CASE STUDY

セントラル短資ＦＸ、RSA NETWITNESS®を導入し セキュリティ基盤を万全に 充実の専門サービスを活用し、限られたリソースでも スムーズな導入を実現

インターネット時代の金融事業者、侵入を前提とした体制への進化を決意

FX（外国為替証拠金取引）は、インターネットの普及と共に、とりわけこの十数年ほどの間に大きく拡大し、個人投資家にとって、今や株式投資に並ぶ身近な金融商品となっている。そんなFXサービスを提供するセントラル短資ＦＸ株式会社(以下、セントラル短資ＦＸ)は、高度化するオンライン犯罪から顧客を保護すべく、様々なセキュリティ対策を講じてきたという。同社でそうした情報セキュリティ対策の最前線にあたるのが市場業務部である。清水　純部長は、今を遡ること2年ほど前から、「万一侵入を許したときの『中から中』、『中から外』の脅威対策の強化が必要と考えるようになった」と言う。現場の問題意識によって見直しが推進されたのは本件の特徴と言えるだろう。

とはいえ、市場業務部でこうした課題に取り組める要員は、清水氏の他には、桑原 優介氏と廣田　高氏のわずか二名しかいなかった。両名とも情報セキュリティを専任として担当していたわけでもない。しかも、同部が抱える課題には、Windows 7のサポート終了(EOS)問題なども含まれていた。

社外に目を転じれば、国際的なスポーツイベントの東京開催が決まったことで、サイバー攻撃の活発化が見込まれていた。当局からサイバーセキュリティに関するヒアリングを受けたのもこのころだった。その席で、「万が一問題事案が発生したときに適切なインシデント･レスポンス(以下、IR)について相談できる第三者機関とのつながりを持った方がいい」と助言されたことが、セントラル短資ＦＸとRSAの縁を結ぶきっかけとなったのである。

当局の助言や潜在的な組織のニーズにマッチしたRSA IRインシデントホットライン

自らの問題意識の高まりに当局の助言も加わって、新しいセキュリティ・ソリューションの選定･検討が始まった。その中でRSAと接点ができたのは、2018年10月に開催されたDell Technologies Forumでのことだった。IR対応をサポートする IRホットラインサービスについてはもちろんだが、併せて紹介された、社内のネットワーク空間を可視化するRSA NetWitness Platform(以下、NetWitness)も、IT分野のキャリアが長い清水氏の眼鏡にかなう存在だったという。

セントラル短資FX

セントラル短資ＦＸ株式会社は企業理念に『Quality FX～外国為替投資に、確かな答えを。』を掲げる国内有数の外国為替証拠金取引取り扱い事業者である。

インターネットとの親和性が高く、オンライン投資家の人気の高いこの分野で、100年以上の歴史に裏打ちされたセントラル短資グループの信用力や、最先端のアプリケーション、高度なセキュリティの提供によって、多くの投資家の支持を集めている。

その後、IRホットラインサービスは条件を満たした最適なサービスと判断され、導入に向けての動きが始まった。紹介を受けた翌月の11月中旬には正式に発注するという即断即決で、年明けの1月から利用が始まった。

ネットワークの可視化と端末のイベント監視をRSA NETWITNESSで統合

清水氏は、NetWitnessの選定についてもスピード感のある検討をされ、紹介を受けた同月末に開催されたワークショップに桑原氏、廣田氏を伴って参加している。このワークショップは、NetWitnessを使ったCTFコンテストが中心で、現実に想定される環境で発生した事案について検知や分析の実務を体験できるというものである。ワークショップに参加した桑原氏は、「この体験を通じて、NetWitnessであれば、今日の暗号化通信が前提となったネットワーク環境においても可視化、そして脅威の検知や追跡、調査が可能だと実感できた」と語っている。

なお、当初は、NetWitnessの可視化を担うRSA NetWitness Network(以下NetWitness Network)のみの導入が検討されていた。しかし、清水氏は、ワークショップに参加してRSA NetWitness Endpoint(以下NetWitness Endpoint)のある環境を体験したことで、これまで利用してきた端末のイベント監視(EDR)製品を刷新しようと考えたという。その理由は「可視化とEDRの統合効果に対する期待」と「既存製品の「効果への疑問」の二点。前者についていうと、NetWitness NetworkとNetWitness Endpointを連携させると、ネットワークの可視化と端末のEDRを統合運用できるので、脅威の検知･追跡がずいぶんとやりやすくなることがわかったのだという。後者については、当時社内の全PC(およそ150台)に導入されていたEDR製品は、3年ほどの運用期間の間で導入当初において数えるほどしか脅威を検知しなかったという。その結果を単純に鵜呑みにすることのリスクを感じたこともあって、端末のEDR機能に関し品質と効率で優ると見込めるNetWitness Endpointに刷新することを決めたのだった。

仮想アプライアンスとして導入することでコストの削減に成功

セントラル短資ＦＸのNetWitness導入計画で目を引く点の一つに、NetWitness Networkの仮想アプライアンス形態での導入がある。NetWitness Networkは、従来から最適に調整された「ハードウェアアプライアンス」として提供されている。顧客がこの形態で導入することには、必要なリソースに頭を悩ませることなく手軽に導入できるというメリットがある。一方で、顧客の用意する環境に仮想アプライアンスとして導入する形態も選択できる。「ハードウェアを伴わない『仮想アプライアンス形態』が選べたので、導入コストがかなり削減できた」と清水氏は語った。

導入に先立って実施されたPoCでは、取り立てて問題は起きなかったという。同社の環境に即したデータの収集環境を整備してしまえば、日常の運用でしなければならないことはほとんどなく、一ヶ月のPoC期間のうちで、NetWitnessを操作したのは、ほんの一週間ほどだったという。実際に脅威の侵害が確認されたわけではなかったこともあって、「思った以上に導入に関するハードルが低いことを実感した」(清水氏)というほどだった。

仮想アプライアンス提供を選んだことで、実装に際して負担が増えるといったデメリットに悩まされることもなかった。後述の導入支援サービスを利用したこともあって、環境の準備から実装まで、リスクや負担を感じることなく終えられたのだという。リソースの準備も、3ヶ月分のデータ保全などの要件を満たすリソースを用意するだけだった。しかも、「導入後に求められたリソース量が実際に必要とした量とほぼ一致したので感心した」と清水氏は語っている。

“万一侵入を許したときの『中から中』、『中から外』の脅威対策の強化が必要と考えた”

“NetWitnessに今のところまったく不満はない。高い水準で要求を満たしてくれている”

– 清水 純氏

充実した関連サービスを活用して、たった3人で導入できた

セントラル短資ＦＸのNetWitness導入計画で目を引くもう一つの特徴が、関連サービスの積極的な活用である。限られた人数の、しかも情報セキュリティの専任ではないスタッフで導入･運用していくために、メンバーの学習曲線の最適化と日々の運用負荷の軽減を目指したためだという。同社は、すでに述べたIR ホットラインサービスの他、以下の3つのサービスを利用している。

- エデュケーションサービス……NetWitnessの基礎知識から基本的な使用法までを体系立てて学べる教育プログラム
- IRジャンプスタート サービス……RSAのエキスパートによるオンサイト型の導入支援サービス。自社環境に即した高度なチューニングを行うだけでなく、運用や調査に対する助言も得られる。
- マネージドセキュリティサービス……MSSプロバイダとして定評のある株式会社ケイズの提供によるエンドポイント監視サービス

最も評価が高かったのは、導入を支援するIRジャンプスタート サービスだった。先述の仮想アプライアンス形態での導入が容易だったのも、このサービスが貢献している。また、運用担当の桑原氏は、IRジャンプスタート サービスを利用したことで、プロフェッショナルによる手本を学んだ上で運用を始められた点を評価した。「自分たちだけでは、今のようには運用できていないでしょう。プロによる実務に即した考え方と手法を隣で見て学べたことは、とても助かった」と振り返った。

“自分たちだけでは、今のようには運用できていない。プロによる実務に即した考え方と手法を隣で見て学べたことは、とても助かった”

– 桑原 優介氏

文字通りの教育プログラムであるエデュケーションサービスについても、NetWitnessの運用に必要不可欠な情報を短期間で理解できたおかげで、IRジャンプスタート サービスで得られる知見をキャッチアップできたという。桑原氏と共に運用を担当する廣田氏にも、「NetWitnessを導入することで得られる情報量はとても多いので、エデュケーションサービスやIRジャンプスタート サービスを利用していなかったら、どこから手を付けたらいいか、わからなかったと思う。併用をお奨めします」と両サービスの価値を高く評価いただいた。

“得られる情報量がとても多いので､エデュケーションサービスやIRジャンプスタート サービスを利用していなかったら､どこから手を付けたらいいか、わからなかったと思う”

– 廣田 高氏

高い水準で要求を満たしてくれたNETWITNESSとRSA

「製品としてのNetWitnessに、今のところまったく不満はありません。高い水準で要求を満たしてくれています」と、清水氏からは望外の高い評価をいただいた。廣田氏や桑原氏からも、さらに「社内ネットワークの障害発生時の原因の切り分けなど、情報セキュリティ領域以外の用途にも役立っている」とお褒めの言葉をいただいた。清水氏からは、それに加えてRSAの顧客サポートに対しても高い評価をいただけた。実は、導入後に不幸にして仮想環境にハードウェア障害が発生し、一時的に同社のNetWitness環境が失われるという事故が発生した。再構築は同社自身の手で行うこととなったが、その際の電話問い合わせへの対応など、RSAの手厚いサポートに助けられたと言っていただいた。

最後に、清水氏に今後の課題について尋ねたところ、「ログ監視の強化に取り組む」との答えが返ってきた。「NetWitnessの導入目的である『脅威の検知と影響範囲の正確な把握』という目標を、より高い水準で達成するためには、(NetWitnessのSIEM機能を担う)RSA NetWitness Logsのような製品によるログ監視の強化が必要だと考えています」(清水氏)

もちろん、セントラル短資ＦＸの新たなチャレンジのお手伝いしていきたいと願うRSAである。

RSAについて

RSAはBusiness-Driven Securityソリューションを提供し、さまざまな組織が、統合的な可視性、自動化されたインサイト、および組織的なアクションを使用してデジタルリスク管理のための統合的なアプローチを採用できるようサポートしています。RSAのソリューションは、高度な攻撃の効果的な検出と対応、ユーザー アクセス制御の管理、さらにビジネス リスク、不正行為、サイバー犯罪の削減を目的として設計されています。RSAは、世界中の数百万人のユーザーを保護し、Fortune 500の企業の90%以上が成功し、革新的な変化に継続的に適応できるように支援しています。詳細はrsa.com/ja-jpをご覧ください。