

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。

## ●テレワークでのVPN利用にセキュリティリスク…米当局が注意喚起

<https://japan.zdnet.com/article/35150877/>  
<https://news.mynavi.jp/article/20200318-997441/>



### このニュースをザックリ言うと…

- 3月13日(現地時間)、米政府機関のCISAおよびUS-CERTより、新型コロナウイルス対策に伴う**テレワーク(リモートワーク)実施におけるセキュリティリスク**について**注意喚起**がされています。
- テレワークにおいて社内ネットワークへのVPN接続を行う場合が多く、その際のセキュリティリスクとして「VPNを利用する企業について**これまで以上に多くの脆弱性を悪用される**」「VPNが**年中無休で動作**することにより、VPNに関する**システムへのセキュリティパッチが適用されない**」「**在宅勤務者を標的としたフィッシングメールによりアカウント情報が奪取される**」「**リモートアクセスに多要素認証を採用しない企業では、よりフィッシング攻撃を受けやすくなる**」「VPN**同時接続数の制約の超過により接続できないユーザーが発生する**」といった可能性が挙げられています。
- CISAでは、対策として「**VPNやネットワークインフラ機器、リモート接続で使用する機器では最新のセキュリティパッチや構成を適用する**」「**フィッシング攻撃増加の可能性について従業員への注意喚起**」「**ログの確認による攻撃の検知等の体制を整える**」「**全てのVPN接続で多要素認証を実装、あるいは強力なパスワードを設定する**」「**可能なら帯域幅を必要とするユーザーに優先順位を付けたり、転送レートの制限を設けたりする**」等を挙げています。

### AUS便りからの所感等

- **VPN機器**については、**昨年9月に複数メーカーの機種において脆弱性が発表され、それに対する攻撃も確認**されています(AUS便り 2019/9/24号参照)。
- テレワークを行う各従業員の多くは自宅のネットワークから行うと考えられ、ユーザー側・企業側とも**社内LANとはまた別のリスクを同時に考慮**する必要があるでしょう。
- 「対策が行われているシステムを信頼する」ものとは正反対の、全てを「信頼せず」「常に検査・確認する」、いわゆる「ゼロトラストネットワーク」に基づくシステム構築も提唱されているものの、VPNはおろか社内LANをも撤廃し、クラウドを全面活用することも念頭に置くこととなり、移行にはユーザー側の意識の変化も含め大規模な手間がかかることも考えられます。
- ともあれ、例えばVPNを新たに構築したことにより生じた隙を突破されただけで、そのシステムのすべてが乗っ取られるような事態にならないよう、**複数の対策でカバーできる体制を構築することは、テレワーク云々を考えるまでもなく平生より考慮すべきこと**であり、アンチウイルス導入やその確認、あるいはUTMの活用もまた、そういった対策の一つとして取り入れられるべきものです。



テレワークでのVPN利用にセキュリティリスク--米当局が注意喚起

ZDNet Japan Staff 2020-03-16 13:34

米国土安全保障省傘下のCybersecurity and Infrastructure Security Agency (CISA) は3月13日、新型コロナウイルス対策に伴うテレワークでのVPN利用について企業などにセキュリティ上の注意喚起を行った。

CISAは、企業が新型コロナウイルスの感染拡大を防止するために、在宅勤務などのテレワークを実施するにはVPNの利用が必要であり、より堅牢なセキュリティ対策が確保されているべきだと解説する。

セキュリティのリスクとしては、VPN利用が広がるにつれてサイバー攻撃者は、組織の脆弱性を探る動きを活発化させる恐れがある。在宅勤務者を標的としたフィッシングメールによってユーザー名やパスワードなどの情報を窃取する攻撃を拡大させ、リモートアクセスで多要素認証を使用しない組織ではフィッシング攻撃を受けやすくなると警鐘を鳴らす。



新型コロナウイルスで増えるテレワーク狙う、サイバー攻撃に警戒を

後藤大地 2020/03/18 10:32

関連キーワード: 新型コロナウイルス, テレワーク, サイバー攻撃

United States Computer Emergency Readiness Team (US-CERT)は2020年3月13日(米国時間)、「Enterprise VPN Security | CISA」において、新型コロナウイルスの影響で、企業は働き方の選択肢としてテレワークを提供し、そのセキュリティ対策としてVPNを導入するケースが増えている中、攻撃者がVPNを狙うリスクが高まっているとして注意を喚起した。

### ●新型コロナウイルス便乗の詐欺・サイバー攻撃に注意

<https://news.mynavi.jp/article/20200314-995168/>  
<https://www.itmedia.co.jp/news/articles/2003/13/news123.html>  
[http://www.kokusen.go.jp/news/data/n-20200312\\_1.html](http://www.kokusen.go.jp/news/data/n-20200312_1.html)



### このニュースをザックリ言うと…

- **新型コロナウイルスに便乗したネット上の詐欺ないしサイバー攻撃**について、**国内外で注意喚起**がされています。
- 3月12日(日本時間)、国民生活センターが発表した情報では、「**30枚41,800円でマスクを売る**」と偽り、**個人情報・クレジットカード情報等を詐取**するような不正なサイトに誘導する手口が確認されていることです。
- 3月12日(米国時間)、セキュリティベンダーの米Digital Shadows社の情報では、「**日本の障害者福祉施設や保健所を騙り**、マルウェアEmotetへの感染を狙う日本語のメール」「**米国の大学による正規の新型コロナウイルス感染分布図**が添付されたフィッシング詐欺」「**WHO(世界保健機関)を騙るフィッシング詐欺**」といった例が挙げられています。

### AUS便りからの所感

- 国民生活センターでは「**実在する企業名が書かれたメール**でも、**記載された電話番号に電話したり、リンクをクリックしたりせず、企業のWebサイトを直接確認し、必要に応じて問い合わせる**」よう呼び掛けています。
- Digital Shadows社も同様に、**公式な機関のガイダンスのみに従うことや、慈善寄付を募るメールに注意すること、また非公式の業者から医療機器を購入しないこと**等と呼び掛けています。
- **新型コロナウイルスとマルウェアとで必ずしも一概に比較できるものではありませんが、最新の正しい情報を的確に収集し、慎重に行動しつつ適切な対策をとるのが肝要であることは共通している**と言えるでしょう。

国立行政法人 国民生活センター  
NATIONAL CONSUMER AFFAIRS CENTER OF JAPAN

注目情報	相談事例・判例	相談・紛争解決 / 情報受付	研修・相談員資格 / 研修施設	ライブラリ	当センターについて
現在の位置: <a href="#">トップページ</a> > <a href="#">注目情報</a> > <a href="#">消費生活</a> > <a href="#">新型コロナウイルスに便乗した架空の「マスク販売広告メール」にご注意!</a> (速報第2弾)					
[2020年3月12日:公表]					
<p><b>新型コロナウイルスに便乗した架空の「マスク販売広告メール」にご注意!</b> (速報第2弾)</p> <p>*詳細な内容につきましては、本ページの最後にある「報告書本文(PDF形式)」をご覧ください。</p> <p>新型コロナウイルスの感染拡大に関連した相談が、全国の消費生活センター等に寄せられています。今回、マスクの入手が困難な状況に便乗した不審なマスク販売広告メールに関する情報が「<b>消費者トラブルメール速報</b>」に寄せられ、調査の結果、架空の広告であることがわかりましたので被害の未然防止のために紹介します。</p>					
<p><b>相談事例</b></p> <p>【事例】不審なマスク販売広告メールがスマートフォンに届いた。産業資材を扱うメーカー名の送信者名(差出人名)で、マスクの画像と共に「ウイルス、バクテリア、PM2.5、H7N9などを防いで、汚染された空気の吸入を予防します」などと記載され、「ご購入はこちら」とURLが付いたメールがスマートフォンに届いた。価格は30枚41,800円と高額で「新型コロナウイルスの影響により、物流時間が長くなる可能性があります」などがある。怪しいので情報提供する。 (受付年月: 2020年3月 情報提供者: 40歳代 男性)</p>					
<p><b>調査結果</b></p> <p>国民生活センターよりメールの送信者名となっている産業資材メーカーに確認をしたところ、次のことがわかりました。</p>					
<p><b>注目情報</b></p> <ul style="list-style-type: none"> <li>▼ 発表情報</li> <li>▼ テーマ別当番</li> <li>▼ 製品テスト</li> <li>▼ リンク集「くらしの危険」</li> <li>▼ 良守り情報(高齢者・障がい者・子どものトラブル防止)</li> </ul> <p><b>相談したい</b> (消費生活センター等一覧)</p> <p><b>テーマ別特集</b> (ネットトラブル、高齢者被害…)</p> <p><b>身近な消費者トラブルQ&amp;A</b></p>					

### ● 10億台以上のAndroidデバイスが危険な状態

<https://news.mynavi.jp/article/20200310-992519/>  
<https://press.which.co.uk/whichpressreleases/void-android-more-than-one-billion-android-devices-at-risk-of-hacking-attacks/>



### このニュースをザックリ言うと…

- 3月6日(米国時間)、ネットメディア「Which? Press Office」より、**世界中の10億台以上のAndroidデバイスがセキュリティアップデートの対象外となっており、サイバー攻撃に対して脆弱な状態にある**と指摘する記事が発表されました。
- 記事によれば、2019年5月の時点で、Androidのアクティブユーザの**42.1%がAndroid 6.0およびこれよりも前のバージョンを使用**している一方、**Android 7.0未満に対するセキュリティパッチは2019年にリリースされていない**ことを指摘しています。
- 最近サポートの対象外となったAndroidデバイスは今すぐに危険とは限らないとしつつも、**Android 7およびそれ以前についてはバージョンアップ**することを推奨し、バージョンアップできない場合、**特にAndroid 4以前についてはデバイスを買換える**よう呼び掛けています。

### AUS便りからの所感

- 記事ではこの他にも**Google公式のアプリストア(Google Playストア)以外からはアプリをダウンロードしないこと、(少なくとも2箇所)バックアップをとっておくこと、およびAndroid向けのアンチウイルスソフトの導入**と呼び掛けていますが、これは**現在サポートされているAndroid 8以降であっても重要な事項**と言えます。
- Androidの各バージョンにおいてセキュリティパッチのリリースが保証されているのは最低でも2年で、**同じバージョンを3年を超えて使い続けることは概ねリスクが伴うもの**となる上、バージョンアップやパッチが提供されるかは機種によっても異なることに注意し、**必要に応じてデバイスの乗り換えが行える体制**を用意しておくことが肝要です。

### マイナビニュース

#### 10億台以上のAndroidデバイスが危険な状態

◆ 後藤大地 © 2020/03/10 12:44  
関連キーワード: サイバー攻撃, エンドポイントセキュリティ, スマホセキュリティ

Which? Press Officeは3月6日(米国時間)、「[Void Android: More than one billion Android devices at risk of hacking attacks - Which? Press Office](#)」において、世界中の10億台以上のAndroidデバイスがセキュリティアップデートなどのサポート対象から外れており、サイバー攻撃に対して脆弱な状態にあると指摘した。

これは世界のAndroidユーザーのうち、5人に2人がGoogleからの重要なセキュリティアップデートを受け取っていないことを意味するという。結果として、データ窃取や身代金要求、その他のマルウェア攻撃のリスクにさらされているおそれがある。