ISO/IEC27001
情報セキュリティ
マネジメントシステムの
必要性

ARM Standard Co., Ltd.

はじめに

情報セキュリティ対策の実施には、情報セキュリティに対する知識とそれに対応する仕組みを作ることが大切です。

そのためには、企業としての基本方針の策定や、適切な投資が必要であり、経営層の意志決定が必要です。

経営層が、自社にはどのような**情報資産**があり、どのようなリスクがあるかを把握した上で、自ら率先して情報セキュリティ対策の指揮をとることで効果的な情報セキュリティ対策ができます。

上記を実現するためには、 ISO/IEC27001を利用し、情報セキュリティに関するマネジメントシステム（**I**nformation **S**ecurity **M**anagement **S**ystem⇒略称：**ISMS**）を運用・維持することが有効です。

1 こんなことはありませんか？

最近、情報漏えいや不正アクセスのニュースが多く、社内に情報セキュリティに詳しい人を養成する必要があると感じている。

取引の際に秘密保持契約の締結が増え、事故発生時の損害賠償責任まで規定されている為対応しなくてはならない。

官公庁の入札要件や取引先の委託要件に「ISMS認証取得」とある。

2 社会的要求が高まっています

- ＩＴに支えられた現代社会。セキュリティ事故、不正、システム障害がビジネスに及ぼす影響は、想像をはるかに超えてしまいます。
- ニュースになる事故は一部に過ぎず、実際には身近で多発しています。

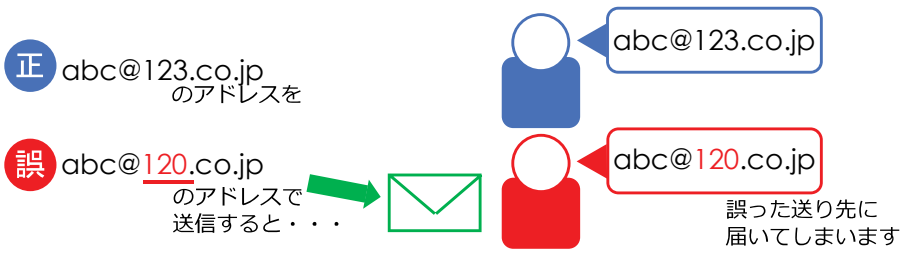
情報被害の例

- パソコンの起動に時間がかかるようになった、または起動できなくなった
- システムの動作速度が遅くなった、または途中で動かなくなった
- 画面上に奇妙なメッセージが表示された、または音楽が流れた
- 突然データが消えた
- 身に覚えのないメールを送信している
- ネットワークトラフィックが異常に高くなっている

当社では…

宛先指定ミスによる情報漏えい

指定したメールアドレスが、想定した相手のものとは違っていても、アドレスそのものが実在する場合、そのアドレスを所有している第三者にメールが届きます。



- 関係のない第三者にメールの内容を知られる
- 企業の機密情報がメールに記載されていた場合、機密情報が漏えいする
- 本文の内容によっては、本来の宛先となる人（お客様や取引先企業など）の個人情報が漏えいする

当社では…

情報セキュリティ事故が与える企業への影響

直接的被害

・業務の停止

ネットワークの停止、メール送受信の停止、Webページの閉鎖

・情報の紛失・改ざん・漏えい

営業活動の停滞・中断、関係先への連絡・お詫び、情報拡散防止対策

・対策費用の増大

情報の回復・保護費用、事故の原因究明・対策費用、情報システムの原状回復費用、改善費用 、情報拡散防止対策費用、見舞金・謝罪費

当社では…

間接的被害

・損害賠償

漏えいした情報の持ち主、二次被害を与えた他者への損害賠償

・公的な処罰

事業免許の取り消し・停止、行政指導による業務停止等

・社会的信用の低下

社会的信用の喪失、ブランドイメージの毀損、風評の悪化、株価下落

・売上の減少

顧客からの取引縮小・停止、営業機会の損失、マーケットシェア低下

・社内の業務効率・モラルの低下

対策に伴う業務効率の低下・過重労働、従業員の不安・不満、モラル低下

当社では…

二次的な被害

①漏えいした個人情報で、情報主体（個人情報の本人）に被害がおよぶ
※プライバシー侵害、秘密の曝露など

②マルウェアに感染したメールなどを送信してしまい、顧客企業のネットワークに感染を広げてしまう

③サーバが踏み台になり、迷惑メールなどの不正中継を許してしまう

当社では…

④パソコンがボットネット*1に組み込まれ、DoS攻撃*2の一翼を担ってしまう

*1 ボットネット

ウイルスなどによって多くのパソコンやサーバに遠隔操作できる攻撃用プログラム(**ボット**)を送り込み、外部からの指令で一斉に攻撃を行わせるネットワークのこと。
攻撃を指令するサーバと有害プログラムに感染したコンピュータ(**ゾンビマシン**)群から構成され、攻撃指令は主としてIRCプロトコルで送信される。

*2 DoS攻撃

通信ネットワークを通じてコンピュータや通信機器などに行われる攻撃手法の一つで、大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むこと。

当社では…

3 ISMSの構築・運用のメリット

対外的

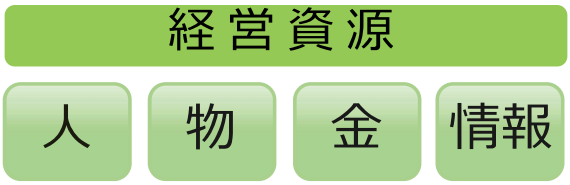
・お客さま、取引先等へ情報の安全性、信頼性をアピール
・同業他社との差別化（競争力の増大）

内的

・情報セキュリティの強化
・情報セキュリティ事故の減少
・社員の意識改革
・自社の**情報資産**の整理

情報資産とは

ISMSの構築の際に基礎となる考え方の一つです。
企業活動の過程で生み出される価値あるもの全てのことです。商品や不動産など、目に見えるもの（有形資産）もあれば、財務情報、人事情報、顧客情報、技術情報など、目に見えないもの（無形資産）もあります。
これらの保護・管理の方法を考えることがISMS運用は必要です。



情報は
人、物、金につぐ
第４の資産

情報資産の種類

情報そのものの資産
・データベースやデータファイル
・ユーザマニュアル

人
・社員／契約社員／第三者常駐者
・顧客

文 書
・契約書、社内文書

サービス(外部より受ける)
・通信サービス
・サーバ運用管理サービス

ソフトウェア資産
・アプリケーション・ソフトウェア
・開発ツールとユーティリティ

サービス(企業イメージ・評判)
・高い技術
・迅速、的確なサービス

ハードウェア資産
・コンピュータ、通信機器
・メディア（USBメモリ／DVD/CD等）

当社では…

情報資産の価値

情報資産の価値を決める３つの要素があります。

1. 機密性(confidentiality)
   情報資産を正当な権利を持っている人だけが利用できる状態にしておくことです。

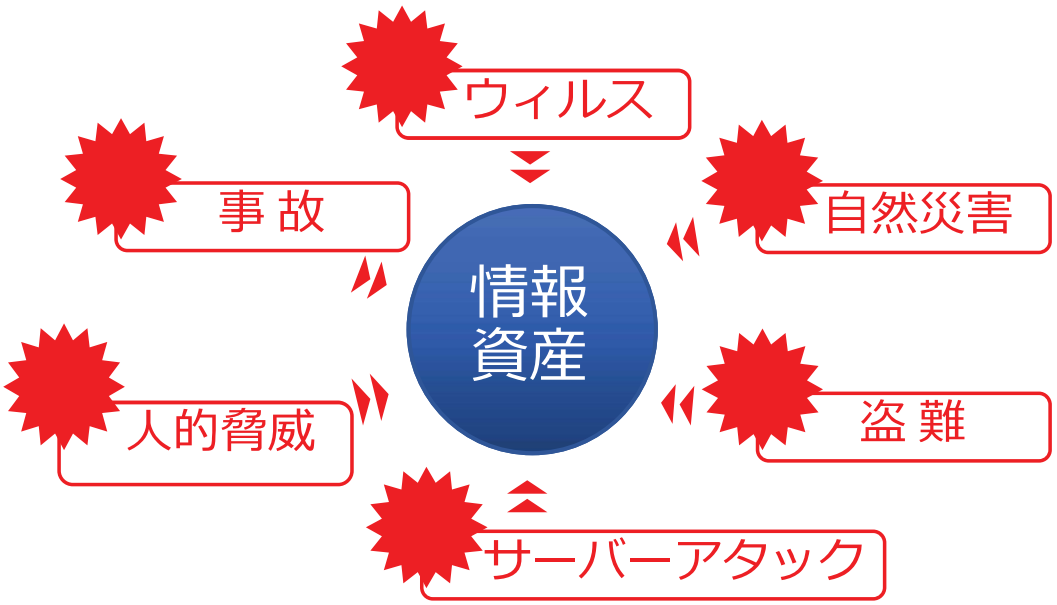
2. 完全性(integrity)
   情報資産が正確かつ最新の状態で管理することです。

3. 可用性(availability)
   情報資産を使いたいときにすぐに使える状態にしておくことです。

当社では…

情報資産の危険性

「機密性」、「完全性」、「可用性」を脅かすもの



当社では…

マルウェア(Malware)

マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称です。

当社では…

ウイルス

他のプログラムに寄生して、そのプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、感染機能や自己拡散機能を持つ

ワーム

独立のファイルで、他のプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、感染機能や自己拡散機能を持つ

トロイの木馬

ユーザの意図に反し、攻撃者の意図する動作を侵入先のコンピュータで秘密裏に行うプログラム

スパイウエア

感染したパソコンの内部情報を外部に勝手に送信する

キーロガー

ユーザのキーボード操作をそのまま外部に送信する
スパイウェアの一種

バックドア

攻撃者が侵入するためのネットワーク上の裏口を開ける

ポット

攻撃者からの指令により、他のコンピュータやネットワークへの攻撃や、サーバからのファイルの盗み出しなど有害な動作を行うプログラム

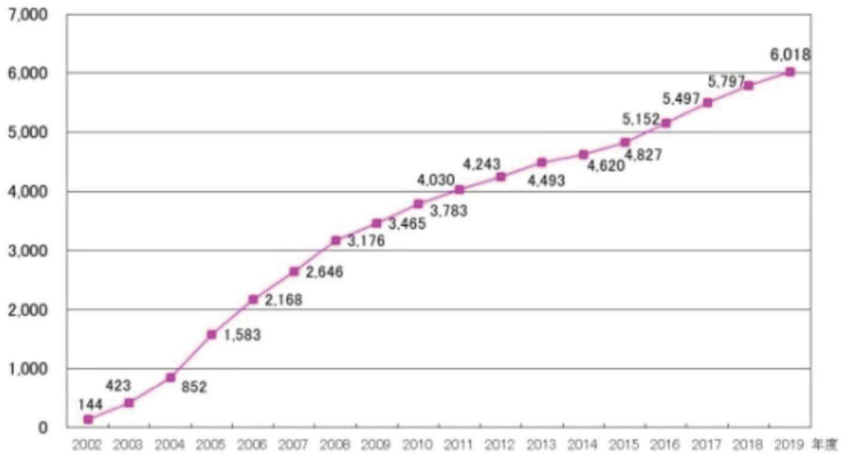
当社では…

4 ISMSは情報セキュリティの国際基準です

ISMSは国際規格であるISO/IEC27001を基準として、組織の情報セキュリティへの取り組みを認証機関が審査し、認証する制度です。
国内では2002年から運用が始まり、情報セキュリティに対する社会的要求の高まりを背景に、既に行政機関や民間企業約6,000事業者が認証を取得している情報セキュリティの国際基準です。

ISMS
認証取得
組織数
推移

一般社団法人
情報マネジメントシステム認定センター
ホームページから引用



※上記の数字は2019年11月11日現在

情報セキュリティマネジメントシステム（ISMS）とは？

Information Security Management System

情報資産 → 情報セキュリティ ← セキュリティ

情報を管理するため、「機密性」「完全性」「可用性」を満たす

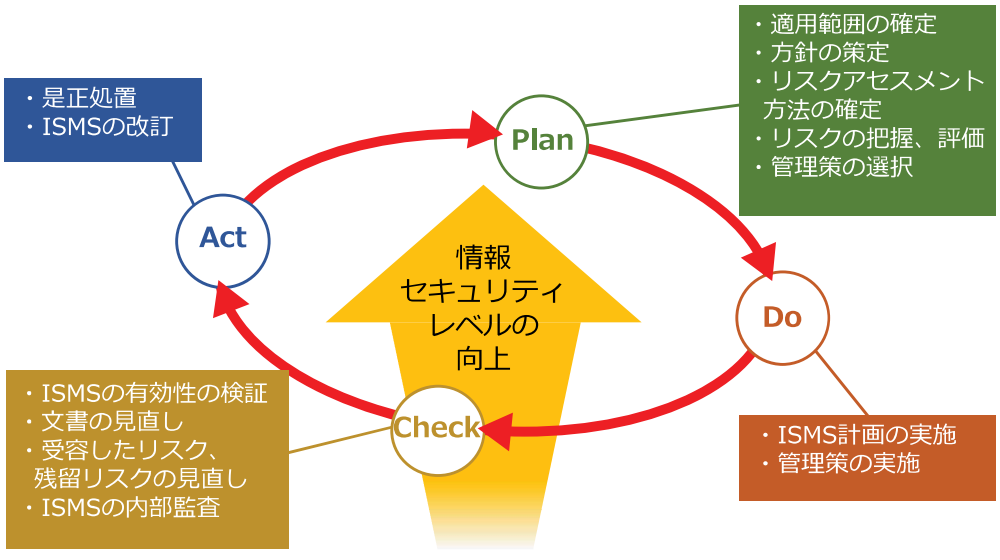
情報セキュリティマネジメントシステム

組織の規定を作り、それに基づいて組織全体で実践するプロセス

当社では…

PDCAによるマネジメントシステム

継続的という考え方がなければ、一時的なセキュリティ対策で終わってしまう



当社では…

5 ISMS認証を取得するには

組織のマネジメントシステム（ISMS）が情報セキュリティの国際規格であるISO/IEC27001に適合しているかについて、第三者である認証機関が審査を通じて評価します。
審査は定期的に行われるため、活動の継続性が保たれます。

6 ISMSよくある質問と答え

Q：取得するには、どのような費用がかかりますか？

A. 認証機関の審査・登録費用が必要です。企業規模にもよりますが、最近は小規模事業者の取得が増加していることもあり、認証機関によっては低額ながら質の高い審査を提供する機関もあります。この他に構築を外部の専門家に依頼したり、設備等を増強する場合は、別途費用が必要です。

Q：取得すると事業上のメリットになりますか？

A. 商取引の際には必ず情報の授受関係が発生します。特に昨今はインターネットを利用して取引事務の効率化を図ることが多いため、ISMS取得は競合他社との差別化になり、提案コンペの際等には有利になります。

Q：認証機関はどのように選定したらいいのですか？

A. 現在30の認証機関があります（ISMSーAC登録組織より21年10月現在）が、どの認証機関に申請するかは、受審を希望する組織で自由に決めることができます。審査費用も一律ではありませんので、各認証機関に見積提案を提出してもらい比較して条件に見合った機関を選定すると良いでしょう。

Q：ISMS認証は、難解な規格を理解し、リスク分析や文書作成、記録維持に膨大な作業が必要と聞いていますが、小規模企業でも取得できますか。

A. 認証機関によっては文書、記録に重点をおく形式的な審査ではなく、業務効率を阻害せず、規格本来の趣旨に沿った合理的な活動を評価する機関もありますので、過大な作業不可を懸念する必要はありません。

規格は、企業にとって必要なことのみを求めています。形式的に文書や記録を作り過大に作業負荷を増加させることがないよう、規格の趣旨、組織の状況に応じた審査を行う機関を選ぶことが重要です。

ARM Standard
アームスタンダード

最後に

アームスタンダード株式会社ではISO/IEC27001の審査業務、
並びにお客様がマネジメントシステムを自力で構築できるよう、
ITツールをご用意しております。
是非、同封の「WebMiCS体験セミナー」のチラシをご覧ください。

本書をご覧いただきありがとうございました。

MEMO

MEMO

アームスタンダード株式会社
〒103-0012　東京都中央区日本橋堀留町1-10-15
Ｊ Ｌ日本橋ビル1F
TEL:03-3666-8788（代表）／ 03-3666-8814（営業部）
FAX:03-3666-8752
HP ：https://www.armstandard.com/
E-mail：contact@armstandard.com