

チェック・ポイントのデータセンター・セキュリティがもたらす効果

コスト、管理、法令遵守面でのメリットを提供

課題

近年、大規模企業のIT部門は、データ・センターにおけるコスト構造の改善と運用効率の向上に関して、大きな成果を上げています。こうした取り組みが行われる背景には、サーバおよびストレージの高性能化・大容量化を求める際限のない要求に応えると同時に、それに伴うハードウェア・コストおよび電気料金、設置スペースに関する費用、管理労力などを含む運用コストの増大を抑制することが強く求められているという事情があります。また、法令遵守とセキュリティ監査対応を促進するため、全社レベルでのIT統制を強化し、その可視性を高めることを目的としているケースもあります。こうした目的を達成するためにIT部門が採用したのは、データ・センター拠点の集約、サーバおよびストレージの統合と仮想化、IT機能および監視機能の集中化、標準化によるベンダー/製品/IT管理ツールの絞り込みといった手法でした。プロジェクトを成功に導くことのできた組織では、これらの手法は大きな効果を生み、ROIの面でも明確な成果を上げています。

その一方、各種の脆弱性や攻撃からデータ・センターを保護することの重要性も、この数年でますます大きくなってきています。しかし残念ながら、データ・センターにおける多くのIT投資は、同じようなIT目標を追求しながら、セキュリティの信頼性向上とコストの削減を両立できずにいるのが現状です。実際のところ、セキュリティ問題に直接対処しようとしていないIT統合/仮想化プロジェクトは、データ・センターの保護をより脆弱に、より非効率にしてしまう恐れすらあります。データ・センターにおけるIT投資にセキュリティ・コンポーネントを組み込むにあたっては、データ・センター環境に最適な信頼性のあるセキュリティ機能と、大規模な分散ネットワーク環境向けの効率的な管理ツールを備えた、標準技術に基づくソリューションを選択することが課題になります。

解決策

チェック・ポイントが提供する、データ・センター向けセキュリティ・ソリューションは、データ・センターにおける多くのIT投資と同様のコスト、管理、および法令遵守面でのメリットを、セキュリティについても享受できるように支援します。データ・センターのセキュリティを向上させるために使用される集中化、統合化、仮想化、標準化といった技術や手法は、多くの一般的なITプロジェクトで用いられる技術・手法と共通であるため、データ・センター・プロジェクトにチェック・ポイントのデータ・センター向けセキュリティ・ソリューションを追加することで、プロジェクトの効果とROIをさらに向上させることができます。

チェック・ポイントのソリューションは、各国で事業を展開するグローバル企業や、複数の事業部門または拠点を持つ企業のニーズに応えられるように設計されています。特に、ファイアウォールやVPN、侵入防御(IPS)といった機能を提供するゲートウェイを多数導入し、それらが増え続けているような企業では、チェック・ポイントのソリューションを導入することで大きな効果が得られます。また、インターネットに接続されるサービス(リモート・アクセス、エクストラネット、各種のコンシューマ向けアプリケーションなど)の増加や、これらを少数のデータ・センターに集約することに伴って、ファイアウォールのルールが肥大化・複雑化している大規模企業においても、チェック・ポイントのセキュリティ・ソリューションは大きなメリットをもたらします。

ソリューションの概要

チェック・ポイントのデータ・センター向けセキュリティ・ソリューションは、大規模企業がデータ・センターに対するIT投資によって得ているメリットと同様の—コストおよび複雑さの軽減、法令遵守の促進、資産管理の強化—を、セキュリティ面でも享受できるようにします。

ソリューションの特徴

- マルチ・ドメインに対応した集中的なセキュリティ・ポリシー管理
- セキュリティ・ゲートウェイおよびネットワーク・デバイスを統合化・仮想化
- セキュリティ・イベントのロギング、相関分析、レポート、および分析を集中化
- すべてのセキュリティ機能を、標準化された方法によりマルチ・ティアで管理

ソリューションのメリット

- セキュリティ・デバイスのハードウェア・コストおよび運用コストを削減
- 管理性、可視性、法令遵守対応を改善
- データ・センターにおけるセキュリティの信頼性、効率性、ポリシーの一貫性を向上
- 法令遵守対応を強化しつつ、インシデントへ対応するために必要な時間を短縮
- SmartDefense™サービスにより、最新の脅威にも対応

データセンター向けに設計された統合セキュリティ

チェック・ポイントが提供する包括的なデータ・センター向けセキュリティ・ソリューションは、次の4つの要素で構成されています。

- **管理機能：**企業ネットワークのファイアウォール/VPN/IPSゲートウェイを、その数や設置場所にかかわらず、マルチ・ティア/マルチ・ドメインですべて集中管理
- **仮想化機能：**関連するネットワーク・デバイスと共に、ファイアウォール/VPN/IPSゲートウェイを仮想化
- **ロギング/分析/レポート機能：**ネットワークおよびエンドポイントにおけるセキュリティ・イベントを、企業全体にわたって継続的・自動的にロギング、分析およびレポート。分析に必要なデータは、ベンダー各社の多様なネットワーク・デバイスおよびセキュリティ・デバイスから収集可能
- **コンサルティング・サービスおよび導入支援サービス：**チェック・ポイントが認定したセキュリティ専門の販売代理店またはベンダーが、データ・センター・セキュリティに関するコンサルティング・サービスおよび導入支援サービスを提供

これら4つのソリューション・コンポーネントをすべて組み合わせることにより、最大限の導入効果が得られます。ただし、各コンポーネントは段階的に導入することも可能です。ソリューション・コンポーネントを1つまたは2つ導入するだけでも、運用面およびコスト面で大きなメリットが得られます。したがって、必ずしもこれらのコンポーネントを一度に全面展開する必要はありません。

管理の統合化・集中化

データ・センターに対するIT投資のうち、特に大きなメリットが得られるのは、分散配置されたITリソースの管理を集中化するための投資です。この集中化が重要であるのは、チェック・ポイントのデータ・センター向けセキュリティ・ソリューションにおいても同様です。チェック・ポイントのセキュリティ・ソリューションでは、管理製品のProvider-1®が提供する集中管理コンポーネントを使用することで、1つの中心的なIT/セキュリティ・チームが、全ゲートウェイ(物理ゲートウェイ、仮想ゲートウェイ、ローカル・ゲートウェイ、リモート・ゲートウェイ)のファイアウォール/VPN/IPSポリシー(ポリシー・コンポーネント)を定義および実施できるようになります。マルチ・ドメインに対応した管理により、部門などの組織ごとに分割された各ドメインのセキュリティ・ポリシー、ログ、およびデータベースは、例えそれらが単一の共有ハードウェア上で管理されている場合でも、他のドメインからは完全に分離されます。また、マルチ・ティア/ロール・ベースの管理アカウントにより、階層型のポリシー制御と権限の分担が可能になり、これによって、管理者以外の方(ヘルプデスク担当者や監査担当者など)に、セキュリティ・データに対する適切なレベルのアクセス権を容易に付与できるようになります。さらに、支社・支店などのリモート・サイトの管理者に対し、ローカルのゲートウェイおよびポリシーを管理するための管理権限を与えることも可能です。

データ・センターのセキュリティが集中管理可能になることには、効率性や拡張性が向上すること以外にもいくつかのメリットがあります。その一つとして、セキュリティ・ポリシー自体と、企業全体におけるその実施状況に対する可視性(および管理性)が向上するという点が挙げられます。これにより、リモート・サイトでのポリシー実施に関する信頼性と一貫性が大幅に向上すると共に、重要なITサービスおよびデータのためのビジネス継続性維持/ディザスタ・リカバリの仕組みが正しく導入されているかどうかを、セキュリティ担当者がどこからでも確認できるようになります。また、ポリシー管理やレポートといった、複雑なセキュリティ環境の管理作業を集中化することは、機密情報を保護するために企業が従う必要のある法規制およびセキュリティ監査要件を遵守するうえでも大きな役割を果たします。

ハードウェアの統合化・仮想化

チェック・ポイントのデータ・センター向けセキュリティ・ソリューションでは、仮想化技術を用いることにより、単一のハードウェア上で最大250台分のセキュリティ・ゲートウェイ、スイッチ、およびルータを実行することが可能です。これは、物理デバイスを最大249台減らすことができるということを示します。これらの仮想システムはブリッジ・モードで動作させることもできるため、既存のセキュリティ・デバイスをチェック・ポイントのセキュリティ仮想化コンポーネントであるVPN-1® Power VSX™に置き換える際、ネットワーク設定やトポロジはほとんど変更せずに済みます。このVPN-1 Power VSXは先進のクラスタリング技術を搭載しており、ノンストップの運用を可能にする可用性と共に、最も効率性と拡張性に優れた仮想セキュリティをデータ・センター環境に提供します。VPN-1 Power VSXは、キャリア・グレードの複数種類のハードウェア・プラットフォームで稼働し、ギガビット・クラスの通信速度で動作させることが可能です。

ストレージやオペレーティング・システムの仮想化と同様、このセキュリティの仮想化においても、さまざまな面で大幅なコスト削減を見込むことができます。例えば、現在および将来のセキュリティ・ハードウェアに対する投資や保守/アップグレード・コストの削減、セキュリティ機器や空調設備による電力消費量の低減、データ・センターの設置スペースに関する費用の削減、そして管理コストの削減といった効果を得ることができます。またセキュリティの仮想化に伴う省エネルギー効果は、社会的にも大きなメリットとなります。

チェック・ポイントのセキュリティ仮想化ソリューションが提供するメリットは、コスト削減に留まりません。例えば、フル機能のファイアウォール、VPN、およびIPSを備えた仮想セキュリティ・ゲートウェイは、物理ゲートウェイよりも素早く簡単にプロビジョニングすることができます。データ・センターにおいてセキュリティ機能を迅速にプロビジョニングできるということは、新しいビジネス・プロジェクトに素早く対応できるということでもあります。さらに、これらの仮想セキュリティ・ゲートウェイは、物理的なファイアウォール/VPN製品として世界的に定評のある、チェック・ポイントのVPN-1が提供するセキュリティ技術をベースとしており、その信頼性の高さはほかを圧倒しています。

レポート、分析、インシデント・レスポンスの集中化

法令遵守や監査対応を最大限に支援するため、チェック・ポイントでは、イベント管理、レポート、および分析の機能を集約し、セキュリティ・ソリューションの集中ポリシー管理機能と統合しています。Eventia Reporter™は、チェック・ポイントの各種ネットワークおよびエンドポイント・セキュリティ製品から膨大な量のログ情報を収集し、これを実用的でグラフィカルなサマリーおよび傾向分析レポートに変換するコンポーネントです。カスタマイズ可能で監査用途にも対応するこのレポートは、ネットワーク・セグメント・レベルからネットワーク全体のレベルまで出力レベルを変更できるため、データ・センターのプランニングからインシデント・レスポンス、法令遵守の検証にまで効果的に活用することができます。またレポートの生成と配布をスケジューリングして自動化すると、これら重要な機能をより効率的に利用することが可能になります。企業全体にわたるこの集中レポート機能は、セキュリティ担当者が、データ・センターに対するセキュリティ投資の必要性和妥当性を経営幹部に説明する際にも役立ちます。

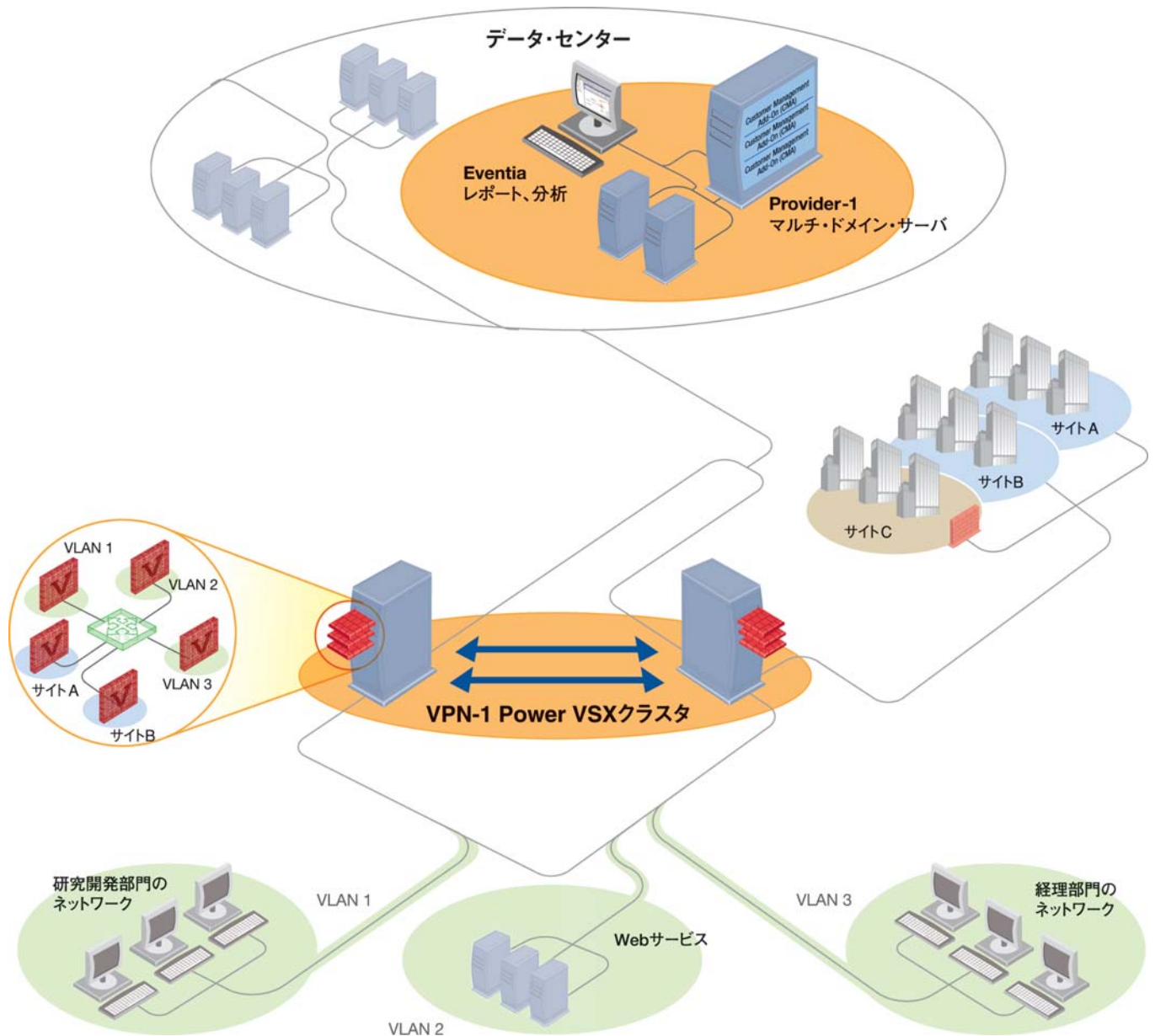
ITアプリケーションを大規模なデータ・センターに集約すればするほど、それに伴ってインシデント・レスポンスの迅速さが求められることとなります。チェック・ポイントのデータ・センター向けセキュリティ・ソリューションでは、このニーズに応えるために、チェック・ポイントのセキュリティ・ソリューション、およびサードパーティのセキュリティ製品、ネットワーク製品、IT製品が日々生成する何百万件ものログ・レコードを集計し、相関分析を

行います。Eventia Analyzer™は、攻撃パターンを検出すると、それが本当の脅威であるかどうかを判別し、優先順位を付けてから、設定に応じて管理者に通知するか自動的に対応策を実施します。このように、大量のセキュリティ・イベントをリアルタイムで自動的に処理することにより、データ・センターの保護が強化され、手動でデータ分析を行うことによるコストと煩雑さが軽減されます。また、競合他社のセキュリティ情報/セキュリティ・イベント管理製品では、何人もの管理者やコンサルタントが1年ほどかけてチューニングすることが必要になる場合もありますが、チェック・ポイントのソリューションは、最小限の導入作業ですぐに効果が出せるように設計されています。

ソリューションの導入効果の最大化

データ・センターへのセキュリティ・ソリューションの導入効果を最大化するには、情報セキュリティ・インフラストラクチャをチェック・ポイントの

ソリューションで標準化することが重要です。チェック・ポイントのデータ・センター向けセキュリティ・ソリューションを構成する各コンポーネントは、それ単体でもセキュリティの信頼性と管理効率の向上に大きく貢献します。しかし、チェック・ポイントのNGX統一セキュリティ/管理アーキテクチャを共通基盤とするこれらのコンポーネントは、相互に連携し動作することによって、個々の総和よりもさらに大きな相乗効果をもたらします。統一されたインフラストラクチャは、組織全体でセキュリティ・ポリシーの一貫性を保ち、各防御システム間の隙間を埋め、管理業務を簡素化することを可能にします。こうしたことは、断片的なセキュリティ技術をただつなぎ合わせるだけでは決して実現することができません。重要性の高い情報リソースを確実に保護するためには、チェック・ポイントのように、セキュリティのみに注力する専門ベンダーが提供するソリューションが不可欠です。データ・センターへのIT投資にセキュリティを組み込むことが、その効果とROIをどれだけ向上させるか—詳細については、チェック・ポイントの製品取り扱い代理店までお問い合わせください。



この図は、チェック・ポイントのデータセンター向けセキュリティ・ソリューションの概念図です。この図では、Provider-1が、ローカル・サイトとリモート・サイトに設置されたすべての物理VPN-1ゲートウェイとVPN-1 Power VSX仮想システムの管理を行い、Eventia Suiteが、すべてのドメインで発生したイベントのレポートと分析を集中的に行います。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおけるトップ企業として、世界中の企業向けファイアウォール、パーソナル・ファイアウォール、データ・セキュリティおよびVPN市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理ソリューションを含む広範囲なポートフォリオにより、ITセキュリティへのPUREなフォーカスを実現します。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、リモート・ユーザ、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースに対する広範なセキュリティ保護を実現する、統一されたセキュリティ・アーキテクチャを提供しています。更にチェック・ポイントは、業界をリードするデータ・セキュリティ・ソリューションである、PointSec製品ラインナップを通じ、PCやモバイル端末に保存してある各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界中のパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F

<http://www.checkpoint.co.jp/> E-mail : info_jp@checkpoint.com Tel : 03 (5367) 2500