

TTCオンラインセミナー

「ニューノーマル時代のIoTエリアネットワークとセキュリティに関わる標準化・技術動向」

ID管理に関する ITU-T SG17の取組み

2021年11月30日(火)

日本電気株式会社

武智 洋

1. ITU-T SG17 課題10の概要
2. 活動経緯と勧告
 - 過去の活動と勧告
 - ID管理技術の進展と勧告
3. 関連活動フォローとフォーカス

ITU-T SG17 課題10の概要

ITU-T SG 17

◆ SG 17 は以下の項目のリードスタディグループ

■ セキュリティ

■ ID管理(Identity management (IdM))

■ 言語と記述技術 (Languages and description techniques) - ASN.1、OID等

■ E, F, X, Z シリーズの勧告

◆ SG17 : ID管理に関する Joint Coordination Activities (JCAs)活動

■ 課題10が実際的に JCA IDM の活動をコーディネートしている

◆ 課題9と課題10のマージ

課題 9：テレバイオメトリクス(Telebiometrics) と、課題10：ID管理技術のメカニズム及びアーキテクチャー (Identity Management mechanism and architecture) が統合され、

課題10：ID管理とテレバイオメトリクスのアーキテクチャー及びメカニズム (Identity Management Telebiometrics architecture and mechanism)

となった。

ID管理とテレバイオメトリクスのアーキテクチャー及びメカニズム

◆ 2021年SG17の課題9と課題10が統合された

◆ Motivation and Focus

■ Biometric

- Biometrics is gaining acceptance in identity verification/authentication in applications such as e-commerce, tele-medicine, and e-health.
- Biometric application systems present various challenges related to operational and technical data protection, reliability, and security of biometric data for biosafety and biosecurity applications.

■ バイオメトリクス

- バイオメトリクス（各人に固有の身体的または行動的特徴）は、eコマース、遠隔医療、e-ヘルスなどのアプリケーションでのID検証/認証で受け入れられつつあります。また、（ID検証/認証だけでなく、）バイオメトリクスを活用したシステムでは、バイオセーフティおよびバイオセキュリティアプリケーションにおいてバイオメトリックデータの運用的および技術的なデータ保護、信頼性確保、セキュリティに関連した様々な課題がある。

ID管理とテレバイオメトリクスのアーキテクチャー及びメカニズム（続き）

◆ Motivation and Focus

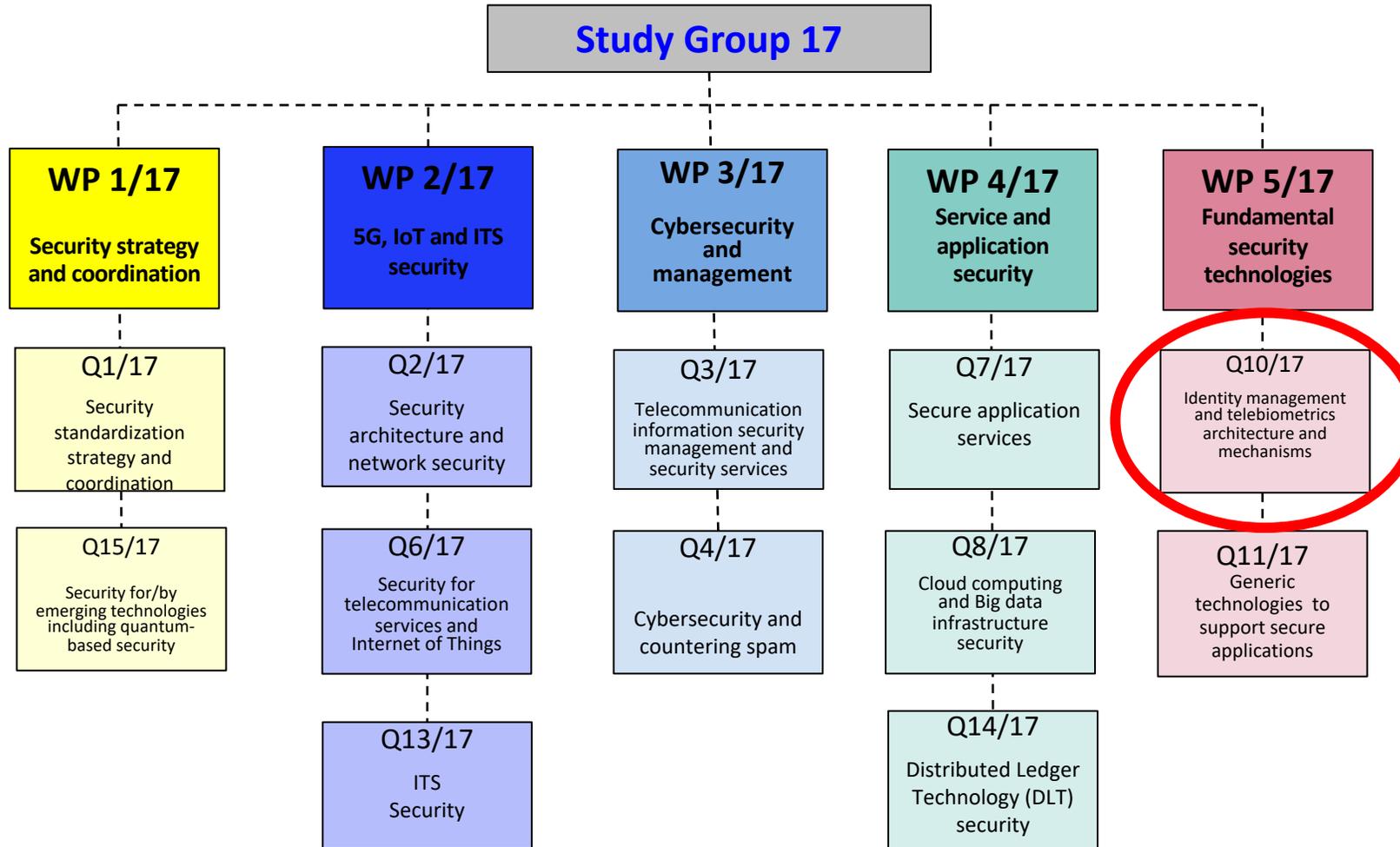
■ Identity Management

- Identity management (IdM) is essential for securing enterprises and consumer facing applications.
- Identity vetting, authentication are essential for on-line security
- Developing requirements, capabilities, and strategies for achieving interoperability between different IdM systems is essential.
- impact of decentralization (Distributed Ledgers) on identity systems including wallet, W3C decentralized identifiers and W3C verifiable credentials.
- Develop mechanisms for IdM interoperability to include identifying and defining applicable profiles to minimize interoperability issues?
- Develop mechanisms for the protection and disclosure of personally identifiable information (PII)?
- What are the requirements to protect IdM systems from cyber-attacks?

■ ID管理

- ID管理（IdM）では、企業と消費者向けアプリケーションを保護するための重要な要素として、以下を検討する
 - オンラインセキュリティに不可欠な身元確認、認証、
 - 異なるIdMシステム間の相互運用性を実現するための要件、機能、および戦略を開発、
 - ウォレット、W3C分散型識別子、W3C検証可能資格情報などのIDシステムに対する分散型（分散型台帳）の影響の検討、
 - 相互運用性の問題を最小限に抑えるために、適用可能なプロファイルの識別と定義を含むIdM相互運用性のメカニズムの開発、
 - 個人を特定できる情報（PII）の保護と開示のためのメカニズムの開発、
 - IdMシステムをサイバー攻撃から保護するための要件

ITU-T SG17の現在の構成



❖ The WP structure above will be reconsidered after WTSA20 in 2022.

Joint Coordination Activity on Identity Management (JCA-IdM)

- ◆ ITU-T ID管理活動に関して、他のITU-T SGおよび、外部団体との協調/調整
- ◆ ITU-T SG17会合に合わせて開催し、課題10が担当
- ◆ ID管理はITU-Tの以下のSG活動と関連しており、調整が必要になる場面がある。
 - SG2, SG13, SG15, SG16, SG20.
- ◆ IdM関連標準分析と課題10に関するロードマップの維持管理
 - Part 6: Identity Management (IdM) Landscape: IdM standards, organizations and gap analysis
<https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part06.aspx>
- ◆ ITU-T内およびその他のSDO /フォーラムとの重複活動を避けるために連絡窓口として機能
- ◆ JCA-IdMは外部コラボレーションの役割として、他の関連する承認されたSDO/フォーラムおよび地域/国の組織の代表者をJCA-IdMに招待することができる

IdM Coordinationの参加組織



26/179

活動経緯と勧告

過去の活動と勧告 (1)

◆ 2006/12～2007/9 ITU-T Focus Group on identity management (FG-IdM)

■ IDシステムについての標準化を開始にあたり、FG-IdMによって（その当時の）IDシステムに存在した課題を明確にし、以下のような勧告が課題6 Cybersecurity (2005～2008)で策定された

- **X.1250 : Baseline capabilities for enhanced global identity management and interoperability**

- アイデンティティ関連データを交換する際のID管理モデルの勧告

- **X.1251 : A framework for user control of digital identity**

- ウォレットと情報カードを使用したID情報のユーザー中心モデルの標準に関する勧告

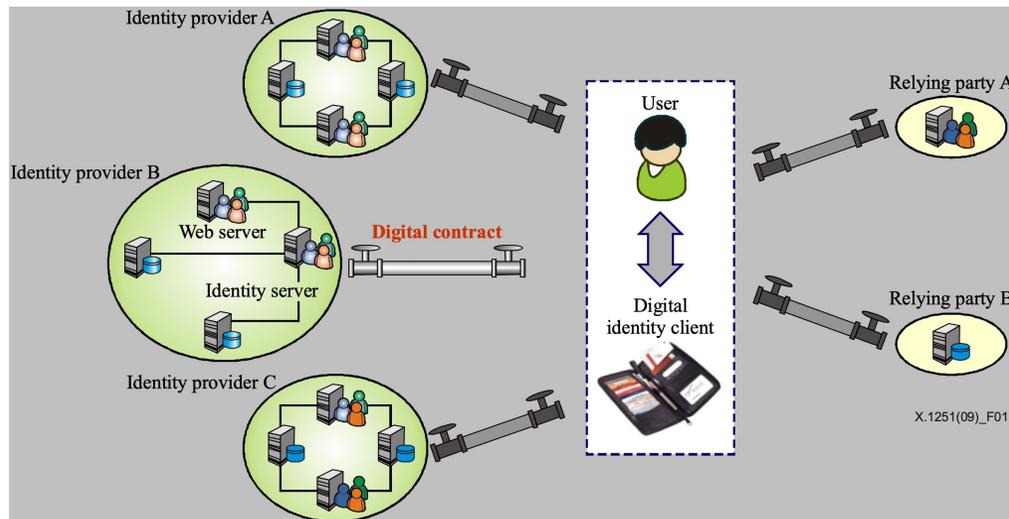


Figure 1 – The conceptual model for digital identity interchange

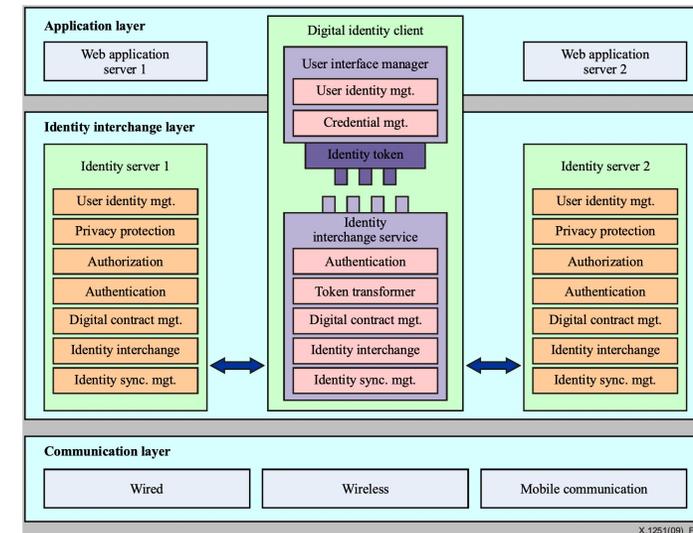


Figure 4 – Digital identity interchange framework

過去の活動と勧告 (2)

◆ 2006年 ITU-T Focus Group on identity management (FG-IdM) 発足

- **X.1252 : Baseline identity management terms and definitions**

- ITU-Tおよび多くのフォーラム全体でID管理用語の定義を調和するための勧告

- **X.1253 : Security guidelines for identity management systems**

- **X.1254 : Entity authentication assurance framework – ITU**

- NIST 800-63-3-1 をベースとした勧告で、当初はISO/IEC JTC1 SG 27 WG 5 との共同文書 ISO/IEC29115 ととして開発

- より強力なID登録と認証のためのガイドラインを提供するエンティティ認証フレームワークを形式化したもの (Level of Assurance: 1-Low, 2-Medium, 3-High, 4-Very high)

- 保証レベルの定義に関する最初の試み (審査と認証の組み合わせ)

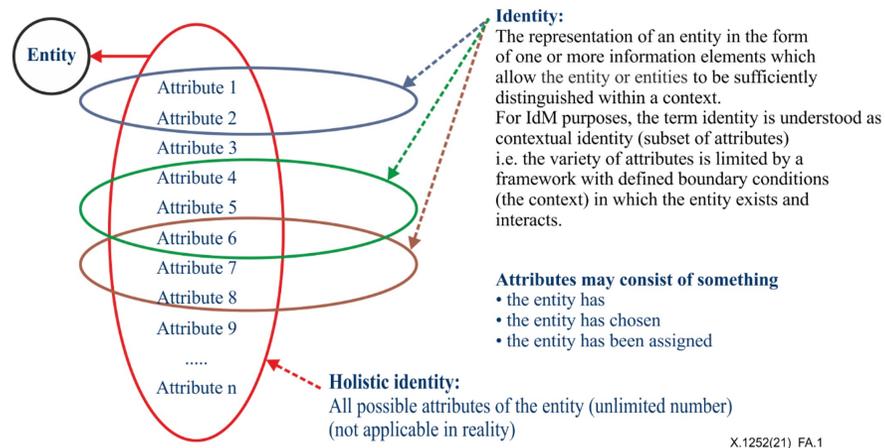


Figure A.1 – Relationships between entity, identities and attributes

X.1252 : Baseline identity management terms and definitionsより

	Technical	Management and organizational
Enrolment phase	<ul style="list-style-type: none"> • Application and initiation • Identity proofing and identity information verification 	<ul style="list-style-type: none"> • Record-keeping/recording • Registration
Credential management phase	<ul style="list-style-type: none"> • Credential creation • Credential pre-processing • Credential issuance • Credential activation • Credential storage 	<ul style="list-style-type: none"> • Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping
Entity authentication phase	<ul style="list-style-type: none"> • Authentication • Record-keeping 	<ul style="list-style-type: none"> • Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities

Figure 1 – Overview of the entity authentication assurance framework

X.1254 : Entity authentication assurance framework(旧バージョン 2012年) より

過去の活動と勧告 (3)

◆ 2006年にOASIS標準 SAMLとXACMLをITU-T勧告

■ X.1141 : Security Assertion Markup Language (SAML 2.0)

■ X.1142 : eXtensible Access Control Markup Language (XACML) 2.0 - ITU

■ SAML

- ID管理システムにフェデレーションメカニズムを提供する上で重要な役割
- ITU-Tで勧告化した後に普及
- 多くのIDシステムで実装されており、現在もIDシステムを保護するために重要な役割を担っている。

■ XACML

- ポリシーベースのアクセス制御を提供
- SAMLでうまく機能するように設計されており、徐々に採用されている

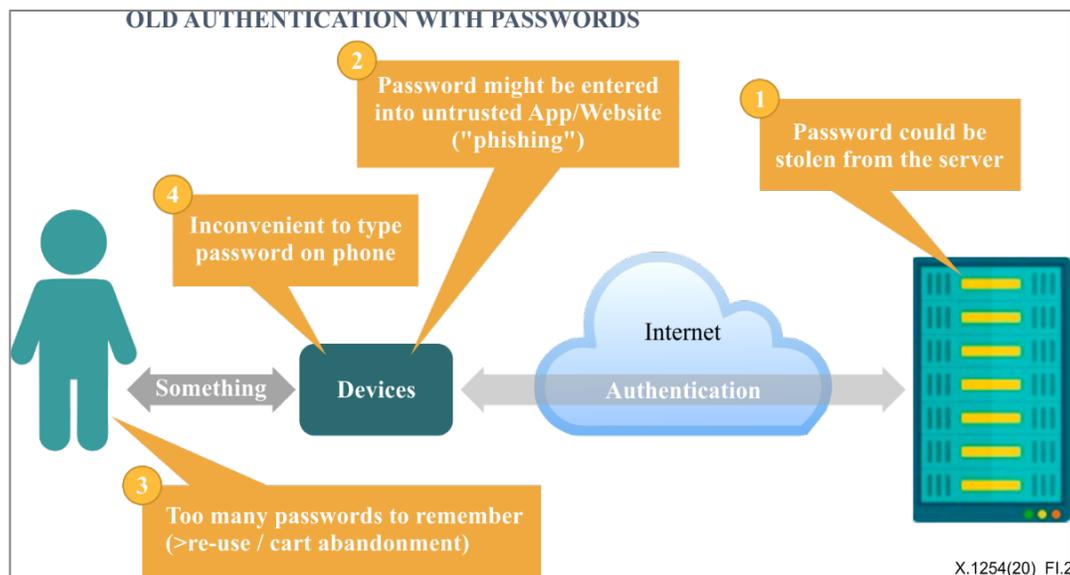
ID管理技術の進展と勧告 (1)

◆ 課題10の目的

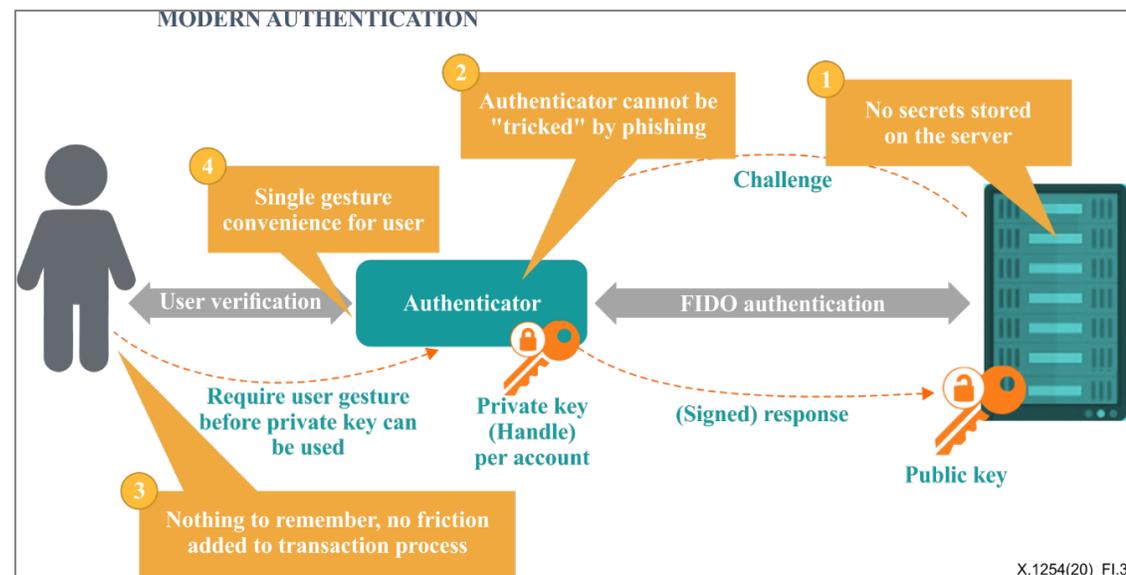
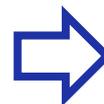
- ID管理システムのセキュリティを向上させるための継続的改善と様々な関連する最新技術を標準を取り入れていくこと

1. パスワードベースの認証システムのセキュリティを向上させるために**FIDO Alliance** 標準を勧告化

- X.1277 : Universal authentication framework
- X.1278 : Client to authenticator protocol/Universal 2-factor framework



Old authentication with passwords



New authentication with UAF/CTAP

ID管理技術の進展と勧告 (2)

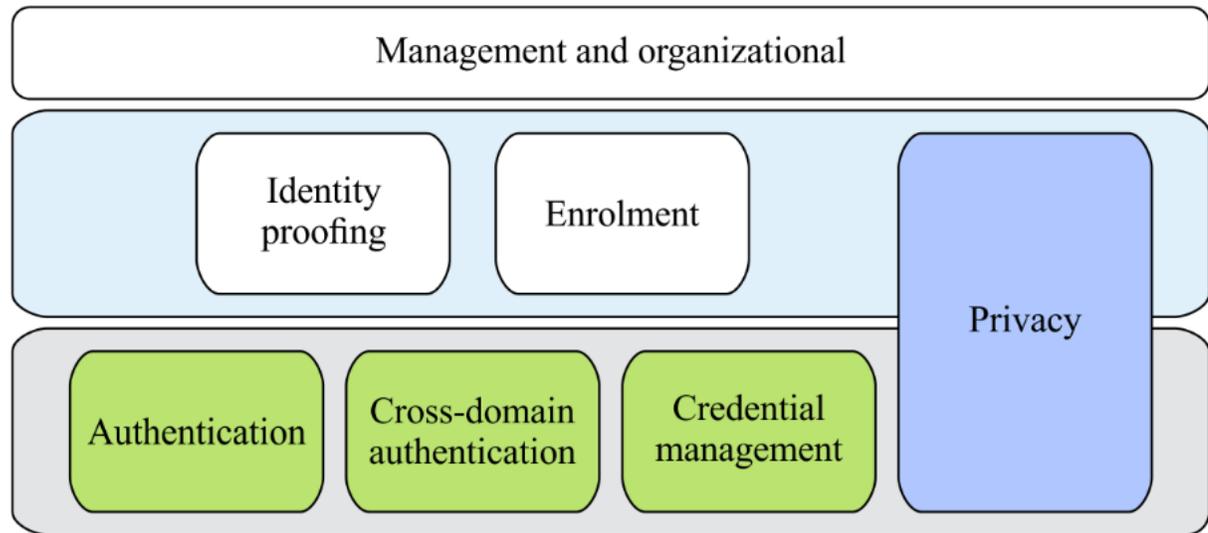
1. 最新動向に沿った各既存勧告更新

■ X.1252, “Baseline identity management terms and definitions”.

- *Decentralized identity* に関する用語・定義の取り組み

■ X.1254, “Entity authentication assurance framework”.

- NIST SP800-63-3更新に追従し、SP800-63-3bを取り入れるとともに、FIDOの認証も含んだ改訂を行なった
- **Level of Assurance (LoA)**の4レベルから、**identity assurance levels (IAL)**、**Authentication assurance levels (AAL)**、**Federation assurance levels (FAL)**の3つに分解し、それぞれ3レベルに



X.1254(20)_F02

Core aligned identity management standards

Assurance component	Descriptions	Activities
IA <i>Identity assurance</i>	Robustness of the identity proofing process and the binding between the authenticator and the identity-proofed individual.	<ul style="list-style-type: none"> • Identity proofing <ul style="list-style-type: none"> • Resolution • Validation • Verification • Enrollment • Binding
AA <i>Authentication assurance</i>	Confidence that a given claimant is the same as the previously authenticated subscriber.	<ul style="list-style-type: none"> • Authentication • Credential management <ul style="list-style-type: none"> • Credential issuance • Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement
FA <i>Federation Assurance</i>	Combines aspects of the federation model, assertion protection strength, and assertion presentation	<ul style="list-style-type: none"> • Key management • Runtime decisions • Attribute management

X.1254(20)_F6-2

Digital identity assurance levels

ID管理技術の進展と勧告 (3)

2. 現在改訂作業中

- X.1250, "Baseline capabilities for enhanced global identity management and interoperability"
- X.1251, " A framework for user control of digital identity"

- 集中型IdMシステムと分散型IdMシステムと組み合わせたハイブリット型モデルが市場に増えてきており、そのトレンドに追従すると共に、クラウドベースのソリューションも含めたモデル

3. 現在検討中の勧告案

- X.gpwd “Threat Analysis and guidelines for securing password and password-less authentication solutions”

- 強力な認証に関するガイドライン
 - 脅威分析
 - パスワードレス認証の定義
 - パスワードレス認証のセキュリティ

- X.tec-idms “Management and protection techniques for user data protection in distributed identity systems”

- PII in decentralized systemsのセキュリティ

- QRに依存したパスワードレス認証に関する検討

- OASIS ESAT TC でのQRコードを使った認証システムのセキュリティ検討

- X.1403 “Security guidelines for using distributed ledger technology for decentralized identity management”.

- 課題14: Distributed Ledger Technology (DLT) security との共同開発

- X.srdidm “Security requirements for decentralized identity management systems using distributed ledger technology”

関連活動フォローとフォーカス

◆ 課題10では、JCA-IdMを通じて、現在進んでいる産業界活動をフォロー

1. Accountable Digital Identity Association(ADIA)

• <https://adiassociation.org/>

2. Global Assured Identity Network(GAIN)

• <https://nat.sakimura.org/2021/09/14/announcing-gain/>

3. Trust Over IP (TOIP)

• <https://trustoverip.org/>

◆ 将来なフォーカスとして

■ Decentralized IdM systems

■ Zero Knowledge solutions

まとめ

◆ ITU-T SG17 課題10活動

- ID管理に関する産業界の最先端の活動をフォローし、標準化を通じてIDを基盤としたシステムの普及・推進を図り、ユーザ・アイデンティティのセキュリティの向上を目指している。
- （ある特定の実装に偏ることないように）相互接続性・運用性を重視し、SDO/フォーラム、国、その他関連組織間のコラボレーションを推進しています。

ITU-T SG17 課題10では皆様の参加をお待ちしております。

Q&A

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

\Orchestrating a brighter world

NEC