

IT 資格 道 場

CCSP 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)

ISC2「CCSP Certification Exam Outline」(2026年8月1日発効・日本語版の試験概要
も同日付) 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]

出題分野と配点比率:どこに時間を使うか [intro]

第1章 Cloud Concepts, Architecture and Design

[1.1/1.2/1.3/1.4/1.5/1.6]

クラウドコンピューティングの定義と役割 [1.1]

クラウドリファレンスアーキテクチャ [1.2]

クラウドのセキュリティ概念 [1.3]

安全なクラウドの設計原則 [1.4]

クラウドサービスプロバイダーの評価 [1.5]

人工知能と機械学習の理解 [1.6]

サンプルはここまでです

このテキストの位置づけ: 3 点セットの本編。これだけで問題が解けるようになることが目標で、クラウドセキュリティの用語・仕組み・計算・場面の判断を合格ラインの深さで扱う。

進め方: ① 学習用を読む → ② 頻出度別で解き方を掴む → ③ 問題演習で腕試し → ④ 頻出度別に戻って再確認。暗記用は空き時間や用語の再確認に使う。

SAMPLE

試験の概要 [intro]

CCSP は、ISC2 が実施するクラウドセキュリティの認定試験です。この本文は、**2026 年 8 月 1 日施行の試験範囲 (Exam Outline)** に合わせています。

項目	内容
方式	CAT (コンピュータ適応型) 。1 問ごとに次の問いが選ばれる
問題数	100～150 問 (CAT のため、解く数は受験者ごとに変わる)
時間	最大 3 時間
見直し	できない 。答えを確定すると、見直しも変更もできない
合格点	1000 点満点中 700 点
出題形式	選択式問題と、発展的問題 (表や図を読む問題、計算、順序回答、ドラッグアンドドロップ、ホットスポット、シナリオなど)
会場	ピアソン VUE のテストセンター
言語	日本語で受験できる

受験料や受験資格は変わることがあります。申し込み前に ISC2 の公式サイトで最新の情報を確認してください。

出題分野と配点比率：どこに時間を使うか [intro]

分野	配点	この本文の章
1 クラウドの概念、アーキテクチャ、設計	17%	第 1 章
2 クラウドデータセキュリティ	20%	第 2 章
3 クラウドプラットフォームとインフラストラクチャセキュリティ	17%	第 3 章
4 クラウドアプリケーションセキュリティ	16%	第 4 章
5 クラウドセキュリティオペレーション	17%	第 5 章
6 法務、リスク、コンプライアンス	13%	第 6 章

見出し末尾の [1.1] は、試験範囲の細目の番号。

第1章 Cloud Concepts, Architecture and Design [1.1/1.2/1.3/1.4/1.5/1.6]

- 配点 17%・細目 1.1～1.6

この章はクラウドの言葉と型を決める章です。定義、役割、サービスの分け方、守る仕組みの名前、設計の物差し、提供者の評価、AI の扱いを順に読みます。CAT 方式では 1 問ごとに次の問いが選ばれます。用語の取り違えが続くと問いが難しくならず、点が伸びません。言葉の線引きを先に固めます。

クラウドコンピューティングの定義と役割 [1.1]

クラウドコンピューティングの定義 (NIST SP 800-145 ほかの用語)

NIST SP 800-145 の定義は次のとおりです。共有の構成可能なコンピューティング資源 (ネットワーク・サーバ・ストレージ・アプリケーション・サービス) に、どこからでも便利にオンデマンドでネットワーク経由でアクセスできるモデルです。資源は、最小限の管理の手間や提供者とのやり取りで、迅速に提供し、解放できます。[^c1-1]

この定義は 3 つの数字で覚えます。5 つの基本的な特性、3 つのサービスモデル、4 つの展開モデル。サービスモデルと展開モデルは 1.2 で扱い、ここでは特性と役割を固めます。

NIST のほかに、ISO/IEC の語彙があります。ISO/IEC 17788 は特性を 6 つに数えます (17788 は 2023 年に、用語集の 22123-1 と概念の 22123-2 へ置き換えられました) 。[^c1-3] NIST は 5 つ、ISO/IEC は 6 つという数の違いが、試験でよく問われます。

クラウドの役割と責任(顧客・CSP・パートナー・ブローカー・規制当局)

役割の名前には 2 つの体系があります。NIST SP 500-292 のクラウド参照アーキテクチャは、5 つの役者を置きます。[^c1-2]

- クラウド利用者: サービスを使う
- クラウド提供者: サービスを提供する
- クラウドキャリア: 利用者と提供者の間にネットワークや通信回線を運ぶ
- クラウド監査人: サービス、運用、セキュリティを独立の立場で評価する
- クラウドブローカー: 利用者と提供者の間に立ち、サービスを仲立ちする

ブローカーのサービスは 3 種類。仲介(intermediation)は、既存のサービスに機能を足して価値を上げます。集約(aggregation)は、複数のサービスを 1 つにまとめて統合します。裁定(arbitrage)は集約に似ていますが、束ねるサービスは固定ではありません。ブローカーが状況に応じて選び替えます。

ISO/IEC 17789 (クラウドの参照アーキテクチャ。2023 年に 22123-3 へ置き換えられました)は、役割をクラウドサービス顧客(CSC)、クラウドサービス提供者(CSP)、クラウドサービスパートナー(CSN)と呼びます。パートナーには監査人、ブローカー、開発者などが入ります。[^c1-4] NIST の監査人とブローカーは、ISO/IEC ではパートナーの一種に束ねられます。

規制当局は、サービスの提供者でも利用者でもありません。法令の遵守を外から検査する立場で、責任の線引きに影響します。責任は契約と法令の両方で決まります。作業を CSP に任せても、データの管理責任が顧客から消えることはありません。

場面で見分けます。ある会社が複数の CSP のサービスを組み合わせ、窓口を 1 つにして顧客に売っています。組み合わせは固定で、料金も 1 本にまとめており、日ごとの変更はありません。この会社の役割はクラウドブローカーで、サ

ービスは集約です。組み合わせる提供者を日ごとの価格で選び替えるなら、裁定に変わります。

クラウドコンピューティングの主要な特性

NIST の 5 つの基本的な特性は次のとおりです。

- **オンデマンドセルフサービス**: 利用者が提供者の担当者と話さず、必要な時に自分で資源を確保する。
- **広範なネットワークアクセス**: 標準的な仕組みでネットワーク越しに使い、スマホや PC など様々な端末から届く。
- **リソースプーリング**: 提供者の資源を複数の利用者で共用し、需要に応じて割り当てる。利用者は通常、資源の正確な場所を知らず、制御もできない(国や地域、データセンターのような粗い単位では指定できる場合がある)。
- **迅速な弾力性** (rapid elasticity。ISO/IEC 17788 では rapid elasticity and scalability): 必要に応じて資源を増やし、減らす。利用者から見ると容量は無限に近い。
- **測定サービス** (measured service): 使った量を測り、報告し、制御して、課金や管理に使う。

ISO/IEC の特性は、この 5 つにマルチテナンシーを足した 6 つです。マルチテナンシーは、複数の利用者(テナント)が同じ物理資源を共用しながら、互いのデータやアプリを分けておく性質を指します。NIST ではリソースプーリングの中に含まれる考え方です。6 つ目を聞かれたら、答えはマルチテナンシー。

間違えやすい点が 3 つあります。セルフサービスは「利用者が何でも設定できる」という意味ではありません。資源の確保に提供者の人手が要らないという

意味です。測定サービスは、請求のための仕組みにとどまりません。制御と最適化にも使います。弾力性は、増やすだけでなく減らす方向も含みます。

ビルディングブロック技術(仮想化・ストレージ・ネットワーク・データベース・オーケストレーション)

クラウドは 5 つの部品の上に作られています。仮想化は、1 つの物理機器を複数の論理機器に見せ、資源をプールにする技術です。ストレージは、ブロック、ファイル、オブジェクトなどの型でデータを保持します。ネットワークは、仮想ネットワークによる利用者ごとの通信の分離。データベースは、管理を提供者が肩代わりするサービスとして使えます。オーケストレーションは、複数の資源の作成、構成、連携を自動の手順で調整する仕組みです。

部品ごとに、守り方が変わります。

部品	主な守り方
仮想化	分離 (1.3 で扱う)
ストレージ	暗号化とアクセス制御
ネットワーク	分割と通信の検査
データベース	認証と暗号化、権限の絞り込み
オーケストレーション	自動化に使う権限を最小にする

オーケストレーションの権限を奪われると、大量の資源をまとめて操作されます。ほかの部品より、権限の範囲を狭く保たなければなりません。

クラウドリファレンスアーキテクチャ [1.2]

クラウドコンピューティングの活動(役割ごとの活動)

参照アーキテクチャは、役割ごとの活動を並べた図です。ISO/IEC の役割の説明では、顧客の主な活動は、サービスの利用、事業面の管理、利用の管理です。提供者は、サービスの提供、展開と監視、事業計画の管理、監査データの提供などを行います。パートナーは、提供者か顧客の活動を支える役で、監査人やブローカーが例です。[^c1-4]

試験での使い方は単純です。ある作業が誰の活動かを聞かれます。顧客が仮想マシンの利用状況を見る作業は、顧客の活動です。物理サーバーの保守は提供者の活動で、第三者がクラウドの統制を検査する作業は、監査人（パートナー）の活動になります。

クラウドサービスの能力の型（アプリケーション・プラットフォーム・インフラストラクチャ）

ISO/IEC 17789 は、クラウドが提供する能力を 3 つの型に分けます。アプリケーション能力型は、利用者がアプリケーションを使える能力です。プラットフォーム能力型は、アプリを配置し、動かし、管理できる能力です。インフラストラクチャ能力型は、処理、ストレージ、ネットワークを利用者が使える能力です。[^c1-4]

「能力の型」と「サービスのカテゴリ」は別の語です。どちらも ISO/IEC 17788 の語です。能力の型は、使う資源で機能を分けた 3 つの型です。サービスのカテゴリは、共通の性質を持つサービスの群で、SaaS・PaaS・IaaS などがあります（NIST は同じ 3 つを「サービスモデル」と呼びます）。おおまかな対応は、アプリケーション能力型が SaaS、プラットフォーム能力型が PaaS、インフラストラクチャ能力型が IaaS です。ISO/IEC では、1 つのカテゴリが複数の能力型を含む場合もあります（例: CaaS (Communications as a Service・通信のサービス) はアプリケーション能力型とプラットフォーム能力型を持つ）。

サービスのカテゴリ（SaaS・PaaS・IaaS）

3つのカテゴリの違いは、利用者が何を管理するかで決まります。NIST SP 800-145 の定義を表にします。[^c1-1]

カテゴリ	提供者が出すもの	利用者が管理するもの	例
SaaS	提供者のアプリケーション	利用者ごとの限られた設定だけ。インフラも OS もアプリの機能も管理しない	Web メール、勤怠管理の Web サービス
PaaS	言語・ライブラリ・ツールを備えた実行環境	配置したアプリと実行環境の設定。ネットワーク・サーバ・OS・ストレージの基盤は管理しない	アプリを置くだけで動く実行基盤
IaaS	処理・ストレージ・ネットワークなどの基本資源	OS・ストレージ・配置したアプリと、一部のネットワーク部品（ホストのファイアウォールなど）	仮想マシンと仮想ディスク

表は、下の行へ進むほど利用者の管理範囲が広がります。SaaS はほぼ全部を提供者が持ちます。IaaS は OS から上を利用者が持ちます。責任の細かい線は 1.4 で改めて表にします。

間違えやすい点は 2 つ。PaaS の利用者が管理するのはアプリとその設定で、OS ではありません。OS のパッチは提供者の仕事です。IaaS でも、物理機器とハイパーバイザーは提供者が管理しており、利用者は触れません。

場面で組み合わせます。ある開発チームが、アプリを動かす基盤を探しています。OS のパッチは自社でやりたくありませんが、アプリの実行設定は自分たち

で決めたい、という要件です。この条件に合うのは PaaS。OS まで自分で決めたいなら IaaS、設定もほぼ要らないなら SaaS になります。

分類で迷いやすいのは、管理を任せるデータベースと、関数を実行するサービス。Microsoft は、関数の実行サービスとマネージドの SQL データベースを PaaS の例に挙げています。[^c1-20] 仮想マシンの上に自分でデータベースを入れたなら IaaS です。提供者が OS のパッチも運用も行うデータベースサービスなら PaaS になります。同じデータベースでも、型を決めるのは、誰が OS を管理するか。

展開モデル (パブリック・プライベート・ハイブリッド・コミュニティ・マルチクラウド)

NIST は 4 つの展開モデルを定義します。

- **パブリック**: 一般の組織や人に開かれ、提供者の敷地にある。
- **プライベート**: 1 つの組織だけが使う。運営は組織自身でも第三者でもよく、敷地の内外も問わない。
- **コミュニティ**: 共通の関心 (任務、セキュリティ要件、方針など) を持つ特定の組織群が使う。
- **ハイブリッド**: 2 つ以上の別々のクラウド基盤 (プライベート・コミュニティ・パブリック) を、データやアプリを移せる標準または独自の技術で結びつける。

マルチクラウドは NIST の 4 つの外にあり、公式の範囲では例示に入っています。複数の CSP のサービスを使い分ける構成。ハイブリッドは、別々のクラウド基盤を、データやアプリを移せる形で結びつけた構成です。[^c1-1] マルチクラウドは複数の CSP を使うこと自体を指し、SP 800-145 には出てこない語で

す。1 社のパブリッククラウドだけを使う構成は、マルチクラウドではなくパブリックです。

場面で見分けます。医療機関が集まって共同の基盤を作り、同じ規制に合わせて運用する形は、コミュニティ。1 社が自社のデータセンターのプライベートクラウドと AWS のパブリックを専用線でつないで使うなら、ハイブリッドです。同じ会社が AWS と Azure に別々のシステムを置くなら、マルチクラウドです。

共有の考慮事項①相互運用性・ポータビリティ・可逆性

相互運用性は、システム同士が情報をやり取りして、それを使える性質です。ポータビリティは、データやアプリを別の環境へ移せる性質です。ISO/IEC 19941 が、この 2 つの枠組みを定めています。[^c1-5]

可逆性 (reversibility) は、顧客がデータとアプリの成果物を取り戻し、提供者が合意した期間の後に顧客のデータを消す過程です。[^c1-3] 契約の終わりを決める、出口戦略の中心。

3 つの違いを場面で見ます。別の CSP へ乗り換える時にデータ形式が合わず取り出せないなら、ポータビリティの問題です。2 つのサービスが API で連携できないなら、相互運用性の問題です。契約を終えた後もデータが提供者に残り続けるなら、可逆性の問題です。可逆性を含むのは、取り戻すことと消すことの両方。

共有の考慮事項②可用性・回復力・性能・サービスレベルと SLA・監査可能性

可用性は、必要な時にサービスを使える割合です。回復力 (resiliency) は、障害が起きても機能を保ち、元に戻る力です。性能は、処理の速さと待ち時間。監査可能性は、提供者の統制を検査できる性質で、顧客が監査できる範囲は契約で決めます。

SLA (サービスレベル契約) の概念と用語の枠組みは、ISO/IEC 19086-1 が定めます。[^c1-6] SLA には、指標 (可用性など)、目標値、測り方、未達の場合の補償 (サービスクレジットなど) が入ります。補償は損害の全額ではありません。料金の一部の返金という形が多い点に注意してください。

可用性の数字を読めるようにします。30 日 (43,200 分) の月と 365 日の年で、停止が許される時間を並べた表。

可用性	30 日あたりの停止の許容	1 年あたりの停止の許容
99.0%	432.0 分	5,256 分 (約 87.6 時間)
99.9%	43.2 分	525.6 分 (約 8.8 時間)
99.95%	21.6 分	262.8 分
99.99%	4.32 分	52.56 分
99.999%	0.43 分	5.26 分

部品をつなぐと、全体の可用性が変わります。可用性 99.9% のサービスを 2 つ直列につなぐと、全体は $0.999 \times 0.999 = \text{約 } 99.8\%$ に下がります。可用性 99% のシステムを 2 つ並列に置き、どちらかが動けばよいなら、 $1 - (0.01 \times 0.01) = 99.99\%$ まで上がります。全体の SLA は、部品の SLA の組み合わせで決まります。

3 つ直列でも同じ式で、0.999 を 3 回掛けた約 99.7% (0.997003)。可用性 99.5% のシステムを 2 つ並列に置くと、 $1 - (0.005 \times 0.005) = 99.9975\%$ になります。直列は数が増えるほど下がり、並列は数が増えるほど上がる関係。

共有の考慮事項③セキュリティ・プライバシー・ガバナンス・規制・アウトソーシング・保守とバージョン管理

セキュリティとプライバシーは、データの保護と個人情報の扱いに関わる要件です。ガバナンスは、組織の方針と統制がクラウドを使っても保たれる仕組みを指します。規制は業種や地域の法令で、データの置き場所に条件が付くことがあります(6章で扱います)。アウトソーシングは運用を外部に任せることです。責任まで外に出るわけではありません。

保守とバージョン管理は、提供者が基盤を更新した時の影響を指します。SaaSで提供者が機能を変えると、利用者の運用や連携が影響を受けます。変更の予告期間と、古い版の維持期間を、契約で確かめます。IaaSのOSを更新するのは顧客。更新を怠った時の責任は、提供者ではなく顧客にあります。

関連技術①データサイエンス・機械学習・AI・ブロックチェーン

データサイエンスは、データから知見を取り出す分野です。機械学習は、データからパターンを学ぶ技術で、AIの一部に当たります。クラウドは、学習に要る大量の計算とデータの置き場を提供します。セキュリティ上の主題は、学習データの機密、モデルの盗難、学習データの汚染です(1.6で詳しく扱います)。モデルの盗難は、学習済みのモデル(重みのファイルなど)を複製して持ち出されることで、学習データに触れなくても起きます。

ブロックチェーンは、改ざんに強い分散台帳です。ブロックはハッシュで前のブロックとつながります。[1-9]動きを見る例。3件の取引を鎖にして、先頭の「A→B 5」を「A→B 9」に書き換えると、先頭のブロックのハッシュが別の値に変わります。2つ目以降のハッシュも連鎖して全部変わります。1か所の改ざんが、後ろの全ブロックの不一致として表に出ます。

関連技術②IoT・コンテナ・エッジコンピューティング

IoTは、センサーや機器がネットワークにつながり、クラウドにデータを送る仕組みです。機器の数が多く、更新も難しいため、弱い認証と古いファームウェア

が主なリスク。

コンテナは、OS の機能を共有しながらアプリを隔離して動かす技術です。仮想マシンより軽く、起動が速い一方、カーネルを共有するので分離は弱くなります。エッジコンピューティングは、利用者や機器に近い場所で処理する形。遅延が減り、クラウドへ送るデータ量も減ります。分散した拠点の物理管理とパッチ適用は難しくなります。

エッジはクラウドの代わりにはなりません。クラウドと組み合わせる配置。コンテナは仮想マシンの一種ではなく、カーネルを共有する別の分離方式です。

場面で考えます。工場の機器から大量のセンサーデータが届き、遅延を小さくしたい要件があります。クラウドまで毎回送ると遅れるので、工場の近くのエッジで一次処理をして、要約だけをクラウドへ送ります。弱点は、更新しにくい機器に残る古いファームウェア。

関連技術③量子コンピューティング・機密コンピューティング・DevSecOps

量子コンピューティングは、現行の公開鍵暗号 (RSA や楕円曲線) を破る可能性があります。NIST が最初に FIPS として確定した耐量子暗号は 3 つで、FIPS 203 (ML-KEM・鍵カプセル化)、FIPS 204 (ML-DSA・署名)、FIPS 205 (SLH-DSA・ハッシュ型署名) です。公表日は 2024-08-13。[^c1-8] 鍵交換には 203、署名には 204 と 205 を使います。

将来、量子計算機が今日の通信を解読できるなら、今日盗まれた暗号文が後で読めます。移行は、長く守るデータから先に。

場面で考えます。30 年保存する医療記録を、今のクラウドの暗号で守っています。通信を今の公開鍵暗号で保護していれば、盗まれた暗号文が将来、量子計算機で解読される恐れがあります。守る期間が長いデータほど、移行を先に

進めます。鍵交換には FIPS 203 (ML-KEM) を、署名には FIPS 204 と 205 を使う。

機密コンピューティングは、ハードウェアに基づく信頼できる実行環境 (TEE) の中で計算し、使用中のデータを守る技術です。[^c1-7] 保存時と転送時の暗号化では守れない、メモリ上の平文を守ります。クラウドの管理者や、同じ機器を使う他の利用者からも、処理中のデータは見えません。

DevSecOps は、開発と運用の流れにセキュリティを最初から組み込み、検査を自動化して早い段階へ寄せる (シフトレフト) 考え方です。[^c1-24] 具体的な手順は、1.4 の DevOps のセキュリティで扱います。

クラウドのセキュリティ概念 [1.3]

暗号と鍵管理 (保存時・転送時・鍵のライフサイクル)

暗号化は、データの 3 つの状態に分けて考えます。保存時はディスクやオブジェクトに置かれたデータ、転送時はネットワークを流れるデータ、使用中はメモリ上で処理されるデータです。保存時の標準は AES。AES のブロック長は 128 ビット、鍵長は 128、192、256 ビットの 3 つで、バイトにすると 16、24、32 バイトになります。[^c1-10] 転送時は TLS で守り、現行の版は TLS 1.3 です。TLS 1.3 の仕様は RFC 8446 (2018 年) で、2026 年 7 月に RFC 9846 が置き換えました (版の番号は 1.3 のまま)。[^c1-43] 使用中のデータを守る主な手段は、1.2 で見た機密コンピューティング。

鍵の管理は、暗号化そのものと同じ重さを持ちます。鍵をデータと同じ場所に置くと、データを盗んだ人が鍵も手に入れます。クラウドでは、鍵を管理する専用のサービス (KMS) や、鍵を物理的に守る HSM を使い、データの保管場所と鍵の保管場所を分けます。

鍵を誰が持つかで、3つの形があります。

- 提供者の鍵を使う形
- 顧客が作って持ち込む形 (BYOK)
- 顧客が鍵を手元だけに置く形 (HYOK)

顧客が鍵を握るほど、提供者の管理者がデータを読む可能性は下がります。代わりに、運用の負担と、鍵を失うリスクが増えます。

場面で考えます。金融機関が、提供者の管理者にも平文を読ませたくないという要件で、クラウドのストレージを使う。提供者の鍵を使う形では、鍵の管理が提供者の側に残ります。BYOK なら、鍵は顧客が作りますが、使う時は提供者の鍵管理の中に置かれます。HYOK なら、鍵が顧客の手元から出ないので、提供者は復号できません。代わりに、手元の鍵が使えない間は、クラウド側の処理も止まります。要件の強さと、止まった時の影響を天秤にかけて選びます。

鍵のライフサイクルは、NIST SP 800-57 Part 1 の鍵の状態で見えます。[^{c1-11}]

状態	意味
前活性 (pre-activation)	作られたが、まだ使えない
活性 (active)	使える
停止 (suspended)	一時的に止めている
非活性 (deactivated)	新しい処理には使わず、既存データの復号や署名の検証だけに使う
危殆化 (compromised)	漏れた疑いか事実があると判断された
破棄 (destroyed)	鍵を復元できない

暗号鍵の有効期間 (cryptoperiod) は、特定の鍵の使用が許される期間で、鍵の種類と用途で決めます。期間を区切る理由は 2 つあります。同じ鍵で暗号化するデータ量を限ると、鍵を割り出す材料が減ります。1 本の鍵が漏れた時の被害も、期間の中に収まります。[^c1-11]

間違えやすい点は、「破棄」と「非活性」の区別です。非活性の鍵は、過去のデータを復号するために残します。危殆化した鍵は、新しい暗号化に使えません。調査のために扱いを決めておきます。

エンベロープ暗号化も出ます。データはデータ鍵 (DEK) で暗号化し、そのデータ鍵を鍵暗号化鍵 (KEK) で暗号化して、データのそばに置きます。KEK だけを KMS に置けば、守る対象は KMS に絞られます。KEK を回転して古い KEK を廃止する時に再暗号化するのは DEK だけで、大量のデータには触れません (KMS の自動回転のように古い鍵の版を残す場合は、DEK の包み直しも要りません)。

ID とアクセス制御 (ユーザー・特権・サービスのアクセス)

クラウドでは、境界のファイアウォールより先に、ID が防御線になります。アクセスは 3 種類に分けます。

- **ユーザーのアクセス:** 社員や顧客が使う。多要素認証 (MFA) とシングルサインオンで守る。
- **特権アクセス:** 管理者や root のように大きな権限を持つ。必要な時だけ昇格し、操作を記録し、承認を必須にする。
- **サービスのアクセス:** アプリやスクリプトが他のサービスを呼ぶ。人のパスワードではなく、ワークロードに割り当てた ID や短期の認証情報を使い、長期の鍵をコードに埋め込まない。

基本の原則は 2 つ。最小権限は、仕事に必要な権限だけを与えます。職務の分離は、1 人が申請と承認の両方を持たないようにします。権限が大きい操作ほど、事前承認、一時的な付与（ジャストインタイム）、全操作の記録を重ねます。

認証は、フェデレーションで受ける形が多く使われます。自社の ID 基盤で一度認証し、クラウド側はその結果を信頼する形。離職者の権限を自社側で止めれば、クラウド側にも反映されます。アカウントの消し忘れが減ります。

場面で考えます。開発者が、長期のアクセスキーをうっかり公開リポジトリに載せたとします。最初にやるのは、そのキーの失効。次に、キーが使われた形跡をログで調べます。再発の防止として、サービスには短期の認証情報を使い、コードの中の秘密情報を自動で検出する仕組みを入れます。キーを消さずに調査を先に進めると、その間も悪用されます。

データとメディアのサニタイズ(上書き・暗号消去)

メディアのサニタイズは、NIST SP 800-88 Rev.2 で 3 つに分けます。[^c1-12]

区分	中身
クリア (Clear)	通常の読み書きの操作で上書きなどを行い、簡単な復元的手段から守る
パージ (Purge)	物理または論理の方法で、最新の研究室の技術でも復元できないようにし、媒体は再利用できる可能性を残す
破壊 (Destroy)	媒体を物理的に壊し、再利用できなくする

暗号消去 (cryptographic erase) は、暗号化したデータの鍵を消して、データを読めなくする方法で、パージの一種です。物理媒体に触れないクラウドで、主な消去手段になります。論理的な(仮想の)記憶域では、物理媒体が抽象化さ

れ、顧客が直接触れません。SP 800-88 Rev.2 は、クラウドの記憶域では暗号消去がパージの唯一の実用的な方法になりうると述べています。[^c1-12]

場面で組み合わせます。契約を終える顧客が、オブジェクトストレージのデータを確実に消したいと言っています。提供者は、物理ディスクの破壊を顧客に見せられません。顧客が自分の鍵で暗号化していたなら、その鍵を KMS から削除すれば、データは読めなくなります。鍵が提供者の管理下だけにあったなら、提供者の消去手順と証明書に頼ります。暗号消去が確実に働く前提は 2 つあります。データが最初から強い暗号で暗号化されていること、鍵の複製がほかに残っていないことです。

ネットワークセキュリティ(ネットワークセキュリティグループ・トラフィック検査・ジオフェンシング)

ネットワークセキュリティグループ (NSG) は、仮想ネットワークの中で通信を許可、拒否する規則の集まりです。Azure の NSG で動き方を読みます。規則の優先度は 100 から 4096 で、小さい数が先に評価されます。通信が規則に当たると、その時点で評価は止まり、後ろの規則は見ません。既定の規則は 65000 から 65500 に置かれて最後に評価され、受信は最終的に全部拒否 (DenyAllInBound、65500) です。[^c1-13]

規則は、送信元、送信元ポート、送信先、送信先ポート、プロトコルの 5 要素で評価します。NSG はステートフルです。許可した通信の戻りには、別の規則を書く必要がありません。同じ優先度と方向の規則は、2 つ作れません。[^c1-13]

読み方の練習をします。仮想ネットワーク (ピアリング先を含む) のアドレス空間を 10.0.0.0/8 とし、次の規則 (受信) が置かれているとします。

優先度	名前	送信元	ポート	動作
100	AllowWeb	Internet	TCP 443	許可
200	DenyTenantA	10.1.0.0/16	TCP 443	拒否
65000	AllowVNetInBound (既定)	VirtualNetwork	すべて	許可
65500	DenyAllInBound (既定)	すべて	すべて	拒否

Internet から TCP 443 は、優先度 100 に当たって許可されます。10.1.2.3 から TCP 443 は、Internet ではなく VirtualNetwork に属するので、100 には当たりません。200 に当たって拒否です。10.2.2.3 から TCP 22 は 65000 に当たって許可。Internet から TCP 22 は、どの規則にも当たらず、65500 で拒否されます。

落とし穴は優先度の順序です。拒否の規則を許可の規則より後ろに置くと、同じ送信元には許可が先に当たり、拒否は効きません。個別の例外は、広い規則より小さい数にします。

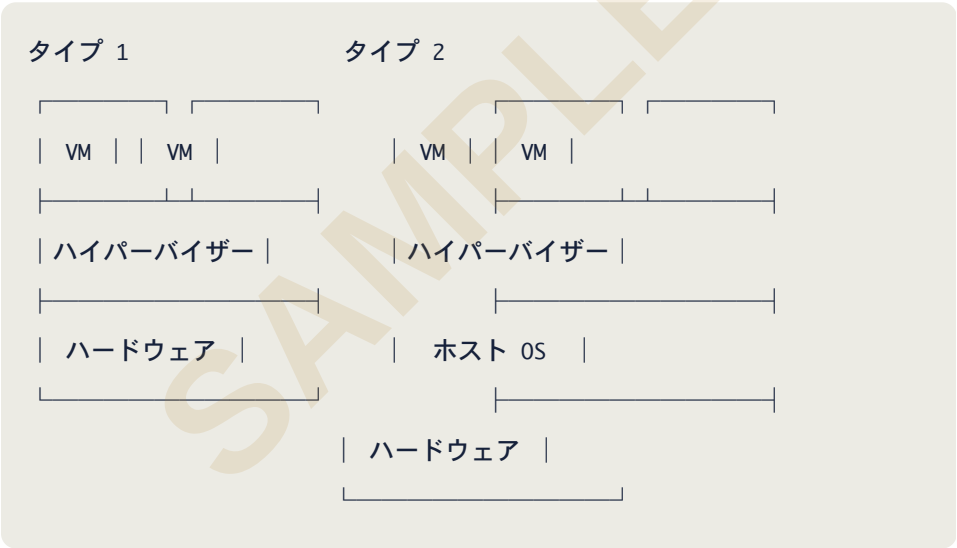
NSG には、ほかにも読み取りの型があります。送信元や送信先には、IP アドレスや CIDR のほか、サービスタグ(提供者のサービスの IP 群)と、アプリケーションセキュリティグループ(仮想マシンをアプリの役割で束ねた単位)を指定できます。規則を消しても、すでに張られた接続は切れません。規則が影響するのは新しい接続だけで、接続中の SSH の許可を消しても、その接続は続きます。新しい SSH だけが拒否されます。[^c1-13]

トラフィック検査は、通信の中身を調べて不正を見つける仕組みです。IDS は検知して通知するだけ。IPS は検知して止めます。クラウドでは、仮想ネットワークの通信記録(フローログ)を集めて異常を探します。ジオフェンシングは、

位置情報に基づいてアクセスの許可を制限する方法で、許可した国や地域だけからの接続を通します。データの置き場所を国内に制限する要件と、アクセス元を制限する要件は、別の話です。

仮想化セキュリティ①ハイパーバイザー(タイプ1・2・VM エスケープ)

ハイパーバイザーは、1 台の物理機器で複数の仮想マシンを動かす基盤です。タイプ1 はハードウェアの上で直接動き(ベアメタル)、パブリッククラウドの基盤はこちらです。タイプ2 はホスト OS の上で動くアプリとして動き、開発者の PC で使う仮想化ソフトがこれに当たります。[^c1-14]



タイプ2 はホスト OS の層が 1 つ多く、攻撃対象が広がります。そのため、機密データを扱う環境には向きません。クラウド事業者の基盤にタイプ2 を使うことは通常ありません。

VM エスケープは、ゲストの仮想マシンからハイパーバイザーや他のゲストへ抜け出す攻撃で、分離の失敗にあたります。[^c1-14] 成功すると、同じ物理機器にいる他の顧客のデータに届く恐れがあります。対策は 4 つです。ハイパー

バイザーのパッチを早く当てる。不要な機能（仮想デバイスなど）を無効にする。不要な機能はゲストが攻撃に使う入口になるので、無効にすれば入口が減ります。管理用の通信を分ける。管理用の通信を顧客の通信と分けると、ゲストから管理側へ入り込む経路が減ります。共有する資源（メモリや CPU のキャッシュ）の隔離を強める。顧客にできることは限られるため、提供者の対応を評価する話に結びつきます。

場面で考えます。同じ物理機器で動く別の顧客の仮想マシンから、自社の仮想マシンのメモリが読めてしまう脆弱性が公表されたとします。これは VM エスケープで、分離が破られた状態。顧客が直せるのはゲスト OS の側の対策までで、ハイパーバイザーのパッチは提供者が当てます。顧客は、提供者の通知とパッチ適用の時期を確かめ、必要なら専用の物理機器を使う構成を検討します。

仮想化セキュリティ②コンテナ・エフェメラル・サーバーレス・分離

コンテナはカーネルを共有するため、仮想マシンより分離が弱くなります。NIST SP 800-190 は、リスクを 5 つの対象に分けます。[^c1-15]

対象	リスクの例	手当て
イメージ	古い部品、脆弱性、埋め込まれた秘密情報	作成時に検査する
レジストリ	偽のイメージの混入、通信の盗聴	信頼できる提供元に限り、通信を暗号化する
オーケストレータ	管理者権限の悪用	権限を絞る
コンテナ	過大な実行権限、特権コンテナ	実行時の権限を最小にする
ホスト OS	ホストの脆弱性	コンテナ専用の最小構成にする

エフェメラル(一時的な)コンピューティングは、短時間だけ存在し、終わると破棄される資源の使い方です。状態を持たないので、攻撃者が居座りにくく、設定のずれも起きにくくなります。一方で、ログを外に出さないと、破棄された後に調査の材料が消えます。サーバーレスは、提供者が実行基盤を管理し、顧客は関数のコードと設定だけを持つ形。OSのパッチは提供者の仕事です。顧客の責任は、関数の権限、入力の検証、依存部品、秘密情報の扱いに絞られます。

分離(アイソレーション)は、これらすべての土台。仮想マシンはハイパーバイザー、コンテナはカーネルの機能で分離します。サーバーレスの分離は、提供者の実行環境が担います。分離が強い順は、おおむね専用機器、仮想マシン、コンテナの順。同じ機器を共有する範囲が広いほど、分離が破られた時の影響も広がります。

場面で考えます。開発チームが、公開レジストリから取ってきたイメージを、そのまま本番で動かしています。このイメージには、古い部品や、埋め込まれた秘密情報のリスクがあります。対策は、作成時の検査と、信頼できる提供元に限ること。実行時は、特権を外して最小の権限で動かします。すべてを仮想マシンで包む必要はありません。分離の強さと軽さのどちらを取るかで選ぶ問題。

一般的なクラウドの脅威

CSA (Cloud Security Alliance) は、クラウドの重大な脅威の報告を定期的に出しています。2024 年版は 11 の脅威を挙げ、上位 3 つは次の順です。[¹⁶]

1. 設定の誤りと不十分な変更管理
2. ID とアクセス管理
3. 安全でないインターフェースと API

4 位以下には、クラウドのセキュリティ戦略の選択と実装の不備、安全でないサードパーティの資源、安全でないソフトウェア開発が続きます。意図しないクラウドでの公開、システムの脆弱性、クラウドの可視性の不足、認証なしの資源の共有、APT (高度で持続的な脅威) も並びます。

脅威は、設定ミスから始まるものが目立ちます。典型は、公開設定になった保存先、広すぎる権限、履歴の残らない手作業の修正。対策は、設定をコードで管理して差分を見ること、変更を承認の流れに載せること、設定の逸脱を自動で検知することの 3 つです。

脅威	起きること	効く対策
設定の誤り	保存先の意図しない公開	設定基準の自動検査、変更管理
ID とアクセスの不備	盗まれた認証情報で侵入	MFA、最小権限、特権の管理
安全でない API	認可の抜けを突かれる	認証と認可、入力を検証、レート制限
可視性の不足	侵害に気づけない	ログの集約と監視
意図しない公開	機密が外から見える	データの分類、公開の禁止設定

場面で考えます。ストレージが意図せず公開され、顧客データが外から読める状態だったとします。原因は、設定の誤りと、変更管理の不足です。根本の対策は、公開設定を禁じる基準を作り、設定を自動で検査し、変更を承認の流れに載せること。ログを見る体制は、気づくための手段で、原因そのものは防ぎません。

セキュリティハイジーン(パッチ・ベースライン・不変アーキテクチャ・ハードニング)

ハイジーンは、毎日の基本的な手入れです。パッチ管理は、脆弱性の修正を、重大度と影響を見て優先順位を付けて当てる作業です。ベースライン(基準構成)は、承認された安全な設定の見本で、実際の設定と見比べて逸脱を見つけます。ハードニングは、不要なサービス、ポート、アカウントを無効にして攻撃対象を減らす作業。CIS Benchmarks は、OS、クラウド、製品ごとの安全な設定の基準で、ハードニングの基準線になります。[^c1-17]

不変(イミュータブル)アーキテクチャは、動いている資源を直さず、直したイメージで作り直して置き換える方式です。サーバーに入って手で直すと、設定のずれが積み重なります。イメージを直して入れ替えれば、全台が同じ構成になり、問題が起きた時は前の版のイメージに戻せます。パッチも同じ。動いている機器に当てず、パッチ済みのイメージで作り直します。

間違えやすい点は、不変アーキテクチャでもパッチは当てるとのこと。変わるのは方法で、動いている機器に当てる代わりに、作り直して当てる点。

場面で考えます。100 台のサーバーに、重大度の高い脆弱性のパッチを当てます。可変の運用では、1 台ずつ入って更新するので、台ごとにずれが出ます。不変の運用では、パッチ済みのイメージを作り、新しい台に入れ替えて、古い台を捨てます。ベースラインとの見比べて、全台が同じ状態かを確認できる点も、この方式の強み。

安全なクラウドの設計原則 [1.4]

クラウドの安全なデータライフサイクル

CSA のクラウドセキュリティガイダンスは、データのライフサイクルを 6 段階で示します。作成、保存、使用、共有、アーカイブ、破棄の順。[^c1-18] 順序には理由があります。作ってから保存し、保存したものを使い、使ったものを共有し、使わなくなったものをアーカイブし、保存期間が過ぎたら破棄します。

段階ごとに、先に打つ手が決まっています。

段階	打つ手
作成	分類とラベル付けで、以降の扱いを決める
保存	暗号化とアクセス制御を適用する
使用	権限を確認し、メモリ上の保護を考える
共有	DLP と、共有先の制限を使う
アーカイブ	保存期間と、長期の暗号鍵の保管を決める (保存期間は破棄へ進む時期を決め、長期の鍵の保管はアーカイブ中のデータを読める状態を守る)
破棄	暗号消去などで、データを読めなくする

並べ替えの型で出る点があります。分類は作成の直後で、保存の後ではありません。分類が先にないと、保存時の暗号化の強さを決められないからです。破棄はアーカイブの後で、共有の前ではありません。共有に使うデータを、先に消すことはないためです。

場面で考えます。営業が顧客リストを作り、保存し、取引先に共有します。共有の前に、DLP で個人情報の持ち出しを検査します。契約が終わり、保存期間が過ぎたら、アーカイブから破棄へ進み、暗号消去で読めなくする流れ。

クラウドベースの BC/DR 計画

事業継続計画 (BCP) は、障害の間も重要な業務を続ける計画です。災害復旧計画 (DRP) は、止まった ICT を復旧する計画で、BCP の一部にあたります。クラウドは、複数のアベイラビリティゾーンや複数のリージョンに分けて置けます。自前の拠点を持たなくても、冗長な構成を作れます。責任は共有。提供者

は基盤の可用性を担い、顧客は自分のデータとアプリをどこまで分散するかを決めます。

目標の語は 3 つあります。[^c1-19]

- **MTD** (最大許容停止時間): 業務が止まってよい最大の時間
- **RTO** (目標復旧時間): 復旧までの目標時間
- **RPO** (目標復旧時点): 失ってよいデータの時点。どこまで遡るかを表す

RTO は MTD を超えないように決めるので、通常は MTD より短くなります。
RPO は MTD の一部ではありません。データ損失の許容を表す、別の軸です。

計算で確かめる例です。バックアップを 4 時間ごとに取り、12:00 の取得の後、13:30 に障害が起きたとします。失うデータは、12:00 から 13:30 までの 1 時間 30 分。最悪の場合は、取得の間隔と同じ 4 時間分を失います。RPO が 1 時間なら、間隔 4 時間のバックアップでは目標に届きません。間隔を 1 時間以下に縮めるか、継続的に複製する方式へ変えます。

AWS は、復旧の方式を 4 つ示しています。[^c1-41]

方式	中身	復旧の速さ	費用
バックアップと復元	バックアップから、基盤、設定、アプリを作り直す	最も遅い	低い
パイロットライト	データは常に複製し、アプリのサーバーは止めておく。要求を処理するには、起動と拡大が先に要る	速くなる	やや低い

方式	中身	復旧の速さ	費用
ウォームスタンバイ	縮小した完全な環境を常に動かす。縮小のまま、すぐ要求を処理できる	さらに速い	中
マルチサイト(アクティブ/アクティブ)	複数のリージョンで同時に動かす。切り替えの概念がない	ゼロに近い	最も高い

下の行ほど復旧は速くなり、費用は高くなります。パイロットライトとウォームスタンバイの違いは、追加の作業なしで要求を処理できるかどうか。選ぶ時は、BIA で決めた RTO と RPO を満たす方式のうち、最も安いものを選びます。

場面で考えます。RTO が 15 分、RPO が 5 分の決済システムがあります。バックアップと復元では RTO が届きません。パイロットライトでも怪しくなります。ウォームスタンバイ以上を選び、データは継続的に複製します。1 つのリージョンだけに置くと、リージョン全体の障害で止まるので、別のリージョンにも複製を持ちます。計画は試験して初めて意味を持ちます。定期的な演習での、RTO と RPO の実測。

計画の作り方には順番があります。NIST SP 800-34 は、7 つの手順を示します。[^c1-19]

1. 計画の方針を決める。
2. BIA を行う。
3. 予防の対策を特定する。
4. 復旧の戦略を作る。
5. 計画を文書にする。

6. 試験、訓練、演習を行う。

7. 計画を保守する。

実際に障害が起きた後は、3つの局面で進みます。起動と通知（被害を評価して計画を発動する）、復旧（代替の環境で業務を再開する）、元の状態への復帰（本来の環境を戻して切り戻す）の順です。BIAが計画より先で、演習が計画の後ろにある点が、並べ替えて問われます。

事業影響度分析(BIA)と費用対効果分析・ROI

BIA（事業影響度分析）は、業務が止まった時の影響を調べ、復旧の優先順位と目標を決める作業です。手順は次の順です。

1. 業務と、それを支える資源（システム、人、依存先）を洗い出す。
2. 停止が続く時間ごとに、影響（収益、法令、評判など）を見積もる。
3. 影響が許容を超える時点から MTD を決め、RTO はそれを超えないように導く。RPO は MTD とは別に、失ってよいデータの量から決める。
4. 復旧の優先順位を付ける。

クラウドの BIA は、提供者への依存も範囲に入れます。サービスの停止、提供者の廃業、契約の終了が、自社の業務にどう響くかを見ます。

費用対効果分析は、対策の費用が、減らせる損失より小さいかを比べる分析です。式は3つあります。

- 年間の損失予測 (ALE) = 1 回の損失額 (SLE) × 年間の発生率 (ARO)
- 対策の価値 = 対策前の ALE - 対策後の ALE - 年間の対策費用 (正なら採用する価値がある)
- 投資利益率 (ROI) = (得られる便益 - 費用) ÷ 費用

数字で確かめます。1回の損失が250,000円で、年に0.4回起きるなら、ALEは100,000円です。対策を入れると発生率が0.1回になり、ALEは25,000円に下がります。減らせる損失は75,000円。対策の費用が年30,000円なら、価値は $75,000 - 30,000 = 45,000$ 円で、ROIは $45,000 \div 30,000 = 150\%$ です。

別の例です。便益が180,000円で費用が120,000円なら、ROIは $(180,000 - 120,000) \div 120,000 = 50\%$ です。費用が80,000円の対策が75,000円の損失しか減らないなら、価値は負になります。リスクの受け入れか、別の対策の検討。ROIの分母は便益ではなく費用で、ALEのSLEは年間ではなく1回の損失です。

複数の案を比べる例。1回の損失250,000円で、今のALEは100,000円とします。案Aは費用が年30,000円で発生率が0.1回、案Bは年50,000円で0.05回、案Cは年10,000円で0.3回になります。減らせる損失は、Aが75,000円、Bが87,500円、Cが25,000円。費用を引いた価値は、Aが45,000円、Bが37,500円、Cが15,000円で、ROIはAが150%、Bが75%、Cが150%です。減らせる額が最大なのはBですが、価値が最大なのはAです。ROIが同じ150%でも、AとCの価値は3倍違います。比率だけで選ばず、絶対額でも比べます。

機能的セキュリティ要件(ポータビリティ・相互運用性・ベンダーロックイン)

ベンダーロックインは、独自の形式や機能に依存して、別の提供者へ移れない(移す費用が高い)状態です。^[^c1-18] 対策は、設計の段階から入れます。

- データを標準の形式で出せるようにする
- 独自機能への依存を限る
- インフラをコードで定義して、別の環境でも再現できるようにする

- コンテナなど、移しやすい単位を使う
- 契約に出口の条項（データの返却と消去、移行の支援）を入れる

トレードオフもあります。ロックインを避けるために共通の機能だけを使うと、提供者の強みを活かせず、運用の費用が増えます。完全に避ける必要はありません。どの機能に依存するかを意識して選び、出口の費用を見積もっておきます。ポータビリティと相互運用性は 1.2 の定義のままで、この要件を測る物差しとして使います。

場面で考えます。ある会社が、提供者独自の分析機能に強く依存したシステムを作ったとします。乗り換えを考えた時、データは出しても、分析の手順が移せません。設計の段階で、標準の形式、コンテナ、インフラのコードを選んでいれば、移す費用は小さくて済みます。

カテゴリごとのセキュリティの考慮事項と責任 (SaaS・IaaS・PaaS の責任共有)

責任共有モデルは、安全の仕事を提供者と顧客で分ける表です。IaaS は OS から上が顧客、PaaS はアプリの構成とコード、データが顧客（アプリの基盤は提供者と共有）、SaaS はデータとアカウントとアクセスが顧客です。どの型でも、データ、設定、ID とユーザーは顧客の責任です。端末は、Microsoft の表では SaaS だけ「共有」（Microsoft が端末管理の機能を出し、端末の保護は顧客）ですが、同じページは端末を常に顧客に残る責任にも挙げています。

[^c1-20]

領域	IaaS	PaaS	SaaS
顧客のデータ	顧客	顧客	顧客
設定	顧客	顧客	顧客
ID とユーザー	顧客	顧客	顧客

領域	IaaS	PaaS	SaaS
端末	顧客	顧客	共有
アプリケーション	顧客	共有	共有
ネットワーク制御	顧客	共有	提供者
OS	顧客	提供者	提供者
物理ホスト・物理ネットワーク・データセンター	提供者	提供者	提供者

表の上の行は、どの型でも顧客に残る責任です。下の行へ進むほど、提供者の持つ範囲が広がります。「OS」の行で IaaS だけが顧客になっている点が、IaaS と PaaS の境目です。「ネットワーク制御」の行は、SaaS では提供者で、IaaS では顧客が自分でファイアウォールを設定する点と対になります。物理の層は、どの型でも提供者の責任。

場面で確かめます。SaaS の顧客管理サービスで、退職した社員のアカウントが残っていて、外部から不正にログインされたとします。責任は顧客側。アカウントと ID の管理は、どの型でも顧客に残るためです。IaaS の仮想マシンの OS に重大な脆弱性が見つかったなら、パッチを当てるのは顧客です。PaaS の実行環境の OS なら、提供者が更新します。

クラウドの設計パターン (SANS のセキュリティ原則・Well-Architected・CSA エンタープライズアーキテクチャ・セキュアバイデザイン)

セキュリティの設計原則は、古くからある決まりです。試験範囲は例に「SANS のセキュリティ原則」を挙げますが、ここでは、広く使われる Saltzer と Schroeder の古典的な原則を中心に、よく使われる設計原則を表にします。

原則	意味
最小権限	仕事に必要な権限だけを与える
多層防御	防御の層を重ね、1つ破られても止める
フェイルセーフ	失敗した時は、安全な側に倒す
完全な仲介	アクセスのたびに許可を確認する
設計の公開	安全性を、設計の秘密に頼らない
機構の経済性	仕組みを単純に保つ

Well-Architected フレームワークは、設計を評価する物差しで、柱で分けます。

クラウド	柱
AWS (6 つ) [^c1-21]	運用上の優秀性・セキュリティ・信頼性・パフォーマンス効率・コスト最適化・持続可能性
Azure (5 つ) [^c1-22]	信頼性・セキュリティ・コストの最適化・オペレーショナルエクセレンス・パフォーマンス効率

数の差は、持続可能性が AWS の柱にあり、Azure の柱にはないことから生まれます。

CSA のエンタープライズアーキテクチャは、クラウドの設計と評価に使う参照モデル。ドメインは 4 つあります。事業運営支援サービス (BOSS)、IT 運用とサポート (ITOS)、技術ソリューションサービス (TSS)、セキュリティとリスク管理 (SRM) です。[^c1-23]

セキュアバイデザインは、製品を作る側が、設計の初めから安全を組み込む考え方です。CISA が示す 3 原則は、顧客のセキュリティの結果に責任を持つこ

と、徹底した透明性と説明責任を持つこと、それを実現する組織と経営層の仕組みを作ること(トップから率いる)です。[^c1-42] 安全な設定を初期値にして、利用者に追加の費用や手間を負わせない点が、具体的な形になります。

見分け方を確かめる場面。設計レビューで「失敗した時に安全な側へ倒れるか」と聞かれたら、原則はフェイルセーフです。「AWS にだけある柱は何か」なら、持続可能性。「製品を作る側が、設定を安全な初期値で出す」なら、セキュアバイデザインです。

DevOps のセキュリティ

DevOps の流れの全段に、セキュリティを入れます。流れは、計画、コード、ビルド、テスト、リリース、配置、運用。

段	入れるセキュリティ
コード	秘密情報をコードに書かない。依存部品を検査する
ビルド	静的解析と部品の脆弱性検査を自動で回す。成果物に署名する
配置	インフラのコード (IaC) を検査する。承認を経た成果物だけを本番に出す
運用	ログと監視で、逸脱を検知する

秘密情報は専用の仕組みに置き、実行時に短い期間だけ渡します。パイプラインそのものも攻撃の対象です。パイプラインの権限を絞り、変更を記録すること。NIST SP 800-218 (SSDF) は、安全なソフトウェア開発の実践を体系化した枠組み。[^c1-24] ソフトウェア部品表 (SBOM) は、成果物に含まれる部品の一覧で、脆弱性が出た時に影響範囲を調べるのに使います。

場面で考えます。コードから本番まで、人が触れずに進む配置の自動化があります。ビルドで脆弱性を検査し、署名のない成果物は本番が受け付けません。パイプラインの管理者権限を奪われると、署名済みの偽の成果物を出されてしまいます。だから、権限と変更の記録を絞ります。

クラウドサービスプロバイダーの評価 [1.5]

基準に照らした CSP の検証 (ISO/IEC 27001・27017・SOC 2・CSA STAR・PCI DSS)

CSP を評価するとは、第三者が検証した証拠を読むことです。証拠の種類を並べた表。

基準	何を示すか	読み方
ISO/IEC 27001	組織の情報セキュリティマネジメントシステム (ISMS) が要求事項を満たす	認証の範囲 (どのサービスと拠点か) を確かめる
ISO/IEC 27017	クラウドサービスの情報セキュリティ管理策の実践の規範 (27002 に基づく)。顧客と提供者の両方に向けた手引き	責任の分担が書かれているかを見る
ISO/IEC 27018	パブリッククラウドで PII を処理する提供者の、PII 保護の実践の規範	個人情報を預ける時に見る
SOC 2	提供者の統制を、監査人が信頼サービス基準で報告する	Type の違いと対象期間を見る
CSA STAR	クラウドに特化した保証の制度	レベル 1 か 2 かを見る

基準	何を示すか	読み方
PCI DSS	カード会員データの保護の基準	提供者の対象範囲と、顧客の責任を確かめる

27017 と 27018 の位置づけは表のとおり。[^c1-25][^c1-26] SOC 2 は、AICPA の信頼サービス基準 (セキュリティ、可用性、処理の完全性、機密保持、プライバシー) に沿った報告書です。Type 1 は、ある時点で統制が適切に設計されているかを示します。Type 2 は、一定の期間にわたって統制が実際に運用されていたかを示します。購入者が見るべきは、期間が最近の Type 2 です。[^c1-39]

CSA STAR は 2 段構え。レベル 1 は、提供者が自己評価 (CAIQ) を公開します。レベル 2 は第三者の監査で、ISO/IEC 27001 に基づく STAR 認証と、SOC 2 に基づく STAR 証明があります。[^c1-27] STAR は、CSA のクラウドコントロールマトリックス (CCM v4) が土台です。CCM v4 は 17 のドメインと 197 の管理目標を持ちます。[^c1-28] CAIQ は、CCM を質問の形にしたもの。

PCI DSS は、カード会員データを扱う組織に適用されます。提供者が準拠していても、顧客の側の構成まで準拠になるわけではありません。責任の分担表で、どの要件を誰が満たすかを確かめます。[^c1-40]

場面で選びます。個人情報に預けるパブリッククラウドを選ぶ会社が、第三者の検証済みの証拠を探しています。ISO/IEC 27001 の認証は組織の ISMS を示しますが、クラウド固有の管理策は 27017 が、PII の保護は 27018 が補います。統制の運用の実績を期間で見たいなら、答えは SOC 2 の Type 2。自己評価の公開で済ませる提供者より、STAR のレベル 2 を持つ提供者のほうが、第三者の検証がある分だけ強い証拠になります。

FedRAMP は、米国連邦政府がクラウドサービスを使うための、標準化した評価と認可の制度です。[^c1-32] 連邦政府の顧客に売るなら必要で、一度の評価結果を複数の機関が再利用できます。

製品の認証(コモンクライテリア・EAL・FIPS 140-2/140-3 のレベル)

ここまでが組織とサービスの検証で、この項は製品やモジュールの認証です。コモンクライテリア (ISO/IEC 15408) は、製品のセキュリティ機能を評価する国際規格です。評価の要求は保護プロファイル (PP) に書き、製品が実際に主張する内容はセキュリティターゲット (ST) に書きます。評価の深さを表すのが、評価保証レベル (EAL) 1 から 7 です。[^c1-29]

EAL	名前
EAL1	機能テスト
EAL2	構造テスト
EAL3	方式的テストとチェック
EAL4	方式的設計・テスト・レビュー
EAL5	準形式的設計とテスト
EAL6	準形式的検証済み設計とテスト
EAL7	形式的検証済み設計とテスト

数字が大きいくほど、評価の厳密さ(保証)が増します。EAL が高い製品が「安全な機能を多く持つ」という意味ではありません。機能の強さではなく、評価の深さを表します。

FIPS 140-3 は、暗号モジュールの要件で、レベル 1 から 4 があります。レベルが上がるほど、物理的な耐タンパ性と、ID に基づく認証などが求められます。[^c1-30]

レベル	求める保護
1	基本的な要件。特別な物理的保護は求めない
2	改ざんの痕跡を残す仕組みと、役割に基づく認証
3	改ざんへの抵抗と、ID に基づく認証
4	改ざんの検知と対応、環境の異常への耐性

クラウドの KMS や HSM を選ぶ時は、規制や契約が要求するレベルで検証済みかを確かめます。

コモンクライテリアと FIPS 140 は、見るものが違う規格。コモンクライテリアは、製品のセキュリティ機能が主張どおりに作られ、試験されているかを、保証の深さ (EAL) で評価します。FIPS 140-3 は、暗号モジュールの実装が、暗号の要件を満たすかを、レベル 1 から 4 で検証します。KMS の暗号処理の強さを確かめたいなら FIPS 140-3、製品全体の保証の深さなら EAL です。ISO/IEC 27001 の認証と SOC 2 の報告書も、別物。前者は審査機関が組織の仕組みを認証する制度で、後者は監査人が統制を報告する形式です。

FIPS 140-2 は、FIPS 140-3 の前の版です。2026-09-21 に、FIPS 140-2 の検証は履歴の一覧へ移りました。履歴の一覧のモジュールも、既存のシステムでは使えます。^[^c1-31] 新しく選ぶ時は FIPS 140-3 を優先します。選択肢に両方があるなら、現行は 140-3 です。

人工知能と機械学習の理解 [1.6]

AI/ML によるクラウドの脅威の検出と分析

機械学習は、平常時の動きを学び、そこからのずれを異常として見つけます。ログイン時刻、アクセス先、転送量のずれから、乗っ取りや内部者の不正に気づけます。ルールを書かなくても未知の手口を拾える点が強み。弱みは、誤検知(正常を異常と判定)と見逃し(異常を正常と判定)が出ること、学習データに無かった状況に弱いことです。

AIを守る側の知識も問われます。NIST AI 100-2 E2025 は、敵対的機械学習の攻撃を、学習の段階(訓練時・配備時)と攻撃者の狙いで整理しており、狙いは可用性・完全性・プライバシーの侵害、生成 AI ではこれに悪用の可能化が加わります。代表的な攻撃は次の4つです。[^c1-34]

- **回避(evasion)**: 入力を細工して誤判定させる
- **汚染(poisoning)**: 学習データを細工してモデルをゆがめる
- **プライバシーへの攻撃**: メンバーシップ推論やデータ再構成で学習データの情報を、モデル抽出でモデルの情報を引き出す
- **プロンプトインジェクション(生成 AI)**: 細工した指示で、モデルの制限をすり抜けさせる(悪用の可能化)、情報を引き出すなど

MITRE ATLAS は、AI システムへの攻撃の戦術と技術を集めた知識ベースで、ATT&CK の AI 版にあたります。[^c1-35]

データソースの検証と確認

AI の判断は、入れるデータの質で決まります。データソースの検証は、出所(誰が作ったか)、完全性(改ざんされていないか)、鮮度(古くなっていないか)、偏りの有無を確かめる作業です。署名やハッシュで改ざんを検出し、受け入れる提供元を限り、取り込み前に外れ値と異常な偏りを調べます。汚染の攻撃は、学習データに少量の悪意あるデータを混ぜて起きます。入口での検証が防御の中心。

クラウドのログを AI に読ませる時も同じ考え方です。ログが改ざんされていたり、一部の資源のログが欠けていたりすると、検出は鈍ります。ログの完全性と網羅性は、先に確かめておくこと。

場面で考えます。外部から買った脅威情報のデータを、検出モデルの学習に使います。出所の署名を確かめ、取り込み前に外れ値を調べ、重要なデータは自社の記録と突き合わせます。何も検証せずに取り込めば、汚染された学習データでモデルがゆがみます。

SOAR(セキュリティのオーケストレーション・自動化・対応)

SOAR は、セキュリティのオーケストレーション、自動化、対応の略。手順(プレイブック)に沿って、アラートの調査と対応を自動でつなぎます。[1-38] 例えば、不審なログインのアラートが出たら、IP の評判を照会し、ユーザーに確認を送り、返事がなければアカウントを一時停止して、チケットを作ります。チケットは対応の記録で、後から人が確かめられるようにします。

SIEM との違いも出る論点。SIEM はログを集めて相関を取り、アラートを出す仕組みです。SOAR は、そのアラートを受けて調査と対応の手順を自動で動かす仕組みです。両者は組み合わせて使われる関係。自動化には、人の承認を挟む段が要ります。アカウントの停止や通信の遮断のように業務に影響する操作は、誤検知の時の被害が大きいからです。

場面で考えます。AI の異常検知が、深夜の大量ダウンロードを警告したとします。誤検知かもしれないので、プレイブックの最初の手は、利用者への確認。返事がない場合にだけ、権限を一時停止します。いきなり停止しない理由は、正当な作業を止める恐れ。

AI の倫理的懸念(偏り・説明可能性・透明性)

3つの語を区別します。

- **偏り:** 学習データや設計の片寄りが、特定の集団への不公平な結果を生むこと
- **説明可能性:** モデルがなぜその結果を出したかを、人が理解できる性質
- **透明性:** AI を使っていること、その能力と限界、データの扱いを、関係者に開示すること

NIST AI RMF 1.0 は、リスク管理の 4 つの機能を置きます。統治 (Govern)、マップ (Map)、測定 (Measure)、管理 (Manage) で、2023-01 に公表されました。[^c1-33] 統治は方針と責任の置き場、マップは文脈とリスクの洗い出し、測定は分析と評価、管理は対応と優先付けです。信頼できる AI の特性は 7 つで、妥当で信頼できる、安全、セキュアで回復力がある、説明責任と透明性がある、説明可能で解釈可能、プライバシーが強化されている、有害な偏りが管理されて公平、です。

AI の規制要件

EU AI 法 (Regulation (EU) 2024/1689) は、AI をリスクの段で規制します。許容できないリスクは禁止、高リスクは厳しい義務、限定的なリスクは透明性の義務、最小限のリスクは自由です。[^c1-36]

適用の日は段階的です。

日付	適用されるもの
2024-08-01	発効
2025-02-02	禁止の規定
2025-08-02	汎用 AI モデルの義務
2026-08-02	残りの大部分

日付	適用されるもの
2027-12-02	Annex III の高リスク(デジタルオムニバスで延期)
2028-08-02	Annex I の製品に組み込まれる高リスク(同)

高リスクの義務は、2026-08-02 の原則の日から外れ、延期されています。
[^c1-36]

場面で考えます。採用の選考に AI を使う会社が、EU の応募者を扱います。雇用の選考は高リスクの分野に当たり、適用は 2027-12-02 からです。求められるのは、人による監督と記録。

ISO/IEC 42001 は、AI マネジメントシステムの要求事項 (2023) で、ISO/IEC 27001 の AI 版にあたる認証の枠組みです。[^c1-37] 規制は地域で異なります。クラウドの AI サービスを使う組織は、サービスを提供する地域と、データの主体がいる地域の両方の法を確かめます。

サンプルはここまでです

続き(第2章～巻末)は、CCSP 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。

CCSP 学習用テキスト(無料サンプル)

版

2026年10月版(ISC2「CCSP Certification Exam Outline」(2026年8月1日発効・日本語版の試験概要も同日付) 準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

「CCSP」は ISC2 (International Information System Security Certification Consortium, Inc.) の登録商標です。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 ISC2 公式の試験範囲 (CCSP Certification Exam Outline・2026年8月1日発効) と公開されている規格・文書を基に作成したもので、ISC2 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。