

弁護士 企業経営とサイバーリスク が解説 ～個人情報保護法改正が中小企業に与える影響～

八雲法律事務所 弁護士／情報セキュリティスペシャリスト 山岡 裕明

2010年弁護士登録。カルフォルニア大学バークレー校情報大学院卒、同校客員研究員(2019-2020)、内閣サイバーセキュリティセンタータスクフォースメンバー(2019-2020)も務める。サイバーセキュリティ法務に特化した業務を展開している。



2022年4月1日より、改正個人情報保護法が施行されます。法改正によりサイバー攻撃による情報漏えい時の通知等が義務化されますが、その概要と法改正が中小企業に与える影響について、サイバーセキュリティの専門家である八雲法律事務所の山岡裕明弁護士に解説いただきました。

個人情報保護法の改正

改正前の個人情報保護法においては、情報漏えい等がなされないように安全管理措置をとることを個人情報取扱事業者に義務付ける規定は置かれていましたが、情報漏えい時に個人情報取扱事業者がなすべき対応についての規定は置かれていませんでした。

個人情報保護委員会が定めるガイドライン等においては、情報漏えい等時に個人情報取扱事業者が実施することが望まれる対応として、本人への連絡や個人情報保護委員会への報告に関する事項は定められていましたが、本人への連絡、個人情報保護委員会への報告は努力義務とされていました。

改正個人情報保護法においては、一定の類型の情報漏えい等事案においては、個人情報取扱事業者に対して個人情報保護委員会への報告が新たに義務付けられることとなりました。加えて、個人情報保護委員会

への報告が必要となる場合においては、本人に対する通知等も新たに義務付けられることとなりました。そして、個人情報保護委員会への報告及び本人への通知等が義務付けられる一定の類型の情報漏えい等事案の中には、サイバー攻撃により個人情報が漏えいした場合が含まれます。

また、上記の報告、通知等義務に違反した個人情報取扱事業者に対しては、個人情報保護委員会から違反行為を是正するよう勧告や命令が出せる規定が新たに設けられており、個人情報保護委員会は命令違反をした個人情報取扱事業者を公表することができるうえ、命令違反をした個人情報取扱事業者は、個人については1年以下の懲役又は100万円以下の罰金刑、法人については1億円以下の罰金刑に処せられる可能性のある罰則規定も新たに設けられています。



改正個人情報保護法の概要 (2022年4月1日より施行)

企業が個人情報を漏えい等した場合の

- ・個人情報保護委員会(もしくは監督官庁)への報告
- ・被漏えい者本人への通知等

さらに、報告・通知等義務に違反した場合・・・



原則義務化!

個人情報取扱事業者の公表

1億円以下の罰金刑 (法人の場合)

(裏面に続く)

企業のサイバーセキュリティ対策に与える影響

企業においてサイバー攻撃による個人情報の漏えいが発生してしまうと、上記のように個人情報保護委員会への報告や本人への通知等といった対応を余儀なくされることとなり、対応に係る負担及びコストの増加が見込まれます。

加えて、本人への通知等が必須であることから、顧客や取引先にセキュリティレベルの低い企業と捉えられてしまい、以後の業績に影響するおそれも十分にあります。

そのため、情報漏えい等が生じた際の上記の負担等を避けるために、サイバー攻撃による情報漏えいに備え、サイバーセキュリティ対策を新たに講じる企業や従前の対策を見直す企業が増加することが見込まれます。

法改正に対する企業の備え

企業としては、上記のようなサイバーセキュリティ対策を強化するといった備えの他に、実際にサイバー攻撃による情報漏えいが生じた場合の対応について備える必要があります。

個人情報保護委員会への報告については、漏えいのおそれのある個人情報の項目・件数等の一定の内容を、事態を知った日から概ね3～5日以内に報告する「速報」と、原因や再発防止策等も盛り込み30日以内(サ

イバー攻撃により個人情報が漏えい等した場合には「60日以内」)に報告する「確報」の2段階の報告が求められます。

そのため、企業としては、情報漏えい事案の発生の原因調査を行い、報告すべき内容を検討して個人情報保護委員会への報告を行うといった対応を、情報漏えい事案の発生後から短期間のうちに行う必要がある、このような有事の対応が可能な体制や環境を事前構築することが企業の備えとして必要となります。

原因調査等にはフォレンジック*業者が必要となり、個人情報保護委員会への報告や本人への通知等の具体的な対応については弁護士のアドバイス等が有益となります。

企業としては、フォレンジック業者や弁護士といった専門事業者にいつでも依頼できる体制を平時から構築する必要がありますが、その分野に長けた専門事業者を把握している企業は一握りです。そのため、専門事業者を紹介でき、かつ、その費用も支出可能なサイバー保険に加入しておくことは、法改正に対する企業の備えとしてまさに打ってつけといえます。

※フォレンジック

…サイバー攻撃などによる事故発生時に、原因や被害の範囲等全容を明らかにするために、コンピューターや記録媒体に残された証拠を調査すること。専門事業者による対応が必要となる。

POINT



2022年4月の改正個人情報保護法においては、企業による情報漏えい事案の発生時、個人情報保護委員会や被漏えい者本人に対する通知等が義務付けられます。



速報・確報に向けて、有事の際には迅速かつ詳細な対応が要求されるため、専門事業者の確保が極めて重要となります。



有事の対応が可能な体制や環境を平時から構築するコスト及び有事の際の専門家を確保するコストが加わり、企業にとって、これまで以上にサイバーセキュリティ対策に要するコストも増加します。



専門事業者を紹介でき、かつその費用を補償可能なサイバー保険への加入は、サイバーセキュリティ対策として有効です。

三井住友海上火災保険株式会社

MS&AD INSURANCE GROUP



損害保険・生命保険の総合代理店

緑富士株式会社

<お問い合わせ先>