JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

内部統制におけるアイデンティティ管理とは

2007年度　内部統制におけるアイデンティティ管理WG成果報告

グローバルセキュリティエキスパート株式会社
宮川　晃一
政策部会

2008 年 6 月13日

本WGの目的

内部統制におけるアイデンティティ管理WGの目的

J-SOX法における「内部統制」の必要性が叫ばれている中で、ITの全般統制として、ITセキュリティに関する対応の必然性が求められています。

その中でも、ID管理（アイデンティティマネージメント）分野については、セキュリティポリシーを実装する上での共通基盤として注目されている分野です。

内部統制とアイデンティティ管理の関連をWG討議の中で紐解き、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を狙うことを目的にしています。

2007年度の活動内容

1. 全体WGの開催 (3回)

   成果物のレビューを中心に開催した。

2. 事務局メンバWG (6回)

   成果物作成のための意見交換を中心に討議した。

3. 合宿 (1回)

   2008年2月22、23日　三浦マホロバマインズ　9名参加

   最終成果物の作成に向けた討議を実施

成果物

ータイトルー

「内部統制におけるアイデンティティ管理解説書」（第１版）

ー本書の目的ー

アイデンティティ管理に対する正しい理解をしていただき、

計画的で失敗のないシステム導入に寄与することを目的にした。

ー目次ー

第１章　アイデンティティ管理とは

第２章　アイデンティティ管理の意義

第３章　IT内部統制におけるアイデンティティ管理の位置づけ

第４章　アイデンティティ管理システム導入指針

（ＪＮＳＡ　ＨＰにて公開予定）

第1章　アイデンティティ管理とは (1)

第1章　アイデンティティ管理とは

アイデンティティ管理の必要とされる背景について考察した。

また、ID管理の目的と意義について解説し、その構成要素についても解説をした。

1．1　ID管理登場の背景 (歴史)

コンピュータパラダイムの変遷とID管理の必要性

ID情報をめぐる多くのステークスホルダー

1．2　定義

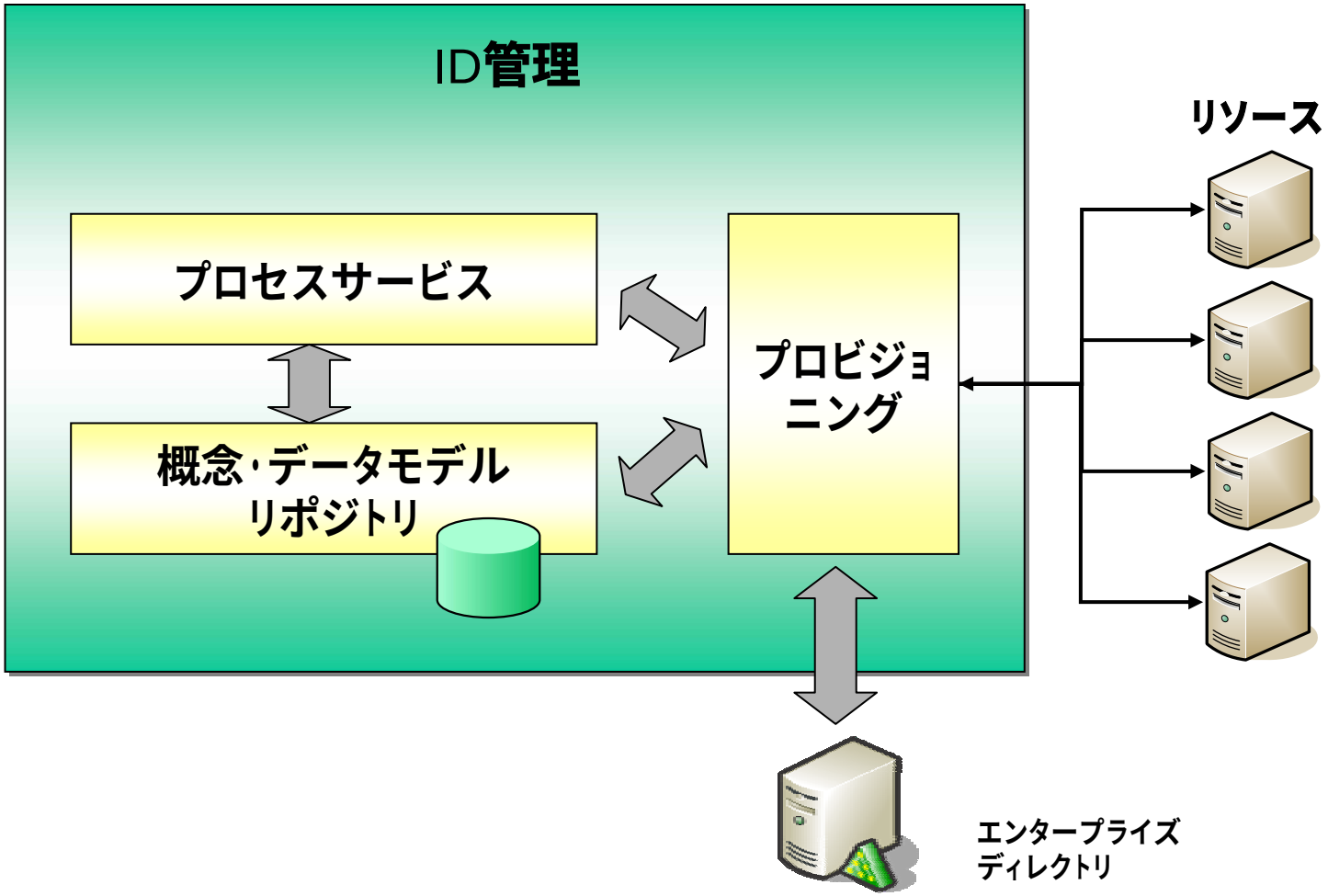
デジタルIDとは　‥‥　システム上に存在するユーザ個人のID

ユーザの視点からみるID情報　‥‥　ID情報の統制について

ID管理とは　‥‥　デジタルIDのライフサイクルを管理するもの

ID管理の構成要素　‥‥　プロビジョニング、IDサービス、リポジトリ　等

第1章　アイデンティティ管理とは (2)



第1章　アイデンティティ管理とは（3）

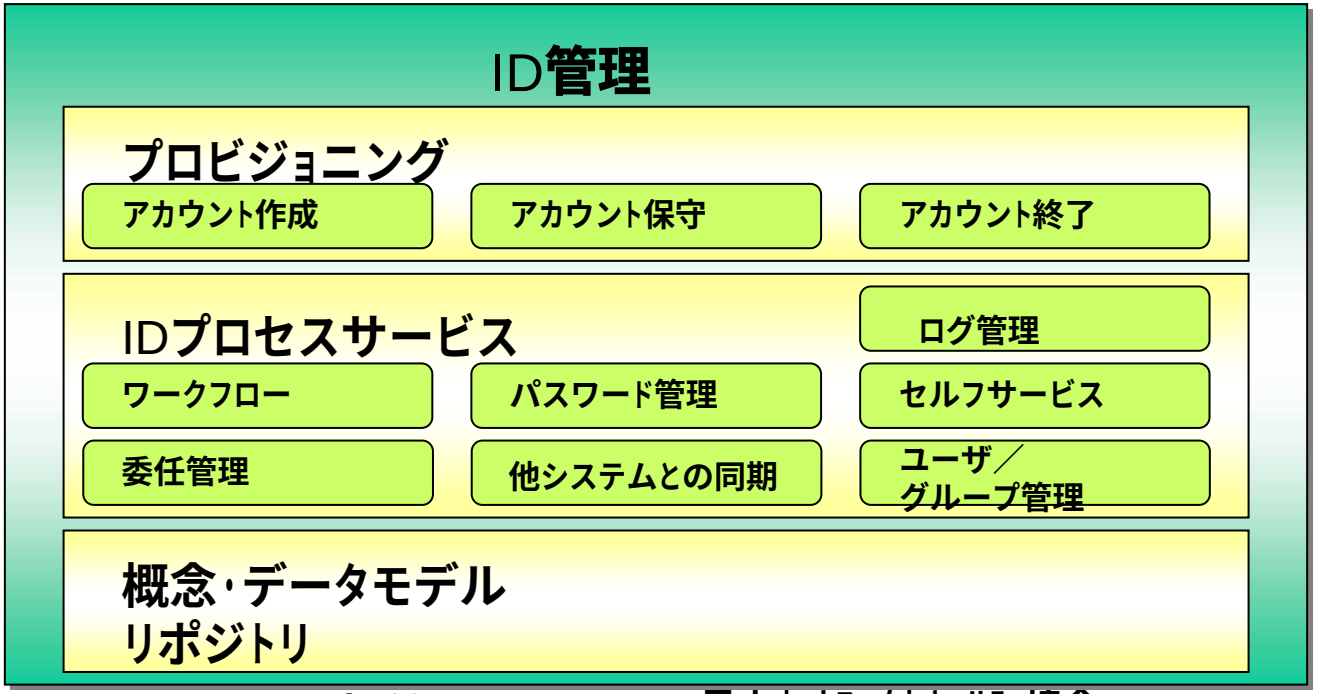
1．3　目的

・効果的にコンプライアンス要件を実現すること（内部統制、セキュリティ）

・企業の生産性向上

・コスト低減をはじめとしたIT管理効率の向上

1．4　内容



第2章　アイデンティティ管理の意義 (1)

第2章　アイデンティティ管理の意義

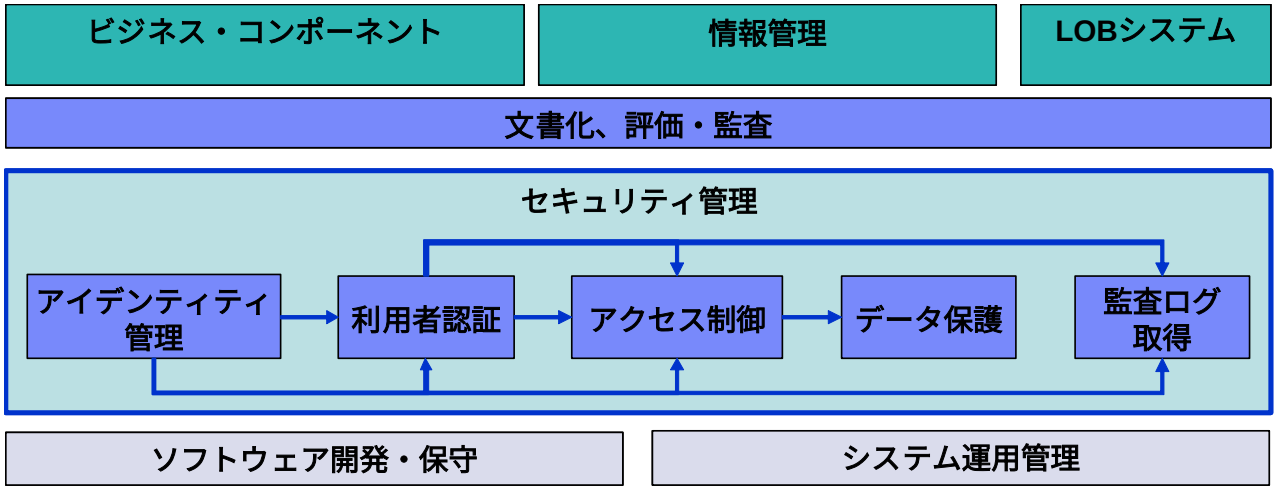
アイデンティティ管理の不備から発生したインシデント (事故) における教訓から
その果たす役割と意義について解説した。

2．1　企業システムにおけるアイデンティティ管理の位置づけ

2．1．1　IT全般統制におけるアイデンティティ管理

2．1．2　アイデンティティ管理に関連するインシデントと教訓

2．1．3　アイデンティティ管理の必要性



第2章　アイデンティティ管理の意義 (2)

2．2　アイデンティティ管理基盤導入における課題と解決

課題点	解決策
ID 運用管理ポリシの不備	実行性のある ID 運用管理ポリシのみに限定したポリシの策定
ID 管理基盤導入に対する認識不足	監査要求への対応コスト例示などによる外圧対応などのアプローチの検討
部門間の調整	ID 管理基盤導入についての認識を関連部局と共有し、漏れのない要件確定を担保
ID ライフサイクルの多様化	関連部局との調整
現状 ID 管理業務とのギャップ	全体最適の観点でのプロセス/システムの共通基盤化
データの標準化	順次巻き取りといった現実的な展開計画など、一部柔軟性を残した対応
各国法令への対応	法務部門との連携など個別管理より企業全体の基盤としての整備
広域 ID 管理基盤構築の課題	展開、運用、保守など多様な視点からの地域的差異を考慮した全体設計が必須

第2章　アイデンティティ管理の意義（3）

2．3　アイデンティティ管理の導入メリットと業界ごとの特徴

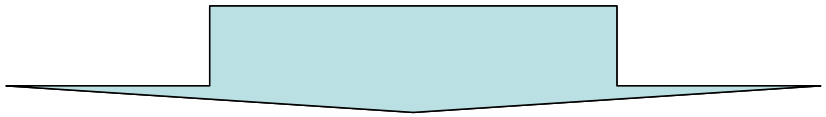
・セキュリティレベルの向上、コンプライアンス・内部統制への対応、
運用コストの最適化、監査コストの最適化

■作業工数算定式
①アイデンティティ（含む属性）を作成・更新・削除する作業
システム数×従業員数×人件費/時間×更新作業時間/件×更新回数/年

②登録する情報を伝達する作業および人的ミスによるコスト
システム数×人件費/時間×伝達ミスの浪費時間×連絡回数/件×年間勤務日数×（登録情報が間違っている割合/100）×従業員数

■想定パラメータ

・システム数	：10
・従業員数	：5,000人
・人件費/時間	：3,000円
・更新作業時間/件	：0.5時間
・更新回数/年	：1回
・伝達ミスによる浪費時間	：0.1時間
・連絡回数/件	：1回
・年間勤務日数	：200日
・登録情報間違いの割合	：1％



■アイデンティティ管理基盤導入前
①アイデンティティ（含む属性）を作成・更新・削除する作業
システム数×従業員数×人件費/時間×更新作業時間/件×更新回数/年
10×5,000×3,000×0.5×1＝75,000,000円
②登録する情報を伝達する作業および人的ミスによるコスト
システム数×従業員数×人件費/時間×伝達ミスの浪費時間×連絡回数/件×年間勤務日数×（登録情報が間違っている割合/100）
10×5,000×3,000×0.1×1×200×（1/100）＝30,000,000円
合計：***105,000,000円***

■アイデンティティ管理基盤を導入することによる削減コスト
①アイデンティティ（含む属性）を作成・更新・削除する作業
（システム数－1）×従業員数×人件費/時間×更新作業時間/件×更新回数/年
（10－1）×5,000×3,000×0.5×1＝67,500,000円
②登録する情報を伝達する作業および人的ミスによるコスト
システム数×従業員数×人件費/時間×伝達ミスの浪費時間×連絡回数/件×年間勤務日数×（登録情報が間違っている割合/100）
（10－1）×5,000×3,000×0.1×1×200×（1/100）
＝27,000,000円
合計：***94,500,000円***

削減効果＝10,500,000円/年

第3章　IT内部統制における アイデンティティ管理の位置づけ（1）

第3章　IT内部統制におけるアイデンティティ管理の位置づけ

IT内部統制においてアイデンティティ管理がどのように位置づけられており、

また、IT内部統制の観点からどのようなことが要求されるのかについて解説を行なった。

3．1　IT内部統制の必要性

3．2　IT内部統制のフレームワーク

3．3　COBITにおけるアイデンティティ管理の位置づけと要求事項

3．4　ISMSにおけるアイデンティティ管理の位置づけと要求事項

3．5　COBIT、ISMSにおけるID管理についての考察

第3章　IT内部統制における アイデンティティ管理の位置づけ（2）

COBIT DS5.3 IDマネジメント

IT システムにおける**すべてのユーザ**(内部、外部、臨時かどうかを問わず)と、
ユーザの**すべてのアクティビティ**(ビジネスアプリケーションやシステムの操作、開発や保守)を、
個々に識別しなくてはならない。

システムやデータに対するユーザのアクセス権は、**文書化された業務上の必要性や職務要件に即したもの**でなければならない。

ユーザのアクセス権は、**ユーザ管理職の申請に基づいてシステムオーナが承認**し、
セキュリティ責任者が実装する。

ユーザID とアクセス権は、**単一のリポジトリで集中管理**する。

ユーザの識別、認証の実施、およびアクセス権の徹底管理のために、**費用効率に優れた技術面および手続面での対策**を講じ、常に継続的な改善を行う。

出展：日本ITガバナンス協会（ITGI）

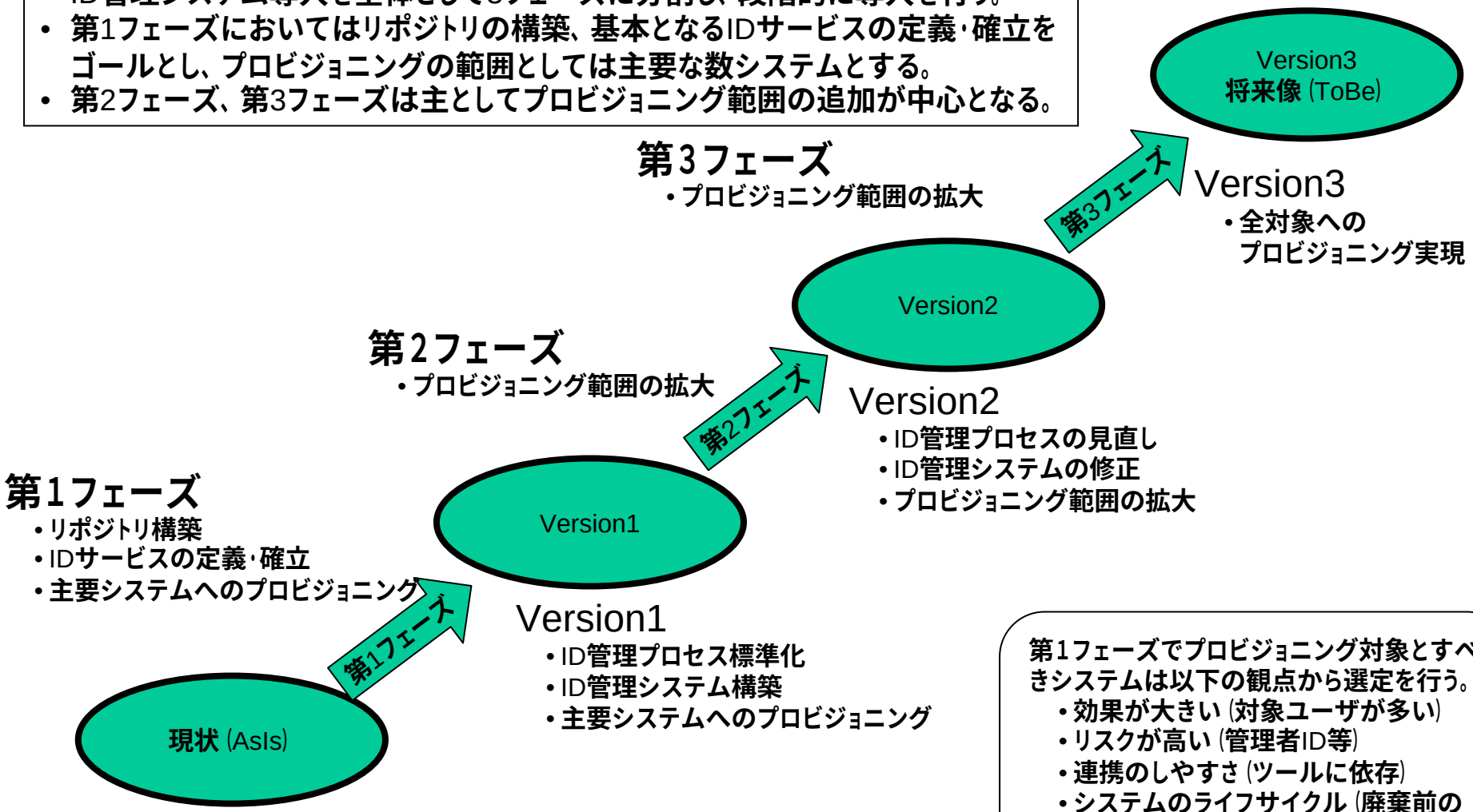
第4章　アイデンティティ管理
システム導入指針（1）

第4章　アイデンティティ管理システム導入指針
　アイデンティティ管理システムを導入するにあたってのステップと導入に際して注意すべき点を中心にまとめた。

4.1. 概要
4.2. プロジェクト管理
4.3. 全体計画
4.4. 導入計画策定
4.5. IDサービス定義
4.6. IDサービス設計（外部設計）
4.7. IDサービス設計（詳細設計）
4.8. IDサービス実装・テスト
4.9. プロビジョニング
4.10. プロビジョニング設計
4.11. プロビジョニング実装・テスト
4.12. リポジトリ
4.13. 移行
4.14. 基盤（インフラストラクチャ）定義
4.15. 基盤設計
4.16. 本番環境構築
4.17. 開発・テスト環境構築
4.18. 運用定義
4.19. 運用設計
4.20. 教育・トレーニング

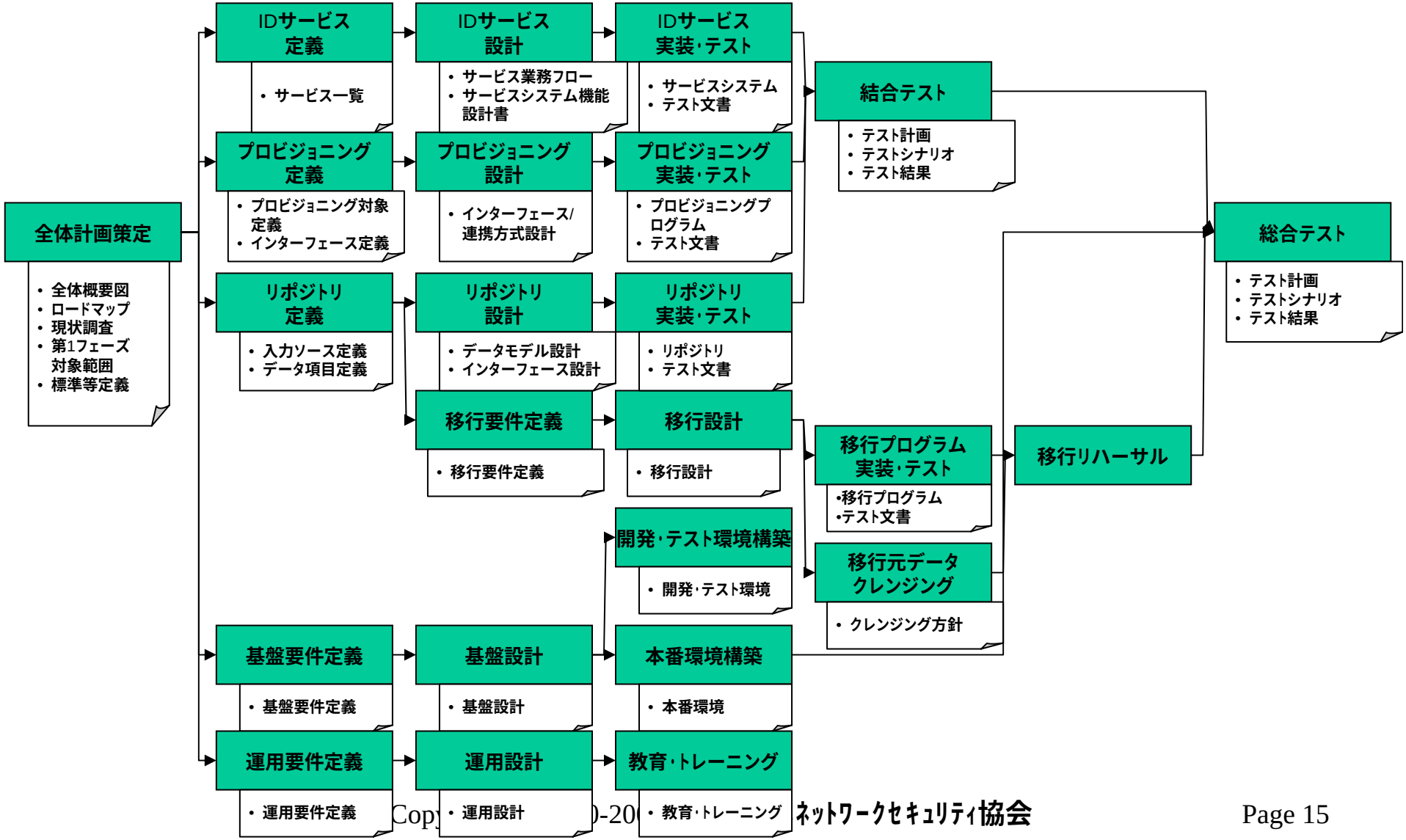
第4章　アイデンティティ管理
システム導入指針（2）

- ID管理システム導入を全体として3フェーズに分割し、段階的に導入を行う。
- 第1フェーズにおいてはリポジトリの構築、基本となるIDサービスの定義・確立をゴールとし、プロビジョニングの範囲としては主要な数システムとする。
- 第2フェーズ、第3フェーズは主としてプロビジョニング範囲の追加が中心となる。



第1フェーズでプロビジョニング対象とすべきシステムは以下の観点から選定を行う。
- 効果が大きい（対象ユーザが多い）
- リスクが高い（管理者ID等）
- 連携のしやすさ（ツールに依存）
- システムのライフサイクル（廃棄前のシステムには行わない）
- RBACがきちんと整備されている

第4章　アイデンティティ管理
システム導入指針（3）



謝　辞

本成果物にご協力していただいた皆様へ

ご協力いただき、大変ありがとうございました。

本書執筆メンバー（順不同、敬称略）

中島　浩光	株式会社インフォセック
星野　敏彦	日本ヒューレット･パッカード株式会社
長崎　健一	日本ヒューレット･パッカード株式会社
丹羽　奈津子	日本アイ･ビー･エム株式会社
竹日　正弘	日本アイ･ビー･エム株式会社
酒井 美香	日本アイ･ビー･エム　システムズ･エンジニアリング株式会社
北野　晴人	日本オラクル株式会社
澤井　真二	日本オラクル株式会社
小林　智恵子	東芝ソリューション株式会社
富士榮　尚寛	伊藤忠テクノソリューションズ株式会社

謝　辞

ワーキングメンバー（順不同、敬称略）

柿崎　　司	株式会社アクシオ
工藤　浩	伊藤忠テクノソリューションズ株式会社
佐藤　隆哉	ＮＥＣネクサソリューションズ株式会社
茂垣　武文	ＮＴＴコミュニケーションズ株式会社
番野 邦彦	キヤノンシステムソリューションズ株式会社
小澤　浩一	京セラコミュニケーションシステム株式会社
篠原　信之	グローバルセキュリティエキスパート株式会社
鈴木　靖	グローバルセキュリティエキスパート株式会社
神宮寺　　健	グローバルセキュリティエキスパート株式会社
石田 弘也	日商エレクトロニクス株式会社
山本　扇治	日本アイ･ビー･エム　システムズ･エンジニアリング株式会社
大星　歓子	日本CA株式会社
鈴木　良信	日本CA株式会社
小坂　嘉誉	日本CA株式会社
則房　雅也	日本電気株式会社
柴田　浩一	日本電気株式会社
堀部　修一	日本ユニシス株式会社
小宮山 智之	日本ユニシス株式会社
高木　経夫	株式会社ネットマークス
大竹　章裕	株式会社ネットマークス
川口　龍之進	株式会社日立製作所
富山　朋哉	株式会社日立製作所
下江　達二	富士通株式会社
石井　章夫	富士通株式会社
渡木　厚	富士通株式会社
恵美　玲央奈	株式会社富士通ソーシアルサイエンスラボラトリ
今堀　秀史	富士通関西中部ネットテック株式会社
江谷　為之	富士通関西中部ネットテック株式会社
勝見　勉	リコー･ヒューマン･クリエイツ株式会社