Japan Information Security
Management Systems User Group

ISO/IEC27001と国内ガイドラインの違いと融合点の考察

日本ISMSユーザグループ　インプリメンテーション研究会

山口　宏治（富士ソフト株式会社）

Copyright (c) JNSA Japan ISMS User Group. 2025

Step0　契機

自己紹介

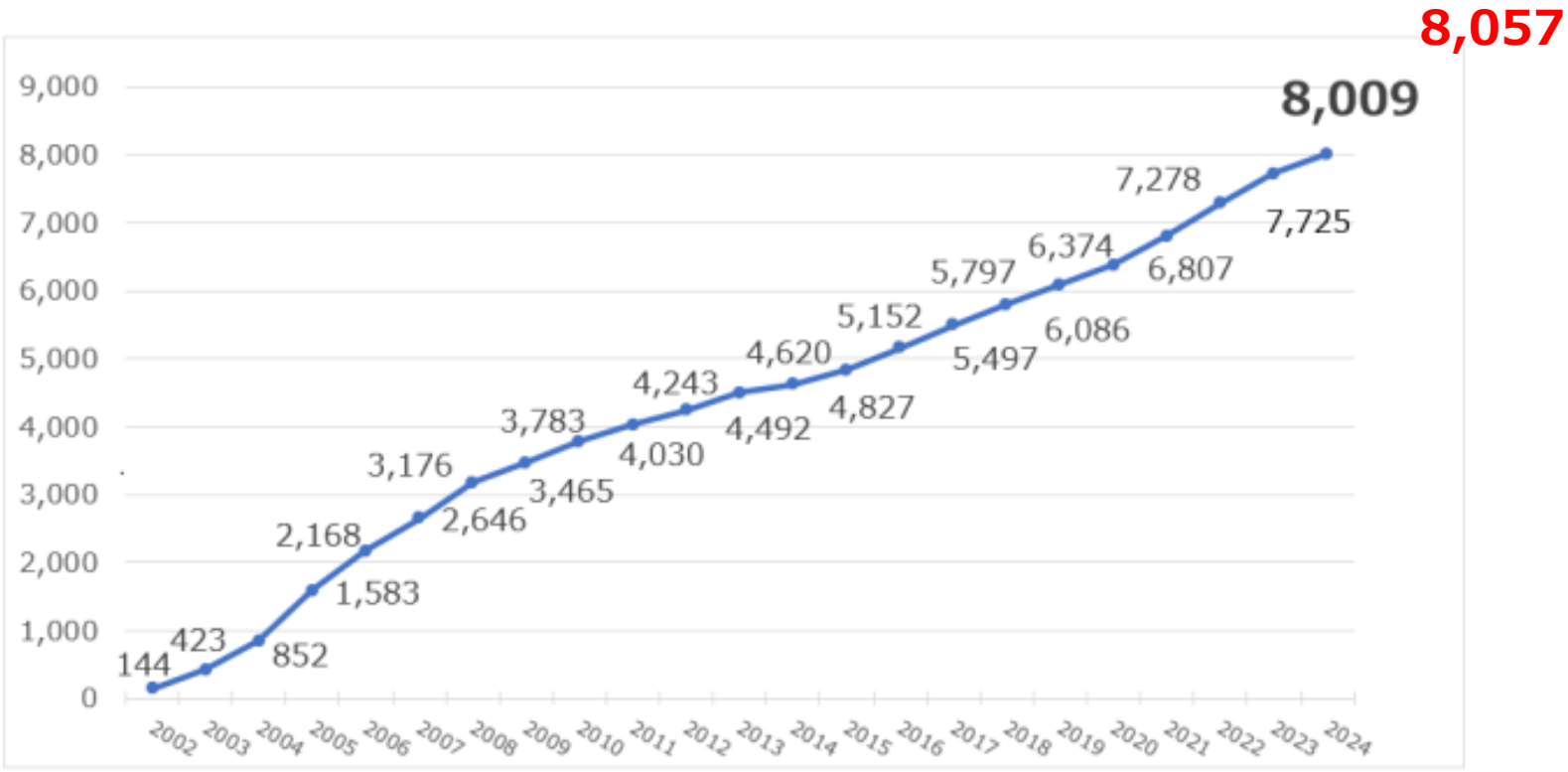
山口　宏治　1970年生まれ　熊本県出身
富士ソフト株式会社　主任（エキスパート）

JRCA認定　ISMS審査員補、ISMS-CLS

金融関連のシステム開発やPMO関連の業務を約25年ほど経験し、米国のグループ会社の監査を支援した事をきっかけに、セキュリティ関連に携わりました。
普段は、情報セキュリティの経験と知識をベースにお客様のセキュリティ対策支援や各種業界ガイドラインの詳解などを行う、情報セキュリティコンサルタントに従事しています。今回は貴重な時間を頂きましたので、多いにISMSを語りましょう。
また、情報セキュリティ対策でお困りごとがあれば、お気軽に相談ください。

Copyright (c) JNSA Japan ISMS User Group. 2025

ISMSの認証組織数の推移



出典：ISMS-ACニューストピックより

日本の企業総数は300万社以上あると
言われているので、まだまだ伸びしろはある。

Copyright (c) JNSA Japan ISMS User Group. 2025

ISMS認証（ISO27001）の取得のメリット

ISMS認証取得企業が伸びている背景として、メリットを挙げると主に以下の3点と言えるでしょう。
組織によって思惑は異なるので、これだけではない部分もありますが、セキュリティを準拠する組織として必要な事が組み込まれていると感じています。

- **情報セキュリティの信頼性の向上**
  - ・顧客に対して、「情報を適切に保護している組織」であることを客観的に証明できます。
  - ・サプライチェーンや入札要件において評価アップに繋がります。

- **リスク管理の強化**
  - ・情報資産に対する脅威や脆弱性を体系的に洗い出し、対策を講じることで、インシデントのリスク低減が行えます。
  - ・セキュリティ対策が、計画的かつ継続的に運用されるようになります。

- **業務の効率化と内部統制の向上**
  - ・情報の取扱いに関するルールや手順が標準化されることにより、業務の効率化がはかれます。
  - ・内部監査の実施やPDCAのサイクルと通じて、継続的な改善が組織に根付くきっかけになります。

Copyright (c) JNSA Japan ISMS User Group. 2025

ISMSを国際規格として認めている主な地域

ISO/IEC27001は、IAF（国際認定フォーラム）による相互承認制度のもと、各国の認定機関が認めた認証は、他国でも有効とされている、国際的に有効な規格です。

Copyright (c) JNSA Japan ISMS User Group. 2025

Step2　考察

自身の業務経験からの考察

背景

・お客様から取引条件におけるセキュリティガイドライン準拠の相談を幾つも受ける

気づき

・根底にある「共通の軸」が存在を感じ、多くのガイドラインに共通する考え方があると気づく

比較

・ガイドラインとISO/IEC27001の管理策を一覧化して比較してみると、類似事項が多い

まとめ

・改めて、ISMSとは新たなルールやフレームワークにも応用しやすい
・初見でも構造が見えやすく、新しいルールでも慌てずに対応することが出来る

つまり、ISMSを知っていると、様々なガイドラインを理解しやすいのではないか？

Copyright (c) JNSA Japan ISMS User Group. 2025

Step3　比較

日本における重要インフラの各種ガイドラインとの比較について

日本国内には各業界に様々なガイドラインが存在ます。その中でも、今回は重要インフラと言われる、15の分野のセキュリティガイドラインを対象に比較する事にしました。

分野	所管省庁	ガイドライン	関係機関等
金融	金融庁	金融分野におけるサイバーセキュリティに関するガイドライン	・サイバーセキュリティ関係省庁 （総務省、経済産業省等） ・事案対処省庁 （警察庁、防衛省等） ・防災関係府省庁 （内閣府、各省庁等） ・サイバーセキュリティ関係機関 （NICT、IPA、JPCERT/CC等） ・サイバー空間関連事業者 （サプライチェーン等に関わるベンダー等）
情報通信 **政府・行政サービス**	総務省	地方公共団体における情報セキュリティポリシーに関するガイドライン	
医療	厚生労働省	医療情報システムの安全管理に関するガイドライン	
電力 **ガス** **化学** **クレジット** **石油**	経済産業省	情報セキュリティ管理基準 サイバーセキュリティ経営ガイドライン	
航空 **空港** **鉄道** **水道** **物流** **港湾**	国土交通省	航空分野における情報セキュリティ確保に係る安全ガイドライン 空港分野における情報セキュリティ確保に係る安全ガイドライン 鉄道分野における情報セキュリティ確保に係る安全ガイドライン 水道分野における情報セキュリティガイドライン 自工会_部工会サイバーセキュリティガイドライン 港湾分野における情報セキュリティ確保に係る安全ガイドライン	

Copyright (c) JNSA Japan ISMS User Group. 2025

Step3　比較

整合点と独自ポイントについて 「情報セキュリティ管理基準」

＜整合点＞

	ISO/IEC27001	情報セキュリティ管理基準
全体的マネジメント	要求事項にPDCAプロセスを明示	ISQ27001と整合し、監査や管理の観点を準拠
管理策のカテゴリ	4カテゴリ93管理策	132コントロール（952サブコントロール）
リスクマネジメント	附属書Aでリスク対応の管理策選定	ISO基準に準拠し詳細サブコントロールを提供
物理的・技術的セキュリティ	物理・技術分類の管理策を含む	ISOと同等項目多数（技術面ではより詳細要件あり）

＜独自ポイント＞

情報セキュリティ管理基準
●詳細サブコントロールの定義 952のサブコントロールで細かい実践レベルを規定 **●国内制度への適応** 日本の法律や慣行を反映し、報告義務等に関する要件も含む

Copyright (c) JNSA Japan ISMS User Group. 2025

Step3　比較

整合点と独自ポイントについて 「医療情報システムの安全管理に関するガイドライン」

＜整合点＞

	ISO/IEC27001	医療ガイドライン
情報セキュリティの3要素	機密性・完全性・可用性を重視	機密性・完全性・可用性を中心に構成（基本的な目的は共通）
リスクマネジメント	リスクアセスメント・リスク対応が中心	リスク分析・評価・対応策の明確化（リスクベースのアプローチ）
管理策	4カテゴリ93管理策	技術的・物理的・組織的管理策や運用管理（共通点が多い）
教育・訓練	情報セキュリティ教育が必須	医療従事者、職員への教育や訓練が義務化
アクセス制御	ユーザアクセス、特権管理認証等定義	電子カルテ等のアクセス制御やID管理を明記
インシデント管理	インシデントへの対応体制構築	医療情報の漏洩への対応手順や体制を明記
継続的改善	PDCA適用	情報セキュリティの継続的改善を推奨

＜独自ポイント＞

医療ガイドライン

- **医療業界に特化**
  医療機関・診療所・クラウド事業者等立場ごとに義務を定義
- **国内法との連携**
  個人情報保護、医療法、マイナンバー法、サイバーセキュリティ基本法等と密接に連携
- **クラウド事業者への要求が明確**
  医療情報を取り扱うクラウド事業者への具体的な順守事項が必要

Copyright (c) JNSA Japan ISMS User Group. 2025

Step3　比較

整合点と独自ポイントについて 「港湾分野における情報セキュリティ確保に係る安全ガイドライン」

＜整合点＞

	ISO/IEC27001	港湾分野のガイドライン
経営とガバナンス	機密性・完全性・可用性を重視	重要インフラとしての任務保証を踏まえ、経営層との関与と自己検証
管理策の体系	組織的・人的。物理的・技術的管理策	国内外のベストプラクティスを参照し、同趣旨の管理策群を要求
評価と見直し	適用状況の評価、内部監査、教育訓練やインシデント対応、事業継続の枠組み	内部監査や自己点検による評価とインシデントの対応・復旧等、ISMSと同様の枠組みを要求

＜独自ポイント＞

港湾分野における情報セキュリティ確保に係る安全ガイドライン

- **港湾固有の役割分担を明文化**
  導入編、経営者層編、セキュリティ責任者編、システム構築・運用者編、港湾管理者等編に分冊
  事業者だけでなく、港湾管理者や港湾運営会社が有事にとる対応を具体化
- **TOS（Terminal Operating System）を中核資産として特記**
  コンテナターミナルのTOS停止が港湾機能全体に与える影響を踏まえ、TOSを前提とした対策を強調
- **制度との紐づけ**
  2024年に港湾分野が重要インフラに追加ことにより、制度面の要求が具体化
- **国内基準群との接続**
  NISCや政府統一基準群、個人情報ガイドライン、情報セキュリティガイドライン等を明示的に参照し、港湾分野に落とし込む構成

Copyright (c) JNSA Japan ISMS User Group. 2025

海外のガイドライン

組織によっては国内のみならず、海外企業との取引が行われているところもあるかと思われます。
サプライチェーンによるインシデントの発生がビジネス継続に大きな影響をもたらす事もあるので、
調達におけるガイドラインは今後も益々厳しくなっていくと考えられます。

Copyright (c) JNSA Japan ISMS User Group. 2025

国際規格と調達基準のガイドラインについて

調達基準の1つの例として、NIST SP800について解説しつつ、ISO/IEC27001との比較をしてみます。NIST SP800シリーズの中でもSP800-171は、米国政府に納入する調達品等に採用されます。日本の企業はこのSP800-171が適用される事が多いかと思われますので、こちらと比較します。

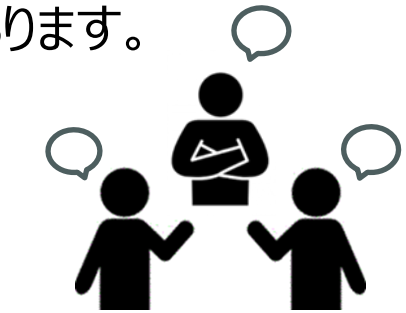
	ISO/IEC27001	NIST SP800-171
種類	国際規格（マネジメント認証）	ガイドライン、推奨事項 (米国連邦政府向けが主)
目的	ISMSの確立・運用・継続的改善、外部への証明	情報システムセキュリティの具体的な実装・運用ガイダンス
アプローチ	リスクベース、フレームワーク、PDCAサイクル	実践的、詳細、特定の技術や脅威への対応
認証	認証取得が可能 (第三者機関による監査)	基本的に認証制度はない (政府機関の評価基準として利用)
柔軟性	組織の状況に応じた柔軟な適用が可能	詳細な要件が多く、比較的厳格な適用が求められる
適用範囲	世界中のあらゆる組織	米国連邦政府機関へ納品する全ての組織

Copyright (c) JNSA Japan ISMS User Group. 2025

Step5　議論

議論テーマ

比較してみて多くの類似点があることが分かり、ISMSを知っているとガイドラインの管理策の理解はしやすいと感じています。但し、ISMSとガイドラインには決定的な違いがあります。



- **目的と範囲の違い（ISMSの仕組み規格と実務的なセキュリティ要求）**
  ⇒『内部統制の強化及び信頼性の証明』と『調達や入札における要求事項』
- 要求の抽象度の差（リスクベースと具体的対策）
- 認証の有無（第三者審査ありとなし）

	メリット	デメリット
ISO/IEC27001	第三者認証による信頼性を得る 組織のセキュリティ体制を強化	取得や維持にコストとリソースがかかる 中小企業には運用負担が大きい
セキュリティガイドライン	取引先等の実務的な最低限を満たせる 自社の規模やリスクに合わせられる	第三者認証ではないので、証明力は弱い ガイドライン毎の対応が必要になる

日本の企業にとってISMS認証取得とガイドラインの遵守のどちらが実務的かという考えは有益か？

短期的にはガイドライン準拠が実務的ではありますが、セキュリティは継続的に対応するものです。
セキュリティ対策の取組みをきっかけにISMS認証の取得を検討してみては如何でしょうか？

Copyright (c) JNSA Japan ISMS User Group. 2025

ご清聴有難う御座いました。

Special Thanks !

以下の本を比較時の参考にさせて頂きました。

Copyright (c) JNSA Japan ISMS User Group. 2025