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

中小企業をサポートするセキュリティの参考書

- 2つのレベルから解説
- 中小企業に共通する対策
- 10の事例で多様なケースに対応

IPA®

目次

1. 目的と概要.....1
2. 情報・情報資産と情報セキュリティ.....1
3. 共通して実施すべき対策と企業毎に考慮すべき対策.....2
4. 共通して実施すべき対策.....3
4.1 情報セキュリティに対する組織的な取り組み.....4
4.1.1 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.....4
4.1.2 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.....4
4.1.3 管理すべき重要な情報資産を区分する.....4
4.1.4 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.....4
4.1.5 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.....4
4.1.6 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.....5
4.1.7 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.....5
4.2 物理的セキュリティ.....5
4.2.1 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.....5
4.2.2 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.....5
4.2.3 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.....5
4.3 情報システム及び通信ネットワークの運用管理.....6
4.3.1 情報システムの運用に関して運用ルールを策定する.....6
4.3.2 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.....6
4.3.3 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.....6
4.3.4 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.....7
4.3.5 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.....7
4.4 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.....7

4.4.1 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 7
4.4.2 重要な情報に対するアクセス権限の設定を行う 8
4.4.3 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 8
4.4.4 無線 LAN のセキュリティ対策（WPA2 の導入等）を行う 8
4.4.5 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 8
4.5 情報セキュリティ上の事故対応 8
4.5.1 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 8
4.5.2 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 9
5. 企業毎に考慮すべき対策 10
5.1 企業を取り巻く様々な脅威と脅威への対策 10
5.1.1 従業員の情報持ち出し 10
5.1.2 退職者の情報持ち出し、競合他社への就職 12
5.1.3 従業員による私物 PC の業務利用と Winny の利用による業務情報の漏洩事故 14
5.1.4 ホームページへの不正アクセス 16
5.1.5 アウトソーシングサービスの利用 19
5.1.6 委託した先からの情報漏えい 21
5.1.7 在庫管理システム障害の発生 22
5.1.8 無線 LAN のパスワードのいい加減な管理 24
5.1.9 IT 管理者の不在 25
5.1.10 電子メール経由でのウイルス感染 27
5.2 企業の情報セキュリティに対する考え方の整理 29
5.2.1 情報資産の洗い出し 29
5.2.2 事故の可能性と影響 30
5.2.3 対応方針の決定 31
5.2.4 情報セキュリティの波及効果 32
6. 参考文献 33
6.1 情報セキュリティ対策に活用できる制度・ツール等 33
6.2 情報セキュリティ対策に関する資料 33
6.3 コンプライアンス 33
6.4 その他 34

付録 1：情報セキュリティ対策チェックリスト i
付録 2：共通して実施すべき項目と企業毎に考慮すべき対策とのマッピング.....i

1. 目的と概要

本ガイドラインは、一定以上の情報セキュリティ上のリスクに曝されており、また、一旦情報漏えい等の事故が発生した場合、自社の業務に影響が及ぶだけでなく、取引先などに対しても大きな迷惑をかける可能性のある中小企業を対象とする。そのため、一定のコストをかけて情報セキュリティ対策を行う必要があるが、中小企業のバリエーションの多さ（規模、業種等）を考えると、具体的にどのような対策を行うべきかについて、一律な基準を示すことは困難である。

そのため、本ガイドラインでは中小企業であれば共通して実施すべき対策と、企業毎にそれぞれの特徴を考慮して実施すべき対策の 2 つに分けて説明を行う。共通して実施すべき対策だけでも相当な効果があると考えられるが、十分な対策をとるためには企業毎に考慮すべき対策について各自検討を行い、必要な対策をとることが望まれる。

さらに、本ガイドラインに基づいた対策を行った中小企業は、情報セキュリティ対策ベンチマークを利用することで、求められる対策の達成状況を把握したり、様々な企業の中での自社の位置づけを把握することができる。これにより、不足している対策が判明した際は、再び本ガイドラインを参考に、必要な対策について検討することが重要である。

2. 情報・情報資産と情報セキュリティ

「情報セキュリティ」とは「情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めても良い。」と定義[1]されているが、簡単に言えば、企業の場合、企業秘密や個人情報などの情報をどのように守るのか、あるいは、その情報を扱う情報システムをどのように守るのかということである。

企業が守るべき「情報」には電子的な情報だけでなく紙情報も含まれる。さらに、例えば製造業であれば、試作品や金型など、純粋な情報だけではなく「物に化体した情報」も含まれる場合がある。このような「物に化体した情報」は、特許などで守ることは難しく、秘密情報として管理することが適切な場合があるからである。

「情報」と似た言葉に、「情報資産」という言葉がある。「情報」と「情報資産」はほとんど同じ意味で用いられることも多いが、「情報資産」は、様々な「情報」のうち、企業として管理すべき対象として選択されたものを呼ぶ。これは、企業の中で飛び交う情報を全て管理することは不可能であり、また意味がないためである。例えば、従業員が作成した「安くておいしいランチマップ」も「情報」であるが、これは特殊な場合を除き、企業と

[1] JIS Q 27001 :2006

して管理すべき対象、つまり「情報資産」ではない。また、情報システムなども「情報資産」に含める場合がある。「情報セキュリティ」の第一歩は、それぞれの企業が自社の「情報資産」が何なのかを把握することである。

3. 共通して実施すべき対策と企業毎に考慮すべき対策

本ガイドラインでは、中小企業にとって共通して実施すべき対策（4 章）と、企業毎に考慮すべき対策（5 章）の 2 つに分けて説明を行う。

4 章の共通的な対策では、本ガイドラインの対象となる企業であれば、その企業の規模や業種によらず必要となる対策について、例を示しながら説明を行っている。

5 章の企業毎に考慮すべき対策では、中小企業において重点的に取り組むべき様々なシナリオを提示することで、4 章に示した「共通して実施すべき対策」の徹底と、場合によっては必要とされる高度な対策について示す。これは企業それぞれが、自身の業務内容などを考え、必要となる対策を選択するための手がかりを与えることを狙いとしている。具体的には、企業が自社が直面する危険や問題点（情報セキュリティリスク）への気づきを与えるため、幾つかの典型的なシナリオの中から自社に適合するものを選択し、それに対応する対策を自ら選ぶことになる（5.1 企業を取り巻く様々な脅威と脅威への対策）。なお、全ての対策を行うことは不可能であるので、どのような考え方で対策の取捨選択をすべきかについての基本的な考え方も示した（5.2 企業の情報セキュリティに対する考え方の整理）。

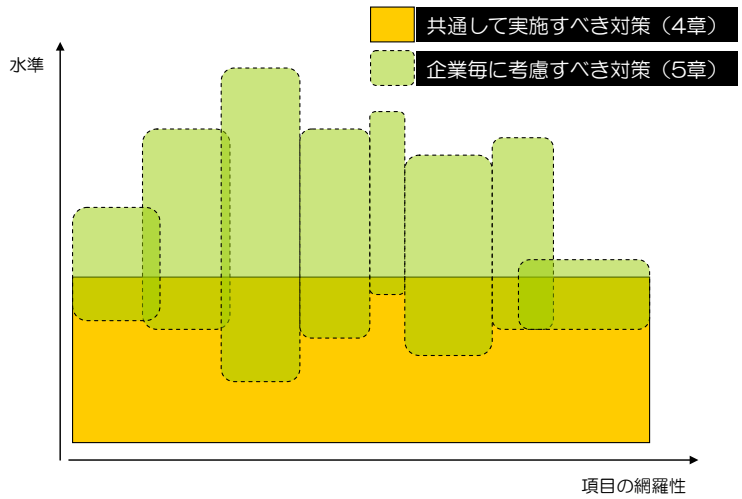


図 1　共通して実施すべき対策と企業毎に考慮すべき対策

なお、本ガイドラインで示した様々な対策の中には、基本的に必要な対策項目と、最近の脅威への対策として必要な項目が含まれている。脅威は常に変化しているため、脅威の動向を常に把握しつつ、新たな対策を適宜とる必要がある。

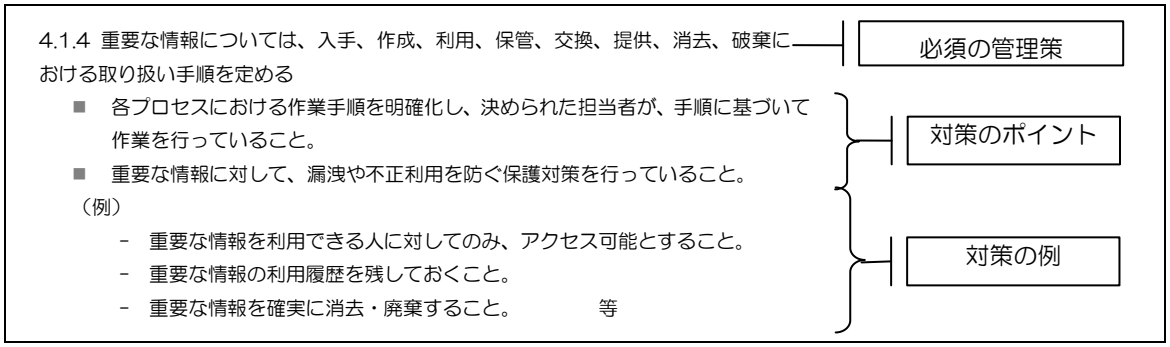
4. 共通して実施すべき対策

ここでは、中小企業であれば共通して実施すべき対策について示す。ここでは、規模や業種にはよらないが、中小企業の中でも企業として組織的な対策をとりうる企業を念頭においている。

共通して実施すべき対策では、以下の５つの分類に従って、管理策をまとめている。

1. 情報セキュリティに対する組織的な取り組み：経営者あるいは経営管理者が整備すべき社内的体制や規程類の整備に関する項目
2. 物理的セキュリティ：建物や記憶媒体など、物理的な物の管理に関する項目
3. 情報システム及び通信ネットワークの運用管理：PC やネットワークなどの管理に関する項目
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：情報や情報システムに対するアクセス制御に関する項目と、情報システムの導入時に考慮すべき項目
5. 情報セキュリティ上の事故対応：情報セキュリティに関する事故が発生した場合への準備に関する項目

それぞれに記載された対策の読み方であるが、「必須の管理策」が項目番号の直後に記載されており、企業が共通して実施すべき管理策が示されている。ただし、ここで示された管理策を具体的にどのように実現するかは企業にまかされている。そのため、管理策を実現する上での「対策のポイント」を、「必須の管理策」の後に示した。「対策のポイント」が全て満たされないと、「必須の管理策」が実現しないというわけではないが、管理策の実効性を担保するためには、「対策のポイント」と同等程度の対策が実施される必要があることに留意すべきである。



なお、対策のポイントについて、具体的な「対策の例」を適宜示した。

4.1 情報セキュリティに対する組織的な取り組み

4.1.1 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。

4.1.2 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。

4.1.3 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。

4.1.4 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

4.1.5 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。
- 契約に基づく作業に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

4.1.6 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。

4.1.7 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。

4.2 物理的セキュリティ

4.2.1 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。

4.2.2 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。

4.2.3 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。

4.3 情報システム及び通信ネットワークの運用管理

4.3.1 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。

4.3.2 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（ファイアーウォール機能、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。

4.3.3 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。

4.3.4 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。

4.3.5 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。

4.4 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

4.4.1 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。

4.4.2 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。

4.4.3 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。

4.4.4 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。

4.4.5 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。

4.5 情報セキュリティ上の事故対応

4.5.1 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。

4.5.2 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。

5. 企業毎に考慮すべき対策

本章では、中小企業において重点的に取り組むべき様々なシナリオを提示することで、４章に示した「共通して実施すべき対策」の徹底と、場合によっては必要とされる高度な対策について示す。

5.1 は、情報セキュリティに関わる様々な脅威や危険について、KYT（危険予知トレーニング）的なシナリオを提示することで、「気づき」を持ってもらうことを狙いとしている。さらに、典型的な対策について、「4.共通して実施すべき対策」との関連を明らかにしつつ、紹介している。

5.2 は、脅威や危険について気がついた企業が、どのような対応方針で情報セキュリティ対策の実施の可否を決めるか、という問題に対して、一般的な手法を紹介している。

5.1 企業を取り巻く様々な脅威と脅威への対策

本節の基本的読み方としては、それぞれの事例におけるシナリオの前半【状況】を読み、自社に置き換えた場合、どのような事故が発生しうるのか、どのようか危険があるのかを想像する。その上で、【発生した事故】を読むことで、自社が抱えている危険性（リスク）に気がつく、あるいは再確認するのが効果的である。シナリオ自体が自社業務に当たらない場合は、読み飛ばしてもかまわない。

「⑵対策の例」では、各シナリオにおいて「4. 共通して実施すべき対策」の中で特に徹底して対策を施すべき項目を示すと共に、それ以外の追加的対策についても示している。

5.1.1 従業員の情報持ち出し

(1) 典型的な状況

シナリオ 1
【状況】 技術力に定評のある中小企業であるＡ化学工業の主力製品は、液晶パネルメーカー向けの液晶材料である。特に携帯電話用の高性能液晶パネル向けの液晶材料では他の追随を許さないが、その秘密は液晶材料の調合比率にあった。 Ａ化学工業では、信頼できる従業員だけが、この調合比率を知ることが出来たが、特に会社としては情報の管理を行っておらず、全従業員がアクセスするサーバーの上には秘密として管理すべき情報と、そうでない情報が分類整理されずに保管されている。 

ある日、本来は液晶の調合比率を知る立場にない営業部の B 営業課長代理は、現在営業中の液晶パネルメーカー、C電器に対する営業用の参考資料を探していたところ、調合比率が記載されたプレゼンテーション資料を見つけ、この資料を印刷し、C電器の担当者に手渡した。C電器は相見積もりを取るため、A 社のライバルであるDマテリアルに、資料に記載された比率で液晶を調合した場合の見積りを依頼した。

【発生した事故】
プレゼンテーション資料を入手した D マテリアルの営業は、その資料を製造部門の担当者に見せたところ、担当者はその情報の重要性に気がついた。Dマテリアルは A 化学工業と同様の液晶材料をより安価に提供することにより、A化学工業の市場シェアは急落することになった。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 様々な情報が分類・整理されていない
- 従業員が機密情報か否かを判別できない
- 重要な情報に誰でもアクセスできるようになっている（アクセス制御が出来ていない）

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■様々な情報が分類・整理されていない	■管理すべき重要な情報資産を分類する（4.1.3）。 ■情報資産を分類するために、情報資産管理台帳を作成する（情報資産の洗い出しと分類については、5.2.1 も参照のこと）。
■従業員が機密情報か否かを判別できない	■ある情報が機密情報か否かを従業員が容易に判別できるように、紙資料であれば印を押したり、電子媒体であればファイル名の先頭に機密情報である旨の表示をつけるなどする。
■重要な情報に誰でもアクセスできるようになっている	■従業員それぞれにサーバ等へのアクセスに必要な ID を発行すると共に、見る必要の無い情報へはアクセスできないようにOSの機能

	等を用いてアクセス制限をかける。 ■サーバ等へのアクセスには ID だけではなく、パスワードを要求するようにし、パスワードは容易に推測できないようにする。 ■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（4.1.4）。 ■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、盗難防止対策を行う（4.2.3）。特に、重要な情報には印刷制限をかける。 ■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（4.4.1）。 ■重要な情報に対するアクセス権限の設定を行う（4.4.2）。 ■アクセス記録（閲覧、ダウンロードなど）が取得され、ログレポートが管理者（経営者）に提出されていることを従業員に周知する。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- どのような情報が機密情報なのか、あるいは機密情報の取扱いについて規程等を定めると共に、社員教育や研修の実施などにより、従業員に対する周知を行うことが重要である。
- 結果として情報が漏洩した場合、法的な保護を受けることが考えられる。このような法律として、不正競争防止法が制定されている。不正競争防止法の営業秘密としての保護を受けるためには、日頃から以下の要件を満たすように管理を行っておく必要がある。具体的には、経済産業省の『営業秘密管理指針』を参照のこと。
  (a) 情報にアクセスできる者を制限していること
  (b) 情報にアクセスした者にそれが営業秘密であると認識できること

5.1.2 退職者の情報持ち出し、競合他社への就職

(1) 典型的な状況

シナリオ２
【状況】  A 化学工業で 15 年にわたって製品開発に携わってきた B 技師は、上司との飲み会のトラブルが原因で、会社を退職することになった。その際、B 技師は研究開発を続けるため自分が作成した技術資料を CD-R に焼いて持ち出した。 B 技師は、A 化学工業が最近発売した特殊な表面加工を行ったプラスチックプレートの開発者であり、製法のノウハウなどに精通している。A 化学工業では、この技術の特許は取得せず、製法を秘密にしておけば競合製品が登場しないと考えていた。 B 技師は、退職後すぐに、以前学会で知り合った C 化成の研究部長に誘われ、C 化成に就職した。なお、A 化学工業では B 技師と退職後に関する取り決め等は一切結んでいなかった。 【発生した事故】 C 化成では、B 技師の研究開発により、A 化学工業よりも優れた特性を持つプラスチックプレートの製品化に成功、A 化学工業にを押さえてトップシェアを獲得した。 A 社は同社の技術が使われているとして、C 化成にクレームをつけたが、特許等の侵害はなく、また、B 技師が C 化成に就職することを妨げる契約等を結んでいなかったため、取り合ってもらえなかった。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 退職後の機密保持策や競業避止対策の未整備
- 営業秘密管理の不徹底

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■退職後の機密保持策や競業避止対策の未整備	■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ならないかを明確にする（4.1.6）。特に、退職後の機密保持義務や競業避止のため、誓約書等を取る

	こと。
■営業秘密管理の不徹底	■管理すべき重要な情報資産を分類する（4.1.3）。 ■重要な情報に対するアクセス権の設定を行う（4.4.2）。特に、退職に際してはアクセス権限を見直し、退職者が不必要に情報を持ち出さないようにすること。 ■会社の重要な営業秘密・知財については、必要に応じて特許を取得したり、不正競争防止法により保護されるように、日頃から対策を講じること（5.1.1 も参照）。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- 退職後の従業員の競業避止義務、機密保持義務を定める方法としては、基本的には就業規則において、主に以下のような定めを課すことが考えられる[2]。しかし同時に、『これらの定めの効力等は、それぞれ異なる枠組みの下で判断され認められうる効力も異なる』とされることから、これらの適用に際しては慎重な判断が必要である。詳細については、（公表予定）経済産業省『情報セキュリティ関連法令に関する調査報告書』を参照することが望ましい。
  - (a) 従業員に対して、在職中に知り得た会社の機密情報を他者に洩らしたり、自ら利用したりしない義務（機密保持義務）を課すこと
  - (b) 従業員に対して、会社の業務と競合する事業を自ら営んだり、このような事業に就職したりしない義務（競業避止義務）を課すこと
  - (c) 従業員が第二に挙げた競業行為を行った場合に、支給される退職金の額を減らす、若しくは支給しない（既に退職金が支給されている場合、その全部又は一部を返還させる）旨を定めること

5.1.3 従業員による私物 PC の業務利用と Winny の利用による業務情報の漏洩事故

(1) 典型的な状況

シナリオ３
【状況】 A 化学工業では、全事務系社員にデスクトップパソコンを支給し業務を行っていた

[2] （公表予定）経済産業省『情報セキュリティ関連法令に関する調査報告書』

が、ノート PC については予算の関係で、共用のノート PC がごく少数あるだけだった。一方、A 化学工業の営業担当は、夜の 8 時までにその日の営業報告を会社のサーバに保存することが社内規定により義務づけられている。しかし、顧客との打ち合わせが長引いたり、遠隔地の顧客を訪問した場合などは、8 時までに帰社し営業報告を作成することが困難な事がしばしばある。営業部の B 営業課長代理は、移動時間やちょっとした空き時間に営業報告を作成するため、私物のノート PC を業務に用いていた。私物の PC を仕事で使うことは禁止されていたが B 課長代理はその規定を知らなかった。

【発生した事故】
ある日、A 化学工業の総務部に、A 社の顧客リストのファイルらしきものが Winny で流れているとの通報が社外からあった。顧客リストの内容を確認すると、確かに自社の得意先リストと間違いがないことが分かった。顧客リストの内容を見ると B 課長代理の担当顧客であったことから、B 営業課長代理に問いただしたところ、B 課長代理の私物のノート PC に Winny がインストールされており、さらに感染すると、PC 内の情報を勝手に Winny ネットワークに放流するウイルスに感染していることがわかった。B 課長代理自身は Winny をインストールした覚えはなかったが、B 課長代理の長男が音楽ファイルをダウンロードするために、勝手に Winny をインストールしていた。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 業務に必要な PC を支給していなかった
- 規定の存在が周知されていなかった
- 守られることが期待されない実効性の低い社内規定の存在
- 情報が第三者に流出した場合も想定した対策の不備

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■業務に必要な PC を支給していな	■業務に必要な PC は会社から支給する。

かった	
■社内規定の存在が周知されていなかった	■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（4.1.1）。 ■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ならないかを明確にする（4.1.6）。 ■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（4.1.7）。
■守られることが期待されない実効性の低い社内規定の存在	■実際の業務を分析し、遵守可能な社内規定とする。
■情報が第三者に流出した場合も想定した対策の不備	■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（4.3.5）。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- 情報セキュリティに限らず、実質的に守ることができない社内規定は、モラルハザードを引き起こす大きな原因となる。規定の形骸化は、規定の不備よりも有害な場合がある。
- ウイルス対策やファイルシステムの暗号化等、必要な対策を強制できるように、業務で必要な PC 等の設備は、会社から支給する。私用 PC が業務に用いられている場合、私用 PC がセキュリティ上の大きな穴となりうるが、会社として私用 PC のセキュリティ対策実施を強制することは出来ない。

5.1.4 ホームページへの不正アクセス

(1) 典型的な状況

シナリオ４
【状況】 老舗輸入食品販売の A 物産は、近年自社ショッピングサイトを開設し、主に個人を顧客に様々な食品を直接販売することで、売り上げを伸ばしてきている。自社ショッピングサイトの開発は、従来より A 物産の業務システムを開発してきた B システムズに外注した。A 物産には情報システムに詳しい人間がおらず、IT 部門などの担当

部署もないため、基本的には仕様の策定から開発・運用まで丸投げしていた。
ショッピングサイトの顧客 DB はインターネットから直接アクセスできない社内ネットワーク上の業務サーバーに置かれ、インターネットからアクセスされるショッピングサイトのサーバーからの問い合わせを処理するような構成になっている。

近年、百貨店向けの販売不振から、経費節減のため、B システムズとのショッピングサイトシステムの運用契約を解除し、A 物産からの要求があった場合に対応する形態の契約に変更した。

【発生した事故】
A 物産のショッピングサイト問い合わせ窓口に、外部機関から、Web サイトにウイルスが埋め込まれている、という連絡があった。A 物産は B システムズに依頼し調査を行ってもらったところ、OS の脆弱性をついてショッピングサイトのページが書き換えられており、ウイルスが埋め込まれていることが確認された。さらに、Web サーバーのログを分析したところ、SQL インジェクションにより顧客 DB に対して不正なアクセスが行われ、顧客の個人情報が約 1 万件漏洩したことが判明した。
また、A 物産の発表前に、ネット上の掲示板で問題が公表され、問い合わせが殺到したが、責任者も不明確で、またどのような対応をとるべきかが分からなかったことから、マスコミに批判的な記事が出るなど会社のイメージが大きく低下した。
その後、A 物産では、情報が漏洩した顧客に対する謝罪を行うとともに、1000 円分の割引券を発行した。またシステムの改修が終わるまでショッピングサイトを閉鎖したため、その間の売り上げが減少、再開後も顧客が事件前に戻るのに 1 年程度を要した。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 開発管理の不備
- 脆弱な運用体制
- 不十分な不正アクセス対策
- 事故対応体制の未整備

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■開発管理の不備	■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（4.4.5）。 ■Web アプリケーションの脆弱性に関しては、開発時にセキュリティを考慮した仕様書を示すと共に、公開前に専門家による確認を行うことが望ましい。
■脆弱な運用体制	■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（4.1.2）。 ■情報システムの運用に関して運用ルールを策定する（4.3.1）。特に、必要なログが正確に取得されるようにしておく必要がある。 ■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（4.3.2）。 ■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（4.3.3）。
■不十分な不正アクセス対策	■インターネット接続に関わる不正アクセス対策を行う（4.4.3）。 ■特に重要なシステムや、インターネットに直接接続されたシステムについては、IDS（侵入検知システム）や IPS（侵入防御システム）などを導入する。
■事故対応体制の未整備	■情報セキュリティに関連する事件や事故等の緊急時に、何をすべきかを把握する（4.5.2）。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- 近年発生している不正アクセス事件の多くは、SQL インジェクション等の Web アプリケーションの脆弱性をついたものである。従って、Web アプリケーションの開発・運用に際しては、IPA の『安全なウェブサイト運営入門』等を参考に、既知の脆弱性への対策を行う必要がある。
- 事故対応体制もしくは、事故時に何をすべきかを事前に把握しておくことが重要である。顧客への対応はもちろんであるが、法令遵守の観点も重要である。具体的には個人情報保護法などへの対応が重要である。

5.1.5 アウトソーシングサービスの利用

(1) 典型的な状況

シナリオ５
【状況】 市場調査を行っているＡマーケティング社のＢ調査員は、会社の了解を得ずに、地理情報システムとして無料の SaaS（Software as a Service）型のサービスである、C 社の C-World を使っている。 C-World がネットワーク上で提供している地図、衛星写真などの地理情報に、B 調査員が調査したマーケット調査結果を C-World サーバーに送信し、結果を地図情報と重ね合わせて顧客へのプレゼンテーションに利用している。    【発生した事故】 ある日、A マーケティングでは B 調査員の顧客から、前回の調査結果がインターネット上に公開されており、誰でも見ることができるようになっている、というクレームを受けた。A マーケティング社で調べたところ、確かに C-World サーバーからマーケット調査結果が誰でも見ることができる状態になっていた。これは C-World の無料サービスの約款では、ユーザーが登録した情報はデフォルト状態では一般に公開されることになっており、B 調査員はそれを知らずにそのままの状態で使っていたためであることがわかった。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 外部サービスの無許可利用
- 外部サービスのサービス内容についての不十分な理解

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■外部サービスの無許可利用	■SaaS、ASP も含む、新たなソフトウェアや、

	システムを導入する場合、セキュリティ上のリスクを把握した上で導入の可否を決定する。 ■業務上、必要のないツールの利用制限を行う。
■外部サービスのサービス内容についての不十分な理解	■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とる（4.1.5）。 ■サービス約款・SL 等について十分に理解したうえで、利用の可否を判断する。 ■ツール（SaaS、ASP も含む）を使用する場合は、デフォルトの設定を確認し、セキュアな設定を行うよう注意する。 ■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（4.3.4）。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- SaaS 等、外部サービスのセキュリティ水準は、一般事業者のセキュリティ水準よりも高いことが期待される。したがって、リソースの面で十分なセキュリティ対策の実施が困難な中小企業にとって、SaaS 等の利用はセキュリティの観点からも望ましい場合が多い。
- 一方で、外部のサービスを利用する場合、事前にサービス提供事業者に対して、情報セキュリティの観点から確認を行うことが重要である。具体的には以下のような点である[3]。詳細については、経済産業省『SaaS 向けSLA ガイドライン』を参照のこと。
  - (a) 各種セキュリティ規格の準拠性に関する確認事項：サービス提供事業者がJIS Q 27001:2006 等に準じた管理を行っているか、等
  - (b) 機密性に関する確認事項：脆弱性や脅威に対する対策の状況、アクセス制御がユーザーニーズを満たすものであるか、等
  - (c) 完全性に関する確認事項：預託データの完全性、整合性検証について対策が施されているか、預託データを再利用可能か、等
  - (d) 可用性に関する確認事項：災害時、障害時にどの程度システムが停止する可能性があるのか、等
  - (e) 運用保守における確認事項：サービス提供事業者が保守計画を管理してい

[3] 経済産業省、『SaaS 向け SLA ガイドライン』

るか、等

(f) コンプライアンス対応における考慮事項：ID 管理とログの保全、事象（イベント）管理が行われているか、等

5.1.6 委託した先からの情報漏えい

(1) 典型的な状況

シナリオ６

【状況】

市場調査を行っているＡマーケティング社のＢ調査員は、アンケートを送付するため、Ｃ印刷株式会社に送付先の個人情報リスト（1 万人分）を渡して、宛名ラベルの印刷を委託した。Ｂ調査員は日頃からＣ印刷と取引があるため、Ｃ印刷における情報管理について確認することなく、個人情報リストを電子メールでＣ印刷の担当者に送付し、後日、注文書を送った。Ｃ印刷では、従業員であれば誰でも入室できる場所に設置してある、誰でもログインできるPC に個人情報を格納した。

【発生した事故】

Ｃ印刷の担当者から、Ｂ調査員から受け取った個人情報を含む個人情報を、Ｃ印刷の従業員が持ち出して名簿業者に販売していた疑いで、警察に逮捕されたとの連絡があった。

Ａ マーケティングでは、漏洩した個人に連絡すると共に、謝罪文の作成・発表、監督官庁への報告等のため業務遂行に大きな影響があった。また、売り上げも減少するなど、企業業績にも影響が及んだ。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 法令遵守に対する意識の低さ
- 委託先管理の不十分さ

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■法令遵守に対する意識の低さ	■個人情報保護法が求める個人情報保護対策を実施する。 ■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（4.1.2）。 ■管理すべき重要な情報資産を分類する（4.1.3）。 ■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（4.1.4）。 ■情報セキュリティに関連する事件や事故等の緊急時に、何をすべきかを把握する（4.5.2）。
■委託先管理の不十分さ	■委託先の安全管理措置が個人情報保護法を満足するかを確認する。 ■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とる（4.1.5）。 ■重要な情報を保管したり、扱ったりする場所の入退出管理と施錠管理を行う（4.2.1）。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- 個人情報保護法への対応については、所管省庁が公表する個人情報の保護に関するガイドライン等を参考に対策を行う必要がある。（例：経済産業省、『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』）
- 情報セキュリティ事故の多くは、業務の委託先等において発生しているため、個人情報や営業秘密等を委託先に渡す場合については、何らかの管理が必要になる場合が多い。具体的には『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』を参照のこと。

5.1.7 在庫管理システム障害の発生

(1) 典型的な状況

シナリオ７
【状況】

卸売り業を営むＡ商会は、IT 化にも積極的で、5 年前から在庫管理は全てシステム化していた。データのバックアップについては、テープバックアップ装置は設置されていたものの、使い方が分からないため、ほとんど使われていない。また、IT が停止した場合を想定した事業継続計画は策定していない。

【発生した事故】
ある日、震度 4 の地震が発生し、A 商会の在庫管理サーバの脇に置いてあったパーティションが倒れ、サーバにぶつかった。この影響でサーバの HDD が故障し、サーバが正常に起動しなくなった。サーバの予備機はなく、ベンダーに修理を依頼したが、緊急時を想定した契約を結んでおらず、ベンダーが来て修理したのは地震発生 1 週間後であった。またデータは半年前にバックアップしただけだったため、業務には全く役に立たず、在庫を調査して再度データ入力が終わったのは 1 ヶ月後であった。その間、A 商会は、急遽手作業で出荷等の作業を行っていたが、手作業による出荷管理等のマニュアルが無かったため、現場は大混乱を来たした。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 事業継続への意識の低さ

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■事業継続への意識の低さ	■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（4.5.1）。 ■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（4.2.2）。 ■事業継続計画を策定するなど、事業継続マネジメント体制を構築する。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- 企業の業務が IT に依存すればするほど、IT に異常が発生した場合の業務に対する影響も大きくなる。そのため、災害時や IT 障害が発生した際でも、業務を継続する場合は、事業継続に関する検討が重要である。
- 事業継続に関して具体的に検討を行う際には、経済産業省『事業継続計画策定ガイドライン』、経済産業省『IT サービス継続ガイドライン』、内閣府『事業継続ガイドライン』等を参照することが望ましい。

5.1.8 無線 LAN のパスワードのいい加減な管理

(1) 典型的な状況

シナリオ 8

【状況】

Web デザイン企業の A メディア株式会社では、会議室でのプレゼンテーション用に、無線 LAN を導入している。セキュリティを確保するため、無線 LAN には WEP（Wired Equivalent Privacy）を設定していたが、WEP キーは、無線 LAN 機器に最初に設定されていたものをそのまま用いている。

【発生した事故】

A メディア社内のコンピュータから、外部のサイトに不正アクセスが行われている、という通知メールが、ある日 ISP から届いた。A メディアで社内を調査したところ、不正アクセスは確かに A メディア社内のネットワークから行われているが、それは無線 LAN を介して行われた不正アクセスで、その時間帯には社員はだれも在社していなかった。結局犯人は見つからなかったが、隣のビルなど、電波の圏内から A メディアの無線 LAN に不正にアクセスし、A メディアを踏み台として使ったのではないかと推測された。不正アクセスをしていた外部のサイトには ISP を介して謝罪すると共に、対策がすむまで無線 LAN を停止するなど、業務にも影響があった。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 無線 LAN の危険性に対する認識の不足

■　パスワード管理の重要性に対する認識の不足

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■無線 LAN の危険性に対する認識の不足	■無線 LAN のセキュリティ対策(WPA の導入等）を行う（4.4.4)。 ■インターネット接続に関わる不正アクセス対策を行う（4.4.3)。
■パスワード管理の重要性に対する認識の不足	■情報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 の管理を行う（4.4.1)。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- 無線LANは有線LANと異なり、物理的に接続を制御することが出来ないので、より慎重なセキュリティ対策が求められる。無線 LAN でよく用いられているセキュリティ対策のWEPは既に脆弱性が発見されているため、比較的簡単にWEPキーを破られてしまう。そのため、より強度の高い WPA を用いることが望ましい。
- パスワード（今回の例では WEP キー）については、システムに当初設定されていたデフォルトのものを用いたり、容易に推測できるようなものを用いないことが重要である。また、パスワードの定期的な変更などの対策も効果的である。

5.1.9 IT 管理者の不在

(1) 典型的な状況

シナリオ９
【状況】 Webデザイン企業のＡメディア株式会社の情報システムは、IT に詳しいＢディレクターが管理している。Ｂ氏は、システムの設定やパスワードについて忘れないようにテキストファイルでメモを作成し、自分の業務用 PC に保存している。 

【発生した事故】
B 氏は 2 週間の長期休暇を取って、アフリカに旅行に出かけた。その最中、A 社の電子メールサーバに障害が発生し、電子メールの送受信が出来なくなった。業者を呼んで、OS は立ち上がるようになった。しかし、システムの設定等はマニュアル化されていないため誰も再設定できなかった。またデータはバックアップからリカバリする必要があるが、B 氏以外に出来る人間がいないため、結局 B 氏が帰国するまで、A 社では電子メールを使うことができなかった。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 特定の個人や委託先のスキルに依存しすぎている
- 代替要員やマニュアル等の未整備

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■特定の個人や委託先のスキルに依存しすぎている	■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（4.1.2）。 ■どのようなシステムも複数人が管理できるようにしておく。
■代替要員やマニュアル等の未整備	■情報システムの運用に関して運用ルールを策定する（4.3.1）。 ■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。 ■運用手順については、情報システムが停止時にも参照できるように、紙にも印刷しておくこと。 ■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（4.5.1）。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- 中小企業の場合、情報システムの管理に多くの人員を当てることはリソースの面

から困難である。しかし、特定の個人に依存しすぎた場合、社員の出張・退職などにより、情報システムの運用が困難になったり、さらには業務にも支障が発生する。また、業者に委託する場合でも、業者の倒産や、業者の担当者の異動により同様の事態が発生しうることに注意する必要がある。

5.1.10 電子メール経由でのウイルス感染

(1) 典型的な状況

シナリオ 10

【状況】

Web デザイン企業の A メディア株式会社では、セキュリティの重要性を認識しており、ウイルス対策ソフトを基本的にすべての社内 PC に導入している。重要な業務アプリケーションを動作していた共用 PC は、古いアプリケーションを動作させるために、ウイルス対策ソフトを導入していないが、ウェブ等へのアクセスは行わないため、特に対策はしていない。ウイルス対策ソフトのパターンファイル更新は自動にしているので、実際にパターンファイルが更新されたかは確認していない。また、ポリシー管理ツールなどは導入していない。また、業務のため、社員のデザイナーの多くは様々なソフトウェアを自由にインストールして使用している。

【発生した事故】

あるとき、A 社内の PC の一部がウイルス感染してしまった。ほとんどの PC は、ウイルス対策ソフトにより感染を免れたが、重要な業務アプリケーションを動作していた共用ファイルサーバに感染し、データの一部が削除されてしまった。また、感染したユーザのクライアント PC から、業務データの一部が漏洩してしまった。調べたところ、最初に感染した PC の定義ファイルの自動更新ができなくなっていた。ユーザがインストールしたソフトとの競合が原因だということが推測できた。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- ウイルス対策ソフト等の動作の確認を定期的にしていない
- ウイルス対策等が十分に出来ない PC への考慮が不十分

- エンドユーザーがシステム構成等を変更することへの考慮が不十分

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■ウイルス対策ソフト等の動作の確認を定期的にしていない	■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（4.3.2）。 ■ウイルス対策ソフト等の動作を手動で確認（手動監査で、定義ファイルの日付をチェックする等）。 ■クライアント PC の自動チェックツールやポリシー管理ツールを導入する。
■ウイルス対策等が十分に出来ない PC への考慮が不十分	■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（4.3.3）。 ■不要なサービスの停止、パーソナルファイアウォールの導入。 ■未対策アプリケーションの局所化（ファイルサーバと分離する等）。
■エンドユーザーがシステム構成等を変更することへの考慮が不十分	■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（4.3.2）。 ■社内情報システムの構成や設定が、情報セキュリティに影響を与えないように、必要に応じてエンドユーザが行うことのできる操作に制限を加える（ソフトウェアのインストール等）。

(3) 対策のポイント

対策のポイントは以下のようなものである。

- ウイルス対策ソフトの導入は重要であるが、運用がしっかりと出来ていなければ、せっかくのソフトウェアも機能を果たさない点に注意する必要がある。

5.2 企業の情報セキュリティに対する考え方の整理

ここでは、5.1 等を通じて気づいた自社にとって危険なシナリオに対して、中小企業が対策を講じようとする際に、どのような点に留意することが望ましいかについて、簡単にまとめる。以下に記載するのは、情報セキュリティ対策におけるリスク管理の基本的な考え方を中小企業向けに簡単に解説したものであるので、詳細については、たとえば IPA『情報セキュリティマネジメントと PDCA サイクル』の『リスクアセスメント』『リスクへの対応』などを参照されたい。

5.2.1 情報資産の洗い出し

2.でも述べたように、「情報セキュリティ」の第一歩は、それぞれの企業が自社の「情報資産」が何なのかを把握することである。「情報資産」は、様々な「情報」のうち、企業として管理すべき対象として選択されたものを呼ぶ。これは、企業の中で飛び交う情報を全て管理することは不可能であり、また意味がない。

ではどのような「情報」を重要な「情報資産」として把握するべきなのかというと、これは企業毎、業種毎に異なるため一概には言うことができないが、例えば以下のような情報は重要な情報資産という事が出来る。

- その情報が漏洩したとき、会社の経営に大きな影響があるもの（例：個人情報）
- その情報が改ざんされたとき、会社の経営に大きな影響があるもの（例：財務会計情報）
- その情報が紛失したり利用できなくなったとき、会社の経営に大きな影響があるもの（例：設計図面）

なお、「情報資産」には、電子的な情報だけではなく、紙の情報や、情報システムを含むことがある。

情報資産を把握する際によく用いられるのが、情報資産管理台帳である。金型企業を例に取った具体例を図 2 に示す。

管理No	情報資産名	対象(媒体)	保管・格納場所	利用範囲	管理部門情報			台帳登録日	廃棄日	保存期間	最終棚卸し日	影響度			備考
					管理責任部門名	管理責任者	連絡先					機密性	完全性	可用性	
記入要綱	別紙「情報資産分類」を参考に記入 情報資産例より細かくても、それらを組み合わせたものでも良い、管理する単位で洗い出すこと	情報資産が情報の場合、情報が保存された状態あるいは保存されている媒体を記入 例) ・紙 ・設計製造システム ・CD－R ・ファイルサーバ 等	情報資産が保管・格納される場所を記入 例) 情報の保管場所がサーバ、PCの場合 ・ホスト名 を記入、 紙の場合 ・ロッカー ・キャビネット 等	情報資産の利用範囲を記入 ・全社 ・部内 ・課内 ・グループ内 ・XXプロジェクト内 ・幹部社員内 等		情報資産の実際の管理責任部門名、管理責任者、連絡先(内線、外線、ﾒｰﾙｱﾄﾞﾚｽ)を記入	情報資産の本台帳への登録日を記入	情報資産を廃棄する場合、廃棄した日を記入(初回記入時は空白)		登録日に情報資産の保存期間を記入 特に情報の場合、法令や契約を考慮して記入すること	情報資産の棚卸しを最後にした日を記入(初回記入時は現在の日にち)	別紙「CIA影響度」を参考に情報資産が情報か情報以外かに注意して影響度を記入			
記入例															
1	要求仕様書	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
2	構想図面	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		5年	2008/8/26	2	3	3	
3	承認図	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
4	設計図面データ	設計製造システム	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
5	設計図面	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
6	部品図	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
7	加工データ	設計製造システム	サーバルーム	製造部門	製造部門	製造部長	内線:4444	2008/8/26		永久	2008/8/26	2	3	3	
8	加工図面	紙	鍵つきキャビネット	製造部門	製造部門	製造部長	内線:4444	2008/8/26		1年	2008/8/26	2	3	3	
9	購買情報 (取引先/コスト/納期情報)	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		1年	2008/8/26	2	3	3	
10	購買情報 (取引先/コスト/納期情報)	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		1年	2008/8/26	2	3	3	
11	設計製造システム	-	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		-	2008/8/26	2	3	3	
12	製造ネットワーク(DNC)	-	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		-	2008/8/26	2	3	3	
13	ファイルサーバ	-	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		-	2008/8/26	2	1	1	
14	ノートPC	-	オフィス内個人キャビネット	営業部、品質管理部	情報システム部	情報システム部長	内線:3333	2008/8/26		-	2008/8/26	2	1	1	
15	会計情報	ファイルサーバ	MAIN(サーバ名)	経理部	経理部	経理部長	内線:2222	2008/8/26		5年	2008/8/26	2	3	2	
16	営業秘密情報	ファイルサーバ	オフィス内営業部キャビネット	営業部	営業部	営業部長	内線:5555	2008/8/26		10年	2008/8/26	3	3	2	
17	MS Officeライセンス	紙	サーバルームキャビネット	全社	情報システム部	情報システム部長	内線:3333	2008/8/26		5年	2008/8/26	1	1	1	

図 2　情報資産管理台帳の例（金型企業）[4]

5.2.2 事故の可能性と影響

重要な情報資産を把握することが出来たら、次に行うのは、情報資産がどのような脅威にさらされているかを検討することである。具体的には、以下のような脅威を考える。

- 外部の要因（例：コンピュータウイルス、不正アクセス、サービス妨害）
- 内部の要因（例：セキュリティ対策の不備、ソフトウェア欠陥、操作ミス）

また、これらの脅威がどの程度起こりうるかについて、簡単な評価を行う。例えば、1）頻繁におこる（月１回程度）、2）たまに起こる（年１回程度）、3）めったに発生しない（数年に１回）など。

次に、脅威が実際に発生したときに、情報資産がどの程度の影響を受けるかについて、

[4]NPO 日本ネットワークセキュリティ協会、『中小企業の情報セキュリティ対策支援WG活動報告書』 http://www.jnsa.org/result/2008/west/0812report.pdf

例えば、1） 影響度大（会社の存亡にかかわる）、2）影響度中（業務が停止する）、3）影響度小（業務効率が低下する）など、３段階くらいに分けて考える。

このような評価に良く用いるのが、リスクマトリクスと呼ばれる図である（図 3）。

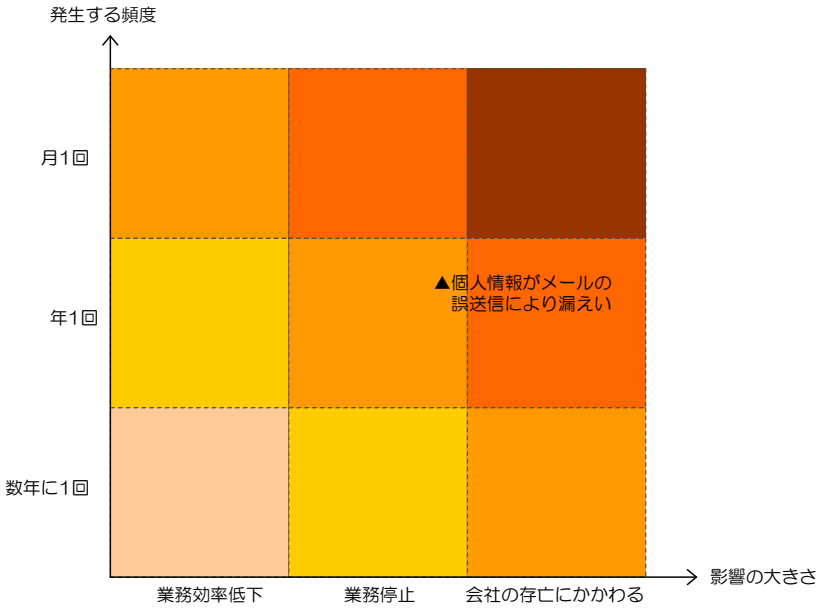


図 3　影響の大きさと発生する頻度

なお、影響の大きさを測る指標として、被害額などをとる考え方などもあるが、目的や使いやすさに応じて決めればよい。いずれにせよ、発生する頻度、影響の大きさを厳密に求める必要は無く、目安として考えれば十分である。

5.2.3 対応方針の決定

影響の大きさと発生する頻度が分かったら、次に、会社としての対応方針を決める。全ての脅威に対して対策をとるのはコストもかかるので現実的ではない。従って、業務に影響があり、ある程度、発生する可能性のあるものに、情報セキュリティ対策の投資を集中することが多い。

良く用いられる考え方では、以下のような 4 通りの対応方針に分類することが推奨されている。

- 影響度中で、たまに発生するものについては、情報セキュリティ対策を実施することで、影響や発生確率を下げる、という対応方針（リスクの低減）
- 影響度大で、頻繁に発生するものについては、経営上も大変問題があるため、やり方を変えるなり、そのような業務を実施しない、という対応方針（リスクの回避）
- 影響度大だが、めったに発生しないものについては、他社に委託したり、保険などをかける、という対応方針（リスクの移転）

■ 影響度小で、めったに発生しないものについては、無視する、という対応方針（リスクの保有）

これらの対応方針を先ほどの図の上に示すと図 4 のようになる。

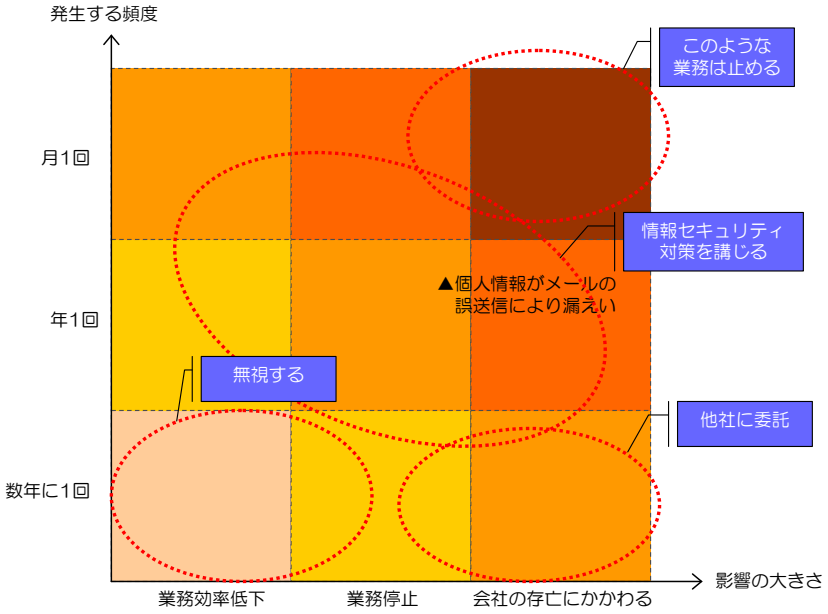


図 4　対応方針

どのような領域を情報セキュリティ対策で対応する範囲とするかについては、コストの問題も含め各社それぞれの判断であるが、合理的な対処方針を考える際にはこのような手法が参考になる。

5.2.4 情報セキュリティの波及効果

情報セキュリティ対策の実施にはお金がかかるが、一方で情報セキュリティ対策を実施することで、業務効率化などを通じて、結果として全体コストの削減に繋がる場合がある。以下はそのような例である。

- 情報セキュリティ対策のため、業務フローやシステムの見直しにより、見せなくて良い人に対するデータの隠蔽や、同じデータの重複した入力等の無駄な作業をなくすことが出来る可能性がある。これによって、作業効率の向上や、ミスの削減に繋がることがある。
- 情報セキュリティ対策を厳格に行うため、管理対象となるサーバを統合し削減することで、システム運用コストの削減などに繋がる。

このように、情報セキュリティを単なるコストとしてみるのではなく、コスト削減の道具であるとか、企業価値の創造に繋がるものとして、捉えてみることも重要である。

6. 参考文献

6.1 情報セキュリティ対策に活用できる制度・ツール等

- IPA, 『情報セキュリティ対策ベンチマーク』
  http://www.ipa.go.jp/security/benchmark/index.html
- IPA, 『安全なウェブサイト運営入門』
  http://www.ipa.go.jp/security/vuln/7incidents/index.html
- IPA, 『小規模企業のための情報セキュリティ対策』
  http://www.ipa.go.jp/security/fy18/reports/contents/soho/soho.pdf
- IPA, 『情報セキュリティマネジメントと PDCA サイクル』
  http://www.ipa.go.jp/security/manager/protect/management.html
- IPA, 『SQL インジェクション検出ツール iLogScanner V2.0』
  http://www.ipa.go.jp/security/vuln/iLogScanner/index.html
- 経済産業省, 『産業競争力のための情報基盤強化税制』
  http://www.meti.go.jp/policy/it_policy/zeisei/index.html
- IPA, 『情報セキュリティセミナー』
  http://www.ipa.go.jp/security/seminar/seminar.html
- IPA, 『コンピュータウイルス 110 番』
  http://www.ipa.go.jp/security/virus110/index.html
- IPA, 『不審メール 110 番』
  http://www.ipa.go.jp/security/virus/fushin110.html
- IPA - JPCERT/CC, 『JVN』、『MyJVN』
  http://jvn.jp/
  http://jvndb.jvn.jp/apis/myjvn/index.html

6.2 情報セキュリティ対策に関する資料

- IPA, 『情報セキュリティ白書 2008』
  http://www.ipa.go.jp/security/publications/hakusyo/2008/hakusyo2008press.html
- IPA, 『情報セキュリティ読本』
  http://www.ipa.go.jp/security/publications/dokuhon/2006/index.html
- IPA, 『セキュリティ対策まんが　クジョたいさく物語』
  http://www.ipa.go.jp/security/personal/kujo_manga/index.html

6.3 コンプライアンス

- 経済産業省, 『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』

http://www.meti.go.jp/policy/it_policy/privacy/080229kaisei-guideline.pdf

- 内閣府，『個人情報の保護に関するガイドラインについて』
  http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html
- 経済産業省，『営業秘密管理指針』
  http://www.meti.go.jp/press/20051012002/3-kaiteishishinn-set.pdf

6.4 その他

- 経済産業省，『事業継続計画策定ガイドライン』
  http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf
- 経済産業省，『IT サービス継続ガイドライン』
  http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf

付録１：情報セキュリティ対策チェックリスト

項目番号	内容	チェック
1. 情報セキュリティに対する組織的な取り組み状況		
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ますか？	□
1-2	情報セキュリティ対策に関わる責任者と担当者が明示されていますか？	□
1-3	管理すべき重要な情報資産を区分していますか？	□
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ていますか？	□
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っていますか？	□
1-6	従業者（派遣を含む）に対して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確にしていますか？	□
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ていますか？	□
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っていますか？	□
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に配慮し適切に配置・設置していますか？	□
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っていますか？	□
3. 情報システム及び通信ネットワークの運用管理状況		
3-1	情報システムの運用に関して運用ルールを策定していますか？	□
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っていますか？	□
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っていますか？	□
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していますか？	
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していますか？	□
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の状況		
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）を行っていますか？	□
4-2	重要な情報に対するアクセス権限の設定を行っていますか？	□
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）を行っていますか？	□
4-4	無線LANのセキュリティ対策（WPA2の導入等）を行っていますか？	□
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っていますか？	□
5. 情報セキュリティ上の事故対応状況		
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していますか？	□
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していますか？	□

シナリオ１　従業員の情報持ち出し	■
このシナリオに該当する場合の対策：	
内容	チェック
■様々な情報が分類・整理されていない	
管理すべき重要な情報資産を分類する（4.1.3）	□
情報資産を分類するために、情報資産管理台帳を作成する。	□
■従業員が機密情報か否かを判別できない	
ある情報が機密情報か否かを従業員が容易に判別できるように、紙資料であれば印を押したり、電子媒体であればファイル名の先頭に機密情報である旨の表示をつけるなどする。	□
■重要な情報に誰でもアクセスできるようになっている	
従業員それぞれにサーバ等へのアクセスに必要な ID を発行すると共に、見る必要の無い情報へはアクセスできないように OS の機能等を用いてアクセス制限をかける。	□
サーバ等へのアクセスには ID だけではなく、パスワードを要求するようにし、パスワードは容易に推測できないようにする。	□
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（4.1.4）。	□
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、盗難防止対策を行う（4.2.3）。特に、重要な情報には印刷制限をかける。	□
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（4.4.1）。	□
重要な情報に対するアクセス権限の設定を行う（4.4.2）。	□
アクセス記録（閲覧、ダウンロードなど）が取得され、ログレポートが管理者（経営者）に提出されていることを従業員に周知する。	□

シナリオ２　退職者の情報持ち出し、競合他社への就職	■
このシナリオに該当する場合の対策：	
内容	チェック
■退職後の機密保持策や競業避止対策の未整備	
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	□

ればならないかを明確にする（4.1.6）。特に、退職後の機密保持義務や競業避止のため、誓約書等を取ること。	
■営業秘密管理の不徹底	
管理すべき重要な情報資産を分類する（4.1.3）。	□
重要な情報に対するアクセス権の設定を行う（4.4.2）。特に、退職に際してはアクセス権限を見直し、退職者が不必要に情報を持ち出さないようにすること。	□
会社の重要な営業秘密・知財については、必要に応じて特許を取得したり、不正競争防止法により保護されるように、日頃から対策を講じること（5.1.1 も参照）。	□

シナリオ３　従業員による私物 PC の業務利用と Winny の利用による業務情報の漏洩事故	■
このシナリオに該当する場合の対策：	
内容	チェック
■業務に必要な PC を支給していなかった	
業務に必要な PC は会社から支給する。	□
■社内規定の存在が周知されていなかった	
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（4.1.1）。	□
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ならないかを明確にする（4.1.6）。	□
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（4.1.7）。	□
■守られることが期待されない実効性の低い社内規定の存在	
実際の業務を分析し、遵守可能な社内規定とする。	□
■情報が第三者に流出した場合も想定した対策の不備	
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（4.3.5）。	□

シナリオ４　ホームページへの不正アクセス	■
このシナリオに該当する場合の対策：	

内容	チェック
■開発管理の不備	
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（4.4.5）。	□
Web アプリケーションの脆弱性に関しては、開発時にセキュリティを考慮した仕様書を示すと共に、公開前に専門家による確認を行うことが望ましい。	□
■脆弱な運用体制	
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（4.1.2）。	□
情報システムの運用に関して運用ルールを策定する（4.3.1）。特に、必要なログが正確に取得されるようにしておく必要がある。	□
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（4.3.2）。	□
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（4.3.3）。	□
■不十分な不正アクセス対策	
インターネット接続に関わる不正アクセス対策を行う（4.4.3）。	□
特に重要なシステムや、インターネットに直接接続されたシステムについては、IDS（侵入検知システム）や IPS（侵入防御システム）などを導入する。	□
■事故対応体制の未整備	
情報セキュリティに関連する事件や事故等の緊急時に、何をすべきかを把握する（4.5.2）。	□

シナリオ５　　アウトソーシングサービスの利用　　■	
このシナリオに該当する場合の対策：	
内容	チェック
■外部サービスの無許可利用	
SaaS、ASP も含む、新たなソフトウェアや、システムを導入する場合、セキュリティ上のリスクを把握した上で導入の可否を決定する。	□
業務上、必要のないツールの利用制限を行う。	□
■外部サービスのサービス内容についての不十分な理解	
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とる（4.1.5）。	□

サービス約款・SL 等について十分に理解したうえで、利用の可否を判断する。	□
ツール（SaaS、ASP も含む）を使用する場合は、デフォルトの設定を確認し、セキュアな設定を行うよう注意する。	□
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（4.3.4）。	□

シナリオ６　委託した先からの情報漏えい	■
このシナリオに該当する場合の対策：	
内容	チェック
■法令遵守に対する意識の低さ	
個人情報保護法が求める個人情報保護対策を実施する。	□
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（4.1.2）。	□
管理すべき重要な情報資産を分類する（4.1.3）。	□
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（4.1.4）。	□
情報セキュリティに関連する事件や事故等の緊急時に、何をすべきかを把握する（4.5.2）。	□
■委託先管理の不十分さ	
委託先の安全管理措置が個人情報保護法を満足するかを確認する。	□
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とる（4.1.5）。	□
重要な情報を保管したり、扱ったりする場所の入退出管理と施錠管理を行う（4.2.1）。	□

シナリオ７　在庫管理システム障害の発生	■
このシナリオに該当する場合の対策：	
内容	チェック
■事業継続への意識の低さ	
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（4.5.1）。	□
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（4.2.2）。	□

事業継続計画を策定するなど、事業継続マネジメント体制を構築する。	□

シナリオ８　無線 LAN のパスワードのいい加減な管理	■
このシナリオに該当する場合の対策：	
内容	チェック
■無線 LAN の危険性に対する認識の不足	
無線 LAN のセキュリティ対策（WPA2 の導入等）を行う（4.4.4）。	□
インターネット接続に関わる不正アクセス対策を行う（4.4.3）。	□
■パスワード管理の重要性に対する認識の不足	
■情報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 の管理を行う（4.4.1）。	□

シナリオ９　IT 管理者の不在	■
このシナリオに該当する場合の対策：	
内容	チェック
■特定の個人や委託先のスキルに依存しすぎている	
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（4.1.2）。	□
どのようなシステムも複数人が管理できるようにしておく。	□
■	
情報システムの運用に関して運用ルールを策定する（4.3.1）。	□
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。	□
運用手順については、情報システムが停止時にも参照できるように、紙にも印刷しておくこと。	□
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（4.5.1）。	□

シナリオ 10　電子メール経由でのウイルス感染	■
このシナリオに該当する場合の対策：	
内容	チェック
■ウイルス対策ソフト等の動作の確認を定期的にしていない	
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（4.3.2）。	□

ウイルス対策ソフト等の動作を手動で確認（手動監査で、定義ファイルの日付をチェックする等）。	□
クライアント PC の自動チェックツールやポリシー管理ツールを導入する。	□
■ウイルス対策等が十分に出来ない PC への考慮が不十分	
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（4.3.3）。	□
不要なサービスの停止、パーソナルファイアウォールの導入。	□
未対策アプリケーションの局所化（ファイルサーバと分離する等）。	□
■エンドユーザーがシステム構成等を変更することへの考慮が不十分	
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（4.3.2）。	□
社内情報システムの構成や設定が、情報セキュリティに影響を与えないように、必要に応じてエンドユーザが行うことのできる操作に制限を加える（ソフトウェアのインストール等）。	□

付録２：共通して実施すべき項目と企業毎に考慮すべき対策とのマッピング

4. 共通して実施すべき対策	5.企業毎に考慮すべき対策
4.1 情報セキュリティに対する組織的な取り組み	シナリオ番号
4.1.1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	3
4.1.2 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	4, 6, 9
4.1.3 管理すべき重要な情報資産を分類する	1, 2, 6
4.1.4 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	1, 6
4.1.5 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	5, 6
4.1.6 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確にする	2, 3
4.1.7 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	3
4.2 物理的セキュリティ	
4.2.1 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	6
4.2.2 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	7
4.2.3 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	1
4.3 情報システム及び通信ネットワークの運用管理	
4.3.1 情報システムの運用に関して運用ルールを策定する	4, 9
4.3.2 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	4, 10
4.3.3 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	4, 10
4.3.4 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	5
4.3.5 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	3
4.4 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	
4.4.1 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	1, 8
4.4.2 重要な情報に対するアクセス権限の設定を行う	1
4.4.3 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	4, 8
4.4.4 無線LANのセキュリティ対策（WPAの導入等）を行う	8
4.4.5 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	4
4.5 情報セキュリティ上の事故対応	
4.5.1 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	7, 9
4.5.2 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	4, 6

中小企業経営者の皆様、大切な情報を安全に守るために、各種情報をご活用ください。

セキュリティ対策に役立つ情報

- **漏れたら大変！ 個人情報** ～個人情報漏えいを防ぐために、チェックしましょう～
  http://www.ipa.go.jp/security/kojinjoho/index.html

- **情報セキュリティ対策のしおり**
  一般のご家庭や企業（組織）内でパソコンを利用する方々を対象に、情報セキュリティ上の様々な脅威への対策を分かりやすく説明しています。
  下記のアドレスにアクセスしていただくとダウンロードすることができます。
  http://www.ipa.go.jp/security/antivirus/shiori.html

※営利を目的としない用途に限り、原本のまま印刷し配布することに関して制限はございません。

- **情報セキュリティ安心相談窓口を開設** ～情報セキュリティ関連の相談に一元的に対応する窓口～
  http://www.ipa.go.jp/about/press/20101019.html

- **情報セキュリティ安心相談窓口**
  URL：**http://www.ipa.go.jp/security/anshin/**
  TEL：**03-5978-7509**（IPA職員による対応は、平日の10:00～12:00および13:30～17:00）
  FAX：**03-5978-7518**　E-mail：**anshin@ipa.go.jp**

- **5分でできる！ 中小企業のための情報セキュリティ自社診断**
  http://www.ipa.go.jp/security/manager/know/sme-guide/index.html

- **情報セキュリティ対策の診断テスト「情報セキュリティ対策ベンチマーク」**
  ～Web上の質問に答えると、診断結果が自動的に表示され、他社との比較もできます～
  http://www.ipa.go.jp/security/benchmark/

- **中小企業のためのセキュリティツールライブラリ** ～Yes/Noチャートで最適なツールをご案内！～
  http://www.ipa.go.jp/security/manager/know/tool/index.html

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

2011.1 Version 1.0