情報セキュリティマネジメントシステム

（ISMS: Information Security Management System）

社員教育テキスト

（初級編）

はじめに

このテキストでは**情報セキュリティマネジメントシステム（ISMS）**に則して

- 情報セキュリティ方針の内容
- ISMS への取組みの成果によって得られるメリット
- ISMS の要求事項などを守らなかった場合のデメリット
- 規程類に定められた手順
- ISMS への取組みの成果に対して自分がどのように貢献できるのか

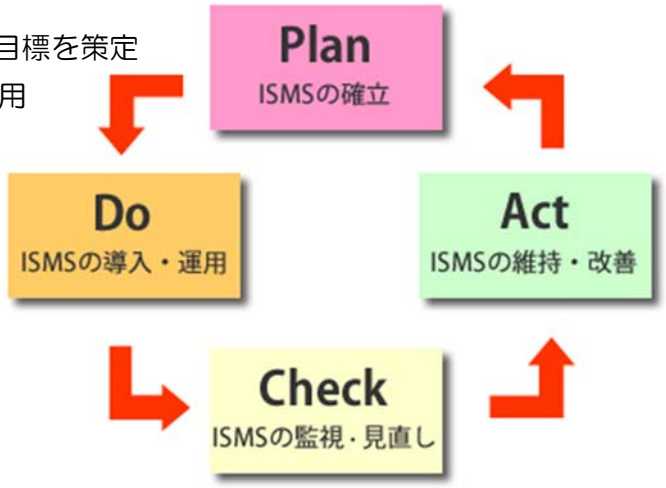
について学んでいきます。

情報セキュリティ（情報の安全を守ること）のために私たちができること、その第一歩は**情報セキュリティマネジメントシステム（ISMS）**のルールを守って日常業務を行うことではないでしょうか。このテキストでは ISMS に合わせて日常業務の手順を確認していきます。情報の安全を保ちながら業務を行う考え方と手順を身につけていきましょう。

まず、**情報セキュリティマネジメントシステム（ISMS）**とは何でしょう？
ＩＳＭＳ（あいえすえむえす）は「Information Security Management System」の頭文字を取ったものであり、わかりやすく言えば「**情報セキュリティを管理**（マネジメント）するための**仕組み**（システム）」です。
日本語では「**情報セキュリティマネジメントシステム**」として一般化しています。

情報セキュリティマネジメントシステムでは、情報を守るための基本的な考え方や進むべき方向を色々と考えて決定し、継続的に運用していきます。
この継続的に改善し運用していく手法は**ＰＤＣＡサイクル**として、仕事を進める際にいろいろな機会で使われます。ISMS での使い方は下記のとおりです。

Plan：情報セキュリティ対策の具体的な計画・目標を策定
Do：計画に基づいてさまざまな対策を実施・運用
Check：実施した結果を点検・監視
Act：経営陣による見直しを通して、
　　システムを改善



【論理的アクセス制御（通信のセキュリティ）】
●ネットワークやソフトウェアへのアクセスについて考えてみましょう。

利用者が勝手に未許可のネットワークに接続したり、ソフトウェアを利用したりすることは組織の情報資産を危険に晒すことになりかねません。
情報の漏えい（機密性）や、改ざん・誤りがない（完全性）ように業務を行うためには会社（組織）が示す**アクセス制御**に対する**方針（考え方）**に従って業務を行いましょう。

Wi-Fi を利用する場合は、会社（組織）で許可されたネットワークを選択しましょう。見知らぬ SSID や無料だからと安易に未許可のネットワークを利用すると通信内容を盗聴されたり情報を不正利用されたりする危険があります。

- 会社（組織）で Wi-Fi 利用のルールが決められている場合は確認しておきましょう。
  会社（組織）にルールが無く主体性に任されている場合は、もし Wi-Fi を利用する場合、安全に使用する方法を考えてみてください。

●資産利用の許容範囲について考えてみます。
この会社（組織）で働いているからといって全ての情報にアクセスして利用可能なわけではありません。
業務内容によって許可された情報や範囲があります。情報の漏えいや改ざん、必要なときに使える状態を保つために会社（組織）が決めた**アクセス制御**に対する**方針（考え方）**に従ってアクセスする情報を守りましょう。