Vol.2011-CSEC-54 No.9
Vol.2011-SPT-1 No.9
2011/7/12

本人認証における信頼の考察

鵜野幸一郎[†]　桝野隆平[††]

安全と安心の双方を充足することは信頼にとって欠かせない条件と考えられる．安全・安心マトリックス上の「非安全・安心」「安全・非安心」象限をそれぞれ優良誤認，劣位誤認と捉え，本人認証技術に関する誤認識を例にとって考察する．優良誤認及び劣位誤認を低減するため，産官学メディアにより国民を啓発することが，技術への信頼を向上させ，安全・安心なデジタル社会の定着に寄与すると考える．

Viewing credibility of personal verification techniques

KOICHIRO UNO[†]　RYUHEI MASUNO[††]

Satisfying both SAFETY/SECURITY and SENSE OF SAFETY/SECURITY is the prerequisite for establishing TRUST. We propose to analyze the cases of Lack of SECURITY + Sufficiency of SENSE OF SECURITY and Sufficiency of SECURITY + Lack of SENSE OF SECURITY in our hope that it will help establish TRUST for cybersecurity.

1. はじめに

安全・安心な情報社会の発展と維持のためにはセキュリティ技術に対する利用者の信頼を獲得し維持することが不可欠である．

安全とは，危険がないことの客観的な状態であり，安心とは，危険がないことを自ら納得しているという主観的な心持ちのことをいうとすれば，客観的な安全と主観的な安心の双方を充足することが「信頼」を得るための必須条件と考えられる．

[†]日本セキュアテック研究所
Nihon SecureTech Labo.
[††](株)ニーモニックセキュリティ
Mnemonic Security Inc.

本論文では，この安全・安心を４象限のマトリックス　に区分けし，「信頼」の実現にとって問題となる「非安全・安心」「安全・非安心」の象限をそれぞれ「優良誤認」「劣位誤認」と捉え，本人認証技術に関して幾つかの事例を考察しながら，そうした誤認の起こる原因とそれによって引き起こされる問題点及び解決策を論じる．

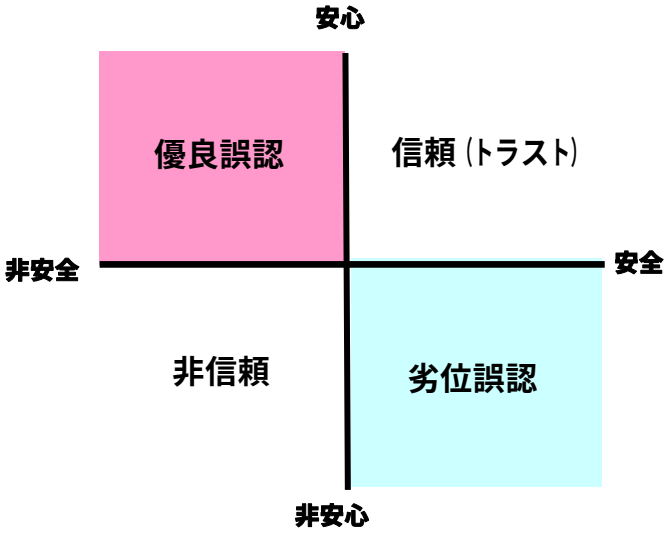

図１　安全・安心マトリックス

２．「安全・安心」４象限の示す意味

安全の度合いを横軸に，安心の度合いを縦軸にとってマトリックスを作ると，「安全・安心」「非安全・安心」「非安全・非安心」「安全・非安心」の４象限が区分される．これらのうち，「非安全・安心」と「安全・非安心」に位置づけられるものが「信頼」の形成と維持にとって大きな問題となる．

図１の「非安全・安心」の象限は，実際は安全でない製品・サービスにも拘わらず安心の心持ちで当該製品・サービスを利用する状況を示す象限で，「優良誤認」（用語の所以については次項に記述）を形成する．安心だと思い込んでいた製品・サービスが，実は非安全な製品・サービスだったということは著しく信頼を阻害するものであり，利用者側の誤解によって「優良誤認」が発生している場合は適切な理解を促すこ

Vol.2011-CSEC-54 No.9
Vol.2011-SPT-1 No.9
2011/7/12

とが要請される．とりわけ，医薬品，自動車のブレーキ或いは情報セキュリティ製品・サービスなどといった国民の生命・財産保護に関わる製品・サービスに関してはなおさらである．

その対隅が「安全・非安心」の象限であり，実際は十分安全な製品・サービスであるにも拘わらず，安心感がもてないあまり当該製品・サービスの利用を遠ざけがちになる状況を示す象限である．優良誤認の正反対なので「劣悪誤認」とすべきではあるがここでは「劣位誤認」と名づけておく．せっかく役に立つ製品や技術があるのに十分世の中に活用されず，当該製品や技術を使用することで得られるはずの便益が得られないという社会的ロスを生み出すものである．この劣位誤認の例については第４章で述べる．

３．優良誤認

「非安全・安心」とは，性能表示で述べられている効用が実際には存在しないにも拘わらず存在するかのように利用者が錯覚することで起こる．安全ではないにも拘わらず安全であると称して提供されている技術，製品があり，利用者は“安心の心持ちで”利用するという構図である．

公正取引委員会は，「不当景品類及び不当表示防止法」(昭和 37・5・15・法律 134 号 改正平成 17・4・27・法律 35 号)で，「適正とはいえない広告や表示によって，製品或いはサービスが実際よりも著しく優良であると消費者が誤認すること」と定義している．「非安全・安心」の領域は，まさに公正取引委員会がいうところの誤認と同じものなので，「非安全・安心」の構図での製品提供を「優良誤認」と名づけた．本人認証分野を見渡すと，ワンタイムパスワード，ＰＫＩ，生体認証において優良誤認とみなせるケースが存在していると考えられるので誤認の代表例として以下に考察する．

３－１　ワンタイムパスワードをパスワードと錯覚させる優良誤認

パスワードの脆弱性（「覚えやすいものは破られやすく，破られにくいものは覚えにくい」というジレンマ）を解決するために従来様々な管理，運用方法が提案されてきた．ワンタイムパスワードはパスワード問題を解決する究極のパスワードという触れ込みで登場し，トークンと呼ばれる専用のパスワード生成器などを使って，時刻同期方式或いは数学的アルゴリズムに基づくチャレンジレスポンス方式などにより，異なる使い捨ての「パスワード」を生成するため，従来のパスワードを超える最高水準のセキュリティ技術であると，利用者に安心感を抱かせる説明がなされてきた．利用者は，「ワンタイムパスワード」という名称から本人だけが知るパスワードを連想し，その生成アルゴリズムが高度に専門的であるという事実とあいまって，“なんとなく安心”してしまうのである．

トークンの生成するパスワードは一般にパスワードとして理解されているものと同じ範疇のものと考えるべきではない．トークンを今保持している人間であれば，そのトークンの正規の所有者であろうがなかろうが誰にでも送出できるような文字列が，トークンの正規の所有者本人であることを証明する合言葉であるはずはないからである．

トークン自体は盗用に対しては無力である．つまり認証サーバ側はアクセスしてくる人が認定されたデバイスを持っていることは判るが，そのデバイスが今誰の手中にあるかについては判断することができず，盗用に対して無力であることについては他の所持物照合方式と何ら変りはない．盗用に対して有効な対策を取ろうとすると，正規所有者であることを証明するための所有者認証が別途必要となる．そうなるとセキュリティはこの所有者認証にかかる本人認証手段の選択に大きく依存してしまうことになる．

「ワンタイムパスワード生成トークン」と暗証番号とを組み合わせた２要素認証という方式もある．「所持物照合は盗用に無力だが，記憶照合の一つである暗証番号をもう一つの要素として組み合わせ，２要素認証とすれば必要な安全性を提供できるだろう」，というものである．２要素＞１要素　ゆえに「１要素よりも強い」とは言えるであろうが，２要素だからいつでも大いに安心といった過大な評価は避けるべきである．特に屋外（モバイル）の運用では一般に携帯端末も認証用トークンも共に一人の利用者に張り付かざるを得ないため，盗難にあう時には両方一緒に盗まれることを想定しておく必要がある．この場合には２要素の意味は薄くなる．

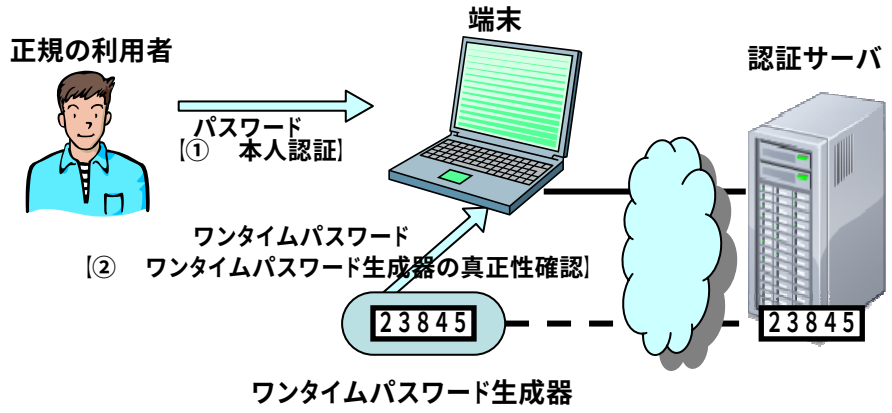

図２　パスワード（本人認証）とワンタイムパスワード
（ワンタイムパスワード生成器の真正性確認）

Vol.2011-CSEC-54 No.9
Vol.2011-SPT-1 No.9
2011/7/12

ワンタイムパスワードはパスワードの脆弱性を解決した上位技術ではなく，IC カードや USB トークンといった，本人ならば持っているはずの所持物による認証方法の一つと考えるべきであり，ＩＰＡ（情報処理推進機構）の『本人認証技術の現状に関する調査報告書(2003.03)』(参考文献[1]）においてもワンタイムパスワードは「所持による認証」として取り扱われている．しかしながら，世間一般での認識は，「仮に盗んでも数分後には無効になっているワンタイムパスワードは，盗むとその後相当期間に亘って使えてしまう固定パスワードの限界を破るものであり，固定パスワードの上位技術である.」といったものである．多くの人々がそのように思い込んでしまうのは，トークンが発生する「使い捨てデータ」が「ワンタイム“パスワード”」という名称で呼ばれていることと，利用者が自らの手で数字列ないし文字列の入力を行うように要求されることが原因と思われる．

パスワードの上位代替技術でないにも拘わらず究極のパスワードであるかのごとくに思い込んでしまう優良誤認を避けるためには，提供者側が「ワンタイムパスワード」という誤認につながる名称でなく「使い捨てデータ」という用語を使うことが望ましいと考える．

３－２　ＰＫＩないしＰＫＩ搭載ＩＣカードに関わる優良誤認

ＰＫＩないしＰＫＩ搭載ＩＣカードに関わる“安心な心持ち”もまた根強く利用者に蔓延しているように見受けられる．

ＩＣカードや携帯端末などの格納媒体との関係で言えば，ＰＫＩが有する暗号・認証・署名機能は，あくまで正規の利用者の手中に格納媒体がある場合にのみ効用を発揮するものであり，格納媒体が盗用された場合には正規の利用者とは異なる他人をしっかりと認証するだけに終わる．

ところが，「ＰＫＩ搭載ＩＣカードはＰＫＩを搭載しているゆえパスワードの保護なしでもＩＤ／パスワードよりも本人認証効果が高い.」との優良誤認的表現が散見される．パスワードで保護されるＰＫＩ搭載ＩＣカードが単なるＩＤ／パスワードよりもセキュリティが高いのは当然であるが，これは二要素法（記憶＋所有物）が単一要素法よりセキュリティが高いという構造によるものであって，ＰＫＩの効用によるものではない．

３－３　生体認証技術の性能表示の際，本人拒否率（ＦＲＲ）と他人受容率（ＦＡＲ）を独立変数のように扱うことによる優良誤認

生体認証における生体照合精度は，他人受容と本人拒否の精度の相関関係が示されねば「安全」が保証されるかどうかの判断ができない．したがって，他人受容率０．０１％の時に本人拒否率は０．１％といった対（つい）の指標によって性能を表示すべきものである.（図３）　前提条件なしで一方の値のみを言ってもまったく意味がないにも拘わらず,『他人受容率は０．０００００１％以下（約１０００万回に１回）である』と表示するだけで，対の値である本人拒否率を同時に示していないものが散見される．利用者は他人受容率の低さという性能値のみを見て“安心の心持ち”を得ることになり，優良誤認の元となる．

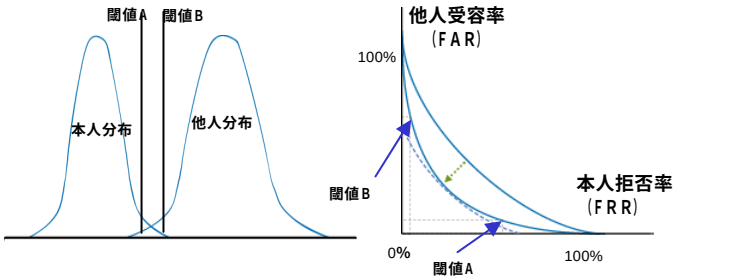

図３　生体照合におけるＦＲＲとＦＡＲとの関係

３－４　安全性を犠牲にして可用性を上げる運用

本人認証を含む情報セキュリティの製品・サービスには，機密性と同時に可用性・利便性の考慮も必要であるが，利便性を優先するあまり肝心の機密性がおろそかになり，結果として「非安全・安心」となってしまうケースがある．

例えば，生体認証で救済用パスワードを併用するものがあるが，パスワード単独による本人認証よりも，２つある攻撃対象の弱いほうさえ破ればよくなるため，セキュリティ強度が低くなるのは論理的帰結であるにも拘わらず，パスワードを併用する事実もそれに伴うリスクも，パンフレット等販売用資料において明確に謳われていないケースが多い．

Vol.2011-CSEC-54 No.9
Vol.2011-SPT-1 No.9
2011/7/12

また，本人拒否が起こった際に，利用者が生体認証機能を任意にキャンセルして，パスワードだけで認証を可能としているものがあり，セキュリティ強度がパスワード単独方式を上回ることはないにも拘わらずその事実が知らされていないケースも見受けられる．

３－５　サーバ認証に関わる潜在的優良誤認

今アクセスしているサーバが偽物であればそのことを利用者が認識し得るようにと様々なサーバ認証技術が提供されているが，その殆どは「正規サーバとの接続が確立した」旨のメッセージを文章，アイコン，配色変更などで画面に表示するものである．一般にはこの表示画面がいつもと同じものであれば安心してよいということになっている．しかし，実際にはこれだけで接続したサーバが本物であると安心しきってしまうのは早計であるかも知れない．真正サーバと接続されていないにも拘らず「正規サーバとの接続が確立した」旨を表示した偽画面を見させられている可能性を排除しきれないからである．真正サーバでなければ表示しない筈の画像や壁紙が表示される方法もあるが，この場合にも利用者が今見ている画面が複製された画面である可能性を排除できない．

サーバ認証の確立を平面的な画面表示だけで利用者に告知する方法にはこうした制約が潜んでいることは多くの利用者には知らされていない．

４．劣位誤認

劣位誤認とは，性能表示で述べている効用は存在し客観的に「安全」と評価できる本人認証技術にも拘わらず，その利用者は心持ちが「安心」して利用できないという構図である．「安全・非安心」（劣位誤認の象限）の象限はこれまで対象として取り上げられることが殆どなかったが，以下，画像選択型本人認証を例にして考察する．

画像選択型本人認証は，画像を照合データとして登録し，囮画像を含めた画像の中から登録画像を正しく選択した者を本人と認証する手法である．この画像選択型本人認証では，セキュリティに関する数学的強度，覗き見，推測攻撃などについて劣位誤認といえる誤認識が存在するようである．

数学的強度の劣位誤認とは，実際には母数と登録数を増加することによって任意の強度が得られるにも拘わらず，画像の母数も登録個数も小さなケースのみを見て数学的強度が劣ると誤認するものである．

覗き見について，無防備・無警戒に画面に大きく鮮明に表示される特異性の強い画像は簡単に覗き見できてしまえるので，このことから画像選択方式そのものが覗き見に弱い方式であると誤認されるものである．実際には無防備・無警戒であれば文字の入力も簡単に覗き見できてしまううえ，昨今は迅速な指の動きでもスロー再生できるビデオ盗撮も心配せねばならなくなった．画像だから弱いという問題ではない．

推測攻撃については，利用者の趣味・交流関係などの情報を入手できる場合は登録画像を推測できてしまうというものである．実際には無防備・無警戒な利用者を想定すると文字でも同じことで，要は運用状況に応じて推測されにくいデータを登録すればよいのである．

図４　画像選択型の事例

５．優良誤認や劣位誤認の発生原因

５－１本人認証技術の本質に関する理解不足

パスワードは，本人認証において「記憶照合方式」を代表する方式であり，本人があらかじめ登録し，認証をする度に入力する文字・数字列を指す．この本来的な定義を外れて「認証をする度に入力する文字・数字列」という部分のみが切り離されてしまうと「記憶照合」の意味がなくなり，パスワードではないものがパスワードとして扱われる誤認が生じる．

５－２　製品・サービス提供側の不作為・注意欠如による情報発信

救済用パスワード併用生体認証製品・サービス：次の２つは，この情報発信に該当するものである．

①生体認証機能には本人拒否時の救済手段が必要であるにも拘わらず，組み込まれている救済用パスワードの存在を表示しない．

②「パスワードよりも高いセキュリティを実現」といった，パスワード運用によってはセキュリティが低下することもあるという情報を伝えない．

Vol.2011-CSEC-54 No.9
Vol.2011-SPT-1 No.9
2011/7/12

５－３　不注意による情報発信のこだま効果（誤認を招く情報の再生産）

製品・サービスを提供する側の情報発信が一旦行われ，社会に受容されてしまうと，それがどんなに不正確なものであっても，検討を加えられることなくマスコミ等で同一の情報発信が何回も繰り返されることがしばしば見られる．そうなると優良誤認，劣位誤認を招く情報がこだまのように再生産され,「大メーカーのいうことだから」「マスコミがいうことだから」と無批判に受容する人が増える結果となる．

５－４　製品・サービス提供側が，誤解を恐れて正確に伝える努力をしていない

他社が自社基準に基づいて表示している中で第三者評価機関での計測値のような厳密な値(他社比較の際不利となる値)を表示するのは得策でないと判断することや，あえて技術の限界についての利用者の理解を促すような記述を避けることがあるのではないかと思われる．

５－５　検証なしの思い込み

上記はいずれも利用者が製品・サービス提供側の情報を検証なしに信じてしまうことによって誤認が発生する原因となっている．権威に弱く，有名ブランドを過信するあまり，検証することなしに思い込んでしまうという利用者側の習性が背景にあると考えられる．

６．課題の取組み・解決の方向性提言

６－１　適正な表示のガイドラインの作成と普及

リスクの提示とリスクに応じた対応策を決めるという考え方及び具体的な例を示したガイドラインを作成し，供給者に普及する必要がある．また，景表法の情報セキュリティ製品或いはサービスへの適用を徹底することにより,解決できることは多い．そのために，同じく今後は優良誤認の起こり得る画像選択型本人認証も含め，セキュリティ製品・サービスに関する適正な表示のためのガイドライン等を作成することが望ましい．

６－２　産官学メディアへの適正な情報の提供，利用者，消費者への啓発

消費者団体，教育機関，自治体などを通じて適正な情報の提供，利用者への啓発を進める．特に，専門家・提供側の不勉強や思い込みによる誤った情報と，その情報をもとに再生産された不適正な情報や不親切な情報に関しては，内閣府，防衛省，警察庁，経済産業省，総務省，文部科学省を始めとした各省庁及び各自治体への情報の提供，学会，メディアへの啓発が必要と思われる．

７．結び

客観的な安全と主観的な安心の双方を充足することが「信頼」の条件である以上，「優良誤認」と「劣位誤認」はそのどちらの誤認もデジタル社会への信頼にとって大きな障害となるものである．本論文では，あらゆるセキュリティ要素技術にとって基礎的与件でありセキュリティの根幹部分となる本人認証の分野を例にとって両誤認の発生と原因及び対策について論じた．セキュリティ製品・サービスにおいては未だ提供側は詳細で正しい性能情報の開示を義務付けられているとはいいがたく，誤認の発生する危険性は今後もなお高い．優良誤認及び劣位誤認を減らすため，産官学メディアにより正しく適切な情報発信を行い国民を啓発することが，技術への信頼を向上させ，安全・安心なデジタル社会の定着に寄与すると信ずるものであり，本論文がそのきっかけとなればまことに幸いである．

参考文献

［１］情報処理振興事業協会（IPA）セキュリティセンター：本人認証技術の現状に関する調査報告書(2003.03)

［２］電子政府ガイドライン作成検討会セキュリティ分科会,「オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン」（2010.02）

［３］鵜野幸一郎，小泉雄介：次世代電子行政サービスの安全運用を支える本人認証基盤の確立に向けて，日本セキュリティ・マネジメント学会第 23 回全国大会研究報告書，（2009.07）

［４］鵜野幸一郎，原岡望，力利則，本人を認証する製品の優良誤認を防ぐための提言，2007 年 JSSM 第 21 回全国大会研究報告書

［５］『バイオメトリクス・セキュリティ評価に関する研究会 中間報告書』平成 18 年 12 月 27 日独立行政法人 情報処理推進機構　セキュリティセンター