中小企業の皆様へ

マイナンバー（個人番号）が万が一漏えいしてしまったら…

愛称：マイナちゃん

事業者が取り扱うマイナンバーの漏えい事案その他の番号法違反の事案又は番号法違反のおそれのある事案が発覚した場合には、事案の内容に応じて、次のように対応することが考えられます。

発覚時の対応

※　次ページに「発覚時対応の例」を掲載

(1) 事業者内部における報告、被害の拡大防止

責任ある立場の者に直ちに報告するとともに、被害の拡大を防止するために迅速に(2)～(5)を実施しましょう。

(2) 事実関係の調査、原因の究明

事実関係を調査し、その原因の究明を行いましょう。

(3) 影響範囲の特定

(2)で把握した事実関係による影響の範囲を特定しましょう（例：誰の、どのような情報が、どこに漏えいしたのか、等）。

(4) 再発防止策の検討・実施

(2)で究明した原因を踏まえ、再発防止策を検討し、速やかに実施しましょう。

(5) 影響を受ける可能性のある本人への連絡等

二次被害の防止、類似事案の発生回避等の観点から、事案の内容等に応じて、事実関係等について、速やかに、本人へ連絡し、又は本人が容易に知り得る状態に置きましょう。

(6) 個人情報保護委員会等への報告の要否の確認

「漏えい等報告」のページをご参照ください。

発覚時等対応のヒント

マイナンバーの漏えいが発覚した場合の対応は事案により異なりますが、対応のヒントとして参考にしてください。

《例示》
経理担当者が自宅で作業をするために、マイナンバーを保存している電子媒体（USB メモリ）を鞄に入れて持ち帰る途中で、鞄を紛失してしまった。

〈発覚時対応の例〉

□　事業者内部における報告、被害の拡大防止
→　責任者へ報告する。
→　警察等への紛失届の提出及び当日の行動範囲に落ちていないかの確認等、USB メモリを探索し回収する。

□　事実関係の調査、原因の究明
→　どのような取扱いをしていたのかを本人から聴取し、ルールに沿った取扱いか、ルールに反した取扱いかを確認し、紛失に至った原因を究明する。

□　影響範囲の特定
→　USB メモリ保存データに誰のどのような情報が含まれているかを特定し、外部に情報が流出した場合の影響を想定する。
→　USB メモリの保存データの暗号化やパスワード設定の状況を確認する。
→　USB メモリを回収できた場合には、回収までの経緯を確認し、不特定の者に情報漏えいしていないかを確認する。

□　再発防止策の検討・実施（⇒次ページに「再発防止策の例」を掲載）
→　発生原因が人的原因かルール自体の欠陥かを特定し、再発防止のための対応方法（例えば、実務研修や倫理研修の実施、ルールの改正等。）を検討の後、従業員に周知して適切に実施する。

□　影響を受ける可能性のある本人への連絡等
→　影響を受けるであろう USB メモリ保存データに含まれている情報の該当者に連絡して、漏えいの事実について謝罪し、不審電話による詐欺被害（例えば、金銭の要求等。）の防止のために注意喚起する。
→　マイナンバーが漏えいして不正に用いられるおそれがあると認められるときは、マイナンバーの変更をお住いの市区町村に請求できるので、問い合わせるよう本人に説明する。

□　個人情報保護委員会等への報告の要否の確認

→　個人情報保護委員会等への報告が必要かどうかを確かめ、必要な場合は報告する。(「重大な事態」が生じたときは、個人情報保護委員会への報告義務があります。)

※　次ページの「漏えい等報告」をご参照ください。

〈再発防止策の例〉

□　ルールに沿った取扱いをしていましたか。

→　ルールに沿った取扱いがされなかったために事案が発生した場合には、ルールどおりに取り扱うよう適切に研修を実施してください。

□　ルールの内容は適切ですか。

→　持出しの適否や許可、持出しができる場合の情報の保護としてデータの暗号化やパスワードの設定等のルールを再確認しましょう。

□　計画的に研修は実施していましたか。

→　事務取扱担当者のみならず、他の従業員にも、マイナンバーの基本的な取扱いの研修は実施しましょう。

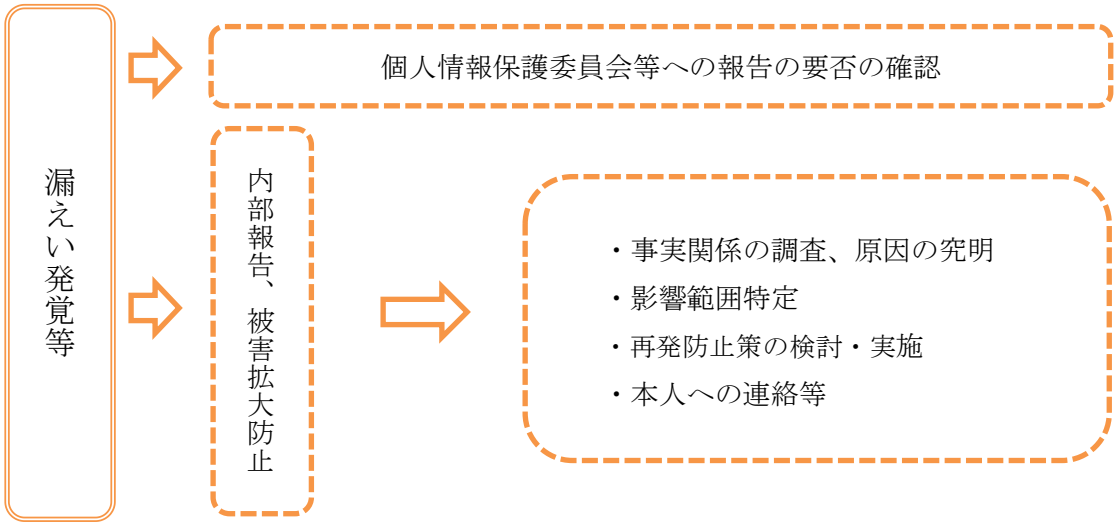
□　漏えい発生後直ちに責任者に報告されましたか。

→　漏えいが発生した際には、被害の拡大及び二次被害の防止等の早急な対応が必要となりますので、責任者への連絡体制を再確認しましょう。

□　定期的に責任ある立場の者が取扱いを確認していましたか。

→　責任ある立場の者がマイナンバーの保管を含む取扱状況やルール等について、定期的に点検しましょう。

※マイナンバーが漏えいしてしまった場合の対応フロー（例）



漏えい等報告

《個人情報保護委員会等への報告》

マイナンバーが漏えい等した場合には、次に従い対応してください。

1　個人情報保護委員会に報告する場合

個人情報保護委員会ウェブサイト「特定個人情報の漏えい事案等が発生した場合の対応について」（https://www.ppc.go.jp/legal/rouei/）に設置されている「漏えい等の報告」から報告してください。

なお、影響を受ける可能性のある本人全てに連絡した場合、実質的に外部に漏えいしていないと判断される場合等の要件を全て満たす場合には、個人情報保護委員会への報告は不要です。

2　個人情報保護委員会以外に報告する場合

「事業者における特定個人情報の漏えい事案等が発生した場合の対応について」に従って、該当する報告先（認定個人情報保護団体、所管官庁等）に報告してください。

（所管官庁から個人情報保護委員会に報告されますので、１の報告は不要です。）

3　「重大な事態」が生じて個人情報保護委員会に報告する場合

「重大な事態」が生じたときには、個人情報保護委員会に報告することが法令上の義務となります。

「重大な事態」とは…

1．漏えい・滅失・毀損又はマイナンバー法に反して利用・提供された特定個人情報に係る本人の数が 100 人を超える事態

2．特定個人情報ファイルに記録された特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり、かつ、その特定個人情報が閲覧された事態

3．不正の目的をもって、特定個人情報ファイルに記録された特定個人情報を利用し、又は提供した者がいる事態　等

※　詳しくは個人情報保護委員会ウェブサイト「特定個人情報の漏えい事案等が発生した場合の対応について」（https://www.ppc.go.jp/legal/rouei/）をご覧ください。