2016 年 12 月 22 日
株式会社日立製作所

標的型サイバー攻撃の不審な活動を検知する「拡散活動検知ソフトウェア」の機能追加

仮想化環境への適用や統合システム運用管理「JP1」との連携強化

株式会社日立製作所(執行役社長兼 CEO:東原 敏昭／以下、日立)は、情報システム内における標的型サイバー攻撃の拡散を検知することができる「拡散活動検知ソフトウェア」の機能を強化し、2017 年 1 月 31 日より販売開始します。クラウド上のサーバやクライアント PC などの仮想化環境への適用や、ヴイエムウェア株式会社の「VMware NSX®」および日立の統合システム運用管理「JP1」との連携を強化するなど、「拡散活動検知ソフトウェア」の機能を強化しました。機能強化により、情報システム運用者の負担軽減や、幅広い業種への導入拡大、既存情報システムの管理環境と親和性を維持した効率的なセキュリティ対策が可能となります。

近年、高度化・巧妙化している標的型サイバー攻撃への対策は、企業にとって重要な経営課題となっています。企業ではセキュリティ対策の導入が進んでいますが、業務システムの刷新などにより、クラウド上の仮想化環境へのシステム移行が進み、仮想化環境に対応したセキュリティ対策が必要になっています。また、様々な運用管理ソリューションやセキュリティ対策ソリューションの導入により、運用が複雑化していることや、従来のセキュリティ対策を回避する高度なサイバー攻撃が出現し、さらにきめ細かく分析・対策が必要になるなどの課題があります。

そこで、日立は 2016 年 6 月より提供している「拡散活動検知ソフトウェア」の機能を強化し、これらの課題解決を支援します。具体的には、従来のネットワーク型センサ方式(アラクサラネットワークス社製「AX260A」と連携)に加え、新たに仮想化環境に対応したホスト型センサ方式(エージェントソフトウェア)を提供することで、様々な仮想化環境上においても標的型サイバー攻撃を検知することが可能になります。また、仮想化市場をリードするヴイエムウェア株式会社のネットワーク仮想化製品「VMware NSX®」のマイクロセグメンテーション機能と連携し、「拡散活動検知ソフトウェア」が攻撃を検知した仮想マシン(仮想 PC)を自動的に仮想ネットワークから隔離し、攻撃の影響を局所化できるようになります。さらに、「JP1」との連携により、日常の標的型サイバー攻撃監視業務の負担を軽減しつつ、万一のサイバー攻撃発生時には迅速な状況把握と対処することが可能になります。

また、日立は、「日立 - VMware コンピテンスセンター」に「VMware NSX®」の利用環境を新たに用意しました。これにより、「拡散活動検知ソフトウェア」や「JP1」も含め、導入前に動作検証できる環境を顧客へ提供します。

■「拡散活動検知ソフトウェア」の機能強化の特長

1. 仮想化環境上の情報システムで拡がる標的型サイバー攻撃を可視化、対処

仮想化環境上に構築したサーバやクライアント PC 上で動作するホスト型センサ(エージェントソフトウェア)が分析マネージャに情報を送信し、標的型サイバー攻撃を検知することができます。分析マネージャが備えているシンプルかつ直感的な画面により、標的型サイバー攻撃がいつ、どの端末から、どの経路で進入されたかを一目で把握できます。また、検知した結果は「VMware NSX®」に通知し、仮想ネットーク上のポリシーを自動変更することで、サイバー攻撃を受けた仮想化環境を隔離できます。

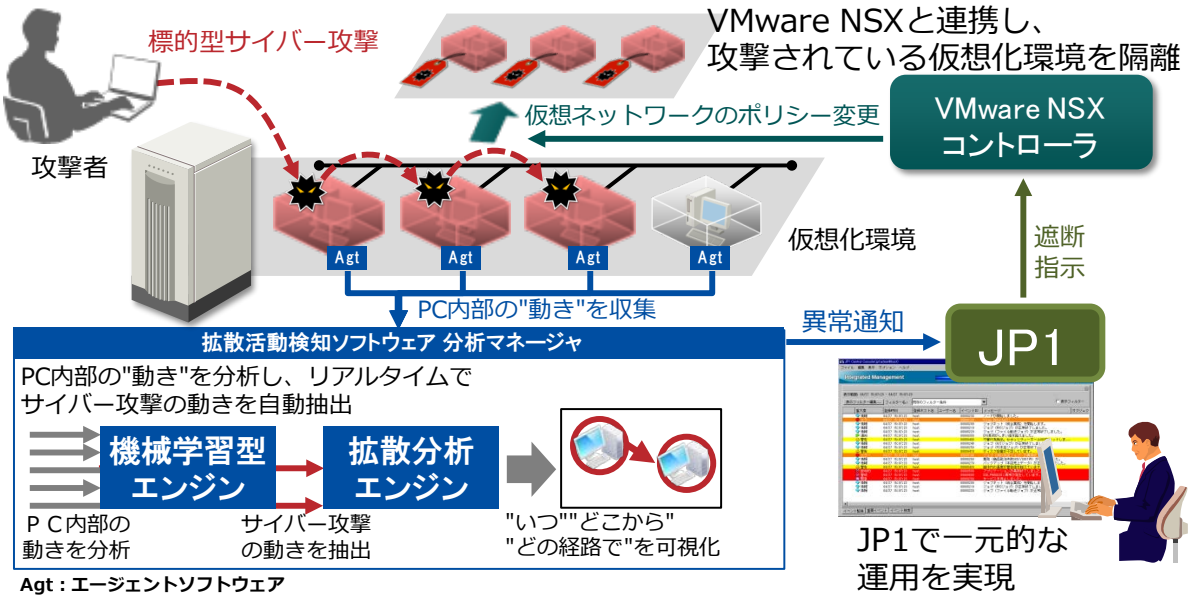
2.「JP1」との連携により更なる運用負荷軽減

国内運用管理ソフト市場で 19 年連続売上トップを継続する「JP1」と連携し、システム運用管理とセキュリティ対策運用の一元化による、情報システム運用者の負担軽減を実現します。「拡散活動検知ソフトウェア」は専門家による日常的なメンテナンスを必要としないことに加え、検知したサイバー攻撃の情報を JP1 統合管理「JP1/Integrated Management」で確認できるようになります。また、セキュリティ管理製品「JP1/秘文 Device Control」を活用することで、サイバー攻撃を受けたクライアント PC を物理ネットワークから隔離できます。

3. ホスト型センサによるきめ細かく高精度な監視

今回提供を開始するホスト型センサ方式(エージェントソフトウェア)は、従来から提供するネットワーク型センサ方式による通信監視のほか、サーバやクライアント PC 内部の動きを監視します。これにより、分析マネージャに搭載された機械型学習エンジンおよび攻撃拡散分析エンジンで分析可能な情報が増え、より微細な動きをするサイバー攻撃を検知することが可能となります。

■本製品の適用イメージ



■ヴイエムウェア株式会社 ストラテジックアカウントビジネス本部長 秋山 将人氏からのコメント

ヴイエムウェア株式会社は、日立製作所の「拡散活動検知ソフトウェア」の強化にともなう、「VMware NSX®」との連携の実装を歓迎いたします。

脅威動向が急速に変化する現状において、セキュアなネットワークの実現は急務となっています。この機能拡張により、お客様は標的型攻撃に対してより強固な防御を実現することができます。

ヴイエムウェアは今後も日立グループと更なる協調を進め、お客様のネットワークのすべての階層とすべての機能に必要不可欠な高いセキュリティを提供し、サイバー脅威に影響されることのないデジタルトランスフォーメーションの実現を推進してまいります。

■セミナー開催について

日立は今回発表した内容について、幅広いお客さまへ紹介するためにヴイエムウェア株式会社との共催によるセミナーを開催します。

・セミナー名　　:最新の仮想化技術と高精度な検知で、標的型サイバー攻撃を防御
・開催日時　　:1 回目:2016 年 12 月 27 日(火) 開催時間　15:00～17:00
　　2 回目:2017 年 2 月 14 日(火) 開催時間　15:00～17:00
・会場　　: 品川イーストワンタワー13F ハーモニアス・コンピテンス・センター
・申し込み URL　:1 回目 https://hjid.ext.hitachi.co.jp/public/seminar/view/1369
　　2 回目 https://hjid.ext.hitachi.co.jp/public/seminar/view/1370

■関連情報サイト

・日立製作所の統合システム運用管理「JP1」
http://www.hitachi.co.jp/jp1/
・ヴイエムウェア株式会社のネットワーク仮想化製品「VMware NSX®」
http://www.vmware.com/jp/products/nsx.html
・2016 年 6 月発表「情報システム内における標的型サイバー攻撃の拡散を検知するソリューションを販売開始」(「拡散活動検知ソフトウェア」販売開始)
http://www.hitachi.co.jp/New/cnews/month/2016/06/0606.html

■商標に関する表示

■お客さまお問い合わせ先

株式会社日立製作所　ディフェンスビジネスユニット
サイバーセキュリティソリューションに関するお問合せフォーム:
https://www8.hitachi.co.jp/inquiry/hitachi-ds/cybersecurity/form.jsp

以上