

IT 資格 道 場

Microsoft Cybersecurity Architect (SC-100) 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)

SC-100 出題範囲(Study guide・Skills measured as of October 21, 2026)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

この教材の使い方

準拠する版: Skills measured as of October 21, 2026

試験の基本情報

出題分野と配点比率: どこに時間を使うか

第1章 Design solutions that align with security best practices and priorities [1.1/1.2/1.3]

業務の回復性の目標と、業務に欠かせない資産への脅威 [1.1]

BCDR の考え方: RPO・RTO・Azure Backup と Azure Site Recovery [1.1]

安全なバックアップと復元: 不変・論理削除・多重の承認 [1.1]

ランサムウェア対策の優先順位: 3 つの手順 [1.1]

ランサムウェア対策での特権アクセスの保護の優先 [1.1]

セキュリティ更新の方式の評価: Azure Update Manager・Windows Autopatch・Intune の更新リング [1.1]

MCRA の構成と使い方: 機能の地図・参照の図 [1.2]

MCSB の制御ドメインと、制御を設計に当てはめる [1.2]

内部・外部・サプライチェーンの攻撃への防御のベストプラクティス [1.2]

AI ソリューションを MCSB に合わせる: AI セキュリティの制御 [1.2]

ゼロトラストの 3 原則: 明示的に検証・最小特権・侵害を想定 [1.2]

ゼロトラスト導入フレームワーク: 業務のシナリオと技術の柱 [1.2]

安全な AI 導入の戦略: 導入シナリオ・シャドー AI・責任ある AI [1.3]

CAF の段階とセキュリティの方法論 (Secure)・セキュリティの役割 [1.3]

WAF のセキュリティの柱: 設計原則と推奨事項による新規設計・既存の評価 [1.3]

CAF と WAF に基づくセキュリティとガバナンスの推奨 [1.3]

Azure ランディングゾーン: 設計領域・プラットフォームとアプリケーションのランディングゾーン・管理グループ [1.3]

サンプルはここまでです

SAMPLE

このテキストの位置づけ: 3 点セットの本編。これだけで場面の問題が解けるようになることを目標に、枠組み・製品・プランの選び分けを合格ラインの深さで説明します。① 学習用を読む → ② 頻出度別で選び方を掴む → ③ 問題演習で腕試し → ④ 頻出度別に戻って再確認(試験直前もここ)。暗記用は空き時間や用語の再確認に使います。

SAMPLE

この教材の使い方

SC-100(Microsoft Cybersecurity Architect) は、セキュリティ全体の設計者に向けた試験です。問われるのは設定画面の操作ではなく、場面の条件を読んだうえでの判断。どの枠組みか、どの製品とプランか、どの順番か。似た2つの機能のどちらを取るかで迷わせる設問が中心になります。

各章は細目ごとに節が分かれていて、見出しの末尾の [1.1] は公式の試験ガイドの細目の番号。節の中には、名前の似た機能の切り分けを表にして置き、難しい論点には場面の判断を1段落ずつ添えてあります。

脚注の番号は、出典の該当箇所を指します。本文で迷ったときは、末尾の「商標と出典」から一次情報を開いて確かめるとよいでしょう。

準拠する版:Skills measured as of October 21, 2026

このテキストは、2026 年 10 月 21 日版の Study guide に合わせてあります。日本語版の試験は英語版より遅れて切り替わるので、受ける言語の版は申し込みの前に公式サイトで確かめておいてください。

試験の基本情報

項目	内容
試験名	SC-100: Microsoft Cybersecurity Architect
出題範囲の版	Skills measured as of October 21, 2026
合格点	700 点(1 から 1,000 までの換算点)

項目	内容
問題数と試験時間	公式の試験ページには記載がなく、申し込みの時に表示される
出題形式	公式は試験ごとの形式を公表していない。 選択式、ケーススタディ、はい/いいえの組などがあり得る

受験料と対応言語は、申し込みの前に試験の公式ページで最新の案内を確かめてください。

出題分野と配点比率：どこに時間を使うか

分野	配点	対応する章
1 セキュリティのベストプラクティスと優先順位に沿った設計	20～25%	第 1 章
2 セキュリティ運用・ID・コンプライアンスの設計	25～30%	第 2 章
3 インフラストラクチャのセキュリティ設計	25～30%	第 3 章
4 アプリケーションとデータのセキュリティ設計	20～25%	第 4 章

分野 2 と分野 3 は配点が最も厚く、この 2 つで全体の過半を占めるので、時間が足りないときは、第 2 章と第 3 章を先に固めます。

第1章 Design solutions that align with security best practices and priorities [1.1/1.2/1.3]

分野 1 の配点は 20～25% です[^c1-1]。設定画面の操作より、場面に対して「どの枠組みか、どの機能か、どの順番か」を選ぶ設問が中心になります。名前が似ている 6 つの枠組みの役割を、先に並べます。

枠組み	答える問い	単位	出てくる部品
MCRA	Microsoft の機能をどう組み合わせる 端から端まで守るか	組織全体の目標像	機能の地図、ゼロトラストのユーザーアクセス、SecOps、OT、マルチクラウドの図
MCSB	どの制御を満たせば構成が安全か	制御 (ID 付き) と Azure Policy	12 のセキュリティドメイン、他の基準への対応表
ゼロトラスト	何を信頼せず、どの順で導入するか	3 原則と導入の 6 段階	業務のシナリオ、技術の柱
CAF	Azure を組織へどの段階で導入するか	組織と環境	7 つの導入フェーズ、Secure の方法論
WAF	1 つのワークロードをどの観点で設計・評価するか	ワークロード	5 本の柱、セキュリティの設計原則
Azure ランディングゾーン	CAF の Ready で作る環境の実体	管理グループとサブスクリプション	プラットフォームとワークロードのランディングゾーン

細目 1.1:ランサムウェアなどの攻撃に対する回復性の戦略

業務の回復性の目標と、業務に欠かせない資産への脅威 [1.1]

業務の回復性の目標は、攻撃を受けても事業を続けられる水準を、時間とデータの量で先に決めた数字です。ランサムウェアの攻撃者は、身代金を払えば元に戻るという圧力で金を取ります。Microsoft の手順は、復旧できる状態を作って支払う動機を減らすことを狙い、バックアップを最重要の要素として最初に扱います[^c1-2]。

最も直接的に効く行動は、攻撃者にも自分たちにも書き換えられない不変のストレージから、企業全体を復元できる状態にすることです[^c1-3]。支払っても復号の鍵が届く保証はありません。届いても、全システムを戻せるとは限りません。

業務に欠かせない資産の優先順位付けは、次の 3 手で進めます[^c1-3]。

1. 侵害されたときの損害が最も大きい業務資産を決める。経営層が脅迫に応じかねない資産が目安になる。
2. 業務資産を IT 資産に置き換える。ファイル、アプリ、データベース、サーバー、制御システムが対象になる。
3. 一般の IT 環境に入った攻撃者が触れないように、保護または隔離する。

脅威の優先順位は、深刻度で並べた攻撃経路の一覧、つまり脅威モデリングの結果で決めます。WAF は、攻撃されやすい重要コンポーネントとデータの流れに、制御を優先して置くよう求めています[^c1-4]。MCRA も、セキュリティの作業に徹底して優先順位を付ける姿勢を前提にしています[^c1-5]。態勢の改善は、露出した特権、安全でない構成、監視されていない資産といった、測れるリスク低減の大きさを順番で決めます[^c1-6]。

場面で見ます。受注システムと設計図面サーバーが事業の中心にあり、受注が 4 時間止まると損失が大きい会社です。全システムを同じ水準で守る設計

は成り立ちません。この 2 つの資産に RTO 4 時間、RPO 1 時間といった目標を先に決め、その復旧に必要なバックアップ、特権の管理、隔離の順で投資します。ただし最重要資産の特定と高い保証水準での保護は、長く難しい作業です。Microsoft はこれを始めつつ、手順 1 と 2 の完了を遅らせないように求めています[^c1-3]。

BCDR の考え方：RPO・RTO・Azure Backup と Azure Site Recovery [1.1]

BCDR は事業継続 (BC) と災害復旧 (DR) の組です。BC は人、手順、技術を含む事業全体を止めない計画です。DR は、障害のあとにシステムを戻す部分を指します[^c1-7]。目標は 2 つの数字で決めます。

用語	意味	例
RPO (Recovery Point Objective)	許容できるデータ損失の最大時間	「30 分ぶんのデータ」
RTO (Recovery Time Objective)	許容できる停止の最大時間	「8 時間の停止」

コンポーネントや流れごとに、別の値を持てます。RPO と RTO を 0 にする設計は難しく、費用もかかります。技術と事業の関係者が話し合い、現実的な値を決めます[^c1-7]。

確かめ方は単純です。要件が RPO 8 時間、RTO 4 時間だとします。構成は 24 時間おきのバックアップで、復元に 5 時間かかります。最悪のデータ損失は 24 時間なので RPO を満たしません。復元の 5 時間も RTO の 4 時間を超えます。

Azure Backup と Azure Site Recovery (ASR) は、役割が違います。

項目	Azure Backup	Azure Site Recovery
役割	時点を持つコピーを保管して復元する	継続的なレプリケーションとフェールオーバーで業務を動かし続ける
保管先	Recovery Services コンテナー、Backup コンテナー	複製先のリージョンまたは Azure
データ損失	前回のバックアップ以降は失う	複製の頻度に左右される。計画済みのフェールオーバーなら損失なし
位置づけ	最後の手段として復元する	復旧目標を短く保つ主役

バックアップからの復元には、データ損失と復元時間が付きまといます。DR 計画には、バックアップに頼る前に試す手順の順序を書きます。復元の所要時間は RTO に含めて数えます[^c1-7]。

ASR で複製できる主な組み合わせは、次の 3 つです。ほかに、Azure Extended Zones からつながるリージョンへ、Azure Stack の VM から Azure へ、オンプレミスから別のサイトへの複製もあります[^c1-8]。

- Azure VM (リージョンから別のリージョンへ)
- オンプレミスの VMware、Hyper-V、物理サーバー (Azure へ)
- AWS の Windows インスタンス (Azure へ)

Hyper-V の複製頻度は最短 30 秒です。回復計画で多層アプリの起動順を決められ、Azure Automation のランブックや手動の操作も組み込めます。訓練用のテストフェールオーバーは、進行中の複製を止めずに実行できます。計画済みのフェールオーバーはデータ損失なし、計画外は複製頻度に応じた最小限の損失です[^c1-9]。

継続レプリケーションは、元のデータの変更を複製先へ追従させる仕組みです。削除や暗号化を過去の時点へ戻す用途は、時点を持つバックアップの役割になります。どちらか一方だけで足りる設計は、ありません。

ハイブリッドとマルチクラウドでは、次の形になります。Recovery Services コンテナは、VM、ワークロード、サーバー、クライアントのバックアップコピーを保管する Azure のストレージ エンティティです。オンプレミスの DPM、Azure Backup Server、MARS エージェントも、ここへバックアップできます。Azure の資産とオンプレミスの資産を見る画面は、別々にする必要があります [^c1-10]。他クラウドの Windows は、ASR で Azure へ複製します。

WAF は、復旧用のリソースと手順にも、本番と同じ水準の制御とバックアップ頻度を求めています。安全な状態を保存しておかないと、フェールオーバー先やバックアップの復元が脅威を持ち込むからです [^c1-4]。

安全なバックアップと復元：不変・論理削除・多重の承認 [1.1]

バックアップを狙う攻撃は、身代金を払わざるを得ない状況を作ります。そのためにバックアップと、復旧の手順書を先に壊します [^c1-3]。Azure Backup の防御は、層になっています。

層	仕組み	防ぐもの
隔離	コンテナのデータは Microsoft 管理のサブスクリプションとテナントに保管され、外部ユーザーとゲストは直接触れない	本番環境の侵害の巻き込み
RBAC	復旧ポイントを扱う組み込みロールが 3 つある	過剰な権限

層	仕組み	防ぐもの
論理的な削除 (soft delete)	削除後も一定期間データを残す	誤削除と悪意の削除
不変コンテナー	復旧ポイントを失う操作を遮断する	保持期間の短縮、削除
多重の承認 (MUA)	重要操作に別の人の承認を要求する	管理者の資格情報の悪用

論理的な削除の既定の保持は 14 日で、14～180 日に設定できます。14 日までは追加費用がかかりません。超えた日数には、通常のバックアップ料金がかかります。Recovery Services コンテナーでは標準で有効になり、無効にできません (secure by default)。Backup コンテナーも、3 つのリージョンでは一般提供です。ほかのリージョンはプレビューで、ポータルから無効にする選択肢が残ります[^c1-11]。コンテナー自体も、削除すると論理削除の状態へ移ります。

保持が 14 日を超えると、無料になるのは保持の末尾の 14 日です。保持 60 日で削除の 52 日後に復元すると、課金されるのは最初の 46 日です。最後の 6 日は無料になります[^c1-12]。この数え方は、次のコードで確かめました。

```
def billed(retention, restored_after, free=14):
    paid = min(restored_after, max(retention - free, 0))
    return paid, restored_after - paid    # (課金される日数, 無料の日数)

print(billed(60, 52))    # (46, 6)
```

不変コンテナーの状態は 3 つあります。

状態	動作
無効	何も遮断しない
有効	失う操作を遮断する。設定は無効に戻せる
有効かつロック済み	WORM ストレージを有効にし、ロックは不可逆。無効にできない (WORM にまだ対応しないリージョンやワークロードでも、ロックはバックアップのサービスが強制する)

状態が重要なのは、攻撃者が不変の設定を外せるかどうか、ロックで決まるからです[^c1-13]。

有効にするときの保持方式は 2 つです。バックアップポリシーに従う方式が既定で、不変の期間はポリシーの保持と一致します。保持を短くして復旧ポイントを消す変更は通りません。指定した日数だけ不変にする方式もあります。ポリシーの保持が 180 日で不変が 30 日なら、30 日を過ぎた復旧ポイントは削除できます。保持を 30 日未満へ短縮する変更は、できません[^c1-14]。

遮断される操作は、データを削除する保護の停止、保持を短くするポリシー変更、保持の短いポリシーへの差し替えです[^c1-15]。不変は、BLOB、ファイル、ディスクの運用バックアップには効きません。日数を指定する方式は、Recovery Services コンテナが対象です[^c1-16]。

多重の承認は、Resource Guard という別の Azure リソースで、重要操作を守ります。成り立つ条件は 2 つです。Resource Guard を別の人が所有していること。そして、コンテナの管理者が Contributor、Backup MUA Admin、Backup MUA Operator の権限を、Resource Guard に持たないことです。別のサブスクリプション、さらに別のテナントに置くほど、分離は強くなります[^c1-17]。

保護する操作には、必須と任意があります。論理削除などセキュリティ機能の無効化と、MUA 保護の解除は必須で、外せません。保護の削除、ポリシーの変更、暗号化設定の変更、不変の無効化、ハイブリッドコンテナの削除は任意です。復元は既定で保護の対象外になっています[^c1-18]。

重要操作の実行者は、セキュリティ管理者から Backup MUA Operator を期限付きで受け取ります。付与と取り消しには、PIM のような just-in-time の仕組みを使います。Contributor や Backup MUA Admin を一時的に渡すと、Resource Guard の削除権限まで渡ります。そのため渡すのは Operator だけです。データソース側で直接行う操作は、Resource Guard の守備範囲の外にあります[^c1-19]。

場面で見ます。バックアップ管理者の資格情報が盗まれ、攻撃者がバックアップの削除、論理削除の無効化、保持を 1 日にするポリシー変更を試みます。論理削除は無効にできない設定なので、残る試みは保持の短縮です。これは復旧ポイントの削除につながるため、不変コンテナのロックと Resource Guard が止めます。ロック済みなら、管理者が不変そのものを外すことはできません。承認者も別の人です。

逆に、不変だけでは、MUA が守る暗号化設定の変更などは止まりません。論理削除だけでは、保持を短縮する変更そのものは通ります（消えた復旧ポイントは、論理削除の保持期間だけ残る）。層が揃って初めて、攻撃者がバックアップを消して身代金を取る筋が閉じます。Microsoft の分類では、MFA や PIN などの帯域外の手順を挟むのが強い保護で、オンラインの不変ストレージやオフラインでの保管が最強の保護です[^c1-3]。

ランサムウェア対策の優先順位:3 つの手順 [1.1]

Microsoft が示す優先順位は 3 手順で、並びそのものに意味があります。ゼロトラスト導入の業務のシナリオにも、「侵害による業務被害の予防と軽減」が

あります[^c1-41]。前提は「侵害を想定する」ことです。緊急性が通常の IT やセキュリティの優先順位より勝つ、という前提で作られています[^c1-2]。

手順	狙い	主な項目	期限の目安
1 復旧の準備	身代金を払わず復旧できる状態にする	重要データの自動バックアップ、BC/DR 計画の定期的な訓練、バックアップの保護、復旧に要する文書の保護	30 日以内に MTTR を目標へ
2 被害の範囲を限る	攻撃者が複数の重要システムへ届く特権アクセスを減らす	特権アクセスの戦略、検出と対応	30～90 日
3 侵入を難しくする	入口を締める	リモートアクセス、メールとコラボレーション、エンドポイント、アカウント	30 日以内に全員の MFA

手順 1 の項目は 4 つです[^c1-21]。

1. 重要データを、決まった間隔で自動的にバックアップする。
2. BC/DR 計画を定期的に訓練する。ランサムウェアを自然災害と同じ重みで扱う。
3. バックアップを、意図的な消去と暗号化から守る。
4. 復旧に要する文書を守る。手順書、構成管理データベース、ネットワーク図が対象になる。

3 つ目の保護には 2 段階があります。強い保護は、バックアップを変更する前に MFA や PIN などの帯域外の手順を要求する方法です。最強の保護は、オン

ラインの不変ストレージ (Azure Blob など) か、完全なオフラインまたはオフサイトに保管する方法です。復旧に要る文書は、攻撃者が狙うので守ります。

手順 3 は、攻撃者が好む入口を領域ごとに締めます[^c1-36]。

領域	主な対策
リモートアクセス	機器とソフトの更新を保つ。Microsoft Entra ID と条件付きアクセスでユーザーとデバイスを検証する。既存のサードパーティ VPN の設定を固める。Azure の Point-to-Site VPN、Microsoft Entra アプリケーションプロキシ、Azure Bastion を使う
メールとコラボレーション	Office VBA の AMSI を有効にする。Defender for Office 365 など高度なメール保護をかける。攻撃面の縮小ルールを、まず監査モードで入れ、影響を確かめてからブロックモードにする
エンドポイント	攻撃面の縮小ルール、改ざん防止、初見のブロックを有効にする。セキュリティベースラインで強化する。更新とサポート対象のバージョンを保つ。安全でないシステムとプロトコルを隔離または廃止し、ホストのファイアウォールで想定外の通信を止める
アカウント	管理者と優先アカウントから、強力な MFA かパスワードレスを強制する。Microsoft Entra Password Protection で弱いパスワードを拒否し、オンプレミスの AD DS にも広げる

略称 ASR は、Azure Site Recovery と、攻撃面の縮小 (attack surface reduction) ルールの両方を指します。文脈で見分けます。

チェックリストの並びは、優先順位であって技術的な依存の順ではありません。そのためチームごとに並行して進めます。ただし手順 3 は項目が多く、時間がかかります。手順 1 と 2 の完了を遅らせてはいけません[^c1-2]。

場面で見ます。バックアップは一部のシステムだけで、オフラインでも不変でもなく、復元の訓練もしていません。AD DS のドメインコントローラーのような重要な IT システムも、含まれていません。この状態では、手順 1 は完了していません。MFA の展開 (手順 3) を先に進めたくりますが、バックアップの保護と訓練、ドメインコントローラーのバックアップを先に固めます[^c1-2]。

ランサムウェア対策での特権アクセスの保護の優先 [1.1]

特権を持つ攻撃者は、ほかのどの制御も無効にできます。ランサムウェアの攻撃者は特権アクセスを、重要資産を押さえて恐喝へ進む近道にします[^c1-22]。手順 2 の戦略は、4 項目です。

項目	内容	使う仕組み
エンドツーエンドのセッション保護	管理インターフェースへ入る前に、ユーザーとデバイスの信頼を検証する	Microsoft Entra の条件付きアクセス
ID システムの保護と監視	ディレクトリ、ID 管理、管理者アカウントとグループ、同意の付与の設定を守り、特権昇格を防ぐ	ID の保護と監視
横展開の緩和	1 台の侵害が、ほかの全デバイスの制御へ広がらないようにする	ローカルアカウントとサービスアカウントのパスワードの管理 (Windows LAPS など)
迅速な脅威対応	攻撃者の滞在時間とアクセスを減らす	検出と対応

30～90 日の目標は 3 つです。管理者の 100% が、保護された専用のワークステーションを使います。ローカルのワークステーションとサーバーのパスワードを、100% ランダム化します。特権昇格の緩和策を、100% 展開します[^c1-23]。エンドポイント、メール、ID への一般的な攻撃を数分で修復できるよう、検出と対応も備えます。その項目は次の 5 つです[^c1-23]。

1. 入口を優先する。Microsoft Defender XDR のような統合 XDR で質の高いアラートを出し、パスワードスプレーなどの総当たりを監視する。
2. 攻撃者がセキュリティを無効にする動きを監視する。イベントログの消去（特に Security と PowerShell Operational）や、セキュリティツールの無効化が対象になる。
3. ありふれたマルウェアを軽視しない。攻撃者は標的への侵入口を闇市場で買う。
4. 社外の専門家（Microsoft の DART など）を手順に組み込む。
5. Defender for Endpoint で、影響を受けた端末を素早く隔離する。

手順 2 で使う PIM（権限を常時は持たせない）、Privileged プロファイルの PAW（管理者の端末を最高の水準で守る）、緊急アクセス用アカウント（障害時の入口）、アクセス レビュー（権限の棚卸し）は、第 2 章の 2.3 の各節で詳しく説明します。

ゼロトラストの最小特権では、必要な期間だけ必要な権限を与えます。この仕組みが just-in-time と just-enough-access (JIT/JEA) です[^c1-41]。前の節で見た、MUA の Operator ロールを期限付きにする運用も、同じ考え方です。

場面で見ます。バックアップ管理者が、不変の設定を一時的に無効にする必要が生じました。正しい手順は、セキュリティ管理者が PIM で Backup MUA Operator を期限付きで付与し、作業のあとに取り消すことです。Contributor を渡す手順は、Resource Guard の削除権限まで渡るので使えません。

セキュリティ更新の方式の評価: Azure Update Manager・Windows Autopatch・Intune の更新リング [1.1]

選ぶ軸は、対象の種類です。

対象	サービス	要点
サーバー OS (Azure VM、Azure Arc 接続のオンプレミスと他クラウド、Windows と Linux)	Azure Update Manager	24 時間ごとの定期評価、メンテナンスウィンドウでの更新、動的スコープ、Azure Policy による自動化
Windows クライアント、Microsoft 365 Apps、Edge、Teams	Windows Autopatch	段階的なデプロイリング
Windows クライアントの更新の方針	Intune の更新リング、機能更新ポリシー、品質更新ポリシー	延期期間、期限、再起動の挙動

Update Manager は、Azure VM と Arc 接続マシンの更新の準拠状況を、1 つの画面で見せます。更新は、今すぐ適用することも、定義したメンテナンスウィンドウで適用することもできます。適用先は動的スコープで条件から選べるので、1 台ずつ指定する必要はありません。自動ゲストパッチは Azure VM に自動で更新を当て、ホットパッチは再起動なしで重要な更新を当てて停止時間を減らします。

Update Manager は、Log Analytics と Azure Automation に依存しません。アクセス制御はリソース単位の RBAC です。月例のパッチ Tuesday に合わせた周期も組めます[^c1-25]。

Intune の更新リングは、延期期間、期限、再起動の挙動を決め、段階展開を行うポリシーです。機能更新ポリシーは、特定の Windows バージョンに端末

を固定します。品質更新ポリシーは、月例の累積更新を配信し、ホットパッチと緊急の expedite を制御します[^c1-26]。

Autopatch グループは、Entra のデバイスグループと更新ポリシーをまとめる単位です。既定で Test と Last のリングを持ち、1 グループに最大 15 のリングを作れます。ユーザーベースの Entra グループは使えません[^c1-27]。Windows の品質更新は、対象の端末 (Up to Date の条件を満たす端末) の 95% 以上を最新の品質更新に保つことを目標にしています[^c1-28]。

Windows Server を Autopatch で管理する設計は、成り立ちません。Autopatch は Windows クライアントと Microsoft 365 などのアプリの担当で、サーバー OS は Update Manager が担当します。重大な脆弱性への緊急対応は、更新リングの延期を待たず、expedite で上書きします。

細目 1.2: MCRA と MCSB に合わせたソリューション設計

MCRA の構成と使い方: 機能の地図・参照の図 [1.2]

MCRA (Microsoft Cybersecurity Reference Architectures) は、技術的な参照アーキテクチャ集です。ゼロトラストの原則で、端から端までのセキュリティを導入するために使います。対象は「hybrid of everything」の環境で、レガシー IT、マルチクラウド、IoT、OT、AI が含まれます[^c1-29]。

Microsoft の Security Adoption Framework (SAF) の構成要素で、現行は 2025 年 4 月版、前の版は 2023 年 12 月版です。

含まれる内容は、アンチパターンとベストプラクティス、脅威の傾向と攻撃パターン、ゼロトラストの標準や組織の役割への対応づけ、そして図です。図の種類は次のとおりです。

- Microsoft のサイバーセキュリティ機能の地図

- ゼロトラストのユーザーアクセス
- SecOps (SOC): SOC のツールの構成と統合点
- OT
- マルチクラウドとクロスプラットフォーム: Azure 以外のクラウドや OS をまたぐ機能の構成
- 攻撃チェーンのカバー範囲
- インフラストラクチャと開発のセキュリティ: 開発の仕組みとクラウド基盤の保護
- セキュリティ組織の機能: セキュリティ部門の機能と役割の整理

2025 年 4 月版の機能の地図の変更は、次のとおりです[^c1-29]。

- 追加: Microsoft Security Exposure Management、Windows LAPS、パスキー、Microsoft Entra Verified ID
- 削除: 廃止された Microsoft Entra Permissions Management

使い方は主に 5 つです。目標像のテンプレートにする、すでに持つ機能と比べる、Microsoft の機能を学ぶ、統合点を知る、サイバーセキュリティそのものを学ぶ、の 5 つです[^c1-29]。MCRA は「何をどう組み合わせるか」を示す地図です。個別の制御を監査する基準ではありません。制御の基準は、次に見る MCSB が担います。

MCSB の制御ドメインと、制御を設計に当てはめる [1.2]

Microsoft cloud security benchmark (MCSB) v2 (プレビュー) は、v1 を置き換えます。420 件を超える Azure Policy の組み込み定義が割り当てられ、リスクと脅威に基づくガイダンスを持ちます。制御ドメインは 12 です[^c1-30]。

略号	ドメイン	略号	ドメイン
NS	ネットワークセキュリティ	LT	ログと脅威検出
IM	ID 管理	IR	インシデント対応
PA	特権アクセス	PV	態勢と脆弱性管理
DP	データ保護	ES	エンドポイントセキュリティ
AM	資産管理	BR	バックアップと復旧
DS	DevOps セキュリティ	AI	AI セキュリティ

制御の ID は、ドメインの略号と番号です (AI-1、DP-1、NS-2 など)。各制御は、ID、Azure Policy、セキュリティ原則、軽減するリスク、MITRE ATT&CK、実装ガイドンス、実装例、重要度、制御の対応表で構成されます。Azure Policy が付かない制御もあるため、すべての制御を Policy で強制できるとは限りません。

重要度は、Must have、Should have、Nice to have の 3 段階です。対応表は、NIST SP 800-53 Rev.5、PCI-DSS v4、CIS Controls v8.1、NIST CSF v2.0、ISO 27001:2022、SOC 2 への紐づけです。この対応が示すのは、Azure の機能で要件を満たせるということです。その基準への準拠そのものを、意味しません [^c1-31]。

設計への当てはめは、要件から「リスク、制御、ポリシー」の順にたどります。バックアップの例では、BR-1 (定期的な自動バックアップ) と BR-2 (バックアップと復旧データの保護) が Must have です。BR-3 (監視) と BR-4 (定期的なテスト)

ト)は Should have です[^c1-32]。DevOps セキュリティは、DS-1 から DS-6 までが Must have で、DS-7 (ログと監視) が Should have です[^c1-33]。

12 ドメインの制御は、合わせて 81 あります。ドメインごとの内訳は次のとおりです[^c1-56]。重要度は、記載のない制御がすべて Must have で、例外だけを括弧に書きました。

ドメイン	制御(ID と内容)
NS (10)	NS-1 セグメント化の境界、NS-2 クラウドネイティブサービスのネットワーク制御、NS-3 企業ネットワーク境界のファイアウォール、NS-4 IDS/IPS、NS-5 DDoS 保護、NS-6 WAF、NS-7 ネットワークセキュリティの一元管理、NS-8 安全でないサービスとプロトコルの検出と無効化、NS-9 プライベート接続、NS-10 DNS セキュリティ
IM (8)	IM-1 ID と認証の一元化と分離、IM-2 ID と認証システムの保護、IM-3 アプリケーション ID の安全な自動管理、IM-4 サーバーとサービスの認証、IM-5 アプリへの SSO、IM-6 強力な認証、IM-7 条件に基づくアクセスの制限、IM-8 資格情報とシークレットの露出の制限
PA (8)	PA-1 高特権ユーザーの分離と制限、PA-2 常時アクセスの回避、PA-3 ID と権限のライフサイクル管理 (Should)、PA-4 アクセスの定期的な確認、PA-5 緊急アクセス、PA-6 特権アクセスソリューション、PA-7 最小限の管理 (JEA)、PA-8 クラウドプロバイダーのサポート用アクセスの手順

ドメイン	制御(ID と内容)
DP (8)	DP-1 機密データの検出・分類・ラベル付け、 DP-2 機密データへの異常と脅威の監視、 DP-3 転送中の暗号化、DP-4 保存データの 既定の暗号化、DP-5 必要時のカスタマーマ ネージドキー (Should)、DP-6 キー管理、 DP-7 証明書管理、DP-8 キーと証明書のリ ポジトリの保護
AM (5)	AM-1 資産インベントリとリスクの追跡、 AM-2 承認済みサービスのみ使用 (Should)、AM-3 資産ライフサイクルの保護 (Should)、AM-4 資産管理へのアクセス制 限、AM-5 VM で承認済みアプリのみ使用 (Should)
LT (7)	LT-1 脅威検出の有効化、LT-2 ID とアクセス 管理の脅威検出、LT-3 調査用のログ、LT-4 ネットワークログ、LT-5 ログの一元管理と分 析、LT-6 保存期間 (Should)、LT-7 承認済みの 時刻同期 (Should)
IR (7)	IR-1 計画と手順の更新、IR-2 通知の設定、 IR-3 質の高いアラートからインシデントを作 成、IR-4 インシデントの調査、IR-5 優先順位 付け (Should)、IR-6 対応の自動化 (Should)、IR-7 教訓の整理と証拠の保存 (Should)
PV (7)	PV-1 安全な構成の定義、PV-2 構成の監査 と強制、PV-3 コンピューティングの安全な 構成の定義、PV-4 コンピューティングの監 査と強制、PV-5 脆弱性評価 (Should)、PV- 6 脆弱性の迅速な自動修復 (Should)、PV- 7 定期的なレッドチーム演習 (Nice)

ドメイン	制御(ID と内容)
ES (3)	ES-1 EDR、ES-2 最新のマルウェア対策、ES-3 マルウェア対策とシグネチャの更新
BR (4)	BR-1 定期的な自動バックアップ、BR-2 バックアップと復旧データの保護、BR-3 バックアップの監視 (Should)、BR-4 定期的なテスト (Should)
DS (7)	DS-1 脅威モデリング、DS-2 ソフトウェアサプライチェーン、DS-3 DevOps インフラの保護、DS-4 SAST、DS-5 DAST、DS-6 ワークロードのライフサイクル、DS-7 ログと監視 (Should)
AI (7)	AI-1 承認済みモデル、AI-2 多層のコンテンツフィルタリング、AI-3 安全メタプロンプト、AI-4 エージェント機能の最小権限、AI-5 ヒューマンインザループ、AI-6 監視と検出、AI-7 継続的な AI レッドチーム

この表の使い方は、要件の動詞から領域を決めることです。「ログを集める」は LT、「権限を時間で絞る」は PA、「承認していないものを使わせない」は AM か AI-1、「構成を基準に保つ」は PV です。

承認していないモデルを本番へデプロイさせたくない、という要件を考えます。当てるのは AI-1 です。Azure Policy で「承認済みレジストリのモデルだけをデプロイする」定義を、効果 Deny で割り当てます[^c1-34]。

内部・外部・サプライチェーンの攻撃への防御のベストプラクティス [1.2]

攻撃の種類ごとに、守りの置き場所が違います。

攻撃	起点	守りの要	使う仕組み
内部	退職者、過失、悪意のある従業員	行動の検出と特権の制限	Microsoft Purview Insider Risk Management、PIM、データ損失防止
外部	ID の侵害、フィッシング、リモートアクセスの悪用	入口の検証と、侵害想定 の封じ込め	条件付きアクセス、MFA、エンドポイントとメールの保護、攻撃面管理
サプライチェーン	依存ライブラリ、モデル、パイプライン	来歴の検証と署名	DevOps セキュリティのスキャン、承認済みモデルのみ、コード署名

内部リスクの管理は、Microsoft 365 と Microsoft Graph のログから、IP の窃取、データ漏えい、セキュリティ違反といったリスクを検出し、調査して対処します。ユーザーは既定で仮名化され、氏名がそのまま見えるわけではありません。

内部リスクの管理は、ポリシー、アラート、トリアージ、調査、対処の順に流れます。ポリシーは、用意されたテンプレート（退職者によるデータ窃取、データ漏えい、リスクのあるユーザーによるデータ漏えい、セキュリティポリシー違反など）と条件から作ります。トリアージでは、アラートをケースの作成、既存ケースへの追加、却下のいずれかに振り分けます[^c1-35]。

代表的なシナリオには、次のものがあります（ほかに、リスクのあるユーザーの行動、医療機関の患者データの悪用などもある）[^c1-35]。

- 退職者によるデータ窃取（ポリシーテンプレートを使うには Microsoft 365 の HR コネクタが要る）

- 機密情報の意図的または偶発的な漏えい

外部攻撃は、ネットワークの境界ではなく、ID の侵害、フィッシング、セッションの乗っ取りで起こります。ゼロトラストが境界を前提にしないのは、このためです[^c1-24]。ランサムウェア対策の手順 3 は、入口を 4 つ挙げます。リモートアクセス、メールとコラボレーション、エンドポイント、アカウントです[^c1-36]。

サプライチェーンの対策は、複数の枠組みに分かれて出てきます。MCSB の DS-2 は、依存関係とライセンスのスキャン、脆弱性管理、SBOM の生成、全コンポーネントの来歴と完全性の検証を求めます[^c1-33]。WAF の完全性の原則は、ビルド時と実行時の両方でサプライチェーンの脆弱性をスキャンすることを求めます。証明、コード署名、証明書、暗号化で、信頼を確かめます[^c1-4]。

Defender for Cloud の DevOps セキュリティは、Azure DevOps、GitHub、GitLab を横断して、スキャン結果を 1 つの画面に集めます。対象は、コード、シークレット、オープンソース依存関係、IaC です。プルリクエストへの注釈で、開発者に修正を促します[^c1-37]。

場面で見ます。開発者の PC が侵害され、パイプラインに悪意のあるスクリプトが入りました。入口の ID 防御だけでは足りません。DS-3 (DevOps インフラの保護)、DS-2 (サプライチェーン)、シークレット管理、ブランチの保護といった、複数の層で検出点を作ります。コードが本番に届く前に感染すると、通常の検問を素通りしやすくなります。ピアレビュー、IDE のセキュリティプラグイン、セキュアコーディング基準、ブランチのレビューが、前段の防御になります[^c1-38]。

AI ソリューションを MCSB に合わせる:AI セキュリティの制御 [1.2]

AI セキュリティのドメインは、3 つの柱で整理され、制御は 7 つあります。7 つとも重要度は Must have です[^c1-39]。

柱	守るもの	制御
AI プラットフォームのセキュリティ	モデルと学習データを含む基盤	AI-1 承認済みモデルの使用 (この柱の関連制御:IM-3、NS-2、LT-3、AI-1、DP-4)
AI アプリケーションのセキュリティ	設計から連携までのアプリ	AI-2 多層のコンテンツフィルタリング、AI-3 安全メタプロンプト、AI-4 エージェント機能の最小権限、AI-5 ヒューマンインザループ(関連:DP-1)
監視と対応	悪用と逸脱の検出	AI-6 監視と検出、AI-7 継続的な AI レッドチーム

リスクから制御を選ぶ対応は、次のとおりです。

想定される事象	当てる制御	具体策
汚染された第三者のモデルや学習データの持ち込み	AI-1	モデルレジストリで来歴と承認を管理し、Azure Policy で未承認のデプロイを拒否する
プロンプトインジェクションと有害な入出力	AI-2	入力、内部処理、出力の各段階でフィルタをかける (Azure AI Content Safety など)

想定される事象	当てる制御	具体策
指示の上書きと脱獄	AI-3	システム側の指示を優先させ、信頼できないデータをスポットライティングで隔離し、Prompt Shields で検知する
エージェントの過大な権限と横展開	AI-4	機能ごとに能力を絞った権限を与える
重大な操作の自動実行	AI-5	実行前に人間が確認して承認する
脱獄の試みと、推論を利用したデータ流出	AI-6	Microsoft Defender for Cloud の AI サービス向け脅威保護
未知の弱点	AI-7	PyRIT や Azure AI Red Teaming Agent による攻撃的テスト

AI-2 と AI-3 は、混同しやすい組です。AI-3 は、モデルへ渡す指示そのものに安全な役割を埋め込む対策で、入出力の検査は担いません。AI-2 は、入出力を検査して遮断します。取り込んだ文書など信頼できないデータに紛れた命令が指示を上書きする事態（間接的なプロンプトインジェクション）には、システムの指示を優先させ、スポットライティングで信頼できないデータを隔離する AI-3 を主に当て、AI-2 の検査で補います。AI-4 と AI-5 も別物で、AI-4 は与える権限を絞り、AI-5 は実行の前に人の判断を挟みます[^c1-39]。

ゼロトラストの 3 原則：明示的に検証・最小特権・侵害を想定 [1.2]

ゼロトラストは、「決して信頼せず、常に検証する」考え方です。誰が、どのデバイスで、どこから、どんなリスクでアクセスするかを検証します。検証は 1 回で

終わらず、セッションの間も続きます[^c1-24]。

原則	意味	具体
明示的に検証する (Verify explicitly)	あらゆるアクセス要求を、使える全シグナルで認証・承認する	ID、場所、デバイスの正常性、ワークロード、データ分類、異常
最小特権アクセスを使う (Use least privilege access)	必要な期間だけ、必要なアクセスだけを与える	JIT/JEA、リスクに応じた適応型ポリシー、データ保護
侵害を想定する (Assume breach)	攻撃者が環境内にいる前提で、影響の範囲を狭め、検出と対応を速める	爆発半径の最小化、セグメント化、エンドツーエンドの暗号化、分析

3 原則を見分ける型の設問があります。設計の例と原則の対応は、次のとおりです。

設計の例	当てはまる原則
条件付きアクセスでデバイスの正常性を検証する	明示的に検証する
管理者権限の常時付与を JIT に変える	最小特権アクセス
ネットワークを分割し、ログで異常を検出する	侵害を想定する

従来の境界型は、ネットワークの内側を安全とみなし、セキュリティを担当部門だけの責任にします。ゼロトラストは、すべての要求を信頼せず、現在の状況で判断します。責任は全員に広げます[^c1-24]。

ゼロトラスト導入フレームワーク：業務のシナリオと技術の柱 [1.2]

導入モデルは 3 つの要素で、実装の段階で 4 つ目が加わります[^c1-40]。

要素	問い	内容
業務のシナリオ	なぜ	重要な成果を決める
セキュリティのディシプリン	何を	戦略、アーキテクチャ、プロセス、制御
技術の柱	どこで	ID、エンドポイント、データ、アプリ、インフラ、ネットワーク、SecOps の 7 本
技術ソリューション(実装時)	どうやって	柱ごとの実装手順

業務のシナリオは 5 つです。

- 1. セキュリティ態勢の迅速な近代化
- 2. リモートとハイブリッド勤務の保護
- 3. 機密データの特定と保護
- 4. 侵害による業務被害の予防と軽減
- 5. 規制とコンプライアンス要件の充足

各シナリオは 4 つの実装ステージに分けます。全シナリオでステージ 1 を揃えて進めるのが目安です[^c1-41]。

導入のライフサイクルは、CAF と同じ段階をゼロトラスト向けに調整した 6 つです。Define strategy、Plan、Ready、Adopt、Govern、Manage の順に進みます。

CAF との違いは、広げ方にあります。CAF の導入は、1 つのアプリやサービスを環境へ入れる作業の繰り返しです。ゼロトラストは、データ保護のような 1 つの要素を環境全体へ広げ、次の要素へ進む 2 次元の動きで、1 回の導入では終わりません。

成果の計測は、事業へのリスクの軽減と、アーキテクチャ全体の戦略目標の達成の2つの面で行います。リスクの評価には ISO/IEC 27001:2022 と ISO 31000 を使います。Microsoft Security Exposure Management の Zero Trust イニシアティブは、導入の進捗を業務のシナリオに沿った指標で追跡できます。すべての制御を導入しない組織では、製品内の進捗率が正確になるとは限りません[^c1-42]。

場面で見ます。CISO が主導し、成果を事業と結ぶ型があります。セキュリティを IT 部門へ任せ、短期のコスト最適化に向かう型もあります。ゼロトラストは、後者の縦割りの製品を1つの構想に束ね、測れる指標を与えます。経営層の理解が要るのは、セキュリティの支出を事業のリスクとして管理するためです[^c1-41]。

細目 1.3: CAF と WAF に合わせたソリューション設計

安全な AI 導入の戦略: 導入シナリオ・シャドー AI・責任ある AI [1.3]

AI には、次の3種類があります[^c1-43]。

- 従来型: 予測、分類、異常検出を行う
- 生成 AI: 文章やコードを作る
- エージェント型 AI: 目標に向けて道具を使い、許可された範囲で動く

導入は、次の3つの行動から始めます。

1. リーダーが、成果と意思決定の権限を定める。
2. 組織全体の AI ガバナンスを集約する (AI Center of Excellence など)。
3. 承認済みの AI へ、訓練とともに広くアクセスさせる。

解決策は、運用責任が最も少ないものを承認します。道筋は、AI 戦略、計画、Ready、ガバナンス・セキュリティ・管理の順です。

責任ある AI の原則は、次の 6 つです。

- AI のプライバシーとセキュリティ
- 信頼性と安全性
- 公平性
- 包括性
- 透明性
- 説明責任

CAF の AI のガバナンスは NIST AI Risk Management Framework に沿って、リスクの評価、方針の文書化、強制、監視の 4 段で回します。この 4 段は CAF の分け方で、NIST AI RMF 自体の 4 つの機能 (Govern・Map・Measure・Manage) とは別です。方針の文書化には、モデルの選定と導入、第三者のツールとデータ、保守と監視が入ります[^c1-44]。

セキュリティは、3 つの塊で進めます[^c1-45]。

塊	やること
AI のリスクの発見	STRIDE などの既存の脅威モデルから始める。データ漏えい、プロンプトインジェクション、モデルの反転をテストし、レッドチームを回す
AI の資源とデータの保護	Azure Resource Graph で資産を棚卸しする。マネージド ID と仮想ネットワークで通信を守る。Microsoft Purview でデータを分類して DLP をかける。モデルとデータセットは、プライベートエンドポイント配下の BLOB に置く

塊	やること
脅威の検出	Defender for Cloud の AI セキュリティ態勢管理を使う。AI 向けのインシデント対応を用意する

シャドー AI は、組織の IT やセキュリティが知らず、承認も管理もしない状態で使われる AI ツールです。放置すると、機密データの漏えい、規制への不適合、評判の毀損につながります。

Microsoft の展開モデルは 4 段です。AI アプリを発見する。未承認アプリへのアクセスをブロックする。承認済みアプリへの機密データの流出をブロックする。AI アプリへ送るデータをガバナンスする。順序には意味があります。発見には Defender for Cloud Apps、機密データの制御には Purview の DLP を使います[^c1-46]。

場面で見ます。従業員が顧客データを公開の生成 AI に貼り付けている疑いがあります。全面禁止にすると、承認済みの AI を広く使わせて価値を探る方針と逆を向きかねません。正しい順は、まず利用実態を発見し、次に未承認のアプリをブロックし、承認済みの AI にも機密データを渡さないよう DLP をかけることです。送るデータのガバナンスは、そのあとも続けます。教育だけで済ませる設計や、検出なしでブロックだけを行う設計は、順序が成り立ちません。

CAF の段階とセキュリティの方法論 (Secure)・セキュリティの役割 [1.3]

CAF は、Azure の導入で意思決定者の判断を速くするための枠組みです。Azure の導入は 7 つのフェーズで、成果物は Azure ランディングゾーンと運用の標準です[^c1-47]。

フェーズ	答える問い
1 Strategy	導入はどんな姿か
2 Plan	組織はどう準備するか
3 Ready	ランディングゾーンをどう作るか
4 Adopt	移行、近代化、構築をどう進めるか
5 Govern	環境をどう統制するか
6 Secure	環境をどう守るか
7 Manage	継続的にどう運用し最適化するか

CAF のシナリオは、Azure 導入（基盤）、データプラットフォーム、AI 導入、AI エージェント、ソブリン、Azure VMware Solution の 6 つです。ゼロトラストの導入は 6 段階で、CAF の 7 フェーズと違って Secure を含みません。

Secure の方法論は、セキュリティを戦略から運用まですべてのフェーズに適用します。戦略のテーマは、次の 6 つです。

- 態勢の近代化
- インシデントの準備と対応
- 機密性
- 完全性
- 可用性
- 態勢の維持

このうち機密性、完全性、可用性の 3 つは、CIA に対応します。

原則	守るもの	実現する手段
機密性	機密データへのアクセス	暗号化、鍵管理、ID、分離、分類
完全性	データの正しさと完全さ	ハッシュ、署名、不変ストレージ、サプライチェーン
可用性	サービスとデータへの時間内のアクセス	冗長、障害の分離、バックアップ、DR

態勢の維持は、Defender for Cloud の Secure Score などですら測ります[^c1-48]。チェックリストは 7 ステップで、役割の理解、戦略への統合、計画、Ready、導入、統制、管理の順に進みます。

セキュリティの役割は、6 つの塊に分かれます。

役割	担うこと
クラウドサービスプロバイダー	基盤のセキュリティ機能。仮想のチームメンバーとして扱う
インフラとプラットフォームのチーム	セキュリティ、プライバシー、コンプライアンスの制御を実装する
セキュリティのアーキテクチャ・エンジニアリング・態勢管理	戦略と標準を設計パターンに落とす。態勢管理は攻撃面と脆弱性を扱う
SecOps/SOC	検出と対応
GRC (ガバナンス・リスク・コンプライアンス)	方針とリスクの管理
セキュリティの教育と方針	教育、意識向上、方針

SaaS の時代には、セキュリティチームの重心が実装から統制へ移ります。セキュリティチームは方針、標準、構成ベースラインを出します。SaaS の設定そのものは、所有するチームが行います[^c1-49]。

WAF のセキュリティの柱:設計原則と推奨事項による新規設計・既存の評価 [1.3]

Azure Well-Architected Framework (WAF) には、5 本の柱があります[^c1-50]。

柱	ワークロードの関心事
信頼性 (Reliability)	回復力、可用性、復旧
セキュリティ	データ保護、脅威の検出と軽減
コストの最適化	コストのモデル化、予算、無駄の削減
オペレーショナル エクセレンス	全体の可観測性、DevOps の実践
パフォーマンス効率	スケーラビリティ、負荷テスト

セキュリティの柱は、機密性、完全性、可用性 (CIA) を守ります。ゼロトラストを羅針盤にします。設計原則は 5 つの束です。セキュリティ準備の計画、機密性の保護、完全性の保護、可用性の保護、態勢の維持と進化です[^c1-51]。

原則の束	代表的な推奨	結びつくゼロトラスト
準備の計画	セグメント化、役割別の訓練、インシデント対応計画、コンプライアンス要件の把握	全体
機密性	必要最小限のアクセス、データ分類、保存中・転送中・処理中の暗号化、流出の防止、監査証拠	最小特権、明示的な検証、侵害の想定

原則の束	代表的な推奨	結びつくゼロトラスト
完全性	強い認証と承認、サプライチェーンのスキャン、署名と証明書、不変で暗号化されたバックアップ	最小特権、明示的な検証、侵害の想定
可用性	JIT/JEA による常時権限の置き換え、DDoS などへの対策、パッチと防止策、復旧環境にも同じ水準の制御	最小特権、明示的な検証、侵害の想定
態勢の維持	資産の棚卸し、脅威モデリング、ベースラインとの比較、侵入テスト、検出と復旧、事後の分析	全体

新規設計と既存の評価では、使う道具が同じではありません。新規設計では、設計原則とセキュリティのチェックリストを使います。既存のワークロードは、Azure Well-Architected Review で評価し、改善の優先順位を付けます。Azure Advisor は柱を基準に構成と使用状況を分析し、Advisor スコアを柱ごとに分類できます[^c1-50]。

場面で見ます。稼働中の本番ワークロードのセキュリティを評価し、投資の優先順位を付けたい場合は、Azure Well-Architected Review で現状を測り、Azure Advisor のスコアで柱ごとの改善効果を比べます。一方、これから新規に設計するワークロードは、設計原則とセキュリティのチェックリストを起点にして、ランディングゾーンの上に置きます。既存の評価と新規の設計では、入口が同じにはなりません。

セキュリティと信頼性は、セキュリティの設計が単一障害点と運用の複雑さを増やすため、引っ張り合うことがあります。WAF は、このトレードオフを意識して選ぶよう求めています[^c1-51]。

CAF と WAF に基づくセキュリティとガバナンスの推奨 [1.3]

CAF は組織と環境の単位、WAF はワークロードの単位で見る階層になっています。CAF の Ready で作るランディングゾーンが共通の土台とガードレールを与え、その上でワークロードごとに WAF のレビューで設計を評価します。推奨を選ぶ型は、次のとおりです。

要件	推奨	根拠となる枠組み
全サブスクリプションで同じ統制を強制する	管理グループに Azure Policy を割り当て、ポリシー駆動のガバナンスにする	ランディングゾーンの設計原則
1 つのワークロードのセキュリティ設計を評価する	Well-Architected Review と Advisor	WAF
態勢を継続的に測る	Defender for Cloud の Secure Score と、リスクの大きさに沿った指標	CAF の Secure (態勢の維持)
新技術 (AI) を導入する	CAF の AI 導入シナリオと、ランディングゾーン上のポリシー更新	CAF
事業継続の要件を満たす	信頼性の柱とセキュリティの柱の両方で復旧を設計する	WAF

場面で見ます。子会社が独自にサブスクリプションを作り、暗号化のないストレージを置いてしまいました。個別に是正するだけでは再発を防げません。統制は 3 層で使い分けます。ガバナンスは、管理グループに割り当てた Azure Policy で、逸脱を防ぎます。態勢は、Defender for Cloud の Secure Score で、現状を測ります。ワークロードの設計は、WAF のレビューで見直します。

ランディングゾーンは、新しい技術を取り入れるときも、アーキテクチャを変えません。プラットフォームのポリシーを更新して、全ワークロードへ一貫して適用します[^c1-52]。

Azure ランディングゾーン: 設計領域・プラットフォームとアプリケーションのランディングゾーン・管理グループ [1.3]

Azure ランディングゾーンは、複数サブスクリプションの Azure 環境を、統制、保護、拡張するための構成です。要素は、次の 2 つです。

- プラットフォームランディングゾーン: 統制、セキュリティ、共有リソースを担う中央の基盤
- ワークロードランディングゾーン: チームがガードレールの中でワークロードを動かす環境

どちらも、実装は 2 通りです。Microsoft のアクセラレータでコードから展開する方法と、カスタム構築です[^c1-52]。Microsoft Entra テナントごとのプラットフォームランディングゾーンは、通常 1 つです。ワークロードのランディングゾーンを払い出す仕組み (サブスクリプション ベンディング) も含みます。ワークロードのチームが、自分のサブスクリプションに独自のファイアウォールや Virtual WAN を置きたいと要望したときは、共有のネットワーク資源は中央のプラットフォームが担うので、Platform の Connectivity のものを使わせます。チームはガードレールの中でワークロードを動かすので、独自に置くことは認めません。

設計領域は 8 つです。環境側の 4 つは、Azure の請求と Entra テナント、ID とアクセス管理、リソースの編成、ネットワークポロジと接続です。統制側の 4 つは、セキュリティ、管理、ガバナンス、プラットフォームの自動化と DevOps です[^c1-53]。

設計原則は、次の 5 つです[^c1-54]。

- サブスクリプションの民主化
- ポリシー駆動のガバナンス
- 単一のコントロールプレーンと管理プレーン
- アプリケーション中心のサービスモデル
- Azure ネイティブな設計とロードマップとの整合

管理グループの階層で、基準の構成は次のとおりです[^c1-55]。

管理グループ	役割
Platform (Security、Management、Identity、Connectivity)	プラットフォームの共通機能。Security は Sentinel など、Management は Log Analytics、Identity は AD DS、Connectivity は Azure Firewall や Virtual WAN のサブスクリプションを収める
Landing zones	ワークロードを包む親。ワークロードを問わないポリシーを持つ
Online	インターネットへの直接の入出力があるワークロード、または仮想ネットワークが不要なワークロード
Corp (Internal)	ハブ経由で社内ネットワークとの接続やハイブリッド接続が必要なワークロード
Local	Azure Local クラスター上のワークロードと、クラスター自体
Sandbox	試験用。ほかの環境から隔離され、ポリシーは緩い
Decommissioned	廃止されたランディングゾーン。30～60 日後に Azure が削除する

ネットワークポロジは、Hub-Spoke か Virtual WAN です。Hub-Spoke は共有サービスをハブの仮想ネットワークに集約してスポークの仮想ネットワークをつなぎ、Virtual WAN は Microsoft が管理するバックボーンで多数の拠点と仮想ネットワークをつなぎます。

管理グループの運用には、守る型があります。階層は 3～4 階層までと浅く保ち、ポリシーの割り当てに使います。ワークロードのチームには、管理グループのスコープで RBAC を付けません。サブスクリプションかリソースグループのスコープで付与します。本番、テスト、開発ごとの管理グループは作らず、同じ管理グループの中でサブスクリプションを分けます。リージョンごとの管理グループも作りません。データの所在などの規制がある場合だけ、場所に沿った構成にします[^c1-55]。

場面で見ます。社内の ERP に接続する基幹ワークロードは Corp、パブリックに公開する Web アプリは Online、Azure Local 上のアプリは Local に置きます。新しいサブスクリプションがルート直下に置かれると、統制が効きません。専用の既定の管理グループ (Sandbox が候補) を設定して、ルート直下に落ちないようにします。

CAF に沿った DevSecOps のプロセス [1.3]

DevSecOps は、セキュリティを開発の最後の門にせず、設計から本番までの各段階へ組み込む進め方です。MCSB の DevOps セキュリティは、3 つの柱で整理されています[^c1-33]。

柱	制御
設計とサプライチェーンの保護	DS-1 脅威モデリング (STRIDE)、DS-2 ソフトウェアサプライチェーン

柱	制御
制御を左へ寄せる	DS-3 DevOps インフラの保護、DS-4 SAST、DS-5 DAST、DS-6 ワークロードのライフサイクル。IaC とシークレットのスキャンを CI/CD に統合し、シークレットは Key Vault で一元管理する
DevOps の監査と監視	DS-7 ログと監視

CAF の Secure の方法論は、セキュリティを戦略から運用まで全フェーズに適用します。検証はポリシー、IaC、継続的な準拠スキャン、Secure Score の追跡で自動化するよう求めています[^c1-48]。DevSecOps の制御は、この枠の中で段階ごとに置き、最後の門だけには置きません。設計と導入の段階では脅威モデリングとスキャンを CI/CD に組み込み、統制の段階ではポリシーと準拠スキャンで逸脱を検知します。運用の段階では、DevOps のログと監視を使います。

DevOps では、パイプラインの自動化、コード検証、コードリポジトリが攻撃者の主な入口になり、開発者の ID と端末も狙われるため、開発者のマシンも守る対象です。ピアレビュー、IDE のセキュリティプラグイン、ブランチのレビューを組み込みます。GitHub Actions から Azure へは、OIDC のフェデレーション ID を使い、長期のシークレットを GitHub に保存しません[^c1-38]。

Defender for Cloud の DevOps セキュリティは、コードからクラウドまでの文脈を付けて、修正の優先順位を決めます[^c1-37]。本番で公開されているワークロードにつながる指摘のように、影響の大きいものは、後回しにはしません。

場面で見ます。パイプラインのデプロイ用資格情報が、リポジトリの変数に長期保存されています。是正は、フェデレーション ID (OIDC) への置き換えに加

えて、シークレットのスキュアをプルリクエストに組み込み、Key Vault でシークレットを一元管理することです。DS-7 のログと監視は Should have なので、DS-1 から DS-6 の Must have を先に固めます。

SAMPLE

サンプルはここまでです

続き(第2章～巻末)は、SC-100 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

Microsoft Cybersecurity Architect (SC-100) 学習用テキスト(無料サンプル)

版

2026年10月版(SC-100 出題範囲(Study guide・Skills measured as of October 21, 2026)準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

Microsoft、Azure、Microsoft Entra、Microsoft Defender、Microsoft Sentinel、Microsoft Purview、Microsoft 365 および Microsoft の製品名・サービス名は、Microsoft Corporation 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。

本教材は公式シラバスの内容を基に作成したもので、Microsoft Corporation 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。