情報処理学会論文誌 Vol.60 No.4 1108–1118 (Apr. 2019)

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調査支援システム

岩崎 信也[1,a)] 角田 朋[1] 関口 悦博[1] 小西 幸洋[1] 大鳥 朋哉[1] 薦田 憲久[2]

受付日 2018年7月4日, 採録日 2019年1月15日

概要：ファイアウォ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，攻撃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，分析担当者による必要時間を平均63.1%削減できた．

キーワード：サイバーセキュリティ，SOC，アラート，インシデント対応

Alerts Investigation Support System for Expediting Incidents Response in Outsourced Security Center

Shinya Iwasaki[1,a)] Tomo Kakuta[1] Yoshihiro Sekiguchi[1]
Yukihiro Konishi[1] Tomoya Ohtori[1] Norihisa Komoda[2]

Received: July 4, 2018, Accepted: January 15, 2019

Abstract: We propose a support system for efficiency of incident response to investigate alert of security devices such as firewall and intrusion detection system. Investigation of alerts takes time due to three problems. First, the format of the alert varies depending on the security devices. Secondly, the survey requires aggregation by various kinds of commands. Thirdly, require shaping to figure out the flow of occurrence of alert. The propose system converts alerts into a uniform format. In addition, structures alerts according to the time interval between alerts and visualizes locality and continuity in an easy-to-understand manner to analyst. The aggregation processing is divided into standard pre-aggregation and request aggregation and executed. As a result of the trial, the propose system reduces the required time by 63.1% compared with the existing system.

Keywords: cyber-security, soc, alert, incident response

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とらえられる事象」を指す [1]．例として情報流出や不正アクセス・ウェブサイト改ざんなどがある．インシデント対応では，インシデントの疑いが検知された際に優先度の決定や，対応が必要かを判断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．このアラートは多量かつその大部分が問題ないことが分かっている [2]．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

[1] 株式会社日立システムズ
Hitachi Systems, Ltd., Shinagawa, Tokyo 141–8672, Japan
[2] コーデソリューション株式会社
Code Solutions Co., Ltd., Osaka 550–0002, Japan
[a)] shinya.iwasaki.fb@hitachi-systems.com

り異なることや，調査のためのコマンドの作成，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．先行研究として，これらの問題に対し，特定の攻撃調査を対象とした，最適な可視化方式やアラート形式の変換方式などが提案されている．しかし，アラート調査全体を支援することができておらず，インシデント対応を実運用するうえでの迅速化としては，不十分である．

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．アラートを攻撃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担当者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の判断・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，ファイアウォールや侵入検知システム（IDS：Intrusion Detection System）など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．これに対して CSIRT は検知されたインシデントに対し適切な対処を実施する．しかし，昨今は 1 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 [3]．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 2 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．後述のアウトソース型 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 サービスやセキュリティデバイス監視サービスとして提供されており，契約した他企業のセキュリティを監視する．アウトソース型 SOC は，多種多様な企業のセキュリティを監視するため，規模が大きく監視対象のセキュリティ機器も多様である．アウトソース型 SOC を活用した場合，その利用企業は比較的小規模なセキュリティに対応する組織を持ち，自組織で実施すべき領域や自組織を中心に連携すべき領域のみに対応し，専門的な知識が必要となる領域を外部委託する．これは「ミニマムインソース」,「ハイブリッド」型と呼ばれる組織形態であり，専門のセキュリティ部門を持たず IT 部門がセキュリティも担当するユーザ企業では最も標準的である [3]．本稿では主にアウトソース型 SOC を利用したこれら 2 つの形態を対象として説明する．

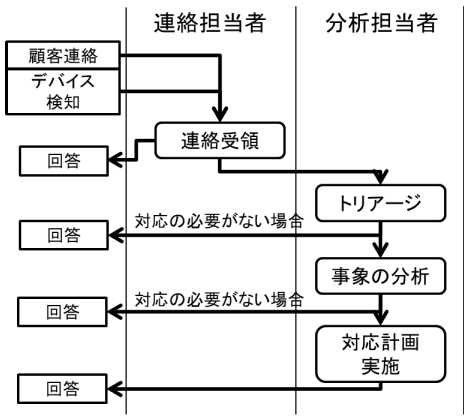


図 1 インシデント対応フロー
Fig. 1 Incident response flow.

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 [4]．

インシデント対応は，セキュリティ機器などあらかじめ用意したシステムによって異常が発見される場合や，監視対象の内部関係者からの異常の連絡，専門組織などの外部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，連絡担当者がその情報を受領する．事前に用意された手順書などの判断基準により，その情報が分析担当者に転送するべきインシデントであるかを確認する．連絡された情報が，誤情報や，サーバのメンテナンスなどの予期された障害など，分析担当者が対応する必要がない場合もある．これらの場合は，分析担当者には転送せずに，回答が必要な場合は，その旨を回答し収束させる．もしインシデントの可能性がある場合は，起票し分析担当者に転送する．

(2) **トリアージ**

トリアージは，分析担当者が，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 節に記述する．

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．侵害の想定度合いや，SOC の形態によっては，マルウェアの感染が疑われる PC（Personal Computer）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や PC のイベントを 1 つずつ追跡して感染の広がりを把握することで，侵害の全容を明らかにする．

(4) 対応計画/実施

事象分析の結果を基に，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．アラートは統合脅威管理（UTM：Unified Threat Management），IDS やファイアウォールなどのセキュリティ機器が，ネットワークトラフィックを監視し，異常や攻撃の可能性が高いイベントを検知した際に発生させる．たとえば，**図 2**，**図 3** はセキュリティ機器が発生させたアラートの一例である．

これらのアラートは，少しでも攻撃の可能性があると発生するが，実際の攻撃につながるのは一部である [5]．このため，アラートが発生した際には攻撃の可能性を調査する必要がある．

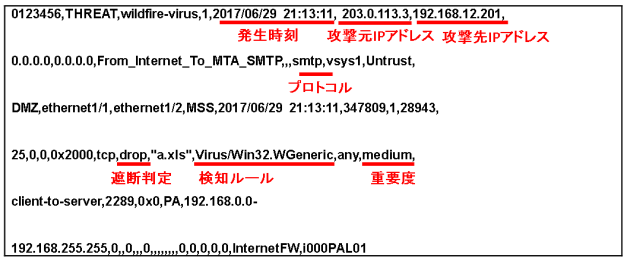


図 2 UTM（Palo Alto Networks 社）のアラートログ
Fig. 2 Alert log of UTM (Palo Alto Networks).

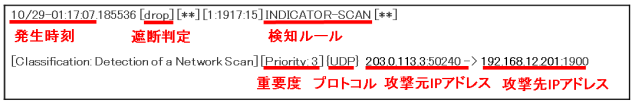


図 3 UTM（Snort IDS）のアラートログ
Fig. 3 Alert log of UTM (Snort IDS).

アラート調査はイベント調査と統計調査に分かれる．

2.3.1 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．主な調査観点は下記のとおりである．

- 日付
- 攻撃元 IP（Internet Protocol）アドレス
- 検知ルール
- 攻撃先 IP アドレス
- 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．たとえば，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短期間に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，何らかの情報を外部に発信している可能性などがあげられる．また，標的型攻撃などは IDS などの検知を逃れるため，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攻撃元や攻撃先に関連するアラートが発生していないかを調査する．

2.3.2 統計調査

統計調査では，アラート数などの時間的変化を調査し，長期的な傾向から攻撃の兆候が発生していないか確認する．統計調査は一件の攻撃に対応する面よりも，社会的なサイバー攻撃の発生の予兆などを把握し，セキュリティ体制を高度化する事前対策の面が強い．

アラート調査の標準的な調査工程は，下記のとおりである．

(1) 起票情報からアラートを取得し，関係するセキュリティ機器への接続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やアラートが蓄積されているサーバにアクセスする．

アラートの蓄積方式は，セキュリティ機器の機種や，設置されているネットワークによって異なる．そのため，調査対象の機種やネットワークに応じた手順書を確認し，アラートが蓄積されている機器・サーバなどにアクセスする必要がある．

(3) 調査観点のコマンドを作成する．

調査手順書を確認し，調査する観点・機種に適したコ

```
zcat /var/log/palo/logs/vulnerability/vulnerability.log-201810*.gz |
    grep -i '{攻撃元IPアドレス}' | awk -F',' '{$30=="{検知ルール}"}{print $0}' > temp_alert.txt
```

図 4 特定の攻撃元 IP アドレスかつ，特定の検知ルールのアラートを抽出するコマンド（Palo Alto Networks 社 UTM）

Fig. 4 Command for searching alerts of the same attacker IP address and same detection rule (Palo Alto Networks UTM).

```
zcat /var/log/snort/logs/alert.log-201810*.gz |
    grep -i '{攻撃元IPアドレス}' | awk '{$5=="{検知ルール}"}{print $0}' > temp_alert.txt
```

図 5 特定の攻撃元 IP アドレスかつ，特定の検知ルールのアラートを抽出するコマンド（Snort IDS）

Fig. 5 Command for searching alerts of the same attacker IP address and same detection rule (Snort IDS).

```
zcat /var/log/palo/logs/vulnerability/vulnerability.log-201806*.gz
    | grep drop | awk -F',' '{print $5}' | cut -b 1-10 | sort | uniq -c
```

図 6 特定の攻撃元 IP アドレスかつ，遮断したアラートの日ごと件数を出力するコマンド（Palo Alto Networks 社 UTM）

Fig. 6 Command for outputting the daily number of blocking alerts from a particular source IP address (Palo Alto Networks UTM).

マンドを作成する．アラートは，機種によってフォーマットが異なるため，作成するコマンドの対象ファイルのパスやパラメータ名を変更する必要がある．たとえば，**図 4** では，Palo Alto Networks 社製 UTM の特定期間のアラートが蓄積されているファイルから，特定の攻撃元 IP アドレスかつ検知ルールを条件に抽出するものである．これに対して，Snort IDS から同様の条件で抽出するコマンドは**図 5** となり，対象とするファイルやパラメータが異なる．ファイルのパスは，機器の設定で統一することもできる．しかし，分析担当者が誤って違う機種のコマンドを実行した場合，アラート形式が異なり，予期せぬ動作が起きる可能性がある．そのため，運用上の誤操作防止の観点から，アラート形式が異なる機種のアラートを蓄積するファイルのパスを変えていることが多い．

また，調査観点ごとに，コマンドを作成する必要がある．たとえば，調査観点の 1 つとして，セキュリティ機器が遮断したアラート件数の時間的な変化を調査する場合がある．このコマンドは**図 6** であり，図 4 のコマンドと異なっている．このように，調査観点により，コマンドの種類や数，パラメータを変更する必要がある．

(4) (3) で作成したコマンドを，アラートファイルに実行する．

(5) 結果を表計算ツールなどに記録する．

調査観点が複数の場合や，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．

発生日時	間隔	UTM名	アラート
2017/5/9 18:16		Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 18:16	0:00:22	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 20:21	2:04:38	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 20:23	0:02:13	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 20:23	0:00:10	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 20:24	0:00:39	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 20:55	0:31:21	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 22:25	1:29:37	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 22:26	0:01:11	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/9 22:26	0:00:00	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/10 0:32	2:05:49	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/
2017/5/10 1:36	1:04:00	Paloal	0123456,THREAT,wildfire-virus,1,2017/05/

図 7 表計算ツールによるアラートの整形

Fig. 7 Format the alert with the spreadsheet tool.

(6) 記録した結果を人が判断しやすいように整形する．

局所性と継続性を見るために，表計算ツールなどで，加工する．**図 7** は，特定の攻撃元 IP アドレスかつ，特定の検知ルールのアラートを抽出した結果（図 4 のコマンドの実行結果）を記録し，アラート間の時間間隔を表示したものである．1 時間以上の間隔で，2 回の局所的なアラートが発生していることが分かる．

(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，(2) に戻り，追加で調査する．

2.4 アラート調査の問題点

アラート調査は短時間で完了する必要があるが，下記の課題により時間を要し問題となる．

(1) **セキュリティ機器によりアラート形式が異なる．**

種類やメーカが違うセキュリティ機器のアラートは構文や項目名の形式が異なる．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いる．その結果，コマンド作成する際の対象となるファイルのパスや，パラメータ名が変わる．

(2) **調査観点ごとにコマンドを作成する必要がある．**

アラートの調査観点ごとに対応したコマンドを作成しなければならない．たとえば，一定期間内に発生したアラートの攻撃元が過去関係したアラートを調査する場合，攻撃元 IP アドレスをリストアップし，攻撃元 IP アドレスの数だけ，コマンドのパラメータを変え，実行する必要がある．

(3) **局所的・継続的なアラート発生の調査に整形を必要とする．**

アラートの局所性や継続性を確認するために，一定期間のアラート群を，人が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. 先行研究

アラート調査の迅速化として，これまで分析担当者に対してアラートや関連したトラフィックを可視化する研究がさかんである．通信元および通信先の傾向を二次元

マップにより可視化する事例 [6]，監視センサとダークネットとの通信を可視化しマルウェアの伝搬を可視化する事例 [7]，アラートをグループ化しその相関を視覚的に可視化する事例 [8]，アラート内の情報の出現頻度を可視化する事例 [9] や，複数の IDS のアラートを関連付けて可視化する事例 [10] などがある．これらの研究は，特定の攻撃や異常を発見するために，特定の観点でアラートやトラフィックを可視化する手法を提案している．しかし，実際のインシデント対応では，さまざまな攻撃の可能性を分析するうえで，分析担当者による多角的な観点での迅速な調査が必要である．このため，特定の観点で可視化するこれらの研究では，アラート調査に必要な観点を網羅できないという課題がある．

複数のログを可視化し，時系列的な出現頻度を視覚化する事例もある [11]．この研究では，クライアントデバイスのログを含む多種のログを可視化することで，同一の時間帯に発生したログを横断的に調査することができる．しかし，クライアントデバイスのログは，そのサイズの点で，コストが高いため，収集していないことが多く，アラートが発生するたびにクライアントデバイスを含む多種のログを収集して調査することは難しい．

また，機械的に誤検知を削減する事例として，アラートを含めたさまざまな情報を集約して異常検知する事例 [12]，アラートを比率分析・しきい値学習分析などの統計手法により誤検知を削減する事例 [13] もある．これらは，誤検知の可能性が高いアラートを提示することを目的としている．しかし，近年のサイバー攻撃は，多様かつ巧妙化しており機械的な分析のみではインシデントの判断が難しい．

アラートの形式が異なる問題への対応としては，syslog で送信されたログを，正規表現を用いて指定の形式に変換，格納する事例 [14] がある．これは，提案されている可視化手法のためのアラート収集方式である．そのため，転送方式は syslog であり，収集対象となる項目が決まっている．実運用されているセキュリティ機器は，設置されているネットワークにより，必ずしも syslog を利用できるわけではない．また収集対象項目が，固定的かつ提案する可視化手法に必要な最低限の項目であり，アラート調査観点を調べるために必要となる項目を充足していない．

アラートのフォーマットとして，STIX（Structured Threat Information eXpression）[15] や，IDMEF（Intrusion Detection Message Exchange Format）[16] がある．双方とも多種のシステム間でのデータ交換を目的としたフォーマットであり XML で構成され，XML タグを定義する必要がある．そのため，アラート 1 件あたりのサイズが大きくなり，アラートの発生量が 1 日で数万件になるアラート調査用のアラートデータ蓄積には適さない．また，汎用的なログ収集ソフトウェアとしては，fluentd [17] や logstash [18] がある．これらのソフトウェアは，定義ファイルにより，多種の機器からログを収集し，変換し，他のシステムに，転送することができる．しかし，これらのソフトウェアでアラートを収集しようとする場合，複雑な定義ファイルを必要とし，これらのソフトウェアの知識を持たない場合，利用が難しい．また，アラートの変換では，アラートと他のファイルを対応付けて，項目を追加する処理が必要となるが，既存のソフトウェアでは対応できない．

4. 提案システム

4.1 システム概要

本研究ではアラートをさまざまな定型パターンで分析，可視化し，分析担当者によるアラート調査に必要となる多角的な観点からの調査を支援するシステムを提案する．

本システムの構成を図 8 に示す．本システムは，デバイスが発生させる形式が異なるアラートを統一的な形式に変換し，攻撃元 IP アドレス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 2 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分析担当者はリクエストできる．分析担当者は集計結果をパーツとして画面上で好きなように配置可能であり，担当範囲により，必要な可視化結果のみ表示できる（図 9）．

4.2 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

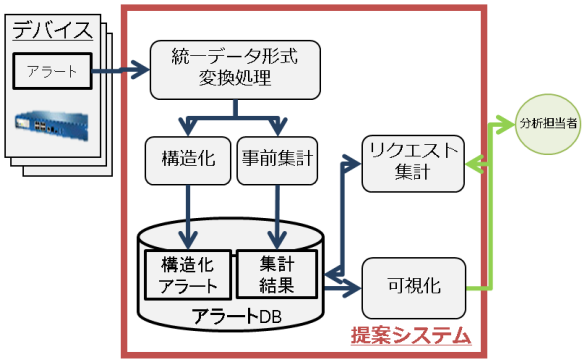


図 8 システム構成図
Fig. 8 System configuration of proposed system.

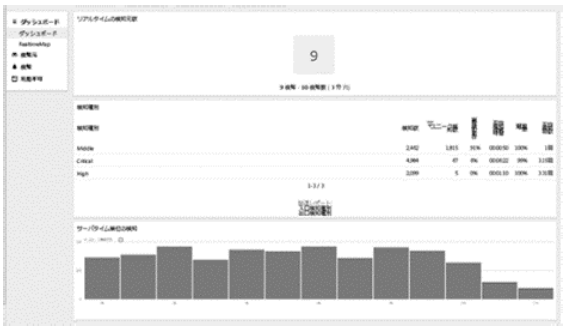


図 9 提案システムの可視化結果
Fig. 9 Visualization example of proposed system.

表 1 統一的データ形式
Table 1 Unified data format of alert.

	key	項目名
共通部	logtype	アラートの種類
	time	発生時刻
	devid	機器識別番号
	attackerip	攻撃元 IP アドレス
	attackerport	攻撃元ポート
	victimip	攻撃先 IP アドレス
	victimport	攻撃先ポート
	severity	重要度
	attack	検知ルール
	protocol	通信プロトコル
	action	遮断判定
カスタム部		任意 (スキーマレス)

を定義する．これにより，多種の機種のアラートを同一の形式に変換し，調査観点の集計・可視化に必要な処理を統一する．アラートを統一形式に変換し，DB に蓄積することで，機種によりコマンドの対象ファイルのパスやパラメータが異なることがなくなる．このため，分析担当者は，調査対象の統一的な操作で，すべての機種のアラートを調査することができる．

IDMEF のフォーマットを参考に，アラート調査に最低限必要な項目を共通部として，それ以外の追加項目を，カスタム部として統一的データ形式に変換する．

統一的データ形式を**表 1** に示す．

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，任意の数を任意のキーで指定できる．

アラートの統一的データ形式への変換は，fluentd を基にしており，定義ファイルで設定が可能である．定義ファイルは，アラート変換のみを対象として，fluentd と比べて簡略化しており，データ変換への知識を持たない分析担当者でも定義が可能である．定義ファイルの更新は，それほど高頻度では必要がないが，新しい種類のセキュリティ機器の追加や，セキュリティ機器の更新によりデータ形式が変更されたときに必要となる．そのため，分析担当者が，定義ファイルを作成・変更できるのは，重要である．

定義は大きくアラート入力定義とアラートマッピング定義の 2 つに分かれる．

アラート入力定義は，**図 10** のとおり対象となるアラートの入力方法を定義する．

基本的には入力のプロトコル（file, syslog, http）と各プロトコルに必要な情報を記述する．入力アラートの形式が file 監視の場合は，type に tail と指定することで，path

```
# アラート入力定義
## ファイル or syslogの場合
<source>
 type {tail|syslog}
 tag {タグ名}
 path /var/log/palo6.log
</source>

## HTTPの場合
<source>
 type http
 port 8888
</source>
```

図 10 アラート入力定義の形式
Fig. 10 Alert input definition.

```
# アラートマッピング定義
<match {タグ名}>
 ## 共通部
 format ${none|csv|json}
 logtype ${}
 time ${}
 devid ${}
 attackerip ${}
 victimpip ${}
 attackerport ${}
 victimport ${}
 severity ${}
 proto ${}
 attack $}
 action ${}
 ## カスタム部
 custom_name1 ${}
 custom_name2 ${}
 custom_name3 ${}
</match>
```

図 11 アラートマッピング定義
Fig. 11 Alert mapping definition.

のファイルを監視し，追記されたときにそのデータを処理する．http の場合は，受信ポートを指定することで，[https://domain:port/tag] の形式でアラートを受信する．ここでの tag とは，マッピング定義を指定するための識別子である．

アラートマッピング定義は**図 11** となり，key と，アラートから項目を抜き出すための形式を指定する．

${} 内は，アラートから項目を抜き出すためのマッピング指定を行う．マッピング指定は対象アラートのフォーマットにより異なる．たとえば csv の場合は，format を csv とし，csv_param[列番 (0...n)] とする．区切り文字がない形式の場合，format を none とし，アラートログに対する正規表現によって指定する．たとえば「...Action="{遮断判定}"...」の場合，(/^.*?Action="([^"]*)".*$/) となる．この正規表現の書式は，ruby 言語に準拠する [19]．カスタム部 [custom_name1∼n] は，任意の key 名で，セキュリティ機器が独自に持つパラメータを設定することができる．また，セキュリティ機器により，分析に必要な項目の一部が，

図 12 テンプレートの作成画面
Fig. 12 The screen for creating a template.

別のファイルにリスト化されている．たとえば，検知されたルールが，なぜ発生したかの説明項目などである．これに対応するため，別ファイルとアラートの項目を対応付け，別ファイルのデータを挿入することができる．

4.3 テンプレートベースの集計機能

コマンドを作成する時間を削減するため，2 つのテンプレートベースの集計機能を提供する．

1 つ目は事前集計機能であり，アラート調査に必要な標準的な集計機能をテンプレートとして事前に定義し，アラート発生時に集計する．主に統計調査に必要な調査観点別の集計を行う．事前に集計することで，複雑な条件や大規模なデータに対する処理で高速化が望める．なお，登録されていない機能が必要になる場合は，随時テンプレートを追加登録することができる．

2 つ目はリクエスト集計機能である．分析担当者は必要になった際に，テンプレートを作成し実行する．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．リクエスト集計機能では，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ため，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．

テンプレートは**図 12** のように，画面上の簡単なフォームで条件を入力し，実行タイミングを事前集計機能もしくはリクエスト集計機能に設定することで作成できる．

4.4 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分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 2 段階に構造化する．**図 13** はアラートの構造化モデルである．同一攻撃元 IP アドレスのアラートで，アラート間の時間間隔が一定以下の場合に 1 つの「攻撃」として関連付ける．複数の「攻撃」は一定時間ごとに「攻撃元」と関連付けられる．

図 14 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) **攻撃テーブル**

攻撃テーブルには，ネットワーク識別情報，一意な ID と攻撃回数を表す攻撃番号，攻撃の始点・終点時刻・継続

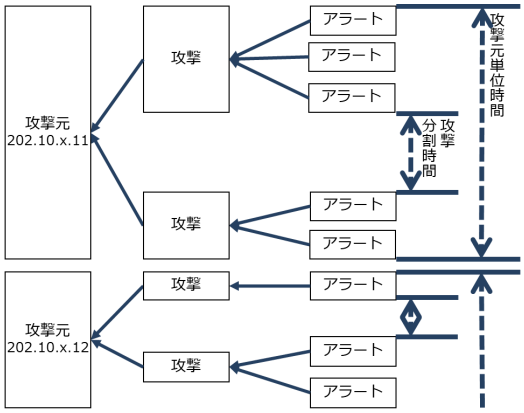


図 13 アラートの構造化モデル
Fig. 13 Structured model of alert.

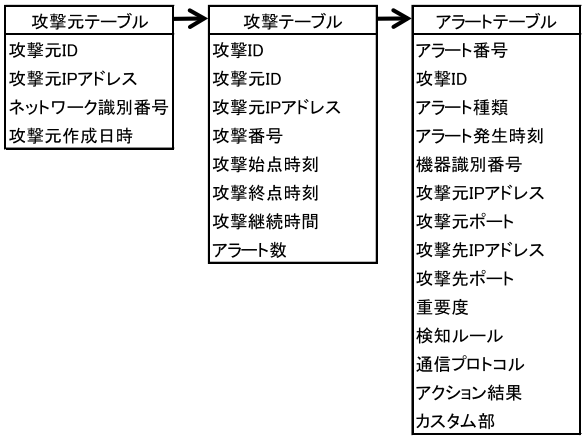


図 14 構造化したアラートの論理スキーマ
Fig. 14 Logical schema of structured alert.

時間，関連付けられているアラートの数を格納する．攻撃テーブルは，アラートテーブルと攻撃 ID によって関連付けが行われる．ここでの攻撃の始点，終点時刻とは，関連付けられているアラートのうち，最初に関連付けられたアラートの時刻を始点時刻，最後に関連付けられたアラートの時刻を終点時刻としたものである．これにより 1 回の攻撃が何時から何時まで続いたのかを容易に把握できる．

(3) **攻撃元テーブル**

攻撃元テーブルには，攻撃元 IP アドレスとネットワーク識別番号，攻撃元作成日付を格納する．攻撃元テーブルは攻撃テーブルと攻撃元 ID によって関連付けられる．

図 15 は構造化したアラートの可視化画面である．「攻撃」ごとにアラートを分割して可視化しており，1 つの「攻撃」内のアラートは局所性があることが分かる．「攻撃元」内の「攻撃」の数によりその攻撃元からの攻撃の継続性が分かる．また，アラートは一覧化され，必要であれば具体的な情報も可視化できる．分析担当者は不審な「攻撃」のアラート 1 件ごとの中身を追うことで，アラートの優先度を判断できる．このように単純にアラートを表示するよりも，局所的なアラートやアラートの流れを分析担当者が確

図 15 構造化アラートの可視化画面（攻撃元・攻撃先 IP アドレスはマスキング済み）
Fig. 15 Visualized screen of structured alert.

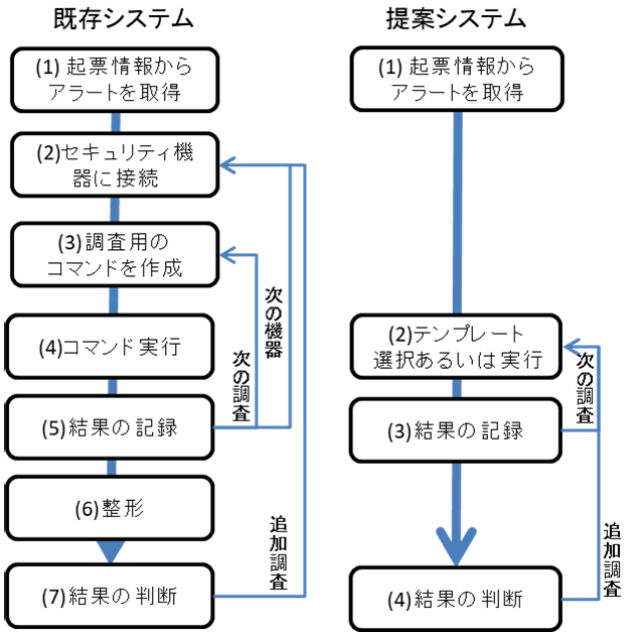


図 16 既存システムと提案システムのアラート調査手順
Fig. 16 Alert investigation procedure of existing system and proposed system.

認しやすい．

4.5 調査手順の比較

提案システムと既存システムのアラート調査手順を比較したものを図 16 に示す．

既存システムと提案システムにおけるアラート調査手順の違いは下記の点となる．

- 提案システムでは，事前にセキュリティ機器からアラートを収集しており，既存システムのようにアラート調査の度に，調査対象のセキュリティ機器に接続する必要がなくなる．
- 既存システムの手順では，(3) 調査用のコマンドを作成し，(4) コマンドを実行することが，必要であるが，提案システムの手順では，アラート調査観点に必要となる標準的な集計機能を事前に処理しているため (2) テンプレート選択するだけで必要な情報が入手できる．
- 既存システム (6) のように，アラートの局所性や継続性を見るために，整形する必要がなくなる．提案システムでは，アラートを局所，継続性を確認するために，アラート発生時に，自動的に構造化しており，必要な際に確認できる．

5. 評価

5.1 評価方法

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，セキュリティ機器のアラートをコマンドベースで検索するシステムを指す．

5.2 評価環境

本実験は 2.1 節で述べたハイブリッド形態におけるアウトソース型 SOC で実施した．この SOC では既存システムが稼働中であり，並行して提案システムを稼働させた．

評価時の対象機器は Palo Alto Networks 社，Check Point 社，Fortinet 社の UTM である．UTM は，IDS やアンチウィルス，ウェブフィルタリングなどの異なる機能を持った複数のセキュリティツールを 1 つにまとめたものであり，統合脅威管理とも呼ばれる．このため 1 つの機器からさまざまな種類のアラートを発生させる．たとえば Palo Alto Networks 社の UTM では，インシデント対応において重要となる以下 3 種類のアラートを発生させる [20]．

- 脅威アラート
- URL フィルタリングアラート
- WildFire（サンドボックスマルウェア分析）アラート

提案システムでは，事前にこれらの機器のインシデント対応に重要となるアラートを取り込めるように，定義ファイルを定義した．

実験対象ネットワークは，4 ネットワークであり，このうち，3 ネットワークは 1 機種のセキュリティ機器，1 ネットワークは 2 機種のセキュリティ機器が設置され，平均 3 種類のアラートを発生させる．1 ネットワークあたり 1 カ月平均で約 84,000 アラートを発生させる．アラートは，それぞれのネットワーク内の専用サーバに一度蓄積される．蓄積されたアラートは，4 台の収集サーバによって，定期的に統一的データ形式へ変換される．変換されたアラートは 1 台の DB・可視化サーバにより，可視化する．これらのサーバは，アラート量や，システムへの接続数に応じて，台数を増やし，分散させることができる．

ネットワーク上での実験の結果，提案システムにおいて，1 つの「攻撃」に平均 17.4 件のアラートが関連付けられ，「攻撃元」には平均 2.9 件の「攻撃」が関連付けられた．なお，分析担当者の意見のもと，実験での攻撃元分割時間は 1 時間，攻撃元単位時間は，1 週間とした．また，提案シス

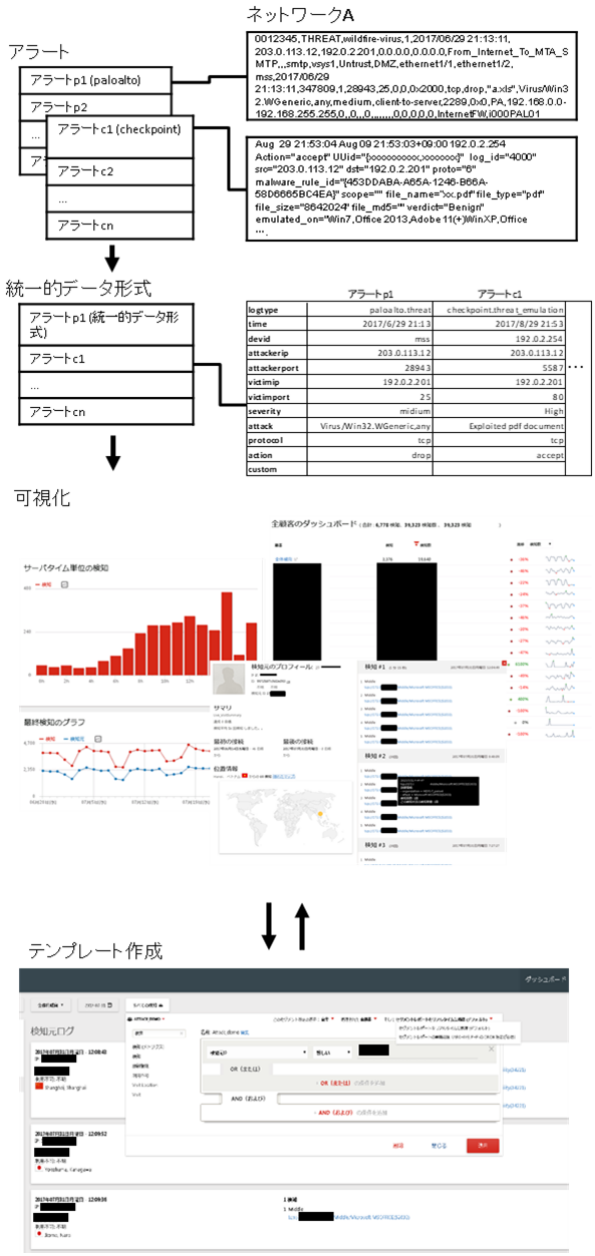


図 17 提案システムの動作例

Fig. 17 Example of operation of the proposed system.

テムの初期状態として可視化されるパーツは，分析担当者の要望によりカスタマイズしている．このカスタマイズは提案時のヒアリングにより実施され，その後のチューニングは行っていない．

実験環境上の提案システムにおける処理例を，**図 17** に示す．

この例では，1 つのネットワーク A 上に 2 つの異なる機器があり，それぞれのアラート [p1~pn,c1~cn] を定義に沿って統一的データ形式に変換している．その統一的データ形式のアラートを元に，テンプレートの実行による集計結果がダッシュボードに可視化される．

表 2 調査 1 回あたりの入力回数の比較結果

Table 2 Comparison result of the command input number per alert survey.

調査観点	既存システム (コマンド)	提案システム
日付	1.73	0.55
攻撃元 IP アドレス	3.18	0.45
検知ルール	2.82	1.00
攻撃先 IP アドレス	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	12.18	3.36

5.3 入力回数の比較

テンプレートを整備することにより，どの程度コマンドが集約され，どの程度入力回数が減るのかを調査観点ごとに把握するため，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 における分析担当者によ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．入力回数は対象機器，システムへのログイン後から記録した．

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）：1 回のコマンド作成
- 提案システム　　：1 回のテンプレート選択

既存システムのコマンド入力ログでは，ミスタイプによる誤操作は除去している．また，提案システムの入力回数は，既存システムのコマンド入力の結果と同様な結果を，提案システムにおいて表示できるまでの最適なテンプレート選択の回数となる．

全 11 件の入力回数の平均を調査観点別に比較したものを**表 2** に示す．

表 2 において，平均が 1 以下となることが生じる理由は調査する必要ない観点が存在するためである．たとえば，分析担当者が，ある観点で調査した結果，アラートに問題がないと判断した場合，そこで調査を打ち切る．この場合，それ以後の調査観点は省略される．また，本実験ではリクエスト集計は実施されなかった．

既存システムと提案システムを比べると，入力回数が 72.4%削減された．このうち，攻撃元 IP アドレスの調査時の入力回数が約 7 分の 1 となり，最も削減された．これは，攻撃元 IP アドレス調査のための作業は，既存システムでは平均入力回数が 3.18 回と他の調査観点の平均 1.50 回に比べ多数のコマンドを必要とするが，比較的定型的な作業が多く，提案システムではそれらをまとめて 1 つのテンプレートとすることで集約できたことが要因である．また，全体的に入力回数が減っているのは，テンプレートの

表 3 調査 1 件あたりの必要時間の比較結果
Table 3 Comparison result of the necessary time for alert survey.

	件数	調査一件当たりの必要時間[分]			
		平均	最小	最大	中央
既存システム (コマンド)	19	22.3	4.9	58.4	19.6
提案システム	11	8.2	2.0	24.6	7.0

整備により，繰り返しコマンドを作成・実行する必要がなくなったことが要因である．

5.4 必要時間の比較

提案システムを実際に試行して既存システムと比較した結果を**表 3** に示す．分析担当者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担当者が既存システムで対応した 19 件の実際のインシデント対応時間を記録した．なお，両者のインシデントの複雑さは同程度である．

アラート調査 1 件あたりの平均必要時間を既存システムと比べると提案システムでは 63.1%削減できた．これは 2 つのテンプレートによる集計・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．ただし，必要時間の削減率 63.1%は，入力回数の削減率 72.4%よりも低い．この要因は，分析担当者が，可視化結果からアラートの優先度を判断するために時間を要しているためと考えられる．

分析担当者からは，構造化やテンプレートによってコマンド作成の手間や整形する手間が減り，提案システムは有用であるとされた．また，セキュリティ機器の検知ルールのアップデート時に，誤検知が多発することがあり，すべてのセキュリティ機器のアラートが，一元的に収集されていることで，アップデート後のアラート発生の挙動を簡単に調査できるようになったとのコメントも得られた．アラートの優先度の判断のさらなる迅速化としては，通常は発生しないユニークなアラートが，同一の攻撃内に発生したとき，提案システムでは一覧化されているだけであるため分かりにくく，分かりやすく可視化するような仕組みがあると良いとのコメントを受け，今後の課題としている．

6. 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，分析担当者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，必要時間を平均 63.1%削減できることが分かった．

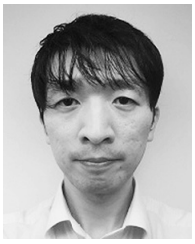
参考文献

[1] JPCERT コーディネーションセンター：インシデント対応とは？，入手先 ⟨https://www.jpcert.or.jp/ir/⟩（参照 2018-11-03）．
[2] 藤田直行：侵入検知に関する誤検知低減の研究動向，電子情報通信学会論文誌 B，Vol.89, No.4, pp.402–411 (2006).
[3] 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，入手先 ⟨http://www.jnsa.org/result/2016/isog-j/⟩（参照 2018-11-03）．
[4] JPCERT コーディネーションセンター：インシデントハンドリングマニュアル，入手先 ⟨https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf⟩（参照 2018-11-03）．
[5] 水谷正慶，白畑 真，南 政樹ほか：Session Based IDS の設計と実装，電子情報通信学会論文誌 B，Vol.88, No.3, pp.551–562 (2005).
[6] Abdullah, K., Lee, C.P., Conti, G., et al.: IDS RainStorm: Visualizing IDS Alarms, *IEEE Workshop on Visualization for Computer Security* (*VizSEC '05*), pp.1–10 (2005).
[7] Inoue, D., Eto, M., Suzuki, K., et al.: DAEDALUS-VIZ: Novel real-time 3D visualization for darknet monitoring-based alert system, *Proc. 9th International Symposium on Visualization for Cyber Security - VizSec*, pp.72–79 (2012).
[8] Livnat, Y., Agutter, J., Moon, S., et al.: A visualization paradigm for network intrusion detection, *Proc. 6th Annual IEEE Systems, Man and Cybernetics* (*SMC*) *Information Assurance Workshop*, pp.92–99 (2005).
[9] 高田哲司，小池英樹：見えログ テキストマイニングと情報視覚化を用いたログ情報ブラウザ，情報処理学会シンポジウム論文集，No.7, pp.541–546 (2000).
[10] 井上和哉，立岩佑一郎，片山喜章ほか：複数の IDS を用いたログ解析によるネットワーク診断システムについて，マルチメディア，分散協調とモバイルシンポジウム 2014 論文集，pp.461–475 (2014).
[11] 江端真行，小池英樹：不正侵入調査を目的とした複数ログの時系列視覚化システム，情報処理学会論文誌，Vol.47, No.4, pp.1099–1107 (2006).
[12] 宮本貴朗，泉 正夫，田村武志ほか：ネットワーク・サーバ運用監視支援システム，システム制御情報学会論文誌，Vol.15, No.6, pp.279–287 (2002).
[13] 竹森敬祐，三宅 優，中尾康二ほか：Security Operation Center のための IDS ログ分析支援システム，電子情報通信学会論文誌 A，Vol.87, No.6, pp.816–825 (2014).
[14] 津田 侑，金谷延幸，遠峰隆史ほか：NIRVANA 改によるライブネット分析，情報通信研究機構研究報告，Vol.62, pp.59–66 (2016).
[15] OASIS Open: Introduction to STIX, available from ⟨https://oasis-open.github.io/cti-documentation/stix/intro⟩ (accessed 2018-11-03).
[16] The IETF Trust: The Intrusion Detection Message Exchange Format (IDMEF), available from ⟨https://www.ietf.org/rfc/rfc4765.txt⟩ (accessed 2018-11-03).
[17] Fluentd: Fluentd, available from ⟨https://www.fluentd.org/⟩ (accessed 2018-11-03).
[18] Elastic: Logstash, available from ⟨https://www.elastic.co/jp/products/logstash⟩ (accessed 2018-11-03).
[19] Ruby サポーターズ：改訂 2 版 パーフェクト Ruby，技術評論社 (2017).
[20] 三輪賢一，伊原智仁，前川峻平ほか：Palo Alto Networks 構築実践ガイド 次世代ファイアウォールの機能を徹底

活用 Palo Alto Networks 構築実践ガイド，技術評論社 (2015).

岩崎 信也 （正会員）

2016 年東京情報大学大学院総合情報学専攻修士課程修了．同年（株）日立システムズ入社．研究開発本部研究開発センタ勤務．セキュリティサービスの研究開発に従事．



角田 朋

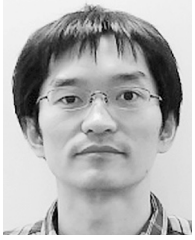
（株）日立システムズ研究開発本部研究開発センタ研究員．セキュリティサービスの研究開発に従事．CISSP（Certified Information Systems Security Professional）認定保持者．

関口 悦博

（株）日立システムズ研究開発本部研究開発センタ主管研究員．セキュリティサービスの研究開発に従事．CISSP 認定保持者．

小西 幸洋

（株）日立システムズビジネスクラウドサービス事業グループネットワークセキュリティサービス事業部ネットワークセキュリティオペレーション本部第一部技師．セキュリティサービスの開発・運用に従事．



大鳥 朋哉

（株）日立システムズビジネスクラウドサービス事業グループネットワークセキュリティサービス事業部ネットワークセキュリティオペレーション本部第一部主任技師．セキュリティサービスの開発・運用に従事．技術士（情報工学）．

薦田 憲久

1974 年大阪大学大学院工学研究科修士課程修了．同年（株）日立製作所入社．1991 年大阪大学工学部助教授，1992 年 8 月同大学教授．2015 年大阪大学名誉教授，コーデソリューション（株）顧問．工博．技術士（情報工学）．IEEE，電気学会の終身会員．