CISSP®

Certified Information
Systems Security Profession

ISC2 Certification

CISSP 8ドメインガイドブック

ISC2™

Your Future. Secured.

はじめに

情報セキュリティ専門家には幅広い知識とスキルが必要とされているだけではなく、それらを体系的に理解し、あらゆる場面で活かせることが求められています。その基準の一つとして国際的に認められているのが、その一つの基準が、ISC2 の CBK(Common Body of Knowledge：共通知識分野)です。CBK は、それを理解していることを証明する資格である CISSP と共に、多くの国や企業、組織で認められたグローバルな内容として注目されています。

本書では CBK に基づく CISSP オフシャルセミナーで学習する内容について紹介します。

ISC2 とは

ISC2 (International Information Systems Security Certification Consortium：アイエスシー・トゥー)は、安全で安心できるサイバーセキュリティの世界を実現することを目的とした国際的な非営利団体です。高い評価を得ている CISSP(Certified Information Systems Security Professional)を始めとした各種資格を提供することにより、セキュリティに対して ISC2 は網羅的、そして計画的にアプローチしています。サイバー・情報・ソフトウェア・インフラストラクチャセキュリティの専門家から成り立つ 16 万人を超える資格保持者は、その資格によって他との差別化を図るとともに、業界の発展に貢献しています。

ISC2 は、情報セキュリティの共通言語となる CBK を策定し、情報セキュリティ人材評価におけるゴールドスタンダードとなる認証制度を開発、提供しています。あわせて、世界中の情報セキュリティ専門家を教育、認定することによって、CBK をグローバルでより良いものとし続けています。

CISSP とは

CISSP(Certified Information Systems Security Professional)は、ISC2 が認定を行うベンダーフリー・カントリーフリーの情報セキュリティの専門家資格です。CISSP には、情報セキュリティにおける理論やメカニズムを理解するだけでなく、その知識を体系的かつ構造的に整理し、状況に応じた適切な判断を行うための、合理的かつ実践的な「知識」と「理解度」が求められます。

資格取得のためには業務経験が必要です。試験合格後の認定登録手続きで業務経験を明記した職務経歴書とエンドースメント(推薦状)を提出し、それを証明する必要があります。認定期間は 3 年間となっており、3 年毎の認定継続要件をパスすることが必要です。

ANSI(米国規格協会)より、ISO/IEC 17024 の認証を受けた厳正な資格開発、運用、運営、維持に加え、米国国防総省のキャリアパスにおいて取得が義務付けられている資格の一つにも認定されており、CISSP は知識と実務経験を兼ね備えた、常に最新の知識をもった情報セキュリティプロフェッショナルであることを証明します。

CBK とは

CBK は、ISC2 CBK 委員会が、CISSP 認定試験の作成に先駆け、情報セキュリティ専門家が理解すべき知識を国際規模で収集し、分野(ドメイン)別に体系的にまとめたものです。

情報セキュリティの共通言語である CBK をベースとすることで、CISSP をはじめとする情報セキュリティ専門家は、地域や専門分野を問わず、円滑なコミュニケーションが可能となります。CBK は毎年、多くの世界各国のセキュリティのプロフェッショナルへの定期的なヒアリング調査を行い、「最新の知識」として更新、維持されています。その中で CISSP に必要とされるものをまとめたのが CISSP CBK 8 ドメインであり、CISSP 認定試験の範囲として活用されています。

CISSP の CBK は、2021 年 5 月にコンテンツを更新し、新たな知識が追加されました。

CISSP CBK を理解するためのエッセンス

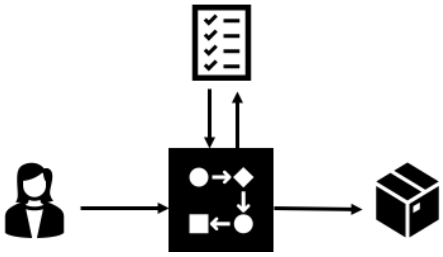
CISSP CBK を理解しようとした時に、最初に驚かれるのはその範囲の広さです。

リスクマネジメントや暗号、ネットワークセキュリティだけではなく、ソフトウェア開発やコンピュータシステムのアーキテクチャなどもその範囲に入っているためです。また、これらは独立した知識として身につければ良いわけではなく、関連性をもって体系的に理解する必要があるということです。

一方で、体系的に理解するということは、原則を理解していれば、それをベースにして知識を増やしていけば良いということにもなります。原則を理解してしまえば、新たな知識はそこに関連づけられ、適切な理解ができるようになるということです。

たとえば、ゼロトラストアーキテクチャを理解する際にも、CISSP CBK の「アイデンティティとアクセスの管理」ドメインにある原則をベースにすることで適切な理解が促されます。

アクセス制御の基本的な概念として「強制アクセス制御(MAC)」があります。これは、だれか(サブジェクト)がなにか(オブジェクト)にアクセスする際に、必ず仲介するプログラムがあり、このプログラムはポリシーを必ず参照して、アクセスの可否を決定します。

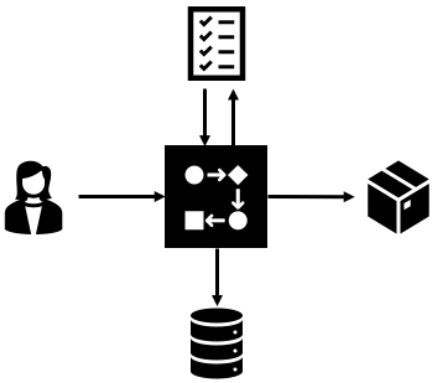


この仕組みを理解していれば、ゼロトラストアーキテクチャのポリシー強制の意味がわかるようになります。そして、このポリシーが動的に作成され、反映されていることがゼロトラストアーキテクチャでいうところの動的ポリシー制御であることも理解できます。

さらにこの強制アクセス制御のモデルを発展させると、説明責任を果たすための仕組みや、完全性確保のための仕組みが理解できるようになります。必ず仲介しなくてはならないプログラムが、すべてのやり取りを記録することによって、ユーザやエンティティの振る舞いを記録することができるようになり、その挙動を分析することで UEBA(ユーザとエンティティのふるまい分析)のためのデータを作ることができるようになります。これらのロギングについては「セキュリティの運用」ドメインで原則を理解したり、これをソフトウェアで実現することを考えれば「ソフトウェア開発セキュリティ」ドメインでのセキュリティ要件での原則を当てはめることもできます。

これまでのことをまとめると、以下のような図になるのですが、これは「セキュリティアーキテクチャとエンジニアリング」ドメインで学ぶ「クラークウィルソン」というセキュリティモデルであり、完全性確保のための仕組みであることが理解できます。アクセス制御を通して、機密性の確保だけではなく、完全性の確保を実現できることも同時に理解できます。

このクラークウィルソンモデルは、別名でリファレンスアーキテクチャといい、これが現代の OS に採用されているセキュアカーネルの基本的な考え方であることも理解でき、さらにこのカーネルが取得するイベントログが、最近では EDR のシグナルとして活用されていることも理解できるようになります。



サブジェクトの信頼性(トラスト)については「アイデンティティとアクセスの管理」ドメインで、オブジェクトの信頼性については「資産のセキュリティ」ドメインで学びます。リスクに応じたポリシーの変更については「セキュリティとリスクマネジメント」ドメイン、ログの取得と活用については「セキュリティの運用」ドメインで学びます。もちろんこの原則は CISSP CBK が策定され始めた当初からあるものです。

このように、ゼロトラストアーキテクチャという比較的新しいキーワードでさえ、CISSP CBK を適切に理解していれば、セキュリティ専門家が本来求めていたものであり、それを実現するための技術が現実的なコストで利用できるようになっただけであることを理解することができます。

CISSP CBK をベースに考えることによって、セキュリティに関連するキーワードはすべて理解できるのではないかと考えています。

CISSP ホルダーにとって必要なのはいつも理想的な対策を考え、それが技術的に、そして現実的なコストで実現できるかどうかを考えることです。リスクが高いからそれを実行しないという考え方は CISSP らしい考えとは言えません。安全にクラウドサービスを使うためには、どのような対策を実施すれば良いのか、それを理解してもらうためにはどのような説明をすれば良いのかを考えるのがプロフェッショナルとしての CISSP らしい考え方ということになります。危険だからやらない、リスクが高いから諦めるというのは、プロフェッショナルの考え方としては適切ではないということです。

CISSP CBK を理解し、CISSP 認定試験に合格するためには、いつもイネーブラーとしての意識を持っておくことが重要です。ビジネスや IT をサポートし、実現するための手段として知識やスキルを活かすことができるように、CISSP のそれぞれのドメインを学習してください。

目次

CISSP CBK の8ドメイン

CISSP CBK は以下の 8 ドメインで構成されています。

1．セキュリティとリスクマネジメント
2．資産のセキュリティ
3．セキュリティアーキテクチャとエンジニアリング
4．通信とネットワークのセキュリティ
5．アイデンティティとアクセスの管理(IAM)
6．セキュリティの評価とテスト
7．セキュリティの運用
8．ソフトウェア開発セキュリティ

CISSP CBK 8 ドメインはそれぞれが独立した知識として提供されているのではなく、それぞれのドメインで提示された知識やスキルを組み合わせることで、セキュリティ計画や具体的な対策に役立てることができるようになっています。

これは CISSP の認定試験においても同様で、単一のドメインの知識を有していることを判断するのではなく、複数のドメインの知識を活用して、課題に対応していくことが求められています。

8 ドメインの共通的な考え方は組織のガバナンスにあります。ガバナンスとは、組織全体の把握をし、適宜修正を行いながら、組織の目的や目標を効率に達成するためのプロセスです。ベストプラクティスを理解し、それを実践するだけではなく、そのベストプラクティスが自らの組織に合ったものであるかどうかを判断し、もしも適切なものでないとした時に組織に合わせた形に修正(テーラリング)できるようにしなければなりません。

CISSP の 8 ドメインを通して、このような情報セキュリティの推進に必要なコンセプトを理解し、それらを実践するための技術的な知識を網羅的かつ体系的を身につけていただきたいと考えています。

1．セキュリティとリスクマネジメント

「セキュリティとリスクマネジメント」のドメインでは、情報セキュリティ専門家としての姿勢と役割に関する知識とスキルが求められます。

情報セキュリティ専門家として第一に重要なことは倫理的な行動です。

情報セキュリティ専門家は多くの機密情報に触れる機会も多く、その扱いについても厳正な対応を求められます。また、専門家として意見を求められた際に、ただ不安だけを煽るような発言をするようなことがあってはいけません。情報セキュリティ専門家は組織が成し遂げようとする目的に対して協力的かつ適切な助言や対応を行うために職業倫理について理解が必要です。

情報セキュリティはリスクマネジメント、リスクガバナンスの一つの分野です。

将来起こりうる事故やトラブルに備え、それが発生しないように、また発生した際の被害を受容できる範囲内に収めるために、セキュリティ対策を計画し、実施します。そして、その計画が組織の目標や目的に沿ったものであるかを判断し、適宜修正をしていくためのモニタリングや評価の基盤も構築しておかなければなりません。

ガバナンスの範囲は組織内にとどまらず、サプライチェーンにも適用されるべきですし、その内容はセキュリティ、コンプライアンス、プライバシーと幅広くなっています。

それぞれを個別の課題として捉えるのではなく、包括的かつ一元的に管理するための知識とスキルが求められます。

求められるスキルと関連するキーワード

1.1　職業倫理を理解し、遵守し、促進する
- » 職業倫理、組織的倫理規定
- » ISC2 倫理規約

1.2　セキュリティの概念を理解し、適用する
- » 機密性、完全性、可用性、信頼性、否認防止

1.3　セキュリティガバナンスの原則を評価し、適用する
- » セキュリティ機能と事業戦略、目標、ミッション、目的との合致
- » 組織におけるプロセス(買収、会社分割、ガバナンス委員会等)
- » 組織における役割と責任
- » セキュリティコントロールフレームワーク
- » デューケア/デューデリジェンス

1.4　コンプライアンスおよびその他の要件を決定する
- » 契約、法律要件、業界標準、規制要件
- » プライバシー要件

1.5　情報セキュリティに関連する法的および規制上の問題を総合的に理解する
- » サイバー犯罪とデータ漏洩
- » ライセンス供与および知的財産(IP)における要件
- » 輸入/輸出管理
- » 越境データフロー
- » プライバシー

1.6　調査の各種類(すなわち、行政、刑事、民事、規制、業界標準)の要件を理解する

1.7　文書化されたセキュリティポリシー、スタンダード、プロシージャ、およびガイドラインを策定し、実施する

1.8　事業継続(BC)要件を特定し、分析し、優先順位付けする

» 事業インパクト分析
» 範囲と計画を作成し、文書化する

1.9 人員のセキュリティポリシーとプロシージャに貢献し、実施する
» 雇用志願者の審査と採用
» 雇用契約とポリシー
» 雇用の採用、異動、終了のプロセス
» ベンダー、コンサルタント、委託の合意と管理
» コンプライアンスポリシーの要件
» プライバシーポリシーの要件

1.10 リスクマネジメントの概念を理解し、適用する
» 脅威と脆弱性の特定
» リスク評価/分析
» リスクレスポンス
» 対策の選択と導入
» 適用管理策の形式(防止的、検知的、是正的等)
» 管理の評価(セキュリティとプライバシー)
» 監視と測定
» 報告
» 継続的改善(リスク成熟度モデリング等)
» リスクフレームワーク

1.11 脅威モデリングの概念と手法を理解し、適用する

1.12 サプライチェーンリスク管理
» ハードウェア、ソフトウェア、およびサービスに関わるリスク
» サードパーティの評価および監視
» 最低限のセキュリティ要件
» サービスレベル要件

1.13 セキュリティ意識、教育、トレーニングプログラムを確立し、管理する
» 意識向上とトレーニングの方法と技術(ソーシャルエンジニアリング、フィッシング、セキュリティチャンピオン、ゲーミフィケーション等)
» 内容の定期的なレビュー
» プログラム有効性評価

2．資産のセキュリティ

「資産のセキュリティ」ドメインでは、情報のライフサイクル全体を通じた資産の入手、取り扱い、保護についての知識とスキルが求められます。情報分類と資産の取り扱いをベースに、情報、システム、ビジネス・プロセスなどの所有権についての理解も求められます。

デジタルトランスフォーメーションの推進による情報や資産のデジタル化に伴い、一般的な企業の機密管理だけではなく、プライバシーに配慮した情報の管理も求められるようになりました。プライバシーについてはビジネスニーズに応じて、コンプライアンス的な観点から国際的な課題を理解し、利用範囲や手段についても適切に把握しておく必要があります。

CISSP には、適切なデータセキュリティ対策を選択できることが求められるため、ライフサイクルに従って取り扱い要件を理解しなければいけません。特に情報分類にともなうラベリングの実践や法的な要求に伴う暗号化や廃棄手法などの要件を評価し、ポリシーや管理手順を策定できる知識とスキルが求められます。

求められるスキルと関連するキーワード

2.1 情報と資産を特定し、分類する
- » データの分類
- » 資産の分類

2.2 情報と資産の取り扱い要件を確立する

2.3 リソースを安全にプロビジョニングする
- » 情報と資産の所有権
- » 資産インベントリ(有形、無形等)
- » 資産運用管理

2.4 データライフサイクルを管理する
- » データの役割(すなわち、所有者、管理者、保管者、処理者、ユーザ/対象者)
- » データの収集
- » データの場所
- » データの維持
- » データの保持
- » データの復元
- » データの破棄

2.5 適切な資産保持を確実にする(エンド・オブ・ライフ(EOL)、エンド・オブ・サポート(EOS)等)

2.6 データセキュリティ管理とコンプライアンス要件を決定する
- » データの状態(使用中、転送中、保管中等)
- » 範囲とテーラリング
- » スタンダードの選定
- » データ保護の方法(デジタル著作権管理(DRM)、データ損失防止(DLP))クラウドアクセスセキュリティブローカー(CASB)等)

3．セキュリティアーキテクチャとエンジニアリング

「セキュリティアーキテクチャとエンジニアリング」ドメインでは、セキュリティ計画に必要な原則の理解と、それを実践するための技術的な知識やスキルが求められます。このドメインの知識範囲は広く、システムの設計・構築をもとにしたセキュリティ要件の定義、それに必要な暗号システムなどを中心としたセキュリティ技術の理解、論理的セキュリティをサポートする物理的なセキュリティについてもカバーします。

このドメインを理解するために必要なことは、情報システムがどのように設計され、構築されているかのプロセスを理解することです。情報システムの形態はさまざまで、デバイス、サービス(サーバ)、ストレージ、ネットワークなどのエンティティの組み合わせによって求められる機能を提供しています。もちろんユーザや管理者など、人も関わることでさらに複雑な構造になっています。それぞれのシステムの構成を理解し、潜在的な弱さを理解することで、ベースラインとなるセキュリティ対策を計画することができるようになります。

セキュリティ対策を実践するには、その原則を理解しなくてはいけません。

多くのベストプラクティスは想定された環境に依存するものとなっていて、ユニバーサルであるとはいえません。環境に応じた対策を計画し、実践するためには、情報セキュリティの原則を理解する必要があります。たとえば、最小権限(Least Privilege)という原則を理解することで、アクセス制御の認可において、権限の粒度を設定することができるようになります。管理者とユーザという大きな分け方ではなく、誰が何をすることができるのかという実践的なものとすることが可能になります。

暗号システムはいまや情報の秘匿のためだけに使われるものではありません。

鍵を持っているということが、その情報やシステムに対する権限を有するという考え方のもとに、アクセス制御や否認防止に利用することもできます。もちろんこれらの鍵の利用状況をユーザやエンティティの振る舞いとしてモニタリングに利用することもできるようになりました。暗号を適切に理解することが組織のポリシーを実現するための必須知識となっているのです。

また、論理セキュリティをサポートするものとして、物理セキュリティがあります。

CISSP には、物理セキュリティの専門家と意見交換をしながら、お互いを補完するような提案ができる知識とスキルが求められます。

求められるスキルと関連するキーワード

3.1 安全な設計原則を使用してエンジニアリングプロセスを調査し、導入し、管理する
- » 脅威モデリング
- » 最小特権、職務の分離
- » 多層防御
- » フェイルセーフ、フェイルセキュア
- » システムやサービスの単純化
- » ゼロトラスト
- » ″Trust but verify″
- » 共同責任モデル
- » プライバシー・バイ・デザイン

3.2 セキュリティモデルの基本概念を理解する
- » 状態マシン、格子モデル
- » Bell-LaPadula、Biba、Clerk Wiilson

3.3 システムセキュリティ要件に基づき管理策を選択する

3.4 情報システムのセキュリティ能力を理解する
» メモリ保護
» Trusted Platform Module (TPM)
» 暗号化／復号
3.5 セキュリティアーキテクチャ、設計、およびソリューション要素の脆弱性を評価し軽減する
» クライアントベースシステム
» サーバーベースシステム
» データベースシステム
» 暗号化システム
» 産業制御システム(ICS)
» クラウドベースシステム(サービスとしてのソフトウェア(SaaS)、サービスとしてのインフラストラクチャ(IaaS)、サービスとしてのプラットフォーム(PaaS)等)
» ディストリビューテッドシステム
» IoT
» マイクロサービス
» コンテナ化
» サーバーレス
» 組み込みシステム
» 高性能コンピューティング(HPC)システム
» エッジコンピューティングシステム
» 仮想化システム
3.6 暗号化ソリューションを選択し、決定する
» 暗号化のライフサイクル(キー、アルゴリズムの選択等)
» 暗号化の方法(対称、非対称、楕円曲線、量子等)
» 公開キー基盤(PKI)
» キー管理の実務
» デジタル署名とデジタル証明書
» 否認防止
» 完全性(ハッシュ等)
3.7 暗号解読攻撃の方法を理解する
» ブルートフォース
» 暗号文のみ
» 既知の平文
» 頻度分析
» 暗号文選択
» 実装攻撃
» サイドチャネル
» フォールトインジェクション
» タイミング
» 中間者(MITM)
» パス・ザ・ハッシュ
» ケルベロスの悪用
» ランサムウェア
3.8 事業所および施設の設計に安全な原則を適用する
3.9 事業所および施設へのセキュリティ管理を設計する
» 配線用クローゼット/中間配電盤
» サーバールーム/データセンター
» 媒体保管施設
» 証拠保管
» 立入禁止区域および作業区域のセキュリティ
» ユーティリティおよび暖房、換気、および空調(HVAC)
» 環境の問題

» 防火、火災検知および消火
» 電源(冗長、バックアップ等)

4．通信とネットワークのセキュリティ

「通信とネットワークセキュリティ」ドメインでは、ネットワークアーキテクチャ、伝送方法、トランスポートプロトコル、制御デバイスのほかオープンなネットワークやクローズなネットワークを介して送信される情報の機密性、完全性、可用性を維持するために利用されるセキュリティ対策の理解が求められます。

CISSP は、ネットワークの基礎(トポロジー、アドレス、セグメンテーション、スイッチングやルーティング、無線、OSI や TCP/IP モデルおよびプロトコルスイートなど)を十分に理解していることが求められます。また、セキュアなネットワークを実装するための暗号、ネットワーク機器のセキュリティ対策など広範なトピックについても理解しておかなければなりません。ネットワーク機器の(スイッチ、ルータ、無線 LAN アクセスポイントなど)の安全な設置と維持管理に関する知識とスキルが求められます。ネットワークにおけるアクセス制御、エンドポイントのセキュリティ、コンテンツ配信ネットワーク(CDN)についての知識も必要です。

CISSP はネットワークを利用した多くのアプリケーション(データ、音声、リモートアクセス、マルティメディアなど)の利用を推進するために様々な技術を利用して、セキュアな通信チャネルを設計および実装できるスキルが求められます。また、これらのアプリケーションに対する攻撃ベクトルの知識や、それらを防止、低減する知識やスキルについても求められます。

求められるスキルと関連するキーワード

4.1 ネットワークアーキテクチャに安全な設計原則を評価し、適用する
- » オープンシステム相互接続(OSI)および TCP/IP モデル
- » IP ネットワーク(IPSec、IPv4/6 等)
- » 安全なプロトコル
- » マルチレイヤプロトコルの影響
- » コンバージドプロトコル(ファイバーチャネルオーバーイーサネット(FCoE)、iSCSI、ボイスオーバーインターネットプロトコル(VoIP)等)
- » マイクロセグメンテーション(ソフトウェア定義ネットワーク(SDN)、仮想拡張可能ローカルエリアネットワーク(VXLAN)、カプセル化、ソフトウェア定義の広域ネットワーク(SD-WAN)等)
- » 無線ネットワーク(Li-Fi、Wi-Fi、Zigbee、衛星等)
- » セルラーネットワーク(4G、5G 等)
- » コンテンツ配信ネットワーク(CDN)

4.2 安全なネットワークコンポーネント
- » ハードウェアのオペレーション(冗長電源、保証、サポート等)
- » 伝送媒体
- » ネットワークアクセス制御デバイス(NAC)デバイス
- » エンドポイントセキュリティ

4.3 安全な通信チャネルを設計し構築する
- » 音声
- » マルチ媒体コラボレーション
- » リモートアクセス

5．アイデンティティとアクセスの管理(IAM)

「アイデンティティとアクセスの管理(IAM)」ドメインでは、機密性を維持するために必要な、人、デバイス、サービス、アプリケーション、データなどのエンティティの相関を理解し、それを適切に管理するための知識とスキルが求められます。

アイデンティティ(Id)は単にユーザアカウントのことを指すのではなく、組織の資産全てを適切に判別し管理を行うために必要な、個別の識別子とその属性です。これらの情報を活用して、組織の求める安全な状態の維持を実践することが可能になります。

アクセス管理において最も重要なことは、機密性の理解です。機密性(Confidentiality)とは、情報の機微性(Sensitivity)や重要性(Importance)ではなく、権限の維持ができていることを指します。つまり、誰かが何かにアクセスできる状態を適切に維持するということです。誰か(Subject)がなにか(Object)に対して、どのような権限が与えられているか。これを最小権限の原則に基づいて設計したり、職務の分離の原則に基づいて設計したりすることが、アクセス管理です。

アクセスポリシーをどのように構築するか。リスクやアクセス時の属性に応じて動的にポリシーを構築し適用する仕組みがゼロトラストです。このドメインのキーワードである「強制アクセス制御」および「属性ベースのアクセス制御」における認可の仕組みを理解すれば、ゼロトラストも構築できるようになります。

「アイデンティティとアクセスの管理(IAM)」の知識とスキルを身につけることで、さまざまなセキュリティソリューションの仕組みを容易に理解できるようになります。

求められるスキルと関連するキーワード

5.1 資産への物理的および論理的アクセスを制御する
- » 情報
- » システム
- » デバイス
- » 施設
- » アプリケーション

5.2 人、デバイス、サービスの特定および識別を管理する
- » アイデンティティ管理(IdM)の実装
- » 単一/多要素認証(MFA)
- » 説明責任
- » セッション管理
- » アイデンティティの登録、証明、確認
- » ID 連携管理(FIM)
- » クレデンシャル管理システム
- » シングルサインオン(SSO)
- » ジャスト・イン・タイム(JIT)

5.3 認証システムを実装する
- » Open ID Connect、OAuth
- » SAML
- » ケルベロス
- » RADIUS、TACACS

5.4 認可の仕組みを実装し管理する
- » ロールベースアクセス制御(RBAC)
- » ルールベースアクセス制御
- » 強制アクセス制御(MAC)

» 裁量アクセス制御(DAC)
» 属性ベースのアクセス制御(ABAC)
» リスクベースアクセス制御

5.5 アイデンティティおよびアクセスプロビジョニングのライフサイクルを管理する
» アカウントアクセスの審査(ユーザー、システム、サービス等)
» プロビジョニングとプロビジョニング解除(入退社と異動等)

5.6 サードパーティのサービスとしてアイデンティティを統合する
» オンプレミス
» クラウド
» ハイブリッド

6．セキュリティの評価とテスト

「セキュリティの評価とテスト」のドメインでは、セキュリティの運用やソフトウェア開発のセキュリティと関連して、日々のセキュリティ活動におけるセキュリティ対策の評価や、ソフトウェアが適切に開発されているかを確認するためのテストなど、セキュリティ機能の有効性を測るための知識とスキルが求められます。

評価やテストは十分に準備してから行われなければなりません。それは正しい評価を行うためでもあり、サービスやシステムへの影響を最小限にする必要があるためです。ソフトウェアのテストなどはテスト環境で実施できますが、日常的なセキュリティ対策の評価やテストは本番環境で行うことも少なくないためです。

CISSP はさまざまな種類のテストについて、その目的と手法を理解し、対象に合わせた適切なものを選択しなければなりません。例えば、侵入対策が適切にできているかを評価する場合にはペネトレーションテストを、対策したはずの脆弱性が見逃されていないかどうかを評価するためには脆弱性テストを選択します。評価したい内容によってはこれらを組み合わせて利用することもありますし、攻撃者がそのテスト手法を利用する可能性がないかなども検証したりします。

また評価の結果を活かした改善プロセスを通じて、事業継続やレジリエンス、セキュリティ対策の継続的向上などにも役立てることができます。

セキュリティの評価とテストは単独のドメインとして取り上げられていますが、他のドメインの知識やスキルをサポートするものとして重要な要素が含まれています。CISSP は評価やテストの知識やスキルを情報セキュリティのライフサイクルに活かすことが求められています。

ドメインの主題となるキーワードと関連する要素

6.1 評価、テスト、監査を設計し、検証する
- » 内部
- » 外部
- » サードパーティ

6.2 セキュリティコントロールのテストを実施する
- » 脆弱性評価
- » ペネトレーションテスト
- » ログレビュー
- » 代理トランザクション
- » コードレビューとテスト
- » 悪用ケーステスト
- » テスト範囲の分析
- » インターフェーステスト
- » 侵害攻撃シミュレーション
- » コンプライアンスチェック

6.3 セキュリティプロセスデータを収集する(技術と管理等)
- » アカウント管理
- » 管理の審査と承認
- » 重要業績指標とリスク指標
- » 検証データのバックアップ
- » トレーニングと意識向上
- » 災害復旧(DR)と事業継続性(BC)

6.4 テスト出力を分析し、レポートを生成する
- » 改善

- » 例外処理
- » 倫理的開示

6.5 セキュリティ監査を実施または促進する

- » 内部
- » 外部
- » サードパーティ

7．セキュリティの運用

「セキュリティの運用」ドメインでは、組織の情報セキュリティの機能や計画を維持し、適切に改善していくための知識とスキルが求められます。機能や計画が維持できているかを判断するためには、セキュリティ対策やポリシーの遵守状況などに関する情報収集が必要になります。また、インシデント対応や調査活動もセキュリティ運用の重要な要素です。

情報収集を適切に行うためには、事前の準備が必要になります。例えばセキュリティ対策を目的通りに実施しているということを確認、または証明するためにはエビデンスが必要になります。このエビデンスは後から作ることができませんので、ログ管理、モニタリング機能を設計する際に十分に検討しなくてはいけません。

準備できていなかった場合には、フォレンジックスなどの技術を活用してエビデンスを掘り起こす必要があります。このような作業には非常に大きなコストと時間がかかることから、日常的な運用に必要な情報はいつでも取得できるように準備しておきます。

モニタリングの結果、トラブルや事故の予兆があった場合には、その対応が必要になります。明確な事故が発生していない場合は資産の保護を改めて実施し、インシデントの発生が見られた場合には、インシデント対応を実施します。

CISSP には、このような日々の運用に必要な活動を十分に理解することが求められます。

セキュリティの運用に関するさまざまな知識は、運用担当者だけではなく、開発担当者にも必要になります。DevSecOps 環境においては、運用担当者がどのような情報を必要としているか、そして運用上の修正作業を開発者が直接関与することなく運用担当者だけで行うためにはどのような機能の提供が必要かなどを検討する必要があるためです。

たとえば、クラウド上でのサービス運用においてサーバのパフォーマンスが足りない場合にサーバの台数を増やすといったことが必要になります。これらの作業を運用担当者が評価し、開発担当者に伝え、確認の上で開発担当者が構成をし直すといった場合、適切な時間で作業が終了しないことがあります。このような場合には運用担当者用のインタフェースをあらかじめ作成し、自ら修正ができるようにしておくのが望ましいと言えます。

このような判断をするためにも、セキュリティの運用とソフトウェア開発、アクセス制御、リスクマネジメントのそれぞれのドメインの関連について CISSP は熟知しておく必要があります。

運用セキュリティにおいては、セキュリティ担当者の日常的な活動を把握し、それをサポートするためのインフラの構築について理解しなくてはいけません。CISSP には、セキュリティ担当者が効率的に日常的な活動を実践し、継続的なセキュリティ対策の維持ができる環境を計画、提案することが求められます。

ドメインの主題となるキーワードと関連する要素

7.1　調査を理解し、遵守する
- » 証拠の収集と取り扱い
- » 報告および文書化
- » 調査手法
- » デジタルフォレンジックツール、戦術、および手順
- » アーティファクト(コンピュータ、ネットワーク、モバイルデバイス等)

7.2　ロギングと監視活動を実施する
- » 侵入の検知および防止

» セキュリティ情報及びイベント管理(SIEM)
» 継続的な監視
» 出力監視
» ログ管理
» 脅威インテリジェンス(脅威フィード、脅威ハンティング等)
» ユーザと事業体の行動分析(UEBA)

7.3 構成管理(CM)の実行(プロビジョニング、ベースライン、自動化等)
7.4 基礎的なセキュリティ運用概念を理解し適用する
» 知る必要性に基づいた最小特権
» 職務分離(SoD)と責任
» 特権アカウント管理
» ジョブローテーション
» サービスレベル契約(SLAs)
7.5 リソース保護手法を採用する
» 媒体管理
» 媒体保護技術
7.6 インシデント管理を実施する
» 検出
» 対応
» 緩和
» 報告
» 復旧
» 改善
» 教訓
7.7 検知および防止策を運用し維持する
» ファイアウォール(次世代、Web アプリケーション、ネットワーク等)
» 侵入検知システム(IDS)および侵入防止システム(IPS)
» ホワイトリスティング／ブラックリスティング
» サードパーティのセキュリティサービス
» サンドボックス
» ハニーポット/ハニーネット
» マルウエア対策
» 機械学習と人工知能(AI)ベースのツール
7.8 パッチおよび脆弱性管理を実施しサポートする
7.9 変更管理プロセスに参加し理解する
7.10 復旧戦略を実施する
» バックアップストレージ戦略
» 復旧サイト戦略
» 複数処理サイト
» システム障害許容力、高可用性、サービス品質(QoS)、およびフォルトトレランス
7.11 災害復旧(DR)プロセスを導入する
» 対応
» 人員
» コミュニケーション
» 評価
» 復元
» トレーニングと意識向上
» 教訓
7.12 災害復旧計画(DRP)をテストする
» リードスルー/テーブルトップ
» ウォークスルー
» シミュレーション

- » 並行
- » 完全な中断

7.13 事業継続性(BC)の立案および訓練に参加する

7.14 物理的セキュリティを実装し管理する

- » 境界セキュリティ制御
- » 内部セキュリティ制御

7.15 個人の安全に関する懸念への対処に参加する

- » 出張
- » セキュリティトレーニングと意識向上
- » 緊急管理
- » 強要

8．ソフトウェア開発セキュリティ

「ソフトウェア開発セキュリティ」ドメインでは、コーディングだけではなく、ソフトウェアの開発における環境や手法を含めた、開発ライフサイクル全般についてのセキュリティに関する知識とスキルが求められます。SDN や IoT など、これまではハードウェアのセキュリティとして捉えられていた分野も、ソフトウェア化されることにより、ますますソフトウェアに関するセキュリティへの依存度が高まっているなか、CISSP もソフトウェア開発について十分な知識が求められるようになりました。

システムライフサイクル(SLC)におけるソフトウェア開発ライフサイクル(SDLC)について正しく理解し、開発者のプロセスや責任を明確にした上で、セキュリティ専門家が助言できる内容について把握します。開発と運用、そして品質管理を統合的に管理するための DevSecOps を実践するために、運用を考慮した開発についても支援します。

また、開発手法や開発環境の選択においても、複数の手法や環境の目的を正しく理解した上で、メリット・デメリットを判断し、プロジェクトに応じて選択できるようにセキュリティの視点から助言をします。単に開発を迅速に行うだけではなく、サービスのデプロイ時間を考慮して、効率的なテスト手法の選択、サービスレジリエンスを実現するための仕組みなどを提案します。

ソフトウェア開発においては、実際にコーディングするスキルが必要なわけではなく、開発チームの役割や責任、システムライフサイクルにおける活動を適切に理解し、機密性、完全性が維持できるような助言を実施できるスキルと知識が求められます。

ドメインの主題となるキーワードと関連する要素

8.1　ソフトウェア開発ライフサイクル(SDLC)におけるセキュリティを理解し適用する
- » 開発手法(アジャイル、ウォーターフォール、DevOps、DevSecOps 等)
- » 成熟度モデル(能力成熟度モデル(CMM)、ソフトウェア保証の成熟度モデル(SAMM)等)
- » 運用と保守
- » 変更管理
- » 統合製品チーム(IPT)

8.2　開発環境においてセキュリティ制御を認識し執行する
- » プログラミング言語
- » ライブラリ
- » ツールセット
- » 統合開発環境(IDE)
- » ランタイム
- » 継続的インテグレーションと継続的デリバリー(CI/CD)
- » セキュリティのオーケストレーション、自動化、応答(SOAR)
- » ソフトウェア構成管理(SCM)
- » コードリポジトリ
- » アプリケーションセキュリティテスト(静的なアプリケーションのセキュリティテスト(SAST)、動的なアプリケーションセキュリティテスト(DAST)等)

8.3　ソフトウェアセキュリティの有効性を評価する
- » 変更の監査とロギング
- » リスク分析と低減

8.4　取得したソフトウェアのセキュリティインパクトを評価する
- » 市販品(COTS)
- » オープンソース
- » サードパーティ

» 管理サービス(サービスとしてのソフトウェア(SaaS)、サービスとしてのインフラストラクチャ(IaaS)、サービスとしてのプラットフォーム(PaaS)等)

8.5 セキュアコーディング規定とガイドラインを定義し適用する

» ソースコードレベルでのセキュリティの弱点と脆弱性
» アプリケーションプログラミングインターフェース(APIs)のセキュリティ
» 安全なコーディングの実践
» Software Defined Security

確認テスト

1. Alice は小さなオンライン小売会社を経営しており、顧客の多くは米国の人達です。現在は、ブロックチェーンベースの決済のみ受け付けていますが、クレジットカードの利用も検討しているそうです。PCI DSS(Payment Card Industry Data Security Standard)の要件を調査した結果、彼女はコンプライアンスのコストが収益の増加を上回ると判断しました。この決断を最もよく表しているのは、次のうちどれでしょうか。

   A. ソーシャルエンジニアリング
   B. PCI DSS マーチャントレベル 3
   C. カード検証値(CVV)
   D. リスク回避

2. ISC2 の倫理規定によると、苦情は _____ 提出しなければなりません。

   A. ISC2 のウェブサイトを通じて
   B. 書面で
   C. 匿名で
   D. 告発された違反行為から 1 年以内に

3. ビジネス・インパクト・アナリシス(BIA)では、以下の項目以外はすべて考慮する必要があります。

   A. 組織の資産の価値
   B. 業界標準
   C. 組織に特有の脅威
   D. 損失の可能性

4. _____ は、組織がクリティカルパスを失っても、企業として存続できなくなるまでの期間を表しています。

   A. 回復時間目標(RTO)
   B. リカバリーポイント・オブジェクティブ(RPO)
   C. 最大許容ダウンタイム(MAD)
   D. 年間損失期待値(ALE)

5. 次のセキュリティ教育のうち、リアルタイムフィードバックの可能性が最も高いのはどれですか。

   A. コンピュータベースのトレーニング
   B. 繰り返しによる暗記
   C. ライブトレーニング
   D. 報酬の仕組み

6. 組織と従業員の間の責任について、正式に詳細に説明したものはどれですか。

   A. 機密保持契約(NDA)
   B. 雇用契約

C. アクセプタブル・ユース・ポリシー(AUP)
D. セキュリティポリシー

7. 次のうち、シニアマネジメントが公布し、組織の戦略的ビジョンと目標を概説するものはどれですか。

A. ポリシー
B. 手順
C. ガイドライン
D. 規格

8. 次のどのエンティティが、特定の一連の個人識別情報(PII)に関連する個々の人間ですか？

A. データオーナー
B. データ管理者
C. データ対象者
D. データプロセッサー

9. 次のどの国の組織が、EU 市民の個人データを処理することを許可されていませんか？

A. ドイツ
B. アルゼンチン
C. シンガポール
D. 米国

10. 次のうち、DRM ソリューションの共通の特徴ではないものはどれですか？

A. 永続性
B. 継続的な監査証跡
C. 自動失効
D. バーチャルライセンス

確認テスト 解答

1. 正解: D

これは、リスク回避の典型的な例です。シニアマネジメントは、報酬がリスクに見合わないため、その事業が戦略的目標に適合しないと判断したのです。

2. 正解: B

ISC2 では、宣誓供述書として ISC2 のコンプライアンスフォームを使用することが義務付けられています。

3. 正解: B

業界標準は、組織が独自の BIA を決定する際にはあまり関係ありません。

4. 正解: C

これが MAD の定義です。

5. 正解: C

教室におけるライブのインストラクターは、フィードバックのための最良の機会を提供します。

6. 正解: B

これが雇用契約の定義です。

7. 正解: A

これがポリシーの定義です。

8. 正解: C

これがデータ主体の定義です。

9. 正解: D

アメリカには、個人のプライバシーを管理する EU 法である一般データ保護規則(GDPR)に準拠する包括的な連邦法はありません。よって、米国内の組織では、一部の例外を除き、EU 市民の個人データを処理することはできません。

10. 正解: D

″バーチャルライセンス″は意味のある言葉ではなく、この文脈では単なる誤答に過ぎません。

CISSP 受験から認定までの流れと認定維持

CISSP 認定試験

- **申込み(実施機関)**
  認定試験は、Pearson VUE にて実施されます。試験の申込みや会場などに関する情報は、Pearson VUE Web サイトを参照してください。
  https://www.pearsonvue.co.jp/Clients/ISC2.aspx

- **出題範囲**
  CISSP CBK 8 ドメイン

- **問題数**
  250 問／4 択 Computer Based Testing(CBT)(日本語・英語併記)
  250 問中、25 問は調査のために入っており、採点対象とはなりません。

- **試験時間**
  6 時間(途中休憩可・途中退出可)
  ・試験開始前に 30 分程度の試験説明があります(必須)
  ・試験監督の監視のもとでの休憩となります
  ・途中退出後は、試験会場に戻ることはできません

- **受験料**
  749 米ドル

- **必須持ち物(忘れると受験不可)**
  写真・署名付き公的身分証明書と署名付き身分証明書(計 2 点)

  合格点
  1000 点満点中 700 点以上で合格
  (スケールドスコアなので、各問題の配点は同じとは限りません。)
  受験後に会場で合否がわかります(非公式)。
  6 週間～8 週間後に公式な結果が電子メールで通知されます。不合格の場合には、8 ドメインについて、最もスコアがよかったドメインから最もスコアが悪かったドメインまでの 1～8 の順位が記載されます。

- **CISSP 試験ドメインの各ドメイン出題比率**

ドメイン	出題比率
1. セキュリティとリスクマネジメント	15%
2. 資産のセキュリティ	10%
3. セキュリティアーキテクチャとエンジニアリング	13%
4. 通信とネットワークセキュリティ	13%
5. アイデンティティとアクセスの管理(IAM)	13%
6. セキュリティの評価とテスト	12%
7. セキュリティの運用	13%
8. ソフトウェア開発セキュリティ	11%
	100%

- **CAT(Computer Adaptive Testing)について**
  CISSP 英語版試験のみ CAT による試験が行われます。日本語を選択した場合には該当しません。
  CAT の詳細はこちらをご覧ください。
  https://www.isc2.org/Certifications/CISSP/CISSP-CAT

CISSP 認定要件

- CISSP に認定されるには、下記要件をすべて満たすことが必要です。

1. CISSP 認定試験に合格すること
2. CISSP CBK 8 ドメインのうち 2 ドメインに関連した 5 年以上の業務経験があること
   下記どちらかに該当する方は、1 年分の経験が免除され、4 年の業務経験で認定可能です。(免除は最長で 1 年分)
   ・大学卒業学位取得者
   ・ISC2 が認める資格の取得者
   対象資格は https://www.isc2.org/Certifications/CISSP/Prerequisite-Pathway 参照
3. 実務経験が事実であることを証明すること
4. ISC2 の倫理規約に合意すること
5. ISC2 認定資格保持者(CISSP, SSCP, CSSLP など)から推薦されること
6. 無作為に行われる業務経験に関する監査に合格すること
7. 犯罪歴等に関する 4 つの質問事項(https://www.isc2.org/Register-for-Exam/Background-Qualifications)に該当する場合は、認定を受けることができない場合があります。

認定登録手続

- 推薦状(エンドースメント)をオンライン上で提出
  試験合格者は、CISSP として認定されるために、ご自身のプロフェッショナル経験を証明することのできる、現役の ISC2 認定資格保持者(CISSP, SSCP, CSSLP など)からのエンドースメント(推薦)を提出する必要があります。合格者に試験後 2 日以内に配信されるメールに、試験結果およびオンラインエンドースメント(推薦状)プロセスについての記載があります。

CISSP 認定継続要件

- CISSP の資格を維持するためには、下記要件をすべて満たすことが必要です。

1. ISC2 倫理規約に従い行動する
2. 年会費を支払う(125 米ドル／年・複数の資格を保有している場合でも同額)
3. 継続教育単位(CPE クレジット)を 3 年間で 120 ポイント取得する
   ISC2 イベントやその他ベンダーによる情報セキュリティ関連セミナー受講等で CPE を取得することができます(1 時間の教育受講で CPE 1 ポイント)。CPE は監査を受けることがあります。

その他

記載している情報は 2022 年 3 月現在の内容です。最新情報は ISC2 ホームページにてご覧ください。

ISC2 日本語Webサイト	https://japan.isc2.org/
CISSP認定試験案内	https://japan.isc2.org/examination_cissp.html
ISC2 CISSP CBK 公式トレーニング案内	https://japan.isc2.org/cissp_training.html

本書の取り扱いについて

CISSP 8 ドメインガイドブック

2021 年 12 月 1 日 第 5 版発行

お問い合わせ先

ISC2

E-mail: infoisc2-j@isc2.org

TEL: 03-5322-2837

URL: https://japan.isc2.org/