Vol.2021-IFAT-142 No.9
Vol.2021-DC-120 No.9
2021/3/26

# IDSデータ項目グループ化に基づく Tableau Desktopを用いた可視化の試み

輪島 幸治[1,a),b)]　井上 大介[1,c)]

**概要**：近年，計算機の性能向上と情報社会の発展で，大量データの可視化が必要とされている．情報セキュリティ分野における大量データ分析では，各種アラートの異常値検知やマルウェアの挙動解析を目的として，データマイニングや可視化が行われている．しかし，可視化対象となるデータセットは，データ量が大量であることから，本論文では，IDS データ項目のグループ化を用いて，収集されたデータの可視化を行う．本研究で評価対象とする侵入検知システム (IDS) のアラートは，可視化におけるデータの加工処理リソースが必要とされており，迅速かつ一意的な可視化方法が必要である．そこで，本研究の可視化では，Tableau Desktop を用いた．Tableau Desktop は，クライアントアプリケーションだが，標準機能で，カスタムフィールドの作成，データのユニオン，データのグループ化といったデータの加工を行うことができる．ゆえに，IDS アラートが複数のファイルに分割されている場合や，分析のグループ化設定を一意的にノンコーディングで行うことができる．したがって，分析者は，可視化の分析軸の作成に注力できる．本研究で可視化を行う分析軸には，グループ化した IDS 項目及び出力日時項目やアプライアンス項目で，異常値検出や変化点検出を行った．本論文の提案法による分析軸で，大量データに対する分析の有効性及び変化点が検出できたので報告する．

**キーワード**：Tableau Desktop，可視化，IP アドレス，ポート番号，組織行動

# An Attempt to Visualization and Alert Filtering using Tableau Desktop based on IDS Item Grouping

***Abstract:*** In recent years, with the improvement of computer performance and the development of the information society, Visualization of large amounts of data is needed. In the mass data analysis in the information security field, data mining and visualization are performed for the purpose of detecting outliers of various alerts and analyzing the behavior of malware. However, these datasets are not common because they require processing resources for visualization due to the large amount of data. Therefore, at present, a quick and unique visualization method is indispensable. In this paper, from the alert data and darknet data of the intrusion detection system (IDS), Visualize the collected data using Tableau Desktop. Tableau has custom field creation, data unions,By grouping the data, the alert data can be divided into multiple files and the analysis can be grouped without coding. Visualization with Tableau allows you to set analysis axes based on grouping and dataset characteristics. Outlier detection and change point detection were performed. Using the visualization method used in this paper, we have confirmed the effectiveness of the analysis for a large amount of data and the reproducibility of the analysis axis in existing research.

***Keywords:*** Tableau Desktop，Visualization，IP Address，Port Number，Organization Behavior

## 1. はじめに

脅威アラート検出を目的に，侵入検知システム (IDS) を対象とした研究が，数多く行われている [1]．機械学習を用いた手法は盛んに提案されているが，一次調査では，まずアラートを可視化して，概要を把握することが重要である．

[1] 国立研究開発法人 情報通信研究機構
National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
[a)] wajimak@nict.go.jp
[b)] kwajima@ce.slis.tsukuba.ac.jp
[c)] dai@nict.go.jp

研究においても，アラートを可視化して，通信状況の概要を把握して，傾向を明らかとする取り組みは，盛んに行われている．IDS データが対象である場合，対象データのデータ量の課題から，専用の可視化アプリケーションを構築する必要があり，これまでは，処理コストに課題があるとされていた．そこで本研究では，Tableau Desktop に着目した．近年では，急速なデジタル化による「情報爆発」と呼ばれるビックデータへの対応 [2] や，利用者の維持・管理コストが少なく，早期に導入可能な Tableau Desktop のようなパッケージソフトへの要望は大きい [2]．Tableau Desktop は，専用の可視化アプリケーションを構築することなく，大量の IDS アラートを可視化できる．提案法では，IDS アラートを観測場所とポート番号基づいて，グループ化した．各月に分割された IDS のアラートを対象に，アラートを可視化して，通信状況から不正通信の検知や，スパイクポイントの検出，時系列データのを試みる．本研究では，評価対象とする観測場所は，IP アドレスのネットワーク部及びホスト部から，ラベル付けして評価している．

IDS アラート量と送受信状況及び各観測場所におけるアラート状況や各使用ポート番号におけるアラート状況，定常性と非定常性といった複数の観点で，IDS アラートの可視化に成功した．結果を報告する．以下，本論文では，2 章にて，関連研究を紹介する．3 章では，提案法を詳述する．4 章は，本論文の評価対象及び観測場所のラベル付けについて述べる．5 章で，Tableau Desktop を用いて，可視化した結果を述べる．6 章では，提案法で可視化できなかった箇所を示して，最後にまとめと今後の課題を示す．

## 2. 関連研究

### 2.1 侵入検知と異常検知に関する研究

本研究では，IDS アラートを可視化して，異常を検知することを目的としている．これまで，侵入検知や異常検知などの検出を目的に数多くの研究が行われてきた [1]．異常検知の場所，異常と呼ばれる典型的な異常値パターンとしては，外れ値検出，変化点検出，異常値部位検出などがあり [3]，所定した閾値を越えたら異常と判断する定義としてのネイマン・ピアソン決定則がある [3]．また，正規分布や多項分布，経験分布など分布で，異常値を判断するベイズ決定測 [3] や，マージン最大化近傍法などの手法もある [3]．IDS におけるアラート分析は，商用 IDS システムの分析で，以前から行われてきた [4][5]．

既存研究においては，IDS システムの攻撃分類や事前スキャンなど，多くの研究が行われている [6][7]．IDS は，異常検知など通信を監視するシステムである．研究においては，UNSW-NB15[8] など，研究用のベンチマークデータが提供されている．UNSW-NB15 を用いた研究には，攻撃検出性能の比較，新モデルを用いた性能評価，比較など多くの研究が行われている [9][10][11]．

## 3. 提案法

本研究における提案法では，IDS アラートの可視化の分析軸に，IP アドレスを用いて，各観測場所をグループする第 3.1 節の方法．ポート番号をグループ化する第 3.2 節の方法という 2 種類のグループ化手法から構成する．

### 3.1 IP アドレスのネットワーク部とホスト部

IP アドレスを用いたグループ化手法を示す．本研究で，対象とする IP アドレスは，IPv4 の IP アドレスである．組織における IP アドレスのネットワーク部は，主に，観測場所や敷地内の建築物，あるいは部署や研究室，サーバ室などで異なる．ゆえに，IP アドレスに基づいて，可視化することで，組織の通信の可視化で，組織的な行動を可視化すること．また，異常値検知の場合は，場所ごとの特異性，侵入検知の場合は攻撃対象を，明らかにすることが期待できる．IP アドレスのネットワーク部とホスト部の設定では，固定で設定するクラスフルや，CIDR（Classless Inter-Domain Routing）を利用して，可変長で設定する方法がある．本研究では，ネットワーク部の判断を 16 ビットに固定，ホスト部は，8 ビットづつ 2 個に分割してグループ化する手法を用いた．グループ化した結果に対して，観測場所のラベル付けを行い可視化する．本研究で用いる IP アドレスのグループ箇所を下記に示す．

$$\underbrace{XXX.XXX}_{(1)}.\underbrace{XXX}_{(2)}.\underbrace{XXX}_{(3)} \tag{1}$$

**(1)** IP アドレス ネットワーク部：16 ビット
**(2)** IP アドレス ホスト部 (1)：8 ビット
**(3)** IP アドレス ホスト部 (2)：8 ビット

本研究では，第 4.2 節にて示すが，分割した IP アドレスのネットワーク部とホスト部を用いて，既存の IP アドレス割当表から，ラベルを設定して，可視化した．

### 3.2 ポート番号のグループ化

ポート番号を用いたグループ化手法を示す．本研究では，ポート番号の種別をグループ化することで，一般的なアプリケーションの通信なのか，特殊なアプリケーションが，一時的に通信している状態なのかなど，通信状態の概要を把握を目的としている．ポート番号の範囲は，0 番から 65535 番までと値の種類が多く，個別で可視化するには数が多い．ゆえに，本研究では，Internet Assigned Numbers Authority (IANA，アイアナ) と呼ばれるインターネット番号割当機関が管理している種別で，ポート番号を 3 種類にグループ化した．グループ化した内容を箇所を表 1 に示す．本研究では，送信元のポート番号にて分析を行った．

**表 1** ポート番号のグループ

| グループ名 | ポート番号の範囲 |
|---|---|
| WELL KNOWN PORT | 0 番 - 1023 番 |
| REGISTERED PORT | 1024 番 - 49151 番 |
| DYNAMIC AND/OR PRIVATE PORT | 49152 番 - 65535 番 |

## 4. 実装

### 4.1 評価対象

本研究の評価対象として，情報通信研究機構の LAN で 2017 年 1 月 1 日から 2017 年 10 月 31 日までの 10 ヶ月間に発報された IDS アラートのデータセットを用いた．本研究で評価対象とした IDS アラートは，プログラミング言語である Python を使用して，各月で CSV ファイルに分割する前処理を行っている．評価実験に用いた CSV ファイルの総レコード数（アラート数）は 131,902,019 件，合計サイズは 27.9GB であった．Tableau Desktop では，各月に分割された CSV ファイルを読み込み処理し，データのユニオンを作成してから可視化を行った．Tableau Desktop をインストールした Windows Server 2019 では，メモリサイズは，24GB を設定して，評価実験している．

### 4.2 IDS アラートの観測場所のラベル付け

IP アドレスは，一般的に，企業や場所，敷地内の建築物などで，IP アドレスの割り当てが異なる．本研究では，第 3.1 節にて示した IP アドレスのネットワーク部を用いて，IP アドレスの割り当て表から，観測場所をラベル付けする．ラベル付けする IDS アラートは，情報通信研究機構内のアラートのみを対象とした．

ところで，送信元 IP の観測場所が明らかとなった場合でも，異常値検出などでは，詳細な観測場所で，可視化する必要がある場合もある．そこで，本研究では，ラベル付けの方法を大分類である “観測場所”，小分類である “箇所” に分けた．ラベル付けの単位を分けることで，異常値検出を目的とした細かな可視化が期待できる．本研究における大分類の具体的な単位は，情報通信研究機構の所在地案内などに示している単位である[*1]．小分類の具体的な単位は，NICT 本部建物の地図の単位[*2]や，研究紹介などに示されている各研究分野の研究室[*3]や，情報通信研究機構の出版物に記載の土地建物 [12] などである．“観測場所” が小金井本部である場合の一例を表 2 に小分類を示す．

**表 2** IP アドレス別 IDS アラート観測場所 (小金井本部の例)

| No. | 場所名 | No. | 場所名 |
|---|---|---|---|
| 1 | 小金井本部 1 号館 | 7 | 小金井本部 箇所 (7) |
| 2 | 小金井本部 2 号館 | 8 | 小金井本部 箇所 (8) |
| 3 | 小金井本部 3 号館 | 9 | 小金井本部 箇所 (9) |
| 4 | 小金井本部 4 号館 | 10 | 小金井本部 箇所 (10) |
| 5 | 小金井本部 5 号館 | 11 | 小金井本部 共用 |
| 6 | 小金井本部 6 号館 | 12 | 小金井本部 その他 |

表 2 で示した箇所は，小金井本部のみで 12 箇所である．本論文では，表 2 の No.7 から No.10 は，部門名の記載を省略する．第 5 章にて後述するが，評価実験では，12 の “観測場所”，合計 45 の “箇所” を評価対象としている．

*1 NICT - 所在地案内:https://www.nict.go.jp/about/location.html
*2 NICT-NICT 本部建物ご案内: https://www.nict.go.jp/about/hq_building.html
*3 NICT-研究紹介:https://www.nict.go.jp/research/index.html

また，本研究で論文に示す評価実験の結果では，具体的な名称を示すことで攻撃対象となる場合や，各研究室の情報公開のポリシーに抵触する場合を考慮して，図中のラベル名を，具体的な観測対象となる場所を特定しないように，観測場所 (1)，観測場所 (2)…観測場所 (12) や，箇所 (1)，箇所 (2)…箇所 (45) といった表記で示している．

## 5. 評価

### 5.1 IDS アラート全体のアラート量と送受信状態

まず，IDS アラートの各月におけるアラートの量を示すために，図 1 に，IDS アラートのレコード件数をバブルチャートにしてにして可視化する．図 1 では，各月でバブルチャートをラベル付けした．合わせて，IDS アラートにおける送信先 IP アドレスと送信元 IP アドレスから，アラートにおける送受信の状態を明らかにするために，図 2 に送信元 IP 及び送信先 IP のネットワーク部のみ対象に，ヒートマップを用いて可視化した結果を示す．図 2 は，行は送信元 IP アドレスの観測場所，列は送信先 IP アドレスの観測場所である．図 1 及び図 2 における可視化対象は，すべての IDS アラートであり，情報通信研究機構外への通信で出力されている IDS アラートも可視化している．

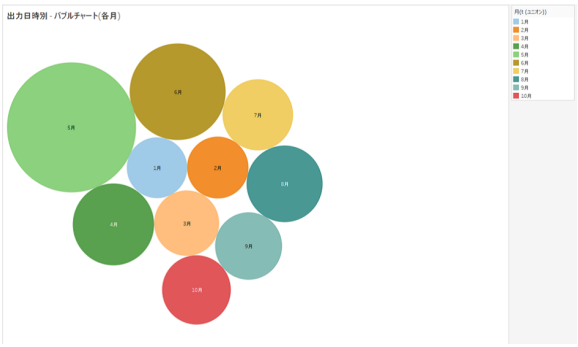


**図 1** 各月の IDS アラートの規模


**図 2** 宛先別 IDS アラートの可視化 - ヒートマップ

結果，図 1 から，評価対象とした IDS アラートは，5 月が最もアラート量が大きい．また，4 月や 6 月も同様の状況が続いていることから，第 1 四半期の期間に，アラートが多い状況であったと推測される．図 2 の結果では，特定の送信先 IP に対してのみ通信を行っている送信元 IP のアラート，すべての送信先 IP に対する通信から出力されたアラートなどが明らかとなった．結果から，本研究で用いる観測場所や，送信元ポート番号などで，詳細にアラートを可視化する必要があることが明らかとなった．

### 5.2 IDS アラートの観測場所

第 4.2 節にて示した観測場所の大分類及び小分類で，情報通信研究機構のアラートのみに対象を絞って，可視化を行う．まず，図 3 から図 5 に観測場所の大分類で可視化した結果を示す．図 3 における可視化対象は，情報通信研究機構内のみ通信を評価対象としている．図 3 では，バブルチャートで，各観測場所のアラート量を明らかとする．また，図 4 で，時系列グラフで，各観測場所でのスパイクポイントを明らかにする．縦軸は，各観測場所，横軸はアラートの発報日時である．加えて，勤務時間帯や深夜時間帯で IDS アラートの量が変化するか評価するために，アラート出力日時の時間帯のみに着目して作成したグラフを図 5 に示す．図 5 の横軸はアラートが発報された時間帯である．縦軸は，アラート量で，軸のグループ化で，送信元 IP の観測場所である．

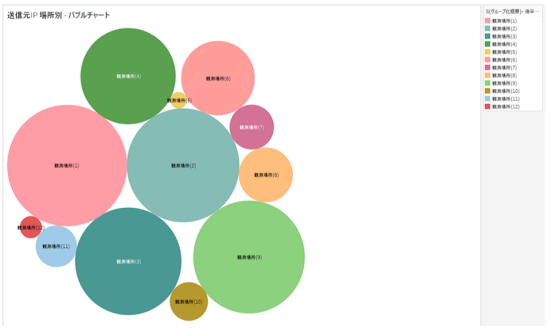

**図 3** 送信元 IP 場所別 - バブルチャート

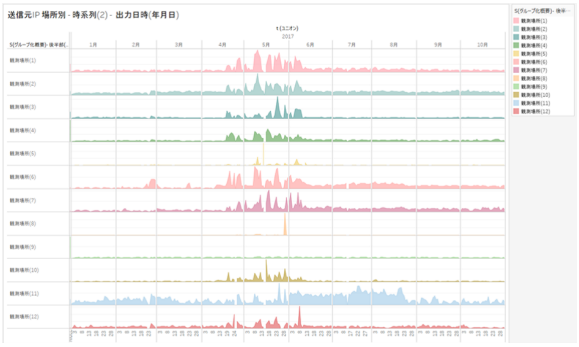

**図 4** 送信元 IP 観測場所別 - 時系列グラフ

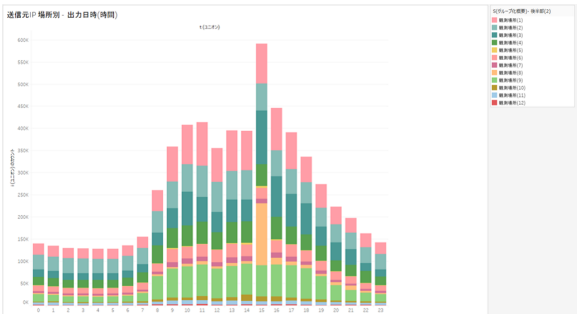

**図 5** 送信先 IP 観測場所 - 時間帯グラフ

結果から，図 3 では，“観測場所 (1)”，“観測場所 (2)”，“観測場所 (9)”，“観測場所 (3)”，“観測場所 (4)” のアラート量が大きい．ゆえに，定常的にアラートを出力するアプライアンスが存在すると推測できる．

また，図 4 の結果から，12 個の観測場所中，9 個の観測場所で 4 月から 6 月にかけてスパイクポイントが確認できた．一方で，“観測場所 (5)”，“観測場所 (8)”，“観測場所 (9)” では，アラートが確認できない．このことから，観測場所に限定したアラートで，問題が発生していたと推定できる．加えて，“観測場所 (11)” については，4 月から 6 月だけでなく 7 月，8 月もアラート継続してアラートが発生していたことが明らかとなった．図 5 においては，アラートが出力されている時間帯で集計した結果，15 時に，“観測場所 (8)” のアラートが大量に出力されていることから，15 時に “観測場所 (8)” で，何らかの大量アラートが発生していた日時があったと推定できる．

次に，図 3 のバブルチャートで評価対象とした，IDS アラートをヒートマップを用いて，可視化した結果を図 6 及び図 7 に示す．図 6 は，行が送信元 IP の観測場所，列が送信先 IP の観測場所である．定常的な通信の場合，どのような通信であるか可視化する必要があることから，図 7 では，通信プロトコルと第 4.2 節にて示したグループ化したポート番号を，列に使用している．ゆえに，図 7 は，行が送信元 IP の観測場所，列がアラートのポート番号である．

**図 6** ヒートマップ - 送信元 IP と 送信先 IP

**図 7** ヒートマップ - 送信元 IP とポート番号

結果から，図 6 で可視化した限りは，各観測場所から，“観測場所 (9)” 宛ての定常的なアラートが送信されていることが明らかとなった．最も，顕著であったのは，“観測場所 (3) - 箇所 (31)” から “観測場所 (9)” 宛てのアラートである．一方で，“観測場所 (9) - 箇所 (45)” は，“観測場所 (1)” 宛て宛てのアラートが多い．また，“観測場所 (11)” 宛てに，“観測場所 (2) - 箇所 (20)” や，“観測場所 (7) - 箇所 (43)” からのアラートが多いことなどが明らかとなった．

図 7 でポート番号で可視化した場合は，“WELL KNOWN PORT” や “REGISTERED PORT” でのアラートが多いが，“観測場所 (9) - 箇所 (45)” や “観測場所 (1) - 箇所 (11)” などは，“DYNAMIC AND/OR PRIVATE PORT” のアラートも多いことが明らかとなった．

### 5.3 IDS アラートのポート番号

第 3.2 節にて示したグループ化した送信先ポート番号で，情報通信研究機構のアラートのみに対象を絞って，可視化を行う．まず，図 8 に通信プロトコルとグループ化した送信先ポート番号を用いて，バブルチャートで可視化した結果を示す．図 8 のバブルチャートでは，各送信先ポート番号での IDS アラートの量を明らかにする．また，図 9 に時系列グラフで，各観測場所のアラートを時系列グラフに表した際のスパイクポイントを明らかにする．縦軸は，各観測場所，横軸はアラートの発報日時である．加えて，勤務時間帯や深夜時間帯で IDS アラートの量が変化するか評価するために，アラート出力日時の時間帯のみに着目して作成したグラフを図 10 に示す．図 10 の横軸はアラートが発報された時間帯である．縦軸は，アラート量で，軸のグループ化で，送信元 IP の観測場所である．

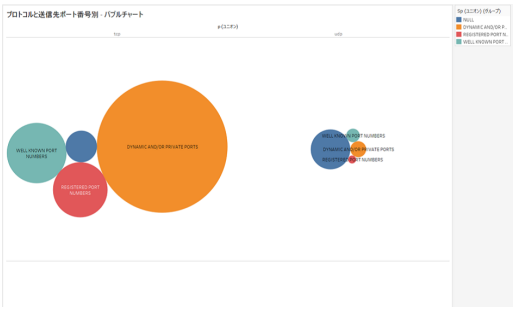

**図 8** 通信プロトコルと送信先ポート番号別 - バブルチャート

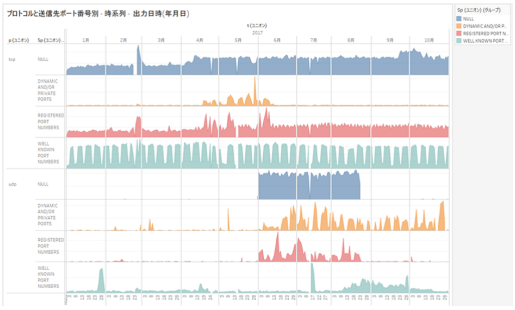

**図 9** 通信プロトコルと送信先ポート番号別 - 時系列グラフ

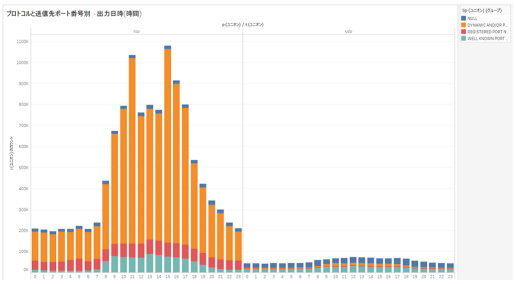

**図 10** 通信プロトコルと送信先ポート番号別 - 時間帯グラフ

結果から，図 8 で可視化した限りは，TCP 及び UDP は，“DYNAMIC AND/OR PRIVATE PORT” のアラートが多いことから，アラートの多くは，一時的に割り当てられているポート番号で通信を行ったアラートであることが明らかとなった．また，図 9 の結果からは，通信プロトコルが TCP の場合は，4 月中頃から 6 月初旬の期間に “DYNAMIC AND/OR PRIVATE PORT” で一時的なアラートが発生していたことが明らかとなった．通信プロトコルが UDP の場合は，アラートはいくつか確認できたが，6 月頃から 8 月の期間に送信先ポート番号の項目値が “NULL”，“REGISTERED PORT”，“DYNAMIC AND/OR PRIVATE PORT” の場合に非定常的なアラートが発生していたことが明らかとなった．図 10 においては，アラートが出力されている時間帯で集計した結果では，8 時から 20 時の一般的な勤務時間の期間中に，“DYNAMIC AND/OR PRIVATE PORT” のアラートが多いことが明らかとなった．

### 5.4 アプライアンス種別を用いた考察

本節では，第 5.2 節及び第 5.3 節で可視化したアラートの観測場所及びポート番号の可視化結果に対して，アプライアンスを分析軸に加えて考察する．まず，図 11 及び図 12 に，アプライアンスで可視化した結果を示す．図 11 では，アラートの通信プロトコルに基づいて，各アプライアンスのアラート量を示す．図 12 では，勤務時間帯や深夜時間帯で，どのアプライアンスのアラートの量が増減するかを明らかとするために，アラート出力日時の時間帯のみに着目して，作成したグラフを図 12 に示す．縦軸は，アラート量で，軸のグループ化で，アプライアンスの観測場所である．

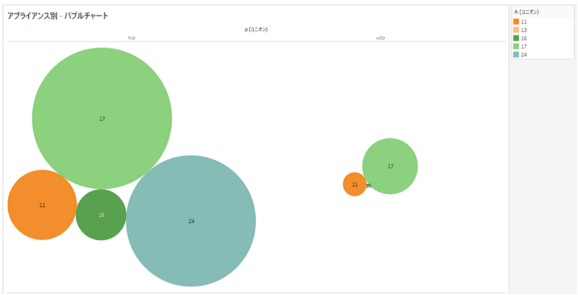

**図 11** 通信プロトコルとアプライアンス別 - バブルチャート

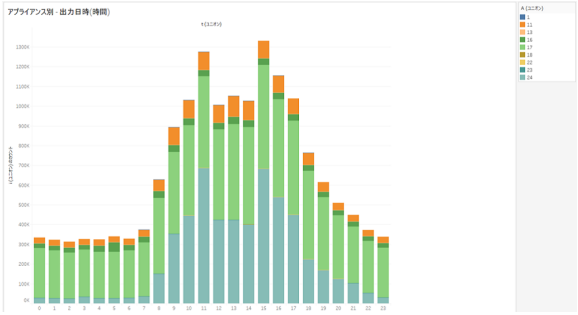

**図 12** アプライアンス別 - 時間帯グラフ

結果から，図 11 では，アプライアンス ID が “17” のアラート量が最も多く，次いで “24” のアラート量が多いことが明らかとなった．図 12 の結果から明らかとなったのは，アプライアンス ID が．“17” のアラートは時間帯に限らず，定常的にアラートが出力されていた．対して，アプライアンス ID が “24” のアラートは，8 時から 17 時の間のみ，出力アラート量が多いことから，勤務時間に依存したアプライアンスであると推定できる．

次に，IDS アラートの観測場所及び送信先ポート番号をアプライアンスの軸を追加して，時系列グラフで可視化した結果を図 13 及び図 14 に示す．図 13 の横軸はアラートが発報された時間帯である．縦軸は，アラート量で，軸のグループ化で，アプライアンス ID と送信元 IP の観測場所を使用している．また，図 14 の横軸はアラートが発報された時間帯である．縦軸は，アラート量で，軸のグループ化で，アプライアンス ID と送信先ポート番号を使用している．

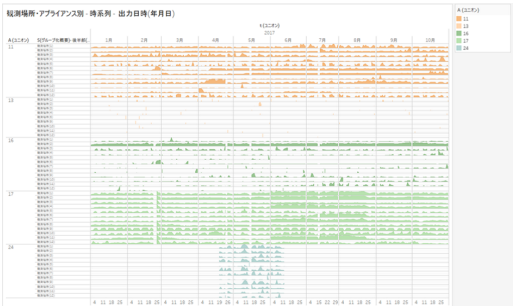

**図 13** アプライアンスと観測場所- 時系列グラフ

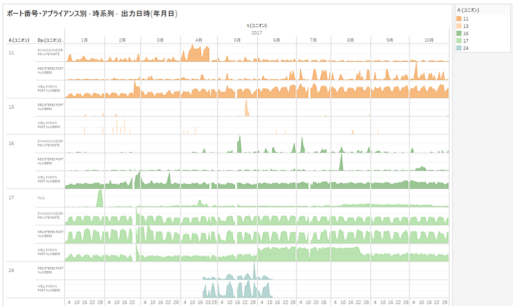

**図 14** アプライアンスと送信先ポート番号- 時系列グラフ

結果，図 13 では，4 月後半から 6 月前半までの期間のみ，アプライアンス ID“24” のアラートが出力されていることが明らかとなった．また，アプライアンス ID と観測場所で絞った場合，特定の組み合わせでアラート量が多い場合が明らかとなった．図 14 の結果，各アプライアンスは，定常的に同じポート番号を使用していることが明らかとなった．アプライアンス ID“11” は，4 月に “DYNAMIC AND/OR PRIVATE PORT” の通信が多く，アプライアンス ID“24” は，4 月から 6 月に “WELL KNOWN PORT” のアラート量が多いことが明らかとなった．そして，図 13 及び図 14 の結果から，定常的にアラートが出力されている観測場所やポート番号の通信をフィルタリングすることで，アラート数が少ないアラートを可視化することなどが期待できる．

## 6. まとめ

本研究では，IDS アラートを対象に，観測場所，ポート番号，アプライアンス種別などを用いて，バブルチャート，各分析軸を用いた時系列グラフ，ヒートマップ，時間帯グラフなどで，アラートを可視化した．結果，出力した結果から，観測場所及び箇所ごとのスパイクポイントや，頻繁にアラートが出力されている送信先 IP アドレスや，ポート番号の種別などが明らかとなった．また，アプライアンス軸を追加した場合の各アプライアンスの出力特性などが明らかとなり，勤務時間で，アラートが増減している様子が可視化できた．今後は，ネットワーク障害や，マルウェアなどの問題との要因分析を加えて，詳細な要因分析を行いたい．

### 参考文献

[1] I. Butun and P. Österberg and H. Song. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Communications Surveys &Tutorials, 1, 22, 616-644, 2020.
[2] 岩本敏男, IT 幸福論, 東洋経済新報社, 2013 年 12 月 26 日
[3] 井手 剛，杉山 将，機械学習プロフェッショナルシリーズ - 異常検知と変化検知，講談社，2015.
[4] 神鳥 泰章, Part2 ブロードバンド時代のセキュリティ対策 (5)IDS 技術とその動向 (セキュリティ最新動向) , Business communication, ,No. 12, Vol. 39, 111–114, Dec 2002.
[5] 高橋 正和, セキュリティ最新動向 (6) 不正侵入検知装置 (IDS) の概要と最新動向について〔含 News&Topics セキュリティ関連製品&サービスの最新情報〕, Business communication, ,No. 6, Vol. 41, 93–98, Jun 2004.
[6] L. N. Tidjon and M. Frappier and A. Mammar. Intrusion Detection Systems: A Cross-Domain Overview. IEEE Communications Surveys &Tutorials, 4, 21, 3639–3681, 2019
[7] Ankush Singla, Elisa Bertino, Dinesh Verma. Preparing Network Intrusion Detection Deep Learning Models with Minimal Data Using Adversarial Domain Adaptation. Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, 127-140, Oct 2020.
[8] N. Moustafa and J. Slay, UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), 2015 Military Communications and Information Systems Conference (MilCIS), 1-6, 2015.
[9] A. Binbusayyis and T. Vaiyapuri. Identifying and Benchmarking Key Features for Cyber Intrusion Detection: An Ensemble Approach. IEEE Access, No. 7, July 2019.
[10] K. Jiang and W. Wang and A. Wang and H. Wu. Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network. IEEE Access, Vol. 8, 2020.
[11] B. A. Tama and L. Nkenyereye and S. M. R. Islam and K. Kwak. An Enhanced Anomaly Detection in Web Traffic Using a Stack of Classifier Ensemble. IEEE Access, Vol. 8, 2020.
[12] 情報通信研究機構 10 年の歩み，国立研究開発法人 情報通信研究機構，2015 年 9 月，https://www.nict.go.jp/publication/10th-anniversary/，最終閲覧日 (2021 年 2 月 27 日)