session2

実践的な ID 管理・特権ID管理への道のり

- 効果的な特権ID管理とは -

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

何を伝えたいの？

- 企業規模・業種問わず必要な**特権ID管理を考えるきっかけ作り**-

なぜ今特権ID管理が注目されているのでしょうか？

特権IDは高権限を持っており、
あらゆる操作ができるため、攻撃者にとって目的実行の一番の近道なのです。

IPAのセキュリティ10大脅威の上位を占めるランサムウェア、内部不正、標的型攻撃、は特権IDの不適切な管理が大きく関連しています。
特に最近のランサムウェア攻撃のほぼすべてで、特権IDが不正利用されているものにあります。

2024年1月末に発表

情報セキュリティ10大脅威 2024（組織の脅威のみ5位まで抜粋）

順位	組織向け脅威（2024）
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)

出典：情報セキュリティ10大脅威 2024、情報処理推進機構、
https://www.ipa.go.jp/security/10threats/10threats2024.html

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

はじめに：特権ID、PAMってなに？

特権IDってとりあえず取っ付きづらい！

起：PAMの製品で導入で完璧！？

製品導入で楽々PAM管理！。。。え、なぜ特権ID関連の事故が起こるの！？

承：よくある導入後の課題

ベンダーがいう”理想系”、なんで実態とGapが生まれた！？

転：特権ID管理の勘所

どこでも通用する考え方と設計方針

結：アクションの提言

これであなたも特権ID管理が好きになる！？

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

自己紹介

氏名：桜井　剛

経歴：エンジニア歴 **１５年**

1.国内金融向けインフラSE　7年

2.海外拠点向けセキュリティプリセールス　５年

3.セキュリティアーキテクト 兼 セキュリティビジネス開発 3年

主な業務：セキュリティアセスメント/ロードマップ策定等の上流工程

今日の紹介内容

- **PAMを考えてみよう！（どうやる、何が必要、構成は？はあと）**-

お話する事	お話しない事（次回？）
1.特権IDってなに？ 2.特権ID管理の必要性 3.特権IDを取り巻く環境 4.PAMの導入効果・機能 5.導入後の困った、、、の声 6.無駄にしない特権ID管理の勘所 7.特権ID管理のススメ	1.具体的な設計内容 2.技術的な機能紹介 3.製品に特化した話 4.製品の売り込み

はじめに：特権ID、PAMってなに？

よく聞く人も初めて聞く人も改めて整理

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

特権ID、PAMってなに？

- そう、よく使うなんでもできるIDです！ -

＜特権ID＞

「特権ID」とは、一般のユーザーIDとは異なり、システムの設定変更やデータベースへのアクセス、重要なデータの操作など、システム全体や機密情報に影響を及ぼす操作を行える権限を持つIDを指します。例えば、システム管理者アカウント（administrator）やrootアカウントなどが含まれます。

＜特権ID管理/PAM＞

PAM（Privileged Access Management、特権アクセス管理）は、特権IDや高権限を持つアカウント（特権アカウント）の管理を行うためのソリューションや仕組みを指します。PAMの目的は、特権IDのセキュリティを強化し、アクセス制御や監査を通じて不正アクセスやデータ漏洩リスクを軽減することです。

PAMはITシステムに必ず存在する**強い権限のIDを管理する事**！

特権ID管理、PAMはなにをすればいい？

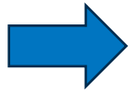
- 管理くらいなら工夫すれば簡単にできるんじゃない？ -

PAM（特権アクセス管理）で必要な主な機能は以下の通りです：

1. **パスワード管理**：特権IDのパスワードを安全に管理・リセット。
2. **アクセス制御**：アクセス許可を管理し、多要素認証でセキュリティを強化。
3. **セッション管理**：操作を記録・監視して、不正アクセスを防止。
4. **監査とレポート**：操作履歴を保存し、監査やレポート作成が可能。
5. **一時的な権限付与**：必要な時だけ一時的に権限を付与し、リスクを抑制。
6. **アカウント検出**：特権アカウントを自動検出し、管理範囲に追加。

これらの機能により、特権アクセスの安全性と運用効率が高まります。

これならできそう！
もう少し詳細に！



PAM（Privileged Access Management）ソリューションで必要とされる主な機能は以下の通りです。これらは、特権IDの管理やアクセス制御を効率的かつ安全に行うために重要な要素です。

PAMにおける主な機能

1. **特権パスワード管理**
   - 特権IDのパスワードを自動で生成・保存・管理する機能。
   - 使用後にパスワードを自動でリセットすることで、不正アクセスのリスクを軽減。
2. **アクセス制御と認証**
   - 特権IDへのアクセスを制限し、アクセスの許可・拒否を管理する機能。
   - 多要素認証（MFA）などの追加認証手段を提供し、アクセスの安全性を高める。
3. **特権セッション管理**
   - 特権IDを使用した操作を記録し、監視可能にする機能。
   - リアルタイムのセッションモニタリングや記録保存、アクセスの中断などが含まれる。
4. **監査・レポート**
   - すべての特権アクセスを詳細に記録し、誰が何を行ったかを確認できる機能。
   - コンプライアンス対応のための監査証跡や、定期的なレポート作成機能が重要。
5. **特権エレベーション（権限昇格）とディエスカレーション**
   - 必要に応じて、一時的にアクセス権限を付与し、必要がなくなった際には権限を自動的に削除する機能。
   - 必要最小限の権限付与により、セキュリティリスクを最小限に抑える。
6. **アカウントディスカバリとオンボーディング**
   - ネットワーク内のすべての特権アカウントを自動検出し、管理対象に追加する機能。
   - 新しいアカウントのオンボーディングを効率化し、管理の抜けを防止。
7. **シークレット管理**
   - APIキーや証明書、トークンなどのシークレットを安全に保存・管理する機能。
   - DevOpsやクラウド環境でのアプリケーション間通信における認証情報の保護が求められる。
8. **ロールベースのアクセス制御（RBAC）**
   - 役職や業務に応じて、ユーザーに適切なアクセス権限を割り当てる機能。
   - 権限の集中管理により、ポリシーに基づいたアクセス制御が可能。

あれ、難しい。。。
どうやるんだ！？

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

PAMってなんか必要なの？

- 結局、自力じゃ難しい。。。だからPAMの市場って存在するんです-

PAM（特権アクセス管理）は専用製品を使うことが一般的ですが、製品を使わずに実施することも可能です。しかし、製品なしのPAM管理には、手作業や個別の管理が多くなるため、以下のような課題が伴います。

1. アクセス管理の複雑さ

- PAM製品がない場合、特権IDのパスワード管理やアクセス権の付与・削除を手動で行う必要があります。特に複数のシステムにわたる場合、手作業での管理は難しく、セキュリティリスクが高まります。

2. 監査とセッションの監視

- PAM製品は、特権アカウントの操作を監視し、監査ログを自動で記録する機能を備えています。製品なしでは、ログの収集と分析を一貫して実施するのが難しくなり、セキュリティ監査に対応するのも手間がかかります。

3. 手間と運用コスト

- 特権ID管理を手作業で行う場合、IT部門の運用負担が増加し、ミスや手抜かりが発生しやすくなります。PAM製品の導入は初期費用がかかりますが、運用コストの削減やセキュリティ強化につながります。

製品なしでのPAM代替策

- **アクセス制御のポリシー設定**：WindowsやLinuxのシステム上で、ローカル管理者権限やアクセス権を厳密に管理する。
- **多要素認証の活用**：特権アクセス時に多要素認証（MFA）を追加。
- **ログ収集と分析ツールの活用**：オープンソースのログ管理ツール（例：ELKスタック）を活用してログを管理・監視する。

製品なしでPAMを行うことも可能ですが、セキュリティの一貫性や運用効率を考えると、特定のPAM製品を導入するメリットは大きいです。

起：PAMの製品って完璧！？

ならPAMを導入すればいいじゃないか

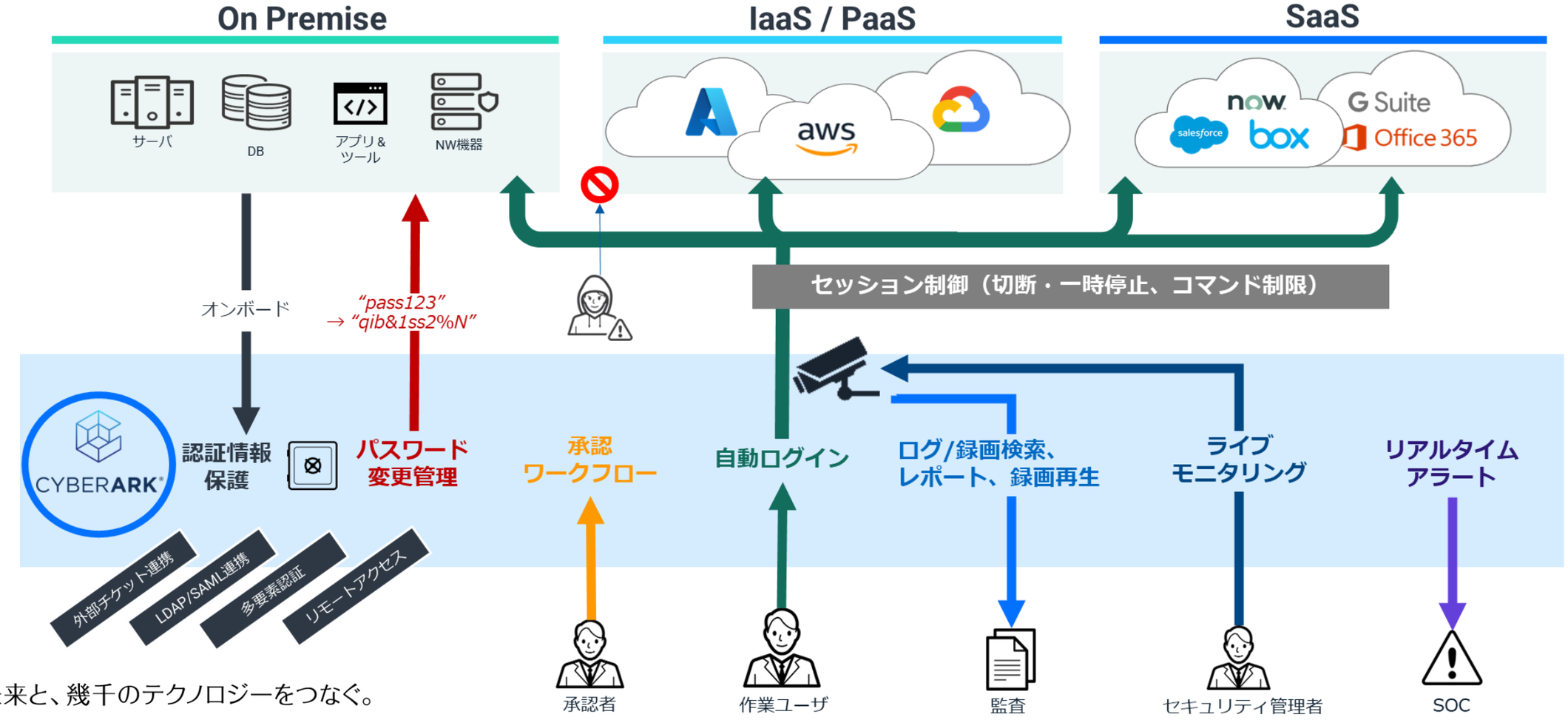
業界No1の実力

- いわゆるデファクトスタンド、これを入れておけば完璧な気がする -

No. 1 特権アクセス管理において揺るぎないリーダー

6,900+ 全世界でCyberArkを利用中の顧客数

50%+ フォーチュン500の50%以上の企業が利用



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

起 承 転 結

業界No1の実力

- いわゆるデファクトスタンド、これを入れておけば完璧な気がする -

特権アクセス管理において揺るぎないリーダー

全世界でCyberArkを利用中の顧客数

フォーチュン500の50%以上の企業が利用

アクセス制御、トレーサービリティ

- 共有IDであっても、どの機器のどのIDを誰が利用できるのかをコントロールする。
- 必要に応じ申請・承認を要求する。
- 誰が、いつ、どのIDを利用したのかを判別する。

パスワード保護、秘匿

- 暗号化やアクセス制御が施された安全な場所に保管する。
- 利用者はパスワード自体を知る必要はなく、踏み台サーバーからの自動ログインで作業できる。
- 漏洩リスクを大幅に削減。

パスワード自動更新

- 法令要件や社内ポリシーにそって、パスワードを定期変更を自動的に行う。
- パスワード管理運用コストを削減し、抜け漏れリスクを低減。

セッション録画レビュー

- セッションで行われた作業をテキストだけでなく録画記録する。
- 「何が行われたのか」までレビュー・追跡可能なり、レビューの精度向上やインシデント対応スピードアップに。

監視、不正検知

- 特権IDの不審な利用や、ルールに違反した利用をメールやSIEM連携でアラート。
- リスクをいち早く検知し、自動・手動の対応をトリガーする。

一元管理

- 多様なITインフラ、認証情報を可能な限り同じシステムで管理する。
- セキュリティベースラインを標準化。例外運用をなくし、業務効率とガバナンスが向上。

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

起 承 転 結

PAMを取り巻く環境

- （高い投資して）導入は進んでいるのに、特権侵害の被害は高いまま -

PAM入れてID管理しているのになぜ？？

①高い導入率

主な金融規制に対応するための
金融機関での導入・対応率

- PCI DSS対応率: 85%
- SOX法対応率: 78%
- GDPR対応率: 65%

※データ出典: 2022年金融セキュリティ調査
ガートナー、ENISA

②高い業務効率性

PAM導入による投資対効果

- セキュリティリスク90%以上削減
- ROI平均192%
- 監査対応時間40%短縮

出典: CyberArk 2023年PAM導入効果調査、Gartner 2023
Forrester Total Economic Impact Report 2022】

③高い被害率

特権ID侵害の被害状況

- データ侵害の約80%が
  特権IDの不正使用が原因
- 平均被害額: 約400万ドル
- 特権ID侵害事件の34%が
  重大インシデントに

※データ出典:出典: Verizon Data Breach Investigations Report 2023、出典: Ponemon Institute, Cost of a Data Breach Report 2023

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

承：よくあるPAM導入後の課題

セキュリティ事故は”複数の課題の副産物”

起 承 転 結

仮説：PAMを入れるだけじゃ不十分

- 要はちゃんと使えこなしていないからダメ？-

PAM（特権アクセス管理）を導入しても特権侵害が減らない原因には、以下のような課題が関係しています。

1. **特権アカウントの可視性不足**
   多くの組織では、特権アカウントが全て把握されておらず、特に古いアカウントやサービスアカウントが見落とされがちです。これにより、使われていないアカウントが悪用されるリスクが生じます。Thycoticの調査によれば、約55％の企業が特権アカウントの自動検出を行っておらず、管理対象の特権アカウントが漏れている可能性があります JAS SOLUTION 。
2. **多要素認証やパスワード管理の不徹底**
   特権アカウントに対する多要素認証（MFA）やパスワード管理が不十分であると、特権IDへの不正アクセスが発生しやすくなります。BeyondTrustの調査でも、多くの組織が特権アカウントに対してパスワードの定期変更を行っておらず、これが侵害リスクを増大させる要因となっています BEYONDTRUST 。
3. **セッション監視と監査の欠如**
   特権アカウントの利用をリアルタイムで監視したり、操作記録を定期的に監査する体制が整っていない場合、不審なアクティビティを見逃しやすくなります。日本の多くの企業でも、内部不正や操作ミスによるインシデントが頻繁に発生しており、これを防ぐためには、特権アカウントの利用状況をリアルタイムで把握し、異常を早期に発見できる監視体制が必要です ビジネス+IT NRI SECURE 。
4. **PAM導入後の運用プロセス不足**
   PAMソリューションを導入しても、組織全体で適切な運用プロセスが確立されていない場合、十分な効果が得られません。特に中小企業ではPAMの管理体制が整わないことが多く、運用の徹底に難があると指摘されています GII.CO.JP 。

これらの理由から、PAMの導入は重要な一歩ですが、特権IDの可視化、定期的な監査、運用の徹底といった追加対策を講じることが不可欠です。

俗にいう”**ツール導入だけじゃなく、運用も考えましょう**”というやつですね！

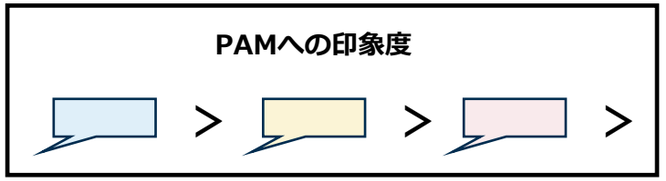
ただ、PAMを使った運用ってどうやる？
マニュアルには書いていないし、どの企業も開示していない情報だよな。。。
PAMに詳しいエンジニアは組織にいない。。。

SIerさん、お任せします！
運用を考えた、PAM導入してもらえますか？

今日のお伝えしたい事①
まって！高いお金を払う前に、PAMの導入には何を考えればいいのか？を知りましょう

PAM導入後によくある問題

- 海外３件、日本２件のPAM提案・アセスメント・導入経験から-



	案件前・PAM構築時	PAM利用開始直後	PAM運用中（事故発生時）
SIer/コンサル	ベストプラクティスを考慮して PAMシステム構築しました。 現行運用から変更をして下さい	そんな特殊な現行運用があったんですね ベストプラクティスを守るべく個別対応せず共通 ルールを適用すべき。利用者を教育しましょう	監査、ID棚卸し、PAM外部で の特権ID利用の把握は実装 できません
セキュリティ担当 (PAM導入案件担当)	ITシステムにどんどん展開して セキュリティ高めましょ。 利用者から既存運用やご要望を 聞きましょう	既存運用の考慮漏れ！？PAM登録の自動化、監査 機能の強化、個別対応要望をどう検討しよう！？	PAMの展開・機能拡張、維持 の予算が通らない！！
開発部門・運用部門 (PAM利用者)	現行業務があるので、PAM入 れて変更されると困ります。 何か必要なら言ってください	PAMの利用方法だと既存のIT運用はまわらない！どのID がPAMへ登録する対象？あと、IT管理ツールとの連携を したんだけど、なんですぐできない？	
経営層・監査部門 （システムオーナー）	PAM導入でセキュリティ対策、 金融規制にも対応してほしい （高いけど効果は期待！）	日常的な特権ID利用、ID登録漏れ、退職者の ユーザ残存、限定的なPAM対象範囲などの管理 不足による監査指摘がたくさんあるんだけど！	セキュリティ事故の 原因が特権ID不正利用？

純粋なPAM案件と捉えるとこのような事が発生する！

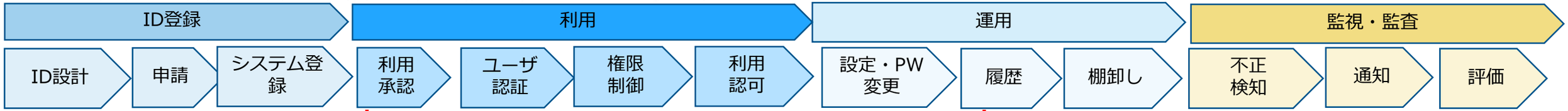
起 承 転 結

PAMじゃカバーできない領域

- PAMってIDライフサイクルの一部しかできないの！？-

今日のお伝えしたい事②
PAMはIDプロセスの一部に特化

特権IDのサイクル (sailpoint https://www.sailpoint.com/ja/identity-library/identity-and-access-management/



PAMの機能（得意分野）

PAM導入後に問題になるTop3

よくある課題・考慮不足ポイント(経験則)

1 **特権IDの定義**
対象選定の基準

2 **MFAの適用対象**
個別適用の必要性

3 **ITチームのレガシーなID設計思想の見直し**
・あいまいな特権ID作成基準
・クラウド、DevOps不適合
・複雑なID、権限設計

4 **利用承認レビュー観点**
・申請内容の理解と評価
・ID毎の複雑な承認ワークフロー

5 **アクセス先システムの制限**
・利用可能、申請者の制限設計
・既存運用の変更、個別ID追加作成

6 **ベンダーの利用**
・ライセンス費用
・障害復旧時の非常時アクセス（break-glass-account)

7 **日常利用（特権ID利用の低い牽制力）**
・ワークフローの形骸化（レビュー観点、申請外作業、特定IDのみ利用）
・作業内容のレビュー、不正検知 困難
・監査指摘事項 No1

8 **PW変更不可**
・不透明な変更影響
・PWハードコーディング
・CyberArkサポート対象外製品

9 **非利用IDの残骸**
・IDオーナーの認識不足
・野良ID（ただの脆弱性

10 **間接利用時の監査不可**
・SSO
・sudo

11 **不正検知と防止**
・不正の定義とその検知方法
・翌日の摘発（予防不可）

12 **BCP/障害対処フロー**
・CyberArk障害時の対処
・BCPプロセス等既存オペへの影響

CTC Financial Services

転：特権ID管理の勘所

全体感をどれだけ持てるか

PAM導入の目的を達成するには？

- 案件の捉え方をシフトする事が必要 -

①PAM導入ではなく、特権ID管理プロセスの強化

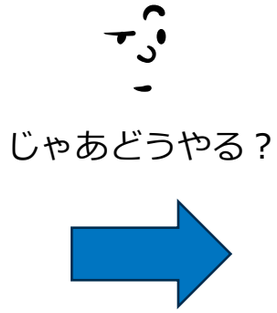
PAMはID管理プロセスの一部。
PAM以外も含めた全体プロセスも同時に検討

②既存運用ベースではなく、特権ID管理プロセスベース

現状運用ベースの検討は特権ID管理の一貫性に影響。
まずはあるべき姿を描き柔軟な利用環境・プロセスを事前に定義

③製品ベストプラクティスではなく、合理的な投資

導入したら永続しえる継続投資。
ずっと使うからこそ、最初にしっかり方針・ロードマップを定義



導入テンプレートでの
評価・検討から始める
（０から検討はしない）

条件1.網羅的な検討事項

条件2.自社視点で検討・議論が可能

条件3.業界標準フレームワーク準拠

導入テンプレート（ソース）

今日のお伝えしたい事③
機能よりプロセスが重要、は業界標準

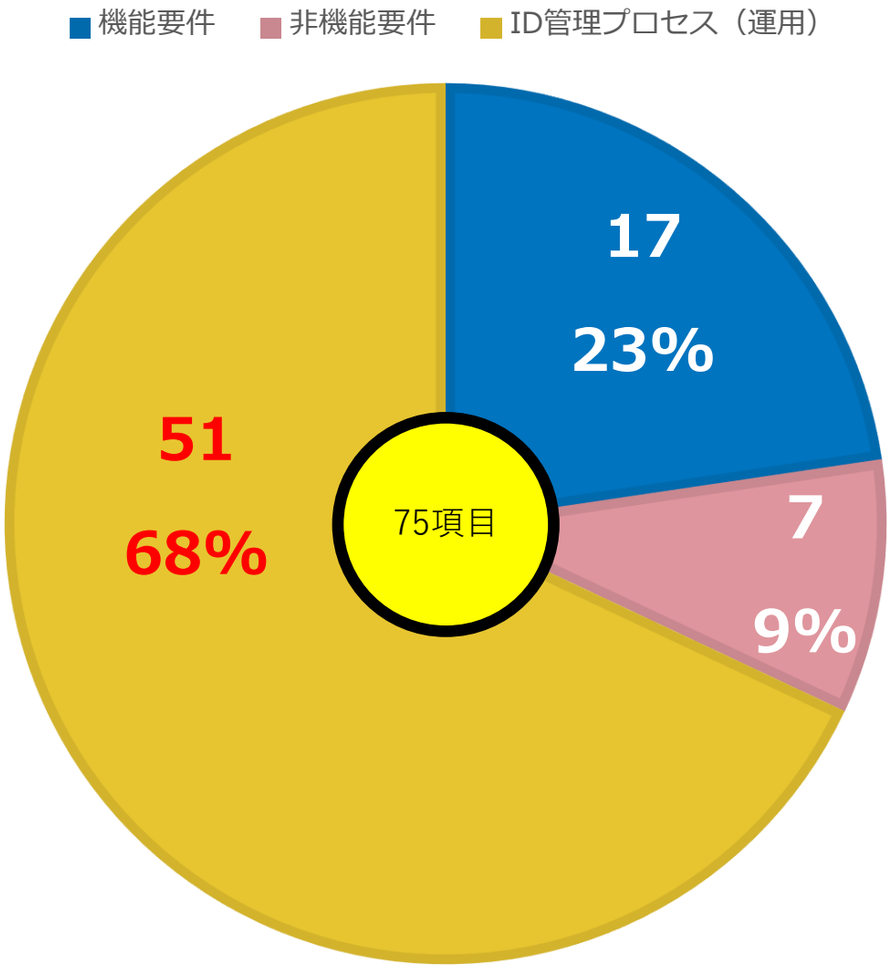
-業界標準のフレームワークの内、プロセスに関する項目が68 %(最重要事項)

NIST National Institute of Standards and Technology
-SP 800-53
-SP800-63A
-SP800-63B
-SP800-63C

CIS Center for Internet Security®
CIS Controls ver8

FISC 金融情報システムセンター The Center for Financial Industry Information Systems
NISTSP1800-18 Playbook

JNSA
特権IDガイドライン



無限の未来と、幾千のテクノロジーをつなぐ。
CTC Financial Services Group

起 承 転 結

導入テンプレート（イメージ）

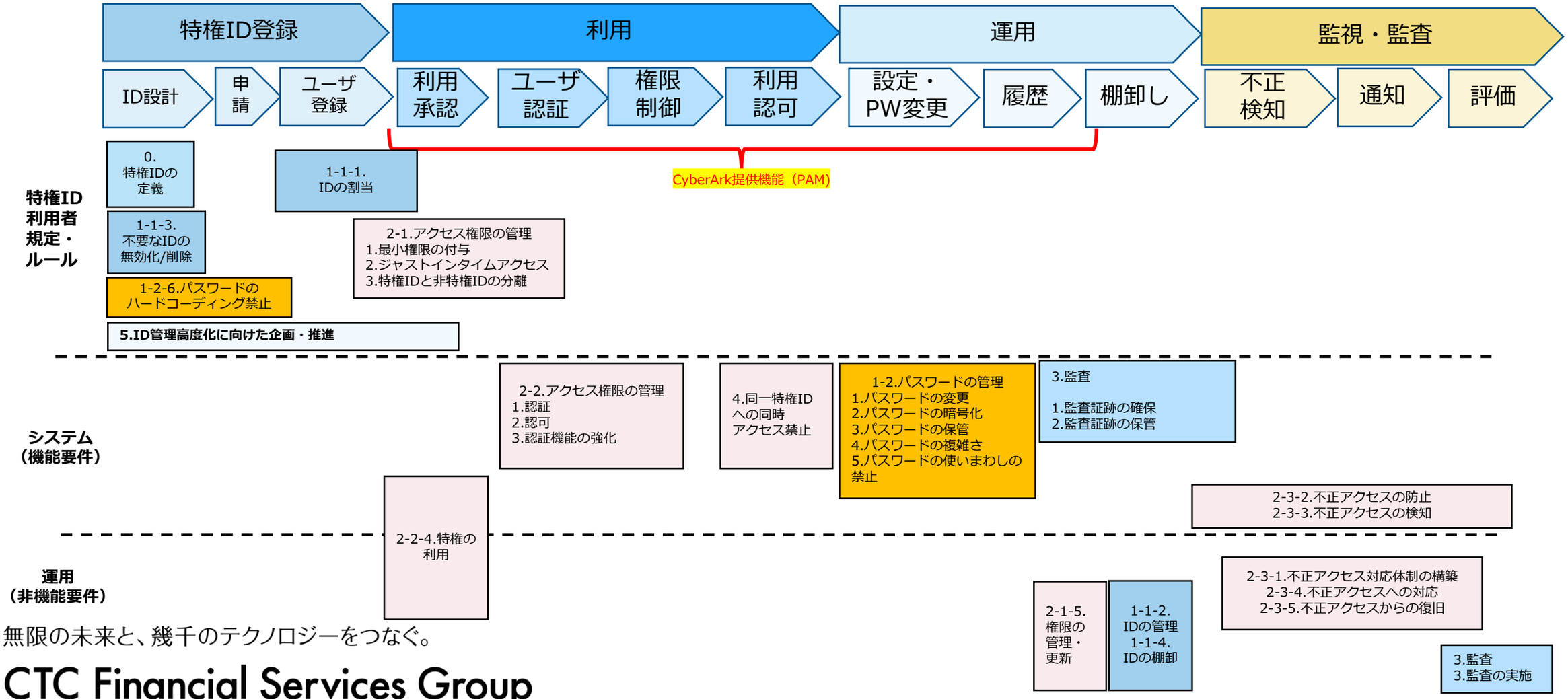
- 検討・評価ができるレベルでのチェックリストが有効的-

おおよそ75個

#	大分類		中分類		小分類	PAM導入時の推奨事項	要件タイプ（CTCの理解）		
							PAM(CyberArk)ツールに対する要件		特権IDの管理に対する要件
							機能要件	非機能要件	ルール・運用
0	全体	-	-	-	-	"特権ID"定義の明確化	N/A	N/A	○
1	ID/パスワード管理	1	ID管理	1	IDの割当	・原則、特権IDにアクセス可能なIDは一つの対象(※)と紐づけられ、特権IDにアクセス可能なIDから対象が一意に特定できること。	○	N/A	○
						・原則、特権IDにアクセス可能なIDの共用や単一の対象(※)の集合（組織・グループなど）への特権IDにアクセス可能なIDの割り当てを行わないこと。※人、デバイス、システム、アプリケーションなどの、管理対象となるものを指す。	○	N/A	○
				2	IDの管理	・特権IDの範囲と数を把握し、一覧として管理すること	○	N/A	○
						・特権IDにアクセス可能な全てのID（ユーザID・システム用IDの双方）を把握し、一覧として管理すること	○	N/A	○
		2	パスワード管理	1	パスワードの変更	・特権パスワードは利用後に変更すること	○	N/A	N/A
				2	パスワードの暗号化	・強力な暗号化アルゴリズムを使用して、特権パスワードを暗号化すること	○	N/A	N/A
2	アクセスの統制とコントロール	1	アクセス権限の管理	1	最小権限の付与	職務を遂行するために必要最低限の特権IDへのアクセス権限のみが許可されること	N/A	N/A	○
		1		2	ジャストインタイムアクセス	・特権IDへのアクセス権は必要最低限の期間のみ許可すること ・利用期間終了後、延長して利用する場合はその必要性を再度確認してから許可すること	N/A	N/A	○
		2	アクセス制御	1	認証	・ユーザやシステムが特権管理基盤にアクセスする際に、アクセスが正当なものであるか識別するために認証機能を実装すること。	○	N/A	N/A
				2	認可	・ユーザやシステムが特権管理基盤にログイン後、アクセス可能な特権IDを制御できるようにすること。	○	N/A	N/A
				3	認証機能の強化	・強度の高い認証方式（多要素認証など）で、正当性を確認すること	○	N/A	N/A
		3	不正アクセス対策	1	不正アクセス対応体制の構築	・不正アクセスを速やかに検知するための組織体制や役割の整備を行うこと。	N/A	N/A	N/A
						・不正アクセスが発生した場合の復旧手順、連絡手段を、マニュアル等により事前に明確にしておくこと。	N/A	N/A	○
						・不正アクセス検知時に速やかに対応をするために、適宜訓練等をおこなうこと。 ※不正アクセス対応に関するプロセスについての詳細は今後別途整理し、整理内容から改めてポリシーとして記載すべき事項を精査	N/A	N/A	○

CTC流 PAM導入時の検討テンプレート

- 簡単ではない、だからこそテンプレートを活用-



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

結：アクションの提言

今日おぼえて帰って欲しいこと

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

今日お伝えしたかった事

- ２０分でお伝えしたかったこと -

① まって！高いお金を払う前に、PAMの導入には何を考えればいいのか？を知りましょう

②PAMはIDプロセスの一部に特化

③機能よりプロセスが重要、は業界標準

特権ID管理の対応が必要

PAM導入案件

SIerさん、ベストなPAMを
提案してください

特権IDに対応したID管理プロセス高度化案件

チェックリスト

私等が考える特権IDに必要な
PAMはこれですね！

一番言いたい事

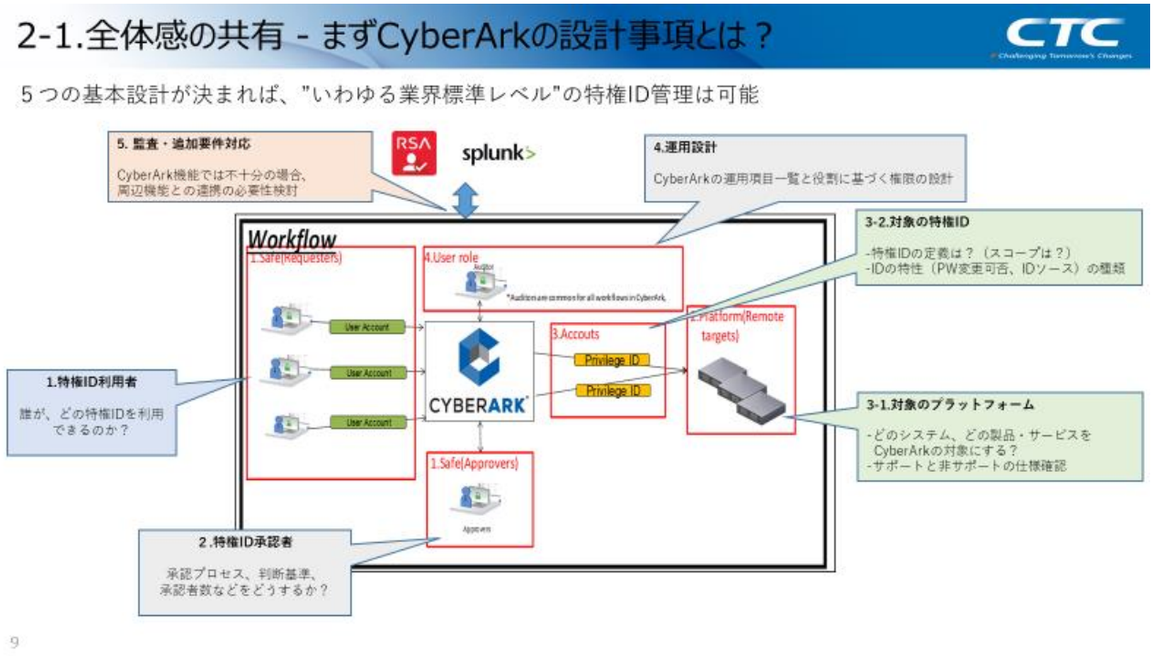
無限の未来と、幾千のテクノロジーをつなぐ。

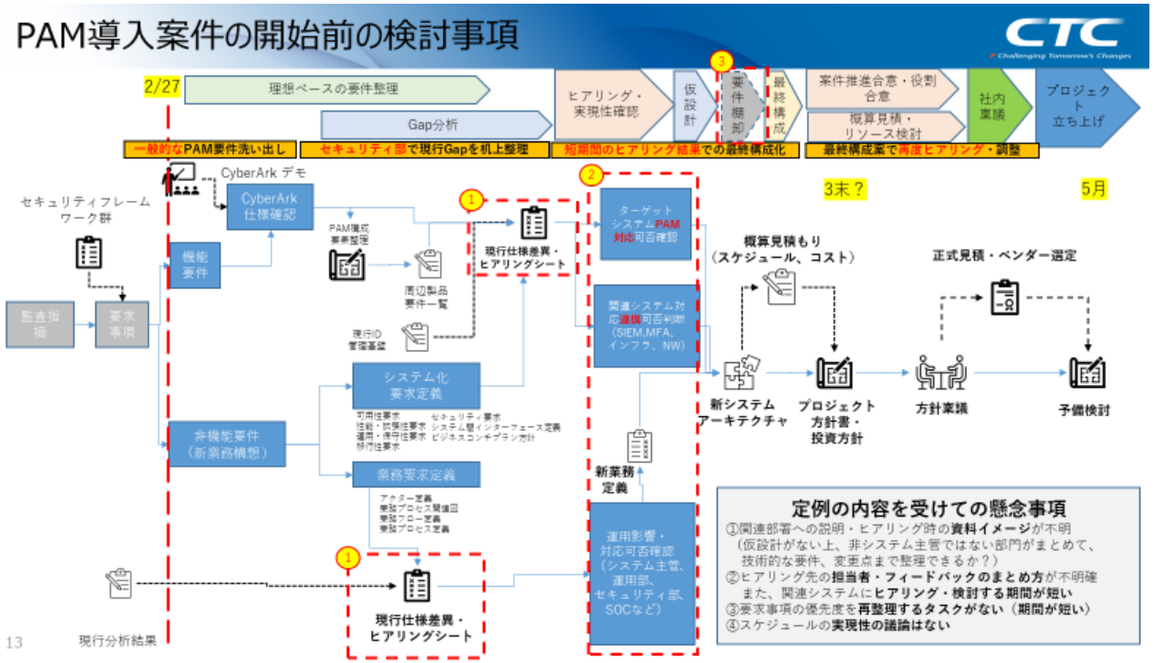
CTC Financial Services Group

予告編 実践編

・理屈はわかった。具体的な設計内容を知りたい
・案件を計画しないといけない、どういう検討プロセスをふむべき？
・関係部署が多く、巻き込み方の工夫はあるか？

※ご要望があればアンケートに”次回も希望”と記載の上、具体的にお聞きになりたい内容をご教示下さい





無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group