

教育の情報化と情報セキュリティ

星 野 朗^{*} 松 島 良 人^{**} 當 間 文 隆^{***}

I テーマ設定理由

「e-Japan 戦略」では、IT 基盤整備、IT 利用・活用重視する政策が打ち出され世界最高水準の高度情報通信ネットワークがうたわれたが、その安全性及び信頼性の確保が重要となってきた。これを受けて、2006 年に策定された「IT 新改革戦略」の中で、「情報セキュリティ先進国」への躍進をはかり、世界一安心できる IT 社会を目指すことがうたわれ、情報セキュリティを重視する政策が打ち出された。

本県でも IT 基盤整備の中で「教育情報化推進計画」をもとに、IT 利用・活用重視する施策が打ち出され、教育の情報化が推進されてきた。情報セキュリティを重視する取り組みとしては、本県教育委員会で平成 15 年 11 月に「IT 安全管理マニュアル」を発行し、児童生徒の人権を尊重しながら、安全かつ効果的にインターネットを利用した教育および学習活動を行うための基本的な共通ルールを提示した。

しかし、高度情報化の進展にともない、コンピュータウイルスだけでなく、フィッシング詐欺やスパイウェア、ボット等、その当初は想定し得なかった新手の脅威が続々と発生し、継続的な対策が必要となり、各学校で今一度、ネットワークやセキュリティ、個人情報の管理運用規定を見直す時期にきている。

本研究において、学校における情報セキュリティの現状と課題を調査し、情報セキュリティの管理運用規程を見直す際の参考となる研究をおこなう。また、各学校における個人情報保護と情報モラル教育の推進を支援するための研究をおこなう。

II 研究内容

1 学校における情報セキュリティの現状と課題

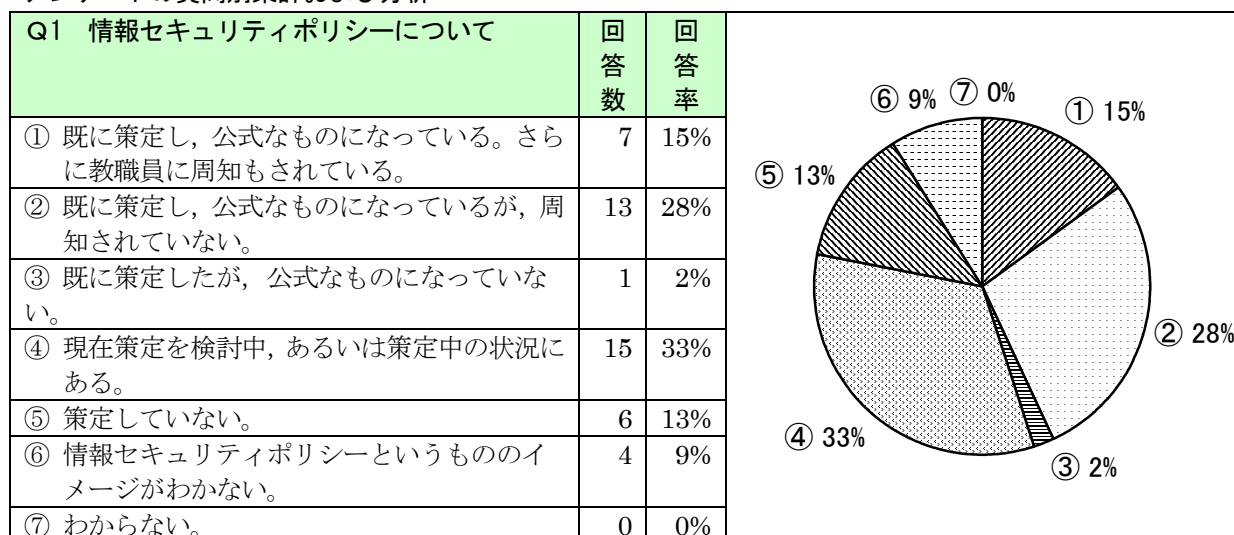
平成 14 年度から教育情報の拠点として IT 教育センターが運営を開始し、沖縄県教育情報ネットワークが確立された。すべての県立高校において校内 LAN の整備が整い、コンピュータに生徒の個人情報や校務にかかるデータが大量に蓄積され活用されている。校内 LAN が整備されて 4 年以上経過し、これまでに ICT にかかる社会環境の変化もめまぐるしいものがある。インターネットの利用に関しても、携帯電話やゲーム機などインターネット端末の多様化や、個人でブログや電子掲示板等で情報を発信することも容易となるなどインターネットの利用形態も大きく変わってきた。生徒の個人情報や校務にかかるデータを持ち出し、ファイル共有ソフト等でインターネット上に情報が流出する事件も後を絶たない。このような ICT にかかる社会環境の急速な変化と「個人情報保護法」の施行にともない、学校における個人情報の取り扱いについては今一度大きく見直す必要がある。

学校における情報セキュリティ対策を検討及び推進するにあたり、学校における情報セキュリティの実態や学校ネットワークの管理状況等を調査したものである。小中学校においては、市町村ごとに校内 LAN の整備状況や利用状況が異なるため今回のアンケート対象からは除いた。また、アンケート項目については、経済産業省委託調査研究である「平成 15 年度初等中等教育現場における情報セキュリティに係る現状調査」を参考にした。

(1) 調査方法と調査対象

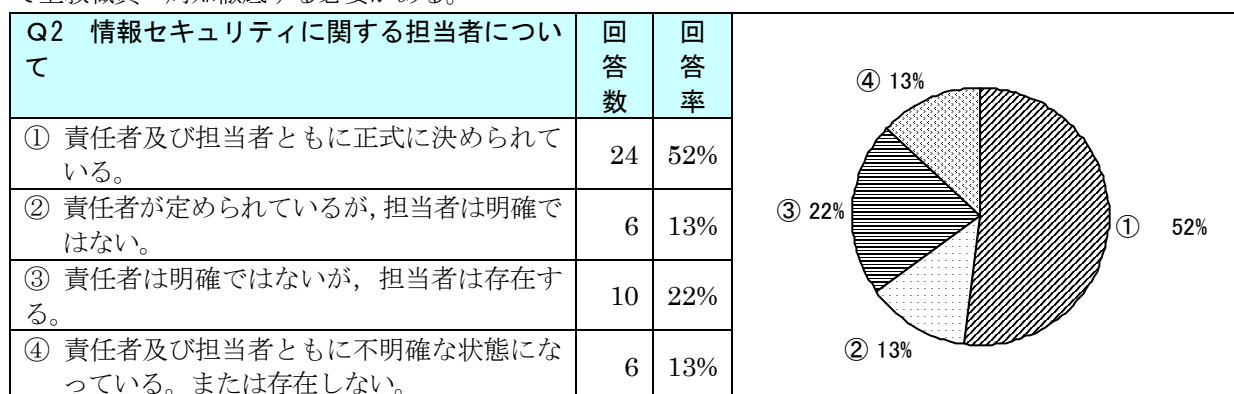
調査方法	アンケート方式
調査期間	平成 18 年 11 月 21 日～平成 18 年 11 月 24 日
アンケート対象と回収率	県立高校全日課程 62 校、校内 LAN 担当者、回収 46 校、回収率 74%

(2) アンケートの質問別集計および分析



情報セキュリティポリシーが公式なものになっていて職員に周知されている割合は 15%にとどまっている。また、検討中や策定中を含めると 55%の割合で情報セキュリティポリシーがない状態である。

情報の機密性や情報システムの安全性を確保し、維持管理するためには組織として遵守すべき事項を定め組織全体に周知徹底する必要がある。情報セキュリティポリシーは学校管理者の承認のもと策定し、校内研修等で全教職員へ周知徹底する必要がある。



情報セキュリティに関する担当者が正式に決められている割合は 74%に及んでいる。

情報セキュリティに対する予防策の承認や事件・事故の対応時などに学校を代表する責任者は校長であるが、情報セキュリティの維持管理及び向上について実務を担当する担当者を明確に定めることが重要である。

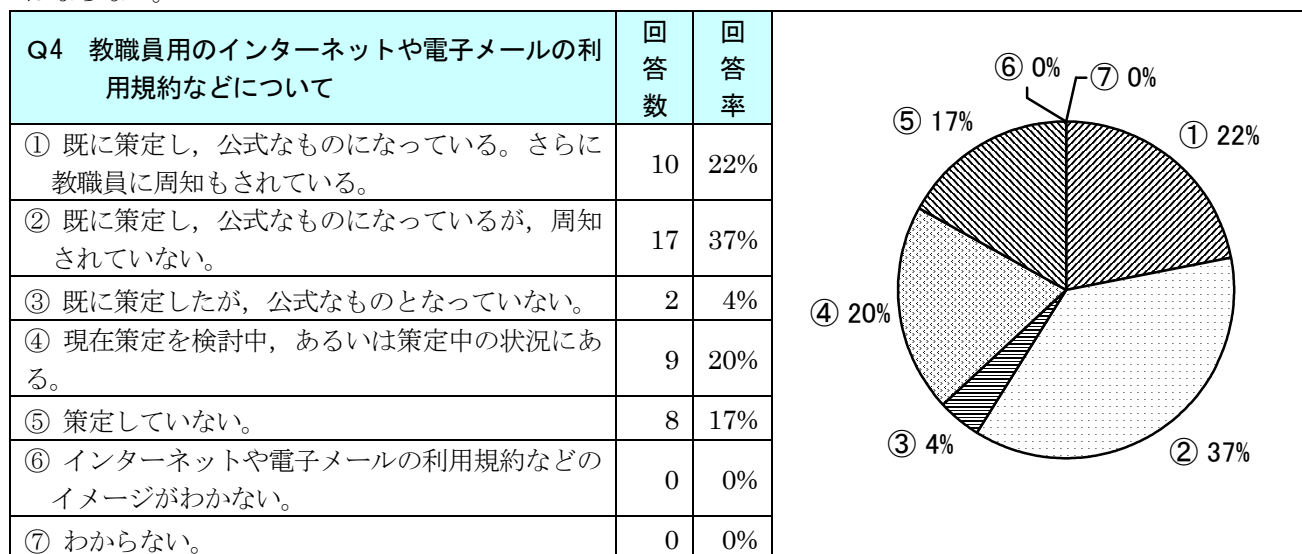
担当者が正式に定められている学校の割合に比べて、情報セキュリティポリシーが定められていない学校の割合が多いことより、個人情報の取り扱いについて、組織的な対応がなされていない学校が多いと思われる。学校における管理者においては、個人情報等の扱いにおいて、組織的に取り組む体制作りが急務である。



情報セキュリティに関する教育を、教職員に対して実施している割合は 69%、生徒に対して実施している割合は 61%、教職員、生徒など全員に実施している割合は 39%である。

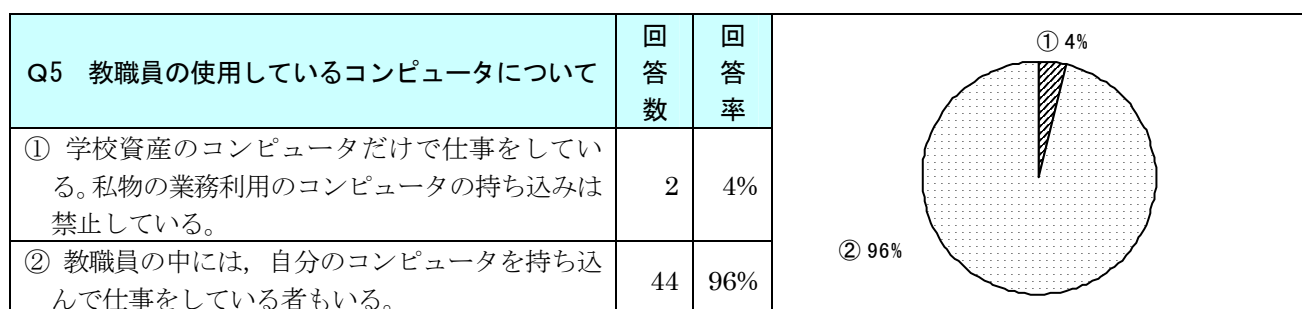
情報セキュリティとは何か、なぜ必要か全職員に理解させた上で、学校における情報セキュリティポリシーを周知徹底する必要がある。児童生徒においては各自の個人情報をいかに守るかまた、他人の個人情報を侵害

することのないよう教育していかなければならない。また、情報セキュリティに関する教育は定期的に行わなければならない。



策定し公式なものとして教職員へ周知されている割合は 22%、公式なものでないか教職員へ周知されていない割合は 78%である。

情報セキュリティのガイドラインの中でも、インターネットや電子メールにおける利用規程は特に重要な位置づけとなる。個別に具体的な利用規程を定め全職員へ周知徹底する必要がある。



自分のコンピュータを持ち込んで仕事をしている学校の割合は 96%である。

平成 17 年 10 月に県教育長から各市町村教育委員会教育長、各県立学校長、各教育事務所長宛ての通知「個人情報及び校務に関わる情報等の取り扱いについて」における留意事項で個人所有のパソコンの利用範囲を、「個人所有のパソコンを学校内で使用する場合は、教材作成等の範囲とし、個人情報及び校務に関わる情報等に関するデータの取り込み及び作成は禁止する。」と定めている。また、平成 18 年 3 月に県教育庁総務課長より各課室長、各出先・教育機関等の長、各県立学校長への通知「業務情報の適正な管理について」において「個人所有パソコンによる業務情報の処理は行わないこと。」とした上で、「但し、県立学校においては、教員一人一台のパソコンを整備していないことにより、個人所有のパソコンを使用する場合には、ウイルス対策を講じた上で、教材作成の範囲において使用を認めることとします。」と通知された。96%の学校で教職員の個人所有のパソコンで仕事をしているが、使用する範囲は教材作成等の範囲に限定されなければならない。これらの通知を個人所有のパソコンで仕事をしている各教職員で遵守されているか、情報セキュリティ管理責任者で常にチェックすることは困難である。これらの通知を遵守するためには校内研修等で、各教職員に個人所有のパソコンで個人情報及び校務に関わる情報等に関するデータを取り扱う危険性を把握させ、これらの通知を遵守することの重要性を理解させなければならない。

Q6 教職員の使用しているコンピュータのネットワーク接続について	回答数	回答率	
① 教職員が自分で持ち込んだコンピュータのネットワーク接続は、一切禁止している。	1	2%	
② 教職員が自分で持ち込んだコンピュータのネットワーク接続については、許可の基準(コンピュータウイルス対策など)を決めて許している。	42	91%	
③ 教職員が自分で持ち込んだコンピュータのネットワーク接続については、許可の基準(コンピュータウイルス対策など)もなく依頼された場合、そのまま接続を行わせている。	3	7%	
④ 教職員が自分で持ち込んだコンピュータのネットワーク接続することなどの要望は発生していない。	0	0%	

一切禁止または許可なく禁止している割合は93%である。許可の基準なく接続している割合は7%である。

平成17年10月に県教育長から各市町村教育委員会教育長、各県立学校長、各教育事務所長宛ての通知「個人情報及び校務に関わる情報等の取り扱いについて」における留意事項で個人所有のパソコンの校内LANへの接続について「個人所有のパソコンの校内LANへの接続は、原則として禁止する。ただし、校務上必要な場合は、学校長へ接続許可申請を行い、申請が適切である場合のみ許可する。」「学校長は、個人所有のパソコンの接続許可をする場合は、ファイル交換ソフトがインストールされていないこと、ウイルス対策ソフトがインストールされ、ウイルス定義ファイルが常に最新のものとなっていることを条件とする。」と定めている。

各学校において接続の許可の基準を定める場合は、上記の条件を最低条件として、新手の脅威に対応できるように常に基準の見直しを行い情報セキュリティが十分確保できるように努めなければならない。

Q7 校内ネットワーク運用管理規定は定期的に見直していますか。	回答数	回答率	
① 年に1回見直している。	11	24%	
② 学期毎に見直している。	0	0%	
③ 問題発生時に見直している。	22	48%	
④ 見直していない。	13	28%	

年に1回定期的に見直している割合は24%、問題発生時に見直している割合は48%である。また、見直していない割合は28%である。

「校内ネットワーク運用管理規定」は問題発生時の見直しだけでなく、現状の課題および問題点を常に調査して定期的に見直しして全職員へ周知徹底しなければならない。

(3) アンケートの分析結果の総括

アンケートの結果より、サーバの状態のチェックやバックアップ、コンピュータの処分等の情報セキュリティ担当者の取り組みは比較的良好な状態にあるが、情報セキュリティポリシー等の規定作りや教育用ネットワーク管理委員会等の組織作りの取り組みが不十分であることがわかった。県立学校全日課程においてはほとんどの学校で進路相談支援システムを活用し生徒の個人情報や校務処理にかかるデータを活用している状況で、情報セキュリティポリシーが教職員に周知徹底されていないのは情報流出に関してとても危険な状態であるといえる。早急に情報セキュリティポリシーを策定し教職員へ周知徹底する必要がある。

また、平成17年10月の県教育長からの通知「個人情報及び校務に関わる情報等の取り扱いについて」における留意事項で個人所有のパソコンの利用範囲を、「個人所有のパソコンを学校内で使用する場合は、教材作成等の範囲とし、個人情報及び校務に関わる情報等に関するデータの取り込み及び作成は禁止する。」と通知され、平成18年3月に県教育庁総務課長からの通知「業務情報の適正な管理について」においても「個人所有のパソコンによる業務情報の処理は行わないこと。」と通知されているが、ほとんどの学校で個人所有のパソコンを持ち込んで仕事をしている現状にある。以上の通知の中で、個人所有のパソコンの利用は、教材作成等

の範囲に限られることが明記されている。個人情報及び校務に関わる情報の流出を防ぐためには、以上の通知で定められたことを遵守する必要があるが、遵守するためには教職員一人一人が「遵守することの必要性」と、「遵守されなかったときに起こる情報流出等の脅威」を、校内研修等を通して教育情報化推進リーダーは全教職員に対して徹底して理解させる必要がある。

各学校においては、情報セキュリティに関する委員会を組織し、責任者および担当者を明確にし、学校全体で情報セキュリティに取り組む体制を早急に築き上げなければならない。

校内ネットワーク運用管理規定の見直しについても、「見直していない」または「問題発生時に見直している」学校の割合が約8割であることから問題を未然に防ぐための取り組みが不十分であることがわかる。また、インターネット利用等におけるトラブル発生時に外部からの苦情の窓口となる担当者が明確に定められていない学校が約4割もあることから発生して後で対応を検討するが情報セキュリティポリシー等の規定の整備、教職員および生徒への周知やその教育体制が不十分であることがわかる。

また、情報セキュリティポリシー策定後は定期的にそれを見なおし、学校全体の情報セキュリティに対する取り組みが有効に機能しているか常にチェックすることが必要である。

2 学校における個人情報保護と情報モラル教育の推進

情報化の進展とともに、情報社会に生きる私たちは、情報化の光の恩恵を受けるだけでなく、影にも対処することを学ばなければならない。情報教育を考える場合、「情報化の光と影」の部分を考える必要がある。学校では、「情報化による光の部分（便利な側面）」を学ぶとともに、「情報化による影の部分（危険な側面）」を克服するための教育をバランスよく進めていくことが大切である。

情報化の影の部分についての理解を深め、情報モラルの育成に努めることは、情報教育の重要な内容である。特に、情報の真偽に関わることや、著作権やプライバシーの問題などについては、具体的場面が発生した時に、見過ごすことなく繰り返し触れることが重要であり、すべての教員が正しい知識を持ち適切に指導できることが必要である。さらに、今後各教科の教材・指導計画の作成等や学習状況の整理・分析にコンピュータやネットワークが活用される中、著作権や個人情報の取り扱いは、すべての教員が正しく認識しなければならない重要な課題である。

このようなことから、今後の校内研修の中では、個人情報保護と情報モラル教育に関する内容を充実していくことが必要である。

(1) 個人情報の保護

個人情報は、いわゆるプライバシーに密接に関わる情報であり、その取り扱いの形態によっては、個人の人格的・財産的な権利利益を損なう恐れがある。この意味で、すべての個人情報は、個人の人格尊重の理念の下に慎重に取り扱われる必要がある。特にネットワーク環境の下では、適切な管理を怠ると個人情報が流出しやすいので注意が必要となる。教員は児童生徒の個人情報の取り扱いに留意するとともに、児童生徒に対しても適切な取り扱い方について指導しなければならない。

① 個人情報とは

氏名や住所、性別、生年月日、電話番号、学校名など、個人を特定できる情報のこと。

「個人情報」とは、「個人に関する情報で、特定の個人が識別され、または識別され得るもの」をいう。「特定の個人が識別される」とは、一般的にみて、情報の内容そのものから、特定個人のものと識別できるものを指す。また、「識別され得るもの」とは、その情報だけでは特定個人を識別できなくても、他の情報と組み合わせることで、容易に本人を識別できるものを指す。例えば「〇〇大会優勝者」とか「〇〇部のキャプテン」といった情報だけでも、特定の個人が識別できる個人情報にあたる。

② 個人情報の取得

個人情報の取得は利用目的の達成に必要な範囲内に限定して、原則として本人から取得するなど、適法かつ適正な方法で取得すること。

個人情報を取得する際は、その目的を明確化することが大切である。明確化することにより、必要な個人情報を限定できる。また、本人及び保護者の同意を得なければならない。本人および保護者が不安を感じることなく納得のいくように、利用目的を具体的にわかりやすく説明する必要がある。第三者への提供の可能性等があれば、その可能性等についても明確にする必要がある。例えば、同窓会やPTA等への名簿の提供がこれに当たる。個人情報を利用した場合に想定される危険性についても十分説明した上で同意を得るようにする。

③ 個人情報の利用

本人に利用の実態がわかるように利用目的を明確にして、その利用目的の範囲で取り扱い、むやみに第三者に提供しないこと。

個人情報を利用する際は、取得時に本人および保護者に明示した利用目的の範囲内で適切に利用しなければならない。利用目的の範囲内かどうか不明な場合は個人で判断せず、必ず学校管理者等に確認すること。

④ 個人情報の廃棄

個人情報を廃棄する際は漏えいに注意し、安全な方法で速やかに廃棄すること。

電子化された情報については、一般的な消去や初期化の操作等であれば復元される可能性がある。個人情報が第三者に漏えいしないように、専用ツール等を利用して一切のデータが復元されないようにするか、もしくは物理的破壊をして解読不可能な状態にする必要がある。

⑤ 個人情報の保護とその必要性

漏えいや改ざんなどがないように、適切な安全保護措置を講じること。

個人情報は、流出し悪用されるとさまざまな問題を引き起こす可能性がある。したがって、個人情報は「個人情報保護に関する法律」によって保護されている。基本四情報を含む個人情報が流出した場合、生命・財産が脅かされ、個人の権利利益が侵害される場合がある。（詐欺グループへの売渡、個人情報の買取請求、架空請求、振り込み詐欺、ストーカー事件等）また、病歴など医療に関する個人情報や、財産など経済活動に関する個人情報は、犯罪につながる可能性もあるため、これらの個人情報の保護について常に意識する必要がある。

○個人情報流出の事例

- ・生徒によるデータ流出（2005年6月）

中学校で生徒がパソコンを使い、校内LANから生徒約200人分の成績などの個人情報を不正に引き出した。

- ・個人所有パソコンからウィニーで流出（2005年6月）

学校で全生徒と職員の個人情報がインターネット上に流出。個人所有のパソコンがウィニーウイルスに感染していた。

- ・委託業者によりウィニーで流出（2006年2月）

学校でハードディスクの補修をした業者のウィニーウイルスに感染していた私用パソコンから、生徒と職員のデータが流出。

⑥ 学校における個人情報の安全管理のための取り組み

ほとんどの情報漏えいは人的な問題から派生しているので、安全管理体制を徹底すること。

学校における取り組みとして最も重要なことは、全職員の同意を得ると同時に、安全管理体制を徹底することであ

る。ほとんどの情報漏えいの問題は人的な問題から派生しているため、各学校では安全管理マニュアル等を作成し、職員研修等で周知徹底する必要がある。

○学校における個人情報の安全管理のための取り組みの参考例

- ・個人情報等の取り扱いに関する校内研修
- ・個人情報保護方針の内外への通知
- ・個人情報の取り扱いに関する保護者への通知・許諾等
- ・個人所有パソコンの使用，安全管理等
- ・個人情報流出等に備えた危機管理マニュアルの整備

(2) 情報モラル教育の推進

情報化の進展に伴う課題への対応として、インターネット等の利用に起因したトラブルや、インターネット上で人格形成に悪影響を及ぼすおそれのある有害情報が増えている現状を踏まえ、学校において「情報社会で適正な活動を行うための基となる考え方と態度」を育成する情報モラル教育の充実を図る必要がある。

① 情報モラルとは

情報社会で適正な活動を行うための基になる考え方と態度のこと。

情報モラルとは、「情報社会で適正な活動を行うための基になる考え方と態度」である。

情報通信ネットワークを介したコミュニケーションでは、しばしば通信先の相手の存在を忘れて、自分の目の前にあるコンピュータ端末に対して応答している錯覚に陥ることがある。また、ビデオゲームの場合などコンピュータの自動応答を人間的なものと混同することもある。通信相手が人であるかモノであるかを場面に応じて区別し、特に、情報の収集、発信、コミュニケーションなどの活動は、基本的には「人と人との間のコミュニケーション」であることを常に意識し、日常のモラルを適用していかなければならない。

② 情報モラル指導の配慮事項

情報社会について理解し、情報の受信者を意識した情報伝達の在り方やその責任について理解すること。

ア 情報の収集の場面において

適切な手段を用いて情報を収集することや、著作権などの知的財産権の尊重、情報の信憑（びよう）性（信頼性や品質）についての知識を持たせることが重要である。

a) 適切な手段を用いた情報の収集

あふれる情報の中から、自分を見失わず、情報がどのような過程を経て伝達されてきたのかを理解し、必要な情報を主体的に収集し、的確に判断する必要がある。また、情報源の違う情報を比較することができれば、情報を正しく判断することができる。

b) 著作権などの知的財産権の尊重

学校においても著作物を利用する機会が増える傾向にある。しかし、すべての著作物は、著作者本人の知的創作活動の所産であり、無断で複製、転載、改変等を行うことは原則として禁止されている。ただし、教育、福祉、報道等において、「例外的」に利用が認められる場合があるので、学校において権利侵害が起こらないよう、教員は著作権に関する正しい認識を持つ必要がある。

○著作権法 35 条

- ・「学校その他の教育機関（営利を目的として設置されているものを除く）において教育を担任する者及び授業を受ける者は、その授業の過程における使用に供することを目的とする場合には、必要と認められる限度において、公表された著作物を複製することができる。」

- ・著作物とは・・・「思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものをいう（著作権法第2条第1項第1条）。」教師が作成した教材だけでなく、幼児や児童生徒が描いた絵や文章であっても著作権が発生する。
- ・著作権とは・・・著作物など創造的活動によって生産された作品や発明や発見によって得られたものを知的財産と呼んでいる。知的財産のうち、小説や音楽、美術など文化的価値の高い創造物を保護する権利が著作権である。
- ・著作権の保護期間・・・著作権は、著作物が創造された時点から、著作者の死後 50 年（映画は公開されてから 70 年）保護される。

○学校における著作物の利用に関する「例外」事項

例外事項	例
私的使用（個人の学習目的を含む）のための児童生徒による複製	・児童生徒が調べ学習で、ホームページにあった資料を印刷して自分で使う
自分の授業のための教員による複製	・担任の教員が、他人のホームページにあった資料をダウンロードし、コピーして生徒に配る
引用	・児童生徒がインターネットから取り込んだ資料を、学習成果の発表のため、自分の意見の補強教材として「引用」する（資料名や著作者名の表示が必要）
試験問題への複製	・担任の教員が、他人のホームページにあった資料をダウンロードし、それらの資料を試験問題に利用する
非営利の上映・演奏	・ブラスバンド部が発表会で他人の曲を演奏すること、また、同時に校内放送で流す

c) 情報の信憑性

信憑性とは、伝わってきた情報を信頼することができる度合いである。情報を収集して受け取る際に、その情報の信憑性を十分に検討する必要がある。

○正確な情報を収集する際の注意点

- ・公共機関など責任ある組織や人が発信している情報かどうか確認する
- ・はじめからひとつの情報元からの情報を信じずに、情報の妥当性について検討する
- ・複数の情報元で確認する

イ 情報の発信の場面において

プライバシーの保護、著作権などの尊重、発信する情報の信憑性（正確性や信頼性）、情報の受信者を考慮した表現方法の工夫などの意識を持たせることが必要である。

a) プライバシーの保護

個人情報や無断で開示するなどして、他人のプライバシーを侵害しないこと。また、プライバシー侵害等の被害予防のために、むやみにプライバシーを開示しないこと。

b) 著作権などの尊重

情報の発信者として、著作物の利用には著作権の許諾が原則として必要であり、著作者の権利の保護の観点から、著作物の取り扱いに注意を払うこと。

○著作者の了解が必要な場合の例	
事 例	対 応
児童生徒の作品	・ 本人及び保護者の同意を得る
リンク集の作成	・ 他のホームページに掲載されているリンクをそのまま掲載できない ・ リンクを張ることは許諾なしで行えるが、許諾を得るマナーを心掛ける
ホームページの利用と作成	・ 出典を明記する ・ 著作権者に許諾を得る
電子掲示板、電子メールの情報	・ 内容を蓄積しメーリングリストなどで発信する場合は「複製権」「公衆通信権」に違反しないよう、許諾を得る
音楽やパソコンソフトのコピー	・ コピーをすることは著作権法違反となり原則として不可 (CDやフロッピーにコピーする場合だけでなく、ハードディスクにインストールすることも複写となる。また、1つのソフトを校内LANで各端末PCにインストールすることも複写となり、違反である)
教育情報資料のデータベース構築	・ サーバーに載せること自体が「複製権」等に関わるため、あらかじめ利用形態、利用範囲、期間を明確にして許諾を得る。
教材のデジタル化	・ 教材として使用するために既存の著作物をデジタル化する場合に許諾を得る

c) 情報の信憑性

電子メールや電子掲示板など、インターネット上のサービスの充実により、個人が自由に情報発信することが容易になった。ところが、その容易さと裏腹に、誤った情報が広がる可能性も高くなった。インターネット等を通じて発信した情報は不特定多数の人に見られることになり、ちょっとした間違いや誤った操作が、ネットワークを介して瞬時に世界中に伝達され、予想しえない影響を与えてしまう可能性がある。また、ネットワーク上では人と人との対面のコミュニケーションでは考えられないような誤解を生じることが起こりえる。このようなことから、情報モラルとあわせて、自らの作り出す情報が他の人々や社会に及ぼす影響などを十分認識して、情報発信に伴う責任について理解させることが大切である。

ウ コミュニケーションの場面において

日常生活と同様、情報通信ネットワークを介したコミュニケーションにもエチケットがあり、こうした「ネチケット」に留意することや、相手の人数やTPO（Time,Place,Occasion）に応じたメッセージのやりとりを行うことに配慮することが必要である。

③ 情報社会に参画する態度とは

情報社会に積極的に参加し、よりよい社会にするために貢献しようとする態度のこと。

社会生活の中で情報や情報技術が果たしている役割や及ぼす影響を理解し、情報モラルの必要性や情報に対する責任について考え、望ましい情報社会の創造に参加しようとする態度である。

④指導者としての教師の役割

児童生徒自身の、不適切な情報に対処できる能力を育成すること。

学校教育において大切なことは、情報教育を通じて、あふれる情報の中から正しい情報を主体的に判断できる能力の育成や、情報化の影の部分についての理解を深め、情報モラルの育成に努めることである。しかし、こうした不適切な情報への対応のための指導は、情報教育だけで行われるべきものではない。生徒指導の充実とともに、学校教育全体として、日頃より、道徳性の涵養（かんよう）とともに、薬物乱用や性に関する情報への対応など適切な意思決定や行動選択の必要性への理解などに努めることが必要である。

○指導者としての教師の役割の参考例

- ・バーチャルコミュニティでは、活動していくために必要な常識や決まりが確立していない
- ・社会経験の不足による未熟な判断・行動が危険を招く恐れがある
- ・周囲（教師・保護者）による保護と警戒が必要
- ・児童生徒自身の判断力を養成（必要に応じ適切な助言や判断上の観点を示す
＝過干渉は避ける）

Ⅲ 成果と課題

今回の調査により、学校における情報セキュリティポリシーが策定されていないこと、策定されていても教職員に周知徹底されていないこと、また、策定されていても定期的に見直しがされていない実態が把握できた。また現在、学校で策定された情報セキュリティポリシーは、平成15年11月に沖縄県教育委員会より発行された「IT安全管理マニュアル」を参考に策定されたものである。この「IT安全管理マニュアル」はインターネット利用におけるガイドラインの解説となっており、現状においては個人情報及び校務に関わる情報等の取り扱いに関するガイドラインをより明確に打ち出す必要がある。そこで、個人情報及び校務に関わる情報等の取り扱いに関する規定を重視して「情報セキュリティ管理マニュアル」を作成し、資料編に掲載した。また、情報セキュリティに関しては委員会を設置して組織で対応する必要があるが、半数以上が設置されていない現状である。そこで「情報セキュリティ管理マニュアル」の中で、その委員会の編成に際して参考となる具体例をあげた。また、情報セキュリティに関するトラブル発生時の対応についても参考となる具体例を挙げた。学校における情報セキュリティポリシーの策定や見直しに際する参考資料として、資料編に掲載した「情報セキュリティ管理マニュアル」や「ネットワークセキュリティガイドライン」を学校に提供できたことが本研究の成果である。

各学校の情報セキュリティポリシーを見直す具体的な参考資料として「情報セキュリティ管理マニュアル」を作成したが、ICTにかかる環境の変化はめまぐるしいものがあり、各学校においては、各学校の情報セキュリティポリシー策定後も、ICTにかかる環境の変化に対応して情報セキュリティを十分に確保できる体制を継続していかなければならない。

Ⅳ 主要参考文献

- ・横浜市教育委員会「インターネット利用にあたってのガイドライン（学校向け解説書）」2002年4月
- ・阿濱茂樹 日本情報教育開発協議会 「インターネット社会を生きるための情報モラル（中学生版）」2006年9月
- ・沖縄県教育委員会 「第2次沖縄県教育情報化推進計画」 2006年3月
- ・文部科学省「情報教育の実践と学校の情報化～新『情報教育に関する手引き』」～ 2002年6月
- ・熊本県教育委員会 「インターネット・携帯電話の利用に関する家庭向け指導資料」 2005年3月
- ・埼玉県教育委員会 情報化に対応した安全管理体制の整備 2003年3月
- ・経済産業省委託調査研究 「平成15年度初等中等教育現場における情報セキュリティにかかる現状調査報告書」
「学校における情報セキュリティの現状報告について(アンケートの部)」 2004年3月