

このコマンドの効果は、オーナーの所属グループに書き込みの権限を追加し、その他のユーザーから実行の権限を削除します。また、このコマンドは既存の権限の置き換えにも使用できます。例えば、次のコマンドは、最初の権限文字列で表された構成に対応します。

```
chmod u=rwx,g=rx,o=rx home
```

絶対モードでは、権限は8進数表記を使用して割り当てられます(r=4、w=2、x=1)。例えば、次のコマンドにも同じ効果があります。

```
chmod 755 home
```

## 強制アクセス制御と属性ベースアクセス制御

DACおよびRBACモデルでは、特権アカウントが侵害の脅威に曝されます。制限のさらに強いアクセス制御モデルを使用することで、この脅威を低減することができます。

### 強制アクセス制御(MAC)

**強制アクセス制御(MAC)**は、セキュリティクリアランスレベルから着想を得ています。リソースにACLを定義する代わりに、各対象と主体にラベルと呼ばれるクリアランスレベルを付与します。使用されるモデルが階層モデルの場合（つまり、クリアランスの高いユーザーはクリアランスの低い対象へのアクセスできる）、主体は自身のクリアランスレベル以下の対象へのアクセスのみが許可されます。

対象と主体のラベル付けは、事前設定されたルールを使用して行われます。重要なポイントは、これらのルールが主体アカウントによって変更できないことです。そのため、「強制」となります。また、主体は対象のラベルの変更や、自身のラベルの変更を許可されません。

### 属性ベースアクセス制御(ABAC)

**属性ベースアクセス制御(ABAC)**は、最も細分化した種類のアクセス制御モデルです。ABACシステムはこの名称からも分かるように、主体と対象属性に加え、コンテキストに沿った属性やシステム全般の属性との組み合わせに基づいてアクセスの判断を行うことができます。グループ/ロールのメンバーシップに加えて、これらの属性には現在使用されているOS、IPアドレス、最新のパッチやアンチマルウェアの存在に関する情報が含まれます。属性ベースのシステムでは、ユーザーアカウントやリソースに伴うイベントや警告の件数を監視したり、アクセスリクエストの推移を追ったりすることで、リクエストのタイミングや地理的位置に関する一貫性を確保します。M-of-N制御や職務分掌などのポリシーを実装するためにプログラミングされる場合もあります。

## ルールベースアクセス制御

ルールベースアクセス制御とは、アクセス制御ポリシーがシステムユーザーではなくシステムが実施するルールによって決定されるアクセス制御モデルを示す用語です。したがってRBAC、ABAC、MACのすべては、ルールベース（または強制）アクセス制御の例だと言えます。形式的なモデルだけでなく、ルールベースのアクセス制御の原則を導入することで、裁量的なアクセスに基づくコンピュータシステムやネットワークシステムを、DACで起こりうるような誤った設定から保護することも増えてきています。

### 条件付きアクセス

条件付きアクセスはルールベースアクセス制御の一例です。条件付きアクセスのシステムは、アカウントやデバイスのセッション全体における挙動を監視します。特定の条件が一致した場合、そのアカウントは一時停止されるか、そのユーザーは再認証（おそらく2段階認証が使用されます）を求められます。ユーザーアカウント制御(UAC)や特権アカウントのsudo制限は、条件付きアクセスの例です。より高い権限を必要とするリクエストが作成された時に、ユーザーはその確認や認証を求められます。ルールベースの権限管理とABACシステムは、条件付きアクセスに対して多くの基準（場所ベースのポリシーなど）を適用することができます ([docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview))。

## 特権アクセス管理

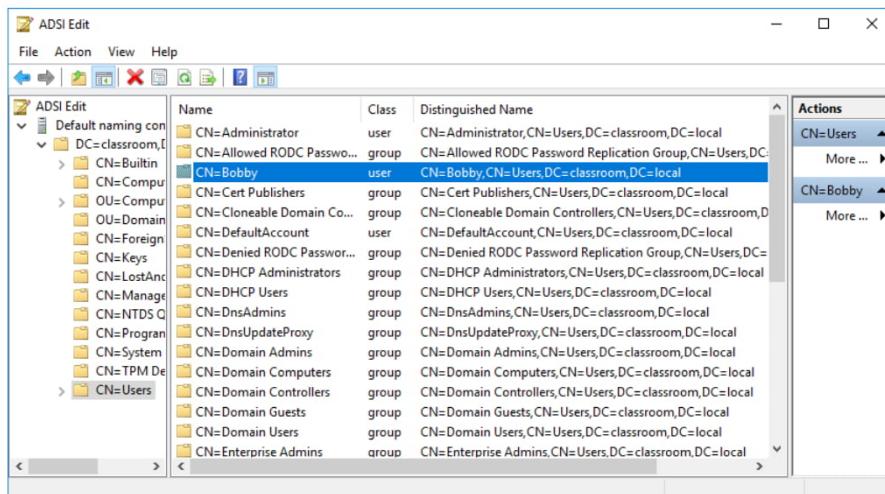
特権アカウントは、ソフトウェアのインストール、ファイアウォールやその他のセキュリティシステムの無効化など、ホストに対する重要な構成変更を行うことができるアカウントです。また、ネットワークアプライアンスやアプリケーションサーバーにログインする権限も持ちます。

**特権アクセス管理(PAM)**とは、特権アカウントの悪用を防ぎ、特権に対する脆弱な構成管理によるリスクを低減するための、ポリシー、手順、技術的制御を意味します。これらの制御は特権アカウントを特定して文書化することでそれらの使用状況を可視化します。また、それへのアクセスに使用された認証情報を管理します([beyondtrust.com/resources/glossary/privileged-access-management-pam](http://beyondtrust.com/resources/glossary/privileged-access-management-pam))。

## ディレクトリサービス

**ディレクトリサービス**は、企業ネットワークにおける特権管理と認可を提供する主要な手段であり、ユーザー、コンピューター、セキュリティグループ/ロール、およびサービスに関する情報を保存します。ディレクトリはデータベースのようなもので、オブジェクトはレコード、そのオブジェクトに関して判明している情報（属性）はフィールドに例えることができます。異なるベンダーの製品を相互運用するためには、ほとんどのディレクトリが同じ規格に対応している必要があります。Lightweight Directory Access Protocol (LDAP)はクエリとX.500フォーマットのディレクトリの更新に広く使用されているプロトコルです。

識別名(DN)は、X.500のようなディレクトリ内の任意のリソースを表す一意の識別子です。識別名はコンマで区切られた属性と値のペアで構成されています。具体性の高い属性から始まり、徐々に意味の広い属性へと続きます。最も具体的な属性は相対識別名(Relative Distinguished Name)と呼ばれ、連続する（親）属性値のコンテキスト内でオブジェクトを一意に識別することができます。



Active Directory LDAPスキーマでのオブジェクトの閲覧。  
(スクリーンショットはMicrosoftからの許可を得て使用。)

属性の種類、含まれる情報、属性を通じてオブジェクトタイプが定義された方法（これらの一部は必須、その他はオプション）がそのディレクトリスキーマによって表されます。通常使用される属性の一部として、共通名(CN)、組織単位(OU)、組織(O)、国(C)、ドメインコンポーネント(DC)が挙げられます。例えば、英国のWidget社が運用するWebサーバーの識別名は、次のようにになります。

```
CN=WIDGETWEB, OU=Marketing, O=Widget, C=UK,
DC=widget, DC=foo
```

## フェデレーションとアステーション

オンプレミスのネットワークでは、アカウントやデバイスの管理を一元化できるため、LDAPやKeberosなどの技術を利用することができます。Windows Active Directoryネットワークとして実装されることが多いです。ビジネスパートナーとのリソースの共有やパブリッククラウドでのサービスの使用ために、この種類のネットワークを拡張することは、フェデレーション技術の一種を実装することを意味します。

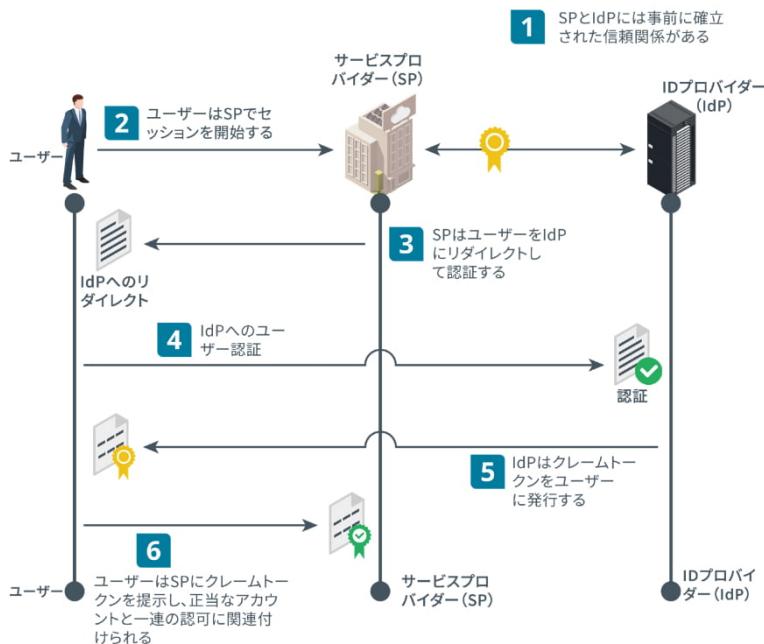
### フェデレーション

**フェデレーション**（認証連携）は、しっかりと定義された従業員グループだけでなく、より多くのユーザーがアクセスする必要のあるネットワークを表す概念です。ビジネスにおいては、企業が自社ネットワークの一部をパートナー、サプライヤー、顧客に公開する必要がある場合があります。この企業は従業員用アカウントは十分に管理できます。しかし、各サプライヤーや顧客のアカウントを社内で管理することは、それよりも難しい場合があります。フェデレーションとは、この企業が他のネットワークによって作成、管理されたアカウントを信頼することを意味します。消費者の立場からの別の例を挙げると、ユーザーがGoogle AppsとTwitterの両方を使用したいと思う場合があります。GoogleとTwitterが認証と認可を目的としてフェデレーションネットワークを確立した場合、その後ユーザーはGoogleの認証情報を使用してTwitterにログインできるようになります。その逆も可能になります。

### IDプロバイダーとアステーション

これらのモデルでは、ネットワークがフェデレーションID管理を実行しています。あるネットワークのユーザーは、自分のアイデンティティを証明するアステーション（証明書）を提供することができます。ごく一般的に言えば、Kerberosの認可と同様のプロセスで、次のように動作します。

1. ユーザ（プリンシパル）は、サービスプロバイダ(SP, Service Provider)、あるいはリリングパーティ(RP, Relying Party)にアクセスしようとします。サービスプロバイダはプリンシパルを**IDプロバイダ(IdP)**にリダイレクトして認証を行います。
2. プリンシパルはIDプロバイダーで認証され、アイデンティティのアステーション（証明書）を取得します。これはIdPが署名したトークンやドキュメントなどの形式になります。
3. プリンシパルはこのアステーション（証明書）をサービスプロバイダーに提示します。サービスプロバイダーはそのIdPとの信頼関係により、IdPが署名した証明書の正当性を認めます。
4. ここで、サービスプロバイダーは認証されたプリンシパルを自身のアカウントデータベースに接続できます。プリンシパルがこの種類のアクセスを認可されている場合、サービスプロバイダーはIdPの保有するユーザーアカウントプロファイルの属性をクエリすることができます。



フェデレーションID管理の概要。(画像提供: © 123RF.com)

### クラウドベース要件とオンプレミス要件の比較

ある企業がクラウドサービスの使用やビジネスパートナーのネットワークとリソースの共有を行う必要がある場合、認証と認可の設計にはより厳しい制限とより多くの要件が伴います。ウェブアプリケーションはKerberosをサポートしていない場合があり、サードパーティのネットワークはActive Directory/LDAPと直接のフェデレーションをサポートしていない場合もあります。これらのクラウドネットワークの設計では、ウェブアプリケーション間でのフェデレーションやアテストーションを実行するための使用基準が必要となる可能性が高いのです。

### セキュリティアサーションマークアップ言語

フェデレーションネットワークやクラウドでは、ユーザーID証明の実装と、プリンシパル、リライジングパーティ(RP, Relying Party)、IDプロバイダー間のアテストーション(証明書)の受け渡しを行うための固有のプロトコルや技術が必要となります。セキュリティアサーションマークアップ言語(SAML)は、そのようなソリューションの1つです。SAMLアテストーション(または認可)は、拡張マークアップ言語(XML)で記述されます。通信はHTTP/HTTPSとSimple Object Access Protocol (SOAP)を用いて確立されます。これらのセキュアなトークンはXML署名仕様を用いて署名されます。このようなデジタル署名を使用することで、RPはIDプロバイダーを信頼することができます。

SAML実装の例として、Amazon Web Services (AWS)がSAMLサービスプロバイダーとして機能していることが挙げられます。これにより、AWSを利用してクラウドアプリケーションを開発する企業は、自社顧客のユーザーアイデンティティを管理し、AWS上で権限を付与することで、ユーザのアカウントを直接AWS上に作成する必要がなくなります。

```
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="200" Version="2.0"
```

```

IssueInstant="2020-01-01T20:00:10Z"
Destination="https://sp.foo/saml/acs"
InResponseTo="100".
<saml:Issuer>https://idp.foo/sso</saml:Issuer>
<ds:Signature>...</ds:Signature>
<samlp:Status>... (success)...</samlp:Status>
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
XMLSchema-instance"
xmlns:xss="http://www.w3.org/2001/XMLSchema" ID="2000"
Version="2.0"
IssueInstant="2020-01-01T20:00:09Z">
<saml:Issuer>https://idp.foo/sso</saml:Issuer>
<ds:Signature>...</ds:Signature>
<saml:Subject>...
<saml:Conditions>...
<saml:AudienceRestriction>...
<saml:AuthnStatement>...
<saml:AttributeStatement>
<saml:Attribute>...
<saml:Attribute>...
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>

```

## OAuthとOpenID Connect

多くのパブリッククラウドが、SOAPではなくREST (Representational State Transfer)に基づくアプリケーションプログラミングインターフェイス(API)を使用しています。これらは通常、RESTful APIと呼ばれます。SOAPが厳密に指定されたプロトコルであるのに対して、RESTはより緩やかなアーキテクチャのフレームワークです。これによってサービスプロバイダーは、実装する要素についてより多くの選択肢を得ることができます。SOAPやSAMLと比較して、モバイルアプリへの対応が充実しています。

### OAuth

RESTful APIの認証と認可は多くの場合、**Open Authorization (OAuth)**プロトコルを使用して実装されます。OAuthは、サイト間でのユーザープロファイル内の情報（リソース）共有を促進するように設計されています。ユーザーはIDプロバイダー(IdP)で、パスワードで保護されたアカウントを作成します。ユーザーはそのアカウントを使用して、OAuthコンシューマーサイトにパスワードを提示することなくログインすることができます。ユーザー（リソースオーナー）はクライアントにアカウントの一部にアクセスするための認可を与えます。ここでのクライアントは、アプリケーションやOAuthコンシューマーサイトを意味しています。

このユーザー アカウントは、1つ以上のリソースサーバーによってホストされます。リソースサーバーは、クライアント（OAuthコンシューマー サイトやモバイルアプリ）がユーザー属性にアクセスするための機能をホストするため、APIサーバーとも呼ばれます。認可のリクエストは、認可サーバーによって処理されます。単一の認可サーバーが複数のリソースサーバーを管理することができます。同様に、リソースと認可のサーバーが同じサーバーのインスタンスになることがあります。

クライアントのアプリケーションやサービスは、認可サーバーへの登録が必要です。このプロセスの一環として、クライアントはリダイレクトURLを登録します。これが認可トークンを処理するエンドポイントになります。また登録によって、クライアントにIDと秘密鍵が提供されます。このIDは人目に触れても問題ありませんが、秘密鍵はクライアントと認可サーバーの間で秘密情報として維持される必要があります。クライアントのアプリケーションが認可をリクエストする時、ユーザーは認可サーバーが適切な方法を用いてそのリクエストに応じることを承認します。OAuthは、サーバーからサーバー、モバイルアプリからサーバーといった、さまざまな状況で使用される複数の種類やフローの付与に対応しています。フローの種類に応じて、クライアントは認可サーバーが検証したアクセストークンを得ます。クライアントはこのアクセストークンをリソースサーバーに提示して、トークンが有効だった場合はリソースへのリクエストを承認します。

OAuthはデータの要求にJavaScript Object Notation (JSON) Web Tokens (JWT) フォーマットを使用します。JWTはURLとHTTPヘッダーでBase64エンコード文字列として容易に渡すことができ、認証と完全性のためにデジタル署名を行うことができます。

### OpenID Connect (OIDC)

OAuthは要求を認可することを目的として明確に設計されたもので、ユーザーを認証するものではありません。トークン内のフィールドと属性の詳細は定義されていません。認可リクエストを開始したユーザーがログインしたままの状態で留まっているかを検証するメカニズムはありません。一度付与されたアクセストークンには、認証情報は含まれません。**OpenID Connect (OIDC)**とは、精密に定義されたトークンフィールドを持つ、OAuthフローの特別な種類として実装される認証プロトコルです。



OpenIDは、2005年～2007年の間に開発された早期のプロトコルを意味する場合もある点に注意してください。これは、類似のフレームワークを実装し、早期には「～でサインオン」機能を支えていたのですが、現在ではすでに使用されていません。OpenIDはXMLフォーマットのメッセージを使用し、ウェブアプリケーションのみに対応し、モバイルアプリは対象外です。

# レビュー アクト ティビティ：

## 認可ソリューション

次の質問にお答えください。

1. 強制アクセス制御ポリシーに対して、中央化されていない任意アクセス制御ポリシーの利点は何ですか？
2. セキュリティグループの権限管理とロールベースの権限管理の違いは何ですか？
3. ルールベースアクセス制御のモデルにおいて、サブジェクトがアクセス特権についてデータオーナーとネゴシエートすることは可能ですか？その理由もあわせてお答えください。
4. ディレクトリサービスの目的は何ですか？
5. 次の記述は正しいですか、誤りですか？以下の文字列は、識別名の一例です。  
**CN=ad, DC=classroom, DC=com**
6. あなたは、ユーザーがウェブ経由またはモバイルアプリからソーシャルメディアアカウントを使用してログインできるクラウドアプリケーションについて業務を行っています。検討すべき、最適な選択となるプロトコルは何ですか？

# トピック8D

## 人事ポリシーの重要性を説明する



### 対象試験範囲

5.3組織のセキュリティに関するポリシーの重要性について説明することができる

アイデンティティおよびアカウント管理のための技術的制御の実装に加え、従業員が適切なセキュリティ手順とポリシーを確実に遵守できるようにする必要があります。人的要素は顕著な攻撃対象領域となっており、ソーシャルエンジニアリング攻撃は特にこの部分に関わるものです。セキュリティのプロフェッショナルとして、人事(HR)部門と協力し、ポリシー策定や、セキュリティ意識向上/トレーニングプログラムの開発、提供を支援します。

### 行動に関するポリシー

業務に関するポリシーには、特権/認証情報管理、データの取り扱い、インシデント対応が含まれます。その他の重要なセキュリティポリシーには、従業員の行動の監督、プライバシー保護などがあります。

### 利用規定

**利用規定(AUP)**の施行には、従業員による設備の不正使用に関するセキュリティおよび法的問題から組織を保護するという重要な役割があります。通常、これらのポリシーは詐欺行為や誹謗中傷、違法マテリアルの入手を目的とした設備の使用を禁止しています。また、承認されていないハードウェアやソフトウェアのインストールを禁止し、従業員がアクセスを許可されていない機密データのスヌーピングやその試みを明示的に禁止しています。利用規定は合理的でなければならず、従業員の基本的な職務を阻害したり、プライバシー権を侵害したりするものではありません。組織によっては、AUPで業務外のインターネットツールの使用を禁じたり、休憩時間に使用するよう制限している場合があります。

### 行動規範とソーシャルメディア分析

**行動規範**または行動指針は、期待される職業上の行動基準を定めたものです。例えば、従業員によるソーシャルメディアの使用やファイル共有は、ウイルス感染やシステムへの侵入、労働時間の損失、著作権侵害、誹謗中傷など、組織に重大なリスクをもたらします。従業員は、組織のコンピューターシステムを介したデータ通信（電子メールなど）はシステムやサーバー、バックアップデバイスに保管される場合があることを認識しておく必要があります。また、このような通信は記録や監視をされている場合もあります。雇用者が、従業員個人のソーシャルメディアアカウントを対象に分析と監視を行い、ポリシー違反をチェックする場合もあります。

コンピューターシステムへの特権アクセスを付与する従業員を検討する際にも行動規範は大切です。技術者やマネージャーは、特権の乱用（他の従業員に関する情報を盗み見る、セキュリティ機構を無効化するなど）を自らに禁止する条項を遵守する必要があります。

### 職場における個人所有デバイスの使用

スマートフォンやUSBスティック、メディアプレーヤーなどのポータブルデバイスは、ファイルを容易にコピーできるため、データセキュリティに深刻な脅威をもたらす可能性があります。カメラや音声録音機能も明らかに危険をはらんでいます。このようなデバイスの企業ネットワーク

への接続を防止するには、ネットワークアクセス制御/エンドポイント管理やデータ損失防止ソリューションが役立ちます。こうしたデバイスの職場への持ち込み禁止を進めている企業もありますが、これを徹底することは簡単ではありません。

また、従業員による個人所有のソフトウェアの不正使用や、従業員がプロジェクトに承認されていないソフトウェアやサービスを使用すること（シャドーIT）を検討することも重要です。個人所有のソフトウェアには、個人用電子メールやインスタントメッセンジャーなど、ローカルにインストールされたソフトウェアかホストされたアプリケーションのいずれかが含まれており、組織にさまざまなセキュリティ上の脆弱性をもたらす可能性があります。このようなプログラムは、データ流出やマルウェアの転送メカニズムの経路になったり、会社が責任を負うソフトウェアライセンスの違反につながる場合もあります。ここに挙げたのは問題の可能性のほんの一例です。

### デスクの整理整頓ポリシー

**デスクの整理整頓ポリシー**とは、各従業員の業務エリアに一切の書類が放置されていないようにする必要があるとするポリシーです。このポリシーの目的は、承認されていないスタッフや来訪者による、職場での機密情報の取得を防ぐことです。

### ユーザートレーニングと役割に基づくトレーニング

セキュアなシステムにおけるその他の重要な要素として、効果的なユーザートレーニングが挙げられます。トレーニングを受けていないユーザーは深刻な弱点となります。ソーシャルエンジニアリングやマルウェア攻撃を受けやすく、機密情報や要配慮情報の取り扱い時に適切な注意が払えない場合があるためです。



セキュリティ慣行に関するユーザートレーニング。(画像提供：dotshock © 123RF.com)

適切なセキュリティへの意識向上トレーニングを全レベルの従業員（エンドユーザー、技術系スタッフ、経営陣）に提供する必要があります。トレーニングの対象とする必要のある一般的な項目は次の通りです。

- 組織のセキュリティポリシーと違反した場合の罰則に関する概要。
- インシデントの特定と報告手順。

- 安全訓練、来訪者の案内、セキュリティ保護された領域の使用、個人所有デバイスの使用など、サイトセキュリティの手順、制限事項、推奨事項。
- ドキュメントの機密性、PII、バックアップ、暗号化など、データの取り扱い。
- パスワード管理とアカウント管理、パソコンやモバイル機器のセキュリティ機能。
- フィッシング、Webサイトの悪用、スパムなどのソーシャルエンジニアリングやマルウェアの脅威に対する意識向上、新たな攻撃に対する警告方法。
- ブラウザやメールクライアントなどのソフトウェアのセキュアな使用、ソーシャルネットワーキングサイトなどへの適切なインターネットアクセス。

セキュリティに関わる職務を実施するスタッフを特定し、必要なトレーニングや教育のレベルを区分（初心者、中級者、上級者など）するシステムも必要です。トレーニングプログラムの定義では、役職ではなく役割に注目する必要があります。従業員はさまざまな役割を抱っており、各役割に応じたトレーニング、教育、意識向上の必要性があるためです。

 NISTのNational Initiative for Cybersecurity Educationフレームワーク([nist.gov/itl/applied-cybersecurity/nice](https://nist.gov/itl/applied-cybersecurity/nice))では、サイバーセキュリティに関わるさまざまな役割の知識、スキル、能力(KSAA)を定めています。セキュリティ意識向上プログラムは、[SP800-50\(nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf\)](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf)に記載されています。

## トレーニング技術の多様性

セキュリティトレーニングは、エンドユーザーが対応できる言葉で構築する必要があります。また教育では、ユーザーに関する責任や脅威に焦点を当てるべきです。出現している新たな脅威（ファイルレスマルウェア、フィッシング詐欺、ソフトウェアのゼロデイ攻撃など）についてユーザーを教育する必要がありますが、これもユーザーが理解できる言葉で説明するようにしましょう。

さまざまなトレーニング技術の使用は、従業員の参加意識の向上や記憶の定着に役立ちます。トレーニング方法として、ファシリテーターによるワークショップやイベント、1対1の説明やメンタリングに加え、コンピューターベースやオンラインのトレーニング、映像、書籍、ブログ/ニュースレターなどのリソースが活用できます。

### フィッシングキャンペーン

フィッシングキャンペーンのトレーニングイベントでは、ユーザーにフィッシングメッセージを送信して、シミュレーションを行います。メッセージに応答したユーザーはフォローアップトレーニングの対象となります。

### キャプチャーザフラッグ

キャプチャーザフラッグ(CTF)は、通常、倫理的ハッカー養成プログラムやゲーム要素をえた競技に使用されます。参加者はフラッグを発見するために、仮想化したコンピューター環境内で一連の課題を完了する必要があります。このフラッグは脅威アクターの活動（ブルーチーム用の演習）か脆弱性（レッドチーム用の演習）のいずれかであり、参加者は分析ツールや適切なツールを用いてそれを発見します。キャプチャーザフラッグでは、ユーザーは次のレベルに進み、新たな課題にチャレンジすることができます。参加者が入門レベルに合格したら、チームに加わり、競技イベントに参加します。ここでは、その環境内に複数のフラッグが埋め込まれており、それらをキャプチャーすることで参加者とチームにポイントが入ります。

### コンピューターベースのトレーニングとゲーム的要素

CTFイベントでの競技的な課題に対する参加者の反応は良好です。この種類のゲーム的要素は、他の役割のセキュリティに対する意識向上にも使用できます。コンピューターベースのトレーニング(CBT)では、学習者が以下のような実践的でさまざまな種類の活動を完了することで、スキルと経験を得ることができます。

- ・ シミュレーション — システムのインターフェイスを複製するか、エミュレーターを使用することで、学習者が構成タスクを練習します。
- ・ 分岐シナリオ — 学習者は、サイバーセキュリティインシデントや構成上の問題を解決するための最善の選択肢を選び出します。

CBTでは、参加意欲向上するためにテレビゲーム的な要素が使用される場合があります。例えば、学習者はバッジや、ゲーム内のアバターを強化するスキルやデジタルアイテムなどのレベルアップのボーナスを獲得します。シミュレーションでは、学習者が3Dの世界の地図からインシデントを選び、シミュレーション環境で取り組めるようなものが提示されるかもしれません。

# レビューアク ティビティ： 人事ポリシーの重要性

次の質問にお答えください。

1. 昨年あなたの会社は、フィッシング攻撃の被害を数回受けました。脅威アクターはこれらの攻撃により認証情報の取得に成功し、それらを使用して主要なシステムを侵害しました。このようなソーシャルエンジニアリングの成功に利用された脆弱性は何ですか？また、その理由は？
2. 組織が役割に基づいたトレーニングプログラムを策定するべき理由は何ですか？
3. 製造企業向けのセキュリティ意識向上プログラムを企画しています。リソースに関しては、小冊子で十分と言えるでしょうか？

# レッスン8

## 概要

インサイダーの脅威やアカウント侵害のリスクを低減する、組織的および技術的ポリシー、トレーニング/意識向上プログラムを適用できる必要があります。また、必要に応じて任意アクセス制御カルールベースアクセス制御を実装し、フェデレーションIDネットワーク全体で認可をやり取りするプロトコルを使用できる必要があります。

### アイデンティティおよびアカウント管理制御実装のためのガイドライン

ローカルネットワークやクラウドへのアクセス用に、アイデンティティおよびアカウント管理制御を実装する際には、以下のガイドラインに従ってください。

- 任意、ロールベース、強制、属性ベースの各アクセス制御に関する要件と、その要件がフェデレーションサービス（例えば、オンプレミスとクラウドの連携など）が含むかどうかを確認する。
- アカウント/ロール、リソースを構成し、最小限の特権の原則を使用して適切な権限を設定する。
- 次のアカウントポリシーを構成して、完全性を保護します：
  - 一般アカウントと特権アカウントの保護を確保できる認証情報に関するポリシー（セキュアなパスワードの選択など）。
  - 共有、デバイス、サードパーティ/APIの機密を管理する認証情報に関するポリシー。
  - 場所と時間に基づいた条件付きアクセスを適用するアカウント制御。
  - 職務分掌を適用し、職務に応じたセキュリティ意識向上プログラムとトレーニングを実施する組織的ポリシー。
- デジタルアイデンティティとアカウント認証情報をセキュアに発行するための、オンボーディング手順の確立。
- アカウントの使用状況と権限の割り当てを確認する監査手順の確立。
- 従業員や請負業者との契約終了時にアクセス権限を削除するオフボーディング手順の確立。
- オンプレミスのネットワークやクラウドサービス/アプリケーションの間でシングルサインオンを実現する、SAMLまたはOAuth/OIDCの導入。



# レッスン9

## セキュアなネットワーク設計を実装する

### レッスン概要

ユーザーの認証や認可を管理することは、セキュアな情報技術サービスを構築する一部分に過ぎません。ネットワークインフラストラクチャは、機密性、完全性、可用性の各特性と共にサービスを実行するよう設計されなければなりません。あなたは設計を直接担当していないかもしれません、設計関連の決定を支える要素を理解し、ルーター、スイッチ、アクセスポイント、ロードバランサーをセキュアな構成でデプロイ（展開）して、設計を実装できるようになる必要があります。

### レッスンの目的

このレッスンの内容は、以下のとおりです。

- セキュアなネットワーク設計を実装する。
- セキュアなルーティングとスイッチングを実装する。
- セキュアなワイヤレスインフラストラクチャを実装する。
- ロードバランサーを実装する。

# トピック9A

## セキュアなネットワーク設計を実装する



### 対象試験範囲

3.3 与えられたシナリオに基づいて、セキュアなネットワークデザインを実装することができる。

あなたは現在の職務でネットワーク設計を担当していないかもしれません、ネットワークアーキテクチャの弱点から生じ得る脆弱性と、良好に設計されたネットワークの実現に向けた一般的な原則のいくつかを理解することが重要です。そうすれば、プロジェクトに貢献して耐性を向上させ、改善に向けた提言を行うのに役立ちます。

### セキュアなネットワーク設計

セキュアなネットワーク設計は、ビジネスのワークフローを支える資産とサービスに、機密性、完全性、可用性の特性を持たせます。ネットワークアーキテクチャの脆弱性によって、検知されない侵入や壊滅的なサービス障害に繋がる影響をより受けやすくなります。一般的な脆弱性には、以下のものがあります。

- シングルポイント障害 — 単一のハードウェアサーバーまたはアプライアンス、もしくはネットワークチャネルに依存する「ピンチポイント」。
- 複雑な依存関係 — 多数の異なるシステムの使用を必要とするサービス。個々のシステムやサービスの障害が、他のネットワークサービスのパフォーマンス全体に影響を与えないことが理想です。
- 可用性が機密性と完全性に優先する — 「ショートカット」を使ってサービスを起動・実行させる誘惑に駆られることがあります。セキュリティを犠牲にすることで素早い修復が可能になっても、長期的なリスクが発生します。
- 文書化と変更管理の欠如 — ネットワークセグメント、アプライアンス、およびサービスが、適切な変更管理手順を経ずに追加され、ネットワークの構成方法に関する可視性が失われてしまうことがあります。ビジネスワークフローとそれを支えるネットワークサービスを、ネットワーク管理者が理解することが不可欠です。
- 境界セキュリティに対する過度の依存 — ネットワーク・アーキテクチャが「フラット」であれば（つまり、どのホストも他のホストと接続できるのであれば）、ネットワーク周辺部から侵入することで、脅威アクターが自由に動き回ることができます。

CiscoのSAFEアーキテクチャ ([cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing\\_safe.html#-overview](https://cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html#-overview))は、ネットワークアーキテクチャ設計という複雑なトピックを理解する優れた出発点です。SAFEガイダンスは「ネットワーク内の場所(PIN)」に触れています。PINは、キャンパスネットワーク、支店、データセンター、およびクラウドなど、ネットワークロケーションの各タイプを示すものです。これらのネットワークには、インターネットエッジとWANという2つの特別な場所があり、拠点間や信頼できないネットワークとの接続を容易にしています。

それぞれのPINは、脅威防御、セグメント化、セキュリティインテリジェンス、および管理といったセキュリティ機能分類の、セキュリティ制御や能力で保護することができます。

## ビジネスワークフローとネットワークアーキテクチャ

ネットワークアーキテクチャは、ビジネスワークフローをサポートするように設計されます。電子メールなどの単純なワークフローを分析することで、どのような判断が必要なのかを説明することができます。

- アクセス — クライアントデバイスはネットワークにアクセスし、物理チャネルと論理アドレスを取得しなければなりません。電子メールアプリケーションを使用するにあたり、ユーザーは認証と認可を受ける必要があります。そこから導けるのは、不正なユーザーやデバイスにはアクセスを拒否しなければならない、ということです。
- メールボックスサーバー — 認可されたクライアントのみがメールボックスにアクセスでき、可用性と耐障害性を持つようにします。電子メールサービスが最低限の依存関係で動作し、障害に対する耐性を有するように設計されていることが必要です。
- メール転送サーバー — これは信頼できないインターネットホストと接続しなければならないので、信頼できないネットワークと信頼できるLANとの通信は、慎重に制御しなければなりません。ネットワークを出入りするすべてのデータとソフトウェアは、ポリシーを基にした制御の対象とする必要があります。

このタイプのビジネスフローには、ネットワーク内のさまざまな場所のシステムが関わることがわかります。すべてのクライアント、メールボックス、およびメール転送サーバーを同じ論理ネットワーク「セグメント」の中に配置することで、多くの脆弱性が生じます。データがそれらロケーション間をどのように流れるかを理解して制御することは、セキュアかつ効果的なネットワーク設計の重要な部分です。

## ネットワークアプライアンス

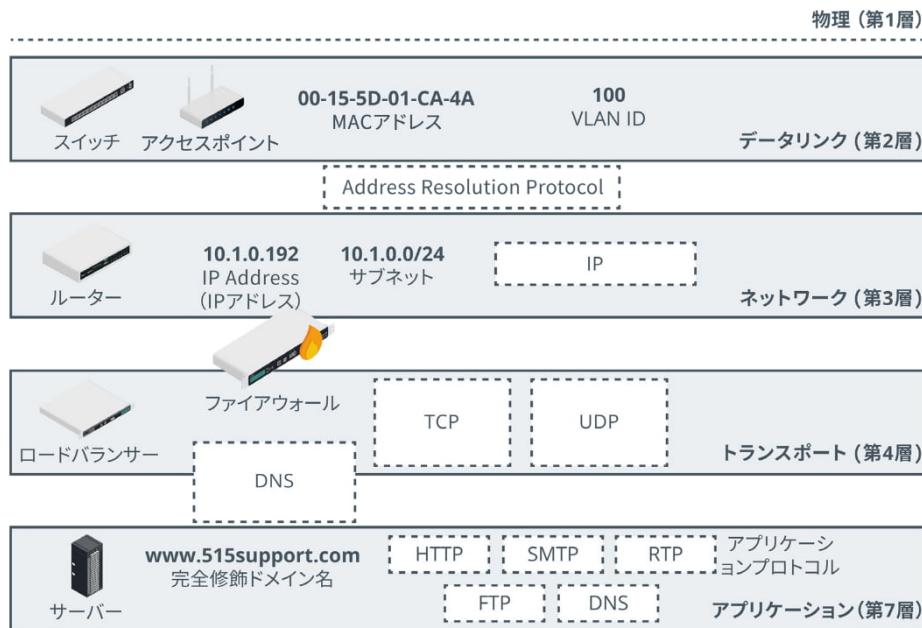
ネットワークアーキテクチャのプロビジョニングには、多数のネットワークアプライアンスが関わっています。

- **スイッチ** — ケーブル接続されたネットワーク内のノード間でフレームを転送します。スイッチはOSIモデルの第2層で動作し、接続されたノードのハードウェアまたはMAC (Media Access Control)アドレスを基に、転送の決定を行います。スイッチは、配線に直接マッピングするか、スイッチのコンフィギュレーションで**仮想LAN (VLAN)**として作成された論理的なセグメントにマッピングすることにより、ネットワークセグメントを確立することができます。



ネットワークの設計やトラブルシューティングを行う場合、機能を個別の層に区分けすることが有効です。ネットワーク機能の階層を定義する方法として、*OSI (Open Systems Interconnection)*モデルが広く引用されています。

- **ワイヤレスアクセスポイント** — ケーブル接続されたネットワークと、ワイヤレスクライアントまたはステーションとの接続点となります。アクセスポイントはOSIモデルの第2層で動作します。
- **ルーター** — 相互接続ネットワークでパケットを転送し、IPアドレスを基に転送の決定を行います。ルーターはOSIモデルの第3層で動作します。ルーターはネットワーク内の各セグメントに論理IPサブネットアドレスを割り当てることができます。
- **ファイアウォール** — アクセス制御リスト(ACL)を適用することで、ネットワークセグメントを出入りするトラフィックをフィルターします。ファイアウォールはOSIモデルの第3層以上で動作します。
- **ロードバランサー** — ネットワークの各セグメント間または各サーバー間でトラフィックを分配し、パフォーマンスを最適化します。ロードバランサーはOSIモデルの第4層以上で動作します。
- **DNS (Domain Name System)サーバー** — ネームレコードをホストし、名前解決を行うことで、アプリケーションとユーザーがIPアドレスでなく完全修飾ドメイン名(FQDN)を使用して、ホストとサービスのアドレスを指定できるようにします。DNSはOSIモデルの第7層で動作します。名前解決はネットワーク設計における重要なサービスです。名前解決の悪用は一般的な攻撃ベクトルです。



OSI ネットワークレイヤーレファレンスモデル内のアプライアンス、プロトコル、およびアドレス機能。  
(画像提供 : © 123RF.com)

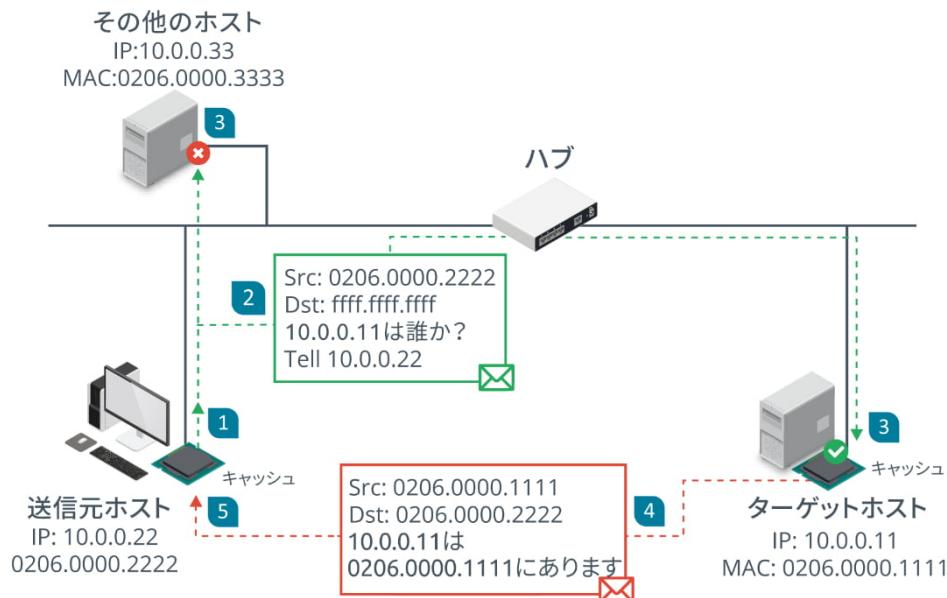
## ルーティングとスイッチングのプロトコル

ネットワークの基本的な機能は、あるノードから別のノードにトラフィックを転送することです。転送を実行するにあたっては、多数のルーティングプロトコルとスイッチングプロトコルが使用されます。転送機能は2つの異なる層で実行されます。

- 第2層の転送は、すべて同じブロードキャストドメイン内にある、同一のローカルネットワークセグメント上の各ノード間で行われます。第2層において、ブロードキャストドメインは、同一の物理的なアンマネジドスイッチに接続されたすべてのノードか、1つ以上のマネージドスイッチ上で構成された仮想LAN (VLAN)内のすべてのノードのどちらかです。また第2層においては、各ノードはネットワークインターフェイスのハードウェアか、MAC (Media Access Control)アドレスのどちらかによって識別されます。MACアドレスは16進数で記述された48ビットの値です (例 : 00-15-5D-F4-83-48)。
- 第3層の転送、またはルーティングは、論理的かつ物理的に定義されたネットワーク間で行われます。単一のネットワークを複数の論理ブロードキャストドメインに分割することを、サブネット化といいます。ルーターによって結合された複数のネットワークは相互接続ネットワークを形成します。第3層において、各ノードはインターネットプロトコル(IP)アドレスによって識別されます。

## アドレス解決プロトコル (Address Resolution Protocol : ARP)

アドレス解決プロトコル(ARP)は、ネットワークインターフェイスのハードウェアの(MAC)アドレスとIPアドレスを対応させます。通常、あるIPアドレスにパケットを送信する必要があるものの、受信側デバイスのMACアドレスを知らないデバイスは、ARPリクエストパケットをブロードキャストし、それに一致するIPを持つデバイスがARPリプライで応答します。



## インターネットプロトコル(IP)

IPは論理ネットワークおよびサブネットのアドレス指定メカニズムを提供します。32ビットのIPv4アドレスはドット形式10進表記法で記述され、ネットワークID部分とホストID部分にアドレスを分割するためのネットワークプレフィックスかサブネットマスクを伴っています。一例を挙げると、172.16.1.101/16というIPアドレスにおいて、/16プレフィックスは、そのアドレスの前半(172.16.0.0)がネットワークIDである一方、残りの部分がそのネットワーク上のホストを一意に識別することを示しています。この/16プレフィックスは、255.255.0.0という形でサブネットマスクとしても記述することができます。

またネットワークは、128ビットのIPv6アドレスも使用しています。IPv6アドレスは16進表記法を用いて、次の一般的なフォーマットで記述されます。2001:db8::abc:0:def0:1234. IPv6において、最後の64ビットはホストのインターフェイスIDとして指定されています。また最初の64ビットには、一定の階層構造内のネットワーク情報が含まれています。例えば、ISPルーターは最初の48ビットを使用して、そのネットワークがグローバルインターネット上のどこにホストされているかを判断することができます。そのネットワーク内で、サイト管理者は(64ビットの)残りの16ビットを使用することで、ローカルネットワークをサブネットに分割することができます。

## ルーティングプロトコル

相互接続ネットワーク内の個々のネットワークにどう到達するかについての情報は、ルーティングテーブルにその情報を保存しているルーターによって処理されます。あるネットワークへのルートは静的に構成できますが、ほとんどのネットワークはルーティングプロトコルを使用することで、ルーター間の更新された新しいルートを送信しています。一般的なルーティングプロトコルとして、**BGP (Border Gateway Protocol)**、**OSPF (Open Shortest Path First)**、**EIGRP (Enhanced Interior Gateway Routing Protocol)**、および**RIP (Routing Information Protocol)**があります。

## ネットワークのセグメント化

ネットワークセグメントでは、そのセグメントに接続されたすべてのホストがローカル（第2層）転送を使用し、別のホストと自由に通信できます。それらのホストは、同じブロードキャストドメイン内にあると言われます。セグリゲーション（分離）は、あるセグメント内のホストが、別のセグメント内のホストと通信するにあたり、その方法が制限されていることを意味します。それらのホストは、例えはある特定のネットワークポートを介してのみ通信することができます。



「自由に」とは、いかなるネットワークアプライアンスやポリシーも通信を防いでいないことを意味します。それぞれのホストはアクセス規則やホストファイアウォール、またはアクセスを防ぐその他のセキュリティツールで構成することができますが、「ネットワークからの視点」とは、同じセグメント内のすべてのホストが自由に通信を試みることができるという意味です。

またイーサネットネットワークについて言えば、1つのセグメント内の全ホストを1つのスイッチに、別のセグメント内の全ホストを別のスイッチに接続することで、物理的にネットワークセグメントを確立させることができます。これら2つのスイッチはルーターによって接続することができ、そのルーターはネットワークポリシーやアクセス制御リスト(ACL)を実行することで、2つのセグメント間の通信を制限することができます。

通常、企業ネットワークは数百ものスイッチングアプライアンスやネットワークポート（ワイヤレスアクセスやリモートアクセスは言うまでもありません）を擁しているので、セグメント化は仮想LAN (VLAN)を用いて実行される可能性がより高くなっています。スイッチのポートは、スイッチの物理的な位置に関係なく、同じトポロジー内の任意のVLANに割り当てることができます。第2層でVLANによって実行されるセグメント化は、第3層でIPサブネットによって実行される論理的分割と対応させることができます。

## ネットワークトポロジーとゾーン

セグリゲート（分離）されたネットワークセグメントを作成する能力があれば、異なるネットワークゾーンのトポロジーの定義を始めることができます。トポロジーは、コンピューターネットワークが物理的または論理的にどう構成されているかを説明するものです。論理的または物理的なネットワークトポロジーを分析し、脆弱性のある箇所を特定すると共に、機密性、完全性、可用性の目標が設計によって満たされるようにしなければなりません。

セキュリティトポロジーを構築する主要なブロックはゾーンです。ゾーンとは、あるネットワークにおいて、そのネットワーク内の全ホストのセキュリティ構成が同一であるエリアのことです。VLANとサブネットを用いて物理的または論理的にセグメント化することで、ゾーンはお互いにセグリゲート（分離）されなければなりません。ゾーン間のトラフィックは、セキュリティデバイス（通常はファイアウォール）を用いて厳しく制御する必要があります。

キャンパスネットワークやデータセンターをゾーンに分割することは、各ゾーンが異なるセキュリティ構成を有していることを示しています。主なゾーンとして次のものがあります。

- **イントラネット（プライベートネットワーク）** —これは、組織が所有・管理している信頼できるホストのネットワークです。イントラネットの内部には、サーバー、従業員のワークステーション、VoIP電話機、および管理用ワークステーションなど、異なるホストグループのサブゾーンがあるかもしれません。



あなたの管理コントロールの下にあり、あなたがネットワークを守るためにセットアップしたセキュリティメカニズム（アンチウイルスソフトウェア、ユーザー権限、またはソフトウェアのアップデートなど）の対象になっているという意味で、ホストは信頼されています。

- エクストラネット—通常はビジネスパートナー、サプライヤー、顧客など、ある程度信頼できるホストのネットワークです。ホストがエクストラネットに加わるには、認証を経なければなりません。
- インターネット/ゲスト—これは、信頼できないホストによるインターネット経由の匿名のアクセス（または匿名のアクセスと許可を得たアクセスの組み合わせ）を許可しているゾーンです。