情報倫理ビデオと情報セキュリティ監視サービスと ISMS を組み合わせた大学の情報セキュリティ強化

Reinforcement of Information Security Combining Computer Ethics Video Clips, Managed Security Service and ISMS

山之上　卓†，古屋　保†，下園　幸一†
小田　謙太郎†，升屋　正人†，森　邦彦†

Takashi Yamanoue†，　Tamotsu Furuya†，　Koichi Shimozono†
Kentaro Oda†，　Masato Masuya†，　Kunihiko Mori†

yamanoue@cc.kagoshima-u.ac.jp, furuya@cc.kagosima-u.ac.jp, simozono@cc.kagoshima-u.ac.jp
odaken@cc.kagoshima-u.ac.jp, masatom@cc.kagosima-u.ac.jp, mori@cc.kagoshima-u.ac.jp

†鹿児島大学学術情報基盤センター

† Computing and Communications Center, Kagoshima University

概要

鹿児島大学における，情報倫理ビデオと商用通信監視サービスと情報セキュリティマネージメントシステム(ISMS) を組み合わせた情報セキュリティ強化について述べる．情報セキュリティは人と運用と技術の３本柱により実現可能である．人の面の情報セキュリティの強化について我々は情報倫理ビデオを利用している．技術面については，商用通信監視サービスなどを利用している．商用通信監視サービスの利用により，大学の出入り口における 24 時間 365 日の監視を実現することができた．ところが運用に関しては，我々は標準的な情報セキュリティ強化の手段を持っていなかった．このことは大学間連携の障害にもなった．利用者の信頼を得るためにもなんらかの標準的な運用手段を持った方が好ましい．この問題を解決するため，ISMS を導入することを決定し，2013 年 4 月に認証を受けた．ISMS を導入し認証を受ける過程で，多くのの時間と労力を費やしたが，ISMS で実施する規定類の多くは，我々がいままで明文化せずに行っていたものであった．ISMS は情報セキュリティの強化だけでなく，日常的な業務やセンター教職員の管理の改善にも役に立っている．

キーワード

情報セキュリティ，ISMS，運用規則，情報倫理，セキュリティ監視

1. はじめに

多くの大学は学生や教職員にネットワークやネットワークに接続されたコンピュータを提供しており，学生や教職員は電子メールや他のサービスを学内で利用できるようにしている．このような状況において情報セキュリティは，これらのすべての大学にとって最も重要な事項の一つである．情報セキュリティは人と運用と技術の３本柱によって実現可能である[1]．我々は人の面の情報セキュリティの強化に関し，情報倫理ビデオを利用している．技術の面については商用情報セキュリティ監視サービスの利用やファイヤーウォールの設置やウィルス対策ソフトの利用や迷惑メール対策システムの利用や認証付ファイル共有サーバの利用などを行っている．運用面に関し，我々は 2012 年に情報セキュリティマネージメントシステム(ISMS)の導入を決定し，2013 年 4 月に認証を受けた．本論文では情報倫理ビデオと商用情報セキュリティ監視サービスの概要を述べ，ISMS 認証までの過程について示す．

2. 情報倫理ビデオ

国立大学情報処理教育センター協議会とメディア教育開発センターが協力して，「情報倫理デジタルビデオ小品集」(Part I) を 2002 年に開発した．Part I が好評だったことをふまえ，また，最新の情報セキュリティの問題に対応するため，Part II, Part III, Part IV が開発された．Part II, Part III は ACM SIGUCCS の賞を受賞している[2][4]．この開発は，Part I を作成したタスクフォースと，メディア教育開発センター，その事業の一部を引き継いだ放送大学および大学 ICT 推進協議会の協力によって行われた．小品集の多くは物語編とその解説編によって構成されている．物語は大学生の情報倫理にかかわる演劇で紹介される．大部分の物語は，解説編の中で技術的および法的側面から説明が行われる．物語のいくつかには正解はなく，授業内での議論を促すようになっている．以下は情報倫理ビデオを使った授業の例である．

- 物語を学生に見せる
- 物語についてクラスの中で議論を行う
- 解説編を学生に見せる
- 解説編についてクラス内で議論する
- 学生は視聴した物語編と解説編を元にして，レポートを作成し，提出する．

我々の大学では個人情報や重要な情報の紛失や漏えいを防止するため，2011 年に小品集 Part II, No.4 の「個人情報紛失に備えるノウハウ」を使って，教職員対象の講習会を行った．この講習会は，担当者が本学のすべての部局に巡回し，教職員の受講率 100%を目指して，それぞれの部局の教授会が開催される前に実施した．このことにより，講習会の未受講者の数を少なくすることができた．講習会の実施と認証付ファイル共有サーバのサービスを組み合わせることにより，その後の USB メモリ紛失事故を減少させることに成功した．2012 年には，すべての新入学生に対して，情報リテラシ入門教育において

- ログインログアウト(Part I, No.1)
- パスワードを忘れたらどうする？(Part III, No.3)
- 安直なパスワードで重大事件(Part III, No.2)
- 個人情報紛失に備えるノウハウ(Part III, No. 4)
- SNS についた謎のコメント(Part III, No. 15)

を視聴することを推奨した．

2013 年度からは，本学すべての学生が共通教育用 Moodle サーバにログインすることにより，Part IV を視聴できるようにしている．情報倫理ビデオを利用することにより，情報セキュリティに関する教育を行いやすくなった．すべての学生，教職員に対して大学の情報セキュリティの重要性やポリシーを理解してもらうためにも役立っている．

3. 商用情報セキュリティ監視サービス

大学ネットワークは街と類似している．街に良い人も悪い人もいるのと同様に，良いパケットや悪いパケットが行き来している．外部からもパケットが入ってくる．大学ネットワークの管理者は街の警察官と同様に，大学のネットワークを安全に保つ役割を果たしている．街の安全を保つために警察官は街の見回りを行っている．街の見回りがなければ犯罪を発見することは難しい．警察官による街の見回りは，ネットワーク管理者によるネットワークの監視に相当する．近年，ネットワークの監視はネットワーク管理者の重要な仕事の一つである．ネットワークの監視なしにネットワークの安全を保つことは難しい．街の条例と同様に，ネットワークセキュリティの監視を義務化することを情報セキュリティポリシーの条文に掲載することは一般的である．しかしながら，限られた人員，時間，費用によって大学のネットワークの隅々を監視することは非常に難しい．この問題に対処するため，我々は商用の情報セキュリティ監視サービスを大学の出入り口で利用している[3]．

表 1. コンサルタントとの会議

No.	日付と内容	No.	日付と内容
1	2012 年 8 月 8 日 ● コンサルタントとの最初の会議 ● サンプルマニュアル ● 既存文書の調査	9	2012 年 10 月 11 日 ● サイトツアーの実施 ● リスクアセスメント結果報告書およびリスク対応計画の解説 ● 事業継続計画の確認 ● 内部監査についての確認
2	2012 年 8 月 17 日 ● スケジュール確認 ● 文書の解説	10	2012 年 11 月 13 日 ● 事業継続計画および訓練計画の確認 ● リスク対応計画書についての確認 ● 内部監査についての確認
3	2012 年 8 月 24 日 ● リスクアセスメント概要の説明 ● 情報資産の棚卸について ● 脅威と脆弱性について ● 「基本方針」「適用範囲」の見直し結果について	11	2012 年 11 月 15 日 ● 内部監査
4	2012 年 9 月 7 日 ● 棚卸内容の確認	12	2012 年 11 月 16 日 ● 内部監査のフォローアップ ● マネージメントレビューの解説 ● 審査準備の助言
5	2012 年 9 月 11 日 ● マニュアルの第 1 章と第 2 章の確認	13	2012 年 11 月 22 日 ● リスク対応計画の検討・決定 ● 有効性の測定項目の検討・決定
6	2012 年 9 月 21 日 ● 適用範囲の確認 ● 情報資産棚卸リストの見直し ● リスクアセスメント結果報告書の解説	14	2012 年 12 月 4 日 ● 内部監査に関するフォーローアップ
7	2012 年 10 月 3 日 ● セキュリティ教育の実施 ● 事業継続訓練の解説 ● 文書および記録についての解説… マニュアルの 3 章と 4 章の確認	15	2013 年 1 月 8 日 ● 審査事前準備
8	2012 年 10 月 10 日 ● 内部監査員研修	16	2013 年 2 月 8 日 ● NCR 進捗確認 ● リスク対応計画の進捗確認 ● 有効性の測定確認 ● 審査前対応

その他の部分では，ウィルス対策ソフト(ESET NOD32)の学内配布，アプリケーションの通信内容の判定なども行う高機能ファイヤーウォール(paloalto)の設置，迷惑メール対策システム(IronPort)，認証付ファイル共有サーバ(Proself)などを利用している．

商用情報セキュリティ監視サービスを利用することにより，24 時間 365 日の監視を実現することができた．侵入検知が発生したときは，サービス業者からメールで本学担当者に通知が行われ，勤務時間外でもメールで該当部局に連絡したり，VPN を使って遠隔ログインして対処したり，場合によっては夜間や休日に緊急出勤して，対応を行っている．

4. ISMS

運用は情報セキュリティ強化の 3 本柱の一つである．我々は情報セキュリティの運用面の標準的な対策を最近まで持っていなかった．このことは，大学間連携を行う場合の障害にもなった．利用者の信頼を得るためにもなんらかの標準的な運用手段を持った方が好まし

い．このような問題に対処するため，我々は情報セキュリティママネージメントシステム (ISMS, JIS Q 27001)の導入を決定し，2013 年 4 月に ISMS の認証を受けた．ISMS は情報セキュリティの世界的な標準規格として良く知られている．JIS Q 27001 は組織が望む情報セキュリティのレベルを ISMS Plan-Do-Check-Act (PDCA) と呼ばれる方法によって達成することを支援する．ISMS PDCA は組織内でポリシーや管理策やセキュリティ組織を確立する．

4.1 ISMS 導入の過程

我々の一部は以前から大学の情報セキュリティポリシー策定にかかわっており，情報セキュリティに関する知識はある程度持っていた．

2011 年の東日本大震災は予測不可能な事故に対する準備の重要性を我々に認識させた．

我々鹿児島大学学術情報基盤センターは 2011 年 9 月 30 日に，山口大学メディア基盤センターとデータバックアップ実験を開始した．

山口大学メディア基盤センターはすでに ISMS の認証を受けており，我々は山口大学側から ISMS 認証取得の打診を受けた．その後，どのようにしたら ISMS 認証を受けることができるか調査を行った．以下に，その後の ISMS 導入の過程を示す．

- 2011 年 12 月，ISMS のコンサルタントの調査を開始．
- 2012 年 4 月，学術情報基盤センターの会議(センター会議)において，ISMS 導入を決定．
- 2012 年 5 月 8 日-9 日，山口大学の ISMS 研修会に鹿児島大学の学術情報基盤センターのスタッフが参加．
- 2012 年 5 月 28 日，ISMS のコンサルタント選定手続きを開始．
- 2012 年 6 月 20 日，他大学の例を調査．
- 2012 年 7 月，入札により，コンサルタントを決定．
- 2012 年 8 月，コンサルタントとの会議を開始．表 1 にコンサルタントとの会議の日程と内容を示す．情報資産リストの棚卸開始．
- 2012 年 9 月，コンサルタントから提示されたサンプルを使い，ISMS マニュアルの執筆を開始．コンサルタントと共にリスクアセスメントを実施．
- 2012 年 10 月，学術情報基盤センター教職員に対する教育と BCP 訓練を実施．
- 2012 年 11 月，コンサルタントの支援を受けて内部監査を実施．ISMS 認証を受けている他大学の調査を実施し，その組織がマニュアルから，具体的な手順を述べた「規範」集を分離していることを知り，我々も同様に「規範」を利用するよう方針を変更した．
- 2012 年 12 月から 2013 年 1 月，内部監査より作成された不適合報告書への対応．不適合報告書は 2 件の不適合と 23 件の要是正と 6 件の改善の機会の項目があった．この中で，不適合の 1 件は学生のテスト回答および採点結果がセキュリティの保たれていない場所に保管されていたもので，この不適合はすぐに修正された．もう一件は情報資産のラベル付けが行われていなかったものである．不適合報告書への対応の過程で，多くの規範と記録を作成した．不適合報告書への対応社業はマニュアルや規範や他の文書の改善に最も効果があった．
- 2013 年 2 月，第 1 回の外部監査実施．監査内容は主に文書内容に関する面談．結果を受けて，文書の一部を修正．
- 2013 年 3 月，第 2 回目の外部監査実施．内容は ISMS 対象範囲の見学と面談．
- 2013 年 4 月 23 日，認証．

4.2 ISMS 文書の特徴

表 2 に文書と記録のリストを示す．我々の ISMS は以下の特徴を持つ．

- 修正手続きが困難なマニュアルから「規範」を分離することにより，比較的短いサイクルで文書の改良を行うことが可能になった．情報セキュリティポリシーの文書構造と対応付けた場合，マニュアルはポリシーの対策基準に対応し，規範は実施手順に対応する．マニュアルは 1 冊であるが，規範については様々な業務に対応して小さなものを沢山作成している．マニュアルは ISMS を運用するための最上位の文書であるため，その追加や修正にはそれなりの慎重さが求められるが，規範の 1 つ 1 つは具体的な手順が中心であるため，気軽に修正できる．2013 年 2 月の ISMS の外部監査実施以降，毎月情報セキュリティ委員会(定例のセンター会議)において規範の追加や修正を行っている．まだ不足している規範が沢山存在しているが，徐々に増えており，人に依存する運用からの脱却を少しずつ行っている．
- 第 3 章に述べた商用セキュリティ監視サービスやその他の技術的対策をマニュアルや規範に組み込み，管理策の有効性測定に必要な測定値を得るためにも利用している．
- 文書の正本は紙で保持することにしたが，同じものを，ID とパスワードによる認証が必要な Web 上のファイル共有システムに置いている．このことにより，教職員が必要なときいつでも最新の文書を閲覧して業務を行うことが可能になっている．

4.3 ISMS 導入の効果

ISMS 認証取得の効果については，今後の経過観察が必要であるが，今までの経過から以下の効果がある

と思われる.

- 情報関連業務の透明化がはかれた.
- 以前と比べて，大学間の協力が行いやすくなる.
- 文書と記録の作成は情報資産と業務に関して我々が共通認識を持つのに役立った．たとえば，文書化された規範はスタッフ内の意見対立 解消に役立った.
- 「クリアデスククリアスクリーン」の管理項目は事務所や教員室の整理整頓に役立った．クリアデスクとは，大事な情報の紛失を防ぎ，必要な情報を必要な時にすぐに手に取ることを可能にするため，散らかった部屋や机の上や棚の中を整理整頓することである．クリアスクリーンとは，パソコン画面ののぞき見やパソコンの不正操作による情報漏えいなどを防ぐため，一定時間，操作が行われていない時に自動的にスクリーンロックの状態になるように設定し，パソコンの ID とパスワードをきちんと設定することである.

表 2. ISMS の文書と記録

文書番号	文書名	文書番号	文書名
ISMS-1-01	ISMS 基本方針	ISMS-5-R18	セキュリティカード発行管理簿
ISMS-1-02	情報セキュリティマネジメントシステムマニュアル	ISMS-5-R19	カギの貸出管理簿
ISMS-1-02-01	適用範囲	ISMS-5-R20	入室・退室票ならびに秘密保持契約
ISMS-1-02-02	情報資産棚卸リスト	ISMS-5-R21	特権 ID 管理台帳
ISMS-1-02-03	リスクアセスメント結果報告書	ISMS-5-R22	ソフトウェア管理台帳
ISMS-1-02-04	適用宣言書	ISMS-5-R23	アクセス制御リスト
ISMS-1-02-05	リスク対応計画書	ISMS-5-R24	特権 ID 管理台帳
ISMS-3-01	事業継続計画	ISMS-5-R25	USB 管理台帳
ISMS-4-01	主な適用法令一覧	ISMS-5-R26	部局専用サーバ（仮想マシン）ホスティング台帳
ISMS-4-02	ISMS 文書管理台帳	ISMS-5-R27	重要情報資産の保管および分類状況調査記録
ISMS-5-R01	ISMS 年間計画表	ISMS-5-R28	クリアデスククリアスクリーンチェック記録
ISMS-5-R02	教育記録	ISMS-5-R29	モバイル PC 管理台帳
ISMS-5-R03	有効性評価測定シート	ISMS-5-R30	WWW&Mail ホスティング管理台帳
ISMS-5-R04	内部監査計画書		
ISMS-5-R05	内部監査マトリックス		
ISMS-5-R06	内部監査チェックリスト	ISMS-6-N01	利用者登録に関する規範
ISMS-5-R07	内部監査報告書	ISMS-6-N02	利用者パスワードの管理に関する規範
ISMS-5-R08	不適合報告書	ISMS-6-N03	利用者パスワードの利用ルールに関する規範
ISMS-5-R09	予防処置報告書	ISMS-6-N04	利用者リストの引き渡しに関する規範
ISMS-5-R10	マネジメントレビュー議事録	ISMS-6-N05	ホストリストの引き渡しに関する規範
ISMS-5-R11	事業継続計画リスクアセスメント	ISMS-6-N06	学術情報基盤センター教職員が当センター外で業務を行う場合に関する規範
ISMS-5-R12	事業継続計画テスト結果記録	ISMS-6-N07	部局専用サーバホスティングサービスに関する規範
ISMS-5-R13	改善提案書	ISMS-6-N08	期間限定利用に関する規範
ISMS-5-R14	障害報告書	ISMS-6-N09	サーバの管理運営に関する規範
ISMS-5-R15	ハードウェア一覧	ISMS-6-N10	ネットワークの管理運営に関する規範
ISMS-5-R16	サーバハウジング管理台帳	ISMS-6-N11	作業記録に関する規範
ISMS-5-R17	アクセスレベル一覧	ISMS-6-N12	業務委託に関する規範

4.4 ISMS 導入の欠点

ISMS の導入のためには多くの時間と労力が必要であった. ISMS 認証を得ることはできたが, それが実際の情報セキュリティの強化にどのくらいの効果があるか, すぐに実感できるわけではない. 内部のすべての教職員が ISMS 実施に積極的に参加するようになるのは簡単なことではない. ISMS 実施への積極的な参加が教育や研究を目的としている教員にも, 事務や実運用を行っている職員にも, 大きなメリットが得られるような工夫を今後行っていく必要があると思われる.

5. 関連研究

5.1 静岡大学の ISMS 文書の管理運用手法

長谷川らはワードプロセッサやマインドマップなどの安価な汎用性ツールを用いて, 管理文書の機密性, 完全性, 可用性を大きく向上させることについて述べている[5].

我々もマニュアルの修正は Microsoft Word の校閲機能を利用している. バージョン管理について, git の利用も検討した. 電子文書の扱いに慣れていない教職員もいるため, 現時点では文書の正本は紙で扱うこととした.

5.2 山口大学の ISMS 構築テンプレート

山口大学では ISMS 構築のためのテンプレートを開発している[6]. 我々もこのテンプレートを利用することについて検討したが, このテンプレートを利用する代わりに, コンサルタント会社が提供したサンプル書類を利用した.

5.3 徳島大学の事例

上田らは徳島大学情報化推進センターにおける ISMS 取得の経緯と, それが外部評価に役立ったことについて述べている[7]. この論文の中でも不適合報告書への対応が有効だったことが述べられている.

6. おわりに

ISMS 導入に多くの時間と労力が必要であったが, 以前から行っていた大学の情報セキュリティポリシー策定の作業の経験が役に立った. また, ISMS の情報セキュリティ管理策の多くは, 我々が以前から明文化せずに行っていたことであった. ISMS は情報セキュリティを強化するだけでなく, 日常業務を改善することに役立つ. 情報倫理ビデオと商用セキュリティ監視サービスと ISMS を組み合わせることにより, 情報セキュリティ強化を保持する自信を強めることができた.

本報告で述べた様々な手法により, 大規模な情報漏えい事件のようなセキュリティ事故は発生していない. しかしながら, 2013 年 5 月から 6 月にかけて, 本学内の組織が管理する Web ページの改ざんが発覚した. これは業者に Web 作成や更新を委託した Web ページについて, 更新のための ftp の ID とパスワードが盗まれたことが原因だった. 商用情報セキュリティ監視サービスは ftp の総当たり攻撃や脆弱性を狙った攻撃は検知しているが, 盗まれた ID とパスワードによる Web ページ改ざんは, 通常の Web の更新と見なされ, 検知することができなかった. 今後, このような, 今までの対策では不十分であったリスクへの対応方法を検討していく予定である.

7. 謝辞

本学情報企画課の本田敏幸課長代理に ISMS 導入に関する様々な作業を支援していただきました. ISMS コンサルタントの株式会社サン・パートナーズ様に, ISMS 導入のコンサルタントをしていただきました. この他, 多くの皆様に ISMS 導入の支援をいただきました. ここに感謝します.

8. 参考文献

[1] Amanda Andress: Surviving Security: How to Integrate People, Process, and Technology, CRC press, 2003.

[2] Takashi Yamanoue, Michio Nakanishi, Atsushi Nakamura, Izumi Fuse, Ikuya Murata, Shozo Fukada, Takahiro Tagawa, Tatsumi Takeo, Shigeto Okabe, Tsuneo Yamada : Digital Video Clips Covering Computer Ethics in Higher Education, Proceedings of the 33nd annual ACM SIGUCCS conference on User services, pp.456-461, Monterey, California, US. 6-9 Nov. 2005.

[3] Masato Masuya, Takashi Yamanoue, Shinichiro Kubota : An Experience of Monitoring University Network Security Using a Commercial Service and DIY Monitoring, Proceedings of the 34nd annual ACM SIGUCCS conference on User services, pp.225-230, Edmonton, Alberta, Canada. 5-8 Nov. 2006.

[4] Izumi Fuse, Takashi Yamanoue, Shigeto Okabe, Atsushi Nakamura, Michio Nakanishi, Shozo Fukada, Takahiro Tagawa, Tatsumi Takeo, Ikuya Murata, Tetsutaro Uehara,

Tsuneo Yamada: Improving Computer Ethics Video Clips for Higher Education, Proceedings of the 36th annual ACM SIGUCCS conference on User services, pp.235-242, Portland, Oregon, US. 6-9 Oct. 2008.

[5] 長谷川孝博, 井上春樹, 八巻直一:ISMS 文書の低コストかつ高効率な管理運用手法, 情報処理学会研究報告, Vol. 2009-IOT-6, No.7, 2009 年 6 月.

[6] 市川他: 山口大学における情報セキュリティマネジメントシステム(ISMS)構築テンプレート作成および適用範囲拡張について, 情報処理学会研究報告, Vol. 2011-IOT-14,No.6, 2011 年 7 月.

[7] 上田哲史, 佐野雅彦: 組織評価と ISMS, 情報処理学会研究会報告, Vol. 2012-IOT-16, No.41, 2012 年 3 月.