# CSIRT の実効性を高めるサイバーセキュリティ演習

## Cyber Security Exercise to Enhance the Effectiveness of CSIRT

佐　藤　重　之

**要　約**　セキュリティインシデント対応の体制は SOC（Security Operation Center）と CSIRT（Computer Security Incident Response Team）で構成される．SOC はセキュリティインシデントを検知し通信記録（ログ）等を分析する．CSIRT はインシデントが発生した際のインシデントハンドリングに加えて，インシデント事前対応やセキュリティ品質向上対応を行いインシデントマネジメント活動の中核を担う．CSIRT の実効性を確実にするためにはサイバーセキュリティ演習が有効である．日本ユニシスグループでは，CSIRT のサイバーセキュリティ演習を，演習の企画，演習の実施，フィードバック，課題整理という流れで実施しており，重大インシデント発生時の初動対応の能力強化に注力し，要員全体のスキルアップと組織としての連携を深めることができた．

**Abstract**　The organization for responding to security incidents consists of a Security Operation Center (SOC) and a Computer Security Incident Response Team (CSIRT). The SOC detects security incidents and analyzes communication records (logs) and the like. In addition to incident handling when an incident occurs, CSIRT plays a central role in incident management activities by responding to incidents and improving security quality. Cyber security exercises are effective to ensure the effectiveness of the CSIRT. The Nihon Unisys Group is carrying out CSIRT's cyber security exercises as a series of exercise planning, exercise execution, feedback, and problem arrangement, focusing on strengthening the ability to respond initially to serious incidents, and skills for the entire workforce, and we were able to deepen cooperation between the upskill and the organization.

## 1. は　じ　め　に

昨今，セキュリティインシデントは必ず発生するという前提を持って，セキュリティ対策やセキュリティ対応組織を整備することが一般的な考えとして定着してきている．2015 年 10 月，経済産業省が独立行政法人情報処理推進機構（IPA）と共に策定して初版を公開し，2017 年 11 月に Ver2.0 として改訂した「サイバーセキュリティ経営ガイドライン」[1]では，サイバー攻撃は避けられないリスクであると定義されており，企業における重要な経営課題としてとらえられ始めている．このような背景から多くの企業で，サイバー攻撃などのセキュリティインシデントへの備えとして，CSIRT（Computer Security Incident Response Team）等のセキュリティ対応体制の整備が進められているが，実効性の伴わない組織も多く，対応能力の向上が急務となっている．サイバーセキュリティ経営ガイドラインにおいても，演習が実施されていないと適切な行動ができないことを例として挙げた上で，その対処としてインシデント発生時の対応について，適宜実践的な演習を実施させることを経営層に求めている．

本稿では，セキュリティインシデントへの対処（インシデントハンドリング）の実効性を高

めるサイバーセキュリティ演習について述べる．まず2章にて演習を実施する対象となるセキュリティ対応体制を整理した上で，3章で演習によって向上させなくてはならないインシデントハンドリング能力を示し，4章でサイバーセキュリティ演習を解説し，5章で日本ユニシス株式会社とグループ会社（以降，日本ユニシスグループ）のCSIRTで実践した演習を紹介することを通じて，演習によって得られる成果や整理できる課題について述べる．

## 2. セキュリティ対応体制の概要

多くの企業や組織において，セキュリティインシデントに対応するための体制が構築されているが，それらは法律や規格で定められているものではなく形態は様々である．本章では，日本セキュリティオペレーション事業者協議会（ISOG-J）が公開している「セキュリティ対応組織（SOC/CSIRT）の教科書」[2]を参考にセキュリティインシデントへの対応体制に求められる役割を整理する．セキュリティインシデント対応の役割は，主にセキュリティインシデントの検知や通信記録（ログ）等の分析，インシデントが発生した際の対応（インシデントハンドリング）である．多くの場合，前者はSOC（Security Operation Center），後者はCSIRT（Computer Security Incident Response Team）と呼ばれる体制で対応する．これらの体制は，組織の中で同一の要員で構成されることもあれば，全く異なる要員で構成されることもあるが，一連のインシデント対応において密接に連携し，被害を食い止める，若しくは被害を最小化することを目的として共に活動する組織である．各セキュリティ対応体制の役割と関係を図1に示す．

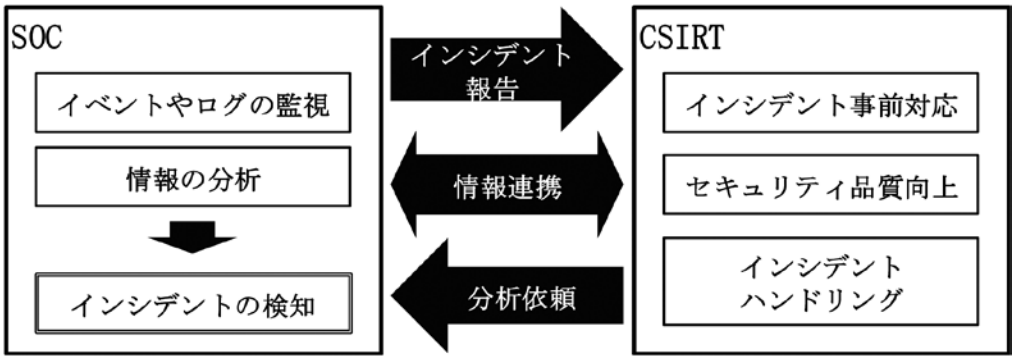


**図1　セキュリティ対応体制の関係図**

### 2.1　SOC（Security Operation Center）

SOCは，組織に導入されている侵入検知/防御装置（IDS/IPS[*1]）やWebアプリケーションファイアウォール（WAF[*2]）などのセキュリティ対策ソリューションから通知されるセキュリティイベント（アラート）や，ファイアウォールやルータのアクセスリストで処理された通信のアクセスログなどを監視する．SOCのアナリストは，監視している装置から通知された情報を分析し，インシデントを検知してCSIRTへ報告する．SOCは，自組織の中で体制を保持（プライベートSOC（PSOC）と呼ばれることもある）することもあるが，導入されているセキュリティソリューションの提供ベンダーやセキュリティ専門ベンダーなど，外部のベンダーにその役割を委託することもできる．

### 2. 2　CSIRT（Computer Security Incident Response Team）

CSIRT は，前節にて説明した SOC から報告されたセキュリティインシデントや，組織内外からの申告に応じてインシデントハンドリングを実施する以外にも，多くの役割や活動がある．セキュリティ関連情報の収集と注意喚起や脆弱性への対応（パッチ適応）などのセキュリティインシデント発生のリスクを低減させるための準備を実施するインシデント事前対応，組織内のリスクアセスメントによるリスクの特定，セキュリティの教育による普及活動を始めとしたセキュリティ品質向上対応により，インシデントマネジメント活動の中核を担う．SOC と同様に，外部のセキュリティ専門ベンダーの CSIRT 運用支援サービスなどを活用することもできるが，インシデントハンドリングを実施する際の全体統括，事象や得られた情報を基に対応策の優先順位を判断する作業，社内外の情報を収集/連携して正しい判断材料を得たり，状況に応じて外部のセキュリティ団体の支援を受ける調整をするといった自組織のビジネスインパクトに関わる主要な役割は自組織内で対応する能力が求められる．次章にて CSIRT のインシデントハンドリング能力について述べる．

## 3.　CSIRT のインシデントハンドリング能力

セキュリティ対応体制と同様に，CSIRT のインシデントハンドリングも組織によって対応範囲が異なるが，ここでは一般社団法人 JPCERT コーディネーションセンターが公開する「CSIRT ガイド」[3]を例として，インシデントハンドリングについて整理する．

インシデントハンドリングは，CSIRT が対応を担うインシデントマネジメントの一部である．インシデントの連絡受付（PoC：Point of Contact）やトリアージと呼ばれる対応優先順位決め作業，インシデントへの対処（インシデントレスポンス），そして報告や情報公開と様々

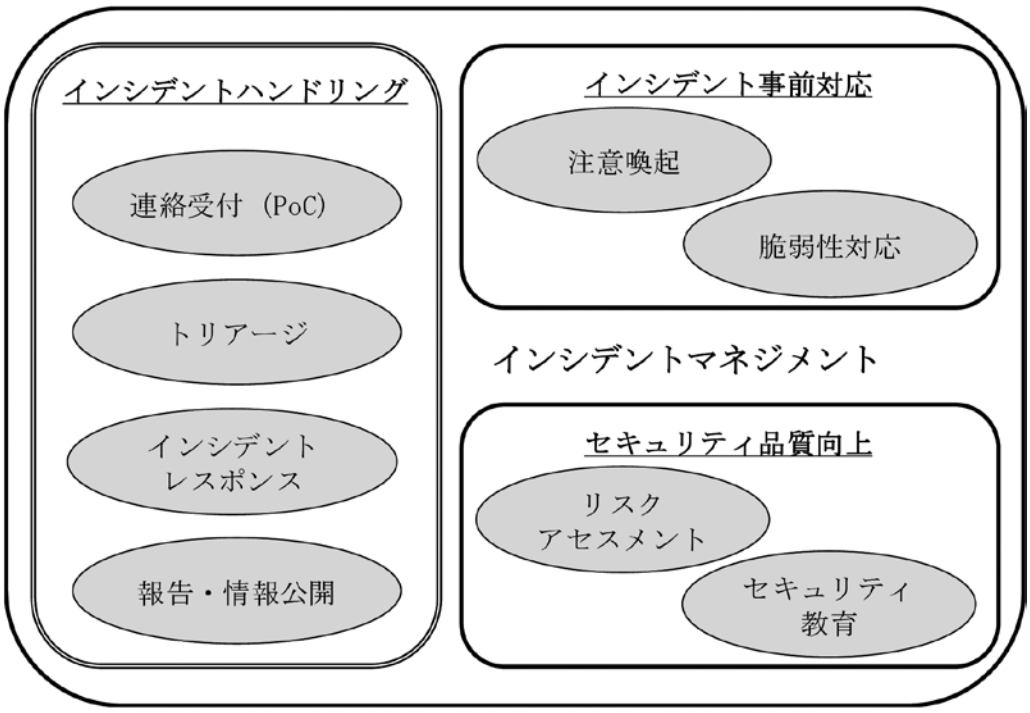


図 2　インシデントマネジメントとインシデントハンドリングの関係

な対応に分類されるインシデントハンドリングには，それぞれの対応を実行する能力が求められる．インシデントマネジメントとインシデントハンドリングの関係を図2に示す．当然ながら，どの対応もCSIRTが構築されれば即座に実行できる能力が備わっているものではなく，継続的に強化していかなくてはならない．本章では，CSIRTの要員・組織の役割と対応能力を整理し，対応能力の強化について述べる．

### 3.1　CSIRTに求められる要員の役割と対応能力

CSIRTの対応能力は，個々の要員の能力と組織としての能力に分類される．個々の要員の役割と必要と考えられる能力について，日本シーサート協議会（NCA）より公開されている「CSIRT人材の定義と確保」（Ver. 1.5）[4]を参考にして表1に示す．CSIRTには多くの役割があり，要員はそれぞれ前提となる各役割のスペシャリストとしての能力が求められる．さらに，CSIRTの要員には，様々な部署や組織，外部のCSIRTやセキュリティ団体などと連携するためのコミュニケーション能力と，重要な情報を取り扱う者としての高い倫理観が求められる．

**表1　CSIRT要員の主な役割と必要な能力**

| 要員の役割 | 役割概要 | 役割の遂行に必要と考えられる能力 |
|---|---|---|
| PoC（Point of Contact） | 組織内外の連絡担当 | セキュリティ知識（基礎） |
| リーガルアドバイザー | 法務関連担当 | 法律知識，ガイドライン |
| ノーティフィケーション担当 | 情報発信担当 | セキュリティ知識（全般） |
| リサーチャー/キュレーター | 情報収集・分析担当 | セキュリティ技術，情報収集分析技術 |
| 脆弱性診断士 | 脆弱性診断・評価担当 | 脆弱性知識，診断手法 |
| セルフアセスメント担当 | アセスメント担当 | セキュリティポリシー |
| ソリューションアナリスト | セキュリティ対策戦略担当 | セキュリティ技術，製品知識 |
| コマンダー | 全体統率 | インシデントレスポンス手法，マネージメント |
| インシデントマネージャー | インシデント管理担当 | インシデントレスポンス手法，マネージメント |
| インシデントハンドラー | インシデント処理担当 | インシデントレスポンス技術，セキュリティ技術 |
| 調査担当（インベスティゲーター） | 調査・捜査担当 | 攻撃手法，調査手法，法律知識 |
| トリアージ担当 | 優先順位選定担当 | 攻撃手法 |
| フォレンジック*3担当 | フォレンジック担当 | インシデントレスポンス技術，セキュリティ技術 |
| 教育担当 | 教育・啓発担当 | セキュリティ知識（全般） |

一方，CSIRTの組織としては，インシデント発生時の被害を最小限にとどめるというダメージコントロールの目的を遂行するため，それぞれの要員が持つ知識や技術が組織の中で最大限に活用されるように様々な準備や仕掛けが求められる．例えば，そのCSIRTが対応する対象となる範囲や責任を定義し，各要員に対する明確な役割を任命する．そして，日々の活動ポリ

シーやインシデント発生時の対応マニュアル，エスカレーションルールなどの規程や手順類を整備しておき，要員に対して周知され実践することで，初めて CSIRT として求められる活動を遂行することができる．

### 3. 2　CSIRT の能力強化策の分類

前節で述べた通り，CSIRT には多くの能力が求められ，それぞれが能力を発揮できるように強化していくための対応策を検討しなければならない．要員と組織それぞれの能力を強化する手法について，米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が公開している「SP800-84　IT 計画および IT 対応能力のためのテスト，トレーニング，演習プログラムのガイド」[5][6]を参考に，その分類を整理する．

#### 3. 2. 1　トレーニング（要員の強化対応）

トレーニングとは，CSIRT 要員に対して役割と責任に関連する技能を高めることである．主に，専門の教育サービスを受講したり，セキュリティの専門書籍などで学習したりする方法がある．CSIRT の役割におけるセキュリティ技術の研鑽や知識の習得に特化した教育サービスは様々なベンダーより数多く提供されており，例えば，SANS Institute は世界的にも有名なトレーニングプログラムを提供している．セキュリティ全般の概要を知識として得るコース，ファイアウォール・IDS/IPS・WAF・ログ統合管理ツール（SIEM[*4]）など様々なセキュリティ対策ソリューションの機能や活用方法を習得するコース，ネットワークトラフィックやハードウェアのフォレンジック技術を学ぶコース，脆弱性診断[*5]の手順やペネトレーションテスト[*6]の技法を実践するコースなど，様々なトレーニングコースが用意されている．また，サイバーレンジ（サイバー攻撃や防御を疑似的に実行する空間やシステム）を使ったトレーニングを提供している教育サービスも存在する．サイバーレンジを使うことで，実際のシステムに類似した環境の中で，攻撃を受けたときのセキュリティ装置の反応やシステムへの影響，解析の手順や防御の方法による対策の効果など，一連のインシデントレスポンスを疑似的に体験できる．CSIRT 要員として，特にインシデントハンドラーや調査要員にとっての技術力強化に有効である．サイバーレンジでのトレーニングは，機能演習と呼ばれることもあるが，3. 2. 3 項で述べる演習とは異なり，本稿では要員の能力向上のためのトレーニングの一種と定義している．

トレーニングは，各要員が実際のインシデント対応に臨むための準備となり，次項以降で述べるテストや演習を実施する上で，必要な知識や技術を習得しておくために先立って実施することが有効である．

#### 3. 2. 2　テスト（予測値の正当性確認と活動手順の評価）

テストとは，定量化できる測定基準または予測される結果を用いて，対象となるシステムや手法の正当性を計測するための評価手段である．即ち，CSIRT がインシデント発生時に活用するインシデント対応フローなどの手順やマニュアルが，予測の上で定義された結果の通りに運用できるかを確認することである．これは想定した事態への対応方法を学習することが目的ではなく，その対応方法や手順が正当で実効性があるかを確認し，改善すべき問題点を検出することが本来の目的となる強化策である．

例えば，セキュリティ機器がイベントを検知してから定められた時間内にエスカレーションすることができるかを確認するテスト，マニュアル化されたインシデント（コンピュータの紛失や機器の故障などの作業手順が明確なインシデント）が発生した際の対応手順を実際に実行して手順通りに作業が進められるかを確認するテストを行うことで，準備されている手順通りの対応ができるかを評価する．

テストの内容によっては，要員がテストした作業手順を正しく認識することができるといった能力向上にも繋がるが，定義された手順通りに実行できないことで，その手順やマニュアルの不備を発見して正すことができるため，組織としてのインシデント発生への備えを最適化させることに繋がる．また，システム運用に関わる対応マニュアルについては，システムのバージョンアップや設定情報の変化が想定され，エスカレーションルートは，組織改編や人事異動，担当職員の退職などで変更されるため，定期的なテストによる記述の確認が推奨される．

#### 3. 2. 3　演習（組織の能力向上）

演習とは，インシデントレスポンスのシミュレーションを実施することである．例えば，インシデントハンドリングへの備えとして，インシデント対応計画や操作マニュアルなどのCSIRT の活動ドキュメントを活用し，インシデント発生を想定したシナリオに対して，円滑に正しい判断をすることができるかを検証することである．

CSIRT の要員は，トレーニングで断片的，または疑似的にインシデントハンドリングの技術を学習できるが，それだけでは実際に発生する可能性のあるインシデントに対して，組織として連携して対応する能力を得ることは難しいため，演習を通じてインシデントハンドリングの経験を積むことが重要な能力強化となる．しかし，単にインシデントのシナリオを検討してシミュレーションすれば，良好な組織の能力向上を達成できるわけではない．要員へのトレーニングが不十分なことによって知識や技術が備わっていない場合やドキュメント整備などのインシデントハンドリングへの備えが十分にできていない状態だと，演習を実施しても想定したシナリオに沿った対応をすることができず，全体的に演習の効果が得られにくい状況となる．演習については，改めて 4 章で詳細に述べる．

なお，この活動を訓練と呼称することもあるが，訓練は定められた手順を，より正確にスピーディーに実施することを指す場合が多く，本稿では，テストの一環と考えて分類に含めないものとした．

### 3. 3　CSIRT 能力の評価

前節で述べた通り，組織として未成熟な CSIRT では，演習を実施しても十分な成果が得られない可能性が高くなる．要員の能力については，役割に応じた知識を測るためのセキュリティ関連資格や技術資格があり，取得状況によって一定の評価が行える．しかし，組織としてCSIRT の成熟度合いを，基準や評価項目の無い中で自ら正しく測定することは非常に困難である．

CSIRT の能力を客観的に評価する指標の一例として，欧州を中心に活用されている評価モデル「SIM3（Security Incident Management Maturity Model）」[7]が活用できる．SIM3 は，「Organisation（組織）」「Human（人材）」「Tools（ツール）」「Processes（プロセス）」の四つの領域に分かれた合計 45 個のパラメータに対して，それぞれレベル 0 ～ 4 の 5 段階のレベル

で CSIRT を評価できるツールである．各パラメータを用いて，組織がどのような状況であればどのレベルに該当するかを評価し，それぞれのパラメータに自組織のレベルを設定していく．パラメータは，CSIRT 内で何も議論がなされていないまたはチーム内で認識されていなければレベル 0，対応方法を認識しているが文書化されていなければレベル 1，文書化されていればレベル 2，その文書が CSIRT の管理者によって承認されていればレベル 3，そして，組織の経営層が内容を把握して組織の正式な文書として承認されていればレベル 4 となる．

SIM3 を利用した成熟度評価方法が，欧州ネットワーク・情報セキュリティ機関（ENISA）より公開されており[8]，SIM3 の各パラメータに対して実効的な CSIRT を運用するために，それぞれどのレベルであるべきかといった指標も掲載されている．

## 4.　サイバーセキュリティ演習の概要

CSIRT が構築されると，様々なプロセスの検討やドキュメントの作成などの準備がなされているものと考えるが，その実効性をより確実なものにするためにはサイバーセキュリティ演習が有効とされている．本章では，演習の必要性と種類を整理し，演習を実施すべきタイミングについても述べる．

### 4. 1　演習の必要性

CSIRT 要員それぞれがセキュリティ分野におけるスペシャリストであっても，それぞれの要員が自身の役割やチーム内での情報伝達のルールや連携方法などの認識を共有していないと，セキュリティインシデントが発生した際の対応が混乱し，適切な対応ができず被害が拡大してしまう．このような混乱や対応不備を発生させないために，インシデントの発生を想定したサイバーセキュリティ演習が有効である．インシデント発生時に，CSIRT が完全に稼働できる状態とは限らない．最悪の状態を想定して，対応する要員が，その時の最善の対応を実施し，できる限り被害を最小化するためにも，定期的なサイバーセキュリティ演習を実践し，CSIRT としての熟練度を高めておくべきである．サイバーセキュリティのインシデント対応では，被害を食い止めるための緊急対策を適用し，様々な調査を繰り返しながら攻撃者の手段から真因を明らかにした上で，恒久的な再発防止策を適用するという，限られた時間の中での対応の柔軟性が求められる．セキュリティインシデントの実戦の機会が限定的であることも，演習が必要とされる大きな理由である．

### 4. 2　演習の種類

CSIRT が中心となって実践する演習は，主にサイバーセキュリティ演習と呼ばれ，机上演習（TTX：Table Top Exercise）の形式で実施されることが多い．机上演習は，CSIRT メンバーを会議室などの部屋に集合させ，ファシリテーターの進行により，ワークショップ形式で議論を行う方式で実施される．演習の企画担当者によって準備されたインシデントシナリオに沿って，その時の状況に応じた望ましい対処や，様々な事象に適した対応策をメンバーで議論しながら進行していく．その際，CSIRT で準備した対応プロセスやインシデント対応マニュアル等を活用することで CSIRT の実効性を確認することができる．しかし，机上演習は実施する形態によって，演習実施のステップや準備の労力，得られる成果や効果が大きく異なる．本節では，机上演習を実施する形態に応じたメリットとデメリットを示した上でそれぞれの期待さ

れる効果と共に，演習を実施すべきタイミングについて述べる．

#### 4.2.1　単独演習

システム環境，システムの利用状況，業務形態や体制など，単独の CSIRT の活動範囲の中で発生する可能性のあるインシデントを想定してシナリオを作成し，その組織単独で実施する演習を単独演習と呼ぶ．

単独演習では，実在の環境を考慮して実施するため，組織内で実際に発生するインシデントに対する CSIRT の活動と同等のインシデントハンドリング対応を疑似的に経験することができ，CSIRT が現実にインシデントハンドリングを実践する際の実効性を測ることができる．

しかし，単独演習を実施するには，単独組織で演習の企画や準備を実施するため，対応コストが次項で述べる共同演習に比べて大きくなることが想定される．企画担当者をはじめ，CSIRT や社内システム関係者，シナリオによっては広報部門や法務部門など多くの部門が演習に携わることもあるため，それぞれの要員にかかるコストや演習実施日程の調整，参加者が兼務の場合は業務の調整などの負担を伴う．また，セキュリティの知識が乏しいメンバーが演習の企画担当となった場合，現実的に発生する可能性のあるインシデントを想定してシナリオを作成すること自体が困難となることも考えられる．特に初めて単独演習をする場合は，インシデントハンドリング対応をするための文書やプロセスの準備状況からセキュリティ専門ベンダーの助言を受け，演習の企画作業やファシリテーションに対しても支援を受けることは，有益な演習とするために有効である．

従って，単独演習は，ある程度成熟した CSIRT であれば，CSIRT の活動範囲に対して能力の向上が見込める演習形態であるが，相応のコストが発生する上に，未熟な CSIRT では実施することが困難な演習である．

#### 4.2.2　共同演習

セキュリティ専門ベンダーが提供する演習サービスや，業界団体と官庁などが主催して開催され，複数の企業や団体の CSIRT やセキュリティ技術者が同一の会場に参集して，同一のシナリオを使って行う演習を共同演習と呼ぶ．

共同演習は，演習を主催している演習サービスの講師や団体の事務局が用意した架空のインシデントシナリオを用いて，主催者側のファシリテーションによって進行される演習である．そのため，団体で実施する共同演習の企画グループに加入していない限り，シナリオや演習進行のカリキュラムなどを準備することはない．単独での演習企画が難しい経験の浅い CSIRT であっても予算や時間の捻出ができ，所属する外部団体における参加資格があることにより容易に参加することができる．このように，少ない労力で演習を実施することができるため，演習を実施したことが無い組織であれば，CSIRT 立ち上げ初期の第一段階の策として活用する意義がある．しかし，複数の組織が同一のシナリオで演習を実施するため，必ずしも自組織の中で発生する可能性のあるインシデントであるとは限らない．また，各社の CSIRT はそれぞれ異なる課題があるものと想定されるため，個々の CSIRT の課題を明確にすることを目的とするには不適切な演習である．なお，業界団体が主催する共同演習は，多くの場合，特定の業種や業界の組織に参加が限られた開催となり，誰もが参加できるわけではないことも注意すべきである．

### 4. 3　各団体で実施されている共同演習

前節で述べたように，共同演習は様々な団体で実践されている例がある．国が中心となって推進する社会経済活動の基盤となる重要な設備（重要インフラ）を担う事業組織や金融庁が主催する金融機関向けのサイバーセキュリティ演習が代表的な共同演習である．本節では，代表的な共同演習の実践状況について述べる．

#### 4. 3. 1　重要インフラ事業者向け分野横断演習

内閣官房に設置された内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）が主催する共同演習である．主に 14 の分野に分類された重要インフラ分野に属する事業を担う事業者や所管省庁などが参加する国内で最大規模の共同演習である．2006 年度から継続的に実施されており，2018 年度には約 2900 名が複数の会場に分かれて演習に参加している．

本演習は，重要インフラ事業者における事業継続計画や官民・分野横断的な情報共有体制に関する実効性の検証及び課題の抽出を行うことにより，障害対応体制の強化を図ることが目的とされている．主催者の NISC は本演習に対して，各事業者で発生の確率が高く発生時の対応によって被害が甚大となるケースをシナリオとして用意した上で，運営担当者（ファシリテーター）がそのシナリオを順次提示して参加者が議論して対応策をまとめていく机上演習の形式で実施している．その際，参加者が運営側で準備した会場に一堂に会して実施する場合と，参加組織の社内ネットワークを使用して遠隔で実施する方式，あるいはそれを併せた参加方法がある．

#### 4. 3. 2　金融業界横断的なサイバーセキュリティ演習（通称：Delta Wall）

金融庁が主催し，主要銀行及び地方銀行，信用金庫・信用組合，証券会社，生命保険会社・損害保険会社，外国為替証拠金取引業者（FX 業者）・仮想通貨交換業者など，約 100 の金融機関が参加する，金融業界横断的に実施されるサイバーセキュリティ演習である．本演習は，サイバーセキュリティ対策のカギとなる「自助」，「共助」，「公助」の三つの視点（Delta）と防御（Wall）を掛け合わせて，通称 Delta Wall と呼ばれる．2016 年より毎年開催され，2018 年度で 3 回目の開催となっており，業態別に 5 日間に亘り実施された．

金融庁では，金融分野におけるサイバー攻撃の高度化・複雑化が進む中，サイバーセキュリティの確保は，金融システム全体の安定のため喫緊の課題としており，特に中小金融機関のサイバーインシデント対応能力の底上げを図ることを目的として，本演習を開催している．金融庁では，共通のシナリオだけでなく，信金・信組などには Web サイトの改ざん，証券・FX 事業にはオンラインサービスページへの DDoS 攻撃と，業務特性を反映した業態毎のシナリオも用意している．それぞれのシナリオは，各金融機関が陥りやすい弱点が浮き彫りとなり，参加者が気づきを得ることができる内容としている．また，本演習は，演習会場に集合する演習形態ではなく，各金融機関が職場から参加する形式を採用していることも特徴となっている．特定部門の職員が少数のみ参加するといった限定的な参加ではなく，より多くの職員の参加を実現している．

### 4. 4　演習実施のタイミング

ここまで述べたように，サイバーセキュリティ演習はCSIRTのインシデントハンドリングの実効性評価と組織としての対応能力の向上に対して有効な手段であると考えられる．しかし，CSIRT要員の知識や技術が不足している状態や組織として規程やルールが何も定まっておらず手順の整備も不十分，若しくは組織としての課題が認識できてない未成熟な状態で演習を実施しても，効果的な成果を得ることが難しいことから，演習実施のタイミングを見定めることが重要となる．

まずは，それぞれの要員がトレーニングを受講することで，役割を遂行するために必要な知識や技術を備える．組織としては，活動範囲の中で発生する可能性があるインシデントを調査して，インシデントハンドリングするための対応プロセスや対応マニュアルを整備し，テストを用いて内容の精査を進める．この段階で，3.3節で紹介したSIM3などのCSIRT能力の評価ツールを用いて，CSIRTとしての成熟状況を評価し，不足している能力を見定める．効果的なサイバーセキュリティ演習を実施する上では，各成熟度パラメータがENISAの成熟度評価における基本（Basic）レベルであれば，著しく検討が不足したパラメータが無い状態と判断できるため，参考にされることを推奨する．また，外部の教育サービスによる演習コースを受講し，外部団体による共同演習に参加するなどして，机上演習の進行や特性についても，各要員に学ばせるべきである．

要員トレーニング，ドキュメントの整備とテスト，共同演習による演習の経験といった一連の準備を実施し，自己評価による網羅性の確認をすることで，効果的な単独演習を実施することができる状態に到達するのである．

## 5.　日本ユニシスグループで実施したサイバーセキュリティ演習

日本ユニシスグループでは，グループ内のセキュリティマネジメントの意思決定を行う組織として日本ユニシスグループ総合セキュリティ委員会が設けられており，その配下に情報セキュリティ事故への対応を技術的にサポートすることを主な役割とした，日本ユニシスグループCSIRT（UCSIRT：Nihon Unisys Group Computer Security Incident Response Team）が設置されている．UCSIRTでは，セキュリティインシデントハンドリングの実効性を確認するために単独でのサイバーセキュリティ演習を図3の流れで実施している．

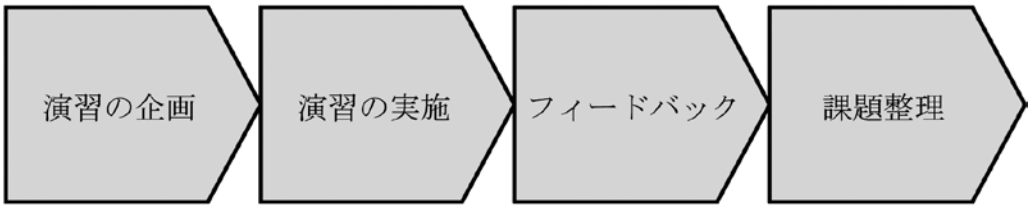


**図3　UCSIRTサイバーセキュリティ演習の流れ**

本章では，UCSIRTのサイバーセキュリティ演習を紹介すると共に，演習によって得られた成果と課題，そして今後の展望について述べる．

### 5.1　演習の企画

サイバーセキュリティ演習は，演習の企画から作業が開始される．UCSIRT では，演習の企画のためにコーディネータチームを形成して，演習の約 2 ヶ月前から演習実施に向けて準備を開始した．コーディネータチームは，UCSIRT の事務局となっている CISO オフィスを中心として，これまで多くのインシデントハンドリングを経験したメンバーで編成した．本節では，このコーディネータチームが実施した UCSIRT サイバーセキュリティ演習の企画フェーズについて述べる．

#### 5.1.1　目的の定義

サイバーセキュリティ演習では，実施の目的を具体的に定義することが重要な要素の一つである．目的が正しく定義されていることで，インシデントシナリオの作成や参加者にどのようなポイントを確認させてどのような能力を向上させるべきかなど，企画フェーズでの検討や想定から外れることなく，確実に遂行するための道標となる．

本演習では，コーディネータチームにて，現状の UCSIRT の課題を整理し，その課題を改善するための具体的な目的を検討した結果，主に二つの課題を定義し，その課題の改善に向けた目的を掲げることとした．

一つ目の目的は，整備されているドキュメントの実効性評価である．UCSIRT では，サイバーセキュリティインシデント対応に関する手続きやルールをドキュメントとして整備しているが，メンバーの知識や経験に差異があるため，メンバー間での理解が異なることが想定された．そのため，演習課題によるメンバー内での議論を用いて，インシデント対応に関わる認識を相互確認することで，インシデントレスポンスの実効性をより確実なものとすることを計画した．二つ目は，役割分担や情報共有といった連携の重要性について，要員の理解を深めることを目的とした．

#### 5.1.2　参加者の検討

UCSIRT は，複数の部署を横断した，様々な領域における情報セキュリティの知見を持ったメンバーで構成されており，セキュリティインシデント発生時は，事故発生部門への技術的な支援を行うことが主な役割となる．本演習では，この技術的な支援をさらに強化するために，UCSIRT メンバー内の認識の相互確認と連携の強化を目的として定めたため，UCSIRT メンバーのみを参加者として演習を実施することとした．

演習では，二つの演習グループにチームを分け，それぞれのチームの役割を定義した．全体統括役のコマンダー，システム構成やログ監視（SOC）の情報を持ったシステム基盤系の担当，セキュリティ対策状況やセキュリティソリューション知識を持つ技術支援担当，PoC や社内調整を担当するリスク管理担当，インシデント対応を円滑に実施するための事務局に対して，それぞれメンバーの経験も踏まえて割り当てることで参加者のチーム分けを確定した．

#### 5.1.3　演習の準備

演習を実施するまで，大きく四つのステップに作業を分割して準備を実施した．ステップの流れを表 2 に示す．

**表 2　演習準備のステップ**

| ステップ数 | 作業項目 | 作業内容 |
|---|---|---|
| ステップ 1 | 対象とするインシデントの特定とタイムテーブル案の作成 | どのようなインシデントが発生し，それをどのような流れで対応（ハンドリング）していくかを検討し，タイムテーブルに落とし込んでいく． |
| ステップ 2 | シナリオの作成と強化ポイントの特定 | インシデントがどこから発生するか，CSIRT へどのように情報が連携され，対応が開始されるかなど，シナリオを作成する．また，インシデントハンドリング手順において，どのポイントを重点的に強化していくかについて特定する． |
| ステップ 3 | 演習資材の準備とリハーサル | 演習時に配布する資料や構成図などの演習素材を準備し，実際に演習が進められるものか，コーディネータチーム内でリハーサルを実施する． |
| ステップ 4 | 事前説明会 | 演習本番の約 1 週間前に，UCSIRT 要員に対して，本演習の目的や各自の役割，当日の進め方を案内すると共に，演習当日までに，インシデント対応手順や，CSIRT 関連ドキュメントの再確認を依頼する事前説明会を開催した上で当日に臨む． |

演習の準備の大きなポイントは，ステップ 2 で実施した，シナリオの作成と強化ポイントの特定である．シナリオが実際に発生する可能性がないインシデントでは，演習の中で実環境の情報を基に議論する上で，コーディネータチーム側で想定した議論にならないことも考えられるため，複数の案を挙げ，チーム内で時間をかけて議論した．また，UCSIRT のメンバーは 20 名程度の要員で構成されているが，一つのグループとしてしまうとワークショップの人数としては多くなり過ぎてしまうため，要員が積極的に参加できるように二つの演習グループに分けて要員それぞれに役割を設定し，事故発生時の第一報から一次対応（封じ込め）までの手順や対応のポイントに対して，重点的に認識を深められるようにした．

### 5. 2　演習の概要（シナリオ）

日本ユニシスグループでは，次世代ファイアウォール[*7]や次世代エンドポイントセキュリティソリューション[*8]などの先進的なセキュリティ対策を運用しており，マルウェアの混入や外部からの不正侵入などのサイバー攻撃に備えている．しかし，昨今の攻撃手法の巧妙化や日々公開されるゼロデイ攻撃[*9]といった脅威の進化により，マルウェア混入の可能性は拭い去ることはできない．このような背景から，社内システムが未知のマルウェアに感染して重要情報が社外に漏れたケースを題材としてシナリオ検討を進めた．シナリオの概要は表 3 の通りである．

**表 3　演習のシナリオ**

| No. | シナリオ内容 |
|---|---|
| 1 | 外部のセキュリティ支援団体が攻撃者のものと思われるサーバを調査した結果，当社の IP アドレスとの通信ログが発見されたとの通報を受信する． |
| 2 | 外部のセキュリティ支援団体からの通報に基づき，UCSIRT の招集および情報セキュリティの事故報告を行う．（演習課題 1） |

| | |
|---|---|
| 3 | UCSIRT が招集され一次切り分けを実施した結果，サイバー攻撃の可能性が高く，影響の範囲が特定できないことから，詳細対応が必要との判断を行う． |
| 4 | 事実確認をするためのシステム構成の詳細情報を共有する．（演習課題 2） |
| 5 | 外部のセキュリティ支援団体からの通報に対して事実確認を実施するため，調査対象の整理を実施する．（演習課題 3） |
| 6 | 事実確認の調査結果から，サイバー攻撃の侵入経路が判明する． |
| 7 | 侵入状況に基づいた初動対応策の検討および影響範囲の確認内容の整理を実施する．（演習課題 4） |

本演習は，社内システムでのインシデントを題材としてシナリオを作成したため，社内システムの構成を認識していることを前提として対応方法を議論してもらう想定であったが，社内システム担当者以外の UCSIRT 要員の中にはシステム構成の詳細についての認識が充分でない要員も存在した．そのため，実際にインシデントが発生した場合の想定も兼ねて，敢えて演習課題の一部としてシステム情報の共有を実施した．

### 5. 3　演習の実施（演習当日の流れ）

演習当日は，一つの会議室に参加者を集めて開催した．二つの演習グループの境にホワイトボードを置き，ファシリテーターの説明は全体に行えるよう図 3 の通り演習の会場設置に工夫を施した．

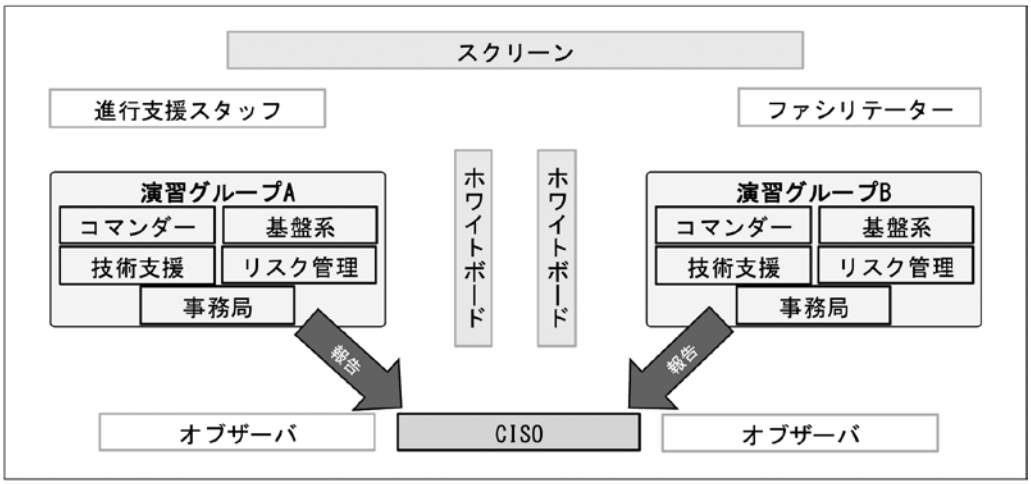


**図 4　演習会場の構成**

発生したインシデントに対して，表 4 に示した四つの演習課題に沿ってグループ毎にコマンダーを中心として議論を進め，議論の内容や想定した対策内容をそれぞれ発表，CISO やファシリテーターを交えてフィードバックを実施することを繰り返した．演習時間は，休憩時間を含めて約半日をかけた．

表 4　演習課題

| 演習 No. | 演習題目 | 演習内容 |
|---|---|---|
| 1 | UCSIRT の招集・情報セキュリティ事故報告の実施 | 外部のセキュリティ支援団体から通報された情報を基に，UCSIRT 要員を招集し，情報セキュリティ事故報告を実施する． |
| 2 | システム環境の共有 | インシデント調査の事前準備として，システム環境について演習グループ内で共有しながら，インシデントの原因を特定するために必要とされる各種ログの有無や入手経路を特定する． |
| 3 | 事実確認の検討 | ここまでに得られた情報を基に事実と想定を整理していく．さらに調査が必要な対象を特定し，調査の指示内容を依頼先も考えながら，具体案に落とし込み文書化する． |
| 4 | 初動対応策の検討，及び，影響範囲の確認指示の検討 | 発生したインシデントに対して，今後の展開予測や更に起こりうる追加のリスクを考慮した初動対応（一次対応）と，発生したインシデントによる影響範囲を確認するための指示を整理して報告する． |

### 5. 4　フィードバック

演習を終了し，最後にフィードバックを実施した．まずは，ファシリテーターから，シナリオの全体を振り返りながら，各演習課題で求められた対応とコーディネータチームで想定した対応例を示した上で，実際のインシデントハンドリングにおける最終報告までの流れを説明した．また，各グループのコマンダーから順に，参加者より演習全体の感想を述べてもらい，同席した CISO，オブザーバメンバーから講評を実施した．そして，参加者には後日アンケートに回答してもらい，今後実施する演習に対しての改善点と検討材料を得た．

### 5. 5　成果と課題の整理

本演習を実施して，UCSIRT 要員のインシデントハンドリングに対する理解を深耕することができたと考えられ，一定の成果と目的の達成が確認できた．特に，経験の浅い UCSIRT 要員は，本演習によって他メンバーの考え方を相互に確認し，実際のインシデント対応でも活用できる知識として定着させられたと考えている．一方，いくつかの課題も洗い出される結果となった．対応プロセスの中で，属人化されてしまっている箇所が発見され，ドキュメントの見直しが必要となった点，演習課題の中でステークホルダーや今後のリスクに対する考慮に不足が見られた点，経営層に対する報告内容の整理が充分でなかった点などが挙げられた．また，本演習について，日本ユニシスグループの社内ホームページにて，全社員に対して演習の概要と成果を報告した．

### 5. 6　今後の実施に向けて

今回の日本ユニシスグループにおけるサイバーセキュリティ演習では，重大インシデント発生時における初動対応の能力強化に注力し，UCSIRT 要員全体のスキルアップと組織としての連携を深めることができた．しかし，実際のインシデントハンドリングでは，対外的な発表を必要とする重大事案や一時的に自社のサービスを停止するといった重大な経営判断を迫られる場合もあり得る．このような判断は，UCSIRT 要員以外のメンバー，例えば，対外発表で

あれば広報部門，提供しているサービスを停止するならば，そのサービスを提供している主管部門との連携と迅速な経営判断が求められる．日本ユニシスグループ全体としてインシデント対応能力を向上させるためにも，UCSIRT 以外のメンバーが参加する演習を企画し，継続的に実践していく必要がある．

## 6. お わ り に

セキュリティインシデントはいつ発生するか予測ができないため，発生することを想定して，インシデント対応能力を高めておく必要があるが，実際のインシデント対応は，マニュアル通りに進まないことがほとんどである．また，できる限り早期にリスクを認識し，インシデントを予知，抑制していくことが理想ではあるが，サイバー攻撃の進化や革新的な技術によりシステム環境が急激に変化していることで，インシデントを完全に防ぐことも困難である以上，留まることなく組織自体のレジリエンスを高めると共に，インシデント対応組織側も進化し続ける必要があると認識することが重要である．

最後に，本稿執筆にあたり，ご協力およびご指導いただいたすべての皆様に深く感謝し，御礼申し上げます．また，本稿が読者のインシデント対応組織におけるインシデントハンドリング能力向上の一助となれば幸いである．

---

＊ 1　IDS/IPS：Intrusion Detection System/Intrusion Prevention System の略．異常な通信を検知/防御するシステム．
＊ 2　WAF：Web Application Firewall の略．Web アプリケーションへの攻撃を検知/防御することに特化したシステム．
＊ 3　フォレンジック：セキュリティ事故発生時の原因究明などのためにコンピュータに残された証拠を調査する技術．
＊ 4　SIEM：Security Information and Event Management の略．様々な機器やソフトウェアの動作状況の記録（ログ）を一元的に蓄積・管理・分析するシステム．
＊ 5　脆弱性診断：対象のサーバやシステムに対して，特定のコマンドを送信して，どういった脆弱性を持っているのかを確認する．
＊ 6　ペネトレーションテスト：対象のサーバやシステムに対して，サイバー攻撃手法を用いて，システムへ侵入できるか確認する．
＊ 7　次世代ファイアウォール：従来のファイアウォール機能を拡張し，アプリケーションの識別やコンテンツの制御など，幅広い脅威に対応する機能を実装したファイアウォール．
＊ 8　次世代エンドポイントセキュリティソリューション：従来のパターンマッチングによるウイルスの検知ではなく，機械学習や振る舞い検知，保護された領域で疑似的に動作させて解析するなどの機能を有したエンドポイント対策．
＊ 9　ゼロデイ攻撃：脆弱性に対する修正プログラム（パッチ）が提供される日より前に，その脆弱性を悪用して行われるサイバー攻撃．

**参考文献**　［1］ 経済産業省/独立行政法人情報処理推進機構（IPA），サイバーセキュリティ経営ガイドライン，Ver2.0，2017 年 11 月 16 日，https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
［2］ 日本セキュリティオペレーション事業者協議会，セキュリティ対応組織（SOC/CSIRT）の教科書，第 2.0 版，2017 年 10 月 3 日，https://isog-j.org/output/2017/Textbook_soc-csirt_v2.0.pdf
［3］ 一般社団法人 JPCERT コーディネーションセンター，CSIRT ガイド，2015 年 11 月 26 日，https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf
［4］ 日本コンピュータセキュリティインシデント対応チーム協議会，CSIRT 人材の定義と確保，Ver.1.5，2017 年 3 月 13 日，https://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf
［5］ NIST：National Institute of Standards and Technology, “SP800-84 Guide to Test,

Training, and Exercise Programs for IT Plans and Capabilities”，2006 年 9 月，
https://csrc.nist.gov/publications/detail/sp/800-84/final
［6］ 米国国立標準技術研究所（NIST：National Institute of Standards and Technology），“SP800-84 IT 計画および IT 対応能力のためのテスト，トレーニング，演習プログラムのガイド”，IPA 情報処理推進機構，2009 年 2 月，
https://www.ipa.go.jp/files/000025350.pdf
（SP800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities 和訳）
［7］ Don Stikvoort, “SIM3：Security Incident Management Maturity Model”，2015 年 3 月 30 日，https://www.trusted-introducer.org/SIM3-Reference-Model.pdf
［8］ ENISA：The European Union Agency for Cybersecurity, “ENISA Maturity Evaluation Methodology for CSIRTs”，Version2.0，2019 年 4 月 9 日，
https://www.enisa.europa.eu/publications/study-on-csirt-maturity

※ 上記注釈及び参考文献に含まれる URL のリンク先は，2019 年 7 月 11 日時点での存在を確認.

**執筆者紹介** 佐 藤 重 之（Shigeyuki Sato）
2016 年日本ユニシス(株)中途入社．前職のシステムインテグレータでは，主にネットワークセキュリティ製品の提案・設計・構築・運用支援対応に従事．現職は主にセキュリティコンサルティングサービスに従事．日本ユニシスグループ CSIRT（セキュリティインシデント対応チーム）メンバー，テクニカル・エバンジェリスト（Security）．情報処理安全確保支援士（登録番号第 001924 号）．