HP Sure Click Enterpriseご紹介資料

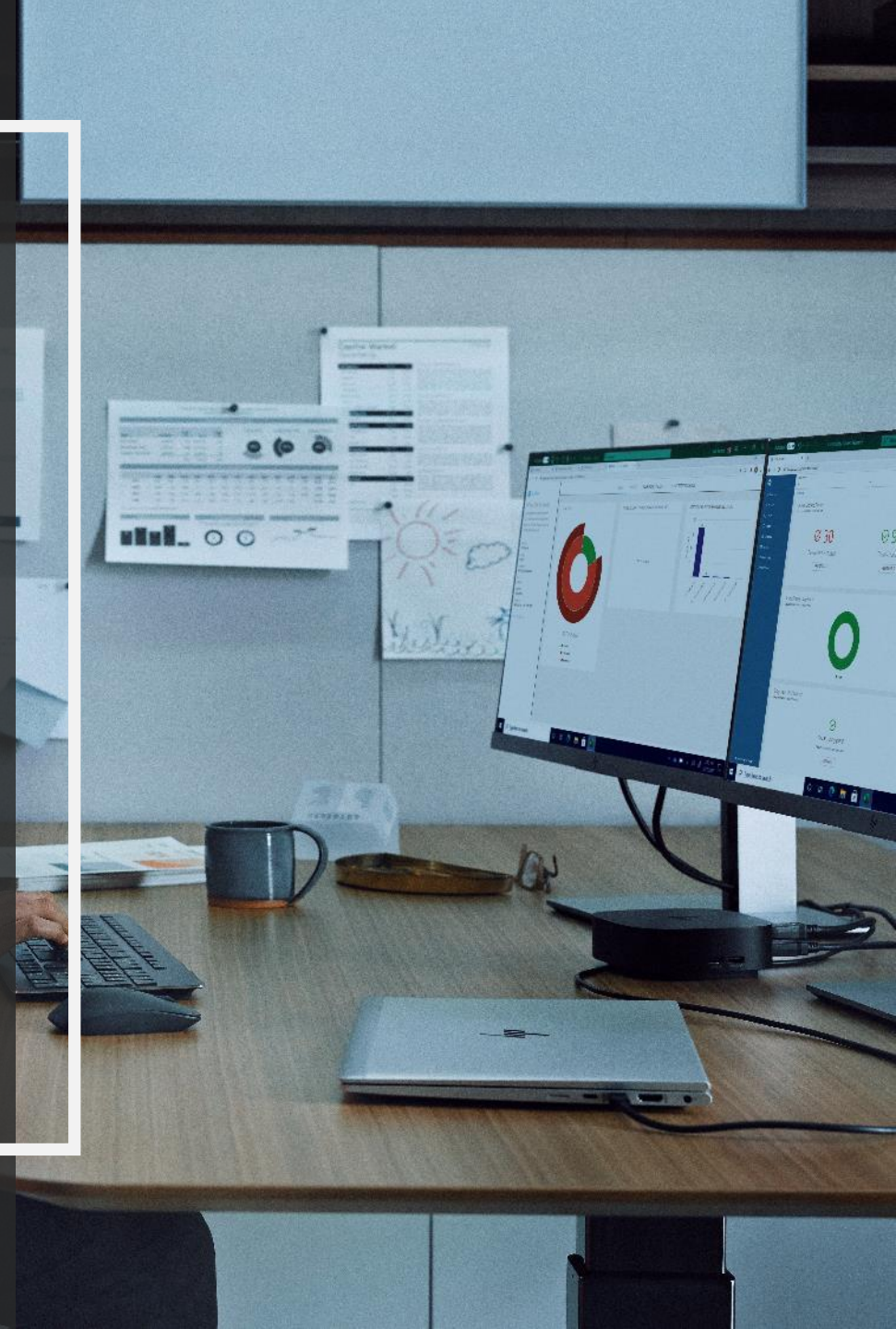
HP WOLF SECURITY

株式会社 日本HP
サービス・ソリューション事業本部

HP WOLF SECURITY

アジェンダ

- エンドポイントセキュリティの重要性
- HP Sure Click Enterpriseの特長



米最大の石油パイプラインの停止

ランサムウェア攻撃の侵入ルート

①メールに記載されたリンクや添付ファイル
②Webサイト
③USBメモリなど外部ストレージ

モダンなサイバー攻撃は人間の脆弱性を狙う

94%

マルウェア感染の中でEメールの添付ファイルに起因する割合[1]

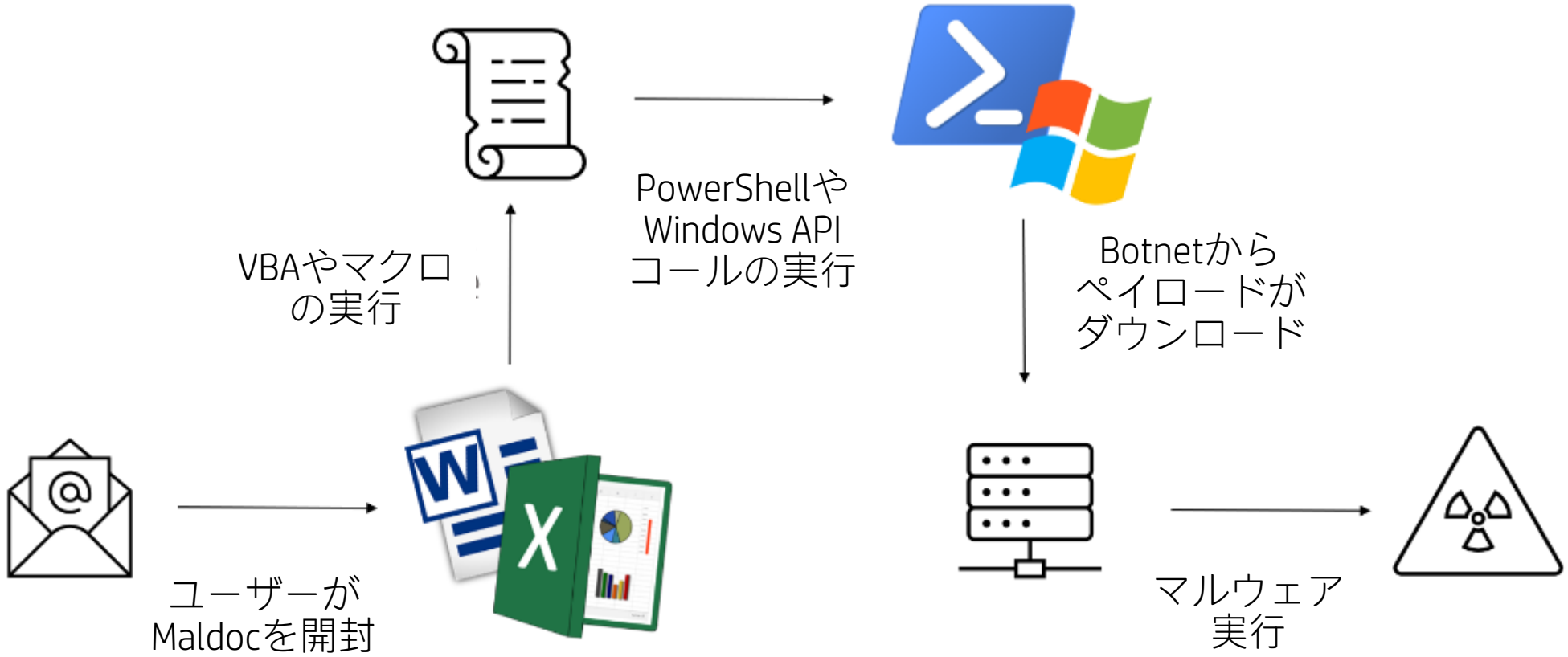
57%

アンチウィルスが見逃したエンドポイント攻撃の割合[2]

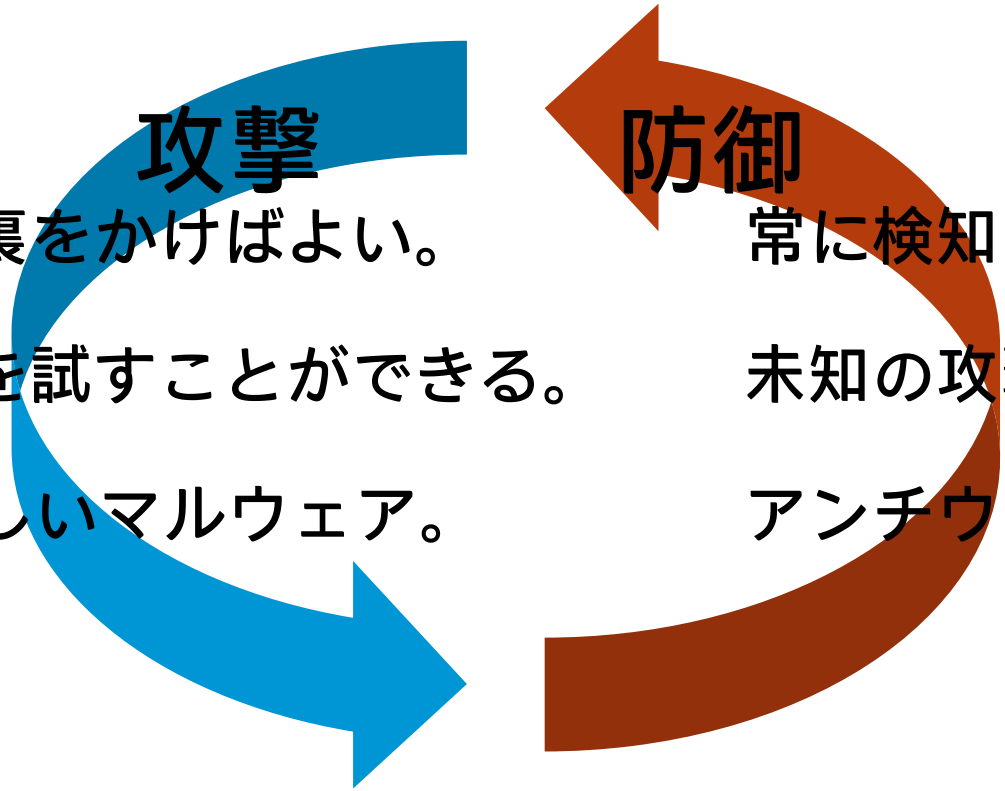
Source: [1] 2018 Data Breach Investigations report 11th Edition, Verizon, 2018; [2] Ponemon Institute 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018

セキュリティポリシーとアンチウイルスだけでは十分ではありません。
組織は追加の防衛線を必要としています。

階層防御の迂回を前提としたサイバー攻撃シナリオ



サイバーセキュリティにおける検知の問題点



攻撃

一度だけ検知の裏をかけばよい。

市販の防御製品を試すことができる。

一日35万個の新しいマルウェア。

防御

常に検知を成功させる必要がある。

未知の攻撃を試すことはできない。

アンチウイルスの成功率57%。

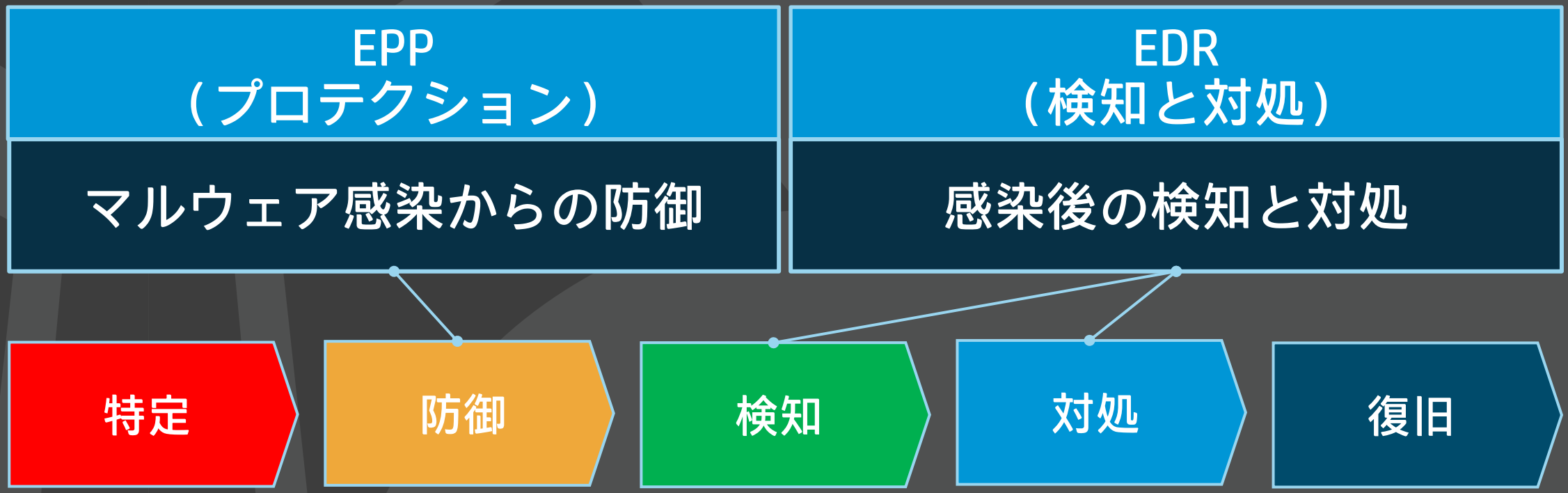
ゼロデイ攻撃への対策が本質的に難しい

HP WOLF SECURITY

HP Sure Click Enterpriseの特長

HP WOLF SECURITY

エンドポイントセキュリティ：EPPとEDR



? 防御が不十分なまま、EDR導入とSOC運用
× 行き過ぎた防御と生産性のトレードオフ（目的はビジネスを成長させることだが・・）

HP WOLF SECURITY

HPのプロテクション・ファースト・アプローチ

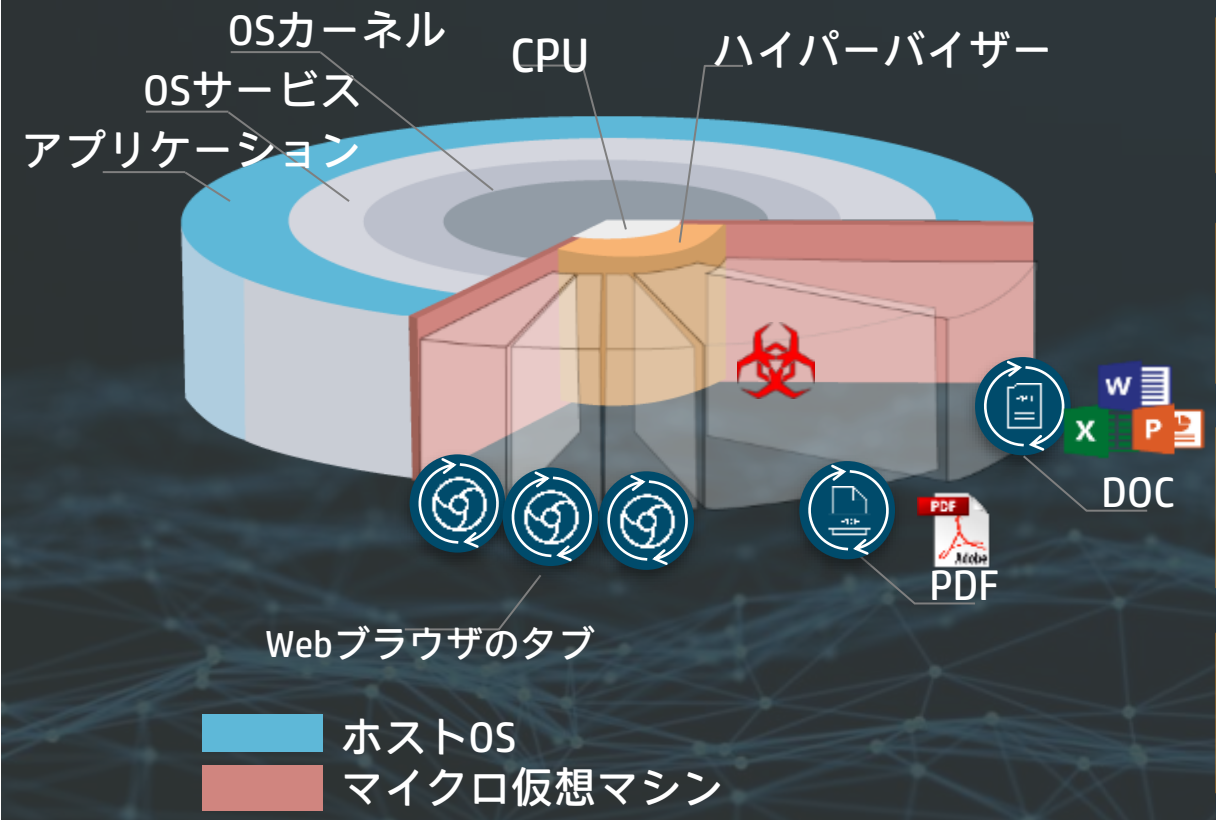
HP Sure Click Enterprise

プロテクションを強化しながら、安全に検知、シンプルな対処

特定	防御	検知	対処	復旧
	主要な攻撃経路に対する完全な隔離保護	隔離環境の中で安全に検知	隔離済の環境で一時対処がその場で完了 Black List登録で横展開阻止	

HP Sure Click Enterprise

テクノロジースタックビュー



最新のWindows PCで利用可能なCPUハードウェアで強化する仮想化技術(Intel VT/AMD-V)を使用しています。

マイクロ仮想マシン（マイクロVM）をミリ秒単位で生成し、ホストOSから完全に隔離してOSやアプリケーションのインスタンスを実行します。

電子メール添付ファイルやWebダウンロードを開く、リンクのクリックなど、リスクの高いタスクごとに新しいVMを生成します。

ユーザーエクスペリエンスは変わりませんが、マルウェアは無害化されます。何も盗めない; 横展開できない; 永続化できない。

HP Sure Click Enterpriseの保護領域

エンドポイントのアタックサーフェスを9割以上減らす

Eメール 添付/ チャットアプリ/ USBメモリ	共有 リンク	ファイル ダウンロード
悪意のあるEメール に対する保護	**悪意のあるリンク に対する保護**	**悪意のあるダウンロード に対する保護**
ランサムウェア マクロを悪用したトロイの木馬 ファイルレスマルウェア 悪意のあるリンク	Eメール内の悪意のあるリンク ブラウザーエクスプロイト 偽のFlash/Javaアップデート 悪意のある広告 Skype内のリンク	意図的なダウンロード 実行可能ファイルの 偽造アップデート ドキュメントへのリンク 不正なDNS/URLリダイレクト 偽のドライバとユーティリティ

HP Sure Click Enterpriseの保護対象

	カテゴリ	対象
Micro-VMで実行可能なアプリ	ブラウザ	Internet Explorer / HP Sure Click Secure Browser(Chromium) / Firefox(特定バージョンのみ)
	オフィス	Word（表示/編集/印刷/保存） / Excel（表示/編集/印刷/保存） / Power point（表示/編集/印刷/保存）
	PDF	Adobe Acrobat（表示/編集/印刷/保存）
	メディア	Windows Photo Viewer / Windows Media Player
	その他	Notepad（表示/編集/印刷/保存）
ダウンロードファイル、およびリンク先参照が保護対象となるブラウザ		Edge / Internet Explorer / Chrome / Firefox
Micro-VMで検査が可能なアプリ/ファイルタイプ	ブラウザ	Browser(.htm, .html, .xml)
	オフィス	Word(.doc, .docm, .docx, .dot, .dotm, .dotx, .odt, .rtf, .wbk, .wpd, .wps) Excel(.csv, .iqy, .ods, .slk, .xl, .xla, .xlam, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw) PowerPoint(.odp, .pot, .potm, .potx, .ppa, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .thmx)
	PDF	Adobe Acrobat Reader(.PDF)
	メディア	Photo Viewer(.bmp, .dib, .gif, .ico, .jpeg, .jpg, .png, .tif, .tiff, .wdp) Windows Media Player (.3g2, .3gp, .3gp2, .3gpp, .aac, .adt, .adts, .aif, .aifc, .aiff, .asf, .asx, .au, .avi, .m1v, .m2t, .m2ts, .m2v, .m3u, .m4a, .m4v, .mid, .midi, .mod, .mov, .mp2, .mp2v, .mp3, .mp4, .mp4v, .mpa, .mpeg, .mpg, .mpv2, .mts, .rmi, .snd, .ts, .tts, .wav, .wm, .wma, .wmv, .wmx, .wpl, .wvx)
	その他	Archive(.7z, .arj, .bz2, .cab, .chm, .flv, .gz, .jar, .nsis, .rar, .swf, .swfc, .tar, .taz, .tbz, .tbz2, .tgz, .txz, .wim, .xar,.xz, .Z, .zip, .zipx) Scripts/Executable(.bat, .cmd, .exe, .hta, .js, .jse, .lnk, .ps1, .scr, .vbe, .vbs, .wsf)

仮想化技術の第一人者による高度で独自なテクノロジー

Ian Pratt
Global Head of Security for Personal Systems,
HP Inc.

Xenプロジェクトをリードしたイアン・プラットが、仮想化技術ノウハウを活かして
独自のセキュリティ技術を開発。
2011年にBromium社を設立、セキュリティ効果を飛躍的に向上させ、65件以上の特許を取得。
2019年9月、HP Inc.がBromiumを買収、現在イアン・プラットはHP Inc. セキュリティ事業責任者

米国国防総省で55万台の導入実績

導入事例

米国国防総省が最新のエンドポイントセキュリティスタックを
最後の防衛線として実装

米国国防総省は、変化する脅威の状況に対処するために封じ込め（アプリケーション隔離と封じ込め）技術とEDR技術の組み合わせを活用し、今後のエンドポイントセキュリティスタックをアップグレードおよび近代化しています。

既存のHBSS（Host Based Security System：階層型防御ソリューション）と組み合わせることにより、組織はエンドポイント上のエージェントの数を減らしながら、サイバー攻撃に対する最高レベルの効果を達成し、誤検出を排除する運用コストを削減できます。

これらのアプローチのそれぞれは、攻撃の時間、インシデントの発生前または発生後、インシデントの場所、ホスト上、または封じ込め環境内などの違った側面から脅威を見ることで、個々のエンドポイントとエンタープライズで発生していることをより全体的に把握することを可能にします。

日本における導入実績

お客様①	建設
初回契約数量	250Lic
受注の決め手	お客様のIT担当者の判断 利用者の操作性低下が他ツールより少なく、利便性が重視される点

お客様②	損保
初回契約数量	500Lic
受注の決め手	VDIなどと比べて安かった点、利便性が確保される点、 一次対応を早急に対応しなくてもいい点（マイクロVMの中で感染の事象が発生するので、最悪そのままにしても実環境へ影響がないことをメリットとして感じて頂けた。 （すぐにLANケーブルを抜いたり、すぐにIT担当者が現物確認をしなくても保護されている）

お客様③	損保
初回契約数量	3,800Lic
受注の決め手	インターネット分離を検討 分離◎、無害化〇　理論上は分離と同じと考えられる。

日本における導入実績

お客様④	社会インフラ
初回契約数量	1,000Lic
受注の決め手	仮想ブラウザよりセキュリティ強度が高い。VDIより費用が安い。 仮想ブラウザ、VDIより利便性が高い。 インターネット物理分離より、HP Sure Click Enterpriseの論理分離を選択。

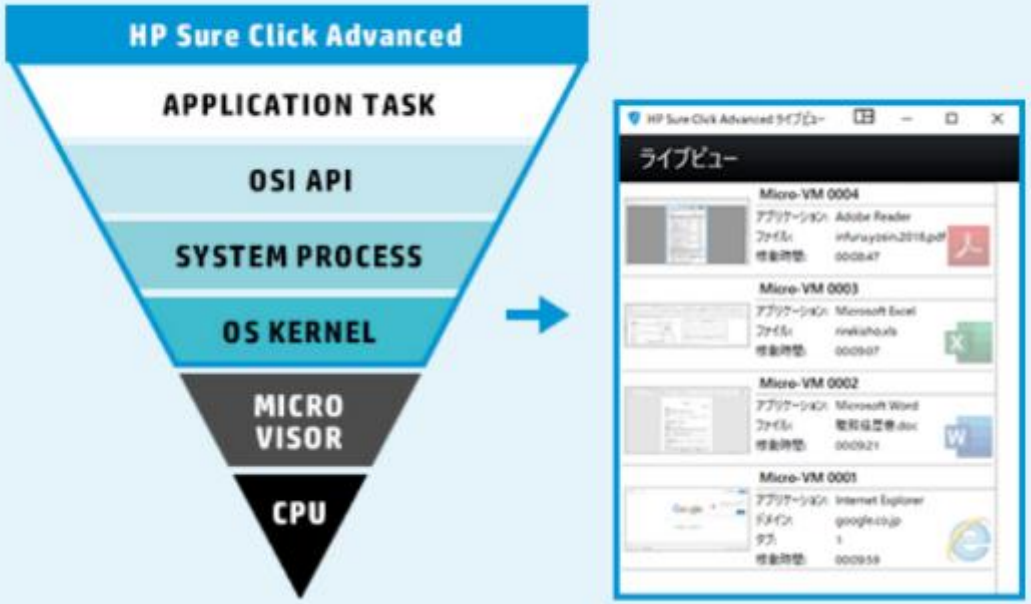
お客様⑤	損保
初回契約数量	2,000Lic
受注の決め手	インターネット分離として検討、POC内容がほぼ想定通りだったため。

お客様⑥	建設
初回契約数量	6,000Lic
受注の決め手	EDRの代替として検討、EDRのアラートをチェックし続けることに限界を感じ、リプレイスを検討。 HP Sure Click Enterprise守られている安心感は何ものにも代えがたいとのことで採用を決めていただけた。

特長① セキュリティソリューション導入による パフォーマンス低下や操作フローの変更をなくす。

CPUの仮想化支援機能「Intel Virtualization Technology（Intel VT）」や「AMD Virtualization（AMD-V）」を活用し、オーバーヘッドを極力軽減することにより、システム負荷を抑えます。

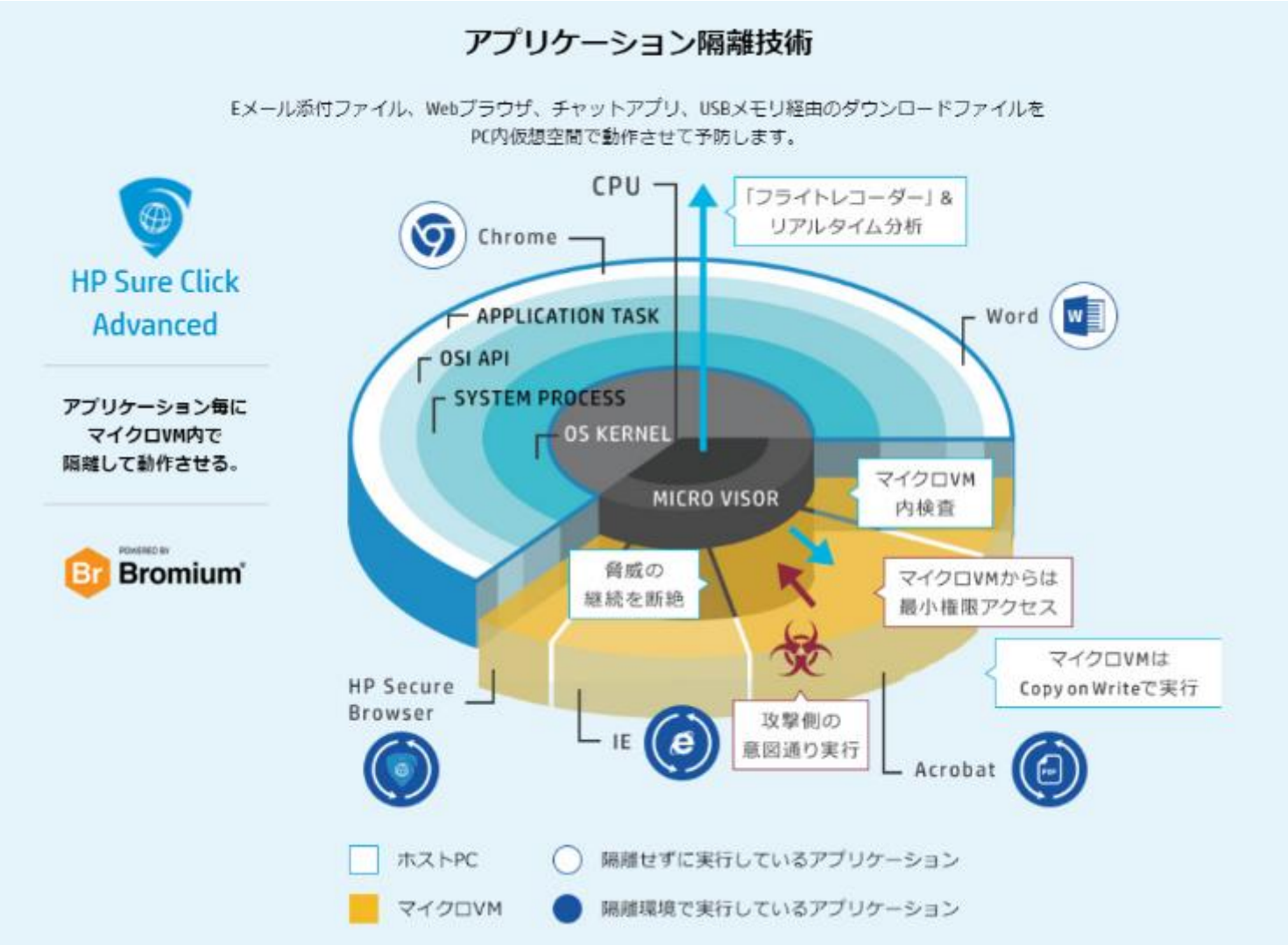
intel. AMD



- Windows PCのハードウェアレベル仮想化技術を使用
- メモリ内にマイクロ仮想マシン（VM）を瞬時に作成し、単一のアプリケーションを隔離して実行
- マイクロVMは都度生成の使い捨てでアプリケーションが終了する際に同時に消滅
- 信頼できるファイルとリンクは通常どおり実行されるが、信頼されないファイルとリンクは「コンテナ」に隔離され、マイクロVMで実行

軽量でネイティブアプリと変わらない操作性

特長② 事後対策ではなく、事前対策（防御）を強化する。

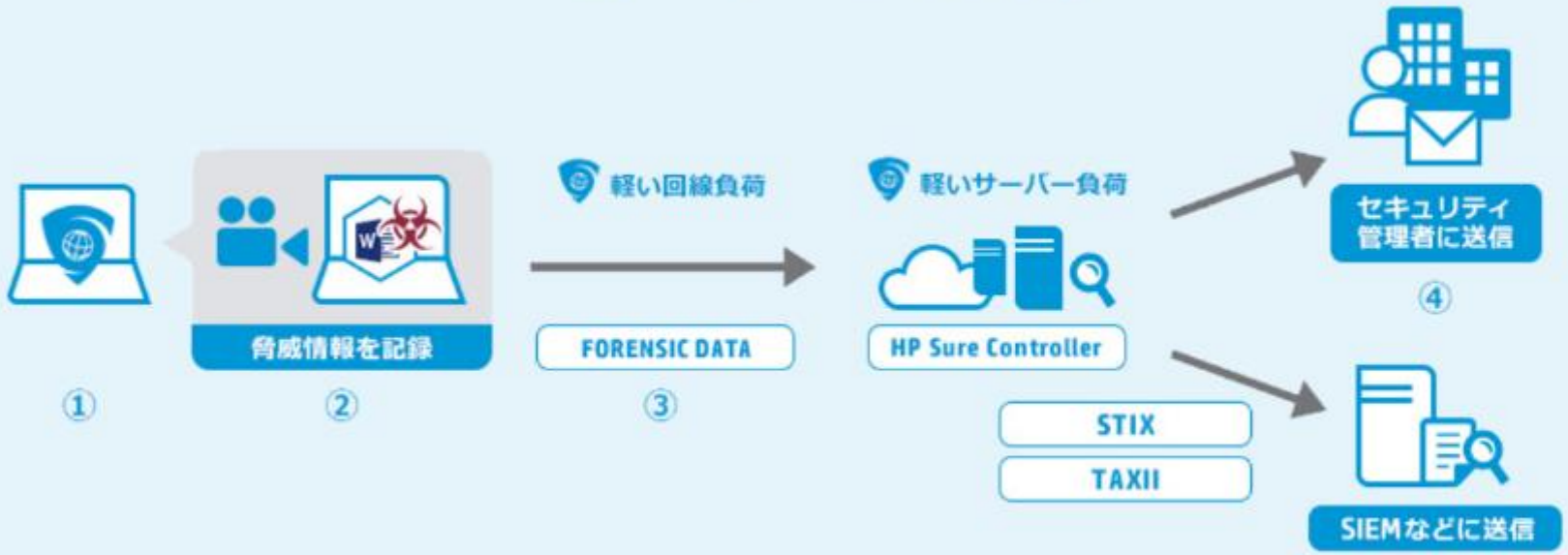


主要な攻撃経路に対する100%完全な隔離と事後対処をこれ一つでカバー

特長③ 防御しつつ、脅威情報をリアルタイムに詳細に把握する。

PC上で記録分析した脅威情報を管理サーバーで集中管理

エンドポイントエージェントの脅威情報分析



①PC上で実際に脅威が動作したときのみ記録

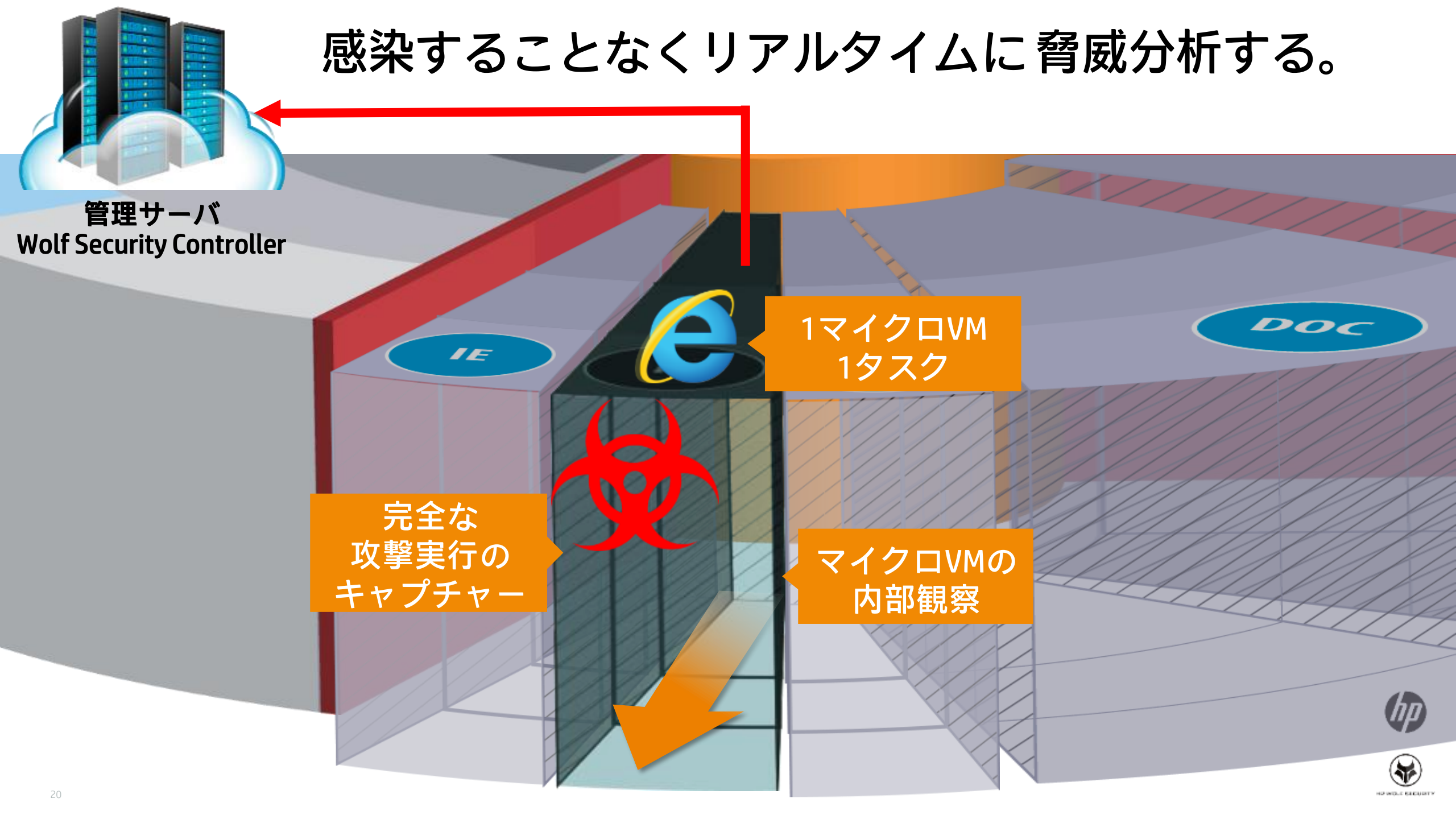
②脅威動作の一部始終（Kill-Chain）を仮想マシンのタスクが終了するまで記録

③記録終了後に脅威情報を分析し、結果を管理サーバに送信

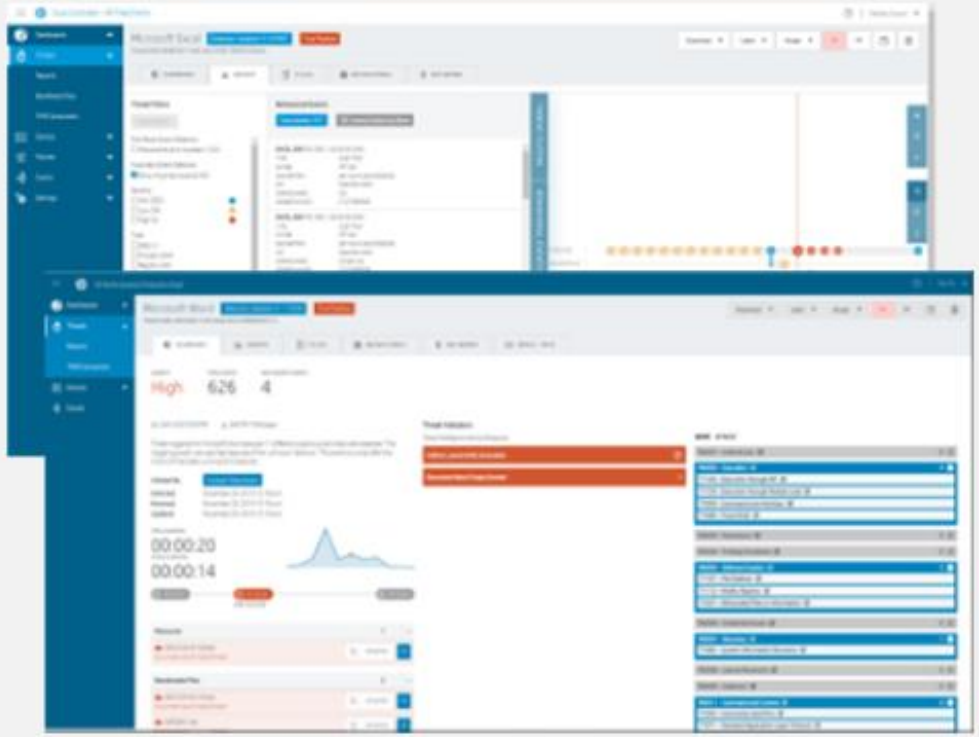
④管理サーバから、セキュリティ管理者にメールで通知 STIX/TAXII情報をSIEM(Security Information and Event Management) 等他製品へ送信する事も可能

記録・分析された脅威情報はリアルタイムにサーバーに送信

感染することなくリアルタイムに脅威分析する。



Wolf Security Controller (管理サーバ)上で提供される情報例

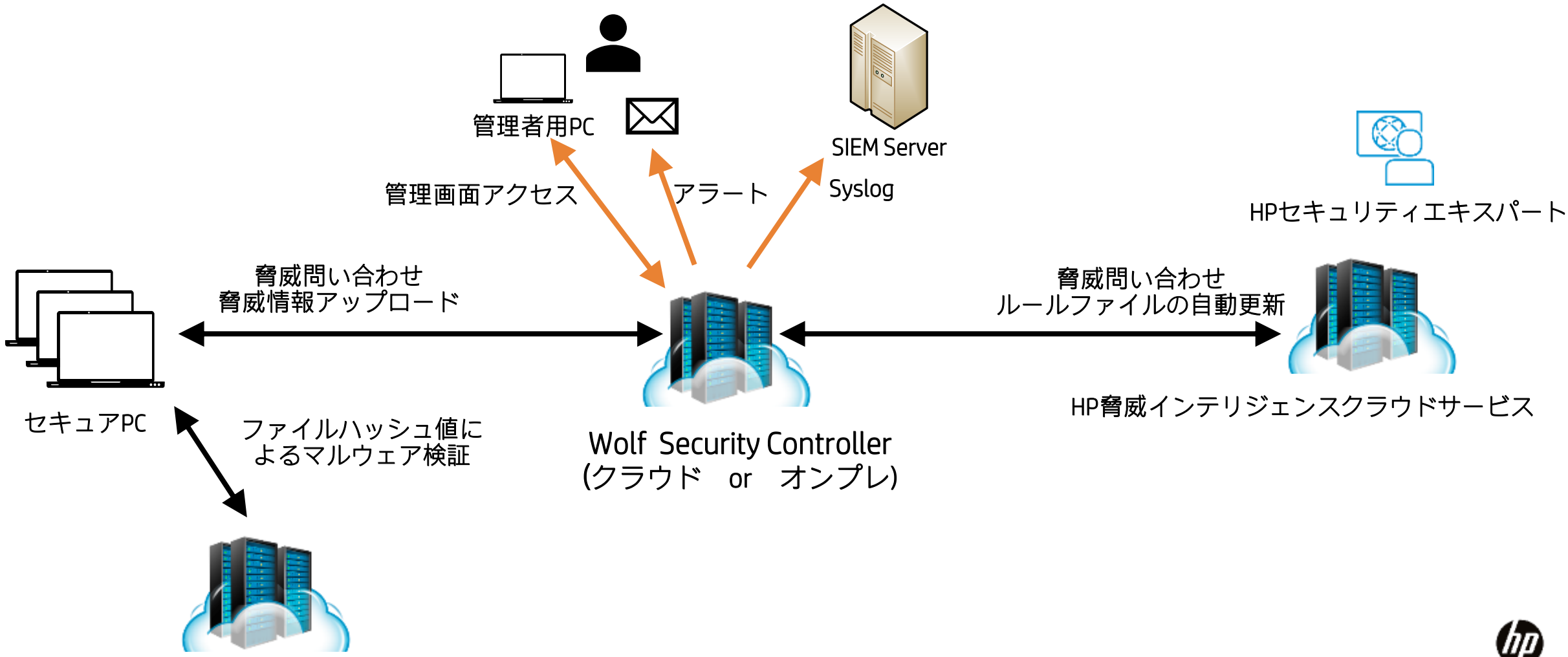


各脅威の個別分析情報

MITRE ATT&CKベースの脅威評価を含む
統合分析レポート

セキュリティチーム、経営層が必要な情報を優れたインターフェースでご提供

HP Sure Click Enterprise全体構成



HP Sure Click Enterprise端末側システム要件

ハードウェア/ソフトウェア	要件
CPU	システムBIOSでIntel Virtualization Technology (Intel VT)とExtended Page Tables (EPT)が有効になっているIntel Core i3、i5、i7。 最大32個の論理プロセッサ(LCPU)を備えたシングルソケットIntel XEONワークステーションクラスプロセッサ Rapid Virtualization Indexing (RVI)がついたAMDプロセッサ。Sure Click Enterpriseは、2011年以降に販売されているほとんどのエンタプライズクラスのAMD CPUをサポートしています。サポートされているモデルはRyzenプロセッサと、A4/A6/A8/A10（この後に、最初の桁が3以外の4桁の数字が続きます）タイプのモデルです。Sure Click Enterpriseは、最適なパフォーマンスのためにクアッドコアのAMD CPUをお勧めします。 VDI / ネストされた仮想化環境では、Sure Click EnterpriseはIntel CPUのみをサポートします。 vProチップセットを搭載したコンピュータを強くお勧めします。
メモリ	8 GB 以上 ※インストール前に1800 MBの使用可能なメモリが必要です。
ディスク	6 GB のディスク空き容量
オペレーティングシステム	Windows 10 64-bit (Professional, Enterprise) サポートバージョンは下記サポートポリシーに記載 https://support.bromium.com/s/article/Bromium-Windows-10-Support-Policy


HP WOLF SECURITY
THANK YOU