TIS
TIS INTEC Group

＜セッション２＞

特権ID管理ソリューション導入の現場から見える、導入ポイントと気づき

なぜ特権ID管理ツール「SecureCube Access Check」が選ばれるのか
～販売代理店が効果的な導入方法を具体的に解説～

TIS株式会社
IT基盤技術事業本部
IT基盤サービス事業部
セキュリティサービス部

アジェンダ

はじめに
- TIS のご紹介
- TIS の セキュリティビジネスの取り組み

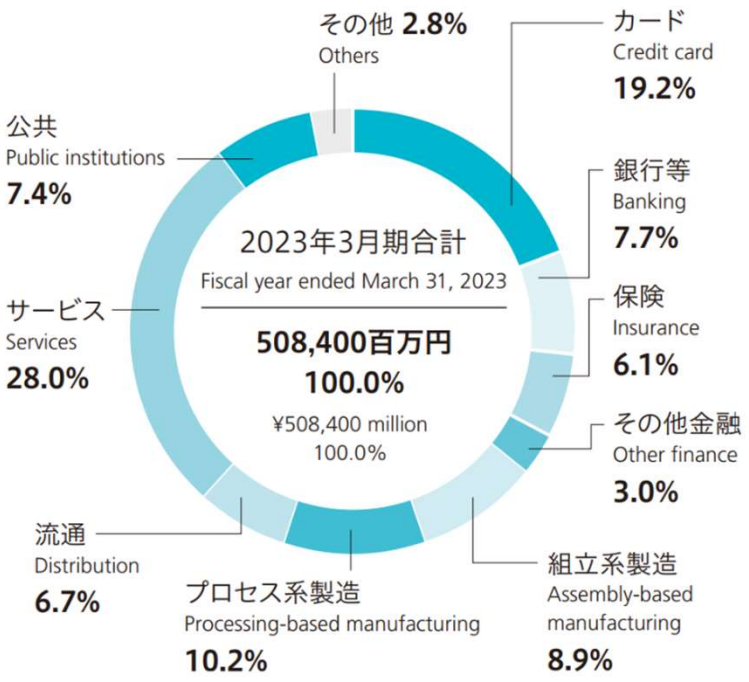
特権ID管理を導入する際の「ご検討ポイント」「導入ポイント」

TIS SI支援について
- TIS が考える “特権ID管理” を導入する際のポイント
- ケース１：災害対策
- ケース２：SaaS 特権ID管理

はじめに

TIS の ご紹介　～会社紹介：TIS株式会社～

社　　名	TIS株式会社 (TIS Inc.)
代 表 者	代表取締役社長　岡本 安史
従 業 員	単体：5,834名（2024年3月31日現在） グループ：21,972名
業種別売上高	



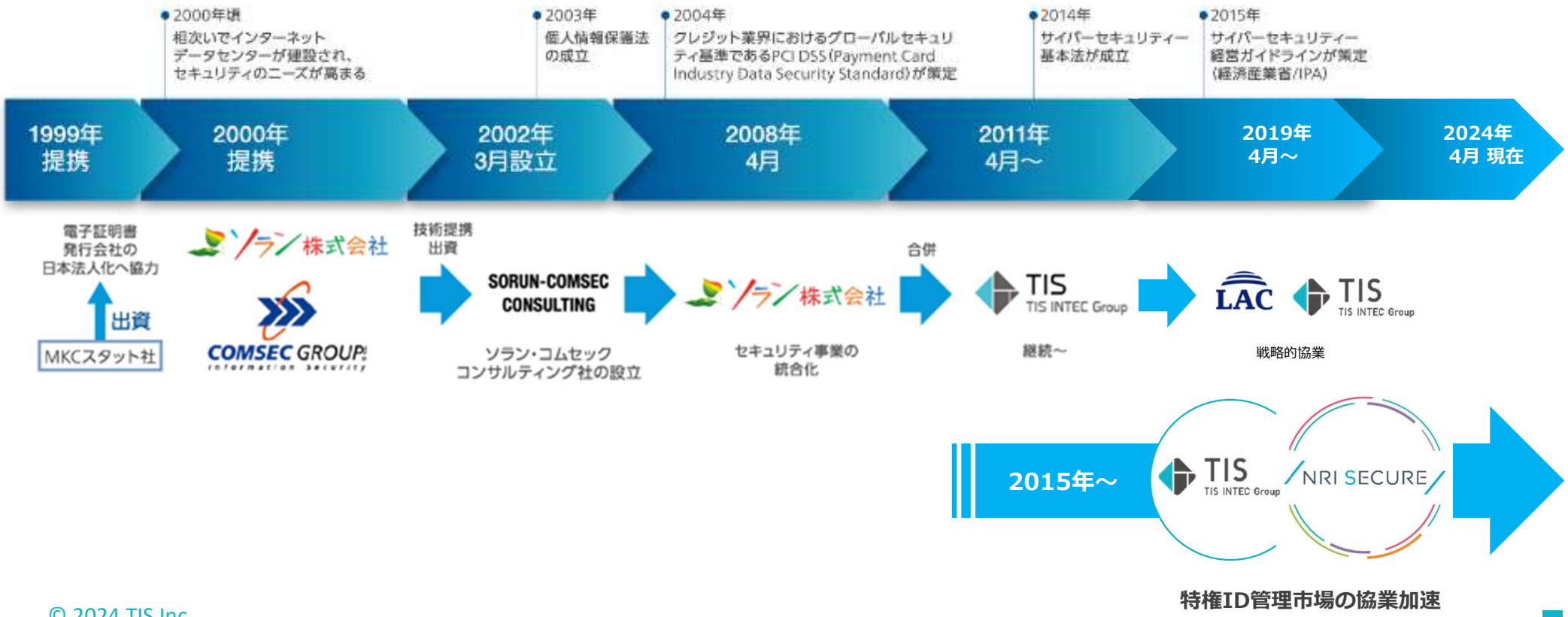
創　　業	1971年 4月 28日
資 本 金	100億円
売 上 高	549,004百万円 （2024年3月期連結）

■ **事業領域**

- 事業戦略コンサルティング
- ペイメント
- デジタルマーケティング
- エンタープライズ
- **ITプラットフォーム・セキュリティ**
- AI・ロボティクス
- R&D (研究開発)

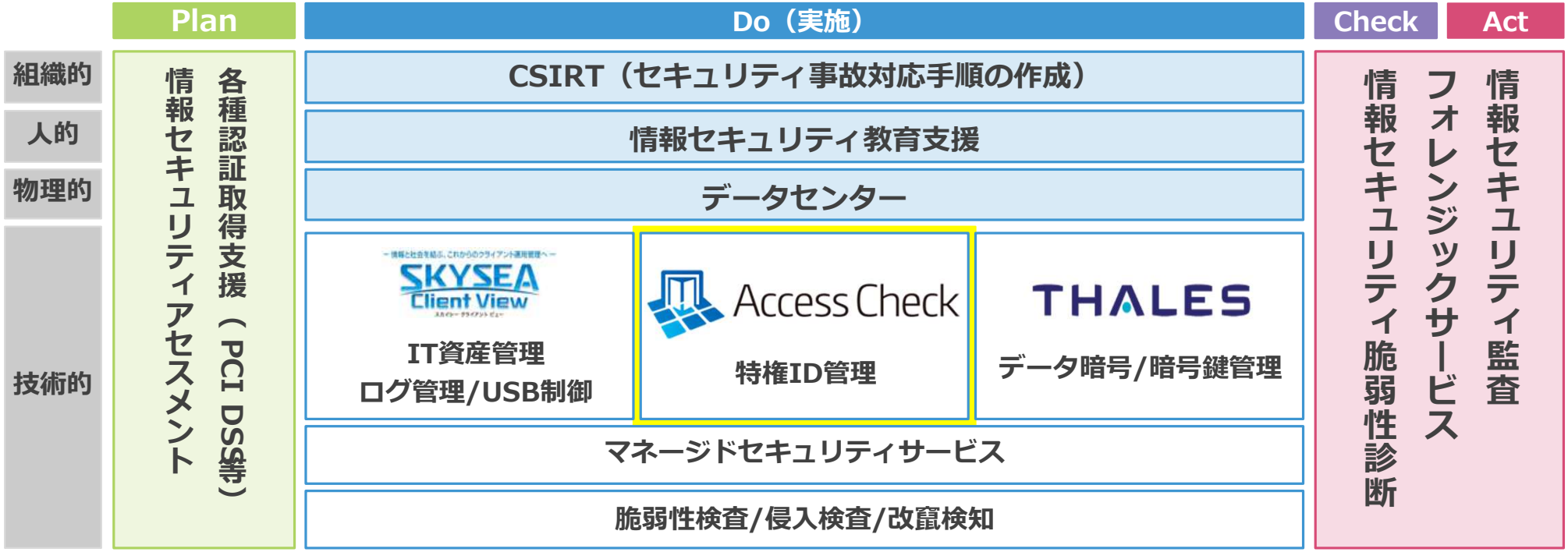
TIS の セキュリティビジネスの取り組み

TIS ではお客様のセキュリティ課題を解決するための幅広いソリューションを提供しております。
20年以上の実績経験に加え、戦略的な協業推進と共に、**SIerとして培ってきたシステム構築ノウハウ**を活かし、最適なソリューションをワンストップでご提供いたします。



TIS の セキュリティビジネスの取り組み

PDCAサイクル（「計画(Plan)」「実施(Do)」「確認(Check)」「改善(Action)」）および「組織的」「人的」「物理的」「技術的」な観点で、TISでは、全方位ソリューションによる情報セキュリティ対策のご支援が可能です。



特権ID管理を導入する際の「ご検討ポイント」「導入ポイント」

TIS が考える “特権ID管理” を導入する際のポイント

特権ID管理を導入する際の「ご検討ポイント」は、運用や目的(Goal)のイメージに即したシステムにするため、“**特権とユーザの紐づけ**“ と ”**機能するシステム**” の2点があります。

また「導入ポイント」は、特権ID管理サーバが稼働する基盤の耐障害性の考慮は、もちろんのこと、“**既存環境や関連する機能（例：バックアップ等）**” も考慮する必要があります。

1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

2．使えるシステム（機能するシステム）

3．ネットワークを含めたシステム構成

TIS が考える “特権ID管理” を導入する際のタスク（導入の流れ）

NRIセキュアテクノロジーズ社で用意されている初期構築パックの役割分担と考慮するポイント

タスク		役割分担（貴社：お客様）	役割分担（弊社：NRIセキュア）	成果物
要件定義	現状調査	• サーバ、ネットワーク環境などの現状調査	• Access Checkの仕様を踏まえた設計 アドバイザリ（メール、電話でのQ&Aベース）	
	アクセス要件定義	• 導入に伴うアクセス要件定義 - IPアドレス制御　- プロトコル制御　-ワークフロー　など		
	環境要件定義	• 導入に伴う環境要件定義 - 運用設計　- 性能設計　- ネットワーク設計など		
導入・構築	設定シート作成	• 初期設定に必要な下記設定シートを記入 - 『OS・ミドルパラメータシート』 - 『Access Checkパラメータシート』	• 設定シートの項目について説明 • 設定シート記入時のアドバイザリ(最大1ヶ月) • 設定シートの内容チェック	• 『OS・ミドルパラメータシート』 • 『Access Checkパラメータシート』
	SecureCube Access Check 導入準備	• ハードウェアおよびOSの調達 • データセンターへの設置 • OS・ミドルウェア導入作業の立会い	• OS・ミドルウェアのインストール • OS・ミドルウェアの初期設定	
	SecureCube Access Check 導入・設定	• Access Check 導入作業の立会い	• Access Check のインストール • Access Check の初期設定	
	稼働確認	• 稼働確認の立会い • （必要があれば）ネットワーク設定変更	• Access Check の稼働確認	• 『稼働確認チェックシート』
	操作説明	• 管理者操作説明への参加	• Access Check の管理者操作説明（最大2時間）	• 『作業完了報告書』
検証	マスタ登録	• ユーザ、ノード、ポリシーなどのマスタを登録	※基本的に保守サポート範囲内で対応します。	
	検証	• 検証環境での検証利用（必要に応じネットワーク設定変更）		

TIS が考える “特権ID管理” を導入する際のタスク（導入の流れ）

NRIセキュアテクノロジーズ社で用意されている初期構築パックの役割分担と考慮するポイント

タスク		役割分担（貴社：お客様）	役割分担（弊社：NRIセキュア）	成果物
要件定義	現状調査	• サーバ、ネットワーク環境などの現状調査		
	アクセス要件定義	• 導入に伴うアクセス要件定義 - IPアドレス制御　- プロトコル制御　-ワークフロー　など	• Acces プ	
	環境要件定義	• 導入に伴う環境要件定義 - 運用設計　- 性能設計　- ネットワーク設計など		
導入・構築	設定シート作成	• 初期設定に必要な下記設定シートを記入 - 『OS・ミドルパラメータシート』 - 『Access Checkパラメータシート』	• 設定シートの項目について説明 ザリ(最大1ヶ月)	• 『OS・ミドルパラメータシート』 • 『Access Checkパラメータシート』
	SecureCube Access Check 導入準備	• ハードウェアおよびOSの調達 • データセンターへの設置 • OS・ミドルウェア導入作業の立会い	ル の初期設定	
	SecureCube Access Check 導入・設定	• Access Check 導入作業の立会い	• Access Check のインストール • Access Check の初期設定	
	稼働確認	• 稼働確認の立会い • （必要があれば）ネットワーク設定変更		• 『稼働確認チェックシート』
	操作説明	• 管理者操作説明への参加		• 『作業完了報告書』
検証	マスタ登録	• ユーザ、ノード、ポリシーなどのマスタを登録		
	検証	• 検証環境での検証利用（必要に応じネットワーク設定変更）	す。	

特権IDとユーザと制御の
紐づけ を、どうすれば良いか？
＝機能するシステムとは？

ネットワークを含めた
最適なシステム構成の検討は？
＝既存環境への影響は？

日々の運用への定着／
無理のない運用か？
現行の運用がどう変わる？
＝機能するシステム

TIS が考える “特権ID管理” を導入する際のタスクとポイント

お客様のご要望に沿ってデザインした “TIS SI支援” になぞって、ポイントを解説いたします。

タスク		役割分担（弊社：ＴＩＳ）	役割分担（弊社：NRIセキュア）	成果物
要件定義	現状調査	• サーバ、ネットワーク環境などの現状調査		
	アクセス要件定義	• 導入に伴うアクセス要件定義 - IPアドレス制御　- プロトコル制御　-ワークフロー　など	• Access Che アドバイザリ	
	環境要件定義	• 導入に伴う環境要件定義 - 運用設計　- 性能設計　- ネットワーク設計など		
導入・構築	設定シート作成	• 初期設定に必要な下記設定シートを記入 - 『OS・ミドルパラメータシート』 - 『Access Checkパラメータシート』		ト』 ート』
	SecureCube Access Check 導入準備	• ハードウェアおよびOSの調達 • データセンターへの設置 • OS・ミドルウェア導入作業の立会い	• OS・ミドルウェアのインストール • OS・ミドルウェアの初期設定	
	SecureCube Access Check 導入・設定	• Access Check 導入作業の立会い		
	稼働確認	• 稼働確認の立会い • （必要があれば）ネットワーク設定変更	• Access Check の稼働確認	• 『稼働確認チェックシート』
	操作説明	• 管理者操作説明への参加		
検証	マスタ登録	• ユーザ、ノード、ポリシーなどのマスタ		
	検証	• 検証環境での検証利用（必要に応じネットワーク設定変更）		

気を付ける点も
TIS SI支援の中で吸収！

1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

2．使えるシステム（機能するシステム）

3．ネットワークを含めたシステム構成

TIS SI支援について

TIS SI支援 の サービス背景・お客様の声

SI支援が必要な理由

- お客様のご利用規模に合わせた最適な構築計画を提案し、ご利用可能な時期を見込むことができる。
- 豊富な過去実績からお客様のご要件に沿った細やかな設計に対応できる。
- Access Check の設計、構築時の前提条件、留意事項を把握しているため、ノックアウトポイントによる手戻りを低減できる。

お客様からの評価ポイント

- Access Check 側のタスクを明確にすることで役割分担が整理でき、作業漏れなく効率的にプロジェクトを遂行できた。
- 導入案件の場合、製品の初期導入で引き渡すケースが多いが、その点、Access Check の機能だけでなく、非機能部分についても顧客要件に沿って設計、導入まで対応範囲で取り組んでくれたことで作業負荷を低減できた。
- 顧客のID統制の要件に合わせたポリシー設計について、主体的にヒアリングと検討を取組み、最適に整理できた。
- 顧客の受入れ対応期間において、運用に準じた操作や技術的な問合せまで的確に対応することで、スムーズなサービスインを迎えられた。

TIS が考える “特権ID管理” を導入する際のポイント

特権ID管理を導入する際の「ご検討ポイント」は、運用や目的(Goal)のイメージに即したシステムにするため、“**特権とユーザの紐づけ**“ と ”**機能するシステム**” の2点があります。

また「導入ポイント」は、特権ID管理サーバが稼働する基盤の耐障害性の考慮は、もちろんのこと、“**既存環境や関連する機能（例：バックアップ等）**” も考慮する必要があります。

1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

2．使えるシステム（機能するシステム）

3．ネットワークを含めたシステム構成

TIS が考える “特権ID管理” を導入する際の「ご検討・導入ポイント」

お客様のご要望に寄り添った設計をご支援いたします！

Access Check の設計においては、以下3点が設計のポイントになります。設計要素はお客様毎のご要件や環境によって異なっております。
弊社では、それぞれ異なるご要望に対して、かなえるべくご支援をさせていただきます。

1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

2．使えるシステム（機能するシステム）

3．ネットワークを含めたシステム構成

- お客様のご利用要件に合わせ、特権ID、ユーザ、ノードの紐付け等、ポリシー定義をご提案し、設定・導入から運用定着までご支援させていただきます。
- Access Check の機能、非機能の設計について、弊社 特権IDエンジニアがお客様 と ご一緒に検討いたします。
- 弊社の これまでの設計・構築経験より、オンプレミス、クラウド基盤問わず、ご要望に沿った最適な構成検討をご支援させていただきます。

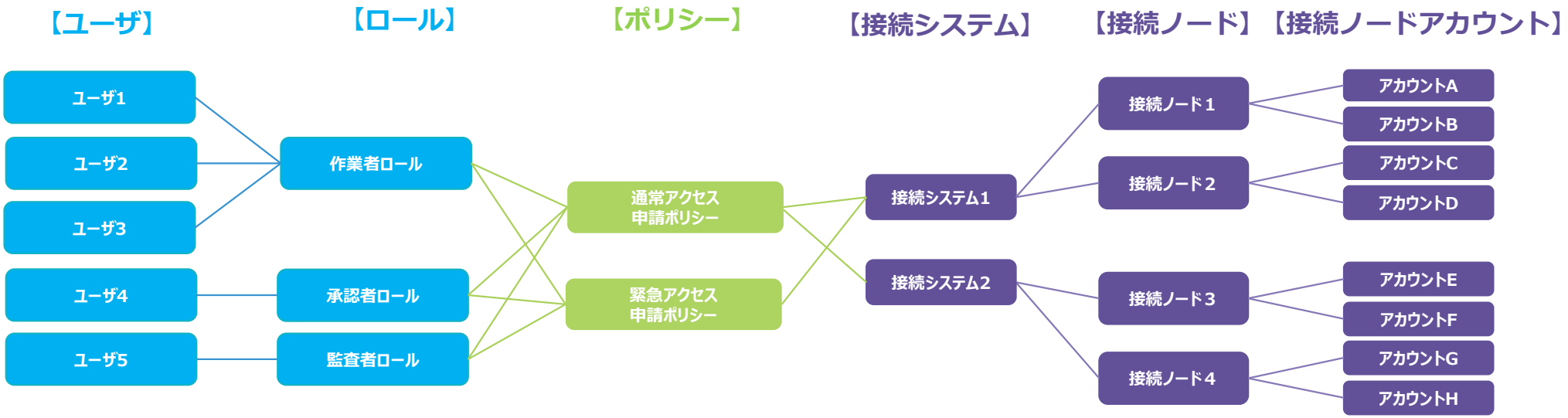
1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

Access Check の実装より、実はポリシー設計が大切です！

ID統制の観点より特権ID、管理対象ノード、アカウント、プロトコルなど、どのように紐づけて管理すべきか悩まれるケースが多くございます。

弊社では、これらポリシーとしてお客様からのヒアリングを行い、ご一緒に整理いたします！



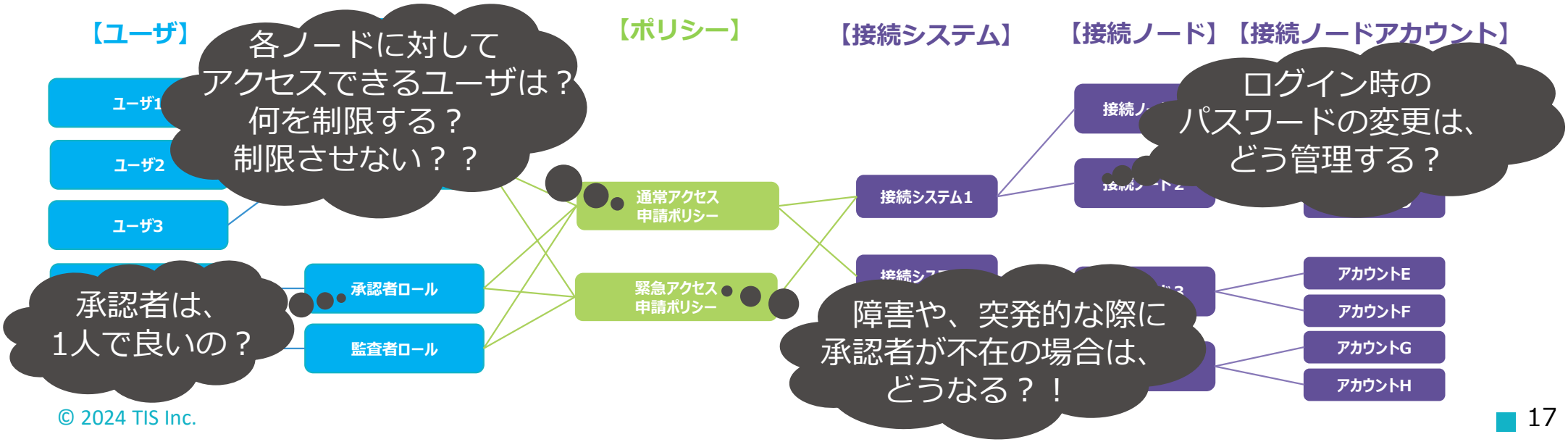
1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

Access Check の実装より、実はポリシー設計が大切です！

ID統制の観点より特権ID、管理対象ノード、アカウント、プロトコルなど、どのように紐づけて管理すべきか悩まれるケースが多くございます。

弊社では、これらポリシーとしてお客様からのヒアリングを行い、ご一緒に整理いたします！



TIS が考える “特権ID管理” を導入する際の「ご検討・導入ポイント」

1．特権ID と ユーザ と 制御 の紐づけ（＝ポリシー）

弊社は各ポリシーの設計要素(特権ID、ユーザ、接続ノード 等)とお客様のご利用要望をヒアリングと整理を繰り返し行い、ご要望に適したポリシー作成をご支援いたします。

＜現状把握と整理＞

ヒアリング

ご利用の要望

ポリシー整理

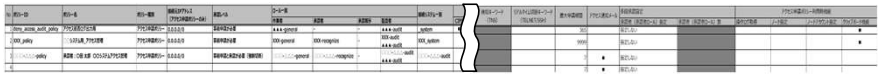
＜相談ポイント＞

・承認者は1人で良いのか？
・各ノードに対してアクセスできるユーザの何を制限する？制限させない？？
・障害や、突発的な際に承認者が不在の場合はどうなる？！
・ログインパスワードの変更の管理は？

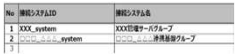
＜ポリシー設計＞

・承認者は1人で良いのか？
　→承認者となるユーザの整理
・各ノードに対してアクセスできるユーザの何を制限する？制限させない？？
　→ユーザとノードの紐づけの整理
・障害や、突発的な際に承認者不在の場合は？
　→運用に適したロールの整理
・ログインパスワードの変更の管理は？
　→接続ノードのアカウント運用の整理

■ポリシー 一覧

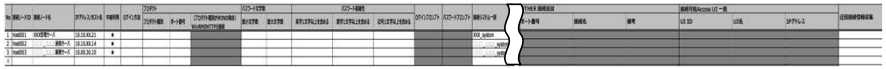


■接続システム 一覧



■接続ノードアカウント一覧

■接続ノード一覧



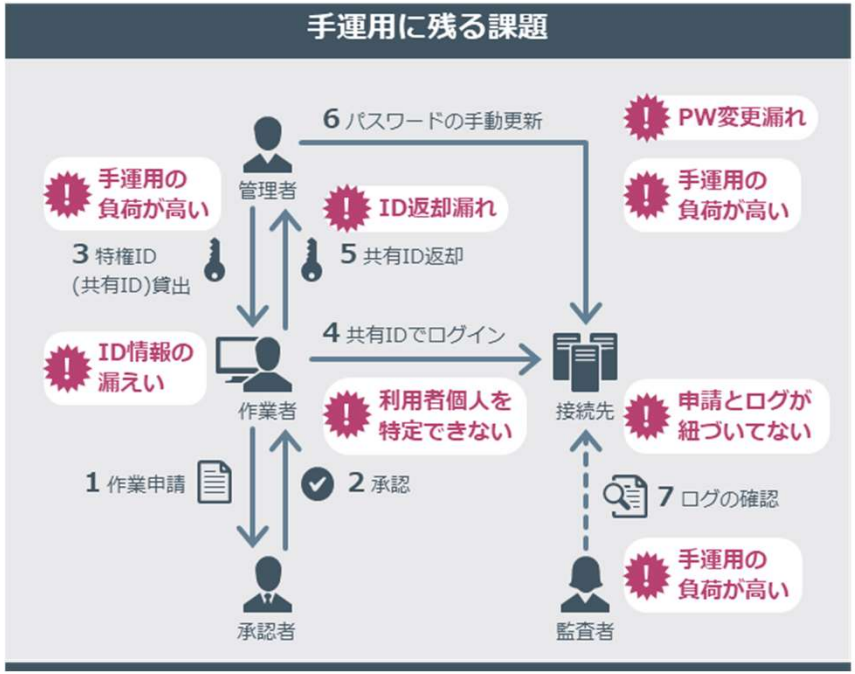
■ロール一覧

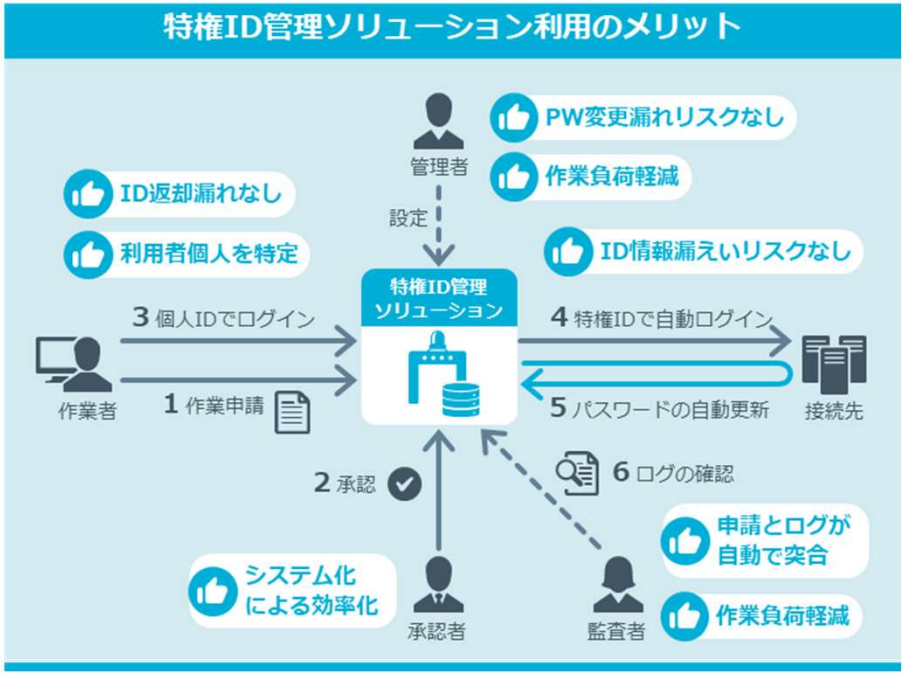
■ユーザ一覧

2．使えるシステム（機能するシステム）

2．使えるシステム（機能するシステム）

お客様の多くは、社内の監査や社内規定に準じた 特権ID管理とすることを、ご要望いただくケースが非常に多くございます。
弊社では、各種監査や法令基準における特権ID管理を行うため、 Access Check の機能、非機能だけではなく、お客様の**運用ルールに基づき最適な設計となるようご支援**させていただきます。
また、**ID統制の観点から運用面や社内規程に則したコンサルティングを含めたご支援**も可能です。





3．ネットワークを含めたシステム構成（Access Check の構成）

3．ネットワークを含めたシステム構成

弊社では**要件定義工程よりご支援させて頂き、Access Check 自体のご利用方法をヒアリングさせていただき、お客様の環境にあった構成をご提案**させていただきます。

【構成提案に向けたアプローチ】

1. 現状確認
2. ご利用のご要望確認
3. ヒアリング結果取り纏め
4. 要件に合わせた構成のご提案
5. 要件に合わせた構成の合意

■構成検討例

機能（例）

■インフラ
- **提供基盤の決定**
  →お客様環境にあう基盤(オンプレ / クラウド)の選定
- **システム構成**
  →Access Check コンポーネントの最適な構成
- **動作環境**
  →お客様のご利用規模に応じた動作環境

■特権ID管理（Access Check）
- **ID、パスワード管理**
  →お客様のID統制に応じた管理方法
- **ワークフロー(承認プロセス)**
  →お客様の運用に則したアクセス申請～承認のプロセス管理
- **AD連携**
  →社内アカウントを利用した Access Check ユーザ管理

非機能（例）

■保守・運用
- **冗長化設計**
  →お客様が考えるサービス継続性に則した冗長化構成
- **バックアップ**
  →お客様の運用に則したバックアップ
- **ログ保管**
  →お客様規程に則したログ保管場所、保管期間

TIS が考える “特権ID管理” を導入する際の「ご検討・導入ポイント」

3．ネットワークを含めたシステム構成 ～導入・運用が容易な「ゲートウェイ方式」～

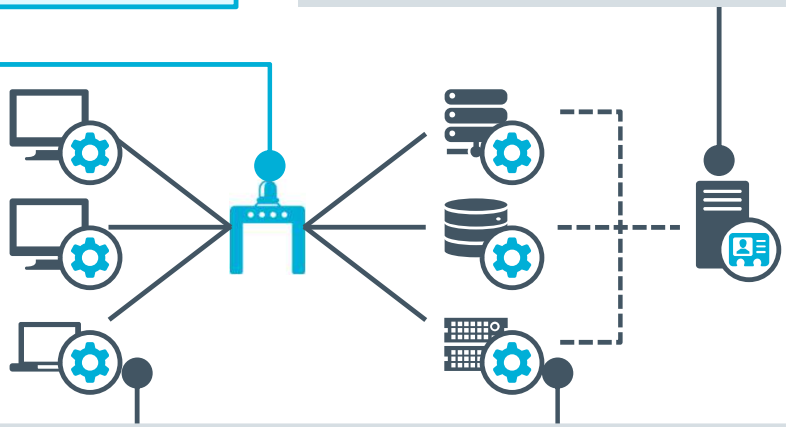
Access Check

ゲートウェイ方式（完全エージェントレス型）

クライアント端末と管理対象機器の間に関所（ゲートウェイ）を設置して、一元管理する方式。関所上で、個人ID管理、アクセス制御、及びログ管理を統合するため構成がシンプル。**管理対象機器が多い場合や、既存環境への影響を最小限にしたい場合**などに最適。

ID・パスワード貸出方式

管理対象機器の特権ID棚卸とパスワード貸出管理で制御する方式。
アクセス制御用にクライアントエージェントを必要としたり、認証用サーバを別途立てたりする必要がある。**特権IDが少ない場合や、統合ID管理システムが稼動済みの場合**などに最適。



エージェント方式

クライアント・エージェント型

アクセス元のクライアント端末ごとにエージェントをインストールする方式。
クライアントごとで、本人認証（特権ID利用者の特定）とログ取得を行う。**ログを詳細に取得したい場合や、管理対象機器への接続用端末が特定されている場合**などに最適。

サーバ・エージェント型

アクセス先の管理対象機器ごとにエージェントをインストールする方式。
管理対象機器ごとに個人ID管理、操作制御、ログ取得を行う。**物理コンソールでの接続を含めたアクセス制御とログを取得したい場合や、管理対象機器側で詳細な操作制御を行いたい場合**に最適。

TIS が考える “特権ID管理” を導入する際の「ご検討・導入ポイント」

3．ネットワークを含めたシステム構成　～導入・運用が容易な「ゲートウェイ方式」～

ゲートウェイ方式はエージェントレスのため、お客様システムの稼働影響が少ないため、
SIの観点から**新規システムだけでなく、既存環境への導入**にも最適と考えます。

比較項目	システム導入	システム運用	アクセス制御	ログ取得
おすすめ **ゲートウェイ方式**	◎ エージェントレスのため導入が容易	◎ 拡張性に優れ、システム構成がシンプルなため運用が容易	○ ゲートウェイでアクセス制御可能、迂回アクセス対策が必要※1	○ エージェントレスで取得可能 迂回アクセス対策が必要※1
サーバ・エージェント型	△ 各サーバへの導入影響がないか調査・検証が必須	△ メンテナンスごとに影響の調査・検証が必須	◎ ローカルログインを含めたきめ細かい制御が可能	◎ ローカルログインを含めたログの取得が可能
クライアント・エージェント型	○ 各クライアントへの導入影響がないか調査・検証が必須※2	△ アクセス制御とログ取得は別製品が必要となり、運用が煩雑	○ エージェント未導入の端末からのアクセス対策が必要	○ エージェント未導入の端末からのアクセスログは取得できない
ID棚卸・貸出方式	△ ID・パスワードの棚卸が必須 パスワード変更できないIDは別対策が必要	○ ID・パスワードの管理（定期棚卸など）が必須、パスワード変更できないIDは別管理	○ パスワード変更できないIDの対策が必要	△ ID貸出・利用のログは取得できるが、操作内容の取得のためには別の仕組みが必要

※1　ネットワーク機器で制限する、特権パスワードを秘匿化する、管理対象機器のログと突合する　等の対策が考えられます。
※2　Windows Terminal Serverを用意し、そこにクライアントエージェントを導入することで導入を簡素化するケースがあります。

TIS SI支援について

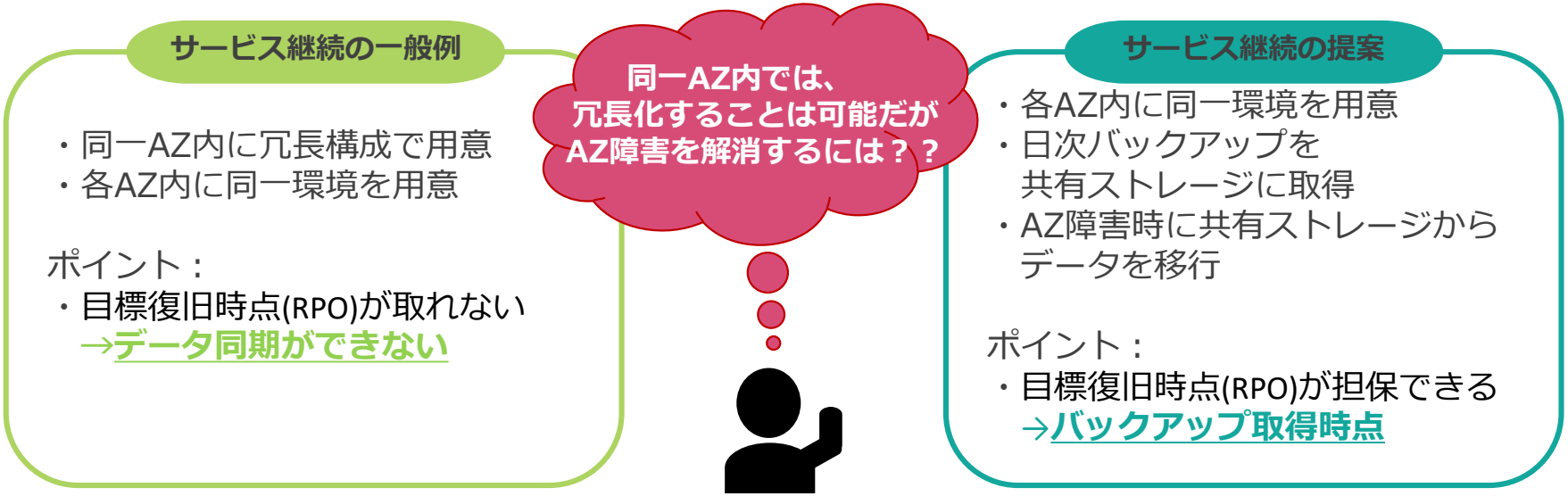
ケース１：災害対策を考慮したシステムにしたい
ケース２：SaaS の 特権ID も管理したい

ケース１：災害対策を考慮したシステムにしたい

クラウド環境のご利用の増加に伴い、Access Check を AWS上で構築される お客様も多くいらっしゃいます。そんな中、災害対策を考慮したシステム設計として、Access Check の仕様を考慮しつつ、AWS環境下において、お客様がご希望される災害対策のご提案を行ったケースとなります。

構成ご提案事例：

サービス継続性の観点にて、AWS環境でアベイラビリティゾーン(以下、AZ)における障害を考慮する場合のケースでのご相談をいただきました。AWS基盤上、物理障害のない状況において冗長化を組むことより、AZ障害でのサービス継続性が取れなくなることを懸念されていらっしゃいました。



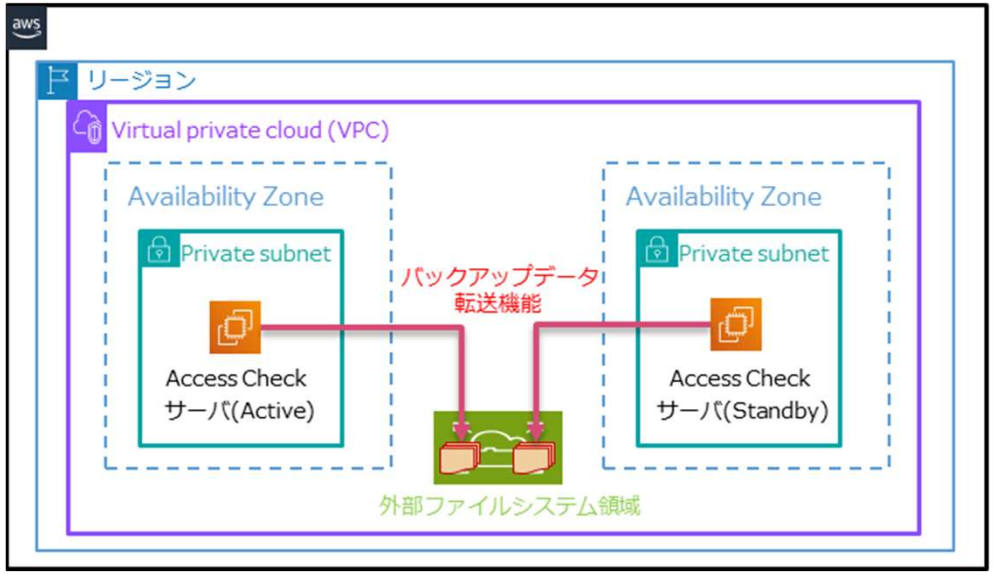
ケース１：災害対策を考慮したシステムにしたい

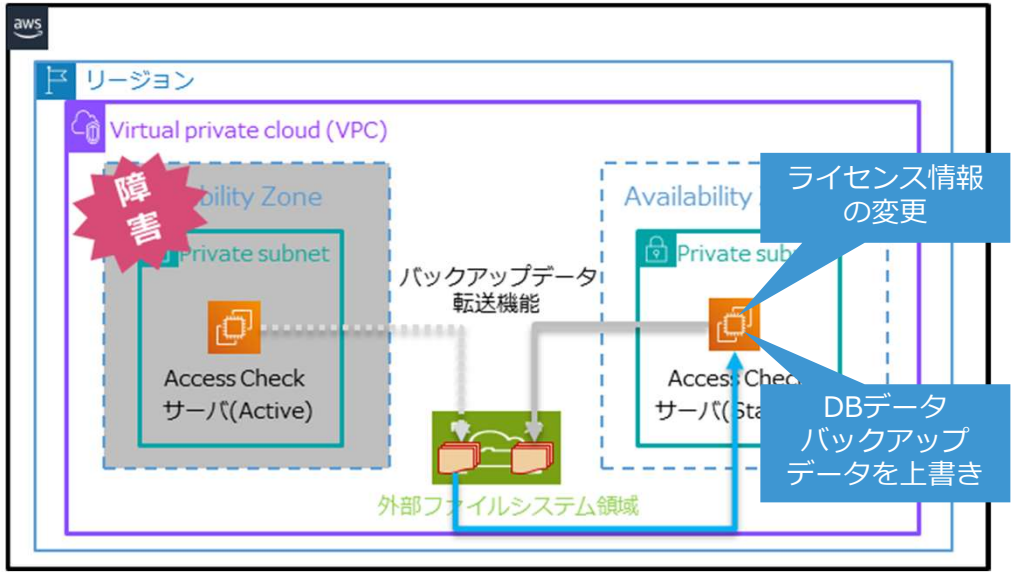
サービス継続の提案内容：

【バックアップデータ転送機能を転用したAZ障害時の対応】

■Access Check のバックアップデータ転送機能とは
バックアップ対象ファイル(操作ログ、日次レポート、DBデータ)を外部ストレージへ転送し、外部領域へバックアップする機能

■AZ障害時の切替え方法
Active側の外部ファイルシステム領域へ取得したバックアップデータを、Standby側のDB内にActive側のDBデータを上書きする。
また、Standby側はDBデータがActive側に置き換わったことを認識させるため、ライセンス情報も、Active側の内容に書き換えることでDBデータを認識することが出来る。





ケース２：SaaS の 特権ID も管理したい

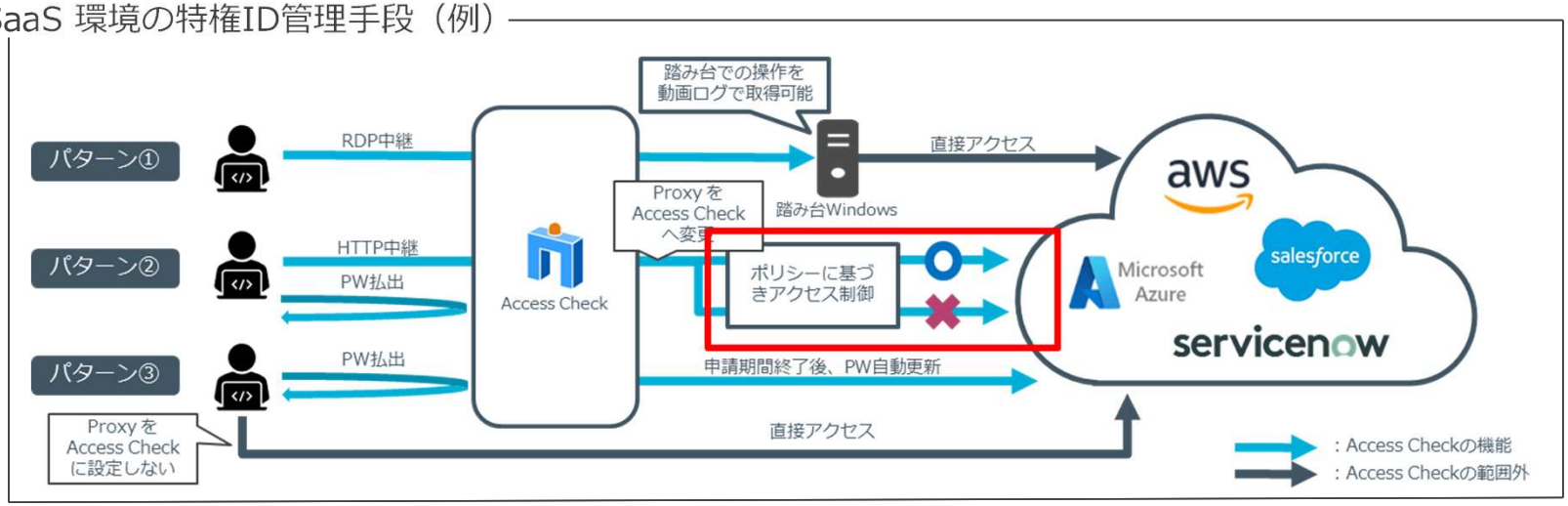
SaaS の 特権ID を Access Check で管理（申請・承認／アクセス制御／ログ取得）したいとの ご希望をいただくことが増えてきましたが、SaaS 側には不透明な部分もあり、特権ID管理のハードルは決して容易なものではありません。弊社は、簡易 PoC にて、お客様がご判断いただける情報をご提示いたしました。

SaaS中継の課題：

SaaS環境への自動中継アクセスについて、Access Check Ver6.2.0 より機能改善され、且つ、中継自動接続(ARC)機能を利用することで、格段にユーザ利便性が向上しています。

しかし、急激に SaaS環境が増え、お客様の利用増加と共に、SaaS環境の特権ID管理のご要望が増えています。

■SaaS 環境の特権ID管理手段（例）



ケース２：SaaS の 特権ID も管理したい　～中継自動接続（ARC）機能～

SecureCube Access Checkで提供している各種中継の開始処理を、クライアントアプリに統合
管理対象機器への接続処理をワンクリックで実行可能

※最大10接続まで同時起動が可能

1 | 個人IDでログイン

中継自動接続（ARC）ツールを実行後、SecureCube Access Checkの個人IDでログインします。

2 | 接続ノードを選択して中継開始

ログインしたユーザが中継を許可された接続ノードが一覧表示されます。中継を開始する接続ノードを選択して（複数可）、[中継開始]ボタンからワンクリックで接続できます。

中継自動接続ツール

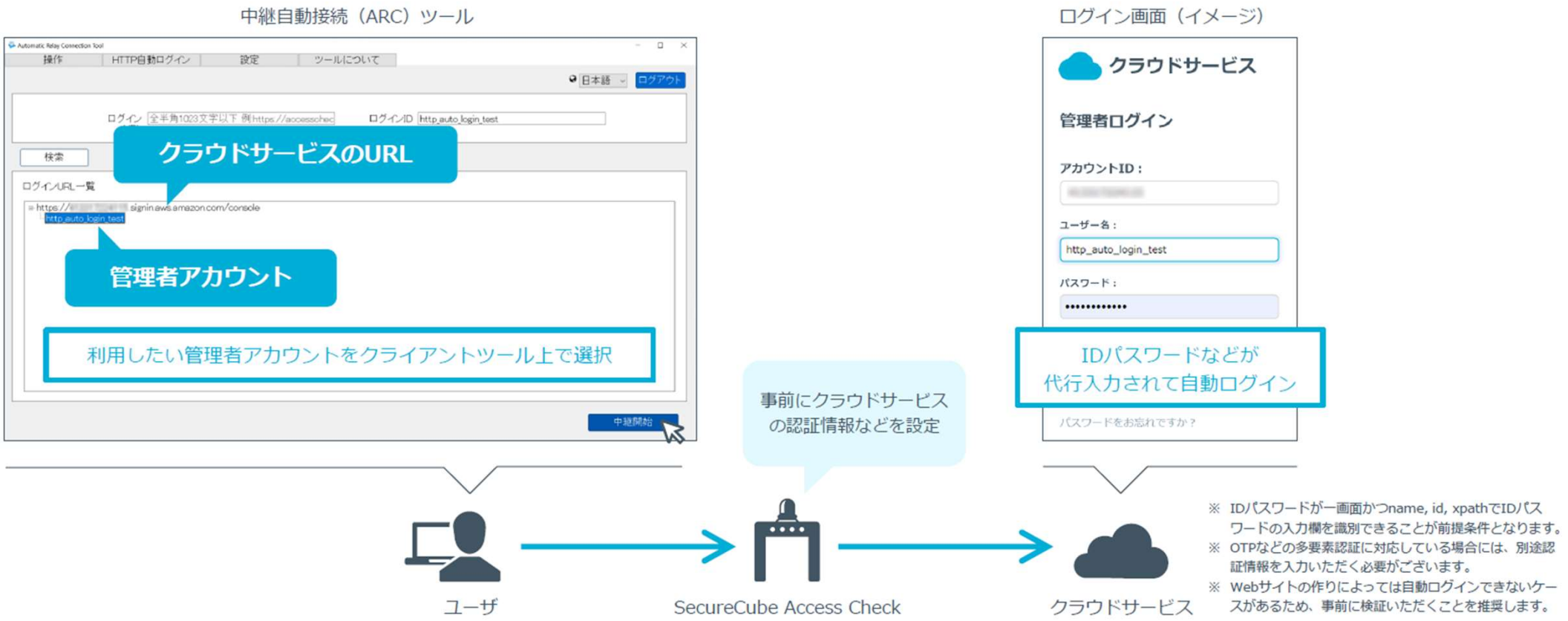
選択された接続情報に従い、次の動作を自動実行します。

1. クライアントソフトの起動
2. Access UIの指定
3. Access Checkへのログイン（ID・PW認証）
4. 接続ノードの指定
5. 接続ノードへのログイン（ID・PW認証）

※ ツールをお使いいただくには、ウィルスチェックの除外対象としていただく必要があります。
※ 接続ノードのIPアドレスがレンジ指定で登録されている場合、4.と5.は手動です。
※ 自動ログインOFFの接続ノードでは5.は手動、アカウント登録があればパスワードのみ手動です。
※ ログインIDを未選択の場合、5.は手動です。

ケース２：SaaS の 特権ID も管理したい　～中継自動接続（ARC）機能～

クラウドサービスの管理者アカウントを利用する際も、パスワードを秘匿化してログイン可能
中継自動接続ツールにて、利用したい管理者アカウントを選択するだけで自動で接続可能

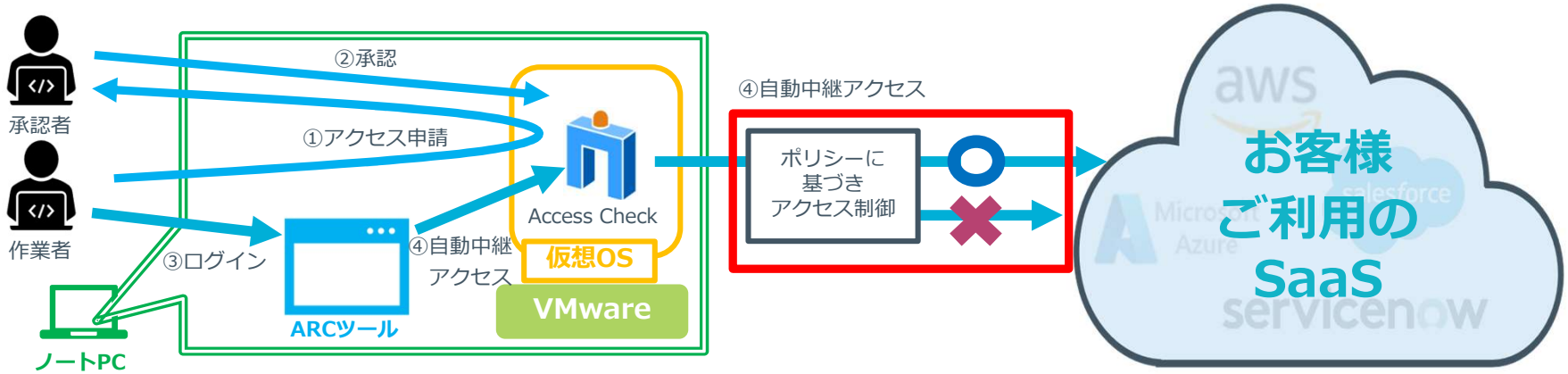


ケース２：SaaS の 特権ID も管理したい

弊社では簡易PoC環境を用意することで、**事前にお客様がご利用している SaaS環境に対する調査を可能**といたしました。これにより **PoC環境のご用意いただく準備期間や工数を費やすことなく、特権ID管理とする対象の SaaS を事前に把握**いただけます。

簡易対応チェックにおける作業プロセス

SaaS環境の簡易対応のチェックイメージ



簡易調査環境

ケース２：SaaS の 特権ID も管理したい　～お客様のリアルな ご感想～

SaaS の管理イメージが具体的になり、利便性も高いと高評価

ARCツールを使うことで
接続作業が、シンプルで
使い勝手が良さそうだ！

提案時点で
具体的に確認できたため、
社内へ導入根拠
が示せる！

接続イメージが
見れたため、導入後の
運用が安心だ！

最後に　～これから ご検討を はじめられる お客様へ～

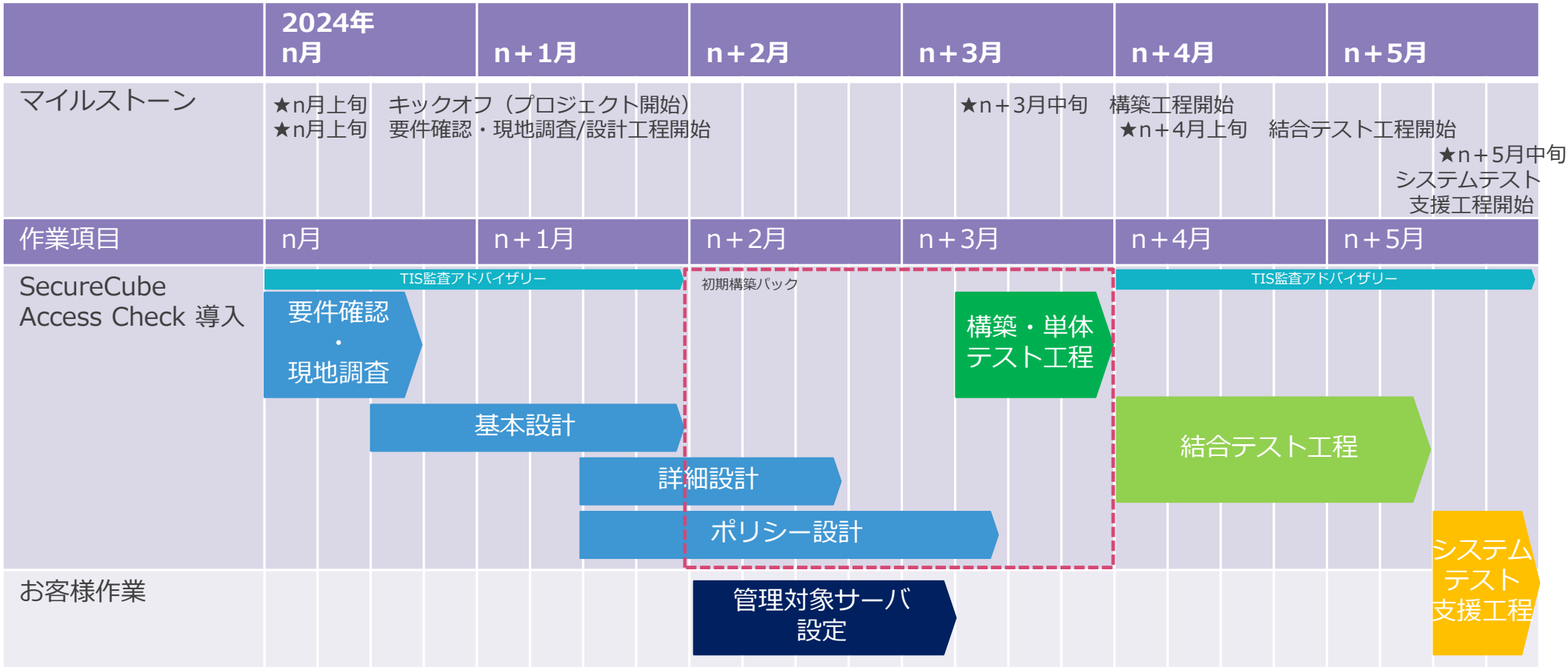
TIS が考える “特権ID管理” を導入する際のタスクとポイント

TIS SI支援 には、「ご検討ポイント」と「導入ポイント」の ノウハウ が詰まっています。

タスク		役割分担（弊社：ＴＩＳ）	役割分担（弊社：NRIセキュア）	成果物
要件定義	現状調査	• サーバ、ネットワーク環境などの現状調査	• Access Checkの仕様を踏まえた設計 アドバイザリ（メール、電話でのQ&Aベース）	
	アクセス要件定義	• 導入に伴うアクセス要件定義 - IPアドレス制御　- プロトコル制御　-ワークフロー　など		
	環境要件定義	• 導入に伴う環境要件定義 - 運用設計　- 性能設計　- ネットワーク設計など		
導入・構築	設定シート作成	• 初期設定に必要な下記設定シートを記入 - 『OS・ミドルパラメータシート』 - 『Access Checkパラメータシート』	• 設定シートの項目について説明 • 設定シート記入時のアドバイザリ(最大1ヶ月) • 設定シートの内容チェック	• 『OS・ミドルパラメータシート』 • 『Access Checkパラメータシート』
	SecureCube Access Check 導入準備	• ハードウェアおよびOSの調達 • データセンターへの設置 • OS・ミドルウェア導入作業の立会い	• OS・ミドルウェアのインストール • OS・ミドルウェアの初期設定	
	SecureCube Access Check 導入・設定	• Access Check 導入作業の立会い	• Access Check のインストール • Access Check の初期設定	
	稼働確認	• 稼働確認の立会い • （必要があれば）ネットワーク設定変更	• Access Check の稼働確認	• 『稼働確認チェックシート』
	操作説明	• 管理者操作説明への参加	• Access Check の管理者操作説明（最大2時間）	• 『作業完了報告書』
検証	マスタ登録	• ユーザ、ノード、ポリシーなどのマスタを登録	※基本的に保守サポート範囲内で対応します。	
	検証	• 検証環境での検証利用（必要に応じネットワーク設定変更）		

TIS が考える “特権ID管理” の導入スケジュール感 ～ ご参考イメージ ～

某お客様（監視対象数：約100台）向け SecureCube Access Check 導入スケジュール（案）となります。



TIS が考える “特権ID管理” の導入プロジェクトタスク ～ ご参考イメージ ～

SecureCube Access Check 導入時の作業工程となります。

要件確認・現地調査	基本設計	詳細設計	ポリシー設計	構築・単体テスト	結合テスト	システムテスト
要件定義	**Access Check の基本機能の設計**	**Access Check のパラメータ設計**	**特権管理対象のポリシーを定義**	**Access Check の構築・設定・単体テスト**	**ポリシー定義に合わせた動作テスト**	**お客様の受入れ確認テスト**
現状の業務内容について、**特権ID管理の観点からヒアリングを実施**し、機能要件を決定するためのご支援を行います。 (実施作業) a. ヒアリングシートの作成 b. ヒアリング実施 c. 要件定義書作成支援	要件定義を前提に**Access Check で実現する基本機能の設計**のご支援を行います。 合わせて、非機能の設計についてもご要望に合わせてご支援いたします。 (実施作業) a. 機能、非機能の基本設計の整理 b. 基本設計書作成	基本設計を基にAccess Check 導入に向け、実際の**構築時に使用するパラメータシートを用いてパラメータメータ設計**のご支援を行います。 (実施作業) a. パラメータシート作成	お客様の**特権ID管理の要件に合わせユーザと接続先の紐づけ管理方針や承認フローなどの決定**をご支援します。 (実施作業) a. 利用要件ヒアリング b. ポリシー整理・設計	Access Check の詳細設計を基にNRIS社にて**構築パックのサービスによる初期構築後の支援**を行います。 (実施内容) a. 単体テスト仕様書作成 b. 単体テスト実施	ポリシー設計に基づいた**ポリシーの反映と動作テスト** (実施内容) a. 結合テスト仕様書作成 b. ポリシー内容に則した動作テスト	お客様による動作確認テストに伴う**お問合せ対応** (実施内容) a. テスト実施に伴う操作や、挙動に対するお問合せ対応

TIS監査アドバイザリー
ご要望に応じて、ID統制の観点からお客様の規定に沿った機能が提供出来るかご支援します。

初期構築対応
NRIS社の構築パックサービスによる Access Check 構築作業

ITで、社会の願い叶えよう。

TIS INTEC
Group