

レッスン1

セキュリティロールとセキュリティ管理を比較する

レッスン概要

セキュリティは、要求事項の評価、組織のセキュリティシステムの構築、強化、および監視、進行中の攻撃への対応、そして脅威アクターの抑止を含む継続的なプロセスです。セキュリティのプロフェッショナルとして、セキュリティ機能が部門またはユニットとしてどのように実行されるかや、さまざまな組織内での職務上の役割（ロール）を理解するのが重要です。また、セキュリティ管理の選択を進めるにあたり、コンプライアンスの要素と、ベストプラクティスのフレームワークの重要性を説明できなければなりません。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- 情報セキュリティロールを比較対照する。
- セキュリティの管理とフレームワークの各タイプを比較対照する。

トピック1A

情報セキュリティロールを比較対照する



対象試験範囲

このトピックは、セキュリティ専門家の役割についてその背景となる情報を提供するものであり、特定の試験範囲はカバーしません。

セキュリティのプロフェッショナルとして成果を挙げ、信用を得るには、ビジネスにおけるセキュリティを一から理解しなければなりません。同時に、他のセキュリティ専門家が技術文書や刊行物で使用している、セキュリティ関連の主要な用語や考え方も知る必要があります。セキュリティの実行は、巨大な建物が個々の煉瓦から建設されるように、基本的なブロックから構築されます。このトピックは、そうしたブロックを理解し、自分のセキュリティキャリアの基礎として活用できるようにするのをサポートします。

情報セキュリティ

情報セキュリティ（またはinfosec）は、不正なアクセス、攻撃、窃盗、または損害から、データリソースを保護することを指します。保存、転送、および処理の方法のために、データが脆弱である場合もあります。データの保存、転送、処理に使用されるシステムには、セキュリティの各特性が備わっていなければなりません。セキュアな情報には次の3つの特性があり、しばしば**CIAトライアド**と呼ばれます。

- **Confidentiality (機密性)** は、特定の情報は特定の人間にのみ知らされるべきである、ということを意味します。
- **Integrity (完全性)** は、データは意図されたとおりに保存および転送される必要があり、変更には必ず認可が必要である、ということを意味します。
- **Availability (可用性)** は、閲覧または変更を許可された人間がデータを要求したときに、データへのアクセスや使用が可能である、ということを意味します。



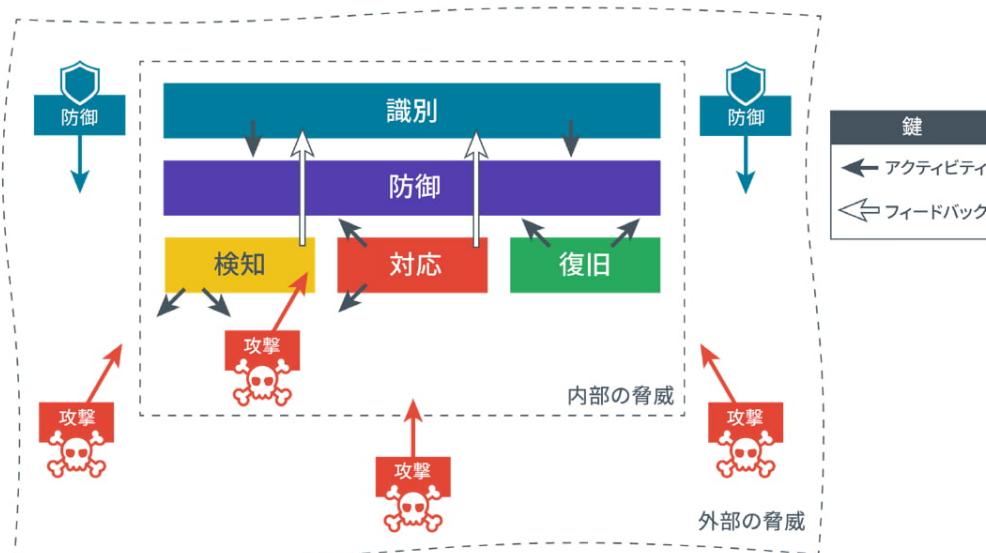
中央情報局(Central Intelligence Agency)との混同を避けるために、CIAトライアドは「AIC」とも呼ばれます。

セキュリティのモデルや研究者の中には、セキュアなシステムが示すべきその他の特性を明らかにしているものもあります。それらの中で最も重要なのは否認防止です。**否認防止**は、リソースの作成、変更、または送信などを行ったことを、対象者が否定できないことを意味します。一例を挙げると、遺言書などの法律文書は通常、署名の際に立ち会いが必要とされます。その文書が正しく執行されたかどうかについて紛争が起きた時、立会人がその証拠を提供できるのです。

サイバーセキュリティフレームワーク

情報セキュリティを確保するという目標の中で、サーバーセキュリティは特に、ハードウェアとソフトウェアのセキュアな処理を提供することを指します。情報セキュリティとサイバーセキュリティのタスクは、[米国国立標準技術研究所\(NIST\)が開発したフレームワークに従い、次の5つの機能に分類されます\(nist.gov/cyberframework/online-learning/five-functions\)](https://nist.gov/cyberframework/online-learning/five-functions)。

- ・識別—セキュリティポリシーと能力を開発する。リスク、脅威、脆弱性を評価し、それらを軽減するセキュリティ管理を推奨する。
- ・防御—ITハードウェアおよびソフトウェア資産の入手/開発、インストール、運用、そして使用停止という運用ライフサイクルの各段階において、セキュリティを要求事項として組み込む。
- ・検知—監視を継続的・積極的に行い、管理が効果的であり、新種の脅威から保護できることを確認する。
- ・対応—システムとデータのセキュリティに対する脅威を識別・分析し、封じ込めて根絶する。
- ・復旧—サイバーセキュリティ耐性を実装し、その他の管理が攻撃を防げない場合であっても、システムとデータを修復する。



中核となるサイバーセキュリティ業務。

情報セキュリティ能力

セキュリティの責任を負った職務に携わるITプロフェッショナルは、ネットワークやアプリケーションの開発から、調達および人材(HR)に至るまで、幅広い分野の能力を有していくなければなりません。そうした職務に典型的なアクティビティとして、次のものがあります。

- ・リスク評価とセキュリティシステムのテストに参加し、提言を行う。
- ・セキュアなデバイスとソフトウェアの特定、調達、インストール、および構成を行う。
- ・アクセス制御とユーザー特権プロファイルのドキュメントを構築・維持する。
- ・監査ログの監視、ユーザー特権の見直し、アクセス制御の文書化を行う。
- ・セキュリティ関連のインシデント対応とレポートを管理する。

- ・ ビジネスの継続性、および災害復旧計画と手順を立案・テストする。
- ・ セキュリティトレーニングや教育プログラムに参加する。

情報セキュリティロールと責任

セキュリティポリシーは、組織内でセキュリティがどのように実装されるかを定義する、正式な声明です。機密のデータやリソースの機密性、可用性、および完全性を保護するためにその組織がとる手段を説明しています。多くの場合、それは複数の個別ポリシーから構成されます。CIAトライアドの目標をサポートするためのセキュリティポリシーの導入は、学校、多国籍の会計事務所、または工作機械メーカーで大きく異なるかもしれません。しかし、そうした組織のそれぞれ、または（営利組織か非営利組織かを問わず、経済のあらゆるセクターに属する）他のすべての組織は、従業員、装置、およびデータが攻撃や損害に対してセキュアであるようにすることに、同じ関心を抱かなければなりません。

効果的な組織セキュリティの方針を採用するにあたり、そのプロセスの一環として、従業員は自分の責任を認識する必要があります。セキュリティに関する責任の構造は、組織の規模とヒエラルキーに左右されますが、それらの職務は一般的なものです。

- ・ セキュリティに関する組織内の全体的責任が、セキュリティ部長、チーフセキュリティオフィサー (CSO)、または**チーフインフォメーションセキュリティオフィサー (CISO)**によって運営される、専門部署に割り当てられることもあります。歴史的に見て、セキュリティに関する責任は、情報・コミュニケーションテクノロジー (ICT) や経理など、既存の業務ユニットに割り当てられてきました。

しかし、ネットワーク管理者の目標がセキュリティの目標と常に一致しているわけではなく、ネットワーク管理は機密性よりも可用性の方に焦点を当てています。結果としてセキュリティは、それ自身の管理構造を持つ専門の機能ないし業務ユニットとして、ますます考えられるようになっています。

- ・ 管理者は、構築管理、ICT、または経理など、1つの領域に対して責任を負っています。
- ・ 技術スタッフと専門スタッフには、ポリシーの実行、維持、および監視の責任があります。セキュリティがシステムおよびネットワーク管理者の中心的能力にされることもあれば、専門のセキュリティ管理者が置かれることもあります。そうした肩書きの1つに、**情報システムセキュリティオフィサー (ISSO)**というものがあります。
- ・ 非技術スタッフには、ポリシーとすべての関連法令を遵守する責任があります。
- ・ セキュリティに関する外部への責任（しかるべき注意または義務）は主として取締役や所有者に課せられますが、ここでもすべての従業員に一定の責任を共有させることが重要です。



NISTの「サイバーセキュリティ教育の国家イニシアチブ(NICE)」は、サイバーセキュリティ業界内部の職務と役職を分類しています(gov/itl/applied-cybersecurity/nice/nice-framework-resource-center)。

情報セキュリティ業務ユニット

組織ヒエラルキー内でセキュリティ機能実施を担当するために、次のユニットがしばしば置かれます。

セキュリティ運用センター (SOC)

セキュリティ運用センター (SOC)は、経理、総務、販売/マーケティングといったその他の業務部門にまたがる重要な情報資産を、セキュリティのプロフェッショナルが監視・保護する部所です。SOCを配置して維持し、予算を確保するのが困難なこともありますので、通常は政府機関や医療関連企業など、大規模な組織で採用されています。



IBMセキュリティ本部（マサチューセッツ州ケンブリッジ）
(画像提供 : John Mattern/Feature Photo Service for IBM.)

DevSecOps

ネットワーク運用とクラウドコンピューティングの活用により、ソフトウェアコードによる自動化がますます利用されるようになっています。従来、ソフトウェアコードはプログラミングチームや開発チームの責任でした。個別の開発および運用部門（またはチーム）が壁となり、各チームが他のチームと効果的に連携できないこともあります。

開発と運用(DevOps)は、開発者とシステム管理者との連携を大きく促す、組織内の文化的シフトです。高度に調整された環境を生み出すことで、ITスタッフと開発者はより迅速に、かつ信頼性が高い形で、ソフトウェアの構築、テスト、リリースを行うことができます。クラウドサービスプロバイダーが提供する潜在的なメリットを組織が最大限に活用するには、DevOps管理アプローチが唯一の方法であると、多くの人が考えています。

DevSecOpsはその境界をセキュリティの専門家とスタッフにまで広げたもので、ソフトウェアの開発とデプロイ（展開）の各段階においてはセキュリティが主たる検討事項であるという原則を反映しています。これはシフトレフトとしても知られ、セキュリティの検討事項は最後に継ぎ合わされるのではなく、要件定義と計画の立案段階で作成する必要がある、ということを意味します。DevSecOpsの原則はそれを認めるものであり、どの開発プロジェクトにもセキュリティ技能が組み込まれていなければならぬことを示しています。これに付随するものとして、セキュリティ業務はソフトウェア開発プロジェクトとして捉えることができる、という認識があります。セキュリティツールはコードで自動化できます。結果として、検知と監視を改善するにあたり、開発者の技能がセキュリティ業務に取り入れられる必要があります。

インシデント対応

セキュリティインシデントを報告する単独の連絡先として、専門のサイバーアインシデントレスポンスチーム(CIRT)、コンピューターセキュリティインシデントレスポンスチーム(CSIRT)、またはコンピューター緊急事態対応チーム(CERT)があります。SOCがこの機能を担当することもあれば、独立した業務ユニットとして配置されることもあります。

レビュー アク ティビティ：

情報セキュリティロール

次の質問にお答えください。

1. セキュアな情報処理システムの特性は何ですか？
2. 送信者がメッセージを送信したことを否定できないという、セキュアなネットワークの特性を説明する用語は何ですか？
3. 多国籍企業は大量の価値ある知的財産(IP)データに加え、顧客やアカウント所有者の個人データを管理しています。そうした重要かつ複雑なセキュリティ上の要求事項を管理するのは、どのタイプの業務ユニットですか？
4. 業務が急速に拡張しており、所有者は既存のIT部門とプログラミング部門との対立を心配しています。そうした問題を解決するのに役立つのは、どのタイプのセキュリティ業務ユニット（または部署）ですか？

トピック1B

セキュリティの管理とフレームワークの各タイプを比較対照する



対象試験範囲

5.1さまざまな制御タイプを比較対照することができる。

5.2組織のセキュリティ体制に影響を及ぼす適用される規制、標準、フレームワークの重要性について説明できる。

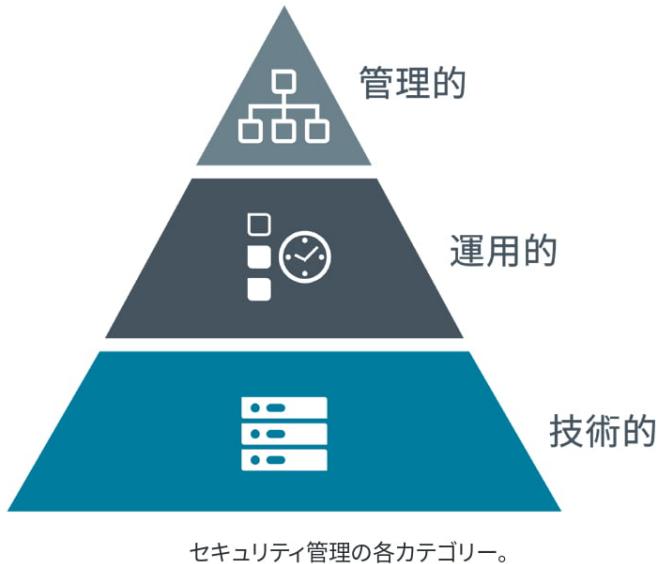
情報セキュリティとサイバーセキュリティは、セキュリティ管理を実行することで保証されます。あなたは情報セキュリティのプロフェッショナルとして、セキュリティ管理の各タイプを比較できなければなりません。また、管理の選択と構成に対してフレームワークがどう影響を及ぼすかを説明できる必要があります。セキュリティ管理の基本的なタイプを識別し、主要なフレームワークや法令がコンプライアンスをどう推進するかを突き止めることで、特定のシナリオに最も適した管理をよりよく選択・実行できるようになります。

セキュリティ管理のカテゴリ

情報セキュリティとサイバーセキュリティの保証は通常、ビジネスリスク管理のプロセス全体の中で行われると考えられています。多くの場合、サイバーセキュリティ機能の実行はIT部門の責任です。ビジネスニーズ全体を満たすためにITサービスがどう統制されるべきかについては、多くの異なる考え方があります。組織の中には、ITサービスのフレームワークを開発して、ITおよびサイバーセキュリティの実行に向けたベストプラクティスのガイドを提供したところもあります。それらのフレームワークは会社のポリシーを形作り、理想的に実施されるべき手順、アクティビティ、および技術のチェックリストを提供することができます。そうした手順、アクティビティ、およびツールをセキュリティ管理（制御）と総称することができます。

セキュリティ制御は、システムないしデータ資産に、機密性、完全性、可用性、および否認防止の特性を与えることを目的としたものです。制御は3つの広いカテゴリに大別され、それぞれが制御の実行方法を示しています。

- **技術的**—この制御はシステム（ハードウェア、ソフトウェア、またはファームウェア）として実行されます。一例を挙げると、ファイアウォール、アンチウイルスソフトウェア、およびOSアクセス制御モデルは技術的制御です。技術的制御は論理的制御とも呼ばれます。
- **運用的**—この制御は主に、システムではなく人によって実行されます。例えば、警備員やトレーニングプログラムは、技術的制御というより運用的制御です。
- **管理的**—この制御は情報システムを監督するものです。例として、リスクの識別や、他のセキュリティ管理の評価と選択を可能にするツールが挙げられます。



セキュリティ管理の各カテゴリー。

これはより複雑なスキームを使用していますが、国立標準技術研究所(NIST)がセキュリティ管理をどのように分類しているかを認識するのは有益です(nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)。

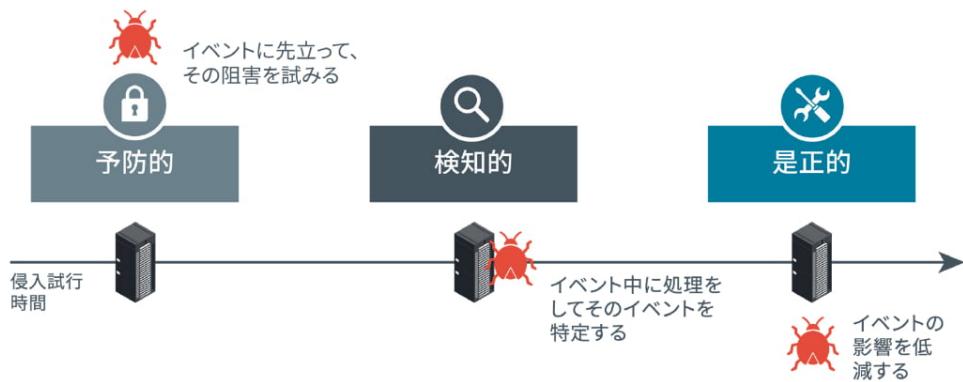
セキュリティ管理の機能タイプ

セキュリティ管理（制御）は、その目標や実施する機能ごとにタイプ分けすることもできます。

- **予防的**—この制御は、攻撃が成功する可能性を除去または低減するために機能します。予防的制御は、攻撃が発生する前に実行します。ファイアウォールやファイルシステムオブジェクト上で構成されている**アクセス制御リスト(ACL)**は、予防的制御です。マルウェア対策ソフトウェアも、悪意があると識別されたプロセスの実行を防ぐことで、予防的管理として機能します。指令書や標準運用手順(SOP)は、予防的制御の経営管理バージョンとして捉えることができます。
- **検知的**—この制御ではアクセスの予防や抑止は不可能ですが、侵入の試みや成功した侵入を識別・記録することができます。検知的制御は、攻撃の進行中に実行します。検知的制御の好例の1つにログがあります。
- **是正的**—この制御は、侵入イベントの影響を除去または低減します。是正的制御は攻撃後に用います。その好例の1つに、侵入中にダメージを受けたデータを修復できるバックアップシステムがあります。別の例として、攻撃中に悪用される脆弱性を除去するパッチ管理システムがあります。

ほとんどの制御は予防的、検知的、是正的といった機能別に分類されますが、それ以外の場合を定義するために用いられるその他のタイプもあります。

- **物理的**—アラーム、ゲートウェイ、ロック、照明、防犯カメラ、警備員など、施設やハードウェアへのアクセスを抑止および検知するための制御は、しばしば別のものとして分類されます。
- **抑止的**—この制御は、アクセスを物理的または論理的に防止できませんが、脅威アクターによる侵入の試みを心理的に防ぎます。これには、無断立入や侵入に対する罰則を記した掲示や警告が含まれるでしょう。
- **補完的**—この制御はセキュリティ標準の推奨に応じて、主たる管理の代替として機能し、同レベル（またはより高いレベル）の保護を提供するものの、異なる手段や技術を用いるものです。



その他の管理機能の種類:

物理的

抑止的

補完的

セキュリティ管理の各機能タイプ。(画像提供: © 123RF.com)

NISTサイバーセキュリティフレームワーク

サイバーセキュリティフレームワーク(CSF)は、リスクを軽減するために実施されるアクティビティと目標のリストです。フレームワークを用いることで、組織は現在のサイバーセキュリティ能力の客観的なステートメントを作成したり、目標とする能力レベルを設定したり、その目標の達成に向けた投資の優先順位をつけたりすることができます。これは内部のリスク管理手順を構造化するという点で価値あるものであり、外部向けに立証可能な規則遵守のステートメントを提供します。また、組織がセキュリティプログラムを一から構築する手間を省いたり、重要なセキュリティコンセプトを含まない基礎の上にプログラムを構築しないようにするという点でも、フレームワークは重要です。

さまざまなフレームワークが存在していますが、その1つ1つはサイバーセキュリティのアクティビティと管理をわずかに異なる形で分類しています。それらのフレームワークは、特定の業界の特定の規制に対処することを目的としていないという点で、規制に関するものではありませんが、ITセキュリティガバナンス全般の「ベストプラクティス」を示しています。歴史的に見て、ほとんどの組織はある特定のフレームワークを選択していますが、複数のフレームワークを組み合わせて使用している組織もあります。

ほとんどのフレームワークは国際的な対象者のために開発されていますが、国内の対象者に焦点を当てたものもあります。フレームワークのほとんどは認証プログラムと結びついており、スタッフやコンサルタントがその手法を正しく適用できていることを示します。

米国国立標準技術研究所(NIST)のサイバーセキュリティフレームワーク(CSF)は、ITガバナンスの分野に比較的最近追加されたものであり、ITサービスの提供全般ではなく、ITセキュリティにのみ焦点を当てているという点で、他のフレームワークと異なっています(csrc.nist.gov/projects/risk-management/rmf-overview)。これはアメリカの対象者向けに開発されたものであり、アメリカ政府にもいくらか焦点を当てていますが、その推奨事項は他の国や別種の組織向けに適合させることができます。

CSFに先立つ存在として、NISTのリスク管理フレームワーク(RMF)があります。CSFが企業向けの実践的なサイバーセキュリティに焦点を当てている一方、RMFはより規範的なものであり、連邦機関による利用を主な目的にしています(csrc.nist.gov/projects/risk-management/rmf-overview)。

NISTはサイバーセキュリティとリスクのフレームワークだけでなく、連邦情報処理標準(FIPS)に加え、特別刊行物と呼ばれる勧告ガイドの発行も担当しています(csrc.nist.gov/publications/sp)。CompTIA Security+でカバーされている標準や技術の多くは、それらの文書の中で論じられています。

ISOおよびクラウドフレームワーク

国際標準化機構(ISO) 27K

国際標準化機構(ISO)は国際電気標準会議(IEC)と共同でサイバーセキュリティのフレームワークを開発しました。このフレームワークは2005年に策定され、2013年に修正が行われています。NISTのフレームワークと違い、ISO 27001情報セキュリティ管理標準は購入する必要があります(iso.org/standard/54534.html)。ISO 27001は、情報セキュリティ標準関連の27000 (27K)シリーズ全体の一部です。それらの中で、27002はセキュリティ管理、27017と27018はクラウドセキュリティ、そして27701は個人データとプライバシーを対象にしています。

ISO 31K

ISO 21Kがサイバーセキュリティのフレームワークであるのに対し、ISO 31K (iso.org/iso-31000-risk-management.html)はエンタープライズリスク管理(ERM)全体のフレームワークです。ERMは財務、顧客サービス、競争、および法的責任の要素を含めることで、サイバーセキュリティを越えたリスクと機会を検討するものです。ISO 31Kは、リスク評価を行なうベストプラクティスを定めています。

クラウドセキュリティアライアンス

非営利組織クラウドセキュリティアライアンス(CSA)は、クラウドサービスプロバイダー(CSP)がセキュアなクラウドプラットフォームを構築してデリバリーするのを支援する、さまざまなリソースを提供しています。そうしたリソースは、クラウドサービスの評価と選択を行うクラウドコンシューマーにとっても有益です。

- セキュリティガイダンス(cloudsecurityalliance.org/research/guidance)—クラウド環境に独自の課題と、オンプレミス管理をそれに適合させる方法を分析する、ベストプラクティスの要約です。
- エンタープライズリファレンスアーキテクチャ(ea.cloudsecurityalliance.org)—CSPがクラウドソリューションを構築する際に使用する、ベストプラクティスの手法とツールです。そうしたソリューションは、リスク管理およびインフラストラクチャ、アプリケーション、そしてプレゼンテーションサービスなど、多数の領域に分かれます。
- クラウドコントロールマトリックス(cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix)—CSPが実行すべき特定の管理や評価のガイドラインを列挙しています。このマトリックスはCSPが満たすべきセキュリティ能力のベースラインレベルを提供するものであり、クラウドコンシューマーにとってはクラウドの契約と合意のスタート地点として機能します。

証明業務基準書(SSAE)サービス組織統制(SOC)

証明業務基準書(SSAE)は、米国公認会計士協会(AICPA)が策定した監査基準です。そうした監査は、サービスプロバイダ（特にクラウドプロバイダだが、あらゆる種類のホスティングサービスやサードパーティーサービスを含む）が業務上の基準を満たしていることを、コンシューマーに保証するものです(aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html)。SSAE No.18（現在の基準）には、次に挙げるいくつかの報告書レベルがあります。

- サービス組織統制(SOC2)—サービスプロバイダーが実行している内部統制を評価し、顧客データを保存・処理する際に信託業務基準(TSC, Trusted Services Criteria)を遵守していることを保証します。TSCは、セキュリティ、機密性、完全性、可用性、およびプライバシーの各特性を対象としています。SOC2タイプI報告書はシステム設計を、タイプII報告書は6～12カ

月にわたるセキュリティ構造の継続的有効性を評価します。SOC2報告書は極めて詳細にわたりており、機密扱いが前提となっています。これらの情報は、監査人と規制機関、および重要なパートナーとのみ、秘密保持契約書(NDA)の条件の下で共有されなければなりません。

- SOC3—SOC2の遵守を証明する、簡略版の報告書です。SOC3報告書は自由に配布できます。

ベンチマークとセキュアな構成のガイド

フレームワークはITサービスをどう立案すべきかについて「俯瞰的な」視点をもたらしますが、詳細な実行ガイドとなることは通常ありません。システムレベルにおいて、サーバーやアプリケーションのデプロイ（展開）は、ベンチマークとセキュアな構成のガイドがカバーしています。

インターネットセキュリティセンター (CIS)

インターネットセキュリティセンター (ciscosity.org)はSANS Instituteが設立に参加した非営利組織で、有名な「The 20 CIS Controls」を刊行しています。CIS-RAM（リスク評価手法）を用いることで、セキュリティへの取り組みを全体的に評価できます(learn.ciscosity.org/cis-ram)。

CISはサイバーセキュリティのさまざまな要素に関するベンチマークの策定も行っています。一例を挙げると、**PCI DSS**、NIST 800-53、SOX、およびISO 27000といった、ITフレームワークやコンプライアンスプログラムの遵守に関するベンチマークがあります。また、Windows Desktop、Windows Server、macOS、Linux、Cisco、Webブラウザ、Webサーバー、データベースサーバー、電子メールサーバー、およびVMware ESXiなど、製品に焦点を当てたベンチマークもあります。CIS-CAT（構成アクセスツール）を、自動脆弱性スキャナと一緒に用いることで、それらのベンチマークに照らしてコンプライアンスをテストすることができます(ciscosity.org/cybersecurity-tools/cis-cat-pro/cis-cat-faq)。

OS/ネットワークアプライアンスプラットフォーム/ベンダー別ガイド

オペレーティングシステム(OS)ベストプラクティス構成は、クライアントワークステーション、認証サーバー、ネットワークスイッチ/ルーター/ファイアウォール、およびWeb/アプリケーションサーバーなど、コンピュータープラットフォームが定義された役割で動作する際に適用されるべき、設定とコントロールを列挙しています。

ほとんどのベンダーは、ネットワークアプライアンス、オペレーティングシステム、Webサーバー、アプリケーション/データベースサーバーのデプロイを構成・検証するためのガイド、テンプレート、ツールを提供しています。それら各デバイスのセキュリティ構成はベンダーごとだけでなく、デバイスまたはバージョンごとに異なっているでしょう。構成ガイドは（セットアップ/インストールガイド、ソフトウェアのダウンロードおよび更新と共に）ベンダーのサポートポータルにホストされていることもあれば、Webの検索エンジンを用いて簡単に見つけることができます。

また詳細なガイダンスを提供している組織もいくつかあり、ベンダーを限定しないデプロイをカバーすると共に、ベンダー製品のデプロイに関するサードパーティの評価とアドバイスを提供しています。CIS管理以外に、よく知られたソースとして次のものがあります。

- 国防総省サイバーエクスチェンジはセキュリティ技術実装ガイド(STIG)に加え、さまざまなソフトウェアおよびハードウェアソリューションの強化ガイドラインを提供しています(public.cyber.mil)。
- またNISTによるNational Checklist Program (NCP)は、さまざまなオペレーティングシステムやアプリケーション向けのチェックリストとガイドラインを提供しています(nvd.nist.gov/ncp/repository)。

アプリケーションサーバー

ほとんどのアプリケーションアーキテクチャは、クライアント/サーバーモデルを使用しています。これは、アプリケーションの一部がクライアントソフトウェアプログラムであり、サーバーアプリケーションのコードとは独立したハードウェア上にインストールして実行されることを意味します。クライアントはネットワークを介してサーバーとやり取りを行います。従って、攻撃はローカルクライアントのコード、サーバーアプリケーション、またはそれらをつなぐネットワークチャ

ネルに向けられることになります。アプリケーションはコーディングの問題だけでなく、プラットフォームの問題も考慮に入れる必要があります。クライアントアプリケーションは、潜在的に悪意のある他のソフトウェアと一緒に、コンピューター・ホストで実行します。クライアント上で実行するコードを信頼してはいけません。サーバーサイドのコードには、入力が想定通りであることを確認するルーチンを実装する必要があります。

Webサーバーアプリケーション

Webアプリケーションは特定のタイプのクライアント/サーバーアーキテクチャです。Webアプリケーションは既存の技術を活用することで、開発を簡素化しています。そうしたアプリケーションは市販のクライアント(Webブラウザ)と、標準化されたネットワークプロトコルおよびサーバー(HTTP/HTTPS)を使用します。アプリケーションの特定の機能は、クライアントおよびサーバー上で実行されるコードを用いて開発されます。また、Webアプリケーションが多層アーキテクチャを使用することもあり、サーバー部分はアプリケーションのロジックと、データの保存および検索に分割されます。現在のWebアプリケーションではマイクロサービスやサーバーレスなど、さらに分散化したアーキテクチャが使用されることもあります。

Open Web Application Security Project (OWASP)は非営利のオンラインコミュニティであり、Top 10 list of the most critical application security risks (重大なアプリケーションリスクのTop10リスト)など、セキュアなアプリケーション開発のリソースを刊行しています(owasp.org/www-project-top-ten)。また、Zed Attack ProxyやJuice Shop (わざと危険にしたWebアプリケーション)などのリソースを開発し、ペネトレーションテストやアプリケーションのセキュリティ問題の調査と理解をサポートしています。

規則、標準、および法令

国の法律/規則に関する要求事項や、業界固有の規則を遵守していることを実証するために、主要なフレームワーク、ベンチマーク、および構成のガイドが使われることもあります。デューデリジェンス（しかるべき注意）は、責任ある人物が自身の責務を果たすにあたり、怠慢でなかったことを意味する法律用語です。怠慢によって刑事上・民事上の責任が生じる場合もあります。多くの国で、情報管理における怠慢を罰する法律が制定されています。例えば米国では、**サーベインス・オクスリー法(SOX)**により、リスク評価、内部統制、および監査手順の実行が義務づけられています。コンピューターセキュリティ法(1987)は連邦機関に対し、機密情報を処理するコンピューターシステム向けのセキュリティポリシーを立案するよう求めています。2002年には、連邦政府機関が処理するデータのセキュリティを統制する、連邦情報セキュリティ管理法(FISMA)が導入されました。

! 特定のサイバーセキュリティ管理要件を有する規則もあれば、単に特定の業界のフレームワーク、または国際的なフレームワークによって示される、「ベストプラクティス」を義務づけるだけの規則もあります。規制者が1つの規則だけの使用を指定している場合、NISTやISO 27Kなど、さまざまな業界フレームワーク間でマッピングを行う必要があるかもしれません。逆に、フレームワークの使用がそのように義務づけられていないものの、強力かつ十分なセキュリティプログラムを実施していると、監査人が想定することもあります。

個人データおよび一般データ保護規則(GDPR)

サイバーセキュリティのデリューデリジェンスを対象とする各種の法律がある一方、情報セキュリティはプライバシーや個人データに影響を与えることから、その全体ないし一部に焦点を当てた法律もあります。プライバシーはセキュリティと個別の概念です。プライバシーは、個人情報の収集と処理が安全かつ公正であることを求めています。ヨーロッパ連合の**一般データ保護規則(GDPR)**などによって立法化された公正性とプライバシー権は、十分な説明を行い同意を得ること（インフォームドコンセント）なく、個人データの収集、処理、保管を行ってはならないことを意味します。インフォームドコンセントとは、データは言明された目的のためにのみ収集・処理されなければならないならず、その目的は法律用語でなく簡明な言葉でユーザーにはっきり説明されなければならない、という意味です。GDPR (ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr)はデータの対象者に対し、同意を取り下げ、自分に関するデータを検査、修正、および消去する権利を与えています。

国家、準州、または州の法律

コンプライアンス問題は、法律の制定主体が異なっているという事実のせいで複雑になっています。一例を挙げると、GDPRは米国のデータ対象者には適用されませんが、EU諸国の国民の個人データを収集または処理する米国企業には適用されます。米国には連邦法や州法に加え、米国の準州（プエルトリコ、アメリカ領バージン諸島、グアム、およびアメリカ領サモア）に適用される法体系があります。連邦法は、FISMAをはじめとする連邦機関向けの規則や、特定の産業に影響を及ぼす「縦割り型」の規則に焦点を当てがちです。後者の例として、金融機関を対象とする**グラム・リーチ・ブライリー法(GLBA)**や、医療保険の相互運用性と説明責任に関する法律(HIPAA)があります。

また一部の州では、GDPRによるアプローチと同様の、「水平型」の個人データ規則の導入が始まっています。現在注目を集めている州法の1つに、カリフォルニア州消費者プライバシー法(CCPA)があります(csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html)。



米国のプライバシー関連法律については、Varonisのブログに有益な概要が掲載されています (varonis.com/blog/us-privacy-laws)。

ペイメントカード業界データセキュリティ基準(PCI DSS)

コンプライアンス問題は、業界が義務づけている規則から生じる場合もあります。一例を挙げると、ペイメントカード業界データセキュリティ基準(PCI DSS)は、財務情報の安全な取り扱いと保管を定義しています(pcisecuritystandards.org/pci_security)。

レビュー アクティビティ：

セキュリティ管理とフレームワークの各タイプ

次の質問にお答えください。

- あなたはソーシャルネットワークサイトへのアクセスをブロックする、セキュアなWebゲートウェイを実装しました。あなたはこの種のセキュリティ管理をどのように分類しますか？
- ある企業が敷地の周囲に、動作検知型の投光照明器具を設置しました。このセキュリティ管理のクラスと機能は何ですか？
- ファイアウォールアプライアンスは、ポリシーに違反しているパケットを捕捉します。それはアクセス制御リストを自動的に更新し、そのソースIPからのその後のパケットをすべてブロックします。このセキュリティ管理が実行している2つの機能は何ですか？
- あるセキュリティ制御が運用型および補完型と説明された場合、その性質と機能について何を判断することができますか？
- ある企業が、セキュリティ管理の選択においてベストプラクティスに従っていることを確認しようとする場合、どのようなリソースがガイダンスとなりますか？

レッスン1

概要

カテゴリーや機能のタイプを使用して、セキュリティ制御を比較対照できる必要があります。また、セキュリティのポリシーと制御を選択し、それを検証するために、規則、フレームワーク、およびベンチマークがどのように使用されるかを説明できる必要があります。

セキュリティロールとセキュリティ管理を比較するためのガイドライン

組織におけるセキュリティ制御、フレームワーク、ベンチマークの利用を評価する際には、以下のガイドラインに従ってください。

- CIAトライアド（機密性、完全性、可用性）の重要性を強調する、セキュリティミッションの声明やそれを支援するポリシーを策定する。
- セキュリティの業務と責任がはっきり理解され、セキュリティへの影響が組織全体で評価・軽減されるように役割を振り分ける。
- 業務ユニット、部門、またはプロジェクトを立ち上げ、SOC、CSIRT、DevSecOpsなどのセキュリティ機能をサポートすることを検討する。
- 自分のビジネスにコンプライアンス上の要求事項を課している法律と業界規則を特定・評価する。
- コンプライアンス上の要求事項とビジネスニーズを満たすフレームワークを選択する。
- 現在導入されているセキュリティ制御のマトリックスを作成し、カテゴリーと機能を特定する。また現状に合わない機能について、追加の制御を導入することを検討する。
- 資産を開拓するベースラインとして、ベンチマーク、セキュアな構成のガイド、および開発のベストプラクティスを使用する。
- フレームワークの階層に照らしてセキュリティ能力を評価し、サイバーセキュリティ能力をさらに向上させ、全体的な情報セキュリティ保証を改善するための目標を特定する。

レッスン2

脅威アクターと脅威インテリジェンスを説明する

レッスン概要

セキュリティを効果的に評価するには、防御と攻撃両方を戦略的に説明できなくてはなりません。あなたの責任は主に資産を守ることにあると思われますが、そのためには脅威アクターの戦術、技術、手順を説明できなければなりません。また、脅威アクターのタイプと能力を区別できなくてはなりません。脅威の背景は進化し続けているため、脅威インテリジェンスやリサーチの信頼できる情報源を識別できなくてはなりません。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- 脅威アクターのタイプと攻撃ベクトルを説明する。
- 脅威インテリジェンスの情報源を説明する。

トピック2A

脅威アクターのタイプと攻撃ベクトルを説明する



対象試験範囲

1.5 さまざまな脅威アクター、ベクトル、インテリジェンスの情報源を説明することができる

脅威アクターのタイプごとに能力を分類し見極めることで、リスクをより効果的に評価し緩和できます。ネットワークの攻撃対象領域を評価したり、攻撃ベクトルをブロックするための制御をデプロイするには、脅威アクターがネットワークやシステムに侵入する際の手口を理解していることが必要不可欠です。

脆弱性、脅威、リスク

セキュリティの評価と監視の一環として、セキュリティチームは、システムがどのような方法で攻撃を受ける可能性があるかを識別する必要があります。こういった場合、脆弱性、脅威、リスクを評価します。

- **脆弱性**とは、誤ってトリガーされたり意図的にエクスプロイトされた場合に、セキュリティ侵害の原因となり得る弱点のことです。脆弱性の例に含まれるのは、不適切に設定またはインストールされたハードウェアやソフトウェア、ソフトウェアパッチやファームウェアパッチの適用やテストの遅れ、テストされていないソフトウェアパッチやファームウェアパッチ、ソフトウェアや通信プロトコルの誤った使用、設計に不備のあるネットワークアーキテクチャ、不十分な物理的セキュリティ、安全でないパスワードの使用、ユーザーの入力を確認しないと言ったソフトウェアやオペレーティングシステムの設計上の欠陥などです。
- **脅威**とは、人や物が脆弱性を悪用したりセキュリティを侵害する可能性のことです。脅威は、**意図的**である場合も**意図的でない**場合もあります。脅威をもたらす人または物を脅威アクターまたは脅威エージェントと呼びます。悪意のある脅威アクターが使用する経路やツールを、脅威ベクトルと呼びます。
- **リスク**とは、脅威アクターが脆弱性を悪用する可能性と影響（または結果）のことです。リスクを評価するためには、脆弱性を特定し、それが脅威によって悪用される可能性と、悪用が成功した場合の影響を評価します。



脆弱性、脅威、およびリスクの関連性。



リスク管理に関する定義と詳細情報はNISTのSP 800-30に含まれます
(nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)。

脅威アクターの属性

歴史的に見て、サイバーセキュリティ技術は、ウイルスまたはルートキット、トロイの木馬、ボットネット、特定のソフトウェアの脆弱性など、既知の「静的」脅威を識別することに専ら依存していました。これは、自動化されたソフトウェアを使ってこれらの脅威のタイプを識別しスキャンするという比較的簡単な方法でした。残念なことに、敵対者は、このタイプのシグネチャベースのスキャンを迂回する手段を開発しました。

精巧な特性を持つ現代のサイバーセキュリティ脅威に対抗するには、挙動を説明し分析できなくてはなりません。分析の際は、場所、意図、能力の観点から脅威アクターの属性を識別します。

内部/外部

外部の脅威アクターまたはエージェントとは、対象となるシステムのアカウントやアクセス権を保持していない人のことです。悪意のある外部脅威は、マルウェアやソーシャルエンジニアリングを使って、セキュリティシステムに侵入する必要があります。外部脅威アクターは、遠隔操作やオンプレミス（例えば企業の本社に侵入するなど）で攻撃を行います。外部と定義されるのは、攻撃方法ではなく脅威アクターです。

逆に、内部（またはインサイダー）脅威アクターは、システムでアクセス許可を得ている人のことです。これは、一般的には従業員のことですが、インサイダーの脅威は、契約社員やビジネスパートナーから発生する場合もあります。

意図/動機

意図は、脅威アクターが攻撃を行うことによって実現したいことを表し、動機は、脅威アクターが攻撃を行う理由を表します。悪意のある脅威アクターは、例えば欲望、好奇心、何らかの不満などの感情が動機となり得ます。意図とは、システムを破壊し混乱させたり、何かを盗み出そうとすることです。具体的に組織がどの程度標的にされているかによって、脅威は、構造的または非構造的（すなわち標的型と日和見型）として特徴づけられます。例えば、顧客の財務データを盗もうと試みる犯罪組織は構造的、標的型脅威であり、「I Love You」メールワームの類を送るスクリプトキディは非構造的、日和見型脅威です。

悪意のある意図と動機は、過失による、または意図しない脅威アクターやエージェントと対照を成すものです。意図しない脅威アクターとは、事故、見落とし、および他のミスを指します。

巧妙さ/能力およびリソース/資金

様々な敵対者の巧妙さと所有するリソース/資金のレベルについても検討する必要があります。能力とは、新しいエクスプロイトのテクニックとツールを作成する脅威アクターの能力を指します。最も能力の低い脅威アクターは、WebやダークWeb上で幅広く入手できるコモディティ化した攻撃ツールを使用します。より有能なアクターは、オペレーティングシステム、アプリケーションソフトウェア、組み込み式制御システム内のゼロデイエクスプロイトを活用することができます。最高レベルの脅威アクターは、例えば非サイバーツール（政治的または軍事的資産）を利用する可能性があります。能力は相当な予算があって初めて成り立つものです。巧妙な脅威アクターグループは、カスタマイズされた攻撃ツール、優れた戦略、設計者、プログラマー、ハッカー、およびソーシャルエンジニアなどのリソースを手に入れる必要があります。最も能力の高い脅威アクターグループは、国家や犯罪シンジケートから資金を受け取ります。

ハッカー、スクリプトキディ、ハクティビスト

意図と能力を正確に評価するには、様々なカテゴリーの脅威アクターの識別が有益です。

ハッカー

ハッカーとは権限の無い、または承認されていない手段で、コンピューターシステムへのアクセス権を取得するスキルを持つ人物を指します。本来、ハッカーとは、コンピュータープログラミングやコンピューターシステム管理に秀でたユーザーを指す中立的な用語でした。システムに対するハッキングは、技術的スキルと創造性があることの表れであり、次第に違法または悪意のあるシステム侵害に結び付けられるようになりました。用語**ブラックハット**（権限がない場合）と、**ホワイトハット**（権限がある場合）は動機を区別する際に使われます。もちろん、ブラックとホワイトの間には様々な濃淡のグレーが存在します。**グレーハットハッカー**（ある程度権限がある場合）は、所有者に承認を求めずに、製品またはネットワークの脆弱性の発見を試みますが、発見した脆弱性のエクスプロイトを試みることはできません。グレーハットは、任意の報酬（バグバウンティ）を求める場合がありますが、強要目的でエクスプロイトを行うことはありません。個人のシステムやプライエタリシステムのペネトレーションテストを行う場合、ホワイトハッカーは常に認可を求めます。

スクリプトキディ

スクリプトキディとは、必ずしもハッカーツールの動作を理解せず、また新しい攻撃を作り上げることなく、ツールを使用する人を指します。スクリプトキディは注目されたい、あるいは技術的な能力を証明したいというだけで、特定のターゲットや妥当な目的を持たない場合があります。

ハッカーチームとハクティビスト

ハッカーはこれまで、わずかなリソースや資金で単独活動をしているというイメージがありました。こういった「一匹狼的なハッカー」も注視すべき脅威であり続けますが、現在の脅威アクターの多くはチームまたはグループの一員として活動しているようです。チームで協力して取り組むことで、こういったタイプの脅威アクターは、精巧なツールと新しい戦略を生み出すことができます。

Anonymous、WikiLeaks、またはLulzSecなどのハクティビストグループは、サイバー兵器を使用して政治的アジェンダを実行します。**ハクティビスト**は、機密情報の入手やパブリックドメインへの公開、DoS攻撃の実行、ウェブサイトの書き換えなどを企てます。政治、メディア、金融関連の団体や企業がリスクに晒される可能性が最も高いのですが、環境保護団体や動物愛護団体が、様々な業界の企業をターゲットにする可能性があります。

国家的アクターとAPT攻撃

多くの国家がサイバーセキュリティ関連の専門技術を開発しており、サーバー兵器を使って軍事的目的や商業的目的を達成します。セキュリティ関連企業であるMandiantの中国サイバースパイ行為ユニット(fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)に関するAPT1レポートは、用語の形成や最新のサイバー攻撃ライフサイクルの理解に影響を及ぼしています。**APT (Advanced Persistent Threat、高度標的型脅威)** 攻撃という用語は、新しいタイプのサイバー敵対者が取る行動を理解するために作られた造語です。APTとは、システムがウイルスやトロイの木馬に感染するという観点から考えるのではなく、アクセス権を取得し維持するために、様々なツールや技術を使ってネットワークセキュリティを侵害する敵対者の発展的能力を指します。

国家的アクターは、特にエネルギー・医療関係のネットワークシステムに対して多くの攻撃を行ってきました。国家的アクターの目的は主に、スパイ行為を行ったり戦略的に優位な立場に立つことですが、北朝鮮をはじめとする国家が、純粋に商業的な利益を得るために企業を標的にすることはよく知られています。