多面的ビューを持つインターネットセキュリティ管理支援システムの提案

礒川 弘実[†]　萱島　信[†]　寺田 真敏[†]　中野 喜之[††]　山崎 隆行[†††]

(株)日立製作所 システム開発研究所[†]
日立中部ソフトウェア(株)[††]
(株)日立情報ネットワーク[†††]

要旨

インター／イントラネットを基盤とする企業情報システムが，企業の業務遂行やビジネスのために重要な役割を担うようになり，企業情報システムのセキュリティや安定稼動の重要性が増しつつある。これらセキュリティや安定稼動を維持するため，多くの企業では，管理支援システムを導入し，企業情報システムの運用管理の効率化を図っている。ところが，既存の管理支援システムには，管理者へ提供する情報が管理できるオブジェクト単位で，管理者毎の欲しい情報が得にくいといった問題があった。本稿では，管理支援システムの利用者へのより効率的な情報提供，管理機構の提供を図るため，セキュリティ管理者，ネットワーク管理者や一般ユーザなど，利用者の役割に応じた“ビュー”を提供するという特徴を持つ管理支援システムを提案する。

A proposal of a Internet security management support system that provides multi-sided user views

Hiromi ISOKAWA[†]　Makoto KAYASHIMA[†]　Masato TERADA[†]
Yoshiyuki NAKANO[††]　Takayuki YAMAZAKI[†††]

Systems Development Laboratory, Hitachi, Ltd.[†]
Hitachi Chubu Software, Ltd.[††]
Hitachi Information Network, Ltd.[†††]

Abstract

In many enterprises, the information network infrastructure based on Internet/Intranet has come to be more important for performing works or business. Therefore, the quality of the enterprise network system, such as security and availability is being more significant. To keep the quality good, the system administrators of the enterprise network use some network management support systems. In this paper, we propose a security management support system that can provide multi-sided user views, such as security administrator's view, network administrator's view and end-users' view.

1．はじめに

インターネット技術を基盤とした企業情報システムは，社外最新情報の早期収集，社外への情報発信，電子モールや企業間商取引といった EC (Electronic Commerce)ビジネス提供など，世界規模のビジネス展開に利用され，その重要性が増しつつある。これに伴い，企業情報システムには，(1)不正アクセスなどの脅威に対するセキュリティの確保と，(2) 24 時間 365 日の安定した稼動性の確保が求められるようになってきている。

このような企業情報システムを運用管理するにあたっては，安全性の確保，安定性の確保という二つの見地から進めていく必要がある。

(1)安全性

企業情報システムを不正アクセスやウィルスなどの脅威から保護することであり，セキュリティポリシーに従ったセキュリティ対策と共に，セキュリティポリシーに従った運用を実施していく必要がある。

(2)安定性

24 時間 365 日，企業情報システムの安定した稼動環境の提供することであり，二重化やバックアップによる信頼性向上と共に，障害発生時の検知ならびに復旧作業の迅速化を図る必要がある。

本稿では，安全性と安定性の双方の管理支援を実現するシステムとして，セキュリティ管理者，ネットワーク管理者や一般ユーザなど，利用者の役割に応じた管理画面“ビュー”を提供することを特徴とするシステムを提案する。これは，利用者に必要な“ビュー”を管理支援システムから切り出すことで，利用者への効率的な情報提供や運用管理の支援を可能とするものである。

2．既存の管理支援システムの課題

企業のネットワーク管理部署では，企業情報システムの維持のため，セキュリティ対策，障害復旧などの運用管理作業を日々行っている。このような運用管理作業には，多数台のシステム機器を統合的に管理し，不正アクセス監視などの日常的な定型作業や障害復旧などの突発的な対策作業などを支援する管理支援システムが有用である。

しかし，多くの既存管理支援システムには，以下のような課題があると考えている。

(1)対象オブジェクトに基づく“ビュー”の提供

管理者の役割に応じた管理“ビュー”を提供するのではなく，管理することのできる対象オブジェクトに基づいた管理“ビュー”に留まってしまっている。このため，より上位階層の管理者に対しては，管理者の役割に応じた管理“ビュー”として，月間報告書などのようなサマリ情報を紙の報告書として提出していることが良く見受けられる。

(2)管理情報の提供先の限定

運用管理に関する情報提供先は管理者のみであるという考え方があり，利用環境に影響を与える運用管理情報は一般のユーザには提供されていない。

3．多面的なビューシステム

本章では，既存管理支援システムの課題を解決する，ネットワーク管理者やセキュリティ管理者，一般ユーザなどの利用者の役割に応じた多面的な管理“ビュー”について述べる。

3.1 多面的ビューシステム

多面的ビューシステムとは，管理支援システムが管理情報や管理機構を画面で提供する際に，利用者の役割に応じ，管理“ビュー”を提供するシステムである。

例えば，企業情報システムの安全性確保について考えた場合，インターネットからなどの不正アクセスを防止する不正アクセス対策では，企業のセキュリティニーズにあわせ，「調査」「構築」「保証」の対策フェーズ，「短期」「中期」「長期」などの対策スパンに分かれる作業を，サイクルとして継続的に繰り返しながらセキュリティ強化を図っていくことが求められる(図1)。

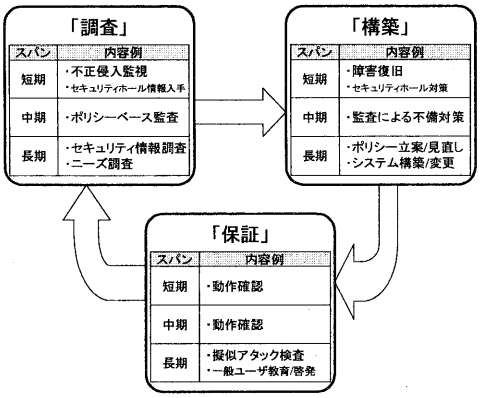

図 1　不正アクセス対策のサイクル

このような不正アクセス対策サイクルに基づいて，セキュリティ管理を考えてみると，セキュリティ管理支援システムに求められる機能は，各フェーズ／各スパンの個別管理から対策サイクル全体管理を網羅する管理支援機能である。また，ここで考慮すべきことは，多くの運用管理において，管理者はその役割に応じて階層化されている点である。例えば，不正アクセス対策サイクルで見ると，管理者の役職に合わせ，「各フェーズ／各スパンの個別管理の一部を担当する管理者」「スパンの全体管理を担当する管理者」「不正アクセス対策サイクルの全体管理を担当する管理者」といった階層化形態となる(図 2)。

これらのことを踏まえると，各フェーズ／各スパンの個別管理から対策サイクル全体管理を網羅する管理を効率化するには，単に機器の稼動状態やセキュリティ警告など管理対象オブジェクト単位の管理“ビュー”ではなく，管理者の役割に応じた管理“ビュー”を提供する管理支援システムが有効である。

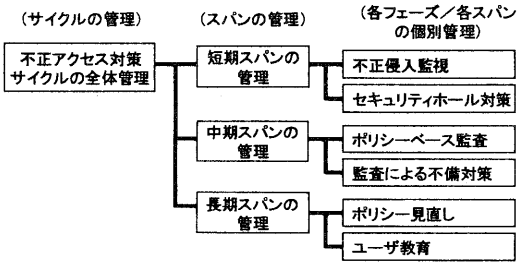

図 2　管理の階層化

また，インターネット技術をベースに構築されている企業情報システムの一般ユーザは，ネットワークやサーバ障害，ネットワーク性能状況，セキュリティ上の問題が利用環境に与える影響を即座に把握することのできる情報を欲している。逆に，企業情報システムの管理者も，ウィルスなどのセキュリティ上の対策情報や，予定されたネットワーク停止連絡等の情報を，一般ユーザに対して迅速確実に提供することで，一般ユーザレベルの運用管理の効率化を図りたいと考えている。

これらのことから，一般ユーザを考慮した運用管理の効率化を支援するには，運用管理に関する情報を，管理者だけでなく一般ユーザに提供する管理支援システムが有効である。

以上述べたように，インターネット環境の運用管理を支援するシステムのビューとして，(1)管理者の役割に応じたビューの提供，(2)一般ユーザ向けのビューの提供，を基本コンセプトとする多面的ビューシステムが有効であると考えている。

3.2 多面的ビューの画面イメージ

多面的ビューシステムが提供する画面のイメージを具体的画面(図 3～図 5)を用いて示す。

(1) [図 3]不正アクセス対策サイクル全体の管理を担当する管理者向け画面

緊急メッセージフィールドには，他管理者からの連絡事項のみを表示する。メニューフィールドには，セキュリティ監査のサマリ情報や，他管理者の進捗管理機能などに一操作でアクセスできるボタンを表示する。

(2) [図 4]不正アクセス対策の短期スパンの管理を担当する管理者向け画面

緊急メッセージフィールドには，他管理者からの連絡事項に加え監視機構からの不正アクセスに関する情報を対策機構と共に表示する。メニューフィールドには，不正アクセス詳細調査情報や自身の進捗管理機能，他管理者へのメッセージ送信機能などにアクセスするためのボタンを表示する。

(3) [図 5]一般ユーザ向け画面

緊急メッセージフィールドには，最新ウィルス情報など管理者からの情報と一般的なネットワーク稼動状況情報を表示する。メニューフィールドには，ネットワーク利用規約情報などを表示するためのボタンを配置する。

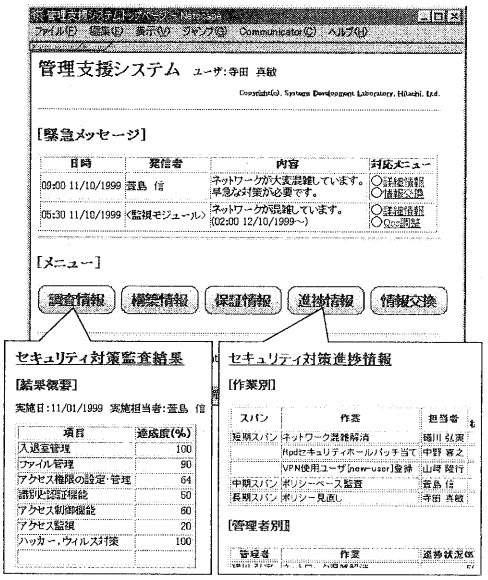

図 3 全体サイクル管理者用画面

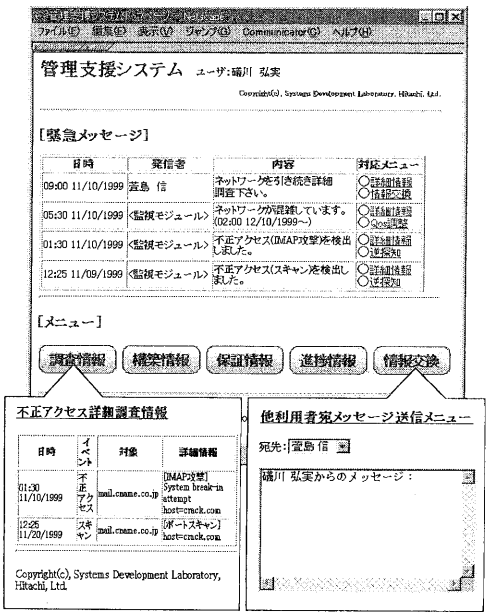

図 4 短期スパン担当管理者用画面

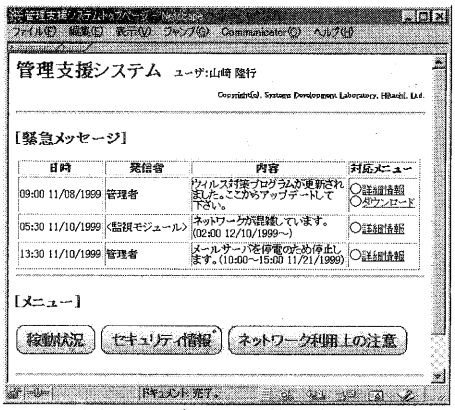

図 5 一般ユーザ用画面

3.3 多面的ビューシステムのアーキテクチャ

多面的ビューとして利用者の役割に応じた管理画面を生成するということは，管理支援システム自身が保持している情報の切り出し方を様々に変えることである。そこで，多面的ビューシステムの構成として，情報収集機構と，利用者の役割に応じた管理画面生成機構を独立した構成にすることで，情報の切り出し方を容易に変更できるようにする。

また，情報収集機構では複数情報源の統合化を，管理画面生成機構では画面の部品化を行う。

(1)複数情報源の情報の統合化

SNMP(Simple Network Management Protocol)管理製品や IDS(Intrusion Detection System)製品など，複数の情報源から管理対象の情報収集を行い，取得した多くの情報から共通情報や関連項目を整理し統合化する。これにより，個々の管理製品から得られる情報の関連付けなど，利用者は情報を再構成する手間を省くことができる。

(2)画面の部品化

管理画面を表やボタンなど管理情報／管理機構別に細分化，部品化し，画面部品の集合として管理画面を構成する。これにより，管理画面を部品で管理することができ，利用者単位の管理画面のカスタマイズが容易になる。

以上を取り入れた多面的ビューシステムのアー

キテクチャの概要を図6に示す。情報収集モジュールにおいて，複数の情報源から情報を収集／管理すると共に，情報の統合化を行う。そして，画面作成モジュールにおいて，個々に異なる情報／機能を持った画面部品を作成した後，利用者に応じ画面部品を組合わせ，利用者毎の管理画面を構築する。

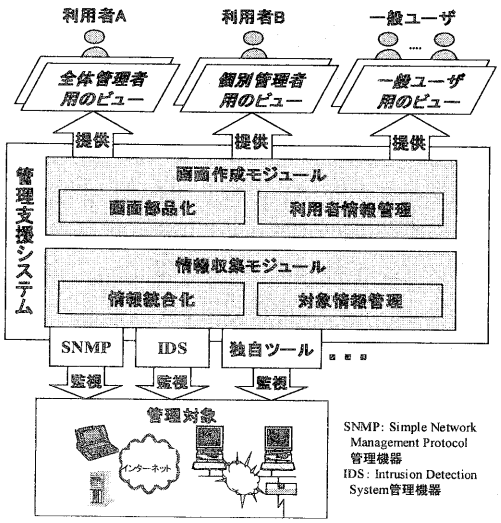

図 6　多面的ビューシステムのアーキテクチャ

4. プロトタイプシステム

利用者の役割に応じてビューを切り替えることを考慮した構成を持つ，管理支援システムのプロトタイプシステムを開発した。

4.1 プロトタイプの機構

プロトタイプシステムは，以下の機構を持つ。

(1)マネージャ／エージェント型

管理対象に関する情報収集および設定支援を行うエージェントと，複数のエージェントからの情報を収集し，ビューを生成するマネージャの二つのモジュールで構成される。

(2)ソフトウェアチップ機構

拡張性を高めるサーバ監視項目の細分化機構である“ソフトウェアチップ”(以下チップ)機構([2][3])を取り入れ，各管理項目を一つのチップとして取り扱うと共に，チップをエージェントで動作させることで各管理項目を管理する。これにより，インターネット環境のように頻繁に新しいソフトウェアが生まれても，新しいソフトウェアに対する管理項目を容易に拡張できる。

(3)コレクタ／チェッカ／レポータ機構

マネージャにおける管理ビュー生成を，エージェントからの情報収集を行うコレクタ，収集した情報の統合化を行うチェッカ，画面部品を生成し管理ビューを構成するレポータの連携によって行う。

(4)セキュア運用管理インフラ

リモートサイトに設置された管理対象計算機を安全に運用管理するために，管理計算機と管理対象計算機間の相互認証ならびに，通信メッセージの暗号化を行う。これにより，インターネットを含むリモートサイトに設置された管理対象計算機も運用管理の対象とする。

(5)Web ベース管理ビュー

管理ビュー生成の容易化を図るため，Web ベースの“ビュー”機構を持つ。

4.2 プロトタイプのシステム構成

以上の機構を持つプロトタイプシステムの全体構成を図7に，各機能モジュールの概要を表 1に示す。

表 1　各機能モジュールの概要

モジュール	機能概要
マネージャコントローラ	管理者からの要求や，全体定義ファイルの内容に基づきレポータ，チェッカ，通信モジュールを制御する。
エージェントコントローラ	マネージャコントローラからの要求や，チップ定義ファイルの内容に基づき，監視チップおよび設定チップを制御する。
監視チップモジュール	エージェントコントローラにより定期的もしくは，オンデマンドで起動され，監視対象サービスの稼動状況や，システムのセキュリティ設定等の情報を収集する。

設定チップモジュール	エージェントコントローラによりオンデマンドで起動され，サーバセキュリティ，OS等の設定を行う。
チェッカモジュール	マネージャコントローラにより定期的に起動され，チップ監視ログから警告，エラーの判定結果を示すチェッカログを生成する。
レポータモジュール	マネージャコントローラにより定期的に起動され，チップログやチェッカログから利用者の役割に応じた管理“ビュー”を提供するためのWebコンテンツ(HTMLファイル等)を生成する。
セキュア通信モジュール	エージェント側で作成したチップログをマネージャモジュール側へ転送する。またマネージャコントローラの指示をエージェントコントローラへ転送する。マネージャとエージェント間の相互認証ならびに，通信メッセージの暗号化も受け持つ。

4.3 プロトタイプの機能

プロトタイプは，以下の機能を持つ。

(1)インターネットサーバ監視

インターネットサーバ上で動作するメール，Web，ニュース，DNSの各インターネットサービスの稼動状態を監視する。サービスの稼動状態は，プロセスの有無，ネットワークを介した応答によって監視し，異常があった場合には，管理ビューにて管理者に報告する。また，サーバディスクの空き容量などのリソース状態も監視する。

(2)インターネットサーバ設定支援

インターネットサーバ上で動作するメール，Web，ニュース，DNSの各インターネットサービスの設定をリモートから変更する機能を提供する。サポートする機能は，設定ファイルの書き換え及びサービスプロセスの再起動である。

5．まとめと今後の課題

本稿では，企業ネットワーク環境の安全性と安定性の双方の管理支援を実現するシステムとして，利用者に応じた管理画面“ビュー”を特徴とするシステムを提案した。これは，利用者に必要な“ビュー”を切り出すことで，利用者へのより効率的な情報提供や運用管理の支援を図るものである。

今後は，サイクル全体管理者や一般ユーザ向けのビュー提供機能など，プロトタイプシステムの開発をさらに進め，多面的ビューの効果を評価する予定である。

参考文献

[1]乾泰司：ユーザ企業のIT部門からみた分散システムの統合運用管理について，情報処理学会 分散システム／インターネット運用技術研究報告 99-DSM-13, pp.13-18, May 1999.

[2]礒川弘実他:インターネットサーバの特徴を考慮したサーバ稼動監視システムの提案，情報処理学会 分散システム運用技術研究報告 98-DSM-9, pp.1-6, May 1998.

[3]伊藤武他:インターネットサービスの特徴を考慮したサーバ稼動監視システムの実装，情報処理学会 分散システム運用技術研究報告 98-DSM-10，pp.25-30，July 1998.

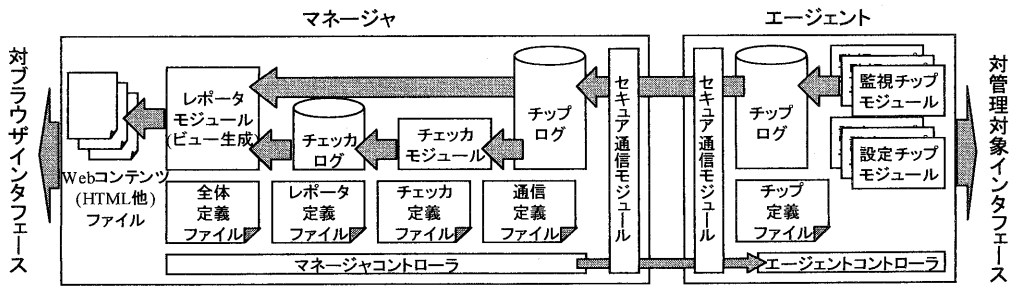

図 7　プロトタイプシステムの構成