



エンドポイントは“検知”から“設計”へ —HPのハードウェア起点のセキュリティの歩み

株式会社日本HP

セキュリティエバンジェリスト 木下和紀エドワード



/



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を担当。
- ・ 2024年、日本HP セキュリティ エバンジェリスト就任

2025年の 攻撃手法の振り返り



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							
						T12							



分解 & 分析

ステージごとの手法



偵察	武器化	初期アクセス	実行	持続化	権限昇格	回避	認証情報	インフラ探索	横移動	資産探索	統制	持ち出し	インパクト
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	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	T1098	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

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

T1221
T1205
T1127
T1535
T1550
T1078
T1497
T1600
T1220

2025年後半の3つの ケーススタディー

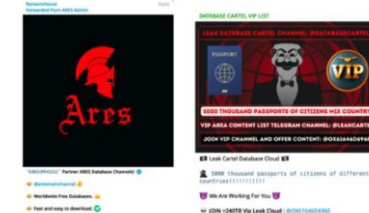
Aホールディングス

- 2ヶ月超のシステム停止により事業販売が2割以上減、決算にも遅れ
- Qilin RaaSによる攻撃



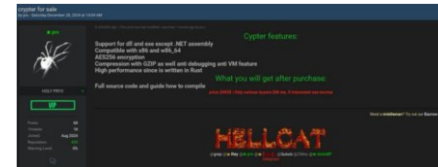
A社

- 2ヶ月超のシステム停止により売上高95%減
- RansomeHouse RaaSによる攻撃



J社 (イギリス)

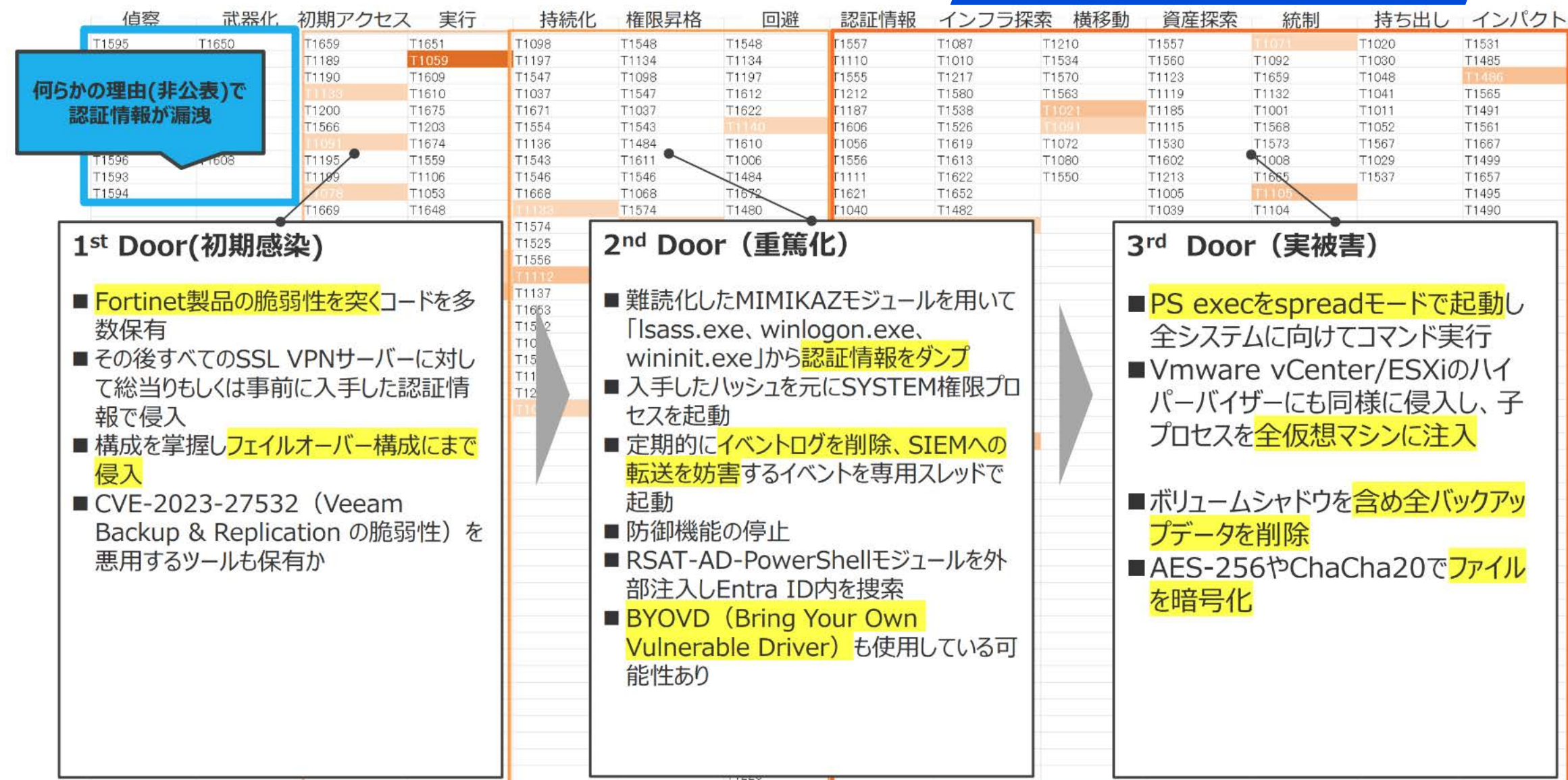
- 1ヶ月超のシステム停止により4000億円の経済損失を生み決算は赤字転落
- HELLCAT RaaSによる攻撃



共通するサイバー攻撃のパターン
インフォスティーラー + LoTL/BYOVDを使ったランサムウェア攻撃

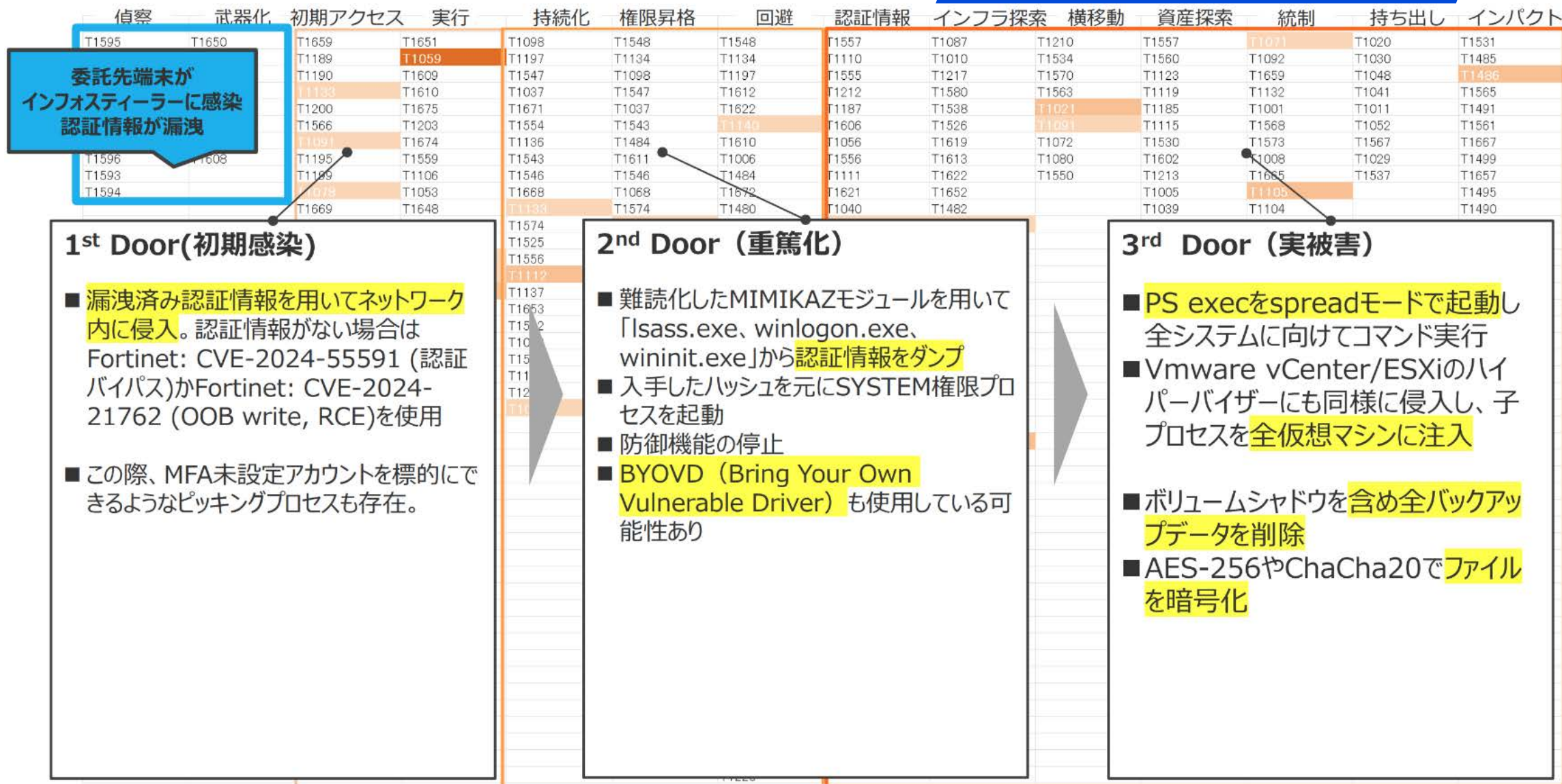
分解 & 分析

A HDを攻撃したとされるQilinが用いる典型的な攻撃パターン



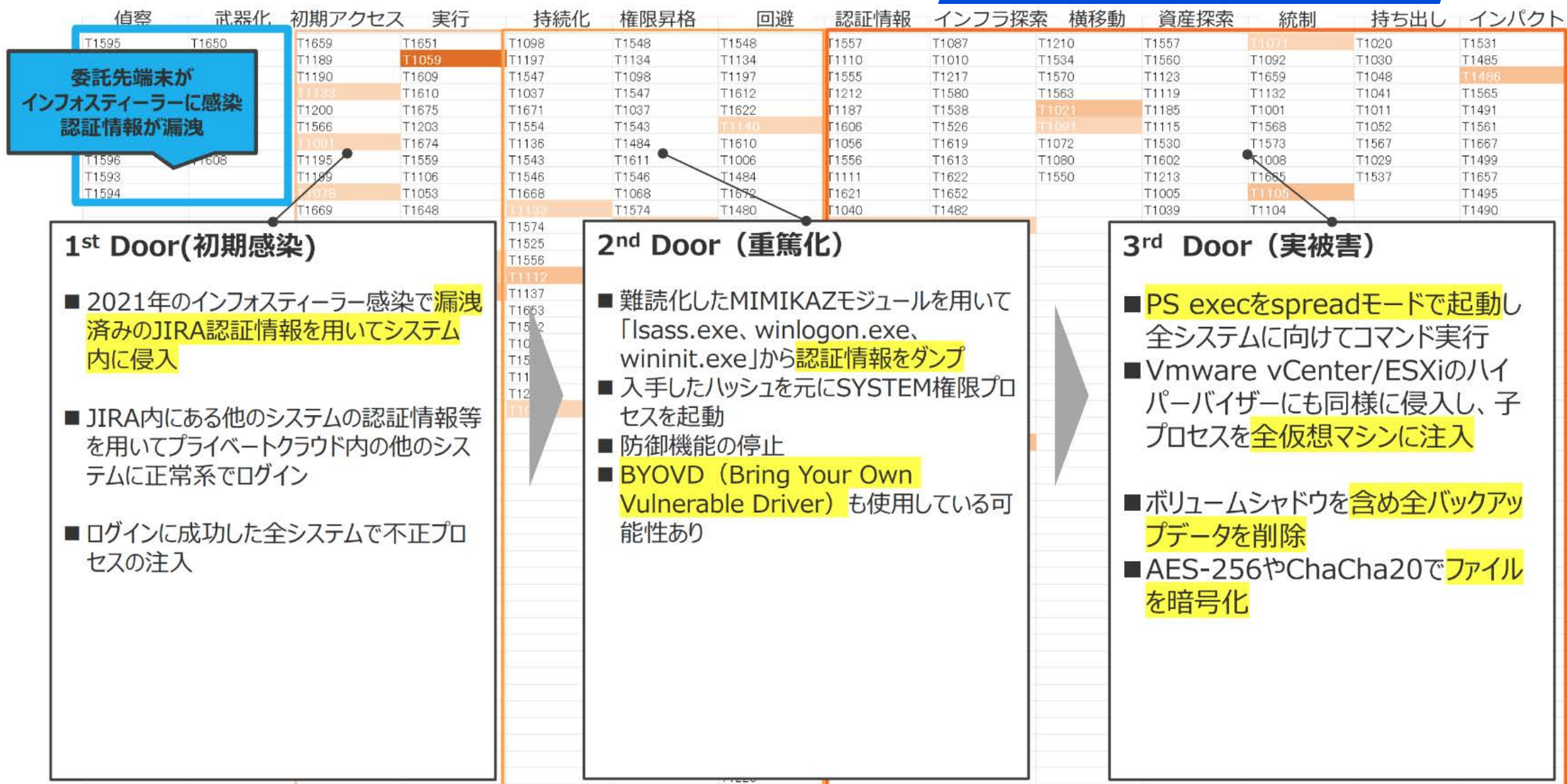
分解 & 分析

A社を攻撃したとされるHELL CATが用いた攻撃パターン

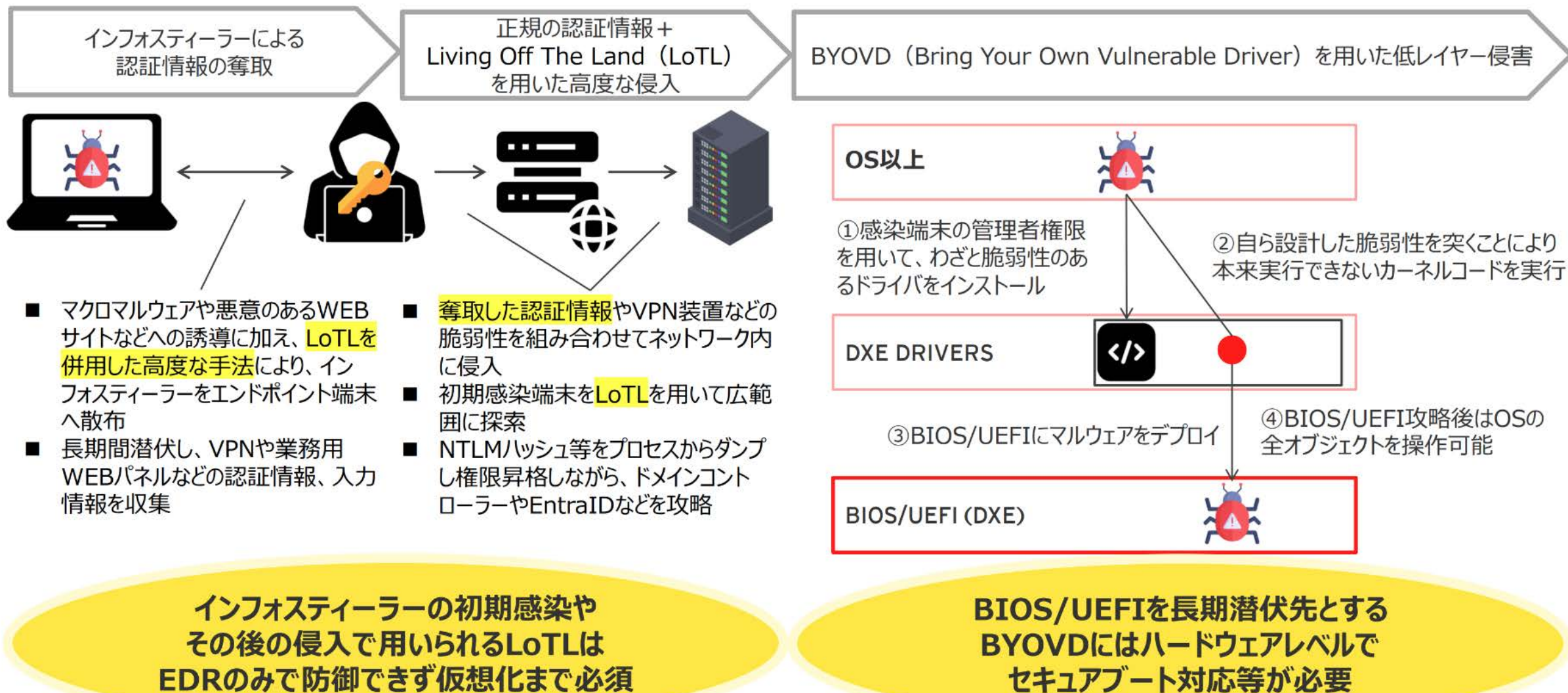


分解 & 分析

J社を攻撃したとされるHELL CATが用いた攻撃パターン



最新のランサムウェア攻撃は インフォスティーラー型 + LoTL/BYOVD



漏洩アカウントの優位性



Infostealerとは



Generated by Whisk

従来のマルウェアと同じように以下のような感染経路が確認されている

1. メールの添付ファイルによる感染
2. メールやWEBサイトに記載されたリンクからの感染
3. WEBの不正な広告を経由した感染
4. 偽のソフトウェアインストーラー/アップデートファイルによる感染

また、新たな感染経路として、ClickFixという手法が発達している

Complete these Verification steps

To prove you are not robot, please:

1. Press **Windows Key** + **R**.
2. In the verification window, press **Ctrl + V**.
3. Press **Enter** on your keyboard to finish

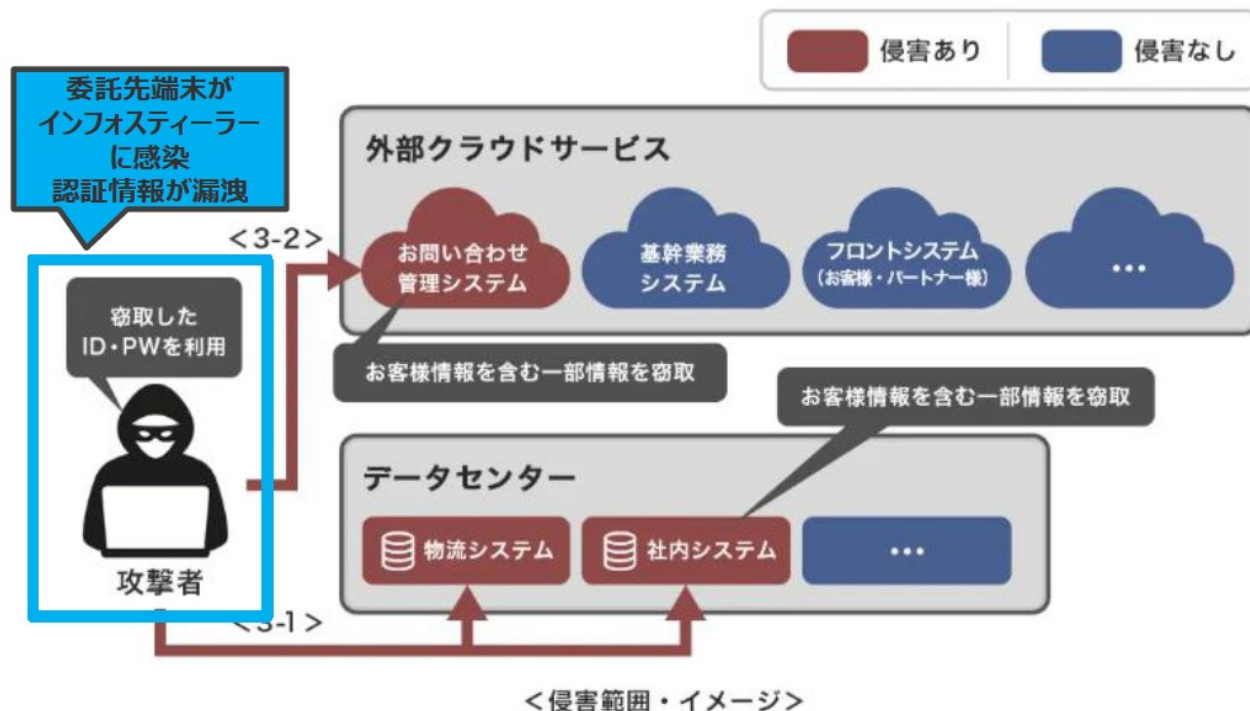
Perform the steps above to finish
verification

VERIFY

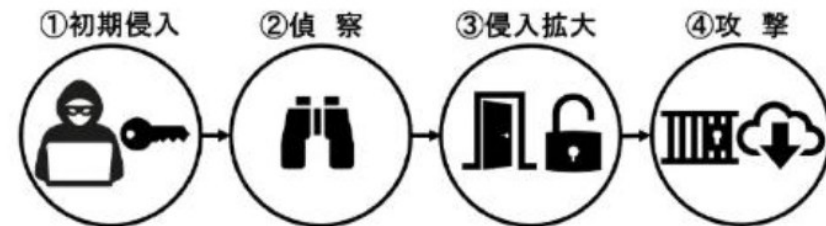
人間による操作かどうかを検証すると称して、不正なPowerShellスクリプトを手動で実行させる

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
ローカルプロキシのように振る舞うことで暗号化済み通信も盗聴可能
窃取した情報は直接利用されるか、Deep Web/ Dark Webのマーケットで売買される

漏洩済みアカウントを利用した攻撃



典型的なインフォスティーラー型攻撃

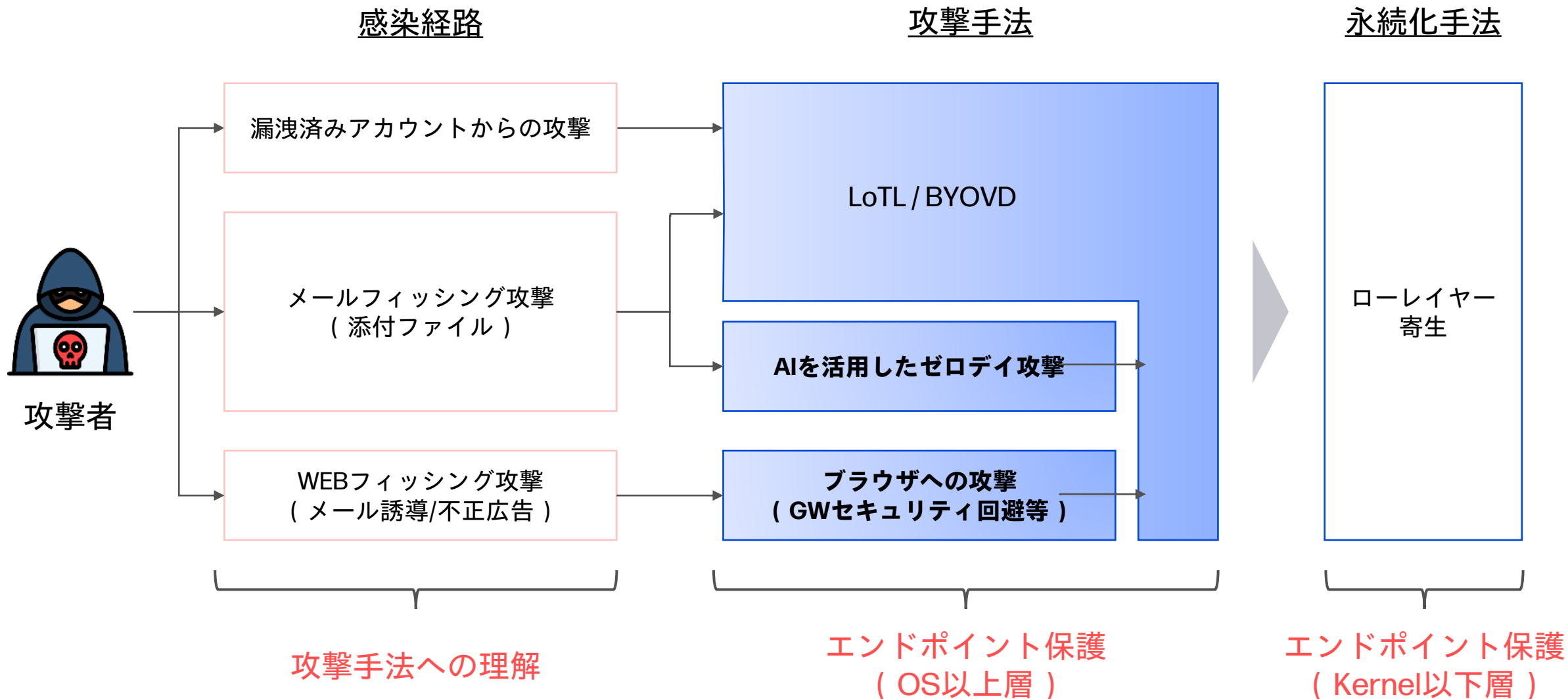


時期	2025/6/5	2025/6 ~ 2025/10/9	2025/7/9 ~ 2025/10/19	2025/10/19 ~
概要	業務委託先用のアカウントを使用して社外より初期侵入	管理者権限等の取得を目標としたログイン試行(全て失敗)	脆弱性対策ソフトを無効化したうえで物流システムおよび社内システム、端末に侵入拡大し、ランサムウェア配置	事前設定された時刻にランサムウェアが起動し、サーバ暗号化、ファイル削除、クラウド情報窃取

- 攻撃者は、EDR等の脆弱性対策ソフトを無効化したうえで複数のサーバ間を移動し、必要な権限を取得してネットワーク全体へのアクセス能力を取得していきました。
- なお、本件では複数種のランサムウェアが使用されました。この中には、当時のEDRシグネチャでは、検知が難しいランサムウェアも含まれていました。

PRタイムズ記事より引用

LOTLという攻撃手法



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。。。



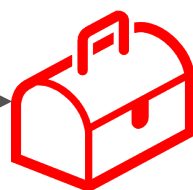
攻撃者



1st Stager



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。

EDRの無効化

Cyber Security News

Qilin Ransomware Uses Malicious DLL to Kill Almost Every Vendor's EDR Solutions

By [Guru Baran](#) - April 2, 2026

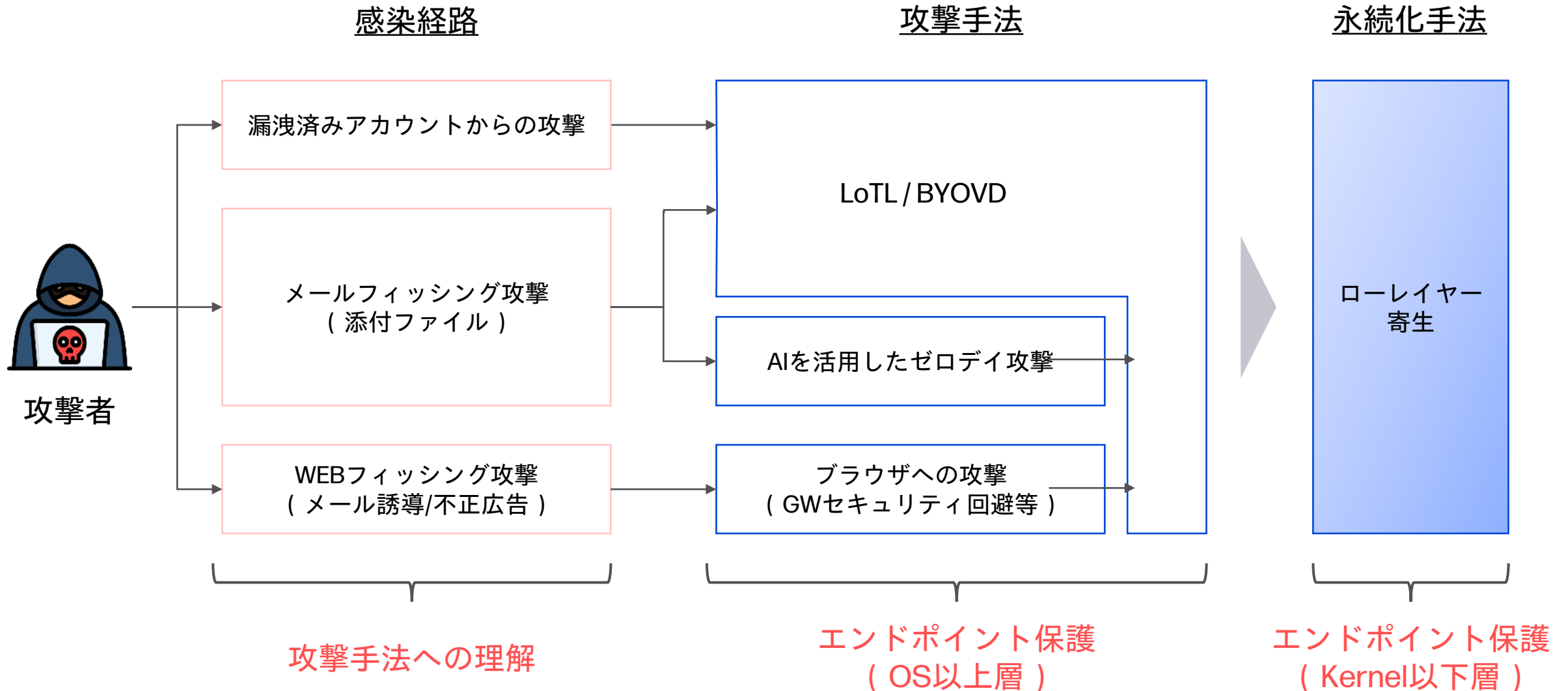


「最新のランサムウェアは、防御システムそのものを先に無力化してから攻撃してくる段階に入っています。」

[Qilin ransomware group](#) is deploying a sophisticated, multi-stage infection chain via a malicious msimg32.dll that can disable over 300 endpoint detection and response (EDR) drivers from virtually every major security vendor.

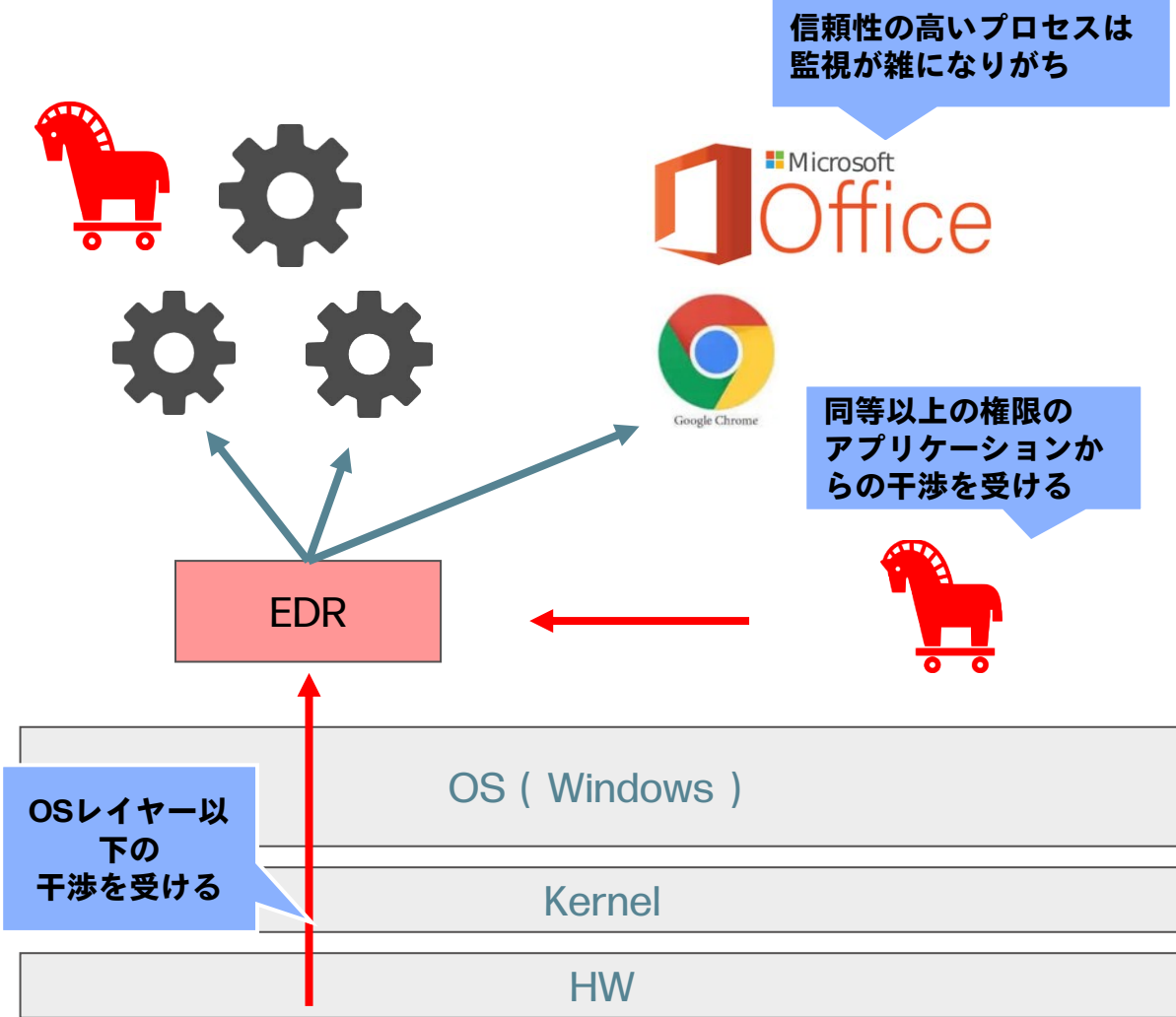
<https://cybersecuritynews.com/qilin-ransomware-kill-edr/>

永続化手法

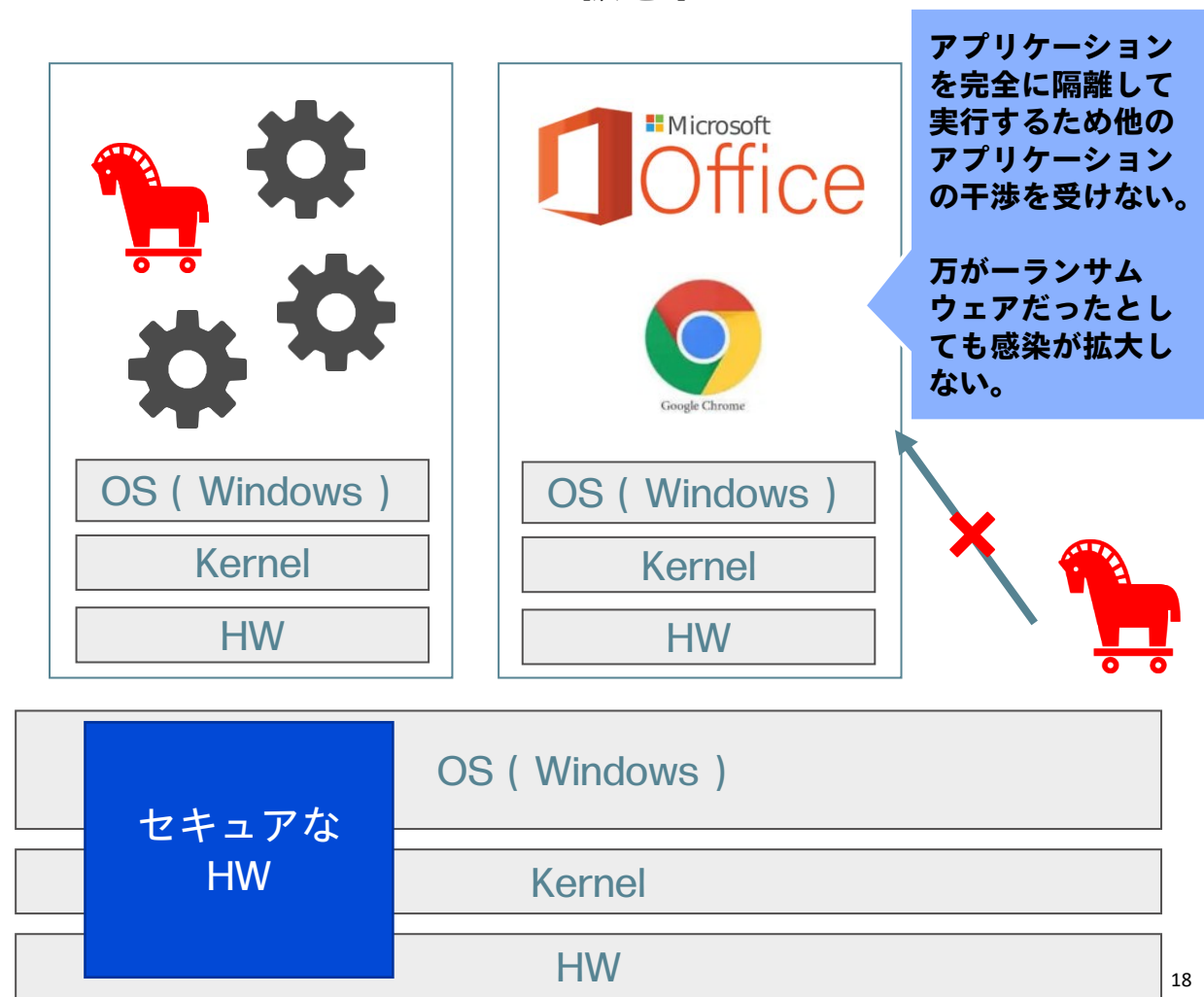


EDRと仮想化とHW

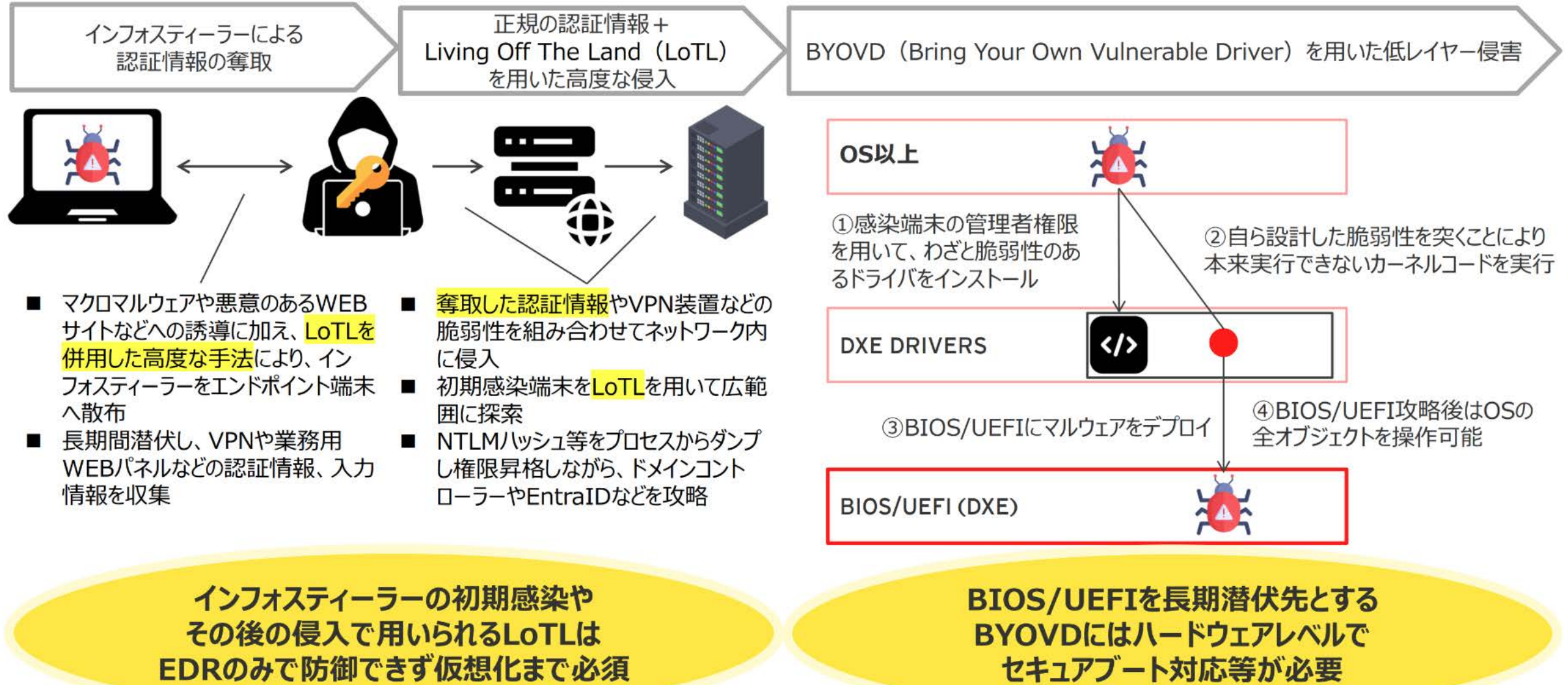
EDR



仮想化



最新のランサムウェア攻撃は インフォスティーラー型 + LoTL/BYOVD



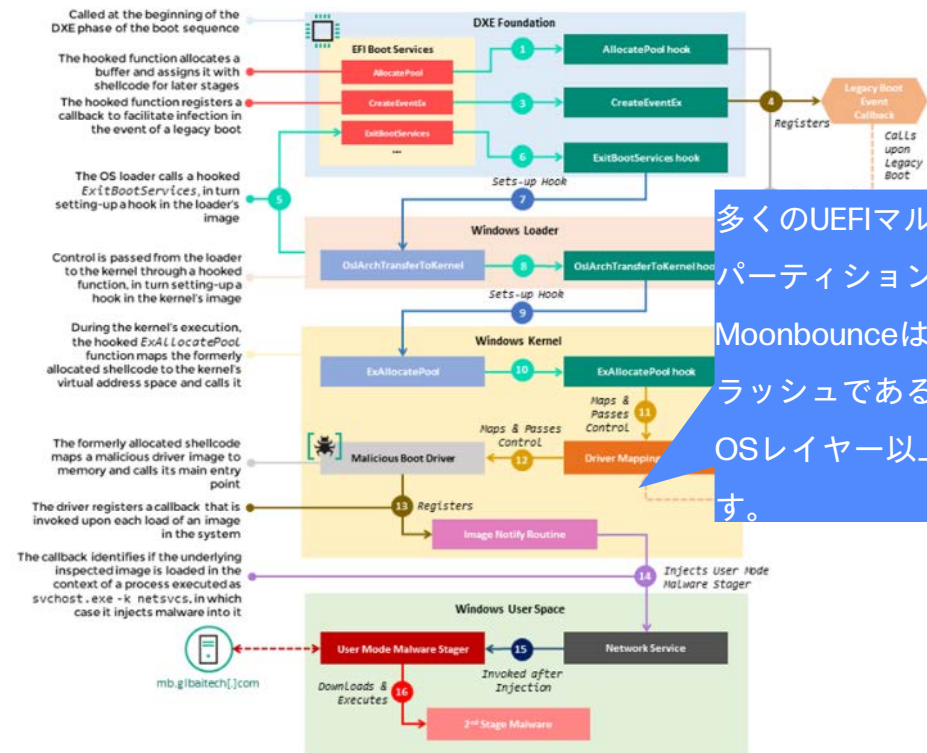
ローレイヤー攻撃対策

- HW ソリューション -



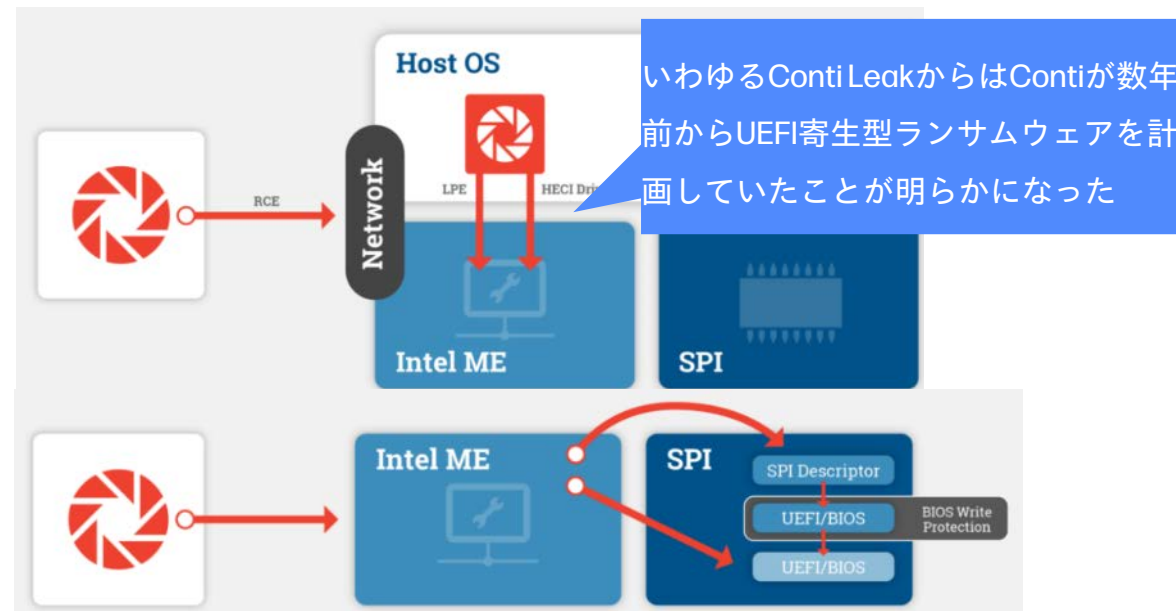
ローレイヤー領域への攻撃

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



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。

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)

TPM

CPU

NPU

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

ファームウェアのレジリエンス

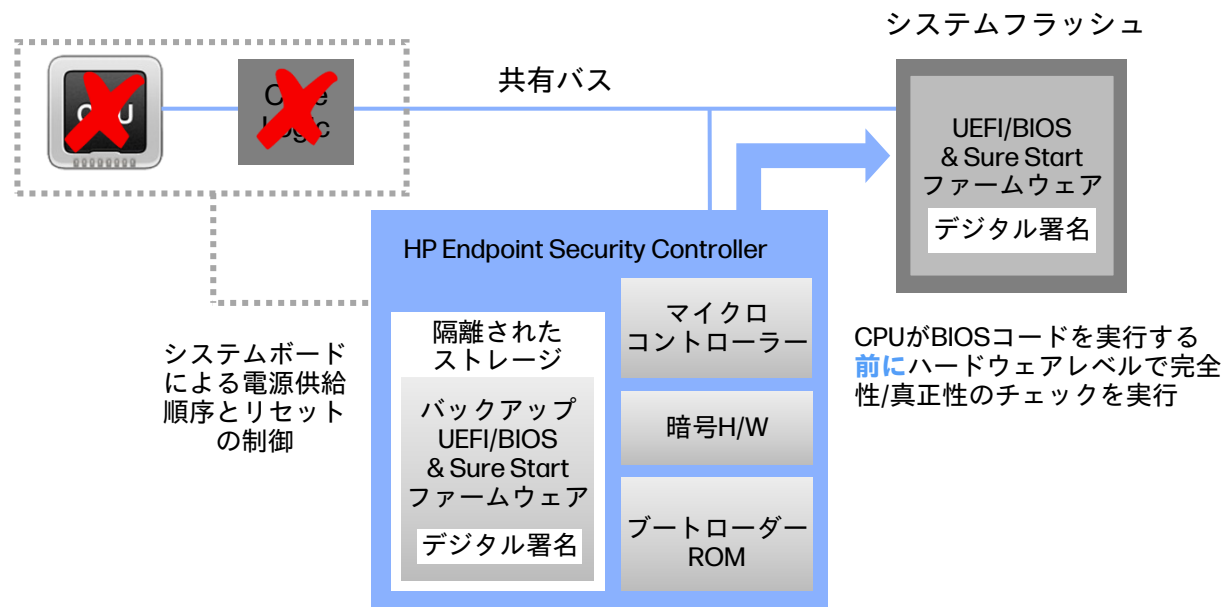
Endpoint Security ControllerとSure Start

NIST要件を超えた項目

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。

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レベルの保護がブリーンストールされ、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。

新ソリューション - TPM Guard

HP launches TPM Guard to help defeat physical TPM attacks

News

Mar 24, 2026 • 4 mins

Current TPMs can be compromised with \$20 of hardware, allowing attackers to bypass BitLocker and access encrypted content.



Credit: JLSStock

The Trusted Platform Module (TPM), developed by the Trusted Computing Group (TCG), is a mandatory security component in any computer running Windows 11. It stores sensitive information such as encryption keys in a separate, secure chip, passing it to the CPU as required.

Related content

NEWS

CISA urges IT to harden endpoint management systems after cyberattack by pro-Iranian group

By Howard Solomon

Mar 19, 2026 • 6 mins

Cybercrime

Endpoint Protection

Hacking

OPINION

Are you ready for shape-shifting apps?

By Jonny Evans

Mar 18, 2026 • 6 mins

Apple App Store

Mobile Security

iOS Security

NEWS

Google warns of two actively exploited Chrome zero days

By Howard Solomon

Mar 13, 2026 • 4 mins

Browser Security

Endpoint Protection

Zero-Day Vulnerabilities

Info Stealer & LOTL対策

- 仮想化ソリューション -



Sure Click vs Sure Access

Sure Click



脅威を箱の中に封じ込める

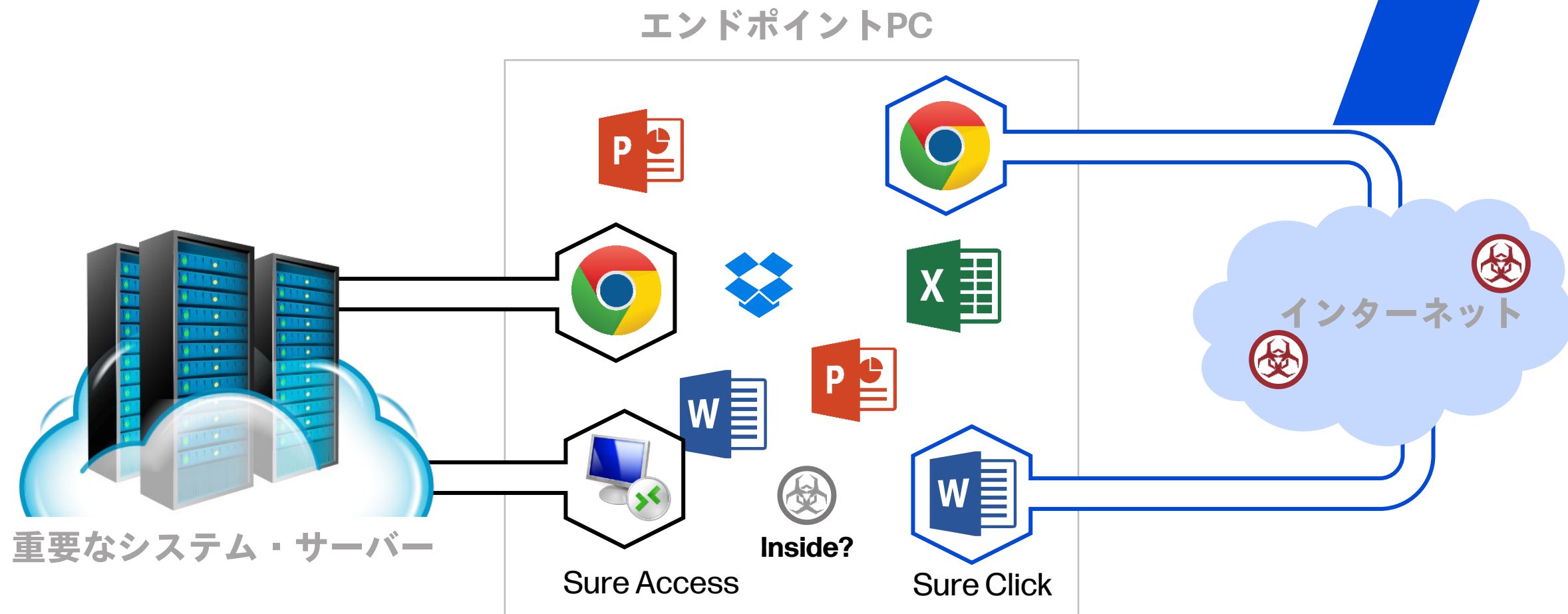
vs

Sure Access



脅威を箱の外に留める

Sure AccessとSure Clickの保護のイメージ



検出ではなく、**分離**による保護。
エンドポイントでコンテンツを分離するためのハードウェアベースのVM

脅威の封じ込め

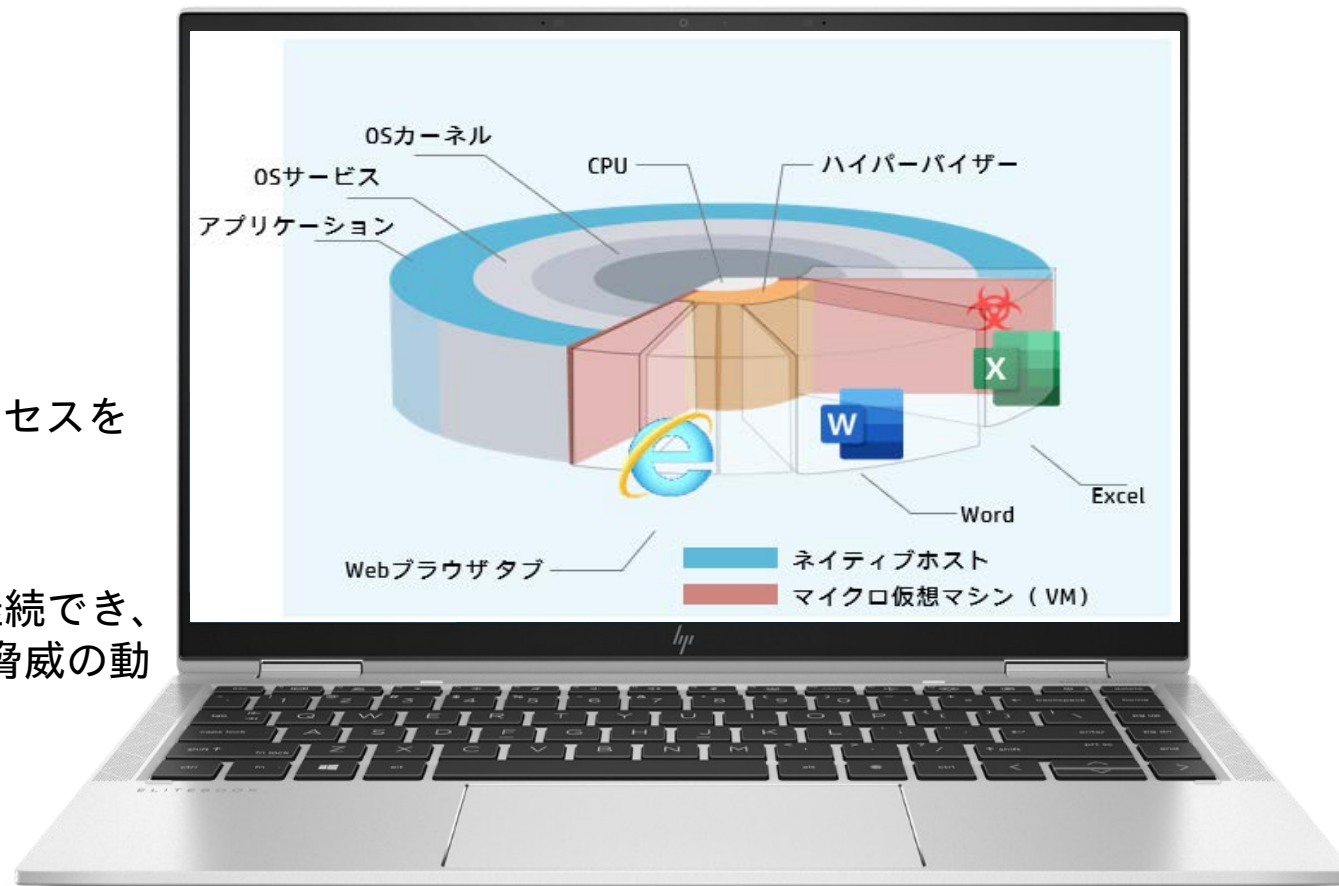
HP Sure Click

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



米国国防総省で5万台の導入実績

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することで、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。



A solid blue parallelogram graphic located at the bottom right of the page.

端末内の**仮想隔離環境**（使い捨て）でアプリケーションを実行することで、**マルウェア**や**脆弱性**が突かれたとしても、ネイティブOS側には影響がなく、消せ（**閉じれ**）ばなかったことになります。

ウイルスを攻撃者の意図通りに実行させることにより、完全な動作ログを、ノイズ少なく、迅速に、サーバへ収集し、分析することができます。

ネイティブOSと仮想隔離環境で別々にネットワーク設定(Proxy)することで、端末内でネットワークを分離することができます。

仮想化の守備範囲

次世代エンドポイント保護

偵察	武器化	初期アクセス	実行	持続化	権限昇格	回避	認証情報	インフラ探索	横移動	資産探索	統制	持ち出し	インパクト
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
		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		
			T1047	T1137		T1562	T1539	T1135		T1113	T1219		T1529
				T1653		T1550	T1552	T1040		T1125	T1205		
				T1542				T1201			T1102		
				T1053				T1120					
				T1505				T1069					
				T1176				T1057					
				T1205				T1012					
				T1048				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							

初期感染を
如何に防ぐか

如何に最初のコード実行を検出して無害化するかが、LoTLを含むアプリケーションへの攻撃の抑止に効く

重篤化を
如何に防ぐか

「初期アクセス」「実行」で検知できなかったとしても、仮想空間内の動きを細かくトレースし検出できる。
それも失敗したとしても汚染されるのは仮想空間のみである。

