

IBM PowerSC

プライベート・クラウド保護のために設計されたセキュリティとコンプライアンスのソリューション

ハイライト

- セキュリティー管理とコンプライアンス評価を簡素化
 - データセンター全体のセキュリティ・コンプライアンスを素早く表示するユーザー・インターフェース
 - コンプライアンス規則を順守するための管理コストを削減
 - 仮想化システムに対する監査機能を強化
 - セキュリティー監査の準備に必要な時間とスキルを低減
 - 仮想化環境におけるセキュリティ・リスクの検出を強化
-

セキュリティとコンプライアンスは多くの企業にとって重要な検討課題です。セキュリティ・リスクから個人情報や企業情報を保護するために規制が制定され、その規制要件に準拠する必要がある現在、特にその傾向は強まっています。一般的な業界セキュリティ標準に IT システムを確実に準拠させて、システム・セキュリティを維持することは、今日の仮想化 IT インフラストラクチャーでは特にワークロードを要する困難な作業となることでしょう。IBM® Power Security and Compliance (PowerSC) は、PowerVM と Power Systems による仮想化環境向けに最適化されたソリューションを提供し、セキュリティとコンプライアンスへの対応を支援します。

システムを自動的に構成し、セキュリティとコンプライアンスを最適化

第三者機関のセキュリティ標準にシステムを確実に準拠させるプロセスには、多くの場合、多大な労力と時間が必要になります。コンプライアンス標準は一般的に文章が長く複雑なため、内容を理解して AIX または Linux オペレーティング・システムの構成に適切に反映することは簡単ではありません。また、標準の対象範囲はオペレーティング・システムや仮想化ソフトウェアのさまざまな領域にわたるため、複数の管理インターフェースからシステムを構成することが必要になることもあります。

PowerSC は、Web ベースの管理インターフェースと事前構成済みのコンプライアンス・プロファイルを備えることで、最も代表的な外部のセキュリティ標準とコンプライアンス標準のうちの一部への準拠に伴う管理作業を容易にします。

PowerSC のセキュリティとコンプライアンスの自動化は、Payment Card Industry Data Security Standard (PCI DSS) と Health Insurance Portability and Accountability Act Privacy and Security Rules (HIPAA)、North American Electric Reliability Corporation (NERC)、米国国防総省の Security Technical Implementation Guide for UNIX (DoD STIG) に対応するプロファイルを提供するとともに、Control Objectives for Information and related Technology (COBIT) に規定されているベスト・プラクティスの導入をサポートします。米国サーベンス・オクスレー法の適用対象となる株式公開企業の多くは、COBIT のベスト・プラクティスを導入しています。PowerSC は、データベース・サーバーの最適なセキュリティの構成を自動化するためのセキュリティ自動化プロファイルも提供しています。



PowerSC の最新のリリースでは、Web ベースのユーザー・インターフェースから、上述したプロファイルを適用して監視できるようになりました。シンプルなユーザー用の画面から、以下の操作が可能になります。

- 環境全体の正常性と状況を表示するための役割ベースのアクセス
- 提供されているプロファイルに基づいてカスタム・プロファイルを作成可能
- カスタム・グループに入れられた類似のエンドポイントを表示して、アクションを実行可能

PowerSC のセキュリティーとコンプライアンスの自動化は、システム構成設定の管理作業を大幅に軽減するため、セキュリティー管理者は、システム構成設定以外の要件に準拠するために時間をかけることができます。

仮想インフラストラクチャーの可視化と強化を促進

PowerSC は、仮想マシンの信頼性を根本から保証する機能を幅広く提供します。機能には、Trusted Computing Group が提供する Trusted Platform Module (TPM) の仮想実装である「Trusted Boot」が含まれます。PowerSC の Trusted Boot 機能は、Power Systems 上で PowerVM ハイパーバイザーとともに実行中の AIX 仮想マシンに対して仮想 TPM 機能を提供します。

この TPM 機能は、各仮想マシンのシステム・ブート・プロセスを評価します。また AIX Trusted Execution テクノロジーと連携し、ディスク上のブート・イメージ、オペレーティング・システム全体、そしてアプリケーション層においてセキュリティーと信頼性を保証します。各仮想マシンは独自の仮想 TPM を備えており、信頼性を根本から検証するために使用される固有の評価データを保持しています。この機能は、POWER8 テクノロジーを用いて構築されるすべての Power Systems または eFW7.4 ファームウェア以降を実行しているシステムで使用できます。

PowerSC とともに提供される OpenPTS という信頼性の高いモニターから、管理者は監視し、AIX 仮想マシンの信頼性を保証できます。モニターにより、PowerVM と Power Systems による仮想化環境の信頼性とセキュリティーのレベルが明確になります。

サイトのセキュリティー・ポリシー順守を仮想マシンにおいても保証

複数のシステムにまたがって構成された仮想マシンをメンテナンスする場合は、従来の物理システム環境とは異なる管理上の問題が生じます。例えば、パッチ適用プロセス中に、仮想マシンがサスペンド状態にされたり、電源が切られたり、別のサーバーに移動されたりすることがあります。また、仮想マシンの移動が、脆弱（ぜいじゃく）性につながることもあります。パッチ・レベルが移動先の物理システムで要求されるものと異なることがあるからです。

PowerSC の Trusted Network Connect (TNC) と Patch Management は、仮想化データセンター向けに制定された企業パッチ・ポリシーに違反している AIX 仮想マシンを検出します。違反している仮想マシンが検出されると、アラートが発行されます。TNC と Patch Management は、Service Update Manager Assistant (SUMA) と Network Installation Manager (NIM) の両方のデータを分析して、各仮想マシンをネットワークの起動時にチェックします。

TNC と Patch Management は、IBM Electronic Customer Care システムも監視して、AIX システムに影響を与えるセキュリティー・パッチやアップデートが新たに公開された場合にアラートを発行します。ショート・メッセージ・サービス (SMS) で携帯電話にアラートを送信するように構成することもできます。

最新のリリースでは、TNC と Patch Management は、AIX ツールボックスや、AIX オープン・ソース・パッケージのその他の Web ダウンロード・サイトからダウンロードされたパッケージの基本 AIX 用に提供されているオープン・ソース・ソフトウェアも監視します。

仮想環境内の監査証跡管理を強化

PowerSC の Trusted Logging は、同一サーバー上のすべての仮想マシンの AIX システム・ログを集中管理し、単一の PowerVM Virtual I/O Server (VIOS) インスタンス上に保持できるようにします。このセキュア VIOS 仮想マシンは、各 AIX 仮想マシンから受信したすべてのログ・データを保護します。セキュア VIOS 上に保持されたシステム・ログの削除や変更は、AIX 仮想マシンの管理者にはできません。

Trusted Logging が提供するロギングの集中管理を導入することで、システム・ログのバックアップやアーカイブ、監査にかかわる管理者のワークロードを大幅に削減できます。

仮想ネットワーク・コンプライアンスを制御し実行

PowerSC の Trusted Firewall は、ネットワークのフィルター処理と制御をローカル・サーバー仮想化環境内で可能にする仮想ファイアウォールを提供します。また、仮想マシン間を安全かつダイレクトにつなぐローカル・ネットワーク・トラフィックを実現することで、パフォーマンスを向上させ、ネットワーク・リソースの消費量を抑えます。さらに、トラフィックを監視し、ファイアウォールに追加すべきトラフィックに関するアドバイスを提供します。そして、仮想マシンのネットワーク・セグメントを Trusted Firewall に追加するための適切なコマンドを生成します。

ネットワーク分離ポリシーへのコンプライアンスを監視

PowerSC の Trusted Surveyor は、ネットワークの構成ドリフトを監視し、定義済みのポリシーにネットワークが準拠しているかに関するレポートを作成する機能を備えています。この機能により、仮想化ネットワーク・インフラストラクチャーに対する独立した監査とガバナンスが可能になり、構成変更の一貫性を維持し確実に

IBM Systems
Data Sheet

制御できます。さらに、ネットワーク・コンプライアンスに対する監視を自動化することで、管理コストを削減できます。また、Trusted Surveyor コンプライアンス・モニターは、AIX、IBM i、Linux を含むすべての Power の仮想マシン・タイプで機能します。Trusted Surveyor は PowerSC のファミリー製品であり、別途ご購入が必要ですが、その他の PowerSC の機能は、PowerSC Standard Edition で提供されています。

IBM は、信頼できるセキュリティー・アドバイザーとして、数多くの世界的な企業や行政機関に対応しています。IBM は、セキュリティーを中核として設計したサーバーやストレージ、アプリケーション、サービスのオフリングを幅広く提供しています。Power Systems 使用環境におけるセキュリティーとコンプライアンスに関する IBM の専門知識の深さと幅広さは、業界トップレベルの水準です。

特長	メリット
セキュリティーとコンプライアンスの自動化 AIX、Linux	<ul style="list-style-type: none"> 業界セキュリティー標準への準拠にかかる管理コストを削減
コンプライアンスのリアルタイム・モニタリング AIX	<ul style="list-style-type: none"> セキュリティー・ポリシーに違反する原因となる システム変更がないかを継続的に監視し、発生した場合にはアラートを出す
コンプライアンス・レポート AIX、Linux	<ul style="list-style-type: none"> セキュリティーとコンプライアンスに関するレポートを監査員に提供するのにかかる時間とコストを削減
PCI、DoD STIG、HIPAA、NERC、COBIT セキュリティー標準に対応するデータベース・サーバー用の事前構成済みプロファイル AIX のすべてのプロファイル、Linux PCI および HIPAA	<ul style="list-style-type: none"> 業界セキュリティー標準の導入に伴う時間やコスト、リスクを低減
Web ベースのユーザー・インターフェース AIX	<ul style="list-style-type: none"> データセンター全体のセキュリティー・コンプライアンスを認識 業界のセキュリティー標準への準拠
Trusted Boot AIX	<ul style="list-style-type: none"> AIX オペレーティング・システム・イメージが誤ってまたは不正に変更されることを防止することでセキュリティー侵害のリスクを低減
Trusted Monitoring AIX	<ul style="list-style-type: none"> 信頼性のあるシステム構成に参加しているすべての AIX システムの状況を表示することで高度な信頼性を保証
Trusted Logging AIX	<ul style="list-style-type: none"> AIX 仮想マシンのシステム・ログを PowerVM Virtual I/O Server 上に安全に保管することでセキュリティー問題の改ざんや隠ぺいを防止 監査ログを VIOS で集中保管することでバックアップとアーカイブの時間を短縮
Trusted Network Connect および Patch Management AIX	<ul style="list-style-type: none"> サイトのパッチ・レベル・ポリシーの順守を仮想ワークロードにおいて保証 パッチ・レベルの前提条件を満たしていないシステムのアクティベーションに対して、コンプライアンス違反を通知
Trusted Firewall すべての仮想マシン・タイプ、AIX、Linux、IBM i	<ul style="list-style-type: none"> 仮想化層でローカルにファイアウォール・サービスを提供することでパフォーマンスを向上させ、ネットワーク・リソースの消費量を削減
Trusted Surveyor すべての仮想マシン・タイプ、AIX、Linux、IBM i	<ul style="list-style-type: none"> 仮想化ネットワークを確実に分離できるように可視化を提供し、セキュリティー・コンプライアンスを維持

詳細情報

IBM PowerSC の詳細については、日本 IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。

ibm.com/systems/jp/power/software/powersc/



© Copyright IBM Corporation 2016

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

Produced in Japan
October 2016

IBM, IBM ロゴ、ibm.com、AIX、Power Systems、PowerVM、PowerSC および POWER8 は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、ibm.com/legal/copytrade.shtml をご覧ください。

本書の情報は最初の発行日の時点で得られるものであり、予告なしに変更される場合があります。

本書に掲載されている情報は特定物として現存するままの状態を提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。



Please Recycle
