

抜粋版

2016年6月15日

第38回 情報セキュリティ 管理者勉強会  
情報セキュリティセミナー

セッション1

待ったなし個人情報保護法改正 と  
マイナンバー 個人事業主（委託先） 管理方法について

セッション2

新米情報セキュリティ管理者のための、基礎講座  
第2回目 『ネットワーク機器編について』 について  
株式会社エスケイワード

# 本日のテーマ

## セッション1 最新セキュリティトピックス

**その1 Windows 10 アップグレード 注意点 第2回** (社員にアップグレード後の端末を渡す前にここまで実施しておきましょう。)

約1か月後に迫った windows10の無料アップグレードですが アップグレードしたままの状態ですら業務で関係ないアプリ表示や(ゲームやストア等)またバックグラウンドで動くアプリ等、設定を管理者側で変えておかないといけません。今回はどの設定が推奨か、前回に続き、解説いたします。

**その2 台湾 文化事情 & IT セキュリティ レポート**

観光立国を目指す日本ですが、インバウンド消費は現在3兆円規模の経済効果があると言われております。国別で、訪日人数が多いのは、2年前までは台湾でした。(昨年の1位は爆買い効果で中国、2位は台湾、3位は韓国、4位は香港)最近では中国本土のニュース(政治、経済、サイバーセキュリティ等)をよく見かけますが、昔から、文化、ビジネス、IT分野等 日本と結び付きが強く親日国を言われている台湾とはどのような国なのでしょう。筆者は8年前に台湾に訪問しましたが、今月再度訪問しました。台湾の文化 並び にIT事情がどう変わったか?現地レポートをいたします。

**その3 待ったなし 個人情報保護法改正**

個人情報保護法が改定となり、次年度その対応をすべての企業が実施しなければなりません。具体的に何を実施するか、また保護法がどう変わるか、そもそも個人情報保護法の定義は何か?何がどう変わるか?またこれから企業は何を実施すべきかを、分かりやすく 解説いたします。

**その4 まだ間に合う 委託時 個人事業主 からの マイナンバー収集方法について**

個人事業主へ年間5万円以上委託している場合、マイナンバーを年内中に収集しなければなりません。既に社員様のマイナンバーは収集した企業もありますが、委託先で個人事業主のマイナンバーまでまだ収集していない企業様も多いと思います。幸い今の法律では、マイナンバーの使用が限定されている為、一般企業にお勤めされている社員様は、会社から → 社労士さん や 税理士さん へ提出するぐらいですが個人事業主(フリーランス)の方は 年間5万円以上 委託した複数の企業先へ提出するとなると、一般企業の方より漏えいのリスクが高まります。もしかして、5年後や10年後に、個人事業主の方からマイナンバーが漏えいしたということで、提供先の企業に片っ端からクレームするという事が起こるかもしれません。それらを防ぐ為に、今しっかりと対応をしておけば、まだ間に合います!何を実施するか、どう集めればよいか実施すべき工程を、分かりやすく解説いたします。

## セッション2 新米情報セキュリティ管理者のための、情報セキュリティ管理方法を学ぶ ~ISMS (ISO27001) を活用して~ 第2回目 ( 計5回 ) 30分 『ネットワーク機器編について』

第1回 ランサムウェア、マルウェア、不正攻撃編

**第2回 ネットワーク機器編について**

第3回 情報システム基礎知識講座計

第4回 クラウドサービス、ソーシャルメディア、オンラインストレージ編

第5回 スマートフォン、タブレット端末編』

← 本日のテーマ

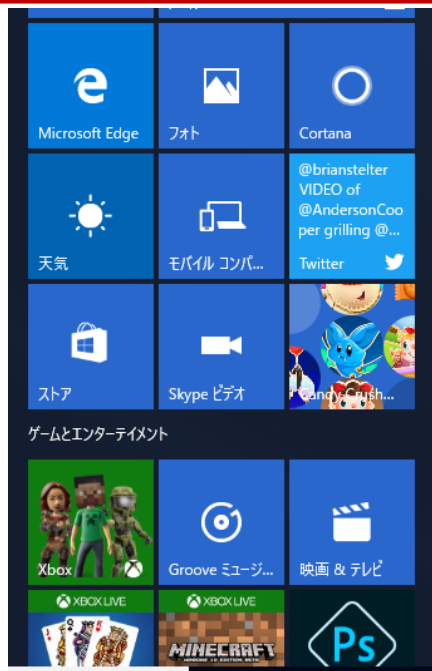
# 不要なアプリの削除と非表示（ビジネス用）

- 標準でもビジネスでは使用しないアプリケーションが入っている為、アンインストールするか、標準のライブタイルからは削除しておくことをお勧めします。また、**ライブタイルには、ビジネス用途でないアプリケーションはすべて削除の方がよろしいでしょう。（ピン止めを外す）**

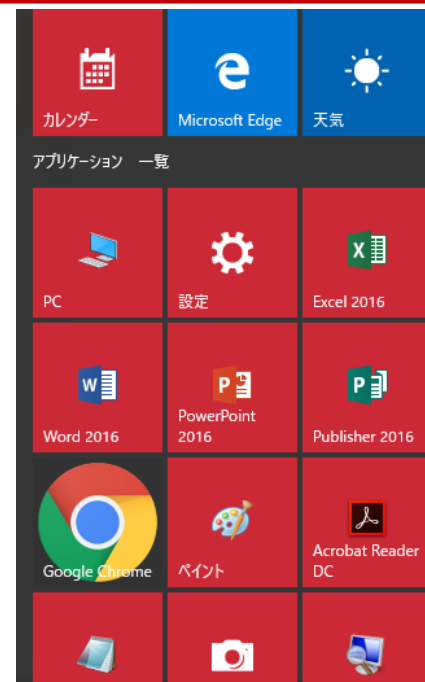
標準の状態（ビジネス用途以外が表示）

よく使うアプリのみ表示へ

ビジネス用途以外の  
アプリが標準で  
インストールされている



ライブタイル 設定前



ライブタイル 設定後

## Windows 10 アップグレード注意点 その2 WINDOWS10不要な設定を外す設定方法 (サービスの一覧から外す)

①スタートにマウスを置いて右クリック → ②コントロールパネルを開く → ③管理ツール開く → ④サービスを開く → ⑤サービスの表示の一覧が表示される → ⑥不要なサービスを起動しないように無効化の設定をする。ビジネス使用もしくは環境において（デスクトップPCなのに、ノートパソコンやタブレットの機能等）明らかに不要だと思われるものを無効にすれば、PCの速度がアップが期待されるでしょう。（メモリ節約や高速化）

③ 管理ツール

⑤ サービスの一覧

コントロールパネル > すべてのコントロールパネル項目 > 管理ツール

名前	更新日時	種類	サイズ
ISCSI イニシエーター	2015/10/30 16:17	ショートカット	2 KB
ODBC データ ソース (32 ビット)	2015/10/30 16:18	ショートカット	2 KB
ODBC データ ソース (64 ビット)	2015/10/30 16:17	ショートカット	2 KB
Windows メモリ診断	2015/10/30 16:17	ショートカット	2 KB
イベント ビューアー	2015/10/30 16:17	ショートカット	2 KB
コンピューターの管理	2015/10/30 16:17	ショートカット	2 KB
コンポーネント サービス	2015/10/30 16:17	ショートカット	2 KB
サービス	2015/10/30 16:17	ショートカット	2 KB
システム構成	2015/10/30 16:17	ショートカット	2 KB
システム情報	2015/10/30 16:17	ショートカット	2 KB
セキュリティが強化された Windows ファイアウ...	2015/10/30 16:17	ショートカット	2 KB
タスク スケジューラ	2015/10/30 16:17	ショートカット	2 KB
ディスク クリーンアップ	2015/10/30 16:19	ショートカット	2 KB
ドライブのデフラグと最速化	2015/10/30 16:17	ショートカット	2 KB
パフォーマンス モニター	2015/10/30 16:17	ショートカット	2 KB
リソース モニター	2015/10/30 16:17	ショートカット	2 KB
ローカル セキュリティ ポリシー	2015/10/30 16:18	ショートカット	2 KB
印刷の管理	2015/10/30 16:18	ショートカット	2 KB

ファイル(F) 操作(A) 表示(V) ヘルプ(H)

サービス (ローカル)

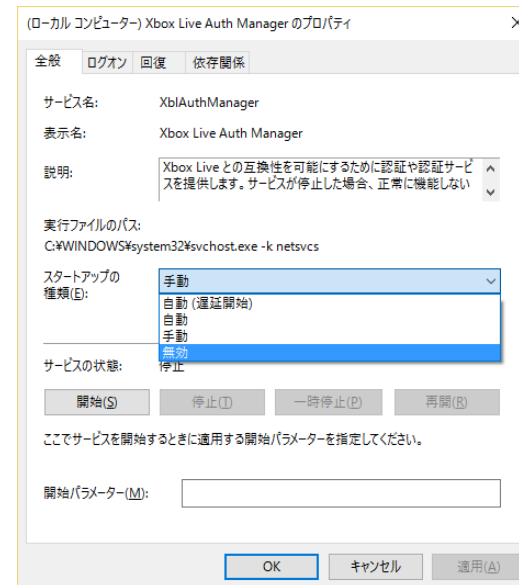
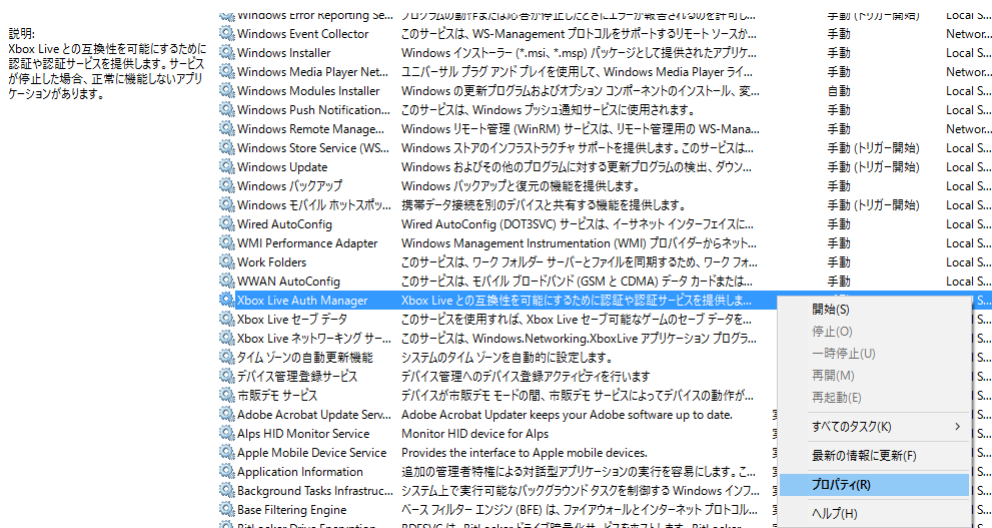
項目を選択すると説明が表示されます。

名前	説明	状態	スタートアップの種類	ログオン
ActiveX Installer (AxinstSV)	インタ...	手動	Local S...	
Adobe Flash Player Update ...	このサ...	手動	Local S...	
AllJoyn Router Service	ローカ...	手動 (トリガ-開始)	Local S...	
App Readiness	ユーザ...	手動	Local S...	
Application Identity	アプリ...	手動 (トリガ-開始)	Local S...	
Application Layer Gateway ...	インタ...	手動	Local S...	
Application Management	グリ...	手動	Local S...	
AppX Deployment Service (...)	スタ...	手動	Local S...	
Background Intelligent Tran...	アイ...	自動 (遅延開始)	Local S...	
Block Level Backup Engine ...	WBE...	手動	Local S...	
Bluetooth Handsfree Service	コンピ...	手動 (トリガ-開始)	Local S...	
BranchCache	このサ...	手動	Networ...	
Certificate Propagation	ユーザ...	手動	Local S...	
Client License Service (ClipS...	Micr...	手動 (トリガ-開始)	Local S...	
COM+ System Application	コンポ...	手動	Local S...	
Connected Device Platform ...	このサ...	無効	Local S...	
DataCollectionPublishingSe...	The ...	手動 (トリガ-開始)	Local S...	
Delivery Optimization	コンテ...	自動 (遅延開始)	Local S...	
Dell Digital Delivery Service	Dow...	自動 (遅延開始)	Local S...	
Dell.CommandPowerManag...		手動	Local S...	
Device Install Service	ユーザ...	手動 (トリガ-開始)	Local S...	
Device Setup Manager	デバイ...	手動 (トリガ-開始)	Local S...	
DevQuery Background Disc...	アプリ...	手動 (トリガ-開始)	Local S...	
Diagnostic System Host	Diag...	手動	Local S...	
Distributed Transaction Coo...	デー...	手動	Networ...	
dismwppushsvc	WAR...	手動 (トリガ-開始)	Local S...	
Downloaded Maps Manager	ダウン...	自動 (遅延開始)	Networ...	
embeddedmode	埋め...	手動 (トリガ-開始)	Local S...	
Encrypting File System (EFS)	暗号...	手動 (トリガ-開始)	Local S...	
Enterprise App Managemen...	エンタ...	手動	Local S...	
Extensible Authentication R...	拡張...	手動	Local S...	
Fax	このユ...	手動	Networ...	
File History Service	ユーザ...	手動 (トリガ-開始)	Local S...	
Google Software Updater	Goo...	手動	Local S...	

使用していない機能 (FAX等) や  
ビジネスで不要と  
思われるサービスを無効にする。

# 無効にした方がよいと思われる機能

- Fax (必要ないのでFaxのサービスを無効にします。)
- Hyper-V (仮想マシンを使う場合。使用しないので同じサービスが8つすべて無効)
- Smart Card (カード認証を行う場合であれば別ですが、通常使用しないので無効。他の3つも無効)
- Telephony (ビジネス用の電話を連動して使用する場合)
- Windows Biometric Service (生体認証がなければ無効)
- Xbox Live (ビジネスでは使用しないので無効 3つの項目すべて無効)
- 市販デモサービス (販売時のデモをするケース以外では不要の為、無効)



## その他 使用状況に応じては無効にした方がよいと思われる機能

- Bluetooth (機器を使用している場合は 有効にしておくこと)
- Touch Keyboard and Handwriting Panel Service (タブレット端末やノートPC等で、タッチキーボードでなければ不要)
- Remote Desktop (リモートデスクトップ実施しない場合は無効)
- Routing and Remote Access (システム担当者等でリモート作業をしない端末ならば無効)
- Secure Socket Tunneling Protocol Service (VPN使用していない環境であれば無効)
- Sensor Data Service (端末にセンサー在りで、使用中以外、または同様の開発関係者以外は無効)
- Windowsモバイルホットスポットサービス (使用しない場合は無効。)

### まとめ

2016年7月28日まで Windows 10 無料でアップグレードが可能 (win7 win8.1 対象)

(※Windows7はあと5年後の2020年にはサポートが終了する。)

ビジネス用途で使用しないアプリケーションや機能の無効や表示のOFFを実施してから

社員に展開する方がよい。

# 数年前2008年と現在（2016年）の変化

8年前 に訪問した際と今月訪問した際の違い

## Before（8年前） 台湾訪問時の所感

- ①日本のチェーン店は複数出店あり。繁体字と日本語の併記の看板やメニューが多くあった。日本人観光客というより、日本語表示のブランドという意味合いも強く感じた。
- ②『日式』の文字が人気で、テレビのCM等で、高級感あるイメージで宣伝されていた。日本のCM等はそのまます幕で放映されていた。（化粧品やゲーム等）
- ③高層ビルの台北101の高さ世界一位（2010年ドバイにあるブルジュ・ハリファ）また、原付の台数世界一位。
- ④携帯電話の機種の種類は豊富で、日本のキャリアが販売している機種は少なかった。
- ⑤台北市駅ではデジタルサイネージが多く使用されていた。
- ⑥PCのマザーボード産業シェアは世界一（現在も）世界のPC9割は台湾製。
- ⑦ iphone は当時日本では発売されておらず、台湾では発売されていて人気だった。

## After（現在）台湾訪問時の所感

- ①日本旅行ガイドブックは人気。但し名古屋、中部版のガイドブックはほとんど無い（東京、大阪、京都、北海道、沖縄の本は沢山あり、逆輸入本もほぼ同値段で販売）
- ②『日式』の文字が相変わらず多く表記されているが、ニュースでは、安全性・安心・健康のキーワードとして取り上げられている（健康食品や品質面にて日式は安心）。
- ③本や看板のデザインは昔ながらのデザインではなく、ほぼ日本と変わらず（グローバルデザイン）萌え系のキャラ等も在り。
- ④中国では携帯の通信速度向上が図られていてG5の導入中で台湾も同じく導入予定。
- ⑤台北市内は無料WIFIが多く、旅行者だけでなく、市民にも開放されている。
- ⑥ドローンが人気で、落下して人が怪我をしたという事件がニュースで流れていた。
- ⑦iphone や ipad等 価格に関しては日本と変わらない価格

# 台湾 文化事情 & IT セキュリティ レポート

台湾の書店では日本旅行の雑誌やガイドブックは多く陳列されている  
但し名古屋や中部圏の本はたった6種類しかない



名古屋 中部圏のプロモーションはこれから伸びる余地あり



- 台湾では FB登録されている国別では利用率は世界一位（約60%以上）
- Iphone 等 人気機種の場合はほぼ日本で購入する金額と変わらず
- 日本はWi-Fiスポット(無料、有料を含め)の数が少なく、後進国とも言われています。（海外では日本ほどにセキュリティの意識が高くないことから、制度上のハードルが低い）外国人旅行者からみると利用可能なWi-Fiスポットの数が少ない事で、不満の声が多いが、台湾は、無料Wifi が多く、パスポートを空港で提示すれば、期間中外国人でもWi-Fiスポットにいけば、使用できる。（日本でもの都市や商店街など、普及が必要）



台湾町並み



Wifi登録は日本語メニュー在り



価格、陳列は同じ

- モバイル向けの主なサイバー脅威では、カスペルスキーの最新の調査によると、最も多く攻撃を受けた国は中国で、約40%がモバイルでの脅威に遭遇したとの事です。続いて攻撃が多かった国は、バングラデシュ（28%）とウズベキスタン（21%）一方、比較的安全な国と地域は、**台湾（2.9%）**、オーストラリア（2.7%）、日本（0.9%）との事で、モバイル（スマートフォン）使用率が多い割には比較的安全なモバイル環境を使用している。※先月講演した、標的型攻撃メール等のコンピューターウイルスは台湾（繁体字・はんたいじ）からのではなく中国本土の（簡体字・かんたいじ）のケースが多いと予測される。
- 世界のPCのマザーボードは全て台湾製といってもよい。

ASUS(アスス)、ASROCK、GIGABYTE、FOXCONNなどが有名なマザーボードのメーカー



ITに関しては、日本より進んでいる所もある。他国のIT動向も注視しながら、セキュリティ対策の動向もつかむ事も重要である。

# 待ったなし 個人情報保護法改正 具体的に何が変わるか？

対象：全企業

- **① 個人情報の定義を拡充**  
→ (指紋・顔認識データ・旅券・免許証番号 と 要配慮個人情報)
- **② 「ビッグデータ」を活用しやすくする**  
→ (一定の条件のもと自由な利活用を可能とするルールの整備)
- **③ 個人情報の保護を強化するための規定の整備**  
→ (システム面やルール整備が必要)
- **④ 小規模事業者への対応**  
→ (少量である場合の個人情報取扱事業者からの除外規定を削除)
- **⑤ 個人情報取扱事業者による努力義務への個人データの削除の追加**
- **⑥ 開示等請求権の明確化**

今回は①と③と⑤を中心に講演します。

# ※個人情報の定義はどう変わるか？

## 個人情報の定義の明確化

特定の個人の身体の一部の特徴を電子計算機のために変換した符号

※指紋認識 データ や 顔認識 データ

対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号 ※旅券番号 や 免許証番号

## 要配慮個人情報

従業員の雇用管理情報

「病歴」が含まれることがある・どの宗教を信教しているか・デモ活動等の情報等 ※収入や信用情報は、原則としてあたらないと考えられる

各省庁のガイドラインによる規制に注意

**個人情報一覧表に追加、業務洗い出しとリスクアセスメント実施が必要**

# 待ったなし 個人情報保護法改正 企業の安全管理措置はどうか？

## 情報管理に関する対応

### ■ 情報管理の内容

(1) 個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置(各省庁のガイドライン等において示されている。)

※ ●データベースへのアクセス制御 ●ワンタイムパスワード等 ●不要アカウントの無効化 ●管理者権限の分割 ●アクセス記録 ●ウイルス対策ソフトウェアの有効性確認 ●データ移送時の秘匿化 ●ファイアウォールの設置 ●ウイルスソフトウェアの導入

(2) 従業員に対する必要かつ適切な監督

(3) 委託を受けた者に対する必要かつ適切な監督

(4) データ内容の正確性の確保等 (改正点・**消去の努力義務が規定された**)

※個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、**利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。** (以前からのガイドラインに既に努力義務であるとされている為、大きな変更点では無いが、法律として規定された。)

■ マイナンバー法の安全管理措置は2016年1月から適用がある (従業員100人以下等の事業者に軽減措置あり)

# ※企業が具体的に実施すべき項目

※下記は一般的な呼称となっております。各企業様毎に置き換えて対応願います。

## 規定・様式 Pマーク/ (ISMSカッコ内)

- ・組織図
- ・法令・法規・ガイドライン一覧表
- ・個人情報一覧表 (情報資産表)
- ・業務フロー図 リスク分析表
- ・個人情報取り扱い同意書
- ・社員情報の取扱いについて
- ・個人情報管理規程
- ・情報システム規程
- ・教育 規程 教育マニュアル

## 企業が実施すべき項目

- ・個人情報保護委員会の新設及びその権限
- ・法令・ガイドライン見直し
- ・個人情報適用範囲分追加
- ・追加分 リスクアセスメント
- ・追加分あれば修正
- ・追加分あれば再取得
- ・新ルール策定 規定変更
- ・新ルール策定・システム設定・規定変更
- ・再教育実施

### まとめ

個人情報の保護に関する法律が、2015年9月（約10年ぶり）改正され、  
今後2年以内の施行が見込まれています。

法律が施工前に具体的に実施しなければならない項目を事前に確認し、  
準備を早めに進めておくことがよいでしょう。

下線の箇所が個人事業主（フリーランス）用の周知文書となります。

## マイナンバーを正当な理由なく、故意に漏洩した場合は4年以下の懲役 または200万円以下の罰金

### その1

マイナンバーは大切に管理 口外しない！ 許可無く収集しない！

- ・マイナンバーは、一生使うものです。番号が漏えいし、不正使われるおそれがある場合を除き、一生変更されませんので、大切にしてください。法律に規定があるものを除いて、マイナンバーを含む個人情報を収集したり、保管したりすることを禁止しています。※くれぐれも、人の目に触れないように取扱いは注意してください。（紙に書いてある場合は放置しない、SNS等で公開しない、**他人のマイナンバーを収集しない**）

### その2

自社の担当者以外からはマイナンバーは収集しない。

- ・マイナンバーは2015年10月から、みなさまの住民票の住所先に届いています。**また個人事業主（フリーランス）の委託先へ年間5万円以上発注をした場合はマイナンバーを収集する必要があります。該当する個人事業主（フリーランス）へは取扱担当者から収集します。発注担当者から個人事業主（フリーランス）へマイナンバーを直接収集することは原則禁止です。**

### その3

マイナンバーに関連するシステム等の開発引き合い時は 即 管理者へ相談

- ・マイナンバーに関連する案件の引き合いがあった場合は、必ずリスクを考える必要があります。万が一漏洩した場合のリスクを想定しなければならない為 この場合は情報セキュリティ管理責任者へ直ぐに（引き合いがあったら直ぐ）相談してください。

# よくある質問

- Q1 : マイナンバーを請求書に同梱してもよいか？
- A1 : 請求書と一緒に送付してくると、担当者（発注をした営業担当者、ディレクター、コーディネーター等）がマイナンバーに目に触れることとなります。その際に紛失のリスクがひそみます。
  
- Q2 : 経理が請求書に同梱するマイナンバーを仕分けすればよいか？
- A2 : 請求書仕分けだけでも大変な作業となります。封筒にマイナンバーを取り扱う担当者名を記載して 親展 で送付してもらった方が全部の封筒を確認する必要がありません。
  
- Q3 : 封筒にマイナンバー在中と記載してよいか？
- A3 : NGです。（配送中 盗み見される恐れあり）
  
- Q4 : マイナンバーはいつまで保管するか？
- A4 : 原則個人事業主の方は、契約期間が終わって 翌年までは必用ですが、その期間がなくなれば廃棄しても構いません。
  
- Q5 : マイナンバーで年間5万円支払いがいかないかたでも収集が必要？
- A5 : 原則不要です。
  
- Q6 : 収集した個人事業主のマイナンバー提供先は？
- A6 : 個人事業主の場合、マイナンバーは税務署への支払調書の提出だけです



# 年内実施する為の想定スケジュール案

## 項目

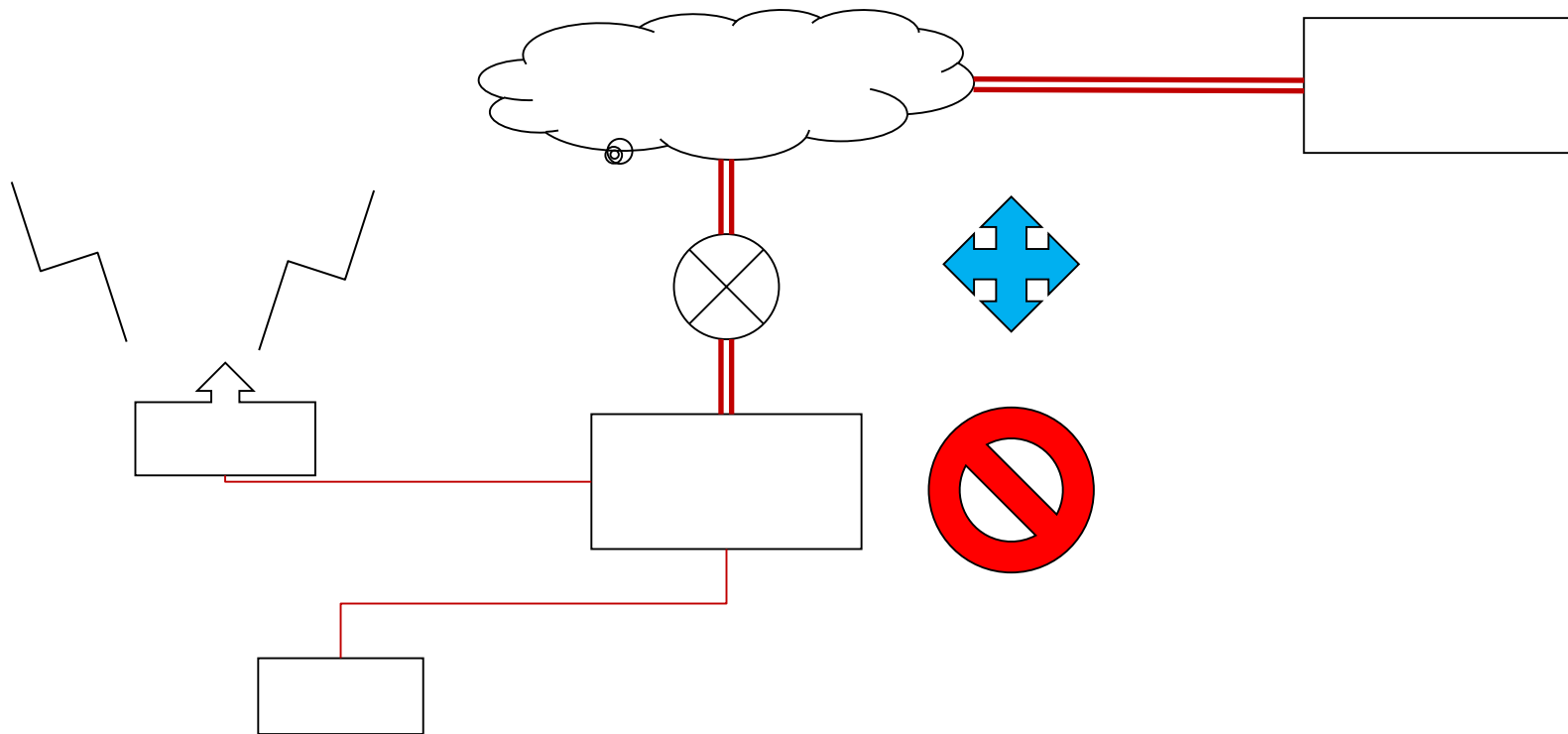
## 具体的な実施内容

## 実施者

現状分析	・マイナンバー収集 フロー リスク分析（データフロー 図修正）・通知文書 作成	個人情報管理責任者
対象調査	・各部門にて個人事業主 5万円OVERの発送分リストアップ	各部門セキュリティ委員の メンバー当に依頼
事前通知	・メールにて 個人事業主 マイナンバー収集の対象者へ 事前通知（本文マイナンバー収集の 依頼 添付ファイ ル ①通知文 『※②委託先調査票 ③情報セキュリティ についてのしおり（外部委託先）』（※②③は推奨）	各部門セキュリティ委員の メンバー当に依頼
発送	・マイナンバー 1回目 収集分 通知発送 ※既に年間5万円over確定分 もしくは 確実に超えると 想定される方対象	経理（事務取り扱い担当 者）（※マイナンバー専任 の担当）
収集	・マイナンバー 個人事業主分 1回目 収集	経理（事務取り扱い担当 者）（※マイナンバー専任 の担当）
発送	2016年度分 収集 ・マイナンバー 2回目 収集 ※1回目 発送分から 5万over 確定分	経理（事務取り扱い担当 者）（※マイナンバー専任 の担当）
収集	2016年度分 収集 ・マイナンバー 個人事業主分 2回目 収集	経理（事務取り扱い担当 者）（※マイナンバー専任 の担当）

# 実施事項まとめ (下線が追加)

- 担当者の明確化と番号の取得 ⇒ 組織図 と 担当者の役割
- 社内アナウンスと教育 ⇒ 教育内容の確認と担当者選定
- 番号の収集時期のアナウンス ⇒ 実施時期選定 (予定でも可)
- 方針の明確化と規定、様式整備 ⇒ セキュリティポリシー  
マニュアルの整備
- 安全管理措置の検討 ⇒ 現行のシステム見直し  
必要であれば、機器導入検討
- 影響範囲特定 (マイナンバー導入) ⇒ 実施対象者、特定のルール化
- 業務分析 (個人番号取扱業務) ⇒ 実施担当者の選定  
現行ルールの見直し
- リスク分析 (個人番号取扱業務) ⇒ リスクが高い場合は  
ルールの見直し
- 委託先 送付住所 リストアップ ⇒ 5万円OVERか 正しい住所の確認
- 送付先 案内文書作成 ⇒ 特定個人情報収集の案内文書  
収集用紙作成



- ルーター
- ファイアウォール
- 無線LANアクセスポイント
- ハブ
- スイッチ

# 次回 開催のご案内

2016年9月 21 日（水） 18時30分開始  
株式会社エスケイワード名古屋本社 セミナールーム  
愛知県名古屋市東区泉一丁目21番27号

泉ファーストスクエア 9階

主催：株式会社エスケイワード コンサルティング事業部

セッション1：最新セキュリティトピックス

『防災 BCPを今一度 考える（自然災害時）』

セッション2 情報セキュリティ管理者のための、  
情報システム基礎知識講座 第3回目

（計 5回開催） 『サーバ編（ハードウェア、ソフト  
ウェア）について』