Orchestrating a brighter world

NEC

Trellix Application Controlのご紹介

2023年01月

日本電気株式会社

\Orchestrating a brighter world

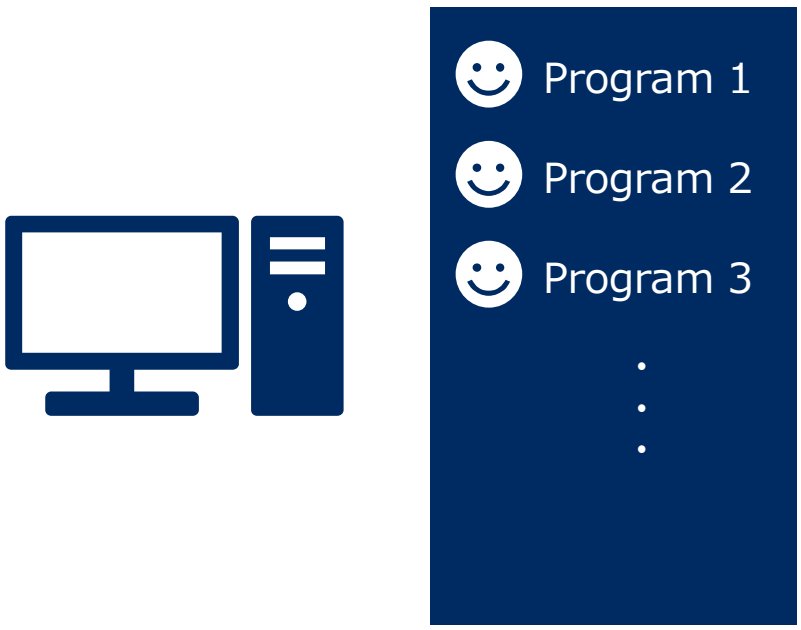
未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

Trellix Application Controlとは

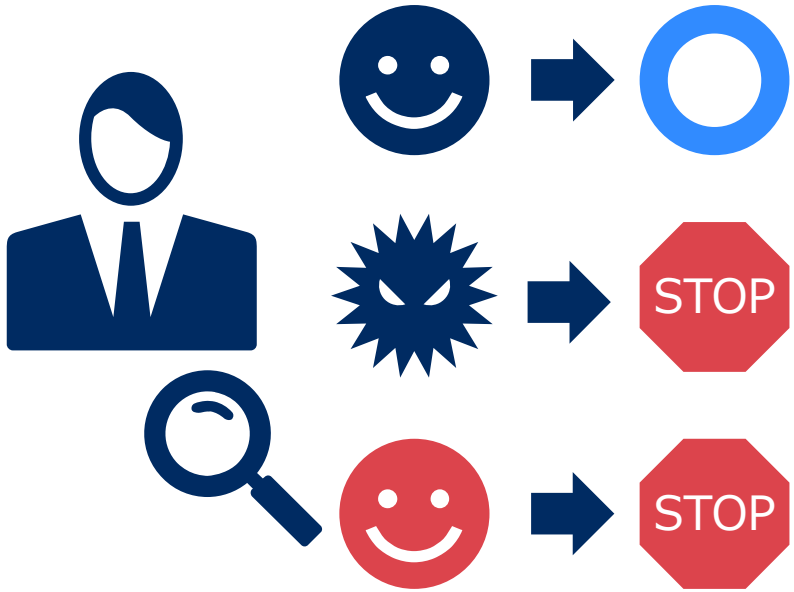
正規のプログラムのみを動作させる
ホワイトリスト方式を利用したセキュリティソフトウェア

運用前



予め動作させるプログラムを登録

運用中



登録されたプログラムのみを動作

Trellix Application Controlの特長

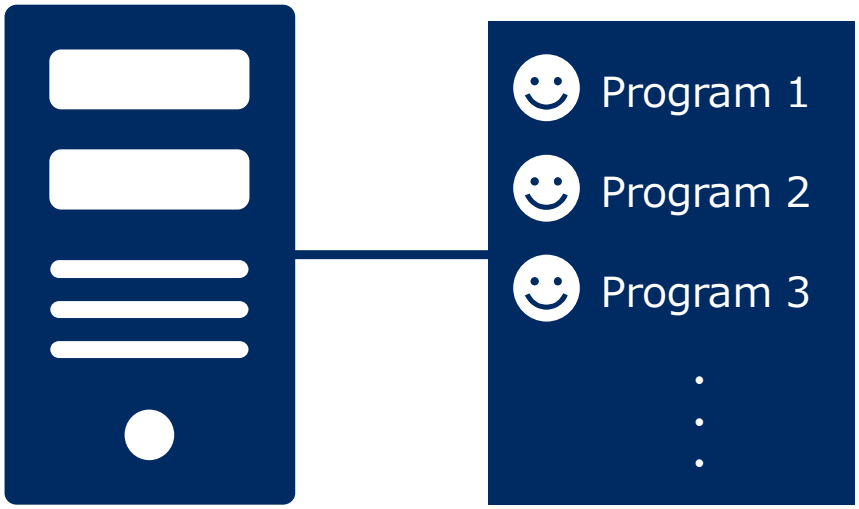
1	強固なセキュリティ
2	改ざんの防止と検知
3	リストの定期的な更新が不要
4	システムへの影響が軽微
5	ぜい弱性攻撃への対応
6	管理製品との連携

強固なセキュリティ

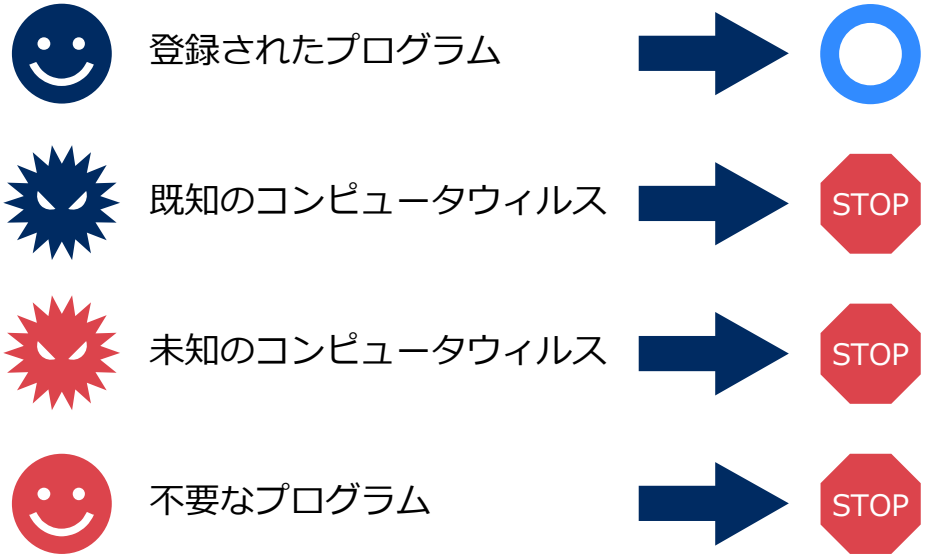
予めリストに登録されたプログラムだけを動作させることでセキュリティ強化

- 既知のコンピュータウィルスだけでなく、今後、出現する未知のコンピュータウィルスにも対応
- 不要なプログラムの動作も禁止することができ、エンドユーザの不用意なシステム変更によるトラブルも防止

予め動作させるプログラムをリスト化し、
リストに登録されたプログラムだけを動作



登録されていないプログラムは
全て動作を禁止



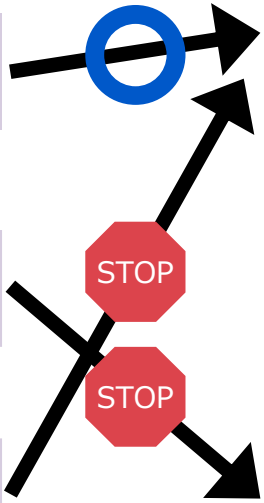
プログラムの改ざんの防止と検知

改ざんの防止と検知にてシステムを保護

- ホワイトリストに登録されているプログラムの変更（更新、削除）を防止
- ホワイトリストには、実行ファイルの絶対パスだけでなく、ハッシュ値も登録しているため、改ざんされたプログラムの実行も阻止

実行ファイルの起動時に、
実行ファイルの情報（絶対パスとハッシュ値）が
システムインベントリに登録されているか確認

	C:¥program1.exe	44f6e5a9
	C:¥Virus.exe（ウィルス）	90a9ffe9
	C:¥program1.exe（改ざん）	4ef6e509



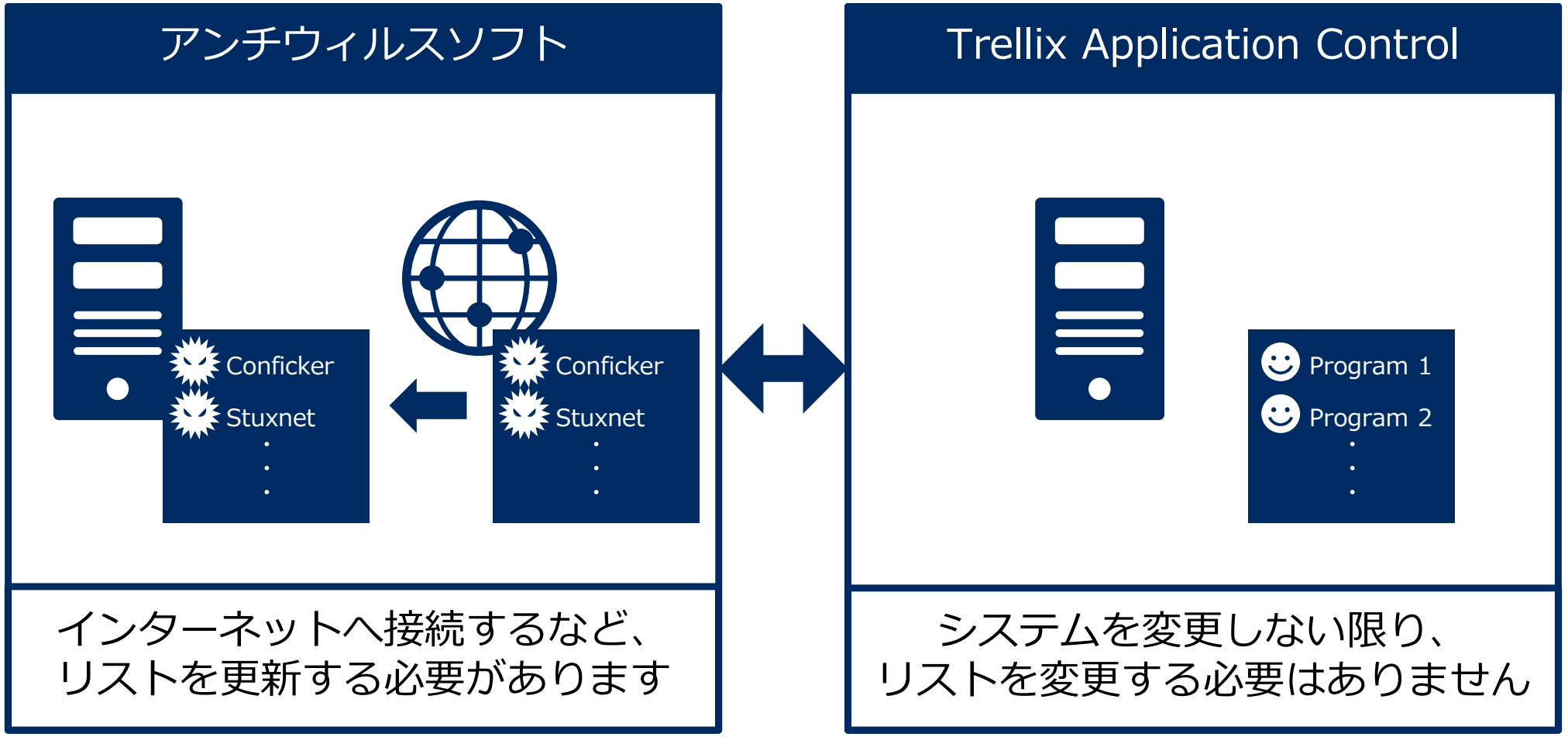
ホワイトリスト（イメージ）

実行ファイルの絶対パス	ハッシュ値
C:¥program1.exe	44f6e5a9
C:¥program2.exe	42a78ef3
C:¥program3.exe	6a4a8fb5
C:¥program4.exe	7fbb1b78

リストの定期的な更新が不要

リストの定期的な更新が不要のため、インターネットに未接続の環境でも利用可能

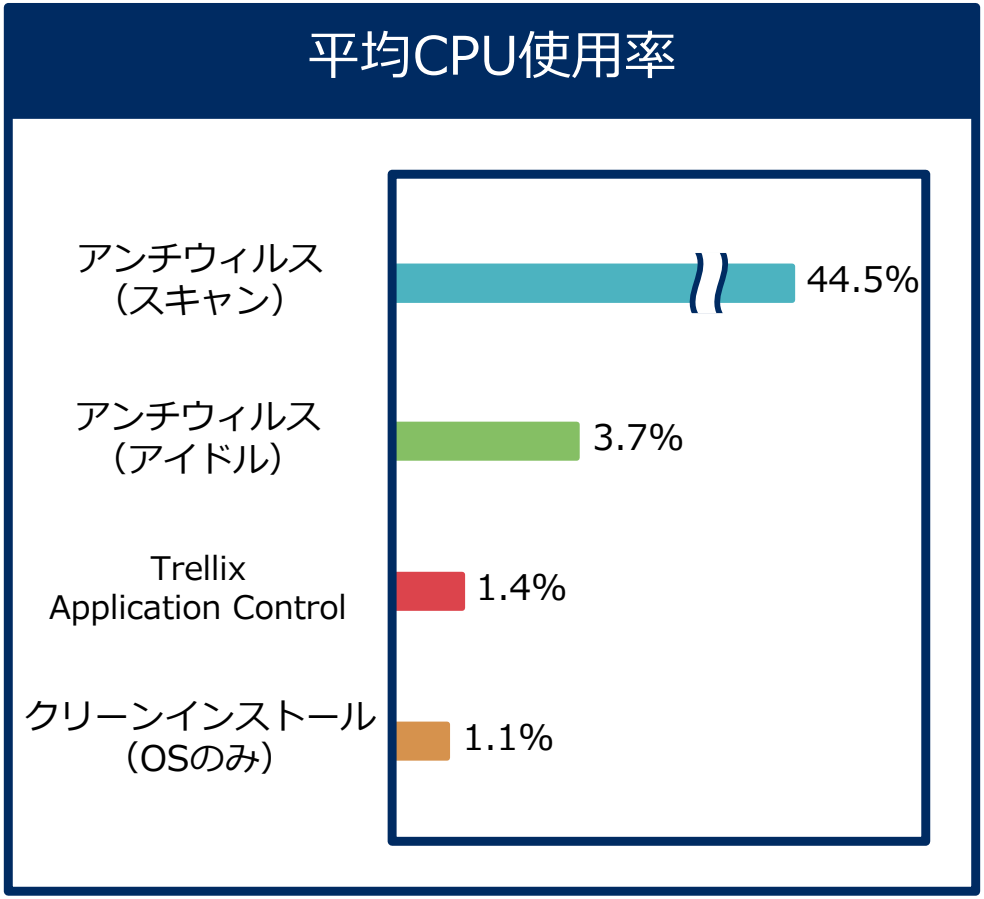
- 一般的なアンチウィルスソフトのようなリストの更新が不要
- リストを更新するためにインターネットへの接続やサーバの設置が不要

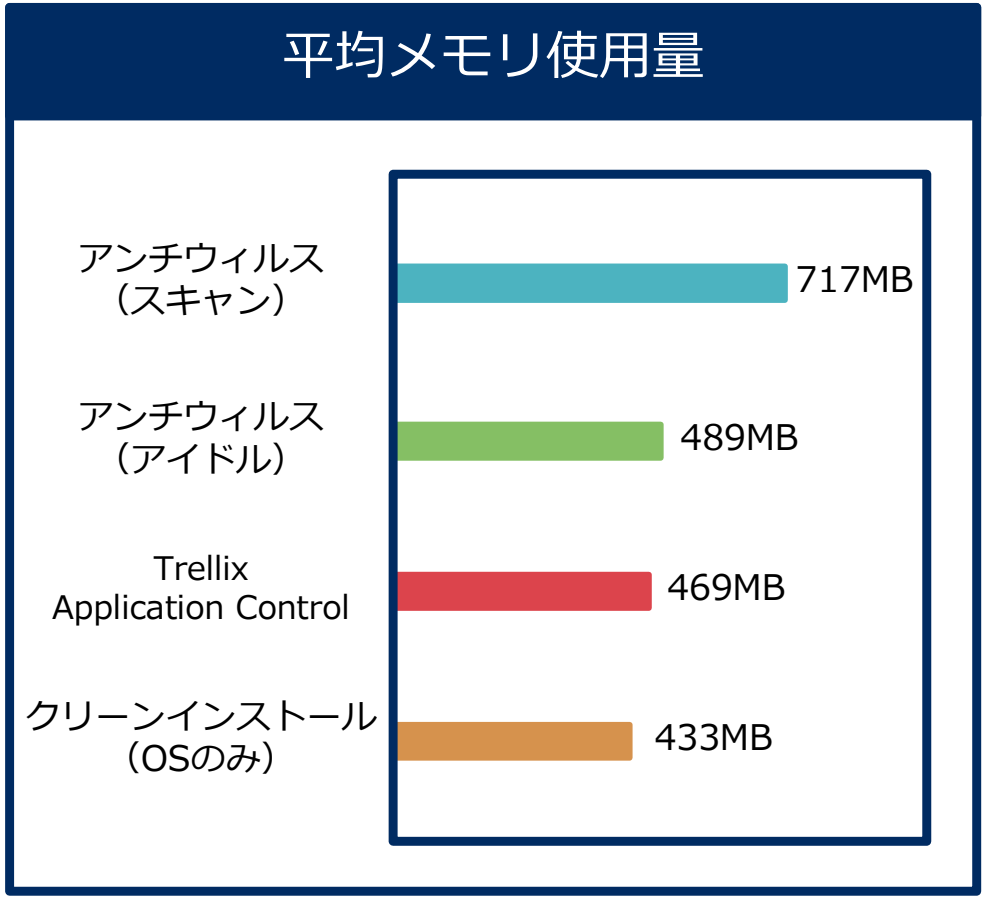


システムへの影響が軽微

アンチウィルスソフトの適用が難しい場合でも利用が可能

- コンピュータリソースの少ない機器でも利用可能
- 一般のアンチウィルスソフトと比べ、システムパフォーマンスへの影響が少ない



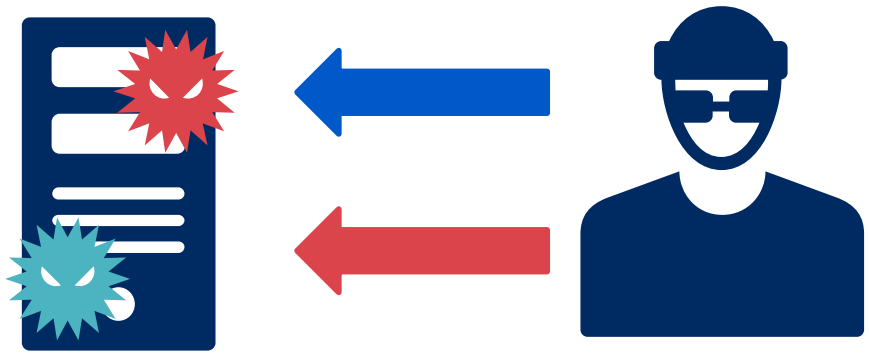


メモリ保護機能

ぜい弱性攻撃に利用されるバッファオーバーフロー攻撃からシステムを保護

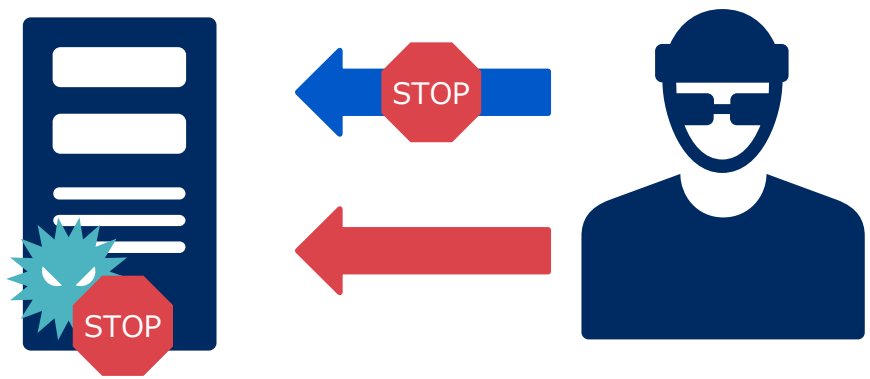
- ぜい弱性攻撃に利用されるバッファオーバーフロー攻撃からシステムを保護することで、サポート終了後のセキュリティリスクを軽減
- ぜい弱性攻撃によりウィルス送り込まれてもホワイトリストにより停止

メモリ保護機能なし



ぜい弱性を利用した攻撃により、
ウィルスによる被害を受けてしまいます

メモリ保護機能あり

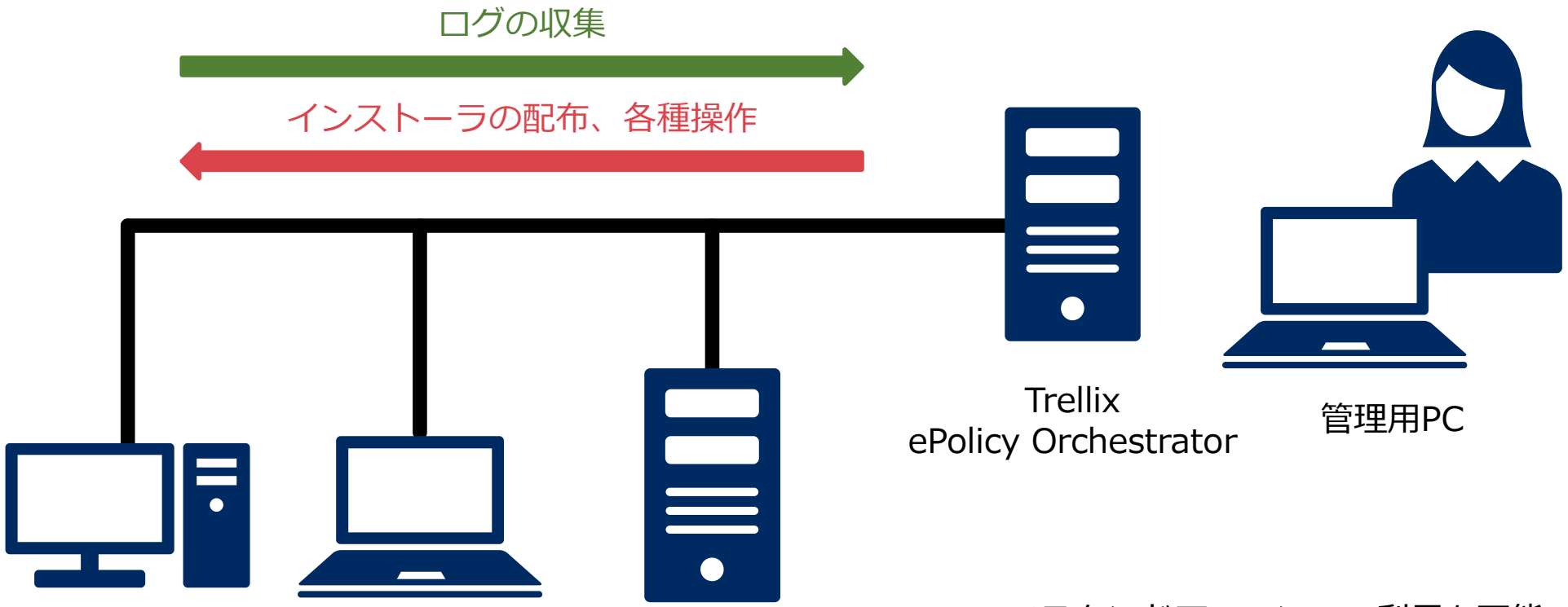


攻撃を無効化、もし無効化できずにウィルスを
送り込まれても動作を止めることが可能です

管理製品との連携

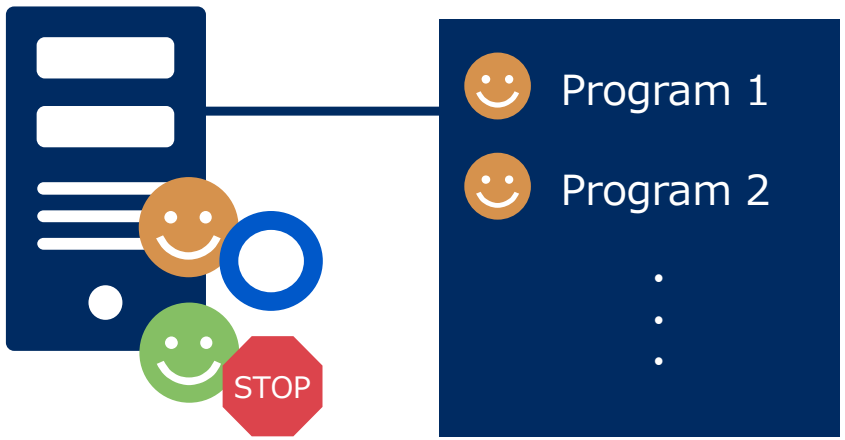
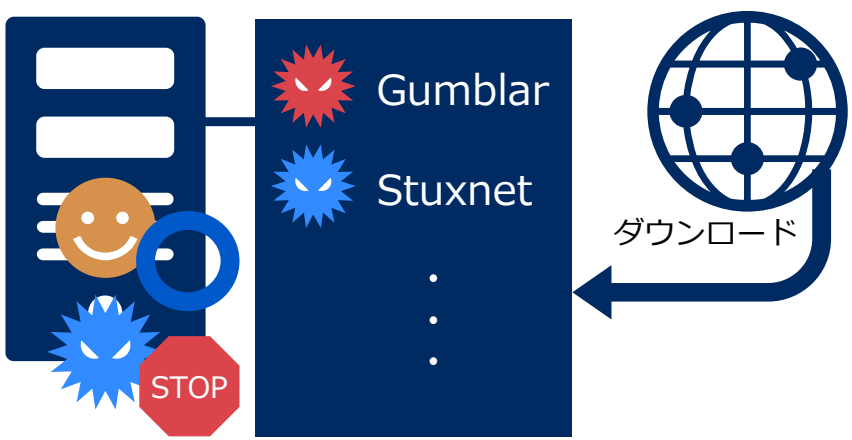
Trellix ePolicy Orchestratorによるセキュリティの一元管理

- 管理製品であるTrellix ePolicy Orchestratorとの連携により、他のTrellix製品と一元管理が可能
- 各端末へのTrellix Application Controlのインストールや各種操作、各端末のログの収集などが可能



※スタンドアローンでの利用も可能です

一般のアンチウィルスソフトとの違い

ホワイトリスト方式		ブラックリスト方式 （一般のアンチウィルスソフト）
		
リストに記載されていないプログラムを禁止	⇔	リストに記載されているプログラムを禁止
プログラムを変更しない限りリストは更新不要	⇔	リストの常時更新が必要
インターネットへの接続が不要	⇔	インターネットへの接続が必要
未知のコンピュータウィルスも対応	⇔	既知のコンピュータウィルスのみ対応

一般のアンチウィルスソフトとの比較

項目	Trellix Application Control	アンチウィルスソフト
手法	ホワイトリスト方式	ブラックリスト方式
既知のコンピュータウィルス	有効	有効
未知のコンピュータウィルス	有効	無効
不要なアプリケーション	有効	無効
マクロウィルス	無効※1	有効
プログラムの改ざん防止	あり	なし
パフォーマンスへの影響	軽微	大きい
リストの更新	ファイルの変更時	常時
配信サーバ、もしくはネットワーク接続	不要	必要
システム更新の手間	若干増える※2	—

※　この表は技術的見地に基づくものであり、必ずしもセキュリティを保証するものではありません

※1 Microsoft Office製品では電子署名を使用することにより対処することができます

※2 一度、保護された状態を解除する、もしくは、更新を許可する設定を行う必要があります

動作環境　クライアント用

2022/12現在

主な動作要件

- x86-64/AMD64 アーキテクチャ対応するプロセッサー
- メモリ容量2 GB RAM(Windows 64-bit)/メモリ容量1 GB RAM(Windows 32-bit)
- システム ボリュームに 100 MB の空きディスク容量(インストール用)
- 固定化されている各ボリュームに 100 MB の空きディスク容量
- TCP/IP プロトコルがシステムにインストールされていること

OS

- Windows 10 Enterprise　LTSC 2021/LTSC 2019/LTSB 2016
- Windows 11
- Windows 11 IoT
- Windows 10 (version1507-21H2)
- Windows 10 IoT (Version 1507-2021)
- Windows 8.1/8※1
- Windows Embedded 8.1/8 Industry

2026年12月31日でLegacy Platform Support保守終了

- Windows 7
- Windows Embedded 7 POSReady

備考

- 弊社技術支援のもと、ハードウェア毎に個別に検証していただきます

※1 メモリ保護機能はご利用になれません

動作環境　サーバ用

2022/12現在

主な動作要件

- x86-64/AMD64 アーキテクチャ対応するプロセッサー
- メモリ容量2 GB RAM(Windows 64-bit)/メモリ容量1 GB RAM(Windows 32-bit)
- システム ボリュームに 100 MB の空きディスク容量(インストール用)
- 固定化されている各ボリュームに 100 MB の空きディスク容量
- TCP/IP プロトコルがシステムにインストールされていること

OS

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012/2012R2

2026年12月31日でLegacy Platform Support保守終了

- Windows Server 2008/2008R2
- Windows Server 2003

備考

- 弊社技術支援のもと、ハードウェア毎に個別に検証していただきます

動作環境

2022/12現在

サポートが終了したOS向けにLegacy Platform Supportを提供しています

対象OS

- Microsoft Windows 7 /Embedded /Embedded POSReady
- Microsoft Windows XP / XPE
- Microsoft Windows Embedded Point of Service(WEPOS)2009
- Microsoft Windows Server 2003 / 2003 R2
- Microsoft Windows Server 2008 / 2008 R2 / Core

価格

- **個別見積**になりますので、別途お問い合わせください

サポート期間

- Trellix社の延長サポートが伸びたために**2026年12月31日**までとなります。

詳細

- 詳細については、下記URLをご確認ください
  https://kcm.trellix.com/corporate/index?page=content&id=KB85993&actp=null&viewlocale=ja_JP&locale=ja_JP

Trellix Application Control 価格体系

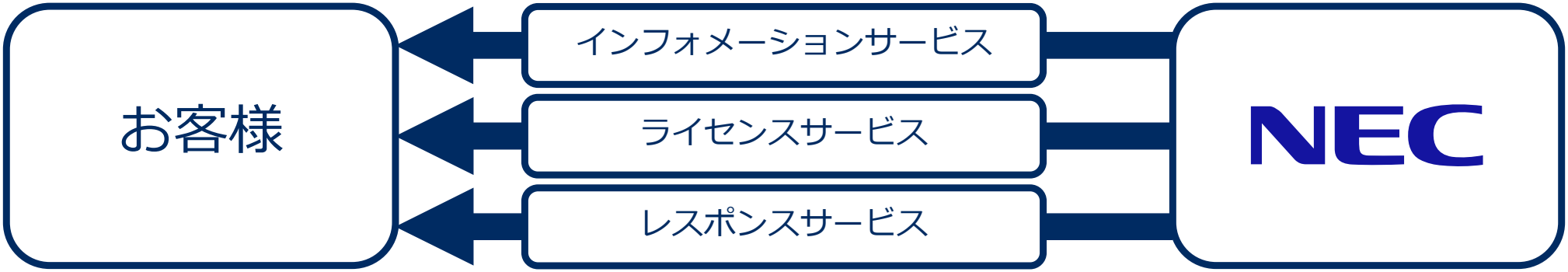
2022/12現在

- ライセンスは 無期限
- サポートは 1年間単位
- 購入ライセンス数にて単価が決定
- Legacy Platform Supportについては別途費用が発生

ノード数	PC		Server	
	新規	更新	新規	更新
1 - 25	15,884	3,437	128,416	28,046
26 - 50	12,866	2,784	103,009	22,496
51 - 100	12,709	2,751	90,076	19,671
101 - 250	11,119	2,407	77,278	16,876
251 - 500	10,803	2,340	70,755	15,452
501 - 1,000	9,848	2,133	62,266	13,599
1,001 - 2,000	8,764	1,898	51,057	11,152
2,001 - 5,000	6,575	1,424	40,846	8,919
5,001 - 10,000	4,930	1,065	31,860	6,959
10,001 -	3,696	802	24,212	5,289

お問合せについて

PPサポートの標準サービスを提供いたします



インフォメーション サービス	ソフトウェア製品に関わる各種情報を専用Webサイトや、電子メールによるニュースレターにてご提供いたします。
ライセンス サービス	ソフトウェア製品のアップデートモジュールをご提供いたします。
レスポンス サービス	ソフトウェア製品の導入や運用中に発生した様々な問題や疑問点について、迅速に原因解決または回避方法をご提示いたします。 サービス時間 月曜日～金曜日　8：30～17：30（土日、祝祭日及びNECの休日を除く）

まとめ

Trellix Application Controlは、アンチウィルスソフトの利用が難しい
環境でのセキュリティ向上に貢献します

① 強固なセキュリティ
② 改ざんの防止と検知
③ リストの定期的な更新が不要
④ システムへの影響が軽微
⑤ ぜい弱性攻撃への対応
⑥ データ保護

ホームページ　http://jpn.nec.com/soft/mcafee/application_control/
お問合せ先　soft@embd.jp.nec.com


Orchestrating a brighter world
NEC

Trellix Application Controlのご紹介

Trellix Application Controlの運用について

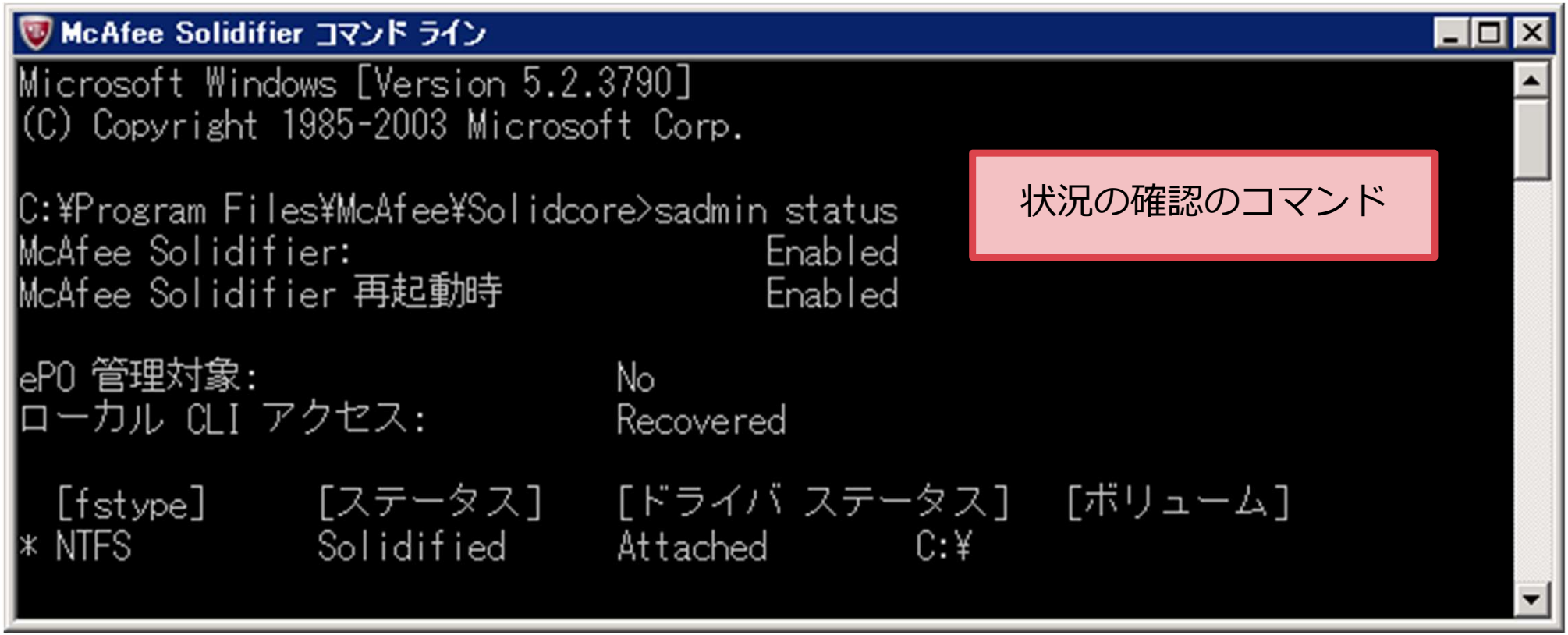
Trellix Application Controlの管理

コマンドプロンプトでの操作が可能

- 管理者でないエンドユーザによる安易な設定変更を防止

コマンドをバッチファイル化することが可能

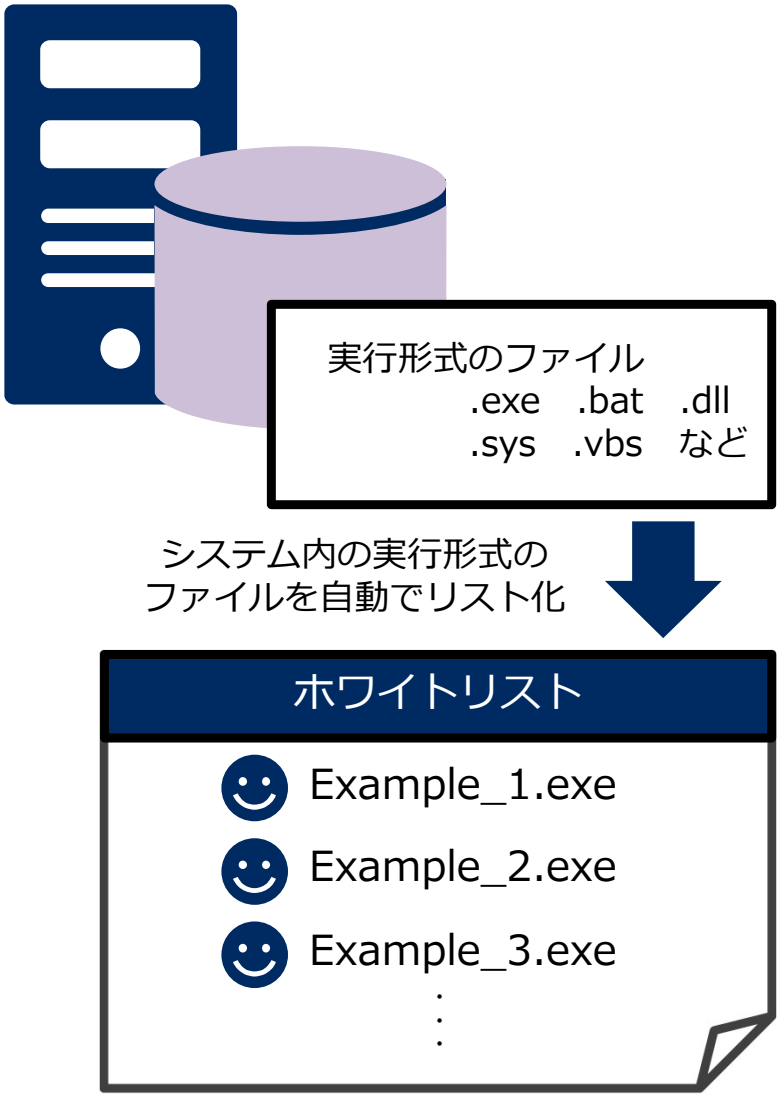
- 既存の更新手順に組み込むことが可能



Trellix Application Controlの導入

システム構築後にホワイトリストを作成

1. システムの構築
2. ホワイトリストの作成（システムを固める）
   ※ コマンドによる自動登録
3. 各種設定（必要に応じて）
   ※ バッチファイルにて設定可能
4. システムの保護の開始



アプリケーションの更新について

改ざん防止機能のため、そのままではプログラムの更新はできません

- Trellix Application Controlは、ホワイトリストに登録されたプログラムの変更（更新、削除）を防止します

- このため、プログラムを正規に更新しようとしても、通常の手順（インストーラ実行、ファイルの置き換え、など）では更新に失敗します

- Trellix Application Controlでは、プログラムの更新を行う方法として、下記の方法を用意しています

1. 更新モードへの切り替え
2. 更新を行うプログラムに権限を付加

更新モードへの切り替え

プログラム更新専用のモードにて作業を実施

- これまでの更新作業の前後にコマンドを実行
- 更新作業の内容は自動でホワイトリストに登録

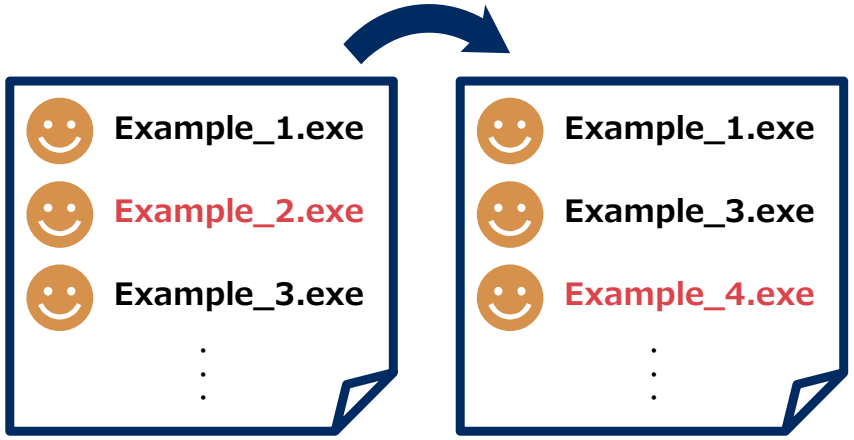
1. 更新モードへの切り替え
   ※ コマンドを実行、再起動不要

Example_2.exe を削除、
Example_4.exe を追加

2. 更新作業を実施
   ※ 更新内容は自動的でホワイトリストに反映

ホワイトリストを自動的に更新
※ ホワイトリストの再作成は不要

3. 更新モードを終了し、運用モードに戻す
   ※ コマンドを実行、再起動不要

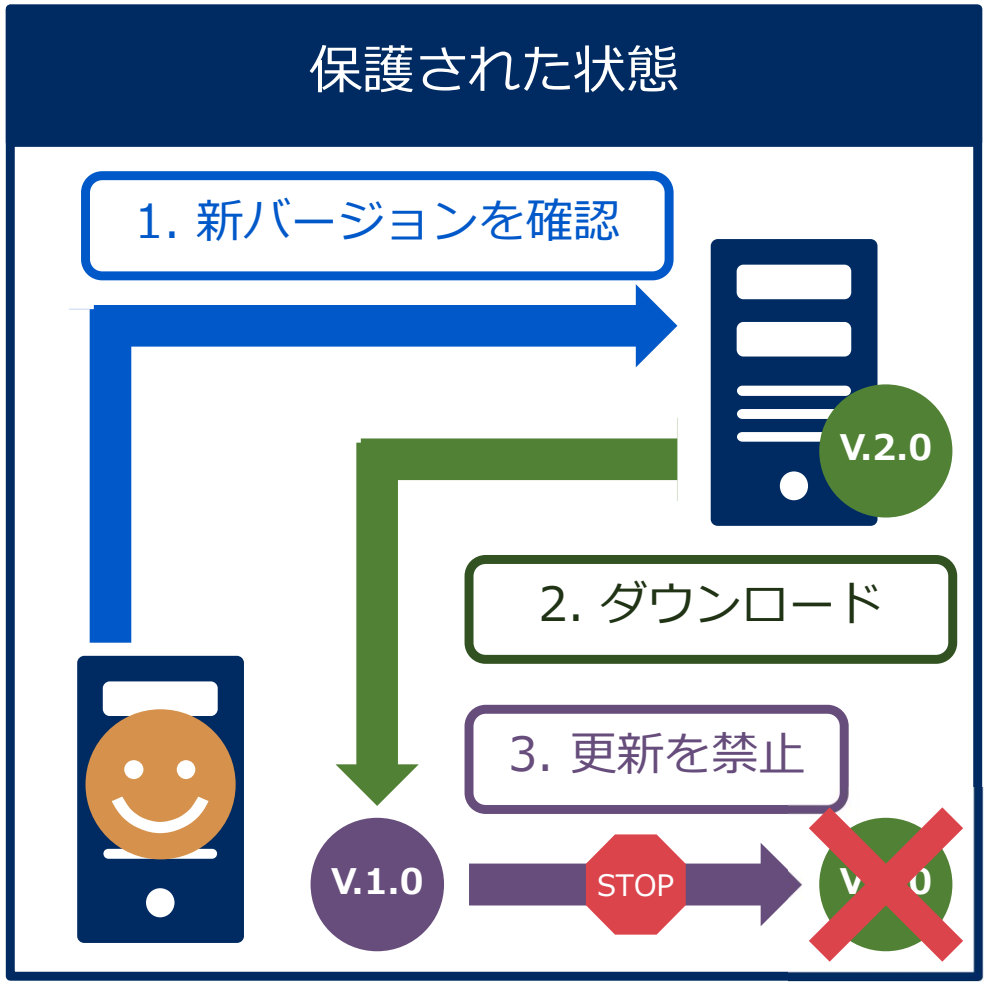


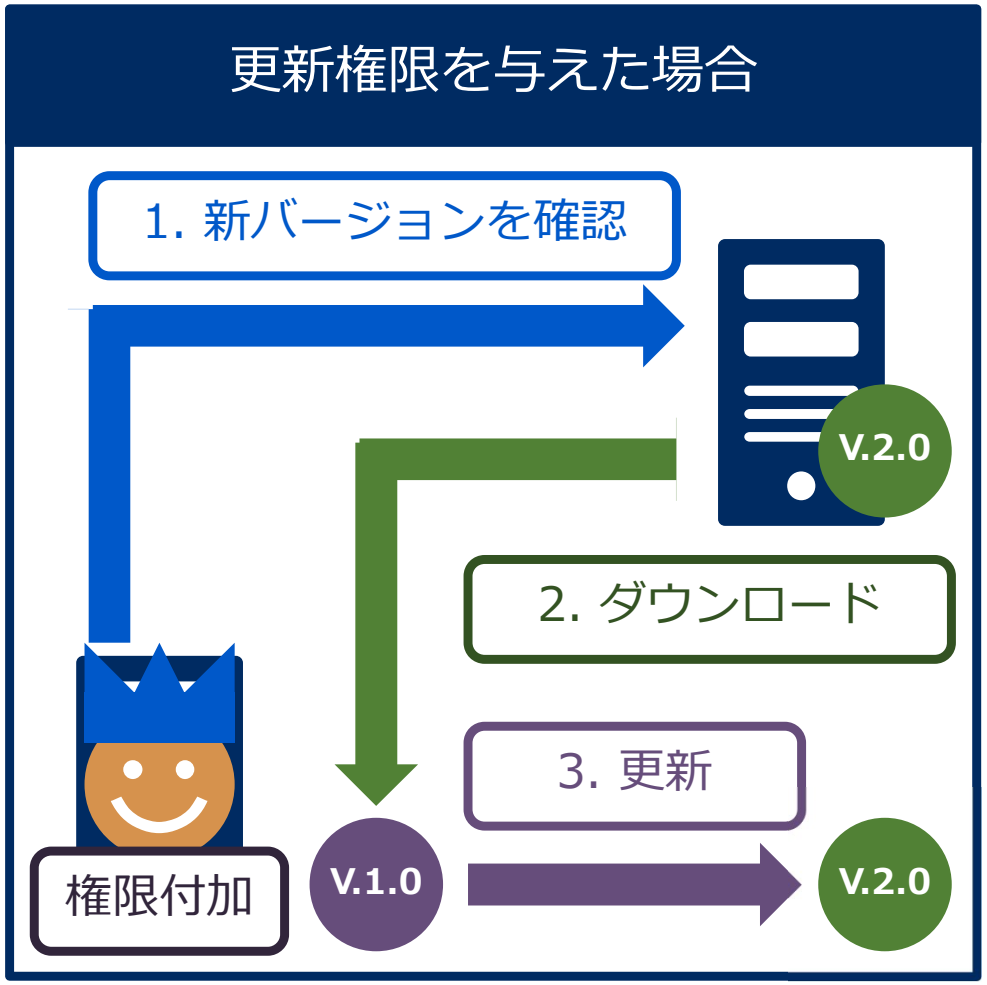
※ 更新作業中にウィルスが混入した場合、
ホワイトリストに登録されますので、
更新するファイルにはご注意ください

更新を行うプログラムに権限を付加

「更新を行うプログラム」に更新権限を与える

- 保護された状態での更新が可能
- sadmin updaters add ＜更新を行うプログラム＞





Trellix Application Controlのご紹介

Trellix Application Control　運用上の注意点

次のような実行ファイルは設定が必要

実行中に、自分自身や他の実行ファイルを書き換える

- ホワイトリストに登録されたファイルは書き換えが不可となります
- 自分自身や他のプログラムの書き換えを可能にするには、（保護されているファイルの書き換えを行う）実行ファイルに対して、下記の設定を行います

  sadmin updaters add ＜実行ファイル＞

ネットワークドライブから実行される

- ネットワークドライブは、ホワイトリストを作成することが出来ませんので、下記の設定を行います

  sadmin attr add –a ＜実行ファイル名＞

  もしくは

  sadmin trusted –i ＜実行ファイルが含まれるフォルダ＞

  ※ホワイトリストに登録された場合と異なり、実行ファイルは保護されません）

  ※trusted –i の場合、フォルダ内に存在する実行ファイルが全て実行可能となります

次のようなプログラムは設定が必要

メモリに直接アクセスする

- メモリ保護機能により、メモリに直接アクセスした際にうまく動作しない場合があります
- このような場合、下記の設定を行うことで回避可能です

  sadmin attr add –c <実行ファイル>　　※32bitの場合

  sadmin attr add –n <実行ファイル>　　※64bitの場合

ファイル、メモリに頻繁にアクセスする

- 1秒間に数千回のファイルオープン／クローズを行うなど、ファイルやメモリに頻繁にアクセスする場合にパフォーマンスに影響が出る場合があります
- ファイルに頻繁にアクセスする場合、下記の設定を行うことで回避可能です

  sadmin attr add –p <実行ファイル>
- ファイルに頻繁にアクセスする場合、下記の設定を行うことで回避可能です

  sadmin attr add –c <実行ファイル>　　※32bitの場合

  sadmin attr add –n <実行ファイル>　　※64bitの場合