〈2〉ゼロデイ脆弱性市場の現在 — 二つの市場と独力の中国 —

一般社団法人先端技術安全保障研究所（GIEST） 所長 小沢 知裕

1. ゼロデイ脆弱性	406
2. 攻撃に利用される脆弱性	407
3. スパイウェア販売会社での利用	407
4. グレーな領域からの脱却	408
5. 脆弱性を国家が買う	408
6. 二つの市場	409
7. 独力の中国	409
【年表】	410
文献目録	411

1. ゼロデイ脆弱性

コンピューターシステムを使用する限り、頻繁なプログラムの更新はセキュリティ上必須の作業となる。オペレーティングシステム（OS）の更新もまた同様に重要である。これらの更新によって、それらシステムが抱える「脆弱性（vulnerability）」が改善され、安全性が高まる。システムの管理者や端末の使用者がこれらの脆弱性を放置しておく、他者にそれを利用され、システムに対して何かしらの害を加えられてしまう可能性が残ることになる。このような脆弱性の情報を売り買いする業者が存在し、脆弱性販売会社（vulnerability provider）あるいは脆弱性仲介業者（vulnerability broker）などと呼ばれている。

最近の傾向を見る限り、システムへの不正侵入を

試みようという者—たとえばクラッカー（cracker：犯罪を行うハッカー）など—にとって、脆弱性を利用することは必ずしも主流な手段ではなくなっている^[1]。とはいえ、最も有効な手段の一つであることに変わりはない。そのことは、それらの情報が昨今の市場において以前にも増して高額で取引されていることが示唆している^[2]。システムへの侵入経路として活用され得る脆弱性は、常にソフトウェアやファームウェアといったプログラム上に存在するので、ソフトウェアやハードウェアの販売会社はそれらを発見して修正したプログラム（パッチ）をネットワーク経由で使用者に配信する作業を繰り返している。プログラムの使用者が、その送られてきたパッチをプログラムに反映させるというプロセス（パッチを当てるといふ）を経て、脆弱性は初めて改善される。このパッチが配信される前の脆弱性をゼロデ

イ脆弱性 (zero-day vulnerability) と呼ぶ^[3]。

2. 攻撃に利用される脆弱性

このような脆弱性を販売会社自身が他者に先んじて見つけることができれば、これをプログラムの修正に利用して事なきを得ることができるわけだが、販売側に属さない人物 (民間ハッカーなど) が先に発見すれば、その販売会社に売り込んで利益を得ることができる。しかし、販売会社に売り込まずに活用する場合は、さらに高額な利益に結び付けることができるかもしれない^[4]。例えば、米国を本拠とする脆弱性販売会社ゼロディウム (Zerodium) 社は、1件につき最大で250万米ドル (2025年4月現在のレートで3億6千万円程度) で脆弱性の情報を買取るとしている^[5]。販売会社に属さない誰かであっても、これらのゼロデイ脆弱性の情報を早期に入手することによって、パッチが当たる前の段階で、当該の脆弱性を利用した攻撃に備えることができるかもしれない。しかし、悪意を持った者がその情報を手に入れた場合、他者のシステムに不正に侵入したり、乗っ取ったりすることに活用することもまたできるだろう。つまり、脆弱性を入手した者は、それを防御的ではなく攻撃的な用途に使用することもできる。従って、これらはクラッカーにとっても、軍や法執行機関、国家情報機関などの国家機関にとっても活用の価値のあるものである。

このようなゼロデイ脆弱性 (情報) は貴重で高価なものであるが、一度でもこれを使用して第三者のシステムに悪影響を与えてしまえば、いつかはその異常にシステム管理者などに気付かれ、その存在は露見してしまうことになる。そして最終的には、ソフトウェア販売会社に対応を取られてしまいパッチを当てられ使えなくなってしまうことになる。このため、攻撃側としても使用方法や使い時は選ばざるをえない。それなりの必要性があるときにのみ、使用することになる。また、そもそも潤沢な資金を持っているか、プログラムの未知の脆弱性を見つけ出すことができるほどの高度な人材を抱えているか、もしくはその双方を備えた組織なり人物のみがこれらを入手し得る。過去には、贅沢にもゼロデイ脆弱性を4種 (5種や5種以上という意見もある) も使用したマルウェアが発見されたこともある。2010年に

イランで発見された最初の高度なサイバー兵器と呼ばれるスタックスネット (Stuxnet) がその一つである^[6]。このサイバー兵器あるいはマルウェアは、イラン中部の町ナタンズ近郊にある地下核施設をターゲットとしたもので、その主要設備である遠心分離機を秘密裏に約1千台破壊したとされる強力なものだった。これは、米国家安全保障局 (National Security Agency : NSA) とイスラエル軍のサイバー作戦部隊である8200部隊によって開発されたものと広く信じられている^[7]。ところで、ナタンズの核施設であるが、これは数万基の遠心分離機の運用を可能とするウラン濃縮施設である。天然ウランは濃縮し濃縮ウランとすることによって、原子力発電に使用する核燃料とすることができる。そして施設を高度化することさえできれば更に濃縮度を高めて、核ミサイルの弾頭に使用できる高濃縮ウランを生産することも可能である。イランはその核開発をあくまで平和利用のためのものであると主張してきた。しかし、実際には核兵器の保有を目指しているのではないかとイスラエルや米国、欧州諸国に疑われてきており、国際原子力機関 (International Atomic Energy Agency : IAEA) からも疑問符を突き付けられている^{[8][9]}。

また2021年に露見して、米国やNATO (北大西洋条約機構 : the North Atlantic Treaty Organization)、日本などが、その実行者として中国を名指しして非難したMicrosoft Exchange Serverのハッキング事件は、世界中のメールアドレス数十万アカウントに影響を与えた大規模なサイバースパイ事件と見られているが、これに使用されたゼロデイ脆弱性もまた4種であった^[10]。いずれも資金の潤沢な組織、即ち国家機関がその実行者として疑われているわけである。

3. スパイウェア販売会社での利用

ところで、主に法執行機関や情報機関といった国家機関にスパイウェアを提供してきた企業がある。そのような企業としては、例えば、Pegasusを提供するイスラエル企業NSOグループ (NSO Group Technologies) 社や「ガリレオ (Galileo)」の愛称で呼ばれるハッキングツール・リモートコントロールシステム (Remote Control System : RCS) を提供するイタリア企業ハッキングチーム (Hacking Team) 社、FinFisher (別名 FinSpy) を提供する独フィンフィッ

シャー社 (FinFisher) などが挙げられる^[11]。スパイウェアとは、第三者の端末 (PC やスマホ) にその使用者に気付かれぬ間に仕込まれ、カメラやマイクから得られる映像、音声や端末内のデータなどを盗み出すプログラムのことである。ここではこのような企業をスパイウェア販売会社と呼ぶこととしたい。これらの企業によるスパイウェアの供給には批判があり、例えば上述の Pegasus に関しては、権威主義国家における人権弾圧に利用されたケースが人権団体に集計され、繰り返しレポートされている^[12]。

このようなスパイウェア販売会社も、その製品に脆弱性を活用している。例えば Pegasus は iPhone や Android 端末に侵入して情報を盗むスパイウェアだが、複数のゼロデイ脆弱性を使用していたことがわかっている^[13]。また、ハッキングチーム社は 2015 年に自らもハッキングを受け、社内情報をリークされているが、その際に、少なくとも 7 種のゼロデイ脆弱性を保有していたことがわかっている^[14]。

4. グレーな領域からの脱却

脆弱性販売会社は真っ先に脆弱性を抱えるソフトウェア販売会社に情報を提供するようなことはしない。また、その商品 (つまり脆弱性情報) が犯罪者に使用され得ること、人権弾圧に利用され得ることなどの懸念があることから、その市場はグレーな存在として誕生したといえる。例えば、2008 年に創業されたフランス企業ヴーベン・セキュリティ社 (Vupen Security : 以下、ヴーベン社、米ゼロディウム社の前身) の創業者シャウキ・ベクラ (Chaouki Bekrar) は、発見した脆弱性に基づいて、商品となるシステム侵入手段 (exploit) を開発し、それをその脆弱性を抱えたソフトウェアの販売会社に教えることはせず、あくまでそれを利用する用途で第三者に販売する方針を取っていた。もし販売会社に教えてしまえば、対応が取られてしまい、それ以降は脆弱性ではなくなってしまう。パッチが当てられて以降は、その (かつての) 脆弱性を利用した侵入手段は無効になってしまう。このため、侵入手段を顧客に販売する時には、そのようなことが起こらないように、脆弱性の内容を公開したり転売したりすることをしないよう禁じる契約をしていた^[4]。同社によるグレーな領域でのビジネスには、「バグを一社に販

売することは、他の者全てをその使用にさらすことにはならないか」との批判があった^[15]。

また、同じく 2008 年創業の脆弱性販売会社、米エンドゲーム社 (Endgame, Inc.) の創業者クリス・ルーランド (Chris Rouland) は、サイバー攻撃をしてくる相手に対して企業自身が反撃できてしかるべきだという持論を展開した。但し、同社そのものが自らサイバー攻撃に手を染めることはなかったという。あくまで、企業側からの反撃のための情報やツールを商品として顧客企業へ提供した^[16 ページ:105-106]。しかし、この方針は後に改められている。2012 年末に就任したナサニエル・フィック (Nathaniel Fick) CEO はゼロデイ販売ビジネスを「くだらない (crummy)」として、同ビジネスから撤退する方針を掲げた^[17]。

比較的新進の米エクソダス・インテリジェンス社 (Exodus Intelligence : 以下、エクソダス社) は上記 2 社とはかなり異なるスタンスを打ち出している。同社の場合は、発見した脆弱性の分析結果を 6 か月以内に脆弱性を抱える当該のソフトウェア販売元に提供するとコミットしている。このような期間を設定する理由について、その間に顧客がパッチに先んじることでもできるし、脆弱性が公知のものとなるまでの間、適切な防御ができていないか再確認することもできるからだとしている^[18]。定期購読料を支払えば、100 以上のゼロデイ脆弱性レポートと被害を低減するための手引きにアクセスできるとしている^[19]。つまり、顧客がもしこれらゼロデイ脆弱性情報を利用して「パッチに先んじて」攻撃的な手段に利用しようと思えば、それは可能な仕組みとなっている。

5. 脆弱性を国家が買う

先に少し触れたヴーベン社は、外部から脆弱性を仕入れることをしないで、社内で分析して自ら見つけ出していた^[20]。そして、同社はその顧客を NATO 加盟諸国やそのパートナー国の情報機関や法執行機関に限定していた^[4]。どの国のどの機関がゼロデイ脆弱性を購入したのか、同社は秘密としているが、フランスや米国の国家機関への販売を第一に想定したビジネスだったと考えて良いだろう。少なくとも、米 NSA は 2012 年に始まる一年間は同社と「バイナリー分析と侵入手段サービス」の年間サブスクリプ