

提供の両方が行われます。ただし現在では、ネットワークの大部分でサードパーティのクラウドサービスが使用されています。そのような状況では、ウェブベースのサービス全体でフェデレーションID管理を実施するために、さまざまなプロトコルやフレームワークが利用できます。つまり、ユーザーは1つのプロバイダーでデジタルアイデンティティを作成でき、他のサイトがそのアイデンティティを使用してアプリケーションの使用を認可できるということです。

バックグラウンドチェックとオンボーディングポリシー

アイデンティティとアクセス管理 (IAM)は、IT/セキュリティの手順や技術、人事(HR)ポリシーの両方に関わるもので、人材管理ポリシーは次の3つの段階で適用されます。

- 採用活動（雇用）— 特定の職務を遂行できる人材を探し選考するプロセス。この段階では、候補者の審査とバックグラウンドチェックに関連してセキュリティ問題が発生する場合があります。
- 業務（労働）— 大規模な組織ではトレーニングと人材開発の専門部門を設置している場合もありますが、通常はHRが従業員へのポリシーの周知とトレーニングを担当します。そのため、HRマネージャーは、従業員がセキュリティの重要性を学ぶことができるトレーニングプログラムを作成する必要があります。
- 雇用契約終了や退職（解雇や退職）— 従業員の離職が自主的か非自主的かを問わず、雇用の終了は数多くのセキュリティ問題の潜む難しいプロセスです。

バックグラウンドチェック

バックグラウンドチェックでは、ある人物について、本人が自称する身元と相違ないこと、犯罪歴や破産歴を隠していないこと、不適切なまたは危険な関係性を隠していないことを確認します。機密性の高い環境で業務を行う従業員や高価値の取引に関するアクセス権を持つ従業員については、より厳重な審査の対象とする必要性があることは明らかです。一部の職業、特にセキュリティ審査の必要な連邦関係の職業では、バックグラウンドチェックは必須です。バックグラウンドチェックは社内で実施されることもあれば、外部のサードパーティによって実施される場合もあります。

オンボーディング

人事部門レベルのオンボーディングとは、組織に新たな従業員を迎えるプロセスを意味します。また、同様の原則がサプライヤーや請負業者を新規採用する場合にも適用されます。同様のチェックやプロセスの一部は、顧客アカウントやゲストアカウント作成時にも使用されます。オンボーディングの一環として、IT部門とHR部門は協力して、ユーザーがコンピューターシステムにアクセスするためのアカウントを作成し、適切な権限を割り当て、アカウントの認証情報を正当なユーザーのみに確実に知らせます。これらの部門は連携して、過失によって構成の脆弱性を生みだすこと（IT部門が実際に雇用されていない従業員のアカウントを作成してしまうなど）を避けなければなりません。オンボーディングのプロセスに関わる他の業務やプロセスには、次のものがあります。

- 認証情報のセキュアな送信** — 初期パスワードを作成して送信する、またはスマートカードをセキュアに発行します。このプロセスでは、管理スタッフの不正に対する保護策が必要です。単純なパスワードやデフォルトパスワードを持つ新規作成のアカウントは、簡単に悪用されてしまうバックドアです。
- 資産の割り当て** — ユーザーにコンピューターやモバイル機器を提供するか、BYOD（私物情報端末の持ち込み）のハンドセットの使用に合意します。
- トレーニング/ポリシー** — セキュリティ意識向上や役割に関連する適切なトレーニングや資格検定を計画します。

秘密保持契約書(NDA)

秘密保持契約書(NDA)の条項は雇用契約書内に組み込まれている場合や、別の文書として用意されている場合があります。従業員や請負業者はNDAに署名し、機密情報をサードパーティと共有しないことを表明します。

権限管理のための人事ポリシー

HRとITが協力し、効果的な権限管理を実施する必要があります。これらのポリシーは、インサイダーの脅威のリスクを最小化することを目的とします。

職務分掌

職務分掌とは、重要なシステムや手順がインサイダーの脅威により危険にさらされる可能性に対して、抑制と均衡の確保を構築する手法です。倫理的衝突や職権乱用を防止するために、職務や責任は複数名で分担する必要があります。



従業員は会社の利益のみのために働くことが期待されます。従業員が自分の個人的な利益やサードパーティの利益のために行動するような状況を利益相反と呼びます。

職務分掌は、従業員がセキュリティポリシーに従う義務を負うことを意味します。

- 標準業務手順書(SOP)とは、重要な業務の実施に関するプロトコルで、従業員は必ずこれに従わなければなりません。
- 権限の分担とは、1人のユーザーが自分の権限に対してアクションを実行したり、変更を加えることはできないことを意味します。変更する場合は、少なくとも2名の認可が必要です。例として、購買（発注）とその支払いの承認に、責任を分散させることが挙げられます。別の例としては、アカウント作成の依頼は承認と監視の対象となることが挙げられます。



職務分掌によってリスクが完全に除去されるわけではありません。複数人が癒着する機会は依然として残っています。ただし、従業員が単独で不正を働くよりも発生の可能性は各段に低くなります。

最小限の特権

最小限の特権とは、ユーザーが自分の職務を実施するために必要な権限のみを付与することを意味します。これによって、アカウントが侵害されて脅威アクターの支配下に置かれた場合のリスクが低減されます。認可クリープ(Authorization creep)とは、直接またはセキュリティグループやロールに追加されることで、ユーザーがさらに多くの権限を取得していく状況を意味します。最小限の特権は、業務のワークフローを詳細に分析し、定期的なアカウント監査を実施して、業務に必要な権限を評価したうえで決定すべきです。

ジョブローテーション

ジョブローテーション（または職務ローテーション）とは、同じ職務に既定よりも長い期間就くことは許可されないことを意味します。例えば、マネージャーは定期的に別の部門に異動し、従業員は年間を通じて担当業務がいくつ切り替わり、複数の役割を担います。ファイアウォール管理者やアクセス制御担当者のような役割をローテーションさせることで、信頼できる従業員間で重要な制度面における知識が拡大されるため、組織は特定の担当者に依存しそぎすぎなくなくなります。またジョブローテーションは、職権濫用を防ぎ、業務のマンネリ化を低減し、個人の職業的技術を高めることに役立ちます。

強制休暇

強制休暇とは、従業員が強制的に休暇を取得させられるもので、その間は別の誰かがその職務を遂行します。一般的な強制休暇ポリシーでは、従業員は少なくとも年に1回丸1週間の休暇を取り、連続して5日間以上職務から離れるよう定めています。この休暇の間に、会社の監査とセキュリティの担当者が従業員の活動に逸脱がないかを調査し、発見する時間を得ることができます。

オフボーディングポリシー

退職時面談（またはオフボーディング）は、従業員が適切に会社を退職できるようにするプロセスです。またオフボーディングは、請負業者やサードパーティを使用するプロジェクトの終了時にも使用されます。セキュリティの点では、完全に実施する必要のあるプロセスが複数あります。

- アカウント管理 — ユーザーアカウントと権限を無効にします。その従業員が作成または管理したが、会社の所有物である情報資産（暗号鍵やパスワードで保護されたファイルなどについて）に確実にアクセスできるようにします。
- 会社の資産 — モバイルデバイス、鍵、スマートカード、USBメディアなどを回収します。従業員が情報資産のコピーを保持していないことを確認する必要があります。また、それを証明する必要がある場合もあります。
- 個人の資産 — 従業員の個人所有のデバイスから会社のデータやアプリケーションを消去します。また従業員が一部の情報資産（個人の電子メールや連絡先情報など）を保有することを許可される場合もあります。これは有効なポリシーによって異なります。

一部の従業員が離職する際には、ネットワークシステムの安全性を再強化するための追加プロセスが必要となります。例えば、セキュリティシステムや手順に関する詳細な知識を持つ従業員や、共同使用アカウントや汎用アカウント認証情報にアクセスできる従業員などです。これらの認証情報は直ちに変更する必要があります。

セキュリティアカウントの種類と認証情報の管理

オペレーティングシステム、ネットワークアプライアンス、ネットワークディレクトリの製品では、権限管理システムの基盤として、標準的なアカウントの種類が使用されます。これには、一般ユーザーアカウント、管理ユーザーアカウント、セキュリティグループアカウント、サービスアカウントが含まれます。

一般ユーザーには限定的な権限が付与されます。特に、プログラム実行へのアクセスや、自分のプロファイルに属するファイルのみを作成、修正できます。

従業員向けの認証情報管理ポリシー

不適切な認証情報の管理は、ネットワーク脅威アクターにとって最も成功率の高いベクターの1つです。組織がパスワードベースの認証情報に依存し続けなければならない場合、その使用方法を強力なポリシーやトレーニングで管理する必要があります。

パスワードポリシーでは、パスワードの選択と維持に関するベストプラクティスに基づいてユーザーに指示します。より一般的には、認証情報の管理ポリシーは、パスワード、スマートカード、生体認証IDなどの認証方法を安全に保つ方法をユーザに指示する必要があります。パスワード保護ポリシーは、脅威アクターが特定のアカウントを侵害して、ネットワーク上で他の攻撃を実行するリスクを緩和します。また認証情報管理ポリシーでは、さまざまな種類のソーシャルエンジニアリング攻撃をユーザーに警告する必要があります。ユーザーは、フィッシングやファーミングの試行を検知できることが求められます。これによって、セキュアでないサイトや偽装サイトに認証情報を入力することが避けられます。

ゲストアカウント

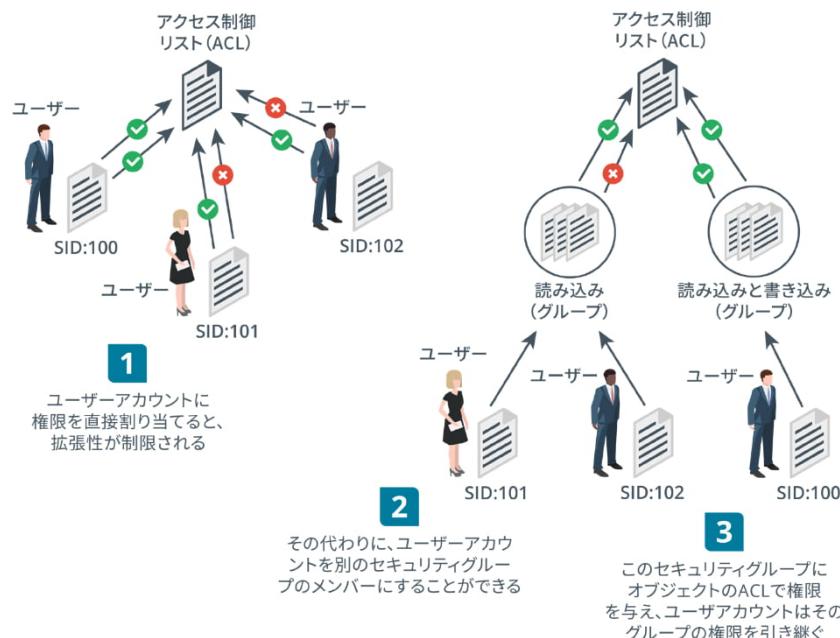
ゲストアカウントは、特別な種類のパスワードのない共有アカウントです。匿名かつ未認証で、リソースへのアクセスを許可するものです。Windows OSはインストール時にゲストユーザーーアカウントとグループアカウントを作成しますが、ゲストユーザーーアカウントはデフォルトで無効にされています。また、Webサーバーの大部分が未認証のアクセスを許可するため、ゲストアカウントはウェブサービスのインストール時にも作成されます。

セキュリティグループベースの権限

ローカルコンピューター上のリソースを使用する際のアカウントと同様に、ユーザーがネットワーク上のリソースを使用する際も通常はアカウントが必要となります。実際、大部分のアカウントはネットワークディレクトリで作成され、その後に特定のコンピューターやワークステーションにログインする権限を与えられます。

ネットワーク権限管理のアプローチの1つとして、ユーザーーアカウントに権限を直接割り振る方法があります。この方法は、ユーザー数が少ない場合にのみ用いることができます。ユーザー数が多い場合は、監査や一貫した権限ポリシーの適用が難しくなります。

セキュリティグループアカウントのコンセプトとは、権限の割り当ての管理プロセスを単純化し、一元化することです。システムのオーナーは権限を直接割り当てるのではなく、セキュリティグループアカウントごとに権限を割り当てます。ユーザーーアカウントは、セキュリティグループのメンバーになることで権限を取得します。ユーザーは複数のグループのメンバーになることができるため、複数のソースから権限や許可を得ることができます。



セキュリティグループを使用して権限を割り当てます。(画像提供: © 123RF.com)

管理者/ルートアカウント

管理者アカウントや特権アカウントでは、アプリやデバイスドライバーのインストールや削除、システムレベルの設定変更、ファイルシステム内のあらゆる対象へのアクセスが可能です。理想的には、専用に作成されて、特定の権限を割り当てられたアカウントのみがこの種の高次の権限を持つようにすべきです。実際、デフォルト管理者アカウントを削除することは非常に困難です。**デフォルトアカウント**とは、オペレーティングシステムやアプリケーションをインストールする際に作成されるアカウントです。このデフォルトアカウントにはあらゆる権限が付与されます。WindowsではAdministrator、Linuxではrootと呼ばれています。また、このタイプのアカウントは、スーパーユーザーアカウントとも呼ばれます。

汎用管理者アカウントの管理

スーパーユーザーアカウントは、最小限の特権の原則と職務分掌の原則に矛盾するものです。そのため、通常の状況ではスーパーユーザーアカウントによるログインを禁止すべきです。デフォルトのスーパーユーザーアカウントは、障害復旧作業での使用に制限する必要があります。通常Windowsでは、このアカウントはデフォルトで無効となっており、グループポリシーを使用してさらに制限することができます(docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-h--securing-local-administrator-accounts-and-groups)。ただし、セットアップ時に作成される最初のユーザー アカウントにはスーパーユーザー権限があります。



Windowsネットワークでは、ローカル管理者とドメイン管理者を見分ける必要があります。ローカル管理者の権限の範囲は、そのアカウントをホストする機器に制限されます。ドメイン管理者は、ドメインに参加しているあらゆる機器に対する権限を持ちます。

Ubuntu Linuxでも同様の方法を採用しています。ルート(root)アカウントはパスワードなしで構成されてロックされ、ログインが防止されます。別のスーパーユーザーアカウントがセットアップ時に作成されます。その他のLinuxディストリビューションでは、通常、インストール時にパスワードが設定されます。このパスワードは可能な限り安全に保管する必要があります。

管理者の認証情報に関するポリシー

デフォルトのスーパーユーザーは、所定の職務に対して十分な権限を持つ1つ以上の名前付きアカウントに置き換える必要があります。これは、汎用アカウントの禁止とも言えます。管理者の活動を監査することができ、システム全体が否認防止の特性に従うことを意味します。



管理アカウントの数を可能な限り制限することが望まれます。アカウントが多いほど、そのうちの1つが危険にさらされる可能性が高まります。一方で、管理者がアカウントを共有することは、説明追跡性を脅かすことになるので避けたいものです。

管理者権限を持つユーザーは、認証情報管理に最大の注意を払わなければなりません。特権アクセスアカウントには強力なパスワードを使用し、多要素認証(MFA)を使用することが理想的です。

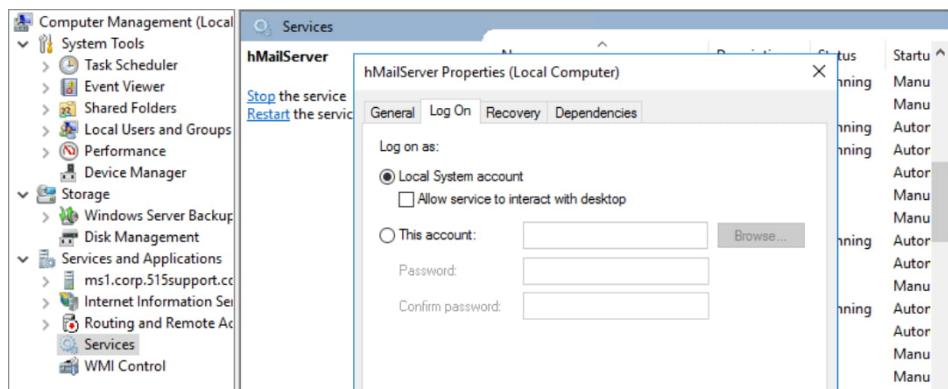
デフォルトセキュリティグループ

ほとんどのオペレーティングシステムでは、デフォルトでセキュリティグループも作成され、これにはデフォルトで一連の権限が与えられます。Windowsでは、権限が直接ユーザー アカウントに割り当てられるのではなく、ローカルグループアカウント（ユーザーと管理者のグループ）に割り当てられます。異なる権限を持つセキュリティグループをカスタマイズして作成することもでき、これによって最小限の特権の原則を強化します。Linuxでは通常、特権アカウントはユーザー アカウントかグループアカウントのいずれかを/etc/sudoersファイルに追加することで設定します(linux.com/training-tutorials/start-fine-tuning-sudo-linux)。

サービスアカウント

サービスアカウントは、スケジュールされたプロセスや、データベースなどのアプリケーションサーバーソフトウェアで使用されます。Windowsには、デフォルトのサービスアカウントが数種類あります。これらは、ユーザーがインターラクティブにログインすることはありません。次のようなプロセスやバックグラウンドサービスの実行に使用されます。

- システム — Windowsアカウントの最上位の特権を持ちます。ローカルシステムアカウントは、ユーザーがログインする前にWindowsを起動するホストプロセスを作成します。このシステムアカウントを使用して作成されたプロセスは、ローカルコンピューターに対する全権限を持ちます。
- ローカルサービス — 一般的なユーザー アカウントと同等の権限を持ちます。匿名のユーザーとしてネットワークのリソースにアクセスすることのみが可能です。
- ネットワークサービス — 一般的なユーザー アカウントと同等の権限を持ちますが、ネットワークのリソースにアクセスする際にはコンピューターのアカウント認証情報を提示します。



Windows Serverで実行するサービスの認証情報の構成。このサービスはローカルシステムアカウントを使用しています。このアカウントには、ローカル管理者の全権限が割り当てられています。
(スクリーンショットはMicrosoftからの許可を得て使用。)

Linuxでも、同様のサービスアカウントのコンセプトを使用して、Webサーバーやデータベースなどのインターラクティブに操作されることがないデーモンプロセスを実行します。通常これらのアカウントは、サーバーアプリケーション用のパッケージマネージャーで作成されます。パスワードを不明の値に設定して、シェルアクセスを否定することで、ユーザーがこれらのアカウントにログインできないようにすることができます。

名前付きアカウントがサービスを実行するように手動で構成される場合、そのサービスアカウントのパスワードは複数の管理者に事実上共有されます。多くのオペレーティングシステムがサービスアカウントの認証情報の自動割り当てを採用しており、インサイダーの脅威のリスクを低減しています(techcommunity.microsoft.com/t5/ask-the-directory-services-team/managed-service-accounts-understanding-implementing-best/ba-p/397009)。



サービスアカウントの使用が適切な場合に個人アカウントを使用するリスクを理解しましょう。あなたが個人アカウントを使用しており、ユーザーが何らかの理由でそのパスワードを変更したりアカウントを無効にした場合、そのサービスは実行できなくなります。これは業務用アプリケーションに深刻な問題をもたらす恐れがあります。

共有/汎用/デバイスアカウントと認証情報

共有アカウントとは、複数の人物がそのパスワード（またはその他の認証情報）を知っているアカウントのことをいいます。一般的に、シンプルなSOHOのネットワークデバイスでは複数のアカウントを作成することができないため、1つの「Admin」アカウントを使用してそのデバイスの管理を行います。このようなアカウントは、デフォルトパスワードを使用して設定される場合があります。その他の例としては、Windowsの「Administrator」や「Guest」、Linuxの「root」のような、デフォルト（または汎用）のOSアカウントや、デフォルトのセキュリティグループに追加されたアカウントなどが挙げられます。また共有アカウントは、臨時スタッフ用に設定することもできます。

共有アカウントは否認防止の原則から外れるもので、正確な監査証跡の確保が困難になります。また、そのアカウントのパスワードが危険にさらされる可能性が高くなります。その他の主なリスクには、アカウントのパスワード変更があります。頻繁なパスワード変更は一般的なポリシーとなっているため、組織はアカウントへのアクセス権を持つ誰もがそのパスワードの変更時期と、新しいパスワードについて必ず理解しているようにする必要があります。このような場合、人数の多いグループにパスワードを通知する必要があるため、この行為自体がセキュリティ上の大きな課題となります。共有アカウントはこれらのリスクを理解し、許容できる場合のみの使用に制限されるべきです。

デバイスの認証情報ポリシー

企業用に設計されたネットワークアプライアンスがデフォルトアカウントを1つだけに制限することはまれです。TACACS+を使用して各自のアカウントと役割ベースの権限をサポートします。デバイスが共有パスワードによってのみしか運用できない場合は、そのデバイスが許可された構成を維持できるように職務分掌を徹底する必要があります。

特権アクセス管理

最新の注意をもって設計された役割ベースの権限を使用したとしても、共有/デバイス/ルートパスワードの使用を完全に無くすことは不可能と言えるでしょう。企業用**特権アクセス管理**製品は、これらのハイリスクの認証情報をスプレッドシート以外の場所に保存し、引き上げられた権限を全般的に監査するソリューションを提供します(gartner.com/reviews/market/privileged-access-management)。

セキュアシェル鍵とサードパーティの認証情報

セキュアシェル(SSH)は広く使用されているリモートアクセスプロトコルです。デバイスやサービスの管理に使用される可能性が非常に高いものです。SSHは2種類の鍵のペアを使用します：

- ホスト鍵のペアでSSHサーバーを特定します。クライアントがそのサーバーに接続した時に、サーバーが公開の部分を開示します。クライアントは何らかの方法で、この公開鍵の有効性を判断しなければなりません。有効な場合、この鍵のペアを使用してネットワーク接続を暗号化し、セッションを開始します。
- ユーザーの鍵のペアは、クライアントがSSHサーバーにログインするための手段です。サーバーはクライアントの公開鍵のコピーを保管します。クライアントは、そのペアである秘密鍵を使用して認証リクエストを生成し、そのリクエスト（秘密鍵ではない）をサーバーに送信します。サーバーがそのクライアントに対する正しい公開鍵を持っている場合のみ、このリクエストが正当と認められます。

SSH鍵は正しく管理されていないことが多く、数多くのセキュリティ侵害に繋がっています。この最も有名な例がソニー・ピクチャーズ・エンタテインメントへのハッキング事件です(ssh.com/malware)。SSH鍵の管理用のベンダーソリューションがあります。また、アイデンティティの検証には、サーバーやクライアントを構成して公開鍵インフラストラクチャ(PKI)と認証局(CA)を使用することもできます。

サードパーティの認証情報は、ベンダーのサービスやクラウドアプリを管理するために企業が使用するものです。管理者のログインと同様に、SSHまたは**アプリケーションプログラミングインターフェイス(API)**を介してホストにアクセスするには、デバイスとサービスにパスワードや暗号化鍵を設定します。コードやスクリプトを平文のまま残すなど、このような情報の不適切な管理が数多くの侵害の原因となっています(nakedsecurity.sophos.com/2019/03/25/thousands-of-coders-are-leaving-their-crown-jewels-exposed-on-github)。

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation pane with options like Dashboard, Access management (with 'Users' selected), Roles, Policies, Identity providers, Account settings, Access reports, and Credential report. The main area is titled 'Summary' for a user named 'Scouter'. It shows the User ARN (arn:aws:iam::605794230193:user/Scouter), Path (/), and Creation time (2020-01-08 10:20 UTC). Below this, there are tabs for Permissions, Groups (1), Tags, Security credentials (which is selected), and Access Advisor. Under 'Sign-in credentials', it lists a Console sign-in link. Under 'Access keys', it shows one active access key with details: Access key ID (redacted), Created (2020-01-08 10:20 UTC), Last used (2020-01-08 ...), and Status (Active). There's also a 'Create access key' button.

Amazon Web Services (AWS)アカウントのセキュリティ認証情報。ユーザーはパスワード認証情報か、スクリプト内のアクセス鍵を使用して認証できます。このアクセス鍵はユーザーのクライアントデバイスにのみ保存され、コンソールを介して回復することはできません。しかし、無効化や削除は可能です。

レビュー アクト ティビティ：

アイデンティティとアカウントタイプ

次の質問にお答えください。

- あなたは、ユーザー認証の新しい方法について、ある会社のコンサルティングをしています。従業員がクラウドプロバイダーでアカウントを作成するとコストを節約でき、多要素認証(MFA)をよりよくサポートできると提案しています。これによって、会社の担当者は認可と権限の管理に注力することができます。このクラウドベンダーはどのような種類のサービスを提供しますか？
- アカウントを正当なユーザーのみに作成すること、適切な権限のみを割り当てる事、正当なユーザーのみにアカウント認証情報を知らせることを確保するプロセスは何ですか？
- ユーザーには必要最低限の権限を割り当てるべきとするポリシーとは何ですか？
- SOPとは何ですか？
- 重要な業務プロセスの監視には2名以上で行うことを定めている組織的ポリシーの種類は何ですか？
- 最近、1週間前に雇用が終了したユーザーのアカウントを脅威アクターが侵害しました。彼らはこのアカウントを使用してネットワークの一部にアクセスし、重要なファイルを削除しました。この攻撃で悪用されたアカウントの脆弱性は何ですか？

7. インタラクティブなログインができないのは、どの種類のアカウントですか？

8. サードパーティの認証情報管理の実施のために監査が最も必要とされるファイルの種類は何ですか？

トピック8B

アカウントポリシーを導入する



対象試験範囲

3.7 与えられたシナリオに基づいて、アイデンティティとアカウント管理制御を実装できる

アカウントポリシーでユーザーができること、できないことを設定することで、特権管理ポリシーを実装します。これによって、強力な認証情報ポリシーを実装でき、侵害されたアカウントによるリスクを検出して管理することができます。監査と権限のレビューを実施して、セキュリティを突破しようとする疑わしい行動や試行をあぶり出します。

アカウント属性とアクセスポリシー

ユーザー認証と同様に、アカウントをユーザープロファイルの属性に基づいて設定することができます。また、アカウントオブジェクトは権限やアクセスポリシーを割り当てる際にも使用できます。

アカウント属性

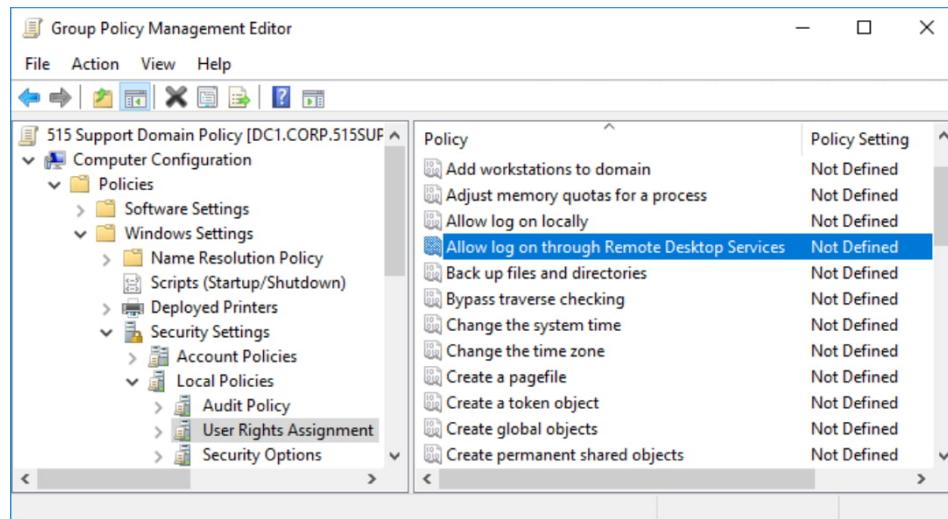
ユーザーアカウントは一意のセキュリティ識別子(SID)、名称、認証情報で定義されます。各アカウントにはプロファイルが紐付けられています。このプロファイルは、ユーザーを説明する個別のアイデンティティの属性（氏名、メールアドレス、連絡先番号、部門など）で定義されます。また、アカウント写真などのメディアにも対応しています。

属性と同様に、プロファイルは通常、ユーザーが作成したデータファイルの保存用のロケーション（ホームフォルダ）を提供します。また、ソフトウェアアプリケーション用のアカウント毎に設定を保存することもできます。

アクセスポリシー

各アカウントには、ファイルや他のネットワークリソースに対する権限、ネットワークホストの使用や構成に対するアクセスポリシーや特権が割り当てられます。これらの権限はアカウントに直接割り当たる場合もあれば、セキュリティグループやロールのメンバーシップを通じて引き継ぐこともあります。アクセスポリシーは、ローカルでまたはリモートデスクトップを介してコンピューターにログインする権限、ソフトウェアをインストールする権限、ネットワーク構成を変更する権限などを決定するものです。

Windows Active Directoryネットワークでは、アクセスポリシーはグループポリシーオブジェクト(GPO)で構成することができます。GPOはユーザー/グループ/ロールアカウントのアクセス権限を設定することもできます。GPOは、Active Directory内にあるネットワーク管理の境界（サイト、ドメイン、組織単位(OU)など）にリンクされています。



Windows Server 2016でグループポリシーオブジェクトを使用したアクセスポリシーと権限の構成。
(スクリーンショットはMicrosoftからの許可を得て使用。)

アカウントパスワードポリシーの設定

システムが実施するアカウントポリシーは、ユーザーが決定するパスワードの要件を次のように規定することで、認証情報管理の原則の実施に役立ちます。

- パスワードの長さ — パスワードの最小の長さを規定します。最大の長さである場合もあります。
- パスワードの複雑さ — パスワードの複雑さに関するルール（パスワードにユーザー名を含めない、大文字/小文字の英数字と英数字以外の文字を組み合わせた少なくとも8文字）を規定します。
- パスワードの使用期限 — 設定した日数を過ぎたら、ユーザーに新しいパスワードを設定するように強制します。
- パスワードの再利用と履歴 — 過去に使用されたことのあるパスワードの使用を防止します。履歴属性では、使用をブロックする過去のパスワードの数を設定します。

この背景として、NISTが発行した最新ガイダンス(nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)では、パスワードポリシーの「伝統的な」要素の一部は現在は使用されていないことに注意する必要があります。

- 複雑さに関するルールは実施すべきではありません。ユーザーには、8～64のASCIIまたはUNICODE文字（スペースを含む）のパスワード（または、記憶できるその他の秘密）の選択を許可するべきです。唯一の制限は、一般的なパスワード（辞書にある文言、文字列の繰り返し（12345678など）、侵害されたパスワードのデータベースに載っている文字列、関連情報（ユーザー名や社名などの繰り返しとなる文字列）を禁止することです。
- 使用期限ポリシーは実施すべきではありません。パスワードを変更すべき場合や時期をユーザーが選択できるようにするべきですが、侵害が検知された場合は、システムがパスワード変更を強制できるようにする必要があります。
- パスワードのヒントは使用すべきではありません。パスワードのヒントとは個人情報（最初に通った学校の名前やペットの名前など）に関する回答を送信することで、アカウントを回復できるようにするものです。



xkcd.com/936の漫画で、パスワードのエントロピーに関するポリシーの効果が描かれています。

パスワードのヒントに代わる方法の1つには、これを第2のパスワードとして扱い、「正直な」回答ではなくランダムかつ記憶可能なフレーズを送信させるものがあります。パスワードのヒントを許可することのリスクは、Adobeのデータ侵害で回復されたデータ(nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder)からも分かります。



仕事のパスワードを他の場所（特定のWebサイトなど）で使用することも「パスワードの再利用」となります。このような行為は「ソフト」ポリシーでしか取り締まることはできません。

アカウント制限

ユーザーセキュリティシステムを侵害するタスクをより困難にするために、アカウント制限を使用します。

位置ベースのポリシー

ユーザーまたはデバイスは、IPアドレス、サブネット、仮想LAN (VLAN)、オーガニゼーションユニット(OU)によって特定される論理的なネットワークロケーションを持ちます。これは、アカウント制限のメカニズムとして使用することができます。例えばユーザー アカウントが、制限されたOU内のサーバーへログインすることを防げます。

またユーザー やデバイスの地理的位置を、位置情報メカニズムを使用して割り出すこともできます。**位置情報**のタイプはさまざまです。

- IPアドレス — 地図上の位置と紐付けられており、登録者によって発表された情報（名称、国、地域、市など）に基づいていますため、正確さには幅があります。登録者は通常、インターネットサービスプロバイダー (ISP)であるため、受け取ることができる位置情報はそのISPの管理するホストのおおよその位置となります。そのISPが広域またはさまざま地理的範囲を対象としている場合、ISPのホストの正確な位置を取得できる可能性は低くなります。GeoIP (maxmind.com/en/geoip-demo)などのソフトウェアライブラリがこのデータのクエリに対応しています。
- 位置情報サービス — OSが使用する方法で、デバイスの地理的位置を算出します。全地球測位システム(GPS)センサーの付いたデバイスは、外出時も非常に正確な位置を報告します。位置情報サービスは基地局やWi-Fi ホットスポットとの三角測量を行うこともでき、GPSに対応していない場合はBluetooth信号でも行えます。

ジオフェンシングとは、所在地に基づいてアクセスリクエストを承認したり、拒否したりすることを意味します。またジオフェンシングは、ユーザーが特定の領域に入った時にデバイスに警告やアドバイスを送信するプッシュ通知にも使用されます。ジオタギングとは、位置に関するメタデータをファイルやデバイスに追加することを意味します。デバイスが適切な場所に維持されるようにするために、資産管理の一環として使用されることがよくあります。

時間ベースの制限

時間ベースのポリシーには主に3種類があります。

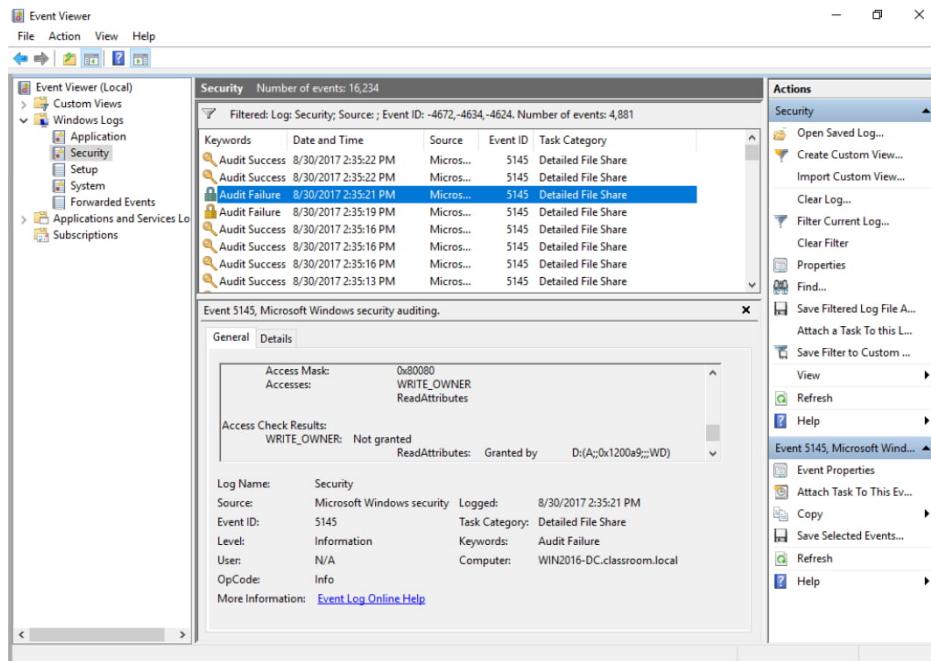
- 時刻のポリシー**では、アカウントに対してログイン時間を承認して指定します。
- 時間ベースのログインポリシーでは、アカウントがログインを継続できる最長の時間を指定します。

- 不可能な移動時間/危険なログインに関するポリシーでは、常にログイン時の位置情報を追跡記録します。これらがしきい値から外れた場合、アカウントが使用できなくなります。例えば、ユーザーがニューヨークにあるデバイスからアカウントにアクセスしたとします。その2~3時間後にロサンゼルスからログインが試行された場合、これは拒否され、警告が出ます。ユーザーがこの両方の場所にいることは不可能なためです。

アカウント監査

アカウント監査のプロセスは、あるアカウントが侵害されたり、悪用されたりしていないことを調査するために使用します。セキュリティログや監査ログは、アカウントの悪用の検出を促進するために次の事項に使用します。

- ユーザーが実施したすべての行動に対するアカウント監査。変更やバージョンを管理する仕組みには、ファイルが変更される時期と変更担当者が明確である必要があります。またアカウント監査は否認防止にも役立ちます（つまり、ユーザーは自分がファイルへアクセスしたことや変更したことを後から否定できません）。この主な問題としては、成功したアクセス試行を監査するために大量のディスク容量が急速に消費されること、ログの分析に長時間かかることが挙げられます。
- 侵入と侵入の試行の検出。ここでは、侵入に成功したイベントも通常とは異なるアクセスパターンを示すかどうかを明らかにできますが、失敗した試行イベントの記録はより有益な情報が得られる可能性があります。

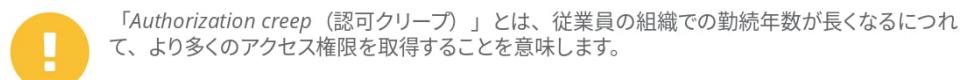


監査対象フォルダのオーナーシップを取得しようとして失敗に終わった試行を記録しています。
(スクリーンショットはMicrosoftからの許可を得て使用。)

またアカウント監査は、より全般的な変更管理を意味します。そのため、リソースやユーザーの変更を考慮する必要があります。リソースが更新やアーカイブされた、またはそのクリアランスレベルが変更された場合や、ユーザーの退職、追加、職務（ロール）の変更があった場合などです。例えば、ユーザーが新しい職務に異動した場合、これまでの権限を取消し、新たな権限を付与する必要があります。このプロセスを再証明(recertification)といいます。これらの種類の変更を効果的かつセキュアに管理するには、効果的な標準業務手順書(SOP)と、部門間（例えばIT部門と人事部門など）の明確でタイムリーなコミュニケーションが必要です。

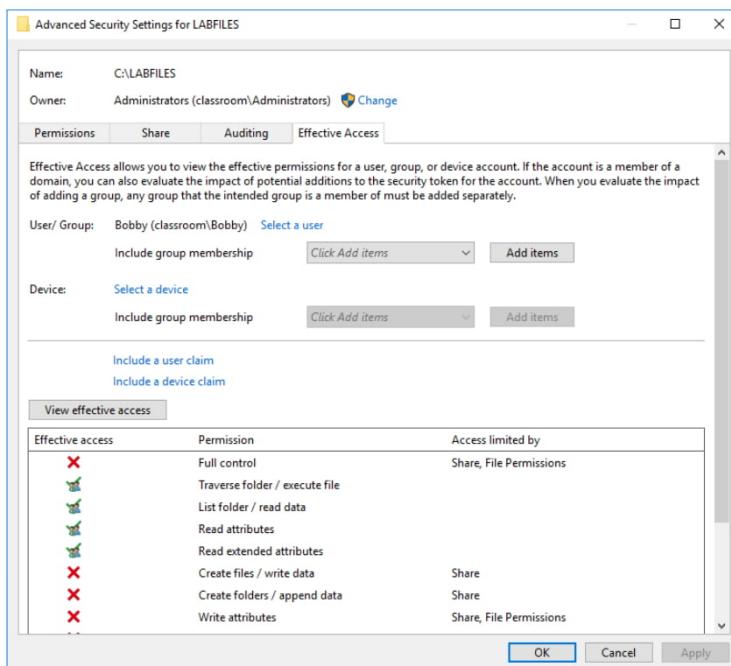
アカウント権限

多くのユーザー、グループ、ロール、リソースが関わっている場合、アカウント権限の管理は複雑で時間がかかるものになります。アカウントが不適切に構成されると、2種類の異なる影響が生じます。1つ目は権限に厳しすぎる制限を設定した場合で、これによって多くのサポートが必要となり、生産性が低下してしまいます。2つ目は権限をユーザーに過度に付与した場合で、これによってシステムのセキュリティが弱まり、マルウェア感染やデータ侵害などのリスクが高まります。



ユーザーは、一時的に高められた権限を付与される場合があります（エスカレーション）。この場合は、合意した期間の終了時にその権限が確実に取り消されるようにシステムを配備する必要があります。

監査システムを配備して、権限を定期的に見直す必要があります。監査には、グループのメンバーシップの監視、各リソースに対するアクセス制御リストの見直しに加え、不要なアカウントの特定や無効化の実施が含まれます。



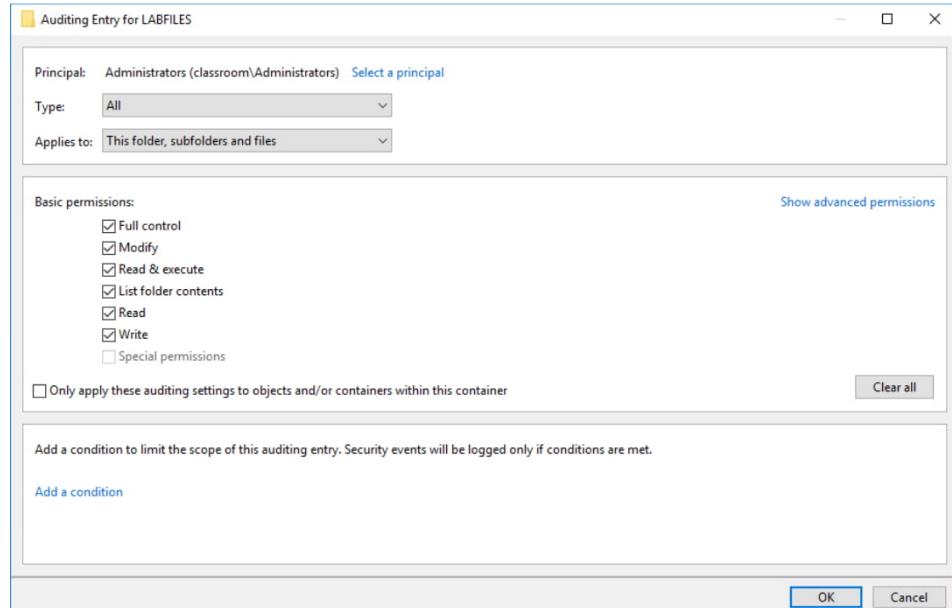
共有フォルダへの効果的な権限の決定。
(スクリーンショットはMicrosoftからの許可を得て使用。)

使用状況の監査

使用状況の監査とは、セキュリティログを構成して主なインジケーターを記録し、疑わしい活動についてそのログを確認することを意味します。ログ内容の決定は、ネットワーク管理者が直面する最も重要な課題の1つです。Active Directoryでは、基本的な要件と、より強固なセキュリティが必要なネットワークのための要件について、Microsoftが監査ポリシーの推奨事項を発表しています(docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations)。

ログ内容の典型的なカテゴリーには以下があります。

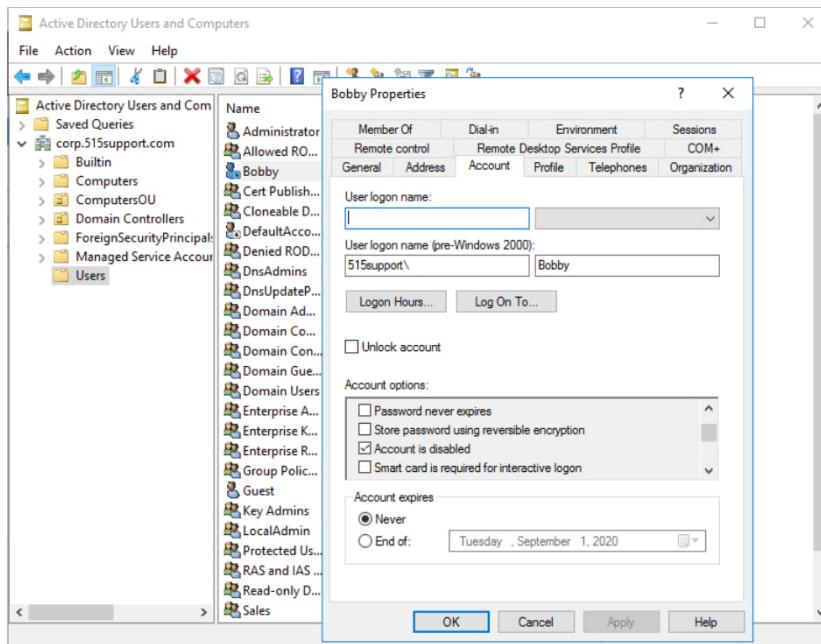
- アカウントのログインイベントや管理イベント
- プロセスの作成
- オブジェクトへのアクセス（ファイルシステム/ファイル共有）
- 監査ポリシーの変更
- システムセキュリティと完全性への変更（アンチウイルス、ホストファイアウォールなど）



Windowsのフォルダの監査エントリの構成。（スクリーンショットはMicrosoftからの許可を得て使用。）

アカウントの無効化とロックアウト

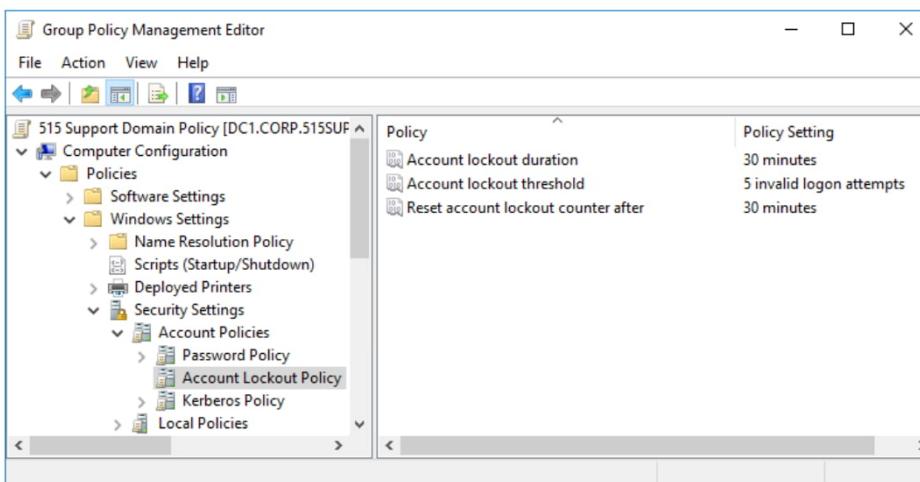
アカウントの悪用が検出されたり、その疑いがある場合、アカウントプロパティを設定することでそのアカウントを手動で無効にすることができます。これによって、そのアカウントがログインに使用されることを防ぎます。ただし、アカウントを無効にした場合でも、実行中のセッションは終了していないことに注意してください。セッションを終了するには、リモートでログオフのコマンドを発行します。アカウントの無効化とは、管理者がそのアカウントを手動で再度有効にするまで、恒久的にログインできなくなる状況を意味します。



アカウントを無効にするプロパティの設定。(スクリーンショットはMicrosoftからの許可を得て使用。)

アカウントのロックアウトとは、一定期間ログインできなくなる状況を意味します。ロックアウトはポリシー違反が検出された場合に手動で実施されることがあります、次のような場合は自動的に適用されます。

- 正しくないアカウントパスワードが繰り返し入力された場合
- アカウントの有効期限が設定されていた場合**アカウント有効期限**を設定したアカウントは、その期日を過ぎると使用できなくなります。このオプションは、臨時スタッフや契約スタッフ用のアカウントとして有用です。
- 時間ベースまたは場所ベースの制限を使用する場合、サーバーはユーザーが継続してネットワークを使用する権限があるかどうかを定期的に確認します。ユーザーにその権限がない場合は、自動ログアウト手順が開始されます。



アカウントロックアウトポリシーの構成。(スクリーンショットはMicrosoftからの許可を得て使用。)

レビュー アカウントポリシー：

アカウントポリシー

次の質問にお答えください。

1. 同じドメイン内のオブジェクトのサブセットに対して異なるセキュリティポリシーを適用する場合、どのような仕組みを使用しますか？
2. ユーザーに毎月パスワードを変更させることが生産的ではないとされる理由は何ですか？
3. ユーザーに以前のパスワードを再使用させないポリシーを何といいますか？
4. IPアドレスをコンテキストベースの認証に使用できる2つの方法とは何ですか？
5. アカウンティングはどのように否認防止として機能しますか？
6. 使用状況の監査を実施する必要があるのはどの情報リソースですか？
7. アカウントのロックアウトと無効化の違いは何ですか？

トピック8C

認可ソリューションの実施



対象試験範囲

- 2.4認証と認可の設計コンセプトを要約することができる
- 3.8与えられたシナリオに基づいて、認証と認可のソリューションを導入することができる
- 4.1与えられたシナリオに基づいて、適切なツールを利用して組織のセキュリティを評価することができます (chmodのみ)

効果的な認可ソリューションシステムを実装するには、そのようなシステムの基盤となるさまざまなモデルを理解する必要があります。オンプレミスのネットワークではアカウントと権限の管理にローカルディレクトリを使用できますが、組織はサービスをクラウドへ移行していることから、フェデレーションID管理ソリューションを使用してこれらの認可を行う必要があります。

任意アクセス制御とロールベースのアクセス制御

セキュリティシステムを設計する際の重要な検討事項として、ユーザーが権利や**権限**を受け取る方法を決定することがあります。このさまざまなモデルは、アクセス制御スキームと呼ばれています。

任意アクセス制御(DAC)

任意アクセス制御(DAC)とは、リソースのオーナーに任せる方法です。オーナーとはファイルやサービスの最初の作成者で、所有権が他のユーザーに割り当てられていることもあります。オーナーにはリソースに対するフルコントロール許可が付与されており、これはオーナーがアクセス制御リスト(ACL)を修正して権利を他者に付与できることを意味します。

DACは最も柔軟なモデルで、現在コンピューターやネットワークのセキュリティに広く実装されています。ファイルシステムのセキュリティについては、これは大部分のUNIX/Linuxディストリビューションでデフォルトとなっており、Microsoft Windowsでも使用されているモデルです。ただし、最も柔軟性が高いモデルですが、一元管理されているセキュリティポリシーを徹底するのが難しいため、最も脆弱なモデルもあります。また、侵害が最も簡単もあります。インサイダーの脅威や侵害されたアカウントの悪用に対して脆弱なためです。

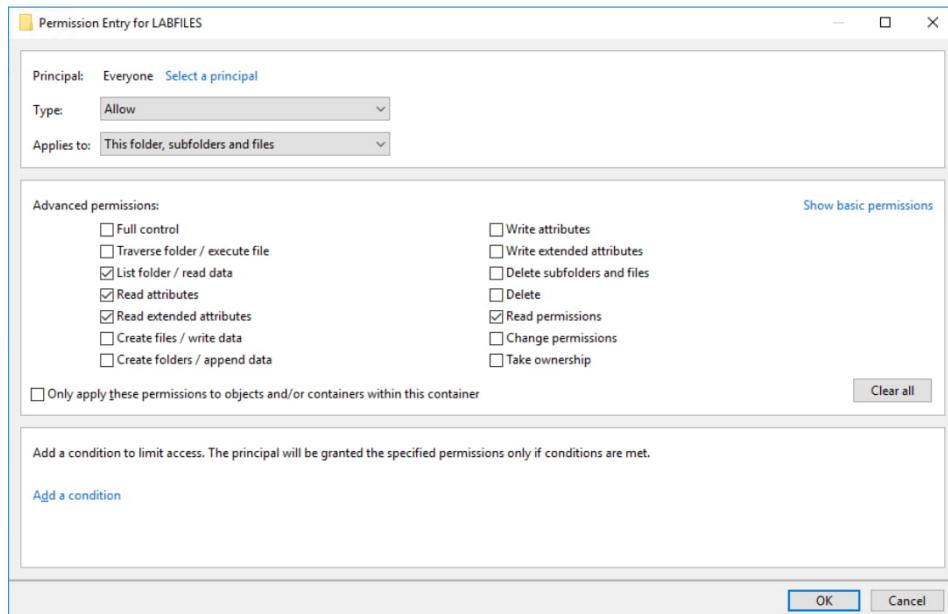
ロールベースアクセス制御(RBAC)

ロールベースアクセス制御(RBAC)は、DACモデルに集中管理型の制御を追加したものです。RBACでは、一連の組織単位のロールが定義され、それらのロールに主体が割り当てられます。このシステムでは、ロールを変更する権限はシステムオーナーが維持します。そのためこのシステムは強制であり、各主体のアカウントにはリソースのACLを変更する権限はありません。ただし、別の方でリソースを変更できる場合があるかもしれません。ユーザーは明示的に権限を直接割り当てられるのではなく、ロールを割り当てられることで默示的に権限を取得します。

RBACはセキュリティグループアカウントの使用を介して部分的に実装することも可能ですが、全く同じスキームにはなりません。セキュリティグループのメンバーシップはその大部分が任意によるものです（システムが決定したのではなく、管理者によって割り当てられます）。また理想としては、主体はロールの権限を永続的に保持するのではなく、特定のタスクを完了するために引き継ぐのみとすべきです。

ファイルシステムの権限

アクセス制御モデルは、あらゆる種類のデータやソフトウェアリソースに適用することができますが、最も親和性が高いのはネットワーク、ファイルシステム、データベースセキュリティです。ファイルシステムセキュリティでは、ファイルシステムの各オブジェクトにはそれに伴うACLがあります。ACLにはリソースへのアクセスを許可されたアカウント（プリンシパル）と、それらのリソースに対する権限のリストが含まれています。ACLの各レコードはアクセス制御エントリ(ACE)と呼ばれます。ACL内のACEの順序は、所定のアカウントの効果的な権限の決定に大切です。ACLは、権限をサポートするファイルシステム(NTFS、ext3/ext4、ZFS)によって実施されます。



フォルダのアクセス制御エントリの構成。(スクリーンショットはMicrosoftからの許可を得て使用。)

例えば、Linuxには3つの基本権限があります。

- 読み取り(r) — ファイルのコンテンツにアクセスして表示します。また、ディレクトリのコンテンツを一覧表示します。
- 書き込み(w) — ファイルへの変更を保存します。また、ディレクトリ内でファイル作成、ファイル名の変更、ファイル削除を行います（実行の権限も必要です）。
- 実行(x) — スクリプト、プログラム、その他ソフトウェアファイルを実行します。また、ディレクトリへアクセスしたり、そのディレクトリからファイルを実行したり、そのディレクトリでファイル検索などのタスクを実行します。

これらの権限は、オーナーユーザー(u)、グループアカウント(g)、その他すべてのユーザー/ワールド(o)のコンテキストに適用できます。権限の文字列には、以下のコンテキストのそれぞれに付与される権限の一覧が表示されます。

```
d rwx r-x r-x home
```

上記の文字列は、ディレクトリ(d)について、オーナーに読み取り、書き込み、実行の権限があり、オーナーの所属グループとその他のユーザーには読み取りと実行の権限があることを表します。

chmodコマンドは、権限を修正する際に使用します。シンボリックモードまたは絶対モードで使用します。シンボリックモードではこのコマンドは次のようにになります。

```
chmod g+w, o-x home
```