家庭での常時接続における security

Security in continuous connection at home

青井 桂子，水田 伯典
Keiko AOI，Takanori MIZUTA

Abstract: Today, mainly the analog circuit is used to connect to the Internet. However, since the users of the Internet have increased rapidly, the circuit is often jammed. Many users are asking for the high-speed communication. In this paper, I would like to describe the continuous connection and the problem of security at home.

1　はじめに

これまで，家庭でのインターネットの接続手段はアナログ回線 (56kbps) によるダイヤルアップ接続が主流であった．しかし，昨今では加入者が急増したため回線が混みあい，インターネットを快適な速度で利用できるとは言い難くなった．一般家庭で常時接続をするには，月額数万円以上もする専用線を利用するしかなかった．その中で安価で高速な常時接続を求めるユーザー側のニーズが高まった．これまでは大学や企業などの一部のものであった常時接続が家庭において増えつつある．
本発表では常時接続とセキュリティの問題について示し，その対策を紹介する．

2　家庭での常時接続

2.1　ネットワーク接続の普及率

現在の日本のインターネットの普及率は約 20 %，2,500 万人程度である．そのうち，100 万人足らずの人が高速通信での常時接続サービスを利用している．昨年来，高速接続の DSL や CATV 接続のサービスが本格的にはじまり，アナログモデムから乗り換えるユーザーは増えている．その様子を Fig. 1 に示す．

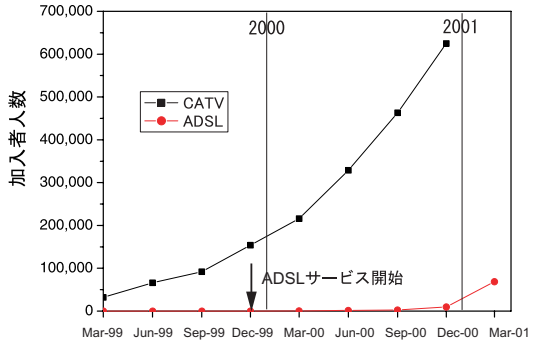

Fig. 1　常時接続の加入者の変遷 [1)]

2.2　接続の形態

現在，日本で普及しつつある常時接続の接続方法は主にフレッツ ISDN，ADSL，CATV インターネットの 3 つである．Table 1 に各々の特徴を述べる．

Table 1　常時接続の接続形態 [2)]

	ISDN	ADSL	CATV
通信速度 *1	64/64 kbps	250/640 kbps*2	100/512 kbps*2
初期費用	2,800 円	27,000 円	22,000 円
月額料金	4,950 円+ α	6,300 円	6,000 円
エリア	全国	首都圏 県庁所在地 (一部除く)	全国 (一部除く)

*1 上り[1]/下り[2]
*2 通信速度は一例

- フレッツ ISDN
  NTT が各県に準備した地域 IP 網と呼ばれるネットワークを利用する．ADSL と CATV に比べメリットが少ないが，初期費用が安い点や全国的に均一なサービスが受けられる点では優位に立つ．

- ADSL
  既存の電話回線をそのまま利用できる高速通信サービスで，電話線に電話とは別の波長帯の信号を流し，その上でデータの送受信を行う．現在は都市部でしか利用できないという欠点がある．

- CATV インターネット
  テレビ放送用のケーブル網を使ったインターネット接続サービス．現在 130 社以上の CATV 事業者が市区町村単位で提供している．サービス対象地域であってもマンションなどでは導入できない問題がある．また地域ごとに提供事業者が異なり，料金や通信速度などサービスに偏りがある．

近年光ファイバー (Fiber To The Home:FTTH)[3]で光多重通信という新しい技術が登場して更なる通信容量の大容量化が可能になる．

[1]ユーザからプロバイダへの通信
[2]プロバイダからユーザへの通信
[3]ガラス繊維でできた通信ケーブルにより，光信号で通信を行う．一本のケーブルで数百 Mbps と大容量である．

3　security 問題

現在，一般家庭レベルにおけるネットワーク攻撃というとメールに添付ファイルをつけてウイルスを送ることなどが主流である．常時接続が普及するとさまざまなスキャンやアタックなどが行われ，何らかのセキュリティ対策を講じないと知らない間に被害者どころか犯罪者の濡れ衣まで着せられる可能性もある．つまりインターネットに常時接続するということは，常時外部からの危険にもさらされているということである．

一般に個人ユーザーのセキュリティに対する認識は甘いと思われる．外部に公開する Web サーバーを運営しているわけでもないし，守るべき重要なデータはパソコンには入っていないとして無防備な状態で長時間インターネットに接続しがちである．

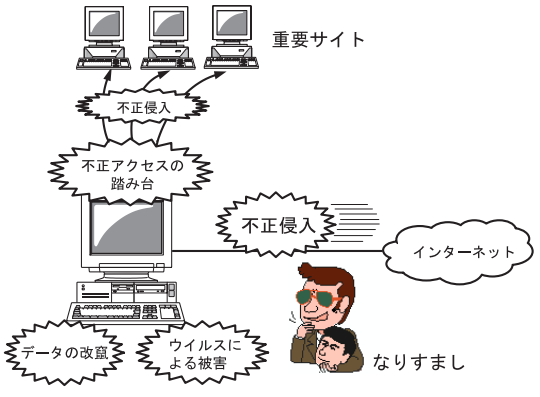

Fig. 2　常時接続サービスに潜在するリスク

ウイルス対策は一般ユーザーからコンピュータのプロフェッショナルまで幅広い層で対策がとられているものの，個人用ファイアウォールを設置する必要性の認識は未だ低い．米 Symantec 社の調査から，一般消費者の 87.1 %, プロ技術者の 94.7 %がワクチンソフトを利用しており，ウィルス対策はしっかりと行われていることが分かった．しかしながら，常時接続環境ではこれだけでは不充分である．その実例として以下に被害例を示す．

- IP Spoofing
  IP アドレス偽装攻撃．
- 不正侵入
  リソース (資源) 消費，他サイトへの攻撃の踏み台，機密情報への不正アクセスなどが行われる．
- DoS 攻撃
  標的の機器 (サーバやルータ，クライアントのマシンなど) をハングアップさせたり，ネットワークのトラフィックを増大させたりなどしてネットワークの機能を麻痺させる．
- 盗聴
  ネットワーク上を平文で流れるパスワードやメールの中身を盗聴する．
- 踏み台・不正中継
  他サイトへの攻撃・SPAM メールの中継．

これらの不正侵入を受けた PC は事前に必ずポートスキャン[4]が行われる．ポートスキャンはログの解析で，検出が可能である．しかし，不正侵入された時には外部からの侵入を防ぐための防御壁，ルーターやファイアウォールが必要になる．しかし，ファイアウォールを個人的に設置している人は一般消費者で 19.5 %，プロ技術者でも 48.9 %にとどまっている．

4　security 対策

ルーターやパーソナルファイアウォールのフィルタリング機能により外部からの不要なパケットを制限する．一方で，パーソナル IDS ではパケットを監視し，不正な行為などをチェックするネットワーク型とサーバーのログ情報を解析して，不正な行為などを検出するホスト監視型がある．これらは不正侵入や DoS 攻撃を防いでくれる．これらの概念図を Fig. 3 に示す．

その他にインターネットを利用していない時は接続を切る，Windows の共有設定を見直す．PC ベンダーやプロバイダーのデフォルト設定の見直しなどが必要である．

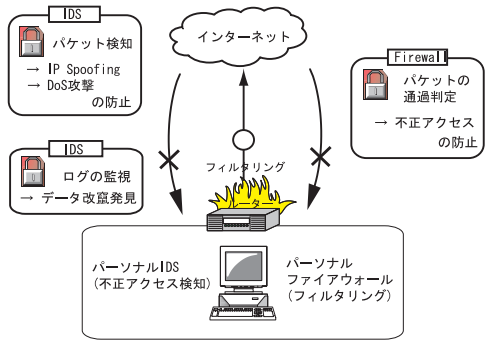

Fig. 3　セキュリティ対策の概念図

5　今後の展望

現在は常時接続の利便性や高速性に比べ，リスクが軽視されがちである．しかし今後，常時接続が一般的になればセキュリティ問題が社会問題として大きく掲げられ，セキュリティに対する危機意識とその対応が，ますます必要になる．常時接続の市場拡大に伴い，セキュリティ関連産業，技術が発展する．将来的に高いセキュリティ技術が提供されることになるが，最終的にセキュアな環境を構築できるかどうかは，ユーザの意識改革そのものである．

参考文献

1) http://www.ntt.co.jp/

2) 日経コンピュータ 2001.1.29

[4]不正アクセスの準備段階，つまり攻撃するターゲット PC を見つけたり，ターゲット PC の上で動作している攻撃しやすいサービスを見つけたりするために行われる．