人に安全なことを感じさせるUIに関する考察

山口（繁富）利恵†

一般的に，情報セキュリティの向上とユーザの利便性は相反する問題であり，両立は難しいといわれている．利便性を追求するような場合，情報セキュリティ上の対策は表に出ないようにすることで対策を講じたり，表に出たとしてもユーザの動きを妨げないような対策となっていることが多い．現状の社会システムでは，ユーザが全て自身で確認することができないため，ユーザの利便性を保つように代理人や監査等を活用し実現しているが，電子情報化社会においては，監査等の観点が不足しユーザ本人がやらなければならないことが多い．本論文では，相手を認証する方法と選挙において紙と電子化情報の比較を行い，ユーザにどのように認識をしてもらっているかの現状について述べ，今後のセキュリティのUIについて述べる．

A Note on UI for Feeling Secure Systems

Rie Shigetomi YAMAGUCHI†

There is competing issue for information security and userbility so seems an incompatibility problems. If sysem engineers only focus on userbility, they must hide security mechanism. Even if users are able to see these mechanism, users feel nothing to happen in the system for security. In our social system, users cannot check every process because the system is difficult to understand or can not bother users. Thus, for userability, people manage audit or third party certification mechanism. In this paper, we will explain the difference between non-digital and digital setting about authentication process and voting system and discuss UI in next generation.

1. はじめに

現在，利便性の確保や費用対効果の観点からも，情報の電子化やネットワーク化が進み利便性の向上がなされつつある．情報の電子化等が進むにつれ，ユーザの利便性が上がると同時に，情報セキュリティの問題が表面化してきている．

しかし，セキュリティと利便性は相対する問題で両立することは難しく，セキュリティを向上すればするほど，ユーザの利便性が下がるという問題がある．例えば，ドアの鍵が増えればそれだけ攻撃者にとって複雑となることからセキュリティが上がっているということができる．一方，複雑な鍵の発明など，技術の向上で従来よりもセキュリティが向上するような場合もある等，単純には説明できないこともある．

現状のITシステムにおいて，利便性を追求するような場合，情報セキュリティの対策は表に出さないようにすることでユーザの利便性を追求することをしていることも多い．インフラ化したネットワークにおいては暗号化等のセキュリティ対策が施されているが，ユーザはその暗号化がなされいることを感じることなく，安全性が保たれているということもある．

ここでは，現状既に行われている情報セキュリティ対策において，どのようなユーザへの表現方法があるかを提示する：

- ブラウザ上でのSSLの利用について解説し，ユーザにどのように提示しているか
- 選挙と電子選挙の違いについて説明し，電子的な選挙を行うために注意すべきこと．

それによって，利用者がセキュリティシステムの安全性を理解することがこういったシステムの普及につながると考え，どのようなUIが有効かを考察する．また，今後必要となるセキュリティ対策について考察する．

2. ブラウザにおけるSSLでの提示

認証という言葉は，メッセージ等に対しても可能であるが，ここでは，本人や団体等相手を認証するような場合について取り上げる．

† （独）産業技術総合研究所 情報セキュリティ研究センター
Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST)

現在，日本語において，IT システム上で使われる相手認証には二つの意味がある.「認証」という言葉は，その方法によって certification と authentication の両方で利用されており，場合によって利用の仕方が違う.

認証 (authentication) という言葉は，ある行為の「実行主体」と，当該主体が主張する「身元識別情報」との同一性を検証することによって,「実行主体」が身元識別情報にあらかじめ関連付けられた人物（あるいは装置）であることの信用を確立するプロセスのこと，を指す．また，認証 (certification) は，製品，プロセス，サービスが特定の要求事項（基準・標準・規定）に適合していること，つまり“適合性”を第三者が文書で保証する手続きを指す.

ここでは，電子署名を利用した認証 (authentication) の仕組みについて解説し，現状ユーザがどのように電子署名の検証（確認）を行っているかについて説明する.

2.1 偽造防止と電子署名

従来，本人や団体の本人性を確認する場合には，運転免許証等の第三者機関が発行した証明書を活用して確認することが多い．この確認手法は，第三者が行った正しい発行プロセスが実現できたと仮定した場合，公印や複雑なカード等を利用して偽造が困難であることに依存して，実現している．一方，電子的な場合には，コピー&ペースト等が簡易であるため偽造が容易となる．特に，紙で実現されている公印や署名なども，コピー&ペーストの実現によって簡単に偽造が行うことができてしまうため，電子文書には捺印の効力がない.

そこで，IT システムにおいては，公開鍵暗号を使って電子署名という方式で偽造が困難な方法を実現している.

2.1.1 公開鍵暗号と PKI

公開鍵暗号と PKI の機能・性質について述べる．ユーザは，公開鍵暗号を利用して確認する場合，事前に確認する相手の公開鍵を取得し，署名の検証を行う．しかし，事前に相手の公開鍵を持つことが難しく，かつ，本当の相手から取得しているのかをネットワーク上での確認が困難なため，PKI の認証局を利用し確認することが一般的である.

そこで，第三者機関である PKI の認証局がルートの公開鍵を含むルート証明書を発行し，ユーザが事前にこのルート証明書を取得しておく．各証明書は，木構造になっており，ルート証明書を活用することで木構造の末端の証明書の検証を行うことができる．これによって，ユーザは相手を確実に確認して事前に公開鍵を取得せずとも，第三者が確実に確認したという情報を利用することによって，セッションが起こった際に相手を検証することができる.

図 1 ブラウザ上の警告 (Internet Explorer)

2.1.2 ソフトウェアが正しいことの確認

公開鍵暗号方式の場合，お互いにアルゴリズムをわかっているため，自分の選択して信頼できるソフトウェアの利用をすることで第三者的な確認を可能にしている．一方，ソフトウェアを検証しなければならない相手から取得する場合，たとえ公開鍵暗号を利用して証明できたとしても正しいアルゴリズムを利用しているのかの確認ができないという問題もある.

2.2 ブラウザを利用した Web サイト証明

公開鍵暗号方式を活用している例として、ユーザがブラウザ上で Web サイトを確認する方法について解説する。

現在利用されているブラウザには，複数の PKI のルート証明書が事前に含まれている．このブラウザに含まれるルート公開鍵証明書を，厳格に管理することによって，ユーザが証明書を取得せずともサーバを確認することができる．また，ユーザが公開鍵証明書をインストールすることも可能である.

各 Web サーバは，ユーザと SSL を介した通信を正しく行うために，各証明書発行団体より公開鍵を取得し，ユーザとの SSL のセッションを確立している．このセッションの確立は，電子署名によって実現しており，ユーザは，偽造していないサーバとやりとりをしていることを確認することができる.

2.2.1 証明書の警告

現状で利用されている多くのブラウザでは，ルート証明書に含まれていない証明書を利用した Web サーバに接続しようとした場合，図 1 のように「この Web サイトのセキュリティ証明書には問題があります.」等のという警告がでることにより，ユーザは確認することが可能である[3]．ユーザはセキュリティの警告のウィンドウのボタンを押さなければ，そのサーバへ接続す

図 2 ブラウザ上の鍵マーク (Internet Explorer)

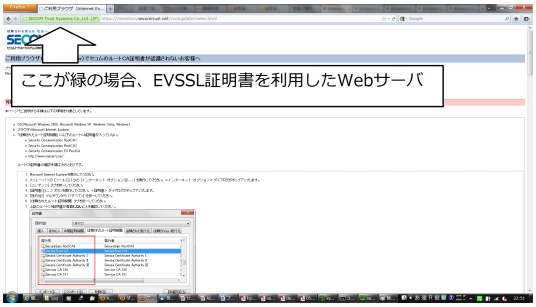

図 3 EVSSL を利用したブラウザ (Firefox)

ることができない．

しかし，あるデータによると，問題があると表示されていたとしても，ユーザはその警告を無視をしてリンク先へつないでしまうという問題もある[2]．

2.2.2 鍵 マ ー ク

正しく SSL のセッションを確立した場合，ブラウザ上において URL を記載する欄の右側に図 2 のように鍵マークがでる．この鍵マークを確認することによって，ユーザは正しく SSL が活用されていることを確認できる．

2.2.3 EV-SSL におけるユーザへの周知

一方，ルート証明書が確実に手に入れられたとしても，各 Web サーバが費用を払えば証明書を取得できるため，証明書発行会社によっては，簡単に発行しているという現実もある．

そこでできたのが，EV-SSL 証明書という新たな証明書である[4]．EV-SSL 証明書は，取得をより難しくすることによって，Web サーバの確実性を保証している．

また，この証明書をもった Web サーバの場合は，ブラウザの一部が緑になることで，ユーザが安全なサイトであることを確認することができる．

この EV-SSL 証明書は，発行プロセスが従来に比べより困難になっているが，社会的信用の高い企業しか取得できないということではない．ここでは，表示に工夫を行ってわかりやすい，という点で取り上げた．

3. 選挙とプライバシ

また，現状の選挙を電子的に行う場合，どのように実現するのかについて説明し，紙で実現してきたセキュリティの問題をどのように電子的に実現しているのかを説明する．

3.1 現状の選挙とプライバシの実現

この章では，現在の選挙おいて，不正禁止とプライバシを実現しているのかについて説明する[5]．

3.1.1 二重投票等の本人の不正禁止

選挙は，選挙権を持つ人物へ，選挙の権利を提示しなければならない．日本においては，満 20 歳以上（投票日の翌日が 20 歳の誕生日の場合まで含む）の日本国民に与えられる．地方選挙に関しては，3 か月以上当該選挙区内に住んでいることが必要とされる．選挙区に住んでいる人が選挙人名簿に記載がされ，その名簿に従って，事前に郵便で選挙の案内が送られることが一般的である．不在者投票等，別の枠組みもあるが，今回は議論しないこととする．この案内を投票所へ持参し，本人を確認する．なお，案内を持参しないでも選挙人名簿に記載があり，本人だと確認できれば選挙用紙をもらうことができる．

本人が正しく投票しているかどうかは，先に述べた案内を持参した人，もしくは，証明書の提示等で本人を証明することができた場合に，1 枚だけ投票用紙をもらうことで実現している．また，二重投票は入り口における投票管理者の本人確認に依存する．案内を不正に入手し投票が行われた事例も存在するが，ここでは投票をスムーズに行うことに重点が置かれており，紙の案内の偽造困難性に依存している．投票管理者は，選挙管理委員会（国政選挙，地方選挙によって異なる）によって選任される．

3.1.2 一度投票した票が他の人への投票等にならないことの確保

現状，先に述べた投票用紙に記載した人が正しく自分の一票として加算されているのかを確認することは，投票した本人では困難である．これを実現するために，日本においては，選挙管理委員会が選任した投票・開票立会人によって第三者的に確認を行う．

まず，投票が公正に行われているかは，投票立会人が確認を行い，投票箱を開票所へ装置する．正しく装置が行われた後で，開票立会人が開票事務が正しく行われているかどうかを確認する．

つまり，立会人が手続きを公正に行われているかど

うかを監査するわけである．

3.1.3 匿名性の確保

入り口では，本人を確認することで二重投票等の不正を禁止しているが，誰に投票したのかはわからないようにしなければならない．その実現のために，投票用紙には投票人の名前の記載をしておらず，また，投票用紙を投票箱にいれることで後からの追跡を防いでいる．投票人本人も，第三者の監査によって実現することを認識しており，また，箱にいれるという行為で匿名性を確保されていることを確認している．

つまり，本人自身が確認しなくても，正しく選挙が実現していることを第三者が確認できる方式が存在する．

3.2 投票の電子化での問題

匿名性の確保等を本当に実現していることを確認するためには，電子的に実現した場合，様々な確認を行う必要性がある．

3.2.1 現状の電子選挙

現状，自治体によっては地方選挙において電子選挙が行われていることがある．従来の選挙と同様の本人確認が行われているが，タッチパネル等で選択を行い，集計を電子的に行っている．二重投票の防止のために，投票の案内を提示した後にバーコードや IC カードを介し，電子的なシステムでタッチパネルやボタン等を利用して入力を行う．

ただし，現状の電子選挙の仕組みにおいて，監査の必要性等には言及されていない[1]．

3.2.2 二重投票の防止

従来において二重投票等で不正を禁止してきたことは，紙の偽造困難性で実現してきた．電子的に行う場合には，より偽造が容易となるために，電子署名等で実現することが必要となる．先に述べた PKI 等を組み合わせることで，本人を確認をすることが可能である．

3.2.3 票の行く先の確認と匿名性の確保

日本においては,「投票所投票主義」があるため，ネットワークを介した投票をどのようにするのかが難しいが，電子的に行う場合，票の行く先の確認は匿名性の確保との両立の観点から非常に難しい．

電子的な仕組みの場合，プログラムを正しく実現されているのかの確認を監査等で実現できていない．つまり，紙であれば，不正の入力が困難であったであろうことが，電子的に行われることによって，本当に正しくプログラムが存在しているかの検証などが必要になる．恐らく国内の納入業者が正しく実現しているはずであるが，バグ等があるのかの第三者的な確認手段はまだ確立されていない．

図 4 みんなの投票チャンネル (Wii HP より)

同時に数学的にトレースが不可能な仕組みもあるが，これは一般には理解が難しい．

そのため，投票用紙を箱をいれることによって実感していた自分の票が正しく反映されているかどうかを実感することが難しい．

3.3 UI の実現

自分の票が正しく反映されていることを実感するための方法として，Nintendo が実現している「みんなで投票チャンネル」という方法がある[6]．これは，Mii という自分の分身を Wii 上で作成し，自分の代わりにシステム上で投票を行い，投票結果には，自身の Mii が結果に反映されているため，視覚的に確認できる．

Mii で自分の票がどこにあるのかを確認することができる一方，Mii という形になっているため，自分（家族）等，Mii と本人の関係を知っている人以外は確認をすることができない．この方式の場合，Nintendo を完全に信用して二重投票の防止と匿名性の確保が行われているわけであるが，票の行き先の確認を実感することが可能となっている．

4. 今後のセキュリティ対策の議論

ここでは，情報セキュリティの普及と理解に向けた議題について述べる．

4.1 ソフトウェアの安全性

現状では，ソフトウェアが本当に機能を正しく実装されているのかを確認することは難しいことが多い．

現状の社会システムでは，監査や評価・認証等も活用し，第三者機関による確認も充実している．その理由として，市販のものすべてをユーザ自らが仕組みを理解し，その仕組み通りに実現されているかの確認ができないからである．特に監査等は，法律で定められたプロセスが存在し，資格のある人が確認を行っている．

一方，ソフトウェアといったプログラムについては，

資格は存在するものの，本当にその資格をもつ人が作成したソフトウェアかどうかについては，確認することは難しい．資格についても，現状では第三者的な資格も存在するが，たいていは大規模ソフトウェアや機器メーカーによって定められた資格の有無によってのみ定められる傾向があり，その大規模ソフトウェア会社が本当に信頼できるものであるのかは，わからないという現実もある．オープンソフトウェアであれば，第三者評価という点では十分な確認がなされているといえるが，メンテナンスや完全性の点で問題を持つことが多く，ソフトウェアが安全であるとは限らない．

従来はIT システムが単純であり，何らかの不正を混ぜることが困難であることが多かった．しかし，IT のシステムが複雑になるにつれ，ユーザだけでなくシステムエンジニアであっても，全てのソフトウェアを把握しているとは言いがたい．現状では，暗号ソフト等には検証の仕組みが存在するが，ソフトウェアの実装についても監査等の仕組みが必要となる可能性もある．

4.2 オオカミ少年

安全性の高いシステムが多々提案されている中，費用や現状のシステム変更の困難性等で導入されないことが多い．しかし上記で挙げた問題だけが，採用のハードルになっているわけでなく，そもそも安全というものがわかりにくい，入っていることが当たり前であって追加での導入の必要性を見いだせないことが多いためである．ある研究によると，セキュリティシステムの導入へ一番の方法は，利用者に恐怖感を与えることである，とある．しかし，このやり方は，やり過ぎると「おおかみ少年」につながることとなり，継続的な普及のためには諸刃の剣となる．

一般的に，安全に対してコストをかけるという意識をもたらすのが難しいのはある程度はやむを得ないが，現状の社会システムにおいてどうやって監査等を実現してきたのかを考慮すべきである．

4.3 攻撃の深刻さと対象の拡大

従来，インターネット上の攻撃は，愉快犯的なことが多かった．ところが，近年では金銭を獲得を目的としたものに加え，システムの中身をより理解した上での国家的で甚大なセキュリティ問題が増大している．攻撃者は，ソーシャルアタックを含むより簡単なところからの攻撃をする．ネットワーク越しでの対策をすることも大事であるが，身近なパスワードの管理なども大事である．

今後は，ゲーム機やテレビ等の家電や組み込みを含む制御システムなど，従来攻撃の対象にならなかったものも，脅威にさらされていると言ってよい．こういった組み込み系の対策を行うことをどのようにユーザに対して表示していくかは大変難しいが，よりわかりやすくかつ使いやすい対策が必要である．

4.4 普段の動きを邪魔しないセキュリティ対策

ユーザの利便性を追求する場合，セキュリティ対策がユーザの動きを邪魔しないようにする設計にしたほうが，ユーザにとっては負担が少ない．つまり，セキュリティ対策は，すべてインフラシステムで実現しており，その対策が正しく行われているかの検証を監査や評価・認証等で実現することが必要ではないであろうか．一方，現状，様々な情報セキュリティ監査等が存在しているのは事実だが，まだ，社内の対策について言及することはあったとしても，ユーザの情報や安全性の確保が行われているとは言いがたい．

現状の社会システムにおいても，何らかの行為が正しく行われていることを確認するための手段として，監査や評価認証などの制度が存在し，情報セキュリティの機能においても様々な評価や認証制度が存在する．この評価・認証を確認するために，ユーザが目視できる「シール」等が存在する．

一方，電子化された社会システムにおいては，従来の監査，評価・認証制度ではやり過ぎな事例も存在する可能性がある．こういったバランスをどうとっていくかは今後の課題である．

5. 結論と今後に向けて

本論文では，認証と選挙を例にとり，現状のセキュリティ対策をどのようにユーザに対して提示しているかを紹介した．攻撃の深刻さは日々深化しており，また，対象も拡大の一途をたどっている．一方でセキュリティのユーザへの表現方法の研究が進んでいるとは言いがたい．特に，利便性を追求する場合，普段の動きを邪魔しないように設計するため，セキュリティ対策を見にくくする傾向があり，情報セキュリティの対策が裏に隠れてしまうことになる．これは，社会が成熟してきたものである一方，本来対策が行われるべきことに対しても対策が行われていない可能性をはらんでいるものでもある．今後は，情報セキュリティ対策の表現方法の研究も必要ではないであろうか．

参 考 文 献

1) 総務省，電磁的記録式投票制度について，http://www.soumu.go.jp/senkyo/senkyo_s/news/touhyou/denjiteki/index.html
2) Joshua Sunshine, Serge Egelman, Hazim Al-

muhimedi, Neha Atri, and Lorrie Cranor, Crying wolf: An empirical study of SSL warning effectiveness in Proceedings of Usenix Security 2009
3) マイクロソフト，証明書のエラーについて，http://windows.microsoft.com/ja-JP/windows-vista/About-certificate-errors
4) ベリサイン，EVSSL 証明書とは，https://www.verisignsecured.jp/ev/
5) 総務省，なるほど！選挙，http://www.soumu.go.jp/senkyo/senkyo_s/naruhodo/index.html
6) 任天堂，みんなで投票チャンネル http://www.nintendo.co.jp/wii/features/poll/