Vol.2011-DPS-146 No.24
Vol.2011-CSEC-52 No.24
2011/3/10

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開発

西村啓渡[†]　加藤弘一[††]　勅使河原可海[†]

インシデント被害の局所化と再発防止は重要であり，インシデントを正確に検出する必要がある．しかし，多種多様な機器を経路としたインシデントの検出は困難である．また，対策変更時には監視箇所や検出手法を見直す必要がある．本研究ではこれまで，対策変更に適応可能な監視箇所と検出ルールの決定，および状態遷移モデルに基づく相関分析手法について検討してきた．本稿では，本方式に基づくプロトタイプを実装し，システムの有効性を検証する．簡易実験により，インシデントおよびその発生経路を自動的に特定し，かつ対策変更に対する監視の切り替えを実現できる見通しを得た．

Development of Network Monitoring System Adaptable to Changes in Security Countermeasures

Keito Nishimura,[†] Koichi Kato[††]
and Yoshimi Teshigawara[†]

In network monitoring, we must detect security incidents accurately because it is important to minimize damage by the incidents and prevent recurrence of them. However, to detect incidents routed through a variety of devices is difficult. In addition, to review monitoring points and detection rules are required as security countermeasures are changed. We have studied a decision method of monitoring points and detection rules adaptable to changes in security countermeasures, and a correlation analysis method based on the state machine model. We implemented a prototype system and evaluated the effectiveness of the system through simple simulations. From experimental results, we expect that our system can automatically detect incidents and their routes, and also change monitoring points and detection rules corresponding to the change of security countermeasures.

1. はじめに

企業や学術機関といった組織における情報システムのインフラ化と，不正アクセスを初めとする脅威の増加や多様化から，セキュリティ対策の導入・運用が重要視されている．一方，対策がすべての脅威から情報資産を守ることは困難であるため，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）の検出を目的としたネットワーク監視も同様に重要である．本稿におけるネットワーク監視とは，サーバや PC，ネットワーク機器から収集したログやパケットを利用し，情報資産のセキュリティ状況を把握することと定義する．

ネットワーク監視における重要な役割は，インシデント被害の局所化と再発の防止である．被害局所化のためにはリアルタイムかつ過不足のないインシデント検出，再発防止のためにはインシデントの発生経路や原因の特定が必要である．和泉らは，ネットワークトラフィックにおける任意の 2 つの観測量の相関係数を算出し，評価することで，ネットワークの異常状態，およびその原因を特定している[1]．しかし，観測対象がネットワークトラフィックのみであるため，管理者権限の奪取やファイルの改ざんなどホスト内部で発生するインシデントの漏れのない検出は困難であると考えられる．野口らは，不正アクセスが起こるまでの手順を状態遷移図で表現し，イベント間の依存関係を分析することで，任意のイベントから派生する可能性の高い不正アクセスを予測している[2]．しかし，実際に発生したイベント間の因果関係の特定方法は述べておらず，インシデントの発生経路を特定することは困難であると考えられる．

ネットワーク監視は，リスクを抑止・予防するためのセキュリティ対策が脆弱もしくは未実施の箇所に対して運用される場合が多く，対策の実施状況の変化は監視設定に影響を与える．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選定手法も存在する[3][4]．しかし，対策と連動したネットワーク監視方式は，筆者らの知る限りでは存在しない．

本研究は，対策変更に適応可能な過不足のないインシデント検出を目的とし，7W1H を用いた監視箇所と検出手法の決定，および状態遷移モデルに基づく相関分析による解決を図る．

2. 研究上の課題

2.1 インシデント発生プロセスを特定可能なシナリオ分析

情報セキュリティの国際標準では，インシデントを「単独もしくは一連のセキュリ

[†] 創価大学大学院工学研究科
Graduate School of Engineering, Soka University
[††] 創価大学工学部
Faculty of Engineering, Soka University

Vol.2011-DPS-146 No.24
Vol.2011-CSEC-52 No.24
2011/3/10

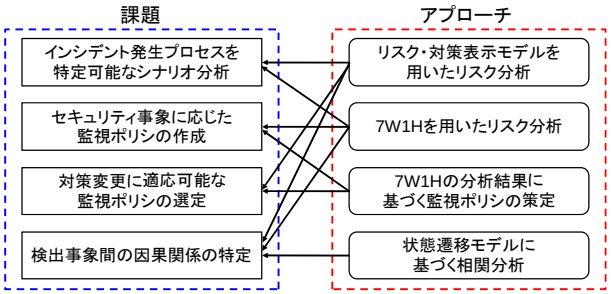

図 1　課題とアプローチの関係

ティ事象によって発生するもの」と定義している[5]．本研究ではこの定義に基づき，インシデント発生の原因となった個々のセキュリティ事象を網羅的に検出し，一連のセキュリティ事象の発生の因果関係を特定することにより，インシデントを検出するという方針を採る．

インシデントを漏れなく検出するためには，その発生プロセスであるセキュリティ事象，およびそれらの順序関係を特定可能なシナリオ分析が必要となる．

2.2　セキュリティ事象に応じた監視ポリシの作成

ネットワーク監視を導入するためには，「監視対象データ」「検出手法」を特定しておく必要がある．本研究では，セキュリティ事象検出のために収集するログやパケットの種類を監視対象データ，ログやパケットの内容からセキュリティ事象が発生しているかどうかを判断するための手法を検出手法，また 1 つのセキュリティ事象に対応する監視対象データと検出手法の組を 1 つの監視ポリシとしてそれぞれ定義する．

セキュリティ事象の概念には「権限昇格」「ファイル改ざん」など性質の異なる事象が混在しており，セキュリティ事象を漏れなく検出するためには，監視ポリシを体系立てて作成する必要がある．

2.3　対策変更に適応可能な監視ポリシの選定

異なる任意のリスクにおいて顕在化プロセスの一部が重複する場合があるため，リスクとセキュリティ事象の関係は多対多となる．本研究ではセキュリティ事象と監視ポリシの関係を 1 対 1 で扱うため，リスクと監視ポリシの関係は多対多となる．また，1 つの対策が複数のリスクに対し効果を発揮する場合があるため，リスクと対策の関係は多対多となる．

対策変更に柔軟に適応可能な監視を行うためには，リスク，監視ポリシ，対策の関係を体系的に表現しておく必要がある．

2.4　検出事象間の因果関係の特定

セキュリティ事象の発生主体や発生時刻の違いなどから，分析時におけるセキュリティ事象と検出時におけるセキュリティ事象の関係は 1 対多となる．そのため，一連のセキュリティ事象の発生の因果関係を特定するためには，因果関係の有無の判断方法や判断基準を決定しておく必要がある．

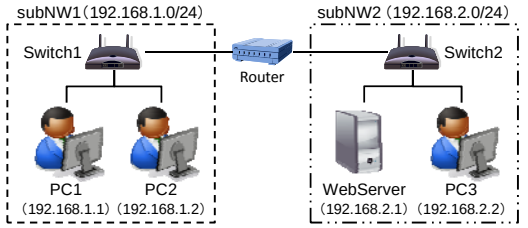

図 2　想定環境

表 1　対象リスク

ID	対象リスク
1	subNW1のPCによる，WebServer内のファイル改ざん
2	subNW1のPCによる，WebServerのアプリケーション停止
3	subNW2のPCによる，WebServer内のファイル改ざん
4	subNW2のPCによる，WebServerのアプリケーション停止

3.　対策変更に適応可能なネットワーク監視方式

2 章で挙げた課題と本章で述べるアプローチの関係を図 1 に示す．本方式では，状態遷移図と 7W1H を用いたリスク分析結果を利用し，監視ポリシを策定する．その監視ポリシに基づき，対象ネットワークからログやパケットを収集し，セキュリティ事象を検出する．そして，検出されたセキュリティ事象に対して相関分析を行い，インシデントを検出する．

3.1　リスク・対策表示モデルを用いたリスク分析

リスク顕在化プロセス，およびリスクと対策の関係を分析するために，リスク・対策表示モデルを利用したリスク分析を行う[6]．リスク分析の対象として想定したネットワーク構成を図 2 に，対象としたリスクを表 1 にそれぞれ示す．

図 2 および表 1 を対象として，状態遷移モデルを用いたリスク分析結果を図 3 に示す．なお，subNW1 の PC1 と PC2 はネットワーク構成やリスク顕在化プロセスが同一となるため，集約した．また，本研究ではインシデントとセキュリティ事象の関係を図 4 のように定義する．

このモデルではリスク顕在化までの手順を状態遷移図で表現するため，異なる任意のリスク間での顕在化プロセスの重複部分が結合できる．また，ネットワーク構成を

Vol.2011-DPS-146 No.24
Vol.2011-CSEC-52 No.24
2011/3/10

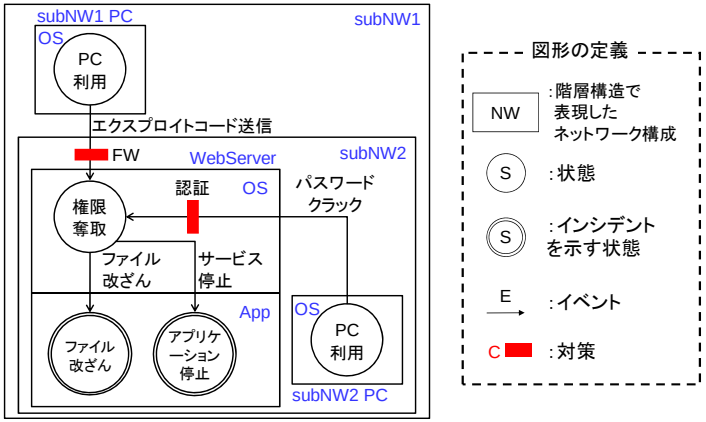

図 3　状態遷移モデルを用いたリスク分析結果の一例

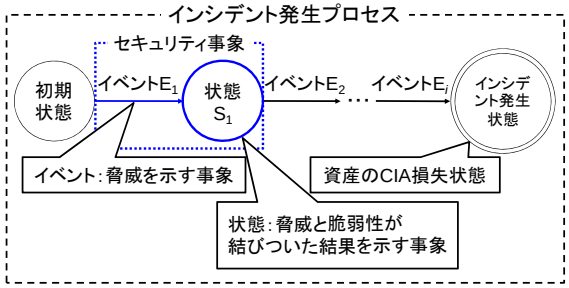

図 4　インシデントとセキュリティ事象の関係

階層構造で表現するため，セキュリティ事象の発生箇所や対策の実施箇所の正確な分析が可能となる．このように，状態遷移モデルを用いた分析を行うことで，リスクとセキュリティ事象，対策の関係の体系的な表現が可能となる．

3.2　7W1H を用いたリスク分析

セキュリティ事象の構成要素である“イベント”と“状態”を一意に識別するために，7W1H を用いたリスク分析を行う．文献 7)では，犯罪事実の調査における八何の原則に基づき,イベントと状態の一意識別のための情報を 7W1H として整理している．監視ポリシ導出に必要な情報を加え，再定義したイベントと状態における 7W1H を表 2 に示す．表 2 における値の定義域とは，イベントや状態の 7W1H の具体的な値が，値として取り得る可能性のある集合であり，データ型と同じ概念である．

表 2　イベントと状態における 7W1H の定義

		イベント	状態	値の定義域
誰が（人間）	Who	攻撃主体者（人間）	その状態を引き起こした人間	外部者，内部者，管理者
どのような権限で（システムの観点）	As who	・攻撃主体（システム） ・イベント実行時の権限	・その状態を引き起こしたシステム ・その状態時の権限状態	・送信元IP，送信元Port ・アカウント，システム権限
何に対して	To whom	攻撃客体（システム）	その状態におけるシステム	宛先IP，宛先Port， OS，アプリケーション，ファイル
何をした、何が起きた	What	何をした，何が起きた（行為）	何をした，何が起きた（結果）	故意，過失，事故
どのような経路で	Where	経由する層（領域）	発生する層（領域）	サーバ，PC，ネットワーク機器
いつ	When	イベント発生時刻	状態発生時刻	YY/MM/DD hh:mm:ss
どのようにして	How	実行方法	システムの観点での「状態」 （どのような状態になっているか）	バッファオーバーフロー， SQLインジェクション，DoSなど
どのような脆弱性を突いて	Why	利用されうる脆弱性	利用された脆弱性	対策が脆弱，存在しない， 対策の未実施

表 3　7W1H を用いたリスク分析結果の一例

7W1Hを用いたリスク分析結果

	値	定義域ID	値	定義域ID
ID	SecurityEvent1			
	Event1		State1	
Who	外部者	-	外部者or内部者	-
AsWho	subNW1のPCのIPアドレス（192.168.1.0/24）	1	any（IPアドレス）， any（アカウント名）/管理者権限	1
ToWhom	WebServerのIPアドレス（192.168.2.1）	3	WebServerのIPアドレス（192.168.2.1）	3
What	subNW1のPCによる， WebServerへのexploitコード送信	-	WebServerの 管理者権限が奪取された	-
Where	subNW1， subNW2， WebServer (OS)	-	WebServer (OS)	-
When	any	6	any	6
How	エクスプロイトコード送信	7	権限の昇格	11
Why	OSのパッチ未適用	-	OSの脆弱性，不適切な設定	-

定義域の一例

ID	7W1H	定義域
1	AsWho	送信元IPアドレス
2		アカウント/権限
3	ToWhom	宛先IPアドレス
4		アプリケーション
5		ファイル
6	When	YY/MM/DD hh:mm:ss
7	How（Event）	exploit
8		パスワードクラック
9		ファイル変更操作
10		アプリケーション停止操作
11	How（State）	権限昇格状態
12		ファイル変更状態
13		アプリケーション停止状態

As who，To whom，Where，When，How はそれぞれ実行主体，実行客体，発生箇所，発生時刻，発生方法を表わし，監視ポリシ策定の際に利用する．また，What は識別子の役割として利用する．一方，Who や Why は監視ポリシ策定の際に直接利用しない情報であるが，一意識別のために有用な情報と考え，取り入れた．例えば，端末を操作する人間（Who）が変化すると，セキュリティ違反となる場合がある．また，脆弱性（Why）が異なると，攻撃に対するシステムの状態が変化する場合がある．イベントと状態を一意に識別することで，インシデント発生プロセスの網羅的な特定や，漏れのないイベントや状態の検出の達成を図る．

図 3 の状態遷移モデルを用いたリスク分析結果に対応した，7W1H を用いたリスク分析結果の一部を表 3 に示す．

3.3　7W1H の分析結果に基づく監視ポリシの策定

(1)　監視対象データの特定

監視対象データを特定するための事前準備として，管理者が，対象ネットワークで

Vol.2011-DPS-146 No.24
Vol.2011-CSEC-52 No.24
2011/3/10

表 4　ログ・パケットの定義域および収集箇所の一例

ID	ログ・パケット名	AsWhoの定義域ID	ToWhomの定義域ID	Whenの定義域ID	Howの定義域ID	収集箇所	収集機器
1	Packet	1	3	6	7, 8	subNW1	Switch1
2	Packet	1	3	6	7, 8	subNW2	Switch2
3	OSLog	1, 2	3	6	-	WebServer(OS)	WebServer
4	AccountLog	-	-	6	11	WebServer(OS)	WebServer
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

表 5　シグネチャ定義およびアノマリ検出手法の一例

Signature定義

ID	Signature	Howの定義域ID
1	.ida	7
2	.idq	7
3	psss	8
4	FileWrite	9
5	ApplicationStop	10

Anomaly検出手法例

ID	検出手法	評価値	Howの定義域ID
1	管理者権限のアカウント数の監視	管理者権限のアカウントの増加	11
2	異なる時点におけるファイルのハッシュ値比較	ファイルのハッシュ値が異なる	12
3	サービスの稼働状況の監視	サービスの停止	13

収集可能なログ・パケットの「種類」「取得可能な内容の定義域」「収集箇所および機器」について整理しておくこととする．

ログ・パケットの情報の具体例を表 4 に示し，表 3 の Event1 を例に，監視対象データ特定の流れを述べる．Event1 の Where の値（subNW1，subNW2，WebServer（OS））と，ログ・パケットの収集箇所を対応付け，一致する値として，Packet（ID2），OSLog，AccountLog を抽出する．次に，抽出されたログ・パケットの 3W1H（As who, To whom, When，How）の定義域と，Event1 の 3W1H の定義域を対応付け，3W1H すべてを特定可能なログ・パケットを抽出する．以上から，Event1 における監視対象データ，監視箇所はそれぞれ，Packet，Switch1 となる．なお，監視対象データとなるログ・パケットは複数種類となる場合もある．

(2) 検出手法の決定

イベントは手順や発生パターンを事前に定義し易いため，シグネチャ型検出手法を用いて検出する．一方，状態は任意の状態への遷移を検出する必要があるため，アノマリ型検出手法を用いて検出する．

検出手法を決定するための事前準備として，管理者が，シグネチャの「値」「定義域」や，アノマリ検出手法の「手法」「評価値」「定義域」を整理しておくこととする．

シグネチャやアノマリ検出手法の具体例を表 5 に示し，表 3 の Event1 を例に，検出手法決定の流れを述べる．Event1 の How の定義域（exploit）と，シグネチャの定義域を対応付け，一致する値として，.ida, .idq を抽出する．また，2W1H（As who, To whom, When）の値をログ・パケットが取り得る値の形式に変換する．抽出されたシグネチャと，変換された 2W1H の値の組を検出手法とする．表 3 の 7W1H のリスク分析結果に基づき，生成した監視ポリシを表 6 に示す．

表 6　7W1H の分析結果に基づき生成した監視ポリシ

対象事象ID		SecurityEvent1		SecurityEvent2	
		Event1	State1	Event2	State1
検出手法	AsWho	192.168.1.0/24	any(IPAddress), any(Account)/root	192.168.2.0/24	any(IPAddress), any(Account)/root
	ToWhom	192.168.2.1	192.168.2.1	192.168.2.1	192.168.2.1
	When	any	any	any	any
	How	.ida, .idq	管理者権限のアカウントの増加	psss	管理者権限のアカウントの増加
監視箇所	AsWho	Packet	OSLog	Packet	OSLog
	ToWhom	Packet	OSLog	Packet	OSLog
	When	Packet	OSLog	Packet	OSLog
	How	Packet	AccountLog	Packet	AccountLog
	device	Switch1	WebServer	Switch2	WebServer

対象事象ID		SecurityEvent3		SecurityEvent4	
		Event3	State2	Event4	State3
検出手法	AsWho	any(Account)/root	any(Account)/root	any(Account)/root	any(Account)/root
	ToWhom	File	File	Application	Application
	When	any	any	any	any
	How	FileWrite	ファイルのハッシュ値が異なる	ApplicationStop	サービスの停止
監視箇所	AsWho	FileAccessLog	FileHashLog	CmdLog	ProcessLog
	ToWhom	FileAccessLog	FileHashLog	CmdLog	ProcessLog
	When	FileAccessLog	FileHashLog	CmdLog	ProcessLog
	How	FileAccessLog	FileHashLog	CmdLog	ProcessLog
	device	WebServer	WebServer	WebServer	WebServer

なお，ログ・パケットが取り得る値は，7W1H における As who，To whom，When，How のみであるため，監視ポリシの作成においては 3W1H のみを扱うこととした．

(3) 監視ポリシの選定

図 3 に基づき，リスク，監視ポリシ，対策の関係を整理したものを図 5 に示す．本方式では，監視対象のリスクを構成するセキュリティ事象を特定し，それら事象に対応した監視ポリシを，監視運用の際に用いるポリシとして選定する．例えば，リスク 1 を監視対象とした場合，監視ポリシ P_1 と P_3 が選定される．

また，対象ネットワークにおいて対策が変更された場合，監視ポリシを見直す必要がある．例えば，運用されていた FW を停止させる状況があった場合，FW に関連するリスク 1 とリスク 2 が抽出され，それらのリスクを監視対象，もしくは非監視対象に変更することができる．

3.4 状態遷移モデルに基づく相関分析

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，事象間の 7W1H の値の変化に注目した相関分析を行う．相関分析の流れを図 6 に，相関分析に用いるルールを表 7 にそれぞれ示す．

本方式における相関分析では，まず監視運用により検出されたイベント・状態の中

Vol.2011-DPS-146 No.24
Vol.2011-CSEC-52 No.24
2011/3/10

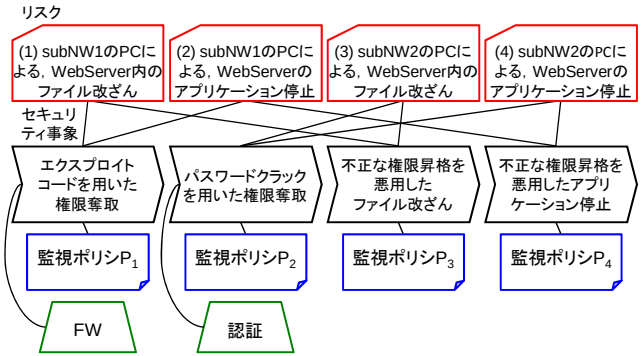

図 5　リスク，監視ポリシ，対策の関係

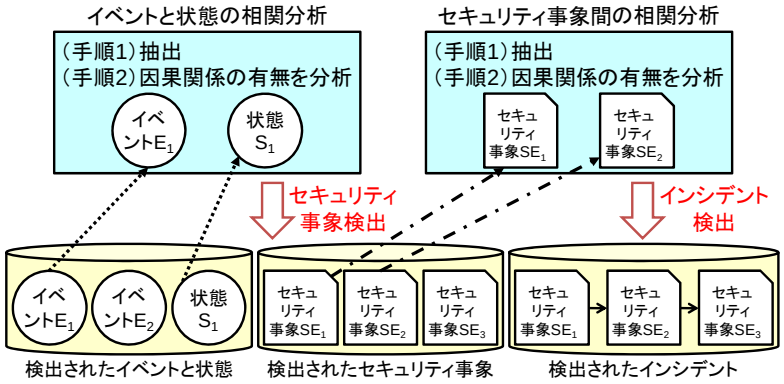

図 6　状態遷移モデルに基づく相関分析手法

から，因果関係の分析対象とするイベントと状態を抽出する．そして，イベントと状態の分析のために定めた相関分析ルールを用い，因果関係の有無を分析する．因果関係が有ると判断した場合はセキュリティ事象として検出する．セキュリティ事象間の相関分析も同様の手順で行う．一連のセキュリティ事象の発生に因果関係が有ると判断した場合に，インシデントとして検出する．

4.　プロトタイプシステムの開発

本方式の実現可能性，および 2 章で述べた課題達成の検証のため，プロトタイプを開発した．開発言語には Microsoft Visual Studio 2008 C++，データベースには MySQL Community Server 5.1.51 をそれぞれ使用した．本システムの構成を図 7 に示す．

表 7　相関分析に用いるルール

	イベントと状態の相関分析ルール	セキュリティ事象間の相関分析ルール
Who	–	–
AsWho	SourceValue=DestinationValue	SourceStateValue=DestinationEventValue
ToWhom	SourceValue=DestinationValue	–
What	–	–
Where	–	SourceStateValue=DestinationEventValue
When	SourceValue<DestinationValue AND DestinationValue-SourceValue<00:01:00	SourceStateValue<DestinationEventValue
How	–	–
Why	–	–

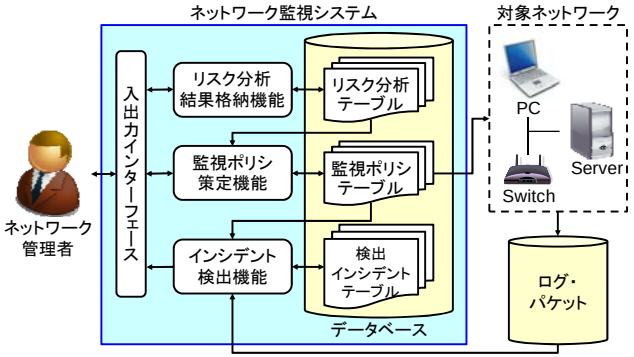

図 7　システム構成

4.1　リスク分析結果格納機能の実装

(1)　状態遷移モデルを用いたリスク分析結果の格納

管理者から入力されるリスク名，リスクを構成するセキュリティ事象およびその順序関係，セキュリティ事象名，セキュリティ事象を構成するイベントと状態，ネットワーク構成に関する情報をリスク分析テーブルに格納する．

(2)　7W1H を用いたリスク分析結果の格納

管理者から入力されるイベントや状態の 7W1H を用いた分析結果や，定義域に関する情報をリスク分析テーブルに格納する．イベントに関する入出力画面を図 8 に示す．

(3)　リスクと対策の関係の格納

管理者から入力される対策名，実施箇所，効果のあるイベントに関する情報をリスク分析テーブルに格納する．

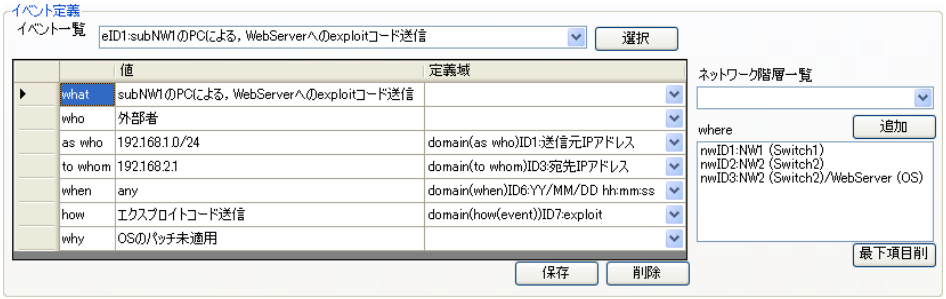

図 8　7W1H を用いたリスク分析結果の入出力

図 9　対策変更に影響のあるリスクの提示

4.2　監視ポリシ策定機能の実装

(1)　監視ポリシ生成のための定義情報の格納

管理者から入力されるログ・パケット，およびシグネチャ，アノマリ検出手法に関する情報を監視ポリシテーブルに格納する．

(2)　監視ポリシの生成

データベースに格納されている定義情報と 7W1H によるリスク分析結果から，3.3 節で述べた方式と同様の流れで監視ポリシを生成する．

(3)　対策変更に適応した監視ポリシの選定

管理者により監視対象とされたリスクから，監視運用に用いる監視ポリシを選定する．また，対策を変更した際に，影響のあるリスクを提示する．対策変更に影響のあるリスクの提示画面を図 9 に示す．

(4)　相関分析ルールの設定

管理者により設定される，イベントと状態，およびセキュリティ事象間に用いる相関分析ルールを監視ポリシテーブルへ情報を格納する．

4.3　インシデント検出機能の実装

(1)　イベントおよび状態の検出

監視ポリシに基づいて収集されるログ・パケットと，検出手法のそれぞれの As who,

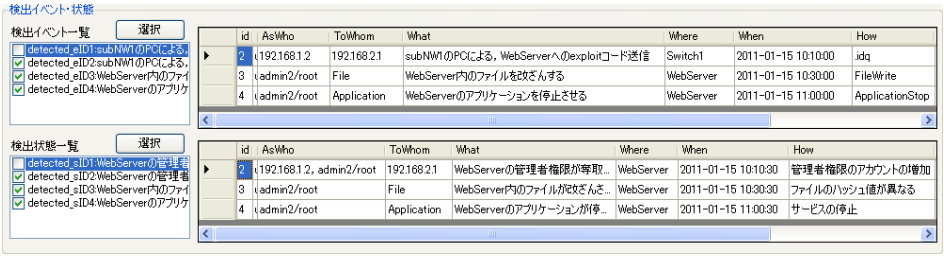

図 10　イベントおよび状態の検出結果

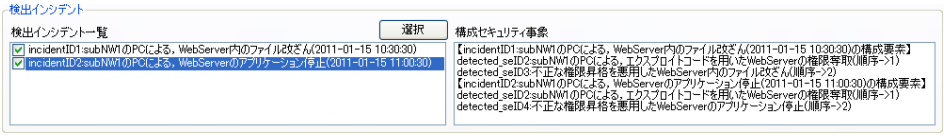

図 11　インシデントの検出結果

To whom，When，How をパターンマッチングさせることにより，イベントや状態を検出する．イベントと状態の検出結果画面を図 10 に示す．

(2)　セキュリティ事象およびインシデントの検出

3.4 節で述べた方式と同様に，検出されたイベントや状態，セキュリティ事象に対し，相関分析ルールを適用し，セキュリティ事象，インシデントを検出する．インシデントの検出結果画面を図 11 に示す．

5.　仮想データを用いた実験

5.1　実験概要

(実験 1)　ネットワーク監視導入を想定した実験

実験 1 ではインシデントおよびその発生経路を特定できるかどうかを検証する．図 2 を実験の想定環境，表 1 を対象リスクとする．また，実験用に想定したデータを表 8 に示す．PC1 はセキュリティ事象，PC2 はインシデント ID1 および ID2 を発生させ，PC3 は正規利用を行う．表 8 のデータに基づき，実験用に作成した仮のログ・パケットを表 9 に示す．なお，ログ・パケットは便宜上，4W1H の形式に正規化している．

(実験 2)　セキュリティ対策の変更を想定した実験

実験 2 では対策変更に対する監視の切り替えが行えるかどうかを検証する．想定環境と対象リスクは実験 1 と同一とする．また，実験用に想定したデータと，ログ・パケットをそれぞれ表 8，表 9 に示す．対策と監視状況の違いによる結果を網羅的に検

Vol.2011-DPS-146 No.24
Vol.2011-CSEC-52 No.24
2011/3/10

表 8　実験で想定したデータ

実験において発生させるインシデント

実験番号	ID	インシデント名
実験1，実験2	1	subNW1のPCによる，WebServer内のファイル改ざん
実験1	2	subNW1のPCによる，WebServerのアプリケーション停止

実験用に想定したデータ

実験番号	実行機器	手順1	手順2	手順3
実験1	PC1（subNW1）	WebServerにexploitコードを送信し，管理者権限を奪取	－	－
実験1，実験2（実験2は手順2まで）	PC2（subNW1）	WebServerにexploitコードを送信し，管理者権限を奪取	WebServer内のファイルを改ざん	WebServerのアプリケーションを停止
実験1	PC3（subNW2）	WebServerに一般権限でログイン	WebServer内のファイルに追記	－

実験2における監視状況のケース

ケース番号	FW停止前	FW停止後
1	インシデントID1は非監視対象	インシデントID1は非監視対象
2	インシデントID1は非監視対象	インシデントID1は監視対象
3	インシデントID1は監視対象	インシデントID1は非監視対象
4	インシデントID1は監視対象	インシデントID1は監視対象

証するため，想定環境で運用されている FW を停止させる状況を想定し，FW 停止前と停止後において関連インシデント ID1 を監視対象・非監視対象とする．

5.2　実験方法

(1)　リスク分析とシステム設定

想定環境（図 2）における対象リスク（表 1）について，状態遷移モデルおよび 7W1H を用いたリスク分析を行う．次に，本システムに対し，リスク分析結果と，監視ポリシの事前定義情報であるログ・パケットの定義域と収集箇所，検出方法を入力する．そして，監視ポリシを導出する．最後に，監視対象とするインシデントを決定する．

(2)　インシデント検出

監視対象としたインシデントから選定された監視ポリシ，および想定ログ・パケット（表 9）をパターンマッチングさせ，イベントと状態を検出する．そして，検出されたイベントや状態，またセキュリティ事象に対し，相関分析ルール（表 7）を適用することで，セキュリティ事象およびインシデントを検出する．

5.3　実験結果

(1)　リスク分析結果と導出された監視ポリシ

図 2 および表 1 に対して，リスク分析結果はそれぞれ図 3，表 3 のようになった．このリスク分析結果に対応して，監視ポリシの事前定義情報を表 4，表 5 のように設定した．この結果，本システムが導出した監視ポリシは表 6 のようになった．

(2)　実験 1，実験 2 におけるインシデント検出結果

実験 1 における実験結果は図 10，図 11 のようになった．図 10 はイベントと状態，図 11 はインシデントの検出結果である．実験 1 ではインシデント ID1 および ID2 を検出した．また，インシデント ID1 および ID2 の発生主体を PC2 と特定した．

実験 2 ではケース番号 2 および 4 においてインシデント ID1 を検出し，ケース番号 1 および 3 においてインシデントは検出されなかった．

表 9　実験用に想定し，操作ごとに分類したログ・パケット

操作	PC1(subNW1)：WebServerにexploitコードを送信し，管理者権限を奪取			PC3(subNW2)：WebServerに一般権限でログイン			PC3(subNW2)：WebServer内のファイルに追記	
Log・Packet	Packet	OSLog	AccountLog	Packet	OSLog	AccountLog	FileAccessLog	FileHashLog
収集機器	Switch1	WebServer	WebServer	Switch2	WebServer	WebServer	WebServer	WebServer
AsWho	192.168.1.1	192.168.1.1, admin1/root	-	192.168.2.2	192.168.2.2, guest/user	-	guest/user	guest/user
ToWhom	192.168.2.1	192.168.2.1	-	192.168.2.1	192.168.2.1	-	File	File
When	2011-01-15 10:00:00	2011-01-15 10:00:30	2011-01-15 10:00:30	2011-01-15 10:20:00	2011-01-15 10:20:30	2011-01-15 10:20:30	2011-01-15 10:40:00	2011-01-15 10:40:30
How	.ida	login	管理者権限のアカウントの増加	syn	login	一般権限のアカウントの増加	FileWrite	ファイルのハッシュ値が異なる

操作	PC2(subNW1)：WebServerにexploitコードを送信し，管理者権限を奪取			PC2(subNW1)：WebServer内のファイルを改ざん		PC2(subNW1)：WebServerのアプリケーションを停止	
Log・Packet	Packet	OSLog	AccountLog	FileAccessLog	FileHashLog	CmdLog	ProcessLog
収集機器	Switch1	WebServer	WebServer	WebServer	WebServer	WebServer	WebServer
AsWho	192.168.1.2	192.168.1.2, admin2/root	-	admin2/root	admin2/root	admin2/root	admin2/root
ToWhom	192.168.2.1	192.168.2.1	-	File	File	Application	Application
When	2011-01-15 10:10:00	2011-01-15 10:10:30	2011-01-15 10:10:30	2011-01-15 10:30:00	2011-01-15 10:30:30	2011-01-15 11:00:00	2011-01-15 11:00:30
How	.idq	login	管理者権限のアカウントの増加	FileWrite	ファイルのハッシュ値が異なる	ApplicationStop	サービスの停止

6.　考察

6.1　インシデント発生プロセスを特定可能なシナリオ分析の達成検証

5.3 節のリスク分析結果から，不正アクセスの手順が明確な範囲において，インシデント発生プロセスを特定可能なシナリオ分析が行えたことを確認した．

図 3 において，実際のネットワーク環境と対応した分析や，異なる任意のインシデントにおける発生プロセスの重複部分の結合，またインシデント発生プロセスに対する対策のマッピングを行い，リスク分析の不整合を発見や修正ができた．また，表 3 において，イベントや状態に対して 7W1H を用いたリスク分析を行い，イベントや状態が一意に識別可能かどうかを検証し，状態遷移モデルにおけるリスク分析結果の見直しや修正ができた．

6.2　セキュリティ事象に応じた監視ポリシの作成の達成検証

5.3 節の監視ポリシの導出結果から，セキュリティ事象に応じた監視ポリシの作成が行えたことを確認した．

表 3 において，セキュリティ事象の性質を 7W1H として分解，整理した結果，監視

Vol.2011-DPS-146 No.24
Vol.2011-CSEC-52 No.24
2011/3/10

対象データや検出手法の決定に必要となる要素を特定することができた．また，表 4，表 6 において，7W1H を用いた分析結果と対応した，ログ・パケットに関する情報の整理方法を定義した結果，監視対象データを体系立てて特定することができた．さらに，表 5，表 6 において，7W1H を用いた分析結果と対応した，シグネチャ，アノマリ型検出手法に関する情報の整理方法を定義した結果，検出手法を体系立てて決定することができた．

6.3 対策変更に適応可能な監視ポリシの選定の達成検証

5.2 節のシステム設定および 5.3 節のインシデント検出結果から，対策変更に適応可能な監視ポリシの選定が行えたことを確認した．

図 5 において，リスク，監視ポリシ，対策の体系的な表現を行った結果，監視対象とするリスクの顕在化を検出するために必要な監視ポリシを選定することができた．また，対象ネットワークで対策変更が生じた際に，影響のあるリスクを特定でき，監視対象リスクの変更に即した監視ポリシの変更を行うことができた．

実験 2 の結果から，対策変更に対する監視ポリシの切り替えの実現が期待できる．

6.4 検出事象間の因果関係の特定の達成検証

実験 1 では，PC1 と PC2 を図 3 の状態遷移モデルにおける「権限奪取」という状態に共に遷移させ，インシデントの発生主体を混在した．また，PC2 を「権限奪取」の状態から，「ファイル改ざん」「アプリケーション停止」の順に 2 つの状態に遷移させ，インシデント発生プロセスを分岐した．さらに，PC3 に Web サーバ内のファイル内容を変更させ，正規利用とインシデント発生を混在した．

実験 1 の結果から，本システムがインシデントの発生主体の違いや，同一主体によるインシデントの分岐，また正規利用とインシデントの違いを認識できたことを確認した．このことから，本システムがインシデントの発生経路を正確に捕え，過不足なくインシデントを検出できる見通しを得た．

7. 今後の課題

7.1 実環境における適用実験

実際のログやパケットを対象とした実験を行い，本システムが実環境においても過不足なくインシデントが検出できるかどうかを検証する．また，対策変更に対する監視ポリシの切り替えが実現できるかどうか，また監視ポリシ変更によるログ・パケットの取りこぼしや，検出手法の適用漏れが生じるかどうかを検証する．

ネットワーク監視の運用中，検出手法の数やログ・パケットの量が多くなると，本システムの処理が追いつかない可能性が考えられる．そこで，多量のトラフィック状況における，本システムの即時性や検出漏れに関するパフォーマンス測定も行う．

7.2 ネットワーク環境に応じた相関分析ルールの決定

本稿では，イベントと状態，およびセキュリティ事象間の相関分析ルールを表 8 のように定義した．しかし，相関分析のルールは対象とするネットワーク環境によってカスタマイズしなければならない．そこで，汎用的，もしくは体系的な相関分析手法を検討する．

7.3 リスク分析における網羅性の確保

リスク顕在化プロセスを過不足なく特定するためには，セキュリティ事象に関する粒度を定める必要がある．リスク分析に用いた 7W1H は粒度を決定する一要素であるが，7W1H による分析がイベントと状態を一意に識別する十分条件であることは示さなかったため，今後検討する必要がある．さらに，この課題の解決は，相関分析手法の発展にも繋がると期待できる．

8. まとめ

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，対策変更に適応可能な監視箇所と検出手法の決定，および状態遷移モデルに基づく相関分析手法を述べた．また，本方式に基づくプロトタイプを実装し，仮想データを用いた実験を通して，インシデントおよびその発生経路を自動的に特定し，かつ対策変更に対する監視の切り替えを実現できる見通しを得た．

今後は 7 章で述べた課題に取組み，実環境のネットワークにおいて，対策変更に適応可能なインシデント検出システムの実現を目指していく．

参考文献

1) 和泉勇治，廣瀬淳一，角田裕，根元義章：相関係数発生確率行列を利用したネットワーク状態評価方式，電子情報通信学会論文誌 B，Vol.J90-B，No.7，pp.660-669，2007.7
2) 野口大輔，白石善明，栗林稔，桑門秀典，森井昌克：時系列上でのイベント依存モデルに基づく被害予測システムの開発，情報処理学会 CSS2005 論文集，Vol.2005，pp.151-156，2005.10
3) 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
4) 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，情報処理学会 CSS2007 論文集，Vol.2007，No.10，pp.193-198，2007.11
5) ISO/IEC 27001：2005
6) 加藤弘一，勅使河原可海：事象連鎖の把握と原因推測が可能なリスク・利便性・対策表示モデルの提案，情報処理学会論文誌，Vol50，No.9，pp.2243-2256，2009.9
7) 加藤弘一，濱口昌宏，西村啓渡，間形文彦，西垣正勝，佐々木良一，勅使河原可海：訴訟対応のためのイベントと状態に基づく取得情報と相関分析の検討，情報処理学会 DICOMO2010 シンポジウム，pp.206-212，2010.7