日印産連・プライバシーマーク審査センター

平成27年度　第1回「個人情報保護研究セミナー」
―個人情報保護の最新情報の理解とサイバー攻撃脅威への備え―

平成 27 年 10 月 13 日（火）に日本印刷会館において、情報セキュリティ部会主催の「個人情報保護研究セミナー」が開催された。

9 月 3 日、個人情報保護法とマイナンバー法の両改正案が可決、成立しました。一方で、標的型攻撃メールによって日本年金機構から個人情報の漏えいに至る被害が発声し、サイバー攻撃の脅威に社会は不安を募らせています。

本セミナーでは、改正個人情報保護法の改正ポイント、サイバー攻撃へのセキュリティ対策等をテーマに解説し、参加者 150 名は理解を深めた。

以下に講演内容の主な点を示します。

Ⅰ.『改正個人情報保護法及び番号利用法（マイナンバー法）の解説』

慶應義塾大学 総合政策学部　　教授　新保　史生

「個人情報の保護に関する法律及び行政手続きにおける特定の個人を識別するための番号法の利用等に関する法律の一部を改正する法律」（平成 27 年 9 月 9 日法律第 65 号）についての解説があった。

1. 法改正の意義と論点

(1) 形式的な個人情報保護から実質的な個人情報保護へ
- 個人情報は基本情報とそれに付加されるプライバシーに関する情報により色分けする
- プライバシー保護（非公知情報、機微情報）への取組み

(2) 裏活用から利活用へ
- 安易な匿名化による脱法的な「裏利用」から適正な手続きに基づく「利活用」へ

(3) 本来の規制目的と実際の法適用及び運用における新たな課題発生の可能性
- 第三者提供にあたっての個人データの取り扱いに（第三者提供）に係る記録義務
- 匿名加工情報（個人情報には該当しない情報）の取り扱いにあたっての新たな義務

(4) 新たな過剰反応・過小評価への懸念
- 不十分な理解や誤解に基づくもの
- 法令順守意識の軽視によるもの

(5) 個人情報保護委員会への期待
- 今回の法改正の最重要課題はプライバシーコミッショナー制度（第三者機関）の創設
- 個人情報保護委員会の体制整備・委員会の機能強化が重要な課題

2. 改正法のポイント

改正法と現行法の主な相違点は以下であり、新設、修正がなされた。

(1) 個人情報の定義 **（修正）**
- 「個人情報」の定義（範囲）に変更なし
  →定義の明確化のための明記・追加

(2) 匿名加工情報 **（新設）**
- 特定の個人を識別することができないよう加工した情報

(3) 利用目的制限の緩和 **（微修正）**
- 「相当の」が削除される
  →利用が可能となる場面は?

(4) 機微情報（要配慮個人情報）の取得制限 **（新設）**
- 差別の要因となる個人情報の取得は禁止

(5) 個人データの第三者提供に係る確認及び記録の作成の義務付け **（新設）**

(6) 不正な利益を図る目的による個人情報データベース提供罪 **（新設）**
- 不正な利益を図る目的での個人データベース等の提供・盗用
  →罰則の適用

(7) オプトアウト規定 0 の見直し **（修正）**
- オプトアウトを実施する場合
  →個人情報保護委員会への提出→委員会から公表

(8) 小規模事業者の適用除外撤廃 **（削除）**
- 誰もが、個人情報保護法を遵守する義務を負う

(9) 消去の努力義務 **（修正）**
- 個人データを利用する必要がなくなったとき
  →遅滞なく消去

(10) 開示等請求権 **（修正）**
- 開示、訂正等、利用停止等の請求を裁判上の権利として明記

(11) 個人情報保護委員会の設置 **（新設）**
- 監督権限の統一・明確化／立入検査も含む執行権限の強化

(12) グルーバル化への対応 **(新設)**
- 国境を越えた個人情報の取扱いにも法執行
- 外国執行当局への情報提供
- 個人データの外国にある第三者への提供の制限

II.『被害に遭わないために実施すべき対策は？ ～守るべきものをしっかり守ろう～』

独立行政法人 情報処理推進機構　技術本部 ｾｷｭﾘﾃｨｾﾝﾀｰ
情報ｾｷｭﾘﾃｨ技術ﾗﾎﾞﾗﾄﾘｰ　研究員　　土屋　正

サイバー攻撃対応の最前線にあって啓発活動を続けている、独立行政法人　情報処理推進機構（IPA）から、企業にとって必要とされている対策の解説があった。

1. 情報セキュリティ対策の基本

(1) 5つの基本対策

①ソフトウェアの更新
- ソフトウェアの欠陥である脆弱性は、ソフトウェアを更新して根本的に解消する。

②ウイルス対策ソフトの導入
- ウイルス対策ソフトを導入し、流行しているウイルスの感染を未然に防ぐ

③パスワードの適切な管理と認証の強化
- 推測されにくい「記号・英数字」を含む「十分な文字数」のパスワードを設定
- 複数のウェブサービスでパスワードを使い回さない
- 二要素認証等、強い認証方式が利用できれば利用する

④設定の見直し
- 不要な設定は無効にする
- フォルダや顧客管理システム等へのアクセス制限を適切に行う

⑤脅威や手口を知る
- 新聞やインターネット等から情報を自発的に収集し、被害に遭わないよう手口を事前に知る

(2) 2つの考え方

①対策の考え方「資産を守る」
- 新たな脅威に備えたセキュリティ対策手法の例示を追加
- 「共同利用」制度の趣旨の明確化等
- 消費者に対する分りやすい説明のための参考事項を追記

②対策の考え方「多層防衛」
- 第三者からの適正な取得の徹底
- 社内の安全管理措置の強化
- 委託先等の監督の強化

(3) 10大脅威における基本対策の効果

2014年において社会的影響が大きかったセキュリティ上の脅威について表1のとおり順位付し、10大脅威における基本対策の効果を示す。

表1　10大脅威における基本対策の効果

順位	脅威	5つの基本対策				
		ｿﾌﾄｳｪｱの更新	ｳｲﾙｽ対策ｿﾌﾄ	ﾊﾟｽﾜｰﾄﾞの強化	設定の見直し	手口を知る
1位	インターネットバンキングやクレジットカード情報の不正利用	○	○	○		○
2位	内部不正による情報漏えい	○	○	○	○	○
3位	標的型攻撃による諜報活動	○	○	○	○	○
4位	ウェブサービスへの不正ログイン	○	○	○		○
5位	ウェブサービスからの顧客情報の窃取	○	○	○	○	○
6位	ハッカー集団によるサイバーテロ	○	○	○	○	○
7位	ウェブサイトの改ざん	○	○	○	○	○
8位	インターネット基盤技術を悪用した攻撃	○	○		○	○
9位	脆弱性公表に伴う攻撃	○	○		○	○
10位	悪意のあるスマートフォンアプリ		○		○	○

凡例：○ 対策効果あり、または部分的に効果あり

2. 注目すべき課題や懸念

(1) 今後の課題や懸念から紹介

迅速に対応できる体制の構築が不可欠であり、脆弱性の公表や事件発生に対応できる体制作りが必要。
- 様々なセキュリティの問題に迅速に対応するため、組織としての体制が求められる

(2) 迅速な対応が求められた2014年の事例

- 広く利用されている製品の脆弱性が相次いで公表

サーバーソフトウェア：Apache、Struts、OpenSSL、Bash 等
クライアントソフトウェア：Internet Explorer、Adobe Flash Player 等
- 内部不正による情報漏えい事件が発生

ベネッセ、3,504 万件の顧客情報が漏えい

(3) 体制を構築するには

- 経営層が対策の実施に責任を持つ
- 体制構築と継続的な対策の実施のために予算を確保
- 企業・組織内にセキュリティ対策チーム「CSIRT」（シーサート）を設置

－参考－

IPA　独立行政法人　情報処理推進機構
セキュリティセンター
http://www.ipa.go.jp/security/

【次回セミナーのお知らせ】
平成 27 年度　第 2 回「個人情報保護研究セミナー」は、平成 28 年 3 月 22 日（火）13：00 ～ 16：00 に