

McAfee Policy Auditor

より効率的な監査とパッチの評価

監査作業では正確性と適時性が重要なポイントとなります。法規制の要件は厳しさを増しています。脆弱性に対する攻撃を阻止するには、システムに対するパッチの適用状況を迅速に把握する必要があります。法的責任を軽減するためには、ベストプラクティスに従っていることを証明しなければなりません。McAfee® Policy Auditorを利用すれば、このような負担を軽減できます。この管理しやすい管理ソリューションでは、プロセスが自動化され、簡素化されています。パッチの配備状況をすばやく把握し、問題のあるセキュリティ構成をモニタリングできます。業界の主要な規制や内部ポリシーに対するインフラ全体あるいは特定のシステムの対応状況を定期的に報告することができます。McAfee Policy Auditorでは、コンプライアンスを維持しながら、コストと労力を軽減し、可視化を強化できます。

現在の企業環境でコンプライアンスの維持は以前よりも難しい状況になっています。新しい規制は次々に増え、それに対応していかなければなりません。多くの企業はコンプライアンス対応に疲弊しています。罰金や利益損失のリスクを回避するため、コンプライアンス対応に追われています。監査プロセスの大半を手動で行っているため、再現性がなく、作業を効率的に進めることができません。セキュリティ製品を継ぎ接ぎで使用しているため、作業が煩雑になり、環境全体を一目で把握することもできません。このため、監査は手間のかかる作業になっています。

McAfee Policy Auditorを利用すると監査作業の負担を軽減することができます。管理プラットフォームとして機能するMcAfee® ePolicy Orchestrator®と統合されているので、ポリシーを簡単に作成し、カスタマイズできます。ベンチマークの選択、調査、作成を行い、監査対象のIT資産に割り当て、監査結果を1つのダッシュボードで表示できます。また、ドリルダウン機能で詳細を確認できます。

主な特長

- 業界の主要なベンチマーク、パッチ要件、セキュリティ ベスト プラクティスへの対応状況を証明します。コンプライアンス対応を自動化し、管理作業の負担を軽減します。
- 内部ポリシーと外部ポリシーに対して正確で一貫したレポートを生成します。
- 大規模なマルチプラットフォームの企業環境で、システムへのパッチ、ポリシー、構成の適用状況をモニタリングし、検証します。
- 1つの管理ウィンドウでインフラ全体のセキュリティ状況を確認できます。
- 米国土安全保障省の継続的な診断と緩和 (CDM) の要件で義務付けられ、NIST (National Institute of Standards and Technology) で検証されたSCAP 1.2標準に準拠しています。

McAfeeとつながる



データシート

自動化で手動プロセスをなくす

McAfee Policy Auditorは、エージェント ベースのIT評価ソリューションで、SCAP (Security Content Automation Protocol) を使用して、内部および外部のIT監査に必要なプロセスを自動化します。時間や労力がかかる非効率な作業を行う必要ありません。McAfee Policy Auditorは、監査プロセスを自動化し、内部/外部ポリシーに対して正確で一貫性のあるレポートを作成します。これにより、監査作業の負荷を軽減し、セキュリティを強化できます。

変化の激しい現在の状況に対応するには、新しいコンプライアンスに迅速に対応し、監査要件を満たす必要があります。プロセスを簡素化し、推論に基づく監査作業を排除するため、McAfee Policy Auditorには、CIS、CJIS、PCI DSS 3.2、SOX、GLBA、HIPAA、FISMA、EU GDPR、ISO 27001、NIST 800-171、COBITなど、最新規格への対応状況を評価するテンプレートが用意されています。外部の新しいベンチマークを使用したり、ベンチマークのカスタマイズが必要な場合でも、コンプライアンスやプログラミングの専門知識は必要ありません。McAfee Policy Auditorでは、テスト値が自動的に設定されるMcAfeeのテンプレートを使用して、必要なベンチマークを簡単に作成できます。

内部または外部の規制に対する対応状況を診断するには、ネットワーク上にどのようなデバイスがあり、何が行われているのかをすぐに確認できる状態でなければなりません。McAfee Policy Auditorでは、自社のITインフラでネットワークに接続しているデバイスの状況をすぐに把握できます。Microsoft Windows環境用に設計されている高度なホスト診

断エンジンがアプリケーションのインベントリを作成し、ソフトウェアのインストールをモニタリングして、オープンポートとアクティブなサービスを検出します。

パッチの評価が簡単に

McAfee Policy Auditorでは、様々なプラットフォーム、オペレーティングシステム、企業環境でよく利用されるアプリケーションのパッチの適用状況を確認できます。プラットフォームとしては、Windows Server 2016、Windows 10 RS3、Red Hat Enterprise Linux 7 (RHEL 7) などに対応しています。Windows、Linux、Unixオペレーティングシステムに対応した包括的なパッチ ベンチマークも用意されています。アプリケーションのパッチ診断では、Adobe Acrobatなど、日々の業務で使用しているツールや、よく使われているブラウザ、Apple QuickTime、Java JRE/JDKなどの状況を確認できます。

McAfee Policy Auditorでは、Microsoft オペレーティングシステム、Microsoft Office、Adobe製品などに専用のベンチマークが用意されています。また、Internet Explorer、.NET、Microsoft Officeなどの最新バージョンに対するベンチマークも用意されています。カスタム ベンチマークを作成する必要はありません。次のような一般的なデスクトップアプリケーションに最新のパッチを適用できます。

- Adobe: Flash、Reader、Acrobat、Shockwave
- Google Chrome、Mozilla Firefox、Mozilla Thunderbird
- Java JRE/JDK、Apple iTunes、Apple QuickTime

データシート

パッチの適用、セキュリティ構成、コンプライアンス検証を迅速に行うため、最新のデータを使用したレポートを自動的に生成できます。また、ダッシュボードやレポートをカスタマイズしたり、組み込みの適用除外を管理できます。適用除外はMcAfee ePOで専用のインターフェースが用意されていますが、McAfee Policy AuditorのテンプレートはMcAfee ePOのレポートインターフェースに統合されています。

統合で管理とレポート作成が簡単に

McAfeeのセキュリティエコシステムで重要なコンポーネントであるMcAfee ePOでは、セキュリティとコンプライアンスの管理を1つのコンソールで行うことができます。これにより、煩雑な作業がなくなり、コストを大幅に削減できます。McAfee Policy AuditorとMcAfee ePOの統合により、評価作業の生産性が向上します。McAfee ePOコンソールで内部ま

たは外部のポリシーベンチマークを定義し、これらのベンチマークを選択することで様々な資産タイプを評価できます。監査にかかる時間を短縮するだけでなく、すべての資産の状況を1つのレポートで報告できます。セキュリティ構成、パッチの適用、コンプライアンスの状況を1つのコンソールで確認できるので、全体のセキュリティ状況を迅速に把握することができます。

McAfeeテクノロジーの機能はシステム構成に依存します。機能を十分に活用するため、対応のハードウェア、ソフトウェア、サービスの利用が必要になる場合があります。詳細については、www.mcafee.com/jp をご覧ください。絶対に安全なコンピューターシステムはありません。



〒150-0043
東京都渋谷区道玄坂1-12-1
渋谷マークシティ ウエスト20F
Tel. 03-5428-1100 (代表)
www.mcafee.com/jp

McAfee、McAfeeのロゴ、ePolicy Orchestrator、McAfee ePOは米国法人McAfee, LLC または米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2018 McAfee, LLC. 3895_0418
2018年4月