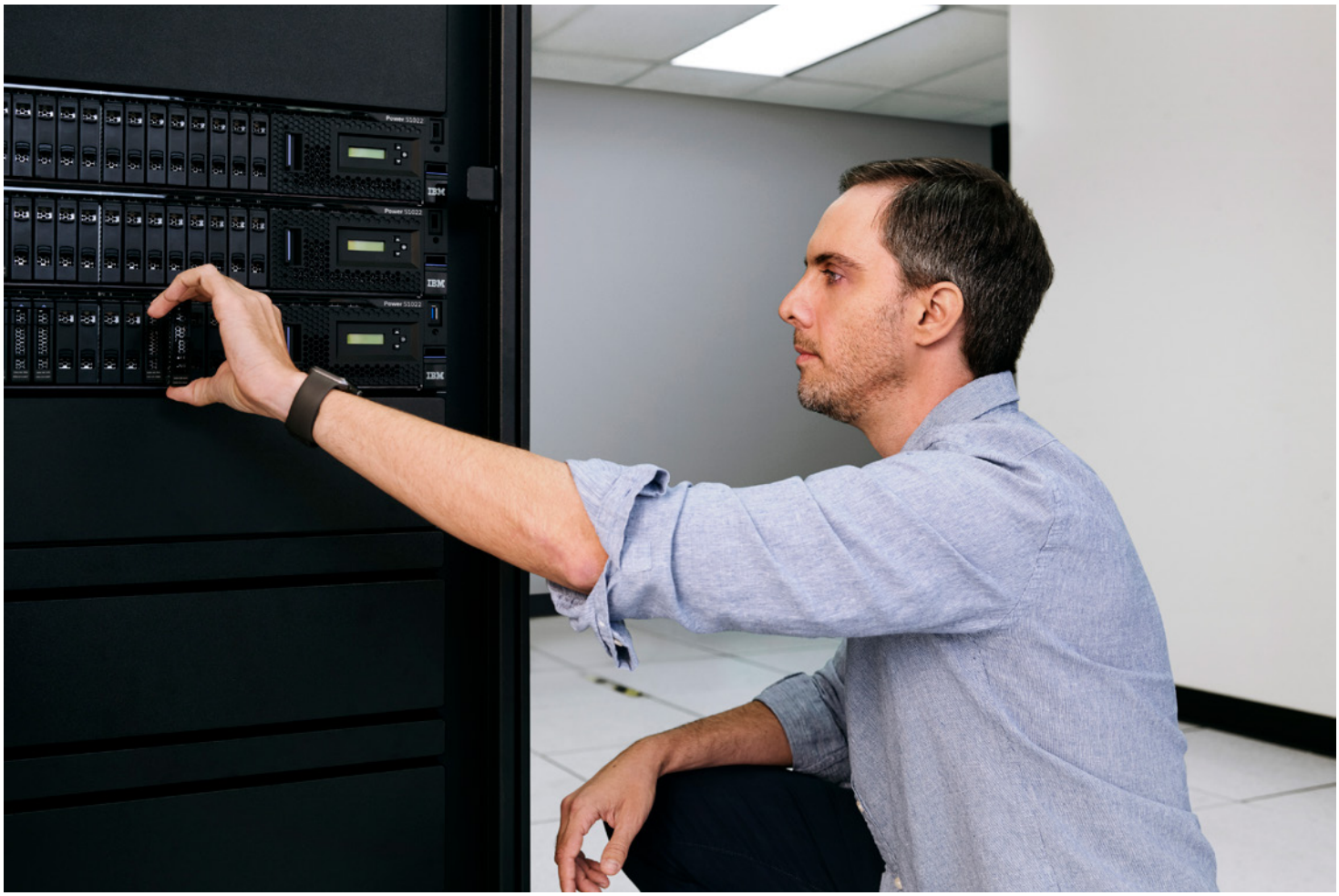
IBM Powerを活用したセキュリティーへの多層型アプローチ

ゼロトラスト・アプローチに不可欠なインフラストラクチャー



目次

巧妙なサイバー攻撃時代における企業IT

今日のIT事情

COVID-19の大流行が始まって以来、驚異的な数の壊滅的なデータ侵害が記録されています。データ侵害の平均コストは現在424万ドルで、昨年の386万ドルから10%増加しています。これは業界における過去7年間で最大の増加率であり[1]、これによりセキュリティーが最大の関心事となりました。セキュリティー戦略を改善し、常時接続している世界で迅速、安全、かつセキュアにビジネスを展開することが、今日多くのエグゼクティブの関心事となっており、その結果、セキュリティー予算が増加しています。しかし、支出の増加や技術の変化により、新たな複雑性やリスクも発生し、ITセキュリティーは常に脅かされることになります。セキュリティー専門家が最も懸念していることの1つは、巧妙な攻撃経路が増え続け、今日のビジネスが、かつてないほど多くの側面にさらされ続けていることです。

ハードウェアやファームウェアレベルでの脆弱性は、最近までは大きな関心事ではなかったかもしれませんが、現在では、今日の脅威の現状における主要なターゲットとなっています。

多くの点で、今日のビジネスが克服しなければならないサイバーセキュリティーに関する課題は、次の立証された真実に集約されます。

- ITスタックは拡大しており、ハッカーは活動範囲を 広げている。
- 組織は、将来の脅威を先取りし、ハイブリッドクラウド・インフラストラクチャーを守るため、最高レベルのセキュリティーでプラットフォームを保護する必要がある。

424万ドル

データ侵害の平均コストは現在**424万ドルで、**昨年の 386万ドルから**10%増加**しています。

現在の脅威の実態

包括的アプローチ

企業は、知的財産、機密情報、顧客データ、ワークロードのプライバシーに対する現在および未来の脅威を防ぐために、セキュリティー・システムに依存しています。

データ侵害やサイバー攻撃を防ぐため、専門家がどのように戦略的にITセキュリティーに取り組むかが非常に重要です。セキュリティーの脆弱性は、ダウンタイムにつながるだけでなく、どのような組織においてもコスト増加につながります。ランサムウェア攻撃は最大の脅威であり、企業は1度の攻撃につき平均462万ドルの損害を被っています。[1]。IBM®Power®のプラットフォームの整合性は、エンドポイント検出と応答（EDR）、および継続的な多要素認証（MFA）などのゼロトラストの概念を導入することにより、ランサムウェアのリスクを軽減することができます。

ビジネス主導型、コンプライアンス主導型、あるいは金銭主導型のアプローチを採用するだけでは、高まるITシステムのリスクからビジネス・プロセスを十分に保護することはできません。単独でのアプローチでは、効率的で統合されたセキュリティー戦略における重要な分野横断的な側面を見落とす可能性があります。理想的な行動方針には、セキュリティーに関連する主要な分野にわたるリスクを特定するための計画と評価が含まれます。IBM Powerのテクノロジー、およびIBM®Power10プロセッサーをベースとするシステムは、お客様のセキュリティー戦略に合わせた包括的なゼロトラストによる多層型アプローチを提供して、組織の安全とコンプライアンスを確保します。この多層型アプローチには次のものが含まれます。

– ハードウェア
– オペレーティング・システム
– ファームウェア
– IBM® PowerSC 2.0テクノロジー
– ハイパーバイザー

包括的なセキュリティー・アプローチを採用することで、セキュリティー環境に 影響を及ぼす脅威に対処できます。

ハッカーの巧妙化

組織が従来のオンプレミス型のデータセンターの制約から外れ、ハイブリッドクラウドやマルチクラウド環境に移行すればするほど、サイバー攻撃者は既成概念にとらわれない思考をする余地が増えることになります。最小権限を導入し、境界にベースの制御を強化することで、増加する脅威への対処が可能になります。従来のサイバー攻撃はネットワーク・レベルでは収まらず、より広域な領域でより強力な攻撃が行われるようになっています。

データ・アクセスの増加に伴うセキュリティーの重要性

現在さまざまなサーバー、ハイブリッドクラウド環境、多数のモバイル・デバイスやエッジ・デバイスなど、組織内のデータは、従業員により実質的にどこからでも保存、アクセスできるようになりました。このサーバーとデバイスが密接に交差するこの状況は、デジタル変革やモダナイゼーション進行の副産物です。アクセスしやすさにより、攻撃経路が大量に生みだされ、悪用される可能性があります。

規制強化はリスク・プロファイルに影響する

規制へのコンプライアンスを確保するために導入されたプロセスは、意図しないリスク露出につながる可能性もあります。一般データ保護規則（GDPR）は、こうした最近の傾向の1つに過ぎません。管理機関は組織のデータ使用法に対し細心の注意を払っています。しかし、その一方で、日々の業務に複雑な要素を加える原因にもなります。

従業員が 脆弱性の原因となる

昨年のデータ漏えいの20%は従業員の過失によるデータ漏えいが原因でした[1]。ログイン情報の他、フィッシング詐欺や電子メールの流出により、従業員が知らないうちに企業の情報を危険にさらしていることがあります。どのようなセキュリティー対策を行い、どのように脆弱性に対処しても、従業員から発生するリスクは常にある程度存在します。サイバー犯罪の時代には、これらの一般的なセキュリティー脅威に関して従業員を教育し、報告システムを導入することは不可欠です。エンドポイントの保護やコンプライアンスの遵守に費やした努力は、ミスや巧妙な悪意ある攻撃によって水の泡になる可能性があります。

一方、多くの組織は有能なサイバーセキュリティーの人材の確保と維持に苦労しており、常にスキル不足に陥っています。このようなスキル不足に対処するため、組織は、運用、コンプライアンス、パッチ適用やモニタリングを自動化した簡易なセキュリティー管理を導入できます。エンドポイント検知を増やして保護するために設計されたエンドツーエンド・セキュリティーを、リソースを追加せずに受けることができます。

ITアーキテクチャーが進化し続け、テクノロジー、ワークカルチャー、およびコンプライアンスの変化に対応し続ける中、サイバー脅威の現状の規模、種類、および速度は、増加の一途をたどっています。つまり、セキュリティー戦略もネットワーク・レベルを超えて進化する必要があります。

ゼロトラスト戦略の重要性

包括的アプローチ

ゼロトラスト概念を導入することで、そそきの複雑化しがちなIT環境における、セキュリティーに対応することができます。IT担当者は、ハイブリッドクラウドとマルチクラウド環境における可視化と管理に奮闘しています。ゼロトラストは、パフォーマンスやユーザー体験に影響を及ぼさずに、アクセス管理を制限するより包括的な戦略に移行することによって、リスクを管理します。さまざまなサード・パーティー・ベンダーのセキュリティー・ソリューションを導入することで、スタックの各レベルにセキュリティーを組み込むことは可能です。しかし、このアプローチはすでに存在する複雑さを悪化させ、ネットワークにさらに多くの脆弱性と露出のポイントを生じさせます。最善の方法は、多層型ゼロトラスト・アプローチを採用することです。これは、組織のすべてのデータとシステムを保護すると同時に、複雑さを最小限に抑えるものです。こうした点を踏まえ、IBM® Information Security Frameworkは、ビジネス主導のセキュリティーに包括的なアプローチを使う際、ITセキュリティーのあらゆる側面に適切に対応できるよう支援します。

IBM Information Security Frameworkは、以下に重点を置いています：

1. インフラストラクチャー ー ユーザー、コンテンツ、およびアプリケーションに対する洞察を把握し、巧妙な攻撃から保護します。
2. 高度なセキュリティーと脅威の研究 ー 脆弱性と攻撃手法に関する知識を得て、その洞察を保護技術によって適用します。
3. 人 ー 包括的アイデンティティー・インテリジェンスによりセキュリティー・ドメイン全体にわたり企業のアイデンティティーを管理、拡張します。
4. データ ー 組織の最も信頼される資産のプライバシーと整合性を確保します。
5. アプリケーション ー より安全なアプリケーション開発のコストを削減します。
6. セキュリティー・インテリジェンスと分析 ー コンテキストの追加、自動化と統合によってセキュリティーを最適化します。
7. ゼロトラスト哲学 ー 適切なユーザーと適切なデータを接続、保護しながら組織を保護します。

IBM Security Framework (PDF, 25.2 MB)に関する詳細と、さらにドリルダウンする方法はこちらをご覧ください。

IBM Powerテクノロジーで スタックを保護する仕組み

IBM Powerの概要

IBM Powerテクノロジーは、プロセッサ、ファームウェア、OS、ハイパーバイザー、そしてアプリやネットワーク・リソース、セキュリティー・システム管理に至るまで、スタック全体を統合する包括的なエンドツーエンドのセキュリティーにより、サイバー耐性を高め、リスクを管理することが可能です。

ハードウェア、ファームウェア、およびハイパーバイザー

オンチップ・アクセラレーター
IBM　Power10プロセッサー・チップは、サイドチャネル攻撃の軽減性能を強化するよう設計され、サービス・プロセッサーからのCPU分離が改善され搭載されています。この7nmのプロセッサーは最大3倍の容量増加に対応し、より高いパフォーマンスを実現します[2]。

エンドツーエンドの暗号化
IBM Powerソリューションの透過的なメモリー暗号化は、企業が今日直面する厳しいセキュリティー基準を満たす、エンドツーエンドのセキュリティーを実現するよう設計されています。また、暗号処理の高速化、耐量子暗号、完全準同型暗号に対応し、将来の脅威から保護するよう設計されています。最新のIBM Powerシステム・モデルで加速された暗号は、IBM Power E980のテクノロジーのコアあたり高度暗号化標準(AES)[3]の暗号性能が2.5倍高速化されています。組織は、追加の管理設定なしに、透過的メモリー暗号化のメリットが受けることができます。

EDRソフトウェア
外部からの脅威の増加により、顧客データとデジタル資産の保護する上で、エンドポイント・セキュリティーが重要にります。エンドポイントで潜在的脅威を検知することにより、組織はビジネスの継続性を妨げることなく、迅速に行動し、インシデントを解決できます。統合されたアプローチによって複雑さを排除し、最も危険な攻撃からも組織を保護することができます。

2.5倍

最新のIBM Powerシステム・モデルによる高速暗号化では、IBM Power E980のテクノロジーと比較して、**コアあたり2.5倍の高速の高度暗号化標準(AES)暗号性能**を発揮します[3]。

多要素認証や最小権限などの原則を導入することで、すべてのAPI、エンドポイント、データ、およびハイブリッド クラウドのリソースを保護し、保護を強化します。

ゼロトラスト原則
組織は増大する脅威を管理するため、ゼロトラスト原則を採用するように進化しています。多要素認証や最小権限などの原則を導入することで、すべてのAPI、エンドポイント、データ、およびハイブリッドクラウドのリソースを保護し、さらなる保護を実現します。

IBMのゼロトラスト・フレームワークは、このコンセプトを実現します。

- **洞察の収集** – ユーザー、データ、およびリソースを理解して、完全な保護を保証するために必要なセキュリティー・ポリシーを作成します。
- **保護** – コンテキストを迅速かつ一貫して認証し、ポリシーを適用することで、組織を保護します。
- **検知と対応** – 業務への影響を最小化し、セキュリティー侵害を解決します。
- **分析と改善** – より多くの情報に基づいた意思決定を行うために、ポリシーとプラクティスを調整することによって、セキュリティ体制を継続的に改善します。

ゼロトラスト原則を導入することで、企業は安全にイノベーションを起こし、ビジネスを拡張することができます。

IBM Power10ソリューションにおけるセキュア・ブート

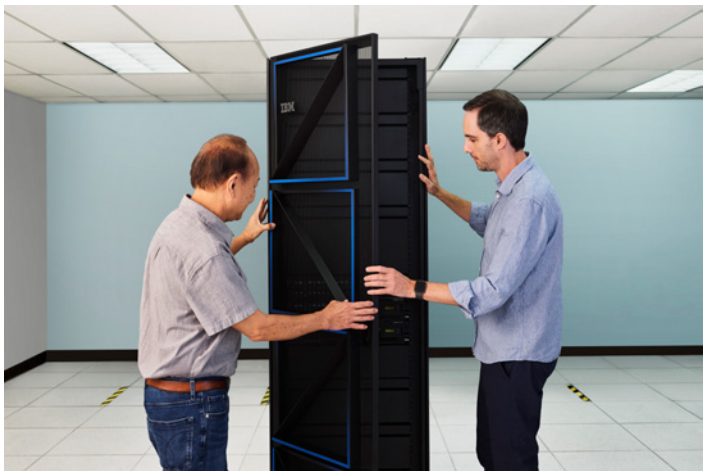
セキュア・ブートは、デジタル署名ですべてのファームウェア・コンポーネントを検証、認証することにより、システムの整合性を保護するよう、設計されています。IBMがリリースしたファームウェアはすべて、ブート・プロセスの一部としてデジタル署名され、検証されています。すべてのIBM Powerシステムには、サーバーにロードされたファームウェア・コンポーネントすべての測定値を蓄積し、その検査とリモート検証を可能にするトラステッド・プラットフォーム・モジュールが搭載されています。

IBM PowerVMエンタープライズ・ハイパーバイザー
IBMPowerVM®エンタープライズ・ハイパーバイザーは、主要競合他社と比較して、優れたセキュリティー実績を有しているため、安心して仮想マシン(VM)や クラウド環境を保護できます。

オペレーティング・システム

IBM Power Systemsは、IBM® AIX®、IBM i、およびLinux®などの幅広いオペレーティング・システムに先進的なセキュリティー機能を提供します。EDR for IBM Powerのテクノロジーは VMのワークロードにさらなるセキュリティーを提供し、ネットワーク内のすべてのエンドポイントで完全な保護を保証します。パスワードに依存するシステムの安全性を確保するために、AIX および Linuxオペレーティング・システムでは、IBM PowerSC多要素認証(MFA)を使用して、すべてのユーザーに対し追加の認証レベルを要求し、パスワード・クラッキング・マルウェアから保護します。OSにより機能は異なりますが、例えば以下のようなことが可能です。

- セキュリティーを犠牲にすることなく、通常rootユーザーに割り当てられる管理機能
- 個々のキーストアを通しでファイル・レベルのデータを暗号化する
- ユーザーが使用できるコマンドや機能、アクセス可能なオブジェクトの制御を強化する
- ユーザーやオブジェクトのシステム値やオブジェクト監査値を使用し、セキュリティー監査ジャーナルにオブジェクトへのアクセスを記録する
- ドライブ全体を暗号化し、最初にオブジェクトを暗号化し、その後暗号化された形式で書き出す
- 要求するユーザーに対してファイルを開く前に、すべてのファイルを測定し、検証する



ワークロード、VM、コンテナー

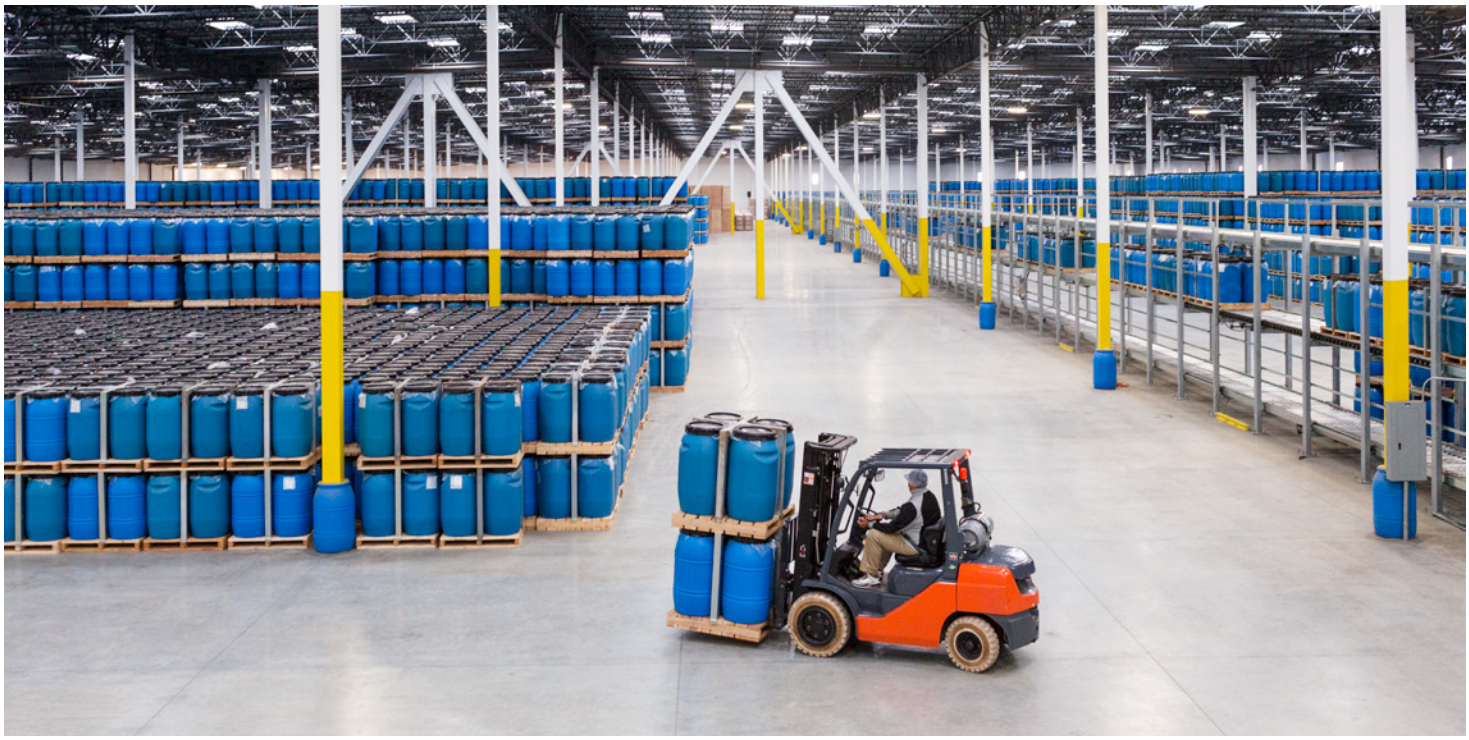
ワークロードはオンプレミスのデータ・センターだけに制限されることはなく、仮想化されたハイブリッドクラウドおよびマルチクラウド環境に継続的に移行しています。例えば、多くの組織がコンテナーを採用して、ハイブリッド・インフラストラクチャーに新規および既存のアプリケーションを導入しています。

これらのようにますますダイナミックになる環境やワークロードには、同ように柔軟性のあるセキュリティー機能が必要です。IBM Powerソリューションでは、暗号化アルゴリズムの高速化、セキュアなキー・ストレージ、ポスト量子暗号と完全準同型暗号(FHE)暗号アルゴリズム用のCPUサポートによりワークロードのプライバシーを保護し、セキュリティーのニーズを満たすことができます。

IBMは、コンテナー展開の特有のセキュリティ要件に対応するため、IBM PowerのテクノロジーとRed Hat® OpenShift® Container Platformを使って、ライフサイクルを通じてさらにセキュアなコンテナーを構築している独立系ソフトウェア・ベンダー(ISV)Aqua Security社とも提携しています。

IBM Powerサーバーは、オンプレミスからクラウドに至るまで、エンドツーエンドのメモリー暗号化と高速暗号化性能によってデータを保護するよう設計されています。VM、コンテナー、およびサーバーレス機能を含む、クラウドネイティブ・ワークロード向けに組み込まれたポリシーは、アプリケーションのモダナイゼーションのためのセキュリティーおよびコンプライアンス要件を統合する際、Red Hat OpenShiftおよびIBM Powerの顧客をサポートするために構築されています。

Live Partition Mobility(LPM)
IBM Powerのテクノロジーで移動中のデータを安全に保護できます。LPMは、あるシステムから別のシステムに移行する必要があるときに、暗号化でVMを保護します。オンプレミス・データセンター、ハイブリッドクラウド環境、またはその両方を仮想化する場合、この機能は非常に重要です。



IBM Powerソリューションに統合されたセキュリティー製品

IBM PowerSC 2.0テクノロジー

IBM® PowerSC2.0テクノロジーは、クラウド環境および仮想環境における企業のセキュリティーおよびコンプライアンスをのための統合ポートフォリオ製品です。IBM PowerSC2.0テクノロジーは、IBM Powertechnologyのセキュリティー機能を管理するためのWebベースのUIを提供しながら、スタックの最上位に位置し、最下位レベルのソリューションから存在するものです。

IBM PowerSC 2.0テクノロジーは、シンプルさと自動化機能により、コンプライアンスの監視と実施を合理化することにで、時間、コスト、およびリスクを削減することができます。このソリューションは、監査プロセスをサポートし、お客様がコンプライアンス認証をより効率的に取得できるように支援します。また、スタック全体の可視性を高めることにより、セキュリティー・リスクも削減することができます。

IBM PowerSC 2.0 Standard Editionの機能

多要素認証（MFA）技術

MFAは現在、IBM PowerSC 2.0ソリューションに統合されています。これにより「信頼せず、常に検証」というゼロトラスト原則に従ったMFAメカニズムの導入が容易になります。このアプローチは、RSA SecurIDに基づく認証、および共通アクセス・カード（CAC）や個人認証検証（PIV）カードを含む証明書認証オプションにより、ユーザーがログインするための代替要素をサポートします。IBM PowerSC MFAでは、ユーザーに追加認証要素を求めることにより、システムの保証レベルを向上させます。

IBM PowerSC 2.0 テクノロジーが時間、費用、リスクを削減

EDR機能
IBM PowerSC 2.0ソリューションは、EDR for Linux on IBM Powerのワークロードを導入し、侵入検知と防止、ログ検査と分析、異常検知とインシデント対応など、エンドポイント・セキュリティーを管理する最新の業界標準機能を提供します。

コンプライアンスの自動化
IBM Powerファミリーには、無数の業界標準に対応したプロファイルがあらかじめ組み込まれています。これらのプロファイルをカスタマイズして、Extensible Markup Language(XML)に触れることなく、企業ルールに統合することができます。

リアルタイム・コンプライアンス
セキュリティー上重要なファイルを開いたり、操作しようとする人がいれば、検知して警告します。

信頼できるネットワーク接続
VMが規定パッチ・レベルではない場合に警告します。修正プログラムが利用可能になると通知されます。

トラステッド・ブート
AIX論理パーティション上で動作するすべてのソフトウェア・コンポーネントの整合性の検査とリモート検証が可能です。

トラステッド・ファイアウォール
AIX、IBM　i、Linuxオペレーティング・システムの内部ネットワーク・トラフィックを保護、ルーティングします。

トラステッド・ロギング
バックアップ、アーカイブ、管理が容易な一元化された監査ログを作成します。

事前構成された報告とインタラクティブ・タイムライン
IBM PowerSC Standard Editionは、事前構成された5つのレポートによる監査をサポートしています。インタラクティブ・タイムラインにより、VMのライフサイクルやイベントを確認することができます。

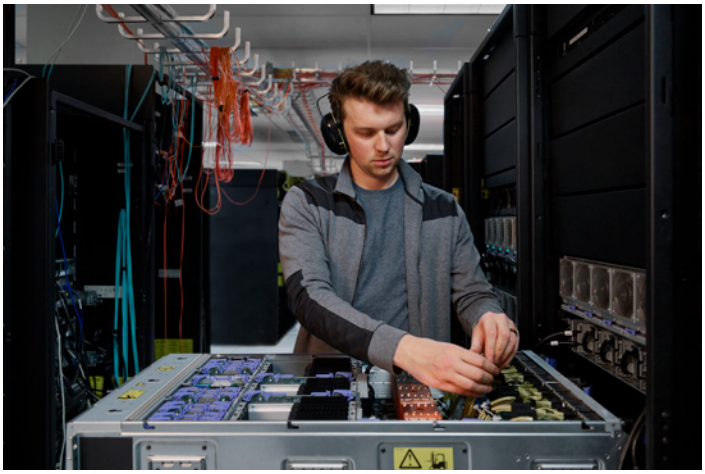
IBM PowerSC in Cloudと仮想化環境を使用して、ITセキュリティーとコンプライアンスの管理を簡素化する方法については、こちらをご覧ください

セキュリティに対する最も強力なアプローチは、シームレスに統合されたもの

シームレスな統合

巧妙化するサイバー犯罪者の手口や技術の進化が、今日のビジネスに新たな脆弱性を生み出し続ける中、多層型でゼロトラスト、組織の複雑性を増大させることのないセキュリティー・ソリューションを統合させることが重要とです。IBM Powerのソリューションは、単一ベンダーの緊密に統合された詳細なソリューションにより、エッジからクラウド、そして、コアに至るまで、スタックのあらゆるレベルを保護することができます。複数のベンダーと協働すると、最終的に様々な意味でコスト高となる複雑性を招きます。IBM Powerテクノロジーは、パフォーマンスに影響を与えることなく、プロセッサー・レベルでエンドツーエンドの暗号化をサポートします。インフラストラクチャーを統合することで、スタックの各層に焦点を当てることができます。

単一ベンダーによるセキュリティーは、セキュリティー戦略を簡素化し強化する自然な利点を提供することができます。30 年に及ぶセキュリティーのリーダーシップを基盤に、IBM Power テクノロジーは、IBM 内外の他の組織と広範なパートナーシップを結び、セキュリティの専門知識をさらに深め、広めることができます。このようなパートナーシップにより、IBM Powerテクノロジーは、さらに大きなセキュリティー専門家のコミュニティーを利用することができ、問題を迅速に特定し、自信をもって対処できるようになります。また、IBM Security®およびIBM Research®ビジネス・ユニットからの支援により、PowerSC 2.0ポートフォリオも活用して、Power10サーバーは、インサイダー攻撃を含む複数の脅威を徹底的に阻止することが可能です。



IBM Powerソリューションの可能性を探るためのコンサルテーションを予約する

お問い合わせ →

注
1. Cost of a Data Breach Report 2021, IBM Security, July 2021 (PDF, 3.6 MB)
2. 3倍の性能は、2×30コア・モジュール付きPOWER10デュアル・ソケット・サーバー製品と、2×12コア・モジュール付きPOWER9デュアル・ソケット・サーバー製品との比較による、整数、エンタープライズ、浮動小数点環境のプリシリコン・エンジニアリング分析に基づいています。両モジュールのエネルギー・レベルは同じです。2 10～20倍のAI推論能力向上は、2×30コア・モジュールを搭載したPOWER10デュアル・ソケット・サーバー製品と、2×12コア・モジュールを搭載したPOWER9デュアル・ソケット・サーバー製品との比較による、各種ワークロード（Linpack.Resnet-50 FP32, Resnet-50 BFloat16, Resnet-50 INT8）のプレシリコン・エンジニアリング分析に基づいています。
3. RHEL Linux 8.4とOpenSSL 1.1.1gライブラリで得られた予備測定によると、IBM Power10E1080(15コアモジュール)とIBMPOWER9E980（12コアモジュール）とを比較した場合、GCMモードとXTSモードの双方でAES-256がコアあたり約2.5倍高速で実行されます。

IBM Cloud
日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21

米国で作成
2022年6月