紹　介

佐々木良一
『インターネットセキュリティ入門』

澤　喜司郎

(I)

インターネットの普及には目覚ましいものがあるが，インターネットは全世界に広がり，どこから攻撃されるか分からないし，攻撃する側と防衛する側との間に技術力の差が存在する場合が多いため，インターネット社会では安全性（セキュリティ）に特に注意しなければならないという。つまり「インターネットは，コンピュータを利用するものであるため，テレビや携帯電話と違い，将来も人々の間での技術を利用する能力の差は残る。したがって，インターネット上で技術強者が弱者に対して攻撃を加えようとすれば，対策を適切に行っておかなければ簡単に実行されてしまう」のである。

さらに「インターネット社会を安全にすごすには，被害に遭わないようにするだけでなく，意識しないうちに加害者になったり，犯罪者になったりすることのないようにするための心構えと，具体的な方法を知っておくことが望ましい。無意識の加害は抵抗を生み，被害者になる可能性が高くなるからである。また，知らずに罪を犯すことは，国家から罰を受け一種の被害につながるからである」とし，「コンピュータやネットワークの知識をあまり持たない技術弱者」である「一般ユーザーがインターネット社会で被害者にも，加害者にも，犯罪者にもならないための方法を提示することを目的」として執筆されたのが本書である。

なお，本書の構成は

1章　はじめに
2章　インターネット社会に脅威が迫る
3章　安全を守る技術
4章　被害者にならないために
5章　加害者にならないために
6章　犯罪者にならないために
7章　おわりに

であり，本稿では各章の内容を要約的に紹介したい。

(Ⅱ)

インターネットは匿名性，不特定多数性，無痕跡性（無証跡性）など元々いろいろな危険をはらんでいるため，セキュリティが問題になるという。つまり「現在のネットワーク上では顔や声などの身体的特徴・実名をさらけ出す必要はなく，個人はそれぞれ付与されたIDとパスワードによってのみ識別され…したがって，他人のIDとパスワードを入手すれば，容易にかつ完全に他人に成りすますことができ，それを見破るのは現在では不可能に近い」ばかりか，「電子掲示板等にメッセージを掲載すれば，不特定多数の人間に容易に情報を伝達することができ…また，当該メッセージにおいて自らのIDを示せば，関心のあるものからの電子メールを受け取ることができ，見知らぬ者同士が容易に関係をもつことができる」とともに，「ネットワーク上ではコミュニケーションのすべてが電子データを活用してなされるため，物理的な痕跡は残らず，唯一の痕跡である電子データは瞬時に抹消することができる」のである。

そして，インターネットのグローバルでオープンな運用つまりアクセス対象者の非常な広がりやソフトウェアのオープン化，それにネットワーク管理主体の多様性等によってセキュリティへの脅威が増すことになるといい，「どのような倫理観，思想，信条，技術力を持った人がアクセスしているか分からない。…ゲリラ組織や，カルト的な宗教組織，さらには各種の犯罪組織もインターネット上にホームページを持っているといわれ…日本の従来の常識では計り知れないいろいろな脅威にさらされていると思っておかねばならない」し，「従来は，オペレーティングシステムや応用ソフトが違うので他のシステムに侵入できなかったり，そこでプログラムを不当に動かすことができないという…（それが）セキュリティ上の一種の防波堤になっていた」が，通信プロトコルや各種ソフトウェアのオープンなど誰にでも開かれたオープンなものであるインターネットでは「今やその防波堤が取り払われてきている」と指摘している。

また，インターネットはさまざまなネットワークの複合体であるため「その管理者にどのような人がいるかわからない。…電子メールなどでは，自分が直接アクセスしているサーバーから送信先のサーバーに至る過程でどのようなサーバーを経由して送られるかを事前に知ることは困難で…したがって，強い権限を持った管理者がその気になれば，データを盗み見したり改ざんしたりすることが比較的容易であ

る。また，セキュリティ対策を全くとっていないネットワークも存在する可能性がある」とし，とりわけ企業情報ネットワークのイントラネット化は「企業情報ネットワークのデータの破壊，改ざんなどの危険性を増大させ…このような破壊や改ざんは多大な損失を企業にもたらすだけでなく，この企業が，銀行や，鉄道，電話会社など公共性の高いものであった場合には国民生活に及ぼす影響も大きい」としている。

なお，インターネットのセキュリティに対する脅威には偶発的な脅威と意図的な脅威があり，偶発的なものには天災，故障，誤操作があり，それらは広義のセキュリティに対する脅威に含まれるが，本書では狭義の意図的なものを対象とし，この意図的なものには第三者の悪意の行為と，電子商取引における取引相手による脅威があるとしているが，以下，本稿では第三者の悪意の行為に限定して紹介することにする。

(Ⅲ)

第三者より加えられる脅威から守るべき対象はコンピュータやネットワーク上の情報であり，とくに通信路にインターネットを利用する場合にはインターネットを構成する通信路とそれに接続されたコンピュータ内の情報の安全性が対象になるという。そして，インターネットセキュリティに対する脅威には機密性の喪失，完全性の喪失，可用性の喪失の3つがあり，機密性の喪失とは不適切な主体にインターネット上の情報を見られることで，例えばインターネットに接続されているメールサーバーのパスワードが不当に盗まれるようなものである。完全性の喪失とはインターネット上の情報を不当に破壊，改ざんされることであり，可用性の喪失とはメールサーバーに大量の無効のメールを送りつけるという外部のコンピュータの不当な利用によって一般の利用者がメールを使えなくなるというようなものである。

なお，通信路上でのデータは，無線の場合は通常，周波数を合わせるだけで容易に傍受できるばかりか，ケーブルの場合でも間にプロトコルアナライザーを挿入すれば内容を知ることができ，またディスプレー上の表示内容は目で見なくても電磁波の状態を観測することにより理解できるといわれ，さらにハードディスクなどでのデータの読み出しは他人への成りすましやセキュリティホールの利用によって実現されうると指摘している。

悪意の攻撃者は外国のスパイ，テロリスト，犯罪者，企業スパイ，クラッカー等の愉快犯に大別されるが，家庭でインターネットを使っている場合にはクラッカー

等の愉快犯の攻撃に注意すればよく，このような悪意の攻撃者として第三者がインターネット上の情報や資源に攻撃を加える手段には直接的操作と間接的操作の2つがある。直接的操作とは悪意の攻撃者が他人に成りすましたり，セキュリティホールを巧妙に見つけてネットワークを経由して対象とするコンピュータに侵入し，ファイルなどへ攻撃を行うというもので，間接的操作とは悪意の攻撃者がコンピュータウィルスなどのソフトウェアを利用することにより，間接的にコンピュータ内のファイルなどへの攻撃を行うというもので，これにはフロッピーディスクなどを経由して侵入するものと，ネットワークを経由して送り込まれるものとがあると指摘している。

クラッカー等の第三者が侵入する手段には，他人への成りすましとセキュリティホールの利用があり，前者については現在の情報システムでは本人であるかどうかの確認はパスワードを知っているかどうかで行われているために，他人に成りすまして侵入するには他人のパスワードを使えばよいのであって，他人のパスワードを知るにはシステム管理者と嘘をつき，人を騙して聞き出すという方法と，本人や家族の誕生日，電話番号等を知り，そこから幾つかのパスワードを類推しつつ合致するまで繰り返す方法があるという。後者のセキュリティホールとは開発段階でテスト用などに開発した機能をそのまま残していたり，不正な侵入への配慮を欠いたために存在するもので，例えば古いバージョンのプログラムでは管理者権限で離れた場所からプログラムを立ち上げられるようになっており，そのプログラムをクラッカー等が立ち上げてしまった場合にはパスワードファイル等のデータを電子メールで送信されてしまう可能性が高いと警告している。

また，第三者が悪意の攻撃者としてインターネット上の情報や資源に攻撃を加える手段として利用されるコンピュータウィルスとは，フロッピーディスクやネットワークを経由してファイルからファイル，プログラムからプログラム，コンピュータからコンピュータへと増殖していく不正なプログラムで，これはユーザーが意図しないのに実行され，周りのプログラムやデータファイル，コンピュータシステムなどに被害を与える。そして，インターネットの世界では電子メールの添付ファイルを経由してコンピュータ内のファイルへ感染したり，WWWからダウンロードしたデータの中にウィルスが潜んでおり，感染する場合が多いと指摘している。

(Ⅳ)

セキュリティ対策の方法を知っておくことは，一般のインターネットユーザーが

セキュリティに対する適切な認識を持ち，具体的に何をしなければならないかを知る上で不可欠であるばかりか，不正行為を行おうとする人間の大部分は一般のユーザーに比べれば技術強者であるが天才ではなく，最近ではインターネットを経由して入手した攻撃ツールを使うだけの技術レベルの低いクラッカーが増加しているため，攻撃の8割以上はよく知られた攻撃法であり，そのため簡単な対策をきちんと行っているだけで安全性は大幅に高まるという。

セキュリティ対策は，侵入などの攻撃を防止する直接的対策と，侵入などの発生を予防したり，検知したり，発生前の状態に回復するための間接的対策に大別され，直接的対策にはアクセス管理や暗号化等がある。アクセス管理は直接的対策の中心をなすもので，攻撃対象である情報への不当なアクセスを防止することによりセキュリティを確保しようとするもので，それを適切に行うためにはユーザー認証とアクセス制御という2つの技術が必要となる。ユーザー認証は自分のパソコンへのアクセス時などに実施され，その認証技術には暗証番号やパスワード等の本人の知識を利用するもの，磁気カードやICカード等の本人の持ち物を利用するもの，指紋や声紋等の本人の身体的特徴を利用するものの3つがあり，現在のコンピュータシステムではパスワードだけを用いるものが中心である。しかし，パスワードだけで今後要求される安全性を守るのは難しくなってきており，安全性を高めるためには幾つかの対策技術を組み合わせて用いることが重要で，コンピュータシステムにおいてもパスワードとICカードを併用することによって安全性を高めるべき時期に来ているといわれ，それはユーザー認証に失敗して他人に成りすまされてしまったら，その後どんなに厳密な対策でブロックしようとしても本人に許されていることは成りすました人にはすべてできるからであると指摘している。

また，インターネットなどの分散システムでは，ネットワークを経由して離れた場所にあるサーバーにアクセスするときもユーザー認証を行う必要があるが，その場合にはパスワードなどの情報が通信路上で誰かに見られたり，その情報を記録し再送するリプレイスアタックといった脅威にさらされることになる。つまり，単純にパスワードを入力し，サーバーに送信するという方式ではネットワーク上で盗聴されることによりパスワードが盗まれ，その情報を使って第三者がパスワードの持ち主に成りすますことができるという。そのためユーザー側のコンピュータとリモートのサーバーの間で暗号鍵を共有し，パスワードを暗号化して送るという方法が考えられるが，通常パスワードはサービス要求時に繰り返し使用され，パスワードと暗号鍵が毎回同じならば暗号化したパスワードとして毎回同じデータが通信され，

このデータを盗聴して後で正当なユーザーと偽ってサービスを要求するときに盗聴したデータを送れば，サーバーは正当なユーザーが返すデータと区別がつかずに認証してしまうため，不正者は正しいパスワードを知らないまま正当なユーザーに成りすますことができると警告している。このようなリプレイアタックを考慮すれば，分散システムでは一般にユーザー認証のためにやり取りされるデータは毎回異なるもの（ワンタイムパスワード方式）にすべきであるという。

アクセス管理を適切に行うための方法としてはユーザー認証とともにアクセス制御があり，サブネットワークの入口でのブロック（ファイアウォール技術），コンピュータの入口でのブロック（コールバック方式等），ファイルの入口でのブロックなどのアクセス制御によって不正なアクセスを防御できるが，ユーザー認証に失敗し他人に成りすまされたり，セキュリティホールを利用して侵入された場合には無力であり，そのためアクセス制御は他人への成りすまし対策やセキュリティホール対策，さらには暗号化対策などと組み合わせて実施していく必要があるとしている。

（V）

アクセス管理が完全であれば管理領域内の情報は安全であるはずであるが，他人に成りすましたり，セキュリティホールを利用して不正に侵入されることも考えておかねばならず，そのような場合にも安全を保てるようにするのが暗号化技術であり，これは通信路のデータやファイル内の蓄積データなどの情報を入手されても情報を表す文字やデータを第三者に理解できなくするための技術である。そのため，第三者が情報を理解できないので機密性の喪失対策として有効であり，完全性の喪失対策のうち第三者にとって都合のよい改ざんをできなくするにも有効であるが，それ以外には効果がなく，暗号を用いてもファイルの破壊などは防止できないことを認識しておく必要があるという。

ビジネスの世界で用いる暗号はアルゴリズムを公開しても鍵さえ秘密に保てば安全の強いアルゴリズムになっており，アルゴリズム公開型暗号は共通鍵暗号方式と公開鍵暗号方式に大別され，前者は暗号化用の鍵と復号化用鍵が同じか容易に類推できる暗号方式で，後者は暗号化用鍵と復号化用鍵が異なり，一方から他方への類推が実質的に不可能な暗号方式をいう。両者を比較すれば，共通鍵暗号は公開鍵暗号に比べ処理速度が2～3桁速く，大量データの暗号処理に適しているが，通信路暗号に用いようとすると送る側と受け取る側で同じ鍵を持つ必要があるため，この鍵をどのように安全に送信し，共有するかという問題がある。これに対して，公開

鍵暗号には一対一に対応する2種類の異なる鍵があり，一方をみんなに公開し，もう一方を自分で秘密に保持するということが可能で，鍵管理が容易であるが，処理速度が遅いという問題があるという。いずれにしても，暗号がいったん破られ鍵が分かってしまった場合，同じ暗号アルゴリズムと鍵によって作成された暗号文はすべて解かれることになり，被害者にとっては暗号が解かれているということがなかなか自覚できないため，同じ暗号アルゴリズムを使い続けて被害を大きくしてしまうという危険があると指摘している。

そのため，セキュリティ対策をきちんと行うためにはアクセス管理や暗号化等の直接的対策だけでは不十分で，間接的対策もきちんと行わなければ本当のセキュリティは決して確保できないとし，この間接的対策はセキュリティへの攻撃に対し直接的効果はないが，そのような状況が発生しないよう予防したり（予防対策），発生しても直ちに検知し（検知対策），できるだけ早い回復を図る（回復対策）ものである。予防対策にはセキュリティ評価やセキュリティ教育等があり，このうち企業等におけるセキュリティ教育は外部からの攻撃に対して強い運用をするのに役立つと同時に，従業員が意識的，無意識的にコンピュータ犯罪に荷担するのを防止する効果もあるという。また，検知対策にはセキュリティ監視があり，それはシステムの運用段階で監視を続けることにより，セキュリティ犯罪の発生は直接防止できなくても発生の検知を早めたり，犯罪者が誰であるかを早く知るためのものであるばかりか，ネットワーク上の弱点（セキュリティホール等）を発見する機能つまりセキュリティ検査という機能もある。ただし，外部型検査ツールを悪意を持った人が使うと侵入可能なサーバーがどこにあるかが直ちに分かるため，犯罪を助けるものとなりかねない危険性を含んでいると危惧している。

なお，ウィルス対策用のワクチンプログラムも攻撃を検知し回復するための手段であり，一種の間接的対策であるとして，情報処理振興事業協会の「パソコンユーザーのためのウィルス対策7カ条」つまり①最新のワクチンソフトを活用すること，②万一のウィルス被害に備えるためデータのバックアップを行うこと，③ウィルスの兆候を見逃さず，ウィルス感染の可能性が考えられる場合はウィルス検査を行うこと，④メール添付ファイルはウィルス検査後に開くこと，⑤ウィルス感染の可能性のあるファイルを扱うときはマクロ機能の自動実行は行わないこと，⑥外部から持ち込まれたフロッピーディスクおよびダウンロードしたファイルはウィルス検査後に使用すること，⑦コンピュータの共同利用時の管理を徹底すること，を紹介した後，いずれも大切な提言であるが，「最近のウィルス被害は電子メールなどに添付

されたWordやExcelの文書ファイルについたマクロウィルスによるものが増加し…この場合は，電子メールを受け取ると自動的にウィルスもコンピュータの中に入ってくるようになったので，従来の対処方法だけでは効果がない。このため，予防や，ウィルス駆除の機能を持つワクチンプログラムが重要性を増してきている」が，新しいウィルスが次々に現れてきているため古いワクチンプログラムでは新しいウィルスには十分対応できず，そのため常に最新のワクチンプログラムを用いるのが望ましいと注意を促している。

(Ⅵ)

インターネット社会は，世界中の技術強者が攻撃を試みる可能性のある社会であるため，被害者にならないためには「自分の安全は自分で守る」という気概を持つ必要があるが，自分の力だけでは当然安全は守りきれない。そのため，気概を持ちつつ自分の限界をよく認識し，自分でやるべきことはきちんとやり，専門家に依頼することはきちんと依頼するということが大切であると説いている。

そして，一般ユーザーが自分で責任を持ってやらなければならないこととして，パスワード管理，ウィルス対策，暗号化の確実な実施，電子メールや電子掲示板の責任ある利用をあげている。

パスワード管理については，パスワードを安全に管理することは不可欠で，決して「パスワードを教えてくれ」などのインターネットプロバイダーからの依頼には不用意に答えてはならず，パスワードを盗まれると他人に成りすまされ，勝手に買物をされたり，詐欺などの別の犯罪行為の当事者にされ，損害賠償を要求される場合もある。そのため，パスワードは最初のログインの際に仮パスワードから正式なものに必ず変更すること，パスワードは３カ月に１回以上は必ず変更すること，パスワードは他人に秘密で管理し，パスワードを紙に書いて他人の目につきやすいところに貼るようなことを決してしないこと，パスワードは他人が推測し難いものにすること，パスワードをファイルに書き込んだり，通信路上を暗号をかけずに送ったりしないこと，他人が見ている前でパスワードを入力しないこと，パスワードは６文字以上にすることが必要であるという。

また，電子メールで秘密情報を送る場合には必ず暗号化して送付すること，秘密情報などデータのハードディスクへの格納時には必ず暗号化し，暗号化しない場合にはフロッピーディスク等の外部記憶装置に入れて施錠管理すること，情報操作時には情報を見られることが多いため長時間離席する場合にはパスワードロックをか

け，再ログイン時に正しいパスワードを入力しないと操作できないようにすること，WWW経由でウィルスが入ってきたり，プライバシーが侵害される恐れがあるため，信頼できるウェブサイトにアクセスすること，最近はWWWにアクセスするとクッキーがつき，どういうWWWにアクセスしたかという履歴が分かるようになっているため，プライバシーを守る場合にはクッキーを取り除くなどの対策をすること等が必要であると指摘している。

とくに，クッキー問題については「アクセス履歴を記録したクッキー情報から，アクセス傾向が分かり，プライバシーをおかされる可能性がある。さらに，これらのクッキー情報から不適切なWWWを覗く傾向があるということが分かり，それをインターネット上にばらまかれたくなかったら，金をよこせという恐喝が行われる可能性も否定できない」といい，プライバシー対策には特に注意すべきであるという。これに関連して，メールのアドレスを公表すると不特定多数の人から多様なメールが来ることを覚悟する必要があり，またインターネットを利用して買物をする時にはクレジットカードの番号や買物額が簡単に外部に漏れるようなシステムを利用してはならないと警告している。

(Ⅶ)

インターネットの利用においては，自分が意識しないで加害者になることがないようにするための心構えが必要であり，それは意識しないで加害者になることにより他人を傷つけないためであり，同時に害を与えることにより相手から反発を招き，自分が被害者にならないようにするためでもあるという。

インターネット社会で行動するにあたっては，法律がある場合には法律に基づいて行動し，法律がない場合にはエチケットのような社会的規範に基づいて行動しなければならないが，エチケットのような社会的規範がない場合には根源的規範である倫理といったものによって行動するしかないとした上で，どのようなエチケット(ネットワークの世界で守るべきエチケットはネチケットといわれる)があるかを知っておかないと，気づかずに他人に不愉快な思いをさせ加害者になってしまうことがあり得るとしている。そして，ヴァージニア・シャーの『ネチケット—インターネットのエチケット』(松本功訳，ひつじ書房，1996年)から，面と向かって言えないことを言ってはいけない，相手の時間を無駄に消費させたり，通信回線を浪費させてはならない，オンライン上では書いたものしか相手に伝わらないので相手に誤解を与えないような書き方をすべきであり，罵倒を誘うような書き方をしてはいけない，

罵倒自体を禁じるものではないが，それが繰り返される罵倒戦争はすべきではない，他人のプライバシーを尊重する，他人の小さなネチケット違反を大げさに指摘してはならない等を紹介している。

そして，これらは一般的なルールであり，メールを利用する時には非常に大きいサイズのファイルを送ってはいけない，不要な人にまで送らない，他人のメールは無断で第三者に公開しない等をあげ，とりわけ他人のメールや他人が作成したデータを転送する場合にはプライバシーや著作権の問題に十分注意する必要があると指摘し，またニューズグループに加入したり，メーリングリストに名前を登録してみんなで議論する場合には相手を誹謗中傷しない，公人としての発言か私人としての発言かを明確にし発言に責任を持つ，冷静になって議論し，あげあし取りのような議論をしない，他人のプライバシーに配慮する等としている。

なお，このようなネチケットがあるということは「現実のインターネットの世界では…面と向かっていえないようなことをいい罵倒しあったり，多量な無駄なメールを送り他人の時間と通信回線を浪費させたりということが起こっている」ということで，その「背景の一つに，インターネットのメールやニューズグループでは，書き言葉だけでやり取りされており，表情や音の調子が分からないので，相手に誤解を与えやすい」からであるといい，日本人の大部分はネチケットが大切だと思っているようであるため「神経質になりすぎる必要はないが，一般のインターネットユーザーがこれらのネチケットを守り，ぜひ，加害者にならないようにしてほしい」という。

(Ⅷ)

インターネットでの犯罪について，「コンピュータ内のデータを改ざんしたり破壊したりするような完全性の喪失にかかわる行為は，⑴電磁的記録不正作出（刑法161条の２），⑵電磁的記録毀棄（刑法258条，259条），⑶器物損壊（刑法261条），⑷電子計算機使用詐欺（刑法246条の２），⑸電子計算機損壊等業務妨害（刑法234条の２）などとなり，刑法に触れる犯罪行為となるようである。ところが，他人のデータを覗いたり，パスワードを盗んだりといった機密性の喪失にかかわる行為や，他人のコンピュータやネットワークを勝手に使ったりする可用性の喪失にかかわる行為は，日本では刑法に触れない。スイスと日本などを除く多くの国では，これらの行為も刑法で犯罪として取り締まっており，日本でも見直しの気運が高まっている」という。

著者は「本書の読者には，刑法に触れようと，触れまいと，データの改ざんや破壊，不正アクセスなどを故意にやろうとする人はいないと信じたい。問題は，意識しないで法を犯してしまうこと」であるとし，まず著作権の問題を取りあげ，ホームページを自分で作ろうとすると著作権の問題に十分注意しなければならないとしている。そして「自分のホームページから，別のホームページにリンクを張っておくこと自体は問題がないようだが，リンクを張るにあたり，一応，了解を得ておくのがルールになっている。ホームページに他人が撮った写真や他人が書いた長い文章を無断で入れれば相手の著作権に触れることになる。雑誌や，WWWなどに掲載された記事を一部引用することは可能である。しかし，その場合は，引用したことと，引用した著作物の題号と著作者名の表記は最低限必要であろう。WWWのホームページなどでタイトルなどの表記がないときはホームページのURLを記載する必要がある。URLを引用するのは，その内容が時間と共に変わり，引用したものが本当に掲載されているのかという問題があり，出典の記載法としては不十分だとする意見もある。…また，引用したことを明確にすれば，他人の書いた文章をそのまま記載してもよいといっても，全体の中で引用されたものが主となってはならないといわれ」，さらに「正式に購入したマルチメディアデータや，プログラムであっても，無断でコピーして他人に配ったら，当然のことながら，明らかな著作権法違反であり，損害賠償に応じなければならない」し，「他人の写真を本人の承諾なしに撮って，自分のホームページに掲載した場合は肖像権に抵触すると考えられる」としている。

次に，わいせつ図画公然陳列罪の扱いはインターネット以外の世界と基本的に同じで，わいせつ物と判断される写真などを自分のホームページに掲載した場合には，わいせつ図画公然陳列罪（刑法175条）に該当し，そのようなホームページにわいせつな写真や画像を提供した場合にはわいせつ図画公然陳列ほう助罪が成立する場合があるとするとともに，アメリカのサーバーを使った画像の開示に対しても警察はサーバーがどこの国にあろうと，日本人が日本から画像を送信している限りは国内犯であるとの考えで摘発を続けていると紹介している。

また，海外では認可されているが，日本では許されていない海外での賭博（例えばワールドカップの勝敗に対するイギリスのブックメーカーが主催する賭けなど）にインターネット経由で日本から参加することについては，いろいろな意見があるが，警察庁は「日本で許されていないことに日本から参加するので明らかに違法行為であるという」とし，さらにインターネットの世界においてもネズミ講の運営，加入，加入の勧誘は無限連鎖防止法で禁止されているばかりか，ネズミ講やマルチ

商法は自分が被害者であり，加害者であり，犯罪者にもなるので特に注意しなければならないと警告している。

(Ⅸ)

著者は「これからのインターネット社会は，さまざまな攻撃を受けるだろう。…セキュリティ対策は，これで完全かと言われると完全であるとは答えられない。これで十分かと言われれば，分からないとしか答えられない。しかし，私たちは完全とは言えなくても，セキュリティ，対策コスト，使いやすさ等を考慮しつつ，最善だと思う手を打ち続けるしかない。…そしていろいろな手を打っておけば，確実に安全性は高まる」と結んでいる。

また，著者は警察庁が356の企業と51の大学を対象に1997年に実施した「ネットワークセキュリティに関するアンケート」の結果を紹介しているが，本学部では自分のパスワードを留学生を含む学生に教えているスタッフもいるし，連番方式で機械的に作成されたパスワードを一方的に割り当てられるという現状では他のスタッフ等のパスワードを容易に知ることもできるという状況にある。

以上，やや詳細に本書の内容を紹介したが，それは多くのインターネットユーザーとりわけ学生諸君に本書をぜひとも読んでいただきたいからである。最後に，筆者が浅学非才なために本稿において本書の的確な紹介ができず，また筆者の不勉強による誤読の可能性もあり，この点については著者のご海容をお願いする次第である。

(岩波新書，1999年，206＋12頁，660円＋税)