

「個人情報の保護に関する法律についてのガイドライン」及び  
「個人データの漏えい等の事案が発生した場合等の対応について」  
に関するQ & A（抜粋）

平成 29 年 2 月 16 日  
（平成 29 年 5 月 30 日更新）  
個人情報保護委員会

「個人情報の保護に関する法律についてのガイドライン」及び  
「個人データの漏えい等の事案が発生した場合等の対応について」  
に関するQ & A（抜粋）  
目次

- 5 個人データの漏えい等事案対応告示 ..... 1
- Q12-1 漏えい等事案が発覚した場合に講ずべき措置の「(1) 事業者内部における報告及び被害の拡大防止」にある「責任ある立場の者」とは、どういう役職を想定していますか。 ..... 1
- Q12-2 漏えい等事案が発覚した場合に講ずべき措置の「(1) 事業者内部における報告及び被害の拡大防止」にある「漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる」とは、具体的には、どのような対応をとることが考えられますか。 ..... 1
- Q12-3 漏えい等事案が発覚した場合に講ずべき措置の「(3) 影響範囲の特定」にある「把握した事実関係による影響の範囲を特定する」とは、どういうことですか。 ..... 1
- Q12-4 漏えい等事案が発覚した場合に講ずべき措置の「(5) 影響を受ける可能性のある本人への連絡等」にある「本人が容易に知り得る状態に置く」とは、どういうことですか。 ..... 1
- Q12-5 漏えい等事案が発覚した場合に講ずべき措置の「(5) 影響を受ける可能性のある本人への連絡等」及び「(6) 事実関係及び再発防止策等の公表」について、「漏えい等事案の内容等に応じて」とされていますが、どのような場合に本人への連絡等や公表をしなくてもよいのですか。 ..... 1
- Q12-6 漏えい等事案について個人情報保護委員会等に報告する際の様式はありますか。 ..... 2
- Q12-7 「法第 44 条第 1 項に基づき法第 40 条第 1 項に規定する個人情報保護委員会の権限（報告徴収及び立入検査）が事業所管大臣に委任されている分野」とは、どの分野ですか。また、報告先はどこになりますか。 ..... 2
- Q12-8 個人情報保護委員会等への報告を要しないと規定されている場合であっても、個人情報保護委員会等への報告を行うことは可能ですか。 ..... 2
- Q12-9 委託先において漏えい等事案が生じた場合、委託先が個人情報保護委員会等への報告を行うことになりますか。 ..... 2
- Q12-10 実質的に個人データ又は加工方法等が外部に漏えいしていないと判断される場合に該当する「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」とは、どのような場合が該

- 当しますか。 ..... 3
- Q12-11 テンプレート保護技術（暗号化等の技術的措置を講じた生体情報を復号することなく本人認証に用いる技術）を施した個人識別符号が漏えいした場合も、個人情報保護委員会等への報告、本人への連絡等並びに事実関係及び再発防止策等の公表を行う必要がありますか。 ..... 3
- Q12-12 取引先に荷物を送付するに当たり、誤って宛名票を二重に貼付してしまい、本来の送付先とは無関係の第三者の宛名情報が漏えいした場合も、「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合」に該当し得ますか。 ..... 4

## 5 個人データの漏えい等事案対応告示

Q12-1 漏えい等事案が発覚した場合に講ずべき措置の「(1) 事業者内部における報告及び被害の拡大防止」にある「責任ある立場の者」とは、どういう役職を想定していますか。

A12-1 「責任ある立場の者」の役職は限定されていませんが、あらかじめ、取扱規程等により、漏えい等事案が発覚した場合の適切かつ迅速な報告連絡体制を整備しておくことが必要です。

Q12-2 漏えい等事案が発覚した場合に講ずべき措置の「(1) 事業者内部における報告及び被害の拡大防止」にある「漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる」とは、具体的には、どのような対応をとることが考えられますか。

A12-2 例えば、外部からの不正アクセスや不正プログラムの感染が疑われる場合には、当該端末等の LAN ケーブルを抜いてネットワークからの切り離しを行うなどの措置を直ちに行うこと等が考えられます。

Q12-3 漏えい等事案が発覚した場合に講ずべき措置の「(3) 影響範囲の特定」にある「把握した事実関係による影響の範囲を特定する」とは、どういうことですか。

A12-3 事案の内容によりますが、例えば、個人データの漏えいの場合には、漏えいした個人データに係る本人の数、漏えいした個人データの内容、漏えいした手段、漏えいした原因等を踏まえ、影響の範囲を特定することが考えられます。

Q12-4 漏えい等事案が発覚した場合に講ずべき措置の「(5) 影響を受ける可能性のある本人への連絡等」にある「本人が容易に知り得る状態に置く」とは、どういうことですか。

A12-4 本人がアクセス(ログイン)できるホームページへの掲載や専用窓口の設置による対応などが考えられます。

Q12-5 漏えい等事案が発覚した場合に講ずべき措置の「(5) 影響を受ける可能性のある本人への連絡等」及び「(6) 事実関係及び再発防止策等の公表」について、「漏えい等事案の内容等に応じて」とされていますが、どのような場合に本人への連絡等や公表をしなくてもよいのですか。

A12-5 例えば、漏えい等事案に係る個人データ又は加工方法等情報について、第三者に閲覧されることなく速やかに回収した場合、高度な暗号化等の秘匿化がされている場合、漏えい等をした事業者以外では特定の個人を識別することができない場合であって本人

に被害が生じるおそれがない場合など、漏えい等事案によって本人の権利利益が侵害されておらず、二次被害の防止の観点からも必要はないと認められる場合等には、本人への連絡等や公表を省略することも考えられます。

なお、公表については、サイバー攻撃による場合等で、公表することでかえって被害の拡大につながる可能性があると考えられる場合にはこれを差し控え、専門機関等に相談することも考えられます。また、漏えい等事案の影響を受ける可能性のある本人全てに連絡がついた場合に公表を省略することも考えられます。

Q12-6 漏えい等事案について個人情報保護委員会等に報告する際の様式はありますか。

A12-6 参考となる報告書の様式を、個人情報保護委員会のホームページにおいて公表していますので、そちらをご利用ください。なお、様式に規定された事項が全て含まれるものであれば、異なる様式による報告も可能です。

(平成 29 年 5 月更新)

Q12-7 「法第 44 条第 1 項に基づき法第 40 条第 1 項に規定する個人情報保護委員会の権限（報告徴収及び立入検査）が事業所管大臣に委任されている分野」とは、どの分野ですか。また、報告先はどこになりますか。

A12-7 法第 44 条第 1 項に基づき法第 40 条第 1 項に規定する個人情報保護委員会の権限（報告徴収及び立入検査）が事業所管大臣に委任されている分野及びその報告先については、個人情報保護委員会のホームページにおいて公表していますので、そちらをご参照ください。

(平成 29 年 5 月更新)

Q12-8 個人情報保護委員会等への報告を要しないと規定されている場合であっても、個人情報保護委員会等への報告を行うことは可能ですか。

A12-8 可能です。また、個人情報保護委員会等への報告を要しない場合に形式的に該当する場合であっても、漏えい等事案に係る個人データ又は加工方法等情報の件数が膨大であるなど社会的影響が大きいと考えられる事案の場合には、個人情報保護委員会等への報告を行うことが望ましいと考えられます。

Q12-9 委託先において漏えい等事案が生じた場合、委託先が個人情報保護委員会等への報告を行うことになりますか。

A12-9 委託先において漏えい等事案が発生した場合であっても、委託元が漏えい等事案に係る個人データ又は加工方法等情報について最終的な責任を有することに変更ありませんので、原則として、委託元が個人情報保護委員会等へ報告するよう努めていただ

きます。ただし、漏えい等事案に係る個人データ又は加工方法等情報の実際の取扱状況を知る委託先が報告の内容を作成したり、委託元及び委託先の連名で報告するといったことが妨げられるものではありません。

Q12-10 実質的に個人データ又は加工方法等が外部に漏えいしていないと判断される場合に該当する「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」とは、どのような場合が該当しますか。

A12-10 実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。

第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。

また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。

Q12-11 テンプレート保護技術（暗号化等の技術的措置を講じた生体情報を復号することなく本人認証に用いる技術）を施した個人識別符号が漏えいした場合も、個人情報保護委員会等への報告、本人への連絡等並びに事実関係及び再発防止策等の公表を行う必要がありますか。

A12-11 テンプレート保護技術を施した個人識別符号について、高度な暗号化等の秘匿化（Q12-10 参照）がされており、かつ、当該個人識別符号が漏えいした場合に、漏えいの事実を直ちに認識し、テンプレート保護技術に用いる秘匿化のためのパラメータを直ちに変更するなど漏えいした個人識別符号を認証に用いることができないようにしている場合には、「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」に該当し、個人情報保護委員会等への報告は不要と考えられます。

なお、本人への連絡等並びに事実関係及び再発防止策等の公表については、事案に応じて必要な措置を講ずることとされています。

Q12-12 取引先に荷物を送付するに当たり、誤って宛名票を二重に貼付してしまい、本来の送付先とは無関係の第三者の宛名情報が漏えいした場合も、「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合」に該当し得ますか。

A12-12 御指摘の場合も、誤って貼付した宛名票において、宛先及び送信者名以外に個人データ又は加工方法等情報が含まれていないのであれば、「FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合」に該当すると考えられます。