リスクマネジメントを活用した情報倫理の指導法

白井智也[1,2]　横山節雄[1]　宮寺庸造[1]

[1]東京学芸大学
〒184-8501 東京都小金井市貫井北町 4-1-1
E-mail: {m013309, yokoyama, miyadera} @u-gakugei.ac.jp

[2]埼玉県立越谷総合技術高等学校
〒343-0856 埼玉県越谷市谷中町 3-100-1
E-mail:shirai@ksg-h.ed.jp

概要

ミレニアム・プロジェクト「教育の情報化」により，すべての教室にコンピュータが設置され，専用教室・専門教員の管理のもとでの利用から，生徒・教員が自由に利用できる環境となった。そのため問題行動を未然に防ぐための情報倫理の実践が重要な鍵となっている。そこで，本研究では，高校生を対象に問題行動を，現実的かつ内面的にとらえさせる指導法の開発として，リスクマネジメントを活用することとした。このことで，情報倫理上の問題をポリシ・リスク・セキュリティに分け評価・分析し，リスク排除の実践，再評価する態度を身につけさせ，情報倫理の継続的な実践を促すことをねらった。

1. はじめに

平成１４年度から実施された「体系的な情報教育」の流れを受けて，平成１５年度より，すべての高等学校で普通教科「情報」が実施されることとなった。そして「情報社会に参画する態度」にて，情報倫理教育を扱うこととなり，内容の全体を通して情報モラルの育成を図ることとなった[1]。しかし，普通教科「情報」では，扱う内容が多岐にわたる上，興味・関心を高めることが優先されるため「ルール」・「エチケット」・「事例の検証」などの情報モラルに関する内容に焦点をあてた継続的な実習授業を行うことは難しい。そのため教員が一方的な説明をするだけで情報倫理教育を終わらせてしまうのではないかと懸念されている[2]。必要なルール・マナーに関しての教え込みは重要であるが，心構えについて考えさせ様々な状況に応じて一般化できる能力の育成も並行して行わないと，受け手は「押しつけられた」と感じ，自発的な実践につながらなくなる。よって，この２つのバランスが情報倫理教育の鍵となる。一方，学校教育における授業時数は，週３０単位時間であり，どの教科でも十分な時間が確保できない状況にあるため，複数の教科・領域で総合的に情報倫理教育を指導することが求められる。そのため，「ルール等の教え込み」「心構えの一般化」を「短時間」「複数科目」で「継続的的」に「興味関心を高めながら指導する」ことが重要な要素となる。

このような背景から，学校教育における情報倫理（情報モラル）の指導法に関する報告や研究がされている[3][4][5][6][7]。

文献[3][4]においては，具体的な事例が多く指導

A Teaching Method for Information Ethics Using Risk Management
Toshiya Shirai, Setsuo Yokoyama and Youzou Miyadera
Tokyo Gakugei University

方法についても提言されているが，大変広範囲であるため，すべての事例を授業で扱うのは難しいといえる。そこで，ＣＡＩ教材[6]で時間的・内容的に補完し，授業等で情報倫理に関する演習を可能としているが「心構えの一般化」という点を読みとることができなかった。文献[6][7]においては，ルールの押しつけ型にならない指導法を提案している。道徳的知識と情報社会で発生する問題点を比較させたり，意図的に問題のあるサイトにアクセスさせたりしているが「継続性」という点を読みとることができなかった。

そこで，本研究は，上記の報告で指摘した要素を，総合的に行うために「リスクマネジメント」を活用した情報倫理の指導法を提案することを目的とする。「リスクマネジメント」では，問題の発生を回避するためのポリシ（方針），ルールの決定だけにと止まらず，日常の監視や評価も行うため，授業においても禁止行為の説明だけにとどまらず，そのルールの監視や再評価なども扱うこととなる。

セキュリティ技術がめざましく発展している情報社会の中では既成概念が，すぐに陳腐化してしまうため「評価・監視・再評価」が重要な鍵となる。よって，この評価方法を学ぶことでポリシ，ルールの再評価が常に行われるため，情報倫理教育における「心構えの一般化」「継続性」が補完できると考えている。

第２節で「リスクマネジメント」を情報倫理教育に活用する理由を整理し，第３節で指導法を提案する。第４節では，提案した指導法に基づいた授業実践について報告する。

2. リスクマネジメント

2.1. リスクマネジメントとは

情報セキュリティにおけるリスクマネジメントとは，セキュリティポリシの適用範囲として規定されたセキュリティリスク領域を対象とし，潜在するリスクを洗い出して，セキュリティポリシが目標とするリスク制御水準を維持するためのセキュリティコントロールを実施するプロセスを意味する。具体的には，リスク分析プロセスでリスク評価を行い，目標とするリスク強度より大きいセキュリティリスクを適切なリスク処理方法を選定して制御するリスク対策プロセスを実施する。また，リスク対策結果の評価とセキュリティ監査を行う[8]と定義している。そして，このリスクマネジメントを行うための工程をリスクマネジメントサイクルといい，工程は次の通りとなる。

(1) リスク分析
(2) リスク処理策の選定
(3) リスク処理の実施・運用
(4) リスク処理結果の監視・評価

2.2. リスクマネジメントの情報倫理教育への適用

情報倫理教育をリスクマネジメントに適用させるために「ポリシ」「リスク」「セキュリティ」を整理する。

情報倫理における「ポリシ」は，情報社会に参加する際に
(1) 自分の財産を守る
(2) 自分のプライバシーを守る
(3) 自分の生活を守る
(4) 自分のポリシ（生き方・考え方）を守る
ことである。

「リスク」は，情報倫理入門書や情報モラル事例集で提示されている問題事例である。これらは，その行為をすると必ず発生するものではないため，「自分のこと」として捉えることが難しい。

「セキュリティ」は，リスクが発生しないための対策である。

「ポリシ」「リスク」「セキュリティ」は，情報倫理教育の目的である「情報社会に参画する態度」を達成させるための根幹であるといえる。

さらにリスクマネジメントサイクルでは「セキュリティ監査」「結果の評価」をおこなう。情報倫理教育においても，ルールを遵守しているかを監査し，その結果を評価するということは重要であ

り，必ず実施しなければならない。

よって，リスクマネジメントサイクルの工程は，情報倫理教育でのアプローチに応用できるといえる。

次に，情報倫理教育におけるリスクマネジメントサイクルを次の通り提示する。

(1) 貨幣価値を用いた評価（リスク分析）
(2) 発生確率及び処理策の予測（リスク処理策の選定）
(3) 技術的に回避できる処理方法の実習（リスク処理の実施・運用，リスク処理結果の監視・評価）

情報セキュリティにおけるリスクマネジメントでは４工程であったが，情報倫理教育におけるリスクマネジメントでは３工程で行う。

情報倫理での「ポリシ」が直接「自分」に関わる上，その実施・運用・監視・評価も「自分」でやらなければならないため「実施・運用」と「監視・評価」の２工程を統合した。

2.3. リスクマネジメントの情報倫理教育への適用に対する意義

リスクマネジメントは，非常に先の見える企業の保険管理者と危険と保険の学者によって，広げられた視野の結果生じたものである[11]。現在は情報セキュリティ分野をはじめ，様々な分野（環境，金融）で，広く適用されており，この基本的な考え方や実施方法を理解することは，幅広い応用性につながる。

さらに，情報コミュニケーション技術（ＩＣＴ）への応用にも期待ができ，リスク・コミュニケーション[16]を，リスクマネジメントサイクルで分析し，コミュニケーションに失敗しないための対策や，自分の意見を相手に正しく伝えるための対策などが評価できる。

リスクマネジメントの情報倫理教育への適用は，リスクマネジメントという技法を，普通教科「情報」の時間で，すべての高校生に教えることができる上，様々な分野での応用が期待できることから大変有効であるといえる。

3. リスクマネジメントを活用した情報倫理の指導法

3.1. 教材等

教材及びコンピュータ環境は，次の通りである。

(1) 情報倫理に関する事例集[3][4]
(2) ネットワークセキュリティ入門書[12][13][14][15]
(3) 表計算ソフト
(4) インターネット環境

授業形態は，生徒３名程度のグループ学習で行い，話し合いを中心とした実習となる。教員はそのアドバイザとなり，議論の方向性を監視する。

3.2. リスク分析に関する指導法

リスク分析では「リスクの認識」と「貨幣評価」を行う。分析の道具として，表計算ソフトを利用する。

「リスクの認識」においては，教員がポリシを示し，生徒は情報倫理に関する事例集等[3][4]をもとに問題点を項目毎に抽出する。ここでは，実際に問題が発生すると，何を失い，取り戻すにはどのくらい費用がかかるかを整理することが目標となる。抽出項目は，次の６項目である。

(1) 問題行動
(2) 行動原因
(3) 得るもの
(4) 失うもの
(5) 取り戻すのに要する日数
(6) 損失額

「問題行動」については，表題として抽出する。

「行動原因」については，情報通信ネットワークを使用する上での行動パターンを明確化するため，選択形式で入力する。項目は次の通りである。

(a) Web 受信	(b)Web 送信
(c)Web 作成	(d)Mail 送受信
(e)chat 参加	(f)BBS 書込
(g)すべての行為	(h)その他の行為

「得るもの」については「行動原因」を参考にグループ毎に予測させる。

「失うもの」については，予測が難しいため事例集や教員の助言・指導を交えながらグループ毎に議論をする。

なお「問題行動」に対して，複数「得るもの」「失うもの」が発生した場合は「問題行動」をキーとして行を追加し入力する。

「取り戻すのに要する日数」については，「失うもの」に対しての「復旧日数」を計算させる。なお，日数を予測させることは大変難しいため，教員が6つの計算式を提示する。ただし，この計算式は必ず使わなければならないものではない。計算式は次の通りである。

(a) 自分が信用失墜行為をした場合
式　：　年齢×３６５日
理由　：　年齢が増すほど日数も増す
(b) 相手から信用失墜行為をうけた場合
式　：　（８０年－年齢）×３６５日
理由　：　年齢が若いほど日数が増す
(c) 情報の信頼性が欠如した場合
式　：　１００年×３６５日
理由　：　取り戻すのに一世紀はかかる
(d) 生命の危機の場合
式　：　８０年×３６５日
理由　：　人生８０年
(e) 法律違反の場合
式　：　最高刑期年×３６５日
理由　：　法規に記載されている
(f) 金銭トラブルの場合
式　：　実際の損失額÷４，２００円
理由　：　時給５２５円×８時間

「損失額」については「取り戻すのに要する日数」×「4，２００円」とする。この金額については，教員がその理由を説明し，現実性を強調する。理由は次の通りである。

【日額「4，２００円」は，自動車損害賠償責任保険で請求が認められている「慰謝料」である（2002/4/1 現在）。慰謝料については，たんに財産上の損害だけでなく，生命・身体や，自由・名誉などを侵害されたことによる精神的な損害についても認められる賠償金[9]であるため，リスクを貨幣評価する上で，もっとも中立的な金額である。なお，身体的に傷害を受けた場合の金額として自動車損害賠償保障法施行令の後遺障害別等級表[10]を確認すること。】

3.3. リスク処理策の選定に関する指導法

リスク処理策の選定においては「発生確率」と「期待値」を計算し，セキュリティリスク（対策を施すリスク）を選定する。前節での「損失額」は実際に発生した場合の金額であったため，この節では発生確率を予測し，１日あたりのリスク負担額を求めることを目標とする。

なお，この節を生徒に実習させる前に，教員が会計学上の注意をする。注意の内容は次の通りである。

【予測期間を１年間とし，その予測期間を会計期間として費用を計算する。よって「算定期間を１年間とした場合の，１日あたりの費用」を計算する。】

それでは，８項目を抽出し１日あたりの費用を計算する。項目は次の通りである。

(1) 発生日数（回数）
(2) 発生確率
(3) 回避前損失額
(4) 対策
(5) １回あたりの費用
(6) 年間対策回数
(7) １日あたりの費用
(8) 回避後損失額

なお「回避前損失額」及び「回避後損失額」のそれぞれの合計が，「期待値」となる。

「発生日数」については，１年間あたりの発生日数をグループ毎に入力する。最小を１日，最大は３０日とし，１日に何回発生しても１日として計算する。

「発生確率」については，

式　：　発生日数　／　３６５日

とする。

「回避前損失額」については，

式　：　損失額×発生確率

とする。引き続き「回避前損失額」の合計をとり，「期待値」を求める。「期待値」を計算させた後，教員がその理由を説明する。理由は次の通りである。

【「期待値」は「宝くじ」における「１本あたりの金額」に相当するものであり，ここでは「１日あたりの金額」に相当する。】

「対策」「１回あたりの費用」「年間対策回数」については，グループ毎に話し合って入力させる。なお，セキュリティ技術で回避できるリスク等はネットワークセキュリティの入門書等[12][13][14][15]を利用して予測する。特に，ここでは，具体的な対策方法（セキュリティ技術を含む）を検討するため教員の助言・指導を交える必要がある。なお，複数対策方法が考えられる場合は，最も効果のある対策を選択する。また，効果が同等である場合は，最も安価なものを選択する。

「１日あたりの費用」については，

式　：　１日あたりの費用×年間対策回数／３６５日

とする。

「回避後損失額」については，

不等式：　回避前損失額＞１日あたりの費用

が成立した，セキュリティのみをセキュリティリスクとして採用し，「回避前損失額」と「１日あたりの費用」を入れ替えて再計算する。

3.4. リスク処理の実施・運用・監視・評価についての指導法

リスク処理の実施・運用・監視・評価について，３つの実習を提案する。

(1) 浪費，ネット中毒，希薄な人間関係対策

方法　：　日記帳（小遣帳）の作成

(2) 著作権，個人情報保護対策

方法　：　契約書（ポリシ）の作成

(3) 技術的対策

方法　：　ＩＰアドレス漏洩対策

方法　：　ウィルス対策

方法　：　外部アタック対策

これらの実習を通して，具体的にリスクを処理し，監視，評価をしていく。

4. 実践事例

4.1. 実践場所

埼玉県立越谷総合技術高等学校情報処理科３年生４１名の生徒を対象に「課題研究（４単位）」にて実践した。実践については３名１グループとなり，週４時間を２週行った。

4.2. リスク分析に関する実践

「リスク認識」においては，はじめに教員がポリシを説明し，具体的な情報倫理に関する問題事例（事例集[3] 第２章）および整理方法を生徒へ提示した。生徒は事例集[3]および整理方法を参考に，分析していった。その結果３３事例を５７問題点に分析し，３時間でデータベース化することができた。抽出したデータを表１に示す（一部抜粋）。

	問題点	行動	得るもの	失うもの
1	有害サイト	Web 受信	好奇心	信用
2	無計画購入	Web 送信	高額商品	金銭
3	無計画購入	Web 送信	大量商品	金銭
4	無計画購入	Web 送信	偽物	金銭
5	オークション無責任参加	Web 送信	購入権利	契約不履行で信用
6	くもがくれ	Web 送信	なし	金銭
7	くもがくれ	Web 送信	なし	クレジットカード番号
8	偽物被害	Web 送信	偽物	金銭
9	甘い勧誘	Mail 送受信	好奇心	信用
10	甘い勧誘	Mail 送受信	好奇心	個人情報
11	甘い勧誘	Mail 送受信	好奇心	自由な生活(逮捕)

12	甘い勧誘	Mail 送受信	好奇心	プロバイダとの契約
13	うそ情報	Web 受信，Mail 送受信	うそ情報	信頼性
14	うそ情報	Web 受信，Mail 送受信	うそ情報	健全さ
15	知らない間の被害	Web 送信	不正プログラム	金銭

（表１）問題点の抽出

次に，「失うもの」に対して，具体的な損失額を生徒に予測させた。生徒は，巨額な損失が計算されるたびに，その事件の「恐ろしさ」を感じていた。さらに，この金額が時給換算で５２５円であるということに気がつき，現実感が増していた。

計算したデータを表２に示す。なお，これは表１の後に引き続き入力されたものである。

	問題点	失うもの	日数	損失額
1	有害サイト	信用	6,570	27,594,000
2	無計画購入	金銭	30	126,000
3	無計画購入	金銭	30	126,000
4	無計画購入	金銭	1	4,200
5	オークション無責任参加	契約不履行で信用	6,570	27,594,000
6	くもがくれ	金銭	10	42,000
7	くもがくれ	クレジットカード番号	365	1,533,000
8	偽物被害	金銭	1	4,200
9	甘い勧誘	信用	6,570	27,594,000
10	甘い勧誘	個人情報	6,570	27,594,000
11	甘い勧誘	自由な生活（逮捕）	6,570	27,594,000
12	甘い勧誘	プロバイダとの契約	10	42,000
13	うそ情報	信頼性	36,500	153,300,000
14	うそ情報	健全さ	36,500	153,300,000
15	知らない間の被害	金銭	30	126,000

（表２）損失額の計算

これら手続きを踏むことで，どのような行動で問題行動が発生するかを，生徒たちは客観的にとらえていた。また，たくさんの考え（認識）から共通の方向性を導き出すという過程を通して，一つの問題点においても多様な価値観があるということを理解していた。さらに，著しく道徳に反する行為に対して法的規制はないのかなど，これらの工程を通して問題行動を自分のこととしてとらえるようになった。

4.3. リスク処理策の選定に関する実践

「リスク処理策の選定」においては，３３事例５７問題点を，２時間でデータベース化することができた。抽出したデータを表３に示す。

	失うもの	損失額	回	確率	回避前損失
1	信用	27,594,000	10	2.74%	756,000
2	金銭	126,000	1	0.27%	345
3	金銭	126,000	1	0.27%	345
4	金銭	4,200	1	0.27%	12
5	契約不履行で信用	27,594,000	1	0.27%	75,600
6	金銭	42,000	1	0.27%	115
7	クレジットカード番号	1,533,000	1	0.27%	4,200
8	金銭	4,200	1	0.27%	12
9	信用	27,594,000	2	0.55%	151,200
10	個人情報	27,594,000	2	0.55%	151,200
11	自由な生活（逮捕）	27,594,000	2	0.55%	151,200
12	プロバイダとの契約	42,000	2	0.55%	230
13	信頼性	153,300,000	10	2.74%	4,200,000
14	健全さ	153,300,000	10	2.74%	4,200,000
15	金銭	126,000	1	0.27%	345
		4,465,734,000	46		9,690,804

（表３）１日あたりの費用（回避前）

なお，表３における損失総額，発生総数，期待値の金額は１５事例のものである。３３事例５７問題点の損失総額・発生総数及び期待値は，損失

総額「¥3,564,100,601」，発生総数「¥186」，期待値「¥37,916,018」であった。

「対策」「１回あたりの費用」「年間対策回数」「１日あたりの費用」「回避後損失額」については表４に示す。

	対策	1回費用	回数	1日あたり費用	回避後損失額
1	アクセス中止	0	10	0	0
2	保護者の同意	0	1	0	0
7	データ暗号化確認	0	1	0	0
8	公式サイトのみ利用	0	1	0	0
9	甘い話にのらない	0	2	0	0
13	信憑性確認(新聞)	120	365	120	120
14	信憑性確認(現場)	240	10	2,400	7
15	ダウンロードしない	0	1	0	0

（表４）１日あたりの費用（回避後）

「対策」については，できるだけ具体的な対策を考えるように指示を出したが，ほとんど同じような対策となってしまった。しかし，その対策を決める際に，「どうしてやってはいけないのだろうか」や「ほかの人はどう思っているのだろうか」「私の意見とあなたの意見は違う」などの疑問が飛び交い，たくさんの意見交換が行われた。そして，その対策を決定し，期待値を再計算すると「回避前」と「回避後」で大きく変化したため，生徒は，その対策の重要性をあらためて感じていた。なお「回避前」の期待値は「¥37,916,018」で，「回避後」の期待値は「¥20,992」であった。しかし，この時点では１日あたりのリスク分担金が２万円と大きかったため，さらに議論が行われた。その結果，「盗まれた個人情報」の対策が「なし」となったためであることが分かった。「盗まれた個人情報」の損失評価額は「¥765,000」で，１日あたりの負担額が「¥20,712」であった。そのため，この点を生徒たちは重視し「個人情報を盗まれないようにするために」という視点が芽生えていった。これにより「盗まれる前の対策」の重要性が認識できた。なお「盗まれた個人情報」に対する対策費を除くと１日あたりのリスクが「¥280」になったため，生徒はその重要性を理解するとともに，安心感もグループ内に広がった。

なお，１５の事例における回避後損失額は「¥127」であった。

4.4. リスク処理の実施・運用・監視・評価の実践

(1) 浪費，ネット中毒，希薄な人間関係対策

この対策として日記帳(小遣帳)をつけさせた。ここでは，新しいタイプの日記帳に慣れ親しみ，日記帳の必要性と回顧の重要性を認識させることが目標となった。

授業においては，課題研究日誌を「表計算ソフト」に置き換えて実施をした。いままでの「日誌の記入」からの変更である。その結果，情報処理科の生徒であるためキーボード入力に慣れており「入力しやすさ（消しゴムがいらない）」「読みやすさ」「データの整理」「図やグラフの挿入」という点でよかったと答えている。さらに，すべてのコンピュータがネットワークで結ばれているため，「日誌の持ち運び」が不要となり，いつでもどこでも入力できるという点で高い評価を得た。

この作業は，日常生活の「データベース化」であり，問題が生じた場合の原因追及資料となる。このことで，浪費，ネット中毒，希薄な人間関係がどこで始まり，どうすればよいかを自分自身で考える「データベース」を手にすることができる。

しかし，授業毎での日記帳（小遣帳）を強制させても「忘れ」「怠け」が起こってしまうため，今後は，スケジューリングソフトの活用も視野に入れ改善を図る予定である。これらを通して，もう一度「日記帳（小遣帳）」の必要性と継続的な作業の重要性を理解させる必要があり，これが問題解決の鍵となるといえる。

(2) 著作権，個人情報保護対策

この対策として契約書の作成をさせることとした。ここでは，契約書の重要性を認識させること

が目標となる。

はじめに，インターネット上で公開しているサイトの「利用」「著作権」についてのポリシを読み，自分がこのサイトを利用する場合の問題点を考える。次に自分がサイトを開設，運用する場合のポリシを考え契約文を作成する。この実習は現在準備中であるが，これらを通して，「契約」に対して意識させることができれば，著作権，個人情報保護対策につながると考えている。

(3) 技術的対策

書籍やサイトを紹介することで，刻々と変わるセキュリティ状況を理解させることをねらうとともに，家庭でもできるセキュリティ技術をすぐに実践できるようにすることをねらう。この実習は随時行っており，特別な時間は要さないため，今後とも続けていく予定である。

4.5. 考察

本研究では，リスクマネジメントを指導法として取り入れ，情報倫理教育を行った。その結果，「心構えの一般化」「継続的性」「興味関心を高めながらの指導」を，一つ一つ工程を踏んで実施することができた。今後は「短時間」「複数科目」という点において，具体的な指導方法を示していきたい。

5. おわりに

本研究では，コンピュータに興味のある生徒を対象に実践をしたため，大変効果が上がったといえる。しかし，コンピュータにあまり興味を持っていない生徒に対しての検証を行っていないため引き続き実践をしていく予定である。その際，コンピュータスキルによる生徒の実践力の差や，男女による意識の違いなどを焦点に被験者を集めて検証する予定である。

なお，本研究の実践は，情報倫理に関する事例集[3]から３３事例５７問題点を一括して評価したため，大変時間がかかってしまった。実際の授業では，その単元で扱われる範囲で「事例」を抽出し分析することで時間的制約をクリアする予定である。今後は，教科・科目・単元・本時の内容まで踏み込んで「リスクマネジメントを活用した情報倫理の指導法」について考えていきたい。

参考文献

[1]文部省：高等学校学習指導要領,1999.

[2]文部科学省：平成１４年度　新教科「情報」現職教員等講習会テキスト（１）,2002.

[3]文部科学省：インターネット活用のための情報モラル指導事例集：財団法人コンピュータ教育開発センター,2001.

[4]情報教育学研究会：インターネットの光と影：北大路書房,2000.

[5]中條道雄,高橋参吉,西野和典,野口紳一郎,田中規久雄：情報倫理教育のための Web 教材の開発と活用：情報教育シンポジウム,2001.

[6]玉田和恵,松田俊樹:異なる知識の組み合わせによる「情報モラル」指導法の検討：日本教育工学会誌 24,2000.

[7]宮田仁,石原一彦:小学生を対象とした情報モラル学習の試み：日本教育工学会誌 25,2001.

[8]ＴＡＣ情報処理講座：情報セキュリティアドミニストレータ基本テキスト：ＴＡＣ出版,2001.

[9]加藤一郎：商業法規（新訂版）：実教出版,2001.

[10]http://www.nliro.or.jp/contents/research/index.html

[11]ニールクロックフォード,南方哲也：リスクマネジメント概論：長崎県立大学学術研究会,1999.

[12]ＴＪmook：セキュリティ特濃！集中！戦力アップ：宝島社,2002.

[13]鳥居壮行：わかりやすい情報セキュリティ：オーム社出版局,1998

[14]http://www.ipa.go.jp/

[15]http://www.trendmicro.co.jp/

[16]吉川肇子：リスク・コミュニケーション：福村出版,1999