高まるサイバー演習の重要性と有効活用のための考え方

金融業界に対するサイバー攻撃の脅威が高まる中、各国政府レベルで金融業界における対応能力強化が意識されてきている。特にサイバー演習は有力な強化手段として位置づけられており、日本を含む各国政府が参加機会を提供しているが、有効活用のためには、目的の明確化など事前の準備が肝要である。

サイバー演習の有効性と類型

サイバー攻撃は物理的なテロ攻撃と異なり、ネットワークを介して瞬時に組織の弱い部分を攻撃してくる。いついかなる箇所が攻撃にさらされても、対応チームをはじめ組織の主要な構成員が、同じ状況認識（Situational Awareness）を共有して対処しなければ、組織における対応の乱れをついて、サイバー攻撃による被害は拡大する恐れがある。同じ状況認識を共有し行動するには、正しい情報が適時に適切な部署に伝達されている必要があり、このためにサイバー演習が有効とされている。

サイバー演習には様々な類型がある。CSSC（制御システムセキュリティセンター）の定義によれば、サイバーセキュリティに関するセミナーも演習の一つに分類される。しかし、いわゆるサイバー演習として想起されるのは、図表1で机上演習カテゴリに含まれるゲーム演習[1)]、机上演習[2)]、あるいは機能演習カテゴリに含まれる通知（情報連携）演習[3)]、組織機能演習[4)]、総合演習[5)]であろう。本稿では、特に金融機関のサイバー攻撃対応チームにとって重要と思われる機能演習カテゴリに属する演習について取り上げたい。

機能演習は通常、背景となるシナリオ情報（攻撃が行われる目的、想定される攻撃先、攻撃の方法など）の下で生じる様々なイベントを想定し、それらに対する情報連携を実際に組織がシミュレートする形で行われることが多い。例えばサイバー犯罪組織がマルウエア（悪意のあるソフトウエア）をしこんだ標的型メール攻撃をしかけ、社内外で次第に感染が広がっていく想定の下、どのような情報連携・意思決定・行動をするのかが問われる。

参加組織にはシナリオの内容を知らないプレイヤーを置き、すべてのイベントの発出タイミングや発出先を制御するコントローラーが事務局に置かれる。また組織内にシナリオの内容を知る評価者を置き、情報連携の質・量、スピード等について評価させる場合もある。

図表1　サイバー演習の類型

カテゴリ	演習名称
研究的演習（セミナー等学習的なもの）	セミナー
	ワークショップ
机上演習（課題抽出を目的とした議論）	ゲーム演習
	机上演習
機能演習（実際に組織等を動かす演習）	通知(情報連携)訓練
	組織機能演習
	総合演習

（出所）CSSC（制御システムセキュリティセンター）HP等より野村総合研究所作成

内外のサイバー演習事例と有効活用のための考え方

サイバー攻撃はますます高度化・複雑化しており、金融業界に対する攻撃も増加している。サイバー脅威は直接的な被害もあるが、金融ITインフラやネットワークの信頼性を脅かしかねない点で、個別金融機関だけでなく、金融業界全体として取り組む必要があるものである。サイバー攻撃に対する自社ネットワークやシステム自体の防御を固めることは当然であるが、今日の進んだサイバー攻撃手法に対して、完全に攻撃を防ぎきることは困難である。攻撃を受けた際に被害を最小化し、他システム等への被害拡大を防ぐためには、サイバー演習が有効であるとの認識が国内外で高まっている。

サイバー攻撃を想定した機能演習は2000年代初頭より英・米を中心として多くの取り組みがある。とりわ

NOTE

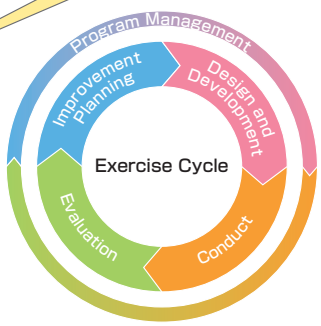
1) RED team、BLUEチーム等に分かれ、ダミーのシステム環境等を利用して、攻防をシミュレートし熟練度を上げたり、新技術を創出するための演習。
2) 既存のサイバー対応マニュアルや体制の課題抽出を目的として、いくつかの議題について参加者間で議論をする形式の演習。
3) サイバー攻撃の発生時において、社内外での情報連携体制の有効性を確認するため、実際に特定のシナリオ下での情報連携を実施する演習。
4) 情報連携演習に加えて、組織における意思決定機能も合わせて検証する演習。
5) 多数組織が参加し、意思決定・情報連携を含めた総合的な演習を実施するもの。
6) 米国DHS（Department of Homeland Security：合衆国国土安全保障省）主導により、米国内の政府機関、民間事業者等を対象に、2006年よりほぼ隔年で実施されているサイバー演習。
7) 米国SIFMA（Securities industry and Financial Markets Association：米国証券業金融市場協会）主導による主として証券市場を対象としたサイバー演習。2011年より実施。
8) 英国FCA（Financial Conduct Authority：金融行動監視機構）、BOE（Bank of England）等が主導する官庁、民間金融機関共同による金融業界を対象としたサイバー演習。2011年より実施。
9) わが国初めての金融業界横断的演習として、金融庁主導により、2016年10月24日～27日まで約80の金融機関が参加して実施された。
10) 米国DHSにより2013年に策定された演習の企画、実行、評価、改善に関するガイドライン。

図表2　HSEEP概要

HSEEPでは、プログラムマネジメント+各フェーズの活動を「演習サイクル」として定義している。

「コア能力」とは演習で検証したい最も中核となる能力。
「状況判断力」「情報連携力」等演習によって異なる。

- **プログラムマネジメント**
  - 適切な責任者の関与
  - 複数年の訓練計画（机上、実オペ）
- **演習設計（Design and Development）**
  - **演習の目的設定、検証する「コア能力」の識別**
  - シナリオ策定
  - 演習計画チームの組成
  - ドキュメンテーション
- **実施（Conduct）**
  - 演習の準備（ロジ）
  - 演習中の各担当者の役割
- **評価（Evaluation）**
  - 評価計画の策定
  - 演習参加、報告書作成
- **改善（Improvement Planning）**
  - 改善計画の立案（能力ベース）



HSEEP Exercise Cycle

（出所）DHS “Homeland Security Exercise and Evaluation Program（HSEEP）” 2013より野村総合研究所作成

け米国におけるCyber storm[6]、Quantum Dawn[7]、英国のWaking Shark[8]等は大規模なものであり、一部は金融機関に特化した内容となっている。

わが国でもNISC（内閣サイバーセキュリティセンター）が2012年以降、金融機関を含む重要インフラ企業（サイバー攻撃を受けた場合、国民の社会・経済生活に大きな影響を与えかねない企業）を対象として、分野横断的演習という名称で機能演習の場を提供している。また金融庁も平成28年度の検査マニュアルに「サイバー演習に参加したか」との項目を設け、金融機関にサイバー演習への参加を促しているほか、昨秋には金融庁が主催する中小金融機関向けのサイバー演習“Delta Wall”[9]が実施されたところである。

サイバー演習への参加をよりよく生かすためには、事前の準備が肝要である。米国のHSEEP（Homeland Security Exercise and Evaluation Program）[10]はサイバー演習に限らず、米国政府が行う演習において用いられている手法であり、演習を効率的に実施するためのポイントがまとめられている（図表2）。HSEEPでは演習目的の明確化、特にその演習で検証すべき重要な組織の能力（Core capability）が何であるかを定義し、明確にした上でシナリオや検証項目、検証方法を組み立てることが望ましい、としている。

また演習の成功を左右するのは、事務局、コントローラー、評価者などのスタッフであり、演習に先立ちこれらの役割の明確化、適切な訓練の実施が必要である。演習事後においては、主要な参加者による振り返りの打ち合わせを実施するなど、演習の目的の達成度、あるいは演習の方法自体に対する反省や気づきを共有し、次につなげることが望ましい。

機能演習では、あらかじめ情報連携に係る手続き（情報連携のタイミング、内容、手段、秘密保持の範囲など）を文書化しておくことが望ましい。その内容と実際の演習結果を比較することで、手続き自体の問題点や、手続きの定着度合いを測ることができるからである。

なお自社で演習を企画する際には、シナリオ策定など一定の専門性が必要となることから、各種の演習に参加することによりノウハウを吸収すること、外部の知見を借りることも初期の段階では検討すべきである。

国内外で金融業界に対するサイバー攻撃へのリスク認識が高まる中、サイバー演習などを通じて金融機関の対応能力強化を図ることが今後ますます重要となろう。

Writer's Profile

平塚 知幸 Tomoyuki Hiratsuka
金融システムリスク管理部
上級コンサルタント
専門は金融、BCP、サイバーセキュリティ
focus@nri.co.jp