M-100

セキュリティ対策進捗管理システムの提案

Proposal of Security Update Progress Manager

礒川　弘実†　　萱島　信†
Hiromi Isokawa　Makoto Kayashima

1．まえがき

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インフラとなるに伴い，不正アクセスやワームなどの攻撃の影響が，より広範囲で深刻なものとなっている。実際，Code Red や Nimda ワームの感染により，サーバやネットワークの負荷が増大し，イントラネットが一時不通になるような事態も発生している。

このような被害を防ぐためには，情報システムの設計，構築，運用というライフサイクル全体を体系的に管理し，効率的かつ効果的なセキュリティ対策を行うことが必要となる[1]。特に，新たに発見されたセキュリティホールに対するパッチの適用など，運用フェーズにおけるセキュリティ対策作業は，攻撃ツールが早い段階で開発・公開されることもあるため，迅速かつ的確に実施する必要がある。また，イントラネット内に一部でも弱い箇所があると全体へも悪影響を与えてしまうため，セキュリティ対策はイントラネット全体で抜け漏れなく実施することが重要である。

現状セキュリティ対策は，実施すべき作業項目や対象計算機が多いため，複数の管理者が分担して行うことが多い。そのため，イントラネット全体で対策をフォローしていくためには，各管理者の進捗をイントラネット全体で集計することが必要となる。また，複数の事業所にまたがって進捗把握を行っている場合にも，早期に対策漏れを発見したり，対策が遅延している管理者にフォローするための環境整備に対するニーズは高い。

そこで，イントラネット全体の対策進捗管理とフォローを支援し，セキュリティ対策を抜け漏れ無く行えるように運用フェーズの管理を行う「セキュリティ対策進捗管理システム」の検討および開発を行った。本稿では，本システムのコンセプト提案と，プロトタイプの開発報告を行う。

2．セキュリティ対策進捗管理システムのコンセプト

2.1　目的と課題

セキュリティ対策進捗管理システム(Security Update Progress manager，以下 SUP と略す)の目的は，イントラネット全体でのセキュリティ対策作業(パッチの適用など)の進捗管理と，未対策のサイトや計算機に対する適切な対策フォローの実施を可能にすることである。SUP の実現に向けては，開発時，構築時，運用時の有効性確保やコスト抑制のために，下記の課題を解決する必要がある。

(1)新規セキュリティ項目への迅速な対応

新たなホールへの対策など新規の作業項目を迅速に進捗管理の対象にする。また，作業内容が変更となった場合には即座に追従することで，作業内容を最新に保つ。

(2)管理者階層への対応

管理者はその役割に応じて，「ある事業所のメールサーバの担当管理者」「事業所全体を管理する管理者」「複数事業所からなるイントラネット全体を統括する統合管理者」など，階層化されている。各階層の管理者毎に有用な管理機能を提供する必要がある[2]。

(3)対策作業項目毎及び計算機毎の進捗管理

管理者は，危険度大のホールへの対策など，特定の対策作業項目の進捗状況を見ながら適宜対処する必要があるため，例えば Code Red 対策状況はどうかなど対策作業項目毎に進捗を把握可能とする。また，対策は計算機単位で行うため，計算機単位の進捗管理も可能とする。

(4)セキュリティの確保

SUP が提供する進捗情報は，未対策ホールがある計算機など計算機の脆弱性状況に関する情報を含むため，他者への漏洩を防止する必要がある。

(5)対策の要請

適宜必要に応じて管理者に対策の要請(フォロー)を行う。

(6)ランニングコストの抑制

SUP を運用するために必要なコストを抑制にする。

3.2　実現方式

前節で述べた課題に対する解決策を下記に夫々示す。

(1)セキュリティ情報提供 Web サイトとの連携

新たなホール情報や対策すべき情報は，JPCERT など多くの Web サイトにて，発見され次第早急に提供されている。SUP ではこのような Web サイトを頻繁に調査し，SUP の管理する対策作業項目との情報の整合性を保つことで、新規セキュリティ項目への迅速な対応を実現する。

(2)一般管理者と統括管理者毎の管理機能提供

SUP では，管理者階層として，サイト毎の一般サイト管理者とイントラネット全体を統括管理する統合管理者を設定可能とする。一般管理者には，担当計算機に対する進捗管理機能を提供し，統括管理者には，イントラネット全体の進捗管理機能と対策フォロー機能を提供する。

(3)対策作業項目毎及び計算機毎の管理機能提供

対策作業と計算機毎に進捗状況を保存することとし，下記の状況をそれぞれ把握できる機能を提供することで，対策作業項目毎及び計算機毎の進捗管理を可能とする。

(a) 対策作業項目別進捗：対策作業項目毎に，未対策の計算機一覧と，対策済/対策中/未対策の台数/割合一覧を提供する。
(b) 計算機別進捗：サイト計算機毎に，未対策の作業項目一覧と，対策済/対策中/未対策の項目数/割合の一覧を提供する。

(4)管理者毎のアクセス制御

サイトの進捗情報は該当サイト管理者のみが，イントラネット全体の進捗情報は統合管理者のみが入手可能となるようにユーザ認証，暗号化を行う。

(5)メールによる対策要請

定期的に対策状況を調査し，一定時間以上未対策のまま放置されている場合には，該当サイト管理者に対策の要請メールを送信する。

(6)Web ページ上での進捗入力，定期作業の自動化

進捗入力は，サイト管理者が Web 上の簡単操作で容易に入力可能とする。また，Web サイト情報収集，進捗レポート作成，対策要請メール送信は定期的に自動で実行することで，ランニングコストを抑制する。

† （株）日立製作所　システム開発研究所

3．プロトタイプシステムの開発

3.1 概要

開発したSUPプロトタイプのシステム構成を，図1に示す。SUPは，社内の不正アクセス対応機関HIRT(Hitachi Incident Responce Team) [3]の提供するセキュリティ情報提供Webサイトを定期的に調査し，新規の作業項目があった場合には，作業項目DBに追加し進捗管理の対象とする。また，対策進捗の入力や進捗状況の確認を行うWebインターフェースをサイト管理者や統合管理者に提供する。さらに，適宜サイト管理者へ対策要請メールを送信する。

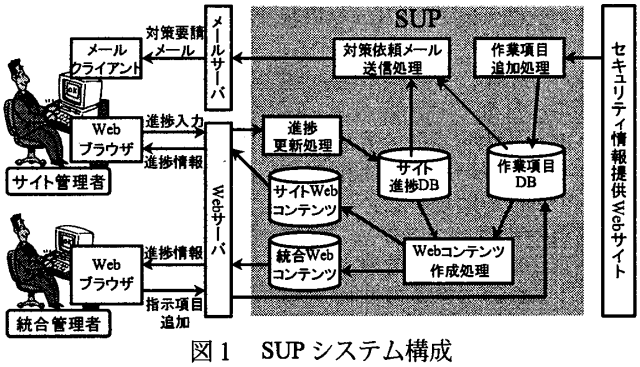

図1　SUPシステム構成

4.2 機能

(1)セキュリティ対策進捗レポート作成機能

サイト進捗DBの内容から，サイトや計算機毎の進捗状況をまとめレポート化する。進捗状態の種別を表1に示す。

表1　進捗種別リスト

分類	種別	説明
未対策	未登録	進捗状況がSUPに登録されていない状態。新規に追加された作業項目は，最初全てこの状態となる。
	未対策	対策がなされていない状態
対策中	対策中	対策を実施中である状態
	再対策中	一旦対策完了としたが，不具合があり再度対策を行っている状態
	対策中(ベンダ対応待ち)	ベンダの対応(対策ソフトの開発など)を待っている状態
対策完	対策不要と判断	対策の対象外として対策を不要と判断した状態
	対策完了	対策を完了した状態

(2)進捗レポート提供Webインターフェース機能

作成した進捗レポートは，Web画面上で各サイト管理者，統合管理者毎にそれぞれ提供する。例を図2に示す。

(3)対策要請メール送信機能

作業項目が追加された時や，作業項目が一定時間以上未対策/対策中の状態である時に，サイト管理者向けに対策実施の要請をメールで送信する。メール例を下記に示す。

Subject: [SUP] Security Update Follow(02/26,00:05)

セキュリティ対策進捗管理システム(SUP)より、セキュリティ対策のお願いです。下記項目対策を早急にお願いします。
<項目ID>:<対象ホスト>(状況)
・HIRT-01013：server1(未対策[再フォロー])
server2(対策中[予定日付=2月21日])
・HIRT-01017：server1(対策中[予定日付=2月21日])
必要なセキュリティ対策を実施した後、進捗管理システムにて必ず御報告願います。 http://sup.domain.co.jp /index.html

(4)進捗情報変更Webインターフェース機能

作業項目に対する進捗状況をサイト管理者が入力するためのWebページを提供するものである。進捗登録ページの例を，図3に示す。本ページにて，左フレームで指示項目を選択し，右フレームにて進捗選択を行う。

5．まとめと今後の課題

セキュリティ対策の抜け漏れ防止のため，イントラネット全体の対策状況の把握と対策フォローを支援する「セキュリティ対策進捗管理システム」を検討し，プロトタイプを開発した。今後は，下記課題に取り組む予定である。

(1)複数のセキュリティ情報提供Webサイトとの連携

現状では，セキュリティ情報を1つのWebサイト(社内HIRTサイト)からのみ収集しているが，情報の網羅性確保の為に，複数のWebサイトからの収集を可能にする。

(2)脆弱性検査ツールとの連携

サイト管理者による進捗入力作業の更なる効率化のため，脆弱性検査ツールと連携し，診断結果による進捗の自動登録を一部可能とする。

参考文献

[1] 萱島信他：統合セキュリティ運用管理システムの提案，情報処理学会研究報告 2000-CSEC-11，pp.85-90，Sep. 2000.
[2] 磯川弘実他：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，情報処理学会研究報告 2000-CSEC-7，pp.7-12，Jan. 2002.
[3] 寺田真敏他：企業内不正アクセス対策情報サービスシステムの構築，情報処理学会論文誌 Vol.41 No.8，pp.2246-2253，Aug. 2000.

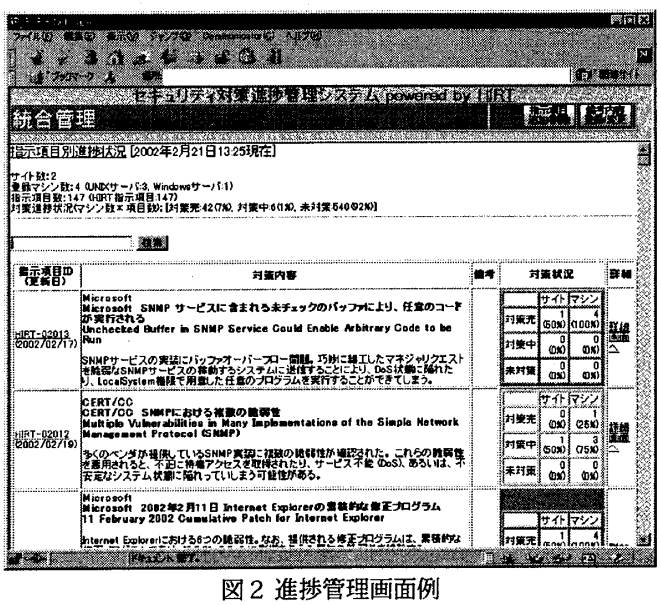

図2 進捗管理画面例

図3 進捗入力画面例