HITACHI
Inspire the Next

News Release

2015年6月9日
株式会社日立システムズ

サイバー攻撃や内部犯行に対するプロアクティブ型対策として、SOCを活用したログ相関分析サービスの提供を開始

SOCと連動したセキュリティインシデントへのトータル対応が可能に

株式会社日立システムズ(代表取締役 取締役社長:髙橋 直也、本社:東京都品川区/以下、日立システムズ)は、サイバー攻撃や内部関係者による情報漏えいなどの対策として、「SHIELD SOC*1」を活用したログ相関分析サービスの提供を開始します。「SHIELD SOC」を活用することでログ相関分析システムの利用時に難しいとされる検知ポリシーをノウハウ化し、最新の脅威や攻撃の兆候をリアルタイムに検知できます。

*1 SHIELD SOC:日立システムズのセキュリティオペレーションセンター。

昨今、サイバー攻撃や内部関係者の持ち出しにより企業の機密情報や顧客情報が漏えいするなど、セキュリティ事件・事故が深刻化しています。こうした情報漏えいを防ぐ手段として、スマートフォンや外部記録媒体(HDD、USBメモリーなど)の社内システムへの接続制限や、ファイアウォールや侵入検知装置を設置し、外部からの不正侵入対策を強化するなどの対策が考えられます。しかし、次々と新しい種類の外部記録媒体が登場し、不正侵入の手口も日々進化しており、完全な対策を行うのは困難です。また、情報漏えいが発生していることに気付かずにいると、時間の経過とともに被害が甚大になるため、こうしたセキュリティインシデントに対して、被害を最小化するための予防的対策(プロアクティブ対策)が求められています。

日立システムズは、こうした課題の解決のためにサイバー攻撃の予兆や兆候をリアルタイムに検知する「SHIELD ログ相関分析サービス」の提供を開始します。

「SHIELD ログ相関分析サービス」は、お客さまの情報システム上のファイアウォールや侵入検知装置などのネットワーク機器に加え、Webサーバー、データベース、クライアントPCなど、さまざまなデバイスのログを監視ツールにより収集し、それらのログを日立システムズの「SHIELD SOC」のアナリストが相関的に分析することで重要なセキュリティインシデントの兆候やその予兆を検知、または対策を行い、お客さまにご報告するものです。

単一のデバイスのログにおいては、正常な動作を装い行われる不正な行動からセキュリティインシデントを見抜くことは難しく、複数のログを相関的に分析し、過去の事例や不正行動パターンと照合することで、いつどのような不正が行われたかを把握することができるようになります。また、本サービスの導入を従業員に周知することにより、内部犯行の抑止にも効果があります。

本サービスは、24時間365日体制の「SHIELD SOC」から提供するため、セキュリティインデントの検知・報告はリアルタイムで行われます。そのため、セキュリティインシデントの兆候やその予兆に即対応することができ、被害を最小限に抑えることができるようになります。

株式会社 日立システムズ
〒141-8672東京都品川区大崎1-2-1
Tel. 03 5435 5002
www.hitachi-systems.com

Human * IT

また、「SHIELD　SOC」のアナリストが培った長年にわたる運用ノウハウと、既に提供中の「SHIELD グローバルインテリジェンスサービス」を組み合わせることにより、高度化、複雑化するサイバー攻撃に対応します。

さらに、「SHIELD　セキュリティデバイス監視サービス」や「SHIELD　クラウド CSIRT サービス」と組み合わせることでインシデントの早期検知から早期対策のアドバイスまで、セキュリティインシデントに対するトータルな対応が可能となります。

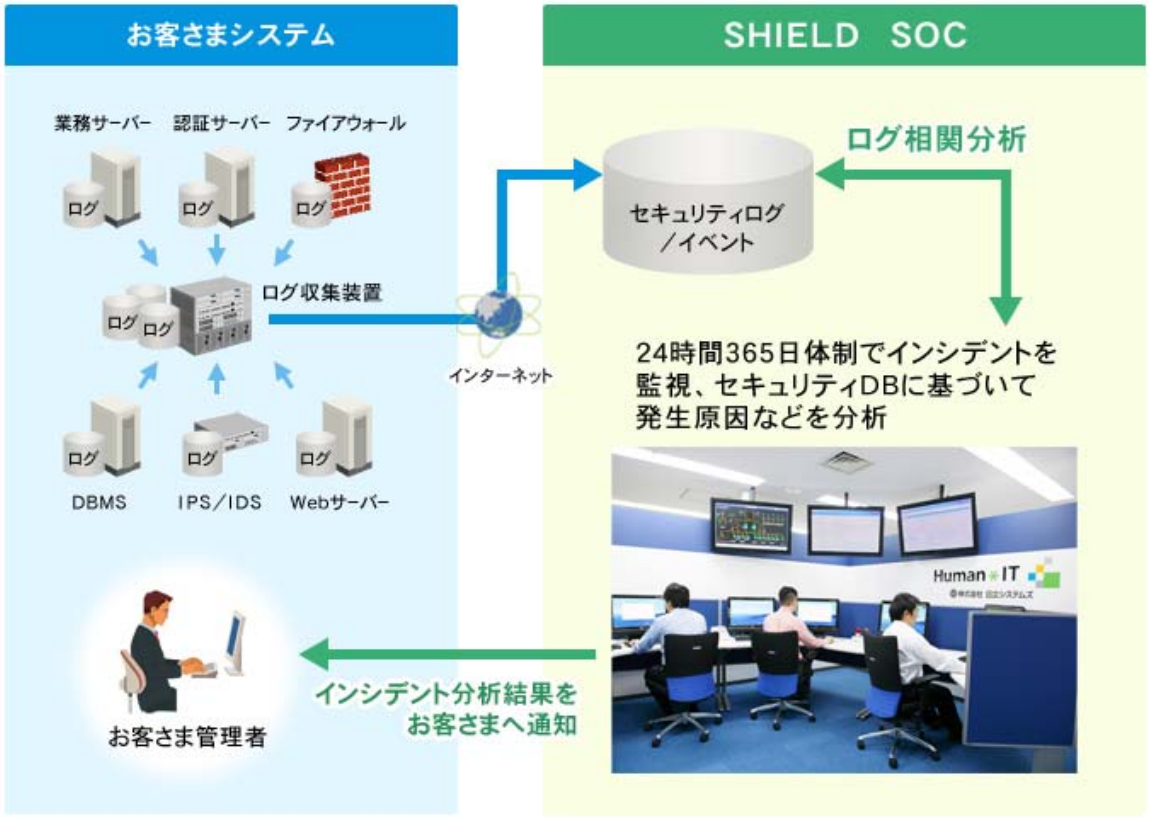
日立システムズは、当サービスをはじめとする企業に対する高度なセキュリティ運用サービスの提供により 2018 年度末までに 40 社導入、約 7 億円の販売をめざします。

日立システムズは、今後もサイバー攻撃や内部関係者による情報漏えいなどの対策について、Secureplaza コンソーシアム*2 と連携して順次拡充していきます。

*2　Secureplaza コンソーシアム：日立グループの総合力を結集してトータルなセキュリティソリューションをご提供するための組織

■SHIELD ログ相関分析サービスについて

お客さまの情報システム上のファイアウォールや IPS（侵入防止システム）などデバイスのログを収集し、それらのログを「SHIELD SOC」のアナリストが相関的に分析します。また、セキュリティインシデントを検知した際には、お客さまに報告します。



株式会社 日立システムズ
〒141-8672東京都品川区大崎1-2-1
Tel. 03-5435-5002
www.hitachi-systems.com

Human * IT

■SHIELD ログ相関分析サービスの Web サイト

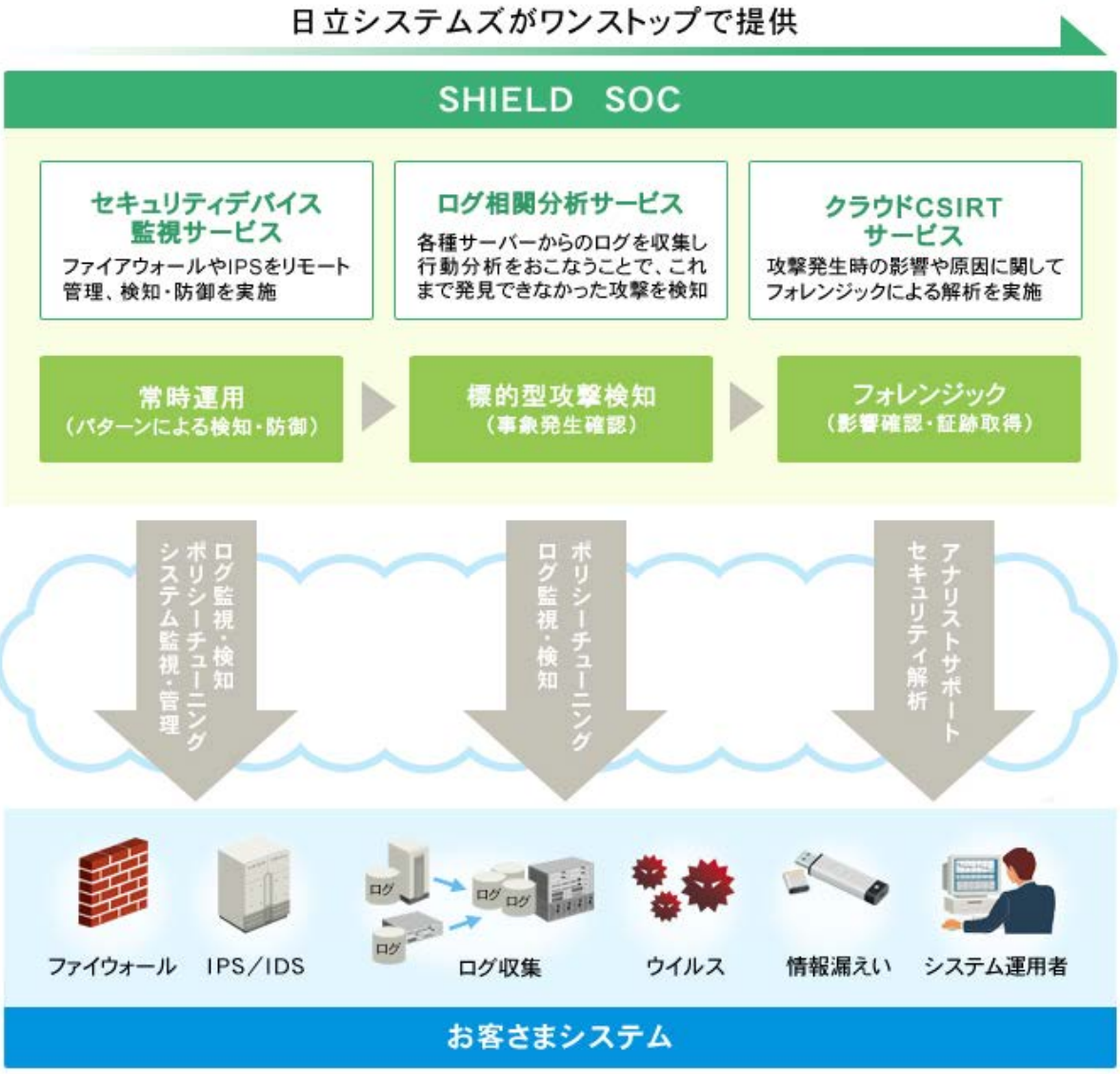
http://www.hitachi-systems.com/solution/t01/shield/log.html

■ログ相関分析サービスで検知できるセキュリティインシデント例

監視対象	分析対象ログ	分析によってわかること
外部からのサイバー攻撃	侵入検知システム（IDS）の攻撃検知ログ、侵入防止システム（IPS）、ファイアウォール、Web サーバー、ファイルサーバー	情報漏えい被害の発生の有無、攻撃ルート、攻撃者の目的（取得したいデータ）
内部関係者による犯行	クライアント PC、ファイルサーバー、入退室管理システム	不正取得を実行した ID、用いられた端末、外部媒体、取得データ

■SHIELD　SOC と連携したセキュリティインシデントへの対応

本サービスは「SHIELD　SOC」で提供している既存サービス（セキュリティデバイス監視サービス、クラウド CSIRT サービス等）との連携により、サイバー攻撃の検知・防御から発生後のフォレンジック対応まで、ワンストップでトータルセキュリティ対策が可能です。



■SHIELD　グローバルインテリジェンスサービス

日立システムズが長年にわたり築き上げたセキュリティベンダーや各団体で構成されるグローバルインテリジェンス網により、ハクティビズム（政治・社会的な主張をもととしたハッキング活動）やサイバーテロなどの情報を収集、「SHIELD SOC」で分析し、お客さまに情報提供するサービスです。

http://www.hitachi-systems.com/solution/s003/johoteikyou/

■SHIELD　セキュリティデバイス監視サービス

ファイアウォール、IDS／IPS などのセキュリティデバイスを、「SHIELD　SOC」から 24 時間 365 日、監視・運用するサービスです。

http://www.hitachi-systems.com/solution/s002/shield/security-device/

■SHIELD　クラウド CSIRT サービス

「SHIELD　SOC」のアナリストが、セキュリティインシデント情報の提供や分析サービスを専用のポータルサイト経由で提供することで、お客さまの CSIRT の運用を支援するサービスです。

http://www.hitachi-systems.com/solution/t01/shield/csirt/

■日立セキュリティソリューションセミナーについて

2015 年 6 月 10 日(水)に東京コンベンションホールで開催する日立セキュリティソリューションセミナーにおいて、今回発表した製品を紹介します。

詳細は http://www.hitachi.co.jp/Prod/comp/Secureplaza/security_seminar/　をご覧ください。

■日立システムズのサイバーセキュリティへの取り組みについて

日立システムズは経営課題となるセキュリティに対する情報を以下のサイトで提供しています。

http://www.hitachi-systems.com/secure/

■お客さまからのお問い合わせ先

株式会社日立システムズ

商品お問い合わせ窓口：TEL 0120-346-401(受付時間：9時～17時／土・日・祝日は除く)

お問い合わせWebフォーム：https://www.hitachi-systems.com/d-inquiry/contact.cgi

■報道機関のお問い合わせ先

株式会社日立システムズ　CSR 本部　コーポレート・コミュニケーション部　杉山、住川

〒141-8672　東京都品川区大崎一丁目 2　番 1　号

TEL：03-5435-5002(直通)　E-mail　：　press.we@ml.hitachi-systems.com

以上

＊記載の会社名、製品名はそれぞれの会社の商標または登録商標です。