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2回「個人情報保護研究セミナー」
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ー

平成28年3月22日(火)に企業行動委員会 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」が東京で開催された。

本セミナーでは、「改正個人情報保護法の詳解」、「高度化するサイバー攻撃への備え」をテーマに解説し、100名弱の参加者が理解を深めた。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の詳解』

慶應義塾大学
総合政策学部 教授
新保 史生 氏

「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）についてパーソナルデータの位置づけ、制度改正の骨子、認定個人情報保護団体の役割り等の詳細な解説があった。

1.改正法のポイント

改正法について詳細な解説があった。

(1) 個人情報の定義

「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

・「個人識別符号」の定義の明記
　① 身体特徴量
　② 役務利用、商品購入又はカード等に付される符号
・「要配慮個人情報」、「匿名加工情報」、「匿名加工情報取扱事業者」、「匿名加工情報データベース等」の定義の追加

(2) 匿名加工情報

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（個人情報として復元できないもの）

・個人情報取扱事業者としての義務：
　【作成】加工方法／公表／明示／復元の禁止
・匿名加工情報取扱事業者としての義務：
　【提供】公表／明示
　【識別行為の禁止】再識別化の禁止【安全管理措置等】

(3) 利用目的制限の緩和

「相当の」が削除される→利用が可能となる場面は？

(4) 要配慮個人情報の取得制限

差別の要因となる個人情報の取得を禁止

・本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実
・不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述

(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

【提供する場合】：記録 提供した年月日、提供先の第三者の氏名又は名称その他の委員会規則で定める事項
【提供される場合】：確認 ① 提供元の氏名又は名称及び住所
② 取得の経緯
記録 提供を受けた年月日、確認に係る事項
その他の委員会で定める事項

(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

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) オプトアウト規定の見直し

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
1.第三者提供すること　2.個人データ項目　3.提供の手段又は方法　4.求めに応じた提供停止　5.本人の求めを受け付ける方法

(8) 小規模事業者の適用除外撤廃

誰もが、個人情報保護法を遵守する義務を負う
特定の個人の数が5000件以下の小規模事業者の適用除外規定が削除される

(9) 消去の努力義務

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
個人データのクリーニング、不要な情報の消去（削除ではない）

(10) 開示等請求権

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

監督権限の統一・明確化／立入検査も含む執行権限の強化
苦情処理は「認定個人情報保護団体」が実施

(12) グローバル化への対応

① 国境を越えた個人情報の取扱いにも法執行
② 外国執行当局への情報提供
③ 個人データの外国にある第三者への提供の制限

2. 個人情報取扱事業者の義務の改正事項

トレーサビリティ確保の手続に関して詳細な解説があった。

(1) 第三者提供に係る記録の作成等

・適法な個人情報データの提供と個人情報の適正な取得を確認するための手続
　① 第三者提供時の記録
　② 第三者提供を受ける際の確認と記録に関する手続
　③ 個人情報データベース等提供罪

(2) 提供する際の手続（国内の第三者への提供）

・個人データを第三者に提供したときの記録作成義務
　① 年月日
　② 第三者の氏名又は名称
　③ その他の個人情報保護委員会規則で定める事項に関する記録
　記録を作成した日から個人情報保護委員会規則で定める期間保存

(3) 提供する際の手続（外国にある第三者への提供）

・提供元の個人情報取扱事業者と法人格が別の関連会社や子会社も第三者

(4) 提供を受ける際の手続

・個人データの提供を受ける際の提供（受領側）における確認義務
　① 提供元である第三者の氏名又は名称及び住所・法人等は代表者の氏名
　② 提供元である第三者による当該個人データの取得の経緯

(5) 第三者提供の制限を受けない手続

・匿名加工情報の取扱いに係る手続
・匿名加工情報の提供にあたっては、「本人同意」を得ることなく提供が可能

Ⅱ.『高度化するサイバー攻撃に備えて』
～予防・防御では間に合わない 最近のセキュリティ事情とその対策～

NPO法人 日本ネットワークセキュリティ協会 講師
（株式会社ディアイティ セキュリティサービス事業部 部長）
山田 英史氏

企業にとって必要な情報セキュリティリスクの認識から、サイバー攻撃の入口・内部・出口対策からログ管理によるセキュリティ強化についての分り易い解説があった。

1. 進化するサイバー攻撃

(1) サイバー攻撃とは

サイバー攻撃の主要な形態には、ウェブサイト等に大量の通信を送り付け、サービス提供を妨害する行為（サービス停止攻撃）、様々な攻撃手法を組み合わせて情報・データの窃取・改ざん・破壊やシステムの機能阻害等をもたらす攻撃（標的型攻撃）等がある。

(2) 最近のサイバー攻撃の特徴と対策のポイント

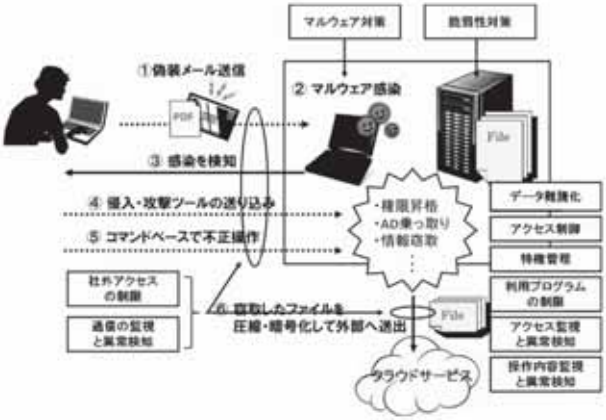
① 最近のサイバー攻撃の特徴

② サイバー攻撃対策のポイント

- 侵入されていることを前提に考える
- いかに早く異常を検知するか
- いかに情報流出を最小限にするか
- いかに流出情報を不正利用されないようにするか

※可能なら! 重要情報を扱うシステムはインターネットから隔離する。

(3) サイバー攻撃対策



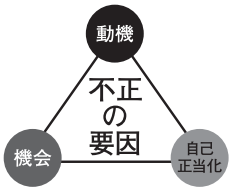
2. 無視できない内部不正

(1) 無視できない内部不正（2005年～2013年）

漏えい人数（母数：105,400,241人）

1位	管理ミス	37.95%
2位	**内部犯罪・内部不正行為**	**18.68%**
3位	不正アクセス	12.82%
4位	紛失・置き忘れ	11.83%
5位	盗難	4.39%

(2) 不正のトライアングル



① 動機

- インセンティブ（換金性、組織に対する仕返し等）
- プレッシャー（借金、待遇への不満等）

② 機会

- 働いている場所、使える時間、利用できる環境（端末、高速ネットワーク等）、権限（管理者権限、知りえる内部情報等）、力量（専門知識、技術スキル等）

③ 自己正当化

- 組織の姿勢・合理化、社員の論理観の欠如など

※ITセキュリティでは機会をいかに少なくするかがポイント

(3) アクセス権管理、検知、抑制がポイント

① アクセス管理

- 各自に一意のID
- 最少人数への権限付与
- 役割に応じた最小の権限
- 権限の分割
- 権限とID見直し

② 検知

- アクセスの成功、失敗
- 閾値（いきち）を逸脱するアクセス

③ 抑止

- 相互牽制
- 秘密保持誓約書への署名
- 記録（ログ、監視カメラ）
- 退職者の利用していたハードディスクの保存

3. 検知・監視能力を高める

(1) ログ管理によるセキュリティ強化

- ログ（記録）の生成

分類	装置	ログ（記録）
コンピュータ	PC端末	・イベントログ
	サーバ	・イベントログ ・アクセスログ
ネットワーク	ファイアウォール、IDS/IPS、Proxy、ルータ	・通信ログ
物理	監視カメラ 入退室認証装置	・録画映像 ・入退室ログ

(2) ログの目的

- 何かあった時のための記録
- 異常、不正の検知のため
- 異常、不正の監視のため
- 正当性の証明のため

(3) ログの役割

攻撃	ログの利用
標的型攻撃	外部から社内への異常通信の検知・監視（入口）
	社内から外部への異常通信の検知・監視（出口）
	社内から社内への異常通信の検知・監視（内部）
	不正プログラムの起動の検知・監視
	データ容量の変化の検知・監視
	インシデント発生時の原因分析・影響範囲分析
内部不正	サーバへの不審なアクセス検知・監視
	不審な操作の検知・監視
	外部デバイス（USBメモリ、スマホなど）へのデータ持ち出し検知・監視
	インターネット上のデータの転送（メール、オンラインストレージ等）
	入退室記録との突合

（出典） 図等は日本ネットワークセキュリティ協会資料