社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (77)
2007－CSEC－ 36 (77)
2007／3／2

情報セキュリティマネジメントのIT化による セキュリティレベルの維持とPDCAサイクルの実現

國分 俊介† 今井 功† 相浦 利治†
†三菱電機株式会社 情報技術総合研究所

企業や団体における情報セキュリティ対策としてセキュリティツールの導入や、情報セキュリティマネジメントシステムの実施などが行われているが、管理対象となるIT機器に対する専門性の確保や、分散環境における維持管理作業、新たに報告されるセキュリティ脅威への対応などに課題がある。本稿では、管理対象IT機器に対してセキュリティ設定の一貫性を確保すると共に、新たに報告されるセキュリティ脅威に対する現状システムの脆弱性分析作業を自動化するセキュリティ運用管理システムを提案する。

Maintenance of a security level and realization of a PDCA cycle by IT of information security management.

Shunsuke KOKUBU,† Isao IMAI,† and Toshiharu AIURA†
†Information Technology R&D Center, Mitsubishi Electric Corporation.

A countermeasure for security threats in a company becomes more and more important. Therefore we introduce security tools and deploy information security management system. Although we make such efforts, we still have following issues such as how to keep expert knowledge for IT system, how to maintain distributed system, how to cope with new kind security threats persistently. In this report, we suggest security operation management system that automates vulnerability analysis for current system facing security threats dynamically all the time and also enables governance of system security.

1. はじめに

企業や団体における情報セキュリティ対策として、組織のセキュリティ運用規則の策定と、規則に基づいたIT機器に対する管理(セキュリティツールの導入、セキュリティ設定など)を行わなければならない。しかし、管理対象となるIT機器は数、種類とも多く、正しくセキュリティ設定を行うためには機器に対する専門的な知識が必要となる。また、利用者毎に提供されているPC (Personal Computer) は、新規導入、廃棄、持出、修理後の再初期化などが日々行われており、変化に追従したセキュリティ設定管理が求められる。さらに、OSやアプリケーションのセキュリティホールの検出と、対応するパッチの提供、新たなウィルスの出現など、最新の脅威に関する情報収集と対策の適用が必要となる。

我々は、前述したセキュリティ運用管理に対する課題に関して、ITによる支援システムの開発（参考文献[1]）を行っており、本稿では、管理対象IT機器に対するセキュリティ対策の徹底を行うとともに、外部から報告されるセキュリティ脅威に対する現状システムの脆弱性分析作業を自動化するシステムを提案する。2章では本システムの開発に至った背景とセキュリティ運用管理の課題を示す。3章では本システムの構成と目標とする機能の概要について示す。4章では各機能の実現方法を示し、5章にてIT化の有効性に対する考察と今後の課題について示す。

2. 背景と課題

2.1 セキュリティ運用の課題

PCの普及やインターネットによる情報流通の利便性が向上する一方、個人情報保護法の全面施行（2005年4月）や、機密情報の漏洩による賠償問題など、企業や団体におけるセキュリティ対策はますます重要になってきている。主要なセキュリティ対策として、PCへのセキュリティツールの導入や、情報セキュリティマネジメントシステムISMS（Information Security Management System）の実施などが行われている（参考文献[2]）が、セキュリティ運用の現場では以下のような課題が報告されている。

(1) セキュリティ規則に基づいたツールやIT機器に対する設定
一般的に規定されているセキュリティ規則では、ツールやIT機器の設定を導出するために曖昧部

分が存在する。また、暗号化、外部媒体へのアクセス制御、ログ収集など様々なセキュリティツールや、PC、サーバ、ネットワークなどのIT機器に対する専門性が求められるため、現場での作業に限界がある。

(2) 大量に展開したIT機器（特にPC）に対するセキュリティレベルの維持
一般的なオフィス環境では一人に1台のPCが整備され、セキュリティ設定を含めた管理も利用者に任されている。新規導入、廃棄、持出、修理後の再インストールなどは日常的に行われているため、セキュリティレベルの維持といった観点ではリアルタイムに近いレベルでの監視を行うべきであるが、確認作業のための人員の確保やそのコストを考えた場合、現実的ではない。

(3) 新規に報告されるセキュリティ上の脅威や脆弱性情報の収集と対策に向けた評価
新たな脆弱性やウィルスの出現など、IT機器に搭載されるソフトウェア（OS、アプリケーション）を取り巻く環境は、常に動的に変化している。IT機器を保有する組織は、IT機器に対する安全性を確保する為、脆弱性の確認とセキュリティ対策の実施について継続的なリスク管理のための枠組みが必要である。

2.2 課題に対する現状の取組み

前節にて示した課題に対して、IT機器のセキュリティ設定については、現状ではツールのヘルプ機能や説明書の充実程度で、有効な対策は存在せず、現場の判断で決められているケースが多い。また、セキュリティレベルの維持については、規則の実施状況を確認するチェックリストや管理台帳の整備といった対策が取られるが、実際の作業は各機器の利用者に任されており、管理作業の負担によるルールの形骸化が発生する恐れがある。セキュリティレベルを維持するため、定期的なセキュリティ監査が行われ、形骸化防止やセキュリティ対策の最新化に効果を上げているが、業務への影響を考慮すると数ヶ月に1回程度の頻度となる。また、監査以降に実施されたセキュリティ規則の変更や、新たな脅威の出現に伴う設定値の最新化の指示が、IT機器へ反映されるか否かは機器の利用者に任されている。利用者の過失あるいは故意で、セキュリティ設定が最新化されない場合、該当機器がセキュリティホールとなり、情報漏洩やウィルス感染などのセキュリティ事故が発生する可能性がある。

また、新規のウィルス情報や情報システムに対するDoS（Denial of Services）攻撃といった不正アクセス等による新たな脆弱性情報は、例えば参考文献[3]に示す様な情報提供サイト等によって次々と公開される。このような脆弱性情報は、信頼できる情報や風潮デマといったものの類まで実に様々な情報がある。セキュリティ管理担当者は、IT機器の環境をセキュアな状態に保つ為に、上記の情報提供サイトを監視し信頼性の高い情報を常に把握する必要がある。更に、公開された脆弱性情報が管理対象のIT機器に該当する情報を分析しセキュリティ対策を検討するためには、脅威・脆弱性に対する専門的な知識を必要とすると共に、管理すべきシステムの規模に比例して作業コストが増大していく。従来から脆弱性診断ツール（参考文献[4]）によって個々のIT機器に対する脆弱性診断や、対策管理が行なわれてきた。しかしながら、脆弱性に対する対策の必要性の判断や、複数の脆弱性が発見された場合にどの脆弱性から優先的に対策を施さなければならないのか、また何時までにどのような手順で実施するべきか等といった事が考慮されていないといった問題がある。

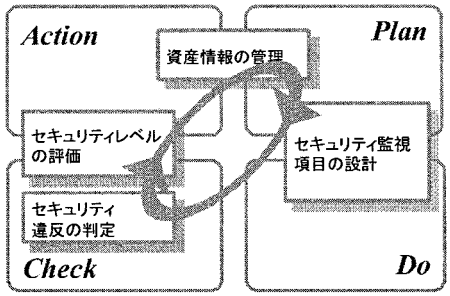

図1 PDCAサイクルのIT化の実現

3. セキュリティ運用管理システムの提案

本章では、前節で示した課題を解決するために、セキュリティ運用業務をIT化する上で求められる要件の整理、及び、要件を実現するセキュリティ運用管理システムの概要を示す。

3.1 システム要件とIT化方針

本稿で提案する運用管理システムは、前章で挙げたセキュリティ運用上の課題を解決することを目的とし、図1に示す通りセキュリティマネジメントにおけるPDCA（Plan-Do-Check-Action)の各サイクルを支援する為の機能を実現する。

前章にて示したセキュリティ運用の課題を元に整理したIT化の要件を以下に示す。

(1) IT機器に対するセキュリティ監視項目の設計簡単化
組織のセキュリティ規則に基づいたセキュリティ監視項目を設定可能であること。

(2) IT機器に対するセキュリティ設定状況の把握
(1)で設計したセキュリティ監視項目に応じたIT機器のセキュリティ設定状況が導出可能であること。また、導出するために必要な資産情報が管理されていること。さらに、設定したセキュリティ監視項目と比較することで、セキュリティ違反を

判定できること。

(3) IT機器に対するセキュリティレベルの評価
最新の脆弱性情報から管理対象のIT機器に対する影響度を分析評価できること。また、セキュリティ対策の必要性、具体的な対策方法及び対策期限（時期）を提示出来ること。

3.2 セキュリティ運用管理システムの構成

セキュリティ運用管理システムの構成図を図2に示す。本稿で提案するセキュリティ運用管理システムのポイントとなる機能を以下に示す。

- 機能1：セキュリティ監視項目の設計
- 機能2：資産情報の管理
- 機能3：セキュリティ違反の判定
- 機能4：セキュリティレベル評価

3.2.1 セキュリティ監視項目の設計

本機能では、組織内のセキュリティ規則をベースに、セキュリティ管理担当者がセキュリティ設計運用ツールを利用して、確認したいIT機器のセキュリティ設定項目とセキュリティ違反として判定する閾値を指定する。また、設計したセキュリティ監視項目を他組織内で運用しているセキュリティ運用管理システムで利用できるように、テンプレート化する。

3.2.2 資産情報の管理

本機能では、3.2.3項でのセキュリティ違反の判定を行う上でのベースとなるIT機器の情報（資産情報）を収集及び管理する。資産情報は定期的に収集される。資産情報としては、IT機器固有の情報（IPアドレス、MACアドレス、ホスト名等）やインストールされているOSの情報/ソフトウェア情報、各セキュリティツールの設定、資産管理者名、資産管理者所属、資産番号、資産価値等を含む。ここで、資産価値とは、IT機器の重要度をIT機器に含まれる情報資産をCIA（機密性、完全性、可用性）の観点でレベル付けしたものである。

3.2.3 セキュリティ違反の判定

本機能では、3.2.1項で設計したセキュリティ監視項目と3.2.2項で収集した資産情報をもとに、設計した値になっているか（もしくは設計した値の範囲内にあるか）を判定し、セキュリティ違反を検出する。判定結果は、セキュリティ設定運用ツールを通して、セキュリティ管理担当者へ報告する。また、判定結果を利用して、セキュリティレベル評価を行う。

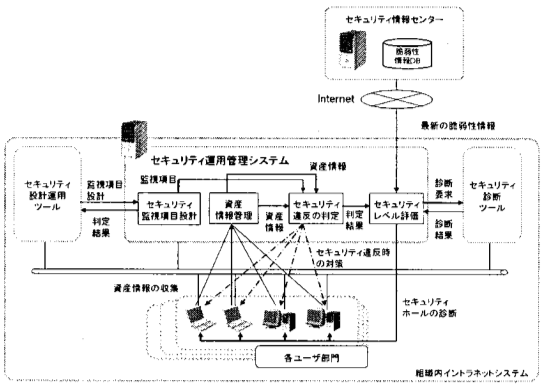

図2 セキュリティ運用管理システムの構成

3.2.4 セキュリティレベル評価

本機能では、各IT機器に対する脆弱性の影響度を分析評価し安全性の度合いを表現する手段として、各IT機器に対するリスク値を算出する。このリスク値により、どの脆弱性から、いつまでに、どのような手段をもって対策を取らなければならないか明確にする。

本機能では、セキュリティ情報センターから配信される最新の脆弱性情報を元に、3.2.2項で述べた資産情報により管理対象のIT機器への影響が考えられる脆弱性を絞り込む。そして、3.2.3項におけるセキュリティ違反の判定結果や、セキュリティ診断ツールによるセキュリティホールに対する脆弱性診断結果から、各IT機器のリスク値を算出する。

4. セキュリティ運用管理システムの実現方式

本章では、前章で示したセキュリティ運用管理システムを構成する各機能の実現方式について示す。

4.1 セキュリティ監視項目設計方式

IT機器のセキュリティ設定の監視を行うために、セキュリティ監視項目設計では、以下の項目を設定する。

(1) セキュリティ監視項目
監視を行う項目と本来のセキュリティ設定状態として正しい値（閾値）を設定する。監視項目の例を表1に示す。各監視項目にはそれぞれの情報をIT機器から収集するための情報収集プログラムが割り当てられている。

表1 セキュリティ監視項目例

ｸﾞﾙｰﾌﾟ	項目	概要
ｼｽﾃﾑ	OS名	指定のOSを利用する
	OSﾊﾞｰｼﾞｮﾝ	
	OSｻｰﾋﾞｽﾊﾟｯｸ	
	OSﾊﾟｯﾁﾘｽﾄ	指定のOSﾊﾟｯﾁを適用する
ﾊﾟｽﾜｰﾄﾞ	最小長	ﾊﾟｽﾜｰﾄﾞは一定長以上にする
	有効期間	ﾊﾟｽﾜｰﾄﾞは定期的に変更する
ｽｸﾘｰﾝｾｰﾊﾞ	有効	ｽｸﾘｰﾝｾｰﾊﾞを利用する
	ﾊﾟｽﾜｰﾄﾞ	ｽｸﾘｰﾝｾｰﾊﾞはﾊﾟｽﾜｰﾄﾞﾛｯｸを利用する
禁止ｿﾌﾄｳｪｱ	対象ﾘｽﾄ	対象ﾘｽﾄに挙げるｿﾌﾄｳｪｱの利用を禁止する
ﾌｧｲｱｳｫｰﾙ	有効	ﾌｧｲｱｳｫｰﾙを利用する
	許可ﾎﾟｰﾄ	許可ﾎﾟｰﾄ以外のﾎﾟｰﾄの開示を禁止する
ｳｨﾙｽ対策	有効	ｳｨﾙｽ対策ｿﾌﾄｳｪｱを利用する
	自動ｱｯﾌﾟﾃﾞｰﾄ	自動ｱｯﾌﾟﾃﾞｰﾄ機能を利用する
暗号化ｿﾌﾄｳｪｱ	有効	暗号化ｿﾌﾄｳｪｱを利用する
	ﾊﾞｰｼﾞｮﾝ	暗号化ｿﾌﾄｳｪｱは指定のﾊﾞｰｼﾞｮﾝを利用する
…	…	…

(2) セキュリティ違反検出時の対策
(1)で設定した値（閾値）を越えた場合（または、設定した値に反する場合）の対策動作を設定する。動作例としては、何もしない、メール送付、ソフトウェアのインストール等である。

(3) セキュリティ違反判定の周期
(1)で設定したセキュリティ監視項目に関して、セキュリティ違反を判定する周期を設定する。

(4) 対象のIT機器情報
セキュリティ違反の判定を行う対象のIT機器を指定する。

(5) 監視するセキュリティ設定に該当する企業内セキュリティ規則情報
(1)で設定したセキュリティ監視項目に対応する企業内のセキュリティ規則を設定する。本項目を設定することで、監視結果を参照する際に、どのセキュリティ規則に該当した違反検出結果なのかを把握することができる。経営者に対して詳細なセキュリティ設定情報を報告しても、それが是正処置の対象かどうかを判断することは困難である。本項目を設定することで、セキュリティ規則に沿った報告を行うことが可能となり、経営的判断に基づく対策の導出を支援する。

上記(1)から(5)の項目をセキュリティ設計運用ツール（図3参照）より設定し、4.3節のセキュリティ違反判定方式においてセキュリティ違反を検出する。

また、設計したセキュリティ監視項目は、他組織内で稼動しているセキュリティ運用管理システムで使用できるように、テンプレート化を可能としている。通常、企業内では上位のセキュリティ管理組織がセキュリティ規則を策定し、標準的なセキュリティ対策手順を作成した後、各組織に展開・セキュリティ規則遵守徹底を指示する。展開先の各組織では、上位のセキュリティ管理組織が作成した対策手順をそのまま利用するか、展開されたセキュリティ対策手順をもとに、自らの組織に合わせて修正する。本テンプレートに、IT機器に対するセキュリティ設定値を含めて配布することで、現場スタッフの能力に依存しない一貫性の在るセキュリティレベルの確保が可能となる。これにより、展開先の各組織はテンプレートを適用する、もしくは、組織内の実情に合わせた部分的な修正を行うのみでよい。

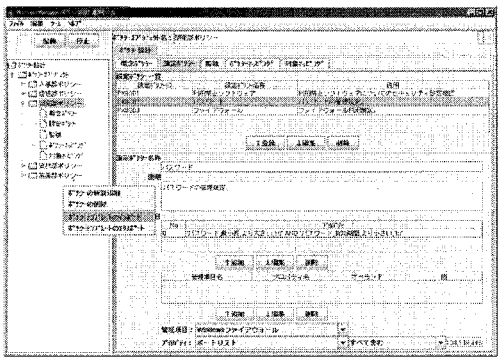

図3 セキュリティ設計運用ツール

4.2 資産情報管理方式

本セキュリティ運用管理システムでは、4.3節のセキュリティ違反の判定や4.4節のセキュリティレベル評価のリスク値算出のために資産情報を利用する。そのため、本システムは以下の資産情報を管理する。

- IT機器固有の情報（IPアドレス、ホスト名、等）
- インストールされているOS情報、OSパッチ情報、ソフトウェア情報
- セキュリティツールの設定情報
- 資産管理者名、資産管理者所属、資産番号、資産価値

資産情報は、4.1節のセキュリティ監視項目に対応した情報収集プログラムや既製の資産管理ツール等により、定期的に収集される。管理対象IT機器上での情報収集プログラムの実行制御は、市販の資産管理ツール等から可能としている。

4.3 セキュリティ違反判定方式

4.1節で設計されたセキュリティ監視項目の値（閾値）と4.2節で収集された資産情報をもとに、セキュリティ運用管理システムは、セキュリティ違反を判定する。判定の流れは以下の通りである。

(1) 4.1節(3)で定義した時刻になると、4.1節(4)で定義した対象IT機器情報をもとに、セキュリティ違反の判定を行う対象IT機器に関する資産情報を抽出する。

(2) 選択した資産情報の中から、4.1節(1)で定義した項目と値を抽出する。

(3) 抽出した値に関して、4.1節(1)で定義したセキュリティ監視項目の値と比較する。

(4) 4.1節(1)で定義したセキュリティ監視項目の値に反する場合は、セキュリティ違反として検出し、4.1節(2)で定義したセキュリティ違反検出時の対策動作を実行する。対策動作は4.2節の情報収集プログラムと同様に、市販の資産管理ツール等から可能としている。

(5) セキュリティ違反判定結果（セキュリティ違反有り/無し）は4.1節(5)の企業内セキュリティ規則と合わせてデータベースで管理し、セキュリティ設定運用ツールを通してセキュリティ管理担当者に報告される。

表 2 脅威に関する情報

項目	内容
攻撃の種類	脆弱性の利用(悪用)の方法。 (ex.リモート／ローカル等)
攻撃のインパクト	脆弱性の種類（ex.クロスサイトスクリプティング）と発生時に想定される影響度
攻撃コードの有無	脆弱性を突くために開発し公開プログラムコード。

表 3 脆弱性に関する情報

項目	内容
公開パッチの有無	攻撃コードに対応する修正プログラムの公開の有無
回避策の有無	公開パッチが無い場合に、当面に回避策(ex.ポートの閉鎖等)の有無
危険度	脆弱性に対する対策実施のための緊急性の度合い

4.4 セキュリティレベル評価方式

セキュリティレベル評価では、以下の手順で管理対象の IT 機器から必要な情報を収集し、分析評価を行う。

(1) 最新の脆弱性情報の収集
本稿で提案するセキュリティ運用管理システムでは、インターネット上で公開される最新の脆弱性情報を収集する手段として、榊原等が開発したセキュリティ情報センター(参考文献[5])を利用する。同センターでは、OS/Web サーバ/ブラウザ等のソフトウェアに関する脆弱性情報を複数の情報提供サイトから効率よく収集し、表 2 及び表 3 に示す脅威・脆弱性に関する情報を分析している。

(2) 脆弱性確認対象候補の抽出
4.2 節で述べた資産情報管理機能から、管理対象の IT 機器の識別情報、資産価値、及びインベントリ情報等を取得する。取得されたインベントリ情報と上記(1)で収集した脆弱性情報を分析することにより、管理対象の IT 機器への確認対象となる脆弱性情報を絞り込む。

(3) 脆弱性有無の確認
上記(2)で絞り込まれた脆弱性情報に対し、実際に各 IT 機器に脆弱性が有るかを検査する。検査方法としては 2 通りの手段がある。1 つは、脆弱性に対応するパッチの適用状況により脆弱性の有無を確認する方法であり、もう 1 つは、既知のセキュリティホール(クロスサイトスクリプティング、DoS 攻撃等)に対する診断により脆弱性の有無を確認する方法である。前者は、4.3 節のセキュリティ設定判定機能から得られる結果であり、IT機器内部に対する検査である。一方、後者はセキュリティ診断ツールとの連携により得られる結果であり、IT 機器に対する外部からの検査方法である。

(4) リスク値の算出
管理対象の IT 機器に対するリスク値を算出する。リスク値算出の基本的な考え方は、資産価値、脅威、脆弱性の組み合わせにより求める方式である。本機能では、脅威や脆弱性の要素を細分化することにより、リスク値の精度を向上させる。本機能では、リスク値算出のため、上記(1)～(3)までの結果から得られた資産価値、脅威（表 2）、及び脆弱性（表 3）の各情報（パラメータ）に対し予め数値を設定しておく。参考文献[4]においても、同様の要素を元にリスク値を算出しているが、本方式では、上記(3)の結果から脆弱性の有無を確認する事により、脆弱性に対する対応状況や改善レベルを分析し、リスク値算出のために要素に含めた。また、各機器に対する脆弱性情報は、必ずしも 1 つとは限らない。そのために、上記により個々の脆弱性に対するリスク値を算出した後、総和を求めることにより機器単位のリスクを導出すると共に、算出された全対象機器のリスク値を脆弱性の種別にまとめることにより、全体としてどの脆弱性が、どの程度、IT 機器に影響を与えているかを算出する。

(5) リスク値算出結果とセキュリティ対策の提示
上記のリスク値算出結果と、検出された脆弱性に対するセキュリティ対策結果を提示する。評価結果の一例を図 4 に示す。評価結果では、各脆弱性に対して、影響範囲として脆弱性が確認された機器の台数、リスク値、脆弱性に対する対策方法を優先度の高い順に提示している。

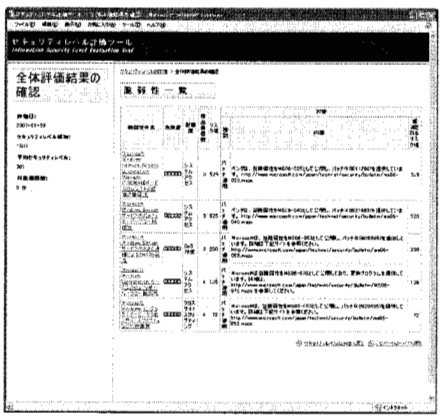

図 4 セキュリティレベルの評価結果例

5. まとめと今後の課題

本セキュリティ運用管理システムを用いることで、以下の効果を見込むことができる。

(1) セキュリティ運用の完全性向上
本システムを用いることで、セキュリティ設定確認作業が自動化されるため、確認作業としての曖昧性を排除することができる。また、企業内のセキュリティ規則とセキュリティ監視項目を関連付けて管理することで、IT機器に対する専門知識を有しない対象者に対してもセキュリティ違反を容易に把握できる。さらに、リスクの数値化により、現状のセキュリティレベルが視覚的に把握できるため、セキュリティ運用の完全性が向上する。

(2) 運用管理負荷の軽減
本システムを用いることで、セキュリティ管理担当者もしくはIT機器の所有者がこれまで行っていたセキュリティ設定確認作業を自動化することができる。また、各組織へのセキュリティ監視項目もテンプレートとして展開することができる。これらにより、セキュリティ運用負荷を軽減することが可能となる。

(3) 脆弱性情報の収集から対策提示のための継続的な支援
本システムでは、セキュリティ情報センターとの連携により、常に最新の脆弱性情報を継続的に収集すると共に、セキュリティレベルの評価によるIT機器への脆弱性の発見、優先的な対策提示を継続的に支援することを可能とした。

今後の課題としては以下が挙げられる。

- 今回提案したシステムで用いたセキュリティ規則のテンプレートは、一般的なガイドラインなどを参考に作成した。しかしながら、様々な組織に対応できる汎用的なテンプレートの作成までは至っていない。また、管理対象IT機器のレパートリ拡大や、新たに開発されたIT機器にも対応できる拡張性を実現する必要がある。
- セキュリティレベル評価では、検出された脆弱性の影響範囲や対策のための優先順位については実現できたが、対策の実施時期や期限といった時間的な問題やネットワークシステムを考慮した場合の脆弱性診断や対策提示について検討する必要がある。

6. おわりに

本稿では、企業内におけるセキュリティ対策の実施状況や報告された脆弱性に対する脅威、改善すべき項目等を把握する支援を行うセキュリティ運用管理システムを提案した。今後は、上記課題に対して検討を進める予定である。

参考文献

[1] 國分、他：情報セキュリティガバナンス確立に向けたセキュリティ運用の自動化、電子情報通信学会 2006 総合大会講演論文集、A-7-16、2006

[2] 日本規格協会：JIS Q 27001:2006（ISO/IEC 27001:2005）情報セキュリティマネジメントシステム－要求事項、2006

[3] Bugtraq、 http://www.securityfocus.com

[4] マルクーア、他：ネットワーク脆弱性の検出および報告のためのシステムならびに方法，公表特許公報、特表 2005-515541、2005

[5] 榊原、他：セキュリティ情報センターの開発、情処理学会第 67 回全国大会講演論文集、2D-4、2005