

# 社内情報基盤の安全性を検証すべく フルスコープのRed Teamテストを実施 システムや人を狙った攻撃に 適切に対処できることを実証

お客様名：株式会社北國銀行  
資本金： 266億7300万円  
設立： 1943年12月18日  
本店所在地：  
石川県金沢市広岡2-12-6  
URL: [www.hokkokuibank.co.jp](http://www.hokkokuibank.co.jp)

## ソリューション

Red Teamテスト(フルスコープ)

## プロジェクトのゴール

管理者権限の奪取や  
疑似マルウェアの実行・情報奪取、  
物理侵入等、最近の脅威などを  
考慮してゴールを設定しました。

## プロジェクト実施期間

2022年9月～12月



## デジタル技術をフル活用し 先進的な金融サービスを展開

北國フィナンシャルホールディングス(以下、北國FHD)の中核企業である北國銀行は、石川・富山・福井の北陸三県を中心に事業を展開する地方銀行である。同行では1943年の設立以来、地域のリーディングバンクとして個人／法人顧客の多様な金融ニーズに対応。産業や暮らしを支える重要な役割を担い続けてきた。中でも注目されるのが、先進デジタル技術によるビジネス変革を積極的に推進している点だ。社内業務のペーパーレス化や地域のキャッシュレス化にいち早く取り組んだほか、勘定系システムのオープン化／フルクラウド化も他行に先駆けて実施。こうした取り組みが評価され、2021年には経済産業省が定める「DX認定事業者」の認定も取得している。

顧客の重要な資産を預かる業種だけに、サイバーセキュリティ対策にも抜かりはない。「当セキュリティグループでは、メール／エンドポイントの監視や各種アラートへの対応など、セキュリティに関わる業務を幅広く担当。不審な行動を早期に検知・対処できるようにしています。また、当社では多くの業務システムを内製化しているため、開発業務の初期段階から関わってセキュリティ面での安全性を担保する『シフトレフト』の取り組みも進めています」と語るのは、北國銀行 システム部 セキュリティグループ 松井 千明氏。また、同グループ 田村 寿乃氏も「セキュリティを守る上では、人の意識も重要なファクターとなります。そこで、職員への教育・啓発活動に力を入れると同時に、最新のセキュリティ情報を周知するための掲示板なども運営しています」と続ける。

## セキュリティ対策の実効性を確認すべく 国内で豊富な実績があり、物理侵入も含めた フルスコープでのテストができる セキュアワークスにRED TEAMテストを依頼

さらに今回、同行では、社内情報基盤を対象としたRed Teamテストを実施した。現在は北國FHDグループのコンサルティング企業である株式会社CCイノベーションに籍を置く丸金 正和氏(プロジェクト実施当時は北國銀行 システム部 セキュリティグループ)は、その背景を「これまでツールを用いたセキュリティ診断などは行ってきました。とはいえ、高いハッキング技術を持つ攻撃者に実際に攻撃されたらどうなるかまでは分かりません。そこで、何らかの形でテストを行いたいとは常々思っていたのですが、一般的な攻撃シナリオに基づくTLPT(脅威ベースのペネトレーションテスト)などだと、本当に弱い部分が見えてこないおそれもあります。このため、なかなか実施までには踏み切れませんでした」と振り返る。

加えて、セキュリティは、どこまでやれば十分なのか非常に難しい分野でもある。コストを掛けようと思えばいくらでも掛けられるが、それが果たして適正なのか判断がつきにくい。この点も大きな悩みだったとのこと。丸金氏は「我々も様々なベンダーと相談しながら環境を作り上げてきました。しかし、複数のソリューションを組み合わせるわけですから、どこかに抜け・漏れがあるのではないかとこの懸念が完全には払拭できない。かといって、自分が気付いていないことを認識するのも無理な話です。何かこれまでの対策の実効性を確認するいい手はないものかと感じていました」と続ける。

こうした状況を変えるきっかけとなったのが、セキュアワークスからの提案であった。「たまたまセキュアワークスと話をしていた時に、Red Teamテストのサービスをやっていると紹介を受けました。内容を詳しく聞いてみると、国内でも豊富な実績がある上に技術力面でも信頼が置けそうでした。こちらの質問や要望に対しても真摯に向き合ってくれましたし、物理侵入も含めたフルスコープでのテストも可能とのこと。これなら、我々が知りたいことを明らかにできると確信し、すぐに実施することを決めました」と丸金氏は語る。

## システムや人を狙った攻撃に 適切に対処できることを実証

実際にテストを行うにあたっては、セキュアワークスのアドバイザーも積極的に活用。たとえば物理侵入については、関連部署とあらかじめ情報共有を行うなどして、無用なトラブルを招かないようにした。「ただし、それ以外の部分では、平常時と特に違った態勢は敷いていません。あくまでも普段通りの状況の中で、インシデントにきちんと対応できるかどうかを重視しました」と丸金氏は語る。

約2ヶ月にわたるRed Teamテストの結果、得られた成果も多かったとのこと。「まず一点目として、これまで行ってきたシス

テム的な対策が十分に機能していると確認できた点が挙げられます。各種ツール類の設定などについても、相当頑張って煮詰めてきましたので、これが実証できたことは大変良かった。セキュアワークスの担当者から、『様々な手法で攻撃を仕掛けたものの、なかなかうまくいかず苦労しました』と言ってもらえたことも、大きな励みとなりました」と丸金氏は語る。

また田村氏も「もう一つのポイントが、標的型攻撃メールへの対応がきちんと行えた点です。セキュアワークスのフィッシングメールを受け取った社員からは、すぐ『おかしなメールが来ている』とエスカレーションがありました。不審なメールは開かず報告して欲しいと日頃から訴えているのですが、そうした地道な活動が実を結んでいたのは大変嬉しかったですね」とこやかに語る。

ちなみに、今回のRed Teamテストでは、思わぬエピソードもあった。丸金氏は「テスト期間中に検知したある攻撃が、Red Teamテストの実施によるものなのか、本当の攻撃なのか、確認が必要な一幕もありました。結局はこれもセキュアワークスの攻撃だったのですが、それが判明するまではかなり緊迫しました。今では本当にリアルなテストができて、かえって良かったと感じています」と苦笑する。こうした経験を通して、他社のインシデント情報なども、より現実感を持って受け止められるようになったという。

今回実施したRed Teamテストの満足度を、丸金氏は「内容、コストを含めて120%だった」と高く評価する。とはいえ、テストから見てきた課題が全くなかったわけではない。同行ではセキュアワークスの報告を元に、さらなる改善・強化に取り組んでいく構えだ。

「今後特に力を入れたいと考えているのが、人のプロセスに関わる部分です。セキュリティはシステムと人が両輪で回らないと担保できませんので、ポリシー/ルールの見直しやコミュニケーションの円滑化など、できることからステップ・バイ・ステップで改善を進めていきたい。こうした人に依存する部分については、机上の検討だけではなかなか見えてこない面があります。そこを明らかにできたという意味でも、今回のRed Teamテストには大きな意義がありましたね」と松井氏は語る。Red Teamテストだけでなく、Blue Team演習の実施なども前向きに検討していくとのことだ。

加えて、もう一つ見逃せないのが、セキュリティ面での地域貢献だ。丸金氏が現在籍を置く株式会社CCイノベーションは、地元企業の経営改革や業務改善、デジタル活用などを支援するミッションを負っている。「地元企業のお客様と会話する中でも、セキュリティに関するお悩みを何うケースが増えていきます。北國FHDグループでは、『デジタルで地域を良くする』ことをDXの目的にも掲げていますので、今回の経験も活かしつつセキュリティ面でも地域への貢献を果たしていきたい」と丸金氏は展望を述べた。

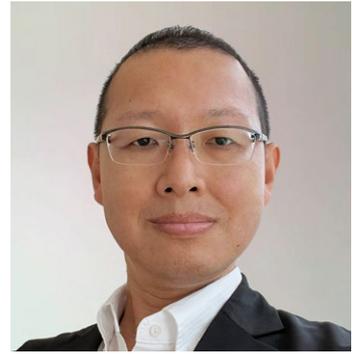
## 導入事例



株式会社北國銀行  
システム部 セキュリティグループ  
マネージャー  
松井 千明 氏



株式会社北國銀行  
システム部 セキュリティグループ  
チーフ  
田村 寿乃 氏



株式会社CCイノベーション  
コンサルタント  
丸金 正和 氏

- ・ 取材 2023年7月
- ・ 記載内容は、2023年8月10日時点のものです。
- ・ 本文書に記載されている仕様は2023年8月時点のものであり、予告なく変更する場合があります。最新の仕様については、弊社ホームページにてご確認ください。

### セキュアワークス株式会社

Secureworks(セキュアワークス、NASDAQ: SCWX)は、Secureworks® Taegis™を通じてお客様のビジネス進捗を保護するサイバーセキュリティのグローバルリーダーです。Taegisはクラウドネイティブなセキュリティ分析プラットフォームであり、20年以上にわたる実業務を通して蓄積された脅威インテリジェンスとリサーチに基づき構築されています。お客様は、高度な脅威を効果的に検知し、合理的な調査と関係チーム間のコラボレーションを行い、そして適切な対応アクションを自動化することが可能となります。



詳細は当社のセキュリティ  
専門家までご相談ください。

03-4400-9373  
[secureworks.jp](https://secureworks.jp)