2019年セキュリティ予測

WatchGuard’s Security Predictions for 2019

<https://www.watchguard.co.jp/resource-center/2019-predictions>

[**AIを活用したチャットボットによる攻撃**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction1)

1. [**公共施設や産業用制御システムがランサムウェアの標的になる**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction2)

[**公共施設や産業用制御システムがランサムウェアの標的になる**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction2)

1. [**国連がサイバーセキュリティ条約を提出する**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction3)

[**国連がサイバーセキュリティ条約を提出する**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction3)

1. [**国家規模の「Fire Sale」攻撃が開始する**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction4)

[**国家規模の「Fire Sale」攻撃が開始する**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction4)

1. [**自己増殖型ファイルレス「vaporworms」攻撃**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction5)

[**自己増殖型ファイルレス「vaporworms」攻撃**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction5)

1. [**WPA3 Wi-Fiのハッキングによって、業界全体の無線セキュリティの欠如が浮き彫りになる**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction6)

[[**WPA3 Wi-Fiのハッキングによって、業界全体の無線セキュリティの欠如が浮き彫りになる**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction6)](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction1)

1. [**生体認証の大規模ハッキングにより単一要素認証が終焉を迎える**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction7)

[[**生体認証の大規模ハッキングにより単一要素認証が終焉を迎える**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction7)](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction2)

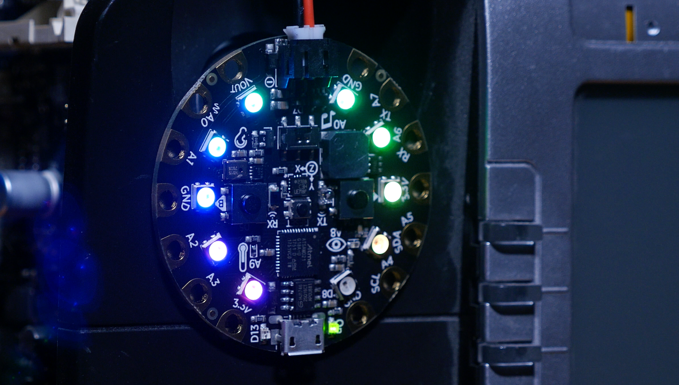
1. [**攻撃者によってインターネットが支配される**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction8)

[**攻撃者によってインターネットが支配される**](https://www.watchguard.co.jp/resource-center/2019-predictions#prediction8)

**1AIを活用したチャットボットによる攻撃**

2019年には、サイバー犯罪者や悪意のあるハッカーが不正なチャットボットを作成し、ソーシャルエンジニアリングにより、リンクをクリックさせたり、ファイルのダウンロードを促したり、あるいは個人情報の詐取を目論むことが予測されます。  
  
人工知能や機械学習のテクノロジがこの数年間で大きな進化を遂げたことで、自動化されたチャットロボットがさまざまな場面で利用されるようになりました。最近では、カスタマサポートの第1段階としてチャットボットが活用されるようになったことで、人間のサポート担当者が複雑な問題に集中できるようになりました。  
  
しかしながら、本物の人間のように思えるAIチャットボットは、新たな攻撃ベクトルをハッカーに与えることにもなります。チャットボットが乗っ取られ、正規のリンクに見せかけた極めて悪質なリンクへとユーザが誘導されてしまう恐れもあります。さらには、正規のWebサイトのWebアプリケーションに存在する脆弱性を攻撃者が悪用し、無害であるサイトに悪意あるチャットボットを挿入する場合もあるでしょう。たとえば、金融機関のWebサイトの閲覧中にヘルプを必要としているユーザに対して、攻撃者が偽のチャットボットを強制的にポップアップ表示し、本物に見せかけた偽のリンクを表示してクリックするよう指示します。このようなリンクを使えば、マルウェアのインストールから金融機関のサイト接続の乗っ取りまでのあらゆる不正操作を攻撃者が実行できるようになります。  
  
2019年には、このような悪意あるチャットボットによるソーシャルエンジニアリングの実験を攻撃者が開始すると予測されます。当初はテキストベースの簡単なボットから始まりますが、将来的には、Google Duplexなどの人間の声を使ったボットを活用し、電話を始めとする音声接続のソーシャルエンジニアリングに発展すると予測されます。

**2公共施設や産業用制御システムがランサムウェアの標的になる**

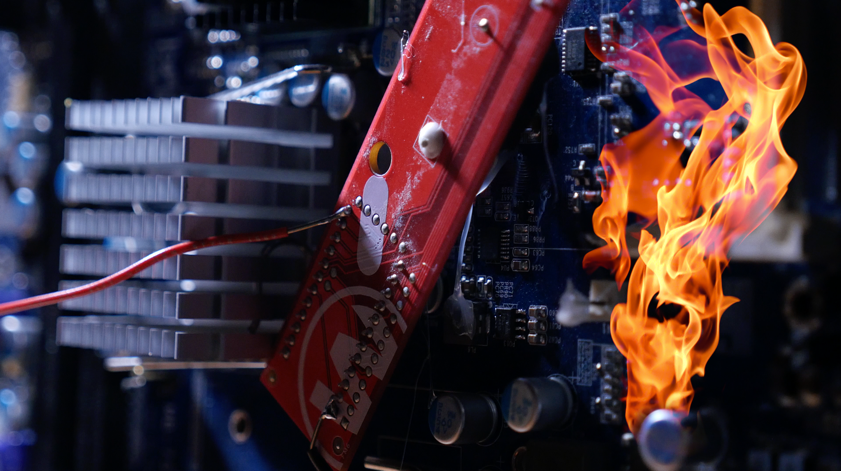


2019年の標的型ランサムウェア攻撃では、公共施設やICS（産業用制御システム）が最大の標的になり、攻撃回数は平均してこれまでの65倍に達し、1回の要求金額が約300ドルから20,000ドルになることが予想されます。そして、このような攻撃によって、実社会において停電や公共施設の麻痺といった深刻な被害がもたらされることが想定されます。  
  
ランサムウェアは過去5年間でインターネットを席巻し、暗号化ランサムウェアの初の成功例と言われているCryptoLockerに始まり、短時間で拡散する特性を持つ初のランサムワームであるWannaCryで頂点に達しました。サイバー犯罪者は、あらゆるユーザを標的にランサムウェア攻撃を仕掛け、身代金は比較的少額であるものの、可能な限り多くのユーザに感染を拡大しようとしていました。  
  
ところが、昨年になると、標的型攻撃へと移行するハッカーが増加し、多額の身代金が要求されるようになりました。基幹サービスを提供する組織をランサムウェア攻撃の標的に選べば、高い確率で身代金を手に入れることができます。2017年のランサムウェア攻撃の45%は、英国のNHS（国民健康サービス）を始めとする医療機関を標的にするものでした。2016年には、米国のHollywood Presbyterian Medicare Centerが17,000米ドルもの身代金を支払うことでコンピュータシステムの制御を取り戻し、MedStar HealthやAlvarado Hospital Medical Centerなどの数十の医療分野の組織が大規模ランサムウェア攻撃の被害者になりました。2017年と2018年には、ボルチモアやアトランタを始めとする米国の多くの都市もランサムウェア攻撃を受けました。  
攻撃回数は平均してこれまでの**65倍以上**に達し、1回の攻撃で要求金額が**約300ドルから20,000ドル**になることが予想されます。2019年には、サイバー犯罪者が公共施設やICSを標的にするようになるでしょう。これらの基幹サービスは、これまでは広範囲のランサムウェア攻撃の標的になることが少なかったため、この種の攻撃に対する備えがおそらく十分ではありません。サイバー犯罪者は、これらのサービスのダウンタイムにつながる可能性のあるランサムウェアがあれば、脅迫の十分な材料になり、多額の身代金を要求できることを知っています。このような攻撃が成功すれば、水道や電気が完全に停止し、使えない状態になる恐れがあります。2019年には、ランサムウェア攻撃の件数については減少する見込みですが、標的型の攻撃、その中でも公共施設やICSを標的にする攻撃が増加して、身代金の要求金額が65倍になることが予想されます。

**3国連がサイバーセキュリティ条約を提出する**

国連が2019年に国際サイバーセキュリティ条約を制定し、国家が背後で支援するサイバー攻撃の増加への取り組みを強化することが予想されます。  
  
国家が背後にいるという疑惑や確証のあるサイバー攻撃は数多く存在します。米国とイスラエルは、Stuxnet攻撃を開始したとされており、ロシア政府は、エストニアに対するDDoS攻撃をすべて影で操り、ウクライナの大規模停電を主導し、米国の選挙や政治関連のハッキングにも関与したと疑われています。北朝鮮は、公共や民間の組織やインフラを攻撃し、ソニー・ピクチャーズに対する攻撃を仕掛け、WannaCry攻撃では数十億ドルの被害をもたらしたとされています。多くの政府が、知的財産を標的にするさまざまなサイバー攻撃に関与したとして中国を非難してきましたが、それに追い打ちをかけるかのように発生した、Supermicroのサプライチェーン攻撃では、バックドアを密かに組み込んだサーバを世界中に出荷したとして、PLA（人民解放軍）への非難が集中しています（ただし、この件については今も多くの議論が続いています）。これらの攻撃の損害額は数十億に上るとされており、コンピューティングデバイスの90％を提供するサプライチェーンにリスクをもたらしたことから、サイバー攻撃が当初の標的だけにとどまらず、多くの企業や個人に莫大な経済的損害を与えることがわかります。  
  
これらの攻撃の犠牲になる民間人が増え続けていることで、国連が国際サイバーセキュリティ条約を制定し、国家が背後で支援するサイバー攻撃の重大な影響を緩和するべく、強い意志を持って取り組みむようになることが予想されます。国連においては、これまでにもサイバー攻撃に関する議論が進められてきましたが、最近のサイバー攻撃の増加と影響の拡大という傾向が2019年も続くと予想されることから、条約の制定という最終局面を迎えることになるでしょう。

**4国家規模の「Fire Sale」攻撃が開始する**



映画「ダイ・ハード」シリーズ4作目に登場したフィクションの「Fire Sale」攻撃は、米国の交通システム、金融システム、公共施設、通信インフラを標的にする同時多発サイバー攻撃でした。彼らは、この攻撃で引き起こされた恐怖や混乱に乗じて、いかなる痕跡も残すことなく、大金をせしめて姿を消すことに成功しました。2019年には、映画の中の架空の物語だったこの攻撃が現実化することになるでしょう。  
  
2000年代後半にはこのような攻撃は非現実的であったかもしれませんが、最近の多くのサイバーセキュリティ関連の事件は、国家やテロリストによってこのような攻撃の手段がすでに開発されていることを示唆しています。サイバー犯罪者や国家が大規模DDoS（分散型サービス拒否）攻撃を開始することで、国全体のインフラを停止に追い込み、通信システムを確実に妨害できることがわかっています。米国政府は、外国人犯罪者が公共施設やエネルギーシステムを狙い、入念な調査を既に進めていると主張しています。SWIFTなどの金融システムを標的とする国家規模の攻撃で何百万件もの情報が盗まれた例も報告されています。国家規模の攻撃では、偽ニュースを一般ユーザに広める目的で、ソーシャルメディアやその他のコミュニケーションシステムも使われています。  
  
これらの攻撃は、いずれもすでに実行可能なものであり、どこかの国が大規模攻撃の隠れ蓑として多くの攻撃を同時に仕掛けるようになるのも、時間の問題でしょう。

**5自己増殖型ファイルレス「vaporworms」攻撃**

2019年には、脆弱なシステムを介して自己増殖するワームのような性質を持つ新種のファイルレスマルウェア「vaporworms」が台頭することになるでしょう。  
  
何十万台もの脆弱なMicrosoft IIS Webサーバから拡散した、15年以上も前の初期のファイルレスワームの1つであるCode Redコンピュータワームの登場以来、ワームとファイルレスマルウェアはどちらも世界中の多くのネットワークに大きな影響を与えてきましたが、この両方が1つの攻撃で同時に使われた例はほとんどありません。  
  
感染システムにファイルを残すことなく、メモリ内でのみ動作するファイルレスマルウェアが増加し、主流になりつつあります。  
高度な攻撃者がこの方法を好むのは、スキャンの対象になる不正ファイルが存在しないことから、従来型のエンドポイントアンチウイルスによる制御でのファイルレスの脅威の検知とブロックが困難であるためです。その結果、感染の確率は高くなります。このような状況に、パッチが適用されずに動作するシステムと脆弱なソフトウェアの存在が加われば、ワームを拡散させる絶好の機会を攻撃者に与えることになります。  
  
昨年は、Shadow Brokersと呼ばれるハッカー集団によるMicrosoft Windowsの複数のゼロデイ脆弱性の公開が発端となり、大きな被害へと発展することになりました。攻撃者はわずか1ヶ月でこれらの脆弱性をランサムウェアに追加し、過去最大の被害をもたらしたサイバー攻撃の2つである、WannaCryとNotPetyaを完成させました。Windowsの新しいゼロデイ脆弱性がワームの増殖に悪用された例はこれが初めてではなく、もちろん、これで終わりでもないでしょう。2019年には、脆弱性を悪用して自己増殖するファイルレスマルウェア「vaporworms」が登場することになるでしょう。

**6レイヤ2脅威ベクトルによるWPA3の回避**



2019年には、Trusted Wireless Environment Frameworkで定義されている6つのカテゴリの1つが、新しいWPA3暗号化標準での機能強化にもかかわらず、WPA3 Wi-Fiネットワーク突破の手段として使われることになると予想されます。より包括的なセキュリティが無線LANインフラに適用されない限り、WPA3に対するユーザの不安が払拭されることはなく、悪魔の双子APなどの脅威を受けやすい状況が続くことが懸念されます。  
  
WPA3は、Wi-Fi暗号化プロトコルの進化版であり、WPA2の機能が大幅に強化されましたが、6つの既知のWi-Fi脅威カテゴリからの保護は引き続き提供されていない状況です。これらの脅威は主としてレイヤ2で動作し、具体的には、不正AP、不正クライアント、悪魔の双子AP、隣接AP、アドホックネットワーク、構成ミスが存在するAPがこれに含まれます。  
  
たとえば、悪魔の双子APの場合はEnhanced Open Wi-Fiで使われる可能性が極めて高く、これは、OWE（Opportunistic Wireless Encryption）を被害者のクライアントと攻撃者の悪魔の双子APの間で実行できるためであり、攻撃者が用意する悪魔の双子APは、近くにある正規のAPと同じSSID（そして、おそらくは同じBSSID）をブロードキャストします。OWEによってセッションを盗聴からの保護は可能になりますが、被害者のWi-Fiトラフィックが悪魔の双子APを経由して中間者（MitM）の手に渡れば、認証情報を傍受したり、マルウェアやリモートのバックドアを埋め込んだりできるようになります。   
2019年には、脅威カテゴリの少なくとも1つがWPA3ネットワークの侵害に使われ、悪魔の双子APの対策が緊急の課題となるでしょう。

**7生体認証の大規模ハッキングにより単一要素認証が終焉を迎える**

生体認証によるログインの一般化に伴い、2019年には、生体認証のみに頼る認証方法に対する大規模な攻撃をハッカーが仕掛けてくることが予想されます。  
  
スマートフォンやゲーム機に搭載された、顔や指紋の読み取り機能による生体認証のログイン方法は、ハッカーの格好の標的となります。生体認証は、いくつもの複雑なパスワードを覚えるより便利であり、弱いパスワードより安全ではありますが、1つの認証方法であることに変わりありません。ユーザが認証の第2の要素を追加しなければ、生体認証のハッキングを成功させたサイバー犯罪者がユーザの個人情報や財務データへのアクセスを簡単に手に入れることができます。  
  
しかしながら、生体認証の突破は容易なことではないはずです。2002年にはグミを使って指紋認証を突破した研究者が現れ、2013年にはハッキング愛好家たちがiPhoneのTouch idの突破に成功し、2017年にはベトナムのセキュリティグループがAppleのFace IDを突破できるマスクを作成したと主張しました。生体認証が認証の唯一の方法として使われるようになっていることを考えれば、ハッカーがこれらの方法を完成させるのは時間の問題です。もちろん、ユーザが多要素認証を使用すれば、これらのハッキングを防ぐことができますが、生体認証を唯一の認証方法として使う傾向が2019年も続くと予想されることから、ハッカーが疑いを持たないユーザを攻撃し、生体認証をハッキングするようになるでしょう。

**8攻撃者によるインターネットの支配**



2019年には、ハクティビストの組織または国家規模において、インターネットインフラに対する組織的な攻撃が仕掛けられる可能性があります。  
  
DNSホスティングプロバイダのDynに対するDDoS攻撃によって、Twitter、Reddit、Amazon.comなど多くの人気Webサイトがダウンしたことで、セキュリティ業界は、インターネットインフラの核心部分への攻撃による影響の大きさを認識することになりました。セキュリティの専門家Bruce Schneier氏によれば、この攻撃と同時期に、インターネットに不可欠な同様のサービスを提供している複数のプロバイダを調査する活動が確認されており、サービスの弱点を見つけることを目的とするものと考えられます。Verisignなどの主要なレジストラがこの規模のDDoS攻撃の標的になると、WebサイトのTLD（トップレベルドメイン）が完全に停止してしまう恐れがあります。.comアドレスが一つ残らず解決できなくなってしまったとしたら、どれほど深刻な影響を受けることになるのでしょうか。  
  
インターネットを動作させるプロトコルであるBGP（Border Gateway Protocol）も、このシステムに大きく依存しています。ルート乗っ取りからの保護を可能にする有効なRPKI（Resource Public Key Infrastructure）レコードが存在するインターネットアドレスは全体の10％に過ぎません。さらに深刻なことに、インターネットのAS（自律システム、組織の制御下にあるIPアドレスルートの集まり）でRoute Origin Validationが有効になっている割合は0.1％に過ぎないため、残り99.9％はルート乗っ取り攻撃のリスクが極めて高いということになります。   
以上のことから、インターネットを支える複数のクリティカルポイント、あるいは根幹を成すプロトコル自体にDDoS攻撃が実施されることで、インターネットが危険に晒される恐れがあります。ハクティビストや国家規模の攻撃が急増していることを考えれば、2019年には、サイバー攻撃によるインターネットの停止が現実化してもおかしくない状況です。

MarcとCoreyによる2019年セキュリティ動向予測の解説

[**www.secplicity.org**](http://www.secplicity.org/)**では、ブログ記事、Firebox Feedのライブデータ、Coreyのデイリーセキュリティバイトを始めとする、ウォッチガード脅威ラボによる最新のセキュリティインサイトをご紹介しています。  
  
ウォッチガードのポッドキャスト「The 443 Security Simplified」に登録していただくと、セキュリティ関連の知識を楽しみながら習得できます。**