何をどこまで決めるべき？

はじめての「情報セキュリティ研修」計画

マルウェアなどによる情報漏えいリスクは高まる一方ですが、従業員に情報セキュリティ教育を行なっている企業は少ないのが現状です。そこで、情報セキュリティ研修計画の立て方を解説します。

牛島総合法律事務所
弁護士
影　島　広　泰

情報セキュリティ研修の必要性

近年、情報セキュリティのリスクは高まる一方で、セキュリティ教育の重要性も高まっています。

たとえば、サイバー攻撃の手段がクラウドサービスで提供され、手軽に多数人で世界中の企業に攻撃を行なう犯罪者集団も登場しています。このように、サイバー攻撃が商業化、洗練化したことで、企業が攻撃を受けるリスクも高まっているのです。

一方、情報漏えい等の原因をみると、誤交付、誤送付、誤廃棄、紛失といった「うっかりミス」が全体の8割を占めています（**図表1**）。情報セキュリティは、サイバーセキュリティのイメージがありますが、実はうっかりミスのほうが発生の頻度は圧倒的に高いのです。仮に、うっかりミスがなくなれば、漏えい等の8割はなくなると考えられます。

企業としては、防御および検知などの技術的な対策を講ずるとともに、日々進化する攻撃に対応するために従業員等への定期的な教育を行なう必要があります。そも、従業員等への教育は、法的な義務でもあります。

個人情報保護法では、23条に基づく「人的安全管理措置」として、「従業者の教育」が義務付けられているとともに、同24条に基づいて「従業者に対する監督」をしなければならないと義務付けられています（**図表2**）。

教育が義務付けられている対象者

法的に教育が義務付けられている対象者は、個人情報保護法における「従業者」（24条）です。

従業者とは、「個人情報の保護に関する法律についてのガイドライン（通則編）」（以下「通則ガイドライン」）に次のとおり定義されています。

「個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者等をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる」（通則ガイドライン3-4-3）

すなわち、取締役や監査役はもちろん、派遣社員等も含め、社内で業務を行なっている者全員が、教育の対象者となります。

情報セキュリティの教育内容

(1) 教育全体の構成

教育プログラムには、様々な構成が考えられますが、①近時の自社・他社の事故・被害等事例を紹介し、②法令などのルールを解説した後、③社内ルールを①の事故事例をカバーする部分を中心に解説するという構成が、オーソドックスで効果的でしょう。

まずは、①事例を紹介し、身近な「自分ごと」としての関心を持ってもらいます。

そのためには、自社で発生した事故があればそれを紹介するのがよいでしょう。他社事例についても、可能であれば、同業他社の事例や自社の業務で発生しそうな事例を選びましょう。

次に、②法令やガイドラインが定める法的義務としてのルールを解説します。

そのうえで、③社内ルールを説明します。

従業員等のなかには、情報セキュリティに関する社内ルールが面倒で業務の邪魔に感じているケースもあります。そのため、①の事例で身近に感じてもらったうえで、②法令等による法的義務が厳しいことを伝え、それを踏まえて③社内ルールが存在しているのであって、決して「きれいごと」として定められているのではなく、必要最小限のルールであることを認識してもらいましょう。

(2) サイバー攻撃についての教育

①の事例のうち、サイバー攻撃については、攻撃の内容が日々変化していることから、最新の動向を解説することが重要です。

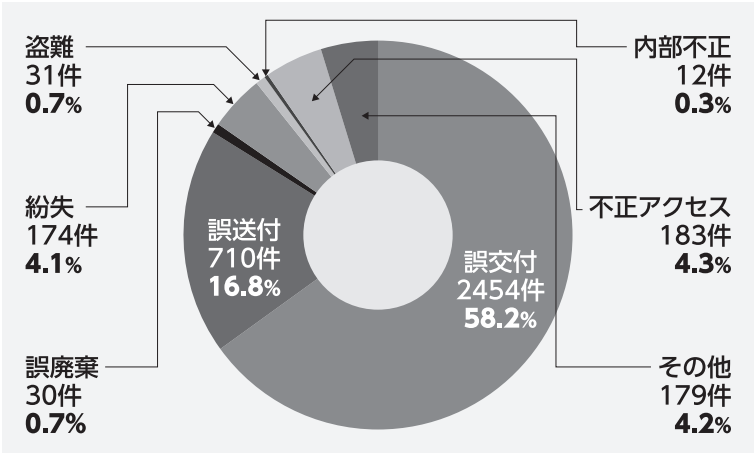
IPA（独立行政法人情報処理推進機構）が、毎年「情報セキュリティ10大脅威」を公開しています（**図表3**）。

これは、情報セキュリティ分野の研究者、企業の実務担当者など約200名が審議・投票を行なってランキング形式で公表しているものであり、いま、企業が留意すべきサイバー攻撃が端的に示されているものです。

IPAでは、この情報セキュリティ10大脅威に基づいて、「情報セキュリティ10大脅威　セキュリティ対策の基本と共通対策」を公表しています。

ここには、ランキングされたそれぞれの脅威について、どのよう

図表1　個人データの漏えい等の原因
（個人情報取扱事業者が漏えい元であった場合）



出典：個人情報保護委員会「令和4年度個人情報保護委員会年次報告」を基に作成

図表2　人的安全管理措置

講じなければならない措置	手法の例示
○ **従業者の教育** 従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行なわなければならない	● 個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行なう ● 個人データについての秘密保持に関する事項を就業規則等に盛り込む

出典：個人情報の保護に関する法律についてのガイドライン（通則編）10-4

図表3　情報セキュリティ10大脅威2024〔組織〕

順位	「組織」向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

出典：IPA

(※1)https://www.ppc.go.jp/personalinfo/hiyarihatto/

な対策が考えられるかが具体的に解説されています。社内教育の内容を検討するにあたり、大いに参考になりますので、ぜひ活用してください。

(3) うっかりミスに対する教育

個人情報保護法が安全管理措置の対象としている個人データの「漏えい等」とは、漏えい、滅失および毀損をいうとされています(23条)。「漏えい」だけではなく、「滅失」と「毀損」がないように教育する必要もあるので注意しましょう(**図表4**)。

研修内容としては、自社における事故事例があればそれを紹介するとともに、他社において頻発している事故についても紹介し、防止策を教育することが重要です(**図表5**)。

たとえば、自社の事故事例に加え、誤交付、誤送付、誤廃棄、紛失の事例が多いことを伝え、それぞれについて、留意点や対応策を説明していきます。

また、個人情報保護委員会が「個人情報の研修資料・ヒヤリハットコーナー(※1)」を設けているので、こちらも研修資料の作成の参考にするとよいでしょう。

(4) インシデント発生時の対応についての教育

インシデント発生時の初動についての社内ルールも、教育の内容に含める必要性が高いものです。

個人情報の保護に関する法律施行規則(以下「規則」)8条1項が定める個人情報保護委員会への「速報」は、初日算入で「概ね3~5日以内」に行なうことが求められています(通則ガイドライン3-5-3-3)。

インシデント発生時には、いち早く担当者・担当部署に報告してもらい、会社として素早く対応する必要があります。

また、個人情報保護法の安全管理措置(23条)としても、組織的安全管理措置の「組織体制の整備」の義務を果たすために、通則ガイドライン別添10-3において「法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実または兆候を把握した場合の責任者への報告連絡体制」および「個人データの漏えい等事案の発生または兆候を把握した場合の責任者への報告連絡体制」が例示されており、「漏えい等事案に対応する体制の整備」も義務付けられています。

なお、インシデント発生時の対応を教育する際、個人情報保護法26条2項が定める本人への通知義務についても説明するとよいと考えられます。

個人情報保護委員会への報告および本人への通知は、以下の場合において、規則7条で規定されています。

i 要配慮個人情報の漏えい等またはそのおそれ

ii 経済的な損失を伴うこととなるおそれのあるような個人データの漏えい等またはそのおそれ

iii 不正の目的をもって行なわれたおそれがある当該個人情報取扱事業者に対する行為による個人データ(当該個人情報取扱事業者が取得し、または取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む)の漏えい等またはそのおそれ(※2)

iv 1000人分を超える個人データの漏えい等またはそのおそれ

このうち、個人情報保護委員会への報告は会社として行なうものですが、本人への通知は、漏えい等を発生させた当人やその所属部署が自ら行なう必要があるケースもあります(規則10条)。

本人への通知というのは、ビジネス的な言い方をすれば本人への「謝罪」を求められることであり、たとえば、取引先の情報を漏えいすれば、その当人や所属部署が取引先に謝罪する必要があり、人事情報が漏えい等すれば、人事部がその事後対応を自ら行なうことになります。

このように、個人データが漏えい等したときは、個人情報保護法の義務として、自らが本人に「謝罪」することが必要になることを周知しましょう。

情報セキュリティの教育方法

以前は、会議室に集まって研修を行なうことが一般的でしたが、現在では動画配信を採り入れる企業も増えています。ただし、動画配信の場合は、効果が劣らないように、最後にテストを行なうなどの工夫が必要です。

また、パート・アルバイトが多いなど、教育に時間をとることが難しいケースでは、eラーニング

(※2) iii は2024年4月1日施行の改正施行規則7条を反映したもの

のシステムを利用してもよいでしょう。

評価とフィードバック

教育の後に、テストを行なうと教育の効果が高まります。

実は、教育の開始時に「終了後にテストがあります」と言うだけでも、教育を受ける者の真剣さが変わります。

逆に言えば、教育内容をしっかりと聞いてもらうことがテストをする目的なので、内容そのものについては、簡単なものでかまわないでしょう。

たとえば、

Q「情報漏えいの可能性があると感じたら、上長と情報システム部に必ず文書で報告しなければならない。○か×か」

A「正解×：報告は文書でなくても構いません。口頭でよいのでいち早く報告してください」

といった簡単な問題を10問程度出題するイメージです。

また、次年度以降の参考にするために、教育の方法や内容についてアンケートをしておくとよいでしょう。

継続的な実施と内容の見直し

情報セキュリティ教育は、繰り返し行なって知識を定着させることが重要です。この点については、個人情報保護委員会の「個人情報保護法ガイドラインに関するQ&A」に、「研修の頻度は、事業者の規模や取り扱う個人データの性質・量等によっても異なるため、それらを踏まえて適切に判断する必要がありますが、適切な内容の研修であれば、年1回程度でも少ないとはいえないと考えられます」とあります。

つまり、「年1回程度でも少ないとはいえない」と言うのですから、少なくとも毎年教育を行なう必要があることになります。

しかし、教育の担当者からは、ことしの「ネタ」を考えることが大変であるといった話もよく聞きます。

前述した①近時の自社・他社の事故事例については、図表5で紹介した各種サイトに最新の事例が紹介されているので、それでカバーできるでしょう。また、生成AIに研修テーマのアイデア出しをしてもらうのも一法です。

他方、②法令などのルールおよび③社内ルールについては、同じネタの繰り返しになっても問題ありません。

教育は知識の定着を目的としている以上、どうしても覚えておいてほしいポイントは繰り返し説明して覚えてもらう必要があるためです。

研修に出席した従業員等が「これは去年も聞いたな」と思ったのであれば、むしろ教育としては成功していると考えられます。▲

図表4　滅失および毀損の定義と事例

	定義	該当する事例
滅失	個人データの内容が失われること	● 個人情報データベース等から出力された氏名等が記載された帳票等を誤って廃棄した場合 ● 個人データが記載または記録された書類・媒体等を社内で紛失した場合
毀損	個人データの内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となること	● 個人データの内容が改ざんされた場合 ● 暗号化処理された個人データの復元キーを喪失したことにより復元できなくなった場合 ● ランサムウェア等により個人データが暗号化され、復元できなくなった場合

出典：個人情報の保護に関する法律についてのガイドライン（通則編）3-5-1-2、3-5-1-3

図表5　教育資料の情報ソース

対象	事例の情報ソース（例）	対応策の情報ソース（例）
サイバーセキュリティ	IPA情報セキュリティ10大脅威	情報セキュリティ10大脅威　セキュリティ対策の基本と共通対策
自社事例	自社の過去の事例	自社の情報セキュリティに関するルール
他社事例	個人情報保護委員会の年次報告 https://www.ppc.go.jp/aboutus/report/	JIPDEC（一般財団法人日本情報経済社会推進協会）の「統計情報」および「お役立ちツール（社内教育用参考資料）」 https://privacymark.jp/system/reference/index.html

かげしま　ひろやす　牛島総合法律事務所所属パートナー弁護士。企業グループのデータ・ガバナンス体制の構築や漏えいインシデントの対応の案件等に従事。「法律家・法務担当者のためのIT技術用語辞典」（商事法務）ほか著書・論文多数。