「プライバシーマーク教育テキスト」 Ver.2019_01

はじめに

個人情報の事故事件が相次いで起こっています。
個人情報をルールに基づいて取扱い、事故事件を防ぎ、保護に努めることは、顧客の期待に応えることになるため、当社にとって重要な課題です。
皆さん一人一人がリスクを意識して、ルールに沿って行動することが重要です。
今回の教育を通じて、あたらめて業務における個人情報の保護を徹底してください。

①個人情報とは

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別できるもの(他の情報と容易に照合することができ､それによって特定の個人を識別することができることとなるものを含む｡)
なお、死者の情報の適正な取扱いと管理が必要であると判断する場合は，　死者の情報も対象とする。

また、平成 29 年 5 月 30 日より全面施行された改正個人情報保護法により、以下「個人識別符号」が含まれるものを個人情報とすることで、時代の変化に合わせてより保護対象が明確になりました。
①身体の一部の特徴を電子計算機のために変換した符号（DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋等）
②サービス利用や書類において対象者ごとに割り振られる符号（旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証等）

②プライバシーマークとは

個人情報を適切に扱っているつもりでも、それを自社で証明することはできません。
そこで、第三者から認定してもらう制度があります。
それが、プライバシーマーク制度です。
プライバシーマーク制度は、審査機関によって審査され、一定の基準を満たすことで認定となった事業者に対し、プライバシーマークの使用を許諾されます。

なお、プライバシーマークを取得、維持するには、継続的に個人情報保護活動を行う仕組み作りを構築する必要があり、この仕組み作りのことを「個人情報保護マネジメントシステム」と言います。

③個人情報保護マネジメントシステムとは

自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。
略称としてＰＭＳ（Personal information protection Management Systems）とも言います。

⑧情報セキュリティ 10 大脅威 2018」（上位 3 位）のご紹介

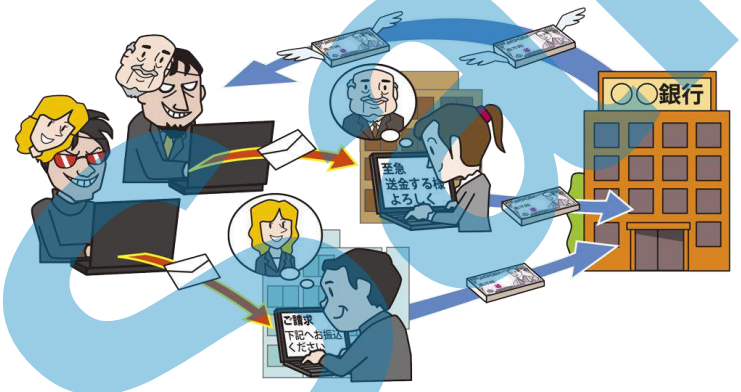
第 1 位　標的型攻撃による被害

企業や民間団体や官公庁等、特定の組織を狙う、標的型攻撃が引き続き発生している。メールの添付ファイルを開かせたり、悪意あるウェブサイトにアクセスさせて、PC をウイルスに感染させる。その後、組織内の別の PC やサーバーに感染を拡大され、最終的に業務上の重要情報や個人情報が窃取される。さらに、金銭目的な場合は、入手した情報を転売等されるおそれもある。

第 2 位　ランサムウェアによる被害

ランサムウェアとは、PC やスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、金銭を支払えば復旧させると脅迫する犯罪行為の手口に使われるウイルスである。そのランサムウェアに感染する被害が引き続き発生している。さらに、ランサムウェアに感染した端末だけではなく、その端末からアクセスできる共有サーバーや外付け HDD に保存されているファイルも暗号化されるおそれがある。組織内のファイルが広範囲で暗号化された場合、事業継続にも大きな支障が生じる。また、2017 年は、OS の脆弱性を悪用し、ランサムウェアに感染した端末が接続しているネットワークを介して感染台数を増やすランサムウェアも登場した。

第 3 位　ビジネスメール詐欺による被害



「ビジネスメール詐欺」は巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもある。以前は主に海外の組織が被害に遭ってきたが、2016 年以降、国内企業でも被害が確認されている。

※「情報セキュリティ 10 大脅威 2018」は、独立行政法人情報処理推進機構(IPA)が 2017 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、IPA が脅威を順位付けしたものです。

詳細は　https://www.ipa.go.jp/security/vuln/10threats2018.html

⑨個人情報取扱いのための基本ルール

以下は、プライバシーマーク認定基準である JISQ15001:2017 から主な原則事項を抜粋したものです。
まず原則事項をご理解下さい。
実務と乖離がある場合や疑問、質問がある場合は、上司や個人情報保護管理者へ相談してください。

(1) 利用目的

1) 個人情報を取り扱うに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な範囲において行う。

(2) 適正な取得

1) 個人情報は、適法、かつ、公正な手段によって取得する。

(3) 要配慮個人情報

1) 要配慮個人情報（人種、信条、社会的身分、病歴、犯罪の経歴等）の取得は、あらかじめ書面による本人の同意を得る。

(4) 個人情報の取得

1) 新種の個人情報（例：新たな事業で取得する従来とは異なる種類のもの）を取得する場合、利用目的の公表を行う。

2) 本人から直接個人情報を取得する場合あらかじめ本人の同意を得る。

※採用応募、Web サイトからの問合わせ等が考えられます

(5) 個人情報の利用

1) 特定した利用目的の達成に必要な範囲内で個人情報を利用する。

2) 関係者以外の閲覧や目的外利用をしない。

(6) 個人情報の提供

1) 個人情報を第三者に提供する場合、あらかじめ本人の同意を得る。

2) 個人情報を第三者に提供した場合、記録を作成し、保管する。

3) 個人情報を第三者より提供された場合、提供元へ、その個人情報が適正なものかどうかを確認する。

(7) 個人情報の保管

1) 個人情報は、利用目的の達成に必要な範囲内において、正確、かつ、最新の状態で管理する。

2) 個人情報を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。

(8) 委託先の監督

1) 個人情報の取扱いの全部又は一部を委託する場合は、十分な保護水準を満たしている委託先を選定する。

2) 個人情報の取扱いの全部又は一部を委託する場合は、委託先とは個人情報の取扱いに関する覚書を締結する。

(9) 個人情報に関する開示請求

1) 本人から個人情報に関する開示請求（開示、訂正、削除）を受けた場合、速やかに対応する。

2) 本人から個人情報に関する開示請求を受けた場合、請求者が本人または代理人であることの確認を行う。

3) 本人から個人情報に関する開示請求を受けた場合、社内の所定の手続きを行う。

(10) 従業者の認識

1) 従業者は少なくとも年１回、プライバシーマーク教育を受講しなければいけない。

(11) 苦情及び相談への対応

1) 本人から個人情報に関する苦情や相談を受けた場合、速やかに対応する。

2) 本人から個人情報に関する苦情や相談を受けた場合、社内の所定の手続きを行う。

(12) 緊急事態への準備

1) 個人情報の緊急事態（個人情報への不正アクセス、個人情報の漏えい、個人情報の滅失等）が発生した場合、速やかに、上司や個人情報保護管理者へ報告する。