実環境における試行検証の
検証結果について

令和２年４月

独立行政法人情報処理推進機構

目次

1. はじめに

経済産業省は 2017 年 12 月に「産業サイバーセキュリティ研究会」を設置し、ワーキンググループ 3（サイバーセキュリティビジネス化）において、有効性検証を通じ日本発のサイバーセキュリティ製品・サービスのマーケット・イン促進に資するサイバーセキュリティ検証基盤（以下、検証基盤）の構築を目指すとしている。

経済産業省の委託を請け、独立行政法人情報処理推進機構(以下、IPA)では、検証基盤の在り方を検討する「サイバーセキュリティ検証基盤構築に向けた有識者会議[1]（以下、有識者会議）」を設置した。有識者会議の検討において、検証基盤の対象製品を日本発のスタートアップ製品とし、その優れた特長について検証する仕組みとして具体化すること、また今年度は、脅威・脆弱性の可視化及び IT 資産管理に係る製品分野を検証対象とすること、を方針とした。

具体的な検証方式として経済産業省の計画では、(1)専門家による客観的な「セキュリティ製品の有効性検証」と(2)利用者の「実環境における試行検証」の 2 種類を実施することとしている。そこで有識者会議は、この計画に基づいた検証体制や検証方法等の実施案を検討し、さらにその効果や課題を明らかにするため試行検証を行うこととした。まず、対象となるセキュリティ製品を公募し、上記二つの検証方法それぞれ1製品、計 2 製品を選定して、試行検証の題材とし、IPA が事務局となって実際に試行検証を実施した。

以下、アラクサラネットワークス株式会社「AX-Network-Visualization」を対象に実施した「実環境における試行検証」の検証結果について示す。

2. 検証対象製品 AX-Network-Visualization について

2.1. 概要

AX-Network-Visualization（以下、AX-NV）はアラクサラネットワークス社が提供するネットワークの可視化、異常検知のソリューションである。

通信全体を可視化するために通信状態がわかる NetFlow を記録することで、大規模なネットワークであっても長期間のデータの記録ができ、通信全体を俯瞰して可視化ができる。

[1] IPA サイバーセキュリティ検証基盤構築に向けた有識者会議
https://www.ipa.go.jp/security/economics/kensyokiban2019.html

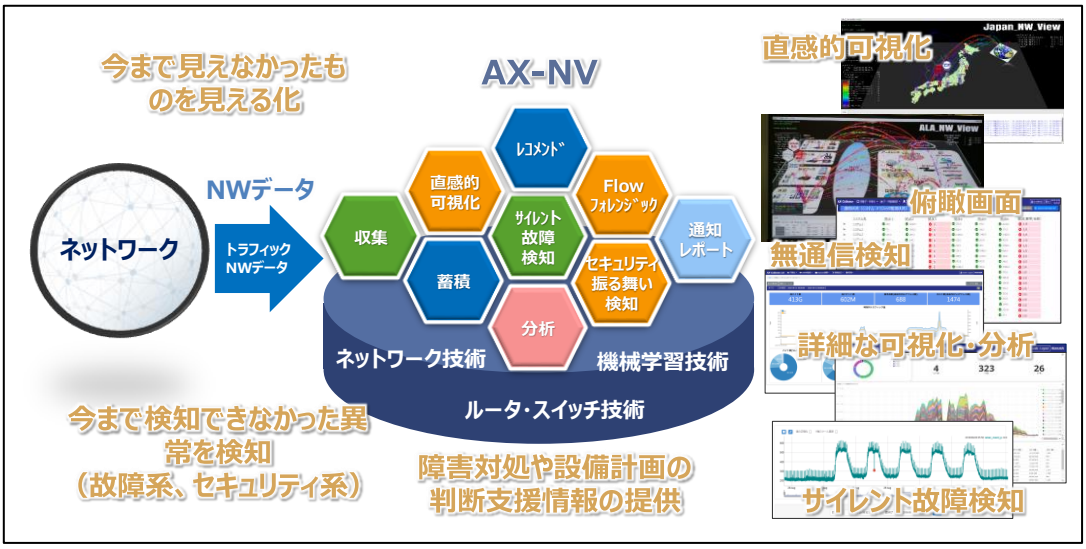

図 1 AX-NV のイメージ（アラクサラネットワークスより提供）

2.2. NetFlow とは

NetFlow とは、米シスコシステムズ社が開発したネットワークの通信を分析して送信元、宛先、通信量を監視・分析するための技術である。NetFlow には、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、プロトコル[2]番号、通信量などの情報が含まれており、それらを分析することで通信状況を把握できる。実際に伝送する実データは含んでいない。

近年、常時 SSL[3]化など多くの通信が暗号化されつつあるが、NetFlow では暗号化される実データを含まないため、平文の通信と同じ条件で監視・分析ができる。AX-NV では、NetFlow V9 をサポートしている。

2.3. 製品特徴

サンプリング無しのデータ収集を行い、検証環境に流れる全ての通信を可視化ができる。NetFlow 技術によりデータが集約されるため長期間のデータの保存ができ、インシデントが発生した場合にも過去に遡って通信の影響調査ができる。

ネットワーク通信を可視化でき、表示方法もグラフや集計値、地図やネットワーク構成図を使った表示により、直感的な通信の可視化ができる。ダッシュボードのカスタマイズができ一元的に通信を把握できる。機械学習を使った異常検知により、サイレント故障の検知ができる（機械学習機能は今回の検証範囲外）。

---

[2] プロトコル：通信に関する規約を定めたもの。「通信プロトコル」とも。

[3] SSL：Secure Sockets Layer（セキュア・ソケット・レイヤ）の略。インターネット上でのデータの通信を暗号化し、盗聴や改ざんを防ぐ仕組み。

3. 検証項目

ネットワークおよびセキュリティ管理者の観点でネットワーク上の脅威を分析・管理をする上で有効と考えられる以下の項目について検証した。

3.1. インシデント解析

IPS[4]やアンチウイルス等でマルウェアによるインシデントを検知した際に、他の端末に同じマルウェアの感染がないか影響を調査するため、以下を検証項目とした。

検証項目 B1-1: 不審な IP アドレスを基に通信状態を分析して、影響のある端末を抽出できるか

3.2. 脅威となる通信の抽出および解析

通信全体を分析した統計情報から、脅威となる可能性のある通信を抽出し分析することで、外部からの脅威ならびに、検証環境の問題を検出するため、以下を検証項目とした。

検証項目 B2-1:統計情報から脅威となり得る通信を分析し、攻撃または調査活動で狙っている端末やポートを抽出できるか

検証項目 B2-2:統計情報から脅威となり得る通信を分析し、外部からの通信に想定外のポートで応答する設定ミスが疑われる端末を抽出できるか

検証項目 B2-3:不正なデータ転送を調査し、インシデントの被害にあっていないか分析できるか

3.3. 既存ネットワークに影響を与えない導入容易性

新規に機器を導入する際に既存ネットワークに極力影響が発生しないことが望ましいといった観点から、以下を検証項目とした。

検証項目 B3-1:既存ネットワークに影響がなく容易かつ安全に導入できるか

3.4. 通信全体の可視化

ネットワーク運用監視を想定し、回線利用状況の把握や管理外端末の検出など、セキュリティ以外の観点から以下を検証項目とした。

---

[4] IPS:Intrusion Prevention System の略。不正な通信を検出し通知するほか、その通信を遮断する機能を持つ侵入防止システム。

検証項目 B4-1:通信全体を可視化し、統計的にみることで回線利用状況を把握できるか

検証項目 B4-2:ネットワーク管理者が認知していない管理外の端末を洗い出せるか

4. 検証環境

今回は、国立情報学研究所の検証環境に、以下の構成で AX-NV を試行導入して検証を行った。

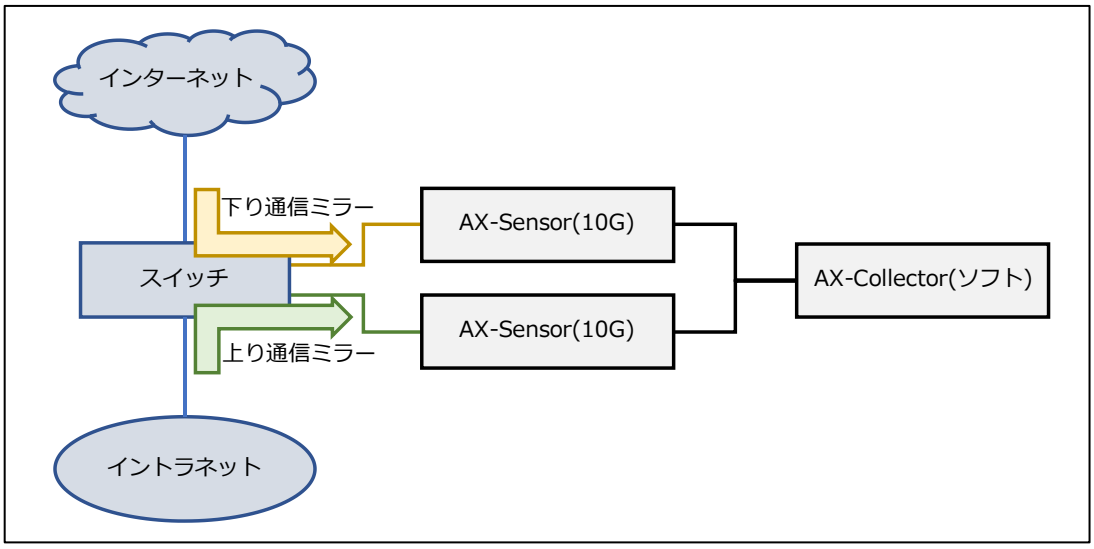

図 1 検証環境の機器構成イメージ

スイッチ[5]の上り通信と下り通信にミラーポート[6]を設け、それぞれの通信を収集する為に AX-Sensor[7]を接続する。ミラーポートである為、既存ネットワークに影響を与えない。

AX-Collector[8]に複数の AX-Sensor を接続することで、各 AX-Sensor が収集した情報を用いて様々な情報の分析が可能となる。

参考に今回の検証環境で AX-Collector をインスト―ルしたサーバの機器仕様を表 1 に示す。

---

[5] スイッチ:コンピュータネットワークの集線装置の一種で、受信したデータの宛先を見て、接続された各機器への転送の可否を判断する機能を内蔵したもの。「ネットワークスイッチ」とも。

[6] ミラーポート:ネットワークスイッチやルータの持つ機能の一つである、あるポートが送受信するデータを、同時に別のポートから送出する機能である「ポートミラーリング」において、コピーされたデータが流れてくる側のポート。

[7] AX-Sensor:ミラーデータを受けて、各種トラフィック情報を収集する装置

[8] AX-Colletor:ネットワーク機器からデータを集約し、可視化や異常検知を行うサーバ上で動作するソフトウェア

表 1 サーバ機器仕様

CPU	Xeon Gold 5218 2.3GHz 16C/32T
メモリ	128GB
HDD	800GB SSD x 2 + 2.4TB SAS x 3
OS	CentOS 7.7

5. 検証結果

5.1. インシデント解析

5.1.1. 検証項目 B1-1:

不審な IP アドレスを基に通信状態を分析して、影響のある端末を抽出できるか

検証結果:

不審な IP アドレスと期間を限定して通信を絞り込むことで、抽出できた。

検証内容詳細:

本検証では、マルウェアに感染させた疑いのある不審な IP アドレスがわかっている前提で通信の分析をした。送信元を不審な IP アドレスに限定し、検証環境の端末を宛先にした通信を抽出する(図 1 不審な IP アドレスから検証環境の端末への通信状況の例)。宛先 IP アドレスやポート番号、通信量、平均パケット長を確認する。

また、この際の通信に対する応答を調べるために、宛先を不審な IP アドレスに限定し、送信元 IP アドレスやポート番号、通信量、平均パケット長を確認する。上りと下りの通信内容から、マルウェアの感染の疑いのある端末を特定する。

サンプリングせずにデータを保持していることから、過去に遡って不審な IP アドレスにアクセスしている端末がないかの調査が容易にできるため、インシデント解析時の影響有無の切り分けにも有用である。

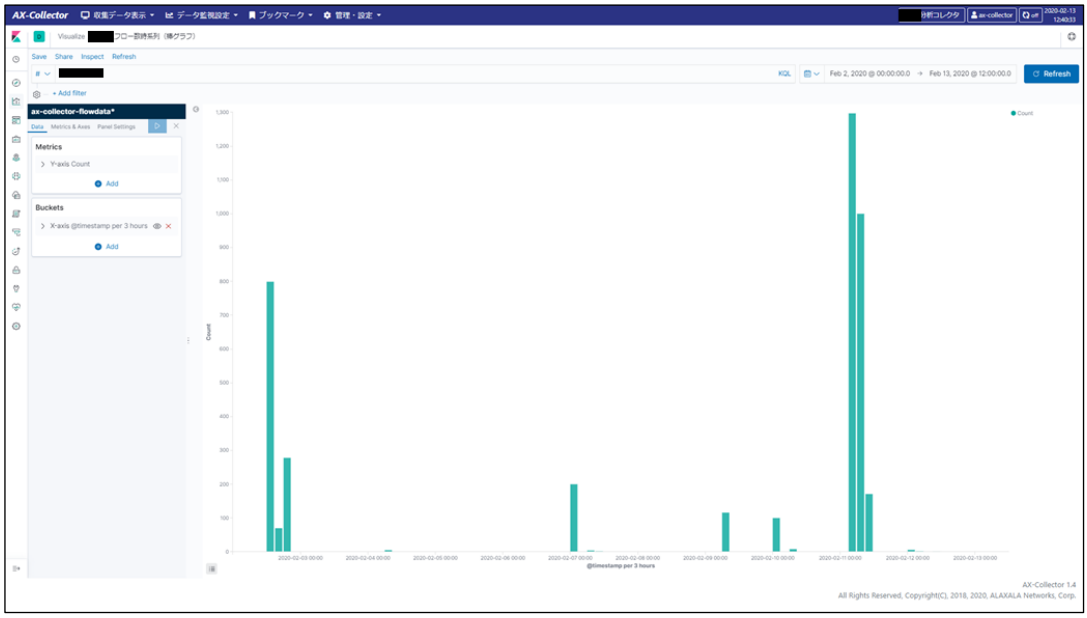

図 1 不審な IP アドレスから検証環境の端末への通信状況の例

図 1 のグラフは、横軸が期間、縦軸が不審な IP アドレスからアクセスのあったフロー数[9]を表示している。期間や宛先となった端末の通信状況を分析することで、マルウェアに感染した可能性のある端末を特定できる。抽出条件とした不審な IP アドレスや検証環境の情報は黒塗りでマスキングしている。

5.2. 脅威となる通信の抽出および解析

5.2.1. 検証項目 B2-1:

統計情報から脅威となり得る通信を分析し、攻撃または調査活動で狙っている端末やポートを抽出できるか

検証結果:

検証環境の端末を対象にした攻撃、または調査活動をしている通信を抽出できた。

検証内容詳細:

[9] フロー数:NetFlow では、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、通信量の組み合わせを 1 つのフローとしてデータに残す。この組み合わせが異なると別のフローとして記録する。例えば同じ送信元 IP アドレスと宛先 IP アドレスにて、ポート番号を 80～89 番までポートスキャンした場合、フロー数として 10 のデータができる。

外部から検証環境の端末に対する High ポート[10]へのポートスキャン[11]を以下の3点の方法で抽出することで、攻撃または調査活動をしている可能性のある通信を抽出できる。

① 宛先ポート番号毎に、宛先 IP アドレスの異なり数[12]を集計することで、外部から攻撃や調査活動として狙っているポート番号を抽出できる。

② 送信元 IP アドレス毎に、宛先 IP アドレスの異なり数を集計することで、攻撃や調査活動をしている外部の IP アドレスを特定できる。

③ 送信元 IP アドレス毎に、宛先ポート番号の異なり数を集計することで、ポートスキャンなどの活動をしている外部の IP アドレスを特定できる。

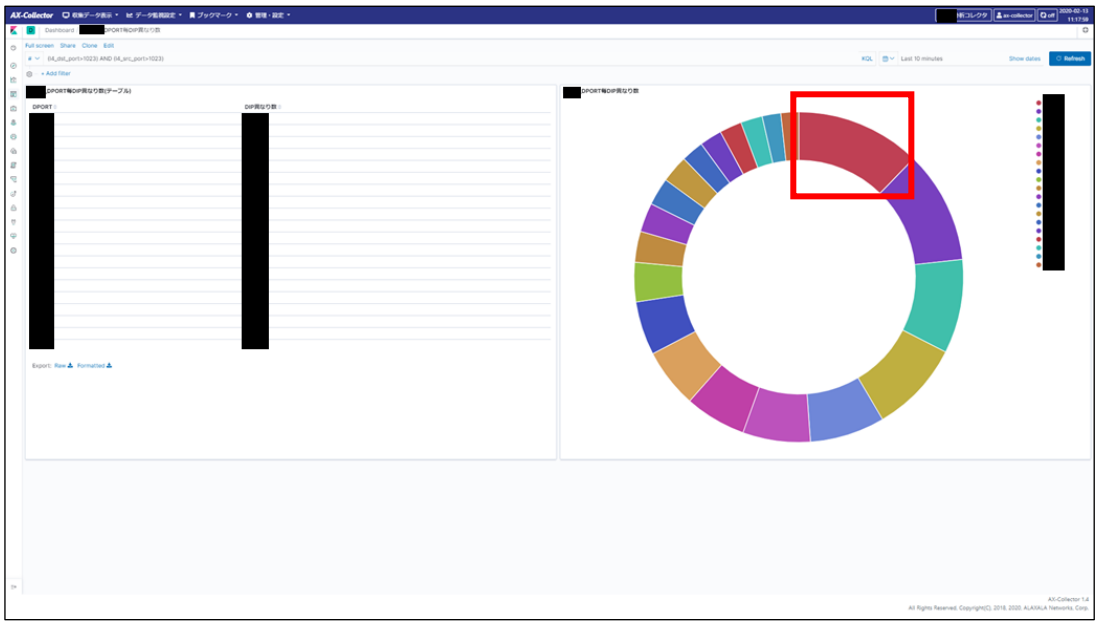

図 2 宛先ポート毎に宛先 IP アドレスの異なり数を表示した例

図 2 のドーナツグラフは、High ポートに限定した宛先ポート番号毎に、宛先 IP アドレスの異なり数を表示している。あるポート番号に対し外部から検証環境の複数端末への通信があると円グラフの幅が広くなる。赤で示すポート番号へのアクセスが一番多い。公開意図がないポート番号の場合、外部から何らかの攻撃や調査を行っている状況が把握できる。宛先ポート番

[10] High ポート:65536 個のポート番号のうち、慣例的に予約されホストで特定のサービスのために使用されるウェルノウンポート番号(0 - 1023)以外のポート番号。アプリケーションによってそれぞれが規定して独自に使用する。

[11] ポートスキャン:ネットワークに接続されているサーバ上の稼働サービスを調査するために、外部から特定のデータを送信して、それに対応する応答を調べる行為。

[12] 異なり数:異なる IP アドレスやポート番号を集計した数。例えば宛先 IP アドレスの異なり数が 10 であれば、10 種類の異なる宛先 IP アドレスに通信があったことを示す。

号、宛先 IP アドレスの異なり数、検証環境の情報は黒塗りでマスキングしている。

5.2.2. 検証項目 B2-2:

統計情報から脅威となり得る通信を分析し、外部からの通信に想定外のポートで応答する設定ミスが疑われる端末を抽出できるか

検証結果:

外部からのポートスキャンなどの通信に対して、TCP[13]/UDP[14]/ICMP[15]で応答している端末を分析することで、設定ミスが疑われる端末の抽出ができた。

検証内容詳細:

ポートスキャンが疑われる通信に対し、期間を限定することで、外部からの通信に応答している組織内端末の抽出が可能である。

本検証の例では、High ポートに対してポートスキャンを行う外部 IP アドレスに対して、応答を返している検証環境の端末を抽出している。該当するプロトコル、ポート番号が外部公開しているサービスの応答であれば問題無いが、意図しない応答の場合、端末の設定ミスなどの可能性があり個別に端末の調査が必要となる。

---

[13] TCP:Transmission Control Protocol(トランスミッション・コントロール・プロトコル)の略。通信プロトコルのひとつ。相手との接続(コネクション)を事前に確立し、通信相手ごとに通信の状態を管理する「コネクション型」と呼ばれる方式を採用しており、到達確認や再送処理を行う特徴がある。

[14] UDP:User Datagram Protocol(ユーザ・データグラム・プロトコル)の略。通信プロトコルのひとつ。UDP はコネクションレス型のプロトコルで、通信相手が確実にデータを受け取ったかどうか確認したり、データの欠落を検知して再送したり、送信順と着信順を一致させるといった制御を行わないという特徴がある。

[15] ICMP:Internet Control Message Protocol(インターネット制御通知プロトコル)とは、通信処理で使われるプロトコルのひとつで、Internet Protocol のデータグラム処理における誤りの通知や通信に関する情報の通知などのために使用される。

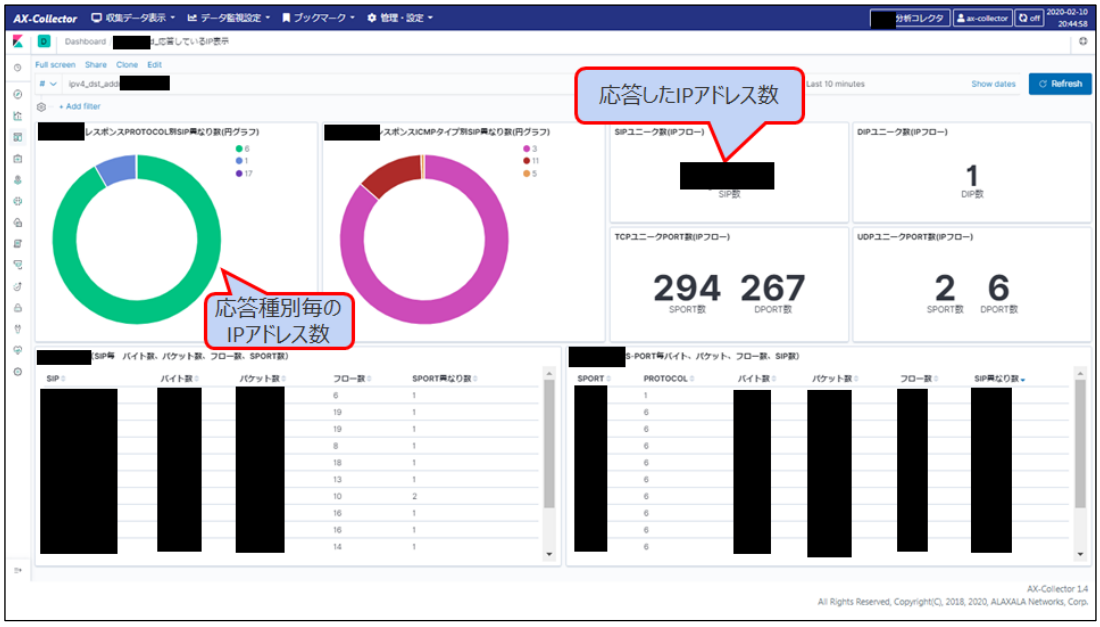

図 3 検証環境から外部へ応答を返している端末の確認例

図 3 は外部からの High ポートに対するポートスキャンに対して応答を返している検証環境の端末の例である。緑のドーナツグラフは、プロトコル番号毎に応答した管理端末の数を表示し、ピンク色のドーナツグラフは ICMP のタイプ別に応答した管理端末の数を表示している。右側には、集計値で応答した端末の総数、TCP と UDP それぞれに対して応答した宛先および送信元ポート番号の数を表示している。下部は端末の IP アドレスおよびポート番号毎に、通信量やパケット数、フロー数などを表示している。意図せず応答を返している場合、設定ミスなどの可能性があるがその状況を把握できる。また、画面をカスタマイズすることで1画面に多くの情報を表示できる。IP アドレス、ポート番号、応答した管理端末の総数、バイト数、フロー数、検証環境の情報は黒塗りでマスキングしている。

5.2.3. 検証項目 B2-3:

不正なデータ転送を調査し、インシデントの被害にあっていないか分析できるか

検証結果:

外部に大量のデータ転送をするインシデントの疑いのある端末は抽出できた。ただし、マルウェアによるデータ流出などのインシデントかどうかは個別に切り分ける調査が必要となる。

検証内容詳細:

大量のデータが流出するインシデントを想定し、検証環境から外部へデータ送信を行う通信量が多い端末の送信元 IP アドレスを抽出する。該当の送信元 IP アドレスから外部の宛先 IP

アドレスやポート番号、データ転送量を確認し、問題ない通信かどうかの切り分けを行う。転送したデータの中身は AX-NV では確認できないため、別途端末等の調査が必要となる。

データ流出を少量ずつ何度も行うような場合は、少ないデータ転送を行う送信元 IP アドレスを対象に調査が必要となる。AX-NV では、サンプリングせずに全通信の NetFlow を記録しているため少ないデータ転送量の通信に対しても分析はできるが、正常通信と切り分けるための分析方法の検討など工夫が必要である。

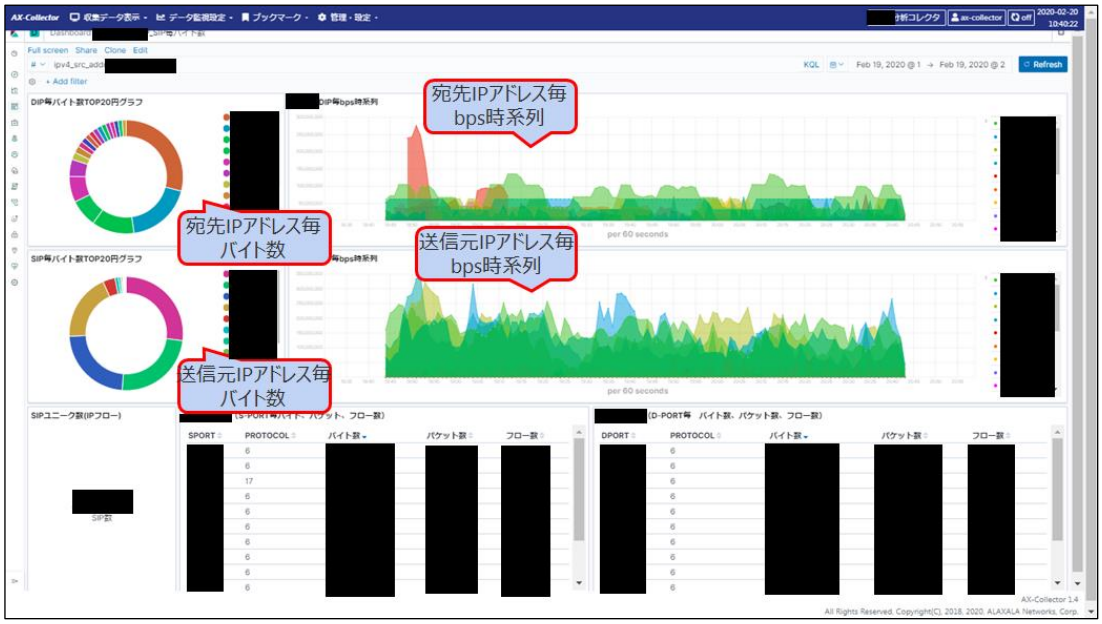

図 4 検証環境から外部へ大量データを送信している端末の確認例

図 4 は検証環境から外部へデータ送信を行う通信を可視化した例である。左側上部のドーナツグラフは外部宛先 IP アドレス毎のバイト数、左側下部は管理端末の送信元 IP アドレス毎のバイト数を表示している。中央上部のグラフは、外部宛先 IP アドレス毎のバイト数を時系列表示しており、中央下部のグラフは管理端末の送信元 IP アドレス毎のバイト数を時系列で表示している。時系列の表示により、期間毎の通信量の状況が把握できる。外部の宛先 IP アドレスが意図しない宛先であれば、管理端末内のなんらかの情報が流出した疑いがある。IP アドレス、ポート番号、バイト数、パケット数、フロー数、検証環境の情報は黒塗りでマスキングしている。

5.3. 既存ネットワークに影響を与えない導入容易性

5.3.1. 検証項目 B3-1:

既存ネットワークに影響がなく容易かつ安全に導入できるか

検証結果:

外付けの設置になるため、既存ネットワークの構成に大きな影響なく導入できた。

検証内容詳細:

検証環境のネットワーク構成は図 5 を参照。既存スイッチにミラーポートを設定し、配下に上り通信データ抽出用の AX-Sensor 1 台と下り通信データ抽出用の AX-Sensor 1 台の計 2 台を設置した。抽出したデータは、通信の可視化や分析を行う AX-Collector 1 台に集約しており、上り下りの全通信をまとめて分析できる。

外付けの設置になるため、既存ネットワークの構成に大きな影響なく導入できた。

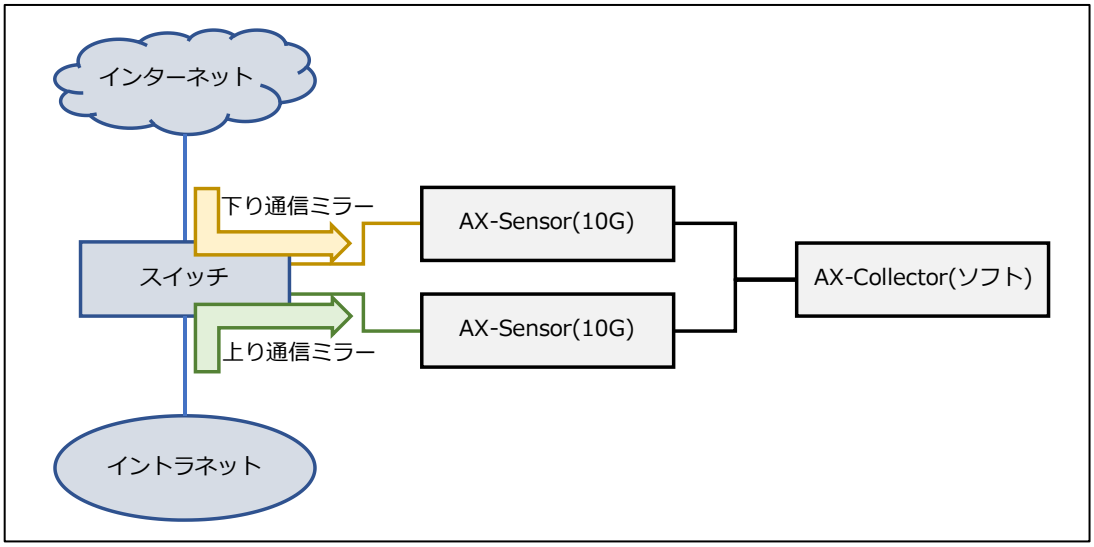

図 5 検証環境の機器構成イメージ(図 1 の再掲載)

5.4. 通信全体の可視化

5.4.1. 検証項目 B4-1:

通信全体を可視化し、統計的にみることで回線利用状況を把握できるか

検証結果:

回線利用状況を含め、通信全体または一部の可視化ができる。各種グラフや統計情報を利用し、通信状態を複数の観点で表示できた。

検証内容詳細:

ダッシュボード機能を使った例では通信量(バイト数)、パケット数、フロー数に対して、総量、時系列グラフや、IP アドレス、ポート番号、プロトコル番号毎の通信量(バイト数)をまとめて

表示したり、グラフではなく集計した数字で表示したりもできる。カスタマイズすれば 1 画面に多くの情報が表示でき、現在の通信状況を俯瞰して把握できる。

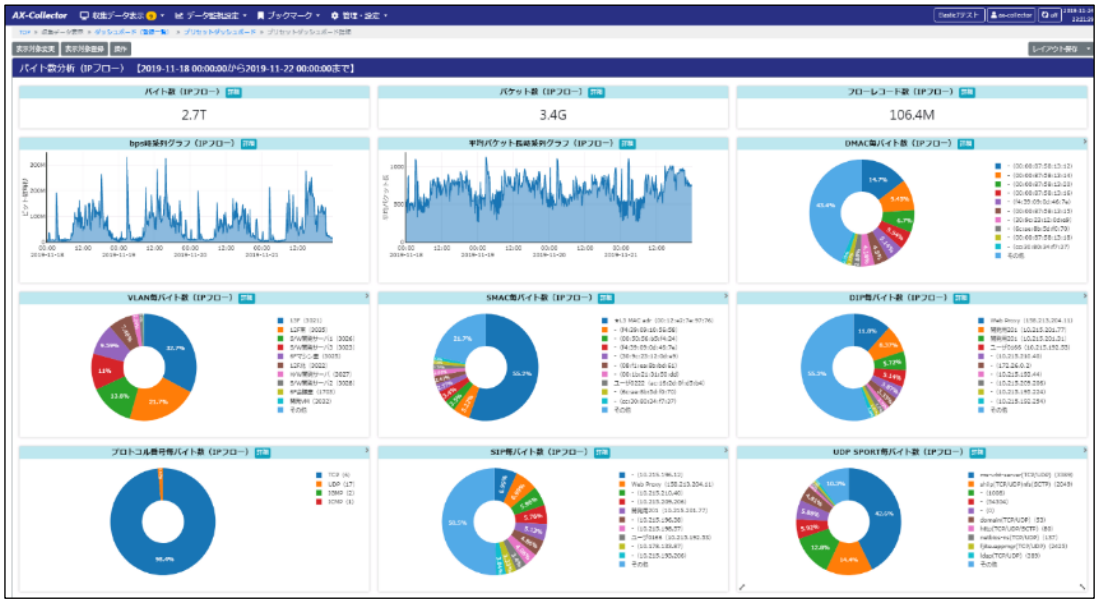

図 6 通信全体を俯瞰したダッシュボード（アラクサラネットワークスより提供）

ダッシュボード機能により、一定期間の通信状況を可視化できる。通信量（バイト数）、パケット数、フロー数に対して、総量、時系列グラフや、IP アドレス、ポート番号、プロトコル番号毎の通信量（バイト数）をまとめて表示している。

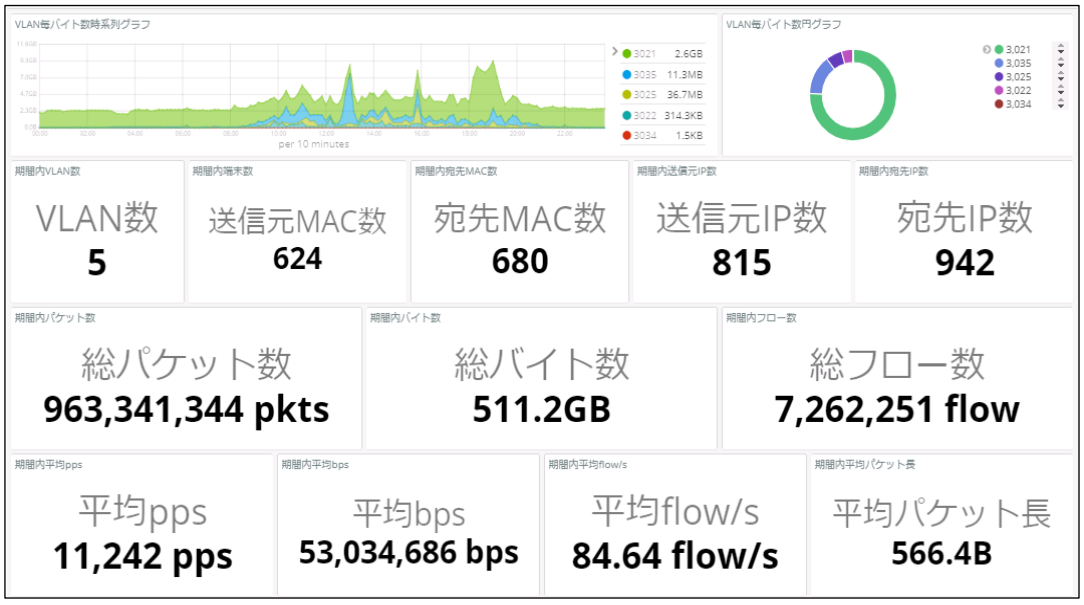

図 7 1 日の通信を可視化した例（アラクサラネットワークスより提供）

可視化は各種形式のグラフ表示や数字による表示ができる。図 7 は 1 日の通信を可視化した例であるが、宛先 IP アドレス数や通信量や通信速度などの情報をまとめて直感的に把握できる。

5.4.2. 検証項目 B4-2:

ネットワーク管理者が認知していない管理外の端末を洗い出せるか

検証結果:

管理下にある端末に予めエイリアス(名前)を付加することで、洗い出しができた。

検証内容詳細:

資産管理している端末の IP アドレスや MAC アドレスに紐付くホスト名をあらかじめエイリアスとして登録しておけば、ホスト名一覧を表示できる。このときにホスト名が未登録の場合、「-」で表示されるためシャドーIT[16]など管理者が認知していない端末を把握できる。

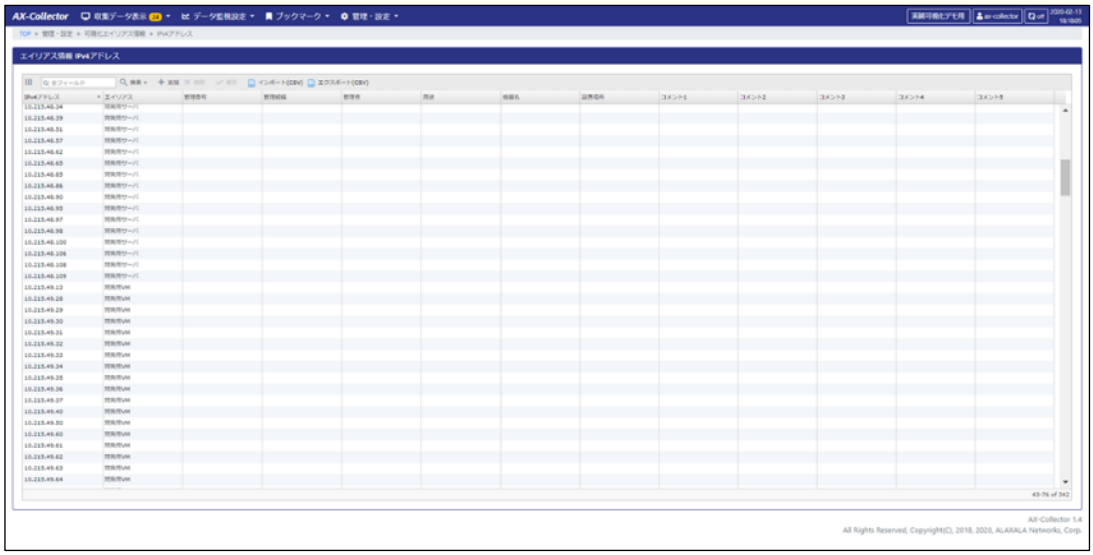

図 8 管理している端末のエイリアスを登録(アラクサラネットワークスより提供)

資産管理している端末情報から IP アドレスに対応するホスト名をエイリアスとして登録する。今回の例は IP アドレスに対して登録しているが、MAC アドレスに対してエイリアス登録もできる。

[16] シャドーIT:企業・組織が利用の実態や存在を把握していない、従業員または部門が業務に利用しているデバイスやクラウドサービス等を指す。

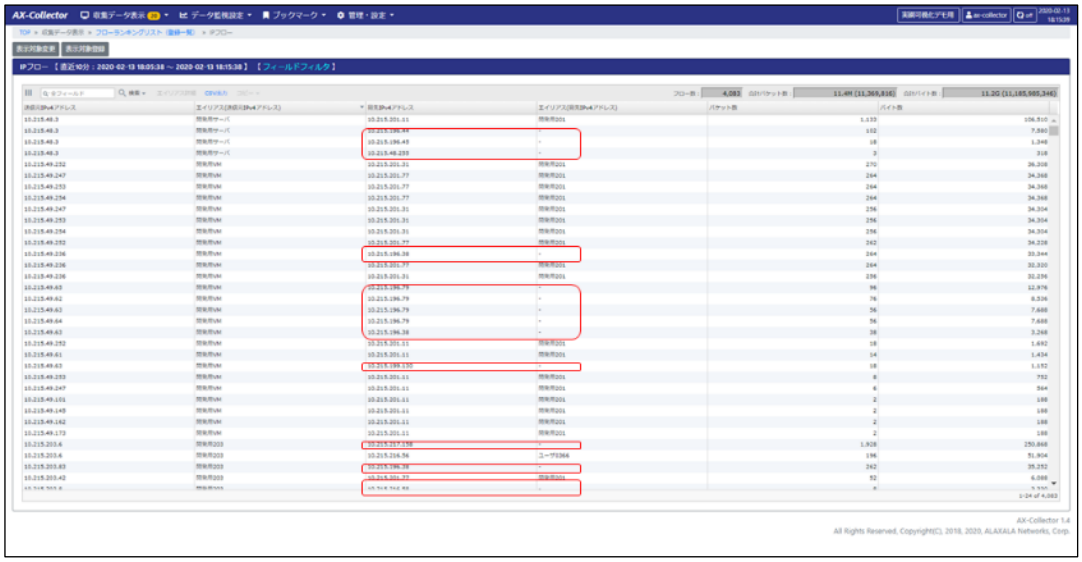

図 9 未登録ホストを表示した例（アラクサラネットワークスより提供）

ホスト名が登録されてない端末は、ホスト名の部分は「-」の表示になる。シャドーIT など回線を利用しているにも関わらず資産管理できていない端末を容易に確認することができる。

6. まとめ

AX-NV は、NetFlow 技術を使って通信全体を可視化するためのソリューションである。サンプリングせずにデータを保持しているため、過去に遡って通信状況の調査・分析ができ、セキュリティの観点においても活用できる。同じくネットワーク監視をする IPS/IDS[17]のように攻撃通信をシグネチャで検知する製品ではなく、全体の通信に対してインシデントの影響調査や、新たな脅威を分析する際に有効である。そのため IPS/IDS から切り替える製品ではなく、補完関係になる製品といえる。今回は、検証に至らなかったが、サンプリングせずに全データを保持していることから、セキュリティ監視製品を回避するために少しずつ情報漏えいさせる攻撃の検知にも使える可能性がある。

カスタマイズ性は高く、セキュリティと通信レイヤーの知識が必要であるが通信の宛先や送信元、通信量などを抽出・集計ができ、さまざまな観点の分析ができる。

近年、常時 SSL 化など多くの通信が暗号化され、IPS/IDS がシグネチャによる監視ができないケースもあるが、AX-NV では通信が暗号化されていても NetFlow が見ているデータには変わりが無いため、平文の通信と同じ条件で監視・分析ができることも特徴である。

---

[17] IDS：Intrusion Detection System の略。悪意のある第三者からのアクセス・侵入を検出し通知する侵入検知システム。

ネットワーク全体の通信可視化については、全体を俯瞰して直感的に状況を把握できる機能があり、ネットワークオペレーションセンター（NOC)のソリューションとして活用できる。

これまで長い経験と深い知見が必要とされていたデータ分析が AX-NV を導入することで容易となり、様々な脅威への対策が迅速に行えるだけでなく、ネットワーク管理コストの軽減に貢献するソリューションといえる。

7. 用語集・略語集

High ポート:

65536 個のポート番号のうち、慣例的に予約されホストで特定のサービスのために使用されるウェルノウンポート番号(0 - 1023)以外のポート番号。アプリケーションによってそれぞれが規定して独自に使用する。

ICMP:

Internet Control Message Protocol(インターネット制御通知プロトコル)とは、通信処理で使われるプロトコルのひとつで、Internet Protocol のデータグラム処理における誤りの通知や通信に関する情報の通知などのために使用される。

IDS:

Intrusion Detection System の略。悪意のある第三者からのアクセス・侵入を検出し通知する侵入検知システム。

IPS:

Intrusion Prevention System の略。不正な通信を検出し通知するほか、その通信を遮断する機能を持つ侵入防止システム。

IP リーチャブル:

IP パケットが到達可能であること。

MAC アドレス:

Media Access Control address の略で、ネットワーク機器固有のアドレス。

SSL:

Secure Sockets Layer(セキュア・ソケット・レイヤー)の略。インターネット上でのデータの通信を暗号化し、盗聴や改ざんを防ぐ仕組み。

TCP:

Transmission Control Protocol(トランスミッション・コントロール・プロトコル)の略。通信プロトコルのひとつ。相手との接続(コネクション)を事前に確立し、通信相手ごとに通信の状態を管理する「コネクション型」と呼ばれる方式を採用しており、到達確認や再送処理を行う特徴がある。

UDP:

User Datagram Protocol（ユーザ・データグラム・プロトコル）の略。通信プロトコルの一つ。UDP はコネクションレス型のプロトコルで、通信相手が確実にデータを受け取ったかどうか確認したり、データの欠落を検知して再送したり、送信順と着信順を一致させるといった制御を行わないという特徴がある。

アンチウイルス：

コンピュータウイルスを検出・除去するためのソフトウェア。ウイルスなどの特徴を記録したデータファイルとコンピュータ内部でやり取りされるデータを比較し、ウイルスなどを検出する「パターンマッチング型」と、検査対象のデータを自動的に解析し、ウイルスのような不審な振る舞いをするプログラムコードやウイルス特有のプログラムコードが含まれていれば、ウイルスとして検出する「ふるまい検知型」がある。

インシデント：

ISO22300 (2.1.15)では「中断・阻害、損失、緊急事態、危機に、なり得るまたはそれらを引き起こし得る状況」と定義されている。

エイリアス：

別名、通称などの意味。

クラウド：

インターネット等のネットワーク経由で、ユーザーにサービスを提供する形態。

コレクタ：

AX-NV を構成する機器の 1 つ。ネットワーク機器からデータを集約し、可視化や異常検知をするサーバ上で動作するソフトウェア。

コントローラ：

AX-NV を構成する機器の 1 つ。以上を検知した際に、ネットワークの制御をするサーバ上で動作するソフトウェア。

サイバーセキュリティサーベイ 2019：

KPMG コンサルティング「「サイバーセキュリティサーベイ 2019」
https://home.kpmg/jp/ja/home/insights/2019/09/cyber-security-survey-2019.html

サイバーセキュリティビジネス化：

産業サイバーセキュリティ研究会 WG3 サイバーセキュリティビジネス化

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/index.html

サイレント故障：

コンピュータシステム上の監視ツールで検知できない障害を指す。サイレント故障の多くは、パフォーマンスの低下やネットワークの遅延、または通信不能といった状況で発覚することが多い。

シグネチャ：

セキュリティにおけるシグネチャとは、コンピュータウイルスなどに含まれる特徴的なデータ断片や、サイバー攻撃に含まれる特徴的なパターンやルールを指す。

シャドーIT：

企業・組織が利用の実態や存在を把握していない、従業員または部門が業務に利用しているデバイスやクラウドサービス等を指す。

スイッチ：

コンピュータネットワークの集線装置の一種で、受信したデータの宛先を見て、接続された各機器への転送の可否を判断する機能を内蔵したもの。「ネットワークスイッチ」とも。

ソリューション：

解決策や回答などの意味を指す。特に IT 分野では、企業がビジネスやサービスについて抱えている問題や不便を解消すること、および、そのために提供されるシステム製品やサービスなどを指す。

ダッシュボード：

様々なデータを収集して簡潔にまとめ、集約して表示する画面を指す。

バイト数：

データ量の単位。1 バイト＝8 ビット。AX-NV では通信量をバイト数で表示する。

パケット数：

ネットワーク経由でやりとりされる情報の伝送単位であるパケットがいくつ送ったか示す数量。

フロー数：

NetFlow では、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、通信量の組み合わせを 1 つのフローとしてデータに残す。この組み合わせが異なると別のフローとして記録する。例えば同じ送信元 IP アドレスと宛先 IP アドレスにて、ポート番号を 80～89 番までポートスキャンした場合、フロー数として 10 のデータができる。

プロトコル：

通信に関する規約を定めたもの。「通信プロトコル」とも。

ポートスキャン：

ネットワークに接続されているサーバ上の稼働サービスを調査するために、外部から特定のデータを送信して、それに対応する応答を調べる行為。

マルウェア：

malicious software の略語で、悪意のソフトウェア。

マルチバイト文字列：

1 文字を複数バイトで表す体系。日本語の全角文字等が該当する。

ミラーポート：

ネットワークスイッチやルータの持つ機能の一つである、あるポートが送受信するデータを、同時に別のポートから送出する機能である「ポートミラーリング」において、コピーされたデータが流れてくる側のポート。

異なり数：

異なる IP アドレスやポート番号を集計した数。例えば宛先 IP アドレスの異なり数が 10 であれば、10 種類の異なる宛先 IP アドレスに通信があったことを示す。

産業サイバーセキュリティ研究会：

経済産業省　産業サイバーセキュリティ研究会

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html

以上