※本リリースは、株式会社日立ソリューションズ、株式会社ブロードバンドセキュリティから配信しております。
重複して配信される場合がございますが、あらかじめご了承下さい。

2016年5月31日

株式会社日立ソリューションズ
株式会社ブロードバンドセキュリティ

マシンデータ利活用基盤と次世代ファイアウォールを連携し、情報漏洩リスクを軽減

ログ解析で不正な通信を即時遮断、24時間365日のセキュリティ監視サービスにより円滑な運用を実現

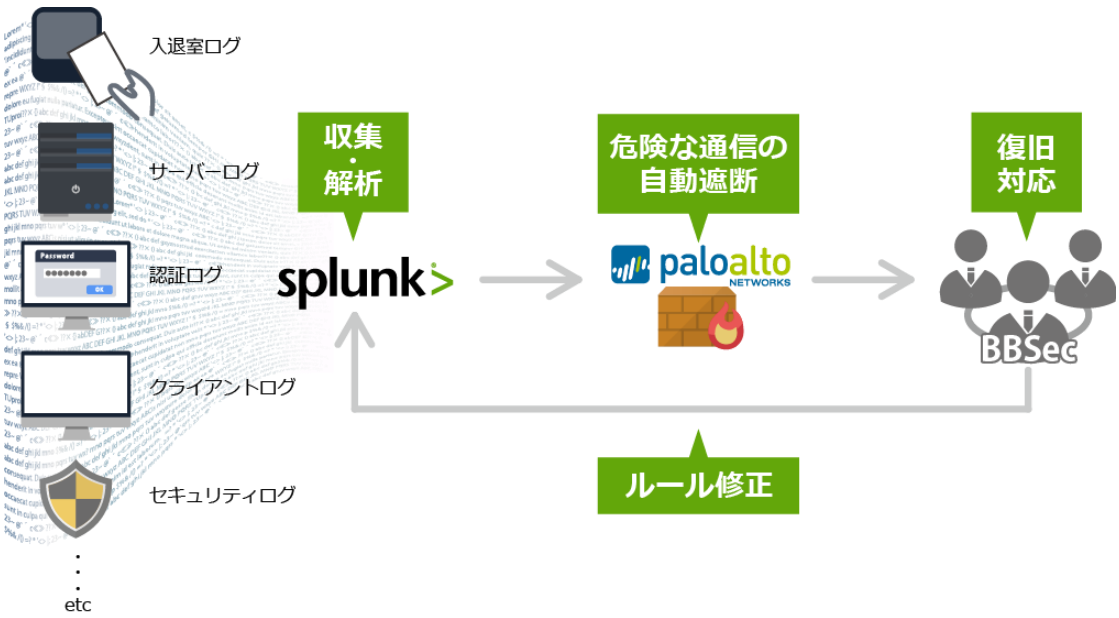
株式会社日立ソリューションズ(本社:東京都品川区、取締役社長:柴原 節男／以下、日立ソリューションズ)と株式会社ブロードバンドセキュリティ(本社:東京都新宿区、代表取締役社長:持塚 朗／以下、BBSec)は、米国 Splunk Inc.のマシンデータ利活用基盤「Splunk」と、米国 Palo Alto Networks, Inc.の次世代ファイアウォールを連携し、情報漏洩リスクを軽減するソリューションを6月1日より提供開始します。

本ソリューションは、日立ソリューションズとBBSecのノウハウを融合させて、企業や組織内の機器や通信、認証などのログを「Splunk」を用いて統合的に解析し、情報漏洩リスクのある外部への通信をPalo Alto Networksの次世代ファイアウォールのURLフィルタリングやセキュリティポリシーを用いて即時遮断します。

また、情報セキュリティの専門チームが24時間365日体制で遮断した通信を監視・分析し、誤遮断があった場合は、速やかに復旧します。

これにより、企業や組織は、機密情報や個人情報の漏洩リスクを軽減するとともに、誤遮断による業務への影響を最小限に抑えることができます。

■ソリューションイメージ



■背景

昨今、企業や組織の機密情報や個人情報の不正な取得を目的としたサイバー攻撃の被害が増大しています。これは、攻撃の手法が巧妙化し、シグネチャベース※1 のセキュリティ対策を回避する新たな攻撃の発生頻度が急増していることに起因しています。

このような攻撃に迅速に対応するためには、攻撃者の振舞いを多角的に解析し、標的型攻撃プロセスの「基盤構築段階」や「システム調査段階」※2 において、外部への不正な通信を即時に遮断し、情報漏洩を未然に防ぐことが求められます。

外部への通信を即時遮断する場合、スピードを優先するが故に業務上、必要な通信が誤って遮断される可能性があり、これを回避する運用が課題となっています。

※1　過去に識別された攻撃パターンをデータベース化し、ひとつの攻撃パターンをひとつのシグネチャとして管理したうえで、パターンマッチングを行う考え方

※2　出典:IPA『『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」 3.「新しいタイプの攻撃」の流れ

■ソリューションの特長

1. セキュリティ知識とログ解析で、情報漏洩リスクのある通信を迅速に察知

マシンデータ利活用基盤「Splunk」を用いた多くのノウハウとセキュリティ知識に基づいて、企業や組織内で出力される通信ログ、クライアントログ、認証ログ、入退室ログ、セキュリティログなどを過去の傾向などから解析し、情報漏洩リスクがあると考えられる通信を速やかに察知します。

2. 外部への通信を即時遮断

「Splunk」での解析結果から、情報漏洩リスクがあると判断された外部への通信を URL や IP アドレスを基に Palo Alto Networks の次世代ファイアウォールを用いて即時に遮断します。

3. 遮断した通信内容を 24 時間 365 日体制で監視し、円滑な運用を実現

即時に遮断した通信を BBSec のマネージドセキュリティチームが 24 時間 365 日体制で監視し、遮断原因を精査します。業務の支障となる誤遮断が発生した場合は、速やかに接続可能な状態に復旧することで、業務への影響を最小限に抑えます。

4. 未知のマルウェアへの対応

本ソリューションは BBSec が提供する「モダンマルウェア検知サービス」と組み合わせて利用することが可能です。「モダンマルウェア検知サービス」は、サンドボックスによる振舞い検知を複合的に組み合わせたサービスで、未知のマルウェアに対応可能です。

■今後について

日立ソリューションズとBBSecは、今後も両社のセキュリティ製品やサービスを組み合わせ、セキュリティイベントの検知から分析、遮断までをワンストップで対応するソリューションを提供していきます。

■価格

個別見積

■Splunk Inc.　Country Manager Japan　綱嶺　昌嗣(こうけつ　まさつぐ)氏のエンドースメント

企業は数十年に渡って確立した弛まぬ企業努力の結果、高い品質の製品やサービスを提供し続け、信頼を得てきていますが、洗練されかつ高度なサイバー攻撃により大量の顧客情報の漏洩、機密扱いである知財が漏洩してしまうことで、その信頼を失う危険にさらされています。

Splunkは、日立ソリューションズ様とブロードバンドセキュリティ様が、脅威に対する自動遮断ソリューションを提供されることを歓迎いたします。その中で、当社は、サーバーやネットワーク、Webなどの非セキュリティ・マシンデータとセキュリティデータを活用することでサイバーキルチェーンを見つけ出し、連動する脅威を分断することに寄与いたします。

■マシンデータ利活用基盤「Splunk」

「Splunk」は、サーバーやネットワーク機器、業務システム、センサーなどのマシンデータを収集、インデックス化することで、リアルタイムに検索、分析、可視化することが可能なマシンデータ分析ソフトウェアです。

紹介URL:http://www.hitachi-solutions.co.jp/splunk/

■パロアルトネットワークス株式会社　代表取締役会長兼社長　アリイ　ヒロシ氏のエンドースメント

サイバー攻撃は依然として日本企業を脅かす複雑な問題です。この課題を解決するためには、既存のシステムとネットワークを、次世代のアーキテクチャに再編する必要があります。パロアルトネットワークスは、日立ソリューションズ様とブロードバンドセキュリティ様が、脅威に対する自動遮断ソリューションを提供されることを喜ばしく思います。当社の次世代ファイアウォールで、堅牢なセキュリティの実現に貢献します。

■次世代ファイアウォール「Palo Alto Networks 次世代ファイアウォール」

Palo Alto Networks の次世代ファイアウォールは、トラフィック内のアプリケーションを識別し、可視化、制御することができます。これにより、ポートの開閉だけでは不可能だったきめ細かなセキュリティポリシーを実現し、標的型攻撃などによる情報漏洩を防止します。

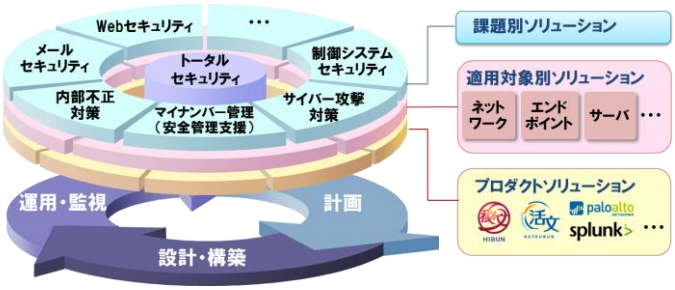
紹介URL:http://www.hitachi-solutions.co.jp/paloalto/sp/

■日立ソリューションズの「トータルセキュリティソリューション」について

日立ソリューションズは、企業のセキュリティライフサイクルを総合的に支援するため、自社やアライアンスの製品・サービスを「課題」「適用対象」「プロダクト」の 3 つの視点をもとに、システムのライフサイクルに必要なコンサルテーションと運用・監視のプロセスを強化した「トータルセキュリティソリューション」として体系化しています。

本ソリューションは、課題別ソリューションの一つとして提供している「サイバー攻撃対策ソリューション」の標的型攻撃対策メニューに位置づけられます。

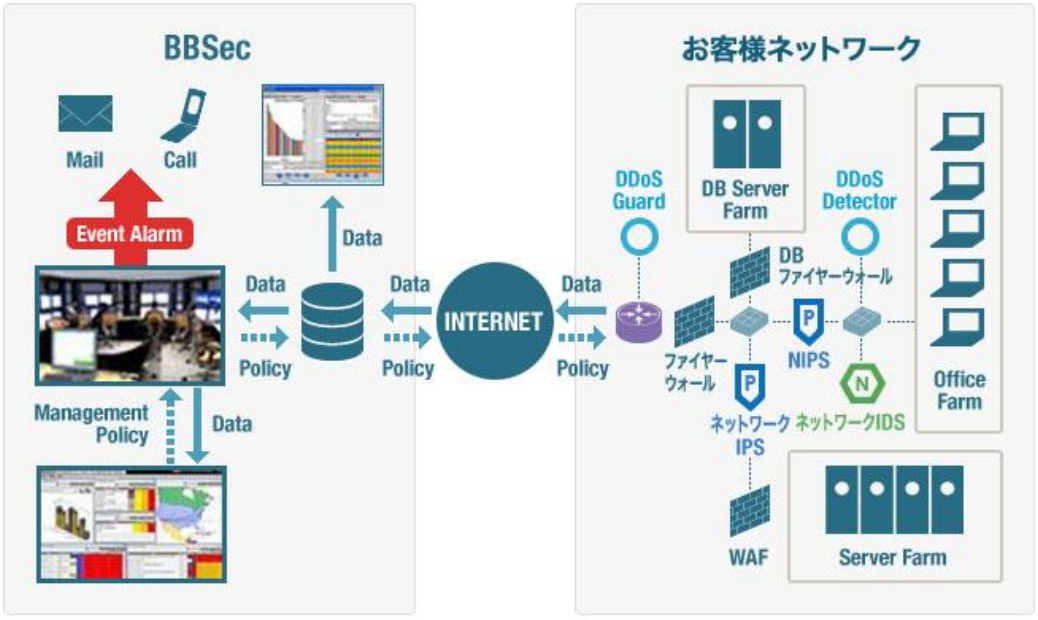
紹介 URL:
http://www.hitachi-solutions.co.jp/security/



■ブロードバンドセキュリティの「マネージドセキュリティサービス」について

お客様の Web サイトや IT システムに対する不正アクセス・攻撃を 24 時間 365 日体制でリアルタイムに監視し、適切な防御対策を実施します。イベントの発生時には、エンジニアによる誤検知などのフィルタリング実施後にお客様にご連絡し、攻撃の遮断等の対策を施します。

紹介 URL：https://www.bbsec.co.jp/service/security-outsourcing/service/mss.html



■商品・サービスに関するお問い合わせ先

日立ソリューションズ ホームページ：https://www.hitachi-solutions.co.jp/inquiry/　Tel：0120-571-488

BBSec ホームページ：https://secure.bbsec.co.jp/questionnaire/　Tel:03-5338-7425

■報道機関からのお問い合わせ先

株式会社日立ソリューションズ
担当部署:　経営企画本部 広報・宣伝部
担当者:　竹谷、安藤
Tel：03-5479-5013　Fax：03-5780-6455　E-mail：koho@hitachi-solutions.com

株式会社ブロードバンドセキュリティ
担当部署:　経営企画室
担当者:　高田
TEL：03-5338-7430　E-mail：press@bbsec.co.jp

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
