Soliton®

Zerona PLUS CaseStudy 導入事例

株式会社九州しんきん情報サービス 様

User Profile

株式会社九州しんきん情報サービス

所 在 地 ： 福岡県福岡市博多区博多駅前1-17-21 NTTデータ博多駅前ビル4F

九州地区にある27の信用金庫に対して、ソフトウェアの開発や運用、サポートを行う。1988 年の設立以来、「金庫の経営を様々な角度から支援する」「金庫経営の支援を通して地域経済発展に貢献する」などを企業理念とし、信用金庫の経営や事務の効率化など幅広い業務をシステムの面から支え続けている

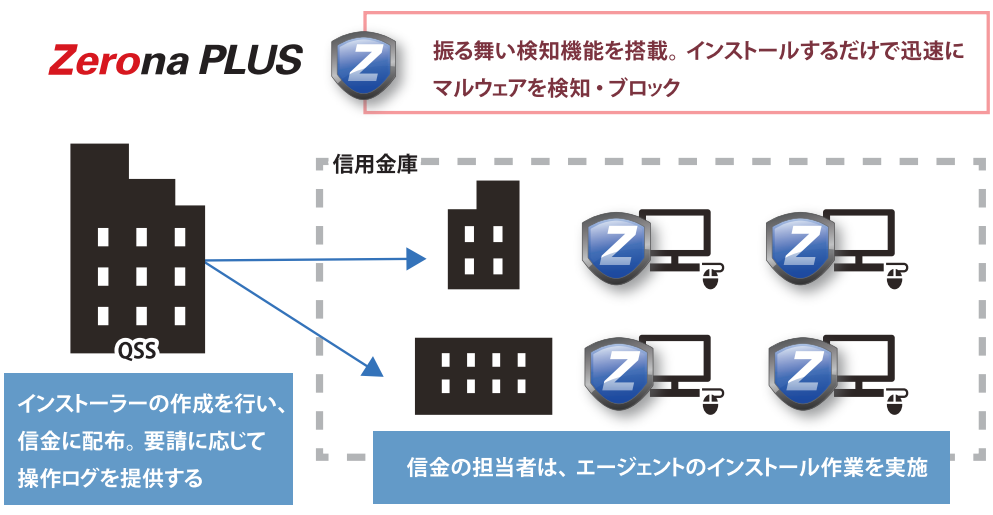
信用金庫ごとに異なる環境下のセキュリティを一斉強化
侵入を考慮した、被害を拡大させない仕組みづくりを実現

課 題	導入効果
1 侵入されることも考慮して、セキュリティ対策を強化したい	マルウェア対策とログ取得で、侵入を考慮した対策を実現 素早い被害状況の把握が可能に
2 インターネットやクラウドに接続できない環境でも対策したい	パターンファイルの更新なしでマルウェア対策を強化 オフラインの環境下でも最適な状況を維持
3 異なる利用環境下でも管理を簡単に行いたい	信金ごとに設定の管理ができるため、柔軟な対応が可能

九州しんきん情報サービス 様 利用イメージ図

信用金庫（信金）のエンドポイント対策強化を目的として Zerona PLUS を選定した。九州しんきん情報サービス（QSS）で基本設定を行ったエージェントインストーラーの準備を行い、端末への導入作業は各信金の担当者が行う。信金では、全台展開の前に一部でテスト運用を行い、既存ソフトとの共存を確認。必要に応じてQSS 側で検知除外の設定を行い、順次展開を進めている。

アラート発生時には信金から QSS へ連絡。Zerona PLUS では PC 操作ログの取得も行なっているため、信金からの要望に応じてアラート前の PC 操作ログを提供する。



九州しんきん情報サービス 様

侵入を防ぐ対策から 侵入を前提とした対策へ

株式会社九州しんきん情報サービス（以下、QSS）は九州地区にある27の信用金庫（信金）に対してソフトウェアの開発や運用、サポートを行っている。QSSでは、ITの力を駆使して各信金の業務効率化、顧客サービス向上を進めるとともに、マルウェア対策にも力を入れている。ソーシャルエンジニアリングを駆使した標的型攻撃や未知のマルウェアから、各信金が持つ膨大な顧客情報データを守るため、セキュリティのさらなる強化を検討し始めた。

九州しんきん情報サービス
営業開発部
開発課
課長
嶋田 秀一郎 氏

「これまでは出口・入口対策の強化など、侵入を防ぐことに重点を置いていました。しかし、信金業界のネットワークが閉域であっても、侵入される可能性はゼロではありません。そのため、これからは侵入されることを前提とした対策にも力を入れたいと考え、製品を探していました」

QSSの営業開発部 開発課 課長 嶋田秀一郎氏は、導入に至った背景をこう述べた。さらに、同課の課長代理 塚本泰之氏は今回の導入を後押しした事柄を次のように紹介する。

「ちょうど同じ時期に、振る舞い検知機能を持った製品を導入してほしいという声が各信金からも挙がっていました。少人数で情報システム部門を運用している信金も多く、中には他部署と兼任している場合もあります。そのため、導入するのであればできるだけ担当者に負荷をかけずに運用できる製品にしたいと考えていました」

九州しんきん情報サービス
営業開発部
開発課
課長代理
塚本 泰之 氏

エンドポイント対策強化の必要性が高まってきたことから、プログラムの動作（振る舞い）からマルウェアかどうかを検知する、振る舞い検知機能を持った製品を導入する事とした。この導入により、標的型攻撃を受けたり未知のマルウェアに侵入されたとしてもすぐに察知し、対応する事ができる。振る舞い検知機能のほかに、次の4つが製品の選定条件として挙げられた。
(1) QSSがサポートする27の信用金庫ではネットワーク分離を進めているため、外部のインターネットに繋がなくても、最適の状態を保てる製品であること、(2) 各信金で異なる既存のアンチウイルスソフトと併用できること、(3) コストが抑えられること、(4) ライセンス数に柔軟に対応できることだ。

負荷のかからない運用、高い検知能力を実感

「ご紹介いただいたのが、ソリトンシステムズのマルウェア対策ソフトウェア、Zerona PLUSでした。いくつか検討した中で唯一選定条件を全てクリアしていた製品だったということもあり、導入を決めました」（嶋田氏）

検討から製品決定までは約半年ほどと、同様の製品を導入する時と比べ、早いスピードで進められた。同課 主任 岩尾亮平氏はソリトンシステムズの対応について次のように評価した。

九州しんきん情報サービス
営業開発部
開発課
主任
岩尾 亮平 氏

「問い合わせに対する反応も早く、滞りなく作業を進めることができました」

2017年5月より、Zerona PLUSの導入申し込みの受付を開始。現在は申し込みのあった信金から順次導入を進めている段階だが、ユーザー数は順調に増えている。11月現在では800ユーザー、年内には1,000ユーザーを越す見込みだという。塚本氏は、Zerona PLUSの導入過程と実際の動作について、次のように語る。

「インストーラーの準備はこちらで行いますが、実際に使用する端末にソフトウェアをインストールするのは各信金の担当者です。専任の担当者ではない場合や一人だけで運用・保守を行なっている場合もあるのですが、特にトラブルなくスムーズに導入が完了できたと聞いています。導入後については、パターンファイルに依存しておらず、パターンファイル更新や頻繁なフルスキャンも不要ということもあり、動作が重くなるなど端末に負荷がかかっている様子もありません。端末にZerona PLUSがインストールされていることに気づかない職員もいるため、導入前とほとんど変らない操作です」

2017年5月の導入開始より、半年ほど経つが過検知による大きなトラブルもない。

「年賀状用のソフトを、たまたまインストールしようとした社員がいたのですが、Zerona PLUSが検知してくれたので、驚きました」（塚本氏）

操作ログを活用して被害状況を確認

QSSではZerona PLUSが持つPC操作ログの取得機能を使用したログの提供も行っている。インシデントが発生した場合、各信金からの要請を受け発生時刻の前後2、3時間のPC操作ログを提供し、原因究明に役立ててもらうという狙いだ。このように、今後は侵入されることを前提として、インシデント発生時の対応を迅速かつ的確に行えるような対策に力を入れていくという。嶋田氏は、対策を考えるポイントは個人情報・機密情報を漏えいさせない仕組みを作ること、そして脅威から社内の情報資産を守ることだと話す。このポイントをおさえた上で、バックアップをとっておけばマルウェアに侵されてデータが破壊された場合でも、復元することができる。万が一情報漏えいなどのインシデントが発生した場合、被害状況を瞬時に把握できるよう、Zerona PLUSのようなPC操作ログ機能を持つ対策製品を導入しておくことも重要だそうだ。

九州しんきん情報サービス
営業開発部
部長
中野 道求也 氏

同部 部長 中野道求也氏は「Zerona PLUSの優れた検知能力に満足しています。ソリトンシステムズは国産メーカーということで顧客の要望を受けた場合、製品に反映できることが強みだと思っています。アップデートによる機能追加や強化に期待しています」と語ってくれた。

Soliton®
株式会社ソリトンシステムズ　https://www.soliton.co.jp/
〒160-0022　東京都新宿区新宿 2-4-3
TEL 03-5360-3811　netsales@soliton.co.jp
大阪営業所 06-6821-6777　福岡営業所 092-263-0400
名古屋営業所 052-217-9091　東北営業所 022-716-0766
札幌営業所 011-242-6111

このカタログは2018年3月現在のものです。仕様、デザインは予告なく変更することがあります。　CS-ZeronaPLUS-1803A