変化する脅威に立ち向かう：エンドポイントセキュリティの最前線

～近年の大規模サイバーインシデントに対処するための視点～

株式会社日本HP

エンタープライズ営業統括

大津山　隆

Contents

HPのエンドポイントセキュリティにおけるリーダーシップとイノベーション

変化するサイバー脅威

今日の典型的なサイバー脅威 – 事業妨害型攻撃：ランサムウェア

変化する脅威と対策

2025年上半期のサイバー攻撃

偵察	攻撃態勢の確立	接触	実行	永続化	権限昇格	防衛回避	認証情報へのアクセス	探索	ラテラルムーブメント（侵入拡大）	収集	コマンドアンドコントロール(C&C)	持ち出し	影響
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							

重複数

出典：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

Qilin RaaSの典型的攻撃パターン

偵察	攻撃態勢の確立	接触	実行	永続化	権限昇格	防衛回避	認証情報へのアクセス	探索	ラテラルムーブメント（侵入拡大）	収集	コマンドアンドコントロール(C&C)	持ち出し	影響
T1595	T1650	T1659	T1651	T1098	T1548	T1548	T1557	T1087	T1210	T1557	T1071	T1020	T1531
T1592	T1583			T1197	T1134	T1134	T1110	T1010	T1534	T1560	T1092	T1030	T1485
T1589	T1586			T1547	T1098	T1197	T1555						
T1590	T1584			T1037	T1547	T1612	T1212						
T1591	T1587			T1671	T1037	T1622	T1187						
T1598	T1585			T1554	T1543	T1140	T1606						
T1597	T1588			T1136	T1484	T1610	T1056						
T1596	T1608			T1543	T1611	T1006	T1556						
T1593				T1546	T1546	T1484	T1111						
T1594				T1668	T1068	T1672	T1621						
				T1133	T1574	T1480	T1040						
				T1574	T1055	T1211	T1003						
				T1525	T1053	T1222	T1528						
				T1556	T1078	T1564	T1649						
				T1112		T1574	T1558						
				T1137		T1562	T1539						
				T1653		T1656	T1552						
						8							
						T1216							
						T1221							
						T1205							
						T1127							
						T1535							
						T1550							
						T1078							
						T1497							
						T1600							
						T1220							

Fortinet製品の脆弱性を突くコードを多数保有

その後すべてのSSL VPNサーバーに対して総当りもしくは事前に入手した認証情報で侵入

構成を掌握しフェイルオーバー構成にまで侵入

CVE-2023-27532（Veeam Backup & Replication の脆弱性）を悪用するツールを保有

難読化したMIMIKAZモジュールを用いて「lsass.exe、winlogon.exe、wininit.exe」から認証情報をダンプ

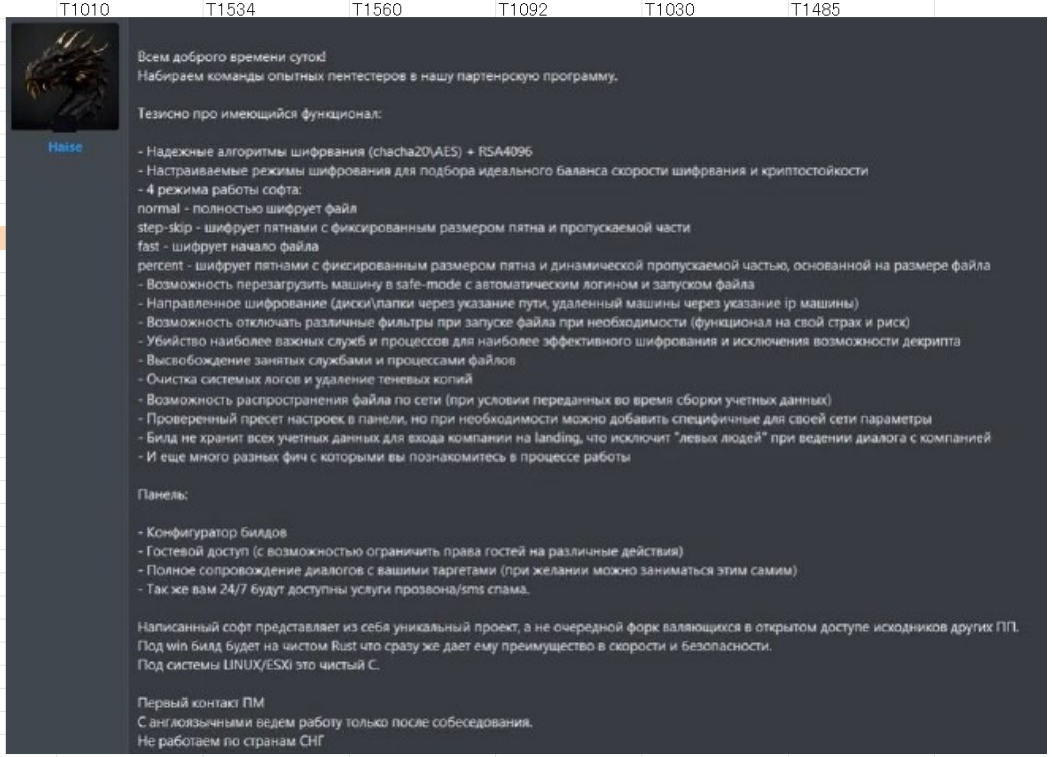
入手したハッシュを元にSYSTEM権限プロセスを起動

定期的にイベントログを削除、SIEMへの転送を妨害するイベントを専用スレッドで起動

防御機能の停止

RSAT-AD-PowerShellモジュールを外部注入しEntra ID内を捜索

BYOVD（Bring Your Own Vulnerable Driver）も使用している可能性



PS execをspreadモードで起動し全システムに向けてコマンド実行

VMware vCenter/ESXiのハイパーバイザーにも同様に侵入し、子プロセスを全仮想マシンに注入

ボリュームシャドウを含め全バックアップデータを削除

AES-256やChaCha20でファイルを暗号化

出典：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

今日の典型的なサイバー脅威 - ステージ毎の手法の分析

偵察	攻撃態勢の確立	接触	実行	永続化	権限昇格	防衛回避	認証情報へのアクセス	探索	ラテラルムーブメント（侵入拡大）	収集	コマンドアンドコントロール(C&C)	持ち出し	影響
T1595	T1650	T1659	T1651	T1098	T1548	T1548	T1557	T1087	T1210	T1557	T1071	T1020	T1531
T1592	T1583			T1197	T1134	T1134	T1110	T1010	T1534	T1560	T1092	T1030	T1485
T1589	T1586			T1547	T1098	T1197	T1555	T1217	T1570	T1123	T1659	T1048	T1486
T1590	T1584			T1037	T1547	T1612	T1212	T1580	T1563	T1119	T1132	T1041	T1565
T1591	T1587			T1671	T1037	T1622	T1187	T1538	T1021	T1185	T1001	T1011	T1491
T1598	T1585			T1554	T1543	T1140	T1606	T1526	T1091	T1115	T1568	T1052	T1561
T1597	T1588			T1136	T1484	T1610	T1056	T1619	T1072	T1530	T1573	T1567	T1667
T1596	T1608			T1543	T1611	T1006	T1556	T1613	T1080	T1602	T1008	T1029	T1499
T1593				T1546	T1546	T1484	T1111	T1622	T1550	T1213	T1665	T1537	T1657
T1594				T1668	T1068	T1672	T1621	T1652		T1005	T1105		T1495
				T1133	T1574	T1480	T1040	T1482		T1039	T1104		T1490
				T1574	T1055	T1211	T1003	T1083		T1025	T1095		T1498
				T1525	T1053	T1222	T1528	T1615		T1074	T1571		T1496
				T1556	T1078	T1564	T1649	T1654		T1114	T1572		T1489
				T1112		T1574	T1558	T1046		T1056	T1090		T1529
						2	T1539	T1135		T1113	T1219		
							T1552	T1040		T1125	T1205		
								T1201			T1102		
								T1120					
								T1069					
								T1057					
								T1012					
								T1018					
								T1518					
								T1082					
								T1614					
								T1016					
								T1049					
						3							
						T1218							
						T1216							
						T1221							
						T1205							
						T1127							
						T1535							
						T1550							
						T1078							
						T1497							
						T1600							
						T1220							

1st Stage
初期感染

メール等による悪意のあるリンクやファイルの実行

外部公開サーバーの脆弱性悪用

漏洩アカウント悪用

不正な内部プログラムの実行（LoTL）

2nd Stage
重篤化

外部通信可能な正規ソフトウェアをインストール（LoTL）

他プロセスへのコード注入

マルウェアの隠蔽（UEFI含む）

セキュリティ機能の無力化（BYOVD）

不正な内部プログラムの実行（LoTL）

3rd Stage
実被害

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取得

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**

データの暗号化/破壊/身代金の請求

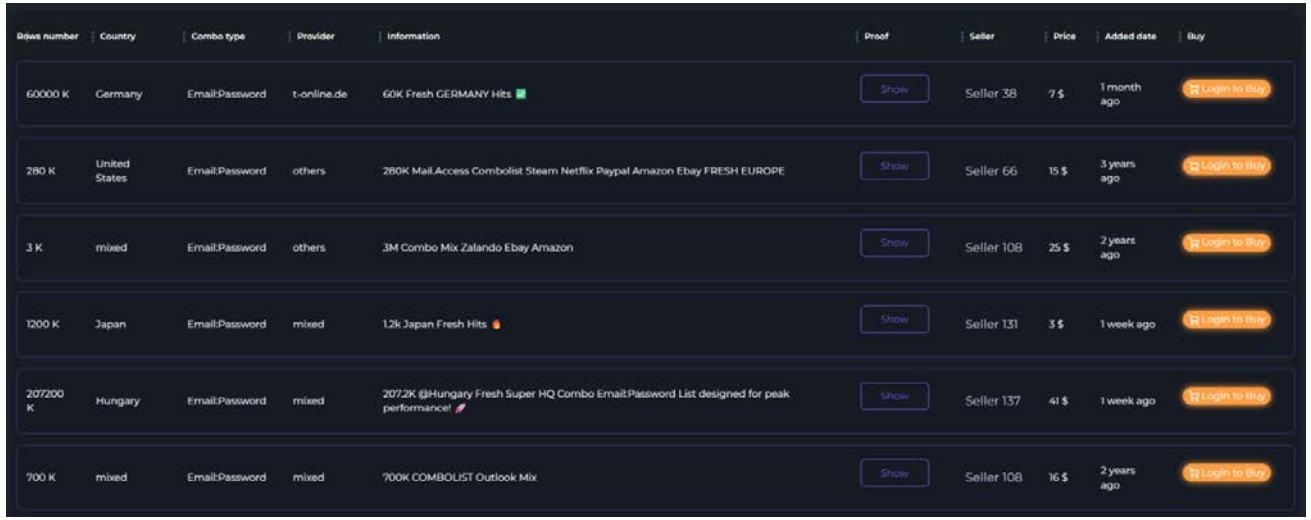
事業妨害型の攻撃ランサムウェアのROIはいかに広く侵入し被害を大きくできるかに依存する

出典：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

インフォスティーラー

従来のマルウェアと同じような感染経路が確認されている

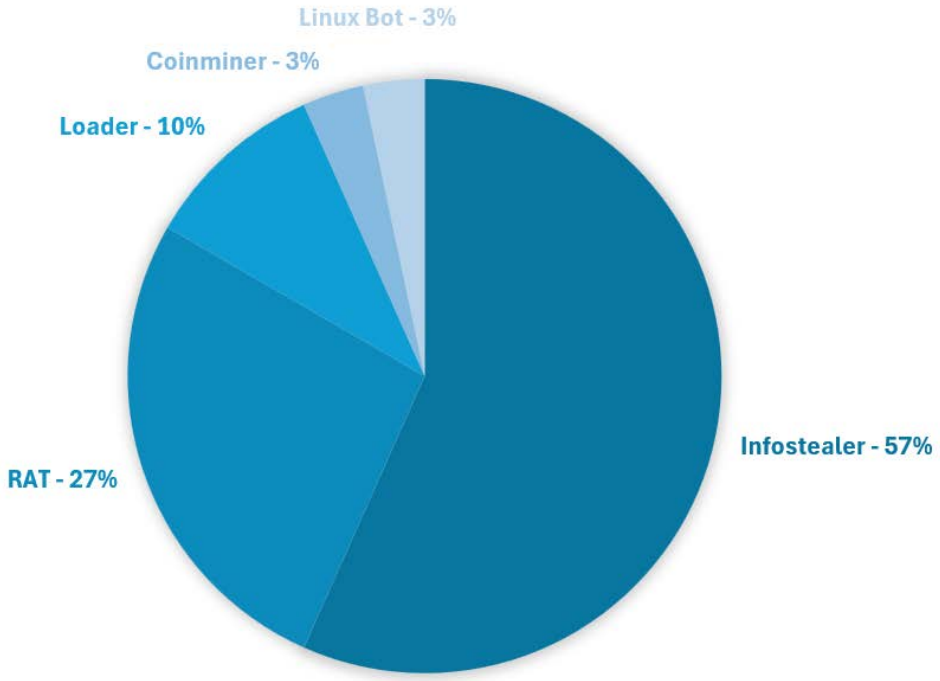
- 感染後、ブラウザ内に保存されたCookieやID/PWなどの認証情報、フォームの自動入力情報などあらゆる情報を窃取する
- 感染後にWebフォームから送信したすべての情報を窃取したりローカルプロキシーのように振る舞うことで暗号化済み通信も盗聴可能
- 認証Cookieを不正に入手した場合、アクティブなセッションを乗っ取り、システムへの不正アクセスが可能。MFA（多要素認証）でもこのケースの保護は提供されない
- 窃取した情報の利用方法
    - 感染デバイスでの直接利用
    - Deep Web/ Dark Webのマーケットで売買される



Rows number	Country	Combo type	Provider	Information	Proof	Seller	Price	Added date	Buy
60000 K	Germany	Email:Password	t-online.de	60K Fresh GERMANY Hits	Show	Seller 38	7 $	1 month ago	Login to Buy
280 K	United States	Email:Password	others	280K Mail.Access Combolist Steam Netflix Paypal Amazon Ebay FRESH EUROPE	Show	Seller 66	15 $	3 years ago	Login to Buy
3 K	mixed	Email:Password	others	3M Combo Mix Zalando Ebay Amazon	Show	Seller 108	25 $	2 years ago	Login to Buy
1200 K	Japan	Email:Password	mixed	1.2k Japan Fresh Hits	Show	Seller 131	3 $	1 week ago	Login to Buy
207200 K	Hungary	Email:Password	mixed	207.2K @Hungary Fresh Super HQ Combo Email:Password List designed for peak performance!	Show	Seller 137	41 $	1 week ago	Login to Buy
700 K	mixed	Email:Password	mixed	700K COMBOLIST Outlook Mix	Show	Seller 108	16 $	2 years ago	Login to Buy

盗まれた認証情報を売買するハッキングマーケットプレイスの広告の例

猛威を振るうインフォスティーラー



2025年第3四半期にMalwareBazaarに提出されたサンプルのマルウェア種別分布

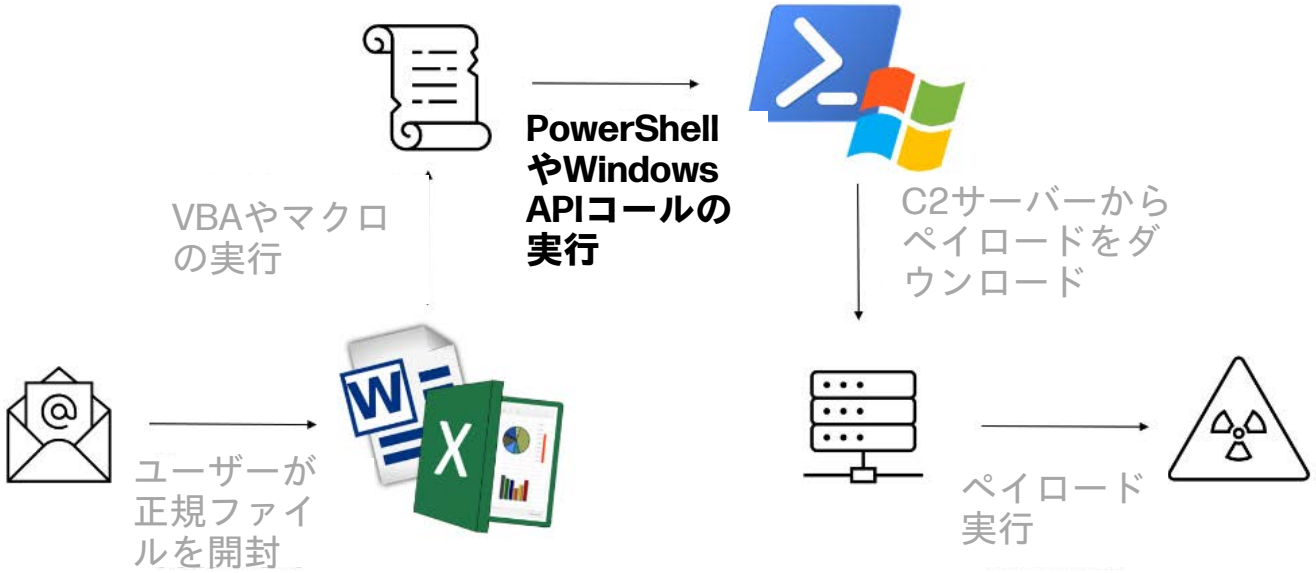
2025年5月ユーロポールとセキュリティチームがLumma Stealerのテイクダウンを実施

Heat map detailing global spread of Lumma Stealer malware infections and encounters across Windows devices.

- Lumma Stealerは古典的なインフォスティーラーで、Webブラウザのセッションから Cookieを抽出し、攻撃者が制御するサーバーへ持ち出すことが可能
- 2025年3月から5月にかけて、Microsoftは世界中で394,000台以上のWindowsコンピュータが本マルウェアに感染していることを確認
- 2025年5月21日、マルウェアのインフラを標的とし、数千のドメインを押収またはリダイレクトするとともに、C&Cサーバーを無効化
- しかしながら、マルウェアの活動は2025年7月に再開されており、攻撃者がインフラを再構築し、マルウェアの配布を再開

LoTLとBYOVD

Living off The Land(LoTL)



PowerShell、WMIなどの正規のツールを使い環境調査（EDRの有無・種類）、権限状況の確認、横展開の可否を判断する

Bring Your Own Vulnerable Driver(BYOVD)

管理者権限の取得

署名済みの脆弱な
ドライバーのロード

自ら設計した脆弱性を突き
カーネルコードを実行

EDR無力化、LSASSの保護解
除により認証情報取得

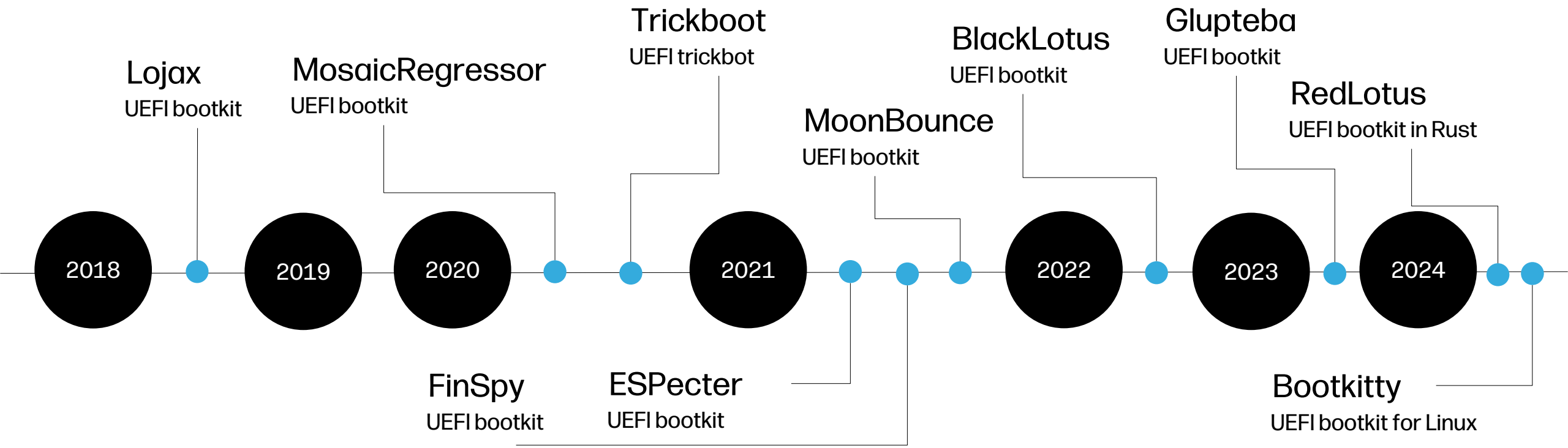
管理者権限でも越えられない“カーネル防御”を破壊し自由に攻撃できる状態を作る

EDRから見えにくくし、最終的に無効化できる攻撃手法が発達

変化するサイバー脅威

もう一つの今日の脅威- ファームウェア攻撃

もう一つの今日の脅威



ファームウェア攻撃が現実化

深刻なファームウェア攻撃の被害

永続性：UEFI/BIOSは回路基板上の不揮発性メモリに存在し、ハードドライブを消去するだけでは削除できません。

制御：UEFI/BIOSは、OSドメインの外で最高特権レベルで実行され、OSに依存しないマルウェアを可能にします。

ステルス性：UEFI/BIOSは、OSおよびシステムソフトウェアが完全にアクセスできないメモリ領域を占有します。アンチウイルスでスキャンすることはできないため、決して検知されない可能性があります。

復旧の難しさ：これらのすべての側面は、システムボードの交換を含むサービスイベントに頼ることなく、この種の感染から回復することを非常に困難にします。

事業妨害型攻撃の永続性の手段として用いられると復旧時の完全性の判断が極めて困難

二次攻撃・被害の長期化

変化するサイバー脅威

検討を開始すべき次の脅威

Post Quantum Cryptography(PQC)

検討すべき次の脅威 – Post Quantum Cryptography(PQC)

- 公開鍵暗号（ RSA/ECC/DSA等 ）の破綻リスク

- 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

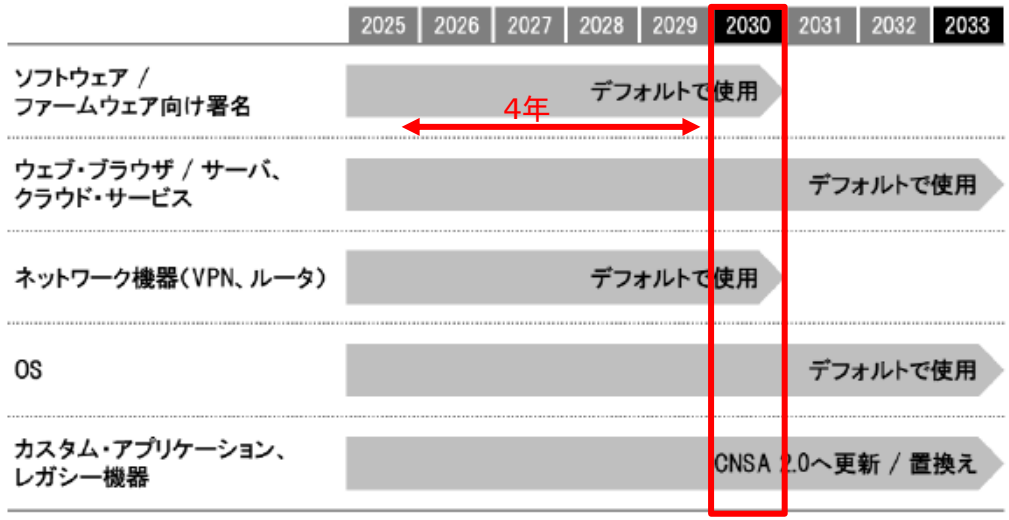
- 長寿命データ（ 個人情報/医療/政府/知財/産業制御ログ ）
  - 特に高リスク
  - OT/ICSや医療、政府記録など“10年以上の秘匿”を要する分野でのリスク顕在化

- 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

*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。

海外・国内のPQC対応のロードマップ

図 3.2　CNSA 2.0 搭載の暗号製品の調達可能時期に関するタイムライン



（備考）Announcing the Commercial National Security Algorithm Suite 2.0 (September 2022) をもとに作成。

出典：預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書

政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）

令和７年 11 月

政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議

≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈≈

４．政府機関等の移行に向けた工程表（ロードマップ）の策定について（検討すべき論点６）

（１）工程表（ロードマップ）の方向性

量子計算機技術については、その進展に伴い、現在広く使われている公開鍵暗号の安全性の低下・危殆化が懸念されている。このような中で、米国や欧州連合（EU）等の諸外国においては耐量子計算機暗号（PQC）への移行についての方針をそれぞれ公表しており、その多くが 2035 年までを期限として進めている。サイバー空間の安全性・信頼性は、情報の秘匿や改ざんの防止、認証等のために用いられる暗号技術の基盤の上で成立しており、国際連携等の観点を踏まえれば、我が国における移行が遅れた場合、サイバーセキュリティや安全保障上の支障も懸念される。

我が国のサイバーセキュリティの確保等のため、政府機関等における耐量子計算機暗号（PQC）への移行について、原則として、2035 年までに行うことを目指し、政府機関等における暗号技術の利用状況等も踏まえ、関係府省庁の連携の下、2026 年度に工程表（ロードマップ）を策定し、我が国における円滑な移行を推進していく。

出典：政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）

変化するサイバー脅威に対応する

今日と次の脅威に備える

/ Windows 11

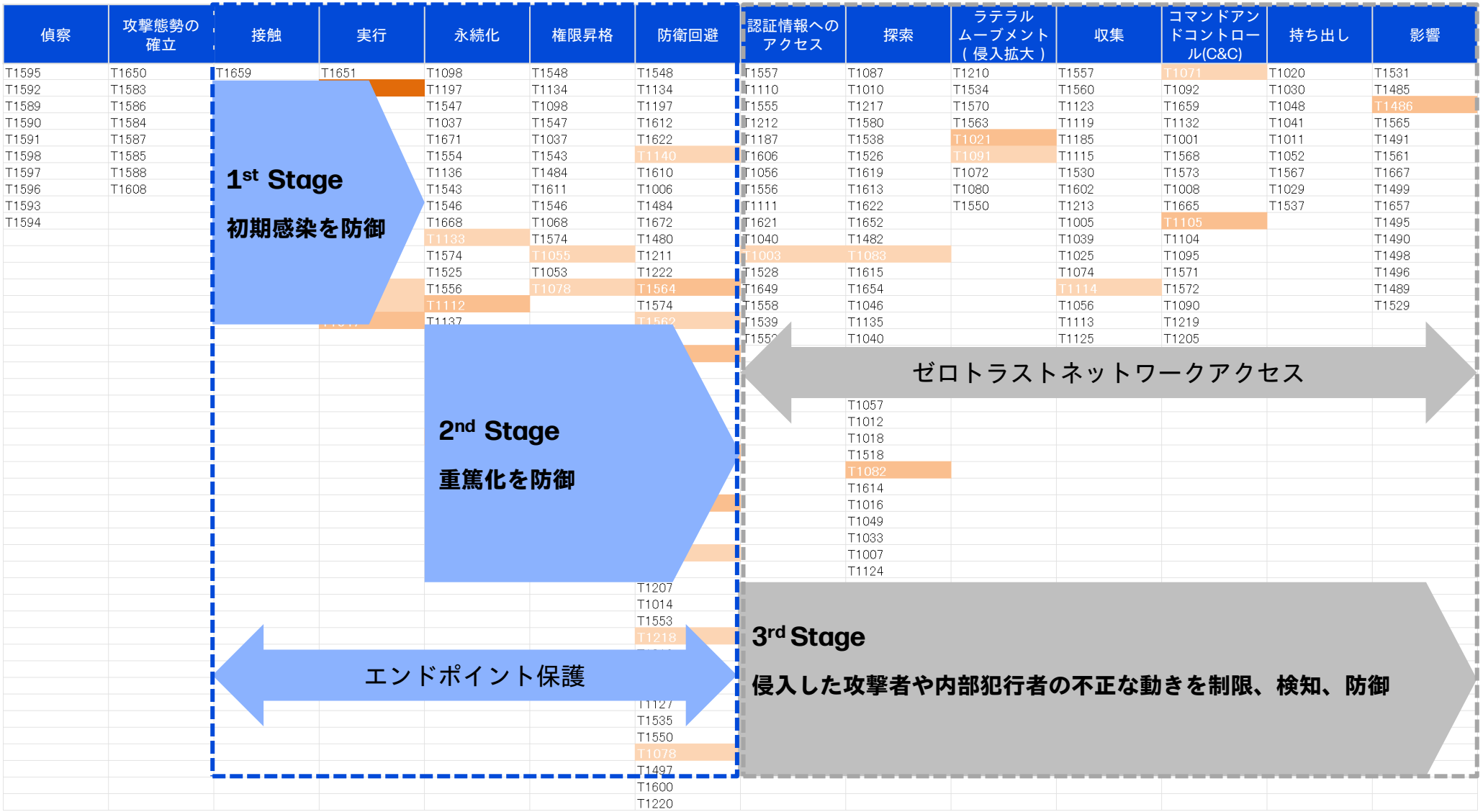
侵入の拡大を防ぎレジリエンスを実現するためのアプローチ

	アプローチ	エンドポイント	ネットワーク
1	基本的保護策と対応 • サイバーハイジーン • 対侵入性の向上		• パッチ対応 • 脅威の検知
2	攻撃者のゲームプランの撹乱 • 攻撃者の作業負荷の増大 • 被害の限定化	• マイクロ仮想化 • 仮想マシンの使い捨て	• マイクロセグメンテーション • 認証の強化
3	システムのレジリエンスの実現 • 攻撃への対応と回復 • サイバー攻撃の予測		• 脅威イベントの集約 • 脅威インテリジェンス • 復旧の自動化、自立化

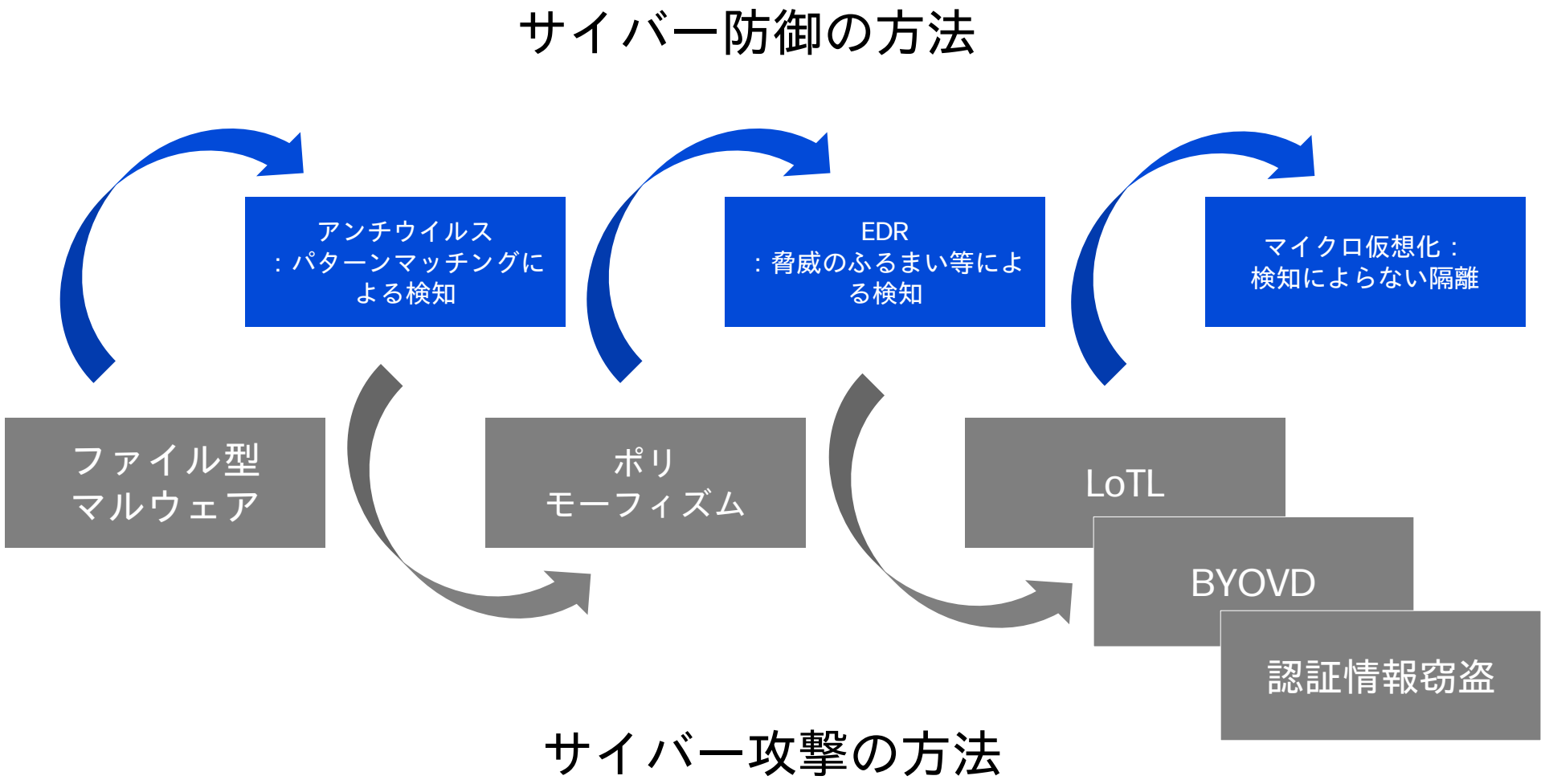
Defending Enterprise Systems from the Inside Out by Ron Ross, computer scientist and Fellow at NIST
https://www.linkedin.com/pulse/defending-enterprise-systems-from-inside-out-ron-ross/ を基に日本HPが作成。

サイバー防御の考え方

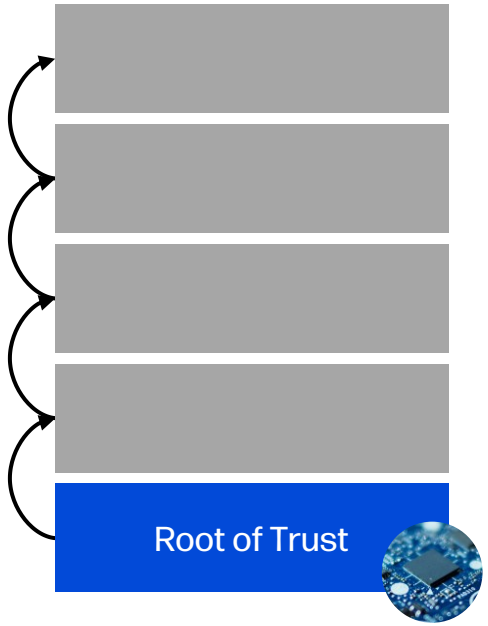
2つのオプション：エンドポイント/ネットワーク



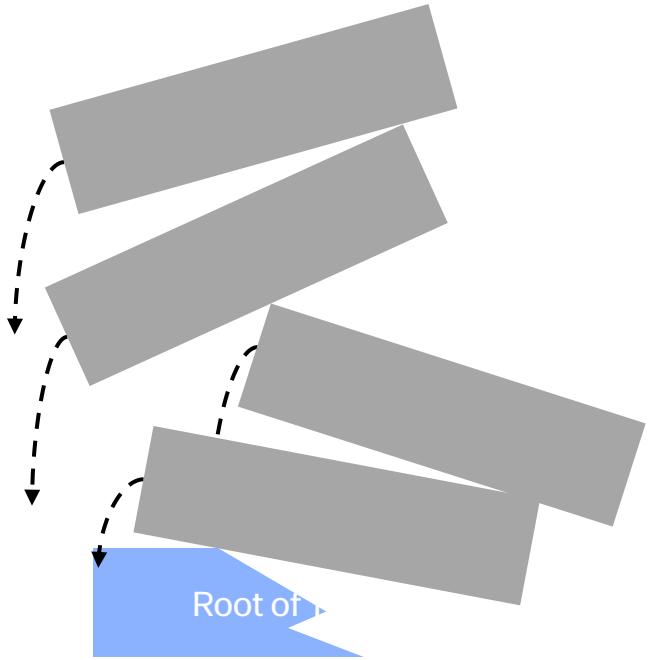
エンドポイントへのサイバー攻撃手法と防御方法の変遷



書き換え不能なシリコンに基づくエンドポイントのレジリエンス



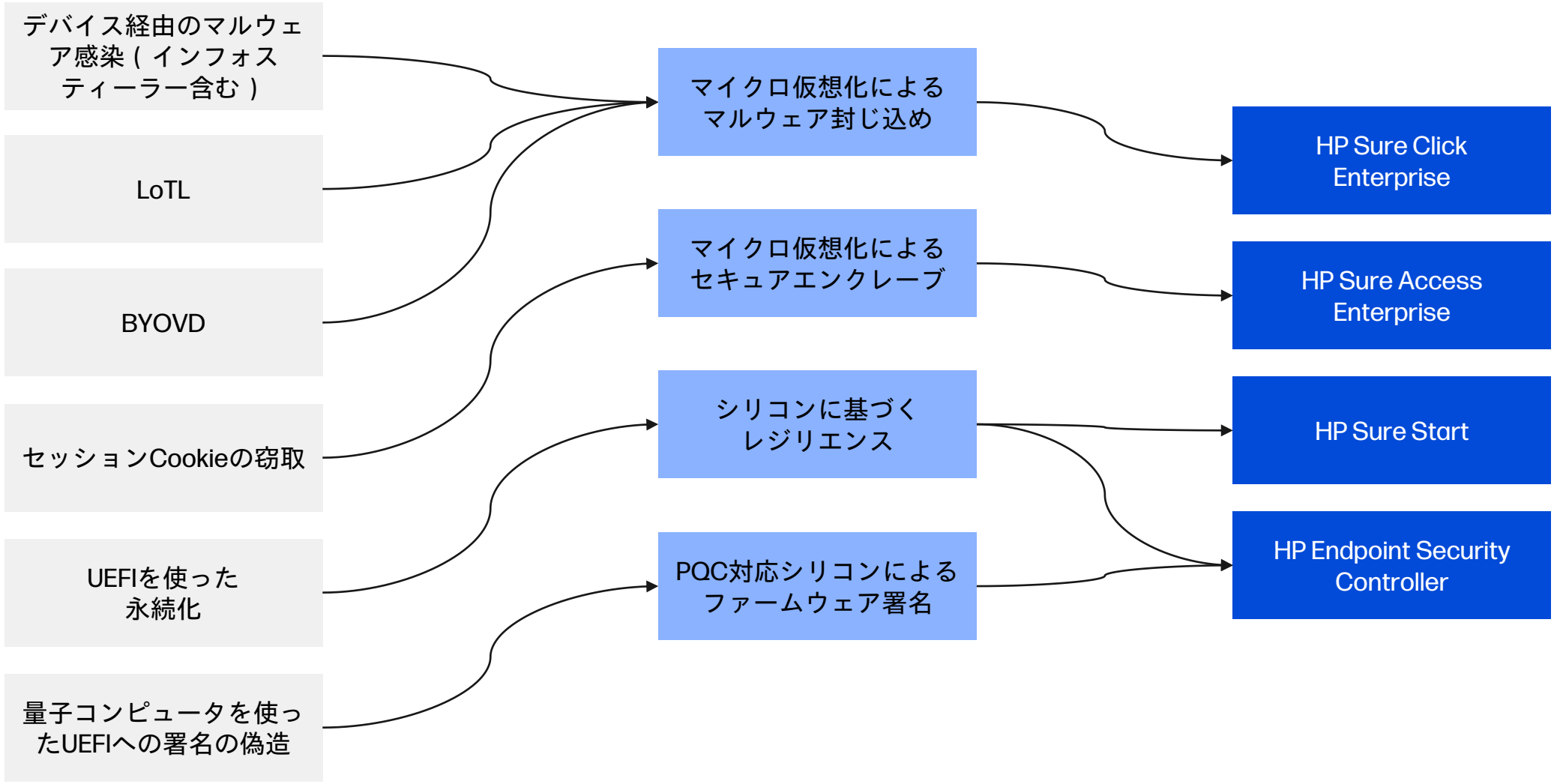
書き換え不能なシリコンに基づくRoot of Trustに基づき復旧したシステムは信頼できる。



Root of Trustが信頼できないと復旧後のシステムが信頼できない。永続化された脅威による2次攻撃のリスクを否定できない。

書き換え不能なシリコンに基づくRoot of Trustを起点にすることにより、**完全性を信頼すること**ができ、**自律的な自動復旧**と組み合わせることで、事業妨害の**被害を最小化**することができる。

サイバー攻撃手法とHPセキュリティソリューションのマッピング



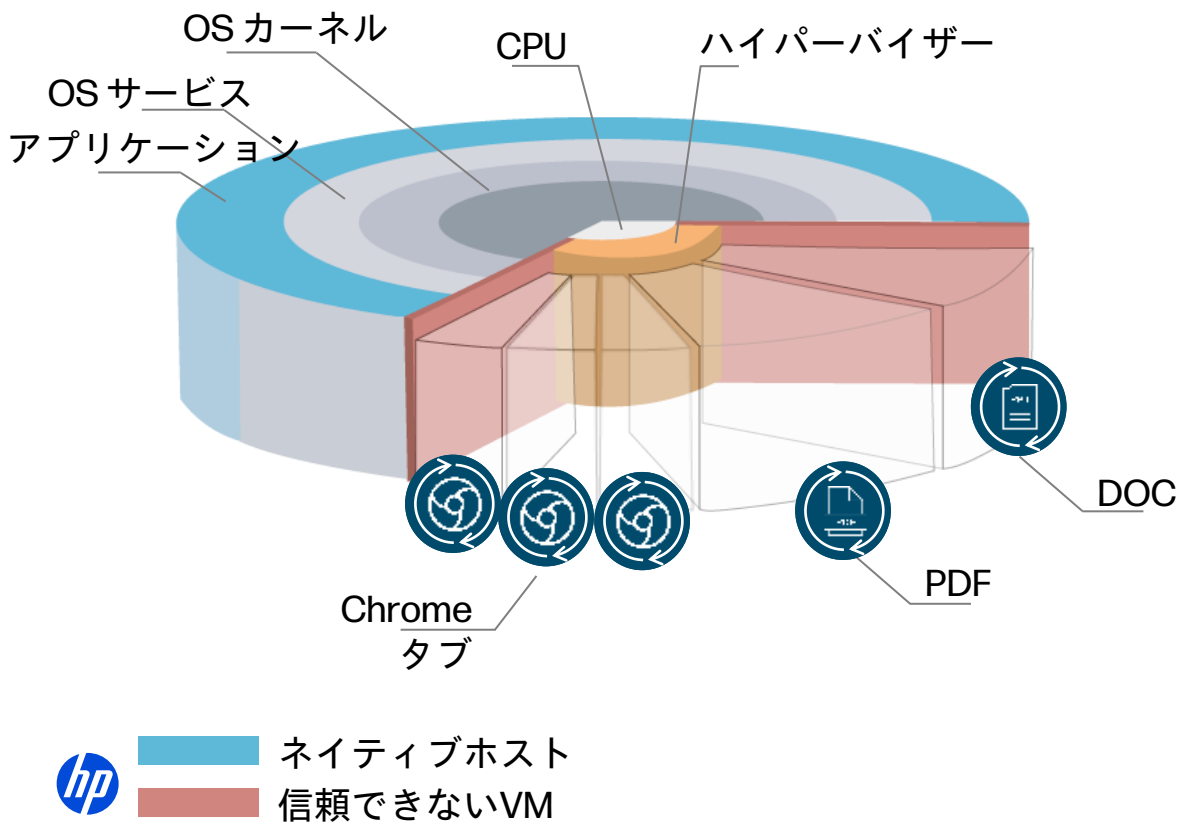
HPセキュリティソリューション

仮想化によるアプリケーション隔離

HP Sure Click Enterprise
他社製含むWindows 11 PCで動くソフトウェアソリューション

エンドポイントのマイクロ仮想化：HP Sure Click Enterprise

テクノロジースタックビュー



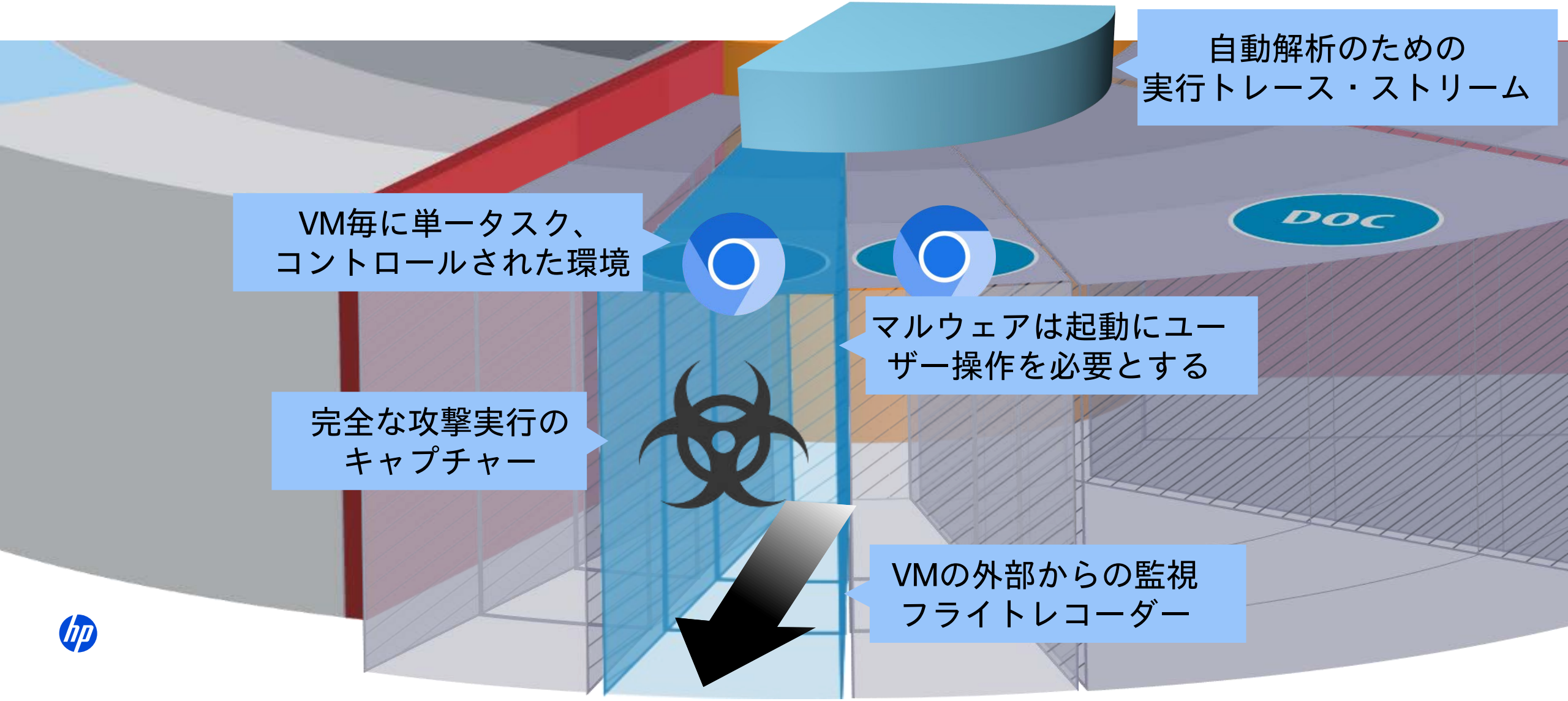
最新のIntel/AMD Windows PCで提供されるCPUハードウェアで強化した仮想化技術を利用。

仮想マシン（VM）をミリ秒単位で生成し、ホスト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。

ユーザーが実行するリスクの高いタスク（Eメールの添付ファイルやWebダウンロードを開く、リンクをクリックするなど）ごとに、新しいVMを作成。

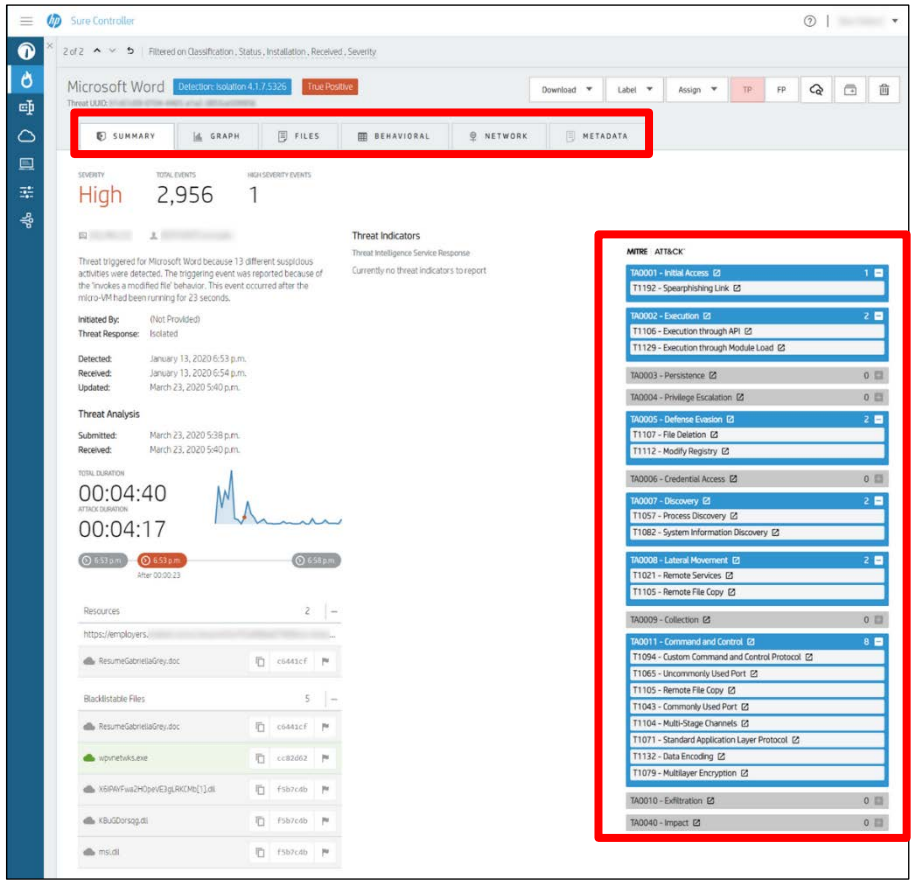
ユーザーエクスペリエンスは何も変わらず、マルウェアは無害化。何も盗めない;横展開できない;永続化できない。

侵害無しのリアルタイム脅威インテリジェンス

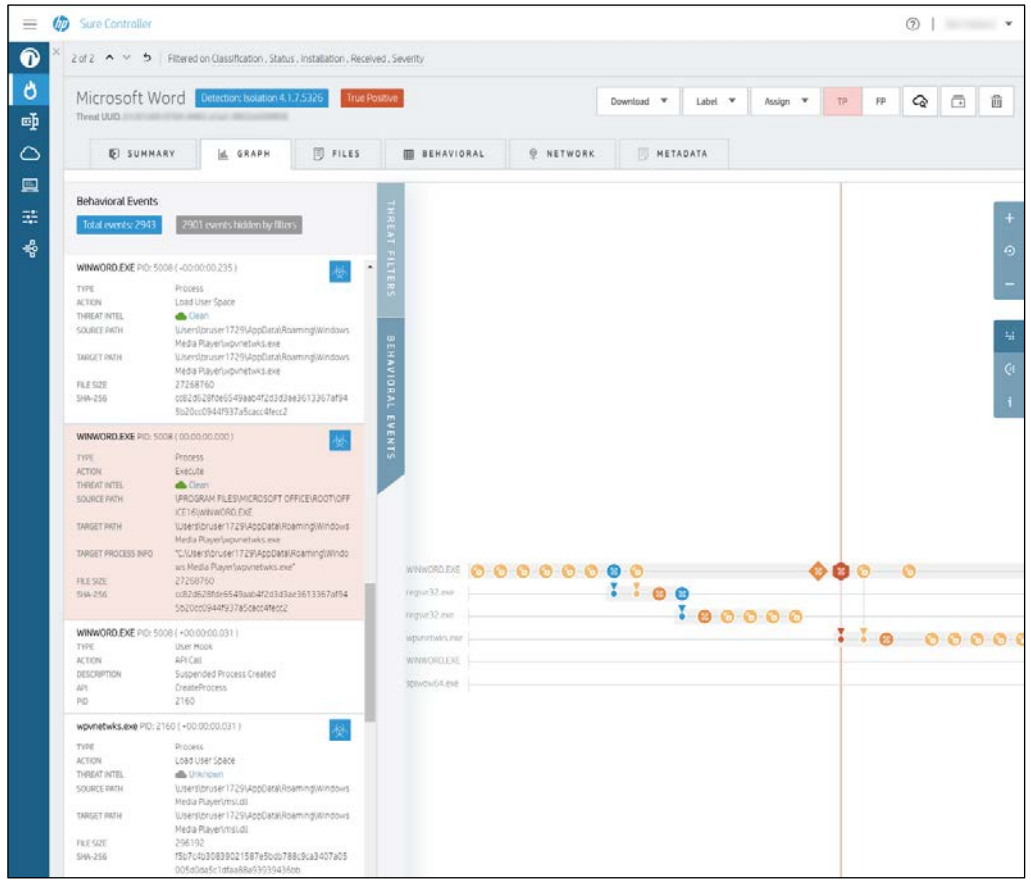


HP Sure Click Enterprise ： Wolf Security Controller

マルウェアペイロード全体とキルチェーンの完全なフォレンジック分析と可視化



サマリータブ
アラートに関する情報の概要

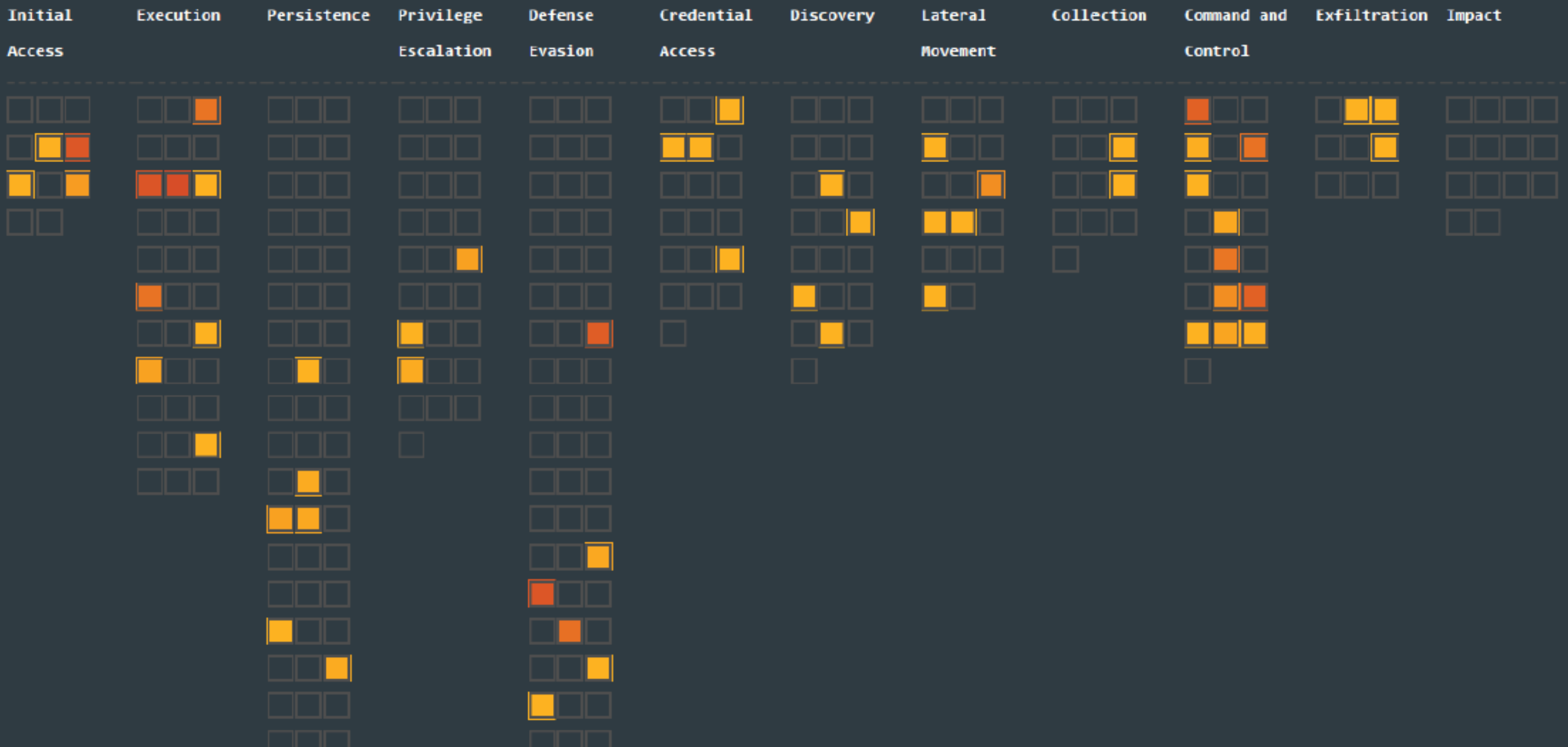


グラフタブ
マイクロVMで発生したイベントがタイムライン表示され、調査者はイベントごとにアクティビティをトレースして詳細を把握

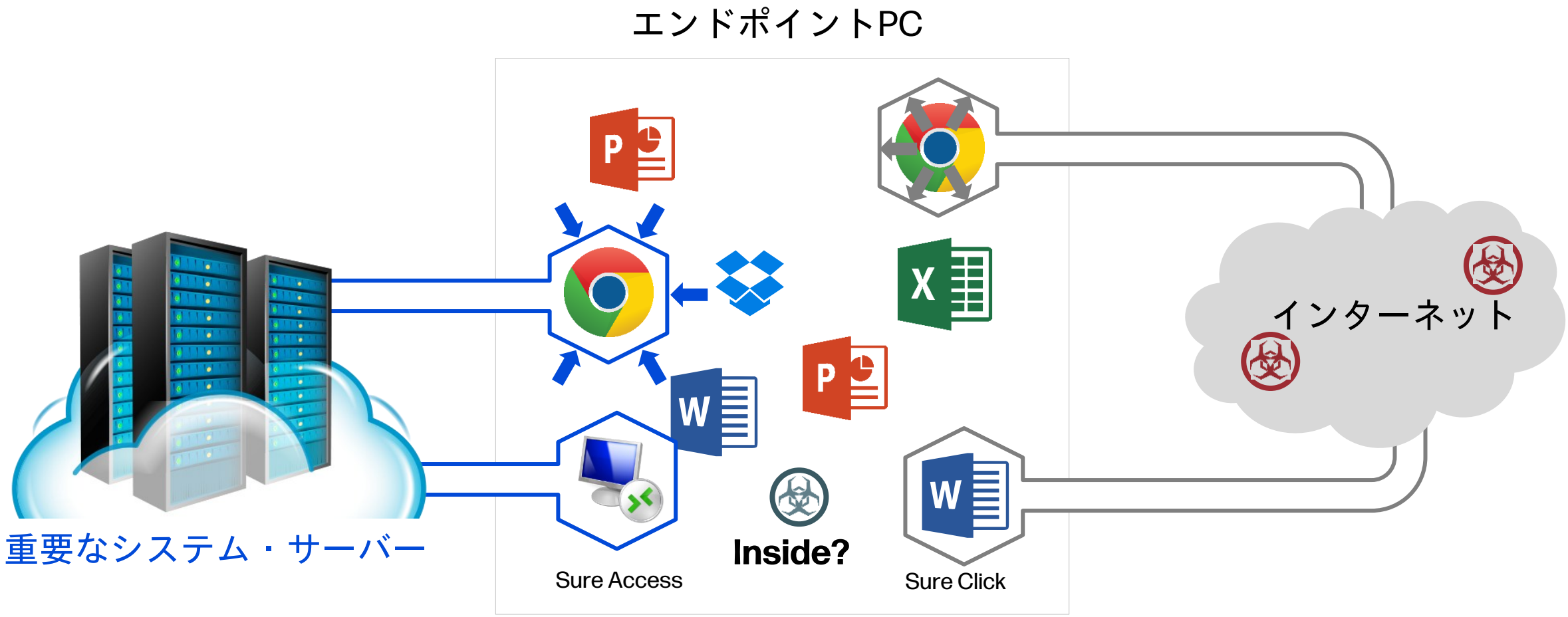
MITRE | ATT&CK™

HP Sure Click Threat Report

4万ユーザを管理する組織　4ヵ月間の脅威レポート



Sure AccessとSure Clickの保護



検知ではなく、**隔離**による保護。
エンドポイントでコンテンツ隔離するための**ハードウェアベースのVM**

HP Sure Access Enterpriseの特長

Sure AccessのProtected VM：

インターセプトまたは注入されたキーストロークを防止

HPのハイパーバイザーは対等的な分離をサポートし、VMをホストOSから保護

実行またはI/O状態へのアクセスを保護

ホストOSが侵害された場合やホスト管理者が悪意を持っている場合でも、保護されたVMの機密性と整合性を保証

表示ウィンドウのスクリーンショットを禁止

保護されたVMへのセキュアなIOパスは、キーのログ記録やキーの注入、画面のスクレイピングを防ぎ、安全なストレージとネットワークを実装

ハードウェアのルート証明を使用して保証された構成証明と暗号化を施した隔離VMを利用

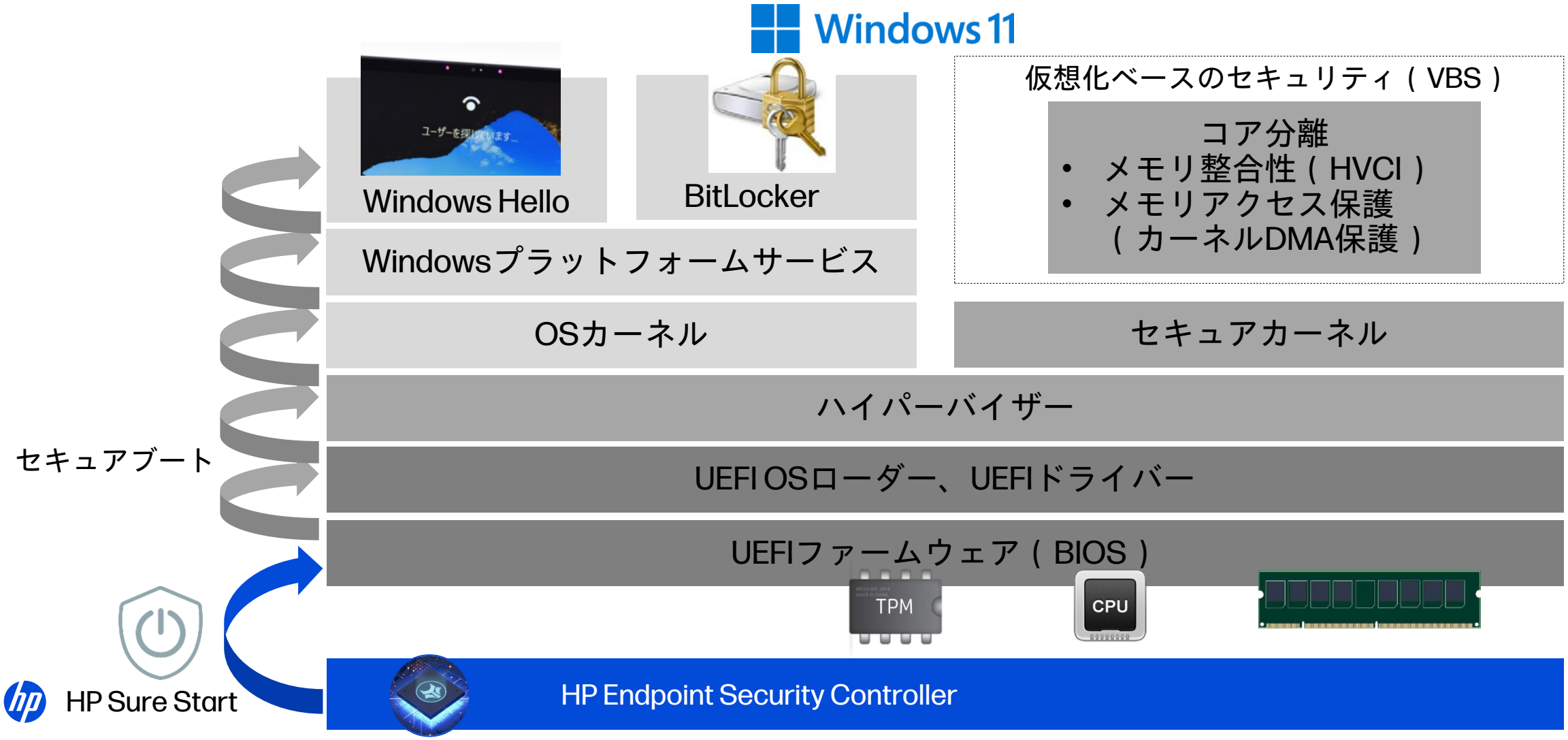
HPセキュリティソリューション

シリコンに基づくファームウェアのレジリエンス

HP Endpoint Security Controller & HP Sure Start
一部を除くすべてのHPビジネスPCの標準機能

/ Windows 11

HP Endpoint Security ControllerをRoTとするセキュアブート

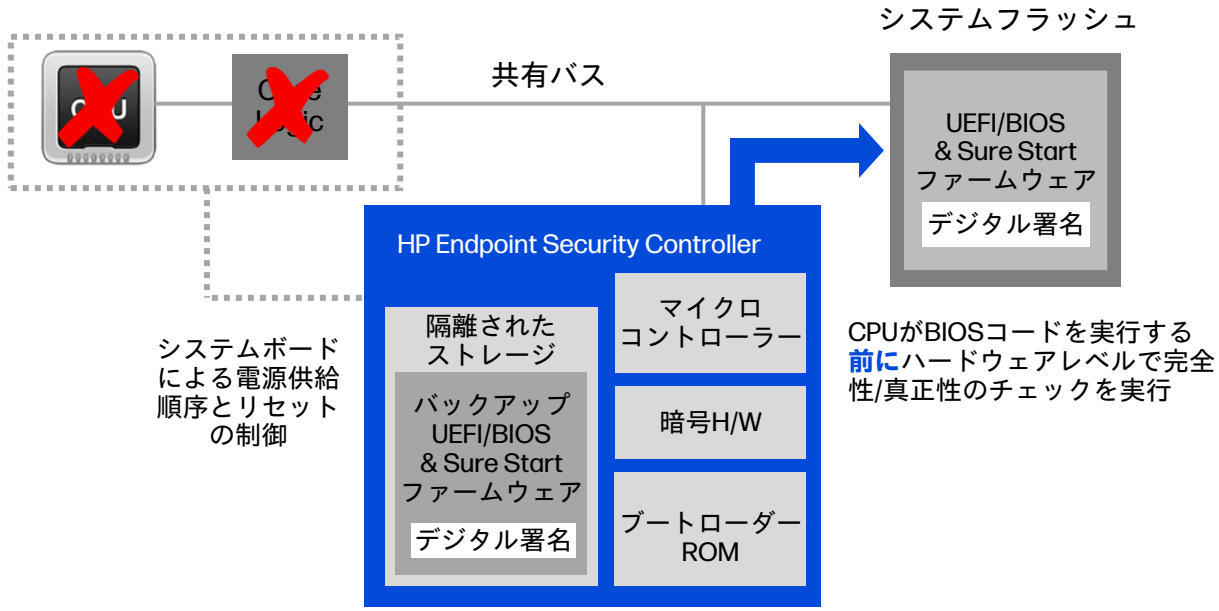


HP Sure Startによるファームウェアのレジリエンス

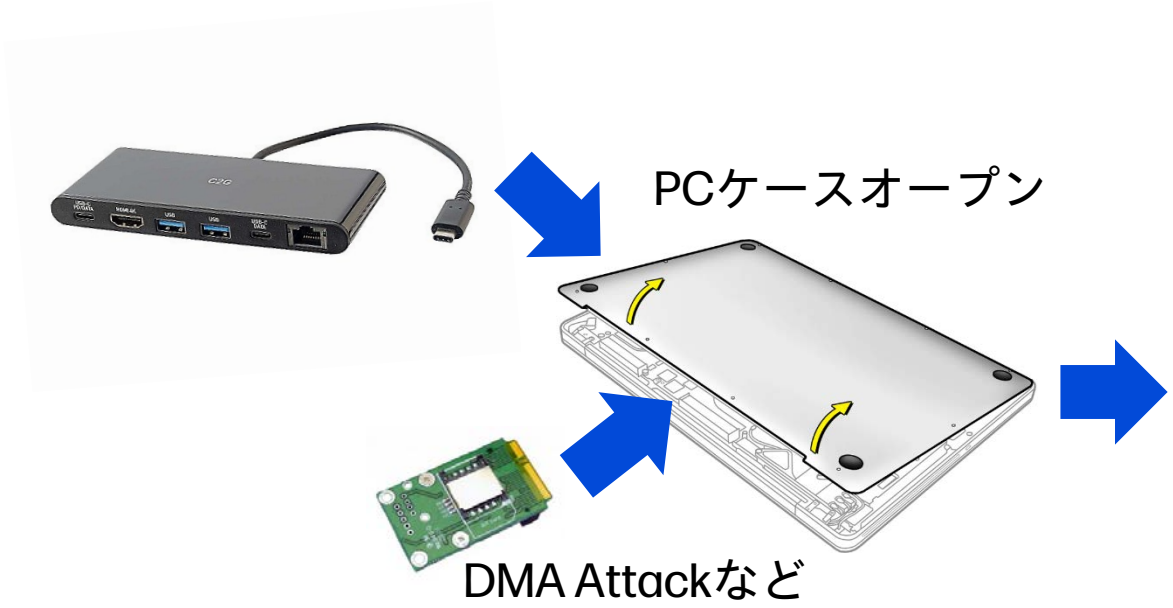
機能	NIST要件	HP Sure Start
ルート・オブ・トラスト	必須	●
書き換え可能コードの保護とアップデート	必須	●
書き換え不能コードの保護	必須	●
重要プラットフォームFWのランタイム保護	必須	●
重要データの保護	必須	●
破損コードの検知	必須	+
重要データの破損の検知	必須	●
書き換え可能コードの復旧	必須	●
重要データの復旧	必須	+
ロギングと通知	オプション	+
ポリシーベースの制御	オプション	+
自動か手動の復旧オプション	オプション	+
ローカルかリモートの復旧	オプション	+
ロールバックの阻止	オプション	+
ランタイム侵入検知	未定義	+
物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

NIST要件を超えた項目

● NIST要件を満足
＋NIST要件を超える



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る。
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。

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セキュリティソリューション

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

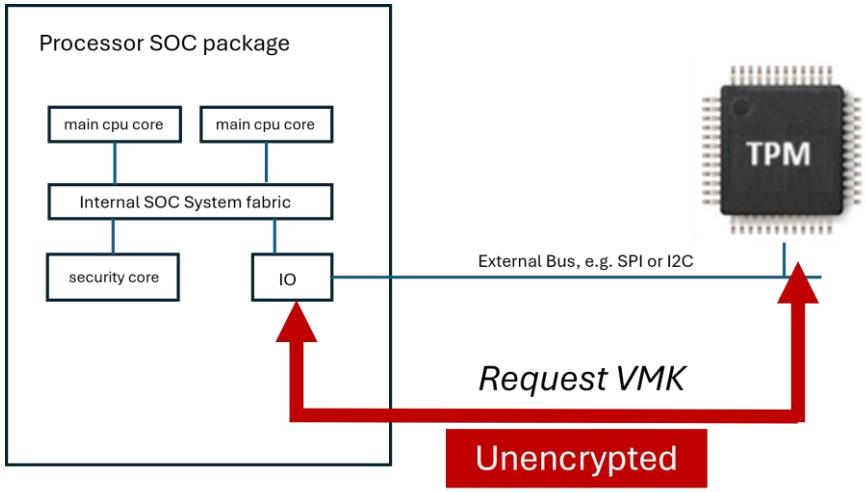
最大
48 TOPS[6]
Copilot+PC

intel CORE ULTRA

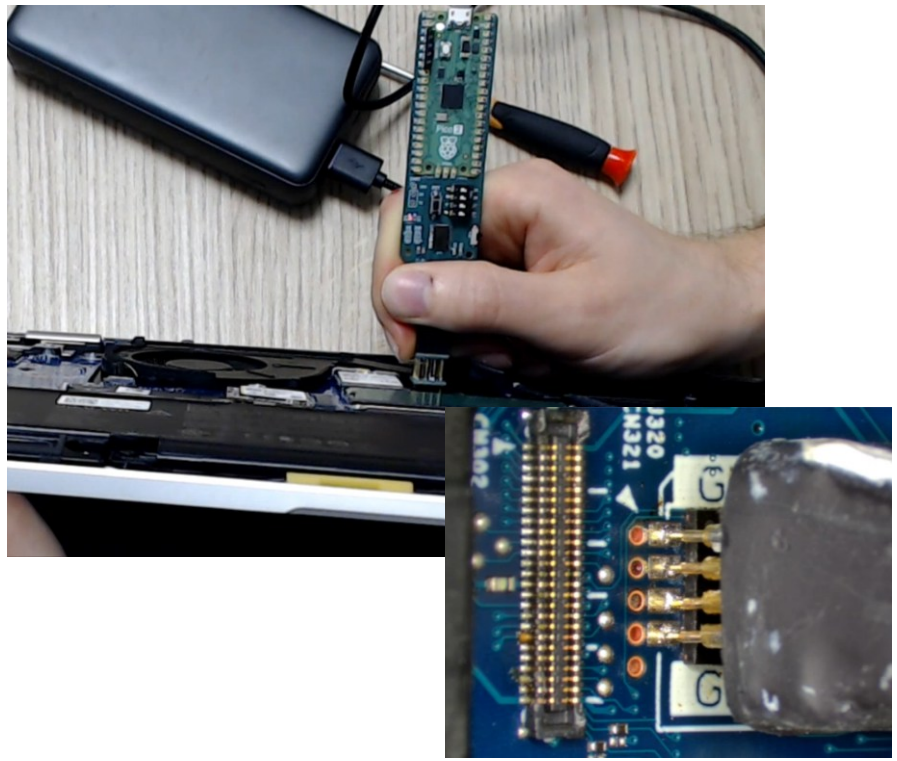
ポータブル
スタイリッシュ
多機能

hp / Windows 11

Why worry about TPMs?

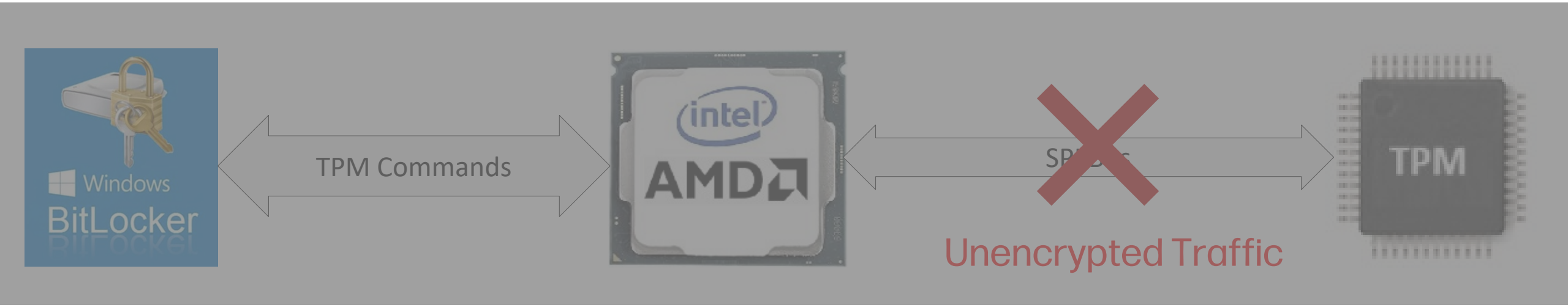


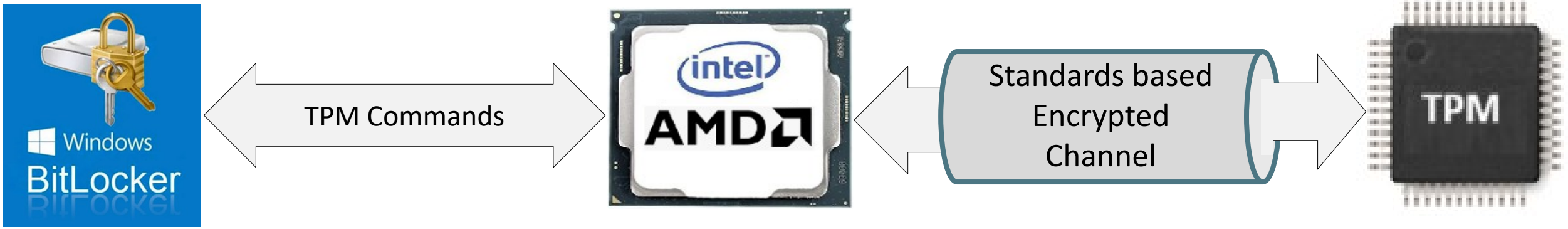
VMK is the Volume Master Key, used to unlock BitLocker.



Key gone in how many seconds??

TPM Guard: High-level Architecture





Appendix

セキュアな調達仕様

調達仕様によりエンドポイントのセキュリティを確保する

組織は、常に次の2つを明確に理解し、調達仕様をアップデートする必要があります：

- エンドポイントデバイスの調達に必要な最小限のセキュリティベースライン
- エンドポイントセキュリティとレジリエンスが戦略的優先事項である場合に優先的に考慮すべき最先端の技術

1. ベンダーのセキュリティを作り込む組織的体制を確認する要件
2. Windows 11のセキュリティ機構を保護するための機能要件
3. ハードウェアプラットフォーム（H/W、F/W）のレジリエンスを強化する機能要件
4. 製品ライフサイクルを通じての安全性と保守性を確保するための機能要件

Thank You