

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。

●消費増税に便乗、三井住友銀行騙るフィッシングに注意

<https://internet.watch.impress.co.jp/docs/news/1209504.html>
https://www.antiphishing.jp/news/alert/smbc_20190926.html
<https://www.smbc.co.jp/security/attention/index23.html>



このニュースをザックリ言うと…

- 9月26日(日本時間)、フィッシング対策協議会より、**三井住友銀行を騙るフィッシングメールおよびSMSが確認された**として注意喚起がなされています。

- フィッシングメールは、件名が「**重要：お客様の【三井住友銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定してください。**」等、また文面にて「**消費税率引き上げに伴うSMBCダイレクトの各種手数料改定**」を名目としたもの等が例に挙げられており、同銀行のネットバンキングサービス「SMBCダイレクト」のログイン画面に巧妙に似せた偽サイトにリンクしています。

- 協議会では、このようなフィッシングサイトにて、**店番号、口座番号、契約者番号、第一暗証、電話番号などの情報を絶対に入力しない**よう呼び掛けています。

AUS便りからの所感等

- 大きなイベントにはそれ便乗したフィッシング等のサイバー犯罪が付きものですが、それはオリンピックやラグビーワールドカップといったスポーツイベントに限らず、国民の多くが興味を持つ政治・経済的な出来事でも同様と言えます。

- SMBCダイレクトでは実際に税率引き上げによる手数料改定を行う予定ですが、そういった情報の確認時に偽のサイトにアクセスしないよう、**通常使用するサービスのサイトはブラウザのブックマークに予め登録しておくこと**、また**不審なメール・SMSについてネット上の報告がないか確認**する習性をつけ、かつ**ブラウザ・アンチウイルスおよびUTMのセキュリティ機能による防御**を確実に行うことが肝要です。

- なお、本物のSMBCダイレクトのログインページでは**EV-SSL証明書**を使用しているものの、**Chromeは現バージョン77でアドレスバーに直接組織名を表示しないよう変更**されており、**Firefoxも次期バージョン70で同様の変更を行う予定**となっている(<https://gigazine.net/news/20190813-extended-validation-certificate/> ※鍵アイコンをクリックすれば組織名は表示されます)ため、これによるサイトの確認には依存しないよう注意が必要です。

三井住友銀行

SMBCダイレクトへのログインや電話番号の入力を求める不審なサイトへ誘導するショートメッセージにご注意ください

三井カード/通帳連絡 インターネット 振り込み/引き その他

このようなケースが発生しています。

SMBCダイレクトのログイン画面に似せたURLにアクセスさせ、ログインや本人確認情報の入力を誘導する不審なショートメッセージが確認されています。
例) お客様の【三井住友銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定:htp://xxxx.xx
銀行の口座番号や暗証番号、本人確認情報が第三者に知られると、インターネット/バンキングで不正入金される被害につながる恐れがありますので、十分ご注意ください。

手口の特徴

- 当行を騙ってURLにアクセスさせるショートメッセージを送る。
例) お客様の【三井住友銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定:htp://xxxx.xx
- 当行を装い、SMBCダイレクトのログイン画面に似せた画面を表示し、口座番号や第一暗証を入力させる。
- 本人確認と称し、電話番号等の本人確認情報を入力させる。
- 入手した口座番号や第一暗証、電話番号等の本人確認情報を使用し、不正送金する。

フィッシング対策協議会 Council of Anti-Phishing Japan

三井住友銀行をかたるフィッシング (2019/09/26)

概要

三井住友銀行をかたるフィッシングの報告を受けています。

メールの件名

【重要】お客様の【三井住友銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定してください。
【重要】「三井住友銀行の口座」カード・通帳一時利用停止、再開のお手続きの設定してください。

(上記以外の件名が使われている可能性があります)

詳細内容

三井住友銀行をかたるフィッシングサイトへ誘導するメールおよびショートメッセージ (SMS) の報告を受けています。

1. 2019/09/26 16:00 現在フィッシングサイトは標榜中であり、JPCERT/CC にサイト懸念のための調査を依頼中であります。類似のフィッシングサイトが公開される可能性がありますので、引き続きご注意ください。
2. このようなフィッシングサイトにて、店番号、口座番号、契約者番号、第一暗証、電話番号などの情報を絶対に入力しないように、ご注意ください。
3. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

【参考情報】

SMBCダイレクトへのログインや電話番号の入力を求める不審なサイトへ誘導するショートメッセージにご注意ください
<https://www.smbc.co.jp/security/attention/index23.html>

緊急情報

2019年09月26日

メール本文



サイト



●Windows 7の有償延長サポート、中小企業にも提供へ

<https://japan.zdnet.com/article/35143400/>
<https://gigazine.net/news/20191003-microsoft-windows-7-extended-update-support/>
<https://www.microsoft.com/microsoft-365/partners/news/article/announcing-paid-windows-7-extended-security-updates>



このニュースをザックリ言うと…

- 10月1日(現地時間)、マイクロソフト(以下、MS)より、Windows 7(ProfessionalおよびEnterprise)に対し2020年1月の一般サポート終了後に提供する有償の延長サポート「Windows 7 Extended Security Updates(ESU)」について、**提供範囲を中小企業にも拡大**することが発表されました。
- 昨年9月にESUが発表された当初は、ボリュームライセンス契約に対してのみ提供される予定でした(AUS便り2018/9/18号参照)が、今回その制限が解除され、**Windows 7 ProfessionalないしEnterpriseであれば企業の規模に拘らずMSのクラウドソリューションパートナーを通じてESUの購入が可能になる**とのこと。
- ESUは2023年1月まで提供され、**課金はデバイス単位、かつ料金は毎年引き上げられる**こととなります(例えばProにおける提供料金は1年目が50ドル、2年目が100ドル、3年目が200ドルとなる模様です)。

AUS便りからの所感等

- MSは1月に「2020年の一般サポート終了時点で、Windows 7が稼働するPCが約1,750万台残存する」と予測しており(<https://japan.zdnet.com/article/35131276/>)、今回のESUに関する方針転換はこういった状況を鑑みてのものと考えられます。
- それでも、特に2023年まで利用した場合にかかる料金を鑑みて、単純に「お金を払えば2020年以降もWindows 7を使い続けられる」とすべきなのかという問題はあり、やはり基本的には**Windows 10へ移行することを前提とし、早急な移行計画をとるべき**でしょう。
- もちろん、ESUを購入せず、**パッチが提供されない状態のWindows 7あるいはそれ以前のOSを無計画にネットワークに接続するのはもってのほかであり、マルウェアへの感染の可能性、あるいは社内外へマルウェアの拡散や不正アクセスを発生させてしまう可能性を考慮し、適切な隔離等を行うことが重要**です。

Microsoftは米国時間10月1日、「Windows 7 Extended Security Updates」(ESU)をさらなる顧客に提供すると発表した。ボリュームライセンス契約のある大手企業のみではなく、規模にかかわらずすべての企業に提供するという。

2020年1月14日までに「Windows 7」からの移行準備が整わない中小企業(SMB)も、2019年12月1日からESUを購入できるようになる。

Microsoftは、2020年1月14日にWindows 7の無償サポート(とセキュリティ更新プログラム)を終了する。これら中小企業も、認定クラウドソリューションプロバイダー(CSP)と契約することで最長3年間ESUを手でできるとMicrosoftは説明している。

●個人情報の事故、「メール誤送信」「ノートPCの盗難」などに注意…JIPDEC調べ

- <https://webtan.impress.co.jp/n/2019/09/25/34033>
- <https://privacymark.jp/news/other/2019/0918.html>



このニュースをザックリ言うと…

- 9月18日(日本時間)、日本情報経済社会推進協会(JIPDEC)より、「個人情報の取扱いにおける事故報告集計結果」(2018年度)が発表されました。
- 同協会が運営するプライバシーマークが付与されている16,275事業者のうち**912事業者から、2,323件の個人情報の取扱いにおける事故が報告されており**、原因別では「**誤送付**」が1,345件(57.9%)、次いで「**紛失**」478件(20.6%)、「**その他漏えい**」330件(14.2%)、となっています。
- また「誤送付」のより詳しい原因で最も多いのが「**メール誤送信**」586件(25.2%)とされた他、「**紛失**」および「**盗難**」にあった媒体別では「**書類**」274件(51.5%)が過半数を占める一方で「**ノートPC・モバイル機器**」が2017年度の32件から2018年度には76件と増加しているとのこと。

AUS便りからの所感等

- 「メール誤送信」および「ノートPC紛失」についてAUS便りで取り上げた例としては、「大学病院、メール誤送信により患者情報3,275人分流出の可能性」(2019/8/19号)、「顧客情報67,000件超を記録したノートパソコンを紛失」(2019/9/17号)等が挙げられます。
- うち後者については、遠隔でPCを使用できなくするソリューションが導入されており、こういった「**インシデント発生時にも可能な限りの流出の可能性を抑制する**」防御策をシステム側で導入することを検討することにより、**単に利用する人間に対し「ルールを守らせる」「注意してもらう」ことに依存しない情報流出対策**をとって頂ければ幸いです。

2018年度中にプライバシーマーク制度運営機構(JIP-PMK500「プライバシーマーク付与に関する規約」第11条)に基づき、プライバシーマーク付与事業者の皆さまより当協会および審査機関にご報告いただいた個人情報の取扱いにおける事故について取りまとめました。

皆さまのご協力に感謝するとともに、前年度までの報告資料と合わせ、個人情報の取扱いにおける事故の発生防止・再発防止等に活用いただければ幸いです。

※本資料よりタイトルを「個人情報の取扱いにおける事故報告集計結果」に変更しました。

概要

2018年度の報告件数

1. 2018年度は、912の付与事業者より2,323件の事故報告があり、報告事業者数、事故報告件数ともに前年度とほぼ同じでしたが(2017年度:報告事業者数911事業者、事故報告件数2,399件)。

2. 2018年度末時点の付与事業者数に占める事故報告事業者の割合は5.6%であり、これは前年度と比較