— AUS（アルテミス・ユーザ・サポート）便り 2018/11/19号 —
https://www.artemis-jp.com

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。

●Twitterで公式アカウントの乗っ取り相次ぐ…ビットコイン詐欺に悪用

https://www.nikkei.com/article/DGXMZO37463220X01C18A1000000/
http://www.itmedia.co.jp/news/articles/1811/15/news030.html

このニュースをザックリ言うと･･･

- 11月5日（日本時間）頃より、Twitterで大手企業等の公式アカウントが乗っ取られ、ビットコインに関する詐欺に悪用されるケースが複数発生しています。

- 例えば、米国の出版社Pantheon Books社のアカウントは、アカウント名とアイコンが米Teslaのイーロン・マスクCEOのものに改変され、「ビットコイン0.1BTCを指定のアドレスに送金すれば2BTCを送り返す」等と投稿しています。

- また国内でも、朝日新聞新潟総局のアカウントが乗っ取られて上記Pantheon Booksのアカウントに不審なリプライをしたケースや、講談社「コミックDAYS」の公式アカウントが米トランプ大統領をかたるアイコン・バナーに改変されるケースが発生しています。

AUS便りからの所感等

- 乗っ取られたアカウントは、いずれもTwitterから公式アカウントであることを示す「認証済みバッジ」が付与されたものであり、またなりすまし後も本物のアカウントのツイートをリツイート（RT）する等してユーザをだまそうとした形跡があります。

- 今のところアカウント乗っ取り後の行動は全てワンパターンであり、手口を知っておくことは詐欺にだまされないための防衛に有効ですが、攻撃者が今後やり方を変える可能性は当然考えられます。

- SNSアカウントの乗っ取りは、必ずしも組織のネットワークへの侵入や個人情報の流出に繋がるものではありませんが、悪用の用途次第ではブランド等の毀損を引き起こすことも考えられます。

- SNSアカウント（およびアカウントに登録したメールアドレス）のパスワードは推測されにくい複雑なものとすること、二段階認証を設定すること、連携するアプリは必要最低限とすること、などが乗っ取りや悪用のリスクを抑止するために重要です。


日本経済新聞

朝日新聞のTwitter乗っ取り、ビットコイン詐欺に利用

ネット・IT　科学&新技術　BP速報

2018/11/7 11:56

保存　共有　印刷　その他

朝日新聞社の新
乗っ取られてい
の広報担当が6日
ス「archive.to

新潟総局のTwitterアカウントから、「I sent 1 BTC and got back 10 BTC!（1ビットコインを送ったら10ビットコインを送り返してもらえた）」「THANK YOU」「＋10BTC」といった不自然な書き込みがあったことを確認できる。これらの書き込みの一部は、「PantheonBooks」というアカウント宛てになっていた。

PantheonBooksは米出版社パンテオン・ブックスの公式アカウント。海外の報道によればこのアカウントは第三者に乗っ取られ、米テスラのイーロン・マスク最高経営責任者（CEO）を名乗っていたとされる。このアカウントからは「0.1～3ビットコインを送れば、10倍のビットコインを送り返す」という趣旨のコメントと、ビットコインアドレスが書き込まれていたという。新潟総局のTwitterアカウントは、ビットコイン詐欺の宣伝に利用されたとみられる。

朝日新聞新潟総局 @asahi_niigata

Replying to @PantheonBooks

I sent 1 BTC and got back 10 BTC!

2:26 AM - 5 Nov 2018

1 Retweet　3 Likes

朝日新聞新潟総局 @asahi_niigata · 4h

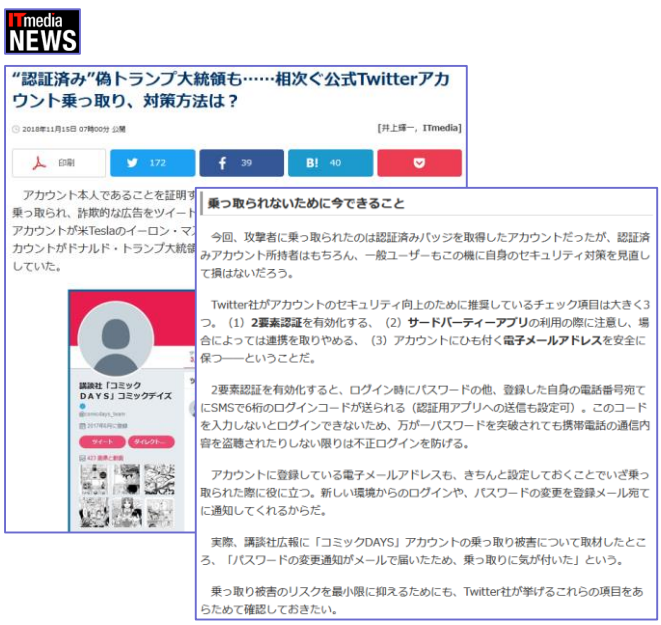
Replying to @asahi_niigata @PantheonBooks

THANK YOU!!!!!!!!!!!!!!!!!!!!

朝日新聞新潟総局 @asahi_niigata · 4h

+10 BTC!!!!!!

画像の拡大


ITmedia NEWS

“認証済み”偽トランプ大統領も……相次ぐ公式Twitterアカウント乗っ取り、対策方法は？

2018年11月15日 07時00分 公開　[井上輝一, ITmedia]

印刷　172　39　B!　40

アカウント本人であることを証明す
乗っ取られ、詐欺的な広告をツイート
アカウントが米Teslaのイーロン・マ
カウントがドナルド・トランプ大統領
していた。

乗っ取られないために今できること

今回、攻撃者に乗っ取られたのは認証済みバッジを取得したアカウントだったが、認証済みアカウント所持者はもちろん、一般ユーザーもこの機に自身のセキュリティ対策を見直して損はないだろう。

Twitter社がアカウントのセキュリティ向上のために推奨しているチェック項目は大きく3つ。（1）**2要素認証**を有効化する、（2）**サードパーティーアプリ**の利用の際に注意し、場合によっては連携を取りやめる、（3）アカウントにひも付く**電子メールアドレス**を安全に保つ――ということだ。

2要素認証を有効化すると、ログイン時にパスワードの他、登録した自身の電話番号宛てにSMSで6桁のログインコードが送られる（認証用アプリへの送信も設定可）。このコードを入力しないとログインできないため、万が一パスワードを突破されても携帯電話の通信内容を盗聴されたりしない限りは不正ログインを防げる。

アカウントに登録している電子メールアドレスも、きちんと設定しておくことでいざ乗っ取られた際に役に立つ。新しい環境からのログインや、パスワードの変更を登録メール宛てに通知してくれるからだ。

実際、講談社広報に「コミックDAYS」アカウントの乗っ取り被害について取材したところ、「パスワードの変更通知がメールで届いたため、乗っ取りに気が付いた」という。

乗っ取り被害のリスクを最小限に抑えるためにも、Twitter社が挙げるこれらの項目をあらためて確認しておきたい。

●気象庁の「津波警報発表」を装う迷惑メールに注意

https://www.jma.go.jp/jma/press/1811/08c/WARNmail.html

このニュースをザックリ言うと・・・

- 11月8日（日本時間）、気象庁より、同庁発表の警報等を装った迷惑メールが確認されたとして注意喚起が出されています。

- 発表で挙げられた例では、件名が「津波警報発表」、本文が「10時55分頃、地震がありました。3メートルを超える津波警報を発表しました。…」となっており、詳細情報のページへのリンクとして「.jma-go.jp」というドメインを含む、マルウェアがダウンロードされる不審なURLを記載したものとなっています。

- 同庁では、政府機関は原則として「.go.jp」で終わる名前のドメインを使っており、まぎらわしいドメインを使用したURLにはアクセスしないよう呼び掛けています。

AUS便りからの所感等

- 災害の警報・速報を装ったマルウェアメールは、つい先日も10月下旬に「エリアメール」をかたる不審なSNSが確認されたばかりです（AUS便り 2018/11/05号参照）。

- うっかりフィッシングサイトにアクセスしたり、マルウェアをダウンロードしたりした場合の被害を食い止められるよう、Web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いましょう。


国土交通省 気象庁

気象庁発表の警報等を装った迷惑メールにご注意下さい

報道発表日

平成３０年１１月８日

概要

最近、気象庁発表の警報等を装った迷惑メールが届いたという情報が寄せられております。心当たりのないアドレスから届いたメールに不審なリンクがある場合はアクセスしないようご注意ください。

本文

気象庁を含め、政府機関は原則として「.go.jp」で終わる名前のドメインを使っています。「jma-go.jp」など、正規の政府機関とまぎらわしいドメインを使用したURLは、気象庁とはまったく関係がありません。アクセスしないでください。
もし、このような迷惑メールによって金銭的な被害などを受けた場合は、速やかにお近くの警察署に被害届を出すようお願いいたします。

- 気象庁では他にも、事業者のサービス等でメールを受け取っている場合に、メールの配信元アドレスや文面等をあらかじめ各事業者のWebサイト等で確認するようにとも呼びかけており、一方で上記で例に挙げられたメールのように、発信元メールアドレス（From:）として本物のドメイン使っていることも珍しくないことには注意が必要です。

●Adobe、Flash Player・Acrobat・Reader等のセキュリティアップデート公開

http://www.itmedia.co.jp/news/articles/1811/14/news087.html

このニュースをザックリ言うと・・・

- 11月14日（日本時間）、Adobe社より「Flash Player」「Acrobat/Acrobat DC」「Acrobat Reader/Reader DC」および「Photoshop CC」のセキュリティアップデートがリリースされました。

- リリースされたバージョンはFlash Playerが31.0.0.148、AcrobatおよびReaderが2019.008.20081（DC 連続トラック）・2017.011.30106（Classic 2017）・2015.006.30457（Classic 2015）、Photoshop CCが19.1.7および20.0となっており、それぞれ脆弱性が修正されています。

- AcrobatおよびReaderの脆弱性「CVE-2018-15979」についてはシングルサインオン用のパスワードが奪取される可能性があるとされ、既に攻撃コードが出回っていることから、特にアップデートの優先度が高くなっています。

AUS便りからの所感等

- 同日にはマイクロソフトからも月例のセキュリティパッチがリリースされており、Edge向けFlash Playerについても最新版が提供されています。

- PDFリーダーについてはAcrobat Readerでなくともwebブラウザ各種にリーダー機能が備わっており、他にも代替となるリーダーソフトもありますが、そういったAdobe以外のリーダーソフトにおいても脆弱性が報告されることがあります（AUS便り 2018/10/22号参照）ので、OSからあらゆるソフトウェアに至るまで、必ずアップデートを確認し、最新の状態に保つようにしましょう。


ITmedia NEWS

Adobe、Flash Playerなどの更新版公開
Acrobat／Readerは優先度高

2018年11月14日 12時15分 公開 [鈴木聖子, ITmedia]

印刷 30 4 B! 0

米Adobe Systemsは11月13日、Flash PlayerとAcrobatおよびReader、Photoshop CCのセキュリティ情報を公開し、それぞれ脆弱性を修正する更新版をリリースしたことを明らかにした。

Adobeのセキュリティ情報によると、Flash Playerの更新版では、1件の情報流出の脆弱性が修正された。優先度は「2」、緊急度は3段階で上から2番目の「重要」に分類している。

更新版はWindows、macOS、Linux、Chrome OS向けにリリースされ、いずれもFlash Playerのバージョン31.0.0.148で脆弱性が修正されている。

AcrobatとReaderの更新はWindowsが対象で、優先度は「1」と最も高い。修正された情報流出の脆弱性は「重要」の分類だが、既にコンセプト実証コードが公開されているといい、悪用されればユーザーのハッシュ化されたNTLM認証のパスワードが流出する恐れがある。