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

JNSA 2017年度活動報告会

「2017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(FDIT)
宮川　晃一

2018年　6月　12日

WG活動報告内容

1．WGの紹介

2．2017年度の活動内容サマリ

3．IoTにおけるチャットボットの認証と認可等

4．認証要素、認可要素、その関係の整理

5．2018年度の活動テーマ

Copyright (c) 2000-2018　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) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

WGの目的

「アイデンティティ管理ＷＧの目的」

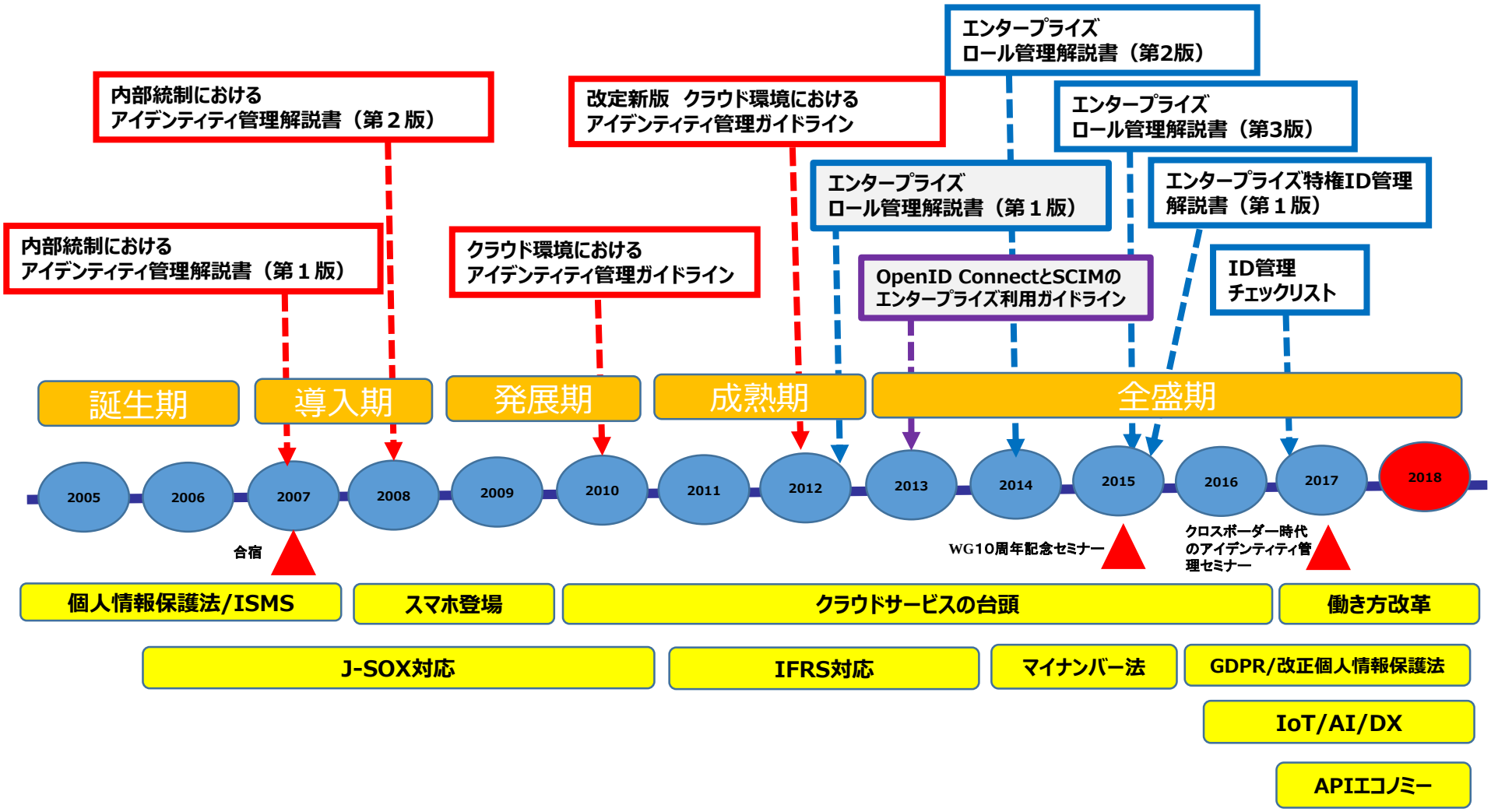
ＩＤ管理（アイデンティティマネージメント）分野は、セキュリティポリシーを実装する上での共通基盤として非常に注目されている分野です。

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１３年目のWGです。

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

WGの沿革



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

公開中の成果物

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

Copyright (c) 2000-2018　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) 2000-2018　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

JNSA 特定非営利活動法人 日本ネットワークセキュリティ協会 Japan Network Security Association

HOME ▶ お問い合わせ

部会・WGについて

公開資料・報告書をお探しの方 | 部会・WGについて | JNSAについて | イベント・セミナー情報 | 会員専用ページへ

HOME ＞ 部会・WGについて ＞ アイデンティティ管理WG

- 社会活動部会
- 調査研究部会
- 標準化部会 ▶
- 教育部会
- 会員交流部会
- マーケティング部会
- 西日本支部
- U40部会
- 産学情報セキュリティ人材育成検討会
- SECCON（セキュリティコンテスト）実行委員会
- ISOG-J
- ISEPA
- 活動カレンダー

アイデンティティ管理WG

活動メンバー（2017年7月31日現在）

■ リーダー

宮川 晃一（日本電気株式会社）»

■ メンバー（会社名順）

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）
富士榮 尚寛
（伊藤忠テクノソリューションズ株式会社）»
新嘉喜 康治
（伊藤忠テクノソリューションズ株式会社）»
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）
竹内 和弘（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）
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）

2018年度メンバー

計４９名　敬称略
会社名：五十音順

JNSA

標準化部会 アイデンティティ管理WG

出欠	会社名	氏名
1	日本電気株式会社	宮川 晃一
2	株式会社アイビーキューブ	貞弘 崇行
3	EMCジャパン株式会社	八束 啓文
4	EMCジャパン株式会社	齊藤亘
5	イオンアイビス株式会社	篠原 信之
6	伊藤忠テクノソリューションズ株式会社	富士榮 尚寛
7	伊藤忠テクノソリューションズ株式会社	稲吉 英宗
8	伊藤忠テクノソリューションズ株式会社	新嘉喜 康治
9	株式会社インテック	木村 慎吾
10	SCSK株式会社	深澤 聡
11	SCSK株式会社	金子 敬祐
12	NECソリューションイノベータ	内田 健一
13	NECソリューションイノベータ	岡崎　一洸
14	株式会社エヌ・ティ・ティ・データ	山田 達司
15	エヌ・ティ・ティ・データ先端技術株式会社	杉村 耕司
16	株式会社エヌ・ティ・ティ・データ	星野 亮
17	NTTテクノクロス株式会社	久米田　博
18	KPMGコンサルティング株式会社	深谷 貴宣
19	KPMGコンサルティング株式会社	齊藤 光司
20	株式会社Speee	森岡 周平
21	株式会社ディアイティ	伊藤 栄二
22	有限責任監査法人トーマツ	櫻田仁詩
23	有限責任監査法人トーマツ	大森潤
24	有限責任監査法人トーマツ	古友亮輔
25	有限責任監査法人トーマツ	大島和紘
26	トレンドマイクロ株式会社	栃沢 直樹
27	日本アイ・ビー・エム株式会社	板倉 景子
28	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	酒井美香
29	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	市川 貴浩
30	日本オラクル株式会社	飯塚 昭
31	日本セーフネット株式会社	木村　優一
32	株式会社 日本総合研究所	吉嶋 正和
33	日本電気株式会社	桑田 雅彦
34	日本電信電話株式会社	駒沢 健
35	日本ビジネスシステムズ株式会社	見上 昌成
36	日本ビジネスシステムズ株式会社	川田 拓
37	日本マイクロソフト株式会社	安納 順一
38	日本マイクロソフト株式会社	上杉康雄
39	日本マイクロソフト株式会社	小野寺 匠
40	ネットワンシステムズ株式会社	渥美 淳一
41	パナソニック株式会社	福田 尚弘
42	富士通株式会社	新井 雅
43	富士通関西中部ネットテック株式会社	今堀 秀史
44	富士通関西中部ネットテック株式会社	福原 幸一
45	株式会社富士通ソーシアルサイエンスラボラトリ	恵美 玲央奈
46	株式会社ラック	大竹 章裕
47	サブスクライバ（株式会社マインド・トゥー・アクション）	中島 浩光
48	サブスクライバ	佐藤 公理
49	情報セキュリティ大学院大学（教授：特別顧問）	後藤 厚宏

２．2017年度の活動内容サマリ

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

2017年度の活動内容サマリ

2017年度活動状況

【成果物】

・ID管理チェックリスト＝＞JNSA HP公開

【テーマ】

・IoTにおけるチャットボットの認証と認可等**＝＞継続実施（本日ご説明）**
・アイデンティティとIoT（IDoT）＝＞継続実施
・認証要素、認可要素、その関係の整理（貞弘さん）**＝＞継続実施（本日ご説明）**
・プライバシー勉強会（情報セキュリティ大学院大学の湯浅先生）＝＞独自セミナー
・アイデンティティLT大会（初心者向け）＝＞継続実施
・IDaaSの動向について＝＞要望が薄く実施せず
・GDPRの動向について（トーマツリスクサービス北野氏）＝＞独自セミナー
・セミナー企画（若手育成テーマ、プライバシー動向含む）＝＞独自セミナー

【その他】

・JASA・ISACA大阪講演＝＞チェックリスト解説
・JICS2017講演＝＞講師対応

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

３．IoTにおけるチャットボットの認証と認可等

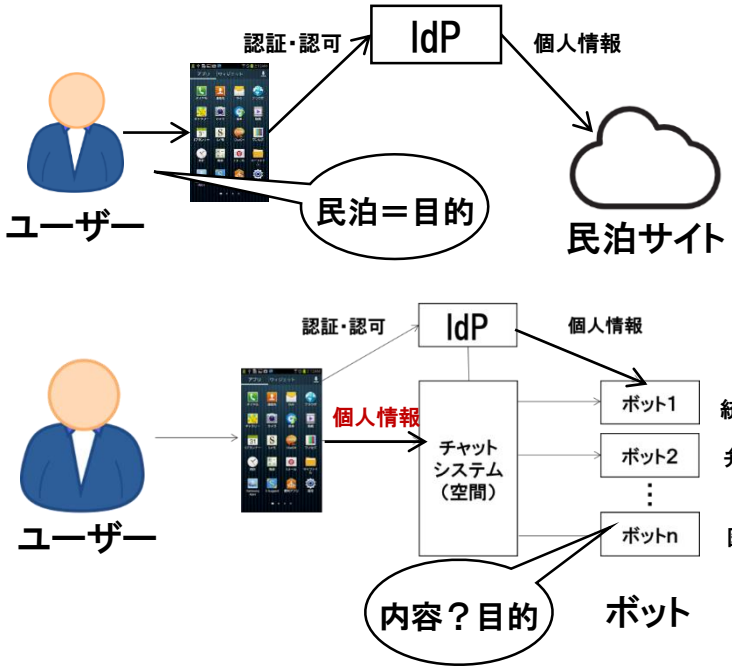
Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

課題提起

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）



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？

課題まとめ

チャットボットでの認証認可の課題まとめ

項目	課題
チャットチャネルでのプライバシー保護について	・認証認可でプライバシー情報転送は最初の接続時のみ ・チャットでは都度、様々なレベルの情報がボットへ転送 認証認可(OIDC／OAuth2)の仕組みで、今後もよいか？
チャットチャネルとボットのあり方	プライバシー保護の観点から、ボットとの接続はどうあるべきか？ 接続構成{1対1、1対n、n対n}？アクセス権{Read/Write}？
バックエンドでのボットの結託	ボットの結託(DB統合)では、 バックエンドで情報共有(結託)の可能性？

リアルタイム情報(チャット、音声、画像等)での
うまい認証認可の手段がない？

４．認証要素、認可要素とその関係の整理

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

背景とゴール

JNSA

【背景】

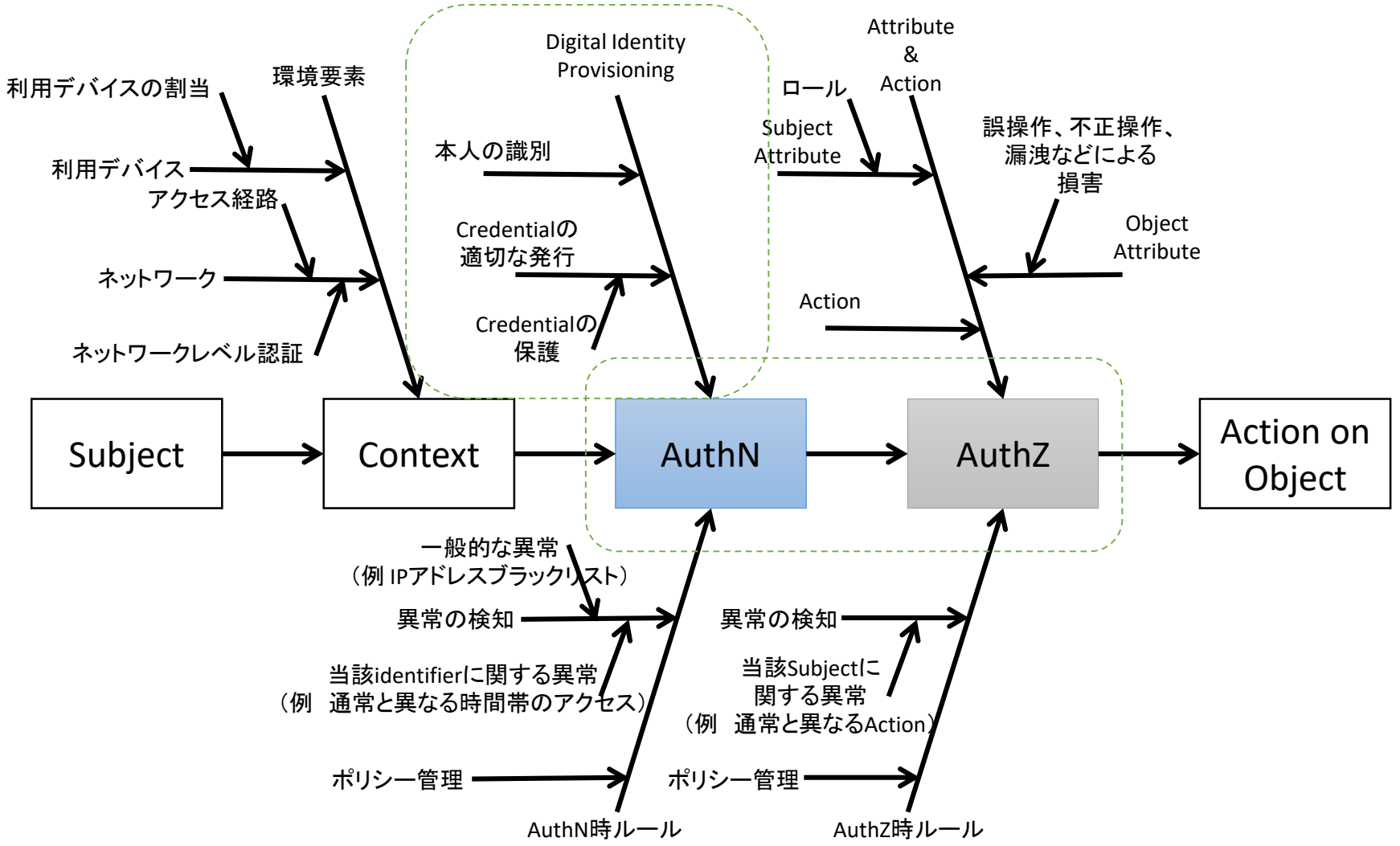
- アクセスコントロール系はいろいろとキーワード（リスクベース認証、トランザクション認証）や概念があって個々
  にどのようなモノかは分かるが、その関係がよく分からない

【ゴール】

- アクセスコントロールのモデルにおける、認証と認可の位置づけを確認
- アクセスコントロール系キーワード/概念のそのモデルにおける位置づけを確認
- 実際のユースケースを踏まえて、認証時に使う要素と認可時に使う要素の特徴と関係を明確化

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

一旦、時系列でまとめてみた



Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

課題・コメント

【課題･コメント】

- NIST 800-63-3 に沿った形での整理が必要
- Subjectは「人」に限定したほうがわかりやすい
- いくつかのユースケースで検討を進める
- トランザクション認証などは状態遷移を含めないと整理ができない
- AuthNとAuthZはもっと細かく考えたほうがよい

など

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

NIST SP800-63-3

JNSA

Digital Identity Guidelines: Now Available

https://pages.nist.gov/800-63-3/
https://www.jipdec.or.jp/sp/topics/event/20171013.html

June 22, 2017

The finalized four-volume SP 800-63 *Digital Identity Guidelines* document suite is now available, both in PDF format and online.

The Trusted Identities Group (TIG) thanks all that contributed to the development of these documents.

PDF versions of the documents are available from:

Document	Title	URL
SP 800-63-3	Digital Identity Guidelines	https://doi.org/10.6028/NIST.SP.800-63-3
SP 800-63A	Enrollment and Identity Proofing	https://doi.org/10.6028/NIST.SP.800-63a
SP 800-63B	Authentication and Lifecycle Management	https://doi.org/10.6028/NIST.SP.800-63b
SP 800-63C	Federation and Assertions	https://doi.org/10.6028/NIST.SP.800-63c

Links to the online version of the SP 800-63 suite are below.

デジタル認証のガイドライン

登録プロセス 身元保証

認証とライフサイクル管理

フェデレーションとアサーション

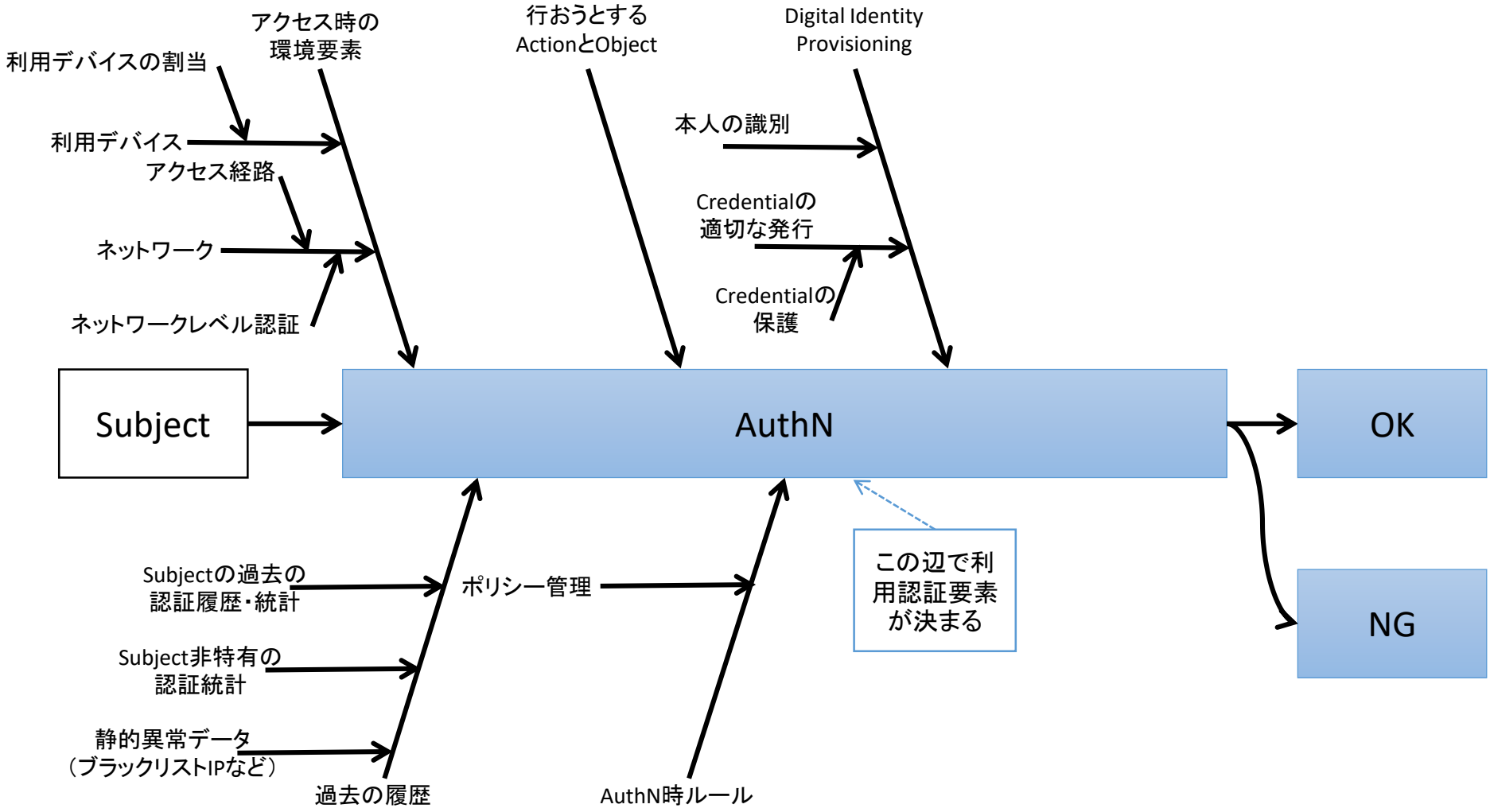
SP 800-63-3
Digital Identity Guidelines

SP 800-63A
Enrollment & Identity Proofing

SP 800-63B
Authentication & Lifecycle Management

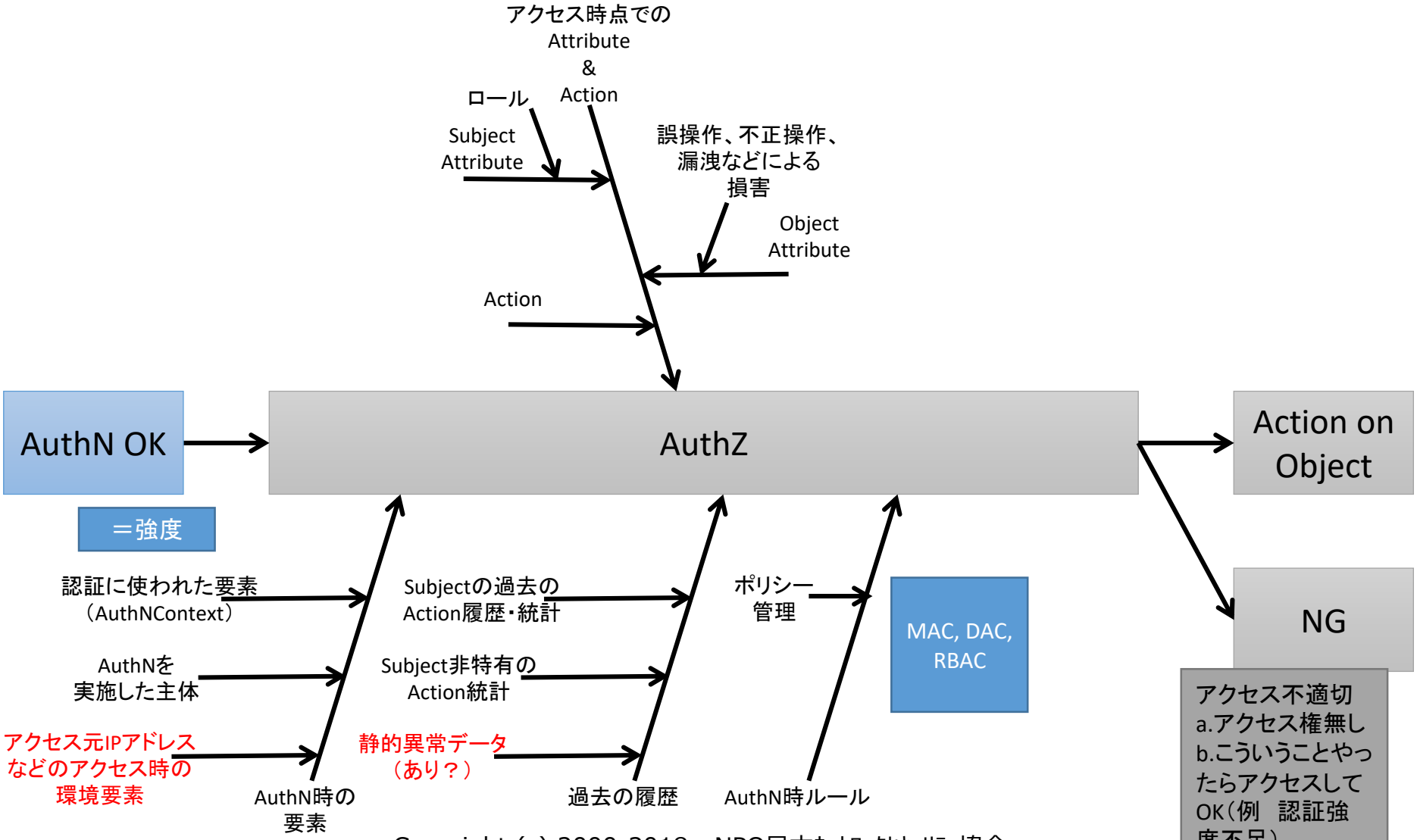
SP 800-63C
Federation & Assertions

再整理（１）：認証（AuthN）



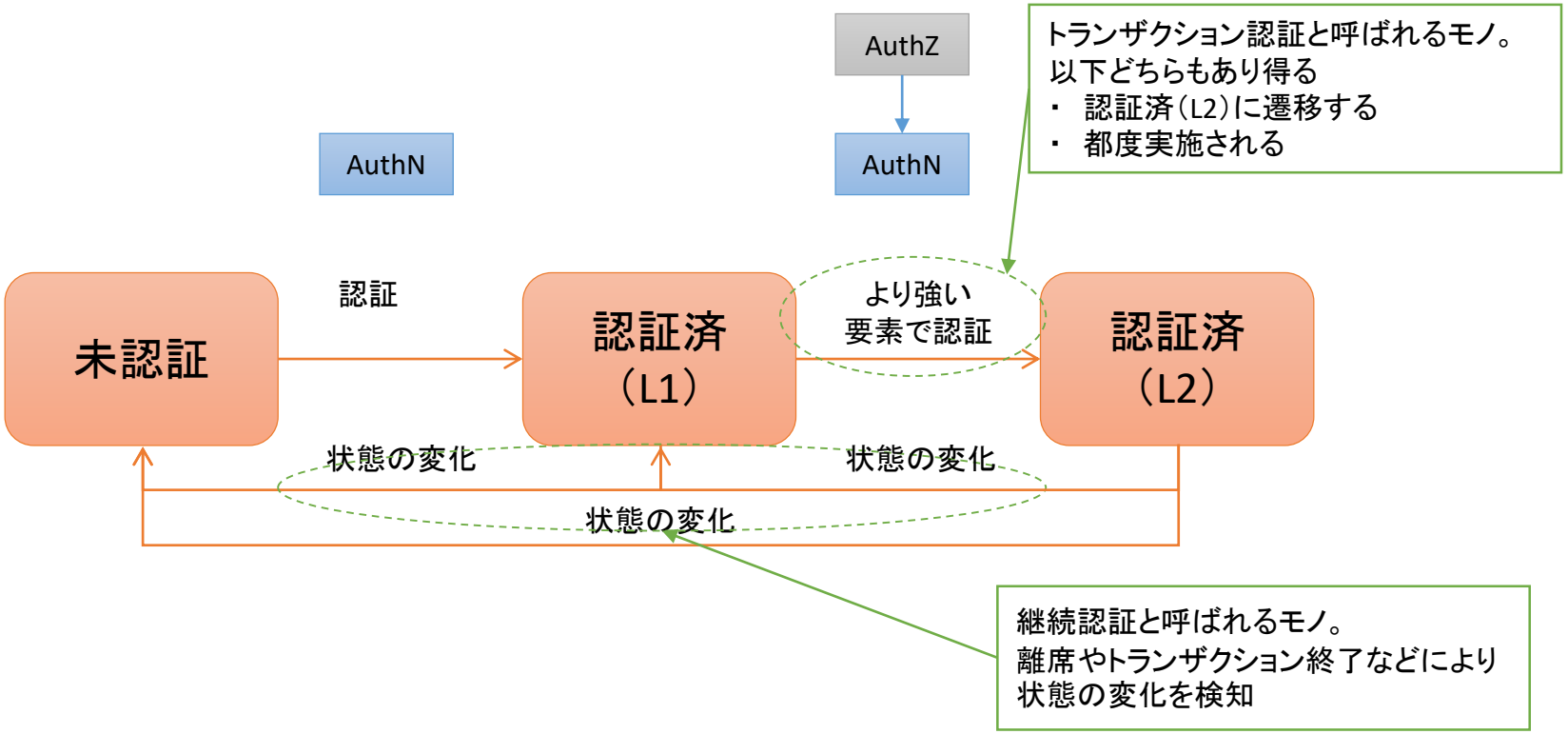
Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

再整理（２）：認可(AuthZ)



Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

トランザクション認証



認証の状態変化
→ 認証した瞬間だけでなくそれ以降の状態変化も考慮に入れる必要あり

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

方針転換

【元々の方針】

- アクセスコントロール系のキーワードや概念の定義をはっきりさせて、それを元に（汎用的なユースケースで使える）アクセスコントロールモデルを整理する

【転換後の方針】

- WGメンバの知見から特定のユースケースのアクセスコントロールモデルを描き、それにキーワードや概念をマッピングする

- 対象ユースケースは、人によるインターネットサービスへのWebブラウザーアクセスとする

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

今後の方針

【モチベーション】

- NIST 800-63における各種レベル（LoIA, LoA, etc.）への背景理解を助ける

【対象者】

- 認証、認可について、学び始めた人たち

【ゴール】

- アクセスコントロールのモデルにおける、認証と認可の位置づけを明確化
- 実際のユースケース（人によるWebサービス利用）を踏まえて、認証及び認可に影響する要素を図示＋明確化
- 認証・認可に関わるキーワードは、上図の中にどう位置付けられるか定義

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

５．2018年度の活動テーマ

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

2018年度の活動テーマ

【テーマ】

- IoTにおけるチャットボットの認証と認可等
- アイデンティティとIoT（IDoT）
- 認証要素、認可要素、その関係の整理
- アイデンティティLT大会
- ID管理チェックリストのCCMへの逆マッピング
- 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
- 教育コンテンツ制作検討（オンライン教育）

【その他】

- 他団体対応

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

JNSA