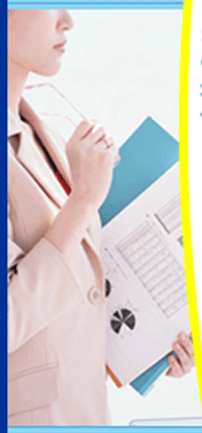
経営情報
レポート

Available Information Report for Corporate Management

顧客・企業を守る！

中小企業の情報セキュリティ対策

1. 情報セキュリティ対策の必要性
2. 守るべき情報とは
3. 中小企業における3つの情報セキュリティ対策
4. ケース別に見る情報セキュリティ対策



株式会社　常陽経営コンサルタンツ

1 情報セキュリティ対策の必要性

近年の情報流出事件と損害賠償

近年、新聞やニュース等でも情報流出事件や事故が多く報道されています。2005 年～2007 年が情報流出事件・事故のピークであり、ここ２年間は減少傾向にあるものの、情報流出・事故は絶えません。

ここ最近の情報流出事件をまとめると以下のようなものがあります。

2010/03/03	（株）三井情報
約 10 万件の個人情報（氏名、生年月日等）が流出漏えい。派遣社員が顧客から預かった個人情報等が記録された派遣元会社所有のノートパソコンを入れた鞄を帰宅途中に紛失。	
2008/11/03	（株）セガ
アルバイトの応募者合計 115 名分の個人情報が外部に流出漏えい。氏名、年齢、住所、本籍地、生年月日、電話番号等。	
2008/10/30	品川近視クリニック
患者情報約１万８千人が外部に流出漏えい。患者氏名、住所、生年月日、電話番号等。なお、流出漏えいした情報が、どのような方法で外部へ漏えいしたのか不明。	

実際にこのような事件があった場合、損害賠償は判例をまとめると以下の通りとなります。

■京都府宇治市

京都府宇治市の住民基本台帳 21 万数千人分が流出した事件では、外部委託業者のアルバイト大学生に対する宇治市の使用者責任を認め、住民１人当たり１万円（プラス弁護士費用 5,000 円）の損害賠償の支払い（02 年 7 月 11 日最高裁判決）。

■ヤフーＢＢ

運営会社のＢＢテクノロジーとヤフーに、１人当たり 5,500 円の損害賠償が課せられた（07 年 6 月 21 日大阪高裁判決）。

また、情報を流出した企業には、上記のような損害賠償だけではなく、個人情報保護法に基づいた、法的責任も問われることになります。

なぜ情報を守らなければならないのか

企業は、企業目的の実現のために、顧客満足の高い製品やサービスを作り出し、顧客を獲得し、製品提供やサービス提供を行い、それらの活動から利益を生み出す一連の活動を効果的・効率的に行わなければなりません。これらの活動に関する情報が流出した場合、企業の信用は失墜し、ビジネスにも悪影響を及ぼします。

したがって、企業の競争力や信用にかかわる情報は、積極的かつ継続的に保護し続けなければなりません。

本レポートでは、企業が守るべき情報や情報に係る脅威を整理し、中小企業に必要な情報セキュリティ対策、そしてケース別の対応策について解説します。

■情報流出における企業への影響

内部情報流出による悪影響	外部情報流出による悪影響
ライバル企業の営業先回り 設計・製造ノウハウ流出 特許の先願 営業秘密 コピー商品の横行 脅迫	賠償金の支払い 株価の低下 ブランドイメージの低下 謝罪広告 顧客離れ 裁判闘争 対応窓口の設置 売上げ減少 悪評 商談中止 ビジネスチャンスの減少

2 守るべき情報とは

守るべき情報資産とは

「情報資産」とは、パソコンやネットワーク機器、ソフトウェアやデータなど、企業が守るべき価値のある資産のことです。

パソコンの導入やインターネットの普及により、企業や自治体などの組織における情報資産の量が急増しており、顧客情報など、その企業でのみ使用されるべき情報が外部に流出すると、企業の信用性の低下や損失を招きます。

また、顧客情報などの個人情報はプライバシーの観点からも保護が必要であり、この情報が漏えいしてしまうと、企業・組織の信頼性の低下は避けられませんので、情報は資産と同様企業経営にとって重要なものとして扱う必要があります。

情報資産は「有形資産」と「無形資産」とに分類できます。

■有形資産の例

- 紙に印刷されたデータ
- サーバーやコンピュータなどのハードウェア
- ネットワーク機器

■無形資産の例

- 顧客情報や売上情報などのデータ
- 人事管理情報
- ＯＳやアプリケーションなどのソフトウェア
- 人間の知識や経験・ノウハウ

情報資産への脅威

企業が「情報資産」を守るためには、以下のような仕組みをつくる必要がありますが、決して難しいものではありません。

●盗まれない	●見られない
●コピーされない	●壊されない
●聞かれない（盗聴されない）	●改造・改ざんされない

しかし、実際にトラブル・事故は起きています。それは、以下のような脅威が情報資産の周りには存在しているからです。

脅威	例
人による脅威	操作ミス、不正行為、不正アクセス
障害による脅威	ハードウェア障害、ネットワーク障害、設備障害
自然災害による脅威	地震、火災、水害

①人による脅威

人による脅威とは、人間の操作ミスや不正行為といった行動から発生する脅威のことで、「過失による脅威」と「故意による脅威」に区分できます。

また、「内部の脅威」と「外部からの脅威」という分類もすることができます。最近の情報セキュリティ事件では、内部による不正行為、犯罪、操作ミスといったものが、原因の大半を占めます。

②障害による脅威

障害による脅威とは、コンピュータの故障やネットワークの不具合など、主にハードウェアやソフトウェアの障害が原因で発生する脅威です。

昨今は、ＡＳＰやクラウドの普及により、様々なネットワークへのアクセスが増えていますが、ハードウェアやソフトウェアにアクセスできなくなったり、場合によっては壊れてしまう可能性があり、これにより業務の遂行やサービス提供に支障をきたします。

③自然災害による脅威

自然災害による脅威とは、地震、火災、水害などが原因で発生する脅威です。

自然災害による脅威は、人による脅威とは違い、発生を抑制することは難しく、発生後の対応を含めた対策を講じることになります。

情報資産の維持管理

情報資産を維持管理するためには、情報資産を「機密性」、「完全性」、「可用性」に係る脅威から保護することが必要となります。

①機密性（Confidentiality）
許可された者だけが情報にアクセスできるようにすること **機密性が維持できていないと　→　不正アクセス、機密漏えい**
②完全性（Integrity）
情報が正確かつ完全であること **完全性が維持できていないと　→　データの改ざん**
③可用性（Availability）
許可された者が必要なときにいつでも情報にアクセスできるようにすること **可用性が維持できていないと　→　サービス停止**

①機密性(Confidentiality)

コンピュータやシステム、データベースなどにアクセスできるユーザーを制限することを意味しています。許可されていないユーザーが、情報やシステムにアクセスすることができないようにしたり、データを閲覧することはできるが書き換えることはできないようにしたりします。このことは、不正アクセスや情報漏えいに対する防御につながります。

②完全性(Integrity)

許可されていない者によって情報が改ざんされたり、破壊されたりしないことを指します。

③可用性(Availability)

正規のユーザーが情報を利用しようとしたときには、いつでも情報にアクセスすることができることを意味しています。つまり、可用性を維持するということは、情報を提供するサービスが常に動作するということを表します。

これらに対する脅威から情報資産を維持管理するということが、情報セキュリティ対策に要求される行為になります。そして、企業や組織の保有する情報資産の特質をよく検討して、機密性、完全性、可用性のバランスを考慮することが大切です。

3 中小企業における3つの情報セキュリティ対策

4つの情報セキュリティ対策

前章で示した３つの脅威及び維持管理の視点を踏まえた中小企業における情報セキュリティ対策は「人」「物」「技術」の３つの視点で対策を講じる必要があります。

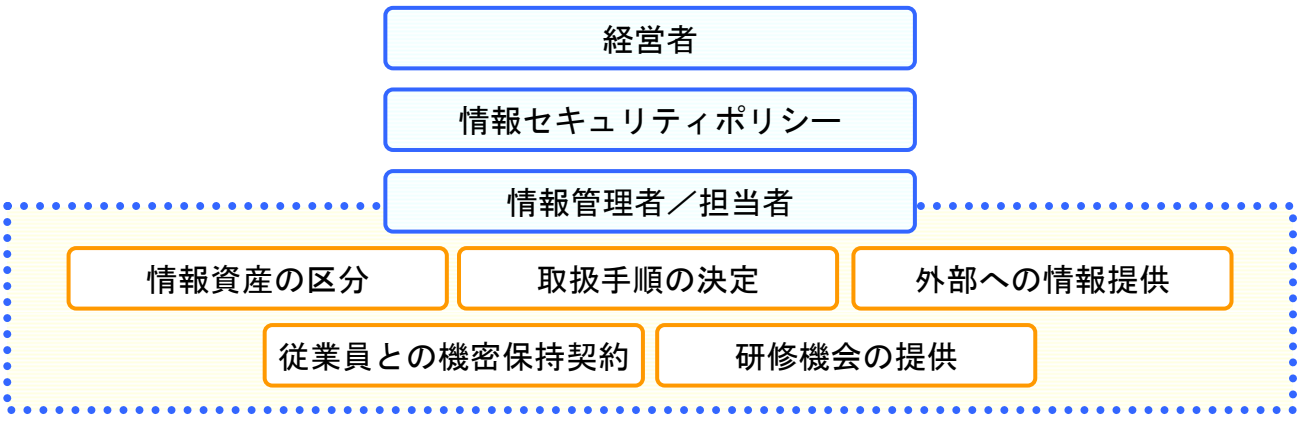
①人的セキュリティ対策
②物理的セキュリティ対策
③技術的セキュリティ対策

①人的セキュリティ対策

人的セキュリティ対策とは、情報資産を守るための管理体制を明確にしたり、利用者のセキュリティ意識を高めたりすることです。

人的セキュリティ対策では、まず情報セキュリティに関しての根本的な考え方である情報セキュリティポリシー（セキュリティ基本方針）を策定します。ここでは、情報セキュリティに関する経営者の意図を従業員に明確にし、実現に対して責任を持つことが求められます。

■情報資産管理体制（概念図）



情報セキュリティポリシーを基に、情報セキュリティ対策に関わる責任者と担当者を配置します。

具体的な取り組みとしては、管理すべき重要な情報資産を区分し、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ます。例えば、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や、重要な情報の利用履歴を残しておくことなどの手順などです。

また、外部の組織と情報をやり取りする際には、情報の取り扱いに関する注意事項について合意を取ることも必要です。

さらに、従業員（派遣を含む）に対し、セキュリティに関しての守秘義務契約や誓約書を交わし、就業上何をしなければいけないかを明示し、併せて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持ち、情報に対する意識を高めることも重要です。

②物理的セキュリティ対策

施設や建物など，物理的な部分にかかわるセキュリティのことです。業務を行っている建物や重要情報を扱うコンピュータを設置している部屋などを対象に、物理的な方法で実施する情報セキュリティ対策です。物理的な人・物の出入り，施設・設備そのものの品質を言います。

具体的には、以下のように決めておく必要があります。

■建物・設備

●重要な情報が管理されている室内は監視を設けること
●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・設置すること
●重要なシステムが設置されている部屋は利用者の入室を制限し、入退室の履歴を管理すること

■無形資産

●重要な書類、モバイルＰＣ、記憶媒体などについて、整理整頓を行うこと
●盗難防止対策や確実な廃棄を行う
●保存した情報の消去方法を決める消去ソフトの活用など、確実に処分する
●私有パソコンの持ち込みの禁止
●記憶媒体の持ち出し禁止

■有形資産

●書類の廃棄（シュレッダー・焼却）手順の決定
●書類保管場所の施錠管理

など

③技術的セキュリティ対策

情報システム及び通信ネットワークの運用管理はシステム管理とウィルス対策を確実に行うことをいいます。この対策では以下のことを整備し、システム運用管理者を定め、管理者を中心に管理・運用していきます。

■情報システム及び通信ネットワークの運用管理事項

- システムの運用手順
- ウィルス対策
- ぜい弱性対策
- 通信などの暗号化
- 外部へのデータ持ち出し

具体的には、以下のような項目を定めなければなりません。

■ＩＤ・パスワード

●システムのアクセスにはパスワード認証を設けること
●パスワードは６文字以上 12 文字以内で設定すること

■ウィルス対策ソフト

●全てのパソコンにウィルス対策ソフトを導入すること
●パターンファイルの更新は管理者側で行うこと
●パターンファイルの更新は毎日手動で行うこと

■不正アクセス防止

●サーバーにファイアウォールを設置すること

■その他

●○○ソフト起動中に休憩時間、席を外す場合にはパスワード付きのスクリーンセーバーを起動するか、コンピュータのシャットダウンを行うこと

4 ケース別に見る情報セキュリティ対策

ケース別の対応策

最後に、会社内でよく見られるケースとその対処方法についてまとめます。

事例は、①情報資産の持ち出し、②ユーザーＩＤとパスワードの管理、③パソコン・データの処分、④メールによるウィルス対策の４つのケースについて説明します。

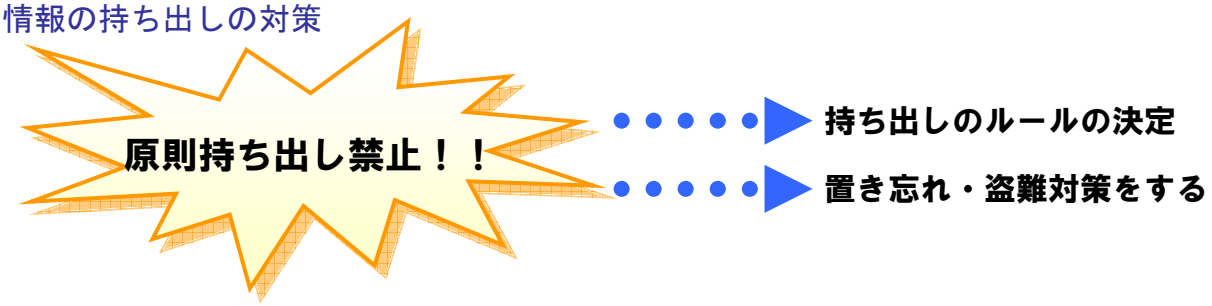
(ケース1)情報資産の持ち出し

重要な書類やデータは、置き忘れと盗難のリスクがあるため、原則として持ち出しを禁止します。

具体的な対策は以下のようなルールを定めます。

①データの持ち出し禁止
②持ち出す場合のルールを決める
③置き忘れ・盗難対策をする→パスワード設定・暗号化・アクセス権設定

■情報の持ち出しの対策



(ケース2)パソコンやデータを処分する

例えば、個人で購入したパソコンを会社内に持ち込みし、業務を行い、新たなパソコンを購入し、パソコンを廃棄した際に、情報が流出する場合もあります。

この場合、表面上データは削除されていますが、全ての情報が完全にパソコンから削除される訳ではありません。一度記憶されたものは、ハードディスクや記憶媒体に残っており、それが情報の流出に繋がります。

このような場合の対策は次の通りとなります。

①個人使用のパソコンの持ち込み禁止
②パソコン・記憶媒体を廃棄する場合の取扱いルールの決定

■パソコン・記憶媒体を廃棄する場合のルール

●物理的に破壊する
●完全消去ツールを使い、データ消去する

(ケース3)ユーザーIDとパスワードの管理

パソコンのＯＳやソフトウェアのユーザーＩＤとパスワードが簡便すぎるために、ＩＤやパスワードを特定され、情報が漏えいしてしまったという事例も少なくありません。

まず、確認しなければならない事項は、パスワード等が従業員の電話番号や誕生日など、他人が情報として知ることが可能なものになっていないかを確認します。また、電話番号や誕生日は使っていなかったとしても、例えばパスワード等が「0001」からはじまり、連番になっていないかということも併せて確認します。

その他にも、ＩＤやパスワードを付箋などに記入してパソコンなどに貼っていることも良く見る光景です。

したがって、ＩＤやパスワードは、他人に推測されないよう難解なものにして、厳格に管理する必要があります。また、定期的にパスワード等を変更することも重要です。

具体的には、以下のような対策を講じます。

①パスワード・ＩＤの管理方法の決定
②他人に解読されない設定をする（暗号化など）
③定期的に変更する

■解読されないパスワード（例）

覚えやすく、かつ他人に解読されない方法のひとつに「文字置換の作成」があります。たとえば、以下のような読替ルールを決めます。

以下の読替ルールを決定する

a→@　p→+　s→1　w→＊　o→＞　r→？　d→&

ルールに従って「ｐａｓｓｗｏｒｄ」を読み替えると

＋@１１＊＞？&

（ケース4）メールによるウィルス感染

コンピューターウィルスによる被害は後を絶ちません。

例えば、発信元が取引先や知人からのメールだったとしても、ウィルスに感染したということがあります。いわゆる、なりすましメールによる被害です。これは、発信者側が自由に発信者名をコンピュータに設定できるからです。

これを防ぐための対策は以下のようなものが挙げられます。

①発信元が不明なメールは読まずに削除する
②添付ファイルに注意する
③ウィルス対策ソフトを使用する

■注意すべき拡張子

拡張子：ファイル名のうち、「.」（ピリオド）で区切られた一番右側の部分。例えば、ファイル名が「e-words.txt」ならば「txt」が拡張子です。

●exe　●com　●bat　など

■ウィルス以外のメールの脅威

●迷惑メール（スパムメール）

受信側の意志とは関係なく大量に送られてくるメール。
宣伝や広告を目的としたもの。対策には、受信拒否設定などがあります。

●チェーンメール

不特定多数のユーザーに転送されるメール。対策としては、メールをそのまま削除することが確実です。

●フィッシングメール

ＩＤやパスワードを詐取するためのインターネットバンキングサイトなどへ誘導するメールです。ＩＤとパスワードの確認を促す内容のメールを送りつけ、メール中に記載されているＵＲＬにクリックさせる手口です。
対策としては、送信元に確認するなどの対応を行います。

最も重要な対策は従業員への教育

情報流出の大半は、実は従業員のうっかりミスが多く、誰もが引き起こすリスクがあります。内閣府の調査によると、情報漏えい元は事業者が約 7 割、業務委託先が約 3 割となっています。事業者と委託先で実際に漏えいに関わった者についてみると、従業員（社員や派遣・アルバイトなど）が約 8 割で、その原因の 7 割強が不注意によるものです。

情報流出は、何も悪意のある犯罪者が引き起こす事件とは限りません。個人情報を取り扱う従業員であれば、誰もが情報流出のリスクを背負っています。

今やビジネスツールとして不可欠の存在となった電子メールも、情報流出経路の一つであり、内部統制の面からも社員の電子メールをいかに監視するかが、企業にとって重要な課題となっています。

勝手に社員の電子メールを見るとプライバシー侵害と言われたこともありましたが、過去の判例では、社会通念上相当な範囲であれば、会社が電子メールをモニタリングするのはプライバシーの侵害に当たらないとしています。

「このくらいは」と高をくくっていると、思わぬリスクを背負い込むことになります。

以上のような仕組みをつくり対策を打つことが、中小企業に求められる課題ですが、最も重要ことは、従業員の情報流出・情報セキュリティに対する意識を高めることです。

■参考文献

「国民のための情報セキュリティサイト」　総務省
「よくわかる事例で学ぶ情報セキュリティ」　ＦＯＭ出版
「ビジネスマンのための情報セキュリティ入門」　東洋経済新報社
「中小企業の情報セキュリティに関する報告書」
「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」
共に　独立行政法人情報処理推進機構