社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－IS－94（2）
2005／11／18

e-Japan/u-Japan における一般利用者のための情報セキュリティ認知の社会環境に関する一考察

桑原　悟

新潟国際情報大学

日本政府の「e-Japan 戦略」及び「u-Japan 構想」では，情報通信基盤を利用した様々なアプリケーションの一般利用者は，一般消費者全体と考えてよい程に広く拡大する。しかし，一般利用者の情報セキュリティ上の安全の認識は現在十分とは言えず，u-Japan の完成する 2010 年においてもその度合いは大きく改善されることは期待し難い。そこで，本論文では，健全なネットワーク社会の発展のために，一般利用者が直接認識できない脅威について考え，一般利用者でもネットワークアプリケーションの安全性を認知できるようにする方法及びそのために必要となる社会環境における課題について考察する。

A study about an environment for end-users' recognition of information security in "e-Japan/u-Japan" or the ubiquitous network society

Satoru KUWAHARA

Niigata University of International and Information studies

Abstract：In the strategy of "e-Japan" and the design of "u-Japan", the users of the various applications that used an information and communication technology will be general consumers. In this paper, I examined social environment that helps these users who have only general recognition ability to recognize the situation of information security of these applications.

はじめに

日本政府は，「e-Japan 戦略」での通信インフラの整備や IT サービスの利活用の推進に引き続き，2004 年 5 月に提示した「u-Japan 構想」で，2010 年までに日本をユビキタスネット社会へと発展させていくことを目標としている。

この構想では，単に生活の利便性を向上させることだけでなく情報通信技術の利用による地域や経済への波及効果も視野に入れており，また，プライバシーや情報セキュリティ，電子商取引環境の整備などの課題も認識し，それらを解決するための技術開発・研究実験も視野に入れている。

いずれにしても，情報通信技術の発展と利用の拡大は，疑うべくもない事実として今後も進んでいくものと考えられる。そしてこのことは，現在よりも利用者が拡大し，一般利用者は，一般消費者のほぼ全体になるであろうと考えられる。しかし，この一般利用者側の情報セキュリティに関しての知識や実際のアプリケーションの利用における安全性の認知については，その高度化や専門化は期待できない。

したがって，u-Japan が目指すネットワーク社会が健全に実現されるためには，一般消費者が，情報セキュリティ上の安全を正しく認識できる仕組みを社会環境として構築することが必要となる。

１．u-Japan での取り組み

総務省の取りまとめた「u-Japan 政策パッケージ」では，「ICT 安心・安全 21 戦略」として，次の 10 分野，21 課題について利用環境整備を行うとしている。

１）プライバシーの保護
　医療におけるプライバシー保護
　医療機関や事業者の保有する個人情報保護
２）情報セキュリティの確保
　一般ユーザの情報セキュリティ意識
　情報ネットワークの脆弱性
　コンピュータウィルス
３）電子取引環境の整備
　電子決済の安全性
　ネットを利用した悪質商法
４）違法･有害コンテンツ，迷惑通信への対応
　迷惑メール
５）知的財産権への対処
　知的財産戦略
　デジタル財の著作権保護
　コンテンツの二次利用不足

６）新たな社会規範の定着
情報技術の研究開発における科学技術倫理
７）情報リテラシーの浸透
教育における ICT 利用
高度な ICT 人材の不足
８）地理的デバイドの克服
高度サービスの地域格差
社会資本整備における ICT の優先度
電子自治体における格差
９）地球環境や心身の健康への配慮
青少年の発達への影響
１０）サイバー対応の制度･慣行の整備
電子政府の利便性
地方公共団体の業務の標準化
医療における ICT の利活用

一般利用者の情報セキュリティに関連しているものは，上記の分野２）と３）であげられた，「一般ユーザの情報セキュリティ意識」，「情報ネットワークの脆弱性」，「コンピュータウィルス」及び「電子決済の安全性」の４課題である。

これらの詳細は現在明らかではないので，このなかでネットワーク社会の健全な発展のための一般利用者のための情報セキュリティ認知の社会環境構築が含まれているのか，含まれているとすればどのようなものであるのかは，不明である。

２．一般利用者が晒される脅威

ここでは，一般消費者がインターネットにアクセスする環境である，家庭のパソコン，キオスク端末，携帯情報機器などにおける，情報セキュリティ上の脅威について検討する。

２.１ 家庭のパソコンと周辺機器における脅威

通信が盗聴される脅威，成りすましによって不正使用される脅威，コンピュータウィルスにより使用不能となる脅威に加え，悪意のあるハードウェア，ソフトウェア，たとえば，キーボードとそのドライバソフトが，利用者の打ち込んだパスワードを含むキーストロークを記憶して，悪意のサイトに送るなどの脅威，また，取引内容のコピーをまったく別のサイトに送る又は，利用者の電子署名を利用者の意思によらず施して高額な商品を発注するなどの脅威が存在する。

さらに，ディスプレイ装置への映像信号は，電磁波として放射されるので，離れた場所からこれを受けて映像を再現することができる。この脆弱性を攻撃される脅威も存在する。

２.２ キヨスク端末における脅威

ユビキタス環境において，一般利用者は家庭のパソコン以外にも，外に設置されたキオスク端末を利用する状況が生まれる。

端末機器としてパソコンを使用している限りにおいては，前述の脅威はそのまま存在する。

加えて，通常は，端末装置が利用者の管理下にないので，偽の設備や正規の設備に仕掛けられた偽の入力装置などで利用者の情報が盗まれる又は，利用者が意図しない取引に利用者の電子署名がなされるなどの脅威も存在する。

２．３携帯情報機器における脅威

PDA や WEB アクセス機能をもつ携帯電話や PHS もまた，電子取引に用いることができる。

これらは，入出力装置が本体と一体化されており，パソコンに比べて脅威は少ないと考えられるが，基本的には，パソコンと同様の脅威が存在する。

３．一般利用者の対抗策

一般消費者は，情報セキュリティに関しては非専門家であるため，前述の脅威に対して直接的な対抗策を講じることは不可能である。

一般消費者が実行し得る対抗策とは，ごく簡単なものに限られる。たとえば，「外出時に戸締りとその確認をする」という程度及び「食品などの安全性を示す表示があることを確認する」という程度であると考えられる。

そこで，前述の一般利用者の環境における脅威に対する専門的対抗策を，ごく簡単なものに変換する仕組みを社会環境に導入する必要が生じる。ここでは，その基本的考え方と必要となるセキュリティ要件について述べる。

３.１ 基本的考え方

デジタル署名を利用して，一般利用者の端末装置であるパソコンの本体，OS，周辺機器，ソフトウェアのそれぞれに，自身を証明するプライベート鍵とセキュリティ要件に適合したことを表す情報に署名・暗号化したものを内蔵させ，OS にこれらを確認し利用者に安全性の表示として知らせる機能をもたせる。

OS 自身の真正性の確認は，一般利用者向けに，これを確認し利用者に知らせる機能をもった IC カードを導入し，これを当該のパソコンに接続して行う。このとき，OS もまたこの IC カードの真正性を確認し利用者に安全性の表示として知らせる。

これらすべての確認のために必要な情報を与

える信頼サイトをインターネット上に構築する。
これにより，一般利用者は，脅威に対する対抗策として次をするだけでよいことになり，これは，十分対処可能である。

① ハードウェアの封印が破壊されていないかの確認
② OS が警告を表示するなどして停止していないかの確認
③ 電子取引用 IC カードの管理
④ 利用しているブラウザの確認
⑤ 接続しているサイトと通信経路の安全性表示の確認
⑥ 利用者側環境の安全性表示の確認

３.２ 各構成要素のセキュリティ要件

ここでは，３．１で示した対策を確かなものにするための各要素のセキュリティ要件について述べる。

（１）周辺装置のセキュリティ要件

３．１であげた脅威に対する直接の対抗策としては，「周辺機器が本来の機能と動作以外をしないこと」をセキュリティターゲットとした IS015408 認証を取得することがあげられる。この認証を取得したことを証明する情報に審査機関のプライベート鍵で署名・暗号化を施して内蔵しておくことが必要となる。

また自身のプライベート鍵を安全に内蔵し，自身の証明のために，これを使って暗号化をする機能が必要である。

（２）ソフトウェアのセキュリティ要件

一般利用者の端末装置として動作するパソコンのソフトウェアに関しても同様に，「本来の機能と動作以外の動きをしないこと」をセキュリティターゲットとした IS015408 認証を取得することがあげられる。また，周辺機器と同様に，この認証を取得したことを証明する情報に審査機関のプライベート鍵で署名・暗号化を施して内蔵しておくことが必要となる。

また，ここでも自身のプライベート鍵を安全に内蔵し，自身の証明のために，これを使って暗号化をする機能が必要である。

（３）パソコン OS のセキュリティ要件

パソコン OS もソフトウェアであることから，前述の（２）のセキュリティ要件は備える必要がある。加えて，パソコン OS は，電子取引を行うに際し，動作させる必要のある周辺機器及びソフトウェアのチャレンジ・レスポンスによる確認と，内蔵されている前述の署名・暗号化されたセキュリティ要件適合情報を確認する機能が必要である。

この確認には，デジタル署名自身，耐用年数情報及び，危殆化した機器及び危殆化したソフトウェアの情報との照合が含まれる。

この確認で，問題のあった周辺機器については，電子取引に必要でないものはパソコン本体の機能に命じて，電気的に遮断する。また問題のあったソフトウェアについては，動作を終了させる。

電子取引に必要な周辺機器やソフトウェアである場合は，その旨を表示しするなどして利用者に知らせ，電子取引に関するそれ以降の処理は行わない。

これらを実現するために，OS は，信頼できるサイトから次の情報を得る機能を必要とする。

・現在日時
・必要なデジタル証明書情報
・危殆化した機器のリスト
・危殆化したソフトウェアのリスト

また，後述の一般利用者の所有する IC カードに対しても周辺機器と同様のチェックを行う。

（４）パソコン本体のセキュリティ要件

パソコン本体も機器であることから，３．１であげた脅威に対する直接の対抗策としては，「本来の機能と動作以外の動きをしないこと」をセキュリティターゲットとした IS015408 認証の取得とこれを示す署名・暗号化された情報を内蔵することがあげられる。

また，ここでも同様に自身を証明するためのプライベート鍵を安全に内蔵し，自身の証明のために，これを使って暗号化をする機能が必要である。

これらに加えて，パソコン本体は，電子取引を行う際に OS からの指令によって，周辺機器の接続されているポートを電気的に遮断することができる機能が必要である。

これは，必ずしもすべての周辺機器が電子取引に必要でないことから，電子取引以外の用途に使用しているときに，認証を持たない機器を脱着するわずらわしさを排除するためである。

（５）信頼サイトの導入

前述の確認を行うために，信頼サイトとして次のものを導入する。

・ 現在日時を提供するサイト
・ 必要なデジタル証明書を表示するディレク

トリサービス及びリボケーションリストサイト
・ 危殆化した機器及びソフトウェアのリストを提供するサイト
・ キヨスク端末の検査情報を提供するサイト
・ OS，ドライバ，ブラウザなどのソフトウェアの検査情報を提供するサイト
・ PC，周辺機器の検査情報を提供するサイト

（６）一般利用者向け IC カード

一般利用者向けの IC カードは，パソコンの OS の真正性を確認し，OS の確認した前述のすべての確認事項をこれによって正当なものとみなすために導入する。そのための機能として，次のものが必要である。

① チャレンジの発生機能
② 信頼サイトの証明書情報
③ 信頼サイトへのアクセス機能
④ 暗号化機能
⑤ 署名及びレスポンスの確認機能
⑥ パソコンの確認結果の表示機能(LED など)

パソコン OS に対してチャレンジを送り，レスポンスを得てこれを信頼サイトから得たパソコンの証明書関連の情報を用いて確認する。このとき，信頼サイトへのアクセスは，パソコンを経由して行われることになるので，この経路中つまり，パソコンの中を通る信頼サイトとの通信は，パソコンから分からないように暗号化する必要がある。

また，IC カード自身も接続された周辺機器の一つでもあるので，前述の周辺機器のセキュリティ要件は同様に適用される。

さらに，パソコンをはじめとする環境の検証が終了したあとには，実際の電子取引がおこなわれることになるが，そこでは，一般利用者個人としての証明が必要になる。そこで，この IC カードには，個人の認証関連情報も内臓されることになる。

（７）キヨスク端末のセキュリティ要件

キヨスク端末でもパソコンを使用していることが普通であると考えられるので，これまで述べてきた要件が適用される。偽の全体設備や偽の入力装置も，一般利用者向け IC カードの導入とパソコン OS の確認機能で排除できる。

（８）携帯情報端末のセキュリティ要件

PDA や Web アクセス機能をもった携帯電話，PHS においても，基本的には，パソコンを端末として利用する場合と同種のセキュリティ要件となる。

しかし，本体と入出力装置が一体であること，また，特に形態電話と PHS に関しては，OS が本体に組み込まれていることから，パソコンを利用する場合に比べ，セキュリティ要件が少なくてすむ特徴がある。

４．既存の社会システム

前章で述べた情報セキュリティ要件の検査，認定については，専門知識と能力をもつ信頼できる機関によって成されることが前提となる。

基本的には，信頼できる機関のいわば「お墨付き」を確認することで，専門家ではない一般の利用者が，サイト，ハードウェア及びソフトウェアを信頼できる仕組みが構築される。

この種の構造は，社会環境としては，情報セキュリティ以外で，これまで様々な社会システムが構築，運用されている。

ここでは，その例をあげ，情報セキュリティ関連で，類似の社会システムが有効に機能するかどうかを検討する。

４.１ 既存の社会システムの例

（１）HACCP

1960 年代に米国で宇宙食の安全性を確保するために開発された食品の衛生管理の手法であり，国連の国連食糧農業機関(FAO)と世界保健機構(WHO)の合同機関である食品規格(CODEX)委員会が各国に採用を推奨している手法である。

HA（Hazard Analysis）すなわち，食品の原材料から最終製品にいたるまでのすべての工程で発生する恐れのある微生物汚染等の危害についての調査・分析と，CCP(Critical Control Point)すなわち，より安全性が確保された製品を得るために，製造工程における特に重点的に管理すべきポイントである殺菌工程や包装工程などでの重要管理点を設定，管理する。

乳及び乳製品，食肉製品，水産加工品，味噌，醤油，冷凍食品など 20 の食品種類ごとに行政によって認められたそれぞれ一つの指定認定機関が認定する。

農林水産省は，『HACCP 方式を，食品の製造工程に導入すれば，食品の安全性は従来の製造方法より高まるが，製造された食品の安全性が完全に確保されるわけではない』という説明をしている。取得の動機は，設備改善などでの金融，税制面での優遇措置があることが挙げられる。

また，HACCP 取得の製品への標記は任意とされ

ている。

（２）IS01401（環境マネジメント規格）

組織が自ら環境方針および目的を定め，PDCA サイクルを確立し，環境に与える有害な負荷を減少させることをねらいとしている。

審査登録機関による審査を受け，認証されれば取得となる。審査では，環境マネジメントシステムが規格の要求事項に適合していること，文書化された環境マネジメントシステムが確実に運用されていることなどが，具体的証拠をもとに確認される。

法的拘束力は無く，環境活動に関する具体的な数値等も求められてはいないが，取得の動機は，日本や外国の政府機関関連の受注に有利又は必須とされるなどが上げられる。

（３）公認会計士による会計監査

投資家が投資しても良いかどうかの判断を下すために，財務諸表を見るが，この財務諸表の正当性を，公認会計士が行う会計監査により裏付ける仕組みである。監査の基本的考え方は，大航海時代に遡るともいわれ，歴史のある社会システムである。

この場合，投資家は，財務諸表の見方とその限界の認知については自ら責任をもつことになる。

４.２ 既存の社会システムに関連した事案

ここは，４．２であげた既存の社会システムが，情報セキュリティ関連の安全性認知の構造として有効な仕組みとして取り入れられるかどうかを検討する。そのために，これまでに報道などで明らかとなった当該の社会システム関連の事案を検討する。

（１）HACCP 関連の事案

2000 年 6 月にＹ社の低脂肪乳を原因とする発症者 10,650 人の大規模な食中毒事件が発生した。工場の立ち入り検査などが行われ，ずさんな温度管理，品質保持期間の改ざんなどが明らかになった。この工場は，既に HACCP の認証を取得しており，本来であれば，このようなことが起こらないことが期待される工場であった。

認定されている施設においてなぜこのようなことが起こったのかの解明は当然必要であるが，これらの認証を与えた機関についての責任の構造についても考える必要がある。

Ｙ社に関連する報道が誰にでも知られる程度なのに対して，認証を与えた側に関する情報は，その対象とはなっていない。

（２）IS014001 関連の事案

2000 年 3 月に神奈川県藤沢市の引地川に放水されている雨水幹線の水質から，環境基準値である 1〔pg〕に対し，8,100〔pg〕の高濃度ダイオキシン類が検出された。立ち入り調査の結果，Ｅ社藤沢工場の焼却炉の排ガス洗浄廃水が，誤って雨水管に接続されていたことが原因と判明した。

この工場は，1997 年 2 月 5 日に IS014001 の認証を取得しており，本来であれば，このようなことが起こりえないと通常判断される工場である。

当時，Ｅ社は IS014001 の返上を申し出たが，認定機関はこれを受け入れず，認定の取り消しを行った。ここでも，認定者の責任については明らかではない。

（３）公認会計士による会計監査関連の事案

1999 年 12 月に，当時のＯ監査法人が，当時のＮ銀行の虚偽の半期報告が適正であるとする監査証明を行ったことに対して，Ｎ銀行の当時の株主から損害賠償の訴えを起こされている。

この事案は，監査法人及び公認会計士が，積極的に粉飾決算に加担したという最近起こった別の事案とは違い，犯罪行為としての告発ではない。監査法人が不当な決算内容を指摘できなかったことに対しての民事訴訟である。

公認会計士による会計監査は，歴史も長く，これまで有効に機能してきたと考えられるが，監査人の監査能力に関しては，公認会計士の国家資格の保有は前提とされるが，実施結果により，自動的に監査者の責任が問われる仕組みにはなっていないことを示している。

５．有効な社会システムの構築のための課題

ここでの主題は，既存の社会システムのその分野での問題点ではなく，u-Japan における一般利用者にとっての情報セキュリティ認知の仕組みとして，類似の社会システムが採用できるかを考えることであるが，４．２の事案が示すように，どれも一般利用者にとって十分に分かりやすく，十分に情報セキュリティ上の安全性を担保するものとしては，期待することが難しいと考える。

その理由も一つとしては，社会システムのもつ宿命として，その構想時から実際の運用時までに，様々な立場の人間の思惑が入り込み，純粋な目的とのずれが生じることが考えられる。

その一方で，前述の仕組みそのものには明示されないものの，その分野の行政や業界に共通

に認識された判断基準が存在し，通常の場合は，これが抑止力となって問題の発生にはいたらない構造であることは，十分に考えられる。

そうすると，４．２の事案は，何らかの事象が想定される程度を超えたことで起こった事案ということになり，社会システムとしてこれらの仕組みの外側にある，広く一般が対象となる法律に照らす事案となったと考えられる。

一方で，ネットワーク社会は，その拡大の範囲が特定の業界に限定されないので，分野に依存した抑止力は期待できない。

ここで取り上げたような種類の問題が，一般利用者のネットワークアプリケーション利用の局目で顕在化すると，安全の裏付けとなる社会システムへの信頼性が大きく揺らぐことが考えられる。

したがって，情報セキュリティ上の安全を担保するのに必要な社会システムの設計には，本来の機能が損なわれない工夫が必要となる。

５．１　構造を明示する表記法

前述の工夫を実現するための道具立てとして考えられるのは，社会システムの設計にその目的を果たす機能があるかを客観的に確認できる表記法を導入することである。

現代社会においては，多くにおいて言葉による説明が原則であるが，自然言語は，その特徴として，あいまいな表現や不正確な表現，誤解を誘発するような表現も成され得る。制度の設計から運用の開始まで，どの段階でも，その社会システムが目的の機能を果たすことを客観的に正確に表現するためには，それを正確に記述できる表記法は有効であると考える。

この表記法に必要な要素は，次のとおりである。

・信頼の連結を確認できる
・確認項目の変換構造を確認できる
・安全度合いを表現できる

情報セキュリティ上の安全を複数の構成要素で担保する場合がある。たとえば，検査機関の認定が電子署名とともに付される場合，その検査機関が認定を与えたことと，その検査機関の電子署名の正当性の両方でその安全性を利用者は確認できるということを示すことが出来なければならない。

また，検査機関による検査項目と安全性の間の論理代数的関連や，検査結果が最終的に利用者による認定の印章の確認に置き換わる構造も記述できなくてはならない。さらに，安全性に度合いや段階がある場合も考えられるので，これについても表現できなくてはならない。

表記法の形態については，数学記号様の形態と図表の形態が考えられるが，これらの詳細については，さらに研究が必要である。

また,表記法の評価手段として，ここで取り上げた情報セキュリティ以外の社会システムや，その他の社会システムで，弱点が知られているものについて記述し，その弱点を指摘できる表記法であることを確認することが有効であると考える。

５．２　Web サイト上の表現規約

前述のように，一般利用者は，専門化による検査の結果確認することが必要となる。これは，現在サイトに表示されているプライバシーマークや RSA 社の Web サイト証明と同様，ブラウザを使ってサイトにアクセスしたときに視認性の高い印章として表示されることが必要である。

また,その印章の意味する安全性についての解説，認証を与えた機関の情報，問い合わせ先，問題発生などの場合の相談窓口の情報に簡単にアクセスできる仕組み及び社会システムとしてそれらを規定する規約が，必要となる。

これらについては,その項目，アクセスの形態，表示の様式などの詳細な検討を行う必要がある。

おわりに

ここでは，2010 年を目標とした u-Japan，すなわち高度ネットワーク利用の社会の健全な実現のために，一般利用でもネットワークアプリケーションの安全性を確認できるようにするための課題について考察した。

今後はここで示した，社会システムが安全を担保することを表現する表記法の開発と，実際に一般利用者が Web サイト上で確認するための表現規約の詳細の検討を進める。

また，u-Japan における「ICT 安心・安全 21 戦略」の詳細で，これらについての研究開発についての項目が，今後取り入れられることを期待したい。

参考文献

1) 総務省：http://www.soumu.go.jp/s-news/2004/pdf/040701_1_b1.pdf
2) 総務省：http://www.soumu.go.jp/s-news/2004/041217_7.html
3) 経済産業省：http://www.meti.go.jp/polICy/netsecurity/digitalsign.htm
4) 経済産業省：http://www.meti.go.jp/polICy/netsecurity/digitalsign-law.htm
5) 経済産業省：http://www.meti.go.jp/polICy/netsecurity/iso_iec15408.htm
6) 農林水産省：http://www.maff.go.jp/sogo_shokuryo/haccp_hp/index.htm
7) （財）食品産業センター：http://www.shokusan.or.jp/pmss/index.html
8) Satoru KUWAHARA : Mobile phone as a secure terminal for e-business
9) 桑原　悟：組織の情報セキュリティ実現のための組織内外の役割とその遂行に必要な教育に関する検討，情報処理学会第 63 回全国大会予稿集，2B-1，第 3 冊 pp.621-622
10) 桑原　悟：一般消費者のインターネット利用環境における脅威と対処可能な対抗策，情報処理学会第 65 回全国大会予稿集