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

2006－DPS－126（23）
2006－CSEC－32（23）
2006／3／16

セキュアなイントラネット運用を目的とするネットワーク運用支援システムの提案

畑田 充弘　NTT コミュニケーションズ㈱
仲小路 博史　㈱日立製作所
山形 昌也　日本電気㈱

企業ネットワークを代表とするイントラネットでは，支店や部門単位のネットワークであるサイトが相互に接続されており，その特性からセキュリティ管理上の様々な課題が存在する．本稿では，その解決策の一つとして，サイトの脆弱性と脅威を定量評価し，サイト間で共有することにより，セキュアなイントラネット運用を実現するネットワーク運用支援システムを提案する．

Proposal of Network Operation Support System for Secure Intranet Operation

Mitsuhiro HATADA　NTT Communications Corporation
Hirofumi NAKAKOJI　Hitachi, Ltd.
Masaya YAMAGATA　NEC Corporation

In Intranet such as a corporate network, the site that is the network of the branch and each section is connected mutually, and various problems in the security management exist. In this paper, as one of the solutions, we propose the network operation support system that achieves secure Intranet operation by sharing the quantity evaluation of the vulnerability and the threat of the site between sites.

1. はじめに

近年，企業におけるセキュリティ対策が進められている一方で，セキュリティ被害や事故が後を絶たない状況にある．このため，セキュリティレベルを維持，向上するための継続的なセキュリティ対策や，緊急対応策などの実施の必要性が増してきている．また，対策に伴う管理負荷の軽減も求められている．

本稿では，企業ネットワークを代表とするイントラネットの実態を踏まえて，セキュリティ対策上の課題を述べる．各課題における対策方針をもとに，セキュアなイントラネット運用を目的とするネットワーク運用支援システムを提案する．

2. 背景

イントラネットのセキュリティ対策として，インターネットからの脅威を最小限に抑えることを目的に，ゲートウェイ対策はクローズドポリシーで運用されてきた．具体的には，ファイアウォールを用いて，企業のセキュリティポリシーに準拠したプロトコル（HTTP や SMTP など）だけに通信を絞り込むといった運用が挙げられる．一方，イントラネット内の対策は，ネットワーク自体が可用性や拡張性を追及して発展しており[1]，そのために IP ネットワーク上で動作する様々なアプリケーションの接続性に重点が置かれた結果，オープンポリシーに基づく運用が一般化した．（図 1）

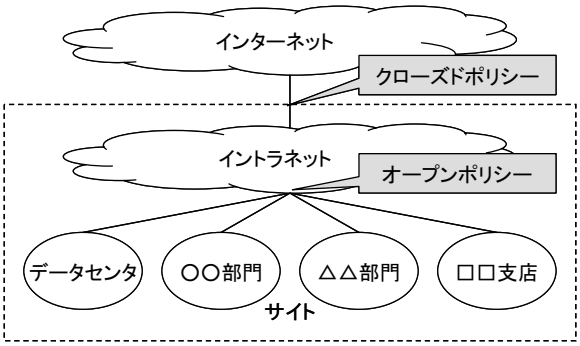

図 1 企業ネットワークの構成と接続ポリシー

3. 課題と対策方針

イントラネットはオープンポリシーであったが故に，多種多様な OS やアプリケーションが混在する複雑なネットワークとなった．また，企業において部門や支店単位のネットワークであるサイトは地理的に分散していることが多く，個々のサイトのセキュリティ管理者は管理権限こそ有しているものの，技術面に関して不慣れな人員が多いのが実情である．このような状況を踏まえ，セキュアなイントラネットの運用を実現するために３つの課題を提起する．

サイトを新たに接続する場合，そのサイトが企業のセキュリティポリシーに準拠しているか否かといった形式的な要件に基づいており，接続後もサイトが危険であるか否かの判別がつかない．これらの実情を踏まえ，１つ目の課題として，ネットワーク接続の可否を判断することが可能な，セキュリティ上のリスクを計る指標を作成する．詳細は 3.1 で述べる．

現状のイントラネットでは深刻な脆弱性を保有する大半のノードに対してパッチを適用するのに，ある程度の期間を要することが報告されている[2]．加えて，フィッシングやスパイウェアなど侵害手段も巧妙になってきており，対策も後手にならざるを得ない状況である．そこで，2 つ目の課題として，日常的な予防や早期警戒あるいは緊急措置を行っていくために，各サイトの脆弱性や脅威の動向など様々なセキュリティ情報を管理し，効果的に利用する仕組みを作成する．詳細は 3.2 で述べる．

最後に，具体的な対策手段を分析し，実施することが 3 つ目の課題であり，3.3 で詳細を述べる．

3.1. ネットワーク接続可否の判断指標

一般的にセキュリティリスクは「情報資産」「脆弱性」「脅威」の３つの要素の積で表される．本稿では，サーバや PC などのノードを情報資産として，OS やアプリケーションの脆弱性と，それらの脆弱性を悪用する脅威を対象とする．

脆弱性の指標として，CVSS（Common Vulnerability Scoring System）[3]では個別の脆弱性の数値化モデルを提案している．また，nCircle IP360[4]では個別の脆弱性の数値化モデルに加えて，脆弱性毎の数値の総和によりネットワーク単位での脆弱性の指標化を行っている．一方，脅威の指標として，ALERTCON[5]や ThreatCon[6]などが公知である．しかし，両者ともインターネット全般の傾向を表したものであり，算出方法は非公開である．

多種多様な脆弱性が日々新たに発見され，脆弱性を悪用する攻撃手法も複雑化する中で，サイトのセキュリティ管理者が日常的にセキュリティ管理状況を把握し，ネットワーク接続可否の判断を行うことは現実的に困難であるため，判断指標となる理解しやすい定量値を算出するモデルが必要となる．そこで，サイトに内在する脆弱性と，サイトが実際に受けている脅威をもとに，脆弱性レベルと脅威レベルという定量値を算出する．算出のための客観的な情報源として，脆弱性はセキュリティ監査などで利用される脆弱性スキャナを用い，脅威は不正アクセス監視に利用されている IDS を用いて，

それぞれ情報収集を行う.

各サイトのセキュリティ管理者がレベルを見た際に,リスク状況を把握し易くするために,レベルがどのように算出されたかという理解の容易性と比較性が求められる.さらに,脆弱性スキャナや IDS のイベントログは一般的にベンダ間の互換性が無いため,汎用性と拡張性が求められる.

脆弱性レベルの定量化モデルの場合,脆弱性が一般に公表されてからの期間に応じて,その危険性が変化するため,時間的要素を考慮することが重要となる.一方,脅威レベルの定量化モデルの場合,一定期間過去から現在に至ってのイベントの発生状況によってインシデントが起こりうる危険性が変化するため,発生頻度を考慮することが重要となる.

3.2. セキュリティ情報の管理と利用

サイト間の信頼関係が確立していないイントラネットにおいて,接続先のサイトと直接セキュリティ情報を共有する P2P モデルでは,他のサイトから提供される情報の信憑性や,経路を遮断したサイトとの疎通性に問題が生じる.そこで,セキュアで安定したセキュリティ情報の流通を実現するために,各サイトの信頼点となりセキュリティ情報を中継する役割を担う第三者機関(センタ)が必要となる.以降,センタに求められる要件について述べる.

3.1 で述べたように,サイトでの脆弱性レベルや脅威レベルの定量化にあたり,マルチベンダ環境における機器の互換性の欠如が課題であった.そのため,本稿で提案するシステムで取り扱うセキュリティ情報の交換やセンタの決定に基づいた対策支援情報の画一的な形式化が望ましく,円滑な情報共有と対策の支援の達成にあたっては,汎用性・将来性・拡張性を具備したインタフェースの利用が重要となる.

センタの現状の課題として,IDS による脅威情報等の大半が誤検知(フォールスポジティブ)によるものであるため,本来の脅威を見つけるのに時間を要することが挙げられる.また日常的に大量に発生する脅威や無害な攻撃はルーチンワークによって解決できる場合が多く,これらの対応に有スキル者(アナリスト)の作業時間の大半を割かれている現状がある.このため,アナリストの負荷軽減を実現し,本来の脅威への対応にリソースを集中させるための自律支援を行う仕組みが必要となる.

一方,イントラネット内部を発信源とした情報に限定した分析や判断ではインシデント発生前の早期警戒が困難である.そのため,イントラネット外部のセキュリティに関連する情報を発信する機関からの情報収集が重要である.情報収集にあたっては,独自のポリシーや方式で運用された外部機関との連携を実現するためのアーキテクチャの設計が必要となる.

3.3. 対策手段の分析と実施

サイトのセキュリティ対策として,パッチの適用や,ユーザあるいはデータなどのアクセス権限管理など様々な対策手段が挙げられる.まずは,導入率の高さや即時性から,サイトをイントラネットに接続するルータやファイアウォールを使用したアクセス制御を対策手段として提案する.

サイトのセキュリティ管理者が,状況に応じて容易にアクセス制御を実施するためには,各種の情報をもとに分析を行って,対策手段を検討・提示する必要がある(以降,この対策手段の提案をリコメンドと記す).このリコメンドは,自サイトあるいは接続先のサイトの脆弱性レベル・脅威レベルに加えて,個別の脆弱性や脅威の傾向を加味する必要がある.

イントラネットでは,業務に不可欠な通信が

行われていることが多いため, 対策実施にあたっては可能な限り最小限の制限, あるいは短時間の制限に抑えることが望まれる. そこで, アクセス制御では, ネットワーク接続の可否だけではなく, プロトコル毎の通信可否やトラフィックシェーピングといった複数の対策手段を考える. また, ルータやファイアウォールといったアクセス制御対象機器は, サイト毎に異なる機種や異なるベンダの機器が利用されている場合が多い. このため, 機器の種類やベンダの差異による影響を受けない仕組みが必要である.

4. システム概要

本稿で提案するネットワーク運用支援システムは, セキュリティ情報管理センタ（SIMC : Security Information Management Center）のセキュリティ情報管理システム（SIMS : Security Information Management System）と, 各サイトのサイト管理システム（SMS : Site Management System）で構成される. 全体構成を図 2 に示し, 各システムの詳細はそれぞれ 4.1 および 4.2 で述べる. SIMS の利用者はアナリストであり, SMS の利用者は各サイトのセキュリティ管理者である.

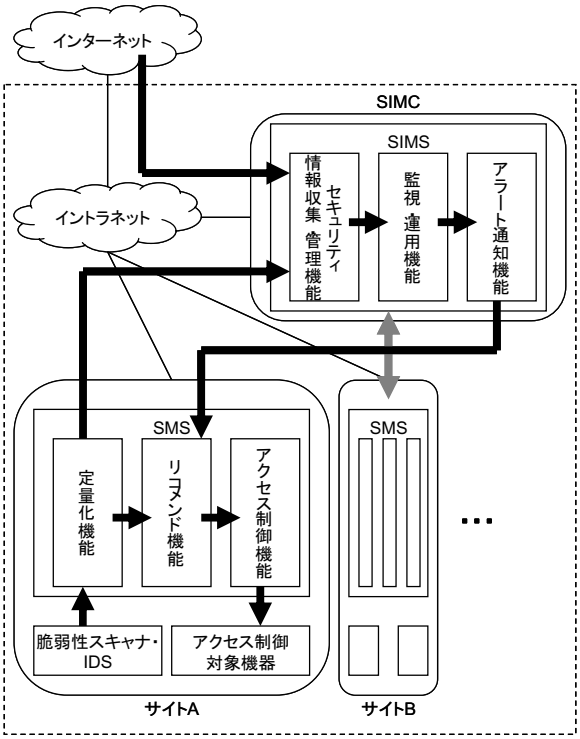

図 2 システム構成

4.1. セキュリティ情報管理システム (SIMS)

SIMS は, 3.2 で述べた要件を満たすために, 大きく以下の 3 つの機能から構成される.

・セキュリティ情報収集・管理機能,
・監視・運用機能
・アラート通知機能

セキュリティ情報収集・管理機能は, SIMS と SMS, あるいは外部機関と情報の交換を行う機能を有する. 情報共有の観点から, IETF によって仕様策定が推進されている IODEF[7]を拡張して汎用的な情報交換フォーマットを策定した. IODEF は, JPCERT/CC や CERT/CC などのインシデント対策チーム（IRT : Incident Response Team）間におけるインシデント情報交換フォーマットとして既に採用実績があり, 既存の IRT と本機能との連携が実現可能である. また, IODEF 標準化の完了に伴い, さらなる利用シーンの拡大が期待できる.

監視・運用機能は, 収集・管理機能により収集した情報の監視や分析, および分析結果に基づいた運用を支援する機能を有する. 本機能は, 刻々と変化する脅威に柔軟に対応するために, パターン化された脅威を機械的に処理する機能や, アナリストの分析を支援するための機能を有し, これら機能をモジュール単位で追加・変更可能なアーキテクチャを採用して, 脅威への適用性を確保する. これより, アナリストの負荷削減や柔軟で高度な分析の支援を実現でき, アナリストのリソースの一元化を達成する. 例えば, 分析支援モジュールとして, 統計分析

[8]やベイズ推定[9]，周波数解析[10]などで知られている最新の分析手法を適用する．

アラート通知機能は，監視・運用機能によって得た結果をサイトに通知する機能を有する．アラートは，情報共有の観点からセキュリティ情報収集機能と同様に IODEF をベースとしたフォーマットを用いて通知し，疎通性を確保する．例えば，アナリストが特定のサイトに対するアクセス制御の実施が望ましいと判断した場合，対象となるサイトに関する情報（ネットワーク情報など）を含んだアラートを生成・送付し，サイトに対策を促す．

一方，SIMS はセキュリティ情報収集・管理機能およびアラート通知機能に IODEF をベースとしたフォーマットを採用しているため，本仕様に準拠した外部のセキュリティ情報提供機関との連携が可能である．つまりは ISDAS[11]のようなインターネット観測情報などを分析の情報源として利用が可能となる．このような仕組みによって，イントラネット外における脅威の発生傾向を早急に把握でき，情報源の拡大や，ひいては脅威に対する早期警戒に有効である．

4.2. サイト管理システム（SMS）

SMS は 3.1 と 3.3 で述べた要件を満たすために大きく以下の３つの機能から構成される．

・定量化機能
・リコメンド機能
・アクセス制御機能

サイトの脆弱性レベルと脅威レベルを算出する定量化機能は，脆弱性スキャナと IDS のイベントログからベンダが定義している個別の危険度や検出日時といった共通的な情報を利用することで拡張性を備えている．また，収集した情報をもとにイベント単位，ノード単位，サイト単位という階層的なアプローチにより各レベルを算出する．算出の過程では，SIMS を経由して得られた他サイトのレベル情報に基づいて偏差値を求め，全サイトを俯瞰する相対レベルの算出により，比較性および理解の容易性の実現を図る．また，特定の脆弱性や脅威の傾向あるいはノードやサイトの重要度に応じて係数を乗じることで，より現実的なレベルの算出を図る．この結果，算出したレベルが高くなればリスクが高いことを表し，各サイトのセキュリティ管理者がレベルの確認を行うことで，相互監視効果を果たし，イントラネット全体のセキュリティの向上が期待できる．

リコメンド機能は，定量化機能で得た脆弱性・脅威レベルや SIMS からのアラートに基づき，自サイトに実施すべきリコメンドを提示する機能である．脆弱性レベルはサイトのセキュリティ管理の実施状況を表し，脅威レベルはサイトの顕在化した脅威の実態を表すと考えられる．各レベルの高まりや，両レベルのバランスによって，セキュリティ管理者は対策の判断を容易に行うことができるため，インシデント発生を予防する効果が期待できる．また，SIMS からのアラートに基づいて，特定の脆弱性や脅威に対する早期警戒や緊急措置の対策を提供することで，インシデント発生時の影響範囲を最小化するといった効果も期待できる．

アクセス制御機能は，リコメンド機能が提示した内容に従い，アクセス制御対象機器に対して，通信の制限を行う機能である．3.3 で述べたように，アクセス制御対象機器は，サイト毎に異なる可能性がある．このため，機器に依存しない制御インタフェースが必要となる．このインタフェースを介することにより，リコメンド機能はアクセス制御対象機器に依存しないリコメンドの提示が可能となる．

SMS は定量化機能，リコメンド機能，アクセス制御機能を備え，SIMS と有機的な連携を

果たすことで, サイトのセキュリティ管理者による日常的な情報収集・分析から対策実施までの一連の作業を効率的に行うことができる.

5. まとめ

本稿では, セキュアなイントラネット運用を実現するために, 脆弱性と脅威という側面から定量的にサイトを評価し, 評価結果やイントラネット内外のセキュリティ情報を活用して, 各サイトに対策を提示するネットワーク運用支援システムを提案した. 本システムを利用することで, サイトのセキュリティ管理者による自主的なセキュリティ対策を行うことができ, 相互監視効果を果たして, イントラネット全体のセキュリティの向上が期待できる. 今後, 各課題の詳細な検討を進め, 実ネットワークでの実証実験を通して, システムの有効性評価を行っていく予定である.

謝辞

本研究は独立行政法人情報通信研究機構から委託を受け実施している「ネットワーク環境の脆弱性レベルをリアルタイムで定量評価し, 情報流通をセキュアに運用するための意思決定システムの研究開発」の成果の一部である.

参考文献

[1] S.Rungta, et al.: エンタープライズ・ネットワークにおけるプロアクティブなセキュリティ対策, インテル・テクノロジ・ジャーナル, vol.08, issue04, 2004年11月

[2] G.Eschelbeck, Qualys, Inc.: The Laws of Vulnerabilities", proc. of BlackHat USA 2004, Jul 2004

[3] National Infrastructure Advisory Council: The Common Vulnerability Scoring System, http://www.packetfactory.net/papers/CVSS/, Oct 2004

[4] nCircle Network Security, Inc.: nCircle IP360 Vulnerability Scoring System Version1.2, White Paper, Nov 2001

[5] Internet Security Systems, Inc.: ALERTCON, https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp

[6] Symantec Corporation: ThreatCon, https://tms.symantec.com/Default.aspx

[7] R.Danyliw, et al.: The Incident Object Description Exchange Format Data Model and XML Implementation, IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-05.txt, Nov 2005

[8] 竹森 敬祐, 他：攻撃イベント数に関する調査および理論統計分布へのモデル化, 電子情報通信学会NS研究会, NS2003-286, pp.171-174, 2004年3月

[9] M.Ishiguro, et al.: Internet Threat Detection System Using Bayesian Estimation, FIRST Conference 2004, Budapest Hungary, Jun 2004

[10] 仲小路 博史, 他：周波数分析に基づくインシデント傾向検知手法に関する検討, Computer Security Symposium 2005, ISEC-193, SITE-192, pp.83-88, Jul 2005

[11] JPCERT/CC: Internet Scan Data Acquisition System (ISDAS), http://www.jpcert.or.jp/isdas/