別冊資料　3

# 情報セキュリティ
# マニュアル

Security

2025.4　初版

全国教職員互助団体協議会

# 目　　次



# はじめに

情報システムやインターネットは、互助団体の事業運営に欠かせないものとなりました。それらは、各団体における利便性向上に寄与する一方、その脆弱性を標的とした悪意を持った第三者からの攻撃という危険に直面することにもなっています。

ひとたび事故が起こると、情報システム停止による損失、個人情報の漏洩による組織の信頼低下など大きな被害に繋がりかねません。

情報セキュリティに対するリスクマネジメントは、重要な経営課題であり、特に個人情報を取扱う我々教職員互助団体は、これを保護することが社会的責務となっています。

このため、情報セキュリティに対する意識を高め、事故を未然に防ぐとともに、万一事故が起こった時にも迅速で適切な対応を行えるよう、本マニュアルを作成いたしました。

各団体におかれましては、是非このマニュアルをご一読のうえ、リスクへの備えや職員のセキュリティ意識の向上にお役立ていただければ幸いです。

2025 年 4 月　全国教職員互助団体協議会

# 情報セキュリティ事故(インシデント)

## 情報セキュリティ事故とは

情報セキュリティ事故は、「インシデント」とも呼ばれ、情報漏洩やウイルス感染、情報システムの機能停止等、金銭被害や信用低下といった損害に繋がる可能性のある事象が発生することを指します。

(代表的な事例)

＝内的要因＝
- 職員のメール誤送信や添付、送信設定ミスによる情報漏洩
- アクセス権限者によるデータ消去や改ざん
- ログイン ID やパスワードの使い回しといった杜撰な管理がもたらす不正アクセス
- 私物端末利用による情報漏洩やウイルス感染
- 重要情報が含まれたデバイス（CD、USB メモリ等）の紛失、盗難

＝外的要因＝
- サイバー攻撃による身代金要求
- 不正ログインによる乗っ取りやなりすまし
- 天災（火事、地震、雷など）による情報損失


↑上場企業とその子会社が公表している個人情報の漏洩・紛失事故調査。
2023 年に発生した事故は 175 件、漏洩した個人情報は約 4,091 万人分（前年比約 7 倍）

## 法人が被る不利益

情報セキュリティ事故が発生することにより、以下の不利益を被る可能性があります。

(1)金銭の損失

インターネットバンキングに関連した不正アクセスや不正送金といった直接被害、また預かった機密情報や個人情報を万一漏洩させ、顧客（取引先や会員（組合員））から損害賠償請求を受ける間接被害により大きな経済的損失を背負う可能性があります。

(2)関係者や社会に対する信頼喪失

重要な情報に関する事故が発生した場合、たとえそれが不可抗力であっても管理責任が問われ、社会的信用が失われます。また、法人の代表者や管理職は善管注意義務違反や任務懈怠に基づく責任が問われることもあります。

(3)事業の停止

情報システムが使用できなくなることで、事業の停止や遅延を招き、通常の業務が阻害される場合があります。

(4)職員への心理的影響

情報セキュリティ事故の原因が、セキュリティ対策の不備を悪用した内部不正だった場合、職員のモラル低下の原因にもなります。また、事故の原因となった職員のみを罰して管理職が責任をとらなかった場合、管理職への信頼が薄れ、働く意欲を失うことも考えられます。

# 現状把握と対策

情報セキュリティに関わる項目を種類別に挙げました。設問ごとに自法人の実施状況を確認し、取組みが不足していると考えられる項目については、対策を検討してください。

| 項目 | No. | 内　　容 | ﾁｪｯｸ | 掲載ﾍﾟｰｼﾞ |
|---|---|---|---|---|
| 1<br>ネット<br>ワーク | 1-1 | PC 等、情報機器の OS やソフトウェアは常に最新の状態にしていますか？ | | → P5 |
| | 1-2 | ウイルス対策ソフトを導入し、ウイルス定義ファイル等を常に最新の状態にしていますか？ | | |
| | 1-3 | 無線 LAN を安全に使用するために適切な暗号化方式を設定するといった対策をしていますか？ | | |
| | 1-4 | パスワードは破られにくい複雑なものにしていますか？ | | → P6 |
| | 1-5 | パソコンやサーバーのウイルス感染、故障による重要情報の消失に備えてバックアップを取っていますか？ | | |
| | 1-6 | インターネットを介したウイルス感染や SNS への書き込みに起因するトラブルへの対策をしていますか？ | | |
| | 1-7 | クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？ | | → P7 |
| 2<br>電子<br>メール | 2-1 | 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気を付けていますか？ | | → P8 |
| | 2-2 | 電子メールの送信ミスを防ぐ取組みをしていますか？ | | |
| | 2-3 | 重要情報は電子メール本文ではなく、添付するファイルに記載しパスワード等で保護していますか？ | | |
| 3<br>重要情報<br>の取扱い | 3-1 | 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は、書庫等に安全に保管していますか？ | | → P9 |
| | 3-2 | 重要情報が記載された書類や電子媒体を持ち出す際には、盗難や紛失に備えた対策をしていますか？ | | |
| | 3-3 | 重要情報が記載された書類やデータを破棄する際には、復元できないようにしていますか？ | | |
| | 3-4 | 重要情報の授受を行う取引先との契約書には、秘密保持条項を規定していますか？ | | |
| 4<br>事務所内<br>留意事項 | 4-1 | 離席時に PC 画面の覗き見や勝手な操作ができないようにしていますか？ | | → P10 |
| | 4-2 | 退社時に PC や備品を施錠保管する等、盗難防止対策をしていますか？ | | |
| | 4-3 | 事務所が無人になる時の施錠忘れ対策をしていますか？ | | |
| 5<br>組　織 | 5-1 | 第三者からの新たな脅威や攻撃の手口を知り、職員間で共有していますか？ | | → P11 |
| | 5-2 | 職員に守秘義務を理解させ、業務上知り得た情報を外部に漏らさないといったルールを守らせていますか？ | | |
| | 5-3 | 職員に情報セキュリティに関する教育や注意喚起を行っていますか？ | | |
| | 5-4 | 個人所有の情報機器を業務で利用する場合のセキュリティ対策や注意喚起を行っていますか？ | | |
| | 5-5 | セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するといった対策をしていますか？ | | → P12 |

## 1. ネットワーク

### 1-1　PC 等、情報機器の OS やソフトウェアは常に最新の状態にしていますか？

Windows 等の OS やソフトウェアには、時間の経過とともに脆弱性と呼ばれる不具合が発見されることがあります。

脆弱性を放置していると、たとえウイルス対策ソフトを導入していてもウイルスに感染してしまったり、ウイルス付きの電子メールが他の人に自動的に送られてしまったり、悪意のあるホームページを見ただけで PC 内部のシステムが破壊されてしまったりすることがあります。

脆弱性は、プログラムの不具合や設計ミス等に起因するもので、それらを修正するための修正プログラムがメーカーから配付されています。修正プログラムの有無を定期的に確認したり、自動的に適用したりするための自動アップデートを利用し、OS やソフトウェアを常に最新の状態にしておきましょう。

### 1-2　ウイルス対策ソフトを導入し、ウイルス定義ファイル等を常に最新の状態にしていますか？

PC や職場内のネットワークを防御するためには、ウイルスへの適切な対策が必要です。最近のウイルスは多様かつ巧妙化しており、ID・パスワードを盗む、遠隔操作を行う、ファイルを勝手に暗号化する、といったものが増えています。

ウイルス対策ソフトを導入することはもちろん、ウイルス検知用データ（ウイルス定義ファイル）を常に最新のものに更新しておきましょう。自動更新機能を設定しておくと便利です。

### 1-3　無線 LAN を安全に使用するために適切な暗号化方式を設定するといった対策をしていますか？

無線 LAN は、機器のレイアウトの変更が容易である等の利便性から、職場内でも導入が進んでいます。

しかし、無線 LAN は電波を利用する通信であるという性質上、他人から通信内容を読み取られたり、不正に接続されて犯罪行為に悪用されたりする被害を受ける可能性があります。安全に利用するために、以下の点にご注意ください。

- 強固な暗号化方式（WPA3）を選択する
- パスワード（ネットワークセキュリティキー）の初期設定が簡易なものである場合は、文字数を増やす・文字／数字／記号を組み合わせる等して容易に推測されないようにする
- アクセスポイント（SSID）が正規のものであることを確認する（偽アクセスポイントに接続しないよう注意）
- 業務で使用する端末（PC、タブレット等）を公衆無線 LAN（フリーWi-fi など）に接続しないようにする

## 1-4　パスワードは破られにくい複雑なものにしていますか？

組織で利用するパスワードは、情報資産へのアクセスの可否を決める重要なものです。パスワードの重要性を再認識し、適切なパスワード管理を心がけてください。

◇パスワード作成の 3 箇条＝「長く」「複雑に」「使い回さない」
「長く」　…　文字列は 10 文字以上が望ましい
「複雑に」　…　・大文字、小文字、数字、記号を混在させる
・名前、電話番号、誕生日、簡単な英単語等を避け、安易に推測しにくいものにする
「使い回さない」…同じ ID やパスワードを複数サービス間で使い回さない

＊パスワードの定期的な変更について

これまでは、パスワードの定期的な変更が推奨されてきましたが、内閣サイバーセキュリティセンター（日本）や国立標準技術研究所（米国）から、必ずしもパスワードを定期的に変更する必要はないことが示されています。

これは、定期的な変更をすることで作成方法がパターン化し、単純なパスワードになりやすいことや、使い回しが起こりやすいことに対する懸念によるものですが、万一の流出時やサービス側に変更を求められた場合は当然変更が必要となります。パスワード設定の際は、機器やサービスの間で使い回しのない、固有のパスワードを設定することを重視しましょう。

## 1-5　パソコンやサーバーのウイルス感染、故障による重要情報の消失に備えてバックアップを取っていますか？

電子データは、機器の故障や誤動作、ウイルス感染等により保存したデータが消失してしまうことがあり、バックアップが不可欠です。職場内でバックアップのルールを作成し、定期的なバックアップを取得してください。

バックアップには、ファイルサーバ、インターネット上のオンラインストレージ、外付けハードディスクにコピーする方法、CD や DVD 等の外部の記憶媒体を利用する方法等があります。バックアップは複数作成し、可能であればそのうち 1 つは万一の災害に備え遠隔地に保存することを推奨します。

## 1-6　インターネットを介したウイルス感染や SNS への書き込みに起因するトラブルへの対策をしていますか？

インターネットには様々なホームページが公開されていますが、それらの中には個人情報を収集することや、嫌がらせが目的のものもあります。また、ホームページによっては、閲覧しただけでウイルスに感染したり、PC を破壊されたりしてしまうものもあります。

このような被害を受けないためには、OS やブラウザを最新の状態に更新しておくこと（→1-1）、ウイルス対策ソフトを用いて常に監視すること（→1-2）に加え、Web ブラウザの設定を見直すことも大切です。JavaScript の実行時に警告を出すようにする、もしくは信頼できる Web サイト（信頼済みサイト）以外では JavaScript を実行させないといった対

策が考えられます。
　また、職員が SNS やネット掲示板等に秘密情報を勝手に掲載して組織に被害を及ぼすことがあります。業務でのインターネット利用に一定のルールを設けることで、被害を未然に防ぐことが必要です。

## 1-7　クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？

　昨今、企業や組織において、情報資産をクラウドサービスに預けるという利用が進んでいます。一方で、利用者の ID やパスワード等、アカウント情報の管理不備が原因で、不正アクセスによる情報漏洩等の事故が多く発生しています。クラウドサービスは、どこからでも情報にアクセスしやすいことが利点ですが、このことがセキュリティ上の脅威ともなり得ます。正しい利用者のみが許可された操作が行えるように、アカウントの管理に細心の注意を払ってください。
　また、クラウドサービスでは、業者側での障害や運用の不備等が原因でシステム上に置いたデータが消える、サービス自体が使えなくなるといった事案も発生しています。サービス選定の際には、コスト優先ではなく、性能や信頼性、補償内容を十分吟味するようにしましょう。また、サービスが使えなくなった時のために、データのバックアップを取得する（→1-5）ことはもちろん、代替の手段やサービスを用意することもご検討ください。

## 2. 電子メール

### 2-1 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気を付けていますか？

電子メールに関する情報セキュリティ事故の大きな要因が、添付されたファイルや URL によるウイルス感染やフィッシングサイトへの誘導です。メールの差出人をよく確認のうえ、身に覚えのない電子メールの添付ファイルや URL リンクへのアクセスはしないようにしましょう。

### 2-2 電子メールの送信ミスを防ぐ取組みをしていますか？

上記 2-1 に加え、電子メールに関する情報セキュリティ事故のもう一つの大きな要因が、誤送信による情報漏洩です。

誤送信の原因の 1 つとして挙げられるのが、自動補完機能（オートコンプリート）によるアドレスの誤入力です。電子メール作成時には、メールアドレスの先頭部分を入力するだけで自動的に全部の文字列が入力される便利な機能ですが、この機能で表示されたメールアドレスをよく確認せず、間違った宛先を指定してしまうというケースがあります。

また、よくある誤りが、CC（カーボンコピー）と BCC（ブラインドカーボンコピー）の取り違いです。本来は BCC で送信すべきところを CC で送信してしまうことにより、受信者に他の全ての受信者のメールアドレスが伝わってしまうという事例が多く発生しています。送信前に「送信トレイ」に一時保留するように設定変更する等して、送信ミスを防ぐ取組みを行ってください。

### 2-3 重要情報は電子メール本文ではなく、添付するファイルに記載しパスワード等で保護していますか？

重要情報を電子メールで送信する際は、できるだけ本文には書きこまず、文書ファイル等に記載してパスワードで保護した後、メールに添付しましょう。文書ファイルの保護解除パスワードは、別送の電子メールや電子メール以外の手段（携帯電話のショートメッセージサービス等）で伝えるようにしてください。

## 3. 重要情報の取扱い

### 3-1　紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は、書庫等に安全に保管していますか？

職場の机上に放置された情報は、持ち去り、盗み見等、危険にさらされています。重要情報は、関係者以外が見たり触れたりすることができないように正しく管理しましょう。鍵付き引き出しやケースに納め、必要な場合のみ持ち出し、終了後は速やかに元に戻す習慣が必要です。

### 3-2　重要情報が記載された書類や電子媒体を持ち出す際には、盗難や紛失に備えた対策をしていますか？

重要情報を職場外に持ち出す場合、思わぬ盗難に遭ったり、うっかり紛失したりすることがあります。ノートパソコン、USB メモリ、DVD 等各種記憶媒体を持ち出す際には以下の点にご注意ください。

- 重要情報の持ち出しは許可制にして、持ち出し・返還の記録を行う
- ノートパソコン、スマートフォンにはパスワードロックをかける
- USB メモリや DVD に保管するファイルは、暗号化して保存する
- 個人所有の USB メモリを使用しない（ウイルス感染防止）

### 3-3　重要情報が記載された書類やデータを破棄する際には、復元できないようにしていますか？

重要情報が漏洩するのは、ネットワーク経由とは限りません。紙書類を処分する、PC を廃棄するといった場合に、情報が第三者の目に触れ、重大な漏洩事故を引き起こすことがあります。

紙書類を処分する場合は、シュレッダー（クロスカット方式が望ましい）を利用するか、専門サービス（業者）に溶解処分を依頼して証明書を取得しておきましょう。

電子機器や電子媒体に保存された情報は、ファイル削除の操作やハードディスクをフォーマットしただけでは、データが消えているように見えても特殊なソフトウェアを利用することにより削除されたはずのファイルを復元することが可能です。データ消去用のソフトウェアを使用する、専門業者のデータ消去サービスを利用する、ハードディスクや記憶媒体を物理的に破壊して再生不能な状態にするといった方法を用いて、適切な処分を行ってください。

### 3-4　重要情報の授受を行う取引先との契約書には、秘密保持条項を規定していますか？

取引先が情報の内容から判断して「当然秘密にしてくれるだろう」という一方的な期待は禁物です。取引先に重要情報を提供する場合は、契約書や覚書に秘密保持や具体的な対策を明記し、機密として取り扱ってもらうことが必要です。

## 4. 事務所内留意事項

### 4-1　離席時に PC 画面の覗き見や勝手な操作ができないようにしていますか？

PC を使用した作業の途中でそのまま席を離れたり、パスワードなしでログインできるパソコン等、誰でも操作できる状態の PC は、不正に使用される可能性があります。離席時にスクリーンロックをかける等の対策を行いましょう。

また、情報通信技術を使用せずに、ネットワークに侵入するために必要となるパスワード等の重要情報を盗み出す「ソーシャルエンジニアリング」にも気を配る必要があります。具体的には、なりすまし電話をかけて個人情報を盗む、PC 画面を覗き見してパスワードを盗む（ショルダーハッキング）、ごみ箱を漁って個人情報を盗む（トラッシング）といった「アナログな」方法です。個人情報を取扱う際には職場におけるルールを設定して事故を未然に防ぐことが重要です。

### 4-2　退社時に PC や備品を施錠保管する等、盗難防止対策をしていますか？

ノートパソコンやタブレット端末、USB メモリ等は手軽に持ち運べる便利さがある反面、盗難や紛失の危険性も高くなっています。退社時には、施錠可能な引き出しに保管するといったハード面の対策の他、ノートパソコンやタブレット端末をシンクライアント化（端末にデータを保存しない仕組み）するといったソフト面の対策も有効です。

### 4-3　事務所が無人になる時の施錠忘れ対策をしていますか？

事務所の鍵の管理を徹底することはもちろんですが、最終退出者や退出時間等の記録を残すことも重要です。記録を残し、最終退出者による施錠の責任意識を向上させるようにしましょう。

## 5. 組　織

### 5-1　第三者からの新たな脅威や攻撃の手口を知り、職員間で共有していますか？

取引先や関係者と偽ってウイルス付のメールを送ってくる（標的型攻撃）、正規のウェブサイトに似せた偽サイトを立ち上げて ID やパスワードを盗もうとする等、巧妙な手口が増えています。特に標的型攻撃メールのウイルスは、ウイルス対策ソフトでは検出されないものが多いため、感染に気付きにくく知らぬ間に被害が拡大しているケースがあるため、深刻な問題となっています。

標的型攻撃をひとつの手段で防ぐことは困難ですが、手口をよく知り、疑わしいメールに添付されたファイルは開封しない、URL リンクをクリックしない（→2-1）といった意識付けを行うことが大切です。

また、ネットワーク管理を担っている方は、IPA（独立行政法人 情報処理推進機構）等、セキュリティ専門機関のウェブサイト等で最新の脅威や攻撃の手口を定期的にチェックすることも必要です。

### 5-2　職員に守秘義務を理解させ、業務上知り得た情報を外部に漏らさないといったルールを守らせていますか？

職員の守秘義務や機密保持については、通常就業規則等で定められ、職員採用時には説明されていると思いますが、日常業務に慣れてくると機密情報、個人情報の取扱いが蔑ろにされがちです。

どのような情報が秘密なのか、何をしたらいけないか等、具体的な内容について、職場内研修等を用いて定期的に職員に理解させるといった努めが必要です。

### 5-3　職員に情報セキュリティに関する教育や注意喚起を行っていますか？

日々の仕事では常に様々な情報を取扱いますが、日常的であるがゆえに管理の意識がつい疎かになりがちです。職員に対して定期的な研修の機会を与え、情報セキュリティの大切さを啓発してください。

### 5-4　個人所有の情報機器を業務で利用する場合のセキュリティ対策や注意喚起を行っていますか？

個人所有の PC やスマートフォンを業務で使用する場合、管理が行き届かず、セキュリティの確保が難しくなります。個人所有端末の業務利用をルール化し、認める場合にも許可制を導入する等、一定の制約が必要です。

また、外出先で無線 LAN を利用してインターネットに接続する場合は、信頼できるアクセスポイントを選ぶ、適切な暗号化等の設定を行うことも重要です。

## 5-5　セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するといった対策をしていますか？

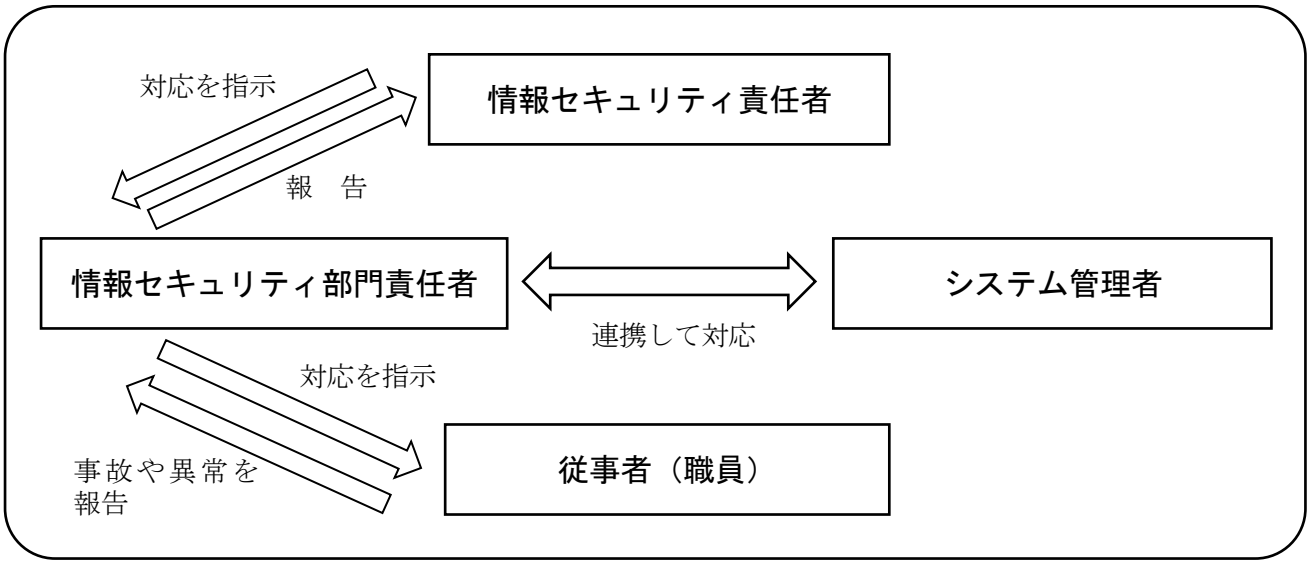
実際に事故が起きてからだと、冷静に対応する余裕がなくなってしまいます。また、対応が後手に回り、それが原因でさらに深刻な事態になりがちです。重要情報の流出や紛失、盗難があった場合の対応手順書（マニュアル）を作成し、「誰が」「いつ」「何をするのか」をまとめておくことで、万一の際にも落ち着いて対応ができるようになります。

# 事故に備える(組織体制)

## 体制づくり

情報管理及び緊急対応体制を構築し、役割と責任を明確化することで適切なセキュリティ管理や緊急時のスムーズな対応を心がけましょう。

【事故発生時の対応体制（例)】




■**情報セキュリティ責任者**（例：事務局長）
情報セキュリティ対策などの決定権限を有し、全責任を負います。事故発生時には、事故の影響を判断し対応について意思決定します。

■**情報セキュリティ部門責任者**（例：総務課長）
情報セキュリティ対策の実施等の責任と権限を有します。事故発生時には、情報セキュリティ責任者の判断・意思決定に基づき、システム管理者と連携して適切な処置を行います。

■**システム管理者**（例：情報管理課長、社外に委託している場合は委託業者の担当者）
情報システムの管理を司り、情報セキュリティ対策の導入・見直しを行います。事故発生時には、情報セキュリティ部門責任者と連携して適切な処置を行います。

■**従事者（職員）**
情報セキュリティ部門責任者から指示された情報セキュリティ対策の確実な遂行に努めるとともに、事故や異常の発生を認知した場合は、速やかに情報セキュリティ部門責任者へ報告し、指示を待ちます。

## 取組方針の明確化

○基本方針の策定

組織が情報セキュリティをどのように捉えているのか、安全な体制をどのように維持していくのかを宣言する方法として「基本方針」の策定があります。情報セキュリティに関する社内体制の整備やコンプライアンス（法令遵守）、事故対応等の事案に対して法人の方針を定め、ホームページに掲載、職場で掲示するといった方法により内外に周知します。

【情報セキュリティに関する基本方針（例）】

情報セキュリティに関する基本方針

○○○○法人○○○○（以下、「本会（本組合）」という。）は、本会（本組合）が保有する情報資産を事故や犯罪などの脅威から守り、会員（組合員）及び社会の信頼に応えるべく、以下の方針に基づき情報セキュリティに取り組みます。

1.社内体制の整備

本会（本組合）は、情報セキュリティの維持及び改善のために組織を設置し、組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.職員の取組み

本会（本組合）の職員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

3.法令及び契約事項の遵守

本会（本組合）は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守します。

4.違反及び事故への対応

本会（本組合）は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

20〇〇年〇月〇日

○○○○法人　○○○○互助会（組合）

理事長 ○○　○○

## 関連規程の整備

法人の事業内容や取扱う情報、職場環境、IT の利用状況に合わせ、対応すべきリスクとその対策を明文化した「情報セキュリティ関連規程」の整備も有効です。

【情報セキュリティ関連規程の項目（例)】

| 項　　目 | 概　　要 |
|---|---|
| 組織的対策 | 情報セキュリティのための管理体制の構築や点検、情報共有等のルール |
| 情報資産管理 | 管理職及び職員の責務や教育、人材育成等のルール |
| アクセス制御及び認証 | 情報資産の管理や持ち出し方法、バックアップ、破棄等のルール |
| 物理的対策 | セキュリティを保つべき事務所、部屋及び施設等の領域設定や領域内での注意事項等のルール |
| IT 機器利用 | IT 機器やソフトウェアの利用にあたってのルール |
| IT 基盤運用管理 | サーバーやネットワーク等の IT インフラに関するルール |
| システム開発及び保守 | 開発及び保守を行う情報システムに関するルール |
| 委託管理 | 業務委託にあたっての選定や契約、評価のルール |
| 情報セキュリティインシデント及び事業継続管理 | 事故対応や事業継続管理等のルール |

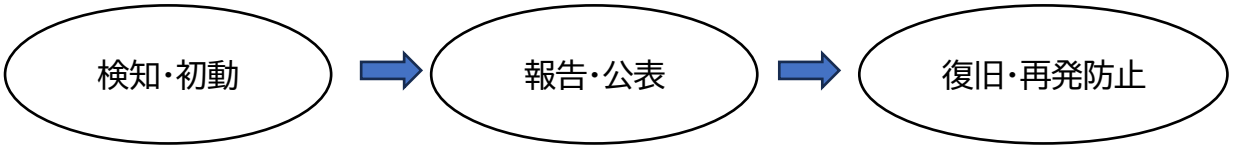
※独立行政法人情報処理推進機構が、情報セキュリティ関連規程（サンプル）を公開しています
https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx

# 事故(インシデント)が起こったら・・・

## 事故対応の基本ステップ

セキュリティ事故（インシデント）に備え、被害や影響範囲を最小限に抑えるために具体的な対応策を決めておきましょう。

【事故対応時の基本手順】




## 事故が起きたときは

セキュリティ事故が発生したら、体制（→P13）に従い、情報セキュリティ責任者・情報セキュリティ部門責任者・システム管理者（委託している場合は委託業者）が連携して対応します。

### 検知・初動

○職員が次のような状況を検知したときは、速やかに情報セキュリティ責任者に報告します。
- PC 画面に身代金を要求するようなメッセージが表示
- ウイルス対策ソフトの警告表示
- 内部情報（会員の個人情報等）が第三者に渡っていることが発覚
- 操作ミスによるメールの誤送信

○検知内容により以下の初期対応を行います。
- PC がウイルスに感染した恐れがあるときは、感染した PC をネットワークから切り離し、サーバーの利用を停止します。
- 使用端末に不正アクセスの恐れがあるときは、その端末をネットワークから切り離してサービスを停止します（証拠保全のため電源は落とさない）。
- クレジットカード情報、登録サービスのアカウント情報が漏洩した恐れがあるときは、カード会社やサービス運営会社に連絡して利用を停止します。
- メール誤送信で送信先が明らかなときは、送信先に受信した情報の削除を依頼します。
- 内部犯行が疑われるときは、社内システムへのアクセス制限及び PC 等の端末の利用を一時的に制限して証拠の保存に努めます。

## 報告・公表

○事故が影響する範囲を想定し、報告・公表を行います。
- 影響を及ぼす恐れのある取引先や会員（組合員）に対し、インシデント発生について報告します。
- ウイルス感染による情報漏洩等により、業法等で報告が求められている場合は所轄の省庁に報告します（例：個人情報漏洩→個人情報保護委員会へ報告）
- 原因が不正アクセスや内部犯行等、犯罪性があると疑われる場合は警察に届け出ます。
- システム停止等で一定期間サービス提供停止の必要がある場合は、ホームページ等で公表します。

## 調査・復旧・再発防止

○調　査
- ウイルス感染の場合は、他の PC やサーバーが感染していないかチェックします。
- 情報漏洩の恐れのある場合は、漏洩した情報の「範囲・原因・被害」について調査します。

○復　旧
- ウイルス感染の場合は、ウイルス対策ソフトに従ってウイルスを駆除します。駆除できない場合は OS の再インストールを行い、全てのプログラムを再度インストールします。
  データ等のバックアップを行っている場合は、それを用いてデータを復元します。
- 不正アクセスの場合は、侵入されたサーバーの安全が確認できたらサービスを復旧します。
- アカウント情報等が漏洩した場合は、アカウントの再発行やパスワードの変更を行います。

○再発防止
- アカウント情報等が漏洩した場合は、アカウント情報等の管理方法の見直し、アクセス権限の見直しを行います。
- 内部犯行の場合は、社内の情報管理体制を見直します。
- メールの誤送信等、人的な作業ミスによる場合は、作業手順やチェック体制を見直します。

# 情報セキュリティ教育

情報セキュリティ教育とは、ウイルス感染や情報漏洩といった情報セキュリティ事故を未然に防ぐために行われる社内教育です。

組織がリスクに対応すべく、規則の制定や様々なセキュリティ製品を活用しても、情報を取扱う職員のセキュリティに対するリテラシーが低ければ重大な事故を招く可能性があります。情報セキュリティに対する意識を高め、業務上のルール遵守を徹底するためには、日頃から社内教育に取組む必要があります。

【具体的な取組み】

○社内研修

自社の基本方針や規程の学習、職場内のルール、平時や事故発生時の各職員の役割等、職場に合わせた内容で研修ができるため自由度が高いが、会場準備や資料作成等、手間が多くかかる。

○社外研修

情報セキュリティに精通した専門家の解説を聞くことができ、その場で質問も可能であることから、より深い知識を得ることができる。反面、汎用的な内容であることから定期的に参加しないと一過性のものとなってしまう可能性もある。

○ｅ－ラーニング

職員の都合に合わせて受講でき、反復学習も可能であることから知識が確実に身に着く。責任者等は、職員の受講状況を管理して習熟度を把握できる。インターネット環境が必須。

**上記研修を併用して各職員が業務上に潜むリスクを学ぶとともに、業務における職場内ルール遵守を常に意識し、万一事故が起こった際には自らの役割を遅滞なく果たせるようにしておきましょう。**

# 参　考　＝情報セキュリティに関する情報＝

**◆独立行政法人　情報処理推進機構　セキュリティセンター（IPA）**
https://www.ipa.go.jp/security/

**◆国民のためのサイバーセキュリティサイト**
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

**◆サイバーセキュリティポータルサイト（内閣サイバーセキュリティセンター／NISC）**
https://security-portal.nisc.go.jp

**◆個人情報の取扱いにおける事故報告（2023 年度／プライバシーマーク推進センター）**
https://privacymark.jp/guideline/wakaru/g7ccig0000002vj1-att/2023JikoHoukoku_240815.pdf