2014 年 11 月 19 日
NRI セキュアテクノロジーズ株式会社

400 種類以上の情報システム機器に対応した「セキュリティログ監視サービス」を提供開始

～グローバル企業に必要な IoT 時代のサイバーセキュリティ対策を支援～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：増谷 洋、以下「NRI セキュア」）は、企業の情報システムで利用されているさまざまな機器（サーバ、ネットワーク機器、クライアント端末等、以下「情報システム機器」）が出力するログ情報を、NRI セキュアが持つ独自の技術で分析し、迅速にセキュリティインシデント（情報セキュリティ上の問題や事件）を見つけ出す「セキュリティログ監視サービス」を、グローバルで提供開始します。本サービスは、世界で IT ベンダーが販売している 400 種類以上の情報システム機器に対応しています。

外部からのサイバー攻撃や内部者の不正犯行による情報漏洩事件が後を絶たない昨今、その多くが企業経営に大きな打撃を与えています。攻撃の複雑化や情報流出経路の多様化により、従来とられてきた単体のセキュリティ製品に頼る対策では、多種多様な脅威を防ぐことは困難になっています。現実的には、「脅威を防ぐこと」から「脅威による被害を最小限に抑えること」に主眼を置いた、より現実的なセキュリティ対策を講じることが重要になっており、以下の特長を持つ本サービスの利用が有効な対処策となります。

■ 400 種以上の情報システム機器のログを独自技術で分析し、脅威を早期に発見

企業で日々使用する情報システム機器とそのログ情報の種類や量は膨大であり、さらに専門知識や技術力の不足、人手の不足、情報システム全体の状態の可視化が不十分、といったさまざまな要因が重なると、脅威の兆候を示す重要なログを見つけることは困難を極めます。

こうした課題を解決するために、本サービスは、企業の情報システムで広く利用されている 400 種類以上の情報システム機器に対応しています。それらの機器から出力される膨大なログ情報の監視を一元化し、NRI セキュアが独自に設計したロジックによる相関分析[*1]をリアルタイムでおこなうことで、セキュリティ対策の観点からみて重要なログを迅速に抽出します。それによって、サイバー攻撃や内部不正犯行などの脅威による被害を最小限に抑える上で不可欠なセキュリティインシデントの早期発見が可能となり、情報漏洩などのリスクを確実に軽減します。

また、対象機器の幅を広げたことにより、従来のインシデントレスポンスサービスでセキュリティ機器単体のログ情報を監視することでは不可能であった、内部不正犯行などのインシデントも発見できます。さらに、監視・取得するログ情報のフォーマットを任意に定義することが出来るため、家電や計測装置など、さまざまなデバイスがインターネット

に接続される IoT（Internet of Things）時代を迎えて、新たにセキュリティリスクを抱える種々のシステムへの応用が期待されます。

■ 導入企業ごとに脅威を想定したサービスや、攻撃に対する「自動防御機能」を提供

各導入企業のネットワーク構成、情報資産、ユーザ情報を把握した上で、発生する可能性のある脅威を想定し、情報システムやデータの重要性を考慮した、重点的な監視サービスの仕組みを構築します。また、導入企業のビジネスにあわせて、ネットワーク上の通信やデータへのアクセス状況の監視をおこなうことも可能です。

さらに本サービスでは、サイバー攻撃に対しての「自動防御機能(Active Defense)」も提供します。これは、重大なセキュリティインシデントを検知した際に、導入企業のファイアウォール等のセキュリティ機器を自動的に遮断処理するものです。これにより、セキュリティの担当者が異常に気付いておこなう遮断作業よりも、防御までの時間を大幅に短縮できます。

■ グローバル企業のサイバーセキュリティ対策を支援

NRI セキュアが日米に置いているセキュリティ監視センター(SOC)から、高度な資格を有したセキュリティアナリスト[*2]が 24 時間 365 日の体制で監視・分析をおこない、セキュリティインシデントを迅速に発見します。日本語と英語による電話・メールでの監視状況の報告や助言をおこなうことが可能で、グローバルに事業を展開する企業のサイバーセキュリティ対策を全世界で支援します。

なお、サービス価格は個別見積もり[*3]で、日本国内でのサービス提供は 2015 年 1 月からを予定しています。なお、米国では 2014 年 10 月から提供を開始しています。

NRI セキュアは、今後も、グローバル企業の情報セキュリティ対策を支援するさまざまなサービスを提供し、安全・安心な情報システム環境と社会の実現に貢献していきます。

*1 相関分析：

複数のログやイベントの情報を関連づけることにより、より効果的、効率的にセキュリティインシデントを発見する分析手法。

*2 セキュリティアナリスト：

当社のセキュリティアナリストは GIAC（Global Information Assurance Certification）や CISSP（Certified Information Systems Security Professional）などの高度セキュリティ資格を有しています。

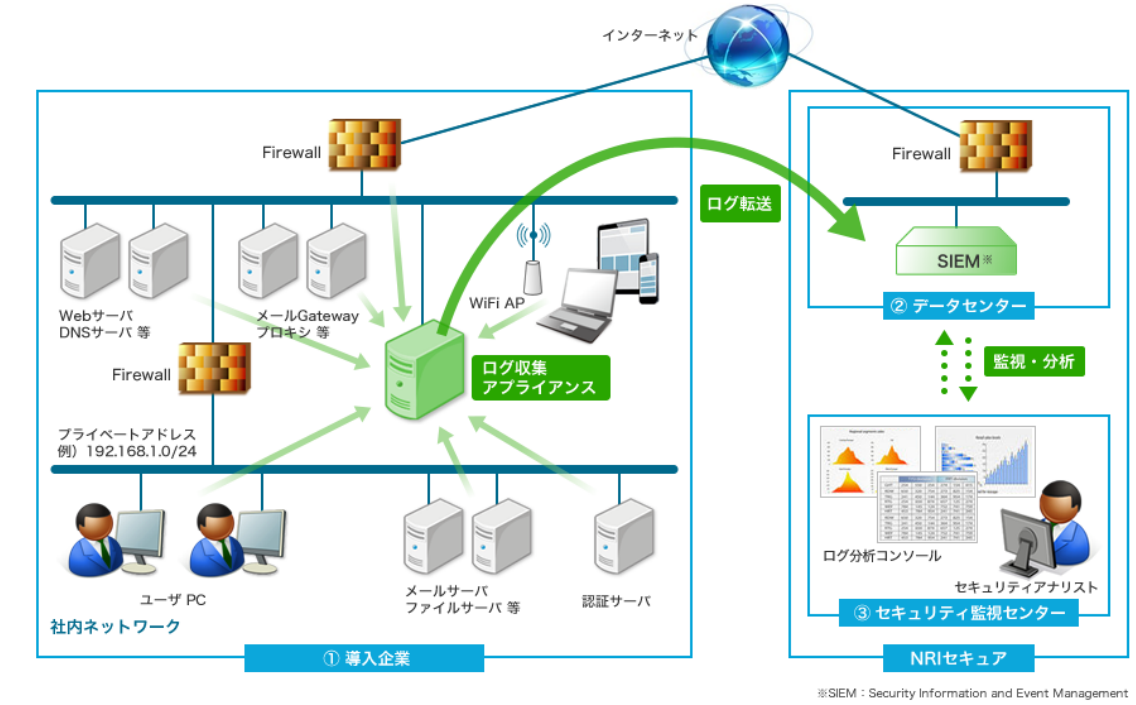
*3 見積もりの例

ファイアウォール(小) 1 台、Windows ドメインコントローラ(小) 1 台を監視した場合、月額 30 万円からとなります。

【ニュースリリースに関するお問い合わせ】
株式会社野村総合研究所　コーポレートコミュニケーション部　十河、海藤
TEL：03-6270-8100　E-mail：kouhou@nri.co.jp
【サービスに関するお問い合わせ】
NRI セキュアテクノロジーズ株式会社　MSS 開発部　吉田、初谷
（広報担当）若尾
TEL：03-6706-0500　E-mail：　info@nri-secure.co.jp

【ご参考】

●サービス概要図



① 導入企業にて：社内に設置したログ収集アプライアンス（装置）が、情報システム機器から出力されるログを自動的に収集し、NRI セキュアデータセンター内の SIEM（セキュリティ情報イベント管理）と呼ばれる装置に転送します。

② NRI セキュアのデータセンターにて：転送されたログに対して、NRI セキュアが独自に設計したロジックによる相関分析をおこないます。

③ NRI セキュアのセキュリティ監視センターにて：セキュリティアナリストが 24 時間 365 日の体制で監視・分析をおこない、セキュリティインシデントを迅速に発見し、必要な対応を行います。

「セキュリティログ監視サービス」の詳細は、以下の URL をご参照ください。
http://www.nri-secure.co.jp/service/mss/log_monitoring.html