資料5

公的個人認証サービスによる
オンライン認証の提供

１　主なオンライン認証手段

情報システムにアクセスする人を認証する手段として考えられる方法は、以下のとおり。

１　記憶による認証

その人にしか知り得ない情報を用いて認証を行う。
（例：暗証番号、ID・パスワード）

２　所有物による認証

その人しか持ち得ない所有物を基に認証を行う。
（例：IDカード、ICカード、トークン）

３　本人の特徴による認証

その人の持つ身体的、行動的特徴を利用して認証を行う。
（例：指紋、虹彩、静脈、音声認識）

４　上記１～３の組合せ

２　オンライン認証手段のメリット・デメリット

主なオンライン認証手段のメリット・デメリットを比較すると以下のとおり。

	記憶	所有物	本人の特徴
例	暗証番号、 ID・パスワード	IDカード、ICカード、 トークン	指紋、虹彩、静脈、音声認識
メリット	実装コストが安価、 持ち運びの問題がない	操作が容易	生涯不変、 忘却の恐れなし、 持ち運びの問題がない
デメリット	忘却の恐れ、盗聴、 類推、総当り攻撃	実装コストが高価、 貸し借り、紛失、盗難、 耐タンパー性の確保、 ハードウェア障害のおそれ	実装コストが高価、 プライバシー面のリスク、 体調（ケガ、病気）により認証できない可能性

※　トークン：利用権限のあるユーザに与えられる、認証を補助する機器。

※　耐タンパー性：非正規な手段による機密情報の内部解析や改変を防護する能力。

3　記憶による認証（ID・パスワード方式の危険性）

ID・パスワード方式は広く一般で用いられているが、以下のような危険性が存在する。

① フィッシング

偽造メール等で顧客を本物そっくりの偽造サイトに誘導し、IDやパスワード等の個人情報を盗み出す。

② スパイウェア

知らないうちにパソコン内に侵入し、IDやパスワード等の個人情報を盗み出す。（キーボードの入力情報を盗むキーロガー等）

その他、総当り・類推によるヒットや、管理の困難性（パスワードの忘却、メモの紛失・盗難）等の問題。
→　より複雑なパスワード設定、厳重な保管、定期的な変更が欠かせない。

（参考）フィッシング、スパイウェアによる被害の状況

１　フィッシング

- 米国では、年間で約7，300万人が平均50件以上のフィッシングメールを受け取り、被害額は約9億3千万ドル（約1，000億円）に達する（米国ガートナー社調べ）。
- わが国でも、2005年6月、フィッシングに対する初めての摘発。今後、フィッシングによる被害の拡大が懸念される。

２　スパイウェア

- わが国では、2005年11月、スパイウェアを使った不正振込事件で逮捕者。セキュリティソフトなどと偽り、スパイウェア添付のCD－ROMを被害者に送付し、インターネットバンキングのパスワードを入手。4金融機関の口座から、合計10件、約1，140万円を不正に振り込んだ疑い。2006年1月にも、スパイウェア作成、銀行口座からの不正振込容疑で摘発。

４　所有物による認証（ワンタイムパスワード方式）

所有物（トークンなど）と組み合わせることにより、毎回異なるパスワードを入力する仕組みとするもの。→　従来のID・パスワード方式が抱える危険性を軽減できる。

タイムスタンプ方式

ユーザにトークン（パスワード生成器）を配布。トークンに表示される番号（時刻の経過に従い変化）をログイン時にパスワードとして入力、送信。

【問題点】

- トークンとサーバで時刻同期を図っておくことが必須。
- 利用者はトークンを厳重に管理しておく必要。

チャレンジレスポンス方式

ユーザからアクセス要求を行った際に、サーバから送られる「チャレンジ」（毎回変わる）に対し、ユーザが計算を行い、解答（レスポンス）をサーバに送信。サーバ側の計算結果と一致した場合にログインできる。

【問題点】

- サーバとユーザでソフトウェアを一致させる必要。
- 「チャレンジ」が簡単だと見破られる可能性。一方、難しい場合はユーザが対応できない可能性。

５　本人の特徴による認証（生体認証方式）

現在は、指紋、網膜、虹彩、顔、声紋、掌形、静脈パターン、DNAなど、個人を識別可能なあらゆる部位・行動が、利用の対象となっている。

端末やOSへのアクセス時に生体情報を利用

端末

メリット

○　何度でも使用可能（認証を行う度にパスワードを取得したり、計算を行うような煩雑さはない。）。
○　ID・パスワード方式と比較した場合、盗難は困難。
○　総当り・類推でヒットしてしまう可能性もない。
○　ID・パスワード方式のように忘却する恐れはない。

デメリット

○　実装コストが高価。
○　体調（病気、ケガ）次第では認証できない可能性。
○　ハンディキャップ等により、サービスを当初から利用できない可能性。
○　インターネットを介したログイン等には、生体情報が流れるリスク。
○　個人の生体情報を管理されることに伴う心理的な抵抗感。
○　身体的特徴は基本的には生涯不変であり、盗難、偽造等された場合に変更困難。

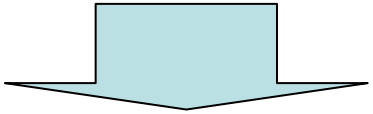
６　公開鍵認証基盤（PKI）の活用

現在、公的個人認証サービスにも用いられているPKIは、公開鍵暗号方式を採用することにより、通信相手の本人性の確認や通信内容の完全性の保障といった認証機能を果たすことが可能な仕組み。

セキュリティ	◆「成りすまし」の防止 パスワード盗難による「成りすまし」の被害について、公開鍵暗号方式を採用するPKIでは、秘密鍵が盗難されない限り「成りすまし」が起きることはありえない。 ◆「改ざん」「送信否認」防止（電子署名） 公開鍵暗号方式の採用により、通信途上でメッセージを書き換えてしまう「改ざん」、送信者の送信内容を否認する「送信否認」も防ぐことが可能。
拡張	◆「所有物による認証」との組合せ 秘密鍵を格納する媒体として、ICカード等の所有物を使用することが可能。 ◆利用用途の拡張性 PKIの技術は、署名、認証、暗号化等多くの用途に利用可能。
問題点	◆秘密鍵の厳重な管理 秘密鍵が盗難されないよう、耐タンパー性（内部解析や改変に対する防護）を保障する媒体（例：ICカード）への格納等を考える必要。 また、仮に格納媒体が盗難に遭っても、ただちに秘密鍵が他者に使用されないよう、PIN（個人用識別番号）の設定等も考慮する必要。 ◆実装コストの高さ PKIの搭載にかかる費用は、ID・パスワード方式と比較した場合高価。また、「所有物による認証」と組み合わせた場合はさらに費用がかかる。

7　公的個人認証サービスでの提供に係る課題①

PKIは署名だけでなく、認証や暗号化（秘匿）など様々な用途への利用が可能な技術であり、公的個人認証サービスの基盤を利用してオンライン認証を提供することは、技術的には問題がない。



オンライン認証機能を公的個人認証サービスに搭載するにあたっては、以下の点に留意が必要。

（1）オンライン認証機能の提供に対する具体的なニーズ
（2）オンライン認証機能を利用するサービスの性格、利用シーン
（3）公的個人認証サービスで提供する意義・必要性
（4）現行の公的個人認証制度との整合性
（5）オンライン認証機能の搭載に要する費用及びその負担

7　公的個人認証サービスでの提供に係る課題②

仮に公的個人認証サービスにおいてオンライン認証を提供することとなった場合、電子証明書の発行形態次第で制度、システム構築、運用のあり方が大きく変わってくるものと考えられる。

公的個人認証サービスが認証用途の電子証明書を発行する形態としては、以下のようなパターンが考えられる。

① 現行の公的個人認証サービスの署名用途の電子証明書を認証用として併用する。【併用型】

② 現行法を改正し、公的個人認証サービスの都道府県認証局から、署名用途の電子証明書とは別に認証用途の電子証明書を発行する。【別発行型】

【検討会　論点整理（本年５月公表）より抜粋】

次回以降、国内外における事例を紹介するとともに、併用型、別発行型のそれぞれの論点を整理していく。

主な論点の整理（案）

２　カードの要件

（カード利用時の本人確認等）

・　社会保障分野の個人情報は、プライバシー保護の必要性が高い情報が含まれ、適正な取扱いの実施を確保する必要があることから、カードを用いて情報を電子的に閲覧する際には、カードの使用者がカードの所有者本人であること等をその必要性に応じて確認する必要があるのではないか。

・　現在オンラインでの行政手続における厳格な本人確認手段として利用されている公的個人認証サービスは、地方公共団体という公的主体が自ら運営し、もっとも高いレベルのセキュリティや信頼性を有するサービスであることから、同サービスの社会保障カード（仮称）への活用を検討するべきではないか。