“この会報は、「テロ対策ネットワーク岐阜」事務局より定期的に発行しています”

テロ対策ネットワーク岐阜通信

CTNG

本号では、最近発生した主なテロ事件と、皆様の身の周りでも起きるおそれのある、サイバーセキュリティ上の脅威について説明していきます。

No.7　平成31年4月

最近発生した海外の主なテロ事件

2018/11/9	オーストラリア	オーストラリア南東部のメルボルンで、男が、乗り付けたピックアップを炎上させ、通行人を襲撃、１人が死亡、２人が負傷。
2018/11/16	フィリピン	フィリピン南部で、ISIL に忠誠を誓うグループが国軍を襲撃、兵士５人が死亡、23 人が負傷。
2018/11/23	パキスタン	パキスタン北西部の市場で、自爆テロが発生、少なくとも 31 人が死亡、51 人が負傷。
2018/12/11	フランス	フランス東部ストラスブールのクリスマスマーケット付近で、男が銃と刃物で、通行人を襲撃し、５人が死亡、12 人が負傷した。
2018/12/31	フィリピン	フィリピン南部ミンダナオ島で、ショッピングモール入り口付近に設置された爆弾が爆発２人が死亡、34 人が負傷。
2019/1/27	フィリピン	フィリピン南部にあるカトリック教会で、外国人の男女が相次いで自爆、23 人が死亡、95 人が負傷。
2019/1/29	パキスタン	パキスタン南西部で、警察署に対する自爆及び襲撃テロが発生、９人が死亡、21 人が負傷。

国内でも、原宿の竹下通りで車両を暴走させた男が逮捕されています。

男は、「明治神宮で高圧洗浄機を使い灯油を噴射しようとしたが失敗した」と述べており、無差別殺傷事件を起こそうとしたことが明らかとなっています。

皆様も、身の回りで

○　誰の物か分からない鞄が隠すように置いてある

○　多くの人が集まる場所で、周囲をうかがいながら何度も行ったり来たりしている

○　乗車したまま長時間駐車している

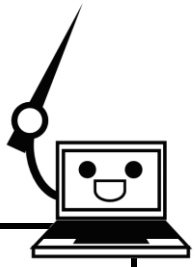
など、「あれ、おかしいな？」と思うことがあれば、すぐに 110 番通報してください。

サイバーセキュリティ上の脅威について

本年１月 30 日、独立行政法人情報処理推進機構（IPA）が、「情報セキュリティ 10 大脅威 2019」を発表しました。

これは、2018 年に発生した社会的反響が大きかったと考えられる情報セキュリティに関連する事案から、「個人」と「組織」の異なる視点で選出・決定されたものです。

「情報セキュリティ 10 大脅威 2019」



	個人	組織
1	クレジットカード情報の不正利用	**標的型攻撃による被害**
2	フィッシングによる個人情報の詐取	**ビジネスメール詐欺による被害**
3	不正アプリによるスマートフォン利用者の被害	**ランサムウェアによる被害**
4	メールや SNS を使った脅迫・詐欺の手口による金銭要求	サプライチェーン(※)の弱点を悪用した攻撃の高まり
5	ネット上の誹謗・中傷・デマ	内部不正による情報漏えい
6	偽警告によるインターネット詐欺	サービス妨害攻撃によるサービスの停止
7	インターネットバンキングの不正利用	インターネットサービスからの個人情報の詐取
8	インターネットサービスへの不正ログイン	IoT 機器の脆弱性の顕在化
9	ランサムウェアによる被害	脆弱性対策情報の公開に伴う悪用増加
10	IoT 機器の不適切な管理	不注意による情報漏えい

（出典：IPA プレスリリース http://www.ipa.go.jp/securitey/vuln/10threats2019.html）

(※)サプライチェーンとは、原材料や部品の調達、製造、在庫管理、物流、販売までの一連の商品流通及び流通に関わる複数の組織群を指します。

このうち、組織編で 1～3 位にランクインした 3 つの脅威についてご説明いたします。

１　標的型（メール）攻撃

標的型（メール）攻撃は、

①　**不正なプログラムに感染させる目的**で

②　**業務に関連した電子メールを装い、市販のウイルス対策ソフトで検知できない、不正なプログラムを添付した電子メールを送信**

③　**受信したコンピュータを不正プログラムに感染させる**

攻撃です。

標的型攻撃は、**Microsoft Office の文書ファイルを悪用したもの**が多く観測されています。

例えば、「.csv」、「.wiz」、「.iqy」、「.slk」等、Excel や Word に関連付けされたファイルを開くと警告画面が表示されます。

その際に「**～を有効にする**」等、何らかの命令を許可する操作を選択すると、ウイルスに感染するおそれがあります。

昨年、警察庁が確認した「標的型メール攻撃」は、過去最多の 6740 件にのぼるなど、日本の企業や組織の情報が狙われています。

【実際の事例①】オリンピックに便乗した標準型攻撃

昨年９月、「東京 2020 夏季オリンピックへの無料航空券をお届けします」等とうたった偽のメールが確認されました。

○　**添付ファイルの確認**

○　**メールに記載したリンクをクリックし、リンク先の偽のサイトにアクセス**

することにより、リンク先の不正なサイト又は添付されたファイルを通じて、不正なプログラムがダウンロードされ、最終的に受信者の情報が盗み取られるおそれがあるとのことです。

２　ビジネスメール詐欺（BEC　Business Email Compromise）

ビジネスメール詐欺とは、**海外の取引先や自社の経営者層等になりすまし、偽の電子メールを送信、入金を促す詐欺**のことです。

当初は、主に海外の組織が被害にあっていましたが、ここ数年で国内企業でも被害が確認されはじめ、昨年７月には、**日本語のビジネスメール詐欺**の事例も確認されました。

【実際の事例②】

大手会社に、支払先である海外の会社担当者になりすまし、「料金振込先の口座が変更された」と記した偽の請求メールが届きました。

このメールは、

- ○　正規取引とのやり取りに割り込む形で届く※
- ○　正規取引先のメールアドレスと酷似している
- ○　偽の請求書が本物と酷似、担当者の氏名も同じ

であったため、担当者が気づかず、指示通りに指定口座に振り込んでしまい、数日後、全額が引き出され回収不能になってしまいました。

※　本事案では、実際の取引先から請求書が届いた直後に、「訂正」として偽の請求書が添付されたメールが送信されるなど、攻撃者が何らかの方法により取引の情報を入手した上で攻撃を行っています。

３　ランサムウェア

ランサムウェアとは、

- ○　悪意のあるソフトウェア（マルウェア）の一種
- ○　感染するとPCやサーバに保存してあるデータが暗号化されてしまい、正常に使えない状態になる
- ○　元に戻すために、仮想通貨で身代金の支払いを要求する画面を表示する

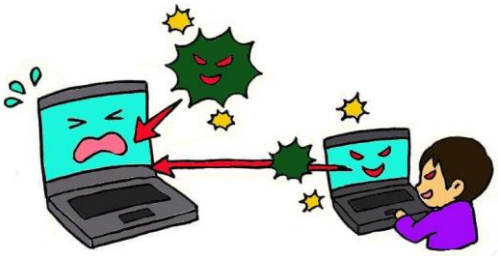
ものです。

ランサムウェアには、メールに添付されたファイルやURLを開いたり、悪意のあるソフトウェアが仕込まれたウェブサイトにアクセスしたりすることで感染します。

【実際の事例③】

昨年７月、埼玉県内の鉄道運営会社の業務用ファイルサーバがランサムウェアに感染させられる被害にあいました。

また、列車の運行に関わるシステムや定期購入に関わるシステムは別系統で管理されており、列車の安全運行等には支障はありませんでした。



【実際の事例③】

昨年 10 月、奈良県内の病院がランサムウェアに感染、電子カルテのシステムが約 2 日間使用できない被害を受けました。

感染は、システム会社の不備により、**最新のセキュリティソフトがインストールされていなかった**ことが原因でした。

サイバー攻撃から身を守るためには…

○　ソフトウェアを更新するなど、常に最新の状態に保つ

→　脆弱性を解消し、攻撃によるリスクを低減

○　セキュリティソフトの利用

→　相手からの攻撃をブロック

○　パスワードの適切な管理・認証の強化

→　不正なログインの防止

○　設定の見直し

→　誤った設定を攻撃に利用されないようにする

○　脅威・手口を知る

→　攻撃者の手口から重要視すべき対策を理解する

岐阜県警では、テロ未然防止に向けて、皆様と様々な訓練を行っています。

訓練・講演等のご要望は、事務局までよろしくお願いします。

（この通信は、IPA の「情報セキュリティ上の 10 大脅威 2019」を参考にしています。）

岐阜県警察