サルでもわかる ISMS

Think Funs inc.

ISMSってなに？？

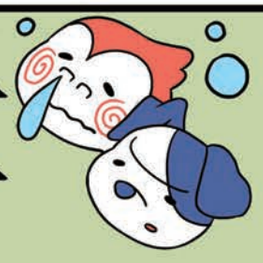
登場人物

ISMSとは？～CIAと情報セキュリティについて～

ポイント：ISMS活動では、「CIA」の確保が重要！

ISMSとは？

Information Security Management Systemの略称。
日本では、「情報セキュリティマネジメントシステム/ISO27001」として有名です。
ISMSは組織の情報管理の仕組みを整え、様々な脅威から情報を適切に守るための役割を担うシステムです。
ISMSでは、情報セキュリティを主に情報の
「機密性/Confidentiality」「完全性/Integrity」「可用性/Availability」
を確保することで適切に管理することと定義されています。
この3つの要素は、それぞれの頭文字から**「CIA」**と呼ばれています。
情報セキュリティでは、「CIA」をバランス良く運用することが重要です！



CIAとは？

情報セキュリティを実施する際に、**リスクを主に3つの側面から検討**します。
それを「CIA」と呼び、それらを必要に応じて確保できるようにします。

C：機密性/Confidentialityの確保

許可のある人だけが使用でき、
許可のない人は閲覧することが出来ない状態にしておくこと。
例）アクセス制御の実施、パスワード認証などの導入　等

I：完全性/Integrityの確保

情報が正確かつ最新な状態であること。
例）データの改ざん防止、検出を行う　等

A：可用性/Availabilityの確保

情報を必要な時に使用できる状態にしておくこと。
例）バックアップの実施、災害復旧計画の作成、
クラウド化による利便性向上　等

マネジメントシステムとは？

ポイント：周りの関係者すべての理解と協力が重要！

ISMSって、日本語で言うとすごく長いよね。
「情報セキュリティマネジメントシステム」って、
ことばにするだけで疲れちゃうよ･･･

「情報」も「セキュリティ」も聞いたことあるけど、
「マネジメントシステム」って何だ？？

ワン吉くん！良い質問だね！
次は「マネジメントシステム」について説明しよう！

マネジメントシステムとは？

マネジメント：組織に成果をあげさせるための道具･機能･機関のこと。
マネジメントシステム：組織の目標を 定め、**その目標を達成するための仕組み**のこと。

マネジメントシステムとは組織の目標を達成するために、
またセキュリティ対策のために、方針･マニュアル･ルール等を整備し、
実践、改善を行うことです。

ISMSの中には「マネジメントシステムの運用において、PDCAサイクルを
回して継続的改善を図りなさい」という考え方があります。
この考え方は、様々なマネジメントシステム規格に共通して要求されており、
マネジメントシステムの基本になります。
Plan(計画)→Do(実行)→Check(確認)→Action(改善)のサイクルを繰り返し、
継続的な改善を促す活動は、組織の品質･サービス向上と信頼度向上にも
つながります。

また、マネジメントシステムの活動は、組織内部のみで完結するものではありません。
関係するすべての人の理解と協力を得ることが大切です。

みんなで協力して活動することが大切なんだね！

2人とも重要な協力者の1人だよ！

情報資産とは？～情報資産の洗い出し～

ポイント：守るべき資産は「自らの事業に影響を及ぼす資産」

保有情報

- デジタルデータ
- 紙に記録された情報(書類や記録)
- スタッフの知識や情報

ソフトウェア資産

- 業務利用する様々なアプリケーション
- クラウドサービス
- webシステム

物理的資産

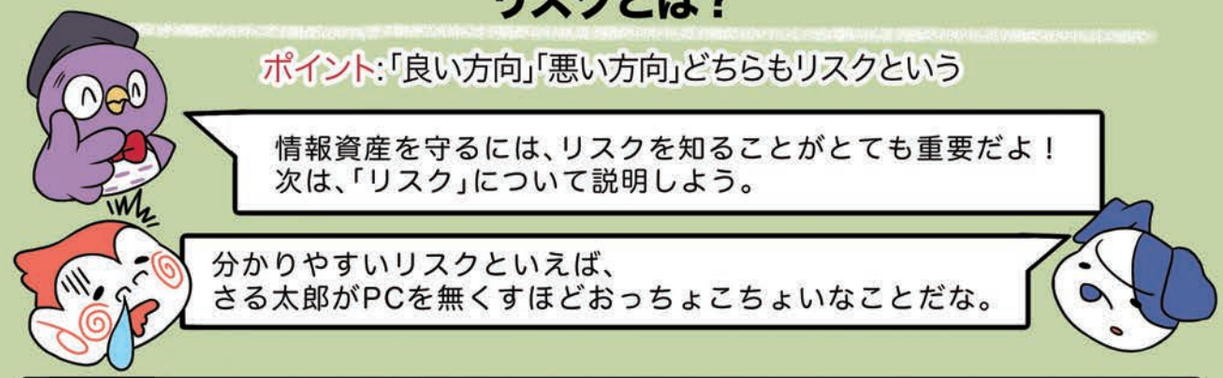
- PCやモバイル機器 サーバーなど ネットワーク機器
- 事業の為に必要な機器や設備
- オフィス

その他無形資産

- 企業ノウハウ(プロセス)
- 人財(人材) コミュニケーション
- 特許や営業機密情報

リスクとは？

ポイント：「良い方向」「悪い方向」どちらもリスクという



リスクとは？

目的に対する不確かさの影響のこと。
不確かさの影響とは、期待している事から離れることを指します。
「良い方向」「悪い方向」どちらも「リスク」と言います。
不確かさのすべてをコントロールすることは難しいのですが、
事業を進めていく上での悪い方向(脅威)については、
できるだけ前もって対策しておく必要があります。

例えば、さる太郎くんのPCが見つからなかった場合、こんなリスクがあります。

リスク

この他にも沢山のリスクが隠れています。
リスクや脅威を知る事で予防対策ができ、リスクを適切に管理することができます。

情報資産に対するリスクはたくさんあり、日々変化し続けています。
すべてを認識する事は難しいのですが、できるだけ適切にリスクを認識するために、
ISMS活動では「リスクアセスメント」を行います。

リスクアセスメントとは？

組織の情報資産に対する脅威と脆弱性を明確にし、リスクの大きさを評価し、
リスクが受容できるか否かを意思決定するプロセスのことです。

リスクをゼロにすることは出来ないんだ。
しかし、できるだけ安全な範囲(受容)にすることで安全を確保できるよ。
その時受容したリスクへの対策も変化に応じて実施する事が大切だよ！

機密情報とは？～守るべき資産　その1～

ポイント：機密情報(営業秘密情報)を適切に守り、活用することが重要！

守るべき資産の中には、**「機密情報(営業秘密情報)」**と呼ばれるものがあるんだ。

「機密情報(営業秘密情報)」ってなーにー？？

機密情報(営業秘密情報)とは？

技術上もしくは**営業上**で**価値のある情報**のこと。
紙、データ、口頭を問わず、個人情報も含みます。
機密情報(営業秘密情報)は、1度でも漏えいすれば価値を失い、
組織に致命的な悪影響を与えることもあります。

めちゃめちゃ怖い情報だな・・・・

機密情報(営業秘密情報)を怖がる必要はないんだよ。
逆に機密情報(営業秘密情報)を適切に取り扱うことができれば、**大きな強み**になるよ！

具体的には、こんなものが
機密情報(営業秘密情報)と呼ばれているよ。

個人情報・要配慮情報とは？～守るべき資産　その2～

ポイント：個人情報や要配慮個人情報は身近に存在している。

他にも守るべき資産として、
「個人情報」「要配慮個人情報」
があるよ！！

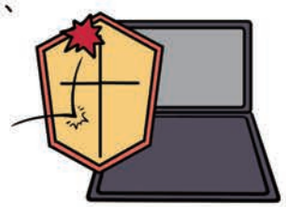
情報セキュリティ対策～情報セキュリティ5か条～

ポイント：情報セキュリティ5か条を参考にしてみよう！

1：OSやソフトウェアは常に最新の状態にしよう！

OSやソフトウェアを古いまま放置していると、
セキュリティ上の問題点が解決されず、
それを悪用したウイルスに感染してしまう危険性があります。
お使いのOSやソフトウェアには、**修正プログラムを適用する**、
もしくは**最新版を利用する**ようにしましょう。

2：ウイルス対策ソフトを導入しよう！



ID・パスワードを盗んだり、遠隔操作を行ったり、
ファイルを勝手に暗号化するウイルスが増えています。
ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は
常に最新の状態になるようにしましょう。

3：パスワードを強化しよう！

パスワードが推測や解析されたり、
ウェブサービスから流出したID・パスワードが悪用されたりすることで、
不正にログインされる被害が増えています。
パスワードは**「長く」、「複雑に」、「使い回さない」**ようにして強化しましょう。

4：共有設定を見直そう！

データ保管などのウェブサービスや
ネットワーク接続した複合機の設定を間違ったために、
無関係な人に情報を覗き見られるトラブルが増えています。
ウェブサービスや機器を**無関係な人が使えないような設定に
なっている**ことを確認しましょう。

5：脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付のメールを送ってきたり、
正規のウェブサイトに似せた偽サイトを立ち上げて
ID・パスワードを盗もうとする巧妙な手口が増えています。
脅威や攻撃の手口を知って対策を取りましょう。

情報セキュリティ5か条はIPA(独立行政法人情報推進機構)が作成した、実践的な内容のガイドラインです。
※「中小企業の情報セキュリティ対策ガイドライン　付録：情報セキュリティ5か条」を基に作成
SECURITY ACTION公式サイト：https://www.ipa.go.jp/security/security-action/about-sa/index.html

情報セキュリティ対策～自己点検チェックリスト～

ポイント：個人情報保護委員会の自己点検チェックリストを紹介！

個人情報の取扱いについては
個人情報保護委員会の、
『自己点検チェックリスト』を
参考にするといいよ！
右のQRコードから覗いてみよう！
https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf

個人情報取扱いの「ポイント」も
一緒に載ってるから分かりやすいね！

他にもいろいろな
対策方法があるよ！
参考にしてみてね！

初めての個人情報～シンプルレッスン～
https://www.ppc.go.jp/files/pdf/1711_simple_lesson.pdf
出典：個人情報保護委員会

上記のサイトは、主に中小企業を対象として作成されています。
是非、巻末のチェックリストを試してみてください。

中小企業の情報セキュリティ対策ガイドライン　第3版
https://www.ipa.go.jp/files/000055520.pdf

5分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/files/000055848.pdf
出典：独立行政法人情報処理推進機構セキュリティセンター

より具体的な対策を示すガイドラインと、自社診断項目です。

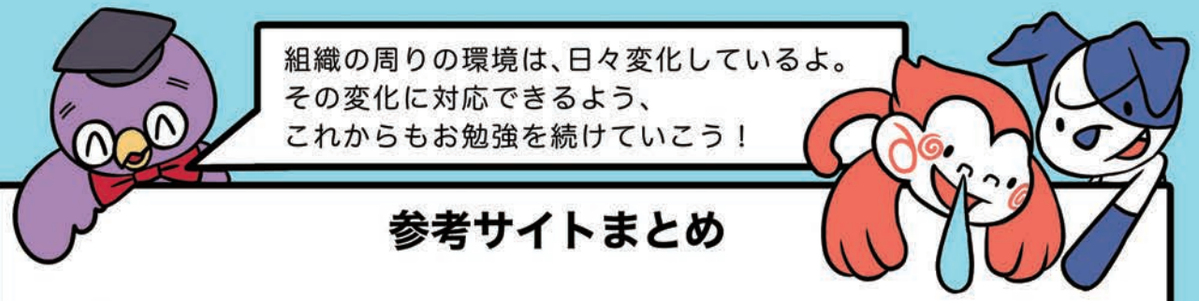
それじゃあ、今まで学んだ事を活かして
さる太郎くんが今後PCをなくさないための
対策を考えてみよう！

まとめ～対策を考えよう～

ポイント：対策は具体的に継続できることを考えよう！

情報セキュリティに関する事故や攻撃が発生してしまった場合、
速やかに適切な対応を行うことが重要です。

2022年4月施行の個人情報保護法より、
「個人情報取扱事業者は、個人情報の漏えい等の発生時は、
個人情報保護委員会に報告し、本人に通知すること義務を負う
（個人情報保護法22条の2）」こととなります。
※一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。
事故発生時に冷静な対応を実施できるよう、
事前に個人情報保護法を確認しておくことも大切です。
対応フローを定め、全体で共有し、訓練しておきましょう。



参考サイトまとめ

■ISMS適合性評価制度
一般社団法人情報セキュリティマネジメントシステム認定センター（ISMS-AC）
https://isms.jp/index.html

■JNSA　特定非利営利活動法人　日本ネットワークセキュリティ協会
https://www.jnsa.org/

■個人情報保護委員会
https://www.ppc.go.jp/

■CDNS　eラーニング講座
https://www.cdns.co.jp/e-learning/sample/s5.pdf

■経済産業省/秘密情報のハンドブック～企業価値向上に向けて～
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

■個人情報保護委員会ウェブサイト「はじめての個人情報保護法～シンプルレッスン～」
https://www.ppc.go.jp/files/pdf/1711_simple_lesson.pdf

■IPAセキュリティセンター　SECURITY ACTION公式サイト
https://www.ipa.go.jp/security/security-action/about-sa/index.html

■独立行政法人情報処理推進機構セキュリティセンター
中小企業の情報セキュリティ対策ガイドライン　第3版
https://www.ipa.go.jp/files/000055520.pdf

■独立行政法人情報処理推進機構セキュリティセンター
5分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/files/000055848.pdf

■個人情報保護委員会　自己点検チェックリスト
https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf

■個人情報保護委員会　漏えい等の対応（個人情報）
https://www.ppc.go.jp/personalinfo/legal/leakAction/

■IPA　独立行政法人情報推進機構　情報セキュリティ10大脅威　2021年
https://www.ipa.go.jp/security/vuln/10threats2021.html

毎年更新されています。現状の脅威を知るためにご活用ください。

QRコードはこちら！

こちらの参考サイトは、
シンク・ファンズ株式会社の
WEBページにもまとめています。

シンク・ファンズ株式会社のISMSに対する取り組み

“私たちは・・・
価値あるサービスの提供を関連企業と共に目指したい!!”

シンク・ファンズ株式会社は、2020年度より
「情報セキュリティマネジメントシステム
(ISMS/ Information Security Management System」に
取り組んでおります。

承認証明書

2021年4月11日付けで、ISMSの第三者認証基準
である国際規格「ISO/IEC 27001:2013」及び
国内規格「ISO/JIS Q 27001:2014」を取得いたしました。
弊社は、情報セキュリティ基本方針を全社員が認識し、
情報セキュリティマネジメントの継続的な運用・改善・向上に
努め組織の信頼をより一層高めることが出るように取り組んで
まいります。

情報通信技術の発展によって、情報の利用・活用を取り巻くリスクと脅威は、
急激に大きく変化しており、様々な脅威が私達の仕事や生活に大きな影響を
与え続けています。しかし、変化は「機会」を生みます。
「機会」に「強み」を投下する事でビジネスを優位に導くことが出来ます。

ISMS(情報セキュリティマネジメントシステム)は、情報リスクをテーマにした
グローバルなマネジメント(仕組み)です。
情報の利活用を考える時、同時にその「リスク」を考えて対応しなければ
なりません。
個人情報に限らず組織のビジネスプロセスを取り巻く様々な脅威・不確実性に
対して取り組む必要があります。
弊社では、情報セキュリティの個別の問題毎の技術対策に対して、
組織のマネジメントとして、リスクアセスメントを行い、
必要なセキュリティレベルを決め、プランを持ち、資源配分して
システム運用しています。

私たちは、価値あるサービスの提供を関連企業と共に目指したい！！
その為に、ISMSの活動に対する皆様の理解と協力を得ることが
重要だと考えています。
皆様の理解と協力を得るきっかけとして、2021年度より本誌の作成、
公式Facebookページの運営、御取引先アンケートの実施を
行っております。公式Facebookページでは、弊社のISMS活動情報を
詳しく発信しております。
QRコードを掲載しておりますので、是非ご覧ください。

Facebook
QRコード

本誌をきっかけに、少しでもISMS(情報セキュリティマネジメントシステム)の
活動に興味を持って頂ければ幸いです。

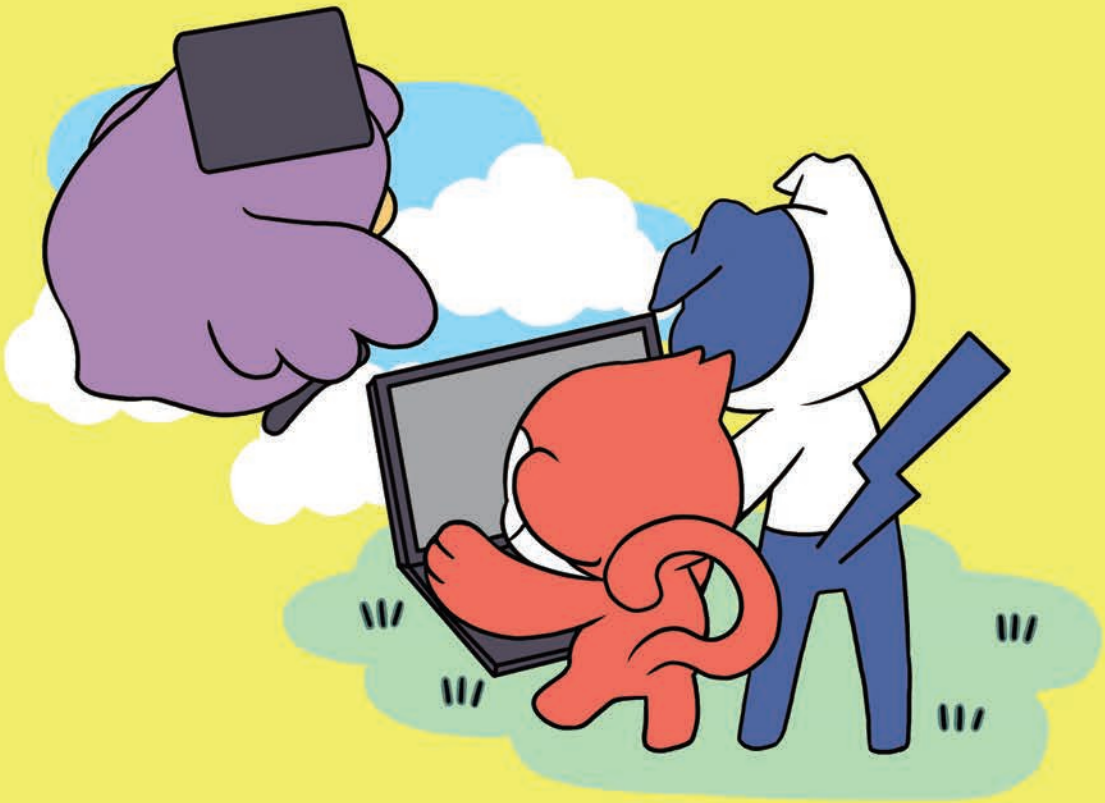
シンク・ファンズ株式会社の考え

90%の面白いって大切な事なのです

我々の仕事は、イベントのプロフェッショナルとして、
よく考え適切な落としどころを睨んだ上で全体のバランスを取って
最大限の効果が出る施策を構築する事なのですが・・・
イベントとは言え、決して派手な事ではなく、
地味な作業の繰り返しなのが実情なのです。
そのイベント業務の割合の90%が事前の準備であり、
残りの10%が実施本番と言っても過言ではなく、
そこでは何か問題が必ず起こるものなのです。
その事前の準備でどれだけしっかりと地味な作業をきちんとやっておくかで、
作品(イベント)の仕上がりが左右され、起こりうる問題に対して
スムーズな対策が講じられるかどうか?と、言う事になるのです。
全体の90%が地味な作業と言う事ですから決して面白いものではありません。
面白くないものは、辛いものなのです。
しかしながら、残り10%のイベント実施時のお客さまの楽しそうな笑顔、
驚き、ワクワク感など、高品質なイベント内容をしっかりと
創造しながら行うからこそ、その90%の地味な作業が面白くなるものなのです。

**我々Think Funs inc.は、
10%のために90%を面白くして
よく考える仕事スタイルです。**

シンク・ファンズ株式会社
代表取締役　加藤 裕紀



2021年10月1日　初版1刷 発行

＜奥付＞
発行：シンク・ファンズ株式会社
発行人：加藤 裕紀
編集担当：福川 理紗、太田 真由子
監修：株式会社コミュニケーションデザインネットワークス　米倉 高次
デザイン、イラスト：上田 紗綾
印刷・製本：中和印刷紙器株式会社

この冊子に関する各種お問い合わせ
シンク・ファンズ株式会社 Think Funs inc.
〒530-0041 大阪市北区天神橋2丁目5番28号
千代田第二ビル 6F
Mail：isms-info@thinkfuns.com　コミュニケーション担当まで
https://www.thinkfuns.com/

IS 744215 / ISO 27001