NTTデータ先端技術/NTTデータ
次世代ファイアウォール監視サービス

日々高度化するサイバー攻撃に対抗するため、24 時間 365 日の専門アナリストによるセキュリティ監視サービスもさらに進化

サイバー攻撃の高度化に伴い、FW（ファイアウォール）やIDS/IPS（不正侵入検知／防御装置）、URLフィルタ、アンチウイルスなどのセキュリティソリューションを複数用いて多層化した防御を行い、被害を最小限に抑える対策が求められています。
NTTデータ先端技術が提供している次世代ファイアウォール監視サービスは、セキュリティ知識を蓄えたセキュリティアナリストが24時間365日で監視を実施して、不正アクセスによる攻撃を検知・防御するサービスです。
複数のセキュリティ機能が検知したログやSOC（セキュリティオペレーションセンター）で独自に収集した情報の相関分析を行うことで、分析力を向上させています。

100%守れるセキュリティは存在しない

標的型攻撃をはじめとした高度なサイバー攻撃による被害が後を絶ちません。2018 年 1 月に IPA（独立行政法人情報処理推進機構）が発表した「情報セキュリティ 10 大脅威 2018」では、前年に続き「標的型攻撃による情報流出」や「ランサムウェアによる被害」が上位を占め、「IoT 機器の脆弱性の顕在化」が順位を上げつつ、「ビジネスメール詐欺」「セキュリティ人材の不足」が新たにランクインするなど、脅威の多様化が進んでおり、数年先を見据えた対策が求められています。「100%守れるセキュリティは存在しない」ことからも検知・監視の必要性が再認識されています。

脅威の対策は、①アクセス制御（FW）、②プログラム起動の防止（アンチウイルス）、③権限管理（アカウント管理）、④監視（検知・遮断）、などの実施が必要とされますが、その中で④監視については、経済産業省発行の「サイバーセキュリティ経営ガイドライン」の中においても、対策が不十分であることが指摘されています。攻撃者による「最初の攻撃」から「データの取り出し」までは非常に短い時間で行われます（図 1 参照）。一方、被害者による「最初の被害」から「封じ込め」までは長期化する傾向にあります。攻撃を「できるだけ早く発見する」ためには、速やかに検知・監視できる仕組みと追跡可能な証跡を保存できる仕組みが必要です。

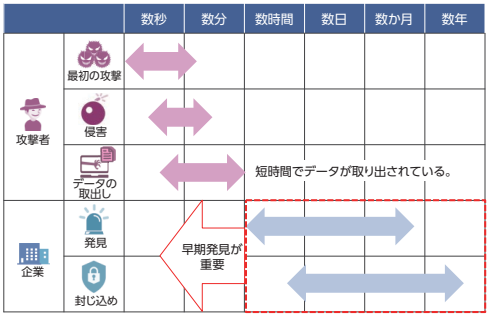

図1　攻撃から封じ込めまでの時間

脅威の変化に対応し、監視サービスも進化

サイバー攻撃の高度化に伴い、従来の FW や IDS/IPS の機能に加えて、URL フィルタ、アンチウイルスなどの機能を搭載した UTM（総合脅威管理装置）の利用が進んでいます。しかし、UTM を導入するだけでは守り続けることはできず、運用をどのように行うのかによって、セキュリティレベルは大きく変わります。例えば、UTM がインシデントを検知すると、対策を決定するために、インシデントの詳細情報、関連する脆弱性情報、一般的な対策方法、自社への影響有無の確認、他社の対処事例など、情報をすばやく収集する必要があります。しかし、専門のセキュリティアナリストがいないと、このような対応を迅速に行うことは困難です。また、そのような人材を含めた体制を自社で用意する場合は多大な費用が必要になります。

NTT データ先端技術では、このような課題を解決する次世代 FW 監視サービスを提供しています（図 2 参照）。これ

までの監視サービスでは、IDS/IPS など限られた機器のみしか監視できませんでしたが、コアエンジンを刷新することで、UTM による監視サービスの提供が可能になりました。

本サービスは、最新鋭のセキュリティ設備を持つ NTT データ先端技術の監視センター（SOC：セキュリティオペレーションセンター）と連携して、専門のセキュリティアナリストが 24 時間 365 日の監視を行うことで不正アクセス攻撃への防御を支援します。

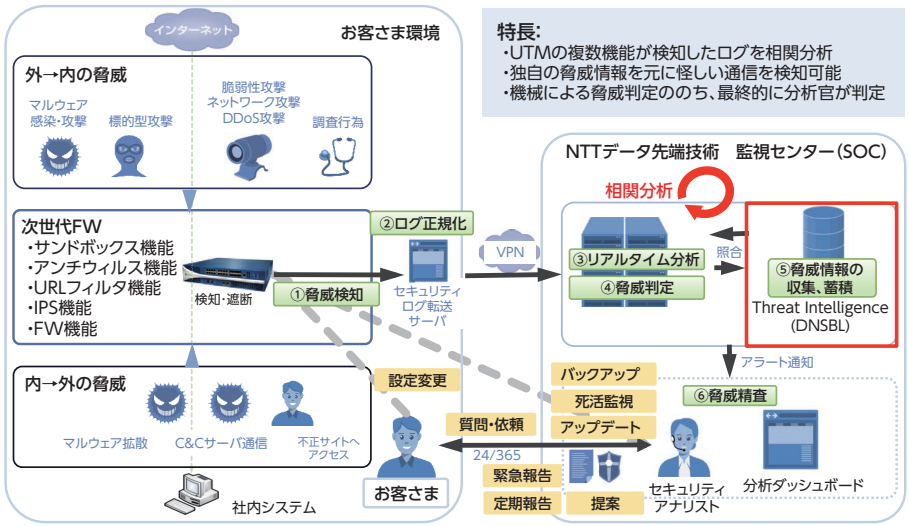

図2　次世代ファイアウォール監視サービスの概要

サービス提供前には試運転により正常通信の誤検知や誤遮断をチューニングします。また、運用開始後にもネットワークの変更やアプリケーション改修などによる誤検知が発生した際は、お客さまと確認しながらチューニングを実施し、検知精度を高い状態に保つようにしています。また、危険度の高いアラートを検知し「防御対象への影響がある」もしくは「内部ネットワークでマルウェアに感染した端末の活動がある」と判断した場合は、速やかに緊急報告を実施します。

分析力をスポット対応で利用できる

NTT データ先端技術では、最新の脆弱性情報などを自社の SOC や CSIRT、ベンダーなどから収集して、これらの情報を分析し、お客さまのシステムを監視するコアエンジンに反映することで、検知・遮断精度の向上を図っています。

また、この分析力をスポットで提供する「ログ分析サービス」の提供も行っています。高い分析力と知見を利用して、初見のお客さまのプロキシログから、危険な通信を見つけ出し、インシデントの危険度を報告します。

インシデント発生時や、自社のセキュリティ対策の充足を確認する目的で利用することができます。

※次世代ファイアウォール監視サービスの URL
http://www.intellilink.co.jp/security/services/scrutiny/06.html

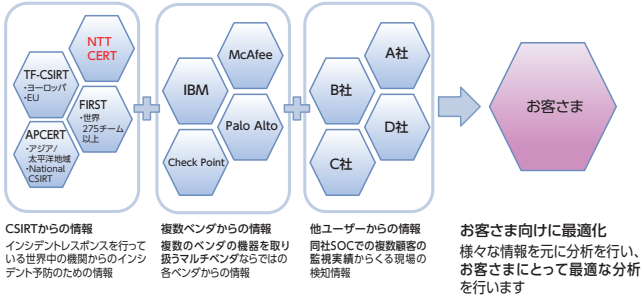

図3　最新の情報を多方面から収集して分析結果をお客さまに提供

20年にわたりミッションクリティカルなシステムを監視してきた実績と、豊富な経験を持つセキュリティアナリストが、セキュリティの最適化をサポートします。

NTTデータ先端技術
セキュリティ事業部　セキュリティオペレーション担当
【左側】サービス提供グループ長　**水野 健生**
【右側】チーフエンジニア　**堤 紀考**

お問い合わせ先
NTTデータ先端技術株式会社　セキュリティ事業部　TEL：03-5859-5422
株式会社NTTデータ　技術革新統括本部　企画部　TEL：050-5547-2671

※http://www.bcm.co.jp/でも閲覧できます。