アウトソース型セキュリティセンタにおける インシデント対応迅速化のためのアラートログ可視化システム

岩崎 信也[†1], 角田 朋[†1], 関口 悦博[†1], 大鳥 朋哉[†2], 薦田 憲久[†3]

概要：ファイアウオールや侵入検知システムなどセキュリティ機器のアラートを調査するインシデント対応の効率化のための支援システムを提案する。アラートの調査ではアラートの形式がセキュリティ機器により異なることや調査のための集計処理の作成、アラートの発生の流れを把握するための整形などに時間を要している。本研究ではアラートを統一的な形式に変換し、検知元とアラート間の時間間隔により 2 段階に構造化することで局所的な発生と継続的な発生を分かりやすく可視化する。さらに集計処理を標準的な事前集計とリクエスト集計に分け実行する。提案システムの試行の結果、既存システムであるコマンド入力による調査に比べ、分析官による入力回数を 77%削減、必要時間を 56%削減できた。

キーワード：サイバーセキュリティ、可視化、SOC、アラート、インシデント対応

1. はじめに

近年、企業や公的機関などのサイバーセキュリティは重要度を増しており、インシデント対応の迅速化が求められている。ここでのインシデントとは、セキュリティインシデントを意味し､「情報システムの運用におけるセキュリティ上の問題として捉えられる事象」を指す [1]。例として情報流出や不正アクセス・WEB 改ざんなどがある。インシデント対応ではインシデントの疑いが検出された際に優先度の決定や、対応が必要かを判定するトリアージが重要となる。トリアージではセキュリティ機器が発生させるアラートを調査する。しかしアラート調査では、アラートの形式がセキュリティ機器により異なることや調査のための集計コマンドの作成、発生アラートの流れを把握するための整形などに時間を要し迅速化の妨げとなっている。

本研究ではアラート調査のための支援システムを提案する。このシステムでは、異なるアラート形式を統一的な形式に変換する。アラートを検知元とアラート間の時間間隔により、2 段階に構造化させることで局所的な発生と継続的な発生を分かりやすく可視化する。また、調査に必要な標準的な集計処理をアラート発生時に事前処理する。必要があればインシデント対応を担当する分析官が簡単なフォームで集計処理を実行できる。

2. インシデント対応

2.1 SOC/CSIRT

インシデント対応とは、インシデントを検知した際に優先度判定・事象分析・対応計画や障害復旧を行うことである。インシデント対応は SOC(Security Operation Center)や CSIRT(Computer Security Incident Response Team)と呼ばれる組織が担当する。

狭義には SOC はファイアウオールや侵入検知システム (IDS : Intrusion Detection System)等のセキュリティ機器を監視・運用し、インシデントを検知する。対して CSIRT は検知されたインシデントに対応する。しかし昨今は一つの組織で双方を実施することが多く、その境界線は曖昧となる [2]。このため、本稿では統一的に SOC とする。

また、SOC の形態は大きく二種類ある。

(1) 社内 SOC

社内 SOC は、監視対象の企業内に設置され自社のセキュリティを監視する。アウトソース型 SOC に比べて規模が小さく、監視するセキュリティ機器も限られる。

(2) アウトソース型 SOC

アウトソース型 SOC は、IT 企業などから SOC サービスとして提供されており、他企業のセキュリティを監視する。アウトソース型 SOC は、さまざまな企業のセキュリティを監視するため、規模が大きく対象のセキュリティ機器の種類も多い。

2.2 インシデント対応フロー

インシデント対応の標準的な流れは図 1 のとおりである [3]。

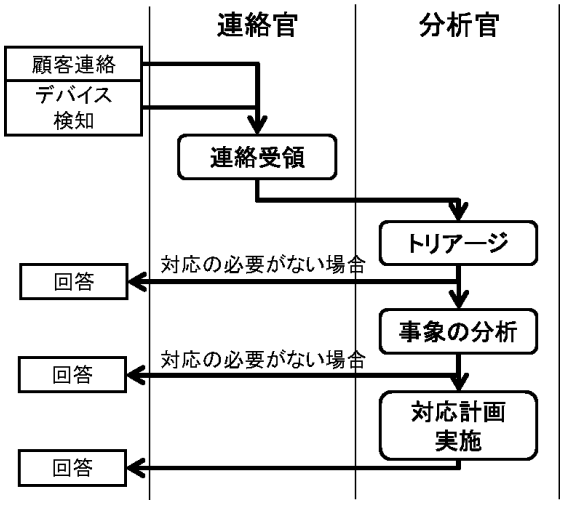

図 1 インシデント対応フロー

†1 株式会社日立システムズ 研究開発本部
Hitachi Systems, Ltd. Research & Development Division
†2 株式会社日立システムズ ネットワークセキュリティサービスグループ
Hitachi Systems, Ltd. Network Security Services Division
†3 コーデソリューション株式会社
Code Solution K.K.

インシデント対応は、セキュリティ機器によるインシデントの検出・発見者や専門組織からの連絡により開始される。

(1) 連絡受領

検知や連絡を受けた際に、連絡官がその情報を確認しインシデントとして起票する。

(2) トリアージ

トリアージは、起票されたインシデントの優先度を判断し、対応が必要かを決定する。誤検知などインシデントではなかった場合や優先度が一定以下の場合などは対応の必要がないと判断する。

この優先度の決定のためには、起票情報だけでは足りず、追加情報の調査が必要となる。追加情報の調査は下記の順となる。

i. 対応表・過去事例調査

事前に決められた対応表や過去に対応した同様の事例を調査する。同様事例が存在する場合、同じように対応することが多い。

ii. セキュリティ機器のアラート調査

アラートは何らかのサイバー攻撃などの疑いが発生した際にセキュリティ機器によって生成され、具体的な攻撃情報などが含まれている。詳細を 2.3 項に記述する。

iii. ネットワークトラフィックのログ調査

アラート調査で疑いが残る場合、プロキシなどのネットワークトラフィックを調査する。

(3) 事象分析

セキュリティ侵害が起きたことを前提に被害の把握や侵害範囲を切り分ける。マルウェアの感染が疑われる PC の詳細な解析やフォレンジック作業を行う。この作業では実環境を模擬した調査環境を構築し、感染したマルウェアを実行し侵害内容を分析する。さらにネットワークトラフィックを一つずつ分析して感染の広がりを確認することで侵害の全容を明らかにする。

(4) 対応計画/実施

事象分析の結果を元に、障害の復旧や情報流出への対応再発防止策などを計画し、実施する。

2.3 アラート調査

アラート調査ではセキュリティ機器が発生させるアラートを調査する。調査はイベント調査と統計調査に分かれる。

(1) イベント調査

イベント調査では起票情報を基に発生したアラートを調査する。主な調査項目は下記のとおりである。

・日付
・検知元 IP (Internet Protocol address)
・検知ルール
・検知先 IP
・遮断判定
・重要度

起票に関連したアラートを調査し不審な点がないか確認する。いつ発生したかではなく、局所的もしくは継続的なアラートの流れが重要となる。

i. 局所的発生

時間的な間隔がなく連続して発生しているアラートを調査する。特に複数の検知ルールによってアラートが発生している場合は、意図を持った攻撃の可能性が高いとされる。例えば、公開ウェブページに対する攻撃などがある。この場合、SQL インジェクションやディレクトリトラバーサル、不正ログインの試み・ポートスキャンなど複数ルールによるアラートが連続して検知される。

ii. 継続的発生

継続的に発生しているアラートを調査する。長期間にわたり継続的に発生している場合は、端末がマルウェアに感染し、情報を送信している可能性などが挙げられる。また、標的型攻撃などは検知を逃れるため、長期間にわたり攻撃する。これらのインシデントの発見のため、長期間にわたり同一の検知元もしくは攻撃元に関係するアラートが発生していないかを調査する。

(2) 統計調査

統計調査では、アラート数などの時間的遷移を調査し、突発的な変動が発生していないか確認する。

アラート調査の標準的な調査工程は、図 2 のとおりである。

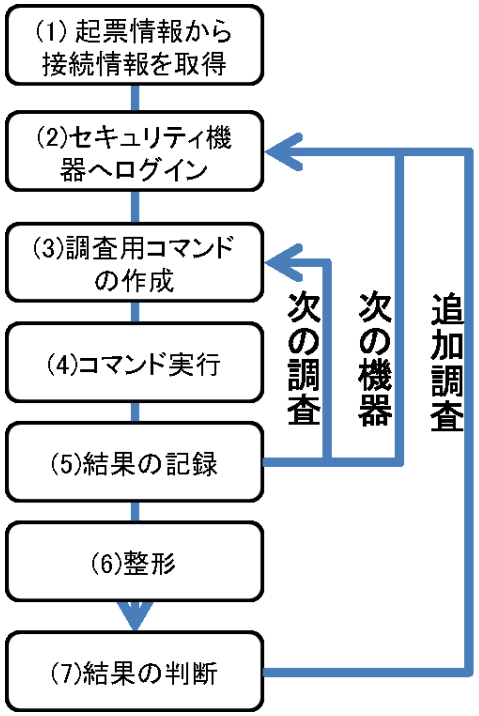

図 2 アラート調査手順

(1) 起票情報に関係するセキュリティ機器のアラート

調査に必要なログイン情報を取得する。

(2) 対象のセキュリティ機器にログインする。

(3) 調査項目のコマンドを作成する。

(4) 作成したコマンドを実行する。

(5) 結果を表計算ツールなどに記録する。

調査する IP が複数ある場合や複数の時間帯を調べる必要がある場合、 (3)から繰り返す必要がある。対象の機器が複数の場合は、接続機器を変更して(2)から繰り返す。

(6) 記録した結果を人が判断しやすいように整形する。

(7) 結果から、重要度や対応を判断する。判断に必要な情報が不足していた場合、追加で調査する。

2.4 アラート調査の問題点

アラート調査では下記の問題点により時間を要しており課題となる。

(1) セキュリティ機器によりアラート形式が異なる [4]。

種類やメーカーが違うセキュリティ機器のアラートは構造や項目名などの形式が異なる。特にアウトソース型 SOC では多種のセキュリティ機器を監視しており、アラート調査のためのコマンドが多岐にわたり作成に時間を要する。

(2) 調査項目毎にコマンドを作成する必要がある。

アラートの調査項目つどに対応したコマンドを作成しなければならない。例えば一定期間内のアラート発生の検知元などを調査する場合、検知元をリストアップし、検知元の数だけコマンドを作成・実行する必要がある。

(3) 局所的・長期的なアラート発生の調査に整形を必要とする。

局所的な検知の流れを確認するために、アラートリストを分析官は解釈しやすいように表計算ツールなどで整形する必要がある。

3. 提案システム

3.1 システム概要

本研究では、分析官によるアラート調査の支援システムを提案する。

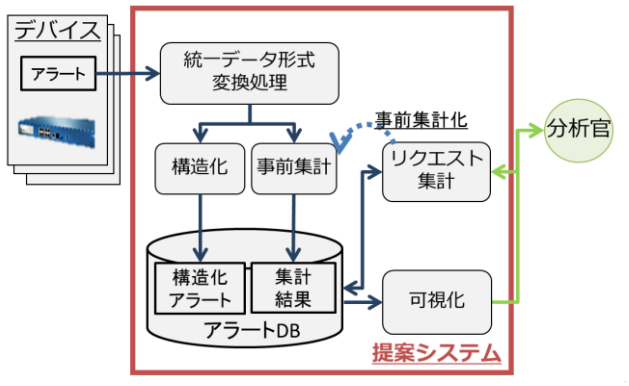

図 3 システム構成図

このシステムでは、形式が異なるアラートを統一的な形式に変換し、検知元 IP とアラート間の時間間隔により構造化する。また、集計処理を二つに分け、標準的な集計はアラート発生時に事前に処理する。他の集計が追加で必要となった場合、専用のフォームからリクエストできる。分析官は調査結果を WEB 上で好きなように配置可能であり、担当範囲により必要な結果のみ表示できる(図 4)。

図 4 提案システムの可視化結果

3.2 統一的データ形式への変換方式

形式が異なるアラートに対応するため統一的データ形式を定義する。統一的データ形式は表 1 となる。

表 1 統一的データ形式

	key	項目名
共通部	logtype	アラートの種類
	time	アラート発生時刻
	devid	機器識別番号
	srcip	検知元 IP
	srcport	検知元ポート
	dstip	検知先 IP
	dstport	検知先ポート
	severity	重要度
	attack	検知ルール
	protocol	通信プロトコル
	action	アクション結果
custom		カスタム部(スキーマレス)

統一的データ形式は共通部とカスタム部に分かれている。共通部は、セキュリティ機器のアラートの標準的な項目を持つ。カスタム部には共通化できない項目を格納する。このためカスタム部はスキーマレスな構造となる。

アラートの統一的データ形式への変換は定義ファイルで設定可能とし、負担が少なくアラート形式を追加できる。

3.3 コマンドの削減方法

コマンドの作成時間を削減するため、二つの方法をとる。

一つ目は事前集計であり、アラート調査に必要な標準的な集計をアラート発生時に事前に集計する。主に統計調査に必要な調査項目別の集計を行う。

二つ目はリクエスト集計である。分析官は必要になった際に WEBUI から簡単なフォーム入力で条件を設定し集計する。主にキーワードベースの抽出や指定の期間での集計に利用される。リクエスト集計では、一度実行した集計処理はテンプレートとして記録される。再度実行する際は条件の再入力が不要になり効率的に集計が可能となる。また、テンプレート化した集計処理は集計タイミングをアラート発生時(事前集計)に設定できる。これによりリクエスト集計の実行時に計算時間が削減され、複雑な条件や大規模なデータに対する処理では高速化が望める。例えば特定のサイバー攻撃の世界的流行や特定 IP からの長期的な攻撃の際に、テンプレート化して事前集計に設定することで、テンプレート化しない場合に比べ計算時間の削減が期待できる。

3.4 アラートの構造化

局所的なアラートと継続的なアラートをわかりやすく可視化するために、提案システムではアラートを二段階に構造化する。

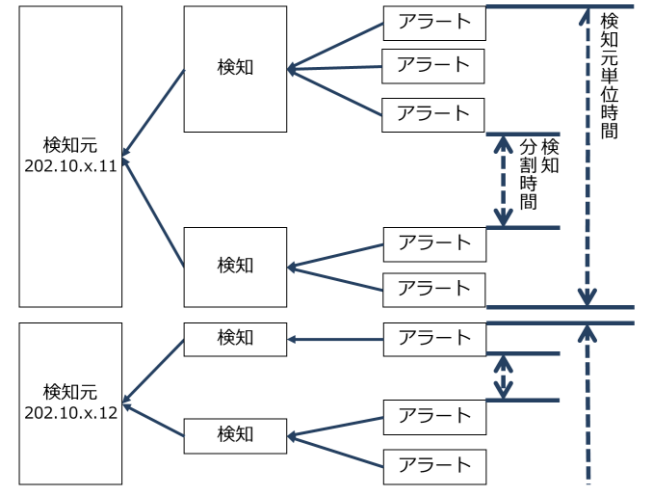

図 5 アラートの構造化モデル

図 5 はアラートの構造化モデルである。同一検知元 IP のアラートで、アラート間の時間間隔が一定以下の場合に一つの「検知」として関連付ける。複数の「検知」は一定時間ごとに「検知元」と関連付けられる。

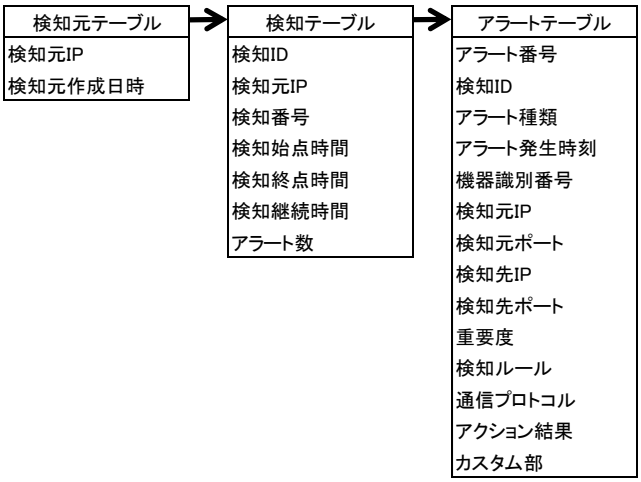

図 6 構造化したアラートの論理スキーマ

図 6 はアラートを構造化した際の論理スキーマである。

(1) アラートテーブル

アラートテーブルには、一意な ID を付与されたセキュリティ機器のアラートが統一的データ形式で格納される。

(2) 検知テーブル

検知テーブルには、ネットワーク識別情報、一意な ID と検知回数を表す検知番号、検知の始点・終点時間・継続時間、関連付けられているアラートの数を格納する。検知テーブルは、アラートテーブルと検知 ID によって関連付けが行われる。

(3) 検知元テーブル

検知元テーブルには、検知元 IP とネットワーク識別番号、検知元作成日付を格納する。検知元テーブルは検知テーブルと検知元 IP によって関連付けられる。

図 7 構造化アラートの可視化画面
(検知元 IP・検知先 IP はマスキング済み)

図 7 は構造化したアラートの可視化画面である。「検知」毎にアラートを分割して可視化しており、単純にアラートを一覧で表示するよりも、局所的なアラートの数やアラー

トの流れを分析官が確認しやすい。

4. 評価

評価として提案システムを試行し、既存システムと入力回数・アラート調査に要した時間を比較した。ここでの既存システムとは、図 2 のとおりセキュリティ機器のログをコマンドベースで検索するためのシステムを指す。

4.1 入力回数の比較

過去のアラート調査事例 11 件を元に既存システムと提案システムでの入力回数を比較した。SOC における既存システムのコマンド入力ログを元に、提案システムで同様の調査結果を確認できるまでを模擬し、その入力回数を記録した。

それぞれの入力回数は下記のとおりである。

既存システム(コマンド)	一回のコマンド入力
提案システム	一回の HTTP リクエスト

全 12 件の入力回数の平均を調査項目別に比較したものが表 2 となる。

表 2 調査 1 回あたりの入力回数の比較結果

調査項目	既存システム(コマンド)	提案システム
日付指定	1.73	0.55
検知元 IP	3.18	0.45
検知ルール	2.82	1.00
検知先 IP	0.36	0.09
遮断判定	2.18	0.73
重要度	1.00	0.36
その他	0.91	0.18
入力回数合計	12.27	3.36
差率(既存システムを 1 とした時)	1.00	0.231

既存システムと提案システムを比べると、入力回数が約 77%削減された。検知元 IP の集計では構造化により、検知元の集計にかかる入力数は大きく削減できることが分かった。全体的に入力回数が減っているのは、標準的な集計を事前集計にしたこと、既存システムでは複数の機器やファイルに対して繰り返しコマンドが必要だが、提案システムでは事前に統合しており一回の集計で済んだことが要因である。

4.2 必要時間の比較

提案システムを試行して既存システムと比較した結果が表 3 である。セキュリティ分析官が提案システムを試用してアラート調査を実施した際の利用ログから、調査に要した時間を求めた。既存システムの場合は、提案システムを試用した分析官が既存システムで対応した実際のインシデント対応ログ 12 件から要した時間を記録した。なお、両者のインシデントの複雑さは同じ程度である。

表 3 調査 1 回あたりの必要時間の比較

	調査件数	一件当たりの平均必要時間
既存システム(コマンド)	19	22 分 19 秒
提案システム	5	9 分 39 秒
差率(既存システムを 1 とした時)	-	0.432

アラート調査一回当たりの必要時間を既存システムと比べると提案システムでは約 56%削減できた。これは事前集計やリクエストのフォーム入力･アラートの構造化により、既存システムに比べてコマンド入力や整形の必要時間が削減できたためと考えられる。

5. まとめ

本研究では、インシデント対応におけるアラート調査を迅速化する支援システムを提案した。支援システムでは統一データ形式への変換・アラートの構造化・事前集計とリクエスト集計により、分析官によるアラート調査を迅速化する。結果として、提案システムは既存システムと比較して、入力回数では 77%の削減、必要時間は 56%の削減ができることがわかった。

引用文献

[1] 一般社団法人 JPCERT , “インシデント対応とは？,” 14 7 2015. [オンライン]. Available: https://www.jpcert.or.jp/ir/#incident. [アクセス日: 15 2017].

[2] 日本セキュリティオペレーション事業者協議会, “セキュリティ対応組織の教科書,” 日本セキュリティオペレーション事業者協議会, 2016/11/25.

[3] 一般社団法人 JPCERT, “インシデントハンドリングマニュアル,” 一般社団法人 JPCERT コーディネーションセンター, 2015.

[4] 藤田直行, “侵入検知に関する誤検知低減の研究動向,” 電子情報通信学会, 2006.