セコムIS研究所
Intelligent Systems Laboratory

偽造キャッシュカード問題と認証システムの考察

セコム株式会社IS研究所
松本　泰

2005 年 4月 15日

偽造キャッシュカード問題と認証システムの考察

セコム IS 研究所
Intelligent Systems Laboratory

- 「認証とは」
  - 概念、範囲、用語などが専門分野により結構バラバラ
  - これを少し整理する　–> SGの議論で噛み合わなかった点など
- CD/ATMの認証システム
  - キャッシュカードの「認証」の問題をすこし説明
- 金融機関の認証システムに関する考察
  - 「認証の安全性」、「システムのコスト」、「金融取引のリスク評価」、「消費者保護のための補償」、これらを含めて「認証システム」と捉え、バランスよく考えられた「認証システムのベストプラクティス」を考察してみる
  - 「偽造キャッシュカード問題」は現在の「金融機関の認証システム」の問題のひとつ

認証とは
「利用者確認情報」と「認証の3要素」

セコムIS研究所
Intelligent Systems Laboratory

- **利用者確認情報**
  - 検証者が利用者の主張する身元の検証をする際に利用する情報
  - キャッシュカードでは
    - 検証者：金融機関、CD/ATM
  - 利用者：預金者
- **認証の3要素**　－　「利用者確認情報」の3つの要素
  - （1） **利用者の記憶による認証**
    - 暗証番号等による認証
  - （2） **利用者の所持による認証**
    - キャッシュカード
  - （3） **利用者の属性による認証（生体認証）**
    - 指紋、顔、静脈、虹彩、etc…
- **2要素認証、多要素認証**
  - 複数の要素を組み合わせた認証

認証とは
利用者の記憶による認証

セコム IS 研究所
Intelligent Systems Laboratory

- 「利用者確認情報」として利用者のみが記憶している情報を使った認証
  - 暗証番号、パスワード
  - 低コスト（利用者側、システム側）
- ポイント
  - 暗証番号などの管理
  - リテラシー??　　教育、年代（年齢）の違い。
- 現状の問題点
  - 現代社会における覚えきらない暗証番号
    - 金融機関に限らず広く利用されている
    - 覚えきらない暗証番号が、暗証番号の漏洩に
  - 暗証番号の漏洩が気付きにくい

認証とは
利用者の所持による認証

セコム IS 研究所
Intelligent Systems Laboratory

- 「利用者確認情報」として利用者が所持できる媒体を使った認証
  - 家の鍵、通帳とハンコ、キャッシュカード、パスポート、運転免許証、などなど沢山ある。
- ポイント
  - 所持物が、複製（偽造）されにくいこと
  - 発行、失効、再発行のプロセス。
    - 盗難、紛失に対応した失効プロセスが重要
      - 24時間対応受付窓口など
- 現状の問題点
  - IT技術の進化が「所持物」の「複製(偽造)」を**「早い」「安い」「簡単」**にしている。磁気ストライプならば数秒で可能。これが「偽造キャシュカード問題」に。他にもハンコは、ハンコの印影から極めて低価格で押印された偽造書類が可能であり、これが「通帳盗難被害」へつながっている。

認証とは
利用者の属性による認証（生体認証）

セコム IS 研究所
Intelligent Systems Laboratory

- 「利用者確認情報」として利用者の生体に基づくデータ（生体認証情報）を使った認証
  - 利用者の身体的特徴（指紋、静脈、虹彩、etc..）
  - 利用者のくせ(筆跡、etc..)
- ポイント
  - 「利用者確認情報」である「生体認証情報」が漏洩しない
  - Etc・・・..
- 現状の問題点
  - 過去に広く利用されたことが無くまだ問題点が顕著化していない（問題だと思われることは多々あるが認識が低い??）
    - キャッシュカードなら「引き出せない」そのため大きな被害こうむるといったリスクの考えられる
  - **取替えのきかない身体的な特徴**であり、暗証番号における利用者確認情報の変更や、所持物の認証における(カード)失効、そして再発行といったことを行なうことは難しい

認証とは
暗号技術に基づく認証とICカード

セコム IS 研究所
Intelligent Systems Laboratory

- 「鍵」を使った演算による認証と**間接認証**
  - 「利用者確認情報」として「鍵」を使った演算結果を使用する
  - 「利用者確認情報」の検証は、演算結果を検証する
  - 利用者(預金者)は「鍵」を使える人ということになる -> 間接認証
- ICカード
  - 「鍵」を守る仕組みが可能
    - 「鍵」の複製を防ぐ。「鍵」がICカードから外に出ない
    - ICカードが盗難にあった場合を想定した**耐タンパ性**が重要 – スキミングが極めて困難
  - カード保有者は「利用者の記憶による認証」や「生体認証」といった手段で「鍵」を利用可能に -> 間接認証
- 2つの基本的な方式
  - 共通鍵暗号方式と公開鍵暗号方式->全体の設計の中では非常に重要

認証とは
その他の考察事項

セコム IS 研究所
Intelligent Systems Laboratory

- 認証に対する脅威
  - 「利用者確認情報」の漏洩、盗難、複製（偽造）
  - **認証に対する脅威を評価**することが重要
- 双方向の認証
  - 利用者(預金者)にとって**信頼できる相手か「認証」**したい
    - 金融機関の看板
    - 貴重品ロッカー(これは、フィッシングサイトと同じ。。。)
    - フィッシング詐欺のサイト – 本物か区別が付かない
  - ICカード型キャッシュカード
    - カード自体が、カード保有者(預金者)にとって信頼できる相手(CD/ATM)か判断する
    - 磁気ストライプのカードはノンインテリジェンス

CD/ATMの認証システム
磁気ストライプ型キャッシュカード

セコム IS 研究所
Intelligent Systems Laboratory

- 元々は「記憶による認証」「所持による認証」の2要素認証のつもりだった??
  - 簡単なスキミング、容易な偽造
    - 「所持による認証」の原則が成り立たない
- 「記憶による認証」の暗証番号
  - 「記憶による認証」は漏洩に預金者が気づかない。そして届出が遅れる -> これが「偽造キャッシュカード」問題へ
- 発行済みの3億枚の磁気ストライプ型キャッシュカードの問題
  - 現在の「磁気ストライプ型キャッシュカード」を前提とした対策が重要
    - 基本的には、限度額の引き下げか
    - 「磁気ストライプ型キャッシュカード」は「所持による認証」をサポートしていない「**低い保証レベルの認証**」のみを提供するという位置づけ
    - この「低い保証レベルの認証」に応じた限度額とする

CD/ATMの認証システム
ICカード型キャッシュカード

セコムIS研究所
Intelligent Systems Laboratory

- 偽造が極めて困難
  - 「所持による認証」の確立
  - 秘密の「鍵」を取り出せない構造（耐タンパ性）
    - こうした**評価は必要**
- カードと暗証番号の適切な管理が必要
  - カード紛失・盗難時の速やかな届出が重要
- 届出受付の運用
  - 「所持による認証」を支える重要な役割
- ICカード型キャッシュカードへの移行
  - コスト負担の問題
  - 互換性のための磁気ストライプ・ICカード共存の問題
    - どちらの認証を使ったかにより限度額も別々にする
      - それぞれの**認証の保証レベル**に合った限度額へ

CD/ATMの認証システム
生体認証とICキャッシュカードの実装モデル

セコムIS研究所
Intelligent Systems Laboratory

- 金融機関側に「生体認証情報」持つやり方
  - 「生体認証情報」をデータベース化することになる
- Store-On-Card (STOC)モデル
  - カード上に「生体認証情報」、カード外(CD/ATM)で比較検証
  - 電子パスポート(生体認証情報は顔、虹彩、指紋など)
- **Match-on-Card (MOC) モデル**
  - カード上に「生体認証情報」、**カード内で比較検証**
  - 生体認証対応ICキャッシュカードはこれが多い??
  - 金融機関は利用者の生体認証情報を直接持たない

CD/ATMの認証システム
生体認証対応キャッシュカードの課題

セコム IS 研究所
Intelligent Systems Laboratory

- 「生体認証対応キャッシュカード」に対する**セキュリティ基準不在**??
  - 情報セキュリティの常識では**客観的なセキュリティ評価**が必要
    - Match-on-Card (MOC) モデルは「生体認証情報」の漏洩を防ぐ比較的よい仕組みを持っているが、これは、仕組みだけの問題ではない。
- 異なる金融機関のCD/ATMでの利用
  - 生体認証方式の違いだけの問題ではない
  - 相互運用の問題
    - 標準化の困難性
      - 現状では、生体認証対応キャッシュカードの標準はない??
    - 生体認証対応キャッシュカードの技術は、生体認証技術、ICカード技術、暗号技術の組み合わせ

金融機関の認証システムに関する考察
認証における利用者の義務と金融機関の責任

セコムIS研究所
Intelligent Systems Laboratory

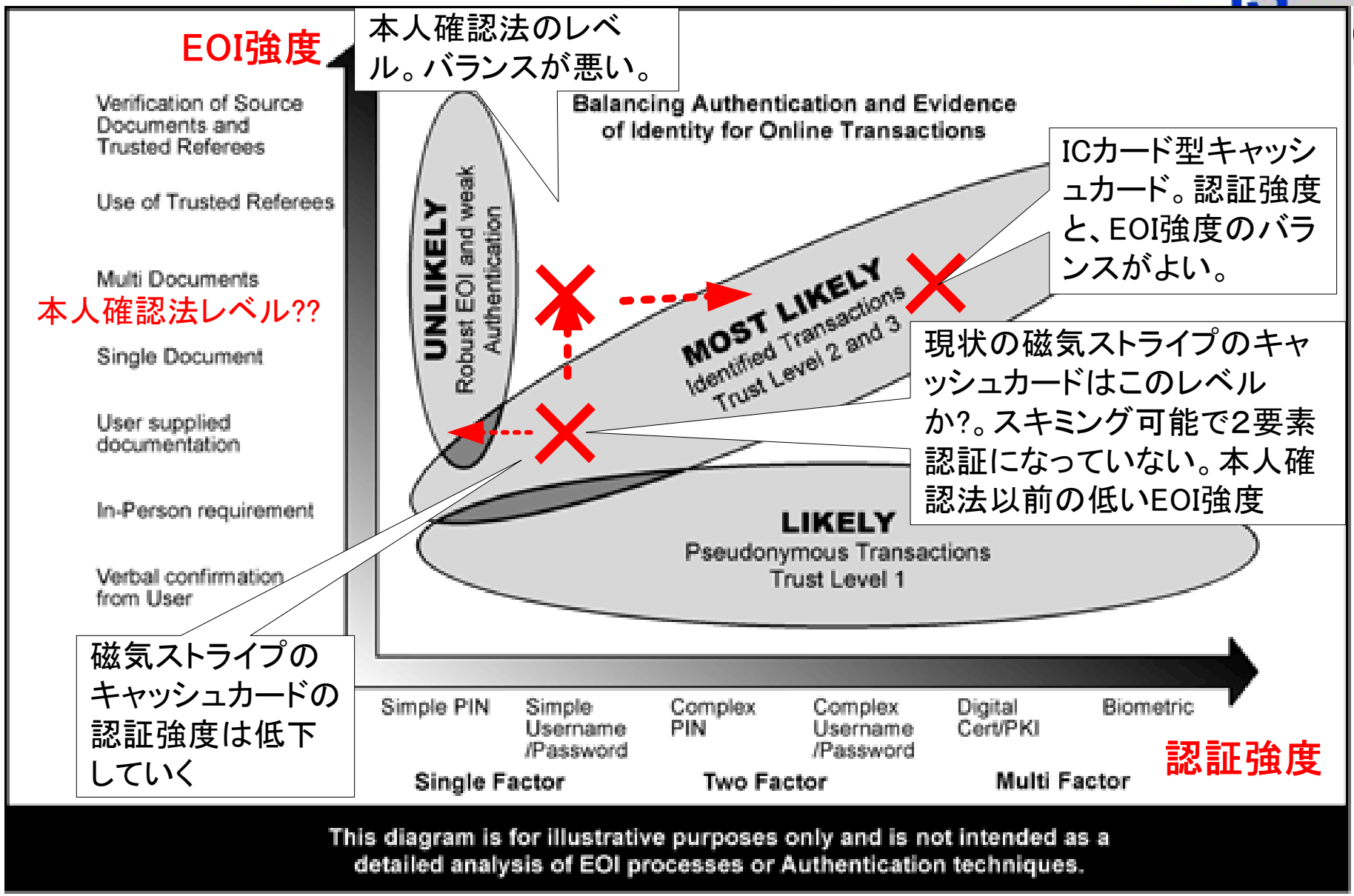
カテゴリ	紛失	盗難	偽造
責任の所在	預金者の責任	預金者の責任とは言い切れない??	金融機関の責任が大きい。
起こり易さ（磁気ストライプ）	預金者の管理次第	預金者の管理次第	スキミングが容易に行なわれる。スキミングを100%防ぐことは困難
起こり易さ（ICカード）	預金者の管理次第	預金者の管理次第	偽造自体が困難。
発覚のタイミング	比較的早い	比較的早い	遅い
悪用のタイミング	比較的遅い	早い	早い。暗証番号の入手方法を隠すために時間をおく場合も考えられる。
暗証番号の漏洩	財布、手帳などに暗証番号を一緒に紛失	巧妙な手口。 財布、手帳など暗証番号を一緒に盗難	巧妙な手口で暗証番号を入手
事件発覚後の預金者の対応	紛失を早期に届ければ被害の可能性は少ない	盗難を早期に届ければ被害を最小減に留められる可能性が高い	発覚のタイミングが比較的遅いため対応は困難であるが早期に届けるべき

金融機関の認証システムに関する考察
本人確認

セコム IS 研究所
Intelligent Systems Laboratory

- 本人確認
  - 「本人」と「利用者確認情報」を結びつける際の「本人確認」
  - 高い信頼には、高い本人確認のレベルも重要。
  - 「低額取引 -> 匿名」=電子マネー。「高額取引 -> 高い本人性」の2極化
- 本人確認法(金融機関等による顧客等の本人確認等に関する法律、2004年1月6日)
  - マネーロンダリング対応。架空口座による詐欺対策??
  - 口座開設時、200万円を超える大口現金取引等 -> MSキャッシュカードではダメも考えられる。。。
- 現状
  - これまでに発行した3億枚キャッシュカードの多くは、本人確認法で要求されるレベルの「本人確認」がされていない??
- 今後の課題
  - 本人確認のための書類の偽造対策
  - 本人確認フレームワーク??の確立?? -
    - そもそも発行機関が汎用的な証明書として認めていない??
  - 証明書の電子化の対応(電子パスポート、ICカード運転免許証)

認証強度と本人確認強度(EOI強度)の関係



Authentication for e-government: Best Practice Framework for Authenticationより
http://www.e-government.govt.nz/docs/authentication-bpf/index.html

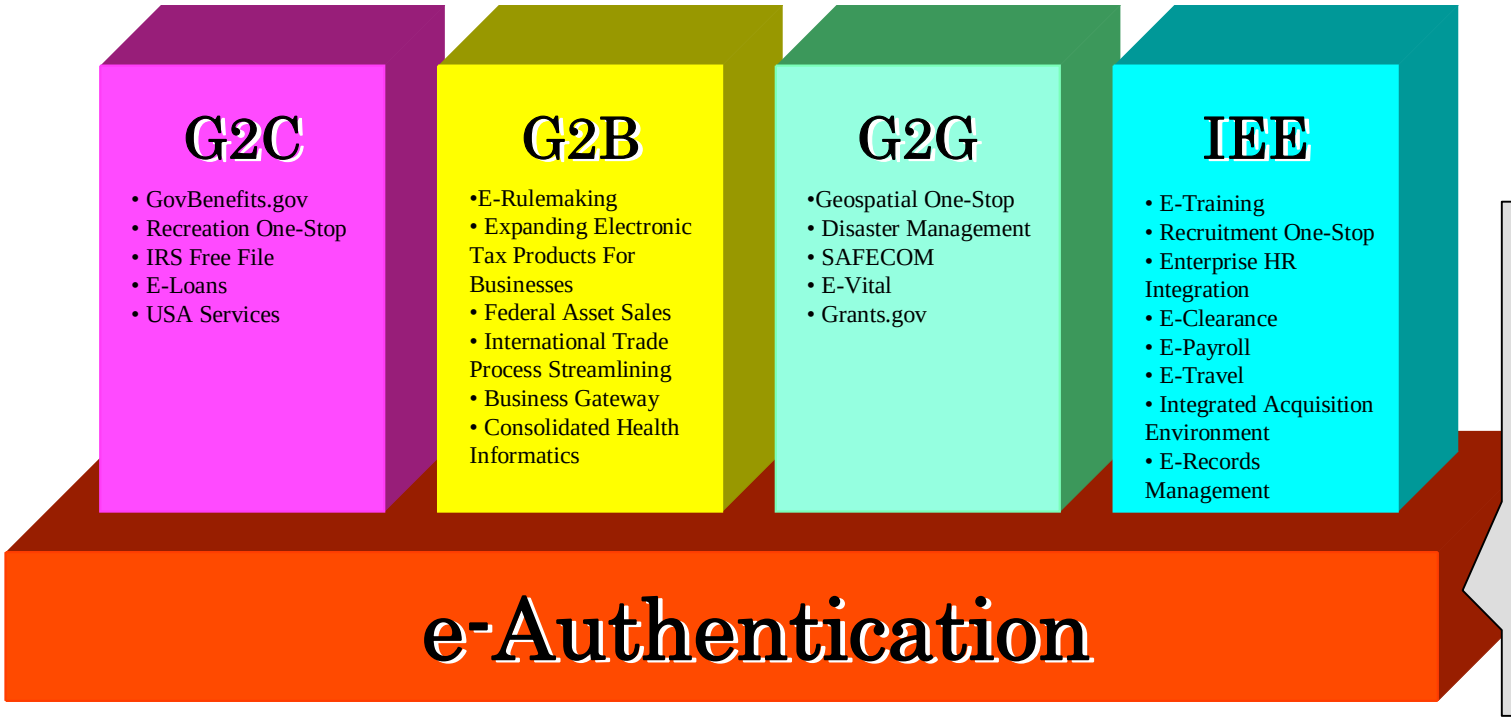
金融機関の認証システムに関する考察
認証のベストプラクティス＆フレームワークの検討

セコムIS研究所
Intelligent Systems Laboratory

- **認証のベストプラクティス** – 最善の選択
  - 磁気ストライプとICカードが並存する現状においてのベストプラクティス
  - ICカードを前提としたベストプラクティス(ToBeモデル)
  - ATM以外の様々な認証を考えたベストプラクティス(ToBeモデル)
    - 銀行窓口取引、デビットカード、オンラインバンキング、電話取引、etc…
- フレームワークの検討範囲
  - 認証の保証レベル(or認証の強度のレベル)
    - 既存のシステムも含め認証システムの保証レベルを評価する。
  - 金融取引のリスク評価
    - 金銭的ロス、機密情報（暗証番号、生体情報）の漏洩、などの観点から
  - 金融取引のリスクに応じた認証の保証レベル
    - 高い限度額の口座は高いリスクを伴う
  - 消費者保護(補償)
    - ベストプラクティスと考えられる認証システムでカバーしきれないところを保険などで補償することを検討する
    - リスクの移転

金融機関の認証システムに関する考察
米国電子政府における電子認証フレームワーク

セコムIS研究所
Intelligent Systems Laboratory



•信頼を提供するための認証システム
•複数の保証レベルの認証
•認証の技術要件
•相互運用性
•Etc…

- 米国電子政府における、政府機関を横断した24のイニシアチブ
  - G2C（政府と市民）、G2B(政府と企業)、G2G(政府機関と政府機関)、IEE（内部効率化）
  - 4つのカテゴリを横断するe-Authenticationイニシアチブ
- これを金融機関に置き換えることを考える。
  - Bank2C（金融機関と預金者）など。
  - 信頼のおける認証システムをベースにした各種の信頼性の高いサービスの提供

まとめ

セコムIS研究所
Intelligent Systems Laboratory

- 金融機関にとって認証は預金者等の顧客に信頼の高いサービスを行うために非常に重要な役割を果たす
  - 「認証システム」の信頼は、「金融機関」への信頼につながる
  - 「偽造キャッシュカード問題」 -> 金融機関の信頼の低下
- 金融機関の認証のベストプラクティスを確立するための「ガイドライン」「フレームワーク」の整備を行うべき
  - CD/ATM、窓口での認証、オンラインバンキング、etc・・・
  - 認証の保証レベル(or認証の強度のレベル)、金融取引のリスク評価、消費者保護(補償)、これらのトータルなガイドライン
  - 金融機関の認証システムのToBeモデルの策定
- EA(エンタープライズアーキテクチャ)による認証システムの再構築
  - レガシーシステムからの脱却??
  - AsIsの調査、ToBeモデルの策定、そして現実的な解へ(認証のベストプラクティス)

金融機関の認証システム全体の問題

偽造キャッシュカード問題

補償問題
- 責任負担
- 補償金を騙し取る可能性
- 預金者による管理努力

セキュリティ対策の多大なコスト
- 預金額や取引内容に応じた対策
- EOIと認証強度のバランス
- ATM回線のセキュリティとのバランス

利便性と認証技術
- 耐タンパ性
- 相互運用性
- 暗証番号の強度

盗難キャッシュカード
盗難通帳への問題

オンラインバンキング等
における犯罪の問題

・・・・等々

- 金融機関の認証のベストプラクティスを確立するための「ガイドライン」「フレームワーク」の整備
  - CD/ATM、窓口での認証、オンラインバンキング、etc・・・
  - 認証の保証レベル(or認証の強度のレベル)、金融取引のリスク評価、消費者保護(補償)、これらのトータルなガイドライン
  - 金融機関の認証システムのToBeモデルの策定
- EA(エンタープライズアーキテクチャ)による認証システムの再構築
  - レガシーシステムからの脱却??
  - AsIsの調査、ToBeモデルの策定、そして現実的な解へ(認証のベストプラクティス)

「認証システム」の信頼は、「金融機関」への信頼につながる

偽造キャッシュカード問題と認証システムの考察

2005 年 4 月 13 日

セコム株式会社 IS 研究所

松本　泰

目次

1　偽造キャッシュカード問題 ..... - 1 -
2　認証とは ..... - 2 -
2.1　認証の概要 ..... - 2 -
2.2　利用者の記憶による認証 ..... - 3 -
2.3　利用者の所持による認証 ..... - 4 -
2.4　生体認証 ..... - 6 -
2.5　暗号技術に基づく認証 ..... - 8 -
2.6　広義の認証と認証の信頼レベル ..... - 9 -
3　CD/ATM における認証 ..... - 12 -
3.1　磁気ストライプ型キャッシュカード ..... - 12 -
3.2　IC カード型キャッシュカード ..... - 12 -
3.3　キャッシュカードと生体認証 ..... - 13 -
3.3.1　生体認証対応キャッシュカード ..... - 13 -
3.3.2　STOC　Store-On-Card ..... - 14 -
3.3.3　MOC　Match-On-Card ..... - 14 -
3.3.4　生体認証対応キャッシュカードの課題 ..... - 15 -
4　金融機関の認証システムに関する考察 ..... - 16 -
4.1　認証における利用者の義務と金融機関の責任 ..... - 16 -
4.2　本人確認 ..... - 18 -
4.3　認証のベストプラクティス ..... - 19 -
4.4　参考例としての海外の電子政府における電子認証 ..... - 20 -
5　まとめ ..... - 23 -
参考文献 ..... - 24 -
1.　米国連邦電子政府の電子認証の動向 ..... - 25 -
2.　電子認証ガイドライン ..... - 26 -
3.　認証における保証レベル ..... - 26 -
4.　認証方法と保証レベル決定プロセス ..... - 28 -
5.　潜在的なインパクトとリスク ..... - 29 -
6.　各保証レベルにおける技術要件 ..... - 30 -

図表番号

表 1　主な生体認証 - 6 -
表 2　キャッシュカード被害の考え方 - 18 -
表 3-1 各保証レベルの定義と説明 - 27 -
表 5-1 潜在的なインパクトと被害 - 29 -
表 5-2 潜在的インパクトのレベルと保証レベルの対応 - 30 -
図 1 EOI と認証の強度の関係 - 11 -
図 1.1　米国電子政府戦略における分類 - 25 -
図 3.1　OMB ガイダンスと NIST ガイドラインの関係性 - 27 -
図 4.1 認証方法と保証レベルの決定プロセス - 28 -

1　偽造キャッシュカード問題

キャッシュカードの偽造による被害が社会的な問題になっている。元来、キャッシュカードによる認証の想定は、後述する「所持による認証」と「記憶による認証」の２要素認証と考えられ、２要素認証は一般的に信頼性の高い認証とされている。しかし「記憶による認証」に関して、キャッシュカードの 4 桁の暗証番号というあまりに少ない情報である。キャッシュカードの「所持による認証」は、もっと深刻な問題を抱えている。つまりスキミングにより簡単に複製が作れてしまう問題である。これまで多くの預金者は、カードさえ盗難にあわなければ安全だと考えていた。本来の「所持による認証」において重要なのは、所持物の複製が作成できないことである。「所持による認証」では、盗難にあう、ないし、紛失したことに気付くことが重要であり、こうした場合、届け出ることによりカードを失効させ、カードを再発行することによりサービスを再開するといった手順を取る。しかし、現在のよく使用されている磁気ストライプ型キャッシュカードは、容易にスキミングが可能で、複製が作れてしまう。これは、預金者にとって所持していれば安心という常識を覆している。

こうしたことから「偽造キャッシュカード問題に関するスタディグループ」(以後「SG」)において偽造キャッシュカードによる被害についての補償問題が主に検討されてきた。しかし、例え補償に関する方策が充実しても、それだけでは犯罪は減らない。また、「制度を悪用して補償金をだまし取る犯罪」の増加にも繋がる可能性も否定できない。こうしたことから、CD/ATM におけるキャッシュカードなどの認証システム自体が、より安全であることが求められている。

偽造キャッシュカード問題が大きくクローズアップされてから、従来からの磁気ストライプ型キャッシュカードが問題だとする指摘の声が強い。そして、IC キャッシュカードや更に生体認証などの導入を促す声もある。公共性の高い業務を行なう金融機関が、セキュリティに対する努力を怠ってきたのではないかという指摘があり、金融機関の責任が問われている。その一方、セキュリティの強化には多くのコストがかかることも十分に念頭におく必要がある。これまでの「ＳＧ」においてもコストという重要なパラメータを無視して議論されてきた面もある。現実にセキュリティに完全はなく、セキュリティに完全を求めるほどに多大なコストがかかる。更に預金者が何の自己管理することなくセキュリティを保てる夢の認証システムもありえない。それでは、実際にどういったセキュリティレベルの認証システムを実現するべきなのか、キャッシュカードなどの認証システムのベストプラクティスとは、いったいどういったものなのか等が認証システムを検討する上で一番重要な点だと考えられる。

偽造キャッシュカードだけではなく、盗難キャッシュカードや盗難通帳の被害の対

応を検討する要望もある。IT 技術の急速な進歩は、印影を元に容易に押印済みの偽造書類の作成することも可能にしてしまい、こうしたことが「盗難通帳の被害」を拡大している。その他にも、金融機関の窓口業務での本人確認に使われる各種の証明書の偽造の問題もある。また、ネットワークにおいてフィッシング等の被害が広がっているが、今後はオンラインバンキング等に関しても更に巧妙な犯罪が行なわれる可能性が高い。こうした問題を考えると、偽造キャッシュカード問題に限らず金融機関の預金者等の顧客に対する認証システム全体の問題として、様々な面から見直す時期に来ているのではないだろうか。

本稿では、以上のことや、「ＳＧ」でのこれまでの議論も踏まえ、キャッシュカード等における認証システムのチュートリアルとして読めることを考慮している。そうした上で最後に、認証システム全体を検討するための認証フレームワークの提案を行なっている。また、本稿は、「ＳＧ」での議論をおおいに参考にして記述しているものの基本的に意見は私見であり、「偽造キャッシュカード問題に関するスタディグループ」及び、筆者の所属・関係する組織の意見ではないことをご了承して頂きたい。

2　認証とは

2.1　認証の概要

認証(Authentication)は、情報セキュリティにおいて最も重要なセキュリティ要件のひとつであるが、その概念は非常に広い。認証は、利用者の真正性の確認といった意味になるが、「偽造キャッシュカード問題」において認証は、CD/ATM における預金者の真正性の確認ということになる。

認証に関連した技術は、非常に幅が広い。様々な認証技術は、独自に発展してきた経緯があるため、それぞれの認証技術に依存した用語等も多い。また、立場等により認証技術の範囲の捉え方や興味の示す分野も大きく異なることが多い。例えば、生体認証技術の研究者にとって認証とは、指紋などのパターンを照合することが認証技術の興味の中心であるかもしれないし、暗号の研究者にとっては、認証で利用される暗号アルゴリズム等が同じく興味の中心かもしれない。

認証技術は、その立場により狭い範囲を示すことが多いが、広義の意味の認証は、認証で利用する利用者確認情報と認証する利用者との結合を行うための利用者確認プロセスの運用までを含めて認証と考えるべきである。偽造キャッシュカード問題においても、キャッシュカードの IC カード化が推進されるべきという意見が多い。しかし、実際には IC カードという技術だけがすべてを解決するものではなく、認証システムは、その運用や補償のフレームワークなども含め検討されるべきであろう。

実際、認証の問題は、個々の認証技術や単体の認証システムだけの問題ではなくな

りつつある。例えば、企業内においても覚えきれないパスワードを強要されるが故、セキュリティが保てなくなるという問題がある。そのため比較的大きな規模のネットワークを抱える企業のイントラネット管理者にとっては、氾濫する認証技術を統合し、シングルサインオンやアイデンティティ管理を実現することまでを含めて認証システムと捉えている。

同様に、様々なカードが利用されている現代社会において、多くの暗証番号やパスワードといったものが使用されている。覚えきれない数の暗証番号を強要される故、同じ暗証番号を再利用し、また、安易なところに暗証番号を記録する。そうすると一番脆弱なところから暗証番号が漏洩する。こうなってくると個々の金融機関だけで解決できる問題ではないといったところもある。個々のカード発行組織は、他の組織などが提供する認証システムのセキュリティの不備から暗証番号が漏洩したことによる補償を行なわなければならないのかと言う問題にも突き当たる。

認証に対して脅威が少なく理論的に利用されるべき認証と、現実的に使用されている認証のギャップも大きい。認証にはより脅威の少ないメカニズムが用いられるべきであるが、実際には、コストとのトレードオフ、過去からの資産の継承や流用といった理由から、脅威の多いと考えられる認証も数多く利用されている。「偽造キャッシュカード問題」における「磁気ストライプ型キャッシュカード」も、こうした例のひとつとして捉えることができる。

以上のように、認証の概念にしても要求にしても様々な見方があるが、ここではまず認証の要素による分類を説明する。認証では、主張された身元（利用者、「偽造キャッシュカード問題」では、預金者）の検証を行うが、この検証を行うための利用者（預金者）確認情報が存在する。利用者確認情報は、一般に以下の３つがある。

(1) 利用者の記憶による認証　（暗証番号等による認証）
(2) 利用者の所持による認証　（キャッシュカードなど）
(3) 利用者の属性による認証　（生体認証）

これらの利用者確認情報を組み合わせた認証は、２要素認証、または、多要素認証と呼ばれ、技術的な観点から、一般的に認証に関する高い強度があると認識されている。

2.2　利用者の記憶による認証

利用者の記憶による認証では、「利用者確認情報」として、利用者のみが記憶している情報を使い認証を行なう。キャッシュカードの場合の利用者確認情報は、暗証番号がこれに当たる。利用者確認情報としての暗証番号の使用は、身元を主張する利用

者のみが知っていることが想定されている。

ネットワークにおける認証において「利用者の記憶」であるパスワードによる認証がよく用いられるが、この場合、ネットワーク盗聴によるパスワードの漏洩の脅威がよく知られている。このため、暗号を伴うプロトコルを利用した上でパスワードによる認証が行われることが多い。しかし、暗号を施すにしても、暗号を行うための鍵と、その管理が必要になることに注意する必要がある。

金融機関の CD/ATM においても専用線のワイヤードタッピングといわれる脅威が指摘されているほか、同じ暗証番号を使用したテレフォンバンキングでの暗証番号が漏洩の可能性の指摘もある。

ネットワークにおける「利用者の記憶による認証」方式全体にいえることであるが、ブルートフォースアタック、パスワード推測攻撃、辞書攻撃といった攻撃から守る方法として、短いパスワード、名前に関連するもの、生年月日、辞書にある単語を避け、長い文字列、大文字/小文字/数字/記号などを含むものとし、できるだけエントロピーの大きなものを使うことが薦められている。

キャッシュカードは、4 桁の暗証番号ということで、短い、更に、数字だけという問題がある。しかしキャッシュカードの利用場面が、一般的なネットワークでの認証とは違いもあり一概に安全ではないとは言い切れないだろう。しかし、4 桁の類推されにくい 4 桁の暗証番号は覚えにくいということはあるかもしれない。

利用者の記憶による認証では、暗証番号等の漏洩を本人が気付かず、被害などにあって初めて気が付く、また、場合によっては、気が付かないまま不正に利用されるといったことも考えられる。

キャッシュカードの暗証番号の漏洩に関して CD/ATM と金融機関間の回線の盗聴の可能性などの指摘もあるが、暗証番号の漏洩の多くは、回線の盗聴以外の原因だと思われる。CD/ATM から後の金融機関のシステムが安全と仮定した場合、暗証番号などの漏洩の脅威として知られているものにネットワークセキュリティ分野で「ソーシャルエンジニアリング」といわれる手口がある。それは、金融機関の人間などになりすまし電話等で暗証番号を聞き出す、肩越しに CD/ATM 画面を覗きキー入力を見る（ショルダハッキング）と言ったいわばローテクな手段であるが、こうした手段の成功率は高いとも言われている。

2.3 利用者の所持による認証

利用者の「所持による認証」では、利用者確認情報として、利用者が所持できる媒体を利用する。この媒体には IC カードなどがあるが、広い意味では、家の鍵、通帳とハンコ、クレジットカード、パスポート、運転免許書なども「所持による認証」の道具と考えてよいであろう。

「所持による認証」において重要なポイントがふたつある。ひとつは、「所持によ

る認証」に利用する所持物が、複製（偽造)されにくいことであり、もうひとつは、所持物の発行、失効、再発行のプロセスである。後者の場合、特に盗難、紛失に対応した失効プロセスが重要である。

「所持による認証」では、紛失や盗難に本人が気づくこと、また、本人の届出に対してその認証に対する効力を失わせるための運用などが重要になる。SG の議論の中でも、キャッシュカードの特に盗難などへの対応としては、24 時間の受付窓口の整備を求める意見があったが、こうしたことは「所持による認証」にとっては重要な意味を持つ。

「所持による認証」ということでは、磁気ストライプ型キャッシュカードも所持による認証のひとつと考えられてきた。しかし、磁気ストライプ型キャッシュカードの場合、磁気記録情報を不正に読み出して複製を容易に作成できてしまうことが、偽造キャッシュカードによる犯罪を生み出した。

磁気ストライプ型キャッシュカードに限らず IT 技術の進化が「所持による認証」で利用する「所持物」の「複製(偽造)」を「早い」「安い」「簡単」にしている。磁気ストライプならば数秒で可能であり、これが偽造キャッシュカード問題になったが、他にもハンコは、ハンコの印影から極めて低価格で押印された偽造書類が可能であり、これが「通帳盗難被害」へつながっている。

「複製(偽造)」を困難にするため「所持による認証」で利用する「所持物」に IC カードなどを使うことが考えられる。

ネットワークにおける認証において、IC カード等の「所持による認証」の媒体では、ネットワークに流す利用者確認情報に暗号技術を用いる「強い認証技術」が利用されている。この暗号技術を用いる強い認証技術を利用する IC カードは、暗号技術的トークン(Cryptographic Token）と呼ばれることもある。こうした暗号技術を用いる強い認証では、ネットワーク上の盗聴等に対抗することができる。

こうした IC カードでは、IC チップに暗号で使用される「鍵」が格納される。その「鍵」を使って IC カード内部において演算結果を利用することにより、カード、ないし、利用者の認証を行なう。IC カード型キャッシュカードでも同様の認証がなされる。

「所持による認証」で使われる IC カードでは、「複製(偽造)」の脅威に対抗するため「強い認証」に利用する「鍵」を保護する機構が盛り込まれている。こうした機構は、耐タンパ性と呼ばれている。

以上のように「所持による認証」に耐えうる機構が盛り込まれた IC カードが存在する。しかし、標準化され大量に配布された IC カードは、ありとあらゆる手段で、その脆弱性が研究されると考えられる。一旦、配布されると回収は非常に困難であり、問題が生じた場合の解決は、極めて困難になる。暗号技術を駆使した IC カードであっても、電力解析、タイミング解析、故障利用解析といった IC カードに対する色々な攻撃方法も存在する。こうしたことから「所持による認証」に使われる IC カード

等についてのセキュリティの評価や認定は非常に重要な意味を持つ。例えば、米国においては、FIPS (Federal Information Processing Standards)140-2 といった暗号製品の信頼性を評価・認定するための米国政府調達基準がある。

2.4 生体認証

生体認証は、利用者確認情報として、利用者の生体に基づくデータ(生体認証情報)により利用者を認証する方法であり、利用者の特性としての指紋、音声、虹彩、顔の形などを識別することにより認証を行なう。表 1 に、生体認証で一般によく使用されるものを示す。

表 1 主な生体認証

種別	生体情報	説明
身体的特徴	指紋	一般に認証精度は高いが、不鮮明指紋の場合等、対応できないケースがある。指紋隆線の特徴点等を用いて認証など、認証方式が数多くあり、また、比較的低コストな入力装置も多い。最も広く普及している。
	虹彩	虹彩の模様を特徴コード化して認証する方式である。 認証精度は最も高い部類であるが、操作性、未対応、高い認証コストが課題となっている。
	顔	顔部品の特徴点、部品配置、輪郭、立体形状等を用いて認証する方式である。入力が簡便で詐称抑止効果が高い。認証精度の向上、耐環境性が課題である。
	静脈	手、指等の血管パターンを特徴コード化して認証する。 比較的新しい生体情報であり、精度等はまだ未知数な面がある。
行動的特徴	音声	音声波形を分析し、特徴コード化して認証する。操作性が高く、電話での認証等において優位性がある。個別暗証番号の割り当てにより音声だけで 1 対 1 認証が可能であるが、雑音等の耐環境性が課題となっている。
	署名	署名の字体、署名時の書き順・筆圧等の動的特徴を用いて認証する。操作は簡単だが模倣される可能性がある。日本ではあまり使われていないが、欧米での利用実績は高い。

身体的特徴は、まさにそれが利用者の証そのものであり、常に自分の肉体に付随している。また、行動的特徴は、いわば利用者の癖であり、利用者であれば、いつどこ

でも再現が可能なものである。従って、生体認証では、暗証番号などの記憶に基づく認証における「忘れる」、「他人に知られる」といった問題や、カードなどの所持に基づく認証における「紛失」、「盗難」、「置き忘れ」の問題を回避できると一般的に言われている。しかし生体情報はアナログな性質を持ち、他人を利用者と誤認する危険性を排除できない。また利用者であるのに利用者でないと認識してしまう問題もはらんでいる。

生体認証では、登録と認証という二つのステップが必要となる。登録では、まず生体情報が入力され、それに対して特徴量抽出処理が施される。これにより個人を識別する「登録用生体認証情報」が生成され、これを利用者の属性と共に保存する。

認証では登録時と同様、入力された生体情報から「認証用生体認証情報」が生成される。これと、あらかじめ登録されている登録用生体認証情報とを照合し、類似度を算出する。この類似度を閾値判定することにより、認証用生体認証情報と登録用生体認証情報との一致／不一致が判定される。一致と判定された場合、生体情報の入力者はこの登録用生体認証情報の属性に基づく利用者であると認証される。

生体認証では、認証用生体認証情報が申告された利用者の登録用生体認証情報と一致するかどうかを確認する方式（1 対 1 認証）と、認証用生体認証情報と一致する利用者の登録生体認証情報を順次照合することにより見つけ出す方式（1 対 N 認証）とがある。現在、金融機関のキャッシュカードで利用されている、また検討されているものの多くは、利用者の登録用生体認証情報と一致するかどうかを確認する方式（1 対 1 認証）である。

生体認証における類似度は、登録用生体認証情報と認証用生体認証情報をパターン照合して算出し、両者が似ているほど大きな値となる 。本人同士の場合でも、異なるタイミングで入力した生体情報は様々な変動要因を含むため、特徴量抽出処理を経て生成される生体認証情報が完全に一致することはない。したがって、本人同士の類似度であっても、その分布は本人と他人の類似度分布と同様に広がりを持つ。

登録用生体認証情報と認証用生体認証情報の一致／不一致は、両者の類似度とあらかじめ実験的に設定された閾値との大小関係によって判定される。この閾値より類似度が大きい場合は比較した生体認証情報が一致したと判定し、そうでない場合は不一致と判定する。生体認証では、利用者の記憶や所持に基づく認証方式とは異なり、このような統計的判定基準が用いられていることが特徴である。

生体認証の精度は、ふたつの認証のエラーの率によって表現されることが多い。ひとつは他人を本人として認証してしまう他人受け入れ率(FAR：False Acceptance Rate)であり、もうひとつは、本人を本人でないとして認証してしまう本人拒否率(FRR : False Rejection Rate）である。これらは、閾値の設定によっても変化するが、認証に対するセキュリティ要件や利便性などの要件により使い分けることになる。

生体認証の精度の客観的な評価は、かなり難しい問題である。静脈などの比較的新しい生体認証方式ほど、客観的な評価がなされていないのが現状である。また、同じ

く新しい生体認証方式ほど、生体情報の経年変化などの基礎的なデータが不足していると思われる。

生体認証では、「未対応」と称される認証に適応できない人が存在することにも注意が必要である。生体認証に関しては、こうした点も考慮に入れて今後検討していく必要がある。

生体認証自体の脆弱性の問題もある。指紋認証においては、安価なグミから作成した人工指によりなりすましが可能となった事例が報告されており、それぞれの方式における生体認証特有の脆弱性の研究の重要性も徐々に認識されつつある。

ネットワークにおけるリモート認証に生体認証を使う場合、生体認証特有の様々な課題があるが、ここでは説明しない。

CD/ATM 等で生体認証を利用する場合、むしろ運用的な側面に近いところでの課題が多い。運用的な側面において、「利用者の記憶による認証」では、暗証番号などの漏洩に関連した脅威を低減するために、暗証番号等の変更などの運用でカバーすることも行なわれる。また、「所持による認証」では、その所持物を紛失や盗難した場合、紛失したその所持物の失効処理を行い再発行するといった手続きが行われる。しかし、生体認証の場合、利用者確認情報である生体認証情報自体が、取替えのきかない身体的な特徴であり、利用者の記憶による認証おける暗証番号の変更や、所持物の認証における失効、そして再発行といったことを行なうことは難しい。

以上のようなことも含め生体認証を大規模に展開するための最大の難関は、プライバシー問題であろう。利用者確認情報である生体認証情報自体が究極の個人情報ではないかといったことも指摘されており、その保護も重要な要件として認識されつつある。

生体認証に関しては、究極の認証という意見と、生体認証の漏洩などが危険だとするかなり極端な賛否両論の意見がある。生体認証は、「記憶による認証」や「所持による認証」に比べ、これまで非常に限定した場所での利用形態が多く、また、過去に広く利用されたことがないため問題点が顕著化していないということは言えるだろう。そのため、問題だと思われることは多々あるが、その問題に対するインパクトの評価が賛否両論とも非常に主観的に語られている面がある。

2.5 暗号技術に基づく認証

これまで説明したとおり、認証に使う利用者確認情報として、利用者の記憶、所持物、属性 （生体認証）が利用される。しかし、ネットワークにおけるリモート認証においてより強固な認証が求められる場合、これらの利用者確認情報が、そのままネットワーク上を流れることは少ない。

同様に、CD/ATM における IC カード型キャッシュカードでは、IC カードに内蔵された「鍵」を使った認証が利用される。強い認証技術で利用される暗号技術には、

暗号のための「鍵」が使用される。多くの場合、利用者の記憶、所持物、属性 （生体認証）などを使ったローカルな認証を使ってこの「鍵」を活性化させる。この鍵を使った暗号の演算で生成したトークン（利用者確認情報）を、ネットワークを介して相手のサーバなどに送信することにより認証を行なう。

暗号を用いた認証技術の基本概念は ISO／IEC9798 エンティティ認証(JIS X 5056)等の標準仕様にまとめられている。暗号を用いた認証技術は、対称鍵（共通鍵）暗号を用いる機構や、公開鍵暗号の署名を用いる機構などに分類されるが、いずれの場合でも「鍵」の管理が重要になる。

一般に公開鍵暗号方式より対称鍵暗号方式の方が効率は良いが、対称鍵暗号方式は利用者(利用者が保持する IC カードやＰＣ)とサービス(CD/ATM やオンラインバンキングのサーバ)で秘密の対称鍵を共有する必要があり鍵の管理が問題となる。公開鍵暗号方式はサービス側に利用者の秘密を持つ必要が無くサービスの安全性が向上する。

2.6 広義の認証と認証の信頼レベル

利用者確認情報による利用者の真正性の確認が出来たとしても、利用者確認情報自体に信憑性がなければ、信頼性の高い認証とは言えないかもしれない。そのため「本人」と「利用者確認情報」を結びつける際の本人確認までを含めて「認証」として捉えるといった考え方がある。

ニュージーランド電子政府の「認証のためのベストプラクティス・フレームワーク 」では、認証の信頼レベルは、認証の３つのコンポーネントの強度により決まるとしている。表 2 に認証の３つのコンポーネントの強度を説明する。

表 2 ３つの認証コンポーネント

コンポーネント	「認証のためのベストプラクティス・フレームワーク 」の説明	説明補足
身元証明(Evidence of Identity) 強度	EOI 強度とは、省庁がユーザから提供された全ての身元情報に求める信頼度である。例えば、第三者からの詳細確認とそのユーザのパスポートを、その人の名前と住所が記載された公共料金と比較したようなもの。	どういった書類（パスポート、運転免許書、etc)で本人確認を行なったかということによる強度。例えば、パスポートの発行時の EOI 強度は比較的高い。パスポートによる本人確認は、その EOI 強度よりも低い。

認証強度	認証強度とは、ある認証方法の使用を通じて示された信頼度のことである。例えば、単独に付けられた単純な 4 桁の PIN は、デジタル証明書または複雑なユーザ ID/パスワードの組み合わせと比べると、認証強度が低い。	単要素認証、２要素認証、それぞれの認証技術要件
トランザクション強度	トランザクション強度とは、省庁があるオンライントランザクションに求める信頼度のことである。例えば、低強度トランザクションは、電子メールであるサービス要請の受理確認通知だけ求めるかもしれない。高強度オンライントランザクションは、あるトランザクションの否認防止要因を多く必要とするかもしれない。例えば、誰が依頼をしたかという証拠、メッセージの送信、受信証明、メッセージが改ざんされていない、安全に保存可能などである。	高いトランザクション強度とは、例えば、「実印登録された印鑑で押印された取引書類」、電子署名がなされた「契約書」etc..など。これは、金融機関の立証責任とも関係が深い。

図 1 は、ニュージーランド電子政府の「認証のためのベストプラクティス・フレームワーク 」における EOI 強度と認証強度に基づく認証の信頼レベルの考え方を示している。縦軸が EOI 強度であり、横軸が認証強度になっている。ここでは、EOI 強度と認証強度の双方が高いものが信頼レベルも高い（Trust Level3）としている。認証強度が高くても EOI 強度が低い、すなわち本人確認のレベルが低いものは、信頼レベルも低い(Trust Level 1)とされている。

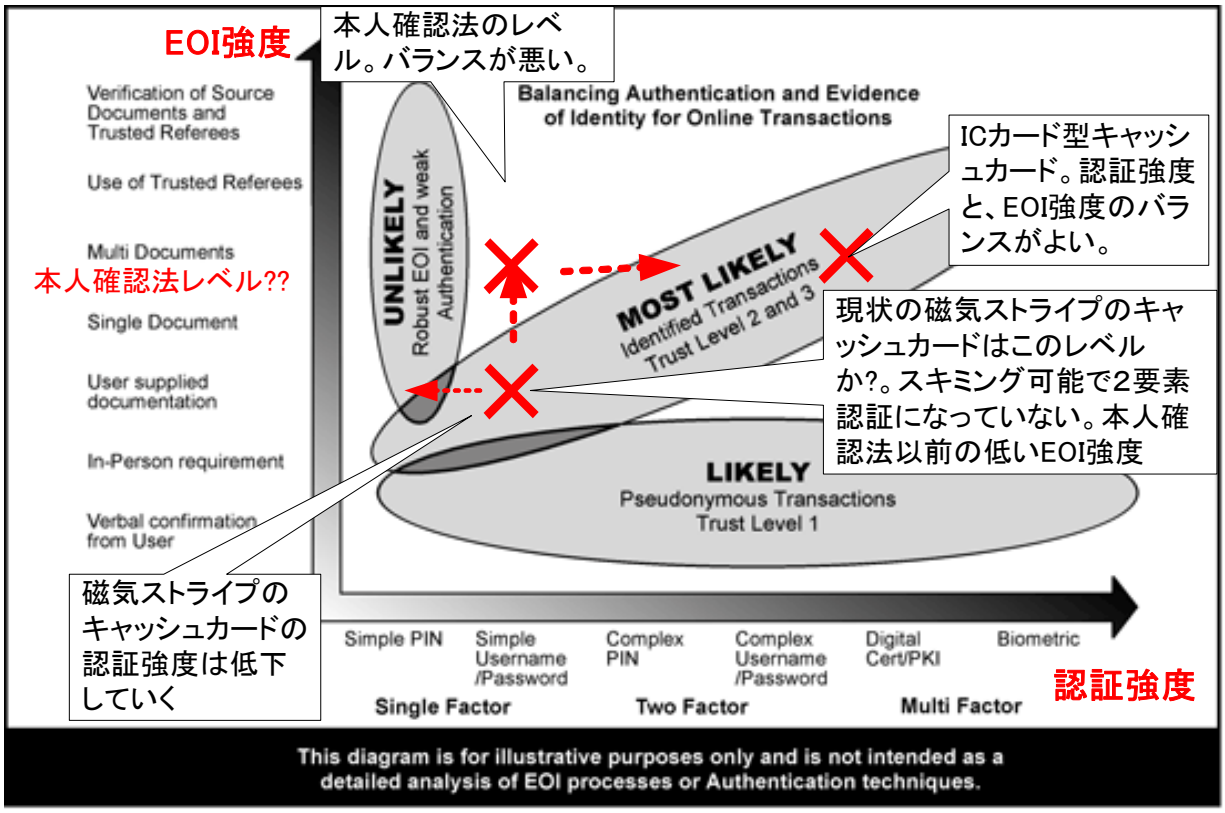


図 1 EOI 強度と認証強度の関係

金融機関は、過去においてあまり厳密な本人確認を行なってこなかったと考えられる。しかし、近年においては、マネーロンダリングや、詐欺に利用される架空口座対策として比較的厳格な本人確認を行なう方向へ向かっており、後述する「本人確認法」の施行にともない口座開設時の本人確認がより厳密になった。

現在の磁気ストライプ型キャッシュカードの場合、容易にスキミング可能であり「認証強度」は、それほど高くないと考えられる。ただし、この図は、電子政府におけるリモート認証の評価が主目的であると考えられるため CD/ATM 等の監視カメラがある環境等のことは考慮されていない。

ここで、仮に本人確認法以前に発行された「磁気ストライプ型キャッシュカード」の「認証強度」と「EOI 強度」が図の「×」の位置にあったとする。「磁気ストライプ型キャッシュカード」は、年代と共に左にシフトして行く。厳密な本人確認を行なうと上にシフトする。しかし、この図の解釈によると「磁気ストライプ型キャッシュカード」のまま、高い本人確認を行なっても信頼レベルは上がらず、バランスの悪い認証システムとなってしまう。

これは、ニュージーランド電子政府の話しであって、日本の金融機関における認証の話しではない。しかし、日本の金融機関における認証システムを考えるにおいても、本人確認のレベル(EOI 強度)と認証強度のバランスを考慮していく必要があるだろう。

3　CD/ATM における認証

3.1　磁気ストライプ型キャッシュカード

現状のキャッシュカードの多くは、「磁気ストライプ型キャッシュカード」が利用されている。「磁気ストライプ型キャッシュカード」のシステム的な問題は、簡単にスキミングされてしまい、容易に偽造が出来てしまうことにある。このスキミングは、キャッシュカードの管理の不備が引き起こす問題でもあるが、キャッシュカードが色々な場面で利用されることが考えられるほどに防ぐことは難しい。例えば、デビットカードは様々な場所で利用されることが実際に想定されている。

このように「磁気ストライプ型キャッシュカード」は本質的な問題を抱えている。「偽造キャッシュカード問題」の対応として IC カード型キャッシュカードへの移行が促進されると考えられる。しかし IC カード型キャッシュカードに置き換えるためのコストの問題もあり、現在発行されている 3 億枚とも言われている「磁気ストライプ型キャッシュカード」が、それほど簡単に移行するとも考えられない。こうしたことから、現在の「磁気ストライプ型キャッシュカード」を前提とした対策が非常に重要な意味を持つ。

キャッシュカードの場合、たとえカードが偽造されたとしても、暗証番号が漏洩されなければ被害に合う可能性は低い。スキミングが防げないと仮定すると、後は、暗証番号の管理が問題になる。暗証番号、すなわち記憶による認証の問題は、暗証番号の漏洩を利用者が気付かず、そのため届け出が遅れることにある。

3.2　IC カード型キャッシュカード

磁気ストライプ型キャッシュカードは、容易にスキミングされ偽造が可能なため、預金者が所持して管理しているつもりなのに、無権限者による犯罪が行なわれるといったことがおきる。これが「偽造キャッシュカード問題」であり、IC カード型キャッシュカードは、こうした問題を解決することになる。

IC カード型キャッシュカードを進める根拠は、偽造が極めて困難ということに尽きる。このことにより「所持による認証」を確立することになり、これは非常に重要な意味を持つ。一方、これは盗難、紛失に関しては、IC カード化の恩恵は比較的薄いということも意味する。

IC カード型キャッシュカードでは、内部に「秘密の鍵」を持っている。この鍵を使って IC カード内部において演算を行ない、その演算結果を検証することによりカードの認証を行なう。この「秘密の鍵」を取り出せない構造になっていることや、「演

算」が破られない、すなわち演算結果から「秘密の鍵」を類推するが困難であることが重要になる。このふたつが何らかの方法で担保されていることが望ましい。

偽造が不可能、ないし、極めて困難であるという仮定の元に２要素認証が確立したことになる。IC カード型キャッシュカードであっても、カードと暗証番号の適切な管理が重要であり、カードが盗難、紛失した場合は、速やかに届けて口座を凍結することが肝要である。

「所持による認証」は、この届出が重要な意味を持つ。従って、この届出を受け付ける運用も非常に重要な意味を持つ。磁気ストライプ型キャッシュカードの偽造では、「所持による認証」の原則が成り立たず、この届出の意味を非常に曖昧にしてしまったところがある。しかし、今後の IC カード型キャッシュカードの普及も踏まえ、預金者がカードの管理を行い、そして、盗難、紛失時には速やかに届けることが重要で、それを約款上でも明記すべきである。

3.3 キャッシュカードと生体認証

3.3.1 生体認証対応キャッシュカード

生体認証をサポートしたキャッシュカードが利用されつつある。現在のところ、生体認証は、生体認証情報が格納された IC カード型キャッシュカードとの組み合わせで利用されていることが多いと考えられる。暗証番号などの記憶による認証では、暗証番号忘れのような問題があるが、生体認証のような身体的特徴を利用した認証では、この暗証番号忘れの問題を回避することができるといった利便性の向上もはかれる可能性がある。

生体認証と IC カードを組み合わせて使う場合、IC カードは、携帯できる生体認証情報のセキュアな格納媒体として役割がある。IC カードは、携帯性のある情報のセキュアな格納場所として発達してきた。

IC カード型キャッシュカードは、外部からの攻撃から内部の情報を守る耐タンパ性を有しているが、認証に利用する「鍵」を安全に格納する同じように、生体認証に使用する生体認証情報を IC カードに安全に格納する。

IC カードに生体認証で使う「生体認証情報」を格納して認証に利用するモデルには、後述する STOC(Store-On-Card)、MOC(Match-On-Card)のふたつの実装モデルがある。

そして、これらの実装モデルを実現するためには、IC カードの高機能化が欠かせない要因となっている。特に MOC(Match-On-Card)のモデルでは IC カード上で複雑なロジックを実行することを要求される。

所持による認証では、所持しているカードなどが盗難などにあった場合の危険性があるが、盗難にあったことをカード保有者が認知できれば、カードの失効、そして再

発行で対処することができる。

こうした耐タンパ性を持った IC カードのようなデバイスは、生体認証においても重要な意味を持つ。すなわち、生体認証情報が格納された IC カードが盗難にあった場合、個人の重要なプライバシー情報である生体認証情報が複製されるリスクを回避することができる。

どこに生体認証情報を保存し、どこで照合処理を行うかといったことは、認証の考え方への要求により異なる。

3.3.2 STOC　Store-On-Card

Store-On-Card (STOC)では、カード上に生体認証情報を格納し、カード外で照合などを行う。実際の照合をカード外のどこで行うかといったことにより、更に色々な実装モデルがある。

生体認証情報がカード外に出ることもあり、カードに格納されている生体認証情報が改ざんされていないかなどを検証するため、生体認証情報の電子署名などが重要になる場合が多い。ICAO(国際民間航空機関 International Civil Aviation Organization ）で検討されている電子パスポートは、生体認証情報を IC カードに格納するが、STOC として実装されている。

STOC では生体認証情報が IC カードから出るため、この生体認証情報の保護が重要な課題になる。生体認証情報の保護は認証のなりすましを防ぐことと共に、カード保有者のプライバシーを守るという二つの重要な側面がある。カード保有者が STOC のカードを利用する場合、カード保有者にとって信頼できる環境で使用されるべきである。一般的な環境においては、カードとカードを利用する装置やソフトウェア間において相互認証などを行い、信頼のおけるパスで暗号化なども行って生体認証情報などの受け渡しを行うことなどが要求される。

STOC の実装は、セキュアな携帯デバイスとして IC カードの機能は要求されるものの、比較的安価な、既存のセキュアなファイルシステム OS カードの IC カード製品を用いて実現が可能である。

非接触型 IC カードを使用し STOC で実現したフィジカルセキュリティに対応した製品も販売されている。こうした製品では、非接触型 IC カード上の生体認証情報を格納し生体認証を実現している。

3.3.3 MOC　Match-On-Card

Match-on-Card (MOC)では生体認証情報が IC カード上に格納され、更に、照合処理等も IC カード上で行う。IC カード上で照合を行うため、生体認証情報が IC カードから出ない仕組みが可能になる。これは、IC カードを紛失した場合などにおいても基本的に重要な情報が IC カード外に出ず、IC カード保有者のプライバシーを守る

ことや、生体認証情報が盗聴されることによるなりすましの危険性を防ぐといったことにおいても重要な意味を持つ。認証などの目的で利用される IC カードは、一般的に耐タンパを有しているものが使用され、物理的な攻撃なども含めカードの複製を防ぐメカニズムを有している。

以上ことから、MOC による生体認証は、かなり理想に近い認証を提供できる可能性がある。ただし現在のところこれは可能性であって、生体認証情報を守るための客観的な評価が行なわれている訳ではない。

MOC は、IC カード上での処理が多く、生体認証が要求する生体認証情報のサイズやその照合に要する演算スピードや、メモリの容量が要求される。

MOC を実装した製品は、その将来性から既に多くの製品が開発されている。しかし、IC カード技術の標準と生体認証技術の標準は、これまで、全く個別に行われてきた過去もあり、十分な相互運用性や柔軟なシステム構成をとることが可能とは言いがたい面がある。IC カードの演算スピードなどの制約から、生体認証としての精度が上げられないのではないかという意見もある。

3.3.4 生体認証対応キャッシュカードの課題

認証に使われる生体認証情報も、重要な個人情報だという考えが欧米でも一般的になりつつある。このためセンターなどで生体認証情報を集中管理することは、法律などにより禁止、又は、大きな運用上の制約が課せられるといった傾向がある。日本においても 2005 年 4 月 1 日個人情報保護法が施行されたが、金融庁でも個人情報保護法に対応した「金融分野における個人情報の保護に関するガイドライン」が公表されており、その中で「生体認証情報」をセンシティブ情報として扱うことが要求されている。

暗証番号による認証では、暗証番号の漏洩は預貯金の金銭的な被害につながる可能性がある。しかしながら生体認証に利用される「生体認証情報」の漏洩は、「生体認証情報」が取替えのきかない身体的な特徴であることから、漏洩した場合は、金銭的被害以上の問題になる可能性をはらんでいる。

暗証番号の漏洩を防ぐため、ＳＧの中間取りまとめにおいて「暗証番号と同じ番号を金融機関以外の第三者との取引で使用していた場合」が預金者の過失となる可能性を示唆している。同じ論理で生体認証を当てはめると「生体認証を金融機関以外の第三者との取引で使用していた場合」預金者の過失となる可能性があるとなってしまう。実際こうしたことが十分検討されているわけではないが、暗証番号の漏洩と、「生体認証情報」の漏洩の違い、すなわち「生体認証情報」が取替えのきかない身体的な特徴であることの意味が十分に理解されるべきであろう。

生体認証対応キャッシュカードの導入に関連して、異なる金融機関が異なる方式の生体認証を採用しており、CD/ATM における相互利用の問題が指摘されている。相

互運用の問題は「異なる方式の生体認証」だけではないことも認識されるべきである。

現状では、生体認証対応キャッシュカード自体の標準化がなされている訳ではない。SG の中での全銀協殿の見解においても「生体認証については、各銀行が先行者リスクを負いながら導入を進めており、創意工夫を凝らし切磋琢磨することで、使い勝手や安全性が向上していくもの」とされている。生体認証自体、標準化が非常に難しく、また、標準化もされていないものが、各行が個別に対応した後で容易に相互運用できるものではないことが認識されるべきである。

生体認証対応キャッシュカードの技術は、生体認証技術、IC カード技術、暗号技術を組み合わせたものであり、非常に高度な相互運用技術が必要になる。安易な標準化や相互運用は、認証システム全体の脆弱性を生みかねないことにも注意すべきである。

4　金融機関の認証システムに関する考察

4.1　　認証における利用者の義務と金融機関の責任

キャッシュカードの偽造による被害が社会的な問題になるほどに、金融機関に対しての対応が強く求められてきた。こうしたこともあり補償に関連して「偽造キャッシュカード問題に関するスタディグループ」の中間取りまとめにおいても、３つの大きな原則が述べられている。

○ 偽造キャッシュカードが使用されたことによる損害は、原則として金融機関が負担。
○ 但し、預金者の責に帰すべき重大な事由がある場合には、預金者が負担。
○ 預金者の帰責事由については、金融機関に立証責任。

補償の考えかたが示されたことは大きな進歩である。こうした補償を前提にキャッシュカードの認証のあり方について検討する必要がある。補償を行なうだけでは、犯罪が減る方向に向かう訳ではなく、根本的な問題が解決されたわけではない。上記の原則により金融機関の責任がより大きくなり、金融機関によりセキュアな認証システムの提供が望まれるところであるが、現実的に、預金者が何の管理に対する義務を果たさずともセキュリティを保てる夢の認証システムはあり得ない。補償を行なうことは、預金者がカード管理や暗証番号の管理を軽視する方向に向かうモラルハザードを生む可能性も指摘されている。金融機関が正当な理由で預金者の帰責事由についての立証ができる認証システムがあるべきであるが、現実的な問題として、現在の磁気ス

トライプ型キャッシュカードにおいても犯罪を防ぐことも重要な課題である。

犯罪を防ぐという観点から預金者の暗証番号の管理はやはり重要であるが、ＳＧの議論でも、暗証番号の預金者の管理についての議論は尽きることが無かった。暗証番号の管理を預金者に求めることは当然としても、求めることに対して現実に預金者の過失とすることはかなり無理がある。現実的には、類推できない暗証番号を数多く覚えることは困難であり氾濫するカードとその暗証番号の問題は、必ずしも個々の金融機関の問題でもないし、また、金融業界だけの問題でもない。

ゴルフ場を舞台として起きた偽造キャッシュカードの事件では、貴重品ロッカーからの暗証番号から漏洩している。こうしたこともありＳＧの中間取りまとめでも「周辺事情を総合的に勘案して、重過失を認定する際の一要素となりうる」例として「暗証番号と同じ番号を金融機関以外の第三者との取引で使用していた場合」をあげている。つまり「金融機関以外」での暗証番号の使用は危ないと言っているに等しい。実際には、CD/ATM と金融機関間から「暗証番号」が漏洩した事件は過去には存在するし、現状でも金融機関側のシステムの不備による暗証番号の漏洩の可能性を完全には否定しきれない。このような「記憶による認証」の立証責任も含め曖昧さ故、「所持による認証」を確立する必要があると考えられる。

預金者にとって何が信頼できるかといったことは非常に難しい問題をはらんでいる。実際「偽造キャッシュカード問題」は金融機関の信頼を揺るがしており預金者は金融機関を 100%信頼するには問題があると考えるようになってきている。ネットワークにおいてフィッシング詐欺といわれる手口が横行しているが、これは例えば信頼できる銀行になりすました Web サイトが暗証番号を要求するといったことが行なわれる可能性がある。ネットワークにおいては、金融機関が預金者と認証すると同時に、預金者が金融機関を認証できる必要がある。

欧州の国では、偽造キャッシュカードは 100%金融機関の補償としている例が多いと報告されているが、これは、偽造防止が進んでいる為でもあると考えられる。金融機関が 100%補償というのは、実際に偽造キャッシュカード被害が起きているからではなく、偽造キャッシュカードを防ぐ努力を金融機関に促していると考えられる。

認証のセキュリティは、必ずしも技術だけの問題ではなく、リテラシーの問題でもある。政府が e-Japan 戦略にあるような、IT 社会への道を推し進めるならば、「認証」は金融機関だけの問題ではないと考えられる。「認証」に対するリテラシー問題も解決の道を探る必要がある。

表 3 に以上の考察や SG での議論を踏まえ、キャッシュカード被害の考え方を筆者の私見としてまとめている。

表 3　キャッシュカード被害の考え方

カテゴリ	紛失	盗難	偽造
責任の所在	預金者の責任	預金者の責任とは言い切れない	金融機関の責任が大きい。
起こり易さ(磁気ストライプ)	預金者の管理次第	預金者の管理次第	スキミングが容易に行なわれる。スキミングを100%防ぐことは困難
起こり易さ(IC カード)	預金者の管理次第	預金者の管理次第	偽造自体が困難。
発覚のタイミング	比較的早い	比較的早い	遅い
悪用のタイミング	比較的遅い	早い	早い。 暗証番号の入手方法を隠すために時間をおく場合も考えられる。
暗証番号の漏洩	財布、手帳などに暗証番号を一緒に紛失	巧妙な手口。 財布、手帳など暗証番号を一緒に盗難	巧妙な手口で暗証番号を入手
事件発覚後の預金者の対応	紛失を早期に届ければ被害の可能性は少ない	盗難を早期に届ければ被害を最小限に留められる可能性が高い	発覚のタイミングが比較的遅いため対応は困難であるが早期に届けるべき

4.2　本人確認

広義な認証は、キャッシュカードの発行時の本人確認も含むと考えられる。本人確認に関しては、2004 年 1 月 6 日に、金融機関等による顧客等の本人確認等に関する法律(本人確認法)及びその政省令が施行されている。本人確認法は、マネーロンダリング防止などを目的とした法律であるが、架空請求詐欺に使われる架空口座対策などにも有効な法律だと考えられる。

本人確認法では、金融機関等に顧客が預貯金口座の開設等の取引を行う際に顧客の氏名・住居・生年月日等（法人の場合は名称・本店等の所在地等）を確認すること、その確認の記録を作成し保存すること、取引の記録を作成し保存することが義務付けられている。

本人確認法では、本人確認の場面として口座開設だけでなく、現金等による 200 万円を超える取引なども想定されている。「現金等による 200 万円を超える取引」にあ

る 200 万円は、通帳と印影による確認による認証の「限度額」とも受け取れる。

本人確認資料としては、運転免許証、パスポート、各種健康保険証などがある。パスポート、運転免許証は、IC カード化が計画されている（パスポートの形状は IC カードタイプではない）が、これらの計画の大きな理由は、それぞれの偽造問題である。つまり現状においては、偽造の可能性があるものを元に本人確認を行なっているとも考えられる。運転免許証や、健康保険証などは、発行元の省庁においては、汎用的な身分証明書としては認めていないという矛盾もある。

パスポート、運転免許証以外の証明書も、今後、IC カード等の電子化がなされていくと思われるが、こうした電子化に対応できるかという問題もある。

4.3 認証のベストプラクティス

キャッシュカードの IC カード化は、欧州においてはロードマップが示され進展しているが、米国においては進んでいないとされている。偽造キャッシュカード問題で、時代遅れのセキュリティのままで、偽造対策を怠ってきたという批判もあるが、実際には、磁気ストライプのカードは、キャッシュカードに限らず幅広く使用されている。

問題は、その使われ方にある。セキュリティに完全を求めるのは費用対効果の面からも無理があり、また、利用者（預金者）の管理意識なしに、認証システムで 100%安全安心なシステムを提供するということも在り得ない。低い限度額や低い預貯金であれば、磁気ストライプ型カッシュカードも、現時点では、まだ現実的な選択肢、すなわちベストプラクティスと言えるかもしれない。

こうしたことの判断は、金融機関がどのようなビジネスモデルを目指しているかといったことにもよる。IC カード型キャッシュカードの対応は、かなりのコストがかかると言われているが、IC カード化したとしても、預金者のカードや暗証番号の管理に対する責務が変わるわけではない。

一般に、高い限度額の口座は、高いリスクを伴うと考えられる。この高いリスクを伴った認証を行なうためには、高いセキュリティを持った認証が提供されるべきであるが、高いセキュリティの認証ほど、高いコストがかかる。金融機関においても、「認証」が要求される場面は、CD/ATM での「認証」だけではなく、窓口での認証、オンラインバンキングでの認証など、様々な場面がある。今後は、オンラインバンキングのようなネットワークにおける認証がより重要になることも予想される。今回の「偽造キャッシュカード問題」での金融機関の対応として「取り扱い限度額」の引き下げがある。これは、磁気ストライプ型キャッシュカードを使った認証レベルに合わせて限度額を引き下げたとも言える。認証に対するリスクは、CD/ATM、コンビニ CD/ATM、デビットカードのように使う場所による違いもある。

以上のようなことから、リスクと認証のレベルと補償の考えかたなどはガイドライ

ンとして整備させるべきと考えられる。リスクと認証のレベルを考慮した認証システムのベストプラクティスは、技術の進歩と、提供するビジネスモデルにより時代と共に変化していく。こうしたことに対応するため認証システムのベストプラクティスを示すガイドラインを作成し、定期的に見直していくことなどが考えられる。現状では、以下の３つを検討すべきだと考えられる。

(1) 磁気ストライプと IC カードが並存する現状においてのベストプラクティス
(2) IC カードを前提としたベストプラクティス
(3) CD/ATM 以外の様々な認証を考えたベストプラクティス

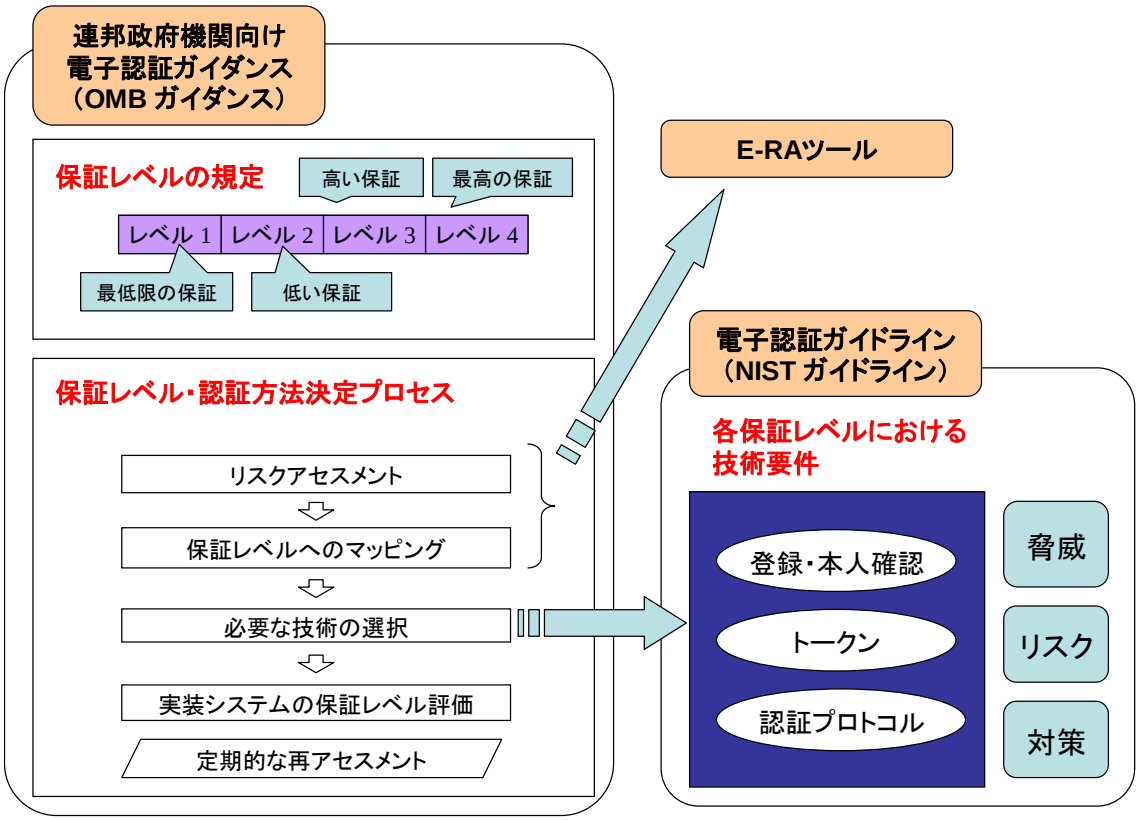
限度額などに対応した適切な認証レベルを検討し、現状の技術やビジネスモデルを考慮したベストプラクティスが策定できれば、リスクと対策のバランスが取れたサービスを提供できることが考えられる。そのサービスは必ずしも 100%のセキュリティを与えるものではないことに注意されたい。ベストプラクティスはあくまで現状での最適性を謳ったものであり、システムではカバーできないリスクは存在してしまう。ベストプラクティスと考えられる認証システムでカバーしきれないところを保険などで補償するといったことなどが考えられる。

4.4 参考例としての海外の電子政府における電子認証

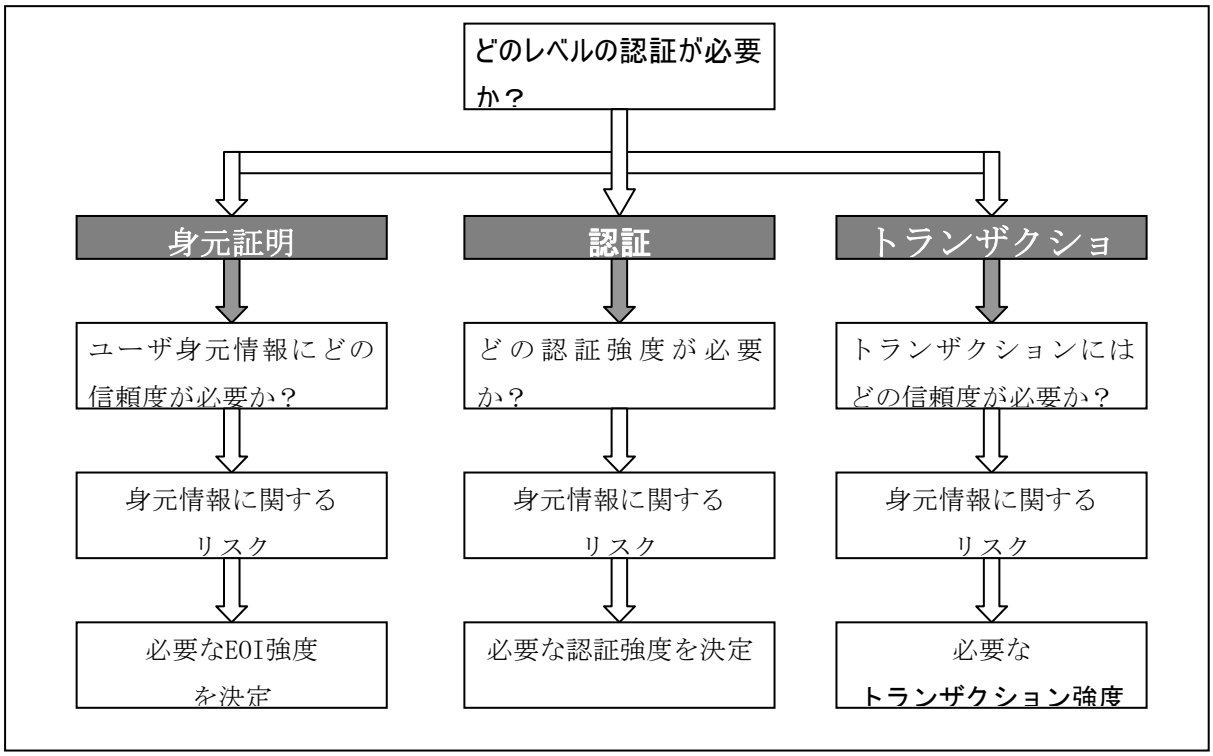
CD/ATM などにおける認証ではないが、リスクと認証のレベルを考慮したネットワークにおける認証のガイドラインの整備は、いくつかの国の電子政府などで進んでいる。米国、英国、オーストラリア、ニュージーランドといった国々の電子政府では、複数の保証レベルを持った特定の技術に依存しない認証のガイドラインを発行し、また、認証フレームワークの構築、または、検討を行なっている。これらの国々では、認証フレームワークを使って電子政府のセキュリティレベルの向上を目指している訳であるが、それだけではなくコストの削減も目標にしている。

これらの中で実際に一番進展しているのは米国の電子政府における認証フレームワークを推進する米国 e-Authentication イニシアチブであろう。米国 e-Authentication イニシアチブでは、最上位のポリシを行政管理予算局（Office of Management and Budget：OMB）が電子認証ガイダンスとして提供しており、その中で４つの保証レベルを示している。そして、この４つの保証レベルを前提に適応アプリケーションのリスク評価を行い必要な保証レベルのマッピングを行なうなどの保証レベルと認証方法の決定プロセスを示している。４つの保証レベルに対応した技術要件は、米国の標準技術局（NIST ： National Institute of Standards and Technology）が「電子認証ガイドライン」としてまとめている。この「電子認証ガイドライン」は、NIST の文書として「NIST Special Publication 800-63」という識別

がされているが、これは、米国電子政府の情報セキュリティのための一連の文書のひとつという位置づけにもなっている。



ニュージーランドの電子政府では「電子政府のための認証・認証のためのベストプラクティス・フレームワーク」を発行しているが、この文書は、認証のチュートリアルとしても非常によく出来ている。この中で、認証処理を、身元証明、認証、トランザクションの 3 つのコンポーネントに分けており、対応するアプリケーション(CD/ATM であれば現金の引き出しなど)に対するリスク評価に応じた３つのコンポーネントに対する強度が要求されるとしている。



身元証明に関しては、更に、身元証明フレームワーク（Evidence of Identity Framework）の開発が進められているとしている。この身元証明フレームワークの開発理由として、「省庁は，身元証明（EOI）に様々なアプローチを取れるようになったため、様々な省庁に応じて様々な身元証明（EOI）の組み合わせを要請された個人は混乱している。こうした混乱を回避するため、特定トランザクションに関連したリスクのレベルに準じ、プロセスを一貫する必要がある」としている。これなどは、金融機関等による顧客等の本人確認等に関する法律(本人確認法)などに記述されている内容に近いが、ニュージーランドの電子政府全体、そして、リスクのレベルに応じた本人確認を確立しようとしたとこがあり興味深い。

米国とニュージーランドのふたつの電子政府における電子認証の取り組みと考え方を簡単に紹介した。なぜ電子政府の認証システムかというと、それぞれの国で政府は IT システムの最大の調達者であり、また、国民や企業へのサービスのために限られたコストで利便性とセキュリティの確保が求められている。色々なサービスを提供する中、セキュリティ、コスト、リスク、利便性を全体的に最適化することを目指しているものと考えられる。こうしたことは各国の電子政府が推し進める EA（エンタープライズアーキテクチャ）に基づくシステム構築とも無関係ではない。電子政府の推進者は、各国の最大の調達者という立場で EA の導入が盛んであり、個別に構築してきたシステムを全体的に最適化するというモチベーションが働く。こうした背景の元に作成された「電子認証のガイドライン」なり「電子認証のベストプラクティス」といったものは、一般的に、特定の技術やソリューションを提供したい個々のベンダ

一企業やベンダー企業中心の組織からは出てきにくいことに注意する必要がある。

5 まとめ

金融機関にとって認証は預金者等の顧客に信頼の高いサービスを行うために非常に重要な役割を果たす。「認証」の信頼は、金融機関への信頼につながっている。「偽造キャッシュカード問題」においては、 金融機関の信頼の低下につながったといえる。

偽造キャッシュカード問題は「セキュリティ対策コストの問題」「認証技術の問題」「消費者保護(補償問題)」等の複数の問題の複合体であり、それぞれを別々に議論していても、全体として適切な解決は見えてこない。

また、取引形態の多様化から偽造キャッシュカードのみが対策されると別の取引形態の脆弱性をついた犯罪へシフトするだけであろう事が容易に想像でき、盗難キャッシュカード/盗難通帳の問題、CD/ATM 以外での取引等も含めた金融機関全体の認証システムの問題として検討すべきである。

これらの問題を解決するための方法として、以下のように行うのが良いのではないか。

１． 認証の保証レベル(ないしは認証の強度のレベル)、金融取引のリスク評価、消費者保護(補償)を分析し、これらのトータルなガイドラインを作る。

２． 金融機関の認証システムの ToBe モデルを策定し、EA(エンタープライズアーキテクチャ)によって、ToBe モデルを見据えて、磁気ストライプ/IC キャッシュカードが並存する期間、IC キャッシュカードに完全移行した期間など移行スケジュールに沿った各期間のベストプラクティスを示し、認証システムを構築してゆく。

低い保証レベルの認証システムが必ずしも悪いわけではない。高い保証レベルの認証はコストとのトレードオフとなる。現行の磁気ストライプキャッシュカードの様な低い認証レベルにおいては「低い取引金額」とすべきであって、即刻使用中止すべきであるといっているわけではない。また金融取引における認証を一括りに「低い保証レベルの認証レベル」にすべきか「高い保証レベルの認証」にすべきか言ってしまうと話が進まない。個々のサービスの内容にあった保証レベルの認証を行えばよい。

金融機関の認証システム全体で、個々のサービス毎に適切な認証が行われることによって、金融機関の認証システムに対する信用回復につながり、さらには金融機関の「信頼の創造」につながってゆくのではないだろうか。

参考文献

本人認証技術の現状に関する調査

http://www.ipa.go.jp/security/fy14/reports/authentication/

情報処理振興事業協会・セキュリティセンター

実施者　セコムトラストネット(株)

各国バイオメトリクスセキュリティ動向の調査

http://www.ipa.go.jp/security/fy15/reports/biometrics/

情報処理振興事業協会・セキュリティセンター

実施者　セコム(株)

平成１６年度情報セキュリティ対策推進事業

「電子商取引（ＥＣ）技術基盤の相互運用性に関する調査研究」

PKI を利用したアプリケーションの実用化に向けての課題と方向性調査

財団法人 日本情報処理開発協会

生体認証システムの脆弱性について -身体的特徴の偽造に関する脆弱性を中心に

http://www.imes.boj.or.jp/japanese/jdps/2005/yoyaku/05-J-02.html

宇根　正志・松本　勉

認証技術 パスワードから公開鍵まで

Richard E. Smith（著）訳：　稲村 雄

ISBN：　4-274-06516-2

米国の標準技術局 SP800-63 Version 1.0 Electronic Authentication Guideline

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

米国の行政管理予算局 “E-Authentication Guidance for Federal Agencies”

http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

米国 e-Authentication イニシアチブ

http://www.cio.gov/eauthentication/

ニュージーランド電子政府のための認証・認証のためのベストプラクティス・フレームワーク

http://www.e-government.govt.nz/docs/authentication-bpf/index.html

ニュージーランド電子政府の Evidence of Identity Framework

http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Framework-Index?OpenDocument

付録　米国連邦電子政府における電子認証の動向と電子認証ガイドライン

本付録では、4 つの保証レベルを規定している米国電子政府の電子認証ガイドラインについて概説する。

1. 米国連邦電子政府の電子認証の動向

2001 年秋以降、米国政府は 24 のイニシアチブを設け電子政府戦略を推進している。24 のイニシアチブは主に 4 つに大別される。まず政府がサービスを提供する対象により、G2C (政府機関対国民：Government　to Citizen)、G2G（政府機関対政府機関：Government to Government)、G2B (政府機関対企業：Government to Business）と分けられている。さらに、政府内部での効率化を目指す IEE（内部効率化：Internal Efficiency & Effectiveness）を加え、4 つの分類を構成する。また、この 4 つの分類とは別に全てのイニシアチブを横断する別イニシアチブとして e-Authentication が位置づけられている（図 1.1)。

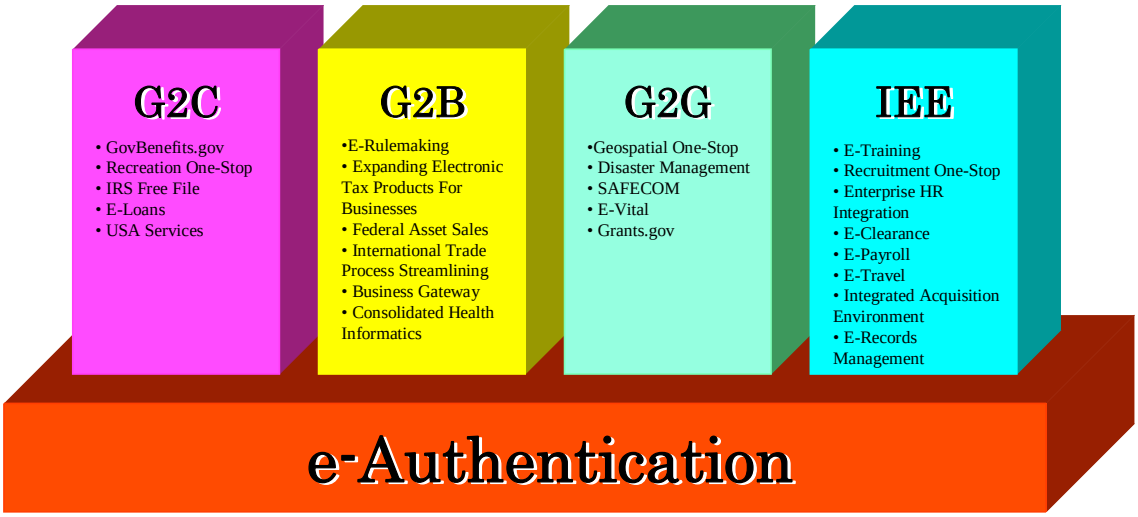


図 1.1　米国電子政府戦略における分類

すでに米国の政府機関では多数の本人認証を伴うシステムが稼動していたが、それらに互換性はなく、また構築や運用もそれぞれが行っていたために、本人認証に伴うコストに多大な負担を強いられていた。その中で、個々の認証システム構築のコスト、また連携したサービス展開、そしてユーザの利便性などを考慮し、e-Authentication イニシアチブが計画された。

2. 電子認証ガイドライン

e-Authentication イニシアチブの成果の 1 つとして、OMB は連邦政府機関向け電子認証ガイダンス（OMB ガイダンス）を発表した。その文書において OMB は電子認証での本人性保証について 4 つのレベルを規定した。そこでは提供されるサービスの重要性や機密性などを考慮した適切な保証レベルを持つ認証の重要性を示している。

適切な保証レベルに加え、OMB ガイダンスでは保証レベルと認証方法の決定プロセスも合わせて提示している。これらプロセスに従うことにより、提供サービスの適切な保証レベルと認証方法を決定することが可能になる。OMB ガイダンスでは技術面に関しては記述しておらず、その部分を NIST が策定した電子認証ガイドラインが受け持つ形になっており、認証のリスクや脅威、さらにはその対策までを含めた観点から 4 つの保証レベルを考慮している（図 3.1）。これら文書は主に米国政府向けに策定されている文書ではあるが、米国の産業界への影響は強く、さらには米国のみならず世界の各国により多く参考とされている文書となっている。

3. 認証における保証レベル

OMB ガイダンスでは認証におけるリスクとその影響度、さらに誤認証の発生確率を考慮して 4 つの保証レベルを定義し、それぞれのレベルにおける要件を述べている。

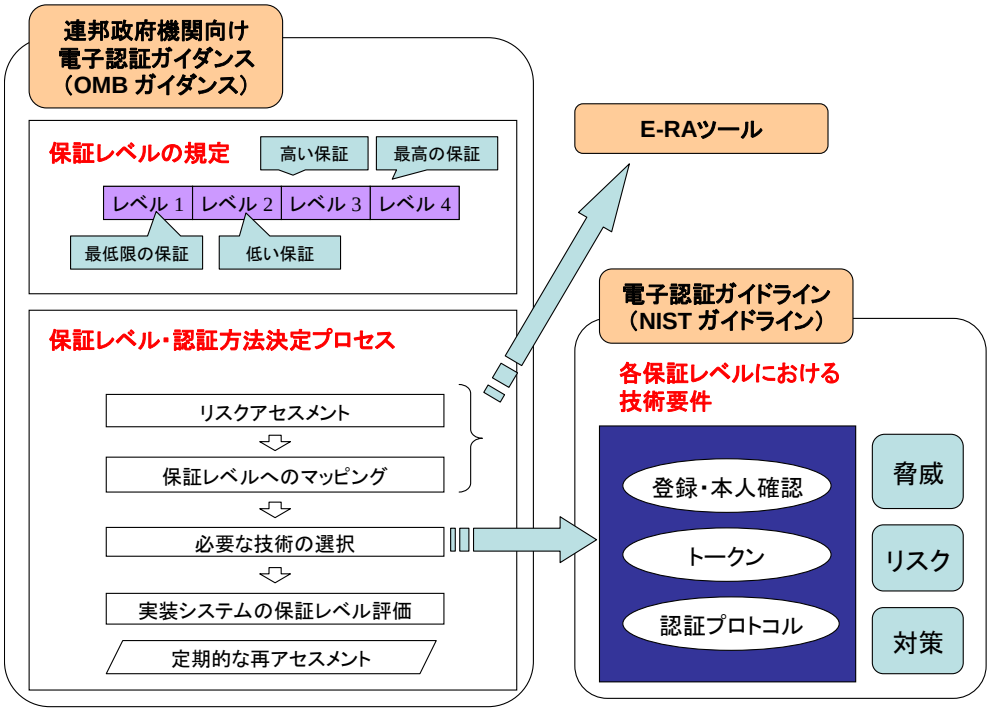


図 3.1　OMB ガイダンスと NIST ガイドラインの関係性

保証レベルの定義に先立ち、OMB ガイダンスでは保証を以下のように定義している。

- クレデンシャル被発行者のアイデンティティ調査プロセスにおける信用の程度
- クレデンシャル利用者がクレデンシャル被発行者であるという信用の程度

ここで言うクレデンシャルとは、トークンとその所持者を結びつける証明をするものであり、X.509 電子証明書などがこれにあたる。また、トークンとは認証に必要なパスワードや秘密鍵などといったものを言う。これをふまえ 4 つの保証レベルを定義した。定義と解説を表 3-1 に示す。

表 3-1 各保証レベルの定義と説明

レベル	定義	説明
1	主張するアイデンティティの正当性の信用が（ほとんど）ない	主張するアイデンティティの正当性の信用が（ほとんど）ない状態。たとえば、自己登録 ID とパスワードの利用によるサービスの利用などがこれにあたる。

2	いくらかの信用性	全般的に見てある程度の正当性が主張するアイデンティティに存在する状態。初期にアイデンティティの確認を必要とする公的サービスにおいて広く適用が可能である。誤認証によって起こる影響が一時的なもので済むような場合などがこれにあたる。
3	高い信用性	アイデンティティの正当性主張において高い信頼性を必要とするトランザクションに適している。たとえば特許申請時での特許情報の送信など、秘密情報の開示が競合相手に大きな利益を生ませるような場合に適用される。また、その財政ロスは重大ではあるが、壊滅的ではなくレベル 4 は妥当ではない場合など。
4	とても高い信用性	アイデンティティ正当性の主張において大変に高い信頼性を必要とするトランザクションに適している。たとえば法執行機関における犯罪情報を含んだデータベースへのアクセスなど、情報が開示したときに多大な問題を起こす場合など。

4. 認証方法と保証レベル決定プロセス

OMB ガイダンスでは保証レベルの定義に加え、認証方法と保証レベルの決定プロセスも合わせて提示している（図 4.1）。

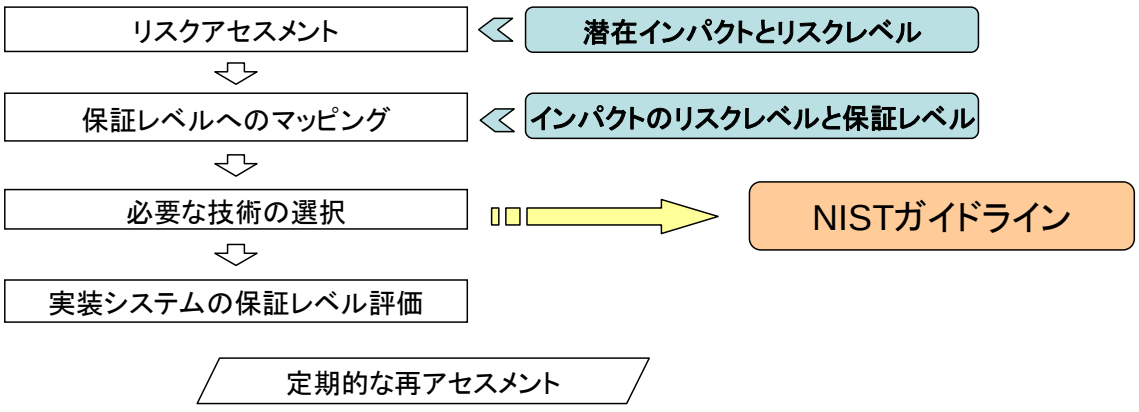


図 4.1 認証方法と保証レベルの決定プロセス

リスクアセスメント時には、認証に関しての潜在的なインパクトとリスクのレベルについて評価を行う。それら評価についての結果をマッピングすることで保証レベルが得られる。潜在的なインパクトとリスクについては次節で解説する。

5. 潜在的なインパクトとリスク

保証レベルを適切に設定するためには、認証における潜在的なリスクを考慮しなければならない。当然、認証エラーが起きた場合の影響が大きい場合には高い保証レベルの認証が必要となる。

OMB のガイダンスでは認証における潜在的なリスクとして、NIST が策定した連邦政府情報と情報システムにおけるセキュリティ分類標準（FIPS 199）に従った 6 つのカテゴリについて、認証における潜在的なインパクトと被害を評価する。表 5-1 に 6 つのカテゴリと、各カテゴリにおける影響度の説明を示す。

表 5-1 潜在的なインパクトと被害

カテゴリ	影響度		
	Low	Moderate	High
不便性、災難、身分や評判への損害	短期間における限定した損害	短期間における深刻な損害、あるいは長期間における限定した損害	長期間における深刻あるいは非常に厳しいな侵害
金銭的ロス、組織の責務	あまり重要でない、取るにたらない回復不可能な金銭的ロスあるいは組織の責務	深刻な回復不可能な金銭的ロスあるいは組織の責務	非常に厳しいまたは壊滅的な金銭的ロスあるいは組織の責務
組織計画や公益への被害	組織運用や資産、公益に対して限定されている逆の効果の波及	組織運用や資産、公益に対して深刻な逆の効果の波及	非常に厳しいまたは壊滅的な逆の効果の波及
機密情報の未許可開示	影響度の低い機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示	影響度が中程度の機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示	影響度の高い機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示
個人の安全	医療措置を必要としない傷害	たいしたことのない傷害の中程度のリスク、あるいは医療措置を必要とする限定したリスク	深刻な障害あるいは死のリスク

民事上あるいは刑事上の違反	通常は法執行を受けることのない民事上あるいは刑事上違反のリスク	法執行をうける民事上あるいは刑事上違反のリスク	法執行計画において非常に重要な民事上あるいは刑事上違反のリスク

OMB ガイダンスではこれら各カテゴリのインパクトと保証レベルの対応表を用意した。各カテゴリのリスク評価を行った後に対応表を利用することで、適切な保証レベルの選択が可能になる。対応表を表 5-2 に示す。

表 5-2 潜在的インパクトのレベルと保証レベルの対応

認証エラーによる潜在的な影響のカテゴリ	保証レベル			
	1	2	3	4
不便性、災難、身分や評判への損害	Low	Mod	Mod	High
金銭的ロス、組織の責務	Low	Mod	Mod	High
組織計画や公益への被害	N/A	Low	Mod	High
機密（sensitive）情報の未許可開示	N/A	Low	Mod	High
個人の安全	N/A	N/A	Low	High Mod
市民や犯罪の違反	N/A	Low	Mod	High

6. 各保証レベルにおける技術要件

OMB ガイダンスでは 4 つの保証レベルについて技術用件は提示しておらず、NIST ガイドラインがその役目を負っている。各レベルで必要とされる技術要件については、3 つの要素より考慮がされる。1 つ目が本人認証に用いるトークン、2 つ目が登録作業とアイデンティティの確認、そして 3 つ目に認証プロトコルである。ここでは、各技術要件の詳細は割愛する。