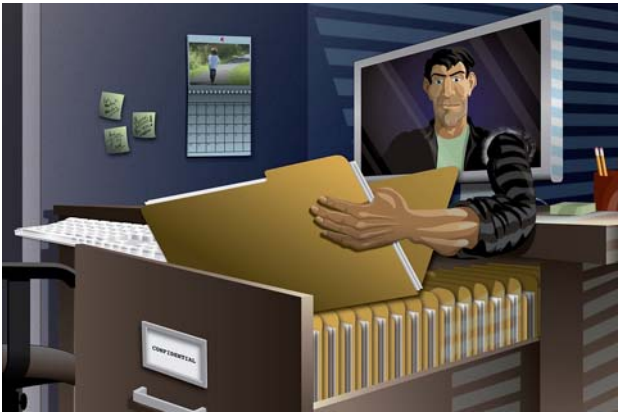
中小企業**経営者**のための
情報セキュリティ対策
（後悔しないために）

御社の重要情報が狙われていますよ！



すぐ対策を！

インターシステム株式会社内
中小企業情報セキュリティ研究会

2018/7/1 初版

目次

経営者へ・・発刊にあたって・・・3

1．経営者が認識すべきこと・・これだけは知っておきたい・・・・・・・・・・・・・・・・・・・・・・・・・5

1．情報セキュリティ対策の不備で、様々な不利益が企業に起きます・・・・・・・・・・・・5

1．経済的損失が発生します

2．大切な顧客をなくすことになります

3．通常の業務運営ができなくなります

4．自社の従業員への悪い影響がでます

2．個人情報については、特に配慮が必要です・・個人情報は、要注意・・

1．個人情報とは

2．個人情報取扱に関する4つの基本ルール

3．個人情報を管理する責任は、法律で罰則があります

2．経営者は何をすればよいか

1．すぐに始める情報セキュリティ対策・・10

1．重要な情報を把握する

2．重要な情報を適切に管理する

3．関係者以外の社内への立ち入りは制限をする

4．重要な情報が記載された資料やそれらが格納された電子媒体が不要になった時

5．重要な情報を外へ持ち出す場合には、盗難、紛失の危険に備える必要がある

6．業務に使用するパソコンをトラブルから保護する対策が必要です

7．パスワードを設定して、利用する

8．電子メールの利用は、宛先の確認が必要です

9．守秘義務を徹底することが必要です

2．できるだけ早く始める対策・・できることから・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・13

1．経営者は情報セキュリティに関する方針を定め提示する必要があります
2．外部委託先への対応が必要です
3．緊急時の連絡体制を明確にする
4．自社の情報セキュリティ対策や、事故が起きた時の対応
3．管理者に実施させる対策……15
1．更なる対策（管理の実践）・・・どう管理したらよいか
2．技術的対策
3．物理的対策
4．人的対策
3．終わりに・・経営者の取組み……21
1．できることからはじめる
2．はじめたら継続する
3．継続していることで役立てる

経営者へ・・発刊にあたって

本冊子は、「中小企業が対応しなければならない情報セキュリティ対策」について、経営者にできるだけ理解し、対応していただけるように、必要最低限のことを分かり易く記述したものです。

これまで以上に、企業活動でのインターネットの重要性が増し、インターネット無しでは、何もできないネット社会になっています。ネット社会では、データの盗用、流出、**サイバー攻撃**等が日常化され、**「最低限の情報セキュリティ対策」**無くしては、大きな経済的損害を

受ける事になり、会社の存続が危ぶまれる事態にもなりかねません。こうした状況を経営者が認識し、対策を立てる事に少しでも役立ちたいと思い、本冊子を作成しました。経営者の中には、①自分の会社は、関係ない②何か起こってから、対応すればよい③費用がかかるだけで、殆どメリットが無い等、色々な理由で、情報セキュリティ対策に無関心であったり、基本的な対策が殆どされていない会社の経営者は、この際、認識を改める必要があります。

本冊子を活用して、情報セキュリティ対策の重要性をしっかりと理解し、必要最低限の対策を立てていただければと思います。

なお、本冊子は、中小企業の経営者および情報管理者の皆様に向けてIPA（(独)情報処理推進機構）にて公開されております「中小企業の情報セキュリティ対策ガイドライン第2.1版」を参考にして情報セキュリティに永年現場で取り組んだメンバーが考えた必要最低限の対策を記載したものです。

1　経営者が認識すべきこと・・・これだけは知っておきたい

1　情報セキュリティ対策の不備で、様々な不利益が企業に起きます

.1　経済的な損失が発生します

自社の重要な情報、個人情報や取引先の機密情報が万一漏洩した場合は、

■取引先、取引先の顧客などから損害賠償請求を受

けたり、

■漏洩情報を記録していたデータベース等の利用を差し止められて、業務に、一時的にできなくなり、大きな経済的損失を与える事になります。

■事例・・・社会的には、インターネットバンキング利用時の偽サイトへの不正送金やクレジットカードの不正利用、ランサムウエア（身代金要求のマルウエア）感染などで直接的な損失を被る企業の数も増えています。平成29年のインターネットバンキングに係る不正送金事犯の発生件数は425件、被害額は 10 億 8,100 万円（警視庁の調査）

.2 大切な顧客をなくすことになります

情報セキュリティ事故を発生させると、その原因が何であれ

■事故を起こした企業に対する責任が問われ、企業の社会的評価は低下し取引は激減します。

■事例・・・特に、教育サービス事業者の場合は、顧客情報漏洩の影響により既存会員の退会が増え、さらに新規営業活動を自粛した結果、前年度比で約 25%程度会員が減少するという影響が現実におこっています（事業報告書・報道資料による）

.3 通常の業務運営ができなくなります

情報セキュリティ上の事故が発生すると、

■被害の拡大を防止するため、自社で運用しているサーバーの停止や、インターネットへの接続の遮断などを行います。この結果、インターネットを通じた取引先からみると、営業を停止しているのと同じ状態になるため、措置を講じている間は営業機会の喪失となります。

■さらに、販売管理、会計などの基幹システムや、電子メールが使えなくなったりすることで、社内の業務が停滞してしまいます

■事例･･･2015 年に発生した特殊法人における個人情報漏洩事故の例では、ウェブサイトの一部コンテンツを脆弱性の確認のため約 6 か月間停止するとともに、職員が使用する外部向け電子メールを使用禁止することになり、業務に大きな支障が出ました。（当事者の公表資料による）

.4 自社の従業員へ悪い影響がでます

情報セキュリティ対策の不備を悪用した内部不正が容易に行えるような職場環境は、

■従業員のモラル低下を招く要因となります。さらに事故を起こしたにもかかわらず、 従業員のみを罰して経営者が責任を取らないような対応をとることで、従業員が働く意欲を失う恐れがあります。

■情報漏洩などの事故による企業としてのイメージダウンを嫌って転職する従業員も現れます。

また、従 業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。

■事例1 海外競合企業への技術情報の流出

2014 年 3 月、F社のフラッシュメモリーの研究データを不正に持ち出し、転職先である韓国の半導体大手H社に提供したとして、F社と業務提携していた半導体メーカー G社の元技術者が、不正競争防止法違反（営業秘密開示）容疑で逮捕された

■事例2 委託 SE による個人情報漏えい

2014 年 7 月、A 社の顧客データベースを保守管理するグループ会社 B社の委託先の元社員が、顧客の個人情報を名簿業者へ売り渡す目的で、記憶媒体にコピーし流出させたとして不正競争防止法違反の疑いで逮捕された。

2 個人情報については、特に配慮が必要です･･･個人情報は、要注意

.1 個人情報とは

.1 生存する個人に関する情報であって、

■当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるものを個人情報という。

■他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含みます。

.2 個人識別符号が含まれるものも個人情報です

■「個人識別符号」とは、

特定の個人の「**身体の一部の特徴**」を文字、番号、記号、符号等で、表現したもので、特定の個人を識別することができるものは、個人情報です。

＊＊＊もっと知りたい（個人情報保護法）＊＊＊　巻末参照

.2 個人情報の取扱に関する４つの基本ルール

.1 個人情報の取得・利用する時は、

■利用目的をできる限り特定しなければならない。

.2 個人データの安全管理ために

■必要かつ適切な措置を講じなければならない。

.3 個人データの第三者提供は

■原則としてあらかじめ本人の同意を得なければならない。

■第三者に個人データを提供した場合または、第三者から個人データの提供を受けた場合は、一定事項を記録しなければならない。

.4 保有個人データの開示請求への対処は

■本人から保有個人データの開示請求を受けたときは、本

人に対し、原則として当該保有個人データを開示しなければならない。

■個人情報の取扱いに関する苦情等には、適切・迅速に対応するよう努めなければならない。

■本人からの請求に応じて、個人情報を開示、訂正、利用停止等をしなければならない。

.3 個人情報の取り扱いを誤ると法律で罰せられることがあります。

個人情報保護法は、企業の個人情報の取り扱いのルールを定めた法律ですべての事業者に適用されます。そのため、保有する個人情報の取扱は、法律で定められたルールを遵守しなければなりません。また、人種、信条、病歴などが含まれる個人情報の取得には原則として本人の同意が必要となります。

＊＊＊もっと知りたい（個人情報保護法）＊＊＊　巻末参照

2 経営者は、何をすればよいか

1 すぐに始めるセキュリティ対策

1. 重要な情報を把握する

その情報が社外に漏れると、会社運営上で重大な問題を引き起こす可能性のある情報を「自社の重要な情報」として把握し、管理する必要があります。特に、個人情報（マイナンバーを含む）は、法律で保護が規定されており、違反の場合は刑事罰が科されますので重要です。

2. 重要な情報は、適切に管理する

重要な情報を机の上などに放置しないで、管理、保管する必要があります。

3. 関係者以外の社内への立ち入りは制限をする

関係者以外の人が、社内への立ち入りを制限する必要があります

4. 重要な情報が記載された資料やそれらが格納された電子媒体が不要になった時

紙の場合には、シュレッダー、電子媒体の場合には、消去ソフトを利用するか、電子媒体を破壊して、読めなくし、一般のゴミとは区別して処理をする必要があります。

5. 重要な情報を外へ持ち出す場合には、盗難、紛失の危険に

備える必要がある

対策としては、

■持ち出しの際は、必ず上司の許可を受け、記録に残し、データ読み取りの際のパスワード設定、暗号化等でデータを守ることが必要です

6. 業務に使用するパソコンをトラブルから保護する対策が必要です

トラブル発生の原因としては、

■コンピュータウイルスなどの悪意あるソフトウエア(以降マルウエアと省略)

■外部からの不正アクセス

■私物のパソコンの利用

■業務データの破損、誤消去

これらの想定される原因への対策が必要です。

7. パスワードを設定して、利用する

パスワードを利用して、本人確認をし、不正利用・アクセスを防ぎます。

パソコン、スマートフォン、携帯電話、インターネット利用時には、殆どの場合、必要になり

特に業務に利用する場合には、パスワードは必ず利用する必要があります。

パスワード作成は

■他人に推測されるパスワードは、使わない

■大文字・小文字・数字・記号の組み合わせで作成する

■パスワードは、8 桁以上で作成する

以上の、要件を充足することが必要です。

＊＊＊もっと知りたい（パスワード）＊＊＊　巻末参照

8. 電子メールの利用は、宛先の確認が必要です

業務の電子メールの内容は、重要な情報が多く、宛先を間違う「誤送信」は、無いようにする必要があります。そのために以下の対策があります。

■送信前に宛先と内容を再確認する

■重要な情報は、本文でなく、パスワードで保護された添付ファイルにする

9. 守秘義務を徹底することが必要です

会社にとって重要な情報は、従業員であれば、対外的には秘密にしなければなりません。それが守秘義務です。採用の際に必ず守秘義務の誓約書に署名させ、入社後は研修を実施して徹底することが大切です。

2　できるだけ早く始める対策・・・できることから

.1 経営者は、情報セキュリティに関する方針を定め、 提示する必要があります

情報セキュリティ対策を組織的に実施する意思を、関係者に明確に示すために、情報セキュリティに関する方針を定め、社内外に提示する必要があります。

＊＊＊もっと知りたい（情報セキュリティに関する方針）＊＊＊ 巻末参照

.2 外部委託先への対応が必要です

業務の一部を外部に委託（共同実施も含む）する場合は、相手先でも少なくとも自社と同等の対策が行われるようにしなければなりません。そのためには契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する必要があります。

.3 緊急時の連絡体制を明確にする

情報セキュリティ対策を実施するとともに、万が一の情報漏洩等の発生（インシデント）に備えて、緊急時の連絡体制を整備しておきます。個人情報の漏洩の場合は、本人への連絡、所管の官庁への連絡などが必要になります。

.4 自社の情報セキュリティ対策や、事故が起きた時の対応

普段から、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが必要です。

3 管理者に実施させる対策

1. 更なる対策（管理の実践）・・・どう管理したらよいか

次に、経営者によって示された情報セキュリティに関する方針に基づいて管理策を実践していくわけですが、管理はコンピュータシステムに限らず、建物や事務室等の施設に係るもの、規則や教育等の組織や従業員に係るものもあります。

ここでは情報セキュリティ対策を技術的対策、物理的対策、人的対策の 3 つで説明いたします。

■技術的対策

認証システムやマルウエア対策などシステムで行う対策

■物理的対策

入退管理や盗難防止など、主に建物や施設で行う対策

■人的対策

規程や手順書などのルール、従業員教育などで行う対策

2. 技術的対策

.1 インターネットに繋がるソフトのアップデート

OSや電子メールソフト、ブラウザー等にセキュリティホール(情報セキュリティ上の欠陥)が見つかるとそのソフトの製造元(ベンダー)から修正プログラム(パッチ)が提供されます。

ほっておくと不正アクセスを招くことになり、即刻アップデーを行う必要があります。

.2 マルウエア対策

新たなマルウエアが見つかると、マルウエア対策ソフトの製造元（ベンダー）からパターンファイルが提供されます。ほっておくとマルウエアの侵入を招くことになり即刻パターンファイルをダウンロードする必要があります。また対策漏れがあるとそこからマルウエアの侵入を招く事になり、全社的なマルウエア対策を行う必要があります。

.3 パスワード管理

標準で組み込まれている ID やパスワードをそのまま使用したり、住所や電話番号、誕生日等をパスワードに設定しているような場合、ソーシャルエンジニアリングやパスワード推測ツールによって簡単に解析されてしまいます。

従って、パスワードはできるだけ推測され難いものに設定する必要があります。また、パスワードを書いたメモをディスプレイに貼ったり、引出しの中に置く等の杜撰な管理はやめるべきです。同じパスワードを使いまわしをしていると、パスワードの漏洩による被害が連鎖的に拡大することになります。パスワードの使いまわしは絶対やめるべきです。

.4 アクセス制御

だれでもが情報のアクセスが可能な状態ではその管理および制御が難しくなります。従って、情報にレベル付けを行い、人や部署を制限する等のアクセス制御を行う必要があります。

.5 インターネットトラブル対策

ウェブサイトの中にはマルウエアが仕組まれているホームページや正規のホームページに似せた偽サイトが存在しており、マルウエアに感染したり、ID やパスワードが盗まれる危険があります。閲覧やSNSへの書き込みの制限等、インターネットを介したトラブルの対策を実施する必要があります。

.6 重要情報（電子）の保護対策

仮に、重要情報（電子）がマルウエアや故障や誤操作等で消失した場合、復旧に時間がかかると自社の業務や取引先の業務に支障をきたすことになりかねません。

従って、重要情報（電子）は定期的にバックアップを行っておく必要があります。

また、復旧の手順も整備しておく必要があります。

.7 無線 LAN の安全な利用

電波が建物の外に飛んでしまうため、適切な情報セキュリティ対策をとっていないとIDやパスワード等の重要な情報が漏洩したり、アクセスポイントが他人に無断で使用される可能性があります。最悪、犯罪に利用され犯人扱いされる場合もあります。

従って、無線LANを使用する時は強固な暗号化を施す等の対策を実施する必要があります。

3. 物理的対策

.1 重要情報(書類)の保護対策

重要な情報(文書)は不要不急の時は書庫に保管して施錠する等、紛失や漏洩しない様な対策を実施する必要があります、

.2 情報機器・文書の盗難防止

退社時にはパソコンや記憶媒体、重要文書等は鍵のかかる書棚・引出しに入れて帰る等、盗難防止対策を実施する必要があります。

.3 部外者の立ち入り制限

事務所に無許可の人が立ち入らないように制限する必要があります。

4. 人的対策

.1 重要情報廃棄ルールの徹底

重要情報を廃棄する場合、文書は裁断、電子データは消去ツールを使用する等、重要情報の廃棄ルールを定め、徹底する必要があります。

.2 採用時の守秘義務説明

従業員を採用する際に守秘義務について説明し、守らせる必要があります。

.3 情報管理教育

従業員への定期的な情報管理の意識付けを行う必要があります。

.4 秘密保護条項

取引先との間で取り交わす契約書に秘密保護条項を規定しておく必要があります。

.5 離席時のパソコンのロック

離席している間に他人にパソコンを操作されることのないように、離席時にパソコンにスクリーンセーバ等によりロックをかける必要があります。

.6 重要情報持出ルールの徹底

重要情報の社外持ち出しのルールを定め、徹底する必要があります。

.7 最終退出ルールの徹底

最終退出時の事務所の施錠や最終退出の記録等のルールを定め、徹底する必要があります。

.8 不信電子メール対策

従業員が不信な電子メールの添付ファイルを開いたりリンク先を不用意に参照したりしないように日頃から教育する必要があります。

.9 重要情報の送信ルール

重要情報を電子メールで送る場合、本文には記述せず、添付ファイルに記述して別の電子メールで送る必要があります。

添付ファイルにはパスワードをかける必要があります。

.10 誤送信対策

電子メールアドレスは極力アドレス帳に登録してある実績のある

もの使用し、送信時は目視により送信アドレスを必ず確認する等の誤送信対策を実施する必要があります。

.11 情報漏洩・紛失・盗難時の対応策

情報漏洩や紛失・盗難発生時の組織やマニュアル等の対応策を明確にする必要があります。

.12 情報セキュリティ注意喚起情報の社内共有

ウェブサービスや製品メーカーが発信するセキュリティ注意喚起情報の社内共有の仕組みを構築する必要があります。

.13 個人所有端末の社内利用のルール化

個人所有のパソコンやスマートフォンの業務利用の可否を明確にする必要があります。可とする場合は、紛失や盗難策を規定する必要があります。

3　おわりに・・経営者の取組み

1　できることからはじめる

情報セキュリティ対策は、経営者にとっては、地震対策と同じように何らかの対策が必要なことは分かっているが、どこまで対応しても、終わりが無く、実際に発生して初めて、その対策が生きる事になります。ただ、情報セキュリティ対策は、最近になってその必要性が社会的にわかってきたのが実情だと思います。

いつ発生するかわからない個人情報、会社の重要な情報の流失、マルウエアに感染による業務の停止への対策として、とりあえず、できることからはじめることが大切です。経営者が情報セキュリティ対策に対して動き始めることで、会社全体の雰囲気が大きく変わります。

2　はじめたら継続する

できることからはじめた情報セキュリティ対策は、続けることが大切です。続ける事によって、習慣化して、自然と情報セキュリティの関心が高まり、対策が効果あるものになります。そのためには、はじめた情報セキュリティ対策が、業務にも役立ち、日常の業務の中に溶け込んでいけるもので、単なる情報セキュリティ対策のため業務であってはなりません。セキュリティ対策を継続することで、さらに業務処理が改善される様な取組みが大切です。

3 継続することで役立てる

情報セキュリティ対策は、残念ながらこれで終わりという事はありません。対策には、費用もかかりますし、手間もかかります。これは、中小の企業の経営にとっては、大きな負担になります。ただ、中小企業の強みは、少人数なので、一人一人の顔が分かることです。この強みを生かして、単なる情報セキュリティ対策のためでなく、日常業務のなかで生かすことをできるようにすることです。余分に必要となる「情報セキュリティ対策コスト」を有効に役立てることが大切です。そのためには、形式的な安全対策は、できるだけ省いて、必要最小限度での対策に止め、問題が発生した場合に迅速で、適切な対応ができるようにすることが何よりも大切です。

＜＜個人情報保護法、パスワード等の詳細な説明はこちらです＞＞

■もっと知りたい（個人情報保護法）

・個人情報保護法について（全体構成）

https://www.ppc.go.jp/personalinfo/

・個人情報の保護に関する法律（平成 15 年法律第 57 号）（全面施行の日（平成 29 年５月 30 日）時点の法律）

https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf

・個人情報の保護に関する法律についてのガイドライン（通則編）

https://www.ppc.go.jp/files/pdf/guidelines01.pdf

・個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）

https://www.ppc.go.jp/files/pdf/guidelines02.pdf

・個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）

https://www.ppc.go.jp/files/pdf/guidelines03.pdf

・個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）

https://www.ppc.go.jp/files/pdf/guidelines04.pdf

■もっと知りたい（パスワード）

・安全なパスワード管理（総務省の HP）

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.ht

■もっと知りたい（情報セキュリティに関する方針）

自社に適した情報セキュリティ対策を行うには、まず企業が活動を行う際に直面する情報セキュリティ関連のリスクを確認し、組織として実行すべき情報セキュリティ 対策を組織の正式な規則として情報セキュリティポリシーを定め、これに基づいて従業員が行動することでリスクを現実的に問題のないレベルまで封じ込める必要があります。

企業が直面するリスクは、事業領域や取り扱う情報、企業を取り巻く環境によっても異なります。自社に適したポリシーを作成する事が重要です。

・IPA（独立行政法人情報処理推進機構）

中小企業の情報セキュリティ対策ガイドライン第２．１版

4. 情報セキュリティポリシーの策定　参照

https://www.ipa.go.jp/files/000055520.pdf

情報セキュリティ対策を行う上での進め方やプライバシーマークの取得、マイナンバーへの対応等のご相談につきまして、弊社では御社の状況等を伺いながら、具体的な対策等のご提案をさせて頂きますので、下記のお問い合わせ先にご連絡下さい。

****

お問い合わせ先:インターシステム株式会社

https://www.inter-system.co.jp/ffff/f-001-fr.htm

****