

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。

## ●長期休暇における情報セキュリティ対策、IPAが呼びかけ

[http://internet.watch.impress.co.jp/docs/news/20150807\\_715558.html](http://internet.watch.impress.co.jp/docs/news/20150807_715558.html)

<http://www.ipa.go.jp/security/measures/vacation.html>



### このニュースをザックリ言うと…

- 8月4日（日本時間）、独立行政法人情報処理推進機構（IPA）は、多くの企業が夏季休暇となる8月10日の週を迎えるにあたり、セキュリティ対策の再度徹底を呼びかけています。
- IPAは、長期休暇の時期は「システム管理者が不在になる」ためにセキュリティ上の被害の対処が遅れてしまう、あるいは「友人や家族と旅行に出かける」ことでSNSへの書き込み内容から思わぬトラブルが発生する等の可能性があるとしています。
- 呼びかけでは、組織内のシステム管理者およびユーザに対し、休暇前・休暇中・および休暇明けにとるべき対策のポイントを挙げており、例えば管理者に対しては、休暇前に「緊急連絡体制の確認」「使用しないサーバ機器の電源OFF」、休暇明けに「パッチの適用」「アンチウイルスの更新」「サーバの各種ログの確認」を呼びかけています。
- また、休暇中の業務対応等の理由で機器やデータを持ち出す必要があるユーザに対しては、休暇前の「持ち出しルールの確認と遵守」、休暇中の「厳重な管理」および休暇明け時にはやはり「パッチの適用」「アンチウイルスの更新」そして「持ち出した機器やUSBメモリ等のウイルスチェック」を行うよう呼びかけています。

### AUS便りからの所感等

- IPAの呼びかけは、何らかの情報機器とインターネットを組織内外で利用する者として、普段からセキュリティを意識した慎重な行動をとることを改めて示す以外にも、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。
- 特に今年の長期休暇は、年末年始よりも前に、9月後半に5連休となる所もあるため、その分だけ特有のリスクも増大することに注意すべきでしょう。
- また、UTMは組織ネットワークの境界における防御を果たすものですが、それがカバーしきれないものも存在し得るため、UTMによる防御と全てのユーザに対する随時のセキュリティ教育は、組織全体におけるセキュリティの向上のためにいずれも欠かせないものでしょう。

**INTERNET Watch**

最新ニュース

まもなく夏季休暇、セキュリティの再チェックをIPAが呼び掛け

(2015/8/7 12:24)

独立行政法人情報処理推進機構 (IPA) は2015年の夏季休暇シーズンを前に、セキュリティ対策を再徹底するよう、注意を呼び掛けている。休暇中に緊急事態が発生した場合の連絡体制確認、休暇明け直後の修正プログラム適用などが重要としている。

長期休暇期間中は、万が一インシデントが発生した場合の被害確認に時間がかかったり、OSなどのシステムに深刻な脆弱性が発見した場合の対処が遅れるといった可能性があるため、通常とは異なるセキュリティ対応が必要となる。

組織のシステム管理者は、委託先企業を含めた緊急連絡体制や、緊急事態発生時の対応手順などを改めて明確化しておく必要がある。連絡フローが現在の組織体制に沿っているか、担当者の電話番号が変わっていないかも確認してほしいという。

また、長期休暇が明けた直後には、修正プログラムやウイルス定義ファイルを早急に適用させたり、ログを確認することも重要としている。

企業内部でPCなどを利用している従業員などは、機器やデータの持ち出しルールを徹底し、紛失や盗難にも十分警戒する必要がある。

**IPA** Better Life with IT 情報処理推進機構

長期休暇における情報セキュリティ対策

掲載日: 2015年8月4日  
独立行政法人情報処理推進機構  
技術本部 セキュリティセンター

0 はじめに

長期休暇の時期は、「システム管理者が不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりやすく、ウイルス感染や不正アクセス等の被害が発生した場合に適切な対処が遅れたり、SNSへの書き込み内容から思わぬトラブルが発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。このような事態とならないよう、以下の対策を実施してください。

1. 組織のシステム管理者向け

～ 長期休暇前の対策 ～

1. 緊急連絡体制の確認

不測の事態が発生した場合に備えて、システム管理・運用の委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認してください。

## ●内閣府Webサイトのメールアカウント乗っ取り、約2万通のスパムメール送信

<http://www3.nhk.or.jp/news/html/20150803/k10010177031000.html>



### このニュースをザックリ言うと…

- 8月3日(日本時間)、内閣府が運営する「内閣府NPOホームページ」のサポートデスクのメールアカウントが不正アクセスによって乗っ取られ、7月30日午前0時過ぎに約2万通のスパムメール送信が行われたことが発表されました。

- 乗っ取りが発生した原因としては、管理先の大手民間業者が短くて推測しやすいパスワードを使用していたためとみられています。

- サポートデスクはシステム上、内閣府のWebサイトから切り離されており、内閣府の内部情報の流出はないとしている一方、サポートデスクを利用するNPOに関する情報が流出していないか確認中とのことです。

### AUS便りからの所感等

- 不正アクセスの詳細は不明ですが、もしサーバ自体への侵入がなくとも、外部からサーバを介してメールを送信するためのSMTP認証が破られることにより、不正なメール送信の踏み台にされ、外部に対し加害者となってしまう可能性があることに注意が必要です。

- SMTP認証、およびメール受信のためのPOP3/IMAP4は、何らかの対策を採らない限り、外部からブルートフォースを行うことが容易であるため、パスワードは可能な限り強固なものとし、かつ不正なログインを試みる外部のアクセス元を遮断する等のサーバ側での設定を行うことが重要です。

- 一方で、内部への侵入のみならず、不審なメール送信等といった、内部から外部への不正な通信をも的確に検知し、不正アクセスの事実を早期に知るためにも、そういった検知・遮断機能を搭載したUTMの設置を強く推奨致します。



#### 内閣府HP メール約2万通が不正送信

8月3日 08時39分

全国のNPO法人に関する情報を取りまとめている内閣府のホームページで、問い合わせに対応するメールアカウントが何者かに乗っ取られ、およそ2万通のメールが不特定多数のアドレスに送信されていたことが分かり、内閣府では個人情報の流出が心配かどうかが調べています。

先月30日 未明

サポートデスクのメールアカウントから、約2万通のメールが不特定多数のアドレスに送信された。NPO法人ホームページのメールアカウントが乗っ取られた。

## ●音声で偽のウイルス検出を警告する詐欺サイトに注意呼びかけ

<https://www.ipa.go.jp/security/txt/2015/08outline.html>

<http://blog.trendmicro.co.jp/archives/11576>



### このニュースをザックリ言うと…

- 8月4日(日本時間)、独立行政法人情報処理推進機構(IPA)が毎月行っている「今月の呼びかけ」の8月度が発表され、音声メッセージを伴う偽のウイルス検出警告に関する相談が6月以降多く寄せられていることが挙げられています。

- 音声メッセージは「あなたのコンピュータでウイルスが検出されました」で始まり、マルウェア除去のための案内と称してある電話番号へ電話をかけるよう誘導するものとなっており、大手セキュリティベンダーのトレンドマイクロ社も、6月に同様の行為を行う詐欺サイトを複数確認していることを発表しています。

- IPAはこのケースについて、不用意な広告のクリックや何らかのリダイレクトによってサイトに誘導された可能性があること、PCのスキャンを行ったりしているわけではなく、実際のマルウェアへの感染の有無に関わらず単にWebページ上で音声ファイルを再生しているに過ぎないこと、また電話をかけることによって何らかのソフトウェアの購入を勧められる可能性があることを説明しています。

### AUS便りからの所感等

- 音声メッセージによる警告は、ユーザへ効果的に不安を与える手段として、「お使いのパソコンの性能が低下しています」等と表示する不正なバナー広告よりもさらに推し進めたものと考えられます。

- 少なくとも現時点では、警告を表示するページや音声メッセージファイルからマルウェアが感染するようなものではないようですが、不審なコンテンツの再生あるいは不審なサイトへの誘導を事前に食い止めるよう、ブラウザあるいはUTMによるアンチフィッシング機能を十分に活用することがこういった詐欺に引っかからないために有効となるでしょう。



#### 月別相談件数推移

