

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。

## ●国民生活センターが「偽セキュリティ警告画面」に注意喚起

<https://securityblog.jp/news/20181115.html>  
[http://www.kokusen.go.jp/news/data/n-20181107\\_1.html](http://www.kokusen.go.jp/news/data/n-20181107_1.html)



### このニュースをザックリ言うと・・・

- 11月7日（日本時間）、国民生活センターより、**インターネット使用中に突然表示される「偽セキュリティ警告画面」**についての注意喚起が出されました。
- 同センターのPIO-NET（全国消費生活情報ネットワークシステム）に寄せられた、偽警告画面で不安になり慌てて偽のセキュリティソフトやサポートを契約した等の相談は、2015年度の988件から2016年度に5,221件と急上昇しています。
- さらに2017年度4～9月期の相談件数1,601件（年間3,093件）に対し、**2018年度4～9月期は2,135件**となっているとのこと。
- 同センターでは、警告画面が表示されても鵜呑みにせず、慌てて連絡や契約をしないこと、不安に思った場合には同センター等に相談するよう呼びかけています。

### AUS便りからの所感等

- 偽警告画面等で脅かして、ユーザにソフトウェアをインストールするよう誘導するといった、いわゆる「スケアウェア」(※)等と呼ばれる手口は以前から存在していますが、2015年頃にいわゆる「サポート詐欺」が国内で確認されるようになったことが2016年度の相談件数の急上昇につながったものとみられます。
- (※)ユーザを脅して恐怖心をあおり、金銭や個人情報を奪うことを目的としたマルウェア
- IPAの安心相談窓口においても、5・6月頃から相談件数が増えたとして、7月18日に注意喚起を行っています (<https://www.ipa.go.jp/security/anshin/mgdayori20180718.html>)。
- とにかくどんな手口があるのか情報収集して熟知し、かつアンチウイルスやUTMによる防御を確実に行うことが重要です。



### 国民生活センターが「偽セキュリティ警告画面」に注意喚起

2018年11月15日

国民生活センターは、11月7日、「インターネット使用中に突然表示される偽セキュリティ警告画面にご注意!」という注意喚起を発表した。

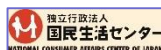


これによると、全国の消費生活センターなどに、インターネットを使用中に突然「ウイルスに感染している」などの警告画面が表示される相談が数多く寄せられているという。その件数は、2013年度(946件)、2014年度(875件)、2015年度(988件)と推移していたが、2016年度は5,221件、2017年度は3,093件と増加し、2018年も9月末までに2,135件と昨年を上回るペースで相談が寄せられている。

同センターが挙げる具体例として、(1)パソコンでインターネットを使用しているときに、「警告画面が表示されても鵜呑みにしない」「あわてて契約や連絡をせず、不安に思った場合は各地の消費生活センターなどに相談する」といったアドバイスをしている。

なお、独立行政法人 情報処理推進機構(IPA)からも、2018年7月に「偽セキュリティソフト(詐欺的セキュリティソフト)に関する注意喚起がなされている(関連記事)。こちらも併せて確認することをおすすめする。

- ・インターネット使用中に突然表示される偽セキュリティ警告画面にご注意!(国民生活センター)
- ・ネット閲覧中の「偽セキュリティ警告」に注意—詐欺的誘導で合法的に料金徴収(セキュリティ通信: So-netブログ)
- ・IPAが「偽のセキュリティ警告」に注意喚起(セキュリティニュース)

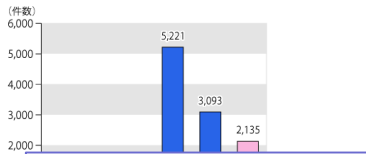


### インターネット使用中に突然表示される偽セキュリティ警告画面にご注意!

\*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)」をご覧ください。

全国の消費生活センター等には、インターネットを使用中に突然「ウイルスに感染している」等の警告画面が表示され、不安になり慌ててセキュリティソフトやサポートを契約してしまったところ、実際には偽の警告画面と思われ不要な契約だったという相談が多く寄せられています。

図 PIO-NETにみる、警告画面や警告音をきっかけとしたセキュリティソフト等に関する相談件数



#### 相談事例からみる問題点等

1. 突然警告画面が表示され、消費者を不安にさせセキュリティソフト等の契約をさせている
2. 解約手続きがスムーズに進まない

#### 消費者へのアドバイス

1. 警告画面が表示されてもうのみならず、慌てて連絡や契約をしないようにしましょう
2. 不安に思った場合やトラブルになった場合は、消費生活センター等に相談しましょう

※消費者ホットライン:「188(いやや!)」番

#### セキュリティソフトをインストールしてしまった場合等の対処方法

- ・偽のセキュリティ警告によって有償の「ソフトウェア購入」や「サポート契約」をしてしまう相談が増加中～インターネット利用中に表示される偽の警告画面にだまされないで!～(安心相談窓口だよ) (2018年7月18日)。(独立行政法人 情報処理推進機構)

## ●WordPress プラグイン「AMP for WP」「WP GDPR Compliance」の脆弱性を突く攻撃に注意

<https://www.sakura.ad.jp/information/announcements/2018/11/22/1968198825/>



### このニュースをザックリ言うと…

- 11月22日（日本時間）、さくらインターネット社より、**WordPressのプラグインの脆弱性とそれを悪用した攻撃について注意喚起**がされています。
- 問題となっているプラグインは「AMP for WP」と「WP GDPR Compliance」で、**脆弱性の悪用により、WordPressを利用しているWebサイトが改ざんされる等の可能性があります**としています。
- 「AMP for WP」は0.9.97.20、「WP GDPR Compliance」は1.4.3で脆弱性が修正されており、アップデートが強く推奨されています（「AMP for WordPress」等、似たような名前のプラグインもあるため注意してください）。

### AUS便りからの所感等

- 上記プラグインの問題と攻撃については、11月9日および20日に、米国のセキュリティ企業Defiant社から警告がされていました。

- **WordPressはそれ自体もたびたび脆弱性を突かれ、時には多くのサイトにマルウェアが感染したケースもある**（AUS便り 2018/06/11号 参照）ため、随時管理画面を参照して本体・プラグインともどもアップデートを確認し、可能な限りセキュリティ機能を提供するプラグインやWAFの導入により防御を固めることを推奨致します。



WordPressのプラグイン「AMP for WP」「WP GDPR Compliance」における緊急性の高い脆弱性についての注意喚起

2018年11月22日

お客さま各位

平素よりさくらインターネットに格別のご愛顧を賜り、誠にありがとうございます。

WordPressで利用できる「AMP for WP」「WP GDPR Compliance」のプラグインに深刻な脆弱性が確認され、ウェブサイトの改ざんなどの被害が報告されています。これらのプラグインを利用しているお客さまは、ご自身のウェブサイトの正常性の確認と併せて、早急に対策を実施いただきますようお願いいたします。

詳細は下記をご覧ください。

さくらインターネットでは、今後もよりよいサービスの提供が行えますよう、精一杯努めてまいります。引き続き変わらぬご愛顧を賜りますようお願い申し上げます。

「AMP for WP」「WP GDPR Compliance」プラグインの脆弱性について

## ●Flash Playerに2週連続で脆弱性、31.0.0.153へのアップデートを

<http://www.itmedia.co.jp/enterprise/articles/1811/21/news066.html>



### このニュースをザックリ言うと…

- 11月20日（日本時間）、Adobe社より、「Flash Player」のセキュリティアップデートとなるバージョン**31.0.0.153**がリリースされました。
- 不正なFlashコンテンツの読み込みにより、PCを乗っ取られる可能性がある脆弱性が修正されているとのことです。
- 同13日のFlash Player 31.0.0.148リリース（AUS便り 2018/11/19号 参照）から**2週連続でのリリース**となりますが、同社では直ちに最新バージョンへのアップデートを行うよう強く推奨しています。

### AUS便りからの所感等

- 今回も、マイクロソフトから同日に、Windows8以降のIE・Edge向けFlash Playerがリリースされています。

- 通常であれば自動的に最新バージョンにアップデートされますが、確認ページ（<https://get.adobe.com/jp/flashplayer/about/>）等で確認するのが良いでしょう。

- 2020年のサポート終了までFlashコンテンツは使われ続け、またFlash Playerの脆弱性を突く不正なコンテンツも現れ続けるでしょうから、**最新バージョンへのアップデートは必須**ですが、併せて各種ブラウザでのFlashコンテンツをブロックする機能や、アンチウイルス・UTMによる防御も普段から必ず行うようにしましょう。



### Adobe、Flash Player更新版を緊急公開 脆弱性に関する詳細を研究者が事前に公表

脆弱性に関する技術的詳細が既に公表されていることから、直ちにFlash Playerを最新バージョンに更新するよう促している。

© 2018年11月21日 09時09分 掲載

【記事文字】ITmedia

Adobe Systemsは11月20日、Flash Playerの脆弱性修正のためのアップデートをWindows、macOS、Linux、Chrome OS向けに緊急公開した。脆弱性に関する技術的詳細が既に公表されていることから、直ちに更新するよう促している。

Adobeのセキュリティ情報によると、Flash Player 31.0.0.148までのバージョンに、悪の取り込み（Type Confusion）に起因する深刻な脆弱性が存在する。悪用されれば任意のコードを実行される恐れがある。

この問題は、最新バージョンの31.0.0.153で修正された。優先度はWindows、macOS、Chrome OSが「1」、Linuxは「3」に分類している。

| Product  | Version  | Platform                             | Priority | Availability  |
|--|----------|--------------------------------------|----------|---|
| Adobe Flash Player Desktop Runtime                             | 30.0.0.3 | Windows, macOS                       | 1        | Flash Player Download Center<br>Flash Player Distribution |
| Adobe Flash Player for Google Chrome                           | 30.0.0.3 | Windows, macOS, Linux, and Chrome OS | 1        | Google Chrome Releases                                    |
| Adobe Flash Player for Microsoft Edge and Internet Explorer II | 30.0.0.3 | Windows 10 and 81                    | 1        | Microsoft Security Advisory                               |
| Adobe Flash Player Desktop Runtime                             | 30.0.0.3 | Linux                                | 3        | Flash Player Download Center                              |

脆弱性が修正された最新バージョンは31.0.0.153となる