セキュリティ対策変更に適応可能なネットワーク監視システムの設計

西村 啓渡† 加藤 弘一† 勅使河原 可海‡

†,‡創価大学大学院工学研究科

Email: †{e09m5231, kokatou}@soka.ac.jp, ‡teshiga@t.soka.ac.jp

あらまし 堅牢なセキュリティの実現には過不足のないインシデント検出が重要である．しかし，ネットワークの監視箇所とインシデント検出ルール（監視ポリシ）は，管理者の知識・経験により決定されることが多く，妥当性を保証できない．また，通常は個別に検出した事象を相関分析し，インシデント発生の有無を判断するが，相関分析のルール作成も妥当性の保証がない．さらに，対策変更時には監視ポリシの変更が必要となる．本研究ではこれまで，対策変更に適応可能な，監視ポリシと相関分析ルールの決定方式を検討してきた．本稿では，本方式を実現するためのシステム設計を行い，機能，データベース，システム構成について述べる．

Design of a Network Monitoring System Adaptable to Changes in Security Countermeasures

Keito Nishimura† Koichi Kato† Yoshimi Teshigawara‡

†,‡Graduate School of Engineering, Soka University

Email: †{e09m5231, kokatou}@soka.ac.jp, ‡teshiga@t.soka.ac.jp

Abstract: It is important to detect incidents in just proportion in order to enhance the network security. However, the validity of network monitoring points and incident detection rules cannot be guaranteed because they are usually determined by the administrator's knowledge and experience. Furthermore, general intrusion detection systems clarify whether an incident had occurred by correlation analysis of individual detected events. However, the validity of created correlation analysis rules also cannot be guaranteed. In addition, when the security countermeasures are changed, to review monitoring policy and detection rules are needed. We have studied a decision method of monitoring policy and correlation analysis rules adaptable to changes in security countermeasure. This paper shows system design to realize the proposed method, and describes its functions, databases, and the system configuration.

1. はじめに

情報システムにおける堅牢なセキュリティを実現するためには，脅威から情報資産を保護する対策だけでなく，インシデントの発生（以後，リスク顕在化と同義として扱う）を検出するためにネットワークを監視することも重要である．しかし，ネットワークの監視箇所とインシデント検出ルール（以後，この組を監視ポリシと呼ぶ）は，管理者の知識や経験，過去の実績により決定されることがほとんどであり，妥当性が保証されていない．

また，インシデントは単独もしくは一連のセキュリティ事象によって発生する[1]．従来は，個別に検出したセキュリティ事象を相関分析し，事象の連鎖関係からインシデントの有無を判断している．しかし，監視ポリシと同様に，相関分析のルール作成は知識や経験に依存している．

インシデントを過不足なく検出するためには，体系的に監視ポリシと相関分析ルールを決定する

必要がある．さらに，組織のネットワークにおいて対策が変更される事例は多く考えられ，セキュリティレベルを維持するための対策決定手法も存在する[2][3]．しかし，対策の緩和がインシデント発生の原因となっていないか，また対策の強化が正常に機能しているかどうかを監視するためには，対策実施状況を反映させた監視ポリシの変更が必要となる．

本研究はこれまで，対策変更に適応可能な，過不足のないインシデント検出方式の確立を目的とし，体系的な監視ポリシと相関分析ルールの作成，およびそれらを用いたインシデント検出方式を検討してきた[4]．本方式が実際のネットワーク環境においてインシデントの発生を過不足なく検出できること，またセキュリティ対策の変更に対応可能であることを確認するためには，監視システムの実装が不可欠である．そこで本稿では，本方式に基づくシステムを実装するための，機能，データベース（以下，DB），システム構成を設計する．

2. システム実現上の課題

インシデント検出までの流れを，リスク分析，監視ポリシの決定，相関分析によるインシデント検出の 3 フェーズに分割し，各フェーズにおける方針と課題について述べる．

2.1 網羅性と妥当性のあるリスク分析

一般的なリスク分析と同様に，資産，脅威，脆弱性を洗い出してリスクを特定する．同時に，インシデントを構成するセキュリティ事象の洗出し，分岐・合流を含む事象の連鎖関係の分析，対策と事象の関係の分析，および事象の属性値の特定を行う．このとき，各分析における網羅性および妥当性を確保しなければならない．なお，本研究では，いつ，どこで，どの主体が，どの対象に，どのような処理を実行したかといった，セキュリティ事象が持つ要素を「属性」，要素の具体的な情報を「属性値」と定義する．

2.2 対策実施状況を考慮した監視ポリシの決定

インシデントの重要さの違いから，必ずしもすべてのリスクに対する監視が必要なわけでない．また，対策変更の際には監視ポリシの変更が必要となる．そこで，考えうる監視ポリシ案の中から，対策実施状況に応じて監視ポリシを決定する．

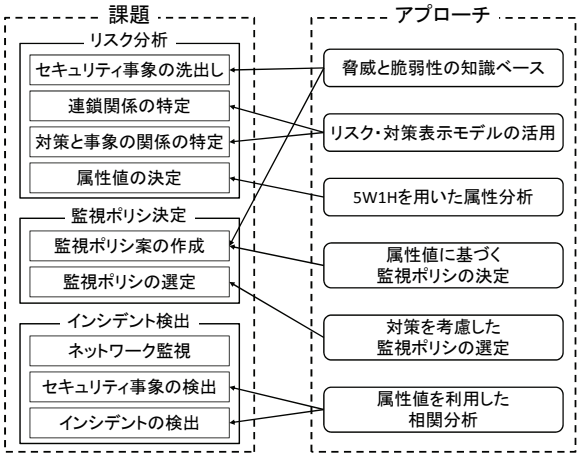

図 1 課題とアプローチの対応関係

そのためには，2.1 節で明らかにした事象の属性値を正確に反映した監視ポリシ案の作成が必要である．そして，対策実施状況を考慮して，監視ポリシを決定できなければならない．

2.3 相関分析に基づくインシデント検出

インシデントを検出するために，個々に検出した事象が実際にインシデントを発生させたかどうかを相関分析する．このとき，網羅的なセキュリティ事象の検出，およびセキュリティ事象間の因果関係の有無を正確に判断できることが必要である．

なお，ネットワーク監視が適切に動作されていること（パケットやログの取りこぼしがなく，全ての検出ルールが正常に動作している）を前提とする．

3. 対策変更に適応可能な監視方式

2 章で挙げた課題を解決するためのアプローチについて述べる．図 1 に各課題とアプローチの対応関係を示す．

3.1 脅威と脆弱性の知識ベース

セキュリティ事象の洗出し，および検出ルール作成のために，脅威と脆弱性の知識ベースを用いる．管理者は外部で公開されている脅威や脆弱性情報を知識ベースに蓄積する．また，知識ベースは組織間で共有することも可能である．

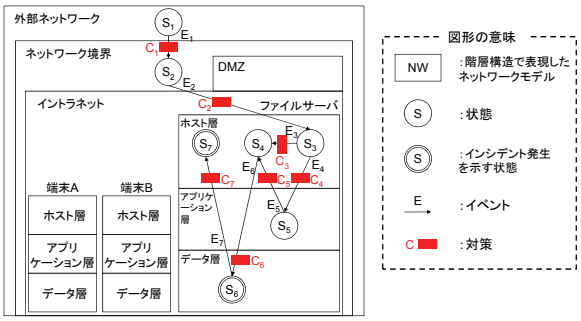

図 2 リスク・対策表示モデル

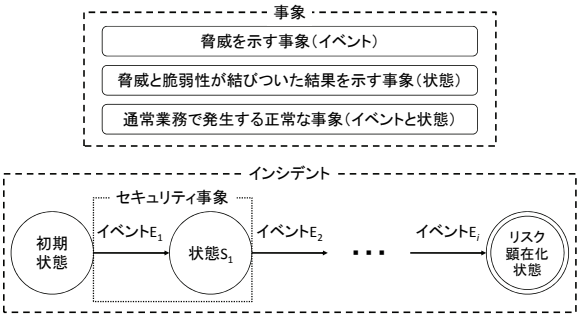

図 3 セキュリティ事象とインシデントの関係

3.2 リスク・対策表示モデルを活用したセキュリティ事象連鎖および対策関係分析

セキュリティ事象の連鎖関係，および対策と事象の関係を分析するために，図 2 のように，リスクの連鎖関係およびリスクと対策の関係を視覚的に把握可能なモデル[5]を活用する．また，セキュリティ事象の発生箇所も特定できるため，属性値を決定する際の支援ともなる．

セキュリティ事象には，脅威を示す事象と，脅威と脆弱性が結びついた結果を示す事象がある．本方式では，洗い出された脅威を「イベント」，脆弱性が突かれた状態を「状態」と表現してネットワークモデルに配置し，イベントと状態の組を 1 つのセキュリティ事象として定義する．また，事象，セキュリティ事象，およびインシデントの関係を図 3 に示す．

3.3 5W1H を用いたセキュリティ事象の属性分析

物事を正確に伝えるためのフレームワークとして 5W1H がよく用いられている．そこで，事象検出に必要な属性を網羅的に特定するために，5W1H を用いた属性分析を行う．

表 1 セキュリティ事象の属性及び属性値の内容

		属性					
		Who	What	Where	When	Why	How
属性値内容	イベント	始点となる主体者	終点となる資産	発生経路	発生しうる時間	–	監視する処理内容（脅威）
	状態	–	状態を示す資産	資産の存在箇所	状態になりうる時間	状態に遷移した要因（脆弱性）	監視する状態の内容

イベントおよび状態検出に必要な属性を整理したものを，表 1 に示す．管理者は，属性値の内容に従って，各セキュリティ事象の属性値を決定する．ここで，イベントの Why にはイベント発生の動機が当てはまるが，動機の検出は困難であるため除外した．また，状態の Who には状態遷移させた主体者が当てはまるが，必ずしも検出できるとは限らないため除外した．

3.4 属性値に基づく監視ポリシ案の作成

知識等に依存せず，網羅的に監視ポリシ案を作成するために，属性値を用いる．監視箇所案の作成には，事象の発生箇所を示す Where 値を用いる．また，本方式では，ネットワークにおける統計情報を必要とせず，適用が比較的容易な不正検出アルゴリズムにより既知の事象を検出するため，検出ルール案の作成には，脅威情報を示す How 値をキーに知識ベースから抽出したシグネチャを用いる．

3.5 対策の実施状況を考慮した監視ポリシの選定

3.2 節での分析結果を用い，インシデント，対策，監視ポリシを関連付ける．そして，インシデント，およびそれに関連する監視ポリシと対策実施状況を管理者に提示し，監視すべきインシデントと必要な監視ポリシを決定する．

3.6 属性値を利用した相関分析

イベントと状態，およびセキュリティ事象間の因果関係の特定のために，属性値を利用した相関分析を行う．相関分析では，まず，属性値を基に因果関係を分析する 2 つ事象を抽出する．そして，属性値を利用した分析により，因果関係の有無を判断する．相関分析に用いる属性値および判断するためのルールの一例を以下に示す．

(セキュリティ事象間の相関分析ルール例)

連鎖元セキュリティ事象の状態の When 値が，

連鎖先セキュリティ事象のイベントの When 値より小さく，かつ値の差が 30 分以内.

4. システム設計

本方式に基づくシステムを実装するための，機能，DB，システム構成の設計について述べる.

4.1 DB 設計

(1) 知識ベース

脅威，脆弱性および脆弱性が突かれた後の資産の状態といった情報を保持する．また，脅威情報には，エクスプロイトコードや，シグネチャ（攻撃のパターンコード）といった具体的な脅威情報も蓄積される.

(2) 情報資産 DB

対象資産, ネットワーク構成, 機器の配置構成, および各機器が備えるアプリケーションの種類といった情報を保持する.

(3) リスク情報 DB

リスク分析により特定されたリスク，セキュリティ事象，事象の連鎖関係，事象の発生箇所，および事象の属性値を保持する．事象の発生箇所については，図 2 のようなネットワークモデルでイベントや状態が配置されている階層名を保持する.

(4) 対策情報 DB

実施済み，もしくは実施する可能性のある対策と，対策と事象の関係を保持する.

(5) 監視ポリシ DB

適用する可能性のある監視箇所や検出ルール，およびログやパケットと収集箇所の関係を保持する．ログ・パケットの収集箇所については，図 2 のようなネットワークモデルの階層ごとに収集可能な情報を整理する．例えば，イントラネット層においてはパケット, 端末のホスト層においては, Syslog やカーネルログなどが収集可能である.

(6) インシデント DB

ネットワーク監視によって検出されたイベントや状態，検出されたセキュリティ事象，検出されたインシデントを保持する.

4.2 機能設計

本システムはリスク分析支援機構，監視ポリシ決定支援機構，およびインシデント検出機構の 3 つの機構から構成される．機能構成および DB との関連を図 4 に示す.

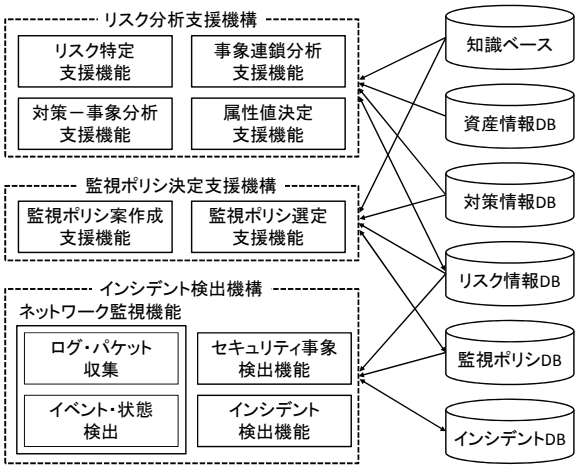

図 4 機能構成と DB の関連

(1) リスク分析支援機構

網羅性と妥当性のあるリスク分析を支援する．本機構は，次の 4 つの機能で構成される.

リスク特定支援機能は，リスク，セキュリティ事象の特定を支援する．リスク特定に関しては，情報資産 DB に保持される資産ごとに，機密性, 完全性, 可用性の損失種別と攻撃者の種別(内部, 外部）の 2 つの種別のすべての組合せを，対象リスクの候補として管理者に提示する．また，セキュリティ事象の特定に関しては，情報資産 DB に保持されるアプリケーション情報をキーとして知識ベースから対象セキュリティ事象（脅威と脆弱性の組）の候補を抽出し，管理者に提示する．管理者は提示された情報から，対象リスクと対象セキュリティ事象を決定し，この情報はリスク情報 DB に出力される．なお，必要に応じて提示された情報に対する修正や追加も可能である.

事象連鎖分析支援機能は，リスク情報 DB に保持される対象リスク・セキュリティ事象を管理者に提示する．管理者は，提示されたリスク情報を基に，インシデント発生の一連の流れの始点と終点を定め，到達するまでの状態遷移を分析する．分析結果はリスク情報 DB に出力される.

対策－事象分析支援機能は，対策と関連する事象の分析を支援する．分析時に，対策情報 DB に

保持される実施済み，もしくは変更される対策を管理者に提示する．分析結果は対策情報 DB に出力される．

属性値決定支援機能は，セキュリティ事象の属性値の決定を支援する．リスク情報 DB に保持される対象セキュリティ事象と事象の発生箇所から，Where，Why，How 値を自動的に付与する．そして，付与した値を管理者に提示し，必要であれば修正する．Who，What，When 値は管理者が付与する．決定された情報は，リスク情報 DB に出力される．

(2) 監視ポリシ決定支援機構

対策実施状況を考慮した監視ポリシの決定を支援する. 本機構は, 次の 2 つの機能で構成される．

監視ポリシ作成支援機能は，監視箇所と検出箇所の案を作成することを支援する．監視箇所に関しては，Where 値をキーとして，監視ポリシ DB に保持されるログやパケットと収集箇所の関係から，セキュリティ事象を検出可能なログ・パケットの候補を抽出し，管理者に提示する．そして，管理者が，属性値すべてを特定可能となるログ・パケットの組合せを決定する．最後に，決定されたログ・パケットを収集可能な機器を監視箇所案とする．一方，検出ルールに関しては，How 値をキーとして知識ベースからシグネチャを抽出し，Who 値を攻撃の主体者, What 値を攻撃先, When 値を監視時間として検出ルール案を作成し，管理者に提示する．管理者は，提示された検出ルール案を必要に応じて修正する．作成された監視ポリシ案は，監視ポリシ DB に出力される．

監視ポリシ選定支援機能は，作成された監視ポリシ案から必要な監視ポリシを決定することを支援する．リスク情報 DB，監視ポリシ DB，対策情報 DB から，リスク，関連する対策，および関連する監視ポリシを管理者に提示する. 管理者は, 提示された情報を基に最終的に適用する監視ポリシを決定する．決定された監視ポリシは，監視ポリシ DB に出力される．

(3) インシデント検出機構

ネットワークを監視し，インシデントを検出する．本機構は，次の 3 つの機能で構成される．

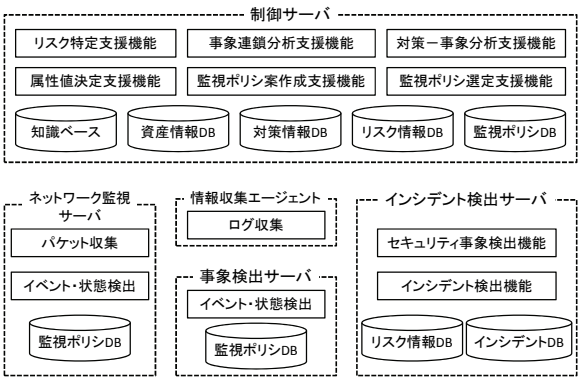

図 5 機能配置図

ネットワーク監視機能は，決定した監視箇所においてパケットやログを収集し，そのパケット・ログに対して検出ルールを適用することで，イベントや状態を検出する．検出したイベントや状態は，インシデント DB に出力される．

セキュリティ事象検出機能は，まず，インシデント DB からイベントを取り出し，そのイベントによって生じた状態を抽出する．そして，相関分析ルールを用い，抽出したイベントと状態の因果関係の有無を判断する．因果関係があると判断した場合，検出したセキュリティ事象がインシデント DB に出力される．

インシデント検出機能は，検出した個々のセキュリティ事象から，インシデントであるかどうかを判断する．まず，リスク情報 DB の事象の連鎖関係を基に，インシデント DB から，因果関係の分析対象となるセキュリティ事象を抽出する．そして，相関分析ルールを用い，抽出したセキュリティ事象の因果関係の有無を判断する．インシデント発生までの一連の流れが形成されていると判断できた場合，検出したインシデントがインシデント DB に出力される．

4.3 システム構成設計

実際のネットワークにおける機能配置を考える．本システムのシステム構成は，制御サーバ，ネットワーク監視サーバ，情報収集エージェント，事象検出サーバおよびインシデント検出サーバとなる. 各機器と搭載機能の関係を図 5 に示す. また，

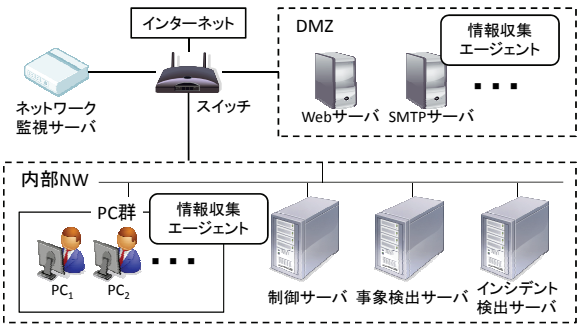

図 6 システム構成例

システム構成例を図 6 に示す.

制御サーバで作成される監視ポリシ DB やリスク情報 DB は，その情報を必要とする機能を搭載する機器にミラーリングする．基本的には，両 DB ともに，制御サーバでのみ更新され，他のマシンの DB を同期させる.

5. 本システムの利点

本システムでは，リスク分析に基づく監視ポリシや相関分析ルールを体系的に作成することにより，決定されたそれぞれの妥当性を保証することができる．また，対策の実施状況に応じた監視ポリシの決定が可能なため，セキュリティ対策に変更が生じる際にも，妥当性を維持したまま，柔軟に対応することができる.

さらに，本システムは 2 章で述べた各課題に対応した単一機能構成をとるため，セキュリティ対策変更への対応が容易に実現できる．つまり，対策変更に関連する機能のみを作動させることで，対策変更に対応できる.

6. まとめと今後の課題

本稿では，対策変更に適応可能な，過不足のないインシデント検出方式の確立を目的とし，事象の連鎖関係や，対策と事象の関連，および属性分析に基づく監視ポリシと相関分析ルールの決定方式の概要を述べた．また，方式に基づくシステムを実装するための機能，DB，システム構成について設計した．この設計に従い，システムの実装を目指す.

今後の課題は以下の通りである.

(1) 分析の粒度

脅威，脆弱性およびセキュリティ事象の分析の粒度の違いは，誤検知数，作業負荷，運用パフォーマンス等に影響を与える．通常，このような粒度は組織の求める分析精度や分析者の知識・経験により決定されるため，妥当性のある粒度の決定は難しい．そのため，粒度の指標を作成するために，例えば実験を繰り返す中で妥当な粒度を模索することが必要である.

(2) 相関分析のルールの決定

セキュリティ事象を 5W1H の観点で分析しているため，事象の因果関係を分析する際に，属性の組合せ方法によって，様々な性質のインシデントを検出することが可能になると期待できる．そこで，相関分析時に用いる属性の組合せと，検出可能な状況について分析する.

(3) 実装による本方式の評価

本方式に基づくシステムを実装し，実環境における実験を行う．実際に運用されているネットワーク環境において，本方式がインシデントの発生を過不足なく検出でき，セキュリティ対策の変更に対応可能であることを確認する.

参考文献

[1] ISO/IEC 27001:2005

[2] 加藤弘一，勅使河原可海：ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案，情報処理学会論文誌, Vol.49, No.9, pp.3209-3222, 2008.9.

[3] 榊啓，矢野尾一男，小川隆一：多目的最適化によるセキュリティ対策立案方式の提案，CSS2007 論文集，Vol.2007，No.10，pp.193-198，2007.11.

[4] 西村啓渡，加藤弘一，勅使河原可海：情報セキュリティ対策変更に適応可能なネットワーク監視方式の検討，情報処理学会 DICOMO2009 シンポジウム, pp1240-1250, 2009.7.

[5] 加藤弘一，勅使河原可海：多層防御の概念に基づくリスクと対策効果のモデル化に関する検討，情報処理学会 DICOMO2008 シンポジウム，pp.1531-1540，2008.7.