解説

情報セキュリティポリシーの全学導入について

家木 俊温　　横井 利彰

現在の社会は情報活用のあらゆる場面でリスクに直面している．情報をサイバー攻撃から護るためには，情報システムに最新のセキュリティ対策を施すと共に，入り口から末端までの各段階での多段防御を整え，それを使う人々のセキュリティ意識を高めて維持してもらう取り組みが必要となる．本稿では，本学の情報セキュリティ向上のために，世田谷・横浜・等々力の全キャンパスの情報基盤センターが連携して，本学に合った情報セキュリティポリシーを策定した取り組みを紹介すると共に，今後一体となって情報セキュリティの維持・向上に参加頂く構成員各位に理解を深めて頂くために，その概要を紹介する．

キーワード：情報セキュリティ，マルウェア，リスクマネジメント

1　はじめに

各種報道で伝えられているように，企業・官公庁・大学において個人情報や機密情報の流出が後を絶たず，またネットワークを介してサーバや情報端末機器へのサイバー攻撃が増加している．これらの手段に利用されるコンピュータウィルスなどのマルウェアに対しては，これまでは入り口で検知するのが主な方法であったが，IPA (情報処理通信機構）のいう「新しいタイプの攻撃」では，入り口での対策が効かず非常に巧妙に内部に入り込み，かつ気づかれにくい動作によって組織の知財や個人情報などの重要な情報が窃取される例が増えているという．また個人対象でも，遠隔操作・誤認逮捕事件にみられるように，個人のコンピュータを乗っ取られて他への攻撃に利用されたり，システムを使用不能にして回復のための身代金を要求するソフトウェアによる事件も起きている．また，大手パブリック・クラウドでのデータ保管会社では，利用者登録情報への不正アクセスが起きるなど，現在の社会は情報活用のあらゆる場面でリスクに直面している．一方で，急速に普及し続けるスマートフォンやタブレットでの情報セキュリティ対策の意識はまだまだ低いといわれている．このような状況下では，情報システムに最新のセキュリティ対策を施すと共に，入り口から末端までの各段階での多段防御を整え，それを使う人々のセキュリティ意識を高めて維持してもらう取り組みが必要となる．

情報セキュリティを高めるには，まずリスクの 3 要素である①情報資産，②脅威，③脆弱性，を認識し，セキュリティ強化のためにこれらが合流しないような対策を講じる必要がある．また，情報セキュリティの要素である①機密性（Confidentiality)，②完全性（Integrity)，③可用性（Availability)，④否認防止（non-repudiation)，⑤責任追跡性（accountability)，⑥真正性（authenticity)，⑦信頼性（reliability）の視点から，自分の属する情報サービスでどう該当するのかを分析し，リスクマネジメントとして①抑止，②予防，③検知，④回復，について適切に対応する必要がある．

このような情報セキュリティ向上のために，世田谷・横浜・等々力の全キャンパスの情報基盤センターでは，連携して本学に合った情報セキュリティポリシーの策定を行い 2 月の大学協議会での承認を経て，平成 25 年 4 月から実施の運びとなった．

本稿では，これまでご協力頂いた各位の取り組みをご紹介すると共に，今後一体となって情報セキュリティ維持に参加頂く構成員各位に向けて，理解を深めて頂くために概要を紹介することといたしたい．

2　情報セキュリティポリシー策定に向けての取り組み

これまで，情報基盤センター（および旧センター組織）では，情報ネットワークの運用規則や倫理規定等により，個別に規則を定めて運用と啓発を行ってきた．しかし，必ずしも網羅的な内容ではなく，新しい事案につ

IEKI Toshiharu
東京都市大学メディア情報学部情報システム学科教授（情報基盤センター運営委員会委員，情報セキュリティポリシーWG主査）
YOKOI Toshiaki
東京都市大学メディア情報学部情報システム学科教授（情報基盤センター前副所長）

いてはその都度協議しながら対応せざるを得ない状況にあった．そこで，情報基盤センターでは，情報システムに関する情報セキュリティポリシーを体系的に定めることで，全学的な方針を明示し，各組織に応じた対策・実施内容の整合性を図ることで，迅速かつ明快な対応を目指したいと考えた．

この実現のために，平成 24 年 4 月に情報基盤センター運営会議（議長：皆川 勝 情報基盤センター所長）の中に「情報システムに関する情報セキュリティポリシーワーキンググループ（略称：SPWG　主査：家木 俊温 教授）」を立ち上げ，ポリシー策定の準備を進めた．作業では，情報セキュリティに関する国際標準や各種国内標準を調査した上で，本学に適する情報セキュリティポリシーを策定した．これにより，先に述べた脅威への対応体制・手順が明確となり対応の迅速さにつながることや，対外的な情報管理の信頼性の向上，構成員のセキュリティ意識向上などの効果が期待できるものと考える．

以降ではその具体的な構成と内容について紹介する．

3　情報セキュリティポリシー

ここでは，情報セキュリティポリシーの構成，内容，狙いなどについて記述する．

3．1　ポリシーの構成

ポリシーは，以下のとおり三部から構成される（図 1）．

第 1 部：基本方針
第 2 部：対策基準
第 3 部：実施手順

このうち，第 3 部は実施マニュアル的な色彩が強いことから，ポリシーに含まない場合もある．以下に各部の内容と狙いを述べる．

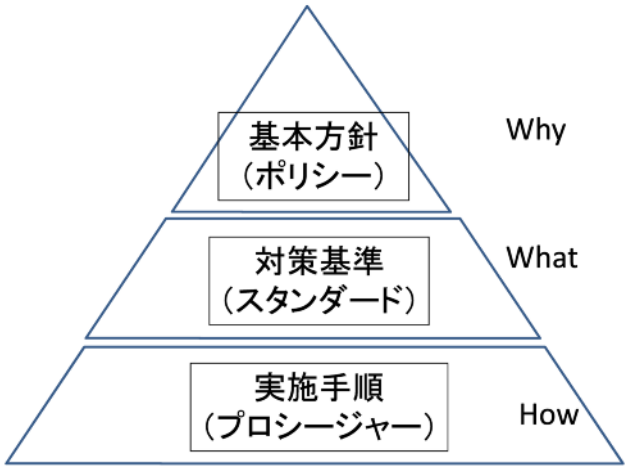

図1　情報セキュリティポリシーの構成

3．2　基本方針

ここで大切なのは，第一条に書かれている「基本理念および目的」であり，以下のとおりである．

① 情報資産（電子化された情報および情報システム）は，本学の教育・研究に重要である．その安全性が守られなければ，教育・研究活動の停滞，信頼の喪失，他社への加害者となる恐れがある．
② 情報資産の安全性を守るためには，本学の全構成員（教職員，学生）が，定められたポリシーを守る必要がある．

今回のポリシー制定とその遵守は，全構成員にとってチャレンジ対象となる．全員が守ることができるポリシーとするためには，全員が PDCA を回し，成長し，ポリシーや実施体制を改善することが要求される．特に，今後社会に出ていく学生にとっては，良い実践的教育の場であると思われる．

3．3　対策基準

ポリシーの中核部分に当たるもっとも重要な部分である．次の 3 つの部分からなる．

(1) 情報資産の脅威とリスク評価

本学の情報資産は，ネットワーク，これに接続された機器（サーバ，PC，スマートフォン，USB などの外部メモリ），およびその中にある情報，ソフトウェアである．これらの情報資産に及ぼすリスクが大きいと評価される脅威には，次のものがある．

① 内部者の不注意，ミスによる脅威

本学の構成員である教職員，学生は，個人情報などの重要な情報をノート PC，USB メモリなどに格納する機会が多いと思われる．もし，これらの紛失，置き忘れ，盗難などが起きると，情報漏えいの恐れが生じる．また，構成員が安易なパスワード設定をしたり，他者に漏らしたりした場合も問題が生じる．

② ウイルスによる脅威

今日では，無数のウイルスがインターネット上に存在しており，サーバ，PC，スマートフォンは常に感染の脅威にさらされている．もし感染した場合，重要な情報の漏えい・改ざん・消去や，ソフトウェアの異常動作を招く恐れがある．ウイルス対策ソフトの不採用，アップデート漏れなどによって脅威が増大する．

以上述べた脅威は，構成員の意識の向上，対策の順守によってかなり防ぐことが可能である．なお，今日対策が困難とされる脅威として，標的型攻撃，サイバーテロがあげられる．この脅威は，国家，企業が狙われることが多く，本校に対しては，目下の脅威となる可能性は極めて少ないと考えられる．

(2) 組織的対策

(1) からも明らかなように，本校の全構成員が対策を順守することは重要である．

そのためには，上位から下位へポリシーの重要性，順守の必要性を教育・指導し，問題の発生や提案を下位から上位へ報告する組織，および，その組織による PDCA の実施が重要である．

本ポリシーでは，全校一丸となった活動となるよう，組織の総責任者を学長とした．

その他の構成員については，以下の通りとした（図 2 に組織図）．

① 教員と学生

この両者は，教育・研究を一体となって活動しており，教授会，ゼミ活動などキャンパス内での活動が多い．そこで，各キャンパスの情報基盤センター副所長の指示のもとで活動することとした．

② 職員

職員組織は，全学的に一体となったものが組織されており，一般的な指示系統はそれに従っているため，ポリシーについても全学的な指示系統とした．

また，PDCA におけるチェックを行うため以下の外部組織を設けた．

① PLAN

ポリシーの作成，修正を行う組織として，セキュリティポリシー WG を設けた．

② D0

実行組織として，上述した組織を設けた．

③ CHECK

実行組織と独立した内部監査委員会を設けた．本委員会は，

・ポリシーが守られているか

・ポリシーは適切か

を監査する．また，全構成員が活動結果を報告するためのツールとして，WEB 入力システムを作成することとした．

④ ACT

監査結果を受けて，セキュリティポリシー WG は修正を，また，実行組織は活動方針の見直しを行うこととした．

(3) 物理的・人的・技術的対策

これらはいずれも先にあげた脅威に対する対策である．各対策の要点を以下に述べる．

① 物理的対策

情報機器や記憶媒体には，個人情報などの機密情報が保管される場合が多い．なかでも，ノート PC や USB メモリは，盗難，紛失の可能性が高い．したがって，機密情報の暗号化や，盗難・紛失対策が必須である．

② 人的対策

組織的対策を行っても，各個人の役割，責任の理解が低いと PDCA がうまく回らない．そこで，各個人に対する教育，指導を充実させ，ポータルサイト情報の確認，障害時の報告などを主体的に行うようにすることが重要である．

③ 技術的対策

いろいろな対策を行う必要があるが，特に重要と思われるのは，パスワード管理とウイルス対策の徹底である．これらに関しては，初年度から厳守されねばならない．特に，スマートフォンにウイルス対策ソフトを入れることが肝要である．

3. 4 実施手順

これは，対策基準で定めた対策を行うための手順を定めたものでポリシーに含めない場合もある．手順の説明を詳しく，わかりやすくするために，学生用，教員用，事務局用の 3 分冊にした．しかし，対策を詳しく伝えるためには，画像情報の活用，技術・商品の詳細説明，新しい情報が出た場合の迅速な対応が必要となる．そこで，これを実現するため，情報基盤センターウェブページを開設し，必要に応じて他のサイトへのリンクを活用することにした．また，手順の理解を助けるため，以下の情報を付録として追加した．

① ISS 管理運用組織図（図 2）

② 構成員の属性毎の年間作業スケジュール

4 まとめ

今般，情報セキュリティポリシーの検討開始から 1 年間のうちに，関係各位のご理解とご協力のもと，ポリシーの策定を終えて承認を頂き，実施の運びとなった．

この情報セキュリティポリシーを実効あるものとするには，関係各位が常に意識して頂いて，継続的に改善を続けることが大切と考えられる．幸い本学では，横浜キャンパスが 1998 年 10 月 28 日に日本の大学として初めて ISO14001 の認証を受けて以来，活動を継続しており，PDCA の活動の大切さについて大学内で情報共有していることは，情報セキュリティポリシーの理解・維持・発展によい刺激となることと考える．

今後は，パブリック・クラウド／プライベート・クラウドの普及や，スマートフォンやタブレットの急速な普及が見込まれる中，適切な対応が求められることになる．

今後とも，各位のご理解とご協力をお願い申し上げる次第です．

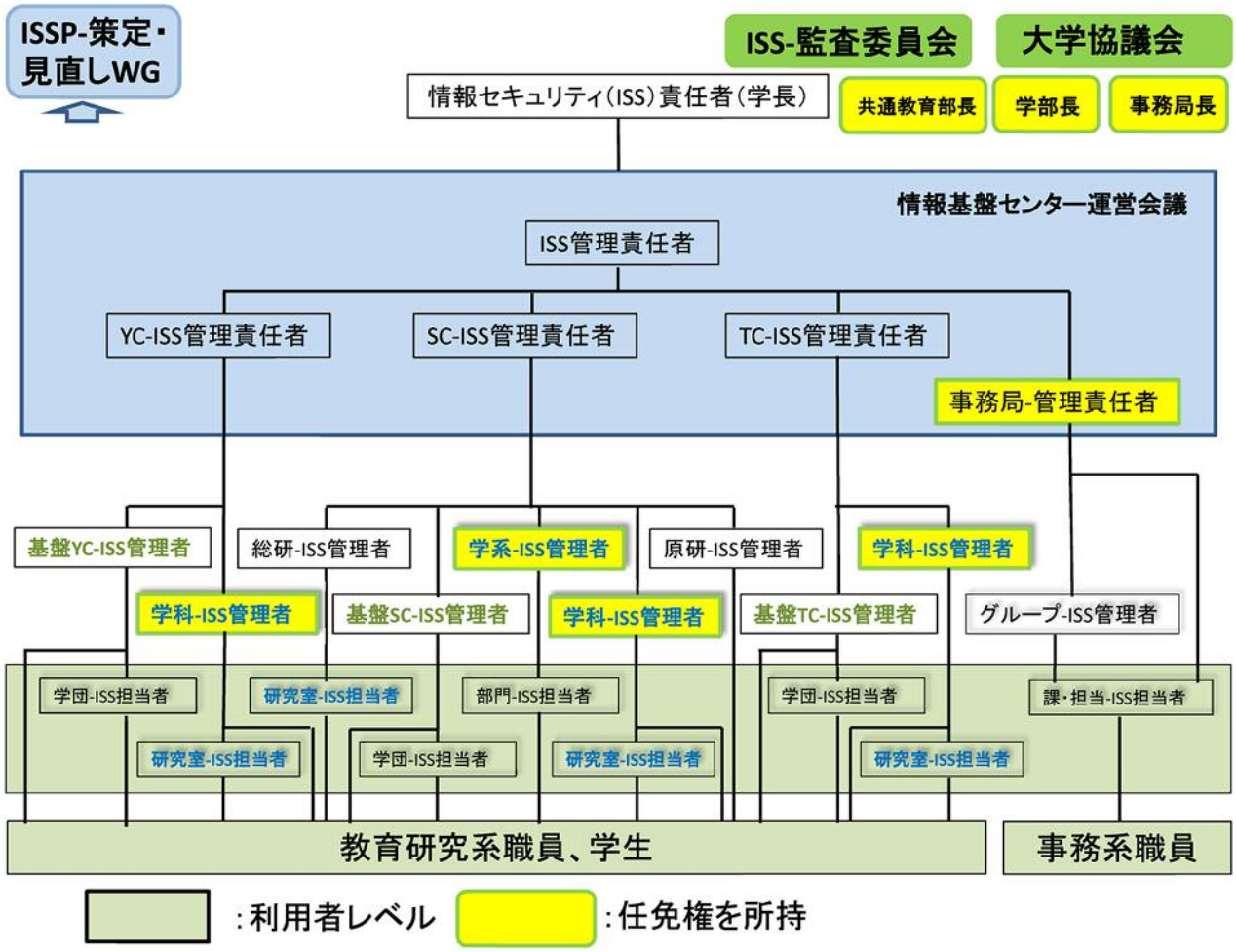

図2　ISS管理運用組織図