5H−05

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　〜セキュリティポリシーの体系化〜

池田　竜朗†, 吉井　大吾†, 大岸　伸之††, 遠藤　清宏††, 森尻　智昭†, 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[1], [2]

近年, ウイルス感染や, DoS/DDoS 攻撃, 踏み台攻撃などによるネットワークの被害が増加している. また並行して家庭におけるインターネット利用者も増加の傾向にある. しかし, セキュリティに対する考え方, 知識はユーザ毎にさまざまであり, 個人ユーザにユーザ環境のセキュリティを一任してネットワークのセキュリティを保つことは, 困難なことである. そこで, 個人ユーザの知識に頼らずに一定レベルのセキュリティを確保することが求められる. その為のセキュリティポリシー体系化について検討する.

2　セキュリティポリシーにおける課題

企業向け, 家庭向けに関わらずインターネットへ接続する環境においては, セキュリティを確保するために, それぞれの環境に適した設定を行う必要がある. そのとき, 機器ごと, アプリケーションごと, あるいは各設定項目ごとなどの個別的な設定では, 環境全体で一定レベルのセキュリティを確保することは難しい. 環境全体の設定方針(ポリシー), すなわちセキュリティポリシーをたて, それにしたがって設定を行う必要がある.

セキュリティポリシーは, 一般的に"ある条件の場合(あることの実行を要望する場合), それに対した処理を行う(設定する)"という形にブレイクダウンすることで実施される. ユーザがセキュリティポリシーに従って適切な設定を実施するには, 環境およびセキュリティに関する知識に基づき, 実際の設定にまでブレイクダウンする能力が求められる. しかし, 全ての個人ユーザに対して, このような知識および能力を要求することは, 非常に困難である.

3　ポリシー体系化[3]

常時接続端末を利用する家庭が増加していく中で, ネットワークが安全に利用されていくために, 個人ユーザのセキュリティに関する知識レベルに関わらず, 一定レベルのセキュリティを確保することが求められている. これを実現するために, 従来散在的に存在しがちであった, セキュリティポリシーとそれに基づき実際の設定までブレイクダウンする知識を整理体系化することを考える. "ポリシー"を知識および方針の複合体ととらえると, これは, セキュリティポリシーの体系化, と表すことができる. 以後, "ポリシー"をこの意味で用いる.

セキュリティポリシーの体系化は, ポリシーを階層的に整理し, 「条件→処理」という構造をもつ要素的なポリシーに部品化することによって行う. 以下にこれを説明する(図1参照). すなわち, ユーザの素朴な要望からその要望を達成するための具体的設定を導くポリシーを, 次のような要素的なポリシーに階層的に部品化する : 要望からこの要望によって生じると考えられるリスクを導くためのポリシー「条件(要望)→処理(リスク)」, リスクとこのリスクを回避するために行うべきと考えられる機器によらない設定を導くためのポリシー「条件(リスク)→処理(メタ設定)」, メタ設定とこのメタ設定から具体的な機器に対して行うべきと考えられる設定を導くためのポリシー「条件(メタ設定)→処理(設定)」. 要望の階層は, さらに細かく階層化してもよい.

部品化されたそれぞれの「条件→処理」構造は要素的なポリシーと考えることができるので, 要素ポリシーと呼ぶことにする(図2参照). 要素ポリシーにおける処理は一般にひとつ以上「条件→処理1, ・・・, 処理 n」である. また, 異なる条件からあるひとつの処理が指定されることもある. 体系化するにあたり, 要素ポリシーの組み合わせが矛盾

Security for Regular-Connected Personal Terminal - Systematization of Security Policies -
Tatsuro IKEDA†, Daigo YOSHII†
Nobuyuki OHGISHI††, Kiyohiro ENDOH††,
Tomoaki MORIJIRI†,
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

を生じないように注意する必要がある.

ユーザが, このセキュリティポリシー体系を利用して, ブラウザを利用する場合を例に挙げる(図3参照). ユーザはブラウザの利用を要望(指定)し, インターネット上の情報を閲覧するのみか, あるいはインターネットショッピングを利用するか等, ブラウザの利用方法や利用形態などを要望(指定)する. このユーザからの要望は, セキュリティポリシー体系に従って, 個々の機器に対する設定内容までブレイクダウンされる. ユーザはこの設定内容に基づき, 必要な機器に対して設定を施す. この場合ユーザに求められるのは, ブラウザを利用するという要望, その利用方法や利用形態の要望を指定することと, それに基づいてセキュリティポリシー体系が最終的に導き出した具体的な機器への設定方法にしたがい, 設定を行うことのみで, 実際に要望から設定方法を具体化する能力は求められない. したがって知識の不足しているユーザでもこの体系を用いることにより簡単に適切な設定を行うことができる.

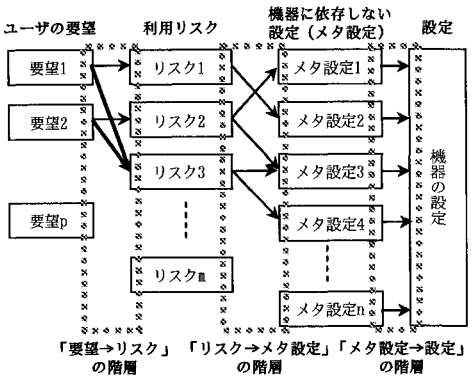

図1．セキュリティポリシー体系構成

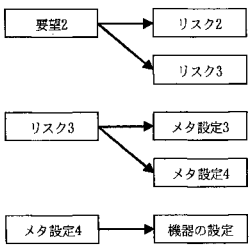

図2．要素ポリシー（例）

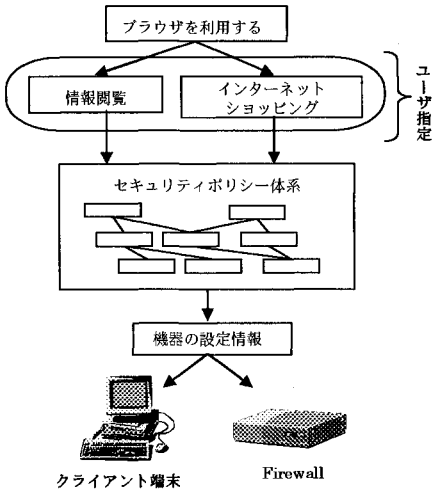

図3．セキュリティポリシー体系を用いた設定例

4　おわりに

以上のような方針でセキュリティポリシーの体系化を行う. 今後は, 作成したセキュリティポリシー体系が最終的に導き出す具体的な機器への設定に基づき, 実際の機器にセキュリティ設定をユーザにかわって行う手法および技術などを検討する.

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] 情報通信審議会; “21 世紀におけるインターネット政策のあり方”
[2] 田淵治樹; “国際セキュリティ標準 ISO/IEC15408 入門”
[3] 社団法人電子情報技術産業協会; “コンピュータセキュリティの市場・技術に関する調査報告書”