1825年に創業し大阪・関西を中心に展開する総合楽器店の三木楽器。同社は、XG Firewallの導入をきっかけに、エンドポイントのセキュリティ対策をIntercept Xへと更新し、Synchronized Securityを活用して、最小限のシステム管理者で最大限の防御と修復を実現し、コロナ禍の中で安全な社内外での働き方を実践している。

CUSTOMER-AT-A-GLANCE

MIKI GAKKI 三木楽器

三木楽器株式会社（MIKIGAKKI Co.,Ltd）

本社所在地	〒541-0057 大阪市中央区北久宝寺町三丁目3番4号
営業拠点	楽器店10店舗・直営音楽教室24会場・外販営業拠点 ほか
創業	1825年（文政8年）
会社設立	1956年（昭和31年）12月1日
代表者	代表取締役会長　古山 昭 代表取締役社長　三木 俊彦
資本金	2億5,000万円
年商	86億4,000万円（連結売上高）2019年6月期
従業員数	200名

事業内容
1）楽器・楽譜の販売
2）音楽教室の運営
3）音楽イベントの企画・制作
4）楽器修理、ピアノ調律ほかアフターサービス
5）楽器および付属品の開発、楽譜の出版
6）その他、音楽／楽器関連事業

Webサイト
https://www.miki.co.jp（コーポレートサイト）
https://www.mikigakki.com（オンラインショップ）

ソフォスソリューションズ
Synchronized Security

ソフォスのSynchronized Securityによるセキュリティ対策は、脅威解析センターによる詳細な分析や自動修復機能などにより、運用管理の大幅な負荷軽減に役立っています。

三木楽器株式会社
総務経理部（兼 システム管理室）
マネージャー 向井 陸 氏

1825年に創業し1888年から楽器販売業務をスタートした三木楽器株式会社は、大阪・関西を中心に多くのスタジオ、放送局、各種学校など音楽の最前線でのサポートや楽器専門ショップの立ち上げなど、専門性の高い顧客ニーズに応え続けている。同

社のビジネスをITで支えるシステム管理室は、総務部に所属する向井氏が中心となり担ってきた。限られた人員で運用するシステム管理室では、社員の利用する各種端末がリモートワークへと急速に移行する中で、セキュリティ対策を強化する必要に迫られていた。そこで、XG FirewallとIntercept Xを連携させたSynchronized Securityを活用して、最大限の防御と修復の自動化を実現し、一人ひとりの社員が安心してリモートワークを実践できる環境を整えた。

ビジネスチャレンジ

「UTM更新のタイミングでXG Firewallを提案してもらい自社にマッチしていると判断」

三木楽器の総務部で社内のITシステム全般を管理するシステム管理室を兼務している向井氏は、ソフォスのXG Firewallを導入するきっかけを次のように振り返る。
「2019年の後半に、UTMの更新を検討しはじめました。そのタイミングで、ITシステム機器の調達などをサポートいただいている株式会社ハイパー大阪支店から、ソフォス

のXG Firewallを紹介いただきました。当社は、10年以上前からソフォスのエンドポイント製品を採用していたので、更新するならば同じソフォスのUTMにした方が運用管理の効率化を図れると考え、決断しました」

音楽関連の事業を展開してきた三木楽器では、多くの社員がMacbookなどのApple製品を仕事で使ってきた。向井氏は「UTMをソフォスのXG Firewallに決めた理由は、マルチプラットフォームに対するエンドポイント製品の信頼度に加えて、エンドポイント対策をIntercept Xに更新することで、SynchronizedSecurityを活用できると判断したからです」と補足する。

Synchronized Securityは、XG FirewallとIntercept Xが連携し、エンドポイント、ファイアウォール、Wi-Fi、モバイル、メール、暗号化など広範囲に渡る豊富な保護機能を提供する。Synchronized Securityを活用することで、インシデント対応の自動化やセキュリティ状態の可視性も強化される。向井氏は「特にSynchronized Securityに期待したのは、詳細な解析処理でした。当社のITシステムは、限られた人材で多くの機器を管理しなければなりません。それだけに、セキュリティ対策を強化するためには、より安全で強固なテクノロジーを導入して、少ない人数でも全社員の端末を安全に利用できる環境を整備したいと考えていました」と話す。

テクノロジーソリューション

「Synchronized Securityの活用でEMOTETなど最新の脅威に備える」

2020年にUTMをXG Firewallに交換し、エンドポイントをIntercept Xに更新するプロジェクトを推進している最中に、コロナ

業務が急速にリモート化やクラウドサービスに移行していく中で、エンドポイントをIntercept Xに切り替える判断は正解でした。以前は、社内に端末がある前提でセキュリティ対策を構築していたので、そのままでは急速な働き方の変化には対応できませんでした」と振り返る。

Intercept Xは、導入された端末が社内でも社外でも、システム管理者がどこにいても、オンプレミスまたはリモートで混在しているデバイスでも、同じコンソールからすべてを容易に管理できる。コロナ禍でリモートワークが加速する現在にあって、働く場所に囚われないIntercept Xによる一元的なセキュリティ

管理は、限られた人材でITを管理する三木楽器のシステム管理室にとって、大きな安心となった。向井氏は「EMOTETに代表されるサイバー犯罪の脅威が増しています。当社では、コロナ禍の影響もあり店頭よりも通信販売の需要が高まっています。そのため、社員の端末にも、対応するお客様の個人情報などが一時的に保管されるケースがあります。こうした端末が、サイバー犯罪の被害に遭わないためにも、Synchronized Securityによる脅威の可視化と、管理や解析の強化は重要になります」と指摘する。

導入の成果

「コロナ禍の中でもリモートで確認できる脅威解析センターでセキュリティ対策を強化」

導入にかかった手間や時間について向井氏は「オンプレ版のエンドポイント製品からクラウド版のIntercept Xへの更新はとても簡単でした。リモートワークが急速に広がる中で、エンドポイント強化が円滑に実施できたことは、とても助かりました」と振り返る。Intercept Xには、悪意のある暗号化プロセスを検出してシャットダウンするランサムウェア対策テクノロジーが搭載されているので、ランサムウェア攻撃が組織に感染して大きな被害をもたらす前にブロックできる。またIntercept Xは、ファイルベース破壊型とマスターブートレコード破壊型のランサムウェアの両方を防止し、暗号化されたファイルはすべて安全な状態にロールバックされるため、在宅で働く社員の業務への影響を最小限に抑える。さらに、クリーンアップ後の詳細情報が表示されるので、システム管理室では脅威がどこに侵入したか、何に触れたか、いつブロックされたかを確認できる。

向井氏は「脅威解析センターで詳細な分析ができるので助かっています。以前は、ウイルスなどに感染した端末があると、私の方で引き取って、システムの初期化によって復旧していました。それが、自動修復により、システム管理室の作業が大幅に低減し、非接触での対応が可能になりました」と評価する。

今後の展望

「Webプロキシの検討や社員へのセキュリティ教育の強化に取り組む」

今後もリモートワークが続いていく中で、向井氏は社員一人一人のセキュリティ意識の強化が大切だと考えている。そのために「ソフォスの提供している従業員向けテスト / トレーニングのSophos Phish Threatの実施を検討しています」と話す。
Sophos Phish Threatは、自動化可能な攻撃シミュレーションや、効果的なセキュリティ意識向上トレーニングとトレーニング結果の分析を通じて、エンドユーザーにフィッシング攻撃のトレーニングやテストを実施する。
「EMOTETのような脅威から社員を守るためには、各自が不用意にメールの添付ファイルを開いたり、感染の危険性がある操作などをしないように心がける必要があります。そのためには、教育を通してセキュリティ意識を高めていくのが、効果的だと考えています」と向井氏は話し「リモートでのクラウドサービス利用などを安全にするために、Webプロキシの導入も検討しています。コロナ禍が続いていけば、VPNによる一括アクセスだけではなく、クラウドサービスやデータセンターへのダイレクトアクセスも増えます。そうしたアクセスを安全に守るためには、Webプロキシが必要になると考えています」と今後に向けた取り組みを語る。

「Synchronized Security による脅威の可視化と、管理や解析の強化は重要になります。また自動修復により、システム管理室の作業が大幅に低減し、非接触での対応が可能になりました」

SOPHOS