Hewlett Packard Enterprise

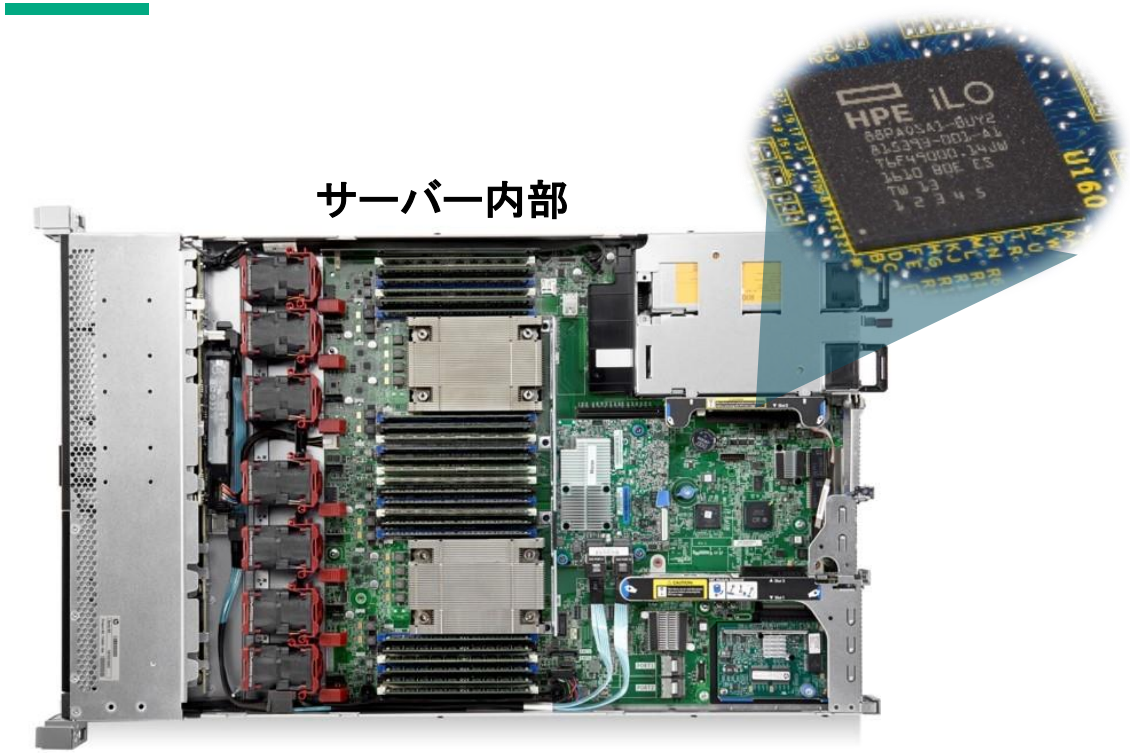
Gen10/iLO 5で強化されたセキュリティに関する機能

日本ヒューレット・パッカード合同会社

2021年12月

HPE iLO 5の概要

iLO（Integrated Lights-Out）とは?
お客様の運用を支え続ける縁の下の力持ち



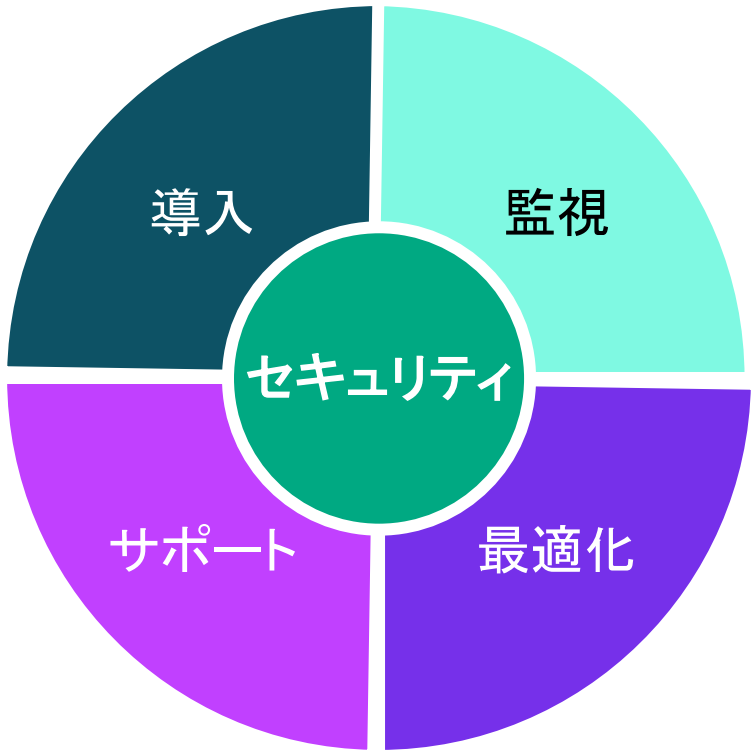
- 主要HPE サーバーに標準搭載されている**「小型コンピューター」**
- サーバー自身のリソースから**独立した専用ASIC**
- リモート操作はもちろん、サーバーの導入から解析まで、**ライフサイクル全般**をカバー
- **自社開発**にこだわり数多くの特許を取得
- お客様の声を反映し、**セキュリティ強化を重視**

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

HPE iLO 5はProLiant Gen10サーバー運用管理の要

サーバーのライフサイクル全体をカバー



- **導入**
  - Intelligent Provisioning
- **監視**
  - Agentless 管理
  - Active Health System
- **最適化**
  - Intelligent System Tuning
- **サポート**
  - Embedded Remote Support
- **セキュリティ**
  - **Silicon Root of Trust**
  - **セキュアリカバリー**

iLOとは？ イノベーションとセキュリティ強化の歴史

お客様の要望を愚直に反映することで劇的に進化

iLO | iLO 2 | iLO 3 | iLO 4 | iLO 5

2002
サーバー内蔵管理プロセッサ

ハードウェアベースのグラフィカルリモートコンソール

日本語対応

iLOファームウェアはデジタル署名済み/セキュアに更新

2003
LDAPとの統合

仮想CDドライブ

2006
内蔵リモートコンソール

高速共有ネットワークポート

2007
AES暗号化

リモートコンソールの録画と再生

認証のロギング

2008
ダイナミックパワーキャッピング

2010
ハードウェアベースのAES暗号化エンジン

2011
Kerberos認証

2要素認証

2012
iLO 3がFIPSフル認証取得

BIOSをセキュアに更新

2012
Active Health System

Agentless管理

内蔵リモートサポート

2013
SNMP v3

2014
iLO連携

2015
iLO 4がFIPS フル認証取得

2017
これからの標準となる新たな進化を実現

セキュリティに関するたゆまぬ強化と進化

HPE Secure Compute Lifecycle
“世界標準の安心サーバー”を実現

Protect

- シリコンベースのセキュリティ
- セキュリティロックダウン
  - ホストからのファームウェアアタックを防御
  - CNSAスイートに対応
- スマートカードを利用した二要素認証をサポート
- ファームウェアダウングレードポリシーの設定

- セキュリティダッシュボード
- サーバー構成ロック
- One-buttonセキュア消去
- サードパーティーキーマネーャーをサポート

Detect

- ファームウェアの改ざんを検知
  - セキュアスタート
  - オンラインでのファームウェアの検証
- サーバー侵入検知センサー

- ラックドア開閉センサー

Recover

- セキュアリカバリー
- 改ざんされたファームウェアの隔離
- サーバーシステムリストア

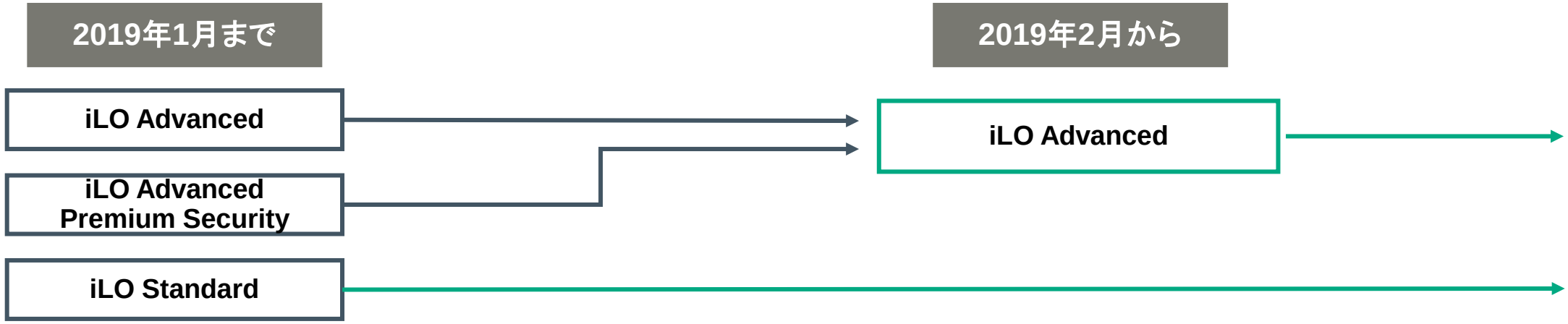
Gen10から利用可能になった機能

2019年2月リリースのiLO 5 v1.40で追加された機能

Gen10リリース後に販売開始された関連オプション

iLO 5 ライセンス体系の簡素化

iLO Advancedですべての機能が利用可能に！



- **今回の変更の目的**
  HPEはセキュリティは非常に重要だと考えており、できるだけ多くのお客様がセキュリティ強化のためだけに追加費用を払う必要なく安心してサーバーをお使いいただくために、今回の変更を決断しました。
- **既存でiLO Advanced Premium Securityをご利用のお客様**
  引き続きすべての機能をご利用可能です。
- **既存でiLO Advancedをご利用のお客様や新規にiLO Advancedを購入されたお客様**
  iLO 5のファームウェアをv1.40以降にアップデートすることで、すべての機能をご利用可能です。

※各ライセンスで利用できる機能の違いは http://www.hpe.com/support/iLO-LicenseMatrix-ja を参照ください。

Protect

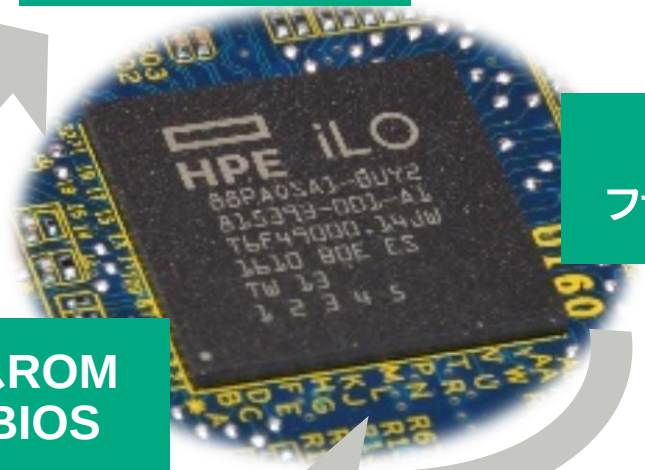
Protect

iLO Standard
(一部機能は
iLO Advanced)

これからの標準：シリコンベースのセキュリティ
HPEが自社で管理チップの設計を行っているからこそ実現できる

Silicon Root of Trust

オプションROMと
OS ブートローダー



iLO 5
ファームウェア

システムROM
/UEFI BIOS

iLO 5

**従来のサイバー攻撃に加えて
ハードウェアのファームウェアレベル
に対するアタックが拡大**

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

- HPE自身が設計した管理チップiLO 5内に、ファームウェアの正常性確認ロジックを組み込み
  - iLO 5チップ自身に組み込まれており、ロジック自身の改ざん不可
  - ***他社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あり***
- 起動時には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
- オンラインでも改ざんのスキャニングが可能（定期実行も可能）

Protect

iLO Standard
(一部機能は
iLO Advanced)

セキュアスタート / セキュアリカバリー
一般的なx86サーバー(UEFIセキュアブート)との違い

industry

➢ UEFIセキュアブート

- UEFIファームウェアが起点
- ほとんどのサーバーメーカーはUEFIファームウェアを自社で開発していないため、信頼の起点を第三者に委ねることになる
- TPMを使用したソリューション（例えばIntel Boot Guard）でも、UEFIファームウェア以外のシステムファームウェアや管理プロセッサは保護されない
- サーバー起動時の確認のみで、サーバー稼働中の確認は行わない

HPE

➢ セキュアスタート

- ***iLO 5ハードウェアが起点***
- HPEはiLO 5ハードウェア、ファームウェア、System ROMを自社開発しており、***信頼の起点に関して自社で責任を持つ***

➢ セキュアリカバリー

- ***サーバー稼働中でも***即時または定期的に***確認可能***
- 問題が見つかったら、自動または手動で***正常な状態に復元***
- ***System ROM、システムファームウェア、管理プロセッサ***が対象

iLOへのアクセスも強固なセキュリティレベルにロックダウン

暗号化とアクセス制御のレベルに応じて4段階から選択

iLO Standard (一部機能は iLO Advanced)

- **環境、業界、コンプライアンス基準に応じた より高度なセキュリティ、暗号化のレベルを選択可能**

プロダクション モード

- 既存ソフトウェアとの互換性を最大化
- セキュアなネットワーク

ハイセキュリティ モード

- ホストインターフェースをロックダウン
- ネットワークインターフェイスでFIPSレベルの暗号を強制

FIPS 140-2 モード

- よりセキュア
- FIPS準拠
- IPMIとSNMP v1をシャットダウン

CNSA モード

- 最もセキュア
- CNSA準拠
- ネットワークインターフェイスでCNSAレベルの暗号を強制

認証 & 認可

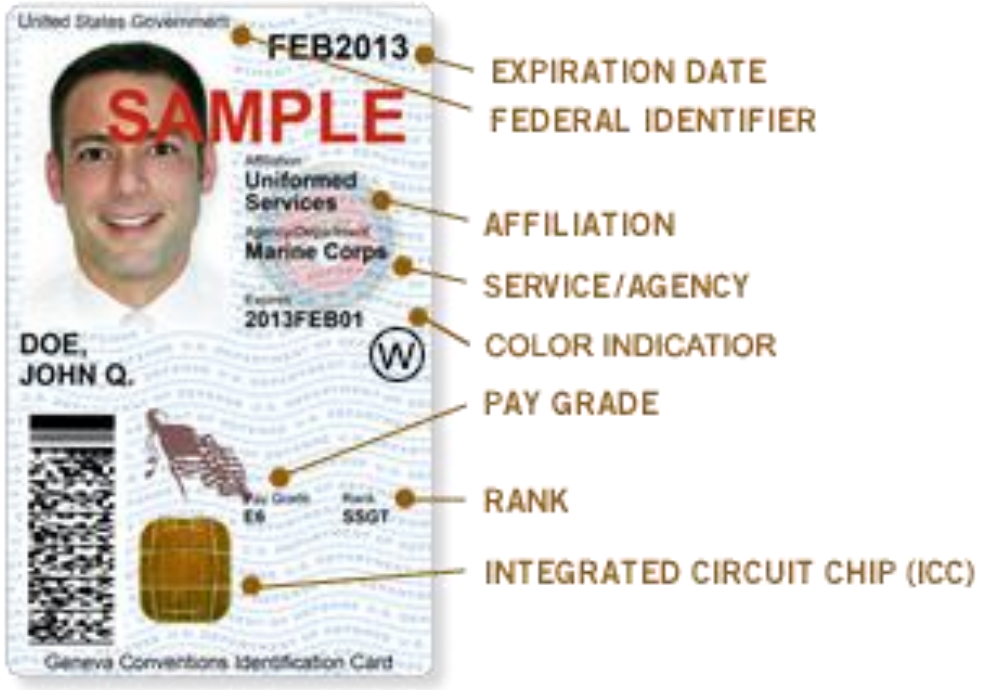
- Active Directory
- LDAP
- Open LDAP
- Kerberos 2要素認証
- CAC 2要素認証

Protect

iLO Advanced

スマートカードを利用した二要素認証のサポート
CAC/PIVに対応

- **セキュリティ強化の一環として、スマートカードを利用した認証に対応**
  - カードにPINと証明書（X.509）を格納
  - Active Directoryと連携して認証
  - Common Access Card（CAC）※1と Personal Identity Verification（PIV）※2カードに対応



※1 米国防総省(DoD)の多要素認証スマートカード。
現役軍人、予備員、軍属、DoD外政府職員、州兵、指定業者社員の標準IDとして発行される。

※2 米国国立標準技術研究所(NIST)が規定した個人識別情報の検証の仕組み。

Protect

iLO Standard

ファームウェアダウングレードポリシーの設定
過去バージョンのファームウェアにダウングレードされるのを防御

- **脆弱性がある過去のバージョンにダウングレードされてしまうのを防ぐオプション**
  - 攻撃者は既知の脆弱性を利用するために ファームウェアのダウングレードを試みることがある
- **System ROM、システムファームウェア、管理プロセッサが対象**
- **以下から選択可能**
  - ダウングレードの許可(デフォルト)
  - ダウングレードには'リカバリセット'の権限が必要
  - ダウングレードを永遠に不許可
    - ***一度これに変更してしまうと、二度と変更できない！***

Protect

iLO Standard

セキュリティダッシュボード

セキュリティに関する推奨の参照と設定を一覧化

- **iLOを中心としたセキュリティに関する現状と推奨をひと目で把握可能**
- **必要に応じて設定を変更するか無視することが可能**

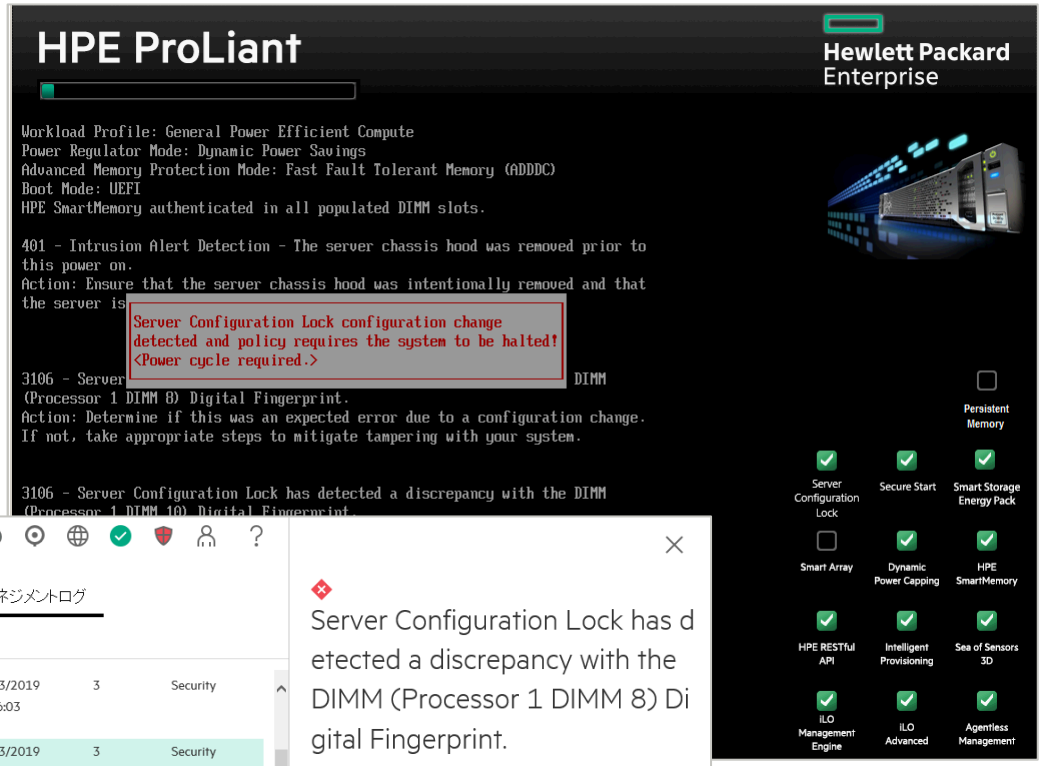
サーバー構成ロック

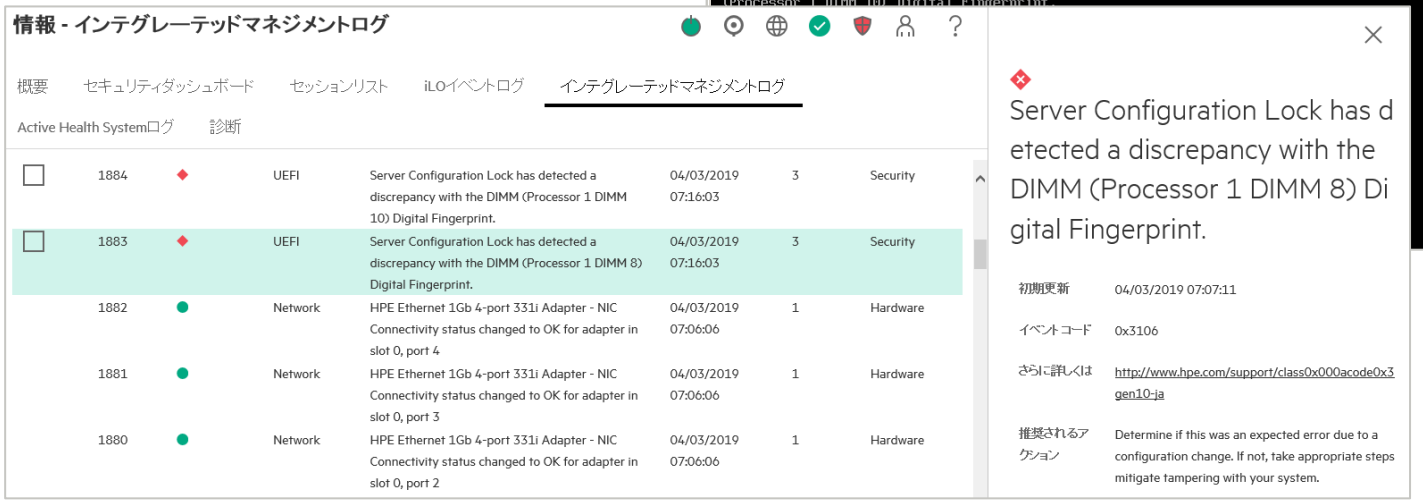
移動中および安全でない場所に展開されたシステムを保護

Protect

iLO Advanced

- **サプライチェーンリスク等に備えて、サーバー構成の変更を検知する機能を提供**
- **設定時に各アイテムの”デジタルフィンガープリント”を生成して、サーバー起動時に毎回変更がないかをチェック**
- **対象アイテム**
  - システムボード
  - CPU
  - メモリ
  - PCIeスロット
  - セキュリティ構成
  - システムファームウェア
- **想定利用ケース**
  - HPE工場からお客様への出荷
  - お客様の拠点間の移送
  - 安全でない環境への展開





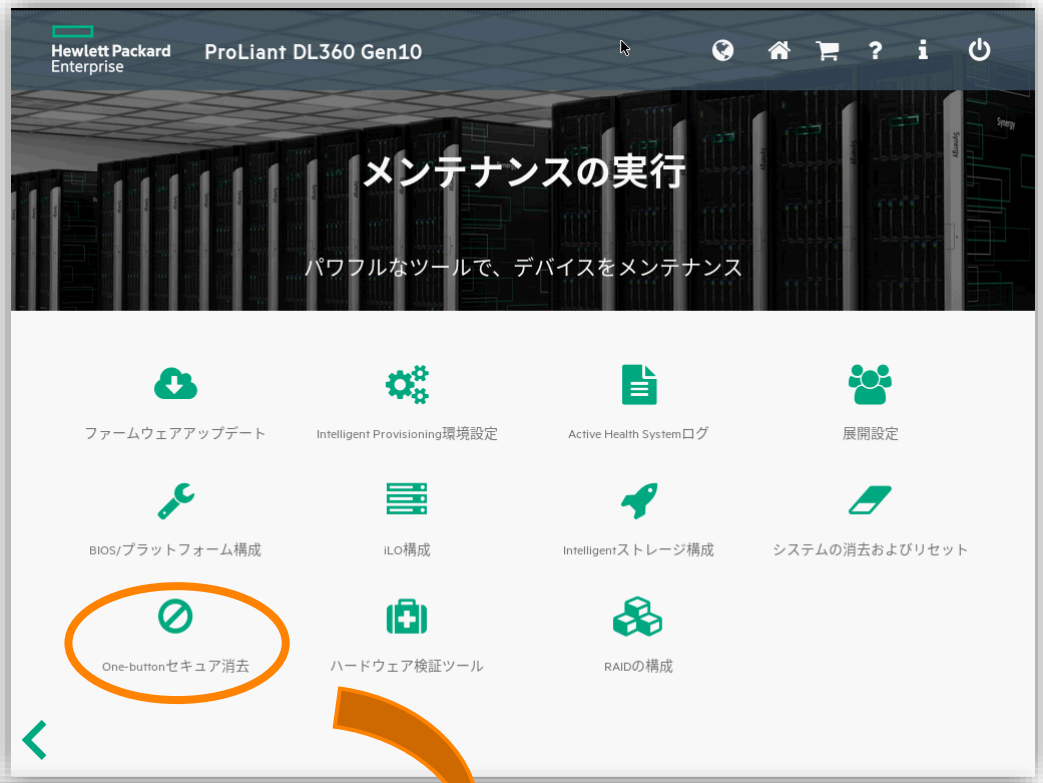
Protect

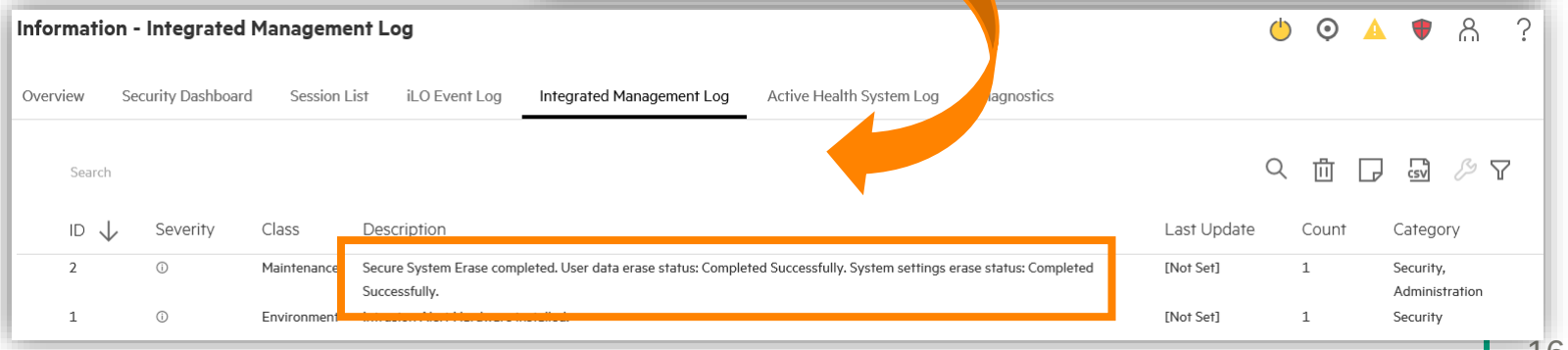
iLO Advanced

One-buttonセキュア消去

サーバーの初期化をワンボタンで実行可能に！

- **サーバーの廃棄や再利用等で初期化が必要な場合に便利な機能**
  - 手動で行うと大量の煩雑な手順を実施する必要がある
- **NIST SP 800-88, Revision 1（媒体のサニタイズに関するガイドライン）に準拠**
- **Intelligent ProvisioningやRESTful APIで実行可能**
- **以下を実行**
  - サーバーの各種設定を工場出荷時のデフォルトに初期化
  - 接続されているすべてのストレージ（セカンダリストレージとNVRAM）を消去





HPE Smart Array Secure Encryption

Smartアレイに接続されたドライブを暗号化

- **業界初のアレイコントローラーによる暗号化処理を実現**
  - 書き込みデータの暗号化によりディスク媒体の不正なデータ解読を防ぐ機能
  - Smartアレイコントローラーによる暗号化
  - 暗号化キーの管理はローカル・リモートの二種類から選択可能
    - リモートの場合、従来のUtimaco Enterprise Secure Key Manager（ESKM）に加えて、SafeNet AT KeySecureとGemalto SafeNet KeySecureにも対応

暗号化機能

Detect

セキュアスタート

iLO 5 を起点とした “安心の” サーバー起動プロセス

Detect

iLO Standard

①Silicon Root of Trust

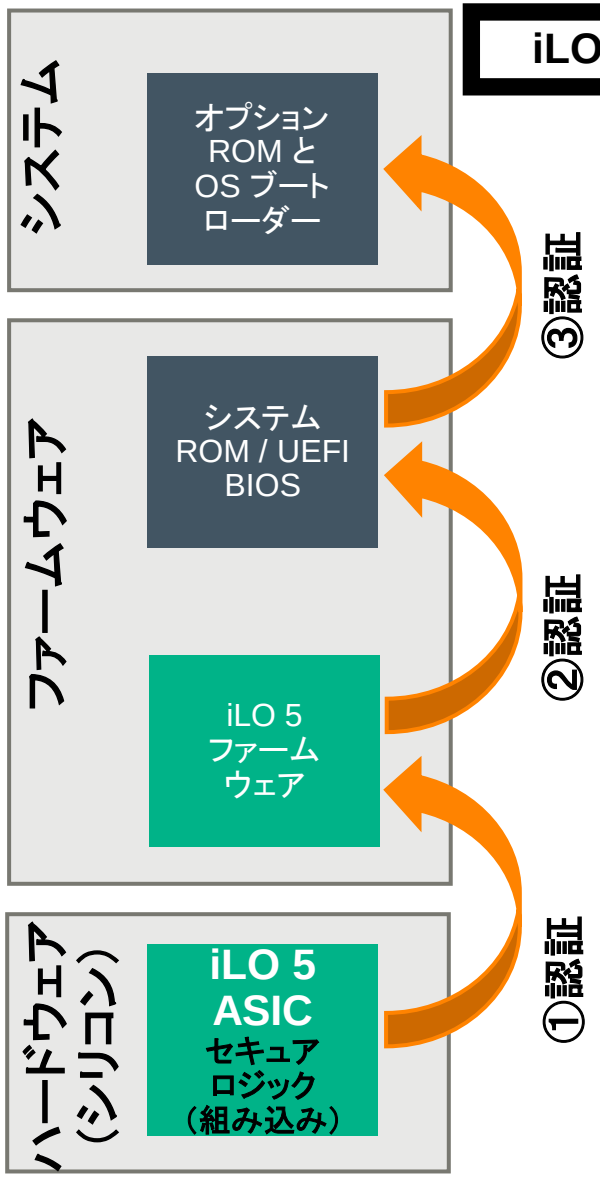
- HPE自身が設計した自社シリコンのiLOチップ内のロジックがiLOファームウェアを証明する
- ロジックはiLOチップ自身に組み込まれており、不変である

②次にiLOファームウェアがシステムROMを認証する

- デジタル証明書が適合しなければならない。改ざんがあった場合、システムROMは起動しない
- まずiLOファームウェアが信頼され、次にシステムROMが信頼される（信頼のチェーン）

③次にUEFIセキュアブートにより、オプションROMとOSブートローダーを認証する

- オプションROMとOSブートローダーは証明されなければ起動しない



Detect

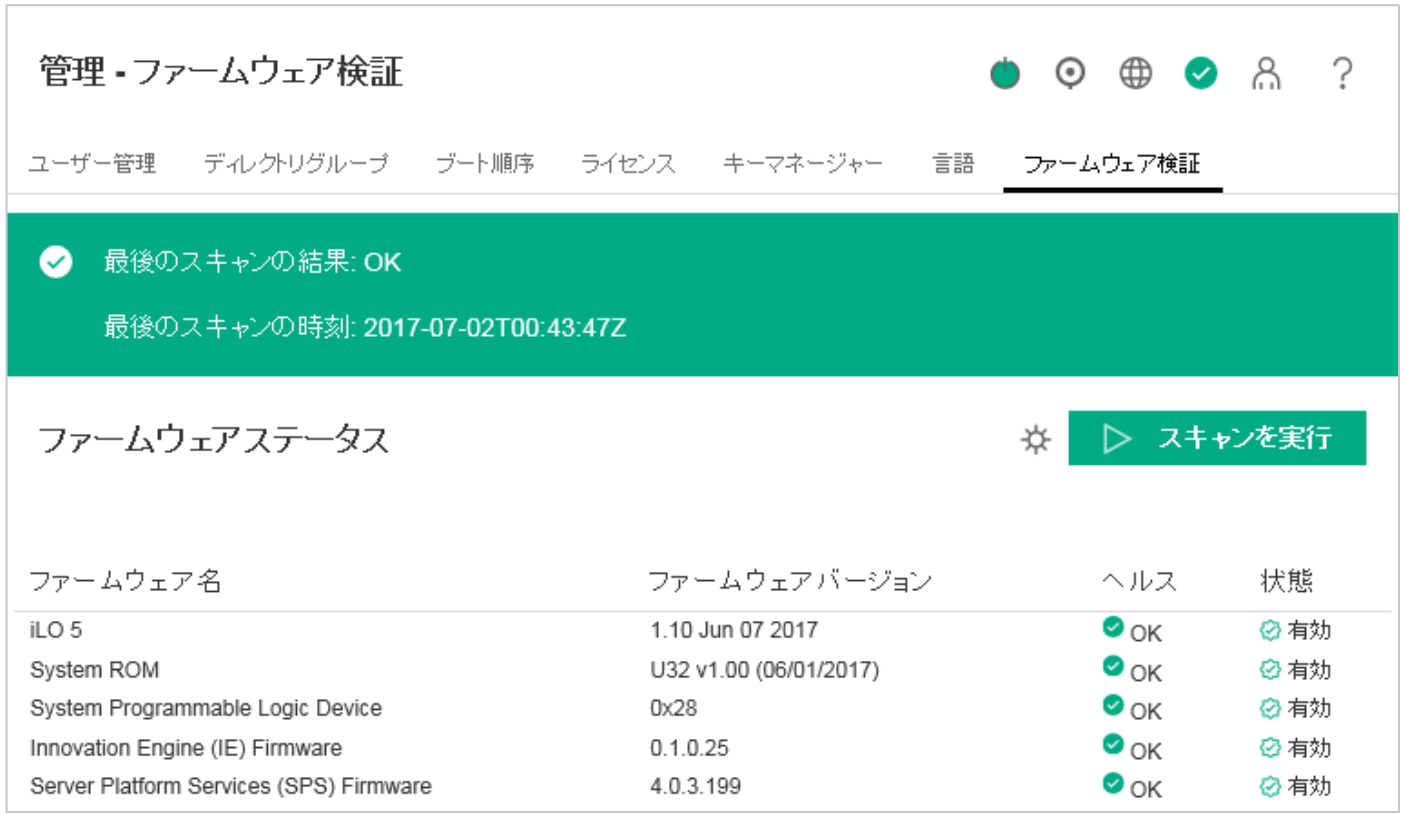
iLO Advanced

オンラインでのファームウェアの検証

オンラインでのファームウェアの検証と復元

- **サーバー稼働中にファームウェアの改ざんを検証**
  - *iLOによってバックグラウンドで実行*
  - *即時に実行することが可能*
  - *定期的に実行するように設定可能*

- 事前に設定された
  正常なファームウェアに復元
  - 工場出荷時、もしくは、
    健全性が証明された最新の設定に復旧
  - 自動復元と手動復元を選択可能
  - iLO, System ROM, CPLD, IE, ME



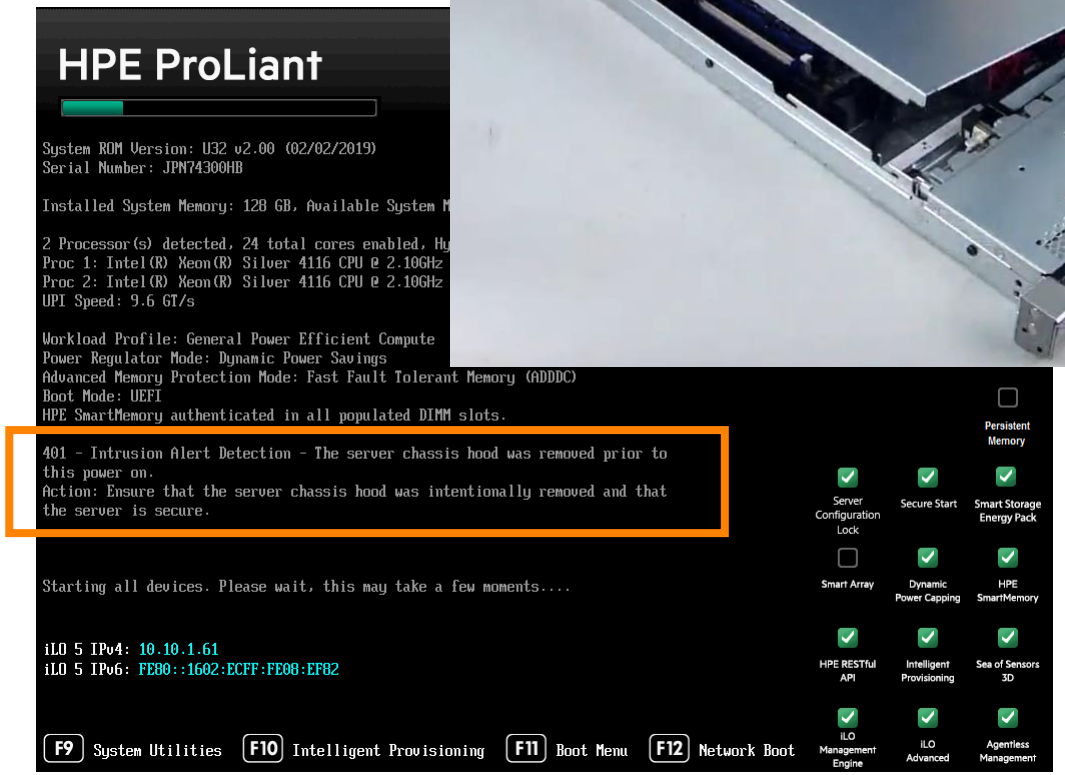
Detect

iLO Standard

サーバー侵入検知センサーオプション

サプライチェーンリスクから大切なサーバーを守る

- サーバーの上蓋を開閉したことを検知する侵入検知センサーオプションを提供※
  - 例えば、工場出荷から納品までの間に、サーバー内部に誰かが何かを仕込まないとも限らない・・・
- iLO 5ファームウェアがセンサーをモニターしてサーバーの上蓋の開閉を検知し記録
- 電源ケーブルが抜かれた状態でも上蓋の開閉を検知可能
  - 電源ケーブルが挿された後にiLOのログに記録

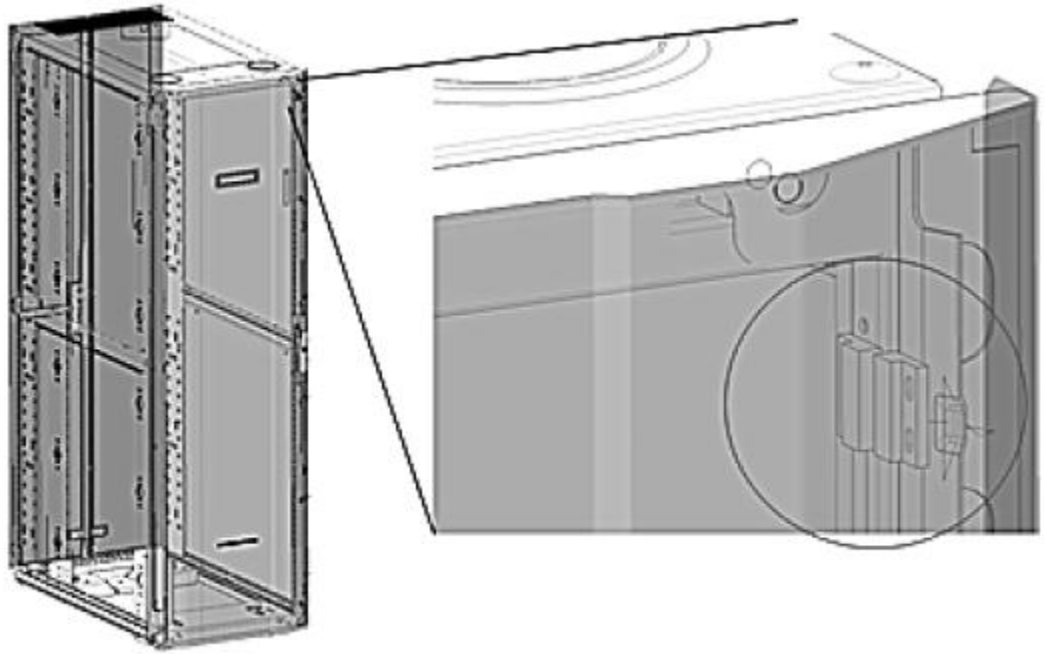


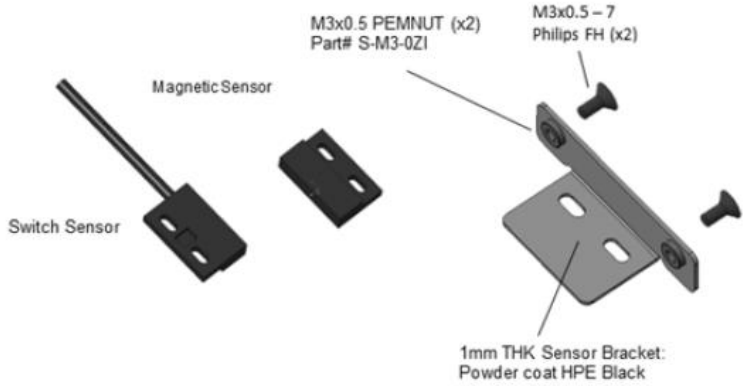
※一部機種を除く

ラックドア開閉センサー

ラックのドアが開閉されたことを検知するPDUのオプション

- センサーが取り付けられているドアが10mmより大きく開かれるとアラームまたは通知を送信
- ドアに取り付ける2つの器具（前面ドア用と背面ドア用）が付属
- スイッチセンサーと磁石センサーの組み合わせでドアの開閉を検知





Recover

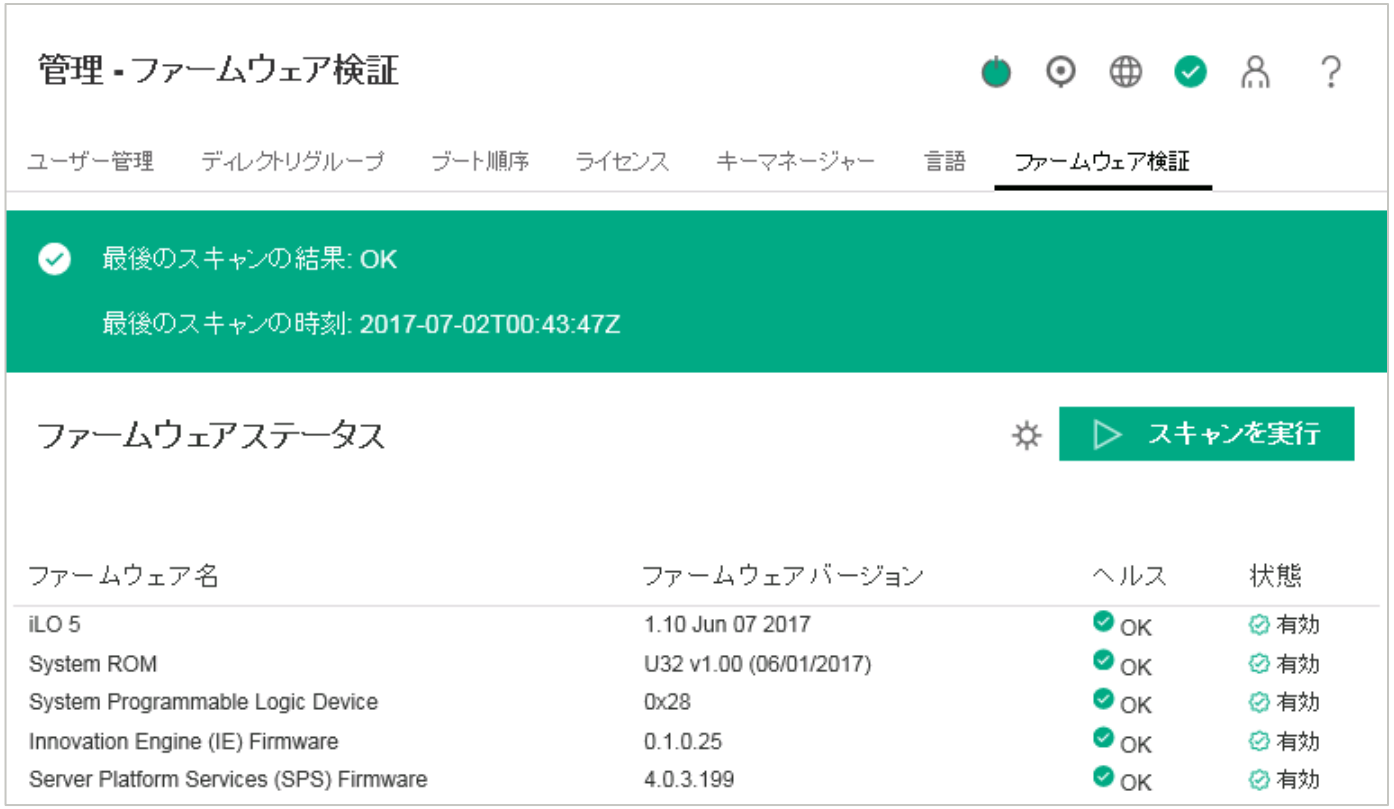
Recover

iLO Advanced

セキュアリカバリー
オンラインでのファームウェアの検証と復元

- サーバー稼働中にファームウェアの改ざんを検証
  - iLOによってバックグラウンドで実行
  - 即時に実行することが可能
  - 定期的に実行するように設定可能

- **事前に設定された正常なファームウェアに復元**
  - *工場出荷時、もしくは、健全性が証明された最新の設定に復旧*
  - *自動復元と手動復元を選択可能*
  - *iLO, System ROM, CPLD, IE, ME*

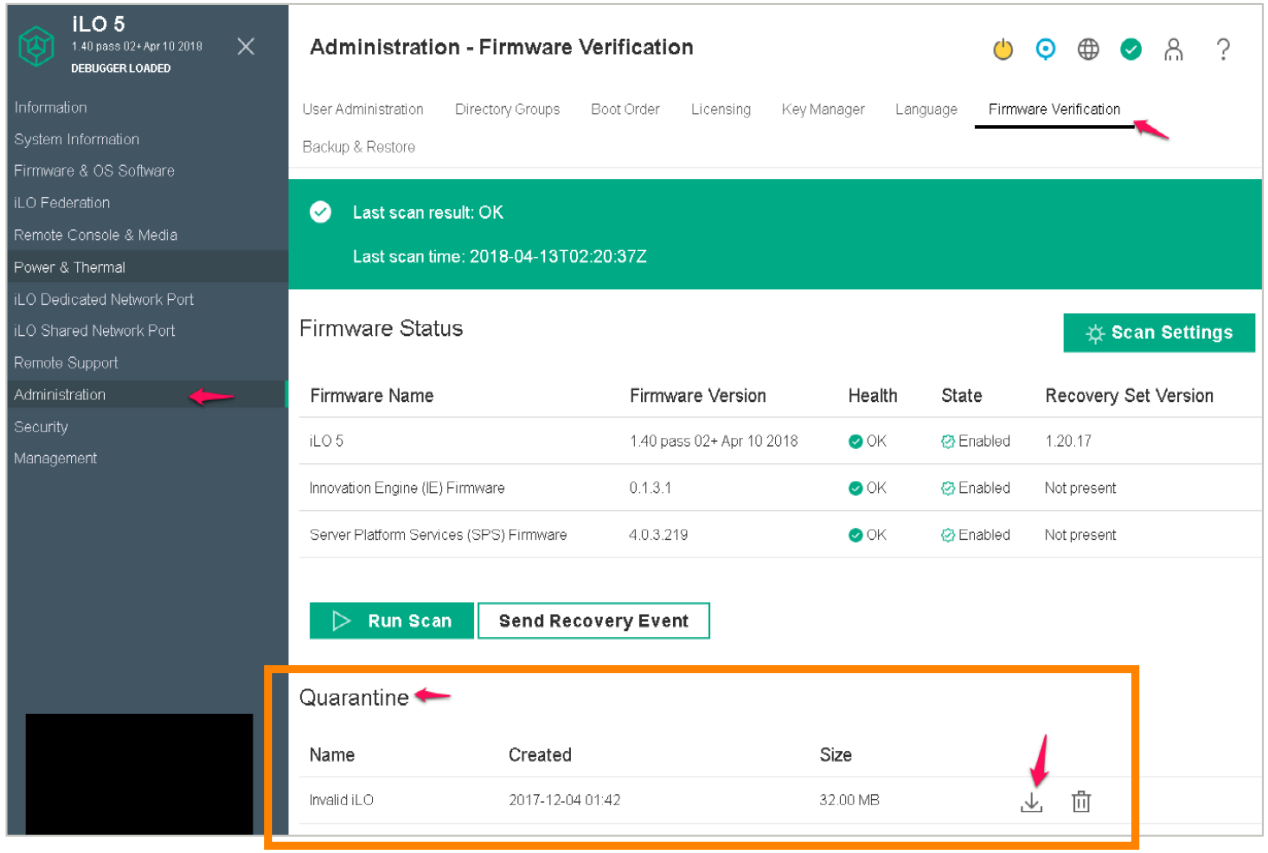


Recover

iLO Advanced

改ざんされたファームウェアの隔離
フォレンジック調査の手段を提供

- 起動時やオンラインでのファームウェア検証時に検知した改ざんされたファームウェアを、後日ダウンロードして分析するために隔離しておくことが可能



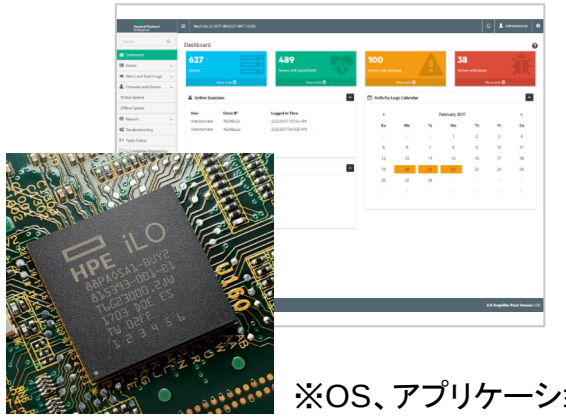
Recover

iLO Advanced

サーバーシステムリストア

ファームウェアの復元からOS・アプリケーションのリストアまでを自動化

- iLO 5とiLO Amplifier Packが連携してサーバーシステムのリストアを自動化
- 以下のベースラインを事前に指定
  - ファームウェア
  - 構成
  - OS
- ファームウェアの破損をトリガーとして、指定したポリシーに従ってシステムを自動または手動で復元



OS アプリケーション	OS、アプリケーション、データのリストアを実行するためのISOイメージ※から起動
システム構成	iLO Amplifier Packに格納された情報を利用して、BIOS、iLO、Smartアレイの構成を復元
ファームウェア	指定されたSPPを利用して、ファームウェアを復元

※OS、アプリケーション、データをリストアする環境およびISOイメージは別途ご用意ください。

Gen10 Plusでの強化ポイント

Gen10 PlusもGen10同様にセキュリティにフォーカス

Gen10発表時から提供

Silicon Root of Trust

ファームウェアの改ざん検知

セキュアリカバリー

セキュリティロックダウン（CNSAなど）

Gen10発表後に強化

セキュリティダッシュボード

サーバー構成ロック

One-buttonセキュア消去

Marsh Cyber Catalystに選出

Gen10 Plusで更に強化

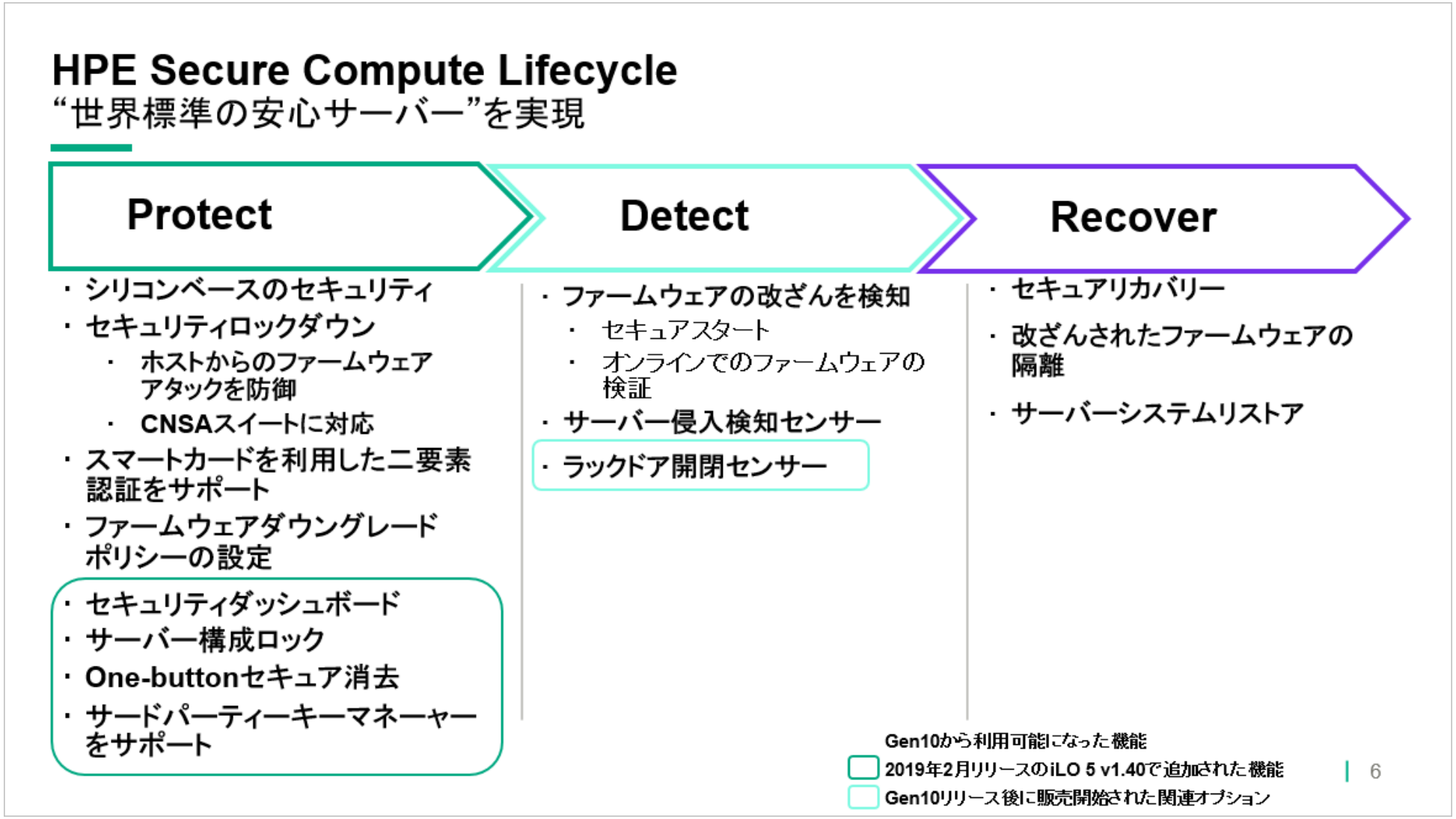
TPMを標準搭載

SEDを提供開始

セキュア ゼロタッチオンボーディング

デバイス証明（プラットフォーム証明書）

Gen10/iLO 5で様々なセキュリティに関する機能を実装



Cyber Catalyst Designated Solutions 2019 / 2020

Marsh により運営される、
”Cyber Catalyst Designations”プログラム

8つの保険業者が、6つの観点（サイバーリスク低減・パフォーマンス・脆弱性・有効性・柔軟性・差別化）からソリューションを評価し、最低6業者の得票をもって選出される。Microsoftが技術アドバイザを行うが、Marsh/Microsoftは投票に関与しない

2019年のプログラムでは、HPEから

- Aruba Policy Enforcement Firewall
- HPE Silicon Root of Trust

2020年のプログラムでは、新たにHPEから

- Aruba ClearPass
- が選出（追加）された

出典: https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/cyber-catalyst-designations-brochure.pdf

Gen10 Plusから追加で実現する、セキュリティに関する機能

- TPM（Trusted Platform Module）を標準搭載
  - セキュリティ強化策の一環
  - Windows Server 2022からTPMが標準に

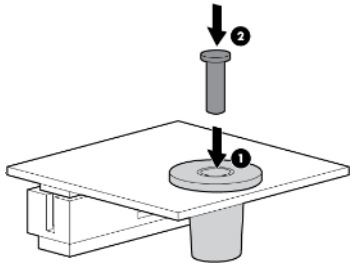
- SED（Self-encrypting Drives）の提供を開始
  - HCIなどRAIDを使わない構成でのデータ暗号化のニーズに対応
  - コントローラーベースのSmart Array Secure Encryptionも引き続き提供

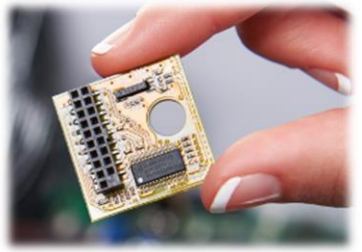
- **セキュア ゼロタッチオンボーディング**
  - お客様環境にサーバーを安全に自動導入・展開

- **デバイス証明（プラットフォーム証明書）**
  - サプライチェーンリスク対策を更に強化

TPM（Trusted Platform Module）を標準搭載

Windows Server 2022の「Secured-Core Server」利用時には必須





Secured-Core Server の要件

- **TPM 2.0**
- DRTM（Dynamic Root of Trust of Measurement）認定CPU搭載サーバー

Secured-Core Server とは？

- H/W、F/W、OS機能を組み合わせて実現する一連のセキュリティ保護機能
- TPMを活用したハードウェアのRoot-of-Trust担保
- Windows Defender System Guard機能によるファームウェア攻撃への対策
- VBS（Virtualization-based security）、HVCI（Hypervisor-Based Code Integrity）やCredential Guardといった仮想化ベースのセキュリティ機能による脆弱性対策、認証情報保護

設定方法はこちら

- https://www.hpe.com/psnow/doc/a50003760enw

対象製品

- **AMD EPYC 7xx3 CPU (Milan)**
  - HPE ProLiant DL325 Gen10 Plus v2 server
  - HPE ProLiant DL345 Gen10 Plus server
  - HPE ProLiant DL365 Gen10 Plus server
  - HPE ProLiant DL385 Gen10 Plus v2 server
  - HPE Apollo 2000 Gen10 Plus System (XL225n)
  - HPE Apollo 6500 Gen10 Plus System (XL675d, XL645d)
- **Intel Intel® Xeon® 3rd Gen CPU (Ice Lake)**
  - HPE ProLiant DL360 Gen10 Plus
  - HPE ProLiant DL380 Gen10 Plus
  - HPE Synergy 480 Gen10 Plus
  - HPE Apollo 2000 Gen10 Plus System (XL220n, XL290n)
  - HPE Apollo 4200 Gen10 Plus System (XL420)

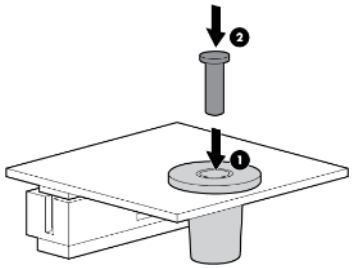
TPM（Trusted Platform Module）を標準搭載

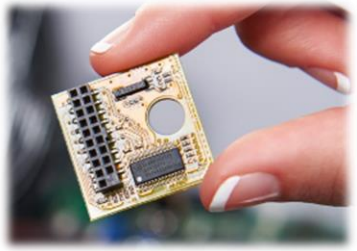
Windows Server 2022の「Secured-Core Server」利用時には必須に

「TPM 2.0」対応チップが必要

Secured-Core Serverに付随する機能を使用する場合は
必須となります

- TPMがなくてもWindows Server 2022を利用することは可能です
  - 既存Gen10 サーバー（WS2019、TPMなし）のアップグレードも可能です
  - 新規でAMD Milan/Intel Ice Lake 搭載モデルにてWS2022を導入される場合は、TPMと一緒にご提案することを強くお勧めします
    - 構成から意図的に外さない限りは自動的に見積もりに入るようになっています
- TPM モジュールは一度装填すると、ユーザー自身で
  取り外したり交換することはできませんのでご注意ください





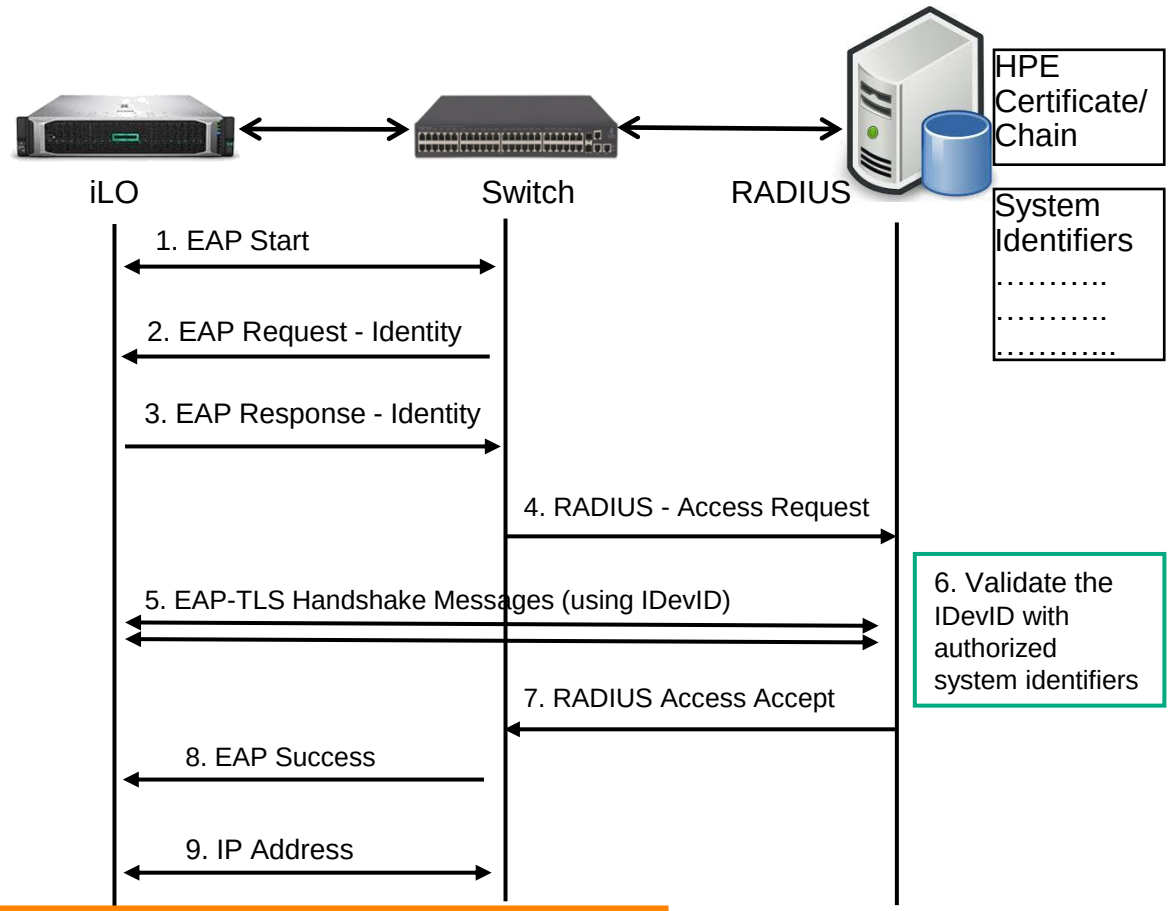
セキュア ゼロタッチオンボーディング

これまでの課題

- 顧客環境に安全にサーバーを導入するには人間の介在が必要で、自動化が難しい
- リモートオフィスやエッジロケーションは安全でなく、サーバーを導入できる技術者もいない場合が多い

Gen10 Plusによる解決策

- 802.1AR(Secure Device Identity)を利用
  - HPE工場でIDevIDをサーバーに格納
  - 顧客ネットワークに接続する前に、ローカルスイッチ/ルーターおよびAAAサーバーを介して、HPEサーバーを「認証」および「承認」することが可能に
- 802.1X EAP-TLSプロトコルをサポート
  - 「ゼロタッチ」(人間の介在なし)で、IDevIDを利用した顧客ネットワークへの安全な接続の確立を可能に



※802.1X対応ネットワーク機器やAAAサーバーはお客様側でご用意いただく想定となります

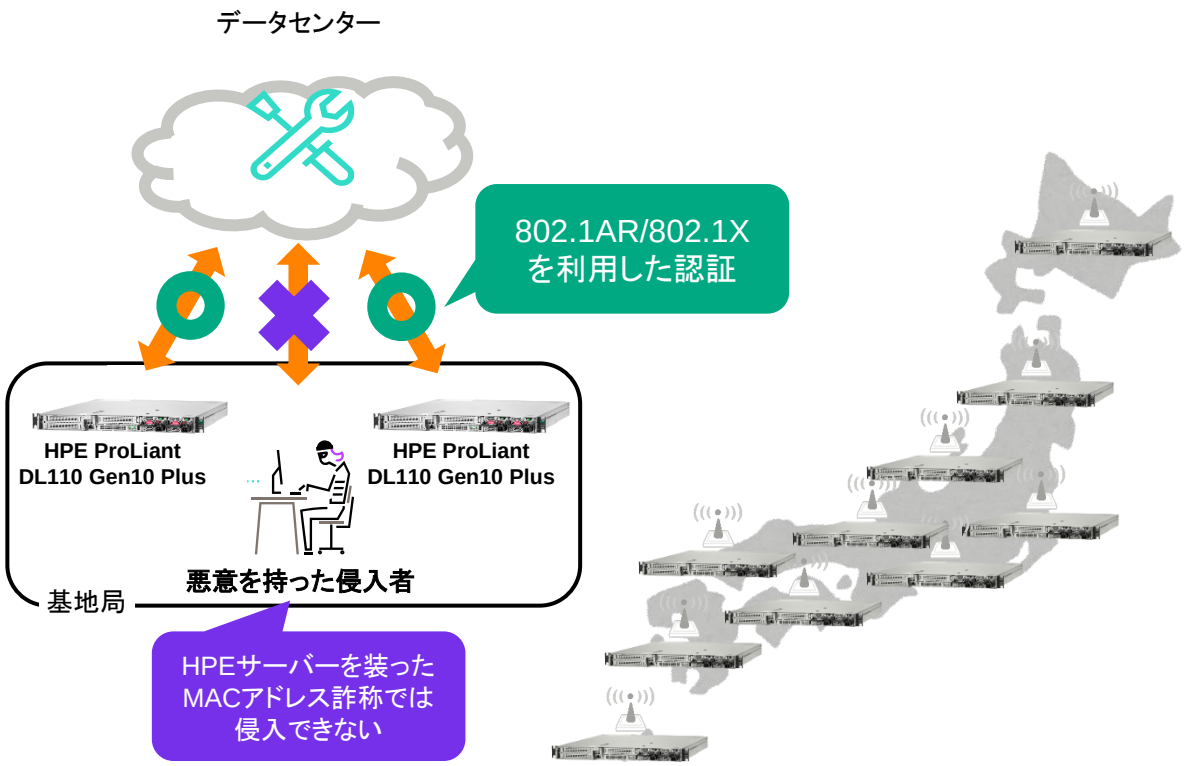
従来型のMACアドレス認証は簡単に詐称されてしまう
よりセキュアな認証方法が求められている

ゼロトラスト対応

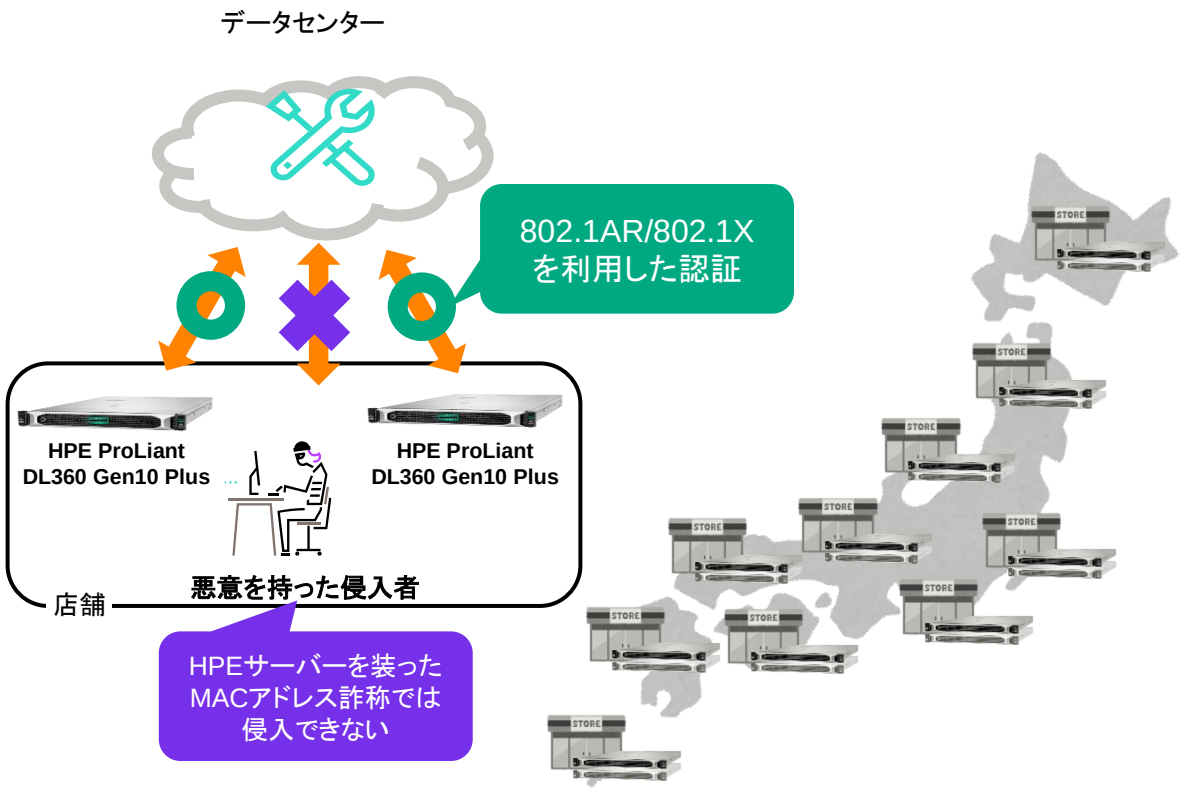
セキュア ゼロタッチオンボーディング

活用例:「正規品」であることを認証してから接続を許可する

5G vRAN(仮想無線アクセスネットワーク)

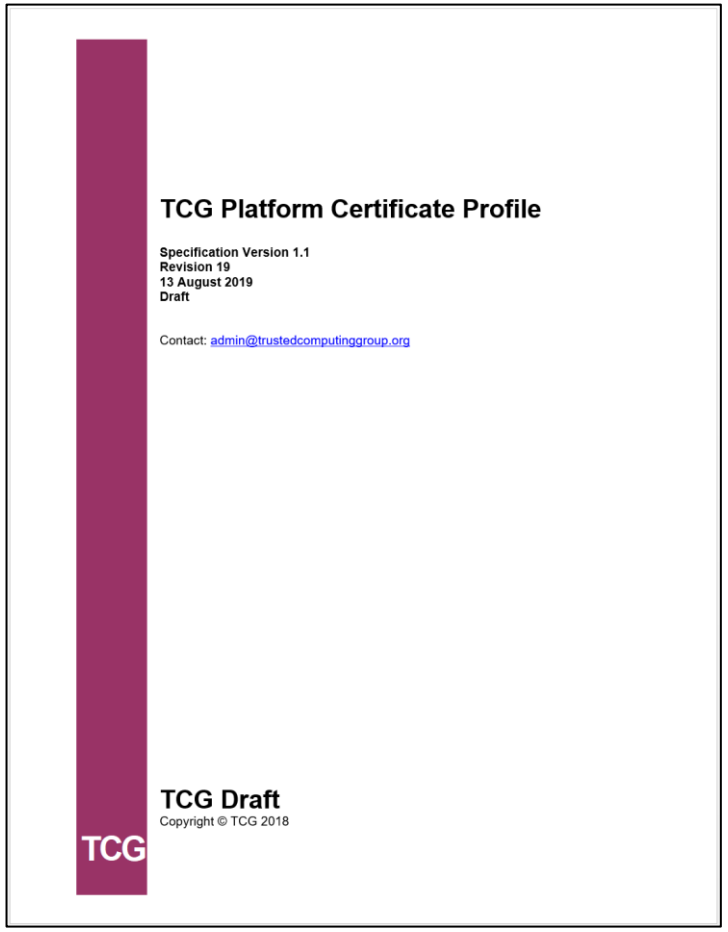


店舗サーバーやIoT用サーバー



- ✓ 不特定多数の人が立ち入りうる場所に設置される可能性が高い
- ✓ 全設置箇所にセキュリティに詳しい技術者を配置するのは非現実的

デバイス証明（プラットフォーム証明書）



https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/

- X.509属性証明書（Attribute Certificate）を利用して、サーバーが製造時から改ざんされていないことを検証する仕組み
- このプラットフォーム証明書には、マザーボード、コンポーネント、ファームウェアに関する情報が含まれており、変更を検知可能

HPE工場

HPE工場でプラットフォーム証明書が作成・電子署名され、サーバー内に保存される

お客様サイト

お客様はHPE提供のツール※を使用してサーバーに変更・改ざんがないことを検証できる

Trusted Computing GroupのPlatform Certificate Profileに準拠

※GitHubでも公開済み
https://github.com/HewlettPackard/PCVT

デバイス証明（プラットフォーム証明書）

活用例: 輸送中の物理的な攻撃からサーバーを守る

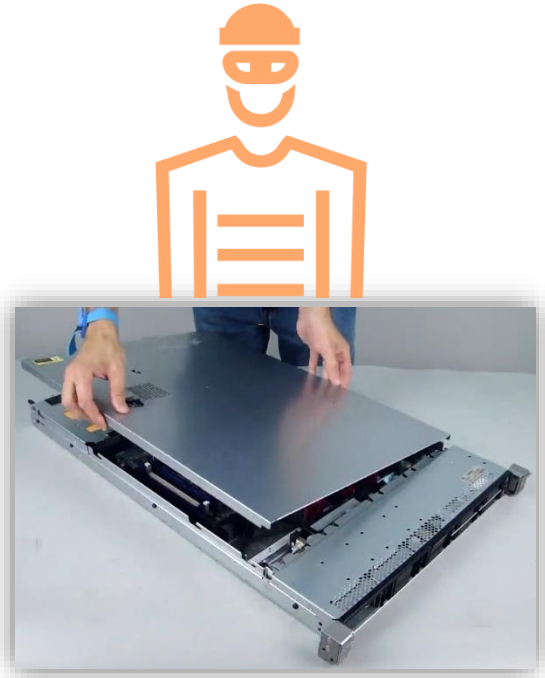
HPE工場

輸送中の変化を検知するために
「プラットフォーム証明書」
を作成してサーバー内に格納

プラットフォーム
証明書格納済み

輸送中

悪そうな人が何かしてる！

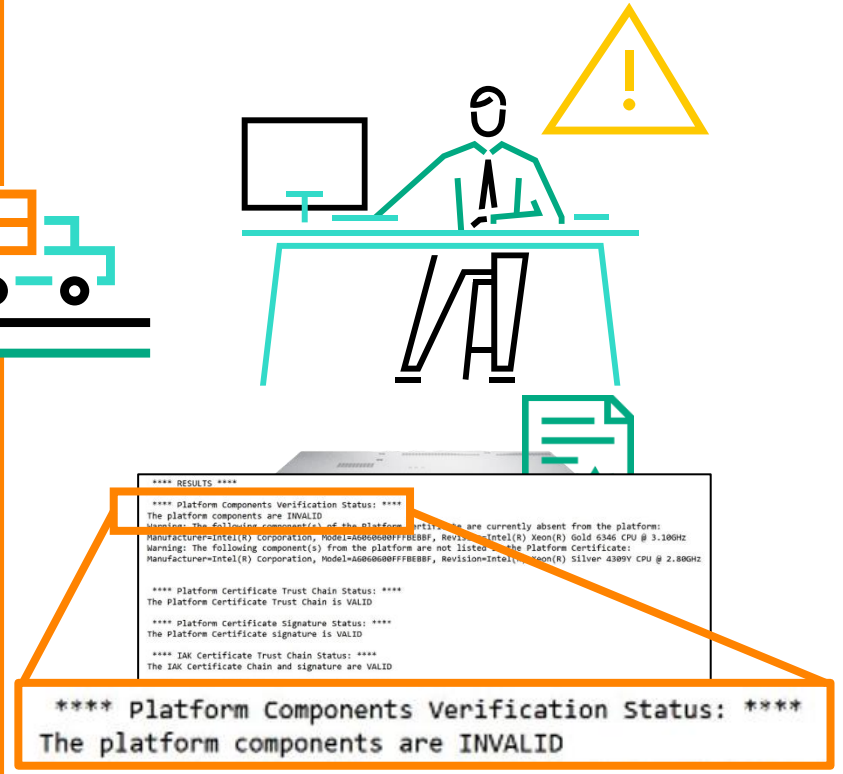


マルウェアを仕込んだ
SSDカードに交換

リスク

お客様先

検証ツールを実行したら
メッセージが！



証明書と実物の
不整合を検知

AMD セキュア プロセッサ（ASP）

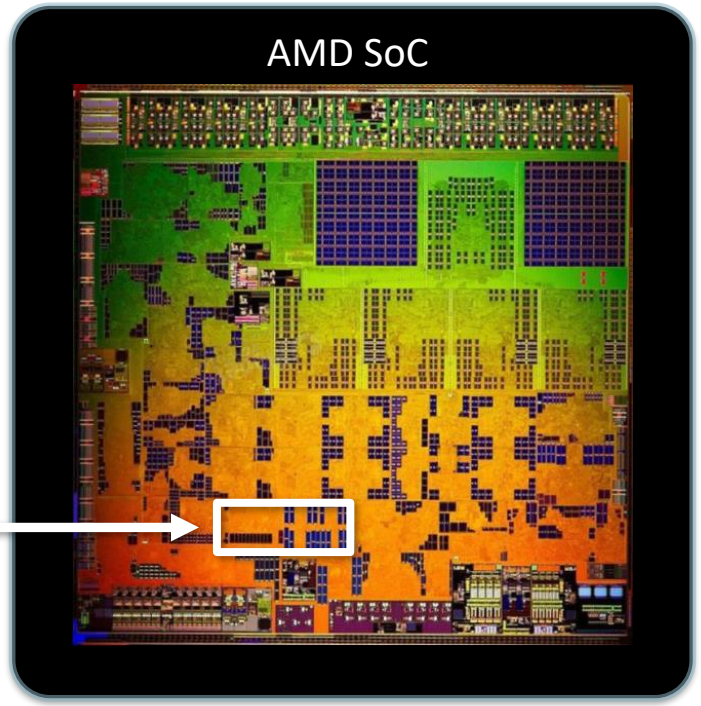
X86 とは別の 独立したプロセッサ

- AMD セキュア プロセッサが内蔵
  - 32-bit マイクロコンピュータ (ARM Cortex-A5)
- セキュア OS/kernel の起動
- ファームウェア、データ用にセキュアオフチップ不揮発ストレージ (例 SPI ROM)
- セキュアキーの生成、管理用の暗号化機能の提供
- セキュア ブート のサポート

AMD EPYC搭載システムをセキュアに利用するための各種機能を提供する専用ハードウェアを内蔵

Root of Trust

AMD Secure Processor

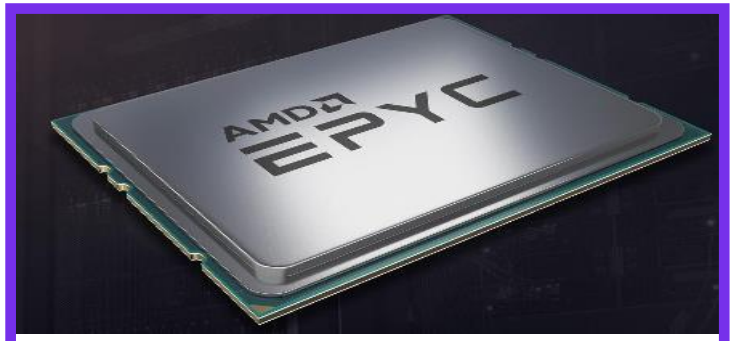


ハードウェアによるルート・オブ・トラストにより
プラットフォームのセキュリティ基盤を提供します

HPE Silicon Root of Trust と AMD Secure Processor が連携

HPE

＋



AMD

HPE Only!

システム
- オプションROMとOS ブートローダー

ファームウェア
- システムROM / UEFI BIOS
- iLO 5 ファームウェア

ハードウェア(シリコン)
- iLO 5 ASIC

認証 / 認証 / 認証 / 認証 / 認証

シリコンベースのセキュリティ

HPE Silicon Root of Trustの検証プロセスの中にAMD Secure Processorが組み込まれ、相互に検証し合う

Secure Memory Encryption (SME)

Secure Encrypted Virtualization (SEV)

AMD Secure Processor
iLOファームウエアがASPの正常性を検証
ASPがシステムROMの正常性を検証

HPE ProLiant DL385 Gen10 / DL325 Gen10 は以下脆弱性の影響を受けない
Meltdown Variant 3, Rogue Data Cache
Foreshadow-NG (OS Kernal/SMM Attack)
Foreshadow-NG (VMM Attack)
Foreshadow- (SGX Attack)
Zombie Load
Spoiler
Fallout
Ram Bleed
SWAPGS

セキュア ゼロタッチオンボーディング
製品型番対応表

2021年12月現在

製品型番	製品名	サポート機種	対応工場	
			日本	シンガポール
P41905-B21	Server Identity FIO Setting	DL110 Gen10 Plus DL360 Gen10 Plus DL380 Gen10 Plus Edgeline e920/e920d/e920t Server Blade	○	○
P49814-B21	Server Identity LDevID FIO Setting	DL325 Gen10 Plus DL325 Gen10 Plus v2 DL345 Gen10 Plus DL360 Gen10 DL365 Gen10 Plus DL380 Gen10 DL385 Gen10 Plus DL385 Gen10 Plus v2	×※	○

※日本でも販売は可能です。

デバイス証明（プラットフォーム証明書）+セキュア ゼロタッチオンボーディング
製品型番対応表

2021年12月現在

製品型番	製品名	サポート機種	対応工場	
			日本	シンガポール
P42104-B21	Server Platform Certificate iLO FIO Setting	DL110 Gen10 Plus DL360 Gen10 Plus DL380 Gen10 Plus Edgeline e920/e920d/e920t Server Blade	○	○
P49803-B21	Server Platform LDevID FIO Setting	DL325 Gen10 Plus DL325 Gen10 Plus v2 DL345 Gen10 Plus DL360 Gen10 DL365 Gen10 Plus DL380 Gen10 DL385 Gen10 Plus DL385 Gen10 Plus v2	×※	○

※日本でも販売は可能です。

セキュリティ機能他社比較

Gen10 Plusで更に強化された、差別化に使える機能

Cyber Catalystソリューション認定機能
iLO Advancedライセンスが必要
工場での組み込みが必要

	HPE Gen10/Gen10 Plus/ Gen10 Plus v2 サーバー※	Dell	富士通
起動時のファームウェア正常性検証	○ Silicon Root of Trust	△（Intel Boot Guard）	△（Secure Boot）
OS起動後のファームウェア正常性検証	○ ファームウェア検証スキャン	×	×
ファームウェア改ざん検知時の自動復旧	○ セキュアリカバリー	×（BIOS手動復旧可能）	×
改ざんされたファームウェアの隔離	○ ファームウェア検証・ファームウェアの隔離	×	×
管理プロセッサーのFIPSモード	○ iLOセキュリティ設定（FIPS 140-2 完全準拠）	△（暗号化ライブラリのみ準拠）	×
管理プロセッサーのCNSAモード	○ iLOセキュリティ設定・CNSAスイート	×	×
構成ロック	○サーバー構成ロック検知（ハードウェア構成変更、FW変更）	変更不可（BIOSパラメータ、FW）	×
サーバー侵入検知センサー	○ サーバー侵入検知センサー（オプション）	○	×
安全なシステム初期化	○ One-buttonセキュア消去（RBSU、iLO、ディスク）	△（ディスク消去のみ）	△（SVS SDカード消去）
サーバーのセキュリティ設定状態の提示	○ セキュリティダッシュボード	×	×
802.1AR/802.1Xを利用した機器認証	○ IDevID/LDevID	×	×
証明書を利用したデバイス証明	○ プラットフォーム証明書(TCG準拠)	○ 独自実装	×

※機種によって非対応の機能もありますので、提案前にご確認をお願いします

Thank you