情報セキュリティ研修
（ 無料トライアル版 ）

２０１４年２月　Ver.1.0

Copyright(C) 2014アーチ株式会社

はじめに

本テキスト『情報セキュリティ 研修』は日常業務で取り扱う、
情報に関する基本的なルールをまとめたものです。

ネット時代の常識として理解、実践していただきたいことを簡潔にまとめて
あります。

情報取扱いルールをすでに策定済みの企業にも利用できるよう、本テキストは
汎用的な内容となっています。

また日常生活でインターネットを利用する場合にも役に立つ内容となっています。

情報セキュリティの必要性

日常の業務で情報を取り扱うリスク

元は米国DARPA （国防高等研究計画局）が開発した軍用ネットワークで
あったインターネットが冷戦終結後に民間に開放され、全世界で利用できる
ネットワークが整備されました。

ＰＣから全世界につながる低コストネットワークの実現で情報革命が起きました。
反面インターネットの常時接続環境を利用することの脅威にもさらされています。

- 個人情報漏えい
- データ改ざん
- ウイルス感染
- システムダウン

ニュースで上記の事例の報道を見ない日はありません。

インターネットの利用は常に危険にさらされており、安心・安全に情報を取り扱
うには「リスク」を具体的に認識し、対策をとる必要があります。

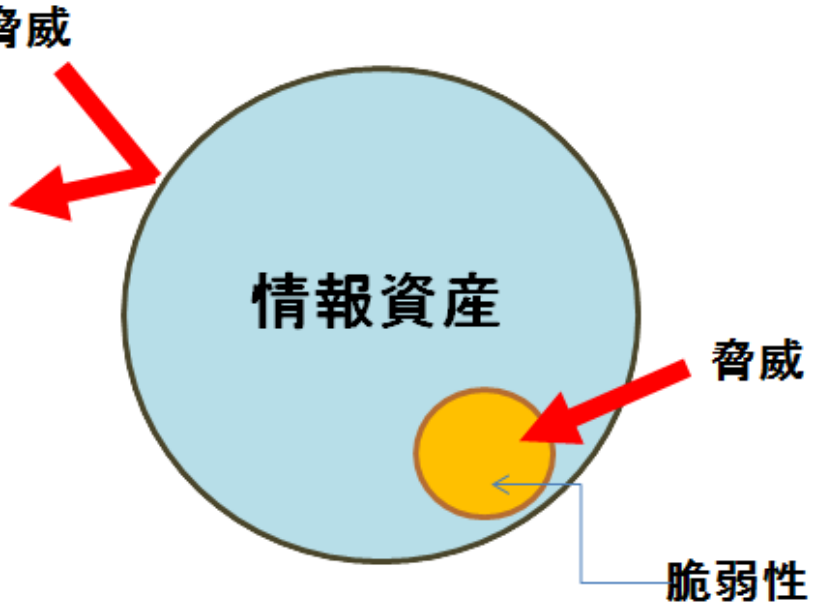
リスクとは

リスクの３要素

リスクを考える場合

- 守るべき情報（情報資産）
- 情報を狙う（脅威）
- 情報資産の弱点（脆弱性）

の３つの要素から考えます。



情報資産が内外の脅威によって棄損される可能性のことを「リスク（Risk）」といいます。

実際に個人情報の流失事故事例などが発生して、情報資産が損なわれた状態のことを「インシデント(Incident)」といいます。

情報セキュリティとは１

リスクへ対応するために必要な情報セキュリティ

いまどきウイルス対策ソフトを業務用PCに導入せずにインターネットに接続する企業はないとは思います。

しかしウイルス対策ソフトの「ウイルス定義ファイル」が古いままならウイルス対策ソフトはPCに入っていないのと同じことです。

LANで社内ネットワークが構築されている場合、全社的に「ウイルス定義ファイル」が最新で統一されてないと 、脆弱な部分からウイルス感染が広がりかねません。

ウイルス対策ソフトひとつをとっても全組織的に「ウイルス定義ファイル」が、最新状態であるかの確認作業が必要になってきます。

このように情報を毀損する脅威から組織を防衛し維持するには、技術的、物理的、人的、組織的な取り組みを推進する必要があります。

この取組のことを「情報セキュリティ 」対策といいます。

情報セキュリティとは２

情報セキュリティ　（information security）

情報セキュリティ　（information security）とは、情報の「機密性」、「完全性」、「可用性」の３要素を維持することをいいます。
この３大要素の頭文字をとって「CIA」といわれています。

※　情報を「CIA」（機密性・完全性・可用性）の観点から維持していくための規格 としてJIS Q 27001（ISO/IEC 27001）/ ISMSがあります。

情報を守る規格１

JIS Q 27001（ISO/IEC 27001）　/　ISMS

情報を「CIA」（機密性・完全性・可用性）の観点から維持していくための規格としてJIS Q 27001（ISO/IEC 27001）　/　ISMSがあります。

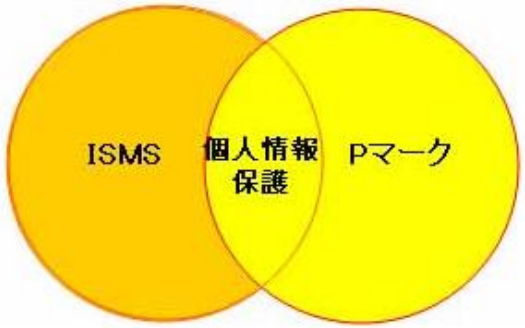
リスクマネジメントとは組織に想定される各種のインシデント（自然災害も含む）を費用対効果にみあった方法で処理するための経営管理法であり、
「情報セキュリティマネジメント」もリスクマネジメントの一部です。

情報を守る規格２

JIS Q 15001　プライバシーマーク

ISMSは情報を資産と考えて守る仕組みですが、個人情報に特化して情報を守る仕組みが「プライバシーマーク」認証制度です。日本工業規格として「JIS Q 15001」があります。

プライバシーマークは組織の保有する情報に含まれる、顧客・従業員情報などの「個人情報」を本人から同意をとった範囲内で利用・保護する仕組みです。
ISMSは個人情報も資産と考え、プライバシーマークは個人情報はあくまで本人から同意して取得、限定された範囲で利用できる預かりものという考え方が違います。

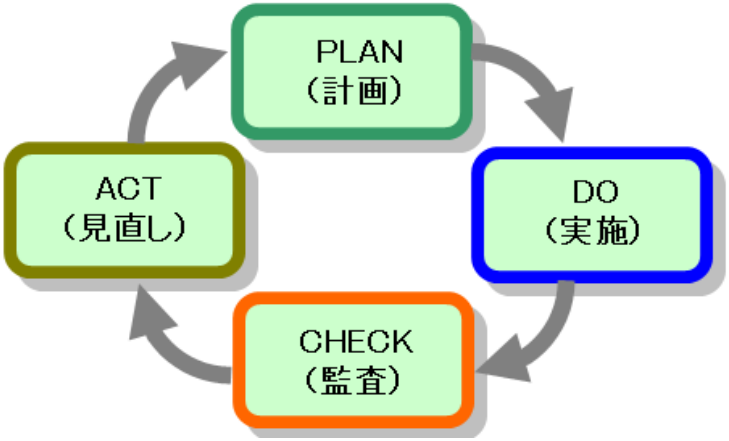


ISMSのマネジメントシステムはPマーク認証取得の規格であるJIS Q 15001の要求事項を全て満たしているわけではありません。

情報を守る規格３

ＰDCAサイクル

ISMSとPマークは「ＰDCAサイクル」を採用したマネジメントシステムという考え方は共通しています。



【Plan (計画) 】　基本方針を策定し対策を具体的に計画し目標を立てる。
【Do (運用) 】　計画に基づいて対策の導入・運用を行う。
【Check(見直し) 】　計画を実施した結果の監視・見直しを行う。
【Act (改善) 】　経営陣による計画の改善・処置を行う。

この「PDCAサイクル」を継続的に繰り返すことで情報セキュリティレベルを維持し、同時にスパイラルアップを図っていきます。

ＰＣの利用者の心得１

常に最新のセキュリティパッチをあてておく

- ＯＳやソフトウエアは常に最新状態ですか？

ＯＳやソフトウエアのセキュリティホール（脆弱性）を突いたウイルス攻撃がインターネット経由で常態化しています。

Windows Updateを有効に設定して、常に最新のセキュリティパッチをＯＳに適用しましょう。

ウイルス対策ソフトは常に最新状態ですか

- ウイルス定義ファイルは常に最新の状態に更新していますか？
- ウイルス対策ソフトのリアルタイム保護機能を有効にしていますか？
- ハードディスク全体のウイルススキャンは定期的に実行していますか？

ウイルス対策ソフトは日々新種が発生するコンピュータウイルスを検出するためには「ウイルス定義ファイル」を常に最新状態に保つ必要があります。

ＰＣの利用者の心得２

不審なメールは開封しない

- 送信元に心当たりのない添付ファイルの付いたメールは開封しない。
- 送信元に心当たりのないＨＴＭＬ形式メールも開封しない。

メールの添付ファイルよりウイルスに感染する例が多発しています。
送信元や添付ファイルの拡張子を偽装するなど手法も巧妙化しています。

また添付ファイルがなくともＨＴＭＬ形式メールだとプレビューだけでマルウエア（ウイルス）に感染する危険性もあります。ＷＥＢサイトにアクセスするだけでウイルスに感染するのと同じ理屈です。

送信元が怪しい場合メールの@以降のドメインを正規の送信元ドメインと比較することで判断できます。

不審なメールは開封しないでそのまま削除してください。

ＰＣの利用者の心得３

ＩＤ・パスワードの管理

- 自分のＩＤを他人に教えない
- ＩＤを共有しない

ネットワークでのサービス利用には本人を識別する「認証」が重要になります。
本人を識別するためＩＤ・パスワードでサービスの利用可否を判定します。

ＩＤ・パスワードで認証することでだれがどの「情報・サービス」にアクセスしたかの記録がサーバー上に残ります。

ＩＤ・パスワードの使用者が１人でないと問題が発生した時の利用者特定できないことになります。

ＰＣ用のＩＤを人に貸すことは首から下げている社員証を人に貸すのと同じです。

ＰＣの利用者の心得４

パスワード

- 他人から推測されないパスワードを設定しましょう。
- ブラウザのパスワード保存機能は切っておく
- パスワードを付箋に書いてＰＣに張り付けない。
- パスワード入力中に人に手元を見られていないか確認しましょう。
- 緊急時でも人にＩＤ・パスワードは人に貸さない。

パスワードは英字大文字、小文字、数字、記号を混在させて作成することが
のぞましいです。会社でパスワード桁数作成規定がある場合は従ってください。

パスワードには生年月日、電話番号、社員番号、ありふれた文字の連続や
容易に推測される文字を使用しないでください。

面倒だからといってブラウザのパスワード自動入力機能やパスワードを付箋
で貼ったりすると、ソーシャルハッキングの対象になりかねません。
ハッキングで一番多いのがソーシャルハッキング
（ソーシャル・エンジニアリング）です。

オフィスでの行動について１

施錠

- ノートPCを使用者はセキュリティワイヤー（ケンジントンロック）で施錠する。帰宅時は鍵の掛かる引き出し、キャビネットで施錠保管してください。

整理整頓

- 帰宅時には机上に書類は置かないくらいの心がけをしてください。
  帰宅時に機密・個人情報を含む書類は引き出しやキャビネットへ
  仕舞い施錠を確認してください。

会議

- ホワイトボードの消し忘に注意してください。
- 会議資料の置き忘れに注意してください。

オフイスでの行動について２

社員証・書類

- 社員証や入館証を紛失しないよう必要以上に持ち歩かないでください。
  鞄を盗難されないよう肌身離さず所持してください。
  （電車の網棚に鞄は置かない。帰宅時、飲酒時は特に注意）

機器の接続

- 社内ネットワークへは社外または個人が所有するPCを無断接続しないでください。（個人が所有するPCを無断で持ち込まない）
- スマートフォンやタブレット等を社内の無線ＬＡＮに接続する必要が業務上ある場合は、管理者の許可を得てください。

機密情報

- 機密情報や社外秘情報を、友達、家族、別の顧客へ話さないでください。
- 居酒屋、電車の中、お手洗い、喫煙室、エレベータ内等で実名を出して企業情報を話題にしないでください。

オフィスでの行動について３

PCの社外持ち出し

- ノートPCはハードディスクの暗号化対策を実施し管理者による許可を得て持出してください。
- お客様先へ持ち込み作業する場合は相手先の指定するセキュリティ対策を実施してください。

ファイル交換ソフトの利用

- ファイル交換ソフトは社内・社外を問わず利用しないでください。

ファイル交換ソフトは著作権違反や情報漏洩が多発していることから、無用なリスクを避けるため自宅での利用も推奨できません。

オフィスでの行動について４

ファックスの利用

- 送信前に宛先を確認して誤送信しないようにしてください。
- ファックスした紙はその場に放置しないでください。

コピーの利用

- コピーした紙、失敗した紙はその場に放置しないでください。
- 裏紙は再利用しないでください。
- 廃棄する紙はシュレッダー処理するか、鍵付きの廃棄用ＢＯＸに入れてください。

オフイスでの行動について５

事故報告

情報漏洩又は漏洩の可能性がある場合は「社内緊急連絡網」に従って連絡してください。

- 会社支給の携帯電話・スマホの紛失・盗難
  （個人携帯スマホも保存データ内容によって報告対象となる場合があります）
- 社員証・入館証の紛失・盗難（お客様の入館証を含む）
- メール / FAXの誤送信
- 郵便・宅配等の誤送付、誤封入
- 機器の紛失・盗難

自宅での行動について

自宅でのPC利用

- 業務データの持ち帰り自宅のPCで作業しないでください。
- ファイル交換ソフトは利用は推奨しません。
- ＰＣにはウイルス対策ソフトを必ず導入しウイルス定義ファイルを常に最新に保ってください。

おつかれさまでした

これで教育テキストは終了です。

コーヒーブレイクでもして一息いれてください。

次に教育理解度確認テストを受けてください。

確認テストに合格すると教育受講終了です。

※右下のボタンかメニュー画面より確認テストを受けることができます。