストール時にプロファイルを設定する場合にメモ頂いたプロファイルIDを入力し[次へ]を押します。



The screenshot shows the 'W/ Elements Agent' interface for selecting a profile ID. The title is 'プロフィールID'. Below the title, there is explanatory text: 'COSMOSの設定でプロファイルIDの値を設定します。プロファイルIDは、URLの中にあることがわかります。例：https://elements.f-secure.com/apps/psb/p#####/profiles/computer-protection/edit/18062053/generalSettings.' There are two radio button options: 'プロフィールIDを設定しない' (selected) and 'プロフィールID:'. At the bottom, there are four buttons: 'キャンセル', '<戻る', '次へ>' (highlighted with a red box), and '完了'.

プロファイルIDはプロファイルを開くと上部に表示されています。



The screenshot shows the 'Windows Client 用プロファイル' details page. At the top, it displays 'プロファイル所有者: Konary_L3 | プロファイルタイプ: windows | 指定したデバイス: 0 | プロファイルID: 51830354 | 更新日: Jul 15, 2025, 4:49:16 PM'. The 'プロファイルID: 51830354' is highlighted with a red box. Below this is a search bar 'プロフィールを検索' and a list of tabs: '一般', '説明', 'エンドユーザーの権利', 'ベーシック', '一般', 'スキャンの設定', 'ウイルスのリアルタイムスキャン', 'マニュアル スキャン'. The '説明' tab is active, showing '説明' and 'プロファイル名'.

⑤ PMから各Clientへインポートした移行用インストーラ用いてインストール指示 (ポリシーベースインストール) [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step9：必要に応じてConnectorを経由する場合にConnectorアドレスを入力し [次へ]を押します。



The screenshot shows the 'Elements Connector' configuration window. The title bar includes 'W/ Elements Agent™' and 'W / T H secure'. The main content area has the heading 'Elements Connector' and a sub-heading: 'クライアントに使用するElements Connectorをプロキシとして設定します。例：http://<Connectorのアドレス>:<Connectorのポート>'.

There are two radio button options:

- Elements Connectorを使用しない
- Elements Connectorのアドレス:

At the bottom, there are four buttons: 'キャンセル', '< 戻る', '次へ >', and '完了'. The '次へ >' button is highlighted with a red border.

⑤PMから各Clientへインポートした移行用インストーラ用いてインストール指示（ポリシーベースインストール） [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step10：必要に応じてConnectorを経由する場合にはプロキシアドレスにもConnectorアドレスを入力し [次へ]を押します。



W/ Elements Agent™

W / T H
secure

プロキシ

ダウンロードに使用するプロキシを上書きします。例：http://<プロキシアドレス>:<プロキシポート>

プロキシの設定を上書きしない

プロキシアドレス:

キャンセル <戻る **次へ>** 完了

※Connectorは使用しないがProxy Server経由でInternetへ接続するといった場合にも設定します。

⑤PMから各Clientへインポートした移行用インストーラ用いてインストール指示（ポリシーベースインストール） [Top](#) ^へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step11：SMBOS GUIDを使用するか否かを選択し [完了]を押します。（通常、物理構成の場合には“使用しない”のままで進めてください）



The screenshot shows a dialog box titled "SMBIOS GUID" from the W/TH Elements Agent software. The dialog contains the following text:

PSBでのCitrixサポートの場合、このマシンの一意の識別子としてSMBIOS GUIDを使用します。

同じマシン（同じSMBIOS GUIDを持つ）が、同じサブスクリプションキーで再度インストールまたは登録を行うと、ポータル上に新しいデバイスを作成する代わりに、ポータル上の同じデバイスに接続されます。

Below the text, there are two radio button options:

- SMBIOS GUIDを使用しない
- SMBIOS GUIDの使用を有効にする

At the bottom of the dialog, there are four buttons: "キャンセル", "<戻る", "次へ>", and "完了". The "完了" button is highlighted with a red border.

⑤ PMから各Clientへインポートした移行用インストーラを用いてインストール指示（ポリシーベースインストール） Top へ

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step12：以下の通りポリシーベースインストール一覧にセットされますので左上部の （ポリシー配布ボタン）を押します。
ポリシー配布画面が表示されましたら[配布]を押します。



The screenshot displays the WithSecure Policy Manager console. The main window shows the 'インストール' (Install) tab for the 'WS2022AGENT' policy. The left sidebar shows a tree view of the domain hierarchy, with 'WS2022AGENT' selected. The main content area shows the installation details, including a table of installed products and a table of policy-based installations.

製品	バージョン	カウント	処理
WithSecure® Server Security	16.01	1	アップグレード
WithSecure® Server Security	合計	1	アンインストール

操作	処理	ステータス
1	ホスト "WS2022AGENT" に WithSecure Elements Agent 24.5 をインストールしています	ポリシーの配布後に開始されます

The distribution preview window on the right shows the 'ポリシーのプレビューを配布する' (Distribute Policy Preview) dialog. It displays the policy name 'インストール' and the distribution status 'ポリシーベースインストール ...'. The '配布' (Distribute) button is highlighted with a red box.

⑤ PMから各Clientへインポートした移行用インストーラを用いてインストール指示（ポリシーベースインストール） [Topへ](#)

[Windows/Windows Server 端末への移行インストーラによるインストール]

Step13： Client側ではポップアップ等表示される事なくElements EPPがインストールされます。
(インストール途中で瞬間的にコマンドプロンプト画面が表示されます)

インストールされた以降は、ClientからPMへの通信は来なくなる為、PM側では以下の通り“進行中”のままの表示となります。

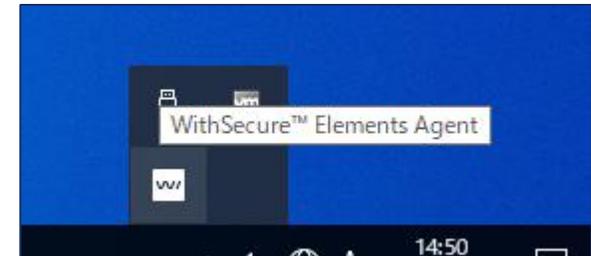
#	処理	ステータス
1	ホスト "WS2022AGENT" に WithSecure Elements Agent 24.5 をインストールしています	進行中

Step14： ESCにて、環境>デバイスをクリックしデバイス一覧に対象Clientが表示されておりましたら移行は完了です。



タイプ	名前	オンライン	登録日	OS名前
Computer	WS2022AGENT	はい	Jul 7, 2025	Windows Server 2
Mobile Device	WIN11	はい	Jul 30, 2024	Windows 11
Computer	WINSRV2022	はい	Apr 10, 2025	Windows Server 2

対象Client側でタスクトレイ内の製品アイコンにマウスをかざすと“WithSecure Elements Agent”と表示され製品が移行された事を確認できます。



※移行インストールが完了しESCのデバイス一覧で確認ができたClientにつきましては、PM上から削除頂く/作業ポリシーグループへ移動頂く等整理ください。

⑥ マイグレーションコマンドによるマイグレーション

[Linux端末へのマイグレーションコマンドによるマイグレーション]

※Linux PMが稼働するサーバ機上のLinux Security 64のマイグレーションは実施しないでください。
以下の手順を行わずにLinux PMをアンインストールするタイミングで⑪Linux PMとLinux Security 64のアンインストールを実施いただいてから⑦アンインストール&インストールのStep5の手順よりインストールを実施してください。

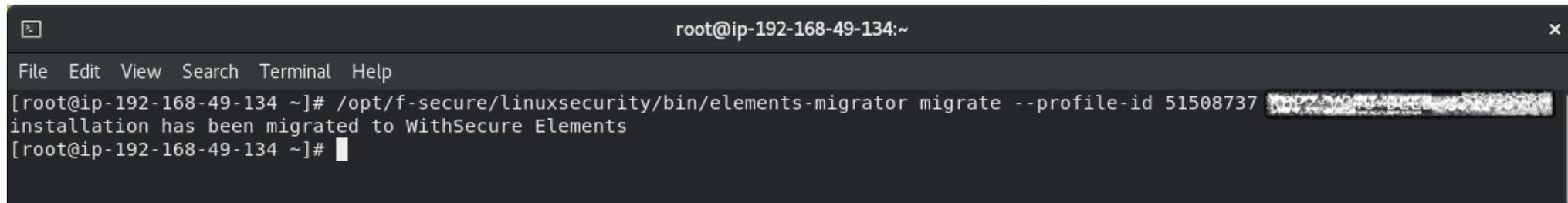
Step1：以下の通り、Linux端末上でroot権限でマイグレートコマンドをサブスクリプションキーを指定して実行する事により、移行できます。

```
/opt/f-secure/linuxsecurity/bin/elements-migrator migrate [SUBSCRIPTION-KEY]
```

また、上記コマンドに「--profile-id」オプションを付けて実行することで、予め作成したプロファイル割り当てることができます。

```
/opt/f-secure/linuxsecurity/bin/elements-migrator migrate --profile-id [PROFILE-ID] [SUBSCRIPTION-KEY]
```

※プロファイルIDを誤って指定すると、デフォルトプロファイルが割り当てられます。



```
root@ip-192-168-49-134:~  
File Edit View Search Terminal Help  
[root@ip-192-168-49-134 ~]# /opt/f-secure/linuxsecurity/bin/elements-migrator migrate --profile-id 51508737 [REDACTED]  
installation has been migrated to WithSecure Elements  
[root@ip-192-168-49-134 ~]#
```

[Linux Security 64 から WithSecure Elements への移行]

https://www.withsecure.com/userguides/product.html#business/linux-security-64/latest/ja/migrating_ls64_to_withsecure_elements-latest-ja

⑥ マイグレーションコマンドによるマイグレーション

[Linux端末へのマイグレーションコマンドによるマイグレーション]

Step2：ESCにて、環境>デバイスをクリックしデバイス一覧に対象Clientが表示されておりましたら移行は完了です。

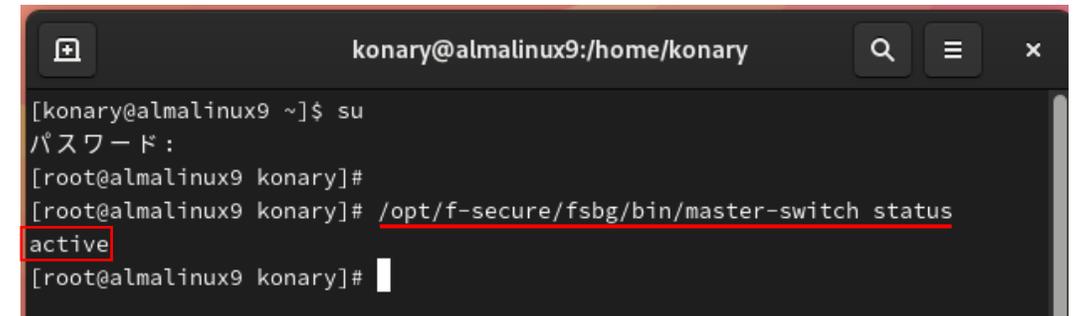


The screenshot shows the 'Environment / Devices' page in the ESC interface. The left sidebar has 'Devices' selected. The main area displays a table of devices with columns for 'Type', 'Name', 'Online', 'Registration Date', and 'OS Name'. Three devices are listed: an AlmaLinux 9.4 VM, a Windows 11 VM, and a Windows Server 2022 VM.

<input type="checkbox"/>	タイプ	名前	オンライン	登録日	OS名前
<input type="checkbox"/>	🖥️	ip-192-168-213-129.ap-northeast-1.compute.internal	はい	Jul 5, 2024	AlmaLinux 9.4 (Seafoam Ocelot)
<input type="checkbox"/>	💻	WIN11	はい	Jul 30, 2024	Windows 11
<input type="checkbox"/>	🖥️	WINSRV2022	いいえ	Apr 10, 2025	Windows Server 2022

root権限で以下のコマンドを実行しスタータスが“active”であれば動作している事を確認頂けます。

```
/opt/f-secure/fsbg/bin/master-switch status
```



The terminal screenshot shows a user named 'konary' on an 'almalinux9' host. The user switches to root using 'su', then runs the command '/opt/f-secure/fsbg/bin/master-switch status'. The output of the command is 'active', which is highlighted with a red box.

```
konary@almalinux9:/home/konary
[konary@almalinux9 ~]$ su
パスワード:
[root@almalinux9 konary]#
[root@almalinux9 konary]# /opt/f-secure/fsbg/bin/master-switch status
active
[root@almalinux9 konary]#
```

※移行インストールが完了しESCのデバイス一覧で確認ができたClientにつきましては、PM上から削除頂く/作業ポリシーグループへ移動頂く等整理ください。

⑦ アンインストール & インストール

[Linux端末へのアンインストール & インストール]

※Linux PMが稼働するサーバ機上のLinux Security 64のアンインストール & インストールは実施しないでください。
以下の手順を行わずにLinux PMをアンインストールするタイミングで ⑪Linux PMとLinux Security 64のアンインストールを実施 いただいたから
⑦アンインストール & インストールのStep5の手順よりインストールを実施 してください。

Step1 : root としてLinux端末にログインします。

アンインストール前に詳細について以下のユーザガイド「23 製品をアンインストールする」を参照ください。

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

※古いバージョンのLinux Security 64をお使いの場合には注意事項があります。

Step2 : 次のアンインストールコマンドを実行しLinux Security 64をアンインストールします。

RHELベースのディストリビューション : `rpm -e linuxsecurity-installer`

Debianベースのディストリビューション : `dpkg -r linuxsecurity-installer`

Step3 : 念のため、以下のコマンドを実行し確実に削除します。

```
rm -rf /opt/f-secure /etc/opt/f-secure /var/opt/f-secure
```

Step4 : Linux端末を再起動します。

Step5 : システム要件を再確認ください。必要な依存関係が不足している場合にはインストールしてください。

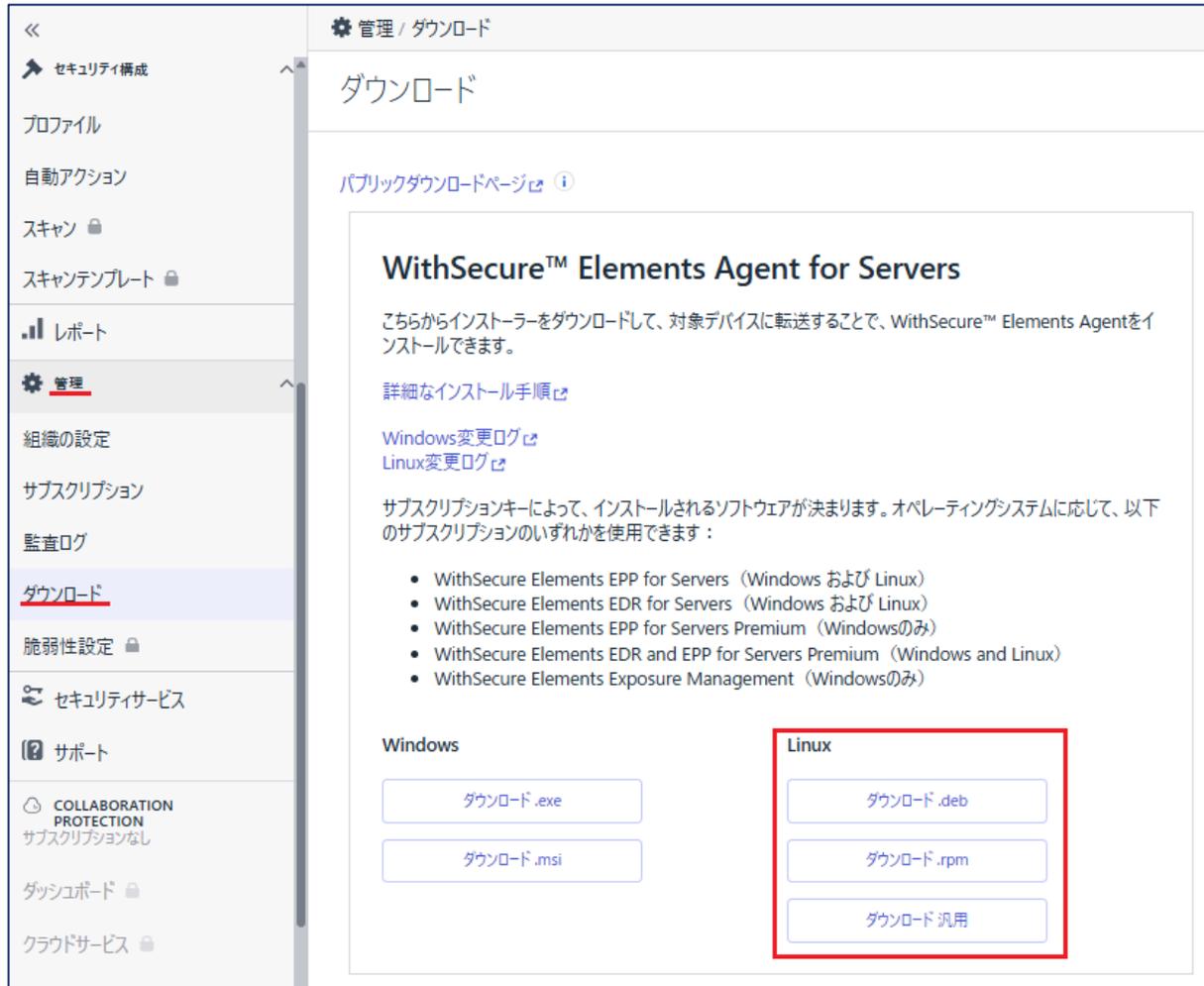
ユーザガイド :

<https://www.withsecure.com/userguides/product.html#business/linux-protection/latest/ja>

⑦ アンインストール&インストール

[Linux端末へのアンインストール&インストール]

Step6 : Linux用インストーラをESC>管理>ダウンロードまたはパブリックダウンロードページから入手しLinux端末へ配置します。



管理 / ダウンロード

ダウンロード

パブリックダウンロードページ ①

WithSecure™ Elements Agent for Servers

こちらからインストーラをダウンロードして、対象デバイスに転送することで、WithSecure™ Elements Agentをインストールできます。

[詳細なインストール手順](#)

[Windows変更ログ](#)
[Linux変更ログ](#)

サブスクリプションキーによって、インストールされるソフトウェアが決まります。オペレーティングシステムに応じて、以下のサブスクリプションのいずれかを使用できます：

- WithSecure Elements EPP for Servers (Windows および Linux)
- WithSecure Elements EDR for Servers (Windows および Linux)
- WithSecure Elements EPP for Servers Premium (Windowsのみ)
- WithSecure Elements EDR and EPP for Servers Premium (Windows and Linux)
- WithSecure Elements Exposure Management (Windowsのみ)

Windows	Linux
ダウンロード .exe	ダウンロード .deb
ダウンロード .msi	ダウンロード .rpm
	ダウンロード 汎用

パブリックダウンロードページ：

<https://www.withsecure.com/en/support/download>

ELEMENTS AGENT FOR SERVERS

Download for Windows (.EXE) →

Download for Windows (.MSI) →

Download for Linux (.DEB) →

Download for Linux (.RPM) →

Download for Linux (Generic/.Tar) →

Business Suite transition support package (.JAR)



⑦ アンインストール&インストール

[Linux端末へのアンインストール&インストール]

Step7: 次のインストールコマンドを実行します。

RHELベースのディストリビューション: `rpm -Uvh linuxsecurity-installer.rpm`

Debianベースのディストリビューション: `dpkg -i linuxsecurity-installer.deb`

Step8: 次のコマンドを実行して、製品をアクティブにします。

`/opt/f-secure/linuxsecurity/bin/activate --psb --subscription-key [SUBSCRIPTION-KEY] --profile-id [PROFILE-ID] --http-proxy=[Host:Port]`

※SUBSCRIPTION-KEYには、Linux用に割り当てられたサブスクリプションキーを指定してください。

※プロファイルを指定する場合には、“`--profile-id 12345678`”の様にプロファイルIDを指定してください。

※Connectorアドレスを“`--http-proxy=192.168.213.200:80`”の様に指定してください。



⑦ アンインストール&インストール

Topへ

[Linux端末へのアンインストール&インストール]

Step9：ESCにて、環境>デバイスをクリックしデバイス一覧に対象Clientが表示されておりましたら移行は完了です。

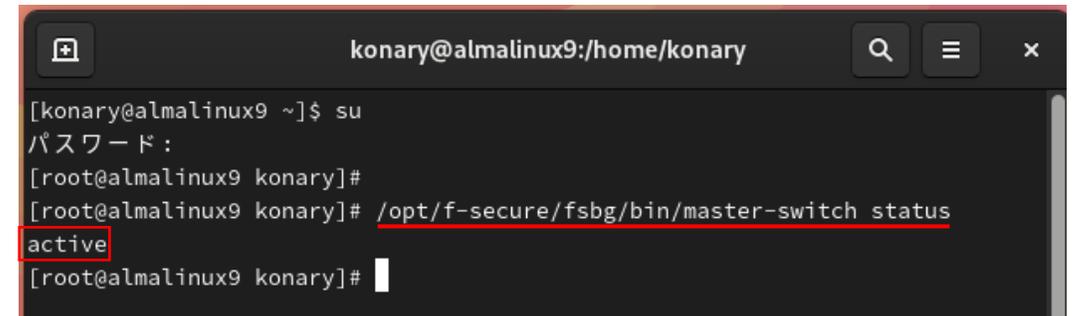


The screenshot shows the 'Devices' page in the ESC interface. The left sidebar contains navigation options like 'Home', 'Environment', 'Devices', 'Cloud', 'Network', etc. The main area displays a table of devices with columns for 'Type', 'Name', 'Online', 'Registered Date', and 'OS Name'. Three devices are listed: an AlmaLinux 9.4 instance, a Windows 11 instance, and a Windows Server 2022 instance.

タイプ	名前	オンライン	登録日	OS名前
🌐	ip-192-168-213-129.ap-northeast-1.compute.internal	はい	Jul 5, 2024	AlmaLinux 9.4 (Seafoam Ocelot)
💻	WIN11	はい	Jul 30, 2024	Windows 11
🖨️	WNSRV2022	いいえ	Apr 10, 2025	Windows Server 2022

root権限で以下のコマンドを実行しスタータスが“active”であれば動作している事を確認頂けます。

```
/opt/f-secure/fsbg/bin/master-switch status
```



The terminal screenshot shows a user named 'konary' at 'almalinux9' in the directory '/home/konary'. The user runs 'su' to become root. Then, the command '/opt/f-secure/fsbg/bin/master-switch status' is executed, and the output 'active' is displayed, which is highlighted with a red box.

```
konary@almalinux9:/home/konary
[konary@almalinux9 ~]$ su
パスワード:
[root@almalinux9 konary]#
[root@almalinux9 konary]# /opt/f-secure/fsbg/bin/master-switch status
active
[root@almalinux9 konary]#
```

※インストールが完了しESCのデバイス一覧で確認ができたClientにつきましては、PM上から削除頂く/作業ポリシーグループへ移動頂く等整理ください。

⑧ 上書きインストール

[MAC端末への上書きインストール]

Step1：システム要件を再確認ください。

ユーザガイド：

<https://www.withsecure.com/userguides/product.html#business/psb-cp-mac/latest/ja>

Step2：MAC端末のOS側でシステム設定またはnetworksetupユーティリティを用いてシステムプロキシ設定を構成しProxy ServerとしてConnectorを経由するように設定します。

Step3：パブリックダウンロードページから入手しMAC端末へ配置します。

パブリックダウンロードページ：

<https://www.withsecure.com/en/support/download>

ELEMENTS AGENT FOR COMPUTERS

Download for Windows (.EXE) →

Download for Windows (.MSI) →

Download for Mac (.MPKG) →

Business Suite transition support package (.JAR)

→

⑧上書きインストール

[MAC端末への上書きインストール]

Step4：次の通り配置したインストーラのファイル名を変更してから実行しインストールを行います。

Client Security for Mac自動的にアンインストールし、新しい製品をアクティブ化し、インストーラー名で指定されたプロファイルを適用します。

```
ElementsAgentInstaller__<subscription-key>__<profile-id>__.pkg
```

※区切り文字として必ず二重アンダースコア (__) を使用してください。

また、プロファイルID は常にサブスクリプション キーと組み合わせて使用する必要があります。

※subscription-keyには、MAC用に割り当てられたサブスクリプションキーを指定してください。

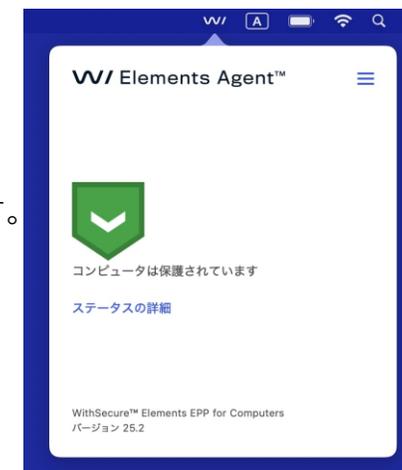
※profile-idには、“12345678” の様にプロファイルIDを指定してください。

Step5：ESCにて、環境>デバイスをクリックしデバイス一覧に対象Clientが表示されておりましたら移行は完了です。



タイプ	名前	オンライン	登録日	OS名前	指定プロファイル
Apple	usemoMacBook-Air	いいえ	Sep 24, 2024	macOS	Test20
Apple	fsecures-MacBook-Pro	いいえ	Jun 13, 2023	macOS	Test20

上部弊社アイコンをクリックし、“W/ Elements Agent”になっていれば移行は完了です。



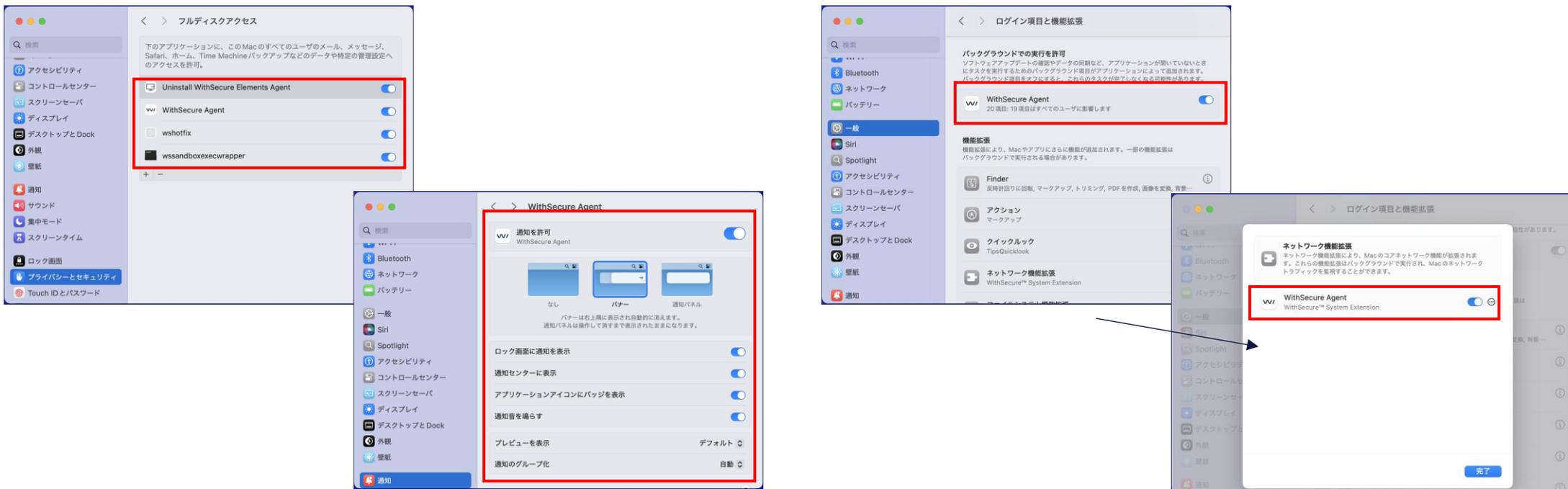
⑧ 上書きインストール

[MAC端末への上書きインストール]

※以下のユーザガイドも合わせて参照ください。

https://www.withsecure.com/userguides/product.html#business/psb-portal/latest/ja/migrating_cs4mac_to_elements4mac-psb-portal-latest-ja

※インストール完了後、以下の通りOS側でONにしてください。



その他の設定も含め、詳しくは以下のユーザガイドのMacデバイスの展開方法内の情報を参照ください。

<https://www.withsecure.com/userguides/product.html#business/psb-portal/latest/ja>

※移行インストールが完了しESCのデバイス一覧で確認ができたClientにつきましては、PM上から削除頂く/作業ポリシーグループへ移動頂く等整理ください。

⑨ アンインストール&インストール

[MAC端末へのアンインストール&インストール]

Step1 : Finderの移動>アプリケーションをクリックします。



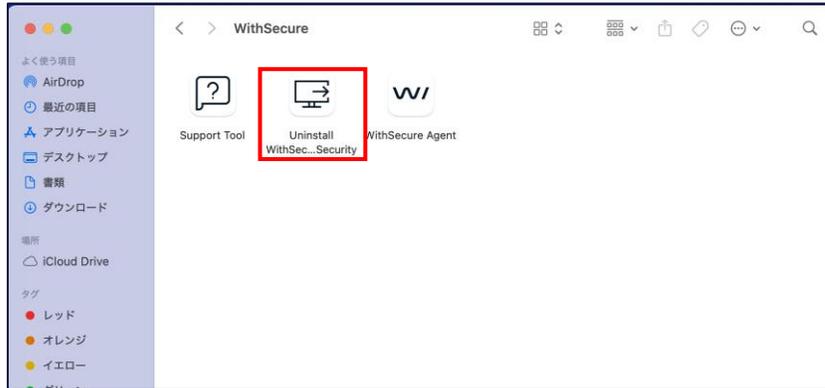
Step2 : WithSecureフォルダを開きます。



⑨ アンインストール&インストール

[MAC端末へのアンインストール&インストール]

Step3：“Uninstall WithSecure Client Security”を実行します。



Step4：[アンインストール]をクリックし、パスワードを入力します。



⑨ アンインストール&インストール

[MAC端末へのアンインストール&インストール]

Step5：再度Touch IDまたはパスワードを入力します。



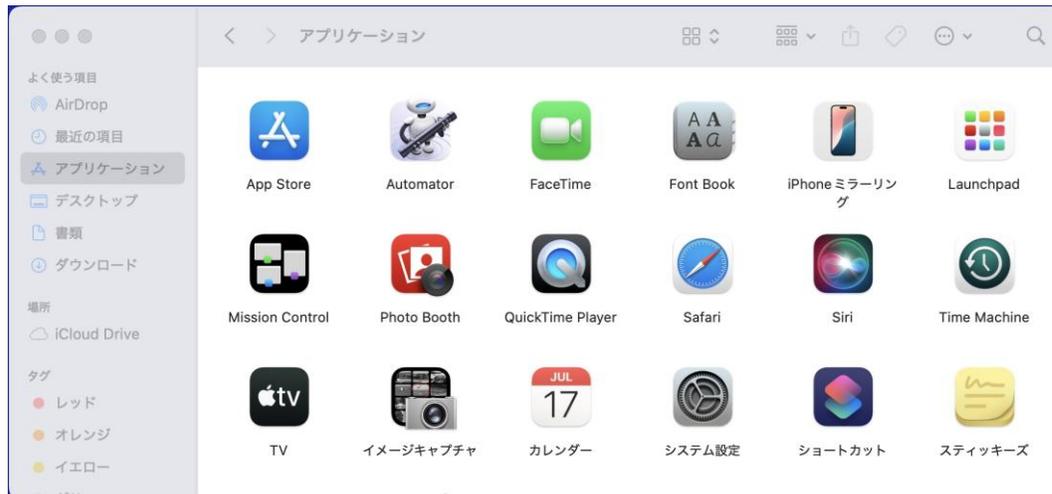
Step6：アンインストールが実施されます。



⑨ アンインストール&インストール

[MAC端末へのアンインストール&インストール]

Step7：アンインストールが完了すると以下のメッセージと共にアプリケーションからWithSecureフォルダが削除されます。



⑨ アンインストール&インストール

[MAC端末へのアンインストール&インストール]

Step8：システム要件を再確認ください。

ユーザガイド：

<https://www.withsecure.com/userguides/product.html#business/psb-cp-mac/latest/ja>

Step9：MAC端末のOS側でシステム設定またはnetworksetupユーティリティを用いてシステムプロキシ設定を構成しProxy ServerとしてConnectorを経由するように設定します。

Step10：パブリックダウンロードページから入手しMAC端末へ配置します。

パブリックダウンロードページ：

<https://www.withsecure.com/en/support/download>

ELEMENTS AGENT FOR COMPUTERS

Download for Windows (.EXE) →

Download for Windows (.MSI) →

Download for Mac (.MPKG) →

Business Suite transition support package (.JAR)



⑨ アンインストール&インストール

[MAC端末へのアンインストール&インストール]

Step11: 次の通り配置したインストーラのファイル名を変更してから実行しインストールを行います。
新しい製品をアクティブ化し、インストーラー名で指定されたプロファイルを適用します。

```
ElementsAgentInstaller__<subscription-key>__<profile-id>__.pkg
```

※区切り文字として必ず二重アンダースコア (__) を使用してください。

また、プロファイルID は常にサブスクリプション キーと組み合わせて使用する必要があります。

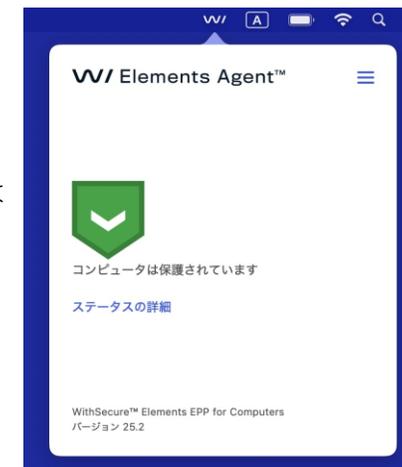
※subscription-keyには、MAC用に割り当てられたサブスクリプションキーを指定してください。

※profile-idには、“12345678” の様にプロファイルIDを指定してください。

Step12: ESCにて、環境> デバイスをクリックしデバイス一覧に対象Clientが表示されておりましたら移行は完了です。



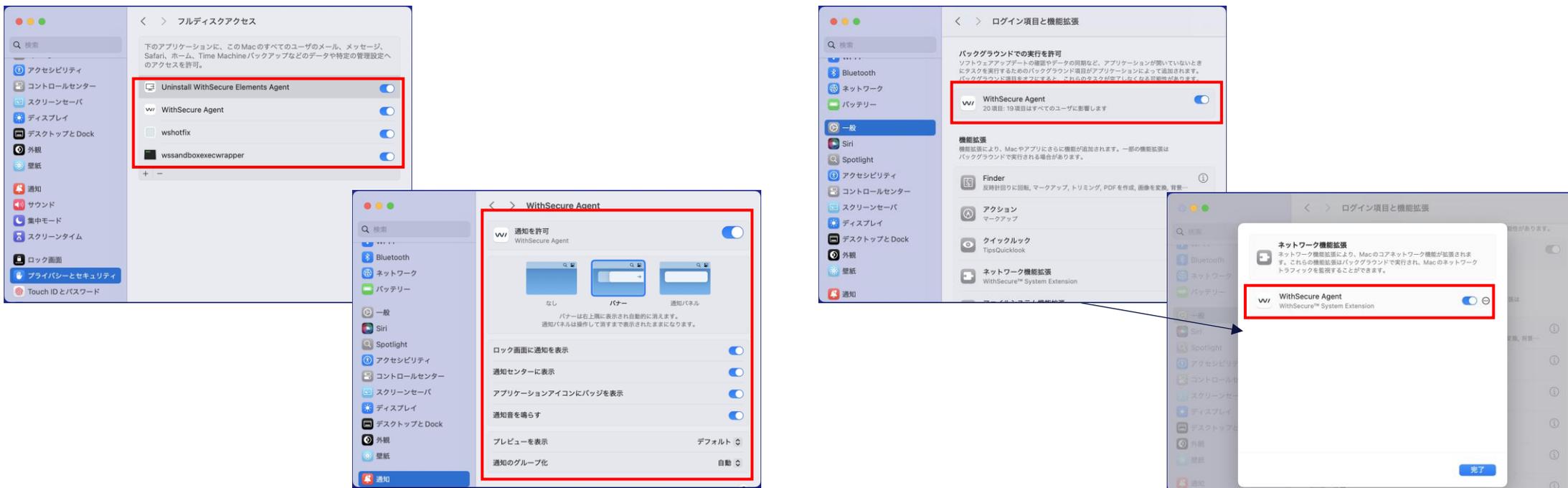
上部弊社アイコンをクリックし、“W/ Elements Agent”になっていればインストールは完了です。



⑨ アンインストール&インストール

[MAC端末へのアンインストール&インストール]

※インストール完了後、以下の通りOS側でONにしてください。



その他の設定も含め、詳しくは以下のユーザガイドのMacデバイスの展開方法内の情報を参照ください。

<https://www.withsecure.com/userguides/product.html#business/psb-portal/latest/ja>

※移行インストールが完了しESCのデバイス一覧で確認ができたClientにつきましては、PM上から削除頂く/作業ポリシーグループへ移動頂く等整理ください。

⑩PMのアンインストール

[Windows PMの場合]

※以下の手順を行う前に、必ず全てのホスト上のオンプレミス製品がElements製品へ移行されている事を確認してください。
PMをアンインストールしてしまうと、オンプレミス製品からElements製品へ移行が個別に手作業となります。

Step1：スタートメニューから [設定] を開き、 [アプリ] に移動します。

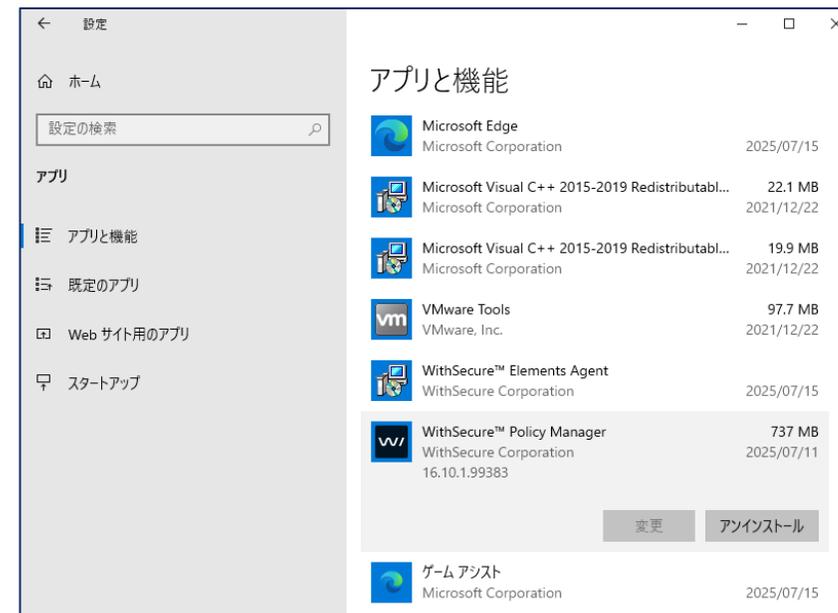
Step2：アプリと機能のリストで「WithSecure ポリシーマネージャ」を見つけます。

Step3：[アンインストール] をクリックしてアンインストールを開始させます。

Step4：アンインストールが完了したら、Windows の設定を終了します。

Step5：アンインストール後、コンピュータを再起動します。

※再起動は、アンインストール後のコンピュータに残ったファイルを消去するために必要です。
また、WithSecureの同製品をインストールする場合にも必要です。



※詳細につきましては、以下のユーザガイド内「16 アンインストール」を参照ください。

<https://www.withsecure.com/userguides/product.html#business/policy-manager/16.00/ja>

⑩PMのアンインストール

[Linux PMの場合]

※Linux PMとLinux Security 64またはLinux Protectionが共存している場合は、以下の手順は行わずに、

[⑪Linux PMとLinux Security 64のアンインストール](#)を参照してください。

※以下の手順を行う前に、必ず全てのホスト上のオンプレミス製品がElements製品へ移行されている事を確認してください。

PMをアンインストールしてしまうと、オンプレミス製品からElements製品へ移行が個別に手作業となります。

ポリシーマネージャのLinux版をアンインストールするには、コンポーネントを決まった順序でアンインストールする必要があります。

Step1: rootとしてログインします。

Ubuntu ディストリビューションを使用している場合、/etc/sudoers に追加された通常のユーザでログインします。

Step2: ターミナルを開きます。

※PMアンインストール後にConnectorを本サーバ機に導入する場合には以下を実行してからサーバ機の再起動実施後にお願いします。

Step3: 次のコマンドを順に実行します。

[RPM ベース]

1. rpm -e f-secure-policy-manager-server
2. rpm -e f-secure-policy-manager-console

[Ubuntu/Debian ベース]

1. dpkg -r f-secure-policy-manager-server
2. dpkg -r f-secure-policy-manager-console

注: ポリシーマネージャが作成した再生不可能なデータ (ログ ファイル、MIB ファイル、ドメイン ツリー、設定ファイルなど) が誤って削除されることを防ぐために、次のディレクトリはアンインストール中に削除されません。今後必要となる可能性があるキーは削除しないことを推奨します。製品を完全にアンインストールするには、rootとしてログインし、次のコマンドを実行します。

1. rm -rf /var/opt/f-secure/fspms
2. rm -rf /var/opt/f-secure/fsaus
3. rm -rf /etc/opt/f-secure/fspms
4. rm -rf /etc/opt/f-secure/fsaus
5. rm -rf /opt/f-secure/fspmc

※詳細につきましては、以下のユーザガイド内「20 アンインストール」を参照ください。

<https://www.withsecure.com/userguides/product.html#business/policy-manager/16.00/ja>

⑪ Linux PMとLinux Security 64のアンインストール

[Linux PMとLinux Security 64 をアンインストールします]

※以下の手順を行う前に、必ず全てのホスト上のオンプレミス製品がElements製品へ移行されている事を確認してください。
PMをアンインストールしてしまうと、オンプレミス製品からElements製品へ移行が個別に手作業となります。

Step1 : root としてLinux端末にログインします。

アンインストール前に詳細について以下のユーザガイド「23 製品をアンインストールする」を参照ください。

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

※古いバージョンのLinux Security 64をお使いの場合には注意事項があります。

Step2 : 次のアンインストールコマンドを実行しLinux Security 64をアンインストールします。

RHELベースのディストリビューション : rpm -e linuxsecurity-installer

Debianベースのディストリビューション : dpkg -r linuxsecurity-installer

Step3 : Ubuntu ディストリビューションを使用している場合、/etc/sudoers に追加された通常のユーザでログインします。

Step4 : 次のコマンドを順に実行してPMをアンインストールします。

[RPM ベース]

1. rpm -e f-secure-policy-manager-server
2. rpm -e f-secure-policy-manager-console

[Ubuntu/Debian ベース]

1. dpkg -r f-secure-policy-manager-server
2. dpkg -r f-secure-policy-manager-console

⑪ Linux PMとLinux Security 64のアンインストール

[Top](#) ^

[Linux PMとLinux Security 64 をアンインストールします]

※以下の手順を行う前に、必ず全てのホスト上のオンプレミス製品がElements製品へ移行されている事を確認してください。
PMをアンインストールしてしまうと、オンプレミス製品からElements製品へ移行が個別に手作業となります。

Step5：念のため、以下のコマンドを実行し確実に削除します。

```
rm -rf /opt/f-secure /etc/opt/f-secure /var/opt/f-secure
```

Step6：Linux端末を再起動します。

※各資料のダウンロード先URL

[本資料最新版]

https://f-secure.my.salesforce.com/sfc/p/b0000000JXpV/a/av000001CltR/eN5yTdq77uV.LihkhD.cX.55IImE9KU_jsG_VwZCgbQ

[サポートリソース] (さまざまなドキュメントリンクを掲載しています)

<https://www.withsecure.com/jp-ja/support/support-resources>