Hewlett Packard Enterprise

“元”同じ会社が語る レジリエンスの重要性とサーバーアーキテクチャ

日本ヒューレット・パッカード株式会社
ハイブリッドIT製品統括本部　カテゴリーマネージャー
阿部 敬則

Agenda

- ファームウェアに深化する、セキュリティ リスク

- 「ゼロトラスト」時代の
  新たなハードウェアセキュリティー標準

ファームウェアに深化する、セキュリティ リスク

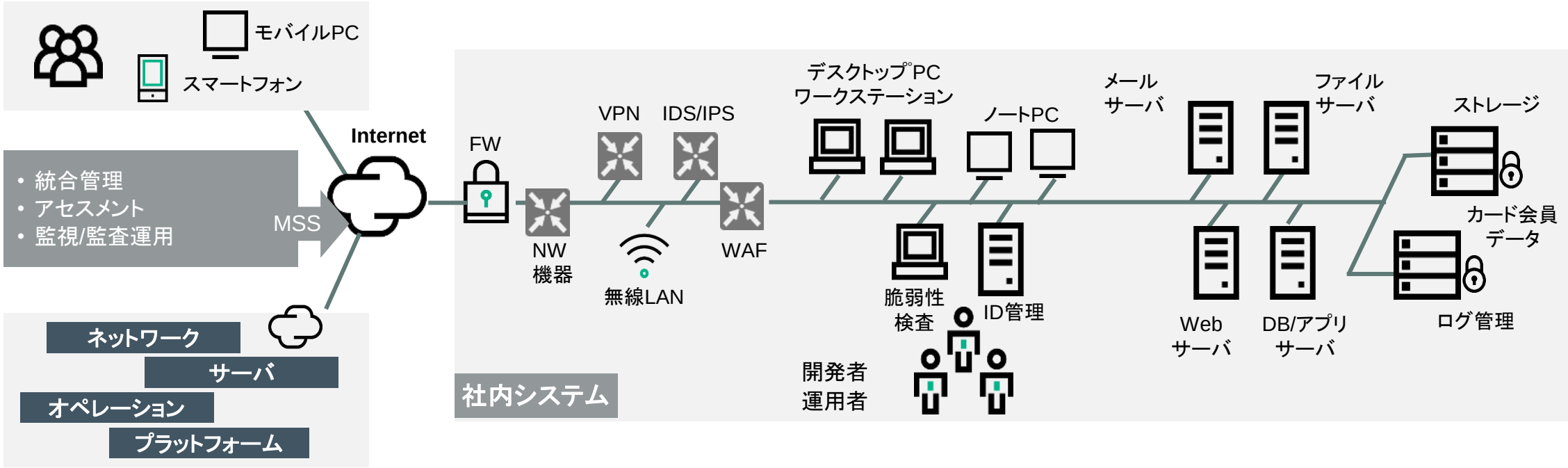
境界防御の限界と多層防御

モバイル層
- アンチウイルス、パーソナルFW
- 持ち出し制御
- ロック、ワイプ
- 変更/構成管理
- 操作ログ取得

ネットワーク層
- FW、VPN、IDS/IPS、ルータ制御
- NWセグメンテーション
- 無線LAN対応（IDS/IPS）
- 変更/構成管理

クライアント層
- アンチウイルス、パーソナルFW
- 持ち出し制御
- 操作ログ取得
- 変更/構成管理

サーバ層
- ID管理、アクセス制御（特権含む）
- OS要塞化
- セキュリティパッチ
- 変更/構成管理



クラウド層
- ※社内システム内と同様
- ネットワーク層
- サーバ層
- オペレーション層
- プラットフォーム層

従業員
- 情報セキュリティポリシーの整備
- 雇用、教育
- インシデント対応計画

オペレーション層
- 変更管理プロセス、インシデント対応
- ID管理、アクセス制御（特権含む）
- 監査証跡、ログ取得
- 脆弱性検査対応（コーディング含む）
- 暗号鍵のライフサイクル管理

プラットフォーム層
- 改ざん対策、消去防止
- データ暗号化
- 物理アクセス制御
- ログ管理

求められる、攻撃者の視点

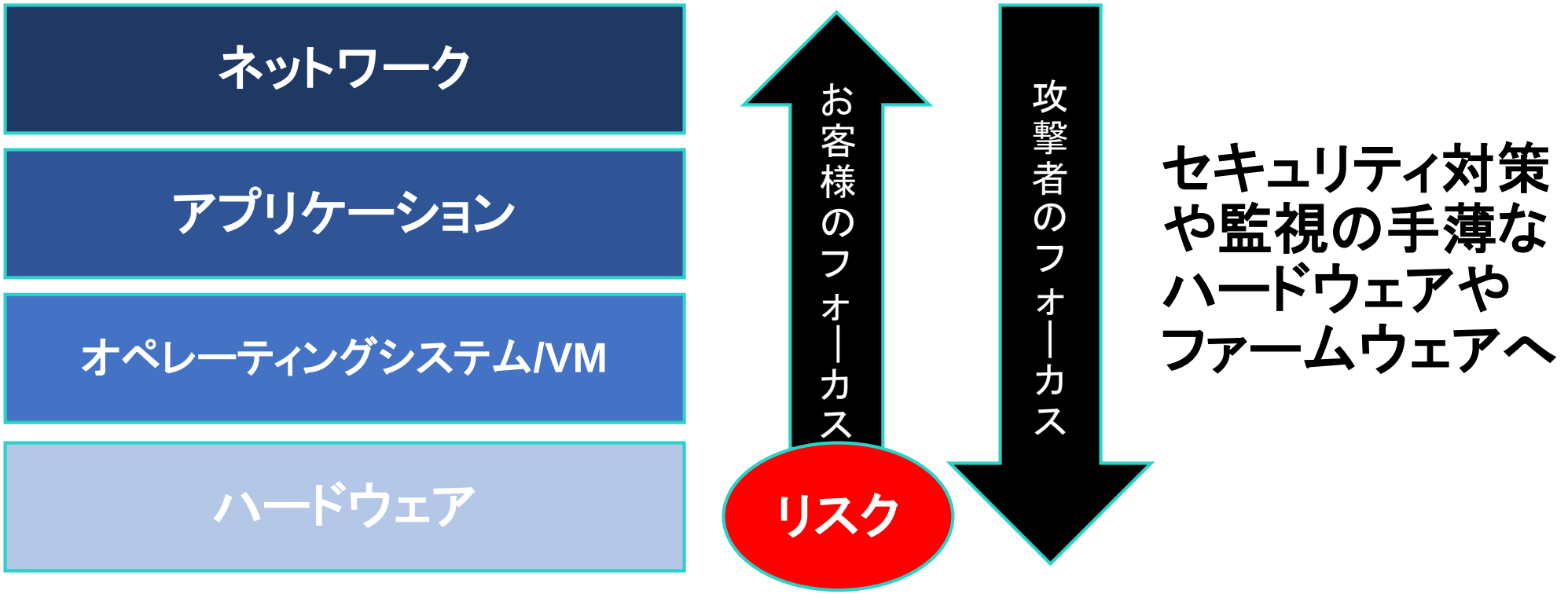
狙うなら、対策がされておらず、

（攻撃コストが少なく）

見つかりにくいもの

よりリスクの少ない死角

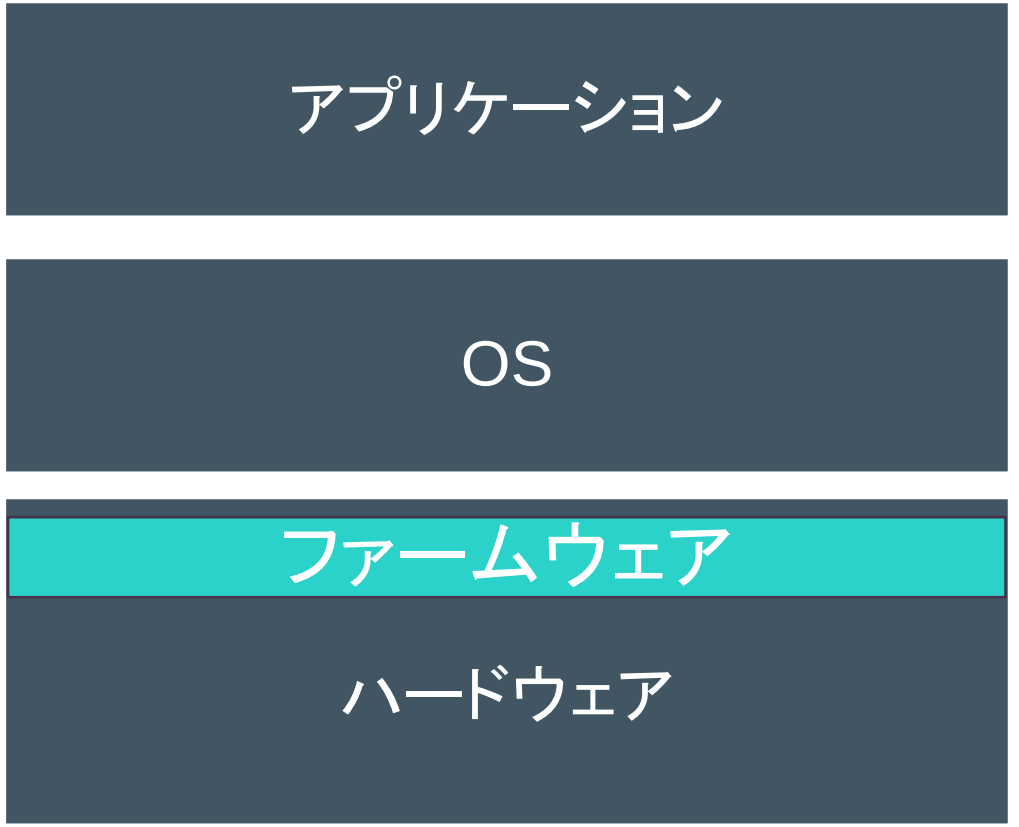
新たな攻撃経路となるハードウェア



出典：2017, Moor Insights & Strategy
https://www.hpe.com/jp/ja/resources/servers/white-paper/hpe-locks-down-server.html?parentPage=/jp/ja/products/servers/gen10-servers

そもそもファームウェアとは？
コンピューター（ハードウェア）を制御するために必須のプログラム

- ROM等の集積回路にあらかじめ書き込まれた状態でハードウェアに含まれる
- ハードウェアの**制御を行う“心臓”部**
- OS起動の前にまず立ち上がる
- バグ修正・機能追加などで、出荷後もアップデートされることが多い
- HDD、SSD、NIC、HBA、アレイコントローラなど様々なデバイスに搭載される
- ファームウェアの一種であるサーバーのBIOS/UEFIなどを、他社で製造・設計したもので賄うケースもある



Hewlett Packard Enterprise

攻撃者にとって、なぜファームウェアは魅力的なのか？

悪意有るコードを埋め込む場所として理想的

- **コントロール**

  OSの起動前に実行される。つまり、ホストプロセッサによって最初に実行される

- **パフォーマンス**

  システムボード上のチップや、組込装置上で実行可能

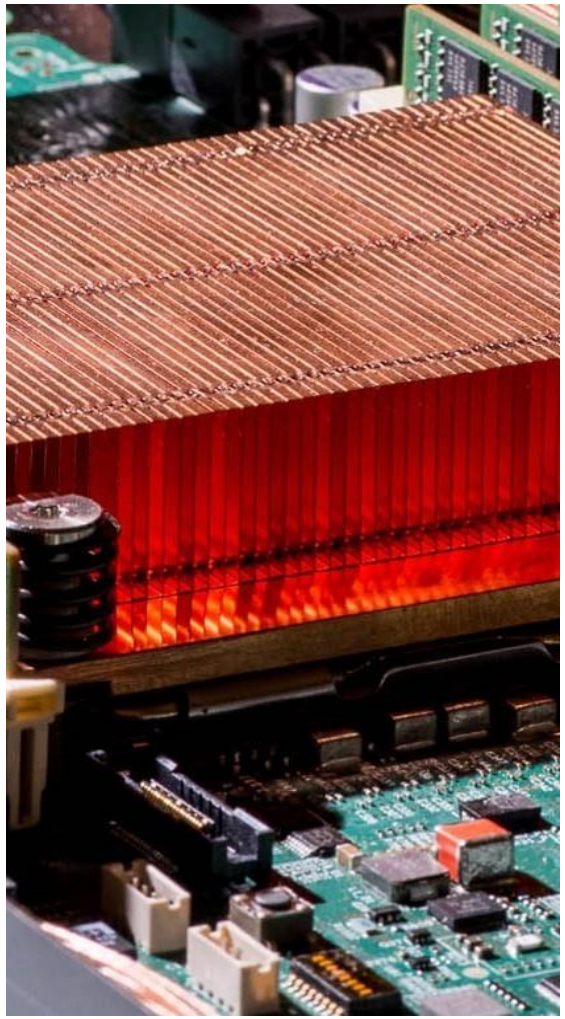
- **検知**

  検知が非常に困難。OSやアンチウイルスソフトウェアからは検出不能

- **復旧**

  通常、マザーボード交換など、ハードウェアメインテナンス作業が必要

考慮すべきリスク要因、インフラストラクチャのセキュリティー



一般的に最も注目される領域

- クラウド
- ファイヤーウォール
- アプリケーション
- ハイパーバイザ/OS

大量データ窃取
一時的サービス拒否

見落とされがち、知らない間に進行

- サーバーファームウェア
- サプライチェーン/コンポーネント外部調達

ステルス
不揮発（消えない）
破壊的（物理破壊にほぼ等しい）

NIST（アメリカ国立標準技術研究所）SP800文書

Special Publications（SP800シリーズ）

SP800シリーズは、CSD[*1]が発行するコンピュータセキュリティ関係のレポートです。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書ですが、内容的には、セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応など、セキュリティに関し、幅広く網羅しており、政府機関、民間企業を問わず、セキュリティ担当者にとって有益な文書です。

出典：IPA　https://www.ipa.go.jp/security/publications/nist/nist_publications.html#r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

※1 CSD: Computer Security Division.

NIST SP 800-147/800-193で警告されている ハードウェアセキュリティー

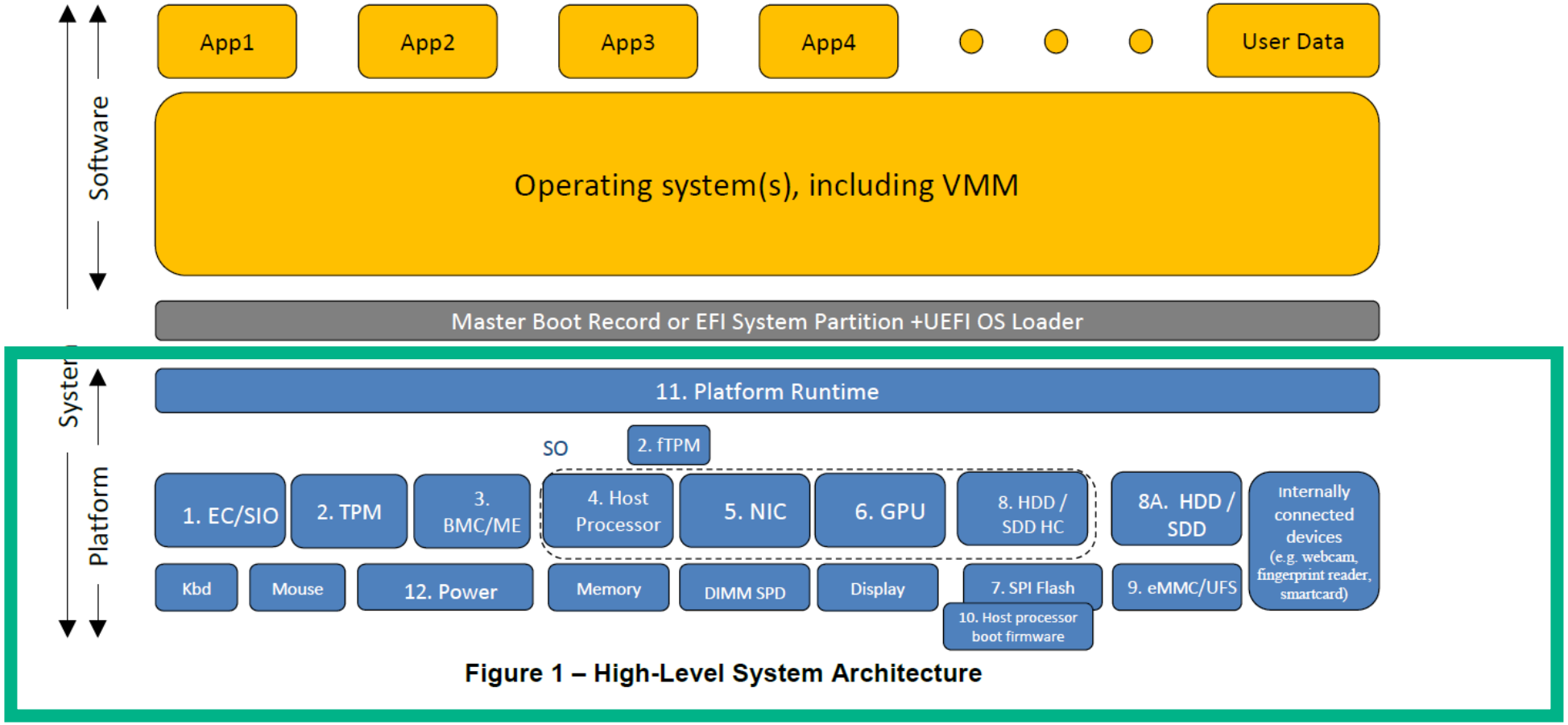


Figure 1 – High-Level System Architecture

出典：NIST SP800-193, 2018, P3
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

FBIがファームウェアレベルへの攻撃の増加に警鐘

FBI コンピューターサイエンティストのモリソン氏、HPE最大のイベントで語る

ファームウェアレベルの脅威が今後、急増する
企業のセキュリティの備えができておらず、早急な対策を訴え

- サイバー犯罪は5年前から急増
- 全世界で200以上の
  サイバー犯罪グループ
- BIOSの破壊(PDoS)、感染ファームウェアによる被害増
- 今後さらに増える見込み
- **企業の備えがあまりにできておらず、
  今後の被害の大きなリスクとなっている**

ジェームズ・モリソン氏
コンピューターサイエンティスト
ヒューストン サイバー タスクフォース,
FBI

2017年6月
HPE Discover 2017
パネルディスカッションより

＊当日の模様は動画にてご視聴いただけます（英語）。
（基調講演に続き、34分くらいから）
Announcing HPE's next-generation compute experience https://youtu.be/XznSNFUYalo

Hewlett Packard Enterprise

ハードウェアの永続ダウンを狙った攻撃手法

PDoS
（Permanent Denial of Service)

ファームウェアを改変し、永続的なサービス拒否を起こす攻撃手法

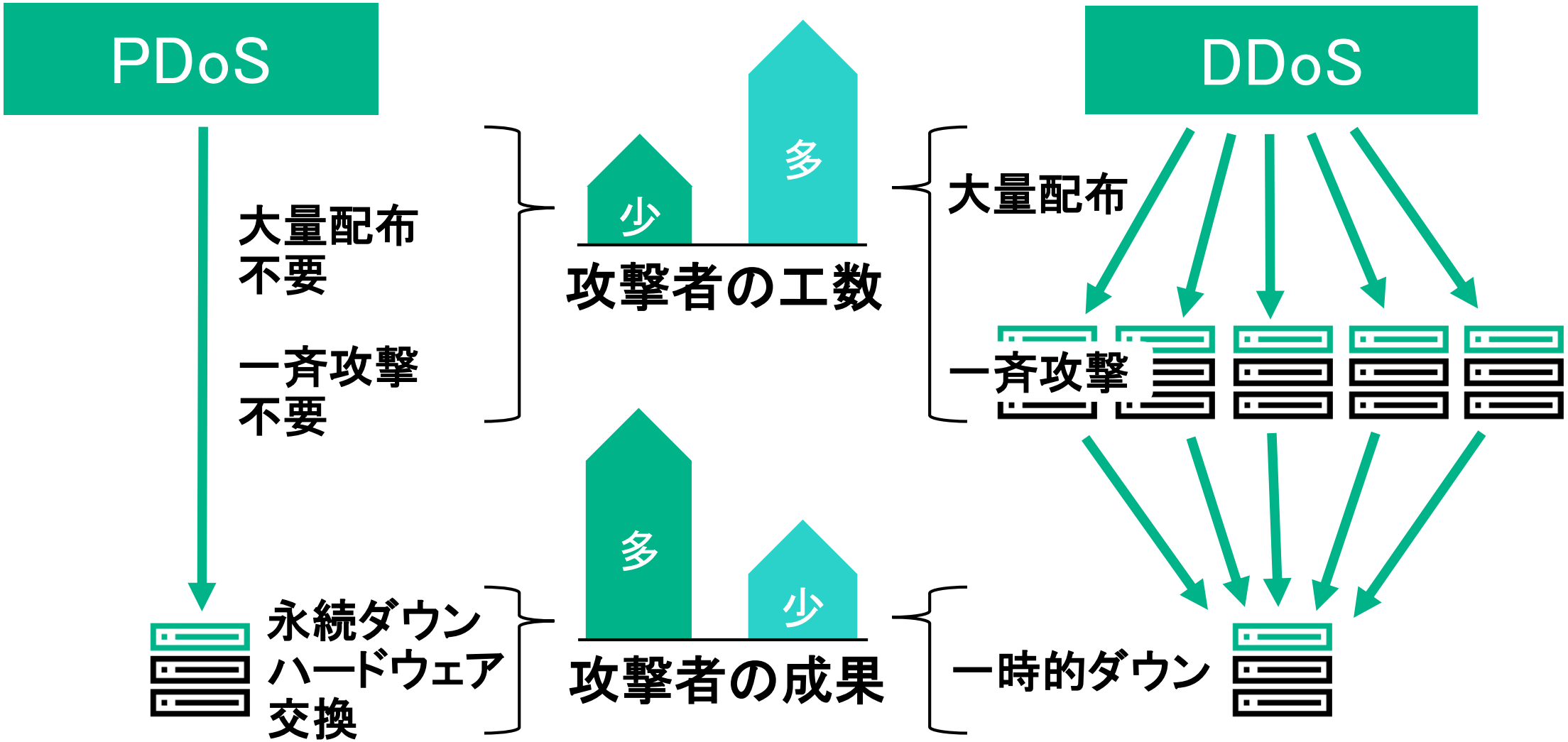
ファームウェアを改変された場合のインパクト

1. サーバーの停止　＝　業務停止
2. 再起動してもOSが起動できない
3. ハードウェア入れ替えしかなくなる
4. ハードウェアの乗っ取り
5. 被害の拡散

サーバーシステムの・・・

- **永続ダウン**
- **乗っ取り**
- **被害拡散**

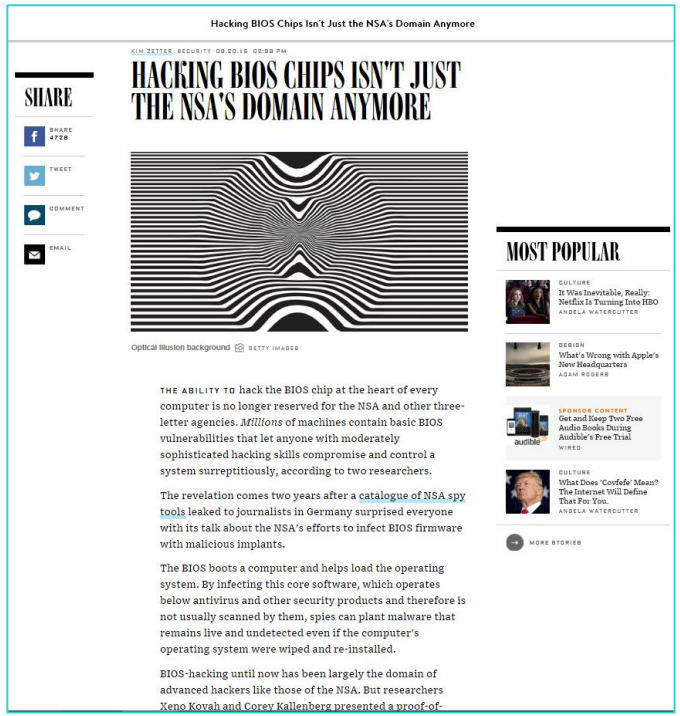
攻撃者目線でみるPDoSの費用対効果



Hewlett Packard Enterprise

既に始まっているファームウェアレベルの脅威

BIOSをハッキングするのはもはやNSA（米国国家安全保障局）だけのテクノロジーではない[1]



Hacking BIOS Chips Isn't Just the NSA's Domain Anymore

KIM ZETTER SECURITY 03.20.15 02:00 PM

HACKING BIOS CHIPS ISN'T JUST THE NSA'S DOMAIN ANYMORE

SHARE

SHARE 4758

TWEET

COMMENT

EMAIL

Optical illusion background GETTY IMAGES

THE ABILITY TO hack the BIOS chip at the heart of every computer is no longer reserved for the NSA and other three-letter agencies. *Millions* of machines contain basic BIOS vulnerabilities that let anyone with moderately sophisticated hacking skills compromise and control a system surreptitiously, according to two researchers.

The revelation comes two years after a catalogue of NSA spy tools leaked to journalists in Germany surprised everyone with its talk about the NSA's efforts to infect BIOS firmware with malicious implants.

The BIOS boots a computer and helps load the operating system. By infecting this core software, which operates below antivirus and other security products and therefore is not usually scanned by them, spies can plant malware that remains live and undetected even if the computer's operating system were wiped and re-installed.

BIOS-hacking until now has been largely the domain of advanced hackers like those of the NSA. But researchers Xeno Kovah and Corey Kallenberg presented a proof-of-

MOST POPULAR

CULTURE
It Was Inevitable, Really: Netflix Is Turning Into HBO
ANDELA WATERCUTTER

DESIGN
What's Wrong with Apple's New Headquarters
ADAM ROGERS

SPONSOR CONTENT
Get and Keep Two Free Audio Books During Audible's Free Trial
WIRED

CULTURE
What Does 'Covfefe' Mean? The Internet Will Define That For You.
ANDELA WATERCUTTER

MORE STORIES

Apple、社内のサーバーに非公式のパッチを誤って適用か[2]

Apple、社内のサーバーに非公式のパッチを誤って適用か

2017/03/21

シェア 4　ツイート

Maria Korolov CSO

米Appleが、社内の開発用サーバーに、正規のものではないファームウエア更新プログラムを誤ってインストールしたとの報道が2017年2月にあった。更新プログラムの入手元には注意すべしというのは、すべての企業に当てはまる教訓だ。

報道によると、このサーバーは米Super Micro Computer（Supermicro）製。Appleが適用したファームウエアにセキュリティ上の脆弱性があったことから、同社はSupermicroとの関係を絶ったとされる。

1 Wired, 2015 https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
2 日経BP CIO, 2017.3月 http://itpro.nikkeibp.co.jp/atcl/idg/14/481709/032100309/

日本も無関係ではいられない

セキュリティ対策を要請　公共のみならず民間も対象　**＜重要インフラ14分野＞**

日本政府も情報漏洩や機能停止の
懸念がある情報通信機器を調達しないよう
重要インフラ14分野の民間企業・団体に要請[1]

1　日本経済新聞　2018年12月13日　記事より抜粋

政府は今春にも、電力や水道といった**重要インフラ**14分野のサイバー防衛対策に関する安全基準の指針を改定する。
当初は2020年の東京五輪・パラリンピック後に見直す予定だったが、巧妙化するサイバー攻撃や相次ぐシステム障害への危機感から前倒しする。重要インフラが攻撃を受ければ国民生活への影響は甚大だ。**事業者は一層の対策強化が不可欠に**なる。[2]

2　日本経済新聞　2019年1月16日　記事より抜粋

情報通信	ネットワーク、編成・運行
金融	勘定系、資金証券系、国際系
航空	運行、予約・搭乗、整備
空港	警戒警備・監視
鉄道	列車運行管理、電力管理
電力	電力制限、スマートメーター
ガス	プラント制御、遠隔監視・制御
行政	地方自治体の情報
医療	診療記録などの管理
水道	水道施設や水道水の監視
物流	集配管理、貨物追跡、倉庫管理
化学	プラント制御
クレジット	クレジットカード決済
石油	受発注、生産管理、生産出荷

2019年　セキュリティが経営課題になる年

現在	2019年4月	2019年春以降	2019年4月
米国政府の セキュリティ基準	防衛 調達における 新情報セキュリティ基準	デジタル時代に対応する 「新たな社会システム」への移行	IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ
米国で事業を行う グローバル企業	防衛省と取引のある 企業	情報通信、金融、航空、空港、鉄道、電力、ガス、行政・サービス、医療、水道、物流、化学、クレジット、石油	官公庁・地方自治体の 公示案件数
6,814社	9,000社	14分野/7045社・団体	約80,000~100,000件/月
NIST SP800-171/53		NIST SP800-171/53 を参照?	サプライチェーン セキュリティ

調達への影響: 適切な仕様化が重要に

NIST SP800-171の「インシデント対応」及び「システムと情報の完全性」に対し
NIST SP800-193 もしくは193で定義されている機能を分解して仕様化

SDLC (NIST etc.)
DoD基準
ルートオブトラスト認証
NIST SP800-193

Hewlett Packard Enterprise

「ゼロトラスト」の時代の、
新たなハードウェアセキュリティー標準

– サーバーセキュリティの新標準

Hewlett Packard
Enterprise

NIST Special Publication 800-193(2018年5月リリース) プラットフォーム・ファームウェアの復旧ガイドライン

– **保護:**
ファームウェア更新の信憑性・正常性の保証等によって、プラットフォーム・ファームウェアのコード及び重要データが正常な状態であり、かつ破損から保護されるメカニズム。

– **検知:**
プラットフォーム・ファームウェアのコード及び重要データの破損及び、正規の状態からの変更を検知するメカニズム

– **復旧:**
プラットフォーム・ファームウェアのコード及び重要データの破損が検知された場合や、許可されたメカニズムによって強制的に復旧が行われる際に、プラットフォーム・ファームウェアのコード及び重要データを正常な状態に回復するメカニズム。復旧は、ファームウェアのコードと重要データの回復能力を範囲とする。

保護:
ファームウェアアップデート時も含めた、コードと設定情報の保護

検知:
コードと設定情報の破損・改ざんを検知する

復旧:
ファームウェア破損時に、認証された正しいイメージに復旧する

※緑字はドラフトからの変更差分
出典:NIST SP800-193, 2018, P10、但し翻訳は講演者による。
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

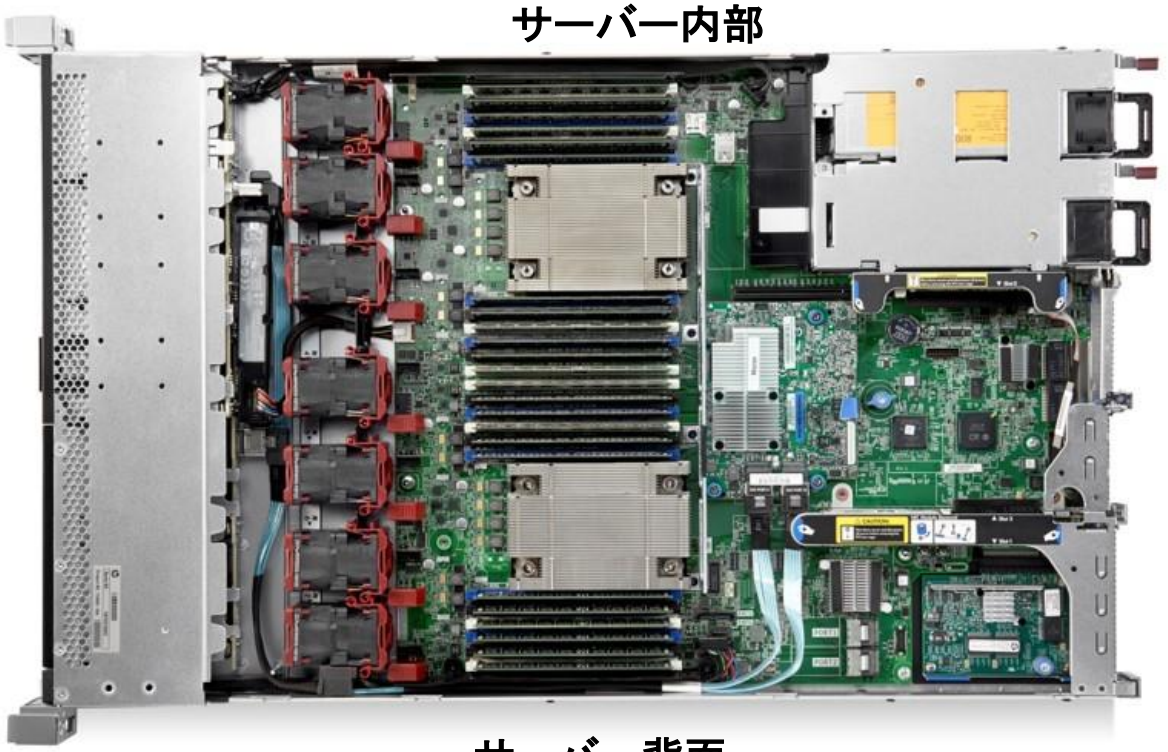
HPE ProLiant Gen10 サーバー プラットフォーム

Hewlett Packard Enterprise

iLO(Integrated Lights-Out)とは?

HPE サーバーを支える縁の下の力持ち

サーバー内部



サーバー背面

- HPE ProLiant サーバーに内蔵されている”小型コンピューター”
- サーバー自身のリソース (CPU, メモリ, ストレージ, ネットワーク) とは独立した専用ASIC
- リモート操作はもちろん、サーバーの導入から解析まで、ライフサイクル全般をカバー

Hewlett Packard Enterprise

HPE Secure Compute Lifecycle

防御・検知・復旧まで全ライフサイクルにわたって保護

Silicon Root of Trust（シリコンレベルの信頼性）

- **自社シリコンチップ (iLO 5) へ“Root of Trust”を埋め込み**
- 業界標準サーバーにてSilicon Root of Trustを実装
- OSが立ち上がる前の百万以上のファームウェアコードの健全性を保証

オンラインでのファームウェア検証

- **定期自動/オンデマンドでシステムファームウェアの信頼性を検証**
- iLO 5 NAND上のレポジトリーに有効で安全なファームウェアコピーを保管
- iLOの監査ログを通じ改ざんされたファームウェアに対して検知、アラート

安全な復旧（レジリエンス）

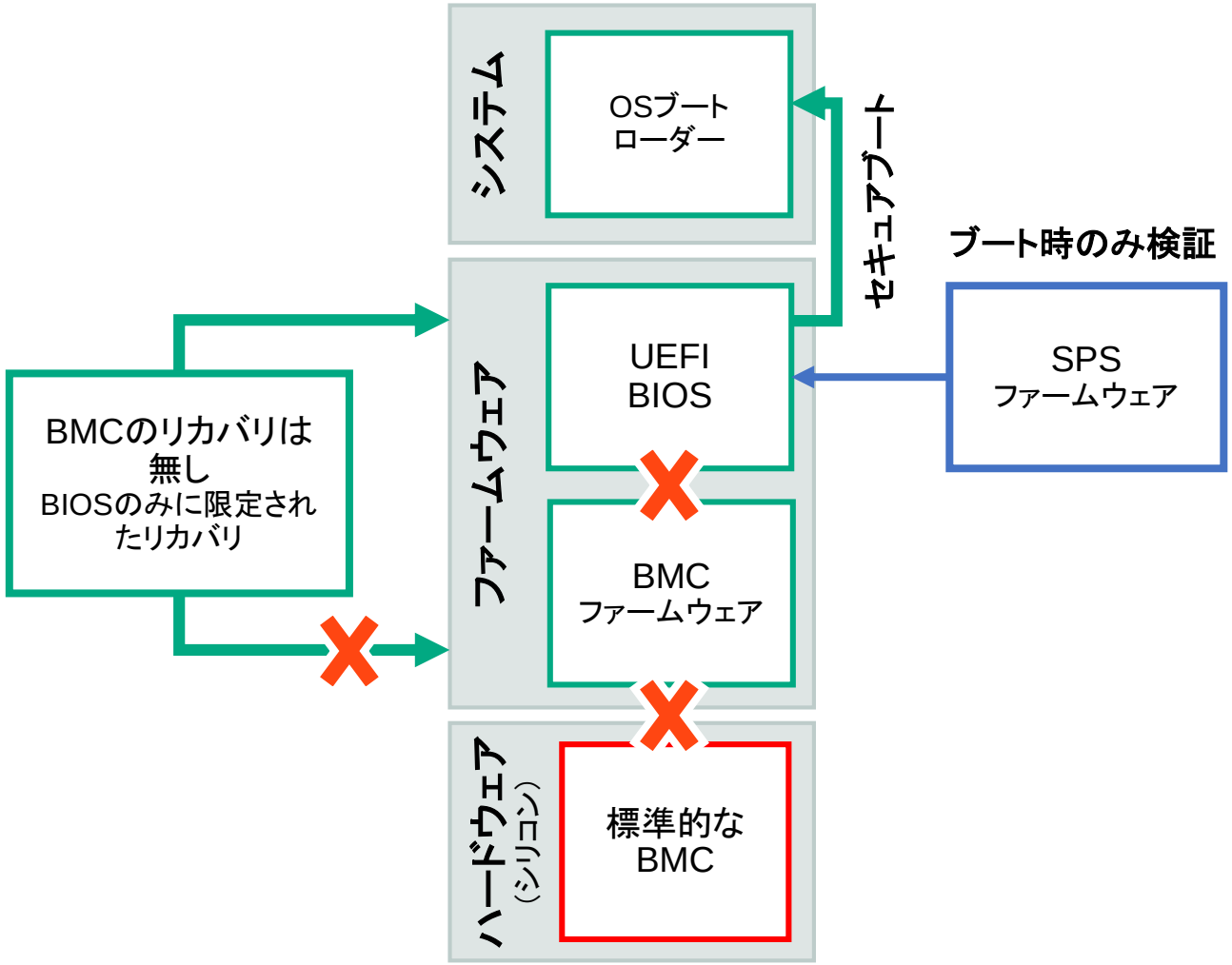
- **改ざんされたファームウェアに対し、最新の健全な状態のファームウェアにまで自動復旧**
- サーバー稼働中の状態で、出荷段階の工場設定への自動復旧、あるいは健全なことが証明されている最新の設定への自動復旧

Commercial National Security Algorithms

- **CNSA最上位レベルのセキュリティ基準**
- 最上位レベルの暗号化をレイテンシなく実施。管理機能の乗っ取りを防ぐ
- 業界で唯一、NIST800-53(多数の業界コンプライアンスの基本)も取得

Hewlett Packard Enterprise

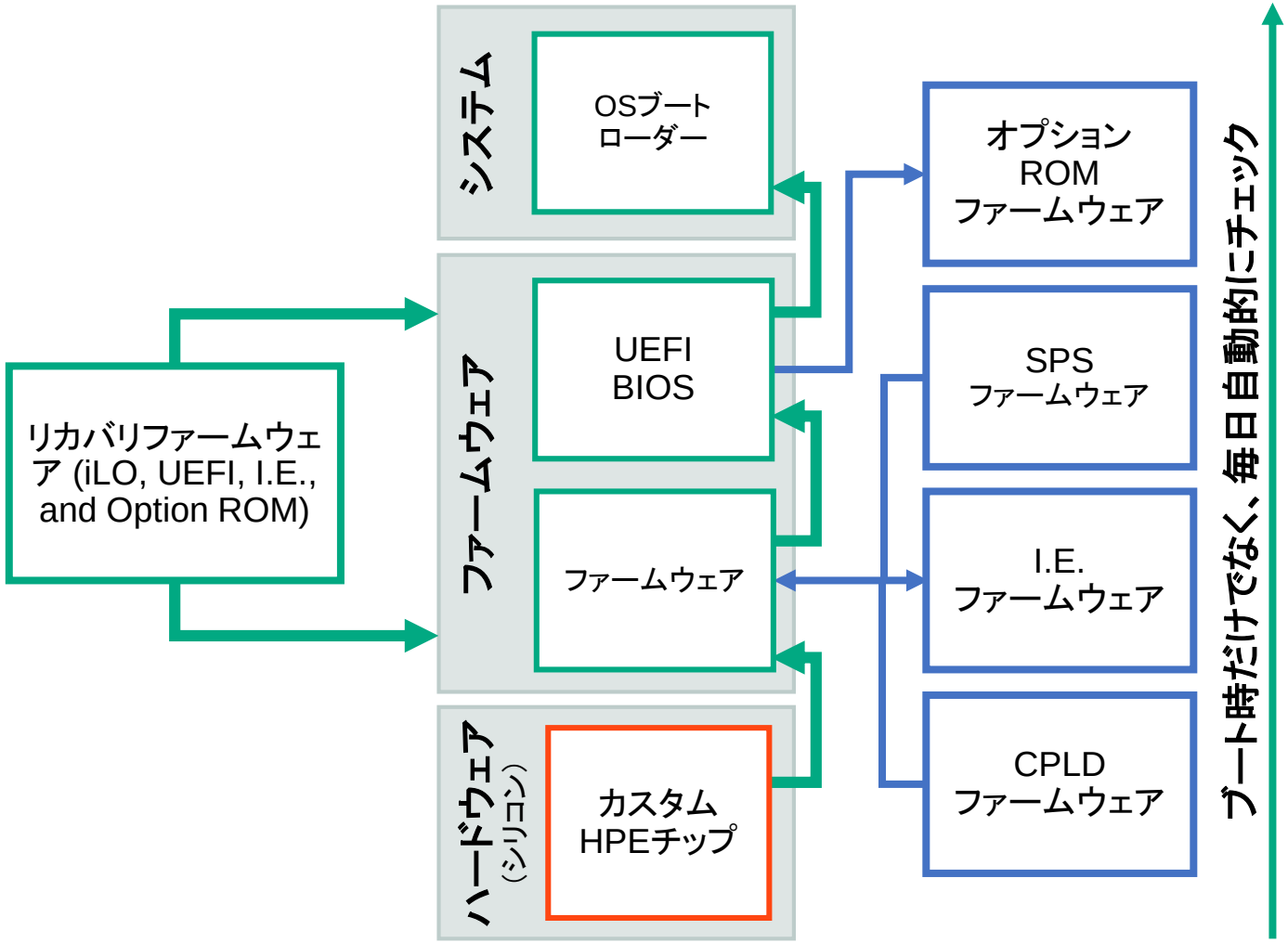
CPUベースでのファームウェア検証プロセスの例



サーバー起動	セキュアブートを使用して、ファームウェアがOSを起動
SPS ファームウェア	Server Platform Services
BMC ファームウェア	サーバー管理ソフトウェアの検証
標準 BMC	既製品のBMC ASIC

BMC: Baseboard Management Controller
システム管理用のコントローラ

Silicon Root of Trust の場合のファームウェア検証&復旧プロセス



オプションROM	オプション ROMの信頼性・正当性を検証
Secure Boot	全てのファームウェアが正しく検証されると、OSの起動を許可
SPS ファームウェア	次に、SPS（Server Platform Services)を検証
I.E. ファームウェア	次に、I.E.（Innovation Engine)ファームウェアを検証
CPLD ファームウェア	次に、iLO ファームウェアがCPLD（Complex Programmable Logic Device）を検証
BMC ファームウェア	サーバー電源投入後、直ぐにシリコンチップがBMCファームウェアを検証
BMC/iLO5 シリコンチップ	ハッシュ値をシリコン上の回路に組込

外部機関によるペネトレーションテスト＊で
HPE Gen10はNo.1を獲得

“HPEは独自の強みとして、自社製のカスタムシリコンにファームウェアを
直接インストールすることで、
当社が検証した競合サーバーの中でとりわけ高いセキュリティを実現しています。“

Jason Shropshire氏
Infusion Points社　シニアバイスプレジデント兼CTO

InfusionPoints
Cyber Security Solutions

＊ペネトレーションテスト：ネットワークに接続されているコンピュータシステムに対し、実際に既知の技術を用いて侵入を試みることで、システムに脆弱性がないかどうかテストする手法のこと。

Hewlett Packard
Enterprise

サイバーディフェンス研究所 技術部 分析官 手島 裕太様

ファームウェアの完全性を十分に意識して作られている優れた製品だ

手島 裕太 様

サイバーディフェンス
研究所　分析官

最近ではハードウェア面での脆弱性診断に関する相談が増加してきた。ハードウェアレイヤからのセキュリティを気にするお客様が増えている。

ファームウェア改ざんに対するハードルは、コストとノウハウの両面で、10年前と比較して劇的に下がっている。

（Gen10サーバーの）BIOSとiLOの動作に影響しそうな領域は順番に改ざんしてみたが、全て検知されてしまうので、検知機構の迂回をあきらめた。

ファームウェアの完全性を十分に意識して作られている。完全性を担保するためのコードや鍵はiLOチップの中に格納されており、手を出せない。IoT機器にとっても『理想の設計』だ。

今回は惨敗したが、次はもっと時間をかけてリベンジしたい。

※出典　https://japan.zdnet.com/extra/hpe_201809/35125875/
ハードウェアレベルでセキュリティを考える サイバーディフェンス研究所がHPE Gen10サーバーの耐性をテスト、その結果とは - ZDNet Japan

NIST Special Publication 800-193（2018年5月正式リリース）
プラットフォーム ファームウェアの復元ガイドライン

4.1.1 Roots of Trust (RoT) and Chains of Trust (CoT)

1. The security mechanisms **shall** be founded in Roots of Trust (RoT).
2. If Chains of Trust (CoT) are used, a RoT **shall** serve as the anchor for the CoT.
3. All RoTs and CoTs **shall** either be immutable or protected using mechanisms which ensure all RoTs and CoTs remains in a state of integrity.

RoTを持ったセキュリティー機構

RoTを起点とするCoT

RoT/CoTの完全性

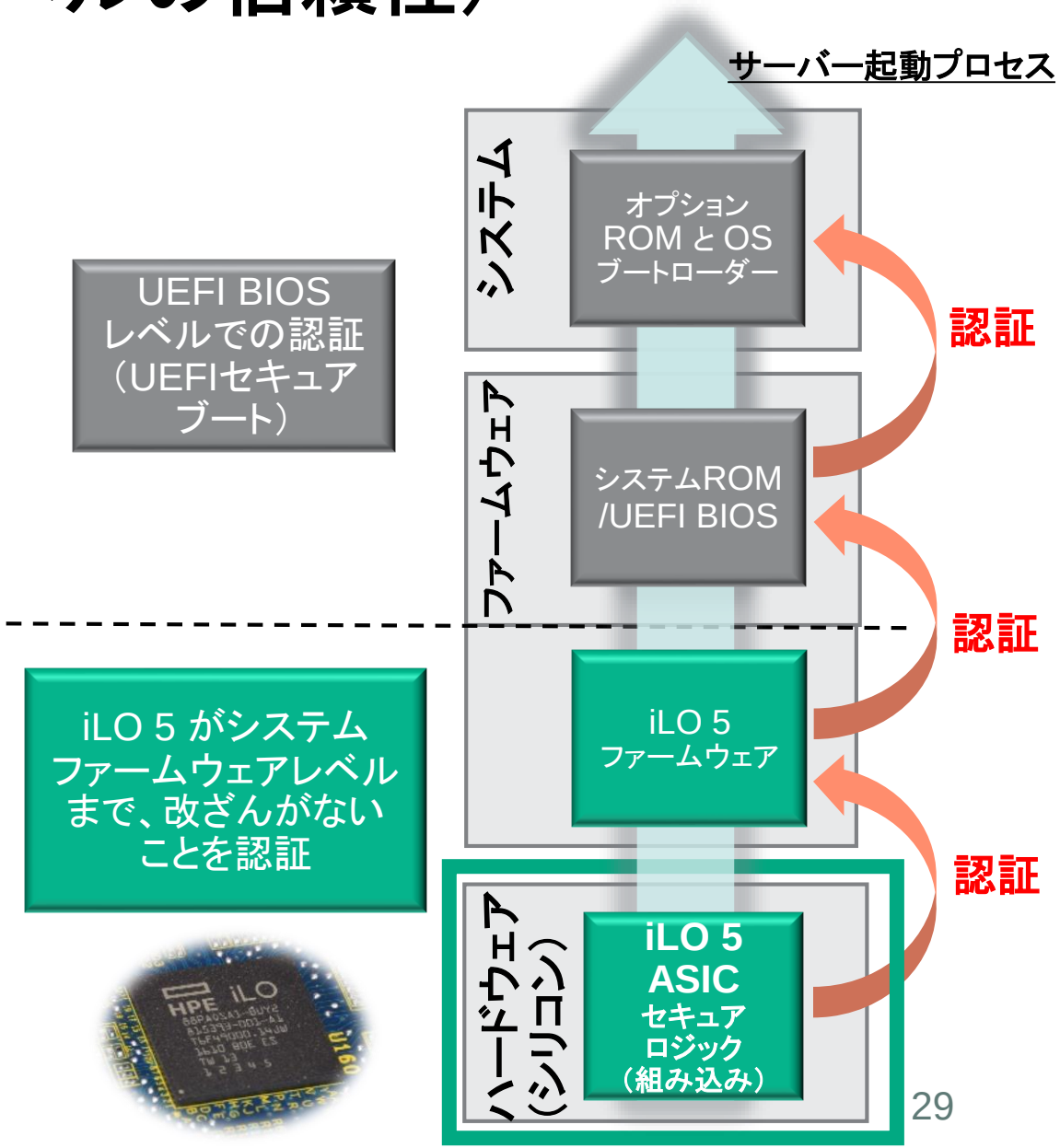
用語の意味：RFC2119,「しなければならない（ MUST ）」この語句、もしくは「要求されている（ REQUIRED ）」および「することになる（ SHALL ）」は、その規定が当該仕様の絶対的な要請事項であることを意味します。

出典：NIST SP800-193, 2018, P20
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

Silicon Root of Trust（シリコンレベルの信頼性）

自社設計・管理の重要性

- 自社で設計・管理している管理チップ内に、ファームウェアの正常性確認ロジックを組み込み
  - **製造段階でチップ自身に物理的に組み込むため、ロジック自身の改ざんは不可**
  - 従来はソフトウェアベースで実装するしかなく、ロジック自身の改ざんリスク
- サーバー起動時にはASICが起点となり、その後に続くファームウェアの改ざんがないことを確認してから起動
- OSレベル以上の対策では検知のできないファームウェアレベルの脅威を排除



ファームウェア改ざんの検知と復旧

セキュアリカバリー：検知・復旧までを実装
オンラインでのファームウェアの改ざん検知と復旧

①サーバー稼働中にファームウェアを検証

- iLOによってバックグラウンドで実行
- 手動で即時にも、定期的に自動でも実行可能

＊ファームウェアが改ざんされた場合

- iLO 5シリコンチップ内のセキュアロジックが
  ファームウェアの改ざんを検知

②リカバリーセットに復旧

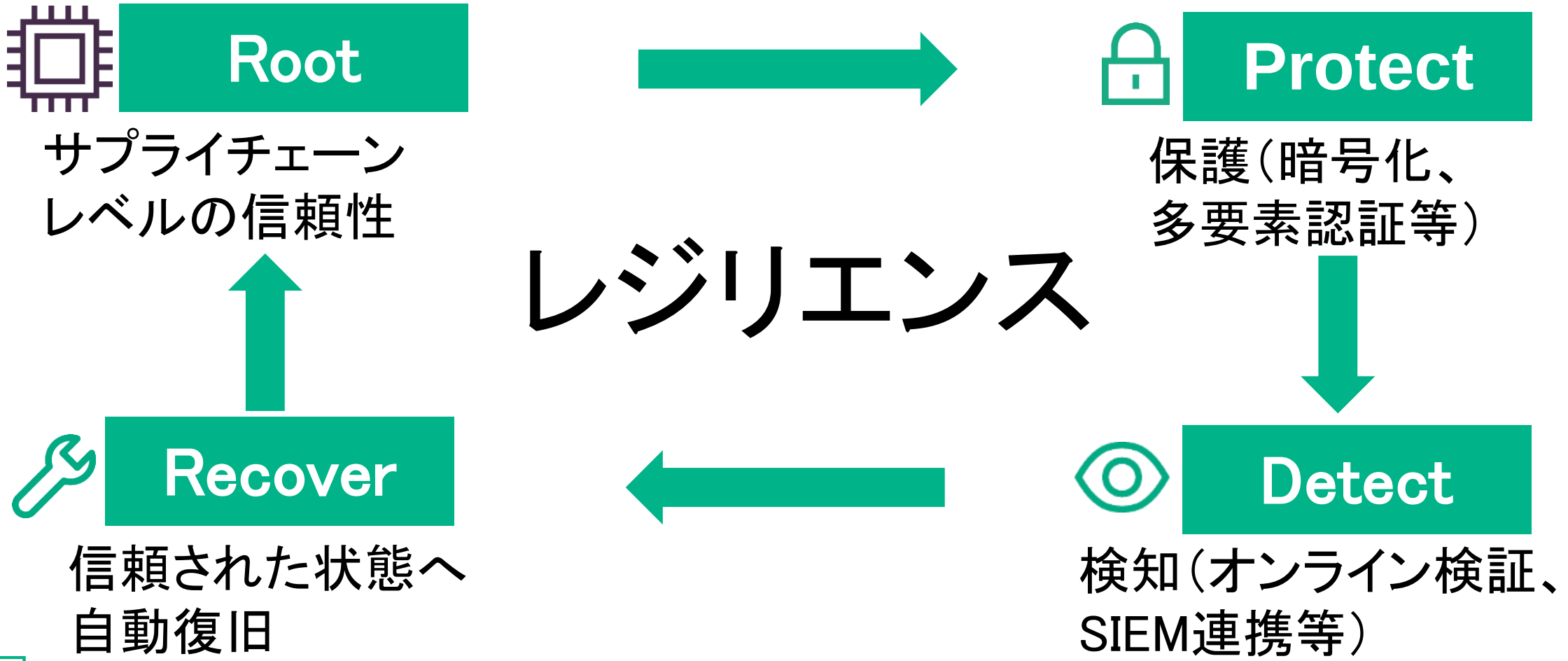
- 工場出荷時にリカバリーセットをiLO NAND内に格納
- お客様が新たなリカバリーセットを設定・保存も可能
- iLO、システムROM等のシステムファームウェア
  を稼働中に自動的に復旧することが可能

＜iLO 5管理画面：ステータス＞

＊iLO Advanced Premium Security Editionで対応

本当に求められているのはレジリエンス（復旧）

攻撃を受けるのは避けられない。大切なのはシステムを止めない・業務を継続すること



Hewlett Packard Enterprise

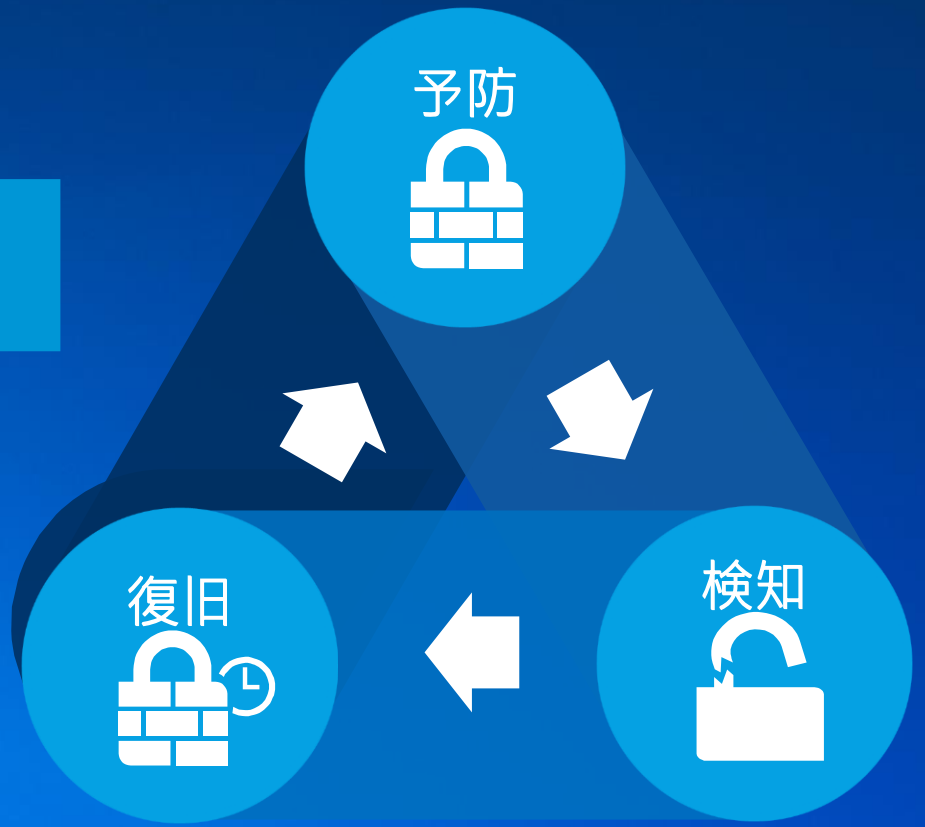
“レジリエンス”を実現する唯一のビジネスPC

HPの各セキュリティソリューション

ブラウジングと添付ファイル	HP Sure Click
ソフトウェアイメージ	HP Sure Recover
アンチウイルスソフト OSセキュリティ機能	HP Sure Run
MBR/GPT BIOS/BIOS設定/SMM	MBR/GPT Security HP Sure Start

信頼の基点となる独自のセキュリティチップを内蔵

「自己回復力」を備える 世界で最も安全なビジネスPC



まとめ

– サーバーとそのファームウェアはシステムの根幹
深奥部へのサイバー攻撃の脅威に“今から”備える必要

– ゼロトラストの時代、個々のサーバーの保護・検知・復旧プロセスの
自働化による、レジリエンスの向上

– 利便性とのトレードオフでは「ない」ファームウェアセキュリティーの
仕組み

Hewlett Packard
Enterprise

Hewlett Packard
Enterprise

ご清聴、誠に
ありがとうございました。