日本における
本人確認基盤（NAFJA）の考察
National Authentication Framework in Japan

2019年5月24日
才所敏明（（株）IT企画）、辻井重男
中央大学研究開発機構

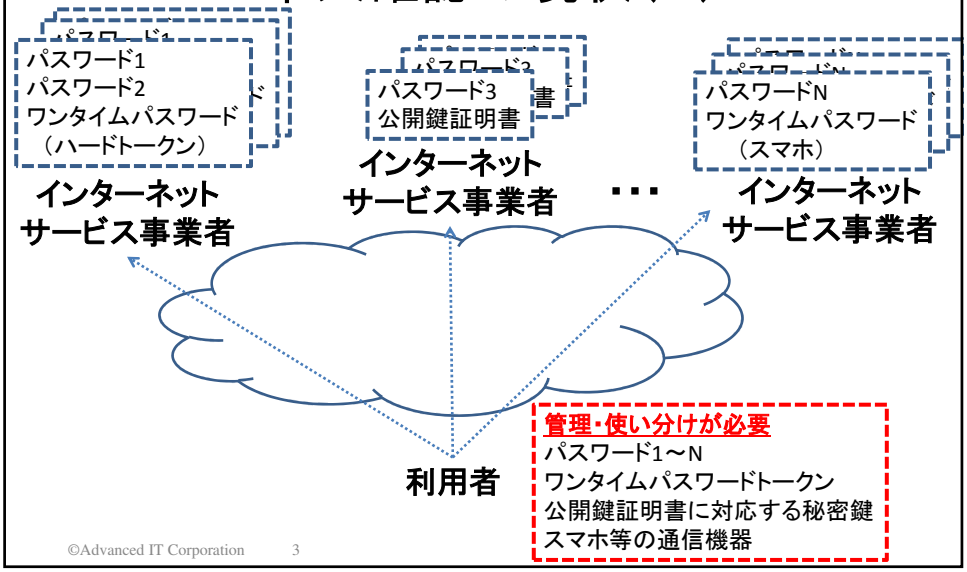
 1

説明項目一覧

 2

1．インターネットサービスにおける本人確認の現状と課題

インターネットサービスにおける本人確認の現状（1）



 3

1．インターネットサービスにおける本人確認の現状と課題

インターネットサービスにおける本人確認の現状（2）

利用者が保有するアカウント数（2018年のIPA調査結果より）
　6人に1人が8個、9人に1人が15個、11人に1人が25個程度保有
管理するパスワード数（2017年米国LastPass調査）
　企業の従業員は平均191個のパスワードを管理

個人情報漏洩事件の多発の状況
　1月28日　オージス総研「宅ふぁいる便」約480万件の個人情報
　1月29日　ジラフ「Peing-質問箱」
　　約150万件の個人情報がインターネット上で閲覧可能
　1月30日　ユニクロ　2017年9月1日～2019年1月16日
　　数百名の個人情報がインターネット上で閲覧可能

 4

1．インターネットサービスにおける本人確認の現状と課題

個別サービスごとの本人確認の課題

①多くの本人確認情報の安全・確実な管理のための、利用者の負担

②サービス利用の都度、サービス事業者ごとに異なる
本人確認情報の提示が求められる、利用者の利便性の悪さ

③本人確認情報を多くのサービス事業者に提供する、利用者の不安
（それぞれのサービス事業者のセキュリティ意識・対策のレベルのばらつき等による、本人確認情報の漏洩事件の多発）

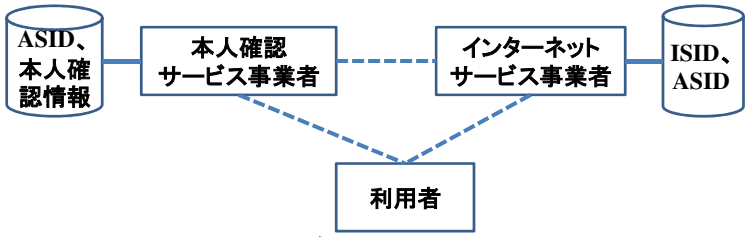
④それぞれのサービス事業者に求められる
本人確認情報の安全な管理、漏洩リスクの負担

⑤本人確認関連技術の発展に伴う
新たな本人確認手段への、サービス事業者ごとの対応の必要性

 5

2．独立した本人確認サービスの可能性と課題

独立した本人確認サービスのモデル



ASID（Authentication Service ID）：
本人確認サービス登録者に割り当てられる本人確認サービス利用者ID

ISID（Internet Service ID）：
インターネットサービス登録者に割り当てられるインターネットサービス利用者ID

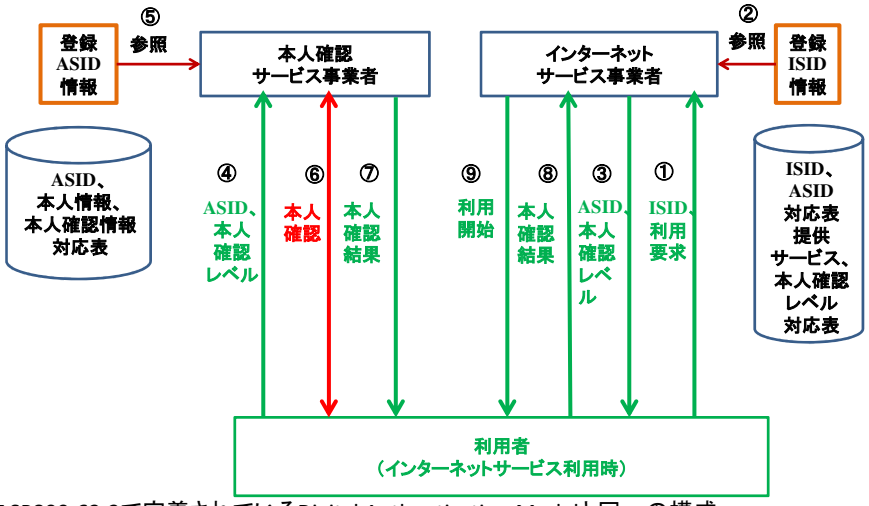
本人確認サービス事業者：ASIDと対応付け、
利用者の本人情報（名前、住所等の本人を特定・追跡可能な情報）、
本人確認情報（パスワード、所有物、生体特徴に関する情報）を管理

インターネットサービス事業者：ISIDと対応付け、
ASIDおよび、提供するサービス内容に応じ求める本人確認レベルを管理

 6

2. 独立した本人確認サービスの可能性と課題

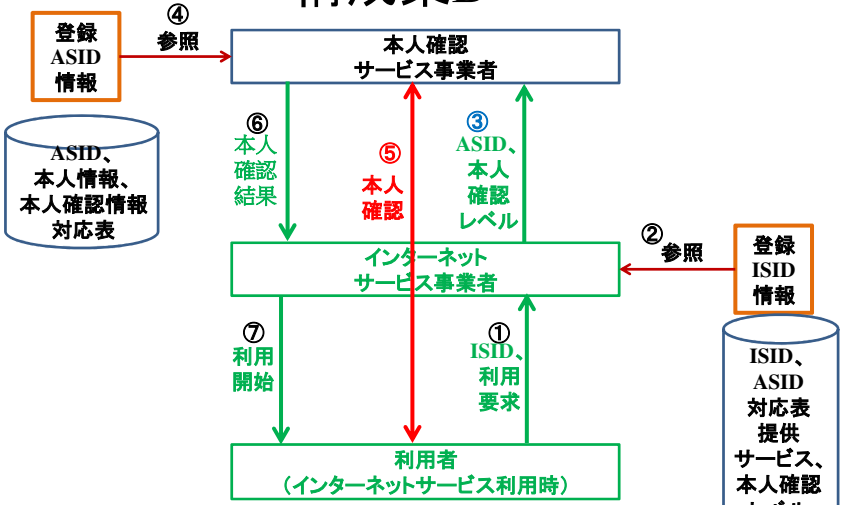
構成案A



NIST SP800-63-3で定義されているDigital Authentication Modelと同一の構成
インターネットサービス事業者の負担が最も少なく、利用者（システム）の負担が大きい構成
本人確認サービス事業者へ利用者とインターネットサービス事業者との関係の開示不要

2. 独立した本人確認サービスの可能性と課題

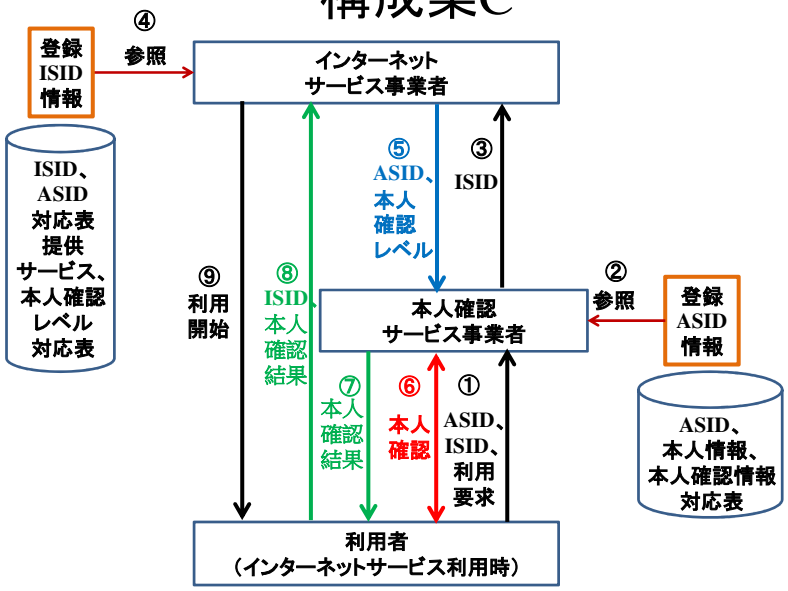
構成案B



インターネットサービス事業者が本人確認の仲介を行い利用者の負担軽減
本人確認サービス事業者へ利用者とインターネットサービス事業者の関係を開示
本人確認手続きの際のやり取りは利用者・本人確認サービス事業者間で暗号化し、
インターネットサービス事業者に漏えいしない工夫が必要

2. 独立した本人確認サービスの可能性と課題

構成案C



本人確認サービス事業者へ利用者とインターネットサービス事業者の関係を開示

2. 独立した本人確認サービスの可能性と課題 ●1/2

独立した本人確認サービス 期待される効果

①利用者にとっての効果

＊本人確認のための秘密の情報や所有物の安全・確実な管理負担の大幅な軽減

＊本人確認手続きが一定レベル標準化され、利便性が向上

＊本人確認情報の提供先が限定されるため、
本人確認情報の漏洩不安の大幅な軽減

＊本人確認情報の更新が一括で実施可能

②各種インターネットサービス事業者にとっての効果

＊利用者の本人確認機能の実装が不要（新たなサービスの導入が容易に）

＊利用者の本人確認結果への責任を本人確認サービス事業者へ移転可能

＊利用者の個人情報である本人確認情報の管理が不要
（個人情報漏洩リスクを回避可能）

＊本人確認技術の進歩に応じた新たな本人確認サービスの社会実装を
本人確認サービス事業者へ期待可能

独立した本人確認サービス 想定される課題

①本人確認機能の過度の集中への不安
➔複数組織による本人登録・確認サービス

②集約される本人確認情報の大量漏洩のリスク
➔暗号化、アクセス制御等による
一括漏洩防止の仕組みの検討

③独立した本人確認サービスのコスト負担の在り方
➔インターネットサービス事業者が負担？
金融機関等、高度な本人確認を必要とする
事業者の付帯事業として？

独立した本人確認サービスの 日本社会への実装

マイナンバー制度の存在

①日本では、行政分野でのネット経由の
本人確認方法についてはガイドラインがあり、
マイナンバーカードによる本人確認へ集約されつつある

②利用者登録時の本人確認が、その後のオンラインでの
本人確認サービスの信頼性を大きく左右するため、
マイナンバー制度を利用した本人確認が望ましい

③将来は行政分野も含めた本人確認基盤の可能性もあるが、
今回は民間サービスで共通に利用できる本人確認基盤
を想定

3．日本の本人確認基盤（NAFJA）の提案

日本の本人確認基盤

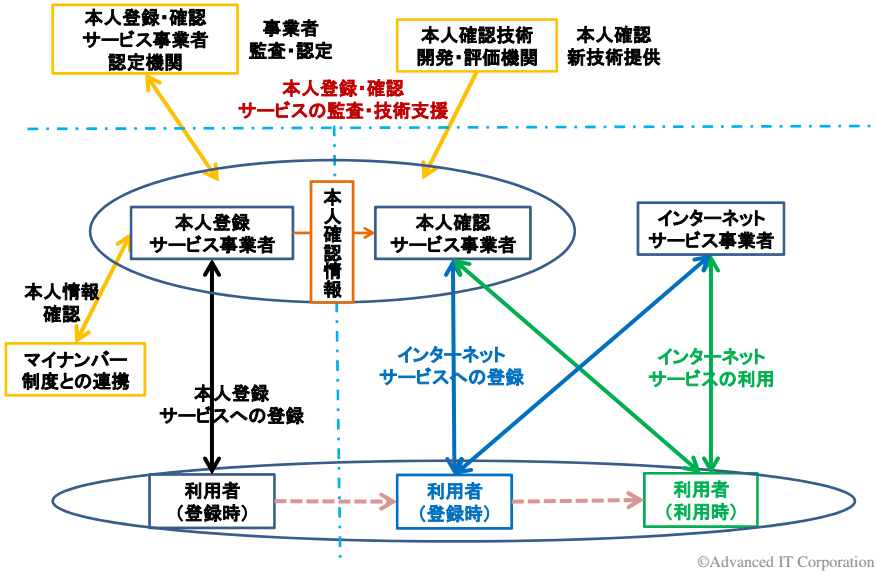
National Authentication Framework in Japan

（1）独立した本人確認サービスを前提とした
インターネットサービス利用のために必要な機能
①本人確認サービスへの登録（本人登録サービス）
②インターネットサービスへの登録（本人確認サービスの利用）
③インターネットサービスの利用（本人確認サービスの利用）
（2）本人確認サービスの信頼性確保のために必要な機能
本人確認サービスの適切な運用・セキュリティ対策の実施
最新技術を含む適切な本人確認方法・技術の採用
➔④本人登録・確認サービス事業者の監査・技術支援
（3）日本の本人確認基盤の構成案
＊利用者中継型の構成Aに基づく本人確認基盤（NAFJA/A）
＊インターネットサービス事業者中継型の
構成Bに基づく本人確認基盤（NAFJA/B）
なお、構成Cに基づく本人確認基盤（NAFJA/C）については省略

 13

3．日本の本人確認基盤（NAFJA）の提案

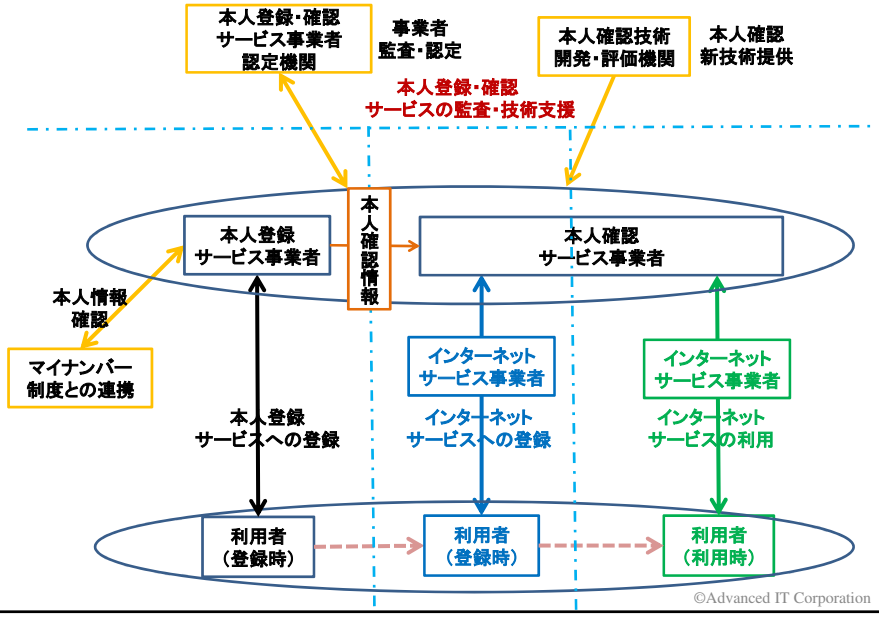
NAFJA/A



 14

3. 日本の本人確認基盤（NAFJA）の提案

NAFJA/B



 15

4. NAFJAの具体化のための主要な検討課題についての考察

NAFJAの具体化のための主要な検討課題

（1）本人登録サービス事業者による本人情報の確認について

（2）本人確認情報の登録・更新手続き

（3）本人確認方法の登録および本人確認レベルの特定

（4）本人登録・確認サービス事業者間での本人確認情報および本人確認方法の共有

（5）本人登録・確認サービスの利用ログ収集・管理

（6）本人登録・確認サービスの監査・技術支援

 16

4．NAFJAの具体化のための主要な検討課題についての考察

（1）本人登録サービス事業者による本人情報の確認について

①NAFJAではしっかりとした本人確認による登録が望ましい
　窓口によるしっかりとした本人確認・本人情報確認が原則
　　本人情報のJLIS登録情報による確認

②「Digital Identity Guidelines Enrollment and Identity Proofing」（NIST SP 800-63A）におけるIAL3（Identity Assurance Level 3）を想定

③いつ、どのような本人情報の確認を行ったか、
結果としての確認レベルも含め、記録を保存しておくのが望ましい

Identity Assurance Level（IAL）

（NIST Special Publication 800-63A（翻訳版），June 2017より抜粋）

IAL	レベルの定義
レベル1（IAL1）	**Applicant を現実世界の特定の Identity と紐づける必要はない.** Subject の行動に関連して提供される Attribute は, Self-asserted であるか, Self-asserted として扱われるべきである (CSP が RP に対して Assert する Attribute を含む). Self-asserted Attribute は確認も検証もされない.
レベル2（IAL2）	**エビデンスにより, Claimed Identity が現実世界に存在することを示す材料とし, Applicant が現実世界の当該 Identity と適切に関連づけられていることを証明する. IAL2 では Remote ないしは対面での Identity Proofing が必要となる.** Attribute は RP に対して CSP によって Assert されることもあり, Pseudonymous Identity が検証済 Attribute を持つこともサポートされる. IAL2 をサポートする CSP は, ユーザーの同意があれば IAL1 の Transaction をサポートしてもよい.
レベル3（IAL3）	**対面での Identity Proofing が必要である.** 識別に用いる Attribute は Authorized かつ訓練を受けた CSP の代理人によって検証される必要がある. IAL2 と同様, Attribute は RP に対して CSP によって Assert されることもあり, Pseudonymous Identity が検証済 Attribute を持つこともサポートされる. IAL3 をサポートする CSP は, ユーザーの同意があれば IAL1 および IAL2 の Transaction をサポートしてもよい.

（2）本人確認情報の登録・更新手続き

①原則として、利用者が使用を希望する本人確認情報を
利用できることが望ましい
記憶による本人確認のための情報：パスワード
所有物よる本人確認のための情報：
ワンタイムパスワードトークン（ソフト/ハード）
メールアドレス、電話番号（ショートメッセージ）
マイナンバーカード、等
生体特徴による本人確認のための情報：
指紋、顔画像、虹彩、等
②本人情報の確認レベルに応じ、
登録できる本人確認情報の制限が望ましい
（本人確認に使用されない不要な個人情報は登録しない）

（3）本人確認方法の登録 および本人確認レベルの特定

①原則として、利用者が使用を希望する
本人確認情報を利用できることが望ましい
単一本人確認情報による本人確認方法
複数本人確認情報による本人確認方法

②利用者は、本人確認方法の指定だけでなく、
本人確認レベルによる本人確認方法の
指定・絞り込みができるのが望ましい

③「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（各府省情報化統括責任者連絡会議決定）および「Digital Identity Guidelines：Authentication and Lifecycle Management」（NIST SP 800-63B）における技術基準を参考に、民間インターネットサービスの実体・事業者の意向・利用者の利用環境を踏まえ、採用する本人確認方法の選定と本人確認レベルを特定することが望ましい

Authenticator Assurance Level（AAL）

（NIST Special Publication 800-63B（翻訳版），June 2017より抜粋）

AAL	レベルの定義
AAL1	Subscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているというある程度の保証をもたらす．AAL1では幅広く利用可能なAuthentication技術を利用した，単一要素または多要素のAuthenticationを必要とする．Authenticationが成功するには，そのClaimantが，セキュアなAuthenticationプロトコルを介して，自身がそのAuthenticatorを所有・制御していることを証明する必要がある．
AAL2	Subscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているという高い確実性をもたらす．セキュアなAuthenticationプロトコルを介して，異なる2つのAuthentication要素を所有・制御していることを証明する必要がある．AAL2及びそれ以上では，Approved Cryptography技術が必要とされる．
AAL3	Subscriberのアカウントに対して結び付けられているAuthenticatorをClaimantが制御しているという非常に高い確実性をもたらす．AAL3におけるAuthenticationは，暗号プロトコルを介した鍵を所有していることの証明に基づいている．AAL3のAuthenticationは，ハードウェアベースのAuthenticatorまたはVerifierに対してなりすまし耐性を提供するAuthenticatorを要求する．この際，同じデバイスが両方の要件を満たしていても良い．AAL3でAuthenticateするために，ClaimantはセキュアなAuthenticationプロトコルを介して2つの異なるAuthentication要素を所有・制御していることを証明する必要がある．Approved Cryptography技術が必要とされる．

4．NAFJAの具体化のための主要な検討課題についての考察

（4）本人確認情報および本人確認方法の共有

①本人登録サービス事業者での共有が望ましい

単一の事業者では無く、少数のしかし複数の認定された
本人登録サービス事業者の存在が望ましい

各本人確認登録サービス事業者が登録した
本人確認情報・本人確認方法は共有されることが望ましい

②本人確認サービス事業者での共有が望ましい

本人確認サービス事業者も、少数のしかし複数の認定された
本人確認サービス事業者の存在が望ましい

登録された本人確認情報・本人確認方法は
本人確認サービス事業者でも共有されることが望ましい

③本人確認情報および本人確認方法の内容は、過去の登録内容も含め、改ざんができないよう、ブロックチェーン等を活用し管理するのが望ましい

④本人確認情報および本人確認方法の内容は個人情報であり、その漏洩対策には万全を期す必要があろう
コンソーシアムタイプのブロックチェーンとし、
アクセス制御および内容の暗号化等の対策が望ましい

⑤登録者本人の登録内容確認のための参照等についても、対応できる必要があろう

 23

4. NAFJAの具体化のための主要な検討課題についての考察

（5）本人登録・確認サービスの利用ログ収集・管理

①本人登録サービス利用ログの収集・管理が望ましい
登録ログ、更新ログ
利用者・インターネットサービスによる参照ログ

②本人確認サービス利用ログの収集・管理が望ましい
利用者・インターネットサービスによる本人確認ログ

③本人登録・確認サービス事業者の
監査機関による定期的な監査が望ましい

 24

4．NAFJAの具体化のための主要な検討課題についての考察

（6）本人登録・確認サービスの監査・技術支援

①NAFJAが信頼できる仕組みとして運用されていることを、
第三者が定期的に監査し、参加できる事業者を
認定する仕組みが望ましい

②NAFJAで使用する本人確認方法や、
本人確認方法の本人確認レベルの認定は、
第三者が技術的に評価し認定する仕組みが望ましい

③事業者の監査や技術の評価は、
公的組織が担当するのが望ましい

4．NAFJAの具体化のための主要な検討課題についての考察

まとめ

（1）本人登録サービス事業者による本人情報の確認について
原則、窓口・対面登録、マイナンバー制度の活用、IAL準拠
（2）本人確認情報の登録・更新手続き
認定本人確認情報登録、本人確認検証
（3）本人確認方法の登録および本人確認レベルの特定
認定本人確認方法登録、本人確認レベル特定、AAL準拠
（4）本人確認情報および本人確認方法の共有
コンソーシアムタイプブロックチェーン、個人情報の保護
（5）本人登録・確認サービスの利用ログ収集・管理
コンソーシアムタイプブロックチェーン、個人情報の保護
（6）本人登録・確認サービスの監査・技術支援
事業者認定、本人確認方法認定、第三者機関（公的組織）

5. 既存のSSOシステムとの関連 ●（20分）

既存SSO（SAML、OpenID Connect）との関連

（1）既存SSOに相当する機能は
NIST Special Publication 800-63C
Digital Identity Guidelines Federation and Assertions
にて定義されている。

（2）本報告では言及しなかった
本人確認サービスが利用者へ提示する本人確認結果
利用者がインターネットサービスへ提示する本人確認結果
の具体的内容・形式は、SAML、OpenID Connectの仕様との整合性に配慮し検討する必要があろう。

（3）NAFJAとSAML、OpenID Connectとの連携を実現し
国民IDおよび国民ID確認システム（日本ではマイナンバー制度）、
と連携したグローバルなID連携が必要となろう。

6. おわりに ●

おわりに

（1）インターネットサービス提供に必要な本人確認機能が事業者個々により提供されている現状の課題を提示

（2）日本社会がますますインターネットサービスへの依存を強める中、本人確認機能の事業者個々による対応では無く、個人情報や個人情報を利用した本人確認機能の専門事業者への集約を提案
日本における本人確認基盤（NAFJA）
National Authentication Framework in Japan

（3）NAFJAの具体化のための主要な検討課題を提示、その対応方法等についての考察結果を提示

（4）オンライン行政手続だけでなく、民間のインターネットサービスにおいても、安心・安全・確実な本人確認の実現に向け、NAFJA構想の具体化を今後も検討予定

終

（ご清聴、ありがとうございました）

