KPMG
cutting through complexity

2015年5月

新たなITリスクに立ち向かう 連載シリーズ 第13回

金融機関に求められるサイバーセキュリティ

金融検査マニュアル等の改正(案)公表を踏まえて

金融機関を取り巻くサイバー攻撃の脅威は、日々深刻化している。警視庁の発表資料によれば、我が国における不正送金被害はこの2、3年で激増した[1]。日系企業が標的型攻撃の被害に遭う事案も報道されており、サイバー攻撃は海外で発生する対岸の火事から、目の前に迫る脅威に変貌した。

このような状況のもと、金融庁より、「主要行等向けの総合的な監督指針」及び「金融検査マニュアル」等の一部改正が公表され、平成27年4月22日より適用が開始されている。

本稿では、金融庁のガイドライン改正を踏まえ、金融機関として求められる対応について解説する。

1. 金融庁ガイドラインの改正

今般の金融庁ガイドラインの改正ポイントは図表1のとおりである。改正事項は計4点であるが、そのうち①情報セキュリティ管理および④システムリスク管理は、既存の枠組みのさらなる強化を促す改正である。一方、②サイバーセキュリティ管理および③インターネットバンキングは、サイバー攻撃の脅威に対抗するための新たな枠組みの整備を要求している。なお、証券取引等監視委員会の「金融商品取引業者等検査マニュアル」においても、ほぼ同様な改正が行われていることについても併せて申し添える。

【図表1】「主要行等向けの総合的な監督指針」及び「金融検査マニュアル」等の改正事項[2]

改正ポイント		概要
①	情報セキュリティ管理に係る監督指針等の改正	外部委託先社員等による不正出金事案等の発生を踏まえ、顧客に関する情報の厳格な管理態勢や外部委託先に対する適切な管理態勢の整備状況について、監督上の着眼点として明確化する等、所要の改正を行う。
②	サイバーセキュリティ管理に係る監督指針等の改正	サイバーセキュリティ基本法の全面施行(平成27年1月9日)、世界的規模で生じているサイバーセキュリティに対する脅威の深刻化等を踏まえ、金融機関に求めるサイバーセキュリティ管理態勢の整備状況について、監督上の着眼点として明確化する等、所要の改正を行う。
③	インターネットバンキングに係る監督指針等の改正	インターネットバンキングに係る犯罪手口が高度化・巧妙化していること等を踏まえ、預金取扱金融機関におけるセキュリティ対策や顧客への対応について、監督上の着眼点として明確化する等、所要の改正を行う。
④	システムリスク管理態勢に係る監督指針等の改正	システムリスク管理態勢に関する着眼点・検証項目の拡充を図るため、「金融商品取引業者等向けの総合的な監督指針」「清算・振替機関等向けの総合的な監督指針」「保険検査マニュアル」について、所要の改正を行う。

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 「主要行等向けの総合的な監督指針」及び「金融検査マニュアル」等の一部改正(案)の公表について(平成27年2月13日 金融庁)
http://www.fsa.go.jp/news/26/20150213-1.html

2. 金融機関に求められる対策

金融機関が具備すべきサイバー攻撃対応態勢を、対策レイヤーと対応フェーズで整理すると図表2のとおりとなる。これまで、金融機関は予防のために多くのコスト投下を行ってきた。また、多くの企業において、サイバー攻撃への対応は主にIT部門の役割であると認識されている。しかしながら、サイバー攻撃の手法が、高度化・個別化の傾向にある中、完全に予防することは困難となりつつある。したがって、金融機関は、仮に侵入されても早期に発見し被害を最小化とするための対策について、全社的に整備していく必要がある。

【図表2】サイバー攻撃対応態勢の全体像

	予防	発見	対処
組織	サイバー情報収集・展開体制	セキュリティ監視体制（SOC）	緊急時対応体制（CSIRT）
	顧客教育プログラム	フィッシングサイト検出体制	賠償方針
プロセス	システム開発管理プロセス	監視項目と規程	BCPの整備と訓練
	リスクアセスメントとPDCA		
テクノロジー	強力な認証	不正取引検出	フォレンジック態勢
	振込上限額の設定	不正侵入検出（IPS/IDS）	振込の遅延・停止

実際、今回の金融庁におけるガイドライン改正においても、「多層防御」という表現がみられる。これは、侵入されることを前提とした対策の必要性を喚起するものであるといえる。具体的には、以下のように、入口対策・内部対策・出口対策から構成される。

- 入口対策

入口対策とは、「侵入を予防するための対策」であり、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入等が該当する。比較的、各金融機関において、すでに導入が進んでいると考えられる分野である。

- 内部対策

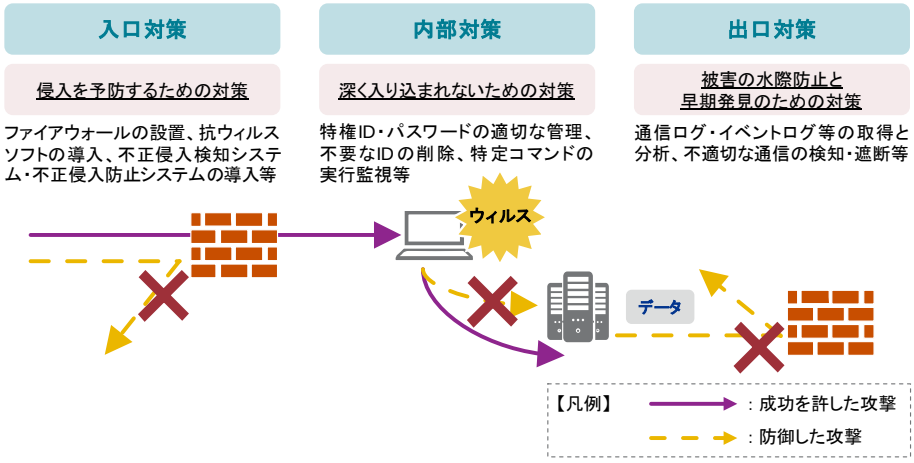
内部対策とは、仮に侵入されても「深く入り込まれないための対策」であり、特権ID・パスワードの適切な管理、不要なIDの削除、特定コマンドの実行監視等が該当する。これまでは、侵入を予防するための入口対策に注力していた企業が多く、侵入された際の対策については手薄な金融機関も見受けられる。

- 出口対策

出口対策とは、「被害の水際防止と早期発見のための対策」であり、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断等が該当する。通信ログの分析を人手で実施するには限界があり、SIEM（Security Information and Event Management）システム等、専用のテクノロジーを導入し対応することが望まれる。

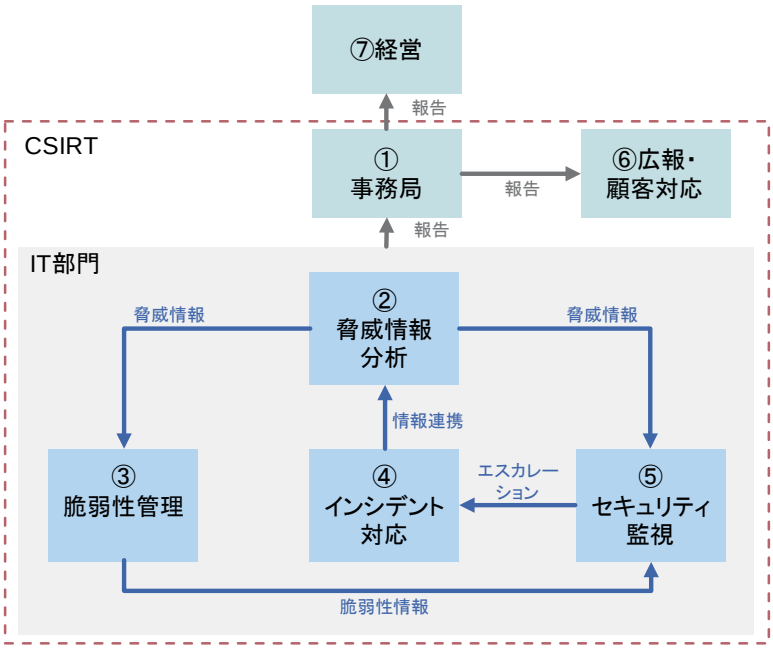
なお、この「多層防御」について、イメージ図として記載したものが図表3である。

【図表3】多層防御



また、サイバー攻撃に対する監視体制、攻撃を受けた際の報告・広報の体制、組織内CSIRT（Computer Security Incident Response Team）等についても、今回のガイドライン改正では言及されている。これらは、IT部門単独で実現されるものではなく、経営や広報、顧客対応部門を含む全社的な協調体制が求められるものである。このような点から考えられるサイバー攻撃対応体制の例を図表4に示す。

【図表4】サイバー攻撃対応体制の例



図表4を例に、サイバー攻撃への対応機能について解説する。

- 平時の対応として以下の機能がある。
  - 外部から収集した脅威情報を分析する、「②脅威情報分析」機能
  - 自社製品の脆弱性情報を管理する、「③脆弱性管理」機能
  - IT機器のログを監視してアラートを発信する、「⑤セキュリティ監視」機能

- 発生したインシデントの対応は、「④インシデント対応」機能で対応する。
- 「①事務局」機能において②～⑤の機能を取りまとめ、「⑦経営」への報告を実施する。
  なお、「⑦経営」については、CIOやCISO等、サイバーセキュリティの責任者が誰なのかを明確にしておく必要がある。

また、有事の際に備えた「⑥広報・顧客対応」への導線設計も整備する必要がある。

3. まとめ

サイバー攻撃の脅威が深刻化しつつある中、金融庁のガイドラインも大きく改正され、サイバーセキュリティ管理態勢の構築が企業に要求されている。なかでも、攻撃を完全に予防しきれないことを想定した「多層防御」と、経営陣の強いリーダーシップに基づく広報・顧客対応部門も巻き込んだ「全社的な対応体制」が態勢構築の肝であると考えられる。

また、各金融機関の特徴やビジネスモデル、ITの構造によって、標的となる資産や脅威となる攻撃手法は異なる。したがって、ガイドラインに基づいた対応を行うだけでなく、自社固有のリスクシナリオを検討・精査し、自社固有の対応を検討していくことが企業に求められている。

KPMGコンサルティング株式会社
ディレクター　山下　雅和

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

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