JIPDEC レポート

NIST SP 800-63-3 の概要と今回の改訂がもたらす影響

OpenID BizDay#11「NIST SP 800-63-3 を読む」より

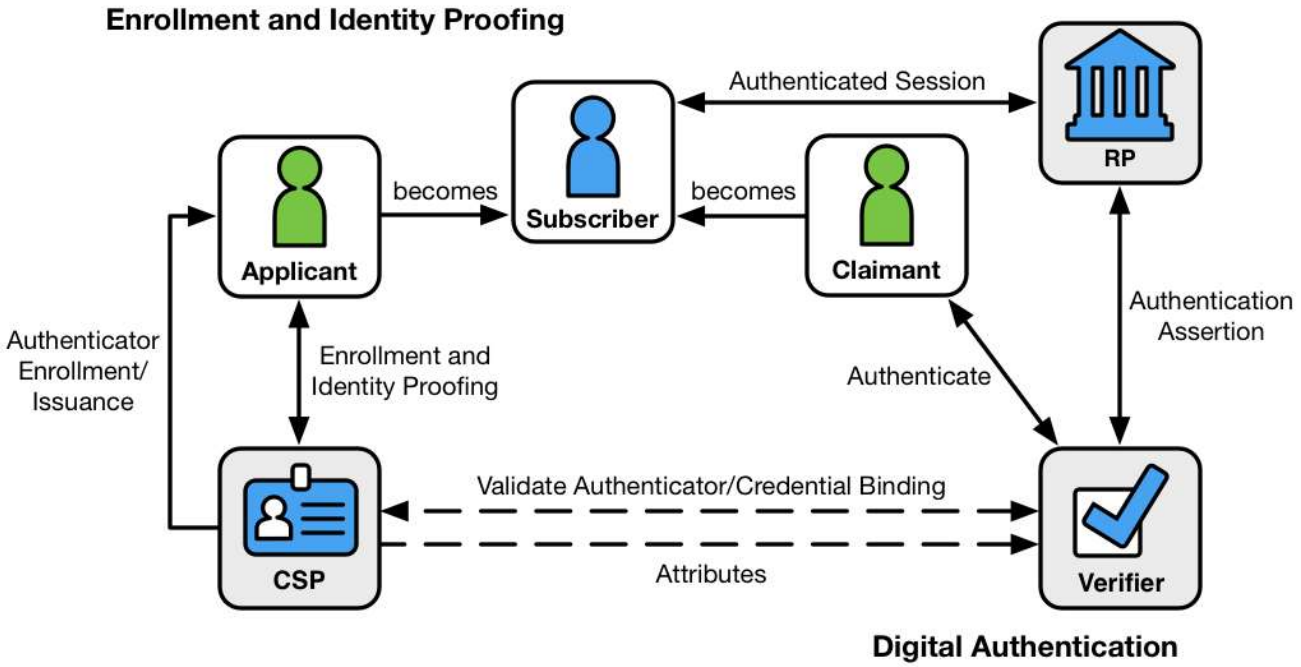
当日の翻訳資料は JIPDEC サイトよりダウンロード可能

米国立標準技術研究所（NIST）の認証に関するガイドライン「Electronic Authentication Guideline（電子的認証に関するガイドライン）」第 3 版（ NIST SP 800-63-3）が 2017 年 6 月に正式発表された。このガイドラインは 米国政府のセキュリティ対策での利用を前提にしているが、政府系システムとの接続要件等にも関係してくるため、世界的にも大きな影響を与える可能性がある。既に ID 管理技術に関する業界団体 Kantara Initiative では、新規格に合わせた認証スキームの更新が進められている。

NIST SP 800-63-3「Digital Authentication Guideline」概要

本ドキュメントは、アメリカ政府機関がユーザ認証やユーザの Identity Proofing を行うシステムを構築する際の実装ガイドラインであり、日本の制度と異なる部分や、民間サービスに合わない部分もあるが参考にすべき点も多い。

これまでの第 2 版では、アメリカの政府システムで認証を行う際の指標（LoA：Level of Assurance）に基づいた要件を定めており、これは日本でも広く参考にされているが、第 3 版では LoA という考え方に代わり、Digital Identity Model の 3 フェーズについて Assurance Level を定義し、Assurance Level ごとにサブドキュメント化することで、サービスの内容に合わせて各フェーズの Assurance Level をより実際のニーズ（仮名性は確保しつつ認証レベルは強化したい等）に合わせて組み合わせることが可能となっている。



IAL、AAL、FAL の概要

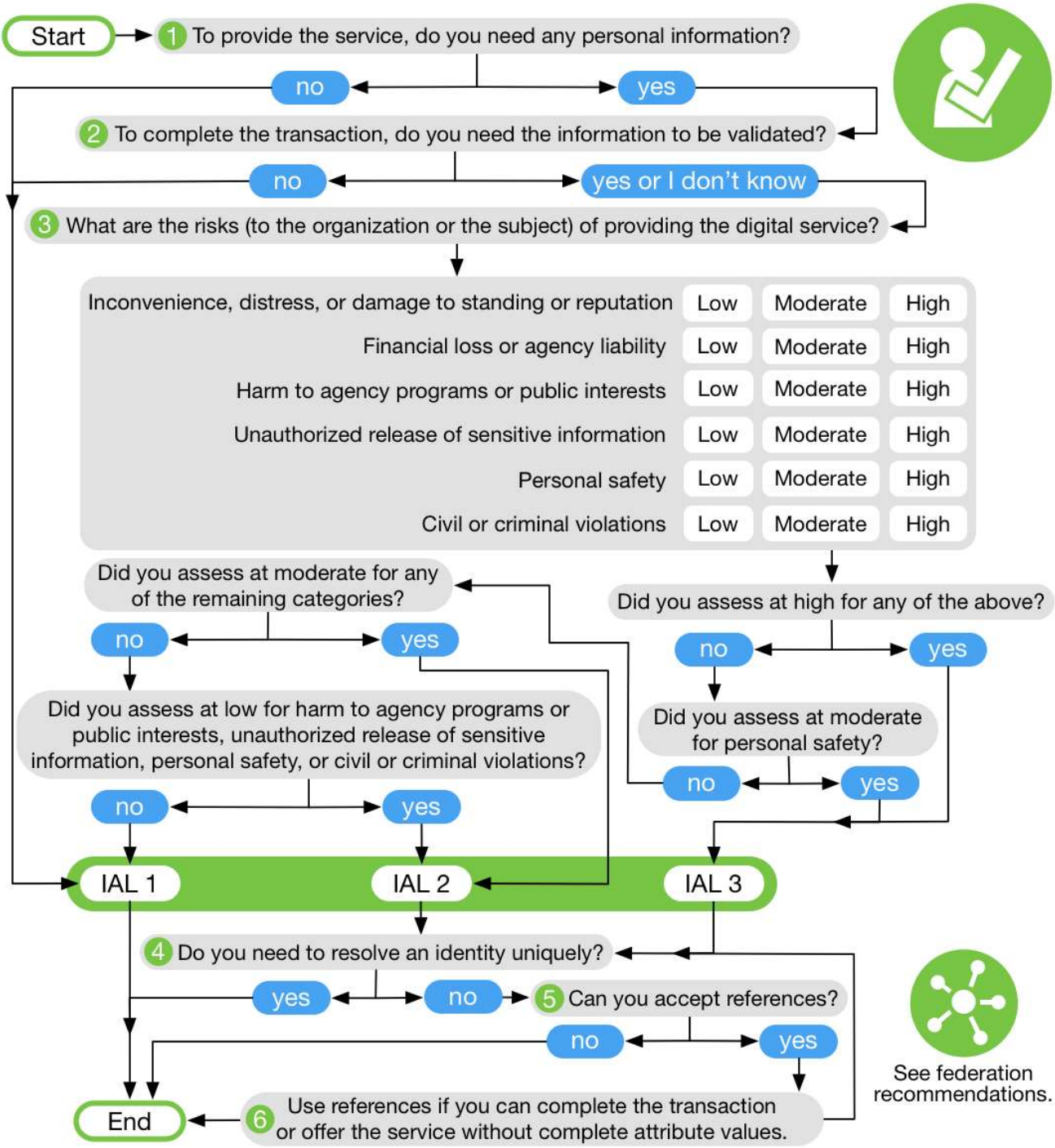
各 Assurance Level とフェーズ、対応するドキュメントは以下のとおり。

- Identity Assurance Level（IAL）（SP 800-63A）
  ユーザが申請者（Applicant）として新規登録（SignUp）する際に、CSP（Credential Service Provider）が行う本人確認（Identity Proofing）の厳密さ、強度を示す
  Lv.1　本人確認不要、自己申告での登録でよい
  Lv.2　サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要あり
  Lv.3　識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者

- Authenticator Assurance Level（AAL）（SP 800-63B）
  登録済みユーザー（Claimant）がログインする際の認証プロセス（単要素認証 or 多要素認証、認証手段）の強度を示す。
  Lv.1　単要素認証で OK
  Lv.2　2 要素認証が必要、2 要素目の認証手段はソフトウェアベースのもので OK
  Lv.3　2 要素認証が必要、かつ 2 要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）

- Federation Assurance Level（FAL）（SP 800-63C）
  ID トークンや SAML Assertion 等、Assertion のフォーマットやデータやり取りの仕方の強度を示す
  Lv.1　Assertion（RP に送る IdP での認証結果データ）への署名
  Lv.2　署名に加え、対象 RP のみが復号可能な暗号化
  Lv.3　Lv.2 に加え、Holder-of-Key Assertion の利用（ユーザごとの鍵と IdP が発行した Assertion を紐づけて RP に送り、RP はユーザがその Assertion に紐づいた鍵を持っているか（ユーザの正当性）を確認）

SP 800-63-3 では、各機関はリスクアセスメントを行った後に IAL、AAL、FAL のレベルを選定するためのチャートが提供されており、該当したレベルの要件をサブドキュメントで確認したうえで、要件を満たすサービス実装を行うことになる（下図　IAL レベル判定チャート）。



第 3 版では、「セキュリティが統制されている」、「リスク評価がなされている」など、800-53 や 800-30 を前提として、各プロセスにレベル分けした要件が定められている。政府機関は独自の体制が出来上がっているが、専門部署を持たない民間企業が実際にリスク評価を行うことができるかが、本ガイドラインを参考にするうえでの今後の課題となる。

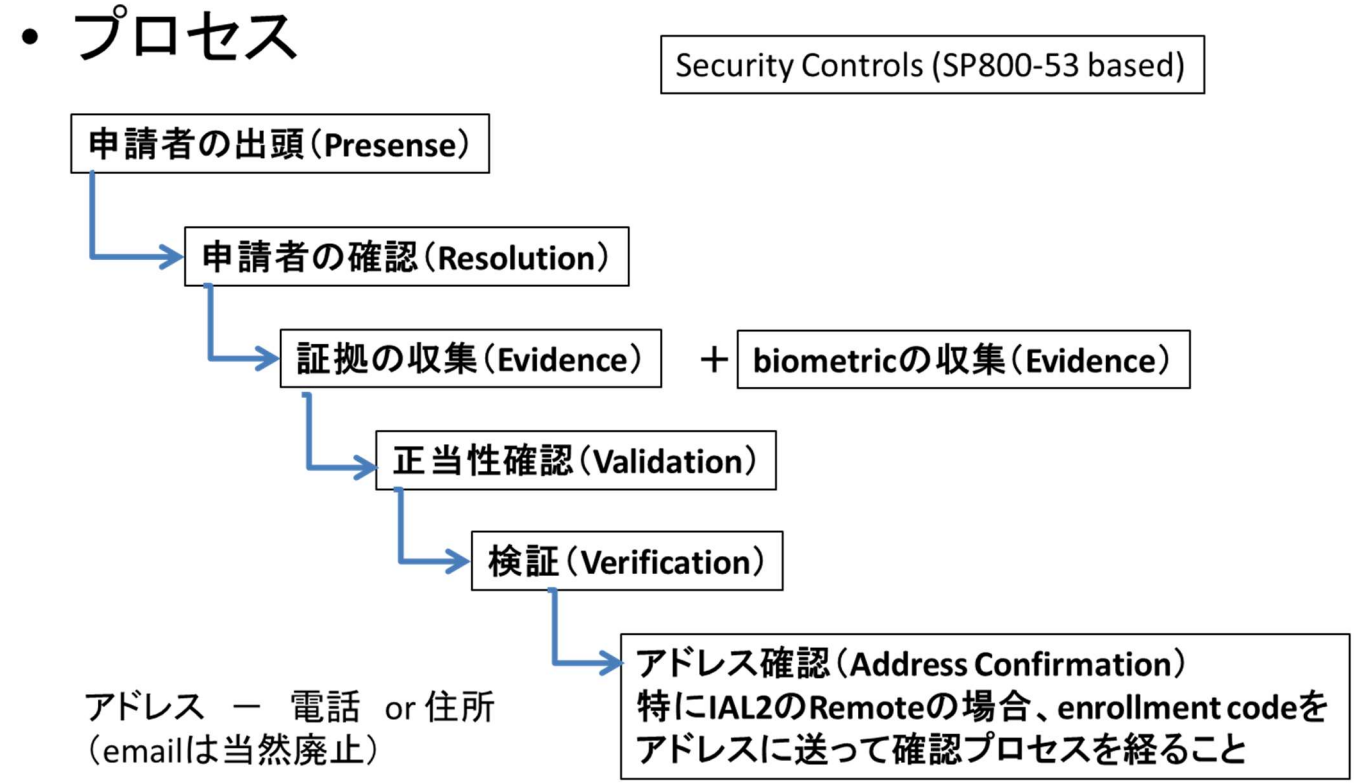
SP 800-63A「Enrollment ＆ Identity Proofing（登録と本人確認）」

63A では、登録と本人確認について必要なプロセス（Resolution（収集）、Validation（正当性チェック）、Verification（検証））の整理と「強さ」を 1～3 のレベルで定義されている。3 段階になったことで、より

明確なレベル分けが可能となった。

エビデンスの収集に関しては、プライバシーの観点から「minimum（必要最小限のものしか収集してはいけない)」が強調されている。

正当性チェックの強さを以て証明するのは、登録しようとするユーザがリアルワールドの人間と結びついているかという点である。過去のインシデントから利用可能な手段が見直され、例えば Knowledge based verification は採用不可となっている。



IAL1 は

- （エビデンスを収集して）属性の有効性チェック検証をしては「ならない」（申告されたとおりに処理すること）
- CSP は、サービス提供のために、申請者に、属性の自己申告を求めることは許容される
- IAL2, IAL3 相当の CSP は、利用者が同意するのなら、IAL1 のみを要求する RP にも対応すべきである（下位互換の保証）

となっている。通常のビジネスであれば十分なレベルである。

IAL2 では、エビデンスの強度（Superior、Strong、Fair）を定義し、Superior または(内部で正当性チェックが可能な)Strong エビデンス、または Strong エビデンス 2 件、または Strong エビデンス 1+Fair エビデンス 1 としている。

SP 800-63B「Authentication and Lifecycle Management（認証とライフサイクル管理)」概要

63B は、登録済みアカウントを利用してデジタル世界でのユーザ認証を行い、その結果の正しさを確認するプロセスについて記述されており、Authenticator タイプや AAL（Authenticator Assurance Level）

が定義されている。

今回の改訂で、ユーザ認証に使われる技術に関する NIST の見解が示されており、米国政府向けとは言いつつも、今後一般的なサービスにも影響が及ぶ可能性が一番高い部分になる。特にパスワードや PIN 等ユーザが記憶する「記憶シークレット」については、今後パスワードからパスフレーズへの移行が意図されていたり、パスワードの定期変更の非推奨、秘密の質問の排除等が盛り込まれている。

このほかにも、乱数表の使用方法が制限されたり、現時点では生体認証を利便性提供のための補助的な認証要素との位置づけられているなど、ID 管理を含むサービス構築の際に考慮すべきポイントが見られる。

AAL 毎の要件サマリ

要件	AAL1	AAL2	AAL3
許可されている Authenticator タイプ	記憶シークレット; ルックアップシークレット; アウトオブバンド; 単一要素 OTP デバイス; 多要素 OTP デバイス; 単一要素暗号ソフトウェア; 単一要素暗号デバイス; 多要素暗号ソフトウェア; 多要素暗号デバイス	多要素 OTP デバイス; 多要素暗号ソフトウェア; 単一要素暗号デバイス; または記憶シークレット及び: •ルックアップシークレット •アウトオブバンド •単一要素 OTP デバイス •単一要素暗号ソフトウェア •単一要素暗号デバイス	多要素暗号デバイス; 単一要素暗号デバイス及び 記憶シークレット; 単一要素 OTP デバイス及び多要素暗号デバイスまたはソフトウェア; 単一要素 OTP デバイス及び単一要素暗号ソフトウェア及び記憶シークレット
FIPS 140 確認	Level 1 (政府機関の Verifier)	Level 1 (政府機関の Authenticator 及び Verifier)	Level 2 総合 (多要素 Authenticator) Level 1 総合 (Verifier 及び単一要素暗号デバイス) Level 3 物理セキュリティ (全ての Authenticator)
Reauthentication	30 日	12 時間 または 30 分 の非活動; 1 つの Authentication 要素でもよい(MAY)	12 時間 または 15 分 の非活動; 両方の Authentication 要素をつかうものとする(SHALL)
セキュリティ統制	SP 800-53 低度のベースライン(または等価)	SP 800-53 中度のベースライン(または等価)	SP 800-53 高度のベースライン(または等価)
中間者攻撃耐性	必須	必須	必須
Verifier なりすまし耐性	不要	不要	必須
Verifier 危殆化耐性	不要	不要	必須
リプレイ耐性	不要	必須	必須
Authentication 意図	不要	推奨	必須
レコード保持ポリシ	必須	必須	必須
プライバシー統制	必須	必須	必須

SP 800-63C「Federation and Assertions（連携とアサーション）」

63C の内容は、すでに ID 連携を行っているサービスに限定される。さらに少なくとも現時点では、FAL（Federation Assurance Level）2 以上が求められる状況は、政府機関のごく一部に限られるので、一般的なサービス事業者への影響は少ない。

今回の改訂がもたらす影響を考える

1)Identity Proofing への影響

63A の内容自体は、例えば免許証の発行プロセスからして国により異なるので細部は調整する必要があるが、エビデンスの強度やプロセス評価に関する部分は日本でも適用できるものとなっている。

ただ、現状、本人確認プロセスが入るコンシューマー向けサービスは少数なので、63A の内容がサービスに与える影響は少ない。コンシューマー向けサービスでは、本人確認から認証までの強度を上げることは、ユーザのハードルを上げることにもつながる。例えば携帯キャリアとのサービスで携帯契約時の本人確認と連携させる等は考えられるが、一方で銀行等高いセキュリティ強度に合わせるとなると、仕組みとしては提供できても全ユーザに強制することが難しく、バランスを見ながら取り組んでいく必要がある。

また、エビデンスの強度は、今後各業界団体等で検討し明確化していく必要がある。

2)Authentication への影響

63B は認証技術を網羅的に整理し、それぞれについて一定の評価がなされ、今後の方向性が示されている。Authenticator 自体は国が変わっても対応が変わるものではないので、日本においてもサービスへの対応を考える上で参照に値する。

ユーザビリティの観点からは、パスワードの定期変更非推奨や記号・数字等の組合せ要件の排除等は望ましい変更だと思われる。NIST は、セキュリティを高めるため人に課す規制は、結果としてセキュリティ強化につながらなかったと結論付け、ユーザビリティ向上がセキュリティ強化につながるかどうかの試行段階に移行したととらえることができる。

一方、現状のサービスの多くは改訂前の LoA（Level of Assurance）を受けてプロファイルを整備してきており、今回の改訂内容をサービスに反映させるには、相応のコスト負担が強いられることとなる。

実際の会員サイト構築の現場では、本来、重要性が高いはずの認証部分が（予算的にも）過小評価されるケースが多いので、突然認証部分の要件が増えれば大きな混乱が予想される。また、すでに「秘密の質問」等不正利用の可能性が指摘されているものでも、ユーザがアカウントリカバリーの手段として利用していれば、簡単に廃止することはできない。

今回非推奨となった認証技術からどのように移行させていくかは、長期的な視野で検討する必要がある。局所的な対応でコストを抑制することが、長期的にはコスト増につながるケースもある。米国政府自体はパスワードを廃止する方向にあるが、すべてに対して利用停止を求めているわけではなく、パスワードでの管理の限界を認識することを促している。日本では強度を強くして延命させるべきか、より強い認証手段に移行するか、リスク評価を行ったうえで検討していく必要があるのではないか。

3)Federation への影響

今回の改訂で、Federation の利用が強く推奨されるようになったが、BtoB、BtoC の世界では当面レベル 1 以外は対象外だと思われる。また、レベル 3 を要求するサービスとの連携ではブラウザ非対応の部分もあり実装に苦慮することも考えられるが、レベル 2 までであれば技術的にはすでに様々なサービスで利用されているものなので問題はない。ただし、すでに動いているサービスへの追加や連携方法の変更には相当期間の時間と相応のコストがかかると思われる。

今後の課題

このドキュメントはあくまでも米国政府向けなので、実ビジネスで同等の対応をしなければならないわけではない。しかし、グローバルにサービスを展開していくためには、ITC ジャイアントの基準は意識せざるを得ない。

リスク評価の体制づくり

日本において、Digital Identity を利用したサービスを提供する際に、我々が NIST と同様のリスク評価プロセスを踏む体制作りは大きな課題となる。業界全体できちんとしたリスク評価がなされる土壌を形成しないと、結果的にサービス全体に対してより厳しい規制・圧力がかかってくる。認証局の世界では、ブラウザ側がパワープレイヤーとしてガバナンスを利かせる役割を果たしているが、Federation 等ではサービス提供側が様々なプレイヤーと協調しながらできるだけオープンに使える仕組みを育てていくことが望ましい。

トラストフレームワークの確立

今後、マイナンバーカードで銀行口座開設等の連携は、国や金融機関主導で推進されることが予想される。一方で、電話番号であればキャリア、郵送先住所であれば EC サイトの商品配送履歴情報など、民間データを活用した連携については、現状なかなか検討が進まない。

今回の改訂で、実装に当たっての概念の整理はしやすくなっているので、この考え方をベースに検討がなされれば、今後、オンライン完結型社会実現に向けて、800-63-3 で得られた知見を共有し、日本でトラストフレームワークの構築が進めば、海外への事業展開や事業連携も容易になる可能性がある。

他基準・ガイドラインへの反映

Azure や、AWS は NIST SP800 等をベースにしているクラウドセキュリティ基準「FedRAMP」を採用して、政府向けプラットフォームとして利用可能なセキュリティ水準を担保している。今後、日本企業がクラウド系・認証系の製品を政府向けに展開しようとすると、（米国向けとはいえ）政府調達要件に適合していることを明確化できる米国企業の製品に対抗することが難しくなっていくことが考えられるので、何らかの対応が必要となってくる。

また、今回のガイドラインでは、パスワードは個人情報を取り扱わない場合に可としているが、現時点では、個人情報保護委員会のガイドラインでの例示や ISMS、PMS の中ではパスワードによる管理が前提となっている。今後、セキュリティ専門家の評価が様々なドキュメントに反映されるような体制づくりも必要になってくる。

これらの課題解決に向けた検討を行う際には、議論のディスカッションコストを下げるためにも、本ガイドラインのような知見を共有し、全体的な知識の底上げ、議論の共通前提としていくことが重要となる。JIPDEC も、引き続き関係団体と連携しながら情報の共有や啓発を行っていきたい。