変化する脅威に立ち向かう
次世代エンドポイントセキュリティの最前線

株式会社日本HP
セキュリティエバンジェリスト　木下和紀エドワルド

/ Windows 11

木下和紀エドワルド

株式会社日本HP
セキュリティエバンジェリスト

・　Account Security Officerとしてお客様環境のセキュリティ製品の運用、提案、導入、インシデントハンドリング、監査対応などを実施。主に製薬・製造・金融のお客様を担当

・　ユーザー企業に転籍後、インフラとセキュリティ基盤を統合・一新し、セキュリティ製品の選定、導入、運用を構築、新たにSIEMの導入に合わせてSOC立ち上げなどを実施

・　2021年にHPへUターンし、Security製品部門にてセキュリティ製品全般を担当。

・　2024年、日本HP セキュリティ エバンジェリスト就任

そのセキュリティ、アップデートしていますか？

昭和 ～ 令和、 世の中変わりました

サイバーセキュリティも変わりました

1990年代	2000-2004	2005-2009	2010-2014	2015-2019	2020-2024
Operation Sundevil/ Mitnick事件など、法執行側と“ハッカー文化”のせめぎ合い サイバー犯罪捜査と電子フロンティア（EFF）の誕生 **法規制とデジタル権利の両立課題**	ILOVEYOU（2000）/ Code Red（2001）/ SQL Slammer（2003）/ Sasser（2004） メール / ワームによる世界規模の感染とインターネット輻輳。数百万台レベルの被害と数十億ドルの損失 **パッチ適用とメール添付ファイルの安全性確保** **IDS/IPS導入の加速**	Sony BMG DRMルートキット（2005） / Conficker（2008）/ Operation Aurora（2009） 企業による「マルウェア化」DRMの社会問題化、最大規模ボットネット、国家支援型APTの台頭 **サプライチェーン / DRMの透明性** **組織横断的脅威インテリジェンス共有**	Stuxnet（2010）/ Heartbleed（2014） 産業制御システムの物理破壊、インターネット全域の暗号基盤動揺 **ICS・OTのゼロトラスト化** **脆弱性開示プロセスと鍵再発行の実戦経験**	Mirai（2016）/ WannaCry（2017）/ Spectre/Meltdown（2018） IoT機器を悪用した史上最大級DDoS、ランサムウェアによる医療・公共機関停止、CPU脆弱性というハード層までの波及 **IoTセキュリティ規制強化** **ランサム対応演習** **マイクロコード更新体制**	SolarWinds（2020）/ Colonial Pipeline（2021）/ MOVEit（2023）/ Change Healthcare BlackCat（2024） サプライチェーン汚染で1.8万社侵害，燃料パイプライン停止，数百社に連鎖する大量漏えい，医療史上最大規模の個人情報流出 **SBOM義務化・インベントリ管理** **重要インフラの分離・レスポンス基準** **多層防御と事業継続計画**

2025年の攻撃手法

2025年上半期
テクニック別攻撃手法

MITRE ATT & CK Frameworkベース

TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
T1595	T1650	T1659	T1651	T1098	T1548	T1548	T1557	T1087	T1210	T1557	T1071	T1020	T1531
T1592	T1583	T1189	T1059	T1197	T1134	T1134	T1110	T1010	T1534	T1560	T1092	T1030	T1485
T1589	T1586	T1190	T1609	T1547	T1098	T1197	T1555	T1217	T1570	T1123	T1659	T1048	T1486
T1590	T1584	T1133	T1610	T1037	T1547	T1612	T1212	T1580	T1563	T1119	T1132	T1041	T1565
T1591	T1587	T1200	T1675	T1671	T1037	T1622	T1187	T1538	T1021	T1185	T1001	T1011	T1491
T1598	T1585	T1566	T1203	T1554	T1543	T1140	T1606	T1526	T1091	T1115	T1568	T1052	T1561
T1597	T1588	T1091	T1674	T1136	T1484	T1610	T1056	T1619	T1072	T1530	T1573	T1567	T1667
T1596	T1608	T1195	T1559	T1543	T1611	T1006	T1556	T1613	T1080	T1602	T1008	T1029	T1499
T1593		T1199	T1106	T1546	T1546	T1484	T1111	T1622	T1550	T1213	T1665	T1537	T1657
T1594		T1078	T1053	T1668	T1068	T1672	T1621	T1652		T1005	T1105		T1495
		T1669	T1648	T1133	T1574	T1480	T1040	T1482		T1039	T1104		T1490
			T1129	T1574	T1055	T1211	T1003	T1083		T1025	T1095		T1498
			T1072	T1525	T1053	T1222	T1528	T1615		T1074	T1571		T1496
			T1569	T1556	T1078	T1564	T1649	T1654		T1114	T1572		T1489
			T1204	T1112		T1574	T1558	T1046		T1056	T1090		T1529
			T1047	T1137		T1562	T1539	T1135		T1113	T1219		
				T1653		T1656	T1552	T1040		T1125	T1205		
				T1542		T1070		T1201			T1102		
				T1053		T1202		T1120					
				T1505		T1036		T1069					
				T1176		T1556		T1057					
				T1205		T1578		T1012					
				T1078		T1666		T1018					
						T1112		T1518					
						T1601		T1082					
						T1599		T1614					
						T1027		T1016					
						T1647		T1049					
						T1542		T1033					
						T1055		T1007					
						T1620		T1124					
						T1207		T1673					
						T1014		T1497					
						T1553							
						T1218							
						T1216							
						T1221							
						T1205							
						T1127							
						T1535							
						T1550							
						T1078							
						T1497							
						T1600							
						T1220							

Sources

MANDIANT

MITRE ENGENUITY. Center for Threat Informed Defense

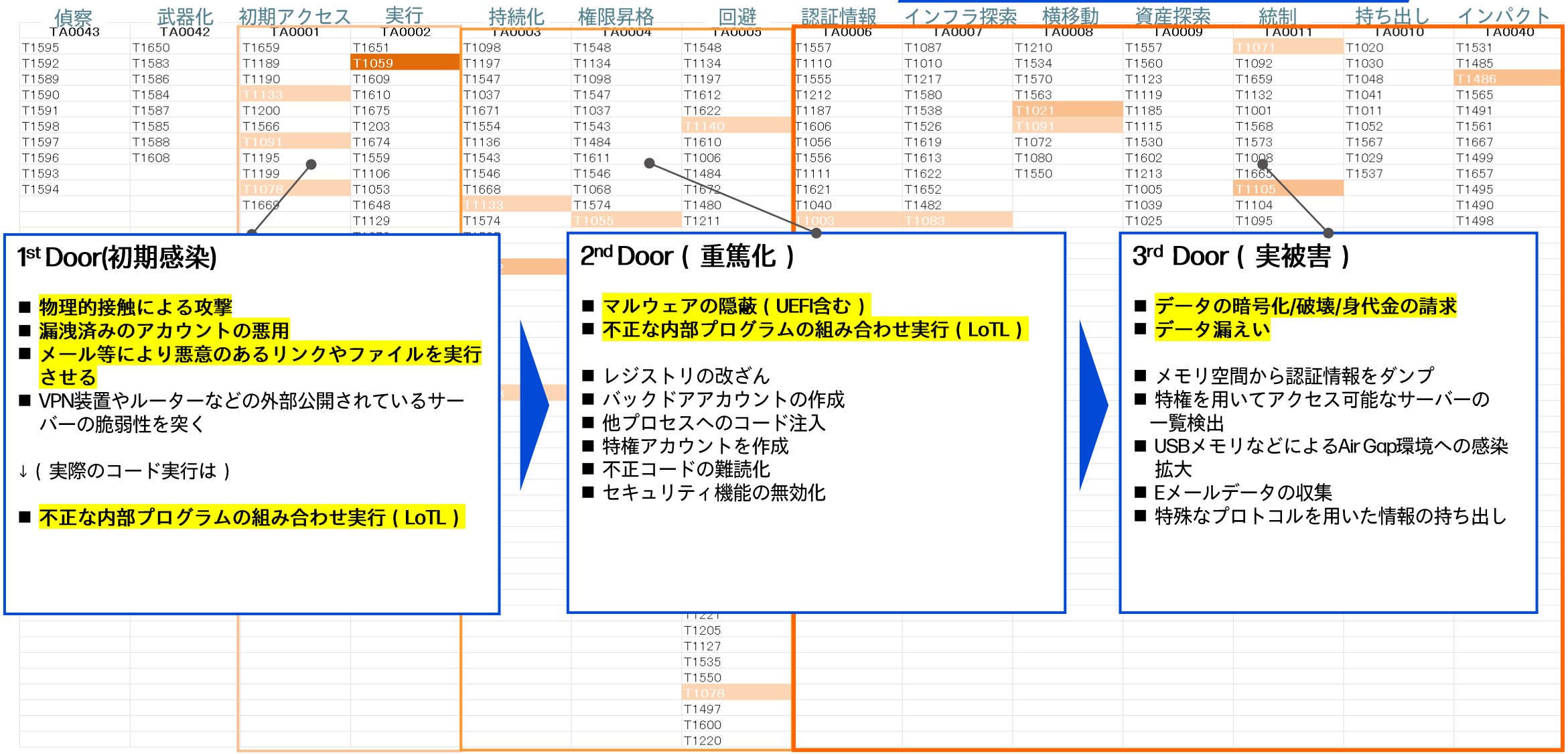
red canary

重複数

*東京大学先端科学技術研究センター 客員研究員　西尾素己

分解＆分析

ステージごとの手法



1st Door(初期感染)

- **物理的接触による攻撃**
- **漏洩済みのアカウントの悪用**
- **メール等により悪意のあるリンクやファイルを実行させる**
- VPN装置やルーターなどの外部公開されているサーバーの脆弱性を突く

↓（実際のコード実行は）

- **不正な内部プログラムの組み合わせ実行（LoTL）**

2nd Door（重篤化）

- **マルウェアの隠蔽（UEFI含む）**
- **不正な内部プログラムの組み合わせ実行（LoTL）**

- レジストリの改ざん
- バックドアアカウントの作成
- 他プロセスへのコード注入
- 特権アカウントを作成
- 不正コードの難読化
- セキュリティ機能の無効化

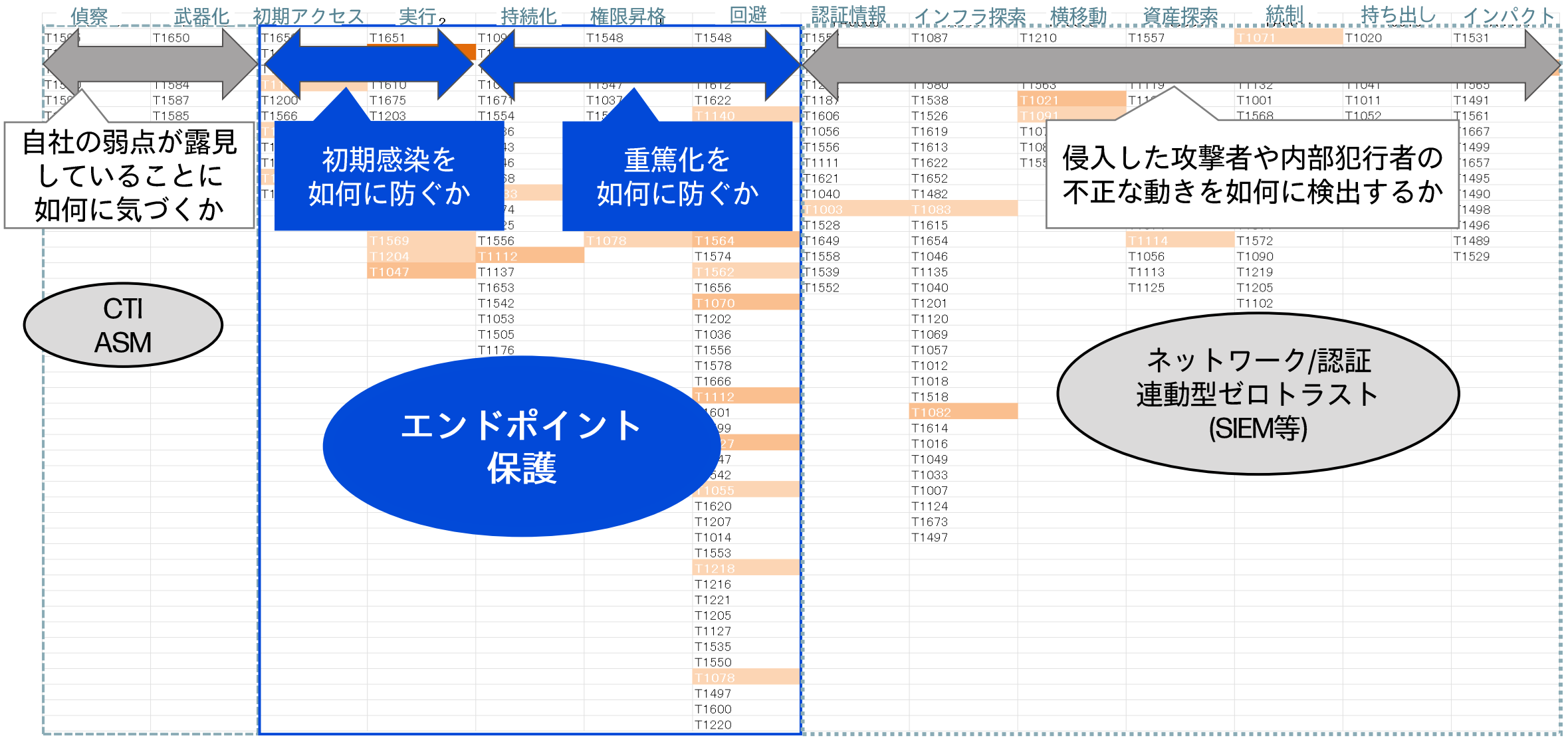
3rd Door（実被害）

- **データの暗号化/破壊/身代金の請求**
- **データ漏えい**

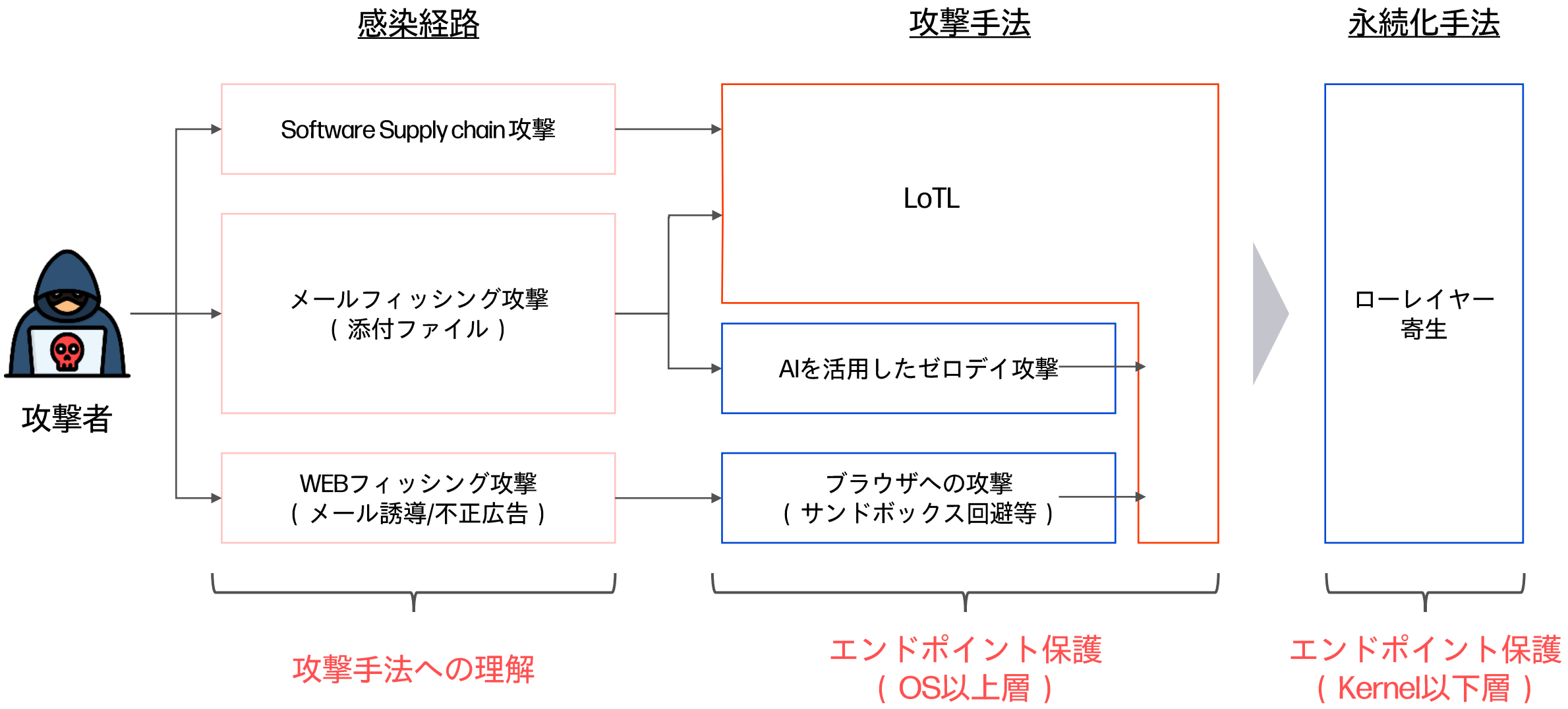
- メモリ空間から認証情報をダンプ
- 特権を用いてアクセス可能なサーバーの一覧検出
- USBメモリなどによるAir Gap環境への感染拡大
- Eメールデータの収集
- 特殊なプロトコルを用いた情報の持ち出し

攻撃のターゲット

エンドポイント保護の重要性



昨今の攻撃手法


感染経路
攻撃手法
永続化手法
Software Supply chain 攻撃
メールフィッシング攻撃
（ 添付ファイル ）
WEBフィッシング攻撃
（ メール誘導/不正広告 ）
攻撃者
LoTL
AIを活用したゼロデイ攻撃
ブラウザへの攻撃
（ サンドボックス回避等 ）
ローレイヤー
寄生
攻撃手法への理解
エンドポイント保護
（ OS以上層 ）
エンドポイント保護
（ Kernel以下層 ）

Living off the land（ LoTL ）とは

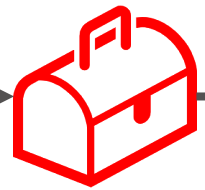
攻撃成功率を上げるため、
なるべく検知されたくない。。。
署名偽装などもすぐに対策されていたちごっこ。。。

攻撃者

1st Stager

MS署名

PowerShell等の
MS標準バイナリ



外部ツール

対策機構

- Microsoft社の正当な署名を持っているWindows標準バイナリはそもそも検閲外であることが多い。
- 振る舞い検知型の製品でも誤検知防止の観点からWindows標準バイナリの振る舞いまでを検出するものは少ない。
- 多くの対策製品はユーザーによる正当な操作であると認識する。

- 一般的でないバイナリが一般的でないプロセスによって、ダウンロード/実行されるのは典型的な不正動作である。
- ネットワークとエンドポイントの２つの観点から検知モデルが確立されている。

2025年上半期
テクニック別攻撃手法

MITRE ATT & CK Framework手法ハイライト

TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
T1595	T1650	T1659	T1651	T1098	T1548	T1548	T1557	T1087	T1210	T1557	T1071	T1020	T1531
T1592	T1583	T1189	T1059	T1197	T1134	T1134	T1110	T1010	T1534	T1560	T1092	T1030	T1485
T1589	T1586	T1190	T1609	T1547	T1098	T1197	T1555	T1217	T1570	T1123	T1659	T1048	T1486
T1590	T1584	T1133	T1610	T1037	T1547	T1612	T1212	T1580	T1563	T1119	T1132	T1041	T1565
T1591	T1587	T1200	T1675	T1671	T1037	T1622	T1187	T1538	T1021	T1185	T1001	T1011	T1491
T1598	T1585	T15	T1203	T1554	T1543	T1140	T1606	T1526	T1091	T1115	T1568	T1052	T1561
T1597	T1588	1	T1674	T1136	T1484	T1610	T1056	T1619	T1072	T1530	T1573	T1567	T1667
T1596	T1608	195	T1559	T1543	T1611	T1006	T1556	T1613	T1080	T1602	T1008	T1029	T1499
T1593		T1199	T1106	T1546	T1546	T1484	T1111	T1622	T1550	T1213	T1665	T1537	T1657
T1594		T1078	T1053	T1668	T1068	T1672	T1621	T1652		T1005	T1105		T1495
		T1669	T1648	T1133	T1574	T1480	T1040	T1482		T1039	T1104		T1490
			T1129	T1574	T1055	T1211	T1003	T1083		T1025	T1095		T1498
			T1072	T1525	T1053	T1222	T1528	T1615		T1074	T1571		T1496
			T1569	T1556	T1078	T1564	T1649	T1654		T1114	T1572		T1489
			T1204	T1112		T1574	T1568	T1046		T1056	T1090		T1529
			T1047	T1137		T1562	T1539	T1135		T1113	T1219		
				T1653		T1656	T1552	T1040		T1125	T1205		
				T154		T1070					T1102		
				T105		T1202		T1120					
				T150		T103		T1069					
				T117		T15		T1057					
				T12		78		T1012					
				T1		666		T1018					
						112		T1518					
						T1601		T1082					
						T1599		T1614					
						T1027		T1016					
						T1647		T1049					
						T1542		T1033					
						T1055		T1007					
						T1620		T1124					
						T1207		T1673					
						T1014		497					
						T1553							
						T1218							
						T1216							
						T1221							
						T1205							
						T1127							
						T1535							
						T1550							
						T1078							
						T1497							
						T1600							
						T1220							

「コマンド / スクリプトインタープリタを悪用して任意のコマンドやスクリプト、バイナリを実行する」 攻撃手法

Windows Management Instrumentation (WMI) を悪用してコマンド実行・情報収集・横展開などを行う手法

レジストリ値やキーを作成・変更・削除する手法

ホスト上に残るログ・ファイル・レジストリ・タイムスタンプなどの「痕跡」を削除 / 改変し、検知やフォレンジック解析を妨害する手法

ファイルやコードを暗号化・圧縮・難読化

OS やアプリの「隠し機能」や属性を悪用して、ファイル・プロセス・ユーザー・設定などの痕跡を不可視化

Sources

MANDIANT

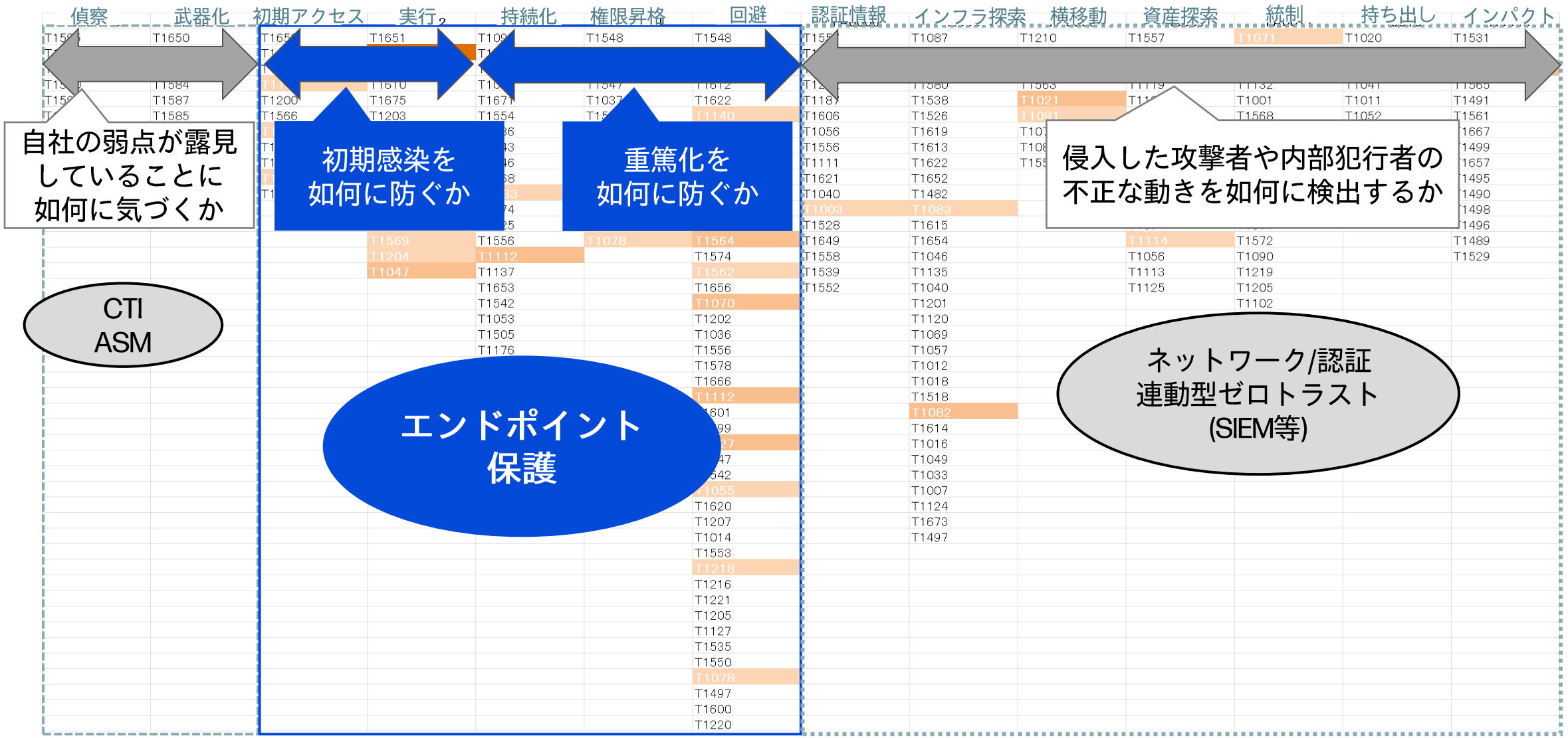
MITRE ENGENUITY. Center for Threat Informed Defense

red canary

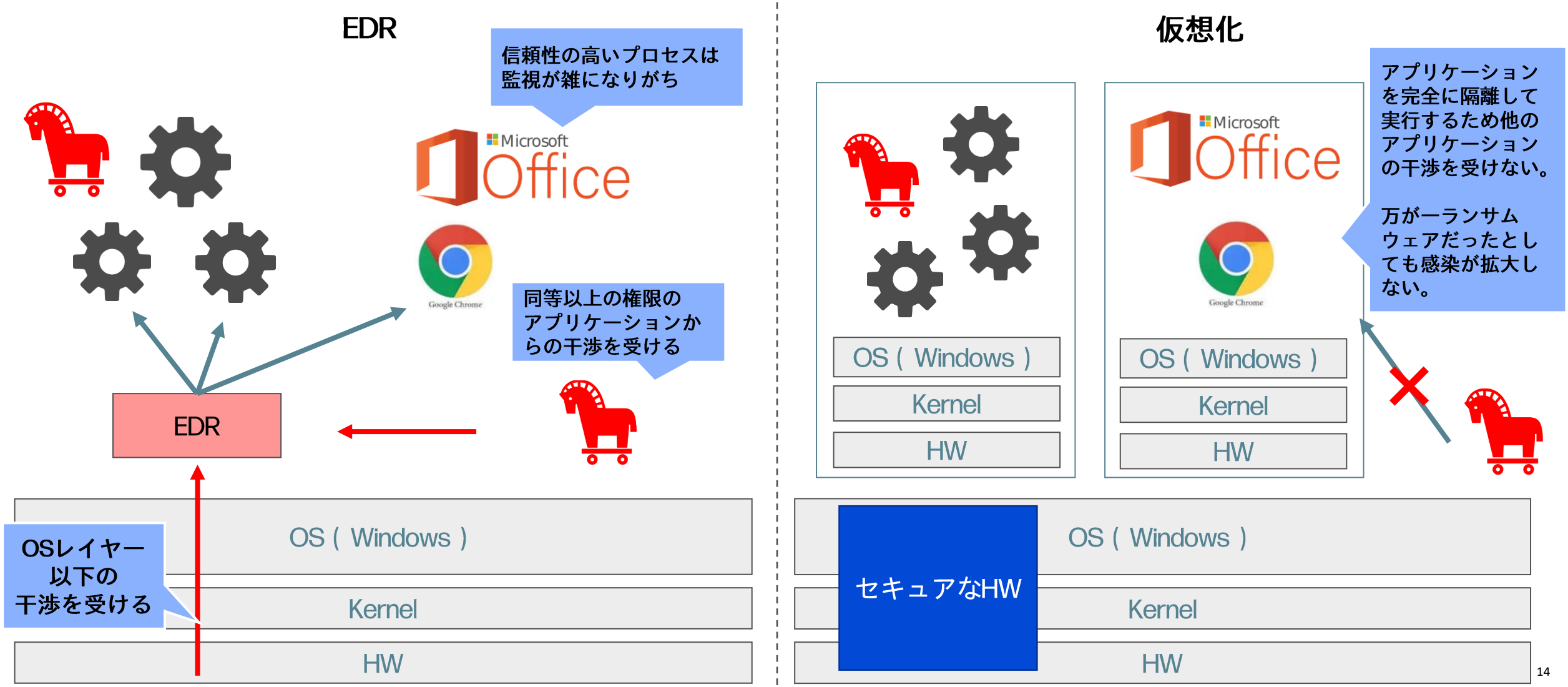
重複数

攻撃のターゲット

エンドポイント保護の重要性

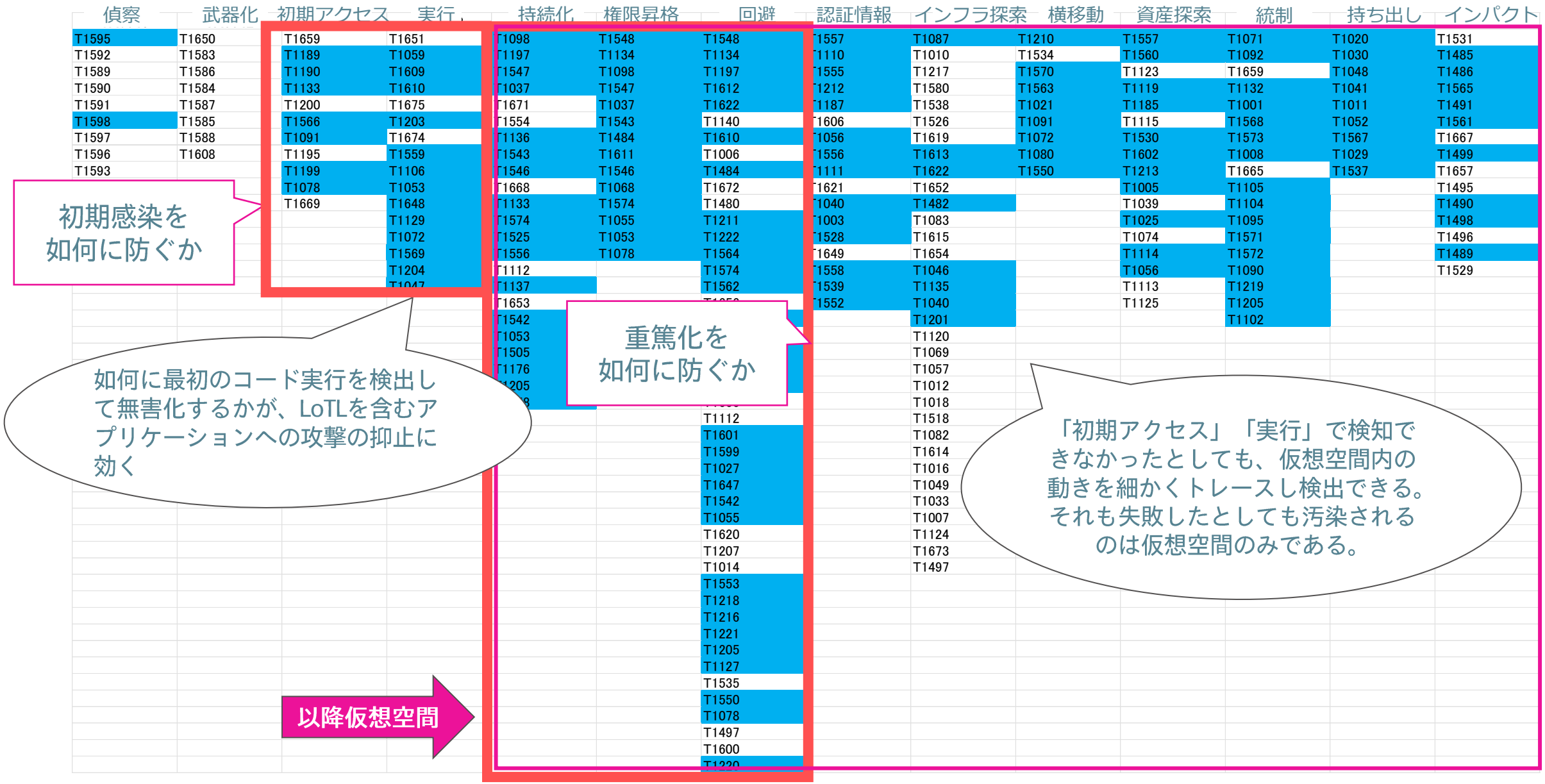


EDRと仮想化


EDR
信頼性の高いプロセスは
監視が雑になりがち
Microsoft Office
Google Chrome
同等以上の権限の
アプリケーションか
らの干渉を受ける
EDR
OSレイヤー
以下の
干渉を受ける
OS (Windows)
Kernel
HW
仮想化
アプリケーション
を完全に隔離して
実行するため他の
アプリケーション
の干渉を受けない。
万が一ランサム
ウェアだったとし
ても感染が拡大し
ない。
OS (Windows)
Kernel
HW
Microsoft Office
Google Chrome
OS (Windows)
Kernel
HW
セキュアなHW
OS (Windows)
Kernel
HW

仮想化の守備範囲

次世代エンドポイント保護



脅威の封じ込め

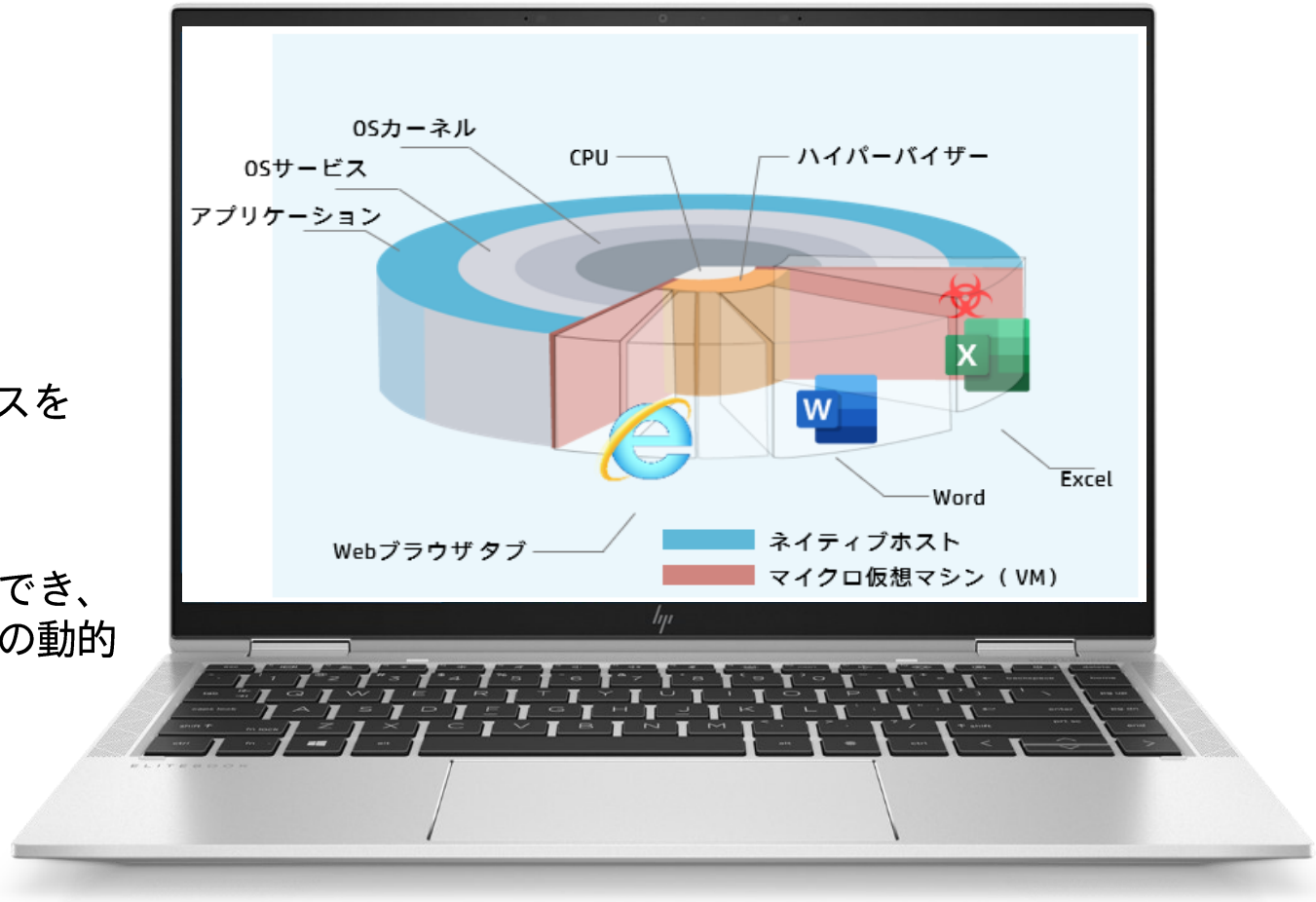
HP Sure Click

攻撃を隔離、封じ込めることで、
初期感染、重篤化を防ぎます

検知に依存しない「隔離と封じ込め」技術で、
ゼロデイ攻撃に対応し、クリーンアップも不要です

Microsoft OfficeやPDFのファイル操作およびWebアクセスを
ユーザーが制約を意識することなく利用可能です

新種のウイルスが侵入した場合でも安心して作業を継続でき、
また「Wolf Security Controller」により、隔離済みの脅威の動的
分析及びMITRE ATT & CK Frameworkの分類が
可能となります



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.

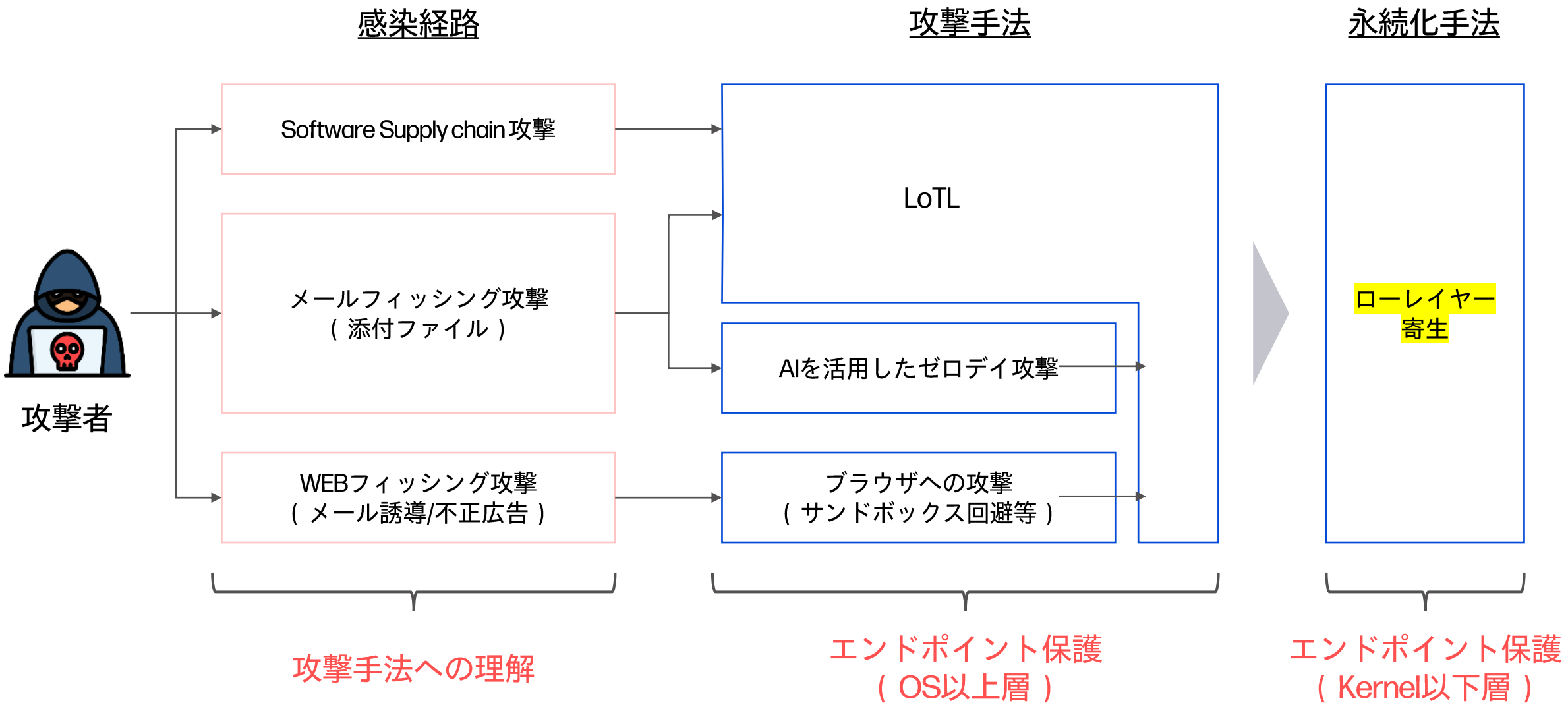
Xenプロジェクトをリードしたイアン・プラットが、仮想化技術ノウハウを活かして
独自のセキュリティ技術を開発。
2011年にBromium社を設立、セキュリティ効果を飛躍的に向上させ、65件以上の特許を取得。
2019年9月、HP Inc.がBromium 買収。
現在イアン・プラットはHP Inc. セキュリティ事業責任者

HP Sure Clickのカバー範囲

MITRE ATT&CK Framework

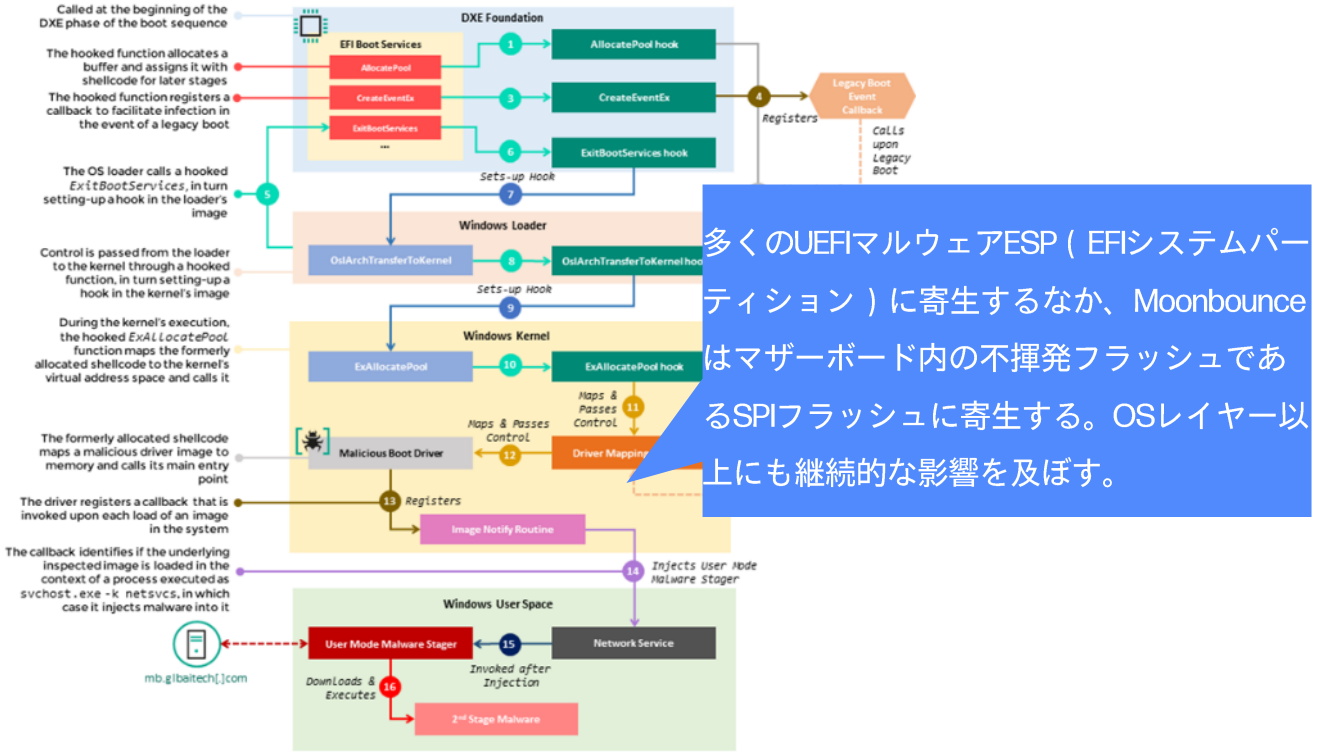
ハードウエア セキュリティ

昨今の攻撃手法


感染経路
攻撃手法
永続化手法
Software Supply chain 攻撃
メールフィッシング攻撃
（ 添付ファイル ）
WEBフィッシング攻撃
（ メール誘導/不正広告 ）
攻撃者
LoTL
AIを活用したゼロデイ攻撃
ブラウザへの攻撃
（ サンドボックス回避等 ）
ローレイヤー
寄生
攻撃手法への理解
エンドポイント保護
（ OS以上層 ）
エンドポイント保護
（ Kernel以下層 ）

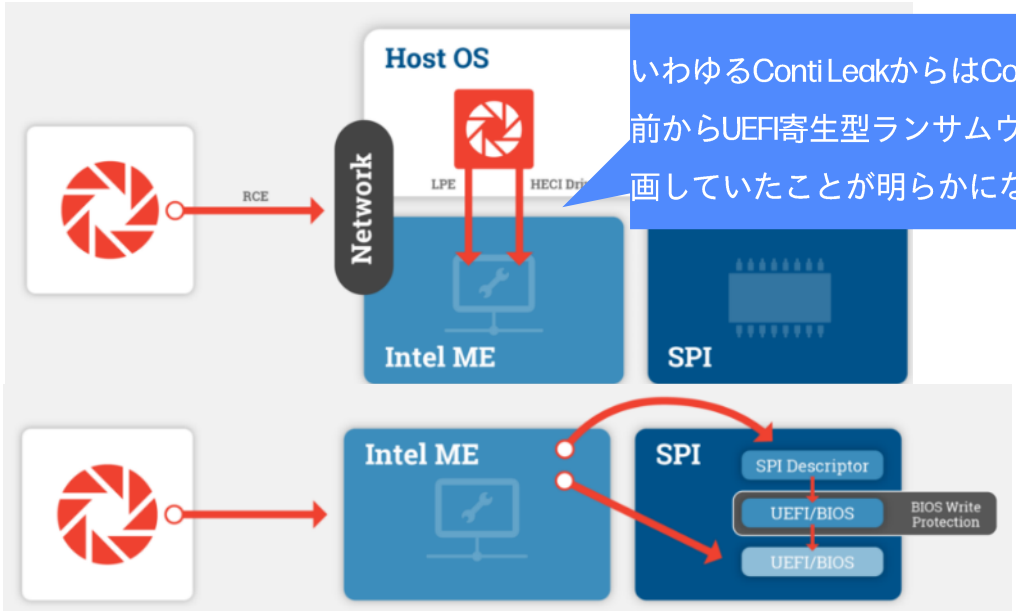
ローレイヤー領域への攻撃

次世代UEFIマルウェアMoonbounce



多くのUEFIマルウェアESP（EFIシステムパーティション）に寄生するなか、Moonbounceはマザーボード内の不揮発フラッシュであるSPIフラッシュに寄生する。OSレイヤー以上にも継続的な影響を及ぼす。

ContiもUEFI寄生型ランサムウェアを検討していた



いわゆるConti LeakからはContiが数年前からUEFI寄生型ランサムウェアを計画していたことが明らかになった

攻撃の激化はアプリケーションレイヤーにとどまらず、低レイヤーにまで及んでいます。

低レイヤーが汚染された場合には、上位レイヤーからの検出は極めて難しいため、同じレイヤーでの対策技術が極めて重要です。

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce_technical-details_eng.pdf　https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/

量子コンピューターの登場

何が脅威なのか?

2025/10月現在、量子コンピューターによる実運用のRSA暗号を破ったという事例はまだありません。

・Harvest-Now, Decrypt-Later（HNDL）、今盗み、後で復号すれば良い
→今日盗まれた暗号化データが将来の量子計算機で復号される恐れ

・長寿命データ（個人情報/医療/政府/知財/産業制御ログ）
→特に高リスク
→OT/ICSや医療、政府記録など“10年以上の秘匿”を要する分野でのリスク顕在化

・TLSセッションの“記録
→将来復号”による過去通信の秘匿性喪失

何が脅威なのか?

・機密ファイル/バックアップの長期窃取と将来の復号

・コード署名・ファームウェア署名の偽造
→攻撃者の正規アップデート成りすまし

・公開鍵暗号（RSA/ECC/DSA等）の破綻リスク
→デジタル署名の無力化
→マルウェア署名/更新/ファームウェアの信頼が揺らぐ
→サプライチェーンと長期証跡（TLS・VPN・eメール・バックアップ）への波及

現在どこまで可能なのか?

誤報1

・格子暗号を解く量子アルゴリズム
　→2024年4月のNIST第5回PQC会議で、「格子暗号を解読し得る量子アルゴリズム」をうたう未査読論文が話題になり、会場でも即時に反証できず一時動揺。

誤報2

・量子アニーリング公開鍵暗号攻撃
　→2024年5月、Chinese Journal of Computingに掲載された論文を起点に、「D-WaveでRSAが破られた」という誤報が広がり、一般メディアやSNSで不安が増幅しました。

現在どこまで可能なのか?

・CRQC（暗号解読に“関連する”規模の量子計算機）は“まだ存在しない”のが政府・標準機関の共通認識

→研究は加速：RSA-2048の量子資源見積りは“2,000万→<100万物理キュービット”へ更新

（理論

→実機は未達だが、“移行は時間がかかる”ため今すぐ準備が必要

HPはどのように考えているのか？

HPの方針は

量子で既存の公開鍵（RSA/ECC）が破られる前に、PC/プリンターの
“最下層＝ファームウェア”をPQCで守るという方針です。

・2024年3月に量子耐性（quantum-resistant）でファームウェア整合性を守るビジネスPCを発表

・2025年3月に量子耐性のデジタル署名検証でファームウェア整合性を守るビジネスプリンターを発表しました。

現在のPCセキュリティは信頼の連鎖が前提

Windows 11

Windows Hello

BitLocker

仮想化ベースのセキュリティ（VBS）

コア分離
- メモリ整合性（HVCI）
- メモリアクセス保護
（カーネルDMA保護）

Windowsプラットフォームサービス

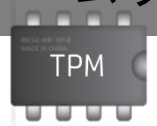
OSカーネル

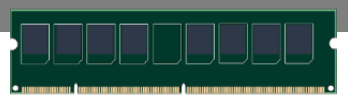
セキュアカーネル

ハイパーバイザー

UEFI OSローダー、UEFIドライバー

UEFIファームウェア（BIOS）





セキュアブート
の
さらに下から

HP Sure Start
でHWを保護

HP Endpoint Security Controller

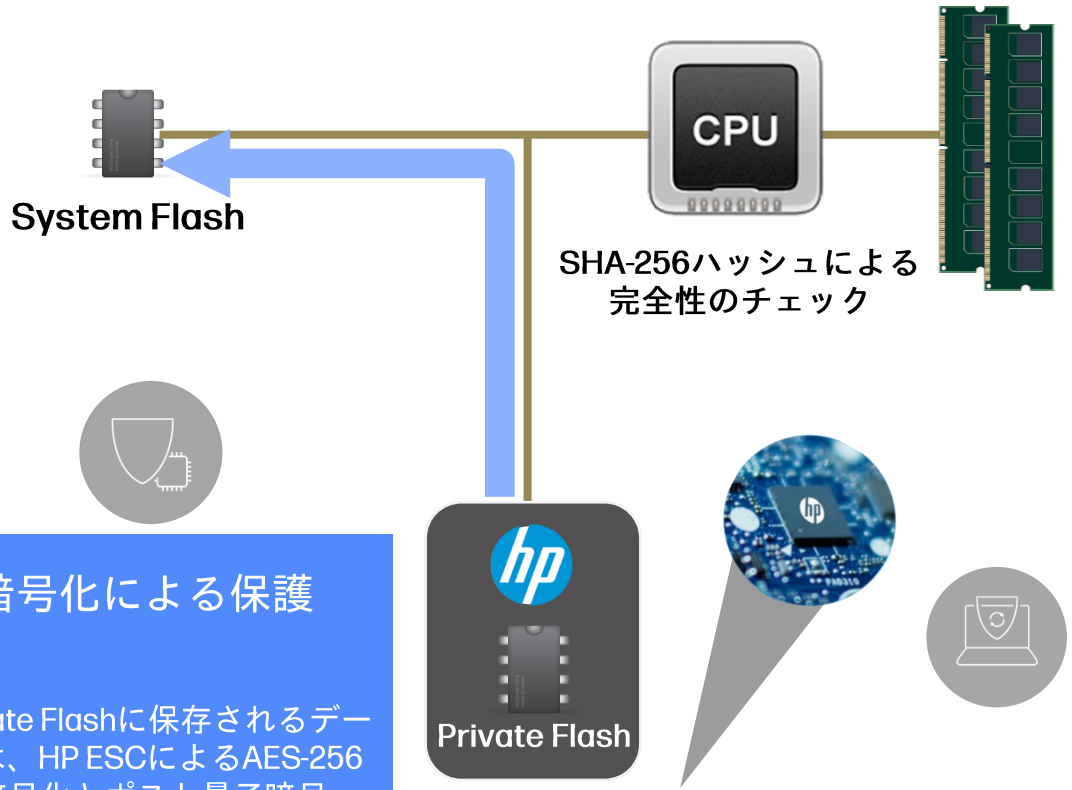
自己修復ファームウエア

Endpoint Security ControllerとSure Start

ファームウェアの復元力

システムの起動前にSystem Flash内のHP BIOSおよび重要なファームウェアの完全性を検証して、故障や改ざんがあった場合にPrivate Flashにあるバックアップコピーを使用して自動回復

- HP BIOS
- HP UEFI BIOS設定
- HP Factory構成情報
- セキュアブートキー
- ハードドライブのGPT
- Intel®マネジメントエンジン(ME)ファームウェア（Intelのみ）
- AMDセキュアプロセッサファームウェア（AMDのみ）



暗号化による保護

Private Flashに保存されるデータは、HP ESCによるAES-256暗号化とポスト量子暗号（世界初）で保護

ランタイム侵入検知

OS実行中のメインメモリ内のBIOSコードへの攻撃を検知

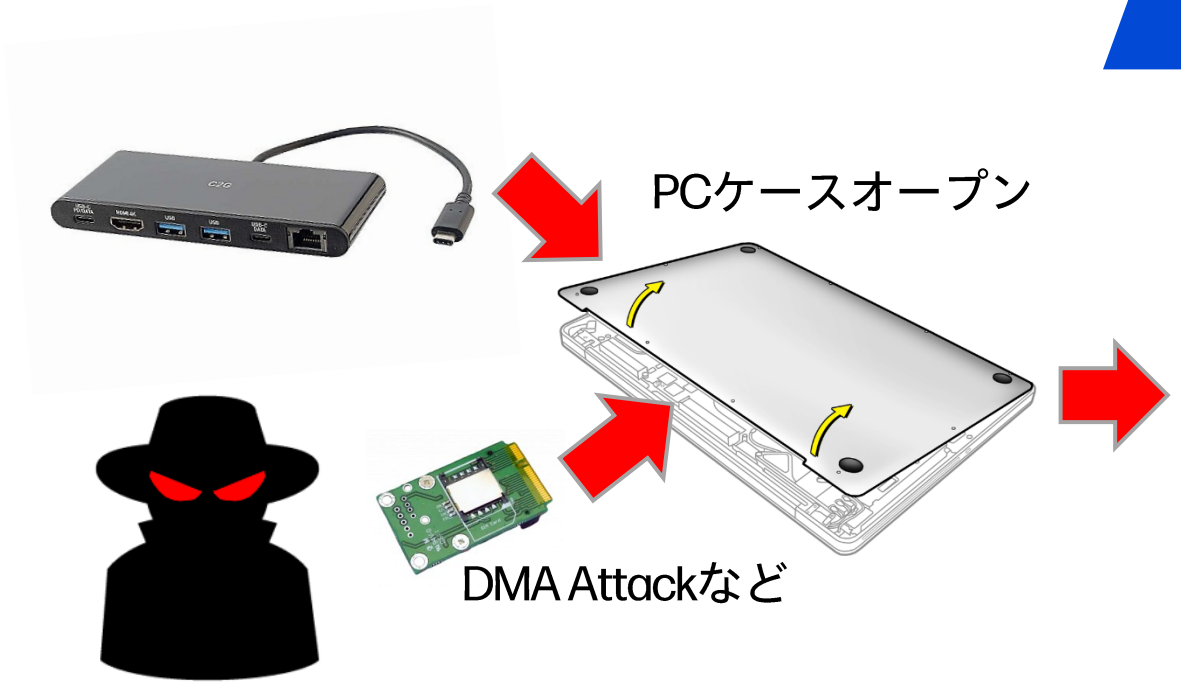
メモリ保護

OS起動前のDMA (Direct Memory Access) 攻撃を防止

悪意のある周辺機器からの保護

HP BIOSハイパーバイザーが接続されたデバイスが、PCに感染するのを防止

HWセキュリティイベント検知



イベントログへの記録

ハードウエアへの改ざんや攻撃の記録は内臓のEndpoint Security Controllerにて記録され、
OS起動後にWindowsイベントログへ反映されます。
セキュリティツールにてイベントIDを監視することで、簡単にHWへの侵害が検知可能です。

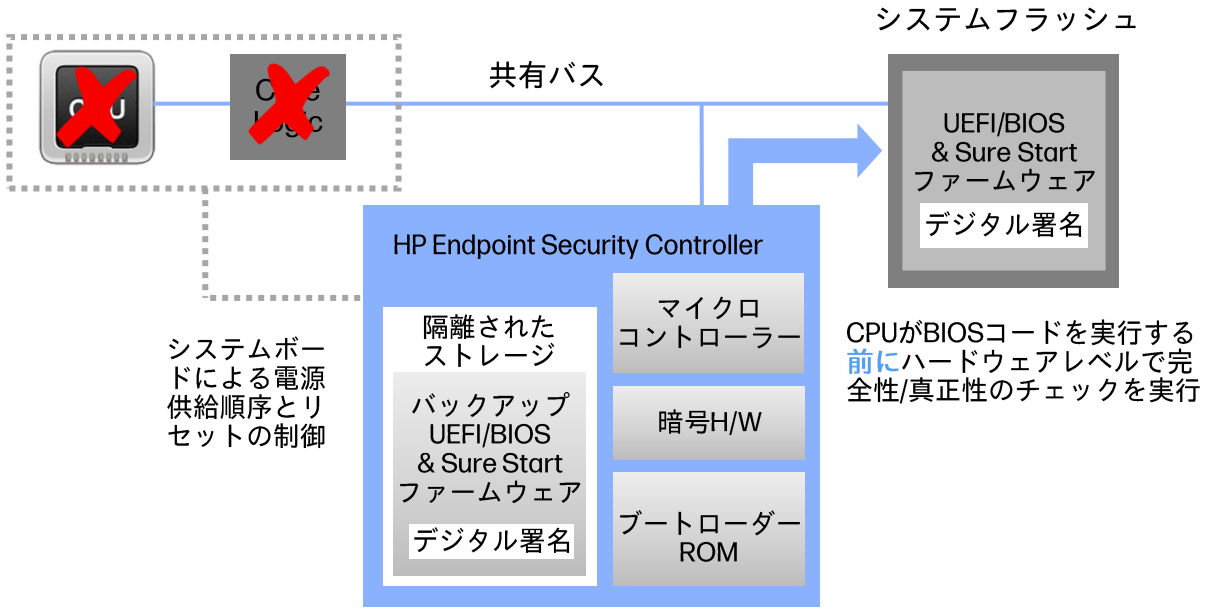
ファームウェアのレジリエンス

Endpoint Security ControllerとSure Start

機能	NIST要件	HP Sure Start
ルート・オブ・トラスト	必須	●
書き換え可能コードの保護とアップデート	必須	●
書き換え不能コードの保護	必須	●
重要プラットフォームFWのランタイム保護	必須	●
重要データの保護	必須	●
破損コードの検知	必須	+
重要データの破損の検知	必須	●
書き換え可能コードの復旧	必須	●
重要データの復旧	必須	+
ロギングと通知	オプション	+
ポリシーベースの制御	オプション	+
自動か手動の復旧オプション	オプション	+
ローカルかリモートの復旧	オプション	+
ロールバックの阻止	オプション	+
ランタイム侵入検知	未定義	+
物理的攻撃の検知	未定義	+
量子暗号による追加の保護	未定義	+

NIST要件を超えた項目

●NIST要件を満たす
＋NIST要件を超える



システムフラッシュはCPUやCore Logicに給電される前にEndpoint Security Controllerによって検証・突合され、整合性が担保できない場合は自動的に書き換え、リカバリーを実施します。

HP Protect and Trace with Wolf Connect

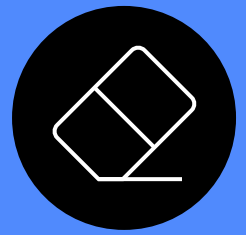
電源が切れていても、
インターネットから切断されていても、
リモートでPCのFind（探索）、Lock（ロック）、Erase（消去）が可能

Find

紛失・盗難されても
現在地を**リアルタイム**で
探索

Lock

決して解除できない
BIOSレベルでのロック



Erase

電源・通信オフでも
確実にデータ消去

HP Protect and Trace with Wolf Connect

“狭帯域”通信モジュール（MNB：Mobile Narrow Band）

- 低コストと低消費電力を実現するLTE-Cat M規格を採用
- [通常（“広帯域”）の4Gまたは5G W-WANモジュールもサポート]

専用の通信契約

- HPにて専用通信回線を提供（費用込み）
- HP Wolf Connect専用（任意通信は不可）
- 世界80か国でのグローバル接続

PCのHP Endpoint Security ControllerがWolf Connectサーバと通信する機能を提供します。

Post-Quantum Cryptography
（耐量子計算機暗号）対応
ファームウェア搭載ビジネスPC

HP Endpoint Security Controller
物理的に分離された専用のセキュリティ
マイクロプロセッサで、BIOSを保護

*1暗号化、認証、マルウェア対策、BIOSレベルの保護がプリインストールされ、MIL-STDテストに合格した、ビジネス向けPCに関するHPの内部分析に基づきます。分析の結果、2024年2月の時点で、UEFI BIOSファームウェアの整合性を保護するために耐量子暗号方式を実装している同クラスの他のPCはありませんでした。

HP QPC対応ビジネスPC例

HP EliteBook X G1i 14 AI PC

ハイブリッドワーク
のための
エンタープライズ性能

ユーザーに適応するPCで最高のパフォーマンス

HP Smart Resource Optimizer [41]を通じてAIを使用し、パフォーマンスを最適化するPCで一日を乗り切る。静かで涼しく動作しながら、終日バッテリー寿命を確保[61]

リモートでも効果的にコラボレーション

poly camera pro

リモートディスカッション用のPoly Camera Pro[8]と対面プレゼンテーション用の多様なポートとタッチパネル(オプション)を使用して、全ての共同セッションでアイデアを主役に

世界クラスの保護で安心

HP Wolf Securityの強靭な多層保護により、進化するサイバー脅威を阻止。これには量子コンピューター攻撃からの将来に備えた防御も含まれいる[10]

軽量なスタイリッシュ筐体でどこでもAIを活用

最大
48 TOPS[6]
Copilot+PC

intel CORE ULTRA

ポータブル
スタイリッシュ
多機能

/ Windows 11