マイナンバーとセキュリティ対策のお話

出典:内閣官房ホームページ

2016年1月　マイナンバー制度が始まります

マイナンバーは今年の10月より配布が開始されます。企業がマイナンバー(特定個人情報)の収集を始める**2015年10月**までには給与パッケージの変更や、**ITセキュリティ対策**の必要があります。

ITセキュリティ対策の必要性について

内閣府：特定個人情報の適正な取り扱いに関するガイドライン（事業者編）より抜粋

c　**外部からの不正アクセス等の防止**

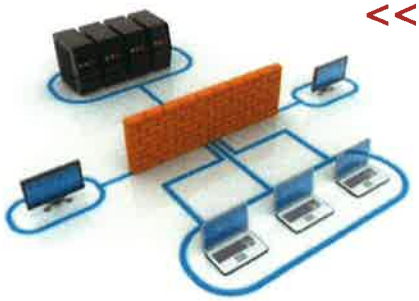
情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。

≪手法の例示≫

- 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。
- 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。
- 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。
- 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。
- ログ等の分析を定期的に行い、不正アクセス等を検知する。

不正アクセスに対しての対策を講じることを明文化されております。また、企業がマイナンバーの収集を始める10月に合わせて、マイナンバーを不正に収集するためのITを使った攻撃（フィッシング詐欺、不正侵入・・・）が増加することが懸念されています。

アメリカでは既に本人確認の手段として広く利用されておりますが、番号を盗まれて年金や生活保護を受ける「ID詐欺」の被害が深刻化しております。一つのIDで管理できる利便性は広がりますが、一度漏えいしたら影響が大きくなるというのが「マイナンバー」のため、情報セキュリティ対策は万全にする必要があります。



<<オールインワンで行うおまかせ情報セキュリティ対策について>>

主な機能

- ファイアウォール
- ウイルス検知
- Ｅメールフィルター
- 不正サイトへのアクセス禁止
- 不正侵入防止

HOME-UNIT

企業が今対策をしなければならないセキュリティを一つのユニットにオールインワンで行います。このユニットは遠隔でキヤノンのコンタクトセンターが運用・管理を行いますのでお客様の負荷なくセキュリティ対策が行えます。

面倒なITセキュリティ対策をオールインで保守運用まで行います
お問い合せは当社まで

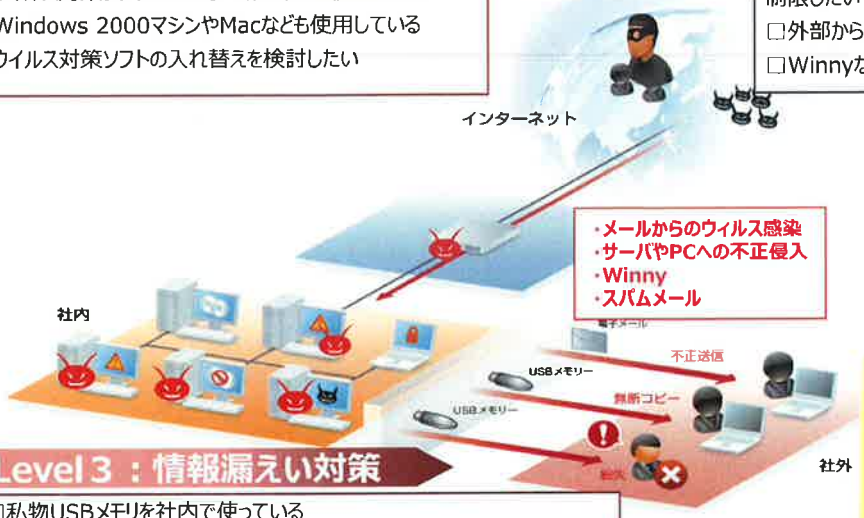
セキュリティ対策チェックシート　※当てはまるものにチェックをしてください

Level 1 ：PCのウィルス対策

□日々新たに発生している新種や亜種のウイルスに脅威を感じる
□ウイルス定義DB更新時などでPCの動作が遅い
□ウイルス対策ソフトについてコストダウンを検討したい
□Windows 2000マシンやMacなども使用している
□ウイルス対策ソフトの入れ替えを検討したい

Level 2：不正侵入対策

□迷惑メールの対策を行いたい
□業務とは関係のないWEBサイトの閲覧を制限したい
□外部からのＰＣへの乗っ取りを防ぎたい
□WinnyなどのP2Pアプリを禁止したい



Level 3 ：情報漏えい対策

□私物USBメモリを社内で使っている
□知らない間に色々なアプリケーションがインストールされている
□社有のUSBメモリの棚卸をしたい
□掲示板サイトやWebメールの書き込みを禁止したい
□社外に送信されたメールが把握したい
□ソフトウェアのセキュリティパッチの適用状況を把握したい

最近のセキュリティ脅威

✓ オンラインバンキングやクレジットカード情報不正利用
✓ 内部不正による情報漏えい
✓ 標的型攻撃による諜報活動

そして・・・
マイナンバー制度での情報厳格管理の必要性

情報セキュリティ対策 導入ステップ

Level1 ウイルス対策

PCやサーバーに、ウイルス対策ソフトを導入します。

●既知のウイルスはもちろん新種・亜種のウイルスも検出可能
●スキャンを感じさせない軽快な動作
●シンプルな購入形態
●Windows / Mac / Linuxはもちろん
●Androidまで多彩なOS環境に対応

ESET

インターネット接続に欠かせない最も基本的な対策！

Level2 不正侵入対策

社内LANとインターネットの境界に、UTMを設置します。

●ネットワーク経由のウイルス検出
●不正なアクセスを検知・遮断
●有害Webサイトへのアクセス制御
●迷惑メールの検出
●ログ管理によるネットワークの利用状況の可視化

HOME

水際ですべての脅威に対応するコストメリットのある効果的な対策！

Level3 情報漏えい対策

PCの利用状況の把握と、利用制御を行います。

●操作ログの取得によるPCの利用状況の可視化
●USBメモリーの利用制限
●不正操作時のアラート表示
●IT資産管理
●ソフトウェアライセンス管理

QGG Quality Gather & Guard　SKYSEA Client View

組織内部からの情報漏えい対策とコンプライアンスの強化

さまざまな脅威に対応する有効な手段。現在は最低限ここまで必要です！

次に必要な社内の情報漏えい対策

マイナンバー制度開始によってさらにセキュリティ脅威が増えていきます。万全な情報セキュリティ対策が急務です！

●お問い合わせは当社まで

あなたの街のトヨジムです TOYOJIMU 株式会社トヨハシ事務器

〒440-0853 愛知県豊橋市佐藤五丁目19番地の12 | 担当
TEL:0532-66-2000 FAX:0532-66-2020