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。

●過去5年間で漏えいした個人情報は7545万人分…東京商工リサーチ

https://japan.zdnet.com/article/35099563/
http://www.tsr-net.co.jp/news/analysis/20170327_01.html

このニュースをザックリ言うと・・・

- 3月27日（日本時間）、東京商工リサーチ（TSR）より、2012年1月～2016年12月の5年間における「上場企業の個人情報漏えい・紛失事故」の調査結果が発表されました。

- 発表によれば、この期間において、漏えい・紛失事故を公表した企業は259社、事故件数は424件で、被害を受けた、あるいはその可能性のある個人情報は累計で最大延べ7545万人分とされています。

- 中でも最大の事件となったのは、2014年7月に発覚したベネッセホールディングスの事件で、被害3504万人分は全体の実に5割を占めるものとなっています。

- 漏えい・紛失の原因として最も多かったのは、「書類などの紛失や誤廃棄」191件、次いで「誤表示・誤送信」85件、「ウイルス感染・不正アクセス」83件となっています。

- また、原因となった媒体では、「書類」180件が最多、次いで「社内システム・サーバ」142件、「記録メディア(USBメモリー等)」39件となっています。

- 漏えい・紛失を公表した259社のうち82.2%にあたる213社が東証1部上場企業となっている一方、近年の官公庁や未上場企業などの主な漏えい・紛失事故（日本年金機構・JTB等）でも流出件数は1000万件近くに達するとし、流出に気づかず表面化していない事故や公表していないケースまで含めると、すでに国民すべてに匹敵する件数の個人情報が不正流出している可能性もあるとしています。

AUS便りからの所感等

- 5年間での漏えい・紛失の原因の割合こそ「書類の紛失や誤破棄」が多いですが、2016年には「ウイルス感染・不正アクセス」が原因の事件が前年より倍増しているとの結果も出ており、2015年以降標的型攻撃が、2016年にはランサムウェアが、それぞれ脅威として広く取り上げられ、今年もその傾向が続くと思われます。

- あらゆる個人情報の管理・持ち出しのルールについて随時見直しと遵守の徹底を行うとともに、サーバ等に保存されるデータとそれを取り扱うPCやUSBメモリー等へのマルウェア感染および不正アクセス、そしてそれによる外部への流出を食い止めるよう、アンチウイルスとUTMによる防御もまた徹底する必要があります。

ZDNet Japan

過去5年間で漏えいした個人情報は7545万人分--東京商工リサーチ

NO BUDGET 2017年04月12日 07時00分

東京商工リサーチ（TSR）は、「上場企業の個人情報漏えい・紛失事故」調査を行い、その結果を発表した。これによると、2012年から2016年の5年間、上場企業と主要子会社で発生した個人情報の漏えい・紛失事故によって漏えいした可能性のある個人情報は、累計で最大延べ7545万人分に達し、単純計算で日本の人口の半分を超えていることが分かった。

この調査は、2012年1月～2016年12月までの上場企業と主要子会社の情報漏えい・紛失事故を、プレスリリース・お知らせ・お詫びなどの、自主的な開示に基づき、発表日ベースで独自集計したもの。個人情報の定義は、氏名、住所、電話番号、年齢、性別、メールアドレス、ログインID等で、リリースの「漏えいの可能性がある」も対象とした。

この期間で個人情報の漏えい・紛失事故を公表した企業は259社、事故件数は424件にのぼる。最大の個人情報漏えい事件は、2014年7月に発覚したベネッセホールディングスの3504万人分で全体の5割を占めた。次いで、2013年5月に外部の不正アクセスで最大2200万件のIDが外部流失した可能性を公表したヤフー、2012年11月に672万人分の過去の顧客取引データを記録したコムフィッシュ（記録メディア）を紛失した三菱UFJフィナンシャル・グループと続く。

TSR 東京商工リサーチ

「上場企業の個人情報漏えい・紛失事故」調査

公開日付：2017.03.27

2012年から2016年の5年間で上場企業と主要子会社で個人情報の漏えい・紛失事故を公表した企業は259社、事故件数は424件にのぼった。漏えいした可能性のある個人情報は累計で最大延べ7,545万人分に達し、単純計算で日本の人口の半分を超えていることがわかった。

最大の個人情報漏えい事件は、2014年7月に発覚したベネッセホールディングス（(株)ベネッセコーポレーション）で、漏えいした個人情報は3,504万人分で全体の5割を占めた。

原因別では、424件のうち書類等の紛失や誤廃棄が191件（構成比45.0%）と最も多く、次いで誤表示・誤送信が85件

個人情報漏えい・紛失 事故発生回数 上位5社

社名	発生回数	産業	市場	漏えい・紛失件数（合計）
日本電信電話（NTTドコモ含む）	29回	情報・通信	東証1部	4,016,357件
東京ガス	12回	サービス業ほか	東証1部	13,145件
りそなホールディングス	10回	金融・保険	東証1部	10,490件
パナソニック	7回	製造	東証1部	80,116件
東京電力ホールディングス	7回	サービス業ほか	東証1部	1,020,387件

※ 2012年1月～2016年12月を対象 情報漏えい・紛失件数は「可能性がある」を含む
※ 100%出資などの主要子会社の開示分も含む

東京商工リサーチ調べ

●宅急便をかたるフィッシングメール活発化、ヤマト運輸も注意喚起

http://www.kuronekoyamato.co.jp/ytc/info/info_170411.html

このニュースをザックリ言うと・・・

- 4月20日（日本時間）、警視庁と日本サイバー犯罪対策センター（JC3）より、ヤマト運輸の宅急便をかたった、ウイルスが添付されたメールが同日から拡散しているとして警告が出されています。

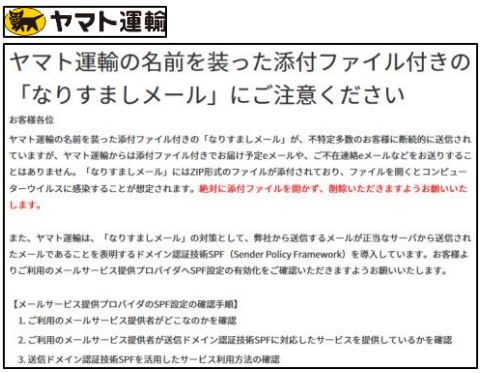
- 確認されたメールは、件名が「宅急便納品完了のお知らせ」で、本文が「ヤマト運輸をご利用いただきありがとうございます。宅急便をお受け取り店舗へ納品しましたので、ご来店ください。」で始まるものとなっており、文書ファイルを装ったウイルスがzip形式で添付されています。

- これを受けてヤマト運輸からも、「添付ファイル付きで連絡メールを送ることはない」とし、絶対に添付ファイルを開かず、削除するよう注意喚起が出されています。

AUS便りからの所感等

- JC3によれば、宅急便をかたってのウイルスメールは4月6日や10日等にも確認されていますが、特に20日に確認されたメールは、差出人名・メールアドレスや本文中の電話番号が本物である等、より受信者を騙しやすい内容となっています。

- ヤマト運輸の注意喚起では、メールの発信元IPアドレスについて、同社が申告する正当な発信元かを照合する手法であるSPF（Sender Policy Framework）に言及しており、これを用いることにより、無関係な第三者のPC等からの発信元を詐称したメールでないか、メールサーバやUTM等で確認することが可能であり、自社ドメインを持っているユーザにおいては、可能な限り設定の検討を推奨致します。


ヤマト運輸

ヤマト運輸の名前を装った添付ファイル付きの「なりすましメール」にご注意ください

お客様各位

ヤマト運輸の名前を装った添付ファイル付きの「なりすましメール」が、不特定多数のお客様に断続的に送信されていますが、ヤマト運輸からは添付ファイル付きでお届け予定eメールや、ご不在連絡eメールなどをお送りすることはありません。「なりすましメール」にはZIP形式のファイルが添付されており、ファイルを開くとコンピューターウイルスに感染することが想定されます。絶対に添付ファイルを開かず、削除いただきますようお願いいたします。

また、ヤマト運輸は、「なりすましメール」の対策として、弊社から送信するメールが正当なサーバから送信されたメールであることを表明するドメイン認証技術SPF（Sender Policy Framework）を導入しています。お客様よりご利用のメールサービス提供プロバイダへSPF設定の有効化をご確認いただきますようお願いいたします。

【メールサービス提供プロバイダのSPF設定の確認手順】

1. ご利用のメールサービス提供者がどこなのかを確認
2. ご利用のメールサービス提供者が送信ドメイン認証技術SPFに対応したサービスを提供しているかを確認
3. 送信ドメイン認証技術SPFを活用したサービス利用方法の確認

- 一方で、内部のPCがマルウェアに感染し、正規のメールサーバを経由して不正なメールを拡散させられる恐れもあり、これについてもメールサーバやUTMにおけるウイルスチェックを行い、外部への送信を遮断するようにしましょう。

●Windowsの脆弱性悪用するNSAのハッキングツール流出か、MSは対応済みと発表

http://www.itmedia.co.jp/enterprise/articles/1704/17/news051.html

このニュースをザックリ言うと・・・

- 4月14日（現地時間）、ハッカー集団「Shadow Brokers」より、米国家安全保障局（NSA）が使っていたとされるハッキングツールが公開されました。

- これを受けてMicrosoftより、公開されたツールの中にWindowsの脆弱性を突く攻撃コードが含まれていたことがブログにて発表されています。

- ただし、攻撃コードの精査の結果、いずれもこれまでリリースされたセキュリティパッチにて対応済みとされています。

AUS便りからの所感等

- 公開されたツール、もしくはそれを改造したツールを悪用する攻撃者は必ず出てくると思われますので、全てのWindows PCに対し最新のセキュリティパッチが適用されているか、そしてアンチウイルスとUTMによる防御を行っているか、確認することが重要です。

- 万が一、現在もWindows XPを利用し続けている場合、2014年のサポート終了以降に発覚した脆弱性を攻撃コードによって突かれる恐れがあります。

- 将来的なリプレースは必須ですが、それまではアンチウイルスのうち現在もXPをサポートし続けている製品を必ず導入し、かつUTM等により、可能な限り他のPCがいるネットワークから隔離するようにしてください。


ITmedia エンタープライズ

「NSAのハッキングツール」新たに大量流出　Windowsの脆弱性悪用も

Microsoftによると、ハッキングツールで悪用されていた脆弱性の大半はすでに修正されている。国際銀行間金融通信協会（SWIFT）のシステムがNSAの標的になっていたとの情報もある。

[松木聖子、ITmedia]

報道各社によると、過去に米国家安全保障局（NSA）のハッキングツール流出にかかわったとされる集団「Shadow Brokers」が4月14日、新たにWindowsの脆弱（ぜいじゃく）性を突くツールを大量に公開した。国際銀行間金融通信協会（SWIFT）がNSAによるハッキングの標的にされていたことも分かったと報じられている。

Microsoftは14日のブログで、Shadow Brokersが公開した情報の中に、Windowsの脆弱性を突くエクスプロイトが含まれていたことを確認した。しかし内容を調べた結果、9件のエクスプロイトについては、既に修正のための更新プログラムが公開されていることが判明したとしている。

それ以外の3件についても、サポート対象のプラットフォームでは攻撃を再現できなかったと述べ、「Windows 7とそれ以降のバージョンのWindows、またはExchange 2010とそれ以降のバージョンのExchangeに危険は及ばない」と説明。4月11日でサポートを打ち切ったWindows Vistaなど、サポート対象外のWindowsについては、「サポート対象の製品にアップグレードすることが望ましい」としている。