ホームページ活用通信 ～WEB マーケティングのヒント　2015 年 7 月号

株式会社ピーシー・ブレイン　お問い合せ電話番号:047-311-6677

☆今月のメニュー

■いまだから再確認！ あなたの会社のセキュリティ

- 標的にされる重要な情報
- 標的型サイバー攻撃
- むき出しの個人情報
- 実践的対策は感染した時のことも想定して！

■社長のつぶやき

～ うわっ！スゴ～～イ！

ファイルが人質に？！

標的型サイバー攻撃とは異なりますが、「ランサムウェア」と呼ばれるマルウェアの被害が増えています。
ランサムウェアとは、PC 内のファイルを勝手に暗号化して、暗号を解くために金銭を要求するメッセージを表示するものです。
感染経路は、メール添付、メール文中からの不正サイトへの誘導などによるものなので、セキュリティソフトやシステムソフトをアップデートしておくことで防御することはできます。
万一感染してしまった場合は、仮に金銭を払ったとしてもファイルを元通りに復元することはできないケースがほとんどです。
バックアップから戻すといった措置が必要になります。
このためにも、日頃からバックアップの習慣はつけておきたいものです

こんにちは、ピーシー・ブレインの高山です。
FIFA 女子ワールドカップのベスト４が出揃いました。なでしこジャパン、頑張っていますね。前回優勝したことで相当マークされている中でも勝ちきる強さ、男子サッカーにも影響与えて欲しいと思います。
さて、ホームページの活用方法を中心とした「WEB マーケティングのヒント」というタイトルで、今月も情報をお届けいたします。

標的にされる重要な情報

この 6 月は「情報漏洩」に関するニュースを耳にする機会の多い月でした。
6 月 1 日に発表された日本年金機構の基礎年金番号を含む 100 万件を超える情報漏洩事件・事故、その 10 日後に発表された東京商工会議所のセミナー参加者名簿などの情報流出と、立て続けに発表されたことで、一気に注目が集まりました。

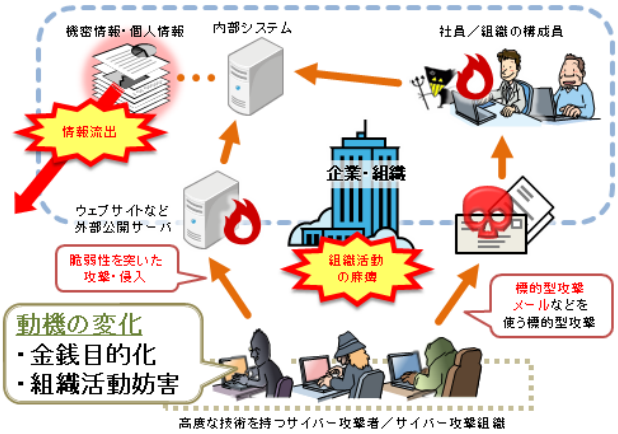
日本年金機構の個人情報流出について

1. 事象の内容
日本年金機構において、職員の端末に対する外部からのウイルスメールによる不正アクセスにより、当機構が保有している個人情報の一部が外部に流出したことが、5月28日に判明しました。現時点で流出していると考えられるのは、約125万件です。

流出した情報	件数
二情報（基礎年金番号、氏名）	約3．1万件
三情報（基礎年金番号、氏名、生年月日）	約116．7万件
四情報（基礎年金番号、氏名、生年月日、住所）	約5．2万件
合計	約125．0万件

特に日本年金機構の場合は、この 10 月から利用開始となるマイナンバー制度のプライバシー問題や、事件後に発生した電話等での詐欺とも関連して大きなインパクトを与えています。

我々のような中小企業であっては、情報流出・漏洩による事業への影響は計り知れず、その対応や対策については不安がつきまといます。



(出所：IPA 近年のサイバー攻撃の特徴)

情報漏洩のインパクトは、本来は不正アクセス・攻撃・ウイルス感染といった被害を受けた立場の者が、加害者になってしまうということです。

今回は、最近の情報漏洩の事件・事故を参考にして、自分たちのセキュリティ・情報保護を考えてみましょう。

何がおきていたのかを整理して課題を見直してみると・・・

まず確認のために、今回発生した事件の経緯を再度確認すると次のような経緯が分かります。

- 不正なプログラムが仕込まれたメールが職員宛に送られる
- 職員の数名がメールの添付ファイルを開封
- 操作した端末がマルウェアに感染
- 感染した端末が外部の指令サーバ(C&C サーバ)と通信しさらに感染が拡大
- 感染したネットワーク内には本来無いはずの個人情報が存在した
- コントロールサーバーからの指令により個人情報を取得持ち出した
- 合計で 125 万件のデータが流出したことが判明

ここで特に注目すべき点は次の 2 点です。

✓　メールによる「**標的型サイバー攻撃**」が行われた

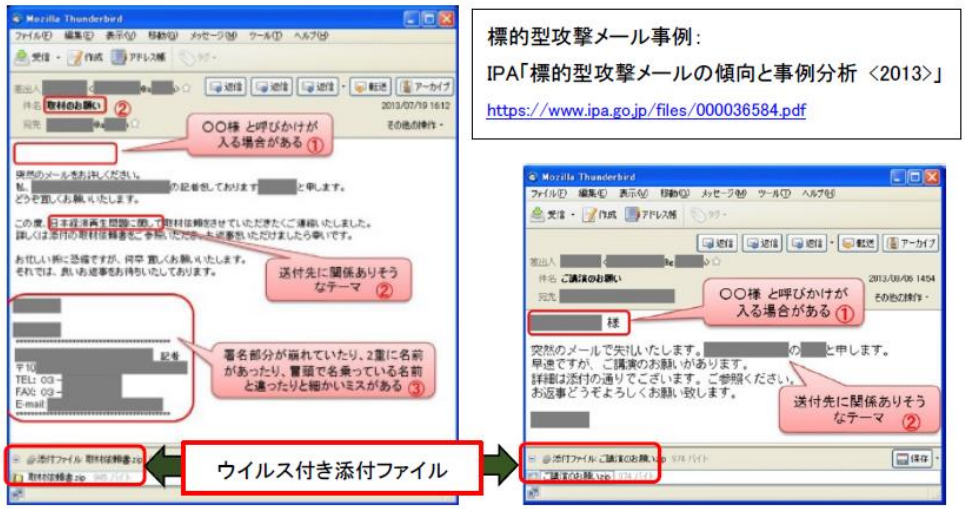
✓　本来はアクセスできないはずのデータがネットワーク上の端末に存在した

ということです。

▼標的型サイバー攻撃とは？

今回の事件では、「標的型サイバー攻撃」あるいは「標的型メール」という言葉がたびたび登場します。これは、従来の攻撃、ウイルスが不特定の人を対象にしたいわゆる「怪しいメール」の形態になっているのに対して、攻撃対象となっている企業・組織・個人にいかにも関連のありそうな内容を装ったものになっていることが大きな違いです。公的機関や取材依頼、あるいは事前に調べた関連会社、取引先に偽装するなど手のこんだ内容になっています。最近ではコピー機からの通知メールを装うものも出てきているようです。

また、感染してウイルスが実行された場合でも、目立つような振る舞いがおきないため気づきにくいという極めて重大な特徴を持っています。気づかないうちに内部へと侵入してゆくとても厄介なものです。



一度感染すると、外部の指令サーバ(C&C サーバ：Command and Control)との通信することで、感染した PC は遠隔から制御される状態になります。

この C&C サーバからの指令によって、奪取・搾取したい情報の所在を特定した上で、最終的に情報の取得・改ざんなどの攻撃を行います。この時の情報流出は内部の感染 PC から外部に持ち出す形なので、単に外部からの攻撃を防御するやり方だけでは漏洩を防ぐのが難しくなっているのです。

▼業務理由によるデータの複製

もう一点は、システム上は感染した端末が存在するネットワークと個人情報を扱う端末は、本来切り離されていたにもかかわらず、データにアクセスできてしまったということです。
その原因は、何らかの理由で別システムからデータを複製して保持していた、ということです。
例えば、端末を切り替えて検索しないといけないので業務の効率が悪い、など業務の使い勝手の悪さは想像つきます。ただこれはセキュリティを維持するという本来の目的を損なうものであって、ルールを変えた運用というのはやはり問題です。本来は安全を担保しつつ業務を考慮したシステム・機能に改修する等の対応を取るというのが正しいやり方です。
業務システムの機能を「運用でカバー」する際には十分な配慮・注意が必要です。
これは USB 等でデータを持ち出すような使い方をしている場合にも当てはまります。

対策は感染した時のことも想定しましょう

▼基本的な対策

まずは脆弱性を下げることと、リスクを回避することにつきます。
外部からの侵入を許さないためにいま一度セキュリティソフトや対策ツールを見直し、常に最新状態を維持すること、そして、怪しい情報には手を出さない、見極めるだけの知識を持っておくことが必要です。
特に最近の攻撃型メールは手が込んでいるので、少しでも不安・不審に思ったら、送信元に電話連絡して確認するくらいの慎重さがあっても良いでしょう。

▼実践的な対策は感染したことも想定して

より実践的に対策するのであれば、万一感染した場合の被害を抑える工夫が必要です。

・分離する
機密性の高い重要なデータを扱う端末は、多少の不便さはあっても、メールやインターネットを日常的に使う端末やネットワークから切り離し、決してコピーを持たないということも有効です。

・制限する
情報が保存されているフォルダやサーバへのアクセス権を見直して厳密にすることも有効です。権限のない端末・ユーザーからの不正アクセスを遮断できます。

・保護する
今回の事件で流出した情報はパスワードや暗号化などの処置がされていない丸裸のデータでした。
最終的なデータをパスワード・暗号化を保護することで、データが流出際のリスクを抑えることができます。
これはいますぐできる対策で有効度も高いのでぜひ適用してみてください。

▼参考情報　以下は、今回参考にしているセキュリティ関連情報です。さらに詳しい情報はこちらへ（IPA）
【注意喚起】潜伏しているかもしれないウイルスの感染検査を今すぐ！　http://goo.gl/AcMtQL
【注意喚起】組織のウイルス感染の早期発見と対応を　https://goo.gl/iJzh2d
【注意喚起】ウイルス感染を想定したセキュリティ対策と運用管理を　https://goo.gl/Ga6QXv
『高度標的型攻撃』対策に向けたシステム設計ガイド　https://goo.gl/8kXO3h
標的型攻撃メールの例と見分け方　https://goo.gl/97mTgE

株式会社ピーシー・ブレイン

〒270-2253
千葉県松戸市日暮 1-2-6
勝どきビル

電話番号
047-311-6677
Fax
047-311-6678
E-mail
info@pcbrain.co.jp

受付時間：
9:00～17:30

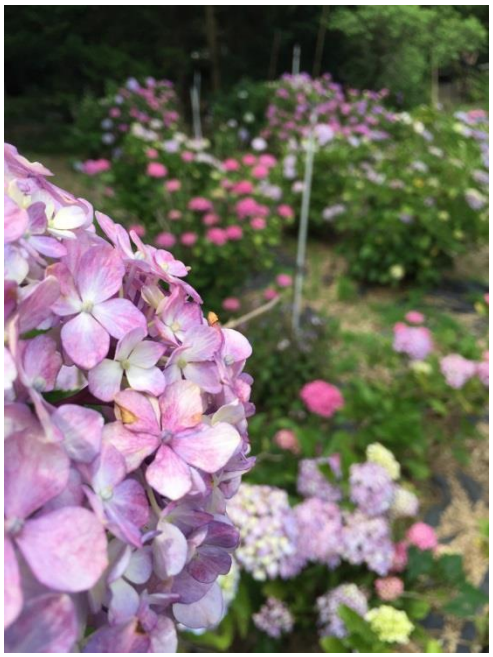
地域で一番ネットを使った商売に詳しいコンサルティング企業

- Web マーケティングコンサル
- ネット集客支援
- ホームページ制作
- SEO リフォーム
- WEB システム開発

当社 Web サイト:
http://www.pcbrain.co.jp
http://www.webquick.jp

社長のつぶやき・・・　うわっ！スゴ～～イ！

見渡す限り、辺り一面ピンクや紫色のあじさい畑。お寺の境内へ入った瞬間、一瞬息が止まるくらいの壮観な光景が目の前に広がっていました。



６月中旬の日曜日、松戸市の本土寺（通称「あじさい寺」）へお散歩に行った時の事。
地元松戸でありながら今まで一度も行ったことが無かった場所なので、ほんとに素直に驚く事ができました。

このあじさい寺（www.hondoji.net/）は、JR 常磐線北小金駅から徒歩 15 分程度。あじさいが見頃のこの時期、お寺までの通りにはたくさんの出店があり、人通りも大変にぎやかです。
当然、我々も境内を出た後は出店の奥テーブルに座り、生ビールと枝豆でとても幸せな休憩時間を過ごさせていただきました。

追伸
若者が撮る写真は友人など人物が多く、年寄りの写真は花や景色が多いと誰かに聞いた事がありますが、改めて自分のスマホを見てみると、花や景色の写真がだんだん増えているような・・・(^_^;)

ニュースレターの感想、取り上げて欲しいテーマ、相談など、ぜひご意見をお聞かせ下さい！
→　FAX:**047-311-6678 /** 電子メール：**info@pcbrain.co.jp**

株式会社ピーシー・ブレイン
発行責任者：高山卓巳

〒270-2253
千葉県松戸市日暮１－２－６
勝どきビル

TEL: **047-311-6677**　FAX: **047-311-6678**　Email: **info@pcbrain.co.jp**