KPMG
cutting through complexity

2015年12月

新たなITリスクに立ち向かう 連載シリーズ 第17回

全社的・組織横断的なCSIRTの整備

金融機関を取り巻くサイバー攻撃の脅威が深刻化していることを受け、金融庁は本年、サイバーセキュリティ管理態勢の強化に関するガイドライン改正や行政方針を相次いで発表している。

4月22日には「主要行等向けの総合的な監督指針」および「金融検査マニュアル」の一部改正があり、7月には「金融分野におけるサイバーセキュリティ強化に向けた取組方針」、9月には「平成27事務年度金融行政方針」が公表された。

そこでは、サイバー攻撃からの利用者保護の取組強化や、経営陣の関与も含む、より組織横断的なサイバーセキュリティ管理態勢が求められている。

本稿では、金融庁の当該公表を踏まえ、金融機関として求められる対策について解説する。

1. 金融機関におけるサイバー攻撃について

金融機関における代表的なサイバー攻撃を以下に示す。警察庁の発表によれば、平成24年には64件、約4,800万円だった被害額が、平成25年には1,315件、約14億600万円、平成26年には1,876件、約29億1,000万円の被害額に達している[1]。さらに平成27年上半期は、既に754件、約15億4,400万円に達したとされており[2]、増加傾向が続いている。

【図表1】金融機関における代表的なサイバー攻撃

攻撃の種類	攻撃内容
標的型攻撃	特定の組織を狙ったサイバー攻撃で、コンピュータウィルスなどの不正なプログラム、コンピュータシステムへの侵入・遠隔操作、アカウントの乗っ取りなどの手法により、企業内の機密情報の搾取や重要システムの破壊、Webサイトの改ざんなどが行われる
DDoS攻撃	ネットワークを通じて大量のデータや不正なデータを企業に送りつけ、企業側のコンピュータシステムを過負荷状態にして、システムスローダウンやシステム停止など、正常な稼働ができない状態に追い込む
フィッシング	金融機関からの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などの重要情報を搾取し、そこで得た情報を基に他人になりすまして不正送金などを行う

1 平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について（平成27年2月12日 警察庁）
https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

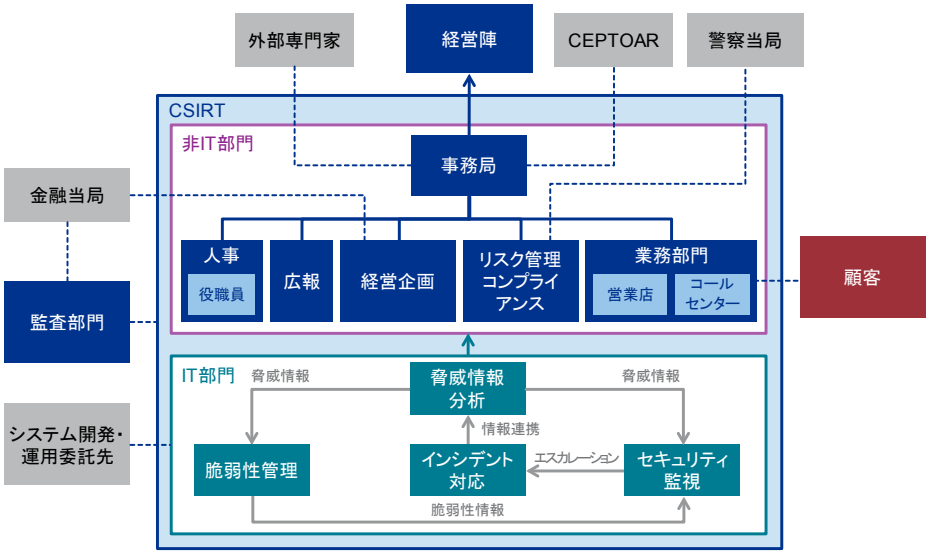
2 平成27年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について（平成27年9月3日 警察庁）
https://www.npa.go.jp/cyber/pdf/H270903_banking.pdf

今日のサイバー攻撃は年々手口が高度化し、また次々と新たな手口で攻撃が仕掛けられており、こうした未知の攻撃に対応するため、攻撃対象となり得るシステムの脆弱性管理や脅威情報の分析など、プロアクティブな対策が必要となる。また、セキュリティインシデントを完全に防止することは困難であるため、万が一インシデントが発生した際の被害を最小限に抑えるため、被害を想定した訓練の実施や、従業員のセキュリティ意識を高めるための啓発活動等、平時の準備も重要となる。そういった役割を担うのが、CSIRT（Computer Security Incident Response Team）である。

2. IT部門主導のCSIRTから全社的・組織横断的なCSIRTへ

近年、サイバー攻撃者が自分の技術力を誇示することを目的とした愉快犯的犯行から、金銭的な被害を伴う営利目的へと変化しているなか、被害発生時には顧客保護や法務的な対応、金融当局への情報連携等が必要となるため、IT部門だけではなく、全社的・組織横断的なCSIRTの構築が重要となってきている。

【図表2】全社的・組織横断的なCSIRTの全体像



図表2は、全社的・組織横断的なCSIRTの全体像である。ここに示したように、「事務局」が司令塔となって、有事のインシデントハンドリングと平時のサイバー攻撃に備えた準備活動を行う。特に重要なのは、「経営陣」への唯一の情報伝達パスになることで、適切な意思決定に必要な情報がタイムリーかつ正確に「経営陣」に報告される体制を実現することである。金融機関によっては、「事務局」に経営企画とリスク管理／コンプライアンスの機能を一体化させて運営する場合もあるだろう。その場合は、「金融当局」と「警察当局」へのインシデント対応状況の報告や、外部機関との情報交換なども主なタスクとなる。

「事務局」の役割を担う人材には、インシデント発生時のビジネスへの影響度合いを理解し、全社的に必要となる対応を見極め、各組織が迅速かつ適切に機能するようコントロールすることが求められる。加えて、ある程度の技術的な知見も有するなど、求められるスキルは広範囲に及ぶため、必要なスキルの定義と人材育成が特に重要となる。経営企画業務の経験と各組織に強いパイプを持つ人材に対して、サイバーセキュリティに関する必要最低限のスキルを習得させる方法が、人材育成のスピード感をあげる1つの選択肢として考えられる。

その他の非IT部門に関しては、「業務部門」では顧客対応として、インシデント防止のための啓蒙活動やインシデント発生時の注意喚起、補償等の対応を行い、「人事」では、必要となる人材の採用や社員教育・啓蒙活動と、内部不正発生時の人事的措置等の実施、また「広報」では、報道機関へのインシデント発生・対応情報の提供等の役割があげられる。

次にIT部門については、「脅威情報分析」で外部から収集した脅威情報を分析し、「脆弱性管理」において自社製品の脆弱性情報の管理を行い、かつ「セキュリティ監視」でIT機器のログを監視してアラートを発信し、「インシデント対応」で発生したインシデントについて対応する。個々の役割定義もさることながら、非IT部門との情報連携設計や、自社の職員とITベンダー等の外部委託先との役割分担の明確化など、現状を把握した上でギャップを埋める対応が肝要となるだろう。

3. まとめ

サイバー攻撃の脅威は、今や金融システムの安定化にとって重大なリスクであり、さらには、金融分野でのインターネット利用拡大や、サイバー攻撃の高度化により、そのリスクも肥大化している。

そうした背景から、金融庁のガイドラインや金融行政方針においても、サイバーセキュリティ管理態勢の強化が求められている。この状況下で、金融機関は業務継続性の確保と利用者保護を最重要課題と捉え、経営陣がオーナーシップを発揮した、より組織横断的なサイバーセキュリティ管理態勢の構築が重要となるだろう。その態勢構築に際しては、CSIRT機能の一部を複数の金融機関で共同化する選択肢も考えられる。

KPMGコンサルティング株式会社
シニアマネジャー　戸田　雅仁

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 ： 03-3548-5305
FAX ： 03-3548-5306

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
〒451-6031
名古屋市西区牛島町6番1号　名古屋ルーセントタワー
TEL ： 052-571-5485

kpmg.com/jp/kc