〔資　料〕

サイバー空間におけるセキュリティとは何か
―CIA の三要素―

福　井　幸　男

Ⅰ　はじめに

筆者は2010年12月に『情報システム論入門－社会を守る暗号セキュリティ編』（日科技連）を刊行した。その第 6 章「認証」についての補録である。

Ⅱ　識別と認証

2-1　ネットワークビジネスの初めに認証ありき

サイバー空間といわれるインターネット社会では、互いに見知らぬ同士での取引が頻繁に行われる。互いに相手を確認しあうことがすべての取引の前提となる。これが実は難しい。互いに顔なじみであれば、問題はないが、顔を見たことも話したこともない相手との取引となれば、万全の体制で臨まなければ安心できない。まさしく、板倉・外川（2010）が『ネット社会と本人認証』冒頭に述べているように、「相手がだれであるかを正しく識別し間違いなく本人であることを認証することは、情報セキュリティの出発点と言われる。確かに不特定多数の人間と関わりあう世の中において、安心して生きていくには、まずお互いの氏素性を相互に確認し合えること（筆者下線）」がサイバー空間上の取引の大前提となっている。

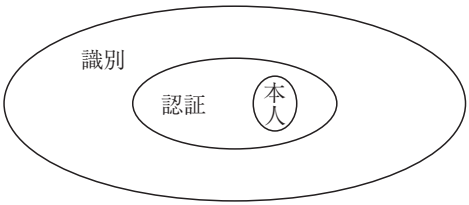
まず、識別（*identification*）と認証（*authentication*）の違いをまず説明したい。これらの用語は、情報システムに限らずありとあらゆる分野をカバーし

ている。人間や組織そして製品まで及ぶ。日ごろ使っている ID カードとは、identification card の略であり、動詞形 identify とは英和辞書先頭に「確認する」の意がある（研究社）。次に、authentic は、ギリシャ語を語源とする言葉であり、「オリジナル」あるいは「本物の」という語義がある。たとえば、使用例文として、「このブランドものは本物（authentic）か贋物（fake, counterfeit）か」などで使われる。さらに、つぎの単語が頻出する。Authentic bill（真札）、authentic copy（正本）、authentic data（確かなデータ）、authentic document（署名や捺印のある証書）、authentic feeling（嘘偽りのない気持ち）、authentic information（確かな情報）、authentic Japanese cuisine（本格的日本料理）、authentic signature（本人の署名）、authentic reproducts（本物を忠実に再現した製品）、authentic history（正史）。まさしく、authentic とは、語義通り、第三者が本物であると認めるニュアンスがある。

本稿で扱う識別および認証の対象を個人に限定する。識別（*identification*）と認証（*authentication*）の違いをまず説明したい。識別とは、多くの人物の中から本人を見つけて区別することを言う。そして、認証とは、識別された人物を本人かどうか検証（verify）することを言う。識別の段階では、1：n の照合であったが、認証の段階になると、1：1 のマッチングの確認を行う（板倉・外川）。

つぎの図 1 が参考になる。

図 1　本人の識別と認証



出所　板倉・外川 p. 3

2-2　識別と認証の実例

また、つぎの例は非常にわかりやすい例であろう。

⑴　ネットワークにつながったコンピュータを使いたい場合、まず、本人に「ユーザー ID」ナンバーを入力させて、ネットワーク内に登録された数多くの ID ナンバーの中から入力された ID ナンバーを識別（照合して探す）する。次に、本人に「パスワード」を入力させて、本人の事前登録したパスワードとの認証(マッチング確認)を行う。

⑵　新生児の入籍

赤ちゃんが生まれると当該市町村役場に、出生届を提出する。新生児の氏名、嫡出子かどうか、出生年月日と時刻、生まれた場所、住所（父母の住民登録地)、父母の氏名、生年月日、同居年月日、本籍地を登録する。出生届けは赤ちゃんが戸籍に入る手続きである。戸籍に赤ちゃんの名前、生年月日、住所そして性別が記載され社会の一員としての識別が完了する。次に、不正な登録を防ぐために、認証段階として、出生証明書（出産に直接かかわった医師や助産婦の署名捺印）が不可欠である。これで本人認証が完了する。

⑶　婚姻、離婚、認知そして養子

婚姻届および離婚届においては、20歳以上の証人 2 人の署名押印が必要である。死亡届の場合には、医師または歯科医の死亡診断書ないし医師の死亡検案書が必要である。子供の認知の場合、⑴血のつながった親子関係では、認知届を出す。父親が子供を認知するのに、母親の同意は不要であるが、子供が胎児のときは母親の同意が必要。子供が成人している場合は、子供本人の同意が必要。父親が認知を拒否した場合は、裁判所の確定証明書が必要。⑵血のつながっていない親子関係の場合、法的な親子関係になる養子縁組届では、20歳以上の証人 2 人の署名押印が必要である。

⑷　入国審査

外国人が日本に入国するには、パスポートとビザを提示した上で、顔写真と両手人差し指の指紋画像を提供して登録される。これが本人識別である。日本在留の外国人が日本再入国の際には登録された情報と本人をつきあわせ

て本人認証を行う。顔写真や指紋を拒否した場合、退去を命じられる。

⑸ 署名と捺印

役所での書類提出に際しては、まず署名をさせる。これは私本人は他人と違うという識別作業である。つぎに実印を使って捺印させることは、私は本人ですという認証機能を持つ。なお、認印は実印（印鑑登録）とは違う。

2-3 NCSC の定義

アメリカ国防総省傘下の NSA の下部組織 NCSC（National Computer Security Center）は、軍用調達のためのコンピュータ製品評価基準を設定して、軍事用 IT 製品のみならずアメリカ政府が調達する IT 製品を評価している。評価基準として、セキュリティを守るための識別と認証の標準仕様を規定する。NCSC ガイドライン（1991）において、「NCSC の目的は、TCS（trusted computer system；信頼すべきコンピュータシステム）の利用普及を奨励する点にある。NSCS は、TCS を評価する基準として、国防総省 TCSEC（Trusted Computer System Evaluation Criteria）を設定した。このガイダンスは、TCSEC にあわせて各ベンダーが、自社製品に対して識別と認証のメカニズムをシステムとして設計し組み込むかについての仕様に関するガイダンスである。さらに、ベンダーや評価者に対してこの識別と認証に関する条件を良く理解してもらうことも本ガイダンスの目的である（文節 1.0）」。TSC の定義として、「そのシステムとは自社データをより強力に保護するものである（文節 FOREWARD）」。さらに、「識別と認証は密接不可分であって、識別とはユーザが誰（グローバルに知られている）であるかという言明であり、認証とは識別の証明である。そして認証はこの識別を検証する過程である（文節 2.0）」と述べている。なお、詳細な必要条件のレベルとして、C1, C2, B1, B2, B3, A1 を掲げてこの順にセキュリティレベルが高くなっている。

2-4　識別と認証のステップ

この識別と認証のステップは、次の図２のようにして進む。

図２　識別・認証のプロセス

⑴ID 登録→　⑵個人識別→　⑶本人認証→　⑷属性認証
（基本的認証）　（付帯的認証）

⑴　ID 登録：社会生活の中では、個の存在がまず尊重されなければいけない。そのためには、個人は生まれた瞬間に、氏名、住所、生年月日そして性別の４種類の情報が役場に届けられて、戸籍簿に登録される。個人識別の基本情報となる。なお、ID として、氏名・住所・生年月日・性別の４情報の他に、電話番号、会員番号、メールアドレスそしてニックネーム（芸名や偽名）がある。

⑵　個人識別：登録しているすべての ID と、今回示された ID をつき合わせて、マッチングする。1：n の照合作業から唯一のマッチングを探す。n 人のなかから一人を探す。

⑶　本人認証：ID 登録以外に登録された個人情報とのつき合わせから確かに本人に間違いないと認定する。1：1 の照合である。

⑷　属性認証：本人認証という基本認証が終わった後で属性情報を活用した付帯的認証が始まる。属性（attribute）とは、ユーザの職責、資格、地位などである。たとえば、本人認証が終わったとしても、それだけではインターネットショッピングの取引は完了しない。クレジット番号や氏名、送り先住所などの属性情報を与えないといけない。つまり、本人であることを証明するに十分な、本人しか持ちえない情報を与えないといけない。免許証や健康保険証、パスポートは属性であるが、出身地や飼い犬の名前は本人属性にはならない。該当者が多数存在するからである。

2-5　属性情報

本人認証が完了した後で、本人の持つ権限によってアクセスの可否を決定

したい場合がある。たとえば、部長以上にのみアクセスを許可する場合がある。ユーザの年齢や住所によって表示するデータを変えたい場合もある。ユーザの属性によってシステムの振る舞いを変えるために、ユーザの属性を確認することを「属性認証」という。

属性の分類法としてつぎのようなものがある。

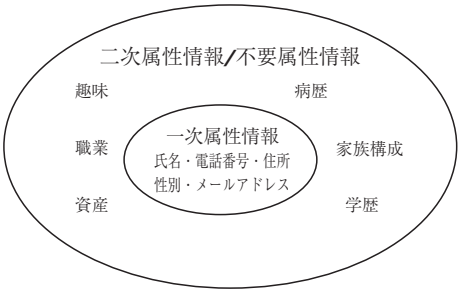
⑴ 時間的に安定しているかどうか。
- ・安定している属性：生年月日、生体情報、学歴、職歴
- ・ほぼ変わらない属性：資格、免許、職業、住所
- ・変化しやすい属性：所属、職責、権限、ランク、資産

⑵ オープンかどうか
- ・オープン：住民基本台帳情報、商業登記情報、資格、免許
- ・クローズ：所属部門、職責、権限、会員資格

⑶ センシティブかどうか
- ・知られたい：氏名、会社名、資格、免許、受賞
- ・知られたくない：戸籍情報、住所、電話番号、経歴、罰、診療記録、成績、年収

⑷ 必要かどうか
- ・コミュニティやサービスに共通の情報（一次属性情報）
- ・コミュニティやサービスで必要な情報（二次属性情報）

図３ 一次属性情報と二次属性情報



出所）電子商取引推進協議会他、 p. 31

・コミュニティやサービスで必要としない情報（不要属性情報）

一次属性情報と二次属性情報を図示したのが図３である。
以上の議論をまとめるとつぎの表１となる。

表１　識別・認証の段階と利用属性

段　階	目　　的	利用する属性
識別	母集団から特定の１人を選ぶ	一次属性情報
基本的認証	本人が事前に提供した情報とアクセス時に入力した情報の照合	二次属性情報
付帯的認証	アクセス時の本人の属性によってアクセス権限を与えてシステムを操作させる	二次属性情報

注）電子商取引推進協議会他、P. 31 を一部改変している。

2-6　個人認証の方法

個人を特定する認証のやり方には、つぎの三種類がある。
① 本人が知っているもの（記憶：*something they know*）
② 本人が持っているもの（所有物：*something they have*）
③ 本人に存在しているもの（身体的特徴：*something they are*）。

順次検討する。まず、①の記憶では、パスワードと秘密鍵が現在の有力な二大情報である。暗証番号（PIN）はパスワードの一種であり、４桁数字に限定している。パスワードを忘れた場合、インターネットのサイトでは、本人や家族のプライバシー情報（母親の旧姓など）を聞いたり、好物の名前を聞いたりしている。事前に登録していたデータと一致していたならばパスワードを再発行する。NCSS（1991）において、最終章ではパスワードを条件付ではあるが非常に利便性が高いものとしていることは興味深い。

②の所有物では、古来から日本では印鑑が使われてきた。８世紀の大宝律

令では朝廷の許可のもとで公印制度が制定されてた。さらに、時代はさかのぼって明治に入ると、1887年に印鑑登録制度がスタートした。民事訴訟法第228条１項で「文書は、その成立が真正であることを証明しなければならない。」としたうえで、４項で、「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。」とある。他に、部屋の鍵、身分証、登録証、カードなどがある。

③の身体的特徴とは生体認証である。指紋、虹彩、静脈、声紋、DNAそして最近では、歩き方や座り方が研究されている。顔認証も進んでいる。本人の唇上部中央と、両目外側を結んだ逆三角形を基点に顔の特徴をデジタル的に解析する。髪型は変わるから本人認証の手段にはならない。手書きの署名も金額が大きくない場合は有効な方法である。③は、①の記憶や②の所有物のように忘却や紛失の恐れがなく、しかも偽造の恐れが極めて少ないことからセキュリティ的に優れている（小松・明石）。

直接本人を知っている場合はいざ知らず、知らない場合には、たとえばカードを持っているから本人と決め付けてよいかというと、これは難しい。サイバー空間では特に難しい。どうするのか。次節以下で検討する。

Ⅲ　情報セキュリティの三要素の保護

3-1　通信の守られるべき三種の正義

そもそも通信とは、「信（よしみ）を通わす」という語義を持つ。信頼した人間同士の意思の疎通と解すれば、それは人間の歴史の最初から登場したことであり、それなくして人間の社会は成立しえなかったであろう。言葉が人間同士の意思疎通の重要な手段であった。ところが、互いが場所的に離れていて互いに直接言葉を交わしての、顔の表情を見ての意思疎通が難しくなったとき、通信が登場してきた。Telecommunication（通信）とは、遠くにあるという「tele」と、伝達するという「communicate」といういずれもラテン語に由来する。

テレコミュニケーションの時代のなかで、通信には守られるべき次の三種の概念が存在すると思われる。

①機密性（*confidentiality*）：英語の「not read」の意である。不正に読み取られない、つまり、悪意のある第三者に通信が傍受されても内容がわからないこと。

②完全性（*integrity*）：英語の「not written」の意である。不正に書き込まれない。つまり、正真正銘であることである。送信データと受信データの完全一致が確認できること。改ざんを阻止しなくてはいけない。

③認証性（*authentication*）：送信者が確かに本人と確認できること。なりすまし（spoofing）を排除しなくてはいけない。

これらはいずれも送信者にとっても受信者にとっても守られるべき当然の特性であり、万が一損なわれた場合大きな影響をうける可能性がある。平凡社の大百科事典にしたがって正義とは「人間の行為を、正しい、正しくないというように判断するための基準」であるとすれば、これらの特性はまさしく通信の守られるべき正義と解釈することができよう。さらに同事典によれば、アリストテレスの正義論で語られる正義とは「均等的、＜価値に相応の＞ということであり、不正とは不均等的、＜過多をむさぼる＞こと」とした。さらに、正義を配分的正義と矯正的正義に二分して、後者の矯正的正義とは「取引の均等とか罪と罰の均等」を意味し、不正な取引で一方が損し他方が得することのないように、また、罪を犯した場合は罰することで均衡させるとした。

具体的な法的正義の形として、機密を侵害した場合、メッセージを改ざんした場合そしてなりすましをした場合には、直接処罰するのである。機密を盗み見た場合には、不正アクセス罪、改ざんでは、電磁的記録不正作出罪、なりすましでは詐欺罪や業務妨害罪が適用される。以上の三種類の概念の正義が守られてこそ、通信が日常世界の安全で信頼すべきインフラとして成立する。

3-2 情報セキュリティの三要素

つぎに、類似の概念として情報セキュリティの三要素がある（電子商取引推進協議会）。頭文字をとって、情報の CIA と呼ばれる。

① 機密性（*confidentiality*）：情報にアクセスすることが認可されたものだけがアクセスできることを保証すること

② 完全性（*integrity*）：情報および処理方法の正確さおよび完全である状態を安全に防護すること

③ 可用性（*availability*）：認可されたユーザのみが、必要なときに情報および関連財産にアクセスできることを保証すること

通信の正義の三要素と、情報セキュリティの三要素では、3 番目が異なる。前者の認証性の代わりに、後者では可用性が入っている。セキュリティ対策として、機密性と完全性は誰しも納得できる概念であるが、これらのみが重視されれば、情報システムの存在自体を損なうものと言える。情報の語源である「飛報軍情」の通り、戦場の様子を味方にいち早く知らせるという意味からしても、情報システムとしては、時間的な速さの意味を持つ可用性ははずせない。必要な情報への迅速なアクセスが滞ることなく利用できることが望まれるわけである。情報セキュリティの場合、大事な情報を金庫に閉まったままで、取り出す事務が煩雑であれば、情報は有事に役に立たない。大事な金庫が開かずの金庫であってはいけない。何度も金庫を開け閉めする手間を惜しんで、だれかが重要書類のコピーを取って机上においておけば機密性が失われ、それを元にデータの書き換えが進めばどれが正真正銘の情報かがわからなくなる。完全性に疑問が出てくる。あるいは最近問題になっている DoS（Denial of Service）攻撃によってサーバーの処理能力が一時停止しメールの送受信ができなくなれば、これも可用性を失ったことになる。

前者で独立していた認証性はどこに入ったかというと、後者の機密性に包含されたのである。情報にアクセスできるかをまず識別・認証して、認められない者にはアクセスを認めないという意味である。情報セキュリティの機密性とは、暗号通信の機密性よりも概念がより拡大しているとみてよい。

以上の情報セキュリティのCIAの概念が守られてこそ、通信が日常世界の安全で信頼すべき（trusted）インフラとして成立する。このインフラを守る盾が法律である。しかし、現行の法律体系では、情報セキュリティの概念をベースとは認識していず、整合的総合的関係にはいまだいたっておらず、不正アクセス禁止法や電磁的記録不正作出罪などの個別対応の域から脱していない。これには理由がある。元々法律は有体物を保護の対象としてきた。すなわち、わが国の法律は明治時代に枠組みが出来上がり、有体財の保護を中心に法制度が組み立てられてきた。ところが情報のような無体財の場合、知的財産制度を除いて、独占が認められていない。憲法第21条の「表現の自由」の含意としては「情報の自由な流通」を保障するものと解釈されている。個人のプライバシーの侵害を除いて、原則は守られてきたのである。

Ⅳ　サイバー空間における識別・認証

2-6節で述べた本人認証のための三種類の属性のなかで、サイバー空間での認証によく使われているのは、①の知識属性である。とくに最もよく使われるのが、パスワードによる認証および公開鍵暗号による認証である。つぎの4種類がある。(a)固定パスワード認証、(b)ワンタイムパスワード認証、(c)チャレンジ＆レスポンス認証、(d) PKI認証。

(a)の固定パスワード認証は、本人しか知りえない予め決めたパスワードを使って、最も普及している認証技術である。(b)は使い捨てパスワードを使うのでセキュリティの低下を防ぐことができる。(c)は認証サーバから送信されてきたランダムな数値（チャレンジ）に対して、本人がパスワードとチャレンジにある関数をかけて求めた数値（レスポンス）を認証サーバにまず送る。同時に認証サーバ側は登録されているパスワードとチャレンジから同じアルゴリズムでレスポンスを計算する。両者が一致すれば、パスワードは正しいとして認証する。万が一、通信途中で盗聴されたとしても、使われる乱数が毎回違うのでパスワードの推測は難しい。(d)のPKI認証は、PKI（Public Key Infrastructure）による認証である。公開鍵暗号方式を用いた基盤を意味

する。

V　PKI 認証の流れと通信の三種の正義の関係

以下では、通信の三種の正義の視点から、PKI に基づいた情報通信の流れを説明する。ハッシュ関数、MAC 関数そしてデジタル署名という三種類のトリックを用いている。本章では、２枚の図を使って、その概略を説明する。詳しくは拙著を参考にされたい。通信の三種の正義概念を埋め込んだ図を作成している点が新しい工夫である。

まず、つぎのような状況場面を前提に説明する。登場人物は、花子と太郎である。サイバー空間において、花子は「100万円を私の口座に入金してください」と太郎に依頼する。メッセージを受け取った太郎はどうするか。太郎の立場からは、本当に花子が発信者なのか、あるいはメッセージ自体は正当なものなのかと気がかりである。花子は認証して欲しい人、太郎は認証する人となる。

5-1　ハッシュ関数

メッセージを受信する場合に、それが正真正銘のものかどうかを判断しなければいけない。通信の完全性の担保である。もしも改竄があるならばビジネス上の被害は避けられない。平文のメッセージをハッシュ関数というある計算手順で暗号化して、ハッシュ値に変換する。平文が同じならば、ハッシュ値は同じになる。平文が異なれば、ハッシュ値も異なる。花子は平文とハッシュ値を同時送信する。太郎は、平文からハッシュ値を計算して、送信されてきたハッシュ値と同じならば、平文は改竄されていないと確認できる（図４参照）。

5-2　MAC 関数

メッセージを受信する場合に、それが正当な発信先からのものかどうかを判断しなければいけない。もしもなりすましであるならばビジネス上の被害

は避けられない。ハッシュ値を使えば、通信の完全性を担保できる。しかし、送信者自身の認証性は担保できない。送信者以外の誰かが「本人になりすましている」可能性を排除できない。

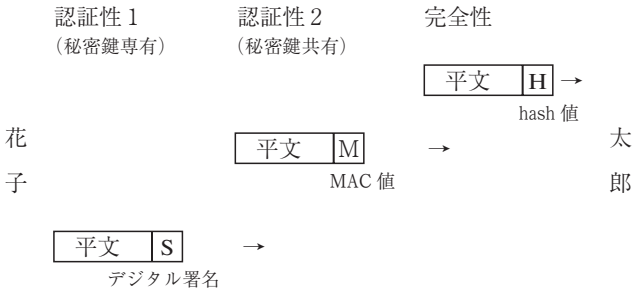
なりすましを防止する手立てがMAC関数（message authentication code, メッセージ認証コード）である。MAC関数は、メッセージの送信者が受信者と共有する鍵を使って固定長ビットの数値（MAC値）を計算する関数である。ハッシュ関数はハッシュ値を計算する際に鍵を使用していない。これに対して、MAC関数では、共有鍵を使う。これとメッセージをひとまとめにダイジェストするから、共有鍵を持たない人はMAC値を計算できない。メッセージが一文字でも変わるとハッシュ値も変わるように、MAC値も変わる。かくして、認証性が担保できる。

しかし、厄介なことに共有鍵を使ってもなお問題点は残る。第三者に対して、送信メッセージが花子のものとは証明できないのである。二人とも共有鍵を持っているから、双方が同一のMAC値を計算できる。当事者以外には真相はわからない。

5-3　デジタル署名

そこで、この問題を解決する手だてとして、公開鍵暗号の発想を活用する。花子は「100万円を私の口座に入金してください」というメッセージに加えて、このメッセージを自分の秘密鍵で暗号文にしたものを太郎に送付する。そもそも秘密鍵で暗号化するという行為自体が秘密鍵を持っている人しか実行できないから、花子本人の「署名」として見てよい。つぎに、太郎は受け取った署名を花子から送ってきた公開鍵で解読する。署名から解読したメッセージと送信された平文メッセージが一致していると認めるならば、太郎はこのメッセージの署名者は花子と認証する。公開鍵であるから太郎だけでなく第三者も検証できる。ここがデジタル署名の強さ。もしも、解読したメッセージと送信メッセージが違えば、正しく復号化できていないと判断して、花子のメッセージではないと判断する。

図 4　通信の三種の正義 (1)



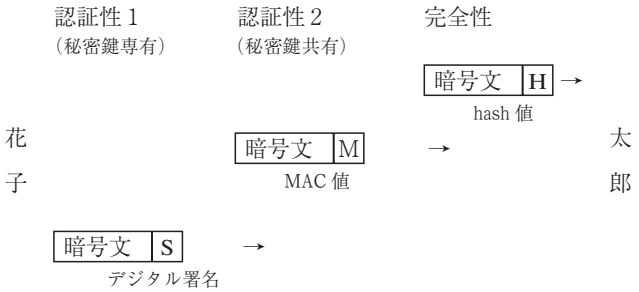
たとえ花子が「そんなものを書いた覚えがなく、太郎が自作自演した」と否認しても、この主張をしりぞけることができる。

図 4 の説明として、平文にハッシュ値を加えて送信することでメッセージの完全性を担保できる。平文に MAC 値を加えて送信することで認証性は確認できる。MAC 関数の場合、花子も太郎も鍵を共有している。認証性の後の 2 は二人の意味である。しかし、共有は万事問題が多いので、花子しか知らない秘密鍵で平文をデジタル署名したものを付加して送信する。これで認証性は担保できる。認証性の後の 1 は一人の意味である。

なお、実際の処理手順として花子のメッセージ全体をデジタル署名すると時間がかかりすぎる。そこで、メッセージのハッシュ値をまず求め、このハッシュ値をデジタル署名する便法がとられることがある。

図 4 では花子は平文をそのまま流している。これでは機密性は保てない。そこで、図 5 では、花子は平文自体を秘密鍵で暗号化している。太郎は花子の公開鍵で元に戻す。手間はかかるが、セキュリティ確保の観点から取られる措置である。

図５　通信の三種の正義（2）



以上、拙著で詳述できなかった側面を中心に、本人識別と本人認証についての解説を試みた。

（筆者は関西学院大学商学部教授）

参考文献

板倉征男・外川政夫（2010）『ネット社会と本人認証―原理から応用まで―』電子情報通信学会

小松尚久・明石正則（2005）「ネットワークへの脅威に対して情報の機密性で安全を保つバイオメトリック認証技術の現状と今後の課題」『*IAjapan Review*』Vol. 5, No. 3

電子情報通信学会（2004）『情報セキュリティハンドブック』オーム社

電子商取引推進協議会・財団法人日本情報処理開発協会電子商取引推進センター（2005）「属性認証ハンドブック：平成16年度 EC 技術基盤の相互運用性に関する調査研究」

福井幸男（2010）『情報システム論－社会を守る暗号セキュリティ編－』日科技連

NCSC（1991）“*A Guideline to Understanding Identification and Authentication in Trusted Systems*”, NCSC-TG-017