News Release

NTT Communications

2019 年 2 月 12 日

Windows Defender ATP を活用した
高機能なエンドポイントセキュリティ対策サービス「EDR」を提供開始
～SOC の高度分析により、未知のサイバー脅威に対する早期発見・早期対処を実現～

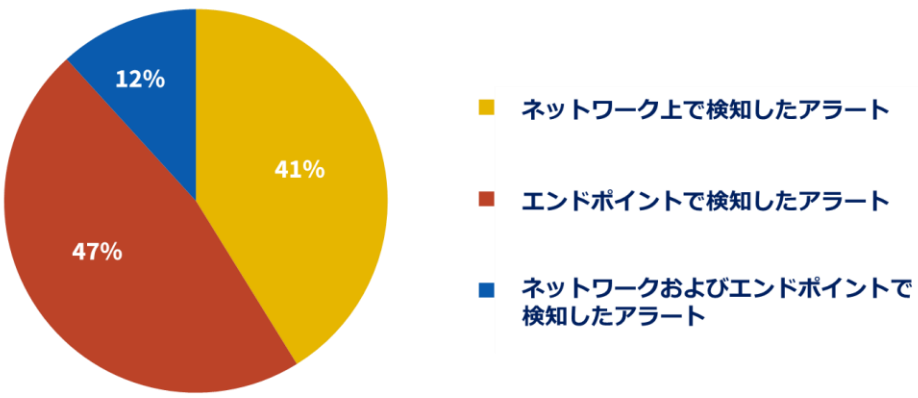
NTT コミュニケーションズ株式会社（以下 NTT Com）は、マイクロソフトの Windows Defender Advanced Threat Protection（以下 Windows Defender ATP）と連携した新たなエンドポイントセキュリティ対策サービス「EDR」※1 を、総合リスクマネジメントサービス「WideAngle」のマネージドセキュリティサービスにおいて、2019 年 2 月 12 日より提供開始します。

1. 背景

昨今のサイバー攻撃では、攻撃自体の暗号化や従来のマルウェアを使わないファイルレスマルウェア攻撃※2 の増加により、インターネットゲートウェイにおけるセキュリティ対策をすり抜け、ICT 環境上の PC 端末やサーバーなどエンドポイントに到達する状況が広まっています（下図参照）。一方で、働き方改革の浸透によりリモート環境での PC 端末利用が拡大しており、巧妙化するサイバー攻撃に直接さらされる機会が増えていることから、PC 端末におけるサイバー攻撃の検知強化の重要性はより一層高まっています。

NTT Com は、多くの企業で導入されている Windows OS 端末において導入しやすいエンドポイントセキュリティ対策サービスの提供をめざして、米国本社マイクロソフトコーポレーション（以下 マイクロソフト）と協力し、Windows Defender ATP と NTT セキュリティ・ジャパン株式会社のセキュリティオペレーションセンター（以下 SOC）で培った高度分析技術を連携することで、高機能な「EDR」のサービスの提供が可能となりました。

ICT 環境上でサイバー攻撃を検知するポイントの割合



NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区大手町 2-3-1　大手町プレイスウエストタワー
OTEMACHI PLACE WEST TOWER 2-3-1 Otemachi, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

2.「EDR」の特長

サーバーや PC 端末上のエンドポイントセキュリティ対策製品と SOC が独自に保有する脅威インテリジェンス※3 を連携することに加えて、SOC のリアルタイムな相関分析プロセスと連動させることで、エンドポイントにおけるサイバー攻撃への防御力の強化および検知精度の向上、さらに高精度な分析結果にもとづいた感染 PC 端末の迅速な隔離を実現できます。これによりお客さまは、ICT 環境全体におけるサイバー脅威の低減および被害拡大の抑制が 24 時間 365 日可能になります。また、働き方改革の浸透により拡大するリモートワークなどのオープンな ICT 環境においても、未知のサイバー脅威の早期発見・対処が可能です。

（1）サイバー脅威の早期発見

Windows Defender ATP の API を活用することにより、マイクロソフトがアップデートする脅威情報、SOC 独自の脅威インテリジェンスをシグネチャ化したカスタム IOC※4 を連携させ、リアルタイムな相関分析を実現することで、エンドポイントで起きているアクティビティ（ファイルやプロセスの挙動、レジストリ変更、通信情報など）とサイバーキルチェーン※5 における一連の攻撃プロセスを関連付けて分析することができ、ICT 環境でのサイバー脅威の早期発見を可能にします。

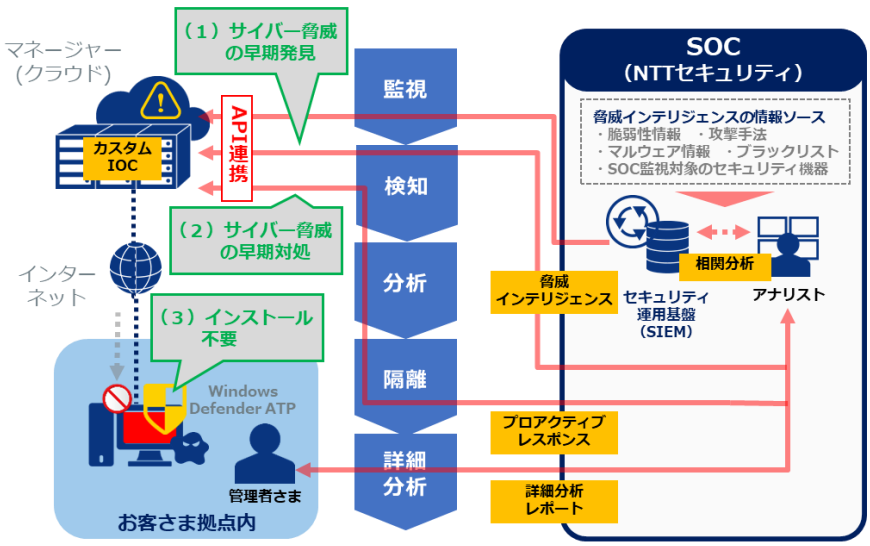
（2）サイバー脅威の早期対処

SOC 独自の脅威インテリジェンスやリアルタイムな相関分析を用いた高度な分析により、感染端末を特定し、オペレーターが遠隔から隔離します（プロアクティブ レスポンス）。これにより、お客さまセキュリティ担当者が不在となる、夜間や休日における被害拡大を防止することができます。

（3）インストール不要の Windows Defender ATP

Windows Defender ATP は、お客さまの PC 端末やサーバーにおいて、ライセンス追加することでアクティベートでき、簡単に導入できます。Windows10 を利用中もしくは利用予定のお客さまのセキュリティ強化に最適です。

<利用イメージ>



4．提供範囲および提供開始日

2019 年 2 月 12 日より日本国内で提供開始

※日本国内にてご契約されているお客さまの海外拠点へも提供可能です。

5．利用料金

個別見積りにつき、詳しくは営業担当者までお問い合わせください。

6. 日本マイクロソフト株式会社

チーフ セキュリティ オフィサー(CSO) 河野 省二 氏からのコメント

このたびの NTT Com による Windows Defender ATP を活用したエンドポイントセキュリティ対策の発表を、心より歓迎します。サイバーセキュリティの課題は増える一方で、人材不足は永遠の課題です。企業が個別のセキュリティ対策を行うのではなく、役割分担と情報共有が必要な時代となりました。マイクロソフトは自社のセキュリティサービスを API として公開し、インテリジェンスを提供することで、さまざまな分野で強みを持つパートナー企業さまとの連携を強化しています。マネージドセキュリティ事業者として NTT Com が培ってきたセキュリティスキルとインテリジェンス、そしてマイクロソフトのセキュリティ API が、企業のセキュリティ担当者の負担を軽減し、これまで以上に広い視野で安心できる IT 環境が構築できると確信しています。

※1：「EDR」は、「Endpoint Detection and Response」の略。エンドポイント（Endpoint）で脅威を検知（Detection）して、対応（Response）を支援する意味であり、エンドポイントにおける脅威の動きを包括的に可視化し、ハッキング活動の検知・観察や記録、攻撃遮断などの応急措置といった機能を提供します。

※2：従来のマルウェアによる攻撃では、メールや Web サイト経由で「.exe」などの拡張子を持つ実行ファイルとして、マルウェアを PC のディスク上に保存させる手法でしたが、ファイルレスマルウェア攻撃では、従来の実行ファイル形式のマルウェアを使用せず、簡易なプログラムなどによって OS のシステム管理機能を呼び出すことでサイバー攻撃を開始します。

※3：脅威インテリジェンス（Threat Intelligence：スレットインテリジェンス）とは、脅威の防止や検知に利用できる情報の総称です。脅威インテリジェンスの活用によって、従来のセキュリティ対策では見逃されていた高度なサイバー攻撃の検知、特定の業界・業種を標的とした巧妙なサイバー攻撃の防御が可能となります。

※4：IOC（Indicator Of Compromised）とは、セキュリティ機器などにおいて攻撃パターンを定義した一連のファイルのことです。

※5：サイバーキルチェーン(Cyber Kill Chain)とは、標的型攻撃における攻撃者の行動(攻撃の手順)を構造化したフレームワークのことです。具体的には、「偵察」「武器化」「デリバリー」「攻撃(エクスプロイト)」「インストール」「C&C(遠隔操作)」「侵入拡大」「目的実行」に分類されます。

攻撃のステップが鎖のように連鎖し、各ステップが移行するにつれ、深刻度が増していく中、なるべく早い段階で攻撃を検知し、このキルチェーンのいずれかの段階で脅威を断ち切ることで、攻撃の最終目的を防げます。