コンピュータセキュリティ　11－15
（２０００．９．８）

統合セキュリティ運用管理システムの提案

萱島 信　寺田 真敏　永井 康彦　礒川 弘実

(株)日立製作所 システム開発研究所

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、情報システムに対する不正アクセスやコンピュータウイルスから情報資産を保護するためのセキュリティ対策が重要となってきている。このため企業は情報システムの設計、構築、運用の個々のフェーズにおいてセキュリティツールを用いたセキュリティ管理・監査を行なうことが一般的になりつつある。

しかし、現状のツールは、個々のフェーズでのセキュリティ管理を独立に支援するものであり、各フェーズにおいてツールが生成したセキュリティ関連情報をフェーズ間で有効に活用する手段が不足しているため、全体的なセキュリティ管理を実現する上で課題がある。本稿では、設計、構築、運用フェーズにおける各種ツールを連動させることで、体系的なセキュリティ管理を行うシステムを提案する。

A Proposal of Integrated Security Management System

Makoto KAYASHIMA　Masato TERADA　Yasuhiko NAGAI　Hiromi ISOKAWA

Systems Development Laboratory, 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 many enterprises become to do security management and security audit using several security tools.

However, it is difficult to achieve total security management efficiently using these individual security tools. We think the cause is the security information is not used effectively between the tools. In this paper, we propose "Integrated Security Management System" which makes systematic and total security control by coupling with various tools.

1. はじめに

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資産を保護するためのセキュリティ対策は、ますます重要となってきている。特に企業においては、ファイアウォールやウイルス対策プログラム等を導入するだけでなく、情報システムに対して定期的にセキュリティ監査を実施するといった

セキュリティ運用管理をあわせて実行することが一般的になりつつある。

このようなセキュリティ管理を正しく実施するには、システムのライフサイクル全体、すなわち、システム運用時だけではなく、情報システムの設計、構築の各フェーズも考慮する必要がある。例えば、設計フェーズにおいては、対象システムのセキュリティポリシーを策定することが必要であり、構築フェーズにおいては、ポリシーに基づき正しくセキュリティ機能を実装することが重要である。また、運用フェーズにおいても、単にファイアウォール等を利用するだけではなく、不正侵入検知ツール(IDS：Intrusion Detection System)やセキュリティ設定診断プログラム等を用いて、新たに発生したセキュリティホールに対する対策を行うことが必要である。

しかし、これまでのセキュリティ管理で使用されているツールは、それぞれ独立したものであり、全体的なセキュリティ管理を行うことを考慮していなかった。このため、ライフサイクルの部分的な支援は可能であっても、ライフサイクル全体にわたるセキュリティ管理を効率よく、かつ効果的に支援するには十分ではなかった。

そこで本稿では、対象システムの設計、構築、運用の各フェーズのさまざまなセキュリティツールにより得られる情報を活用して、体系的な管理を実現することを可能にするセキュリティ運用管理システムを提案する。

2.セキュリティ運用管理の現状と課題

本章では、インターネット接続サイト等の情報システムに対して、ライフサイクルの各フェーズで行われているセキュリティ運用管理の現状と、そこで使用されているツール群について概観し、その課題について述べる。

2.1.運用管理の現状

2.1.1.設計フェーズ

設計フェーズにおいては、情報システムに対する網羅的なセキュリティポリシーを策定した上でセキュリティ設計を行うことが一般化しつつある。特に金融系を中心に、高度なセキュリティを要求される分野では、CC (Common Criteria)[1]を用いてセキュリティポリシーが策定されるようになりつつある。また、一般的なインターネット接続サイトに対するセキュリティポリシーを簡便に作成する支援ツールの開発等も行われている[2]。

2.1.2. 構築フェーズ

構築フェーズにおいては、設計フェーズで策定したセキュリティポリシーをセキュリティ機能として正しく実装することが必要である。ここで述べるセキュリティポリシーは、たとえば「システムファイルに関するアクセス権は最小限に絞る」といったセキュリティに関する目標を示すものであり、本フェーズではこのような記述から具体的なシステム設定パラメータへの落とし込みを行う。

また、セキュリティ設定内容の確認には、一般にセキュリティ診断ツールが用いられている。診断の方法には大きく分けて以下の二通りのやり方がある。

(1) ネットワークベース検査ツールを用いる方法
SATAN[3]等のセキュリティスキャナを用いて、ホストのサービスポートに対してパケットを送信し、その応答を確認することにより脆弱性を調査する

(2) ホストベース検査ツールを用いる方法
COPS[4]等のシステムスキャナを用いて、ホストのファイル等のリソースに対する設定ミスを探すことにより脆弱性を調査する

2.1.3. 運用フェーズ

運用フェーズにおいては、セキュリティ監視・監査作業を実施すると共に、サービスプログラムのセキュリティホールに対する対策が行われるようになりつつある。

これには、セキュリティ診断ツールを用いて、対象システムの利用者による不注意な設定変更や、新たに発覚したセキュリティバグによるセキュリティホールの診断を定期的に行う方法と、不正アクセスに対するリアルタイムの防御を行うIDSを用いる方法が行われている。このIDSは、以下の2つのタイプがよく利用されている。

(1) ネットワークベースIDS
ネットワーク上でパケットを補足し、侵入事象に特有のパターン(シグナチャ)とマッチングを取ることにより侵入を分析する

(2) ホストベースIDS
ホスト上でプログラムが発したアラートにより侵入を分析する

IDSの検知・対策エージェントをファイアウォールやWebサーバに配置し、ネットワークシステム全体に対する不正アクセスを検出から対策まで一貫して行うためのフレームワークの提案もなされている[5]。

また、上記のセキュリティ診断ツールによる検査の結果、システムの設定変更やアプリケーションのバージョンアップが必要になった場合、リモートからセキュアに作業が行える環境があると便利である。そのようなセキュア操作環境としてssh[6]等がよく使用されている。

2.1.4. セキュリティ運用管理ツール

以上で述べた情報システムの設計、構築、運用の各フェーズで使用されているセキュリティ運用管理ツールの種類をまとめると、次のようになる。

・ポリシー作成支援ツール
設計フェーズにおいてセキュリティポリシーの策定を支援する

・セキュリティ診断ツール
構築フェーズおよび運用フェーズにおいてシステムの脆弱性に関する検査を実施する

・セキュリティ運用ツール
運用フェーズにおいて不正アクセスの監視と、リモートからセキュアにシステムの設定変更を実現する

2.2. 運用管理の課題

2.1.節で述べたセキュリティ運用管理ツール群を用いることにより、システムのライフサイクルの各フェーズに対して個別にセキュリティ対策を実現することができる。しかし、ユーザの環境に応じた体系的なセキュリティ管理を実現するには、以下のようないくつかの課題が存在する。

【課題1】
セキュリティポリシーがシステム設定として正しく実装されていることを保証すること

セキュリティ機能を用いた設定が、策定したセキュリティポリシーどおりに正しく設定されていることを確認する一般的な方法は存在しないため、設定内容をセキュリティパラメータに落とし込むには高度な知識とノウハウが要求される。また、設定したセキュリティパラメータが意図した通り正しく機能しているか確認することも高度な知識とノウハウが要求される。

【課題 2】

セキュリティバグが発覚した場合、そのバグの影響を受けるサーバを早急に見つけ出し、対策を実施すること

インターネットの世界では、日々新しいセキュリティバグが発覚している。このセキュリティバグは、ソフトウェアのバージョンや、その稼働環境の違いによって影響を受ける場合と受けない場合があり、問題が発生するサーバを選別するには非常に手間がかかる。また、最新のセキュリティバグの検出を行うためには、最新のセキュリティホール情報に対応したバージョンのセキュリティ診断ツールおよびIDSが必要である。

3. 統合セキュリティ運用管理システムの提案

本章では、2.2.節の課題を解決するものとして、図1 に示すモジュール群により構成される“統合セキュリティ運用管理システム”を提案する。本システムは、2.1.4.節で述べたセキュリティ運用管理ツールを組み合わせて実現されており、ライフサイクルのフェーズ間にまたがった連携機能を実現していることを特徴とするものである。

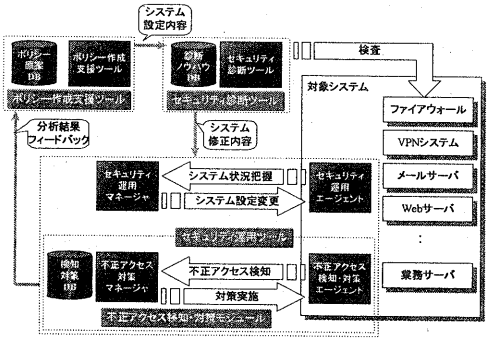

図1. 統合セキュリティ運用管理システムのモジュール構成

3.1.設計-構築フェーズ連携機能

セキュリティポリシーがシステム設定として、正しく実装されていることを保証するには、ポリシーに対応するセキュリティパラメータを明確にすることと、設定状況を確認するための診断項目を明らかにすることが必要であると考えている。そこで、ポリシー作成支援ツールに以下の機能を追加することにした。

表1 UNIX 用 Web サーバに対するセキュリティポリシーの例（抜粋）

詳細項目	ポリシー原案	設定対象
システムファイルへのアクセス権限設定	システムファイルに関するアクセス権を必要最小限に絞る	Web 設定ファイル
	管理ユティリティの利用可能者を制限する	Web ユティリティ
ユーザ ID の管理	パスワードの解析に対する対策を行う	Web 設定ファイル
アクセス制御機能	アプリケーションに対するアクセス制御を実施する	Web 設定ファイル
特権ユーザの牽制機能	特権ユーザの作業内容を把握する手段を設ける	アカウンティング
端末認証方法	IP アドレスにより相手を確認する	tcp_wrapper
本人確認機能	重要なデータに対する Web アクセスでは SSL を用いる	SSL 関連諸設定
	オブジェクトに対するアクセス制御を実施する	オブジェクト
	オブジェクトに対するアクセス権限を分割する	オブジェクト
	監査証跡にアクセスできるユーザを制限する	ログファイル
システムへのアクセス制御	リモートからアクセス可能な時間帯を制限する	tcp_wrapper
記録機能	セキュリティ監査証跡を作成する	アカウンティング
	監査記録へのアクセスを検知する機構を設定する	アカウンティング
ウイルス対策	ウイルスチェッカを定期的に起動する	ウイルスチェッカ
デーモンへの攻撃	デーモン起動機構を定期的にチェックする	COPS
特権ユーザの保護	特権ユーザとして直接ログインできないように制御する	/etc/password, /etc/group
監査プログラムの実施	定期的に監査プログラムを使用する	COPS

(1) ポリシー・設定対象マッピング機能
本機能は、セキュリティポリシーと設定対象の対応付けを行うことにより、設定項目の抜け漏れを防止するものである。
例えば Web サーバに対するセキュリティポリシーと設定対象のマッピングは表 1 のようになる。

(2) 設定・診断マッピング機能
本機能は、設定項目と診断項目の対応付けを行うことにより、上記のセキュリティパラメータの検査の抜け漏れを防止するものである。本機能により、セキュリティ診断ツールが使用する診断項目一覧ファイルを作成する。

また、構築フェーズにおいて、ポリシー作成支援ツールの出力を用いて抜け漏れない検査を実施するため、セキュリティ診断ツールには以下の機能を追加することにした。

(3) バッチ診断機能
本機能は、ポリシー作成支援ツールにより各対象サーバごとに作成した診断項目一覧ファイルを読み込み、その項目に対する検査を実施するものである。

3.2.構築-運用フェーズ連携機能

運用フェーズでは、セキュリティバグの影響を受ける可能性がある管理対象サーバを早急に見つけ出す手段を提供することが必要であると考えている。これを可能にするため、セキュリティ診断ツールに以下の機能を追加することにした。

(4) 稼動環境情報収集機能
本機能は、管理対象サーバから稼動中のソフトウェアの種別、バージョンや、使用する設定ファイル等の環境情報を収集するものである。本機能を用いてサーバの最新の環境情報を収集・管理しておき、セキュリティバグが発覚した時点でその情報を照会することにより、サーバがセキュリティバグの影響を受ける可能性があることを判断することが可能になる。

(5) セキュリティ再診断機能
本機能は、発覚したセキュリティバグに対する検査をリモートから行い、セキュリティ診断結果を出力するものである。本機能を用いることにより、セキュリティバグの影響があるサーバを確認することが可能になる。

また、運用フェーズにおいて、セキュリティバグの影響を受ける管理対象に対しては、セキュリティ診断を実施すると共に、ソフトウェアの設定変更やバージョンアップを行う手段を提供することが必要であると考えている。これを可能にするため、セキュリティ運用ツールに以下の機能を追加することにした。

(6) リモート設定変更機能
本機能は、セキュリティバグの影響があることが判明したサーバに対して、設定変更やバージョンアップをリモートから行えるようにするものである。

3.3.システム動作フロー

統合セキュリティ運用管理システムは、以上の機能を追加することにより、システムのライフサイクル全体に対するセキュリティ運用管理を図 2に示すような流れで実施できるようにすることを目指している。

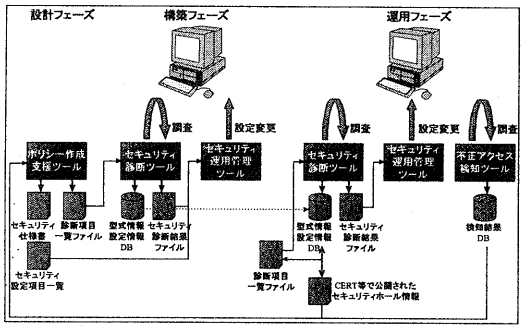

図2. ライフサイクル全体に対するセキュリティ運用管理の流れ

・設計フェーズ

ポリシー作成支援ツールにより、セキュリティポリシーの原案を作成すると共に、セキュリティ設定項目一覧および、診断項目一覧ファイルを出力する。

・構築フェーズ

設計フェーズで作成したセキュリティ設定項目一覧を用いて設定を行うと共に、診断項目一覧ファイルを用いてセキュリティ診断ツールでセキュリティ診断を行う。

・運用フェーズ

管理対象サーバの稼働環境を定期的に把握し、セキュリティバグが発覚した時点で、影響が発生するサーバの切り分け、診断を行うと共に、問題があった場合にはソフトウェアのバージョンアップや設定変更を行う。

また、不正アクセスの検知を行い、不審な事象を検知した場合にはソフトウェアの設定を変更する。

なお、その他のセキュリティ運用管理ツール間の連動機能として、運用-設計フェーズ連携機能が考えられる。この機能により、運用時の知見を新規システム等のセキュリティポリシーに反映させることが可能となる。本機能については現在、実現方式の検討を進めている状況である。

4. まとめと今後の課題

本稿では、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ため、従来の設計、構築、運用フェーズのセキュリティ管理ツールに新たな機能として、設計-構築フェーズ連携機能と、構築-運用フェーズ連携機能を付け加えるた“統合セキュリティ運用管理システム”を提案した。これらの機能を追加することにより、(1) 設計フェーズで策定したセキュリティポリシーを、構築フェーズにおいてセキュリティ設定として直接反映させること、(2) 運用フェーズにおいては、各ユーザの環境に応じたセキュリティ管理を実施し、発覚したセキュリティバグを早急に対策するための枠組みを整えることができるようになると考えている。

今後は具体的にプロトタイプを開発し、実フィールド上でその有効性を検証することが必要であると考える。

参考文献

[1] COMMON CRITERIA PROJECT, http://csrc.nist.gov/cc/

[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] SATAN, http://ftp.cerias.purdue.edu/pub/tools/unix/scanners/satan/

[4] COPS, http://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops/

[5] オープンベンダ不正アクセス対策システムにおける統合フレームワークの提案，鳥居他，CSS'99，1999.10

[6] ssh, http://www.ssh.org/