

Symantec™ DeepSight™ Threat Management System

新たな攻撃や脅威などの最新情報を提供する早期警告サービス

セキュリティ技術のみに頼る対策では、日々次々と報告されている脆弱性や新たな脅威やリスクから企業の情報資産を確実に守ることが困難になっています。強力な情報セキュリティを実現するためには、技術、プロセス、人材、情報の全てを効果的に連携させて取り組むことが必要となりました。

製品の概要

Symantec DeepSight Threat Management Systemは、世界のどこかで今まさに行われている攻撃や潜在的な脅威、重大な脆弱性に関する最新情報を早期に提供することにより、企業におけるセキュリティ施策を強化します。

このサービスは、アラート（用途に応じてカスタマイズ可能）や対応策の決定をサポートする的確な情報を提供します。これらの情報は脅威およびリスクに対する熟達した分析に裏打ちされているため、管理者はより正確かつ効率的に潜在的なリスクへの対策を行うことが可能になります。

〈キーポイント〉

- 180か国40,000箇所以上に設置されたセンサーおよびシマンテック独自の情報源など、世界中に広がる膨大な情報源を活用し、グローバルな視点でセキュリティインシデント情報を収集して分析。結果にもとづき、詳細なアラートをタイムリーに発信
- 8,000社50,000を超えるテクノロジーおよび製品とそのバージョンに関する脆弱性アラートを発信
- 的確な情報をもとに、ユーザーはより効果的な対応アクションを実行することが可能
- 管理するネットワーク環境に応じ、アラート発信の自動化とレポート生成の詳細設定をカスタマイズ可能
- スパイウェアとアドウェアについてのアラートおよびコードの挙動に関する技術的解説などを含む警告情報を配信
- 悪意あるコードのペイロードに特定のドメイン名が存在する場合、ドメイン攻撃のアラートを通知
- 世界をリードするインターネットセキュリティ専門機関Symantec Security Responseによる信頼のバックアップ

製品の特長とベネフィット

最新情報とそれにもとづく適切な対応策により、プロアクティブに防御

Symantec DeepSight Threat Management Systemは、攻撃に関する早期警戒情報やシステムおよびネットワーク環境に関係する脆弱性/悪意のあるコードなどの情報を、ユーザーの企業ネットワークにインパクトが及ぶ前に発信します。また、悪意のあるコードのペイロードに特定のドメイン名が存在する場合はDoS攻撃などのドメインに対する攻撃としてアラートを通知します。これらの情報により、管理者はネットワークをプロアクティブに保護し、ビジネスの停止、生産性の低下、企業の社会的信頼の喪失といった被害を未然に防ぐことができます。

Symantec DeepSight Threat Management Systemのユーザーには、自動化されたアラート発信とWebサイトを通じて、攻撃や脆弱性に関する詳細かつ統計的に信頼性が高い情報が提供されます。また、提供される情報に対しては、時刻、国、その他のパラメータによって、トラッキングを行うことも可能です。バッチ、対抗措置、代替策等に関する具体的な情報も提供されるため、ユーザーは即座に対策を講じることができます。

情報セキュリティのリソースの活用を、さまざまな面で最適化

Symantec DeepSight Threat Management Systemを利用することにより、企業の情報セキュリティ担当者は、攻撃からの防御に専念することができます。まず、事前情報とプロアクティブな対処を行うための情報によって、自社のネットワークに被害が及ばないように最適な対抗措置を講じることができます。情報収集のためのWeb上での検索や電子メールのチェックに要する時間を削減することにより、業務の円滑な遂行を図る一方で、情報セキュリティ関連のリソースを最適化することができます。

迅速なアラート発信

異常なアクティビティや悪意のある行為が発見された場合には、1時間以内に、悪意のあるコードと脅威に関するアラートを発信します。これらのアラートには、対応方法やバッチに関する情報のほか、詳細な技術解説も含まれています。アラート発信に関する詳細設定は、各企業のネットワークやシステム、ソフトウェアの構成/設定に応じて、容易にカスタマイズすることができます。

包括的なレポート

脅威に関する分析レポートでは、攻撃内容とその発信源、被害が及んだ範囲、インパクトを緩和する要素、防御方法の詳細等を解説します。また、セキュリティ管理者と経営者の双方を対象としたサマリーを、日/週/月単位で提供し、攻撃、脆弱性、期間中の発生インシデントの傾向をレポートします。管理者は、それらをベースに、広範にわたる攻撃手法のカテゴリーや詳細なパラメータを調べるなど、さらなる独自の分析を容易に行うことができます。

インターネット上のセキュリティ状況を一望

Symantec DeepSight Threat Management Systemは、IDSとファイアウォールのイベントについてのクイックビュー等のコンテンツを通じ、インターネット上におけるセキュリティ状況をリアルタイムで提供します。また、世界中で行われている攻撃に関するさまざまな詳細情報（発生頻度、国、IPアドレス、ポート、関連製品など）も提供します。さらに、Symantec Analyst Watch ページでは、シマンテックのセキュリティアナリストによる独自のコンテンツ（現在最も注視すべきであると判断されるホットスポットの情報等）も提供されます。

Symantec Security Response によるバックアップ

Symantec DeepSight Threat Management Systemは、Symantec Security Response によってサポートされ、24時間365日絶えることなく、よりタイムリーに、かつ充実した情報提供を行っています。

Symantec Security Responseは、グローバルに展開するインターネットセキュリティ全般に関するリサーチチームとテクニカルサポートチームで構成されており、ウイルスやワームなどの悪意のあるプログラム、不正侵入の手法、OSやアプリケーションの脆弱性とそれを利用した攻撃方法などに関する調査/研究、また、それにもとづくシマンテック製品のバックアップを行っています。

システム要件

- Microsoft Internet Explorer 6.0 以降、または Firefox 1.5 以降（それぞれ、Cookie、JavaScript、SSLを利用できるように設定してあること）
- Adobe Acrobat Reader 5.0 以降（アラートやレポートの閲覧用）
- 電子メールアドレス（アラートやレポートの受信用）

製品に関する最新の情報

シマンテックのWebサイトをご覧ください。

<http://www.symantec.com/jp/enterprise>