5

サイバー攻撃に備えた実践的演習 応般

江連三香
（株）三菱総合研究所

サイバー演習とは

サイバー演習の目的と成果

高度化するサイバー攻撃への備えとして，近年，サイバー演習が注目されている．サイバー演習とは，情報システムにおけるインシデント☆1対応体制・手順や，情報システムやサービスの稼働継続にかかわる手順・規程（IT-BCP 等）に関する実行可能性の検証や課題抽出を行うものである．具体的には，情報システムのインシデント発生を想定したシナリオを設定し，シナリオに基づき付与される状況に対して，演習参加者は，既存のマニュアルやルール等に基づき，望ましい対応を判断し，必要に応じて他参加者と連絡・連携しながら対応（または，判断・対応に関して議論）を行うことで，現状の課題を抽出する．

演習の成果としては，以下の点が期待できる．

- 既存の手順，ルール，ポリシー等の検証，課題抽出
- 組織間の連絡・連携体制，エスカレーション判断の検証，課題抽出
- 組織または個人の判断能力，対応能力・機能の検証，課題抽出
- 問題意識の共有，モチベーションの向上

サイバー演習を成功させるためには，(1) 組織に合致した目的の設定と関係者間での目的の共有，(2) 目的に沿った的確なシナリオの設定，(3) 演習を通じて抽出された課題の対策への反映，が重要であり，これらを継続的に実施することで，自組織のインシデント対応能力の段階的なレベルアップを図ることができる．

サイバー演習の種類

サイバー演習にはさまざまな種類があり（**表 -1**），それぞれの形式によってメリットや実現するためのコストが異なる．組織におけるインシデント対応計画の策定状況や対応能力等を踏まえ，目的に応じた形式で実施することが重要である．一般的には，セミナやワークショップ等，演習参加者の演習に対する意識の向上や目的の理解を図る研究的演習から開始し，議論を中心とした机上演習，実際の指示系統を用いた運用まで行う機能演習へ，段階的にレベルアップする．この際に，演習の各段階で得られた課題を，次の演習改善に反映することが必要である．演習がレベルアップするほど，演習内容の複雑性は増し，要求される組織の能力も上がるが，より深く実践的な課題の検証が可能となる．

主な演習形態を以下に示す．

▌セミナ，ワークショップ（研究的演習）

演習実施の前準備として，セミナ，ワークショップ等の講演形式で，参加者の演習概念や目的意義等の理解，参加者間の意識合わせを行う．講演を通じて，最新のセキュリティにかかわる脅威の動向やインシデント事例を理解し，演習の目的やメリットを理解することで，演習の必要性を認識し，参加者の意欲を高めることができる．さらに，参加者が自組織の対応計画や手順を確認することで，現状の組織の問題を認識し，演習において検証すべき課題を認識することができる．

▌机上演習

ファシリテータ（司会進行）の進行により，会議形式で議論を展開する形態の演習である．演習シナ

☆1 インシデント：事業活動や情報セキュリティを損ねる可能性のある，予期しないまたは望んでいない事象．サイバー攻撃（ウィルス感染や不正アクセス等），情報漏えい，情報システム障害等．

	目的	方法（例）
セミナ	意識啓発，認知，問題意識の共有	脅威や対策の動向，問題意識等についての講演
ワークショップ	対応方法の確認，相互理解の促進	インシデントに応じた対応計画や手順の確認・議論
通知訓練	情報連絡や指示系統の確認	通信手段・連絡先・手順等の妥当性の確認
ゲーム演習	意思決定・判断の検証，新手法の発掘	ゲーム形式（対抗戦等）による，インシデントへの対応の判断，効果的な対応の検討
机上演習	計画や手順の検証・評価	会議形式による，インシデントへの対応計画や手順の妥当性の確認・議論
機能演習	組織機能の検証・評価	実際の組織の連絡・指示系統，あるいは手段・施設等を用いた対応を通じた，インシデントへの対応計画や手順の妥当性の確認・議論
フルスケール演習	総合演習	現実の環境に近く，ほかの参加者のリアルタイムの対応も踏まえた，より実践的な対応計画や手順の妥当性の確認・議論

表 -1　主な演習の種類（例）

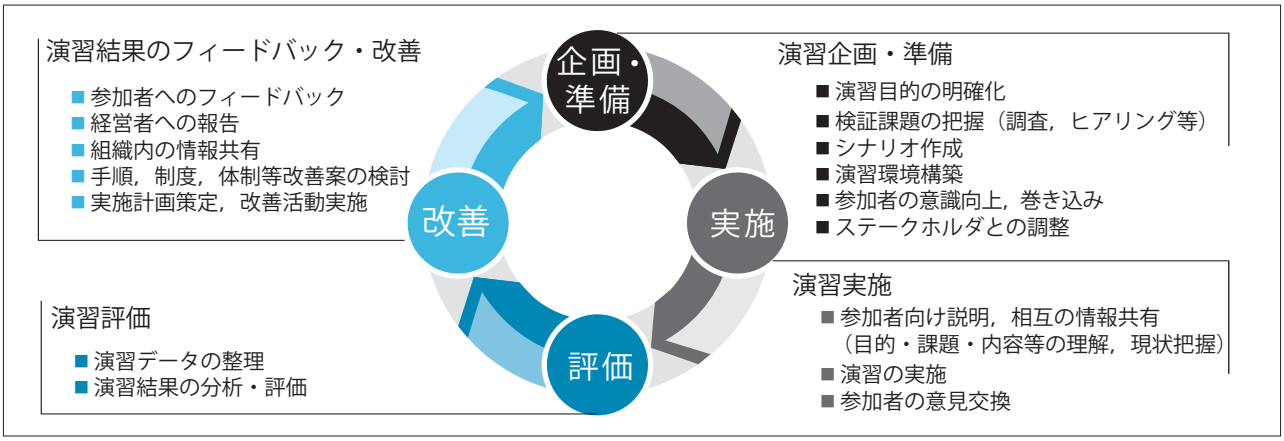

図 -1　サイバー演習の実施サイクル

リオに沿ってインシデントにかかわる状況が提示され，それぞれの状況でファシリテータが参加者に質問を行い，その状況下における望ましい対応や，さまざまな状況に適した対策等について議論を行い，参加者間の連絡・連携体制，対応手順やマニュアル，関連する制度等に関する整合性や有効性を検証する．

▌機能演習

実際の機器やシステム等の実環境を用いて対応を行う形態の演習である．演習シナリオに沿って模擬的なインシデントが実際の機器に発生（あるいはインジェクションとして提示）され，それぞれの状況に応じた望ましい対応を，必要に応じてほかの参加者と連絡・連携しながら行うことで，より実践的な対応課題を抽出する．

演習の進め方

サイバー演習の実施にあたっては，「企画・準備」「実施」「評価」「改善」の PDCA サイクルを回し，得られた課題や気づきを組織の改善計画・実行へ結び付けることが重要である（**図 -1**）．近年の高度化・複雑化する攻撃へ対応するために，一組織におけるインシデント対応機能や能力を高めることは当然のことながら，一組織で対応するには限界もあることから，組織内の部署間・あるいは企業間で共同で，各組織の専門能力や情報を活かしながら，連携を深めることで，全体の対応力を高めることが求められる．

▌企画・準備

演習企画・準備段階では，演習目的を定め，成果や達成すべき事項を明らかにする．参加組織のヒアリング等を通じて検証課題を明確化し，課題が検証可能なシナリオを作成する．また，演習環境（会場，情報インフラ等）を準備し，必要なマテリアルも準備する．

演習実施時には，参加者の問題意識も異なることは自然であり，必ずしも参加者の参加意欲が高い場合だけではない．組織のさまざまな立場の参加者がかかわる場合，それぞれの利害関係が異なることも

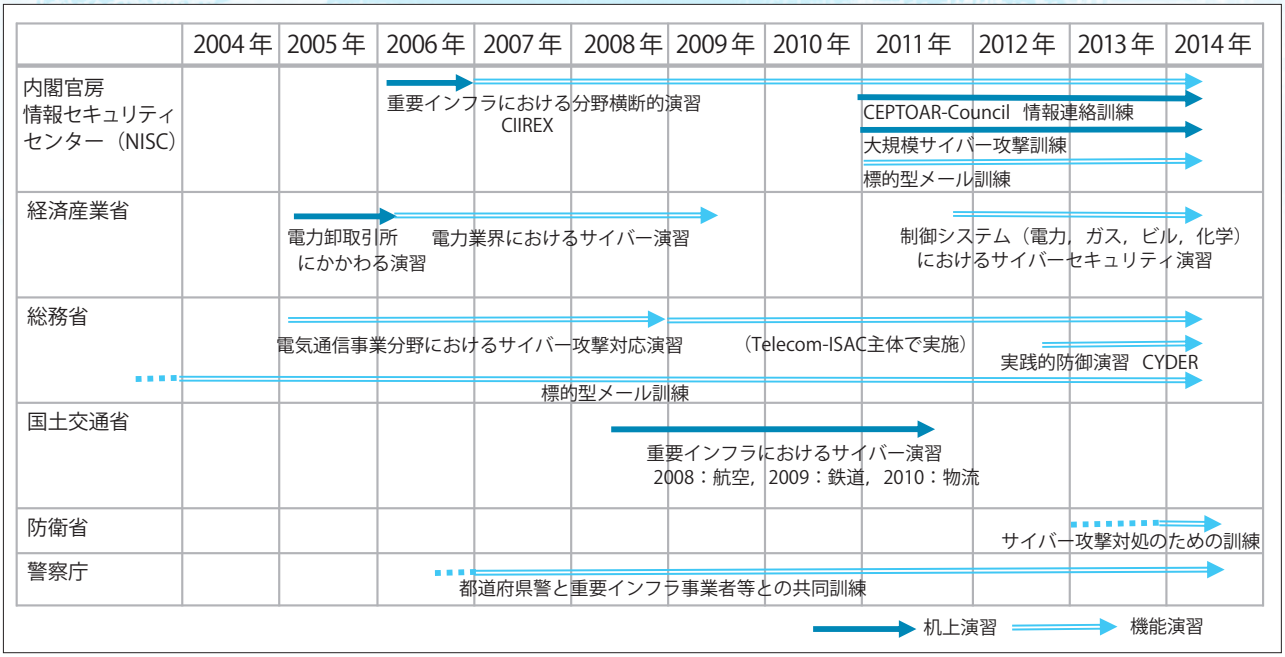

表 -2　国内の主なサイバー演習の経緯

ある．演習実施時には，企画側が一方的に実施を促すのではなく，企画・準備時点から，ステークホルダとの利害関係を考慮し，参加者が自ら積極的に検討に加わる体制・雰囲気を作ることで，参加者の参加意欲や成果に対する意識を高めることが可能となる．

▌実施

演習の前段階として説明会やセミナ等を実施し，演習目的や課題，そして演習実施方法の理解を図った後，実際の演習を実施する．演習では，コントローラ（事務局）よりシナリオに沿った状況付与がなされ，参加者は，既存の体制・手順やルール等に則り，必要な連絡連携・インシデント対応を行う．参加者のアクションによって，状況付与を変化させるダイナミックな進行を行う場合もある．演習終了後は，参加者の意見交換を行い，気づきの共有を行う．参加者のアクションは記録を取得し，後の評価・改善に活用する．

▌評価

演習結果の分析・評価を行う．結果は，演習当日のシステムログ，アクション記録，議事内容等のデータと，参加者によるアンケート結果等の自己評価を組み合わせて行う．検証すべき課題に沿って，コントローラが期待した参加者のアクションと実際のアクションを比較し，期待する行動ができたかできなかったか，その理由，想定する気づきが得られたかどうかを確認する．

▌改善

演習結果の評価を踏まえ，組織の課題を抽出し，次のセキュリティ対策にかかわる改善計画に反映させる．また，演習結果については，参加者にフィードバックすることで，対策実施や改善活動への意欲を高めるとともに，組織における適切なセキュリティ対策の推進のために，経営層にもフィードバックを行うことが有効である．

サイバー演習の動向

国内のサイバー演習の動向

国内でも，さまざまな形態のサイバー演習が実施されており（**表 -2**），重要インフラや政府機関等における脅威の高まりを反映し，特に近年，大規模な演習が実施されている（**表 -3**）．内閣官房情報セキュリティセンター（NISC）が実施している重要インフラにおける分野横断的演習は 2013 年度に 8 回目を数えており，重要インフラ分野における官民連携体制の機能向上を目指している．2012 年度は，経済産業省が制御システム分野におけるサイバーセ

	名称	目的	参加者	方法
内閣官房情報セキュリティセンター（NISC）	重要インフラ分野横断的演習（CIIREX）	重要インフラ事業者におけるBCP等の実効性の確認・問題点抽出	重要インフラ事業者等，セプター※1，関係機関，重要インフラ所管省庁，NISC	IT環境を利用した機能演習
経済産業省	サイバーセキュリティ演習【制御システムセキュリティセンター】	制御システムにおけるセキュリティ脅威の認識と対策等の知見の獲得	重要インフラ事業者等（電力，ガス，ビル，化学）	プラントの模擬システムを利用した機能演習
総務省	実戦的サイバー防護演習（CYDER）	官公庁・大企業等のLAN管理者のサイバー攻撃対応能力の向上	省庁，独立行政法人，民間企業	組織内ネットワークを模擬した環境を利用した機能演習

※1 セプター：CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）．各重要インフラ分野で整備されている情報共有体制．情報共有・分析機能を示す英文字の頭文字．

表-3　国内の主なサイバーセキュリティ演習

キュリティ演習を開始，2013年度は，総務省が実戦的サイバー防護演習（CYDER）を開始している．

国内のサイバー演習事例

▌制御システムセキュリティセンター「サイバーセキュリティ演習」

経済産業省では，2012年度より制御システムを対象としたサイバーセキュリティ演習を実施している．2013年度は，実施主体を技術研究組合制御システムセキュリティセンターに移し，電力・ガス・ビル・化学分野において，模擬プラントを利用したサイバーセキュリティ演習を実施した．演習の目的は，制御システムを運用する現場の担当者，技術者等における，(1) 制御システムセキュリティ上の脅威の認識，(2) インシデント発生の検知手順や障害対応手順の妥当性の検証，(3) セキュリティ対策等の知見の獲得である．制御システムセキュリティセンターでは，制御システムの特徴的な機能の一部を模擬的に再現した7種類の模擬システム（排水・下水，ビル制御システム，組立プラント，火力発電所訓練システム，ガスプラント，電力広域制御，化学プラント）を東北多賀城本部に備えている．これらの模擬プラントを利用して，模擬的にインシデントを発生させ，参加者が実際に対応することで，より実践的な課題の抽出を実現している．さらに，参加者が攻撃側・守備側に分かれて演習を行う手法を採り入れることで，現実的な攻撃手法と対策に関する課題を抽出している．

従来のサイバー演習は情報システムを対象としたものが中心であり，制御システムを対象とした演習事例は少ない．制御システムは，従来クローズで独自OSやプロトコルを用いたシステムであったが，近年汎用技術を利用する場合も出てきており，情報系の脅威も高まりつつある．24時間365日稼働を前提とした制御システム環境における効果的な対策の方法について，関係者間の議論・検討がなされているところである．演習環境を活用し，模擬プラント機能や演習シナリオのブラッシュアップを継続し，参加者が得られた気づきを組織の対策に活用することに加え，得られた知見を国や業界における対策推進のための制度・仕組み等の構築に反映させていくことが，制御システムセキュリティの向上に有効であろう．

▌内閣官房情報セキュリティセンター「分野横断的演習」

内閣官房情報セキュリティセンターでは，2006年度より継続して重要インフラにおける分野横断的演習を実施している．この演習の目的は，重要インフラ事業者におけるBCP☆2等の実効性の確認・問題点抽出を通じて，分野横断的な脅威に対する共通認識の醸成，他分野の対応状況把握による自分野の対応力強化，官民の情報共有をより効果的に運用するための方策検討を推進し，分野横断的な重要インフラ防護策の向上を目指すことである．8回目の実施となる2013年度は，重要インフラ事業者等（10分野☆3 38機関），セプター（10分野15セプター），政府機関等，過去最大の61組織212名が参加した

☆2 BCP：Business Continuity Plan，事業継続計画．

☆3 重要インフラ10分野：情報通信（通信・放送），金融，航空，鉄道，電力，ガス，政府・行政サービス，医療，水道，物流．

写真 1　サイバー演習の様子
監視室で異常検知し，現場に連絡

写真 2　火力発電所訓練システム
現場で使われる実際の画面を表示

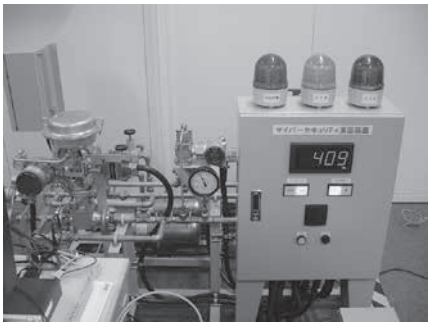

写真 3　ガスプラントシステム
不正な制御による圧力上昇等を再現

（うち 3 組織 10 名が自職場参加）.

分野横断的演習は，2005 年 12 月「重要インフラの情報セキュリティ対策に係る行動計画」（第 1 次行動計画）でその実施を取り決められたことに端を発し，2006 年度には，我が国における IT 障害に関する初の分野横断的演習として机上演習が実施され，官民連携の仕組み作り，官民連携の枠組みの実効性向上のための取り組みや課題の発見がなされた．第 1 次行動計画の 3 カ年は，官民の情報共有・連絡連携の仕組みの構築・実効性の検証が目的とされたが，2009 年 2 月「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」（第 2 次行動計画）では，分野横断的な重要インフラ防護対策のさらなる向上を目指し，官民連携体制の検証に加え，演習参加者における BCP の策定・改訂に向けた気づきの獲得，課題の抽出にも重点が置かれている．

2013 年度の演習は，複数の情報セキュリティインシデントにかかわる予兆が検知される中，複数分野においてサービスへの影響が発生，うち一部の影響が他分野にも波及することで，多くの重要インフラ事業者等において，インシデントの防止や被害最小化，事業継続対応が迫られる事態を想定した演習であった．各重要インフラ事業者においては，予兆に対する日頃からの対応準備，復旧の優先順位策定，インシデントの影響範囲に応じた対策や体制の事前の検討，他社の対応を参考にした自社の取り組みへの反映等が重要であるとの意見が得られた．

2014 年度からは「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」に基づき，重要インフラ保護対策が推進される．分野横断的演習についても，重要インフラ分野の IT 障害対応体制を強化する中核的な取り組みとして充実を図り，ほかの省庁の演習・訓練との相互連携や補完を通じた，分野内の「縦」方向と分野間の「横方向」の体制強化，重要インフラ分野内の成果の浸透，行動計画の他施策への反映等が目指されている．さらに，重要インフラ分野は，従来の 10 分野に加え，化学・石油・クレジットの 3 分野が新たに追加される．我が国の重要インフラ防護能力の維持・向上のために，分野横断的演習の果たす役割はますます重要となるであろう．

海外のサイバー演習の動向

▌米国のサイバー演習の動向

米国では，軍を中心に，サイバー攻撃対処計画の改善や対処能力の向上を目的として，1990 年代後半からさまざまなサイバー演習が実施されてきた．現在，実施されている最も規模の大きな演習は，米 国 DHS（Department of Homeland Security：国土安全保障省）が実施する「サイバーストーム（Cyber Storm）」で，官（連邦／州政府／自治体）および民間セクタ（主に重要インフラ事業者），各分野の ISAC[☆4] 等が参加する，官民のインシデントに対する準備・防護・対応強化のための演習である．Cyber Storm（I ～ IV）全体に共通する目的は，(1) インシデントとその潜在的な影響に対する組

☆4 ISAC：Information Sharing and Analysis Centers，米国の重要インフラにおける情報共有体制.

織対応能力の検証，(2) 国家方針（National Cyber Incident Response Plan 等）と整合した戦略的意思決定と省庁間のインシデント対応連携の訓練，(3) 状況認識のための情報共有関係・連絡パスの検証，(4) 機密情報を保護しつつ，組織間の情報共通を行うためのプロセスの検証政府の意思決定・調整機能であり，これまで，2006 年，2008 年，2010 年，2012 ～ 2013 年の 4 回が実施されている．直近の「Cyber Storm IV」は，特に「サイバー対応力の評価」「変化する脅威に対する対応プロセスの検証」「連邦政府，州政府，国外組織，民間組織との情報共有の強化」に重点が置かれており，海外からも日本を含む 10 カ国が参加した．演習結果は，米国のインシデントに関する情報共有・インシデント対応体制に関する計画である「国家サイバーインシデント対応計画（National Cyber Incident Response Plan：NCIRP）」に基づくプロセスや体制の改訂や，国家演習プログラム（National Exercise Program：NEP）に基づき実施される計画，組織化，遂行，評価等のための国家レベルの包括的な演習である「National Level Exercise 2012（NLE12）」の計画にフィードバックされている．

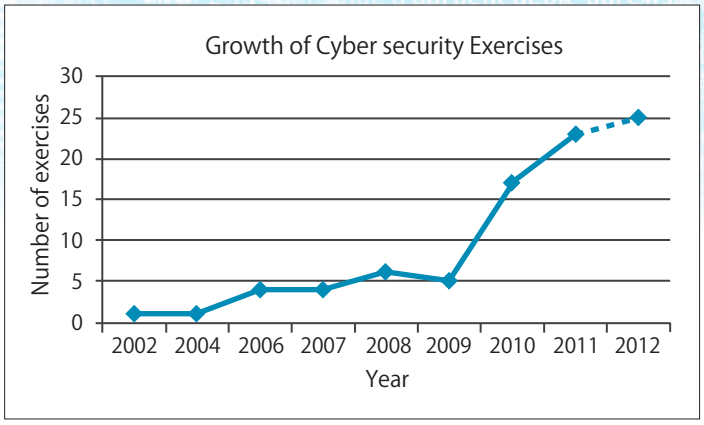

図 -2　欧州におけるサイバー演習の推移

▌欧州のサイバー演習の動向

EU では，ENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁）がサイバーセキュリティに関して EU 加盟国や欧州諸機関への提言や連携促進を行っている．ENISA が 2010 年，2012 年に実施したサイバー演習「Cyber Europe」は，大規模なサイバー攻撃に対する欧州諸国の対応強化のための連携体制の構築を目的とし，EU 加盟国の関連省庁，CERT[☆5] 組織，情報機関等が参加した．Cyber Europe 2012 の目的は，「欧州の政府機関のための既存メカニズム，手順，情報の流れについての効率性とスケーラビリティの検証」「欧州の官民ステークホルダの連携」「欧州におけるサイバーインシデントの対応力に関するギャップと課題の特定」である．2014 年には過去 2 回より規模と複雑度が増した「Cyber Europe 2014」が行われる．

ENISA によるレポート「National and International Cyber Security Exercise」は，サイバー演習に参加する欧州および国際組織に対する知見や教訓の提供を通じたサイバー演習の実施支援を目的としており，2002 年から 2012 年までの 85 のサイバー演習を対象とした調査結果がまとめられている．このレポートによると，調査対象とした演習の 71 % が直近の 3 年間（2010 年～ 2012 年）に実施されており（**図 -2**），欧州各国政府や民間組織がサイバー攻撃を深刻に捉えている状況が窺える．また，演習の 39% が多国間演習であることから，今後国際レベルでの協力が進展すること，さらに，57% に公共部門と民間部門の両方が参加していることから，インシデントへの対応においては民間部門が重要な役割を果たしており，サイバー演習における官民協力は今後増加することが想定される．

サイバー演習の有効活用に向けて

国内外におけるサイバー演習であるが，今後さらに有効に活用するためのポイントを 3 つ挙げる．

1 点目は，国内各省庁，あるいは世界的に実施されているサイバー演習で得られた専門知識や課題の共有による，より実践的な課題の検証と気づきの深

☆5 CERT：Computer Emergency Response Team，コンピュータ緊急対応センター．

化である．現在，サイバー演習にかかわる取り組みは個々に行われているが，関係者間で演習にかかわる知見を共有し，協調を進めることで，演習手法を向上し，双方の学びの効果を高めることが可能と考えられる．また，日本では防災分野での演習・訓練の知見が豊富にあり，関連分野との協力の在り方の検討も有用であろう．

2点目は，サイバー攻撃に対する組織間・官民・国際連携の重要性を踏まえた，関係者を拡大したより実践的で複雑なサイバー演習の実施である．多くのサイバー攻撃は，国境を越え，その対応には国家間の連携が必要である．また，一組織においても，情報システム部門・情報管理部門・広報部門・現業部門等，多くの部門が連携し，対応にあたらなければならない．さらに，高度化する攻撃に対しては，インシデントにかかわる情報を，国家間･官民等，関係者間で適切に共有し，インシデントの予防や被害拡大防止に向けて適切な備えを行うことが，防御力を高めるために重要である．そのためには，各国･官民の関係者が連携し，異なるプロセス，戦略を持つ複数の組織が，複雑なインシデントを模擬的に経験することが可能なサイバー演習を企画・実施することが有効である．

3点目は，サイバー演習から得られた気づきをフィードバックする仕組みの構築である．サイバー演習は国家レベルから，一組織のレベルまでさまざまなレベルで行われているが，いずれの演習においても，演習結果を適切に対策の向上につなげることが演習の目的である．演習の実施レベルに応じ，適切なフィードバックを行うための体制・仕組み作り，演習成果の展開，演習記録・分析のための管理ツールの開発等を進めることが，演習の効果を高める上でさらに重要となるだろう．

（2014年4月15日受付）

江連三香　e-mika@mri.co.jp

1999年，（株）三菱総合研究所入社．サイバーセキュリティを中心に，情報技術，情報政策等に関する調査研究･コンサルティングに従事．重要インフラのサイバー演習等を支援．