マルチメディア通信と分散処理　101－5
コンピュータセキュリティ　12－5
（2001．2．20）

ポリシーベースセキュリティ構築支援システムにおける機器設定機能の実装

石田 育士‡　　萱島 信†

‡(株)日立情報ネットワーク　†(株)日立製作所

要旨

インターネット技術を用いた情報システムが、企業や社会の重要な基盤になるにつれ、不正アクセスやコンピュータウイルスから情報システムを保護するセキュリティ対策が重要になってきている。このため報告者らは，情報システムの開発工程全体，すなわち，セキュリティポリシーの策定・セキュリティ仕様設計・検査の各手順を総合的に支援するポリシーベースセキュリティ構築支援システムを提案している。ポリシーベースセキュリティ構築支援システムを実現するには，セキュリティポリシーを基に各機器の設定パラメータを作成する“セキュリティ設定生成ツール”を新たに開発する必要がある。

そこで本稿では，ファイアウォールを対象機器として開発したセキュリティ設定生成ツールの実装方式について述べる。

A technique of supporting to set up a machine in Policy-based Security Management System

Yasuji ISHIDA‡　Makoto KAYASHIMA†

‡Hitachi Information Network, Ltd.　†Hitachi, Ltd.

Abstract

As the information system which used the Internet technology becomes the important base of the enterprise and the society, it has been getting important to protect information system from the unauthorized access or computer virus. Therefore, we propose “policy-based security management system” which makes systematic and total security control for system development process.

To realize policy-based security management system, we must develop new tool which named “security parameter formation tool.” In this paper, we report the implementation method of our development tool.

1. はじめに

インターネットをベースとする情報システムは，組織や社会の情報基盤として重要な役割を果たすようになり，今後その重要性はますます増大することが予想されている。しかしインターネットは，本来オープンなシステムであるため，外部からの不正アクセスやコンピュータウイルスの混入といったさまざまなセキュリティの問題を抱えている。そこで，より強固なセキュリティを

実現するため，情報システムの開発から運用まで，体系的なセキュリティ管理を実施することが重要になっている[1]。

この中の開発工程では，(1) 情報システムで発生しうる脅威を分析し，さまざまな脅威に対して抜け漏れなく対策指針(セキュリティポリシー)を立案することと，(2) セキュリティポリシーを具体化してセキュリティ設計を行い，情報システムを構築することと，(3) 構築したシステムが正しく設定されているか検査すること が必要である。

これらの作業を実施するには，高度な専門技術と知識を必要とする。このため報告者らは，セキュリティポリシーの簡易的な策定を支援するツールの開発[2] や，セキュリティ設定の検査ツールの開発[3] を行うとともに，これらのツールを連動させることにより，インターネット接続システムの開発工程全体のセキュリティ管理をトータルに支援することを可能にする“ポリシーベースセキュリティ構築支援システム”の提案を行っている[4]。

ポリシーベースセキュリティ構築支援システムの実現には，既存のツール群の連携を可能にする“セキュリティ設定生成ツール”を新たに開発する必要がある。そこで本稿では，ファイアウォールを対象機器として報告者らが開発したセキュリティ設定生成ツールの実装方式について述べる。

2. ポリシーベースセキュリティ構築支援システム

“ポリシーベースセキュリティ構築支援システム”は，セキュリティ設計から構築までの一連の作業を，セキュリティツールを連動させて一貫して行うことにより，インターネット接続システムの開発工程における体系的かつ効率的なセキュリティ管理を実現するものである。

本システムは，以下の4種類のツールを組み合わせることにより構成されるものである。

(1) セキュリティポリシー作成支援ツール
開発システムに対するセキュリティ要求仕様を基に，セキュリティポリシーを策定する作業を支援する

(2) セキュリティ設定生成ツール
セキュリティポリシーから，開発システムを構成する個々の機器に対する設定パラメータと，設定後の診断項目を作成する作業を支援する

(3) セキュリティ運用管理ツール
個々の機器に対してセキュリティ設定パラメータをセットアップする作業を支援する

(4) セキュリティ設定検査ツール
個々の機器におけるセキュリティ設定の検査作業を支援する

図 1 に，ポリシーベースセキュリティ構築支援システムの全体構成を示す。

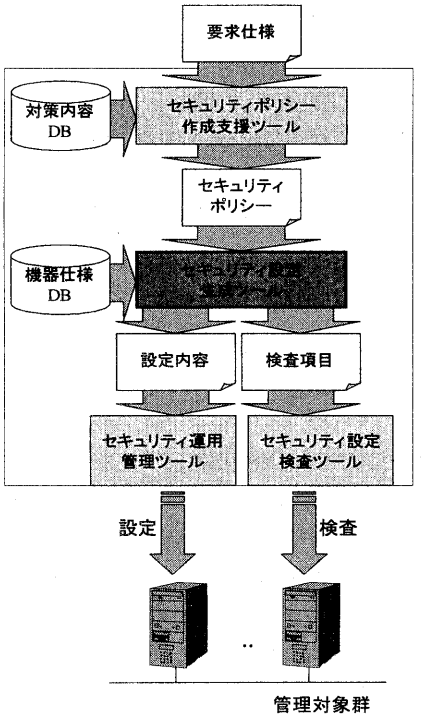

図 1 ポリシーベースセキュリティ構築支援システムのモジュール構成

3.セキュリティ設定生成ツールの実装

セキュリティ設定生成ツールは，設計フェーズにおけるセキュリティポリシーの作成作業の結果を用いて，構築フェーズにおけるセキュリティパラメータの設定および検査を連携して行えるようにするためのツールである。本章では，このセキュリティ設定生成ツールを実装する上での要件と，その実現方針について述べる。

3.1.セキュリティ設定生成ツールの機能要件

セキュリティポリシー作成支援ツールが出力する対策項目から，具体的な機器の設定パラメータを作成するために，セキュリティ設定生成ツールは以下の機能を必要とする。

(1) 対策項目ローディング機能
セキュリティポリシー作成支援ツールは，対象機器で起こりうる全ての脅威に対する対策項目のリストを出力する。対策項目ローディング機能は，これらのリストの内容を読み込む機能である。

(2) 対策－設定項目マッピング機能
対策内容を実現するセキュリティ設定項目は，対象となる機器の種別ごとに異なっている。対策項目－設定項目マッピング機能は，機器種別ごとに対策項目と具体的なセキュリティパラメータの対応付けを行う機能である。

(3) 設定パラメータ作成機能
セキュリティ設定項目の中には，構築対象のシステムに依存して値が決まる設定パラメータもある。このため，設定パラメータを作成する機能が必要である。

3.2.実装における検討

3.1節で述べた機能を実現ために，以下の検討を実施した。

3.2.1.対策と設定項目のマッピング調査

対策機能を実現するセキュリティ設定項目は，対象となる機器の種別ごとに異なっているため，今回はファイアウォールを例に，対策内容を実現ための設定項目の調査を行った。その結果，ファイアウォールで実施すべき対策内容は，以下の 3 種類に分類されることがわかった。

(1) ファイアウォールを設置することで実施される対策
例えば，「ネットワークのアクセス制御を実施する」という対策に関しては，ファイアウォールを設置することそのものが設定内容に相当する。

(2) ファイアウォールのみに関係する設定により実施される対策
例えば「認証の試行による攻撃への対処を実施する」という対策には，一定回数の認証失敗に対してユーザ ID をロックする等の設定が行われる。

(3) ファイアウォールと他の機器との関係により実施される対策
「管理作業を行う端末を制限する」という対策には，特定の IP アドレスからのアクセスのみ許可する等の設定が行われる。この設定は，管理端末の IP アドレス等の，ファイアウォールと関係する他の機器に関する情報も必要になる。

この対策と設定項目の関係を図 2 に示す。

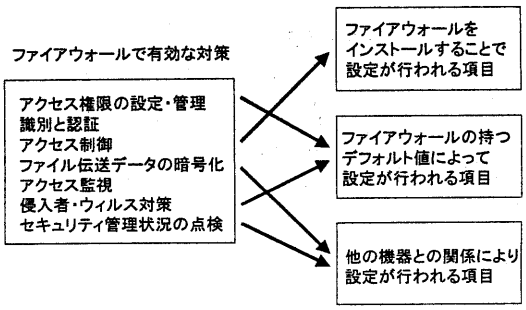

図 2 対策と設定項目の関係

3.2.2.設定パラメータの作成

設定パラメータの作成方法は，対策内容の種別ごとに以下のように実現する方法を検討した。

- ファイアウォールを設置することで実施される対策は，特に設定パラメータを必要としない。
- ファイアウォールにのみ関係する設定により実施される対策は，あらかじめデフォルト値を設定しておき，ユーザがカスタマイズを実施するための手段を提供する。
- ファイアウォールと他の機器との関係により実施される対策は，ユーザが他の機器を定義する手段と，その定義内容を用いて設定内容を作成する手段を提供する。

4.プロトタイプの概要

本章では，3章での検討を踏まえ，ファイアウォールを対象機器として開発したセキュリティ設定生成ツールのプロトタイプに関してその動作概要を述べる。

プロトタイプの大まかな処理の流れは以下のとおりである。

- 対策項目の読み込み
- 対策－設定項目のマッピング
- 関係機器の定義
- 設定パラメータのカスタマイズ

4.1.対策項目の読み込み

プロトタイプでは，表 1に示すようなファイアウォール用の対策項目リストを提示し，実施する対策の選択をユーザに要求するインタフェースを準備した。

表 1 対策実施項目の選択

項目	具体例	対策	施策確認
システムへのアクセス制御機能	ユーザが席から離れたときに計算機を無断借用する	一定時間以上入力が途切れた場合，スクリーンセーバを起動する	☐ チェック
		一定時間以上アクセスが途切れた場合ログアウトし，再度認証を要求する	☐ チェック
	ユーザに成りすましてログインする	リモートからシステムにアクセス可能な時間帯を設定する	☐ チェック
ネットワークのアクセス制御機能	外部ネットワークからユーザに成りすまして内部ネットワークに侵入する	ファイアウォールを使用し，かつ専用の認証機構を行う機器からのみアクセスを許可する	☐ チェック

このインタフェースでは，実施する項目のカテゴリと具体例を併記することにより，対策が必要な項目の選択を容易に行えるようにした。

4.2.対策－設定項目のマッピング

プロトタイプでは，対策項目と、個々のファイアウォール製品の具体的な設定項目との対応付けをあらかじめ行った機器仕様 DB を準備した。

4.3. 関係機器の定義

ファイアウォールと他の機器との関係により実施される対策を実現するため，関係機器の定義を行う。

関係機器に対しては、ホストやルータといった機器のタイプや、アドレス情報を割り当て、互いにユニークなオブジェクトの名称をつけることによって、各々の機器を特徴付けることにした。以下に、構成要素の定義を表 2に示す。

表 2 構成要素の定義

構成要素	設定項目		設定パラメータ
ファイア	オブジェクト名		Firewall
ウォール	IP アドレス	内部	x.x.x.x
		DMZ	y.y.y.y
		外部	z.z.z.z
	機器タイプ		Gateway
認証サーバ	オブジェクト名		Auth
	IP アドレス		a.a.a.a
	機器タイプ		Host

4.4.設定パラメータのカスタマイズ

ファイアウォールにのみ関係する設定パラメータの場合，デフォルト値をユーザに提示し，カスタマイズを要求するインタフェースを準備した。ファイアウォールと他の機器の関係を必要とする設定項目は，4.3節で定義した関係機器の情報を用いて設定パラメータをカスタマイズする。このような項目にはアクセス制御の定義がある。

表 3 アクセス制御の定義

番号	送信元	受信先	プロトコル	アクション
1	外部ネットワーク	Auth	ftp telnet	ユーザ認証
2	…	…	…	許可
3	…	…	…	許可
…	…	…	…	…
N	それ以外	それ以外	それ以外	拒否

5. まとめと今後の課題

本稿では，インターネット情報システムの開発工程におけるセキュリティ管理を支援する“ポリシーベースセキュリティ構築支援システム”を実現する上で，既存のツールを連携させる機能を持つ“セキュリティ設定作成ツール”の実装方式について検討した結果を報告した。

セキュリティ設定作成ツールは，セキュリティポリシー作成支援ツールが出力する対策項目から，具体的な機器の設定パラメータを作成する過程を支援するもので，本ツールの出力を，セキュリティ運用管理ツールおよび，セキュリティ診断ツールに渡すことにより，セキュリティ設計から構築までの作業を一貫して支援することが可能になる。

本稿では，特にファイアウォールを対象としたセキュリティ設定作成ツールのプロトタイプを開発し，ポリシーから設定パラメータを作成する上での問題点を明らかにすることができた。今後は，セキュリティポリシー作成支援ツールを全ての機器タイプに対応できるように拡張を行い，その有効性を検討する予定である。

参考文献

[1] 統合セキュリティ運用管理システムの提案，萱島他，第 11 回 CSEC 研究会，2000.9
[2] セキュリティポリシー作成支援ツールの開発，藤山他，第 8 回 CSEC 研究会，2000.3
[3] 定義ファイルを用いたセキュリティ検査システムの開発，寺田他，CSS'99，1999.10.
[4] ポリシーベースセキュリティ構築支援システムの提案，萱島他，第 12 回 CSEC 研究会，2001.2