Security FREE　SOFT CREATE

高度なセキュリティ体制の構築に成功！

HITOWAホールディングスが導入した、高レベルのセキュリティ見守り番とは？

マルウェアEmotet（エモテット）をはじめとし、サイバー攻撃の手法はますます高度化・巧妙化しており、もはや攻撃を100%防ぐのは不可能な状況だ。そこで求められるのが、たとえ攻撃を受けたとしても、いち早く気がつき、状況を把握し、必要であれば速やかに対処を打つことだ。そのため社内にSOC※1 を立ち上げる企業が増えているものの、セキュリティに対する高度な知見を持ったスタッフが常に稼働していればならないなど、ハードルが高いのも事実だ。

生活総合支援サービスを展開するHITOWAグループでITを統括するHITOWAホールディングスでも、以前は同様の課題に直面していたが、ソフトクリエイトの「Security FREE」を導入。24時間365日のセキュリティ監視業務をプロのSOCチームに一任できたうえ、専門家の知見も得ることができ、社内の負荷を軽減しながら高度なセキュリティ体制の構築に成功した。本稿では、その経緯についてHITOWAホールディングスの担当者に話を伺った。

Security FREE » 導入事例
HITOWAホールディングス株式会社

グループ全体のセキュリティ体制への危機意識が強まる

幼年期から老年期まで、生涯を通して支える生活総合支援サービスを展開するHITOWAグループ。保育施設の運営を始めとする子育て支援、ハウスクリーニングを手掛ける「おそうじ本舗」や靴・カバンの修理サービスを展開している「靴専科」、「KEiROW」ブランドによる訪問マッサージ、「イリーゼ」ブランドによる介護事業など、人生のどのステージにおいても生活を豊かに過ごしていけるようなサービスを提供している。

そして同グループを横断して利用するシステムやインフラ、セキュリティを中心としたITを統括するのが、HITOWAホールディングスの情報システム部である。

同社 情報システム部の部長を務める井出 征希氏は、「最近ではDX推進など時代の変化にも俊敏かつ柔軟に対応すべく、企業経営に寄与することを意識しながら日々の業務に励んでいます」と話す。

HITOWAグループでは、人の手を介したサービスを提供していることから、多くの個人情報を抱えている。「このため、お客様よりお預かりした個人情報や、数千にも及ぶフランチャイズ加盟店の情報を保護することは、とりわけ重大な責務であると考えています」（井出氏）

現在、HITOWAホールディングスの情報システム部のスタッフは10人弱だが、グループ約8,000人のITインフラをこの少人数で支えている。

HITOWAホールディングス株式会社 情報システム部 部長
井出 征希氏

HITOWAホールディングス株式会社 情報システム部 運用保守課 課長
田中 浩二氏

HITOWAホールディングス株式会社 情報システム部 運用保守課 担当課長
高山和也氏

VPNの接続も含め数多くの従業員の業務を数名で管理する状況にあり、かねてより運用保守そしてセキュリティの課題を感じていた。

前職でもセキュリティ対策責任者を務めていた井出氏は、当時抱えていたセキュリティ上の課題についてこう語る。「いつどこで何が起きているのか、目に見えていないけれど何かが起きているかもしれない、しかしそれを証明する手段がない――という状況に危機感を抱いていました。そこにマルウェアEmotetの感染被害が国内でも広がったこともあり“もしウィルスに感染した際にその後の対策機能が未導入だったら、感染時の初動対応や恒久対処が後手に回るリスクがある”と考えるようになったのです」

スムーズに進んだ端末SOCとファイアウォールSOCの導入

このように「何か起きてからでは遅い」と考えたHITOWAホールディングスでは、最先端のセキュリティ施策を模索し始めた。

「入口出口対策など境界型セキュリティ対策は以前より実施していましたが、ゼロトラストセキュリティという新たなアプローチとなると、完全に穴を塞ぐのはもはや不可能です。そこで、もともと“24/365”でのSOC運用の必要性を感じていたのもあり、EDRの導入をはじめとするセキュリティ体制の見直しを進めることにしました」と、井出氏は振り返る。

こうしてセキュリティ対策を強化するために情報収集などを進め、SOC運用については自社での運用だけでなく、外部への委託も視野に入れてベンダーが提供するSOCサービスも検討したという。

「SOCサービスを提供するベンダーには一通り声をかけ、提案してもらいました。そうしたなか、以前からお付き合いのあったソフトクリエイトにも相談したところ紹介されたのが、「Security FREE」でした」（井出氏）

HITOWAホールディングスでは、5年ほど前よりサーバーリプレースなどでソフトクリエイトと取引きしており、現在ではヘルプデスクの運用も委託している。またセキュリティに関しても、入口出口対策の実施とともに、いまはVPNシステムのリプレースもソフトクリエイトに委託している。

HITOWAホールディングスが導入した、高レベルのセキュリティ見守り番とは?

前述のように、HITOWA ホールディングスでは他のセキュリティベンダーの提供する SOC サービスも検討したものの、ファイアウォールに対する侵入 SOC とクライアント PC に対する端末 SOC を同一ベンダーに委託することで、相関的な分析や対応が可能になるという狙いもあり、Secuirity FREE の導入を含めソフトクリエイトへの委託を決定した。

HITOWA ホールディングス 情報システム部 運用保守課の課長、田中 浩二氏は、「当社グループの IT 全般やセキュリティの仕組みを熟知しているソフトクリエイトに対し、新たなセキュリティシステムの構築から運用保守、そして SOC 運用までを一元的に任せることで、効率的な運用体制の構築を目指すこととしました」と語る。

こうして HITOWA ホールディングスでは、ファイアウォールのリプレースと EDR の導入を機に、セキュリティインシデントの早期発見を目的とした監視体制の構築を目指し Security FREE の導入へと動き出した。

Emotetによる被害を未然に防ぎ効果を実感

「攻撃の形跡を見逃さない」を旗印に掲げる Security FREE は、適切で迅速な対処と経営報告により、攻めのセキュリティ運用を支援する。24 時間 365 日のセキュリティ監視業務をソフトクリエイトの SOC チームに一任でき、また検知・解析した結果から脅威レベルを判定し、具体的な対処策を導き出すことで専門家の知見も得られるなど、数々の特徴を有している。

そんな Security FREE の導入からまだ日は浅い HITOWA ホールディングスだが、既にさまざまな効果を実感しているという。

井出氏はこう語る。「もし自社で SOC を構築し運用するとしたら、多大な初期投資とリスクが伴います。また高度なスキルを持ったセキュリティ人材も不可欠でしょう。そこで、Security FREE のようなセキュリティのスペシャリストによる SOC サービスを活用することで、情報セキュリティ対策と監視体制の強化を図れたことは、費用や運用の面からも大きな効果であり成果だと感じています」

実は HITOWA ホールディングスでも、ある端末が Emotet に感染するという事案が発生している。

田中氏は言う。「ある従業員が不審なメールの添付ファイルを開いたところ Emotet だったのですが、即座に SOC チームが検知し、“この端末が怪しい動きをしているので対処を”という指示をもらいました。結局、端末を確認したところ感染は広がっていなかったのですが、SOC サービスのおかげで被害を未然に防ぐことができました。」

井出氏もこう続ける。「“事象を把握しすぐに対策を打った結果、何も問題なかった”という経緯を上に報告できるというのはすごく大事なことです。脅威を検知した段階で最初にすべき打ち手を実施してから連絡してくれるので、安心できるのも Security FREE ならではの魅力でしょう」

さらに、同社 情報システム部 運用保守課の担当課長、高山 和也氏は「SOC サービス導入以前であれば、何か起きたと把握した際、感染元の解明や問題ないかのスキャンなど一連の調査を自分たちで行う必要がありました。しかし現在ではその多くをセキュリティのプロに任せることができるので、我々の負担軽減はもちろんのこと、セキュリティレベルの向上にもつながっています」と高く評価する。

社内CSIRTの立ち上げでセキュリティオペレーションの高度化を目指す

DX 推進に伴う IT 利活用の機会増大に備え、ゼロトラストを意識したセキュリティ対策として、Security FREE を導入した HITOWA ホールディングス。その効果を受け、グループ全社のシステムを統括する同社情報システム部内に、CSIRT（シーサート）※2 を設置し、インシデント発生時におけるより迅速な対応を目指している。さらにはソフトクリエイトの推薦により日本シーサート協議会への加盟も果たしたという。

「今後は、CSIRT の運用においても、Security FREE サービスを武器に、脅威に対して迅速に立ち向かうことのできる強固な体制を築いていければと考えています。また、ガバナンス強化に向けた IT 統制の整備を進めるとともに、サービスの高付加価値化や顧客満足度向上に資する DX を強力に推進し、そのために必要な投資も行なっていく予定です」と井出氏は力強く語り、インタビューを締めくくった。

※1　SOC (Security Operation Center)：
企業のインフラやネットワークを監視・分析し、脅威を検知した場合に、通知や対応策のアドバイスなどを行う専門組織。

※2　シーサート (CSIRT: Computer Security Incident Response Team)：
コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う。（出典：日本シーサート協議会）

HITOWAホールディングス株式会社

HITOWA GROUP

お問い合わせ

SOFT CREATE

株式会社ソフトクリエイト
SOFTCREATE CORP.

〒150-0002　東京都渋谷区渋谷2丁目15番1号　渋谷クロスタワー

お電話でのお問い合わせ　:03-3486-1520（電話受付時間 9:00-18:00）
製品のご相談　:https://www.softcreate.co.jp/solution/security/apply

HITOWAホールディングス株式会社
〒420-8601 東京都港区六本木1-4-5 アークヒルズ サウスタワー
https://www.hitowa.com/