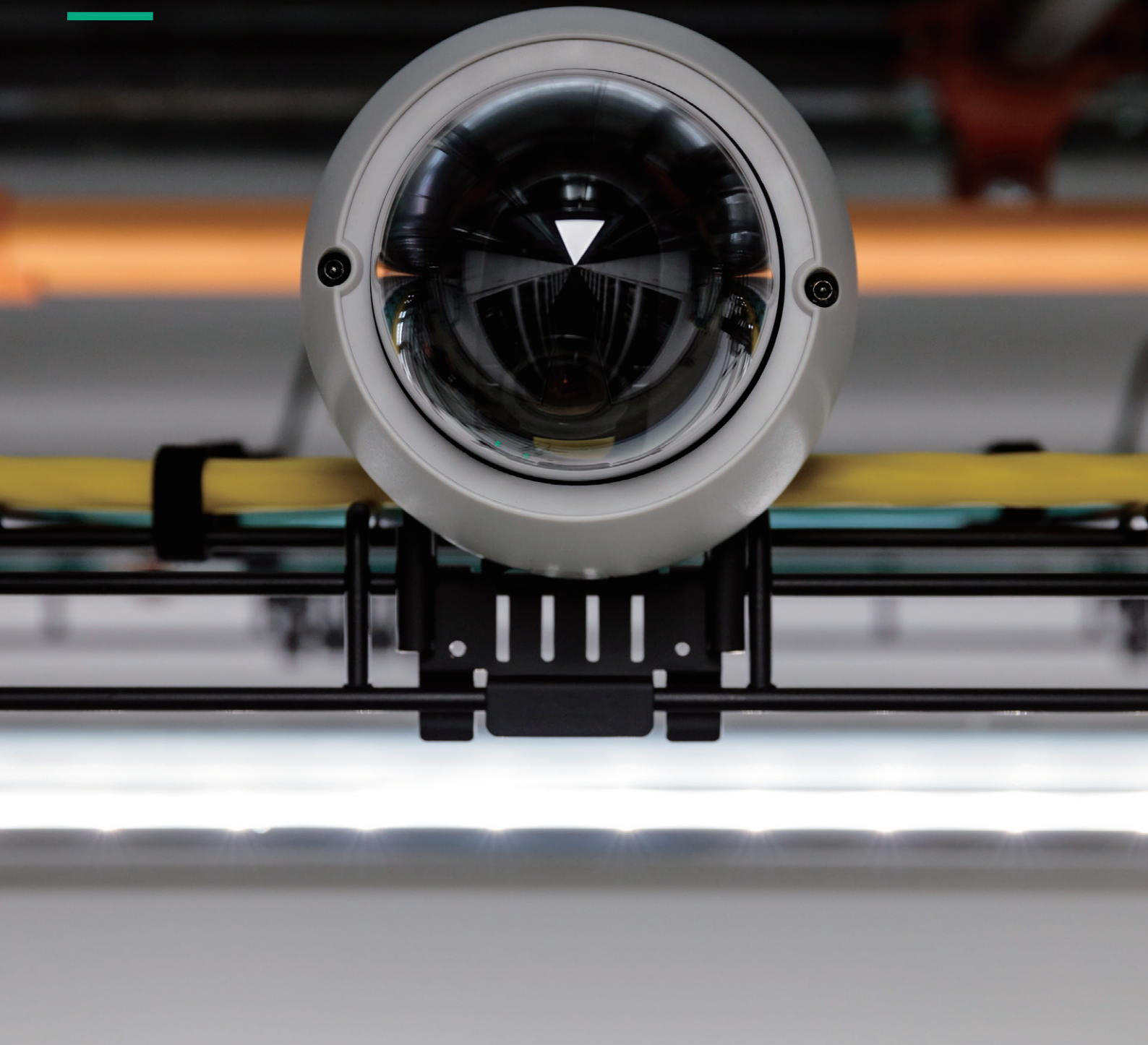
Hewlett Packard Enterprise | Microsoft

Brochure

サイバー攻撃のリスクを低減する“4つの視点”

HPE サーバー セキュリティハンドブック



サイバー攻撃の増大とともに深刻化するセキュリティリスク、ビジネスを守るために必要な行動とは

2022年6月、政府は『重要インフラのサイバーセキュリティに係る行動計画[*1]』を改訂し、情報通信、電力、金融など重要インフラ事業者の「経営者の責任」を明確化しました。その背景には、高度化・巧妙化するサイバー攻撃によるセキュリティ脅威が高まる中、重要インフラ防護の具体策が進まない現状に対する危機意識があります。

サイバー犯罪は年率15%増加

2021年のランサムウェアによる経済的損失は200億ドルを超えました。今後5年間でサイバー犯罪は年率15%で増加し、被害額は2025年には年10.5兆ドル規模になると予想されるなど、問題はいっそう深刻さを増しています。[*2]

サプライチェーンリスクの拡大

2022年3月に国内大手製造業のラインが停止した事件は、「サプライチェーン攻撃」の脅威を知らしめました。IPAが公開した「情報セキュリティ10大脅威 2022[*3]」でも、サプライチェーンリスクは3位に位置づけられています。

顕在化するファームウェアへの攻撃

ブートキットとしてシステム内に潜み、OSが起動する前に動作してUEFIファームウェアを書き換えるマルウェアの発見が相次いでいます。ウイルス対策ソフトでは検知できない「ファームウェア攻撃」への対応が急がれています。

*1: 内閣サイバーセキュリティセンター(NISC)- 2022年6月「重要インフラのサイバーセキュリティに係る行動計画」https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf
*2:Cybersecurity Ventures, Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021
*3:独立行政法人 情報処理推進機構(IPA)- 2022年3月「情報セキュリティ10大脅威 2022」https://www.ipa.go.jp/security/vuln/10threats2022.html

政府は、重要インフラ事業者の「経営者の責任」を明確化

政府・内閣サイバーセキュリティセンターが示した『重要インフラのサイバーセキュリティに係る行動計画』で注目すべきポイントは、「経営陣を含め組織一丸となったサイバーセキュリティへの対応」と「サプライチェーンリスクに対する具体策」を求めていることです。行動計画では、14分野(情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油)が重要インフラ事業者に指定されていますが、今後すべての企業が考慮すべきガイドとなるはずです。

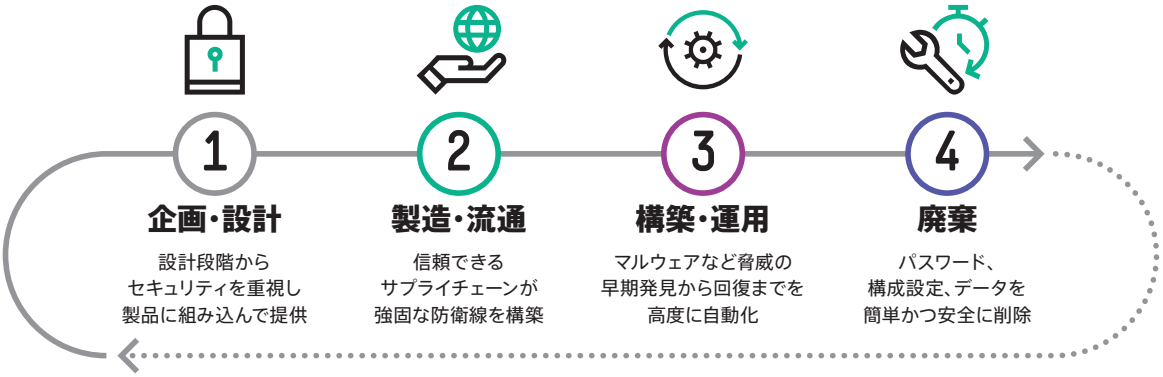
Windows Server 2012/2012 R2
2023年10月 延長サポート 終了

2023年に迫る「Windows Server 2012/2012 R2のサポート終了」

Windows Server 2012/2012 R2 は2023年10月に延長サポートが終了します。新規のセキュリティパッチの提供が行われなくなると、新たな脆弱性が見つかった場合にこれを狙ったサイバー攻撃を防ぐことが困難になります。2023年10月までに最新OSへの移行を完了できるよう、計画を急がなければなりません。

システムのライフサイクル全体を見通し“4つの視点”から、セキュリティを考える

システムのセキュリティ水準を向上させ、ビジネス・企業活動をしっかりと防護するためには、サイバー攻撃のリスクを正しく認識し、システムの企画・設計、機器の調達段階からセキュリティ要件を適切に組み込むことが不可欠です。システムのライフサイクル全体を捉えた「セキュリティ・バイ・デザイン」は、重要インフラを担う事業者に限らず、すべての企業が考慮すべき指針です。



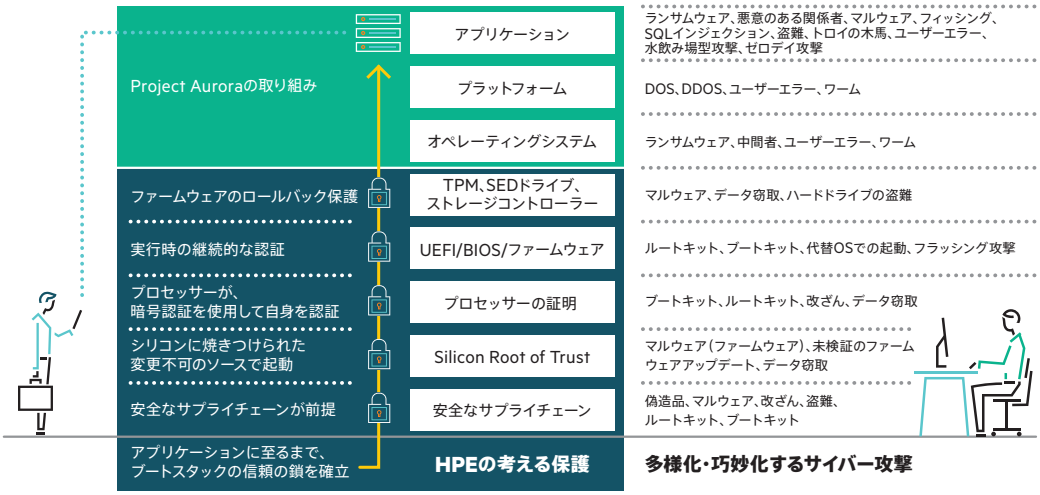
HPEは、サーバー/プラットフォーム製品に「セキュリティ・バイ・デザイン」を採用

インフラストラクチャに「セキュリティ・バイ・デザイン」を適用

グローバル企業として米国をはじめ世界各国の重要インフラに深く携わっているHPEは、「セキュリティ・バイ・デザイン」の考え方を、2017年からサーバーをはじめとするインフラストラクチャに適用してきました。①企画・設計、②製造・流通（サプライチェーン）、③構築・運用、④廃棄に至る4つのステージを一貫して捉え、最先端のセキュリティ技術を組み込んでいます。そして、「システム全体のセキュリティ強度は、根幹にあるハードウェアの強度に依存する」「システム全体を守るには、根幹にあるハードウェアを守らなければならない」という視点に立ち、インフラストラクチャのセキュリティ強化を着実に進めています。

HPEのセキュリティビジョンを「Project Aurora」で具現化

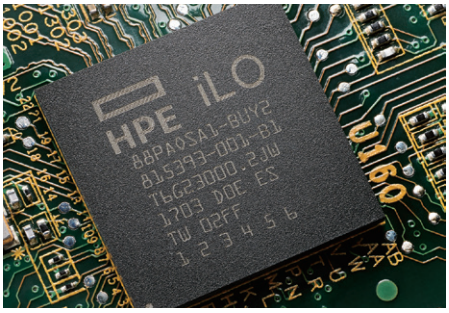
さらにHPEでは、セキュリティが確保された「真のRoot of Trust」を、基礎となるインフラストラクチャおよびサプライチェーンのレイヤーから、その上位にあたるオペレーティングシステム、ソフトウェアプラットフォーム、アプリケーションまで拡大する取り組みを進めています。このHPEの新しいチャレンジ『Project Aurora』では、すべてのレイヤーを自動的かつ一貫して保護するための「組み込み型のセキュリティプラットフォーム」の実現を目指しています。



1

HPEサーバー独自の設計思想
業界随一のSilicon Root of Trust

HPEサーバーが他のx86サーバーと決定的に違う理由――それは、HPE独自開発のシリコンチップ「HPE Integrated Lights-Out 5（iLO 5）」を搭載していることにあります。HPEサーバーの設計思想の象徴ともいえる「iLO 5」は、Silicon Root of Trust（シリコンレベルの信頼性）の起点であり、セキュリティ・バイ・デザインを具現化する中核デバイスです。



HPE Integrated Lights-Out 5（iLO 5）

iLO 5は、サーバーの安全な輸送から、セキュアなサーバー起動、セキュアな構築・運用、問題検知と自動復旧、安全な廃棄までを根底から支える最重要のデバイスです。同時に、サーバーのライフサイクル全体を網羅する先進的な管理機能も提供します。

書き換え不可能なシリコンチップ（ASIC）であることに、iLO 5の圧倒的な優位性があります。HPEサーバーが提供する様々な機能を論理回路としてシリコンチップに焼き込むことで、汎用チップとは比較にならない強靭な基礎を構築しています。

HPEサーバーのコアコンポーネントを自社開発

HPEでは、信頼の起点となる「iLO 5」とともに、ファームウェアやSystem ROMを自社開発しています。Silicon Root of Trustは、ファームウェアの正常性確認ロジックが焼き込まれたiLO 5を起点に、ファームウェアからSystem ROMへと認証をつなぐ「真のRoot of Trust」を実現します。

iLO 5のような管理プロセッサーは、「サーバーがどんな状態でもコントロールできる」ことが必須であるため、サーバーに電源ケーブルが接続されると（サーバー本体の電源がオフでも）即座に起動します。重要なことは、管理プロセッサーは「自分自身を守る仕組みを持つことが必須」であり、それを自社で設計・開発しているのは、数ある管理プロセッサーの中でHPEのiLO 5だけという事実です。

一般的なx86が採用しているUEFIセキュアブートは、ファームウェアが改ざんされる可能性を残しており、「真の意味でのRoot of Trustとは言えない」とHPEは考えています。万一、サイバー攻撃により書き換えられた場合、UEFIファームウェアの入れ替えを伴う中長期的なシステムダウンが発生する可能性があります。

HPEのSilicon Root of Trust

セキュアスタート

- iLO 5 ASICのハードウェアが起点
- HPEはiLO 5 ASIC、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問題を検知可能
- 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、管理プロセッサーが対象

一般的なx86サーバー

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
- Intel Boot Guard などのTPMを使用したソリューションでも、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

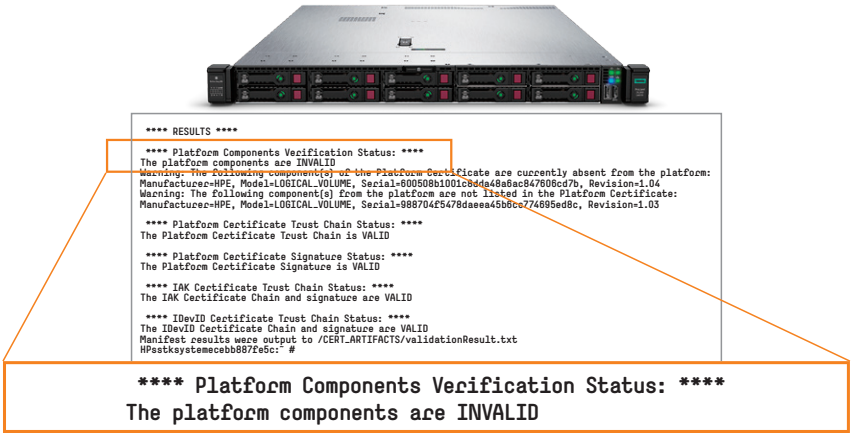
2

サプライチェーンリスクへの対応を万全にするために

情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威 2022」で3位を占めるなど、「サプライチェーンリスク」は、最も警戒すべきセキュリティ課題のひとつとなっています。HPEでは、サーバーの製造・流通工程におけるリスクを低減するために、品質管理プロセスを厳格化するとともに、出荷・輸送段階、システム設置段階での効果的なセキュリティ機能を実装しています。

サーバーの構成が「変更されていないこと」を証明

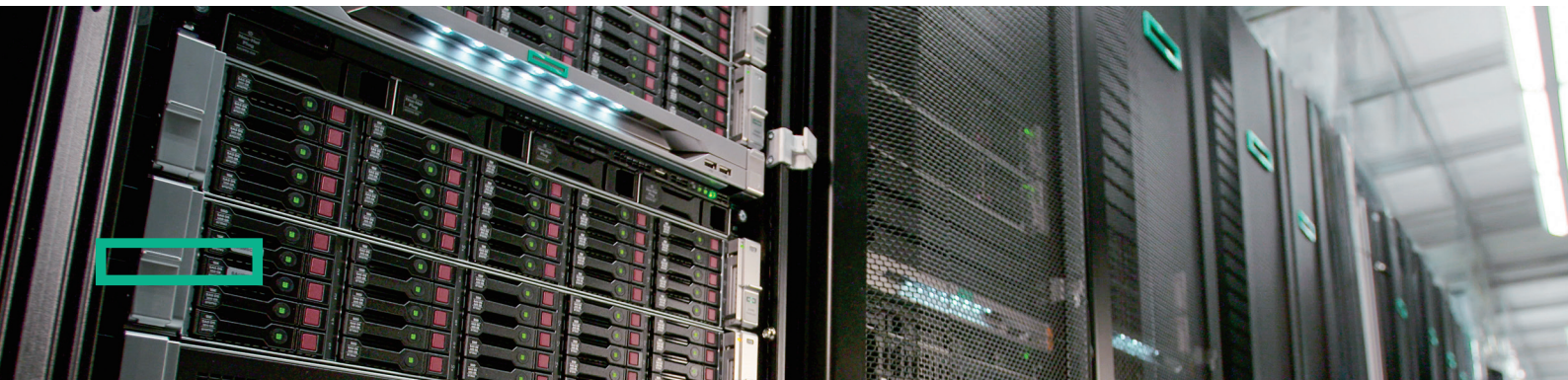
サプライチェーンリスクのひとつに「輸送中のサーバーへの物理攻撃」があります。マルウェアを仕込んだデバイスを組み込むような手口が典型的なものです。HPEサーバーでは、「プラットフォーム証明書（X.509属性証明書）」によって、サーバーの構成（システムボード、CPU、メモリ、PCIeスロット、セキュリティ構成、システムファームウェア）に変更がないかを容易に検証可能。検証ツールを起動すると、プラットフォーム証明書とサーバー実機の不整合を即座に検知します。



また、「サーバー構成ロック機能」および「筐体侵入検知オプション」により、サーバーの輸送・流通段階で本体の蓋の開閉や不正部品の混入があった場合には、ハードウェアへ第三者からの干渉があったものとしてサーバー起動時に警告メッセージを表示します。

複数の拠点へ安全にサーバーを展開

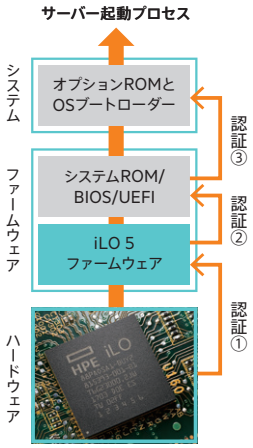
セキュア ゼロタッチオンボーディングは、HPEの工場で製造されたサーバーであることを示す「デジタル証明書（802.1AR）」を埋め込んで出荷し、これをお客様のネットワークに接続する際の「認証」に利用できるテクノロジーです。流通チェーンの店舗、生産拠点や社会インフラなどのIoTシステム、携帯通信の基地局など、多拠点にサーバーを展開する際の安全性を手軽に高めることができます。デジタル証明書ベースの認証は、詐称・書き換えのリスクがあるMACアドレス認証を代替する技術として注目されています。



3

サーバー構築と運用段階での不正の自動検知と自動復旧

MoonBounce、MosaicRegressor、LoJaxなど――UEFIファームウェアを狙う脅威が次々と明らかになっています。システム構築・運用段階では、**Protect**:サーバーの防御と安全な起動から、**Detect**:サーバー稼働中の不正検知、**Recover**:正常な状態への復旧まで、HPE独自のシリコンチップ「iLO 5」によるSilicon Root of Trustが大きな威力を発揮します。



iLO 5

セキュアスタート:HPEだけのセキュアなサーバー起動プロセス

HPEでは、自社開発のサーバーBIOS/UEFIやファームウェア等に対し、厳格な品質管理プロセスを経てデジタル署名を施しています。iLO 5を起点とする「セキュアスタート」では、サーバー起動時に重要な5つのファームウェアを段階的にチェックし、正しく認証されたファームウェアによる「真のRoot of Trust」で起動プロセスを実行します。

①シリコンチップ(iLO 5)に焼き込まれたセキュリティロジックに基づき、iLO 5自身のファームウェアのデジタル署名を参照して認証

②HPE iLO 5ファームウェアがシステムROM(UEFI)を認証

③UEFI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

セキュアリカバリー:オンラインでのファームウェアの問題検知と復旧

運用段階では、iLO 5の「セキュアリカバリー」がファームウェア改変やマルウェア感染の監視・検知に威力を発揮します。稼働中のHPEサーバー上で、任意のタイミングでスキャンを実行することも、定期的に自動検知を行うことも可能です。ステータスはiLO 5のダッシュボードから確認でき、異常を検知したときは、iLO 5内に安全に格納されたバックアップによりオンラインのまま正常なファームウェアに戻すことができます。

Smart Array Secure Encryption:情報流出に備える暗号化機能

HPEサーバーでは、RAIDコントローラーからディスク内のデータを暗号化する「Smart Array Secure Encryption」をご利用いただけます。HPEサーバーに搭載可能なすべてのディスクの暗号化が可能で、性能・容量の要求に応じて自由にSSD/HDDを選ぶことができます。ディスク構成やRAID構成上の制約を受けることはなく、高コストの「自己暗号化ディスク」を導入する必要もありません。

Windows Server 2022の「Secured-Core Server」認定

Windows Server 2022が提供する「Secured-Core Server」は、安全なサーバー起動やファームウェア/ドライバー保護を強化する新機能です。HPE ProLiant Gen10 Plus/Gen10 Plus v2サーバーは、TPM 2.0セキュア暗号化プロセッサーを標準で搭載し、Secured-Core Serverとして認定されたハードウェアです。

Hewlett Packard Enterprise

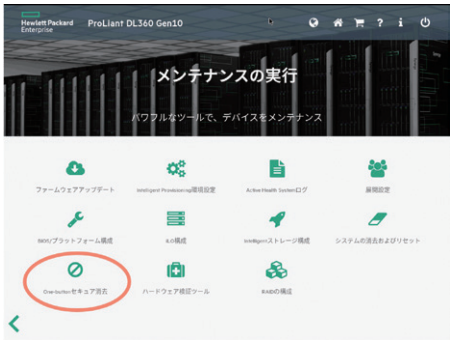
Microsoft

Windows Server 2022: Be cloud ready with hybrid.

4

廃棄時のデータ残留リスクを ワンボタンで解消

2019年、自治体で利用されていたHDDが不正に転売され、個人情報や行政文書が流出した事件が大きな注目を集めました。このようなサーバー廃棄時のリスクを解消するために、HPEは「お客様自身で安全･確実にデータを消去」する方法を提案します。米国立標準技術研究所（NIST）のガイドラインに準拠した、HPEのデータ消去テクノロジーにご注目ください。



「One-buttonセキュア消去」は管理画面から簡単に実行可能

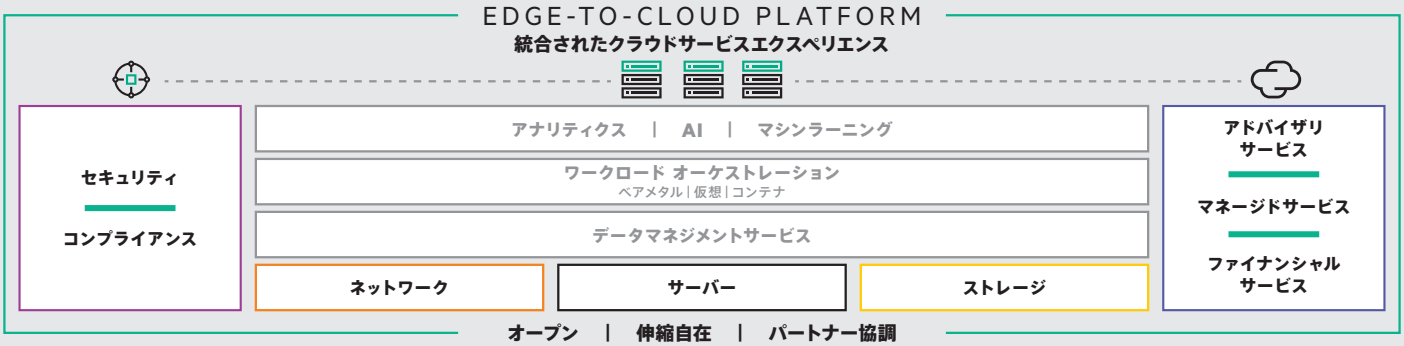
One-buttonセキュア消去：データ消去と初期化処理をワンボタンで

HPEの「One-buttonセキュア消去」は、サーバーに接続されているすべてのディスクのデータから、BIOS設定、ログまでを一括消去してサーバーを工場出荷時の状態に初期化することができます。米国立標準技術研究所が示すメディアサニタイズのガイドライン「NIST SP 800-88, Revision 1」に準拠したデータ消去テクノロジーを活用し、GUIによる容易な操作で安全･確実にデータ消去を行えます。

物理的に機密データの漏えいを防止するオプションサービス

故障交換したHDD/SSDをお客様またはパートナー様にて管理･廃棄される場合は、「故障ドライブ返却不要」の保守サービスをお選びいただけます。また、同サービスにてお客様のメディア（HDD/SSD）の「データ消去をHPEに依頼できるオプションサービス」もご用意しています。お客様の所有となったメディアに対し、お客様が指定する場所でデータ消去を実行、物理的に破壊します。作業完了後はHPEより「作業証明書」を提出いたします。

HPEのセキュリティソリューション＆サービス



ネットワークレベルでの ゼロトラストを実現

昨今のITインフラはゼロトラスト化が進み、守るべき情報資産とセキュリティの脅威が社内･社外問わず存在し、ネットワーク接続する端末も多様化しています。HPE Arubaでは、ネットワークレベルでゼロトラストを実現するために、ネットワークへ接続する端末への認証認可の実施や、認証結果に応じた適切なロールベースでのネットワークアクセス制御（RBAC）、インシデント発生時の隔離など動的なセグメンテーションの実現を可能にします。

ストレージの視点からデータ保護と セキュリティを強化

ランサムウェアの脅威が増大する中、データ保護の重要性はかつてないほど高まっています。巧妙化する攻撃はバックアップデータの消去や暗号化も試みます。HPEのストレージ製品は、オンプレミスおよびクラウドベースのデータ保護ソリューションとサービスにより、ランサムウェアの攻撃が届かない場所にバックアップデータを保管し、迅速かつ信頼性に優れたリカバリ、柔軟性のあるクラウドバックアップ、コスト効率に優れたデータアーカイブを実現します。

インフラストラクチャセキュリティの エキスパートチーム

HPE Pointnextは、お客様のインフラストラクチャセキュリティを支えるHPEのサービス組織です。Edge to Cloud全体にわたる包括的なセキュリティポートフォリオ、深い業界知識に基づくシステムデザインと豊富な実績に基づくプロジェクト推進力、運用を含む全てをas-a-Service型で提供できるサービスモデル――この三本の柱を元に「長期間安定して動作するシステムに適切なセキュリティとは」を提案し実現いたします。

セキュリティ機能対応表

iLO Advancedライセンスが必要

HPE ProLiant Gen10/HPE ProLiant Gen10 Plus/HPE ProLiant Gen10 Plus v2

セキュリティ項目	機能名	MicroServer Gen10 Plus *4	ML30 Gen10 Plus	ML110/350 Gen10	DL20 Gen10 Plus	DL110 Gen10 Plus	DL160/180 Gen10	DL360/380 Gen10/ Gen10 Plus	DL325/345 /365/385 Gen10 Plus /Plus v2	DL560 /580 Gen10
起動時のファームウェア正常性検証	Silicon Root of Trust	○	○	○	○	○	○	○	○	○
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**	○	○	○	○	○	○	○	○	○
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・隔離**	○	○	○	○	○	○	○	○	○
管理プロセッサーのFIPSモード	iLOセキュリティ設定	○	○	○	○	○	○	○	○	○
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**	○	○	○	○	○	○	○	○	○
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**	○	○	○	○	○	○	○	○	○
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	○	○	○	○	○	○	○	○	○
Trusted Platform Module	TPM(オプション)	○	○	○	○	○	○	○	○	○
データの暗号化*1	HPE Secure Encryption(オプション)*2	○	○	○	○	○	○	○	○	○
802.1AR/802.1Xを利用した機器認証	セキュア ゼロタッチオンボーディング*3	—	—	—	—	○	—	○	○	—
証明書を利用したデバイス証明	デバイス証明(プラットフォーム証明書)*3	—	—	—	—	○	—	○	○	—

2022年7月現在

*1: SED暗号化ドライブが必要な場合にはMegaRAIDでの構成を検討ください。
*2: HPE Secure EncryptionはSmartアレイ/SmartRAIDの構成で、HPE Smart Array SR Secure Encryption E-LTU のライセンスが必要となります。
*3: セキュア ゼロタッチオンボーディング、デバイス証明は工場による組み込み作業が必要です。機種により対応工場が異なります。
*4: HPE ProLiant MicroServerでiLO 5の機能を使用するには、別途HPE ProLiant MicroServer Gen10 Plus iLO専用ポート増設/有効化キットが必要です。
詳細及び最新情報は弊社Web等でご確認ください。

お問い合わせはこちら

CALL

カスタマー・インフォメーションセンター
0120-268-186
(フリーダイヤルをご利用できない場合 03-6743-6370)
月曜日～金曜日 9:00～19:00
(土曜日、日曜日、祝日、年末年始、および5月1日お休み)

Hewlett Packard Enterprise

日本ヒューレット・パッカード合同会社
〒136-8711 東京都江東区大島 2-2-1

© Copyright 2022 Hewlett Packard Enterprise Development LP.

本書の内容は、将来予告なく変更されることがあります。日本ヒューレット・パッカード製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。日本ヒューレット・パッカードは、本書中の技術的あるいは校正上の誤り、脱字に対して、責任を負いかねますのでご了承ください。記載されている会社名および商品名は、各社の商標または登録商標です。

A00125522JPN 記載事項は個別に明記された場合を除き2022年7月現在のものです。