ISO 審査機関からみた国立大学法人の ISMS

The progress and problem of The ISMS of National University Corporations through the position of ISMS certification body

山本富夫†
Yamamoto Tomio†
Yamamoto.tm@jaco.co.jp
†株式会社日本環境認証機構
† Japan Audit and Certification Organization (JACO)

概要

大学での ISMS は情報基盤センターなどの IT 運営分野では ISMS と ITSMS の統合導入など新しい動きが進んできているが、大学全体では内部統制分野など企業ほどには進んでいない．本当に重要な情報（産学連携における営業機密、ナーバスな個人情報）を保護するための厳格なセキュリティ文化、体制、手続きなどが不十分な状況にある．本稿ではこのような現状の課題と解決のための方向性（ISMS の深堀と横展開，安心安全社会実現の基礎としての ISMS，システムアシュアランス）を提示する．最後に弊社が提供する大学向けカスタムテイラード監査パッケージサービスについて紹介する．

キーワード

ISMS, 内部統制，営業機密，ナーバスな個人情報，安心安全社会，システムアシュアランス，カスタムテイラード監査サービス，統合マネジメント

1. 大学での ISMS の整備進展状況と課題

大学での ISMS は情報基盤センターなどの IT 運営分野では ISMS と ITSMS の統合導入など進んできているが、大学全体では内部統制分野など企業ほどには進んでいない分野もある．全学規模で e ラーニング受講などにより一般的な情報セキュリティ意識は高まってきている．しかし，情報公開を伝統としてきた大学自治の伝統、歴史の浅い産学連携の状況などの理由により、産学連携における営業機密、医療情報などナーバスな個人情報を保護するための厳格な文化、体制、手続きなどがまだ先鋭的な企業に比べると不十分である．

2. 大学での ISMS の課題解決の方向性

ISMS の対象は全ての業務の土台である情報である。ISMS は、この情報を機密性，完全性，可用性というトータルな視点でリスクアセスメントを行い，対策，点検，アクションするマネジメントシステムである。このため、ISMS は組織の内部統制の土台として活用できる．

また，ISMS は ISO のマネジメントシステムの中では唯一人間の悪意（意図的な不正）を想定している規格である．このため，ISMS を運用するには人間性に対する深い認識，組織文化に対する省察などが必要である．

本稿はこの ISMS の本質に立脚し，大学での課題を具体的に取り上げ，その解決の方向性を示す．一つは ISMS の深堀であり，情報の機密性，完全性，可用性の 3 つの側面を取り扱うマネジメントシステムであることを最大限に生かすことである．二つは ISMS の横展開であり, ISMS を土台にして品質管理，IT サービス管理，事業継続管理など ISMS に隣接するマネジメント分野との統合を目指すことである．

① ISMS の深堀

- 機密性：産学連携での営業機密（共同研究成果など）、大学病院での患者情報、カルテ情報などの重要な情報の戦略的

な保護と安全文化の確立

- 完全性：研究費の不正使用、論文の盗用、データの改ざんなどを防止するための研究業務自体とその管理業務への情報セキュリティの組込み
- 可用性：大学内情報インフラの機密性、サービスのトータルパフォーマンスの向上

② ISMS の横展開

- ISMS を大学情報インフラの品質管理の土台とする．
- ISMS を土台に品質管理 QMS（ISO9001），IT サービス管理 ITSMS，事業継続管理 BCMS（ISO22301）を統合的に構築する．
- ISMS の土台の上に乗せる各分野のマネジメントシステム要求事項を出来る限り ISMS に統合して軽くする．
- 統合マネジメントシステムの整備を行い，カスタムテイラード監査サービスを活用する

3. 安心安全社会の実現の土台としての ISMS

ISMS は単なる情報漏えい対策として見られることが多いが，機密性，完全性，可用性という情報の本質に根ざしたマネジメントシステムであるため，全てのマネジメント分野にとって必須のものであり，土台である．

例えば，IT によって高度にシステム制御された半導体製造プロセスは半導体製造機器へインプットされる情報が誤っていると良品はできない．

また，私たちの社会インフラの電子化（情報化，ソフト化）が進んでいる．このため，その安全性を情報セキュリティが担うようになってきている．このため，社会インフラも情報セキュリティリスクへの対策が必要である．

これから発展するスマートグリッド，スマートシティも広域で複雑な巨大システムであるが，原子力発電所のような専門オペレータに依存できない宿命にある．このような巨大システムの安心・安全を確保するためには情報セキュリティが大きな要素となる．社会の安心・安全は情報セキュリティによって維持されている．

福島原発は国民の安全・安心にとって大きな脅威を与え続けている．私たちは ISMS を安全・安心社会の土台として活用してゆく必要がある．

ISMS の延長線上に上記課題を解決するためのシステムの安全性アシュアランスサービス（システムアシュアランスサービス）がある．

4. ISMS を軸とした JACO が提供する大学向けサービス

最後に ISMS を軸とした JACO が提供するサービスを紹介する．

従来は ISO 審査認証機関である JACO は ISO 認証基準に基づく審査認証サービスに絞ってきたが，お客様の状況として事業環境が厳しくなり，より具体的に経営に貢献するサービスが望まれるようになってきた．

このため，ISO27001 に基づく審査だけではなく，例えば，医療関係組織向けに，ISMS に加え，医療個人情報のためのガイドである「ISO 27799 - 健康情報の情報セキュリティ管理」の要求事項を追加した審査サービスも行っている．これが ISMS に医療分野での要求事項を追加した「ISMS 医療オプション審査サービス」である．

また，ISMS 認証（登録証と認証の外部公開）に価値を求めるのではなく，自らのために内部統制と経営改善を狙うお客様にはカスタムテイラード監査サービスがある．例えば，「ISO 27799 - 健康情報の情報セキュリティ管理」にさらに独自の厳格な要求を付加した独自基準にもとづく組織診断サービスがカスタムテイラード監査サービスの一つである．

カスタムテイラード監査は，監査基準を JACO とお客様が共同作業でテイラリングを行い，その基準をお客様の組織員に教育，トレーニングすることと，その基準がどこまで組織に浸透しているかを監査により確かめる総合的なサービスである．

大学向けサービスとしては次のカスタムテイラード監査サービスが用意されている．ISMS にオプシ

ョンとして組み合わせることも，単独で自己改善のためのカスタムテイラード監査として行うこともできる．また，教育，トレーニング，監査の総合的なパッケージサービスとして利用することもお勧めである．

- 経産省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」によるカスタムテイラード監査サービス
- JISQ150001「個人情報保護マネジメントシステム-要求事項」によるカスタムテイラード監査サービス
- ISO22301（BS25999）「事業継続マネジメントシステム要求事項」によるカスタムテイラード監査サービス
- 経産省「IT サービス継続性ガイドライン」によるカスタムテイラード監査サービス

参考文献

1. JIS Q 27001: 2006「情報セキュリティマネジメントシステム-要求事項」.
2. JISQ150001「個人情報保護マネジメントシステム-要求事項」.
3. ISO22301（BS25999）「事業継続マネジメントシステム要求事項」
4. 経産省「IT サービス継続性ガイドライン」（平成 20 年）.

参考資料

ISMS で扱う情報の 3 つの側面

（1） ＩＳＭＳで価値を保護する 3 つの分野と対象

価値ある情報を創造すると、機密性、完全性、可用性と言う 3 つの視点で情報を保護する必要があります。逆に言うと 3 つの方面から情報に対する脅威があり、そこに脆弱性が存在すると、リスク（被害）が現実化するということです。ISMS はこの 3 つの視点でリスクアセスメントを行い、リスクが現実化することを防ぐマネジメントシステムです。機密性、完全性、可用性は英語の頭文字をとり、略して CIA と呼ぶことがあります。

情報セキュリティと言うと情報漏えいと理解されている場合がありますが、ISMS の対象は、機密性の保護に相当する情報漏えいだけではなく、完全性、可用性も含む広い範囲に及んでいます。

完全性は情報の品質であり、ISMS は情報の品質管理です。また、可用性は情報が必要な時に取り出せることであり、情報サービスの品質管理です。このため、ISMS は企業活動全般を対象として、情報の価値と情報によるサービスを創造し、保護する活動と言えます。

分野	特性	英語	想定リスク	例
C	機密性	confidentiality	情報が漏えいした	個人情報漏洩
I	完全性	integrity	情報が改ざんされた	財務諸表の改ざん
A	可用性	availability	情報が利用できない	情報システムダウン

（2） 3つの側面ごとのリスクの具体的な事例

事故を起こした企業名、具体的な記述は出せませんので、少し抽象的ですが機密性、完全性、可用性ごとにご説明します。ISMS が取り扱うリスクが、どのような性質であるのか、その被害、影響の程度などをイメージできると思います。

C：confidentiality 機密性

- ■ リスク：情報漏えい
- ■ 事例：従業員による情報漏えい
  - 証券会社の顧客になりすまして、オンライントレードのシステムを利用して株の売買を行った情報処理サービス会社の社員 A が、不正アクセス禁止法違反、電磁的記録不正作出及び供用罪で逮捕されました。
  - 情報処理サービス会社の社員であった A は、派遣先の証券会社でオンライントレードのシステムに関わる作業を行った際に、ユーザー名やパスワードなど、約 3 万 8000 人分の顧客情報を自分のノートパソコンにコピーして不正に入手していました。社内の自分の評価に不満があり、トラブルを起こすことそのものが目的であったそうです。

Ｉ：integrity 完全性１ （原本性）

- ■ リスク： 成りすまし
- ■ 事例：メールの成りすましによる詐欺
  - ご入会ありがとうございます。あなたの個体識別番号は以下の通りです。
    2468XXXXX
  - サービスのご利用料金は 1 ヶ月間で 8,000 円です。1 週間以内にお振り込み頂けなかった場合には、ご自宅にまで回収にお伺いすることになります。なお、お支払い頂けない場合には、裁判所からご連絡がいくことになります。

Ｉ：integrity 完全性２ （正確性）

- ■ リスク：改ざん
- ■ 事例：財務諸表の信頼性、品質

- 営業責任者が顧客と共謀して売上金額をピンハネするために稟議決裁なしで、現物の出入りの必要のない役務サービスを、高額で偽装販売しました。
- ノルマ圧力から、小売店に商品を納入した時点で売り上げ計上してしまう「押し込み販売」といった“見せかけの売り上げ作り”がありました。

Ａ：availability　可用性

■ リスク：情報システムダウン

■ 事例：ATM の停止

- ３連休にすべてのＡＴＭが停止する事態に至った銀行のシステム障害。発端は＊日未明に起きた「バッチ処理」のトラブルでした。
  - 銀行は＊日未明、バッチ処理が予定時間までに終了しなかった。原因について同行は「東京都内の特定支店の特定口座への振り込みが想定以上の件数に上った」と説明しており、その段階でシステムが動かなくなった可能性があります。会見で頭取は「一部の口座では、データ容量の上限設定が適切な数値になっていなかった」と人為ミスの可能性に言及しています。