— AUS（アルテミス・ユーザ・サポート）便り 2018/10/15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。

●「サイバー空間をめぐる脅威の情勢」、警視庁が発表

https://this.kiji.is/422167154973312097
http://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/info_security.files/graph.pdf

このニュースをザックリ言うと･･･

- 10月5日（日本時間）、警視庁サイバーセキュリティ対策本部より、「平成30年上半期におけるサイバー空間をめぐる脅威の情勢について」と題した資料が発表されました。

- これは都内の「サイバー犯罪の相談状況」「インターネットバンキングの不正送金事犯の状況」「サイバー犯罪の検挙状況」、および全国の「サイバー攻撃の情勢等」についてまとめられたものです。

- 標的型攻撃メール(※)の件数は2,578件で、前年同期に比べ1,989件増加としており、その約87%にあたる2,246件が「ばらまき型」とのことです。

※警察発表における「標的型攻撃メール」とは、「①迷惑メールと異なり、業務等に関連した内容を装うなど、一見すると正当なメールと区別がつきにくい」「②市販のウイルス対策ソフトで検知できない不正プログラムに感染させようとする」との特徴があるものを指しています。

- サイバー犯罪の相談状況については、相談受理件数の総数が5,623件と前年同期から1,757件減少しており、最も多いのは「詐欺・悪質商法」に関する2,414件（全体の42.9%）となっています。

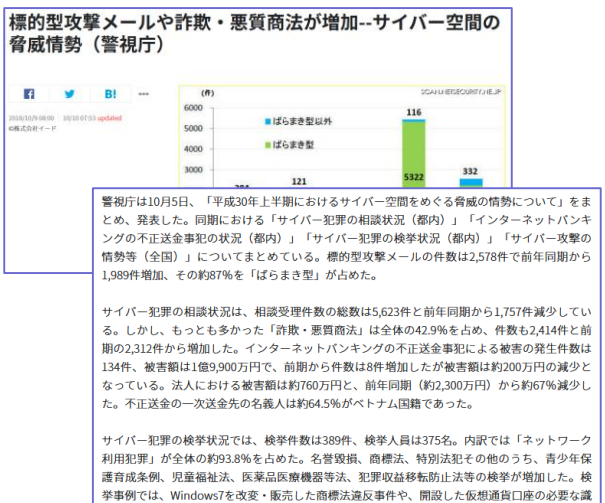
AUS便りからの所感等

- 前述したサイバー犯罪の相談受理件数や、インターネットバンキングの不正送金事犯の発生件数や被害額については、平成28年の結果から概ね減少が続いており、警察や金融機関による監視や決済確認手続き等の徹底が功を奏しているものとされています。

- 一方で標的型攻撃メールの件数については、前年下半期が589件と近年では落ち着いていた一方、同下半期に5,438件と急増、そこから今年上半期の2,578件に半減と乱高下しており、今年下半期やそれ以降の実績がどうなるかは未知数です。

- ともあれ警察やセキュリティ機関からの警告に注視し、あるいはこれらへ適宜相談を行うことを引き続き心がけていき、またアンチウイルス・UTMその他による防御を確実に行うことにより、サイバー攻撃への備えを十分に行って頂ければ幸いです。

ScanNetSecurity



警視庁は10月5日、「平成30年上半期におけるサイバー空間をめぐる脅威の情勢について」をまとめ、発表した。同期における「サイバー犯罪の相談状況（都内）」「インターネットバンキングの不正送金事犯の状況（都内）」「サイバー犯罪の検挙状況（都内）」「サイバー攻撃の情勢等（全国）」についてまとめている。標的型攻撃メールの件数は2,578件で前年同期から1,989件増加、その約87%を「ばらまき型」が占めた。

サイバー犯罪の相談状況は、相談受理件数の総数は5,623件と前年同期から1,757件減少している。しかし、もっとも多かった「詐欺・悪質商法」は全体の42.9%を占め、件数も2,414件と前期の2,312件から増加した。インターネットバンキングの不正送金事犯による被害の発生件数は134件、被害額は1億9,900万円で、前期から件数は8件増加したが被害額は約200万円の減少となっている。法人における被害額は約760万円と、前年同期（約2,300万円）から約67%減少した。不正送金の一次送金先の名義人は約64.5%がベトナム国籍であった。

サイバー犯罪の検挙状況では、検挙件数は389件、検挙人員は375名。内訳では「ネットワーク利用犯罪」が全体の約93.8%を占めた。名誉毀損、商標法、特別法犯その他のうち、青少年保護育成条例、児童福祉法、医薬品医療機器等法、犯罪収益移転防止法等の検挙が増加した。検挙事例では、Windows7を改変・販売した商標法違反事件や、開設した仮想通貨口座の必要な識別情報を他人に提供した事件、対面取引による多額の仮想通貨詐欺事件などを挙げている。

警視庁

●聖教新聞社サイト改ざん…2,481人分のカード番号窃取、個人情報のべ18万人分流出も

https://www.nikkei.com/article/DGXMZO36403810121021018000000/

このニュースをザックリ言うと・・・

- 10月9日（日本時間）、聖教新聞社の通販サイト「SOKAオンラインストア」が不正アクセスを受け、クレジットカード情報・個人情報を不正に取得されていたことが同社およびサイト運営を受託されていたトランスコスモス社より発表されました。

- 発表によれば、7月30日～8月24日の間、同サイトのサーバ上のプログラムが改ざんされ、商品購入時に偽のカード決済画面が表示される状態になっていたとのことで、偽画面に入力された2,481人分のクレジットカード情報（番号、名義、有効期限、セキュリティコード）が被害を受けたとされています。

- これ以外にも、同サイト開設以降に登録していた98,852人、および登録せずに商品購入あるいはお問合せを行った82,848人分の個人情報（氏名、住所、電話番号、メールアドレス他。カード情報は含まず）も不正に取得されていた可能性があるとされています。

AUS便りからの所感等


日本経済新聞

聖教新聞社サイト改ざん、2481人分のカード番号窃取

ネット・IT　科学&新技術　BP速報

2018/10/12 12:00

保存　共有　印刷　その他

日経XTECH

聖教新聞社とトランスコスモスは、トランスコスモスが運営を受託している聖教新聞社の通販サイト「SOKAオンラインストア」が不正アクセスを受け、個人情報を不正に取得されたと2018年10月10日までに発表した。不正取得された可能性があるのは、2481人分のクレジットカード番号・セキュリティコードなどと、約18万人分の氏名・住所・生年月日・電話番号など。

- クレジットカード情報やアカウント情報を詐取する偽のフォームを表示する手口は様々ですが、今回のように実際のサイトが不正アクセスを受けてしまうケースは、ユーザから確実に情報を詐取できる可能性がより高いものであり、最も厄介なものと考えられます。

- 特に今回は、偽画面でのカード情報の入力時には一旦エラーが表示され、本物の決済画面に改めて誘導されるという挙動になっていたとのことで、ユーザ側で自衛策をとることは非常に難しいものであったと考えられます。

- 不正なフォームの埋め込み等を目的としたWebサイトの改ざんについては、不正アクセスの発生といった方面の監視だけでなく、改ざんがされたかどうか等を検知するシステムの導入もまた重要です。

●「Google Chrome 70」「Firefox 63」でSymantec発行のSSL証明書が全て無効に

https://forest.watch.impress.co.jp/docs/news/1136278.html

このニュースをザックリ言うと・・・

- 10月16日（日本時間）リリースの「Google Chrome 70」および同23日リリースの「Firefox 63」において、Symantec社から発行されている各ブランド（Symantec・Verisign・Geotrust・Thawte・RapidSSL）のSSL証明書が無効化されるようになり、これらを使用しているサイトへのアクセスは「信頼されない証明書を使っている」と警告が出てブロックされるようになるとのことです（ページの表示にはブロックを解除する設定が必要です）。

- 既に今年4月リリースの「Chrome 66」と5月リリースの「Firefox 60」では、2016年6月1日以前に発行されたものについては「信頼されない」と表示されるようになっています。

- なお、前述のブランドの証明書のうち、Digicert社から2017年12月以降に発行されているものは無効化の影響を受けません。

AUS便りからの所感等


窓の杜
WINDOWS FOREST

「Firefox 63」でSymantec発行のTLS証明書が無効に ～トップ100万サイトの3.5%に影響

正式版は10月23日リリースの予定

樽井 秀人　2018年8月2日 16:57

10月23日（米国時間）にリリースされる予定の「Firefox 63」では、SymantecをルートとするTLS証明書がすべて信頼されなくなる。公式ブログ"Mozilla Security Blog"によると、トップ100万のWebサイトの内3.5%に影響があるという。

なお、「Google Chrome」では「Firefox 63」と同時期にリリースされる「Google Chrome 70」でSymantec証明書に対する信頼が完全に削除される予定。

- この措置は、2017年6月にGoogle社がSymantec社によるSSL証明書の発行手続きに問題があると指摘し、Chromeにおいて同社発行の証明書を段階的に無効化することを発表したのがきっかけです。

- Symantec社のSSL証明書発行事業は現在Digicert社に移管されており、多くの場合、問題となるケースについては無償での再発行が可能とのことです。

- Chrome 70においては他にも「HTTPでアクセスしたページ上でフォームに入力しようとした場合、アドレスバーに警告が出る」ようになっており、今後も将来のバージョンでブラウザ上の表示に新たに何らかの警告が出る仕様が追加されることが考えられ、警告が出てしまう事態を回避することを考慮するのであれば、随時の情報収集やベータ版をインストールしての表示確認等も担当者にとっては重要となってくるでしょう。