



日本のサイバーセキュリティを「連携」「学び」「創造」

標準化部会 デジタルアイデンティティWG

「特権ID管理ガイドライン「解説編／実践編」のご紹介」

2024/07/19

WGリーダー 宮川 晃一
日本電気株式会社

デジタルアイデンティティWGでは、2024/5/31に特権ID管理ガイドライン「実践編」を公開しました。

昨年度公開した特権ID管理ガイドライン「解説編」に続くドキュメントとなっています。本セッションでは特権ID管理ガイドライン「解説編／実践編」の概要をご紹介します、特に「実践編」でポイントとなる事項について解説いたします。

デジタルアイデンティティWGの紹介

「デジタルアイデンティティWGの目的」

本WGは“デジタルアイデンティティ”全般を広く議論する場として、今年度で設立 **19年目**を迎えました。

本WGでは、デジタルアイデンティティの課題等について議論し、導入指針や各種報告書の提示、執筆活動・セミナー・勉強会等での啓蒙活動および普及促進、関連他団体との連携による市場活性化等を目的として活動を行っています。

メンバー紹介：

https://www.jnsa.org/active/std_idm.html

2024年7月現在 70名のメンバー



WGの歴史

年	成果物等	WG名称
2005	WG設立	内部統制における アイデンティティ 管理WG
2006	合宿実施（三浦マホロバツインズ）	↓
2007	内部統制における アイデンティティ管理解説書（第1版）	
2008	内部統制における アイデンティティ管理解説書（第2版）	
2009		
2010	クラウド環境における アイデンティティ管理ガイドライン （企業向け調査レポート）	セキュリティにおける アイデンティティ管理 WG
2011		↓
2012	改定新版 クラウド環境におけるアイ デンティティ管理ガイドライン（書籍） エンタープライズ ロール管理解説書（第1版）	
2013	OpenID ConnectとSCIMの エンタープライズ利用ガイドライン	アイデンティティ管理 WG
2014	エンタープライズ ロール管理解説書（第2版）	↓

年	成果物等	WG名称
2015	10周年記念セミナー！ エンタープライズ ロール管理解説書（第3版）	↓
2016	エンタープライズにおける特権ID管理 解説書（第1版）	
2017	ID管理システム導入における現状把 握チェックリスト（第1版） クロスボーダー時代のアイデンティティ 管理セミナー！	
2018	内部統制における アイデンティティ管理解説書（第2版）	
2019	クレデンシャルの歴史（読み物）	↓
2020	Software Design 11月号特集（雑誌）	
2021	Enterprise Identity Day！ 標準化部会セミナー！	デジタルアイデンティ ティWG
2022	今さら聞けない暗号技術&認証・認 可（書籍） 改定新版 エンタープライズにおける特 権ID管理ガイドライン（解説編） ミニウェビナー & Youtube 「？？？とアイデンティティ」	↓
2023	改定新版 エンタープライズにおける 特権ID管理ガイドライン（実践編）	

これまでの成果物（ガイドライン、書籍）



デジタルアイデンティティWG これまでの成果物

<https://www.jnsa.org/result/digitalidentity/index.html>

[デジタルアイデンティティワーキンググループのメンバー紹介はこちら>>](#)

▶ 2024/5/31

報告書 「【改定新版】特権ID管理ガイドライン 実践編」を公開しました。
2023年公開の「解説編」もこちらからダウンロード下さい。

▶ 2023/5/8

報告書 ニュージーランド政府による"Identification Management Standards"に関する考察
==NIST SP800-63 "Digital Identity Guidelines"との比較結果等==

▶ 2023/3/31

報告書 【改定新版】特権ID管理ガイドライン 解説編
※2024年5月31日公開の「【改定新版】特権ID管理ガイドライン 実践編」をご覧ください。

▶ 2023/3/6

関連書籍発売 「Software Design 今さら聞けない認証・認可」が再編集されて別冊シリーズで発売されました。
技術評論社さんのページにリンクします。

▶ セミナー **2023/5/25開催** YouTube JNSAChannelで公開中！セミナーページからどうぞ！

セミナー | デジタルアイデンティティWGミニウェビナー「???とアイデンティティ」

2021/11/26

セミナー資料 2021年11月26日（金）開催
「Enterprise Identity Day 再考！！エンタープライズ・アイデンティティ～ゼロトラストセキュリティの礎を確立する～」

▶ **執筆** 「Software Design」2020年11月号

特集1「今さら聞けない認証・認可～セキュアなIAMを実現するために覚えておきたいこと」
技術評論社さんのページにリンクします。

▶ **読み物** 「クレデンシャルの歴史」

▶ **報告書** 「ID管理システム導入における現状把握チェックリスト（第1版）」

▶ **出版書籍** 「＜改訂新版＞クラウド環境におけるアイデンティティ管理ガイドライン」
Amazonにリンクします

▶ **報告書** 「OpenID ConnectとSCIMのエンタープライズ利用ガイドライン」
(JNSAとOpenID Foundation Japanとの共同執筆)

▶ **報告書** 「エンタープライズにおける特権ID管理解説書（第1版）」

▶ **報告書** 「エンタープライズロール管理解説書（第3版）」

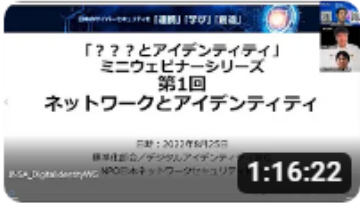
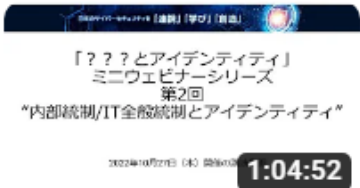
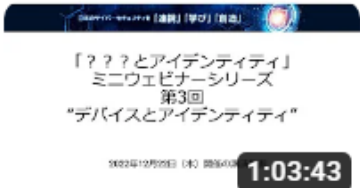
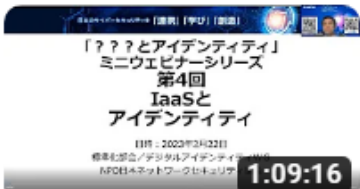


Copyright 2024 NPO日本ネットワークセキュリティ協会

これまでの成果物（動画配信）



<https://www.youtube.com/playlist?list=PL1nvarmw8MRuJfx8nrBf-Zv4hqEqUIhm>

- 1  デジタルアイデンティティWGミニウェビナー第1回「ネットワークとアイデンティティ」
JNSA Channel • 1173 回視聴 • 6 か月前
1:16:22
- 2  デジタルアイデンティティWGミニウェビナー第2回「内部統制/IT全般統制とアイデンティティ」
JNSA Channel • 459 回視聴 • 4 か月前
1:04:52
- 3  デジタルアイデンティティWGミニウェビナー第3回「デバイスとアイデンティティ」
JNSA Channel • 228 回視聴 • 3 か月前
1:03:43
- 4  デジタルアイデンティティWGミニウェビナー第4回「IaaSとアイデンティティ」
JNSA Channel • 162 回視聴 • 1 か月前
1:09:16

改定新版 特権ID管理ガイドライン（解説編/実践編）

成果物公開ページのご案内



【改定新版】特権ID管理ガイドライン 解説編／実践編 (デジタルアイデンティティワーキンググループ)

2023.3.31掲載/2024.5.31 更新

「【改定新版】特権ID管理ガイドライン」について

本書は2016年度に発行した、「エンタープライズにおける特権ID管理解説書（第1版）」について、これまでに多くのご意見やご指摘をいただいたものを反映すべく内容について検討を行い、新たな形で発行するものである。
今回の解説書は2部構成として、1部は「解説編」2部は「実践編」とした。
「解説編」では、特権ID管理の重要性や特権IDの役立ち、インシデント事例などを紹介した。
「実践編」では、実際に特権IDを行うための仕組みや運用方法について解説した。
これから、特権ID管理を導入検討する人には、プロジェクトの推進の準備として、また、現在特権ID管理システムを導入中の人には、現在のプロジェクトをよりよくするためのチェック・ヒント集として、ご活用していただけたらと考えている。
また、この分野について詳細に書かれた書籍がほとんど出版されておらず、その意味でも本書の内容は多くの企業に役立つ内容となっている。
本書は「日本ネットワークセキュリティ協会（JNSA）」の「デジタルアイデンティティ管理ワーキンググループ」のサブグループにて検討した内容となっている。本書があらゆる企業において、特権ID管理の適切な導入・運用に貢献できれば幸いである。

執筆メンバー

解説編（2023年公開）

宮川 晃一（WGリーダー） 日本電気株式会社
菊地 周平 CyberArk Software株式会社
染谷 浩子 CyberArk Software株式会社
大竹 章裕 株式会社ラック
斎藤 知明 TIS株式会社
松井 花緒 日本電気株式会社
吉本 紀浩 デロイト・トーマツサイバー合同会社
今堀 秀史 株式会社SHIFT
金子 昭祐 SCSK株式会社
(順不同)

実践編（2024年公開）

宮川 晃一（WGリーダー） 日本電気株式会社
大竹 章裕 株式会社ラック
斎藤 知明 TIS株式会社
松井 花緒 日本電気株式会社
吉本 紀浩 デロイト・トーマツサイバー合同会社
石崎 貴嗣 デロイト・トーマツサイバー合同会社
金子 昭祐 SCSK株式会社
内田 健一 NECソリューションノベータ株式会社
藤井 孝之 NECソリューションノベータ株式会社
毛利 幹宏 株式会社アシスト
伊藤南菜子 株式会社富士通エフサス
河原林 広 株式会社富士通エフサス
(順不同)

なお、本WGの活動内容およびメンバーは以下の紹介ページを参照いただきたい。

【デジタルアイデンティティWG紹介ページ】
https://www.jnsa.org/active/std_idm.html

【改定新版】特権ID管理ガイドライン

- ・「【改定新版】特権ID管理ガイドライン 解説編」ダウンロード (PDF:2.1MB) (2023.3. 31公開)
- ・「【改定新版】特権ID管理ガイドライン 実践編」ダウンロード (PDF:2.6MB) (2024.5. 31公開)

デジタルアイデンティティワーキンググループの成果物ページに戻る>>

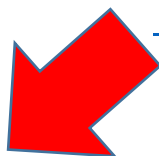
引用のご連絡及び内容に関するお問い合わせは、
「各種公開資料の引用及び、内容に関するお問合せ」をご覧ください。 [こちらから](#)

【改定新版】特権ID管理ガイドライン 解説編／実践編

<https://www.jnsa.org/result/digitalidentity/2024/index.html>

・「【改定新版】特権ID管理ガイドライン 解説編」ダウンロード
(PDF:2.1MB) (2023.3. 31公開)

・「【改定新版】特権ID管理ガイドライン 実践編」ダウンロード
(PDF:2.6MB) (2024.5. 31公開)



解説編のご紹介



第1章 特権IDとは

- 1.1 システムにおける特権IDとは
- 1.2 特権IDの特徴
 - 1.2.1. 一般IDと特権IDの違い
 - 1.2.2. 特権IDが奪取された場合の影響度
 - 1.2.3. 利用用途の観点でのセキュリティリスク

第3章 インシデント事例集

- 3.1 ネットワーク機器への攻撃事例
- 3.2 パスワードリスト攻撃の事例
- 3.3 Webサイトの改ざん事例

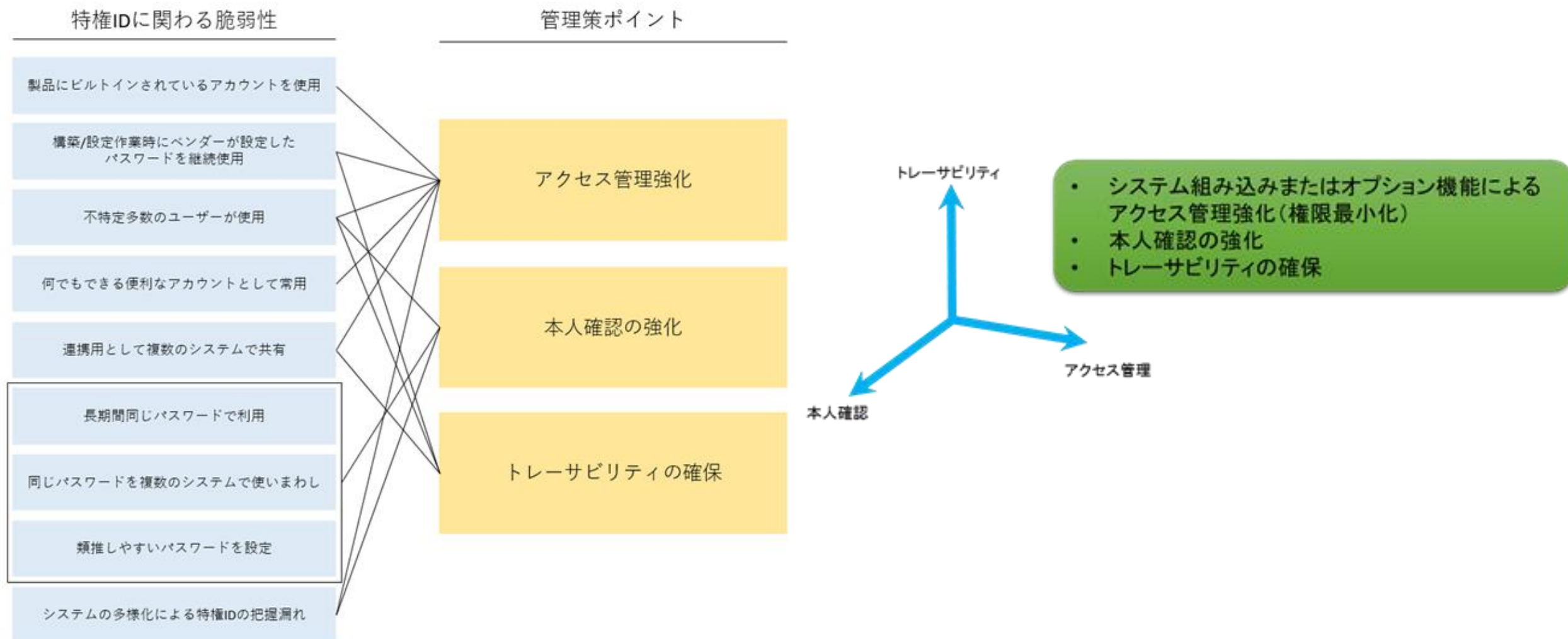
Appendix 各種標準化基準による特権ID管理

- ・ PCI DSS v4.0
- ・ ISO 27001での特権管理
- ・ システム管理基準(平成30年4月20日)
- ・ システム管理基準
追補版(財務報告に係るIT統制ガイダンス)
- ・ NIST SP800-53 Rev5

第2章 特権ID管理の課題と管理策

- 2.1. **特権IDに関わるリスク**
 - 2.1.1. ビルトイン管理者アカウントの利用
 - 2.1.2. 構築/設定作業時パスワードの継続利用
 - 2.1.3. 不特定多数の利用
 - 2.1.4. 特権IDの常用
 - 2.1.5. システム連携用ID
 - 2.1.6. 特権IDへ設定するパスワード
 - 2.1.6.1. 長期間同じパスワードでの利用
 - 2.1.6.2. 複数システムの特権IDに対して
共通のパスワードを設定
 - 2.1.6.3. 類推しやすいパスワードを設定
 - 2.1.7. システムの多様化による特権IDの把握漏れ
- 2.2. **特権IDの管理策**
 - 2.2.1. 理想と現実のギャップ
 - 2.2.2. 特権IDの管理策のポイント
 - 2.2.3. 特権IDの利用における現状と管理策の関係
 - 2.2.4. アクセス管理の強化
 - 2.2.4.1. 物理的なアクセス強化
 - 2.2.5. 本人確認の強化
 - 2.2.6. トレーサビリティの確保

解説編ポイントー特権IDの管理策



実践編のご紹介 1章～3章



第1章 特権IDの実装とは

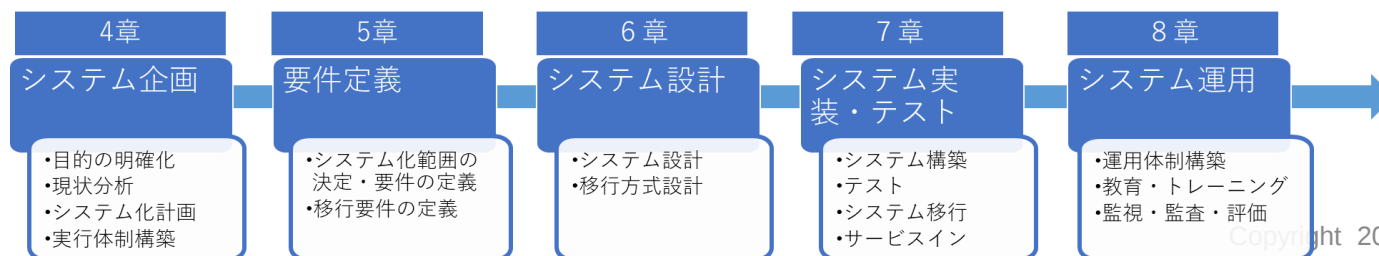
- 1.1. 特権ID管理に求められる内容
- 1.2. 特権ID管理における運用課題
- 1.3. 特権ID管理システムを利用する方式
 - 1.3.1. 特権ID管理システムの方式と違い
 - 1.3.2. 利用形態による違い
- 1.4. 特権ID管理システムを利用しない方式
- 1.5. 特権ID管理を行うための主要機能と標準技術

第2章 特権ID管理の現状把握と課題・リスクの訴求

- 2.1. 特権ID管理状況の現状把握と課題・リスクの明確化
 - 2.1.1. 特権ID管理対象システムの現状把握と課題・リスクの明確化
 - 2.1.2. 特権IDの現状把握と課題・リスクの明確化
 - 2.1.3. 特権ID利用者の現状把握と課題・リスクの明確化
- 2.2. システム環境の現状把握と課題・リスクの明確化
- 2.3. 特権ID管理運用の現状把握と課題・リスクの明確化

第3章 特権ID管理システム導入全体の流れ

- 3.1. 特権ID管理導入の流れ
- 3.2. 前提条件、留意事項



実践編のご紹介 4章～8章



第4章 特権ID管理システム企画フェーズ

- 4.1. 企画フェーズの目的
- 4.2. 特権ID管理の目的の明確化
- 4.3. 現状分析
- 4.4. 特権ID管理システム計画作成
- 4.5. プロジェクト体制

第5章 特権ID管理システム要件定義フェーズ

- 5.1. 要件定義フェーズの目的
- 5.2. 要件定義フェーズの前提条件
- 5.3. 特権IDシステムの要件定義
- 5.4. 実装方式の検討
- 5.5. 移行の要件定義

第6章 特権ID管理システム設計フェーズ

- 6.1. 設計フェーズの目的
- 6.2. 特権ID管理システムの設計
- 6.3. 移行計画の詳細化
- 6.4. 詳細設計

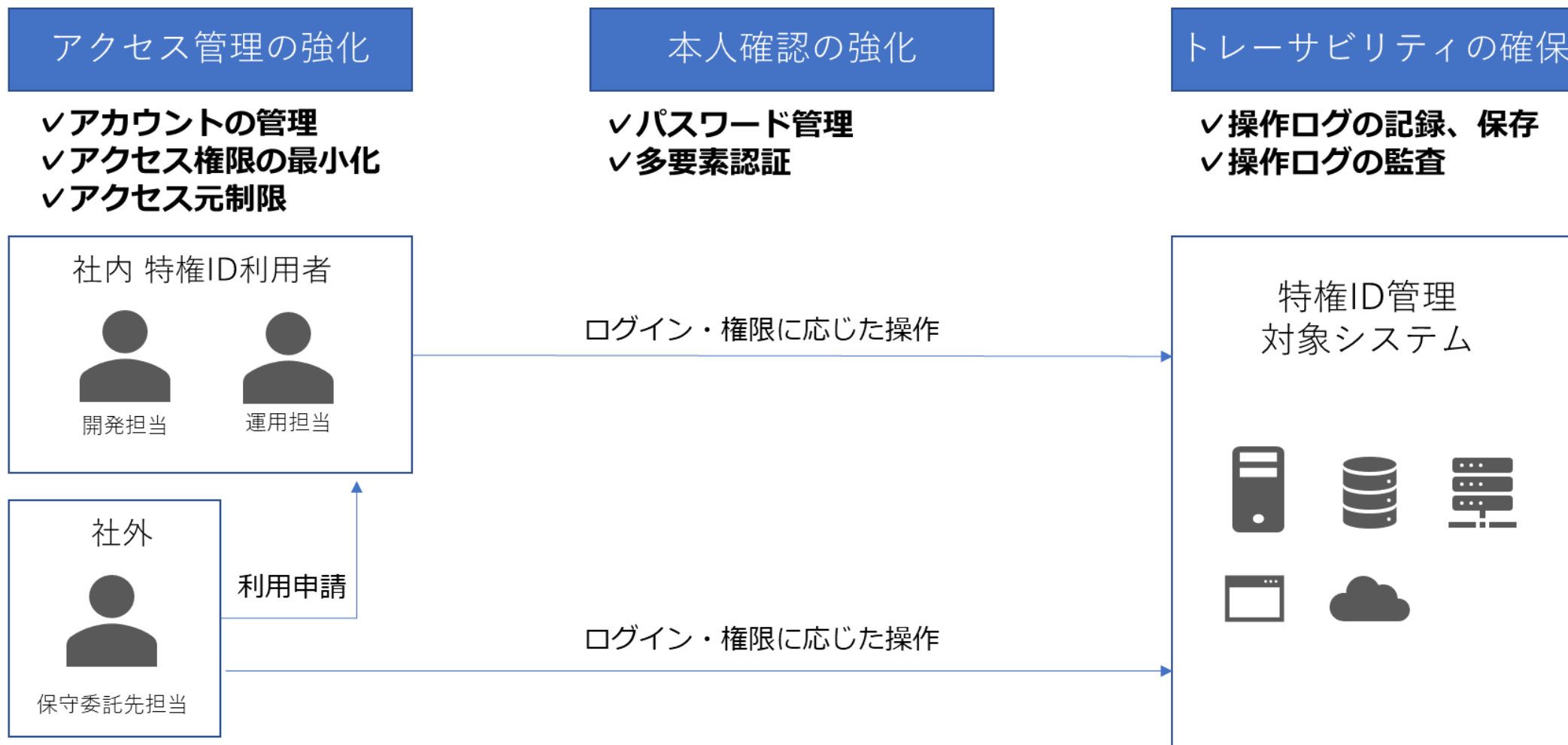
第7章 特権ID管理システム実装・テストフェーズ

- 7.1. システムの実装・テスト
- 7.2. 移行・サービスイン

第8章 特権ID管理システム運用フェーズ

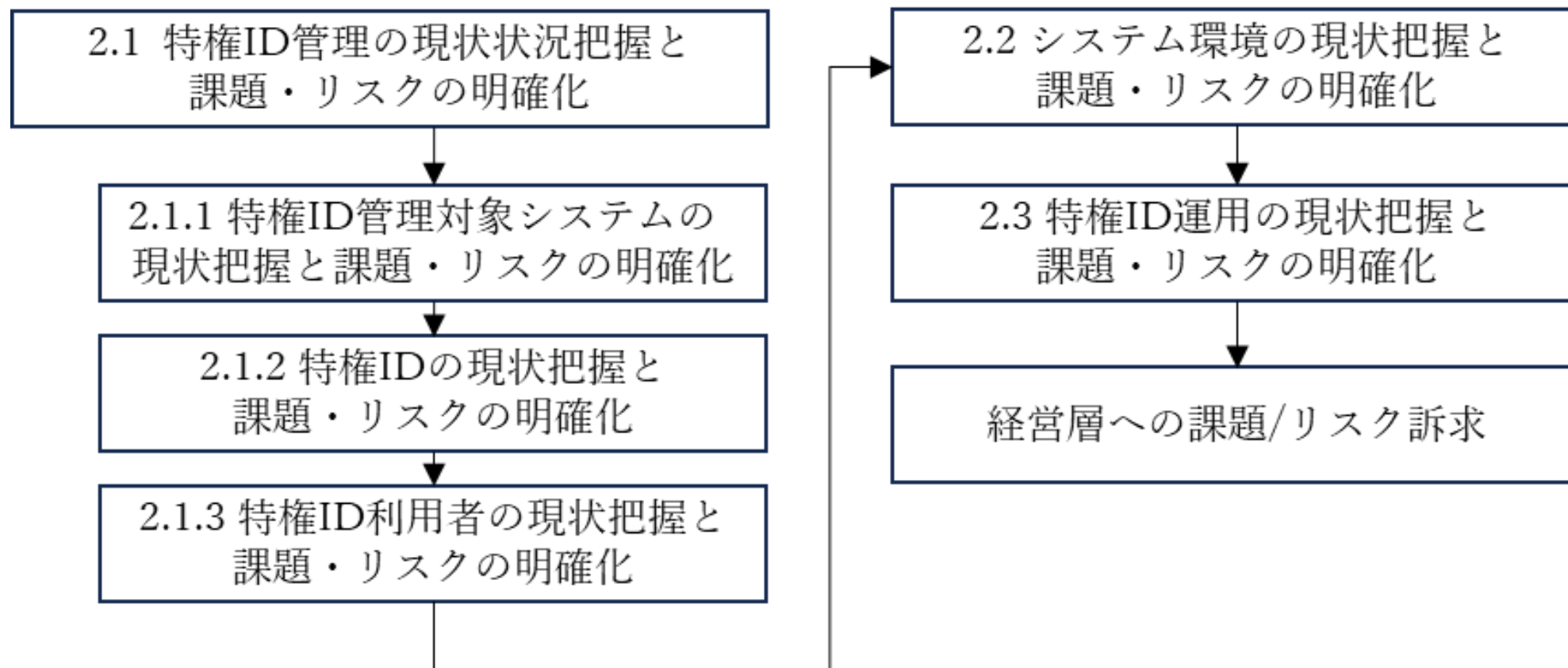
- 8.1. 運用設計
 - 8.1.1. 特権ID利用
 - 8.1.2. 特権ID管理システム運用
 - 8.1.3. 確認・保証
- 8.2. 特権ID管理体制
 - 8.2.1. 特権ID利用プロセス
 - 8.2.2. 特権ID管理システム運用プロセス
 - 8.2.3. ガバナンス/保証プロセス
- 8.3. 教育・トレーニング
 - 8.3.1. 特権ID管理の目的の理解
 - 8.3.2. 特権ID管理システムの利用法のトレーニング
 - 8.3.3. 緊急時対応手順
- 8.4. 監視・監査・レポーティング
 - 8.4.1. 監視
 - 8.4.2. 監査・レポーティング

特権ID管理システムに求められる内容



現状把握とリスクの明確化－ 1

特権IDの課題整理フロー

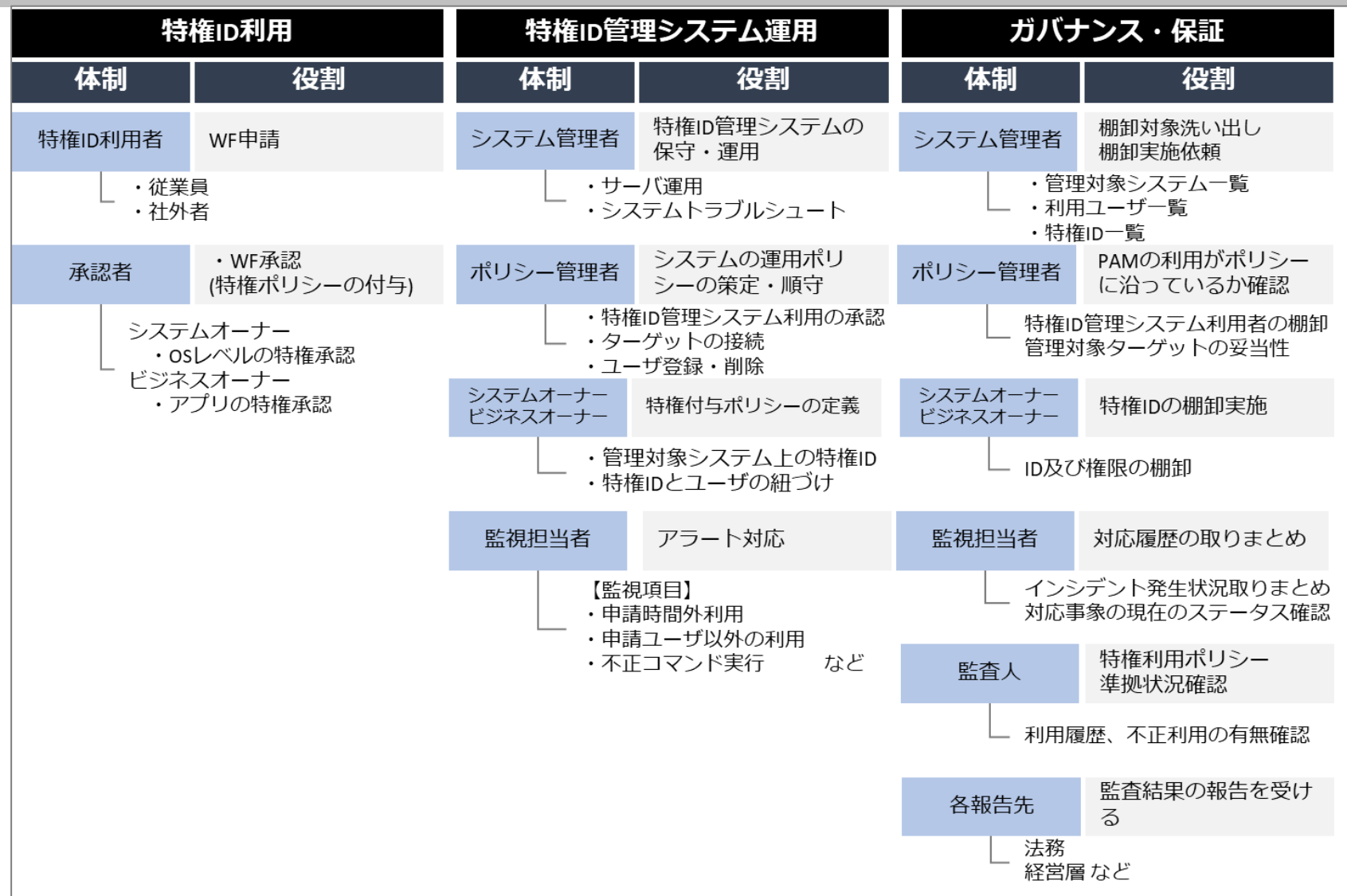


現状把握とリスクの明確化－ 2

特権ID対象システムと特権ID管理対象の洗い出し（例）

システム	環境	OS種別	重要データ/システム	特権ID	特権ID管理管理対象	特権IDの利用者	利用環境
サーバA	本番	Windows	○	Administrator	○	サーバ管理者 1	
サーバA	本番	Windows	○	Administrator	○	サーバ管理者 2	
サーバA	本番	Windows	○	Administrator	○	サーバ管理者 3	
サーバA	本番	Windows	○	サーバ管理者 1	○	サーバ管理者 1	
サーバA	本番	Windows	○	サーバ管理者 2	○	サーバ管理者 2	
サーバA	本番	DB	○	sa	○	DB管理者	
サーバB	本番	Linux	○	root	○	サーバ管理者 4	
サーバB	本番	Linux	○	管理者ID C	○	サーバ管理者 1	
サーバC	検証	Linux	○	root	○	サーバ管理者 1	
サーバD	検証	Linux	－	root	－	サーバ管理者 2	
NW機器A	本番	ネットワークOS	○	root	○	NW管理者 1	
...	...	...	...		...	...	
クラウドコンソール	本番	管理コンソール	○	IAM	○	サーバ管理者 3	
クラウドサーバA	本番	Windows	○	Administrator	○	サーバ管理者 1	
クラウドサーバB	本番	Linux	○	root	○	サーバ管理者 4	
...	...	...	...	...	...	...	

運用管理体制の例



【検討・執筆メンバー】

宮川 晃一 (WGリーダー)	日本電気株式会社
大竹 章裕	株式会社ラック
斎藤 知明	TIS株式会社
松井 祐輔	日本電気株式会社
吉本 紀浩	デロイトトーマツサイバー合同会社
石崎 貴嗣	デロイトトーマツサイバー合同会社
金子 敬祐	SCSK株式会社
内田 健一	NECソリューションイノベータ株式会社
番井 孝之	NECソリューションイノベータ株式会社
毛利 幹宏	株式会社アシスト
伊藤南美子	株式会社富士通エフサス
河原林 広	株式会社富士通エフサス
(順序不同)	

ご意見、お問合せ、WG参加等



事務局まで