5H－03

個人ユーザ向けの常時接続端末におけるセキュリティ保護技術に関する研究開発　～概要～

森尻 智昭†, 池田 竜朗†, 大岸 伸之††, 吉井 大吾†, 才所 敏明†
†(株)東芝 SI 技術開発センター, ††東芝情報システム(株)

1　はじめに

近年、急速に家庭向けの常時接続サービスが普及し，ユーザ数も着実に増加している．また，政府は 2000 年 1 月 e-Japan 戦略を決定し，インターネット網の整備を進めている．しかしその一方で，セキュリティに関する意識や知識は，個人・家庭ユーザでは概ね低い水準にあるのが現状である．

そこで，個人ユーザが使用する常時接続端末のセキュリティを維持するには，ユーザ自身がセキュリティポリシーの作成や設定を容易に行えるようにするための仕組みや，ISP(Internet Service Provider)などによるセキュリティポリシーの作成／設定サービスが必要になってくる．

しかしそれでも，適切なセキュリティ設定がされていない常時接続端末も多数存在する可能性があり，この様な常時接続端末は DoS(Denial of Service)攻撃，DDoS(Distributed DoS)攻撃，そして不正アクセスの温床となる可能性がある．そこで，IP アドレスが詐称されたパケットに対しても，送信元を特定できる仕組みが必要になってくる[1]．

本稿では，個人ユーザ向けの常時接続端末に対する，セキュリティポリシーの簡易設定／集中管理，および IP トレースバックの概要について述べる．

2　セキュリティポリシー簡易設定

家庭内の個人向け端末のインターネット接続環境は複雑化しており，ファイアウォールや各種サーバを備えた環境も増加している(図 1)．ところが，環境の複雑化にともない，セキュリティ設定も複雑化しており，一般の個人ユーザがすべての機器のセキュリティ設定を適切に行うことは難しい状況になってきている．

コンピュータに対する深い知識がないユーザが容易にセキュリティポリシーの作成と設定を行うことができるようにするには，ユーザインタフェースが解りやすいものである

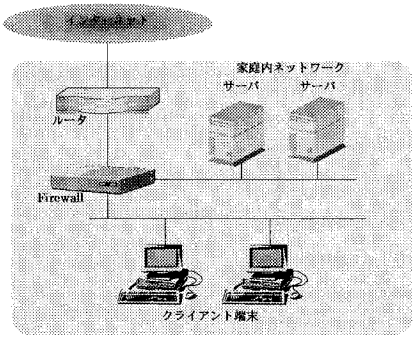

図 1 家庭のインターネット接続環境

必要がある．現在，パーソナル・ファイアウォールやウィルスチェックソフトなどにしても，個人ユーザ向としては比較的複雑なインタフェースを持つものもある．しかし，多くのユーザが設定したい事とは，各セキュリティ装置の設定ではなく，使用するアプリケーションに対するセキュリティ設定である．例えば，「安全に電子ショッピングモールで買い物をしたい」といった要求の場合，ユーザはファイアウォールのフィルタリングルールなどに対する知識を必要とせずにセキュリティを設定できることが望ましい．

そこで，ユーザが使用するアプリケーション毎に大まかなセキュリティ機能を設定した場合，それらを各機器の設定値に変換するエンジンが必要になる(図 2)．

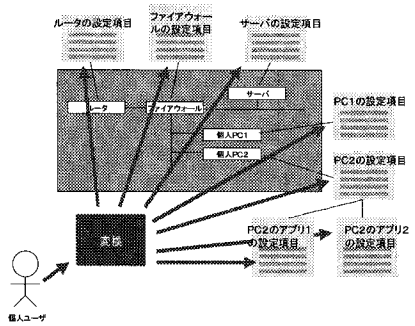

図 2 セキュリティポリシーの変換

なお，この変換エンジンは主に以下の 4 つの機能から成る．

- ポリシー変換機能

Security for Regular-Connected Personal Terminal - Introduction -
Tomoaki MORIJIRI†, Tatsuro IKEDA†,
Nobuyuki OHGISHI††, Daigo YOSHII†,
Toshiaki SAISHO†
†TOSHIBA Co., SI Technology Center, 3-22, kata-machi, Fuchu-shi, Tokyo, JAPAN
††TOSHIBA Information Systems Co., 2-1, Nisshin-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa, JAPAN

ユーザが設定したアプリケーションに対するセキュリティポリシーを実際の機器の設定に変換する.

- 設定実行機能
  ネットワーク上の各マシンやそのうえのアプリケーションのセキュリティ設定を行う.
- 環境把握機能
  ユーザの環境(ネットワーク構成・各マシンのアプリケーションなど)を把握する.
- 整合性検証機能
  各セキュリティ装置(機能)の設定値の整合性を検証する.

3　セキュリティポリシー集中管理

基本的に, 家庭内のセキュリティポリシーはその家庭内で作成し設定することが望ましいが, 上記の様な簡易設定が可能になった場合でも, 実際の運用を考えると汎用的な設定は ISP などが行った方が普及の面からは有利だと考えられる. また, CERT などによる最新のセキュリティ情報を定期的に収集し, 変換エンジンに反映させることは煩雑であるため, ISP が定期的に最新情報を配布することは有用なことだと考えられる. しかし, 各家庭のネットワーク構成とソフトウェア構成をすべて ISP が把握することは困難であると同時に, プライバシー保護の観点からも望ましくない.

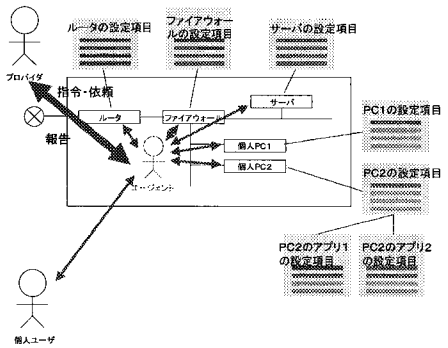

図 3 セキュリティポリシーの集中管理

そこで, 家庭内の PC に ISP のエージェントプログラムを置き, これを介して家庭内のセキュリティ設定を行う方法を考える(図 3). このエージェントプログラムは, 前述の変換エンジンに, サーバとの通信機能を追加することで実現できる. ここで, エージェントプログラムはユーザの環境については ISP に通知しないようにしておく必要がある.

4　IP トレースバック

常時接続環境では端末は常に外部からのアタックにさらされることになる. また, 固定 IP アドレスが多いため, 一度攻撃に遭うと, 定常的に攻撃を繰り返される可能性も高くなる. ところが一般に, 攻撃者は攻撃元の IP アドレスを詐称することが多いため, 被害者は攻撃元を特定することが難しく, 対策を遅らせる原因となっている. この問題を解決するには, アタックに使用したパケットがどの経路を通ってきたかをトレースすることにより, 真の攻撃発信元を特定する IP トレースバックのプロトコルを開発・普及させることが必要である(図 4).

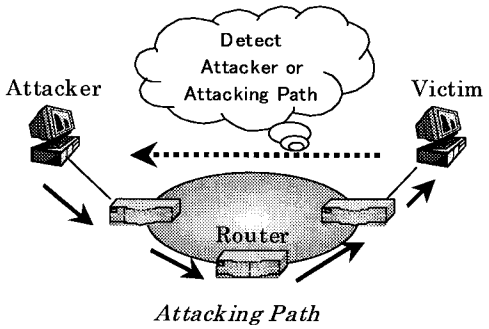

図 4　IP トレースバック

トレースバックを行うには, 経路途中のルータがパケットにトレースバック情報を付加し, 被害者(あるいは調査機関)はそれを利用して発信源を特定するなどの方法がある. 現在, IETF, 奈良先端技術大学院大学, ワシントン大学などからそれぞれ異なる方法が提案／議論されており, どの方法も一長一短がある. そこで, これらの方法について体系的に整理を行うとともに, これらのスキームを組み合わせたスキームを考える必要がある[2].

5　おわりに

本稿は, 家庭向けの常時接続端末に必要となるセキュリティ手段を提供する方法について提案した. 今後, 実証実験などを行い, その効果を確認する必要がある.

謝辞

本発表は, 通信・放送機構が実施する平成 13 年度 高度通信・放送研究に係る委託研究「個人ユーザ向けの常時接続端末におけるセキュリティ保護技術に関する研究開発」の委託を受け, 当社が研究開発しているシステムに関するものである. 関係者各位のご支援に感謝する.

参考文献

[1] 門林雄基, 大江将史, “IP トレースバック技術”, 情報処理 2001 年 12 月号
[2] 大岸, 池田他, “ハイブリッドスキームを利用した IP トレースバック技術”,SCIS2002 予稿集,2002/1