平成１７年度経済産業省　産業技術研究開発委託事業－１
生体情報による個人識別技術（バイオメトリクス）を
利用した社会基盤構築に関する標準化

第６部　金融分野におけるバイオメトリック認証モデルの開発

平成１８年３月

財団法人ニューメディア開発協会

６　金融分野におけるバイオメトリック認証モデルの開発

６．１金融分野の国際標準規格 ISO19092 の調査分析

６．１．１　　背景と目的

バイオメトリック認証に関する標準化は、ISO/IEC JTC1 SC37 を中心に行われているが、ISO/IEC JTC1 SC37 では、バイオメトリック技術のみに限定されており、IC カードや暗号技術などの他のセキュリティ技術に関わる標準仕様については、それぞれの業務分野に関する標準化を推進する団体により、標準化が行われている。例えば、バイオメトリクスデータを書き込んだパスポートについては、ICAO NT-WG（ISO/IEC JTC1 SC17）、免許証は ISO/IEC JTC1 SC17、暗号を連携した通信プロトコルは ITU-T SG17 などがある。これらの標準化団体は、バイオメトリクス技術に関して、ISO/IEC JTC1 SC37 とリエゾン関係を構築し、可能な限りそれぞれの標準文書に齟齬が発生しないように、連携して標準化を進めている[1]。

金融業界の技術仕様については、ISO TC68 SC2 にて標準化が進んでおり、バイオメトリクスによる管理とセキュリティについて、米国 ANSI 標準の X9.84:2003[2]をベースに ISO TC68 SC2WG10 にてプロジェクト番号 19092 として、検討が行われている。X9.84:2003 の詳細については、2004 年度の報告書[1]に詳述したので、参照されたい。

ISO 19092 では、現在、二つのパート構成で、標準化が進んでおり、Part1 では 19092 のセキュリティフレームワーク、Part2 ではバイオメトリクス情報や運用情報のフォーマットの規格化を進めている。

この標準は、金融業務へのバイオメトリクス認証技術の適用をする際に準拠義務が発生する規格であるため、本事業の金融業務におけるバイオメトリック本人認証モデルを検討するうえで、配慮する必要がある。このため、ISO19092 の標準化動向について調査するとともに、ISO TC68 国内事務局の日本銀行研究所からのコメント要請への対応について、続いて詳述する。

６．１．２　　ISO DIS 19092-1

（1）　標準化動向

ISO 19092-1 の標準化動向を下記にまとめる[3]。

Title：	Financial Services – Biometrics – Part1: Security Framework
タイトル：	金融サービス－バイオメトリック認証－パート１：セキュリティフレームワーク
事務局：	ISO TC68（金融サービス）、SC2（セキュリティ）（ANSI X9）
経緯：	2003 年 5 月に NWI として、X9.84:2003 文書が米国 ANC X9 より提案される。 2004 年 7 月に２パート構成の CD 文書が提出。10 月の投票の結果、2ndCD へ。 2004 年 12 月に 2ndCD 文書が提出。4 月の投票の結果、DIS 化が承認。
現在の状況：	DIS 文書を 2005 年 8 月 24 日に発行。2006 年 1 月 24 日投票（75%の賛成で IS 化）。 （日本からは、コメント付き賛成で投票。詳細は(3)節参照）

（2）　DIS 19092-1 の概要

［スコープ］

本国際標準では、金融サービスにおいて個人認証にバイオメトリクスを利用するためのセキュリティフレームワークについて記述している。これらアプリケーションに関係する問題とバイオメトリクス技術のタイプを紹介する。このパートでは、実装するためのアーキテクチャを記述し、効果的な管理のための最小のセキュリティ要件を明らかにし、実運用に利用に適した勧告と管理目標を備えている。

本国際標準のスコープは以下のトピックである。

- 金融サービスに求められる要求 ID の照合と個人識別のような人と従業員の認証のためのバイオメトリクスの利用
- リスク管理により備えられたような認証をサポートするために登録時の提示される証明書の認可方針
- バイオメトリック情報のライフサイクルにおける管理
- バイオメトリクス情報のライフサイクルにおける安全性（完全性、正当性、秘匿性）
- ロジカルおよびフィジカルアクセスコントロールのためのバイオメトリクス応用
- 金融施設と顧客を保護するための監視
- バイオメトリクス情報のライフサイクルで利用される物理的ハードウェアの安全性

以上に対し、以下はスコープ外である。

- バイオメトリック情報の所有権とプライバシー
- バイオメトリックのデータ収集、信号処理、バイオメトリックデータの照合、判定のそれぞれの個別の技術
- バイオメトリック技術を使った本人認証をしない利用方法：匿名のアクセスコントロールなど

［文書の構成と各章の骨子］

第1章　スコープ

第2章　準拠するべき項目

本標準文書において、特に 9 章、10 章、11 章、Annex A の項目により、本標準の準拠が達成できる。

第3章　規定された標準文書一覧

第4章　用語定義

第5章　シンボルと略称

第6章　バイオメトリック技術の概要

バイオメトリック技術について、概略を説明し、指紋や声紋、虹彩、網膜、顔、掌形、動的署名などの技術の概略を説明。

第7章　検討

金融分野のアプリケーションとして、Cash Desk、Dispensing bank notes、Cheque fraud detection を説明。

第8章　基本のバイオメトリック機能の構成

バイオメトリックシステムを構成するサブシステムの機能の説明。具体的には、データ収集、通信、信号処理、照合、判定、保管、トークンなど。

第9章　管理とセキュリティの要件

バイオメトリック機能の全てに適用されるコア要件と､各サブシステムおよび各ライフサイクル(登録、照合・識別、再登録、通信、保管、廃棄、アーカイブ、イベント日誌など）ごとの要件を規定している。

第10章　金融セキュリティ基盤

セキュリティを実装するための技術を紹介している。具体的には、鍵管理、デジタル署名、メッセージ認証コード（MAC)、データ秘匿目的の暗号、物理的保護など。

第11章　バイオメトリックの運用認証のための管理目標

バイオメトリックシステムの運用を認証するための 336 項目の管理目標を規定している。具体的には、定期的なレビューと監査、環境的な管理目標、鍵管理におけるライフサイクル、バイオメトリックのライフサイクルなどで、詳細に規定している。

Annex A　イベント日誌（規定）

バイオメトリックシステムの運用を認証するために必要なイベント項目とその内容について、規定している。

Annex B　バイオメトリック登録（規定）

バイオメトリック情報を登録する際のガイドラインを規定している。具体的には、本人確認のための規準や、照合可能かの品質チェックなど。

Annex C　セキュリティ検討（規定）

バイオメトリックシステムを導入する際に検討するべき、セキュリティ上の課題を明記している。

Annex D　バイオメトリックデバイスのためのセキュリティ要件（規定）

バイオメトリックデバイスの物理的なセキュリティ要件について、（FIPS140-2 のように）規定している。

［セキュリティ要件］

本標準で規定している主な要件を、以下に示す。

システム全般

- ２つのコンポーネントの間で、バイオメトリックデータおよび本人認証結果の完全性が保持される機構（MAC のような暗号機能かデジタル署名機能、または、通信経路の物理的な保護）が無ければならない。
- バイオメトリックデータおよび本人認証結果の送信元と受信先との間で相互認証する機構（MAC のような暗号機能かデジタル署名機能、または、通信経路の物理的な保護）が無ければならない。
- 必要に応じて、２つのコンポーネント間のバイオメトリックデータおよび本人認証結果の秘匿性が保証される機構（暗号、または、通信経路の物理的な保護）が無ければならない。

登録

- 登録するための権限を持つ登録オペレータにより、登録者を保証する機構または手続きが無ければならない。
- バイオメトリックデータを収集する前に、登録者の身元を確認する機構または手続きがなければならない。

- 登録者とバイオメトリックデータの結びつきが保証される機構（MAC のような暗号機能かデジタル署名機能、または、データの物理的な保護）または手続き（登録時の記録との照合）が無ければならない。
- コントロール下では Annex D のレベル２の物理的セキュリティ、コントロールされない状況ではレベル３の物理的セキュリティに合致せねばならない。
- バイオメトリックデータの完全性と正当性は、ライフサイクルを通じて保持されなければならない。さらに、テンプレート発行日も、完全性が維持され、得られなければならない。

照合

- 照合サブシステムは、Annex D のレベル３の物理的セキュリティに合致しなければならない。
- FNMR（誤り非合致率：本人拒否率）は、10^{-2} 以下で無ければならない。
- 登録誤り率は、顧客サービス低下につながらないように、検討されなければならない。

（3）　DIS 19092-1 に対するコメントの内容

DIS19092-1 について、ISO TC68 国内事務局の日本銀行研究所より、ISO/IEC JTC1 SC37 国内委員会へのコメント要請に対応し、次のようなコメントを作成した上で「コメント付き賛成」にて、ISO/IEC JTC1 SC37 WG4 国内委員会および、ISO/IEC JTC1 SC37 国内専門委員会のレビューを受け、ISO TC68 国内事務局へ提出した。これらのコメントは概ね採用され、ISO TC68 国際事務局へ「コメント付き賛成」にて投票された。

①6 章 Biometric technology overview について

この中で指紋、声紋、虹彩、網膜顔、手形、署名を紹介しているが、日本の金融機関で運用が始まっている静脈認証について、触れられていない。6.1 節の最後の段落の列挙に、vein pattern を追加するとともに、6.9 節に、次の静脈認証に関する紹介文の追加を提案する。

6.9　静脈認証（Vein biometrics）

静脈認証は、個人を識別する情報として、人間の体の皮下組織にある静脈の血管パターンを用いる。静脈パターンは近赤外光を用いて読み取る。近赤外光を照射すると、静脈に含まれる還元ヘモグロビンは近赤外線を吸収するので、皮下にある静脈の血管パターンが影となる陰影画像が得られる。その陰影画像から、画像処理技術を用いて陰影部を静脈の血管パターンとして抽出する。その血管パターンを、分岐点の位置や方向などの特徴や、パターンそのものの特徴などを用いて照合する。

実際の製品では、製品ごとに、手のひら、指、手の甲などの、利用者がセンサに血管パターンを提示しやすい部位が照合部位として選ばれており、また、それぞれの照合部位の提示をサポートするガイドや、画像処理による位置合わせなどにより、非常に安定（stable）した認証精度を持っている。静脈認証で用いる静脈の血管パターンは、皮下に隠れている情報なので、通常の環境では他人に知られることがなく、そのため偽造物の作成も困難である。

以上のようなセキュリティや認証精度の優れた特徴が評価され、手のひら、指、手の甲の静脈を用いた複数のベンダによる静脈認証製品が、既に複数の金融機関の ATM(*)や入退室管理シス

テムで運用されている。

(*)日本では、複数の大手銀行、多数の地方銀行などの金融機関の ATM へ、手のひらや指の静脈認証技術が採用されている（2005 年 11 月現在）。

②10.2 項 Physical techniques について

物理的セキュリティ保護機構について、ISO/IEC 19790 を参照しているが、バイオメトリックセンサ面から外側から、バイオメトリック特有の脆弱性を利用した脅威にたいする保護について、明記されていない。例えば、偽造物体によるなりすましなど（横国大：松本教授報告など参照） 。このため、19790 への準拠だけでは、セキュリティが十分ではない。AnnexC C.3 などの検討と、新しく出現するバイオメトリック特有の脆弱性を利用した脅威への対応を明記するべきである。この上で、適切な対策の有無によるレベル付けが必要かもしれない。

③11.4.3 項　照合と識別処理の管理目標について

11.4.3：242 項 BP に従って、バイオメトリック認証失敗時の代替手段を用意するべきとあるが、代替手段がセキュリティホールとなる恐れもあるため、どのように代替手段を決定（同等のセキュリティリスクの代替手段を選択するなど）し、（セキュリティリスクが異なる場合、）代替手段による認証の場合の制限を適切に設定するなどといった、注意書きが必要である。

６．１．３　　ISO 3rdCD 19092-2

（1）　標準化動向

ISO 19092-2 の標準化動向を下記にまとめる[4]。

Title：	Financial Services – Biometrics – Part2: Message syntax and cryptographic repuirements
タイトル：	金融サービス－バイオメトリック認証－パート２：メッセージ構文と暗号要件
事務局：	ISO TC68（金融サービス）、SC2（セキュリティ）（ANSI X9）
経緯：	2003 年 5 月に NWI として、X9.84:2003 文書が米国 ANC X9 より提案される。 2004 年 7 月に２パート構成の CD 文書が提出。10 月の投票の結果、2ndCD へ。 2004 年 12 月に 2ndCD 文書が提出。4 月の投票の結果、DIS 化が棄却 3rdCD へ。
現在の状況：	3rdCD 文書を 2005 年 8 月 18 日に発行。2005 年 12 月 19 日投票。 （日本からは、コメント付き反対で投票。詳細は(3)節参照）

（2）　3rdCD 19092-2 の概要

［スコープ］

本標準は、金融サービスにおいてバイオメトリクス認証の実装する際のバイオメトリックオブジェクトとメッセージの文法と、オブジェクトのための暗号要件を記述したものである。本標準のこのパート

では、以下をスコープとしている。

- セキュリティと互換性とデータ秘匿のためのバイオメトリック情報の暗号保護
- バイオメトリック情報のライフサイクルに渡る安全な通信と保管
- バイオメトリック情報のデータ完全性と正当性、秘匿のための暗号技術

以上に対し、以下はスコープ外である。

- バイオメトリック情報の所有権とプライバシー
- バイオメトリックのデータ収集、信号処理、バイオメトリックデータの照合、判定のそれぞれの個別の技術
- バイオメトリック技術を使った本人認証をしない利用方法：匿名のアクセスコントロールなど

［文書の構成と各章の骨子］

第1章　スコープ

第2章　規定された標準文書一覧

第3章　用語定義

第4章　シンボルと略称

第5章　暗号技術と構文

ASN.1 構文によってバイオメトリックオブジェクトや、ヘッダ、完全性オブジェクト、プライバシーオブジェクトを規定している。さらに規定されたオブジェクトの拡張についても規定している。

第6章　バイオメトリック照合の判定制御

ポリシーに基づく照合判定や判定制御プロトコルについて規定すると思われる。（記述が不十分）

第7章　バイオメトリックイベント情報の管理

イベント日誌の項目とそれぞれの項目の書式を規定している。さらに、イベント日誌の保護についても規定している。

第8章　ISO 8583 メッセージ

ISO 8583 は、金融トランザクションカードのためのビットマップフォーマットを定義した規格である。この ISO8583 メッセージを拡張し、バイオメトリック認証のためのメッセージを規定している。

Annex A　バイオメトリック情報スキーマ（：規則表記）（規定）

ASN.1 にて定義されたバイオメトリック情報を ASN.1 モジュールとして、定義している。

Annex B　バイオメトリックパトロンフォーマット（参考）

CBEFF のパトロンフォーマットとして、BioAPI の BIR と X9.84 がある。BioAPI との互換性と、ISO 19092 の実装について、述べている。

（3）　3rdCD 19092-2 に対するコメント

DIS19092-1 と同様に、3rdCD19092-2 についても、ISO TC68 国内事務局の日本銀行研究所より、ISO/IEC JTC1 SC37 国内委員会へのコメント要請に対応し、次のようなコメントを作成した上で「コメント付き反対：4thCD の作成提案」にて、ISO/IEC JTC1 SC37 WG4 国内委員会および、ISO/IEC JTC1 SC37 国内専門委員会のレビューを受け、ISO TC68 国内事務局へ提出した。これらのコメントは概ね採用され、ISO TC68 国際事務局へ「コメント付き反対」にて投票された。

①8.7 Code Listings (ed)

章タイトルに Annex A(normative)が残っている。また、Table タイトルに、Annex の表タイトルが残っている。

②8 章 ISO 8583 messages

ここで定義するメッセージの前提となる Sender と Receiver のバイオメトリクス認証のシステム構成（テンプレートの格納や照合や識別処理の実装構成）を明示するべきである。また、Part1 の完全性要件を満たす MAC や署名をサポートしていない。このため、Part１との齟齬がある。

③6 章 Biometric matching decision control

8 章の ISO8583 messages と関連がある。また、5.3.2.5 試行回数、5.3.3.2 セキュリティクリアランス、5.3.3.6 判定制御は、6 章や 8 章などと関連する項目である。バイオメトリック登録情報の拡張として定義する情報として定義するのが、適切か検討するべきである。

具体的には、5.3.2.4 の Template の Policy の一つの項目として位置づけて、整理してはどうか？

さらに、6 章・8 章で、バイオメトリック照合の結果の判定処理を定義しているが、Part1 の 11 章で規定したポリシーとの関連を明らかにしながら、明記する必要がある。このため、Part1 の 11 章の組織ポリシーの記述方法を 6 章で明らかにし、この上で、6 章と 8 章の内容を統合し、5.3 で定義された発行時のポリシーを参照した上で、組織ポリシーに合致しているかを判定する処理やプロトコルを新たな章で規定してはどうか？

④5.3.2.4 Biometric Policy

Part1 の 11.4 節 Biometric life cycle において、具体的に BP で定義するべきことを列挙している。Part1 に準拠して、ここであげた項目のうち、Template に記述する事項に ID を割り付け、各 ID ごとにポリシーの記述方法を具体的に定義してはどうか？

６．２金融業務におけるバイオメトリック本人認証モデルの開発

６．２．１　　昨年度の成果と今年度の検討内容

(1)　昨年度の成果

昨年度の基準認証研究開発事業では、金融におけるバイオメトリック認証モデルと要件の検討にあたり、各金融機関の窓口、および、自動支払い機（ATM や CD）における本人認証にバイオメトリック認証を適用した場合の認証モデルと要件を検討範囲（図１）とし、研究開発を行った[1]。

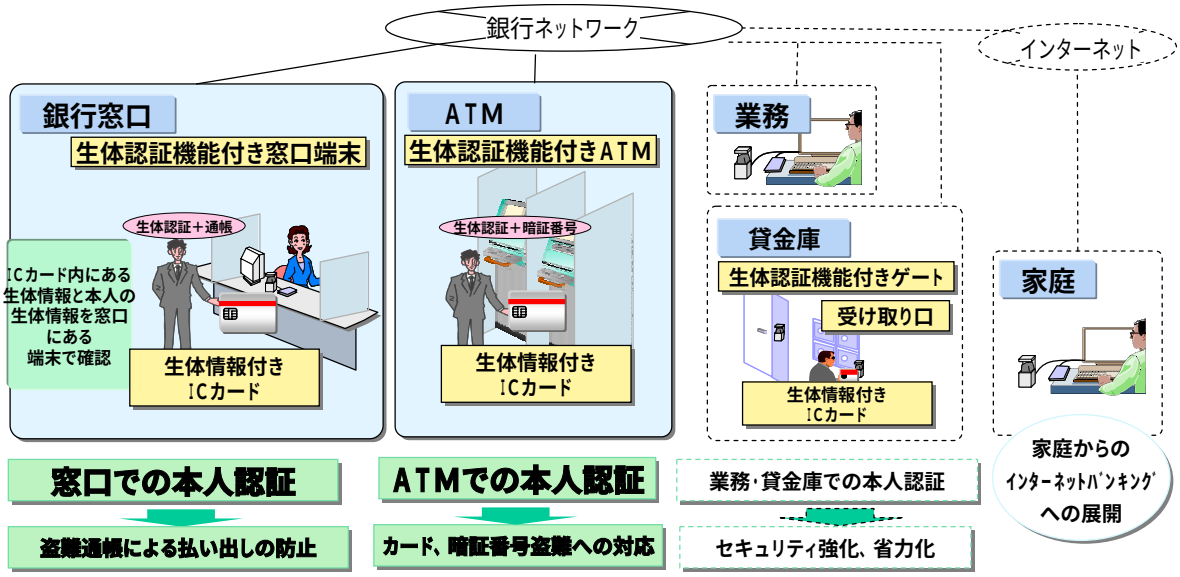


図１　昨年度の検討範囲

（2）　今年度の検討内容

今年度の基準認証研究開発事業においては、別途進む全国銀行協会における ATM カードなどの規格検討や、昨年度の研究開発内容との重複を避けるため、家庭や職場などからインターネットを介して、口座操作を実施するインターネットバンキングにおける本人認証に、バイオメトリック認証を適用した場合の認証モデルと要件を検討対象とし研究開発を実施した（図２）。

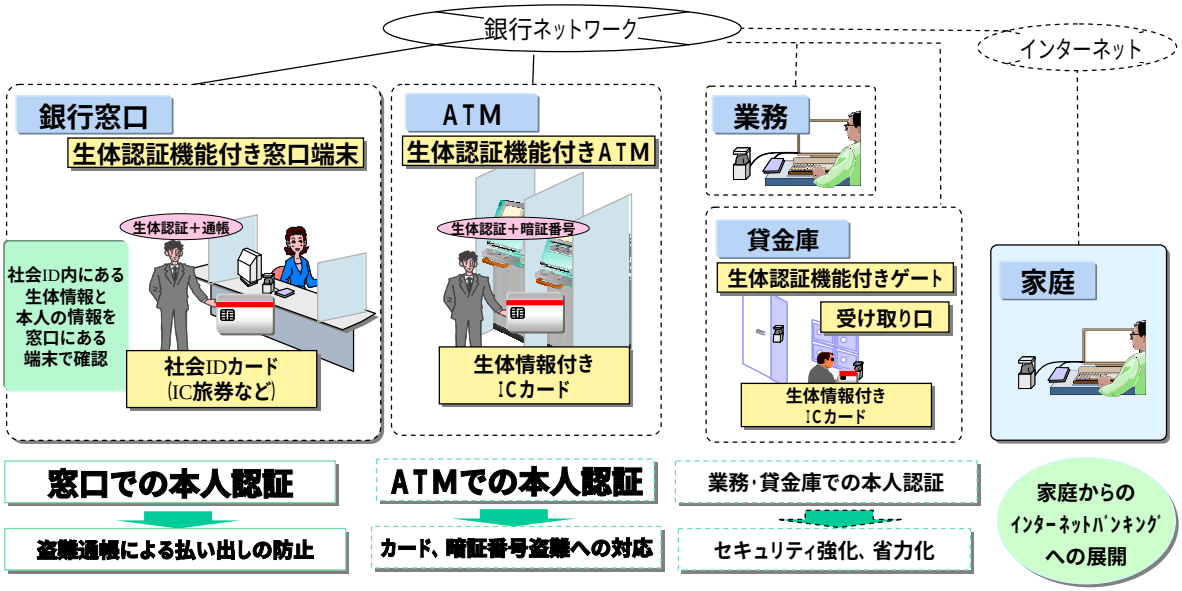


図２　今年度の検討範囲

本報告では、インターネットバンキングはインターネット経由で提供するバンキングサービス全般と定義し、ウェブバンキングは、同じくインターネット経由のウェブブラウザと HTTP プロトコルを利用して提供するバンキングサービスと定義して用いている。

（3）　研究開発のアプローチ

インターネットバンキングにおけるバイオメトリック認証モデルと要件を検討するに当たり、図３に示す５つのステップのアプローチを取った。

ステップ①：インターネットバンキングの動向調査

インターネットバンキングの普及状況や本人認証の仕組み、セキュリティ上の課題について、動向を調査する。

ステップ②：現行のインターネットバンキングのモデル分析

ステップ①の調査結果より、現状のインターネットバンキングのシステムモデルを検討する。

ステップ③：インターネットバンキングの脅威抽出

ステップ①の調査結果、および、ステップ②の現行のインターネットバンキングのシステムモデルに想定される脅威を抽出する。

ステップ④：インターネットバンキングにおける本人認証（バイオメトリック認証）の要件

ステップ③で明らかにした脅威に対する、セキュリティ上の要件を検討する。

ステップ⑤：インターネットバンキングにおけるバイオメトリック認証モデル

ステップ④の要件に従った、インターネットバンキングのバイオメトリック認証モデルを検討する。

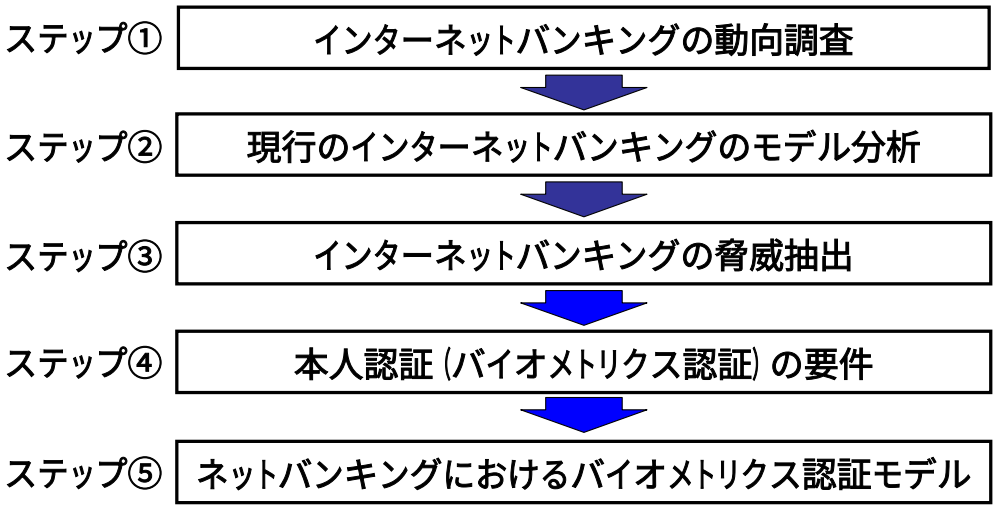


図３　本テーマの研究開発のアプローチ

６．２．２　　インターネットバンキングの動向調査

（1）　インターネットバンキングの普及動向

①アイブリッジ「リサーチプラス」による調査[5][6]

調査対象：インターネット上の 300 人（ネット普及率：約 60%）

ネットバンキングの利用状況：

30%弱（2003 年 11 月）→76.6%（2004 年 11 月）

利用銀行：

イーバンク（39.8%）、ジャパンネット（19.1%）、三井住友（9.0%）、みずほ（4.8%）、UFJ（4.8%）、ソニー（4.8%）、東京三菱（3.6%）、アイワイ（1.6%）

利用しない理由：

セキュリティ（35.7%）、使い方不明（30%）、不要（27.1%）

総務省の情報通信白書[7]によると、2004 年のネット普及率を約 60%であることを考慮すると、約 40%～50%程度の利用率と思われる。

②米国 Ipsos/Insight の米国成人（1000 人）の利用調査 [8][9][10][11]

ネットバンキングの利用状況：

23%（02 年）→40%（04 年）→39%（05 年）

２００２年から２００４年にかけて約２倍弱も利用者が増加したが、２００４年から２００５年にかけては利用者は微減した。これは、スパイウェアなどの蔓延によるセキュリティへの懸念が広まり、この一年の普及は進んでいない。

以上の調査のほか、米国では消費者が銀行を選択する基準として、「オンラインバンキング」が、ATM や支店の場所を上回っており[14][15]、サービスチャネルとしてのインターネットは銀行にとって、無視できないものとなっている。

（2）　現行のセキュリティと本人認証方式

国内の金融機関のインターネットバンキングサービスにおける本人認証方式と、セキュリティ対策を各金融機関のＨＰの情報に基づいて調査した[16]－[28]。

①ネットバンキングにおける現行の本人認証方式

（ｉ）第 2 パスワード方式

インターネットバンキングページへのログインＩＤ用のパスワードと、決済処理要求時の決済パスワードの二段階の本人認証を実施する方式。この中では、最も簡単な（＝低コストな）本人認証方式のため、多くの銀行、郵貯、信用金庫、ネット銀行がこの方式を採用している。（第３パスワードまで設定している金融機関もある[16]。）

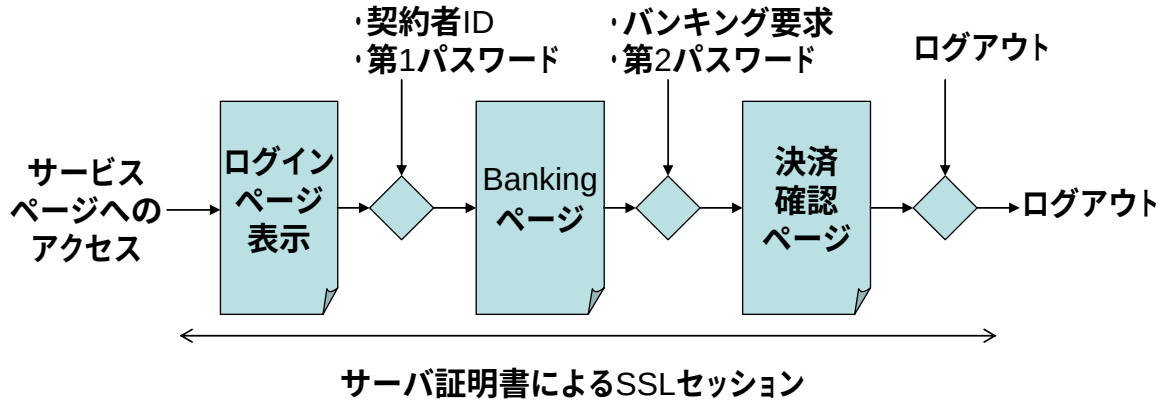


図４　第２パスワードによる本人認証

（ｉｉ）ワンタイムパスワード方式（マトリクステーブル）

インターネットバンキングページへのログインＩＤ用のパスワードと、決済処理要求時に指定されるマトリクステーブルの行列番号の 4 桁数字により本人認証を実施する方式。一部の大手銀行などがこの方式を採用している。

（ｉｉｉ）ワンタイムパスワード方式（トークン）

インターネットバンキングページへのログインＩＤ用のパスワードと、決済処理要求時に入力するワンタイムパスワード発生器の数値により本人認証を実施する方式。一部の大手銀行がこの方式を採用した[17]。

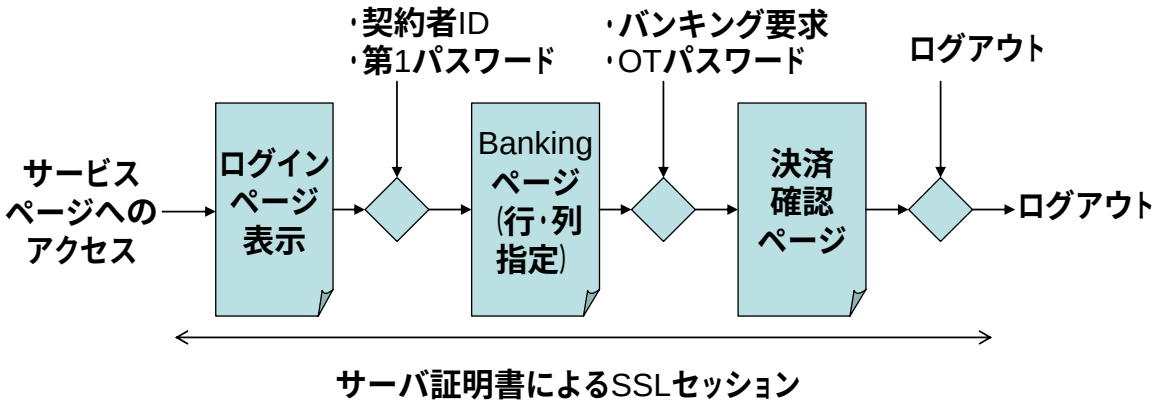


図５　ワンタイム（OT）パスワードによる本人認証

②本人認証時のセキュリティ

（ｉ）サーバ証明書による SSL 通信

インターネットバンキングへのサービスページに対するＨＴＴＰセッションにおいて、バンキングサーバの証明書に基づいて、サーバ認証を実施し、共通鍵交換した暗号鍵により、暗号通信を行うＳＳＬ通信により、通信チャネル上の情報漏えいを防止する。また、サーバのなりすまし脅威についても、証明書の正当性や信頼性を確認することで、対処可能である。この対策は、調査した全ての金融機関で実施している。

（ｉｉ）Cookie 認証

インターネットバンキングを利用しているＰＣを特定し、ページや画面間の情報引継ぎを管理する仕組み。この仕組みＩＤ情報や暗号鍵などの情報を引き継ぐことができる。この対策は、一部の銀行に採用されている。

（ｉｉｉ）利用 PC 認証（自宅 PC をあらかじめ登録し、Cookie 情報の保管）

あらかじめインターネットバンキングに利用するＰＣの情報を記録した Cookie をあらかじめ登録して PC に保管することで、他のＰＣなどからのアクセスを制限する仕組み。この対策は、一部のネット銀行に採用されている。

（ｉｖ）ソフトウェアキーボード

画面上に表示された（英）数字キーをマウスにクリックすることで、キーロガーなどのスパイウェアに対処する仕組み。クリック座標の周辺画像を切り出し保管するスクリーンショットなどのスパイウェアへの対処のため、クリック時の画面を黒塗りする仕組みなどもある金融機関で採用されている。

（ｖ）過去ログの提示。（不正利用の早期発見）

インターネットバンキングへのログイン時に前回のログイン日時を表示することで、不正利用の早期発見に対処できる。あるネット銀行に採用されている。

この他、インターネットバンキングでの決済上限額の指定や、一定時間無操作時の自動ログアウト、連続複数回のログイン失敗時の利用停止、サーバへのファイアウォールなどの対策が実施されている。

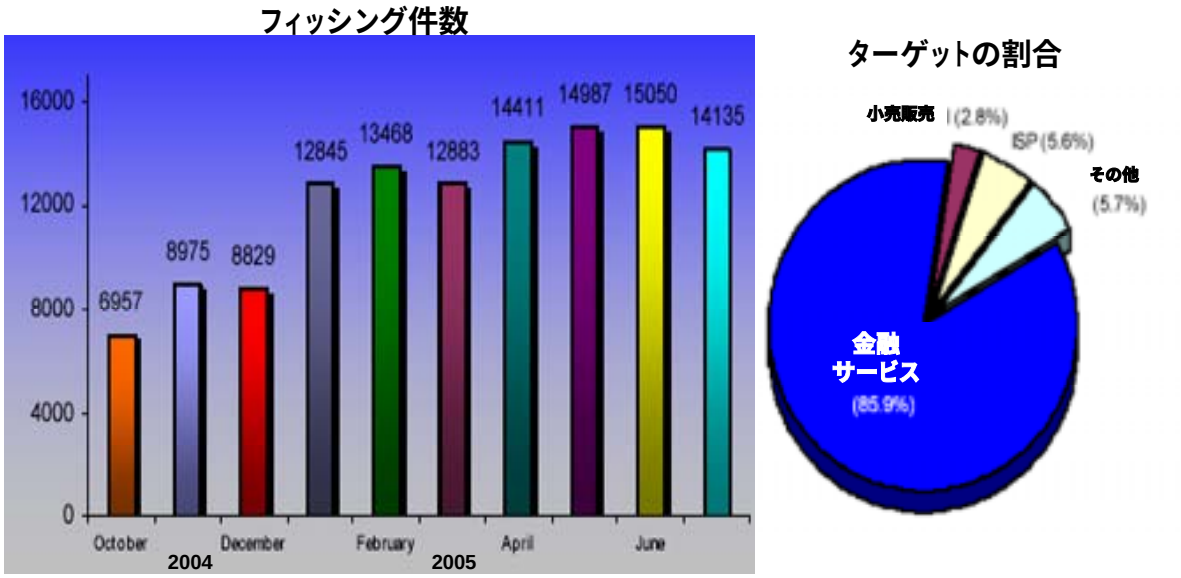
また、インターネットを介したオンライン証券取引においても、各証券会社ごとに独自のポリシーにより、本人認証を行っている。例えば、松井証券では、SSL 通信化においてログインパスワード＋取引パスワードの第２パスワード方式を採用している[26]。一方、野村證券では、ユーザーに PKI の証明書（私有鍵付き）を発行してインストールされた PC を認証する方式をログインパスワードに加えている[27]。日興コーディアル証券では、セキュリティ強化版として、ソフトウェアキーボードからのパスワード入力を可能としている[28]。

③まとめ

各金融機関ごとに独自のセキュリティポリシーにより、本人認証を実施している。これは、ＡＴＭなど行内で発生する決済とは異なり、インターネット経由に利用者と取引する金融機関が直接、接続するため、各行、独自のポリシーでバンキングサービスを提供している。（ＡＴＭや窓口では、他行への口座決済では、全銀チャネルを経由する仕組みとなる。）

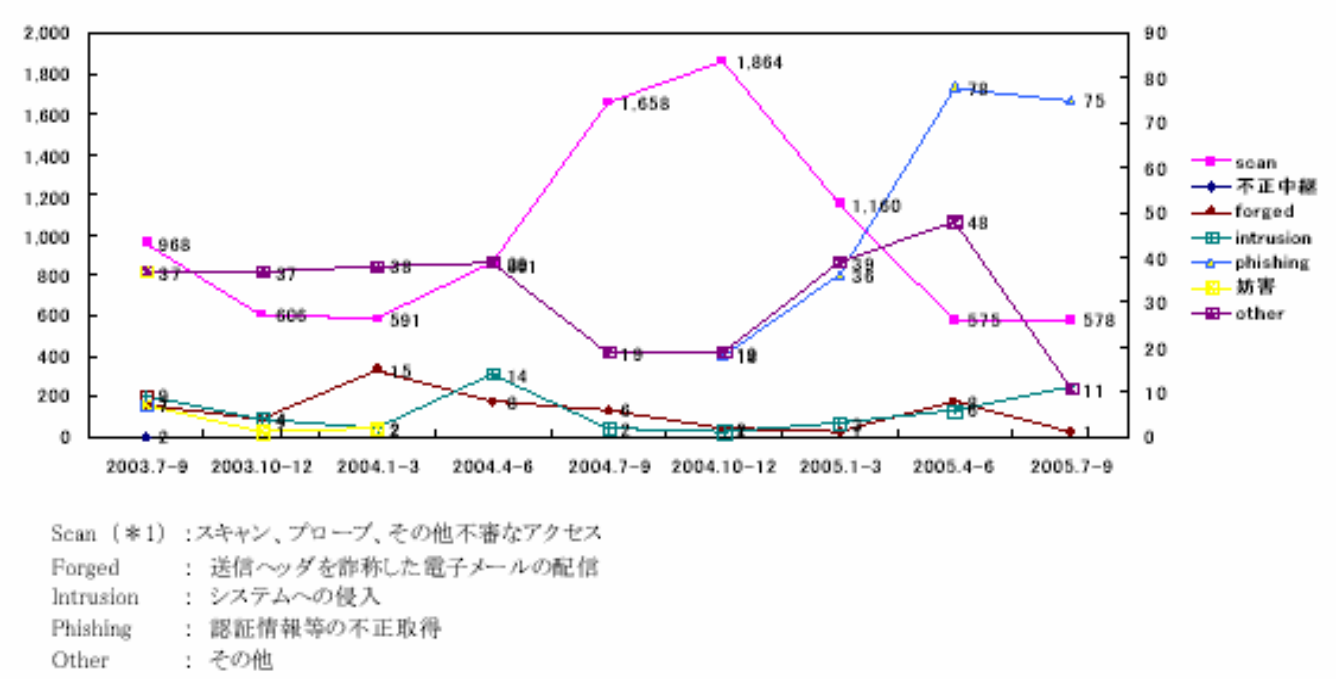
（3）　セキュリティ上の課題

(2)で述べたセキュリティ対策されているものもあるが、インターネットバンキングサービスは、スパイウェアや不正サーバを利用したＩＤ／パスワード詐取による不正決済脅威に晒されている。図６にアンチフィッシングＷＧのフィッシングの調査結果[29]を、図７に JPCERT/CC のインシデント発生件数の報告[30]を示す。米国、日本に関わらず、2004 年以降、フィッシングの件数が急増している。また、そのターゲットも、不正ビジネスに直結する金融サイトへのアクセスに集中している[29]。日本の銀行へのアクセスを想定したスパイウェア（トロイの木馬）も発見されている[31]。



出展：Anti-Phising Working Group:Phishing Activity Trends Report, July, 2005

図６　フィッシングの件数とそのターゲットアプリケーション



Scan（＊1）：スキャン、プローブ、その他不審なアクセス
Forged　：送信ヘッダを詐称した電子メールの配信
Intrusion　：システムへの侵入
Phishing　：認証情報等の不正取得
Other　：その他

出展：インターネットセキュリティに対する JPCERT/CC 2005 年第 3 四半期活動報告

図７　インシデント種類別報告件数

このように、インターネットバンキングがフィッシングのターゲットとなる理由として、パスワードや暗証番号といった利用者の記憶に頼った本人認証方式を採用していることが上げられる。(株) インフ

ォプラント「C-NEWS]と（株）UFJ 総合研究所が実施した共同調査[32]では、一人平均 4 枚のキャッシュカードと 2.8 枚のクレジットカードを所有しているにも関わらず､覚えておける暗証番号は 3.2 個までと、75%の利用者が複数のカードの暗証番号を同じにしており、また、約半数のネットバンキング利用者が、パスワードを他のサービスと共用している実態を明らかにしている。また、同調査によると、利用者に選択・管理が委ねられている暗証番号は、調査した半数近くが生年月日や、電話番号、住所など容易に類推可能な数字を使用しており、非技術的な攻撃に対する潜在的な脅威も示されている。

これらのセキュリティ脅威や、運用上の調査結果は、金融サービスにおいて利用者の記憶に基づいた本人認証方式のリスクが非常に高まっていることを示しており､このリスクへの対処がセキュリティ上、最も重要な課題となる。

このほか、利用者の所有に基づく本人認証方式は、所有物の複製が脅威となる。所有物の盗用も脅威となるが、盗難事故の発生は利用者が気付き易く、被害の発生を未然、もしくは、最小限に止めることができるため、複製脅威の方がより大きい。ATM 用の磁気カードの偽造を目的とした盗撮事件など、所有物の複製脅威の一例である。情報技術の進展により、複製のための技術が一般化しており、このリスクも高まっている。この対策も課題となる。さらに、所有物の借用・誤用の脅威もセキュリティ対策の課題となる。

６．２．３　　現行のインターネットバンキングのモデル分析

前節の調査の結果、現行のインターネットバンキングのモデル図を図８に示す。

インターネットバンキングシステムは、Web サーバとネットバンキングサーバから構成されており、Web サーバはインターネットに接続されてインターネットを介して利用者と接続されており、ネットバンキングサーバから勘定系システムへ決済処理を要求する構成となっている。

利用者は、利用者端末のプラウザから Web サーバの証明書を認証した上で、SSL により暗号接続し、ユーザ ID、パスワードにより、インターネットサービスのページにログインする。この際、既に暗号化通信されており、ネットワーク上は、安全にログイン情報を送信できる。また、Web サーバでは、インターネットバンキングサービス利用者のログインパスワードを管理し、このパスワードを照合する。さらにサービス画面で決済を伴う要求を実施した際に、決済用パスワードを入力・送信する。この情報も通信系路上は暗号化されている。ネットバンキングサーバでは、ID 毎に管理した決済用のパスワードと照合し、一致していれば、勘定系システムへ決済を要求する。

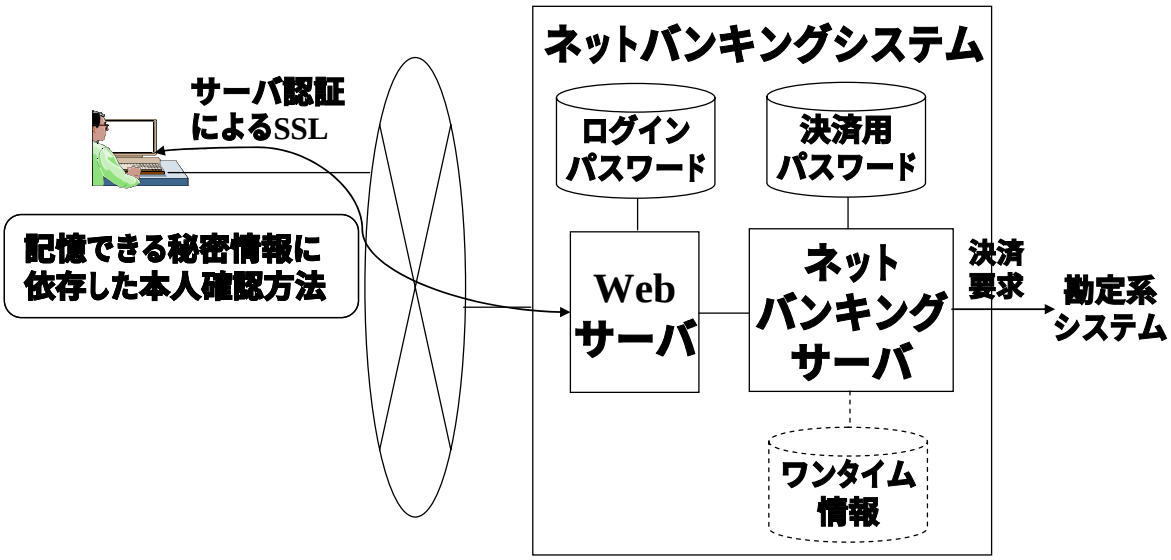


図８　現行のインターネットバンキングの認証モデル

ワンタイムパスワードの場合は、決済パスワードに代えて、ワンタイムパスワードの情報を利用者ごとに管理し、入力された情報を照合することとなる。この際、マトリクステーブル方式の場合は、入力に先立ち、入力要求する行・列の番号をネットバンキングサーバから Web サーバを介して利用者端末に通知する。

６．２．４　　インターネットバンキングの脅威抽出

前節までで、明らかにしたとおり、秘密情報の記憶や携帯物に依存した本人確認方法のため、フィッシングのターゲットとなり、不正引き出しの脅威が増大している。本節では、各認証方式ごとに脅威を明らかにして、それぞれの認証方式のリスクを示す。ここで、サーバ側の情報は、安全に管理されており、暗号も安全に運用されているものとする。

（１）第２パスワード方式

①利用者端末がスパイウェアに感染しており、利用者のパスワードが詐取されることにより、詐取者により不正に口座を操作されるかもしれない。

②インターネットバンキングサイトになりすました不正サイトへ誘導するメールより、不正サイトにアクセスし、利用者のパスワードが詐取されることにより、詐取者により不正に口座を操作されるかもしれない。

③利用者端末が指定している DNS がクラッカーにより攻撃され、IP アドレスのドメインネームが書き換えられることで不正サイトへ誘導され、利用者のパスワードが詐取されることにより、詐取者により不正に口座を操作されるかもしれない。

④利用者の入力画面や入力動作やメモから、利用者のパスワードが詐取されることにより、詐取者により不正に口座を操作されるかもしれない。

⑤利用者がパスワードを忘れたり、他のパスワードと勘違いしたりしたため、インターネットバンキ

ングが利用できなくなるかもしれない。
⑥①～④と同様に、利用者のパスワードが詐取されることにより、詐取者により不正にパスワードを変更されて、インターネットバンキングが利用できなくなるかもしれない。

利用者のセキュリティ意識を高めることにより、リスクを軽減できるが、クラッキング技術と対策技術は、いたちごっこの態を示しており、十分な対策を施しても、完全にリスクを回避できないと考えられる。

（２）マトリクステーブルによるワンタイムパスワード方式

本方式は、パスワードの管理を利用者に委ねず、システム側から指定することで、利用者が選択するパスワードの安全性に起因するリスクを回避でき、（１）の方式と比較すると、安全性の向上は期待できるが、以下のような脅威が残される。

①利用者端末がスパイウェアに感染しており、利用者のパスワードが**繰り返し**詐取されることにより、詐取者により不正に口座を操作されるかもしれない。
②インターネットバンキングサイトになりすました不正サイトへ誘導するメールより、不正サイトにアクセスし、利用者のパスワードが**繰り返し**詐取されることにより、詐取者により不正に口座を操作されるかもしれない。
③利用者端末が指定している DNS がクラッカーにより攻撃され、IP アドレスのドメインネームが書き換えられることで不正サイトへ誘導され、利用者のパスワードが**繰り返し**詐取されることにより、詐取者により不正に口座を操作されるかもしれない。
④利用者の入力画面や入力動作やメモから、利用者のパスワードが**繰り返し**詐取されることにより、詐取者により不正に口座を操作されるかもしれない。
⑤利用者のマトリクステーブルがコピーや書き写し（偽造）されて、別途、（１）の脅威により詐取されたパスワードを使って、不正者により不正に口座を操作されるかもしれない。
⑥利用者のマトリクステーブルが盗難・借用されて、別途、（１）の脅威により詐取されたパスワードを使って、不正者により不正に口座を操作されるかもしれない。
⑥利用者のマトリクステーブルが利用者の手元に無く、インターネットバンキングが利用できないかもしれない。

以上の繰り返し回数は、行・列数によるが、現状は、10×10 が一般的であるため、4 桁入力とすると、30 回程度の繰り返しですべてのカード情報が漏洩する。しかし、30 回の口座操作の実施が確認されないので、利用者が不正操作される前に不正詐取に気づくことができる可能性が高いと考える。

ここで、最も高いリスクは、⑤のマトリクステーブルの偽造であり、非常に容易であり、利用者が偽造に気づく前に口座の不正操作される可能性が高い。偽造に対し、盗用は不正操作される可能性があるが、盗難に早期に気付くことができ、不正操作を防止できる場合もある。それに対し、借用は利用者のマトリクステーブルの管理状況の隙をつくため、不正操作される可能性が高い。

（３）トークンによるワンタイムパスワード方式

①利用者のトークンが偽造されて、別途、（１）の脅威により詐取されたパスワードを使って、不正者により不正に口座を操作されるかもしれない。
②利用者のトークンが盗難・借用されて、別途、（１）の脅威により詐取されたパスワードを使って、不正者により不正に口座を操作されるかもしれない。
③利用者のトークンが利用者の手元に無く、インターネットバンキングが利用できないかもしれない。

以上で、①の偽造については、トークンの偽造対策や不正解析対策により、非常に低いリスクに軽減できる。

この中で、最も高いリスクは、借用による不正な口座操作であり、利用者が不正に気付くのが遅れ、被害金額を膨らむ可能性も考えられる。利用者のトークンの管理次第である。（利用頻度の高い利用者（週に数回以上）は、比較的に適切に管理され、また、早期に不正利用に気付き易いと想定されるが、利用頻度が低い利用者（月に数回以下）は、マトリクステーブルカードと異なり、携帯しない印鑑などと同様な管理となりかねず、また、不正利用に気付くのも遅れることが想定される。

６．２．５　　バイオメトリクス認証の要件

バイオメトリクス認証の適用により、本質的に ID の盗用や借用が困難となるため、従来の本人認証方法と比較して、なりすましによる不正口座操作のリスクを低下させる効果が期待できる。しかし、電子的な詐取による同様の脅威や、バイオメトリクスを採用するうえで発生するプライバシーなどの問題に対処する必要がある。そこで、インターネットバンキングへバイオメトリクス認証を適用する際の要件として、以下の４つを挙げる。

（１）バイオメトリクス認証の完全性の保証

スパイウェアの蔓延による脅威に対して、インターネットを介して、収集・処理されるバイオメトリクス認証処理の完全性をサーバに保証する必要がある。これは、ISO DIS19092-1 の必須要件でもある[3]。このため、利用者側の端末における通信データや入力データの詐取などによるリプライアタックに対し、対処する必要がある。また、利用者端末の安全性についてもサーバへ通知する必要がある。

（２）バイオメトリクス情報のプライバシーの確保

バイオメトリクス情報は個人同定可能な情報であるため、口座情報や氏名情報などと合わせたデータは個人情報となる機微情報である。このため、個人情報保護法の従って、バイオメトリクス情報の管理を徹底するか、あるいは、バイオメトリクス情報を利用者の手元で管理させる構成が必要がある[1]。

（３）可用性の確保

バイオメトリクス認証は、個々の特性により対応できない場合や、体調などで認識できない場合がある。サービスの可用性を確保する上で、別途、対策が必要となる。このため、従来の本人認証の代替させるのではなく、追加して組み込むか、複数種類のバイオメトリクス認証に対応する必要がある。また、この代替手段による認証によって、生じるリスクも適切に管理する必要がある。

（４）利用者側の装置認証とその利用（リスクに見合ったコスト）

バイオメトリクス認証では、各利用者端末にバイオメトリックセンサを追加せねばならない。この導入コストを金融機関が負担するのならば、従来の本人認証のリスクと比較して、適切なコストとならな

ければ、導入への障壁となる。一人当たり、4 枚のキャッシュカードを保有する状況[32]を考慮すると、この負担を各金融機関ごとに実施することは、非効率である。このため、利用者が既に所有するバイオメトリクスセンサを金融機関側で認証できる仕組みを導入し、バイオメトリック認証装置を様々な認証サービスに共有することが効率的であり、金融機関のコストも低減できる。よって、バイオメトリクス装置の認証するフレームワークが必要である。

６．２．６　　インターネットバンキングにおけるバイオメトリック認証モデル

インターネットバンキングにおいて、バイオメトリック認証を適用した場合の前提となる Web ページフローを図９に示す。

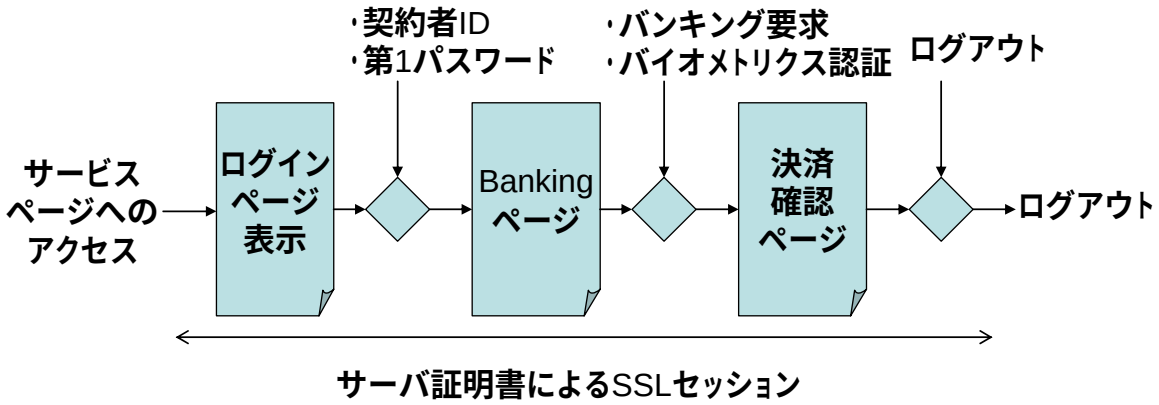


図９　バイオメトリクス認証の前提となるページフロー

従来の本人認証と同様にバンキングサービスへのログイン時と、決済時の 2 回の本人認証を実施する。ここで、①ログイン時と決済時の両方をバイオメトリクス認証で実施する、②ログイン時のみバイオメトリクス認証を実施する、③決済時のみバイオメトリクス認証を実施するの３つの組み込み方が考えられるが、同一認証方式に依存することによるリスクと、リスクの高いサービスにより安全な認証を実施させることを考慮し、③の決済時のみバイオメトリクス認証を実施する前提とした。

決済時のみにバイオメトリクス認証を実施する場合の認証モデルを図１０に示す。

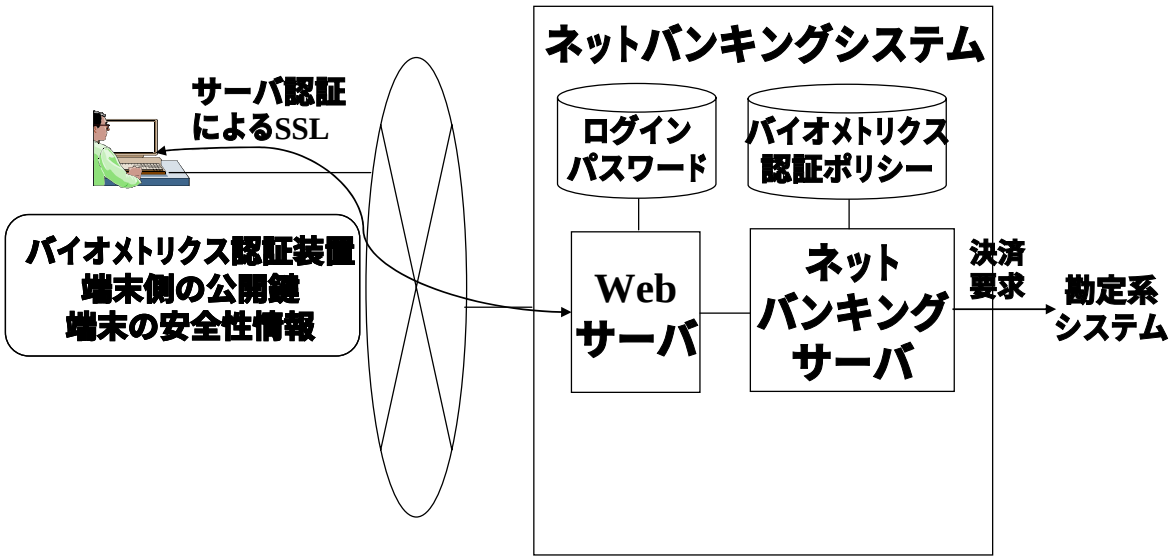


図１０　インターネットバンキングにおけるバイオメトリクス認証モデル

６．２．７　　インターネットバンキングにおけるバイオメトリクス認証モデルにおける脅威分析

本節では、前節で定義したバイオメトリック認証モデルにおける脅威を列挙する。ここで、ＳＳＬの暗号通信の安全性と、インターネットバンキングサーバの安全性は確保されていることを前提とする。

（１）クライアント端末が誤ったＷｅｂサーバに接続し、ログインパスワードが漏えいするかもしれない。

→利用者により、ＳＳＬ通信時に不正なサーバの証明書を確認による対策しかないが、要件（１）に従えば、決済確認は、バイオメトリック認証の結果、チャレンジレスポンスで通知する仕様のため、ログインパスワード漏えいのリスクは、低減できる。

（２）クライアント端末の脆弱性により、スパイウェアに汚染され、ログインパスワードが漏えいするかもしれない。

（３）クライアント端末の脆弱性により、スパイウェアに汚染され、バイオメトリック情報が漏えいするかもしれない。

（４）クライアント端末の脆弱性により、スパイウェアに汚染され、端末側の公開鍵情報（私有鍵）が漏えいし、攻撃者が成りすまされるかもしれない。

（５）クライアント端末の脆弱性により、漏えいしたバイオメトリック情報により、攻撃者にバイオメトリック情報を物理的に偽造され、成りすまされるかもしれしれない。

（６）クライアント端末の脆弱性により、バイオメトリックテンプレートデータが偽造され、攻撃者に成りすまされるかもしれない。

→要件（１）に従えば、クライアント端末から通知された安全性情報により、クライアント端末の安全性をインターネットバンキングサーバで判断することができる。ただし、この安全性情報の信頼性をどのように担保するのかが課題となる。要件（４）のクライアント端末の認証フレームワークが適切に構築され、要件（１）のチャレンジレスポンスにより、解決できると考える。

→個人情報保護の観点で、バイオメトリックテンプレートをバンキングサーバで持たず、クライアント側で処理を実施することで、プライバシーの要件（２）に対処できる。

（７） クライアント端末の脆弱性により、端末の安全性情報が書き換えられ、不正の情報をサーバに送られ、インターネットバンキングサービスの利用を阻害されるかも知れない。

→同じく、要件（４）のクライアント端末の認証フレームワークが適切に構築され、要件（１）のチャレンジレスポンスにより、解決できると考える。

（８） クライアント端末のバイオメトリック認証が失敗（ＦＲＲ）し、インターネットバンキングサービスの利用が阻害するかもしれない。

→要件（３）の可用性が確保されるように、利用者ごとに最適なバイオメトリクスを選択できれば、バイオメトリック認証の失敗による機会損失リスクを減らすことができる。しかし、完全に機会損失リスクを無くすことはできないが、要件（４）の利用者センサを採用することにより、機会損失リスクの原因を利用者センサへ移転することもできる。

本節で述べたように、本人知識や情報を利用した本人確認と比較して、情報の漏えいや盗用･借用によるなりすましリスクは大幅に低減できる。しかし、バイオメトリクス認証処理においても、脅威の発生はクライアント端末の安全性に依存するところが大きいことが判明した。そこで、クライアント端末の安全性を含めたセキュリティ対策処理を次節で述べる。また、バイオメトリック認証を導入することで、新たにＦＲＲやプライバシーなどの新たなリスクが発生することになるので、このリスクに対しても十分検討する必要がある。

６．２．８　　セキュリティ対策と効果

本節では、前節で明らかにした脅威に対して、クライアントの安全性についてのセキュリティ対策処理を含め、詳述する。

前提として、利用者端末には、バイオメトリクス認証装置が実装されており、サーバに対して利用者端末での処理の完全性を伝える公開鍵またはセキュリティ情報が格納する。さらに端末の安全性を通知するための情報を持つ。

一方、インターネットバンキングサーバには、従来同様の Web サーバとネットバンキングサーバが接続されている。ネットバンキングサーバには、各サービス提供元のバイオメトリクス認証に対するポリ

シーを定義して運用するための情報を持つ。

ここで、バイオメトリクス認証のポリシーとしては、例えば、以下の情報を持つ。

- サービスを提供を許可する利用者端末の認証装置の種類やソフトウェアバージョン
- バイオメトリクス認証の照合結果に要求する許容他人受入率
- バイオメトリクス照合の失敗時の許容される繰り返し回数
- バイオメトリクス照合失敗時において、該当する利用者のサービス停止時間（期間）
- 利用者端末に求める安全性情報

ここでのバイオメトリクス認証の処理は、次のようなフローとなる。

（１） 決済要求を受けたネットバンキングサーバは、決済内容により要求する許容他人受入率と許容する認証装置やソフトの情報を認証ポリシーにより決定し、チャレンジコードを生成し、利用者端末に SSL 通信下で送付する。

（２） チャレンジコードを受信した利用者端末は、ネットバンキングサーバから要求されたバイオメトリクス認証の処理を実行し、処理結果と端末プロファイル（バイオメトリック認証の処理情報と端末の安全性情報）に署名し、ネットバンキングサーバへ、SSL 通信下で返信する。

（３） ネットバンキングサーバは、クライアント端末から受信したデータの署名を検証し、バイオメトリック認証の慮離情報が認証ポリシーに合致しているか検証し、さらにクライアント端末の安全性がポリシーに合致していれば、決済処理を実行する。この際、信頼できる第三者期間による評価・認証情報に基づいて検証したり、クライアント端末の公開鍵の有効性を確認したりすることにより、クライアント端末の安全性の安全性を検証する。

以上の処理をまとめた処理フローを図１１に示す。

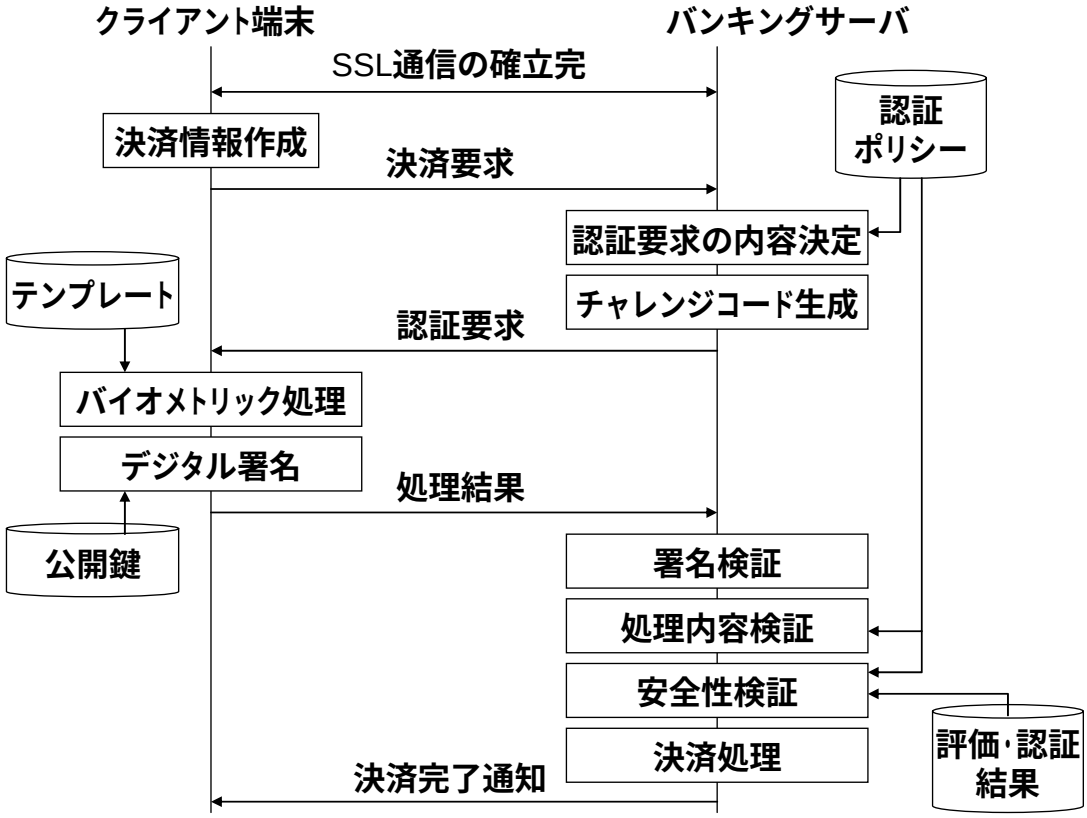


図１１　インターネットバンキングにおけるバイオメトリック認証の処理フロー

要件（と脅威）に対して、ここで、記述したセキュリティ対策の処理フローは、次のような対応関係がある。

（１）バイオメトリクス認証の完全性の保証

バイオメトリクス認証処理の完全性については、チャレンジコードとそのコードを含む認証情報について、利用端末の公開鍵（私有鍵）にて署名をすることにより、対策されている。ただし、ここで署名する鍵情報のやバイオメトリック処理情報の安全性について問題があれば、サーバ側では、利用者端末の処理が正当なものか判断できない。このため、利用者端末の安全性情報を含めて、サーバへ回答する仕様としている。

（２）バイオメトリクス情報のプライバシー

バイオメトリクス情報のプライバシーについては、このモデルでは、クライアント側でバイオメトリクス情報を照合するため、サーバではバイオメトリクス情報を管理しておらず、個人情報保護法の対象とならない構成となっている。ただし、クライアント側で実施するバイオメトリクス照合が正しく行われているかどうかは、（１）と同様に利用者端末の安全性情報に依存する。また、照合する参照テンプレートが本人のデータであることをサーバで認証できる必要がある。この情報も含めて、バイオメトリック情報と安全性情報をサーバに通知する必要がある。

（３）可用性の確保

可用性については、最終的にサーバ側の（バイオメトリクス）認証ポリシーに合致した認証手段によって、合致した照合スコアであれば、サービスを提供できる仕組みであるため、安全性が認証された認証技術であれば、どのような認証技術（バイオメトリクス以外でも）であっても対応できる。また、その条件によって、適切にリスクを管理できる。

（４）利用者側の装置認証とその利用

ここでは、登録時に利用者側の装置認証を行った上で、その場で参照テンプレートの登録を実施することを想定している。その際の認証情報と、テンプレート情報をサービス利用時のバイオメトリクス認証情報と、安全情報として送付するモデルである。しかし、サービス提供者である金融機関で利用者の装置の製品モデルの安全性を認証することは、現実的ではない。このため、信頼できる第三者機関で、安全性を認証された製品モデルの装置であることを確認することになると想定される。

しかし、クライアント端末や生体認証装置の安全性を認証するための第三者機関の評価スキームや運用フレームワークが現状では確立されていない。具体的には、これらの生体認証機能を持つクライアント端末について、ISO/IEC15408 に基づいた共通 PP を策定・確立し、この PP に準拠した製品モデルの ST について、3 章で述べた脆弱性を評価した上で、評価結果を認証する仕組みが必要となる。このために必要となる評価方法に関する標準規格の整備と運用フレームワークの確立が今後の課題となる。

６．３結論

６．３．１　　国際標準化の成果と今後の課題

（１）成果

①ISO TC68 DIS19092-1 の投票対応

ＩＳＯ ＴＣ６８国内委員会から要請されたＩＳＯ ＤＩＳ １９０９２－１の投票について、コメント付き賛成のコメントをまとめ、ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７ ＷＧ４国内委員会、専門委員会の承認の元、ＩＳＯ ＴＣ６８国内委員会へ提出した。この中で、日本で実用化が進む静脈認証技術についての技術紹介の記述が抜けているため、静脈認証技術に関する紹介文章の原案を作成し、英訳作業に協力した。本コメントに基づき、ＩＳＯ ＴＣ６８国内委員会で審議され、ＪＮＢから、コメント付き賛成として、投票された。

②ISO TC68 CD19092-2 の投票対応

ＩＳＯ ＤＩＳ １９０９２－１と同様に、ＩＳＯ ＴＣ６８国内委員会から要請されたＩＳＯ ＣＤ １９０９２－２の投票について、４ｔｈＣＤとする前提でコメント付き反対のコメントをまとめ、ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７ ＷＧ４国内委員会、専門委員会の承認の元、ＩＳＯ ＴＣ６８国内委員会へ提出した。本コメントに基づき、ＩＳＯ ＴＣ６８国内委員会で審議され、ＪＮＢから、コメント付き

反対として、投票された。

（2）今後の課題

金融業界の標準化団体であるＩＳＯ　ＴＣ６８の国内事務局を介した提案となるため、ＴＣ６８国内事務局主導の対応とならざるを得ない。このため、ＩＳＯ　ＴＣ６８にて立ち上がる標準化プロジェクトに対して、対案提出が主な活動となる。このため、標準化プロジェクトとして提案される課題を予想し、事前に検討することが必要と考える。本事業にて、Ｗｅｂバンキングについて、別パートとして分割するようコメントを行い、パート２から削除されており、将来、Ｗｅｂバンキングに関する標準化プロジェクトが成立する可能性が高いと、思われる。このため、今年度の事業において、インターネットバンキングに関して検討を行い、課題と要件、および、システムモデルを明らかにできたことは、今後の標準化活動に寄与できるものと思われる。今年度の事業の関係を継続し、ＩＳＯ　ＴＣ６８に対し、本活動の成果に基づき、ＩＳＯ／ＩＥＣ　ＪＴＣ１　ＳＣ３７を経由して技術協力を継続していく予定である。

６．３．２　　技術開発の成果と今後の課題

（1）成果

1）インターネットバンキングの適用状況の調査

インターネットバンキングにおけるバイオメトリック認証モデルの検討するために、現状のインターネットバンキングの適用状況と認証方式の調査を行い、報告書にまとめた。

2）インターネットバンキングの本人認証モデルとリスク分析

現状のインターネットバンキングの本人認証モデルを明らかにし、それぞれの認証方式ごとにリスク分析を行い、報告書にまとめた。

3）インターネットバンキングにおけるバイオメトリック認証の要件と認証モデルの検討

インターネットバンキングへバイオメトリクス認証を適用する際の要件を明らかにし、その要件に従ったバイオメトリクス認証モデルを明らかにした。さらに、この認証モデルにおける脅威を分析し、セキュリティ対策を施した認証フローを提示した。

（2）今後の課題

インターネットバンキングへバイオメトリクス認証を普及させるためには、金融機関がそれぞれのセキュリティポリシーに合致しているか、利用者の端末および生体認証装置を認証するフレームワークが必要となる。このための基盤技術として、3 章でのべた脆弱性評価方法の確立が重要であるとともに、第三者機関の設立が求められる。

６．３．３　　当初の目標に照らした達成状況とその要因

ＩＳＯ　ＤＩＳ１９０９２－１、ＣＤ１９０９２－２について詳細のコメントを提出し、ＪＮＢのコメントとして採用された。また、このコメント提案の結果、ウェブバンキングについては、別パートに

分けて標準化が進むこととなり、パート２から削除された。このため、将来的にＷｅｂバンキングに関する標準化プロジェクトが成立した際に、今回検討したインターネットバンキングに関する検討内容が国際標準化に寄与できるものと考える。このため、当初の目標を達成したものと考える。

６．４参考文献

[1] 平成１６年度経済産業省委託事業　基準認証研究開発事業　生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化　報告書
[2] ANS X9.84-2003(revision)：「Biometric Information Management and Security for the Financial Services Industry」, Accredited Standards Committee X9, Incorporated(2003）
[3] ISOTC68/SC2:ISO/DIS 19092-1 ”Financial Services – Biometrics – Part1:Security Framework”, (2005/08/24)
[4] ISOTC68/SC2/WG10:ISO/CD 19092-2 ”Financial Services – Biometrics – Part2: Message syntax and cryptographic requirements”, ISO TC68/SC2 N 1386c(2005/08/18)
[5] ITmedia Survey：「ネットバンキングを「利用している」のは 76.6％」, 2004/11/05, http://www.itmedia.co.jp/survey/articles/0411/05/news068.html
[6] 日経ＢＰ：「ネットバンキングの利用者が１年で倍増、首位にイーバンク」, 2004/11/08, http://www.nekeibp.jp
[7] 総務省：「平成 16 年度版　情報通信白書」, 総務省, 平成 16 年 7 月, http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h16/index.html
[8] Ipsos-Insight：「Retail Banks Threatened by Online Peyment Competition」, 2004/11/16, http://www.ipsos.na.com/news/pressrelease.cfm?id=2454
[9] 日経ＢＰ：「米オンライン・バンキング利用率、02 年から倍増の 40％」, 2004/11/18, http://www.nikkeibp.co.jp
[10] Ipsos Insight：「Concerns About Personal Information, Identity Theft, And Services Stall Growth According To Ipsos Insight’s Annual Online Banking Survey」, 2005/9/6, http://www.ipsos-na.com/news/pressrelease.cfm?id=2765
[11] 日経ＢＰ：「米国のオンライン・バンキング利用は過去 1 年横ばい、米調査」, 2005/09/08, http://www.nikkeibp.co.jp
[12] Nielsen//NetRatings：「Online Banking Reaches More Than 30 Percent of the Active Web Population in Five Countries」, 2003/1/8, http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-08-2003/0001868327&EDATE=
[13] 日経ＢＰ：「世界のオンラインバンキング利用状況、利用率トップはスウェーデン」, 2003/1/11, http://www.nikkeibp.co.jp/
[14] 米 Keynote Systems 社プレスリリース:「Online Banking Critical to Bank Selection and Brand Perception」, 2005/01/06, http://www.keynote.com/news_events/release_2005/05jan06.html
[15] 日経 BP ITPro：「『銀行の選択で重要なのは、支店や ATM の場所よりもオンラインバンキング』、米調査」, 2005/01/08, http://itpro.nikkeibp.co.jp/
[16] 三井住友銀行ＨＰ：「セキュリティ」, http://smbc.co.jp/koin/direct/faq/faq02.html
[17] 三井住友銀行ニュースリリース：「新セキュリティサービス『ワンタイムパスワード』の取扱開始について～“使い捨てパスワード”を用いた、より簡易な認証～」, 2006/01/12
[18] 三菱東京ＵＦＪ銀行ＨＰ：「セキュリティ」, http://direct.bk.mufg.jp/secure/index.html
[19] みずほ銀行ＨＰ：「ダイレクトＱ＆Ａ」, http://www.mizuhobank.co.jp/pda/qa/qa1.html
[20] 郵便貯金ＨＰ：「Ｑ＆Ａ」, http://www.yu-cho.japanpost.jp/service/ihs/s4040.htm
[21] ソニーバンクＨＰ：「セキュリティ情報」, http://www.sonybank.net/product/product05.html
[22] 足利銀行ＨＰ：「インターネット・モバイルバンキングセキュリティについて」, http://ashikagabank.co.jp/abk_f005a_1.htm
[23] 鹿児島銀行ＨＰ：「セキュリティについて」, http://www.kagin.co.jp/100_kojin/101_ebank/101_010.html

[24] 静岡中央銀行ＨＰ：「インターネットバンキングご利用の手引き」，http://www.shizuokachuo-bank.co.jp/eb/tebiki/index.html
[25] 殖産銀行ＨＰ：「セキュリティについて」，http://www.shokusan.co.jp/ibankaa/qa/qa003.html
[26] 松井証券ＨＰ：「セキュリティについて」，http://www.matsui.co.jp/policy/security/measures.html
[27] 野村證券ＨＰ：「認証やセキュリティＱ＆Ａ」，http://www.nomura.co.jp/hometrade/login/faq/qa_c02_08.html
[28] 日興コーディアル証券ＨＰ：「オンライントレードデモ画面」，http://www.nikko.co.jp/eztrade/demo/pc/index.html
[29] Anti-Phising Working Group：「Phishing Activity Trends Report, July, 2005」，http://antiphishing.org/
[30] JPCERT コーディネーションセンター：「インターネットセキュリティに対する JPCERT/CC 2005 年第 3 四半期活動報告」，2005/11/7
[31] シマンテック社 HP：「PWSteal.Jginko は、日本の特定のオンラインバンクのアカウント情報を盗み取るトロイの木馬です」，http://www.symantec.com/region/jp/avcenter/venc/data/pf/jp-pwsteal.jginko.html
[32] （株）インフォプラント（株），ＵＦＪ総合研究所ニュースリリース：「金融サービスのセキュリティに関する基礎調査」,2005/10/11，http://cnews.info-plant.com/press/press051011.pdf
[33] 星澤裕二：「基礎解説：フィッシング詐欺、いまさらフィッシング詐欺にだまされないために」,（株）セキュアブレイン，2004/12/25，http://www.atmarkit.co.jp/fsecurity/special/54phishing/phishing.html
[34] 日経ＢＰ ITPro：「pharming（ファーミング）――オンライン詐欺は「釣り」から「農業」へ？」，2005/09/15，http://itpro.nikkeibp.co.jp/
[35]日経ＢＰ ITPro：「個人情報漏えい事件を斬る(10)：社内だけでは防げないフィッシング詐欺の脅威」，2005/02/10，http://itpro.nikkeibp.co.jp/
[36] 南優人／Infostand：「フィッシング：キーロガー、スクリーンショットを使う手口が増加」, 2005/0824, http://hotwired.goo.ne.jp/news/print/20050824304.html
[37]日経ＢＰ ITPro：「オンラインバンキングは身元詐称による被害を減らすことができる」, 2004/04/07, http://itpro.nikkeibp.co.jp/
[38] セコムトラストネット（株）HP：「不正に ID/パスワードが利用される！」，http://www.secomtrust.net/secmeasure/password/column1.html