エッジコンピューティングの時代にサーバーはどこにいくのか、自社製品をハッキングしてもらった話

日本ヒューレット・パッカード株式会社
ハイブリッドIT技術本部
及川信一郎

2020年2月14日

本日の内容

1. データー「センター」からデーター「エッジ」へ

2. サプライチェーン・リスク

   自社製品をハッキングしてもらった話

3. よりセキュアに、対抗策

Hewlett Packard Enterprise | intel

1.データー「センター」からデーター「エッジ」へ

Hewlett Packard Enterprise

intel

「サーバー」のイメージ

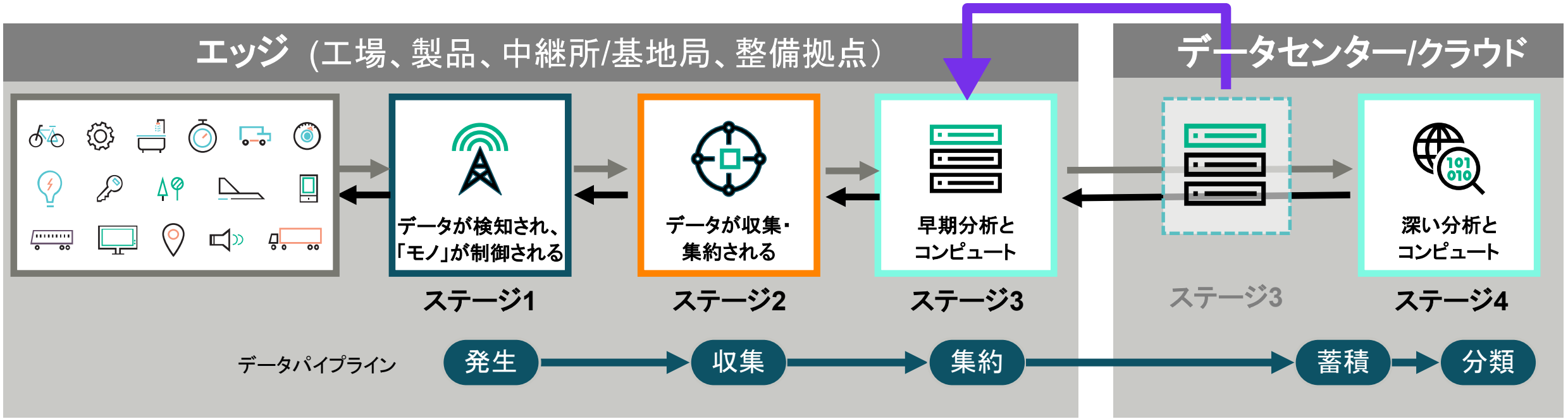
HPE ProLiant DL20 Gen10 Server

Hewlett Packard Enterprise

intel

データーセンター のイメージ

大量のデータから“価値”を得るために



- センサーから発生する大量のデータに**より近いところ**で処理
- データを蓄積して時間をかけて分析を行う前に、**リアルタイムに**データを処理・分析
- データの“賞味期限”切れやアラート検知遅れを防ぎ、**迅速なアクション**を起こす

Hewlett Packard Enterprise | intel

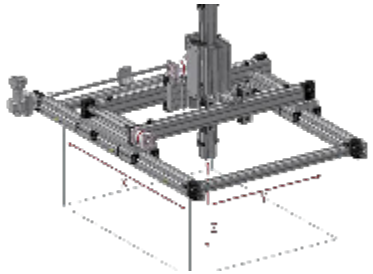
HPE EDGELINE EL300 CONVERGED EDGE SYSTEM

- **過酷な環境**
  - IP50、動作温度-30℃～70℃
- **物理インターフェース**
  - 4port1GbE TSN, CAN Bus, Serial, GPIO
- **リモート管理**
  - iSMでWiFiベースのリモート管理

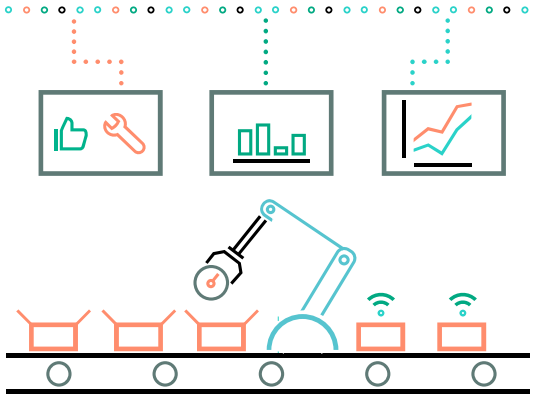
Hewlett Packard Enterprise | intel

FOXCONN MANUFACTURING – MACHINE VISION STATION

Configure to Order(CTO) 製品ラインのインテリジェント監査



ガントリーロボット
カメラ
HPE Edgeline EL4000
機械学習



生産量
45000台/月
1台当たりの監査時間
96秒短縮

Benefits

ROI
~ **1.5** years*
* Depends on factory volume

Product quality
First Pass Yield
+1%
Out Of Box audit
-25%

Customer Experience
Defect on Arrival
-25%

監査に必要な高解像度写真:1枚当たり75MB
リアルタイム処理

処理時間

Cloud
21 seconds

vs.

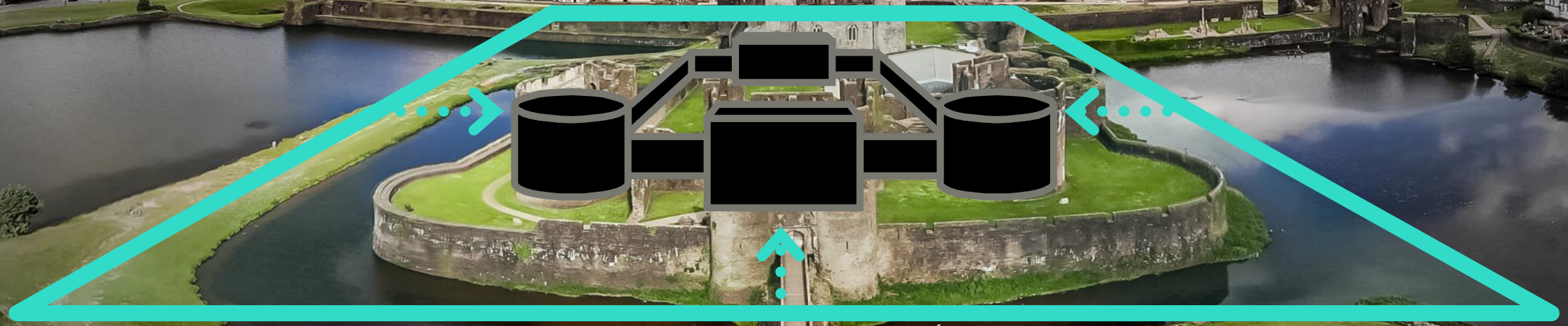
Edgeline
1 seconds

Hewlett Packard Enterprise

intel

新たに生まれてきたセキュリティー上の脅威

- 70%のデータが、データーセンターの「外側」に存在する
- 半数以上のセキュリティー侵入が、ファイヤーウォールの内側で起こっている*
- エッジからデータセンターまでを、セキュアにする必要性



Hewlett Packard Enterprise | intel

*FBI, James Morrison June 2018

FBIが警鐘を鳴らすファームウェアレベルの新たな脅威-2017年

Hewlett Packard Enterprise | intel

サイバーセキュリティの脅威の増大 – 2019年

2021年までにサイバー犯罪は世界経済に6兆ドルの損害を与える予測*

ジェームズ・モリソン
コンピュータ
サイエンティスト
連邦捜査局（FBI）

ボブ・ムーア
ディレクター
サーバーソフトウェア&
セキュリティ
ヒューレット・パッカード エンタープライズ（HPE）

Pants Down

SPOILER

サイバーセキュリティはますます重要に

HPEは、FBIと協力して新しいセキュリティ機能を開発

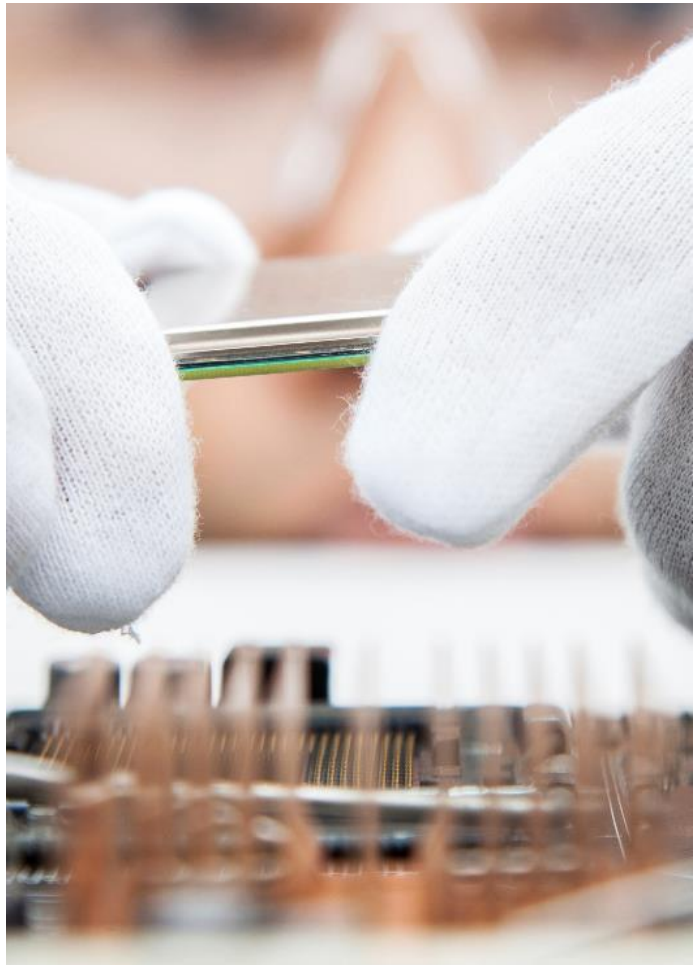
Hewlett Packard Enterprise | intel

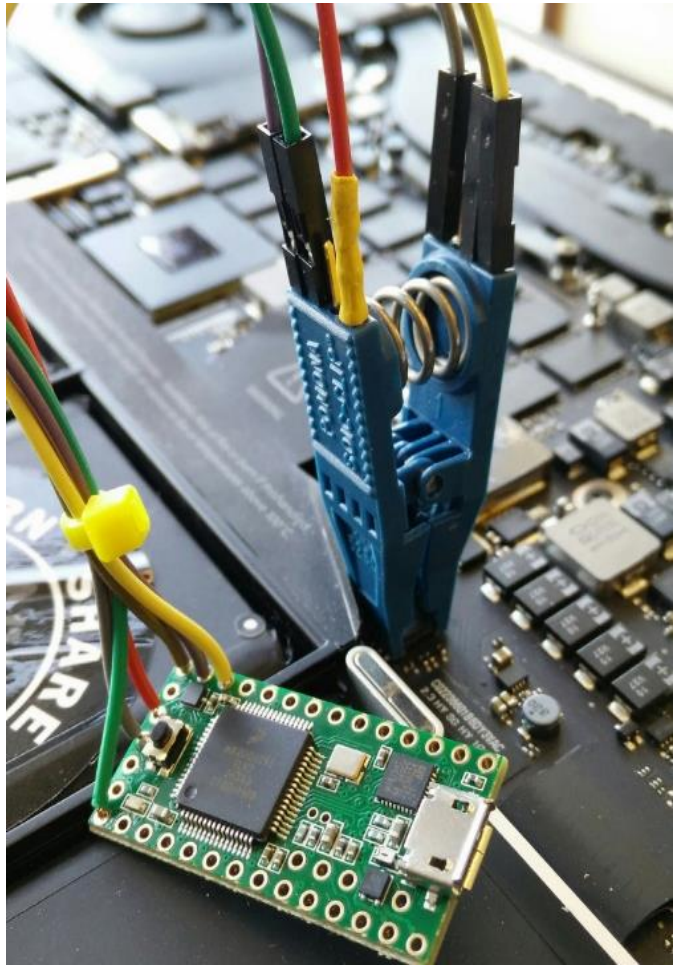
*Cyber Security Ventures Research

2. サプライチェーン・リスク

サプライチェーンへのリスクが増大

ハードウェアレベルの対策が求められる時代





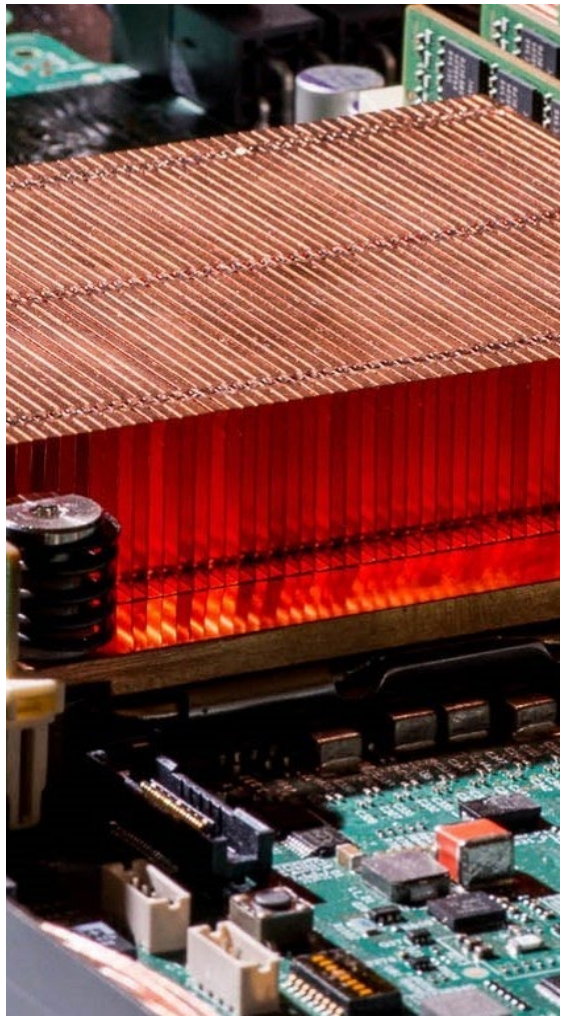
情報セキュリティ10大脅威 2019 組織編

順位	組織における10大脅威	昨年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	**サプライチェーンの弱点を悪用した攻撃の高まり**	NEW
5位	内部不正による情報漏えい	8位
6位	サービス妨害攻撃によるサービスの停止	9位
7位	インターネットサービスからの個人情報の窃取	6位
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開に伴う悪用増加	4位
10位	不注意による情報漏えい	12位

出典：2019年4月、情報処理推進機構（IPA）発表
2018年に発生した社会的に影響が大きかったと考えられる
情報セキュリティ事案から選出
https://www.ipa.go.jp/security/vuln/10threats2019.html

Hewlett Packard Enterprise | intel

新たなリスク要因、インフラストラクチャのサプライチェーン・リスク



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

- 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）

Hewlett Packard Enterprise | intel

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 | intel

外部機関によるペネトレーションテストで*
HPE ProLiant 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

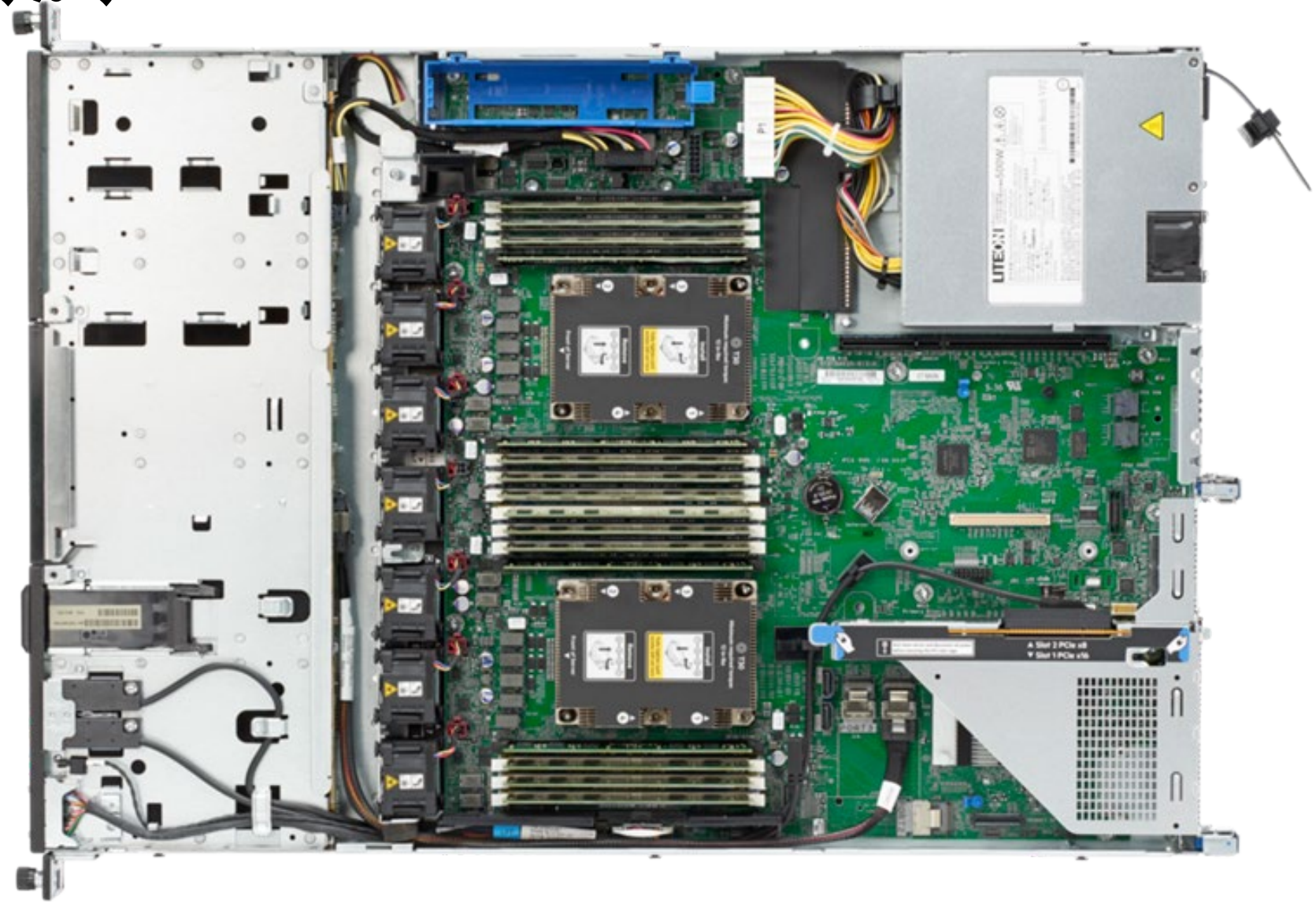
InfusionPoints
Cyber Security Solutions

＊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 | intel

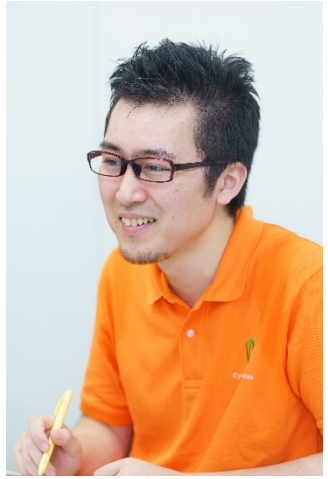
日本ではできないの？

断られ続けた、が、



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。

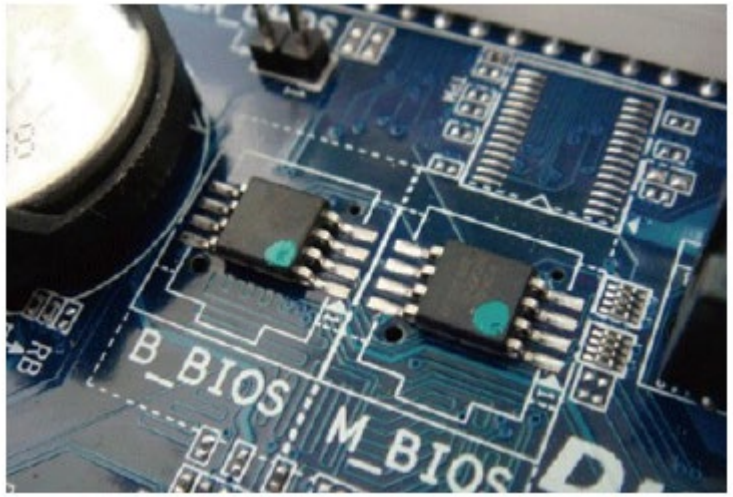
ファームウェアの完全性を十分に意識して作られている。完全性を担保するためのコードや鍵はiLOチップの中に格納されており、手を出せない。IoT機器にとっても『理想の設計』だ。

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

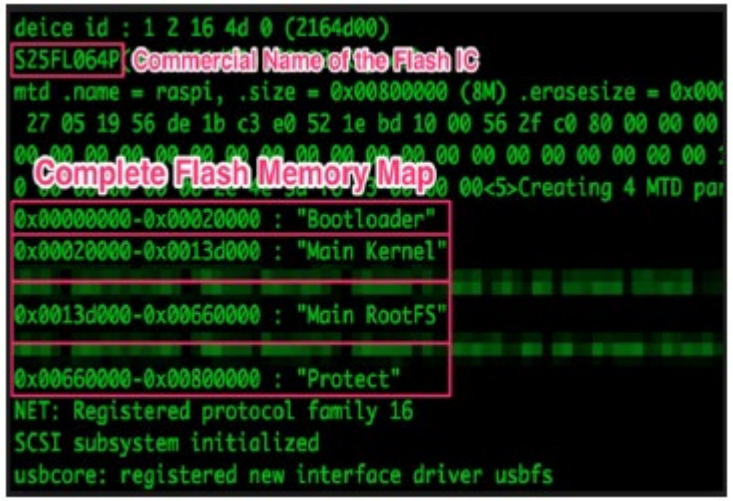
Hewlett Packard Enterprise | intel

WEBや電気街で簡単に買える機材で、クラッキングは可能



標準的なSPI flash メモリは、世界中のあらゆるシステムに搭載されている

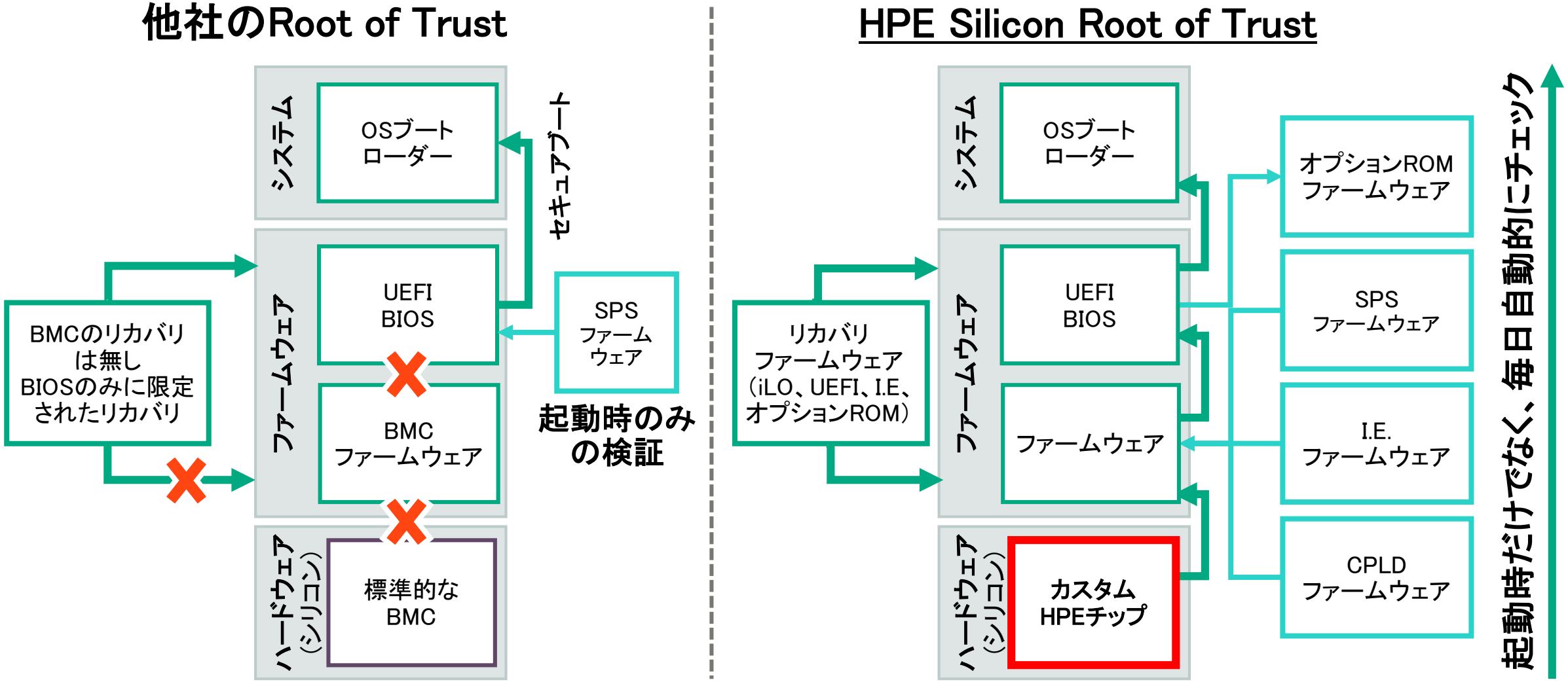
電源が切られた状態であっても、普通に売られているパーツを使って、システムに接続可能



システムの書き換え自体は、技術的に言って、高難度ではない

Hewlett Packard Enterprise | intel

HPE Silicon Root of Trust：他社のRoot of Trustとの違い



Hewlett Packard Enterprise | intel

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

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**

  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

3. よりセキュアな、対抗策

NIST（米国国立標準技術研究所）

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は、科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関です。
　NIST内には、情報技術に関する研究を行っているITL（Information Technology Laboratory）があります。

　ITLは情報技術に関して6つの分野（Security, Information Access, Mathematics and Computational Science, Software Testing, Networking Research, Statistical Engineering）の研究を行っており、ITLの中でコンピュータセキュリティに関して研究を行い各種文書を発行しているのがCSD（Computer Security Division）と呼ばれる部門です。FIPSやSP800シリーズの文書も、CSDが発行しています。

出典：IPA（情報処理推進機構）ホームページより
https://www.ipa.go.jp/security/publications/nist/nist_publications.html

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

Hewlett Packard
Enterprise

intel

ファームウェア保護の必要性 NIST SP800-147B

“Modern computers rely on fundamental system firmware, commonly known as the Basic Input/Output System (BIOS), to facilitate the hardware initialization process and transition control to the hypervisor or operating system. Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS’s unique and privileged position within the PC architecture. “

Abstract, NIST SP800-147B BIOS Protection Guidelines for Servers(2014/8)

現在のコンピュータはその基盤となるファームウェアに依存している。これは、BIOS(Basic Input/Output System)として知られ、ハードウェアの初期化プロセスと、ハイパーバイザー/OSに制御を渡す役割を果たしている。悪意あるソフトウェアにより不正に改ざんされたBIOSは、重大な脅威となる。なぜなら、BIOSはPCアーキティクチャの中で、特殊かつ特権的な位置にあるためである。

摘要、NIST SP800-147B サーバーの為のBIOS保護ガイドライン(2014年8月)

Hewlett Packard Enterprise | intel

NIST SP800-147/800-193が推奨するプラットフォーム・セキュリティ対策

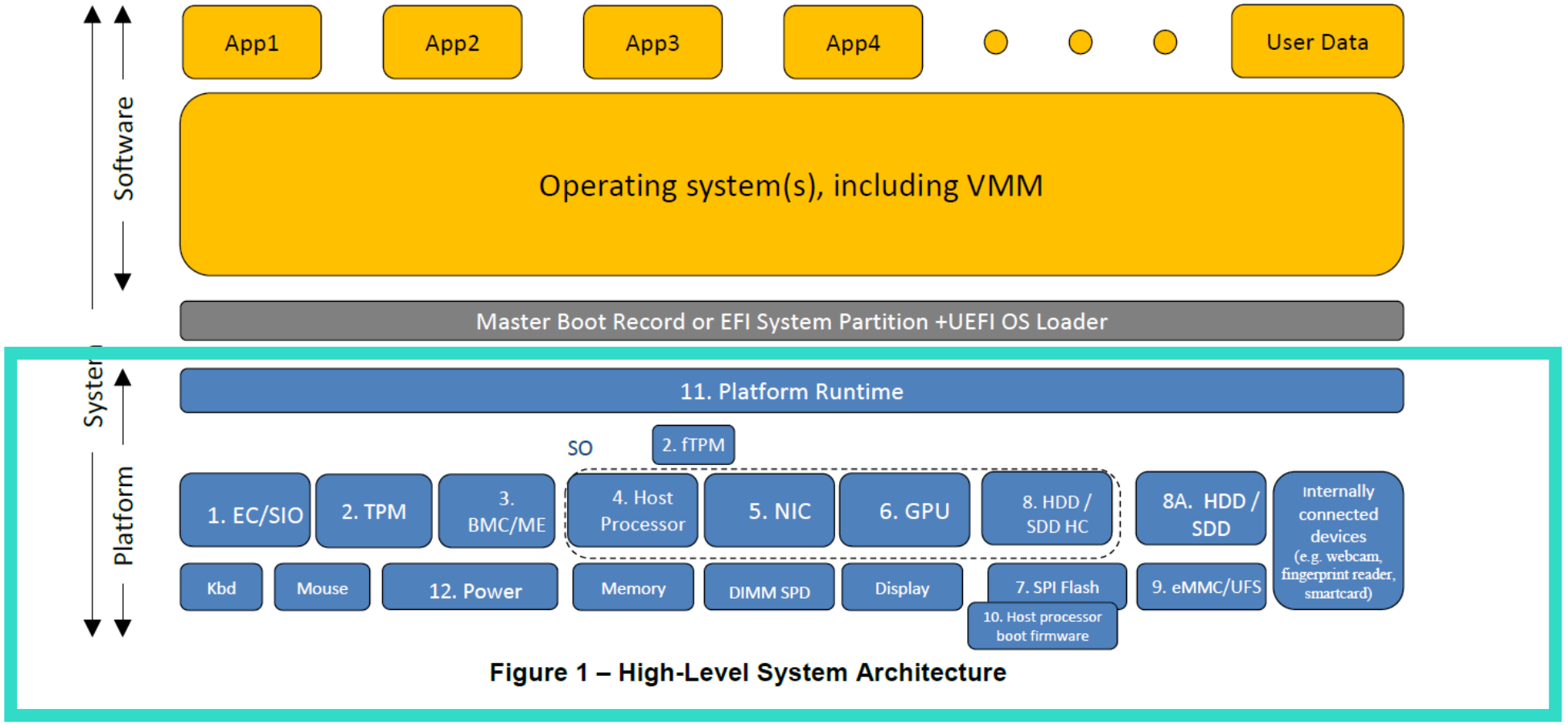


Figure 1 – High-Level System Architecture

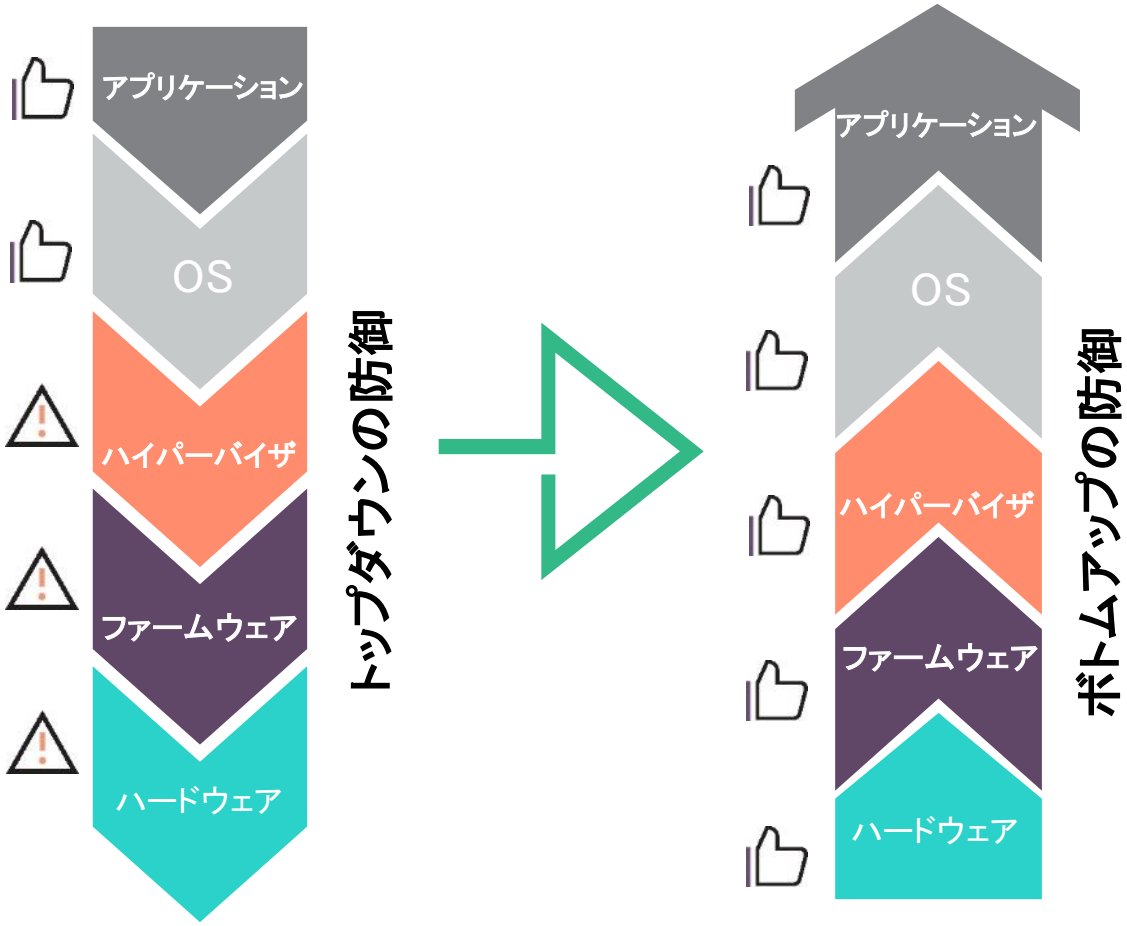
出典：NIST SP800-193, 2018, P3
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

Hewlett Packard Enterprise | intel

HPEのセキュリティビジョン：サーバープラットフォームセキュリティ

総合的なセキュリティアプローチで、インフラの安全性を確保する

- ✓ ルートキット、ブートキット
- ✓ 不正なファームウェアによる更新
- ✓ ファームウェアに対するサプライチェーンアタック
  オプションROMへのアタック
- ✓ 管理プロセッサへのアタック
- ✓ ファームウェア・サプライチェーンアタック



Hewlett Packard Enterprise | intel

第2世代インテル® Xeon® スケーラブル・プロセッサー

インテル® Xeon® Platinum 9200 プロセッサー

新たなクラスの
高度なパフォーマンス

インテル® Xeon® Platinum 8200 プロセッサー

インテル® Xeon® Gold 6200 プロセッサー

インテル® Xeon® Gold 5200 プロセッサー

インテル® Xeon® Silver 4200 プロセッサー

インテル® Xeon® Bronze 3200 プロセッサー

トップクラスのワークロード・パフォーマンス

画期的なメモリー・イノベーション

人工知能アクセラレーション

ハードウェア支援型セキュリティー

俊敏性と使用率の向上

第2世代インテル® Xeon® スケーラブル・プロセッサー

インテル® Xeon® Platinum 8200 プロセッサー

インテル® Xeon® Gold 6200 / 5200 プロセッサー

インテル® Xeon® Silver 4200 プロセッサー

インテル® Xeon® Bronze 3200 プロセッサー

最大 **3.50 倍**

5 年前のシステムからのパフォーマンス向上[4]

インテル® Xeon® プロセッサー E5-2600 v2 製品ファミリーと比較した場合の VM 密度

最大 **1.33 倍**

平均パフォーマンス向上[5]

インテル® Xeon® Gold 5100 プロセッサーとの比較

最大 **14 倍**

インテル® DL ブーストによる AI パフォーマンス[6]

インテル® Xeon® Platinum 8180 プロセッサー (2017年7月) との比較

サイドチャネル攻撃対策

暗号化 + アクセラレーター

インテル® セキュリティー・ライブラリー

ハードウェア支援型セキュリティーによるビジネスの耐障害性

インテル® ディープラーニング・ブースト (DLブースト)

インテル® スピード・セレクト・テクノロジー

インテル® インフラストラクチャー・マネジメント・テクノロジー

効率の向上による俊敏性に優れたサービス提供

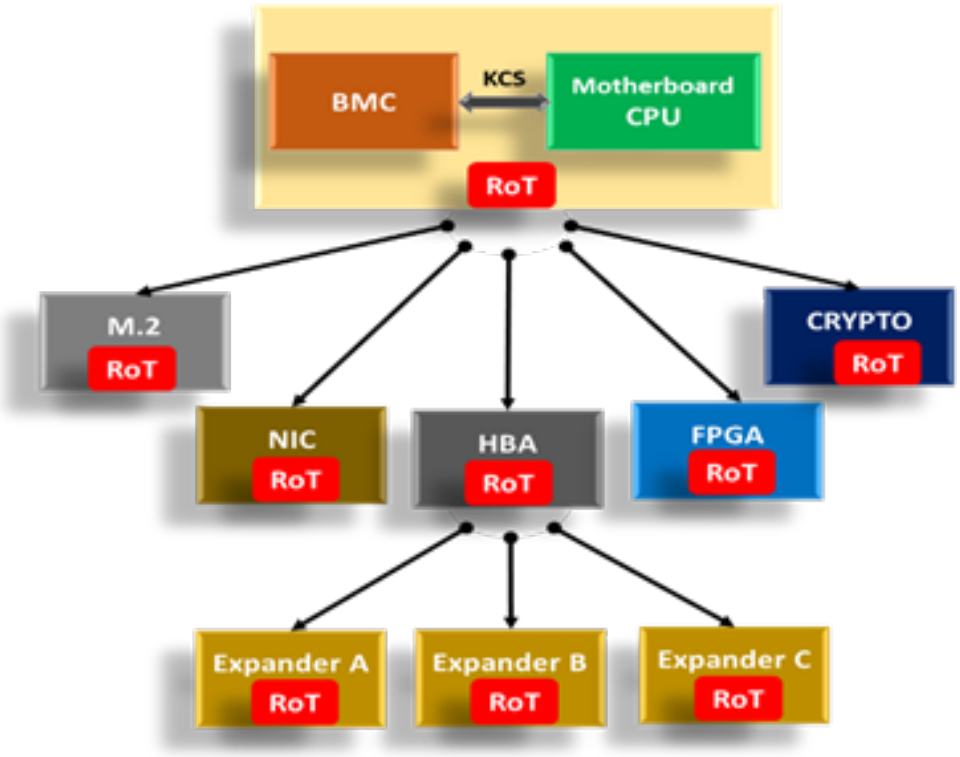
インテル® スピード・セレクト・テクノロジーは一部のプロセッサー上で利用できます。

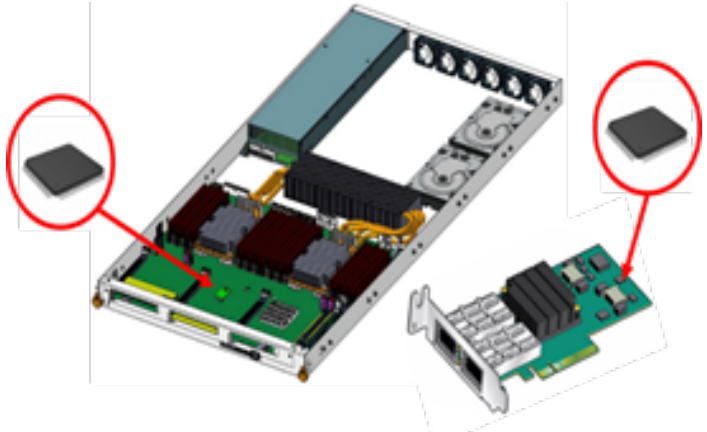
性能の測定結果は、構成に示した日付時点のテストに基づいています。また、現在公開中のすべてのセキュリティー・アップデートが適用されているとは限りません。構成とベンチマークの詳細は、スライド 50 ～ 51 ページに記載しています。 絶対的なセキュリティーを提供できる製品やコンポーネントはありません。 性能に関するテストに使用されるソフトウェアとワークロードは、性能がインテル® マイクロプロセッサー用に最適化されていることがあります。SYSmark* や MobileMark* などの性能テストは、特定のコンピューター・システム、コンポーネント、ソフトウェア、操作、機能に基づいて行ったものです。結果はこれらの要因によって異なります。製品の購入を検討される場合は、他の製品と組み合わせた場合の本製品の性能など、ほかの情報や性能テストも参考にして、パフォーマンスを総合的に評価することをお勧めします。 詳細については、http://www.intel.com/benchmarks/ (英語) を参照してください。

パブリッククラウドベンダーの取り組み状況
Microsoft Azure

- 2017年より、“Project Cerberus”を推進
- セキュリティ用 コ・プロセッサで、Root of Trustを実装

- プロジェクト「Cerberus」はセキュリティ コ・プロセッサであり、コンピューティングプラットフォームのあらゆるデバイスとroot of trustを確立し、プラットフォームファームウェアを以下の様な脅威から守る:
  - 管理者特権や、ハードウェアへのアクセス権を持った悪意ある内部の人間
  - OS,アプリケーション、ハイパーバイザのバグ・脆弱性を利用する、ハッカー及びマルウェア
  - サプライチェーンアタック(生産、組立、輸送)
  - 改ざんされたファームウェアバイナリ



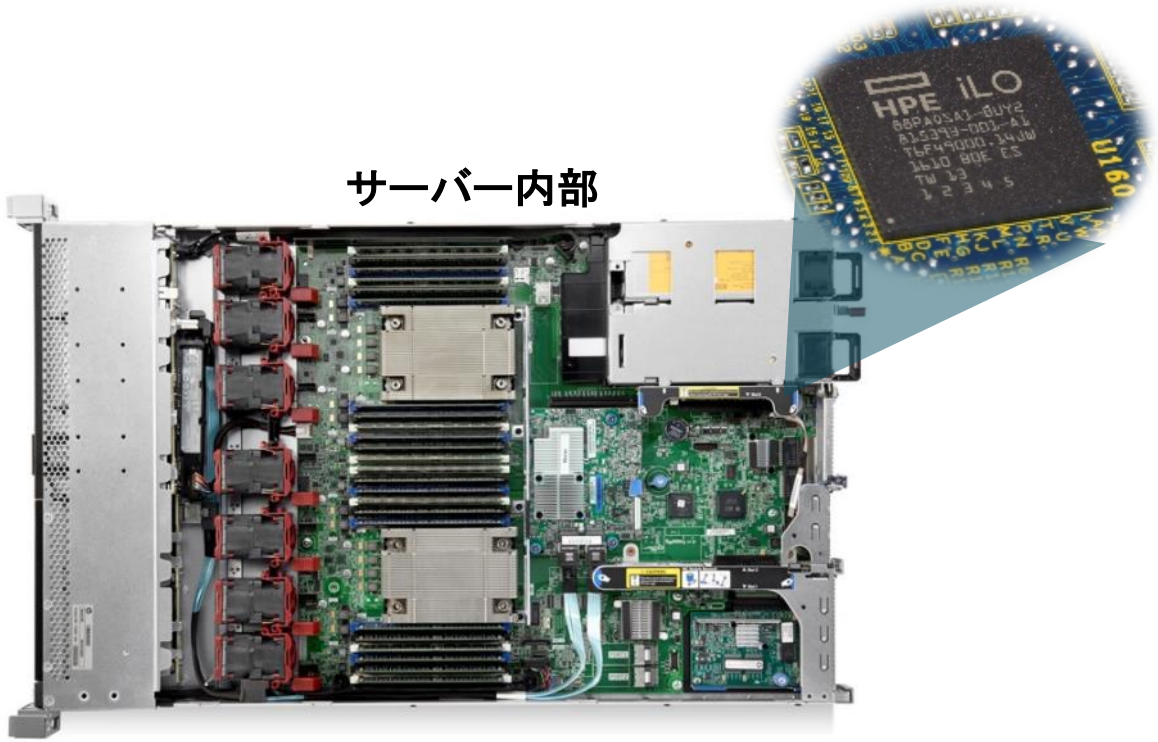


出典:https://azure.microsoft.com/en-us/blog/microsoft-creates-industry-standards-for-datacenter-hardware-storage-and-security/
https://azure.microsoft.com/en-us/blog/microsofts-project-olympus-delivers-cloud-hardware-innovation-at-scale/

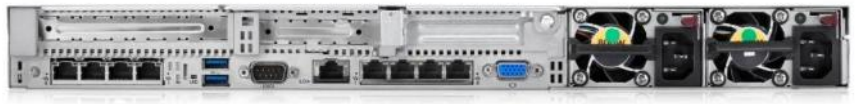
Hewlett Packard Enterprise | intel

iLO (Integrated Lights-Out) とは?
システムの運用を支え続ける縁の下の力持ち

サーバー内部



サーバー背面



- 主要HPE サーバーに標準搭載されている「小型コンピューター」
- サーバー自身のリソースから独立した専用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
- 自社開発にこだわり数多くの特許を取得
- お客様の声を反映し、セキュリティ強化を重視

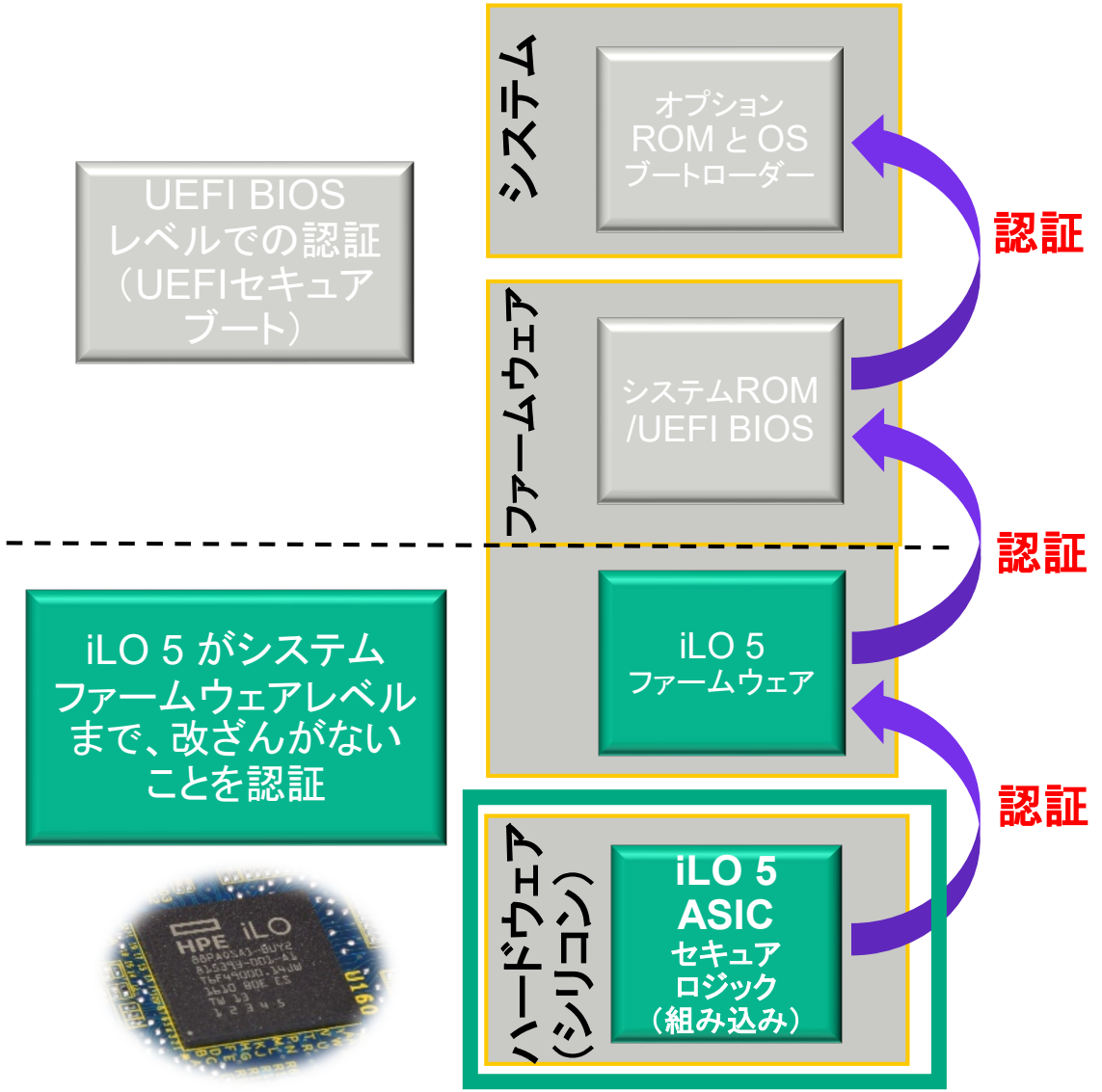
Gen10で iLO 5 に進化

これからのセキュリティの標準となる機能を実装

Hewlett Packard Enterprise | intel

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
  - 起動後、OS稼働中も自動でファームウェアの改ざんチェックを行い、改ざんを検知した場合自動で復旧（HPEだけの特長。＊iLOライセンス必要）
- 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



Hewlett Packard Enterprise | intel

奥行42CM 最もコンパクトな汎用ラックサーバー

コンパクト筐体

組み込み用途
エッジサーバーとして最適

拡張性・信頼性

最大90TB(6SFF)
RAID, 冗長電源対応

安心セキュリティ

HPEだけの改ざんの
検知・修復機能

HPE ProLiant DL20 Gen10 Server

インテル®Xeon®
スケーラブル
プロセッサー搭載

Hewlett Packard Enterprise

まとめ

- サーバーは、データーセンターから外に出て行く
- 「信頼できるハードウェア」の仕組みを、つくっていく
- ProLiant, Edgelineはデーターセンター・エッジで
  信頼できるコンピュートを実現する

Hewlett Packard Enterprise

intel