NEW 2022年4月1日より

# 改正個人情報保護法が施行されます

改正法の施行後に

**一定の基準を満たす個人情報の漏えいが発生すると**

**ポイント1.** **個人情報保護委員会への報告**が義務化されます。

**ポイント2.** **漏えい被害者本人への通知**が義務化されます。

**個人情報保護委員会による命令や委員会への虚偽報告等に対する**

**ポイント3.** **罰金刑が引き上げ**となります。

## 一定の基準を満たす個人情報の漏えいとは？

**いずれかに該当する場合を言います。**

**1 要配慮個人情報(医療情報・犯罪歴等)の漏えい、滅失若しくは毀損**

（例）・従業員の健康診断等の結果を含む個人データの流出
・診療情報や調剤情報を含む個人データを記録したUSBメモリの紛失

**2 財産的被害が発生するおそれがある場合**

（例）・クレジットカード情報の漏えい
・送金や決済機能のあるWebサイトのログインIDとPWの組み合わせの漏えい

**3 不正の目的をもって行われたおそれがあるもの**

（例）・外部からのサイバー攻撃による漏えい
・従業員が顧客の個人データを不正に持ち出して第三者に提供した場合

**4 漏えい被害者が1,000人を超える場合**

（例）・システムの設定ミスや、個人データの誤送付等により、1,000人超の個人情報が漏えいした場合

**情報漏えいが発生した場合には、まず報告対象事由に該当するか否かの判断が必要です。**

# 実務において生じる影響

## 1．個人情報保護委員会への報告の義務化

| | |
|---|---|
| **報告方法** | • 速報と確報の2段階の報告が必要となります。（速報：事由発生から約3日～5日以内、確報：事由発生から30日以内（不正の目的の場合には60日以内）に実施。）<br>• 個人情報保護委員会HPの報告フォームを使用します。 |
| **報告内容** | • 概要、漏えいした個人データの項目、被害者数、原因・二次被害またはそのおそれ、本人への対応の実施状況、公表実施の有無、再発防止措置、その他参考情報 |
| **想定される対応** | • インシデント対応、再発防止策策定のための専門事業者との連携<br>• 原因調査・被害範囲の特定のためのフォレンジック調査<br>• 報告対象有無の確認や報告フォーム作成のための弁護士相談 |

## 2．漏えい対象となった被害者本人への通知の義務化

| | |
|---|---|
| **通知方法** | • 法令上規定されている様式はありません。<br>• 通知すべき内容が「分かりやすく」伝わる方法を選択します。（例：文書、メール）<br>• 通知が困難である場合、代替措置として問合せ窓口を設置し、本人が自らの個人データが漏えい対象となっているか確認できるようにすることも可能です。 |
| **通知内容** | • 概要、漏えいした個人データの項目、原因、二次被害・そのおそれの有無 |
| **想定される対応** | • 被害者からの問い合わせ対応（コールセンター委託費用、超過人件費等）<br>• 漏えい被害者の名前、連絡先の特定<br>• 通知文書作成における弁護士への相談 |

## 3．罰金刑の引上げ

個人情報保護委員会の定める所定の命令に応じない場合や個人情報の不正提供が発覚した場合、最高1億円の罰金が科されます。

- **個人情報保護委員会への報告、被害者への通知のために、以下のような一定の対応と費用が生じる可能性があります。**
  - **専門事業者や弁護士への相談、漏えい被害者への対応**
  - **フォレンジック費用や、被害者への見舞費用**
- **インシデント発生時に、速やかな対応ができるよう、業務フローの見直し、対応手順の策定をご検討ください！**