FFR yarai 脆弱性攻撃防御機能 導入事例

東北電力企業グループ

地域とともに未来をひらく
東北電力

『地域と共に歩む複合エネルギーサービス企業』として、情報安全確保のためのセキュリティガバナンスを確立

東北電力グループは、『地域と共に歩む複合エネルギーサービス企業』を目指すべき企業グループ像として掲げており、安全確保を大前提としたエネルギーサービスの提供に努めています。

東北電力は、青森県、岩手県、秋田県、宮城県、山形県、福島県、新潟県の7県に電力を供給しており、その契約数は700万口以上にのぼります。また、これらの業務は東北電力単体で完結しているものではなく、様々な情報をグループ企業と連携しています。

情報通信部　グループ情報化推進課長
村上 芳博 氏

そのため、東北電力の情報セキュリティを確保するには、企業グループ全体でのセキュリティガバナンスを確立する必要があると考え、特に業務上の連携の深い35社を対象としてセキュリティガバナンス確立を推進しています。

「グループ各社の業種は多岐に渡り、必要な対策のレベルも企業により異なります。そのため、具体的な対策の実施レベルは各社の経営判断に任せるものの、企業グループ共通の情報セキュリティ評価シートを用いて各社の点検・改善活動の状況をチェックすることで、企業グループ全体の情報セキュリティマネジメントの強化に取り組んでいます。

しかし、近年、マルウェア感染による情報流出のリスクが高まってきたことから、『FFR yarai 脆弱性攻撃防御機能（以下、「yaraiZDP」）』の企業グループ35社への導入に踏み切りました。」（村上氏）

導入の背景
セキュリティパッチの公開から適用までの期間に対する危機感

東北電力企業グループ全体では、およそ30,000台のPCが、S-WING（スウィング）という企業グループネットワーク経由でインターネットに接続しており、それらPCのマルウェア対策として、ウイルス対策ソフトの導入に加え、定期的にセキュリティパッチを適用しています。

「セキュリティパッチの適用は、既存の業務システムに影響がないことを確認した上で実施する必要があるため、セキュリティパッチの公開から適用まで、どうしてもタイムラグが発生しますし、コストもかかっていました。」（村上氏）

「これまではそのタイムラグが問題になることはありませんでしたが、2009年に猛威を振るったGumblar攻撃の発生以降、東北電力グループでもWebサイト閲覧によるマルウェア感染が深刻な問題になってきました。東北電力グループでは、マルウェア感染が疑われるPCに対して、必要に応じてフォレンジック調査を実施し、感染による影響の有無を確認しています。幸いなことに、これまでの感染では情報流出などの被害は発生していませんが、マルウェア攻撃の巧妙化は著しく、このままではいつか被害が発生すると危機感を募らせていました。」（五十嵐氏）

情報通信部　グループ情報化推進
五十嵐 良一 氏

導入の経緯
検証環境で脆弱性攻撃を実施し、『yaraiZDP』の実力は本物だと実感

「IPSによるバーチャルパッチなども検討しましたが、サーバーセグメントへの攻撃は防げても、クライアントへのメールやWeb経由での攻撃は防ぎきれないと感じていました。情報を搾取する標的型攻撃などではクライアントPCがダイレクトに攻撃され、しかも被害が非常に深刻化する可能性があります。何か手はないかと考えていました。」パッチをリアルタイムに適用することがセキュリティ対策の基本であると理解はしていても、実践するのは運用面、コスト面で難しく、重要インフラを抱える企業としてジレンマを抱えていたといいます。

「そんな時、セキュリティ診断を依頼している企業の担当者から、『yaraiZDP』の紹介を受け、評価版でいろいろな脆弱性攻撃を実施してみたところ、非常に効果がある事が分かりました。また、『yaraiZDP』のリリース（2010年6月9日）後に発見された脆弱性への攻撃についても評価し、防御できることが確認できたことから、『yaraiZDP』の実力は本物だと実感しました。」（五十嵐氏）

その後、企業グループ35社（東北電力本体の15,000台を含む約30,000台）への導入を決定し、現在、グループ各社で順次導入を進めています。

導入の効果
セキュリティ強化だけでなく、運用の手間もかからないことが最大のメリット

『yaraiZDP』の導入決定後、東北電力グループへの標的型メール攻撃が発生しました。そのメールには、Adobe Readerの脆弱性を攻撃するPDFファイルが添付されていましたが、『yaraiZDP』を導入済みのクライアントは感染を回避することができました。しかも『yaraiZDP』にアラートが表示されたことにより、従来のウィルス対策ソフトでは防御できない攻撃の発生を迅速に検知することができ、情報流出などの被害が発生する前に手を打つことができたといいます。

「運用面については、従来のウイルス対策ソフトと違ってパターンファイルの更新がないので、安定して動作しています。勝手にバージョンアップすることもなく、導入時だけ検証すれば良いため、今後、サーバーに導入する際にも大きなメリットになりますね。管理サーバーを立てて、情報収集までできれば良いのですが、基本的にクライアントに導入しているだけで効果がありますので、運用は割り切っています。逆に言うと、運用に手間をかけなくて良いということが最大の費用対効果と考えています。」（五十嵐氏）

今後の展望
セキュリティレベルを向上しつつ、トータルコストの削減を検討

「『yaraiZDP』の導入により、セキュリティレベルの向上を図ることができます。情報セキュリティのステップを一段上げるということに『yaraiZDP』は大きく貢献したと考えています。システム的な対応がなくなるわけではありませんが、セキュリティ教育による啓発活動や、事故を前提とした対策も考慮したフォレンジック対応などのインシデントレスポンスの体制も整いつつあり、3～5年前の状況と比較して、かなり安心できる状況に変わってきています。」（村上氏）

「『yaraiZDP』の導入完了後は、脆弱性攻撃によるマルウェア感染はほぼなくなると考えています。今後は、『yaraiZDP』の防御効果を前提としたセキュリティパッチの適用頻度の見直しを行い、これまでよりセキュリティレベルを向上しつつ、トータルコストを削減するための検討を行っていきたいと考えています。」
（五十嵐氏）

製品・サービスについてのお問い合わせは
株式会社FFRI
〒150-0013
東京都渋谷区恵比寿1-18-18　東急不動産恵比寿ビル4階
TEL：03-6277-1811　E-mail：sales@ffri.jp
本製品に関する情報はインターネットでもご覧いただけます。
http://www.ffri.jp/

2012年10月現在