NTTアドバンステクノロジ　UTM SOCサービス プラスEDRオプション

境界防御とエンドポイント監視のトータルソリューション「UTM SOCサービス プラスEDRオプション」

新たなワークスタイルとして定着してきているリモートワークや高度化／巧妙化するサイバー攻撃に対応するため、これまでの社内と社外の境界でセキュリティ脅威を防御する境界型に加えて、端末（エンドポイント）でのセキュリティ対策が必要になってきています。NTTアドバンステクノロジ（以下、NTT-AT）では、統合脅威管理製品UTM※1を監視する境界防御型セキュリティと、EDR※2によるエンドポイント監視を組み合わせた監視トータルソリューションとして「UTM SOCサービス プラスEDRオプション」を提供しています。UTM及びEDRについては、お客様の要望に応じて様々な組み合わせが可能で、これにより働く環境に依存しないセキュリティ対策を実現することが可能になります。またNTT-ATは自社のICT-24 SOCを活用した24×365の監視運用サービスで手厚くサポートします。

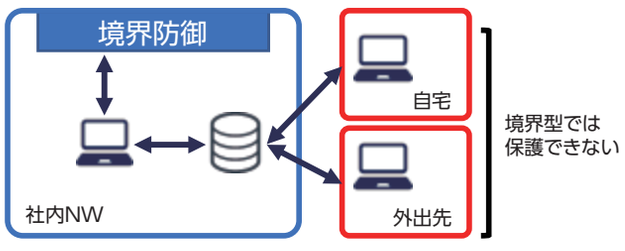
※1 UTM：Unified Threat Management
※2 EDR：Endpoint Detection and Response

エンドポイントセキュリティ対策が不可欠に

近年、サイバー攻撃は高度化／巧妙化しており、その結果、従来のファイアウォールなどのネットワーク通信向けの境界型防御をすり抜けての端末への攻撃が増加しています。さらに、コロナ禍でのリモートワーク環境の普及により、社内ネットワークに接続していない端末から、社内のリモートアクセス環境を経由した攻撃の可能性がでてきています。このような高度化／巧妙化するサイバー攻撃に対応するためには、従来のようなネットワークの内外の境界上で不正な通信を遮断する境界防御型セキュリティ対策だけでは不十分で、個々の端末の振る舞いに着目したエンドポイントのセキュリティ対策が不可欠となっています。

しかし一方で、個々のエンドポイントを管理するための運用業務の負担増も大きな課題となっています。

このような課題を解決し、ニューノーマル時代の働き方改革に向けたセキュリティ対策をトータルに支援する「UTM SOC サービス プラス EDR オプション」を提供しています。



テレワーク等により業務環境が多様化したことで、
境界防御だけではセキュリティが担保できない状態に

図１　境界防御型セキュリティ対策の限界

境界防御とエンドポイント監視のトータルソリューション「UTM SOCサービス プラスEDRオプション」

本ソリューションは、（1）EDR 監視サービス、（2）UTM SOC サービス、（3）オプションサービスの 3 つのサービスからなり、高度な SOC 監視・運用を 24 時間 365 日提供している ICT-24 セキュリティオペレーションセンター（ICT-24SOC）にて、UTM に加えてエンドポイント等の SOC 監視を実施し、脅威を検知した場合には、必要なポイントにて迅速にブロックリストを更新することで被害の拡大を防止します。また、エンドポイントのセキュリティパッチの状況把握などの管理運用業務も提供します。

（1）EDR 監視サービス

端末上の異常を EDR で監視します。多数の端末があっても、監視情報はクラウドで集中管理し、異常を検知した際には、端末の分析に必要な情報を提供するとともに、必要ならば端末からの通信を遮断するための隔離作業を実施します。

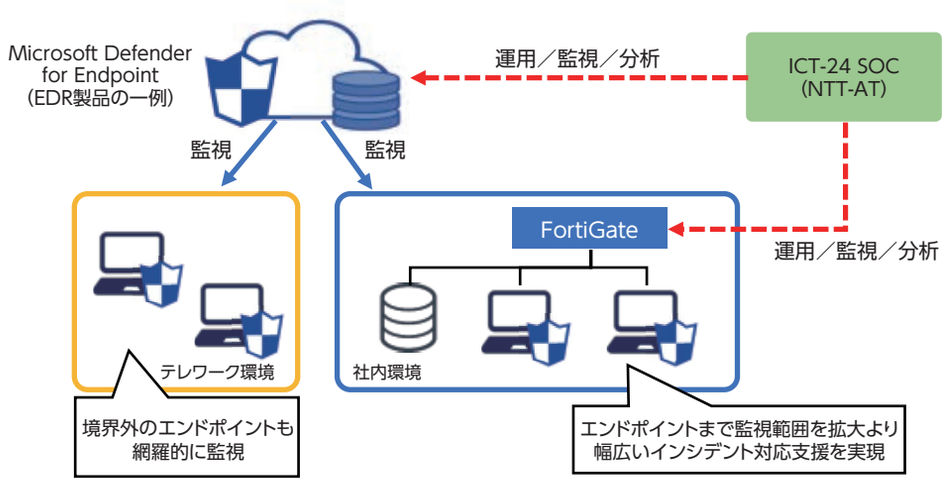


図２　トータルソリューション例「FortiGate SOC プラス EDR オプション」

専門知識をもったアナリストがリスク分析と、推奨する対応をお客様に提示する初動対応支援サービスや端末の詳細解析をするフォレンジックサービス、大規模向け SIEM（Security Information and Event Management）監視、インシデントに備えた訓練サービスなど、セキュリティに関連する高度なサービスをワンストップで提供します。

お客様の要望に応じて様々な UTM と EDR の組み合わせが可能（端末 100 台あたり税込月額 27 万 5000 円から）で、具体的なソリューションとして「FortiGate SOC プラス EDR オプション」などをご提供しています。

①重大なインシデントを確認した場合は、推奨する対策をお客様に通知し、端末の隔離を実施します。
②お客様から依頼があった場合、除外設定などセキュリティ設定を ICT24-SOC にて代理設定が可能です。

EDR 製品としては、「Microsoft Defender for Endpoint」、「FireEye HX シリーズ」などへの対応が可能です。

(2) UTM SOC サービス

お客様環境の UTM を監視し、最新のシグネチャー状態の維持、インシデントの早期発見、定期的なレポートを安価な価格で提供し、運用時には専門技術者がアラート分析とともに推奨する対策案を提示します。これにより、アラート発生時には迅速な対処と同時に、情報セキュリティ担当者の負担を大幅に軽減します。

UTM 製品としては、FortiGate、Paloalto などへの対応が可能です。今後、対応 UTM 製品を順次、追加予定です。

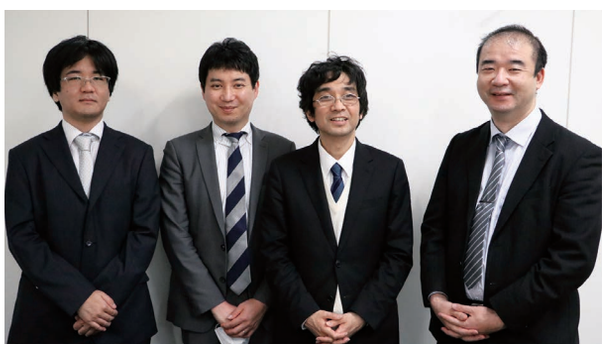
(3) オプションサービス

インシデント発生時には、リモートから問題となった端末のファイル（検体）を取得して、ふるまいを解析し、

今後の予定

コロナ禍でリモートワークが進む中、これまでのファイアウォールなどでオフィスの入口を守る境界防御型セキュリティから、リモートワーク環境も守り、そしてクラウドで守る時代への移行が進んでいます。このような中、NTT-AT ではゼロトラストセキュリティの実現に向け、クラウド PROXY、CASB(Cloud Access Security Broker) 等も拡大サポートしていく予定です。

また、ネットワークとセキュリティの新しいアーキテクチャーである SASE(Security Access Service Edge) を指向したクラウド型 UTM SOC の提供をはじめとし、さまざまなソリューションを展開していく予定です。



NTT アドバンステクノロジ
セキュリティ事業本部　SOC 担当

サイバー攻撃が高度化／巧妙化の一途をたどる中、ひとたび情報漏洩が発生すると、企業価値が大きく損なわれます。NTT-AT では、CISSP や情報処理安全確保支援士など高度セキュリティ資格を持ち、最新のサイバーセキュリティ動向に精通したアナリストが、お客様の大切な情報資産を守るお手伝いをいたします。お気軽にお問い合わせください。

お問い合わせ先
NTT アドバンステクノロジ株式会社　セキュリティ事業本部　SOC 担当
E-mail：ict24soc-promo.tss@ml.ntt-at.co.jp　URL：https://www.ntt-at.co.jp/product/fortigate-soc/edr.html