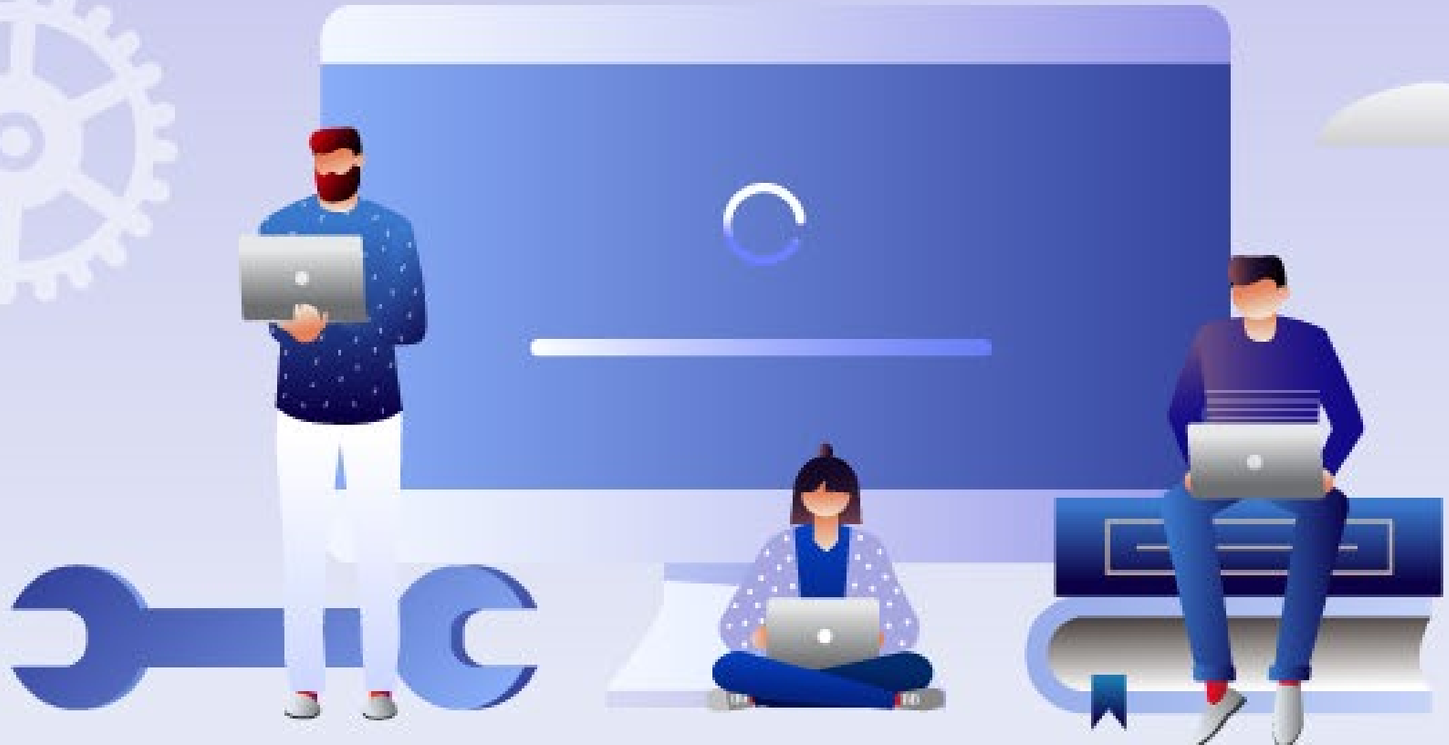
LANSCOPE
Endpoint Manager On-premises

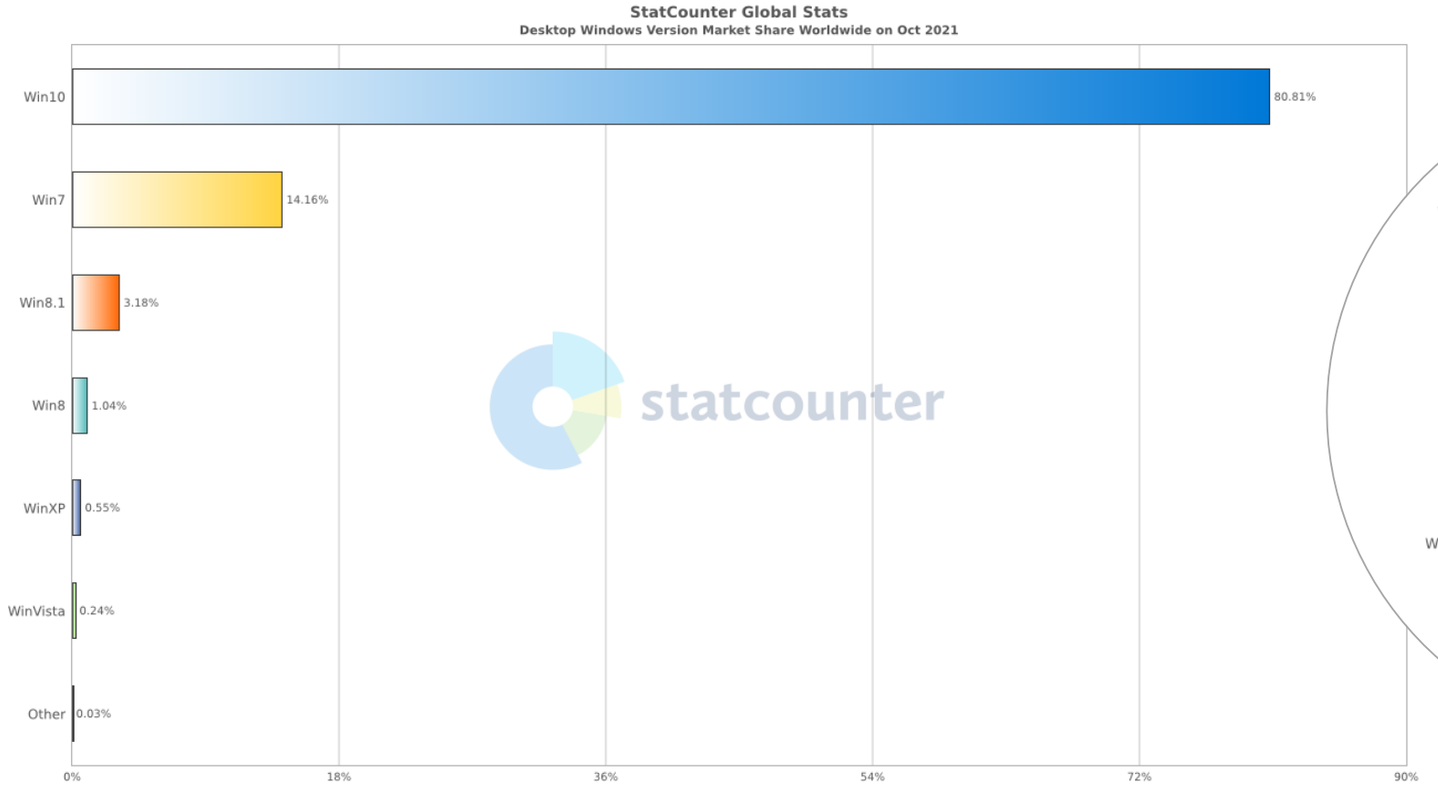
LANSCOPE
Cyber Protection

Windows 10管理のポイントと レガシーOSのセキュリティ対策

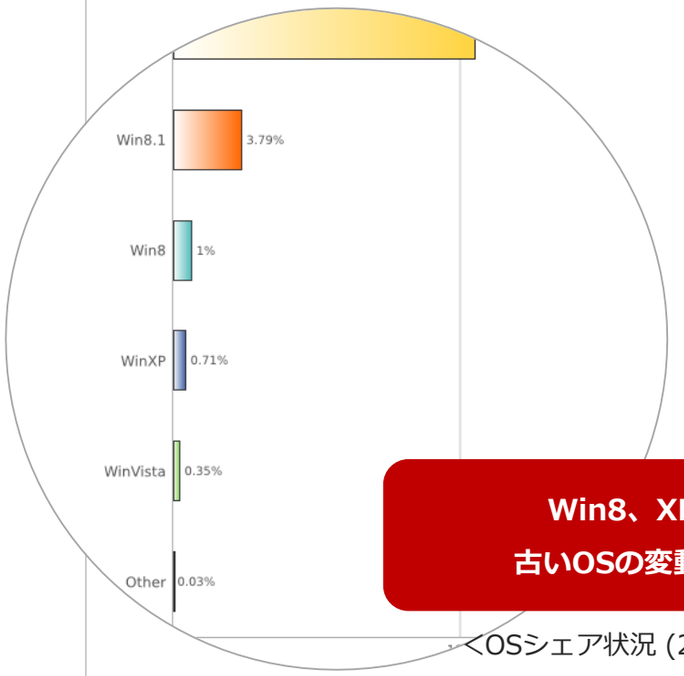


はじめに

2015年7月末のWindows 10一般公開してから約６年、Windows７のサポート期間も終了し、多くの方がWinows10へ移行しました。そして2021年10月にWinows11のリリースされました。Winows10は最終のバージョンと言われていましたが、昨今のPCを取り巻く様々な動向（セキュリティ強化が求められていることなど）を鑑みてアップデートに踏み切ったと考えられます。 StatCounterのWindowsバージョン別シェアデータ1月分によると８割がWinows10に移行済であることが分かります。一方でサポート期限が切れたWindows 7などのレガシーOSの利用は、数は減らしているものの、古いバージョンになればなるほど継続して使われていることが分かります。生産ラインへの組込みPCなどレガシーOSを使い続けなければないケースなどが考えられます。



＜　OSシェア状況 (2021年10月時点)　＞



＜OSシェア状況 (2020年10月時点) ＞

Win8、XPなどの
古いOSの変動は少ない

引用：Statcounter Global Stats
https://gs.statcounter.com/os-market-share

Windows 10
端末管理のポイント

WaaS（Windows as a Service）とは

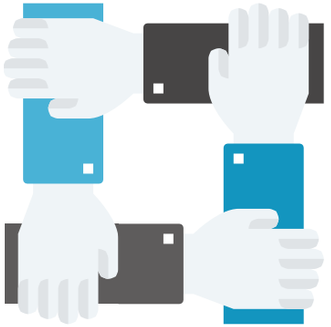
Windows 10 ではオペレーティングシステム（OS）のアップデート方針を Windows as a Service（WaaS）と呼ばれる形に大きく変更しました。WaaS の考え方は、これまでの Windows XP、Windows 7、Windows 8 といった数年に一度の大きなメジャーバージョンアップを廃止し、常に最新のWindows を提供し続けるサービスの形式になります。
この WaaS によるOSの提供は、常に最新のOSを無償で利用できるというメリットがある反面、情報システム部門は半年に1回提供される、最新のWindows 10 に対応した社内運用フローの整理と運用対応が必要となります。次ページ以降で、WaaS に対応する為のポイントを紹介していきます。

＜　WaaS での運用において把握すべき3ポイント　＞

Windows 10 からの新しいアップデート方式の理解とリリースタイミングの把握

Windows 10 の更新プログラムの理解と配信方法の把握

自組織における導入・運用フローの整理



Windowsのアップデート方式の理解とタイミングの把握

Windows 10では、サポート期間が最大30カ月で毎年2回の機能更新となっていました。エディション別に「上期」「下期」の更新がそれぞれ分かれていたのですが、Windows 11からサポート期間が変更され、双方とも年1回の更新となっています。Windows 10 Semi - Annual Channel（SAC、半期チャネル）といわれていた一般利用向けサービスチャネルも名称が変更され、General Availability Channel（GAC、一般提供チャネル）となっています。

Windows 10 エディション	上期更新	下期更新
Home/pro	18か月	18か月
Enterprise/Education	18か月	30か月

Windows 11 エディション	サポート期間
Home/pro	24か月
Enterprise/Education	36か月

本資料は、ビジネス向け（組織）のご紹介資料です

Windows 10の更新プログラムの理解と配信方法の把握

Windowsのアップデート方式、タイミングについて前ページで紹介しましたが、もう一つ押さえておくべきポイントとして配信されるアップデートの種類があります。Windowsで配信されるアップデートは大きく「機能更新プログラム（Feature Updates）」と「品質更新プログラム（Quality Updates）」の2種類に分類することができます。

機能更新プログラム（Feature Updates / FU）

OSのアップデートに相当しOS全体の機能強化・拡張を行う更新プログラムです。例えばスタートメニューやCortana、Edgeブラウザなどの機能追加・変更が含まれます。

リリースタイミング

Windows10は、年2回

Windows11は、年1回

サポート期間

リリースから18ヵ月間

品質更新プログラム（Quality Updates / QU）

従来の更新プログラムに相当するものになります。セキュリティ対策の更新を中心に過去にリリースされた更新を含む“累積更新プログラム”としてリリースされます。

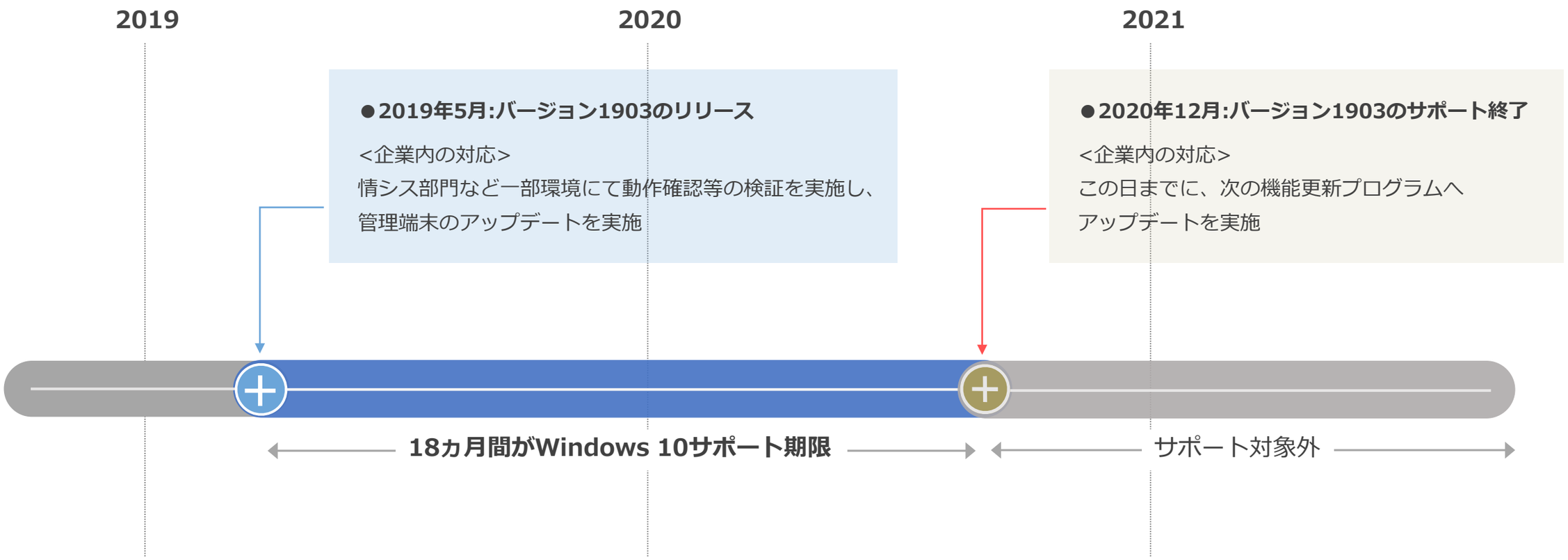
リリースタイミング

毎月1回提供されます。

（日本時間毎月第2OR第3水曜日）

自組織における導入・運用フローの整理

ここまで、Windowsのアップデートのタイミングと更新プログラムの種類を紹介しました。ここからは、実際に Windowsを社内で運用する場合に考慮すべき、Windowsのサポート期限と一般的な組織での導入・検証・運用フローを確認していきます。以下の図は2019年5月21日に配信された機能更新プログラム「Windws 10 バージョン1903」を例にサポート期限を表しています。2019年5月にリリースされたバージョン1903は約18か月間がサポート期間となるため、サポート期限の2020年12月までに次の機能更新プログラムを適用する必要があります。Windows11からは回数が1回減り、サポート期間が＋6か月となります。



自組織における導入・運用フローの整理

実際に組織の中で、Windowsの運用を行う上では、このWindowsの機能更新プログラムの適用計画が非常に重要となります。機能更新プログラムの適用計画は組織の管理体制やルールにもよりますが、大きく２つの計画が考えられます。

（例）Windows10におけるアップデートプラン

プラン	アップデート計画概要	実施タイミング	メリット	デメリット
プラン１	半年に1回の機能更新プログラムを常に組織内で適用する。	半年に1回	常に最新のWindows 10の利用ができ、新規に追加、強化された機能を使える。	半年に1回のOSアップデートに合わせた検証と展開、利用現場への説明など負担が増加。
プラン２	機能更新プログラムの適用を1回スキップし、1年に1回の周期で組織に適用する。	１年に1回	情報システム部門や利用組織の負担が年1回に軽減される	最新のWindows 10でリリースされる機能の利用が遅れる。

理想は常に最新の Windowsの利用が可能なプラン1ですが、実際の情報システム部門の検証にかかる負担や、アップデート後の操作の違い等による利用者の負担・混乱を考え、1年に1回 Windowsをアップデートするプラン2で計画されることが多いようです。また、プラン2の場合でも Windowsのセキュリティを強化する為の**品質更新プログラム（Quality Updates / QU）**を毎月適用することで、セキュリティ面の対策は可能です。

機能更新プログラムの計画案

Windowsの機能更新プログラムの適用を行う場合に必要な工程は大きく、 「更新に向けた情報収集、整理」 、「全体への展開に向けた準備・検証」、「組織全体への展開」の3つの工程が考えられます。

ステップ 1
更新に向けた情報収集・整理

●主な取り組み
- リリーススケジュールの確認と計画作成
- 更新機能の把握
- 展開手段の確認
- 展開対象の確認

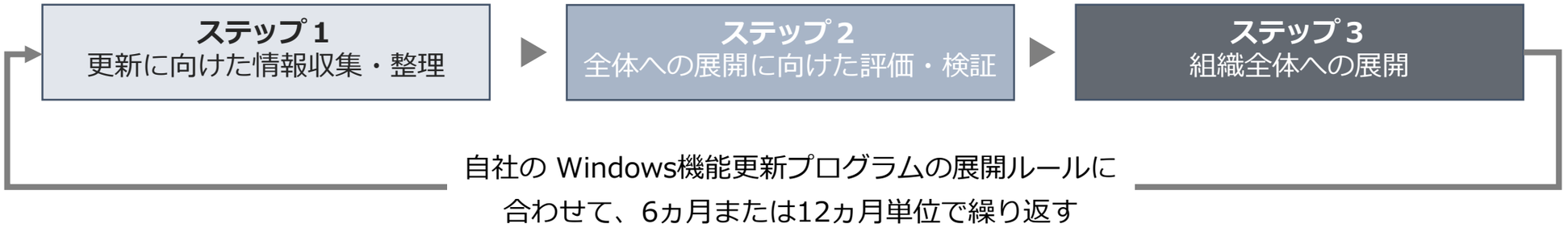
ステップ 2
全体への展開に向けた評価・検証

●主な取り組み
- ソフトウェア互換性確認
- ハードウェア互換性確認
- マニュアルなどの更新
- 展開手段の検証

ステップ 3
組織全体への展開

●主な取り組み
- 更新プログラムの展開
- 展開状況確認と追加対応
- 問合せ対応

Windowsの運用ではバージョンのサポート期限である18ヵ月の中で、この3つのステップを繰り返し行う必要があります。

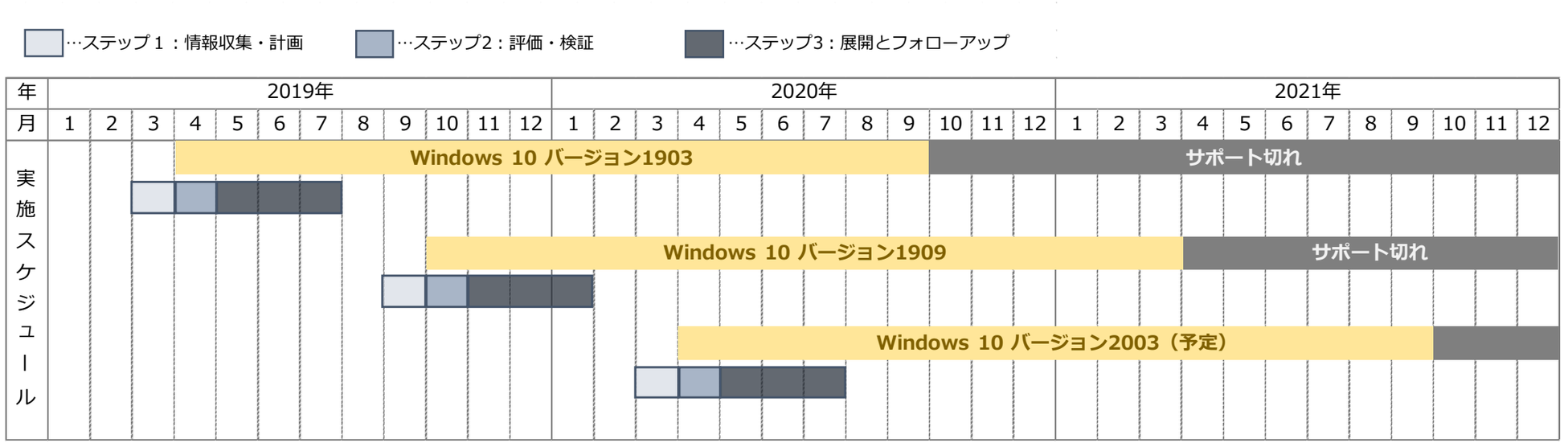


機能更新プログラムの計画案

機能更新プログラムを半年に1回、または1年に1回適用する場合に上記のステップ１～３を行った場合の参考計画です。

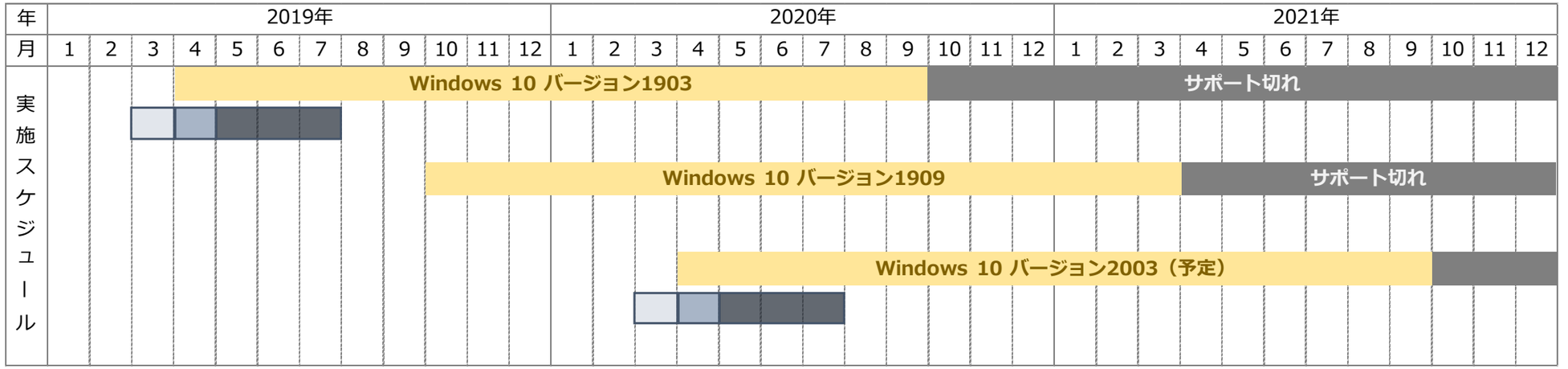
▶半年に1回

機能更新プログラムを適用する場合



▶ 1年に1回

機能更新プログラムを適用する場合



機能更新プログラムの配信方法

Windowsの機能更新プログラムを配信するには大きく3つの方法があり、それぞれメリット・デメリットが存在します。
WSUS を用いた方法がマイクロソフトの推奨となり一般的ですが、IT資産管理ツールにも Windowsのアップデート管理の機能を備えている、もしくは WSUS の運用を補助する機能を備えている製品が存在し、環境に合わせて使い分けることで Windows管理の効率を向上させることができます。

	Windows Update For Business	WSUS (Windows Server Update Services)	IT資産管理ツール
概要	インターネット経由の 自動更新サービス	Windows Server の 更新プログラム管理機能	ファイル配布機能などの データ配布・展開機能
費用	無償	無償	有償
サーバー	不要	WSUSサーバーが必要	管理用サーバーが必要
機能	更新プログラムの自動更新	更新プログラムの自動更新 更新プログラムの管理	更新プログラムの自動更新 更新プログラムの管理 資産管理,ログ管理など様々な情報収集
詳細	利用者が個別に適応する。 Windows 10 Pro エディション以上では、更新プログラムの受信タイミングを延期出来る機能を搭載。(WUfB)	管理者が更新プログラムを 管理し配信を行う	Lエンドポイントマネージャー オンプレミス版の場合、ファイル配布機能でFU,QUの配信を行う事ができ、WSUSとの連携も可能。マイクロソフト社製品以外のアップデートの配布も対応

エンドポイントマネージャー オンプレミス版で支援するWindows 10 アップデート管理

機能紹介とCASE STUDY

IT資産管理・情報漏洩対策・ウイルス対策を支援する統合型のエンドポイント管理ツール

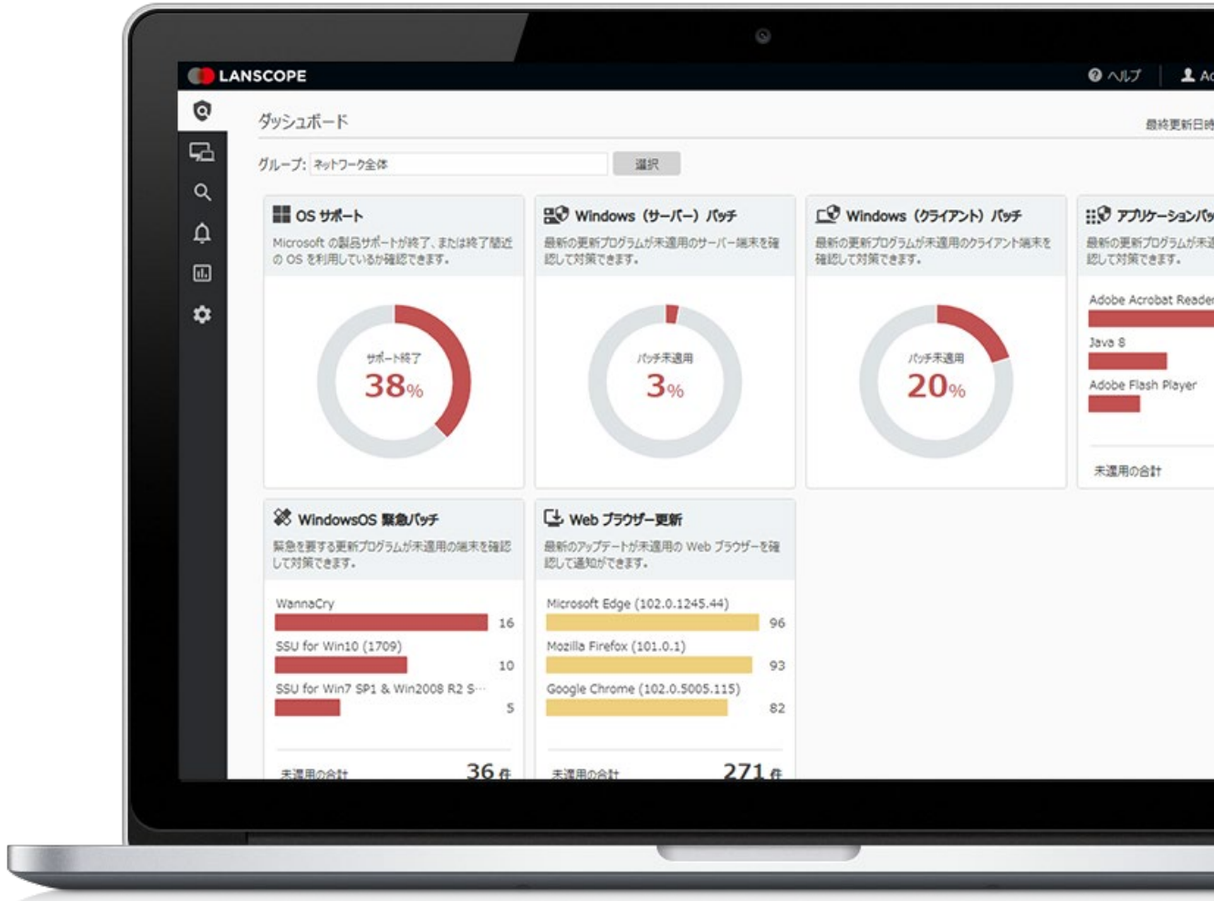
On-premises
LANSCOPE
Endpoint Manager

- IT資産管理・内部不正対策・外部脅威対策がワンストップで対応可能
- 国内のみならず海外端末も一元管理、VPN外でも管理が可能
- 必要な機能だけを選択して導入可能

IT資産管理 | **操作ログ管理** | **Webアクセス制御**

デバイス制御 | **マルウェア対策** | **リモートコントロール機能**

https://www.lanscope.jp/cat/



エンドポイントマネジャー オンプレミス版の対応範囲

Windowsのアップデート2種類のうち、エンドポイントマネジャー オンプレミス版は両方に対応しています。

機能更新プログラム（Feature Updates / FU）

OSのアップデートに相当しOS全体の機能強化・拡張を行う更新プログラムです。例えばスタートメニューやCortana、Edgeブラウザなどの機能追加・変更が含まれます。

リリースタイミング

Windows10は、年2回

Windows11は、年1回

サポート期間

リリースから18ヵ月間

品質更新プログラム（Quality Updates / QU）

従来の更新プログラムに相当するものになります。セキュリティ対策の更新を中心に過去にリリースされた更新を含む“累積更新プログラム”としてリリースされます。

リリースタイミング

毎月1回提供されます。

（日本時間毎月第2OR第3水曜日）

機能更新プログラムの配信方法

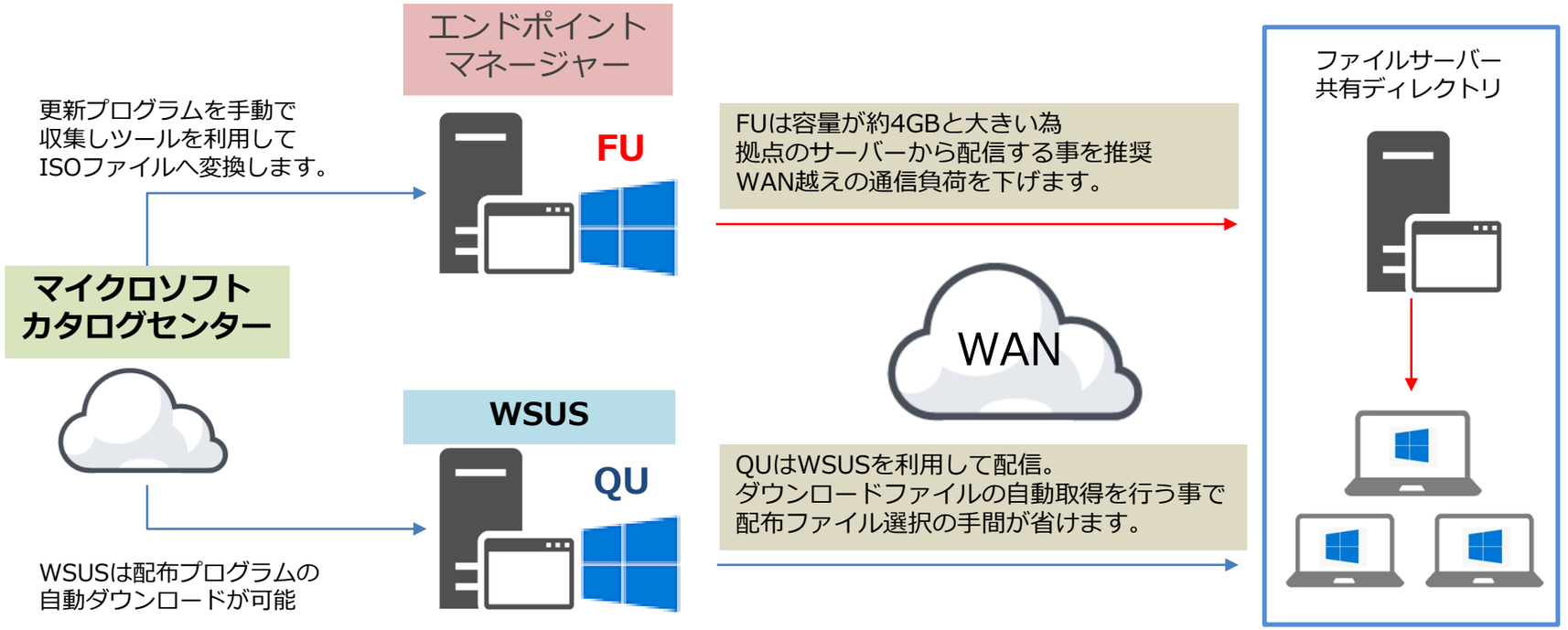
IT資産管理ツール「エンドポイントマネジャー オンプレミス版」と WSUS の機能の比較と、それぞれの利用メリットは以下の通りです。エンドポイントマネジャー オンプレミス版は WSUS にはない機能を備えており、WSUS と一緒に活用することで Windows 10 のアップデート管理をよりスムーズに行うことができます。

	WSUS		エンドポイントマネージャー オンプレミス版	
更新プログラムの入手方法	○	MSカタログセンターから自動取得	△	最新の更新プログラムの入手先URLを通知
配信対応製品	△	マイクロソフト社製品のみ対応	○	**マイクロソフト社製品以外の配信も可能**
最新配信プログラム情報の確認	○	WSUSの管理コンソールで確認	○	**エンドポイントマネージャー オンプレミス版の管理コンソールで確認可能**
負荷分散	△	拠点ごとにWSUSサーバー追加	○	**拠点にもともと存在する共有サーバーを活用可能**
配信先のグループ管理	△	ADのOU単位でグループを指定	○	**OUに依存しない エンドポイントマネージャー オンプレミス版独自のグループを指定して更新プログラムを配信可能**
配信時の通信帯域のコントロール	△	WSUSには機能が存在せず、ルーターで設定を変更する必要がある	○	**エンドポイントマネージャー オンプレミス版の機能でコントロール可能**
更新プログラムの配信タイミング	△	同時時間間隔で配信 （デフォルト22hごと）	○	**詳細な日時指定や、ユーザーが都合のよいタイミングを選択して配信可能**
常駐モジュール	○	無	×	有
サポート	△	スポット対応	○	**MOTEXコールセンターにて問い合わせ受付**
コスト	○	無償	×	有償

配信構成イメージ　FU,QU配信のベストプラクティス案

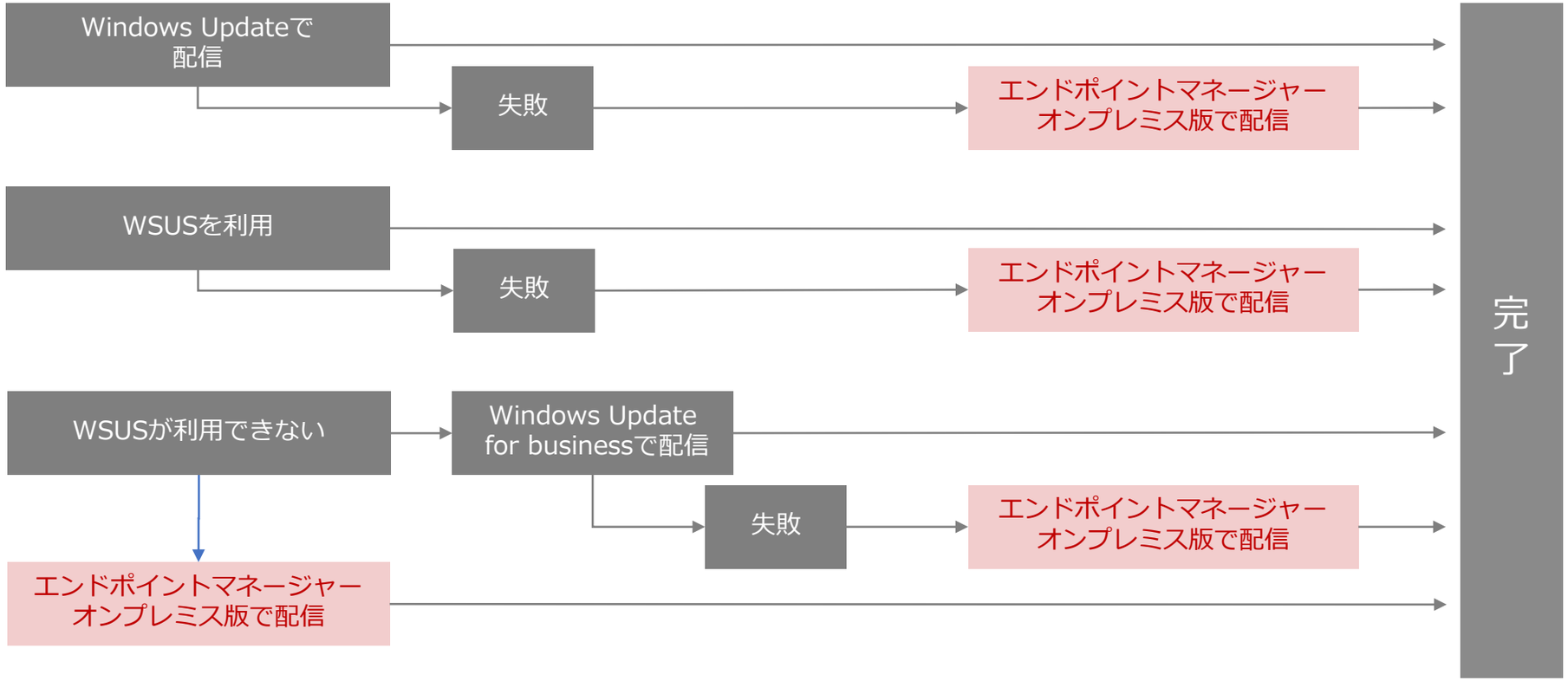
エンドポイントマネジャー オンプレミス版と WSUS を一緒に活用した Windows 10 のアップデート管理の一例です。

この例では、機能更新プログラム (FU) を エンドポイントマネジャー オンプレミス版で、品質更新プログラム (QU) を WSUS で配信します。FUは1ファイルの容量が4GB程度と大容量であるため、特に遠方の拠点に対してWANを超えて配信する場合、ネットワーク負荷を考慮する必要があります。エンドポイントマネジャー オンプレミス版は、拠点にもともとある共有ファイルサーバーなどを利用することで、拠点内でFUの配信を完結することができるため、FUの配信に便利です。一方で、QUは配信頻度が月に1回程度と頻繁で、1ファイル当たりの容量が1GB程度であるため、全拠点に対してWSUS から配信を行う方が効率的です。



WSUS と エンドポイントマネジャー オンプレミス版活用した更新プログラム配信フロー

エンドポイントマネジャー オンプレミス版単独でも、FU・QUを配信することができます。
既に WSUS を活用している場合は、WSUS による配信が失敗した端末へ エンドポイントマネジャー オンプレミス版で配信することで補完する運用も可能です。



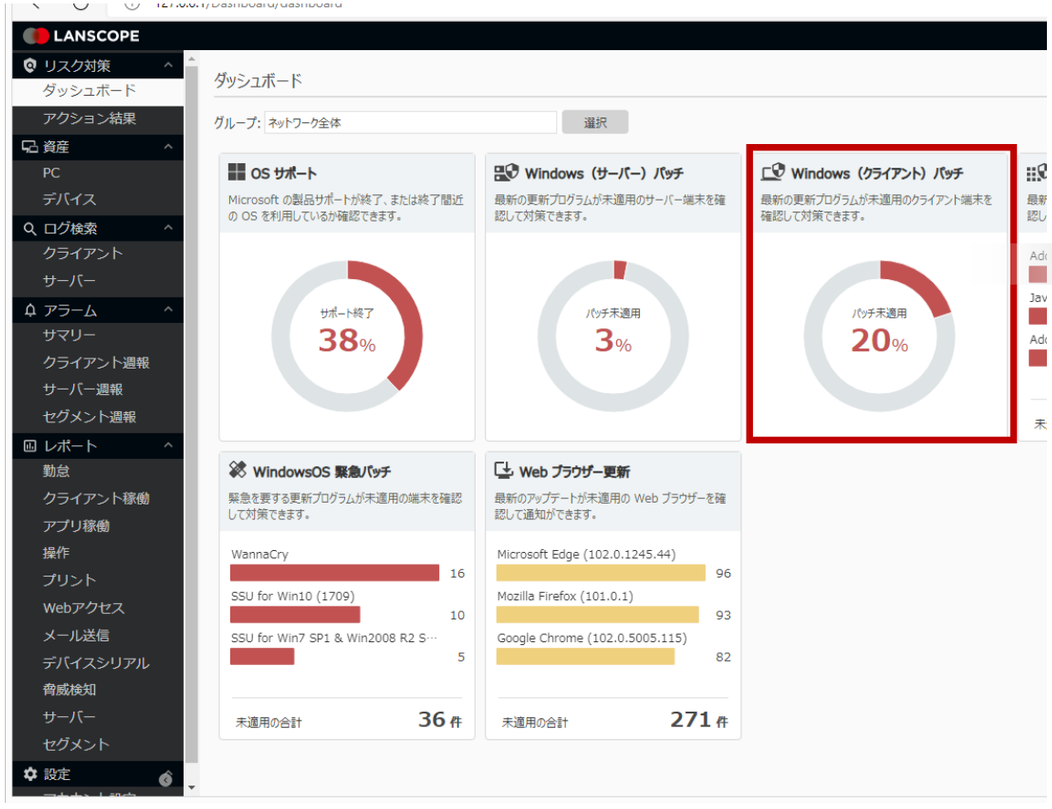
下記のような理由でWSUSが利用できない場合、エンドポイントマネジャー オンプレミス版を使った配信も可能です。

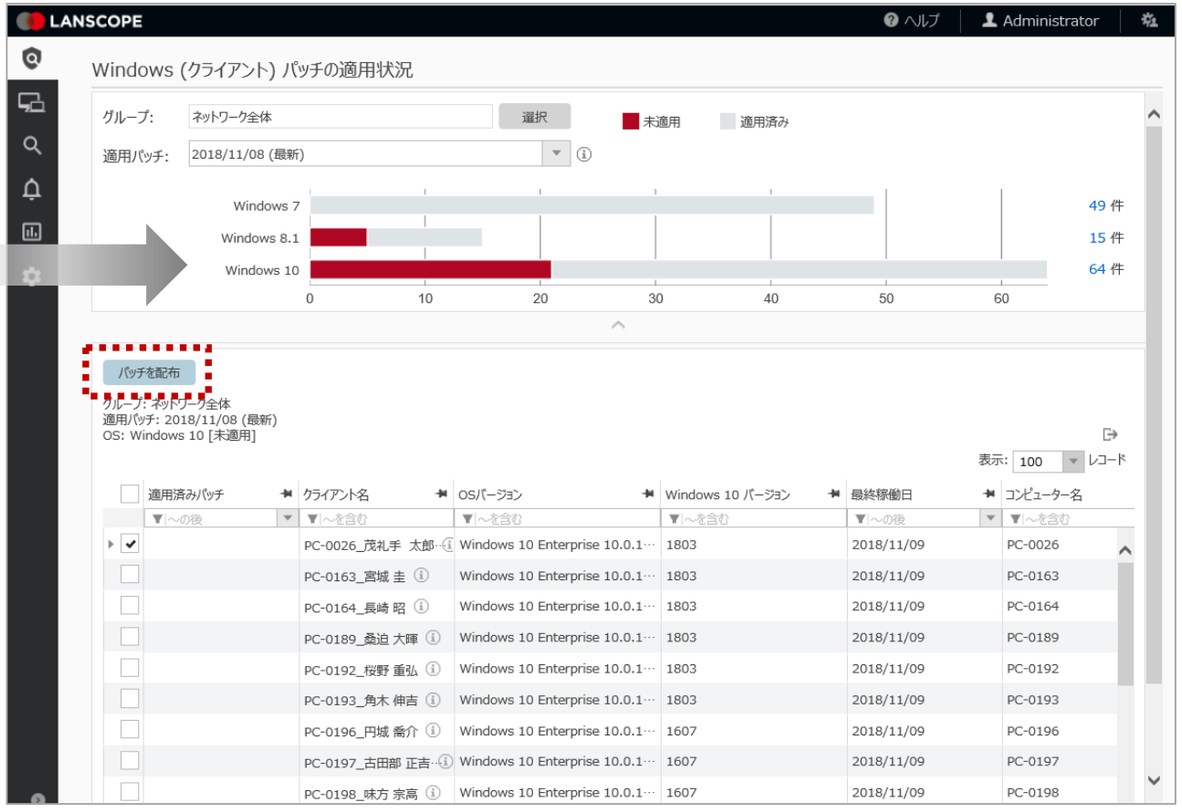
- 正しく配信されない場合や、失敗した原因が分からない
- OUを作っていない
- WSUSやグループポリシーの理解が難しい
- 管理画面が複雑で使えない

【参考】エンドポイントマネジャー オンプレミス版でWindows 10 運用管理画面イメージ：更新プログラムの適用状況の管理と配信

エンドポイントマネジャー オンプレミス版の管理画面では、マイクロソフトが提供する最新の更新プログラムと比較して、ネットワーク内のPCの更新プログラムの適用状況を分析できます。最新の更新プログラムが未適用のPCの割合を円グラフで表しており、気になるグラフをクリックすることで更新プログラムの提供状況の詳細を一覧で確認できます。さらに同じ1つの画面で、更新プログラムの配信までを4ステップで行うことができます。

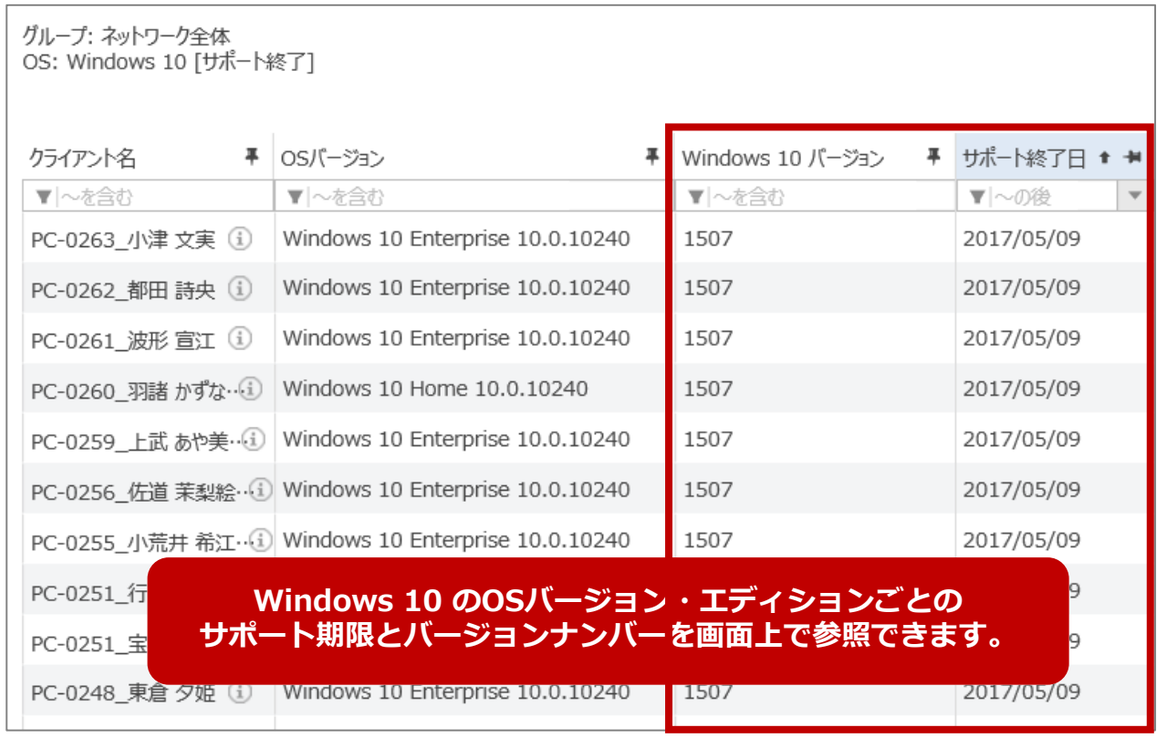
ステップ1 更新プログラム適用状況の確認　ステップ2 該当端末の把握　ステップ3 対策パッチ入手　ステップ4 対象端末に配布





【参考】エンドポイントマネジャー オンプレミス版でWindows 10 運用管理画面イメージ：詳細情報の確認

「OS分布状況」では、管理対象のPCで利用されている Windows 10 の詳細バージョンを確認できるだけでなく、エディション・バージョンごとに異なるOSのサポート期限まで確認することができます。また更新プログラムの配信を行う場合には、更新プログラムの入手先ページのURLまで案内し、エンドポイントマネジャーオンプレミス版の管理画面だけで Windows 10 の運用管理を完結できます。



▲「OS分布状況」の詳細画面

▲「パッチの配布設定」画面

もしアップデートが難しいレガシーOSがあれば…

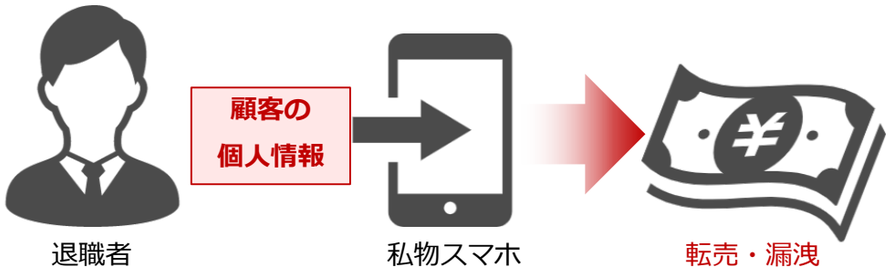
組み込みOS等の切り替えが困難なケース

内部不正による情報漏洩事例

従業員の内部不正による情報漏洩によって多額の損失を被るケースは後を絶ちません。2014年には某教育通信関連企業で、従業員が転売目的で自身のスマートフォンへ顧客の個人情報をコピーして漏洩した事件では、登録会員約2,900万件の個人情報が漏洩し、図書カードや電子マネーギフトによるお詫びを行ったことで、約136億円の赤字となりました。また2019年には、某スポーツ用品メーカーの元従業員が、ライバル企業への退職時に、社内サーバーに保管されていた製品の性能などの情報を記した約3万6千ものファイルを、自身の私用のメールアドレス宛に送信し持ち出したとして、不正競争防止法違反の疑いで逮捕されました。このような事態が発生すると、顧客や取引先への信頼が失墜するだけでなく、賠償金の支払いや営業活動営の影響により、企業の存続に致命的なダメージを与えることが考えられ、レガシーOSに対しても十分な対策が必要です。

某教育通信関連企業

従業員が転売目的で顧客の個人情報を私物スマホにコピー
登録会員約2,900万件の個人情報が漏洩



某スポーツ用品メーカー

退職者が転職先に製品の機密情報を持ち出し
転職先での活動に不正に役立てようとしていた

内部不正の最も効果的な対策は「PC操作ログの取得」

内部不正による情報漏洩への対策は、従業員が不正行為を行わないよう「操作証拠が残る」「操作が監視されている」環境を作り、心理的な抑止効果を働かせることが有効です。IPAが行った、「内部不正行為防止に効果が期待できる対策」のアンケート（複数回答）では、約半数以上の54.2%が「社内システム操作の証拠が残る」を効果が期待できる対策としてあげました。PC操作履歴を取得し、自身の操作が監視されているという意識を従業員に持たせることにより、自ら不正行為を行いにくくする抑止の環境を作ることができます。

従業員の内部不正の意識が低下する対策

順位	割合	内容
１位	**５４．２％**	**社内システムの操作の証拠が残る**
２位	３７．５％	顧客情報などの重要な情報にアクセスした人が監視される
３位	３６．２％	これまでに同僚が行ったルール違反が発覚し、処罰されたことがある
４位	３１．６％	社内システムにログインするためのIDやパスワードの管理を徹底する
４位	３１．４％	顧客情報などの重要な情報を持ち出した場合の罰則規定を強化する

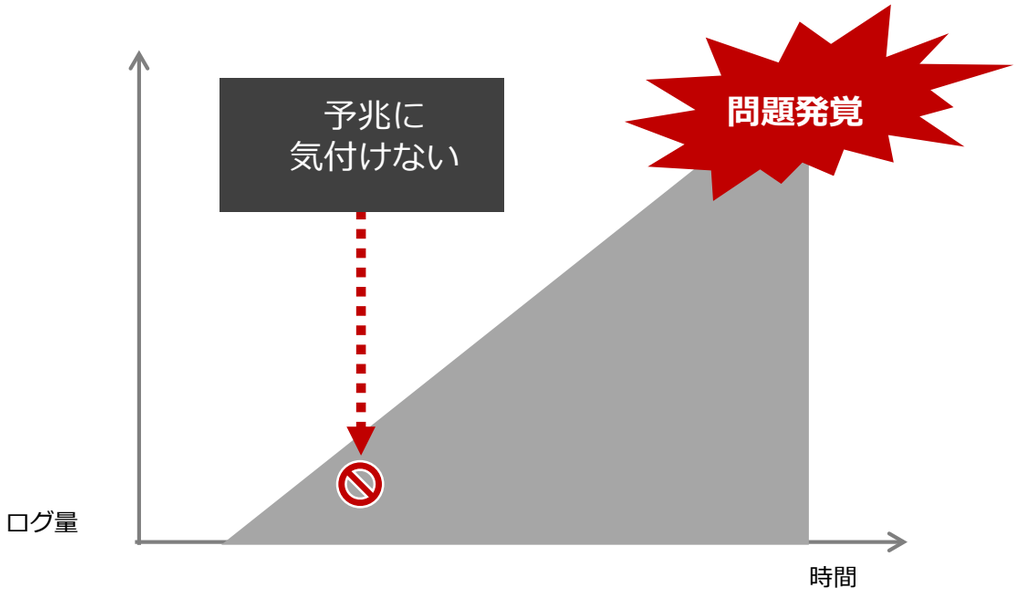
※１ 内部不正への気持ちが低下すると回答した回答者の割合。 （社員:n=3,000）情報処理推進機構（IPA）「組織内部者の不正行為によるインシデント調査」

定期的なログモニタリングの重要性

PC操作ログを取得していても、ただ保管しているだけでは、問題が発覚した後に後追いで原因を確認することはできますが、問題を未然に防ぐための対策とはなりません。社内ルールに違反する不正行為がないかを定期的に確認し、教育を行うことで、大きな問題に発展する前に問題行動を是正できます。PC操作ログを定期的にモニタリングをすることで、小さなルール違反や問題点を発見し、注意・是正することで、大きな問題の発生を防ぐことができるのです。操作ログ管理ツールの選定の際には、ただログを取得できるだけでなく、定期チェックがしやすい機能が備えられているかが重要です。

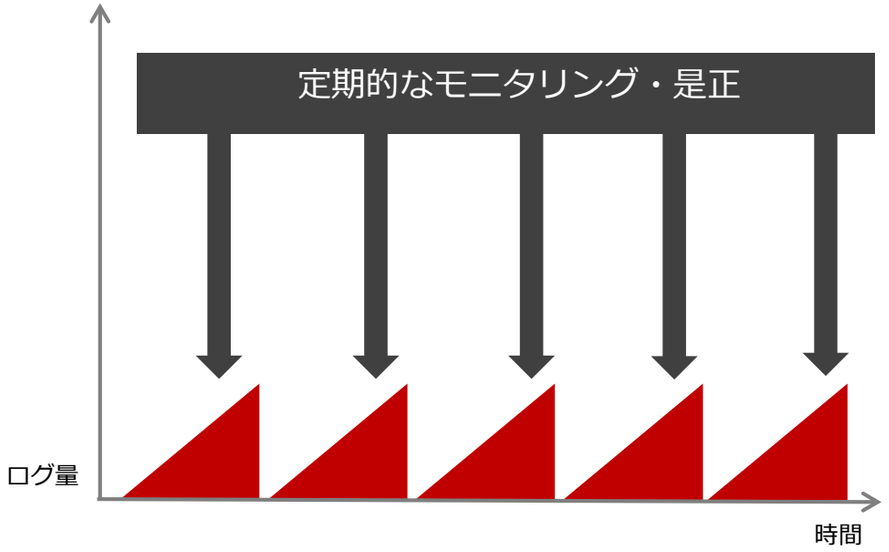
定期モニタリングをしていない場合

問題発覚後に原因を調査することはできても
問題の発生自体を防ぐことはできない



定期モニタリングをしている場合

小さなルール違反や問題点を発見・是正することで
問題の発生自体を防ぐことができる



エンドポイントマネジャー オンプレミス版で支援する操作ログ管理

証跡を取り負担なく定期チェック

事前のルール設定で不正操作を自動分析

エンドポイントマネジャー オンプレミス版の操作ログ管理機能では、あらかじめルール違反となる不正操作を「アラーム操作」として設定します。チェックボックスにチェックをつけるだけで簡単に設定ができる標準のアラーム設定のほか、より詳細にルール違反の条件を設定できるカスタムアラーム機能もご用意しています。「アラーム操作」に該当するPC操作が行われた場合には、エンドポイントマネジャー オンプレミス版が自動で分析し、次の３つのアクションを行います。

STEP1
「アラーム操作」の発生を管理者へ報告

STEP2
ネットワーク全体のセキュリティ度を分析

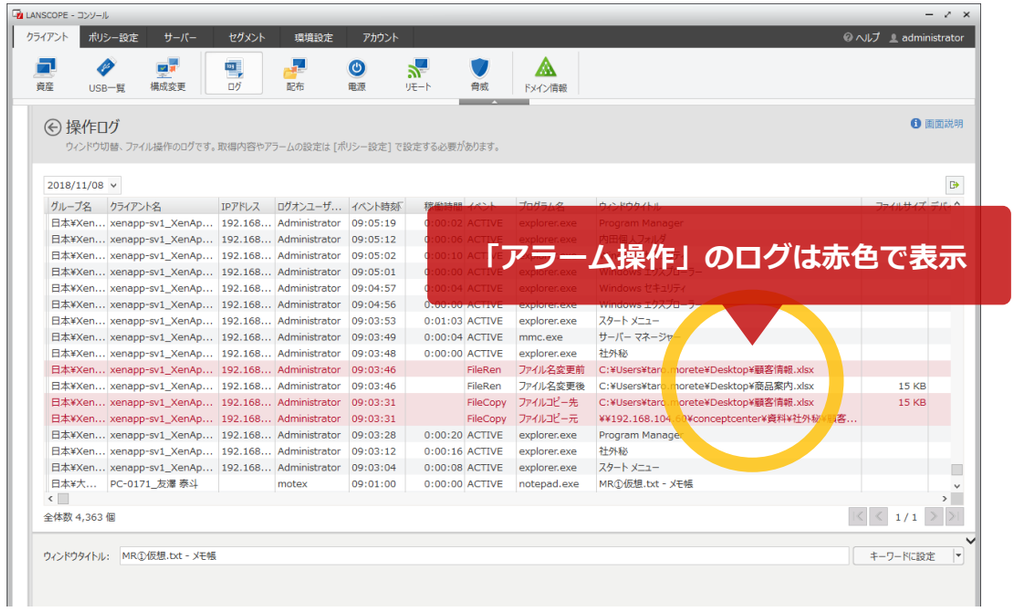
STEP3
利用者や責任者へリアルタイムに「アラーム操作」の発生を通知

▼標準のアラーム設定項目（一部）

カテゴリ	アラーム	ポリシー	項目	禁止
環境	資産	資産ポリシー	IP アドレスの重複・変更	−
			コンピューター名変更	−
			NIC・SCSI・モデムの変更	−
			DMI ハードウェア情報の変更	−
			CPU・メモリサイズの変更	−
			MAC アドレスの変更	−
			日時の変更	−
			リース切れ	−
			新規アプリのインストール	−
			HDD 容量不足	−
	アプリ起動	アプリ稼働ポリシー	新規アプリの起動	−
	アプリ禁止	アプリ禁止ポリシー	禁止アプリの起動・名前変更	○
			レジストリの変更（禁止設定時）	○
			アプリのインストール（禁止設定時）	○
			システム構成の変更（禁止設定時）	○
	通信デバイス	通信デバイスポリシー	不許可通信デバイスの接続	○
効率	時間外	操作ポリシー	業務時間外の操作	−
		サーバー監視ポリシー		−
		アプリID 監査ポリシー		−

カテゴリ	アラーム	ポリシー	項目	禁止
セキュリティ	操作	操作ポリシー	機密フォルダーの操作	−
			CSVの出力	−
			USBメモリなどの外部メディアへの書込み	−
			リモート PC への書込み	−
			ローカル共有フォルダーの作成または書込み	−
			ドライブの追加	−
			ウィンドタイトルアラームに抵触	−
			メールの添付	−
			指定した条件に抵触するファイルの操作	−
	プリント	プリントポリシー	印刷枚数の超過	−
			キーワードに抵触したドキュメントの印刷	−
	Web	Web アクセスポリシー	指定したキーワード・URL に抵触	○
			アップロード・ダウンロード	○
			Web への書込み・Webメールの送信	○
	ファイル操作	サーバー監視ポリシー	サーバーファイルの削除・アクセスの失敗	−
	接続失敗		サーバー接続の失敗	−
	不正接続	不正 PC 検知ポリシー	ネットワークへの不正な接続	−
	不正接続失敗		ネットワークへの不正な接続を禁止	○
	アプリ ID 監査	アプリ ID 監査ポリシー	アプリの ID の作成・削除	−
			不許可設定した PC での操作	−
			操作回数アラームに抵触	−
	メール送信	メールポリシー	キーワードに抵触したメールを送信	−
	脅威	−	マルウェアの検知	−

▼操作ログ取得イメージ



「アラーム操作」の発生を管理者へ報告

「アラーム操作」が発生したかどうかは、管理画面を一目見るだけでわかります。カレンダー形式の「クライアント週報」では、部署ごとに「アラーム操作」の発生状況を種別を示すアイコンと発生件数の数値で表示します。アイコンが表示されていない場合には、「アラーム操作」は1件も発生していない安全な状態ですので、対応は必要ありません。アイコンが表示されている場合には、アイコンをクリックするだけで「誰が」「いつ」「どのような違反操作をしたのか」を一覧で確認できます。面倒な検索操作が必要なく、簡単に状況把握が可能です。

ネットワーク全体のセキュリティ度を分析

「アラーム操作」の発生傾向をもとに、ネットワーク内のセキュリティ度を数値で表現します。PC操作ログの総数に対して、「アラーム操作」に該当する操作ログの割合を分析し、前週や前月に対して「アラーム操作」が増えているか減っているかを視覚的に表現することで、改善行動の成果を測定することができます。さらに「アラーム操作」の多い部門や人をランキング形式で報告し、ネットワーク内のどこに大きな問題があるのかを報告し、効率的に改善行動を行うことができます。

導入時

社内ルール設定・勉強会実施で
社員へ意識付け

1か月後

定期的にレポートを回覧し
適宜対策を実施

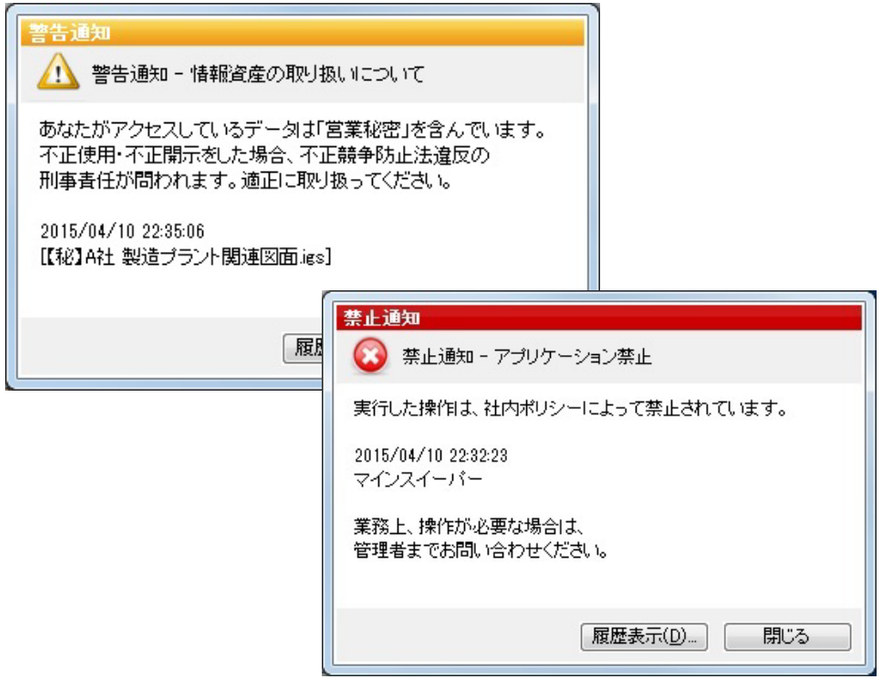
3か月後

前回とのレベル比較で
PDCAサイクル化

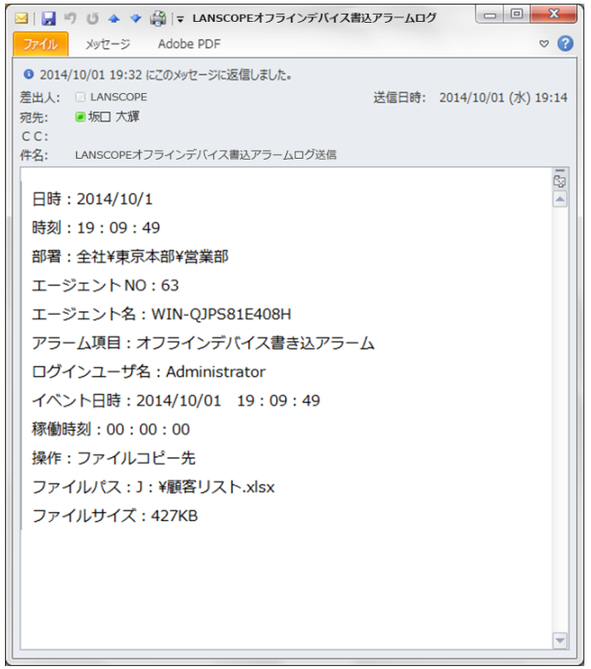
利用者や責任者へリアルタイムに「アラーム操作」の発生を通知

「アラーム操作」が発生した際にPCの利用者自身や上司・責任者に対してリアルタイムに通知を行うことができます。利用者の中には、それが知らずに違反操作を行う場合もあるため、リアルタイムに注意を促すことで、社内ルールの浸透につながります。また、リアルタイムに警告通知が表示されることで、PC操作が監視されている意識付けができ、不正行為を行いにくくする抑止の環境を作ることができます。また、利用者の上司などの責任者に対しても自動で「アラーム操作」の発生を通知することができ、監督責任を各部門責任者にゆだねることで、全社でセキュリティに取り組む環境を作ることができます。

違反者にはリタイムにポップアップ通知



責任者にはリアルタイムに詳細内容を通知

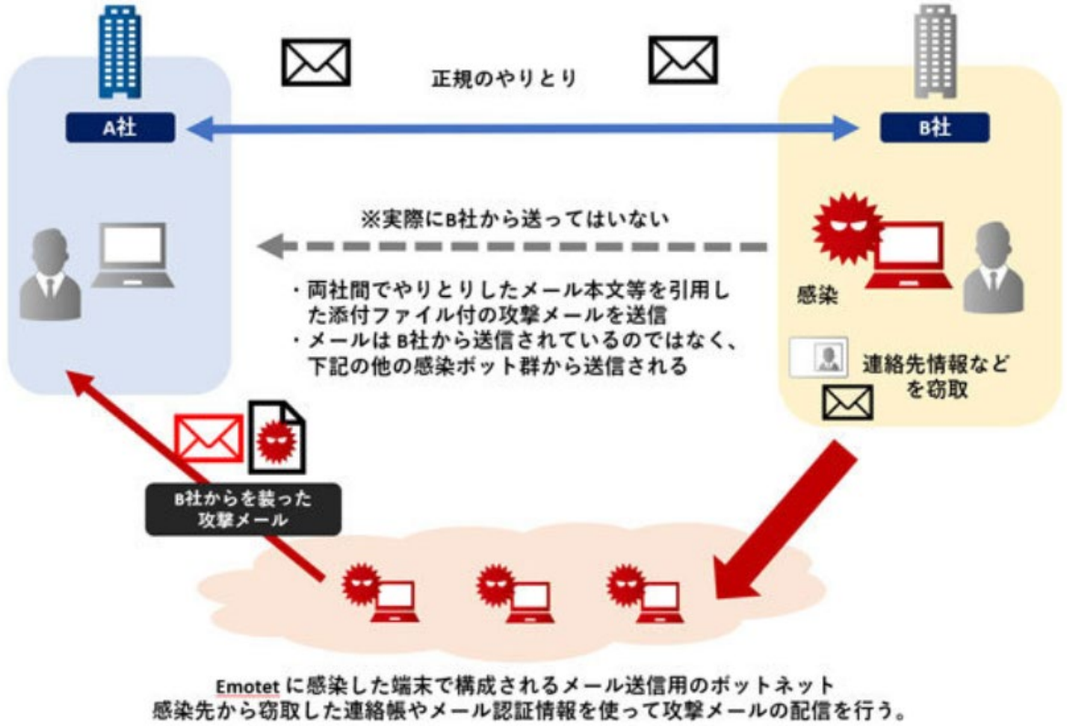


外部脅威対策

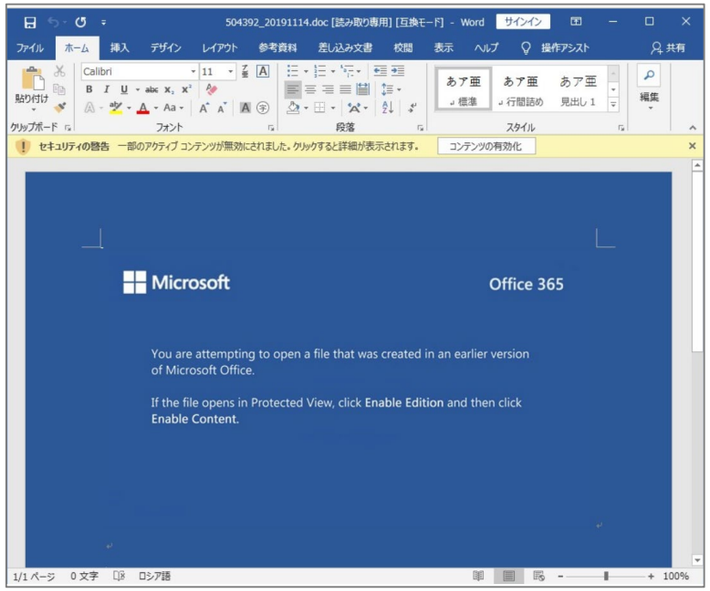
従来型のアンチウイルスでは防ぎきれなくなっている

国内で大流行のマルウェア Emotet (エモテット) とは

「Emotet（エモテット）」2014年ごろに欧州を中心に被害が出始めたマルウェアです。何度もバージョンアップが行われており、現在では他のマルウェアを引き寄せるダウンローダーとしての機能がメインとなっています。現在は、他のマルウェアのダウンローダーとして動作し、感染するとランサムウェアや情報窃取系の不正なモジュールがダウンロードされ、被害を受けます。JPCERTコーディネーションセンター によると、主にメールに添付された Word 形式のファイルを実行し、コンテンツの有効化を実行することで Emotet の感染に繋がることが分かっています。
Emotetは、感染させた端末のOutLookのメール情報を窃取する機能を備えています。もともとのメールに「re：」をつけて実際のメールの返信を装い、元のメールのスレッドに割り込む形でEmotetのダウンロードを誘導するメールを配信するという巧妙な手法で、被害が拡大しており、
JPCSIRTコーディネーションセンターは10月中旬からのわずか1ヶ月で400社から被害報告があったと報告しています。



▼ Emotetの感染メールに添付されるファイルのイメージ



出典：JPCERT/CC

Emotet の感染予防策

ここまで、国内で猛威を振るう Emotet について、その特徴と感染した場合の影響について解説してきました。
Emotet の特徴を踏まえると、対策のポイントとしては次の3点があげられます。

Emotet の特徴	対応策
メール添付したMicrosoft Word やExcel ※のマクロを利用してEmotet の本体ファイルをダウンロードし、感染する。	マクロの利用に対してセキュリティ製品で制御を行う。
情報窃取などの活動を行う際には、専用のモジュールをダウンロードし、メモリ上で動作させる。	メモリ上の不審な動作に対して対策ができるセキュリティ製品を活用する。
ワーム機能を有しており、ネットワーク内で自己増殖し、感染端末を増加させる。	境界型ではなくエンドポイントでのマルウェア対策（アンチウイルス）を強化する。

※2021年11月16日に確認された Emotet は攻撃に Excel も利用していることが報告されています。

また前提として基本的な対策が行われていることも非常に重要となります。
Emotet への対策の基本として、JPCERTコーディネーションセンターでも以下の対策を推奨しています。

●組織内への注意喚起の実施

マクロの自動実行の無効化（事前にセキュリティセンターのマクロの設定で「警告を表示してすべてのマクロを無効にする」を選択しておく）
メールセキュリティ製品の導入によるマルウェア付きメールの検知
メールの監査ログの有効化
OS に定期的にパッチを適用（SMB の脆弱性を突く感染拡大に対する対策）
定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）

出典：JPCERT/CC　マルウェア Emotet の感染拡大および新たな攻撃手法について（2020-09-04）　https://www.jpcert.or.jp/newsflash/2020090401.html

レガシーOS利用のリスク

マイクロソフト社のサポートが終了したOSをレガシーOSと呼びます。レガシーOSの利用には以下のリスクがあります。

- **Windowsの更新プログラムが提供されず、サポート終了後に発見されたOSの脆弱性が修正されない**
- **OSの脆弱性が修正されないため、脆弱性を悪用した攻撃の対象になりやすい**

ベライゾンジャパンが発表した「2015年度データ漏洩／侵害調査報告書」によると、サイバー攻撃に悪用された脆弱性の99.9%がCVE（共通脆弱性識別子）公開後1年以上経過した既知の脆弱性だったという指摘があり、レガシーOSを継続利用するとサイバー攻撃のリスクが大きく高まることを示しています。既知の脆弱性をつくマルウェアで大規模な被害が出た例としては、2017年5月に発生した「WannaCry（ワナクライ）」があります。WannaCryはデータを暗号化して身代金を要求するランサムウェアの一種です。脆弱性攻撃プログラム（エクスプロイトキット）である「エターナルブルー」を悪用していたことで知られます。なお、マイクロソフトは2017年3月にエターナルブルーに対する対策パッチを公開しており、パッチ適用ができていれば防御可能でした。

WannaCryの活動が沈静化した後も、Emotetなどの危険なマルウェアは続々と登場し、組織のセキュリティを脅かし続けています。対策パッチが提供されないレガシーOSを保護するためには、WannaCryのような危険なマルウェアが発生した場合でも確実に検知できる、高精度のアンチウイルスの導入が必要です。

某電機メーカー

2017年5月15日、WannaCryと見られるランサムウエアに社内システムの一部が感染。

国内外の一部の業務用PCで**メールを送受信できない**、**添付ファイルが開けない**といった障害が発生。

某小売業

2017年6月19日、複数店舗システムのコンピュータがマルウエアに感染し、外部に向けて大量のパケットを発信。

通信を圧迫して、**商品購入時のポイントサービスが利用できなくなった**。

某輸送用機器メーカー

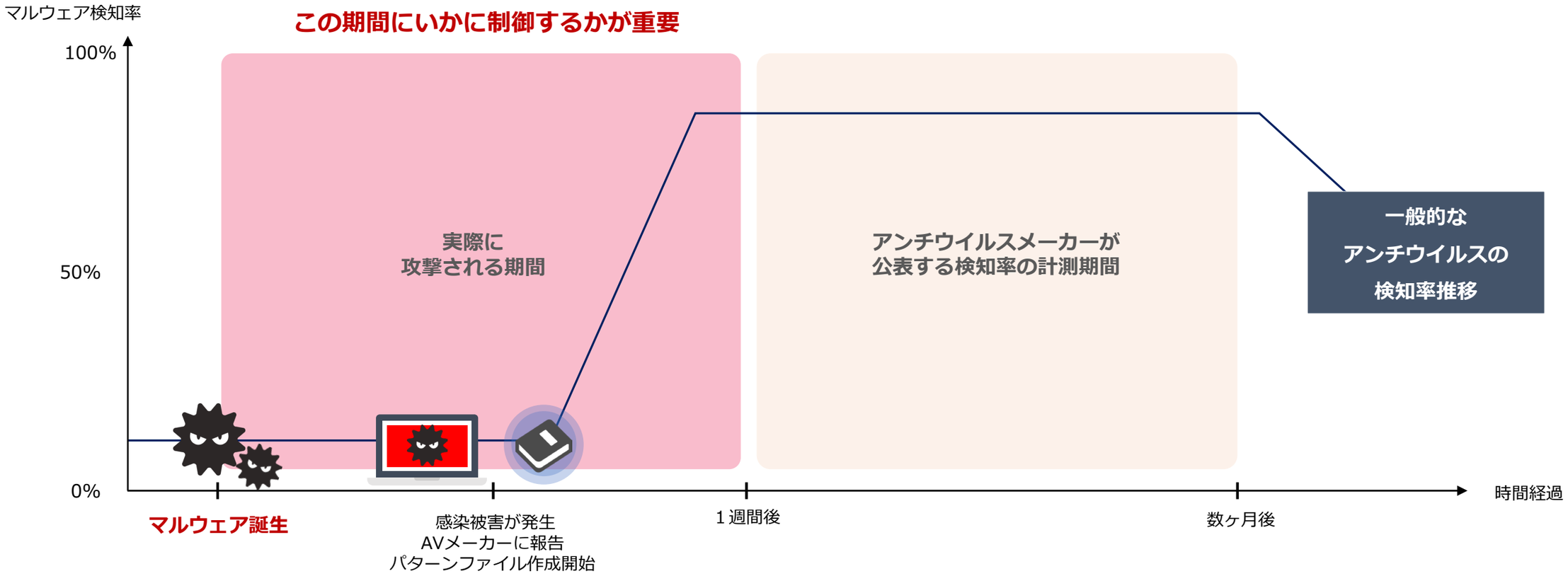
2017年6月21日、**工場など複数拠点でWannaCry感染。**

感染したのは工場設備に付帯するPC。生産ラインの管理などに使うものだったため**一部の生産に影響。**

アンチウイルス選びのポイント

セキュリティ対策として最も広く使われている従来型のアンチウイルスは、日々発見されるマルウェアをブラックリスト化してパターンファイルを更新しています。このアプローチの構造的な問題はゼロディと呼ばれる未知のマルウェアを止めることができないという点です。また仮にマルウェアが発見されたとしても、メーカーがそのファイルを入手し、パターンファイルを作成してエンドポイントに配信されるまでにはタイムラグがあります。攻撃者はこの構造的な欠陥を突くために頻繁にマルウェアコードを変更するようになり、結果的に最近のマルウェアのほとんどが従来のアンチウイルスをすり抜けるようになってしまいました。

シグネチャベースで未知のマルウェアを止めることが出来ないのは構造的な問題です。実際に攻撃に使われてる期間にマルウェアから防御できるかどうかが、アンチウイルス選びの一番のポイントです。



レガシーOSを守るCylancePROTECT

レガシーOSもエンドポイントで確実に守る

AI が未知・既知問わずマルウェアを隔離!
定義ファイルを使わないため、シグネチャ更新管理からも解放されます

CylancePROTECT®

マルウェア検知率99%

高性能な AI により
未知・既知問わず検知可能

毎日のアップデート不要

定義ファイルを使用しないため
毎日のアップデート不要

PC負荷が少ない

サイズは 150MB 以下、
CPU負荷 1% 以下

オフライン環境対応

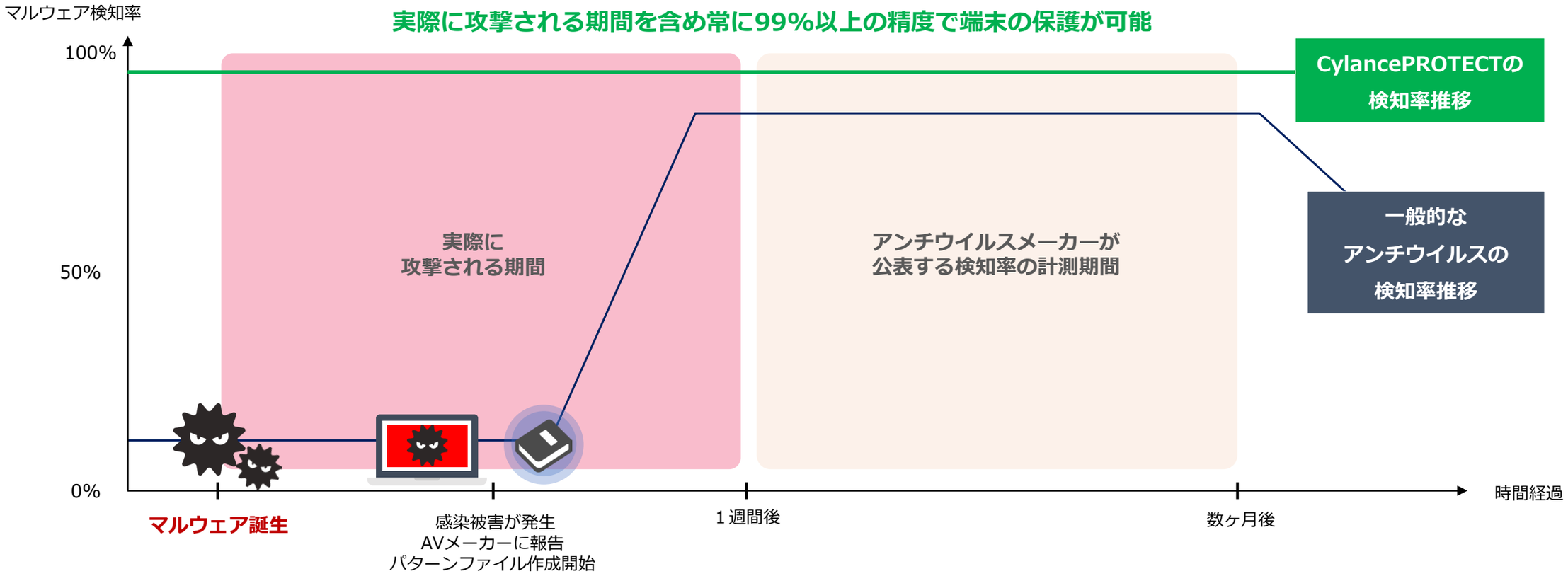
オフラインでも動作*

※インストール時にはインターネット接続が必要です

CylancePROTECTの場合

CylancePROTECTとは、AI技術の1分野であるディープラーニングを活用した次世代型アンチウイルスです。
AIに10億以上のファイルを学習させ、各ファイルから最大700万の特長を抽出して作成した「数理モデル」を検知エンジンとする画期的な手法で、亜種・変異型のマルウェアでも**99%以上**※の超高精度でマルウェアの検知・隔離が可能です。

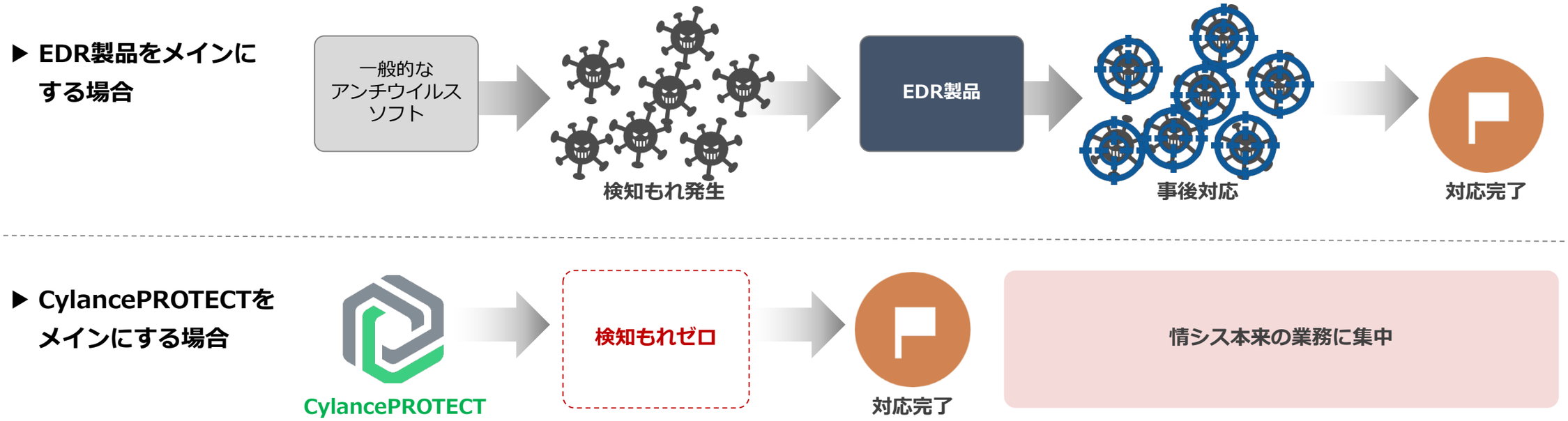
AI技術を活用した「予測脅威防御」で未知マルウェアも99%以上の超高精度で防御します。シグニチャレスの独自のマルウェア検知手法のため、パターンファイルの有無に左右されない検知精度で、一定の検知が可能です。



CylancePROTECTの特徴＝運用の手軽さ ～“アンチウイルスを入れておけば安心“を取り戻す～

CylancePROTECT導入の際に、よく比較検討されるのが、EDR（Endpoint Detection and Response）と呼ばれる製品です。EDRは、「アンチウイルスはマルウェア検知率が低い（マルウェア感染が避けられない）」ことを前提としたセキュリティソリューションです。エンドポイントを監視し、マルウェア感染の発生をいち早く発見して、封じ込めからフォレンジック分析まで行える専門的なツールで、効果的な運用には、収集した様々な情報を分析できるアナリストが必要となります。EDRは、もちろんマルウェア対策に有効です。しかしその一方で、EDRで対処しなければならない頻度が高いと、対応する担当者の工数が大きく割かれ、運用がマンパワーに依存するという課題があります。仮に100個のマルウェアが社内ネットワークに侵入したとして、そのうち10%しかアンチウイルスで感染を防ぐことができない場合、残り90個分のマルウェアに対してはEDRを活用し、感染後の対策を行わなければなりません。

これに対してCylancePROTECTの場合には、AI技術によりマルウェア感染をほぼ100%防ぐことができ、マルウェア感染後の対応をしなければならないケース自体がほぼゼロとなります。マルウェア対策はCylancePROTECTに任せて、情報システム部門本来の業務に集中することができます。



On-premises
LANSCOPE
Endpoint Manager

体験版
お試し限定

今だけ
レポートサービス
実施中

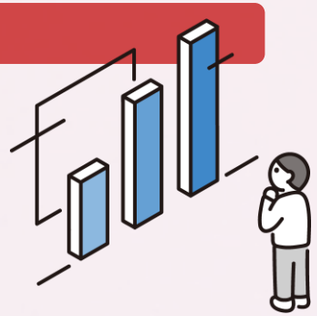
1ヶ月間 無料体験キャンペーン中

インストールから31日間、エンドポイントマネージャー オンプレミス版の全機能利用可能な体験版をご用意しています。体験版は**お手軽な「クラウド環境」**と**「オンプレ版」**の2種類をご用意。最大50台まで管理いただけますので、是非この機会にお気軽にお試しください！

さらに今だけレポート提供、加えて本格的に導入検討方にはメーカーSEによるレポートを用いた運用レクチャーサポートを実施中です。（※申込フォームにてエントリーしてください）

＋ レポートサービス

５台以上に展開・検証の方には
体験版終了後にレポート提供



＋ レクチャーサービス

100L以上で導入検討されている方は
運用フォロー×レポート提供

https://go.pardot.com/l/320351/2017-06-20/c4vz?re

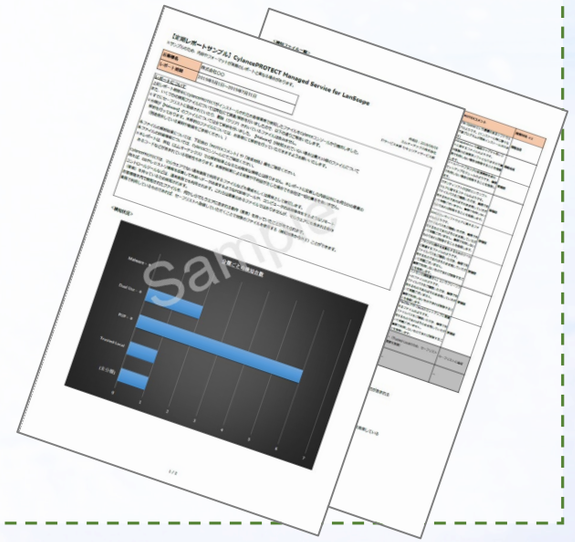
CylancePROTECT

AIアンチウイルス無料体験実施中

～CylancePROTECTを気軽に使ってみよう～

最新AIを活用した新技術で超高精度の検知率を誇る「CylancePROTECT」を**1ヶ月無料**で**何台でも体験**できるキャンペーンがスタートしました。実際に自社のPCにCylancePROTECTをインストールし、コンソールの操作方法や検知力の高さを体験いただけます。

体験終了後、エムオーテックスにて**検知結果のサマリーレポートをご提供**します。AIを活用した最新鋭のアンチウイルス製品を、この機会にお気軽にご体験ください！



●お申し込みはこちらから

https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr?tech06

製品に関するお問い合わせ

■ 営業本部

大阪本社　06-6308-8980

東京本部　03-5460-0775

名古屋支店　052-253-7346

九州営業所　092-419-2390

E-mail　sales@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター　0120-968995 （携帯・PHSからは06-6308-8981）

お電話受付時間　9:30～12:00/13:00～17:30（平日、祝祭日除く）

Email お問い合わせ　support@motex.co.jp