# サイバー戦入門　その３

## －攻撃者の正体を暴く－

三村　守（防大情報工学科）

## １　はじめに

サイバースペースは、陸・海・空・宇宙に続く第５のドメインとして提唱され、その重要性はますます高まっている。かつてはインターネットとほぼ同義であったサイバースペースは、ビークルや機器のスマート化に伴い急速に拡大しており、その範囲は陸・海・空を含む従来のすべてのドメインにおよぶようになってきた。今後、ＩｏＴ[1]や人工知能の普及に伴い、この傾向がますます加速する可能性は極めて高い。したがって、サイバースペースの特性に関する知識は、もはやすべての防衛にたずさわる者にとっても必須の素養と言っても過言ではない。サイバースペースでは、「匿名性が高い。」、「証拠の改ざんが可能」、「地理・時間的な制約がない。」、「被害が不特定多数に拡大しやすい。」等の特性があるとされている。特に、相手が誰であるのかわからない匿名性については、サイバー戦を非対称戦と位置づける重要な特性である。２０１５年に生起した年金機構等を狙った大規模なサイバー攻撃では、様々なレポートや分析結果[2]が公開されているものの、未だに攻撃者の正体は判明していない。その一方で、２０１３年２月には、米国に対する一連のサイバー攻撃が人民解放軍の第６１３９８部隊の仕業であり、その拠点は上海にあるビルであるとのレポート[3]が公開された。このレポートでは、どのようにして匿名性が高いとされる攻撃者の正体を暴いたのだろうか？　さらに、２０１４年５月には米司法省が、サイバー攻撃の実行犯として、人民解放軍の将校５人を告発している[4]。２０１８年には、２０１６年の米大統領選介入に関連する一連のハッキング等の罪で、ロシア連邦軍参謀本部情報総局[5]のサイバー部隊に所属する１２名が起訴されている[6]。さらに同８月には、２０１７年に大流行したランサムウェアのＷｎａｎｎａＣｒｙの作成等に関与したとして、北朝鮮の諜報機関である

---

[1]Internet of Things モノのインターネット

[2]サイバーセキュリティ戦略本部 (2015).「日本年金機構における個人情報流出事案に関する原因究明調査結果」

[3]Mandiant (2013). APT1: Exposing One of China's Cyber Espionage Units

[4] U.S. Department of Justice (2014). "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage"

[5] GRU (Glavnoye Razvedyvatelnoye Upravleniye)

[6] U.S. Department of Justice (2018). "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election"

朝鮮人民軍偵察総局[7]１２１局に所属する男性が起訴されている[8]。サイバー攻撃において攻撃者の正体が判明した場合には、国家間の関係に重大な影響を与える可能性もある。サイバー攻撃における攻撃者の帰属（アトリビューション）は非常に関心の高いテーマであり、その仕組みを理解することは非常に重要である。しかしながら、サイバー攻撃において攻撃者は「どのように痕跡を隠すのか？」、そして分析者は「どのように攻撃者の正体を暴くのか？」といった事項は一般の方々にはほとんど理解されていない。

「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」では、サイバー攻撃とは何かを理解するために必要な基本的な仕組みを、技術的な観点から体系的に解説することを試み、「サイバー戦入門　その２　－サイバー戦の概念と作戦－」ではサイバー戦の概念とサイバー作戦の種類について平易に解説することを試みた。その３からは、サイバー戦に関する各トピックスをより掘り下げて平易に解説することを試みる。本稿では、サイバー攻撃において攻撃者の正体を暴くための技術的な手法についてとりあげる。以下、第２節ではサイバー攻撃の種類と仕組みについて簡単に解説する。第３節では、攻撃者の正体に関する基本的な情報の種類について説明する。第４節では、サービス拒否攻撃等の能動的攻撃において、攻撃者を追跡する手法について考察する。第５節では、標的型攻撃等の受動的攻撃において攻撃者を追跡する手法について考察し、最後にまとめと課題について述べる。

## ２　サイバー攻撃の種類と仕組み

サイバー攻撃は、攻撃者が主体的に任意のタイミングで実施できる「能動的攻撃」と、被攻撃者による何らかの動作を必要とする「受動的攻撃」に分類できる。この節では、能動的攻撃と受動的攻撃の仕組みについて、「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」で説明した内容を簡単におさらいする。

能動的攻撃は、主にインターネットに公開されたサーバを対象としたサイバー攻撃であり、サーバに大量のアクセスを発生させて閲覧を困難にするサービス拒否攻撃[9]や、ホームページのコンテンツの改ざんがこれに該当する。具体的な事例としては、９月１８日[10]等の特異日に発生することが多いとされる政

---

[7] RGB (Reconnaissance General Bureau)

[8] U.S. Department of Justice (2018). " North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions"

[9]DoS (Denial of Service)攻撃、あるいは DDoS (Distributed Denial of Service)攻撃とも呼ばれる。

[10]満州事変の発端となった柳条湖事件が生起した日であり、反日感情が高まることが多いとされる。

府関係機関等へのサイバー攻撃や、アノニマス等のハクティビスト[11]によるサイバー攻撃等が挙げられる。これらの能動的サイバー攻撃に関しては、オンラインのショッピングサイトのように何らかの重要なサービスを提供しているサイトを除外すると、その影響は受動的攻撃よりも軽微であることが多い。また、特別なスキルや準備を必要とせず、容易に実施できるため、個人によるものも多いと考えられる。

受動的攻撃は、主に利用者の端末を対象としたサイバー攻撃であり、マルウェア[12]を添付したメールを送りつけて利用者の端末の制御を奪う標的型攻撃や、不正なコンテンツを埋め込んだホームページを閲覧させて利用者の端末を攻撃し、最終的にその制御を奪うドライブ・バイ・ダウンロード攻撃や水飲み場攻撃がこれに該当する。具体的な事例としては、国内では国会、防衛産業、年金機構等を狙った大規模なサイバー攻撃、人民解放軍の第６１３９８部隊の仕業とされる一連の米国へのサイバー攻撃等が挙げられる。これらの受動的攻撃の事例と能動的攻撃の事例を比較すると明らかなように、社会的に重大な影響をおよぼすサイバー攻撃のほとんどは、利用者の端末を対象とした受動的攻撃である。これらの受動的サイバー攻撃は、機密情報の搾取を目的として隠密に行われることが多く、入念な準備を必要とし、組織に深刻な影響を与えることも珍しくない。その中の一部は非常に高度、あるいは執拗であることからＡＰＴ[13]と呼ばれ、大規模な組織や国家の関与が疑われているものもある。

**（１）能動的攻撃の仕組み**

能動的攻撃の仕組みは図１に示すとおり比較的単純である。

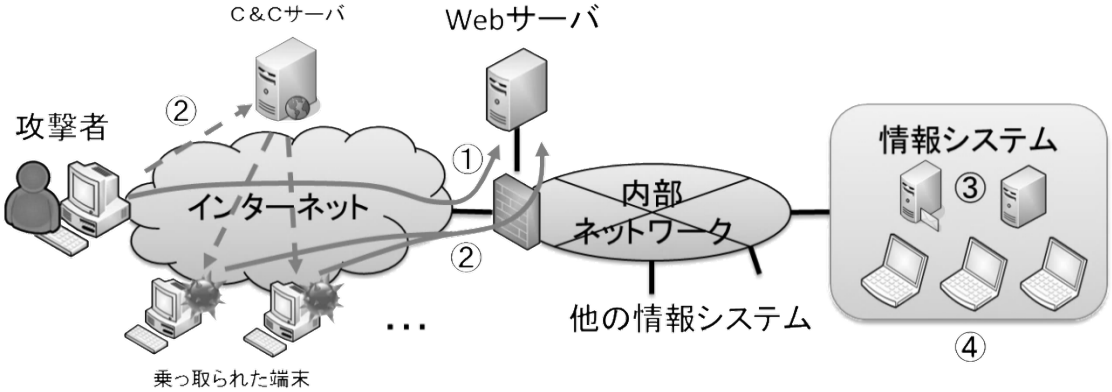


図１：能動的攻撃の概要

[11]何らかの社会的あるいは政治的な主張を目的としてサイバー攻撃を実施する者
[12]利用者の意図しない動作をする不正なプログラムの総称であり、コンピュータ・ウイルスとも呼ばれる。
[13]APT (Advanced Persistent Threat)

攻撃者は、攻撃の対象とするサーバ（ここではＷｅｂサーバ）に対し、ツール等を用いて大量のトラフィック送りつけ、サービスの提供を妨害する（図１①）。あるいは、同サーバの脆弱性を突き、そのコンテンツを改ざんする（図１①）。図１に示すとおり、能動的攻撃の主な対象はインターネットに公開されたサーバであり、内部ネットワークやこれに接続する情報システムが直接影響を受けることはほとんどない。このように攻撃者が直接的にサーバを攻撃する場合には、攻撃者の端末のインターネット上の論理的位置を示すグローバルＩＰアドレス（以下ＩＰアドレス）が、サーバやファイアウォール[14]のログに記録される。このＩＰアドレスは、改ざんのように攻撃者がＷｅｂサーバからの応答を受け取らなければ成立しない双方向通信の攻撃の場合には、偽装することは困難である。したがって、このような直接的な攻撃の場合には、Ｗｅｂサーバのログに記録されたＩＰアドレスが、攻撃者を特定するための手がかりとなる。

もう少し高度な攻撃者の場合には、あらかじめ乗っ取った端末をＣ＆Ｃサーバ[15]を経由して遠隔操作し、同様の攻撃を実施することも可能である（図１②）。このように攻撃者が間接的にサーバを攻撃する場合には、Ｗｅｂサーバのログに記録されるＩＰアドレスは、乗っ取られて踏み台とされる端末のＩＰアドレスとなる。

サーバからの応答を必要としないタイプのサービス拒否攻撃の場合には、踏み台を経由しなくとも送信元のＩＰアドレスを偽装することが可能である。また、近年ではインターネット上の不適切な設定のサーバを悪用し、通信内容を増幅させるアンプあるいはリフレクション攻撃も発生している。これらの場合には、Ｗｅｂサーバのログに記録されるＩＰアドレスは、偽装された任意のＩＰアドレスや悪用されたサーバのＩＰアドレスとなる。

### （２）受動的攻撃の仕組み

より深刻な脅威である受動的攻撃は図２に示すとおりやや複雑である。

---

[14]あらかじめ定められたルールに基づいてアクセス制御を実施するネットワーク機器

[15]C&C or C2 (Command and Control) Server 攻撃者が端末を遠隔操作するための命令を中継する指令サーバ

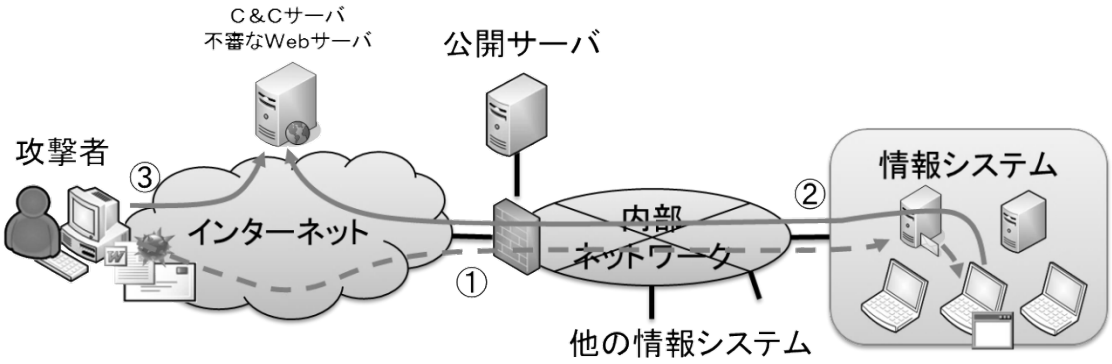


図２：受動的攻撃の概要

まず、攻撃者はマルウェアや不審なＷｅｂサイトへのリンクをメールで送付する（図２①）。メールの添付ファイルを実行した端末、あるいはリンクをクリックして不審なＷｅｂサーバに誘導された利用者の端末はマルウェアに感染し、Ｃ＆Ｃサーバとの通信を開始する（図２②）。攻撃者はＣ＆Ｃサーバを経由して制御を奪った端末を遠隔操作し、機密情報等を搾取する（図２③）。受動的攻撃の場合には、一部のサービス拒否攻撃のように送信元のＩＰアドレスを容易に偽装することはできない。なぜならば、送信元ＩＰアドレスを任意の値に変更してしまうと、遠隔操作の結果や機密情報を回収することができなくなってしまうためである

受動的攻撃の攻撃者を特定するための手がかりは、メールの送付（図２①）に利用されたメールサーバや端末のＩＰアドレス、端末の遠隔操作（図２②）に利用されたＣ＆ＣサーバのＩＰアドレス等がある。メールサーバや端末のＩＰアドレスは、端末を調査して発見したメールのヘッダを確認するか、あるいはその利用者のメールサーバのログから調査することが可能である。Ｃ＆ＣサーバのＩ Ｐアドレス等は、端末やメールサーバから発見したメールの添付ファイルやリンクを専門家が解析することで得られる。この解析では、他にもマルウェアの特徴等の攻撃者に関係する様々な情報も得られる。端末がマルウェアに感染してしまった場合には、遠隔操作の痕跡が残るため、ファイアウォールやプロキシサーバ[16]のログからもＣ＆ＣサーバのＩ Ｐアドレス等を得ることが可能となる。

## ３　攻撃者の正体に関する基本的な情報

サイバー攻撃に用いられたＩ Ｐアドレス等の攻撃者のアトリビューションに関するパラメータは、インディケータと呼ばれており、サイバーインテリジ

[16]端末の代理でインターネットにアクセスする機能があり、一般にすべての端末からインターネットへのアクセスの記録が集約されている。

ェンスのコミュニティでは情報共有が進んでいる。具体的には、情報処理推進機構（ＩＰＡ）が運営するサイバー情報共有イニシアティブ（Ｊ－ＣＳＩＰ）[17]や、警察庁を中心としたサイバーインテリジェンス情報共有ネットワークがある。また、ＣｒｏｗｄＳｔｒｉｋｅ[18]のようにサイバー攻撃のアトリビューションに関するインディケータや、アトリビューションについて分析したレポートを提供するサービスも増えてきている。この節では、アトリビューションに関する一般的なインディケータについて説明する。

**（１）通信先に関する情報**

サイバースペースにおいて攻撃者を特定するための最も基本的なインディケータは、インターネット上の論理的位置を示すＩＰアドレス等である。サイバー攻撃に用いられたＩＰアドレス等は、Ｗｅｂサーバ、ファイアウォール、プロキシサーバ、メールサーバ等のログ、発見した添付ファイルの解析結果から得ることができる。ＩＰアドレス等からさらに、インターネットで公開されているオープン情報を活用し、様々な通信先に関する情報を調査することが可能である。例えば、ＩＰアドレスやドメイン名は国ごとの割り当てが決まっているため、どの地域からの攻撃であるかのおおよその目安をつけることができる。しかしながら、第２節で説明したとおり、ＩＰアドレスは一部のサービス拒否攻撃の場合には偽装が容易であり、それ以外のサイバー攻撃の場合にも踏み台を経由することがある点には注意が必要である。つまり、これらの最も基本的なインディケータは、あくまでも「サイバー攻撃の最終的な経由地」を示すものであり、「サイバー攻撃の本来の攻撃元」を示しているとは限らない。主な通信先に関するインディケータを表１に示す。

表１：主な通信先に関するインディケータ

| | |
|---|---|
| ＩＰアドレス | ネットワーク上の論理的位置を示す数字<br>（例：117.103.185.21） |
| ＦＱＤＮ[19] | ドメイン名等を省略せずにすべて記載したネットワーク上の論理的位置を示す文字列であり、ＤＮＳ[20]によってＩＰアドレスに紐付けられる。<br>（例：www.mod.go.jp） |
| ドメイン名 | ネットワーク上のある領域を示す文字列 |

[17]https://www.ipa.go.jp/security/J-CSIP/
[18]https://www.crowdstrike.com/
[19]FQDN (Fully Qualified Domain Name) 完全修飾ドメイン名
[20]DNS (Domain Name Service) ドメイン名とＩＰアドレスの関係を管理するサービス

| | |
|---|---|
| | （例：mod.go.jp） |
| ＩＰアドレスの利用者 | ＩＰアドレスの利用者の名称や連絡先 |
| ドメインのレジストラント | ドメインの利用者の名称や連絡先 |
| ドメインのレジストラ | ドメインの登録業者の名称や連絡先 |

ＩＰアドレスとＦＱＤＮ及びドメイン名は、ＤＮＳによって相互に変換することが可能である。ＩＰアドレスとＦＱＤＮの対応関係は、１対１となるわけではない。例えば、複数のＦＱＤＮが同じＩＰアドレスに対応する場合もあれば、その逆の場合もある。サイバー攻撃の場合には、一般にＣ＆Ｃサーバのｉｐアドレスを、複数のＦＱＤＮやドメイン名を使って使い回す傾向が認められる。また、ＤＮＳを利用せず、直接ＩＰアドレスを利用してＣ＆Ｃサーバとの通信を試みるマルウェアもある。より洗練された攻撃者は、ＩＰアドレスやドメイン名を何度も取得することによって攻撃に利用するインフラを変更し、追跡を困難にしようと試みる。したがって、ＩＰアドレスやドメインよりもその利用者の方が、攻撃者との関連が強いインディケータであると考えられる。

ＩＰアドレスの利用者、ドメインのレジストラント及びレジストラは、Ｗｈｏｉｓと呼ばれるサービスを利用することで、誰でも容易に調査することが可能である。これらのインディケータには、登録者の名称、住所、電話番号、メールアドレス等が含まれている。これらのインディケータは、より攻撃者との関連が強いものと考えられる。しかしながら、これらの情報は単一の組織によって一元的に管理されているわけではない。その内容の信頼性については、それらの情報を管理する組織の健全性に依存するのが現状である。

**（２）攻撃手段に関するインディケータ**

攻撃者のアトリビューションに関する別のアプローチとしては、使用されたマルウェア、メール等の攻撃手段に注目する手法が考えられる。例えば、メールに添付されたマルウェアが同じ、あるいはメールの件名や本文が同じ内容であれば、それらの攻撃は同じ攻撃者による攻撃である可能性が高いと考えられる。主な攻撃手段に関するインディケータを表２に示す。

表２：主な攻撃手段に関するインディケータ

| | |
|---|---|
| マルウェアのハッシュ値 | ファイルの同一性を識別するために用いられる一定の長さの文字列 |
| マルウェアの動作 | マルウェアが作成するファイル等の名称や挙動 |
| マルウェアやツールの種類 | マルウェアやツールのパッケージの名称 |
| メールの件名 | マルウェア等が添付されたメールの件名 |

| | |
|---|---|
| メールの送信者 | 同メールの送信者 |
| 添付ファイルの名称 | 添付されたマルウェア等の名称 |
| 作成された時間や時刻帯 | 同メールやマルウェアが作成された時間や時刻帯 |

最も基本的な攻撃手段に関するインディケータは、使用されたマルウェアのハッシュ値である。サイバー攻撃に用いられるマルウェアのほとんどはファイルである。ファイルは同じ名称かつ同じ大きさであっても、その中身は異なっている可能性がある。一般にファイルの同一性を確認するためには、ハッシュ値が活用されている。ハッシュ値は、ファイルが少しでも一致しなければ異なる値となるため、人間の識別における指紋のような役割を果たす。マルウェアがコンピュータの内部で作成するファイル名や挙動も、攻撃手段に関する重要なインディケータである。また、マルウェアはビルダーと呼ばれるパッケージを用いて作成されることも多いため、マルウェアやツールのパッケージの名称もその攻撃の特徴となる。これらのマルウェアに関するインディケータは、専門家の解析によって得ることができる。マルウェアに関するインディケータは、偽装するためにはある程度のスキルを要するため、比較的に信頼性の高いインディケータであると考えられる。ただし、広く出回っており、誰もが容易に利用できるような手段については、攻撃者の特徴とはならないこともある。例えば、ＰｏｉｓｏｎＩＶＹ[21]のようなパッケージは容易にインターネットから入手できるため、これを攻撃者の特徴とみなすことは難しい。ＰｌｕｇＸ[22]や年金機構等へのサイバー攻撃で話題となったＥｍｄｉｖｉ[23]であれば、その入手経路も限られてくるため、攻撃者の特徴とみなすことができる。また、マルウェアの作成者とそれを利用する攻撃者が別である可能性についても留意する必要がある。

マルウェア等が添付されたメールの件名、送信者、添付ファイルの名称等も、攻撃手段に関する重要なインディケータである。これらのインディケータは、メールのヘッダかメールサーバのログから得ることができる。メールの件名、送信者、添付ファイルの名称等は、攻撃者が任意に指定することが可能であるため、その特徴が現れる可能性があるが、偽装も容易である点には注意が必要である。

### （３）攻撃者の振舞いに関するインディケータ

これまでに示したインディケータは、ログ、マルウェアの解析結果等から直接的に得られるインディケータか、あるいはそれらのインディケータに何

[21]RAT と呼ばれる遠隔操作を実施するためのマルウェア、あるいはその作成ツールの一種
[22]プロキシを経由してＣ＆Ｃサーバと通信する RAT の一種
[23]改ざんしたホームページをＣ＆Ｃサーバとして利用する RAT の一種

らかの機械的な処理を実施することで得られるインディケータであった。サイバー・キル・チェーン[24]という概念を提唱したロッキード・マーティン社のレポート[25]によると、インディケータは「単一で分離不能なもの」、「加工により得られたもの」及び「振舞いに関するもの」の３種類に整理されている。この概念によると、これまでに示したインディケータは、「単一で分離不能なもの」あるいは「加工により得られたもの」となる。次に説明するのは、様々なインディケータの相関関係を分析し、統計的手法を用いたプロファイリングにより導出する攻撃者の振舞いに関するインディケータである。主な攻撃者の振舞いに関するインディケータを表３に示す。

表３：主な攻撃者の振舞いに関するインディケータ

| | |
|---|---|
| 攻撃者の目的 | 攻撃者の対象となった組織、搾取された情報等 |
| 攻撃者の使用言語 | メールやマルウェアの作成に使用された言語 |
| 攻撃者の活動地域 | メールやマルウェアが作成された時間や時刻帯から推定される攻撃者の活動地域 |
| 攻撃者の能力 | 使用言語、攻撃手段等から推定される攻撃者の能力 |

攻撃者の目的は、サイバー攻撃の対象となった組織や搾取された情報等、「攻撃者はサイバー攻撃によって何を得たのか？」あるいは「サイバー攻撃で利益を得たのは誰か？」といった事項に着目することで推定することができる。メールやマルウェアの作成に使用された言語も有益なインディケータである。英語、スペイン語等の広い地域で使用されている言語を除外すると、攻撃者が使用する言語はその活動している地域にも関係する。もちろん使用する言語は偽装することが可能であるが、スペルや文法の誤り、ネイティブは使用しない表現、機械翻訳を使用した形跡等から、攻撃者の母国語ではないことが浮き彫りとなる場合もある。攻撃者が活動している地域は、メールやマルウェアが作成された時間や時刻帯からも推定することができる。また、攻撃者が使用する言語、攻撃手段等からは、攻撃者の能力を推定することができる。

## ４　能動的攻撃における攻撃者の追跡

この節では、サービス拒否攻撃やホームページの改ざん等の能動的攻撃にお

[24]標的型攻撃の段階を連鎖的に偵察、武器化、配送、攻撃、インストール、遠隔操作、目的実行に区分したモデル

[25]Hutchins, E.M. et al. (2009). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

いて、どのように攻撃者を追跡するのかを考察する。

能動的攻撃の場合、分析の中心となるのは通信先に関するインディケータである。すぐに入手できるインディケータは、Ｗｅｂサーバ、ファイアウォール等のログから得られるＩＰアドレスである。繰り返しになるが、これらのＩＰアドレスは、「サイバー攻撃の最終的な経由地」を示すものであり、「サイバー攻撃の本来の攻撃元」を示しているとは限らない。したがって、それらのＩＰアドレスがどこの国に帰属するかよりも、それらのＩＰアドレスと攻撃者の結びつきの強さが問題となる。これを確認するために着目すべき点は、攻撃のタイプである。攻撃のタイプは、Ｗｅｂサーバ、ファイアウォール等のログ、あるいはＩＤＳ[26]のアラートを分析することで判断することができる。

**（１）一方向性のサービス拒否攻撃の場合**

サイバー攻撃が、サーバからの応答を必要としないタイプのサービス拒否攻撃の場合には、送信元のＩＰアドレスを任意に偽装することが可能であるため、そのＩＰアドレスと攻撃者の結びつきはほとんど期待できない。例えば、ＳＹＮフラッド攻撃[27]と呼ばれるサービス拒否攻撃の場合には、接続を開始するためのパケットを大量に送付するが、攻撃者はその応答を受信する必要がないため、その送信元ＩＰアドレスに実在しない任意の値を設定することが可能である。このようにＩＰアドレスと攻撃者の結びつきがほとんど期待できない場合、攻撃者を追跡するためには、パケットが経由してくる通信経路を物理的にたどる必要がある。

**（２）双方向性のサービス拒否攻撃や改ざんの場合**

サイバー攻撃が、サーバからの応答を必要とするタイプのサービス拒否攻撃や改ざんの場合には、少なくともそのＩＰアドレスのコンピュータはその時点では実在したことになる。例えば、Ｆ５攻撃[28]と呼ばれるサイバー攻撃では、攻撃者はホームページの再読み込みを連続して実施するため、その結果として表示されるページの内容を受信する必要がある。そのため、その送信元ＩＰアドレスには実在の値を設定する必要がある。このようなサーバからの応答を必要とするタイプのサービス拒否攻撃や改ざんの場合には、そのＩＰアドレスと攻撃者の結びつきはある程度期待できる。

次に着目すべき点は、そのＩＰアドレスがあらかじめ乗っ取られた端末、あるいは通信内容を増幅させるために悪用されたサーバ等の踏み台のＩＰアドレスか否かという点である。攻撃が端末から実施されるタイプの場合に

---

[26]IDS (Intrusion Detection System)侵入検知装置

[27]確立しない接続の要求を大量に試みるサービス拒否攻撃の一種

[28]Web ブラウザの再読み込み機能を連続して行うサービス拒否攻撃の一種

は、インターネット等でボットネット[29]に組み込まれている端末の一覧と照合することによって確認できる場合がある。しかしながら、一般的には端末が踏み台か否かの判断は難しい。ＳＨＯＤＡＮ[30]のようなインターネットの接続する機器の情報を提供するサイトを活用すれば、その情報の信頼性から検討をつけることができる可能性はある。例えば、社会的に信頼できる組織が所有するＩＰアドレスからのサイバー攻撃であれば、そのＩＰアドレスは踏み台とされている可能性が高いと考えられる。９月１８日のような特異日に発生するサイバー攻撃の場合には、攻撃者が自らの意思で自身の端末を用いて攻撃を実施する可能性もある。通信内容を増幅させるアンプ攻撃の場合には、一般的にそのＩＰアドレスは踏み台とされたサーバのものである可能性が高いと考えられる。

### （３）通信経路やＩＰアドレスの追跡

通信経路を構成する物理的な機材やＩＰアドレスが国内で管理されている場合には、関係機関と協力することである程度の追跡が可能となる。しかしながら、国外の場合には関係機関との協力が難しく、時間がかかる場合もあり、追跡は困難であることが多い。特に、当該国との国交がない場合には、実質的にそれ以上の追跡は不可能である。また、国家、通信事業者、攻撃者が協力関係にあり、組織ぐるみでサイバー攻撃の調査に協力しない場合にも、それ以上の追跡は現実的ではない。防弾ホスティングサービスと呼ばれる法執行機関の捜査からのサービスの保護を売りとする通信事業者も存在する。そのため、多くの場合に国境を越えた通信経路やＩＰアドレスの追跡は現実的ではないのが現状である。

## ５　受動的攻撃における攻撃者の追跡

この節では、標的型攻撃、ドライブ・バイ・ダウンロード攻撃、水飲み場攻撃等の受動的攻撃において、どのように攻撃者を追跡するのかを考察する。

受動的攻撃の場合、通信先に関するインディケータが短期的には分析の中心となる。通信先に関するインディケータについては、通信の入口であるメールの送信経路を追跡するアプローチと、通信の出口であるＣ＆Ｃサーバを追跡するアプローチが考えられる。

### （１）メールの送信経路の追跡

マルウェアや不審なリンクが記載されたメールの送信元は、当該メールのヘッダに記載された送信者や、当該メールの中継に用いられたサーバのＩＰアドレスからある程度は調査することができる。しかしながら、メールの

---

[29]攻撃者がマルウェア等を感染させて乗っ取った端末で構成されるネットワーク
[30]https://www.shodan.io/

送信者（メールアドレスを含む。）、件名、本文等は攻撃者が任意に設定することが可能であり、偽装が容易である点には十分に注意する必要がある。ＳＰＦ[31]のように送信者のドメインを認証してメールアドレスの詐称を防止するための技術もあるが、これらは十分に普及しているとは言い難い。そもそも、インターネットは一元的に管理されているわけではなく、管理者が異なる様々なネットワーク機器の集合体であるため、このような技術をすべてのサーバに普及させるのは現実的ではない。したがって、これらの容易に偽装が可能なインディケータから送信経路を追跡することは困難な場合がほとんどである。メールのヘッダに記載された情報の中で、ある程度信頼できるインディケータは、中継サーバのＩＰアドレスである。

インターネットにおけるメールは、複数のメールサーバを経由して送信者から受信者のメールサーバに配送される仕組みとなっている。経由の際に、メールのヘッダには中継したメールサーバのＩＰアドレスが追記される。この中継サーバのＩＰアドレスは、ヘッダの先頭から新しいものが追記される仕様となっている。そのため、ヘッダの先頭から中継サーバのＩＰアドレスをたどることで、メールの送信元をある程度追跡することが可能である。

しかしながら、マルウェアや不審なリンクが記載されたメールは、誰もが容易に取得できるいわゆるフリーメールのサービスを活用して送信されることが多い。このような場合、中継サーバをたどったとしても、最終的な中継サーバのＩＰアドレスは、そのサービスを提供する組織が所有するものであることがほとんどである。そのため、他の通常の用途で利用されるフリーメールとの区別ができない。サービスの仕様によっては、メールの送信に用いた端末のＩＰアドレスがヘッダに記載されている場合もあるが、このようなケースは稀である。

メールの送信に利用される端末は、あらかじめ乗っ取られた端末である可能性もある。また、そのような端末があらかじめ用意できない場合にも、ある程度の知識がある攻撃者であれば、送信元のＩＰアドレスを秘匿するために、ＴＯＲ[32]等のサービスを利用するものと考えられる。結局のところ、能動的攻撃の場合と同様の理由により、最終的なＩＰアドレスの追跡は困難となってしまう場合がほとんどである。そのため、メールの送信経路を追跡するアプローチはあまり有益とは考えられていない。

### （２）Ｃ＆Ｃサーバの追跡

感染した端末の遠隔操作に用いられるＣ＆Ｃサーバ、ドライブ・バイ・ダ

---

[31]SPF (Sender Policy Framework)

[32]TOR (The Onion Router) 複数のノードを経由し、通信を多重に暗号化することで、アクセス元の特定を極めて困難にする機能を提供するサービス

ウンロード攻撃や水飲み場攻撃に用いられるＷｅｂサーバのＦＱＤＮやＩＰアドレス等は、ファイアウォール、プロキシサーバ等のログ、発見した不審メールのリンク及び添付ファイルの解析結果から得ることができる。これらのＦＱＤＮやＩＰアドレスは、攻撃者が遠隔操作や情報の搾取のために継続して利用する必要があるため、メールの送信経路よりも攻撃者との関連が強いものと考えられている。そのため、Ｃ＆ＣサーバのＦ ＱＤＮやＩＰアドレスは、攻撃者を追跡するための最も主要なインディケータであると考えられる。

ただし、組織力がある攻撃者は、Ｃ＆Ｃサーバ等の攻撃インフラを短期間で入れ換える傾向が認められる。近年ではホスティングサービスのクラウド化が進んでおり、攻撃インフラを短期間で再構築することが容易となってきている。そのため、その攻撃が発生した時点でのＩＰアドレスの利用者、ドメインのレジストラント、レジストラ等の通信先に関するインディケータを蓄積しておくことが重要である。過去の履歴を検索するためには、インターネットにおける通信先に関するインディケータを蓄積しており、過去の履歴を検索することができるＤｏｍａｉｎＴｏｏｌｓ[33]、ＰａｓｓｉｖｅＴｏｔａｌ[34]等のサービスも活用できる。

Ｃ＆Ｃサーバ等の攻撃インフラを構築するための手法としては、攻撃者が自前で用意する手法、防弾ホスティングサービスを利用する手法、インターネット上の脆弱性があるサーバを乗っ取るか改ざんして悪用する手法等が考えられる。攻撃者が自前でＣ＆Ｃサーバを用意するか防弾ホスティングサービスを利用する場合、そのＦＱＤＮやＩＰアドレスは正規のサイトとは異なる見慣れないものとなるため、通信先に関するインディケータを調査することで見分けることができる場合がある。例えば、海外の見慣れないサイトであり、そのドメインが新しく登録されたものであり、かつ登録内容に不審な記述がある場合、攻撃者が新たに構築した攻撃インフラである可能性を考慮すべきであろう。これに対し、攻撃者側も不審に思われるのを防ぐため、対象国のドメインやＩＰアドレスを取得してその国内に攻撃インフラを構築するケースも目立つようになってきている。中には正規のＩＳＰ[35]を用いて構築したプロキシサーバもあり、これらがサイバー攻撃や違法なサービスの中継に使用されることもある。２０１４年１１月には、中国でサービスを提供するプロキシサーバを運用する業者が、国内で摘発される事件が発生している。そのため、国内の大手ＩＳＰには悪質なプロキシサーバ業者と契約

[33]https://www.domaintools.com/
[34]https://www.riskiq.com/products/passivetotal/
[35]ISP (Internet Service Provider)

しないように求める等の排除に向けた取り組みも始まっている。さらに、攻撃者が正規のサイトを乗っ取るか改ざんし、Ｃ＆Ｃサーバを構築するケースも増加している。このような場合には、通信先に関するインディケータを調査したとしても、正規のサイトとの区別は非常に困難である。このように、受動的攻撃の場合にも、これらのインディケータは、「サイバー攻撃の最終的な経由地」を示すものであり、「サイバー攻撃の本来の攻撃元」を示しているとは限らない点には注意が必要である。

### （３）攻撃者のプロファイリング

結局のところ、「サイバー攻撃の本来の攻撃元」を追跡するためには、通信経路、サーバ、ドメイン、ＩＰアドレス等を管理する組織との協力が必要となってくる。これらが国内や同盟国で管理されている場合には、関係機関との協力がある程度可能であるが、国外の場合には追跡が困難であることが多い。そのため、多くの場合に国境を越えた実世界での追跡は現実的ではないのが現状である。そこで、サイバー攻撃のインディケータを集約し、その相関関係を分析することで、攻撃者のプロファイリングを実施する手法が注目されるようになってきた。相関分析の基本は、各インディケータの相互参照（クロス・リファレンス）である。相互参照の結果、ある攻撃とある攻撃のインディケータが一致した場合には、それらの攻撃が同一の攻撃者による可能性が考えられる。相互参照の結果を視覚化した例を図３に示す。

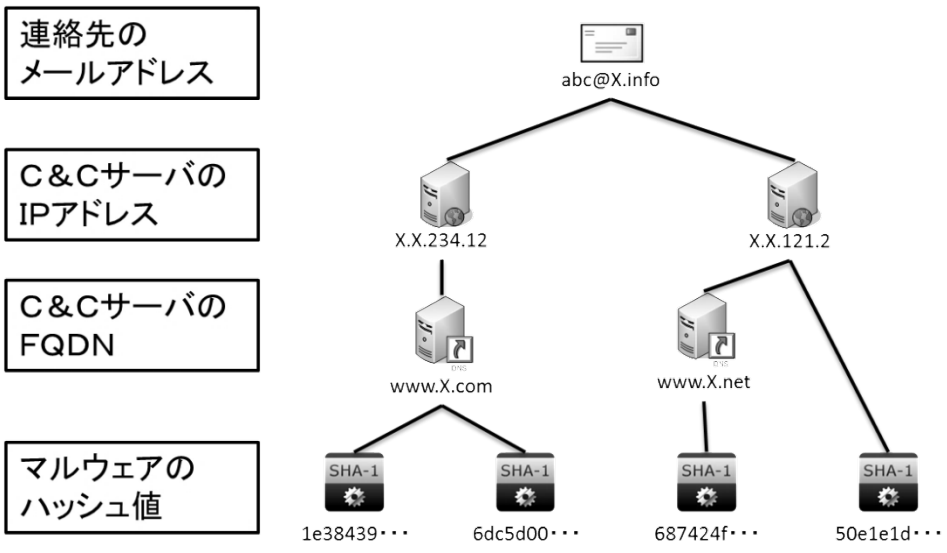


図３：相互参照の結果の視覚化

この例では、マルウェアのハッシュ値から共通するＣ＆ＣサーバのＦＱＤＮ及びＩＰアドレスを参照し、最終的に利用者の登録に用いられたメールア

ドレスが共通であることが判明している。しかしながら、これまでに示したとおり、インディケータには様々な種類があるため、どのインディケータを重視すべきかを判断することは難しい。

重視すべきインディケータを判断するための指標としては、信頼性と関連性が挙げられる。ここで言う信頼性とは、そのインディケータを信頼してよいかを示す指標であり、偽装の困難さを意味する。例えば、メールの送信者（メールアドレスを含む。）、件名、本文等は攻撃者が任意に設定することが可能であるため、その信頼性は高いとは言い難い。これに対し、Ｃ＆ＣサーバのＦ Ｑ Ｄ Ｎや Ｉ Ｐアドレスは、攻撃者が遠隔操作や情報の搾取のために継続して利用する必要があるため、ある程度信頼してよいものと考えられる。もちろん、攻撃者が正規のサイトを乗っ取るか改ざんして構築したＣ＆Ｃサーバはこの限りではない。もうひとつの指標である関連性は、そのインディケータと攻撃者の結びつきの強さを示すものである。例えば、短期的に変化する可能性があるＣ＆ＣサーバのＦ Ｑ Ｄ Ｎや Ｉ Ｐアドレスよりは、その登録に利用された情報の方が攻撃者との関連性は高いものと考えられる。もちろん、その登録に利用された情報の信頼性は、その情報を管理する組織の健全性に依存することになる。信頼性及び関連性の観点から注目されているのは、振舞いに関するインディケータである。

振舞いに関するインディケータは、複数のサイバー攻撃の通信先や攻撃手段に関するインディケータを相関分析し、総合的な判断から導き出される高次のインディケータである。この分析は、犯罪心理学におけるプロファイリングに類似している。例えば、攻撃者の目的はサイバー攻撃の対象となった組織、搾取された情報、サイバー攻撃によりもたらされた被害、組織の利害関係等から推定することが可能である。メールやマルウェアが作成された言語、解析によって得られたタイムスタンプの時刻や時刻帯などからは、攻撃者の使用言語や活動地域が推定できる。マルウェアの種類、使用する脆弱性等からは攻撃者の能力が推定できる。

振舞いに関するインディケータを評価する上で重要となるポイントは、その希少性である。例えば、マルウェアの開発に使用された言語が希少なものであれば、それは攻撃者の能力を示す重要な特徴となる。修正プログラムが公開されていない未知の脆弱性を用いた攻撃であれば、攻撃者の能力は高く、それなりの組織や資金力を有していることが推定できる。例えば、スタックスネットのように複数の未知の脆弱性を用いたマルウェアを作成する能力がある組織は非常に限られている。

### （４）プロファイリングの限界

通信経路、サーバ、ドメイン、ＩＰアドレス等の追跡は現実的ではないと

いう現状を考慮すると、攻撃者のプロファイリングは唯一の現実的な選択肢であると考えられる。しかしながら、プロファイリングにより得られた攻撃者の特徴は、あくまでも状況証拠を積み重ねて分析した結果にすぎないという点には留意する必要がある。したがって、高度な攻撃者であれば、そのプロファイルすら偽装しているという可能性も考えられる。

また、作成したプロファイルを最終的にどうやって攻撃者個人に結びつけるかという課題もある。この課題を解決するために注目されているのは、ＳＮＳ[36]を活用するアプローチである。ＳＮＳには、Ｆａｃｅｂｏｏｋのように実名での利用を前提としているものがある。また、個人の実生活に関する書き込み、写真やその中に埋め込まれているＧＰＳの位置情報、交友関係等、個人を特定するための情報の宝庫でもある。これらの情報の中には、インターネットから誰でも閲覧可能なものもある。これらのＳＮＳから得られた情報とインディケータの相互参照により、攻撃者と個人が結びつけられる場合がある。例えば、人民解放軍の第６１４８６部隊の仕業とされるサイバー攻撃のレポート[37]では、ドメインの取得に用いられたメールアドレスに含まれる「ＣＰＹＹ」という文字列を個人のブログと紐付け、その個人の活動を追跡することで第６１４８６部隊の特定に至っている。このように、サイバースペースにおいて得た状況証拠を積み重ねることにより、プロファイリングの精度を高めることは可能である。また、自組織に対するサイバー攻撃のインディケータと、このようなレポートで公開されているインディケータを相互参照することにより、自組織に対するサイバー攻撃のアトリビューションというパズルの最後の１ピースを埋めるという手段もあり得る。しかしながら、この場合にも第３者によるなりすましであることを主張することで、攻撃者の言い逃れを可能とする余地が残る。サイバースペースにおける調査のみで攻撃者を識別することは、音響や電波のみで潜水艦や航空機を識別することに似ているように思う。そのため、米国に対する一連のサイバー攻撃が人民解放軍の仕業であると断定した事案では、米国はレポートに記載されていない別の決定的な証拠を掴んでいるのではないかという指摘もある。

スパイなどの伝統的なＨＵＭＩＮＴ[38]や、インターネット等の通信網から得られるＳＩＧＩＮＴ[39]は、サイバー攻撃の状況証拠を決定的な証拠とするための手段となり得る。これらを有効的な手段として機能させるのは、伝統的なインテリジェンスの世界におけるストーブパイプ型の組織では難しい。

---

[36]SNS (Social Network Service)
[37]CrowdStrike (2014). PUTTER PANDA, CrowdStrike Intelligence Report
[38]人的情報
[39]信号情報

各インテリジェンス組織がお互いの任務を理解し、必要な情報を共有することが不可欠である。

### （５）サイバー反撃

よりアクティブに攻撃者の正体を暴く手段としては、攻撃者に対してサイバー反撃を実施するという手段も考えられる。２００８年８月に発生した南オセチア紛争では、２０１１年以降もグルジア[40]の政府機関、重要インフラ銀行等を標的としたサイバー攻撃が継続していた。これに対し、グルジアのＣＥＲＴ[41]はマルウェアによる反撃を実施している。まず、自国のパソコンをおとりとして意図的にマルウェアに感染させ、「Georgian-Nato Agreement」という名称のマルウェアを仕込んだファイルを設置した。攻撃者はこのファイルを盗み出し、自らの端末で実行した。その後、攻撃者の端末を乗っ取り、遠隔操作によってその端末の情報を入手し、カメラを操作してその端末の利用者の顔写真を撮影することに成功している。このサイバー反撃の内容や端末の利用者の顔写真は、グルジアのＣＥＲＴが作成した報告書で公開されている[42]。

このようなサイバー反撃を成功させるためには、最新の定義ファイルを適用したウイルス対策ソフトや侵入検知装置に検知されない未知のマルウェアが必要であることに加え、どのように攻撃者を欺くためのおとりのパソコンを準備するかが重要となる。ネットワークや端末の仮想化技術を利用して簡易に構築したおとりの環境では、慎重な攻撃者を欺くことは困難であろう。近年のマルウェアには、仮想環境を検知した場合に動作を止めてしまうものも少なくない。攻撃者の標的となった本物の端末をコピーし、攻撃者に見られてはならない機微なファイル等を削除しておとりを準備することができれば理想である。

このように、サイバー反撃は攻撃者の正体を暴くための有効な手段となり得る。しかしながら、マルウェアを用いたサイバー反撃はプロファイリングとは異なり、攻撃者の端末に不正アクセスを実施することになる。したがって、実施の可否については法的問題が関わってくる点には注意が必要である。この問題を回避するためには、マルウェアを用いずに単に情報収集のためのサーバへのアクセスを誘導するという手段も考えられる。この場合には、攻撃者の端末のＩＰアドレスや、利用する端末に関する情報が得られる可能性がある。以降の分析の手順はプロファイリングと同様に、その得られた情報から相互参照を実施していくことになる。

---

[40]現在のジョージア

[41]CERT (Computer Emergency Response Team)

[42]CYBER ESPIONAGE Against Georgian Government (Georbot Botnet), CERT.GOV.GE. LEPL Data Exchange Agency Ministry of Justice of Georgia (2012).

## ６　おわりに

本稿では、サイバー攻撃において攻撃者の正体を暴くための技術的な手法についてとりあげた。第２節では、サイバー攻撃を能動的攻撃と受動的攻撃に分類し、その仕組みについて簡単におさらいした。第３節では、攻撃者の正体に関する基本的な情報を、通信先、攻撃手段及び振舞いに関するインディケータに分類し、その内容と特徴について説明した。第４節では、能動的攻撃においてインディケータを分析し、攻撃者を追跡する手法について考察した。第５節では、受動的攻撃においてインディケータを分析し、攻撃者をプロファイリングする手法とその限界について考察した。

サイバー攻撃における攻撃者のアトリビューションを調査するためには、通信経路、サーバ、ドメイン、ＩＰアドレス等を追跡するアプローチは現実的ではない。現状では、サイバー攻撃に関するインディケータを継続的に蓄積し、相互参照によりその相関関係を分析し、攻撃者のプロファイリングを実施することが最良のアプローチであると考えられる。プロファイリングを効果的に実施するためには、Ｃ＆ＣサーバのＦＱＤＮやＩＰアドレス等のインディケータ、サイバー攻撃に用いられたマルウェア、その分析レポート等の共有が不可欠である。サイバー攻撃を受けた個々の組織がそれらを共有しなければ、各サイバー攻撃の相関関係や全体像を把握することが困難となり、攻撃者のプロファイリングは不可能となってしまう。しかしながら、サイバー攻撃に関する情報の共有には慎重な姿勢の組織が多いのが現状である。その主な原因は、自組織がサイバー攻撃を受けたことを他者に知られるのではないかという疑念であると考えられる。そのため、サイバー攻撃に関する情報の共有は難しい。サイバー攻撃の攻撃者は、このような被害者側のジレンマを巧みに利用している。これに対抗するためには、一部の情報を削除する等の被害者の匿名性を考慮した処置を実施し、サイバー攻撃に関する情報を積極的に共有することが重要である。しかしながら、サイバー攻撃に用いられたマルウェアや証跡を共有する場合には、自組織に関する機微な情報が含まれている可能性について留意する必要がある。ＶｉｒｕｓＴｏｔａｌ等のマルウェア等のサイバー攻撃に関する情報を共有するサイトでは、機微な情報を含むと考えられるマルウェアがアップロードされていることも珍しくない。したがって、これらの情報を共有する場合には、機微な情報が含まれていないかよく確認する必要がある。また、このような知識のない未熟な解析者や情報システムの利用者が、安易にマルウェアをアップロードすることがないように監督する必要がある。