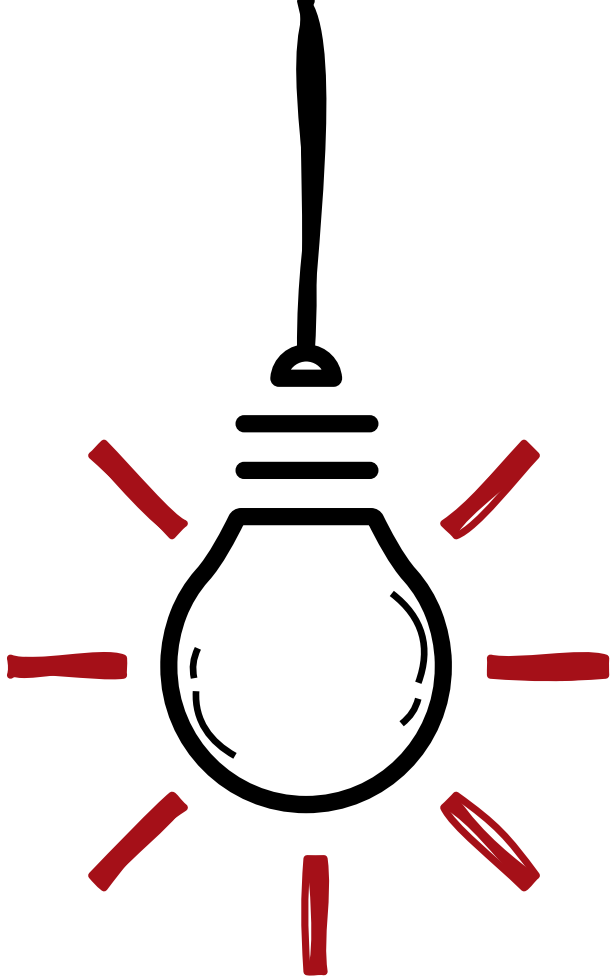
課題発掘セッション
ざんねんなエンタープライズ・アイデンティティ
～あなたの会社のゼロトラストは大丈夫？～

2021年11月26日

デジタルアイデンティティWG　宍戸 りさ
https://www.jnsa.org/active/std_idm.html



JNSA

キャリア 2年半の新人が **エンタープライズ・アイデンティティ** について考えてみた

本日のお話

00 自己紹介

01 ゼロトラストにおける
アイデンティティって??

02 具体的に
何を考えれば良いの??

03 アイデンティティの難しさ

04 アイデンティティの課題を
体系的に整理したい

05 まとめ

登壇者自己紹介

宍戸 りさ　*SHISHIDO, Risa*　情報処理安全確保支援士

(株)NTTデータ　セキュリティ技術部　サイバーセキュリティ統括部
NTT DATA Corporation, Security Engineering Dep., Cyber Security Sec.

“Digital Identity” をキーワードに セキュリティコンサルティングを行っています

- 国内通信事業者さま向け認証基盤見直しPJ
- 国内金融事業者さま向け認証関連要件検討PJ
- デジタルアイデンティティコンサルティングのための フレームワーク作成

など

広く一般の方々向けに情報発信もしています

- **サイバーセキュリティに関するグローバル動向四半期レポート**

「決済サービスに求められるセキュリティについて」ほか多数執筆

- **DATA INSIGHT**

ハンコをやめたい！その時考えるべきこと
https://www.nttdata.com/jp/ja/data-insight/2020/0706/

Zoomを安全に使うには？
https://www.nttdata.com/jp/ja/data-insight/2020/0917/

- **FMひがしくるめ に生出演**

https://www.youtube.com/watch?v=T-uyL1ADt8I

01 ゼロトラストにおける アイデンティティって??

コロナ禍の働き方変革で、情報の「守り方」も大きく変化しました

コロナ禍で働き方が大きく変わりました

働く場所の多様化

オフィスや取引先の拠点
だけでなく、
自宅やカフェ、
シェアオフィスから
仕事をするようになりました

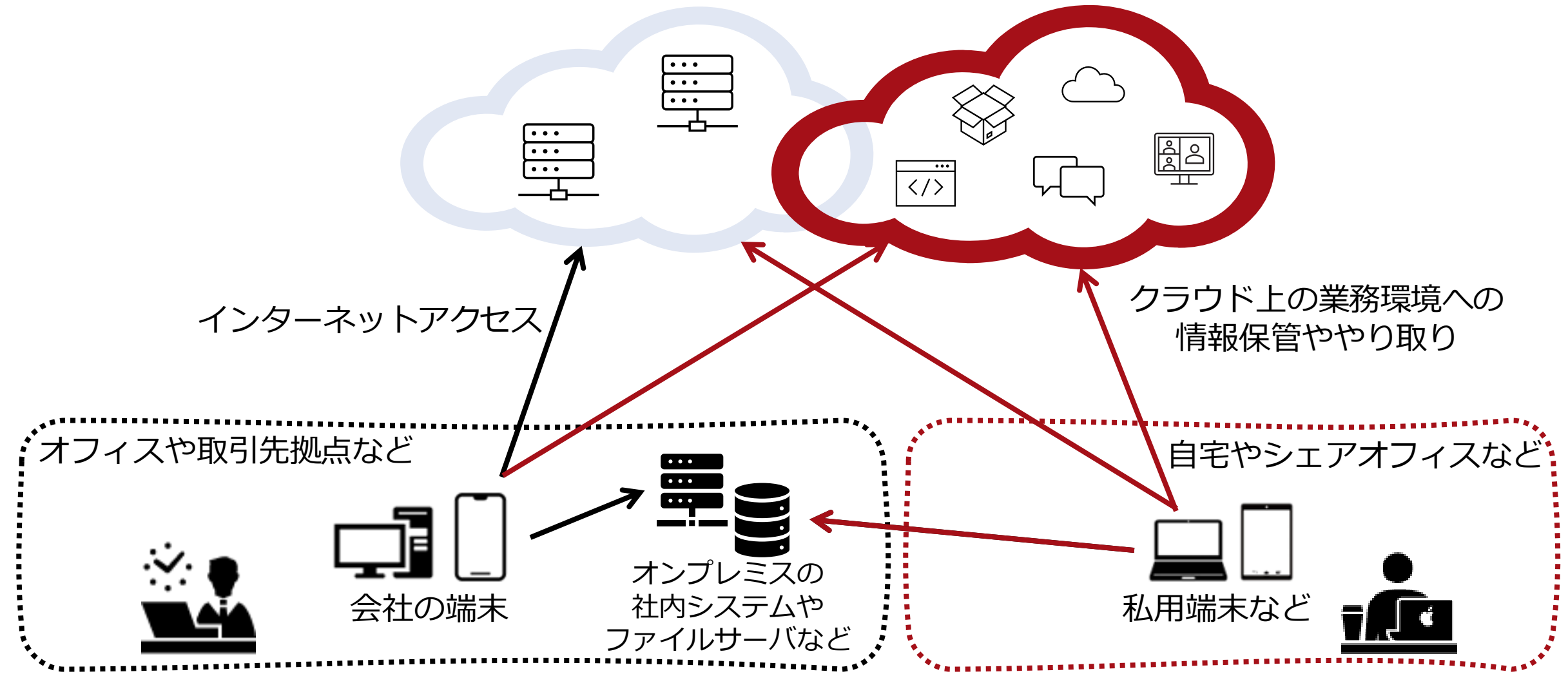
使う端末の多様化

会社備え付けのPC以外に、
貸与するモバイル端末
の種類も増え、
私用端末の業務利用を
許容するケースもあります

接続先の多様化

オンプレシステムや
社内のファイルサーバで
情報を管理していた環境から、
クラウドに業務環境が
大きく広がりました

コロナ禍で働き方が大きく変わりました

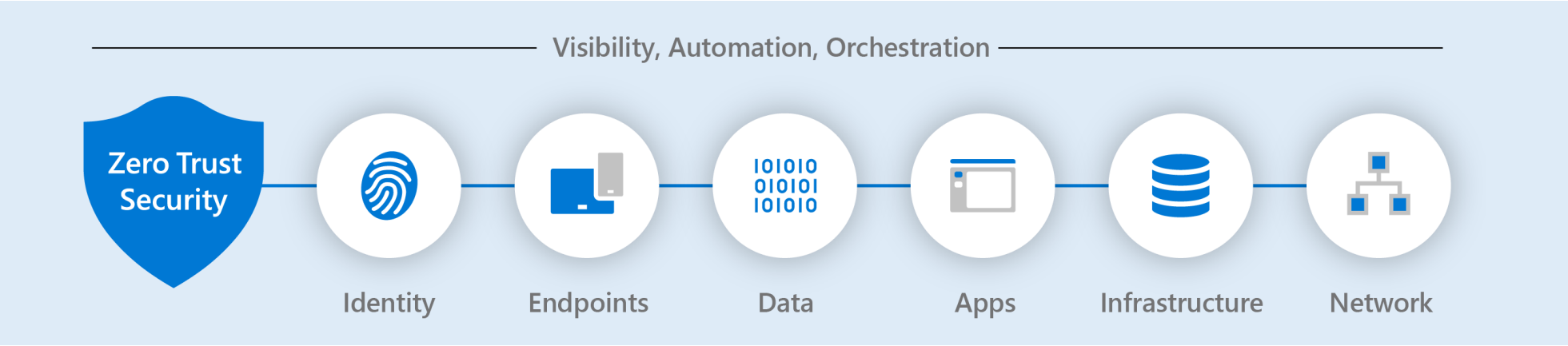


働き方の変革は「守り方」の考え方を変えました

	Before COVID-19	After/With COVID-19
働き方	• オフィスの自席で業務 • 主なアクセス先は社内、データセンタ等 • 対面で会議	• オフィスの自席　＋ 在宅/リモートで業務 • 社内/データセンタ ＋ クラウドなどへアクセス • 対面で会議　→ オンラインで会議
セキュリティ対応	• データセンタにセキュリティ機能を集約し、すべてのアクセスを経由させる • グローバルIPによるアクセス制御を実施	• クラウド/デバイスにセキュリティ機能を持たせ直接クラウドにアクセスする • IPによる制御に頼らず、多要素認証を行いアクセス制御を実施
守り方	極論、NWで強固に守れば良い	**ゼロトラスト**の概念が必要

ゼロトラストって何でしょう??

Microsoftは、下記順番で組織のセキュリティへのアプローチを成熟させ、
ゼロトラストの実装方法を最適化できると提唱しています



企業のFWの後ろにあるすべてのものが安全であると信じる代わりに、
Instead of believing everything behind the corporate firewall is safe,

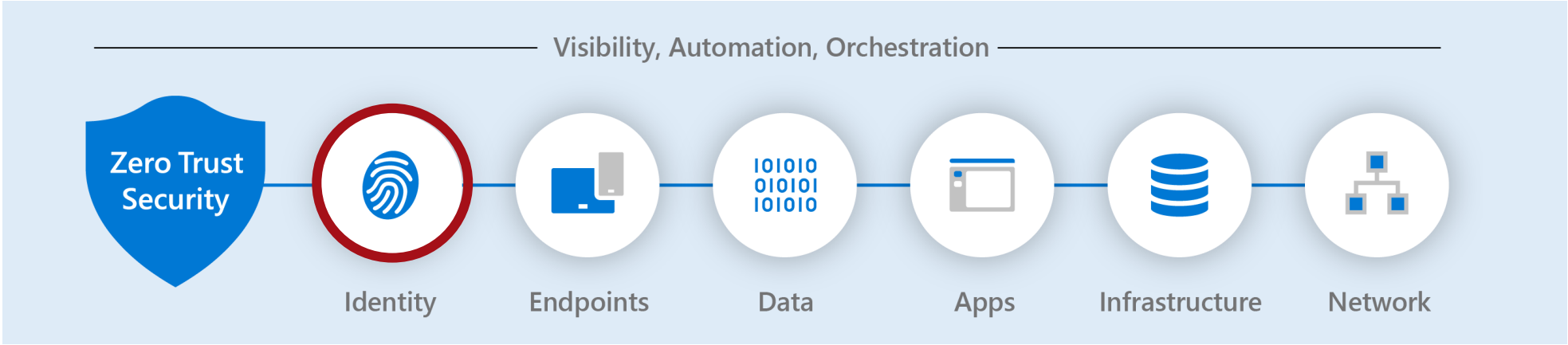
制御外のNWからのアクセスであるかのように各要求を検証します。
the Zero Trust model assumes breach and verifies each as though it originated from an uncontrolled network.

ゼロトラストモデルは、**「決して信じず、常に検証を」**ということを教えてくれます。
（中略）*the Zero Trust model teaches us to "never trust, always verify."*

https://docs.microsoft.com/en-us/security/zero-trust/

ゼロトラストの第一歩がアイデンティティ

Microsoftは、アイデンティティがゼロトラストを実装する上での
最初のキー要素であると提唱しています



アイデンティティって、なに？

社員証のこと？

認証に関係するもの？

ログインに使う “ID” のこと？

ID管理が重要ってこと？

何すればいいんだっけ？

https://docs.microsoft.com/en-us/security/zero-trust/

02 “アイデンティティ”って、具体的に何を考えれば良いの??

アイデンティティに関して気付けている課題は、多くの場合「氷山の一角」です

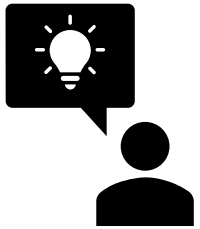
どのようなことを考えれば良いのでしょうか？

リモートワークに伴うセキュリティの課題の1つを
ゼロトラストの概念で解決することを例に考えてみます

クラウドはオンプレのシステムと違って
常に攻撃に晒されており、
PW 認証だけだと不正アクセス
のリスクが高い…

多要素認証をおこない
アクセス制御を実施したいが、
様々なクラウドに一律適用し、
適切に管理・運用するのはとても難しい…

クラウド・モバイル前提では
IP アドレスによる**アクセス制御**は
役に立たない…

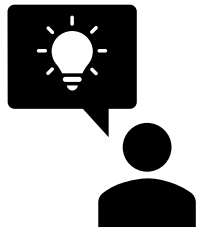


IDaaS* を導入すれば
利便性が上がりそうだ！

＊ クラウド経由でID管理やアクセス制御
などを提供するサービス

どのようなことを考えれば良いのでしょうか？

では、自社の要件にフィットするパッケージ製品や
サービスの選定のみを行えばよいのでしょうか？

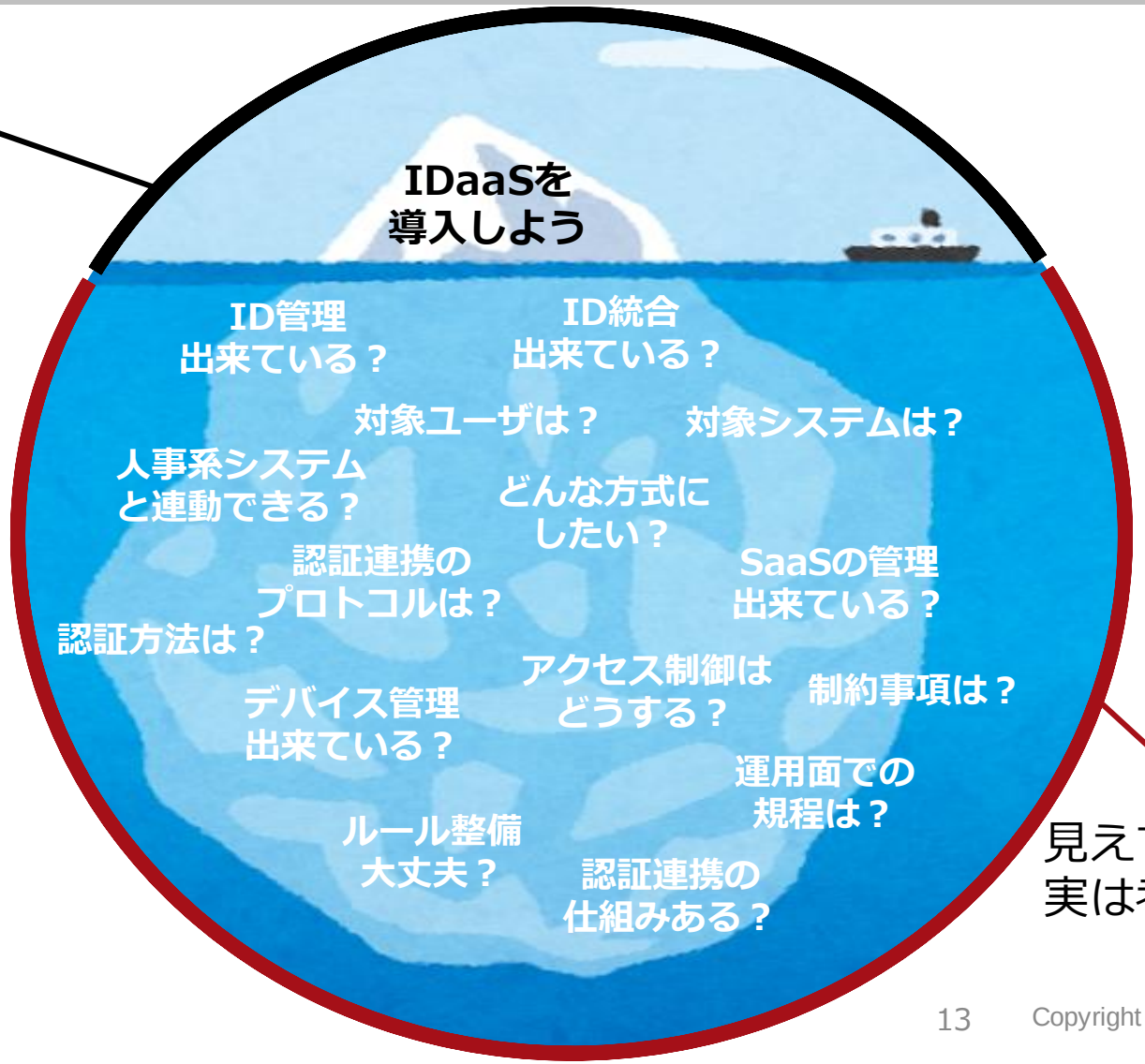


IDaaS* を導入すれば
利便性が上がりそうだ！

＊ クラウド経由でID管理やアクセス制御
などを提供するサービス

エンドユーザに見えている課題だけでは足りません

エンドユーザに
とっての課題感



見えている課題を達成するために
実は考える必要がある様々な要素

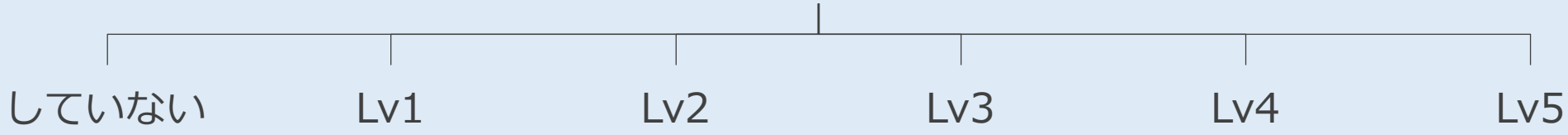
03 アイデンティティの難しさ

アイデンティティの分野は、思っているよりも複雑です

こんな難しさがあります

セキュリティの分野でよく行われるリスクアセスメントでは、
例えばこんなヒアリングが可能です

インターネットとの接続点に
IDS/IPSを設置していますか？



Lv1:初期　Lv2：管理された　Lv3：定義された　Lv4：定量的に管理された　Lv5：最適化している


ある程度明確なベストプラクティス（こうあるべき）が存在し、実施レベルを定量評価できる


お客さまの状況によって回答内容がそこまで変わらない（ある程度想定できる）

こんな難しさがあります

同じようにアイデンティティについてヒアリングしようとするとこうなります

従業員って
どこまで含む？

SaaSはやりたいが
できていない

システム数多くないし、
不便してないからSSOは不要

オンプレはできている

従業員が使うシステムで
SSOは実現できていますか？

SaaSは許可制なので
乱立しているから
管理しきれない

オンプレの中でも
一部だけできている

オンプレとSaaSの間まで
含めてできている

オンプレの中には
こういう種別があって…

- お客さまによって状況はまちまちで、明確なベストプラクティス（こうあるべき）がない
- 前提条件によって分岐させようとすると分岐数が膨大になり、結果の整理が難しくなる
- 一概に「良い/悪い」を定義できず、実施レベルを定量評価できない

普通に課題と原因を分析しようとするとこうなります

ヒアリングで見えた課題

- ID間のID払出数に不整合が生じている
- ・・・
- ID棚卸が手作業、人事情報と連携していないものもある
- ID払出し可否の統一的なルールがない
- ・・・
- ID払出し・アクセス権付与がシステム毎に行われている
- システム利用者個人を特定できない共有IDがある
- ・・・
- ID/PW発行・管理ルールが不明瞭
- パスワード運用がシステム毎に異なる
- ・・・
- ID登録ミスに気づく仕組みがない

原因

- ID体系が複数存在する
- ・・・
- ID管理部門が複数存在する
- ID管理の明確なルールが無い
- ・・・
- ID管理の運用が形骸化している
- 申請手続きがシステム毎に異なる
- 共有IDを利用している

※過去に弊社で実施した課題の整理結果の一部。
本当はもっと数が多くて複雑でした。

- エンドユーザに見えている課題から、原因を紐解くのが難しいケースが多い
- 原因の素因数分解が難しい
- 課題と原因が N:M で関連しており、紐解きが困難
- 課題の全体像や、解決の優先度が見えてこない
- かなり分野に精通した有識者にのみ成せる業…

04 アイデンティティの課題を体系的に整理したい

エンタープライズ・アイデンティティの課題を整理する枠組みを作ってみました

アイデンティティを整理する軸

（エンタープライズ）アイデンティティに関する既存の枠組みには例えばこんなものがあります

NIST SP800-63	NIST（アメリカ国立標準技術研究所）が発行している ”Digital Identity Guideline” 次のページで紹介する観点でアイデンティティ保証レベルを定義しているガイドライン https://pages.nist.gov/800-63-3/
ISO/IEC 24760	ISOによる ”IT Security and Privacy -A framework for identity management-” アイデンティティ管理に主眼をおき、用語や概念を定義している https://www.iso.org/standard/77582.html
AAAモデル	ITシステムにアクセスしてきたユーザが正しいかを確認し、アクセス許可を与え、その情報を記録し管理するという、セキュリティの考え方のモデルの1つ https://www.designet.co.jp/faq/term/?id=QUFB
JNSA DI WGによるチェックリスト	JNSA DI WG が2017年に作成した「ID管理システム導入における現状把握チェックリスト」 どの程度ID管理ができているのか、どの部分が不足しているのかを知るためのワークシート https://www.jnsa.org/result/2017/std_idm/

アイデンティティを整理する軸

	身元確認 Proofing	当人認証 Authentication	認可 Authorization	認証連携 Federation	証跡管理 Accounting	ライフサイクル管理 Lifecycle Management
NIST SP800-63	●	●		●		
ISO/IEC 24760	●	●		●		●
AAAモデル		●	●		●	
JNSA DI WGによる チェックリスト	●	●	●		●	

エンタープライズ・アイデンティティで重要な6軸

身元確認　Proofing

物理的な ”その人” と
電子的な “ID” の紐づけ

当人認証
Authentication

持ち主当人による
ID の使用かどうかの確認

認可
Authorization

アクセス権限の制御と
サービスの提供

認証連携　Federation

複数サービス間での
アカウントの紐づけ

証跡管理　Accounting

利用状況や履歴の記録

ライフサイクル管理
Lifecycle Management

アカウントの状態管理

エンタープライズ・アイデンティティで重要な6軸

身元確認　Proofing

物理的な”その人”と
電子的な“ID”の紐づけ

当人認証
Authentication

持ち主当人

認可
Authorization

アクセス権限の制御と
サービスの提供

問題はこれらの関係性！
案外複雑＆考えなければいけないことが多い！

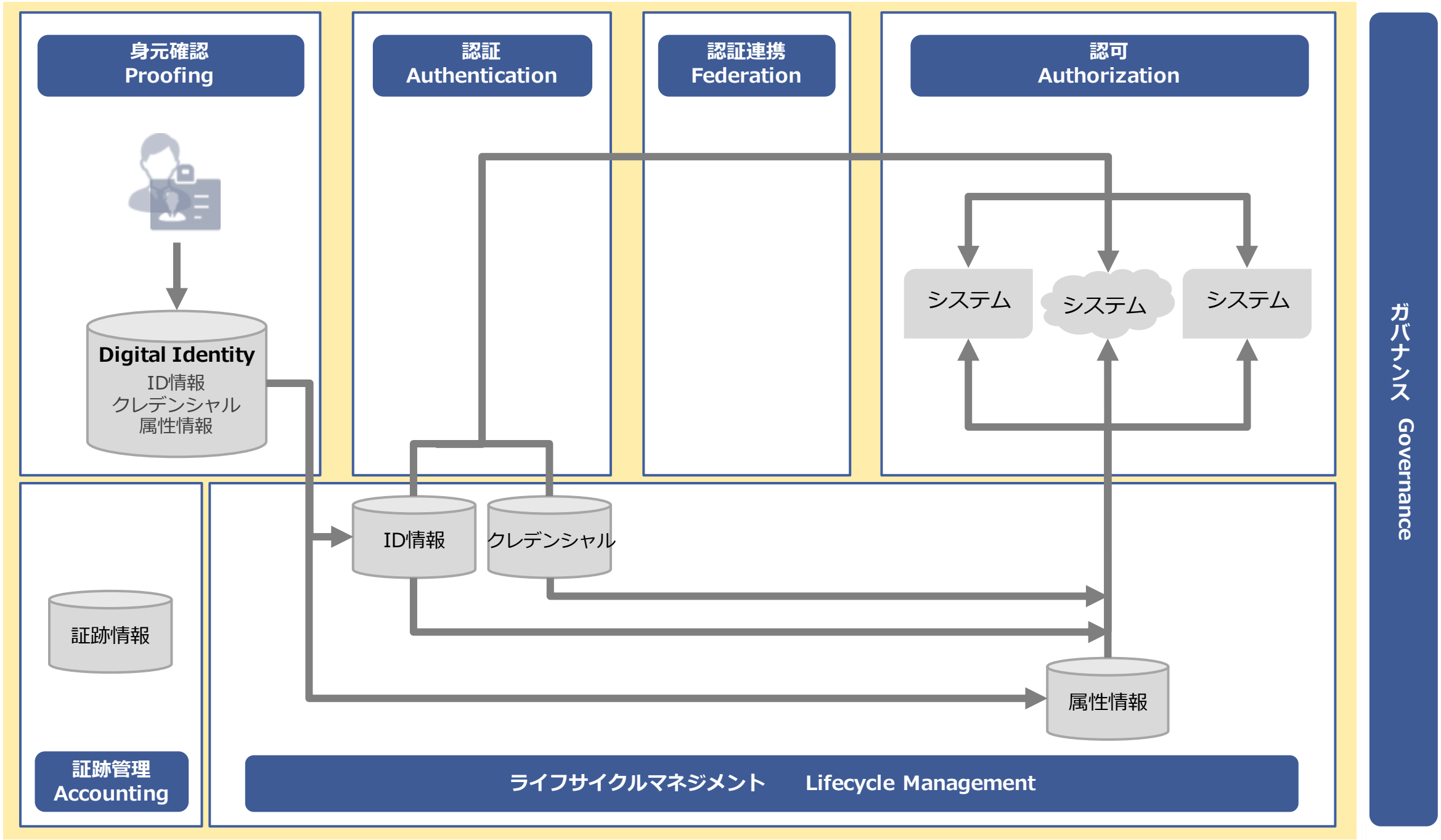
認証連携　Federat

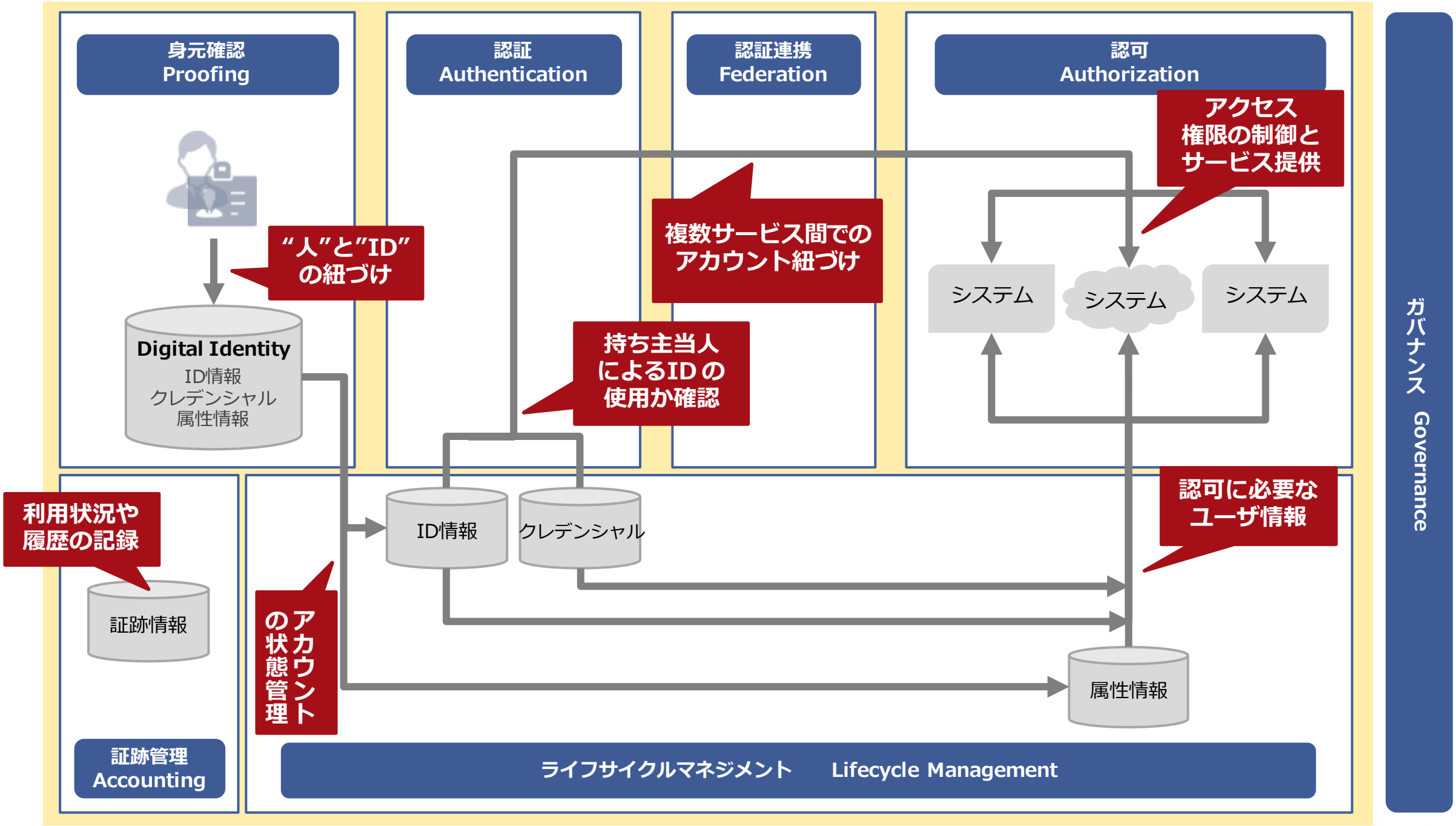
複数サービス間での
アカウントの紐づけ

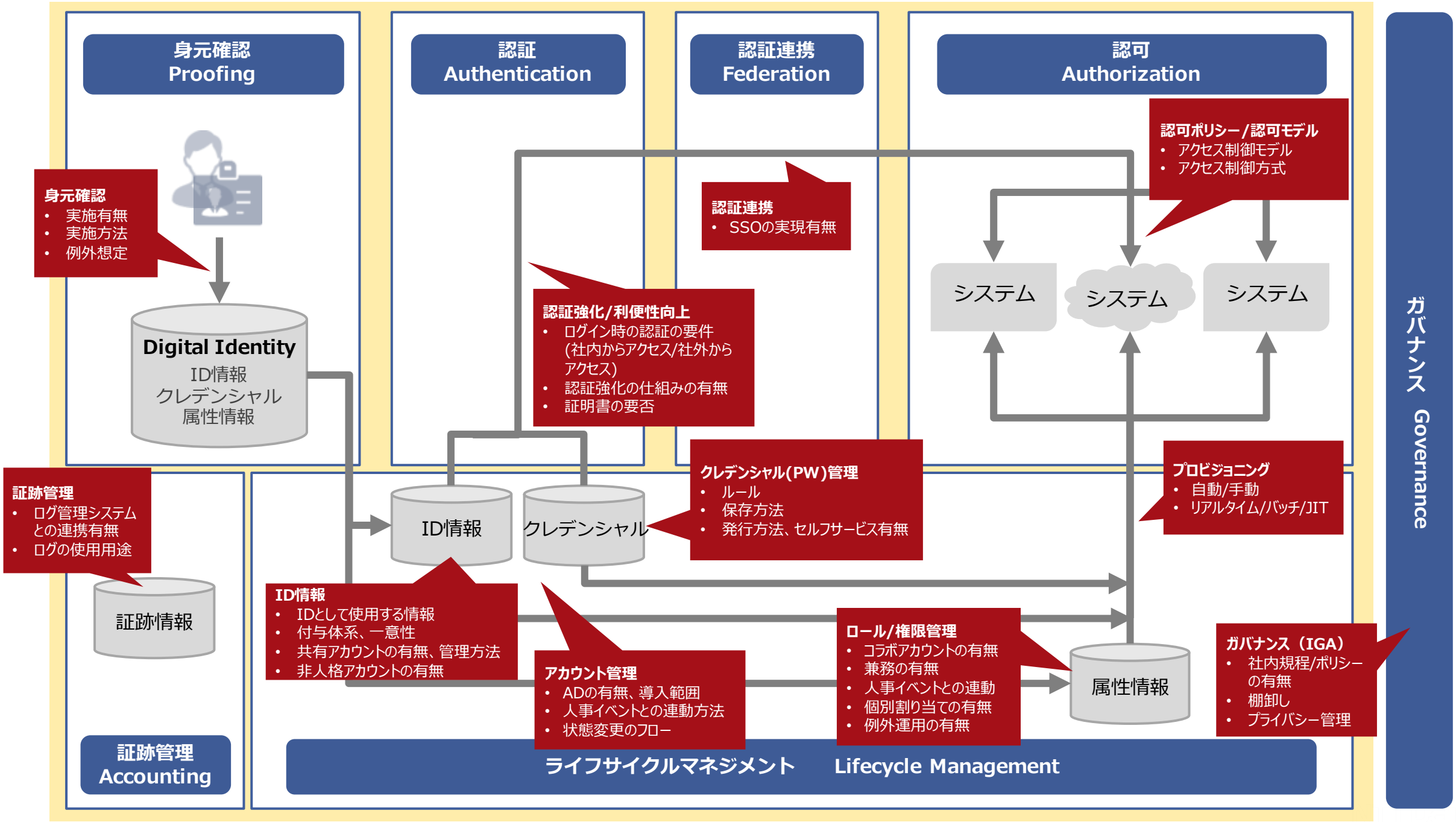
利用状況や履歴の記録

ライフサイクル管理
Lifecycle Management

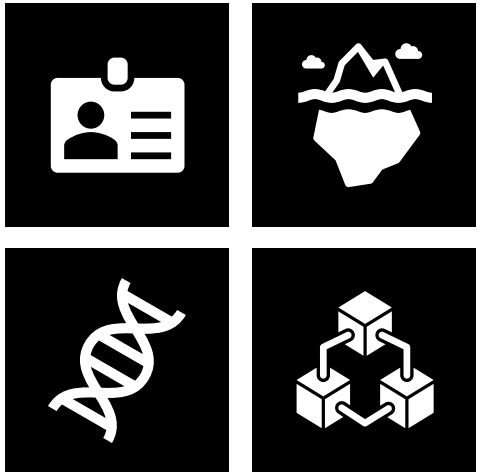
アカウントの状態管理


身元確認
Proofing
認証
Authentication
認証連携
Federation
認可
Authorization
Digital Identity
ID情報
クレデンシャル
属性情報
システム
システム
システム
ID情報
クレデンシャル
証跡情報
属性情報
証跡管理
Accounting
ライフサイクルマネジメント　Lifecycle Management
ガバナンス　Governance


身元確認
Proofing
認証
Authentication
認証連携
Federation
認可
Authorization
“人”と”ID”
の紐づけ
Digital Identity
ID情報
クレデンシャル
属性情報
複数サービス間での
アカウント紐づけ
持ち主当人
によるIDの
使用か確認
アクセス
権限の制御と
サービス提供
システム
システム
システム
ガバナンス Governance
利用状況や
履歴の記録
証跡情報
アカウント
の状態管理
ID情報
クレデンシャル
認可に必要な
ユーザ情報
属性情報
証跡管理
Accounting
ライフサイクルマネジメント Lifecycle Management


身元確認
Proofing
認証
Authentication
認証連携
Federation
認可
Authorization
ガバナンス Governance
身元確認
• 実施有無
• 実施方法
• 例外想定
Digital Identity
ID情報
クレデンシャル
属性情報
認証連携
• SSOの実現有無
認可ポリシー/認可モデル
• アクセス制御モデル
• アクセス制御方式
システム
システム
システム
認証強化/利便性向上
• ログイン時の認証の要件
(社内からアクセス/社外から
アクセス)
• 認証強化の仕組みの有無
• 証明書の要否
証跡管理
• ログ管理システム
との連携有無
• ログの使用用途
ID情報
クレデンシャル
クレデンシャル(PW)管理
• ルール
• 保存方法
• 発行方法、セルフサービス有無
プロビジョニング
• 自動/手動
• リアルタイム/バッチ/JIT
証跡情報
ID情報
• IDとして使用する情報
• 付与体系、一意性
• 共有アカウントの有無、管理方法
• 非人格アカウントの有無
アカウント管理
• ADの有無、導入範囲
• 人事イベントとの連動方法
• 状態変更のフロー
ロール/権限管理
• コラボアカウントの有無
• 兼務の有無
• 人事イベントとの連動
• 個別割り当ての有無
• 例外運用の有無
属性情報
ガバナンス（IGA）
• 社内規程/ポリシー
の有無
• 棚卸し
• プライバシー管理
証跡管理
Accounting
ライフサイクルマネジメント Lifecycle Management

05 まとめ

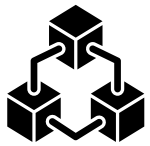


奥深さ・面白さ、分かっていただけましたか？

アイデンティティは
ゼロトラスト環境実現の
ための第一歩です

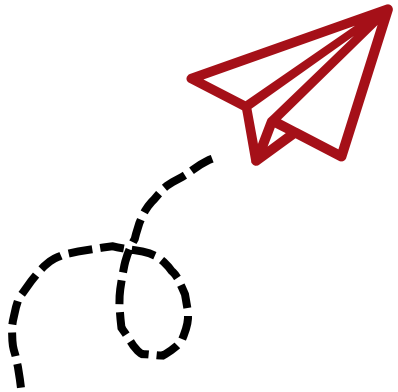
多くの場合、アイデンティティ
に関して見えている課題は
氷山の一角です

エンタープライズ
アイデンティティの課題と原因は
複雑に絡み合っています



エンタープライズ
アイデンティティの全体像を整理
するための枠組みを作成しました

エンタープライズ・アイデンティティって具体的に何を考えればよいのか、
考えるヒントになれば幸いです



ご清聴ありがとうございました☺

本資料に関するお問い合わせは以下までお願いいたします

NTTデータ セキュリティ技術部
security-contact@kits.nttdata.co.jp