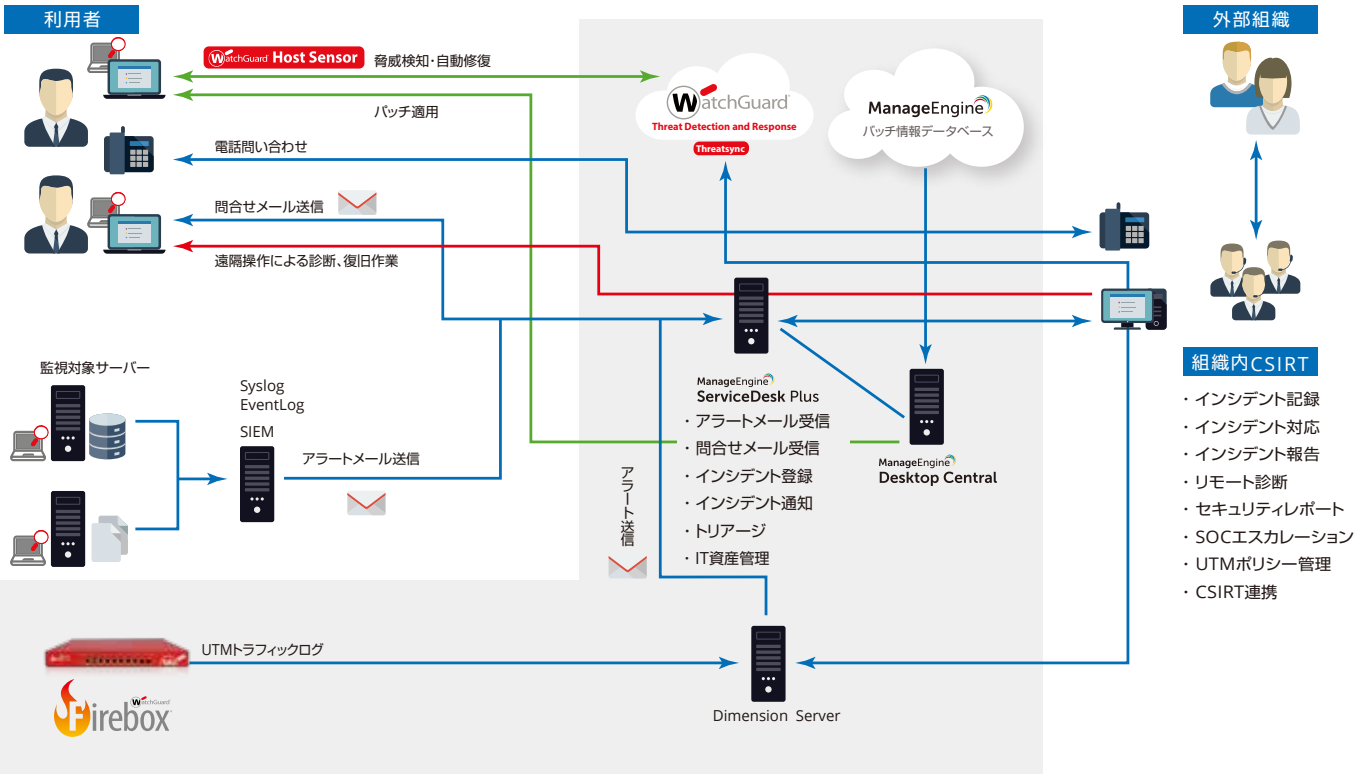
組織内CSIRT

インシデント管理ソリューション



CSIRT（Computer Security Incident Response Team、シーサート）は、情報セキュリティインシデント（以下、インシデント）に関する事象やシステム・ソフトウェアの脆弱性情報を収集・分析し、攻撃予兆を把握するとともに、インシデント発生時の対応方針や手順の策定を実施する組織です。初動対応を誤れば経営危機にも発展しかねないインシデントの発生に備えて、今、企業内に組織内CSIRTを構築する企業が増加しています。

組織内CSIRT向けインシデント管理ソリューション「ServiceDesk Plus CSIRTモデル」は、ゾーホージャパンが提供するITサービスマネジメントツール「ServiceDesk Plus」を情報基盤とした、組織内 CSIRTの事前対応型サービスと事後対応型サービスの一元管理を導入しやすい価格で実現する包括的なソリューションです。セキュリティ脅威の防御からインシデント検知後のトリアージまでに発生する報告や分類といったインシデント管理における非効率な手作業を減らすことで、迅速に解決すべきインシデントへの対応力を高めます。事前対応型サービスとして本ソリューションは、ウォッチガード・テクノロジー・ジャパンの統合セキュリティアプライアンス「Fireboxシリーズ」によるセキュリティ脅威の検知と防御、膨大なセキュリティログデータをセキュリティ対策に有効なインテリジェンスへ変換して監視・管理を実現する「WatchGuard Dimension」を提供します。

さらにクライアント端末の脆弱性パッチ管理を行うためのゾーホージャパンのクライアント管理ツール「Desktop Central」の利用が可能です。これらのサービスを提供することで組織内CSIRTはコンスティチュエンシー（CSIRTサービス対象者）が安心して利用できるネットワーク・システムを提供できるようになります。事後対応型サービスでは、「WatchGuard Dimension」から出力されたアラート情報を「ServiceDesk Plus」にインシデントとして取り込み、分類、脅威の優先度付けまでの自動化を実現します。また「ServiceDesk Plus」のIT資産管理機能と「Desktop Central」のクライアント管理機能の連携により、インシデントが影響を及ぼす可能性のあるビジネスサービスの特定を早めるだけではなく、組織内CSIRTと外部連携しているSOCやセキュリティベンダーとの容易な情報共有を可能にします。

初年度ライセンス参考価格

導入支援サービスをご希望の方は別途ご相談ください。

3,446,000円

【参考価格内訳】

ManageEngine ServiceDesk Plus Professional Edition 5オペレーター（250 nodes）年間ライセンス
ManageEngine Desktop Central Enterprise Edition 250コンピューター&1ユーザー 年間ライセンス
WatchGuard Firebox M500本体+Total Security Suite 1年ライセンス

セキュリティインシデント対応スキーム

防 御

- Desktop Centralによる脆弱性パッチ対策
- WatchGuard FireBoxによる多層防御
- Dimensionによるインシデント検知、レポート
- Thread Detection & Response による脅威検知と自動防御

検知・記録

- ServiceDesk Plusによるインシデント管理
  - 問い合わせの受付
  - アラート受信
  - 分類・優先度付け
- Dimensionによるアラート情報の保管

分析・対応・連携

- 状況の把握・分析
  - Desktop Centralを用いたIT部門からのリモート対応
  - SOCによるインシデント詳細分析
- 情報と対応の調整
  - ServiceDesk Plusからの情報発信
- 対応計画の策定
  - ServiceDesk Plusへの対応計画の記録
  - ServiceDesk Plusでのタスクの割り振り
- 対応・抑制措置
  - ServiceDesk Plusへの対応履歴の記録
  - IT部門によるポリシー変更
  - SOCによる事前・事後対応

クローズ

注意喚起・報告

- ServiceDesk Plusを用いた一斉アナウンス
- 関係機関へのエスカレーション

CSIRTモデル対応製品紹介

ManageEngine
ServiceDesk Plus

インシデントの進捗管理に利用可能なITサービスマネジメントツールです。進捗の主な流れである、受付→トリアージ→対処策の検討・実行→インシデントのクローズをツール上で管理できます。インシデントごとの優先度を素早く把握できる仕組みをCSIRTに提供し、深刻な脆弱性の公開などにより複数のインシデントに同時対応しなければならない場合の進捗管理を効率化します。

ManageEngine
Desktop Central

ランサムウェア対策の基本である脆弱性パッチ管理機能を中心とするクライアント管理ツールです。ネットワーク内にあるWindows & Mac OSの他、Adobeなどのサードパーティー製アプリにも最新パッチを適用し、端末の脆弱性を狙う攻撃を防止します。またリモートコントロール機能により、遠隔地にあるインシデント発生の可能性がある端末の状況確認などが容易になります。

WatchGuard
Firebox & Total Security Suite※

統合型セキュリティアプライアンスと完全なセキュリティパッケージにより、ランサムウェアや標的型攻撃などのネットワーク上のあらゆる脅威の検知、防御、相関分析によるセキュリティ対策を提供します。Total Security Suiteは、不正侵入検知・防御、ゲートウェイアンチウイルス、アプリケーション制御、スパム対策、Webフィルタリング、クラウド型サンドボックスが含まれ、既存の脅威だけでなく、未知のマルウェアやランサムウェアの脅威、機密データの保護を実現します。また、このパッケージには、ネットワークセキュリティの可視化・管理ツールや最新のエンドポイント(Host Sensor)と連携するThreat Detection & Responseが標準で含まれています。

※ WatchGuard Firebox、Total Security Suiteは、ウォッチガード・テクノロジー・ジャパン社が提供するアプライアンス及びサービスです。

株式会社ネットブレインズ

〒104-0044　東京都中央区明石町6-22 築地ニッコンビル 4階
担当:ソリューション事業部　セキュアソリューション営業部
Tel: 03-5550-6370
Email: sol_sales@netbrains.co.jp
URL: https://www.netbrains.co.jp/

NB-17-06-001