2017年6月

金融機関が取り組むべき サイバーセキュリティ教育

サイバー攻撃による不正送金や個人情報の漏えいが、金融機関に対する信頼感の低下や業績に影響を及ぼしかねない重大な脅威となっている一方で、昨今のサイバー攻撃の特徴として、サイバーセキュリティのリテラシーが高くない一般の従業員を対象にした攻撃が増加している。組織としてサイバーセキュリティを維持・向上するには、サイバーセキュリティ業務の関係者に加え、多様な役割の人材にサイバーセキュリティの素養を身につけさせることが必要になってきた。

本稿では、金融機関に求められる、全従業員を対象とした、サイバーセキュリティに関するリテラシーと実践力の向上を目的とする教育の実施について解説する。なお、本文中の意見に関する部分は、筆者の私見であることをあらかじめお断りする。

1. サイバーセキュリティ教育の重要性

昨今のサイバー攻撃の脅威は、業務にかかわらずすべての従業員に身近で、かつ見える形で増してきている。独立行政法人 情報処理推進機構（以下、「IPA」）が公開した「情報セキュリティ10大脅威2017」[1]では、主に攻撃メールをきっかけに開始される「標的型攻撃」「ランサムウェア」が、組織における情報セキュリティ脅威の上位に挙げられた。標的型攻撃は、国内で発生した情報漏えい事案や、海外金融機関で発生した大規模不正送金事案において使用された攻撃手法である。標的型攻撃で送られる攻撃メールは、以前はひと目で怪しいとわかる英文メールが主流であったが、現在では、対象者のプロファイルを考慮して巧妙に偽装された文面で送られてくるように進化している。そのため、標的型攻撃メールを見分けるには、サイバーセキュリティに関する知識と意識が一層求められる。

日本では、金融庁が2015年度に監督指針等を改正し、取締役会等がサイバーセキュリティの重要性を理解すること、およびサイバーセキュリティ人材の育成と確保が求められるようになった。米国では、連邦金融機関検査協議会（Federal Financial Institutions Examination Council：FFIEC）[2]が公開しているアセスメントツール[3]のなかで、経営者を含む全従業員を対象としたサイバーセキュリティ研修実施と企業文化への定着が推奨されている。

1 https://www.ipa.go.jp/security/vuln/10threats2017.html

2 米国の金融機関に対する検査に関する方針・基準等を策定している機関。

3 FFIEC Cybersecurity Assessment Tool（CAT）https://www.ffiec.gov/cyberassessmenttool.htm
金融機関固有のサイバーセキュリティリスクとサイバーセキュリティ成熟度を評価するツール。
個社のリスクに応じて必要とされる対策が把握できる。本ツールを用いて各金融機関が行った評価結果は、当局が行う評価にも活用されている。

組織としてサイバーセキュリティを維持・向上するには、多様な役割の人材に対して、自社の事業および個々の業務に関連するサイバーセキュリティリスクを理解させ、サイバー攻撃に直面した際に適切な行動をとることができる能力を身につけさせることが重要である。

2. サイバーセキュリティ教育の設計

サイバーセキュリティ教育の実施に際しては、組織のサイバーセキュリティにおける役割、および責任を考慮して教育テーマを設定することが重要である。

サイバーセキュリティ教育の目的として考えるべきことは、「リテラシー（知識）」と「実践力」である。前者は、個々の職務上の責任および権限にかかるサイバーセキュリティリスクとその対応策を理解することである。後者は、組織における自らのサイバーセキュリティに関する役割の遂行上必要となるスキルを身につけ、常に使える状態に保つことである。2つの目的に対し、一般的な組織の役割から対象者を定義し、教育すべきテーマについて整理した結果を、参考までに下記に記載する。

【図表1】サイバーセキュリティ教育テーマの設定例

教育目的	対象者	教育テーマ例
リテラシー	経営者	• サイバーセキュリティを取り巻く外部環境変化の理解 • サイバーセキュリティが経営に与えるインパクトの理解 • サイバーセキュリティに関する主要な取組みの理解 • 当局等要求事項の理解
	管理者	• サイバーセキュリティを取り巻く外部環境変化の理解 • サイバーセキュリティが自組織の運営に与えるインパクトの理解 • 自組織が利用または提供するシステム環境に関係するサイバーセキュリティの理解 • サイバーセキュリティに関係する社内手続の理解（管理者役割）
	一般職員	• サイバーセキュリティを取り巻く外部環境変化の理解 • 通常業務に関連するサイバー攻撃の脅威の理解 • サイバーセキュリティに関係する社内手続の理解（不審メール受信時の対応等）
実践力	経営者	• 有事における、定められた権限に応じた意思決定の実践 • 有事における、対外説明の実践
	管理者	• 自組織におけるサイバーセキュリティリスク判定の実践
	一般職員	• 不審メール受信時の初動対応の実践

さらに、CSIRT[4]やセキュリティ部門に所属しサイバーセキュリティ業務を担当する人材に対しては、別途高度な実践力を身につけるための教育テーマの検討が必要である。検討にあたっては、IPA が公開する「ITSS＋」[5]や特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が公開する「SecBok」[6]等を用いて、育成対象者の役割とスキルを定義することを推奨する。

4 Computer Security Incident Response Team。サイバーセキュリティを含む、コンピュータセキュリティに関連するインシデント対応を所管する組織。

5 「セキュリティ領域」および「データガバナンス領域」で必要なスキルについて取り纏めたもの。
https://www.ipa.go.jp/jinzai/itss/itssplus.html

6 情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理したもの。
http://www.jnsa.org/result/2016/skillmap/

3. 一般職員向け教育の勘所

対象者ごとに教育テーマを決めた後、教育計画を策定し運用していくが、経営者や管理者については対象者が限定されることから、集合研修や演習等を開催し、対象者のレスポンスや教育効果を確認しつつ教育を実施することが可能である。一方、一般職員については、対象者の母数が多く、かつ担当業務や責務も多岐にわたるため手段が限られてくる。

また、金融機関の一般職員は、サイバーセキュリティ以外にも業務上理解すべき規制や事務手続が多数あることから、馴染みの薄いサイバーセキュリティは相対的に重視されない恐れがある。一般職員のサイバーセキュリティ教育計画は、限られた機会のなかでサイバーセキュリティリスクを正しく理解させ、各人のサイバーセキュリティ対策上の役割を定着させることが求められる。3つの具体的な取組みを挙げ、それぞれについて説明する。

教材にはリアルな情報を使用

標的型攻撃メールの特徴や不審メール受信時の初動対応等、業務や責務によらず全従業員が理解すべき内容については、教材を配布して研修させることが可能であるが、サイバーセキュリティリスクを正しく認識させるためには、自社を取り巻く脅威情報を教材内に盛り込むことが重要である。これらは、実際に起きた事例や金融ISAC等の情報共有機関から得られる情報と、自社OA環境のログ等を組み合せて分析することで取得できる。教材項目と素材となる情報の例を以下に示す。

• サイバー攻撃発生件数の推移	レポート（金融庁、NISC[7]、IPA、警察庁等）
• 自社における不審メールの検知件数の推移	ログ等分析結果
• 実際に流通している不審メールタイトルの一覧	ログ等分析結果
• 巧妙な不審メールの文面	共有情報（金融ISAC等）、レポート（IPA等）
• ウイルス感染した端末の挙動解説	マルウェア解析結果、レポート（ベンダー等）

メール訓練と研修の連携

多くの金融機関で導入されているメール訓練（不審メールに似せた擬似メールを従業員に送付する）にあたっては、サイバーセキュリティ教育と連携し、教育効果を高めることを検討したい。具体的には、メール訓練前に事前教育を実施し、訓練にてサイバー攻撃を体験し、訓練後に振り返りを実施する。

メール訓練前の事前教育では、メール訓練への橋渡しとなることを考慮し、標的型攻撃メールの特徴や不審メール受信時の初動対応を中心に教育する。メール訓練後の振り返りでは、訓練メールを見分けるポイントや訓練内での好事例の紹介等を行う。特に、メール訓練後は、訓練内で正しい行動をとれなかった職員の危機意識が高まっていることが期待できるため、サイバーセキュリティの重要性を伝える機会に適している。

7 National center of Incident readiness and Strategy for Cybersecurity
（内閣サイバーセキュリティセンター）

管理者との連携の強化

教材を配布した研修やメール訓練の活用は、全従業員に対して効率的に教育を実施できる反面、部門ごとのサイバーセキュリティリスクやリテラシーの違いを考慮することは困難である。そのため、各組織や部門内での、サイバーセキュリティ教育推進の役割を明確にする必要がある。具体的には、各組織や部門の管理者に対して、サイバーセキュリティに関する役割、および責任を明示的に割り当てる。管理者に割り当てる役割、および責任としては以下が考えられる。

- 不審メール受信・開封職員の初動対応サポート
- 所属職員の教育実績の管理（メール訓練結果を含む）
- サイバー攻撃に関する脅威情報の組織内共有組織内勉強会などでのサイバーセキュリティ教育の実施

4. まとめ

サイバーセキュリティ教育は、各金融機関において実際に実現可能な内容に設定することが重要である。2020年の東京オリンピック開催に向けて、金融機関を含む重要インフラへのサイバー攻撃は、さらに増加かつ高度化することが予想されている。サイバーセキュリティ教育に繰り返し取り組むことで、従業員のリテラシーと実践力を継続的に向上させ、サイバー攻撃に対して全社員一丸となって立ち向かう企業の姿を目指してほしい。

KPMGコンサルティング株式会社
マネジャー　田畑　直樹

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ　ノースタワー
TEL ： 03-3548-5111
FAX ： 03-3548-5114

大阪事務所
〒541-0048
大阪市中央区瓦町3丁目6番5号　銀泉備後町ビル
TEL ： 06-7731-2200

名古屋事務所
〒450-6426
名古屋市中村区名駅3丁目28番12号　大名古屋ビルヂング
TEL ： 052-571-5485

kpmg.com/jp/kc