IT資格道場

CompTIA PenTest+ 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)

CompTIA PenTest+ (PT0-003) Exam Objectives Version 5.0 準拠
2026年11月版

SAMPLE

© IT資格道場｜無料サンプル｜転載・再配布・AI学習利用禁止

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。

SAMPLE

目次

この教材の狙いと PenTest+ の性格

第1章 Engagement Management [1.1/1.2/1.3/1.4/1.5]

規制・フレームワーク・標準 [1.1]

交戦規約（Rules of engagement） [1.1]

契約文書の種類 [1.1]

対象の選定 [1.1]

診断の種類 [1.1]

共有責任モデル [1.1]

法的・倫理的な配慮 [1.1]

協働とコミュニケーション [1.2]

OSSTMM・CREST・PTES [1.3]

MITRE ATT&CK・OWASP Top 10・OWASP MASVS [1.3]

Purdue model [1.3]

脅威モデリングのフレームワーク [1.3]

書式の整合・文書の仕様・リスクの採点 [1.4]

定義 [1.4]

報告書の構成要素 [1.4]

テストの制限と前提 [1.4]

報告の際の配慮 [1.4]

技術的な管理策（その1） [1.5]

技術的な管理策（その2） [1.5]

管理的な管理策 [1.5]

運用的な管理策 [1.5]

物理的な管理策 [1.5]

管理策を選ぶ手順 [1.5]

SAMPLE

サンプルはここまでです

SAMPLE

3 冊の使い方は、ダウンロード欄の案内を参照してください。

SAMPLE

この教材の狙いと PenTest+ の性格

このテキストの目的は、ペネトレーションテスト（侵入診断）の資格 **CompTIA PenTest+** の合格です。試験コードは PT0-003（V3）で、出題範囲は公式の Exam Objectives Version 5.0 に沿っています。

項目	内容
問題数	最大 90 問
時間	165 分
合格点	750（100〜900）
問題の形	択一・複数選択・ドラッグアンドドロップ・パフォーマンスベース問題（PBQ）

試験の条件は公式ページに出ています。[1]

5 つの章は、公式の 5 つの分野と同じ順に並べました。

章	分野	配点
第 1 章	Engagement Management	13%
第 2 章	Reconnaissance and Enumeration	21%
第 3 章	Vulnerability Discovery and Analysis	17%
第 4 章	Attacks and Exploits	35%
第 5 章	Post-exploitation and Lateral Movement	14%

SAMPLE

読み方の目印は次の 3 つ。

- 出題の形：場面を読み、手順・道具・管理策を選ぶ問いが中心
- 章の冒頭：その分野の配点（重い分野から固めると点が伸びる）
- 見出しの末尾：公式の出題範囲の細目の番号（例：[4.3]）

この教材は、診断を許可された側に立って書いています。攻撃の名前、見分け方、道具の役割、守る側の対策と報告書での勧め方が中心です。

SAMPLE

第1章 Engagement Management [1.1/1.2/1.3/1.4/1.5]

エンゲージメント管理は、PT0-003 の出題の13%を占める分野です。攻撃の腕は問われません。診断を始める前の取り決め、依頼主とのやり取り、フレームワークの使い分け、報告書の中身、改善策の選び方が出題の中心です。

設問の多くは場面問題です。「この状況で最初にやるべきことはどれか」「この指摘にはどの対策が合うか」という形で、手順の順序と管理策の分類を判断します。語句の暗記だけでは足りません。各節に置いた場面の例まで読み、自分の言葉で答えを出す練習をしてください。

規制・フレームワーク・標準 [1.1]

診断の範囲と進め方は、依頼主が従う規制や基準に左右されます。細目はこれを Privacy と Security の2つに分けています。[2]

Privacy 側は、個人情報の扱いを縛る法令です。EU の GDPR、米国の医療情報を扱う HIPAA、日本の個人情報保護法が代表例です。診断中に個人情報を見つけたとき、どこに保存し、誰に見せ、いつ消すかをこの種の法令が決めます。

GDPR には、診断に直接関わる条文があります。管理者は個人データの侵害に気付いてから72時間以内に監督当局へ通知しなければなりません。処理者は侵害を知ったら遅滞なく管理者へ知らせる決まりです。[3]

診断会社が依頼主のデータを処理する立場なら、侵害の兆候を見つけた時点で依頼主へ伝える動きが要ります。72時間の時計は、依頼主が侵害を知った時点から進みます。

SAMPLE

Security 側は、対策そのものを求める基準です。PCI DSS（カード情報）、ISO/IEC 27001、NIST の各文書、業界のガイドラインが当たります。基準が定期的な侵入テストを求めていれば、依頼の動機は「準拠の証明」にほかなりません。基準が求める範囲と頻度は、スコープから外せません。

試験では、依頼元がどの規制に縛られるかを業種とデータから読み取らせます。決済カードを扱うなら PCI DSS、EU 居住者の個人データなら GDPR、医療情報なら HIPAA という具合です。規制名が文中に書かれているとは限りません。データの種類から逆算してください。

交戦規約（Rules of engagement）[1.1]

交戦規約（ROE）は、診断で何をしてよく、何をしてはいけないかを決めた合意文書です。細目は、次の4つの要素を挙げています：

要素	決める中身	例
Exclusions（除外）	触れてはいけない対象や手法	本番の決済DB、DoS攻撃、特定の役員の端末
Test cases（テストケース）	実施する試験の種類と深さ	パスワードスプレー、フィッシング、物理侵入の可否
Escalation process（エスカレーション手順）	想定外の事態が起きたときの連絡と判断	連絡先の順番、連絡までの時間、停止の権限者
Testing window（テスト時間帯）	試験してよい日時	平日の22時から翌5時、月末の締め処理期間は除く

エスカレーション手順が動く代表的な場面は、次のようなときです。診断中にシステムが落ちたとき。スコープ外の資産に到達したとき。すでに別の攻撃者に侵入された痕跡を見つけたとき。重大な脆弱性を見つけたときです。いずれ

SAMPLE

も、テスターは自分の判断で先へ進まず、ROE に書かれた連絡先へ知らせて指示を待ちます。

この動きを手順にすると、次の順になります。

1. 試験を止める
2. 状況を記録する（時刻、直前の操作、観察した症状）
3. ROE の連絡先へ、定められた手段と時間内に伝える
4. 依頼主の指示を受けるまで、再開しない

場面で確かめます。依頼主の営業時間外（22時から5時）だけが許された環境で、23時に診断対象の Web サーバーが応答しなくなったとします。正しい動きは、試験を止め、ROE の連絡先に電話などで即座に伝え、直前の操作を記録することです。復旧を待たずに別の対象へ移るのは誤り。自分でサーバーを再起動するのも誤りです。再起動は依頼主の権限に属する操作だからです。

別の場面です。ROE のテストケースにフィッシングが含まれていないのに、テスターが「効果的だから」と従業員へ疑似メールを送ろうとしています。ROE にない試験は実施できません。必要なら変更の合意を書面で取り直し、その後に実施します。

スコープ外への到達も同じです。内部ネットワークの診断中に、依頼主の関連会社のサーバーへ通じる経路が見つかったとします。その先は ROE に書かれていないので、触れません。見つけた事実を、エスカレーションの連絡先へ報告するだけです。関連会社が同じグループでも、別法人なら別の認可が要ります。

テスト時間帯では、タイムゾーンも決めます。依頼主が日本、テスターが米国にいるなら、「22時」がどちらの時刻かで食い違います。時刻の基準が文書になければ、この食い違いは防げません。

SAMPLE

契約文書の種類 [1.1]

診断に関わる契約文書は4つあります。名前が似ているため、次の役割で区別します：

文書	役割	覚え方
NDA（秘密保持契約）	診断で知った情報を外へ出さない約束	診断前に結ぶことが多い
MSA（基本サービス契約）	取引全体の共通条件。支払い、責任の上限、知的財産、秘密保持など	同じ会社と何度も仕事をする入れ物
SoW（作業範囲記述書）	その案件の作業内容、成果物、期間、金額	案件ごとに作る個別の約束
ToS（利用規約）	あるサービスを使う条件	相手が決めた条件に同意する形

関係は階層です。MSA が枠になり、その下に案件ごとの SoW がぶら下がります。MSA と SoW の内容が食い違ったときの優先順位は、契約書の条項でしか決まりません。

ToS が診断に関わるのは、対象が他社のサービスの上で動いているときです。クラウドや SaaS の利用規約は、利用者がそのサービスに対して行えるセキュリティ試験の範囲を縛ります。依頼主の同意だけでは、他社の基盤への攻撃が許可されたことになりません。

案件の開始までの順序は、おおむね次のとおりです。

1. 初回の打ち合わせで目的と対象を確認する
2. NDA を結び、機密情報のやり取りを可能にする
3. MSA（まだなければ）と、案件ごとの SoW を取り交わす

SAMPLE

4. ROE を決め、スコープを確定する
5. 認可書に署名をもらう
6. 開始会議（キックオフ）を開いて、連絡先と日程を確認する

試験では「新しい案件の作業範囲と成果物を定めるのはどれか」なら SoW、「複数案件に共通する支払い条件を定めるのはどれか」なら MSA と答えます。診断で得た機密データの扱いが論点なら NDA です。SoW が先で NDA が後、という並べ替えは誤りです。機密情報を渡す前に NDA が要ります。

対象の選定 [1.1]

スコープに載せる対象は、書き方ひとつで意味が変わりかねません。細目は CIDR 範囲、ドメイン、IP アドレス、URL の4つを挙げています。

CIDR 範囲は、IP アドレスをまとめて指定する書き方です。範囲の大きさと境界は、手計算でも出せなければなりません。python3 で確かめた例です。

```
import ipaddress
n = ipaddress.ip_network("203.0.113.0/26")
print(n.num_addresses, n.network_address, n.broadcast_address)
print(ipaddress.ip_address("203.0.113.70") in n)
```

実行結果は `64 203.0.113.0 203.0.113.63` と `False` です。/26 は64個のアドレスを含みます。203.0.113.70 は範囲に入りません。

同じ要領で、10.20.0.0/22 は1024個で、10.20.0.0 から 10.20.3.255 までです。10.20.4.1 は範囲の外。ホストに割り当てられる数は、先頭のネットワークアドレスと末尾のブロードキャストアドレスを除くので、/26 なら62個です。

SAMPLE

/24 を /26 に4分割すると、192.0.2.0/26、192.0.2.64/26、192.0.2.128/26、192.0.2.192/26 になります。依頼主が「この /24 のうち前半の2つだけ」と言うなら、192.0.2.0 から 192.0.2.127 まで、つまり 192.0.2.0/25 に当たります。

境界を読み違えると、許可のない隣接ネットワークへ通信が飛びます。スキャンの設定で範囲を1つ広げただけでも、許可のない通信は止められません。実行する前に、ターゲット一覧を契約書のスコープと突き合わせます。

ドメインは、ワイルドカード（`*.example.com`）で書かれるとサブドメインがすべて対象になります。ただし、サブドメインが第三者のサービス（外部の SaaS など）を指す場合があります。名前が依頼主のものでも、その先の実体が他社のものなら、依頼主の許可では足りません。

IP アドレスは、1つの IP に複数のサイトが同居する共有ホスティングで問題になります。依頼主のサイトだけが対象でも、同じ IP の他社サイトに影響が及ぶおそれがあります。始める前に、同居先への影響を避ける手立て（試験の方法・ホスティング事業者の許可）があるかを確かめます。

URL は、パスまで区切って許可できる最も細かい指定です。`https://app.example.com/shop/` を許可しても、同じホストの `/admin/` が含まれるとは限りません。パスやポートの扱いは、文書で確定させます。

場面で確かめます。スコープは 203.0.113.0/26 です。診断中に、同じ会社の名前を持つ 203.0.113.70 のサーバーが見つかったとします。範囲の外なので、触れません。エスカレーションの連絡先へ伝え、範囲の追加が必要なら、SoW や認可書の更新を受けてから試験します。

診断の種類 [1.1]

診断の種類は、対象のどの層を調べるかで分けます。細目は7種類です。

SAMPLE

種類	調べる対象	典型の論点
Web	Web アプリケーション	入力値の検証、認証、セッション管理
Network	ホストとサービス、ネットワーク機器	開いたポート、古いサービス、設定不備
Mobile	iOS と Android のアプリ	端末内の保存データ、通信の保護
Cloud	クラウドの設定と権限	公開ストレージ、過剰な権限、事業者の規約
API	アプリが公開する API	認可の不備、レート制限、過剰なデータ返却
Application	厚いクライアントなどの実行ファイル、ソースコード	古いライブラリ、秘密情報の埋め込み
Wireless	Wi-Fi、Bluetooth などの無線	暗号化方式、偽アクセスポイント

Wireless は、電波が壁を越える点が落とし穴です。依頼主のオフィスで無線を調べると、隣のテナントの Wi-Fi が見えてしまうことも珍しくありません。スコープに載っていない SSID は、見えても攻撃しません。

Cloud は、ROE や契約に加えて、クラウド事業者のテスト規約が上乗せされます。次の共有責任モデルの節で扱います。

Web と API の違いは、画面の有無です。API は画面を持たない窓口で、リクエストを直接送って調べます。あるユーザーの ID を別のユーザーの ID に書き換えて他人のデータが読めるなら、認可の不備（IDOR）の指摘と見て間違いありません。

SAMPLE

Mobile は端末内に残るデータと通信の保護を調べ、Application はスマートフォン以外の実行ファイルやコードを調べます。どの層を見るのかは、名前から読み取れなければなりません。

共有責任モデル [1.1]

共有責任モデルは、クラウドなどの外部サービスで、誰が何を守るかを分けた考え方です。細目は、次の4者を挙げています：

立場	責任の中身
Hosting provider（ホスティング事業者）	データセンター、物理設備、仮想化基盤など、事業者が運用する層
Customer（利用者）	自分で設定する OS、アプリ、アカウント、データ、アクセス権限
Penetration tester（テスター）	スコープと規約を守る、データを適切に扱う、結果を正確に報告する
Third party（第三者）	依頼主が使う外部サービス（SaaS、CDN、運用委託先）の運営者。自分の層は自分が守る

事業者のテスト規約が、この分担を具体化します。AWS は、許可リストに載ったサービス（EC2、RDS、Lambda、API Gateway、CloudFront など）について、事前承認なしで利用者が侵入テストをしてよいとしています。一方で、DoS と DDoS（模擬を含む）、ポートやリクエストのフラッディング、Route 53 を使った DNS ゾーンウォーキングは禁止です。ツールが DoS を起こさないように設定する責任は利用者にあります。テストで AWS や他の利用者に与えた損害も、利用者が負わなければなりません。[4]

SAMPLE

Microsoft も同じ方向です。テストは自分のテナントと資産の中で行い、DDoS は常に禁止です。他者のデータやシステムへの許可のないアクセスは認められません。誤って権限のないデータに触れたら、直ちに止めます。そのうえで同社へ連絡し、データを消し、報告書にその旨を書く決まりです。発見した脆弱性を概念実証より先へ使う行為も禁止されています。[5]

場面で確かめます。依頼主の EC サイトが AWS の EC2 で動いていて、診断で「負荷に耐えられるか」を試したいという要望が出たとします。EC2 への侵入テスト自体は事前承認が要りません。しかし負荷を大量にかける試験は、DoS 禁止の範囲に入ります。テスターは試験項目から外すか、事業者が別に用意する手続きを確かめます。依頼主の同意だけで進めてはいけません。

別の場面です。依頼主のアプリが外部の決済 SaaS の API を呼んでいて、診断の過程で SaaS 側の脆弱性が疑われたとします。決済 SaaS は第三者です。攻撃的な試験を行うには、その運営者の許可が要ります。依頼主の許可は、依頼主の資産にしか効きません。

責任の割り振りは、層で考えると解けます。物理やハイパーバイザは事業者。OS やアプリの設定と権限は利用者。テスターは自分の行動に責任を持ちます。クラウドの種類（IaaS、PaaS、SaaS）で利用者の持ち分は変わり、SaaS ほど事業者の持ち分が増えます。

法的・倫理的な配慮 [1.1]

細目は3つを挙げています。

Authorization letters（認可書）は、診断を許可する権限を持つ者が署名した文書です。資産の所有者（または所有者の権限を持つ代表者）が、診断する会社と人、対象、期間、連絡先を書いて署名しなければ、認可書として成立しま

SAMPLE

せん。入口で警備に呼び止められたとき、攻撃を検知した SOC が通報の前に確認するときに、これを見せなければ、診断だと証明できません。

署名者の権限が肝心です。同じ会社の情報システム部門が署名しても、対象が別会社の資産なら権限がありません。クラウドや委託先の設備なら、その所有者の認可も要ります。

Mandatory reporting requirements（報告義務）は、法令や契約で、見つけた事実を特定の相手へ知らせる義務です。典型は、診断中に違法なコンテンツや進行中の犯罪の証拠に出くわしたケースです。テスターは試験を止め、それ以上探さず、ROE や契約に書かれた連絡先と、法令が定める当局へ知らせます。自分で収集や分析を続けてはいけません。前述の GDPR の72時間のような通知期限も、この類型に入ることが珍しくありません。

Risk to the penetration tester（テスター自身のリスク）は、許可なく動いたときの法的責任と、安全上の危険です。日本の不正アクセス禁止法は、他人の識別符号を使うなどの不正アクセス行為を禁止し（第3条）、違反に3年以下の拘禁刑または100万円以下の罰金を科します（第11条）。[6] 米国の連邦法 18 U.S.C. § 1030（CFAA）は、許可なく、または許可された範囲を超えて保護されたコンピュータへアクセスすることを犯罪としています。[7]

つまり、認可書の範囲を超えた瞬間に、診断は不正アクセスに変わりえます。物理侵入の診断では、警備員や警察に拘束される危険もあるので、認可書を持ち歩き、緊急連絡先を決めておきます。

倫理面の基本は3つです。見つけた情報を診断の目的以外に使わないこと。スコープ外で見えたものを持ち出さないこと。結果を偽らないことです。

場面で確かめます。物理侵入の診断で、テスターがサーバー室に入った直後に警備員に止められました。まず認可書を示し、書かれた緊急連絡先に確認

SAMPLE

してもらいます。逃げる、隠れる、警備員を説得して先に進む、のいずれも誤りです。

協働とコミュニケーション [1.2]

診断は、依頼主との継続的なやり取りの上で進みます。細目は9項目を挙げています。[2] 関連する項目は、次の表で対応づけて覚えます：

項目	中身	試験での見分け方
Peer review	別のテスターが結果と報告書を点検する	誤検知や記載ミスを提出前に減らす
Stakeholder alignment	関係者の目的と期待を揃える	開始時と進行中の合意形成
Root cause analysis	脆弱性が生まれた原因を掘り下げる	症状ではなく根本原因を報告に載せる
Escalation path	問題が起きたときの連絡経路	誰に、どの順で、いつまでに
Secure distribution	報告書を安全に渡す	暗号化、アクセス制限、受信者の限定
Articulation of risk, severity, and impact	リスク、深刻度、影響を相手に伝わる言葉で説明する	読み手ごとに言い方を変える
Goal reprioritization	診断中の目標の組み替え	変更の合意を文書化する
Business impact analysis	事業への影響の分析	事業の重要度で指摘の優先度を決める
Client acceptance	依頼主が成果物を受け入れる	署名や承認で完了とする

SAMPLE

Root cause analysis は、同じ種類の指摘が複数あるときに効きます。例えばSQL インジェクションが5か所で見つかったとします。5か所を個別に直しても、次の開発でまた生まれます。根本原因は「パラメータ化クエリを使う規約と教育がない」ことかもしれません。報告書にそこまで書けば、再発を防ぐ提案になります。

Secure distribution の手順は、報告書を暗号化した状態で渡し、鍵やパスワードは別の経路で伝えることです。メールに添付して、同じメールに解凍パスワードを書いても保護になりません。受信者は必要な人に絞り、閲覧権限を設けた安全な共有サイトも使います。

Articulation of risk, severity, and impact は、聞く人によって言い方を変える作業です。経営層には「顧客情報が流出すると、どの規制に抵触し、損害がいくらか」と事業の言葉で話します。技術者には再現手順と修正方法を渡します。同じ脆弱性でも、説明の軸が同じとは限りません。

Goal reprioritization の場面です。診断の途中で、依頼主が買収の発表を控えていて、買収先との接続部分を優先して調べたいと言い出したとします。目標の組み替えは、時間と費用に影響します。口頭の了解だけで進めてはいけません。SoW の変更や変更合意書で文書化します。

Business impact analysis（BIA）は、事業の機能が止まったときの影響を見積もる分析です。依頼主の BIA があれば、事業への打撃が大きい資産の指摘を優先できます。CVSS 値が同じ脆弱性でも、受注システムと社内の備品管理では、対応の順番が変わります。

Client acceptance は、依頼主が成果物（報告書など）を確認して受け入れる手順で、診断側が一方的には決められません。承認を得るまで、案件は完了しません。似た言葉に「リスクの受容」があります。直さない判断を依頼主が責任を持って選ぶことで、成果物の受け入れとは別の話です。

SAMPLE

Stakeholder alignment は、開始会議で目的、連絡先、日程、報告の頻度を揃えることから始まり、診断中の進捗報告でも続きます。最終的な決定権を持つ人が不明なままでは、合意は成り立ちません。

OSSTMM・CREST・PTES [1.3]

進め方を定めた枠組みが、細目に3つ並んでいます。[2]

OSSTMM（Open Source Security Testing Methodology Manual）は、ISECOM が発行する方法論です。テストの対象を5つのチャネルに分けます。Human、Physical、Wireless、Telecommunications、Data Networks です。Telecommunications と Data Networks は COMSEC、Physical と Human は PHYSSEC、Wireless は SPECSEC のクラスに属します。[8]

OSSTMM の特徴は、結果を数値で表すことです。攻撃対象領域を測り、Porosity（開口）、Controls（制御）、Limitations（制約）の3つを組み合わせて、rav（risk assessment value）という尺度にします。Controls は2種類に分かれます。相互作用を制御する Class A は Authentication、Indemnification、Subjugation、Continuity、Resilience。プロセスを守る Class B は Non-repudiation、Confidentiality、Privacy、Integrity、Alarm です。

OSSTMM は、テストの型を6つに分けています。

型	テスターの事前知識	対象側の事前通知	別名
Blind	なし	あり	Ethical hacking
Double Blind	なし	なし	Black box、ペネトレーションテスト

SAMPLE

型	テスターの事前知識	対象側の事前通知	別名
Gray Box	限定的	あり	脆弱性テスト
Double Gray Box	限定的	範囲と期間のみ	White box
Tandem	完全	あり	In-house audit、Crystal box
Reversal	完全	なし	Red team

CREST（Council of Registered Ethical Security Testers）は、英国の非営利組織です。会員企業の審査と認定、個人の資格認定を行い、会員は行動規範と倫理規程に署名します。[9] CREST は、テストの手順書ではありません。事業者と個人の品質を保証する認定の仕組みです。

PTES（Penetration Testing Execution Standard）は、診断の流れを7つの段階で示した標準です。標準そのものは技術的な手順を示さず、技術的な手順は PTES Technical Guidelines という別の文書が担います。

1. Pre-engagement Interactions（事前のやり取り）
2. Intelligence Gathering（情報収集）
3. Threat Modeling（脅威モデリング）
4. Vulnerability Analysis（脆弱性分析）
5. Exploitation（悪用）
6. Post Exploitation（侵入後の活動）
7. Reporting（報告）

PTES は、診断を始める前の合意（スコープ、目的、連絡手段）を最初の段階に置いています。[10] 見分け方は次のとおりです。診断の流れ全体を段階として示

SAMPLE

すなら PTES。結果を rav で数値化するなら OSSTMM。会員企業や個人の認定なら CREST です。

場面で確かめます。経営層から「ホワイトボックス寄りで、診断側には防御と資産の情報を一部だけ渡し、相手の担当者にも日程と範囲だけ知らせる形で試したい」と頼まれたとします。OSSTMM の型では Double Gray Box（別名 White box）に当たります。担当者に何も知らせない Reversal（Red team）とは別物で、取り違えてはいけません。

MITRE ATT&CK・OWASP Top 10・OWASP MASVS [1.3]

この3つは、手順書というより、攻撃や弱点を整理した知識の体系です。

MITRE ATT&CK は、実際の観測に基づく攻撃者の手法の知識ベースです。「戦術」は攻撃者の目的（なぜ）、「技術」はその目的を達成する方法（どうやって）、「サブテクニック」はさらに細かい手口を指し、3つを混同してはいけません。戦術の ID は TA、技術の ID は T で始まります。例えば、偵察の戦術は TA0043、能動的スキャンの技術は T1595、そのサブテクニックは T1595.001。[11]

Enterprise 版のマトリクスは、最新版（v20）で Reconnaissance、Resource Development 、Initial Access 、Execution 、Persistence 、Privilege Escalation 、Stealth 、Defense Impairment 、Credential Access 、Discovery 、Lateral Movement 、Collection 、Command and Control 、Exfiltration 、Impact の 15 戦術です。以前の版では Stealth と Defense Impairment の位置に Defense Evasion が1つあり、14戦術でした。版で名前が変わっても、戦術は「目的」の並びだと押さえれば解けます。使い道は、レッドチームの計画、検出の抜けの確認、指摘と手法の対応づけです。

SAMPLE

OWASP Top 10 は、Web アプリケーションの重大なリスクを10個に絞った一覧です。2021年版と2025年版があります。

2021年版	2025年版
A01 Broken Access Control	A01 Broken Access Control
A02 Cryptographic Failures	A02 Security Misconfiguration
A03 Injection	A03 Software Supply Chain Failures
A04 Insecure Design	A04 Cryptographic Failures
A05 Security Misconfiguration	A05 Injection
A06 Vulnerable and Outdated Components	A06 Insecure Design
A07 Identification and Authentication Failures	A07 Authentication Failures
A08 Software and Data Integrity Failures	A08 Software or Data Integrity Failures
A09 Security Logging and Monitoring Failures	A09 Security Logging and Alerting Failures
A10 Server Side Request Forgery (SSRF)	A10 Mishandling of Exceptional Conditions

どちらの版でも、A01 はアクセス制御の不備、Injection は SQL インジェクションや XSS などの入力値の扱いの不備で、意味は変わりません。順位を丸暗記しても、カテゴリの意味を押さえていなければ解けません。[1][2]

OWASP MASVS（Mobile Application Security Verification Standard）は、モバイルアプリの検証基準です。8つの管理策グループ、合計24の管理策から成ります。STORAGE（保存）、CRYPTO（暗号）、AUTH（認証と認可）、NETWORK（通信）、PLATFORM（プラットフォームとの連携）、CODE（コード品

SAMPLE

質）、RESILIENCE（リバースエンジニアリングと改ざんへの耐性）、PRIVACY（プライバシー）です。かつての検証レベル L1、L2、R は、MAS Profiles（MAS-L1、MAS-L2、MAS-R、MAS-P など）に作り直されました。[13] MASVS は「何を満たすべきか」の基準で、テストの手順は別の文書（MASTG）が担います。

3つの使い分けは、対象で決まります。Web アプリなら OWASP Top 10。モバイルアプリの検証基準なら MASVS。攻撃者の行動の整理や、検出の評価なら ATT&CK です。

場面で確かめます。診断チームが、依頼主の SOC の検出ルールにどんな抜けがあるかを、攻撃者の手口の一覧に沿って試します。使うのは ATT&CK です。報告書で各指摘に技術の ID（例：T1595）を添えなければ、依頼主は検出のルールと結び付けられません。

Purdue model [1.3]

Purdue model は、工場や発電所などの制御システム（OT/ICS）を階層に分け、どの階層同士が通信してよいかを整理する参照モデルです。

レベル	役割	例
Level 0	物理プロセス	センサー、アクチュエーター
Level 1	基本制御	PLC
Level 2	監視制御	HMI、SCADA
Level 3	現場の運用管理	製造実行システム、ヒストリアン
Level 3.5	IT と OT の間の DMZ	中継サーバー、ファイアウォール
Level 4	事業計画と物流	ERP などの企業システム

SAMPLE

レベル	役割	例
Level 5	企業全体のネットワーク	外部接続、クラウド

階層の数え方は、下が現場で、上が企業です。NIST SP 800-82 Rev.3 は、Purdue model を OT のネットワーク分割の例に挙げ、IT と OT の間に DMZ を置くことを勧めています。ファイアウォールの規則は隣り合う階層の間だけを許可し、Level 4 の機器が Level 2、1、0 の機器と直接通信することは認めません。[14]

診断への影響は大きいです。OT の機器は古い実装で動いていることが多く、通常のスキャンでも停止する場合があります。OT の診断では、次の方針を取ります。

- 能動的なスキャンの前に、機器の責任者と手法を合意する
- 受動的な観測（通信の記録を読む）から始める
- 停止が許される保守の時間帯に実施する
- 安全に関わる機器は、スコープから外す選択肢も持つ

場面で確かめます。診断で、事務所の PC（Level 4）から、工場の PLC（Level 1）に直接つながる経路が見つかりました。Purdue model の考え方では、これは階層の飛び越えで、指摘の対象です。改善は、Level 3.5 の DMZ を経由する構成に直し、直接の通信を遮断する規則を入れることです。PLC にパッチを当てるだけでは、経路の問題が残ります。

別の場面です。工場の生産ラインで動く HMI（Level 2）に対して、診断で全ポートのスキャンをかけたいという要望が出ました。スキャンで機器が止まれば、生産が止まるだけでなく、安全にも関わります。ROE で止められる範囲と時間帯を決め、受動的な観測から始める進め方が合います。

SAMPLE

脅威モデリングのフレームワーク [1.3]

脅威モデリングは、システムに起こり得る脅威を、設計の段階から洗い出して評価する作業です。細目は、次の3つを挙げています：

STRIDE は、Microsoft が提唱した、脅威を6種に分類する枠組みです。それぞれの脅威が、守るべき性質の侵害に対応します。[15]

脅威	意味	侵される性質
Spoofing（なりすまし）	他人の認証情報を使う	認証
Tampering（改ざん）	データを悪意で変更する	完全性
Repudiation（否認）	行為を後で否定される	否認防止
Information disclosure（情報漏えい）	権限のない者に見える	機密性
Denial of service（サービス拒否）	正規の利用者が使えない	可用性
Elevation of privilege（権限昇格）	低い権限で高い権限を得る	認可

DREAD は、見つけた脅威の優先度をつける採点方式です。Damage（被害）、Reproducibility（再現性）、Exploitability（悪用のしやすさ）、Affected users（影響を受ける利用者）、Discoverability（見つかりやすさ）の5項目を1〜10で採点し、平均を取ります。Discoverability は正確な見積もりが難しいため、すべての脆弱性はいずれ見つかるものとして最大点にする扱いが示されています。[16] 例えば 8、10、7、10、10 の5項目なら、平均は 9.0 で、優先度は低くありません。

SAMPLE

OCTAVE（Operationally Critical Threat, Asset, and Vulnerability Evaluation）は、カーネギーメロン大学の SEI が作った、組織のセキュリティリスクを評価する方法です。技術そのものを調べる方法ではありません。組織の運用上のリスクと情報資産に目を向けます。後継の OCTAVE Allegro は、情報資産がどこで保存され、運ばれ、処理されるかに注目し、4つの段階と8つの手順で進みます。[17]

3つの違いは、役割で覚えます。

- STRIDE は「どんな種類の脅威か」を分類する
- DREAD は「どれから対処するか」の点数をつける
- OCTAVE は「組織の重要な情報資産のリスクを評価する」手順そのもの

場面問題の読み方です。「開発チームが新しい認証機能の設計書から、考えられる脅威を漏れなく挙げたい」なら STRIDE を選びます。「挙げた脅威を、被害と再現性などで点数化して順位をつけたい」なら DREAD です。「経営層を巻き込み、重要な情報資産を中心に組織のリスクを洗い出したい」なら OCTAVE になります。

STRIDE の6種は、事例に当てはめる練習をしないと使い分けられません。ログに操作者が残らず、後から「私はやっていない」と言われる状況は Repudiation で、対策は監査ログと署名です。一般利用者が管理画面の機能を呼び出せてしまう状況は Elevation of privilege で、対策は認可の検査です。

書式の整合・文書の仕様・リスクの採点 [1.4]

報告書は、診断の唯一の成果物として残ります。細目の最初の3つは、報告書全体の作り方に関わります。[2]

SAMPLE

Format alignment（書式の整合）は、報告書の形を依頼主の求めに合わせることです。依頼主が指定する様式、監査人が受け入れる形式、読む人の層に合わせます。

Documentation specifications（文書の仕様）は、報告書の中身の約束事です。ファイル名の付け方、版数管理、機密区分の表示、証拠（画面キャプチャ、ログ）の添付の仕方、時刻の表記が含まれます。第三者が同じ手順で同じ結果を再現できる書き方でなければなりません。

Risk scoring（リスクの採点）は、指摘の深刻度を共通の物差しで表すことです。代表は CVSS（Common Vulnerability Scoring System）で、CVSS v4.0は4つの指標グループを持ちます。

グループ	意味
Base	脆弱性そのものの性質。時間や環境で変わらない
Threat	時間で変わる脅威の状況
Environmental	特定の環境での事情
Supplemental	補足的な文脈

数値を示すときは、どのグループを使ったかを名前で表します。Base だけなら CVSS-B、Base と Threat なら CVSS-BT、Base と Environmental なら CVSS-BE、全部なら CVSS-BTE です。[18] 深刻度の区分は次のとおり：

評価	点数
None	0.0
Low	0.1〜3.9

SAMPLE

評価	点数
Medium	4.0〜6.9
High	7.0〜8.9
Critical	9.0〜10.0

境界の 4.0、7.0、9.0 は、ひとつ上の区分に入ります。python3 でこの区分けを確かめた結果、3.9 は Low、4.0 は Medium、6.9 は Medium、7.0 は High、8.9 は High、9.0 は Critical になります。

CVSS が表すのは脆弱性の深刻度で、依頼主にとっての事業リスクそのものではありません。事業リスクは、これに悪用される可能性と資産の重要度を掛け合わせて決めます。悪用される可能性の物差しが EPSS（Exploit Prediction Scoring System）で、公開された CVE が今後30日以内に実際に悪用される確率を、0から1の値で毎日公表しています。[19]

CVSS が高くても EPSS が低く、外部に公開されていない資産なら、優先度は下がります。逆に CVSS が中程度でも、外部公開で悪用が活発なら、優先度は上がります。

関連の用語も区別します。CVE は個々の脆弱性に付く識別番号、CWE は脆弱性の根にある弱点の種類の分類です。報告書に CVE と CWE の番号がなければ、読み手は調べられません。

定義 [1.4]

報告書の Definitions は、本文で使う語の意味を揃える用語集です。深刻度の各段階（Critical、High など）が何を意味するか、攻撃成功の判定基準、診断の型（Black box など）をここで定義します。読み手が違えば同じ語の理解も違うため、基準を冒頭で固定しなければなりません。

SAMPLE

定義が曖昧だと、食い違いが起きます。報告書が「High」と書いていても、依頼主が自社の基準で「中程度」と読めば、対応の優先度が合いません。「High は CVSS 7.0〜8.9 を指す」と定義しておけば、この食い違いは起きません。

報告書の作成から完了までの流れは、次の順です。

1. 下書きを書く
2. ピアレビューと QC で内容を確かめる
3. 依頼主に提出し、内容の確認を受ける
4. 指摘への質問に答え、必要なら修正する
5. 依頼主が成果物を受け入れる（Client acceptance）

報告書の構成要素 [1.4]

報告書の要素は、読み手ごとに役割が違います。

要素	読み手	中身
Executive summary（経営向け要約）	経営層、非技術者	全体の評価、事業への影響、最優先の推奨
Methodology（手法）	技術者、監査人	使った枠組み、ツール、期間、テストの型
Detailed findings（詳細な指摘）	修正担当の技術者	題名、深刻度、対象、証拠、再現手順、影響
Attack narrative（攻撃の物語）	技術者と管理者の両方	指摘を時系列でつないだ、侵入までの筋書き
Recommendations / Remediation guidance（推奨事項と改善案）	修正担当と管理者	優先順位をつけた具体的な対策

SAMPLE

Executive summary には、専門用語と画面の詳細を入れません。事業の言葉で、結論と優先の対応を書きます。Detailed findings には、再現できる粒度の証拠を入れます。

Attack narrative と Detailed findings の違いは、よく出題されます。Detailed findings は、指摘を1件ずつ独立して書き、つながりは扱いません。Attack narrative は、複数の指摘がつながって攻撃者が目的に到達した経路を、時間の順に1つの話として書きます。「公開サイトの脆弱性で足場を得て、設定ファイルの資格情報で内部の DB に入り、顧客データに到達した」という流れです。個々の指摘が低評価でも、つながると重大になる点は、1件ずつの記述では伝わりません。

Remediation guidance は、直し方の案内です。「修正する」では足りません。「入力値をパラメータ化クエリで処理する」と具体的に書き、短期の応急処置と長期の恒久対策を分けると、依頼主が動きやすくなります。

場面で確かめます。診断チームが、依頼主の取締役会向けに、5か所の SQL インジェクションを発見した結果を報告します。取締役会に渡す部分は Executive summary で、技術用語は載せません。顧客情報の流出リスクと推奨の方針を書きます。開発チームには Detailed findings として、5か所の URL とパラメータ、再現手順、パラメータ化クエリへの修正案を渡します。両方に同じ細かさで書くと、どちらの読み手にも合いません。

テストの制限と前提 [1.4]

Test limitations and assumptions は、診断が何を保証しないかを書く節です。診断は、時間と範囲が区切られた活動にすぎません。見つからなかったことは、存在しないことの証明にならないのです。

SAMPLE

書く内容の例は次のとおりです。テスト時間帯の制約、除外した対象、与えられた資格情報の範囲、診断時点の状態にすぎないこと、診断者が置いた前提。前提の例は「依頼主が提供したネットワーク図が正しい」「テスト用アカウントの権限が本番と同じ」です。前提が崩れると結果の妥当性も変わるので、明記します。

この節は、診断会社を守る役目も持ちます。この節がなければ、「全ての脆弱性を発見した」という誤解は防げません。後で未発見の欠陥が悪用されても、診断が時点と範囲に限った保証だったと示せます。

報告の際の配慮 [1.4]

細目は、次の4つを挙げています：

Legal（法的な配慮）は、報告書に載せる情報の取り扱いです。実在の個人データやパスワードを、そのまま載せません。必要なら伏せ字にします。証拠の保管期間と廃棄の方法、報告書の機密区分は、契約と法令に合わせて決めます。

Ethical（倫理的な配慮）は、結果を正確に、偏りなく書くことです。依頼主に有利なように深刻度を下げる行為や、診断会社の成果を大きく見せる誇張は認められません。不利な事実も、見つかった範囲で書きます。

Quality control（QC）は、提出前の品質確認です。ピアレビュー、誤字や誤記の確認、深刻度の根拠の再確認、再現手順の追試が含まれます。1.2 の Peer review は、この QC の一部として動くもので、別の工程ではありません。

Artificial intelligence（AI）は、報告書の作成に生成 AI を使うときの配慮です。外部の生成 AI に依頼主の機密情報を貼り付けると、情報が契約の外に出ます。契約と依頼主の同意が許す範囲を超えては使えません。AI が書いた文には、もっともらしい誤りが混ざることがあります。人間が内容を検証してから提出し、責任を AI に負わせることはできません。使う順は、契約と同意で渡し

SAMPLE

てよい範囲を確かめる、許可された環境で機密を除いて生成する、人間が検証して直す、検証した担当者の責任で提出する、です。

場面で確かめます。テスターが報告書の下書きを早く仕上げるために、スキャン結果と顧客のホスト名を一般向けの生成 AI サービスへ貼り付けようとしましたが、依頼主の許可は取っていません。契約に外部サービスへの機密データ提供を認める条項がなければ、機密保持の違反になります。正しい動きは、依頼主の許可を得るか、機密を含まない形で使うか、契約で許可された環境の AI を使うことです。

技術的な管理策（その1） [1.5]

1.5 は、診断で見つけた弱点に、どの対策が合うかを選ぶ細目です。管理策は技術的、管理的、運用的、物理的の4分類で出題されます。[2]

System hardening（システムの要塞化）は、不要な機能を減らし、安全な設定に固めることです。既定のアカウントとパスワードの変更、不要なサービスとポートの停止、設定基準の適用が当たります。基準としては CIS Benchmarks があり、製品ごとの具体的な設定を示しています。[20] 「既定の資格情報が使われていた」「不要なサービスが公開されていた」という指摘には、基準の適用なしでは答えられません。

Sanitize user input / parameterize queries（入力値の無害化とクエリのパラメータ化）は、インジェクションへの対策です。SQL 文を文字列の連結で作ると、入力値が命令として解釈されます。パラメータ化クエリは、命令の構造と値を分けて渡すので、入力値が命令になることはありません。python3 の sqlite3 で確かめた結果です。

SAMPLE

```
inp = "' OR '1'='1"
db.execute("select * from u where name='%s'" % inp)   # 連結
db.execute("select * from u where name=?", (inp,))    # パラメータ化
```

連結の方は全行が返り、パラメータ化の方は0行になります。OWASP の対策一覧でも、値はパラメータ化クエリで渡すのが第一の選択です。表名や並び順のようにパラメータにできない部分は、アプリが決めた固定の値の許可リストから選ばせます。入力値の検証はパラメータ化を補うもので、代わりにはなりません。手作業でのエスケープは、強く非推奨とされています。[21] 入力値の検証だけに頼る選択肢は、第一の対策には選びません。

Multifactor authentication（多要素認証）は、知識（パスワード、PIN）、所持（トークン、スマートフォン）、生体（指紋）のうち、異なる種類を2つ以上組み合わせる認証です。盗まれたパスワードだけでは入れなくなるので、パスワードスプレー、使い回しによる乗っ取り、ブルートフォースへの有効な対策になります。同じ種類の要素を2つ重ねても（パスワードと秘密の質問）、多要素にはなりません。

Encryption（暗号化）は、通信中と保存中のデータを保護します。Telnet、FTP、HTTP のような平文の通信への対策は、SSH、SFTP、HTTPS への置き換えです。保存データには、ディスク暗号化やデータベースの暗号化を使います。パスワードは暗号化ではなく、ソルトを付けた低速のハッシュで保存しなければなりません。

Process-level remediation（プロセス単位の是正）は、実行中の個々のプロセスやサービスに対して行う対策です。サービスを最小権限のアカウントで動かす、不要なサービスを止める、アプリケーションの実行許可リストを使う、メモリ保護機能（ASLR、DEP など）を有効にするといった手当てが当たります。

SAMPLE

SYSTEM や root で動くサービスは、侵害されると全権が奪われます。権限を下げるだけで、侵害の被害は全権の奪取まで広がりません。

Patch management（パッチ管理）は、資産を把握し、修正に優先順位をつけ、検証し、配布し、結果を確認する一連の運用です。優先度は、CVSS だけでは決められません。EPSS、外部への公開の有無、資産の重要度も見ます。すぐにパッチを当てられないときは、WAF や IPS の規則で一時的に塞ぐ、ネットワークから隔離するといった補完策を取ります。

技術的な管理策（その2） [1.5]

Key rotation（鍵のローテーション）は、暗号鍵や API キー、SSH 鍵を、定期的に、または漏えいの疑いがあるときに交換することです。鍵が盗まれても、悪用できる期間は長引きません。NIST SP 800-57 が鍵管理の考え方をまとめています。[22] 「古い API キーが何年も使われ続けていた」という指摘には、交換の運用なしでは答えられません。

Certificate management（証明書管理）は、証明書の台帳を持ち、期限を監視し、更新を自動化し、漏えいした証明書を失効させる運用です。期限切れの証明書は、通信の停止を招きかねません。自己署名証明書の乱用や、弱い署名アルゴリズムの使用も指摘の対象です。

Secrets management solution（秘密情報管理の仕組み）は、パスワード、API キー、トークンをソースコードや設定ファイルに直接書かず、専用の保管庫から実行時に取り出す仕組みです。HashiCorp Vault や、クラウド事業者の秘密情報管理サービスが当たります。短い期間で失効する資格情報を発行し、利用の履歴を残せます。リポジトリに資格情報が埋め込まれていた指摘には、保管庫への移行と、漏れた資格情報の失効が欠かせません。

SAMPLE

Network segmentation（ネットワーク分割）は、ネットワークを区画に分け、区画間の通信を規則で絞ることです。侵入者が1台を乗っ取っても、横方向の移動を妨げられます。VLAN とファイアウォールの規則、クラウドのセキュリティグループ、Purdue model の階層分けが具体例です。診断で1台の侵害から全社のサーバーに到達できたなら、分割が足りていません。

Infrastructure security controls（インフラのセキュリティ制御）は、環境全体を守る装置と仕組みの総称で、主なものは次のとおり：

制御	役割
ファイアウォール	許可した通信だけを通す
IDS / IPS	不審な通信を検知（IDS）または遮断（IPS）する
WAF	Web アプリへの攻撃を、HTTP の内容で検査して防ぐ
EDR	端末の挙動を監視し、検知と対応を行う
SIEM	ログを集めて相関分析し、警報を出す
DLP	機密データの持ち出しを検知、阻止する

SAMPLE

場面で確かめます。診断の結果、公開 Web アプリに SQL インジェクションがあり、修正にはアプリの改修が必要で、数週間かかります。直ちにできる応急処置は、WAF にインジェクションを遮断する規則を入れることです。改修を待つ間、何も手当てしないわけにはいきません。恒久対策は、パラメータ化クエリへの修正になります。報告書には、短期の対策と長期の対策を分けて書きます。

別の場面です。診断で、開発者が AWS のアクセスキーを公開リポジトリに載せていたことが見つかりました。最初にやるのは、そのキーの失効と交換（ロ

ーテーション）です。履歴からキーを消すだけでは、すでに複製された鍵は無効になりません。恒久対策は、秘密情報管理の仕組みへの移行と、コミット前の検査です。

管理的な管理策 [1.5]

管理的な管理策（Administrative controls）は、人と組織の決まりごとで守る対策であって、機器の設定ではありません。

Role-based access control（RBAC）は、利用者に直接権限を付けず、役割（ロール）に権限を付け、利用者を役割に割り当てる方式です。最小権限の原則を実現し、異動や退職のときの権限の見直しも簡単になります。過剰な権限や、異動後も残った権限の指摘への答えです。

Secure software development life cycle（セキュアな開発ライフサイクル）は、要件、設計、実装、テスト、運用の各工程にセキュリティの作業を入れる開発の進め方であり、最後に足す検査ではありません。設計での脅威モデリング、実装時のコードレビューと SAST、テスト時の DAST と SCA（依存ライブラリの検査）、リリース前の侵入テストが当たります。同じ種類の脆弱性が繰り返し見つかるなら、個別の修正だけでは追いつきません。

Minimum password requirements（パスワードの最低要件）は、パスワードの方針を定めた規則です。NIST SP 800-63B-4 は、パスワードだけで認証する場合は最低15文字、多要素認証の一部として使う場合は最低8文字を求めています。文字種を混ぜる規則（大文字、数字、記号の必須）は課してはならず、定期的な変更も求めてはいけません。ただし、漏えいの証拠があるときは変更を強制します。[23] 長さを重視し、頻繁な強制変更は避けるのが、現在の考え方です。

SAMPLE

Policies and procedures（方針と手順）は、組織の決まりと実施手順の文書です。利用規程、インシデント対応計画、変更管理、入退社の手続き、委託先の管理が当たります。指摘の根本原因が「決まりがない」「守られていない」なら、方針の策定と周知が欠かせません。

設問が従来の「複雑さの要件」を正解にしているように見えたら、設問の文脈を優先してください。選択肢に、長さの引き上げと多要素認証の導入があるなら、前者は管理的、後者は技術的の管理策です。

運用的な管理策 [1.5]

運用的な管理策（Operational controls）は、人が日々の運用で実施する対策で、文書だけでは完結しません。管理的な管理策が「決まり」なら、運用的な管理策は、その決まりを日常でどう動かすかに当たります。

管理策	中身	防ぐもの
Job rotation（職務ローテーション）	担当者を定期的に入れ替える	不正の隠蔽、特定の人への依存
Time-of-day restrictions（時間帯制限）	ログインできる時間を限る	深夜の不正アクセス、乗っ取り
Mandatory vacations（強制休暇）	一定期間、連続して休ませる	隠れた不正の継続（不在の間に表面化させる）
User training（利用者教育）	攻撃の手口と対処を教える	フィッシングなど人を狙う攻撃

Mandatory vacations は、休暇中に別の担当者が業務を引き継ぐので、前任者が隠していた不正が見つかります。Job rotation も同じように、不正の早期発見に効きます。この2つは、不正を未然に防ぐ管理策ではありません。見つける側の性格が強い管理策です。

SAMPLE

場面で確かめます。経理担当者が何年も同じ業務を一人で担当し、休暇を取らず、不正な送金が疑われます。「休暇を強制し、その間に別の担当者が業務を引き継ぐ」が答えです。パスワードを強くしても、内部者の不正は防げません。

Time-of-day restrictions は、営業時間外のログインを禁止する設定です。深夜に管理者アカウントで接続があれば、盗用を疑えます。

User training は、フィッシングに対して最も直接的です。疑似フィッシングメールの訓練を行い、報告の経路も教えます。

管理的と運用的の見分け方は次のとおり：文書や仕組みで決めるなら管理的。担当や勤務の運用を変える、人を教育するなら運用的と考えます。

物理的な管理策 [1.5]

Physical controls（物理的な管理策）は、建物や設備への物理的な侵入を防ぎ、検知する対策です。

Access control vestibule（アクセス制御ヴェスティビュール）は、2つの扉の間に小さな空間を挟み、片方が閉じてからもう片方が開く仕組みです。一般に mantrap とも呼びます。1人ずつ認証を受けて通るので、他人の入室に便乗する共連れ（tailgating）は成立しません。診断で「正規の従業員のすぐ後ろについて入れた」とあれば、答えはヴェスティビュールです。

Biometric controls（生体認証）は、指紋、虹彩、顔などの身体的特徴で本人を確かめます。カードや暗証番号と違って、忘れたり貸し借りしたりできません。誤って他人を通す率（FAR）と、本人を拒否する率（FRR）の釣り合いが、設計の論点です。

Video surveillance（映像による監視）は、カメラで入口や重要区画を記録します。侵入を防ぐ力は弱く、抑止、検知、事後の調査に効きます。

SAMPLE

物理診断の指摘は、扉の施錠不備、共連れ、カードの複製のしやすさ、カメラの死角として出ることが少なくありません。対応する管理策は、順に、施錠の見直し、ヴェスティビュール、生体認証や多要素の組み合わせ、カメラの増設と保管期間の見直しです。

管理策を選ぶ手順 [1.5]

細目の題は、場面を分析して、報告書の中で適切な是正策を勧めることです。手順は次のとおり：

1. 指摘の根本原因を見つける（設定不備か、実装の欠陥か、運用の不備か、決まりの欠如か）
2. 原因の層に合う分類を選ぶ（技術的、管理的、運用的、物理的）
3. その層の中から、原因を直接塞ぐ管理策を選ぶ
4. 直ちにできる応急処置と、恒久対策を分けて書く

代表的な対応は次のとおり：

指摘	合う管理策	分類
SQL インジェクション	パラメータ化クエリ	技術的
盗まれたパスワードでの不正ログイン	多要素認証	技術的
平文のプロトコルを使用	暗号化された通信への置き換え	技術的
1台の侵害から全体に到達	ネットワーク分割	技術的
ソースに資格情報を埋め込み	秘密情報管理の仕組み	技術的

SAMPLE

指摘	合う管理策	分類
同種の脆弱性が繰り返し発生	セキュアな開発ライフサイクル	管理的
過剰な権限	RBAC、最小権限	管理的
内部者の不正の疑い	強制休暇、職務ローテーション	運用的
従業員がフィッシングに応じた	利用者教育	運用的
共連れで入室できた	アクセス制御ヴェスティビュール	物理的

選択肢が複数とも正しく見えるときは、2点で絞ります。指摘の原因を直接塞ぐか。設問が求める分類か。例えば「パスワードが弱くて破られた」への答えが、パスワード長の要件（管理的）か多要素認証（技術的）かは、設問が分類を指定しているかで決まります。

SAMPLE

サンプルはここまでです

続き(第2章〜巻末)は、PenTest+ 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。

Footnotes

1. CompTIA PenTest+ 試験ページ（Number of questions: maximum of 90 、 Passing score: 750 ） 。 https://www.comptia.org/en-us/certifications/pentest/ ／ 日本語ページ（制限時間:165分）。https://www.comptia.org/ja-jp/certifications/pentest/ ↩

2. CompTIA PenTest+ PT0-003 V3 Certification Exam Objectives, Version 5.0, 1.0 Engagement Management （ 1.1 〜 1.5 ） 。https://lecbyo.files.cmp.optimizely.com/download/1e8cf0febef111efb260822b03028498 ↩ ↩2 ↩3 ↩4 ↩5

3. General Data Protection Regulation, Article 33（Notification of a personal data breach to the supervisory authority）。https://gdpr-info.eu/art-33-gdpr/ ↩

4. AWS, Penetration Testing（許可されるサービスと禁止される行為）。https://aws.amazon.com/security/penetration-testing/ ↩

5. Microsoft Security Response Center, Penetration Testing Rules of Engagement 。 https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement ↩

6. 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）第3条 、 第 11 条 。 https://laws.e-gov.go.jp/document?

SAMPLE

lawid=411AC0000000128 ↩

7. 18 U.S. Code § 1030, Fraud and related activity in connection with computers。https://www.law.cornell.edu/uscode/text/18/1030 ↩
8. ISECOM, OSSTMM 3 - The Open Source Security Testing Methodology Manual, 2.2 Scope 、Chapter 4 。https://www.isecom.org/OSSTMM.3.pdf ↩
9. CREST（Council of Registered Ethical Security Testers）。https://www.crest-approved.org/ ↩
10. The Penetration Testing Execution Standard（7つの section）。https://pentest-standard.readthedocs.io/en/latest/ ↩
11. MITRE ATT&CK, Enterprise Matrix 。https://attack.mitre.org/matrices/enterprise/ と https://attack.mitre.org/resources/ ↩
12. OWASP Top 10:2021 https://top10.owasp.org/2021 と OWASP Top 10:2025 https://top10.owasp.org/2025/ ↩
13. OWASP MAS, The Mobile Application Security Verification Standard（MAS Testing Profiles）。https://mas.owasp.org/MASVS/03-Using_the_MASVS/ ↩
14. NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, 5.2.3.1 Network Architecture 。https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf ↩

SAMPLE

15. Microsoft Learn, Threats - Microsoft Threat Modeling Tool（STRIDE model ）。https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats ↩

16. Microsoft Learn, Call to action and resources (threat modeling for drivers)（The DREAD approach）。https://learn.microsoft.com/en-us/previous-versions/windows/hardware/design/dn613894(v=vs.85) ↩

17. Carnegie Mellon SEI, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (CMU/SEI-2007-TR-012), 1.2.3 。https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf ↩

18. FIRST, Common Vulnerability Scoring System v4.0 Specification Document 。https://www.first.org/cvss/v4-0/specification-document ↩

19. FIRST, Exploit Prediction Scoring System (EPSS) 。https://www.first.org/epss/ ↩

20. Center for Internet Security, CIS Benchmarks 。https://www.cisecurity.org/cis-benchmarks ↩

21. OWASP Cheat Sheet Series, SQL Injection Prevention Cheat Sheet（Primary Defenses 、Input Validation ）。https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html ↩

SAMPLE

22. NIST SP 800-57 Part 1 Rev. 5, Recommendation for Key Management。https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final ↩

23. NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management, 3.1.1.1 と 3.1.1.2 。https://pages.nist.gov/800-63-4/sp800-63b.html ↩

SAMPLE

CompTIA PenTest+ 学習用テキスト(無料サンプル)

版

2026年11月版(CompTIA PenTest+ (PT0-003) Exam Objectives Version 5.0 準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

CompTIA、PenTest+、および関連するロゴ・認定名は、CompTIA(The Computing Technology Industry Association, Inc.)の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。

本教材は公式シラバスの内容を基に作成したもので、CompTIA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。

SAMPLE