BeyondTrust

The Guide to Just-In-Time Privileged Access Management

ジャストインタイム（JIT）の特権アクセス管理（PAM）ガイド

その詳細と必要な理由、
そしてどのように導入すべきか

目次

はじめに

「必要十分」なアクセスを、もう一段階上へ ・・・ 1

JIT PAMの概要

ジャストインタイム(JIT)の特権アクセス管理とは ・・・ 2

JIT PAMの自動化

JITの方式 ・・・ 3

JITのトリガー ・・・ 4

JITのポリシー ・・・ 5

実際のJIT PAM ・・・ 6

BeyondTrustとJIT PAM

BeyondTrustのソリューションはジャストインタイムの特権アクセス管理をどう実現するか ・・・ 7

JIT方式とトリガーのマッピング ・・・ 10

JIT PAMの実装を一歩進めて、サイバーリスクを減らす ・・・ 11

用語集

関連のコンセプトと方法論 ・・・ 12

はじめに

「必要十分」なアクセスを、もう一段階上へ

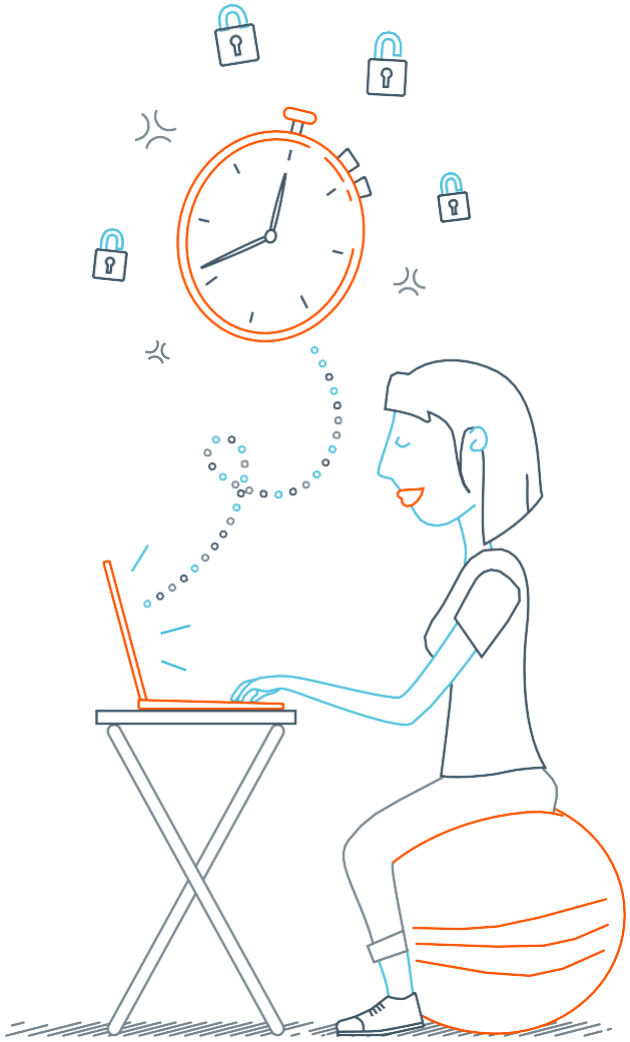
真の意味での最小権限の原則のセキュリティモデルを実現するには、ユーザや処理、アプリケーション、システムなどがタスクを実行するのに「必要十分」な権利を持って――必要な時間の間だけ――アクセスすることが必要です。

組織は特権アクセス管理（PAM）ソリューションを使って、「必要十分」なアクセス手段を効果的に使えるようにしていても、特権ユーザアカウントに関する方程式の中で、期間を限定する部分やリスク評価の部分については、ほぼ無視してきました。

これまでの40年間、管理者アクセスについては「常にオンである」特権アカウントが当たり前の状態であり企業全体に浸透していましたが、これは大きなリスク要因でした。常に有効な状態であるである特権アクセスや権限、許可などは、常時利用可能であるということであり、それは正当な操作と同様に、不当な目的の場合でも同じように使われるのです。そしてこのリスク要因は、仮想、クラウド、DevOpsの環境、モノのインターネット（IoT）デバイスの拡大につれ、ロボットによる業務自動化（RPA）のような新たな分野でも、急速に広がっています。

この背景に照らせば、今日のサイバーセキュリティ侵入事象のほぼ全てにおいて、特権の悪用や濫用が何らかの役割を演じているというのは、何ら驚くべきことではありません。特権アクセスを手にした攻撃者は実質的に悪意の内部者となり、これは、管理職レベルや取締役レベルまであらゆるIT専門家にとって警戒すべき事態です。

特権アカウントはいまや、組織のあらゆるところに存在していますが、従来の水際で食い止める方式のセキュリティ技術では、その境界線の内側でのみ特権アカウントを保護することしかできません。ジャストインタイム（JIT）の特権アクセス管理（PAM）は、企業全体で特権アクセスの脅威にさらされる面を劇的に圧縮し、リスクの低減に役立ちます。JIT PAMを導入するということは、必要な場合に、必要な最短の期間のみ、適切な特権をIDが与えられるということを意味します。このプロセスは完全に自動化されているので、エンドユーザに干渉せず、意識されることもありません。



組織は特権アクセス管理（PAM）ソリューションを使って、「必要十分」なアクセス手段を効果的に使えるようにしていても、特権ユーザアカウントに関する方程式の中で、期間を限定する部分やリスクの部分については、ほぼ無視してきた。

JIT PAMの概要

ジャストインタイムの特権アクセス管理とは何か

ジャストインタイム（JIT）の特権アクセス管理（PAM）は、特権アカウントの利用に対するリアルタイムのリクエストを、権限付与、ワークフロー、適切なアクセスポリシーなどと直接結びつける戦略です。企業はこの戦略を使い、振る舞いやコンテクスト（状況、p6参照）などのパラメータに基づいた時間的な制約を強制的に実施することによって、継続的で常に有効状態のアクセスが持つ欠点から特権アカウントを守るのです。

特権アカウントとは、標準ユーザよりも高い特権や許可を与えられているアカウントと定義されており、以下のようなものがあります。

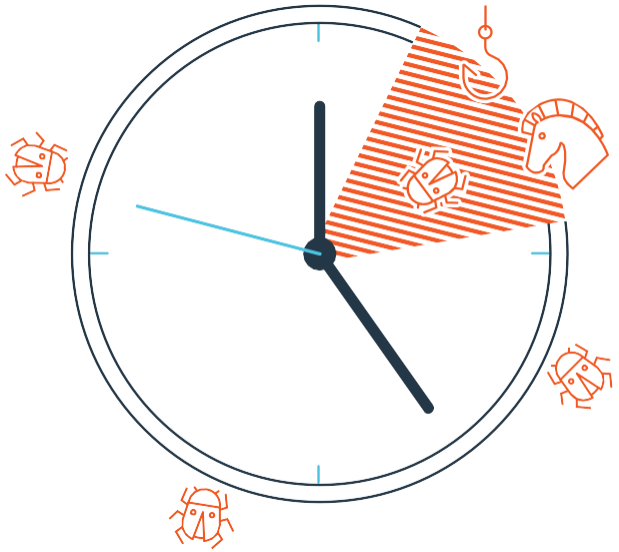
- 管理者（Windows環境において）やroot（Unix/Linux環境において）のように、非常に大きな特権を持つスーパーユーザアカウント
- スーパーユーザと標準ユーザのアカウントの間に当たる特権を持つパワーユーザ（非特権または最小限特権のユーザアカウントとも呼ばれます）

JIT PAMは、あるアカウントが昇格した特権とアクセス権を与えられる期間を厳しく限定することで、その期間以外で脅威の実行者がアカウント特権を悪用してしまう脆弱性の侵入口を、大幅に減らすことができるのです。JITは最小権限の原則を強制的に施行して、承認された使用ポリシーに沿って特権行為使用が行われるようにし、正規のコンテクスト以外の特権行為を防ぐのに役立ちます。

特権をリクエストするとき、その特権がチェックアウトの前に必要なコンテクストのパラメータの条件を満たしていなければなりません――その特権がアカウントに所有されてはならないのです。そうすれば、特権アクセス管理が導入されていない場所で利用されることがあったとしても、悪用のリスクが軽減されます。特権アカウントは実質的に、乱用に対して完全武装で対処しているわけではありません。

例として――週に168時間「特権がアクティブ」となっている、典型的な常時オンの特権アカウントについて考えてみましょう。JIT PAM手法に変えれば、特権アクティブの状態を168時間からたった24分に減らすことができます。組織内のすべての特権ユーザアカウントでこの効果をかけ合わせれば、リスクの軽減には莫大な影響があります。

特権管理方式の一部としてJITを取り入れれば、真の意味で最小権限の原則モデルを企業規模で導入できるということになります。それに、侵害リスクは時間の見に基づいているだけではありません。リソースを通じて利用できる「常時オン」の特権アカウントがなければ、横方向への攻撃のような手法を利用する攻撃ベクトルも減らすことができます。



企業はこの戦略を使い、振る舞いやコンテクスト（状況、p6参照）などのパラメータに基づいた時間的な制約を強制的に実施することによって、継続的で常に有効状態のアクセスが持つ欠点から特権アカウントを守る

JIT PAMの自動化

JITの方式

JITの特権管理の手法には、組織がジャストインタイム（JIT）の特権アクセスのための基準を設定し、このポリシーの範囲内にあるアカウントは、起こりうる緊急アクセスの事態目的の他は使えない前提であると理解する必要があります。

きちんと設定されたJITに類似した概念は、製造など他の分野でも存在しますが、セキュリティや運用のソリューションにこのモデルを応用するときには、導入の際に独特の技術的な検討事項が発生します。

JIT特権アカウントの目的は、承認されたタスクや作業に応じて、必要な特権を「その場で」自動的に割り当て、続いて、そのタスクが完了した後、または認定されたアクセスのウィンドウやコンテクストの期限が切れた後で、これを削除することです。

標準のユーザアカウントを取得し、適切な特権を施すのに必要なモデル化は、次の6種のJIT方式のいずれかを使って実施することができます。

1 JIT特権

この方式では、アカウントには全ての基準を満たせば、個別に権限や許可、資格などが追加されますが、限られた期間のみです。こうした権利類は、業務が完了したら無効にする必要があり、他の特権が不当に変更されないという証明が記載されていなければなりません。

2 JITアカウントの作成 & 削除

この方式では、業務目的に合った適切な特権アカウントの作成と削除をします。このアカウントには、ログや調査のため、リクエストしているIDや、操作を実行する証跡記録が紐づけされる必要があります。

3 JITの「なりすまし」

この方式では、アカウントを予め存在する管理者アカウントとリンクさせて、特殊なアプリケーションやタスクを実行する場合に、証を経て昇格させます。これは一般的に、自動処理やWindowsの「RunAs」、「*Nix SuDo」のスクリプトで行われます。通常、エンドユーザはこの手の動作をする「なりすまし」アカウントとは意識せず、この処理は、常時オンの特権アカウントの移譲と特徴が重なります。

4 JITのトークン化

この方式は、アプリケーションまたはリソースには、OSのカーネルに読み込ませる前に改編できる特権トークンを利用します。この形態の最小権限は、エンドユーザの特権を昇格させずにアプリケーションの特権と優先順位を上げることができるため、主にエンドポイントで使われます。

5 JITのグループ・メンバーシップ

この方式では、アカウントを管理者グループに必要な操作の間、自動で追加したり、削除したりします。このアカウントは、適切な基準が満たされた場合にのみ、昇格グループに追加されるべきです。グループメンバーシップは、業務の完了次第、ただちに無効にしなければなりません。

6 無効化された管理者アカウントJIT

この方式では、ある機能を実行する全ての許可、特権、資格をもつ、無効化された管理者アカウントがシステム上に存在します。これらは特定の処理の実行する際に有効となり、その後、操作基準が満たされれば再び無効になります。この概念は、常にオンである管理者アカウントを持つというのと本来の実行可能機能がJITのアクセス制御に利用されるという点以外は変わりはありません。

JITのトリガー

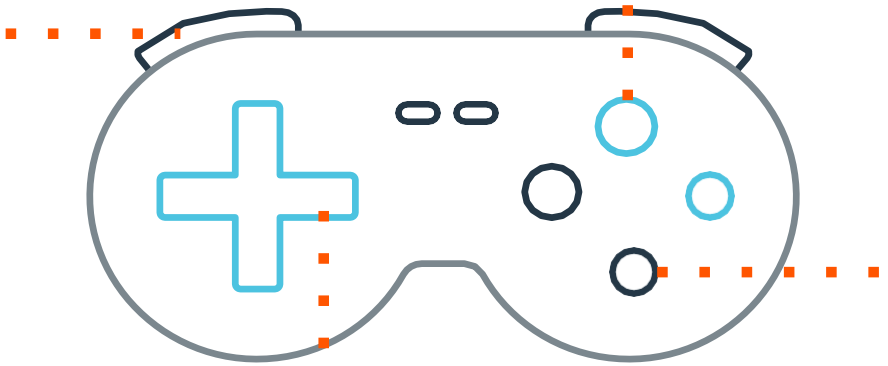
各種の特権アカウント昇格方式が、ジャストインタイム（JIT）の特権アクセス管理の原則に沿って動作させるためには、以下のような基準をトリガーとみなす必要があります。これにはまた、変更制御の枠のための時間や日付といった変数、侵害を示す値や検出された場合の中断や終了の基準も含まれている必要があります。

二要素認証（2FA）または多要素認証（MFA）

常時オンのアカウントまたはJIT特権アカウントへの特権アクセスを承認するための一般的な方法は、2FAかMFAです。これによって2つのアクセス方法の間に差は生じませんが、そのIDが特権アカウントに対して正しいアクセスができることを確認できるため、余計なリスクの回避につながります。こうした認証方式は、上記に挙げた方式のいずれかを使ったアカウントのJITトリガーとして使うことができます。

ワークフロー

ワークフロー承認の概念は一般的に、コールセンターやヘルプデスクその他の情報技術サービス管理（ITSM）ソリューションと結びついています。アクセスへのリクエストが行われると、所定の承認ワークフローを使って許諾されるか却下されます。そのワークフローが承認を受けると、JITアカウントが有効になります。これは通常、変更管理やヘルプデスクのソリューションにおけるユーザや資産、アプリケーション、時間／日付、関連のチケットなどと対応しています。特権セッションモニタリングは通常、この流れでPAMソリューションによって有効となっており、対応する全ての動作が適切であることを検証します。



コンテクスト認識

コンテクスト認識式のアクセスは、アクセス元のIPアドレス、位置情報、所属グループ、ホストのOS、インストールされていたり実行しているアプリケーション、文書化された脆弱性などの基準に基づいています。これらの特徴を論理的に組み合わせ、それに基づいて、ビジネス要件を満たしたり、リスクを回避するために、JITアカウントのアクセスが許諾されたり却下されたりするのです。

権限付与

特権アクセス管理（PAM）がIDアクセス管理（IAM）ソリューションと統合されると、ソリューション間の権限付与が特権アクセス目的で同期されます。この目的でPAMソリューションから直接かIAM付与経由でプログラム的にJITアクセスが付与されます。典型的なIAM付与ワークフローの同期プロセスは時間がかかるかリアルタイムではありませんが、特権に基づくアカウント認証の経路の役目はします。しかしIAMとPAMソリューションがアクセス制御でリンクされるとこの要素は効力がなくなる可能性もあります。

JITの自動化トリガーは、あるアカウントが特権アクセスに備えた状態になるための条件である

JITのポリシー

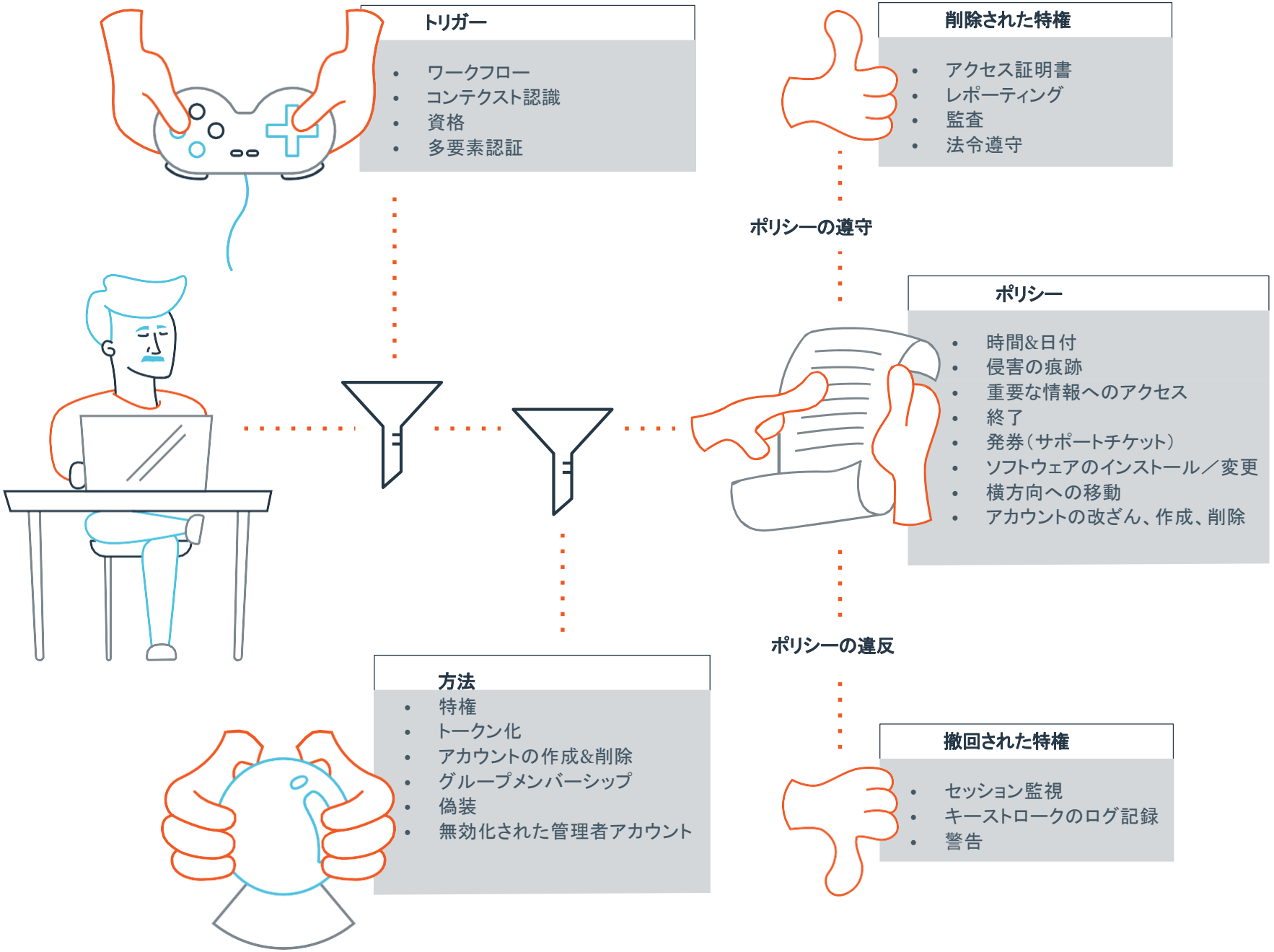
ITチームが考慮する必要がある二つの重要な点は、「正しい特権アクセスのために、JITアカウントを制御するポリシーは何か」そして、「特権アクセスを取り消すには、どのような条件を満たさねばならないか」ということです。

このポリシーには、次のようなものがあります。

1. **アクセスと変更管理のための時間と日付の設定枠**
2. **侵害の痕跡となるコマンドかアプリケーション**
3. **重要な情報へのアクセスの検出**
4. **プライマリセッションの終了**
5. **サポートチケットシステムのソリューションで対応する付属物があること**
6. **ソフトウェアのインストールやファイルの改ざんなど、リソースの不当な変更**
7. **横方向への不審な移動の試み**
8. **ユーザアカウントやデータセットの改ざん、作成、削除**

これは決して、ポリシーの変数をすべて網羅したリストではありませんが、対応するトリガーに基づいて有効にすべき、または終了すべきJITアカウントの基準をふるい分けるのには役立ちます。

実際のJIT PAM


トリガー
ワークフロー
コンテクスト認識
資格
多要素認証
削除された特権
アクセス証明書
レポーティング
監査
法令遵守
ポリシーの遵守
ポリシー
時間&日付
侵害の痕跡
重要な情報へのアクセス
終了
発券（サポートチケット）
ソフトウェアのインストール／変更
横方向への移動
アカウントの改ざん、作成、削除
ポリシーの違反
方法
特権
トークン化
アカウントの作成&削除
グループメンバーシップ
偽装
無効化された管理者アカウント
撤回された特権
セッション監視
キーストロークのログ記録
警告

BeyondTrustのソリューションはいかにしてジャストインタイム（JIT）の特権アクセス管理（PAM）を実現するか

BeyondTrust Privileged Access Management プラットフォームを使うと、JIT PAMセキュリティモデルが組織にとって現実のものとなり、さらに特権アカウントの検索や管理、最小権限、証明書管理、特権の分離と責任の分担、特権監査、特権脅威分析など、お客様のIAM/PAM戦略にとって重要な他の要素も強制的に実行されることで、セキュリティの強化に役立ちます。

BeyondTrustは、様々なトリガーを使い、エンドポイント（デスクトップ、サーバその他）でもリモートアクセス（従業員やベンダーなど）でも、特権ログイン情報（パスワード）やセッション、特権の昇格／移譲などの一元集中管理を可能にすることで、ジャストインタイム（JIT）のモデルをサポートします。BeyondTrustのPAMプラットフォームには統合されたソリューションが複数含まれています。

BeyondTrustは、様々なトリガーを使い、エンドポイントでもリモートアクセスでも、特権ログイン情報（ID/パスワード）やセッション、特権の昇格／移譲などの一元集中管理を可能にすることで、ジャストインタイムのモデルをサポートする

BeyondTrustソリューション	JIT PAMを支援する特徴と機能					
Privileged Password & Session Management	**継続的で自動化されたアカウントの発見&自動登録**	**セキュアなSSH鍵管理**	**アプリケーション間のパスワード管理**	**強化された特権セッション管理**	**適応性のあるアクセス制御**	**特権に関する高度な脅威分析**
あらゆる種類の特権アカウントを発見し、管理し、監査し、監視する	分散型ネットワーク検索エンジンを利用して、全ての資産をスキャンし、特定し、プロファイルする。動的なカテゴリー化でスマートグループに自動登録し、新しいアカウントが検出された際に、効率的な管理とJITアクセスを実現する。	決められたスケジュールに従って、自動的にSSH鍵を変更、きめ細かなアクセス制御とワークフローを強制実行する。プライベート鍵を利用して、ユーザを鍵に紐づけることなく、また特権セッションを全て記録して、プロキシ経由でUnix/Linuxに安全にユーザをログオンさせる。	拡張性と冗長性を持たせるために無制限の数のパスワードキャッシュを含む適応型のAPIインタフェースを使い、ハードコードされた、または組み込まれたアプリケーションの証明書を削除する。これによって、どのアプリケーションの最新パスワードでもJITのアクセスができるようになる	ライブセッション管理によって、真の意味での二重制御ができ、しかも管理者はセッションや生産性を犠牲にすることなく、JIT動作に基づいて疑わしい振る舞いの記録やロックすることやレポート化ができる	ユーザがシステムにアクセスする承認について判断するためにリソースにアクセスする際、日付や曜日、時刻、場所などを考慮することによって、ジャストインタイムのコンテクスト(状況)を評価し、アクセスリクエストを単純化することができる	ある日から翌日までの資産の特徴やユーザの振る舞いを測定し、変更の範囲や速度を評価して、疑わしい差異があれば警告を発する
Endpoint Privilege Management	**最小権限の強制実行**	**切れ目のないアプリケーション制御**	**完全な監査とレポーティング**	特権脅威分析	**セキュリティエコシステムの統合**	
WindowsやMac、Unix、Linux、ネットワークデバイスで最小権限を強制的に実施し、過剰なエンドユーザ特権を取り除く	きめ細かなポリシーに基づいた制御により、ジャストインタイムでタスクを完了するのに必要十分なアクセスを許可しながら、OSの一般ユーザのためにアプリケーションへの特権を昇格させる	アプリケーションの信頼に基づいたホワイトリスト、ブラックリスト、グレイリストなどを、柔軟なポリシーエンジンで作成して幅広い規則を設定する。特権ユーザには自動承認を選択し—完全な監査証跡によって保護される—、JITのアプリケーション制御のために誰、何・応答式のコードを利用する。	全てのユーザ動作について単一で完全な履歴が取れるので、調査分析を迅速に行い、コンプライアンスも簡単に行える	最適なセキュリティソリューションから得られた資産の脆弱性データやセキュリティ情報とユーザの振る舞いを関連づけ、エンドユーザのリスクについて全体像を見られるようにする	ヘルプデスクアプリケーション、脆弱性管理スキャナ、SIEMツールなど、サードパーティソリューションのホストへの組み込み式コネクタを提供し、組織が既存のセキュリティへの投資に対するリターンを得られるようにする	

BeyondTrustソリューション		JIT PAMを支援する特徴と機能					
Secure Remote Access	リモートベンダーとサードパーティのアクセス	**特権アクセス制御**	**セッション監視**	**攻撃対象面の削減**	**パスワード管理との統合**	**モバイル&ウェブのコンソール**	**監査&コンプライアンス**
ベンダーや内部のリモート特権アクセスを保護、管理、監査し、リモートシステムにアクセスしてサポートする		ユーザに対してリモートセッションへの適正なアクセスを与えることによって最小権限を強制実行する	RDP、VNC、HTTP/S、SSH接続用の標準プロトコルを使って、セッションを制御し監視する	1か所かつジャストインタイムで、特権アカウントのトラッキング、承認、監査を統合し、単独のアクセス経路を作ることによって、攻撃面を減らす	クリックひとつ、ジャストインタイムで、サーバやシステムに直接証明書を組み込み、ユーザが平文での証明書について知ることも見ることも必要ないようにする	いつでもどこでもジャストインタイムで、モバイルアプリやウェブベースのコンソールを使ってリモートアクセスタスクを実行できるようにする	詳細なセッションデータをリアルタイムまたはセッション閲覧後に取得することによって、監査証跡、セッション調査その他のレポーティング機能を作成し、コンプライアンスの証明のために立証レポートを作成する
	リモートサポートとヘルプデスク担当者	**チャットサポート**	**幅広いプラットフォームのサポート**	**きめ細かい許可&役割**	**コラボレーション**	**セッションの記録&監査証跡**	**Chrome、Firefox、IEその他によるサポート**
		Click-to-Chatを使い、画面共有とリモート制御へジャストインタイムで昇格させることで、エンドユーザとの接続を切らさずにウェブサイトからその場でサポートが可能になる	Windows、Mac、Linux、iOS、アンドロイドのデバイスのサポートを提供する。また、RDP、Telnet、SSH、VNCを使って旧式のデバイスもサポートする	チームやユーザ、役割、セッション許可設定などをきめ細かく管理して、最小権限の体制を強制実行する	ジャストインタイムで、サポートに関する問題をいち早く解決し、熟練した人材への昇格パスを決定し、しかも適切なチームメンバーを取りこむことによって顧客満足度を高める	チームのパフォーマンスやログセッション動作の履歴を追跡し、セキュリティやコンプライアンス、研修などの監査証跡として役立てる	BeyondTrustのHTML5 Web Rep Consoleは、どんなブラウザからも–ダウンロードの必要もなく–ジャストインタイムで安全なリモートサポートが行えて、すぐに問題解決に着手できる

JIT方式とトリガーのマッピング

下の表は、JIT PAMのトリガーと方式をBeyondTrustのソリューションに当てはめたものです。

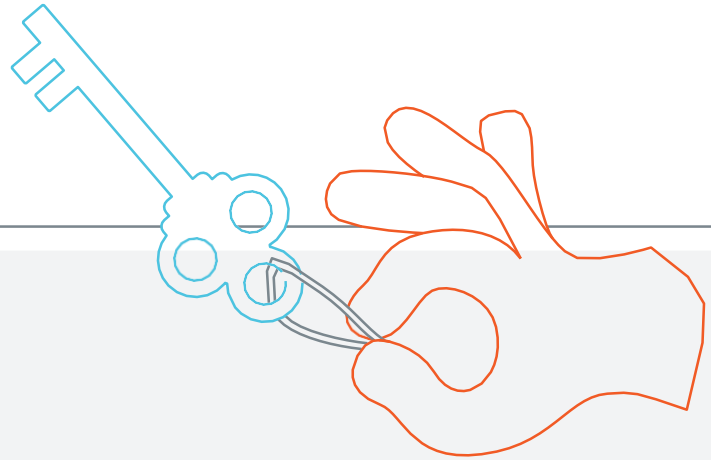
	Privileged Password & Session Management	Endpoint Privileged Management	Secure Remote Access
トリガー			
資格	●		●
ワークフロー	●	●	●
コンテクスト認識	●	●	●
多要素	●	●	●
方法			
アカウントの作成及び削除	●		
グループメンバーシップの特権	●		
偽装（なりすまし）	●	●	●
無効の管理者アカウント		●	
トークン化		●	

JIT PAMの実装を一歩進めて、サイバーリスクを減らす

多くの組織にとって、必要十分なアクセスモデルと合わせてJIT戦略を導入することは、自社の貴重なIT資産を守るための最も効果の高い次の一歩です。

JITの特権管理は、真の最小権限の重要な構成要素と考えるべきです。いったんアカウントを認証してしまったらずっとそれを有効にするのではなく、その使用について適切な業務基準を満たすまで、全ての特権使用行為を禁止するというセキュリティモデルを拡大することで、いつどのように使用するかについて管理を強化します。これには、アカウントアクセスの規制だけでなく、特定のアカウントがリアルタイムで使用できる実際の特権や許可、資格なども含まれます。

JIT PAMは、コンテクスト（状況）で判定されるトリガーを使ってジャストインタイムで特権アクセス管理を有効にし、リアルタイムのポリシーに基づいてユーザの特権アカウントの振る舞いが適切であるようにすることで、常時有効状態のアカウントによる重大な企業規模でのリスクに臨機応変に対処します。これは単に特権アクセス管理が自然進化したというだけでなく、ITリスク管理における飛躍的な前進を示しているのです。BeyondTrustの特権アクセス管理によって、組織は日に日に複雑で雑多になるIT環境に広がる、常時オンの特権アクセスという課題やリスクに取り組みながら、エンドユーザの生産性と安全性を守ることができます。



JIT PAMの主な利点

1. 一元集中管理で自動化され、コンテクスト（状況）と時間ベースの特権のプロビジョニング／プロビジョニング解除によって、特権が危険にさらされかねない脆弱性の範囲を大幅に減らすことができる
2. 真の最小権限の強制実行によって、特権ユーザや特権セッションが減り、このことでセキュリティが向上するのはもちろん、監査やコンプライアンスの手段が簡易にもなる
3. エンドユーザは意識する必要はなく、干渉もない運用なので、業務遂行の阻害とならずに生産性を確保できる
4. 常時有効状態の特権アカウントと、それに伴う攻撃対象面を減らすことができる

用語集

関連のコンセプトと用語

緊急アクセス：コンピュータの世界で緊急アクセスとは、他のアクセス方法がうまくいかなかったりアクセス不能になったりといった重大な緊急事態の際に、通常のアクセス制御手続きを迂回することによって、システムアカウントのパスワードを振り出すことを意味します。ユーザーは緊急アクセスによって、通常ではアクセス権限のないアカウントにすぐにアクセスすることができますが、このアクセスには普通、時間制限があります。

ジャストインタイム（JIT）の特権アクセス管理：JIT特権管理の目的は、承認されたタスクや業務に基づいて、必要な特権を「その場で」割り当て、タスクが完了するか、承認されたアクセスのための時間枠やコンテクストが失効になった後に、これを削除することです。JIT特権管では、振る舞いやコンテクストのパラメータに基づいて強制的に制限をかけることによって、組織が継続的な常時オンのアクセスから特権アカウントを守れるようにします。

最小権限：最小権限とは、ユーザやアカウント、コンピュータ処理のためのアクセス権を、日常的に承認された行為を行うことが絶対に必要である人にのみ制限するという考え方とその実務を意味します。最小権限のセキュリティモデルには、ユーザが自分の役割を実行できる最低レベルのユーザの権限か、遂行する業務を行うために必要な最低限の許可レベルを強制施行することも含まれます。最小権限はまた、処理やアプリケーションシステム、デバイス（IoTなど）にも適用され、そこでは各自が承認された行為を行うために必要な許可のみを与えられるのです。

特権：特権は、特定のセキュリティ制限を無効にしたり回避したりする権限を持ち、システムのシャットダウン、デバイスドライバーのロード、ネットワークやシステムの構成、アカウントやクラウドインスタンスのプロビジョニングと構成といった動作を実行するための許可を表すこともあります。

特権アクセス管理（PAM）：特権アカウントの管理や特権IDの管理（PIM）、または単純に特権管理など、様々に使われますが、PAMは、特権アカウントを管理して保護し、ユーザやアプリケーション、サービス、プロセス、タスクなどに対する特権の移譲や昇格の行為を制御するためのソリューションと戦略を指します。PAMソリューションを使って、管理者権限をユーザから削除し（サーバとデスクトップ両方で）、代わりに、必要に応じて承認されたアプリケーションやタスクに対する特権を昇格させることができます。

特権アカウント：特権アカウントは、非特権アカウント（例えば一般アカウントやゲストユーザアカウントなど）を超えたアクセスと特権を与えるアカウントとみなされています。特権ユーザは、特権アカウントを介するなどして現在特権アクセスを利用しているユーザです。特権ユーザや特権アカウントは能力やアクセスが昇格しているため、非特権アカウントや非特権ユーザに比べてリスクにさらされる可能性が非常に高くなります。

特権セッション：特権セッションは、通常は標準ユーザを超えた特権を必要とする動作を行うなどのコンピューティングセッションです。特権セッションを開始することができるのはユーザ、システム、アプリケーション、サービスです。

特権セッション管理（PSM）：特権セッション管理（PSM）には、昇格したアクセスや許可を含むユーザやシステム、アプリケーション、サービスに関する全てのセッションの監視と管理が含まれます。PSMによって高度な管理や制御を行うことができ、これを利用して、内部の脅威や外部攻撃の可能性から環境をさらに手厚く保護しながら、法令やコンプライアンス上でますます必要性が高まっている重要な調査診断情報を管理することもできます。

一般ユーザアカウント：標準ユーザアカウントは最小権限のユーザアカウント（LUA）または非特権アカウントと呼ばれることもあり、限定的な一連の特権を与えられています。最小権限の環境では、ほとんどのユーザが90%～100%の時間、操作しているであろう種類のアカウントです。標準ユーザはコンピューティング環境（Windows、Mac、Linux、Unixなど）で、基本的なアクセス権を持つ非特権ユーザです。この種のアカウントやユーザには、非常に広い管理者権利や特権アクセスのある特権アカウントやスーパーユーザアカウント（rootや管理者）とは対照的に、リソースや設定へのアクセス機能は限られています。

スーパーユーザアカウント：スーパーユーザアカウントは、特別なIT担当者が主に管理のために使う非常に大きな特権を持つアカウントで、コマンドの実行やシステム変更にはほぼ無制限の権能が与えられています。スーパーユーザアカウントは通常、Unix/Linux環境では「root」として、Windowsシステムでは「管理者」として知られています。スーパーユーザアカウントの特権によって、ファイルやディレクトリ、リソースに対して、完全な読み込み／書き込み／実行の特権で無制限にアクセスが可能になります。スーパーユーザアカウントによって、ファイルやソフトウェアの作成とインストール、ファイルや設定の変更、ユーザやデータの削除など、ネットワーク全体の系統的な変更も可能になります。スーパーユーザはまた、他のユーザのアクセスと許可のプロビジョン、プロビジョン解除を行うこともできます。

BeyondTurstについて

BeyondTrustは特権アクセス管理の分野で、窃取した証明書、悪用された特権、侵入されたリモートアクセスなどに絡むデータ侵入を防ぐための切れ目ない手法を提供する業界最大手です。当社の拡張性の高いプラットフォームによって、エンドポイントやサーバ、クラウド、DevOps、ネットワークデバイス環境全体で増殖する脅威に対し、組織は簡単に特権セキュリティを拡張することができるのです。BeyondTrustは組織に対し、リスクを減らしてコンプライアンスの目的を達成し、運用上のパフォーマンスを上げるために必要な可視性と制御をご提供します。半数がFortune 100掲載企業である20,000件ものお客様やグローバルパートナーネットワークから信頼を得ています。

beyondtrust.com

V2019_07_ENG