企業レジリエンス向上のための
サイバーセキュリティ演習マップ解説書

一般社団法人　日本ＩＴ団体連盟
サイバーセキュリティ委員会
サイバーセキュリティ演習分科会

２０２１年3月５日

推奨文

一般社団法人　日本ＩＴ団体連盟　専務理事　中谷　昇

「演習によって、経験“知”強化すべき」

現在新型コロナウイルスの影響により、産業界においては業績・事業継続に大きな打撃を受ける一方で、データ駆動型経済への変換期を迎えております。

デジタル社会では、ＡＩ・ＩｏＴ・５Ｇなどにより「データ流通」が新たな産業発展の源泉となるデジタルトランスフォーメーション（ＤＸ）の動きがさらに加速する中で、個人情報の保護やサイバーセキュリティの確保はますます重要になっています。

また、多くの人がテレワークをするようになった今、自宅から会社のサーバーにつなぐリモート接続を狙い、パスワードなどを搾取するサイバー攻撃も増え続けています。

海外に目を向けますと、米国の複数の州で、またベトナム国の「サイバー情報保護法（ＬＯＣＩＳ）」で、国の機密組織に対する「サイバーセキュリティトレーニング」の義務化が始まっています。

サイバー演習を実施する組織や個人のニーズに最も応じたプログラムを選択し、経験“知”を最適化することです。２０２１年にはデジタル庁の新設も予定されています。こうした演習から得られるサイバーセキュリティの経験“知”を最適化するために、官民が連携していくことがさらに重要になってきます。その際の手助けとして、本書を活用していただければと思います。

目次

１．はじめに

一般社団法人 日本ＩＴ団体連盟（以下ＩＴ連）の下部組織にあたる、サイバーセキュリティ委員会の「サイバーセキュリティ演習分科会（以下演習分科会）」は、２０２０年初より活動を開始しました。

企業・団体が本当の意味でセキュリティレベルアップを実現し、サイバー攻撃を受けた際にも、早期復旧できる「レジリエンスの高い企業組織」となって頂くため、知識（形式“知”）だけでなく、「経験“知”」つまり事前に経験を積んでおくことにより「いざという際に初動対処行動が再現できるようになる」ことを主眼に「サイバーセキュリティ演習」が有効に実施できるようにするべく調査・分析活動を開始しました。

今年は、デジタル庁発足も予定され、いよいよ本格的にデジタル社会に変革していこうとしており、今後ますます、サイバー攻撃の高度化・複雑化が予想され、どれだけ対策を万全にしていても被害をゼロにすることは困難になります。これから企業・団体に求められるのは、防御の観点に加え、「被害にあうことを前提としたサイバーセキュリティ対策」です。

被害発生後の初動対応に非常に有効なのがサイバー演習です。サイバー攻撃に対抗するには、最新の対策を実施することと同じくらいに、経営者層やセキュリティ担当者はもちろんのこと、全従業員・全組織がサイバー攻撃の手口に対する理解を深めるとともに、攻撃者に騙されないように日頃から訓練や演習を通じて対処態勢を整えておくことが重要になります。

反面、現実的にはセキュリティインシデント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す。

今回こうした背景を踏まえ、サイバーセキュリティ演習の解説と、適した演習形式のナビゲーションを目的に、「サイバーセキュリティ演習マップ解説書」と「サイバーセキュリティ演習マッピングリスト」を公開するに至りました。

本解説書と演習マッピングリストをご活用頂くことにより、国内の企業・団体が「個人と組織全体」の経験“知”の向上につながり、企業のレジリエンス向上の一助となることを祈念し、ご挨拶とさせて頂きます。

２．序章
２．１　本解説書の目的と対象読者

企業においてセキュリティの責任者であるＣＩＳＯ[1]の設置や、セキュリティを専門としたチームであるＣＳＩＲＴ[2]の構築が進んでいます。その数は国内企業の半数以上がＣＩＳＯを設置し、約４割がＣＳＩＲＴを構築しているといった調査結果もあります。

このように、国内企業でもセキュリティ体制が向上している傾向にありますが、自社が実際にサイバー攻撃やセキュリティ事故に遭った際、はたしてどれだけ迅速かつ的確に、そして組織的に動ける組織はどれくらいあるでしょうかでしょうか。当然ながらサイバー攻撃をはじめとするセキュリティ事故の対応には、専門性を持った人材を欠かすことができません。

またセキュリティ事故の対応には、たとえ一個人が優秀で豊富な知識を持っていたとしても、企業・団体全体として迅速かつ的確な対応は行えません。サイバー攻撃やセキュリティ事故への対応は、個人の知識と同時に応用力や組織力が必要となります。この応用力や組織力を高めるためには、知識獲得のための研修に加え、より実践的な経験を積むことができるトレーニングが必要です。

現在、国内では知識獲得のためのセキュリティ研修は、初心者からマネジメント層まで、また一般的な内容から専門性の高いコースまで数多く提供されています。

一方で、「経験“知”」を高める、組織的で実践的なトレーニングについては未導入、未実施の企業も多いのが現状です。

本解説書は、実践的なサイバーセキュリティ人材の育成を目指している、経営者、ＣＩＳＯ、さらにはＣＳＩＲＴをはじめとしたサイバーセキュリティ関連部署の担当者を対象として、演習形式のトレーニングに焦点をあて、必要性や具体的な内容について紹介します。

---

[1] Chief Information Security Officer（最高情報セキュリティ責任者）の略

[2] Computer(Cyber) Security Incident Response(Readiness) Team（コンピュータ（サイバー）セキュリティインシデント（レディネス）チーム）の略

２．２　企業のサイバーセキュリティ対策における課題
～サイバーセキュリティ人材確保の必要性～

サイバーセキュリティの世界は継続的に人材が不足しています。それは私たちの生活が情報技術に頼っている現代社会といった大きな背景があり、その情報技術によってもたらされたシステムやネットワークが大きなリスクに晒されています。

サイバー攻撃は日常的に発生し、人によってはサイバー戦争の状態とも言われる状態において、このサイバーセキュリティ人材の不足は深刻な問題です。昨今では、ＩｏＴ[3]、デジタルトランスフォーメーション（ＤＸ）など、様々なキーワードが出ていますが、共通して言えることは情報技術を活用して、私たちの世界がより便利になろうとしていることです。

そこで、忘れてはならないのは、便利になればなるほど、サイバー攻撃が増える可能性が高く、それは個人に限った話ではなく、組織も同様であるということです。民間企業であったとしても自治体でも、政府機関でも常にサイバー攻撃のリスクがあります。

経済産業省が２０１６年時点で情報セキュリティ人材の不足が２０２０年には１９．３万人に増加といった情報が出て話題になりましたが、すでに２０２０年を過ぎ、２０２１年を迎えています。国内では引き続き人材が不足しており、多くの組織がサイバー攻撃に気が付いたときには、現状のセキュリティ人材の数では不足します。日本はその現実をまだきちんと見られておらず、まずはサイバー攻撃や人材不足の現状から目を背けないことが重要です。

情報通信研究機構のデータでは観測する約３０万ＩＰアドレスにおいてサイバー攻撃関連の通信は、合計５，００１億パケットに上り、１ＩＰアドレス当たり約１８２万パケットが１年間に届いた計算になります。この現実をどこまで私たちは把握できているでしょうか。

このような現実を考えると、企業で使っているシステムやネットワークにもサイバー攻撃がすでに行われているかもしれず、セキュリティ人材の獲得、強化、育成は喫緊の課題です。

[3] Internet of Things の略で、一般的に「モノのインターネット化」とも呼ばれる。

表１：ＮＩＣＴＥＲダークネット観測統計（過去１０年間）

年	年間 総観測パケット数	観測IPアドレス数	１IPアドレス当たりの 年間総観測パケット数
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	約2,121億	約30万	789,876
2019	約3,220億	約30万	1,187,935
2020	**約5,001億**	**約30万**	**1,820,722**

出典：情報通信研究機構『ＮＩＣＴＥＲ観測レポート２０２０』

一方で、企業の経営層（取締役）には「善管注意義務」[4]があり、法律上要求される一定の注意を払う義務がありますが、サイバーセキュリティの領域まで考えられているのか疑問が残ります。また、有名なセキュリティ裁判例として、ＳＱＬインジェクション[5]裁判がありますが、当該判例で、企業として「当時の技術標準」に基づく対応を行わなければならないという通り、現在の技術標準に基づく対策が必要です。

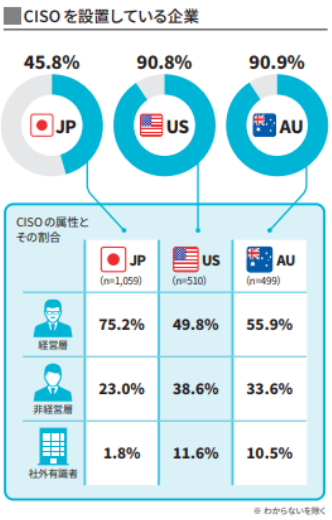
また企業のＣＩＳＯの設置状況から、サイバーセキュリティを真剣に考えていることは明らかですが、それでもＮＲＩセキュアテクノロジーズ社の調査によれば、ＣＩＳＯは全体の半分の企業しかないとし、ＣＩＳＯ設置企業においても、ＣＩＯとの兼務や情報システム部長が兼任している場合など、「とりあえず設置」している企業が多いのが現実です。

[4] 善管注意義務とは、「善良な管理者の注意義務」の略。業務を委任された人の職業や専門家としての能力、社会的地位などから考えて通常期待される注意義務のこと。注意義務を怠り、履行遅滞・不完全履行・履行不能などに至る場合は民法上過失があると見なされ、状況に応じて損害賠償や契約解除などが可能となる。

[5] ＳＱＬインジェクションとは、アプリケーションのセキュリティ上の不備を意図的に利用し、アプリケーションが想定しないＳＱＬ文を実行させることにより、データベースシステムを不正に操作する攻撃方法のこと。また、その攻撃を可能とする脆弱性のことである。ＳＱＬインジェクション対策をしていなかったことについて開発会社の責任が問われ、損害賠償を行った裁判例もある。

最近では事業やプロジェクトの設計段階からの不備によってインシデントが起きる事案も多数発生しています。ブレーキのないアクセルだけの車に乗らないように、設計段階からきちんとブレーキを考える必要があります。しかし、設計段階からサイバーセキュリティを考える人は、言わば事業のストッパーのように見え、関係者や企業そのものからも疎まれることもあるのではないでしょうか。

本来、このようにサイバーセキュリティを真剣に考えれば、サイバーセキュリティを考える人材が不足しているということに気づくことができるでしょう。



出典：ＮＲＩセキュアテクノロジーズ『NRI Secure Insight 2020[6]～企業における情報セキュリティ実態調査～』

もう「知らぬが仏」ではサイバー攻撃の現状や法令などから鑑みても済まされないのが現状です。企業はサイバーセキュリティを真剣に考える必要があり、それを遂行する人材を確保・育成することが急務です。

[6] NRI セキュアテクノロジース「NRI Secure Insight 2020」 https://www.nri-secure.co.jp/download/insight2020-report

3．サイバーセキュリティにおける演習の重要性

企業・団体における、いわゆる人材育成として一般的に行われているのは、知識やスキルの習得を目的に行われる研修や訓練です。研修を受けた後、職場にて実業務遂行するなかで、習得した知識やスキルを実践の場で活用する方法を覚え、企業・団体の業績に貢献できるようになっていきます。

企業・団体で遂行される、事業そのものに関する業務であれば、こうした、教育→訓練→実業務の遂行という人材育成の流れが実現可能です。しかし、サイバー攻撃への対処要員の育成においては、この実務の機会という部分が非常に限定的です。大企業であっても大きなインシデントはたびたび起こるものではなく、仮にインシデントが発生しても、その対処にあたる人員は限られると推測されます。更に、多くの企業においては、インシデントの発生以前に、検知すらできていないと思われます。逆に、セキュリティ対策をしっかり施している企業であればあるほどインシデントも発生しづらくなります。

実務での経験が得にくいという状況はサイバー攻撃の被害特有のものでなく、地震や火災といった災害も同じ状況と考えられます。企業・団体では、火災などを想定した避難訓練を実施しているのではないでしょうか。実際に被害が発生することはほとんどなくとも、こうした災害の発生を想定し、事前に定められた対処を定期的に従業員全員にもれなく訓練することは大事です。

こうした訓練では個人の行動だけでなく、連絡網や組織体制の確認も行い、有事に備えます。

サイバーインシデント対応の演習の位置づけも同じように考えることができます。ここで、知識やスキルといった形式“知”はインシデント対応の基盤になってくれますが、対応力そのものは実務によって得られる経験が重要です。大きなサイバーインシデントは日常的に発生するものではないため、一般的な企業の社員が計画的に経験“知”を取得する手段としては、サイバー演習の場しかありません。

「サイバー演習」とは、実際に起こりうる状況を設定し、参加者に疑似的にインシデントを経験させる方法のことです。個人や組織が、今までに得た知識や経験を使い、状況に対して自分で考えて次の行動を選択します。演習の目的に応じて様々な形態があり、ディスカッション形式の机上演習や、実機を動かして行うハンズオン演習などがありますが、より実際の状況に近いほど得られる気づきは多くなります。

形式“知”を得られる「教育」と、経験“知”が得られる「演習」は相互に補完関係にあります。教育や訓練でスキルを身に着けた後に演習でそのスキルの使い方を学ぶこともできますし、演習で自分に足りないスキルを見つけた後に教育や訓練でレベルアップを図ることもできます。教育と演習のループを回して、能力を継続的にスパイラルアップしていくのが理想的です。実践に近い演習を行うと、成功しても失敗してもその経験は次の教育のモチベーションアップに繋がります。特に、本番で失敗が許されない職務の場合、演習での失敗経験も重要になることがあります。

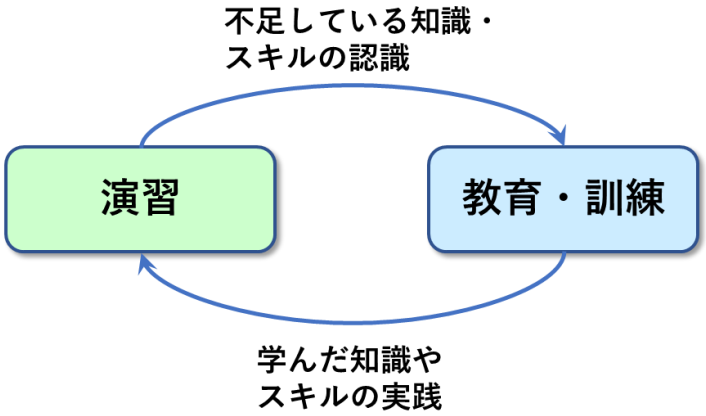


図１：演習と教育・訓練のループ図

組織態勢の強化にはまずは個人のレベルアップが必要ですが、組織自体のレベルアップも重要です。組織対応力の視点からは、セキュリティツールやサービスなどの技術的対策と、教育や組織体制などの人的対策が、有効に機能するかどうかを演習によって明らかにすることができます。

更に、課題を見つけてその対策を行えば、今後のサイバー攻撃への備えを強固にすることができるでしょう。

サイバー攻撃の脅威は日々進化し狡猾になっており、セキュリティ対策も定期的な見直しが必要になっています。定期的に最新のサイバー攻撃を想定した演習を行うことで、自社のセキュリティ対策が有効に機能するかどうかを可視化することができます。

トレンドマイクロ社の調査によると、多くの業種でセキュリティインシデントが発生しており、多大な被害が発生しています。

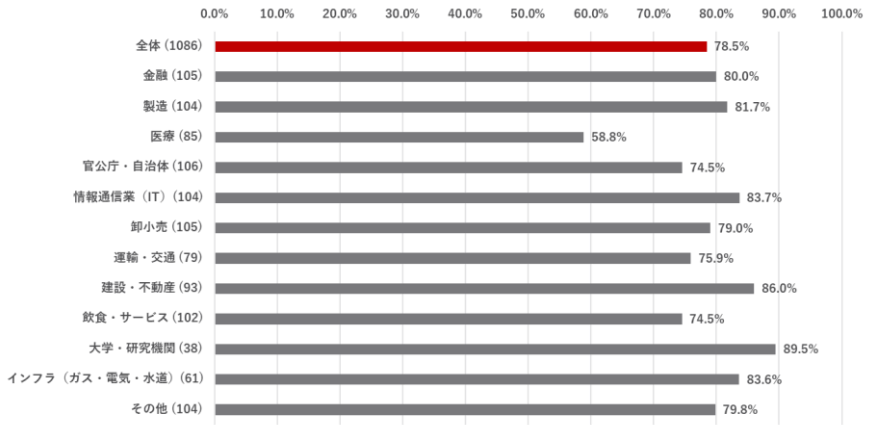


図２：セキュリティインシデント発生率

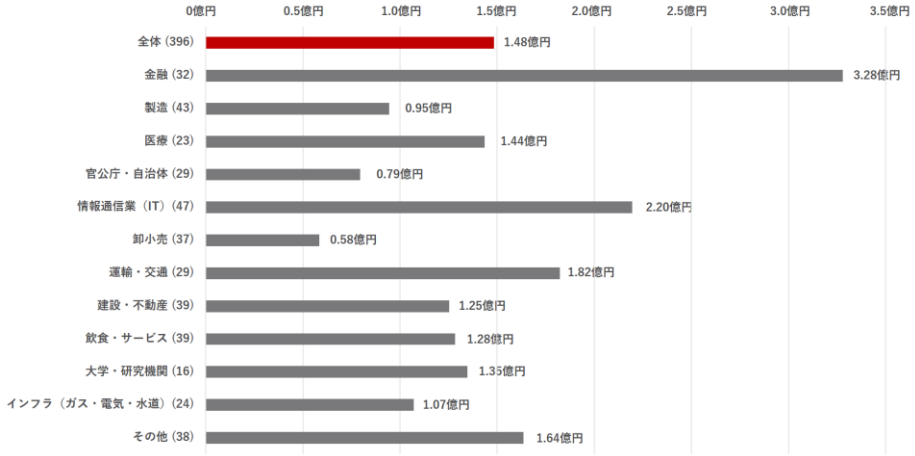


図３：セキュリティインシデントによる年間総被害額

注: インシデントによる被害及び再発防止対策などの費用を含む

出典：トレンドマイクロ『サイバー攻撃から組織を守るために経営層ができること』[7]

サイバーインシデントの被害を最小限に抑えるためには、攻撃を早い段階で発見し、速やかに初動対応を行うことが重要です。攻撃を事前に阻止したり、攻撃が実行されたとしても被害の拡大を抑えられる可能性が高まります。外部の専門業者に対応を依頼するにしても、初動対応は基本的に被害が発生した企業内部で行う必要があります。よって、全ての事業者がサイバーセキュリティ演習を実施し、対応人材を養成すべきです。

[7] トレンドマイクロ「サイバー攻撃から組織を守るために経営層ができること」
https://resources.trendmicro.com/jp-docdownload-form-m277-web-cxo-cyber-attack.html

４．サイバーセキュリティ演習の分類整理

市場に提供されている様々な演習がどの程度あるのかを、当分科会メンバーで調べてみることにしましたが、まずは演習コースに関する情報に必要な要素を洗い出すことにしました。

まず、組織として演習を実施する場合に考えなければならないのは、組織内のどのような役割・人材に効果のある演習なのかということです。

ちょうどタイミングよく、ＩＰＡで公開しているＩＴＳＳ＋（セキュリティ領域）が２０２０年１０月２日に改訂されました。

https://www.ipa.go.jp/jinzai/itss/itssplus.html#section1-6

今回改訂されたＩＴＳＳ＋（セキュリティ領域）の特徴としては、旧版で対象としていたセキュリティを生業とする「セキュリティ人材」のみではなく、デジタル部門、事業部門、管理部門などでセキュリティ以外の業務を生業とする人材がセキュリティ知識・スキルを学び、「プラス・セキュリティ」人材も、分野の中に取り入れられていることです。

次の図は、ＩＴＳＳ＋（セキュリティ領域）で定義されているセキュリティ関連タスクを担う分野の概観図ですが、横方向が「セキュリティ関連タスクの例」、縦方向が「デジタル、セキュリティ、その他」で構成される表となっています。

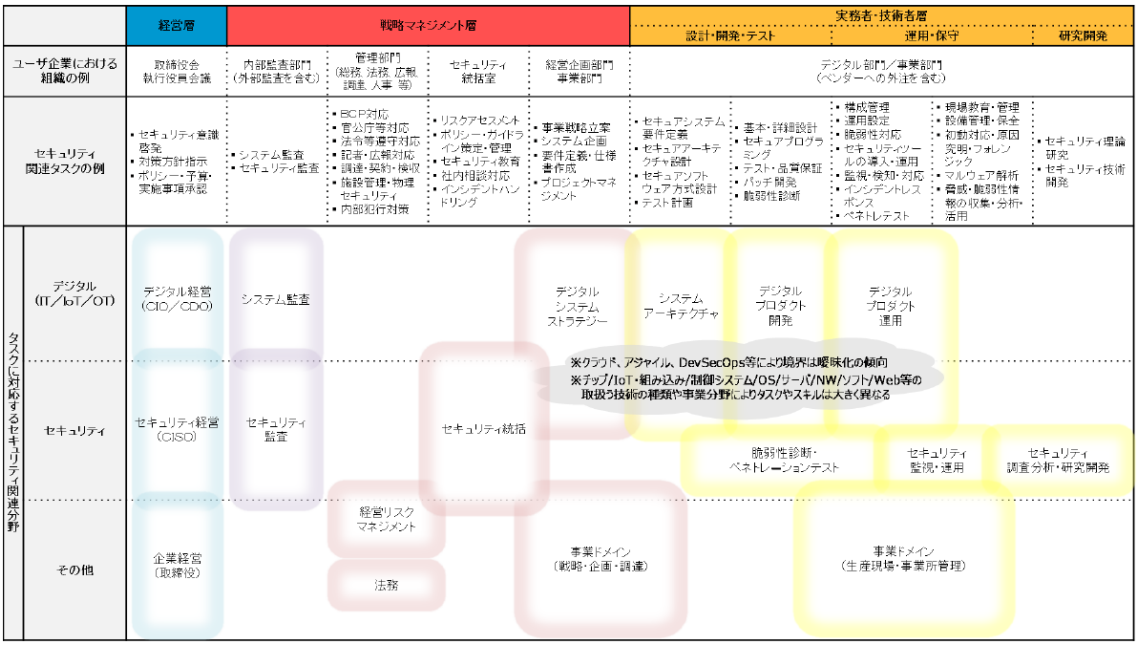


図４：ＩＴＳＳ＋（セキュリティ分野）で定義されている１７分野

出典：令和２年９月 経済産業省・ＩＰＡ
『サイバーセキュリティ体制構築・人材確保の手引き』（第１版）

また、前記の１７分野に対して、セキュリティ関連タスクの例、担当部署／機能をまとめたものが次表のような対応関係とされており、セキュリティ対策の実務を担う部門に対応する業務を確認することができます。

表２：１７分野とセキュリティ関連タスクなどとの対応

	区分	分野名	セキュリティ関連タスクの例	担当部署／機能の例（青字は社外ベンダー等）
経営層	デジタル	IT経営（CIO/CDO）	セキュリティ意識啓発、対策方針の指示、セキュリティポリシー・予算・対策実施事項の承認 等	経営者、経営層（CISOを含む）
	セキュリティ	セキュリティ経営（CISO）		
	その他	企業経営（取締役）		
戦略マネジメント層	デジタル	システム監査	システム監査、報告・助言 等	監査部門 ITベンダー・監査法人（システム監査サービス）
		デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、プロジェクトマネジメント 等	経営企画部門、IT企画部門、IT・デジタル部門の企画機能 IT/セキュリティコンサルタント
	セキュリティ	セキュリティ監査	セキュリティ監査、報告・助言 等	監査部門 セキュリティベンダー・監査法人（セキュリティ監査サービス）
		セキュリティ統括	セキュリティ教育・普及啓発、セキュリティ関連の講義・講演、セキュリティリスクアセスメント、セキュリティポリシー・ガイドラインの策定・管理・周知、警察・官公庁等対応、社内相談対応、インシデントハンドリング 等	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のセキュリティ対策機能
	その他	経営リスクマネジメント	経営リスクマネジメント、BCP／危機管理対応、サイバーセキュリティ保険検討、記者・広報対応、施設管理・物理セキュリティ、内部犯行対策 等	総務部門（リスク管理部門を含む） 経営企画部署、総務部署等のリスクマネジメント機能
		法務	デジタル関連法令対応、コンプライアンス対応、契約管理 等	法務部門、総務部門の法務担当
		事業ドメイン（戦略・企画・調達）	事業特有のリスクの洗い出し、事業特性に応じたセキュリティ対応、サプライチェーン管理 等	事業部門の企画機能 事業戦略コンサルタント
実務者・技術者層	デジタル	デジタルシステムアーキテクチャ	セキュアシステム要件定義、セキュアシステムアーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画 等	IT・デジタル部門の設計機能、IT子会社 IT/OTベンダー
		デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、テスト・品質保証、パッチ開発 等	IT・デジタル部門の開発・保守機能、IT子会社 IT/OTベンダー
		デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、脆弱性対策・対応、インシデントレスポンス 等	IT・デジタル部門の運用機能、IT子会社 IT/OT/セキュリティベンダー
	セキュリティ	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（脆弱性診断サービス）
		セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、セキュリティ監視・検知・対応、インシデントレスポンス、連絡受付 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（セキュリティ監視・運用サービス）
		セキュリティ調査分析・研究開発	サイバー攻撃捜査、原因究明・フォレンジック、マルウェア解析、脅威・脆弱性情報の収集・分析・活用、セキュリティ理論・技術の研究開発、セキュリティ市場動向調査 等	CSIRT/IT・デジタル部門のリサーチ機能、IT子会社 セキュリティベンダー（デジタルフォレンジックサービス）
	その他	事業ドメイン（生産現場・事業所管理）	現場教育・管理、設備管理・保全、QC活動、初動対応 等	運転、保全、計装、品質管理関連部署、PSIRT OT/セキュリティベンダー

出典：令和２年９月 経済産業省・ＩＰＡ
『サイバーセキュリティ体制構築・人材確保の手引き』（第１版）

今回は、役割についてはこのＩＴＳＳ＋（セキュリティ領域）で提示されている１７分野にすることにしました。

次に演習といっても様々な種類や考え方があることに着目し、演習の定義を検討しました。その結果、次の９つの分類を演習として定義することにしました。

(1). フルスケール演習

関わる全ての担当者が参加する総合演習。（定期開催コースとしては存在しないと思われる）

(2). 組織演習（カスタム）

実際に発生しうるインシデントをシミュレートし、組織が各機能を果たすかどうかを確認するための演習。各事業者にヒアリングし、個別にカスタムしたリアルなシナリオを用意して演習を行う。

(3). サイバーレンジチーム演習

サイバーインシデントをシミュレートし、チームで役割分担しインシデントに対処する方法

で訓練するブラインド演習。サイバーインシデントのシミュレートは閉じた仮想空間上で行う。

(4). サイバーレンジ演習
仮想空間上で行うインシデント対応演習。

(5). 実践演習・机上演習
実際のインシデントを想定したシナリオに沿って、各ステップにおいて各組織がどのように動くべきか、グループディスカッション形式で行う。ブラインド演習。

(6). ハンズオン演習
実機を使用した体験型の演習。受講生が何をすべきかの指示に沿って実際のインシデントを追体験するものや、ゲーム要素のある防御演習など、様々な演習がある。

(7). ゲーム形式の組織演習
ボードゲーム形式の演習。発生するインシデントに組織としてどう対応するかを、グループでディスカッションして決定する。

(8). 専門スキルコース（ハンズオン演習含む）
個人の専門スキルを習得する演習を含むコース。ハッキングコースは、受講に必要なスキルも高度なものが要求されることが多い。

(9). サイバー防災訓練・標的型メール演習
一般従業員向けの訓練。

演習コースの分類を行いやすくするために、演習提供機関に対して以下の項目を提示してもらうように様式化し、メンバー各社で調査を開始しました。

【コース調査内容】

- 演習コース名
- 主催会社
- 演習形式（9 分類）
- 個人演習 ｏｒ 組織演習
- 演習難易度（3 段階）
- 受講の前提条件など（保有資格や具体的な技術スキル）
- ＩＴＳＳ＋分野への演習の対応状況（１７分野の役割に対する、受講必須か受講推奨か）

その結果、次のような様式イメージで分科会メンバーの組織が提供、あるいは受講している演習を取りまとめることができました。今回調査した演習コースの一覧は、付録部分に掲載していますので、参考にしてください。

演習コース名	主催会社	演習形式	個人演習 or 組織演習	演習難易度	ITSS＋分野																	
					デジタル経営（CIO／CDO）	セキュリティ経営（CISO）	企業経営（取締役）	システム監査	デジタルシステムストラテジー	セキュリティ監査	セキュリティ統治	経営リスクマネジメント	法務	事業ドメイン（戦略・企画・調達）	デジタルシステムアーキテクチャ	デジタルプロダクト開発	デジタルプロダクトマネジメント	脆弱性診断・ペネトレーションテスト	セキュリティ監視・運用	セキュリティ調査分析・研究開発	事業ドメイン（生産現場・店舗管理）
標的型サイバー攻撃 対応・防御トレーニング　Adv	トレンドマイクロ株式会社	(8) 有料スキルコース（ハンズオン演習を含む）	個人演習	Lev.2 中															○	○	○ 推奨
標的型サイバー攻撃 対応・防御トレーニング　Cybe	トレンドマイクロ株式会社	(8) 有料スキルコース（ハンズオン演習を含む）	個人演習	Lev.3 高															◎	◎	◎ 必須
CIRMコース 基礎演習/実践演習	大日本印刷株式会社	(3) サイバーレンジチーム演習	組織演習	Lev.2 中			○	○	○	○	◎	◎ 必須			○	○	○	○	◎	◎	◎ 必須
COPコース	大日本印刷株式会社	(4) サイバーレンジ演習	個人演習	Lev.3 高							○	○ 推奨				○	○ 推奨	◎	○	○	○ 推奨
CYDER	NICT	(5) 実践演習・机上演習	個人演習	Lev.1 低							○	○ 推奨		○ 推奨					○ 推奨		○ 推奨
SANS 各種専門コース	NRIセキュアテクノロジーズ	(8) 有料スキルコース（ハンズオン演習を含む）	個人演習	Lev.3 高										◎	◎	◎	○	◎	◎	◎	◎ 必
Secure Eggs Webアプリケーションセキュリティコース	NRIセキュアテクノロジーズ	(8) 有料スキルコース（ハンズオン演習を含む）	個人演習	Lev.3 高										○	○	○	○	◎	○	○	◎ 必
Secure Eggs フォレンジック対応コース	NRIセキュアテクノロジーズ	(8) 有料スキルコース（ハンズオン演習を含む）	個人演習	Lev.3 高															○	○	◎ 必須
情報セキュリティ事故対応1日コース 机上演習編	株式会社ラック	(5) 実践演習・机上演習	組織演習	Lev.2 中	○	○	◎	○	○	○	○	◎	◎	○	○ 推奨				○	◎	○	○ 推
情報セキュリティ事故対応2日コース 実機演習編	株式会社ラック	(5) 実践演習・机上演習	組織演習	Lev.3 高			◎ 必須				○	◎	◎	◎ 必須					○	◎	○ 推奨
IR（インシデントレスポンス）ファーストコース	株式会社ラック	(6) ハンズオン演習	個人演習	Lev.3 高											○	◎	○	○	◎	◎	○ 推奨
標的型メール訓練サービス	グローバルセキュリティエキスパート	(9) サイバー防災訓練・標的型メール演習	組織演習	Lev.1 低	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○ 推
認定ネットワークディフェンダー（CND）育成講座	グローバルセキュリティエキスパート	(8) 有料スキルコース（ハンズオン演習を含む）	個人演習	Lev.2 中		○ 推奨					○	○ 推奨			○	○	○	○	◎	◎	◎ 必須
認定ホワイトハッカー（CEH）育成講座	グローバルセキュリティエキスパート	(8) 有料スキルコース（ハンズオン演習を含む）	個人演習	Lev.3 高															○	○	◎ 必須
セキュリティ防災訓練ツール・DECIDEPlatform	アライドテレシス株式会社	(2) 組織演習	組織演習	Lev.2 中	○	○	◎	○	○	○	◎	◎	○	○	○ 推奨				○	◎	○	○ 推

図５：演習コースとりまとめイメージ

この表形式は、受講に適した１７分野の役割や、演習分類が演習コースごとに確認できるため、目的の演習コースの内容を把握するのには、この一覧形式は便利です。

しかし、座学研修や演習を交えた組織全体での研修計画を考える際には、ひと工夫が必要でした。

知識を蓄える座学研修を行ったうえで、一定知識を持った個人を集めた演習を行うことが重要となりますが、組織がまず取り組む研修はどこなのか、その次には何を行うべきかを考える整理の仕方が必要でした。

組織全体のサイバーセキュリティ対応能力を高めるためには、個人能力と組織全体の能力の両方を向上させる必要があります。

また、スキル強化にはリテラシー部分もあれば、専門スキルの向上といった観点もあります。このため、左右に個人と組織を分類し、縦にスキルの高低を分類することで、次の図のような四象限のマップに各演習を整理してみることとしました。

図 6 ：演習マップ（四象限）

この演習マップに各演習コースを配置してみることで、まず行うべき演習は何なのか、その次にはどのような演習を行うと効果的なのかを一目で把握できるようになります。まさに組織全体のサイバーセキュリティ対応能力をスパイラルアップさせていくための道標となるでしょう。

５．サイバー セキュリティ演習マップの解説

「形式“知”」と「経験“知”」を掛け合わせることで、組織全体としてのセキュリティレベルが上がることから、座学などで知識を習得しましたら、その知識を前提として演習実施により体得していくことができます。

これは経営学者の野中郁次郎氏が提唱したＳＥＣＩモデルでも、個人が持つ「暗黙知」は、経験の共有や言葉に変換して伝えたりしながら、集団や組織の共有の知識「形式知」となり、それらをスパイラルさせて組織として向上していくとされています。

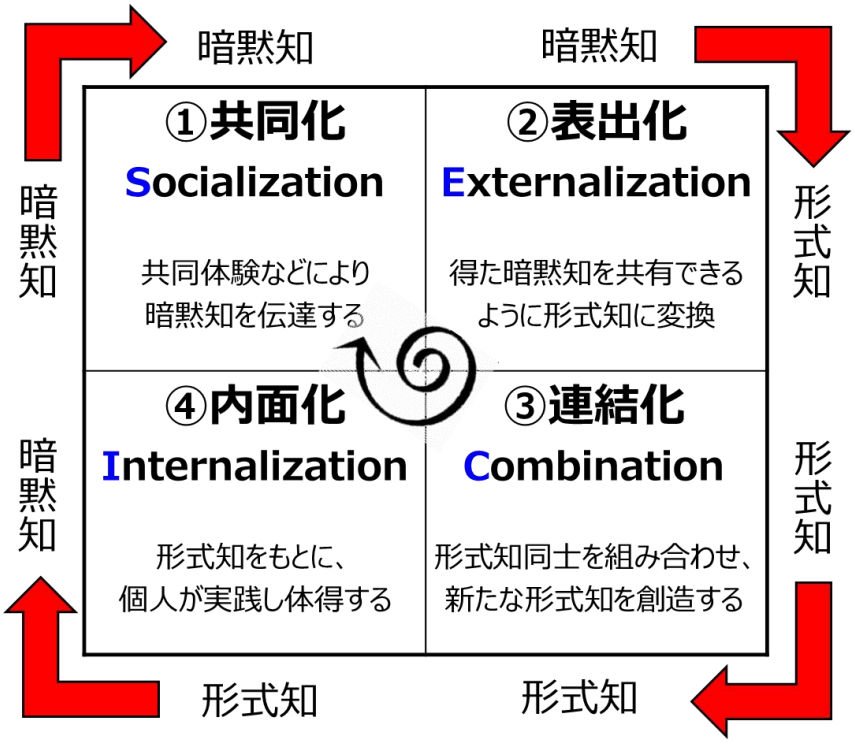


図７：ＳＥＣＩモデル

ＳＥＣＩモデルで説明しますと、形式知を暗黙知に変換する「④内面化」のプロセスが個人演習に該当し、暗黙知を共有する「①共同化」のプロセスが組織演習に該当します。

演習で得られた成果や反省点は、「②表出化」のプロセスとして洗い出しを行い、「③連結化」のプロセスで自組織のセキュリティガイドラインなどに形式知として反映され、それをもとに知識を向上するための座学やｅラーニングなどでの学習を行うこととなります。

これを前提に演習マップを見てみましょう。この演習マップは、企業・団体に在籍する個人と組織そのものの「経験“知”」を上げるための演習を２軸・四象限に整理し、市場に提供されている

演習講座をマッピングするものです。

２軸でマッピングすることで、演習の性格ごとに可視化し、相対比較することができるようになり、自組織で必要となる演習を探したり、中長期でのサイバーセキュリティの組織力向上のロードマップに人材育成・組織開発計画として位置付けておくことができます。

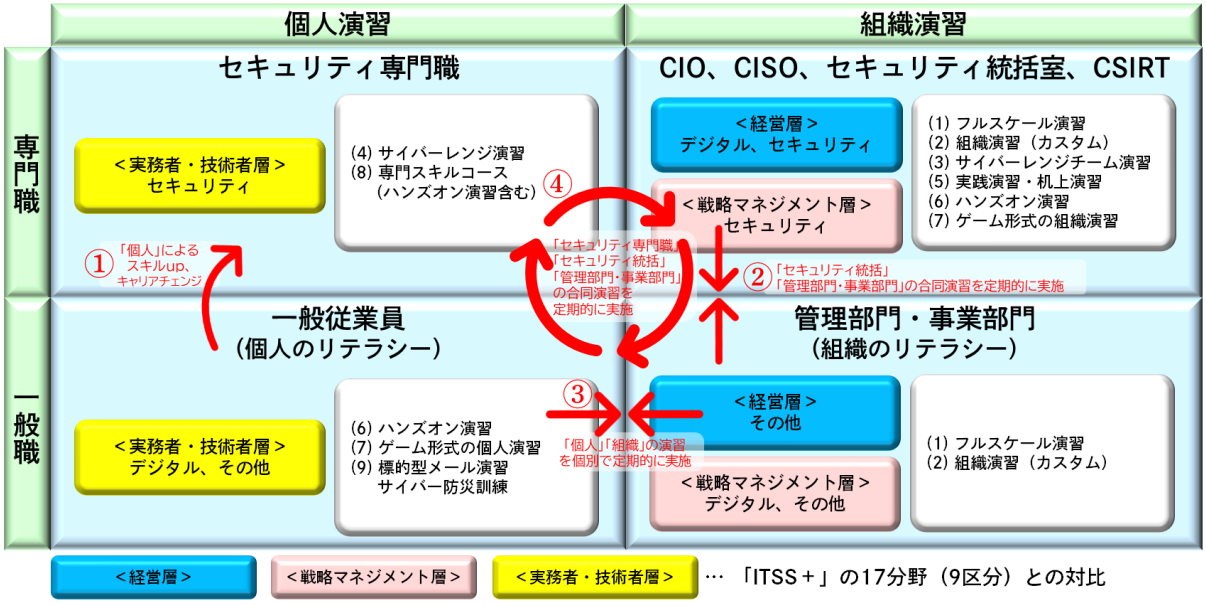


図８：演習マップ（四象限）

サイバーセキュリティの専門的スキルを持った人材がいない、あるいは少ない場合は、当面は外部にお願いすることになると思いますが、将来的には組織内で育成・確保していく必要があります。そのためにはまず演習マップ中の①にあるように『「個人」によるスキルアップ、キャリアチェンジ』を進める必要があります。知識を学習した対象者に演習を行うことで、セキュリティ専門人材に育成していくことになります。

また、演習マップ中の②にある『「セキュリティ統括」と「管理部門・事業部門」との合同演習』を行うことで、事業主体として組織全体を管理している管理部門・事業部門と、サイバーセキュリティ面で組織全体を管理するセキュリティ統括が車の両輪のように組織全体を推進することができるようになります。

演習マップ中の③では『「個人」と「組織」の演習』として、組織のセキュリティポリシーやガイドラインを適正に運用できているのかをチェックすることも重要でしょう。

最後になりましたが、演習マップ中の④にある『「セキュリティ専門職」と「セキュリティ統括」「管理部門・事業部門」の合同演習』を行うことで、インシデント発生時に組織全体のセキュリティ運用が適切に行えるのか、ＣＳＩＲＴ機能は考えているように機能するのかといった確認を行うことができます。

「形式“知”」である座学やｅラーニングなどの知識研修にも言えることですが、「経験“知”」を

あげるための演習についても、どこかの事象のみを実施したからといって組織全体のセキュリティレベルが上がるわけではありません。

演習マップの①から④までを、タイミングよく実施することでセキュリティレベルが上がることから、自組織では四象限のどこができていて、どこができていないかを可視化していただければと思います。

今回は、演習分科会参加企業が市場に提供している演習講座をマッピングし、活用の参考にするために本解説書で公開しましたが、今後は、分科会参加企業以外の講座についても、随時、追加やメンテナンスをしていく予定です。

５．１　各象限ごとの演習について

ここでは、演習マップ（四象限）の個人演習と組織演習、専門職と一般職の４つの象限について対象と演習内容について少し掘り下げてみます。

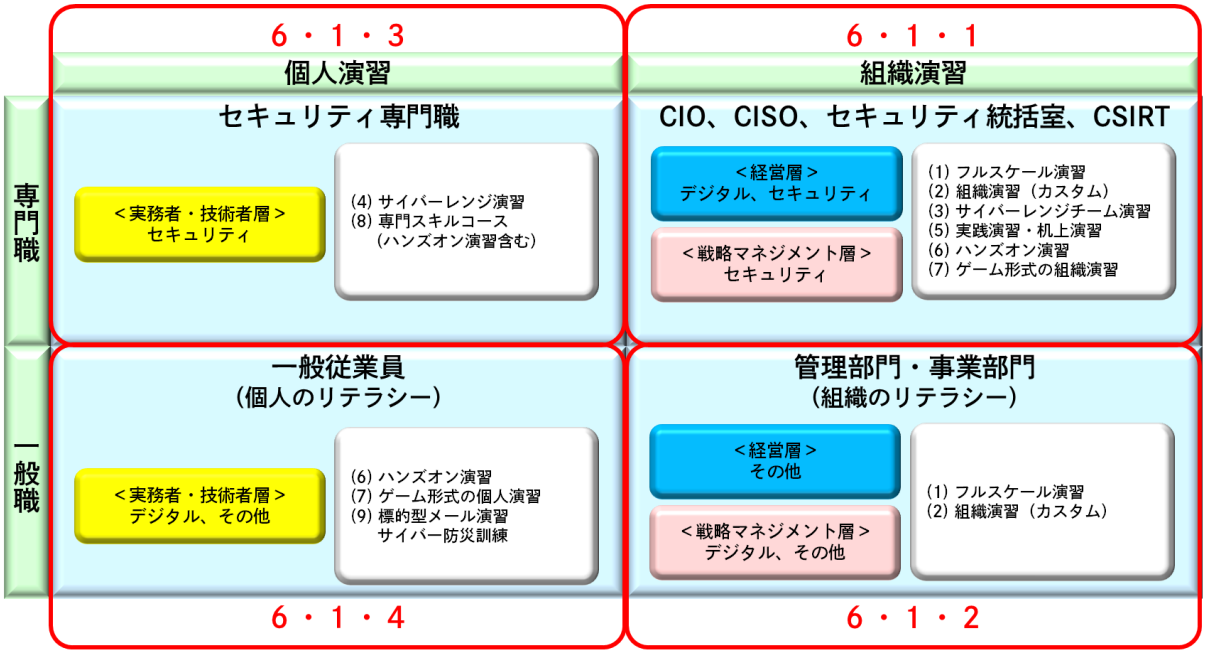


図９：演習マップ（四象限）

５．１．１　「組織演習／専門職」の象限
：ＣＩＯ、ＣＩＳＯ、セキュリティ統括室、ＣＳＩＲＴ

◎この象限の演習対象（ＩＴＳＳ+の１７分野）

「経営層」　　：デジタル経営（ＣＩＯ、ＣＤＯ）、セキュリティ経営（ＣＩＳＯ）

「戦略マネジメント層」：セキュリティ監査、セキュリティ統括

この象限の組織演習は、各サイバーインシデントに応じた、会社として判断が求められる事象についての関連部門演習です。

昨今、ＣＳＩＲＴの業務内容に対するサイバーレンジを用いた大型演習は、各省庁・公共機関においても実施されていますが、省庁の場合、受講者対象が限定されていたり、未だ多くの民間企業が参加できるような演習環境には、至っていない状況です。

本演習では、各種シナリオへのＣＳＩＲＴ対応のみならず、社内部門および仮想の外部機関と連携した形で、シナリオ工程毎にＣＩＯ、ＣＩＳＯとセキュリティ統括室の連携がどの様に

取られるべきかを演習します。この演習により、種々のインシデントに対して企業としてどの様にアクションを実施するべきかの「経験“知”」を習得することで、実際のインシデントに遭遇した場合も、演習した工程毎の対策を慌てず冷静に抜けなく講ずることができ、結果として企業全体のハードニングを実現し、被害額も最低限に抑えることが可能となります。

ただし、本演習の場合、連携部門を多くすると参加者数も増え集客も難しくなり、加えて企業指針を問われるシナリオも多いため経営層自身の演習参加も求められてきます。経営層は、これまで以上にサイバーインシデントが経営に及ぼす脅威を理解し、経営層自ら率先し演習開催を計画することにより、企業内組織間の連携を確認する必要が出てきます。

５．１．２　「組織演習／一般職」の象限
：管理部門・事業部門（組織のリテラシー）

◎この象限の演習対象（ＩＴＳＳ+の１７分野）

「経営層」　　：企業経営（取締役）

「戦略マネジメント層」：システム監査、デジタルシステムストラテジー、
経営リスクマネジメント、法務、事業ドメイン（戦略・企画・調達）

この象限の組織演習は、主にサイバーインシデント発生時に組織単位で対応しなくてはならない部署個別の演習です。

サイバーインシデントが発生した際、管理部門および事業部門では、インシデント発生時の対応プロセス（参考公開資料「ＣＳＩＲＴガイド」[8]）に則った対処を遂行するための演習が必要となります。例えば、一連のインシデント・プロセス対応において、法務では、情報漏洩・内部不正でのインシデントで発生した場合、早期の弁護士相談他が必要となり、広報ではインシデントの重要度に応じた外部メディアへの発信が必要となります。これらは、個人としての知識習得「形式“知”」に加え、組織演習を通じ、各部門業務の未対応・不足部分を明確にすることで適格な対策を講じることが出来る様になります。結果、「経験“知”」に基づく対応能力の向上につながります。

５．１．３　「個人演習／専門職」の象限
：セキュリティ専門職

◎この象限の演習対象（ＩＴＳＳ+の１７分野）

「実務者・技術者層」　：脆弱性診断、ペネトレーションテスト、セキュリティ監視・運用、
セキュリティ調査・分析・研究開発

[8] JPCERT/CC「CSIRT マテリアル」
https://www.jpcert.or.jp/csirt_material/

この象限の演習は、個人としてサイバーセキュリティ分野の前線で活躍を期待される人材となります。

実際のサイバーインシデント発生時下において、短時間で原因を調査し初動対処として、稼働しているシステムの停止など、トリアージ（判断）の提案・実施をすることが求められます。この場合、知識だけでは不十分であり、実践・経験“知”を養うためにも演習が重要となっています。

必要な演習環境としては、サイバーレンジ（サイバー攻撃、防御の実習をクラウド他の仮想空間上で実施する演習の総称）が多用されています。サイバーレンジでは、いくつかのインシデント発生シナリオに応じたＣＳＩＲＴ業務の確認をしたり、ＩＯＣ（Ｉｎｄｉｃａｔｏｒ ｏｆ Ｃｏｍｐｒｏｍｉｓｅ）分析を実環境下で行うなど、実践力を効率的に向上することができます。

また、受講者を攻撃側と防御側に分けて行うハッキング演習ＣＴＦ（Ｃａｐｔｕｒｅ Ｔｈｅ Ｆｌａｇ）もサイバーレンジ演習の特徴であり、国内・国外問わず多くのセキュリティコンテストが開催されています。これらコンテストに参加し、社外のエンジニアと切磋琢磨することも有益なスキルアップ手法と言えます。

５．１．４　「個人演習／一般職」の象限
：一般従業員（個人のリテラシー）

◎この象限の演習対象（ＩＴＳＳ+の１７分野）

「実務者・技術者層」　：デジタルシステムアーキテクチャー、デジタルプロダクト開発、
デジタルプロダクトマネジメント、
事業ドメイン（生産現場・店舗管理）

この象限の演習は、企業の事業運用業務に従事する従業員がサイバーセキュリティに関するリテラシーを向上させるための基礎知識を得た後に、実践力を向上させるための演習を示しています。

例えば、企業での社員教育の一環として、自社のセキュリティポリシーの研修を開催したり、「情報セキュリティ１０大脅威２０２１」[9]のサイバーインシデント脅威について話し合う学習機会を設けている企業も増えてきいます。ＩＳＭＳ（情報セキュリティマネジメントシステム）の認証取得組織数が６３００社を超し増加していることも[10]、定着要因の一つと言えでしょう。

これら座学知識学習による「形式“知”」を、より効果的に実践力に繋げるための「経験“知”」修得のための演習としては、ゲーム形式で各種インシデント対応が経験できる演習プログラムも多

[9] IPA：独立行政法人情報処理推進機構「情報セキュリティ 10 大脅威 2021」
https://www.ipa.go.jp/security/vuln/10threats2021.html

[10] 情報マネジメントシステム認定センター「ISMS 認証登録数」
https://isms.jp/topics/news/20191112.html

くリリースされてきています。また、多くのサイバーインシデント要因である標的型攻撃メールに関しても、社内感染率を下げるため、事前通知がされない形で社員に疑似標的型攻撃メールを送信し、感染率を低減させていく実践演習を始めている企業もあります。

５．２　組織横断的演習の必要性

５．１では各象限の中での演習を説明しました、しかし最終目的は企業・団体全体のサイバーインシデントのハードニング体制であり、実現のためには各組織に閉じた演習だけでは獲得できません。

各象限同士の連携に重きを置いた演習が必要であり、政府も色々な業界の重要インフラを集めた演習を開始していることからも、民間企業も同様に企業内組織全体が連携した演習を実施すべきです。ここでは各象限同士が連携した演習について説明する。演習マップ（四象限）内に記載した①～④の演習について説明します。

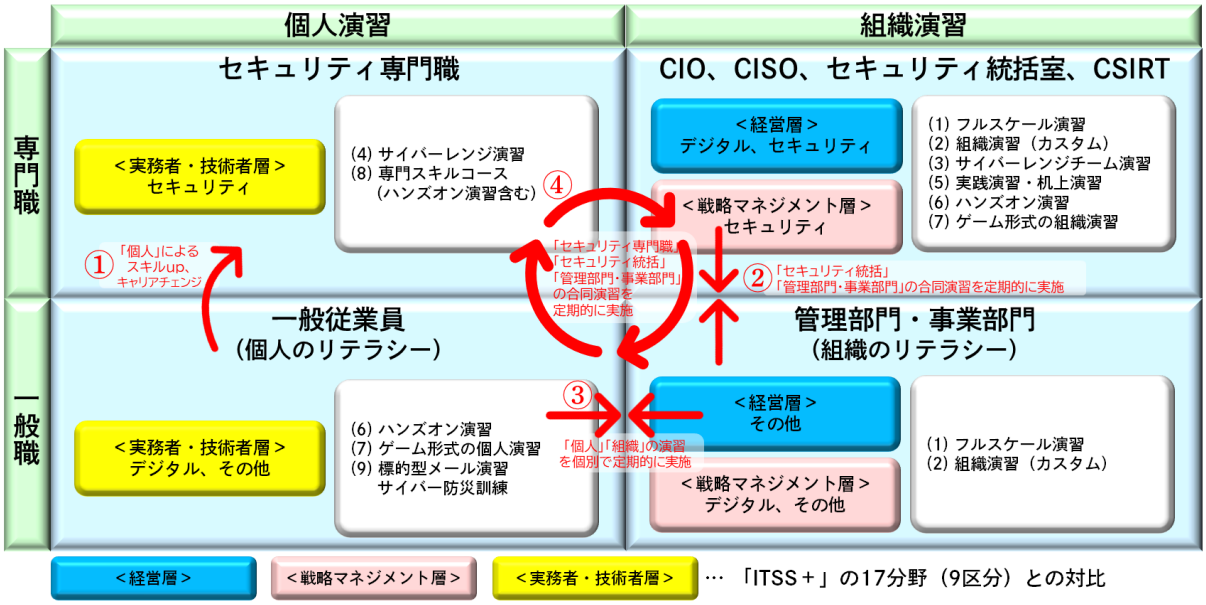


図１０：演習マップ（四象限）

① 個人によるスキルＵＰ、キャリアチェンジ

知識を学習した対象者に演習を行うことで、セキュリティ専門人材に育成していくことになります。業務ミッションもしくは個人のスキルアップ・キャリアチェンジのために、より専門性が高い演習へのステップアップを実施するキャリアパスを示しています。企業・団体としてキャリアチェンジの可能性も示すことが受講者のモチベーションにもつながり、企業としても不足するセキュリティスキルを持つ人材を育成することで、各部門にセキュリティ人員配備ができ、面としての体制を確保できます。

②「セキュリティ統括」「管理部門・事業部門」の合同演習を定期的に実施

企業単位でのサイバーインシデント対応能力を考えた場合、本合同演習は非常に重要と言えます。各インシデント対処工程に、いかに優秀な人材が居たとしても組織連携ができなければ、対外的なアクションが後手に廻ってしまい被害規模が時間の経過と共に大きくなってしまいます。

合同演習により、種々のインデント対応に合致した、会社の対応指針を定義することで、報告義務のある外部機関との連携対策、メディアに対する公表対策ほか有事への企業・団体全体としての対策をスムーズ、かつスピーディに実施することができるようになります。

③「個人」「組織」の演習を個別で定期的に実施

組織のセキュリティポリシーやガイドラインを適正に運用できているのかをチェックすることも重要といえます。組織単位でのサイバー演習を定期的に実施することにより、個人レベルとして不足している能力・技量が明確になります。その課題を個人学習として新たに習得することで、上述①のキャリアパスが実現され、社内のサイバーセキュリティ人材不足解消にも効果が得られます。企業・団体は、①②を具現化できる個人学習を啓発する社内プログラムの提供が必要となります。

④「専門職」「セキュリティ統括」「管理部門・事業部門」合同演習を定期的に実施

「演習マップ（四象限）」中の④のサークルは、社内・社外連携も踏まえた総合的なサイバー演習を意図しています。参加部門が多くなりますが、実際のインシデント発生時のアクションに一番近く、この演習をＰＤＣＡにて廻すことで、企業のハードニングをより向上することができるようになります。加えて、この演習を定期的に実施していくことで、社員一人一人のサイバーセキュリティに対する意識が向上し、四象限の演習連携が効果的に稼働し始め、社内のサイバーセキュリティ人材育成が実現されていく相乗効果も期待できます。

この様な、会社の部門連係、および社外機関との連携も含んだ大型の演習としては、国内省庁（ＮＩＳＣの分野横断的演習[11]、金融庁のＤｅｌｔａＷａｌｌ[12]など）、公共機関（ＮＩＣＴによるＣＹＤＥＲ[13]での全国演習、政令都市でのＩＴ－ＢＣＰなど）主導による大型サイバー演習も開催されてきています。

---

[11] NISC（内閣サイバーセキュリティセンター）「分野横断的演習」
https://www.nisc.go.jp/conference/cs/ciip/dai23/pdf/23shiryou03.pdf

[12] 金融庁「金融業界横断的なサイバーセキュリティ演習（DeltaWall V）について」
https://www.fsa.go.jp/news/r2/20201013.html

[13] 情報通信研究機構（NICT）「CYDER について」
https://cyder.nict.go.jp/

海外では、２０１１年から定期的に実施されてきている米国の米国証券業金融市場協会が主催するＱｕａｎｔｕｍ Ｄａｗｎ[14]、英国のＷａｋｉｎｇ Ｓｈａｒｋ[15]が挙げられます。

米国のＱｕａｎｔｕｍ Ｄａｗｎでの演習シナリオを考察すると、社内組織のみならず外部連携組織の実担当者（個人情報保護委員会、各種ＩＳＡＣ、ＦＢＩ、警察など）も出席することで、より現実性が増したシナリオ演習が具現化されています。また、多くのシナリオ終盤では、企業風土の差異に起因すると考えられますが、インシデント発生企業の株価低下におけるＣＩＳＯ／役員の引責辞任までシナリオ化されているのが印象的です。

ＥＵ「一般データ保護規則（ＧＤＰＲ）」[16]で一企業が２５億円以上の巨額な制裁金請求を受けたり、公共施設から大量の機密データ流出によるＴＶ謝罪など、日本でも経営者が重責を負うケースも少なくありません。この様な場合、単に知識を習得する研修では不十分であり、多くの役員レベルの方も演習に参加した、実践的なサイバーセキュリティのＢＣＰ（事業継続）演習が重要性を増していると言えます。

---

[14] 米国証券業金融市場協会（Sifma）「Quantum Dawn」
https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-v/

[15] Waking-Shark
https://www.bankofengland.co.uk/news/2014/february/cyber-resilience-exercise
https://www.bba.org.uk/wp-content/uploads/2014/02/Banking_3192106_v_1_Waking-Shark-II-Report-v1.pdf.pdf

[16] 一般データ保護規則（GDPR）
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

6．サイバーセキュリティ組織能力の客観的評価について

近年、経営課題としてサイバーセキュリティを取り扱う事は半ば常識となり、経済産業省の「サイバーセキュリティ経営ガイドラインｖ２．０」[17]は、すでに多くの経営者の判断に役立てられていることは間違い有りません。また、ＮＩＳＣの「サイバーセキュリティ２０２０」[18]においても「任務保障」をサイバーセキュリティの最重要課題として位置付けています。これは顧客に対するサービス提供において、正しいリスクアセスメントに基づき、サービスを提供し続けていく事を企業に課せられた一つの義務として捉えることが求められていく事を示しています。

一方、ＤＸ（デジタルトランスフォーメーション）の推進もコロナ禍における新しい社会課題として表出しており、イノベーションの推進とリスクマネジメントのバランスが、ますます喫緊の課題となりつつあります。Ｃ（機密性）、Ｉ（完全性）、Ａ（可用性）の中でも可用性の重みが増し、ビジネスを止めないセキュリティの在り方が、経営判断の上でより大きな意味を持ち、企業の評価を決める重要な要素になっていく事が予想されます。

こういった環境の変化や企業に求められる経営課題を経営指標化し、継続的に改善を図る事が、これからのサイバーセキュリティ経営には必須となっていきます。平時におけるＰＤＣＡを回しながら、事案対処のスピード感においてはＯＯＤＡループ[19]を回しながら、より素早く対処していく組織能力が企業の評価を左右すると言っても過言ではありません。

米国ＮＩＳＴの「Ｃｙｂｅｒ Ｓｅｃｕｒｉｔｙ Ｆｒａｍｅｗｏｒｋ」[20]においては、特定、防御、検知、対応、復旧の５つの機能がサイバーセキュリティにおいては重要であると説明しています。このうち特定、防御、検知はこれまでファイアーウォールに守られた境界型防御中心のセキュリティ対策が中心課題でした。しかし、サイバー攻撃はより高度化し、周到に調査を重ねた標的型攻撃は、もはや境界型防御だけで気づくことは難しくなりつつあります。

不正侵入を前提とした対応、復旧までも見据えた対応能力の向上が組織能力の上でより重要になり、少しでも早く侵入の兆候に気づき、いかに被害を最小限に食い止められるか、そのスピードと対応の正確性が問われているのです。

データ保護主義の高まりにより、求められる対応能力はさらに高度化してきています。ＥＵ「一

---

[17] 経済産業省「サイバーセキュリティ経営ガイドライン」
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[18] サイバーセキュリティ戦略本部「サイバーセキュリティ 2020」
https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf

[19] OODA ループ　「Observe（観察） - Orient（方向づけ） - Decide（意思決定） - Act（行動）」の４つの頭文字から名付けられ、アメリカ空軍の大佐が提唱した意思決定メソッドの１つ。判断を最適にするための理論として生まれ、ビジネスにも応用され始めた。
https://ja.wikipedia.org/wiki/OODA%E3%83%AB%E3%83%BC%E3%83%97

[20] National Institute of Standards and Technology (NIST)「Cyber Security Framework」
https://www.nist.gov/cyberframework

般データ保護規則（ＧＤＰＲ）」においては、データへの侵害が発生した際、７２時間以内の監督機関への詳細な報告が義務づけられます。報告の正確性や対応の妥当性など短時間で多くの情報をまとめなければなりません。こういった報告の義務や速やかな情報開示、公表は企業の社会的信用を守るうえで今後ますます重要になってくものと思われます。

本書で中心的に掲げた演習は、このような組織能力を個々のスキル向上に留まらず、必要な機能が有機的に繋がり総合的に機能する事を経験“知”の向上を通じて目指すものとなっています。

組織能力が目指す水準に到達しているのかどうか、足りない能力は何なのか、そういった組織能力の可視化を継続的に行い、改善していく事が重要です。組織能力を客観的に評価するツールはすでに数多く存在しています。ＥＵの「ＥＮＩＳＡ」[21]がリリースしたＣＳＩＲＴの能力を成熟度モデルで評価する「ＳＩＭ３」[22]、「ＩＳＯＧ－Ｊ」[23]が提供する「セキュリティ対応組織成熟度セルフチェックシート」[24]などは認知度が高く、専門家の知見が反映された使いやすいものになっています。こういった評価ツールは日本シーサート協議会[25]やＩＳＡＣのような情報共有の為の団体に属する事で、同業種との比較や目指すべきレベルといった指標を得ることで、より客観性を担保できます。単にツールを使う事に留まらず、知見の向上や情報共有という観点でこういった組織に属する事による組織力の向上を図ることが、今後さらに求められていきます。また、単にスナップショットで他社と比較するだけでなく、自社の能力の向上を継続的に測定し改善が出来ているか、低下している能力はないかなどの視点を持つことが重要です。

最後に組織能力の向上で最も重要なのは経営者の主体的取り組みです。サイバーセキュリティにおける組織能力の向上が経営者の重要課題である事はすでにご説明させていただきました。それに加え近年グローバルにおいてより重視されている企業のＥＳＧ評価において、評価機関は情報セキュリティをガバナンスの評価項目の一部として捉えています。またその中でもサイバーセキュリティを情報セキュリティの重要要素として捉える動きが強まってきています。つまり、経営者にとってサイバーセキュリティにおける組織能力の向上は企業価値に直結する重要な経営指標となってきているという事を意味しています。

日本ＩＴ団体連盟では、日経２２５を対象に開示情報から各社のサイバーセキュリティ対策

---

21 ENISA　「The European Union Agency for Cybersecurity」の略

22 Open CSIRT Foundation 「SIM3（Security Incident Management Maturity Model）」
https://opencsirt.org/maturity/sim3/

23 ISOG-J（日本セキュリティオペレーション事業者協議会）
https://isog-j.org/

24 ISOG-J「セキュリティ対応組織成熟度セルフチェックシート」
https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

25 日本シーサート協議会
https://www.nca.gr.jp/

情報開示に関する調査結果を公開[26]しています。有価証券報告書やコーポレートガバナンス報告書などの開示情報からサイバーセキュリティや個人情報保護に関する記載内容、更にはＩＳＭＳなどの第三者認証情報などから総合的に企業の取り組み姿勢を調査いたしました。２０２１年以降、調査の対象企業・項目ともに拡大し実施する計画です。また拡大する項目としては、公表されている情報だけではなく、組織としての取り組みなどの非公開情報を含めることを計画しており、サイバーセキュリティに携わる人材の重要性と組織能力の向上の必要性、その価値を経営課題の重要なテーマとして取り組んで頂くためにも、今後調査および評価に盛り込んでいきます。

[26] 日本 IT 団体連盟「サイバーセキュリティ対策情報開示に関する調査結果を公開」
https://www.itrenmei.jp/topics/2020/3678/

7．付録

今年度調査・分析し現時点市場に提供されているサイバー演習講座を、本編で解説した「演習マップ（四象限）」の各象限に対応した演習形式ごとにリスト化した、「サイバーセキュリティ演習マッピング」を別冊として掲載しました。

以下、「演習マップ（四象限）」と「サイバーセキュリティ演習マップ」の使用方法を記載します。

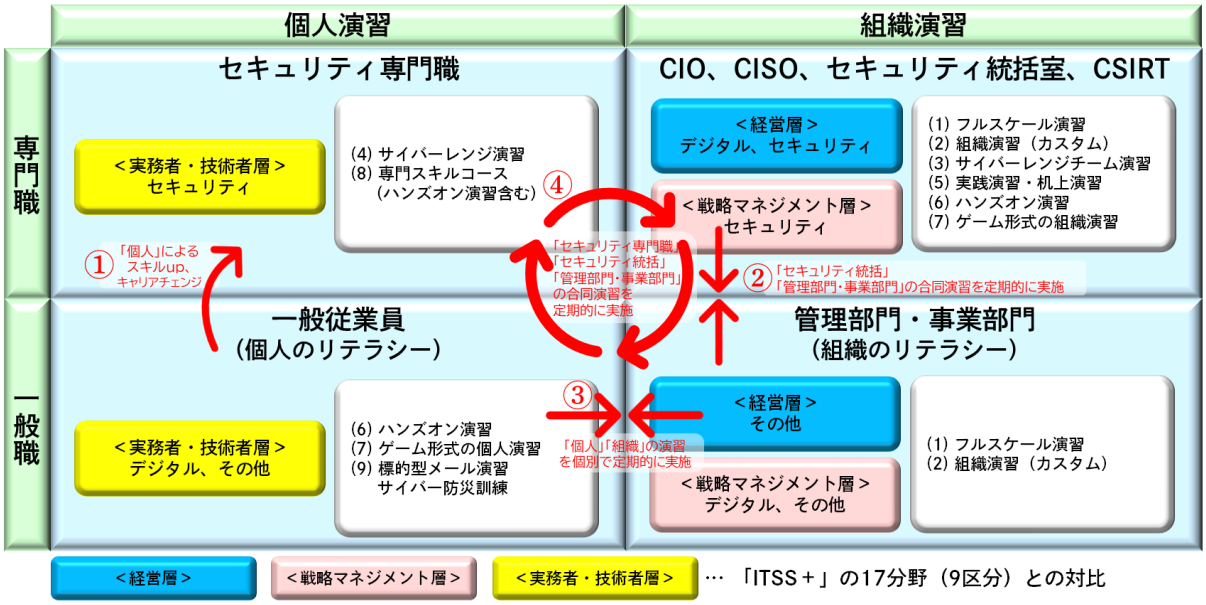


図１１：演習マップ（四象限）

演習マップの見方は、「縦軸」である「個人演習」か「組織演習」かにより大きく大別され、さらにセキュリティの「専門職」か「一般職」かの「横軸」を選ぶことにより、四象限の中の自身・自組織のポジションを選定します。

選定した「象限」の白地の個所に記載がある演習が、同象限に有効と考えられる「演習形式」となります。

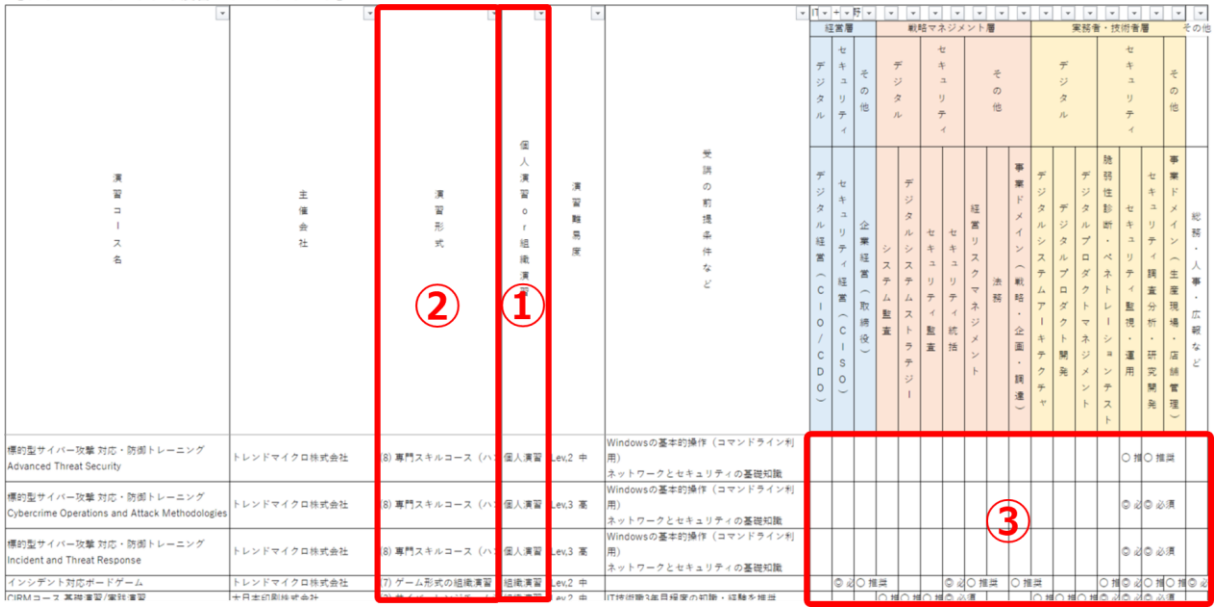
また、「象限」に記載の「青地：経営層」「ピンク地：戦略マネジメント層」「黄地：実務者・技術者層」は、「対象者」を示しており、「ＩＴＳＳ＋」の１７分野（９区分）にて定義されている組織内の役割としています。

赤文字で記載している②から④の「組織演習」は、特に組織として重要と位置づける「組織演習」を示しており、この後説明する「サイバーセキュリティ演習マッピングリスト」にて、対象の「演習コース」選択の際、関連する象限に属する「対象者（◎必須、○推奨）」がマッピングされているか否かをチェックする際の参考として頂ければと思います。

次に、「サイバーセキュリティ演習マッピングリスト」について説明します。
ここでは、「シンプルな絞り込み方」と「組織・役割が明確になっている場合の絞り込み方」の二通りの利用シーンを記載しますが、使用方法をご理解いただいた際には、独自の検索方法により利用されることを推奨します。

表３：サイバーセキュリティ演習マッピングリスト

【サイバーセキュリティ演習マッピングリスト】

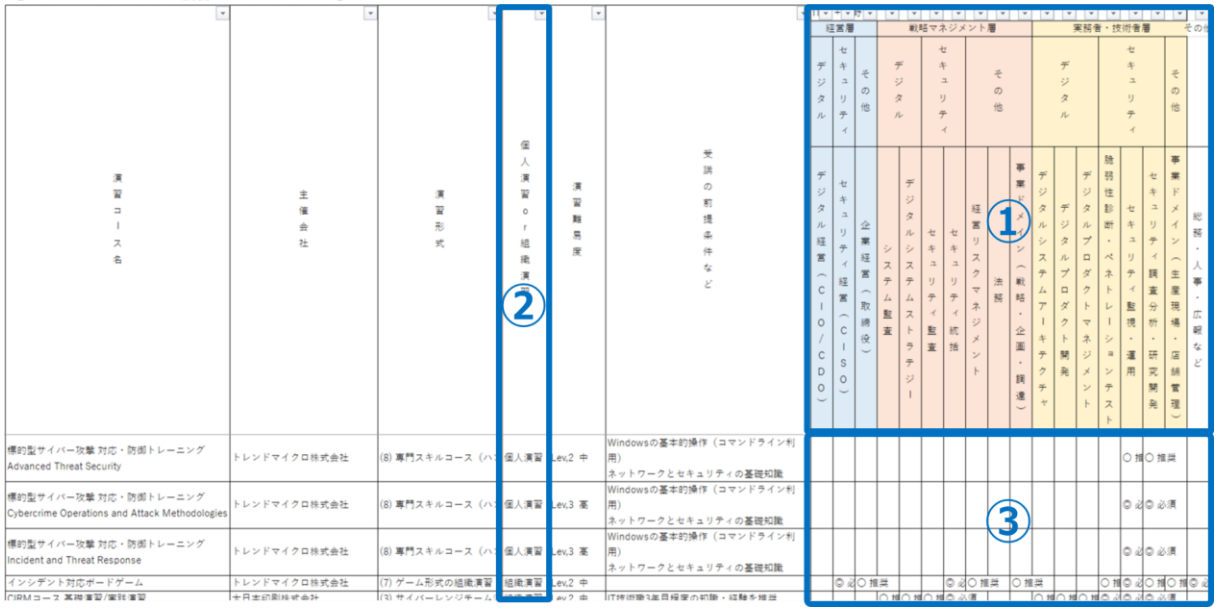


■シンプルな絞り込み方
① で、「個人演習」か「組織演習」をプルダウンより選択
② で、「演習形式」に記載の演習候補より選択
※組織演習の場合は、③に「◎必須」か「○推奨」の記載のある部門・担当者が一堂に会して演習に参加することが望ましい。

※注「サイバーセキュリティ演習マッピングリスト」は、２０２１年３月現在の情報です。
より詳細な情報につきましては、別冊のＥｘｃｅｌ表にてご確認ください。
掲載されている各社の演習が、現在実施中かなどは、主催会社に直接ご確認ください。

表４：サイバーセキュリティ演習マッピングリスト

【サイバーセキュリティ演習マッピングリスト】



■組織・役割が明確になっている場合の絞り込み方

① の、組織・役割列で「◎必須」「○推奨」を片方もしくは両方選択

② で、「個人演習」か「組織演習」を選択

③ に、「◎必須」か「○推奨」が記載されている「演習コース」が適している

※組織演習の場合は、③に「◎必須」か「○推奨」の記載のある部門・担当者が一堂に会して演習に参加することが望ましい。

※注「サイバーセキュリティ演習マッピングリスト」は、２０２１年３月現在の情報です。
より詳細な情報につきましては、別冊のＥｘｃｅｌ表にてご確認ください。
掲載されている各社の演習が、現在実施中かなどは、主催会社に直接ご確認ください。

今回リストに一覧化した演習コース数だけでは、選択方法いかんで、対象コースが存在しないケースもあり得ます。今後分科会にて市場で提供されている演習コースの数を増やすことと、独自に演習化する事も検討していく計画です。

8．おわりに

企業・団体が、真の意味でレジリエンス向上に必要な「経験“知”」獲得を支援する「サイバーセキュリティ演習」の調査・分析と本解説書公開にあたり、これまで相当な時間を提供していただきました日本ＩＴ団体連盟サイバーセキュリティ委員会サイバーセキュリティ演習分科会メンバーの皆さまは勿論のこと、解説書公開への道筋をリード頂きました、企画分科会丸山様、また同団体連盟専務理事の中谷様はじめ事務局の皆さまには、多大なご尽力を頂きました。この場をお借りして御礼を申し上げます。

おわりにあたり、サイバーセキュリティ演習分科会について記載します。

＜演習の定義＞

組織と個人の「能力評価」

⇒対策が機能するか否か、不備の有無の「見える化」

組織と個人の有事における「行動の再現性の獲得」

⇒防災訓練の実践と同じく、平時より実践環境訓練を定期的に実施し、「経験の蓄積」を図るための手段

＜分科会の目的＞

データ駆動型経済の実現に向け、新しいＩＴアーキテクチャー化（ＤＸ化）が促進される中で、企業・団体が強固な事業継続性を確保するために、消防法における「防火管理者の設置」や「消防訓練の実施」のように、サイバーセキュリティでも「定期的な防災訓練を常態化」する。

今年度活動の成果として公開の運びとなった本解説書と演習マッピングリストは、今後特に演習マッピングリストの随時更新は勿論ですが、次のステップとして解説書と演習マッピングリストが実際に有効活用され、たくさんの方々が自組織に適した演習と出会って頂くことで普及し、組織内の個人と組織全体のレベルが上がり、企業・団体のレジリエンスが向上するための具体的な施策について検討していく計画です。

早期に実現できるよう活動は継続していきますが、多くの企業・団体様にサイバーセキュリティ委員会、サイバーセキュリティ演習分科会活動への賛同、また、参加頂ければ幸いです

なお、サイバーセキュリティ演習の「解説書」「演習マッピングリスト」並びにサイバーセキュリティ委員会の各分科会活動についてのご質問は、お問い合わせ先宛てご連絡お願いします。

＜お問合せ先＞

一般社団法人　日本ＩＴ団体連盟「ご入会・お問い合わせ」フォーム

https://www.itrenmei.jp/contact1/

本解説書編纂メンバー

一般社団法人　日本ＩＴ団体連盟　サイバーセキュリティ委員会
サイバーセキュリティ演習分科会グループメンバー

サイバーセキュリティ委員会委員長

下村　正洋	ＮＰＯ日本ネットワークセキュリティ協会

企画分科会主査

丸山　司郎	

サイバーセキュリティ演習分科会主査

谷　建志	大日本印刷株式会社

本書執筆メンバー（所属企業名　５０音順）

小林　　忍	アライドテレシス株式会社
菅谷　光啓	ＮＲＩセキュアテクノロジーズ株式会社
萩原　健太	グローバルセキュリティエキスパート株式会社
松山　哲也	大日本印刷株式会社
日向　　亨	トレンドマイクロ株式会社
持田　啓司	株式会社ラック