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。

●「小さな中小企業とNPO向け情報セキュリティハンドブック」NISCが公開

https://www.itmedia.co.jp/news/articles/1904/19/news057.html
https://www.nisc.go.jp/security-site/blue_handbook/index.html

このニュースをザックリ言うと・・・

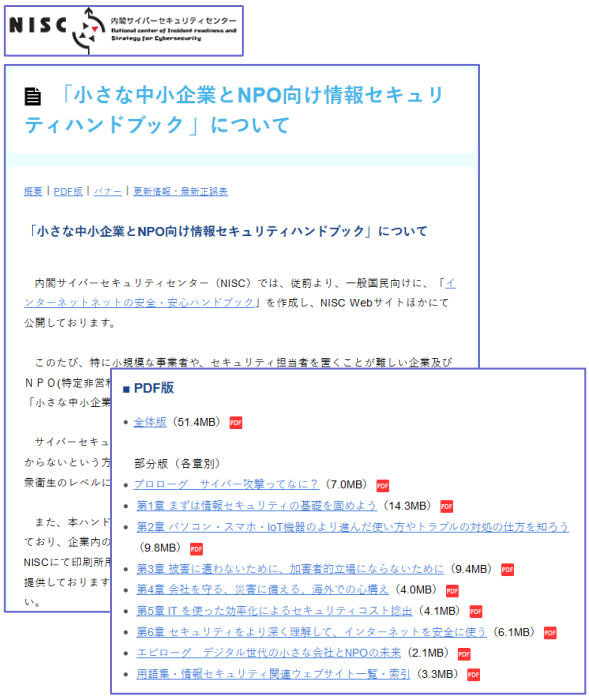
- 4月19日（日本時間）、内閣サイバーセキュリティセンター（NISC）より、「小さな中小企業とNPO向け情報セキュリティハンドブック」が公開されました。

- NISCではこれまでも「インターネットの安全・安心ハンドブック」を公開しており（AUS便り2019/01/28号参照）、今回は新たに小規模の企業、およびセキュリティ担当者を置くことが難しい企業およびNPOを対象としたものとなっています。

AUS便りからの所感等

- 個人から企業まで広いユーザを対象としていた「インターネットの安全・安心ハンドブック」と同様に、
「基本的なセキュリティのポイント」
「パソコン・スマホ・IoT機器のより進んだ使い方やトラブルの対処の仕方」
「最新の攻撃の手口(PC等を乗っ取られることで起こり得ること等)」
等を解説している一方、事業継続計画（BCP）の策定等を紹介する
「会社を守る、災害に備える、海外での心構え」
「ITを使った効率化によるセキュリティコスト捻出」
といった独自の内容も含まれています。

- 企業等の経営者から従業員に至るまでに対する「教育の題材」として、システム・ネットワークの見直しやUTM等セキュリティソリューション導入のための「有用な視点」として、あるいは既に十分なリテラシーを持っているユーザにとっても注意すべきポイントを再度見直す等に活用して頂ければ幸いです。



●使ってはいけないパスワードトップ10万が発表

https://news.mynavi.jp/article/20190422-812944/

このニュースをザックリ言うと・・・

- 4月21日（現地時間）、英国国家サイバーセキュリティセンター（NCSC）より、過去に漏洩したパスワードのデータをもとにした「使ってはいけないパスワード」トップ10万通りが発表されています。

- データは、入力したパスワードやメールアドレスが過去に漏洩していないか調査可能なサイト「Have I Been Pwned」の提供によるものです。

- 発表されたうち上位10通りは「123456」「123456789」「qwerty」「password」「111111」「12345678」「abc123」「1234567」「password1」「12345」となっており、以後も「同じキーの繰り返し入力」「左から右に何個といった規則性のあるキーボード入力を行うことで現れるもの」「単語」が使われる傾向があるようです。

- NCSCではこのデータをテキストファイルとして公開しており、このファイルに使っているパスワードが含まれている場合は直ちに変更するよう推奨しています。


マイナビニュース

使ってはいけないパスワードトップ10万が発表、第1位は？

後藤大地　2019/04/22 09:36

関連キーワード：調査データ

National Cyber Security Centre (NCSC：英国国家サイバーセキュリティセンター)は4月21日(米国時間)、「National Cyber Security Centre - Passwords, passwords everywhere」において、Troy Hunt氏と協力して、同氏が過去に漏洩したパスワードを収集しているWebサイト「Have I Been Pwned」のデータから使ってはいけないパスワードトップ10万を公開した。

データはPwnedPasswordTop100k.txtにおいてテキストファイルで公開されており、このファイルに使っているパスワードが含まれている場合は直ちにパスワードの変更を実施したほうがよいとされている。

AUS便りからの所感等

- これらのパスワードは、今回の発表以前に様々なアカウント奪取を目論む攻撃者が使用する脆弱なパスワードの辞書には既に載っている可能性が高く、Web・メールサービスはもちろん、あらゆる場面において使うべきではありません。

- 今日、パスワード以外にも二段階認証等の様々なアカウント保護機構が採用されており、可能な限りそれを利用することも大切ですが、パスワードを狙う攻撃に対しては、（例えばツールによる管理を用いてでも）他人から推測されにくいある程度複雑なパスワードを設定すること、登録するサービスごとに別のパスワードを用いること、そして万が一流出が確認され次第速やかにパスワードの変更を行うことが肝要です。

●IE・EdgeとChromeに脆弱性、Chromeは最新バージョン更新確認を

https://internet.watch.impress.co.jp/docs/news/1178149.html

このニュースをザックリ言うと・・・

- 4月3日（現地時間）、トレンドマイクロ社より、Internet Explorer（IE）およびEdgeに未修正の脆弱性が存在することが発表されました。

- 4月10日に発表されたIEの脆弱性（AUS便り 2019/04/22号参照）とは別のもので、悪用により、他のサイトで使用しているCookie情報にアクセスされる可能性があるとされ、マイクロソフトからの修正が発表されるまでIE・Edgeの使用を控えるよう呼びかけています。

- 一方、4月23日にはGoogleおよびUS-CERTより、Google Chromeにおける複数の脆弱性を修正したバージョン74.0.3729.108がリリースされたと発表され、至急アップデートするよう呼びかけられています。

AUS便りからの所感等

- Chromeは通常自動更新が行われますが、無効になっていないか、またはタイミング上更新されていないという状況でないか、念のためバージョン情報を確認すると良いでしょう（「右上のアイコン→ヘルプ→Google Chromeについて」で確認可能、最新でなければ更新が開始されます）。

- ブラウザ側で脆弱性の対応が行われる前に攻撃を受ける可能性に対しては、アンチウイルスやUTMによる防御を万全に行うことが重要です。

- 今回発見された脆弱性はそれぞれのブラウザ固有のものであり、脆弱性を回避するという意味では、普段からFirefox等も含め複数のブラウザを適宜使い分けることも有用と言えます。


INTERNET Watch

Microsoft EdgeとIEにゼロデイ脆弱性、セッション情報の露出で個人情報など取得される恐れ

磯谷 智仁　2019年4月3日 19:19

ツイート リスト いいね！191 シェア B! 41 Pocket 1

ウェブブラウザーのMicrosoft EdgeおよびInternet Explorer（IE）に、セッション情報が露出する「同一生成元ポリシー違反」（CWE-346）の脆弱性があるとして、トレンドマイクロ株式会社が同社セキュリティブログで解説している。

同一生成元ポリシーが機能している場合は、不正なウェブサイトに埋め込まれたJavaScriptがクライアントのキャッシュに保存されたセッション情報にアクセスすることはできないが、この脆弱性が悪用された場合は同一生成元ポリシーの回避に成功し、本来アクセスが制限されているリソースにアクセスできるようになる。

この問題を発見したセキュリティリサーチャーのJames Lee氏は、各ウェブブラウザーの脆弱性を検証するための概念実証（PoC）サイト「pwning.click」を公開している。同ウェブサイトにアクセスすると、検索エンジン「Bing」にリダイレクトされるが、同一生成元ポリシーが適切に機能していれば、埋め込まれたJavaScriptはpwning.clickの情報のみを本来は表示する。