

クラウド環境における ID管理プロジェクトの進め方のキモ

伊藤忠テクノソリューションズ株式会社
富士榮 尚寛

Twitter : @phr_eidentity

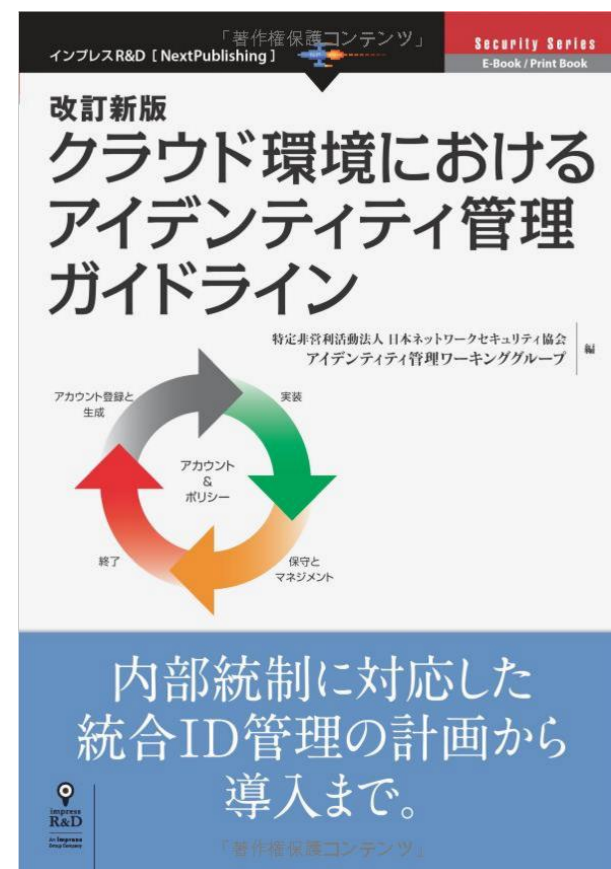
Blog : IdM実験室 (<http://idmlab.eidentity.jp>)



- 当WG主要成果物の紹介
- ID管理プロジェクトの現実
- どうすべきか？
 - 企画フェーズ
 - 要件定義フェーズ
- その他のポイント
- まとめ

当WG主要成果物

1. アイデンティティ管理（ID管理）とは
2. ID管理の意義
3. IT内部統制におけるID管理の位置付け
4. クラウド環境におけるID管理の位置付け
5. グローバルビジネス環境におけるID管理
6. ID管理システム導入指針
7. ID管理システムにおける仮想企業導入事例
8. ID管理アンチパターン
9. ID管理に関するFAQ



ID管理プロジェクトの現実

ID管理プロジェクトの現実

フェーズの進行

企画

要件定義

導入

運用

様々な
課題

絞り込み、
優先順位付け

当初やり
たかった
こと

導入ベンダと
のせめぎあい

コスト検討、
実現可能性

運用対処
する範囲

システム
化範囲

ユーザからの
不満等

PJを開始
後、やり
たくなっ
てくるこ
と

運用開始
後、やり
たくなっ
てくるこ
と

何故ギャップが生まれるのか

フェーズの進行

企画

要件定義

導入

運用

様々な
課題

絞り込み、
優先順位付け

当初やり
たかった
こと

導入ベンダと
のせめぎあい

コスト検討、
実現可能性

運用対処
する範囲

システム

ユーザからの
不満等

PJを開始
後、やり
たくなっ
てくるこ
と

運用開始
後、やり
たくなっ
てくるこ
と

1. 目的の明確化と現状分析の漏れ

⇒課題との対応付けが正しく定義できず、
運用が開始されても効果が出ない

何故ギャップが生まれるのか

フェーズの進行

企画

要件定義

導入

運用

様々な
課題

絞り込み、
優先順位付け

当初やり
たかった

導入ベンダと
のせめぎあい

コスト検討、
実現可能性

運用対処
する範囲

システム

ユーザからの
不満等

PJを開始
後、やり
たくなっ
てくるこ
と

運用開始
後、やり
たくなっ
てくるこ
と

2. 要件定義漏れ

⇒現状分析が甘く、運用が開始されてから例外
ケースが多発したり、運用上無理が発生する

何故ギャップが生まれるのか

フェーズの進行

企画

要件定義

導入

運用

様々な
課題

絞り込み、
優先順位付け

当初やり
たかった
こと

導入ベンダと
のせめぎあい

コスト検討、
実現可能性

運用対処
する範囲

ユーザからの
不満等

PJを開始
後、やり
たくなっ
てくるこ
と

運用開始
後、やり
たくなっ
てくるこ
と

3. I/F設計、移行設計漏れ

⇒対抗システムとのI/F設計・合意が甘く、追加開発が発生したり、移行用の別機能開発が発生

何故ギャップが生まれるのか

フェーズの進行

企画

要件定義

導入

運用

様々な
課題

絞り込み、
優先順位付け

当初やり
たかった
こと

導入ベンダと
のせめぎあい

コスト検討、
実現可能性

運用対処
する範囲

システム

ユーザからの
不満等

PJを開始
後、やり
たくなっ
てくるこ
と

運用開始
後、やり
たくなっ
てくるこ
と

4. 現状分析・課題の抽出不足

⇒企画の段階で課題の抽出があまく、実情に沿わない部分が発生

何故ギャップが生まれるのか

フェーズの進行

企画

要件定義

導入

運用

絞り込み、

導入ベンダと
のせめぎあい

ユーザからの
不満等

**上流工程（企画～要件定義）での
漏れが後々引きずる。**

化範囲

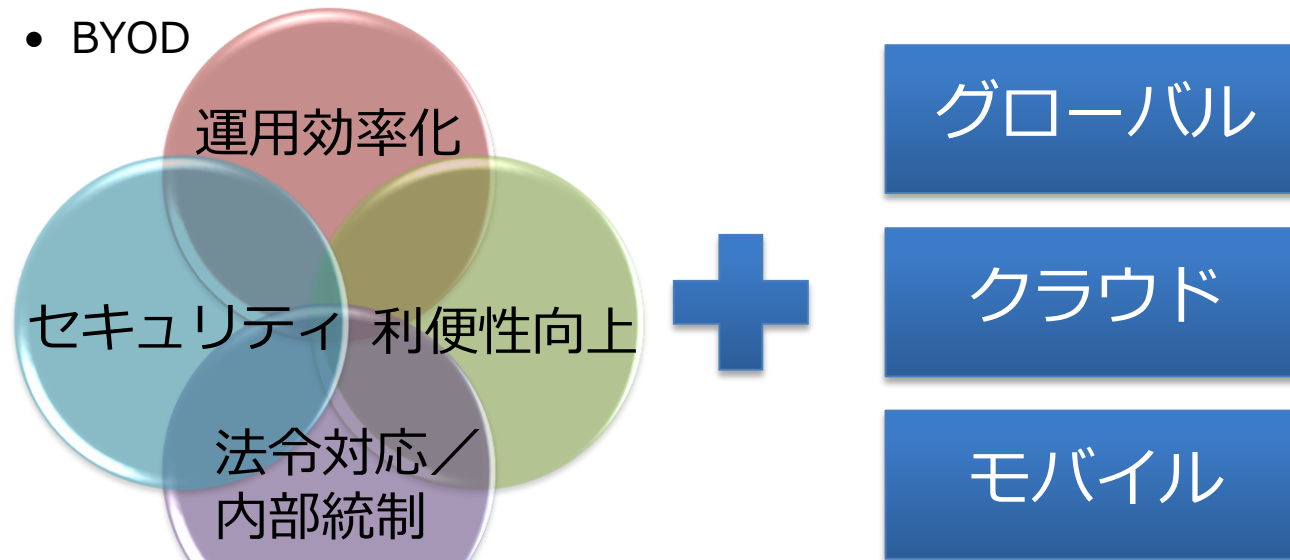
どうすべきか？ (特に企画、要件定義)

- 成果物 第6章 ID管理システム導入指針
 - －6.2 企画フェーズ
 - 6.2.1 目的の明確化
 - 6.2.2 現状分析
 - 6.2.3 ID管理システム計画案作成
 - 6.2.4 ID体系の決定
 - 6.2.5 ID管理運用体制・役割の決定

- そもそもID基盤が何なのか理解できないし、企画を通す上で説明できない
 - 検索すると、SAML（さむる、さむえる、さむおー）やOpenID Connect、OAuth、プロビジョニング、フェデレーションなど謎の用語が出てくる
 - 認証とか認可とかポリシーとかトラストなどの概念的な話が多い
 - そもそもID（番号）とアイデンティティって何が違うの？
- そもそもID基盤の導入なんて誰もやりたくない
 - 目的がはっきりしない
 - 誰がプロジェクト・オーナー？
- 結果、予算が取れない（結構簡単に企画が頓挫・スリップする）
 - 値ごろ感がわからない
 - 業務システム側への影響（改修）が発生するの？

• テクニカル用語は無視、目的をはっきりと！

- そもそもID基盤を導入したい訳ではないのは真実
- 大体のプロジェクトはこんな理由で始まる
 - アプリケーションをグループ&グローバルで共同利用したい
 - 監査に引っかかった
 - クラウド（Office365, GoogleApps, Salesforceなど）を使いたい
 - BYOD



• 目的が明確になれば後は自然に

– プロジェクト・オーナー：課題を抱えている部隊

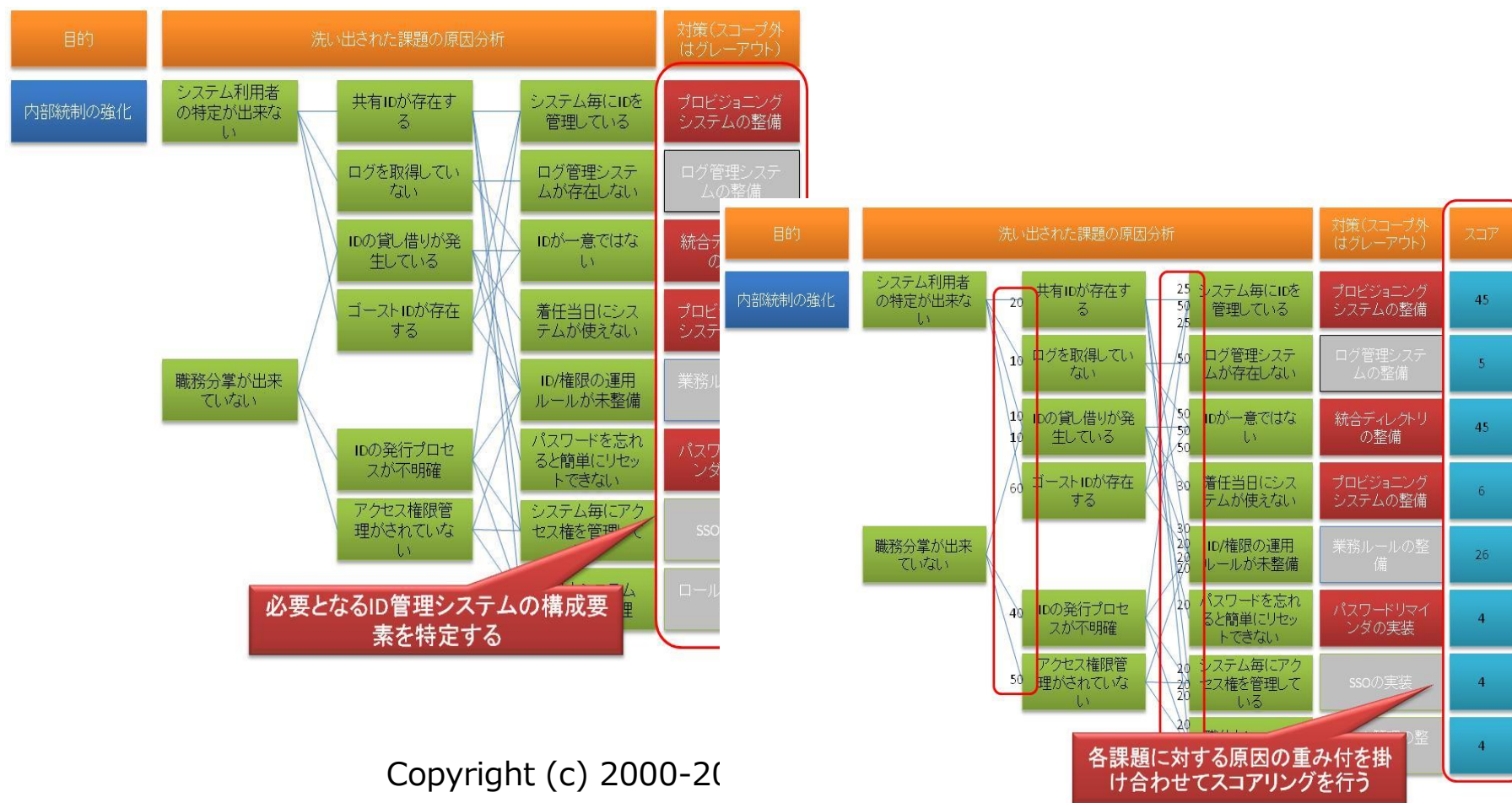
- クラウドを使いたい部隊
- 監査で引っかかって困っている部隊
- アプリケーションや情報を共有したい部隊
- 複数の目的が絡む場合は？
 - 本来一番いいのはトップダウンでの全社プロジェクト
 - スモールスタートがおススメ

– 値ごろ感：ある程度は定量的に比較

- 手運用 vs システム、リスク vs システム化コスト
- RFIレベルでもざっくり比較はできるはず
- 本当は今後のロードマップも踏まえて検討したい

● 目的との対応を明確化するための工夫の例

－ 目的⇒課題と原因⇒対策へのブレイクダウンと定量化



- 成果物 第6章 ID管理システム導入指針
 - 6.3 要件定義
 - 6.3.1 IDサービスの要件定義
 - 6.3.2 プロビジョニングの要件定義
 - 6.3.3 レポジトリの要件定義
 - 6.3.4 移行の要件定義

- そもそも要件定義フェーズは分けられるか
 - 委託者は総額で発注したい、受託者は刻みたい
 - そもそも企画フェーズで明確なRFPが書けていないから？
- 夢、膨らむ
 - 「ついでに」やりたいことが一杯出てくる
 - アクセス権の自動付け替えやグループ（ロール）管理までやりたくなる
- 夢、破れる
 - 信頼できるIDソースなんて存在しないことがわかる
 - 業務システム側のインターフェイス仕様なんて誰も知らない、もしくは業務システム側にも大幅な改修が必要になることが判明する
 - 現状のID管理業務があまりにも属人的なことが判明する

- 最初から開発プロジェクトのつもりで挑む（これは企業側へのお願い事項）
 - 単なる物品の調達とは違う（そのつもりでRFPも書く）
- 目的との対応を定期的に行い、お花畑的な発想は早めに消し去る
 - プロジェクト・ルームに目的を張り出しておいてもやり過ぎではない？
- 100%の網羅性を持つ必要が本当にあるのか
 - 管理対象のグループ会社が10社あったとして3社正しく管理できれば3割バッター。リスクを定量的に低減できる
 - 最初から打率をあげるよりも代替手段の検討をする
 - 徐々に打率をあげて行けば良い
- ID管理に関する業務プロセスを厳密に定義しない
 - 本来はあるべきプロセスを定義した上でシステム化すべき
 - 大ごとになり先に進まず柔軟性も無くなる。後から変えられる設計の方が重要（DevOps的に）

その他のポイント

要件を本当に固められるのか？ JNSA

- 要件定義～設計～開発・・・という儀式は必要か？
 - もっとゆるくシステム化してもよいのでは？
 - スモールスタート、プロトタイピングも一つの手段
- 最近クラウドとの連携がメインということもあり、プロトタイプから始める方がよい？
 - 想像以上にクラウド・サービスの仕様が変わる速度は速く、設計しても無駄になる可能性も
 - 目に見えないシステムなので、どれだけ早い段階で運用をイメージできるか、がポイント
- 統合ディレクトリの整備、IDライフサイクル管理の整備、認証基盤の整備、という順番だけが解ではない
 - キレイなシステム化は不要
 - ある程度のカバレッジがあれば効果は出る
 - スピードの方が大切

要件を本当に固められるのか？ JNSA

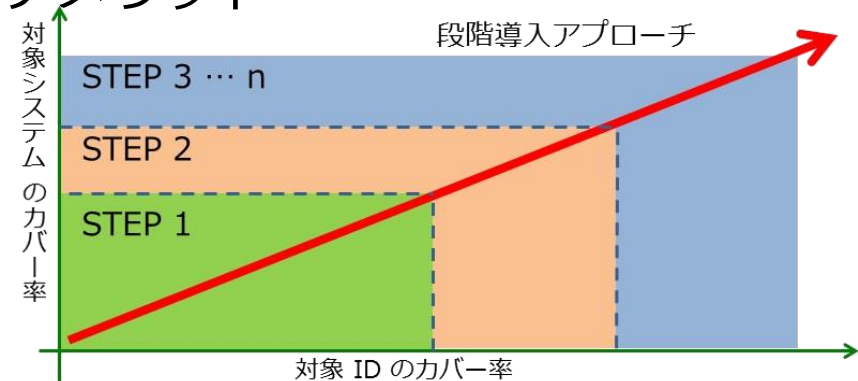
• スモールスタート（段階導入）のススメと留意点

– スモールスタートのメリット・デメリット

- メリット
 - 初期コストが少なく済む
 - 立ち上げスピードが速い
- デメリット
 - 手戻りが発生する場合も

– デメリットを極小化するために

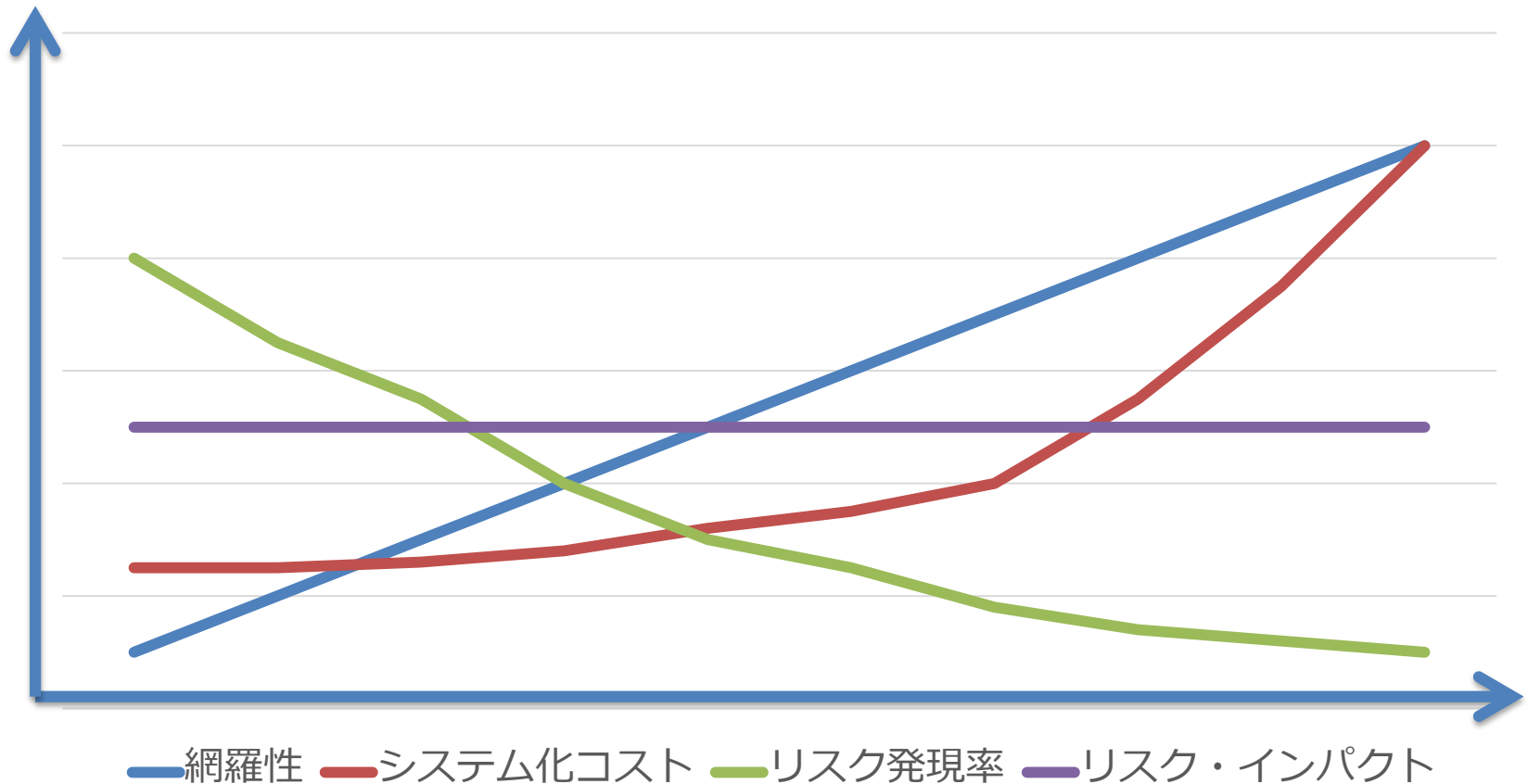
- 手戻りするパターンと事前に考慮しておくべき事項
 - ID体系
 - » グループ企業などへ展開するときに採番体系が足りるか？
 - 接続したいシステムの技術的制約
 - » 利用インターフェイス、プロトコル、ドメイン名（特にクラウドの場合）は十分検討（最悪CSV）
 - » 技術的な制約事項であればID基盤のリプレイス時に機能追加が可能な場合も多い



要件を本当に固められるのか？ JNSA

- 完璧さを求めない

- リスク発現率 × インパクトに応じたシステム化（網羅性）



まとめ

- **セオリー通りに言えば「上流大事」**
 - ここで間違えると後で困る
 - 成果物に進め方、留意点が記載されているので参考に
- **要件が固められる自身がなければプロトタイプニングなど、他の手段も検討**
 - 特にクラウド連携はスピードが大事
 - 完璧を求めない

