


平成 22 年 度

# 「情報セキュリティに関する懸賞論文」受賞作品

テーマ

- 1 インターネット上の脅威にいかに対応すべきか  
サイバー攻撃への対応
- 2 情報セキュリティ意識を向上させるための教育について
- 3 自由課題  
「情報セキュリティ意識の向上に資するもの」として日頃重要だと考えている視点からの提言

平成 22 年 12 月

財団法人 防衛調達基盤整備協会 ®

## 発刊にあたって

財団法人防衛調達基盤整備協会は、情報セキュリティ意識の向上に資するため、平成22年度（第3回）情報セキュリティに関する懸賞論文の募集を行い、より多くの方に応募して頂くことを通して情報保全意識を高めるとともに、優秀な作品を表彰し発表することにより、広く国民各層に情報セキュリティに対する知識と技術を広めたいと考えております。

このため、22年度の懸賞論文のテーマは三つに決めました。

一つは、「インターネット上の脅威にいかに対応すべきか」又は「サイバー攻撃への対応」です。多くの人々が利用しているインターネット上にウィルス感染を始めとする様々な脅威が発生しておりますが、このような脅威に対し、どう対応すべきか。また、どのように考えていくべきなのかについての提言や具体的諸施策に関する考察を期待したものです。

二つ目は、「情報セキュリティ意識を向上させるための教育について」です。例えば、「学校におけるPC教育の在り方」は今後どのようにしていくべきなのか、「永遠のビギナーに対する教育の在り方」とはいかにあるべきなのでしょう。今後ますますITに依存していく現代社会において、情報技術を利活用していく能力が必要なことは明らかなです。情報セキュリティ意識の向上に向けた提言などを期待したものです。

三つ目は、「自由課題」です。具体的には「私が考える情報セキュリティの在り方」とか、「今後大きな社会問題となっていくであろうサイバー攻撃」への所見など、皆様が日頃重要だと考えておられる視点からの提言を期待して選定したものです。

「情報セキュリティに関する懸賞論文」の選考に当たっては、当協会が委嘱した学術、電気通信研究、保全教育、インターネット、報道の各分野の有識者で構成された情報セキュリティ論文選考等委員会で厳正な審査を行い、優れた論文であると答申を受けた三つの作品を表彰させて頂くとともに、受賞作品を小冊子にまとめ、協会ホームページにも掲載致しております。

この小冊子は、情報セキュリティ意識向上に関し、示唆に富む内容としますので、防衛装備品の生産及び調達に携わる方々、防衛省・自衛隊の関係者の皆様の情報セキュリティレベルの向上に貢献し、ひいては、防衛基盤の強化に寄与することができれば幸いです。

平成22年12月

財団法人 防衛調達基盤整備協会  
理事長 宇田川 新一

## 論文選考にあたって

我が国でも国民生活や様々な社会経済活動においてインターネットの利用が促進されてきております。しかし、インターネットの利用が促進するに伴い、高度化・巧妙化したコンピュータウィルスの蔓延、企業・官庁における情報漏洩の多発等、情報セキュリティに関する問題が生じており、適切な対処がこれまで以上に重要視されてきております。

このような状況に鑑み、防衛調達基盤整備協会は情報セキュリティ意識の向上に資するため、「情報セキュリティに関する懸賞論文」を募集し、優秀な作品を表彰、発表する事業を企画し、私どもが審査を担当いたしました。

優秀作品の選考にあたっては、広く国民各層に情報セキュリティに対する知識と技術を広めることを目的として、読み手がそれぞれのテーマについての理解を深め、意識を高められるよう、具体的かつ解り易い内容の論文で、且つ、新鮮度、実証度合、影響度などの観点を重視した審議を重ね、最終的に3点が選ばれました。

最優秀賞の藤巻氏の作品は、高等学校の授業実践事例から情報教育に焦点を当て、「情報機器を使用した実技と情報モラルに留意した講義」を提言したものであり、実証性が高く、内容も具体的であり、社会に与える影響度も高いことを評価したものです。

佳作（サイバーディフェンス賞）の川口氏の作品は、サイバー空間での「抑止」として、多様なサイバー脅威に応じた「テイラーメイド型の抑止」を提案し、具体的、新鮮な内容を評価したものです。

佳作（教職員の意識向上賞）の星野氏の作品は、学校教職員の情報セキュリティ意識向上のため「多重リスクコミュニケーター」を基に、現在開発中の、学校に必要な機能に限定した「簡易多重リスクコミュニケーター学校版」を用いた研修方法を提案しており、新鮮な内容を評価したものです。

いずれも優れた論文であり、発表することによって情報セキュリティ意識の向上に貢献し、ひいては、防衛基盤の強化に寄与することを願っております。

平成22年12月

情報セキュリティ論文選考等委員会  
委員長 中尾 定彦

## 目 次

### 最優秀賞

テーマ：情報セキュリティ意識を向上させるための教育について  
高校における教科「情報」授業実践事例から、  
今後のPC教育の在り方へ

情報セキュリティ大学院大学 博士前期課程  
藤 卷 朗 氏・・・1

### 佳作（サイバーディフェンス賞）

テーマ：自由課題

サイバー空間における「抑止」についての一考察：  
国家安全保障政策の視点から  
東京海上日動リスクコンサルティング株式会社  
研究員

川 口 貴 久 氏・・・13

### 佳作（教職員の意識向上賞）

テーマ：情報セキュリティ意識を向上させるための教育について  
教職員の意識向上のための

情報セキュリティ研修に関する一考察  
情報セキュリティ大学院大学 博士前期課程

星 野 進 氏・・・24

## 最優秀賞

情報セキュリティ意識を向上させるための教育について

～高校における教科「情報」授業実践事例から、  
今後のPC教育の在り方へ～

情報セキュリティ大学院大学 博士前期課程

藤巻 朗

## 1 はじめに

近年コンピュータや携帯端末が各家庭に普及し、誰でも簡単にインターネットが利用できるようになった。結果サイバー犯罪が増加し、子供たちがトラブルに巻き込まれることが多発している。そういった背景もあり 2003 年、高等学校に教科「情報」が初めて導入された。また、小学校では新学習指導要領が昨年度から一部先行実施され、道徳の中で「情報モラル」の指導に留意することに加え、他教科や総合的な学習の時間でもコンピュータを活用する機会が増えることになり、今後益々情報教育の重要性が叫ばれることとなる。そこで、情報セキュリティ意識を向上させるための教育について、教科「情報」の導入時から 6 年間情報科教員として実際に行ってきた勤務校での実践例を通して考察し、今後学校における PC 教育の在り方について述べていく。

## 2 学校の情報教育の現状

### 2-1 小中学校における情報教育

小学校には「情報」に関する科目は設置されていないが、総合的な学習や各教科で情報教育を行うこととしている[1]。しかし、内容については具体的に定められておらず、学校現場に任された状態ある。中学校では、技術・家庭科で情報に関する基礎的な内容が必修化されている[2]。しかし、学校選択項目があるなど、授業時数及び履修学年について地域・学校及び生徒の実態等に応じて、教える内容が統一されていない場合がある。そのため、高校に入学する新入生が、情報の授業を実施するにあたって難しい状況にある。実際 2010 年度入学当初の新入生 320 名対象にパソコンにおける情報リテラシー能力について、アンケート調査を行った。内容は各アプリケーションソフト等について実際に利用したことがある人数と、そのうち授業で習ったことがある人数についてのアンケート調査である。インターネットやワープロは大部分の生徒が利用しているが、プレゼンソフトで約 6 割、表計算ソフトで関数やグラフまで経験したものは半数以下となっており、高校入学前の情報活用能力は差があることが分かる。

表 1 : 情報活用能力アンケート結果 (筆者調査)

2010 年度新入生 320 名対象

	利用したことがある	授業で習った
インターネット・メール	97.8%	77.0%
ワープロソフト	82.0%	59.0%
表計算ソフト	54.6%	45.1%
プレゼンソフト	62.8%	57.4%
Web ページ作成	41.3%	14.2%

## 2-2 高等学校における教科「情報」

高等学校学習指導要領[3]によると、内容の詳細については省略するが、教科「情報」には「情報 A」、「情報 B」、「情報 C」の 3 科目が用意され、1 科目以上を選択して履修することとなっている。埼玉県の場合、普通高校の 70%以上が、「情報 A」を履修している[4]。情報 A は 3 つの中では最も一般的内容であり、学習指導要領では全授業の 1/2 以上実習を行うこととしている。勤務校では 1 年で全員に情報 A を履修させ、3 年で進路に応じた選択科目群に情報 B と情報 C を用意した。

表 2 : 2008 年度の埼玉県立高校における科目実施状況

	目標	実施校数	割合
情報 A	「情報活用の実践力」を養う	133	74.3%
情報 B	「情報の科学的理解」を養う	22	12.3%
情報 C	「情報社会に参画する態度」を養う	24	13.4%

(出典) 埼玉県立高校教育指導課 平成 21 年度教科「情報」スキルアップ研修会資料

## 3 実技と講義を融合させた教育の実践

情報 A は必修科目であるため、表 1 の差をなくすことで全員が統一した情報リテラシー能力を付けることを第 1 の目標とした。そこで、PC を使用する機会を増やすため全授業時間の 8 割以上を実習時間に充て、特に前期は Excel や PowerPoint 等の実習をできるだけ多く行なった。また、後述するが情報セキュリティ意識を向上させるため、アカウント管理・アクセス制御や知的財産権の項目は特に、ネットワーク環境を利用して効果的に知識を定着させるための教育を考えて実践した。それは実際に PC を使用する機会を増やし、実習を通じた体験の中から失敗することも含めて学ばせることであり、実技と講義を融合させることが大切である。その内容を以下に示す。

利用教材		
教科書	「高校情報 A」	実教出版
副教材	「30 時間でマスター Excel 2007」 「ケーススタディ情報モラル」 自作プリント (HP ビルダー操作マニュアル)	実教出版 第一学習社
ソフト	学校間ネットワーク (メール・インターネット) OfficePro2007 HP ビルダー	Microsoft IBM

### 3-1 コンピュータルーム環境

生徒用コンピュータは42台(OSはWindows Vista)で、2人に1台、真中に指導用モニタがある。生徒は、教員が教材等を指導用モニタ転送した画面を見ながら授業を行う。Windows ドメインによるクライアント・サーバシステムを構築しており、すべてのパソコンはユーザーIDとパスワードの入力が必要である。また、教材の配布やレポートの提出等はすべてファイルサーバ上の共有フォルダ上で行い、配布フォルダは読み取りのみ、提出フォルダは書き込みのみ許可されている。更に、環境復元ソフトによって授業終了後にすべての設定等が初期化される。ソフトウェアはOfficePro2007とホームページビルダが台数分インストールされている。インターネットは県の管理センター内のプロキシサーバに接続され、コンテンツによるフィルタリング管理を行っている。

### 3-2 セキュリティ意識の向上

#### アカウント管理

在籍生徒にはすべて入学と同時に、生徒ID、初期パスワード、メールアドレスを付与している。これらは3年間、情報以外の授業や特別活動等でも利用するものとする。生徒IDとメールアドレスは学籍番号+α、初期パスワードは乱数で英数字8文字(ただしIとl、qと9など入力ミスの原因となる数や文字は除く)である。

① 4月最初の授業でIDやパスワードを扱う上での留意点を説明し、初期パスワードを一度その場で変えさせ、以降は各自の責任で管理するよう強く指導する。この時、全員の確認は困難であるが、英数字を混ぜて8文字以上としている。

② 毎年数名程度、パスワード忘れや紛失等によりログインできない生徒が出てくるが、パスワードリセット申請書に、氏名・理由をきちんと書かせて担当者に提出する。

パスワードリセット申請書					
	年		組	番	氏名
ユーザーID					
理由					




図1 : パスワードリセット申請書例

手順を踏ますことで、自身の ID・パスワードを大切にすることを養うことができる。

### アクセス制御

課題の配布や提出をすべてアクセス制御された LAN 上で行う。

- ① ファイルの参照や変更等にはアクセス権限が必要であり、他人のファイルを参照しようとしたり、提出済みファイルの内容を変更しようとしても、アクセスが拒否される。  
これらの行為は、不正アクセス行為であることの意味が実感できる。また、書き込み権限のないフォルダ等へ、課題を誤って提出してしまうミスも防ぐことができる。
- ② 環境復元ソフトがすべてのパソコンにインストールされているので、自分のパソコンのデスクトップなどの指定場所以外に保存すると、シャットダウンの際に環境復元ソフトにより保存したファイルが削除されてしまう。こまめに上書き保存を行い、セキュリティ対策としてバックアップを取得しておくことの重要性も実感できる。失敗することも含めて、実習を通して体験させることを重視することにより、教科書程度のセキュリティ用語の理解や暗記へと発展していく。

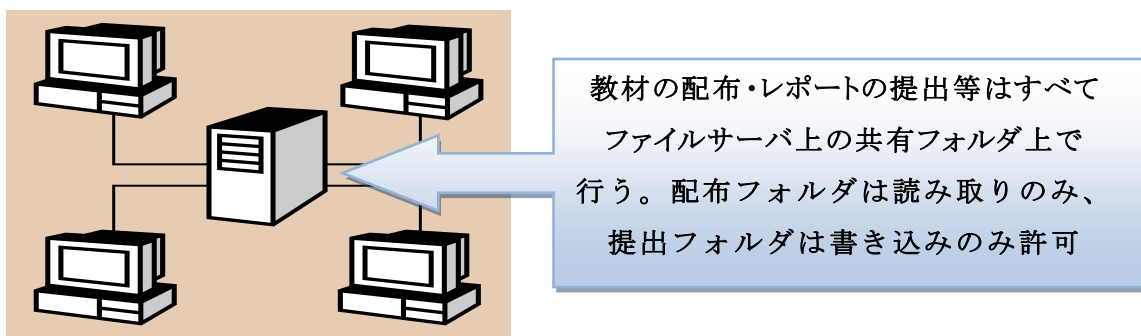


図 2 : アクセス制御

### 3-3 知的財産権

後期の 1 月から、「情報 A」の総まとめの総合演習として、グループ単位で Web ページ作成を行った。実習時間は 2 カ月程度（約 12～14 時間）を充てた。

#### 実習概要

- ① 総合演習として、Web ページ作成を行う。
- ② グループ単位で実習を行うが、コミュニケーション能力向上の観点から好きな者同士ではなく、出席番号順で 4 人 1 組とする。
- ③ コンピュータールーム内のみの公開とする。公開後相互評価を行い、修正後再提出する。

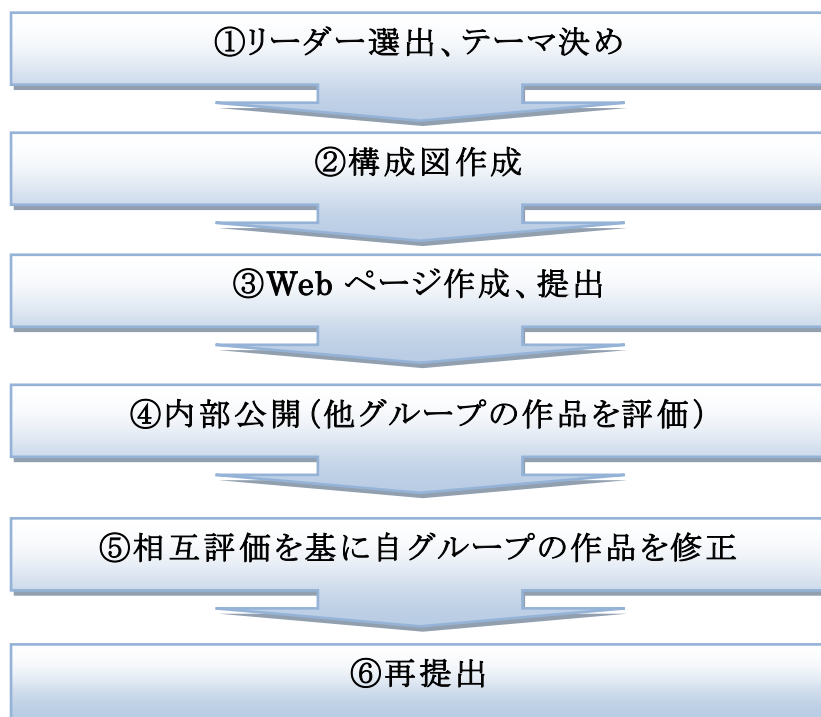


図 3 : Web ページ作成実習手順

**留意事項**

- ① グループ毎にテーマ・分担を決めるが、テーマは自由である。ただし内部ではあるが公開することが前提であることと、後述するが知的財産権の問題から、各グループ内で適切に判断する。また、ファイルサーバ内に、グループ毎の作業用フォルダを用意する。これは同じグループのメンバーのみアクセスでき、このフォルダ内で、メンバー同士のデータの共有や互いのページのリンク挿入作業等行なう。
- ② トップページからのリンク構成や各ページのファイル名を図示した、構成図を提出する。これにより、サイト管理や URL の仕組みについて理解できる。

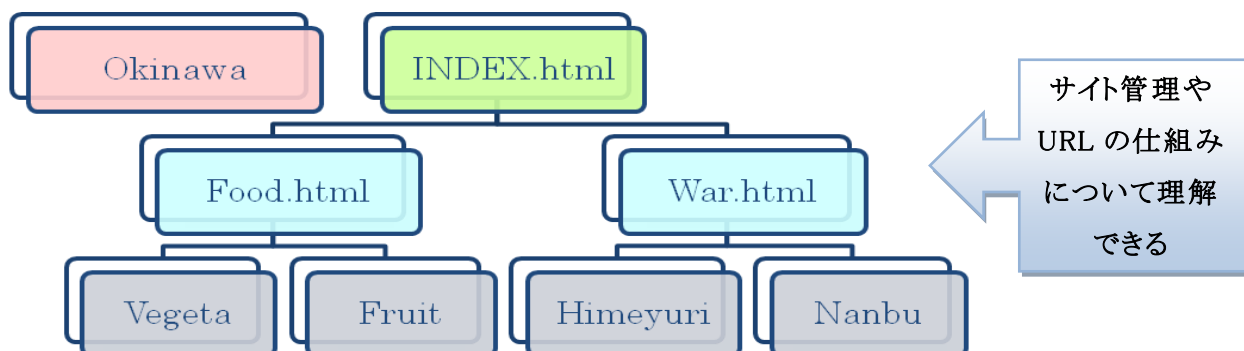


図 4 : 構成図例 (沖縄をテーマとした Web ページの場合)

③ Web ページ作成にあたり、他人のページの引用や写真等の利用を希望する場合は、希望者本人が直接、自分のメールアドレスで県立学校間ネットワークシステムを利用して利用許可願のメールを送信する。そして使用許可メールの受信、または正式な書類等で手続き完了したもの以外は利用させないことで、電子メールのマナーを覚えさせると共に、人の著作物を守ることの重要性を理解させる。また、CC 欄には授業担当者のアドレスを入れさせ、誰が、いつ、どこに、どのようなメールを送信したのかを担当教員が管理できるようにした。

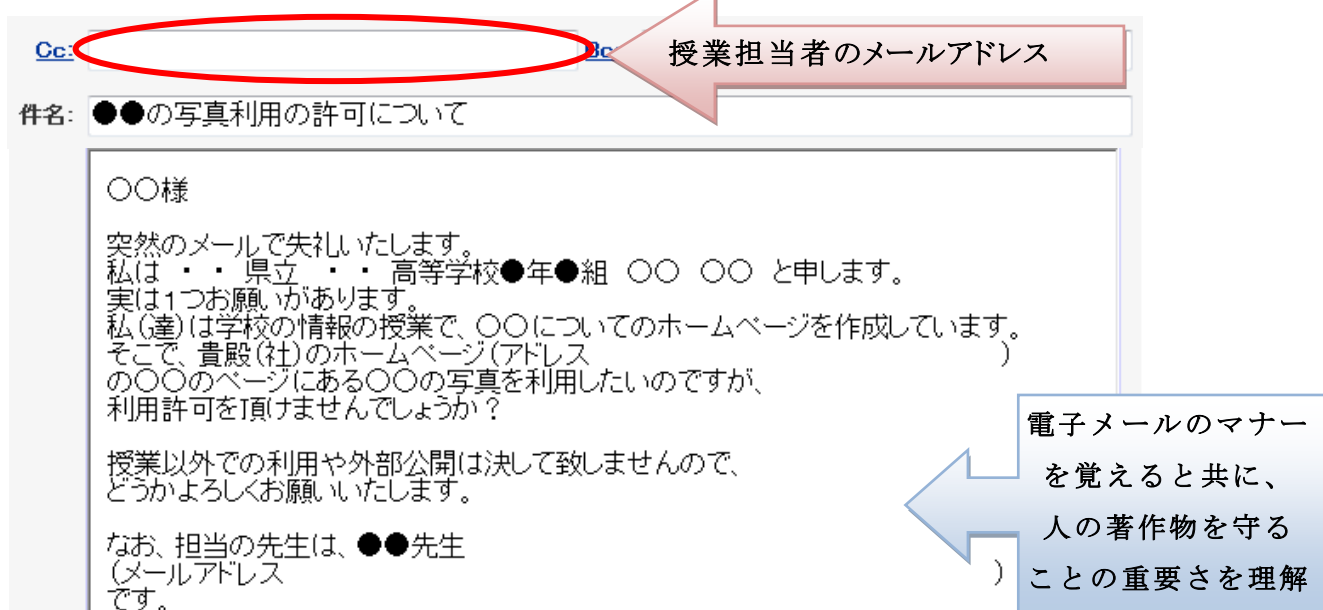


図 5 : 利用許可願メール例

実際テーマを自由に行っているため、最初は芸能人やアニメキャラクターについてのテーマに決めたグループが多い。しかし、芸能人の写真やディズニーなどのキャラクターの利用はパブリシティ権や商標権等の問題により、許可を得るのが非常に困難である。実際数グループは利用許可が得られなかった。その場合、問題点は何かをグループ内で考えさせ、全体の前で取り上げて、解説した。

- ④ 公開はコンピュータールーム内のみの公開とする。全員にチェックシートを配り、チェック項目に評価を 5 段階で記入させ、特に問題点がある場合は直接内容を記述して、各グループにフィードバックさせ、全体で取り上げた方が良い内容に関しては、全体の問題としていくつか取り上げて解説した。また例えば、ある子ども向け製菓に関する内容などで、教員目線では分からなかった問題点が生徒同士の相互評価の中で明らかになるような場合も多数見受けられ、情報発信の際の注意事項を考えるきっかけになった。
- ⑤ 修正では、④でチェックされた内容を中心に修正をしたものを再提出させる。これにより多くの人に分かりやすい情報提供を行うために

配慮する必要がある点（ユーザアクセシビリティ）について考えさせることができ、著作権や操作性については成績の評価に反映させた。

チェック項目	主な観点	評価
1. テーマや目的の到達度	ページの内容がテーマや目的と合っているか	
2. 文字や画像の配置	優先度を考慮した項目配置になっているか 文字や画像の間隔が狭く見にくい	
3. 操作性	多くの人が操作しやすいか	
4. 受信者の状況やネットワーク環境への配慮	閲覧者を配慮した内容・表現か 表示に時間がかかったりしないか	
5. 著作権・プライバシー	著作権違反やプライバシー侵害はないか	
6. デザインや色調などの統一性	判別しやすい配色を心掛けているか	
7. ブラウザでの正しい表示	ブラウザ上でページが正しく表示されているか	
8. 全体的な構造	リンクが複雑になっていないか	

**評価の観点**

著作権、肖像権  
個人情報など

図 6 : チェックシート例

### 付帯効果

Web ページ作成実習の中で、偶然に企業や大学と連携できた事例がある。

①ある製菓会社で製造している数種類の味があるアイスクャンディがある。好きな味を校内でアンケートを取り、その人気ランキングの Web ページを作成したグループがあった。パッケージの写真の利用許可願のメールを送信した際、製菓会社の広報担当者より、逆にその Web ページを見せて欲しいとの依頼があり、可能な範囲でお互い情報交換して完成した。企業とうまく連携して効果があった事例である。

②チョコレートに関する Web ページを作成したグループは、ある大学の研究室のサイトの中に、チョコレートの原料である植物の写真を見つけ、引用許可願のメールをサイト管理者である教授宛に送信したが、「以前に研究室に所属したある国からの留学生が、無断で他のサイトからアップしたものであり、削除予定だったが忘れていた」という連絡を受けた。この事例は全体の問題として考えた方が良くと考え、「日本と外国の知的財産意識の違い」として、「情報」の授業教材で利用する許可を頂き利用した。

大学と連携できた事例である。

## 4 効果と課題

実技と講義をうまく融合させた教育の効果と課題について、2007、2008 年度の期末考査試験の問題より ID・パスワード、セキュリティ用語及び知的財産権に関する部分の一部を示し、その正解率から考察する。

### 4-1 期末考査問題概要

情報 A の定期考査は、前後期それぞれ 1 回ずつ期末に行っている。解答はすべてマークシート方式であり、○×2 択式から、5 択式までである。（受験者数 320 名）

時期	型式	主な範囲
前期 (7月実施)	マークシート方式、 70問前後	ID・パスワード、Web・メール・ インターネット・コンピュータの仕組み、他
後期 (3月実施)	マークシート方式 60問前後	個人情報、セキュリティ、知的財産権、 情報社会への参加、他

### 問題（一部）[5]

次の文の内容や行動が正しいときは○、間違いならば×をマークせよ。

- ① パスワードを忘れると困るので、メモした紙をパソコンに張り付けおいた
- ② IDとは識別をするための名称のことで、氏名などと同様に重複することがある
- ③ 利用開始時に設定された初期パスワードは直ちに変更した方が良い
- ④ パスワードは、英数字や記号などできるだけ多くの文字種を使う方が良い

次の文は、セキュリティに関連する用語を説明したものである。何の用語の説明か。

- ⑤ 有害な情報を排除し、必要な情報のみを選別する仕組み
- ⑥ インターネットなど外部のネットワークと会社や学校など内部のネットワークを  
分けて、外部から不正アクセスを受けないようにする仕組み
- ⑦ 目的の受信者以外に情報を盗聴されないようにする技術
- ⑧ ある人物が、本当にその人物（当人）であるかを、確認すること

次の行為はどのような権利を侵害しているか。

- ⑨ 自分が撮影した、友人が写っている写真を無断で Web ページに掲載した
- ⑩ バッハの曲が収録されている市販の CD をコピーして配布した
- ⑪ 有名アイドルの名前を使って、宣伝に利用した
- ⑫ Web ページに、他人の私生活の情報を本人が特定できる表現を使って無断で  
公表した

### 正解率が低い問題[5]

次の文の（ ）にあてはまる語句を書け。

知的財産権は大きく分けると、（1）権と著作権がある。そのうち前者は、発明に関する特許権、デザインに関する（2）権、考案に関する（3）権、マークなどに関する商標権に分けられる。これらはいずれも、（4）庁に出願し認められることによって初めて、その権利が保護される。一方後者は出願や登録の必要がなくその著作物の（5）の時点で自動的に権利が発生する。また著作者の死後（6）年を過ぎると、著作権は消滅する。

#### 4-2 期末考査正解率から

表 3 : ①～⑫の年度毎の正解率

	①	②	③	④	⑤	⑥
2007年度	—	55.5%	—	91.4%	54.2%	36.8%
2008年度	79.4%	82.6%	93.5%	—	60.4%	52.3%
	⑦	⑧	⑨	⑩	⑪	⑫
2007年度	62.3%	88.5%	75.4%	52.6%	66.0%	75.4%
2008年度	75.9%	96.3%	90.4%	54.5%	58.5%	78.9%

定期考査	
平均点	
2007年	59.0
2008年	64.8

注) 2007年度①③、2008年度④出題せず

(1) ID、パスワードについての問題①～④より、2択式問題からだけでは効果の測定にはならないが、パスワードの扱いについては意識できた生徒が多いと思う。しかし、紙に書いて張り付けることの危険性や初期パスワードの扱いなど、今後の生活の中でパスワードを設定する機会あるときにも意識できるように定着させることが必要である。⑧の認証の意味は、毎回ログイン・ログアウトを繰り返していることで、経験的に理解出来たのではないか。

(2) セキュリティ用語の問題 ⑤～⑧は⑥のファイアウォールなど初めて出てくる用語の意味の定着が低い。実際、高校生にファイアウォールの設定を行うなどの実習は困難であるので、授業ではアクセス制御の関連として説明したが、ネットワーク図を図示して細かく説明するなどの工夫が必要であった。⑤のフィルタリングは、普段の授業の中でインターネットを利用する際に体験しているので、もう少し高い正解率が望まれるが、携帯電話を例にした方がもう少し身近に感じられ良かったかもしれない。なお⑤はアクセス制御、⑥は不正アクセス禁止法とする誤答が多かった。⑦の暗号化は、暗号化の鍵の例として、「文字を50音順に次の文字にずらす」ことを説明したが、他の例を何か考えさせて、発表させるような実習も考えられる。

(3) 知的財産権の問題⑨～⑫は⑩の著作隣接権の意味が苦手な生徒が多い。誤答のほとんどは頒布権である。パッハは死後50年以上経過しているので直接著作権侵害ではないが、CD作成者や演奏家への権利の意味が苦手なようだ。いかに実習の中で定着させるかが課題である。肖像権やパブリシティ権は、実習の効果が大きい。実際に、許可を得ながらWebページを作成し、相互評価をしていく中で、情報発信の際の心構えが意識できたようだ。やはり知的財産権は、法律の知識が乏しいこともあり用語の暗記や法律の条文を読むだけではどうしても定着しない。情報教育には絶対避けては通れないので単元なので、この分野こそ実技と講義をうまく融合させることが大切である。

### 正解率が低い問題

知的財産権の分類や保護期間などは、教科書の本文や図表を暗記することが大半の内容であり、他の分野の問題と比較して正解率が低い結果となっている。

表 4 : 各問の年度毎の正解率

	(1)	(2)	(3)	(4)	(5)	(6)
2007年度	63.3%	53.3%	67.3%	39.7%	42.0%	85.0%
2008年度	52.6%	33.0%	45.8%	29.6%	53.0%	92.2%

教科書では、本文での説明と表が主である。実際に PC を利用しにくい単元であり、用語の正確な暗記や理解が求められる。このような分野にも、実技と講義を融合させる方法を考えていくことが課題となる。

全体的にみて、暗記が問われる設問よりも実習で行った範囲の設問の方が、平均点よりも正解率は高い。一部、実習の内容について検討する課題は残るが、やはり、実技と講義を融合させた教育が効果的であると言える。今後も、実際に PC を使用する機会を増やし、実習を通じた体験の中から失敗することも含めて学ばせることが必要になる。

## 5 新学習指導要領と今後の情報教育

新しい小学校学習指導要領および中学校学習指導要領が 2008（平成 20）年 3 月に告示され、高等学校学習指導要領が 2009（平成 21）年 3 月に告示された[6]。内容については省略するが、新学習指導要領では小学校から情報モラル教育に留意し、系統立てた情報教育を目指している。そのためには、実際に情報機器を使用する機会を増やし、体験の中から学ばせることが大切であり、そのために実技と講義をうまく融合させた教育は小中学校にも拡張できる。特に小学校では機器をパソコンよりも携帯電話やゲーム機を対象にして、プロフや掲示板などを題材にしていく方が効果的ではないか。例えば、プロフ等のサンプルサイトを使って、実際に投稿させて内容等について討論し合う実習や、親と一緒に携帯電話やネット利用のルール作りを行う演習などが考えられる。

## 6 参考文献

- [1] 文部科学省 小学校 現行学習指導要領
- [2] 文部科学省 中学校 現行学習指導要領
- [3] 文部科学省 高等学校 現行学習指導要領
- [4] 埼玉県立高校教育指導課 平成 21 年度教科「情報」スキルアップ研修会資料  
2009 年 8 月
- [5] 実教出版 高校「情報 A」 教科書
- [6] 文部科学省 小学校・中学校・高等学校 新学習指導要領

佳作（サイバーディフェンス賞）

サイバー空間における「抑止」についての一考察：  
国家安全保障政策の視点から

東京海上日動リスクコンサルティング株式会社 研究員

川口 貴久

## はじめに

エストニア（2007年4月）、米・韓の中央官庁（2009年7月）、インターネット掲示板「2ちゃんねる」（2010年3月）へのサイバー攻撃や「中国とGoogle」問題などを契機として<sup>1</sup>、情報セキュリティの重要性がこれまで以上に高まっている。このような状況下で、各国は国家安全保障政策として、サイバー空間の安全確保に取り組み始めた。2010年5月末、『米国家安全保障戦略』は「デジタル・インフラストラクチャーは戦略的国家資産であり、この防衛は...中略...国家安全保障上の優先事項<sup>2</sup>」と位置付け、サイバー安全保障政策を明示的に展開した。また日本でも、「新たな時代の安全保障と防衛力に関する懇談会」で情報セキュリティがテーマとして扱われ、次期『防衛大綱』でサイバー安全保障の重要性が従来以上に高まると推測される<sup>3</sup>。

しかし、サイバー空間の国家安全保障政策の必要性が高まる一方で、その具体的な政策体系・メカニズムが描き切れていないのが現実である。政策体系や理念がなければ、情報セキュリティに関する個々の政策（技術開発、法整備、パートナーシップ構築など）は非効率かつ非効果的な投資に終わってしまうだろう。

そこで本論はサイバー空間の国家安全保障の政策体系・メカニズムとして、「抑止（deterrence）」を提起してみたい<sup>4</sup>。抑止とは「相手に、

---

<sup>1</sup> 2006年以降の主な事件については、James Andrew Lewis, “Cyber Events Since 2006,” Center for Strategic and International Studies (last modified: April 20, 2010).

<sup>2</sup> Barack Obama, *National Security Strategy of the United States* (Washington D.C.: White House, May 2010), pp.27-28. また、2010年2月、米国家情報長官のブレア（Dennis C. Blair）は上院・インテリジェンス委員会へ報告書『年次脅威評価』を提出したが、同報告書はグローバル経済危機やテロよりも「サイバー脅威の広範囲なインパクト」を筆頭にあげ、その重要性を強調している。Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, Senate Select Committee on Intelligence (February 2, 2010), pp.2-4.

<sup>3</sup> というのも、過去の慣例を踏まえると、「新たな時代の安全保障と防衛力に関する懇談会」は次期防衛大綱策定に多大な影響を与える有識者会議である。情報セキュリティがテーマとなったのは、第7回懇談会（2010年5月25日）。また、[日本]情報セキュリティ政策会議も「サイバー空間の安全保障・危機管理」政策を強化していくことを提案している。情報セキュリティ政策会議「国民を守る情報セキュリティ戦略（案）」（内閣官房情報セキュリティセンター、2010年5月11日）。

<sup>4</sup> サイバー空間の安全保障を論じたものとして、Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Cyberpower and National Security) (Washington, DC: National Defense University and Potomac Books, 2009); Greg Rattray, Chris Evans, Jason Healey, “American Security in the Cyber Commons,” in Abraham M. Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World* (Center for New American Security, January 2010), pp.137-176; Joseph S. Nye, *Cyber Power* (Belfer Center for Science and International Affairs, May 2010). 特にサイバー空間での「抑止」について検討したものとして、

さもなければ実行したであろう行為を思いとどまらせること」である（詳細は後述）。サイバー空間で悪意ある攻撃を抑止することは可能なのだろうか。結論を先取りすれば、多様なサイバー脅威を包括できる「テイラーメイド型のサイバー抑止（cyber deterrence tailored）」が、サイバー空間の安全保障政策メカニズムとして機能するだろう。

本論はまず、サイバー空間における国家安全保障政策と個別の試み（技術開発やパートナーシップ構築など）をつなぐ政策体系・理念として「抑止」を提起する【第1節】。「抑止」には様々な形態が存在するが、ある1つの「抑止」形態であらゆるサイバー攻撃を防ぐことは困難である。サイバー攻撃を抑止するには、国家、テロリスト、群衆といったサイバー脅威主体に応じた「テイラーメイド型の抑止」が不可欠である。【第2節】。そして、「テイラーメイド型の抑止」をサイバー安全保障政策の原理・メカニズムと位置付けた上で、技術革新への投資やパートナーシップ構築などの必要とされる個別政策を検討してみたい【第3節】。

## 1. サイバー安全保障の政策体系・理念としての「抑止」

サイバー空間の秩序は変化の中にある。ガバナンス面では、2009年7月のICANN（**Internet Corporation for Assigned Names and Numbers**）問題の「決着」<sup>5</sup>に見られるよう、アメリカ中心の秩序から多角的メカニズムに移行している。アーキテクチャの面でも大きな変化が訪れているが、「クラウド」化やIPv6（**Internet Protocol Version 6**）への移行は安全保障上の脆弱性を高めてしまう面もある。例えば、ICTビジョン懇談会で指摘された「霞が関クラウド」構想<sup>6</sup>は業務効率を高める可能性を持つ一方で、政府機能へのサイバー攻撃に対する脆弱性を高めてしまう。あるいは、巨大なクラウド環境にマルウェアを組み込むことで、クラウド利用者を「ボット」化することも想定される。

---

Richard L. Kugler, “Deterrence of Cyber Attacks,” in *Cyberpower and National Security*, pp.309-340; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND, 2009); Thomas J. Mowbray, “Solution Architecture for Cyber Deterrence,” *SysAdmin, Audit, Network, Security: SANS Institute* (April 12, 2010); James Andrew Lewis, “Cross-Domain Deterrence and Credible Threats,” *Center for Strategic and International Studies* (July 2010).

<sup>5</sup> この「決着」は端的に言えば、ICANNに対するアメリカ国務省の影響力の低下である。ICANNとはIPドメイン割当やルートサーバの運用を行う非営利団体である。ICANNの役割と米商務省との問題については、Kenneth Neil Cukier, “Who Will Control the Internet? Washington battles the world,” *Foreign Affairs*, Vol.84, No.6 (November/December 2005), pp.7-13.

<sup>6</sup> ICT懇談会「スマート・ユビキタスネット社会実現戦略」ICTビジョン懇談会報告書（2009年6月）、5頁。

こうした状況下で様々なアプローチが試みられている。技術革新は最も重要なアプローチであり、特に DDoS 攻撃 (Distributed Denial of Service attack) への対処や SCADA (Supervisory Control And Data Acquisition) システムの防護は最も関心あるテーマであろう。更に、国内及び二国間・多国間の法整備や官民連携といったパートナーシップ構築もサイバー空間の安全を確保する上で欠かせない取組である。

しかし、元内閣官房情報セキュリティ補佐官・山口英を始め多くの論者が指摘しているように<sup>7</sup>、「技術は重要だが、技術だけで問題は解決できない」。法整備やパートナーシップ構築も同様である。こうした試み（技術開発、法整備、パートナーシップ構築）の重要性は言うまでもないが、より重要な点はこれら個別政策を体系化し、全体としての方向性を提示する事である。そして、それは「サイバー空間の国家安全保障政策」というスローガンだけでは不十分であり、より具体的な政策体系や理念を必要とするのである。

その政策原理の1つとなりうるのが、「抑止 (deterrence)」である。抑止とは、相手の「否定的な動機に働きかけることで、事前に与える影響力の一形態<sup>8</sup>」、より簡単に言えば、「相手に、さもなければ実行したであろう行為を思いとどまらせること」である。「抑止」は第二次世界大戦後の（国家）安全保障研究・政策で決定的に重要な位置を占めてきた。実際に核兵器を中心とする抑止体制が米ソ冷戦に「危機の中の安定性」をもたらした、という見解は主流である。

もっとも、サイバー空間での「抑止」は論争的なテーマである。米国家安全保障局長官兼サイバー軍司令部司令官のアレクサンダー大将 (Gen. Keith Alexander) でさえも、サイバー抑止の実現可能性についてポジティブな言及を避けている<sup>9</sup>。また、サイバー空間で抑止は機能しないという見解は根強い。否定論者によれば、サイバー攻撃者の費用便益

---

<sup>7</sup> 「次世代インターネットを探る 第2回 山口英氏」IPv6style (2007年7月27日) 【<http://www.ipv6style.jp/jp/20070730/ngin02.html>】 2010年6月20日アクセス

<sup>8</sup> Jeffrey W. Knopf, "Three Items in One: Deterrence as Concept, Research Program and Political Issue," in T. V. Paul, Patrick M. Morgan & James J. Wirtz, ed., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, 2009), p.37.

<sup>9</sup> Speech by Gen. Keith Alexander, Director, National Security Agency, Commander, U.S. Cyber Command, "CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," Center for Strategic and International Studies (June 3, 2010) Transcript; Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command, US Senate Armed Service Committee (April 15, 2010). アレクサンダー大将を含めた米政府高官や研究者のサイバー抑止についての見解は、John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times* (January 26, 2010)

計算は攻撃を「思いとどまる」という結論に結びつきにくい。加えて、サイバー抑止の否定論者は特に次の2点を主張する。第一に、サイバー攻撃の主体を特定することが難しい点、いわゆる「帰属問題 (attribution problem)」である。更に、善意の第三者アセットを利用したサイバー攻撃 (ボット攻撃) などは「真の攻撃主体」を隠してしまう。第二に、ある行為 (刺激) を敵対的行為と認定することが難しい「閾値問題 (threshold problem)」である。例えば、DDoS 攻撃の主要な方法として、ネットワークやサーバに過剰なリクエストを送信することが想定されるが、悪意あるリクエストと通常のリクエストを区別することは難しい。

このような理由で悲観論が溢れているが、「抑止」は機能するかしないかの二者択一の問題ではない。「抑止は最良の戦略だ」「抑止は機能しない」といった包括的な言明 (blanket statement) は避けなければいけない。新しい安全保障環境下で、抑止は成功する可能性もあれば失敗する可能性もある<sup>10</sup>。重要な事は、どのような状況下で抑止が機能するのか、そのためにはどのような分野に資源を投入するのかを明示することである。

## 2. テイラーメイド型のサイバー抑止 (cyber deterrence tailored)

### (1) 「抑止」の多元性

実際、「抑止」の概念は (部分的ではあるが) サイバー空間の安全保障政策に取り入れられている。2010年3月に公表されたアメリカの『包括的国家サイバー安全保障イニシアティブ (Comprehensive National Cybersecurity Initiative: CNCI)』は、その具体的取り組みの1つとして「揺るぎない抑止戦略及びプログラムの構築・発展」を掲げている<sup>11</sup>。だが、CNCI中の「抑止」は冷戦時代のそれとは異なる哲学を要求している。冷戦時代の膠着した「にらみ合い」型はサイバー空間では全く十分ではない。オバマ政権の国防副長官リン (William J. Lynn, III) は次のように指摘している。

<sup>10</sup> Knopf, "Three Items in One," p.53; Kugler, "Deterrence of Cyber Attacks," p.329.

<sup>11</sup> 「今日まで、米国政府はサイバーセキュリティの問題について伝統的アプローチを実践してきた。そして、こうした手法は必要とされるレベルの安全保障を達成しえなかった。そこで、CNCIは新しいサイバー防衛戦略を構築することを目的としている。この新しい戦略とは、警戒能力の向上、民間セクターの役割や国際的パタンの明確化、国家及び非国家主体への適切な対応能力の構築を通じて、サイバー空間における妨害及び攻撃を抑止するものである」 *Comprehensive National Cybersecurity Initiative* (March 2, 2010)

1度のクリックは0.3秒で地球を2周する。その一方で、攻撃元を特定するのに必要な捜査は数カ月を要する。リアルタイムで攻撃元を特定できなければ、我々の抑止プログラムは破綻する。ミサイルは「返信先」を明らかにしてやってくるが、サイバー攻撃の多くはそうではない。こういった理由で、抑止についての既存モデル（established models of deterrence）はサイバー空間には全く当てはまらない。現在および将来の脅威に対処するために、我々が必要としている抑止構造は攻撃的であり、防衛的であり、インテリジェンス・オペレーションであり、これらを融合させたものなのである<sup>12</sup>。

言い換えれば、サイバー空間での「抑止」は単一のメカニズムに依拠するのではなく、多様なメカニズムからなる複合的形態でなければならない。今日、「抑止」といえば、報復的行為を示唆することによる「懲罰的抑止（deterrence by punishment）」が一般的であろう。だが、抑止には多様な形態が存在する【表1を参照】。

懲罰的抑止が相手の生存合理性に訴えかけるならば、相手の目的合理性に訴えかける「拒否的抑止（deterrence by denial）」という形態も存在する。例えば、一般的に「偏狭な信仰心に基づくテロリストは合理的でない」と考えられるが、彼／彼女らは生存合理性を持ち合わせていなくとも、目的合理性を兼ね備えている場合が多々ある。その場合、拒否的抑止が機能する。つまり、「報復する」というメッセージには効果がないが、「あなたの行為や目的は達成されない」というメッセージは抑止として機能しうる<sup>13</sup>。

また、抑止主体という観点では、同盟国やパートナーが抑止機能を提供する「拡大抑止（extended deterrence）」型も重要である。懲罰的抑止能力であれ拒否的抑止能力であれ、自国で「抑止」の実効性を高められない場合、連携によって抑止能力を確保することが必要となる（日本であれば、日米同盟が拡大抑止の典型例）。

こうした「抑止」の多元性に着目して、様々な抑止政策が主張・展開

---

<sup>12</sup> William J. Lynn, III, Deputy Secretary of Defense, “Remarks at STRATCOM Cyber Symposium,” Omaha, Nebraska (May 26, 2010) US Department of Defense 【<http://www.defense.gov/speeches/speech.aspx?speechid=1477>】 2010年6月20日アクセス

<sup>13</sup> 詳しくは、神保謙、高橋杉雄、古賀慶『日本の対テロリズム政策：多層型テロ抑止戦略の構築』東京財団研究報告書（2005年2月）、6-7頁。

されている。相互依存関係の深化に伴う（主に中国を意図した）「リベラル抑止」は、新興国とのサイバー戦争を抑止する可能性を持つ<sup>14</sup>。ルイス (James Andrew Lewis) がいう「ドメイン横断的な抑止 (Cross-Domain Deterrence)」はサイバー抑止をサイバー空間に限定せず、幅広い文脈で構築するものである<sup>15</sup>。

表 1 : 「抑止」の構成要素

【主体】 誰が？	基本抑止 (central deterrence) ...自らが抑止する。	拡大抑止 (extended deterrence) ...同盟国・パートナーが抑止する。
【手段】 どのような論理で？	懲罰的抑止 (deterrence by punishment) ...報復的行為を示唆することで抑止する。	拒否的抑止 (deterrence by denial) ...相手方の行為が達成不可能であると示唆することで抑止する。

出典 : Lawrence Freedman, *Deterrence: Themes for the 21st Century* (Cambridge : Polity Press, 2004), pp.26-42.を基に筆者改編。この場合、4通りの抑止型（主体 2×手段 2）が想定されよう。また、抑止の構成要素として、フリードマンは以上に加えて「状況（有事 or 平時）」「対象の行為（軍事行動 or あらゆる敵対行為）」を挙げている。しかし、サイバー空間の安全保障を考察する上で「状況」「対象の行為」は省略した。

## （２）サイバー脅威の多様性と「テイラーメイド型の抑止」

このように「抑止」は多元的な形態が存在するが、同様に、サイバー空間の脅威も多様である。脅威の多様性を構成する要素として、サイバー攻撃の主体、方法、ツール、攻撃対象などが挙げられよう。脅威の主体について言えば、中国のような「台頭する国家」からイランや北朝鮮のような「ならず者国家」、テロリストや犯罪組織、群衆や個人（内部犯含む）にまで至る。

こうしたサイバー脅威の多様性をふまえれば、国家安全保障政策としてある 1つの抑止型を提示することの限界は自明である。それゆえ、求められるサイバー空間での「抑止」は「どんなものにも合う (one fits all size)」のではなく、多様なサイバー脅威を念頭におきながら、それぞれ

<sup>14</sup> 植木 (川勝) 千加子「世界構造変動と日米中関係 : 『リベラル抑止』政策の重要性」『国際問題』No. 586 (2009年11月)、15-28頁。

<sup>15</sup> James Andrew Lewis, "Cross-Domain Deterrence and Credible Threats," Center for Strategic and International Studies (July 2010), p.3.

ルイスやナイ (Joseph S. Nye) が論じるように、サイバー空間の安全保障を検討する場合、それはサイバー空間だけに限定されない。現実の物理インフラ（サーバ、ケーブルなど）への攻撃を抑止することも重要である。しかし、紙幅の都合により、本論は「サイバー空間を通じて行われる攻撃」のみを対象とする。

に最適の抑止型を提供する「テイラーメイド (tailored)」でなければならぬ<sup>16</sup>。そこで、本論はサイバー脅威の主体に応じた「テイラーメイド型の抑止」を提示する。より具体的には、サイバー脅威を①国家・準国家組織、②高度にネットワーク化された組織、③緩やかなネットワークに類型化し、それぞれの脅威特徴と「抑止」について検討してみたい<sup>17</sup>。

第一に、ヒエラルキー構造をもった国家や準国家組織である。ロシア国内が発信源とされるエストニア（2007年4月）、グルジア（2008年8月）、へのサイバー攻撃は、国家間のサイバー戦争の現実性を高めた。このような状況の中、アメリカは米統合軍サイバー司令部（US Cyber Command: CYBERCOM）<sup>18</sup>を新設し、同司令部が今年5月から始動している。国家・準国家組織はサイバー攻撃のための独自のインフラを持ち、それを支える官僚制・財源・インテリジェンス機関を兼ね備えている。だが、懲罰的メカニズムを中心とする国家間のサイバー抑止は成立しうる。その際、重要な点は、あるサイバー攻撃の発信元を特定することである<sup>19</sup>。また、懲罰的抑止の効果を高めるための同盟国による抑止力の提供（拡大抑止）はサイバー空間でも十分応用可能である。

第二に、高度にネットワーク化された組織、特にテロリストや国際犯罪集団である。こうしたグループは政府の機密情報（次世代戦闘機情報など）の剽窃や重要インフラ（電力・通信・金融など）への侵入を試みている。例えば、2003年以降に米政府ネットワークや軍需産業に組織的ハッキングを繰り返している「タイタン・レイン (Titan Rain)」や中国

---

<sup>16</sup> テイラーメイド型抑止については、神保謙「安全保障」、日本国際政治学会編『学としての国際政治』日本の国際政治1（有斐閣、2009年）、142-144頁。神保によれば、「テイラーメイド型抑止」のアイデアは米国防省のヘンリー（Ryan Henry）に求められる。

<sup>17</sup> サイバー脅威の分類は、Joseph S. Nye, *Cyber Power* (Belfer Center for Science and International Affairs, May 2010), p.10を参照した。また、注16のヘンリーは攻撃主体別の「テイラーメイド型の抑止」を提示したが、彼は「台頭する国家」「ならず者国家」「過剰な暴力主義」に分類している。神保、同上。

<sup>18</sup> 「統合軍 (Unified Combatant Commands)」とは1986年のゴールドウォーター＝ニコルズ法によって組織された司令部単位であり、陸・海・空・海兵隊の四軍種から構成される。現在、北方軍、南方軍、欧州軍、中央軍、アフリカ軍、太平洋軍（以上、地域別統合軍）、戦略軍、輸送軍、特殊作戦軍、統合戦力軍（以上、機能別統合軍）が組織されている。

<sup>19</sup> Nye, *Cyber Power*, p.16.

表 2：サイバー脅威とそれぞれの対応

サイバー脅威の主体	サイバー攻撃を抑止するための主要ポイント
国家・準国家組織	<ul style="list-style-type: none"> <li>・懲罰的抑止</li> <li>・サイバー攻撃の発信元の特定</li> <li>・拡大抑止</li> </ul>
高度にネットワーク化された組織 (テロリストや犯罪組織)	<ul style="list-style-type: none"> <li>・懲罰的抑止</li> <li>・「先制行動」「抑制」との補完</li> </ul>
緩いネットワーク (群衆)	<ul style="list-style-type: none"> <li>・刑事懲罰の導入 (懲罰的抑止)</li> <li>・サイバー攻撃の認定</li> </ul>

出典：筆者作成

の検索エンジン「百度」のウェブサイトを改ざんした「イラン・サイバー軍」は顕著な例であろう。またアル・カーイダ等によるサイバーテロは常に警戒されている。彼らは政府とは異なって、大規模なアセットを保有しない事で機動性と柔軟性を獲得している。そして、サイバー攻撃のアクセス元を明らかにしたところで、懲罰的抑止は機能しにくい。こうした類のサイバー攻撃を未然に抑止することができるのは、拒否的抑止のみであろう。また「抑止」は、脅威が実害となる前に対処する「先制行動 (preemptive action)」や抑止が必要でない環境形成を意図した「抑制 (dissuasion, dissuading)」と補完的に展開される必要がある<sup>20</sup>。

第三に、緩いネットワーク (群衆や個人) によるサイバー攻撃である。2010年3月、インターネット掲示板「2ちゃんねる」のサーバが機能不全に陥り、復旧までに数日を要した。「2ちゃんねる」は娯楽の側面が大きいが、コミュニケーションの不通がもたらす社会的・心理的ダメージは小さくない。そして、このサイバー攻撃は韓国の一般ユーザーによる DDoS 攻撃であったと推測されている。だが、こうした攻撃主体同士の「つながり」は薄く、細分化すれば「普通の個人」である。それゆえ、懲罰的ロジックが通用する余地が大きく、刑事罰則による懲罰的抑止は機能しうる。だからこそ、国内・国際的な刑事訴訟・損害賠償の法制度化が必要である。その一方で、「抑止」を機能させる上での課題は残る。こういったサイバー攻撃は通常のアksesとの判断がし難く (不特定多

<sup>20</sup> US Department of Defense, *Quadrennial Defense Review Report* (February 6, 2006); The White House, *The National Security Strategy of the United States of America* (September 17, 2002).

数が通常スペックの PC で F5 [リロード] を連打すれば、DDoS 攻撃に転化する)、ある行為を「悪意」と認定する技術設計が要求される。

### 3. 実効的なサイバー安全保障に向けて

以上のように本論は、サイバー空間の国家安全保障政策の中核として「テイラーメイド型の抑止」を提起した。こうした政策体系・理念を提示した上で個別の政策を論じたい。それらは大きく分けて、「技術革新への投資」「重層的なパートナーシップの構築」「法制度の整備」の3点に大別されよう<sup>21</sup>。

「技術革新への投資」はサイバー空間での「抑止」にとって重要な要素である。だが、資源（財政的な面でも人的な面でも）は限られており、投資対象に優先順位を付けることが求められる。第一に、サイバー攻撃への防衛能力の向上である。DDoS 攻撃でのリクエスト処理能力の向上や「論理爆弾」検知は攻撃主体の目的合理性に働きかけ、拒否的抑止の向上に資する。第二に、サイバー攻撃元の鑑識技術の向上である。これは、サイバー攻撃元を明らかにすることで、懲罰的抑止効果（報復措置）を高めることとなる。近い将来では、クラウド環境を利用したボット攻撃への対応（真の攻撃元の特定）が必要となろう。第三に、サイバー攻撃を受けた場合の被害を最小限にする結果管理能力（consequence control）の向上である。

また、今日のサイバー安全保障政策は単独（単一の政府）で確保することは出来ず、「重層的なパートナーシップの構築」が必要とされる。第一に、拡大抑止のネットワークを拡大・深化させることが重要である。同盟（日米安保条約、日豪・日印安全保障共同宣言）のアジェンダにサイバー攻撃への対処を盛り込むことで、サイバー脅威への懲罰的抑止の効果を高めていかなければならない。第二に、サイバー安全保障にかかわる官民連携を深化させる必要がある。海空宇宙といった他の安全保障空間に比べ、サイバー空間は私的領域が果たす役割・影響力は大きく、民間セクターと行政セクターの連携は不可欠である。具体的な取り組みとして、国家安全保障政策という観点では省庁横断的な官民連携スキームを形成する必要がある<sup>22</sup>。

---

<sup>21</sup> オバマ政権もサイバーセキュリティの重点施策として、“Investing in People and Technology”と“Strengthening Partnerships”の2点を強調している。Obama, *National Security Strategy of the United States of America*, pp.27-28.

<sup>22</sup> アメリカでは、官民連携スキームが省庁をまたがって数多く存在することが問題

更に、サイバー空間の安全確保のための「法制度の整備」は今後大きな前進の余地がある。特に「抑止」という観点からは、二国間・多国間取極めによる在外個人・団体への刑事訴訟や賠償請求スキームを構築することが優先課題であろう。

## おわりに

今日、サイバー空間の国家安全保障政策の必要性が高まっているが、重要な点は個々の取り組みを統合するような政策体系や理念の提示である。そして、その体系や理念の1つは本論が提示した「抑止」である。もちろん「抑止」は万能ではないが、機能する局面は大きい。しかし、サイバー空間での「抑止」は単一メカニズムに依拠するのではなく、サイバー脅威ごとに最適な形態をもった「テイラーメイド」でなければならない。国家・準国家組織、テロリスト・犯罪組織、群衆ごとに適した形でのサイバー抑止政策を構築する必要がある。こうした政策体系が存在してこそ、技術開発への投資・多面的パートナーシップ・法整備といった個々の政策がより実効的かつ効率的なサイバー安全保障に結び付くだろう。

---

視されている。Melissa Hathaway, “Why Successful Partnerships are Critical for Promoting Cybersecurity,” **The New New Internet** (May 7, 2010)

## 佳作（教職員の意識向上賞）

情報セキュリティ意識を向上させるための教育について

教職員の意識向上のための  
情報セキュリティ研修に関する一考察

情報セキュリティ大学院大学 博士前期課程

星野 進

## 1 はじめに

情報化社会の発展に伴い、学校にも情報化の波が押し寄せてきている。さらに、個人情報保護法の施行を契機に、学校でも情報資産や個人情報について適正に管理することが強く求められるようになってきた。しかし、個人情報の漏洩や紛失などの事故は後を絶たない。教育の分野では、平成 15 年度に高等学校に必修科目として普通教科「情報」が新設され、平成 20 年に公示された小中学校の指導要領では、「情報を適切に主体的、積極的に活用するための学習活動を充実させること」と明記されるなど、情報の利活用を促す内容が追加されている。また、校務の場面でも平成 18 年の文部科学省の調査によれば、「校務情報化の必要性は認識されている」との報告があるように、情報を取り扱う機会は増加していくことが予想される。学校における情報化は、教育と校務の両面から求められているといえる。さらに、校務の情報化の最大の弱点ともいわれていた校務用コンピュータの整備であるが、平成 21 年度補正予算により整備率は格段に向上した。校務用コンピュータが一人 1 台整備されつつある現状では、情報セキュリティについて従来以上に取り組む必要がある。しかし、教員の情報スキルやモラルに対する知識は十分とはいえない状況である。さらに、教員にとって授業が主体であり、授業に直接関係しない情報セキュリティに対する意識が高まらないという面がある。

本論文では、公立学校の組織の特性をふまえながら、情報セキュリティに対する意識を高めるための情報セキュリティ研修について提案する。

## 2 学校のセキュリティ事情

### 2.1 学校の持つ個人情報と校務の情報化

学校の持つ個人情報は、作成や保存が法令や規則で義務づけられているものから、指導上必要であるため収集しているものまでさまざまある。公立学校では、個人情報を取り扱う際には条例などで「個人情報取扱業務登録」が義務づけられている。これは、個人情報を取り扱う業務を始めるにあたり、あらかじめ所定の事項を登録して地方公共団体の長に届け出なければならない。すなわち、個人情報を取り扱う業務を申請し登録されなければ、収集できない。学校で

は教育の質や効果を高めるためには、対象となる児童・生徒・保護者等の個人情報の収集が必要であると考えられる傾向が強く、学校のみならず教員も多くの個人情報を抱えている[1]。収集される個人情報には、成績や通知表などの教務関連の事務や、転出入や出欠などの学籍関連事務があり、保健指導、生徒指導、校外学習、宿泊学習などの校務に使われている。

これらの個人情報は従来紙で作成し、管理されていたが、近年、校務の情報化による情報機器の導入により、学籍管理や成績処理などを中心に電子化が進んだ。このように、校務を情報化することにより、教職員の負担軽減や業務の効率化を行い、そのことにより「児童・生徒に対する教育活動の質的改善」につなげていこうというのが、「校務の情報化」である。平成 21 年度の補正予算により教員の校務用コンピュータの整備率の全国平均が 98.3%と一人 1 台の状態がほぼ整ったこともあり、今後はいっそう校務の情報化が進み、学校にある様々な情報資産は情報化されていくことになる。

## 2. 2 学校の組織構造

表 1 学校数と本務職員数

平成 21 年度の学校基

本調査[2]によれば、小学校・中学校・高等学校・中等教育学校・特別支援学校の学校数は、39,377 校で、そこに勤める本務教員数は、約 91 万 5 千人であり（表 1）、これは全就業人口の約 1.5%にあたる。この比率は、資格を必要とする専門職業の中でも非常に高い。

学校の中でも教員（ここでは、校長・副校長・教頭・主幹教諭・指導教諭・教諭等のことをいう）は多数を占めている。図 1 に各

	学校数(校)	本務職員数(人)
小学校	22,258	419,437
中学校	10,864	250,782
高等学校	5,183	239,349
中等教育学校	42	1,600
特別支援学校	1,030	70,516
計	39,377	915,346

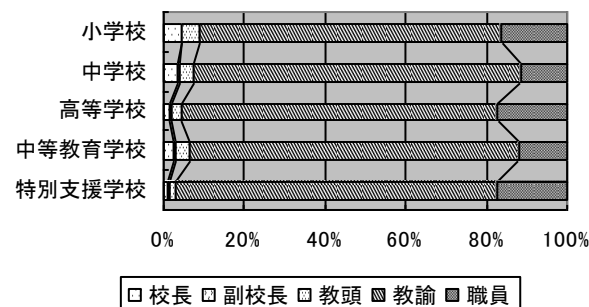


図 1 教職員の割合  
(校種別)

学校種別の本務教員数と他職員の合計人数を比べたものを示す。また、図2からは、教師だけで他の職種の4～5倍いることがわかる。全職員に対する管理職の比率は平均で7.1%であり（図2）、特別支援学校では全職員の2.8%にしかすぎない（図1）。職員数が200人いる学校で、管理職は5～6人しかいないことになる。

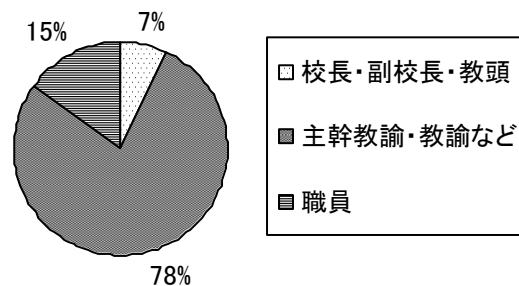


図2 教職員の割合  
(管理職・教諭・職員)

### 2.3校務用PCの整備環境

文部科学省が年度末におこなっている「学校における教育の情報化の実態等に関する調査」[3]によれば、教員の校務用コンピュータの整備率は平成22年3月31日現在で98.3%となっている。前年の平成21年3月には61.6%であったことと比較すると急激に整備されたことがわかる（図3）。この平成21年度補正予算による整備では、校務用コンピュータだけでなく、教育用コンピュータ

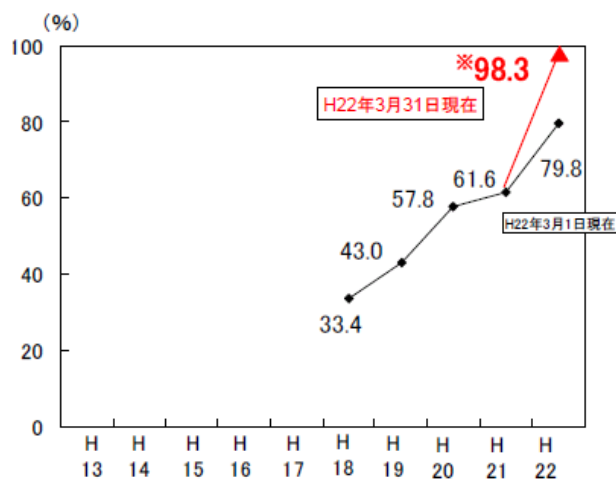


図3 校務用コンピュータの整備率

やLANの整備も並行して行われた。コンピュータ1台あたりの生徒数は7.2人/台から6.4人/台へ増加し、ここ数年5ポイントぐらいいしか上昇していなかった普通教室の校内LAN整備率は64.0%から81.2%に約17ポイントも上昇した。

### 2.4ネットワーク環境

公立学校のネットワーク環境は自治体によって様々であるが、学校を中心とした「教育情報ネットワーク」と、自治体職員共通の処

理を目的とした「首長部局ネットワーク」に分けられる。「教育情報ネットワーク」には、パソコン教室や一般教室などで生徒の学習用として使われる「教育用ネットワーク」と先生が学校事務の処理を目的として使う「校務用ネットワーク」の2つがある。学校ではこの3つのネットワークが混在しているところも多く、「首長部局ネットワーク」と「教育情報ネットワーク」は都道府県で約60%、市区町村で約54%が完全に分離している。「教育情報ネットワーク」についても、文部科学省が「教育用ネットワーク」と「校務用ネットワーク」を論理的または物理的に分けることが好ましいとしているように分けられているところが多い。学校内ではこの3つのネットワークを使い分けながら業務を行うことになる。そのため、授業で使うデータを校務用ネットワークから教育用ネットワークへ外部媒体を使ってやりとりをするケースは当然多くなるといえる。

## 2.5セキュリティポリシーとガイドライン

図4は「校務情報化の現状と今後の在り方に関する研究」[4]の資料をもとに情報セキュリティガイドラインに対する取り組みについて作成したグラフである。ガイドラインがあると回答した学校

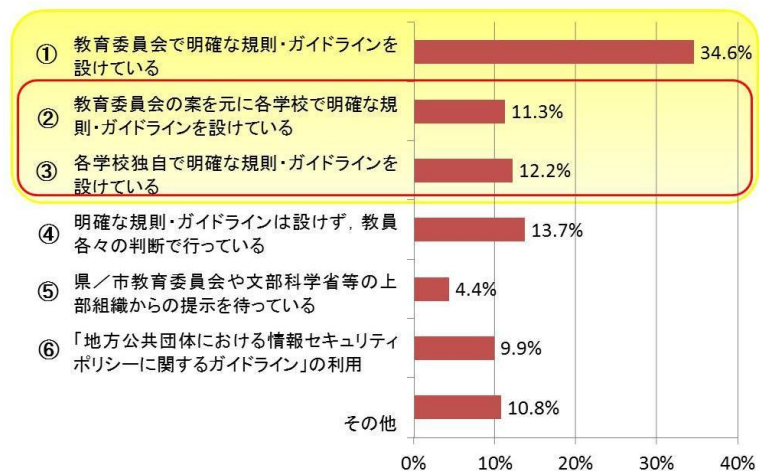


図4 ガイドラインの取り組み

が58.1%（図4の①，②，③の合計）であるが、ガイドラインを独自に考えたり，教育委員会の案を元に作成しているとしたのは全体の23.5%（図4の②，③の合計）であった。図4からは，セキュリティポリシーやガイドラインを自分たちで考え，見直していくものと考えている学校は少ないことがわかる。すなわち，実情に合わせた対策を考えたり，PDCA サイクルを回している学校は少ない。この理由は，情報セキュリティと利便性は二律背反の関係にあることから，上から押しつけられたり，一部の担当者のみが作成した情報

セキュリティポリシー等は無視し、仕事のしやすさを優先させている事例も数多く見られる[5]ことと考えられる。すなわち、セキュリティポリシーやガイドラインは通知されているが、内容が周知徹底されているどころか、その存在すら知らないという人も多い。以下の章ではこれを解決する方策を探る。

### 3 学校における情報セキュリティの特性

学校における情報セキュリティ教育を考えるにあたり、人的な対応については、学校の特性に合わせた内容にしていく必要がある。

藤村は、「学校情報

表 2 学校の特性

セキュリティの現状と課題」の中で、学校の情報セキュリティに関する特性を5つあげている[5]。(表2)

項	学校の特性
①	指揮・命令機能が弱い
②	能力・意識差が大きい
③	専門家が不在である
④	私物 PC の持ち込み・業務利用が一般的
⑤	ネットワーク、システム管理権限がない

この中でまず、①の「指揮・命令機能が弱い」というのが企業や自治体などと大きく異なる点である。「2.2 学校の組織構造」でも述べたが、全職員における管理職の人数は非常に少ない(図2)。ここ数年「主幹教諭」や「指導教諭」の制度も導入されているが、導入されて間もないことから機能している学校はまだ少ない。また、学校では校長や教頭などの管理職も教師層内部の職階であるという認識であるため、学校内での「トップダウンアプローチ」の効果は非常に弱いといえる。このことから、教育委員会や校長などの管理職が行う「トップダウンアプローチ」だけでなく、「ボトムアップアプローチ」も組み合わせることが大切であるといえる。また、②の「能力・意識差が大きい」③の「専門家が不在である」ということから、情報セキュリティに対してあまり知識のない人でも、有効となる教育方法を考えなければならない。藤村[5]は、学校における情報セキュリティ教育では、講義型の研修ではなく、教員が参加して自ら考えることができるワークショップ型の研修が望ましいとしている。本稿では、[5]をベースにしてワークショップ型の情報セキュリティ教育を論じる。

## 4 セキュリティ教育

### 4.1 セキュリティ教育の分類

公立学校の特殊な現状を踏まえ、有効なセキュリティ教育の在り方を考えていかなければならない。津村は「教育者の関わり方」と「教育の重点」という2つの次元から教育者を位置づけた[6]。図5は津村による「4つのタイプの

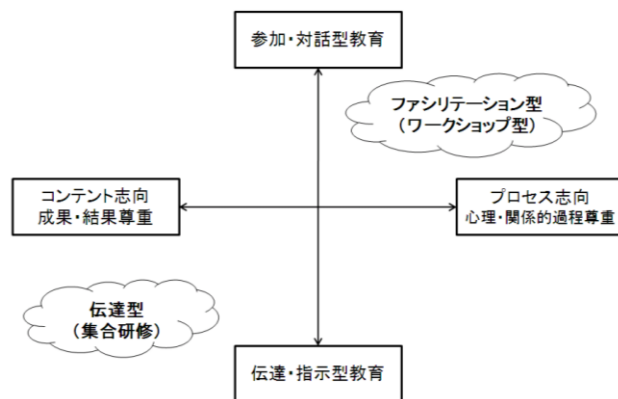


図5 セキュリティ教育の位置づけに加筆・修正

教育者像」に情報セキュリティ研修の型を当てはめたものである。

#### ① 伝達型（集合研修）（[5]では講義型）

この形態の研修は多くの学校で行われている。一斉に多くの人に教育することができることや、知識を効率よく獲得するためには有効な方法であるといえる。しかし、研修を受ける対象者が受動的な態度になってしまいがちになることや、個々のおかれた状況とは関係なく研修が行われるため、たとえ意欲があったとしても予備知識が不足している場合には苦痛を強いるだけの研修になりかねないことに注意が必要である。

#### ② ファシリテーション型（ワークショップ型）

ワークショップ型の教育は、主体的に学ぶことができるプログラムや学習環境を作り、参加者間の相互コミュニケーションをもとにして進めていく研修の方式である。参加者が主体的にコミュニケーションを図るために、ファシリテーター（講師）が一方的な関わりではなく、学習者の関わりなども交え、ヒントを与えたりして関与することで、気づきを進めていく。ただし、ファシリテーション型の教育は、コミュニケーションに基本をおくことや参加者による発見を待つため伝達型と比較すると効率が悪く時間を要する。さらに、ファシリテーション型の教育を行うには、誰もが議論に積極的に参加できるためのツールの提供など学習環境の整備が必要となる。

現在の学校の教員をめぐる状況を考えると、それぞれの学校で情報

セキュリティの状況が異なるため、一律のセキュリティポリシーに従えばよいということにならず、学校に合わせた情報セキュリティを実践することが求められており、情報セキュリティ研修には、ファシリテーション型が望ましい。ファシリテーション型の研修を学校で行うためには、予備知識のあるなしに関わらず誰でも取り組める環境としてのツールが必須である。そのために、後述の簡易 MRC 学校版を活用したリスクコミュニケーションを行うファシリテーション型の研修を提案する。

#### 4.2 リスクコミュニケーションの必要性

学校の情報セキュリティに関するリスクについては、今までは学校側が主体となって考えられることが多かった。リスクの考え方は教員のおかれた立場によって異なるが、今までの教員に対する情報セキュリティ教育では、多様な立場からのリスクをとらえることは不十分であったといえる。佐々木[7]は、リスクには、セキュリティが失われるリスクと、プライバシーが失われるリスク、運用リスク、経済のリスクなど多重なリスクがあり最適解が存在しないことが多い。多重なリスクを考慮しつつ合意形成することが必要であるとした。そして、リスクには両立するものと対立するものがあり、それらの中で対策を考えていかねばならないとし、セキュリティ、プライバシー、コストなどの指標のどれを重要視するかは、意思決定者の選好の問題であるとした。

公立学校のネットワークシステムは教育委員会や教育センターなどが運用しているケースが多いので、学校内で抱えるリスクは、個人情報情報の漏洩による機密性とウイルスなどによるシステム障害による可用性が主である。すなわち、すべての教員の意識が重要なファクターとなる。指揮命令システムの弱いといわれる学校では、リスクコミュニケーションによるリスクの共有や相互理解を深めるためファシリテーション型の教育と組み合わせると効果的であるといえる。

### 5 MRC と簡易 MRC 学校版

MRC (多重リスクコミュニケーター) は、「リスク間の対立を回避する手段の必要性」「多くの関与者間の合意が得られるコミュニケーション手段の必要性」「対策の最適な組み合わせを求めるシステムの

必要性」を目的として、佐々木らが開発したソフトウェアシステムである[7]。MRCは、実際に個人情報漏洩対策などの情報セキュリティ対策に適用されている。しかし、学校の情報セキュリティ教育でリスクコミュニケーションを行うためには、MRCを適用するのが望ましいが、MRCは複雑な演算をインターネットと接続して実施するため、高度なPCや専門家を必要とする。そのため、各学校で、定期的にリスクコミュニケーションでMRCを適用していくことは現実的には難しい。MRCを基に、学校で必要な多重リスクコミュニケーション機能に限定した簡易版ソフトウェアを実現できれば、学校でも利用が進むのではないかと考えた。そこで、簡易MRC学校版を開発（東京電機大学と共同で開発中）することにした。以下にその概要を述べる。

## 5.1 簡易 MRC 学校版

簡易 MRC 学校版は、Excel の VBA で開発されており、インターネットに接続してデータをやり取りすることなく、スタンドアロンで利用できるようにしている。インターネット環境がなくても利用することができる。また、Excel に学校に必要なパラメータをあらかじめ設定することで専門家の関与も最低限となるようにしている。そのため、特別な人や場所・機器を必要とせず、日常の範囲でも適用できる。

簡易 MRC 学校版の開発目的は、教職員に対する情報セキュリティ教育のためのファシリテーション型研修の支援であり、情報セキュリティ対策の策定支援ではない。したがって、詳細なパラメータの設定やきめ細かい演算よりも、グラフが容易に扱えることが望ましいなどをふまえ、簡易 MRC 学校版を開発している。

簡易 MRC 学校版の適用は次のような流れとなる。

### 1. PC などの機器の数や個人情報の件数などの設定情報の入力

生徒数やハードウェアの状況などリスクを計算するための基礎データを入力する。この部分を入力すると、自動で準備される。

No	チェック欄	チェック項目
1	2	パソコンにはウイルス対策ソフトを入れるなど、ウイルス対策を行っていますか？
2	2	ウイルス対策ソフトのウイルス定義ファイルは、常に最新のウイルス定義ファイルになるようにしていますか？
3	1	外部記憶媒体を利用する際には、ウイルスチェックを行っていますか？
4	1	重要情報を外部記憶媒体に入れて校外に持ち出すときはパスワードや暗号化をするなど、盗難・紛失対策をしていますか？
5	2	私物USBの利用について規定を明確にしていますか？
6	2	重要情報を外部記憶媒体で校外に持ち出す際の規定を明確にしていますか？
7	2	学校所有の外部記憶媒体についての管理ができていますか？
8	1	外部記憶媒体の紛失や置き忘れを防ぐための対策をしていますか？
9	1	重要な書類を廃棄する場合は、重要情報が読めなくなるような処分をしていますか？
10	0	重要情報が机の上やプリン列に放置されているようなことはありませんか？

図 6 チェックリスト

## 2. チェックリストの入力

チェックリスト（図 6）に学校の現状を入力する。この情報をチャートで表し、視覚化することで、だれでも現状が把握できるようにしている。また、このチェックリストと対策案が連動しており、対策案を選択するヒントとなる。

## 3. 対策案の選択

学校で想定される対策案が 80 以上事前に入力されている。また、各対策案を比較評価するパラメータはすでに入力されているため、すぐに利用することができる。MRC は複数の対策案の評価値を表示するので、その中から対策案を選択する。

## 4. 簡易 MRC 学校版の適用



図 7 簡易 MRC 学校版（画面 1）

図 8 簡易 MRC 学校版（画面 2）

リスクコミュニケーション時のフォームが 2 つある。1 つは各パラメータをグラフにより可視化した画面である（図 7）。この画面には、学校の情報セキュリティの現状がグラフで表示されており、簡易 MRC 学校版を適用して情報セキュリティ対策案を採択した場合と、どの情報セキュリティがどのように強化されたかが直感的にわかるようになっている。また、情報の漏洩確率や情報活用の利便性やプライバシー負担度、対策コストなどもグラフに表示される。もう一つの画面は、対策案をパラメータとともに表示している。採択された対策は「青」で採択されない対策は「赤」で表示される。リスクコミュニケーションの話し合いにはこれら 2 つの画面を見て、対策案を入れ替えたりしながら進めていく。

## 6 簡易 MRC 学校版を用いた情報セキュリティ研修の方法

ファシリテーター型の情報セキュリティ教育でのリスクコミュニケーションに簡易 MRC 学校版を用いる。これは、リスク対策の合意を形成する過程では、様々な教育効果が期待できるためである。以下では、簡易 MRC 学校版を用いた情報セキュリティ研修の場合を例示する。

### 6.1 目的

簡易 MRC 学校版を用いてリスクコミュニケーションをおこなうにあたり、研修の目的を次のように設定した。

- ・ 参加者が、ロールプレーヤー（管理職・教職員・保護者）となり、リスクコミュニケーションを通して、学校に存在するリスクについての情報を共有する。
- ・ ロールプレイを通し、他の利害関係者におけるリスクについての情報交換をおこない、誤解や理解不足に基づくリスクの顕在化について理解させる。
- ・ 関係者に及ぼすリスクの回避および低減に向け、対策案を簡易 MRC 学校版を利用しながら討論することによって、学校の情報セキュリティに参画していこうとする意識を高める。

### 6.2 事前準備

この研修を行うにあたり、まず学校にある情報資産の洗い出しが重要となる。その後、情報資産へのリスクの洗い出しと対応策の検討を行い、対応策が出た段階で、事前に簡易 MRC 学校版に入力されている対策案と比較し、追加や削除を行う。なお、対策案が多くなりすぎないように、一定数以上の対策案を選択できないように設定する。また、学校の個別環境データ（個人情報の数や環境のデータ）は事前に入力しておく。

これらの事前準備は、意識の向上の面からも学校全体で取り組むことが望ましいが、事前に設定されている対策案を利用することも可能である。

### 6.3 ファシリテーター

ファシリテーション型教育を行うのであるから、当然ファシリテ

ーターの役割は非常に重要になる。そのため、ファシリテーターになる人については、事前に状況を把握しておいたほうが効果的である。今回のケースでは、ファシリテーターに対して事前に講習会を行うこととした。講習会の内容は、簡易 MRC 学校版の使い方と、リスクコミュニケーションの進め方などについてである。

#### 6.4 情報セキュリティ研修会の流れ

情報セキュリティ研修会は以下のような流れで行う。

- ・ 今回の研修の概要についての説明
- ・ 10～15 人程度に分かれてもらい（事前にグループ分け）、ロールプレイヤーを決め、リスクコミュニケーションを行う。対策案について合意形成まで行う。
- ・ 参加者の代表による結果の発表
- ・ 反省会とアンケートへの記入（簡単な問題点なども記入する）

### 7 今後と課題

実際に今回提案した研修方法が情報セキュリティ教育に有効であるか否かを評価する必要がある。今後の予定として

- ① リスクについての集合型研修
- ② リスクの対応策を協議するワークショップ型研修
- ③ 簡易 MRC 学校版を用いたリスクコミュニケーションの研修

を数校で実際に行い、比較検討をしていくことを予定している。その中で、出てくる課題をふまえて正式版に向けて改良していくことを考えている。また、学校が継続的に取り組むためには、利用方法や進め方などのマニュアル作りも必要である。

今回の提案では一斉研修の形で行うことを想定したが、簡易 MRC 学校版は研修だけでなく、校内のセキュリティ運用などでも利用できることから、利用方法を広げていくことも考えていきたい。

## 参考文献

- [1] 角替晃・成田喜一郎,「必携！教師のための個人情報保護実践マニュアル」, 教育出版, 2005 年
- [2] 文部科学省,「平成 21 年度学校基本調査」, 2009 年 12 月
- [3] 文部科学省,「平成 21 年度学校における教育の情報化の実態等に関する調査結果[速報値]」, 2010 年 6 月
- [4] 日本教育工学会,「校務の情報化の現状と今後の在り方に関する研究」, 2007 年
- [5] 藤村裕一,「学校情報セキュリティの現状と課題」, 先進 IT 活用教育シンポジウム in 和歌山, 2006 年, pp30-31
- [6] 津村 俊充,「ファシリテーター・トレーナー自己実現を促す教育ファシリテーションへのアプローチ」ナカニシヤ出版, 2003 年
- [7] 佐々木良一, 石井真之, 日高悠, 矢島敬士, 吉浦裕, 村上優子,「多重リスコミュニケーションの開発構想と試適用」情報処理学会論文誌, 第 46 号, 第 8 巻, 2005 年, pp.2120-2128

本懸賞論文は、防衛調達研究センターの公益事業として行った、第3回目の成果を発表するものです。

また、本論文集は、当協会のホームページ(<http://www.bsk-z.or.jp>)でもご覧いただくことができます。このホームページには、皆様のお役に立つ情報を掲載しておりますので是非ご覧ください。

**平成22年度  
「情報セキュリティに関する懸賞論文」受賞作品**

平成22年12月 発行

非売品 禁無断転載・複製  
発行 : 財団法人防衛調達基盤整備協会  
編集 : 防衛調達研究センター刊行物等編集委員会  
〒160-0003 東京都新宿区本塩町21番3-2  
電話 : 03-3358-8754  
FAX : 03-3358-8735  
メール : [hozen@bsk-z.or.jp](mailto:hozen@bsk-z.or.jp)  
H P : <http://www.bsk-z.or.jp>