

IT 資格 道 場

CCST サイバーセキュリティ 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

Cisco「CCST Cybersecurity Objective Domains」(100-160・公式 PDF の作成日
2023-01-24・版番号の記載なし・2026-10-09 取得)準拠
2026年10月版

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

目次

試験の概要 [intro]

第1章 セキュリティの基本原則 [1.1]

1.1 基本の用語：脆弱性、脅威、リスク CIA [1.1]

1.2 サイバー攻撃の種類 [1.2]

1.3 認証、認可、アカウンティングと多要素認証 [1.3]

1.4 暗号化、ハッシュ、証明書 [1.4]

サンプルはここまでです

試験の概要 [intro]

CCST サイバーセキュリティは、Cisco が実施する入門のセキュリティ試験です。試験コードは 100-160 で、試験時間は 50 分です。問題数は試験ごとに異なり、Cisco は数を公表していません。オデッセイの案内が挙げる出題形式は 3 つです。選択形式、ドロップダウンリスト形式、ドラッグ&ドロップ形式です。3 つ以外の形式は、この案内にありません。

試験は7つの言語で受けられます。英語、アラビア語、中国語、スペイン語、フランス語、日本語、ポルトガル語です。オデッセイの案内に載る受験料は、17,600 円(税込)です。2025 年 7 月 15 日以降に取得した認定の有効期間は、5 年間です。それより前に取得した認定には、期限がありません。

出題範囲は 5 つの分野でできています。この教材の第 1 章から第 5 章は、分野の順を入れ替えています。

章	分野
第 1 章	セキュリティの基本原則 (Essential Security Principles)
第 2 章	ネットワークセキュリティの基本概念 (Basic Network Security Concepts)
第 3 章	エンドポイントセキュリティの概念 (Endpoint Security Concepts)
第 4 章	脆弱性の評価とリスクマネジメント (Vulnerability Assessment and Risk Management)
第 5 章	インシデント ハンドリング (Incident Handling)

第1章 セキュリティの基本原則 [1.1]

1.1 基本の用語:脆弱性、脅威、リスク、CIA [1.1]

脆弱性、脅威、リスクの3語

霞浦ロジテックの倉庫で、更新されていない古い在庫管理ソフトがパソコンに入ったままだとします。このソフトには、外から悪用できる弱点があります。この弱点が脆弱性 (vulnerability) です。弱点があること自体は、まだ被害ではありません。NIST の用語集は、脆弱性を次のように説明します。情報システム、手順、内部統制、実装の弱点で、脅威源に悪用されたり引き金を引かれたりしうるものです。

脅威 (threat) は、害を与える状況や出来事です。不正アクセス、破壊、開示、改ざん、サービス妨害によって、組織の業務、資産、個人に悪影響を与えるものを指します (NIST の定義)。古い在庫管理ソフトの例なら、そのソフトを狙う攻撃者の動きが脅威に当たります。脅威は弱点そのものではありません。

リスク (risk) は、ある状況や出来事にどの程度脅かされているかを表す尺度です。脆弱性や脅威の別名ではありません。決まり方は、起きたときの悪影響の大きさと、起きる可能性の2つです。起きる可能性が低ければ、影響が大きくてもリスクは高くなりません。影響が小さくても毎日起きるなら、リスクは上がります。

語	何を指すか	在庫管理ソフトの例
脆弱性	悪用されうる弱点	更新されていないソフトの欠陥
脅威	害を与える状況や出来事	そのソフトを狙う攻撃

語	何を指すか	在庫管理ソフトの例
リスク	脅かされている程度の尺度	起きたときの被害の大きさと、起きる可能性

エクスプロイト、攻撃ベクトル、攻撃対象領域

エクスプロイト (exploit) は、脆弱性を突く仕組みです。サイバーキルチェーンの「武器化」の段階が分かりやすい例です。この段階では、ウェポナイザーが、マルウェアとエクスプロイトを組み合わせ、送り届けられる荷にします。弱点そのものがエクスプロイトなのではありません。弱点が脆弱性で、弱点を突く手段がエクスプロイトです。

攻撃ベクトル (attack vectors) は、出題範囲に挙がる語です。NIST は APT について、サイバー、物理、欺瞞など複数の攻撃ベクトルを使うと説明します。例に挙がる3つは、どれも別の種類の手口です。攻撃は一つの技術に限られません。

攻撃対象領域 (attack surface) は、攻撃者が侵入、影響、データの持ち出しを試みられる点の集まりです。点が並ぶ場所は、システム、システムの部品、動作環境の境界です。点が増えるほど、領域は広がります。点の数は、攻撃者の人数とは関係がありません。

堅牢化と多層防御

堅牢化 (hardening) は、守りを固める作業です。脆弱性に修正を当て、不要なサービスを止めて、攻撃の手段をなくします。汐見メディカルの受付端末で考えます。使っていないサービスを止め、更新を当てると、攻撃の手段が減ります。堅牢化は、更新を当てるだけの作業ではありません。

多層防御 (defense-in-depth) は、人、技術、運用の力を組み合わせる戦略です。組織の複数の層に障壁を置きます。障壁が1枚だけなら、突破された時点で守りが尽きます。複数の層に置いておくと、1つ越えられても次の障壁が残ります。技術だけに頼る守りは、多層防御ではありません。

機密性、完全性、可用性

機密性 (confidentiality)、完全性 (integrity)、可用性 (availability) の3つを、CIA (セキュリティの三原則) と呼びます。頭文字を並べた呼び名です。3つは、情報のどの性質を守るかで分かります。3つは同じ意味ではありません。

要素	守るもの	損なわれる例
機密性	許可された者だけが情報にアクセス・開示できる状態	患者の診療情報が許可のない人に見られる
完全性	情報が不正に改ざん・破壊されていない状態	請求金額が書き換えられる
可用性	必要な時に確実に情報へアクセスし利用できる状態	予約システムが止まり、予約を確認できない

機密性には、個人のプライバシーや独自の情報の保護も含まれます。決め手は、許可された者に限るという点です。アクセスできる人を絞る話が出たら、機密性です。誰でも見られる情報には、当てはまりません。

完全性には、否認防止と真正性の確保も含まれます。中心は、情報が途中で書き換えられていないことです。数字や記録の正しさが論点なら、完全性です。見られたかどうかは、完全性の論点ではありません。

可用性が問うのは、必要な時に使えるかどうかです。ランサムウェアでファイルが暗号化され、開けなくなった場面を考えます。情報は盗まれていなくても、必要な時には使えません。これは可用性が損なわれた状態です。

攻撃者の種類と攻撃の理由

攻撃者の種類は、NIST の脅威源の分類表が整理しています。敵対的な脅威源は、次の4つに分かれます。

- 個人: 外部者、内部者、信頼された内部者、特権を持つ内部者
- 集団: その場限りの集まり、組織化された集団
- 組織: 競合、供給者、取引先、顧客
- 国家 (Nation-State)

この表は、外部の人だけを攻撃者とは見ていません。

国家 (Nation-State) も、敵対的な脅威源の一つとして分類されています。外部の個人から国家まで、規模や立場はさまざまです。

内部者の脅威 (insider threat) は、組織の中にいる人から来ます。許された権限を、意図的に、または無自覚に使って害を与えます。悪意の有無は、成り立つ条件ではありません。誤って情報を外へ出した場合も、許された権限を使った害に当たります。内部者の脅威は、外部の攻撃者だけを指す語ではありません。

攻撃の理由 (reasons for attacks) の一例が、主張のための攻撃です。主張のために攻撃する集団を、ハクティビスト (hacktivist) と呼びます。サービス拒否 (DoS) 攻撃は、もともとハクティビストが使っていた手口でした。目的は、ネットワークへのアクセスを妨げることでした。

倫理規定 (code of ethics) は、出題範囲に語として挙がっています。出題範囲は、その中身の定義を示していません。

情報漏えい、セキュリティポリシー、情報保証

情報漏えい(exfiltration)は、システムから情報を許可なく持ち出すことです。機密性が破られる典型的な場面です。持ち出された情報が改ざんされるとは限りません。

セキュリティポリシー (security policy) は、組織が機微な情報をどう管理し、保護し、配布するかを定めたものです。法、規則、慣行の集まりとして定義されます。個々の機器の設定だけを指す語ではありません。

情報保証 (information assurance) は、情報とシステムを守る手だての総称です。可用性、完全性、認証、機密性、否認防止の5つを確保して守ります。5つのうち3つが CIA です。情報保証は、CIA の別名ではありません。

場面から語を選ぶ

場面	当てはまる語	決め手
倉庫の古い在庫管理ソフトに、悪用できる欠陥が残っている	脆弱性	悪用されうる弱点
そのソフトを狙って、攻撃者が通信を送り込んでくる	脅威	害を与えうる出来事
被害の大きさと、起きる可能性から、対応の順番を決める	リスク	影響の大きさと可能性の2要素
欠陥を突くための、マルウェアと組み合わせた道具	エクスプロイト	脆弱性を突く仕組み
診療情報が、許可のない人に見られた	機密性の侵害	許可された者に限る状態が崩れた

場面	当てはまる語	決め手
請求金額が、不正に書き換えられた	完全性の侵害	不正な改ざんを防げなかった
予約システムが止まり、必要な時に使えない	可用性の侵害	必要な時に使える状態が崩れた
社員が、許された権限で在庫データを誤って外へ出した	内部者の脅威、情報漏えい	許された権限を使った害

1つの出来事に、複数の語が当てはまることがあります。社員が許された権限で在庫データを書き換えた場合は、内部者の脅威であり、完全性の侵害でもあります。語は、1つの面だけでは決まりません。脆弱性、脅威、リスクは、弱点、出来事、尺度という別の面です。機密性、完全性、可用性は、守る情報のどの性質が崩れたかという面です。

脆弱性があれば、すぐに被害が出るわけではありません。脅威が現れ、悪用されて初めて、害になります。リスクは、その害の大きさと起きる可能性で測ります。弱点が見つかった段階では、まだ被害は出ていません。

場面で考える

汐見メディカルの受付端末で、古い印刷ソフトに既知の弱点が見つかったとします。弱点を残したままでは、エクスプロイトを防げません。更新を当てれば、弱点がなくなります。使っていないサービスも止めれば、攻撃の手段が減り、攻撃対象領域も小さくなります。これが堅牢化であり、更新だけを指す語ではありません。

朱鷺野フーズが、Web サーバーの更新、ファイアウォール、入退室の管理、社員への教育を、すべて組み合わせたとします。1つの対策に頼る形ではありません。

せん。人、技術、運用の力を重ね、複数の層に障壁を置いています。これは多層防御です。多層防御は、技術だけを重ねる形でもありません。

退職の決まった社員が、許された権限で顧客リストをコピーし、外へ持ち出したとします。この社員は、組織の内部にいる人です。許された権限を使って害を与えているので、内部者の脅威です。システムから情報を許可なく持ち出しているので情報漏えいでもあり、守られるべき性質は機密性です。外部から侵入した形ではなくても、内部者の脅威と呼べない理由はありません。

請求システムのデータベースで、金額が不正に書き換えられたとします。情報は外へ出ていません。使えなくなってもありません。崩れたのは、不正な改ざんを防ぐ完全性です。

通信の大量送信で予約システムが止まり、予約の確認ができなくなったとします。情報は盗まれていません。改ざんもされていません。必要な時に使えないので、可用性が損なわれた状態です。サービス拒否の攻撃は、もともとハクティビストが、ネットワークへのアクセスを妨げるために使っていた手口でした。

同じ弱点を持つ2つの会社でも、リスクは同じとは限りません。攻撃を仕掛ける意図や能力のある相手が現れやすいほど、起きる可能性が上がります。被害が大きい業務ほど、影響が大きくなります。リスクは、弱点の有無だけでは決まりません。[^1]

1.2 サイバー攻撃の種類 [1.2]

マルウェアの定義と種類

朱鷺野フーズの経理担当者が、取引先を名乗るメールの添付ファイルを開いたとします。その直後から、パソコンの動作がおかしくなったとします。この場面で疑うのは、マルウェア (malware) です。マルウェアは、有害な目的で意図

的にシステムへ入れられたハードウェア、ファームウェア、ソフトウェアを指します。ソフトウェアだけを指す語ではありません。

マルウェアの例として、次の6つが挙げられます。

- ウイルス
- ワーム
- トロイの木馬
- スパイウェア
- アドウェア
- ランサムウェア

トロイの木馬は、ウイルスやワームと違い、自分で複製するようには作られていません。複製するかどうか、区別の手がかりです。

ランサムウェア (ransomware) は、被害者のデータを暗号化し、その後に身代金を要求するマルウェアです。CISA は、被害者のファイルを暗号化して使えなくし、復号と引き換えに身代金を求めるものと説明します。特徴は、ファイルを使えなくして金銭を求める点です。データを盗むことは、定義の中心ではありません。

サービス拒否、DDoS、ボットネット

サービス拒否 (denial of service、DoS) は、許可された資源へのアクセスを妨げる攻撃です。時間が重要な処理を遅らせる場合も含まれます。侵入して情報を盗むことは、この攻撃の目的ではありません。狙うのは、使えなくすることです。

DDoS には、次の2つの型があります。

- 大量通信型 (volumetric): IoT ボットネットを使う
- アプリケーション層 (L7) 型: サーバーの資源を使い果たさせる

DDoS は、長く続くものばかりではありません。Ping of Death のように、短時間で終わるものもあります。暗号化された通信を使う SSL の DDoS もあります。通信が暗号化されているからといって、安全とは限りません。

ボットネット (botnet) は、robot と network を合わせた語です。乗っ取った多数のコンピューターを、ボットの網としてまとめたものを指します。1台のコンピューターだけでは、ボットネットとは呼びません。

IoT の脆弱性 (IoT vulnerabilities) は、出題範囲に挙がる語です。IoT ボットネットは、大量通信型の DDoS に使われます。つまり、IoT 機器の弱点は、DDoS の材料になりえます。

ソーシャルエンジニアリングとフィッシング

ソーシャルエンジニアリング (social engineering) は、人をだまして、パスワードなどの情報を明かせ、攻撃に使う試みです。技術の弱点を突く攻撃ではありません。突かれるのは、人の判断です。

フィッシング (phishing) は、正規の企業や信頼できる人物を装ったメールや Web サイトで、口座番号などの機微なデータを得ようとする手口です。経理担当者の例なら、取引先を名乗るメールが当てはまります。正規の相手からの連絡ではありません。

フィッシングは、狙い方と手段によって呼び名が変わります。

呼び名	内容
フィッシング (phishing)	メールや Web サイトで機微なデータを得ようとする

呼び名	内容
スパフィッシング	特定の個人や集団を狙ったフィッシング
ヴィッシング (vishing)	音声 (電話) を使うフィッシング
スミッシング (SMiShing)	SMS を使うフィッシング

スパフィッシングは、不特定多数ではなく、特定の個人や集団に絞って送ります。狙いが絞られている点が、通常のフィッシングとの違いです。

ヴィッシングとスミッシングは、メールを使いません。それでも、フィッシングの仲間に入ります。電話なら vishing、SMS なら SMiShing と覚えると、区別がつかます。

USB ベイティングは、物理的なソーシャルエンジニアリングの一つです。USB 機器をわざと置いて、拾わせます。画面の向こうの相手を、だますわけではありません。

テールゲーティング (tailgating) は、物理攻撃 (physical attacks) の一つとして、出題範囲に挙がる語です。NIST の資料は、敵対者が許可された人の後に付いて、立ち入りが制限された場所へ入る手口と説明します。目的は、施設への立ち入りを得て、物理的な検査を回避することです。ネットワーク越しの攻撃ではありません。

中間者攻撃、APT、内部者の脅威、IoC

中間者攻撃 (man-in-the-middle) は、通信する2者の間に攻撃者が入り込む攻撃です。流れるデータを傍受し、改ざんします。通信の両端が、間にいる攻撃者に気づくとは限りません。

APT (Advanced Persistent Threat) は、高度な専門性と豊富な資源を持つ敵が、複数の攻撃ベクトルを使って目的を達成しようとする攻撃です。名前の3語は、飾りではありません。

語	意味
Advanced	標的を絞り、連携し、目的を持つ (Lockheed Martin の説明)
Persistent	長い期間にわたって、目的を繰り返し追い続ける。守る側の抵抗に合わせて手を変え、目的に要るやり取りを保とうとする (NIST SP 800-39 の定義)
Threat	意図、機会、能力を持つ人物 (Lockheed Martin の説明)

内部者の脅威 (insider threat) は、1.1 でも出てきた語です。内部者が許された権限を使って害を与えます。害には、スパイ、不正な開示、資源や能力の喪失などが含まれます。外から来る攻撃だけを想定した守りは、これを防げません。

侵害の兆候 (IoC) は、攻撃が迫っている、進行中、またはすでに侵害されたことを示す、技術的な痕跡や観測です。不審な動きを疑うときの手がかりになります。IoC は、攻撃そのものではありません。

場面から攻撃を選ぶ

場面	当てはまる語	決め手
添付ファイルを開くとファイルが暗号化され、復号と引き換えに金銭を求められた	ランサムウェア	データを暗号化して身代金を要求する

場面	当てはまる語	決め手
取引先を名乗るメールで、口座番号を入力させようとした	フィッシング	信頼できる相手を装う
経理部だけを狙い、社内の事情に合わせた文面のメールが届いた	スパイフィッシング	特定の個人や集団を狙う
銀行を名乗る電話で、口座の情報を聞き出そうとした	ヴィッシング	音声を使う
宅配業者を名乗る SMS のリンクへ誘導された	スミッシング	SMS を使う
駐車場に落ちていた USB 機器を拾い、事務所のパソコンに差した	USB ベイティング	物理的にわざと置いて拾わせる
入口で、社員の後ろに付いて制限区域に入った	テールゲーティング	許可された人の後に付いて入る
通信の途中に別の機器が入り、データを傍受・改ざんした	中間者攻撃	通信する2者の間に入る
乗っ取られた多数のコンピュータから、一斉に通信が届き、サービスが止まった	DDoS、ボットネット	多数の乗っ取り機器を使い、アクセスを妨げる
権限を持つ社員が、許された権限で情報を外へ持ち出した	内部者の脅威	許された権限を使って害を与える

似た語は、何が違うかで切り分けます。トロイの木馬は、自分で複製しない点
が、ウイルスやワームと違います。ランサムウェアと DoS は、どちらもデータや

サービスを使えなくします。違うのは、金銭の要求です。ランサムウェアは復号と引き換えに身代金を求めますが、DoS は金銭の要求を定義に含みません。

ヴィッシング、スミッシング、フィッシングは、同じ系統の手口です。違いは、連絡の手段です。メールや Web サイトならフィッシング、電話ならヴィッシング、SMS ならスミッシングです。スパイフィッシングは、連絡の手段で決まる呼び名ではありません。

マルウェアの種類ごとの特徴

Cisco は、マルウェアの種類を次のように説明します。

- ウイルス: マクロに対応した文書やファイルに付き、コードを実行して、宿主から宿主へ広がる。ダウンロードしても、ファイルが開かれて使われるまでは休眠している
- ワーム: 宿主のプログラムが要らない。ダウンロードしたファイルがネットワーク接続で端末に感染し、指数関数的な速さで増えて広がる
- トロイの木馬: 役に立つソフトウェアに見せかける。自己複製するようには設計されていない
- スパイウェア: コンピューターで密かに動き、遠隔の利用者に報告する。キーロガーは、キー入力を記録して、パスワードや個人情報を明らかにする
- アドウェア: コンピューターの使用状況のデータを集め、それに合う広告を出す
- ファイルレスマルウェア: メモリ常駐のマルウェア。ハードディスクのファイルではなく、メモリから動く

ファイルレスマルウェアには、スキャンするファイルがありません。従来のマルウェアより検出が難しくなります。被害を受けたコンピューターを再起動すると、マルウェアが消えるので、フォレンジックも難しくなります。

アドウェアは、常に危険なわけではありません。ただし、場合によっては、システムに問題を起こします。

複製と広がり方で見分ける

種類	自己複製	広がるきっかけ
ウイルス	する	感染したファイルが開かれて使われる
ワーム	する	宿主のプログラムを必要とせず、ネットワークで広がる
トロイの木馬	しない	役に立つソフトウェアに見せかけて、利用者が入れる

ウイルスとワームの違いは、宿主のプログラムの要否です。ワームは宿主を必要としません。トロイの木馬は、そもそも増えるようには作られていません。

マルウェアの目的

マルウェアの目的は、情報を盗むことだけではありません。Cisco は、5つを挙げます。

- メールや計画、特にパスワードのような機微な情報を、持ち出す
- ネットワークや PC を使えなくする。人質のようにして金銭を求めるものが、ランサムウェア
- コンピューターシステムを壊して、ネットワーク基盤に損害を与える
- 計算能力を使って、ボットネットや暗号資産の採掘 (cryptojacking) を動かしたり、スパムメールを送ったりする
- 組織の知的財産を、ダークウェブで売る

場面から種類を選ぶ

場面	当てはまる語	決め手
キー入力を記録して、パスワードを明らかにする	キーロガー（スパイウェアの一種）	キー入力の記録
ハードディスクにファイルを 残さず、メモリから動く	ファイルレスマルウェア	メモリ常駐
感染したファイルが開かれる まで、休眠している	ウイルス	ファイルが使われるまで休眠
宿主のプログラムなしで、ネットワークを通じて急速に 広がる	ワーム	宿主が不要
役に立つソフトウェアに見せ かけて入り込む	トロイの木馬	自己複製しない
使用状況を集めて、広告を 出す	アドウェア	常に危険とは限らない

ランサムウェアの広がり方と備え

Cisco によると、ランサムウェアは、主に4つの経路で配られます。メールのフィッシング、悪意ある広告 (malvertising)、ソーシャルエンジニアリング、エクスプロイトキットです。感染の多くは、メールの添付ファイルか、悪意あるダウンロードで起きます (Cisco)。

身代金は、暗号資産で求められるのが一般的です。支払えば復号の鍵が届くはずですが、実際には、システムが解除されても、盗んだデータを人質にして、2度目の身代金を求める場合があり、支払えば解決するとは限りません。

備えとして、Cisco は次の点を挙げます。

- バックアップ: 攻撃を受けたら、端末の電源を落とし、イメージを入れ直し、今のバックアップを戻す
- 更新: よく悪用される第三者のソフトウェアにパッチを当てると、多くの攻撃を防げる
- 教育: セキュリティの鎖で最も弱いのは、たいてい人。誰と何を信頼してよいかを教える
- 多層の防御: エンドポイントからメール、DNS の層まで、セキュリティを通す
- アクセスの制限: 攻撃者がたどり着ける資源を絞る

DDoS の動機と標的

DDoS 攻撃は、不要な通信でネットワークを埋め尽くすように設計された攻撃です。結果は、ネットワークの性能の低下か、重要な基盤のサービスの完全な停止です (Cisco)。

DDoS の長さは攻撃によって違い、Ping of Death は短く、Slowloris は成立するまでに時間がかかります。

DDoS の動機は、サービスの妨害からスパイ活動、サイバー戦争まで広がり、狙われる分野ごとに違います。

標的	動機
オンラインゲームとギャンブル	競争上の優位や金銭的な利益
金融サービス	金銭的な利益、評判の毀損、機密データへのアクセス、妨害
政府	知的財産の窃取、業務の妨害、盗聴、スパイ、競争上の優位

標的	動機
オンライン小売	業務の妨害、競争上の優位、評判の毀損、知的財産の窃取

最近の傾向は、次の3つです。

- IoT ボットネットによる大量通信型
- サーバーの資源を使い果たさせるアプリケーション層 (L7) 型
- 暗号化された通信を使う SSL の DDoS

ソーシャルエンジニアリングの手口と備え

ソーシャルエンジニアリングの核心は、説得の心理です。対象の信頼を得て、警戒を解かせ、危険な行動を取らせます。攻撃は、全員に効く必要がありません。だまされた人が1人いれば、組織全体に及ぶ攻撃のきっかけになる情報が、手に入ります。

- スピアフィッシング: 広い集団ではなく、特定の個人を狙う
- ホエーリング: 地位の高い幹部層 (経営層) を狙う
- 水飲み場攻撃: 特定の集団が訪れそうな Web サイトを侵害して、罠を仕掛ける
- ビジネスメール詐欺 (BEC): 経営幹部になりすまし、送金などを不正な目的でさせる
- USB ベイティング: マルウェアを入れた USB メモリを、拾われそうな場所に置く

備えは、教育、方針、物理的な管理の3つです。

- 教育: 意識向上の訓練で、リスクを下げる

- 方針: VPN のような危険度の高いサービスの認証には、固定のパスワードでなく、多要素認証を使う
- 物理的な管理: 来訪者の記録、同行の義務、身元調査。物理的な攻撃は対面で起き、ヘルプデスクの担当、受付、出張の多い人が特に狙われる

[^2]

1.3 認証、認可、アカウントिंगと多要素認証 [1.3]

認証と認可は別の問いに答える

柚ノ木製作所の社員が、社員証をかざして事務棟に入るとします。扉の読み取り機が最初に確かめるのは、その社員証が本人のものかどうかです。この確認が認証 (authentication) です。認証は、利用者、プロセス、機器の身元を確かめることを指します。資源へのアクセスを許す前提になる手順であり、許可そのものではありません。

認証に成功しても、どの部屋にも入れるわけではありません。次に決めるのは、その社員がどこまで入ってよいかです。これが認可 (authorization) です。認可は、利用者やプログラムやプロセスに与えるアクセス権を指し、アクセスを許すか拒むかの判断も含みます。

用語	答える問い	事務棟の例
認証	身元は確かか	社員証が本人のものと確かめる
認可	何を許すか	入ってよい部屋を決める

先に身元を確かめ、次に許す範囲を決める順序で覚えると、取り違えを防げます。身元が不明なまま、範囲だけを決めることはありません。

AAA の3つ目、アカウントティング

AAA は、認証 (Authentication)、認可 (Authorization)、アカウントティング (Accounting) の頭文字です。アカウントティングは、誰が何をしたかを記録する役割です。認証と認可だけでは、記録は残りません。

アカウントティングで残す記録が、監査ログ (audit log) です。特定の出来事の証拠となる記録を指します。事務棟の例なら、誰がいつ扉を通ったかの記録に当たります。記録は、アクセスを防ぐ仕組みではありません。

RADIUS と TACACS+

RADIUS は、認証、認可、設定情報を、ネットワークアクセスサーバーと共有の認証サーバーの間で運ぶ仕組みで、UDP を使います。TCP は使いません。

項目	RADIUS	TACACS+
使うプロトコル	UDP	TCP
ポート	認証は UDP 1812、アカウントティングは 1813	サーバーは TCP 49

2つを見分ける手がかりは、使うプロトコルが UDP か TCP かです。ポート番号は、表のとおりです。

802.1X、ACL、UAC

アクセスを制御する仕組みとして、次の3つが出てきます。

- 802.1X: ポート単位のネットワークアクセス制御の規格 (IEEE)
- アクセス制御リスト (ACL): 資源にアクセスしてよい主体と、それぞれに許すアクセスの種類を並べて、アクセス制御を実装する仕組み

- UAC (ユーザーアカウント制御): 標準ユーザーを超える権限が要るアプリを、管理者トークンで実行させる Windows の仕組み

ACL は、認可の内容を一覧にしたものです。誰に何を許すかを、並べて書きます。許していない相手は、一覧に載りません。

多要素認証とパスワードポリシー

多要素認証 (MFA) は出題範囲に挙がる語で、CISA は MFA を求めることを推奨しています。

パスワードポリシー (password policies) も出題範囲に挙がる語です。NIST SP 800-63B-4 の定めが、現在の考え方を示しています。

- 単一要素の認証にパスワードを使う時は、最低 15 文字を求める
- 多要素認証の一部としてだけ使うパスワードは短くてよいが、最低 8 文字は求める
- 大文字や数字などの組み合わせを強制する規則は課さない
- 定期的な変更を求めない。侵害の証拠がある時は変更させる
- 漏えいしたパスワード、辞書の語、連続や反復の文字などの禁止リストと照らす

文字数の基準は、使い方で2つに分かれます。パスワードだけで認証するなら、15 文字以上です。多要素認証の一部なら、8 文字以上です。他の要素が加わる分、短い基準で足ります。

NIST SP 800-63B-4 は、記号などの組み合わせの強制も、定期的な変更も求めません。変更させるのは、侵害の証拠がある時です。

代わりに行うのが、漏えいしたパスワード、辞書の語、連続や反復の文字などの禁止リストとの照合です。組み合わせの強制や定期変更は、この定めの手

段に入っていません。

場面から用語を選ぶ

場面	当てはまる語	決め手
利用者が名前とパスワードで、身元を確かめられる	認証	身元を確かめる
確かめた利用者に、閲覧だけを許し、編集は許さない	認可	与えるアクセス権を決める
誰がいつ何をしたかの記録を、あとで調べる	アカウントティング、監査ログ	出来事の証拠となる記録
認証サーバーとの通信に、UDP の 1812 番を使う	RADIUS	認証の宛先ポートが UDP 1812
認証サーバーとの通信に、TCP の 49 番を使う	TACACS+	TCP を使い、ポートは 49
接続口ごとに、ネットワークに入る前に身元を確かめる	802.1X	ポート単位のアクセス制御
管理者トークンで、特別な権限が要るアプリを実行する	UAC	権限が要るアプリだけ引き上げる

パスワードの基準は、数字を覚えるだけでは足りません。何に使うパスワードかで、数字が変わります。パスワードだけで認証するなら、最低 15 文字です。多要素認証の一部なら、最低 8 文字です。定期的な変更は求めません。侵害の証拠があるときだけ、変更させます。

認証と認可は、取り違えやすい組です。身元の確認なら認証、許す範囲の決定なら認可です。順番は、認証が先です。認可が先に来ることはありません。

RADIUS と TACACS+ の使い分け

RADIUS は、リンクの認証を求めるネットワークアクセスサーバーと、共有の認証サーバーの間で、認証、認可、設定情報を運ぶ仕組みです (RFC 2865)。初期の実装は UDP の 1645 番を使っていましたが、同じ番号を使う別のサービスとぶつかりました。正式に割り当てられた番号は、認証が 1812 番、アカウンティングが 1813 番です。

TACACS+ は、ルーター、ネットワークアクセスサーバーなどの機器の管理 (Device Administration) に、広く使われています。設計の要は、認証、認可、アカウンティングを分けることです (RFC 8907)。分けておくと、セッションの中の個々のコマンドに対して、認可とアカウンティングを行えます。3つすべてを使う必要はありません。

項目	RADIUS	TACACS+
主な用途	ネットワークアクセスサーバーと認証サーバーの間で、認証、認可、設定情報を運ぶ	ルーターなどの機器の管理
認証、認可、アカウンティング	認証と認可の情報を一緒に運ぶ	3つを分けて扱う
トランスポート	UDP	TCP

管理者が機器にログインして打つコマンドを、1つずつ許可したり、記録したりしたい場面では、TACACS+ が向いています。理由は、認可とアカウンティングを個々のコマンドに対して行えるからです。

多要素認証の方式の強さ

多要素認証 (MFA) は、利用者の身元を確かめる方法を、2つ以上求めて、保護の層を足す仕組みです (CISA)。どの MFA も、無いよりは優れています。ただ

し、守る強さは同じではありません。

CISA は、強い順に、次の5つを挙げます。

1. 物理的なセキュリティキー: 端末に差すか、かざして、ログインする。フィッシングへの防御が最も強い
2. 数字の一致を求める認証アプリ: アプリが通知を送り、ログイン画面に出る数字を入力して確認する
3. ワンタイムコードの認証アプリ: アプリが 30 秒ごとに新しいコードを作る
4. 生体認証: 指紋や顔で身元を確かめる。多くは端末ごとの認証で、別の方法と組み合わせるのがよい
5. テキストまたはメールのコード: 一時的なコードを、電話かメールに送る。最も身近だが、保護は最も弱い

導入は、管理者のアカウントと、機微なデータを扱う従業員から始めます。メール、ファイルの保管、リモートアクセスのような仕組みで、MFA を有効にします(CISA)。

場面で考える

柚ノ木製作所の社内ネットワークに、私物のスマートフォンを接続する場面を考えます。接続の前に、社員が名前とパスワードを入力します。ここで身元が確かめられるので、これが認証です(身元の確認)。確かめられた社員が、人事のファイルサーバーを閲覧できず、営業のファイルだけを閲覧できるなら、認可の働きです。誰がいつ営業のファイルを開いたかが、監査ログに残るなら、アカウントिंगの働きです。

社内の規則を見直す場面です。パスワードを、英字、数字、記号を混ぜて8文字以上とし、3か月ごとに変更させる規則があるとします。NIST SP 800-63B-4

の考え方に照らすと、見直す点は3つあり、どれも現在の考え方に合っていない。文字の組み合わせを強制していること、定期的な変更を求めていること、パスワードだけで認証するのに最低 15 文字を求めているいないことです。

認証サーバーとの通信が UDP の 1812 番なら RADIUS、TCP の 49 番なら TACACS+ です。[^3]

1.4 暗号化、ハッシュ、証明書 [1.4]

暗号化と2つの鍵の方式

蒼波システムズの担当者が、取引先へ見積書を送るとします。中身を変換して送れば、途中で盗み見られても読めません。この変換が暗号化(encryption)です。元の意味が分かる文を平文と呼び、意味を隠した文を暗号文と呼びます。逆の変換は復号です。暗号化は、データを消す操作ではありません。

暗号の方式は、鍵の使い方で2つに分かれます。共通鍵(対称鍵)暗号と、公開鍵(非対称)暗号です。

方式	鍵の数	使い方
共通鍵(対称鍵)暗号	1つ	許された当事者で共有する秘密の鍵を使い、暗号化にも復号にも同じ鍵を使う
公開鍵(非対称)暗号	2つ	一方で暗号化(または署名)し、もう一方で復号(または署名の検証)する

共通鍵暗号では、送る側と受ける側が、同じ秘密の鍵を持ちます。鍵を持たない人には、暗号文を元に戻せません。鍵は、許された当事者の間でだけ共有します。

公開鍵暗号は、別々の2つの鍵を使います。一方の鍵で暗号化したものは、もう一方の鍵で復号します。署名の場合は、一方の鍵で署名し、もう一方の鍵で署名を検証します。共通鍵のように、1つの鍵で両方を行うことはありません。

ハッシュ関数

ハッシュ関数は、出力の長さが固定の関数です。入力の変化があっても、出力の長さは変わりません。一方向性という性質を持つように設計されています。一方向性とは、出力から入力を見つけるのが計算上困難なことです。暗号化とは違い、元に戻す操作はありません。

ハッシュ関数の規格は FIPS 180 が定め、SHA-1 と、SHA-2 系の SHA-224 や SHA-256 などが載っています。

強い暗号と弱い暗号

強度の高い暗号化アルゴリズムと、強度の低い暗号化アルゴリズムの区別が、出題範囲の語です。強度の低い例が、2鍵の Triple DES (TDEA) です。NIST は SP 800-131A で、この方式の使用を認めていません (disallowed)。通信の暗号にも、使わない版があります。RFC 9325 の推奨は、TLS 1.0 と 1.1 を使わないことです。方式が動いているからといって、使い続けてよいとは限りません。

公開鍵証明書と PKI

公開鍵を受け取る側は、その鍵が本当に相手のものかを知る必要があります。その結び付けを保証するのが、公開鍵証明書です。公開鍵と、その持ち主を結び付けたデータで、認証局 (CA) が署名します。

PKI (公開鍵基盤) は、公開鍵証明書を発行し、維持し、失効させるための枠組みです。証明書を1枚発行するだけの仕組みではありません。

データの3つの状態と、暗号を使う仕組み

データは、置かれた状態で3つに分かれ、状態ごとに適した暗号化があります。

- 保存データ (data at rest)
- 送信中データ (data in transit)
- 使用中データ (data in use)

保存データの保護には、ドライブ全体やボリュームを暗号化する機能を使います。Windows の BitLocker と、macOS の FileVault が、その例です。

送信中のデータを守る、暗号を使うプロトコルは、次のとおりです (protocols that use encryption)。

- TLS 1.3: 通信の盗聴、改ざん、なりすましを防ぐ、通信路の暗号の規格 (RFC 8446)
- SSH: 安全なリモートログインなどのための規格。サーバーは TCP ポート 22 で待ち受ける
- IPsec: 認証ヘッダー (AH) と暗号化ペイロード (ESP) の2つのプロトコルを持つ
- DoH (DNS over HTTPS): DNS の問い合わせを HTTPS で運ぶ (RFC 8484)
- HSTS (HTTP Strict Transport Security): HTTPS を強制する仕組み (RFC 6797)
- WPA3: より強い認証と暗号の強さを持つ Wi-Fi の暗号の規格 (Wi-Fi Alliance)

IPsec の2つは、名前で役割を覚えます。認証ヘッダー (AH) は認証、暗号化ペイロード (ESP) は暗号化です。

BitLocker と FileVault は、通信を守る仕組みではありません。ディスクの中のデータを守ります。通信の暗号は、TLS や SSH が受け持ちます。

場面から方式を選ぶ

場面	当てはまる語	決め手
送る側と受ける側が、同じ秘密の鍵を共有して暗号化と復号をする	共通鍵 (対称鍵) 暗号	暗号化と復号に同じ鍵
一方の鍵で暗号化し、もう一方の鍵で復号する	公開鍵 (非対称) 暗号	2つの別の鍵
出力から入力を見つけるのが、計算上困難な関数	ハッシュ関数	一方向性
公開鍵と持ち主を結び付け、認証局が署名したデータ	公開鍵証明書	認証局 (CA) の署名
Windows のドライブ全体を暗号化する	BitLocker	保存データの保護
macOS のボリュームを暗号化する	FileVault	保存データの保護
通信路の盗聴、改ざん、なりすましを防ぐ	TLS	通信路の暗号の規格
DNS の問い合わせを HTTPS で運ぶ	DoH	DNS over HTTPS
HTTP でなく HTTPS を強制する	HSTS	HTTP Strict Transport Security

場面	当てはまる語	決め手
Wi-Fi の暗号を、より強い認証と暗号の強さにする	WPA3	Wi-Fi の暗号の規格

暗号化とハッシュは、取り違いやすい組です。暗号化は、復号という逆の操作で、元の平文に戻せます。ハッシュ関数は、元に戻すことを前提にいません。

共通鍵と公開鍵は、鍵の数で見分けます。鍵が1つで、暗号化にも復号にも同じ鍵を使うなら、共通鍵です。2つの別の鍵を使うなら、共通鍵ではありません。

保存データを守る:BitLocker と FileVault

BitLocker は、ボリューム全体を暗号化する Windows の機能です。紛失、盗難、不適切な廃棄から、データの盗難や露出を防ぎます。ハードウェアの TPM (Trusted Platform Module) と一緒に使うと、保護が最大になります。通常の起動を、PIN の入力か、起動キーを入れたリムーバブル機器が示されるまで止めることもできます (Microsoft の説明)。

TPM のない機器では、起動キーかパスワードを使います。パスワードの方法は安全ではありません。総当たりの攻撃を受けやすく、ロックアウトの仕組みがないからです。推奨されず、既定では無効です。

FileVault は、Mac に組み込まれた暗号化の機能で、保存データをすべて守ります。AES-XTS の暗号化アルゴリズムで、内蔵と取り外し可能な記憶装置のボリューム全体を保護します。FileVault を有効にする前に追加して消したデータは、暗号化されていません。フォレンジックの復元ツールで復元できる場合があります。

有効なログインの資格情報か、暗号の復旧キーがなければ、記憶装置を取り外して別のコンピューターにつないでも、内蔵ボリュームは暗号化されたままです。

通信を守る：TLS、DoH、HSTS、WPA3

TLS は、クライアントとサーバーのアプリケーションが、盗聴、改ざん、メッセージの偽造を防げる形で、インターネット越しに通信するための規格です (RFC 8446)。DoH は、DNS の問い合わせと応答の組を、1つずつ HTTP のやり取りに対応させて、HTTPS で運びます (RFC 8484)。HSTS は、Web サイトが、安全な接続だけでアクセスできると宣言する仕組みです。宣言には、Strict-Transport-Security という HTTP の応答ヘッダーを使います (RFC 6797)。

WPA3-Personal の利用者は、パスワードの推測による攻撃への保護が強まります。Wi-Fi Enhanced Open は、認証のない暗号化を、利用者に提供します。何の保護もなかった従来のオープンなネットワークより、前進した形です (Wi-Fi Alliance)。保護された管理フレーム (PMF) は、管理フレームに保護を広げます。ユニキャストは盗聴と偽造から、マルチキャストは偽造から守られます。

場面から保護を選ぶ

場面	当てはまる語	決め手
ノート PC を紛失した。ディスクを別の機器につないでも、中身を読ませたくない	ドライブ全体の暗号化 (BitLocker、FileVault)	保存データの保護
Web ブラウザーとサーバーの間の通信を、盗聴や改ざんから守る	TLS	通信路の暗号
DNS の問い合わせを、HTTPS で運ぶ	DoH	RFC 8484

場面	当てはまる語	決め手
ブラウザーに、HTTPS のみで接続するよう守らせる	HSTS	Strict-Transport-Security ヘッダー
公共の Wi-Fi で、パスワードなしでも通信を暗号化したい	Wi-Fi Enhanced Open	認証のない暗号化
IPsec で、通信の内容を暗号化する	暗号化ペイロード (ESP)	AH は認証の側

IPsec の AH と ESP の違い

IPsec のセキュリティプロトコルは、2つです (RFC 4301)。

プロトコル	提供するもの
認証ヘッダー (AH)	完全性と、データの送信元の認証。再送の防止は、受け手の判断で選べる
暗号化ペイロード (ESP)	AH と同じサービスに加えて、機密性

ESP で機密性だけを提供し、完全性を付けない使い方は、推奨されません。AH には機密性がありません。通信の中身を隠したいなら、ESP を選びます。

SSH とバージョンの古い暗号

SSH は、安全でないネットワーク越しに、安全なリモートログインなどのサービスを提供するプロトコルです (RFC 4253)。強い暗号化、サーバーの認証、完全性の保護を提供します。鍵交換の方法、公開鍵のアルゴリズム、共通鍵の暗号アルゴリズム、メッセージ認証のアルゴリズム、ハッシュのアルゴリズムは、すべて交渉で決まります。

RFC 9325 は、TLS 1.0 と TLS 1.1 を、交渉してはならないと定めます。TLS 1.0 は、現代の強い暗号スイートの多くを支えられません。TLS 1.1 は、TLS 1.0 よりも改善されていますが、TLS 1.2 で標準になった、より強い暗号スイートの一部を支えられません。実装は、TLS 1.2 を支える必要があります。

NIST SP 800-131A は、2 鍵 TDEA での暗号化を、使用を認めない (disallowed) としています。復号は、従来の使い方としてなら認められます。使用を認めない方式と、従来の使い方としてなら認められる方式は、同じ扱いではありません。

場面から方式を選ぶ

場面	当てはまる語	決め手
IPsec で、完全性と送信元の認証だけを提供する	認証ヘッダー (AH)	機密性はない
IPsec で、機密性まで提供する	暗号化ペイロード (ESP)	AH と同じサービスに加えて機密性
2鍵 TDEA での暗号化	使用を認めない (disallowed)	NIST SP 800-131A
2鍵 TDEA での復号	従来の使い方としてなら認められる	legacy use
TLS 1.0 と TLS 1.1 を交渉してよいか	交渉してはならない	RFC 9325

[^4]

サンプルはここまでです

続き(第2章～巻末)は、CCST サイバーセキュリティ 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

CCST サイバーセキュリティ 学習用テキスト(無料サンプル)

版

2026年10月版(Cisco「CCST Cybersecurity Objective Domains」(100-160・公式 PDF の作成日 2023-01-24・版番号の記載なし・2026-10-09 取得)準拠)

発行

IT資格道場(<https://www.shikaku-doujou.com>)

お問い合わせ

info@shikaku-doujou.com

Cisco、Cisco Systems、CCST は、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は公式の出題範囲の内容を基に作成したもので、Cisco との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。