サイバー演習計画に関する G7 の基礎的要素（仮訳）

はじめに・概要

金融セクターで提供されるほとんどのサービスは、IT サービスの相互依存により左右されるようになっている。その原因が故意・悪意のものであるかどうかにかかわらず、IT の停止は、重要サービスを提供する組織に重大な影響を及ぼす。こうした依存性やインシデントに対する組織の対応力・インシデントからの復旧能力をより良く理解するために、金融分野において官・民ともにサイバーインシデントにおける対応と復旧策について定期的に演習を実施することが重要である。演習においては、サイバー攻撃への対応と復旧を効果的なものとするために、想定されるシナリオにおいて組織単独または横断的に幅広い手法を用いて訓練を実施する。こうした訓練を効果的に実施するため、金融機関や各法域は、複数年に亘る包括的な演習計画を策定することを選択できる。G7 では、破壊的なサイバーインシデントが発生した場合の対応・復旧手順を明確化するとともに、定期的に訓練する必要性の認識のもと、効果的なサイバー演習計画のための基礎的要素を策定した。

「サイバー演習計画に関する G7 の基礎的要素」は、拘束力のないハイレベルなものであり、各利害関係者にとってサイバー演習計画の策定へ導くツールとしての役割がある。また、法域・分野横断的にサイバー演習計画を策定するための指針となり得る。

サイバー演習計画に関する G7 の基礎的要素は、以下のパートで構成されている。

- パート A では、組織のインシデント対応と復旧の態勢・能力を向上させるために、複数の演習の種類・形式の組合せで構成される複数年に亘る演習計画を策定するための基礎的要素を概説する。
- パート B では、サイバー演習計画の中で個々の演習を構築、実施、評価するための基礎的要素を概説する。

Part A：演習計画の基礎的要素

演習計画は、演習の実施、評価、改善、再実施のサイクルからなり、組織における継続的な改善を可能にする。演習計画は、サイバーインシデントにおける対応と復旧対応策に関する理解を促す。演習は次の段階的アプローチの積み重ねにより成り立ち得るものである。(1)複雑化するリスクシナリオに対処することで、組織のサイバー対策を徐々に強化する、(2)インシデント管理プロセスと手順の改善に資する主要リスク指標・基準を構築する、(3)優先事項、脅威、リスクに関する共通理解を醸成する、(4)インシデントから復旧する能力の検証・基準化をする。

サイバーインシデントへの組織としての対応力・復旧力の改善度合いを効果的に測定するために、一連の演習を展開する必要がある。これらの演習を組み合わせることで、(1)組織に必要なあらゆる業務とそれに応じたサイバー脅威を対象とし、(2)必要な対応方針、手

順、能力の評価、(3)対応と復旧の改善の促進、(4)経時的な改善点の把握が可能となる。効果的な演習計画には通常、以下の要素が含まれる。

- 利害関係者の関与
- 複数年態勢における優先事項
- 改善計画

演習計画の基礎的要素 1：利害関係者の関与

まず、利害関係者の関与、特に組織内の重要人物の賛同があることは、良好な演習計画の立案・維持に資するものである。一般的に、演習計画には次の２種類の利害関係者が存在する。(1)演習計画全体の利害関係者、及び(2)演習計画全体の中の個別の演習の利害関係者である。これらの利害関係者を事前に特定しておくことで、演習計画全体の中の個別の演習の優先事項をより効果的に設定することができる。関連する利害関係者を特定する際には、演習計画の立案者は、他の企業や、サードパーティプロバイダなど自社が業務上依存する企業との相互接続関係を評価することがあり、この作業を「エコシステムスキャン（Ecosystem Scan)」と呼ぶ。演習計画には、個別の演習に参画するチームや組織を代表する者と同様の利害関係者を含めておくことが有効である。また、計画の監督・実行を担う合同演習委員会等のワーキンググループに利害関係者間の調整を担わせることができる。

演習計画では、計画を主管する役割を担う者として利害関係者間の調整を担う「主たる利害関係者（lead stakeholder)」を置くことができる。演習計画において、必要となる支援の確保、行動方針に沿った計画の実行、複数年に亘る計画の推進や、組織的な理解の維持のため、主たる利害関係者は、組織内の有力な幹部クラスでなければならない。主たる利害関係者は、演習計画において重点的に取り組むべきリスクを比較衡量することもできる。演習計画の一貫性と安定性を確保するために、演習計画の立案者は利害関係者の頻繁な変更を可能な限り避けるべきである。

複数年に亘る演習計画に包含される個別の演習には、演習計画の利害関係者のほか個別の演習の利害関係者が存在する。個別の演習においては、それぞれの演習の範囲や選択したシナリオに応じて異なる利害関係者も存在する。定期的なエコシステムスキャンの見直しや更新を行うことは、各演習と関連する利害関係者を最新状態に保つ上で有効である。

演習計画の基礎的要素 2：複数年態勢における優先事項

複数年に亘る演習計画は、改善したことを経過観察できるため法域や組織にとって大きな利益となる。複数年に亘る演習計画を成功させる鍵は、演習から学んだ教訓を演習計画や行動計画に採り込むことである。複数年に亘る総合的な演習計画は、演習から得られた教訓の他システム・演習への波及を考慮したり、優先事項を見直したりする点で役立つ。演習計画の立案者は、利害関係者や組織の経営陣によって承認されたリスク評価と複数年に亘る

優先事項を基に、その計画を検討することができる。

効果的な複数年態勢における優先事項は、明確、簡潔、測定可能、かつ現実的であり、リスク評価とも直結させるべきである。リスク評価とは、脆弱性・脅威分析とリスク軽減措置や技術的手法の組合せにより、組織、従業員、業務遂行能力、資産のリスクを特定し、優先順位付けすることである。リスクは、組織が依存していたり、論理的・物理的に接続していたりする外部企業に潜んでいることもある。金融セクターの相互接続性に鑑み、演習計画を立案しようとする組織は、外部企業起因のリスクを特定するために、脅威・リスク評価プロセスの一環としてエコシステムスキャンを実施することもできる。特にサイバーセキュリティの場合、組織におけるリスク・組織に対する脅威は急速に変化する可能性があり、新たな脅威やリスク評価の実施に伴い、定期的に、複数年に亘る優先事項を再評価することが必要となる場合もある。しかし、複数年に亘り定めた演習計画上の優先事項を更新する場合には、それが必須であることを確認するとともに、インシデント対応プロセスの改善を追跡する能力を阻害しないよう、慎重に行うべきである。また、複数年に亘る演習計画における優先事項を特定する際は、その計画の利害関係者が、予算やリソースの制約を考慮に入れることもできる。

演習計画の基礎的要素 3：改善計画

参加者のサイバーインシデントへの対応力・復旧力を向上すべき領域を特定することは、演習を実施する主な理由の一つである。 事後報告書（AAR=After Action Report）は、演習の評価結果を文書化したもので、評価に基づき改善に向けた具体的な提言を行うために活用することができる。改善すべき領域が特定されると、改善を推進するため、然るべき責任者や目標期限、測定可能な是正措置が設定される。

改善計画を AAR に盛り込むことで、特定された改善提案を前に進める際に、利害関係者の理解を得ることができ、サイバーインシデントへの組織としての対応力・復旧力の改善につながる。加えて、その後の演習で是正すべきギャップの特定につながり、演習計画そのものを強固なものとすることができる。

Part B：演習の基礎的要素

演習はインシデント対応における計画、作業、手順に習熟し評価するための機会であるとともに、失敗をしても責任を問われないリスクの低い機会である。そして、インシデント管理に責任を持つ者がインシデント発生時の自身の役割に慣れ親しむための場ともいえる。また、他の関係者を把握し彼らと関係性を築いたうえで、彼らのインシデントに対してどのようにアプローチするのか理解することもできる。複数年に亘る演習計画に含まれる個々の演習は、その規模、種類、複雑さ、目的、または重点分野がそれぞれ異なる場合がある。効果的な演習のためには、以下の要素が一般的に推奨される。

- 演習の計画と進行

- 演習の実施
- 演習の評価

個別演習の基礎的要素 1：演習の計画と進行

演習の計画段階においては、演習の種類、参加者とその役割、趣旨目的、複数年に亘る演習計画との整合性、シナリオの説明を概説し、準備・実施・評価を行うチームを特定する。複数年に亘る演習計画で共通の優先事項と各々の演習は結びついている一方、各々の演習は独自の目標と評価基準を持つことができる。目標は次の(1)～(4)の要素を備えていると最も効果的といえる。(1)明確、簡潔、測定可能であること、(2)達成可能であること、(3)複数年に亘る演習計画と適合していること、(4)脅威やリスク評価と直結していること。

評価基準は、演習が目的に一致するものであったか検証するための手段である。(演習の計画立案者が検討すべき演習の種類についての詳細は、Appendix※を参照。)

演習を効果的なものとするためには、参加者の選定は非常に重要である。演習の計画立案者は、各参加者が演習に独自の視点をもたらすことから、技術的な専門家に加えて、広報部署、法務部署、業務部門の責任者、姉妹機関、法執行機関、インターネットサービスプロバイダや通信事業といった重要なサードパーティなど、幅広い専門家を参加させることを検討してもよい。

演習シナリオを設計する際には、リスク評価と脅威インテリジェンス分析からのインプットを使用することで、より現実的なものとすることが可能である。種々の演習シナリオに対して、様々な脅威の主体とその能力を明示することは、貴重な洞察を提供し、特定の脅威に合わせてシナリオを調整するのに役立つ。対処すべきリスクの優先順位付けを容易にするために、演習計画では、発生可能性と影響度を基準として使用することができる。シナリオは、より複雑なものとなるよう調整することも可能であるが、複雑な演習では、様々な利害関係者や参加者との間で、追加の計画や教育セッションが必要となる場合がある。例えば、機能別演習（Functional exercise）を実践的なものとするうえでは、演習参加者間のコミュニケーションの道筋を確保するための練習が必要となる場合がある。演習と現実との混乱を避けるために、演習におけるコミュニケーションのルールや基準を設けることは重要である。さらに、参加者は、演習中に現実のイベントが発生する場合に備えて、緊急に演習を中断する方法について練習しておく必要があるかもしれない。ただし、机上演習（Tabletop exercise）やセミナー演習(Seminar exercise)といった種類の演習は、ディスカッションがベースとなるため、こうした追加的予防措置は不要である。

演習における行動に関して参加者が練習するときは、演習の計画立案者は演習が計画から脱線してしまう可能性を見据えた事前の準備が可能である。そのため、演習シナリオを作成する際に、演習の計画立案者は、参加者が予期せぬ動きをした場合に演習を元の軌道に戻すための追加のシナリオイベント（一般に「状況付与（インジェクト）」と呼ぶ）を準備し

てもよい。演習の脱線を受容することもあり得るが、それを許容するかどうかは事前に決めておくべきである。特定のプロセスについて検証することが演習の目的であるならば、演習が脱線しても演習の計画立案者は最終的には演習を軌道に戻すことができる。

シナリオを作成し参加者を特定することに加え、演習の計画立案者は、演習プロセス全体において、定期的に計画や教育のためのセッションを設けることができる。これらの目的は、利害関係者・参加者全体が演習の多様な面について共通の理解を有していることの確認である。演習の計画立案者は、主たる利害関係者が最終的な演習の在り方を支持していることについての確認が求められる。

最後に、演習の計画立案者は、計画段階で発見した問題やギャップの解決をしないこととしてもよい。ギャップの解決は他の利害関係者にとっては混乱要因となり、新たなリスクとなる。その代わり、演習の計画立案者は、システム所有者等が対処すべきものとしてギャップを提示してもよいし、演習を通じて参加者があぶり出すもの（もしくはあぶり出せなかったもの）として、ギャップに干渉せずにシナリオを進めてもよい。

個別演習の基礎的要素 2：演習の実施

演習の実施内容（参加者数やそれぞれの役割）は演習の種類によって様々である。全ての演習において、場所、技術、連絡手段、参加者の安全を確保するために、適切な工程管理ができていることが重要である。抜打ちで実施する演習ではない限り、資料の事前配布やブリーフィングミーティングは適宜実施されるべきである。これら考慮事項は、複数の法域が演習に参画するときはより重要である。

業務に不必要な中断、混乱、パニックが起きることを避けるため、重要な原則を検討することが重要である。演習実施に際して、計画者は以下を検討する。(1)演習におけるすべての連絡方法を明確・明瞭に示すこと、(2)通常業務への潜在的影響を最小限に抑えることができる日時、場所、方法を選択すること、(3)役割、責任、管理チームとの連絡方法を概説した状況説明書やその他必要な文書をすべての参加者に配布すること、(4)外部関係者には演習が行われることを適宜周知すること、(5)現実のイベントが発生したとき、これに対応する参加者が演習を離脱できるようにすること。

個別演習の基礎的要素 3：演習の評価

演習を評価する目的は、方針、手順、運用、システムの潜在的な改善点を特定すること、また、今後の演習の練度を高めることである。評価では演習結果をあらかじめ定めた目標・目的と比較し、演習中に記録した一連の出来事から弱点を分析する。

目的にどの程度合致していたかを測定し、現在の計画とのギャップや改善が可能な分野、あるいはうまくいった分野を特定するために、効果的な評価基準を用いる。参加者が、演習において単に合否や高得点を目指さないこと、演習本来の成果をはき違えないことが肝要である。なぜなら、単に合否や高得点を目指す演習の計画者や参加者は、演習中の問題点の

「解決」や発見に傾注できないからである。

演習を効果的に評価するため、演習実施直後に評価者や参加者との短時間のディスカッションセッションを設け、参加者の第一印象や反応を把握することができる。これは、「ホットウォッシュ」または「ホットデブリーフィング」と呼ばれ、改善計画の方向付けに活用されるべきであり、様々な役割に跨った幅広いフィードバックを可能とする。

演習の評価において評価者は、(1)参加者が手元の問題を的確に判断したか、(2)その行動が既存の方針や手順に準拠したものであったか、(3) その行動は問題を解決するのに有効だったか、(4)他の参加者がどのような理由で何をしたかを参加者が認識していたか、を評価することを目的として、参加者がとった行動とその結果を観察するべきである。これらの点は改善計画の基礎となる。

※Appendix は仮訳版では省略しています。