電子化知的財産・社会基盤　6－5
(1999. 10. 9)

電子商取引に関する解説 (II)

齊藤 真也, 稲葉 宏幸, 笠原 正雄

京都工芸繊維大学 工芸学部 電子情報工学科

〒606-8585 京都市左京区松ヶ崎御所海道町
電話　：　075–724–7499
FAX　：　075–724–7400
電子メール　：　saito@payila.dj.kit.ac.jp

あらまし　現在，世界規模で電子ネットワークを利用する新しい社会システムの構築が進められている．これは社会における情報に関係する部分をコンピュータと電子ネットワークで処理するものであり，その中核を成すのが電子商取引である．この電子商取引にいち早く参入した企業や団体を観ると，未だ安定したサービスを提供できているとは言えない．それはクラッキングによる情報流出やシステムダウンなどによるところが大きく，また利用者は，盗聴やウイルスなどセキュリティに対する不安から，サービスの利用を敬遠している．そこで本稿では，電子商取引における脅威とその実状について紹介し，それらに対応するためのセキュリティ対策を考察する．

キーワード　電子商取引，セキュリティ，クラック

Surveys on Electronic Commerce (II)

Shinya SAITO, Hiroyuki INABA, Masao KASAHARA

Department of Electronics and Information Science, Kyoto Institute of Technology

Matsugasaki, Sakyo-ku, Kyoto 606-8585 Japan
Tel　：　075–724–7499
Fax　：　075–724–7400
E-mail　：　saito@payila.dj.kit.ac.jp

Abstract　New society systems that use world-wide information networks have been constructed on a global scale. The system are equipped with all sorts of computers and various electoric networks. An electronic commerce plays central role in such systems. In this paper, we present surveys on electronic commerce. Particularly we review and discuss on various classes of threats related to the electronic commerce. We also observe countermeasures for keeping high-level of security.

key words　Electronic Commerce, Security, Crack

1 はじめに

テクノロジーの発達により新しい社会システム，つまり電子ネットワークを積極的に利用する社会システムの構築が急速に進んでいる．

中でも経済活動の一部あるいはすべてを電子的に行う電子商取引システムに対する取り組みが盛んになされている．企業間商取引ではかなりの部分が電子ネットワークを介して行われており，標準規格が策定されているものもある．その反面，企業対一般消費者の電子商取引に関する取り組みは，試行錯誤の段階であるといえる．実際，電子商取引による売上は増加傾向にあるものの，経済活動全体からみれば微々たるものである．

企業対一般消費者電子商取引が普及しにくい理由は，大きく分けて二つ存在する．一方は，利用者のメリットが少ないということである．新しいシステムに対応するのに必要な投資が大きいにも関わらず，それに見合うだけのメリットを享受することができるシステムが少ない．他方は，セキュリティに対する不安である．事実，インターネットのセキュリティに関係のある事件が連日のように報道されている．それに対処するため，セキュリティに関する様々な研究開発が行われているが，電子ネットワークを利用する犯罪は増加の一途を辿っている．

そこで本稿では，電子商取引における脅威とその現状を取り上げ，その対応策を考察する．

2 電子商取引における脅威

電子商取引における脅威は，コンピュータネットワークにおける脅威と基本的には同じものである．そこで，本節ではコンピュータネットワークにおける脅威を取り上げ，それが電子商取引においてどのような影響があるかを述べる．

2.1 クラック

クラッカー[*1]は，ハードウェアやソフトウェアをクラックすることにより，電子商取引システムのあらゆる場面で暗躍している．そこで本節では，クラックにより電子商取引システムにどのような影響があるのかを述べる．

[*1]RFC-1983によると，クラッカーとはコンピュータシステムに権限を持たないのにアクセスしようとする人物である．これらの人物は悪意を持っており，システムに侵入する多数の手段を思いのままに使う

2.1.1 ハードウェアクラック

ハードウェアクラックとは，カードリーダ・ライタ等のハードウェアの内部機構を解析し，その結果を用いて，ハードウェアの機能を無効化，追加，転用する行為である．そのため，ハードウェアクラックには極めて高度な知識が要され，実行するのは容易ではない．しかしクラックの成功は，ハードウェアの機能が失われるのと等価であり，そのハードウェアを用いているシステムに与える影響は大きい．当然，ある程度のハードウェアクラック防止対策が施されているが，完全に防止するのは想像以上に困難である．

例を挙げると，テレホンカードなどプリペイドカードの偽造がある．磁気を用いたプリペイドカードの偽造は比較的容易であり，かなりの数の偽造事件が発生している．現在では，偽造防止のためにＩＣカードを導入するケースもあるが，ＩＣカードもクラックされたという報告がある[3]．つまり，ＩＣカードも絶対に安全ではなく，ＩＣカードの安全性のみに依存しないような電子マネーシステムを構築する必要がある．

また，コピー防止機構を有するハードウェアのクラックも盛んであり，音楽関連機器，映像関連機器，家庭用ゲーム機などはすべてクラックされている．こうなると，デジタルコンテンツなどの違法コピーが蔓延し，それらを扱っている市場が退廃する可能性がある．

2.1.2 ソフトウェアクラック

ソフトウェアクラックとは，ソフトウェアを解析することにより，コピー防止機能の解除，機能の悪用などをする行為である．クラッカーは解析により得られた情報を用い，

- 情報入手
- 情報改竄
- 情報偽造
- システム破壊
- サービス妨害
- 踏み台

等の行為を他のコンピュータに対して行う．

情報入手は，顧客情報など機密性の高い情報やデジタルコンテンツが対象となる．このような情報の流出は，サービス提供側にとって顧客と社会的信用を失うことになり，サービスの存続が危ぶまれる．また，プロバイダー

などからパスワードが流出した場合，システムの乗っ取り，なりすましによる詐欺などの事件が起こる．

情報改竄は情報の価値を失わせたり，変化させる行為である．情報の改竄の内容が明らかであれば対処は容易であるが，社会的信用は失われる．しかし，情報改竄の内容が明らかでない場合，情報の真正性が保証されなくなり，情報に対する信頼が失われる．これは情報化社会において最も憂慮すべき事態である．

情報偽造は情報改竄とは異なり，価値を無断で生成する行為である．これにはデジタルコンテンツの違法コピーも含まれる．情報偽造の中でも電子マネーや電子公文書が偽造されると，現実社会とは異なり摘発も困難で，一瞬のうちにシステムが崩壊する恐れがある．

システム破壊は最も直接的かつ即効性のある妨害であり，情報の消去やディスクの消去等がこれにあたる．安定したサービスの提供こそが電子商取引成功への最低限の条件であり，商取引の停止は社会的信用に関わる．

サービス妨害(Denial of Service:DoS)は，コンピュータの処理能力以上のサービス要求を行うことにより，サービスを妨害したり停止に追い込む方法である．これは単純かつ容易に行うことができ，最も多く行われている妨害行為の一つである．

踏み台とは，別のコンピュータへ侵入するための足がかり，または，スパムと呼ばれる迷惑メールを送るために，コンピュータを無断で利用する行為である．これは身元を隠すための常套手段となっている．特にスパム行為は世界中で深刻な問題となりつつある．仮に踏み台にされると，相手にはそれが侵入元であるかのように見え，社会的信用は失われることになる．

2.2 クラッキングの手口

クラッキングの手口は多種多様であるが，ここでは代表的なクラッキングの手口を紹介する．

2.2.1 セキュリティホールの利用

クラッカーは相手のコンピュータに侵入するために，ソフトウェアに存在するバグ，特にセキュリティに関するバグ(セキュリティホール)を利用する場合が多い．そして侵入に成功すると，そのコンピュータ内を探索し，可能な限りパスワードなどの情報を収集する．最後に，次回の侵入のためにトロイの木馬や侵入口(バックドア)を設置し，侵入の痕跡を削除する．二回目以降は，前回までの侵入で得られた情報を元に，更に多くの情報を入手し，最終的にはそのコンピュータの管理者権限を取得することもある．

更に，セキュリティホールを用いてクラックする専用ソフトが開発されており，インターネットなどを用いて極めて容易に入手でき，安易な考えでクラックする人が後を絶たない．ただし，このようなクラックツールの一部は，裏を返せばセキュリティホール検知ツールとしても利用でき，一概に悪いと言えるものではない．

2.2.2 ウェブページの利用

悪質なモバイルコード(Java Script，ActiveX Controlなど)を埋め込んだウェブページを作成しておき，アクセスした人が気づかないようにコンピュータにアクセスする．他に，クラックの窓口となる可能性を有しているのは，CGI(Common Gateway Interface)スクリプトである．これは，インタフェースを通してデータのやりとりをするもので，他のコンピュータから情報を入手することも可能である．これは，企業対一般消費者向け電子商取引が発達した場合，クレジットカードや電子マネーの情報が流出する可能性を有している．

2.2.3 ソーシャルエンジニアリング

これは前述の手口とは異なり，人間の心理的な特性を利用した方法である．クラッカーは自分の身分を偽って，攻撃に必要な情報を関係者から直接聞き出す手口である．つまり人から情報を入手するため，ハードウェア，ソフトウェアによるセキュリティ対策が無効化されることもあり，より高度なクラック手口と言える．

2.3 コンピュータウイルス

1995 年に通商産業省によって告示されたコンピュータウイルス(以下，ウイルスとする)の定義[5]は，第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり，次の機能を一つ以上有するものである．

- 自己伝染機能
- 潜伏機能
- 発病機能

このような機能を有するものには現在数万種類発見されており，致命的な破壊を行うものから単なるジョークソフトまで，その種類と機能は様々である．

その中で最近特に増加傾向にあるのが，マクロウイルスである．マクロウイルスとは，マクロ機能[*2]を有するソフトウェアを基に作成されたものである．この種のウイルスは電子文書(契約書など)やデジタルコンテンツに混入されている．通常それらは電子メールを介して取引されるため，ウイルスは一瞬のうちに世界中に拡散され，その被害は深刻なものとなる．

3 セキュリティ対策の現状

コンピュータネットワークの世界に国境という概念は存在せず，従って国外からも容易に侵入を試みることができる．つまり，現実社会とは異なり悪意のある人物は世界中に存在することになる．実際，外国の政府機関が他国のコンピュータに侵入を試みているとの報告もある．このような状況下で，電子商取引のサービス利用者側，サービス提供側，ベンダーがそれぞれどのようなセキュリティ対策を行っているかを紹介する．

3.1 サービス利用者側

現在，コンピュータは一般家庭へ急速に普及しつつあり，それに伴い，インターネットショッピングを行う人も増加している．しかし，大半のユーザはセキュリティに対する知識は皆無であり，無防備状態であると言えよう．

例えば，電子商取引を行う際にクレジットカード番号など個人情報を暗号化を施すことなく送信してしまい，個人情報が流出してしまうケースがあとを絶たない．

一方，ソフトウェアに存在するセキュリティホールに対する対策は，極めて重要であるにも関わらず意識しているユーザは少ない．これはサービス提供側に対してもあてはまることである．

ウイルスについては，最近のコンピュータには最初から簡易なウイルス検知ソフトが付属していることが多いため，ユーザが意識することなくウイルスへの対応がある程度可能である．しかしながら，ウイルスのデータベースの更新を定期的に行わなければ，新種のウイルスに対応することはできず，充分であるとは言えない．

3.2 サービス提供側

インターネットを利用してサービスを提供している企業は，クラックに対して脅威を感じている．インターネット白書99[4]によると，クラックされた経験について，あると答えた企業は5%程度であるが，クラックに関しては気付かない場合も多く，ほぼすべての企業がなんらかの攻撃を受けていると考えるのが妥当であろう．それに伴い，年々ファイヤーウォールを導入する企業が増えている．更に，2割の企業がファイヤーウォール以外のセキュリティ対策を行っている．

また，1998年に米国コンピュータセキュリティ協会(CSI)[6]とFBIが調査したComputer Crime and Security Surveyによると，不正アクセスを受けたことのある米国企業のうち，実に89%が内部社員によるものだと考えていると報告されている．これは日本でも大差はないと考えられるが，社内でクラッカーに対する規制事項を設けている企業は約1割程度しかなく[4]，社内に潜む犯人に対する認識はないに等しい．

今後，公的サービスを提供する可能性がある官公庁のセキュリティ対策の現状は，極めて悪いと言わざるを得ない．その理由として，システム管理者は兼務であり，かつ，ボランティアである場合が多い．システム管理者がいない場合も少なくない．その為，システム管理に集中することができず，セキュリティ対策はおろそかになっている．また，管理者が把握していないコンピュータが無断で増設され，そこがセキュリティホールとなる場合も多い．つまり，管理方法の策定や管理者の育成は進んでいないのが現状である．

3.3 ベンダー側

ハードウェアベンダーは，クラックに対応するために様々な対策を行っている．一般には，容易に分解できないように特殊なネジを採用したり，ネジを用いない構造にすることが多い．しかし，これでもクラックを完全に防げているとは言えない．

ソフトウェアベンダーは，規約条項で逆コンパイルなどのクラック行為を禁止しているが，効果はほとんどない．また，不正コピーに対してもコピープロテクトや電子透かしなどの対策を講じているが，それもすべてクラックされている．また，セキュリティホールに対するサポートは，クラッカーの後手に回っているのが現状である．更に，セキュリティ設定は初心者にわかりにくく，かつその説明もなされていないことが多い．このように，ソフトウェアベンダーのセキュリティに対する対応は，完全とは言えない．

[*2]ワープロ等のアプリケーションソフトウェアに付随し，簡易なプログラミング機能を提供する機能

4 セキュリティレベル向上のために

4.1 サービス利用者側の対応

クラックへの対応として，セキュリティホールに対してソフトウェアベンダーから提供されているセキュリティ対策ファイル(パッチ)を当て，常に最新の状態にしておくことが第一である．勿論，これで万全というわけではないが，セキュリティレベルはかなり向上する．

ウイルス感染への対応としては，

- 最新のウイルスが検知·駆除可能なソフトを導入する
- バックアップをこまめにとる
- 動作不安定など，ウイルスの兆候を把握する
- 外部から持ち込まれるデータはまず検査する

などの予防策をとることによりほぼ完全に感染を防ぐことが可能である．

個人情報流出への対応には，情報へのアクセス権を適切に設定するとともに，暗号を導入することが最適である．また，様々な場面で必要となるパスワードについて，

- 目的ごとに別のパスワードを割り当てる
- 第三者に推測されにくいパスワードを使用する
- 定期的にパスワードを変更する

など注意を払うことも重要であろう．

4.2 サービス提供側の対応

電子マネー発行体や認証機関など電子商取引システムで重要な役割を担う組織は，セキュリティポリシーを作成することにより，組織的に系統立てた対策を講じるべきである．セキュリティポリシーについては，1999 年 6 月に，情報セキュリティ評価基準 (ISO-15408) が技術標準となり，セキュリティ基本設計書(セキュリティポリシー)の作成が規定されている．セキュリティポリシーは，

1. 運用システムが保護すべき保護対象資源の特定
2. 保護対象資源に対する利用方針の決定
3. 保護対象資源に対するセキュリティ脅威の識別
4. セキュリティ脅威や利用方針に対するセキュリティ対策方針の策定
5. セキュリティ対策方針を具体化するための機能要件や品質保証要件を情報セキュリティ評価基準書から選択

の順番で作成する．つまり，実際に行うことは

- 内部のネットワークと外部との接点において強固な保護手段を講じる
- ネットワーク構成を改良する
- 各コンピュータに対してパッチを当て，セキュリティレベルを設定する

となる．

しかし，このようなセキュリティポリシーを作成するには，高度な知識と組織力が要求される．そこで，比較的容易なセキュリティ対策としてファイヤーウォールの導入が考えられる．ファイヤーウォールとは，インターネットなどの信頼できないネットワークから組織内部のネットワークを保護するためのシステムである．通常内部のネットワークから外部はアクセスできるが，外部から内部のネットワークにアクセスが出来ないような1方向のアクセス設定がとられている．また，最近のファイヤーウォールには，DMZ(De-Militarized Zone) と呼ばれる機能が装備されている．これはファイヤーウォールに接続する第3のセグメントであり，ファイヤーウォールの内側からも外側からもファイヤーウォール経由でしかアクセスできない領域である．DMZ により内部から外部に対するアクセスを監視 · 制御することが可能である．ファイヤーウォールの実現方式として，パケットレベルでアプリケーションの使用するポートを制御するパケットフィルタ，TCP のソケットレベルで制御を行うサーキットレベルゲートウェイ，アプリケーションで内外のネットワークをゲートウェイするアプリケーションゲートウェイの3種類がある．

更に高度な対策としては，ネットワークをリアルタイムで監視し，攻撃や侵入を検知すると警報を発してセッションを切るといった，侵入検知システム (Intrusion Detection System:IDS) がある．IDS には大きく分けて2種類あり，1つは接続されたセグメントを流れる IP(Internet Protocol) パケットを監視し，疑わしいアクセスを見つけ出すネットワーク監視型，もう1つは，ホストごとにシステムやアプリケーションのログを監視し，疑わしいアクセスを見つけ出すホスト監視型である．

また，パスワードの利用形態 · 管理方法の改善として，ワンタイムパスワードがある．ワンタイムパスワード方式におけるパスワード生成方式は，

- 時間同期
- カウンタ周期
- チャレンジ & レスポンス

などがある．時間同期方式では，ログインする時刻によって生成するパスワードを変化させる．カウント同期方式では，トークンと認証サーバがそれぞれカウンタを保有し，ログイン毎に値を1つ増やす．このカウンタをパラメータとして，パスワードを生成する．チャレンジ & レスポンスでは，ログインの際にサーバから送られているパラメータを，トークンに入力してパスワードを計算する．チャレンジコードはログイン毎に変更されるため，ログイン毎にパスワードは変化する．どの方式でもワンタイムパスワードは，トークン(専用カード)に設定されたシードと呼ぶ値をパラメータとして生成する．シードはトークンごとに異なる値が設定されているため，トークンを紛失しない限りは不正アクセスはできないはずである．

4.3 ベンダーの対応

ハードウェアベンダーは，耐タンパー性を有するハードウェアの開発が更に必要であろう．

ソフトウェアベンダーにとって，バグが混入しないようにソフトウェアを開発することが理想である．しかし，高機能なソフトウェアは巨大化，複雑化しており，バグをなくすことは事実上不可能である．そこで，セキュリティホールに対処するパッチの開発速度と情報公開，配布形態の改善が望まれる．また，クラッカーによるソフトウェアの解析が困難となるように，ソースの難読性を高めるように設計することが必要であろう．

また，セキュリティ設定が容易となるシステムとインタフェースの設計，説明書の充実により，ユーザにとって扱いやすいソフトウェアの開発が必要である．

5 まとめ

サービス提供側やサービス利用側は，現在公開されているセキュリティ情報やパッチ，市販されているセキュリティソフトを用いることにより，ある一定水準以上のセキュリティは確保できる．

しかし，現在の電子商取引システムにおけるセキュリティの構築は，ハードウェアとソフトウェアにのみ頼っており，実際にそれを管理・運用する人に対しては何ら考慮されていない．つまり，電子商取引システムに関与する人のセキュリティ意識が低ければ，人そのものがセキュリティホールとなり，構築したセキュリティが意味を為さなくなる．実際に 2.2.3 節で紹介したソーシャルエンジニアリングは，人のセキュリティに対する意識の低さをついたものである．

そこで，電子商取引に関する解説(III)では，電子商取引システムに関わる人々の在り方について解説する予定である．

参考文献

[1] 日経ディジタルマネーシステム別冊：
“電子商取引のセキュリティ技術”，日経BP社 (1998).

[2] コンピュータ緊急対応センター：
“不正アクセスの動向”，
http://www.jpcert.or.jp/ (1999.9)

[3] 盛合志帆：
“故障利用暗号攻撃によるブロック暗号の解読”，
SCIS'97-6A

[4] 日本インターネット協会編：
“インターネット白書'99”，インプレス (1999).

[5] 情報処理振興事業協会：
“通商産業省告示第429号”，
http://www.ipa.go.jp/SECURITY/index-j.html
(1999.9)

[6] . “Computer Security Institute”，
http://www.gocsi.com/ (1999.9)