［導入事例］

GREYCORTEX MENDEL

ネットワークの脅威を見逃さない

**一つのソリューションでネットワーク上の端末通信を全て可視化：**
GREYCORTEX 社の MENDEL は企業、政府、重要なインフラ向けの先進的なネットワークトラフィック分析、パフォーマンス監視、脅威検出、および深くまでのネットワーク可視性を提供するネットワークトラフィックアナライザです。

**User's Profile** 兵庫県庁

日本海と瀬戸内海の二つの海に接している兵庫県は、都市部から自然の豊かな地域まで擁する関西の要衝で「日本の縮図」といわれるほど多彩な気候と風土に恵まれています。兵庫県庁の情報企画課システム管理室は、県全域を結ぶネットワークの設備、県職員の PC の活用推進、県内の市町および県公社のセキュリティ対策推進など、県の ICT 政策の重要な業務を担当しています。

## 巧妙化するサイバー攻撃

近年、企業や官公庁等、特定の組織を狙ったサイバー攻撃が増加し、攻撃手法も複雑化・巧妙化しています。かつては不特定多数を対象にした攻撃が中心でしたが、最近は特定の組織を対象にして金銭や機密情報の搾取を試みる悪質な標的型攻撃が増えています。例えば、2018 年夏、初めて日本語のビジネスメールによる詐欺の被害が確認されました。今後 IoT 機器の脆弱性を突く攻撃や人工知能（AI）を用いたサイバー攻撃が、ますます増えると予測されています。このように新しい攻撃手法が続々と登場しているため、最新のサイバー攻撃に対するセキュリティ対策を固めることが、国内の企業組織にとって喫緊の必要不可欠な課題です。

兵庫県
企画県民部
情報企画課
システム管理室
室長
津川　誠司氏

兵庫県
企画県民部
情報企画課
システム管理室
主任
田中　健一郎氏

## 従来型ソリューションの限界

巧妙化するサイバー攻撃に対しては、多層防御が最も有効なセキュリティ対策と考えられています。多層防御とは、社内ネットワークが侵害されないように複数の層（入口・内部・出口）に防御を設置するアプローチです。多層防御とは、サイバー脅威の種類ごとに異なるセキュリティ製品を用意することではなく、様々なソリューションを統合して一元的に管理できる環境を整備することで、効果を最大限に発揮します。具体的には、マルウェア感染のリスクが低減し、インシデント発生時にも早期解決が可能になります。

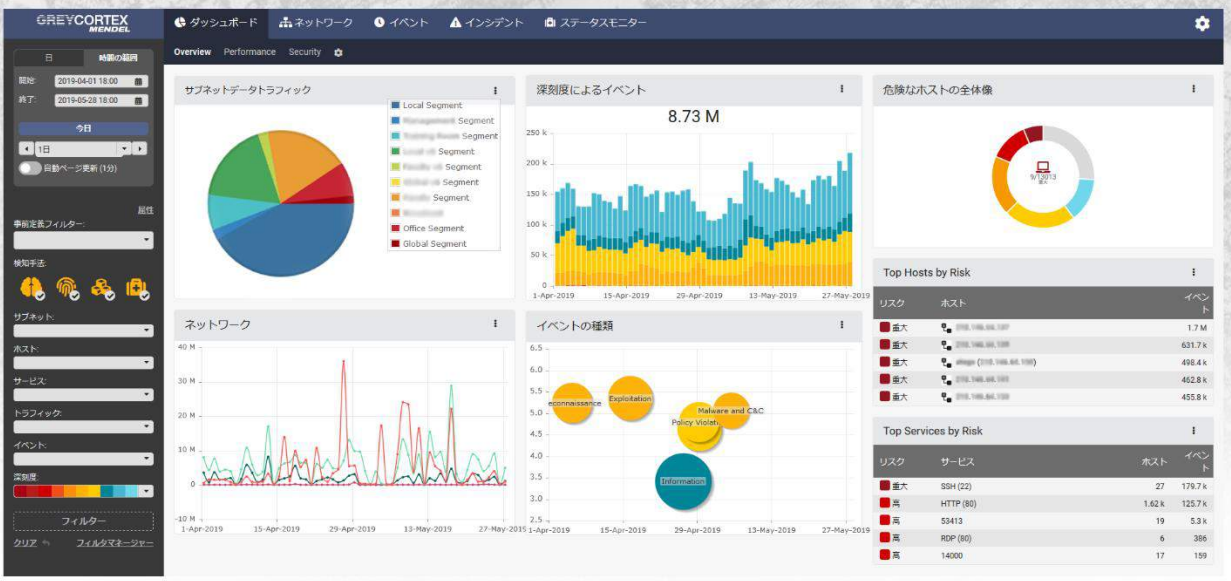
たとえば、社内の保護対象となる端末やネットワークが多様化する中、一つのセキュリティ対策ではもはや充分ではなく、目的に応じて複数の対策を使い分けていく戦略が必要です。だからこそ一般の端末と重要業務システムとが分離できるセキュリティ対策として、多層防御が最も適切だと考えられています。「たとえ多層防御を構築していても、有効に活用できていない企業や組織は多いと思います。最近、サイバー上の脅威が急増している傾向を踏まえると、やはり全体を俯瞰できる包括的なセキュリティ対策が必要になります。」と津川氏は語ります。

「多層防御を採用している組織では、エンドポイントやネットワークなど異なる領域で、各担当者が別々のセキュリティ製品を選定し、組織に導入してしまう可能性があります。その結果、担当者はそれぞれの製品を管理しますが、組織全体のネットワークの状況を一貫して把握できない場合が多いのです。複数のセキュリティ関連データを連続せずに分析すると、重要なリスクを見逃す恐れがあります。」と津川氏は説明します。

「ネットワークのセキュリティ対策が多様化することで、担当者による設定ミスのリスクが高くなるのは事実です。例えば、ネットワーク構築の単純ミスによるループ化は通信障害を招き、ネットワーク自体をダウンさせる恐れがあります。このような場合でも、IP パケットの生成ポイントである PC やサーバがその異常を検知せず、IT 担当者がネットワークの状況を把握できない環境では、ループの発生したポートを一時的に遮断できません。設定ミスの多くはネットワークに流れる情報の可視化によって、素早く検出できるようになります。」と田中氏は語ります。

## ネットワークの脅威を見逃さない MENDEL

兵庫県庁では多層防御の効果を最大化するセキュリティ対策として、GREYCORTEX 社の製品 MENDEL の導入を決定しました。MENDEL とは、機械学習とシグネチャを利用して、ネットワーク上のトラフィックのデータを継続的に収集し、複数の高度なネットワーク振る舞い分析手法やアルゴリズムを組み合わせて異常を検出する、最新型ネッ




**管理しやすい直感的なMENDELのインターフェイス**

トワークトラフィックアナライザです。

「GREYCORTEX 社の MENDEL は既知の攻撃手法や悪意のあるコードだけではなく、従来のセキュリティソリューションでは検知できない最新型の脅威も検出できます。組織の外から侵入する新規の脅威に加え、内部の脅威も検出できます。たとえば、社内ネットワークへ侵入後に横方向の展開で感染拡大を図るラテラルムーブメント型の攻撃についても、リアルタイムで異常として検知できます。」と田中氏は説明します。

「シグネチャとディープパケットインスペクション（DPI）に基づいた検出だけではなく、MENDEL はネットワーク振る舞い分析（NBA）技術も活用しています。ネットワーク振る舞い分析はシグネチャ・ルールベースの検出方法と異なり、機械学習を用いてネットワーク上を流れるトラフィックフローの振る舞いを分析し、正常なネットワークのモデルと比較することで、異常を検出します。ネットワーク振る舞い分析では、定義ファイルやルールのアップデートが不要で、従来の方法では検出が困難なゼロデイ攻撃のようなサイバー攻撃にも対応できます。MENDEL は、既存のソリューションでは見逃されてしまう脅威も、最先端のネットワーク分析手法を用いて、高い精度で検出します。」と津川氏は言います。

## ネットワークの全てを可視化できる MENDEL

「MENDEL のインターフェイスは直感的なので、経験の浅いセキュリティ担当者でもすぐに使えます。検出したインシデントの一覧表示から詳細の調査まで、操作手順が少なく扱いやすいです。また、個々の端末情報の事前登録なしに、ネットワークトラフィックや端末の監視を開始できます。ネットワークを完全に可視化できるため、端末にインストールしなくても、不審な振る舞いを検知した端末を画面上で特定することが可能です。」と津川氏は説明します。

「MENDEL では、サブネットワーク、端末および各端末上のアクティブなサービスの振る舞いがすべて可視化されるので、内外の不審なイベントだけではなく、ネットワークのパフォーマンスも常時監視します。パフォーマンスの異常を検知すると、設定ミスによるボトルネックなどの問題でも、ネットワーク上のどの拠点で発生しているか迅速にアラートが表示されます。大規模なネットワークをもつ企業組織にとっては、社内ネットワークの状況を常時監視するのにとても便利なツールです。」と田中氏は語ります。

さらに MENDEL の導入プロセス自体も簡単です。導入には通信データを収集するセンサーと分析を行うコレクターが必要です。コレクターはユーザの要件に合わせて、オンプレミスでの導入とクラウドサービスの利用のいずれかを選択できます。導入に必要な時間は 1 時間程度、必要な人員は 1 名です。

「兵庫県庁によるセキュリティ対策強化の一環で、ネットワークトラフィックアナライザ製品 MENDEL を利用しています。他のテクノロジーでは検出できない未知の脅威を、MENDEL は人工知能を利用して社内ネットワークトラフィックを多角的に分析するので、リアルタイムで検出できます。

また、国内のセキュリティ人材が不足している現状で、人手不足の企業にとっては、セキュリティ担当者の経験を問わず効果的に活用できる MENDEL はメリットが非常に大きいセキュリティソリューションです。さらに、費用対効果を考えると、とても効果的な製品だと毎日実感しています。」と津川氏は MENDEL を高く評価しています。

iSEC information security inc.
情報セキュリティ株式会社
URL　https://isec.ne.jp/
E-MAIL　inquiry@isec.ne.jp

◎神戸本社
〒650-0012 神戸市中央区北長狭通 4 丁目 9-26
西北神ビル 3 階（受付）・7 階・8 階
TEL ： 078-381-8980（代表） / FAX ： 078-381-8979
◎東京支社
〒103-0021 東京都中央区日本橋本石町 4 丁目 5-5 藤ビル 2 階
TEL ： 03-6271-8930（代表） / FAX ： 03-6271-8931