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。

●マイナンバー、10月に交付、来年1月より運用開始。対応完了企業は2割

http://www.itmedia.co.jp/enterprise/articles/1503/24/news076.html
http://www.itr.co.jp/company_outline/press_release/150324PR/index.html

このニュースをザックリ言うと・・・

- 社会保障・税番号（マイナンバー）制度が2016年1月より運用開始となり、先立って今年10月より順次番号の交付が始まります。

- マイナンバーは社会保障・税・災害対策のための場合に提示が義務付けられるもので、退職者の源泉徴収票、支払調書への印字などの義務付けから始まり、以後も各種書類への印字義務付けが拡大され、行政機関・所属企業等に対する告知、および組織側での番号の保存管理が必須となります。

- 3月24日（日本時間）、日本情報経済社会推進協会（JIPDEC）とITR社が698社に対し実施した「企業IT利活用動向調査2015」の結果が発表され、マイナンバーに関する設問も取り上げられているのですが、現時点でマイナンバー制度へのシステム対応を「完了している」という回答は18.2%、一方「対応の必要はないと考えている」が8.7%、「わからない」が17.6%にのぼっています。

AUS便りからの所感等

- マイナンバーの利用は現時点で前述した社会保障・税・災害対策に限定され、番号だけで本人になりすましてあらゆる不正行為が実行できるようなものではないとされていますが、他の個人情報と同様に適切な保護・管理が求められることは確かです。

- 行政の効率化や国民の利便性向上のための導入が謳われており、一方でセキュリティと利便性のトレードオフは常に存在するのですが、これまでにない全く新しいセキュリティの概念が必要になるわけではなく、最低限、周辺ネットワークにおいてUTM等によるセキュリティの確保を行っているか、改めて確認することが肝要です。

ITmedia エンタープライズ ＞ マイナンバー対応、完了企業は約2割に

2015年03月24日 12時55分 更新

マイナンバー対応、完了企業は約2割に

JIPDECとITRの調査によれば、2016年1月に開始される「マイナンバー」制度への対応では約2割が完了と答える一方、3割近くは「予定なし」「わからない」と回答した。

[ITmedia]

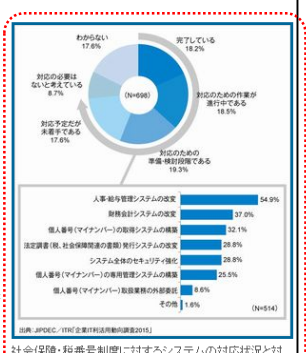
印刷／PDF　ツイート 40　いいね！ 14　チェック　G+1 8　Pocket 14　通知

PR 「高コスト」は実は誤解？セキュアで便利な生体認証の真実
PR 読者限定【先着115名様！】IBM Verse無料登録キャンペーン

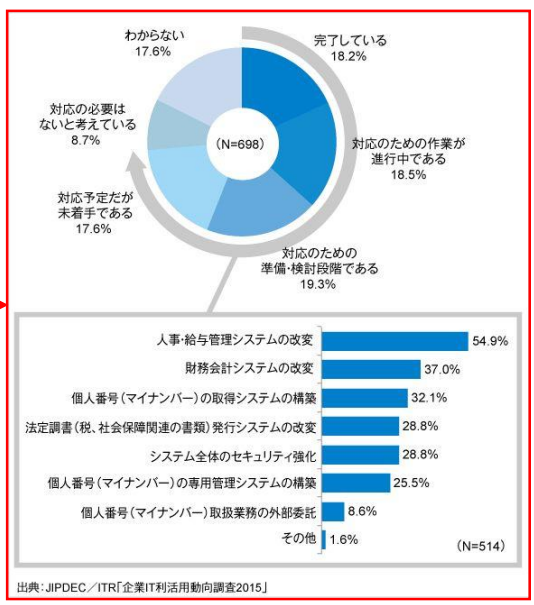
日本情報経済社会推進協会（JIPDEC）とアイ・ティ・アール（ITR）は3月24日、698社のITおよび情報セキュリティ責任者を対象に共同実施した「企業IT利活用動向調査2015」の結果を発表した。2016年1月に開始される「マイナンバー」制度への対応では約2割が完了と答えた。

マイナンバー制度への対応の必要性を挙げる企業は73.7%あり、対応を「完了した」企業は18.2%、「進行中」は18.5%、「準備・検討段階」は19.3%だった。対応内容では「人事・給与管理システムの改変」が54.9%で最も多く、「財務会計システムの改変更」（37.0%）、「マイナンバー取得システムの構築」（32.1%）が続く。

この結果からJIPDECとITRは、多くの企業が既存アプリケーション・システムの改変を中心とした限定的な対応を想定していることがうかがえると指摘。「わからない」とした回答が17.6%あり、IT部門責任者や情報セキュリティ担当者が制度対応の実態を十分に把握できていない様子もあるという。



社会保障・税番号制度に対するシステムの対応状況と対応範囲。出典：JIPDEC/ITR



出典：JIPDEC／ITR「企業IT利活用動向調査2015」

社会保障・税番号制度に対するシステムの対応状況と対応範囲

参考 ： 内閣官房「マイナンバー　社会保障・税番号制度」ページ
http://www.cas.go.jp/jp/seisaku/bangoseido/gaiyou.html

●新手の標的型メール、検出回避にWordの正規機能を悪用

http://www.itmedia.co.jp/enterprise/articles/1503/20/news142.html
http://blog.trendmicro.co.jp/archives/11140

このニュースをザックリ言うと・・・

- 3月20日（日本時間）、トレンドマイクロ社がMicrosoft Office Wordの機能を巧妙に悪用した標的型攻撃を確認したと同社ブログで発表しました。

- 攻撃メールに添付された不正なWordファイルには、画像が「挿入とリンク」という形式で挿入されており、添付ファイルを開いただけで指定された悪意のあるサイトへのアクセスが発生するようになっていたとのことです。

- 「挿入とリンク」は、「挿入」「ファイルにリンク」と同様にWordファイルに画像を挿入する正規の機能であり、不正なリンクへのアクセスを事前に読み込まれていた画像でカモフラージュする意図があったとされています。


ITmedia エンタープライズ ＞ 新手の標的型メール、検出回避にWordの正規機能を悪...

2015年03月20日 19時35分 更新

新手の標的型メール、検出回避にWordの正規機能を悪用

Wordの標準機能を使って不正サイトに接続させる手口を使った標的型攻撃メールが見つかった。

[ITmedia]

印刷／PDF　ツイート 92　いいね！ 136　チェック　g+1 0　Pocket 19　通知

PR 「高コスト」は実は誤解？セキュアで便利な生体認証の真実
PR 読者限定【先着115名様！】IBM Verse無料登録キャンペーン

トレンドマイクロは3月20日、Microsoft Office Wordの標準機能を巧妙に使う標的型攻撃メールを確認したと発表した。不正な点がほとんど見られず、検出が難しいという。

同社が匿名者から得たという標的型攻撃メールには、会計報告書などのファイル名が付いた3つのWordファイルが添付され、うち2つのファイルは裏側で外部の不正サイトと通信をしていた。しかし、解析では不正サイトへ接続するマクロや、脆弱性を悪用する点などは見当たらず、ファイル内の画像に挿入されたハイパーリンクから接続する仕組みであることが分かったという。

AUS便りからの所感等

- 不正なマクロの実行やOfficeの脆弱性を突くようなものではない形であるために、一時はアンチウイルス等によるチェックを回避していたようですが、今後各種UTM・アンチウイルス側で同様の攻撃への対応が行われるとみられます。

- いずれにせよ、これまでに見られた攻撃から今後新たに考えられ得る攻撃までの対応、不正なアクセス先へのアクセス遮断やダウンロードされたファイルのPC上でのチェックのため、UTMやアンチウイルスの導入は必要不可欠です。

●大量生成ホストやHTTPS化 – ブルーコートが語る、さらに「見えにくく」なる攻撃の現状

http://internet.watch.impress.co.jp/docs/news/20150325_694537.html

このニュースをザックリ言うと・・・

- 3月24日（日本時間）、Webセキュリティアプライアンス等を提供するブルーコートシステムズ社が同社のクラウド型Web防御システム「WebPulse」でのログ分析結果をもとにした「マルウェアやフィッシング攻撃などの動向」について発表しました。

- 同社によれば、90日間のログで確認された6億6000万件のホストのうち71%にあたる4億7000件が24時間以内しか存在が確認されない「1日限定サイト」であり、その中には攻撃者が「使い捨て」で立ち上げている悪意のあるホストも含まれており、従来のブラックリスト形式でのブロックでは対抗し切れなくなっているとしています。

- また、マルウェアが自身をPCへダウンロードさせる等の際にHTTPS通信を用いる傾向が強まることで、セキュリティ対策製品が正しく検知できないといったことも問題視しており、今後さらに「見えなく」なってくる攻撃への対応が必要になるとしています。


INTERNET Watch

最新ニュース

東急建設、無線LANの通信障害を改善する電磁波シールドの実用化へ前進 2015/04/06
JeNA、キュレーション事業を拡大、旅・男性ファッション・妊娠～子育ての8ジャンルでも 2015/04/06
INTERNET Watchアクセスランキング【2015/3/30～2015/4/5】 2015/04/06
Apple Watch、10日予約注文開始、Appleが使い方動画を公開中 2015/04/06
日本交通のタクシーにBeacon、広告動画をみると割引クーポンが付与 2015/04/06

ニュース

大量生成ホストやHTTPS化――ブルーコートが語る、さらに「見えにくく」なる攻撃の現状

(2015/3/25 15:03)

g+1 1　B! 23　ツイート 51　いいね！ 13　Pocket 48

ブルーコートシステムズ合同会社は24日、クラウド型ウェブ防御システム「WebPulse」のログ分析から得られたマルウェアやフィッシング攻撃などの動向に関する説明会を開催した。

WebPulseは、クラウドベースのコミュニティ型ウェブ分析・評価サービス。米Blue Coat Systemsのマルウェア研究所では、世界中の政府、企業、個人などのユーザーのウェブトラフィックログをモニター し、1日10億件以上のウェブリクエストをリアルタイムで分析、マルウェアやフィッシングサイトの検出を行っている。

マルウェア研究所アーキテクトのChris Larsen氏は、WebPulseではログをさまざまなソースから長期的に収集しており、そこから「場違いなもの」を探すとともに、それが「悪質」であるかを判断するのがマルウェア研究所の仕事だと説明。さらに、悪質な攻撃を識別および追跡するためのソフトウェアを開発して手順を策定し、そのデータをBlue Coat Systemsの全製品で共有しているとした。

AUS便りからの所感等

- 暗号化通信が攻撃者にとっての隠れ蓑にもなることは決して予想されていなかったことではなく、今後も機密性・可用性・完全性の維持のために必要不可欠なことには変わりないものであり、その解読を伴うセキュリティチェックの採用にはユーザへの十分な説明等を慎重に行うべきです。

- ともあれ、日々新しくなっていく攻撃手段に対しその都度フレキシブルに対応できるようなセキュリティ対策製品を選んでいくことが今後ますます重要になるでしょう。