CUSTOMER SUCCESS STORY
導入事例

いわぎんリース・データ株式会社

ネットワーク可視化の重要性に着目 管理工数削減と 高精度の脅威監視を実現

Before

攻撃メールが増えており、標的型攻撃やランサムウェアへの対策が必要だと感じていたが、ログ監視の手法では手間がかかるうえ、脅威を見逃してしまうリスクがある

After

Deep Discovery™ Inspectorでネットワーク内部を可視化。顕在化した脅威の有無から、不正な通信に関与している端末までを的確かつ迅速に把握できるようになった

導入の背景

岩手銀行の創立40周年記念事業の一環として1972年に設立された、いわぎんリース・データ。リース事業、電算事業という2つの事業を柱としてビジネスを展開している。特に電算事業については、岩手銀行の情報システム部門のサポートを中心に、外部企業に向けてもシステム開発、運用保守、受託業務、IT機器の販売などといった幅広いサービスを提供している。

「Fintech」という造語が生まれるなど、金融業界では、顧客サービスの向上や新サービスの創出に向けて、積極的にIT活用を推進する企業が増えている。岩手銀行も例外ではなく、同社が果たすべき役割は、現在、ますます重要なものとなっている。

同時に同社に求められるのが、さらなるセキュリティの強化である。「積極的なIT活用とセキュリティ強化は表裏の関係です。より厳格な対策が必要になると考えています」といわぎんリース・データの大澤 義信氏は話す。

お客様の課題

特に強化が必要だと感じていたのが、標的型攻撃や、最近、猛威を振るっているランサムウェアへの対策だ。

「増加傾向にある攻撃メールの数からもリスクが高まっていることを感じていました。被害を防ぐために、UTM（統合脅威管理）やウイルス対策ソフトによって出入口とエンドポイントの対策を行うと同時に、定期的にファイアウォールのログを精査し、普段見慣れないIPアドレスにアクセスしている端末がないかなどを人手でチェックしていました」と同社の栗津 伸也氏は言う。

しかし、日々蓄積される膨大なログをチェックするのは非常に大きな手間をともなう。また、ログの精査には高度なスキルが必要なため業務が属人化しがちなうえ、人手で行う以上、攻撃の兆候を見逃してしまうリスクも大きい。

選定理由

そこで、同社が導入を決めたのがトレンドマイクロの「Deep Discovery™ Inspector（以下、DDI）」である。決め手になったのは、DDIが「内部対策」のソリューションであったことだ。

「検討を開始した当初は、どうにか侵入を防がなければならないとゲートウェイ型の製品ばか

›› いわぎんリース・データ株式会社

Webサイト
https://www.igcn.co.jp/

地域
岩手県、日本

業種
IT

従業員
122名

導入製品・ソリューション
- Deep Discovery™ Inspector
- ウイルスバスター™ コーポレートエディション

導入効果
- 標的型攻撃やランサムウェアへの対策を強化できた
- 出入口やエンドポイントでは検出できず、ネットワーク内部に侵入した脅威を可視化できるようになった
- UTMのログを通じて不正な通信を把握する方法に比べ、容易、かつリアルタイムに脅威の存在とリスクを把握できる
- 自社の実践で得たセキュリティ対策にかかわる知見を、顧客に提供していける体制が整った

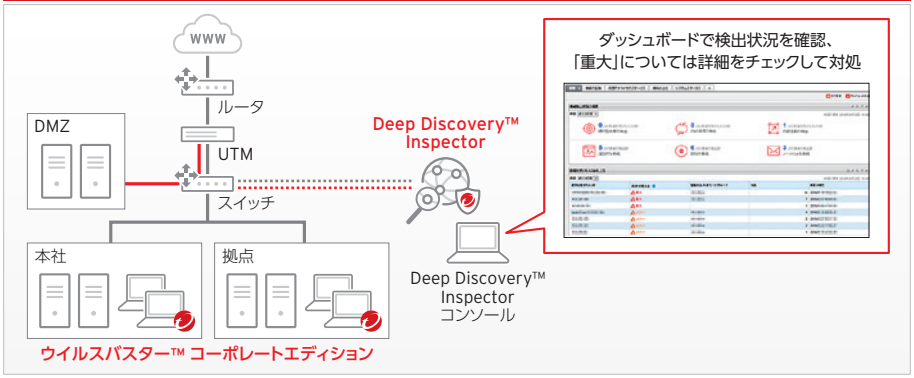
「『うちは大丈夫』という声も聞きますが、セキュリティ被害は『対岸の火事』ではありません。自社の経験をもとに、最適なセキュリティ対策をお客様に提案していきたいと考えています」

大澤 義信 氏
いわぎんリース・データ株式会社
理事
システムソリューション部長

「導入時はもちろん、運用開始後も担当者が定期的に訪問してくれ、様々なアドバイスをしてくれるトレンドマイクロの対応には、とても感謝しています」

粟津 伸也 氏
いわぎんリース・データ株式会社
システムソリューション部
サブマネージャー

いわぎんリース・データにおけるDeep Discovery™ Inspector活用イメージ



りを調べていました。しかし、DDIの存在を知り、ネットワーク内部を可視化して、ゲートウェイの対策をすり抜けて侵入した脅威の活動を捕捉する仕組みが必要だと気づいたのです」と粟津氏は話す。

また、同社では、かねてエンドポイントの対策として「ウイルスバスター™ コーポレートエディション」を利用してきた経緯もあり、トレンドマイクロのソリューションに対する安心感も導入を後押しした。

ソリューション

DDIは、ネットワーク内部を可視化するソリューションである。

近年、脅威は悪質化、巧妙化しており、パターンマッチングをベースとするタイプの対策だけでは、侵入を完全に防ぐのが困難になってきている。侵入した脅威は、ネットワーク内で徐々に準備を整え、ある段階で攻撃行動に移る。通常とは異なる端末間の通信や外部との通信など、怪しいふるまいを検知し可視化できるDDIを利用すれば、攻撃行動に移る前に対策を取ったり、被害が拡大したりすることを防ぐことができる。

コンソールは、一目で脅威の状況やリスクの大きさがわかるように工夫されている。検出した不正な通信などを「重大度」に応じて1～10にランク付けして、色分け表示するほか、ダッシュボード上では、C&Cサーバとの通信やランサムウェアの検出など、脅威の種類ごとに影響を受けたホストの件数がアイコンと共に大きく表示されるようになっている。

重大なものだけをピックアップできるのはもちろん、検出したすべての怪しいふるまいを一覧表示し、そこからドリルダウンして、関与している端末、初期侵入やC&C通信の開始など、脅威がどの段階まで進んでいるかを確認することも可能だ。

導入効果

DDIの導入により、いわぎんリース・データにおける脅威監視のあり方は大きく変わった。仮に、重大な脅威が検知されれば、DDIのコンソール上で一目で確認できるうえ、担当者にメールで通知されるようになっており、即座に対策が打てる環境が整った。

「さいわい、実害が懸念されるような脅威の検知には至っていませんが、これまで捉えきれなかった様々な攻撃を受けているという実態を把握することができました。例えば、ここ数年、頻繁に報告されている、bashの脆弱性を突くいわゆる“シェルショック”攻撃の検知や、ランサムウェアと見られる検知もあり、内部監視の重要性を改めて痛感しました」と粟津氏は語る。

同社では、こうしたDDIの提供する情報を軸に、必要に応じてUTMのログやIT資産管理ツールの情報も調査し、脅威の検出時に、どのユーザが、どんな操作を行った際に問題が発生したのかなどをトレースできるような運用の仕組みも整えている。

今後の展望

今後も同社はDDIを中核とした脅威監視を継続しつつ、運用プロセスを改善するなどしながら、さらに効率的で精度の高い体制を目指す予定だ。また、社内ネットワークの安全性に関する報告などを求められた場合には、DDIのレポートをエビデンスとすることも検討している。

加えて、様々な企業のIT業務を支援する立場から、DDIによる内部対策の重要性を顧客に伝えていくという。「我々自身、DDIで内部を可視化した結果、攻撃を受けている事実を改めて確認しました。最近、ランサムウェアが特に急増していると感じています。お客様や取引先にヒアリングしてみると、実際、ランサムウェアの攻撃を受けている企業は少なくありません。中には、金銭を支払ってしまい、実害を被った話も聞いています。まだ被害に遭っていないお客様にも、セキュリティ被害がもはや『対岸の火事』ではないことを積極的に伝え、私たち自身の経験も踏まえながらDDIをはじめとする適切なセキュリティ対策を提案していきたいと考えています」と大澤氏は意気込みを語った。

導入製品詳細

詳細については、下記にアクセスしてください
www.go-tm.jp/ddi

TREND MICRO™
Securing Your Journey to the Cloud

トレンドマイクロ株式会社
www.trendmicro.com

東京本社 〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
TEL.03-5334-3601（法人お問い合わせ窓口） FAX.03-5334-3639
名古屋営業所 〒460-0002 愛知県名古屋市中区丸の内3-22-24 名古屋桜通ビル7階
TEL.052-955-1221 FAX.052-963-6332
大阪営業所 〒532-0003 大阪府大阪市淀川区宮原3-4-30 ニッセイ新大阪ビル13階
TEL.06-6350-0330（代表） FAX.06-6350-0591
福岡営業所 〒812-0011 福岡県福岡市博多区博多駅前2-3-7 シティ21ビル7階
TEL.092-471-0562 FAX.092-471-0563