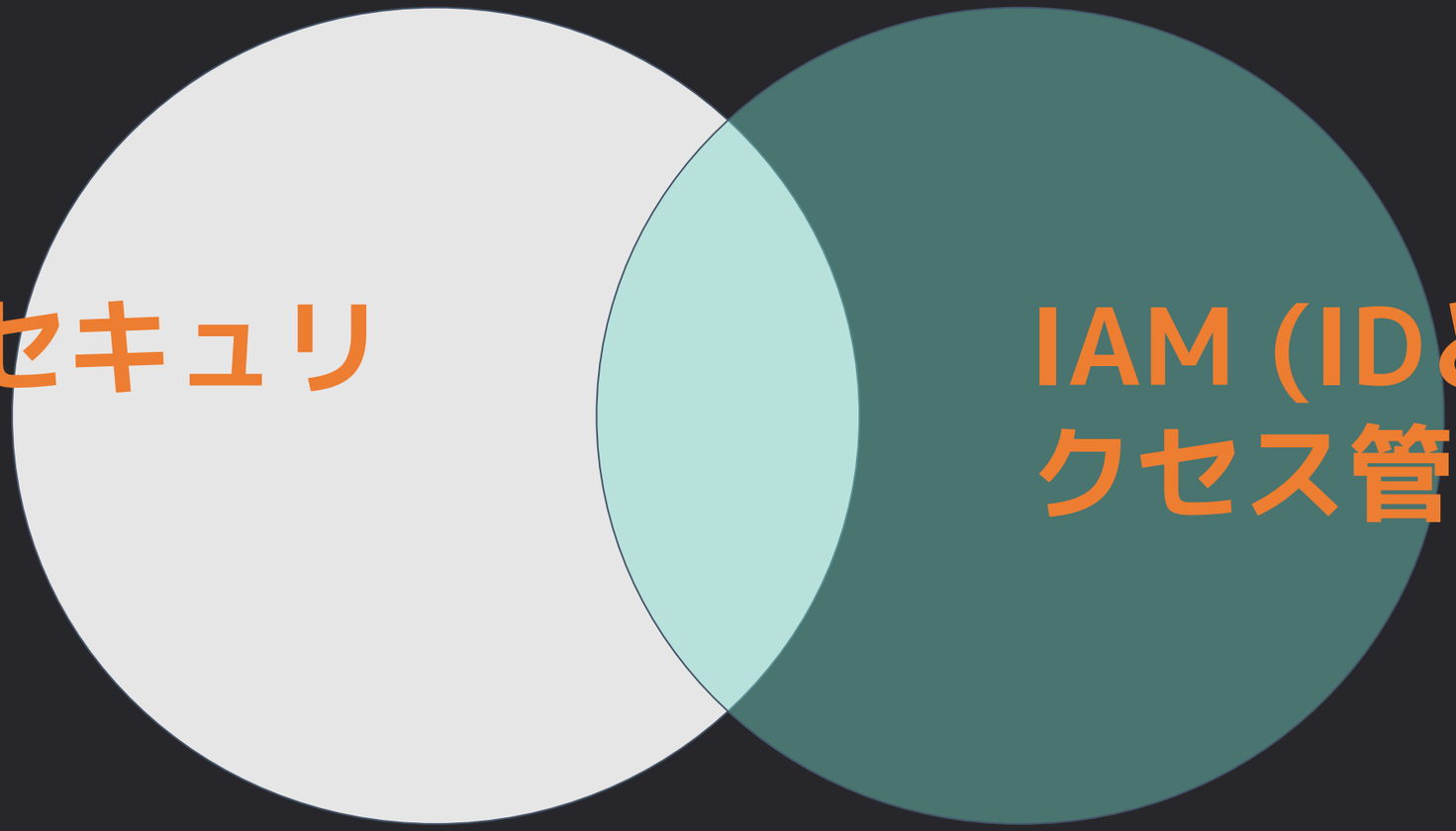
ID管理の死角：なぜ脅威は減らないのか？

～現場の課題と解決への道筋～

by Nat Sakimura / 崎村夏彦

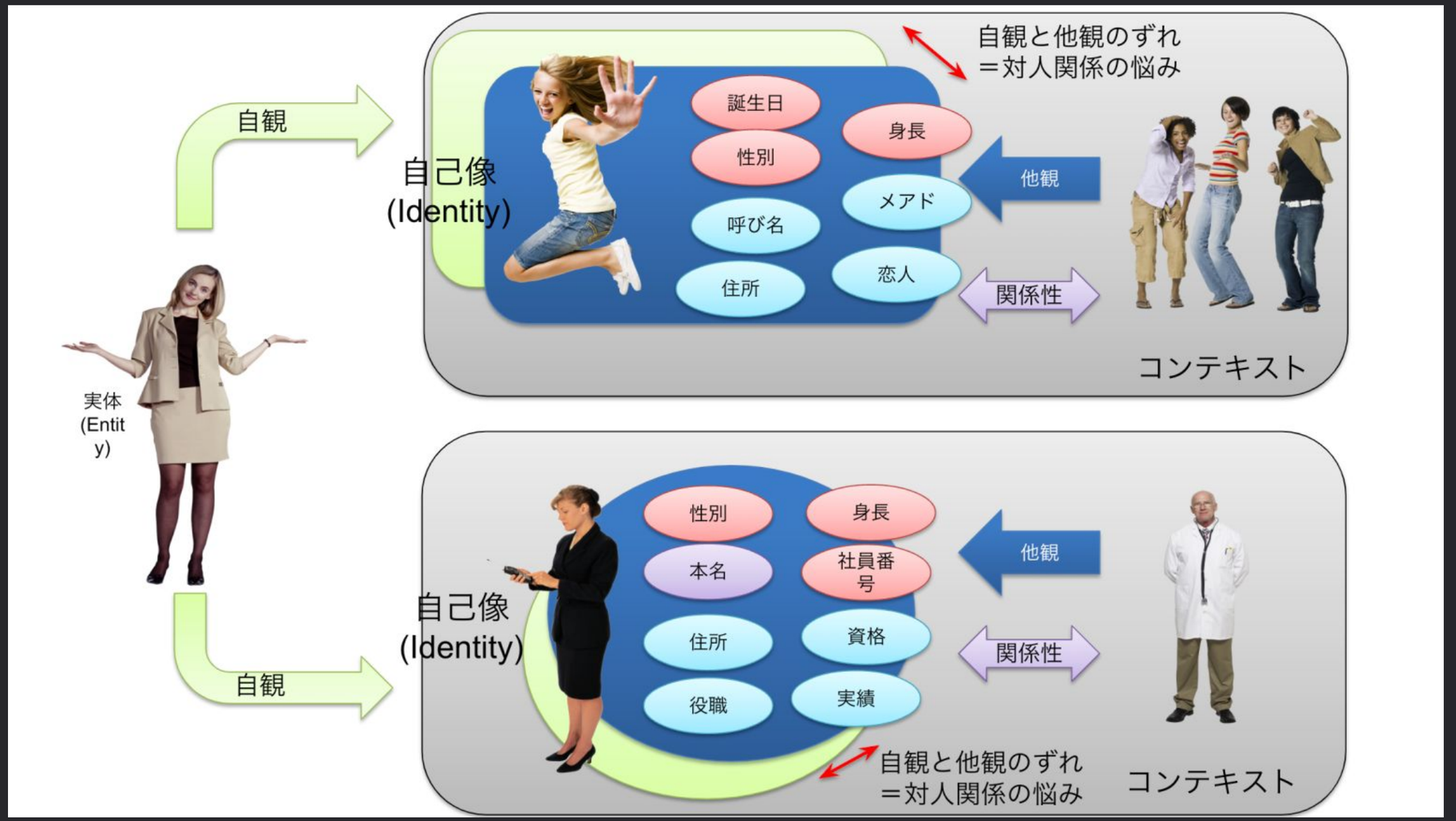


（出所）筆者

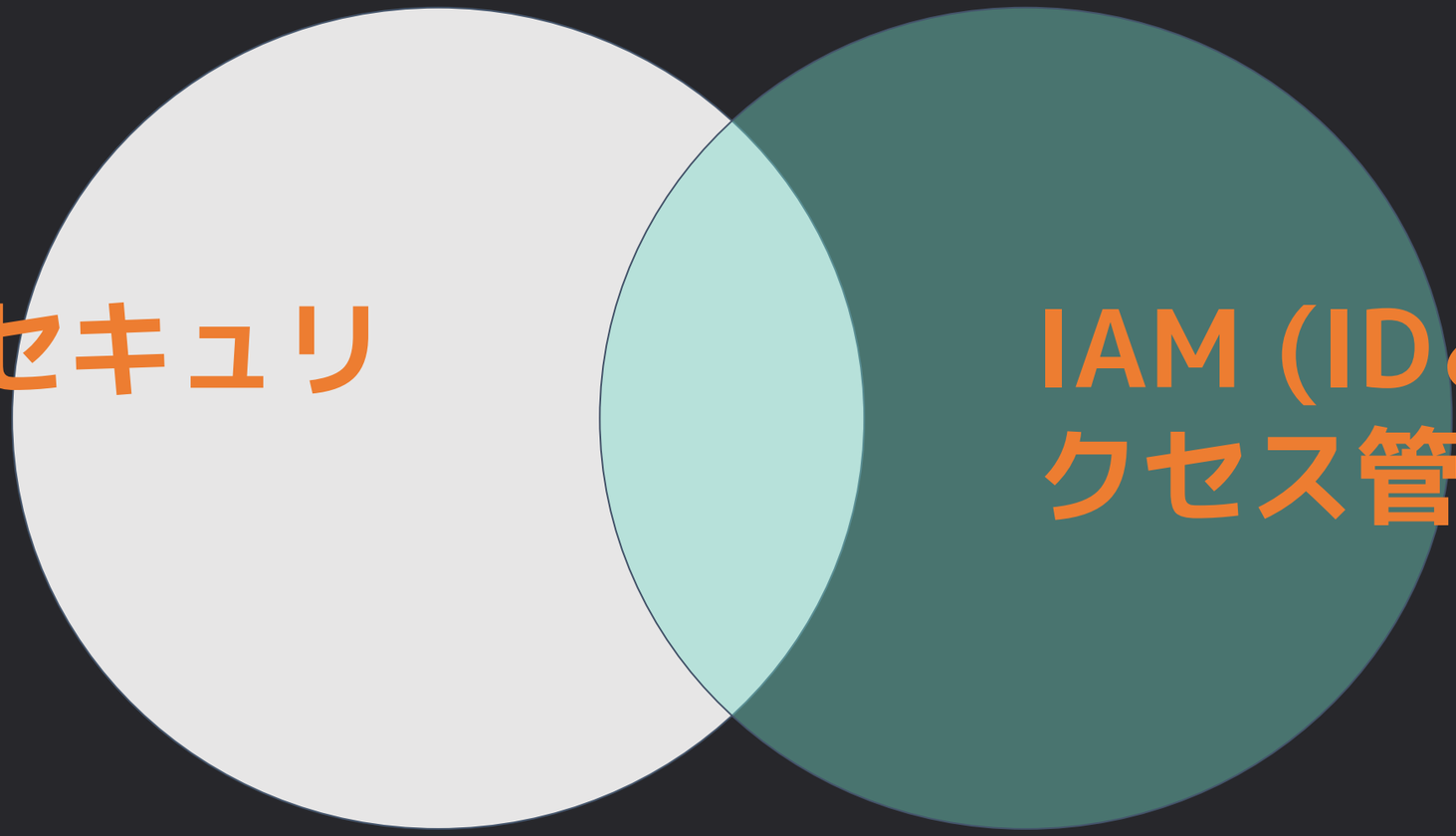
- グーグルがパスポートのウォレット搭載を発表～Google Walletで実現する新時代のデジタルID
- 「マイナ免許証」25年3月導入へ　住所変更ワンストップで。更新時講習もオンラインに。
- デジタル庁デジタル認証アプリ
- Apple、iPhoneにマイナンバー機能を搭載へ–Appleウォレットの身分証明書機能は米国外で初
- 欧州デジタルアイデンティティフレームワーク～デジタルウォレットで資格確認が可能に

より詳しい一覧は
https://www.sakimura.org/2024/08/6233/

アイデンティティの表明と検証



（出所）筆者



（出所）筆者

Nat Sakimura

崎村夏彦 – OpenID Foundation 理事長

https://www.youtube.com/@55id

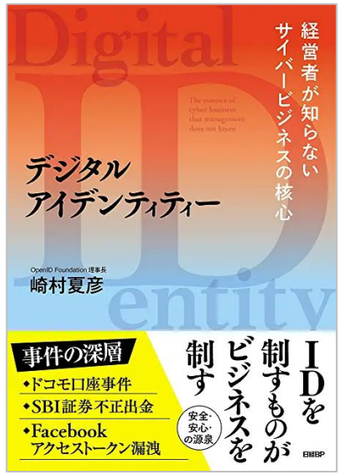
https://www.linkedin.com/in/natsakimura

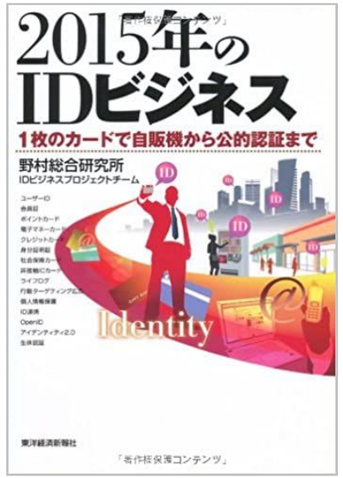
https://www.sakimura.org/

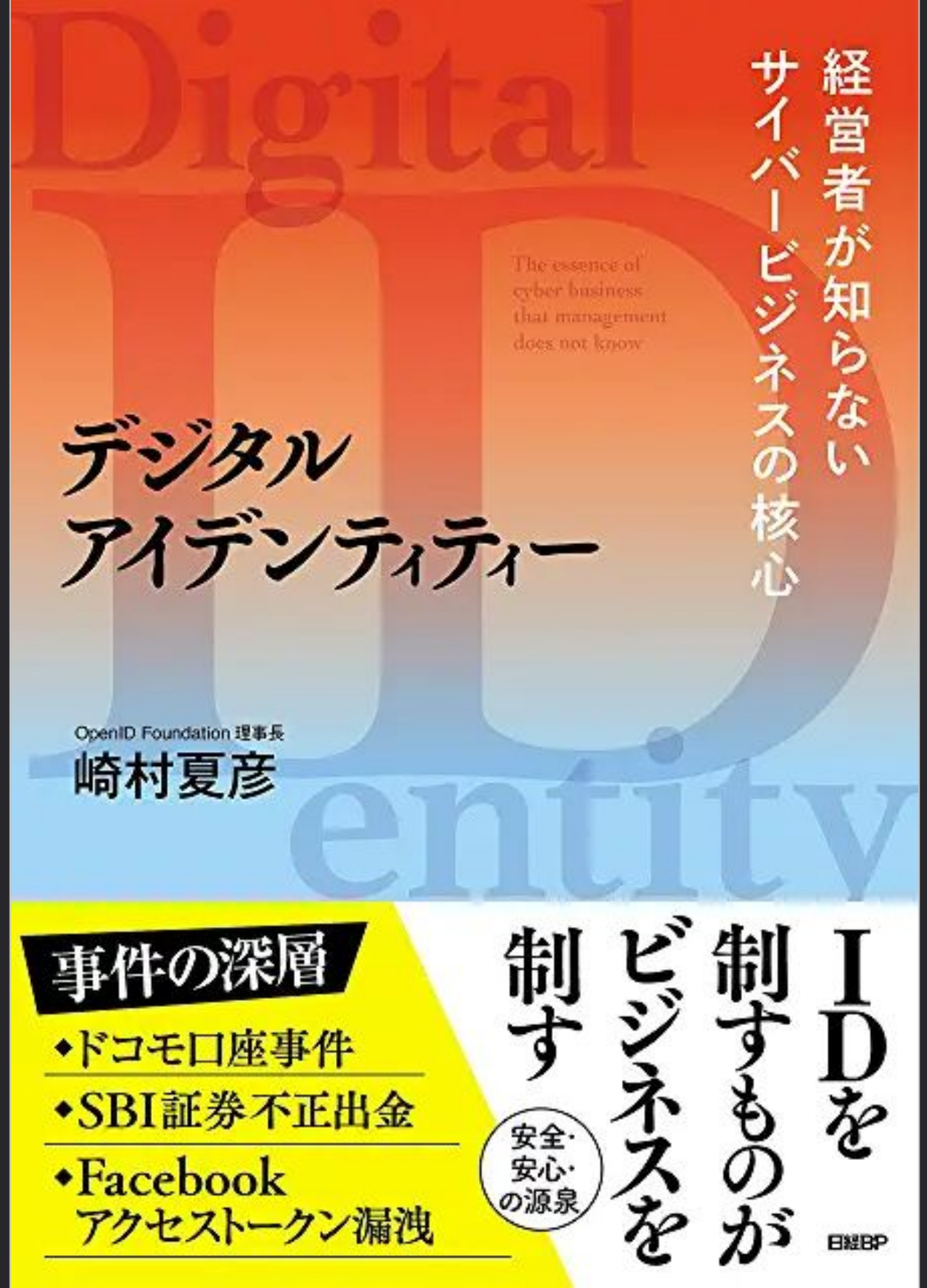
@_nat

アイデンティティとプライバシーに関する標準化アーキテクト

- OpenID Connect, JWT, OAuth PKCE, OAuth JAR, FAPI 1.0, ISO/IEC 29100 Privacy framework, 29184 Privacy notice and consent などの著者／編者
- OpenID Foundation理事長 (2011～)
- Kantara Initiative 創業理事
- MyData Japan 理事長 (2019～)
- ISO/IEC JTC 1/SC27専門委員会委員長
- 公正取引委員会デジタルスペシャルアドバイザー
- NHK中央放送審議会委員
- NATコンサルティング代表
- 東京デジタルアイディアーズ主席研究員
- PwC Japanグループ Digital Identity顧問
- Authlete株式会社 社外取締役

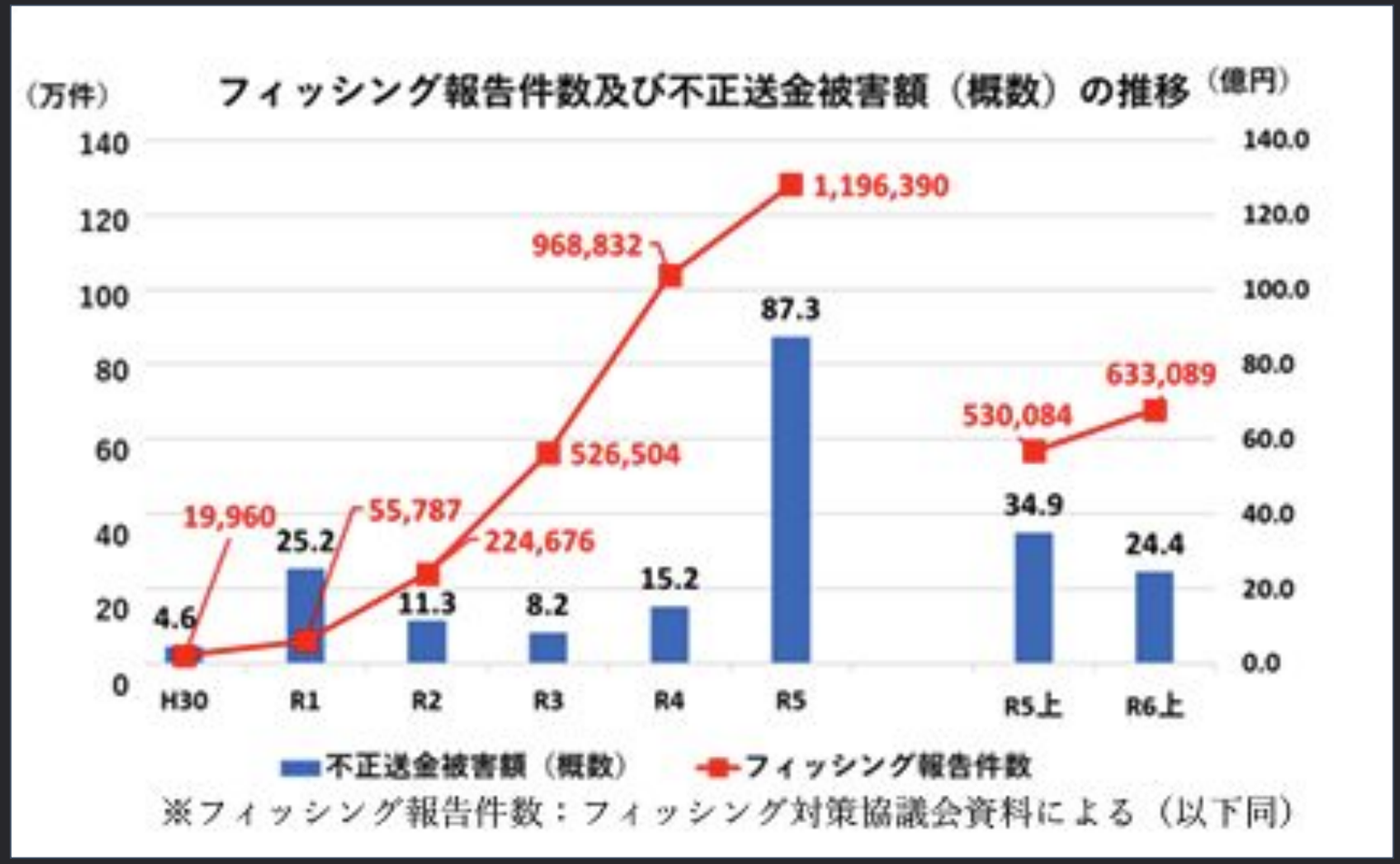






（出所）筆者

フィッシング報告件数の増加



（出所）警察庁「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

DMM Bitcoin

482億円相当の暗号資産が流失

1）システムリスク管理態勢等の整備
2）暗号資産の流出リスクへの対応
3）経営責任の明確化及び経営管理態勢等の強化

https://lfb.mof.go.jp/kantou/kinyuu/pagekthp0270000030.html

60億円は少額？！

（出所）https://x.com/Vivien_BingX/status/1836940851873992845

情報セキュリティにとって

ID管理（IAM）が重要であることは論を待たない

このことは、統計からも明らか

主な侵入経路

認証情報

フィッシング

脆弱性の悪用

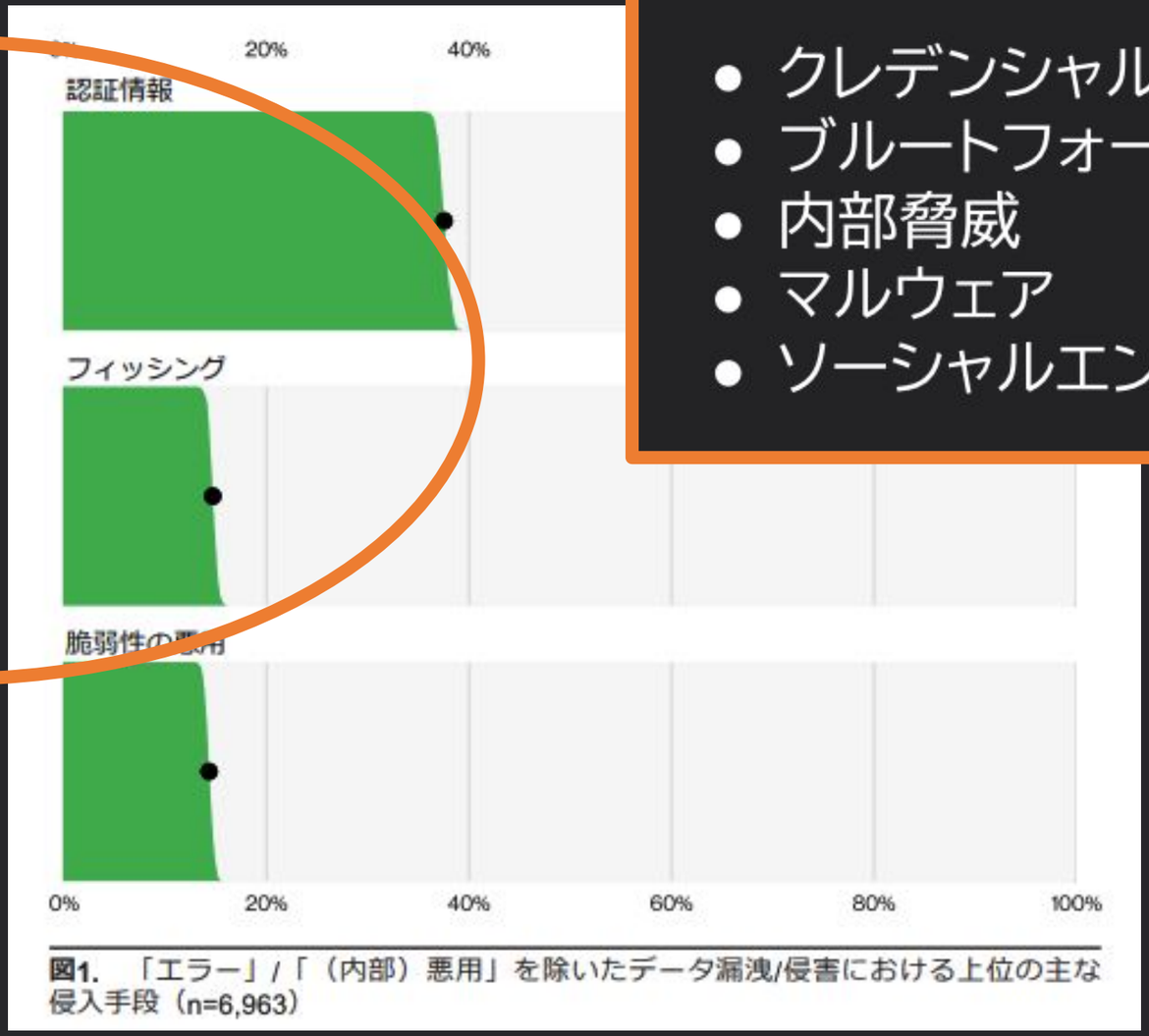


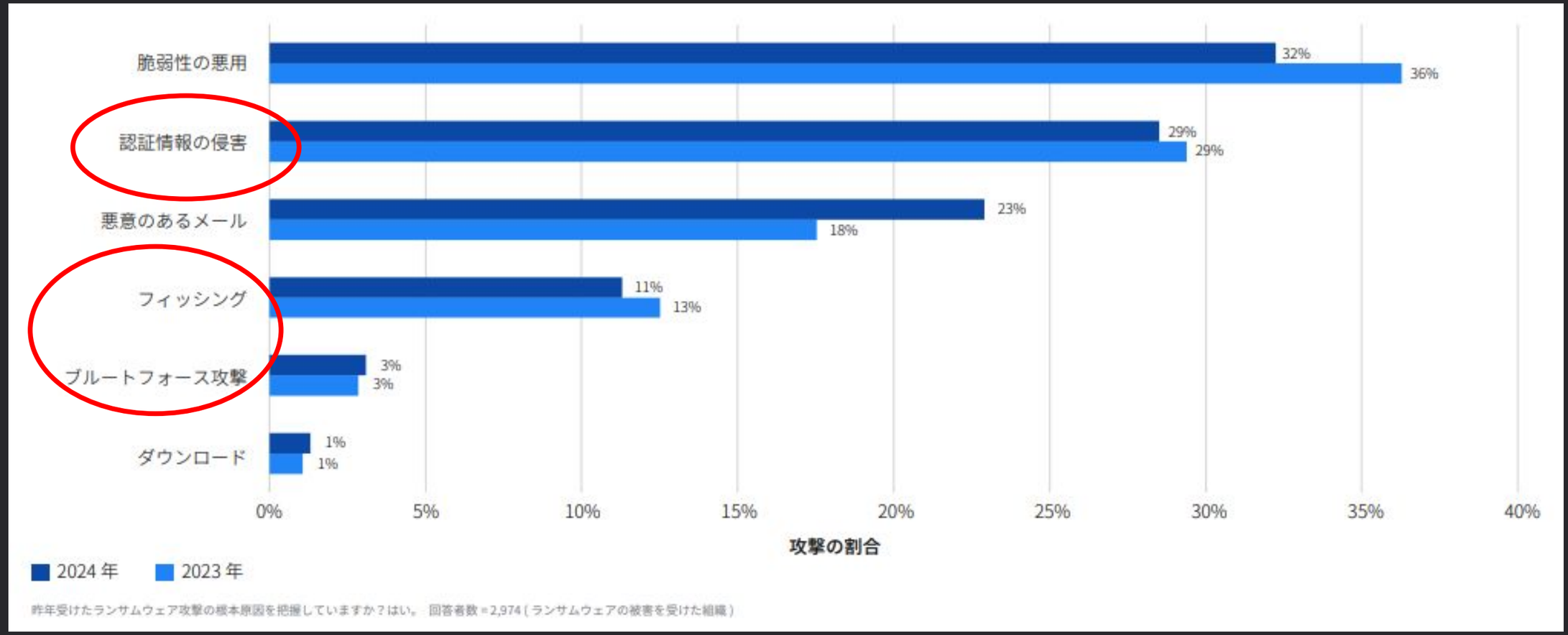
図1. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な侵入手段（n=6,963）

認証情報の侵害

- クレデンシャルスタッフィング
- ブルートフォース攻撃
- 内部脅威
- マルウェア
- ソーシャルエンジニアリング

（出所）ベライゾン「2024年度 DBIR データ漏洩/侵害調査報告書」

ランサムウェアに関しても同様



（出所）Sophos「ランサムウェアの現状2024年版」
https://www.sophos.com/ja-jp/content/state-of-ransomware

これらの多くは「当人認証」の失敗

登録された認証手段を用いた当人認証

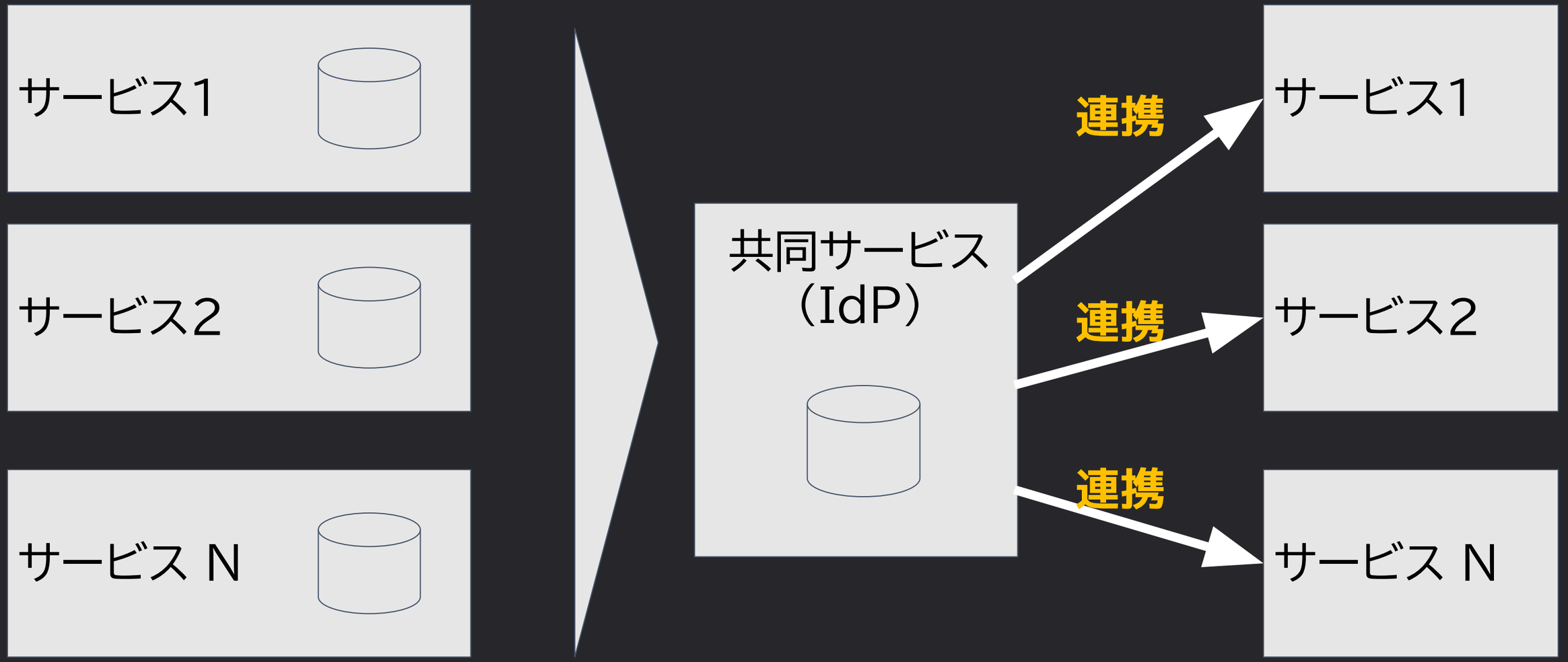
- パスワード
- OTP
- パスキー
- ICカード etc.

IAMの4大要素

身元確認	登録するユーザが誰であるのかを確認(後述) 例:マイナンバーカードで確認
当人認証	いま来ているのがどの登録されたユーザなのかを確認 例:OTPで確認
アイデンティティ連携	当人認証されたユーザの属性と認証された条件などの情報を連携 例:OIDCで認証情報と属性を連携
アクセス管理	属性に応じて、リソースへのアクセスの許可・不許可を決定・実施 例:「人事課長」かつ「社内」ならば参照許可

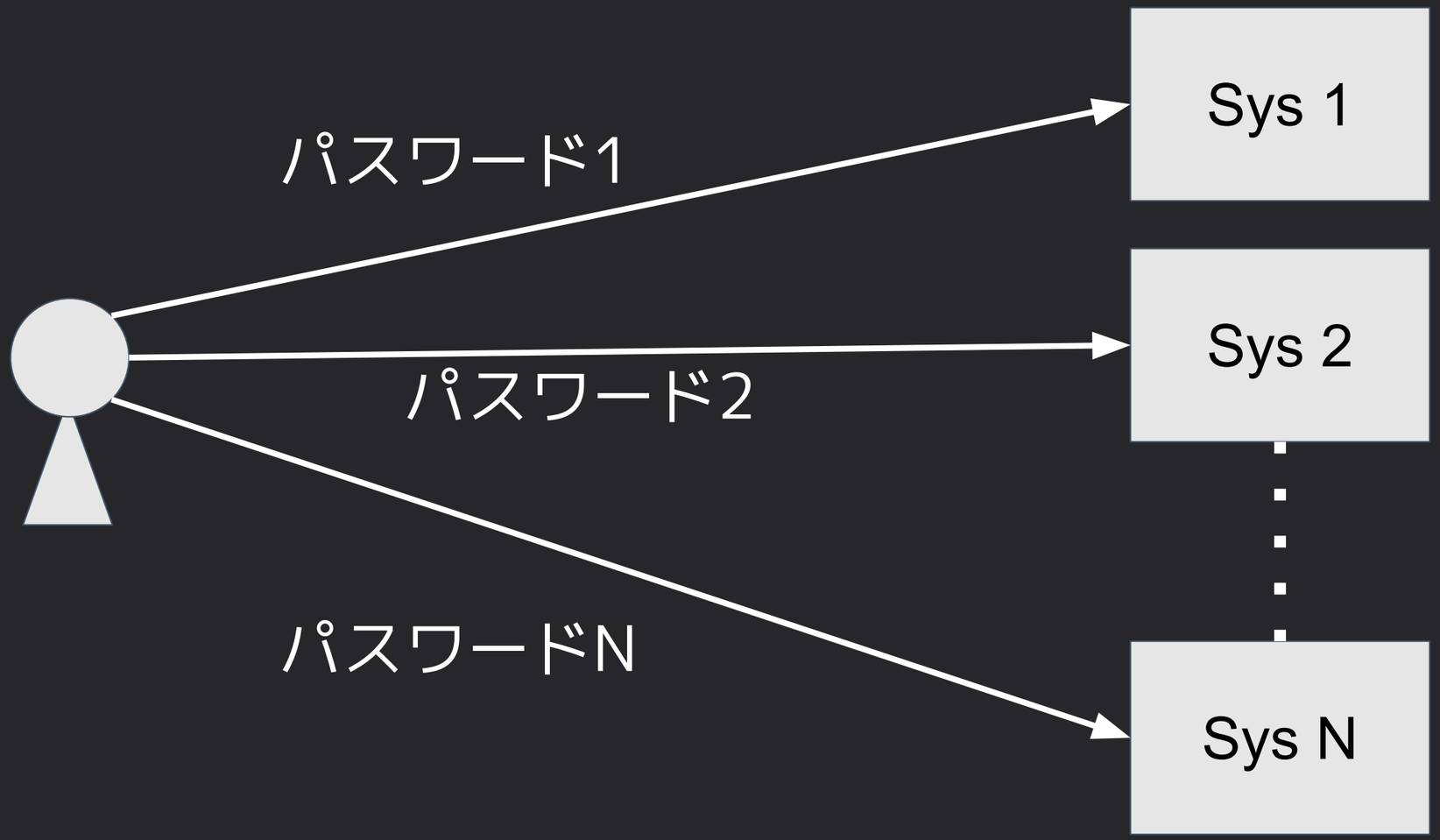
(出所)筆者

なぜアイデンティティ連携？



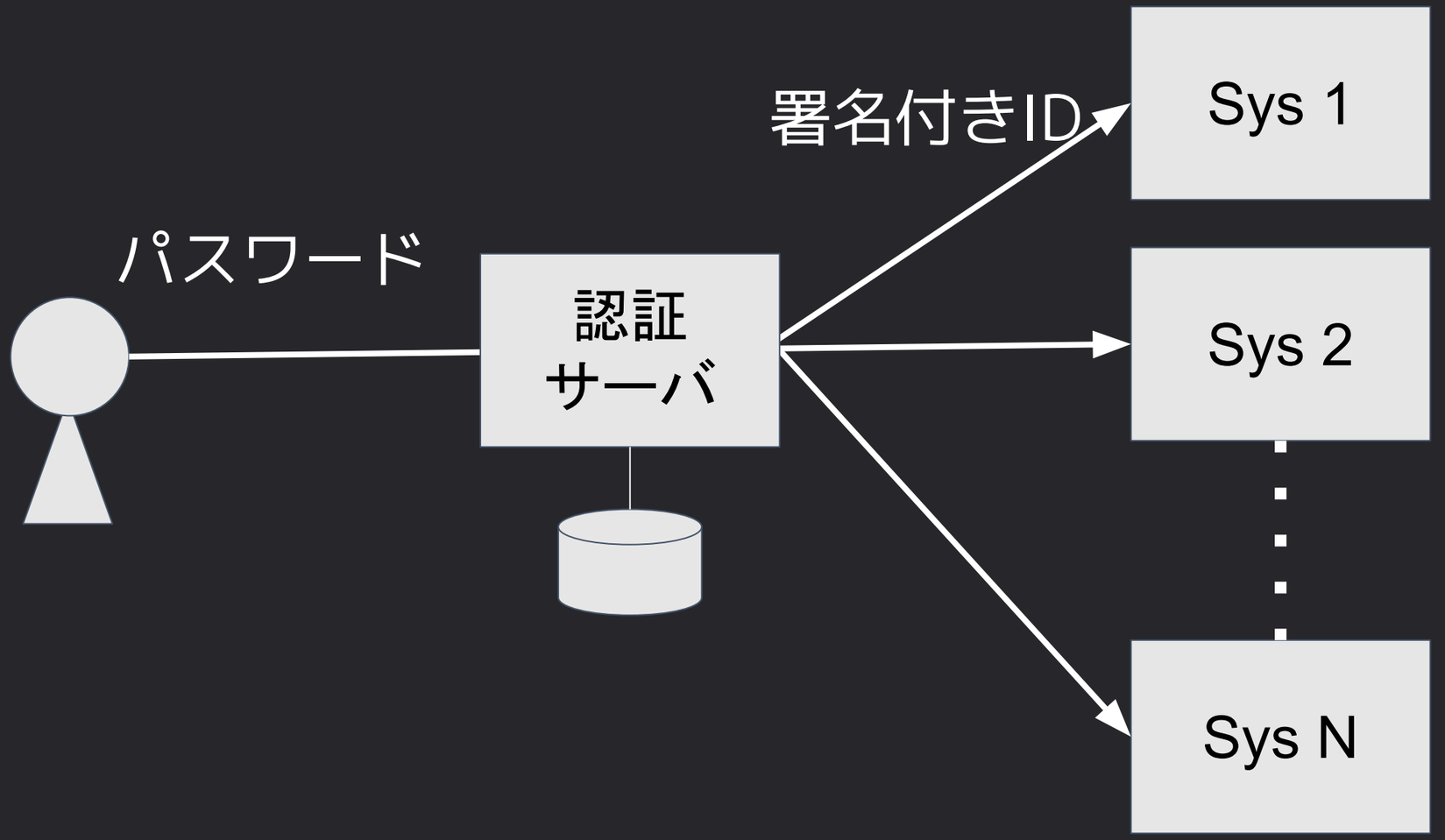
（出所）筆者

管理の複雑性：個別パスワード



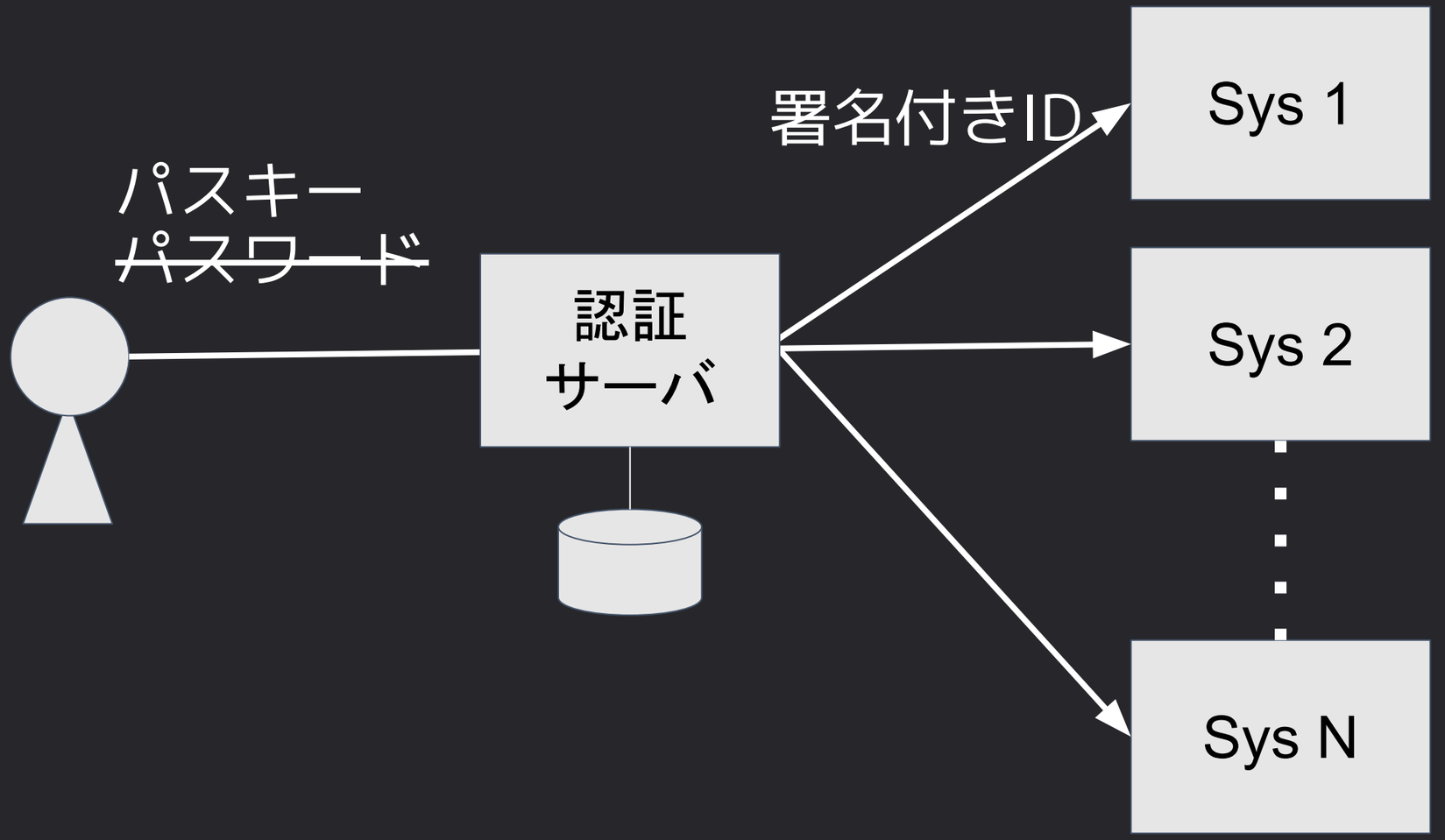
（出所）筆者

ID連携



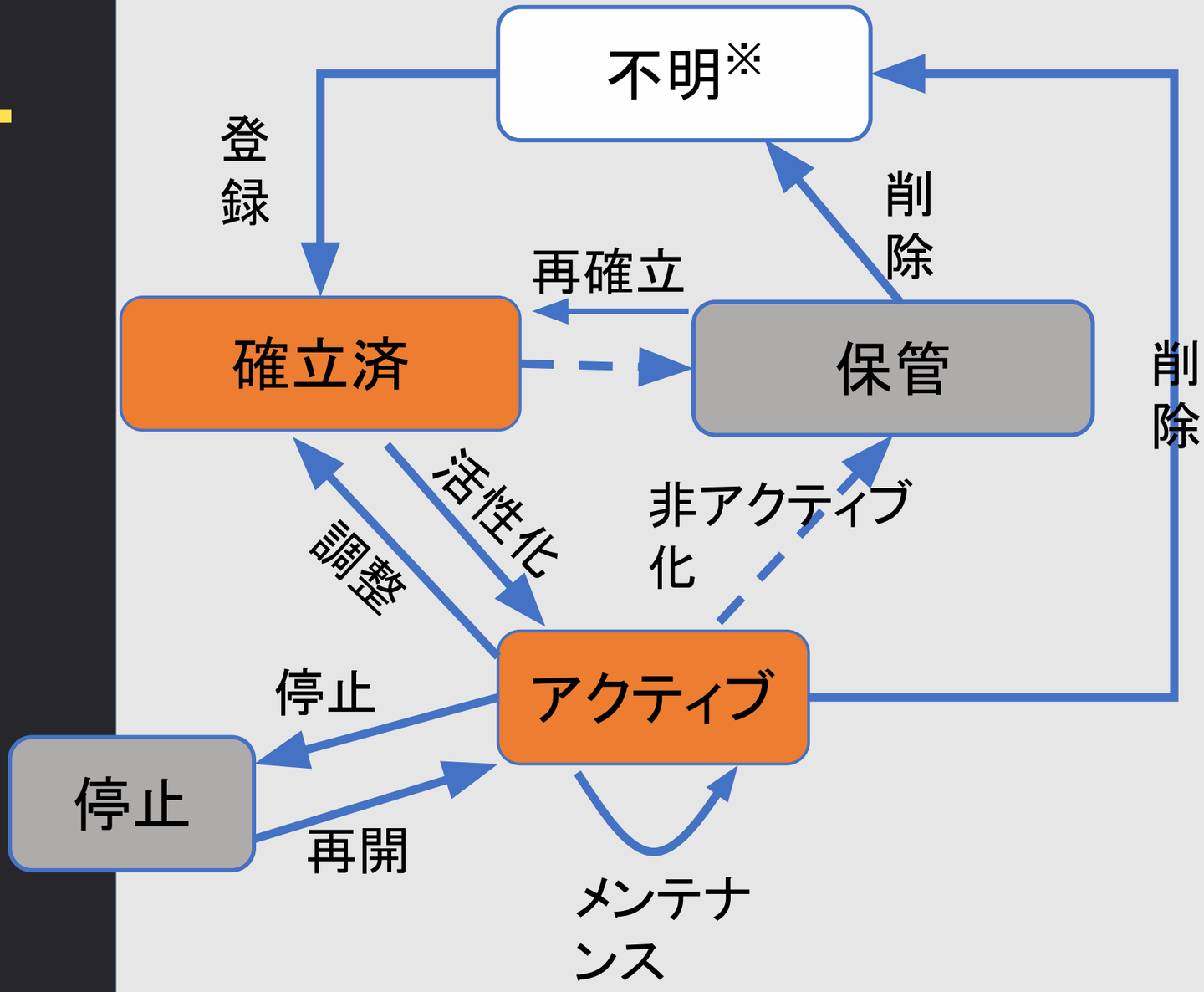
（出所）筆者

ID連携



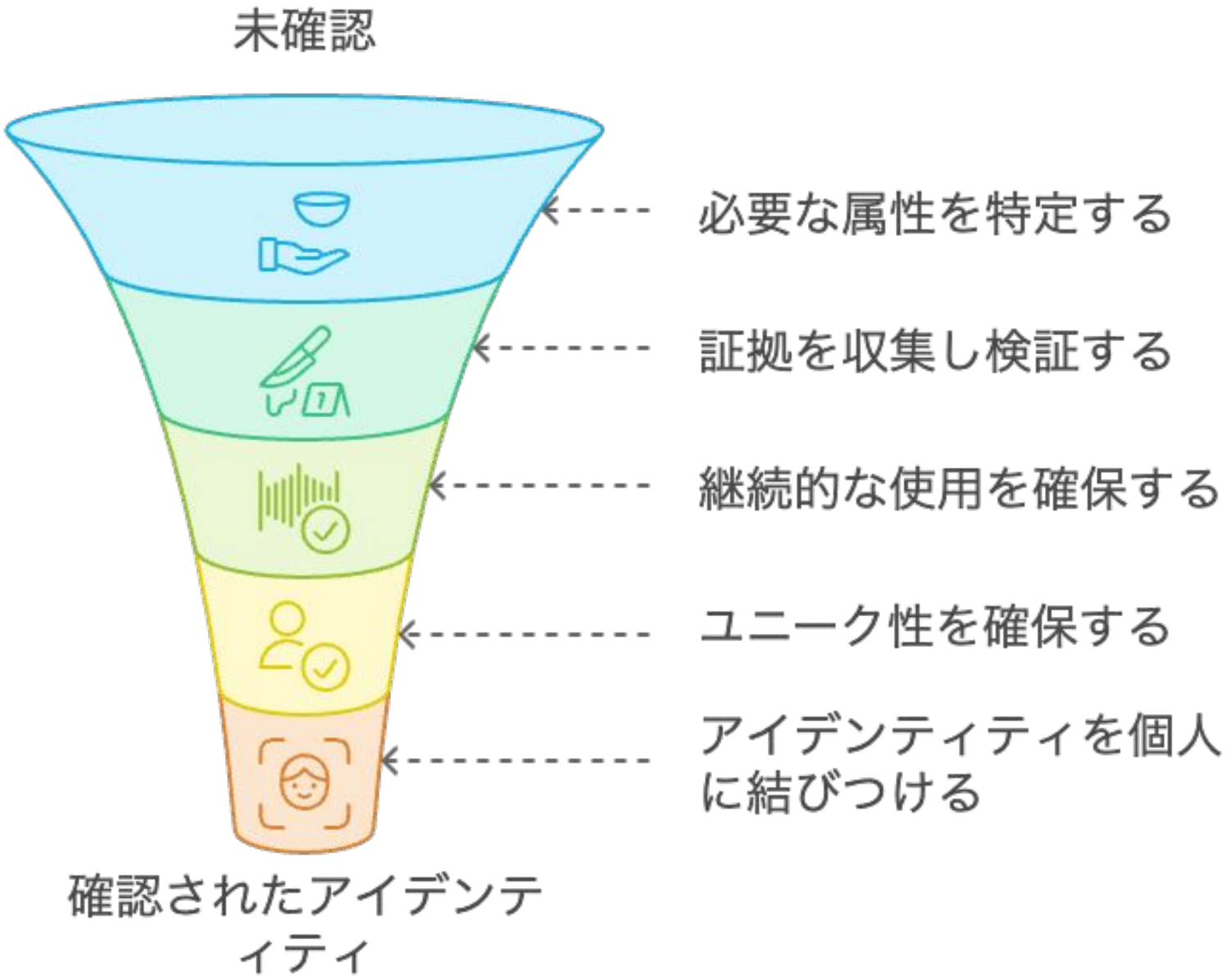
（出所）筆者

アイデンティティ・ライフサイクル



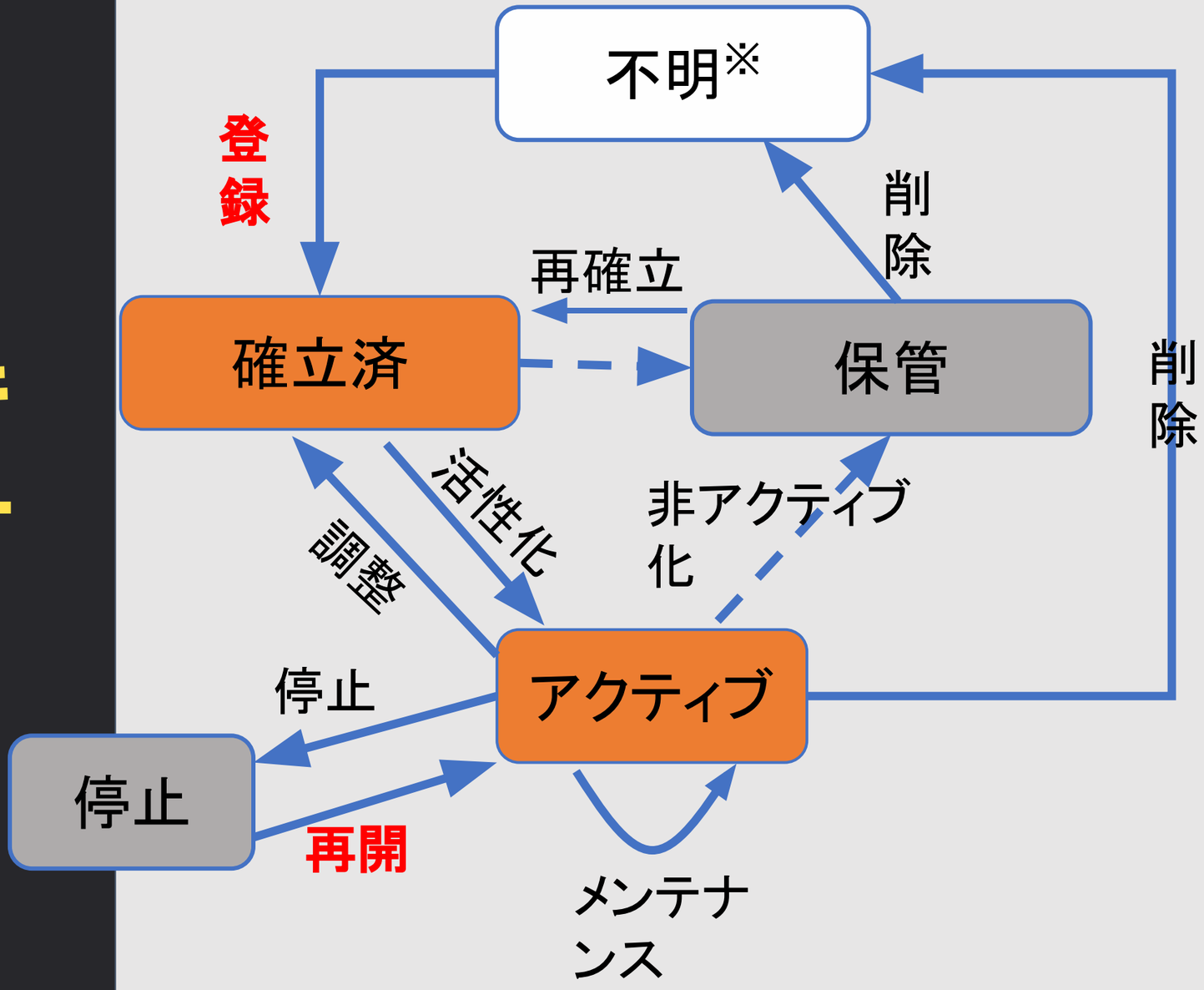
(出所)ISO/IEC 24760 を下に筆者

身元確認



身元確認は

「登録」と
「再開」のとき
に利用されます



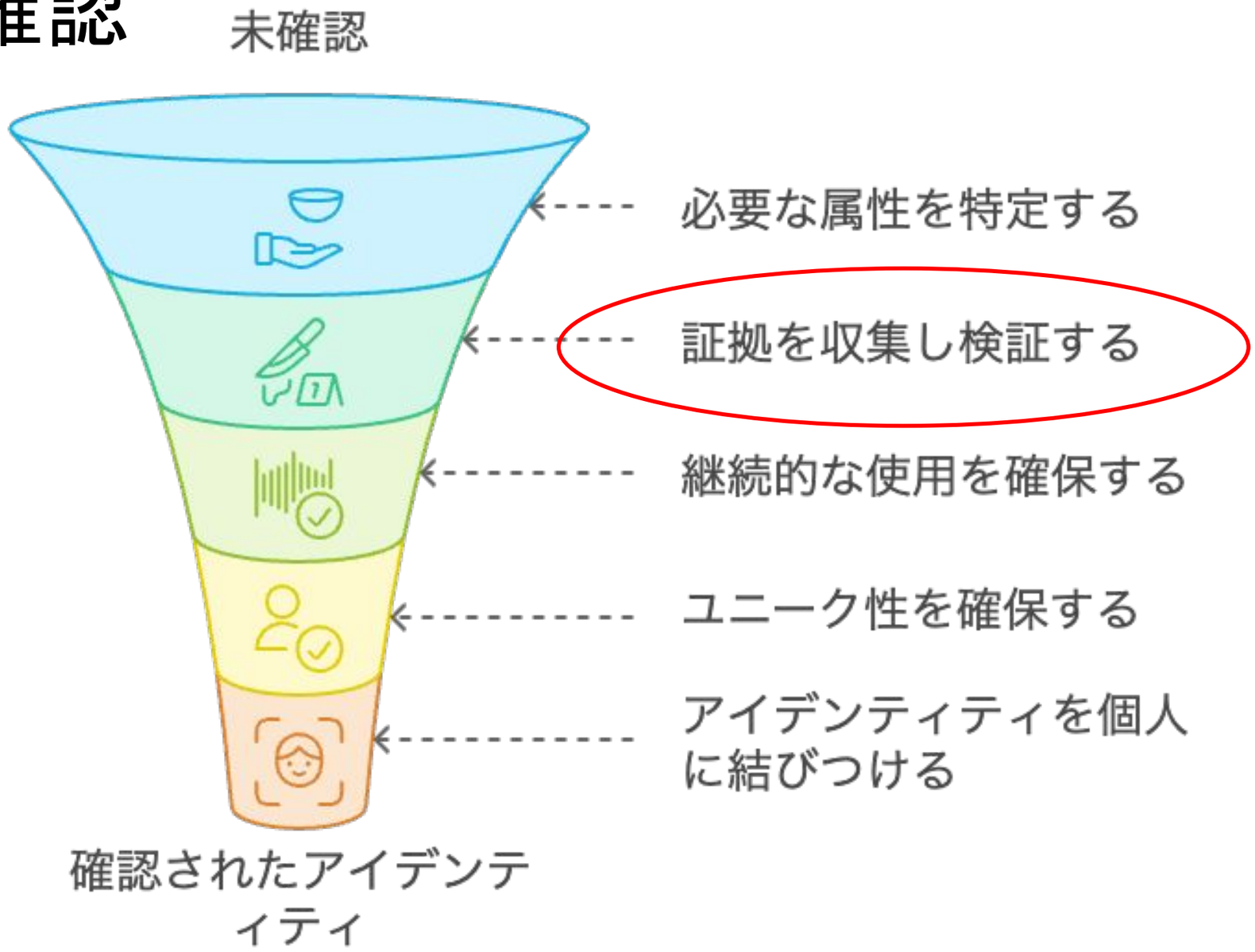
これが失敗していることが多い

マイナカードの情報でネットバンク口座を無断開設か…７０代女性が１４００万円だまし取られる

- 「総合通信局」の職員や警察官を名乗る人物から「口座の情報が流出している」などと電話
- 女性はスマートフォンの機種変更を指示され、スマホのビデオ通話機能で自分の顔やマイナンバーカードを相手側に提示
- 犯人はこの情報を用いてネットバンクに女性名義の口座を作成
- 「あなたの口座が凍結される」などとして預金の移し替えを持ちかけ、振込先に女性名義のネットバンク口座を提示。
- 女性は、口座が開設されたことを知らなかったが、不審に思わず2月28日、二つの金融機関の窓口から現金を振り込み

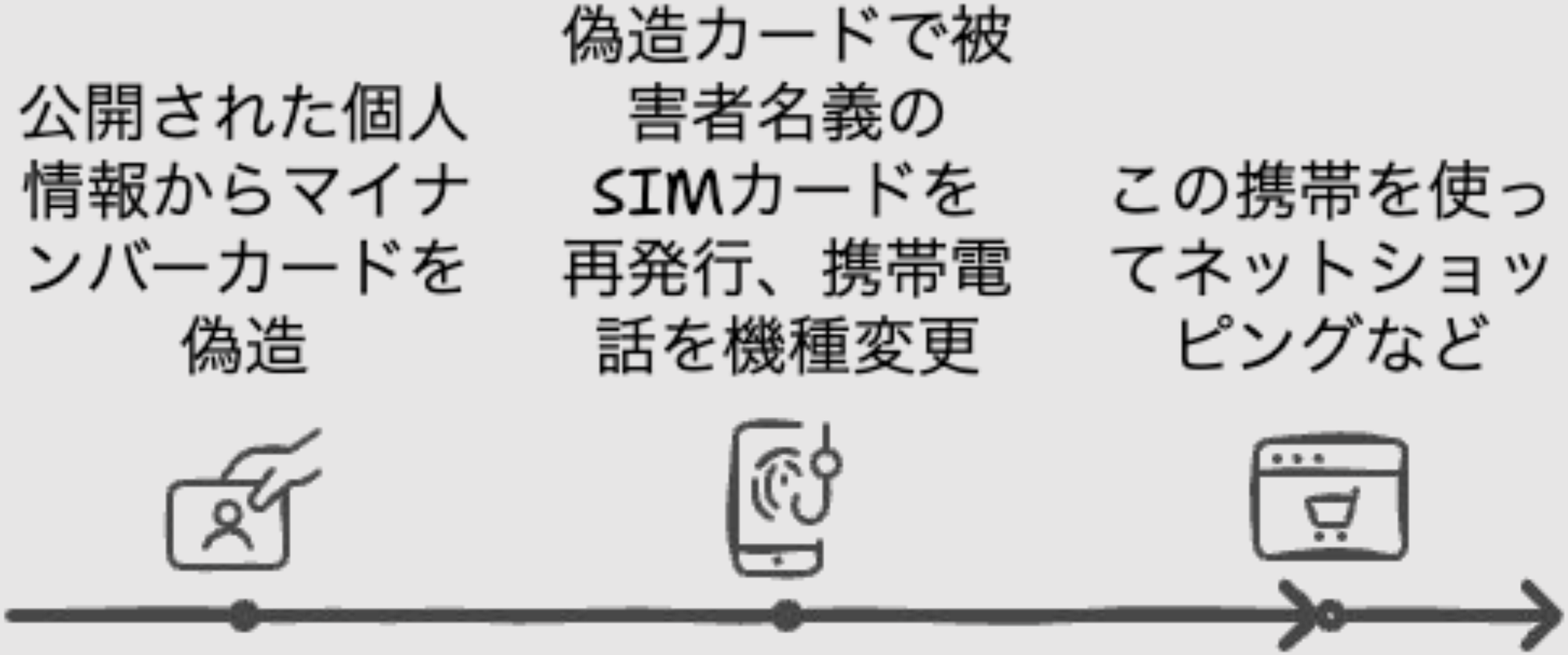
（出所）筆者［DALE-E使用］

たとえば身元確認



(出所)筆者

個人情報をネット公開の議員、マイナカード偽造されたか…スマホ乗っ取られ決済で被害



（出所）筆者

積水ハウス地面師詐欺事件 (55.5億円)

- 偽造パスポートを使って印鑑の改印手続き
- 偽造パスポートと印鑑証明を使って相手を騙した

（出所）写真AC画像をもとに筆者

これらはいずれも身元確認の失敗に起因している

正しくI.D.確認（＝ICチップ情報の確認）を行わなかったのが原因
（人的要因）
正しいプロセスと教育を行わなかった組織の責任（組織的要因）

アクセス制御の失敗

アクセス制御の失敗の例：

- 一人の出向者が全顧客のデータをダウンロード
- あるアカウントが盗られたことによって全データが暗号化
- VPNに侵入されたら中はするするだった
- クッキーやアクセストークンの窃取とその被害の甚大化

Need-to-Know
原則違反

最小権限
原則違反

こうしたことを対策していかなければならない。

そのために制定されているのが

- 米国
  - NIST SP800-63 第4版 が現在策定中
  - 2nd Public Draft がパブコメに付された（8/22）
- 日本
  - デジタル庁本人確認ガイドライン が改定中（DS-511）
  - 7月に中間整理が発表された（7/15）
- ISO/IEC 29115, TS29003, 29246

デジタル庁本人確認ガイドラインの改定の概要

本人確認ガイドラインの主要な改定ポイント

1章 **はじめに**	**① ガイドラインの適用対象と名称を変更** • デジタルによる本人確認がオンラインだけでなく対面にも拡大していることや、改定後のガイドラインの内容・位置づけ等を踏まえ、ガイドラインの適用対象と名称を変更する。
	② ミッション遂行などの基本的な考え方を解説 • 「1.5 基本的な考え方」を新たに設け、ミッション遂行、公平性とアクセシビリティ、プライバシー、ユーザビリティなど、リスク評価プロセスにおいて考慮すべき新たな観点を解説する。
2章 **本人確認の枠組み**	**③ 本人確認の枠組みを定義・解説** • 2章を新設し、身元確認や当人認証の概念を説明する。現行ガイドラインでは言及のない認証連携についても新たに盛り込み、IDプロバイダを利用する実装モデルとして「認証連携モデル」の解説を追加する。
	④ 保証レベルと対策基準の一部を見直し • NIST SP 800-63-4 におけるxALの改定を参考としつつ、身元確認保証レベルと当人認証保証レベルの位置づけや対策基準を見直す。
3章 **本人確認手法の検討方法**	**⑤ リスク評価プロセスを全面的に見直し** • 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直す。 • ガイドライン利用者がリスク評価や本人確認手法の選定を円滑に実施できるよう参考資料を拡充する。

5

（出所）デジタル庁「本人確認ガイドライン改定方針 令和5年度中間とりまとめ」

適用対象の見直し方針（案）

❶「オンラインによる本人確認」 → 対面等も含める

- マイナンバーカードを活用した本人確認はオンラインだけでなく対面にも広まっていることなどを考慮し、オンラインだけでなく対面等での本人確認も適用対象に含める。

❷「個人又は法人等の」 → 個人向け／法人向けで分冊化

- 法人の本人確認は、個人（自然人）の本人確認とは異なる検討事項が多いため、個人向けと法人向けでガイドラインを分冊化する方針とする。法人向け部分は、将来的には別文書として管理することも検討する。

❸「行政手続」 → 内部事務への将来的な拡大を検討

- 行政の内部事務においても情報システムの利用時などで職員等を認証する機会は多くあるため、本ガイドラインを内部事務にも適用すべきでないか検討する。
- ただし影響範囲が非常に広い変更となるため、具体的な拡大範囲、強制力、拡大時期等については慎重に検討する。

（出所）デジタル庁「本人確認ガイドライン改定方針 令和5年度中間とりまとめ」

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

身元確認保証レベルの対策基準（案）　―　レベル2の細分化（案）

対策基準		各保証レベルの要求事項						
		レベル3	レベル2					レベル1
			2A	2B	2C	2D	2E	
身元確認の実施場所（Presence）								
対面		✓	✓	―	―			✓ いずれか
リモート		△※1	―	✓	✓			
申請者と本人確認書類の紐づきの検証方法（Verification）								
生体情報や容貌の比較	a) 申請者の容貌等を対面で確認し、本人確認書類と比較する	✓※2	✓	―	―	✓	―	✓ いずれか
	b) 申請者の容貌等をリモート（カメラ越し）で確認し、本人確認書類と比較する	―	―	✓	―	―	✓	
暗証番号等による認証	c) 本人確認書類の認証機能（暗証番号等）により認証する	―	―	―	✓	―	―	
	d) 住所等に送付した登録コードにより検証する	―	―	―	―	―	―	
本人確認書類の真正性の確認方法（Validation）								
電子的な検証	e) ICチップ内のデータの電子署名を検証する（※有効性確認を含む）	✓	✓ いずれか	✓ いずれか	✓ いずれか	―	―	✓ いずれか
	f) ICチップ内の券面画像と券面を比較する	―				―	―	
物理的な検証	g) 券面の真正性を目視等による外観検査で確認する	―	―	―	―	✓	―	
	h) 券面の真正性をリモート（カメラ越し）で確認する	―	―	―	―	―	―	
	i) 券面の真正性を券面の写し（コピー）で確認する	―	―	―	―	―	―	

※1 保証レベル3における統制環境下のリモート身元確認（Supervised Identity Remote Proofing相当）については具体条件を検討中
※2 保証レベル3においてはVerification時に生体情報（顔写真等）の記録を行うことを想定

29

（出所）デジタル庁「本人確認ガイドライン改定方針 令和5年度中間とりまとめ」

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

当人認証保証レベル２の細分化（案）

青字：主な改定ポイント

対策基準項目		対策基準（案）				
		当人認証保証レベル3	当人認証保証レベル2			当人認証保証レベル1
			レベル2A	レベル2B	レベル2C	
認証要素		耐タンパ性が確保されたHWトークンを含む２要素	２要素			単要素
脅威耐性（新規）	リアルタイム型フィッシング ：ユーザの入力をリアルタイムに中継することでSMSOTP等の2段階認証を突破するタイプのフィッシング攻撃	必須	必須	不要	不要	不要
	多要素認証疲労攻撃 ：大量の認証要求（プッシュ通知）を送り付けることでユーザを疲れさせ認証ボタンを押させる攻撃	必須	必須	必須	不要	不要
	誤ったログイン ：ユーザが意図せず他のアカウントへの認証に成功しログインしてしまうこと	必須	必須	必須	必須	不要
脅威耐性（現行ガイドライン定義済み）	フィッシング／ファーミング※	必須	必須			不要
	リプレイ攻撃※	必須	必須			不要
	中間者攻撃※	必須	必須			必須
	オンライン上の推測※	必須	必須			必須
	盗聴による認証情報の取得※	必須	必須			必須

※現行ガイドラインに掲載されている脅威については具体的な定義を見直し予定

（出所）デジタル庁「本人確認ガイドライン改定方針 令和5年度中間とりまとめ」

ID連携（Federation）はこれから。
SP800-63-4Cから持ってくると…

要求事項	FAL1	FAL2	FAL3
受信者制限	複数で良いが、単一RPを推奨	単一RP	同左
インジェクション保護	推奨	必須: すべてのトランザクションはRP起点	同左
トラスト契約締結	ユーザー主導 or 事前	事前	同左
識別子と鍵確立	動的 or 静的	動的 or 静的	静的
提示	持参人アサーション	持参人アサーション	HoKまたは記名式アサーション

（出所）NIST SP800-63C-4 2pd をもとに筆者

	FAL1	FAL2	FAL3
IdPがアサーションに署名	必須	必須	必須
RPが署名を検証	必須	必須	必須
IdPがRPを制限	必須, RPの集合	必須, 単一RP	必須
RPがaudを確認	集合に入っていることを確認	必須	必須
動的な信頼の確立	しても良い	禁止	禁止
RP と IdP の相互認証			静的URLsからの取得か、事前アップロード

（出所）NIST SP800-63C-4 2pd をもとに筆者

要求事項	FAL1	FAL2	FAL3
プロトコルがインジェクション耐性をもつこと	推奨	必須	必須
トランザクションのRPからの開始	-	必須	必須
FIPS140 L1以上で鍵が守られていること	-	必須	必須
RP がユーザが認証器をコントロールしていることを確認	(Bearer Assertion)	(Bearer Assertion)	必須 HoK or Bound

（出所）NIST SP800-63C-4 2pd をもとに筆者

アクセス権限の洗替

- 共有アカウントは極力廃止
- 異動・退社したアカウントは速やかに反映
- ポリシーベースのアクセス管理で監査しやすく
- Need-to-know, Need-to-access
- 短期間のアクセストークン
- Stateful Token

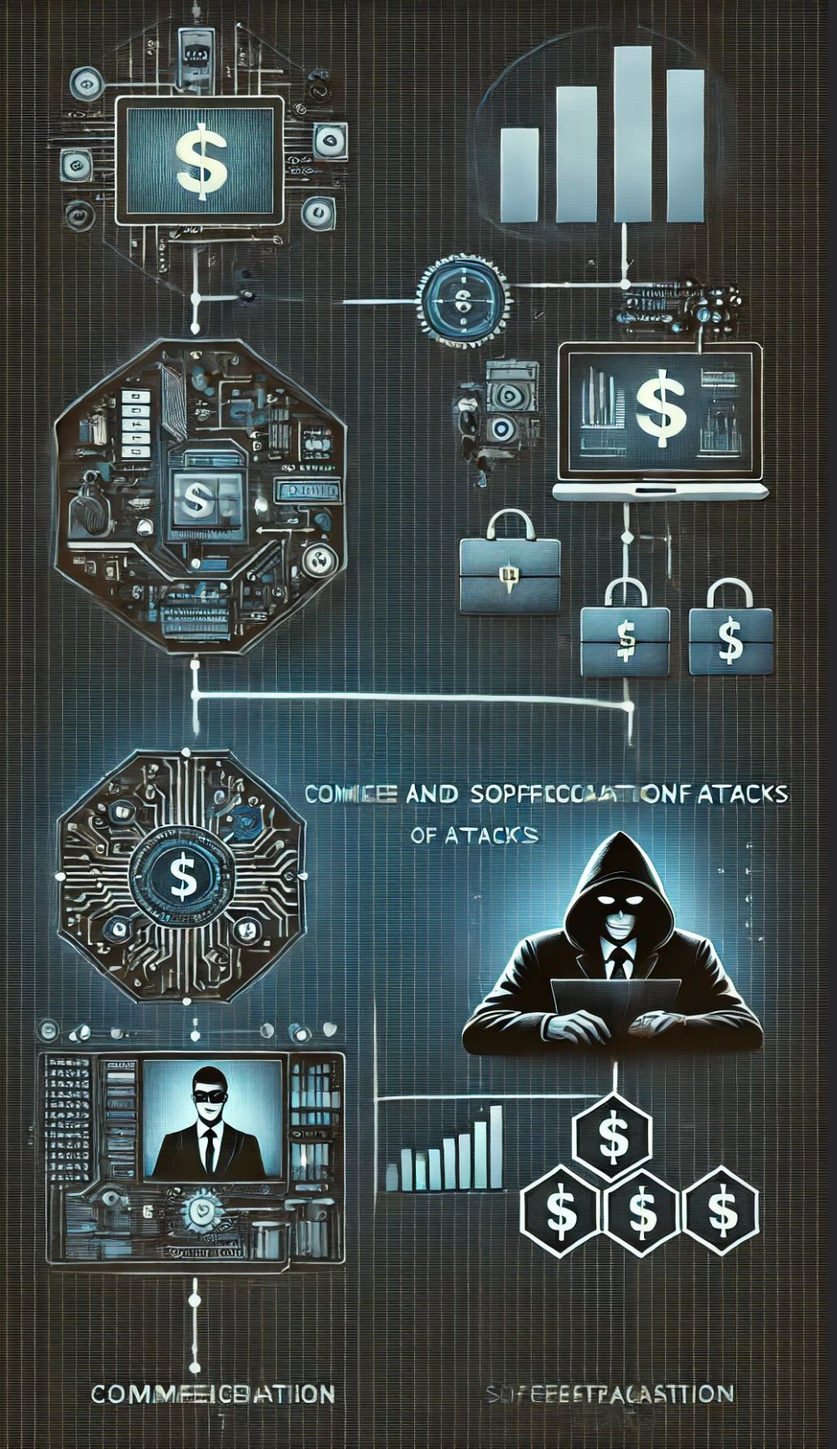
ログの監視

アクティビティ、例外、障害、その他関連するイベントを記録するログは、生成され、保存され、保護され、分析されるべき（特に特権アクセス）

通常と異なるパターンの検出

ISO/IEC 27002 8.15 に詳細あり

なぜ脅威は減らないのか



外部要因

- 攻撃のビジネス化と高度化
  - より高度な攻撃手法がより安価に手に入るように
  - 攻撃の水平分業

- 依存先が分散する中での、依存先の脆弱性

技術的要因

- ID管理の複雑化
  - 複数システムでのID管理
  - クラウドサービスの普及による認証サービスの差異
  - IDライフサイクル管理の煩雑さ
- レガシーインフラ
  - 正しい運用にしようとしても対応できないシステムたち
- 業務プロセス改善の困難性
  - 固定パスワードの例
- ログ収集と分析の困難性
  - 分散したシステムからのログ収集とリアルタイムの分析が難しい
  - 例）ある大手印刷会社では、監査ログの管理不備により、5年間にわたり864万件もの個人情報が流出し続けた

人的要因

- セキュリティ意識の欠如
- 知識・スキルの欠如
- 既存の業務フローを変えることへの抵抗
- 内部不正のリスク

組織的要因

- トップマネジメントの意識
- 不十分なリスク管理
- 不適切なアクセス権管理
  - 例）ある企業では、保守・管理業務担当者に不必要なデータ操作権限が付与されていたため、大量の個人情報が漏洩する事態が発生
- 対策投資の不足
- 不十分な教育プログラム
- セキュリティチームと運用チームの連携不足

火傷ドリブン

効果が出ることは実証済み

A社の事例

- フィッシング被害が1/20に

いつやるの？

今すぐ
しよ！