平成28年度更新事業者向け説明会

1.トピック
2.事業者のセキュリティインシデントと対応（JIPDEC　IT-REPORT2016より）
3.個人情報保護法等の法令改正状況
4.Pマーク審査での指摘事項/継続的改善事項（例）
5.マイナンバー制度とPマーク審査
6.ストレスチェック制度とPマーク審査
7.効果的なPMS運用に関して
8.中産連事務局からの連絡
9.個別相談

一般社団法人　中部産業連盟
Pマーク審査センター

トピック

- Pマーク付与認定状況（平成28年3月現在）
  - 全国：昨年度/2年間
    - 7538社/14755社
  - 中産連：昨年度/ 2年間
    - 472社/895社
- セキュリティ事故
  - J社の事例
  - 標的型メール
  - その他（セキュリティネクストHP）
- JIPDEC関連
  - マイナンバー/ストレスチェックに関するFAQを随時更新中

セキュリティインシデント：2015年（JIPDEC　IT-REPORT2016より）

項目	比率
従業員によるデータ、情報機器の紛失、盗難	23.1%
社内PCマルウェア感染	22.5
スマホ、携帯電話、タブレット等の紛失盗難	17.0
USBメモリ等の紛失盗難	12.8
人為的ミスによる個人情報の漏えい・逸失	11.9
標的型サイバー攻撃	9.5
なりすましメール受信	8.3
WEBサイトへの不正アクセス	7.1
内部不正による個人情報の漏えい・逸失	6.7

概要

- 国内事業者627社回答/2000社（2016年1月調査）
- 製造、サービス、情報通信、卸/小売等
- セキュリティインシデントとは
  - 事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故
- マルウェアとは
  - 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称、ウィルス、ワーム、スパイウェア、キーロガー等

スマートデバイス/クラウドサービス利用（JIPDEC　IT-REPORT2016より）

スマートデバイス利用状況

項目	50%以上で利用	10～50%で利用	予定なし
会社支給のスマホ導入	21%	26.6%	31.1%
会社支給のタブレット導入	13.8	27.7	32.4
私物スマホの業務利用	15.5	12.5	52.4
私物タブレットの業務利用	12.1	12.8	55.8

クラウドサービス/オンプレミス（自社システム）の有利性比較

項目	クラウド	変わらない	オンプレミス
可用性・稼働率の高さ	52.5%	38.5%	9.0%
情報漏えい被害の軽減	39.0	41.1	19.9
データ消失被害の軽減	41.4	46.0	12.6
サイバー攻撃被害の軽減	39.6	45.2	15.2
ログの取得分析	36.9	49.3	13.8
マルチデバイスからのアクセス	47.8	42.4	9.9

BYODを認めていない場合
メールサーバ等へのID/PW以外の認証制限を検討

セキュリティ対策実施状況（JIPDEC　IT-REPORT2016より）

標的型サイバー攻撃対策

項目	実施済
PC管理者のPWの個別化	52.7%
情報資産の隔離	50.4
外部通信の経路制御	49.9
メール添付ファイルフィルタリング	49.6
OS/サーバソフトの脆弱性診断	49.0
クライアントOSのパッチ運用の徹底	47.9
重要データの暗号化	42.9
電子メールの送信者認証	41.8

内部対策

項目	実施済
重要情報へのアクセス制限	55.8%
一般社員向け研修	51.6
外部デバイスへのデータ移動制限	50.1
退職者のアクセス権の早期無効化	50.0
特権ユーザの管理	49.6
PC操作ログの取得保管	47.9
サーバのアクセス権の見直し	46.6
重要情報のログ取得	46.3

個人情報保護法（平成29年4月施行？）

- 「個人情報の定義」の明確化
  - 身体的特徴（指紋/外観等）
  - 要配慮情報（機微情報）
- 「匿名加工情報」に関する加工方法や取扱い（個人情報保護指針の作成や届け出、公表等）の規定を整備
- 第三者提供に係る確認及び記録の作成
- 「不正な利益を図る目的による個人情報データベースの等提供罪」の新設
- 「特定個人情報保護委員会」を「個人情報保護委員会」へ
- グローバル化対応
  - 国境を越えた適用と外国当局への情報提供
  - 国外の第三者へ個人データを提供する規定
- 本人同意を得ない第三者提供の届出や公表等
- 取扱う個人情報が、5,000件以下の事業者への対応

経済産業省ガイドライン（平成26年12月改正）

- 第三者からの適正な取得の徹底
  - 第三者から個人情報を取得する場合には、適法に入手されていること等を確認することが望ましい旨追記
  - 適法に入手されていることが確認できない場合は、取引を自粛することを含め、慎重に対応することが望ましい旨追記
- 社内の安全管理措置の強化
  - 外部からのサイバー攻撃対策の追加
  - 内部不正対策の組織的、物理的、技術的安全管理措置の項目の追加
- 委託先等の監督の強化
  - 内部不正対策の委託先の安全管理措置の確認、定期的な監査等の追加
  - 再委託先以降も同様の措置を行うことが望ましい旨追記
- 共同利用制度の趣旨の明確化
  - 事業者が共同利用を円滑に実施するために共同利用者における責任等を追加
  - 共同利用者の範囲の明確化
- 消費者等本人に対する分かりやすい説明のための参考事項の追記

その他の法令改正等

- 不正アクセス防止法（平成25年改正）
  - 他人の識別符号を不正に取得/保管の禁止、処罰
  - 識別符号の入力を不正に要求する行為の禁止、処罰
  - アクセス管理者の防御措置
    - 識別符号等の適切管理
    - アクセス制御機能の検証および高度化
    - 正アクセス行為から防御するために必要な措置
- 不正競争防止法（平成27年改正）
  - 営業秘密や営業ノウハウの盗用等の不正行為を禁止
  - 他人の商品のデッドコピー商品の取引禁止
  - コピー・プロテクション迂回装置の提供等を禁止
  - 罰則の強化
- 愛知県/岐阜県/石川県/名古屋市/金沢市等の自治体の個人情報保護条例は、平成27年7月や10月に改正
- 特定個人情報に関する記述追加

以下のサイトも参考に

JIPDECの更新事業者向けサイト
https://privacymark.smktg.jp/public/authapi/login?api_key=4e79a0fdc5dbb5af785d9bb3610f68af&api_sig=579f723c356ceb36493b4694d41cfc367cecbac5&callback_url=https://member.privacymark.jp

中産連サイト
http://www.chusanren.or.jp/pmark/link.html

審査で見受けられる指摘/改善事項（例）

- 個人情報の特定/リスク分析対策
  - 新たな個人情報を特定/リスク分析対策していない（マイナンバー等）
  - 個人情報の取り扱い局面に応じて、リスク分析対策していない（クラウドサービスの利用等）
- 法令、国が定める指針等
  - 法令等の改正状況を確認できていない
- 委託先の監督
  - 委託先の重要な個人情報の取り扱いを確認していない
- 安全管理措置
  - 規定された措置を実施していない（パスワードの定期的更新）
  - リスクに応じた措置を適用していない（アクセスログの取得点検）
  - スマホ/タブレット端末等の安全管理措置を規定していない
- 運用の確認/内部監査
  - リスクに応じた運用の確認項目でない
  - 個人情報の取り扱い状況を監査していない
- 代表者による見直し
  - 内部監査以外のPMS運用状況、諸環境の変化、法令等の改正状況を考慮した見直しでない

クラウドサービス利用開始時の事業者の確認項目

項目	内容
利用範囲	利用範囲は明確か
	サービスの種類とコストはどの程度か
	社内ルールとの整合性は確保されているか
利用準備	管理担当者を選任したか
	ユーザとパスワード管理は適切か
	サービス停止に備えてデータをバックアップしているか

項目	内容
提供条件	提供事業者の信頼性は（ユーザー数/事業年数）
	サービスの稼働率、障害発生頻度、障害時の回復目標時間等のサービスレベルは
	セキュリティ対策は公開されているか
	ヘルプデスク/FAQ等は提供されているか
	サービス終了時のデータの処分は

クラウドサービス利用のための情報セキュリティマネジメントガイドライン（平成25年）
中小企業のためのクラウドサービス安全利用の手引き（平成23年）

マイナンバーに関する情報（1/2）

- 行政の状況
  - 積極的に届け出書類（雇用保険等）に個人番号の記載を要求していない様子?
- 事業者の状況
  - 「特定個人情報管理規程を作成」or「PMSを見直し」
  - 従業員からマイナンバーを取得している（通知カードコピーorクラウドサービス利用）
  - キャビネット等に施錠保管
  - 行政への届出等への記載事例は、数例程度
  - 税理士/社会保険労務士へ取り扱い委託している事例も
- 事業者の対応
  - 「特定法令一覧」等に、個人番号法/「特定個人情報ガイドライン（事業者）」を追加
  - 個人情報の特定/リスク分析対策を実施
  - 特定個人情報の取り扱いや利用目的等を従業者に説明
  - 事故発生時の報告先に「個人情報保護委員会」を追加
  - 取扱い責任者/取扱い担当者の選任（総務/社長等）
  - 取扱い区域/保管区域の設定
  - 取り扱い委託先の評価/覚書

マイナンバーに関する情報（2/2）

- 審査状況
  - 直接的に個人番号法の適用状況を審査するわけではない
  - PMSで取り扱う個人情報の一つ
  - 具体的な運用等についてはFAQ参照
    - http://privacymark.jp/privacy_mark/faq/mynumber.html
- 関連情報
  - 社会保険労務士/税理士等のPマーク申請が増加
  - クラウドサービス利用が増加
- 指摘事項例
  - 新たな個人情報として、特定/リスク分析対策していない（クラウドサービス利用を含む）
  - 適用法令等として特定していなくて、実施事項を把握していない
  - 緊急事態の連絡先として、「個人情報保護委員会」を追加していない
  - 委託先の取り扱い状況について、全く確認していない

マイナンバーに関する審査確認事項（1/3）

- 個人情報の特定
  - 手順に従い、特定個人情報を個人情報として特定/更新しているか
- 法令、国が定める指針その他の規範
  - 番号法及び特定個人情報ガイドライン（事業者編）を特定/更新しているか
  - 該当する新たな順守事項を規定等へ反映しているか
- リスク認識分析及び対策
  - リスク認識分析及び対策して、新たな管理策が必要であれば規程等へ反映しているか
- 資源、役割、責任及び権限
  - 特定個人情報取扱い事務担当者の役割,責任権限を明確にしているか
- 直接書面による取得/直接書面以外での取得
  - 利用目的を明示/同意を得て取得しているか
    - 既存従業者等へは、規定/教育等で通知しているか
  - 個人番号を取得する場合、本人確認/番号確認しているか
  - （受託業務等の場合）利用目的を通知又は公表しているか

マイナンバーに関する審査確認事項（2/3）

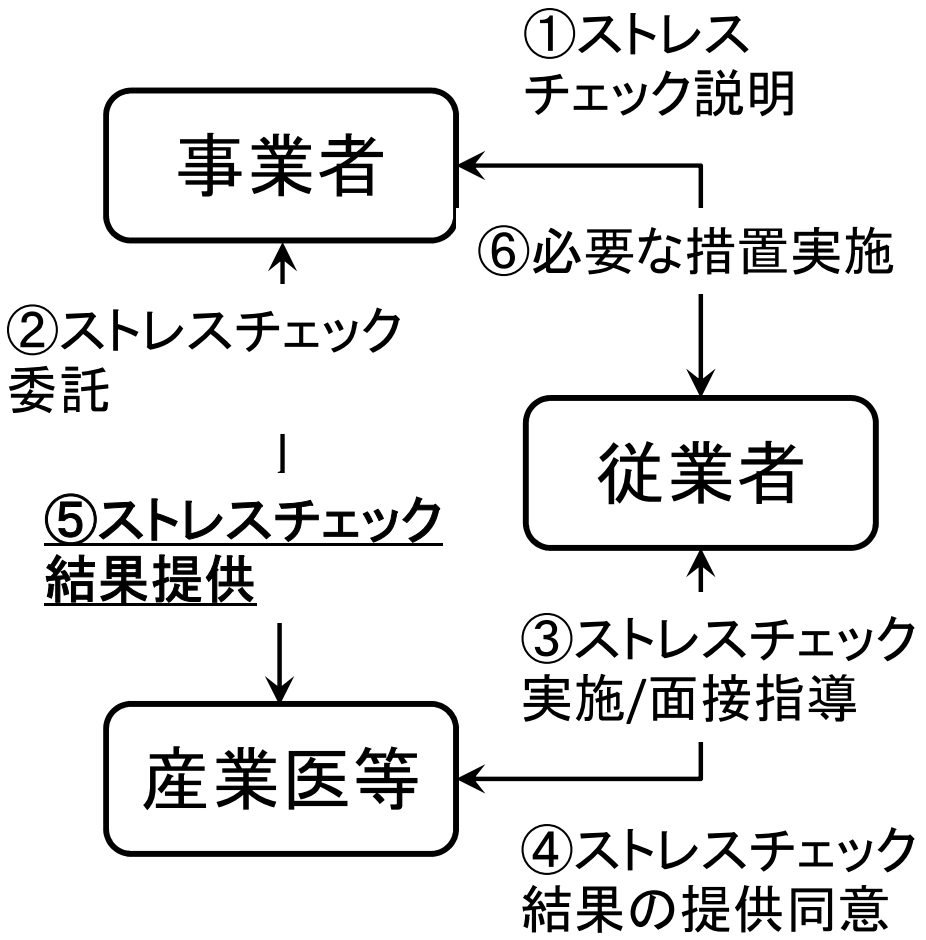
- 個人情報の利用、アクセス、第三者提供
  - 特定個人情報の利用目的を出来るだけ特定しているか（税と社会保障の事務手続き）
  - 番号法の利用目的を超えた利用を禁止しているか
  - 番号法の規定以外の第三者提供を禁止しているか（本人の同意を得ても）
  - 個人番号の共同利用は、原則禁止しているか（他の事業者の閲覧/利用等）
  - 出向/転籍等の場合の個人番号の移動は、本人がコントロールしているか
- 正確性の確保
  - 特定個人情報の保管期間を規定しているか
- 安全管理措置
  - 特定個人情報の保管期間を過ぎたら速やかに処分しているか
  - 処分記録を維持しているか
  - 特定個人情報の取扱いに関する新たな安全管理措置は規定されたか

マイナンバーに関する審査確認事項（3/3）

- 委託先の監督
  - 特定個人情報に関する委託先を、その管理の程度で評価選定しているか
  - 以下を含んだ契約内容か
    - 特定個人情報の持ち出し禁止、目的外利用の禁止、再委託の条件、漏えい事案等の委託先責任、特定個人情報の返却又は廃棄、従業者の監督教育、契約内容順守の報告
  - 再委託事項に関して、規定しているか
    - 再委託の場合の、委託元承諾
    - 再委託先の監督
- 教育
  - 事務取扱い担当者や一般従業者へ教育しているか
- 運用の確認
  - 特定個人情報の取扱いについて、運用確認しているか
- 監査
  - 特定個人情報の取扱い状況を監査しているか
- 代表者による見直し
  - 特定個人情報の取扱い対応に関してインプットしているか
  - その対応についてレビューして、決定しているか

ストレスチェックに関する情報（1/2）

- 制度概要
  - 「労働安全衛生法（平成26年6月改正）」で、規定され、平成27年12月から運用開始
  - 従業者に対して、医師/保健師等による「ストレスチェック」を義務付け（労働者50人未満の事業場は努力義務）
  - 検査結果は、医師師等から直接本人に通知（本人の同意なく事業者に提供禁止）
  - 高ストレスと判定された従業者から申出があった場合、医師による面接指導
  - 面接指導の結果に基づき、医師の意見を聴き、必要に応じ就業上の措置を実施



ストレスチェックに関する情報（2/2）

- 関連ガイドライン等
  - 雇用管理分野における個人情報保護に関するガイドライン（平成27年11月）
  - 雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項（平成27年11月）
  - 労働安全衛生法に基づくストレスチェック制度実施マニュアル（平成28年4月）
- 事業者の準備対応
  - 産業医/社会保険労務士等に相談して、準備中
- Pマーク審査での対応
  - 事業者が取り扱う新たな特定の機微な個人情報として審査
    - 手順に基づく、個人情報の特定/リスク分析対策の実施
    - ガイドライン等の特定
    - 直接書面以外の取得なので利用目的の通知又は提供（提供するのは産業医等）
    - 産業医等は、委託先は該当するが評価選定/覚書迄を求めない

より効果的なPMS運用に関して

- JISQ15001規格3.1
  - 事業者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ改善しなければならない
  - 審査基準
    - JISQ15001規格
    - 個人情報保護マネジメントシステム実施のためのガイドライン
    - （特定法令/ガイドライン）
  - 審査での考慮事項
    - 事業規模や事業内容
    - 事業者の個人情報の取り扱いリスク低減
    - 諸環境の変化に伴うPMSの見直しや有効性向上
- 委託先の監督
  - メリハリのある委託先の評価選定
  - 個人情報の取り扱い状況の確認、約款類の確認
- 教育
  - 個人情報の取り扱いの程度に応じて
  - 社内の情報セキュリティルールの浸透
  - 新たなリスクへの対応
- 運用の確認/監査
  - 運用の確認項目/監査項目の見直し
  - 記録の確認＋ヒアリング＋現地現物の確認

中産連事務局からの連絡(1/2）

- Pマーク有効期限内の更新
  - 有効期限の8か月前に更新連絡
  - 4か月前までに申請（有効期限後の申請は、不受理）
  - 2か月前までに現地審査
- 「審査打ち切り」について
  - 現地審査指摘事項の送付日から、3か月以内に改善報告
  - 6か月を過ぎて改善完了しない場合、審査機関の判断で審査打ち切りが可能（制度運営要領改正/指摘事項文書に明記）
- 確認審査の運用開始
  - 更新事業者に対して、2年毎の更新審査以外の審査が可能になりました。例えば、
    - 更新審査では行けない遠方の事業拠点を審査
    - 個人情報の取り扱いや事業者規程を主体にした第三者監査
  - 希望事業者は、別途事務局まで連絡下さい

中産連事務局からの連絡(2/2）

- 審査料の請求時期変更
  - 現地審査の翌月末日⇒現地審査翌月10日
  - 当月の審査会で登録判定/更新判定する場合は、審査会前迄に
- 指摘事項/改善報告の授受方法変更
  - 書面だけ⇒書面and電子メール添付ファイル（PW保護）（運用開始）⇒ファイル転送サービス利用も追加（検討中）
- 改善報告書式変更
  - 一覧表形式⇒事業者の「是正処置報告書」を使用（10月以降の現地審査から）
- 現地審査後のアンケート
  - 中産連からのアンケートは休止（ご協力ありがとうございました）⇒新規申請事業者に直接訪問
  - JIPDECのアンケートは継続（電子メール/WEB）