CUSTOMER SUCCESS STORY
導入事例

TREND MICRO

川口信用金庫

ネットワークを可視化
「侵入前提」の対策でサイバー攻撃に備える

Before

昨今のサイバー犯罪の状況や金融庁の指針から、侵入を前提とした対策の充実が求められているが、ネットワーク内部の状況が把握できていなかった

After

Deep Discovery™ Inspectorの導入によりネットワークを可視化。脅威を早期に検知し対処できるようになり、安心感が持てるようになった

導入の背景

大正13年に川口鋳物信用販売購買利用組合として設立され、平成26年に設立90周年を迎えた川口信用金庫。埼玉県南部を中心に45店舗を展開する地域密着に徹した相互扶助型の金融機関で、平成28年には本店を新築オープンした。

同金庫は、しんきん共同センターの社員金庫であり、勘定系オンラインシステムと一部情報系システムは、メインフレーム・サブシステムを共同利用。システム課では、勘定系・情報系の全システムの運用と保守、導入システムの企画、またPC150台、物理サーバ50台、シンクライアント500台などを管理する。

お客様の課題

川口信用金庫では、顧客の大事な情報資産を守ることを重点に置き、システム投資を進めてきた。しかし、昨今のサイバー犯罪の状況から、新たな投資の必要性を感じていたという。

「これまでは、ネットワークの入口とエンドポイントを中心にセキュリティ対策を行っていました。しかし、現在のサイバー攻撃は巧妙化、複雑化が進み、従来のセキュリティ対策をすり抜けてくるといいます。金融庁の指針でも、入口・出口・内部対策による『多層防御』が求められており、侵入を前提とした対策の充実、如何にして脅威を早期に検知し、初動を早め対応していくかが問われていました」（国分氏）。

また、ネットワーク内部に脆弱性がないかどうか、懸念もあった。同金庫では、複数のシステム、多くの業務アプリケーションが稼働している。利用するOSやミドルウェアも多岐に渡るが、アプリケーションとの整合性や動作保証の観点から、古いバージョンで利用する必要があったり、バージョンアップやセキュリティパッチの適用ができないなど制約がかかる場合も多く、セキュリティリスクが残る状況になっていた。

このままでは、脆弱性などを突いて侵入してくる脅威に気づくことができず、最悪の場合は、昨今世間を騒がせている大規模な情報漏えい事件の当事者になってしまうという危機感を抱いていたと国分氏は振り返る。

川口信用金庫

Webサイト
http://www.shinkin.co.jp/ksb/

地域
埼玉県、日本

業種
金融

従業員
804名（平成29年3月現在）

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

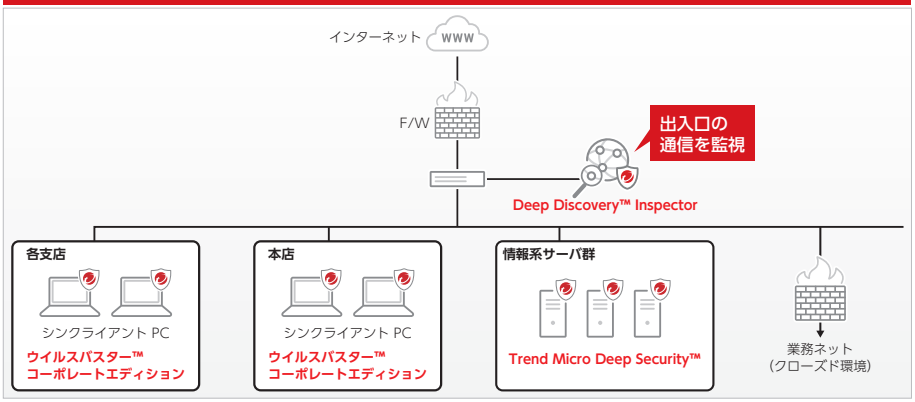
導入効果
- 金融庁の指針である「侵入を前提とした対策」へ対応した
- ネットワークに侵入した脅威を早期に検知し、対処できるようになった
- ネットワークが可視化され、脅威の状況を俯瞰することができ、自社のリスク評価をしやすくなった

前列左から　川口信用金庫 国分氏、同 中村氏　後列左から　トレンドマイクロ 水野、川口信用金庫 伊藤氏、同 富田氏、トレンドマイクロ 飯田

「セキュリティは、経営層含めて取り組むべき重要なテーマです。サイバー攻撃は巧妙化、複雑化しており、金融庁の指針からも侵入を前提とした対策が求められています。DDIの導入でネットワーク内部を可視化し、脅威の早期検知と初動対応の迅速化ができました。リスク評価もしやすくなっています」

国分 良孝 氏
川口信用金庫
事務集中部 システム課
課長

DDIを活用した川口信用金庫情報システム系ネットワークの監視イメージ



選定理由

こうした状況下、トレンドマイクロから提案を受けたのが、Deep Discovery™ Inspector（以下、DDI）だった。

「DDIという素晴らしい製品に出会いました」と言う国分氏は、選定理由のひとつとして、トレンドマイクロが専業セキュリティベンダーであり、知名度と技術力が高いことをあげる。

「海外では、超高度なサイバー攻撃に対して、その国の『軍』や、それに類する強力な組織が対応しています。攻撃する側もバックに大きな組織がいるケースが多く、『個』で対応するには限界があります。世界に通用する技術を有する企業の信頼できる製品を導入して、それを運用することは、有用な対抗手段であると考えました」（国分氏）。

また、同金庫ではエンドポイント対策製品として、ウイルスバスター™ コーポレートエディション (以下、ウイルスバスター)を利用しており、ウイルスバスターとDDIの連携による自動防御、さらに、他のトレンドマイクロ製品とDDIの連携によりネットワーク全体の防御力をより高めることができる点を評価した。

さらに、導入前にDDIを試用できたことも大きかったという。「トレンドマイクロは、いち早くDDIを試用する機会を設けてくれました。約１か月の試用後にいただいたレポートで、脅威の侵入がないことを確認できました。非常に有益で、安心して導入を決めることができました」と国分氏は振り返る。

ソリューション

ネットワーク内部を可視化するソリューションであるDDIは、「ネットワーク内で何が起きているのかを把握したい」という川口信用金庫のニーズに合致していた。

DDIは、ネットワークスイッチのミラーポートに接続し、勘定系以外の外向けの通信を監視するポイントに設置した。システム課の複数担当者が1日3回、DDIの管理コンソール画面で脅威の状況を確認している。

導入効果

導入効果について、国分氏は「安心感」を強調した。「この安心感は、ネットワーク内に危険なものが何もないことを確認できる安心感と、問題が起きたときに素早く把握して初動対応が取れるという安心感です。また、ネットワークが可視化されたことで、リスク評価がしやすくなりました」という。

また、DDIの管理コンソールが見やすい点を実感し、評価している。「コンソール画面のドリルダウン機能により、全体の状況を俯瞰しながら、詳細な情報まで閲覧することができます。また、トラフィックが異常に増えた時など、しきい値を超えた場合は、即時アラートをメールで受信できます。脅威に素早く気づき、対応することが可能です」と、管理、運用面での導入効果も感じている。

さらに同金庫では、統合型サーバセキュリティソリューション「Trend Micro Deep Security™」も導入し、「多層防御」をより強固なものとしつつ、セキュリティ対策をシングルベンダーにまとめることで運用の効率化を図っている。

今後の展望

現在、川口信用金庫では部署横断のセキュリティインシデント対応チームCSIRT（Computer Security Incident Response Team）を立ち上げている。DDIはCSIRTにおいても、脅威を検出するためのSOC（Security Operation Center）の中核を担うとしている。「お客様の情報資産を守ることを出発点に、今後もセキュリティ対策を充実させていきたい」と国分氏は語った。

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

TREND MICRO、Deep Discovery、Deep Discovery Inspector、ウイルスバスター、Trend Micro Deep Security、およびDeep Securityは、トレンドマイクロ株式会社の登録商標です。本ドキュメントに記載されている社名、製品名およびサービス名は、各社の商標または登録商標です。記載内容は2017年2月現在のものです。内容は予告なく変更になる場合がございます。
Copyright © 2017 Trend Micro Incorporated. All rights reserved.
[Item No. BR-CASE-182]

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