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

JNSA 2016年度活動報告会

「２０１６年度 アイデンティティ管理WG 成果報告」

日本電気株式会社（NEC)
金融システム開発本部
金融デジタルイノベーション技術開発室
宮川　晃一

2017 年　6月　12日（月）

ＷＧ活動報告内容

１．WGの紹介

２．2016年度の活動内容サマリ

３．ID管理チェックリスト

４．今年度の活動テーマ

Copyright (c) 2000-2017　NPO日本ネットワークセキュリティ協会

１．WGのご紹介

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

WGの目的

JNSA

「アイデンティティ管理ＷＧの目的」

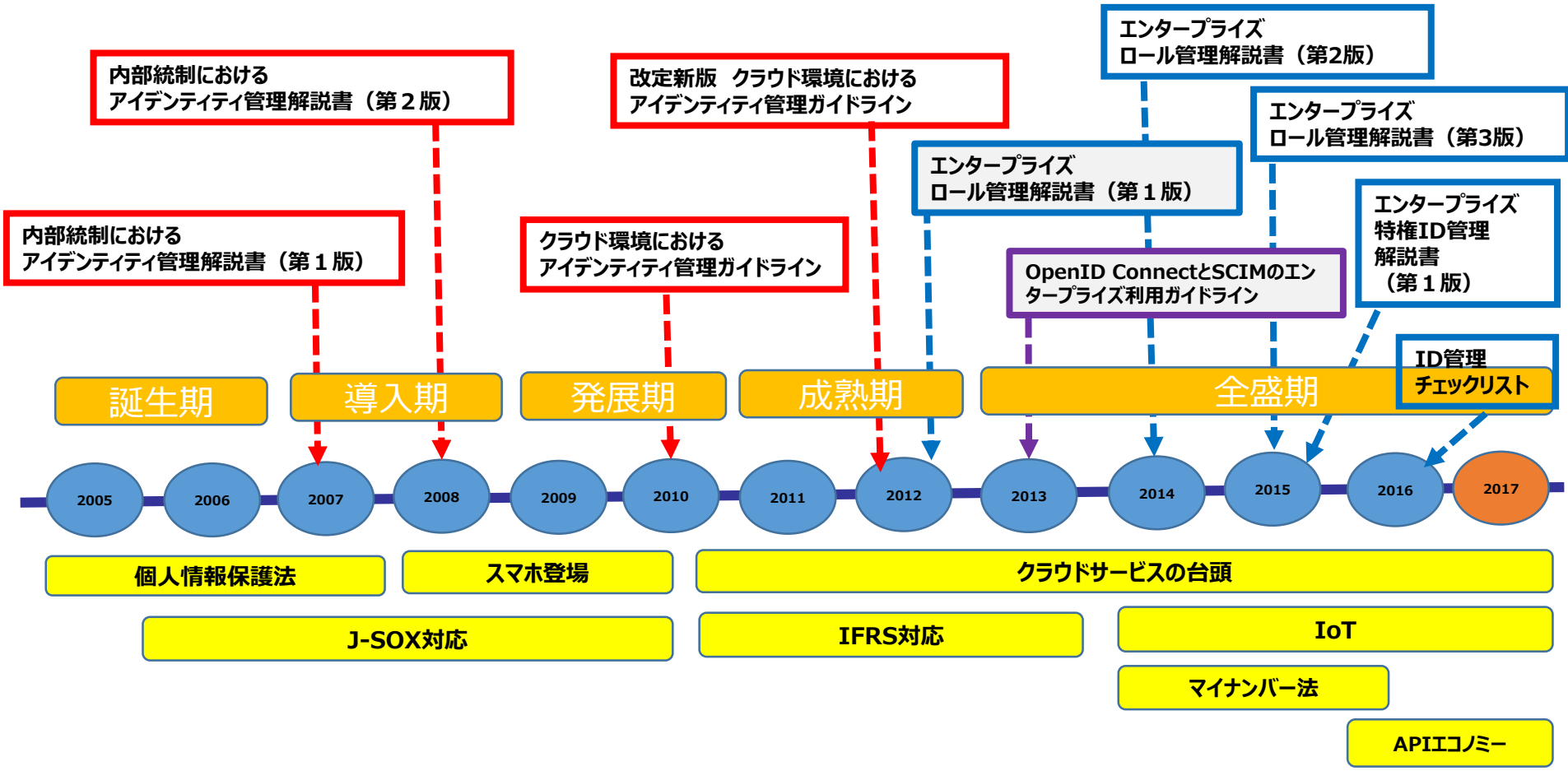
ＩＤ管理（アイデンティティマネージメント）分野は、セキュリティポリシーを実装する上での共通基盤として非常に注目されている分野です。

また、最近のクラウド環境利用においても益々重要な要素になっています。本WGでは、アイデンティティ管理における、様々な課題をＷＧ討議の中で検討し、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を目的に活動しています。

２００５年からWGを発足し今年で１２年目のWGです。

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

WGの沿革



Copyright (c) 2000-2017　NPO日本ネットワークセキュリティ協会

公開中の成果物

JNSA

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

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

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

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

WGメンバー紹介HP

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

Copyright (c) 2000-2017 NPO日本ネットワークセキュリティ協会

WGメンバー紹介

No.	氏名	所属
1	宮川 晃一	日本電気株式会社
2	貞弘 崇行	株式会社アイビーキューブ
3	八束 啓文	EMCジャパン株式会社
4	齊藤 亘	EMCジャパン株式会社
5	篠原 信之	イオンアイビス株式会社
6	富士榮 尚寛	伊藤忠テクノソリューションズ株式会社
7	稲吉 英宗	伊藤忠テクノソリューションズ株式会社
8	新嘉喜 康治	伊藤忠テクノソリューションズ株式会社
9	木村 慎吾	インテック
10	深澤 聡	SCSK株式会社
11	戸谷 祐一	NTTコミュニケーションズ株式会社　システム部
12	山田 達司	NTTデータ株式会社
13	星野 亮	NTTデータ株式会社
14	杉村 耕司	NTTデータ先端技術株式会社
15	深谷 貴宣	KPMGコンサルティング
16	齊藤 光司	KPMGコンサルティング
17	伊藤 栄二	株式会社ディアイティ
18	澤井真二	デロイトトーマツリスクサービス株式会社
19	栃沢 直樹	トレンドマイクロ株式会社
20	板倉 景子	日本IBM株式会社
21	竹内和弘	日本IBM株式会社
22	酒井美香	日本IBMシステムズ・エンジニアリング株式会社
23	市川 貴浩	日本IBMシステムズ・エンジニアリング株式会社
24	飯塚 昭	日本オラクル株式会社
25	木村　偉一	日本セーフネット株式会社
26	桑田 雅彦	日本電気株式会社
27	駒沢 健	日本電信電話株式会社
28	見上 昌成	日本ビジネスシステムズ株式会社
29	安納 順一	日本マイクロソフト株式会社
30	村田 裕昭	日本マイクロソフト株式会社
31	小野寺 匠	日本マイクロソフト株式会社
32	福田 尚弘	パナソニック
33	今堀 秀史	富士通関西中部ネットテック株式会社
34	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
35	佐藤 公理	マカフィー株式会社
36	大竹 章裕	ラック
37	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）
38	後藤 厚宏	情報セキュリティ大学院大学（教授）

計38名（会社名五十音順）

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

２．2016年度の活動内容サマリ

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

2016年度活動内容サマリ

2016年度は以下のテーマで議論・勉強をいたしました。

1. ID管理チェックリスト　=>本日の発表

2. ID管理最新技術およびSLOブロックチェーン勉強会
3. アイデンティティとプライバシー（未実施）
4. IDの融合と分離（まとめ作業）
5. IoTにおけるアイデンティティ管理
6. EU規則勉強会
7. ID&IT 2015 協力（若手勉強会）

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

３．ID管理チェックリスト

作成担当：伊藤忠テクノソリューションズ株式会社
富士榮　尚寛氏　ほか

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

チェックリストの必要性

JNSA

ID管理のシステム化企画の段階における課題

1. どのようにシステム化の検討を進めればよいのか
2. どこまで厳密に管理・制御をすればよいのか

の共通解・基準がない。

⇒企業とベンダ間に**乖離**が発生、**プロジェクト頓挫**

ID管理における定量的な基準となる、
評価軸と**評価基準**の策定が必要

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

チェックリストの目的と目標

特に上流工程において、企業とベンダ間の
認識の乖離によるプロジェクト頓挫を防止すること
を目的とし、企業の現状分析を客観的に行うための
評価軸および評価基準を作成すること
を目標とする。

表1. 上流工程において企業とベンダそれぞれが抱える課題＝認識の乖離の主な原因は現状分析（赤字）

フェーズ	導入対象となる企業・組織の目線	ITベンダ・コンサルタントの目線
企画フェーズ	● 進め方がわからない ● **自組織の現状がわからない** ● **あるべき姿がわからない** ● 必要な予算がわからない、ベンダの見積もりが高額（費用対効果が謳いづらい） ● 企画の通し方がわからない（ステークホルダが多く、面倒）	● 導入対象の企業・組織が何を求めているのかわからない ● **現状がわからない** ● わからないのに総額コストの提示を要求される
要件定義フェーズ	● **自社にあったあるべき姿がわからない** ● ITベンダ・コンサルタントの提示するソリューション・システム化計画の妥当性がわからない	● 過剰と思える機能要求があった時、一般的に妥当な達成水準が示せず、カスタマイズが増え、コスト増となる

スコープと進め方

JNSA

評価軸の策定

ガイドライン*1、CCM*2をベースに

１．全般（法令、管理ポリシー/ルール）

２．データ源泉（対象、保証レベル、整理状況）

３．対象システム（概要、ID関連機能）

のカテゴリで評価項目の洗い出し

評価基準の策定

洗い出した評価項目のスコアリング基準の策定

基準値の算出（業界毎？）⇒FY17以降に検討

*1 当WG成果物、「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」

*2 クラウドセキュリティアライアンス「Cloud Control Matrix」（CCM)

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

評価方法

何が出来ているかではなく、
どこまで把握できているか？を評価

- 4段階評価
  - １：ほぼ把握できていない
  - ２：少ししか把握できていない
  - ３：ある程度は把握できている
  - ４：おおよそ把握できている
- 各サブカテゴリ単位で平均を出す
  - 対象システムはシステム毎に評価する

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

利用にあたっての注意事項

- インフラや運用など非機能面は含まない
  （あくまでID管理に関する現状把握の度合を評価する）

- チェックリストに無い項目は評価不要ではなく、ケースバイケース（業界や業種にも依存）で判断し、項目のカスタマイズを推奨

- 評価項目によっては担当では答えられないものがあるはずなので適宜担当者のアサインをすることを推奨

- 基準が決まっているか？の基準の中身の例は参考資料
  （ガイドラインのテンプレート４，５）を参照

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

評価の実施（Excelシート）

JNSA

チェックリスト_vol.0.9 - Excel　富士榮尚寛

ファイル　ホーム　挿入　ページレイアウト　数式　データ　校閲　表示　アドイン　ロードテスト　チーム　操作アシスト　共有

A6　項番

	A	B	C	D	E
6	項番	カテゴリ	サブカテゴリ	観点	チェック項目
7	1-1	1.法令管理・ポリシー	法令関係	個人情報保護	個人情報を収集し・管理する目的、活用の範囲を明確に定義しているか
8	1-2			業界固有関連法規類	ID管理システムの運用に必要な法規が把握できているか？ （例：PCI DSSなど）
9	1-3		管理ポリシー/ルール	認証	SSOシステム、及び各アプリケーション認証方式は組織内で標準化されているか
10	1-4				組織内で統一されたパスワードポリシーを適用しているか 例） 最小の長さ、複雑さ、履歴、有効期限、ロックアウト、初回利用時の強制変更
11	1-5			ID管理	IDライフサイクルの定義は組織内で標準化されているか
12	1-6			ロール/アクセス権管理	ユーザーにアクセス権を付与・剥奪する際の基準及びプロセスを定めたポリシーを定義 いるか
13	17				ユーザーが担う職務機能に基づく最小権限原則に従ったアクセス権を保持していること 定期的に再評価する際の基準及びプロセスを定めたポリシーを定義しているか
14	2-1	2.IDデータ	管理対象		IdM・SSOシステムの管理・利用対象とするIDの範囲は定義されているか 例） 人（プロパ・パートナー・BtoB・BtoC）、人以外、システム管理者
15	2-2		保証レベル	正社員	正社員のID登録を行う際の身元保証の実施状況を把握しているか
16	2-3			非社員（派遣など）	非社員のID登録を行う際の身元保証の実施状況を把握しているか
17	2-4			社外利用者	社外利用者のID登録を行う際の身元保証の実施状況を把握しているか

評価結果グラフ (記入サンプル)　チェックリスト (記入サンプル) (2)

準備完了　100%

（ご参考）テンプレート４

【テンプレート4】ID管理・認証基盤ヒアリング項目一覧

No.	カテゴリ	ヒアリング事項	ご回答	ヒアリング目的
1	システム	システムの概要について教えてください。 （システムの役割・提供機能など）		システムの概要を把握するため。
2	システム	システムの総利用者数を教えてください。	名	IdM/SSOの際のサイジングに必要な情報 IdM/SSOの際のライセンス費用算出に必要な情報
3	システム	システムを利用しているユーザーの種別および人数を教えてください。		ユーザの種別を把握し、それぞれの運用を意識するために必要。
4	システム	システムの種別について教えてください。	□ パッケージ製品（製品名：　　） □ 開発システム ---------- □ Webシステム □ クラサバシステム □ その他（　　）	SSOの方式を決めるために必要。 IdM連携を行う際に、連携できるかどうかを確認するために必要。
5	システム	システムが動作しているサーバのOSは何ですか？ （バージョンの記載もお願いします）	□ Windows Server（　　） □ Solaris（　　） □ Linux（　　） □ その他（　　）	OSのID連携を行う際に必要。 SSOのエージェントを導入する場合に、サポートOSかどうか確認するために必要。
6	システム	システムが動作しているサーバの台数と設置場所について教えてください。	合計　　台 場所（　　）	IdM/SSOの際のサイジングに必要な情報 IdM/SSOの際のライセンス費用算出に必要な情報 →台数が複数台の場合、冗長化実現の方法について確認し、IdM連携/SSO実現性を検討する。
7	認証	利用者IDの認証の方式を教えてください。	□ ID/PWによる認証 □Basic認証 □Form認証 □その他（　　） □ PKIによる認証 □ バイオ認証（指紋・静脈など） □ その他（　　）	SSOの方式/認証の方式を決めるために必要。
8	認証	利用者IDの認証情報が格納されている場所（リポジトリ）を教えてください。	□ Active Directory（バージョン：　　） □ LDAP（製品名：　　） □ RDB（製品名：　　） □ 独自DB □ 他システム（システム名：　　）	IdM連携を行う際に、連携できるかどうかを確認するために必要。
9	認証	認証を行う際のプロトコルを教えてください。	□ ADSI（Active Directory　バージョン：　　） □ LDAP（バージョン：　　） □ その他（　　）	SSOの方式/認証の方式を決めるために必要。
10	認証	IDや属性情報の外部参照はしていますか？	□ していない □ している（　　）	IdM連携を行う際に、どのような情報を連携すればよいか決めるために必要。
11	認証	二重ログインは禁止していますか？	□ 禁止していない □ 禁止している	SSOの方式/認証の方式を決めるために必要。 セキュリティレベルの確認。
12	ID管理	IDをどのように生成していますか？	□ 別システム（　　）にて認証のためID生成はしていない □ 申請ベースで管理者が登録 □ 申請ベースで顧客管理者が登録 □ その他（　　）	IdMの運用改善検討/IdMシステム検討の」ために必要。 （申請の記録がとられていないから、ワークフローがあったほうがよい、など）

（ご参考）テンプレート５

【テンプレート5】要件定義の観点一覧

要件定義の観点	定義する内容の例や補足
4.3.1. ID管理サービスの要件定義	
①IDライフサイクルの要件定義	
□情報システムユーザ個人のIDが生成されてから削除されるまでの間に、どのようなイベントやタイミングで、IDの状態がどのように遷移するのかに関する要件を定義する。	○例えば企業の従業員の場合、入社してから退職するまでの間に、異動、昇格、休職、復職、出向、復帰などの人事イベントがあり、それに伴い当該従業員が利用を許可される業務システムも変わり、IDの状態も遷移する。退職後も、場合によっては権限を絞り込むだけでIDを無効化しないことや、過去のログから人を特定できるようにIDを削除せずに保存しておくことも必要な場合がある。 ○このようなIDの状態遷移が発生するイベントやタイミングを洗い出し、どのような状態遷移が発生するかを明確にする必要がある。 ○IDの状態遷移は、情報システムユーザの種別（例えば、企業の正社員、派遣、請負、パートタイム、販売店、取引先、システム運用・保守業者など）によって異なるので、ユーザ種別ごとに明確にする。
②ID情報マスタデータソースとの同期の要件定義	
□ID管理システムに登録するデータのマスタデータが別に管理されている場合、ID管理システムとマスタデータソースとの間のデータ同期に関する要件を定義する。	○ID管理システムに登録する各データについて、次に挙げる事項を明確にする必要がある。 ・マスタデータソース ・マスタデータとの同期タイミング ・マスタデータを受け取る際の形式やインタフェース ・マスタデータの精度と、データ手直しの必要性 ・一時に同期の対象となるマスタデータの量の想定 ○例えば企業の場合、正社員のID情報（基本項目）のマスタデータは人事システムで管理されている場合が多く、人事データの更新と同期を取ってID管理システムのデータを更新することになる。 ○一斉の人事異動時など、マスタデータソースと大量のデータ同期を一時に実行することが必要となる場合は、例えば人事異動日に先立って仮のデータ同期を実行しておいたり、夜間休日に複数のタイミングに分けてデータ同期を実行したりといった現実的な解を考慮し、要件を決める必要がある。
③ID管理ワークフローの要件定義	
□ID管理システムのデータを更新（登録・変更・削除）する際に必要となる、申請・承認のワークフローに関する要件を定義する。	○ワークフローの利用場面とデータ更新のパターンを洗い出し、各パターンについて、次に挙げる事項を明確にする必要がある。 ・ワークフローの利用場面は何か ・更新対象のデータは何か、どの範囲か ・申請者と承認者は誰か（多段承認の場合、各段階の承認者は誰か）

採点結果の評価例

1.全般 法令関係
1.全般 管理ポリシー/ルール
2.IDデータ 管理対象
2.IDデータ 保証レベル
2.IDデータ データ整理
3.対象システム（APL①） 概要
3.対象システム（APL①） 識別
3.対象システム（APL①） 認証
3.対象システム（APL①） ID管理
3.対象システム（APL①） ロール/ア…
3.対象システム（APL②） 概要
3.対象システム（APL②） 識別
3.対象システム（APL②） 認証
3.対象システム（APL②） ID管理
3.対象システム（APL②） ロール/ア…
3.対象システム（APL③） 概要
3.対象システム（APL③） 識別
3.対象システム（APL③） 認証
3.対象システム（APL③） ID管理
3.対象システム（APL③） ロール/ア…
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00

チェックリスト公開について

JNSAの成果物公開HPにて近日公開予定！

- チェックリスト（Excell形式を予定）
  （チェックリストのチェックサンプル付）
- チェックリストの使い方（説明資料）

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

４．本年度のテーマ

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

今年度のテーマ

【テーマ】
１．ＩｏＴにおけるチャットボットの認証と認可等の課題
２．アイデンティティとＩｏＴ(IDoT)
３．認証要素、認可要素、その関係の整理
４．EU規則最新情報
５．IDaaSの動向について
６．アイデンティティLT大会
７．独自セミナー開催（１月予定）

【その他】
ID&IT２０１７/JICS2017 協力
その他イベント協賛は随時

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

本年度メンバー募集

【第１回WG＆懇親会】
日時：6月23日（金）16:00～18:00
場所：日本ビジネスシステムズ株式会社
セミナールーム（虎の門ヒルズ１６Ｆ）
https://www.jbs.co.jp/aboutus/access

【参加条件】
・本WGの趣旨にご賛同頂き、積極的にご参加・発言頂ける方
・毎月の部会出席を５０％以上可能な方
・ID管理分野のご経験・知識・ノウハウ等をご提供頂ける方
・各種成果物の作成にご協力いただける方

【申込み＆お問い合わせ】
JNSA事務局（office@jnsa.org）まで、お問い合わせください。

〆切：6/16（金）まで

Copyright (c) 2000-2017　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

JNSA