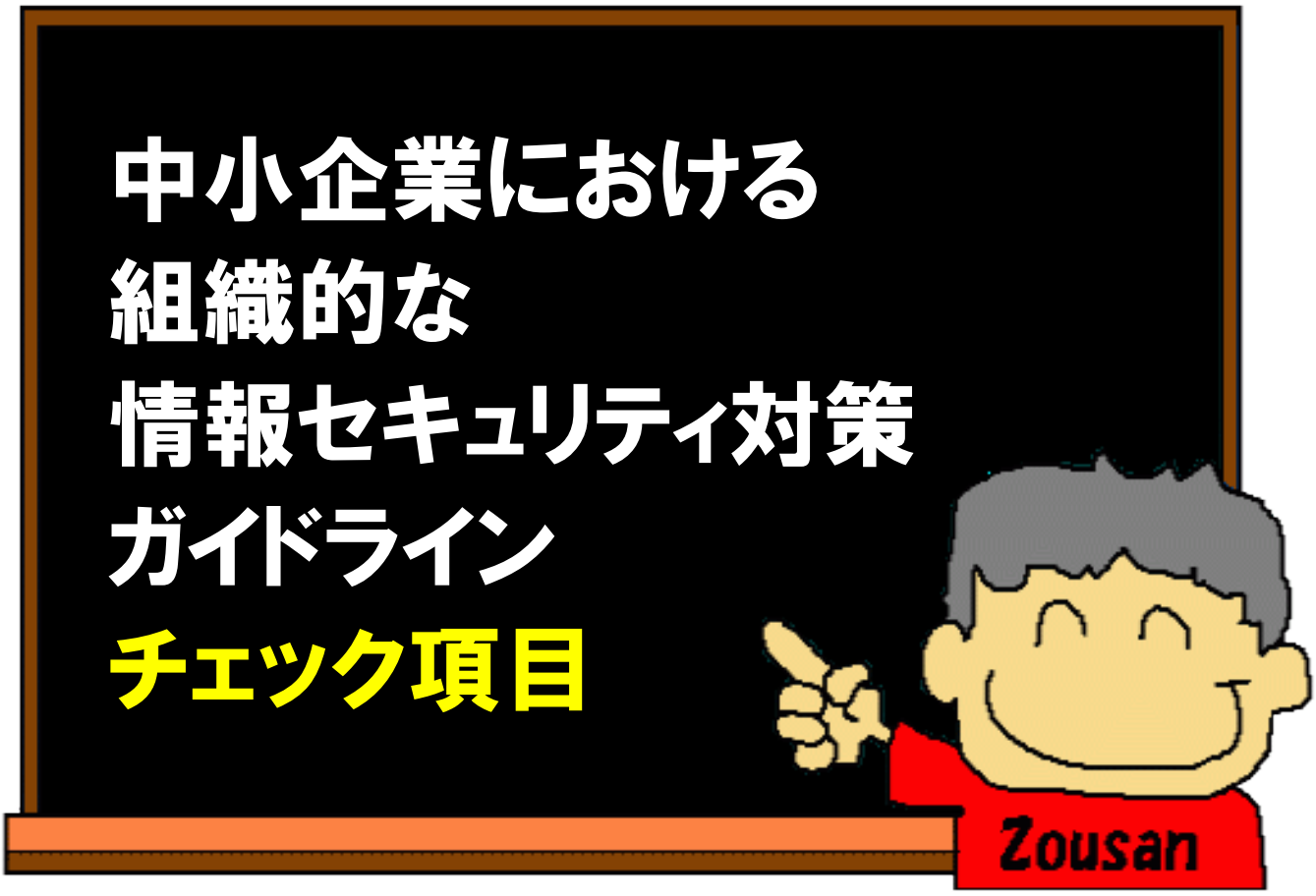
IPA せきゅりていマネジメントのしおり シリーズ (2)

中小企業における組織的な情報セキュリティ対策ガイドライン チェック項目



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

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

2012年9月3日 第1版

目次

本しおりは、『中小企業の情報セキュリティ対策ガイドライン：別冊２　中小企業における組織的な情報セキュリティ対策ガイドライン』から抜粋したものです。

参考情報

- 中小企業の情報セキュリティ対策ガイドライン（IPA）
  http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-guide.pdf
- 中小企業の情報セキュリティ対策ガイドライン：別冊１　委託関係における情報セキュリティ対策ガイドライン（IPA）
  http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-itaku.pdf
- 中小企業の情報セキュリティ対策ガイドライン：別冊２　中小企業における組織的な情報セキュリティ対策ガイドライン（IPA）
  http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-itaku.pdf

1. 情報セキュリティに対する組織的な取り組み

1.1 情報セキュリティに関する経営者の意図が従業員に明確に示されている

- 経営者が情報セキュリティポリシーの策定に関与し、実現に対して責任を持つこと。
- 情報セキュリティポリシーを定期的に見直しすること。

1.2 情報セキュリティ対策に関わる責任者と担当者を明示する

- 責任者として情報セキュリティと経営を理解する立場の人を任命すること。
- 責任者は、各セキュリティ対策について（社内外を含め）、責任者、担当者それぞれの役割を具体化し、役割を徹底すること。

1.3 管理すべき重要な情報資産を区分する

- 管理すべき重要な情報資産を、他の情報資産と分類すること。
- 情報資産の管理者を定めること。
- 重要度に応じた情報資産の取り扱い指針を定めること。
- 重要な情報資産を利用できる人の範囲を定めること。

1.4 重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定める

- 各プロセスにおける作業手順を明確化し、決められた担当者が、手順に基づいて作業を行っていること。
- 重要な情報に対して、漏洩や不正利用を防ぐ保護対策を行っていること。

（例）

- 重要な情報を利用できる人に対してのみ、アクセス可能とすること。
- 重要な情報の利用履歴を残しておくこと。
- 重要な情報を確実に消去・廃棄すること。 等

1.5 外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取る

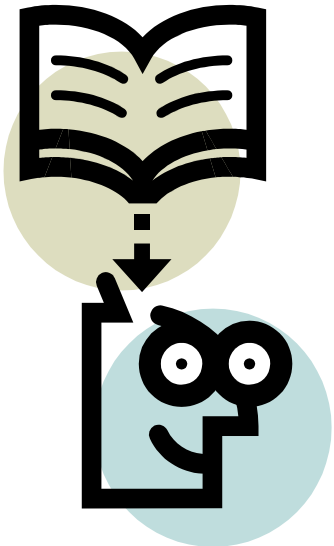
- 契約書や委託業務の際に取り交わす書面等に、情報の取り扱いに関する注意事項を含めること。

（例）

- システム開発を委託する際の本番データ利用時の際の情報管理、例えば管理体制や受託情報の取り扱い・受け渡し・返却、廃棄等について、注意事項を含めること。
- 関係者のみにデータの取り扱いを制限すること。
- 外部の組織との間で情報を授受する場合、情報受渡書を持っておこなうこと。
- 契約に基づく作業を遂行することによって新たに発生する情報（例：新たに作製された、金型・図面・モックアップ等々）の取扱を含めること。
- 等

1.6 従業者（派遣を含む）に対し、セキュリティに関して就業上何をしなければいけないかを明示する

- 従業者を採用する際に、守秘義務契約や誓約書を交わしていること。
- 従業者が順守すべき事項を明確にしていること。
- 違反を犯した従業員に対する懲戒手続きが整備されていること。
- 在職中及び退職後の機密保持義務を明確化するため、プロジェクトへの参加時など、具体的に企業機密に接する際に、退職後の機密保持義務も含む誓約書を取ること。



1.7 情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与える

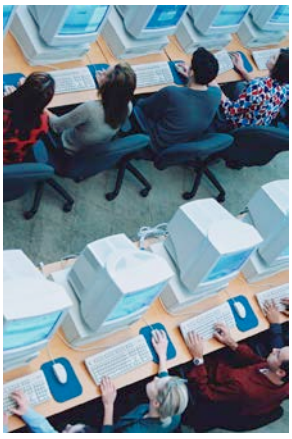
- ポリシーや関連規程を従業員に理解させること。
- 実践するために必要な教育を定期的に行っていること。

2. 物理的セキュリティ

2.1 重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行う

- 重要な情報を保管したり、扱ったりする区域を定めていること。
- 重要な情報を保管している部屋（事務室）又はフロアーへの侵入を防止するための対策を行っていること。
- 重要な情報を保管している部屋（事務室）又はフロアーに入ることができる人を制限し、入退の記録を取得していること。

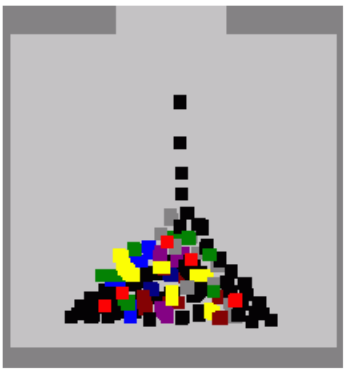
2.2 重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害が起こらないように配置・設置する



- 重要なコンピュータは許可された人だけが入ることができる安全な場所に設置すること。
- 電源や通信ケーブルなどは、他の人が容易に接触できないようにすること。
- 重要なシステムについて、地震などによる転倒防止、水濡れ防止、停電時の代替電源の確保などを行っていること。

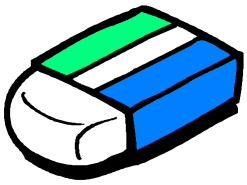
2.3 重要な書類、モバイルPC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行う

（重要な書類について）



- 不要になった場合、シュレッダーや焼却などして確実に処分すること。
- 重要な書類を保管するキャビネットには、施錠管理を行うこと。
- 重要な情報が存在する机上、書庫、会議室などは整理整頓を行うこと。
- 郵便物、FAX、印刷物などの放置は禁止。重要な書類の裏面を再利用しないこと。

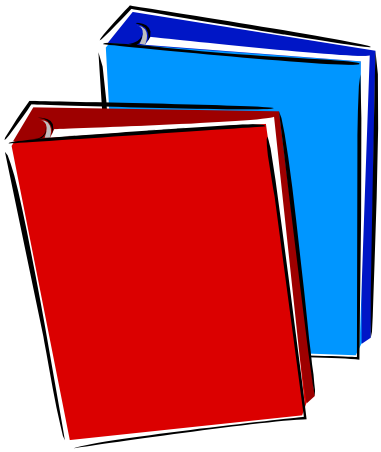
（モバイルPC、記憶媒体について）



- 保存した情報が不要になった場合、消去ソフトを用いるなど、確実に処分していること。
- モバイルPC、記憶媒体については、盗難防止の対策を行うこと。
- 私有PCを会社に持ち込んだり、私有PCで業務を行ったりしないこと。

3. 情報システム及び通信ネットワークの運用管理

3.1 情報システムの運用に関して運用ルールを策定する



- システム運用におけるセキュリティ要求事項を明確にしていること。
- 情報システムの運用手順書（マニュアル）を整備していること。
- システムの運用状況を点検していること。
- システムにおいて実施した操作や障害、セキュリティ関連イベントについてログ（記録）を取得していること。
- 設備（具体例）の使用状況を記録していること。

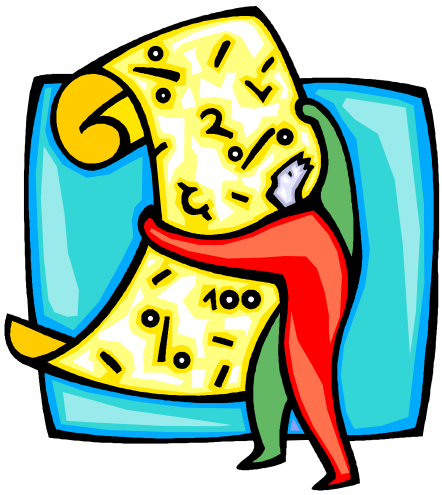
3.2 ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行う

- ウイルス対策ソフトを導入し、パターンファイルの更新を定期的に行っていること。
- ウイルス対策ソフトが持っている機能（ファイアウォール機能、スパムメール対策機能、有害サイト対策機能）を活用すること。
- 各サーバやクライアントPCについて、定期的なウイルス検査を行っていること。
- Winny等、組織で許可されていないソフトウェアのインストールの禁止、あるいは使用制限を行っていること。

3.3 導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行う

- 脆弱性の解消（修正プログラムの適用、Windows update等）を行っていること。
- 脆弱性情報や脅威に関する情報の入手方法を確認し、定期的に収集すること。
- 情報システム導入の際に、不要なサービスの停止など、セキュリティを考慮した設定を実施するなどの対策が施されているかを確認すること。
- Webサイトの公開にあたっては、不正アクセスや改ざんなどを受けないような設定・対策を行い、脆弱性の解消を行うこと。
- Webブラウザや電子メールソフトのセキュリティ設定を行うこと。

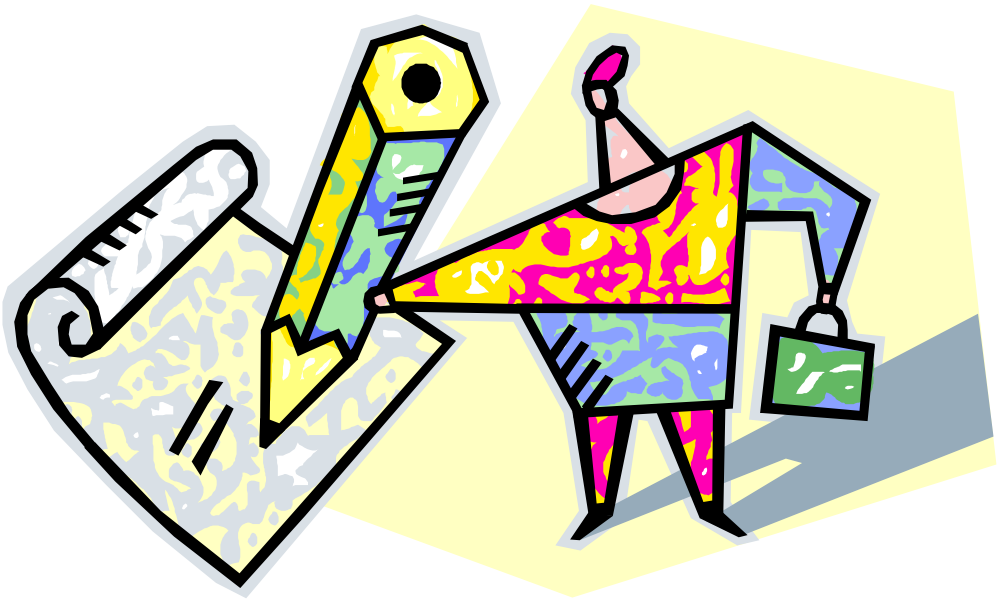
3.4 通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施する



- 必要に応じて、SSL等を用いて通信データを暗号化すること。
- 外部のネットワークから内部のネットワークや情報システムにアクセスする場合に、VPNなどを用いて暗号化した通信路を使用していること。
- 電子メールをやり取りする際に、重要な情報についてはファイルにパスワードを付ける、又は暗号化すること。

3.5 モバイルPCやUSBメモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施する

- モバイルPCやUSBメモリ等の使用や外部持ち出しについて、規程を定めていること。
- 外部でモバイルPCやUSBメモリ等を使用する場合の紛失や盗難対策を講じていること。
- モバイルPCやUSBメモリ等を外部に持出す際は、利用者の認証（ID・パスワード設定、USBキーやICカード認証、バイオメトリクス認証等）を行うこと。
- 保存されているデータを、重要度に応じてHDD暗号化、BIOSパスワード設定などの技術的対策を実施すること。
- PCを持出す場合の持出者、持出・返却管理を実施すること。
- 盗難、紛失時に情報漏えいの脅威にさらされた情報が何かを正確に把握するため、持ち出し情報の一覧、内容管理を行うこと。



4. 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策

4.1 情報（データ）や情報システムへのアクセスを制限するために、利用者IDの管理（パスワードの管理など）を行う

- 利用者毎にIDとパスワードを割当て、そのIDとパスワードによる識別と認証を確実に行うこと。
- 利用者IDの登録や削除に関する規程を整備すること。
- パスワードの定期的な見直しを求めること。また、空白のパスワードや単純な文字列のパスワードを設定しないよう利用者に求めること。
- 離席する際は、パスワードで保護されたスクリーンセーバーでパソコンを保護すること。
- 不要になった利用者IDを削除すること。

4.2 重要な情報に対するアクセス権限の設定を行う

- 重要な情報に対するアクセス管理方針を定め、利用者毎にアクセス可能な情報、情報システム、業務アプリケーション、サービス等を設定すること。
- 職務の変更や異動に際して、利用者のアクセス権限を見直すこと。

4.3 インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISPサービス　等）を行う

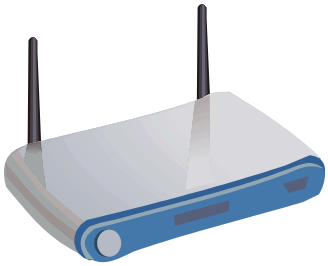
（外部から内部へのアクセス）

- 外部から内部のシステムにアクセスする際、利用者認証を実施すること。
- 保護すべき重要な情報が保存されるシステムは、それ以外のシステムが接続しているネットワークから物理的に遮断する、もしくはセグメント分割することによりアクセスできないようにすること。

（内部から外部へのアクセス）

- 不正なプログラムをダウンロードさせる恐れのあるサイトへのアクセスを遮断するような仕組み（フィルタリングソフトの導入等）を行っていること。

4.4 無線LANのセキュリティ対策（WPA2の導入等）を行う



- 無線LANにおいて重要な情報の通信を行う場合は、暗号化通信（WPA2等）の設定を行うこと。
- 無線LANの使用を許可する端末（MAC認証）や利用者の認証を行うこと。

4.5 ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行う

- ソフトウェアの導入や変更に関する手順を整備していること。
- システム開発において、レビューの実施と記録を残していること。
- 外部委託によるソフトウェア開発を行う場合、使用許諾、知的所有権などについて取り決めていること。
- 開発や保守を外部委託する場合に、セキュリティ管理の実施状況を把握できること。

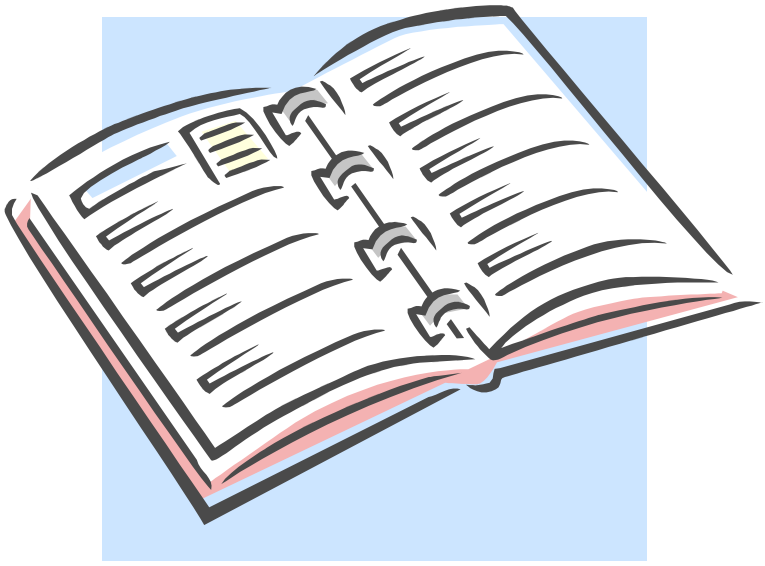
5. 情報セキュリティ上の事故対応

5.1 情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握する

- 情報システムに障害が発生した場合の、最低限運用の必要な時間帯と許容停止時間を明確にしておくこと。
- 障害対策の仕組みが組織として効果的に機能するよう、よく検討していること。
- システムの切り離し（即応処理）、必要なサービスを提供できるような機能（縮退機能）、情報の回復や情報システムの復旧に必要となる機能などが、障害時に円滑に機能するよう確認しておくこと。
- 日常のシステム運用の中で、バックアップデータや運用の記録などを確保しておくこと。
- 障害発生時に必要な対応として、障害発生時の報告要領（電話連絡先の認知等）、障害対策の責任者と対応体制、システム切替え・復旧手順、障害発生時の業務実施要領等の準備を整えておくこと。

（例）

- 大容量データの復元には時間を要するため、復元に要する時間の事前見積りの実施。
- 関係者への障害対応要領の周知や、必要なスキルに関する教育や訓練などの実施を行っていること。

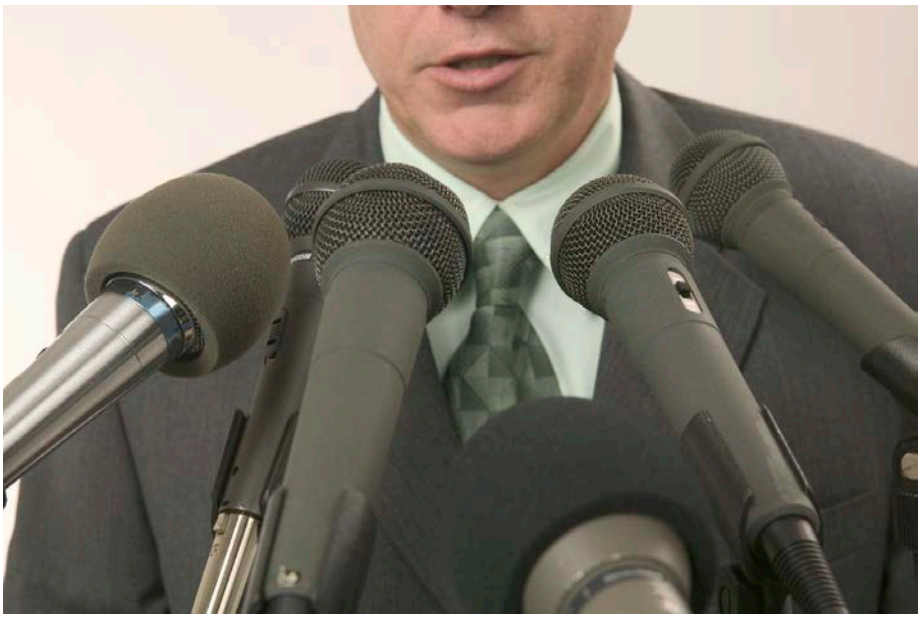


5.2 情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握する

- ウイルス感染や情報漏えい等の発生時、組織内の関係者への報告、緊急処置の適用基準や実行手順、被害状況の把握、原因の把握と対策の実施、被害者への連絡や外部への周知方法、通常システムへの復旧手順、業務再開手順などを整えておくこと。

（例）

- ウイルス感染の場合、ウイルス定義ファイルを最新の状態にしたワクチンソフトにより、コンピュータの検査を実施し、ワクチンソフトのベンダのWebサイト等の情報を基に、検出されたウイルスの駆除方法などを試すことが必要となる。
- 情報漏えいの場合、事実を確認したら速やかに責任者に報告し、対応体制を取ること、対応についての判断を行うため 5W1H の観点で調査し情報を整理すること、対策本部で対応方針を決定すること、被害の拡大防止と復旧のための措置を行うことが必要となる。また、漏洩した個人情報の本人、取引先などへの通知、監督官庁等への報告、ホームページやマスコミ等による公表についても検討する必要がある。



参考情報一覧

- 中小企業の情報セキュリティ対策ガイドライン（IPA）
  http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-guide.pdf
- 中小企業の情報セキュリティ対策ガイドライン：別冊１　委託関係における情報セキュリティ対策ガイドライン（IPA）
  http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-itaku.pdf
- 中小企業の情報セキュリティ対策ガイドライン：別冊２　中小企業における組織的な情報セキュリティ対策ガイドライン（IPA）
  http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-itaku.pdf
- 営業秘密管理指針（経済産業省）
  http://www.meti.go.jp/press/20100409006/20100409006-6.pdf
- 安全なウェブサイト運営入門（IPA）
  http://www.ipa.go.jp/security/vuln/7incidents/
- SaaS 向け SLA ガイドライン（経済産業省）
  http://www.meti.go.jp/committee/materials/downloadfiles/g80207c05j.pdf
- 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（経済産業省）
  http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf
- 事業継続計画策定ガイドライン（経済産業省）
  http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf
- IT サービス継続ガイドライン（経済産業省）
  http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf
- 事業継続ガイドライン（内閣府）
  http://www.bousai.go.jp/MinkanToShijyou/guideline02.pdf

- Winny による情報漏えいを防止するために（IPA）
  http://www.ipa.go.jp/security/topics/20060310_winny.html
- 無線 LAN を他人に使われないようにしましょう！（IPA）
  http://www.ipa.go.jp/security/txt/2011/04outline.html
- ウイルス対策情報（IPA）
  http://www.ipa.go.jp/security/antivirus/antivirus-top.html

IPA せきゅりていマネジメントのしおり シリーズ

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA せきゅりていマネジメントのしおりシリーズ(1)
  企業(組織)における最低限の情報セキュリティ対策のしおり
- IPA せきゅりていマネジメントのしおりシリーズ(2)
  中小企業における組織的な情報セキュリティ対策ガイドライン
- IPA せきゅりていマネジメントのしおりシリーズ(3)
  中小企業における組織的な情報セキュリティ対策ガイドライン 事例集
- IPA せきゅりていマネジメントのしおりシリーズ(4)
  情報セキュリティ対策ベンチマーク

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