マルチメディア通信と分散処理 97－16
コンピュータセキュリティ 8－16
（2000．3．22）

セキュリティポリシー作成支援ツールの開発

藤山 達也† 萱島 信† 永井 康彦† 角田 光弘‡ 山田 知明‡
（株）日立製作所 システム開発研究所†
（株）日立製作所 サービス事業部‡

あらまし: インターネット接続した情報システムのビジネス利用が一般的になり、接続に伴うセキュリティの問題の認知度も高まった。この問題に対してファイアウォールの設置等の個別対策が行われてきたが、最近では、まずシステム全体に対してセキュリティポリシーを策定し、ポリシーに基づいて抜け漏れなくコスト効果の高い対策を施したいというニーズが高まっている。従来より、厳密な脅威分析・リスク評価に基づくポリシー策定が行われてきたが、高度な専門知識と対象毎に個別の分析作業とが必要であることが実施上の課題となっている。本稿では、高度な専門知識を必要とせず、短時間にセキュリティポリシーの原案を作成できるセキュリティポリシー簡易策定手法とその手法を適用したツールについて報告する。

Development of support tool for production of security policies

Tatsuya Fujiyama† Makoto Kayashima† Yasuhiko Nagai†
Mitsuhiro Tsunoda‡ Tomoaki Yamada‡
Systems Development Laboratory, Hitachi, Ltd.†
Information Services Division, Hitachi, Ltd.‡

Abstract: The business use of IT (information technology) systems connecting to the Internet has been prevailing and many people have recognized the security problems with the connection. Conventional countermeasures to the security problems, such as setting a firewall, have been enforced. However, recently it is requested to make security policies first and then enforce cost-effective countermeasures based on the security policies. Conventional analytic method, such as threat analysis and risk assessment, has some problems on practice. In this paper, we propose the method of making security policies easily without sophisticated expertise and the support tool for production of security policies.

1. はじめに

現在ではインターネット技術に基づく企業内情報システムが非常に重要なインフラとなり、インターネットを利用したビジネス活動が一般的になった。また最近では、EC等のインターネットを利用したサービスビジネスが活発になり、サービス提供者と利用者の双方で、インターネット接続された情報システムが構築されつつある。

このようなインターネット接続された情報システムの増大と、接続に伴うセキュリティの問題の認知度の高まりにより、インターネット接続システムに対するセキュリティ診断サービスやセキュアシステム構築サービスの需要が高くなってきている。特にセキュアシステム構築サービスに関しては、ファイアウォールの設置やウイルス対策ソフトの導入といった個別の技術的対策を実施するだけでなく、システム全体に対してセキュリティポリシーを策定し、そのポリシーに基づいて抜け漏れなく、かつコスト効果の高い具体的対策を実施することが国内外で求められるようになってきている。

セキュリティポリシーを策定する手法としては、従来から、厳密な脅威分析とリスク評価を行った後、分析・評価結果に基づいてセキュリティポリシーを立案する解析的な手法が行われている[1][2]。

しかし、厳密な脅威分析とリスク評価には高度な専門技術・知識が必要となるため、一般のセキュリティコンサル SE には実施が困難である。また、分析・評価作業には多くの手間が必要となるため、所要時間やコストが膨大となり、近々にセキュリティポリシーが必要というニーズに応えることができない。そこで、従来の解析的な方法とは別に、より簡易にセキュリティポリシーを策定することが現在求められている。

このような背景の下、報告者らは、インターネット接続された情報システムに対してセキュリティポリシーを簡易に策定するツールを開発した。本稿では、開発する際に検討したセキュリティポリシー簡易策定手法とその手法を適用したツールの概要について報告する。

2. 従来手法によるポリシー策定上の課題

本章では、従来手法に基づくセキュリティポリシー策定作業の課題を述べる。

以下に、従来の解析的なポリシー策定作業の手順と各作業フェーズにおける課題を示す。

表 1: 解析型ポリシー策定手順と課題

解析型ポリシー策定手順	内容	実施上の課題
フェーズ1：評価対象の定義	情報システムや製品を適切な構成要素に分解して、評価対象を定義する（評価対象モデル化）。具体的には、脅威や対策を考慮するために適切な分解レベルを決定し、そのレベルで構成要素を洗い出す。	各評価対象毎に、適度な分解レベルを検討する作業と、構成要素の洗い出しを行う作業とが発生する。
フェーズ2：脅威の抽出	評価対象モデルの各構成要素および評価対象をとりまく環境について、想定される脅威を抜け漏れなく抽出する（脅威分析）。その際、脅威を受ける資産、脅威の実行方法、その実行者等を明確にする。	評価対象が異なれば評価対象モデルも異なるため、その都度、個別に脅威分析を行わなければならない。
フェーズ3：セキュリティポリシーの立案	抽出された脅威に対する技術的、または非技術的なセキュリティ対策目標を策定する。具体的には、脅威の発生確率と被る損害額からリスクを評価し、リスクに見合ったコスト効果の高い対策目標を立案する。	評価対象が異なれば脅威も異なるため、リスク評価に基づく対策目標の立案も評価対象毎に個別に行わなければならない。

以上より、従来手法では、

(1) 対象固有の専門知識

(2) 脅威分析・リスク評価に関する高度な専門技術・知識

(3) 対象毎に個別の解析作業

が必要であり、結果として、膨大な作業コストを要することとなる。また、作業者の技術・知識レベルに依存するため、そのレベルが低ければ、低い品質のセキュリティポリシーしか得られない。

3. セキュリティポリシー簡易策定手法の提案

本章では、インターネット接続システムの特性を利用し、上記の課題を解決するセキュリティポリシー簡易策定手法について述べる。

3.1 インターネット接続システムの特性

インターネット接続システムは、ファイアウォール、公開サーバ等のインフラ部分の構成がシステム毎に大きく異なっており、このインフラ部分の違いがシステムに固有性を与えている。

またインターネット接続システムの場合、図 1のような接続形態が一般的であり、システム毎の違いは大きくない。よって、接続形態の違いよりも各情報機器の有無の方がシステムの固有性へ影響する。

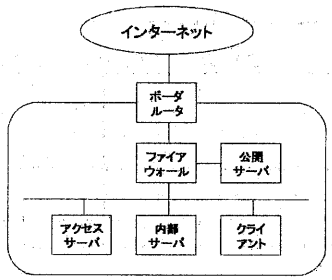


図 1: インターネット接続システム形態例

3.2 インターネット接続システム向けセキュリティポリシー簡易策定手法

インターネット接続システムのインフラ部分の違いがシステムに固有性を与えるという特性を利用して、従来手法を簡略化する手法を提案する。本手法は、(1)情報機器の組み合わせによる対象システムのモデル化と(2)各情報機器の事前分析に基づくポリシー事例の部品化を特徴とする。

3.2.1 評価対象の定義

インターネット接続システムでは、(1)インフラ部分を定義することによりシステムを個別化でき、(2)このインフラ部分の定義は構成する情報機器の種類を特定することで行うことができる。

そこで、本手法では、インターネット接続システムの構成要素を以下の6種類の情報機器に分類し、対象システムを構成する情報機器の組み合わせにより対象をモデル化することとした。

(1) 公開サーバ
　外部ユーザ向けに Web やメール等のサービスを提供する計算機
(2) 内部サーバ
　内部ユーザ向けに Web やメール等のサービスを提供する計算機
(3) クライアント
　サーバアクセスに利用する PC 等の計算機
(4) ファイアウォール
　インターネット等の外部ネットワークと内部ネットワークとの間に設置し、両ネットワーク間の通信データをフィルタリングする計算機
(5) ボーダルータ
　インターネット等の外部ネットワークと内部ネットワークとの間に設置し、両ネットワーク間の通信経路を制御する計算機
(6) アクセスサーバ
　外部から内部ネットワークへのダイアルアップアクセスの接続可否を判別する計算機

これにより、対象システムを構成する情報機器を調査するだけで簡単に評価対象を定義することが可能となり、表 1のフェーズ1の作業を簡略化すると同時に、評価対象モデルに対象システム毎の固有性を反映することができる。

3.2.2 脅威の抽出とセキュリティポリシーの立案

提案手法では、対象システムを構成する情報機器に対して、専門家による脅威分析や過去の事例データの抽出を事前に行い、各情報機器に想定される脅威とそのセキュリティポリシーとをマトリクス化した一覧表（以降、脅威要因分析表と呼ぶ）をポリシー事例の部品一覧として用意する。脅威要因分析表の形式を表 2に示す。

そして、この脅威要因分析表を用いて、情報機器の組み合わせに該当するセキュリティポリシーを抽出し、組み合わせることにより、脅威分析・リスク評価等の解析作業を行うことなくセキュリティポリシーを策定する。

このように脅威分析や事例データに基づく脅威要因分析表を事前に準備して利用することにより、表1のフェーズ2とフェーズ3の作業を簡略化すると同時に、対象システムの固有性を反映したセキュリティポリシーの策定と作業者の技術・知識レベルに依存しない品質確保を実現できる。

表 2: 脅威要因分析表

項番	ポリシー種別	詳細種別	想定される脅威					セキュリティポリシー	構成要素（脅威とその対策目標に該当する機器の欄に○を付ける）					
			攻撃者	保護対象資産	目的	脅威種別	攻撃方法		公開サーバ	内部サーバ	クライアント	ファイアウォール	ボーダルータ	アクセスサーバ
1									○	○				○
2											○			
…												○	○	

4. ツールの開発

提案するセキュリティポリシー簡易策定手法を適用した(1)セキュリティポリシー策定支援機能と(2)セキュリティ評価支援機能を持つポリシー策定支援ツールを開発した。本章では、各機能の概要を報告する。

4.1 セキュリティポリシー策定支援機能

本機能は、対象モデル化の構成要素として、システムを構成する情報機器に加え、システムに要求するセキュリティの強度を考慮することにより、対象システムの固有性をより一層反映したセキュリティポリシーを作成する機能である。以下に、本機能の動作概要を説明する。

本機能は、最初に、(1)対象システムを構成する情報機器と(2)対象システムに要求するセキュリティの強度を入力させる。この時、入力データは、情報機器については 3.2 節で分類した 6 種類の情報機器群から選択させ、セキュリティ強度については「並」「強」「最強」の 3 段階の中から選択させる（図 2）。

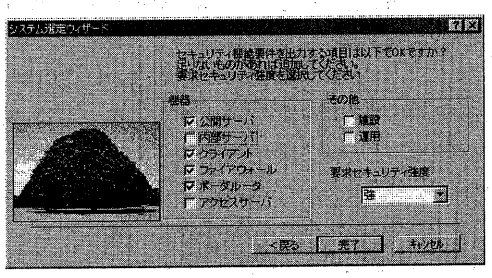


図 2: 対象システム入力画面例

次に、選択した情報機器とセキュリティ強度に基づいて、脅威要因分析表から該当するセキュリティポリシーを抽出する。なお、本機能の脅威要因分析表では、情報機器とセキュリティ強度の組に対して該当するセキュリティポリシーをマトリクス化した。

最後に、抽出したセキュリティポリシーを情報機器毎に一覧表示する（図 3）。

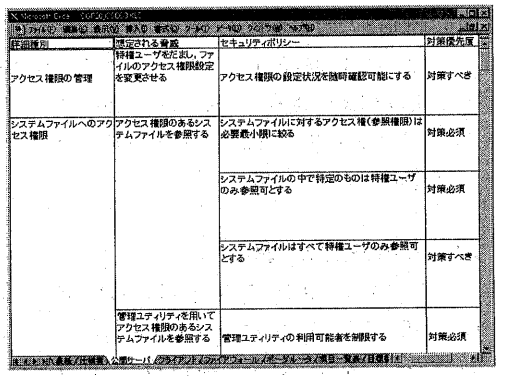


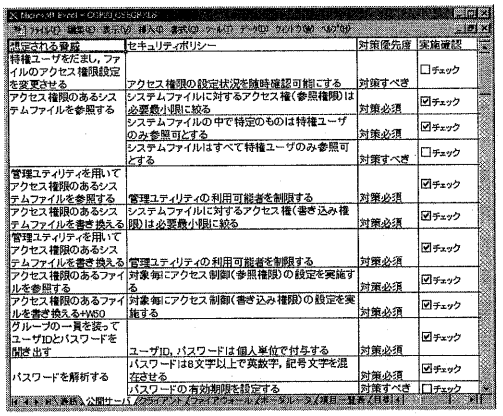
図 3: セキュリティポリシー出力画面例

4.2 セキュリティ評価支援機能

本機能は、対象システムに固有のセキュリティポリシー一覧をチェックリストとし、各ポリシーの実施有無に基づいて、計画中および現行のシステムのセキュリティ状態を評価する機能である。以下に、本機能の動作概要を説明する。

本機能は、最初に、前述のセキュリティポリシー策定支援機能を利用して対象システム固有のセキュリティポリシーを生成する。そして、各セキュリティポリシーに対してチェックボックスを設けたチェックリストを作成し、実施済みのポリシーにチェッ

ク入力をさせる（図 4）。



想定される脅威	セキュリティポリシー	対策優先度	実施確認
特権ユーザをだまし，ファイルのアクセス権限設定を変更させる	アクセス権限の設定状況を随時確認可能にする	対策すべき	□チェック
アクセス権限のあるシステムファイルを参照する	システムファイルに対するアクセス権（参照権限）は必要最小限に絞る	対策必須	☑チェック
	システムファイルの 中で特定のものは特権ユーザのみ参照可とする	対策必須	☑チェック
	システムファイルはすべて特権ユーザのみ参照可とする	対策すべき	□チェック
管理ユティリティを用いてアクセス権限のあるシステムファイルを参照する	管理ユティリティの利用可能者を制限する	対策必須	☑チェック
アクセス権限のあるシステムファイルを書き換える	システムファイルに対するアクセス権（書き込み権限）は必要最小限に絞る	対策必須	☑チェック
管理ユティリティを用いてアクセス権限のあるシステムファイルを書き換える	管理ユティリティの利用可能者を制限する	対策必須	☑チェック
アクセス権限のあるファイルを参照する	対象 毎にアクセス制御（参照権限）の設定を実施する	対策必須	☑チェック
アクセス権限のあるファイルを書き換えるHW50	対象 毎にアクセス 制御（書き込み 権限）の 設定を実施する	対策必須	☑チェック
グループの一員を装ってユーザIDとパスワードを聞き出す	ユーザID，パスワードは 個人単位で付与する	対策必須	☑チェック
パスワードを解析する	パスワードは8文字以上で英数字，記号 文字を混在させる	対策必須	☑チェック
	パスワードの 有効期限を設定する	対策すべき	□チェック

図 4: ポリシー実施有無入力画面例

次に、「アクセス権限の設定・管理」「識別と認証」など17種類に分類したポリシー種別（表 3）毎に、該当ポリシー数と実施済みポリシー数を集計し、その実施割合（実施済みポリシー数／該当ポリシー数 [%]）を計算する。

表 3: セキュリティポリシー種別

項番	ポリシー種別	実施目的
1	アクセス制御	リソースに対して実行可能な操作を限定する
2	アクセス権限の設定・管理	不正なアクセス権の付与を防止する
3	識別と認証	不正ユーザを判別する
4	ファイル・伝送データの暗号化	格納したデータや通信データの機密性を確保する
5	アクセス監視	不正行為を監視する
6	侵入者・ウイルス対策	悪意のある操作を未然に防止する
7	セキュリティ管理状況の点検	セキュリティ機能が適切に使用されているかを確認する
8	人員管理	オペレータ等の不正行為を防止する
9	入退室管理	施設への不正侵入を防止する
10	施錠管理	情報資産への物理的な不正アクセスを防止する
11	端末管理	端末の不正使用を防止する
12	オペレーション管理	機器に対する不正な操作を防止する
13	プログラム管理	ソフトウェアの不正な置き換えを防止する
14	デバッグ管理	ソフトウェアへの不正な機能の混入を防止する
15	インストール管理	システムへの不正な機能の導入を防止する
16	ドキュメント管理	システム等の機密情報の漏洩を防止する
17	データ管理	機器内にあるコンテンツを保護する

最後に、システムを構成する各情報機器について、ポリシー種別毎のポリシー数、実施済みポリシー数、実施割合を集計した一覧表と、各ポリシー種別を軸としたレーダーチャートを表示する（図 5）。

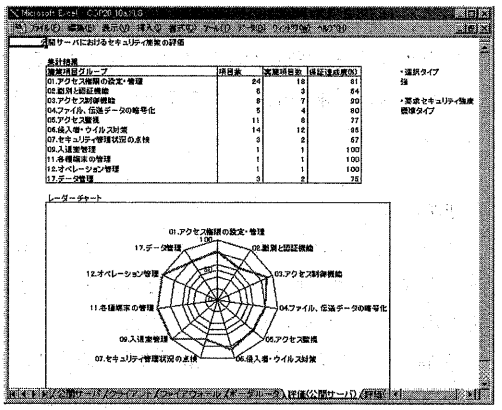


図 5: セキュリティ評価出力画面例

4.3 事例適用に基づく考察

従来の厳密な脅威分析・リスク評価に基づいてセキュリティポリシーを策定する場合と提案手法を適用した機能を用いてセキュリティポリシーを策定する場合とを比較した結果を表 4に示す。なお、比較データは適用実績に基づくものである。

表 4: 従来手法と提案手法の比較

項目	従来手法	提案手法
所要時間	半年～1年	**数週間～数ヶ月**
高度な専門知識・技術	要	**不要**
セキュリティポリシーの品質	作業者の専門技術・知識レベルに応じて、ばらつきがある	作業者の専門技術・知識レベルに依存せず、**一定品質を確保**

セキュリティポリシーの品質の高さについては、高度な専門技術・知識を持つ作業者が、厳密な分析・評価に基づく従来手法により策定する方が優れる。しかし、作業者のレベルに依存しない一定品質を確保したポリシー原案を短時間に少ない費用で策定する場合には、従来手法と比べて提案手法の方が有効である。

5. おわりに

本稿では、インターネット接続システムを対象とするセキュリティポリシー簡易策定手法とその手法を適用したツールの概要について報告した。

本稿で提案する手法は、(1)情報機器を構成要素とする対象システムのモデル化と(2)各情報機器に該当するセキュリティポリシー事例をマトリクス化した脅威要因分析表の利用により、ポリシー事例部品の組み合わせでセキュリティポリシーを策定できることを特徴としている。

この特徴により、本手法を適用したセキュリティポリシー策定では、所要時間やコストの削減と作業者の技術・知識レベルに依存しない品質確保を実現した。

参考文献

[1] 日本セキュリティ・マネジメント学会: セキュリティ ハンドブック I, 日科技連, 1998

[2] FISC: 金融機関等コンピュータシステムの安全対策基準, 金融情報システムセンター(FISC), 1998