最新ランサムウェアからクラウド上のシステムを守る！

クラウド
コスト削減

欧米を中心にWannaCryなどのランサムウェアを使ったサイバー攻撃が続発しています。すでに多くの企業が被害を被っており、日系企業においても工場の停止やメールサーバーへの攻撃など、大きな被害が発生しており決して油断はできません。言うまでもなく、こうしたサイバー攻撃に対処するためには適切にセキュリティ対策を講じる必要があります。

そのセキュリティ対策には、通信経路上で実施するネットワーク型と、セキュリティを強化するソフトウェアをサーバーやパソコン上で実行するホスト型があります。昨今ではサイバー攻撃で使われる手口が極めて巧妙になっており、単純なセキュリティ対策では攻撃を阻止することはできません。ネットワーク型とホスト型を組み合わせた、多層防御の考え方でセキュリティ対策に取り組むべきでしょう。

また、現在では多くのシステムがクラウド上で運用されていることから、そこでの守りをどうするかが大きな鍵となります。この課題を解決するために、NTT Comでは「Enterprise Cloud セキュリティオプション」を提供しています。このサービスでは、ファイアウォールやUTM、Webアプリケーションを守るWAF（Web Application Firewall）、本格的な対処を行うまで、発見された脆弱性に向けた攻撃を防ぐ仮想パッチなど、さまざまなセキュリティ対策をトータルで提供しています。

Enterprise Cloud セキュリティオプションを利用できるのは、NTT Comのクラウドサービスである「Enterprise Cloud」だけでなく、Amazon Web Servicesといった他社のクラウドサービスやオンプレミス環境でもご利用可能です。このため保護対象を選ばずに利用していただけるほか、クラウドサービスのため短期間だけ利用するシステムを保護したいといった場面でも有用です。

すでにサイバー攻撃は経営リスクの1つとして認識されており、トップダウンでセキュリティ対策を進めるべきものとなっています。ランサムウェアの感染などによって大きな被害が生まれる前に、改めて対策を見直しましょう。

続発するランサムウェアを使った大規模サイバー攻撃

2017年5月、WannaCryと呼ばれるランサムウェアを使った大規模なサイバー攻撃が発生、欧米を中心に大きな被害が生まれました。また日本においてもいくつもの大手企業が被害を受けています。

ランサムウェアは感染したパソコンのファイルを勝手に暗号化し、利用不能な状態にした上で身代金を要求するという卑劣なマルウェアです。2017年5月のサイバー攻撃では、世界各地のコンピュータがランサムウェアであるWannaCryに感染し、病院において診療が不可能となったり、工場の操業が不可能になったりするといった事態が発生しています。

そして翌6月には、新たなランサムウェアを使った大規模サイバー攻撃が発生しました。使われていたのは「GoldenEye」などと呼ばれる新種のマルウェアで、WannaCryと同様に世界各地のコンピュータに感染しています。深刻な被害が生じているのも同様で、チェルノブイリ原子力発電所やキエフの国際空港が影響を受けたとの報道もあります。

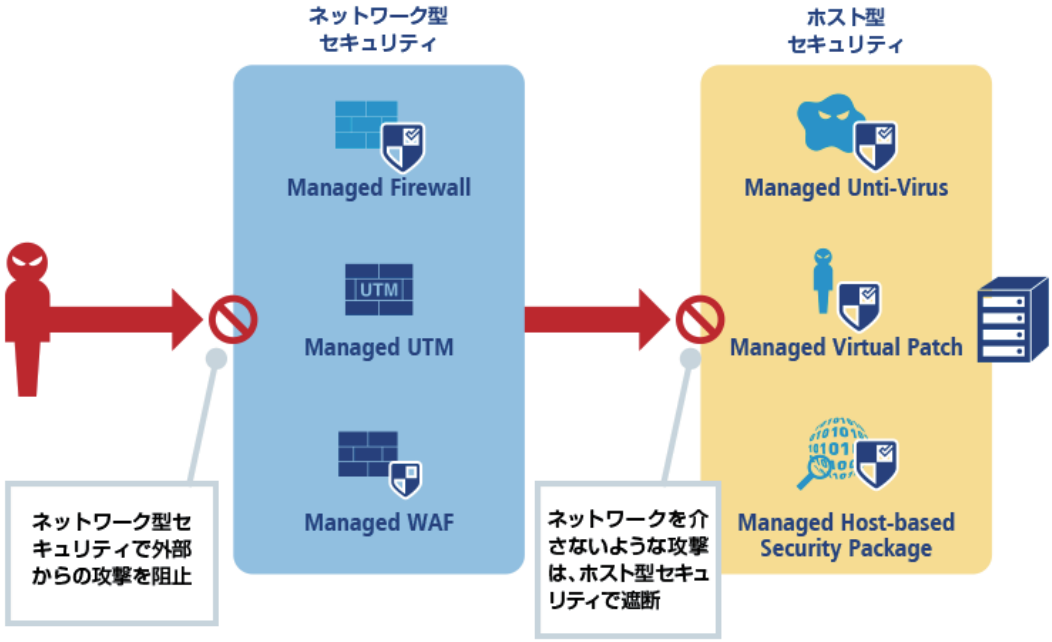
犯罪者にとってランサムウェアは直接的に金銭を窃取できる魅力的な攻撃手法であることから、今後も同様のサイバー攻撃は続くと考えるべきでしょう。

多層防御でサイバー攻撃をシャットダウン!
防御力を高めるネットワーク+ホスト型セキュリティ

NTT ComのEnterprise Cloudセキュリティオプションでは、ネットワーク上で通信を監視する「ネットワーク型」と、サーバーにインストールして利用する「ホスト型」の2つのカテゴリでサービスを提供しています。

この2つのカテゴリのサービスを適切に組み合わせれば、単独で利用するよりもセキュリティ対策をさらに強化することが可能です。組み合わせの一例としては、ファイアウォールとしての機能に加え、IPS／IDSやウイルス対策の機能も併せ持つネットワーク型の「Managed UTM」と、未修正の脆弱性を狙った攻撃を防げるホスト型である「Managed Virtual Patch」の利用が考えられます。これらを利用すれば、サーバーに対する外部からの不正侵入などをManaged UTMで防ぎつつ、さらに対策が実施できていない脆弱性を狙った攻撃をManaged Virtual Patchで防ぐことが可能となり、サイバー攻撃のリスクを低減できるでしょう。

いずれにしてもサイバー攻撃は日常的に行われるようになっており、決して油断できない状況が続いています。ランサムウェアに感染してシステムが利用不能になった、あるいはサーバーへの不正侵入で機密情報が漏えいしたなどといった事態に陥る前に、適切にセキュリティ対策を講じましょう。



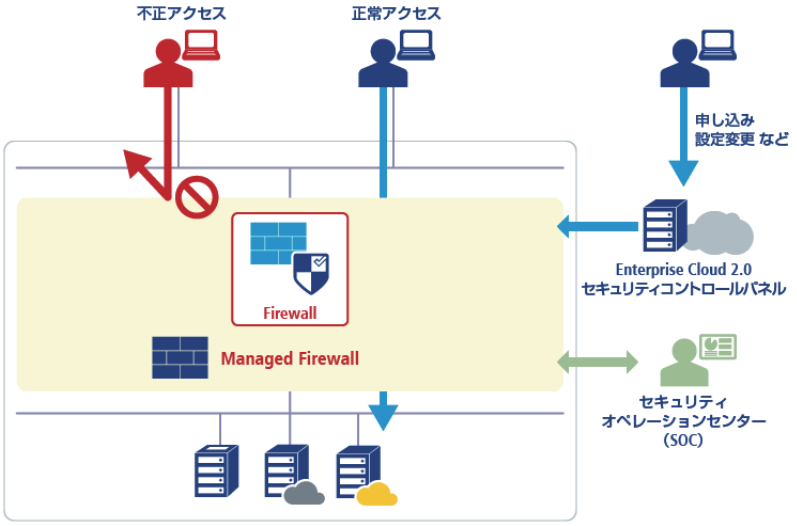
ネットワーク型セキュリティ

サーバーに接続する前のネットワーク領域でセキュリティ対策を実施します。「Managed Firewall」と「Managed UTM」、「Managed WAF」の3つのメニューを用意しています。

ファイアウォールの仕組みをクラウド型で提供

■Managed Firewall

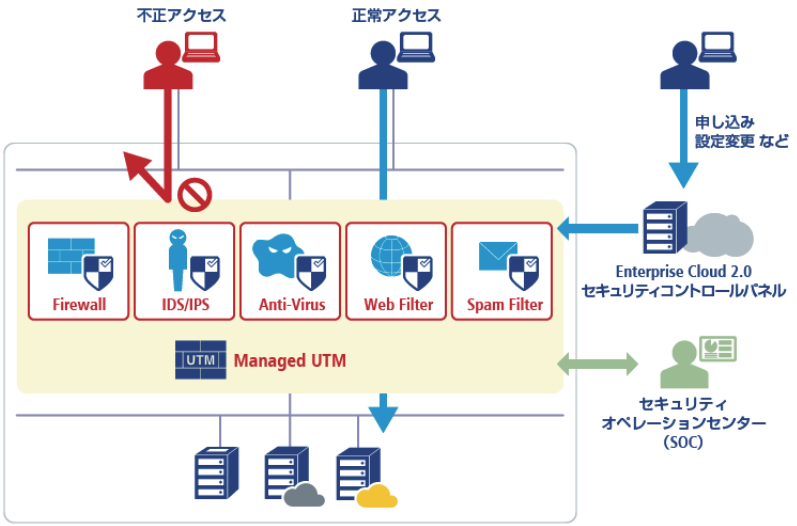
デバイスを通過するトラフィックについて、事前に設定したファイアウォールポリシーに基づいて制御する機能を提供します。トラフィック制御は通過パケットの状態を監視し、行きのパケットの通過を許可した時点で戻りパケットも許可する、ステートフルインスペクションに対応しています。またより高度なセキュリティ対策が必要になった場合は、ワンクリックで次のManaged UTMにアップグレードできます。



セキュリティ対策に必要な機能を網羅

■Managed UTM

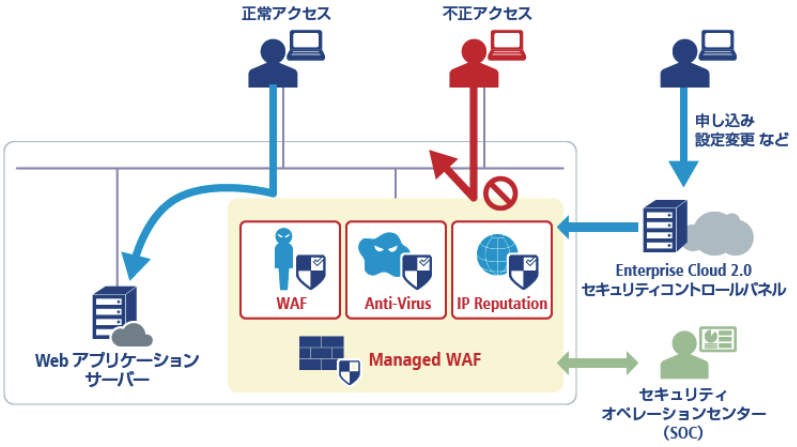
ファイアウォールの機能に加え、危険と判断された通信を検知／防御するIDS／IPS、ウイルスが含まれる通信を遮断するアンチウイルス、Webサイトへのアクセスを検査して通信を制御するウェブフィルターなど、豊富なセキュリティ対策機能をネットワーク上で実施することができるサービスです。



Webアプリケーションを保護

■Managed WAF

Webアプリケーションサーバーへの通信を監視し、攻撃を意図した通信の遮断やウイルスの検知と防御を実現します。また脅威として特定できる情報を元に検知を行うIPレピュテーション機能や、サーバーに対して大量の通信を行ってサービス提供を不可能とするDoS攻撃を防御する機能も備えています。



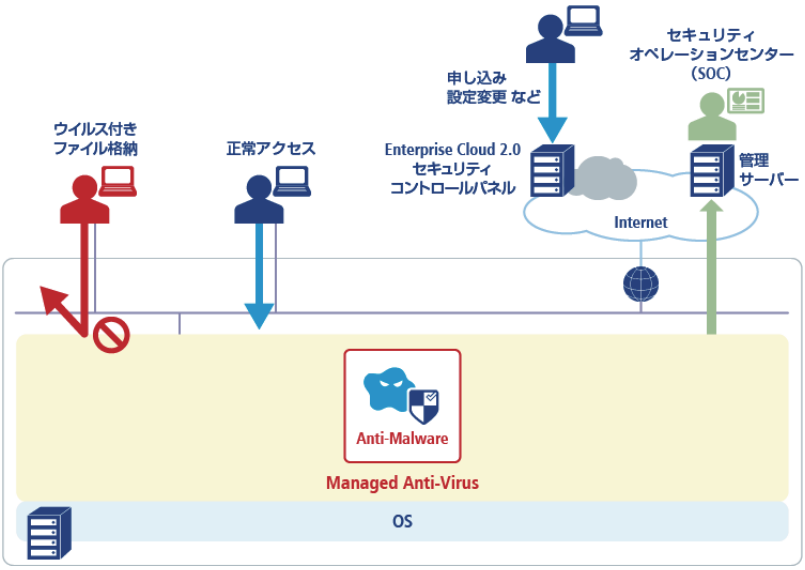
ホスト型セキュリティ

サーバーにセキュリティ機能を組み込み、外部からの攻撃を防ぎます。「Managed Anti-Virus」、「Managed Virtual Patch」、「Managed Host-based Security Package」の3つを用意しています。

迅速に導入できるウイルス対策

■Managed Anti-Virus

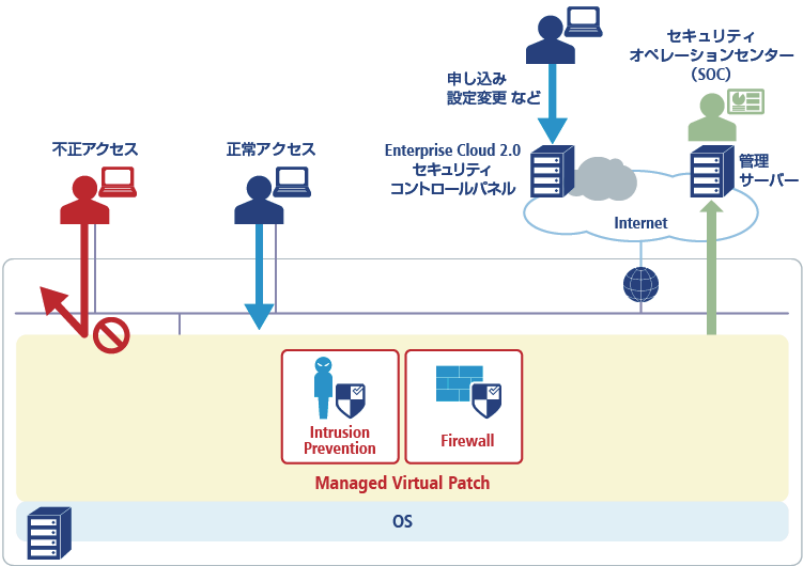
サーバーがマルウェアに感染することを防ぎます。ホストにマルウェアが侵入しようとした際に検出するリアルタイム検索、指定した日時でマルウェアを検査するスケジュール検索が可能です。また、検査対象のファイルや検出された場合の処理などを細かく設定することが可能になっています。



未対応の脆弱性への攻撃を防御

■Managed Virtual Patch

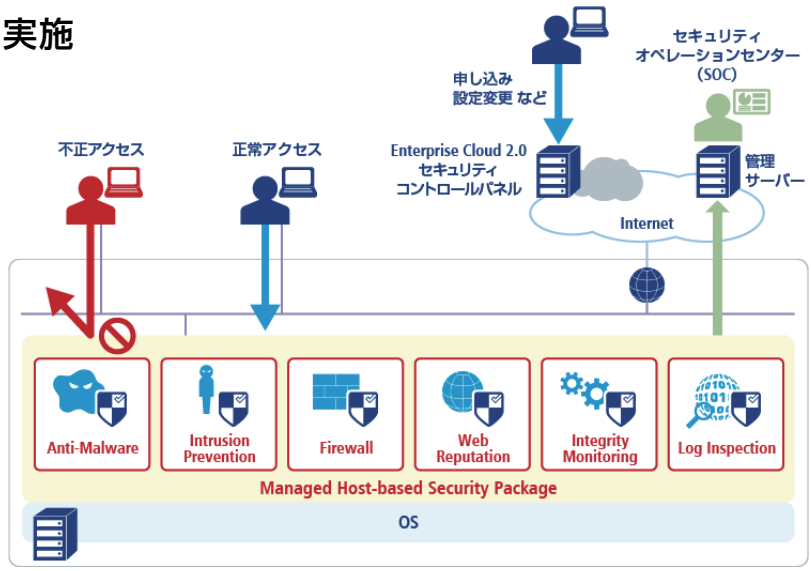
OSやアプリケーションの脆弱性に対する攻撃からサーバーを保護します。これを利用することにより、OSやアプリケーションの脆弱性が発見されてから対処を行うまでの間、その脆弱性を利用した攻撃を防ぐことが可能となります。WindowsやLinuxなどの主要OSのほか、100以上のアプリケーションの脆弱性を保護できます。



高度なセキュリティ対策をワンストップで実施

■Managed Host-based Security Package

Managed Anti-VirusとManaged Virtual Patchの機能に加え、サーバーが不正なURLへアクセスすることをブロックするWebレピュテーション、指定したファイルなどに変更があった場合にアラートを発する変更監視、ログやイベントを監視して異常が発生した際に通知する機能を提供します。



＜ ソリューションサービス ＞

≫Enterprise Cloud セキュリティオプション	NTTコミュニケーションズの実績あるセキュリティサービスをクラウドと連携し利用できるオプションです。サーバーに接続する前のネットワーク領域での対策を行います。
≫WideAngle	人工知能搭載のSIEMエンジンとセキュリティオペレーションセンター(SOC)のリスクアナリストが24時間365日体制で高度なセキュリティ監視を行います。またリスクアセスメントを始めとするプロフェッショナルサービスも提供しています。

クラウド業務で課題をお持ちのお客さま

フリーダイヤル/ナビダイヤル回線から便利な機能まで、お客さまニーズに合わせた最適なソリューションをご提案いたします。

0120-106107

受付時間 | 9:30～17:00（土日祝日を除く）