一般財団法人 関東電気保安協会様

標的型メール攻撃の疑似体験により対応力を向上し、情報漏えいを未然に防止

相次ぐ情報漏えい事故に危機感を募らせた関東電気保安協会様は「標的型メール攻撃訓練」を実施し、協会内の情報セキュリティ浸透度を把握。疑似体験で得たノウハウを協会/職員で共有し、情報漏えい事故の防止につなげています。

実施の背景

相次ぐ情報漏えい事故に新たな情報セキュリティ対策を検討

人々の生活に欠かすことのできない電気。電気を安全かつ安心して使える社会を守り、安定供給をサポートするのが関東電気保安協会様の任務です。現在、関東一円の50を超える拠点で3,000名強の職員が、電気設備の定期調査をはじめ、電気事業法で定められた各種手続きのサポート/技術支援などの調査・保安・広報業務を行っています。

同協会では多数のお客様情報を保有するため、協会内で制定された独自のセキュリティマニュアルに沿って管理が徹底され、セキュリティの専門家である情報システム部が適宜見直しを行っています。一軒一軒個人宅や契約先のビルなどを訪問して行う業務だからこそ、お客様との信頼関係が強く求められています。

世間で情報漏えい対策が叫ばれるなか、2015年6月に発生した情報流出事件を受け、同協会でも社会情勢に見合ったセキュリティマニュアルの見直しと、それによる新たな対策を検討することとなりました。当時を振り返り企画本部 情報システム部長）初鹿 孝夫氏は、こう語ります。「事件がニュースになった際、全職員に対し即座に注意喚起の周知文書を出しました。しかし、相次ぐ情報漏えい事件を目の当たりにし、さらに踏み込んだ対策が必要だと考えました。」

関東電気保安協会
企画本部 情報システム部長
初鹿 孝夫氏

実施検討の経緯

標的型メール攻撃訓練に着目 協会のセキュリティ浸透度を把握

同協会では、E-mailの運用として添付ファイルは必ず暗号化のうえ、別メールでパスワードを送ることがルール化されています。また、社外へのメール送信権限を必要最小限の職員に絞ることで、セキュリティ事故のリスクを最小限に抑えています。しかし、ルールがあってもどこまで社内で遵守・徹底されているかを測るのは難しいのが実情です。そこで、この機会にセキュリティに関するルールや諸注意事項がどの程度周知されているのかを確認することとし、既に他の電気保安協会で実施経験のある「標的型メール攻撃訓練」を役員会で提案し、即承認されました。

標的型メール攻撃訓練とは、標的型サイバー攻撃に対する的確な知識と判断力を身につけることのできる体験教育の支援サービスです。対象者に疑似メールを送信し、添付ファイルの開封やURLのクリック状況をまとめ、浮彫になった課題から改善提言を行います。

同部　副部長）小菅 実氏は語ります。「調べると、同様のサービスはいくつかありました。選定にあたり私たちが重要視したのは、提供企業の信頼性です。提供企業から疑似メールを送信するため職員のメールアドレスを外部へ提供することとなります。富士通SSLとは20年近い付き合いがあるため、安心できました。最終的に2社との比較となり、信頼性とコストの面で富士通SSLを選びました。」 実施検討からサービス選定まで、わずか一ヶ月というスピードでした。

具体的な実施策を検討するなかで、今回の訓練の対象は外部へのメール発信権限を持つアカウントに絞ることとしました。対象となったアカウントは445、このなかには共有アドレスが含まれるので1,800名程度の職員に対し実施されることとなります。さらに添付ファイルとURL、2パターンの疑似メールとし、2回に分けて実施することが決定しました。初鹿氏は打ち明けます。「対象者の選定と実施内容はすんなり決まりました。意見が分かれたのは、事前に告知をするか否か、という点です。反対意見もありましたが、日常の実態を知ることが目的ですから予告無しで実施することが最終決定しました。」

関東電気保安協会
企画本部 情報システム部
副部長　小菅 実氏

実施の効果

添付ファイル開封率1.5% URLクリック率10.3% セキュリティ浸透度の高さを実感

初回の訓練は、お盆休み明けの8月18日に実施、外部アドレスから件名の怪しい添付ファイル付きの疑似メールが送られてきました。事情を知らない職員からは、どのような反応があったのでしょうか。小菅氏は語ります。「正直に言うと、予想より遙かに良い結果でした。1,800名のうち添付ファイルを開封してしまったのは、わずか7名、0.38%でした。共有アドレスが含まれるので、アカウントで比較すると1.5%です。これだけ開封率が低かったのは、不審感を抱いた者が同じ共有アドレスの利用者に声をかけ警告していたことと、すぐに情報

システム部門へ連絡するというルールが遵守されていたためです。“不審な添付ファイルは開封しない”ことは世間の常識ですが、当協会内でどこまで守られているかという不安は杞憂に終わりました。」

初鹿氏は続けます。「共有アドレスを使うことの是非もありますが、業務を円滑に進めるには共有アドレスも必要です。セキュリティと利便性のバランスを図りながら運用しています。今回は共有アドレスの良さが活きた結果と言えるでしょう。不審メールの情報が横展開されていたので、我々情報システム部門へ来た問い合わせは20件程度と僅かでした。」

予告なしで実施した訓練でしたが、手ごたえを感じることができました。

続く2回目の訓練は約一ヶ月後の9月15日に実施されました。今度は内部からの不審メールという設定で件名、差出人名、本文内のURLリンクで標的型を装ったものです。2回目の結果について、小菅氏は語ります。

「もともと内部メールは標的型と気づきにくいうえ、URLリンクはクリックしやすい傾向があります。当社でも2回目は10.3%のクリック率でした。但し、1回目の添付ファイル開封率が富士通SSLの想定より低かったため、2回目はメール内容の見直しを行い疑似メールと判別しづらくしているので、決して悪くない結果だと考えています。今回も不審メールに気づいた職員が、すぐ職場に周知していました。」

URLクリック率10.3%という数値は、本サービスの提供実績と比較すると、はるかに低い数値です。

「メール訓練終了後に実施したアンケートでは、77%の職員から情報セキュリティに対する意識が上がった(変化があったを含む)という回答がありました。不審メールは開封しない、という意識が着実に定着しているといえるでしょう。」(小菅氏)

今後の展望

標的型メール攻撃の疑似体験と教育で対応力を向上し、情報漏えいを防止

今回の標的型メール攻撃訓練を振り返り、初鹿氏はこう語ります。「危険を察知する能力を身につけることはもちろん、標的型メールを体験することも大切だと考えています。一度“ひやり、はっと”を体験すると注意力が高まります。」

同協会では、添付ファイルやURLだけでなく差出人や件名にも細心の注意を払うよう徹底していますが、実際に標的型メールを受け取った経験があれば慎重さや疑うポイントなど実践での対応も格段に違ってくるでしょう。

初鹿氏は続けます。「とはいえ、訓練でどれだけできていても、実際に標的型メールを受け取ったとき一人でも添付ファイルを開いたり、URLをクリックしてしまったらおしまいです。ヒューマンエラーを防ぐには、職員の教育が第一です。現在もセキュリティ教育は実施していますが、今後はe-learningの導入等も検討していく考えです。」

同協会は今回の標的型メール攻撃訓練の結果をもって、セキュリティポリシーやネットワーク通信の診断を行い、セキュリティ対策の強化に取り組みます。

富士通SSLは今後も、関東電気保安協会様の強固なセキュリティを全面的に支援していきます。

担当営業の声

株式会社富士通ソーシアル
サイエンスラボラトリ
第一統括営業部　第一営業部
山本 悠人

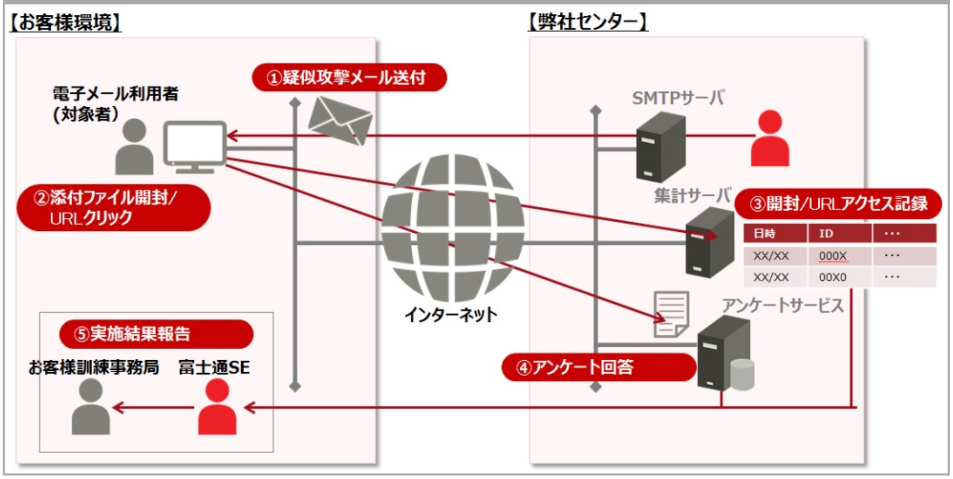
刻一刻と変化するセキュリティ情勢に対応するため、今後も継続的な提案を実施して参ります。

会社概要

一般財団法人 関東電気保安協会

所在地:〒108-0023
東京都港区芝浦4-13-23　MS芝浦ビル
事業内容:電気の安全かつ合理的な使用方法の周知、啓発を通じ地域社会に貢献するために、主に次の事業を展開
・電気の定期調査
・年次点検(保安業務)
・広報業務
設立:1966年2月
従業員数:3,015名(2014年10月1日現在)
ホームページ:http://www.kdh.or.jp/

サービスの実施イメージ



※記載の会社名、商品名は、各社の商標または登録商標です。
※記載の内容は、2015年11月現在のものです。
※記載された情報は、予告なく変更することがあります。

製品紹介ページ
http://www.ssl.fujitsu.com/products/security/targeted-mail-training//

お問い合わせ先
株式会社富士通ソーシアルサイエンスラボラトリ(富士通SSL)
お問い合わせ総合窓口　E-mail : ssl-info@cs.jp.fujitsu.com
〒211-0063 川崎市中原区小杉町1 - 403 武蔵小杉タワープレイス
http://www.fujitsu.com/jp/group/ssl/