

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●2019年度セキュリティ動向予測、ウォッチガード社が発表

<http://www.atmarkit.co.jp/ait/articles/1811/29/news061.html>
https://www.watchguard.co.jp/press-release/2019_predictions.html



このニュースをザックリ言うと…

- 11月27日（日本時間）、大手セキュリティベンダーのウォッチガード社より、**2019年における情報セキュリティ業界の動向予測**が発表されました。

- 発表では以下の8つの動向予測が挙げられています：

- 1：ファイルレス（ファイルを残さず全てメモリ上で活動する）ワーム「vaporworms」が台頭
- 2：攻撃者によるインターネットの支配（ハッカー集団あるいは国家規模での組織的攻撃）
- 3：国家規模のサイバー攻撃の増加を受け、国連のサイバーセキュリティ条約が成立
- 4：AIを活用したチャットボットによる攻撃（攻撃者が正規のサイトを改ざんして設置した偽のチャットボットにより、ユーザを誘導する）
- 5：生体認証の大規模ハッキングにより認証が多要素化
- 6：国家規模の「Fire Sale」攻撃（交通・金融・通信インフラへの同時多発サイバー攻撃）が現実化
- 7：公共機関や産業制御システムを標的としたランサムウェアにより都市機能が麻痺
- 8：WPA3 Wi-Fiネットワークのハッキング

AUS便りからの所感等

- 挙げられている脅威は、**これまで存在していた脅威がさらに攻撃力を増していくものや、利便性と表裏一体で発生するもの等**、様々です。

- またWPA3について「産業全体にわたりWi-Fiインフラでより包括的なセキュリティが適用されない限り、決して安全ではない」とされているように、**WPA・WPA2のような古いプロトコルが使われ続けている限り、新しいプロトコルの持つセキュリティ機能が有効に働かないケースも存在し**、その意味ではソフトウェアのみならずハードウェアについても、計画的な更新が重要と言えるでしょう。

- 話題となっているセキュリティの脅威について随時情報収集を行い、各人が慎重な行動をとり、またシステム管理者においては、万一攻撃が成功した場合の被害を最小限に抑えられるネットワークシステムの構築をUTM等を用いつつ行って頂ければ幸いです。



防御不能マルウェアやインフラ標的の同時多発サイバー攻撃——ウォッチガードが2019年のセキュリティ動向を予測

ウォッチガードは、情報セキュリティについての2019年度の動向を予測した。過去の主な脅威に関するトレンドを分析した結果だ。従来の検知機能では防御できないファイルレスマルウェアの拡散や、国家によるサイバー攻撃を背景とした国連でのサイバーセキュリティ条約成立などを挙げた。

© 2018年11月29日 11時09分 公開



ウォッチガード、**今回発表された予測は、ウォッチガードの脅威ラボ調査チームが、過去の主な脅威に関するトレンドを分析して作成した。予測には、次の8項目が挙げられている。**

1 AIを活用したチャットボットによる攻撃	2 公共機関や産業制御システムがランサムウェアの標的になる
3 国家規模のサイバーセキュリティ条約を提出する	4 国家規模の「Fire Sale」攻撃が増加する
5 自己増殖型ファイルレス「vaporworms」攻撃	6 WPA3 Wi-Fiのハッキングによって、業界全体の無線ネットワークの欠陥が浮き彫りになる
7 生体認証の大規模ハッキングにより第三者による認証が難易度上がる	8 攻撃者によってインターネットが支配される

2019年度セキュリティ予測（出典：ウォッチガード・テクノロジー・ジャパン）



2018年11月27日 (火)
 ウォッチガード・テクノロジー・ジャパン株式会社
 ウォッチガード、2019年度セキュリティ動向予測を公開：
vaporworms、世界的なインターネット攻撃、不正AIチャットボット

8つの予測項目：次世代ランサムウェア、国家規模攻撃の増加、生体認証ハッキング、Wi-Fiプロトコルセキュリティなど

2018年11月27日 (火) —企業向け統合型セキュリティプラットフォームのグローバルリーダーである

WatchGuard (R) Technology Inc. は、2019年には、ソフトウェアの脆弱性を突き、自己増殖するワームのような性質を持つファイルレスマルウェアが増加するものと思われ、ファイルレスマルウェアは、従来のエンドポイントの検知機能で特定・防御することがより困難になります。なぜなら、感染システムにファイルを残すことなく、すべてメモリ上で動作するからです。特定の攻撃に対して脆弱な、パッチが当てられていないソフトウェアを稼働させているシステムが多いことを考慮すると、2019年は「vaporworms」の拡散が懸念されます。

2. 攻撃者によるインターネットの支配：2019年には、ハッカー集団または国家規模でインターネットのインフラに対して組織的な攻撃が仕掛けられる可能性があります。インターネットを制御するプロトコル (BGP) は、自己管理システムで大規模運用されており、2018年にホスティングプロバイダ「Dyn」に対して発生したDDoS攻撃では、ホスティングプロバイダまたは登録機関への単体攻撃で主要なWebサイトを閉鎖できることが明らかになりました。つまり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により、インターネットが危険に晒されることと考えられます。

3. 国家規模のサイバー攻撃の増加を受け、国連のサイバーセキュリティ条約が成立：国連が国際サイバーセキュリティ条約を2019年に制定し、国家が背後で支援するサイバー攻撃の増加に対して強い意志を持って取り組むことが予想されます。

4. AI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正規のサイト上に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、悪意のあるリンクをクリックさせたり、マルウェアを含むファイルのダウンロードを促したり、あるいは個人情報やデータを盗み取ることが予測されます。

●監視カメラへの不正アクセス・乗っ取り50件以上…元自衛官を書類送検

<https://www.asahi.com/articles/ASLCN4K50LCNPIHBO1F.html>



このニュースをザックリ言うと…

- 11月21日（日本時間）、兵庫県警より、**インターネットに接続された監視カメラ等へ不正アクセスを行った電子計算機損壊等業務妨害容疑**で、元自衛官の男を書類送検したと発表されました。
- 4月下旬に、神戸市東灘区の障害者施設の監視カメラ1台と千葉県八千代市の水位監視カメラ2台に不正アクセスし、画面に「I'm Hacked. bye2」と書き込んだり、パスワードを変更したりしてそれぞれ業務を妨害した疑いが持たれています（AUS便り 2018/05/07号も参照）。
- 被害を受けた監視カメラは、**パスワードが初期設定のまま変更されていない**とのこと。

AUS便りからの所感等

- 同様の被害は今年60件以上発生しているとされ、また容疑者も50～100件以上同様の不正アクセスを行ったと供述しています。
- **インターネット上から接続可能な状態になっている複合機やIoT機器等を検索できる「SHODAN」「Censys」といったサーチエンジンが存在し、今回の容疑者のみならず多くの攻撃者が日夜ターゲットとする機器を検索しているものと推測されます。**
- 外部からアクセスされるべきでないサービスポートについては、UTMやファイアウォールによるフィルタリングを行い、画像をWebで公開しているカメラ等についても管理画面にはアクセスされないよう適切な設定を行うようにしましょう。
- 併せて、その状態で外部から不正アクセスを受ける可能性がないか、ネットワーク診断を受けることにより、安全性を確認することも一考に値するでしょう。

朝日新聞 DIGITAL



●Webサーバ「Nginx」の脆弱性を悪用する攻撃準備中か…最新版へのアップデートを

<https://this.kiji.is/435938239837946977>



このニュースをザックリ言うと…

- 11月15日（日本時間）、ビッグデータ分析等を行うシンガポールAntuit社より、Webサーバソフトウェア「Nginx」の脆弱性（CVE-2018-16843, CVE-2018-16844, CVE-2018-16845）を悪用する**大規模な攻撃を攻撃者が計画している**として注意喚起が出されています。
- 同社が11月8日頃からダークウェブフォーラムで傍受していた攻撃者の会話によれば、**脆弱性の影響を受けやすいサーバを探し出すキャンペーンを計画**しており、また脆弱性を突いてサーバの速度を低下あるいは完全に停止させられる攻撃ツールを設計しているとされています。
- また、この攻撃の標的となる可能性がある国は、米・英・日本および東南アジア諸国等とされています。

AUS便りからの所感等

- Nginxは、ApacheやIISと並んで高い人気を誇るWebサーバ（およびプロキシ）ソフトウェアで、ここ最近では脆弱性が報告されることが比較的少なかったのですが、11月7日、DoS攻撃等につながる脆弱性3件が一度に報告されています。
- **近年シェアを伸ばしていることもあり、攻撃者にとって今回の脆弱性が格好のターゲットである**ことは容易に想像できます。
- 脆弱性はNginxバージョン1.15.6以降または1.14.1以降で修正されていますので、利用している場合は速やかに最新バージョンへのアップデートを行うようにしてください。

ScanNetSecurity

