Computer Security Symposium 2020
26 - 29 October 2020

ゼロデイ攻撃対策のための
宛先ポートごとのアクセス傾向モデルの提案と分析

辻本 真喜子[1]　芦野 佑樹[2]　中村 康弘[3]

概要：ポート番号別の脆弱性情報が公開される前に，そのポート番号に集中して行われる接続要求はゼロデイ攻撃の可能性が高いと考えられる．ゼロデイ攻撃は，過去の観測で得たシグネチャを用いることができないため，脅威が顕在化するまで攻撃の存在を検知できないという問題がある．そこで本研究では，過去に報告された 10 件の脆弱性情報の公開時期とその前後の長期間における接続要求の観測結果の傾向を調査し，アクセス傾向のモデル化を行った．不特定多数の接続要求パケットに対してこのモデルを適用することで，未知の脆弱性を狙う攻撃通信の候補を識別できる可能性を見出した．今後，アクセス傾向のモデルを抽出するアルゴリズムを実装することにより，脆弱性情報が公開される前の段階でゼロデイ攻撃パケットを検知できるものと考える．

キーワード：ゼロデイ攻撃，ネットワークセキュリティ，早期警戒，パケット分析，大容量通信データ

Access Pattern Modeling and Analysis for Minus-day Detection of Zero-day Attacks
Focusing Source Address Which Obsessed with a Specific Port

Tsujimoto Makiko[1]　Ashino Yuki[2]　Nakamura Yasuhiro[3]

Abstract: In this study, we investigate the tendency of the observations of 10 vulnerabilities reported in the past, and model the access tendency. By applying this model to a large number of connection request packets, we have discovered the possibility to identify candidates for attacks that target unknown vulnerabilities. In this future, we will implement an algorithm to extract models of access tendencies, which will enable us to detect zero-day attacks before the vulnerability disclosure.

Keywords: zero-day attacks, network security, early warning, packet analysis, big communication data

1. はじめに

近年，脆弱性に対する修正プログラムが適用されていない期間において，当該脆弱性を狙ったゼロデイ攻撃の被害が深刻化している．[1][2]．現在までに，パターンマッチングや通信量の変化に基づいて攻撃通信を検知する研究がある．しかしながら，ゼロデイ攻撃の中には開発者が把握していない脆弱性を標的としたものが存在する．さらに，このような脆弱性の情報を保有する者は，限られているため[3]通信が急増するとは限らない．脆弱性情報公開前に脆弱性のある特定のサービスを狙った通信が発生した場合，それは攻撃者によるゼロデイ攻撃通信の可能性が高いと考えられる．そしてこの通信を観測することにより未だ発見されていない脆弱性への攻撃を発見できる可能性が期待できる．本研究では，ゼロデイ攻撃はシグネチャを利用できない，通信量が急増しないことを前提とし，特定のポート番号のみにアクセスする送信元アドレス数の累計に着目し，累計傾向モデルを提案する．特定アドレス範囲へのすべての着信を観測するセンサが 2017/1/1～2018/12/31 の期間に観測した結果と同期間に公開された 10 件の脆弱性情報について提案手法を適用し，特定のポート番号のみにアクセスする送信元アドレス数を累計することにより，脆弱性情報公開日前にゼロデイ攻撃を捉えられる可能性があることを示す．

2. 研究背景

2.1 脆弱性情報とゼロデイ攻撃

プログラムの脆弱性に関する情報(以下，脆弱性情報)は，開発者としては脆弱性を解消するために必要な情報である．また，ユーザとしては，セキュリティ対策のために必要な情報となる．一方で，攻撃者にとって脆弱性情報は特定の

1 防衛大学校理工学研究科サイバーセキュリティ工学研究室
Cyber Security Engineering, Graduate School of Science, and Engineering, National Defense Academy
2 日本電気株式会社ナショナルセキュリティー・ソリューション事業部 サイバー防衛技術グループ
Cyber Defense Technology Group, National Security Solution Division, NEC Corporation
3 防衛大学校　情報工学科
Computer Science, National Defense Academy

プログラムにおける脆弱性の存在を示す情報になる．攻撃者は脆弱性情報を用いて，当該脆弱性を利用した攻撃通信(以下, 攻撃通信)を行う，または攻撃ツールを作成する可能性がある．脆弱性は発見が困難である上に，発見者により悪用される恐れがある．脆弱性が悪用される前に適切に対処することを目的として，脆弱性情報を管理する組織に報告する制度や脆弱性発見報酬制度があり，開発者にも脆弱性情報が提供される．このような取り組みがある一方で，修正プログラムの公開前に脆弱なプログラムに対する攻撃通信がある[1]．修正プログラムが適用されていない状況下での攻撃通信を一般にゼロデイ攻撃と呼ぶが, 本論文では，修正プログラム公開前のインターネット経由の攻撃通信をゼロデイ攻撃通信と称し以降の議論で用いる．開発者がプログラムの脆弱性を認識してから修正プログラムが提供されるまでは時間を要する．修正プログラムが提供されるまでの期間に脆弱性が悪用されると，さらに被害が拡大する恐れがある．そのため，修正プログラムが公開されるまでの間, 攻撃の兆候を早期に検出して対処を促す必要がある．

2.2 関連研究

2.2.1 パターンマッチングに基づいた検知方法

通信の中からゼロデイ攻撃通信を識別できれば，その識別情報を基にゼロデイ攻撃通信を遮断できる．これによりゼロデイ攻撃通信によってプログラムが受ける影響を最小限に抑えることが期待できる．ゼロデイ攻撃通信を含む攻撃通信の検知には，攻撃通信の特徴を記録してシグネチャとし, これを用いたパターンマッチング技術が用いられる．この技術を応用したものに, 侵入検知システム(IDS)がある．

しかしながら，脆弱性情報公開前の期間においてはゼロデイ攻撃通信を識別することができず，シグネチャは作成できないため，ゼロデイ攻撃通信を検知することはできない．

2.2.2 観測した通信量の変化に基づいた検知方法

脆弱性情報が公開された後は攻撃ツールが作成されるため，攻撃通信が急増することが知られている．この通信量の変化は普段では発生しないことかから，セキュリティ業務に従事する組織が公開する分析レポートには，通信量の変化を併せて記載することが多い．

ゼロデイ攻撃通信の発見は観測センサにおいて特定のサーバや特定のポート番号への通信量が急増し，急増した通信を分析した結果，脆弱性が発見される場合がある．このため各企業や組織はハニーポットなどの観測センサを設置し，通信量を観測，分析している[4][5][6][7].

2.3 本研究の位置づけ

本節では，時系列における脆弱性とゼロデイ攻撃の関係を示した図 1 に基づいて，本研究の位置づけを述べる．

2.2.1 で述べたパターンマッチンで用いるシグネチャの作成には，通常の通信の中からゼロデイ攻撃通信を識別し取り出さなければならない．しかしながら，ゼロデイ攻撃通信を識別するために必要である脆弱性情報が提供されない限りは，パターンマッチングによるゼロデイ攻撃通信の検知は難しい．そのため，パターンマッチングに基づいたゼロデイ攻撃通信の検知が有効であるのは図 1 中の期間(B)以降である．

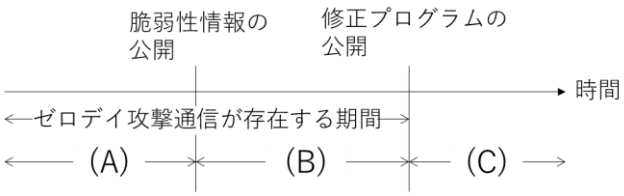

図 1 ゼロデイ攻撃のイベントの時系列

2.2.2 で述べた通り，多くの攻撃者は公開された脆弱性情報に基づいて作成した攻撃ツールを実行していると推定できる．そのため，攻撃通信が急増するのは期間(B)以降であると言える．

昨今のゼロデイ攻撃被害から，脆弱性情報が公開される前(図 1 期間(A))に脆弱性情報を保有している攻撃者がいることが考えられる．脆弱性情報公開前であるため，この時期に攻撃を行う者はプログラムに対する高度な知識を持っている可能性が高い．このような，高い能力を保有した攻撃者の数は，攻撃者全体からすると非常に少ない割合であることが知られている[3]．このことから，図 1 期間(A)においては大量のゼロデイ攻撃通信が発生することはなく，2.2.2 で述べたような通信量の変化に基づいてゼロデイ攻撃通信を検知することは難しい．

仮に，脆弱性情報公開前(図 1 期間(A))に，ゼロデイ攻撃通信の存在を示すことができれば，ゼロデイ攻撃通信の影響を最小限にとどめることが期待できる．また，開発者に対して前述の情報を伝えることで，修正プログラムの作成に着手する時期を早めることができ，結果として修正プログラムを早期の提供につなげることができる．

そこで本研究では，脆弱性情報公開前(図 1 期間(A))の期間におけるゼロデイ攻撃通信の兆候を分析する手法を提案する．

3. 提案手法

脆弱性公開前にゼロデイ攻撃通信を発見するためのアプローチとその分析手法を以下に述べる．

3.1 課題解決のためのアプローチ

3.1.1 特定のポート番号だけを狙うホストからの通信

シャノン・ウィーバーらが提唱した通信モデル[8]によると，通信が発生する場合は必ず送信元の意図を伴う．すなわち通信は，人が「通信する」という目的によって発生し，自然発生する通信は存在しない．この通信モデルは特定のポート番号宛への通信にも当てはまる．

ある送信元ホストが宛先ホストの複数のポート番号に対して通信すると，宛先ホストで使用可能なポート番号を探すことができる．これにより研究機関やセキュリティベンダはインターネット接続機器に関する情報収集のための調査活動[9][10][11]として利用でき，攻撃者は攻撃の準備段階に該当する走査活動[12]として利用できる．一方で，特定のポート番号のみに通信する場合，例えば 80/TCP への通信は，宛先ホストが 80/TCP においてサービスを提供しているため，そのサービスを利用しようとする 80/TCP への通信が発生する．この通信モデルに基づくと，ある送信元ホストがある特定のポート番号だけに通信するのはそのポート番号で提供しているサービスを利用するという目的をもっているからであり，脆弱性のある特定のポート番号を狙う攻撃者からの攻撃通信もこのモデルに当てはめることができる．

3.1.2 特定のポート番号のみを狙うアドレス数の観測

脆弱性情報公開前に脆弱性の存在に気付いている攻撃者は限られている．よって，通信量だけを観測しても攻撃を発見できるとは限らない．

そこで，特定の宛先ポート番号だけに接続要求を行う送信元アドレス数の累計値に注目することによって，脆弱性情報公開前であっても攻撃通信発生の有無を観測できる．

2.2.2 で述べた通り，脆弱性情報が公開されると，公開された情報を利用した攻撃プログラムが作成される．そのため，当該ポート番号を狙った送信元アドレス数は急増する．

一方で，脆弱性情報公開前の当該ポート番号だけに送信するアドレス数は今まで着目されておらず，アドレス数の推移や傾向がどのように表れるか不明であった．

脆弱性情報公開前に当該ポート番号だけを狙う送信元アドレスは脆弱性をあらかじめ知っている可能性が高いと考えられる．

2.3 で示した図 1 の(A)の期間は，攻撃者が脆弱性に基づいて作成したツールを実行した通信を観測者が初めて観測した日(攻撃初回観測日)の前後でさらに期間(A0), 期間(A1)に分割する(図 2).

図 2　ゼロデイ攻撃イベント時系列の分類

A0 の期間は特定の脆弱性を狙った攻撃が観測されない期間である．よって A0 の期間には攻撃目的の通信は発生しない. A1 の期間は一部のユーザもしくは攻撃者が脆弱性に気付いている期間である．脆弱性情報が公開されていない期間であるため，限られた送信元アドレスからしか攻撃通信は発生しないと考えられる．このアプローチが適切であれば，特定の宛先ポート番号だけに接続要求を行う送信元アドレス数の累計値を時系列でグラフにすると図 3 のような傾向を示すものと推定できる．

(A0)　ユーザや攻撃者が脆弱性に気付かないために，当該ポート番号のみに通信するアドレス数は皆無．

(A1)　限られた攻撃者が脆弱性を悪用するため送信元アドレス数の累計値はわずかな増加傾向が表れる．

(B)　脆弱性情報が一般的に公開された後であるため送信元アドレス数の累計値は爆発的に急増する．

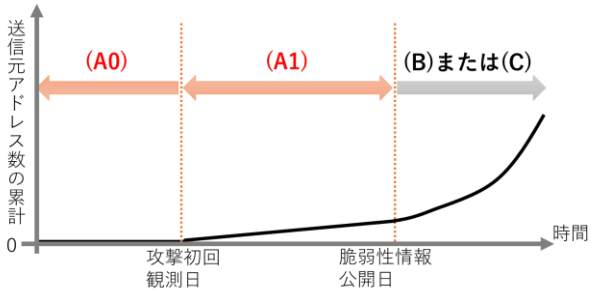

図 3　特定ポート番号のみに通信する送信元アドレス数の累計の時系列変化のモデル図

3.2　分析手順

3.1 で述べたアプローチの分析手順について説明する．はじめに，特定の宛先ポート番号だけに接続要求を行う送信元アドレス数の累計値を求めるための方法を示す．これを実現するため，分析期間において分析対象ポート番号に初めて観測された送信元アドレス数の 1 日単位の累計を求める．図 4 に累計の求め方の一例を示す．

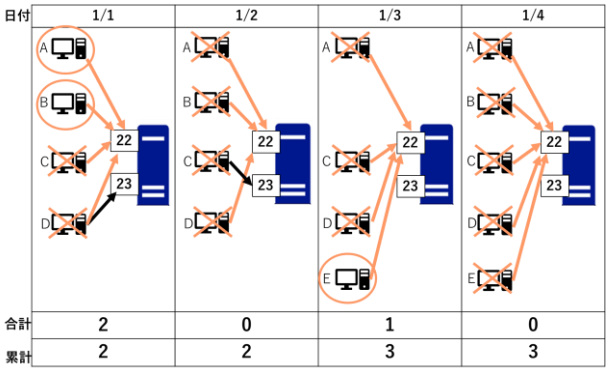

図 4　分析対象ポート番号のみに通信する送信元アドレス数の初回観測日の合計と累計の出力の概要例

図 4 の例では分析対象ポートを 22 番，分析対象期間は 1/1～1/4 とした．まず，1/1 に観測された送信元アドレスは A，B，C，D の 4 アドレスである．このうち，22 番だけに通信しているのは A，B の 2 アドレスだけである．

A は 1/1～1/4 の全期間において 22 番ポートとしか通信していないため，初回観測日である 1/1 に 22 番ポートのみに通信する送信元アドレス数としてカウントする．

B も 1/1 に 22 番ポートのみに通信する送信元アドレス数

としてカウントする．1/3 は B からの通信は観測できていないが，分析対象期間中は 22 番ポートにしか通信していないため，1/1 の B のカウントに変更はない．

C は 1/1 の初回観測日には 22 番ポートとしか通信していないため，当初 1/1 に 22 番ポートのみに通信する送信元アドレス数としてカウントする．しかし 1/2 に 22 番ポート以外と通信しているため，1/1 の送信元アドレス数としてのカウントは削除され(図 4 において×として表記)，1/1～1/4 の全期間において 22 番ポートのみに通信する送信元アドレス数としてカウントされない．

D は 1/1～1/4 までの間毎日 22 番ポートに通信しているが，1/1 では 22 番ポート以外にも通信しているため，C と同様 1/1 のカウントは削除され，1/1～1/4 の全期間において 22 番ポートのみに通信する送信元アドレス数としてカウントされない．よって 1/1 の送信元アドレス数の合計は 2(A と B)となり，累計も 2 である．翌日の 1/2 は 22 番ポートのみに通信する新規の送信元アドレス数はないため，合計値は 0 となり，累計は昨日の 1/1 の 2 のままである．

E は 1/3 に新規に観測され，1/3，1/4 の両日とも E は 22 番ポートとしか通信をしていないため，E の初回観測日である 1/3 に送信元アドレスの合計は 1 となり，累計は 3 となる．

上記のようにして，初回観測日における特定のポート番号のみと通信する送信元アドレス(以下，初出送信元アドレス)を求め，その 1 日単位の合計，累計を求める．

この例を一般化すると，以下の①～⑤の手順により，特定のポート Pn(0≦Pn≦65535)のみに観測された初回観測日における送信元アドレス数の累計処理ができる．

① 観測センサを用いてキャプチャした通信データを観測対象期間分(⊿x(day))取り出す．
② 宛先ポート Pn に送信する送信元アドレスからのすべての宛先ポート番号のセットを作成し，このセットを S とする．
③ S から宛先ポート番号の種類数が 1 かつ宛先ポート番号が Pn である送信元アドレスを抽出し，そのアドレス群を T とする．
④ T が最初に観測センサに出現する日を求め，その日における送信元数を求める．
⑤ 送信元数の 1 日単位の累計を求める．

累計処理終了後，横軸を時間，縦軸を累計としたグラフを作成し，当該脆弱性の情報公開日をグラフにプロットする．

上記手順で得られた脆弱性公開日前に特定のポート Pn のみに通信するアドレスはゼロデイ攻撃を行う攻撃者である可能性が高いと判断する．

4. 実験

提案手法の有効性を検証するため，実験を行った．

4.1 実装

防衛大学校の境界ルータで TCPdump により通信をキャプチャし，pcap ファイルを取得する．近年のサイバー空間は通信量が多いため分析が難しい．そこで，取得した通信データをデータベースに格納し，SQL で処理アルゴリズムを実装した．使用するデータベースは SQLite3 を用いた．

4.2 データセット

本研究で使用するデータセットは，防衛大学校で設置した観測センサが 2017/1/1～2018/12/31 の間に取得したデータである．観測センサはグローバルアドレスが割り当て済みの 1,501 アドレスである．各アドレスは AS に属し，BGP 広告を出しているが，機器が割り当てられていないためサービスは提供していない．データセットの緒元を表 1 に示す．

表 1 データセット緒元

ファイル形式	libpcap
観測期間	2017/1/1～2018/12/31
センサアドレス数	1,501 アドレス
データ容量	11.78TB
パケット数	138,842,348,649 パケット (約 1,388 億 4,234 万パケット)

4.3 検証に用いる脆弱性と公開日

実験に用いる脆弱性情報の宛先ポート番号/プロトコル，当該ポート番号における脆弱性と脆弱性情報公開日を表 2 に示す．公開日はその脆弱性が初めて web ページに公開された日である．使用した web ページは脆弱性情報データベース(NVD)[13]のリファレンスに掲載されているもの，セキュリティベンダの報告，国際会議の日程，公共機関のレポートである．当該 web ページからでは現地時間とグリニッジ標準時を判別できない脆弱性があった．分析する期間は 2 年間であり，1 日の誤差は 0.15%未満である．よって現地時間とグリニッジ標準時とでは大きな誤差はないと判断し，公開日の日付はグリニッジ標準時として扱う．web ページにグリニッジ標準時の記載のあったものは GMT と併記した．脆弱性は 3.1.2 で述べた(B)期間を得ることができるように，2017/1/1～2018/12/31 の期間に公開されたものを用いた．脆弱性の識別には共通脆弱性識別子(CVE)[14]を用いる．

7001/TCP はこの期間中 2 種類の CVE が登録されたが，最初に登録された CVE-2017-1027 の公開日を実験に用いた．

11211 ポートについては脆弱性の対象プロトコルが TCP と UDP であったため併記している．

表 2　脆弱性情報と公開日

宛先ポート番号/プロトコル	CVE	公開日
37215/TCP	CVE-2017-17215[15]	2017/1130[16]
5555/TCP	CVE-2018-0701[17]	2018/2/4[18]
3001/TCP	CVE-2017-15236[19]	2017/10/3[20]
4786/TCP	CVE-2018-0171[21]	2018/3/28(GMT)[22]
6379/TCP	CVE-2017-9805[23]	2017/9/5[24]
7001/TCP	CVE-2017-10271[25] CVE-2018-2628[26]	2017/10/18[27]
7070/TCP	CVE2018-13115[28]	2018/7/2[29]
10554/TCP	CVE-2017-8223[30]	2017/3/8[31]
11211/TCP, 11211/UDP	CVE-2017-9805[32]	2017/11/9[33]
37777/TCP	CVE-2017-6432[34]	2017/1/20[35]

4.4　適用結果

4.4.1 ポート 37215/TCP

37215/TCP における適用結果を図 5 に示す.

縦軸は 37215/TCP のみに送信する初出送信元アドレス数と, それを日ごとに累計した値(対数表示)であり, 横軸は時間である.

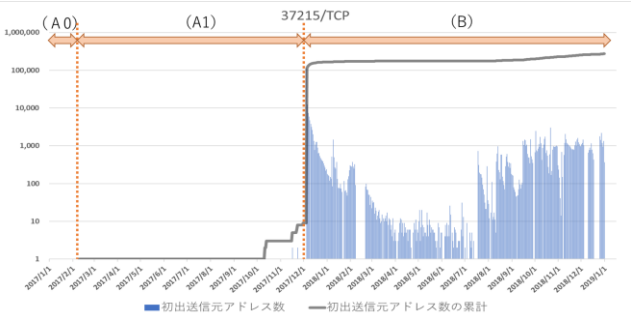

図 5　37215/TCP における
初出送信元アドレス数とその累計

図中の(A0), (A1), (B)は, 3.1.2 で述べた各期間を表す. 37215/TCP では 2017/2/9 に初めてこのポート番号のみに通信するアドレスが 1 アドレス観測された. その後しばらくはこのポート番号のみに送信するアドレスは観測されなかったが, 2017/10/2 に 2 つ目のアドレス, 2017/10/13 に 3 つ目のアドレスと間隔をあけて観測され, 2017/11/30 に累計 9 つ目のアドレスが観測されたあと, 2017/12/5 には前日より 1 万種以上増加し, 112,623 アドレスが観測センサに到達した(表 3).

表 3　日付とアドレス数と累計

日付	アドレス数	累計
2017/2/9	1	1
2017/10/11	1	2
2017/10/13	1	3
2017/11/16	2	5
2017/11/22	1	6
2017/11/23	2	8
2017/11/30	1	9
2017/12/5	112623	112632
2017/12/6	12357	124989

この結果から 2017/2/8 まではこのポート番号だけを狙うアドレスは存在しなかったことと, この脆弱性公開日は 2017/11/30 であり, それまでの間は計 9 アドレスがこのポート番号を狙っていたことがわかる. アドレス数が急増したのは公開から 5 日後の 2017/12/5 であった.

4.4.2 ポート 5555/TCP

提案手法を 5555/TCP に適用した結果を図 6 に示す. 縦軸は 5555/TCP のみに送信する初出送信元アドレス数と, それを日ごとに累計した値(対数表示)であり, 横軸は時間である.

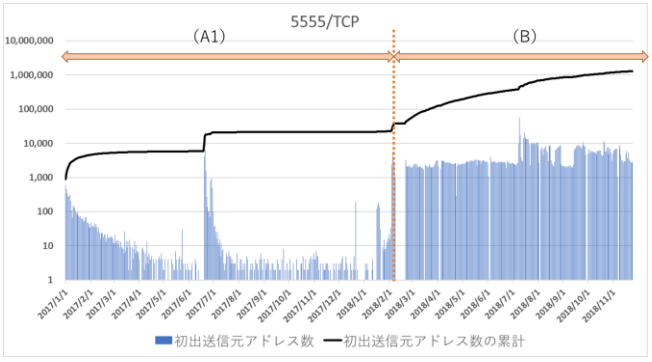

図 6　5555/TCP における
初出送信元アドレス数とその累計

図中の(A1), (B)は 3.1.2 で述べた期間である. 5555/TCP においては(A0)の期間はなく, 2017/1/1 からすでに 287 アドレスが観測された. (A1)の期間の 2017/6/19 に 4,090 アドレスが新規に観測されたが, その後は減少した. 脆弱性情報が公開されたのは 2018/2/6 であり, この直前に新規のアドレスは増加している. その後は新規に観測されたアドレス数は日々1,000 アドレスを超える結果となり, 累計も公開日を境にして爆発的に増加する結果となった.

脆弱性情報公開日直後の 2018/2/8～2018/2/19 日に初出送信元アドレス数が 0 になっているが, これは観測センサの停電の影響であり, 4.4.1 の 37215/TCP においても同期間の初出送信元アドレス数は 0 になっている.

4.4.3　表 2 で示した 10 件の脆弱性の分析

表 2 に示した 10 件の脆弱性について調べた．表 2 の各ポート番号のみに送信する初出送信元アドレスの累計を図 7 に示す．横軸は脆弱性情報公開日を 0 とした日にちを表し，縦軸は各ポート番号における累計の最高値を 100 として正規化し，比率で表している．図中(A0)，(A1)，(B)の期間は，2.1.2 で述べた期間であり，横軸が負の値は脆弱性公開日前の(A0)または(A1)の期間を表し，横軸正の値は(B)または(C)の期間である．

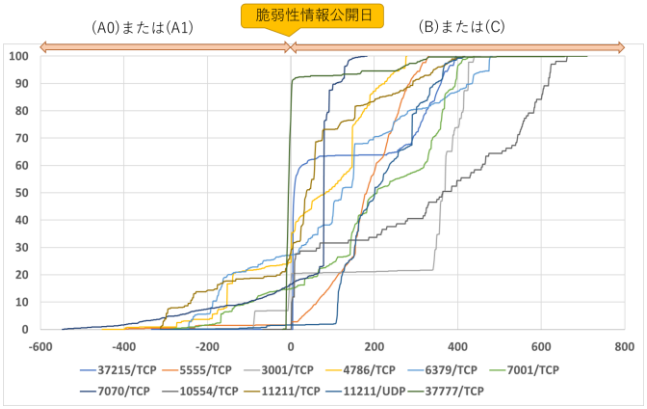

図 7　10 件の脆弱性の各ポート番号における脆弱性公開日を基準日とした初出送信元アドレス数の累計の正規化

脆弱性情報公開日以降は全体的に各ポート番号だけを狙うアドレス数は増加傾向にあることがわかる(図 2 中(B または(C))の範囲)．情報公開日前の期間は(A0)と(A1)が混在しているため，次項で詳細に分析する．

4.4.4　(A0)の期間の分析

2017/1/1～2018/12/31 の期間中表 2 の 10 件の脆弱性の 4.1.2 で述べた(A0)の期間をまとめた表を表 4 に示す．(A0)の期間の判断は，2017/1/1 の当該ポート番号のみに通信する送信元アドレス数が 0 である日が何日続くかで判断した．

表 4　ポート番号/プロトコルと(A0)の期間

ポート番号/プロトコル	(A0)の期間
37215/TCP	29 日
5555/TCP	0 日
3001/TCP	0 日
4786/TCP	32 日
6379/TCP	0 日
7001/TCP	1 日
7070/TCP	2 日
10554/TCP	67 日
11211/TCP	0 日
11211/UDP	8 日
37777/TCP	0 日

表 4 より，37215/TCP，4786/TCP，7001/TCP，7070/TCP，10554/TCP，11211/UDP は(A0)の期間があるが，それ以外は(A1)の期間から観測されている．これは以前には(A0)の期間があったものの，実験した期間の範囲が原因で(A1)からの期間しか観測できなかったためであると考えられる．なお，これらすべての脆弱性は 2017/1/1～2018/12/31 までに公開された脆弱性であるため，必然的に(B)以降の期間は含まれている．

(A0)の期間が得られたポート番号のうち，比較的(A0)の期間が長い 4786/TCP，10554/TCP について初出送信元アドレス数とその累計を 2017/1/1～2017/4/30 の範囲でグラフにした(図 8)．

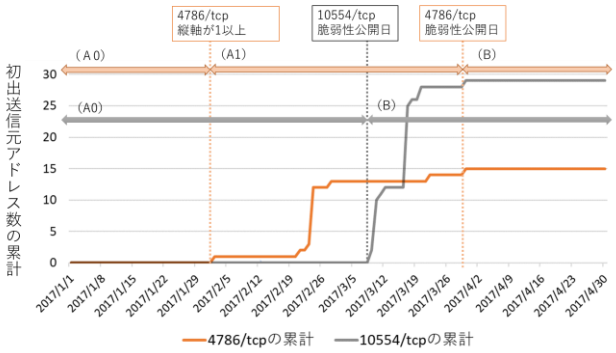

図 8　4786/TCP，10554/TCP(2017/1/1～2017/4/30)
初出送信元アドレス数の累計

4786/TCP については(A0)，(A1)，(B)の期間が明確に分類できている．10554/TCP については(A1)の期間に入る時期と脆弱性情報公開時期が重なってしまったために(A0)の期間と(B)の期間しか存在しない．これは，この実験では 1 日単位で集計しているため，(A1)の期間を得ることができなかった．

5.　考察

5.1　提案手法の有効性について

表 4 に示すようにポート番号・プロトコル別の結果，6 つについては(A0)，(A1)，(B)の期間があり，5 つについては(A1)，(B)の期間があった．4.4.4 でも述べたが，これは以前には(A0)の期間があったものの，実験した期間により(A1)からしか観測できなかったためであると考えられる．よって 10 件の CVE に対して(A0)，(A1)，(B)または(A1)，(B)の期間を確認できた．よって脆弱性情報公開前の期間でもゼロデイ攻撃通信を発見できる可能性を示せたといえる．

5.2　累計傾向モデルについて

3.1.2 で特定のポート番号のみに通信する送信元アドレス数の累計の時系列変化のモデルを提案した．図 3 の(A0)，(A1)，(B)期間それぞれの累計のパターンと結果を比較する．図 7 は脆弱性情報公開日を基準とし，縦軸は累計の比率を

表している．各ポート番号において(A0)と(A1)の期間よりも(B)以降の期間の方が累計比率は高く，累計が急増していることがわかる．この原因は，公開された脆弱性情報に基づいて攻撃ツールが作成され，それを用いて実行したからであると考えられる．脆弱性情報公開前では表 4 より(A0)の期間が表れなかったポート番号もあったが，(A1)の期間中，どのポート番号の累計も脆弱性情報公開後と比べると緩やかな増加傾向であることがわかた．これはごく限られた攻撃者によるゼロデイ攻撃通信である可能性が高い．これらよりこの提案モデルは妥当であるといえる．

5.3 観測期間と分解能について

5.3.1 (A0)期間がなかった脆弱性について

本実験では 2017/1/1～2018/12/31 の期間を分析対象にしている．5555/TCP，3001/TCP，6379/TCP，11211/TCP，37777/TCP は 2017/1/1 の時点で送信元アドレスが観測された．5.1 で述べた通り，これらのポート番号は(A0)の期間が過ぎてしまっていたため(A1)の期間からはじまっていたと考えられる．そこで，2017/1/1 より前の期間から分析を開始すれば(A0)の期間も確認できると推測される．

5.3.2 (A1)の期間がなかった脆弱性について

10554/TCP では(A1)の期間がみられなかった．本実験ではアドレス数の集計を 1 日単位で行ったため，(A1)期間の開始時期と(B)期間の開始時期とが重なったことが原因である．そこで集計を 1 日単位ではなく 1 時間単位にするなどさらに細かく単位を設定することで，(A1)の期間を明確に確認できると考えられる．

5.4 65,535 個のポートについて

各脆弱性は(A0)，(A1)，(B)の期間に分類できることを述べた．そこで，65,535 個のポートそれぞれについて，(A0)の期間と(A1)または(B)の期間について調べた(表 5)．

表 5　65,535 個のポートと期間の分類について

計 65,535 個ポート	期間の分類
58,754 個	(A0)の期間のみ ((A1)，(B)の期間なし)
6,781 個	(A1)，(B)の期間がある

すると，(A1)または(B)の期間は全 65,535 個のポート中，約 1 割のポートしかなかったことがわかった．これらより，約 9 割のポートは(A0)に属するため，現時点では脆弱性がない．もしこれらのポート番号において特定ポート番号のみに通信する送信元ホストが観測されるとゼロデイ攻撃を受けている可能性があるため，通信を詳細に分析するべきであるといえる．

5.5 適用範囲について

上記の脆弱性で用いられるポート番号は well-known ポートや 8080 など比較的よく用いられるポート番号ではなかった．したがって web サービスで一般的に用いられる宛先ポート 80/TCP を用い，提案手法が有効かどうか検討する．分析した期間は 2017/1/1～2017/12/31 である．

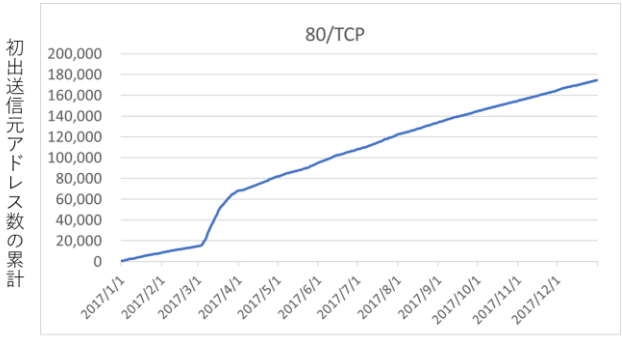

図 9　80/TCP のみに送信する
初出送信元アドレス数の累計

80/TCP は観測開始直後から増加傾向にあるため，提案手法ではゼロデイ攻撃通信か判別することができない．
80 番ポートなどの well-known ポートや一般的によく知られたサービスのポート番号では本提案手法ではゼロデイ攻撃を行うアドレスの様子を観測することは困難である．しかしながら 37215 番のような一般的によく知られていないポート番号に関しては図 5 のようなグラフになることが予想されるため，攻撃者のアクセス傾向の分析として用いることができると考える．

近年では IoT(Internet of Things) の発展により IoT デバイスが普及しているが，IoT 機器のデフォルトポート番号はあまり使用されないようなポート番号が使われることが多いため，セキュリティ対策が十分に施されていない IoT デバイスを狙ったサイバー攻撃にも有効である．

5.6 攻撃者の能力の推定

5.3.1 で述べたとおり，37215/TCP 宛だけに通信する送信元アドレス数が急増したのは脆弱性公開日である 2017/11/30 から 5 日後の 2017/12/5 であった．このことから，攻撃者がエクスプロイトなど攻撃ツールを作成するには約 5 日間かかることが推測できる．このように本提案手法は攻撃者の能力を推定することにも使用できる．

6. まとめ

本研究では，ゼロデイ攻撃の発見には既知のシグネチャを使用できない，通信量が増加しなければゼロデイ攻撃を発見できないという課題を解決するために，特定のポート番号のみに通信する送信元アドレス数の累計を用いるアプローチを提案し，その累計傾向モデルを提示した．10 件の CVE を用いて分析を行ったところ，10 件に対しモデル通りの結果を得ることができた．

今までは顕著な被害が出た後，脆弱性情報が公開された後，通信量が急増した後でなければ対処できなかったが，

本提案手法に基づいて分析すればゼロデイ攻撃通信の早期対処が可能であるといえる．

今後は，宛先ポート数を 2 以上にした場合，宛先アドレス，ペイロードも含めた分析[36][37]を行うことでさらに精度のよい結果を得ることができると考える．

参考文献

[1] 情報通信研究機構：NICTER：available from〈https://www.nicter.jp/〉(accessed 2020-08-15)
[2] ISTR Internet Security Threat Report Volume24 February 2019，available from〈https://docs.broadcom.com/doc/istr-24-2019-en〉(accessed 2020-08-15)
[3] 谷口 星彦：攻撃者の分類の一考察，Security management Vol.31 No.2，pp.17-22(2017)
[4] 情報通信研究機構：NICTER：available from〈https://www.nicter.jp/〉(accessed 2020-08-15)
[5] TSUBAME(インターネット定点観測システム)：available from〈https://www.jpcert.or.jp/tsubame/〉(accessed 2020-08-15)
[6] @police：available from〈https://www.npa.go.jp/cyberpolice/〉(accessed 2020-08-15)
[7] 東條 貴明，池部 実，吉田 和幸：大分大学のダークネットトラフィックにおけるゼロデイ攻撃の影響の分析，マルチメディア，分散協調とモバイルシンポジウム 2017 論文集，pp.1654-1660(2017)
[8] C. E. SHANNON：A mathematical theory of communication， Bell System Technical Journal，Vol. 27，No.3，pp.379-423(1948)
[9] SHODAN：available from〈https://www.shodan.io/〉(accessed 2020-08-15)
[10] Censys：available from〈https://censys.io/〉(accessed 2020-08-15)
[11] Rapid7：available from〈https://www.rapid7.com/ja/〉(accessed 2020-08-15)
[12] EM Hutchins, MJ Cloppert, RM Amin：Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains，6th International Conference on Information Warfare and Security，pp.113-125(2011)
[13] NIST：National Vulnerability Database (NVD)：available from〈https://nvd.nist.gov/vuln/search〉(accessed 2020-08-15)
[14] MITER：Common Vulnerabilities and Exposures(CVE)：available from〈https://cve.mitre.org/index.html〉(accessed 2020-08-15)
[15] MITER：CVE-2017-17215，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17215〉(accessed 2020-08-15)
[16] HUAWEI：Security Notice - Statement on Remote Code Execution Vulnerability in Huawei HG532 Product，available from〈https://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en〉(accessed 2020-08-15)
[17] MITER：CVE-2018-0701，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0701〉(accessed 2020-08-15)
[18] Network Security Research Lab at 360：Early Warning: ADB.Miner A Mining Botnet Utilizing Android ADB Is Now Rapidly Spreading，available from〈https://blog.netlab.360.com/early-warning-adb-miner-a-mining-botnet-utilizing-android-adb-is-now-rapidly-spreading-en/〉(accessed 2020-08-15)
[19] MITER：CVE-2017-15236，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15236〉(accessed 2020-08-15)
[20] SSD Secure Disclosure：SSD Advisory – Tiandy IP cameras Sensitive Information Disclosure，available from〈https://ssd-disclosure.com/ssd-advisory-tiandy-ip-cameras-sensitive-information-disclosure/〉(accessed 2020-08-15)
[21] MITER：CVE-2018-0171，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0171〉(accessed 2020-08-15)
[22] Cisco Security Advisory：Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability，available from〈https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2〉(accessed 2020-08-15)
[23] MITER：CVE-2017-9805，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9805〉(accessed 2020-08-15)
[24] SecurityTracker public archives：Apache Struts REST Plugin XStream Deserialization Flaw Lets Remote Users Execute Arbitrary Code on the Target System，available from〈https://www.securitytracker.com/id/1039263〉(accessed 2020-08-15)
[25] MITER：CVE-2017-10271，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271〉(accessed 2020-08-15)
[26] MITER：CVE-2018-2628，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2628〉(accessed 2020-08-15)
[27] SecurityTracker public archives：Oracle WebLogic Server Flaws Let Remote User Gain Elevated Privileges, Modify Data, and Deny Service on the Target System，available from〈https://www.securitytracker.com/id/1039608〉(accessed 2020-08-15)
[28] MITER：CVE-2018-13115，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13115〉(accessed 2020-08-15)
[29] Utku Sen – Blog computer security, programming：Multiple Vulnerabilities on Kerui Endoscope Camera，available from〈https://utkusen.com/blog/multiple-vulnerabilities-on-kerui-endoscope-camera.html〉(accessed 2020-08-15)
[30] MITER：CVE-2017-8223，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8223〉(accessed 2020-08-15)
[31] IT Security Research by Pierre：Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server，available from〈https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html#pre-auth-info-leak-goahead〉(accessed 2020-08-15)
[32] MITER：CVE-2017-9805，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9805〉(accessed 2020-08-15)
[33] Shengbao Cai, Zhang Lu, and Li Fu：Deluge How to generate 2TB/s reflection DDoS data flow via a family network，available from〈http://powerofcommunity.net/2017.htm〉(accessed 2020-08-15)
[34] MITER：CVE-2017-6432，available from〈https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9805〉(accessed 2020-08-15)
[35] 警視庁@police：「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について，available from〈https://www.npa.go.jp/cyberpolice/important/2017/19824.html〉(accessed 2020-08-15)
[36] 中村 康弘：初期ペイロードに着目したネットワーク走査活動の分析，第 79 回全国大会講演論文集 Vol.2018-CSEC-82，No.1，pp.523-524(2017)
[37] 中村 康弘，梶川 慶太，芦野 佑樹，鮫島 礼佳，須堯 一志，矢野 由紀子：宛先アドレス順序とペイロードに着目したネットワーク走査活動の分析，コンピュータセキュリティシンポジウム 2018 論文集(CSS2018)Vol.2018，No.2，pp.706-712(2018)