

Security Online Day 2026 Autumn | B5 特別講演

検知の限界を超えて

－AI×サプライチェーン×耐量子時代に、
端末を「外」と「内」から設計で守る－

木下 和紀エドワード

株式会社 日本HP / セキュリティエバンジェリスト

Security Online Day 2026 Autumn

木下和紀エドワード

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。
デジタルソリューション事業部にも所属
- ・ 日本HP セキュリティ エバンジェリスト

「守りのボーダーライン」を、どこに引き直すか

AI・サプライチェーン・耐量子。3つの変化を、「端末の信頼をどこから設計するか」で束ねます。

01

検知を素通りする攻撃

AIでマシンスピード化した攻撃は、正規の署名・認証を悪用し“検知”をすり抜ける。
隔離と設計で守る前提へ。

02

サプライチェーンは最低要件

製品・調達のセキュリティが国際的な最低要件に。
守りの起点をOSより下＝シリコンと署名へ。

03

量子前夜の“署名”防御

Q-Dayは2030年代半ば。しかし脅威は前夜の今すでに始まる。
15年先まで効く設計を今から。

着地点：守りの再設計－3つの決断へ。

3つの持ち帰りポイント



01

AIで高速化する攻撃と、検知依存型セキュリティの限界

マシンスピード化・巧妙化する攻撃の実態と、検知“だけ”に依存する防御の限界。



02

AI時代の製品・サプライチェーンリスクと、調達に必要な視点

高まる製品・サプライチェーンのリスクと、調達・経営が押さえるべき論点。



03

ハードウェア起点で、いまと将来の脅威に備える「守りの設計」

現在の攻撃から将来の脅威まで一貫して守る、“守りの設計”の考え方。

被害の実例→検知依存からの発想転換→ハードウェア起点のサイバーレジリエンス

01

検知の限界と、攻撃側の変化

なぜ“今”、これは延長線ではなくパラダイムシフトなのか

AIは技術的障壁を取り除き、攻撃を“民主化”する



マシンスピード化

攻撃・防御の双方がAIで高速化。
脆弱性の発見・悪用にかかる時間
が激減する。



攻撃の民主化

高度な攻撃に必要な技術的障壁
が下がり、誰でも・速く・安く
実行できる時代に。



前提の崩壊

ゼロデイ / ワンデイ攻撃が急増。
「まだ自社は狙われない」と
いう前提が崩れる。

前提が変わった。“これまでの延長線上”の対処では、時代に淘汰される。

数ヶ月規模の事業停止・巨額損失が、現実になっている

A ホールディングス

攻撃者： Qilin RaaS

停止 **2ヶ月超**

被害 **事業販売が2割以上減**

影響 **決算にも遅れ**

A 社

攻撃者： RansomHouse RaaS

停止 **2ヶ月超**

被害 **売上高95%減**

影響 **業務全面停止**

J 社（英国）

攻撃者： HELLCAT RaaS

停止 **1ヶ月超**

被害 **損失 約19億ポンド**

影響 **供給網へ波及**

近年の攻撃で多く見られる手口：認証情報の悪用と、正規ツール・署名済み要素を用いた防御回避。

攻撃者は“解析”を自動化し、発見・悪用の時間を激減させる



プログラムの解析

市販ソフトやOSSの脆弱性を高速で解析し、探し出す。

未知の脆弱性（ゼロデイ）の
発掘コストと時間が激減



パッチファイルの解析

公開パッチや最新バイナリを解析し、差分から逆算する。

旧バージョンに残る脆弱性の
発掘コストと時間が激減

一般企業もゼロデイ攻撃の対象に / パッチ公開から数時間～数日でワンデイ攻撃。
「まだ攻撃されない」だけ、猶予はもう存在しない。

検知して追いかける発想では勝てない。“隔離”と“設計”で守る前提へ。

検知は必要。だが、検知が成立しなかった場合の構造があるか



Detect

検知

兆候を見つける

OS上の監視・振る舞い分析



Contain

封じ込め

影響範囲を限定する

隔離実行環境・使い捨て化



Trust

信頼確認

下位層から状態を確認

ハードウェア起点の検証

検知・隔離・信頼確認は代替ではなく、役割の異なる多層。「検知できなかったとき」の構造があるか。

02 サプライチェーンセキュリティ

国際的な最低要件へ。守りの起点を、端末が届く“前”まで広げる

デバイスが導入前に汚染されると、OS層の対策は無力になる

従来の考え方

- OS・アプリ層で守れば十分
- 調達後にセキュリティ製品を導入
- 製造～納品の過程は“前提として信頼”

導入前に汚染されると検知できない



必要な考え方

- 製造時のHW/FW構成をメーカー署名で証明
- 改ざんを“1台目”から検証
- 守りの起点をOSより下＝シリコンへ

ゼロトラストの“最初の1台目”を検証

サプライチェーンは“製品を買うための前提条件”。国際的な調達の最低要件になった。

OSより下に“信頼の起点（Root of Trust）”を持つ

アプリ / データ

OS (Windows)

ファームウェア / BIOS

ハードウェア (Root of Trust)

↑ CPUより先に起動し、下位から順に完全性を検証



起動前に検証

ESCがCPUから独立して先に起動し、BIOSや重要FWの完全性を検証してからCPUの起動を許可。



自己修復

改ざん時は隔離領域の正本から正規状態へ自動修復（NIST SP800-193準拠）。



20年以上の実績

TPM・BIOS・FW耐性の業界標準づくりをリードしてきた。

検証する側は、検証される側から独立していなければならない。信頼の根はOSより下へ。

サプライチェーンと継続的検証は、各国で調達・規制の要件に



日本

デジタル庁 DS-210 / 統一基準群 (令和7年度版)

- ゼロトラスト適用方針
- サプライチェーン対策・重要度区分
- 委託先統制を要求



米国

NIST SP800-53/-207 / CNSA 2.0 (PQC)

- ゼロトラスト・供給網リスク管理の参照枠組み
- CNSA 2.0はNSS向けに署名の耐量子移行を先行
- 民間へは調達経由で波及



欧州

NIS2指令 (EU) 2022/2555 第21条

- 経営層の責任を明文化
- サプライチェーンを含むリスク管理措置
- 公共行政も対象

継続的な検証とリスクベースのアクセス管理が、国際的な調達・規制の“当たり前”に。

Q-Dayは2030年代半ば。しかし脅威は、前夜の今すでに始まっている



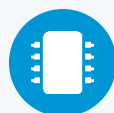
HNDL：今盗み、後で復号

医療・政府・OT等の“長寿命データ”は、将来の復号を狙って今すでに収集されている。



本丸は“署名”の無力化

FW署名が偽造されれば、正規アップデートへの成りすまし＝サプライチェーンへ波及。



15年動く資産を守る

15年以上稼働するIoT/PCでは、今の署名が将来破られる。だから今、ハードで備える。

HPの手

ESC Gen5 は世界初の

PQC対応ファームウェア搭載ビジネスPC

LMS + RSA の二重署名検証（対応は製品・構成ごとに要確認）

守る対象はFW署名の完全性。ハード起点で先行防御。

耐量子は、遠い未来の暗号理論ではなく“今日の調達判断”。長寿命機器ほど、今の選定が効く。

03 HPの絵姿：外と内から守る

silicon-to-cloud。リスクは「外」で隔離し、特権は「内」で保護する

リスクは「外」で隔離し、特権は「内」で保護する

外

Sure Click Enterprise (SCE)

日常利用のリスクを断つ「入口」

- 危険なWeb・メール・ファイルを使い捨てマイクロVMで隔離実行
- 未知の攻撃もVM内に封じ込め、ホストへの影響を抑制
- 日常操作に伴う攻撃対象領域を大幅に削減

内

Sure Access Enterprise (SAE)

高権限業務を守る「奥」

- 基幹系アクセスを保護VMで分離し、情報漏洩リスクを低減
- ホストOSの侵害を想定し、重要業務の機密性・完全性を保護
- 構成証明 + 条件付きアクセスで許可

外 = 隔離で封じ込め、内 = 分離で保護。その土台に、ハードウェア起点の信頼確認を置く。

本日のまとめ

1 AI時代の攻撃は、検知だけでは守りきれない。検知に“加えて”封じ込める構造を。 → 隔離・設計で守る

2 端末の信頼は導入後のOSだけでは作れない。製造・FW・署名まで調達段階から確認。 → 起点はシリコン / 署名

3 量子前夜の今、署名の信頼をハードで先行防御。15年先まで効く設計を今日から。 → 将来まで一貫した設計

守りのボーダーラインを、OSより下＝ハードウェアと署名に引き直す。イベントテーマ“刷新せよ”へのHPの回答です。

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

物理分離された専用セキュリティプロセッサで、BIOS / ファームウェアの整合性を保護

HP EliteBook X G2i 14 AI PC (Copilot+ 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 Optimizer⁴¹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



poly camera pro

リモートでも効果的に コラボレーション

リモートディスカッション用のPoly Camera Pro⁸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の多層防御に加え、ESC搭載の一部構成では量子耐性ファームウェア保護を提供。

軽量なスタイリッシュ筐体でどこでもAIを活用

最大
50 TOPS



intel
CORE
ULTRA

ポータブル
スタイリッシュ
多機能



/ Windows 11

