セキュリティのノウハウと実績をベースに開発した

日立のサイバー攻撃対策ソリューション

マルウェアを介してのデータ破壊や改ざん、システムダウンなどを発生させる標的型サイバー攻撃の被害が世界中で急増しています。日立のサイバー攻撃対策ソリューションでは、こうした攻撃に対処する多層防御の一環として、侵入したマルウェア攻撃を自動的に検知する「拡散活動検知ソフトウェア」と、高優先度のアラートを自動抽出して業務を効率化する「脅威分析ソフトウェア」を開発。攻撃者から大切な情報資産を守り、企業や社会の安全・安心に貢献します。

拡散活動を防止する内部対策を強化

巧妙な手口のサイバー攻撃に対処するためには、組織や情報システムの特性に合わせ、攻撃の各段階に対応する製品の組み合わせで多面的に守る“多層防御”の考え方が重要です。基本的には、マルウェアのシステムへの侵入を防ぐ入口対策、侵入後に情報を探して端末やサーバを渡り歩く拡散活動を防止する内部対策、守りたい情報資産にアクセスされても実被害につながることを防ぐ出口対策から多層防御は構成されます。

これまでは入口・出口対策に向けた製品開発が主流でしたが、日々巧妙化する標的型サイバー攻撃を高い精度で検知し続けるためには、専門家による継続的な定義ファイルの更新やポリシーチューニングが求められるため、運用上大きな負担となっていました。

そこで日立は、システムの多層防御を強化する内部対策製品に着目。日立が長年にわたり培ったセキュリティノウハウと実績を生かし、専門家の継続的なメンテナンス作業を必要とせず、情報システム内に侵入したマルウェア攻撃を自動検知する「拡散活動検知ソフトウェア」を開発しました。

侵入を防げない時代に対応した「拡散活動検知ソフトウェア」

標的型攻撃によって、攻撃者はさまざまな障壁を突破してシステムに侵入します。攻撃手法が巧妙化している現在、侵入後から重要情報を持ち出すまでに発見することが必要です。拡散活動検知ソフトウェアを活用すれば、セキュリティの専門家がいない場合でも、侵入したマルウェアの標的型サイバー攻撃を検知し、大切な情報資産を攻撃者から守ることが可能です（図1）。

■独自エンジンで拡散活動を検知し、自動的に対処

日立が開発した機械学習型エンジンが、各端末での正常なユーザーの挙動を学習し、ホワイトリスト※1を自動作成し、攻撃者の挙動との違いを分析することで、異常を検知します。また、攻撃拡散分析エンジンが複数端末の挙動を俯瞰（ふかん）して監視することで、検知精度を向上し、誤検知による運用負荷の増加を防止。これにより、最新のマルウェア情報を用いずに、巧妙な攻撃手法を用いた標的型サイバー攻撃などに対しても高い精度での攻撃検知率を実現します。

※1 通信を許可するリスト

■日立グループ製品と連携したトータルソリューションを提供

拡散活動検知ソフトウェアは、ホワイトリスト機能を搭載した小型アプライアン

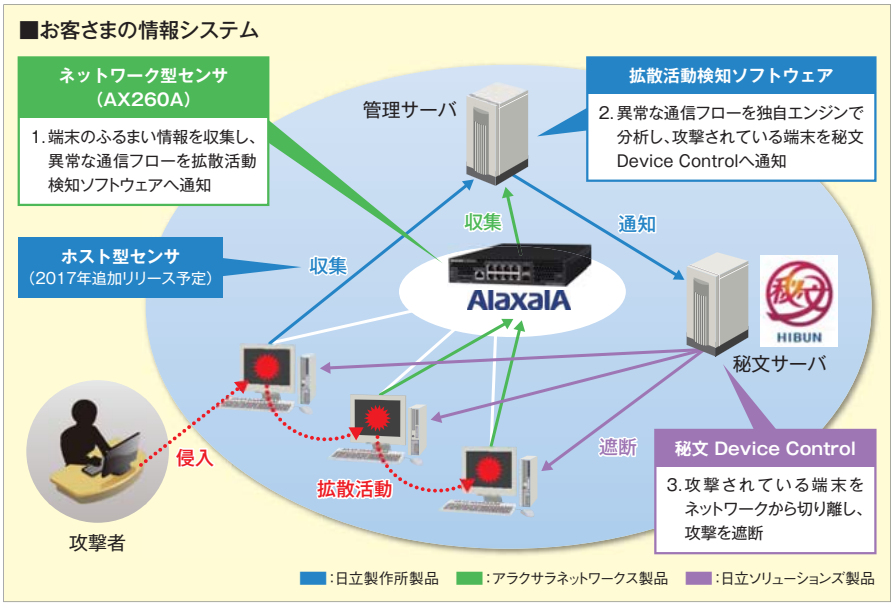

図1「拡散活動検知ソフトウェア」の概要

ス「AX260A」(アラクサラネットワークス株式会社)および情報漏えい防止ソフトウェア「秘文Device Control」(株式会社 日立ソリューションズ)と連携したソリューションとしても提供可能です。

AX260Aはホワイトリストに登録されていない異常な通信フローを検出して拡散活動検知ソフトウェアへ送信するため、情報システム内の端末にエージェントソフトウェアなどのインストールをすることなく標的型サイバー攻撃を検知できます。また秘文 Device Controlは拡散活動検知ソフトウェアからの検知情報を受信すると、攻撃の起点となっている端末をネットワークから切り離し、攻撃者が重要情報を持ち出す前に攻撃を頓挫させることにより、お客さまの大切な情報資産を守ります。

SOC運用の効率化を実現する「脅威分析ソフトウェア」

セキュリティ対策現場における運用効率向上も重要な課題の一つです。ますます高度化するサイバー攻撃に対抗するため、セキュリティ装置やサーバのログを監視し、インシデントを発見するSecurity Operation Center(以下、SOC)という専門組織を立ち上げる企業が増えています。SOCでは一般的にIntrusion Detection System(以下、IDS)と呼ばれる不正侵入検知システムを使ってサイバー攻撃を検知していますが、IDSから日々大量のアラートが着信するため、その確認や優先度判断などで対処に時間がかかり、運用者の負担も大きいことが課題となっています。

そこで日立が開発したのが、IDS検知イベントを詳細に分析し、優先度判断を効率化する「脅威分析ソフトウェア」です(図2)。

■優先度の高いイベントを自動抽出

対象となる業務システムの構成情報を取得後、IDS検知イベントと業務システムのぜい弱性情報の照合結果に基づき、被害につながる可能性のある検知イベントを自動抽出します。

■運用負荷を低減

イベント情報をIDSのCVE(Common Vulnerabilities and Exposures)番号※2に基づき、業務システムのぜい弱性情報と照合します。そしてIDSが潜在的な脅威発見のために積極的に発するアラートの中から、優先度の高いイベントを自動抽出することで、分析・対処業務を効率化します。

※2 さまざまなソフトウェアのぜい弱性を報告・登録される際に付与される識別番号

■業務システムへの影響を最小化

脅威分析ソフトウェアを利用する際には、システム構成情報を取得するためのエージェントソフトウェアをインストールする必要がありません。これにより監視対象業務システムに対する影響を最小化します。

これらの特長により、導入済みのIDSを最大限に活用しながら、優先度の高いイベントの対処に迅速に着手できる環境を整備することで、SOC運用の効率化に貢献します。

今後も日立は、安全・安心に関わる幅広い技術と経験を生かし、社会インフラ全体のセキュリティを強化するサイバー攻撃に対するソリューションを開発・提供していきます。

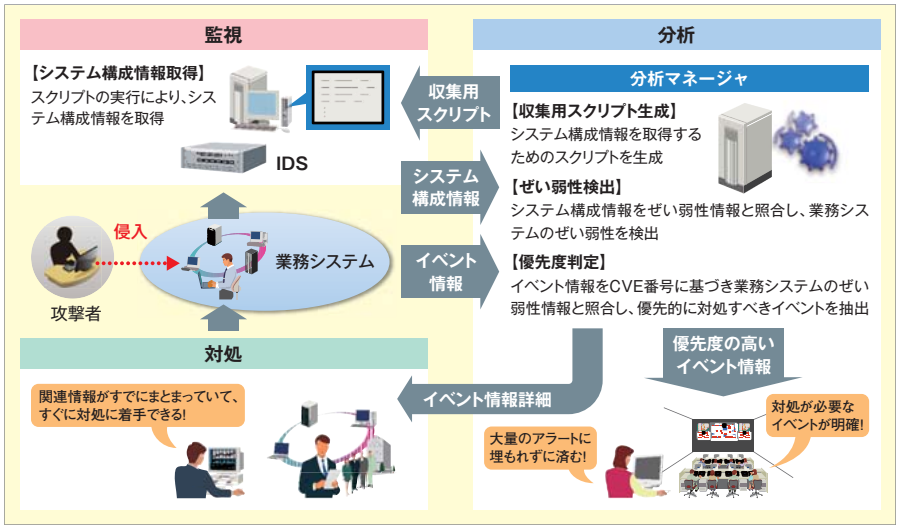

図2「脅威分析ソフトウェア」の概要

お問い合わせ先

(株)日立製作所 ディフェンスビジネスユニット
https://www8.hitachi.co.jp/inquiry/hitachi-ds/cybersecurity/form.jsp