情報漏えい発生時の対応ポイント集

情報が漏えいしてしまった時、何をすべきか!!

独立行政法人情報処理推進機構
セキュリティセンター

http://www.ipa.go.jp/security/

2012年9月3日 第3版

目次

はじめに

本ポイント集は、企業（組織）の情報が漏えいした場合の事後的な対応において、何をしなければならないか、何に注意すべきかを簡潔にまとめています。

本来、企業（組織）として十分な情報セキュリティ対策を行うことにより、情報漏えいを未然に防ぐことが重要です。その一方で、こういった対策にも関わらず実際に情報漏えいが発生してしまった時に、適切な処置を行うことによってその被害を最小限に留めることも重要です。

情報漏えいを未然に防止するための対策については、

「IPA 対策のしおりシリーズ(5) 情報漏えい対策のしおり
―企業（組織）で働くあなたへ7つのポイント！！」
http://www.ipa.go.jp/security/antivirus/shiori.html

をご覧ください。

いざ情報漏えいが起こってしまった、あるいはその疑いがある場合に、対応処置を行う際、本ポイント集を参考としてご利用ください。

対応要領の詳細については、

「情報漏えいインシデント対応方策に関する調査報告書」
http://www.ipa.go.jp/security/awareness/johorouei/index2.html

をご参照ください。

1. 基本的な考え方

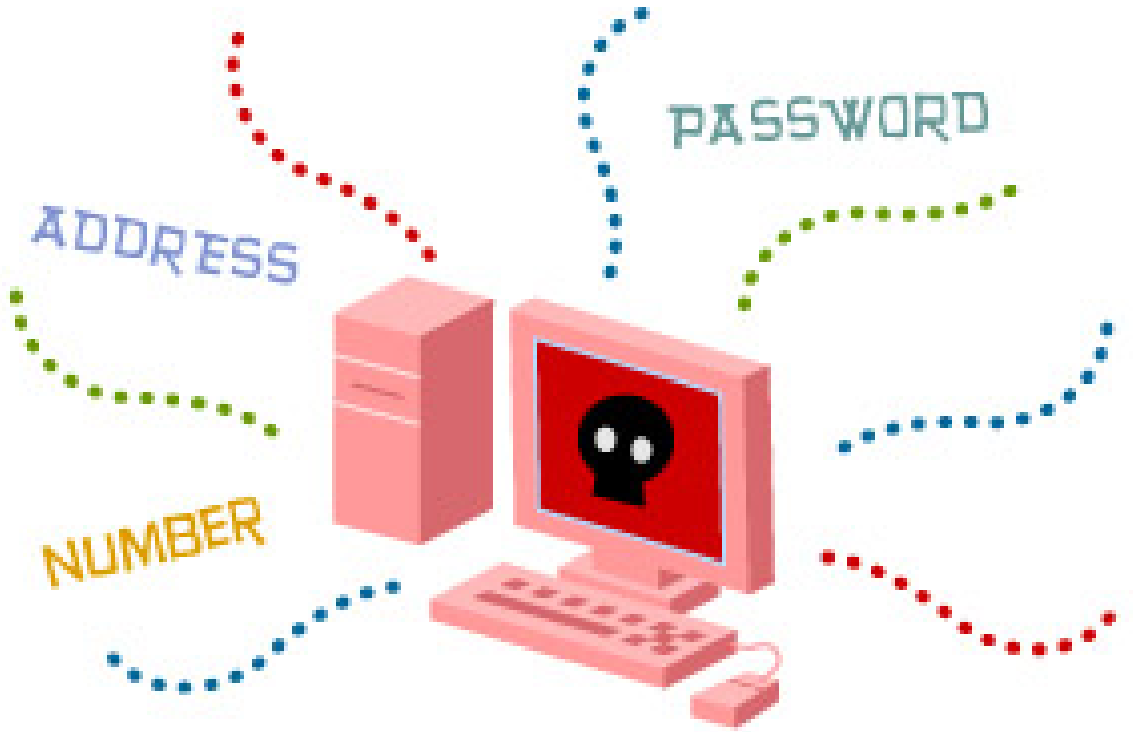
◆ なぜ情報漏えい後の対応が必要なのか？
－情報漏えい対応の目的－

情報漏えい後に対応を行う最大の目的は

「情報漏えいによる直接的・間接的被害を最小限に抑える」

ことにあります。

自分の会社（組織）のことだけでなく、自分に関係のある情報を漏えいされた最終的な被害者、顧客、取引先、株主、親会社、子会社、従業員など情報漏えいによって被害を受ける様々な関係者の被害を最小限に抑える必要があります。自社の経営方針に基づき全体のバランスを考えながら被害の最小化を図ります。



◆情報漏えい対応の5原則

（1）被害拡大防止・二次被害防止・再発防止の原則

情報漏えいが発生した場合に最も重要なことは、情報漏えいによって引き起こされる被害を最小限にとどめることです。漏えいした情報が犯罪等に使用されることを防止しなければなりません。また、一度発生した事故・事件は二度と起こることのないよう再発を防止します。

（2）事実確認と情報の一元管理の原則

情報漏えい対応においては正確な情報の把握に努めます。憶測や類推による判断や不確かな情報に基づく発言は混乱を招きます。組織の情報を一か所に集め、外部に対する情報提供や報告に関しても窓口を一本化し、正しい情報の把握と管理を行います。

（3）透明性・開示の原則

被害拡大防止や類似事故の防止、企業組織の説明責任の観点から必要と判断される場合には、組織の透明性を確保し情報を開示する姿勢で臨むことが好ましいと考えられます。情報公開により被害の拡大が見込まれるような特殊なケースを除いては、情報を公開することを前提とした対応が企業（組織）の信頼につながります。

（4）チームワークの原則

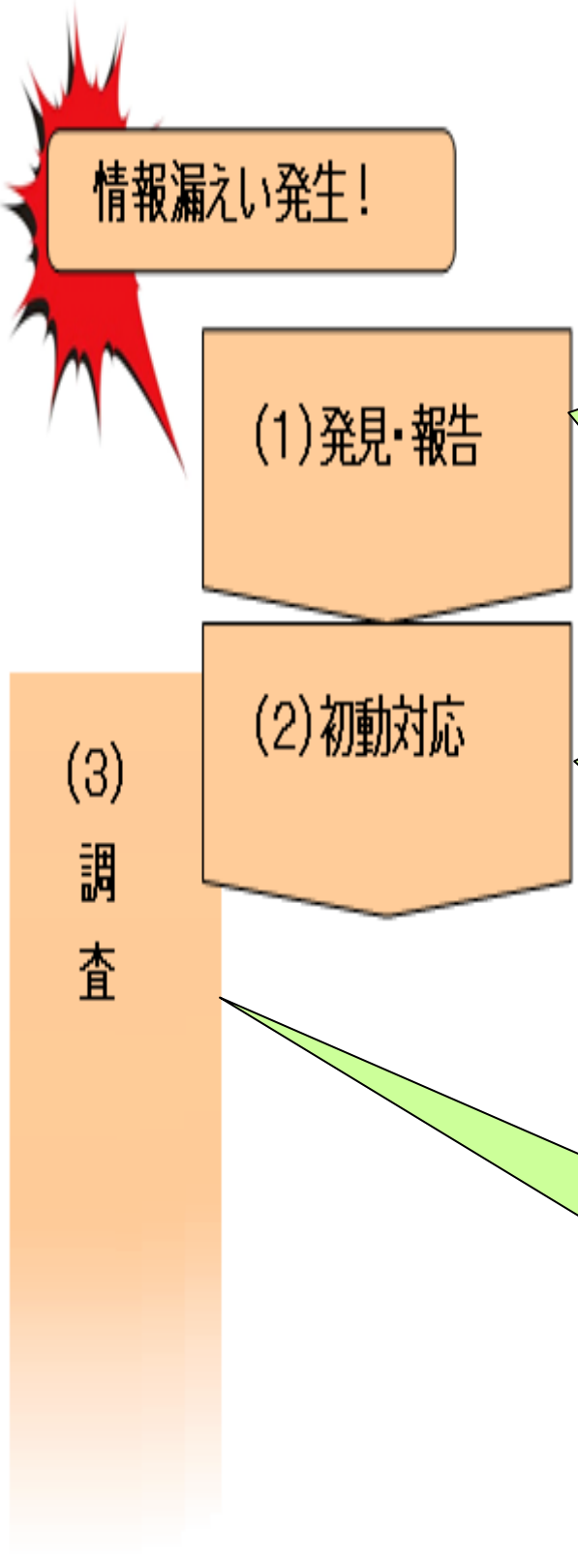
情報漏えい対応においては様々な困難な判断を迅速に行わなければならず、精神的にも大きな負担がかかります。また、経営、広報、技術、法律など様々な要素を考慮する必要があるため、組織として対応していくことが重要です。

（5）備えあれば憂いなしの原則

情報漏えいなど事故が発生した時のことを想定し、あらかじめ緊急時の体制や連絡要領などを準備しておくと、いざという時に大変役立ちます。緊急時にどう対応するべきなのか、方針や手順を作成し、日頃から訓練しておきましょう。

2.情報漏えい対応の基本ステップ

対応方法は情報漏えいのタイプにより異なってきますが、情報漏えい対応の基本的なステップは以下のとおりです。いくつかのステップを同時進行させることもあります。



情報漏えいに関する兆候や具体的な事実を確認した場合は、責任者に報告し速やかに情報漏えい対応のための体制をとります。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えいの可能性がある場合は、不用意な操作をせず、システム上に残された証拠を消してしまわないようにします。また外部から通報があった場合は、相手の連絡先等を必ず控えるようにします。

対策本部を設置し当面の対応方針を決定します。情報漏えいによる被害の拡大、二次被害の防止のために必要な応急処置を行います。情報が外部からアクセスできる状態にあったり、被害が広がる可能性がある場合には、これらを遮断する措置をとります。情報の隔離、ネットワークの遮断、サービスの停止などです。

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)の観点で調査し情報を整理します。また、事実関係を裏付ける情報や証拠を確保します。

(3) 調査

(4) 通知・報告・公表等

漏洩した個人情報の本人、取引先などへの通知、監督官庁、警察、IPA 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します。漏洩した個人情報の本人については特別な理由がない限り通知を行います。紛失・盗難のほか不正アクセス、内部犯行、脅迫等不正な金銭の要求など犯罪性がある場合は警察へ届出ます。すべての関係者への個別通知が困難な場合や、広く一般に漏えい情報による影響が及ぶと考えられる場合などは、ホームページでの情報公開や記者発表による公表を行います。ただし、情報の公表が被害の拡大を招く恐れのある時は、公表の時期、対象などを考慮します。

(5) 抑制措置と復旧

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の措置を行います。専用の相談窓口を設置し被害が発生した場合にはその動向を素早く察知し対応するようにします。また、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、アカウント等を復旧します。

(6) 事後対応

抜本的な再発防止策を検討し実施します。また、調査報告書を経営陣に提示し、被害者に対する損害の補償等について必要な措置を行います。内部職員の責任等について必要な処分手続きを行います。これらについて必要に応じて情報を開示します。

3. 情報漏えいのタイプ別対応ポイント

◆ 情報の種類に関するポイント

漏えいした情報の種類に応じて必要な対応も異なります。以下に情報タイプ毎の注意事項を示します。

個人情報

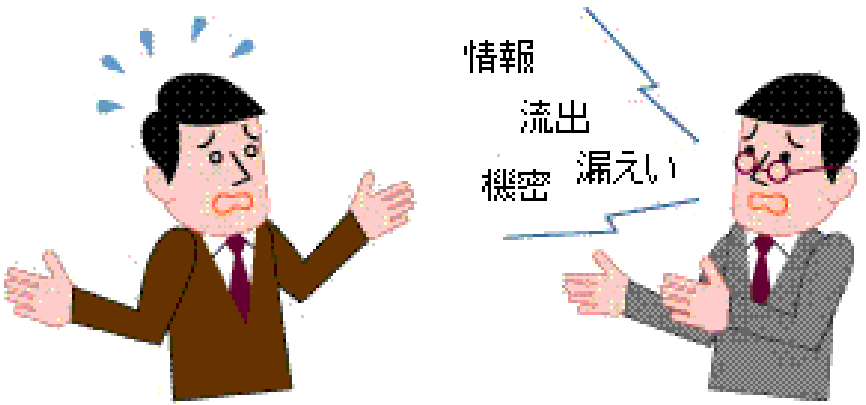
顧客や取引先、社員など個人に関する情報です。漏えいした情報に個人情報が含まれている場合には、個人情報保護法に準拠した対応が必要となります。状況により監督官庁へ報告します。また、個人情報の本人に被害が及ぶ可能性があるため、本人への通知や注意喚起など二次被害防止措置が必要です。

公共性の高い情報

漏えいした情報に発電所や通信設備など社会の重要なサービス、社会の安全に関する情報など公共性の高い情報が含まれている場合には、内容に応じて関係者・監督官庁に報告をしたり、マスコミ等に対して情報を開示する必要が生じます。

一般情報

企業（組織）の情報のうち取引先等の情報が含まれる場合には、取引先に報告し、その意向に沿った対応を行います。企業秘密など組織の重要な情報が漏えいした場合には、その内容に応じた経営判断を行います。



◆ 漏えいのタイプによるポイント

情報漏えいにはどういった形で情報が漏えいしたかによっていくつかのタイプがあります。情報漏えいのタイプによって対応のポイントが変わってきます。本ポイント集では情報漏えいを以下のタイプに分類しています。タイプ毎の注意事項については次のページ以降で解説しています。

(1)紛失・盗難

パソコンや USB メモリの入った鞄を電車の車内や店舗に忘れる、事務所や自宅に保管されていたパソコンが盗難にあうといった事件により情報の紛失や漏えいをしてしまうケースです。

(2)誤送信・Web での誤公開等

本来行ってはならないシステムの操作、設定等により情報が流出するケースです。お互いに関係のない複数のアドレスにあてた電子メールを、他人の宛先が見える形で送信してしまう場合（BCC で送信すべきところを TO や CC で送信）や、Web ページの公開サーバの設定を誤って個人情報などが誰でも見えるような状態にしてしまう場合などです。

(3)内部犯行

企業（組織）内部の従業員が不正に情報を持ち出し、外部の第三者に売ったり渡したりするケースです。名簿業者等で、持ち出された名簿が販売されていることなどもあります。

(4)Winny/Share 等への漏えい

Winny/Share を代表とする匿名ファイル交換ソフトの利用者が暴露ウイルスに感染し、自宅に持ち帰っていた業務データや電子メールの内容などを流出させてしまうようなケースです。

(5)不正プログラム

ウイルスに感染してパソコン内部のデータが電子メールに添付されてばらまかれたり、スパイウェアを送り込まれパソコンで入力した内容が外部に送信されたりするケースです。

(6)不正アクセス

アクセス制限を設けているコンピュータにネットワーク外部から不正に侵入されて情報を盗まれるケースです。

(7)風評・ブログ掲載等

組織の従業員がブログやホームページで本来秘密にすべき事項を掲載してしまったり、社内の者しか知らないはずの情報が匿名掲示板に書き込まれたりするケースです。

3. 1 紛失・盗難の場合の対応

(1)発見および報告

「参考1. 情報漏えい情報共有シート(例)P.23」に記録し、報告します。
紛失・盗難が間違いないか、もう一度確認します。

No	事故事例	発覚のきっかけ
1	パソコンや USB メモリなどを電車の中、飲み屋などに置き忘れた。	・自己申告 ・警察からの連絡 ・取得者からの連絡
2	パソコンや USB メモリなどが入った鞄をひったくりに遭い盗まれた。	
3	置き引きや車上荒らしに遭い、パソコンや USB メモリなど盗まれた。	
4	事務所荒らしに遭い、事務所のパソコンを盗まれた。	
5	請負業者に送った CD-ROM が、輸送中に紛失した。	

紛失場所の管理者(鉄道会社担当窓口、店舗窓口など)に連絡します。

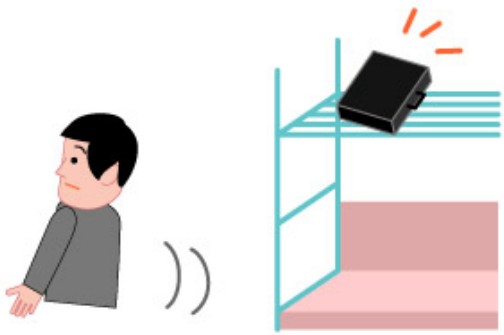
(2)初動対応

何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認します。

事実関係を5W1Hで整理する	
(1) 紛失、盗難の当事者は誰か？ (2) 何(物)が紛失、盗難に遭ったのか？ (3) 紛失、盗難の対象物に格納されていた情報は何か？ (4) いつ紛失、盗難が発生したのか？ (5) どこで紛失、盗難が発生したのか？ (6) なぜ紛失、盗難が発生したのか？ (7) 紛失、盗難が発覚した理由は何なのか？	a) 誰の情報か？ b) 何の情報か？ c) いつ頃の情報か？ d) 情報の量(件数)はどのくらいか？ e) どのような形で保存されていたか？ (暗号化／平文、HDD 保護、認証パスワード保護など)

警察に届出ます。製造番号や製品固有の特徴情報があると発見しやすくなります。
アカウント情報が含まれる場合はパスワードの変更やアカウントの停止を行います。

No	応急処置例	留意点
1	紛失物の捜索、回収	・鞄の形状、大きさ、色などの特徴、 パソコンの機種、製造番号など
2	警察への届出	
3	流出したアカウントの停止、パスワード変更	



（3）調査

企業（組織）内に残された記録から紛失・盗難にあった情報をなるべく正確に把握します。
予想される二次被害を確認します。

被害の重要度を判定する
(1) 漏えいした情報区分は？ （個人情報／公共性の高い情報／一般情報） (2) 漏えいした情報の保護策は、何を実施していたか？ (3) 影響はどこにあるか？ （個人／公共インフラ／特定企業） (4) 管理上の問題点は？

機器・媒体がオークションや中古市場に出回っていないか確認します。

（4）通知・報告・公表等

個人情報が含まれる場合で漏えいの恐れがある場合は、本人への通知とお詫びを行います。（「５（1）情報漏えいに関する公表の考え方」を参照）

また必要に応じて監督官庁に届け出ます。規模や影響範囲が大きい場合は Web 等で経緯を公表します。

（5）抑制措置と復旧

No	二次被害防止策例	留意点
1	クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す	

バックアップやコピーから修復可能な情報を復旧します。

（6）事後対応

各社のポリシーにあわせ、事故の再発防止策を実施する。
建物への侵入防止、情報資産の保管方法、情報資産の持出し管理、情報の暗号化やアクセス制御、およびその徹底など、物理面、技術面、管理面、教育面など問題点を総合的に検討し改善します。

報告行為について評価し、隠ぺい工作が起こらないよう配慮します。

3. 2 誤送信・Web での誤公開の場合の対応

（1）発見および報告

ミスをした本人、もしくはそれを発見した第三者からの指摘により発見されます。外部からの指摘を受けた場合は連絡先を確認します。

「参考1. 情報漏えい情報共有シート（例）P.23」に記録し、報告します。

No	事故事例	発覚のきっかけ
1	相手のメールアドレスを打ち間違え、他人に誤送信した。	・自己申告(内部発見) ・受信者からの指摘 （風評を含む）
2	同報メールの宛先をBCC:に書くべきところ、CC:にして送信した。	
3	FAX で相手の電話番号を間違えて送信した。 郵便で、相手の住所を間違えて郵送した。	
4	Web関係のぜい弱性により、非公開情報が参照できていた。	
5	Webアプリケーションのミスで、他人の個人情報を表示した。	
6	Webサイトから他の会員に誤ってIDパスワードを送信した。	
7	Webで誤って非公開情報を公開情報としていた。（サーバ移行時の非公開情報削除もれ、IDパスワードで保護されるべき情報がサーバの設定ミスで公開エリアに保管した、公開サーバへ誤って非公開情報を転送したなど）	
8	譲渡が禁止されている情報を第三者に売却した。	

（2）初動対応

何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認します。

事実関係を5W1Hで整理する	
(1) 誤送信・Web誤公開の当事者は誰か？ (2) 何(物)を誤送信・Web誤公開したのか？ (3) 誤送信・Web誤公開の対象物に格納されていた情報は何か？ (4) いつ誤送信・Web誤公開が発生したのか？ (5) どこで誤送信・Web誤公開が発生したのか？ (6) なぜ誤送信・Web誤公開が発生したのか？ (7) 誤送信・Web誤公開が発覚した理由は何なのか？	a) 誤の情報か？ b) 何の情報か？ c) いつ頃の情報か？ d) 情報の量（件数）はどのくらいか？ e) どのような形で保存されていたか？（暗号化／平文、パスワード保護など）

誤送信で送信先が明らかな場合は受信者に対しミスについてお詫びし、受信した情報について削除を依頼します。誤公開の場合は直ちに当該情報を削除するか、アクセス制限措置を施し外部から参照できないようにします。

No	応急処置例	留意点
1	【メール・FAX・郵便の誤送信／誤譲渡】 受信者への連絡と情報の廃棄	・受信者に連絡が取れない場合の対応 ・該当 Web 情報を保持または掲載している第三者が情報削除に応じない場合の対応
2	誤って Web に公開した情報の削除	

（3）調査

漏えいした情報の範囲、原因、被害の状況等について調査します。誤公開の場合は、どういった範囲で何人が参照したかアクセスログを使って調査します。

予想される二次被害を確認します。

被害の重要度を判定する
(1) 漏えいした情報区分は？ （個人情報／公共性の高い情報／一般情報）
(2) 漏えいした情報の保護策は、何を実施していたか？
(3) 影響はどこにあるか？ （個人／公共インフラ／特定企業）
(4) 管理上の問題点は？

（4）通知・報告・公表等

個人情報が含まれる場合で漏えいの恐れがある場合は、本人への通知とお詫びを行います。（「５（1）情報漏えいに関する公表の考え方」を参照）

また必要に応じて監督官庁に届け出ます。規模や影響範囲が大きい場合は Web 等で経緯を公表します。

（5）抑制措置と復旧

情報システムの不具合が原因の場合は、システムを修正するか使用を制限します。人的な作業ミスの場合は、ミスを見逃さないよう作業手順にチェックの仕組みを追加します。

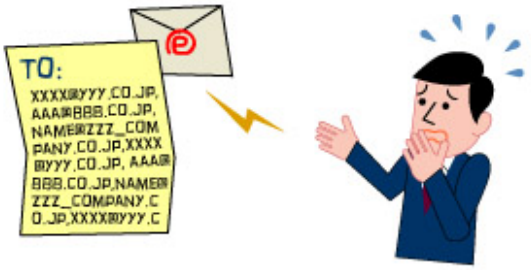
また社員・職員の教育・啓蒙を行います。すべての Web ページの設定を再確認します。

No	二次被害防止策例	留意点
1	クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す	
2	Web 検索サイトからのキャッシュ削除	
3	Web サイトの停止、Web サイトのぜい弱性の除去	

（6）事後対応

違反や管理上のミスがあった場合は必要な処分を行います。また、漏えい情報による被害の補償等救済処置を行います。

各社のポリシーにあわせ、事故の再発防止策を実施する。
多数の宛先への同時送信の作業手順を、ミスをした原因とミスを見逃した原因の両面から見直し、必要に応じて、専用システムの導入等を行います。 Web ページの設定・公開要領を見直します。



3. 3 内部犯行の場合の対応

（1）発見および報告

ダイレクトメールや架空請求、振り込め詐欺など顧客から自分の情報が不正に利用されているようだとの問い合わせを受け発覚するケースが多いようです。また外部から名簿を買い取ってくれというような脅迫を受けたり、マスコミ等から情報が漏えいしているようだとの問い合わせを受け発覚することもあります。相手の連絡先を確認し、どういった情報を持っているのか提示してもらい漏えいの事実を確認します。

「参考1．情報漏えい情報共有シート（例）P.23」に記録し、報告します。

No	事故事例	発覚のきっかけ
1	社内データベースから顧客情報を不正に持ち出し転売した。	・外部からの指摘 （風評を含む）
2	社外 Web システムに、過去に業務で使用していた ID を利用してアクセスし、不正にデータを持ち出した。	
3	社内から設計機密情報を不正に持ち出し、他社に渡した。	

（2）初動対応

何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認します。

事実関係を5W1Hで整理する	
(1) 内部犯行の当事者は誰か？ (2) 何(物)を持ち出したのか？ (3) 内部犯行の対象物に格納されていた情報は何か？ (4) いつ内部犯行が行われたのか？ (5) どこで内部犯行が行われたのか？ (6) なぜ内部犯行が発生したのか？ (7) 内部犯行が発覚した理由は何なのか？	a)誰の情報か？ b)何の情報か？ c)いつ頃の情報か？ d)情報の量（件数）はどのくらいか？ e)どのような形で保存されていたか？（暗号化／平文、HDD 保護、パスワード保護など）

内部犯行の場合は漏えいの規模や範囲が大きくなる傾向があり、慎重な対応が必要です。また、社内に情報を持ち出した犯人がいると思われる場合は、重要な情報を証拠隠滅されないよう注意します。

No	応急処置例	留意点
1	社内対象サイト（イントラネットサーバ、共有ファイルサーバなど）の ID 停止やアクセス制限の実施	・証跡保存を実施する際には、コンピュータフォレンジックを考慮した確保が必要なため、慎重に対応すること。（専門家への依頼など）
2	内部犯行当事者の使用した関連装置の確保(証跡保存)	

（3）調査

漏えいした情報の範囲、原因、被害の状況等を明らかにします。漏えい情報の範囲から、持ち出された時期や当該情報にアクセスできた人物などを絞り込みます。

予想される二次被害を確認します。

被害の重要度を判定する
(1) 漏えいした情報区分は？（個人情報／公共性の高い情報／一般情報）
(2) 漏えいした情報の保護策は、何を実施していたか？
(3) 影響はどこにあるか？（個人／公共インフラ／特定企業）
(4) 管理上の問題点は？

（4）通知・報告・公表等

犯罪に発展する可能性がある場合は、早めに警察に相談します。規模が大きい場合はWeb等での告知の他、記者発表などの要否も検討します。

個人情報が含まれる場合は対象が特定できた時点で、なるべく早く本人に通知できるようにします。（「５（1）情報漏えいに関する公表の考え方」を参照）

また必要に応じて監督官庁に届け出ます。

（5）抑制措置と復旧

犯人を特定した上で再発防止策を講じます。通常は認証やアクセス制御、ログの取得等社内の情報管理体制を強化します。アカウントの再発行や登録情報の変更を行い通常の業務、サービスに復帰します。

No	二次被害防止策例	留意点
1	警察への届出	・第三者からの情報回収 該当情報を保持または掲載する第三者が情報回収に応じてくれない場合の対応
2	漏えいの可能性のある情報の回収	
3	ID パスワード、アクセス権限の見直し	
4	ぜい弱性の除去	
5	クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す	

（6）事後対応

原因の究明と再発防止策の実現をします。違反や管理上のミスがあった場合は必要な処分をします。また、漏えい情報による被害の補償等救済処置を行います。

各社のポリシーにあわせ、事故の再発防止策を実施する。

3. 4 Winny/Share 等への漏えいの場合の対応

（1）発見および報告

外部からの通報により発見することが多いようです。後々の調査のために通報者の連絡先を必ず確認しておきます。またどのような情報が漏えいしているかについてなるべく詳しい情報を聞き、可能であれば取得した情報を提供してもらうようにします。

「参考1．情報漏えい情報共有シート（例）P.23」に記録し、報告します。

No	事故事例	発覚のきっかけ
1	社員が会社の機密情報や個人情報を自宅に持ち帰り(USB メモリでの持ち出しや社内メールを自宅メールに転送するなど)、個人パソコンに情報を保存しており、本人や家族がファイル交換ソフトを利用中に暴露ウイルスに感染し、ファイル交換ネットワークへ情報が漏えいした。	・外部からの指摘（風評を含む）

（2）初動対応

漏えい情報の内容、範囲を確認します。また漏えい元を特定し、調査に対する本人の協力を得ます。

事実関係を5W1Hで整理する	
(1) Winny/Share ネットに流出させた当事者は誰か？ (2) 何(物)を Winny/Share ネットに流出させたのか？ (3) Winny/Share ネットに流出した情報は何か？ (4) いつ Winny/Share ネットへの流出が発生したのか？ (5) どこで Winny/Share ネットへの流出が発生したのか？ (6) なぜ Winny/Share ネットへの流出が発生したのか？ (7) Winny/Share ネットへの流出が発覚した理由は何なのか？	a)誰の情報か？ b)何の情報か？ c)いつ頃の情報か？ d)情報の量（件数）はどのくらいか？ e)どのような形で保存されていたか？（暗号化／平文、HDD 保護、パスワード保護など）

現在も Winny/Share を使用しているようであればただちに停止します。

No	応急処置例	留意点
1	インターネットからのパソコンの切り離し(Winny/Share の利用停止)	・パソコンは調査に必要なファイル等が削除されないように、極力使用時の状態に手を加えないままで提出してもらいます。
2	漏えいしたファイル(情報)の確保	

（3）調査

漏えい情報の内容、範囲、時期等について調査します。また本人がその情報を流出するに至った経緯についても調査します。調査のためにWinny/Share 等を使用することは被害の拡大につながりかねませんので行なうべきではありません。

予想される二次被害を確認します。

被害の重要度を判定する
(1) 漏えいした情報区分は？ （個人情報／公共性の高い情報／一般情報）
(2) 漏えいした情報の保護策は、何を実施していたか？
(3) 影響はどこにあるか？ （個人／公共インフラ／特定企業）
(4) 管理上の問題点は？

（4）通知・報告・公表等

漏えい情報に個人情報が含まれる場合には本人に通知しお詫びします。（「５ (1) 情報漏えいに関する公表の考え方」 を参照）必要に応じ監督省庁への報告を行います。Winny/Share などは要求の多いファイルをネットワーク上の多くのコンピュータに拡散させる仕組みを持っていますので、一旦人々の興味をそそり人気のあるファイルになってしまうと、ネットワーク上にファイルが拡散しいつまでも漏えいが続くことになります。事件の公表がWinny/Share のダウンロードを誘発する恐れがある場合は、しばらくの間公表を控えるという考え方もあります。被害防止の観点から最善と思われる措置をとります。

（5）抑制措置と復旧

Winny/Share の漏えい情報については、とにかく話題性を高めずネットワーク上のファイルが自然に消滅することを待つのが得策といえます。また、多くの場合自宅において業務データを漏えいするケースが多いので、社外へのデータ持ち出しの制限などを再徹底する必要があります。全従業員に対してファイル交換ソフトの利用の危険性を周知し、ファイル交換ソフトの利用状況調査及び対処を行います。

No	二次被害防止策例	留意点
1	ウイルス駆除	・Winny/Share ネットワーク上の情報を完全削除することはほぼ不可能です
2	個人のパソコンから会社の機密情報や個人情報の削除	
3	クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す	

（6）事後対応

違反や管理上のミスがあった場合は必要な処分を行います。また、必要に応じて漏えい情報による被害の補償等救済処置を行います。

各社のポリシーにあわせ、事故の再発防止策を実施する。
会社からの情報持ち出し制限、個人パソコンの業務利用制限、などのルール見直し

3. 5 不正プログラム(ウイルス、スパイウェア等)の場合の対応

(1)発見および報告

不正プログラムの存在は多くの場合、ウイルス対策ソフトやネットワークの監視、メール等を受信した外部からの通知により発覚します。

「参考1. 情報漏えい情報共有シート(例)P.23」に記録し、報告します。

No	事故事例	発覚のきっかけ
1	ウイルスに感染し、パソコンを不正操作され、パソコン内の会社機密情報が悪意のある第三者に窃取された。	・自己申告／内部発見 ・外部からの指摘 (風評を含む)
2	ウイルスに感染し、会社機密情報が Web サイトに掲載され、不特定多数の人に閲覧可能な状態になった。	

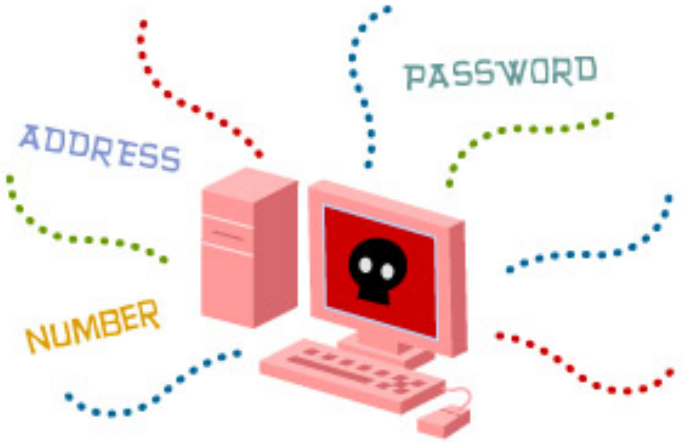
(2)初動対応

何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認します。

事実関係を5W1Hで整理する	
(1) ウイルス感染した当事者は誰か？	a)誰の情報か？
(2) 何(物)がウイルス感染したのか？	b)何の情報か？
(3) ウイルス感染により漏えいした情報は何か？	c)いつ頃の情報か？
(4) いつウイルス感染したのか？	d)情報の量(件数)はどのくらいか？
(5) どこでウイルス感染したのか？	e)どのような形で保存されていたか？
(6) なぜウイルス感染したのか？	(暗号化／平文、HDD 保護、パスワード保護など)
(7) ウイルス感染が発覚した理由は何なのか？	

不正プログラムの存在が確認された場合は、直ちにシステムの使用を停止し、システムから不正プログラムの除去などの対応を行います。不正プログラムの種類が特定できる場合は、IPA やウイルス対策ベンダなどの情報に基づき対処します。

No	応急処置例	留意点
1	ウイルス感染したパソコンの特定	
2	ウイルス感染したパソコンのネットワークからの切り離し	



（3）調査

重要なデータをいったん外部メディアにバックアップします。バックアップには不正プログラムが混入している可能性も高いので取扱いに注意します。パソコンに残されたデータやアクセスの履歴から漏えいした情報を特定します。

予想される二次被害を確認します。

被害の重要度を判定する
(1) 漏えいした情報区分は？ （個人情報／公共性の高い情報／一般情報） (2) 漏えいした情報の保護策は、何を実施していたか？ (3) 影響はどこにあるか？ （個人／公共インフラ／特定企業） (4) 管理上の問題点は？

（4）通知・報告・公表等

漏えい情報に個人情報が含まれる場合には本人に通知しお詫びします。（「５ (1) 情報漏えいに関する公表の考え方」を参照）必要に応じ監督省庁への報告を行います。

（5）抑制措置と復旧

被害にあったパソコンは念のため OS からインストールしなおした方が良いでしょう。プログラムもバックアップから戻さず、再インストールしなおした方が良いでしょう。バックアップのデータについて、最新のウイルス定義ファイル等を使用して検査し復旧します。

No	二次被害防止策例	留意点
1	ウイルス名の特定と駆除	・第三者からの情報回収 該当情報を保持または掲載する第三者が情報回収に応じてくれない場合の対応
2	ぜい弱性の除去	
3	漏えいした情報の回収	
4	クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す	

（6）事後対応

必要に応じて漏えい情報による被害の補償等救済処置を行います。

各社のポリシーにあわせ、事故の再発防止策を実施する。
重要な情報の隔離やウイルス対策製品の導入など再発防止のための技術的な対策を行います。 またユーザに対して不正プログラム対策の注意喚起を行います。

3. 6 不正アクセスの場合の対応

(1)発見および報告

不正アクセスの多くは企業(組織)がインターネットに接続しているサーバに対して行われ、ログの確認やセキュリティ対策機器の警報によって発見されることが多いようです。重要な情報が格納されているパソコンやサーバに対する不正アクセスが確認された場合は、情報漏えいの危険性がありますので対策が必要です。不正アクセスが明らかな場合は警察に相談します。

「参考1. 情報漏えい情報共有シート(例)P.23」に記録し、報告します。

No	事故事例	発覚のきっかけ
1	Web での ID パスワードを不正利用され、情報を他のサイトに掲示された。	・自己申告／内部発見 ・外部からの指摘 (風評を含む)
2	Web でのぜい弱性を悪用し不正アクセスされ、非公開情報を窃取された。	
3	Web アプリケーションのぜい弱性を悪用され、データベースサーバの非公開情報を窃取された。	
4	Web アプリケーションのぜい弱性を悪用され、Web サーバにウイルスを埋め込まれた。	

(2)初動対応

何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認します。

事実関係を5W1Hで整理する	
(1) 不正アクセスした当事者は誰か？	a)誰の情報か？
(2) 何(物)を不正アクセスされたのか？	b)何の情報か？
(3) 不正アクセスされた情報は何か？	c)いつ頃の情報か？
(4) いつ不正アクセスが行われたのか？	d)情報の量(件数)はどのくらいか？
(5) どこで不正アクセスが行われたのか？	e)どのような形で保存されていたか？
(6) なぜ不正アクセスが発生したのか？	(暗号化／平文、HDD 保護、パスワード保護など)
(7) 不正アクセスが発覚した理由は何なのか？	

不正アクセスによって個人情報や機密情報が漏えいする危険性が確認された場合は、直ちにネットワークから切り離してサービスを停止するなどの処置が必要となります。クレジットカードやアカウント情報が漏えいした場合は、カード会社への通知やアカウント停止などの緊急処置を行います。

No	応急処置例	留意点
1	不正アクセスを受けた機器(サイト)のネットワークからの切り離し	・不正アクセスされた原因、経路を特定せずに、代替サイトを立ち上げると、再び不正アクセスされる可能性が高い
2	不正アクセスを受けた機器(サイト)の停止	
3	代替サイトの立ち上げ	

（3）調査

不正アクセスの場合、機器に残された記録は重要な証拠となるため、内容が変更されたり損なわれたりしないよう証拠保全の措置をとります。どのようにして侵入が行われたのか、どういった情報にアクセスした形跡があるかなどについて調査します。

予想される二次被害を確認します。

被害の重要度を判定する
(1) 漏えいした情報区分は？ （個人情報／公共性の高い情報／一般情報）
(2) 漏えいした情報の保護策は、何を実施していたか？
(3) 影響はどこにあるか？ （個人／公共インフラ／特定企業）
(4) 管理上の問題点は？

（4）通知・報告・公表等

個人情報にアクセスされた可能性がある場合は、その範囲を特定し本人に通知しお詫びします。（「５ (1) 情報漏えいに関する公表の考え方」を参照）必要に応じ監督省庁への報告を行います。また規模が大きい場合は Web での情報公開のほか記者発表なども検討します。

（5）抑制措置と復旧

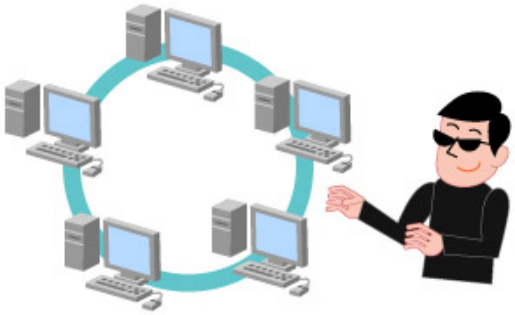
侵入されたサーバ等の内容をバックアップし、再発防止措置を行った上でサービスを復旧します。また、アカウント情報等が漏えいした場合には、アカウントの再発行やパスワードの変更等の措置を行います。

No	二次被害防止策例	留意点
1	漏えいした情報の回収	・第三者からの情報回収 該当情報を保持または掲載する第三者が情報回収に応じてくれない場合の対応
2	Web サーバ設定の見直し	
3	ID パスワード、アクセス権限の見直し	
4	サーバ、Web アプリケーションのぜい弱性の除去	
5	クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す	

（6）事後対応

違反や管理上のミスがあった場合は必要な処分を行います。また、必要に応じて漏えい情報による被害の補償等救済処置を行います。

各社のポリシーにあわせ、事故の再発防止策を実施する。



3. 7 風評・ブログ掲載の場合の対応

(1)発見および報告

風評・ブログ掲載については、社員・職員が発見する場合と、第三者が通報してくる場合があります。

「参考1. 情報漏えい情報共有シート(例)P.23」に記録し、報告します。

No	事故事例	発覚のきっかけ
1	社内の機密情報が匿名掲示板に書き込まれた。	・外部からの指摘 (風評を含む)
2	社員個人が公開しているブログで、会社の機密情報について記載していた。	

(2)初動対応

何の情報がどの程度含まれていたのか、確認します。

事実関係を5W1Hで整理する	
(1) 掲示板、ブログに書き込んだ当事者は誰か？ (2) 何(物)を掲示版、ブログに書き込まれたか？ (3) 掲示版、ブログに書き込まれた情報は何か？ (4) いつ掲示版、ブログに書き込まれたのか？ (5) どこで掲示版、ブログに書き込まれたのか？ (6) なぜ掲示版、ブログへ書き込まれたのか？ (7) 掲示版、ブログへの書き込みが発覚した理由は何なのか？	a)誰の情報か？ b)何の情報か？ c)いつ頃の情報か？ d)情報の量(件数)はどのくらいか？ e)どのような形で保存されていたか？ (暗号化／平文、HDD 保護、パスワード保護など)

漏えい情報の範囲、内容を確認します。個人のブログなどの場合は、本人が悪意を持っていないことが多いので、本人に注意し削除させます。掲示板への書き込みについては反論を書き込むなど表立った反応はせずに、掲示板の管理人に対して削除を依頼します。管理人が削除に応じない場合は、プロバイダ責任制限法に基づく法的手続きをとることも検討します。また従業員等が勝手に反論したりすることのないよう周知徹底します。

No	応急処置例	留意点
1	掲示板に書き込まれた情報の削除	・掲示板の管理人が削除に応じてくれない場合の対応
2	ブログに書き込まれた情報の削除	

（3）調査

漏えいの経路等について調査を行います。また同様の情報が他のページなどに転載されていないか確認します。

予想される二次被害を確認します。

被害の重要度を判定する
(1) 漏えいした情報区分は？ （個人情報／公共性の高い情報／一般情報）
(2) 漏えいした情報の保護策は、何を実施していたか？
(3) 影響はどこにあるか？ （個人／公共インフラ／特定企業）
(4) 管理上の問題点は？

（4）通知・報告・公表等

個人情報が含まれる場合は、本人に通知とお詫びを行います。（「５ (1) 情報漏えいに関する公表の考え方」 を参照）必要に応じ監督省庁への報告を行います。

内容が企業（組織）の不祥事や問題に関するものである場合には、問題解決のためのしかるべき対応をとります。事実を隠ぺいするのではなく誠実な対応をとった方が後々良い結果につながります。

（5）抑制措置と復旧

情報漏えいに至った原因を究明し、再発防止策を講じます。秘密にすべき情報とそうでない情報の区別が明確でない場合はこれを明確にします。多くの場合社員・職員に対する教育・啓蒙が必要です。

No	二次被害防止策例	留意点
1	検索サイトからのキャッシュ削除	

（6）事後対応

被害者へのお詫びや損害の補償、内部処分等を行います。

各社のポリシーにあわせ、事故の再発防止策を実施する。
機密情報の格付け見直しと社員への周知徹底

4.発見・報告におけるポイント

情報漏えい対応においては、事実確認と情報の一元管理が重要です。

情報漏えいを発見したり、外部から連絡を受けたら、口頭ではなく、以下のような情報共有シートに必要事項を記入することで、正確な報告を行いましょう。

参考1. 情報漏えい情報共有シート(例)

件名	**〇〇の情報漏えいについて**		
報告者所属	〇〇事業部〇〇担当	発災当事者所属	〇〇事業部〇〇担当
報告者氏名	情報　太郎	発災当事者氏名	漏洩　次郎
報告者 Tel	03-XXXX-XXXX	発災当事者 Tel	03-XXXX-XXXX
報告者 Mail	XXX@XX.XX	発災当事者 Mail	XXX@XX.XX
下記の事項で、判明していることを記述する。 初報なので、不明な項目は不明として迅速に報告する事。			
◆情報漏えいの情報のソース(誰が発見したのか、どこから漏えい情報を入手したのか)			
◆情報漏えい判明日時			
◆情報漏えい発生日時			
◆情報漏えい内容			
◆情報漏えい内容の件数			
◆想定される原因			
◆対応状況(行なっていれば記述) ・特に組織外からの通報の場合、相手が何を要求しているのかを記述			

5. 通知・報告・公表等におけるポイント

（1） 情報漏えいに関する公表の考え方

透明性・開示の原則から、発生した情報漏えいについてなるべく早く公表を行うことを考えます。個人情報が漏えいした場合は、本人にその事実を知らせお詫びするとともに、詐欺や迷惑行為などの被害にあわないよう注意喚起します。また個人情報漏えい以外の場合でも最初に関係者への通知を考えます。個人情報漏えいの被害者や関係者に通知し意向を確認した上で、一般に公表が必要と判断される場合は、ホームページでの掲載、記者発表などを行います。

公表にあたっては、まず報道機関との窓口を一本化し対外的な情報に不整合が生じないようにします。ホームページのトップページまたはトップページからリンクする形で、下に示す公表用資料の内容を掲載します。記者発表を行う場合は報道機関等に FAX で情報を送付します。取材については電話ではなく、なるべく対面での対応とし、２～３件以上の取材申し込みが来た段階で記者会見の開催を検討します。

取材、記者会見の対応においては記者の背後には多数の読者、視聴者がいることを意識します。公表用資料の他に事実関係を説明する資料を準備し正確な情報が伝わるよう配慮します。記者会見に臨むにあたっては想定問答集を作成するなどして、事前練習を行います。回答できない質問については、その場で無理に回答しようとせずに、確認の上追って回答するようにします。

参考2. 公表用資料に含むべき項目（例）

序文（発生した情報漏えいに関するお詫び、会社としての姿勢など）
事故発生に関する状況報告
事実経緯
調査方法及び状況
漏えいした情報の内容
事故の被害内容（二次被害の影響含む）
事故原因
当面の対応策
再発防止策
問い合わせ窓口（事故に関する連絡先）

（2） 警察への届出

紛失の場合は遺失届を、盗難の場合は盗難の被害届を、下記のような可能性のある場合は、警察へ被害届を行うことを検討します。

(a)従業員の内部犯行によって情報が漏えいしてしまった場合
（背任、不正競争防止法違反等被疑事件）
(b)外部からの侵入等によって情報が漏えいしてしまった場合
（不正アクセス禁止法違反被疑事件）
(c)漏えい情報に関して不正な金銭等の要求を受けた場合
（恐喝・脅迫・強要等被疑事件）

（3） 監督官庁への報告

個人情報が漏えいしてしまった場合は、業種別の監督官庁に対して報告を行わなければなりません。報告要領、報告すべき項目については各監督官庁により定められていますので、巻末の参考情報「個人情報の保護に関するガイドラインについて（消費者庁）」を参考にしてください。以下に報告に含むべき代表的な項目を示します。

参考3. 監督官庁への報告に含むべき項目（例）

事業者名
発覚日
事故原因
漏えいした情報の内容
事故の被害内容（二次被害の影響含む）
警察届出有無
個人への連絡
再発防止策

（4） JPCERT コーディネーションセンターによる支援

不正アクセスなどによる情報漏えい等において、漏えい先あるいは攻撃元となっている組織との調整に関しては JPCERT コーディネーションセンターの支援を受けることができます。JPCERT コーディネーションセンターでは中立的な立場から情報セキュリティインシデントに関する報告の受付、対応の支援活動を行っています。

6. 参考情報

- 個人情報の保護について（消費者庁）
  http://www.caa.go.jp/seikatsu/kojin/

- 個人情報の保護に関するガイドラインについて（消費者庁）
  http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou.html

- 警察庁サイバー犯罪対策（警察庁）
  http://www.npa.go.jp/cyber/legislation/

- 都道府県警察本部のサイバー犯罪相談窓口等一覧（警察庁）
  http://www.npa.go.jp/cyber/soudan.htm

- JPCERT コーディネーションセンター
  http://www.jpcert.or.jp/

- IPA 情報セキュリティ安心相談窓口
  http://www.ipa.go.jp/security/anshin/

IPA 対策のしおり シリーズ
http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(9) 初めての情報セキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(10) 標的型攻撃メール 対策のしおり

- IPA「情報漏えいインシデント対応方策に関する調査」
  http://www.ipa.go.jp/security/awareness/johorouei/index2.html

情報漏えい発生！

（1）発見・報告

（2）初動対応

（3）調査

（4）通知・報告・公表等

（5）抑制措置と復旧

（6）事後対応

IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
（文京グリーンコートセンターオフィス16階）
URL http://www.ipa.go.jp/security/

【情報セキュリティ安心相談窓口】
URL http://www.ipa.go.jp/security/anshin/
E-mail anshin@ipa.go.jp