マルチメディア通信と分散処理 111－17
コンピュータセキュリティ 20－17
（２００３．２．２７）

# 統合セキュリティ運用管理システムにおける設定内容生成機能の提案と実装

笠井真理子* 萱島信* 渡辺義則* 中野喜之**

**あらまし**: インターネット上の脅威の増大や，防御対象となるシステムの大規模・広範囲化に伴い，システム管理者やセキュリティ管理者による設計から運用までのトータルな対策の検討・実施が困難になってきている。こうした状況に対処するために，報告者らは，情報システムの設計・構築・運用の各フェーズにまたがって運用管理をサポートする「統合セキュリティ運用管理システム」を提案している。本システムでは，論理的に設計した内容を正確に機器に適用し，設計どおりの正しい動作をさせることを目標の一つとしている。しかしながら，管理対象となる機器には，さまざまな種類があるため，論理的に設計した内容を機器が正確に実施するように設定することが難しいのが実情である。

そこで，本稿では，論理的に設計した内容をスムーズに物理的な構築に反映させることを支援する設定内容生成モジュールの提案，及び，その実装方式について報告する。

# A technique of supporting to set up a machine in Integrated Security Management System

Mariko Kasai*, Makoto Kayashima*, Yoshinori Watanabe*, Yoshiyuki Nakano**

**abstract** Recently the threat on the Internet is increasing. And, the scale of the system is growing large. For this reason, it is difficult for system administrators and security managers to consider and implement security measures which cover a design to operation in total. Corresponding to such a problem, we have proposed the “Integrated Security Management System” which supports consistently the construction phase and the operation phase from the design phase.The one of the purpose of the system is to support applying to the machine precisely. Reality, however, is not that simple.

Then, this paper proposes the technique of supporting to set up a machine without trouble.

## 1. はじめに

近年，ネットワーク環境においては，管理対象となる情報システムの大規模化・広範囲化が進展すると共に，インターネット接続等に伴う外乱やセキュリティ上の脅威の増大も顕著になっている。このため，システムにおいて発生する障害も，その発生部位や原因が多様化しつつあり，システム管理者やセキュリティ管理者による迅速な障害復旧が困難になってきている。

こうした状況の中，システムの迅速な障害復旧を行うためには，障害に関係する情報収集方法を設計時から考慮するなど，システムの設計から運用にわたってトータルな対策を検討・実施することが重要な課題となる。そこで，報告者らは，システムの設計，構築，

* (株) 日立製作所 システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
**(株) 日立システムアンドサービス
Hitachi Systems & Services, Ltd.

運用の各フェーズのツールを連動させることにより，セキュリティを中心とした運用管理をサポートする「統合セキュリティ運用管理システム」を提案し[1]，システムで管理可能な対象数やネットワークトラフィックへの影響など，スケーラビリティに関する課題に取り組んできた[2][3]。

また，「統合セキュリティ運用管理システム」では，論理的に設計した内容を正確に機器に適用し，設計どおりの動作をさせることを支援することも目標としている。しかしながら，管理対象となる機器には様々な種類(機能，ベンダ)があるため，論理的に設計した内容を機器が正確に実施できるように設定することが難しいのが実情である。

そこで，本稿では，論理的に設計した内容をスムーズに物理的な構築に反映させることを支援する設定内容生成モジュールの提案，及び，その実現方式について報告する。

## 2. 設定内容生成モジュールの検討

### 2.1 統合セキュリティ運用管理システムにおける設定内容生成モジュール

統合セキュリティ運用管理システムを用いたにおける設計から構築までの処理フローを図１に示す。

設計フェーズ支援モジュールは，管理対象となるシステムに対する網羅的なセキュリティポリシー等，機器を運用する上での指針を策定し，それに基づき，管理対象機器に設定すべき情報(設定情報)を生成することを支援する。そして，設定内容生成モジュールが，論理的に導いた設定情報を実際の機器に適用できる形式に変換する。

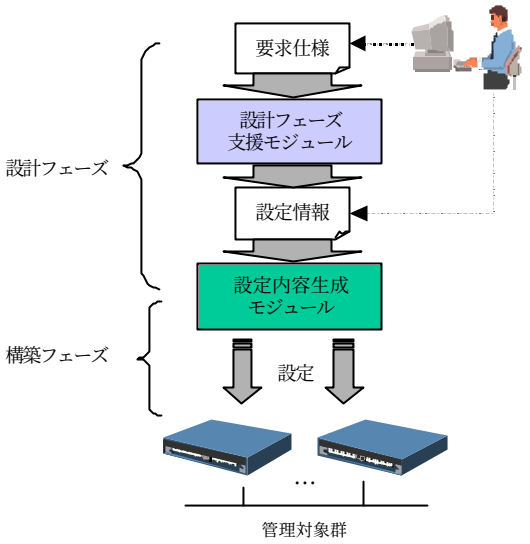


図１　設計から構築までの処理フロー

策定したセキュリティポリシーがシステムに忠実に適用されるか否かは，設定内容生成モジュールが備える機能（ポリシーの具現性）に大きく依存するため，本モジュールの実現方法については十分な検討が必要となる。

統合セキュリティ運用管理システムの管理対象となる装置の中で，インターネットVPN(Virtual Private Net Work)を構成する装置 (以降本稿ではVPN機器と呼ぶ)は，操作業が難航しやすい機器として知られている。これは，例えば，ファイアウォール等のネットワーク機器の場合，一つの機能を設定するためには，設定対象となる1台の機器の設定を行えばよいのに対し，VPNを構築する場合は，図２に示すようにVPNに関する設定情報を，VPNを構成する2台のVPN機器(図中VPN機器A,VPN機器B)の設定が必要で，この設定を行う際，VPNを構成する両機器間の整合性等への配慮が特に必要となるためであると考える。

本稿では，設定内容生成モジュールの検討をVPN機器を例にして実施した。

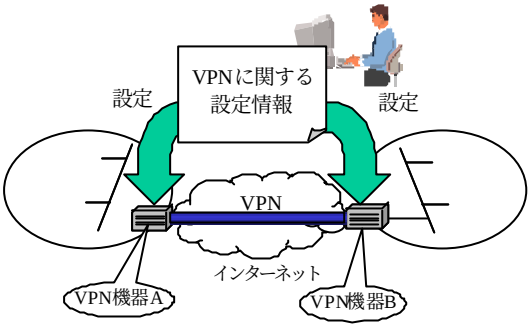


図２　VPN 機器の設定

### 2.2 VPN 機器の現状

VPN 機器設定内容生成モジュールを検討するにあたり，まず，設定作業が難航しやすい要因を VPN 機器の相互接続実験等の経験を元に，四つに分類した。

要因１　機種毎に入力形式が異なる。

設定に使用する方法やデータの形式が機器ベンダ毎に異なる。このため，設定対象となる機器の設定方法に合わせて，設定情報を変換することが必要になる。

要因２　機種毎にサポート範囲が異なる。

インターネット VPN で使用される暗号通信プロトコルは，IPsec(IP Security)[4]として標準化されているが，規定された仕様全てを実装することは求められていないため，そのサポート範囲は機器毎に異なる。このため，設定対象となる 2 台の VPN 機器のうち，一方の VPN 機器には設定情報を設定することができるが，もう一方の機器に同じ設定情報を設定することができず，結果として VPN を構築することができないといった問題が発生することがある。

要因３　IPsec の設定項目自体が複雑である。

IPsec は，暗号方式や認証方式の設定だけにとどまらず，暗号鍵の管理等に関しても，設定する必要があるため，設定項目が細かく，項目数も多い。このため，正しい設定を行うためには，IPsec の動作の詳細を理解する必要があり，設定作業に多くの時間と経験（スキル）を要する。

要因４　異なる VPN 機種間での接続に相性問題が発生することがある。

機器の仕様上設定が可能な値であっても，接続先の機器との相性問題によって接続に問題が発生してしまう場合がある。相性問題は，IPsec の仕様に曖昧な点があるためベンダ毎の解釈の違いによる実装に違いや，IPsec の仕様が膨大であることによる仕様の読み違いや勘違いが主な原因となっている。

### 2.3 VPN 機器設定内容生成モジュールの手段

構築作業をスムーズに行えるようにするために重要な VPN 機器設定内容生成モジュールの手段は，前節で述べた要因から以下に示す三つになると考えられる。そこで，本節では，その具体的手段の検討を行う。

手段１　機種依存性の吸収
(要因 1,2 に対する配慮)

VPN 全体の設定を行う統一されたインターフェースを設けると共に，入力された情報を VPN 機器固有の形式に変換する機能を設ける。また，機種毎のサポート仕様をデータベースとして保持しておき，機器のサポート範囲外での使用などを設定適用前に検知する機能を設ける。これらの手段により，機種毎の仕様差異の吸収を図る。

なお，適切な設定が行われていないことを検知した場合は，セキュリティポリシーの見直しも含めた再設定を促す。

手段２　入力情報の簡略化
（要因 3 に対する配慮）

設定内容生成モジュールに入力する情報は，IPsec の設定に最小限必要な項目のみにあらかじめ絞り込んでおく。これにより，IPsec 自体の複雑さを隠蔽すると共に，入力

情報の設定項目数も低減させる。

簡略化することによって入力情報から除外される設定項目は，デフォルト値を定義しておくことで補完する。そして， 扱う VPN 機器の機種に依存しない共通形式の情報群を生成する。

この共通形式の情報群は，ユーザ入力情報から生成される情報群と，前もって定義したデフォルト値から生成される情報群の２つの情報群で構成される。

手段 3　相性問題の回避
（要因 4 に対する配慮）

機器間の相性に関する情報を所定の形式でデータベースに保持しておき，設定適用前に相性問題を検知する機能を設け，相性問題の発生を回避する。相性問題が発生することを検知した場合は，セキュリティポリシーの見直しも含めた再設定を設定作業者に促す。

## 2.4　実現方法

前節の VPN 機器設定内容生成モジュールの要件を実現するために必要とされる機能は，整理して書き直すと，以下の五つである。

(a)統一された設定編集インターフェースの提供(要件 1)
(b)機器仕様のチェック機能(要件 1)
(c)設定情報補完機能(要件 2)
(d)相性問題のチェック機能(要件 3)
(e)個々の機器固有設定形式への変換機能(要件 1,2)

これらの機能の関連を，機器設定内容生成モジュールの基本処理フローとして図３に示した。

まず，機器仕様との適合性チェック機能(b)を用いて，統一の設定編集インターフェース(a)によってされて入力された VPN 設定情報が，設定対象となる機器の仕様の範囲内にあるかをチェックする。問題がない場合は，設定情報補完機能(c)を用いて VPN 設定情報に含まれない設定項目の情報を補完し，設定に必要な全ての情報が生成される。その後，相性問題のチェック機能(d)を用いて，相性問題が発生する可能性がある設定内容になっていないかのチェックを行う。問題がない場合は，個々の機器固有設定形式への変換機能(e)を用いて，設定対象の機器に対応した形式に設定情報を変換し，機器に適用する。

上述のような機能と処理フローでモジュールを構成することで, システムが扱う VPN 機器の機種が増えたりした場合には，変換機能(e)のみを変更・追加すればよい。また，VPN 機器の仕様や相性に関する情報をデータベース化することで，仕様の変更や相性問題の解決が VPN 機器側で図られた時に，データベースを更新することで速やかに最新状態を扱えるようにした。

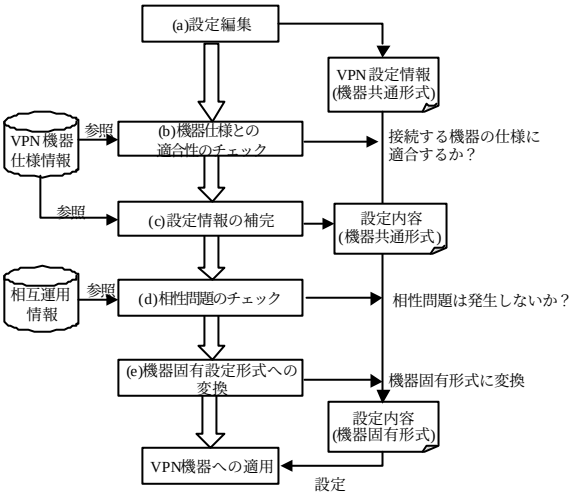


図３　VPN 機器設定内容生成モジュールの基本処理フロー

次に, VPN 機器設定内容生成モジュールが扱う情報について説明する。

(1)VPN 設定情報

VPN 設定情報は，VPN の構築に最小限必要な情報で, VPN 機器設定内容生成モジュールに入力する情報とする。本研究では，VPN の構築に最小限必要な項目は，主要な IPsec

対応製品(5 製品)を対象として調査し，各製品がユーザに設定させている項目を分析することによって絞込みを行った。

(2)VPN 機器仕様情報

VPN 機器仕様情報には，(a) VPN 設定情報の各項目の設定可能範囲，(b) VPN 設定情報に含まれない設定項目のデフォルト値，の各情報が含まれる。 (a)設定可能範囲は，設定情報が設定対象となる 2 台の VPN 機器の仕様範囲内にあるか否かのチェックを行う時に使用される情報である。(b) VPN 設定情報に含まれない設定項目のデフォルト値は，ユーザが設定する項目を簡略化するために VPN 設定情報から除外された IPsec の設定項目を補完するための情報である。

(3)相互運用情報

相互接続情報には，(1)正常に接続できないなどの問題を起こした VPN 機器のペア，(2)不具合を引き起こす項目，(3)不具合の原因となる項目値，(4)問題の種類についての情報が含まれる。問題の種類には，「トンネル両端の機器の仕様上は設定可能であるが実際には正しく動作しない」，「ある機器の組み合わせのときに特定の設定を行わないと正しく動作しない」といったものがある。後者の場合には，動作させるために必要な設定を自動的に行うための情報も含まれる。

2.2 節で述べた通り，相互接続性の問題は仕様書では確認できない問題であり，設定作業を滞らせる要因の一つとなっている(要因 4)。これを回避するためには，実際に運用で発生した問題を蓄積していくこと，また，相互接続試験を積極的に行い判明した問題を蓄積していくことが必要である。

## 3. プロトタイプの開発

図 3 に示した基本構成に基づき，機器設定内容生成モジュールのプロトタイプを作成した。

実際の VPN 機器の設定方法は，シリアルコンソールによるものやファイルによるものなど，様々である。このため，各機器に対する設定操作を行うモジュールまで管理サーバに組み込むと，管理サーバが肥大化する。そこで，本プロトタイプでは，設定インターフェースを提供するマネージャモジュールを管理サーバ上に配置し，マネージャからの指示で実際の処理を行うエージェントモジュールを管理対象機器に常駐させた。そして，図４に示すように，相性問題のチェック機能まではマネージャに，機器独自の形式に変換する機能はエージェントに実行させることにした。なお，エージェントを実装することができない管理対象機器に対しては，管理対象機器と管理サーバ間に，エージェントを実装した機器を置くことによって，対応することができると考えている。

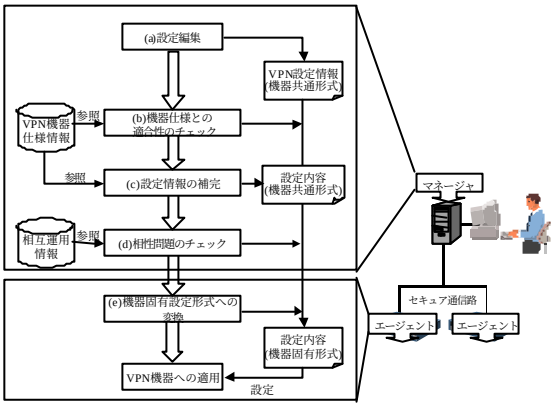


図４　プロトタイプの概要

また，設定内容の配布は，盗聴，改ざんを防止するセキュアな通信路で行わなければならない。本プロトタイプは，既に開発済みの運用管理ツールに組み込みこむことで，セキュアな通信路を使用して設定を行えるようにした。

本プロトタイプで開発した機種依存性を吸収するための設定編集インターフェースの例を図５に示す。

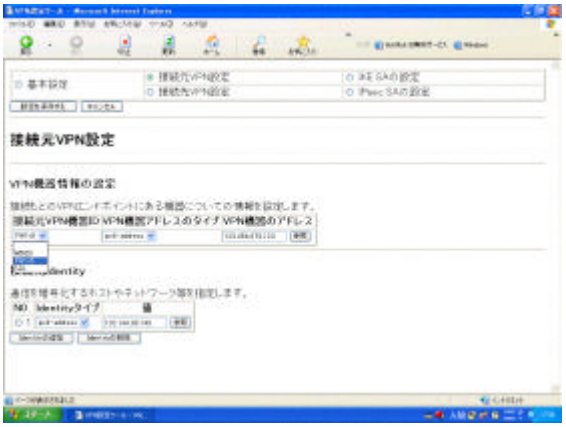


図５　設定編集インターフェース

本プロトタイプでは，IPsec 対応製品(5 製品)の設定項目の調査結果をもとに，IPsec 設定に必要かつ十分と思われる設定項目を抽出した結果に基づき，この設定編集インターフェースで設定する項目数を 20 項目にした。表１に設定作業で入力する項目数の一例を示す。本プロトタイプを適用することによって，適用前と比較して，ユーザが入力する項目数を半数以下に削減することができた。

表１　設定項目数

| 設定対象機器機種 | | 設定項目数 | |
|---|---|---|---|
| 機種名 | | 適用前 | 適用後 |
| Cisco IOS Release12.0 | Windows2000 | 47 (22+25) | 20 |
| Firewall-1 | Windows2000 | 42 (17+25) | |
| Windows2000 | Windows2000 | 50 (25+25) | |

なお，本プロトタイプの動作は，Windows2000 と Firewall-1 の接続構成で確認済みである。

## 4.　まとめと今後の課題

本稿では，統合セキュリティ運用管理システムの目標である論理的な設計した内容を正確に機器に適用し，設計どおりの正しい動作をさせるため，特に VPN 機器を対象とした設定内容生成モジュールを提案し，その実現方式について検討した結果を報告した。

設定内容生成モジュールは，設定作業の効率化と障害誘因を防ぐものであり，簡略化された設定編集インターフェース，機器仕様のチェック機能，相性問題のチェック機能，設定情報補完機能，個々の機器固有設定形式への変換機能で実現することができた。

今後は本プロトタイプを用いて，ユーザ実作業における工数削減効果，調査対象とした機種以外の機種への適用性，相性問題回避機能の実問題への有用性等に対する評価を行い，実際のネットワーク構築に適用できるレベルまで機能を充実させていく。

## 謝辞

本研究は，通信・放送機構(TAO)の委託研究テーマ「インターネットにおける障害情報の収集及び復旧支援技術の研究開発」の一環として行われているものである。

## 参考文献

[1]統合セキュリティ運用管理システムの実現に向けて，萱島他，情報処理学会第 62 回全国大会，2001.3
[2]スケーラビリティ向上を目的とした運用管理システム，礒川他，情報処理学会第 63 回全国大会，2001.9
[3]スケーラブルセキュリティ運用管理システムのネットワークトラフィックに関する評価，礒川他，SCIS 2002，2002.2
[4]RFC2401, http//www.ietf.org/rfc.html