コンピュータセキュリティ　18－2
(2002. 7. 18)

常時接続個人ユーザ端末向けセキュリティポリシーの考察
－セキュリティポリシー簡易設定技術－

吉井 大吾　池田 竜朗　森尻 智昭　才所 敏明

(株) 東芝 SI 技術開発センター 〒183-8512 東京都府中市片町 3-22

E-mail: { daigo.yoshii, tatsuro.ikeda, tomoaki.morijiri, toshiaki.saisho}@toshiba.co.jp

あらまし　本稿では，一般的な個人ユーザが簡単にセキュリティ対策できるしくみについて考察する．個人ユーザのセキュリティポリシーを「やりたいことから，そのときに行うべき環境設定を導くルール」とする．このルールを階層的に細分化して，再利用性を高める．この階層化されたポリシーを用いた個人ユーザ向けセキュリティサービスの一例を示す．

キーワード　常時接続，個人ユーザ，ポリシー，ポリシー体系，階層化，再利用

Security policy for regular-connected personal network terminal
－A Simple Method for All Personal Users－

Daigo YOSHII　Tatsuro IKEDA　Tomoaki MORIJIRI　and　Toshiaki SAISHO

Toshiba Corporation, e-Solution Company, 3-22, Katamachi, Fuchu-shi, Tokyo 183-8512, Japan

E-mail: { daigo.yoshii, tatsuro.ikeda, tomoaki.morijiri, toshiaki.saisho}@toshiba.co.jp

Abstract　We consider a way which helps all the personal users to set up their terminal secure. We suggest that security policy for a personal user should be a set of certain rules. The rule consists of a condition and actions. The condition is what the user wants to do. The actions are what the user should do. The condition is described in plain words. The actions are concrete teaching how to set up his/her terminal. The policy is broken into more primitive rules, which makes the policies reusable. A security service based on the policies is exhibited.

Keywords　regular-connected, personal user, policy, policy system, hierarchisation, reusability

1. 本研究の背景

近年のインターネット環境の発展により，インターネットは一般の家庭へも浸透してきた．普段の生活の中においても重要な位置を占めるようになってきている．個人向けの常時接続サービスは急速に普及し，ユーザ数は着実に増加してきている．図 1に 2001 年 1 月から 2002 年 5 月までの DSL 加入者の推移を示す．政府も平成 13 年 1 月には「e-Japan 戦略」を，同年 3 月には「e-Japan 重点計画」を打ち出し，国家施策としてもインターネット環境の整備に注力している．

一方で，インターネットから個人ユーザ端末への危険性も増加してきている．多くの個人ユーザはインターネットの利便性にのみ関心があり，危険性に対する意識は薄い．企業などある程度大きな組織向けには，たとえば ISO15408 などのセキュリティ対策ガイドラインなどが出されている．しかし，個人ユーザ向けには効果的なガイドラインが出されていないのが現状である．

ブロードバンドが本格的に発展して，一般の人々の生活を豊かにするためには，だれでも簡単に自分の端末のセキュリティを高めることができる技術が必要である．本稿ではその技術について検討する．

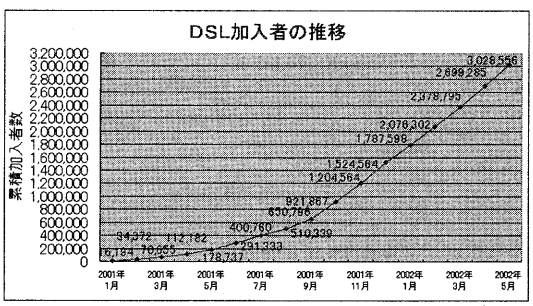

図1　DSL 加入者の推移[1]

2. 本研究のゴール

将来，子供からお年寄りまで日常的にインターネットを利用する社会が来るであろう．そのとき，セキュ

リティ対策が壁となってはならない．我々の考えるセキュリティ対策は，ユーザのアクションにしたがい自動的に行われ，必要なときだけユーザに注意を促すものである．このように，セキュリティ対策をユーザから隠蔽化する技術の開発が本研究のゴールである．

ユーザの代わりにセキュリティ対策を担当するエージェントプログラムは，たとえば次のような仕事をする．まず，ユーザのアクションからユーザのやりたいことを察知する．次に，この要求を実現するときのリスクを分析し，適切な環境設定を導き出す．そして，その設定をアプリケーションや機器等に対して実施する．（この例は，6章で再びふれる．）

このようなエージェントが開発されれば，ユーザは自分の本当にやりたいことに集中できる．子供からお年寄りまで，親しみにくい技術情報に悩まされることなく，インターネットの恩恵を享受することができる．

3. 個人ユーザ向けセキュリティポリシー

2章で述べたゴールを構成する重要な要素の一つに「ユーザのやりたいことにもとづき適切な環境設定を導出する技術」がある．この技術開発を中間目標とする．本稿の目的は，この中間目標への我々のアプローチ法を紹介することである．

企業は，図 2および図 3に示すような手順でセキュリティポリシーを策定・実施し，セキュリティ対策を行っている．

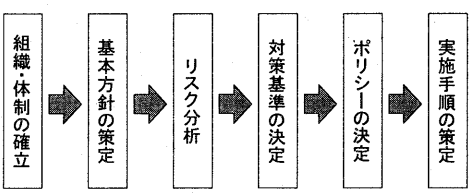

図2　ポリシー策定手順[2]

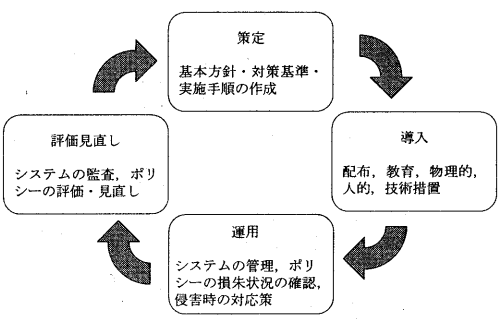

図3　セキュリティポリシーの実施サイクル[2]

しかし，個人ユーザにこのような大掛かりな対策を求めることはできない．個人には，むしろ簡単ですぐにでも実行できるセキュリティ対策がよいと考える．そこで我々は，「やりたいことから，そのときに行うべき環境設定を導くルール」を個人ユーザのセキュリティポリシーとする．これが集まることで，個人ユーザのセキュリティポリシー体系となる．図 4に個人向けセキュリティポリシー体系が個人ユーザをサポートするイメージを示す．

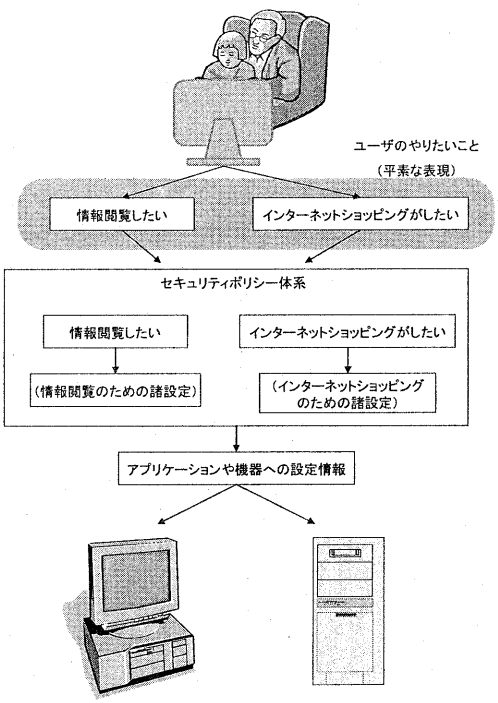

図4　個人ユーザ向けセキュリティポリシー体系

このような個人ユーザのセキュリティポリシーをすべての個人ユーザに随時提供することができれば，個人ユーザは簡単にセキュリティ対策を行うことができるであろう．しかし，提供すべきセキュリティポリシーは千差万別となる．個人個人の機器やアプリケーションなどの環境，また利用目的によってさまざまに変化するからである．セキュリティポリシーの再利用性を高めたい．そこで，個人ユーザ向けセキュリティポリシーを細分化する．その前に IETF によって検討されているポリシーモデルについて紹介する．

4. ポリシー

普通，ポリシーといえば，全体の方針など，概念的・

抽象的な意味で用いられる．しかし，ポリシーが具体化された実施手順である「条件→処理」もポリシーと呼ばれることがある．3章で提案した個人ユーザ向けセキュリティポリシーもこのかたちになっている．

以下，IETF の policy framework working group などで検討されているポリシーのモデルについて簡単に紹介する．ただし“ポリシー体系”という言葉は IETF では標準的には用いられていない．

4.1. ポリシーとポリシー体系[3]

「条件→処理」というルールをポリシーと呼び，ポリシーの集まりをポリシー体系と呼ぶことにする．図5にポリシーのイメージを示す．

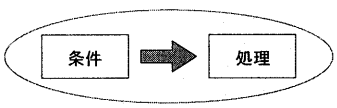

図5　要素ポリシー

複数のポリシーが連鎖することもある．すなわち，あるポリシーの“処理”が別のポリシーの“条件”となって用いられることもある．図 6にそのイメージを示す．

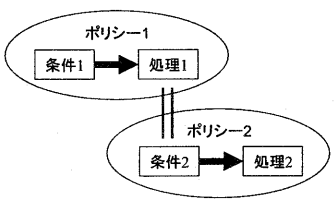

図6　ポリシーの連鎖

ポリシー体系｛ポリシー 1，ポリシー 2，ポリシー 3｝のもと，条件 1 が処理 a，処理 b，処理 c にブレイクダウンされる様子を図 7に示す．図 7においては，ポリシーの内容が省略されている．また，ポリシー1 が条件 1 より導き出した処理 i および処理 ii はそれぞれ条件 i 条件 ii としてポリシー2 およびポリシー3 に入力されている．

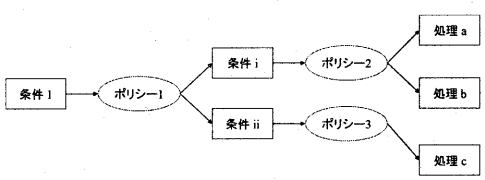

図7　ポリシー体系

ポリシー体系は矛盾した結論を導き出す可能性がある．この矛盾解消はポリシー体系の解決すべき本質的な課題となる．

4.2. ポリシーの階層化

以上の準備の下，個人ユーザ向けセキュリティポリシーを階層的に細分化する．

我々の個人ユーザ向けセキュリティポリシーは，「ユーザのやりたいこと」を“条件”として，その“条件”から「実際の諸設定」を“処理”とするポリシーである．再利用性を高めるために，このポリシーを階層化する．以降では 2 つの層に細分化した例を示すが，もっと多くの層に細分化した場合も考えることができる．

ポリシーをリスク分析に関わる層と設定に関わる層とに細分化し，それぞれ要望－リスク層，リスク－設定層とよぶことにする．ポリシーを，やりたいことに関わるリスクを分析するポリシーと，リスクに対処するための設定を示すポリシーという二つのポリシーの連鎖に細分化するのである．図 8に 2 層に階層化されたポリシーが形成するポリシー体系のイメージを示す．

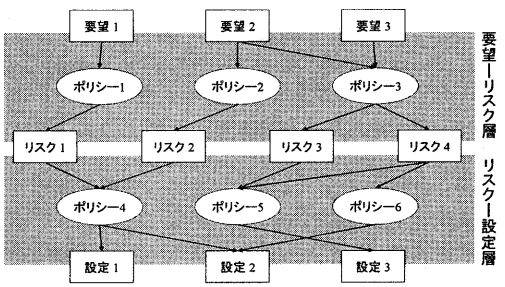

図8　ポリシーの階層化

階層化することでポリシーをコンポーネント化できる．要望－リスク層とリスク－設定層を別々の組織が策定して提供することが可能となる．図 9に，3 層以上に階層化したポリシー体系のイメージを示す．

一方で，コンポーネント化されたポリシーを組み合わせたときに矛盾が生じうるという問題も生み出す．

4.3. サービスモデル

階層化されたセキュリティポリシーを用いたサービス例をあげる．図 10を参照にしながら追ってほしい．

個人ユーザのセキュリティをサポートする組織として，次の三つを考える．すなわち，セキュリティ専

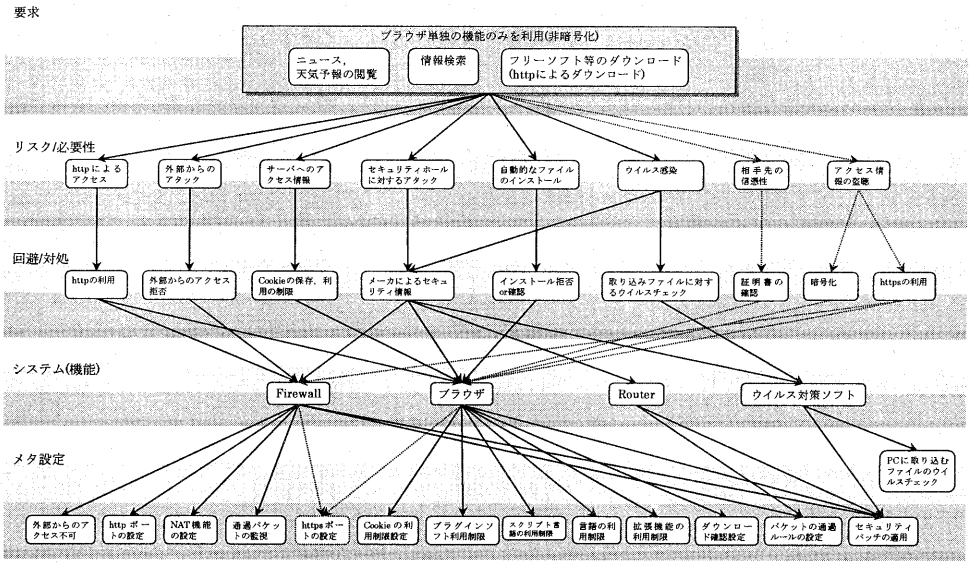

図 9 ポリシー体系

門組織，ベンダ，および SP(Service Provider)である．セキュリティ専門組織は，最新の情報にもとづき一般ユーザの要望に対するリスク分析して，その要望を“条件”，その要望から生じうるリスクを“処理”とするポリシーを作成する．ベンダは，セキュリティ専門組織のあげたリスクに該当する自社製品について，そのリスクを“条件”，リスクに対処する設定を“処理”とする要素ポリシーを作成する．SP は，セキュリティ専門組織およびベンダから提供されるポリシーを随時収集する．そして，ユーザの意向にもとづきポリシー体系を編集して個人ユーザに提供する．セキュリティ専門組織，ベンダ，および SP は，それぞれ図 2および図 3でみたような手順でポリシーを管理する．この様子を図 11に示す．

以上のサービスは，それぞれの組織に負荷が偏らず，比較的現実的なものと考える．

5. 今後の課題

解決すべき課題は以下のとおりである．

・(ポリシー体系の矛盾解消)

複数の設定が競合したときの矛盾解決手法の開発が必要である．

・(ポリシー体系をセキュアにやりとりする方法)

本稿で提案した方法によると，ポリシーがインターネット上を動くことになる．ポリシー自体が盗聴・改ざんされてしまうことがあってはならない．正規のユーザを認証する機能および通信路を守る機能などの開発が必要である．

・(実用性の確認)

上記二項目が開発された後，本稿で提案した方法が実用的かどうかの実証実験が必要である．

6. 今後の開発の方向

1章で本研究のゴールについて述べた．4.3で示したサービス例にもとづき，ゴールのひとつの実現方法を図 12に示す．図 12では，ユーザのエージェントが適切なセキュリティポリシーを SP やベンダ，セキュリティ専門組織のエージェントと相談しながら収集してセキュリティ体系を構築する．ユーザのアクションからエージェントがユーザの要望を察知する．その要望からセキュリティ体系の導きだした設定にもとづき，エージェントが実際の設定を行なう．

7. まとめ

本稿では，一般的な個人ユーザが簡単にセキュリティ対策できるしくみについて考察した．個人ユーザのセキュリティポリシーを「やりたいことから，そのときに行うべき環境設定を導くルール」とした．このルールを階層的に細分化して，再利用性を高めた．この階層化されたポリシーを用いたセキュリティサービスの一例を示した．

8. 謝辞

本研究は，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．

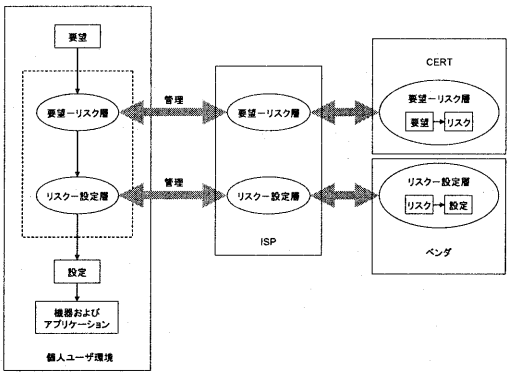

図10　サービスモデル

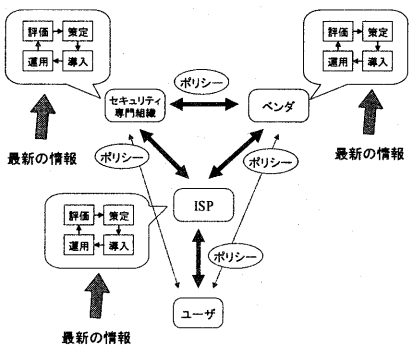

図11　ポリシーの管理

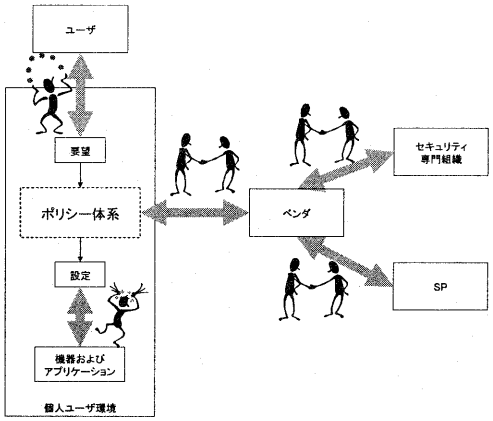

図12　セキュリティ対策の隠蔽化

文　献

[1] 総務省，“DSL 普及状況公開ページ，” 情報通信，DSL 普及状況ページ，http://www.soumu.go.jp/joho_tsusin/whatsnew/dsl/index.html，Jun. 2002

[2] 情報セキュリティ対策推進会議，“情報セキュリティポリシーに関するガイドライン，” 情報通信技術戦略本部，情報セキュリティ対策，http://www.kantei.go.jp/jp/it/security/taisaku/pdfs/ISP_Guideline.pdf，Sep. 2000.

[3] IETF，“Terminology for describing network policy and services，” draft-ietf-policy-terms-00.txt, http://www.ietf.org/proceedings/99jul/I-D/draft-strassner-policy-terms-01.txt, Jun. 1999.

[4] 池田竜朗他，“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～，” 第 64 回社団法人 情報処理学会講演 論文集 (3)，pp413-414，2002.