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

JNSA 2018年度活動報告会

「2018年度 アイデンティティ管理WG 成果報告」

デジタルアイデンティティWGリーダー
日本電気株式会社（NEC)
宮川　晃一

2018年　6月　12日

WG活動報告内容

1．WGの紹介

2．2018年度の活動内容サマリ

3．成果紹介

4．2019年度の活動テーマ

1．WGのご紹介

WGの目的

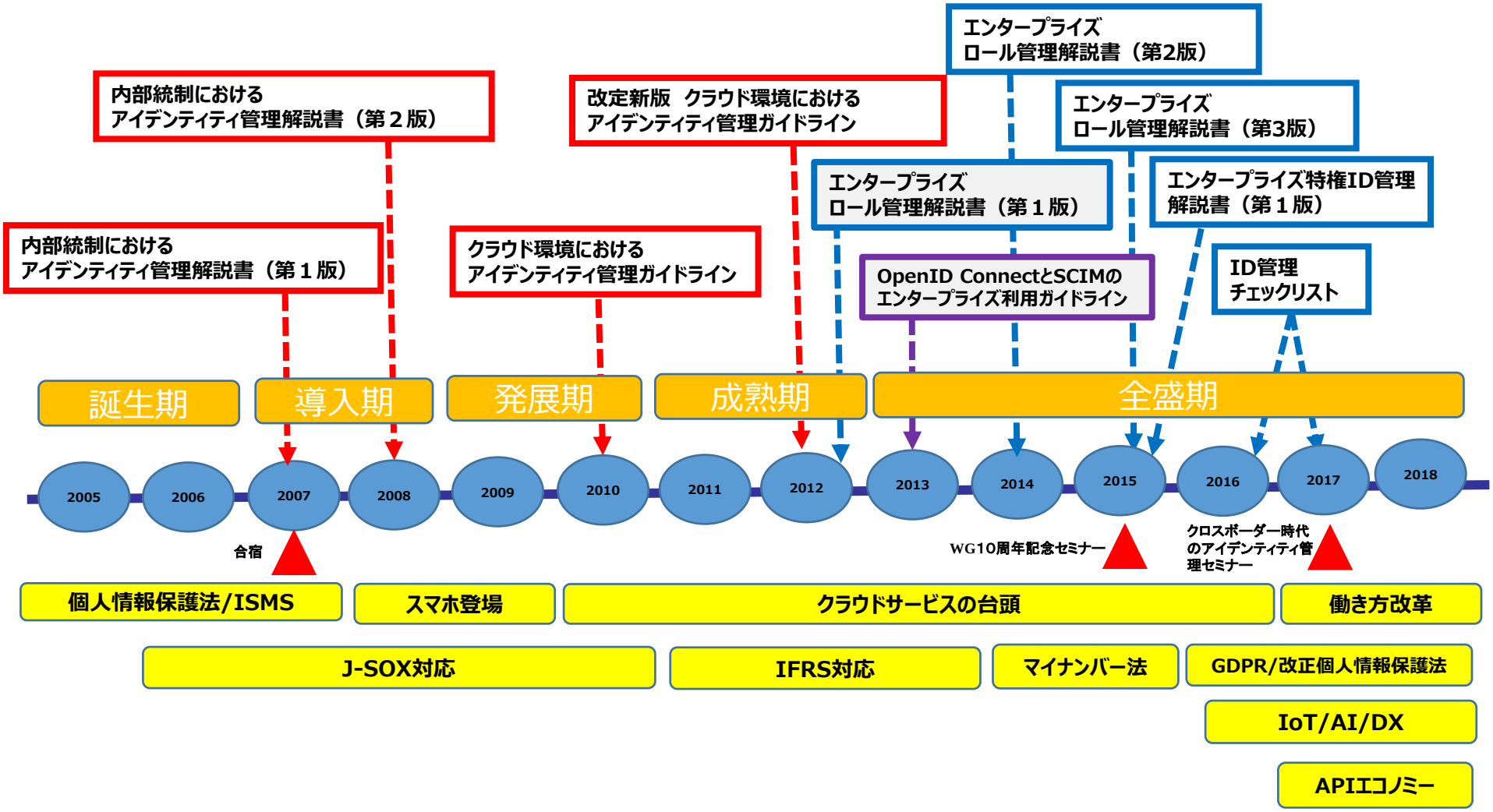
「アイデンティティ管理WGの目的」

昨年度までエンタープライズIDを中心とした「アイデンティティ管理WG」
として活動してきました。
本年度よりWG名称を「デジタルアイデンティティWG」と改変し、
デジタルアイデンティティ全般を広く議論する場にしたく思います。

　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、
導入指針や各種レポートの提示などにより、啓蒙活動、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た活動を行います。

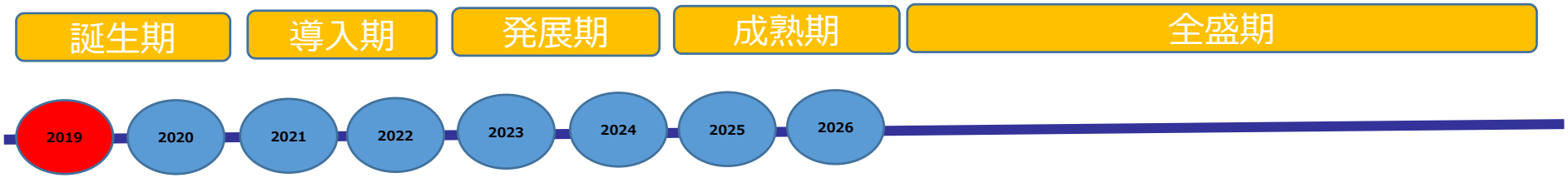
２００５年からWGを発足し今年で１４年目のWGです。

WGの沿革（平成時代）



WGの沿革（令和時代）

デジタルアイデンティティWG（2ndシーズン）



- APIエコノミー
- デジタルKYC
- 情報銀行／PDS
- キャッシュレス決済
- GDPR施行
- ・
- ・
- ・
- ・
- ・
- ・

＜これまでの成果物＞

１．エンタープライズロール管理解説書（第３版）
http://www.jnsa.org/result/2016/idm_guideline/index.html

２．エンタープライズにおける特権ID管理解説書（第１版）
http://www.jnsa.org/result/2016/idm_pum/index.html

３．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）
http://www.jnsa.org/press/2013/131220.pdf
https://www.openid.or.jp/news/2013/12/openid-openid-connectscim.html

４．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

出版書籍の紹介

書籍名：＜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

出版社：インプレスR&D NextPublishing

形態：電子書籍、Ondemand Print(POD)

販売： Amazon
インプレスR&D libura PRO

http://www.amazon.co.jp/dp/4844395866

WGメンバー紹介HP

HP: http://www.jnsa.org/active/std_idm.html

2019年度メンバー

計５７名
敬称略
会社名：五十音順

JNSA

氏名	会社名
宮川　晃一	日本電気株式会社
貞弘 崇行	株式会社アイピーキューブ
八束 啓文	EMCジャパン株式会社
齊藤亘	EMCジャパン株式会社
篠原 信之	イオンアイビス株式会社
新嘉喜　康治	伊藤忠テクノソリューションズ株式会社
富士榮 尚寛	伊藤忠テクノソリューションズ株式会社
稲吉 英宗	伊藤忠テクノソリューションズ株式会社
土井寛子	伊藤忠テクノソリューションズ株式会社
木村 慎吾	株式会社インテック
深澤 聡	SCSK株式会社
金子 敬祐	SCSK株式会社
吉川　由希子	NRIセキュアテクノロジーズ株式会社
内田 健一	NECソリューションイノベータ
岡崎　一洸	NECソリューションイノベータ
星野 亮	株式会社エヌ・ティ・ティ・データ
佐藤　可奈子	株式会社エヌ・ティ・ティ・データ
山田 達司	株式会社エヌ・ティ・ティ・データ
杉村 耕司	エヌ・ティ・ティ・データ先端技術株式会社
久米田　博	NTTテクノクロス株式会社
坂本 泰久	NTTアドバンステクノロジ株式会社
澤井 真二	KPMGコンサルティング株式会社
万仲 隆之	KPMGコンサルティング株式会社
畠山 誠	KPMGコンサルティング株式会社
深谷　貴宣	ServiceNow Japan株式会社
斎藤　知明	TIS株式会社
安部　高城	TIS株式会社
宮村　亮多	TIS株式会社
櫻田仁詩	有限責任監査法人トーマツ
大森潤	有限責任監査法人トーマツ
大島和紘	有限責任監査法人トーマツ
栃沢 直樹	トレンドマイクロ株式会社
板倉 景子	日本アイ・ビー・エム株式会社
市川 貴浩	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
飯塚 昭	日本オラクル株式会社
木村　優一	日本セーフネット株式会社
新谷　佳希	日本セーフネット株式会社
呉 若旻	日本セーフネット株式会社
奥野　雅広	株式会社　日本総合研究所
吉嶋 正和	株式会社 日本総合研究所
桑田 雅彦	日本電気株式会社
駒沢 健	日本電信電話株式会社
見上 昌成	日本ビジネスシステムズ株式会社
川田 拓	日本ビジネスシステムズ株式会社
安納 順一	日本マイクロソフト株式会社
上杉康雄	日本マイクロソフト株式会社
渥美 淳一	ネットワンシステムズ株式会社
福田 尚弘	パナソニック株式会社
小川　剛弘	富士ソフト株式会社
楠田　展久	富士ソフト株式会社
宮崎　弘道	富士ソフト株式会社
福原 幸一	富士通関西中部ネットテック株式会社
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
大竹 章裕	株式会社ラック
中島 浩光	サブスクライバ（株式会社マインド・トゥー・アクション）
佐藤 公理	サブスクライバ
後藤 厚宏	情報セキュリティ大学院大学（教授）

会

２．2018年度の活動内容サマリ

2018年度の活動内容サマリ

2018年度活動状況

【成果物】
・公開成果物はなし

【テーマ】
1) IoTにおけるチャットボットの認証と認可等＝＞完了
2) アイデンティティとIoT（IDoT）＝＞継続実施
3) 認証要素、認可要素、その関係の整理＝＞継続実施
4) アイデンティティLT大会（初心者向け）＝＞完了。継続実施
5) ID管理チェックリストのCCMへの逆マッピング＝＞次年度継続
6) 「クラウド環境におけるアイデンティティ管理」６章の検証＝＞完了

1),6) について、次ページより報告します。

３．成果紹介

・IoTにおけるチャットボットの認証と認可等
・「クラウド環境におけるアイデンティティ管理」６章の検証

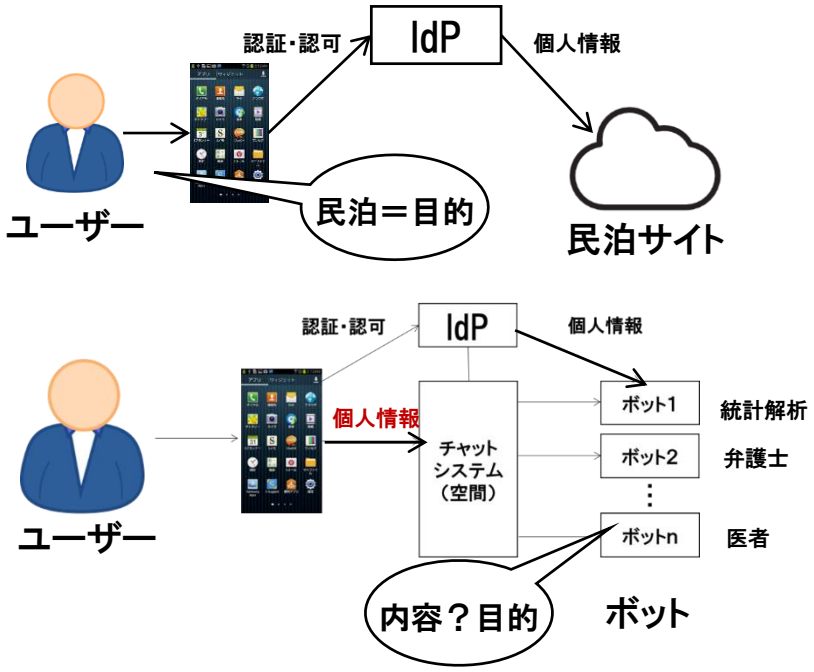
【IoTにおけるチャットボットの認証と認可等】課題提起(2017年度)

なぜチャットボットの認証認可が課題なのか？

- 従来の認証認可の仕組みはユーザーが**能動的**に個人情報を提供するモデル（例：民泊したいので個人情報を提供）
- チャットボットは目的利用（統計解析、弁護士、医療等）ではあっても個人データはユーザーが垂れ流す中で、ボットがデータを**受動的**に得る

  （チャット空間での内容（個人情報）を

  “まずボットが見て”サービスを判断）



利用前：同意は初回のみ

利用後：あらゆるデータ{テキスト、音声、画像} が流れる可能性

（後で削除は困難？）

→「現状技術でうまく同意を取る方法」がない？

チャットボットでの情報コントロールは従来モデルでは難しい？

【IoTにおけるチャットボットの認証と認可等】結論（2018年度）

- チャットチャネルとボットID等の扱いの調査
  - 「Slack、Line」等のチャットボットのID等の扱いに関する調査

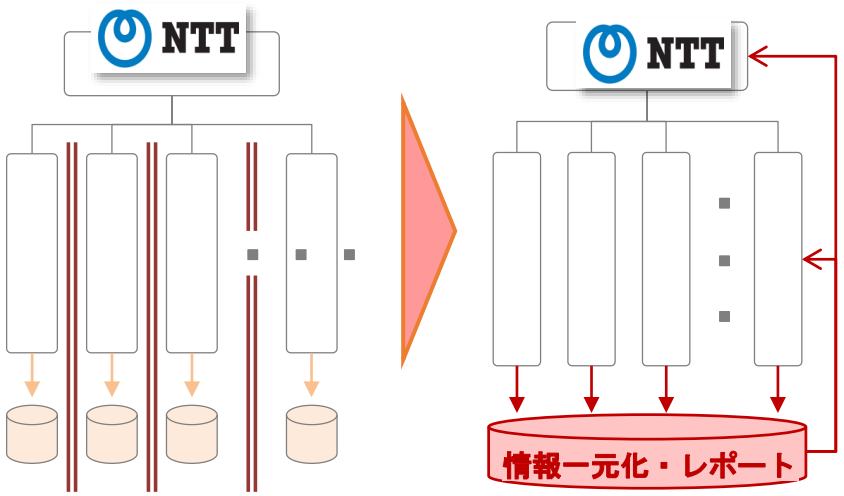
①Line株式会社のセキュリティ専門家を招いての勉強会
②Slackメンバーによるチャット空間でのワークスペース、共有チャネル、ボットの｛作成、召集、参加｝に関する考察とボットの利用約款の調査

チャットボットのセキュリティ／プライバシー保護は約款をベースに慎重に対応がなされている（利用者は仕組みを理解した上で利用すべき）

【６章の検証】
適用対象プロジェクトについて

２０１４年秋
経営幹部より中期経営計画推進メッセージ発信
- グローバルビジネスでの売上げ拡大
- グループシナジー発揮
- コスト最適化

「ITドリブンで経営情報の見える化」

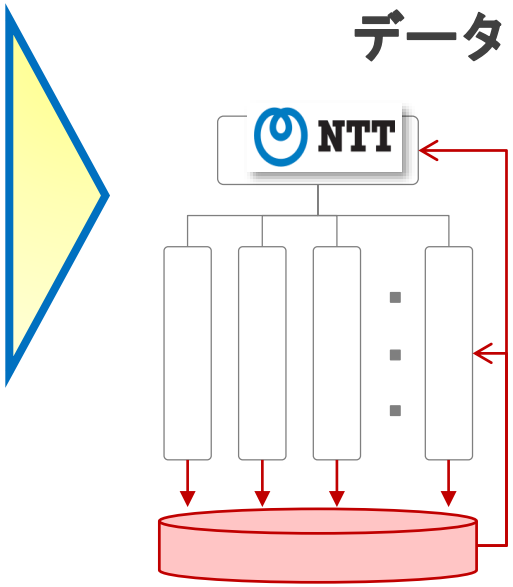


ID管理の仕組みも構築

Finance	Sales	Human Resource	Procurement
ｻｰﾋﾞｽ別収支	海外協業案件	人員数	調達量・ﾍﾞﾝﾁﾏｰｸ

２０１８年冬
中期経営戦略「Your Value Partner 2025」
◎　デジタルトランスフォーメーション
（ICTにより様々なデータを集積･利活用することで、新たな仕組みを創出／既存の仕組みを変革 ）

「データドリブン経営・
データ民主化の推進」

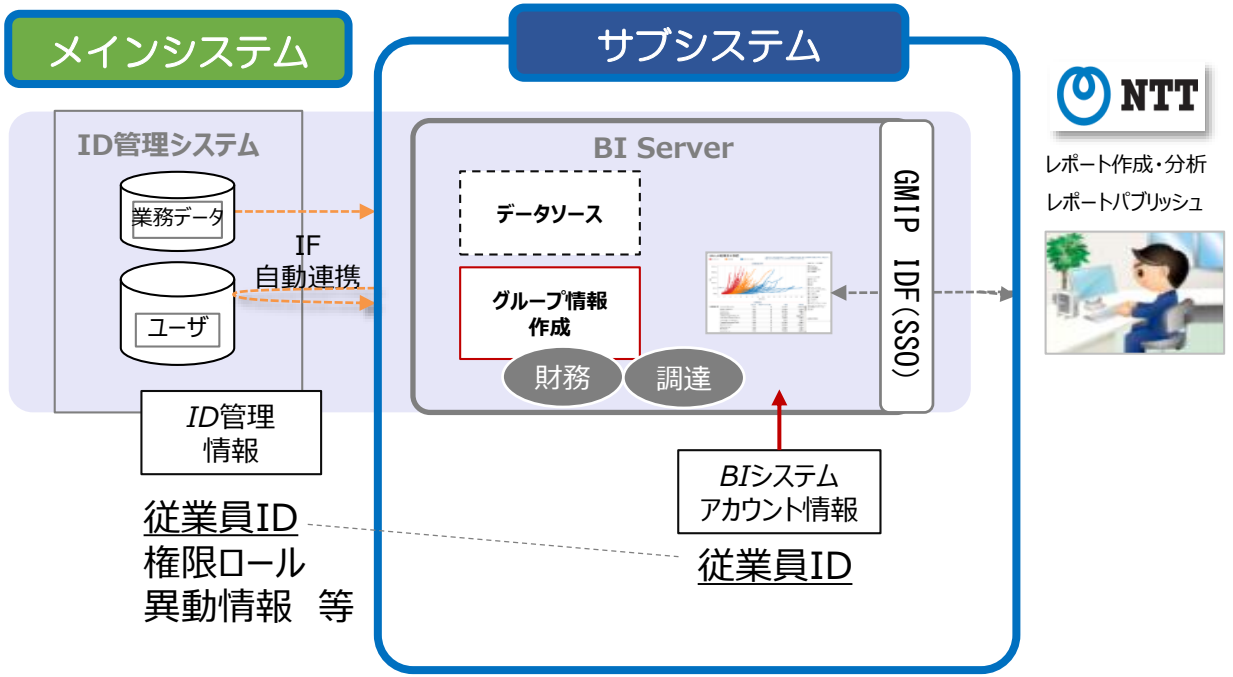


＋

セルフBI導入

【６章の検証】
対象プロジェクトについて

今回構築したサブシステムは、BIServer（分析したデータを適切な社員が参照することを可能にするもの）にて社員のライフサイクルに対応して、権限グループ情報を作成し、運用していくものである。
※社員の情報はメインシステムから自動継承



サブシステム目線からのID管理システム活用について検討
（サブシステム用のガイドラインが欲しい！）

【６章の検証】
議論スコープ

【目的・前提】今回のプロジェクトにおいては、ID管理システムのサブシステムとしての位置付けであり、導入方針の直接の適用とはいえないが、サブシステムから見て、メインシステムのユーザ情報を流通し、それを取扱う際の留意点の拠り所として適用する。

6章：ID管理システム導入方針

	適用内容	
	区分	内容
6.1	ID管理導入の流れ	各工程の概要
6.2	企画フェーズ	目標の明確化 現状分析 計画案作成 ID体系 運用体制/役割
6.3	要件定義フェーズ	IDサービス定義 プロビジョニング定義 リポジトリ定義 移行
6.4	設計フェーズ	IDサービス設計 プロビジョニング設計 リポジトリ設計 移行

	適用内容	
	区分	内容
6.5	実装・テスト フェーズ	IDサービス実装・テスト プロビジョニング実装・テスト リポジトリ実装・テスト 移行
6.6	サービスイン	サービスイン
6.7	教育 トレーニング	教育・トレーニング
6.8	評価	評価

今回はID管理システムとの連携可否を判断することになる企画フェーズに着目

【６章の検証】
そもそも・・・何を求めているのか

○サブシステムから見てID管理システムに何を求めるのか。
⇒「企画フェーズでID管理システムを適用する際、どう進めるのか。
また、ある程度のフィージビリティ、見極めを行うために何をすれば良いのか。」

実際に本開発で気になった点	ガイドライン
そもそものサブシステム検討に当たってのID管理周りの課題を抽出	目標の明確化
ID管理システム側がサブシステム側での要求に叶う情報を持っているか	現状分析
ID管理システム側のアドバンテージを吸収し、どのような対策が打てるか。	計画案作成
ID管理システム側が保持するID体系は、どのようなものか。	ID体系　※
運用面で、ID管理システム担当との役割分担はどう握ればよいか。	運用体制/役割

※ID体系については、サブシステム側で既定された情報を取得するのみであるため、対象外とした。

【６章の検証】
目標の明確化

【目的】※導入方針より
- ID管理システムがビジネス上メリットを創出するものか。業務課題が解決されるか。
- 導入に際して、大きな障壁となるであろう問題点を明確にする。
- 業務が抱える課題を洗い出すこと ＝ ID管理システムの目的を洗い出すこと

【サブシステムからの提言】

■ 業務課題の洗い出しについて、ある程度のパターンを記載できるのでは。
（コスト、仕様、心情における区分は、整理し易いので、そのまま活用。）

区分	課題
コストに関する要望	ID管理機能の実装にコストが掛かる
	ID管理の維持運用にコストが掛かる
	再度キーマンと調整して、仕様化するのに手間が掛かる
	…
仕様に関する要望	人事異動時の対応が複雑
	手運用が入り、メイン/サブシステムの情報に乖離が生じる
	影響調査範囲を局所化したい
	…
心情に関する要望	重複したID/パスワード管理が無駄
	システムアクセスの動線が煩雑
	IDに関わる問合せがバラバラ
	…

こう書くと当たり前のように見えるが、意外に暗黙知化されており、企画毎に練り直していることが多い。

【６章の検証】
現状分析

【目的】※導入方針より
- 前プロセスをベースに、優先度の高い改善項目に関する現状分析を行う。
- 現状問題と指摘されていない業務プロセスも洗い出す。
- OS／バージョン／方式などもリストアップ。（仕様設計等に影響）

【サブシステムからの提言】 ※6.3 要件定義-プロビジョニング記載の内容を本フェーズで把握する

■ID管理システムに提示してもらいたい情報の整理をしたい。

【業務プロセス】

①設定したい権限の基となる項目を保持しているか。

-ライフサイクル（採用、退職、出向、転籍、社内異動、休職、本務/兼務）等

-職位、雇用区分（役員、部長、課長、メンバ、派遣、アルバイト　等）

-その他属性（国、地域、会社、所属　等）

②権限用途以外で管理したい項目を保持しているか

-メールアドレス、氏名、電話番号　等

③粒度はどのような状態か

-特に本務/兼務の場合、1社員に対して2レコード保持している等、1:Nの関係が有るか

【環境面の棚卸し（ソフト/ハード/ネットワーク）】

①ソフト

-インタフェースを提供する仕組み（DB直接、FTP-PUT、API提供 等）、ジョブスケジュール

-認証基盤の有無（シングルサインオン）

②ハード

-オンプレミスorクラウド、システム連携することでの性能面の考慮、バックアップの形態

③ネットワーク

-ネットワーク構成図（そもそもアクセスできるセグメントなのか）

【６章の検証】
計画案作成

【目的】※導入方針より
- 将来像（ToBeモデル）の定義、将来像に向けた導入アプローチ（ロードマップ）
- 課題の原因分析を行い、対策検討を行う。
- 優先順位とコストをふまえ、システム化のロードマップを策定する。

【サブシステムからの提言】

■ 進め方は、そのまま適用できる。ただ、課題と同様、対策もパターン化可能と思われる。

課題

区分	課題
コストに関する要望	ID管理機能の実装にコストが掛かる
	ID管理の維持運用にコストが掛かる
	再度キーマンと調整して、仕様化するのに手間が掛かる
	…
仕様に関する要望	人事異動時の対応が複雑
	手運用が入り、メイン/サブシステムの情報に乖離が生じる
	影響調査範囲を局所化したい
	…
心情に関する要望	重複したID/パスワード管理が無駄
	システムアクセスの動線が煩雑
	IDに関わる問合せがバラバラ
	…

対策

ID管理のロール/権限情報の再利用

SSOの実装

ID運用の重複排除

ID管理機能を利用できるのか、サブシステム側で自前でID管理機能を置くのか、最終的な判断を本フェーズで実施

■ 優先順位の考え方については、下記の詳細化が必要か。

①**法令や社内規定**：特に個人情報保護観点の法律（**GDPR**（EU一般データ保護規則）等）
⇒但し、メインシステム側で整理しているケースが多いため、そのルールに準拠するだけでよいかもしれない。

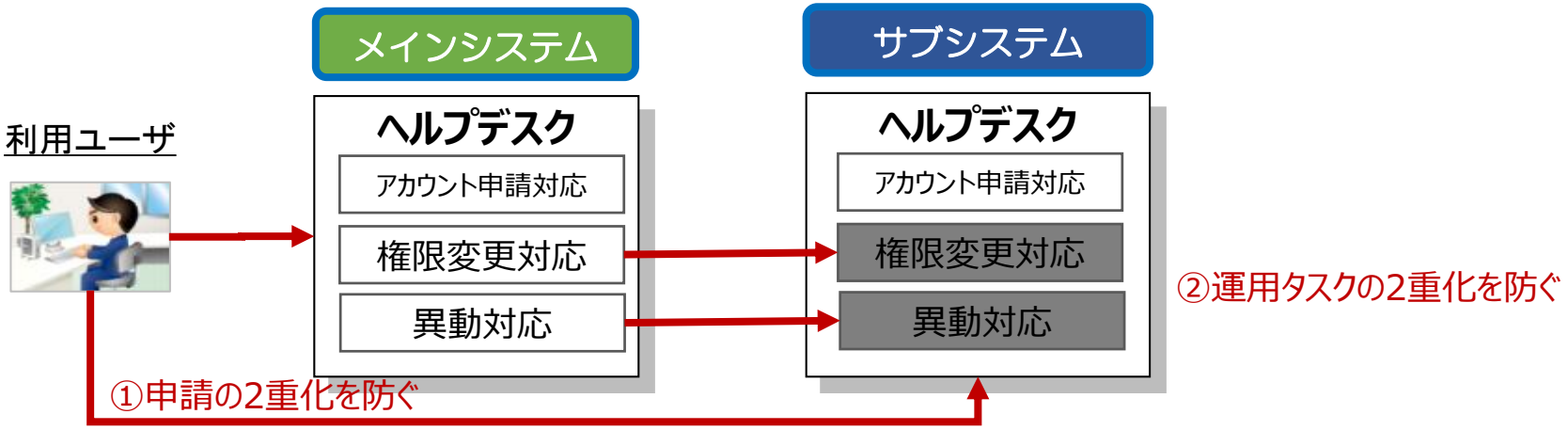
②**難易度**：あまり謳われていないステークホルダマネジメントのテーマがあると良い。
⇒サブシステムから見ると、メインシステム側の情報をそもそも利用してよいかからの調整になるので、それなりの壁がある。利用規約のようなものをID管理システム側から入手できると良い。

【６章の検証】
運用体制/役割

【目的】 ※導入方針より
- 運用を可視化（運用対象範囲となる人／サーバ／システムを洗い出し概要まとめ）
- 運用組織とID管理業務検討（担当毎のID運用の役割と管理業務内容を検討）
- ID管理業務内容の決定（通常運用と棚卸しなどの定期運用を決定）

【サブシステムからの提言】

■ 進め方は、そのまま適用できる。ただ、陥り易い点として下記要素がある。



陥り易い点

これらに陥らないよう「2-2 現状分析」で吸収する

①非正規社員等、ID管理システムで管理していない社員を対象とする場合の対応
(メインシステム側のカバレッジなのか、サブシステム側での個別対応とするのか)
②サブシステム側でID管理システムでの枠を超えた権限変更対応を求められ、手運用が発生。
メインシステムとの情報に乖離が生じ、個別対応が必要となる。

【６章の検証】
所感、総括

■サブシステム目線でガイドラインを活用させていただいたが、
押さえるべき要素として、**十分に適用可能**。
当たり前のようにID管理システムがあるから、何も考えず、利用しようという判断になりがちだが、**体系立ててリスクを意識し、検討するための指針として今後も活用したい。**

■もし、**サブシステム目線での観点**（**チェックリストやテンプレート**もあれば助かります。）が追加されれば、そのまま対向システム側とのコミュニケーションツールとして利用することで、**MECEやリスク抑止、調整稼動削減**といった観点で助かる人は多くいるのでは。

４．2019年度の活動テーマ

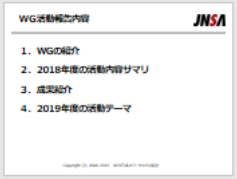
2019年度活動テーマ

【テーマ】

- チェックリストCCM逆マッピング（継続）
- 初心者教育ネタ整理（新規）
- 特権IDの監査（RPAなどのID含む)（新規）
- 認証要素、認可要素、その関係の整理（継続）
- クレデンシャル情報の歴史（新規）
- アイデンティティとIoT（IDoT）（継続）
- LT大会（継続）

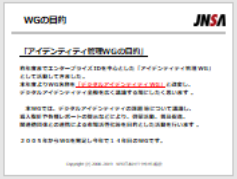
スライドー覧（まとめ）

1

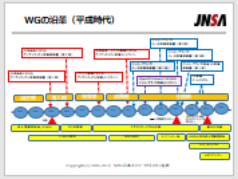


2

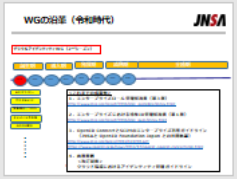
3



4



5



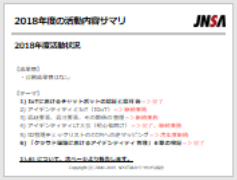
6

7

8

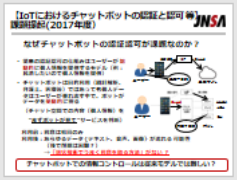
9

10

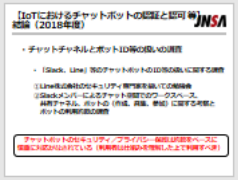


11

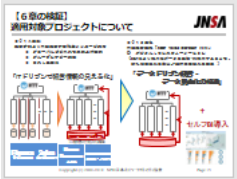
12



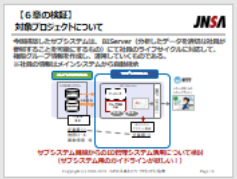
13



14

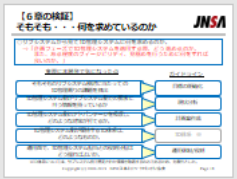


15

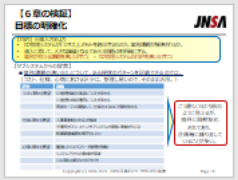


16

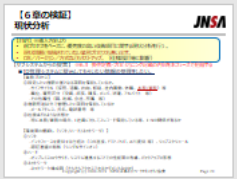
17



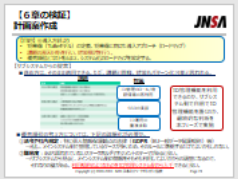
18



19

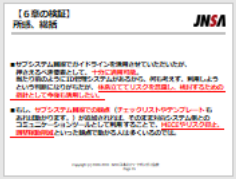


20



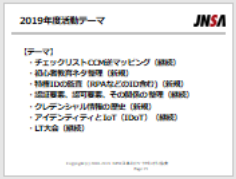
21

22



23

24



25

26

27


JNSA