

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。

●中小企業のセキュリティ支援「サイバーセキュリティお助け隊」の実証実験開始

<https://cybersecurity-jp.com/news/31742>

<https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html>



このニュースをザックリ言うと…

- 6月4日（日本時間）、情報処理推進機構（IPA）より、**中小企業のサイバーセキュリティ対策支援を行う「サイバーセキュリティお助け隊」の実証事業**について発表されました。
- IPAでは、「サプライチェーン」を構成する中小企業のサイバーセキュリティ対策の強化について、**我が国の産業に対する世界の信頼に直結する重要な課題**であるとしています。
- 8地域15府県の中小企業を対象として、サイバーセキュリティに関する悩みや、対策のニーズ、サイバー攻撃被害の実態等を把握するとともに、サイバーインシデントが発生した際の支援体制の構築等に向けた実証を行うとしており、**IPAにて採択された8つのセキュリティ関連事業者**が実証に参加する中小企業へ支援策を行う予定です。

AUS便りからの所感等

- 大企業のみならず中小企業においてもサイバー攻撃を受ける可能性があることは言うまでもありませんが、攻撃者がターゲット企業を介し、そことやり取りを行っている企業へ、マルウェアの伝播を含めたさらなる攻撃を行うこと等に注目しているものと考えられます。
- 今回の実証事業の対象となる地域は限定的なものですが、その結果に基づいて実施地域が拡大され、最終的には**全国の中小企業におけるセキュリティ強度の底上げ**に貢献するよう期待したいものです。

Cyber Security セキュリティ.com

中小企業のセキュリティ支援「サイバーセキュリティお助け隊」の実証実験開始

2019.06.14

サイバーセキュリティお助け隊とは？

サイバーセキュリティお助け隊とは、セキュリティへのリソース配分が困難な中小企業に向けて、情報流出などに対応したセキュリティ体制の構築を手掛けるもの。

IPAにて採択された8つのセキュリティ関連事業者が、実証に参加する中小企業へ支援策を行う予定です。

- セキュリティ機器の配布・設置
- サイバー攻撃の実態や対策状況といった情報の収集
- サイバーセキュリティに関する相談受付および対応窓口の設置、事後対応支援
- 中小企業に適したサイバー保険のあり方の検討

説明会は2019年6月より、順次進む方針です。

参加 中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）/ IPA

IPA Better Life with IT 情報処理推進機構

中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）

最終更新日：2019年6月14日
 独立行政法人情報処理推進機構
 セキュリティセンター 企業部
 中小企業支援グループ

背景

IoTやAIといった技術により実現される「Society5.0」、「Connected Industries」では、データを介したつながりから、新たな付加価値が生み出されていくことが期待されます。一方で、企業間・産業界がつながることで、ネットワーク化されたサプライチェーン上に攻撃の起点が広く拡散していくことになり、悪意のある者にとって新たな攻撃の機会となるおそれがあります。

サイバー攻撃に対して地域の中堅企業でつなぐサプライチェーンを構成する企業です。

こうした状況を踏まえ、サイバーセキュリティお助け隊が、使いやすい支援体制の構築を支援します。

対象地域	実施者	事業説明会（予定）
岩手県 宮城県 福島県	株式会社デジタルハーツ	7月29日（月）午後 仙台市（TKPガーデンシティ仙台） 詳細▶
新潟県	東日本電信電話株式会社	6月中旬～下旬
長野県 群馬県 栃木県 茨城県	富士ゼロックス株式会社	調整中
神奈川県	SOMPOリスクマネジメント株式会社	6月14日（金）15:30-18:00 横浜市（横浜ジャンボ日本興業横浜ビル）
石川県	株式会社PEU	7月
愛知県	MS&ADインターリスク総研株式会社	6月19日（水）10:30-12:30/14:00-16:00 6月24日（月）10:30-12:30/14:00-16:00 名古屋市（TKPガーデンシティPREMIUM 名古屋ルーセントタワー） 詳細▶
大阪府 京都府 兵庫県	大阪商工会議所	7月5日（金）14:00-15:30 大阪市（大阪商工会議所 会議室） 詳細▶
広島県	株式会社日立製作所	7月24日（水）15:00-17:00 7月29日（月）15:00-17:00 広島市（広島商工会議所 会議室）

●Windowsではパスワードの定期的な再設定は不要…MSが改定へ

<https://japan.zdnet.com/article/35138170/>



このニュースをザックリ言うと…

- 5月23日(現地時間)、マイクロソフト(MS)より、Windows 10(およびWindows Server)のセキュリティベースラインにおいて、**「パスワードに期限を設定すべき」としていた推奨事項を削除する意向**が発表されました。
- 同社では「定期的なパスワードの失効はパスワード(またはハッシュ)が有効期間中に盗まれ不正な主体によって使用される場合に対する防御にしかならない。そもそもパスワードが盗まれなければ失効させる必要もない。また、パスワードが盗まれたことを示す証拠があればおそらく有効期限が来て失効するのを待つよりも直ちに行動する方が問題を解決するためには望ましい」等と説明しています。
- 一方で同社では、以前より**「パスワードは企業にとって不便であり、安全性が低く、コストが高い」と主張**しており、複数の形態の認証手段やバイオメトリクス(生体認証)に置き換えられるべきともしています。

AUS便りからの所感等

- ほんの数年前まで、パスワードは「定期的に変更すべき」という意見が強く、国内の多くのセキュリティ機関で推奨事項とされていましたが、頻繁な変更の要求に対しユーザが簡単なパスワードを設定してしまうという問題も指摘されていました。

- 特に2014年、複数のサイトで同じパスワードを設定していたユーザが連鎖的に不正ログインの被害を受ける事件が多発したことにより、パスワード管理に関するこれまでのセオリーの見直しが進み、**2018年には総務省やPマーク認定機関等も定期的な変更を推奨する方針から転換しています。**

- 多くの社内システムにおいては、依然IDとパスワードの入力によりログオンする形式をとっていると思われるが、その中でも、パスワードの管理等について改善を行える箇所はきっとあるはずですので、適宜見直しを行って頂ければ幸いです。



Windowsではパスワードの定期的な再設定は不要--MSがガイドラインの改定へ

Steve Ranger (ZDNet.com) 翻訳校正: 石橋 一郎 2019年06月11日 09時30分

パスワードの有効期限を設定することは、ユーザーアカウントを保護する方法としては時代遅れであり、有害無益だとさえ思えるかも知れない。30日か60日ごとにパスワードの変更を迫られることは、新しいパスワードをひねり出して覚えておかなければならないユーザーにとって頭痛の種である上に、セキュリティの向上にもほとんど役に立たない。

今ではMicrosoftもスタンスを変え、「Windows 10」と「Windows Server」のセキュリティベースラインに含まれていた、パスワードに期限を設定すべきであるという**推奨事項を削除することになった**。*ZDNetのLiam Tung記者が別の記事でも書いた通り、Microsoftは、新しいガイドラインのドラフトを公表する際、有効期限に関するポリシーを廃止する意向を明らかにした。

●フィッシング対策協議会、「フィッシングレポート」「フィッシング対策ガイドライン」2019年度版を公開

https://www.antiphishing.jp/report/wg/phishing_report2019.html

<https://www.antiphishing.jp/news/info/guideline2019.html>



このニュースをザックリ言うと…

- 5月29日(日本時間)、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、フィッシングの被害状況、フィッシングの攻撃技術・手法等を取りまとめた **「フィッシングレポート」および「フィッシング対策ガイドライン」の2019年度版**が公開されました。

- レポートによれば、フィッシング届出件数は**2018年3月以降急激に上昇して以降比較的高い水準で推移**しており、フィッシングサイトのURL件数およびブランドを悪用された企業の件数も増加傾向にある、等としています。

- ガイドラインについては事業者向けと利用者向けがそれぞれ用意されており、昨今のフィッシング動向を反映して内容が改訂されています。

AUS便りからの所感等

- ガイドラインでは、利用者として「フィッシングに引っかからないための対策」だけでなく、Webサイト運営者として「被害の発生を抑制するための対策」「被害の発生を迅速に検知するための対策」および「被害が発生してしまった際の対策」等にも言及されています。

- 例えば、「被害の発生を抑制するための対策」において「利用者が正規メールとフィッシングメールを判別可能とする」ために推奨されている対策だけでも多くの項目が挙げられています。

- ともあれ、ガイドラインを一通り読み込み、実施可能な対策から順次実行を検討していくこと、また対策の実施にあたっては、**適宜ホスティングやクラウドサービスと契約することも視野に入れるのが良い**でしょう。



資料公開: フィッシングレポート 2019 の掲載について

2019年05月29日

フィッシング対策協議会の皆様、関係団体・関係グループは、フィッシングの被害状況、フィッシングの攻撃技術・手法などを取りまとめた「フィッシングレポート 2019」を公開しました。

※レポートの主な内容は以下のとおりです。

資料公開: フィッシング対策ガイドラインの改訂のお知らせ

2019年05月29日

フィッシング対策協議会の皆様、関係団体・関係グループは、2018年度のフィッシング動向や新しい攻撃技術等をまとめ、事業者向けと利用者向けのフィッシング対策ガイドラインをそれぞれ改訂し、2019年度版として公開しました。

詳細は以下 URL をご覧ください。