マルチメディア通信と分散処理　101－4
コンピュータセキュリティ　12－4
（2001．2．20）

# 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 信[†]　石田 育士[‡]

[†](株)日立製作所　[‡](株)日立情報ネットワーク

## 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。このため情報システムは，開発時にさまざまな脅威に対する対策方針(セキュリティポリシー)を策定し，そのポリシーに基づいて構築することが一般的になりつつある。

現在，システム開発工程を支援するためのセキュリティツールが開発されている。しかしこれらのツールは，開発工程を部分的に支援するもので，開発工程全体をトータルに支援する機能を持つものではなかった。そこで本稿では，システム開発工程全体，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セキュリティ構築支援システムを提案する。

# Proposal of Policy-based Security Management System

Makoto KAYASHIMA[†]　Yasuji ISHIDA[‡]

[†]Hitachi, Ltd.　[‡]Hitachi Information Network, 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, in the development process of the information system, it becomes general that to design security policy toward the various menaces of the information system and to construct information system according to the policy.

Recently, security tools which support such development of systems are developed. However, these tools partly support the development process of the system, and these does not have a function to support the whole of the development process. In this paper, we propose "policy-based security management system" which makes systematic and total security control for system development process.

## 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]。

この中で開発工程においては，(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の指針(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。

上記のセキュリティポリシーの策定，セキュリティポリシーを具体化するセキュリティ設計，および設定状態の検査を実施するには，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，メールサーバや Web サーバにより構成されているインターネット接続システムを対象として，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を行うためのツールの開発[3]を行ってきた。

これらの開発ツールにより，インターネット接続システムに対するセキュリティポリシーの原案作成とシステムのセキュリティ検査を，作業者のレベルに依存せず，低コストで作成することができるようになったが，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，実際に機器に設定する作業に関しては，セキュリティポリシーの内容を理解し，かつ具体的な機器のセキュリティ機能に関する高度な知識をもつ作業者が必要であった。

そこで本稿では，上記のセキュリティポリシー作成支援ツールやセキュリティ検査ツールを連動させ，ツールを組み合わせることにより，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”を提案する。

## 2. 開発工程支援の現状と課題

本章では，インターネット接続システムの開発工程における設計フェーズおよび構築フェーズの作業手順とその支援ツールについて概観し，開発工程全体のセキュリティ管理を体系的に実現するための課題について述べる。

### 2.1. 設計フェーズ

#### 2.1.1.対象システムのモデル化

脅威や対策を検討する前に，情報システムを適切な構成要素に分解し，評価対象として定義することが必要である。セキュリティポリシー作成支援ツールは，インターネット接続システムで利用されている機器を表 1 に示す 6 種類のタイプにあらかじめ分類している。このため，開発時では，システムに使用する機器のタイプを選択することにより，対象システムをモデル化できる。

表 1 機器のタイプ

| タイプ | 機能 |
|---|---|
| 公開サーバ | インターネットに向けてサービスを提供する計算機 |
| 内部サーバ | イントラネットに向けてサービスを提供する計算機 |
| クライアント | 一般ユーザが端末として使用する計算機 |
| ファイアウォール | 外部ネットワークと内部ネットワークを接続し，アクセス制御を実施する計算機 |
| ボーダルータ | 外部ネットワークと内部ネットワークを接続する機器 |
| アクセスサーバ | ダイアルアップによるネットワーク接続を実現する計算機 |

### 2.1.2. 脅威抽出／リスク評価

モデル化した個々の機器タイプごとに発生しうる脅威を抜け漏れなく抽出し，発生頻度を加味することによりリスク評価を行うことが必要である。セキュリティポリシー作成支援ツールは，表 1 の機器タイプごとに発生しうる脅威と，その発生頻度を検討した結果をあらかじめ準備している。このため，システム開発時には機器を選択し，各構成要素で発生しうる脅威の一覧を作成することで脅威抽出／リスク評価を実施できる。

### 2.1.3. 対策内容の検討

モデル化した個々の機器タイプごとに，発生しうる各脅威に対する技術面・運用面からの対策内容を検討することが必要である。セキュリティポリシー作成支援ツールでは，発生しうる脅威に対し，表 2 に示すカテゴリの対策内容を検討した結果をあらかじめ対策内容DBとして準備している。このため，システム開発時には機器タイプを選択し，その機器タイプごとの対策内容の一覧を作成することで脅威に対する対策内容の検討を実施することができる。

表 2 対策内容の種別

| 対策種別 | 実施目的 |
|---|---|
| アクセス権限の設定・管理 | 不正なアクセス権の付与を防止する |
| 識別と認証 | 不正ユーザを判別する |
| アクセス制御 | リソースに対して実行可能な操作を限定する |
| ファイル・伝送データの暗号化 | 格納したデータや通信データの機密性を確保する |
| アクセス監視 | 不正行為を監視する |
| 侵入者・ウイルス対策 | 悪意のある操作を未然に防止する |
| セキュリティ管理状況の点検 | セキュリティ機能が適切に使用されているかを確認する |
| 人員管理 | オペレータ等の不正行為を防止する |
| 入退室管理 | 施設への不正侵入を防止する |
| 施錠管理 | 情報資産への物理的な不正アクセスを防止する |
| 端末管理 | 端末の不正使用を防止する |
| オペレーション管理 | 機器に対する不正な操作を防止する |
| プログラム管理 | ソフトウェアの不正な置き換えを防止する |
| デバッグ管理 | ソフトウェアへの不正な機能の混入を防止する |
| インストール管理 | システムへの不正な機能の導入を防止する |
| ドキュメント管理 | システム等の機密情報の漏洩を防止する |
| データ管理 | 機器内にあるコンテンツを保護する |

### 2.1.4. 実施項目の選択

実システムを構築する際には，(1) 対策コストを考慮することが必要であることと，(2) システムの稼働環境によっては省略可能な項目も存在することから，2.1.3節で検討した対策内容の中から実施項目を選択することが必要である。セキュリティポリシー作成支援ツールでは，脅威の発生しやすさと影響度を基にあらかじめリスク評価を実施している。このため，リスクの高いものから順に対策内容を選択することにより，コストに見合ったセキュリティ対策を実施することができる。

### 2.1.5. 機器設定パラメータの設計

実施項目を具体化するため，個々の機器におけるセキュリティ設定として設定パラメータに落とし込む作業が必要である。セキュリティポリシー対策支援ツールは，対象システムの構成機器を 6 種類のタイプにモデル化するものであり，具体的な製品における設定項目に関する情報を管理していない。このため，個々の製品に対する機器設定パラメータは，手作業で設計する必要がある。

## 2.2. 構築フェーズ

### 2.2.1. 機器設定

仕様書に記述された設定パラメータを，ハードウェアに設定を行う作業が必要である。設定作業は，各機器が提供する専用の GUI を利用する方法や，テキスト形式の設定ファイルをエディタで編集する方法を用いて実施することが多い。報告

者らは，Webベースで統一されたGUIを持ち，リモートからセキュアに設定作業を行うことができるセキュリティ運用管理ツールの開発も行っている[1]。

#### 2.2.2. セキュリティ設定検査

構築されたシステムに対し，セキュリティポリシーを正しく反映した設定がなされていることを検査する作業が必要である。セキュリティ設定検査作業には，擬似的な不正アクセスをネットワーク経由で試行することにより診断する方法と，機器の内部で擬似的な不正アクセスを試行することにより診断する方法を実施することが多い。

### 2.3. 開発工程支援における課題

前節までに述べたように，インターネット接続システムを開発する際の設計フェーズおよび構築フェーズにおける作業手順は，現状では図1に示すようにツールによる作業支援が行われている。

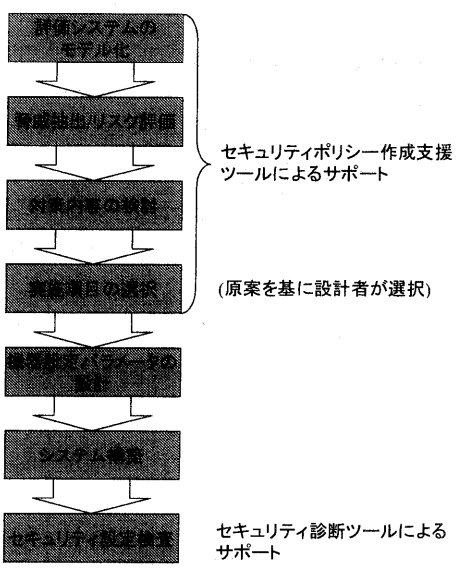


図1　システム開発工程における
セキュリティ管理の支援状況

従って，インターネット接続システムの開発工程においては，要求仕様からセキュリティポリシーの原案を作成するまでの手順と，セキュリティ設定検査を行う手順のみ支援ツールが提供されている状況であり，部分的なセキュリティ管理しか実現されていない。そこで，体系的かつ効率的なセキュリティ管理を実現するには，以下の課題を解決する必要がある。

(1) 機器設定パラメータ作成手順の容易化
策定したセキュリティポリシーから導出した実施項目を，セキュリティ設定の設定パラメータに落とし込み，詳細仕様を作成する作業は，実施項目の内容と，個々の機器のセキュリティ機能を十分理解した上で行う必要がある。このため，作業者には高いスキルと知識が要求される。

(2) 機器設定手順の容易化
インターネット接続システムは，サーバ・ルータ・ファイアウォール等のさまざまな機器により構成されている。これらの機器の設定方法は，製品ごとに異なっていることが多い。このため，作業者は，各機器の設定方法に関して精通している必要がある。

(3) セキュリティ設定検査手順の容易化
設定検査は，策定したセキュリティポリシーから導出した実施項目に対応して抜け盛れなく検査項目を策定する必要がある。

## 3. ポリシーベースセキュリティ構築支援システムの提案

本章では，2.3節に述べた課題を解決することを目的とする“ポリシーベースセキュリティ構築支援システム”を提案する。本システムは，インターネット接続システムの開発工程において，セキュリティポリシー作成支援ツール，セキュリティ診断ツールおよび，セキュリティ運用管理ツール

を連携させるツールを実現することにより，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。

### 3.1. 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

図 2 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。本システムは，セキュリティポリシーを基として，機器設定パラメータおよび検査項目を生成する機能と，管理対象に対して設定および検査を行う機能を実現することにより，インターネット接続システムの開発工程全体を支援する。

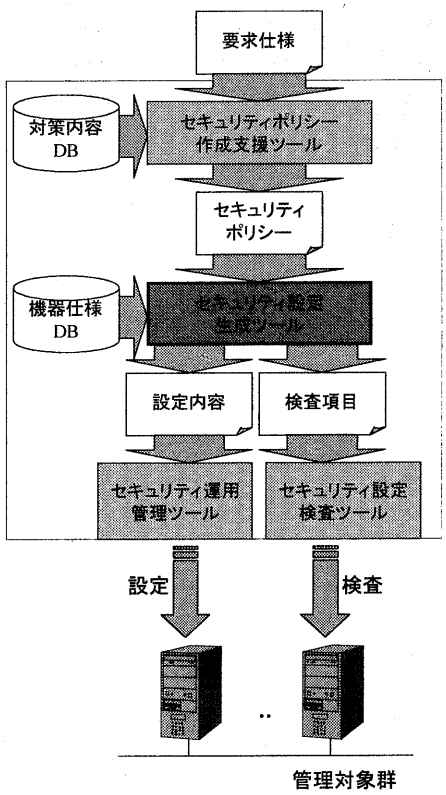


図 2 ポリシーベースセキュリティ構築支援システムのモジュール構成

### 3.2. セキュリティ設定生成ツール

セキュリティ設定生成ツールは，セキュリティポリシー作成支援ツールの出力結果を基に機器設定パラメータ作成手順を容易化するもので，セキュリティポリシーを実現する具体的な製品の設定パラメータと検査項目の作成を支援する機能を持つツールである。本ツールと，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を連携させることにより，機器設定手順の容易化とセキュリティ設定検査手順の容易化を実現することが可能になる。

本ツールによる設定パラメータ作成機能を実現するには，セキュリティポリシー作成支援ツールが出力する対策内容と，個々の製品におけるセキュリティ設定との対応付けをあらかじめ実施することが必要である。

セキュリティポリシー作成支援ツールが出力する対策内容の中で，開発工程における機器設定作業と関連する項目には，以下のものがある。

(1) アクセス権限の設定・管理

ファイルやデバイスなどの，機器の内部リソースに関するアクセス権限に関する対策項目や，機器にアクセスする主体の認証情報が有効な期限等の対策項目がある。

(2) 識別と認証

端末やユーザの認証方法に関する対策項目がある。

(3) アクセス制御

機器の内部リソースに対するアクセス制御を実施するための対策項目と，ネットワークに対するアクセス制御を実施するための対策項目がある。

(4) ファイル・伝送データの暗号化

システム設定用ファイル等の暗号化に関する対策項目と，通信路におけるデータ暗号化に関する対策項目がある。

(5) アクセス監視
機器の内部リソースに対するアクセス監視を実施するための対策項目と，ネットワークに対するアクセス監視を実施するための対策項目がある。

(6) 侵入者・ウイルス対策
侵入検知機構や，ウイルスチェックを実施するための対策項目がある。

(7) セキュリティ管理状況の点検
機器自身や，ネットワークの稼動状況の監査を実施するための対策項目がある。

セキュリティ設定生成ツールは，これらの対策項目と，個々の製品の具体的な設定項目の対応関係を機器仕様DBとしてあらかじめ準備する。システム設計者は，ツールが提示する設定項目のテンプレートに具体的な設定値を記入することにより，抜け漏れなく必要な機器設定パラメータを作成することが可能になる。

また，対策項目とその検査項目の対応関係も機器仕様DBにあらかじめ登録することにより，抜け漏れなく必要な検査項目を作成することも可能になる。

## 4. まとめと今後の課題

本稿では，情報システムのセキュリティ対策をライフサイクル全体に渡って体系的に行えるようにする一環として，特に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”を提案した。

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ことにより，情報システムの開発工程において，セキュリティポリシーから機器の設定パラメータと検査項目の作成を支援する“セキュリティ設定生成ツール”を新たに導入し，従来から使用されている (1) セキュリティポリシー作成支援ツール (2) セキュリティ運用管理ツール(3) セキュリティ診断ツールを連携して動作させることにより，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できるようになると考えている。

現在，セキュリティ設定生成ツールは，ファイアウォールを対象機器として開発を進めている。今後は，セキュリティポリシー作成支援ツールでモデル化された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.