講座 第4回

インターネット活用法

インターネットのセキュリティ

白橋 明弘*

SHIRAHASHI Akihiro

Security on the Internet

4 Series

Utilizing the Internet

[著者抄録] インターネットが爆発的に成長を遂げている現在、インターネットに多数の民間企業などが参加し、社会的に重要な情報が載るようになった。それに伴い、侵入などの行為を組織的に行う犯罪者も現れ、それに対する備えが必要となってきた。さらにインターネット上でのオンライン取引に対する期待が高まるとともに、暗号化や認証といった技術に対する要求も高まってきた。そのような中でのインターネットにおけるセキュリティの取り組み方、基本知識、技術について述べ、セキュリティ対策の重要性を論じた。

[著者付与キーワード] インターネット、パスワード、セキュリティ、電子メール、ファイアウォール、WWW、暗号化、認証

[Author Abstract] Presently Internet grows explosively and a number of private enterprises have participated to it and a lot of socially important information have come to be published on its screens. Accompanying with these facts, criminals who conduct systematically an intrusive act to Internet have been seen sometimes, so it became necessary to secure against such an act. Furthermore, both expectation for online commercial transaction on Internet and demand for materializing technologies to encipher and authenticate in Internet have greatly increased. In such circumstances, comments were made on how to come grips with security on the Internet, its basic knowledges and technologies. Moreover the importance of its security measures was discussed.

[Keywords by Author] Internet, password, security, electronic mail, firewall, WWW, encipherment, authentication

* ネットワンシステムズ(株) ネットワーク技術部
(〒140 品川区東品川2丁目2-8 スフィアタワー天王州) Tel. 03(5462)0871
Net One Systems (2-8, Higashi-shinagawa 3-chome, Shinagawa-ku, 140)

1. インターネットとセキュリティ

インターネットは学術用のネットワークとして発展してきた歴史を持ち、そこでは自由なコミュニケーションによるオープンな情報共有に重きがおかれ、ネットワークの安全性といった問題が重要な課題として問題になることはあまりなかった。ところが、商用ネットワークが登場しインターネットが爆発的に成長を遂げている現在、インターネットはより現実的なものになり、その上で実社会と同様の活動が行われるようになってきた。すなわち、インターネットに多数の民間企業などが参加し、社会的に重要な情報が載るようになると、侵入などの行為を組織的に行う犯罪者も現れ、それに対する備えが必要となってきた。さらにインターネット上でのオンライン取引に對する期待が高まるとともに、暗号化や認証といった技術に對する要求も高まってきている。そうしたセキュリティについての知識や技術を普及させ、またそれを実効あるものとするための組織的な努力は、ようやく端緒についたばかりといえる。

インターネットのセキュリティについては、様々な課題がある。第一に挙げられるのは、インターネットからの不正な侵入者-Cracker*-の攻撃に對する防衛である。Crackerは、データの消去やシステムの破壊、電子メールや一般的な機密情報そしてパスワードなどの情報の漏洩、またデータの改ざんや第三者へのなりすまし(偽称)のようなデータの改変、などを目的とする。自らの組織をインターネットに接続するにあたって、特に企業の場合は、これに對する十分な検討はもはや避けて通れない。

次に大きなテーマは、通信のプライバシーの問題である。暗号化電子メールの利用や、インターネット上を暗号化した通信路で結んで組織内通信

を安全に行う Virtual Private Network といった仕組みが利用可能になりつつある。暗号化技術はまた、ホストコンピュータや個人などの通信相手の確認-認証-技術の基盤としても重要である。これは、オンラインショッピングやその決済、あるいは企業間の電子取引 EDI の実用化に不可欠な技術であり、その標準化をめぐるいくつかの検討が続けられている。

2. セキュリティに関する事例

実際のところ、どの程度事件がインターネット上で起こっているのかについては、その性格上ほとんど公開される事はなく、したがって正確な統計なども得難い。しかし、後述する CERT の活動報告によれば、1995年の半年間で734件の事件に對応したとされており、そのうち組織的・大規模な事件に発展して世界中のネットワーク管理者を慌てて対策に走らせるようなケースも、数回起こっている。

有名な事件としては、推定10万を越えるパスワードが盗まれ「インターネット史上最大の脅威」といわれた“Network Monitoring Attack”や、IPアドレスを詐称することによって一部のルータ等のアクセス制限をすりぬけての侵入が問題になった“IP Spoofing Attack”などがある。また、一般マスコミでも報道され有名になったが、有名なCrackerのMitnickがインターネットに接続しているBBSから200万人分のCredit Card情報を盗み、日本人のコンピュータ・セキュリティ専門家である下村氏の活躍によってFBIに逮捕されたという事件もある。

インターネットに国境はないので、このような事件は日本にも被害を及ぼすことは当然ありうる。実際に、“Network Monitoring Attack”の事

* 一般的には、ハッカー(Hacker)という用語が使われているが、Hackerとはコンピュータのシステムのことを隅々まで知り尽くし、その能力を最大限発揮させるようなエキスパートという良い意味で使われてきた言葉なので、悪意の侵入者に対しては、Cracker(Crack=砕く)という呼び名を使う。

件では日本のいくつかの大学でも侵入を受けていたという事が報道されたりしている。日本ではインターネットの普及がようやく拡大期に入った状況であり、まだ深刻な問題はそう多くは起こっていない。しかし、大学・研究機関を中心に攻撃や侵入を受けたというケースは、ネットワーク管理者の間で知られているものだけでもかなりあり、何も対策をせずにインターネットに接続するのは、自分の家に鍵をかけないでおくようなものであろう。

それでは、学術研究組織などで守らなくてはならない情報は何かないので、インターネット利用の利便性を最優先にしてセキュリティ対策は必要ないという考えは正しいであろうか。そのような場合であっても Cracker の侵入をうければ、そこを中継点にされて犯行の足跡をくらすために使われる恐れがある。このような“踏み台攻撃”はむしろ一般的な事であり、最近ではガードの甘い日本の組織を踏み台用に狙ってくる Cracker もいるという話もある。つまり、自分の所のガードが甘ければ、結果としてインターネット全体に迷惑をかける恐れもありうるのである。実際、海外のサイト(ネットワークあるいは計算機)から、あなたのサイトから侵入を受けたという連絡があって調べてみると踏み台にされていたというケースや、逆に海外のサイトから自分のところを踏み台にあなたのサイトに侵入していた者がいるので注意してほしいという警告を受ける場合もある。また、自分の所は有名じゃないので、攻撃の対象にされる事はないだろうという考えも甘い。インターネットに接続されたばかりの組織はコンピュータやネットワークの設定が不十分な事が多く、極端な話システムアカウントがベンダー出荷のパスワードのままなどという例もあるので、わざわざそのようなサイトを探しだして攻撃してくる Cracker もいる。

以上のように、インターネットに接続する組織では、セキュリティに対する正しい知識をもって対処する努力は不可欠であるといつてよい。安全はただでは手に入らないという至言は、インター

ネットにおいても同様であり、まずその意識を高めていく努力が必要であらう。

3. セキュリティに取り組む考え方

さて、それではインターネットに接続するにあたって、セキュリティ対策にはどのような考えをもって取り組めばよいかを考えてみよう。セキュリティ対策では、技術的な細かい議論よりも、セキュリティについての管理方針—セキュリティ・ポリシー—を確立することが大切である。

インターネットに接続する組織といっても、大学、非営利研究機関、企業の研究開発部門、企業の事業部などその立場は様々である。利用の仕方としても、学術研究なのか、プライベートな連絡用なのか、商取引なのかでもその防御の必要性は違ってくる。まず何をどのレベルまで守る必要があるかははっきりさせる必要がある。場合によっては、組織内の部門によって防御の必要性のレベルが異なりそれに対応した対策を行わなくてはならない場合もあるであろう。

ここで重要なのは、セキュリティと利便性は二律背反である事を認識する事である。すなわち泥棒を防ぐために家に鍵をたくさん付けければ安全性は確かに増すが、家族が家に出入りするための手間は面倒になるというように、セキュリティと使い易さの両方を完全に満足させることは不可能である。セキュリティ対策を導入する際は、この使い易さが損なわれる部分があるという点をよく評価する必要がある。

極端なケースでは、ノーガードならインターネットの使い勝手はもっとも良い。しかし、セキュリティについて何も考慮しないという態度はインターネット全体に迷惑をかける恐れがあり、広く世界に広がった現在では、もはや受け入れられない状況にある。逆に危険を恐れるあまりインターネットに接続しないというのは、インターネットの非常に大きな可能性を考えれば、本末転倒ともいえる考えである。インターネットに接続するにあたっての危険は、正しい知識を持てば十分に評

価およびコントロールできるものだ、という認識を持つ事が大切である。

セキュリティと利便性はトレードオフであるが、コストをかけることにより両者を向上させる事ができる。この場合のコストには、セキュリティ対策に必要なハードウェア・ソフトウェアのような目にみえるコスト以外にも、例えば組織内でセキュリティのマネージャを育成する、そこまでの余裕がない場合は外部のコンサルタントにセキュリティ管理を任せる、あるいは教育啓蒙活動などといった人的な要素も含まれる。

以上のような点に十分配慮して、最良と思われるセキュリティ対策を導入したとしても、バグのないソフトウェアはないように完全なセキュリティ対策というものはない事を理解しておく必要がある。新たなセキュリティ上の問題が生じる場合もあるし、侵入者の手口も高度化する。また、運用上の齟齬(そご)で問題がおこるケースもありうる。セキュリティを保つためには、継続的に努力する必要がある、それにはコストがかかるという事である。

4. パスワードの重要性

“Network Monitoring Attack”をはじめとする多くの侵入事件では、計算機のパスワードを不正な手段で入手して、アカウントを破るという手口が使われている。例えば、UNIX のパスワード

は、8文字までのパスワードを一方通行の関数で暗号化してパスワードファイルに書き込んでいく。ユーザが入力したパスワードにこの暗号化関数を適用して、登録済の暗号化されたパスワードと一致することで認証を行っている。

コンピュータのめざましい高速化によって、このパスワードシステムは必ずしも完全とはいえなくなっている。すなわち、ユーザがパスワードを覚え易い様にと地名、人名、物の名前等辞書に載っている単語などから選んだとすると、その辞書をひきながら次々に暗号化していき、不正な手段で入手した暗号化パスワードと比較していくというやり方で元のパスワードを見つけたという方法「辞書引き攻撃」が、現実的な時間で可能になったのである。残念なことに、安易なパスワードをつけて、このような「辞書引き攻撃」の餌食になってしまうユーザが少なくない。これに対処するには、まずユーザ教育が大切である。「良い」パスワードを選ぶ基準は表1に示すようなものである。

さらに、最近のスーパーコンピュータや超並列マシンを使うと、辞書に頼らずすべての組合せをしらみつぶしにあたることも有限の時間内で可能である。幸いというべきか、そういったコンピュータはまだどこにもありふれているというわけではないが、この可能性に対抗するには、表1にあるようなパスワードの設定に注意するくらいしか対策はない。

管理者にとって問題なことは、このような注意

表1 「良い」パスワードを選ぶ基準

- 1) 辞書にない文字列を選ぶ
- 2) 辞書にある文字列に1文字付け加えたり、順番をいれかえたり、二つの単語を合成したりしたものも不可
- 3) 日本語(をローマ字表記したもの)も不可、最近は日本語の辞書もいろいろなものが出回っている
- 4) 人名、アイドル名、近親者の名前・相性、地名などは使用しない
- 5) 8文字を全部使う
- 6) 英大文字・小文字、数字、記号を(すべて)混ぜて使う

を多数のユーザに周知徹底させることが、非常に困難なことである。そこで、これを強制的にチェックするためには、手間はかかるが、パスワードチェックプログラムで、危ないパスワードを設定しているユーザがいるかどうか定期的に検査する。またユーザがパスワードを設定するときにチェックして、あぶないパスワードの場合は再設定を要求するといった方法がある。また、利用している計算機システムが暗号化パスワードを一般ユーザからはアクセスできないファイルに保存する機能を提供している場合は、これを使用するのも有効な対策である。

現在のパスワードシステムのもう一つの大きな問題点は、ネットワーク上を平文のパスワードが流れる事である。したがって、LAN 上のパケットをモニターログインを監視すると、パスワードを盗むことが簡単にできる事である。“Network Monitoring Attack”ではこれを組織的に行われたために、被害が膨大な範囲に及んでしまったわけである。特に出先からインターネットを介して自組織のコンピュータに接続する場合には、この危険は見逃ごせない。万一、出先の LAN がそのようなモニターをされていた場合、その被害を自分の所にまで広げる手伝いをしてやる事になりかねない。これを防ぐためには、“One Time Password”(一回使い捨てのパスワード)を使用することが普及してきている。

“One Time Password”のシステムでは、生のパスワードがネットワーク上を流れることはないように、システム側が生成したランダムなキーまたは順序番号(チャレンジと呼ばれる)を Local 環境(Local にしかアクセスされない端末ワークステーションのようなもの)で入力したパスワードと演算した結果(レスポンスと呼ばれる)を入力してシステム側に送りかえて照合することで、安全な認証を実現している。“One Time Password”としては、S/Key や現在標準化が進行中の OTP などが代表的である。また、チャレンジ&レスポンス方式は、ダイアルアップ PPP 接続の際の CHAP 認証、POP プロトコルでメールサーバに

アクセスする際の APOP 認証などでも用いられている。

5. セキュリティ監査ツールの活用

UNIX のチェックをするフリーソフトのツールとして COPS (Computed Oracle and Password System)がある。COPS ではシステム関連のファイル・ディレクトリ・デバイスのアクセス権、各種設定ファイルのアクセス権や内容、パスワードファイルの内容などのチェックを行ってくれる。

中の守りをかためるいわば内部監査である COPS に対して、外部監査ツールとしては ISS (Internet Security Scanner)や SATAN (Security Administrator Tool for Analyzing Networks)がある。これらを用いるとネットワーク経由で攻撃を受ける可能性のある既知のさまざまなセキュリティホールについて外部からチェックを行うことができる。

しかし、これらのツールは Cracker に悪用されるおそれがあるばかりでなく、そこまで至らなくてもいたずらに使われる可能性も高い。実際、ISS が後に非公開になってしまったのは、濫用されて ISS によるアクセスが問題になったことと、公開するにはあまりに危険なノウハウが盛り込まれていたためといわれている。また、SATAN についても WWW による簡単なユーザインタフェースが提供されていた事もあって、登場時にはその是非がかなり議論になった。しかし、こうした情報は秘密にしておくよりも公開された方が長期的にはセキュリティを高めることができるのではないかと考えるべきであろう。

6. 不正なアクセスの防止と監視

外部からの不正なアクセスに対処するには、ホストシステムのセキュリティホールを塞ぐ、あるいはパスワードの管理を厳重にするというような消極的な方法の他に、アクセスを防止、監視そし

て撃退するという積極的なアプローチもある。

ネットワークを介してのアクセスに応答するのはUNIXではデーモンと呼ばれるサービスプロセスであるが、システムに標準のデーモンは大抵寡黙で詳しいログは残さないし、IPアドレスなどによるアクセス制限ができるものも少ない。例えば“Network Monitoring Attack”でターゲットにされたTFTPプロトコルのデーモンは一切ログを残さない。これでは、後から侵入の痕跡も調べようがない。これをログを残しアクセス制限もできるものに入れ換えて、例えば通常のアクセスはlocal LANからのものに制限し、それ以外の不正なアクセスはログに残すようにすれば、はるかにセキュリティは強化できる。

UNIXのデーモンは数が多いが、TCP Wrapperというパッケージを使ってデーモンの親玉プログラムであるinetd (super daemon)を置き換えると、inetd経由で起動される全てのデーモンについて、アクセスのログの取得・アクセスの制限・ブービトラップが可能となる。ブービトラップとは、ある条件のアクセスがあった場合に、登録したコマンド(例えばアクセス元にfingerをかける)を実行する機能で、ちょっかいを出してくる不心得者を追跡するのに役に立つ場合もある。

7. ファイアウォールによる防御

7.1 ファイアウォールによる防御の考え方

最近のようにワークステーションやPCが安価になり、一人一台の環境があたりまえになると、多数のコンピュータをきちんと管理する事はきわめて困難になる。新米のユーザにセキュリティ対策を期待することはできないし、有能で献身的な管理者がいたとしても、一人で面倒を見られるコンピュータの台数にはおのずから限度がある。すべてのコンピュータの安全性を高めるというやり方は実質的に無理になっているのが現状である。

そこで登場したのが、ファイアウォール(防火壁)の考え方である。内部(組織のLAN)と外部

(インターネット)を接続する部分に情報の壁を設けて、外部と内部の間のアクセスをその壁の所で制限することによって、内部のコンピュータの安全性を効率よく高めようという方法である。

インターネットへの接続の必要上、外部から直接アクセスできることが必須なネームサーバやメールサーバ、あるいはWWWなどの情報提供などの機能をはたすコンピュータについては、ファイアウォールの外に設置をするか、内部に中継する仕組みを置く。こうすることで外部に対してむき出しのコンピュータは高々数台程度にできるため、きちんと管理して集中的に守ることは十分に可能である。

どのレベルのアクセス制限を行うかは、組織のセキュリティポリシーから決定されるべきものであり、例によってセキュリティと利便性はトレードオフの関係にある。ファイアウォールの技術の要は、いかにセキュリティを維持しながらサービスを提供するかにあるわけであるが、もちろん万能ではない。ファイアウォールを導入することによって、何が失われるのかをよく評価して、その導入を決定する必要がある。

7.2 ファイアウォールの構成

ファイアウォールというものは、単一の製品や技術をさすものではない。様々な技術を組み合わせて、ネットワークの安全性を確保するための総合技術である。その性格上、単にファイアウォールの部分だけでは閉じず、IPレベルの接続性からアプリケーション、オペレーションのレベルまでインターネット接続のすべての側面に関わりが生じる。それだけに、ネットワーク全体のデザインをよく考慮に入れて、ファイアウォールの導入を進めなくてはならない。

ファイアウォールを構成する要素としてはルータ、“Dual Home Gateway”，そしてその他のサービスホストなどがある。ルータは一般にインターネットとの接続の部分に使われるが、多くのルータ製品はある程度のアクセス制限の機能を持つ。その性格上ルータだけで本格的なファイアウォー

ルを構成することはできないが、簡易もしくは補助的にルータのアクセス制限の機能を使用する事はよく行われる。

“Dual Home Gateway”はネットワークインタフェースを2個以上持ち、それぞれ外部接続のセグメントと内部接続のセグメントに接続されて、ファイアウォールで中核的な役割を果たす。内部と外部の間の通信はすべてここを通過しチェックやアクセス制限が行われる。また、外部と内部のサービスを中継する仕事も“Dual Home Gateway”上で行われることが多い。

さらに、“Dual Home Gateway”以外にもホストが外部接続のセグメントに置かれる場合もある。これらのサービスホストは、ファイアウォールの他の構成要素と連携して、中継サービスやインターネットサーバの機能などを果たす。

もちろん、これらの外部から直接アクセス可能なホストについては通常にもまして厳重に管理(要塞ホスト化)する必要がある、一般的な注意の他にも、例えば管理者以外のアカウントは作成しない、必要のないデーモンや機能はすべて停止しておく、などの対策も必要であろう。

ファイアウォールのアクセス制限のレベルは、組織の方針によって決まるものである事は既に述べたが、よく採用される代表的な形態としては、以下のようなものがある。

(1) 特定のプロトコルのみ禁止

TFTPやNISなど、その性格上外部からのアクセスされることはないプロトコルのみをフィルタリング(選別)する。この程度のフィルタリングだとルータの機能でも可能であり、比較的手軽に導入できる。大学や学術研究機関など、どちらかというとセキュリティよりも自由な利用環境を重視する組織で採用される。

(2) 特定のプロトコルのみ許可

内部から外部への通信は全て許可する。逆に外部から内部への通信は特定のプロトコルだけ許可するというやり方。その性格から、半透明ファイアウォールとも呼ばれる。ルータだけでも構成可能であるが、“Dual Home Gateway”上でフィル

タリングのソフトウェアで実現される事もある。うまく設定すれば内部からの使い勝手にはほとんど影響を及ぼさないで、セキュリティを重視する研究機関などで採用される。

(3) IP フォワード禁止

“Dual Home Gateway”でのIPパケットのフォワード(選出)を禁止する。すなわち、外部と内部でのIPレベルの接続性はない。もっとも厳しいファイアウォールで、狭義ではこれを指してファイアウォールと呼ぶ場合もある。もちろんそれだけではなくサービスが使えなくなってしまうので、同時にファイアウォールをゲートウェイとして、上位層(circuit levelやapplication level)での中継サービスを動かすことによって、メールやニュースの中継、内部からのftpやWWWの利用を可能にする。商用のファイアウォール製品にはこのタイプが多い。

7.3 パケット・フィルタリング

前節で述べたように、ファイアウォールのタイプは、内部と外部の間でIPパケットをフォワードするものと、しないものに分類することができる。前者をパケット・フィルタリング、後者をアプリケーション・ゲートウェイと呼ぶ。それぞれに、利点・欠点がある。

パケット・フィルタリングではIPパケットの通過を(送信元アドレス,ポート番号,送信先アドレス,ポート番号)の組み合わせで許可・禁止する。許可されたパケットは直接宛先のコンピュータに届く。パケット・フィルタリングは柔軟な設定が可能なのが特徴で、例えばインターネットで新しいアプリケーションが登場した時に(本当にそうして安全かどうかは検討が必要であるが)対応することはやりやすい。また、処理のオーバーヘッドが少なく、アプリケーション・ゲートウェイと比べて、一般に性能は高い。反面、正しい(安全な)設定をするにはプロトコルに関する知識が必要で、IPパケットを一つ一つ独立に検査するという性格から、単純なフィルタリングではうまく対応できない場合もある。

パケット・フィルタリングは、ルータで行うことも可能であるが、通常のルータのアクセス制限の機能は設定も煩雑であり、またログをとることができないので、正しい設定がされているかのチェックができないという欠点があるので、あくまで補助的なものと考えておいたほうがよい。ソフトウェアのパケットフィルタリングとしては、DEC で開発されたフリーソフトの *screend* や、商品のものとしては、Check Point Software 社の *Fire Wall-1* などがある。*Fire Wall-1* は数少ない商用のパケットフィルタリング型のファイアウォールで、GUI による設定や、単純なフィルタリングでは対応できないケースにも上位層まで検査することによって対応しているなどの特徴を持つ。

7. 4 アプリケーション・レベル・ゲートウェイ

IP パケットをフォワードしない代わりに、上位層での中継サービスを提供するタイプのファイアウォールを、最近ではアプリケーション・ゲートウェイタイプのファイアウォールと総称して呼ぶことが多い。

昔から「出島ホスト」方式のファイアウォールというものがあり、外に出るには一旦出島ホストにログインしてから *telnet* や *ftp* をするというやり方におなじみの方も多いと思う。アプリケーション・ゲートウェイも機能的にこれと似ていなくもないが、大きく違うのは、ゲートウェイのマシンのアカウントにログインはしないで中継を行うことである。そのため、一旦接続した後では、例えばインターネット上の *anonymous ftp* サーバから直接手元のマシンにファイルを転送することができる。また、ゲートウェイ上のマシンに潜在的な弱点となるユーザのアカウントを作成する必要はないというメリットも生まれる。

中継の方法によって、単に TCP のポートレベルでの中継を行いプロトコルの中身にまで触れないものをサーキットレベルのゲートウェイとよぶ場合もあり、SOCKS などが代表的なものである。また、WWW の HTTP proxy など、プロトコル

的にも中継の仕組みが取り入れられクライアントもそれに対応したものをプロキシ (代理) サーバと呼び、*telnet* や *ftp* などのプロトコル毎の中継を行うものを狭義のアプリケーション・レベル・ゲートウェイのように区別する場合もあるが、その名称の使い分けはそれほど明確ではない。

利用者の観点からは、クライアントを使用する時に一旦ゲートウェイに接続して外部への中継を頼むという操作を意識する必要があるかどうかの違いが重要である。HTTP proxy などの場合は、中継の仕組みがプロトコルの中に組み込まれているので、最初にクライアントでプロキシサーバの設定を行えば、その後ユーザがそれを意識する必要はない。それに対して *telnet* や *ftp* の場合はそのような配慮はないので、ユーザが一旦ゲートウェイに接続して、改めて接続したいドメイン名を入力するという二度手間が必要となる。これは、アプリケーション・ゲートウェイの弱点の一つである。

クライアント側でファイアウォール対応と称して、この手間を自動的に処理してくれるものもあるが、ファイアウォール毎に処理は違うので万能とはいかない。この問題を解決するために、最近の商用ファイアウォール製品では、transparent proxy (透過プロキシ) とよばれる技術が採用されているものが増えている。これは、*telnet* や *ftp* のパケットを検出して (そのために、ゲートウェイのホストを内部の default gateway として経路設定しておく必要がある)、対応するサーバを自動起動して対応させるもので、ユーザには中継サーバの存在を見せない手法である。

アプリケーション・ゲートウェイは、アプリケーション層まで見て処理をするので、パケットレベルでの細工をしてくる侵入手口を未然に排除できる可能性が高い、また実装によってはきめの細かいコントロール、例えば *ftp* の *get* は可能だが *put* は駄目といった制御をすることもできる。その代償としてオーバーヘッドが大きく、高速な回線 (6Mbps~) でインターネットに接続している場合や、組織内の LAN 間接続に使用する場合は、

その性能評価を十分に行う必要がある。

また、マルチメディア系のアプリケーションなどで使用される事の多いUDPはほとんどのアプリケーション・ゲートウェイ型のファイアウォールでは利用できない。パケット・フィルタリング型のファイアウォールでならUDPを通せるが、それが偽造されたパケットによる攻撃などに対して安全というわけではないので、十分な注意が必要である。危険をおかしてまでUDPをサポートする必要があるかどうかはよく検討するべきである。UDPを利用するサービスのうちでも、DNSはインターネットの利用に不可欠なので、これは当然サポートする必要がある。そのために、アプリケーションゲートウェイ型のファイアウォールでは、自身がDNSサーバとなってDNSの問い合わせを中継する機能を持っているものが多い。この考えをすすめて、メールサーバやニュースサーバ、ftpやWWWのサーバなどの機能を持ち、一台でファイアウォールとインターネットサーバの役割を果たせることを特色にしている商品もあるが、ファイアウォールの上で動かすソフトウェアを徒に増やすことは、安全性を低下させる可能性があることに十分注意しなくてはならない。

一般的には、アプリケーションゲートウェイ型のファイアウォールは、セキュリティを重視し、その代わりに使えるアプリケーションは電子メールとニュース、WWW程度で十分と割り切れるような場合に適しているといえる。もちろん、おしきせではなく設定変更やソフトウェアを追加するなどすれば、より多くの要求に対応することは可能であるが、それには十分な技術的検討が欠かせない。

アプリケーションゲートウェイの場合、IPパケットを直接中継しないので、内部のアドレスは外部に直接見えない。したがって内部にはNICから正式に割り当てをうけたglobal addressではなくprivate addressを使用することができる。昨今のようにIPアドレスの枯渇が問題になりその浪費を押さえなくてはならない状況では、pri-

vate addressを利用するためにファイアウォールの設置が必要となるケースも増えてきている。

7.5 Circuit Level Gateway と Proxy Server

ここでは、ファイアウォールでの中継サービスの例として、Socks, httpd proxy serverそしてDele Gateについて解説する。

(1) Socks

Socksは、比較的古くから利用されている技術である。アプリケーションのソケットインタフェースの部分を入れ換えて、直接宛先に通信するかわりにゲートウェイ上で動いているデーモン(sockd)と通信を行なうようにし、sockdが外部との中継を行なうことによって、ユーザは自分のマシンから普通に対話的アプリケーションを使用することが可能になる。

sockdは1種類だけゲートウェイ上で動かせばよいが、ユーザが個々のホストで使用するクライアントは個別にSocks対応のものをインストールする必要がある。UNIX上では、ftp, telnetをはじめとして多くのアプリケーションがSocks対応のものが入手できる(Socks対応のクライアントはrftp, rtelnetなどと呼ばれることが多い)し、そうでないものもソースコードがあればSocks化することは可能である。

しかし、最近需要が増えているPCやMacintoshのクライアントに対してはSocks対応されているものはあまりなく、ソースコードも提供されていない場合がほとんどなので、Socksは使用することができないという弱点がある。

(2) CERN httpd

CERN httpdはWWWのサーバであるがファイアウォール上での利用とデータのキャッシュを目的とした代理サーバの機能をもった最初のサーバである。

Mosaic/Netscapeに代表されるWWWクライアントのリクエストは、直接相手に送られる代わりに、ゲートウェイ上で動作しているproxy serverに送られそこで外部に中継される。外部のサーバからのレスポンスは逆方向に中継される。

これによって、ファイアウォールの中から WWW でインターネットにアクセスすることができるようになっている。その利用には Proxy server 対応のクライアントが必要であるが、現在出回っている Xwindow, PC Windows, Macintosh 用のブラウザはすべて proxy 対応である。

WWW では、native のプロトコルである http だけでなく、gopher, ftp, WAIS などのプロトコルも扱えるが、直接接続の場合はクライアントがじかにこれらのプロトコルをしゃべるのに対して、proxy の場合はクライアントと代理サーバの間はすべてのプロトコルが http に変換されて送られ、代理サーバ上でプロトコル変換が行なわれるという仕組みになっている。http proxy を導入するとこれらのプロトコルも同時に中継することができるわけである。

組織内で 2 重、3 重にファイアウォールが構築されている場合(例えば本社と支社の間)でも、個々のファイアウォールごとに httpd proxy server を設定し、その間を多段でつなぐことによって対応できる。

なお、CERN httpd は最終バージョン 3.0A がリリースされ、開発が終了した。また、負荷の重い環境では性能上の問題があることも知られているので、今後は Netscape proxy server のような商用サーバや、proxy 専用としてデザインされている高性能な SQUID、また次に述べる Delegate などへの移行が行われていくと予想される。

(3) Delegate

Delegate は電総研の佐藤豊さんが開発した汎用の proxy server である。扱えるプロトコルは http (WWW), gopher, nntp (Net News), ftp から始まって、Whois, Telnet, X, NNTP, SMTP, POP, CU-SeeMe に及んでいる。Delegate は、最初は gopher を利用するために開発されたので、proxy の規約のない gopher で使用できるように、リクエストおよびレスポンス中のアドレスを双方向で変換する機能を持っていた。Delegate は、現在進行形で開発が続けられており、新しい機能が追加されているが、特に有用なのは、中継

に際しての漢字コード変換機能や MIME ヘッダのデコード機能などのフィルター機能である。例えば、日本語に対応していない WWW や Mail, News のクライアントでも Delegate と組み合わせることで十分に利用可能になるものは少なくない。

また、セキュリティ関連で重要なのは「マウント」機能である。httpd proxy server によってファイアウォールの中から外の WWW サーバにアクセスすることは可能になったが、内部のサーバを外部に公開するのにこれを利用することはできない。WWW サーバを外部に公開するためにはファイアウォールの外側のインターネットからアクセスできる場所にサーバを設置するのが一般的である。しかしそうすると、そこにサーバのデータの保守作業のためのアカウントを作ることになるので、セキュリティ上はあまり好ましくない。そこで、データの作成は内部で行い ftp でデータを公開用サーバに転送するなどの手法が使われているが、データの更新が即時に反映されないなどの不満が生じる。

そこで、delegated をファイアウォールのゲートウェイないしは要塞ホスト上で動かし、ファイアウォール内の本来のサーバを「マウント」するように設定すれば、外からの delegated へのアクセスは内部のサーバへのリクエストに中継される。中継に際しては delegate が URL のアドレスを書き換えてくれるので、外からのユーザから見ると、まるで内部のサーバがつぎこまれて(マウントされて)いるように見える。この機能を使えば、ファイアウォールの管理と WWW サーバの管理をうまく分離させることができる。

8. 暗号化問題

8.1 電子メールの暗号化

現在普通に利用されているインターネット電子メールには、セキュリティのための仕組みは何もないに等しい。原理的には、盗聴や改ざんや第三者に成りすましてのメール送信などが可能であ

る。もっとも実際には盗聴行為などにあう危険は、例えば通常の加入者電話が盗聴される危険と比べてそれほど重大であるとはいえない。プロバイダーの設備やデジタル専用線に物理的にアクセスする事は簡単ではないので、直接宛先に配送される電子メールはかなり信頼してよいものだと考えられる。しかし、デジタルデータの性格上、いったん盗聴行為が仕掛けられると非常に効率良く大量のデータが盗み出される可能性があることには留意しておかなければならない。また、もし内部犯行が行われると防ぎようがないという弱点もある。そういう実質的な安全性は別として、インターネットが現実的なものになってくると、現実世界の書留郵便に相当する仕組みが、電子メールでも必要になるのは当然の事である。それに答えるのが暗号化電子メールである。

暗号化電子メールの目的は、三つある。まず、本文を暗号化することによって盗聴を防ぐことである。次にチェックサムを付けることによって内容の改ざんが行われた際にそれを検出できるようにする。三つ目は、電子署名を添付することによって差出人を間違いなく特定できるようにすることである。これの裏返しで、本人がそのメールを出した事を否認できなくすることができる。これによって、電子メールで契約書を送り、係争がおきた時に(技術的には)裁判の証拠として使うことが可能になる。

実際に、暗号化メールのソフトウェアとしては、PGP (Pretty Good Privacy) や PEM (Privacy Enhanced Mail) といったものが開発され、ワークステーションや PC の上で利用できるようになっている。これまで、あまり普及しなかったのは、良いユーザインタフェースがなかった事と、後節で述べるような暗号・認証技術の問題点があったからであるが、そうした問題も解決しつつあるので、今後は本格的な普及が期待されている。

暗号化電子メールを支えるのは二つの暗号技術の組み合わせである。一つは米国政府が標準的に採用している DES に代表される、送り手と受け手で共通の鍵を使う秘密(共通)鍵暗号である。こ

れは、メール本文の暗号化に使われている。共通鍵暗号だけでは、送受信する間であらかじめ別の手段で鍵の交換を安全に行わなくてはならないので、不特定多数の間のメールのやり取りには使えないというジレンマがある。

この問題を巧妙に解決したのが、RSA に代表される公開(非対称)鍵暗号である。公開鍵暗号では、二つのペアの鍵を生成し、そのうち一つを公開してしまう。ペアの一方の鍵で暗号化したデータは、もう一方の鍵でしか復号化することはできない。したがって、送り先の公開鍵で暗号化して送ればそれは送り先が持っている秘密鍵でしか解読できない。この仕組みを使って、本文の暗号化に使う秘密鍵や Message Digest と呼ばれるチェックサムなどを送るとというのが暗号化電子メールの基本的な仕組みである。電子署名も、ある人の秘密鍵で暗号化したデータがもしその人の公開鍵で解読できたら、それはまちがいがなくその人が暗号化したデータだという特性を利用している。

8. 2 WWW のセキュリティ

インターネットをこれだけ普及させる原動力となったのは、いうまでもなく World Wide Web である。したがって、その上でオンラインショッピングや契約ユーザ向けの情報提供などを行いたいという要望は早くからあった。ところが、WWW でやり取りされるデータについてはいっさい暗号化などはされていない。このために、インターネットでオンラインショッピングをする際にクレジットカードの番号を送るのは危険であるという常識が定着してしまった。しかし、考えてみると、インターネットの WWW のやり取りでクレジットカード番号を送るのと、誰が読むのかわからない FAX でそれを送るのとどちらが危険であろうか？ また、インターネットで送ろうが、店頭で本人が使おうが、良からぬ店ならカード番号を悪用される事は同じである。そうすると、実際的には過度に心配することもないように思われる。問題はむしろクレジットカード会社がまだインターネット上での取り引きに対して対応体制ができていない事

である。インターネット上の使用で被害にあった場合、カード会社による保証が適用されない可能性があるし、一部のカード会社ではそもそもインターネット上での利用を認めないところもある。そのあたりはルールが確立するまでは自己責任でという事になるのであろう。

それはさておき、本格的なオンラインショッピングへの活用にはやはり暗号化や認証・決済の仕組みが必要なことは間違いない。ここでも使われる基本的な仕組みは暗号化電子メールと同じく、公開鍵暗号と秘密鍵暗号の組み合わせである。業界標準をめざして、WWW Consortium の提案する shhttp(secure http)と Netscape Communication 社の SSL (SecureSocket Layer), そしてやや遅れて Microsoft 社から SST/PCT というプロトコルが提案されている。それぞれクレジットカード会社などと連携をして、標準作成の競争を繰り広げている。プロトコルの濫立はユーザの利益にはならないが、一つのブラウザが複数のプロトコルに対応することは可能であるので、独占よりも競争がある事はむしろ良いことであろう。

8.3 暗号・認証技術の問題点

暗号化電子メールや WWW の認証技術の普及のためには、大きな問題がある。それは、暗号技術そのものの問題である。

暗号技術は、米国連邦政府にとって国家安全保証上重要な技術であり、米国外への輸出に厳しい規制をかけている。具体的には、DES を実装したソフトウェアの輸出は原則禁止、Netscape Navigator にも使われている RSA 社の秘密鍵暗号の鍵の長さが輸出分は40bit に制限されている。また、PGP を開発した P.Zimmerman 氏が DES のコードを含む PGP のパッケージを anonymous ftp サーバに置いたことが輸出にあたるとして訴追を受ける恐れにさらされている。しかし、国際情勢の変化、インターネット・コミュニティや自由な輸出を望む業界の働きかけもあって、これまでほとんど認められなかった案件ベースの輸出承認で、RSA の開発キットの日本への輸出が許可さ

れたり、Zimmerman 氏への訴追の調査が中止されたり、米国政府の態度も変化してきている。そうはいえ、米国以外で独自の暗号化技術を開発し、それを標準として広める努力は欠かせないであろう。

もうひとつは、万能解読キーの問題である。米国では日本と違って犯罪捜査のために裁判所の許可があれば電話の盗聴ができる。暗号に対しても同様の論理を適用し、政府の保有する特別の鍵ですべての暗号が解読できるように義務付けるというわけである。Clipper Chip とよばれる暗号チップにこの機能を埋め込もうとした政府は、インターネットを中心とする市民からの猛反発にあっていている。

暗号システムそのものの安全性の問題もある。そもそも暗号の安全性というものは絶対的なものでない。暗号そのものに欠陥があって簡単に解読されてしまうというのは論外としても、一定のコスト(主として計算機のパワー)をつぎ込めば暗号は破れると思ったほうがよい。つぎ込むコストが、暗号を破ることによって得られる利益より十分大きければ安全といえるだけである。例えば、Netscape の SSL の輸出向けの40bit の暗号は多数のコンピュータを使った力任せの解読で破られたが、これは SSL が30秒に一回キーを変更していることも考えれば今の所は問題ではない。しかし、暗号の設計は安全でも、それをソフトウェアに実装する際に問題が起こる場合もある。Netscape Navigator1.2の SSL や、Microsoft の Windows95のパスワードキャッシュの暗号化で問題になったのがこれで、どちらもキーを生成する所の実装が安易であったため比較的簡単に推測されてしまうというものであった。

一方、認証のほうにも問題がある。個人の認証を行うための電子署名の仕組みそのものはうまく働くことが実証されているが、証明書をどこが発行するのかという問題がある。それは政府なのかプロバイダーなのかクレジットカード会社なのか? 現実には、お金のやりとりと直結する WWW の分野では、ブラウザのベンダーと提携し

たクレジットカード会社が認証局を立ち上げてきている。そうすると、今度は複数のカード会社の間の相互認証をどうするかという問題が持ち上がる。また決済などの仕組みは国ごとの商習慣により異なるのでそのあたりのローカライズと統合をどうするかという点もこれからの問題である。電子メールの認証のほうでは、U.S. Postal Service が全米の市民を対象に認証局を運営する計画を進めており、そのような大規模でもシステムがうまく働くかどうか注目される。

日本でも最近のインターネットや電子商取引 (Electric Commerce) への関心の高まりを背景に、通産省のバックアップで「認証実用化実験協議会」や「電子商取引実用化推進協議会」などで技術開発や実証実験などの取り組みがはじまっている。

8. 4 IP プロトコルの暗号化

パスワードの盗聴や改ざんなどの問題が起こるのは、IP パケットそのものに暗号化・認証の仕組みがないせいである。IPv4 と IPv6 の両方に適用できる暗号化・認証の枠組みとして IPSec (RFC1825~RFC1828) が提案されており、ファイアウォール間をセキュアなトンネルで結び仮想的なプライベートネットワークを実現する VPN (Virtual Private Network) 用などに利用されはじめており、今後の普及が期待される。また特定目的には、ワークステーションやパーソナルコンピュータに組み込んだり、LAN に挿入する暗号化専用装置の製品も販売されている。

現在その開発が進行している次世代 IP プロトコルの IPv6 ではセキュリティの強化が重要な課題の一つになっていて、IPSec で提案されているセキュリティ機能は標準的に採用される予定である。AH (Authentication Header) によってパケットの改ざんを防止するチェックサムをつけ、データ内容の暗号化をするには ESP (Encapsulating Security Payload Header) とよばれるヘッダを使用することになっている。現在は、暗号の鍵を管理するためのプロトコルについて、活発な検討

が行われている。

9. セキュリティ情報の入手

セキュリティに関する情報は、頻繁にアップデートされており、緊急度の高いものが多いので、ネットワーク管理者はつねに最新の情報をフォローしておくように心がける必要がある。

(1) ネット・ニュース

セキュリティに関する情報がながされるニュース・グループとしては

comp.security.announce
comp.security.unix
jp.inet.security.announce
fj.comp.security

などがある。後 2 者は日本国内のものである。

(2) メーリング・リスト

国内の IP 接続しているサイトの管理者のメーリング・リスト ip-connection では、緊急度の高いセキュリティ関連情報、例えば「どこそこのサイトから怪しげなやつが侵入しようとしてアクセスしているので注意!」といった警告が流される場合がある。

また、セキュリティの技術についての情報交換を行う国内のメーリングリスト fire-talk もある。

(3) CERT/CC

CERT/CC (Computer Emergency Response Team Coordination Center) とは、Internet Worm 事件の教訓にかんがみ、コンピュータおよびネットワークの安全を脅かすような事態に対処するべく APPA の支援によってつくられた組織である。ここでは、セキュリティ・ホールとなる OS やプログラムの問題点に関する情報を収集し、CERT Advisory として配布している。CERT Advisory はネット・ニュースで流されており、バックナンバーは <ftp://ftp.cert.org/pub/cert-advisories/> から入手できる。

(4) CIAC

DOE の支援を受けた CIAC (The Computer Incident Advisory Capability) という組織もある

る。こちらは(PCやMacintoshを含む)ウィルス関連の情報が豊富なのが特徴。バックナンバーは<ftp://ciac.llnl.gov/pub/ciac/bulletin/>から入手できる。

(5) JPCERT/CC

日本でも、遅ればせながら通産省などの支援をうけて日本版CERT(JPCERT/CC-日本コン

ピュータ緊急対応センター)の設立が準備中であり、96年秋から活動を開始する見込みである。正式にサービスがスタートするまでの問い合わせ先は、(財)日本情報処理開発協会(JIPDEC)情報セキュリティ対策室(TEL:03-3432-9387 E-mail: jpcert@jipdec.or.jp)。

参 照 文 献

- 1) カッコウはコンピューターに卵を生む, クリフォード・ストール
- 2) Practical UNIX Security, S.Garfinkel & G. Spafford, O'Reilly & Associates, Inc. 邦訳: UNIX セキュリティー, 山口英監訳, アスキー出版局
- 3) インターネット環境のセキュリティ, 山口英, 東田学, IP Meeting '94 Proceedings <ftp://ftp.jepg-ip.ad.jp/pub/jepg-ip/ipm94/1007/part2/security.ps.gz>
- 4) Hitch-hiker's Guide to Network Security. 白橋明弘, <ftp://ftp.s.u-tokyo.ac.jp/net/security/doc/hitch-hiker-guide.ps.gz>
- 5) CIAC Bulletin E-09 "Network Monitoring Attacks" <ftp://ciac.llnl.gov/pub/ciac/bulletin/e-fy94/e-09.network-monitoring-attacks>
- 6) CIAC Bulletin E-12 "Network Monitoring Attacks Update" <ftp://ciac.llnl.gov/pub/ciac/bulletin/e-fy94/e-12.net-monitor-attacks-update>
- 7) Network Monitoring Attacksに関するメモ, 市原卓, 白橋明弘. <ftp://ftp.s.u-tokyo.ac.jp/net/security/doc/network-monitoring-attacks.gz>
- 8) Crack Version 4.1, A Sensible Password Checker for UNIX, Alec.D.E.Muffett, Aberystwyth, Wales, UK <ftp://coast.cs.purdue.edu/pub/tools/unix/crack/>
- 9) The Cops Security Checker System, Purdue University Technical Report CSD-TR-993 <ftp://coast.cs.purdue.edu/pub/tools/unix/cops/1.04/>
- 10) Firewalls and Internet Security---Repelling the Wily Hacker--- Cheswick & Bellon, Addison-Wesley, 1994. 邦訳: インターネット接続でのファイアウォール, 川副博監訳, ソフトバンク
- 11) UNIX MAGAZINE 1994年5月号~1996年8月号 転ばぬ先のセキュリティ, 山本和彦
- 12) UNIX MAGAZINE 1994年8月号, ファイアウォールと proxy, 吉村伸
- 13) 企業ユーザのためのインターネットハンドブック, PART5 セキュリティ編, 日経 BP 社 <http://www.phys.s.u-tokyo.ac.jp/people/sirahasi/security.html>
- 14) 日経コミュニケーション, 1995.7.3. No.201 特集インターネットの危うさと付き合い
- 15) インターフェース1995/9, 特集「マルチメディア時代のインターネット技術」, Chapter4 ファイアウォールの基礎と実際, 谷村透
- 16) 暗号についての FAQ <http://www.rsa.com/rsalabs/faq/faq-home.html> <ftp://ftp.rsa.com/pub/faq/faq.asc>
- 17) ファイアウォールについての FAQ <http://www.v-one.com/pubs/fw-faq/faq.htm>
- 18) ファイアウォール製品リスト <http://www.access.digex.net/bdboyle/firewall.vendor.html>
- 19) E-Mail セキュリティ, B.Schneier 著, 力武健次監訳, オーム社

- 20) WWW のセキュリティ <http://www.w3.org/hypertext/WWW/Security/Overview.html>
- 21) passwd+ <ftp://ftp.dartmouth.edu/pub/security/>
- 22) AntiCrack <ftp://ftp.cs.titech.ac.jp/pub/security/anticrack/anticrack-1.1.tar.Z>
- 23) S/KEY N.Haller, The S/KEY (TM) One-Time Password System, Proceedings of the Internet Society Symposium on Network and Distributed System Security <ftp://thumper.bellcore.com/pub/nmh/>
- 24) TCP wrapper <ftp://coast.cs.purdue.edu/pub/tools/unix/tcp - wrappers/>
- 25) screend <ftp://ftp.vix.com/pub/vixie/>
- 26) Socks <ftp://coast.cs.purdue.edu/pub/tools/unix/socks/>
- 27) TIS firewall toolkit <http://www.tis.com/Home/NetworkSecurity/Toolkit.html>
- 28) CERN httpd <ftp://info.cern.ch/pub/www/src/cern - httpd.tar.Z>
- 29) Delegate インターフェース1995/9, 特集「マルチメディア時代のインターネット技術」, Chapter5多目的プロキシ・サーバDeleGateの機能詳細, 佐藤豊 <ftp://etlport.etl.go.jp/pub/DeleGate/INTERFACE-95-09.ps.gz>
- 30) SATAN <http://www.fish.com/satan/>
- 31) IP Spoofing Attack <ftp://ftp.cert.org/pub/cert - advisories/CA-95%3A01.IP.spoofing>
- 32) プライバシ強化メール PEM の公開運用実験, 菊池浩明, IP Meeting '94Proceedings, <ftp://ftp.jepg-ip.ad.jp/pub/jepg-ip/ipm94/1007/part3/pem.ps.gz>
- 33) RSA 社のセキュリティ技術の輸入に成功 <http://www.bug.co.jp/topics/rsa - jap.html>
- 34) Letter from Phil Zimmerman <http://www.netresponse.com/zldf/>
- 35) Netscape security update <http://www.netscape.com/newsref/pr/newsrelease46.html>
- 36) CIAC Bulletin G-06 : Win95Vulnerabilities <ftp://cica.llnl.gov/pub/ciac/bulletin/g-fy96/g-06.Win95.Vulnerability.asc>
- 37) エレクトリックコマース推進事業 <http://www.ipa.go.jp/ASTP/ec-j.html>
- 38) インターフェース1995/6, 情報制御技術としての暗号(3), ユーザ認証(Kerberos)とホスト認証(IP/Secure), 満保雅浩&岡本栄司
- 39) IPv6の技術動向, 西田佳史 IP Meeting '95 Proceedings <ftp://ftp.jepg-ip.ad.jp/pub/jepg-ip/ipm95/1130/conference/ipv6.ps.gz>
- 40) ファイアウォールの性能をテスト, 日経コミュニケーション1996.2.19No.216 <http://www.data.com/Lab - Tests/Firewalls.html>
- 41) PGP URLs <http://www.ipa.go.jp/STC/MMP/people/pgp-link.shtml>
- 42) ツトム・ヤマシタ, ジョン・マーコフ著, テイクダウン <http://www.takedown.com/>
- 43) コンピュータ不正アクセス対策基準 <http://www.ipa.go.jp/SECURITY/ciadr/crack-gl.txt>
- 44) 認証実用化実験協議会 <http://www.icat.or.jp/>
- 45) S/WAN RSA IPsec Interoperability Forum <http://www.rsa.com/rsa/SWAN/>