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*

桑原　悟†
新潟国際情報大学　情報文化学部‡

はじめに

平成１３年４月１日に電子署名に関する法律が施行され，一定の条件を満たしていれば，「電磁的記録とそれに対する電子署名」が，これまでの「書面と署名捺印」と同等の法的効力をもつことになった。

これにより，インターネットを利用した消費者向けの電子取引に法的な拘束力を導入でき，より高額な取引をインターネットで行う際の障壁の一つが取り去られた。

また，電子政府構想，総合行政ネットワーク，電子自治体なども実現され始めており，電子署名を利用した申請・届出や，公的個人認証を利用した各種アプリケーションが，ここ数年で本格的に登場すると考えられる。

これらを実現するための環境に関して，企業や行政などのビジネス側は，様々な情報セキュリティ対策を取り得るが，それに比べて一般消費者側の情報セキュリティは，十分な検討がされているとはいえない。

本論文では，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と，一般消費者が理解可能であり，対応可能な脅威への対抗策について検討する。

なお，行政に対する届出・申請は，「取引」ではないが，情報セキュリティ上，「取引」と同様のセキュリティを施す対象と考え，ここでは，電子取引という表現で代表させる。

１．電子取引における脅威と対抗策

盗聴，改ざん，成りすまし，否認，不正侵入，DoS 及びコンピュータウィルスが，情報セキュリティ上の脅威として知られている。

これらの脅威に対抗するために，盗聴に対しては，暗号化が用いられ，改ざん，成りすまし，否認に対しては，デジタル署名とその応用が用いられる。また，不正侵入や DoS に対しては，ファイアーウォールをはじめとするネットワークセキュリティ技術が用いられる。

さらに，これらの個々の対抗手段を実効性のあるものにするため及び，人間を含めたシステム運用に対し，組織の方針としてのセキュリティ施策を設定するために，情報セキュリティポリシーが制定される。

２．電子取引のための環境

電子取引を行うための構成要素としては，一般消費者側の環境以外に，ビジネス側の環境，デジタル認証関連サービス及びネットワークがあげられる。

２．１ビジネス側の環境

ビジネス側の環境では，電子取引を行う場合の様々な脅威をその専門家を利用して把握し，対抗策を実施することができる。専門家は雇用するか又は，外部の専門家を活用することも可能である。また，その場合に，情報セキュリティ関連の法規，基準，標準などの存在及びシステム監査，ネットワーク診断，各種認定の取得などの対策が専門家から示され，投資との兼ね合で，経営に見合った対策を選択することが可能である。

運用時においても，組織内又はアウトソーシング先の情報システム技術者，ネットワーク技術者を配備することが可能である。

２．２デジタル認証関連サービス

電子取引のためのインフラストラクチャとしては，デジタル認証局や，ディレクトリサービスがあげられる。これらのサービスは，個々のビジネスサイト以上に確固としたセキュリティを実現する責務があり，電子署名・認証に関する法律では，「特定認証業務」の要件を規定し，

*Treats and the Practicable Countermeasure at Internet access Environment for Consumers
†Satoru KUWAHARA
‡Niigata University of International and Information Studies

審査認定を行うとしている。
ここでも当然，これらの組織は，情報セキュリティの専門家を利用して，脅威に対する対抗策を講ずることができる。

２．３　ネットワーク

インターネットの場合，盗聴の脅威があるが，これに対しては，ビジネス側と一般消費者側の両端で暗号化及びデジタル認証の応用技術を用いる対抗策を講ずることができる。
また，インターネットでは，接続や通信速度は保証されていない。これは，ビジネス側やデジタル認証関連サービスが相応のセキュリティを講じていることに比べ危ういといえる。しかしながら，実際には，電子取引のほとんどがインターネットの利用を前提としている。なぜなら，インターネットは，その最大の特徴である接続の容易性と経済性の点で，これにかわる手段がなく，通信の維持や完結及び，伝送速度を犠牲にしてもインターネットを選択するという判断がなされているからと理解できる。
そして，通信の維持や完結及び，伝送速度の問題に起因する不都合が起こった場合は，最低限ビジネス側の連絡先を表示していることで，人間が対応するなど，別な手段での解決に委ねることを前提に成立している。

３．一般消費者の環境における脅威

一般消費者は，家庭のパソコン，キヨスク端末，携帯情報機器からネットワークにアクセスし，電子取引を行う。ここで，ビジネス側及びデジタル認証関連の組織との大きな違いは，消費者自身は，情報セキュリティに関して非専門家であり，また，電子取引に際して専門家を手配して電子取引を行うことは，現実的に不可能であるという点である。
一方で，一般消費者の環境には，次に述べる脅威が存在する。

３．１家庭のパソコンと周辺機器における脅威

コンピュータウィルスの脅威，通信が盗聴される脅威，成りすましの脅威に加え，コンピュータウィルスと同様に，利用者が意図しない悪意のある動作，たとえば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。
また，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など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も存在する。
さらに，ディスプレイ装置への映像信号は電磁波として離れた場所から受け，映像を再現することができるので，この脆弱性を攻撃される脅威も存在する。

３．２キヨスク端末における脅威

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，（１）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。

３．３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。基本的には，パソコンと同様の脅威が存在するが，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。

４．一般消費者の環境における対抗策

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。
一般消費者が対処し得る対抗策とは，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」という程度であると考えられる。そこで，前述の一般消費者の環境における脅威の直接的対策をごく簡単な対抗策に変換する仕組みを導入する必要がある。

４．１基本的考え方

デジタル署名を利用して，一般消費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にこれらを確認する機能をもたせる。
ＯＳ自身の真正性の確認は，一般消費者にこれを確認する機能をもったＩＣカードをもたせて，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する。
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 電子取引用用 IC カードの管理

４．２各構成要素のセキュリティ要件

ここでは，一般消費者の環境を構成する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。この認証を取得したことを証明する情報に審査組織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

一般消費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組織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。

（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／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，後述の一般消費者の所有するＩＣカードについ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，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接続されている認証を持たない機器の脱着の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

（６）一般消費者向けＩＣカード

一般消費者向けの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，一般消費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，一般消費者向けＩＣカードの導入とパソコンＯＳの確認機能で排除できる。

４．３ビジネス側による確認

ここで述べてきた一般消費者側のセキュリティ要件の導入が行われると，ビジネス側も，一般消費者が利用しているＯＳを確認することができる。

また，４．１で述べた，利用者のなすべき対抗策について，一般消費者の利便性と，確実な対策の実施を促すため及び，確かに対策を実施したとする意思表示をビジネス側に記録として残す意味も含め，電子取引の最初の画面などで，これらの項目をチェックボックスとともに表示することは有効である。

（8）形態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，本体と入出職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，パソコンを利用し場合に比べ，セキュリティ要件が少なくてすむ特徴がある。

おわりに

本論文では，電子署名に関する法律の施行を受け今後拡大するであろう，よりセキュリティを必要とする電子取引の際の一般消費者側の脅威と対抗策について検討し，パソコンを端末とする環境においても，一般消費者が十分対処できる範囲の対策でセキュリティを確保できることを示した。

しかし一方で，その前提となるインフラストラクチャの構築が必要であることも明らかになった。今後は，取引の要求するセキュリティレベルに応じた必要インフラストラクチャのカテゴリ化などを検討する。

参考文献

1) 経済産業省：
http://www.meti.go.jp/policy/netsecurity/digitalsign.htm
2) 経済産業省：
http://www.meti.go.jp/policy/netsecurity/digitalsign-law.htm
3) 経済産業省：
http://www.meti.go.jp/policy/netsecurity/iso_iec15408.htm
4) Satoru KUWAHARA : Mobile phone as a secure terminal for e-business
5) 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