

危機管理マニュアル（情報漏洩に関する対応マニュアル）

本マニュアルは、情報漏洩に対する原則的な対応、及び情報漏洩の種類ないし態様に応じた対応について定めるものである。

第1 情報漏洩の対応に関する原則

1 発見・報告（別紙1参照）

- (1) 情報漏洩に関する兆候や、情報漏洩の具体的な事実を確認した場合は、事務局に報告し速やかに情報漏洩対応のための体制をとる。
- (2) 不正アクセスや不正プログラムなど情報システムからの情報漏洩の可能性がある場合は、不用意な操作をせず、情報システム上に残された証拠が消えないようにする。
- (3) 外部から通報があった場合は、当該通報をした者の氏名・連絡先等を必ず記録する。

2 初動対応

- (1) 事務局は、情報漏洩に対する当面の対応方針を決定し、情報漏洩による被害の拡大、二次被害の防止のために必要な応急処置を行う。
- (2) 情報が外部からアクセスできる状態にあたり、被害が拡大する可能性がある場合、情報の隔離、ネットワークの遮断、サービスの停止などの外部からのアクセスを遮断するために必要な措置を行う。

3 調査（別紙2参照）

適切な対応についての判断を行うために5W1H（いつ、どこで、誰が、何を、なぜ、どうしたのか）の観点から調査し、情報漏洩に関する情報を収集・整理する。また、事実関係を裏付ける情報や証拠を確保する。

4 通知・報告・公表等

- (1) 事務局は、漏洩した個人情報の本人、取引先などへの通知、警察などへの届出、ホームページ、マスコミ等による公表を検討する。
- (2) 事務局は、情報漏洩により、個人情報が漏洩したことを確認した場合、当該漏洩した個人情報の本人に対して、個人情報が漏洩した旨を通知する。ただし、特別な理由がある場合は、当該通知を行わない。
- (3) 情報の紛失・盗難、又は不正アクセス、内部犯行、脅迫等不正な金銭の要求などの違法性のある行為が認められる場合、事務局は、警察へ届出、又は被害届の提出等を行う。
- (4) 情報漏洩に関するすべての関係者への個別の通知が困難な場合や、広く一般に情報漏洩による影響が及ぶと考えられる等の場合、事務局は、当法人のホームページでの情報公開や、記者発表による公表を行う。ただし、情報の公表が被害の拡大を招く恐れがある等の特別な理由がある場合は、公表の時期、対象などを考慮する。

5 抑制措置と復旧

- (1) 事務局は、情報漏洩によって発生した被害の拡大の防止と復旧のために必要な措置を行う。
- (2) 情報漏洩による被害の規模が大きい場合、事務局は、専用の相談窓口を設置し、被害が発生した場合、その動向を素早く察知し対応することに努める。また、事務局は、再発防止に向けた具体的

な取り組みを行い、停止したサービス、アカウント等がある場合はそれらを復旧する。

6 事後対応

- (1) 事務局は、情報漏洩に対する再発防止策を検討し、実施する。
- (2) 事務局は、調査報告書を理事及び監事に提示した上で、情報漏洩の概要及び再発防止策等について報告する。
- (3) 理事及び監事は、情報漏洩による被害者に対する損害の補償等を検討し、必要な措置を行う。また、内部職員の責任を追及する必要がある場合、必要な処分手続きを行う。

第2 紛失・盗難

1 事件事例

- (1) 情報が記録されたパソコンやUSBメモリ等（以下、「情報媒体」という。）を電車や飲食店等に置き忘れた。
- (2) 情報媒体が入ったカバンを盗まれた。
- (3) 置き引きや車上荒らしや事務所荒らしに遭い、情報媒体を盗まれた。

2 発見及び報告

情報媒体を紛失又は盗難（以下「紛失等」という。）された者、並びに情報媒体の紛失等を発見した者は、直ちに事務局に報告し、別紙1の「情報漏洩報告シート」に当該紛失等の内容を記入する。

3 初動対応

- (1) 事務局は、情報漏洩報告シートの内容等を基に、紛失等にあった情報の種類・内容、情報が記録された情報媒体を特定する。
- (2) 電車内や飲食店等に情報媒体を置き忘れた場合や、情報媒体を紛失等した場合、事務局は、直ちに警察や鉄道会社、飲食店等に情報媒体を紛失したことを届け出、又は連絡し、情報媒体の捜索・回収を依頼する。
- (3) 紛失等した情報媒体内に、特定のWebページや秘密情報等にログインするためのIDやパスワード等の情報が含まれている場合、事務局は、直ちに当該IDやパスワードを変更するなどして、被害の拡大を防止する。

4 調査

- (1) 事務局は、情報漏洩報告シートその他の情報・記録から、紛失等した情報を可能な限り正確に把握し、予想される二次被害を防止する。
- (2) 事務局は、調査によって得られた情報を精査し、紛失等した情報の重要性及び被害の程度等を判定する。

5 通知・報告・公表等

- (1) 紛失等した情報に個人情報が含まれる場合、事務局は、直ちに当該個人に対して個人情報を紛失等した旨を通知し、謝罪を行う。また、当該個人が二次的な被害を被った場合、その内容の報告を求める。なお、事務局は、当該謝罪等を、情報を紛失等した本人に行わせることができるものとする。
- (2) 紛失等した個人情報が多数である場合、事務局は、ホームページ上にて個人情報を紛失等した旨を掲載する。

6 抑制措置と復旧

- (1) 事務局は、調査によって得た情報や紛失等した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
- (2) 紛失等した情報にクレジットカード、銀行口座番号、ID、パスワード等が含まれていた場合、事務局は、当該情報が当法人の有する情報である場合、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合、直ちに当該情報が紛失等したことを伝え、パスワードの変更等を促す。
- (3) 事務局は、紛失等した情報については、記録媒体やWeb上に残されたデータから、可能な限り復元する。

7 事後対応

- (1) 事務局は、情報が紛失等した原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
- (2) 事務局は、検討した改善策を、理事及び監事に対して報告する。

第3 誤送信

1 事故事例

- (1) メールアドレスやFAX番号を誤って入力し、機密書類等を第三者に対し誤送信した。
- (2) 住所を誤って記載し、機密書類等を第三者に対して誤郵送した。
- (3) Web上に誤って機密情報等を誤公開した。
- (4) アクセス制限が課されているWebページのログインIDやパスワード等を、第三者に誤送信した。

2 発見及び報告

情報を誤送信、誤郵送、又は誤公開（以下「誤送信等」という。）した者、又は情報が誤送信等されていることを発見した者は、直ちに事務局に報告を行い、別紙1の「情報漏洩報告シート」に当該誤送信等の内容を記入する。

3 初動対応

- (1) 事務局は、情報漏洩報告シートの内容等を基に、誤送信等した情報の種類・内容を特定する。
- (2) 誤送信を行った場合に、送信先が明らかである場合、当該情報の受信者に対して誤って機密情報を送信したことを通知し、受信した情報の削除を求める。また機密情報を誤郵送した場合、郵送した情報の内容の重要性が高い場合、直接当該郵送物を回収するなどして、適切な対応をする。なお、事務局は、当該通知等を、誤送信を行った本人に対して行わせることができるものとする。
- (3) 誤公開を行った場合、事務局は、Web上から直ちに当該情報を削除し、又は、当該情報に対してアクセス制限を設けるなどして、被害が拡大しないように対応する。
- (4) 誤送信等した情報に、特定のWebページや秘密情報等にログインするためのIDやパスワード等の情報が含まれている場合、事務局は、直ちに当該IDやパスワードを変更し、被害の拡大を防止する。

4 調査

- (1) 事務局は、情報漏洩報告シートその他の情報・記録から、誤送信した情報を可能な限り正確に把

握し、予想される二次被害を防止する。

- (2) 誤公開をした場合、事務局は、アクセスログ等を調査し、当該公開された情報にアクセスされた回数等を把握する。
- (3) 事務局は、調査によって得られた情報を精査し、誤送信等した情報の重要性及び被害の程度等を判定する。

5 通知・報告・公表等

- (1) 個人情報を誤送信等した場合、事務局は、当該個人に対して誤送信等をした事実を通知し、謝罪を行う。また、当該個人が二次的被害を被った場合、その内容の報告を求める。なお、事務局は、当該通知等を、誤送信を行った本人に対して行わせることができるものとする。
- (2) 事務局は、情報の重要性及び被害の程度等に鑑み、必要に応じて所轄庁に届け出る。また、必要に応じて誤送信等した事実及び経緯等をW e b等で公表する。

6 抑制措置と復旧

- (1) 事務局は、調査によって得た情報や誤送信等した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
- (2) 誤送信等した情報にクレジットカード、銀行口座番号、I D、パスワード等が含まれていた場合、事務局は、当該情報が当法人の有する情報である場合、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合、直ちに当該情報を誤送信等したことを伝え、パスワードの変更等を促す。

7 事後対応

- (1) 事務局は、情報が紛失等した原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
- (2) 事務局は、当法人が作成・使用しているW e bページやシステムの安全性等を確認し、必要に応じてシステムの変更を行う。
- (3) 事務局は、検討した改善策を、理事及び監事に対して報告する。

第4 内部犯行

1 事件事例

- (1) 当法人内データベースから個人情報を不正に持ち出し、転売した。
- (2) 当法人内に保管していた機密書類等を不正に持ち出し、第三者に譲渡した。

2 発見及び報告

情報を不正に持ち出した者又は情報が不正に持ち出されたことを発見した者は、直ちに事務局に報告を行い、別紙1の「情報漏洩報告シート」に当該持ち出しの内容を記入する。

3 初動対応

- (1) 事務局は、情報漏洩報告シートの内容等を基に、持ち出された情報の種類・内容を特定する。また、誰が情報を不正に持ち出したのかを特定する。
- (2) 情報を不正に持ち出した者が当法人内に存在する可能性がある場合、事務局は、当該情報にかかるアクセスや持ち出し等を可能な限り制限し、証拠の隠滅を防止する。
- (3) 情報を不正に持ち出した者が特定できる場合、事務局は、当該者の使用したパソコン等の機器を

確保する。

- (4) 不正に持ち出された情報に、特定のW e b ページや秘密情報等にログインするための I D やパスワード等の情報が含まれている場合、事務局は、直ちに当該 I D やパスワードを変更し、被害の拡大を防止する。
- (5) 情報を不正に持ち出された可能性がある場合、事務局は、直ちに警察や専門家に対して通報・相談し、二次被害を防ぐための専門的な助言を受ける。

4 調査

- (1) 事務局は、情報漏洩報告シートその他の情報・記録から、不正に持ち出された情報を可能な限り正確に把握し、予想される二次被害を防止する。
- (2) 事務局は、調査によって得られた情報を精査し、不正に持ち出された情報の重要性及び被害の程度等を判定する。

5 通知・報告・公表等

- (1) 事務局は、個人の情報が不正に持ち出された場合、当該個人に対して情報が不正に持ち出された事実を通知し、謝罪を行う。また、当該個人が二次的被害を被った場合、その内容の報告を求める。
- (2) 事務局は、不正に持ち出された情報の重要性及び被害の程度等に鑑み、警察に対して被害届を提出し、情報が不正に持ち出された事実を届け出る。
- (3) 事務局は、情報の重要性及び被害の程度等に鑑み、必要に応じて所轄庁に届け出る。また、必要に応じて情報が漏洩した事実及び経緯等をW e b 等で公表する。

6 抑制措置と復旧

- (1) 事務局は、調査によって得た情報や不正に持ち出された情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
- (2) 不正に持ち出された情報にクレジットカード、銀行口座番号、I D、パスワード等が含まれていた場合、事務局は、当該情報が当法人の有する情報である場合、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合、直ちに当該情報が不正に持ち出されたことを伝え、パスワードの変更等を促す。
- (3) 事務局は、情報を不正に持ち出した者に対して、何らかのアカウント、ログイン I D、パスワード等を提供・共有している場合、当該アカウント等の利用を停止し又は登録情報の変更等を行い、更なる情報を持ち出されないよう対応する。

7 事後対応

- (1) 事務局は、情報が不正に持ち出された原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
- (2) 事務局は、当法人が作成・使用しているW e b ページやシステムの安全性等を確認し、必要に応じてシステムの変更を行う。
- (3) 事務局は、情報の重要性及び被害の程度等に鑑み、情報を持ち出した者に対して課す処分の内容を検討する。
- (4) 事務局は、検討した改善策及び処分の内容を、理事及び監事に対して報告する。
- (5) 理事及び監事は、事務局の報告を受け、当該情報を持ち出した者に対する処分の有無及び内容を決定する。

第5 不正プログラム（ウイルス・スパイウェア等）・不正アクセス

1 事件事例

- (1) 当法人が有するパソコン等の機器がウイルスに感染し、当該機器内に存在する機密情報が第三者に漏洩した。
- (2) 当法人が有するパソコン等の機器がウイルスに感染し、機密情報がW e b サイト等に掲載され、不特定多数の人に閲覧可能な状態となった。
- (3) 当法人の職員が有する個人のパソコン等の機器がウイルスに感染し、当該機器内に存在する機密情報が第三者に漏洩した。

2 発見及び報告

パソコン等の機器がウイルスに感染したことを発見した者は、直ちに事務局に報告を行い、別紙1の「情報漏洩報告シート」にウイルス感染の内容等を記入する。

3 初動対応

- (1) 事務局は、情報漏洩報告シートの内容等を基に、感染した機器、感染の経緯、程度を特定し、ウイルスに感染した範囲を把握する。また、当該ウイルスに感染したことにより漏洩した情報を可能な限り特定する。
- (2) 機器がウイルスに感染したことが発覚した場合、事務局は、直ちに感染した機器の使用を停止し、当該機器をネットワークから切り離し、又は切り離させる。また、事務局は、ネットワーク上のシステムがウイルスに感染した場合、当該システムへのアクセスを行わないよう徹底し、又はこれを徹底させる。
- (3) 不正に持ち出された情報に、特定のW e b ページや秘密情報等にログインするためのI Dやパスワード等の情報が含まれている場合、事務局は、直ちに当該I Dやパスワードを変更し、被害の拡大を防止する。
- (4) 機器がウイルスに感染したことが発覚した場合、事務局は、直ちに警察や専門家に対して通報・相談し、二次被害を防ぐための専門的な助言を受ける。
- (5) 事務局は、重要なデータを外部メディアに移すなどし、バックアップを作成する。なお、当該バックアップには、不正プログラムが存在している可能性もあることから、必ず専門家の助言を受け、適切な方法・態様により対処する。

4 調査

- (1) 事務局は、情報漏洩報告シートその他の情報・記録から、漏洩した情報を可能な限り正確に把握し、予想される二次被害を防止する。
- (2) 事務局は、調査によって得られた情報を精査し、漏洩した情報の重要性及び被害の程度等を判定する。

5 通知・報告・公表等

- (1) 個人の情報が漏洩した場合、事務局は、当該個人に対してウイルス感染により情報が漏洩した事実を通知し、謝罪を行う。また、当該個人が二次的被害を被った場合、その内容の報告を求める。
- (2) 事務局は、情報の重要性及び被害の程度等に鑑み、警察に対して被害届を提出し、ウイルス感染により情報が漏洩した事実を届け出る。

- (3) 事務局は、情報の重要性及び被害の程度等に鑑み、必要に応じて所轄庁に届け出る。また、必要に応じて情報が漏洩した事実及び経緯等をW e b等で公表する。

6 抑制措置と復旧

- (1) 事務局は、調査によって得た情報や漏洩した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
- (2) 事務局は、専門家の助言を受け又は専門家に委託する方法により、ウイルスや不正プログラムを除去する。
- (3) 漏洩した情報にクレジットカード、銀行口座番号、I D、パスワード等が含まれていた場合、事務局は、当該情報が当法人の有する情報である場合、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合、直ちに当該情報が漏洩したことを伝え、パスワードの変更等を促す。
- (4) 事務局は、ウイルスに感染した機器を、専門家の助言を受けただうえで初期化を行うなどし、当該機器が再び感染源とならないよう対処する。

7 事後対応

- (1) 事務局は、機器やシステムがウイルスに感染した原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
- (2) 事務局は、当法人が作成・使用している機器やW e b ページ、システム等の安全性等を確認し、必要に応じてシステムやウイルス対策ソフトの変更を行う。
- (3) 事務局は、検討した改善策及び処分の内容を、理事及び監事に対して報告する。

第6 風評被害・SNSへの掲載

1 事故事例

機密情報が掲示板やSNSに書き込まれ、不特定多数の第三者に公開されていた。

2 発見及び報告

機密情報を公開した者又は機密情報が公開されていることを発見した者は、直ちに事務局に報告を行い、別紙1の「情報漏洩報告シート」に情報が公開された経緯や内容等を記入する。

3 初動対応

- (1) 事務局は、情報漏洩報告シートの内容等を基に、公開した者や公開された情報を特定する。
- (2) 当法人内の者が情報を公開していた場合、事務局は、直ちに当該者に対して当該情報が掲載された記事・投稿等を削除させ、必要に応じてアカウントを停止・削除させるなどして、情報の拡散を防止する。
- (3) 第三者が情報を公開していた場合、事務局は、当該第三者に連絡し、機密情報を公開していること、直ちに当該情報が掲載された記事・投稿等を削除するよう依頼する。
- (4) 公開された情報に、特定のW e b ページや秘密情報等にログインするためのI Dやパスワード等の情報が含まれている場合、事務局は、直ちに当該I Dやパスワードを変更し、被害の拡大を防止する。
- (5) 記事・投稿等の削除を依頼したにも関わらず、当該記事・投稿等が削除されない場合、記事・投稿等の削除を依頼できない場合、又は公開された情報の重要性等にかんがみて緊急に削除される

べきである場合、事務局は、当該記事・投稿等がなされたデジタルプラットフォームにおける管理者等に対して、記事、投稿等の削除を依頼する。

4 調査

- (1) 事務局は、情報漏洩報告シートその他の情報・記録から、公開された情報を正確に把握し、予想される二次被害を防止する。
- (2) 第三者が情報を公開していた場合、事務局は、当該第三者に対して事実関係を聴取し、当該情報を取得した経緯等を把握する。
- (3) 事務局は、調査によって得られた情報を精査し、公開された情報の重要性及び被害の程度等を判定する。

5 通知・報告・公表等

- (1) 当法人内の者によって個人の情報が公開された場合、事務局は、当該個人に対して情報が公開された事実を通知し、謝罪を行う。また、当該個人が二次的被害を被った場合、その内容の報告を求める。なお、事務局は、当該通知や謝罪等を、情報を公開した本人に行わせることができる。
- (2) 事務局は、情報の重要性及び被害の程度等に鑑み、必要に応じて所轄庁に届け出る。また、必要に応じて情報が公開された事実及び経緯等をW e b等で公表する。

6 抑制措置と復旧

- (1) 事務局は、調査によって得た情報や漏洩した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
- (2) 記事、投稿等を行った者が特定できない場合、事務局は、必要に応じて発信者情報の開示等を行い記事、投稿等を行った者を特定するなど、法的手続を検討する。
- (3) 公開された情報にクレジットカード、銀行口座番号、I D、パスワード等が含まれていた場合、事務局は、当該情報が当法人の有する情報である場合、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合、直ちに当該情報が公開されたことを伝え、パスワードの変更等を促す。

7 事後対応

- (1) 事務局は、情報が公開・拡散された経緯、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
- (2) 事務局は、検討した改善策及び処分の内容を、理事及び監事に対して報告する。

以上

別紙 1

情報漏洩報告シート	
件名	
報告者氏名	
報告者電話番号	
報告者メールアドレス	
【情報漏洩が判明した日時】	
【情報漏洩が発生した日時】	
【漏洩した情報の内容・件数】	
【情報漏洩が判明した経緯】	
【情報が漏洩した原因・経緯】	
【漏洩した情報にはパスワード等の保護がなされているか】	

別紙2【調査項目】

漏洩の確度、可能性	<ul style="list-style-type: none"> ・ 断定できるのか、可能性にとどまるのか ・ どの程度の可能性があるのか ・ 今後の調査で確度は高まるのか、変わらないのか <p>※本人への通知、ホームページへの公開等の有無及び内容の判断材料となる</p>
漏洩した個人情報の項目	<ul style="list-style-type: none"> ・ 銀行口座番号やクレジットカード番号など、不正使用されると経済的被害に直結するような情報が含まれているか ・ 病歴や犯罪歴など、公表により当然に精神的苦痛をもたらすセンシティブな情報が含まれているか ・ 資産状況や信用状態など、一般に人に知られたくない情報が含まれているか ・ 趣味嗜好や学業成績など、一般には入手し難い情報が含まれているか ・ 勤務先や役職などビジネス上の情報が含まれているか、又は、自宅や家族構成などプライベートに関する情報が含まれているか ・ 氏名、住所、電話番号など、開示される頻度が高い情報が含まれているか <p>※被害者の二次被害の危険性に影響する ※情報が漏洩する範囲・程度に影響する ※被害者に対する慰謝料額、損害賠償額に影響する</p>
漏洩した件数、規模	<ul style="list-style-type: none"> ・ 被害者の数は何人か ・ 件数を特定できるのか、できないのか ・ 漏洩した期間、漏洩の始期を特定できるのか、できないのか <p>※当法人の損失や被害者に対する慰謝料額、損害賠償額に影響する</p>
漏洩した範囲	<ul style="list-style-type: none"> ・ 1か所にとどまっているか ・ 不特定多数の者に拡散されているか <p>※被害者の二次被害の危険性に影響する ※各被害者に対する慰謝料額、損害賠償額に影響する</p>
漏洩した原因	<ul style="list-style-type: none"> ・ 当法人の落ち度によるものか ・ 委託先など他社・他当法人の落ち度によるものか ・ 悪意者の介在によるものか ・ 単なる事務ミスによるものか ・ 制度的欠陥、恒常的欠陥によるものか ・ 犯罪被害によるものか ・ 原因を特定できるか、できないことに落ち度がないか <p>※会社の過失の有無・程度に影響する ※社会的非難の程度や改善策の有無内容に影響する</p>

漏洩から察知までの期間	<ul style="list-style-type: none"> ・当法人はすぐに察知できたのか ・察知が遅れた場合何故察知が遅れたのか ・当法人は事態を放置していたとは評価されないか ・当法人は事態を隠蔽していたと評価されないか <p>※被害拡大に対する社会の落ち度に影響する ※社会的非難の程度に影響する</p>
再発防止の可能性	<ul style="list-style-type: none"> ・実効性のある再発防止策がとれるのか ・再発防止策はすぐにとれるのか、時間がかかるのか ・再発防止策がとれないのか、再発の可能性がのこるのか <p>※当法人の損失の程度に影響する ※社会的非難の程度に影響する</p>