

教育現場における情報セキュリティ事故・対応事例の研究

事 例 集

特定非営利活動法人 NPO 情報セキュリティフォーラム
横浜市神奈川区鶴屋町 2-17 相鉄岩崎学園ビル
TEL 045-311-8777 FAX 045-311-8747
<http://www.isef.or.jp> E-mail: isef@isef.or.jp

教育現場における情報セキュリティ事故・対応事例の研究 事例集

特定非営利活動法人 NPO 情報セキュリティフォーラム

1. 趣旨

インターネットの利用環境や移動体通信環境の整備の進展、e-Japan 戦略などの政府の強力な IT 推進施策によってインターネットが急速に普及し、様々な行政サービスや民間の e ビジネスが誕生しています。また、Web サイトやブログ、電子メールなどを利用した情報の受発信も活発に行われており、インターネットは様々なサービスやコミュニケーション手段をもたらし、いまや私たちの生活に欠かすことのできないものとなっています。

一方で、昨今の報道にありますようにインターネットを中心としたコンピュータや携帯端末、携帯電話を使った事件・事故が急増しています。個人情報の漏えいによるプライバシーの侵害、電子メールを使った架空請求、ワンクリック詐欺やフィッシング詐欺など例を挙げればきりがありません。

インターネットを中心とした情報機器の利用は、その性質上、相手の顔が見えにくく、そのため事件・事故に巻き込まれる対象は、インターネット利用者層の拡大とともに最近では社会経験の少ない高校生やさらに小中学生へと低年齢化が進んでいます。

また、ネットワーク技術やセキュリティプロダクツは極めて速いスピードで技術革新し、新技術に基づく新サービスが次々に誕生していますが、それを利用した事件の手口も巧妙化し、事故も複雑化しています。昨日安全安心であったサービスが今日安全安心であるとは限らないというのが実情となっています。

さらに、インターネットは双方向の通信手段です。利用者は被害者にもなりうる反面ささいな言葉の行き違いで相手を怒らせてしまったり、情報機器の誤操作によって悪意があるわけでもなく意図したわけでもなく加害者にもなりうることも起きてしまっています。

こうした情報化社会の進展に伴うインターネットを中心とした情報機器利用の急増は、残念ながら予期せぬ事件・事故を生み出してしまっていますが、報道など伝達される情報は、被害が中心となっており、事件・事故の手口・経緯やその後の防止対策が児童・生徒・学生、教職員らに正確に伝達・認識されていないケースも多くなっています。また、情報教育が始まったばかりの教育現場では、情報モラルを含む安全教育が思うように進展していない現状もあります。

本研究では、学校における情報教育に限らず、児童・生徒・学生、教職員がパソコン、携帯電話などの様々な情報機器の利用や情報サービスの利用によって起こってしまった事件・事故の事例を収集し、公開し、情報を共有することで、児童・生徒・学生がどのような場面においても事件・事故に遭遇することなく、安全で安心して学校生活、社会生活を営めることを願って実施しております。ぜひとも皆様にご活用いただけることを期待しております。

なお、本研究の成果として取りまとめました本事例集は Web サイト等において広く公開し、より多くの教職員、学校関係者にご利用いただきたい考えでおります。

2. 調査基礎データ

(1) 事例収集期間 平成16年8月～平成18年12月

(2) 収集方法 個別訪問によるヒアリング

(3) 収集事例数 200件

(4) 学校別事例収集内訳

小学校	8件
中学校	24件
高等学校	154件
専門学校	14件

(5) 事例別収集内訳

		被害・事故 事例	対策・指導 事例
個人情報・学校情報関係	45件	9件	36件
著作権関係	5件	0件	5件
ID・パスワード関係	13件	7件	6件
コンピュータウイルス関係	16件	13件	3件
携帯電話・電子メール関係	41件	33件	8件
Webサイト関係	7件	4件	3件
掲示板・チャット関係	28件	23件	5件
サーバ関係	4件	3件	1件
ネットワーク関係	8件	7件	1件
OS・アプリケーション関係	3件	3件	0件
データの削除・改変関係	4件	4件	0件
講習会・授業関係	24件	0件	24件
学校備品の盗難関係	2件	2件	0件

3. 事例概要

(1) 生徒情報・学校情報の管理

平成 17 年 4 月に個人情報保護法が全面施行され、学校においても生徒情報の取り扱いに様々な取り組みを実施している。

一方で、個人情報を適切に管理する具体的な対策が文書化されていない事例も報告されており、学校現場の校務に則した管理対策の文書化が今後の課題として挙げられる。

【高等学校の事例】

個人情報保護法の施行以降、特に生徒の氏名や住所、成績などの情報を適切に取り扱うようにしている。平成 17 年度まで生徒の希望により実施していた資格認定試験を、平成 18 年度から全生徒が取得を目指すべき資格として位置づけ、生徒全員に受験させることとした。平成 17 年度までは、希望者のみが参加していた資格認定試験だったので、希望者から主催者に個人情報を提供する許諾を得ていたが、平成 18 年度は学校全体で参加することになったので、学校から主催者に個人情報を提供する許諾を得るための文書を保護者に発送することとした。

【高等学校の事例】

中学を訪問する際に、中学側から卒業生の様子を聞かれることがある。高校としても生徒の様子を伝えることが必要だと考えており、生徒の成績や進路情報などを訪問時に持参している。持参する際には、情報を途中で紛失しないように注意を払い、また、訪問先の中学校に情報を置き忘れることがないようにするために、全教員に周知徹底している。

中学校側の管理の問題もあるので、持参した生徒情報は必ず学校に持ち帰り、学校で廃棄している。個人情報を適切に管理することは、全教員に口頭で周知徹底しているが、具体的な管理対策が文書化されていない。より適切に個人情報を管理するためにも、具体的な管理対策を文書化することが今後の課題である。

平成 17～18 年にかけて、名簿や顧客情報などの個人情報や技術資料などの重要情報がファイル交換ソフトを介して漏えいする事件・事故が多数報道され、学校においてもファイル交換ソフトを介した情報漏えいへの注意喚起が行われている。

一方で、学校が直接管理している情報ではないが、部活動の OB 会が管理している名簿情報がファイル交換ソフトを介してネットワーク上に流出した事例も報告されており、ファイル交換ソフトを利用している児童・生徒、教職員、保護者への意識向上に向けた取り組みが今後の検討課題として挙げられる。

【高等学校の事例】

教育委員会からの通達があり、学校内で利用するすべてのパソコン、教員の私物パソコンについてファイル交換ソフトの利用状況の調査を実施した。学校内で利用するパソコン、教員の私物パソコンからファイル交換ソフトは発見されなかったが、ファイル交換ソフトの利用について認識が甘い教員もいるので、教員の意識向上のための取り組みを検討している。

今回の調査では、自宅も含めてファイル交換ソフトを利用している教員はいなかったが、仮にファイル交換ソフトを私的に利用しようとする教員がいた場合、強制的に利用をやめさせることは難しいと考えているので、ファイル交換ソフトを利用している教員がいた場合の対応が今後の検討課題と認識している。また、自宅において過去にファイル交換ソフトを利用したことのある教員がいる可能性もあるが、現段階では通常のダウンロードのみで情報漏えいには関係ないと認識している。

ファイル交換ソフトを介した情報漏えいの仕組みを口頭で説明しただけでは教員の認識も変化しないと思うので、デモ環境を構築し、ファイル交換ソフトによる情報流出の現状を見せることも検討している。

【高等学校の事例】

部活動 OB 会が管理している OB 会名簿が、ファイル交換ソフトを介してインターネット上に流出していた。OB 会名簿には数十件の氏名、住所、電話番号が記載されていたが、在校生の情報は記載されていなかった。

部活動 OB 会は任意の団体であり、OB 会の運営について学校側が管理すべきものではないとの認識ではあるが、学校の代表電子メールアドレスに情報流出の連絡メールが届いていたので、該当の部活動の OB 会にインターネット上に OB 会名簿が流出している事実を伝えた。流出してしまった名簿の情報をすべて回収することは困難なことであり、今後同様の事故が発生しないことが大切なので、適切な情報管理を行うように部活動 OB 会にお願いをした。

(2) ID・パスワードの借用

学校内のネットワーク環境の整備にともない、個人認証のもとで利用できる環境が整備され、生徒それぞれに ID・パスワードが付与されているが、生徒の ID・パスワードへの認識の甘さから、ID・パスワードを不正利用していたずらメールを送信した事例が報告されている。

【高等学校での事例】

生徒が、同級生のユーザ ID とパスワードを無断で利用して、その同級生の電子メールアドレスで友人にいたずらメールを送信していた。電子メールは学校外へも送信することが可能だが、学校外へいたずらメールを送信した形跡はなかった。

校内のネットワーク管理者にログ調査を依頼し、ユーザ ID とパスワードが無断で利用されていた時間帯、パソコンを特定した。その時間帯に当該パソコンを利用していたクラスを確認し、不正にユーザ ID とパスワードを利用した生徒を特定した。特定した生徒を呼び出し本人に事実の確認を行ったところ、同級生のユーザ ID とパスワードを無断で利用したことを認めた。また、パスワードを入手した経緯を確認したところ、ユーザ ID とパスワードを不正利用された生徒自らがパソコンの起動を依頼するために自分のユーザ ID とパスワードを教えていたことが判明した。他人のユーザ ID とパスワードを無断で利用する行為は不正アクセス禁止法に抵触する行為で絶対にやってはならないことと指導し、自宅謹慎を含む厳しい処罰を行った。

全生徒に対して、今回の経緯の説明とユーザ ID とパスワードを各自でしっかり管理するように文書で注意を行った。

(3) 携帯電話の利用に伴うトラブル

携帯電話を保有している児童・生徒が増加し、携帯電話の電子メールによるコミュニケーションが盛んに行われているが、些細な出来事からトラブルに発展するケースが報告されている。

【高等学校での事例】

多くの生徒が携帯電話を保有するようになり、学校内でも生徒同士で携帯電話の電子メール機能を利用したコミュニケーションが行われているが、学校内での些細な出来事により頻りにメール交換していた相手に嫌がらせメールを送信するなどのトラブルが発生している。トラブルが発生する時期は主に 4~6 月で、特に高校 1 年生が多い。嫌がらせメールを送信する際に、自分の携帯電話ではなく友人の携帯電話から嫌がらせメールを送信していることもある。

また、携帯電話の電子メールアドレスを偽装して、特定の生徒を誹謗・中傷するなりすましメールによるトラブルも報告されており、情報モラルを含めた携帯電話の適切な取り扱い方を指導する必要性の認識はあるものの、指導時間の確保の難しさから指導できていない現状もうかがえる。

【高等学校での事例】

生徒がメールアドレスを偽装できる Web サイトを使用して他の生徒になりすまし、特定の生徒を誹謗・中傷するメールを送信した。誹謗・中傷を受けた生徒は、メールを送信した生徒に対して抗議を行ったが、抗議を受けた生徒は第三者にメールアドレスを利用されただけで実際にメールを送信していなかった。

個人を誹謗・中傷するメールを送らないようにホームルーム時にクラス全員に注意を行った。その際、生徒の情報から、携帯電話の Web サイトに携帯電話のメールアドレスを偽装して送信するウェブサイトを利用している生徒が多数いることが明らかになった。後日、クラスの中の一人が被害生徒に誹謗・中傷のメールを送信していたことが判明したので、担任教員が誹謗・中傷を行った生徒を呼び出し、メールアドレスを偽装してなりすましメールを送信しないように指導を行った。

【中学校での事例】

生徒に対して、生徒が嫌がる内容を記載したメールが頻繁に届くようになった。メールの内容から、送信者はおそらく同級生によるものと推測できたが、送信メールアドレスを変更するなどして送信者が特定できないようにしている。嫌がらせメールを受け取った生徒はショックを受け、教員に対応方法を相談してきた。

嫌がらせメールが頻繁に届くようになった生徒には、届いたメールは無視するように伝えた。また、メールアドレスを変更して、メールが届かないようにすることも 1 つの対策であることを伝えた。

携帯電話を利用して電子メール、掲示板、ブログを利用する生徒が増えている。また、メール、掲示板、ブログに友人の悪口を記載する生徒も多く、インターネット上に掲載された情報が全世界に公開されているという認識もない。今後は、生徒に情報モラルを指導する予定だが、通常のカリキュラムの都合もあり、現実的に多くの時間を割いて指導できていない現状もあり、適切な指導方法を検討中である。

(4) 掲示板の書込みトラブル

掲示板への不適切な書込みによるトラブル事例が多く報告され、中には書込みが原因で、学校を辞めてしまった事例も報告されている。

また、トラブルの多くが携帯電話を利用しているため、携帯電話専用の掲示板サイトであったり、Web フィルタリングが行われているために、学校のパソコンからすぐに確認できず、対応に時間がかかるケースもみられる。

【高等学校での事例】

個人が管理する学校名を冠した携帯電話専用の掲示板に、複数の生徒の誹謗・中傷が実名つきで書込まれた。誹謗・中傷を書込まれた生徒達はショックを受け、学校を休みがちになったり、学校を辞めた者もいた。

書込みをした人物は特定できなかったが、書込みの内容から同じクラスの生徒の書込みと推測できたので、担任教員がホームルームの時間にインターネット上で誹謗・中傷をせずに、マナーを守って利用するように指導を行った。また、同学年でも同じ掲示板を利用している生徒がいると考えられたので、学年集会で同様の指導を行った。指導後、実名を挙げての誹謗・中傷の件数は減少したものの完全にはなくならなかったため、誹謗・中傷を注意する書込みを担任教員が当該掲示板に行った。担任教員からの書込み以降、当該掲示板において、誹謗・中傷の書込みはなくなった。

【高等学校での事例】

掲示板に生徒の実名を明記した上で、その生徒を誹謗・中傷する書込みが記載されていた。誹謗・中傷の書込みをされた生徒は精神的にショックを受けていた。

生徒からの相談を受け、すぐに当該の掲示板の確認を行った。学校のパソコンは Web フィルタリングを導入しているため早急に該当の掲示板を確認することができなかったため、情報担当教員の自宅のパソコンを利用して掲示板の確認を行った。

書込みを確認し、掲示板の削除方法を確認した上で、学校の代表電子メールアドレスから掲示板運営者にメールにて削除依頼を行った。数日後、掲示板の書込みが削除されたことを確認した。なお、書込みをした人物の特定はできなかった。

(5) 情報モラル・マナーの指導

インターネット利用の低年齢化にともない、学校においても低学年から情報モラル指導や自宅でパソコンやインターネットを利用する際にトラブルに巻き込まれないための指導が行われている。

【中学校での事例】

インターネット利用者の低年齢化を鑑み、今までは中学 2 年生以上を対象に実施していた情報モラル指導を平成 18 年度からは中学 1 年生に対しても実施することとした。小学生の頃よりインターネットを利用している生徒が増えてきており、中学生であってもインターネットのトラブルに巻き込まれる可能性があるため、トラブルに巻き込まれないために入学して間もない中学 1 年生に情報モラル指導を実施することとした。1 年生全員を同じ教室に集め、Web サイトや電子メールを利用してトラブルに巻き込まれない指導を講義形式で行った。最近では、ブログを利用して情報発信をしている生徒もいるので、特に個人情報や他人を誹謗・中傷するような情報を書込まないように指導した。

【高等学校での事例】

架空請求メールやフィッシング詐欺などのインターネットを利用した事件が多発している状況から生徒への安全教育の必要性を感じ平成 17 年 1 月に外部機関主催の安全教育セミナー資料を用いて特別授業を実施した。授業時の生徒の反応もよく、生徒のリテラシー教育に効果のあるコンテンツだったので、平成 17 年度より必修となっている教科「情報」の年間スケジュールに組み込み、毎年実施することとした。

一方で、年間カリキュラムの制約もあり、セキュリティ対策の指導時間の確保や実施方法などの課題も抱えている。

【高等学校での事例】

生徒が学校内で利用するネットワークやパソコンはウイルス対策ソフトやフィルタリングなどのセキュリティ対策が実施されているため、生徒は校内でのパソコン利用にあたってはセキュリティ対策が実施されていることを日常的に体感している。したがって、校内での利用にあたって、セキュリティ上の大きなトラブルは発生していない。しかし、生徒が自宅で利用しているパソコンは、セキュリティ対策が実施されているものも実施されていないものもある。そこで、自宅のパソコンのセキュリティ対策を生徒自身が実施する、また、インターネットを利用する際にトラブルに巻き込まれないための知識を生徒が身につける必要があると認識している。

情報の授業ではカリキュラムの都合もあり、セキュリティ対策のみの時間を設定することが難しい状況となっている。

また、保護者に対して講習会を開催し、家庭における情報セキュリティ教育の実施を推進する動きも見られている。

【高等学校での事例】

生徒は自宅でも Web サイトの閲覧や電子メールの送受信などインターネットを利用しており、生徒がインターネットを利用する際にトラブルに巻き込まれないようにするためには、学校での指導とともに保護者からセキュリティ教育をする必要があると認識している。しかし、子どもを指導するための知識やスキルを保有していない保護者も多いと認識しているため、指導できる知識やスキルを身につけるための安全教室を開催することとした。

目 次

I. 被害・事件事例編

1. 個人情報・学校情報関係

1-1	なりすましによる個人情報の聞き出し	1
1-2	生徒の携帯電話の紛失による情報の漏えい	2
1-3	ずさんなデータ管理 1	3
1-4	ずさんなデータ管理 2	4
1-5	電子メールアドレスの不用意な公開	5
1-6	ファイル交換ソフトを介した部活動 OB 会名簿の流出	6
1-7	女子生徒を狙った盗撮	7
1-8	携帯電話のカメラ機能を利用した盗撮	8
1-9	就職活動情報漏えい	9

2. ID・パスワード関係

2-1	予期しない他人のメールアドレスの取得	10
2-2	ユーザ ID とパスワードの不正利用によるいたずらメールの送信	11
2-3	パスワード解析ソフトを利用した不正なアクセス	12
2-4	パスワードの漏えいによる試験問題流出	13
2-5	ユーザ ID とパスワードの借用 1	14
2-6	ユーザ ID とパスワードの借用 2	15
2-7	ユーザ ID とパスワードの借用 3	16

3. コンピュータウイルス関係

3-1	教員によるコンピュータウイルス感染 1	17
3-2	教員によるコンピュータウイルス感染 2	18
3-3	教員によるコンピュータウイルス感染 3	19
3-4	教員によるコンピュータウイルス感染 4	20
3-5	教員によるコンピュータウイルス感染 5	21
3-6	教員によるコンピュータウイルス感染 6	22
3-7	生徒によるコンピュータウイルス感染 1	23
3-8	生徒によるコンピュータウイルス感染 2	24
3-9	生徒によるコンピュータウイルス感染 3	25
3-10	生徒によるコンピュータウイルス感染 4	26
3-11	スパイウェア被害 1	27
3-12	スパイウェア被害 2	28
3-13	スパイウェア被害 3	29

4. 携帯電話・電子メール関係

4-1	チェーンメール1	30
4-2	チェーンメール2	31
4-3	チェーンメール3	32
4-4	チェーンメール4	33
4-5	チェーンメール5	34
4-6	チェーンメール6	35
4-7	携帯電話を利用した嫌がらせメール1	36
4-8	携帯電話を利用した嫌がらせメール2	37
4-9	携帯電話を利用した嫌がらせメール3	38
4-10	携帯電話を利用した嫌がらせメール4	39
4-11	携帯電話を利用した架空の料金請求メール1	40
4-12	携帯電話を利用した架空の料金請求メール2	41
4-13	携帯電話を利用した架空の料金請求メール3	42
4-14	携帯電話を利用した架空の料金請求メール4	43
4-15	携帯電話を利用した架空の料金請求メール5	44
4-16	携帯電話を利用した架空の料金請求メール6	45
4-17	携帯電話を利用した電子メールのトラブル	46
4-18	生徒同士での脅迫メール	47
4-19	交際を迫る執拗なメール	48
4-20	なりすましメールによる誹謗・中傷	49
4-21	携帯電話へのチェーンメールや架空請求メール	50
4-22	フィッシングメール	51
4-23	不当請求メール	52
4-24	携帯電話を利用した架空の料金請求1	53
4-25	携帯電話を利用した架空の料金請求2	54
4-26	ワンクリック詐欺への対応	55
4-27	不当な料金の請求メールへの対応	56
4-28	公開電子メールアドレスへの大量の迷惑メール1	57
4-29	公開電子メールアドレスへの大量の迷惑メール2	58
4-30	公開電子メールアドレスへの大量の迷惑メール3	59
4-31	公開電子メールアドレスへの大量の迷惑メール4	60
4-32	振り込め詐欺1	61
4-33	振り込め詐欺2	62

5. Web サイト関係

5-1	出会い系サイトを発端とした家出	63
5-2	ブラウザクラッシャー	64
5-3	インターネット上での残虐映像の閲覧	65
5-4	フィルタリングソフトによる Web サイトの閲覧制限	66

6. 掲示板・チャット関係

6-1	掲示板への不適切な書込み被害 1	67
6-2	掲示板への不適切な書込み被害 2	68
6-3	掲示板への不適切な書込み被害 3	69
6-4	掲示板への不適切な書込み被害 4	70
6-5	掲示板への不適切な書込み被害 5	71
6-6	掲示板への不適切な書込み被害 6	72
6-7	掲示板への不適切な書込み被害 7	73
6-8	掲示板への不適切な書込み被害 8	74
6-9	掲示板への不適切な書込み被害 9	75
6-10	掲示板への不適切な書込み被害 10	76
6-11	掲示板への不適切な書込み被害 11	77
6-12	掲示板への不適切な書込み被害 12	78
6-13	掲示板への不適切な書込み被害 13	79
6-14	掲示板への不適切な書込み被害 14	80
6-15	掲示板への不適切な書込み被害 15	81
6-16	掲示板への不適切な書込み被害 16	82
6-17	掲示板への不適切な書込み被害 17	83
6-18	掲示板への不適切な書込み被害 18	84
6-19	画像掲示板への投稿被害	85
6-20	掲示板や個人所有 Web サイトでの誹謗・中傷	86
6-21	掲示板荒らし行為	87
6-22	不適切な画像を利用したイベント広報	88
6-23	掲示板の書込みに対する捜査協力	89

7. サーバ関係

7-1	無停電電源装置の故障によるサーバのダウン	90
7-2	大量パケット送信（攻撃）による Web サーバのダウン	91
7-3	複数の DHCP サーバによる接続障害	92

8. ネットワーク関係

8-1	物理的な LAN ケーブルのショート	93
8-2	ネットワークケーブルの配線ミス	94
8-3	ネットワークコマンドの誤利用によるウイルス騒ぎ	95
8-4	不用意なダウンロードによるネットワーク回線速度の低下	96
8-5	サブネットマスク設定ミスによるネットワーク障害	97
8-6	付箋プログラム利用によるネットワークダウン	98
8-7	誤った無線 LAN 接続先	99

9. OS・アプリケーション関係

- 9-1 ウィンドウズアップデートによる起動停止トラブル100
- 9-2 いたずらによる授業支援システムの停止101
- 9-3 生徒によるシステム設定の変更102

10. データの削除・改変関係

- 10-1 生徒用ファイルサーバ内のデータの改変103
- 10-2 誤操作によるファイルの移動104
- 10-3 生徒による共有フォルダへのいたずら105
- 10-4 教員の誤操作による生徒用フォルダへのデータ保存106

11. 学校備品の盗難関係

- 11-1 学校設置パソコンへの児童によるいたずら107
- 11-2 学校備品の盗難108

Ⅱ. 対策・指導事例編

1. 個人情報・学校情報関係

1-1	生徒情報（個人情報）の管理対策 1	109
1-2	生徒情報（個人情報）の管理対策 2	110
1-3	生徒情報（個人情報）の管理対策 3	111
1-4	生徒情報（個人情報）の管理対策 4	112
1-5	生徒情報（個人情報）の管理対策 5	113
1-6	生徒情報（個人情報）の管理対策 6	114
1-7	生徒情報（個人情報）の管理対策 7	115
1-8	生徒情報（個人情報）の管理対策 8	116
1-9	生徒情報（個人情報）の管理対策 9	117
1-10	生徒情報（個人情報）の管理対策 10	118
1-11	生徒情報（個人情報）の管理対策 11	119
1-12	生徒情報（個人情報）の管理対策 12	120
1-13	生徒情報（個人情報）の管理対策 13	121
1-14	生徒情報（個人情報）の管理対策 14	122
1-15	生徒情報（個人情報）の管理対策 15	123
1-16	生徒情報（個人情報）の管理対策 16	124
1-17	生徒情報（個人情報）の管理対策 17	125
1-18	生徒情報（個人情報）の Web サイト上での管理対策 1	126
1-19	生徒情報（個人情報）の Web サイト上での管理対策 2	127
1-20	生徒情報（個人情報）の Web サイト上での管理対策 3	128
1-21	生徒情報（個人情報）の Web サイト上での管理対策 4	129
1-22	生徒情報（個人情報）の Web サイト上での管理対策 5	130
1-23	生徒情報（個人情報）の Web サイト上での管理対策 6	131
1-24	生徒情報（個人情報）の Web サイト上での管理対策 7	132
1-25	生徒情報（個人情報）の Web サイト上での管理対策 8	133
1-26	生徒情報（個人情報）の Web サイト上での管理対策 9	134
1-27	生徒情報（個人情報）の Web サイト上での管理対策 10	135
1-28	学校 Web サイトで使用する画像の転載対策	136
1-29	なりすましによる個人情報の聞き出しへの注意喚起 1	137
1-30	なりすましによる個人情報の聞き出しへの注意喚起 2	138
1-31	ファイル交換ソフト利用への注意喚起	139
1-32	ファイル交換ソフトの利用状況調査	140
1-33	個人情報の取り扱いに関する保護者からの問い合わせへの対応	141
1-34	Web サイトによる情報公開 1	142
1-35	Web サイトによる情報公開 2	143
1-36	学校の防犯に関する要望	144

2. 著作権関係

2-1	生徒への著作権指導 1	145
2-2	生徒への著作権指導 2	146
2-3	ファイル交換ソフト使用の指導	147
2-4	Web サイトへの掲載情報についての指導	148
2-5	教員向け著作権講習会の開催	149

3. ID・パスワード関係

3-1 ユーザIDとパスワードの貸し借り防止対策1	150
3-2 ユーザIDとパスワードの貸し借り防止対策2	151
3-3 ユーザIDとパスワードの貸し借り防止対策3	152
3-4 ユーザIDやパスワードの管理指導1	153
3-5 ユーザIDやパスワードの管理指導2	154
3-6 ユーザIDやパスワードの管理指導3	155

4. コンピュータウイルス関係

4-1 個人所有パソコン利用教員へのコンピュータウイルス対策	156
4-2 生徒の自宅パソコンへのコンピュータウイルス感染対処方法の指導	157
4-3 コンピュータウイルス感染を誘う手口	158

5. 携帯電話・電子メール関係

5-1 料金の架空請求メールへの指導	159
5-2 振り込み詐欺や料金の架空請求メールへの指導	160
5-3 迷惑メールへの指導	161
5-4 架空請求メールやワンクリック詐欺への指導	162
5-5 フィッシング詐欺やワンクリック詐欺への指導	163
5-6 巧みな呼び込みメール	164
5-7 振り込み詐欺への注意喚起	165
5-8 架空請求メールへの注意喚起	166

6. Webサイト関係

6-1 出会い系サイト利用指導1	167
6-2 出会い系サイト利用指導2	168
6-3 Webサイトでの情報発信時における注意点の指導	169

7. 掲示板・チャット関係

7-1 チャットの利用指導	170
7-2 掲示板・チャットの利用指導	171
7-3 体験学習による掲示板の利用指導	172
7-4 掲示板サイトへの書込み巡回調査1	173
7-5 掲示板サイトへの書込み巡回調査2	174

8. ネットワーク関係

8-1 校内ネットワークフォルダの不正利用防止対策	175
---------------------------	-----

9. OS・アプリケーション関係

9-1 校内パソコンのセキュリティ対策	176
---------------------	-----

10. 講習会・授業関係

- 10-1 生徒指導のためのアンケート調査
- 10-2 生徒のインターネット被害状況の把握
- 10-3 常時接続環境によるインターネット利用への注意喚起
- 10-4 情報教育の依頼
- 10-5 情報モラル指導 1
- 10-6 情報モラル指導 2
- 10-7 情報モラル指導 3
- 10-8 情報モラル指導 4
- 10-9 インターネットの安全利用指導 1
- 10-10 インターネットの安全利用指導 2
- 10-11 インターネットを利用した犯罪に巻き込まれないための指導 1
- 10-12 インターネットを利用した犯罪に巻き込まれないための指導 2
- 10-13 インターネット安全利用の特別授業 1
- 10-14 インターネット安全利用の特別授業 2
- 10-15 インターネット安全利用の特別授業 3
- 10-16 インターネット安全利用の特別授業 4
- 10-17 インターネット安全利用の特別授業 5
- 10-18 インターネット安全利用の特別授業 6
- 10-19 教員向けセキュリティ講習会の開催 1
- 10-20 教員向けセキュリティ講習会の開催 2
- 10-21 教員向けセキュリティ講習会の開催 3
- 10-22 教員向けコンピュータウイルス対策の講習会の開催
- 10-23 保護者・生徒向けインターネット教室の開催
- 10-24 保護者向けセキュリティ教室の開催

I. 被害・事故事例編

なりすましによる個人情報の聞き出し

中学校での事例

◆被害状況

- ・生徒宅に、PTA を装って他の生徒の電話番号を聞きだそうとする電話があった。不審に思った生徒は他の生徒の電話番号を教えなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のセキュリティ対策―

- ・連絡網はクラス全員の連絡先を記載せず、必要最低限の連絡先を記載している。

◆発見の経緯

- ・発見方法：生徒からの申し出により判明した。
- ・発生日時：平成 16 年
- ・発見日：生徒の家に電話がかかってきた翌日
- ・事実確認：

◆被害への対応

―教職員の対応―

- ・対応日：生徒から申し出があった当日
- ・対応担当者：全教員
- ・対応方法：
職員会議で事実を周知し、生徒に PTA を装って電話があった場合には学校に連絡するように指導するよう確認を行った。

―生徒への対応―

- ・対応日：職員会議で確認をした翌日
- ・対応担当者：担任教員
- ・対応方法：
他の生徒の電話番号を聞きだすような電話がかかってきた場合には、自分の判断で答えるのではなく、「学校に問合せをしてください」と返答するように指導した。

◆今後の対策と効果

- ・現状、クラスの緊急連絡網は作成しているが、クラス全員の電話番号は記載していない。しかし、緊急時に連絡網がうまく機能しなかった事例も発生していて、現在も連絡網のあり方を検討している。

生徒の携帯電話の紛失による情報の漏えい

高等学校での事例

◆被害状況

- ・女子生徒が通学途中の電車内で携帯電話を紛失した。携帯電話には同級生の携帯電話番号が数多く登録されていた。
- ・携帯電話を取得したと思われる人物から、紛失した携帯電話に登録してあった複数の同級生の携帯電話に、頻繁に卑猥な電話がかかってくるようになった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：卑猥な電話がかかってくるようになった生徒からの相談により判明した。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：生活指導担当教員
- ・対応方法：

携帯電話の着信拒否機能を活用することをアドバイスした。

学校の規則として、携帯電話の持込みを禁止しているので、学校に通学するときは携帯電話を自宅に置いてくるように指導した。

◆今後の対策と効果

- ・学校への携帯電話の持込みを禁止している。学校にいる平日に緊急連絡がある場合は、生徒の携帯電話から保護者に連絡をするのではなく、必ず学校から保護者と連絡をいれるようにしており、保護者にも事前に説明を行い、携帯電話の持込み禁止に理解を求めている。

ずさんなデータ管理 1

高等学校での事例

◆被害状況

- ・個人情報漏えい等の事故防止の観点から教員が個別にデータをもたないことにするために生徒の成績データを管理するパソコンを1台に限定した。
- ・ところが、成績データの入力は定期試験後の一時期に集中し成績処理に支障がでてしまうため、教員が各自のパソコンで成績データを作成し、フロッピーディスクを用いて管理用パソコンにコピーする運用となったうえに、なかにはコピーに使用した成績データを消去せず、フロッピーディスクを無造作に机の上に放置し、誤って生徒へフロッピーディスクを貸し出してしまいうケースまで起こっている。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：一般利用校内パソコンに成績ファイルが存在していた。
- ・発生日時：平成16年10月
- ・発見日：成績処理日の後
- ・事実確認：

◆被害への対応

- ・成績データらしきファイルは、発見した時点でお互いに消去してしまうことにした。

◆今後の対策と効果

- ・成績データの安全性とデータ入力の効率のバランスをあるところにとらなければならないが、今はあまりにも安全性がないがしろにされている。現実にも可能な運用範囲で安全性を確保しなければならないが、これといった対策を打ち出せないままである。

ずさんなデータ管理 2

高等学校での事例

◆被害状況

- ・情報漏えい防止のために、職員室内のパソコンのハードディスクに生徒の成績データや定期試験の問題などの情報をハードディスクに残さずにメディアに保存するというルールを定めている。
- ・教員にはルールを遵守するように注意しているが、ハードディスクにデータが残っていることがある。なかには、作成中のテスト問題を画面に表示させたまま、席を離れてしまう教員もいる。
- ・幸い、席を離れている隙に生徒がパソコンを見て試験問題が漏えいするという事故は起こっていないが、情報が流出してもおかしくない現状である。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・情報漏えい防止のために、職員室内のパソコンのハードディスクに生徒の成績データや定期試験の問題などの情報をハードディスクに残さずにメディアに保存するというルールを定めている。
- ・生徒の成績データや定期試験の問題などを保存しているメディアは、施錠できる戸棚で保管している。鍵の管理は教頭が行っている。

◆発見の経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

—教員への対応—

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：
情報漏えいを起こさないようにするために、職員会議等を通じて全教員にルールを守るように注意している。

◆今後の対策と効果

- ・注意を行っているにもかかわらず情報漏えいについて認識が甘い教員もおり、特に着任間もない教員や非常勤講師の意識向上が今後の課題である。

電子メールアドレスの不用意な公開

高等学校での事例

◆被害状況

- ・生徒が携帯電話の電子メールアドレスを教室の黒板に大きく書き記していた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒の行動を教員が目撃。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：
- ・対応担当者：
- ・対応方法：

生徒は、メール欲しさゆえの行動であったわけだが、電子メールも個人を特定できる個人情報であり、様々な不要なメールも（宣伝、ウイルス、架空請求など）送られて不愉快な思いをしたり、だまされて事件に巻き込まれたりすることがあると伝えただけで、たとえ級友で場所が校内（教室）といえども公開は好ましくないことを指導した。

◆今後の対策と効果

- ・一部の生徒には、携帯電話の電子メールアドレスや携帯番号は、すでに使い捨てと思っている節があり、簡単に携帯電話やメールアドレスを変更しているようである。このケースも不要メールなどがくるようになったらまたメールアドレスを変更すると言っていたが、事故・事件を未然に防ぐという観点から個人のメールアドレスの公開については慎重に行うことを引き続き指導している。

ファイル交換ソフトを介した部活動 OB 会名簿の流出

高等学校での事例

◆被害状況

- ・部活動 OB 会が管理している OB 会名簿が、ファイル交換ソフトを介してインターネット上に流出していた。
- ・OB 会名簿には数十件の氏名、住所、電話番号が記載されていたが、在校生の情報は記載されていなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：情報発見者から学校の代表電子メールアドレスにメールが届き判明した。
- ・発生日時：平成 18 年 4 月
- ・発見日：平成 18 年 4 月
- ・事実確認：

◆被害への対応

一部活動 OB 会への対応ー

- ・対応日：メールが届いてから 2～3 日後
- ・対応担当者：部活動の顧問教員
- ・対応方法：

部活動 OB 会は任意の団体であり、OB 会の運営について学校側が管理すべきものではないとの認識ではあるが、学校の代表電子メールアドレスに情報流出の連絡メールが届いていたので、該当の部活動の OB 会にインターネット上に OB 会名簿が流出している事実を伝えた。

流出してしまった名簿の情報をすべて回収することは困難なことであり、今後同様の事故が発生しないことが大切なので、適切な情報管理を行うように部活動 OB 会にお願いをした。

◆今後の対策と効果

- ・任意の団体である部活動 OB 会を学校側が管理することはできないが、各部活動の OB 会に対して、適切な管理を実施するようにお願いをしていくこととした。

女子生徒を狙った盗撮

高等学校での事例

◆被害状況

- ・校門を出たところから女子生徒の背後をつけ、デジタルカメラで撮影を続ける者が現われた。生徒は怖くなり、学校に逃げ帰ってきた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：事件発生日
- ・対応担当者：担当教員
- ・対応方法：

学校に逃げ帰ったことで、犯人はいなくなったが、デジタル画像についてはその後どのように扱われたかは不明である。

今後、下校時にこうしたケースに遭遇した場合には、学校へ戻るなど人のいるところへ逃げ込むように指導した。

◆今後の対策と効果

- ・フォーラム事務局より個人を特定できる画像をWebなどで発見した場合には、神奈川県警ハイテク犯罪センターが相談窓口としてあることも伝えた。
- ・また、撮影については、すぐに警察に連絡すれば逮捕が可能であることも伝えた。

携帯電話のカメラ機能を利用した盗撮

高等学校での事例

◆被害状況

- ・校内で男子生徒が女子生徒のスカートの中を盗撮した。盗撮されたことに気づいた生徒がすぐに教員に相談したのですぐに削除することができた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：盗撮された生徒の友人の申し出により判明した。
- ・発生日時：平成 16 年
- ・発見日：
- ・事実確認：盗撮した生徒の携帯電話で事実を確認した。

◆被害への対応

－盗撮した生徒への対応－

- ・対応日：申し出があったその日
- ・対応担当者：担任教員・生活指導担当教員
- ・対応方法：
生徒に個別指導を実施し、盗撮した写真を削除させ、教員が削除されたか否かの確認を行った。

◆今後の対策と効果

就職活動情報漏えい

専門学校での事例

◆被害状況

- ・ 学生が就職活動をする際の参考例として活動をする他の学生の就職活動報告書を Web より参照できるようになっていたが、就職活動報告書 DB が Web サイトと同じディレクトリに置いていたため、DB の URL を入力することで外部より取得することができてしまっていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：学生からの指摘。
- ・ 発生日時：
- ・ 発見日：
- ・ 事実確認：

◆被害への対応

－就職活動報告書 DB への対応－

- ・ 対応日：被害発生日
- ・ 対応担当者：担当教員
- ・ 対応方法：DB を外部より参照できないディレクトリに移動した。

◆今後の対策と効果

予期しない他人のメールアドレスの取得

高等学校での事例

◆被害状況

- ・女子生徒が自宅でインターネットオークションを利用して、出品者からパソコンを落札した。数日後に落札したパソコンが自宅に届き自分の電子メールの設定を行い、送受信を試したところ、出品者のメールアドレス情報が残っており、出品者宛のメールを受信してしまった。
- ・女子生徒は、パソコンに残っていたメールアドレスをどのように扱ってよいかわからず、情報担当教員に相談をしてきた。
- ・女子生徒にある程度知識があったため、他人のメールアドレスの存在と受信に気がついたが、場合によっては気がつかないまま迷惑メール程度の感覚で受信を続けてしまう可能性もあった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：女子生徒からの相談により判明した。
- ・発生日時：平成 17 年 10 月
- ・発見日：平成 17 年 10 月
- ・事実確認：

◆被害への対応

－相談をしてきた生徒への対応－

- ・対応日：相談のあったその日
- ・対応担当者：情報担当教員
- ・対応方法：

パソコンに設定されていたメールアドレスを利用してメールを送受信すると生徒自身が不正アクセス禁止法に違反する可能性があったので、パソコンに設定されている出品者のメールアドレスは使用せずに直ちに削除するようにアドバイスをを行い、メールアドレスの削除方法を指導した。

◆今後の対策と効果

ユーザ ID とパスワードの不正利用によるいたずらメールの送信

高等学校での事例

◆被害状況

- ・生徒が、同級生のユーザ ID とパスワードを無断で利用して、その同級生の電子メールアカウントで友人にいたずらメールを送信していた。
- ・電子メールは学校外へも送信することが可能だが、学校外へいたずらメールを送信した形跡はなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・全生徒にユーザ ID とパスワードを付与し、パソコンのアクセス管理、生徒個人のデータを保存する環境、電子メール環境を校内のどのパソコンからでも利用できるようにしている。

◆発見の経緯

- ・発見方法：メールを不正に送られた生徒からの相談により判明した。
- ・発生日時：平成 17 年 9 月
- ・発見日：
- ・事実確認：

◆被害への対応

ーいたずらメールを送信した生徒への対応ー

- ・対応日：
- ・対応担当者：情報担当教員、契約している校内のネットワーク管理者
- ・対応方法：

校内のネットワーク管理者にログ調査を依頼し、ユーザ ID とパスワードが無断で利用されていた時間帯、パソコンを特定した。その時間帯に当該パソコンを利用していたクラスを確認し、不正にユーザ ID とパスワードを利用した生徒を特定した。

特定した生徒を呼び出し本人に事実の確認を行ったところ、同級生のユーザ ID とパスワードを無断で利用したことを認めた。また、パスワードを入手した経緯を確認したところ、ユーザ ID とパスワードを不正利用された生徒自らがパソコンの起動を依頼するために自分のユーザ ID とパスワードを教えていたことが判明した。

他人のユーザ ID とパスワードを無断で利用する行為は不正アクセス禁止法に抵触する行為で絶対にやってはならないことと指導し、自宅謹慎を含む厳しい処罰を行った。

全生徒に対して、今回の経緯の説明とユーザ ID とパスワードを各自でしっかり管理するように文書で注意を行った。

◆今後の対策と効果

パスワード解析ソフトを利用した不正なアクセス

高等学校での事例

◆被害状況

- ・生徒が、同級生のユーザ ID とパスワードを無断で利用して、その同級生の電子メールアカウントで友人にいたずらメールを送信していた。
- ・その生徒は、パスワード解析ツールを利用して、同級生のパスワードを推測し、不正にログインしていたずらメールを送信していた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・全生徒にユーザ ID とパスワードを付与し、パソコンのアクセス管理、生徒個人のデータを保存する環境、電子メール環境を校内のどのパソコンからでも利用できるようにしている。
- ・ユーザ ID は生徒が記憶しやすいように学籍番号を利用している。また、パスワードはシステムの制限もあり、5桁の数字を利用している。

◆発見の経緯

- ・発見方法：同時期にユーザ ID とパスワードの無断利用によるいたずらメールを送られた事件が発生しており、同様のケースがないか確認を行っている際に判明した。
- ・発生日時：平成 17 年 9 月
- ・発見日：
- ・事実確認：

◆被害への対応

ー生徒への対応ー

- ・対応日：
- ・対応担当者：情報担当教員、契約している校内のネットワーク管理者
- ・対応方法：

校内のネットワーク管理者にログ調査を依頼し、パソコンを利用した時間を特定した。また、その時間にパソコンを利用していたクラスと生徒を洗い出し、不正アクセスを行った生徒を特定した。

本人に確認を行ったところ、ユーザ ID とパスワードを不正に利用したことを認めた。

他人のユーザ ID とパスワードを無断で利用する行為は不正アクセス禁止法に抵触する行為で絶対にやってはならないことと指導し、自宅謹慎を含む厳しい処罰を行った。

ーシステムへの対応ー

- ・対応日：
 - ・対応担当者：情報担当教員
 - ・対応方法：
- パスワードの入力を 5 回間違えると、30 分間はログインできないようにシステムを変更した。

◆今後の対策と効果

- ・生徒用パスワードはシステムの制限により、5桁の数字のみしかパスワードとして利用できない。生徒用パスワードを英数字を利用して作成したいが、システムの制限によりすぐに変更できないので、学校のシステムを更新する際の検討事項となっている。

パスワードの漏えいによる試験問題流出

専門学校での事例

◆被害状況

- ・授業の理解度を確認するための試験問題が流出した。
- ・パスワードを週1回変えていたが、管理するパスワードが多く覚えきれないために机の引き出しにパスワードを書いた紙を入れておいたところ、学生がそのことに気づきネットワークを介してテスト問題を持ち出したことが判明した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

ー学生への対応ー

- ・対応日：
- ・対応担当者：担当教員
- ・対応方法：
試験については、評価するための試験ではなく、学生の理解度確認の試験であったため、再試験といった措置はとらないこととし、授業時間において理解度の確認を過去に遡って、あらためて行っていくこととした。

ーパスワード管理への対応ー

- ・対応日：
- ・対応担当者：担当教員
- ・対応方法：
パスワードを紙に記載すること事体に問題があるが、管理するパスワードが多く変更が必要なため、記憶にとどめることにも限界となっている。
このため、パスワードの記憶違いなどで過去に権利者からパスワード無効、再設定などを何度か行ってもらった経緯もあり今回の事件に発展した。
当面の解決策として、パスワードを記載するがそれを複数の紙に分けて別の場所に保管することとし、かつ施錠できる引き出しに管理することとした。

◆今後の対策と効果

- ・パスワードの管理については、依然として課題が残されている。

ユーザ ID とパスワードの借用 1

高等学校での事例

◆被害状況

- ・数名の生徒が、放課後に担任教員立会いの下、パソコン教室を利用していた。その際に、ある生徒が、自分が利用すべきユーザ ID とパスワードを忘れておりパソコンが利用できない状況になると、その場にいた友人のユーザ ID とパスワードを借りてパソコンを利用していた。
- ・立会っていた教員は、生徒同士でのユーザ ID とパスワードの貸し借りの行為を注意することなく黙認していた。
- ・生徒同士でのユーザ ID とパスワードの貸し借り行為後に、生徒が他の生徒のユーザ ID とパスワードを記憶して無断に使用したということはない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境

- ・パソコンの利用には、ユーザ ID とパスワードが必要となる。
- ・全生徒にユーザ ID とパスワードを付与している。

ー校内のパソコン利用状況や利用形態ー

- ・パソコン教室は教員の立会いの下であれば、休み時間や放課後に利用できる。

◆発見の経緯

- ・発見方法：情報担当教員がパソコン教室に居合わせたために発見できた。
- ・発生日時：平成 17 年
- ・発見日：平成 17 年
- ・事実確認：

◆被害への対応

ー生徒への対応ー

- ・対応日：
- ・対応担当者：情報担任教員
- ・対応方法：

たとえ友人がユーザ ID とパスワードを利用することを許可したとしても、大切な個人情報なので貸し借り行為を行わないよう指導を行った。あわせて、他人のユーザ ID とパスワードを無断で利用すると不正アクセス禁止法に違反し犯罪行為となることを伝えた。パスワードを貸し出した生徒にはパスワードを変更するように指導を行った。

◆今後の対策と効果

- ・今回の件は、たまたま情報担当教員が在室しているときに発見したので生徒に指導することができたが、立会っていた教員がユーザ ID とパスワードの貸し借りを黙認していたことは教員の認識不足であり、またユーザ ID やパスワードの大切さを生徒に教えなければならない立場の教員がユーザ ID とパスワードを安易に考えていることが問題である。今後は教員の意識を高め、すべての教員が指導できるようにすることが必要と認識している。

ユーザ ID とパスワードの借用 2

高等学校での事例

◆被害状況

- ・生徒がパソコン教室のパソコンを利用する際に、生徒同士でユーザ ID とパスワードの貸し借りを行って利用していた。また、教員自ら教員用のユーザ ID とパスワードを貸し出し、生徒に利用させていたこともあった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境

- ・全生徒にユーザ ID とパスワードを付与している

ー校内のパソコン利用状況や利用形態ー

- ・生徒は教員立会のもと放課後にパソコン教室を利用することができる。

◆発見の経緯

- ・発見方法：情報担当教員が教室内で作業している際に発見した。
- ・発生日時：平成 17 年
- ・発見日：平成 17 年
- ・事実確認：

◆被害への対応

ーID とパスワードを貸し出した教員への対応ー

- ・対応日：発見したその日
- ・対応担当者：情報担当教員
- ・対応方法：

生徒に正しい利用方法を伝える立場である教員が、パスワードを忘れてしまった生徒に対して、他の生徒のユーザ ID とパスワードの貸し借りを黙認したり、教員のユーザ ID とパスワードを貸し出してしまったりすることはあってはならないことなので厳しく注意した。

ーシステムの対応ー

- ・対応担当者：情報担当教員
- ・対応方法：

生徒のユーザ ID とパスワードの管理は、情報担当教員が行っており、セキュリティを確保するため他の教員は行うことができない。したがって、情報の授業では、生徒がパスワードを忘れてしまった場合に情報担当教員がすぐにパスワードを再発行できるが、放課後に他の教科の教員が立会ってパソコン教室を利用している際には情報担当教員を探してからパスワードの再発行を行うので時間がかかってしまう。そのため、ユーザ ID とパスワードを必要としないパソコンを図書室に数台設置し、パソコン教室を利用しなくてもパソコンを利用できるように対応した。

◆今後の対策と効果

- ・今回の件以外にも教員がユーザ ID とパスワードの貸し借りを黙認するケースが考えられるので、教員のセキュリティ意識向上をしていく必要がある。

ユーザ ID とパスワードの借用 3

高等学校での事例

◆被害状況

- ・生徒間でのユーザ ID とパスワードの貸し借りが行われている。
- ・情報の授業ではユーザ ID とパスワードの貸し借りは行われていないが、他の授業において生徒に指導する立場である教員が、パスワードを忘れてしまった生徒に他の生徒のユーザ ID とパスワードを貸し借りするように促していたこともあった。
- ・過去には、ユーザ ID とパスワードを借りた生徒が、貸した生徒が作成していたデータを誤って削除してしまったことも発生している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・パソコン教室のパソコンを利用する生徒に個々の利用環境を提供するために、全生徒にユーザ ID とパスワードを付与している。

◆発見の経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：
授業でパソコンを利用するためであっても絶対にユーザ ID とパスワードを貸し借りしないように情報の授業で指導している。

—教員への対応—

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：
職員会議等を利用して、生徒同士でユーザ ID とパスワードの貸し借りを行わないように指導するようお願いしている。
ユーザ ID とパスワードについて認識の甘い教員もいるので、教員対象の研修会を実施したいが、通常の授業や行事などがあり現状ではなかなか研修会を実施することができず、よい対応方法を検討している。

◆今後の対策と効果

- ・ユーザ ID とパスワードの貸し借りを防ぐ有効な手立てを現在も検討中である。

教員によるコンピュータウイルス感染 1

小学校での事例

◆被害状況

- ・ウイルス対策ソフトを導入している職員室のパソコンすべてがコンピュータウイルスに感染した。
- ・ネットワークを経由して外部に感染は拡大していないが、教員の自宅パソコンにウイルスが二次感染した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・職員室のパソコンは LAN 環境が整備されており、インターネットの利用も可能である。

ー校内のパソコン利用状況や利用形態ー

- ・教職員はパソコンを自由に利用できる。

ー校内のセキュリティ対策ー

- ・ウイルス対策ソフトを導入している。

◆発見の経緯

- ・発見方法：パソコンの動作が不安定だったため、導入しているウイルス対策ソフトでウイルススキャンを実施して判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

ー教職員への対応ー

- ・対応日：
- ・対応担当者：パソコン管理担当教員
- ・対応方法：

ウイルスに感染したすべてのパソコンのウイルスを駆除するため、OS から再インストールを実施した。

ウイルス対策ソフトを導入していたにもかかわらずウイルス感染したのは、リアルタイムでウイルスから保護する設定にしていなかったためで、すぐに設定を変更した。

教員の自宅パソコンに感染が拡大していたので、念のため、自宅にあるパソコンと学校で利用するすべてのフロッピーディスクや MO などのメディアをウイルススキャンするように注意した。

◆今後の対策と効果

- ・対策を実施して以降、ウイルス感染の報告はない。

教員によるコンピュータウイルス感染2

中学校での事例

◆被害状況

- ・職員室のネットワーク化に伴い、ウイルス対策ソフトを導入し、今まで利用していたメディアのウイルススキャンを実施したところ、ほとんどのメディアがウイルスに感染していた。
- ・外部へのデータの漏えい、外部への2次感染などの被害は起こっていない。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・職員室のパソコンもネットワーク化し、インターネット等の閲覧が可能になった。

―校内のパソコン利用状況や利用形態―

- ・教員は、職員室内のパソコンを自由に利用することができる。

―校内のセキュリティ対策―

- ・ネットワーク化に伴い、すべてのパソコンにウイルス対策ソフトを導入した。

◆発見の経緯

- ・発見方法：メディアをウイルス対策ソフトでウイルススキャンしたときに判明した。
- ・発生日時：平成16年4月頃
- ・発見日：平成16年4月頃
- ・事実確認：平成16年4月頃

◆被害への対応

―教員への対応―

- ・対応日：事実確認日の次の日
- ・対応担当者：パソコン担当教員
- ・対応方法：
 - 教員には、メディア（フロッピーディスク・USBメモリ）を利用する際には必ずウイルススキャンを行ってから利用するようにお願いした。

―ウイルスへの対応―

- ・対応日：事実確認日
- ・対応担当者：パソコン担当教員
- ・対応方法：
 - ウイルス対策ソフトを利用し、メディアから発見されたウイルスはすべて駆除を実施した。その後、ハードウェアのスキャンを行ったところ、ハードウェアへの感染は確認されなかった。

◆今後の対策と効果

- ・ウイルス対策ソフトは、常駐する設定にし、ウイルス定義ファイルの自動更新する設定にした。
- ・職員室のパソコンを利用する際のルールを全教員に徹底するため、定期的な研修等を行うこととし、啓発活動を継続して行うこととした。

教員によるコンピュータウイルス感染3

中学校での事例

◆被害状況

- ・教員が自宅で作成したデータを学校のパソコンで利用しようとしたところ、自宅から持ってきたファイルがウイルスに感染していた。
- ・ウイルス対策ソフトを導入してあったためパソコンへの感染は防げた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・職員室内のパソコンは、インターネット閲覧用パソコンと教材作成用パソコンがあり、教材作成用パソコンからはインターネットの閲覧ができない。

―校内のパソコン利用状況や利用形態―

- ・職員は、職員室内に設定しているパソコンを自由に利用できる。

―校内のセキュリティ対策―

- ・ウイルス対策ソフトを導入している。

◆発見の経緯

- ・発見方法：教員からの申し出により判明した。
- ・発生日時：平成16年7月
- ・発見日：平成16年7月
- ・事実確認：

◆被害への対応

―教員への対応―

- ・対応日：事実確認日
- ・対応担当者：情報化委員会メンバー
- ・対応方法：
ウイルス対策ソフトの警告画面が出てきたら、警告画面にしたがってウイルスを駆除するよう指導した。
自宅パソコンにウイルス対策ソフトの導入を勧めた。

◆今後の対策と効果

- ・人事異動が落ちついた4月下旬に、前任校や自宅から持参してきたデータのウイルススキャンを行うルールを定め、実施することとする。

教員によるコンピュータウイルス感染4

中学校での事例

◆被害状況

- ・教員が利用するパソコンがコンピュータウイルスに感染した。インターネットに接続しておらず、また生徒用 LAN とも物理的に分割していたため、ネットワークを経由しての二次感染は防げた。
- ・ウイルス感染によるデータの削除・情報漏えいは確認されていない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・職員室内は LAN 環境が整備されているが、教員用パソコンからインターネットへ接続できない。

ー校内のセキュリティ対策ー

- ・職員室内の教員用パソコンはインターネットへ未接続のため、ウイルス対策ソフトを導入していない。

◆発見の経緯

- ・発見方法：パソコンの利用中に強制的に電源が切れてしまったため判明した。
- ・発生日時：平成 16 年 10 月
- ・発見日：平成 16 年 10 月
- ・事実確認：

◆被害への対応

ーウイルスへの対応ー

- ・対応日：ウイルス感染が判明してから 3 日後
- ・対応担当者：情報担当教員
- ・対応方法：
インターネットへ未接続のパソコンでウイルス感染が発生したので、教員が持込んだフロッピーディスクがウイルス感染源と特定できた。
教育委員会にウイルス感染の事実を報告し、契約している保守業者の担当者を学校へ派遣してもらい、ウイルスの駆除を実施した。
インターネットへ未接続のパソコンではあるが、より万全を期すためにウイルス対策ソフトを導入することにした。

◆今後の対策と効果

- ・その後、ウイルス感染の報告はない。

教員によるコンピュータウイルス感染5

高等学校での事例

◆被害状況

- ・教員が職員室パソコンを利用していた際に、ウイルス対策ソフトがコンピュータウイルスを検知し、ウイルス感染が判明した。
- ・感染したパソコンからの二次感染や情報流出などは発生していない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境

- ・全教員にユーザ ID とパスワードを付与している。

―校内のセキュリティ対策―

- ・ウイルス対策ソフトを導入している。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

―感染したパソコンへの対応―

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

アクティブディレクトリを活用し、各教員のデータは環境はネットワーク上の個人フォルダに保管しているため、ウイルス対策ソフトがウイルスを検出した場所を確認して、ウイルス感染をした際にコンピュータを利用していた教員が判明した。

ウイルス感染していた場所がインターネット一時ファイルを保管するフォルダだったため、Web 閲覧時にウイルス感染したものと判断できた。

ウイルス対策ソフトを利用してウイルスを駆除したので、他のマシンに感染することはなかった。

ウイルス感染を引き起こしてしまった教員には、念のため個別に利用しているメディアのウイルスチェックをするように注意を行った。

◆今後の対策と効果

- ・ウイルス対策ソフトは導入済みではあるが、セキュリティパッチは頻繁にあてていない。作業を行う教員が不足していることや自動化のための仕組みを導入するにはコストがかかることなどが理由ではあるが、すべてのパソコンに効率的にセキュリティパッチをあてることが課題である。

教員によるコンピュータウイルス感染6

高等学校での事例

◆被害状況

- ・教員が職員室内のパソコンでコンピュータウイルスに感染した電子メールを開こうとしたところ、利用しているパソコンが停止し、利用できない状態になった。
- ・参加している教育委員会ネットワークのウイルス対策ソフトが作動し、ウイルス感染メールの配信を停止させた。
- ・ウイルス感染メールは配信されなかったため、学校内のパソコンへのウイルス感染は防ぐことができた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・教育委員会が管理・運営しているネットワークに参加している。

―校内のパソコンの利用状況や利用形態―

- ・職員は職員室内のパソコンを利用してインターネットを利用できる。

―校内のセキュリティ対策―

- ・ウイルス対策ソフト導入している。

◆発見の経緯

- ・発見方法：教育委員会からの連絡により判明した。
- ・発生日時：平成17年2月
- ・発見日：平成17年2月
- ・事実確認：

◆被害への対応

―ウイルスへの対応―

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：
参加している教育委員会ネットワークで、ウイルスに感染したメールを開こうとした時点で、クライアントパソコンへの配信を停止させたため、ウイルス感染は防げた。
教育委員会からの連絡を情報担当教員が受け、操作をしていた教員に確認を行った。

◆今後の対策と効果

- ・教育委員会ネットワークへの移行時期であり、ウイルスなどのトラブル発生を心配していたが、ネットワークを経由するウイルスを未然に防ぐことが確認できた。システムの面は整いつつあるが、今回のケースでもわかるように、教員の意識レベルを高めていくことが課題である。

生徒によるコンピュータウイルス感染1

中学校での事例

◆被害状況

- ・パソコン部に所属する生徒が持参したフロッピーディスクがコンピュータウイルスに感染しており、部活動時に利用していたパソコンがウイルスに感染した。
- ・部活動時の出来事だったため、利用しているパソコンが少なく、他のパソコンへの感染は防ぐことができた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・教育委員会が管理・運営しているネットワークに参加している。

―校内のパソコン利用状況や利用形態―

- ・一般生徒の利用は授業時のみとしている。
- ・パソコン部の生徒は、部活動時にパソコンを利用することができる。

◆発見の経緯

- ・発見方法：教育委員会より学校に連絡が入り判明した。
- ・発生日時：平成16年
- ・発見日：教育委員会から連絡を受けた当日
- ・事実確認：教育委員会の連絡を受け、パソコン部の生徒から直接事実確認をとった。

◆被害への対応

―生徒への対応―

- ・対応日：教育委員会から連絡を受けた当日
- ・対応担当者：パソコン部顧問
- ・対応方法：
教育委員会から連絡を受けたパソコン部の顧問が、生徒に直接話を聞き、事実の確認を行った。
ウイルス対策ソフトは導入されていたが常駐する設定になっていなかったため、持参したフロッピーディスクを利用した際に学校のパソコンにウイルスが感染した。
ウイルス対策ソフトを常駐する設定に変更するとともに、生徒に対しては持参したフロッピーディスク等のメディアを利用する際は、必ずウイルススキャンを実施してから利用するよう指導した。あわせて、自宅のパソコンにウイルス対策ソフトを導入するよう助言を行った。

◆今後の対策と効果

- ・その後、フロッピーディスクやUSBメモリ等の持込みメディアによるウイルス感染は発生していない。

生徒によるコンピュータウイルス感染2

高等学校での事例

◆被害状況

- ・コンテスト主催者より生徒が提出した作品がウイルスに感染していると連絡があった。
- ・コンテスト出品作品は授業で利用するパソコンでなかったため、他の生徒への感染は防ぐことができた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・パソコンのみのスタンドアロン環境で利用しており、授業で利用するパソコン教室とは別の部屋で利用している。

ー校内のパソコン利用状況や利用形態ー

- ・一般の生徒は利用できず、クラブ活動のメンバーのみが利用できる。

◆発見の経緯

- ・発見方法：コンテスト主催者からの連絡により判明した。
- ・発生日時：平成16年10月
- ・発見日：平成16年10月
- ・事実確認：平成16年10月

◆被害への対応

ー生徒への対応ー

- ・対応日：事実確認日
- ・対応担当者：クラブ活動顧問
- ・対応方法：

生徒にウイルスに感染していた事実を伝え、原因究明を一緒に行った。

利用していたパソコンはスタンドアロン環境で、インターネットの利用もできなかったため、作品作成をどこで実施したか生徒全員に聞き、学校以外で作成している生徒が見つかった。

該当生徒の家のパソコンでウイルスに感染したことが判明し、自宅のパソコンにウイルス対策ソフトを導入することを勧めた。

ー学校のパソコンへの対応ー

- ・対応日：事実確認日
- ・対応担当者：クラブ活動顧問
- ・対応方法：

スタンドアロンで利用するパソコンでウイルス対策ソフトは導入していなかったため、パソコンの初期化を行いOSの再インストールを行ってウイルスの駆除を行った。

◆今後の対策と効果

- ・スタンドアロン環境のマシンにもウイルス対策ソフトを導入してウイルススキャンを行える環境にする。

生徒によるコンピュータウイルス感染 3

高等学校での事例

◆被害状況

- ・生徒が利用するパソコン教室のパソコン 2 台がコンピュータウイルスに感染した。
- ・幸いなことに感染したパソコン以外への感染の拡大はなく、授業が実施できなくなるような事態にはならなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

－校内のパソコン環境－

- ・校内 LAN が導入されている。

－校内のセキュリティ対策－

- ・パソコン教室のパソコンにはウイルス対策ソフトと環境復元ソフトを導入している。

◆発見の経緯

- ・発見方法：ウイルス対策ソフトがウイルスを検知したことにより判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

－ウイルスへの対応－

- ・対応日：ウイルスを検知したその日
- ・対応担当者：情報担当教員
- ・対応方法：

ウイルス対策ソフトを利用して、ウイルスを駆除した。

ウイルス感染の経路は、ウイルス感染していたファイルがインターネット一時ファイルに保存されているファイルだったため、生徒が Web サイトを閲覧している際に Web ページから感染したものと判明した。また、ウイルス感染の原因は、ブラウザのセキュリティパッチをあてていなかったためであった。

◆今後の対策と効果

- ・現在、OS やソフトウェアのセキュリティパッチ実施が不完全である。情報担当教員のみで約 50 台のパソコンをメンテナンスすることが難しく、またすぐに自動化の仕組みを導入することもできないので、夏休みなどの長期休業期間を利用して、できる限りメンテナンスすることとしたが、対応としては不十分な現状である。

生徒によるコンピュータウイルス感染4

高等学校での事例

◆被害状況

- ・生徒が自宅で利用しているノートパソコンがコンピュータウイルスに感染し、どのように対処すればよいか情報担当教員へ相談してきた。
- ・情報の授業では、ウイルス対策として、ウイルス対策ソフトの導入や定義ファイルの更新について指導を行うが、感染した場合の対処法などは時間的な制約もあり指導はしていない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談により判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：相談があった 2～3 日後
- ・対応担当者：情報担当教員
- ・対応方法：
感染した生徒のパソコンがノートパソコンだったので、学校にパソコンを持参させ、放課後に生徒と一緒にウイルスの駆除や OS の再インストール作業を行った。

◆今後の対策と効果

- ・時間的な制約もあり、ウイルス駆除や OS の再インストール作業などを学校の授業で実施することは難しい。現状では、生徒から相談に対し個別で対応する方法しかない。

スパイウェア被害 1

高等学校での事例

◆被害状況

- ・教員が授業で利用するためにインターネットからフリーソフトをダウンロードしインストールしたところ、パソコン教室の教員用パソコンにスパイウェアがインストールされてしまった。その影響で、Web サイト閲覧時に一定の間隔で広告ウインドウが表示されるようになってしまった。
- ・保守契約業者にスパイウェアを駆除ソフトで駆除してもらったが、後日、再度広告ウインドウが表示される現象が再発した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・パソコン教室の教師用、生徒用パソコンのシステムドライブは環境復元ソフトが入っている。

―校内のセキュリティ対策―

- ・校内のパソコンすべてに、ウイルス対策ソフトを導入している。

◆発見の経緯

- ・発見方法：Web サイトを閲覧中に頻繁に広告ウインドウが表示されたので判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：平成 16 年

◆被害への対応

―スパイウェアへの対応―

- ・対応日：平成 16 年
- ・対応担当者：パソコン管理担当教員
- ・対応方法：

ウイルス対策ソフトは導入していたが、そのソフトではスパイウェアの検出はできなかった。保守契約をしている業者に連絡し、スパイウェアを駆除した。

スパイウェアがインストールされてしまった原因は、教員がインターネット上からダウンロードしたフリーソフトをインストールしたためだった。

同じ事象が 2 回発生したため、インターネット上からのフリーソフトのダウンロードに一定の制限を設けるとともに、ダウンロードしたソフトを利用する際には、利用規約に情報収集活動を行う旨が記載されていることがあるので、利用規約を最後まで読み利用するよう職員会議で周知した。

◆今後の対策と効果

- ・その後、スパイウェアはインストールされていない。
- ・毎回業者を呼んでスパイウェアを駆除するのは手間がかかるし、業者の使用するフリーのスパイウェア駆除ソフトの効果も期待できないので、システムを再インストールするとともに今後はソフトのインストールには十分に配慮する必要がある。

スパイウェア被害 2

高等学校での事例

◆被害状況

- ・外国人教員が海外の Web サイトを閲覧中にスパイウェアが侵入した。Web サイトを閲覧中に広告サイトが頻繁に表示され、スパイウェアに侵入されていることを疑った。
- ・スパイウェアが侵入したパソコンは教員が利用するパソコンではあるが、授業で Web サイトを利用することがなかったため授業への妨げにはならなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のセキュリティ対策―

- ・ウイルス対策ソフトを導入している。

◆発見の経緯

- ・発見方法：Web サイトを閲覧中に広告ページが頻繁に表示されたので、スパイウェアの侵入を疑い、業者に対応してもらい判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

―スパイウェアへの対応―

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：
パソコンに導入しているウイルス対策ソフトでは、スパイウェアを検知することも駆除することもできなかったため、契約しているメンテナンス業者にスパイウェアを駆除してもらった。

◆今後の対策と効果

- ・現状では、スパイウェアを検知または駆除する対策ソフトをすぐに導入することができないので、学校のパソコンを利用して Web サイトを閲覧する際には十分注意を払うよう全教員に注意をした。

スパイウェア被害 3

高等学校での事例

◆被害状況

- ・生徒が自宅で利用しているデスクトップパソコンにスパイウェアが侵入した。
- ・スパイウェアが侵入したため、以前はまったく表示されなかったポップアップ広告（アダルト関係のポップアップ広告）が頻繁に表示されるようになった。
- ・Webサイトを閲覧するたびにポップアップ広告が頻繁に表示され、非常に気になって情報担当教員に相談してきた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談により判明した。
- ・発生日時：平成16年
- ・発見日：平成16年
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

生徒からの相談内容から、スパイウェアの侵入の可能性が高かったため、スパイウェアを駆除するフリーソフトを紹介した。また、最近のウイルス対策ソフトにはスパイウェアを検知・駆除するものがあることも伝えた。

より確実な駆除方法としては、OSの再インストールをすることを勧めた。

◆今後の対策と効果

チェーンメール1

中学校での事例

◆被害状況

- ・生徒が個人的に利用しているパソコンや携帯電話の電子メールに、公序良俗に反する画像が添付されたチェーンメールが流行している。
- ・チェーンメールの内容を真に受ける生徒もおり、真に受けた生徒は非常に不安な気持ちになっている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：チェーンメールを受け取った生徒からの相談により判明した。
- ・発生日時：
- ・発見日：平成16年4月
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：技術家庭の授業時
- ・対応担当者：技術・家庭教員
- ・対応方法：

情報機器を利用するうえで、チェーンメールを含む迷惑メールを受け取る可能性があることを伝え、迷惑メールは削除するように指導した。

迷惑メールの度合いにより、学校経由で警察等に相談することとしているので、教員に申し出るように指導した。

◆今後の対策と効果

- ・利用している情報機器に迷惑メール等が送信されてきた際には、送られてきたメールに対してどのように対応するかを生徒自身で判断できるようになることを指導の基本として、対応方法を身に付けられるよう通常の授業を実施していく。

チェーンメール2

中学校での事例

◆被害状況

- ・生徒同士が携帯電話のカメラ機能を利用していたずら目的で特定の生徒を撮影し、その画像を添付した電子メールを送信したところ、チェーンメールとなり学校中に広まってしまった。
- ・撮影されたうえに、同級生に送信された生徒は、精神的ショックを受けていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒との雑談中に不適切な画像を添付した電子メール送信の事実が判明した。
- ・発生日時：平成16年
- ・発見日：平成16年
- ・事実確認：メール送信をしていた生徒に事実関係を直接確認した。

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：担任教員・生活指導担当教員
- ・対応方法：
電子メールを送信していた生徒達に対して、相手の気持ちを考えて行動するように個別指導を実施した。
一度インターネット上に電子メールを送信してしまうと送信者の意に反して広まってしまふ可能性があり、完全に削除することは難しいので、電子メールを送信する際には、内容をよく確認してから送信するように指導を行った。

◆今後の対策と効果

- ・個別指導を実施した後に、同様の出来事は発生していない。
- ・携帯電話の持込みは禁止しているが、現状では学校への持込みを防ぐ手立てがない。今後も学校への持込みを制限する対策を検討するとともに、生徒に対してのモラル指導をしっかりと行っていく。

チェーンメール3

中学校での事例

◆被害状況

- ・生徒が利用している携帯電話の電子メールに、「メール内に記載された電話番号に電話をかけないと命に危険がおよぶ」と脅しの内容が記載されたチェーンメールが流行している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・学校内での携帯電話の利用は禁止している。登下校時に携帯電話を持たせる保護者もいるので、学校内で生徒同士が携帯電話を利用しないために、携帯電話を登校時に教員に預け、下校時に返却している。

◆発見の経緯

- ・発見方法：チェーンメールを受け取った生徒からの相談により判明した。
- ・発生日時：平成18年
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：相談を受けたその日
- ・対応担当者：担任教員
- ・対応方法：

相談してきた生徒にはその場で、メールの内容は事実無根であり、記載されている電話番号には連絡しないように指導した。

他の生徒も同様のチェーンメールを受け取っている可能性があったので、担任教員を通じて、チェーンメールが届いた場合には、内容を見せず、他人にも転送しないように注意した。

◆今後の対策と効果

- ・チェーンメールの内容を真に受ける生徒もいる。メールの取り扱いを含め情報モラルを指導する機会が通常のカリキュラムの制約もあり難しい状況であり、生徒に情報モラルを指導することが今後の検討課題である。

チェーンメール4

高等学校での事例

◆被害状況

- ・生徒が利用している電子メールに不幸の手紙の類のメールが届くようになり、個別に相談をしてきた。
- ・授業では不幸の手紙の類のチェーンメールには対応しないよう指導しているが、生徒のなかには、チェーンメールとわかっていても不安になる生徒がいて、その都度、相談を持ちかけてくる。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

- －校内のセキュリティ対策－
- ・情報の授業時に電子メールのマナーを確認している。

◆発見の経緯

- ・発見方法：不幸の手紙を受け取った生徒からの相談により判明した。
- ・発生日時：平成16年6月頃
- ・発見日：平成16年6月頃
- ・事実確認：平成16年6月頃

◆被害への対応

- －メールを受け取った生徒への対応－
- ・対応日：相談を受けた日
 - ・対応担当者：情報担当教員
 - ・対応方法：
 - メールの内容を気にしないようにアドバイスした。
 - 今後、チェーンメールが来た場合には学校が準備したチェーンメール受付用アドレスにメールを送信するよう指導した。
- －全生徒への対応－
- ・対応日：情報の授業時
 - ・対応担当者：情報担当教員
 - ・対応方法：
 - 受け取ったチェーンメールには対応しないよう、電子メールのマナーを再確認した。
 - 学校で作成したチェーンメール受付用アドレスを紹介し、どうしても不安な場合にはそのアドレスにメールを送るように指導した。

◆今後の対策と効果

- ・チェーンメールの内容を真に受ける生徒もいるので、チェーンメールを受け取っても対応しないように指導を今後も継続して実施していく。
- ・チェーンメールを送信しないと不安になる生徒の為に、学校で5つほどチェーンメール受付用の電子メールアドレスを作成し、そのアドレスに送るよう指導を行っていくこととした。

チェーンメール5

高等学校での事例

◆被害状況

- ・特定の生徒を「知っている？〇〇ちゃんは、〇〇だよ」といった誹謗・中傷する電子メールが校内で出回った。本人より相談を受けた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

ーチェーンメールを転送した生徒への対応ー

- ・対応日：
- ・対応担当者：
- ・対応方法：

ささいなことをきっかけとしたグループ同士の喧嘩から、ある生徒をターゲットとしたいやがらせのメールであることがわかった。メールを発信、転送したと思われる生徒に話を聞いたところ転送の確認がとれた。誹謗・中傷のチェーンメールは、モラルの面からやっつけてはいけないことを指導した。

また、メールを受け取った生徒のなかには、事実でない内容を事実として信じている状況もあり、インターネットを利用した Web サイト、メールからの情報については、すべてが正しい情報ではないので、きちんと事実を確認することが必要であることをあわせて指導した。

◆今後の対策と効果

チェーンメール6

高等学校での事例

◆被害状況

- ・特定の生徒の校内での様子を携帯電話のカメラで撮影をし、撮影した画像とともに誹謗・中傷のコメントをつけて同級生の携帯電話にメールを作成し送信した。その後、そのメールが生徒間でチェーンメール化した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒から相談により判明した。
- ・発生日時：平成16年
- ・発見日：平成16年
- ・事実確認：

◆被害への対応

ーチェーンメールへの対応ー

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

チェーンメール化したメールが生徒個人の携帯電話に送信されるので、誹謗・中傷された本人やメールをやり取りしている生徒からの申し出がないと事実が判明しにくい。また、発信源を突き止めるのも難しい状況である。

情報の授業時に、チェーンメールの取扱いや情報モラルの指導を行っているが、特定の生徒を誹謗・中傷したメールのチェーンメール化を防ぐ具体的な手立てがないのが現状である。

◆今後の対策と効果

携帯電話を利用した嫌がらせメール1

中学校での事例

◆被害状況

- ・携帯電話のショートメール機能を利用して、特定の生徒に嫌がらせメールが送られてきた。非通知設定にしてショートメールが送られてきたので、ショートメールを送った生徒の特定はできなかった。
- ・あまりにも多くのいやがらせメールが届いたため、生徒は保護者と相談のうえ、携帯電話の番号を変更した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：メールを送られてきた生徒の保護者からの連絡により判明した。
- ・発生日時：平成15年
- ・発見日：平成15年
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：
いやがらせメールが送られてきた事実をクラス全員に伝え、特定の生徒を誹謗・中傷するようなメールを送らないように注意した。
携帯電話番号やメールアドレスなどの個人情報、安易に人に教えないように注意した。
あわせて友人の携帯電話番号やメールアドレスを本人のいないところで勝手に教えないように注意した。

◆今後の対策と効果

- ・携帯電話番号を変更してから、ショートメールは届かなくなった。

携帯電話を利用した嫌がらせメール2

中学校での事例

◆被害状況

- ・生徒に対して、生徒が嫌がる内容を記載したメールが頻繁に届くようになった。
- ・メールの内容から、送信者はおそらく同級生によるものと推測できたが、送信メールアドレスを変更するなどして送信者が特定できないようにしている。
- ・嫌がらせメールを受け取った生徒はショックを受け、教員に対応方法を相談してきた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：嫌がらせメールを受け取った生徒からの相談により判明した。
- ・発生日時：平成 17 年
- ・発見日：
- ・事実確認：

◆被害への対応

ー相談してきた生徒への対応ー

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

嫌がらせメールが頻繁に届くようになった生徒には、届いたメールは無視するように伝えた。また、メールアドレスを変更して、メールが届かないようにすることも1つの対策であることを伝えた。

◆今後の対策と効果

- ・携帯電話を利用して電子メール、掲示板、ブログを利用する生徒が増えている。また、メール、掲示板、ブログに友人の悪口を記載する生徒も多く、インターネット上に掲載された情報が全世界に公開されているという認識もない。今後は、生徒に情報モラルを指導する予定だが、通常のカリキュラムの都合もあり、現実的に多くの時間を割いて指導できていない現状もあり、適切な指導方法を検討中である。

携帯電話を利用した嫌がらせメール3

高等学校での事例

◆被害状況

- ・特定の生徒を誹謗・中傷する内容の電子メールを同級生に大量に送信していた。誹謗・中傷された生徒は、精神的にショックを受けていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：誹謗・中傷されていた生徒の申し出により判明した。
- ・発生日時：
- ・発見日：
- ・事実確認：生徒の携帯電話から実際に送信していた電子メールを確認した。

◆被害への対応

－生徒への対応－

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：

携帯電話の持込みは禁止にしていたが、事実関係を確認するために、ホームルーム中に生徒に携帯電話を提出させ、電子メールの内容を生徒とともに確認し、特定の個人を誹謗・中傷する行為に対して厳しく指導した。

電子メールは不特定多数の人に見られる可能性があり、また一度ネットワークに送信してしまうと、自分の意思で電子メールを削除することができないので、電子メールを送信する際には、内容をよく確認してから送信するように指導した。

－保護者への対応－

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：

今回発生した特定の個人を誹謗・中傷する電子メールが広まった状況説明とともに、生徒が保有している携帯電話の電子メールの内容を確認したことについて、保護者に説明を行った。

◆今後の対策と効果

携帯電話を利用した嫌がらせメール4

高等学校での事例

◆被害状況

- ・ある女子生徒が、特定の女子生徒の携帯電話の電子メールアドレスに、その女子生徒を誹謗・中傷する内容を記載した嫌がらせメールを送信していた。
- ・嫌がらせメールが届いた生徒は、対応に苦慮して教員に相談をしてきた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：いやがらせメールを受け取った生徒からの申し出により判明した。
- ・発生日時：平成17年5月
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成17年5月
- ・対応担当者：情報担当教員
- ・対応方法：
相談してきた生徒へは、嫌がらせメールに記載された内容は無視するように指導した。あわせて、届いたいたずらメールは事態が解決するまで削除せずに保存しておくように伝えた。
相談してきた生徒の携帯電話から嫌がらせメールの送信者がすぐに判明したので、後日、送信した生徒に対して個別指導を実施した。

◆今後の対策と効果

- ・一度の個別指導では、嫌がらせメールはなくなる。嫌がらせメールが届く生徒のケアをしつつ、メールを送信する生徒に繰り返し指導をすることで、事態の解決を図っている。

携帯電話を利用した架空の料金請求メール 1

高等学校での事例

◆被害状況

- ・生徒の携帯電話に、料金の架空請求メールが頻繁に届くようになった。
- ・料金の架空請求メールが届いた生徒は、ダイレクトメールで送られてきた出会い系サイトの Web を閲覧した経験があったので、料金の架空請求メールが届いてどう対処するべきか悩んでいた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：架空請求メールが頻繁に届くようになった生徒から相談があり判明した。
- ・発生日時：平成 16 年 6 月頃
- ・発見日：平成 16 年 6 月頃
- ・事実確認：平成 16 年 6 月頃

◆被害への対応

—相談をしてきた生徒への対応—

- ・対応日：平成 16 年 6 月頃
- ・対応担当者：相談を受けた教員（情報担当教員）
- ・対応方法：

料金の架空請求に応じる必要はないことを伝えた。そのうえで、頻繁にメールが届いて不安になるようであれば、電子メールアドレスを変更するよう指導した。メールアドレスを変更してからは料金の架空請求メールは届いていない。

◆今後の対策と効果

- ・授業の中で、架空請求メールが届いた際には対応しないことを取り入れることとした。

携帯電話を利用した架空の料金請求メール 2

高等学校での事例

◆被害状況

- ・携帯電話の通称ワンギリに対して携帯電話操作を誤ってしまいコールバックをしてしまったところ、数日後に3万円を請求する電子メールが届いた。不安になり教員に相談してきた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：
- ・対応方法：

請求額の振込みをしていないため、実害はないものの、この手の請求をする電子メールは無視することを伝えただけで、適切な対応として情報が多く集まる市役所の消費者相談の連絡先を教えた。

◆今後の対策と効果

- ・当フォーラム事務局よりNTTドコモなど携帯電話会社のWebサイトで最新の情報が手に入ることを、また神奈川県警ハイテク犯罪センターが相談窓口としてあることも伝えた。

携帯電話を利用した架空の料金請求メール 3

高等学校での事例

◆被害状況

- ・教科「情報」を担当している教員が他の教科の授業を実施している時に、自分に届いた架空請求メールを題材にし生徒に架空請求メールの取扱いについて注意を促したところ、授業終了後に教員のもとへ生徒が個別に相談にきた。
- ・相談のなかには、請求金額が高校生でも支払い可能な金額（数千円）であったため、請求に応じてしまったという相談もあった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの個別の相談により判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

ー相談してきた生徒への対応ー

- ・対応日：
- ・対応担当者：相談を受けた教員
- ・対応方法：

架空請求メールが届き、支払うべきか悩んでいる生徒からの相談に対しては、この手の請求をする電子メールは無視してよいことを伝えた。

請求に応じたことがあると申し出をしてきた生徒に対しては、今後同じような電子メールが来ても無視するように伝えた。

◆今後の対策と効果

- ・今後は、電子メールの利用や情報モラルを取扱う教科「情報」の授業の中で、架空請求メール等への対応を紹介することとした。

携帯電話を利用した架空の料金請求メール 4

高等学校での事例

◆被害状況

- ・女子生徒が利用している携帯電話に架空請求メールが届いた。請求金額が 3～4 万円ぐらいで、身に覚えのない請求だったため、請求に応じる前に教員に相談した。
- ・請求に応じる前の相談だったので、教員からメールを無視するようにアドバイスを行うことができ、金銭的な被害はなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒から相談により判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

－相談してきた生徒への対応－

- ・対応日：相談があったその日
- ・対応担当者：情報担当教員
- ・対応方法：
請求に応じる前の相談だったので、教員からメールを無視するようにアドバイスをを行った。

◆今後の対策と効果

- ・架空請求メールが生徒にも横行しているので、情報の授業時に生徒からの相談事例や教員自身に届いた架空請求メールの話を行い、被害にあわないよう指導している。また、国民生活センターなど架空請求を実施している業者リストや手口・対処方法を掲載している Web サイトを利用して、届いたメールが本当に架空請求メールなのかどうか調べるよう生徒に指導している。

－ 参考 －

国民生活センターのサイト

http://www.kokusen.go.jp/soudan_now/kakuseikyu_list.html

携帯電話を利用した架空の料金請求メール 5

高等学校での事例

◆被害状況

- 男子生徒の携帯電話に架空請求メールが届いた。請求金額が 6,000～7,000 円くらいで、生徒自身で支払が可能な金額だったことと、過去に携帯電話のインターネット機能を利用してアダルト系の Web サイトを閲覧した経験があったので、その料金請求と思い込み、架空請求に応じてしまった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- 発見方法：振込みに応じた生徒の相談により判明した。
- 発生日時：平成 16 年
- 発見日：平成 16 年
- 事実確認：

◆被害への対応

—相談してきた生徒への対応—

- 対応日：相談があったその日
- 対応担当者：情報担当教員
- 対応方法：
料金振込み後の相談だったので、振込み後の請求に対しては対応ができなかったが、今後、同じような架空請求に対応しないようアドバイスを実施した。

◆今後の対策と効果

- 相談後、その生徒に架空請求メールは届いているものの、メールに応じることはなくなり、金銭的な被害は発生していない。

携帯電話を利用した架空の料金請求メール 6

高等学校での事例

◆被害状況

- ・女子生徒の携帯電話に架空の料金請求メールが届いた。請求はアダルトサイト関係の内容で、その女子生徒は過去に携帯電話のインターネット機能を利用してアダルトサイトを閲覧したことがあったので、不安になり教員に相談をしてきた。
- ・金銭的な被害は発生していない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談により判明した。
- ・発生日時：平成 16 年
- ・発見日：
- ・事実確認：

◆被害への対応

－相談してきた生徒への対応－

- ・対応日：相談のあったその日
- ・対応担当者：情報担当教員
- ・対応方法：
身に覚えのない請求メールであれば、請求を無視するようにアドバイスした。あわせて、届いたメールに対して絶対に返信しないように指導を行った。

◆今後の対策と効果

- ・架空請求メールについては、生徒同士での情報交換が盛んに行われており、教員に相談してくるケースは稀である。そのため、架空請求メールの受信状況や金銭的な被害状況などの生徒の正確な被害実態の把握が今後の課題である。

携帯電話を利用した電子メールのトラブル

高等学校での事例

◆被害状況

- 多くの生徒が携帯電話を保有するようになり、学校内でも生徒同士で携帯電話の電子メール機能を利用したコミュニケーションが行われているが、学校内での些細な出来事により頻繁にメール交換していた相手に嫌がらせメールを送信するなどのトラブルが発生している。
- トラブルが発生する時期は主に4～6月で、特に高校1年生が多い。
- 嫌がらせメールを送信する際に、自分の携帯電話ではなく友人の携帯電話から嫌がらせメールを送信していることもある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- 発見方法：嫌がらせメールが届いた生徒からの相談により判明した。
- 発生日時：
- 発見日：
- 事実確認：

◆被害への対応

—生徒への対応—

- 対応日：
- 対応担当者：情報担当教員
- 対応方法：

嫌がらせメールが届いた生徒からの相談については、届いたメールをもとに送信者を特定し、送信した生徒を個別指導して対応している。

指導にあたっては、電子メールの送信マナーを伝えるとともに、メールを受け取った側の気持ちを考えさせるようにしている。

主に4～6月にかけてトラブルが発生することが多いので、入学直後に適切な指導を行うように検討している。

◆今後の対策と効果

携帯電話へのチェーンメールや架空請求メール

高等学校での事例

◆被害状況

- 多くの生徒が携帯電話を保有しており、生徒同士で携帯電話のメールでコミュニケーションをとっている。
- 以前はチェーンメールや架空請求メールなどのメールに関するトラブルの相談があったが、最近は携帯電話でメールを扱う機会が増えているにもかかわらず相談がほとんどないので生徒の状況がつかめていない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- 発見方法：生徒からの相談件数が減少傾向にあるため。
- 発生日時：
- 発見日：
- 事実確認：

◆被害への対応

—生徒への対応—

- 対応日：
- 対応担当者：情報担当教員
- 対応方法：

相談件数の減少は日常的に携帯電話でメールを扱うことが多くなり、知人からのメール以外は削除するなど、生徒が情報の取捨選択を行うようになったことが要因と考えている。

一方で、友人と常にメールで連絡を取り合っていないと不安になる生徒も多く、生徒の状況を把握し、かつ携帯電話依存へ対応することが今後の課題である。

◆今後の対策と効果

生徒同士での脅迫メール

高等学校での事例

◆被害状況

- ・携帯電話の電子メールを利用して、複数の生徒が特定の生徒に金品を要求する脅迫メールを送っていた。
- ・脅迫メールを受け取っていた生徒は、金品の要求には応じなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：脅迫されていた生徒の保護者が事実関係を学校に連絡して判明した。
- ・発生日時：平成 17 年 1 月
- ・発見日：平成 17 年 2 月
- ・事実確認：平成 17 年 2 月

◆被害への対応

ー脅迫をした生徒への対応ー

- ・対応日：平成 17 年 2 月
- ・対応担当者：生活指導担当教員
- ・対応方法：

事実関係を確認し、個別指導を実施した。

複数の生徒を個別指導する際には、生徒同士が携帯電話を利用して口裏あわせを行うので、生徒の携帯電話を教員に提出させてから個別指導を実施している。

◆今後の対策と効果

- ・授業で電子メールの扱いについては指導を行っているが、適切に電子メールを利用するように指導を徹底していく。

交際を迫る執拗なメール

高等学校での事例

◆被害状況

- ・ある男子生徒が特定の女子生徒に対し交際を迫る電子メールを一方向的に送り続けていた。
- ・電子メールを送られてきた女子生徒は、あまりのしつこさにどのように対処するべきか悩んでいた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：電子メールが送られてくる女子生徒からの相談により判明した。
- ・発生日時：平成 15 年
- ・発見日：平成 15 年
- ・事実確認：平成 15 年

◆被害への対応

－相談してきた生徒への対応－

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：
一つの方法として電子メールアドレスを変更することを勧めた。
電子メールアドレスは個人情報なので、安易に教えないように指導した。

－電子メールを送信していた生徒への対応－

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：
一方向的に執拗に電子メールを送信していた生徒に対して、電子メールを受ける側の気持ちを考えるように個別指導を実施した。

◆今後の対策と効果

- ・個別指導を実施してから、相談を受けた生徒に執拗に電子メールを送信するという行為は行われていない。

なりすましメールによる誹謗・中傷

高等学校での事例

◆被害状況

- ・生徒がメールアドレスを偽装できる Web サイトを使用して他の生徒になりすまし、特定の生徒を誹謗・中傷するメールを送信した。
- ・誹謗・中傷を受けた生徒は、メールを送信した生徒に対して抗議を行ったが、抗議を受けた生徒は第三者にメールアドレスを利用されただけで実際にメールを送信していなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：誹謗・中傷を受けた生徒と、なりすまされた生徒の相談により判明した。
- ・発生日時：平成 17 年 10 月頃
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：
- ・対応担当者：被害生徒の担任教員
- ・対応方法：

個人を誹謗・中傷するメールを送らないようにホームルーム時にクラス全員に注意を行った。その際、生徒の情報から、携帯電話の Web サイトに携帯電話のメールアドレスを偽装して送信するウェブサイトを利用している生徒が多数いることが明らかになった。

後日、クラスの中の一人が被害生徒に誹謗・中傷のメールを送信していたことが判明したので、担任教員が誹謗・中傷を行った生徒を呼び出し、メールアドレスを偽装してなりすましメールを送信しないように指導を行った。

◆今後の対策と効果

- ・指導後に、メールアドレスを偽装できる Web サイトを使用したなりすましメールのトラブルは発生していない。

フィッシングメール

専門学校での事例

◆被害状況

- ・学校の代表メールアドレス（Web サイトに記載）に、キャンペーンに応募していないにもかかわらず車の当選通知メールが届いた。
- ・メールにはキャンペーンを実施している会社名、当選手続き方法、当選手続き用の URL が記載されていたが、キャンペーンについての問合せ先等の記載はなかった。
- ・最近新聞紙上等で盛んに注意喚起が行われているフィッシングメールの可能性が高いメールなので、学生のリテラシ向上の教材として利用した。
- ・学生に紹介後、今回のメールに関する報道（新聞記事）が行われ、報道（新聞記事）の内容についても学生に伝えた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：学校の代表メールアドレスに届いていたフィッシングメールをメール管理教員が発見した。
- ・発生日時：平成 16 年 12 月中旬
- ・発見日：平成 16 年 12 月 14 日
- ・事実確認：平成 16 年 12 月 20 日 新聞記事により事実確認

◆被害への対応

－学生への対応－

- ・対応日：平成 16 年 12 月中旬～下旬
- ・対応担当者：教員
- ・対応方法：

学生個人が利用しているメールに同様のメールが届いていないか確認し、届いている場合はメールを破棄するよう指導した。

メールに記載されていた URL には cgi を利用して ID が振られていたので、当選手続きを行うとメールアドレスが登録される可能性があることを伝えた。

－参考 メール本文の内容－

Date: Tue, 14 Dec 2004 17:47:11 +0900
 From: ●●精機株式会社 <●●-seiki@●●.or.jp>
 Subject: 御当選通知 ●●精機（株）よりお知らせ
 この度は、テブラコール推進キャンペーンご応募有難う御座いました。
 約 4 2 万通の多数のご応募の中から厳正なる抽選の結果、
 ホンダ・ステップワゴン（ハッピーエディション G-2.0 FF）
 御当選されましたのでご連絡させていただきます。
 後程、当社担当よりご連絡を差し上げますので
 下記 URL よりお手続き下さい。
http://www.●●.com/formgen.cgi?ID=*****
 この度は誠にありがとうございました。

◆今後の対策と効果

不当請求メール

専門学校での事例

◆被害状況

- ・生徒に届いた宣伝メールに従い、URL をクリックしたところ、翌日、利用料金を請求するメールが届いた。
- ・心配になった生徒が教員に対応を尋ねてきたが、料金を支払っていないので実害は発生していない。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談により判明した。
- ・発生日時：平成 17 年 10 月
- ・発見日：
- ・対応方法：

◆被害への対応

一生徒への対応

- ・対応日：平成 17 年 10 月
- ・対応担当者：
- ・対応方法：

ありふれた手口の不当請求メールであったため、生徒に今後料金を請求されるメールが届いても無視するように伝えた。念のため、件名と URL を検索エンジンで検索したところ、公的な機関の Web サイトによる情報として、不当請求メールを送りつけてくる Web サイトであることがわかった。なお、下記①～③のメールが順次送られてきている。

①【*****をご利用頂きありがとうございます】
このメールは動画を閲覧するごとに配信されます。
ご入金がお済になれば配信は停止となります。
ご入金がお済の場合はメールにてお知らせください。

▼登録情報▼

あなたのメールアドレス	*****@*****	あなたの ID	**-*****
あなたのリモートホスト	*****.***-*.****.ne.jp	あなたの接続先 IP	**.*.*.*.*
あなたのプロバイダ名		あなたの閲覧したムービーNo. :	*****

以上の情報及びログを保存いたしました

▼サービス内容▼

通常利用料金 85,000円 ご利用期限 無制限動画見放題 イベント開催中(支払期限内)の利用料金 55,000円

②【XXXXXXXX@XXX.XXX.XX.XX】様へ*****より連絡事項を配信致します。
本電子メールは 2005年10月 にメンバー登録された方のうち、現時点まで登録料金未納と我々が認識している方に配信されています。キャンペーン期間料金の適用は本日の手続きまでとなりますので未だ手続きをされていない様であればお急ぎ下さい。手続き日(消印)を入金日と判断しておりますので遅達等は必要御座いません。問合せ先へご連絡頂ければ結構です。

③本電子メールは 10月20日にメンバー登録して頂いたユーザーID - **-*****登録アドレス
XXXXXXXX@XXX.XXX.XX.XX 様宛に配信されています。
登録者様に対し、当方が必要と考えるご案内は充分に行って参りましたが、未だご入金の確認が取れておりません。近日中の対応が無い場合、我々は本契約者様を違反者として認識いたします。お支払い期限【2005-10-20】から25日以上の期限超過に関しては延滞金発生と併せて回収業務の対象とさせていただきます。掛かる費用の一部は違反者自身の負担となります。ご承知おき下さい。

◆今後の対策と効果

- ・生徒には、不当請求メールであることを伝えたが、そもそも宣伝メールはトラブルに巻き込まれる可能性があるので無視するように指導した。また、Web サイトを活用することで犯罪の手口や注意喚起を促す情報を手に入れることもできるため、利用することも必要であると指導した。

携帯電話を利用した架空の料金請求 1

高等学校での事例

◆被害状況

- ・生徒が携帯電話を使用中、身に覚えのない Web サイトへの登録完了と料金の振込み依頼を示す文章が表示された。
- ・不安を覚えた生徒が教員に対応を尋ねてきた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談があった。
- ・発生日時：平成 16 年 9 月頃
- ・発見日：平成 16 年 9 月頃
- ・事実確認：平成 16 年 9 月頃

◆被害への対応

ー生徒への対応ー

- ・対応日：平成 16 年 9 月頃
- ・対応担当者：担当教員
- ・対応方法：

被害には至っていなかったが、すぐに NTT ドコモ等の Web ページを参照し、同様な事例がないか調査した。その結果、「個人情報を入力していると偽って請求行為を行うサイトについて」のページより本件と同様な事例が掲載されていた。

<http://www.nttdocomo.co.jp/info/f/itsuwari.html>

Webページの内容を参考に、まず詐欺であり請求された料金の支払い義務はないことを伝え、あたかも本人が申込みをしたと錯覚させる携帯電話機情報の表示については、携帯電話機が FOMA なので Web 管理者に機種名は通知されてしまうが、それ以外の個人を特定する情報は通知されないことを伝え、生徒の心配を解いた。

◆今後の対策と効果

本件の対応のほかに、

- ・知らない送信者へ返信メールをしない
- ・知らない電話番号の着信にはでない、コールバックしない
- ・懸賞サイトなどにむやみに個人情報を送信しない
- ・心配ならば電話番号を変更する

といった助言を行った。

携帯電話を利用した架空の料金請求 2

高等学校での事例

◆被害状況

- ・女子生徒が使用している携帯電話に電子メールが送られてきた。女性生徒が電子メールに記載されているリンクを辿って Web サイトを閲覧したところ、携帯電話の固体識別番号として機種や製造番号ともに、登録手続きが完了した旨ならびに利用料金数万円を振り込むよう表示された。
- ・女子生徒は、生徒本人が使用している携帯電話の固体識別番号が表示されたので、すでに本人が特定されており利用料金を支払う必要があるかもしれないと非常に不安な気持ちを抱いていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：料金の請求を受けた女子生徒からの相談により判明した。
- ・発生日時：平成 16 年 9 月
- ・発見日：平成 16 年 9 月
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：相談を受けた当日
- ・対応担当者：情報担当教員
- ・対応方法：

生徒本人が使用している携帯電話の固体識別番号が表示されたので、すでに本人が特定されており利用料金を支払う必要があるかもしれないと非常に不安に感じている様子だったため、時間をかけて相談に応じた。

表示された携帯電話の固体識別番号からは、携帯電話番号・メールアドレス・住所・氏名などの情報は特定できないことを説明し、請求された料金は無視するように助言を行った。

◆今後の対策と効果

ワンクリック詐欺への対応

高等学校での事例

◆被害状況

- ・平成 16 年度に生徒より携帯電話を利用した料金の不当請求の相談が 3 件あった。うち、2 件は生活指導担当教員への相談、1 件は情報担当教員への相談であった。
- ・いずれの相談も携帯電話を利用した Web サイトの閲覧中に、Web ページ内に表示されていた画像等をクリックし、携帯電話の固体識別番号や電子メールアドレスの表示とともに登録完了にともなう料金の請求（1～3 万円ぐらい）画面が表示された。
- ・あたかも個人情報取得しているかと思わせるような情報とともに料金請求が行われていたため、生徒が不安になり教員に相談してきた。幸いなことに、いずれの相談もお金を振込む前の相談だったため、金銭的な被害はなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談により判明した。
- ・発生日時：平成 16 年度
- ・発見日：平成 16 年度
- ・事実確認：平成 16 年度

◆被害への対応

－生徒への対応－

- ・対応日：
- ・対応担当者：生活指導担当教員・情報担当教員
- ・対応方法：

Web ページに表示された携帯電話の固体識別番号には、氏名・住所・電話番号等の個人情報は含まれていないことを伝えた。また、表示された登録完了の画面についても契約自体が無効の可能性が高い※ので、料金を支払う必要はないことを伝えた。

※ 電子消費者契約法では、事業者は消費者に対して申し込み内容を再度確認させるための画面を用意する必要がある。確認措置がない場合は、その申し込みの無効を主張することができる。

正式名：電子消費者契約及び電子承諾通知に関する民法の特例に関する法律

◆今後の対策と効果

- ・生徒の携帯電話所持率が高くワンクリック詐欺の被害に遭う可能性があるため、1 年次に必修で実施している情報の授業時にワンクリック詐欺の事例を紹介しながら被害に遭わないための指導をしていくこととした。

不当な料金の請求メールへの対応

高等学校での事例

◆被害状況

- ・女子生徒が携帯電話を利用して Web サイトを閲覧中にアダルトサイトが表示され、そのサイトに自宅の電話番号と携帯電話の電子メールアドレスを誤って登録してしまった。
- ・電子メールアドレス登録後すぐに、情報閲覧料金の請求が登録した電子メールアドレスに届いた。
- ・アダルトサイトからの料金の請求メールだったため、生徒は請求された料金の取り扱いについて保護者に相談できず、情報担当教員に相談をしてきた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒の相談により判明した。
- ・発生日時：平成 17 年 5 月
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成 17 年 5 月
- ・対応担当者：情報担当教員
- ・対応方法：

生徒はアダルトコンテンツを閲覧しておらず情報登録を行っただけなので、届いた料金の請求メールは不当な請求と判断できた。そのため、料金の請求メールが届いても一切対応しないように指導した。あわせて、神奈川県警ハイテク犯罪対策センターの Web サイトから類似の事例も紹介し、落ち着いて料金の請求メールに対処するように指導した。また、Web サイトから自宅の電話番号を登録しており、自宅に電話がかかってくることも考えられたので、保護者に対してもアダルトサイトに情報を登録した事実と学校で紹介した対策を生徒から伝えるように指導した。

◆今後の対策と効果

- ・料金の請求メールは生徒からの相談後も送信されてきていたが、1 ヶ月間、生徒が何も反応しなかったため、その後メールは届かなくなった。また、自宅に電話がかかってくることもなかった。

公開電子メールアドレスへの大量の迷惑メール1

高等学校での事例

◆被害状況

- ・学校の Web サイトに公開している電子メールアドレスに、迷惑メールが大量に届くようになった。
- ・夏休み期間中に学校と生徒が連絡できるために設けた電子メールアドレスだったため、生徒からの連絡メールを探し出すのに時間がかかった。
- ・迷惑メールが大量に送られてくるので、一時的に学校の Web サイトの公開をとりやめた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・職員室にはネットワークに接続しているパソコンが4台設置しており、各教員に1つずつのメールアドレスを配布している。

―校内のパソコン利用状況や利用形態―

- ・職員室のパソコンは教員であればだれでも利用できる。

◆発見の経緯

- ・発見方法：公開電子メールアドレスの管理者の申し出により判明した。
- ・発生日時：平成16年8月頃
- ・発見日：平成16年8月頃
- ・事実確認：平成16年8月頃

◆被害への対応

―迷惑メールへの対応―

- ・対応日：平成16年8月頃
- ・対応担当者：Webサイト管理教員
- ・対応方法：

迷惑メールが大量に送られてくるので、電子メールアドレスを記載している Web サイトの公開を一時的に取りやめた。迷惑メールが大量に送られてきた電子メールアドレスを変更した。

◆今後の対策と効果

- ・現在も情報管理委員会で迷惑メール対策を検討中である。

公開電子メールアドレスへの大量の迷惑メール2

高等学校での事例

◆被害状況

- ・生徒が個人で Web サイトを作成した。この Web サイトで生徒個人のパソコン用メールアドレスを公開してしまったため、頻繁に宣伝メールが来るようになった。
- ・宣伝メールの配信を止めようと宣伝メール記載のアドレスより停止の連絡を入れたところ、さらに宣伝メールが一日あたり 20 件ほど届くようになった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談。
- ・発生日時：平成 16 年
- ・発見日：
- ・対応方法：

◆被害への対応

ー生徒への対応ー

- ・対応日：
- ・対応担当者：
- ・対応方法：

一度、宣伝メールのターゲットとなると配信停止させることが難しいことを伝えた。

今後とも宣伝メールは徹底的に無視をし、プロバイダの迷惑メール受信拒否機能を利用するよう勧めた。

その後も宣伝メールは減ることはなく、迷惑メール受信拒否機能も相手が複数のメールアドレスを利用してくるため効果がなく、結局、新しいメールアドレスを取得することとなった。

◆今後の対策と効果

Web サイトでメールアドレスを公開する場合の注意点として以下を指導した。

- ・プロバイダの個人所有メールアドレスは、公開しないこと
- ・代わりに無料のフリーメール（Yahoo など）を利用し、宣伝メールなどのターゲットとなったときは、適宜新しいフリーメールアドレスを取得すること
- ・プロバイダの個人所有メールアドレスにもエアリアスサービス（別名アドレス）がついているタイプがあり、場合によってはエイリアスサービスを利用し、適宜変更すること

公開電子メールアドレスへの大量の迷惑メール3

高等学校での事例

◆被害状況

- Web サイトに公開している電子メールアドレスに、迷惑メールが届くようになった。迷惑メールの中にはコンピュータウイルスに感染しているメールもあった。
- 公開している電子メールアドレスは、中学校からの問い合わせや地域住民からの情報提供に利用されており、迷惑メールとの判別に時間がかかってしまう。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のセキュリティ対策―

- サーバにはウイルス対策ソフトが導入されている。

◆発見の経緯

- 発見方法：Web サイトを管理している教員の申し出により判明した。
- 発生日時：
- 発見日：
- 事実確認：

◆被害への対応

―迷惑メールへの対応―

- 対応日：迷惑メールが届く都度
- 対応担当者：Web サイト管理教員
- 対応方法：
毎朝、学校代表の電子メールアドレスに届いている電子メールを確認し、不要なメールはWeb サイト管理教員がその都度削除している。

◆今後の対策と効果

- 現在、ネットワークシステムを移行したため、迷惑メールは届いていない。
- 中学校からの問い合わせや地域住民からの情報提供に利用されているので、電子メールは公開を継続していく。

公開電子メールアドレスへの大量の迷惑メール4

高等学校での事例

◆被害状況

- ・情報公開のために、Web サイトを活用している。公開している Web サイト上には、様々な意見を寄せてもらうために学校の代表電子メールアドレスを記載している。
- ・最近、公開している電子メールアドレス宛に、毎日 30 通以上のスパムメールが届くようになった。また、スパムメールに紛れて、ウイルスメールも届くようになった。
- ・スパムメールが大量に届くために、進学希望者や地域の方々などからの問い合わせ・意見のメールの判別に時間がかかっている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：情報担当教員がメール確認作業時にスパムメールの件数が増えていることを確認した。
- ・発生日時：平成 17 年
- ・発見日：
- ・事実確認：

◆被害への対応

ー迷惑メールへの対応ー

- ・対応日：毎日
- ・対応担当者：情報担当教員
- ・対応方法：

公開している電子メールアドレス宛へのメールは情報担当教員が毎朝確認している。スパムメールと一緒にウイルスメールも届くことがあり、ウイルス感染を防ぐためにも不用意にメールを開かずにメールの送信者名や件名でメールの判別を行っているので、確認作業に 20～30 分程度の時間がかかるようになった。

システムのスパムメールを排除する方法も検討したが、スパムメールに紛れて確認すべきメールも排除されてしまうことが懸念されるので、システムの導入はしていない。

◆今後の対策と効果

- ・フォーラム事務局からスパムメールを防ぐ方法の 1 つとして、Web サイトに公開している電子メールアドレスを既存アドレスから変更して、画像にして Web サイト上に表示する方法があることを紹介した。

振り込め詐欺1

高等学校での事例

◆被害状況

- ・同時期に、複数の男性教員の自宅に振り込め詐欺と思われる電話があった。いずれの電話も、電車内での痴漢行為に関する内容で、示談金を要求する電話であった。
- ・振り込め詐欺と思われる電話を受けた自宅から学校に連絡があり、教職員の所在を確認できたので、金銭的な被害はなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：教員の自宅からの連絡により判明した。
- ・発生日時：平成16年
- ・発見日：平成16年
- ・事実確認：

◆被害への対応

—教員への対応—

- ・対応日：
- ・対応担当者：
- ・対応方法：

同時期に男性教員を対象とし同じ手口（電車内での痴漢行為）の電話が自宅にかかっていたので、全教員に対して、振り込め詐欺の被害に遭わないよう注意喚起を行った。

今回の件では、同時期に複数の男性教員に連絡があり、学校内の情報等がもれている可能性も考えられたので、これまで以上に適切な情報管理を行うよう、教員一人一人の意識の向上を再認識した。

◆今後の対策と効果

振り込め詐欺2

高等学校での事例

◆被害状況

- ・複数の生徒の保護者に振り込め詐欺と思われる電話があった。いずれの電話も、生徒の通学中に交通事故に巻き込まれたという内容だった。
- ・保護者から学校へ問い合わせがあり、生徒の無事が確認されたので、金銭的な被害はなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒の保護者からの連絡により判明した。
- ・発生日時：平成16年
- ・発見日：平成16年
- ・事実確認：

◆被害への対応

－保護者への対応－

- ・対応日：
- ・対応担当者：
- ・対応方法：

学校では、日常の取り組みとして、保護者との連絡を密に実施している。平日の朝の出欠席確認時に、保護者からの連絡なく遅刻あるいは欠席している生徒がいた場合、その保護者に必ず学校側から連絡を入れるようにしている。

今回、生徒の保護者に交通事故に巻き込まれたとの連絡が入ったが、何かあれば学校から連絡があるのに学校からの連絡がない状況だったため、保護者が交通事故に巻き込まれたとかかってきた電話に不信感を抱き、確認のための学校に連絡を入れてきた。

日常から学校と保護者の間で密に連絡を取る体制が整っていたので、冷静に対処することができたと考えている。

◆今後の対策と効果

- ・今後も、学校と保護者の間で密に連絡をとることを継続していき、この手の振り込み詐欺の被害を未然に防いでいく。

出会い系サイトを発端とした家出

中学校での事例

◆被害状況

- ・ある女子生徒が家出をしていた。保護者は警察に捜索願を提出し、学校に家出の事実の連絡をした。家出の連絡を聞いた教員が、女子生徒の携帯電話に連絡をしたところ、女子生徒が電話に応じ、出会い系サイトを通じて知り合った男性と会っていることを伝えてきた。
- ・教員は女子生徒にすぐに帰ってくるよう指示を行い、近くの駅まで迎えに行った。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：保護者からの連絡をもとに女子生徒の携帯電話に連絡を行ったところ、出会い系サイトで知り合った人物と会っている事実を生徒本人が伝えてきて判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成 16 年
- ・対応担当者：担任教員・生活指導担当教員
- ・対応方法：

今回発生した事実を全校生徒に伝えると、どの生徒が出会い系サイトを利用したのかを特定しようとするので、全校生徒には事実を伝えず、家出をした生徒のみ個別指導を実施した。

家出をした女子生徒に対し保護者同伴のもと経緯の説明をさせた。

出会い系サイトの利用は犯罪に巻き込まれる危険性があることと、18 歳未満の者の出会い系サイト利用は法律で禁止されていることを伝え、二度と利用しないよう厳しく指導した。

◆今後の対策と効果

- ・今後、出会い系サイトの利用が凶悪犯罪などに発展する危険性があることや 18 歳未満の者の出会い系サイト利用はインターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律で禁止されていることなど実際の検挙事例を題材にした授業を技術家庭の中で行い、生徒が出会い系サイトを利用しないための指導を行っていく。

ブラウザクラッシャー

高等学校での事例

◆被害状況

- ・教員が学校のパソコンで Web サイトを閲覧中に、新規ブラウザが多数生成されるブラウザクラッシャーの Web ページに遭遇し、操作をしていた教員がブラウザクラッシャーについてあまり知識がなかったのでコンピュータウイルスに感染したと勘違いした。
- ・ブラウザクラッシャーによる大きな実害は発生していない。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・職員室にはネットワークに接続しているパソコンが設置しており、教員は自由に Web を閲覧することができる。

―校内のセキュリティ対策―

- ・学校のすべてのパソコンにウイルス対策ソフトを導入している。

◆発見の経緯

- ・発見方法：ブラウザクラッシャーに遭遇した教員の申し出により判明した。
- ・発生日時：平成 16 年 5 月頃
- ・発見日：平成 16 年 5 月頃
- ・事実確認：平成 16 年 5 月頃

◆被害への対応

―ブラウザクラッシャーに遭遇した教員への対応―

- ・対応日：平成 16 年 5 月頃
- ・対応担当者：情報担当教員
- ・対応方法：

情報担当教員がすぐにパソコンのところに駆けつけ、教員の話と実際の画面を見てウイルスではなく意図的に新規ブラウザが多数生成されるブラウザクラッシャーであることを説明した。

今後被害に遭わないために、信頼のおけない Web サイトでは安易にリンクやボタンをクリックしないよう注意するとともに、キーボードでの対応方法（Alt キーと F4 キーでブラウザを閉じる・Alt キーと Ctrl キーと Del キーでの強制終了）を紹介した。

◆今後の対策と効果

- ・今後、ブラウザクラッシャーに遭遇しないよう、ブラウザの不要な機能を使用しない設定にする方法を教職員に紹介した。
- ・完全な予防は困難なため、信頼のおけない Web サイトでは安易にリンクやボタンをクリックしないよう啓発を行った。

インターネット上での残虐映像の閲覧

高等学校での事例

◆被害状況

- ・イラク戦争時に、生徒達がインターネット上に公開されていた残虐な映像を学校のパソコンから閲覧していた。
- ・プロキシサーバによりフィルタリングの設定をしていたので、情報担当教員はそのような映像は閲覧できないと考えていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・生徒にとって有害と思われる Web サイトを排除するために、学校内に設置しているプロキシサーバを利用してフィルタリングを設定していた。

◆発見の経緯

- ・発見方法：映像を見ていた生徒が教員にも見せようとしたため判明した。
- ・発生日時：平成 16 年
- ・発見日：
- ・事実確認：情報担当教員も映像を生徒と一緒に閲覧して確認した。

◆被害への対応

－生徒への対応－

- ・対応日：映像を閲覧していたその日
- ・対応担当者：情報担当教員
- ・対応方法：

生徒は自宅のパソコンでインターネット上に公開されていた残虐な映像を閲覧していた。閲覧した生徒は友人にもインターネット上で映像が見られることを知らせたくて、学校のパソコンで閲覧を試みたところ、フィルタリングが設定されているにもかかわらず、映像を閲覧することができた。

イラク戦争時の残虐な映像は、テレビや新聞などのメディアでも多数報道されており、戦争について生徒たちに考えさせることが適切なことと判断し、その状況で戦争と平和について話をした。

◆今後の対策と効果

- ・現在は教育委員会のネットワークの下でインターネットに接続しているので、このケースは回避できると思われるが、制限がかかり過ぎて困る場合も多い。

フィルタリングソフトによる Web サイトの閲覧制限

高等学校での事例

◆被害状況

- ・進路指導の一環として大学生と対話する機会を設けた。時間内で話しきれないことも想定されたので、対話終了後はブログを利用して情報交換を行うことを検討していたが、学校のパソコンからブログへの書込みができなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・不特定多数からの書込みが可能な掲示板やブログは、書込み内容によってはトラブルが発生する可能性があるため、フィルタリングソフトを利用して、学校のパソコンから閲覧できないように制限をかけている。

◆発見の経緯

- ・発見方法：進路指導教員からの申し出。
- ・発生日時：平成 17 年
- ・発見日：
- ・事実確認：

◆被害への対応

－Web サイト閲覧の課題－

- ・対応日：
- ・対応担当者：進路指導教員、情報担当教員
- ・対応方法：

進路指導教員から依頼を受けた情報担当教員が当該ブログのみ閲覧可能な状況にするように試みたが、作業に時間がかかり過ぎたり、フィルタリングソフトの制限を抜けて別のブログが閲覧できてしまう可能性があるため、当該ブログを閲覧可能な状況にしなかった。

今回の取組みは、進路指導の一環として実施しているため、学校のパソコンから生徒に書込みをさせたいと考えていたが、フィルタリングソフトの制限により、やむを得ず、生徒の自己責任において携帯電話や自宅のパソコンから書込みを行うように指導した。

フィルタリングソフトによる制限も必要な面はあるが、教員の目が届くなかで、掲示板やブログに書込みする機会も必要と考えており、適切なフィルタリングの制限方法について検討している。

◆今後の対策と効果

掲示板への不適切な書込み被害 1

中学校での事例

◆被害状況

- ・生徒が個人で作成・運営している Web サイトの掲示板に、他の生徒が作成者を誹謗・中傷するような書込みを行った。
- ・書込みをされた生徒の掲示板はパスワードによる書込み制限を行っていたが、書込みを実施した生徒が、パスワードを不正に取得して書込みを実施していた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：Web サイトを運営している生徒からの申し出により判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：生活指導担当教員
- ・対応方法：
書込みを行った生徒を特定することができたので、生徒を呼び出し、他人のパスワードを勝手に利用してはならないこと、誹謗・中傷する書込みをしてはならないことを指導した。

◆今後の対策と効果

- ・技術家庭や総合的学習の時間を利用して Web サイトの利用方法や掲示板・電子メールのマナーなどの情報モラルについて指導を行っていく。

掲示板への不適切な書込み被害 2

中学校での事例

◆被害状況

- ・ある掲示板に、特定の生徒の名前を騙って、他の生徒の悪口が記載されていた。
- ・悪口を記載された生徒の友人がその書込みに反論する書込みを行い、掲示板サイト上で喧嘩状態になっていた。
- ・名前を騙られた生徒は掲示板に悪口を記載した事実はなく、名前を騙られたことによる精神的なショックを受けていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：名前を騙られた生徒の友人からの申し出により判明した。
- ・発生日時：平成 17 年 8 月
- ・発見日：平成 17 年 10 月
- ・事実確認：生徒からの申し出を受けた教員が名前を騙られた生徒本人に確認を行った。

◆被害への対応

－書込みへの対応－

- ・対応日：生徒からの申し出を受けた翌日
- ・対応担当者：情報担当教員
- ・対応方法：
 - 名前を騙られた生徒の友人と情報担当教員が該当の掲示板サイトの管理者に電子メールで削除依頼を行った。
 - 情報担当教員が削除依頼を行った翌日には書込みは削除された。

－生徒への対応－

- ・対応日：平成 17 年 10 月
- ・対応担当者：教頭、生徒の担任、情報担当教員
- ・対応方法：
 - 学年主任から学年集会で生徒に書込みがあった事実を伝え、当該掲示板サイトで書込み、並びに他の掲示板サイトにおいても誹謗・中傷の書込みを行わないように注意喚起した。

－名前を騙られた生徒への対応－

- ・対応日：平成 17 年 10 月
- ・対応担当者：担任教員
- ・対応方法：
 - 名前を騙られた生徒には該当の掲示板の書込みをすべて削除したことを伝え、学年全体に同じことが起こらないように指導することを連絡した。
 - また、名前を騙られた生徒の保護者にも、掲示板の書込みを削除したことと学年集会で生徒に注意喚起を行ったことを連絡した。

◆今後の対策と効果

- ・その後、該当の掲示板で誹謗・中傷する書込みは確認されていない。

掲示板への不適切な書込み被害 3

高等学校での事例

◆被害状況

- ・生徒が趣味で作成したWebサイトが有名掲示板で紹介され、その情報をもとにWebサイトを訪れた者など不特定の者からWebサイト訪問後の感想などとして有名掲示板で誹謗・中傷されるに至った。
- ・Webサイトは、生徒の友人も存在を知っており、誹謗・中傷について知り合いが含まれているのではないかと疑心暗鬼になっており、また場合によっては生徒を知る者が氏名など個人を特定できるような個人情報の書込みをするのではないかと不安になり相談された。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：
- ・対応方法：

個人情報が書込みされなかったため具体的な対応をとるに至っていないが、状況によっては掲示板運営者への個人情報削除依頼、Webサイトの閉鎖、警察への相談などの対応が必要であった。

その後、生徒がWebサイトのアドレスの変更、有名掲示板での書込みの沈静化によって一応の収束となり、その後もトラブルには至っていない。

◆今後の対策と効果

掲示板への不適切な書込み被害 4

高等学校での事例

◆被害状況

- ・ある掲示板に学校名を冠としたスレッドが立ち、そのスレッドに生徒個人を誹謗・中傷する書込みとともに、生徒の実名が公表された。
- ・書込みの内容から同級生による書込みと推測できたが、学校外のパソコンから書込みが行われており、掲示板に書込みをした人物を特定することはできなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・パソコン教室は LAN 環境が整備されており、インターネットの利用は可能となっている。
- ・コンテンツフィルターをかけている。

ー校内のパソコン利用状況や利用形態ー

- ・パソコン教室の授業時以外の利用は禁止している。

◆発見の経緯

- ・発見方法：実名を公表された生徒の保護者が掲示板の書込みを発見し、学校に連絡して判明した。
- ・発生日時：平成 16 年 11 月
- ・発見日：書込みがされた翌日
- ・事実確認：保護者からの連絡を受け、教員が該当掲示板の書込みを確認。

◆被害への対応

ー書込みをされた生徒への対応ー

- ・対応日：保護者からの連絡を受けた翌日
- ・対応担当者：クラス担任教員と校長
- ・対応方法：保護者を通じて、事実確認と全校生徒へ指導する旨を連絡した。

ー全校生徒への指導ー

- ・対応日：書込み事実の確認から 1 週間後
- ・対応担当者：全教員
- ・対応方法：全校集会にて、校長から掲示板に個人名を明記して誹謗・中傷する書込みが行われた事実を伝え、気持ちの良い学校生活を送るためにも、同じ事態を起こさないよう生徒に訓示を行った。

◆今後の対策と効果

- ・その後、当該掲示板への書込みは減少した。

掲示板への不適切な書込み被害 5

高等学校での事例

◆被害状況

- ・ある掲示板に学校名を冠としたスレッドがあり、生徒個人を特定できる書込みや誹謗・中傷する書込みが多く記載されていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの連絡により判明した。
- ・発生日時：平成 17 年 1～3 月
- ・発見日：平成 17 年 1 月
- ・事実確認：該当の掲示板を複数の教員で閲覧して確認した。

◆被害への対応

ー書込みへの対応ー

- ・対応日：生徒の連絡から 2・3 日後
- ・対応担当者：情報担当教員を含む複数（3～4 名）の教員
- ・対応方法：
該当の掲示板を複数の教員で確認し、書込み内容から個人を特定できるか否かまた個人を誹謗・中傷している内容か否かを協議した。
個人を特定できるものと個人を誹謗・中傷していると判断した書込みについては、学校より掲示板の運営者に対し文書にて削除依頼を行った。
数日後、協議をおこなった複数の教員が該当の掲示板を閲覧し、書込みの削除状況を確認したところ、削除依頼をした書込みの 60%程度しか削除されておらず、残りの 40%程度は削除されていなかった。

◆今後の対策と効果

- ・書込みは継続して行われているが、以前に書込まれていた内容がある程度削除されていた効果もあり、生徒個人を特定できる書込みや誹謗・中傷する書込みの件数は減っている。

掲示板への不適切な書込み被害 6

高等学校での事例

◆被害状況

- ・無料で掲示板を設置できるサイトに学校名を冠としたスレッドができ、その中で生徒個人を誹謗・中傷する書込みや教員・学校に対しての批判的な書込みなどが大量にされていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの申し出により判明した。
- ・発生日時：平成 15 年
- ・発見日：平成 15 年
- ・事実確認：当該掲示板を教員が閲覧して確認した。

◆被害への対応

ー 掲示板の書込みへの対応 ー

- ・対応日：
- ・対応担当者：
- ・対応方法：

複数の教員が掲示板の利用規約・運用規約と掲示板内の書込み内容を確認し、利用規約・運用規約に反する書込みが多くされていると判断し、学校から文書にて掲示板運営者に掲示板そのものの閉鎖依頼を行った。

閉鎖依頼を行ってから数日後、該当の無料で掲示板を設置できるサイトを確認したところ、該当のスレッドは削除されていた。

◆今後の対策と効果

- ・現在は学校のパソコンから掲示板への書込みができないようフィルタリングをかけており、生徒は自宅のパソコンや携帯電話を利用して掲示板に書込みをしていると推測される。学校からの書込みが行われなからよいのではなく、インターネット上のマナーやモラルを守って掲示板を利用するように授業を通じて指導をしている。

掲示板への不適切な書込み被害 7

高等学校での事例

◆被害状況

- ・インターネット上のいくつかの掲示板サイトに学校名を冠とするスレッドが多数存在しており、生徒・教員・学校を誹謗・中傷する書込みが行われている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：教員が定期的に掲示板を閲覧している。
- ・発生日時：平成 15 年～
- ・発見日：
- ・事実確認：

◆被害への対応

－書込みへの対応－

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

情報担当教員が生徒や教員を特定できる書込みや誹謗・中傷する書込みの有無を 2～3 ヶ月に 1 回チェックしている。

書込みを発見した場合は、管理職に報告を行い、掲示板の運営者が判明している場合は、管理職を通じて掲示板の運営者に書込みの削除依頼を行っている。

削除依頼を実施した後は、該当の書込みが削除されたか確認を行っている。

◆今後の対策と効果

- ・平成 17 年度から、学校のパソコンのインターネット環境が教育委員会ネットワークの管理下に置かれ、学校内のパソコンから掲示板を閲覧することができなくなったので、学校のパソコンから不適切な書込みをチェックすることが難しい状況となった。現在は、自宅のパソコン等を利用してチェックしている状況である。

掲示板への不適切な書込み被害 8

高等学校での事例

◆被害状況

- ある女子生徒が友人の女子生徒の携帯電話番号を不適切なメッセージとともに掲示板に書込みした。
- 携帯電話番号を書込まれた女子生徒の携帯電話には、頻繁に卑猥な電話がかかってくるようになった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- 発見方法：書込みをされた女子生徒の保護者からの連絡により判明した。
- 発生日時：
- 発見日：
- 事実確認：

◆被害への対応

－書込みへの対応－

- 対応日：
- 対応担当者：書込みをされた生徒の保護者
- 対応方法：

書込みをされた女子生徒は保護者と相談し、保護者から携帯電話番号が記載された掲示板に書込みの削除依頼を行った。あわせて、警察にも相談を行った。

書込みがあった原因は生徒同士での喧嘩で、喧嘩をした相手の生徒がいたずら目的で書込みをしたものと判明した。

書込みを行った生徒も反省している様子だったので、警察へ被害届けを提出することは控えた。

－学校の対応－

- 対応日：
- 対応担当者：生活指導担当教員
- 対応方法：

保護者から連絡で初めて事態を把握した。

書込みをした生徒から事実の確認を行い、同じことを行わないように個別指導を実施した。

◆今後の対策と効果

掲示板への不適切な書込み被害 9

高等学校での事例

◆被害状況

- ・ 掲示板サイトに学校名を冠としたスレッドがあり、スレッド内で生徒や教員を誹謗・中傷する書込みがあった。書込みの中には、教員の実名を記載しているものもあった。
- ・ 生徒や教員を誹謗・中傷する書込みや教員の実名入りの書込みは、書込み内容から生徒によるものと判断できた。
- ・ 掲示板管理者に書込みの削除を求めたところ、運営方針により一部の書込みが削除されずに残ってしまった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：掲示板を見た人物から学校に連絡があり判明した。
- ・ 発生日時：平成 17 年 7 月
- ・ 発見日：平成 17 年 7 月
- ・ 事実確認：

◆被害への対応

—書込みへの対応—

- ・ 対応日：平成 17 年 8 月
- ・ 対応担当者：情報担当教員
- ・ 対応方法：

掲示板の書込みについて、学校より掲示板の運営者に電子メールで削除依頼を行ったが、一部の書込みしか削除されなかった。

掲示板の運営者の見解としては次のとおりであった。

 - ①生徒や教員を誹謗・中傷する書込みについては、学校関係者であれば個人を特定することは可能だが一般の利用者からは特定できないので削除しない。
 - ②教員の実名入りの書込みについては、学校の教員を公人として扱っている。公人であれば実名のみだけの書込みは削除しない。

—書込みをした生徒への対応—

- ・ 対応日：平成 17 年 8 月
- ・ 対応担当者：情報担当教員
- ・ 対応方法：

書込み内容から書込みをした生徒を特定し生徒本人に個別に事実確認を行ったところ、掲示板への書込みを認めた。書込みをした生徒は 5 名で、全員に個別指導を行った。

誹謗・中傷する書込みをされた生徒がその掲示板を見ていない可能性があるため、全生徒に対して今回の経緯を説明することは控えている。

◆今後の対策と効果

- ・ 書込みの削除についてすべてが削除されないこともあるため、生徒への掲示板書込みについての指導を徹底することが課題となっている。

掲示板への不適切な書込み被害 10

高等学校での事例

◆被害状況

- ・生徒が掲示板で構成された Web サイトを立ち上げたが、あるときから偽りの情報や誹謗中傷などが書き込まれるようになってしまい、さらには書き込みをした個人を特定しようとする犯人探しの荒れ方に至った。
- ・個人に対する実名をあげた誹謗中傷や荒れ方から今後、書き込みをした犯人を呼び出そうといった現実の暴力行為などを危惧し、対応を迫られることとなった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 17 年 5 月中旬
- ・発見日：平成 17 年 6 月
- ・事実確認：

6 月中旬頃、教員がたまたま耳にした生徒の会話から主に携帯電話からのアクセス利用による（PC 利用も可）生徒が運営していると思われる学校をテーマとした Web サイトの存在が明らかになった。Web サイトは 5 月中旬に作成されたようで、複数のフリー掲示板によって構成されており、誹謗中傷の書き込みや実名の書き込みも確認された。主に 1、2 年生の利用が中心となっており、口伝えで利用が広まっていったことが確認された。

◆被害への対応

ー生徒への対応ー

- ・対応日：平成 17 年 7 月
- ・対応担当者：
- ・対応方法：

生徒への事情聴取を行い、誹謗中傷された生徒はこの掲示板の削除を望んでいることもあり、また、学校名、実名の掲載があることと、夏休みを控えており生徒指導の機会を失うこともあって緊急性ありと判断。サイト管理者に校長名で掲示板の削除依頼を電子メールで行った。結果、2 日後には掲示板が削除された。

なお、同時期に生徒に対してインターネット利用に関するアンケート調査を実施した。教育効果も兼ねるもので、利用実態調査とともに、例えば、利用者を特定できること、ファイル交換ソフトの違法性、掲示板トラブルの違法性などの確認を行うものとした。（別掲）

◆今後の対策と効果

- ・今回の一連の対応には、生徒指導部、人権委員会、情報教育推進委員、情報担当者、管理職がさまざまに関連するケースであり、教員の現状認識や問題意識の差も露呈している。このため、こうした問題に対応する組織づくりや教員の研修実施なども課題として取り組むこととした。

掲示板への不適切な書込み被害 1 1

高等学校での事例

◆被害状況

- ・ 掲示板に生徒の実名とともに生徒を誹謗・中傷する書込みがされていた。
- ・ 誹謗・中傷の書込みをされた生徒は、どのように対処すべきか担任教員に相談をしてきた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：誹謗・中傷された生徒本人からの相談により判明した。
- ・ 発生日時：平成 17 年
- ・ 発見日：
- ・ 事実確認：

◆被害への対応

－生徒への対応－

- ・ 対応日：
- ・ 対応担当者：担任教員
- ・ 対応方法：
書込みされた内容に反論する書込みを行うと事態が悪化するケースが多いので、書込みに対しては無視するようにアドバイスした。
あわせて、学校から掲示板運営者に削除依頼を行うことも伝えた。

－掲示板への対応－

- ・ 対応日：
- ・ 対応担当者：担任教員
- ・ 対応方法：
掲示板運営者に学校名で削除依頼を実施した。
後日、掲示板を確認したところ、削除依頼していた書込みはすべて削除されていた。
その後、該当の掲示板での実名入りで生徒を誹謗・中傷する書込みは行われていない。

◆今後の対策と効果

- ・ 掲示板に関するトラブルは、誹謗・中傷を書込まれた本人もしくはその友人が教員に相談して発見されるケースがほとんどである。今回の件以外にも生徒が掲示板で誹謗・中傷の書込みをされているケースはあると思うが、実態を把握できない。
- ・ 生徒を誹謗・中傷する書込んだ犯人を特定できないが、書込みの内容から多くの場合が同じ学校の生徒によるものと推測できるので、生徒に対して個人を誹謗・中傷の書込みを行わないための効果的な指導方法を検討している。

掲示板への不適切な書込み被害 1 2

高等学校での事例

◆被害状況

- ・ 掲示板に生徒の実名を明記した上で、その生徒を誹謗・中傷する書込みが記載されていた。
- ・ 誹謗・中傷の書込みをされた生徒は精神的にショックを受けていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：書込みをされた生徒からの相談により判明した。
- ・ 発生日時：平成 17 年 5 月頃
- ・ 発見日：平成 17 年 5 月頃
- ・ 事実確認：

◆被害への対応

ー書込みをされた生徒への対応ー

- ・ 対応日：相談があったその日
- ・ 対応担当者：情報担当教員
- ・ 対応方法：

掲示板の書込みは学校から削除依頼を行うことを伝え、しばらく様子を見ることにした。

ー掲示板への対応ー

- ・ 対応日：平成 17 年 9 月頃
- ・ 対応担当者：情報担当教員
- ・ 対応方法：

生徒からの相談を受け、すぐに当該の掲示板の確認を行った。

学校のパソコンは Web フィルタリングを導入しているため早急に該当の掲示板を確認することができなかったため、情報担当教員の自宅のパソコンを利用して掲示板の確認を行った。

書込みを確認し、掲示板の削除方法を確認した上で、学校の代表電子メールアドレスから掲示板運営者にメールにて削除依頼を行った。

数日後、掲示板の書込みが削除されたことを確認した。

なお、書込みをした人物の特定はできなかった。

◆今後の対策と効果

- ・ 誹謗・中傷の書込みが削除されてから該当の掲示板での書込みが沈静化し、生徒を誹謗・中傷する書込みは確認されていない。

掲示板への不適切な書込み被害 1 3

高等学校での事例

◆被害状況

- ・ある掲示板に学校名を冠としたスレッドが立ち上がっていた。
- ・スレッド内には、個人名は記載されていないが、学校の関係者が閲覧すれば人物を特定できる内容で誹謗・中傷する書込みがされていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談により判明した。
- ・発生日時：平成 17 年
- ・発見日：
- ・事実確認：教員が掲示板を閲覧して確認した。

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：

書込んだ生徒の特定はできないが、書込みをする生徒の多くは、いたずら書き感覚で誹謗・中傷の書込みをしている。

生徒が特定できないので、各クラスのホームルーム時に、担任教員から掲示板に誹謗・中傷の書込みをしないように指導している。

誹謗・中傷を書込まれた生徒には、誹謗・中傷の書込みに対して反論する書込みをしないように指導している。

◆今後の対策と効果

- ・掲示板への不適切な書込みトラブルは、生徒が掲示板に誹謗・中傷を書込む行為を安易に考えているために発生するケースが多い。インターネット上に書込みをすると簡単に情報を削除することができないことを伝え、誹謗・中傷を書込まないように指導することとした。

掲示板への不適切な書込み被害 1 4

高等学校での事例

◆被害状況

- ・携帯電話のみ閲覧と書込みが可能な掲示板に、特定の生徒の氏名と学校名を明記し、その生徒を誹謗・中傷する書込みがあった。
- ・誹謗・中傷の書込みをされた生徒は精神的にショックを受けていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：書込みをされた生徒からの相談により判明した。
- ・発生日時：平成 17 年 9 月頃
- ・発見日：平成 17 年 9 月頃
- ・事実確認：

◆被害への対応

－書込みをされた生徒への対応－

- ・対応日：相談があったその日
- ・対応担当者：生活指導担当教員・情報担当教員
- ・対応方法：

掲示板の書込みは学校から削除依頼を行うことを伝えた。

あわせて、サイバー犯罪に関する相談・問い合わせ先として、神奈川県警ハイテク犯罪対策センターがあることを紹介した。

－掲示板への対応－

- ・対応日：平成 17 年 9 月頃
- ・対応担当者：情報担当教員
- ・対応方法：

携帯電話専用の掲示板だったため、学校のパソコンから掲示板の書込みは確認できなかったため、教員の携帯電話を利用して書込みを確認した。

書込みをされた生徒も削除依頼をしていたが、書込みが削除されていなかったため、掲示板の運営者に学校長名で文書による削除依頼を行い、数日後に書込みは削除された。

◆今後の対策と効果

- ・削除依頼を実施し、該当の書込みが削除されてから、徐々に当該のスレッドでの書込みそのものの件数が減少し、生徒の申し出から 3 ヶ月後くらいには事態は沈静化した。
- ・沈静化してから、生徒を誹謗・中傷する書込みは行われていない。

掲示板への不適切な書込み被害 15

高等学校での事例

◆被害状況

- ・携帯電話を利用して閲覧できる掲示板サイトに、学校名を冠としたスレッドがあり、その掲示板に個人名を明記した上で誹謗・中傷する書込みがあった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：誹謗・中傷を書込まれた生徒からの相談により判明した。
- ・発生日時：平成 17 年 6 月
- ・発見日：
- ・事実確認：

◆被害への対応

―書込みされた生徒への対応―

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

掲示板のトラブルに対する指導の一環として、書込みされた生徒に、掲示板の削除ガイドラインを確認し、生徒本人から削除依頼を出すように指導した。

―全生徒への対応―

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

全生徒に対して、掲示板を利用する際には個人名を含む個人情報や個人を誹謗・中傷する内容の書込みを行わないように注意した。

◆今後の対策と効果

- ・その後、書込みは確認されていない。

掲示板への不適切な書込み被害 16

高等学校での事例

◆被害状況

- ・ 個人が管理する学校名を冠した携帯電話専用の掲示板に、複数の生徒の誹謗・中傷が実名つきで書込まれた。
- ・ 誹謗・中傷を書込まれた生徒達はショックを受け、学校を休みがちになったり、学校を辞めた者もいた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：誹謗・中傷を書込まれた生徒からの相談により判明した。
- ・ 発生日時：平成 17 年
- ・ 発見日：
- ・ 事実確認：被害生徒の担任教員が掲示板を閲覧して確認した。

◆被害への対応

－生徒への対応－

- ・ 対応日：
- ・ 対応担当者：被害生徒の担任教員
- ・ 対応方法：

書込みをした人物は特定できなかったが、書込みの内容から同じクラスの生徒の書込みと推測できたので、担任教員がホームルームの時間にインターネット上で誹謗・中傷をせずに、マナーを守って利用するように指導を行った。また、同学年でも同じ掲示板を利用している生徒がいると考えられたので、学年集会で同様の指導を行った。

指導後、実名を挙げての誹謗・中傷の件数は減少したものの完全にはなくならなかったため、誹謗・中傷を注意する書込みを担任教員が当該掲示板に行った。

担任教員からの書込み以降、当該掲示板において、誹謗・中傷の書込みはなくなった。

◆今後の対策と効果

- ・ 当該掲示板において、誹謗・中傷の書込みはなくなったものの、他の掲示板においても同様のケースが想定されるので、今後情報の授業で情報モラルを重点的に扱い、生徒を指導していく。
- ・ 他の高校と連携し、情報モラルの効果的な教材を検討していく。

掲示板への不適切な書込み被害 17

高等学校での事例

◆被害状況

- ・個人が運営している Web サイト内の掲示板に複数の生徒が学校のパソコンから掲示板の設置趣旨にそぐわない内容の書込みをした。
- ・生徒の書込みを閲覧した他の利用者から掲示板運営者に対して苦情が寄せられた。
- ・苦情が寄せられた掲示板運営者は、書込み元の IP アドレスを調査し、教育委員会ネットワークからの書込みであることが判明したので、教育委員会に直ちに書込みを停止するように依頼した。
- ・当該掲示板は、生徒の書込みが原因となり閉鎖することとなった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：教育委員会からの連絡を受けて判明した。
- ・発生日時：平成 17 年 5 月
- ・発見日：
- ・事実確認：

◆被害への対応

ー生徒への対応ー

- ・対応日：平成 17 年 5 月
- ・対応担当者：情報担当教員
- ・対応方法：

教育委員会からの連絡後、校内のプロキシサーバを調査し、書込みを行ったパソコンが判明し、その時間にパソコンを利用していた目撃情報から書込みをした複数の生徒が特定された。

書込みした複数の生徒へは、書込みが原因で当該掲示板が閉鎖したことを伝え、掲示板に書込む際は、書込みのルールやマナーを守って利用するように指導した。

また、掲示板への書込みに利用したパソコンは、進路指導室に設置しているパソコンであり、進路指導室に設置しているパソコンは、生徒が進路を調査する際に利用することを目的として設置したパソコンだったので、学校で定めているルールを守って利用するようにあわせて指導した。

◆今後の対策と効果

- ・その後、フィルタリング機能が強化されたこともあり、学校のパソコンから掲示板への書込みは発生していない。

掲示板への不適切な書込み被害 18

高等学校での事例

◆被害状況

- ・情報の授業中、ある生徒が掲示板に公序良俗に反する文言を大量に、100回以上書込んだ。
- ・掲示板運営者が書込み元のドメインを調査したところ、教育委員会ネットワークからの書込みであることが判明し、教育委員会に直ちに書込みを止めさせるよう連絡した。
- ・教員は、教育委員会によってフィルタリングがかけられているので、学校のパソコンから掲示板を閲覧できないと考えていたが、今回のケースでは、フィルタリングの網を抜けて書込みをしていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・教育委員会によって、ネットワークが一元管理されており、当該ネットワークからアクセスできる Web サイトは限られている。
- ・生徒一人一人にユーザ ID とパスワードを付与し、生徒が閲覧した Web サイトのアクセス記録をつけている。

◆発見の経緯

- ・発見方法：掲示板運営者の連絡を受けた教育委員会がログを調査し、書込みを行った日時、学校名、使用されたパソコンを特定した。
- ・発生日時：平成 17 年 6 月頃
- ・発見日：
- ・事実確認：

◆被害への対応

—書込みを行った生徒への対応—

- ・対応日：平成 17 年 6 月頃
- ・対応担当者：情報担当教員
- ・対応方法：
教育委員会からの連絡を受けた情報担当教員が、校内サーバのログを調査し書込みを行った生徒を特定した。
後日、情報担当教員が書込みを行った生徒に対し、インターネット上で公序良俗に反する書込みを行ってはならないと指導した。

◆今後の対策と効果

- ・書込みを行った生徒が、学校のパソコンを利用して掲示板に書込むことは行われていない。

画像掲示板への投稿被害

高等学校での事例

◆被害状況

- ・成人向けの画像掲示板に、学校の制服を着ている女性の画像が投稿されていた。投稿されていた画像の制服と記載されていたコメントから学校名が特定できるものであった。
- ・投稿された画像の顔は不明瞭だったので、在校生か否かの確認はできなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：ある機関からの連絡により判明した。
- ・発生日時：平成 17 年
- ・発見日：
- ・事実確認：ある機関からの連絡を受け、コンピュータ委員会と生徒指導課の教員が当該掲示板サイトに掲載されていることを確認した。

◆被害への対応

ー掲示板への対応ー

- ・対応日：ある機関からの連絡を受けたその日
- ・対応担当者：校内分掌で定められたコンピュータ委員会と生徒指導課の教員
- ・対応方法：
コンピュータ委員会と生徒指導課の教員が当該掲示板サイトを確認し、削除依頼方法を確認した。
掲示板の削除依頼方法に則り、掲示板サイト運営者に削除を依頼した。
削除依頼をした翌日には画像とコメントは削除されていた。
削除が確認されてからも毎日該当の掲示板サイトを閲覧し、同じような投稿がされていないか確認することとした。

◆今後の対策と効果

- ・投稿者を特定することは困難である。該当の画像掲示板にいつ画像が公開されるかわからないので、コンピュータ委員会の教員が該当の画像掲示板を定期的に確認することとした。
- ・その後、当該の画像掲示板には、学校が特定できるような画像は公開されていない。

掲示板や個人所有 Web サイトでの誹謗・中傷

高等学校での事例

◆被害状況

- ・生徒が特定の生徒を本人の知らないところで携帯電話のカメラで撮影し、本人の許可なく画像を公開できる掲示板や生徒個人が運営する Web サイトに誹謗・中傷する内容のコメントとともに掲載した。
- ・掲載された生徒は、掲示板や Web サイト上で生徒本人の画像とともに誹謗・中傷されていることは知らなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：Web サイトを閲覧した他の生徒からの申し出により判明した。
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

ー公開された画像への対応ー

- ・対応日：相談があったその日
- ・対応担当者：情報担当教員
- ・対応方法：

掲示板に掲載してある画像や書込みについては、掲示板の運営者に対して学校側から削除依頼を行った。

生徒個人が運営する Web サイトに掲載されている画像やコメントは、運営している生徒本人と個別に話し合いを行い、削除するよう注意を行った。

◆今後の対策と効果

- ・生徒個人が運営する Web サイトに記載している画像やコメントについて、教員から内容や画像の変更・削除を強制することができない。個別の話し合いを行い、生徒に変更・削除するように促すことしかできず対応に苦慮している。

掲示板荒らし行為

高等学校での事例

◆被害状況

- ・ 掲示板運営者から学校の IP アドレスから掲示板の運営を妨害するような書込みがあると連絡があり、生徒に対して適切な指導を行うよう要望があった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

- 校内のパソコン環境 —
 - ・ 校内 LAN を経由して Web サイトの閲覧が可能となっている。
- 校内のパソコン利用状況や利用形態 —
 - ・ 休み時間も教員に許可をもらえば自由にパソコン教室を利用できる。

◆発見の経緯

- ・ 発見方法：掲示板運営者からの連絡により判明した。
- ・ 発生日時：
- ・ 発見日：
- ・ 事実確認：

◆被害への対応

- 生徒への対応 —
 - ・ 対応日：事実判明から 1 週間
 - ・ 対応担当者：情報担当教員
 - ・ 対応方法：
 - 学校内の掲示板に、掲示板荒らしの経緯を説明する内容の掲示を行い、事実関係を生徒に伝えた。
 - 情報の授業時に掲示板やチャットからの書込みのマナーやログが残ることを説明した。

◆今後の対策と効果

- ・ 「情報」の授業の早い時期で、掲示板やチャットのマナーについて紹介する授業を実施し、ルールを守って利用するよう指導を実施することとした。
- ・ 今後同じようなことが発生した場合にはフィルタリングソフトを導入し、掲示板やチャットへのアクセス制限を行うこととした。

不適切な画像を利用してのイベント広報

高等学校での事例

◆被害状況

- ・生徒が学校で開催するイベント案内を画像が掲載できる掲示板に不適切な画像とともに書込みを行っていた。
- ・掲示板を閲覧した人から学校に連絡があり、学校のイベントを広報する方法としては行き過ぎているから指導したほうがよいという要望があった。
- ・書込みは家のパソコンから行われていた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：掲示板を閲覧した人からの連絡により判明した。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

ー生徒への対応ー

- ・対応日：事実判明日
- ・対応担当者：クラス担任・学年担当教員
- ・対応方法：
当該情報を掲載したと思われる生徒を呼び出し、画像と書込みを削除するように指導した。

◆今後の対策と効果

- ・インターネットマナーや情報モラルについての授業を入学時に実施することとした。

掲示板の書込みに対する捜査協力

高等学校での事例

◆被害状況

- ・学校のパソコンを利用して掲示板に人の生死に関係する書込みが行われ、書込みが原因で警察が捜査するという事態に発展した。
- ・警察は書込みが行われたプロバイダとプロバイダを利用している複数の学校のうちの1校からの書込みというところまで特定していた。
- ・学校の特定には至っていなかったため、教育委員会を通じて、該当のプロバイダを利用している複数の学校に捜査協力依頼があった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・校内の生徒用パソコンからインターネットが利用できる。

◆発見の経緯

- ・発見方法：掲示板を閲覧していた一般の人から警察に通報があり、警察の捜査で判明した。
- ・発生日時：平成 15 年
- ・発見日：平成 15 年
- ・事実確認：

◆被害への対応

―捜査協力依頼への対応―

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

警察から提示された日時と掲示板の URL を元に、情報担当教員が学校のプロキシサーバのログ調査を実施した。ログには、警察から提示された日時に該当の掲示板への書込みを示す結果は残されていなかったため、その旨を教育委員会に報告した。

ログの結果から、当校からの書込みではなかったことが判明した。

◆今後の対策と効果

- ・現在は、フィルタリングソフト等を利用して学校のパソコンから掲示板への書込みを制限しているため、学校のパソコンを利用した不適切な書込みは行われていない。

無停電電源装置の故障によるサーバのダウン

高等学校での事例

◆被害状況

- ・パソコン教室のサーバに設置されている無停電電源装置（UPS）が故障し、サーバがダウンし、ネットワークが一時的に利用できなくなった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

－校内のパソコン環境－

- ・校内 LAN が導入されている。

－校内のパソコン利用状況や利用形態－

- ・授業で作成したファイルは、教員の指示で、サーバ上に保存する。

◆発見の経緯

- ・発見方法：授業中にパソコン教室内のパソコンが次々にロックしたため判明した。
- ・発生日時：平成 16 年 9 月頃
- ・発見日：平成 16 年 9 月頃
- ・事実確認：平成 16 年 9 月頃

◆被害への対応

－停止したサーバへの対応－

- ・対応日：サーバがダウンした当日
- ・対応担当者：情報担当教員
- ・対応方法：

サーバの電源を UPS から切り離し、直接コンセントから電源を確保した。

◆今後の対策と効果

- ・今後、UPS を新しいものに交換する予定。

大量パケット送信（攻撃）による Web サーバのダウン

高等学校での事例

◆被害状況

- ・授業中に突然 Web サイトが閲覧できなくなった。教員が校内の Web サーバを確認しところ原因はわからなかったが、サーバがダウンしていた。直ちにサーバを再起動し Web サイト、は閲覧できたが、しばらくすると再びサーバがダウンした。
- ・当面は、サーバがダウンしたら情報担当教員がサーバを再起動することで対応した。
- ・1ヶ月ほど様子を見たが、状況が改善されなかったので業者に調査を依頼した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：ルータの不備により、ルータが踏み台となってサーバを攻撃していることが業者の調査により判明した。
- ・発生日時：平成 16 年
- ・発見日：サーバがダウンするようになってから 1 ヶ月後
- ・事実確認：業者の調査により事実を確認。

◆被害への対応

ーネットワークへの対応ー

- ・対応日：サーバがダウンするようになってから約 2 ヶ月
- ・対応担当者：情報担当教員
- ・対応方法：

Web サーバが頻繁にダウンするようになった当初は、情報担当教員がその都度サーバを再起動して対処していた。

ハードディスクスキャンなど情報担当教員ができるメンテナンスを行い、1ヶ月間様子を見たが、状況は改善されなかったため、業者に調査を依頼した。

調査を依頼してから 10 日後、ルータの不備により、ルータが踏み台となってサーバを攻撃していることが判明した。

状況を改善するために使用しているルータの機種を変更した。

◆今後の対策と効果

- ・ルータを変更してから Web サーバがダウンすることはなくなった。

複数の DHCP サーバによる接続障害

専門学校での事例

◆被害状況

- ・授業のなかでネットワーク接続を開始したところ、ネットワークにつながらないパソコンが発生し、授業を進めることができなくなった。
- ・原因を調べたところ、ネットワーク上に正規の DHCP サーバとは別の DHCP サーバ（特別授業で使用）が動いており、つながらないパソコンはそのサーバから IP アドレスを割り振られていたことがわかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン利用状況ー

- ・校内のパソコンはネットワークでつながっている。
- ・ネットワーク内のパソコンは、IP アドレスを自動で割り振る DHCP サーバを使用している。

◆発見の経緯

- ・発見方法：つながらないパソコンの IP アドレスを調べたところ、校内で使用している IP アドレスとは違う IP アドレスが設定されていた。
- ・発生日時：平成 16 年 9 月
- ・発見日：同日
- ・事実確認：同日

◆被害への対応

ーサーバへの対応ー

- ・対応日：被害発生日
- ・対応担当者：担当教員
- ・対応方法：正規以外の DHCP サーバをとめた。

◆今後の対策と効果

- ・サーバ系のマシンは基本的にネットワークにつなげないように教職員間で確認をした。
- ・授業によりサーバ系のマシンをネットワークにつなげる場合、今回は自動的にプログラムが起動する設定となっていたために起こった事故でもあるので動作していないか確認するようになった。

※DHCP

ネットワークのパソコンに対して、自動で IP アドレスを設定するプロトコル

物理的な LAN ケーブルのショート

高等学校での事例

◆被害状況

- ・ 休み時間になるとネットワークが繋がらなくなるため、調査したところ床下に通している LAN ケーブルがフロアユニットの足に踏まれていたため、その上を人が通るとショートして通信ができなくなっていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・ 通常の教室の床を上げ、ネットワークケーブル等を配線できるようにしてある。

◆発見の経緯

- ・ 発見方法：生徒からの申し出を教員が確認。
- ・ 発生日時：平成 16 年 6 月頃
- ・ 発見日：平成 16 年 6 月頃
- ・ 事実確認：平成 16 年 6 月頃

◆被害への対応

ーLAN ケーブルへの対応ー

- ・ 対応日：被害発生日
- ・ 対応担当者：担当教員
- ・ 対応方法：
教員が LAN ケーブルを交換し、フロアユニットの足に踏まれないように配線しなおした。

◆今後の対策と効果

- ・ 授業中に生徒に対して、本件を紹介しソフトの不都合だけでなく、単純なハードの障害でネットワーク障害が起こることを説明した。

ネットワークケーブルの配線ミス

高等学校での事例

◆被害状況

- ・ネットワークシステムの移行期に校内の LAN 配線を業者に委託したところ、生徒が利用するパソコン教室からインターネットの利用ができなくなってしまった。パソコンの設定に問題はなかったのでネットワークシステムの管理元と連絡をとり配線図を確認したところ、業者が敷設した LAN 配線にミスがあることが判明した。
- ・ネットワークシステムの移行期で授業は実施していなかったため、インターネットが利用できないことによる実害は発生していない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：インターネットが利用できなかったため、事務室に保管してある配線図を利用し、教員が校内を確認して配線ミスが判明した。
- ・発生日時：平成 17 年
- ・発見日：
- ・事実確認：

◆被害への対応

ー配線ミスへの対応ー

- ・対応日：平成 17 年
- ・対応担当者：情報担当教員
- ・対応方法：
配線ミスを確認したので、県への教育委員会ネットワーク接続については、県の方でサーバの設定を現状に合致した設定に変更し、配線業者には正しい配線図を作成し、直させた。

◆今後の対策と効果

ネットワークコマンドの誤利用によるウイルス騒ぎ

専門学校での事例

◆被害状況

- ・授業中、学生AおよびBがコマンドプロンプトから相手にメッセージを送信するコマンドで会話をしていたところ、あるタイミングで送信相手を全員に設定して送信してしまったため、ネットワークに接続されているパソコン全部にメッセージが表示されてしまった。
- ・授業中であったため、ネットワークに接続しているパソコンは相当数あり、ふしぎなコメントが突然画面に表示されたことでウイルスに感染した画面と勘違いするなど学生が騒ぎだし、授業が中断する騒ぎとなった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン利用状況―

- ・WindowsXPで授業を行っている。
- ・全てのパソコンはLANに接続されている。

◆発見の経緯

- ・発見方法：学生からの申し出。
- ・発生日時：平成16年5月頃
- ・発見日：同日
- ・事実確認：同日

◆被害への対応

―学生への対応―

- ・対応日：被害発生日
- ・対応担当者：担当教員
- ・対応方法：
表示されたメッセージはウイルスではないと、学生に説明し騒ぎを収束させた。
また、誤った操作をした学生に対しては、コマンドの使用方法をよく理解した上で利用するよう指導したが、授業時間内に使用すべきコマンドではないことも厳しく指導した。

◆今後の対策と効果

- ・その後、同じような事故は起こっていない。

不用意なダウンロードによるネットワーク回線速度の低下

専門学校での事例

◆被害状況

- ・教員が外部ネットワークにつなげ業務をしていたが、ある日突然つながりが遅くなった。
- ・調べたところ、ある教員が教材として使用するために FTP クライアントソフトを使用して同時に 6 個のファイルをダウンロードしていたため、ネットワークが遅くなり他の人がつながりにくくなったことがわかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン利用状況ー

- ・64K の ISDN 環境で外部ネットワーク環境を利用して業務を行っていた。

◆発見の経緯

- ・発見方法：ネットワーク作業をしていた教員からの申し出。
- ・発生日時：平成 16 年 6 月頃
- ・発見日：同日
- ・事実確認：同日

◆被害への対応

ー教職員への対応ー

- ・対応日：被害発生日
- ・対応担当者：担当教員
- ・対応方法：実質的な被害は生じていない。

◆今後の対策と効果

- ・教職員が FTP や WWW を利用してファイルをダウンロードする場合は、複数のファイルを同時にダウンロードしない取り決めにした。

サブネットマスク設定ミスによるネットワーク障害

専門学校での事例

◆被害状況

- ・特定のパソコンからサイズの大きいファイルを別のパソコンにコピーすると、ネットワークが遅くなる現象が発生し、授業に支障が生じた。
- ・原因を調査したところ、パソコンのネットワークの設定（サブネットマスク）に設定ミスがあり、通信がデフォルトゲートウェイを経由する設定になっていた。そのため校内でファイルコピーを行っただけでもデフォルトゲートウェイに大量のトラフィックが発生していた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・校内で利用しているパソコンはネットワークでつながっている。
- ・ネットワークの授業の時間に、学生にネットワークの設定を実際に行わしている。

◆発見の経緯

- ・発見方法：授業中に教員のチェック。
- ・発生日時：平成 16 年 4 月頃
- ・発見日：平成 16 年 4 月頃
- ・事実確認：平成 16 年 4 月頃

◆被害への対応

ーネットワークへの対応ー

- ・対応日：被害発生日
- ・対応担当者：担当教員
- ・対応方法：
 - ネットワークの授業でサブネットマスクの意味を説明し、学生に再度確認をしてもらい、設定を正しく直した。

◆今後の対策と効果

- ・パソコンが遅くなる原因として、ネットワークの設定ミスでも起こることを学生に説明した。

※デフォルトゲートウェイ

外部のネットワークにアクセスする場合、クライアントパソコンのかわりに外部と通信するためのサーバ。

※サブネットマスク

I P アドレスをネットワーク部分とホスト部分に分割するための値。

付箋プログラム利用によるネットワークダウン

専門学校での事例

◆被害状況

- ・職員が業務連絡用に職員間でネットワーク対応付箋プログラムを利用していたところ、不特定多数の相手に向かってデータを送信（ブロードキャスト通信）していたため、ネットワークに負荷がかかりすぎ、速度低下、最後にはダウンしてしまった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン利用状況―

- ・職員用のネットワークと生徒用のネットワークは別々になっている。

◆発見の経緯

- ・発見方法：教師の申し出。
- ・発生日時：平成 16 年 6 月頃
- ・発見日：平成 16 年 6 月頃
- ・事実確認：平成 16 年 6 月頃

◆被害への対応

―教職員への対応―

- ・対応日：被害発生日
- ・対応担当者：担当教員
- ・対応方法：
 - 職員全員へネットワークがダウンした原因を説明し、ネットワーク対応付箋プログラムの利用を禁止した。

◆今後の対策と効果

- ・その後、職員への連絡は電子メールで行い、職員も常に電子メールを確認するよう指示した。

※付箋プログラム

PC のデスクトップ上に紙でできた付箋と同じ感覚でちょっとした情報を貼り付けておくことができるプログラム。

イベントの期日にアラームが鳴るアラーム機能やネットワークを介して情報を他の PC と付箋情報を共有することができる機能を持つタイプもある。

※ブロードキャスト

ネットワーク上に存在する機器全てに対してデータの送信を行うこと。

誤った無線 LAN 接続先

専門学校での事例

◆被害状況

- ・校内ネットワークとして無線 LAN を利用している。
- ・校舎近隣にオフィスビルがあり、教室の場所によっては校内ネットワークではなく、近隣オフィスのネットワークに接続してしまうことが起こった。
- ・授業でネットワークを経由して提出させている課題の提出ができなくなった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

- －校内のパソコン環境－
- ・学生利用専用の校内無線 LAN

◆発見の経緯

- ・発見方法：生徒からの相談により判明した。
- ・発生日時：平成 17 年 10 月
- ・発見日：
- ・対応方法：

◆被害への対応

- －生徒への対応－
- ・対応日：平成 17 年 10 月
- ・対応担当者：
- ・対応方法：
ネットワークの接続先要求に応じていたために、接続先が近隣企業になっていたため、学内ネットワークの設定に戻すように指示した。

◆今後の対策と効果

ウィンドウズアップデートによる起動停止トラブル

高等学校での事例

◆被害状況

- ・職員が業務で使用しているパソコンに WindowsXP Service Pack 2(SP2)を導入したところ、起動途中で停止してしまうようになった。
- ・パソコンメーカーのホームページで SP2 対策のページを調べたところ、音源ドライバと SP2 の相性の問題で発生していたことが判明した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・校内のパソコンはネットワークでつながっている。
- ・校内のネットワークを使い、インターネットは閲覧可能になっている。
- ・ネットワークを使い、Windows のアップデートが可能。

◆発見の経緯

- ・発見方法： アップデート実施直後に発見。
- ・発生日時：平成 16 年 9 月 20 日
- ・発見日：同日
- ・事実確認：同日

◆被害への対応

- ・対応日：被害発生日の翌日
- ・対応担当者：担当教員
- ・対応方法：パソコンをセーフモードで起動し、音源を使用しない設定で対応した。

◆今後の対策と効果

- ・後日、メーカーより対策方法が発表され、対策方法を実施した。

※WindowsXP Service Pack 2 (SP2)

WindowsXP の既知の問題点を修正したり、セキュリティに関する機能を強化するプログラム。SP2 をインストールする前に、利用しているパソコンや、ソフトウェアの SP2 への対応状況を確認してから利用する。

いたずらによる授業支援システムの停止

高等学校での事例

◆被害状況

- ・ネットワーク環境を利用して生徒の利用するパソコンの電源管理・データ配布・教員が利用しているパソコンの画面提示などを行う授業支援システムを利用しているが、ある生徒が、授業支援システムが動作しなくなるようにパソコンにいたずらを行った。
- ・授業支援システムの停止によって授業が中断するなど直接的な影響はなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・校内 LAN が整備されている。

◆発見の経緯

- ・発見方法：授業時に、授業支援システムが停止したため判明した。
- ・発生日時：平成 17 年
- ・発見日：いたずらが行われた直後
- ・事実確認：

◆被害への対応

―いたずらをした生徒への対応―

- ・対応日：いたずらを確認したその日
- ・対応担当者：情報担当教員
- ・対応方法：

いたずらをした生徒は、利用しているパソコンの画面解像度を変更すると授業支援システムが動作しなくなることを知っていて、わざと画面解像度を変更していた。生徒にはルールを守ってパソコンを利用するよう個別に注意を行った。

◆今後の対策と効果

- ・授業支援システムをさほど利用していないことと、生徒が作成したデータが削除されてしまうなどの被害が発生しているわけではないので、システム的な対応はせず、生徒がルールを守って利用するよう現在も指導を行っている。

生徒によるシステム設定の変更

高等学校での事例

◆被害状況

- ・情報の授業中、ある生徒が利用しているパソコンのシステム設定を変更していた。
- ・生徒が利用しているアカウントは、ハードディスクへの書き込み権限がないため、実際にシステム設定は変更されなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・生徒が利用するパソコンを把握するために座席を固定している。また、教員は教員用モニターで生徒が操作している画面を確認することが出来る。
- ・生徒がいつも同じ環境でパソコンを使用できるように、生徒には書き込み権限のないアカウントを付与しており、システム設定の変更は出来ないようになっている。

◆発見の経緯

- ・発見方法：生徒がシステム設定を変更しているところを教員が教員用モニターを通して発見した。
- ・発生日時：平成 17 年 10 月頃
- ・発見日：同上
- ・事実確認：

◆被害への対応

ーシステム設定を変更した生徒への対応ー

- ・対応日：発見したその日
- ・対応担当者：情報担当教員
- ・対応方法：
パソコンスキルを持っている生徒だったので、授業に退屈してシステム設定を変更した。当該生徒に対し、学校のパソコンは共用であり、勝手に設定を変更することで他の生徒が利用できなくなることもあるので、ルールを守って利用するように個別に注意を行った。

◆今後の対策と効果

- ・その後、生徒によるシステム設定の変更は行われていない。

生徒用ファイルサーバ内のデータの改変

中学校での事例

◆被害状況

- ・生徒が授業中に作成したデータはファイルサーバに保存するようにしているが、以前にファイルサーバに保存してあるデータが本人の知らないうちに書き換えられていた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・パソコン教室は LAN 環境が構築されている。
- ・生徒が授業中に作成したデータはファイルサーバに保存するようにしている。

ー校内のパソコン利用状況や利用形態ー

- ・ファイルサーバ内は、各教科フォルダを作成し、各教科フォルダ内にクラスフォルダを作成し、クラスフォルダ内に出席番号フォルダを作成している。
- ・ファイルサーバのフォルダは、すべての生徒が「読み込み」・「書き込み」・「削除」が行えるようになっている。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 15 年～
- ・発見日：
- ・事実確認：

◆被害への対応

ー生徒用ファイルサーバ内のデータ管理ー

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

以前にファイルサーバ内のデータが本人の知らないところで書き換えられる事象が発生していたので、情報担当教員がファイルサーバ内のデータが書き換えられていないか、確認作業を行っている。

情報担当教員一人で実施するのは大変な作業なので、パソコン部の活動の一環として、ファイルサーバ内のデータ確認作業をパソコン部に所属する生徒も行っている。

パソコン部の生徒が確認作業を行っているときに、ファイルサーバ内に授業で作成したデータ以外が保存されていた場合には、すぐに教員に申し出るように指導している。

◆今後の対策と効果

誤操作によるファイルの移動

高等学校での事例

◆被害状況

- ・作成したファイル进行操作しようとしたところ、ファイルサーバの決められたフォルダにファイルが存在しなかった。ファイル自身は削除されていたわけではなく、他のクラスの生徒が誤って別のフォルダにすべてのファイルを移動してしまったようで、授業への大きな被害は発生しなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン利用状況ー

- ・授業で作成したファイルは、教員の指示のもとファイルサーバの共有フォルダに保存するルールとしている。

ー校内のセキュリティ対策ー

- ・共有フォルダのアクセス権はフルアクセスとなっており、パソコン教室のパソコンからはファイルサーバのフォルダやファイルにフルアクセスすることができる。

◆発見の経緯

- ・発見方法：授業時に生徒の申し出により判明。
- ・発生日時：平成 16 年 2 月頃
- ・発見日：平成 16 年 2 月頃
- ・事実確認：平成 16 年 2 月頃

◆被害への対応

ー生徒への対応ー

- ・対応日：平成 16 年 2 月頃
- ・対応担当者：情報担当教員
- ・対応方法：
ファイル検索を行ったところ別のフォルダに移動していただけなので、ファイル自身が削除されたわけではないことを伝えた。

◆今後の対策と効果

- ・体系的な対策として、生徒一人ひとりにネットワークアカウントとパスワードを作成し、ネットワーク管理を行うことを検討したが、生徒のパスワード管理等を考えると、現状での導入は厳しいと判断し断念した。
- ・授業終了時に、毎回データのバックアップすることとした。

生徒による共有フォルダへのいたずら

高等学校での事例

◆被害状況

- ・生徒にデータを配付する際に利用している共有フォルダの名称が、生徒のいたずらにより変更されていた。教員が発見したので名称は直ちに修正をした。
- ・フォルダ名が変更されたことによってデータの受け渡しが滞ることは無かった。また、共有フォルダ内のデータも削除されていなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・生徒が学校内のパソコンを利用する際には、生徒個人に付与しているユーザ ID とパスワードが必要となる。
- ・データ配付用フォルダは校内の教員・生徒であれば誰でも利用できる前提で設置しているのでアクセス制限は特に設定していない。

◆発見の経緯

- ・発見方法：共有フォルダ名が変更されているのを教員が発見した。
- ・発生日時：平成 16 年
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成 16 年
- ・対応担当者：情報担当教員、契約している校内のネットワーク管理者
- ・対応方法：

校内のネットワーク管理者にログ調査を依頼し、フォルダ名を変更した生徒を特定した。フォルダ名を変更した生徒が特定できたので、生徒を呼び出し、ルールを守って利用するように個別指導を行った。

今回いたずらされた共有フォルダは、校内の教員・生徒であれば誰でも利用できる前提で設置しているので、今回のケース以降も特にアクセス制限は設定していない。

◆今後の対策と効果

- ・その後、共有フォルダへのいたずらは発生していない。

教員の誤操作による生徒用フォルダへのデータ保存

高等学校での事例

◆被害状況

- ・教員が作成した教材用データが生徒用共有フォルダに保存されていた。
- ・生徒用共有フォルダに保存されていたデータは教材用データであったため、テスト問題が生徒に漏れることはなかったが、テスト問題が生徒に流出してもおかしくない状況にあった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・教員は、教員用ネットワークと生徒用ネットワークの共有フォルダにアクセスできるが、生徒は教員用ネットワークは利用できない。

◆発見の経緯

- ・発見方法：他の教員が生徒用共有フォルダに教材データが保存されているのを発見した。
- ・発生日時：平成 15 年
- ・発見日：
- ・事実確認：

◆被害への対応

ー教員への対応ー

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：
ログの調査結果や保存されていた教材データの内容から、生徒用ネットワークにコピーした教員が判明したので、情報担当教員が適切な場所に保存するように注意を行った。
原因は、教員用ネットワークにデータをコピーするところ、誤って生徒用ネットワークにコピーしてしまい、確認作業を怠ったために発生した。

ーシステム的な対応ー

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：
教員が利用するパソコンに教員用と生徒用の両方のネットワークがデフォルトで表示されるようになっていたために、誤ってデータをコピーするということが発生した。
教員が教員用と生徒用の両方のネットワークを意識して利用するようにするために、教員用ネットワークはデフォルトで表示させ、生徒用ネットワークは教員が設定しない限り表示されないように変更した。

◆今後の対策と効果

- ・ネットワークを利用する側の教員の意識も高まり、教員が作成したデータを誤って生徒用ネットワークに保存するということは発生していない。

学校設置パソコンへの児童によるいたずら

小学校での事例

◆被害状況

- ・児童が調べ学習等で利用するために、インターネットが利用できるパソコンを 20 台設置している。授業時に児童がパソコンを利用すると、児童 2 人に対して 1 台のパソコンが利用できる状況だが、児童がマウスの中に入っているボールを抜き取るいたずらをするためマウスが利用できず、児童 2 人に対して 1 台でパソコンを利用できないことがあった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・児童が利用するパソコンは教育委員会ネットワークを經由してインターネットが利用できる。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 16 年
- ・発見日：
- ・事実確認：

◆被害への対応

―いたずらへの対応―

- ・対応日：平成 17 年 3 月
- ・対応担当者：情報主任
- ・対応方法：
マウスの中に入っているボールを抜き取られないための対策を検討し、ボールで動くタイプのマウスから光学式マウスに買い替えを行った。

◆今後の対策と効果

学校備品の盗難

高等学校での事例

◆被害状況

- ・生徒がパソコン教室のノートパソコンを盗みだそうとした。パソコン教室で授業時に先生が他の生徒を対応しているすきにパソコン教室の教師用ノートパソコンを盗もうとしていた。幸いなことに、学校外に持ち出される前に発見したので、未遂で済んだ。
- ・耐震工事の関係でパソコン教室は施錠せず、出入りが自由にできる状況だったため、パソコン教室のデスクトップパソコンが盗まれた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：教員が発見した。
- ・発生日時：平成16年10月
- ・発見日：平成16年10月
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：発見したその日
- ・対応担当者：生活指導担当教員
- ・対応方法：
パソコンを盗み出そうとした生徒には、個別指導を実施した。

－物理的な対応－

- ・対応日：未遂事件発生から1ヶ月
- ・対応担当者：情報担当教員
- ・対応方法：
パソコン教室に設置しているノートパソコンすべてにワイヤーロックを導入し、盗難防止措置を講じた。

◆今後の対策と効果

Ⅱ. 対策・指導事例編

生徒情報（個人情報）の管理対策 1

中学校での事例

◆被害状況

- ・学校で管理している情報を外部に漏えいしないようにルールを定め運用している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

－校内のセキュリティ対策－

- ・成績情報等の個人情報を管理する部門を分掌として定めている。
- ・成績処理や試験問題を作成するパソコンはインターネットへの接続をしていない。
- ・成績処理するパソコンはアクセス権限を設けている。

◆発見の経緯

◆被害への対応

－教職員への対応－

- ・対応日：
- ・対応担当者：分掌で定めてある情報管理委員会
- ・対応方法：

生徒の成績情報は、各教員が作成した成績データをデータ管理責任者が一括で外部ネットワークに接続しないパソコンで処理を行い、MOにデータを保管し管理している。

定期試験等の試験問題は、各教員が外部ネットワークに接続しないパソコンで作成し、パソコンのハードディスクにデータを残さないようにしている。

職員室内のパソコンに成績情報や試験問題等のデータが保存されていないか、情報管理委員会の教員が月に1回チェックを行っている。

◆今後の対策と効果

- ・情報漏えいにつながる事故は発生していない。

生徒情報（個人情報）の管理対策 2

高等学校での事例

◆被害状況

- ・学校内で定めている個人情報の取扱いのルールが学校全体に完全に浸透していない。
- ・生徒情報が外部に漏えいするという大きな事故は発生していない。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・職員室内にスタンドアロンのパソコンが4台。

ー校内のパソコン利用状況や利用形態ー

- ・教員は職員室内に設置してあるパソコンを自由に利用できる。

ー校内のセキュリティ対策ー

- ・生徒に関する情報やそれ以外の個人情報は、職員室内に設置してあるパソコン本体に保存することは禁止している。保存する場合は、外部メディア（フロッピーディスクやCD-ROM）などに保存し、所定の場所に保管するルールを定めている。
- ・情報委員会のメンバーが、月に1回のペースで、職員室内のパソコンに個人情報が保存されていないかチェックする。

◆発見の経緯

- ・発見方法：情報委員会のメンバーが定期メンテナンス中に個人情報を発見した。
- ・発生日時：平成16年6月頃
- ・発見日：平成16年6月頃
- ・事実確認：平成16年6月頃

◆被害への対応

ー個人情報が発見されたときの対応ー

- ・対応日：パソコン本体から個人情報が発見された当日
- ・対応担当者：情報委員会メンバー
- ・対応方法：
 - パソコン内に保存されている個人情報ファイルを作成した教員に直接削除するよう依頼し、情報委員会のメンバーが個人情報を削除するところを一緒に確認した。
 - 学校内で定められているルールをもう一度確認するよう注意した。

◆今後の対策と効果

- ・情報委員会のメンバーが月に1回のペースでパソコン内のデータをチェックしているが、今後も継続していく。
- ・学校内で定められたルールを遵守するよう、教職員に呼びかけを行っていく。

生徒情報（個人情報）の管理対策 3

高等学校での事例

◆被害状況

- ・生徒の成績情報など個人情報の取扱いルールや校内パソコンの利用ルール等を定めているが、教職員に周知徹底されておらず、教職員の情報セキュリティへの認識が低い。
- ・個人情報保護に関する取り組みが法的に求められる状況になるなかで、生徒等の情報を預かっているという当事者としての認識が低い。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：一般利用校内パソコンに生徒の住所や電話番号などのファイルが存在していた。
- ・発生日時：平成 16 年～平成 17 年
- ・発見日：
- ・事実確認：緊急連絡網ファイルからクラス担任と判明

◆被害への対応

－教職員への対応－

- ・対応日：平成 16 年～平成 17 年
- ・対応担当者：情報担当教員
- ・対応方法：

職員会議等で情報セキュリティへの認識を高めるよう継続して呼びかけを実施している。職員会議での呼びかけ以外に、教職員への周知徹底するために、コンピュータウイルス感染した場合などの実際のケースを想定した訓練や、教職員向けに定められたルールが守られているかの検査を抜き打ちで実施するなどして、意識の向上を図っている。個人情報に関しては、成績情報の取扱い以外にポリシー等の整備を進めるよう検討している。

◆今後の対策と効果

- ・学校に関する個人情報保護に関しては、文部科学省から学校向けのガイドラインが公表されていることをアドバイスした。

生徒情報（個人情報）の管理対策 4

高等学校での事例

◆被害状況

- ・生徒に関する個人情報を多数保有しているため、情報漏えいが発生しないように情報管理対策を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

－情報管理方法－

- ・対応日：
- ・対応担当者：
- ・対応方法：

生徒の個人情報はパソコンのハードディスクに保存せず、昨年度まではMO等のメディアに保存し、鍵のかかるロッカーに各自で保管していた。今年度からは教育委員会ネットワークのサーバのみ保存することになっている。

年度の初めに全教員が実施すべき情報管理対策の確認を行い、年度の終わりに事故防止日常点検チェックリストを利用して、実際に情報管理対策を実施したか確認を行っている。個人情報を校外に持ち出す際には、持出許可願を管理職に提出し、管理職が許可した情報のみを持ち出ししている。また、持出許可願を管理職に提出することにより、管理職が個人情報の持出状況を把握している。

◆今後の対策と効果

- ・今後も、全教員が保有している情報の重要性を理解し、適切な情報管理を行うように対策を継続して行っていく。

生徒情報（個人情報）の管理対策 5

高等学校での事例

◆被害状況

- ・ 中学校を訪問する際に、訪問先の中学校を卒業し、高校に入学した生徒の成績情報や進学情報などであったとしても、訪問先の中学校教員に紙媒体などに印刷して提示しないように、全教員に周知している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：
- ・ 発生日時：平成 17 年
- ・ 発見日：平成 17 年
- ・ 事実確認：

◆被害への対応

－教員への対応－

- ・ 対応日：平成 17 年
- ・ 対応担当者：
- ・ 対応方法：

生徒の個人情報を適切に管理するため、生徒から取得した情報で利用目的の範囲を超える情報の取扱いを行わないよう、全教員に周知している。

学校の日常生活の様子などを伝えることはあるが、成績などの個人情報は伝えていない。

◆今後の対策と効果

- ・ 今後は学校としてより適切な個人情報の管理を行うため、プライバシーマークの取得を検討している。また、プライバシーマーク取得への取り組みを通じて、教職員の情報セキュリティ意識の向上を図っていく。

生徒情報（個人情報）の管理対策 6

高等学校での事例

◆被害状況

- ・個人情報の取り扱いの重要性が増すなかで、強固なセキュリティが必要になっている。
- ・すでにネットワーク対策は施しているものの、学校全体として教職員すべてのセキュリティ意識を含む対策が必要となっている。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

ネットワークから不正アクセス、情報漏えいなどを防ぐためにネットワークは次の考え方で分割している。

1. インターネットを利用することが可能なネットワーク
2. 学内だけの利用にとどめるネットワーク
3. 情報教育のみに利用するネットワーク
4. 生徒情報のみに利用するネットワーク

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 17 年
- ・発見日：
- ・対応方法：

◆被害への対応

－教員への対応－

- ・対応日：平成 17 年
- ・対応担当者：
- ・対応方法：

セキュリティの向上のために、全教職員の意識向上も含めた対策として「プライバシーマーク」の取得を予定することにした。

◆今後の対策と効果

生徒情報（個人情報）の管理対策 7

高等学校での事例

◆被害状況

- ・個人情報保護法の施行に伴い、学校で取得する生徒の個人情報について、すべての教員が適正な管理を行うように努めている。
- ・中学校や学習塾を訪問することがあり、学校説明会への参加状況などの情報について、迂闊に提供しないように訪問する教員に指示を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 17 年
- ・発見日：平成 17 年
- ・事実確認：

◆被害への対応

－教員への対応－

- ・対応日：平成 17 年度以降
- ・対応担当者：校内分掌で定められている入試・広報委員会担当教員
- ・対応方法：

校内分掌で定められている入試・広報委員会より、中学校や学習塾を訪問する教員に対して、高校の学校説明会に参加した中学生の個人情報を提示しないように口頭で指示を行っている。

現在は口頭での指示になっているが、個人情報の取扱いについて、学校として整理し明文化することが課題となっている。

◆今後の対策と効果

- ・現在のところ、個人情報取得時の利用目的を超える利用は行われておらず、情報漏えいなどの事故も発生していない。

生徒情報（個人情報）の管理対策 8

高等学校での事例

◆被害状況

- ・個人情報保護法の全面施行や個人情報の悪用もあり、学校においてもさまざまな場面で生徒個人の情報の取扱いの見直しに迫られている。学校内に設置してある掲示板に掲示する情報のうち、生徒の個人情報を扱う場合は、取得した情報の利用目的の範囲を超えないようにしている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 17 年
- ・発見日：平成 17 年
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成 17 年
- ・対応担当者：各学年の教員
- ・対応方法：

校内に設置してある掲示板に定期試験結果・大学合格者情報・資格取得者情報など個人の情報を扱う場合には、利用目的や掲載期間を生徒に説明し、生徒に掲示の意思確認をしてから情報を掲示している。

意思確認時に掲示することについて拒否した生徒の情報については、掲示板への掲載を行っていない。

◆今後の対策と効果

- ・現在は、学年毎に学校内の掲示板に掲示すべき情報か否かを判断しており、個人情報の取扱いにずれが生じているので、学校全体として高いレベルで個人情報を扱う仕組みが必要と考えている。

生徒情報（個人情報）の管理対策 9

高等学校での事例

◆状況

- ・学校は生徒の成績情報をはじめ多くの個人情報を管理している。
- ・常に適切な管理を行うように努めているが、明文化された規定がなく、情報管理の方法が口頭での伝達により行われている。
- ・平成 17 年 4 月には個人情報保護法が施行されることもあり、より適切な管理をしていくために明文化した規定を策定することとした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：より適切な管理をしていくために明文化した規定を策定する必要があるがあった。
- ・発生日時：平成 16 年 9 月
- ・発見日：
- ・事実確認：

◆対処方法

—個人情報への対応—

- ・対応日：平成 16 年 9 月
- ・対応担当者：個人情報保護対策チーム
- ・対応方法：

校長からの指示により、学校としての個人情報の管理規定を策定することとした。

校長と教頭を含む教員 7～8 名の管理規定策定チームを平成 16 年 9 月に発足させた。

月に 1～2 回程度の議論を重ね、平成 17 年 4 月に個人情報の取り扱いに関する基本方針を公表した。

詳細の管理規定については、さらに議論を重ねる必要があったので、1 年間かけて管理規定策定チームで継続して検討を実施した。

平成 18 年 4 月に詳細の管理規定の運用を開始した。

◆今後の対策と効果

- ・今後は、策定した管理規定を教職員に徹底させるとともに、運用をすることにより出てくる管理規定の課題を見直していく必要があると認識している。

生徒情報（個人情報）の管理対策 10

高等学校での事例

◆状況

- ・個人情報保護法の施行以降、特に生徒の氏名や住所、成績などの情報を適切に取り扱うようにしている。
- ・平成 17 年度まで生徒の希望により実施していた資格認定試験を、平成 18 年度から全生徒が取得を目指す資格として位置づけ、生徒全員に受験させることとした。
- ・平成 17 年度までは、希望者のみが参加していた資格認定試験だったので、希望者から主催者に個人情報を提供する許諾を得ていたが、平成 18 年度は学校全体で参加することになったので、学校から主催者に個人情報を提供する許諾を得るための文書を保護者に発送することとした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：
- ・発生日時：平成 18 年 5 月
- ・発見日：
- ・事実確認：

◆対処方法

—資格試験応募への対応—

- ・対応日：平成 18 年 5 月
- ・対応担当者：
- ・対応方法：

認定試験の主催者に生徒の許可なく学校から生徒の氏名、生年月日、所在地の情報を提供することはできないので、保護者に資格認定試験の趣旨、主催者のプライバシーポリシー、提供する情報を文書で配付し、保護者から情報提供の許諾を得ることとした。

本来は全員から賛同するという回答を得ることが望ましいことだが、確認作業に時間を費やしてしまうので、情報提供できないという保護者から書面を提出してもらうこととした。

◆今後の対策と効果

生徒情報（個人情報）の管理対策 1 1

高等学校での事例

◆状況

- 多くの教員・生徒が携帯電話を保有している。生徒との緊急連絡の手段として校外研修や部活動、進路指導などの様々なケースで携帯電話を利用している。そのため、教員が保有している個人の携帯電話には、生徒の氏名・携帯電話番号・電子メールアドレスなどの情報を保有している。
- 現状では、教員が生徒の携帯電話番号や電子メールアドレスをどれぐらい保有しているのか学校として管理していないので保有件数は不明だが、携帯電話を紛失した場合を想定して学校としての管理方法を検討している。
- 教員の携帯電話紛失により生徒情報が漏えいした事実は確認されていない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- 発見方法：
- 発生日時：平成 18 年 4 月
- 発見日：
- 事実確認：

◆対処方法

－情報管理方法への課題－

- 対応日：
- 対応担当者：情報担当教員
- 対応方法：

学校として教員が生徒の携帯電話番号をどの程度保有しているか把握できていないので、今後は管理職の許可を得てから生徒の携帯電話番号を入手するようなルールを導入し、どの教員がどの程度の件数の個人情報を保有しているのか管理することを検討している。教員が携帯電話を紛失するケースも想定され、生徒情報の漏えいを防ぐためにも学校が管理することはやむを得ないと認識しているが、卒業後の進路指導などで生徒と連絡を取り合うケースもあるので、生徒指導の観点も含め柔軟な対応ができるようにすることが課題である。

◆今後の対策と効果

生徒情報（個人情報）の管理対策 1 2

高等学校での事例

◆状況

- ・多くの生徒が携帯電話を保有しており、生徒に直接連絡するために、教員が生徒の携帯電話に連絡することがある。
- ・そのため、教員が個人で所有している携帯電話に生徒の携帯電話番号や電子メールアドレスが保存されており、生徒情報を日常的に学校外に持ち出すことになるので、適切な管理を行う必要がある。
- ・幸い、教員の携帯電話紛失による生徒情報の漏えいは発生していない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：生徒の携帯電話番号の取得について、教育委員会から適切な取り扱いを行うように通知があった。
- ・発生日時：平成 18 年 4 月
- ・発 見 日：
- ・事実確認：

◆対処方法

－生徒の携帯電話番号の取得方法－

- ・対 応 日：平成 18 年 4 月
- ・対応担当者：
- ・対 応 方 法：

生徒の携帯電話番号・電子メールアドレスを教員が取得する際には、管理職の許可を得てから取得することとした。

課外授業や部活動など、校外での活動時には生徒との連絡に携帯電話を用いることがあるが、必要以上に情報を保有しないように連絡先を取得する生徒を限定するなどして対応している。また、生徒が先生の携帯電話に連絡のメールをすることがあるが、教員の携帯電話に生徒の電子メールアドレスを保存すると毎日生徒情報を学校外に持ち出すことになるので、学校のパソコンに電子メールアドレスを保存し、学校のパソコンからメールを送信して対応している。

◆今後の対策と効果

- ・教員の携帯電話紛失による生徒情報の漏えいは発生していない。

生徒情報（個人情報）の管理対策 13

高等学校での事例

◆状況

- ・生徒情報や教務情報を外部に漏らさないための対策を実施している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・生徒が利用するパソコンからネットワークを通じて教員が利用するパソコンのデータを操作できないようにするために校内 LAN は生徒用と教員用を分割している。
- ・教員が職員室で利用する教員用 LAN は、インターネットを経由した情報漏えいやウイルス感染を防ぐためにインターネットに接続していない。教員がインターネットを利用する場合は教員 LAN とは別のインターネットに接続できる専用パソコンを利用している。
- ・職員室には生徒・業者・来訪者など教員以外に多くの人間が出入りするので、生徒の個人情報情報は情報を保管する専用の部屋を設置して管理している。
- ・特に重要な個人情報（家族状況、健康記録）は、教務室、保健室にて施錠管理している。
- ・インターネットに接続できるパソコンを限定している。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—情報管理方法—

- ・対応日：平成 16 年 4 月
- ・対応担当者：情報担当教員
- ・対応方法：

校務で利用するために持ち込む教員の私物パソコンは、教員用 LAN には接続できるが、インターネット接続することはできない。

私物パソコンを持ち込む際には学校内で定めた規定に基づき、セキュリティ対策が実施されたパソコンのみとしている。

生徒情報を保管する部屋への出入りは、鍵を管理している教頭の許可を得ることとしている。

生徒に緊急で連絡をとらなければならない場合は、情報を保管している部屋から情報を持ち出すのではなく、情報を保管している部屋から連絡をするようにしている。やむを得ず情報を持ち出す場合は、教頭の許可を得ることとしている。

◆今後の対策と効果

- ・情報漏えい等の事故は発生していない。

生徒情報（個人情報）の管理対策 14

高等学校での事例

◆状況

- 中学を訪問する際に、中学側から卒業生の様子を聞かれることがある。高校としても生徒の様子を伝えることが必要だと考えており、生徒の成績や進路情報などを訪問時に持参している。
- 持参する際には、情報を途中で紛失しないように注意を払い、また、訪問先の中学校に情報を置き忘れることがないようにするために、全教員に周知徹底している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- 発見方法：
- 発生日時：平成 17 年
- 発見日：
- 事実確認：

◆対処方法

—管理対策—

- 対応日：
- 対応担当者：担任教員
- 対応方法：

中学校側の管理の問題もあるので、持参した生徒情報は必ず学校に持ち帰り、学校で廃棄している。

個人情報を適切に管理することは、全教員に口頭で周知徹底しているが、具体的な管理対策が文書化されていない。より適切に個人情報を管理するためにも、具体的な管理対策を文書化することが今後の課題である。

◆今後の対策と効果

生徒情報（個人情報）の管理対策 15

高等学校での事例

◆状況

- ・学校説明のために中学校を訪問する際に、当該中学校を卒業した生徒の高校での成績や高校卒業後の進路などの情報を中学校側に提供している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—管理対策の課題—

- ・対応日：
- ・対応担当者：中学校を訪問する教員
- ・対応方法：

生徒情報を保護することは最も優先すべき事項と認識しており、情報漏えいが起こらないように適切に管理している。

一方で、中学校を訪問する際に、卒業生の様子を気にかけている中学校に対しては、当該中学校を卒業した生徒の高校での成績や高校卒業後の進路などの情報を中学校側に提供している現実がある。

生徒情報の保護を最優先しつつ、中学校と高校で情報共有できる仕組みづくりが今後の課題である。

◆今後の対策と効果

生徒情報（個人情報）の管理対策 16

専門学校での事例

◆被害状況

- ・職員室内が無人になることはないが、学生は職員室への出入りが可能なので、職員室内に保管している個人情報や試験問題等の情報が学生に持ち出しされないよう対策を実施している。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

－校内のセキュリティ対策－

- ・職員室内が無人になることはない。
- ・個人情報や試験問題を保管するキャビネットへは、第三者がすぐにわかるような名称でラベリングをしていない。
- ・試験実施の前後一週間は職員室への出入りを禁止している。

◆発見の経緯

◆被害への対応

－情報管理方法－

- ・対応日：
- ・対応担当者：全教員
- ・対応方法：

職員室へ学生が出入りをするので、学生名簿や成績情報などの個人情報や試験問題等は、教員の机上に置かないようにしている。

教員が利用するパソコンは、ディスプレイから個人情報や試験問題等の情報が閲覧できる可能性があるため、パソコンから離席する時は、スクリーンセーバがすぐに起動する設定にしており、スクリーンセーバの解除もパスワードを要求するようにしている。

学生の個人情報や試験問題を作成したエクセルやワードのデータは、エクセルやワードの機能を利用してパスワード設定して管理している。

◆今後の対策と効果

生徒情報（個人情報）の管理対策 17

専門学校での事例

◆被害状況

- 成績データなどの生徒情報を教員が自宅に持ち帰る途中、盗難・紛失する事故が報道されている。データを学外に持ち出すことは禁止しているが、勤務形態が様々になるなか他校の非常勤講師を引き受けているケースもあり、すべてのデータ持出し禁止を実践することが困難な状況にある。
- このため、データを持ち出し盗難・紛失時にも読み取られない対策を検討し、実施することとした。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

—情報管理方法—

- 対応日：平成16年
- 対応担当者：教員
- 対応方法：

データにパスワードをかけることができるソフトを採用し実践することにした。

USBメモリには、パスワード設定できるソフト添付で販売されているタイプがあり、またインターネット上にフリーのデータ暗号化ソフトが流通している。

◆今後の対策と効果

- デジタルデータについては、パスワード設定で万が一の盗難・紛失に対策とすることができるが、答案の持ち出しについては引き続き課題となっている。

生徒情報（個人情報）の Web サイト上での管理対策 1

小学校での事例

◆被害状況

- 学校の Web サイトは教員が作成した情報を掲載している。
- 学校内に情報委員会を設置し、Web サイトに掲載する画像や内容について、複数の教員の目で確認してから公開している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

－Web サイト上での注意点－

- 対応日：
- 対応担当者：校内の情報委員会
- 対応方法：

情報委員会に属する教員が、Web サイトに掲載する情報を確認している。

児童の画像を Web に掲載する場合は、児童の顔が判別できないよう加工し、当該児童の保護者から承諾を得て公開している。

◆今後の対策と効果

- 今後は Web サイトによる情報公開をより充実させる予定なので、児童の画像や作品の公開にあたっては、十分な配慮を行うように情報委員会内で徹底していく。

生徒情報（個人情報）の Web サイト上での管理対策 2

高等学校での事例

◆被害状況

- Web サイトを作成し、学校情報の公開をしている。その際、他校でのトラブル事例を鑑み、独自の情報公開ルールによって運営している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のセキュリティ対策―

- Web ページの作成・公開に関するルールを定め、教職員に周知徹底している。

◆発見の経緯

◆被害への対応

―Web サイトでの注意点―

- 対応日：
- 対応担当者：
- 対応方法：

生徒の画像を掲載する際には、作成者以外の複数の教員がチェックを行い、本人が特定できない画像を掲載するように配慮している。

生徒の作品やコメントを掲載する際には、本人の掲載希望などの意思と本人からの同意又は保護者の同意を得るようにしている。

◆今後の対策と効果

生徒情報（個人情報）の Web サイト上での管理対策 3

高等学校での事例

◆被害状況

- 学校の Web サイトに教員と生徒が作成した情報を掲載している。Web ページを公開する際は、教育委員会が定めているガイドラインをもとに、生徒の顔写真や氏名などの個人情報を公開しないようチェックしている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- パソコン教室のパソコンはインターネットに接続できるが、教育委員会ネットワークのフィルタリングを通った Web サイトのみ閲覧できる。

ー校内のセキュリティ対策ー

- Web ページの掲載情報をチェックする体制として、校内にコンピュータ委員会を設置している。
- 生徒が Web ページを作成し公開する場合は、教員が内容の確認及び公開作業を行うようにしている。

◆発見の経緯

◆被害への対応

ー生徒への対応ー

- 対応日：
- 対応担当者：情報担当教員
- 対応方法：

Web ページ作成の授業時に、著作権やネチケットの指導を行い、あわせて校内ルールについても紹介している。

◆今後の対策と効果

生徒情報（個人情報）の Web サイト上での管理対策 4

高等学校での事例

◆被害状況

- ・ 情報公開の一環として、行事や授業の様子などを Web サイトで公開している。その際、生徒の氏名を記載したり、顔が識別できる画像を公開したりしないようにルールを作成し運用している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

— 情報公開への対応 —

- ・ 対応日：
- ・ 対応担当者：
- ・ 対応方法：

生徒の画像を公開することがあるので、入学時に情報公開についての意思確認をとることにしている。

基本的に生徒の画像は、顔を識別することができない状態にして公開しているが、制服などを紹介する Web ページなど顔を識別できる状態で情報公開することが望ましい情報の場合には、入学時の意思確認の書類とは別に、掲載する生徒本人とその保護者から別途同意を得てから公開するようにしている。

◆今後の対策と効果

生徒情報（個人情報）の Web サイト上での管理対策 5

高等学校での事例

◆被害状況

- Web サイトを活用して情報を公開している。
- Web サイトでの情報公開にあたっては、ルールを作成し、ルールを基に Web サイトを運用している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のセキュリティ対策―

- Web サイトの運用ルールを作成し、教職員に周知している。

◆発見の経緯

- 発見方法：
- 発生日時：平成 16 年
- 発見日：平成 16 年
- 事実確認：

◆被害への対応

―情報公開への対応―

- 対応日：平成 17 年
- 対応担当者：Web サイト作成教員
- 対応方法：

生徒の情報を掲載する際には、必ず Web サイト上に掲載する期間を設け、生徒と保護者から掲載についての承諾をとっている。また、画像の掲載は、生徒の顔が識別できない程度の画像を掲載している。

学校の制服を紹介する Web ページなど顔が識別できる状態で Web サイトに画像を掲載したほうがよい場合は、在校生の画像を利用せず、卒業生の在籍時の画像を卒業生本人の承諾をとって掲載している。

◆今後の対策と効果

- 部活動の試合結果など生徒の活躍を伝える情報を学校の Web サイト内で公開したいとの要望もあるが、多くの個人情報を掲載する可能性があり学校の公式 Web サイト上では対応しきれないので、現在、適切な情報公開の方法を検討している。

生徒情報（個人情報）の Web サイト上での管理対策 6

高等学校での事例

◆被害状況

- ・学校の情報公開が積極的に求められているなかで、Web サイトを用いた情報公開は有効な手段と認識している。
- ・在校生の保護者からは、年々、わが子が参加している学校行事やクラブ活動の情報公開を求める要望が多くあり、求めに応じて教員、部活動顧問らが学校の公開基準にあわせて Web サイトの更新をしているところである。
- ・ところが、保護者からは「自分の子どもが画像に写っていない」などの画像悪用の恐れや安全性の認識不足による無理な要望もあり、これに対応する形で一部の顧問や保護者がクラブ専用の Web サイト構築、さらには学校 Web サイトとのリンクを検討しはじめる動きもあり、対応に苦慮している。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 17 年
- ・発見日：
- ・対応方法：

◆被害への対応

—情報公開への対応—

- ・対応日：平成 17 年
- ・対応担当者：
- ・対応方法：

特定のクラブ活動で保護者からの要望ということで学校の Web サイトとの切り分けは、あることになるが、生徒を危険に晒さないというスタンスに変わりはないため、学校の公開基準内で情報提供を行っている考え方を堅持せざるをえない。

◆今後の対策と効果

- ・今後も慎重な情報公開の理解と指導を行っていく。

生徒情報（個人情報）の Web サイト上での管理対策 7

高等学校での事例

◆被害状況

- Web サイトで、学校の情報公開をしている。
- 生徒情報の扱いについては、学校で定めた運用ルールに基づいて、適切な情報公開を行うように対策している。
- 生徒には、入学時に校内で撮影した写真を運用ルールに基づいて Web サイトで利用することを伝えており、同意の書面をとったうえで実際に情報公開時にもあらためて生徒本人の確認を取っている。また、校内で生徒の写真を撮影する際には、その写真を Web サイトで利用することを口頭で伝えてから写真撮影を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- 発見方法：
- 発生日時：平成 17 年
- 発見日：平成 17 年
- 事実確認：

◆被害への対応

—情報公開上の課題—

- 対応日：平成 17 年
- 対応担当者：情報担当教員
- 対応方法：

現在、Web サイトで多様な情報を公開しており、生徒の活動成果の一環として部活動などの活動状況を動画で公開している。

撮影にあたっては生徒の顔が識別できないように遠目から撮影するなどの配慮を行っているが、撮影し公開している動画は静止画より多様な情報が含まれており、より適切な取り扱いが課題となっている。

◆今後の対策と効果

生徒情報（個人情報）の Web サイト上での管理対策 8

高等学校での事例

◆被害状況

- ・学校の Web サイトを活用し情報公開を実施しているが、保護者から、学校の様子をできるだけ頻繁に情報公開して欲しいとの要望が多い。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ―校内のセキュリティ対策―
- ・ブログのコメント機能とトラックバック機能を利用できない設定にしている。
 - ・特定の教員からの書込みのみを受け付けるため、ID とパスワードによる管理を行っている。

◆発見の経緯

- ・発見方法：保護者から Web サイトでの情報公開の要望があった。
- ・発生日時：平成 16 年
- ・発見日：
- ・事実確認：

◆被害への対応

―保護者からの要望への対応―

- ・対応日：平成 17 年 9 月
- ・対応担当者：情報担当教員・各学年主任教員
- ・対応方法：

既存の Web サイトは Web ページ作成の知識が必要となり、知識を持っている教員のみが情報の更新作業を行っていたため、頻繁に情報公開を行うことができなかった。

頻繁に情報公開するためには Web サイトを作成する教員 1 人で対応するのは難しく、また複数の教員に Web ページ作成の知識を習得させるには時間がかかりすぎるので、Web ページ作成の知識を必要とせずに頻繁に情報公開を行う仕組みとして、Web サイト内にブログを設置した。

設置したブログは各学年主任教員が書込みを行い、外部からの不適切な書込みを排除するためコメント機能とトラックバック機能を利用できないようにした。

◆今後の対策と効果

- ・ブログを利用することで、Web ページ作成の知識は必要なくなり、情報公開が以前より頻繁に行われるようになったが、学年間で情報公開の頻度に差が生じている。今後は、携帯電話のインターネット機能を活用して課外活動時などの情報も公開し、より頻繁に情報公開が行われるよう教員の意識を高めることが課題となっている。

生徒情報（個人情報）の Web サイト上での管理対策 9

高等学校での事例

◆状況

- 学校の情報を積極的に発信するために Web サイトを作成し学校情報の公開をしている。
- Web サイトに公開する際は、教育委員会が定めているガイドラインをもとに、生徒の顔写真や氏名などの個人情報を公開しないようにチェックしている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- 発見方法：
- 発生日時：
- 発見日：
- 事実確認：

◆対処方法

—情報管理方法—

- 対応日：平成 16 年頃
- 対応担当者：
- 対応方法：

学校の Web サイトは、不特定多数の者に対しての情報公開となるので、生徒の個人名や顔が識別できる画像等の情報を掲載していない。

一方で、学校案内のパンフレットは、印刷物という点と配布する対象が進学希望者で相手が特定されている点から生徒の顔写真を掲載している。

学校情報を公開する Web サイトにパンフレットの内容をそのまま掲載しようとする、Web サイトでは生徒の顔写真の部分を削除しなくてはならない。

現状、パンフレットの内容を Web サイトに公開する際には顔写真を掲載していないが、同様の内容を取り扱っているにもかかわらず画像の取り扱いのポリシーが異なるので対応に苦慮している。

◆今後の対策と効果

生徒情報（個人情報）の Web サイト上での管理対策 10

高等学校での事例

◆状況

- ・学校行事など学校の情報提供ツールとして Web サイトを活用している。
- ・生徒情報を不用意に公開しないため、学校の公式 Web サイトは学校で定めた情報公開規定に基づいて運用している。
- ・一部、学校の公式 Web サイトとは別に、各部活動において試合結果等の情報を公開する Web ページを運用している。部活動で出場した大会の試合結果などは、生徒の励みとなる情報でもあるので、生徒の氏名や顔が特定できる写真を掲載することもある。そのため、各部活動の Web サイトにおいても、生徒情報を不用意に公開しないようにするための規定を作成し運用している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・Web サイトの運用規定を定め、規定に基づき運用している。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

－情報公開への対応－

- ・対応日：
- ・対応担当者：校内分掌で定められ広報担当教員、部活動の顧問
- ・対応方法：

Web サイトの管理を部活動の OB や保護者が実施する場合でも情報公開規定を作成し、学校側の許可を得て運用するようにしている。また、その規定は部活動に所属する生徒とその保護者に対して、部活動の顧問から入部時に必ず説明している。

部活動の Web サイトに生徒の氏名や顔が特定できる写真を掲載する際には、必ず生徒と保護者の承諾を得ている。また、Web サイトに掲載する情報は、全国大会レベルでの試合結果等で新聞等のメディアでも学校名や生徒氏名が紹介されている情報のみとしている。

部活動の Web サイトは学校の公式 Web サイトとは別のところで開設しているので、校内分掌で定められた広報担当教員や部活動の顧問による確認も最低 1 ヶ月に 1 回は実施し、不用意に生徒情報を公開している場合はすぐに修正している。

◆今後の対策と効果

- ・各部活動において情報公開規定を作成し運用する取り組みを継続して実施しているので、不用意な情報公開が行われることはほとんどない。

学校 Web サイトで使用する画像の転載対策

高等学校での事例

◆被害状況

- ・具体的に被害があったわけではないが、学校の Web サイトにおいて、画像の無断転載や悪用に対応するために生徒個人が特定できない画像を使用している。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

ー学校全体での対応ー

- ・対応日：
- ・対応担当者：Web サイト担当教員
- ・対応方法：

女子生徒を対象とした無断の画像公開やプライバシーに類する情報の公開、誹謗・中傷が掲示板などで事件となっている状況に鑑み、学校紹介のWebサイトに掲載する画像は、すべて生徒個人が特定できない画像（後ろ姿、髪等で見えにくい画像）を使用することとしてWebサイトをリニューアルした。

◆今後の対策と効果

- ・今後ともインターネットの危険性を十分認識しながら適切な対応をとっていくこととしている。

なりすましによる個人情報の聞き出しへの注意喚起 1

高等学校での事例

◆被害状況

- ・生徒の携帯電話に、公的機関の名を騙り、他の生徒の携帯電話番号を聞きだそうとする電話がかかってきた。
- ・同時期に教育委員会から、県内各学校でなりすましによる電話番号を聞きだそうとする行為が横行しているため、生徒に注意喚起するよう連絡があった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの相談と教育委員会からの連絡により判明した。
- ・発生日時：平成 17 年 2 月
- ・発見日：平成 17 年 2 月
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：生活指導担当教員・担任教員
- ・対応方法：

公的機関の名を騙り他の生徒の電話番号を聞きだそうとする電話が多発しているため、迂闊に友人の電話番号を教えないよう、担任教員から生徒に注意喚起を行った。

一部の生徒は、生徒同士でも情報交換を行い、携帯電話の着信拒否機能等を活用して電話がかかってくる相手を限定することで、対策を行っている。

◆今後の対策と効果

- ・生徒同士の情報交換は頻繁に行われているようだが誤った情報で対策を行うこともありえるため、教員からの的確な情報をすばやく提供することが今後の課題と認識している。

なりすましによる個人情報の聞き出しへの注意喚起 2

高等学校での事例

◆被害状況

- ・生徒の携帯電話に、友人の名を騙りさらに他の生徒の携帯電話番号を聞きだそうとする電話が県内の高等学校で横行しているため、生徒指導担当教員が各担任教員に対して生徒に注意喚起を行うように連絡を行った。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：教育委員会からの連絡により判明した。
- ・発生日時：平成 17 年 7 月
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成 17 年 7 月と 9 月
- ・対応担当者：生活指導担当教員・各担任教員
- ・対応方法：

生活指導担当教員から各担任教員に対して、生徒の携帯電話に友人の名を騙り、さらには他の生徒の携帯電話番号を聞きだそうとする電話が横行しているので生徒に個人情報を聞き出そうとする電話には応じないように指導して欲しい旨依頼した。

ホームルーム等を利用して、各担任教員から生徒に友人の名を騙り電話番号を聞きだそうとする電話が流行していることを伝えるとともに、友人の携帯電話の番号を迂闊に教えないよう注意喚起を行った。また、校内に注意を促す掲示を行った。

◆今後の対策と効果

ファイル交換ソフト利用への注意喚起

高等学校での事例

◆状況

- 教育委員会からの通達があり、学校内で利用するすべてのパソコン、教員の私物パソコンについてファイル交換ソフトの利用状況の調査を実施した。
- 学校内で利用するパソコン、教員の私物パソコンからファイル交換ソフトは発見されなかったが、ファイル交換ソフトの利用について認識が甘い教員もいるので、教員の意識向上のための取り組みを検討している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- 発見方法：教育委員会からの通達により調査を実施した。
- 発生日時：平成 18 年 5 月
- 発見日：
- 事実確認：

◆対処方法

—意識向上のための取り組み—

- 対応日：
- 対応担当者：情報担当教員
- 対応方法：

今回の調査では、自宅も含めてファイル交換ソフトを利用している教員はいなかったが、仮にファイル交換ソフトを私的に利用しようとする教員がいた場合、強制的に利用をやめさせることは難しいと考えているので、ファイル交換ソフトを利用している教員がいた場合の対応が今後の検討課題と認識している。

また、自宅において過去にファイル交換ソフトを利用したことのある教員がいる可能性もあるが、現段階では通常のダウンロードのみで情報漏えいには関係ないと認識している。ファイル交換ソフトを介した情報漏えいの仕組みを口頭で説明しただけでは教員の認識も変化しないと思うので、デモ環境を構築し、ファイル交換ソフトによる情報流出の現状を見せることも検討している。

◆今後の対策と効果

ファイル交換ソフトの利用状況調査

高等学校での事例

◆状況

- ・新聞やテレビなどの各種メディアで、ファイル交換ソフトの Winny を介した情報漏えい事故が多数報道されている。
- ・学校内での Winny を介した情報漏えい事故は発生していないが、教育委員会から平成 18 年 2 月頃に注意喚起の文書が、同年 4 月頃に Winny の利用状況について調査する旨の文書が学校に届いた。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：メディア等の報道より Winny への取り扱いに関する注意の必要性の認識と教育委員会からの文書による。
- ・発生日時：平成 18 年 2 月頃
- ・発見日：
- ・事実確認：

◆対処方法

－ファイル交換ソフトの利用状況調査－

- ・対応日：平成 18 年 5 月実施予定
- ・対応担当者：情報担当教員
- ・対応方法：

Web サイトから入手できる無料の Winny 検出ツールを利用して、学校内で利用する生徒用パソコン・教職員用パソコン・教職員の持ち込みパソコンのすべてに対して Winny の導入状況を確認する予定である。

また、教職員用パソコン・教職員の持ち込みパソコンについては、生徒情報（個人情報）がハードディスクに保存されていないかあわせて確認する予定である。

－検出ツールの入手先－

URL http://www.symantec.com/region/jp/winny/winny_tools.html

◆今後の対策と効果

個人情報の取り扱いに関する保護者からの問い合わせへの対応

高等学校での事例

◆状況

- ・個人情報保護法の施行に伴い、学校で取得・保有する生徒の個人情報について、すべての教員が適正な管理を行うように努めている。個人情報の管理方法の教員への周知は、管理職が口頭で実施している。
- ・以前は殆どなかった生徒情報の取り扱いに関する問い合わせが、個人情報保護法施行後の平成 17 年 7 月頃から在学生の保護者を中心に増加してきた。
- ・保護者からの問い合わせ対応は、管理職をはじめ各担任教員が口頭で対応している。
- ・明文化された規定がないので、新たに明文化した規定を策定する必要があると認識している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：個人情報の適切な管理を行うために明文化された規定を策定する必要があるとともに保護者からの問い合わせに対応するため。
- ・発生日時：平成 17 年 7 月頃
- ・発 見 日：
- ・事実確認：

◆対処方法

－保護者への対応－

- ・対 応 日：平成 17 年 7 月以降
- ・対応担当者：情報担当教員
- ・対 応 方 法：
 - 生徒情報（個人情報）をより適切に管理するために、明文化した規定を策定することとした。
 - 平成 17 年 9 月頃から、学校内で個人情報保護に関する諸規定を策定する 5 名程度の検討チームを発足させた。
 - メンバーが中心となり、定期的（1 ヶ月に 1 回程度）に個人情報保護に関する諸規定を検討している。
 - 検討の経過は職員会議等で報告するとともに、保護者にも保護者会で検討経過と今後のスケジュールを報告した。

◆今後の対策と効果

- ・学校が保有する個人情報を適切に管理しつつ、かつ学校の校務に支障が発生しない個人情報保護に関する諸規定を今夏に公表すべく、現在も策定中である。
- ・試行的に平成 18 年 5 月よりプライバシーポリシーを Web ページ上に掲載し、その中で学校が取得する個人情報の目的の事前明示と、第三者提供する個人情報の内容と提供先の事前明示を行い、保護者宛通知状でプライバシーポリシーの内容の同意を求めている。

Web サイトによる情報公開 1

小学校での事例

◆被害状況

- ・インターネットの活用が進み、学校行事や児童の取り組みを Web サイトで公開しているが、Web サイトの情報更新が滞っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

－Web サイトによる情報公開の課題点－

- ・対応日：
- ・対応担当者：
- ・対応方法：

教員も Web サイトを活用して情報公開することの重要性を認識しているところであるが、教務や校務が繁忙のため Web サイト作成の時間がなかったり、教員の Web サイト作成に関するスキル不足があったりするので、Web サイトの情報更新が滞っている。

今後は、Web サイトを活用した情報発信をより積極的に実施する予定であるので、時間不足やスキル不足を解消するために Web サイトをより簡単に更新できる方法や教員のスキルアップを図る方法を検討している。

◆今後の対策と効果

Web サイトによる情報公開 2

高等学校での事例

◆状況

- ・学校の情報を Web サイト上で公開している。在校生、在校生の保護者、進学希望者、地域住民の方々などに学校の様子を伝える情報を公開していく予定であるが、Web サイトに対応する教員が限られており、Web サイトの作成に時間がかかっている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・Web サイトに掲載している情報は、教育委員会が定めているガイドラインに則り、生徒の氏名や顔を識別できる画像は公開していない。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

－Web サイトによる情報公開の課題点－

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

現状、Web サイトの企画・更新は情報担当教員 2 名で担当している。

Web サイトで情報公開すべき内容や生徒情報の取り扱い方など、学校に所属する多くの教員で議論していきたいが、教務や校務が多忙であるとの理由から Web サイトに意識を傾ける教員がいない。

インターネット環境が整備され、学校においても Web サイトでの情報公開が求められているので、教員間で多くの議論ができるようにするための取り組みを検討している。

◆今後の対策と効果

学校の防犯に関する要望

小学校での事例

◆被害状況

- ・長崎県佐世保の小学校 6 年生児童殺傷事件がインターネット上の掲示板に端を発したといわれており、小学校においても教員は情報モラルや情報セキュリティへの対応を課題として十分認識している。
- ・一方、大阪教育大付属池田小の不審者侵入による児童殺傷事件後も 2005 年 1 月には横浜市立小学校で、同年 2 月に寝屋川市立小学校で不審者侵入事件が発生しており、無差別的な事件ゆえに、保護者からも防犯に対する取り組みへの要望が多数寄せられている。
- ・現状では、文部科学省や教育委員会が防犯対策を進めており、情報セキュリティへの取り組みより不審者の侵入等の防犯への取り組みの優先順位が高くなっている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

ー防犯への取り組みー

- ・対応日：
- ・対応担当者：教員
- ・対応方法：

児童の登下校時間を決め、その時間のみ校門を開放し、それ以外は校門を閉じ、施錠している。

防犯カメラを活用し、不審者の侵入の対策を行っている。

児童と教員に対して、不審者侵入を想定した訓練を実施した。

◆今後の対策と効果

生徒への著作権指導 1

中学校での事例

◆被害状況

- ・被害や加害が発生しているわけではないが、著作権侵害を起こさないために教育を実施している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

－生徒への対応－

- ・対応日：11月～12月（論文作成の開始時）
- ・対応担当者：担任教員
- ・対応方法：

もともとは、論文を書くために必要な知識として授業を実施していたが、インターネットを活用した授業で様々なデジタルデータを取り扱う機会があり、生徒が著作権侵害を起してしまう可能性があるため、著作権についての授業を実施している。

－教職員への対応－

- ・対応日：
- ・対応担当者：教頭
- ・対応方法：

教職員が著作権についての最新情報を取得できるように要点をまとめた資料を配布したり、勉強会を開催したりしている。

◆今後の対策と効果

生徒への著作権指導 2

高等学校での事例

◆状況

- ・学校の授業でデジタルプレゼンテーションやレポートを作成する機会が増加した。それに伴い、生徒がデジタルデータを扱う機会も増加している。
- ・デジタルデータは複製が容易に行えるため、生徒が作成するプレゼンテーション資料やレポートには、Web ページや他の生徒が作成した資料やレポートをそのまま複製して提出しているものもある。
- ・Web サイトやブログで情報発信をする生徒もいるので、著作権侵害を起こさないための指導が必要と認識している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

－生徒への対応－

- ・対応日：
- ・対応担当者：教員
- ・対応方法：

情報の授業や調べ学習の時間に、著作権をテーマとして取り扱っている。

情報の授業では、外部に発信する Web ページ作成の時間に必ず著作権の内容を取り扱っているが、生徒の意識は希薄なままと感じている。

生徒の意識を向上させ、著作権侵害を起こさないための指導方法が今後の検討課題である。

◆今後の対策と効果

ファイル交換ソフト使用の指導

中学校での事例

◆被害状況

- ・家のパソコンでファイル交換ソフトを利用し、データ交換を行っていたところ、著作権関係団体からファイル交換ソフトの利用をやめるよう警告のメールが届いた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：メールが届いた生徒と雑談中に判明した。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

ー生徒への対応ー

- ・対応日：事実確認日
- ・対応担当者：パソコンの授業担当教員
- ・対応方法：
どのような内容のデータを交換していたか聞き出し、著作権侵害にあたるデータ交換は行わないよう指導をした。

◆今後の対策と効果

- ・パソコンの授業時に著作権の内容を紹介し、モラルを守って利用するよう指導を行うことにした。

Web サイトへの掲載情報についての指導

高等学校での事例

◆被害状況

- ・学校の Web サイトは公開用と校内専用があり、校内専用の Web サイトには、生徒が作成した Web ページが多数公開されている。教員の指導もあり、個人を誹謗・中傷する内容や著作権に反する画像や内容は公開されていない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- －校内のパソコン環境－
 - ・校内 LAN が整備されている。
- －校内のパソコン利用状況や利用形態－
 - ・生徒はパソコン教室のパソコンから教員が撮影したデジタル画像を自由に持ち出しできる。
- －校内のセキュリティ対策－
 - ・校内専用の Web サイトは学校外から閲覧できないようにしている。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 15 年～
- ・発見日：
- ・事実確認：

◆被害への対応

- －生徒への対応－
 - ・対応日：
 - ・対応担当者：
 - ・対応方法：

学校生活での出来事をデジタルカメラで撮影し、校内のみで公開することを生徒に口頭で伝えている。

校内で公開されているデジタル情報は、生徒が自由に閲覧・取得できる状況になっているので、デジタル情報を利用する際には、著作権や肖像権へ配慮するよう指導を徹底している。

◆今後の対策と効果

- ・今後も、生徒自身が善悪の判断や情報の真偽を判断できるように著作権や情報モラル指導を継続してしっかりと行っていく。

教員向け著作権講習会の開催

高等学校での事例

◆状況

- ・情報や総合的学習の時間などの授業で生徒がデジタルデータを扱う機会が多くなったこともあり、生徒に著作権を侵害しないように指導している。
- ・一方で、生徒に著作権を指導する立場の教員が、パソコンのソフトウェアの貸し借りをしたり、教材を無断で使用したりするなど日常的に著作権侵害行為を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：教員の著作権への認識が甘い現状を鑑み、意識を向上する必要があった。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

－教員への対応－

- ・対応日：平成17年
- ・対応担当者：情報担当教員
- ・対応方法：

教員の著作権への認識が甘く、生徒指導にも悪影響を及ぼすことも考えられるので、情報担当教員が管理職と相談して全教員に対して著作権への意識向上を図る講習会を開催することとした。

講習会は、情報担当教員が講師となり、著作権情報センターが無料配布している冊子をテキストとして使用した。

－著作権情報センター 無償パンフレット－
<http://www.cric.or.jp/mushou/mushou.html>

◆今後の対策と効果

- ・今後も継続して教員の著作権への意識向上を図っていく。

ユーザ ID とパスワードの貸し借り防止対策 1

高等学校での事例

◆状況

- 多数の教科でパソコンを利用する機会がある。生徒が学校のパソコンを利用するためには、ユーザ ID とパスワードが必要となるが、パスワードを忘れる生徒も多い。
- 生徒がパスワードを忘れた場合、パスワードを情報担当教員が再発行していたが、多数の教科でパソコンを利用する状況でありパスワードの再発行を即座に行うことが現実的に難しい状況となっている。また、生徒同士でユーザ ID やパスワードの貸し借りを行うことも十分考えられたので、パスワードを忘れた生徒への対応を検討する必要があると認識している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- 生徒は授業時のみパソコンを利用することができる。

◆経緯

- 発見方法：
- 発生日時：
- 発見日：
- 事実確認：

◆対処方法

ーパスワードの管理方法ー

- 対応日：平成 18 年 4 月
- 対応担当者：情報担当教員
- 対応方法：

パスワード忘れを防ぐために、「パスワード作成ポリシー」に基づき、生徒自身にパスワードを設定させている。

本来は生徒が各自で管理することが望ましいことなのだが、自分で設定したパスワードを忘れてしまう生徒もいるので、設定したパスワードを紙に書いて情報担当教員に提出させている。

提出したパスワードは、ファイルに綴り、パソコン教室の鍵の掛かる引き出しで保管し、パソコン室を利用する教員であればすべての生徒のパスワードを確認できるようにしている。

◆今後の対策と効果

- 生徒同士でのユーザ ID とパスワードの貸し借りは発生していない。

ユーザ ID とパスワードの貸し借り防止対策 2

高等学校での事例

◆状況

- ・パソコン教室のパソコンを利用するすべての生徒にユーザ ID とパスワードを付与すると、パスワードを忘れる生徒がでてくることが考えられる。
- ・また、パスワードを忘れた生徒には、パスワードの再発行を行う必要が生じるが、セキュリティ上パスワードの再発行をできる教員は限定されるべきで、パスワードの再発行を即座に実施することは現実的に難しい状況である。
- ・さらに、生徒同士によるユーザ ID やパスワードの貸し借りが行われることも懸念される。
- ・しかしながら、ユーザ ID やパスワードの重要性を生徒に指導する必要もある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・パソコン教室のパソコンは、授業時のみの利用としている。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

ー生徒への対応ー

- ・対応日：毎年3月下旬
- ・対応担当者：情報担当教員
- ・対応方法：

ユーザ ID とパスワードを付与するのは、必修科目の情報を受けている生徒と選択で情報を履修している生徒のみとし、ユーザ ID とパスワードの有効期限を1年間とすることとしている。

情報担当教員が新規のユーザ ID とパスワードを作成し、パスワードの再発行も情報担当教員のみが対応するようにしている。

情報の授業以外にパソコン教室のパソコンを利用する際は、パソコンに設定してあるゲストアカウントを利用してパソコンを使用できるようにしている。

パソコン教室のパソコンは授業時のみの利用としているため休み時間や放課後には利用できない。しかしながら、休み時間や放課後にパソコンを利用することもあるので、ゲストアカウントを利用して使用できるパソコンを図書室に4台設置し、生徒がいつでも利用できるようにしている。

◆今後の対策と効果

- ・生徒によるユーザ ID やパスワードの貸し借りも行われておらず、運用上の不都合も生じていないので、当面、継続する。

ユーザ ID とパスワードの貸し借り防止対策 3

高等学校での事例

◆状況

- ・平成 18 年度から、生徒に学校のパソコンを利用する際のユーザ ID とパスワードを付与している。
- ・情報の授業以外でも生徒がパソコンを利用することがあり、ユーザ ID とパスワードを忘れた場合、生徒同士によるユーザ ID やパスワードの貸し借りを行うことも想定されるので、パスワードを忘れた場合に教員がすばやく対応できる方法を検討している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—管理対策—

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

生徒がユーザ ID とパスワードを忘れる可能性があるため、情報の初回の授業時に、ユーザ ID とパスワードを紙に印刷して配付している。配付したユーザ ID とパスワードは重要な個人情報なので、取り扱いについては各自でしっかり管理するように指導している。

また、パソコンを利用する際に生徒がパスワードを忘れた場合には、必ず教員にパスワードを確認することになっている。

情報の授業では、情報担当教員がパスワードを確認しすぐに生徒に伝達している。また、総合的な学習の時間でパソコンを利用する際は、情報担当教員がすぐに対応できるようにするために、情報担当教員が総合的な学習の時間の授業に立ち会うようにしている。

◆今後の対策と効果

- ・今のところ生徒同士によるユーザ ID とパスワードの貸し借りは行われていない。今後もユーザ ID とパスワードを適切に管理するように生徒に指導していく。

ユーザ ID やパスワードの管理指導 1

高等学校での事例

◆被害状況

- ・生徒が他の生徒のユーザ ID やパスワードを不正に利用したということはないが、ユーザ ID やパスワードの管理について指導を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・校内 LAN が整備されている。
- ・全生徒にパソコンを利用するためのユーザ ID とパスワードを付与している。

ー校内のセキュリティ対策ー

- ・生徒に付与している初期発行パスワードは、校内のパスワード発行ルールに基づき 6 桁以上の英数字を利用している。

◆発見の経緯

◆被害への対応

ー生徒への指導ー

- ・対応日：毎年 4 月
- ・対応担当者：情報担当教員
- ・対応方法：

1 年次に必修となっている情報の授業の早い時期に、校内のパソコンを利用する際のユーザ ID とパスワードの管理について指導を行っている。特にパスワードにおいては、初期発行パスワードの変更方法と変更する際のルールについて指導を行っている。

本来は生徒が初期発行パスワードを変更し暗記して管理することが望ましいことだが、初期発行パスワードをそのまま利用するケースが多々ある。また、初期発行パスワードがランダムな英数字で覚えにくく、紙に書いて管理するケースがみられるので、生徒の所持率が高い携帯電話のメモ機能等を利用して他人に盗み見されるリスクが少なくなる状況でパスワードを管理するよう指導している。

◆今後の対策と効果

ユーザ ID やパスワードの管理指導 2

高等学校での事例

◆被害状況

- ・学校設備の変更に伴い、平成 16 年度より全生徒にパソコンを利用する際のユーザ ID とパスワードを付与しており、生徒が適切な管理を行えるように指導する必要があった。
- ・パソコンを利用する際にユーザ ID とパスワードを利用することに慣れていない生徒が多いので、情報の授業時にユーザ ID とパスワードの利用方法の指導を行うとともに、あわせてユーザ ID とパスワードを適切に管理するように指導を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境

- ・全生徒にユーザ ID とパスワードを付与している。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 16 年
- ・発見日：平成 16 年
- ・事実確認：

◆被害への対応

ー生徒への対応ー

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

情報の授業時に生徒個別のユーザ ID とパスワードを記載した紙を生徒に配布し、操作方法を指導した。あわせて、パスワードの変更方法も指導し、その場で初期発行パスワードを変更させている。変更時には、他人が推測しやすいものや辞書等に載っている英単語を利用せず、ランダムな英数字で 8 桁のパスワードを作成するよう指導している。

また、ユーザ ID とパスワードを不正に利用した犯罪（不正アクセス禁止法への違反）や検挙事例を紹介し、ユーザ ID とパスワードを適切に管理するように指導した。

◆今後の対策と効果

- ・インターネット上で Web メールやインターネットオークションなどのさまざまなサービスを利用する際に、本人確認の手段としてユーザ ID とパスワードが用いられることが多い。特にインターネットオークションなどではユーザ ID とパスワードを不正に利用した詐欺事件なども発生しており、生徒がインターネット上で被害者にも加害者にもならないようするために、今後も継続的に指導していく必要がある。

ユーザ ID やパスワードの管理指導 3

高等学校での事例

◆状況

- ・生徒に個人情報を各自の責任で管理することを学ばせるために、学校で利用するパソコンにユーザ ID とパスワードを設定し、生徒に付与している。
- ・生徒は学校で使用するパソコンのユーザ ID やパスワードを安易に考えることが多く、パスワードを忘れてしまった場合に生徒同士でのユーザ ID やパスワードの貸し借りが行われることが考えられるので、情報の授業時にユーザ ID とパスワードを適切に管理するように指導する必要があると認識している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・生徒が自主的に学校のパソコンを利用して調査や作品作成ができるようにするために、放課後も学校のパソコン教室を開放している。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—生徒への対応—

- ・対応日：平成 18 年 4 月
- ・対応担当者：情報担当教員
- ・対応方法：

情報の授業は 1 年次に実施している。入学してすぐの授業で、生徒にパソコンを利用する際に必要となるユーザ ID とパスワードを紙で配布し、授業内で記憶させるようにし、配布した紙は回収している。

ユーザ ID とパスワードをしっかりと記憶して管理することも評価の対象としている。したがって、パスワードを忘れてしまった生徒は、パスワードを情報担当教員から伝えるが、パスワードを忘れた行為を減点の対象としている。

◆今後の対策と効果

個人所有パソコン利用教員へのコンピュータウイルス対策

高等学校での事例

◆被害状況

- ・教員が校務で利用するために、個人所有パソコンを学校に持込むことができるが、コンピュータウイルス感染が起こらないように個人所有パソコンを教職員用のネットワークに接続する場合のルールを定めている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・職員室は LAN 環境が整備されている。

ー校内のパソコン利用状況や利用形態ー

- ・教職員は職員室のパソコンを自由に利用できる。
- ・教職員は申請をすれば、個人所有パソコンの持込みができる。

ー校内のセキュリティ対策ー

- ・教職員用と生徒用のネットワークは物理的に分割しており、生徒用のネットワークから教職員用のネットワークへは侵入できないようにしている。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 15 年～
- ・発見日：
- ・事実確認：

◆被害への対応

ー個人所有パソコン利用教員への対応ー

- ・対応日：平成 15 年～
- ・対応担当者：校内のセキュリティ担当教員
- ・対応方法：

個人所有パソコンを利用する場合には、学校側に必ず申請をすることになっている。

利用するパソコンは、セキュリティ担当教員がウイルス対策ソフトの導入などの状況を確認する。

確認の際に、ウイルス対策ソフトを導入していてもリアルタイムで保護する機能が有効になっていない、ウイルス定義ファイルの自動更新が設定されていない、OS のパッチを当てていないなどの不備があれば、セキュリティ担当教員が個別に設定方法や利用方法などを指導する。

◆今後の対策と効果

- ・個人所有パソコンを利用することの是非はあるが、現在のところ個人所有パソコンの持込みによるウイルス感染は発生していない。

生徒の自宅パソコンへのコンピュータウイルス感染対処方法の指導

高等学校での事例

◆状況

- ・生徒が自宅で利用しているパソコンの動作が不安定になり、起動にあまりにも時間がかかるようになったので、生徒が情報担当教員に対処方法を相談してきた。
- ・生徒はウイルス対策ソフトを導入していない状態でインターネットを利用していたので、原因としてコンピュータウイルス感染の可能性を考えていた。
- ・起動に時間がかかるほかには目立った障害は確認されていない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：生徒から対処方法の相談があった。
- ・発生日時：平成 17 年
- ・発見日：平成 17 年
- ・事実確認：

◆対処方法

ー相談してきた生徒への対応ー

- ・対応日：相談されたその日から 1 週間程度
- ・対応担当者：情報担当教員
- ・対応方法：

生徒の相談内容からウイルス感染が考えられたのでウイルスチェックをするように指導する必要があった。しかし、生徒のパソコンにはウイルス対策ソフトが未導入だったので、オンラインでウイルスチェックができる Web サイトを紹介し、ウイルスチェックをするように指導した。

生徒が Web サイトでウイルスチェックを実施したところ、ウイルス感染していることが判明したため、後日、感染したウイルスへの対処方法についての相談をしてきた。紹介した Web サイトではウイルスを駆除することはできなかったため、保護者と相談してウイルス対策ソフトを導入するようにアドバイスをした。

◆今後の対策と効果

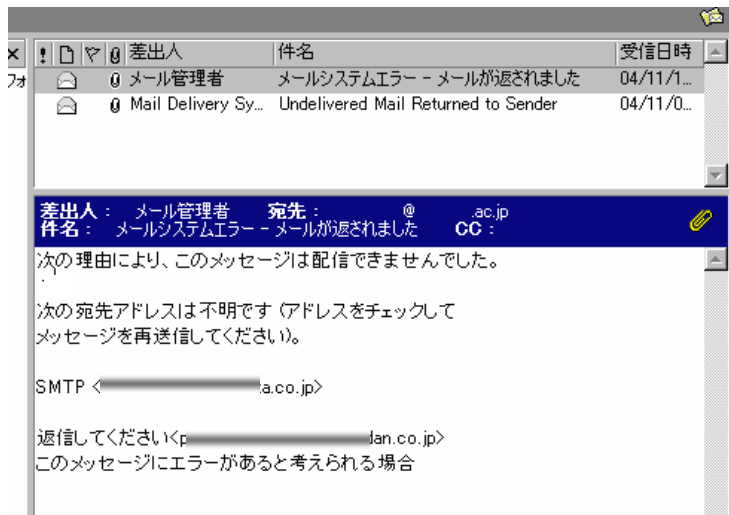
- ・情報の授業では、時間の制約等もあり個別の事象に対応することは難しい状況である。現状では、生徒からの相談は個別に対応している。

コンピュータウイルス感染を誘う手口

専門学校での事例

◆被害状況

- ・宛先不明の電子メールの返信を装い、あたかも自分が出したような錯覚を起こさせる電子メールが届いた。
- ・ファイルが添付されており、ウイルスチェックによりウイルス感染していることがわかり削除したため、被害には至っていない。



※ここでは、内容を併せて表示するため、あえてプレビューウィンドウを利用した。通常はウイルス感染を防ぐためにも利用しないほうが望ましい。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 16 年 11 月
- ・発見日：
- ・事実確認：

◆被害への対応

— 学生への対応 —

- ・対応日：
- ・対応担当者：教員
- ・対応方法：

教員が管理するメールアドレスにウイルス感染したメールが届いた。ウイルス感染を誘発する手口として巧妙であったため、学生への注意・指導題材とした。

◆今後の対策と効果

- ・ウイルスは、巧妙に様々な形態をとりながら感染を仕掛けてきている。教員が体験する具体的な事例を学生に情報提供することが必要と考えている。

料金の架空請求メールへの指導

高等学校での事例

◆被害状況

- ・料金の架空請求メールが横行しており、生徒が利用しているパソコンや携帯電話の電子メールアドレスに料金の架空請求メールが届く可能性もあるので、生徒が被害に遭わないよう指導する必要がある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒の保護者宛に届いた料金の架空請求のハガキを生徒が教員に届けた。また、架空請求に関してメールリングリストを利用して大学の先生に高校生向けの解説を書いてもらい、授業で利用している。
- ・発生日時：平成 16 年 12 月
- ・発見日：平成 16 年 12 月
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成 16 年 12 月
- ・対応担当者：情報担当教員
- ・対応方法：

生徒の保護者宛に送られてきた「電子消費者契約通信未納利用料請求最終通告書」の文面を教材として提示し、実際にハガキや電子メールで料金の架空請求が行われた場合の対応方法について指導した。

あわせて、携帯電話やパソコンで利用している電子メールにも料金の架空請求メールが届く可能性があることを伝え、その手の電子メールが届いた場合には無視するよう指導した。指導に当たっては、メールリングリストを利用して大学の先生に、不正請求の何がおかしいのかを解説してもらった文章も利用している。

◆今後の対策と効果

振り込め詐欺や料金の架空請求メールへの指導

高等学校での事例

◆被害状況

- ・振り込め詐欺の新たな手口の一つとして、大学の名を騙り入学金や授業料を要求する事件が発生し、報道されている。振り込め詐欺と思われる内容の電話を受けた保護者から事の真偽を確かめる連絡が学校に入った。大学受験を控えた3年生が同様の被害をうけることも想定されるので、注意を喚起する必要があった。
- ・振り込め詐欺以外にも料金の架空請求メールやフィッシングメールが横行しているので、あわせて注意することとした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成17年
- ・発見日：平成17年
- ・事実確認：平成17年

◆被害への対応

—生徒への対応—

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：

受験期を控えた3年生に対して、入学手続き等に関する振り込め詐欺の被害に遭わないために、必ず事の真偽を確かめる連絡をするように指導を行った。

料金の架空請求メールやフィッシングメールなどが横行しているので、この手のメールが届いた場合には、メールを無視するように指導を行った。

◆今後の対策と効果

- ・授業で情報モラルの指導を行っているが、今後も生徒が被害に遭わないように適宜、最新の情報を提供するように努めていく。

迷惑メールへの指導

高等学校での事例

◆被害状況

- ・電子メールを題材とした情報の授業時に、架空請求メールなどの迷惑メールをどの程度生徒が受信しているのか、情報担当教員の質問に対して生徒が挙手により回答する方法で状況把握を行った。
- ・その結果クラスの6～7割の生徒が何らかの迷惑メールを受け取っており、架空請求メールの被害に遭う可能性もあるので、架空請求メールの被害事例や対策などを紹介している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成15年
- ・発見日：平成15年
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成16年度の授業から
- ・対応担当者：情報担任教員
- ・対応方法：
授業時に生徒の状況を把握し、生徒のもとに多数のメールが届いていることを確認してから、架空請求メールの被害事例や対応事例を紹介している。その際、まとめて1時間の授業を実施するのではなく、各授業の導入段階の話としてトピック的に紹介している。

◆今後の対策と効果

- ・平成17年度より、携帯電話のショートメール機能を利用したワンクリック詐欺などの事例も取り入れ、生徒が被害に遭わないよう、常に新しい話題を提供するようにしている。

架空請求メールやワンクリック詐欺への指導

高等学校での事例

◆被害状況

- ・社会的に携帯電話を利用した架空請求メールやワンクリック詐欺が多発している。生徒が架空請求メールやワンクリック詐欺の被害に遭ったという報告はないが、多くの生徒が携帯電話を所有しており被害に遭う可能性があるため、情報の授業を受けている1年生を対象としてそれらの被害に遭わないよう指導を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：報道や教育委員会からの連絡等により、生徒への指導の必要性を感じた。
- ・発生日時：平成16年
- ・発見日：
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：平成17年6月・9月
- ・対応担当者：情報担当教員
- ・対応方法：

授業を受けている1年生は、入学当初は携帯電話を所持していない生徒もいるので、多くの生徒が携帯電話を所持する時期（夏休み前ぐらい）に架空請求メールやワンクリック詐欺の被害に遭わないための授業を実施している。

授業では教員のもとに届いた架空請求メールを生徒に見せたり、神奈川県警のWebサイトに掲載されている事例を紹介したりして指導している。

◆今後の対策と効果

- ・携帯電話を所持している生徒同士で情報交換をしているので、架空請求メールやワンクリック詐欺についてのある程度の対応方法を認識している生徒は多いが、授業を通じて事例や対応方法を紹介すると生徒同士の不確かな情報共有だったものが生徒の知識として理解が深まる手ごたえを感じている。

フィッシング詐欺やワンクリック詐欺への指導

高等学校での事例

◆状況

- ・フィッシング詐欺やワンクリック詐欺の被害が新聞報道などで大きく取り上げられており、生徒がフィッシング詐欺やワンクリック詐欺等の被害にあわないための指導を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—生徒への対応—

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

Web サイトや雑誌、教員が自宅でアクセスしたフィッシング詐欺やワンクリック詐欺を試みようとするサイトの画面を印刷物として配付してフィッシング詐欺やワンクリック詐欺への注意を促している。フィッシング詐欺に関しては、個人情報を安易に入力しないこと、個人情報を聞き出そうとするメールが届いても無視することを指導している。また、万メールに記載されている URL をクリックしても、個人情報を入力しないように指導している。ワンクリック詐欺に関しては、一度クリックしただけで料金が請求されても、安易に支払いに応じずに、教員や保護者に相談するように指導している。

◆今後の対策と効果

巧妙な呼び込みメール

専門学校での事例

◆被害状況

- ・特に被害はないものの、学生から最近の迷惑メールの手口として以下のようなメールが届いた旨、情報提供された。

件名：アドレスの確認お願いします (*^-^)

内容：彼女さんへのメールなのかな?? 間違ってメールが届いてるみたいですよ… 私の携帯宛てに届いてたんですけど、パソコン からお返事させていただきました。でわでわ～

+-----+

チヒロ

e-mail 【*****@yahoo.co.jp】

+-----+

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒からの情報提供。
- ・発生日時：平成 16 年 9 月
- ・発見日：同日
- ・事実確認：同日

◆被害への対応

－学生への対応－

- ・対応日：
- ・対応担当者：担当教員
- ・対応方法：
 - うっかり自分が間違いメールを出したと勘違いし、相手のメールアドレスにメールを送ると宣伝メールなどが届くようになることが予想される。
 - このため、こういった身に覚えのないメールなどや少しでも疑問を感じたメールには、極力慎重に対応するよう指導した。

◆今後の対策と効果

- ・今後とも不審なメールについては、徹底的に無視することを指導する。
- ・ささいなことでも構わないので教員に連絡するようにあらためて指導した。

振り込め詐欺への注意喚起

中学校での事例

◆被害状況

- ・ 架空請求メールが横行しており、高校の受験時期を控え、振り込め詐欺の被害の発生が想定されたので、手口を記載したプリントを配布し、注意を喚起した。
- ・ 幸いなことに、振り込め詐欺の被害は発生していない。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：教育委員会から振り込め詐欺についての注意を促す文書が届いた。
- ・ 発生日時：平成 17 年 1 月
- ・ 発見日：平成 17 年 1 月
- ・ 事実確認：

◆被害への対応

—生徒への対応—

- ・ 対応日：平成 17 年 1 月
- ・ 対応担当者：担任教員
- ・ 対応方法：
想定される振り込め詐欺の手口等を記載したプリントを配布し、生徒に注意を促すとともに、保護者に手渡すように連絡した。あわせて、架空請求メールやフィッシングメールについても横行しているので、この手のメールが届いても、すぐに対応せず、無視するように指導した。

◆今後の対策と効果

架空請求メールへの注意喚起

高等学校での事例

◆被害状況

- ・平成 16 年度に、生徒から架空請求メールの相談が 2 件あった。
- ・いずれの相談も、料金を振込む前の相談で、金銭的な被害は発生しなかった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒から相談により判明した。
- ・発生日時：平成 16 年
- ・発 見 日：平成 16 年
- ・事実確認：

◆被害への対応

－相談のあった生徒への対応－

- ・対 応 日：相談があったその日
- ・対応担当者：生活指導担当教員
- ・対 応 方 法：

生活指導担当教員が生徒からの相談に応じ、身に覚えのない請求であれば請求を無視するようアドバイスを行った。

－全生徒への対応－

- ・対 応 日：
- ・対応担当者：生活指導担当教員・担任教員
- ・対 応 方 法：

生活指導担当教員が社会的に架空請求メールが横行している状況について、担任教員を通じて生徒に注意喚起を行うことにした。

その日のホームルームを利用して、各担任教員から生徒に身に覚えのない架空請求メールには応じないよう注意喚起を行った。

◆今後の対策と効果

- ・すべての被害状況等を把握しているわけではないが、生徒が架空請求メールに応じ、金銭的な被害を受けたとの報告はない。

出会い系サイト利用指導 1

中学校での事例

◆被害状況

- ・ 出会い系サイトを利用した被害や加害は発生していないが、生徒が出会い系サイトの利用による犯罪の被害者・加害者にならないように指導する必要がある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・ 発見方法：
- ・ 発生日時：平成 17 年 2 月
- ・ 発見日：
- ・ 事実確認：

◆被害への対応

— 生徒への対応 —

- ・ 対応日：平成 17 年 2 月
- ・ 対応担当者：
- ・ 対応方法：
卒業前の 3 年生全員を対象に、外部の先生による性教育の特別授業を実施した。その中で、性犯罪に巻き込まれる危険性の高い出会い系サイトについて、実際の被害事例や加害事例を紹介し、出会い系サイトを利用しないように指導を行った。

◆今後の対策と効果

出会い系サイト利用指導 2

高等学校での事例

◆被害状況

- ・出会い系サイト規制法違反と詐欺の疑いにより中学3年の女子生徒が検挙された報道があった。援助交際の書込みに応じた男性社員に金額を振り振り込ませ詐取した疑いである。
- ・報道の内容より、自校の生徒が被害者にも加害者にもなりうる状況だという認識をもった。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：出会い系サイトによる被害ならびに加害例は発生していないが、生徒の認識不足により加害者になることを防止する必要があると判断した。
- ・発生日時：平成16年3月
- ・発見日：平成16年3月
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成16年5月
- ・対応担当者：情報担当教員
- ・対応方法：

生徒が出会い系サイトの利用による被害者・加害者にならないように授業で中学生が検挙された事例を紹介し、18歳未満の者の出会い系サイト利用は法律で禁止されていることと出会い系サイトに潜んでいる危険性を神奈川県警察ハイテク犯罪対策センター（<http://www.police.pref.kanagawa.jp/mes/mesd0015.htm>）のWebサイトを閲覧しながら指導した。

◆今後の対策と効果

Web サイトでの情報発信時における注意点の指導

高等学校での事例

◆状況

- ・パソコンや携帯電話を利用して Web サイトやブログによる情報発信をする生徒が増えてきている。しかし、生徒がインターネット上に発信する情報は、適切ではない情報も多くある。
- ・生徒が情報発信を行う際に、適切な情報を発信できるように指導する必要がある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・公開する Web は校内のみで閲覧可能な Web と校外からも閲覧可能な Web とを分けて管理している。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—生徒への対応—

- ・対応日：毎年4月
- ・対応担当者：情報担当教員
- ・対応方法：

単に座学での指導ではなく、情報発信を実際に行い、実体験に基づく指導をするようにしている。

導入は、入学して間もない1年生に自己紹介の Web ページを作成させ、校内のみで閲覧可能な状態にして公開し、情報発信する機会を設けている。その後は、情報の授業内容や他教科の授業内容を報告する Web ページを作成して校内のみで閲覧可能な状態として公開し、生徒が自ら Web ページによる情報発信を行うようにしている。

公開する情報は、1年間公開し続け、全校生徒が見ることを前提としているので、記載する内容も「公序良俗に反しないこと。他人を誹謗・中傷しないこと。電話番号等の個人情報掲載しないこと。」などの情報発信時の注意点を繰り返し指導している。

◆今後の対策と効果

- ・生徒が作成する校内のみで閲覧可能な Web サイト、並びに校外からも閲覧可能な Web サイトに他人を誹謗・中傷した書き込みをしたり、個人情報を記載したりする Web ページは作成されていない。

チャットの利用指導

高等学校での事例

◆被害状況

- ・放課後、チャットの運営者から学校に連絡がはいった。IPアドレスをもとに、発信元をつきとめ連絡したもので、チャット上、不適切な発言が学校より繰り返しあるとのことであった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

－学校のコンピュータ環境・利用状況－

- ・休み時間、放課後ともコンピュータ室のパソコンは自由に利用できる。

◆発見の経緯

- ・発見方法：チャット運営者からの電話連絡。
- ・発生日時：
- ・発見日：
- ・事実確認：チャット運営者からの電話連絡後すぐ。

◆被害への対応

－生徒への対応－

- ・対応日：
- ・対応担当者：担当教員
- ・対応方法：

教員がチャットをしている現場を見つけ、ただちに生徒にチャットをやめさせた。

また、チャット利用についてのマナー説明を行い、後日、校内でのチャット利用の禁止措置をすることとした。

◆今後の対策と効果

- ・その後、チャット利用についてのトラブルは起こっていない。

掲示板・チャットの利用指導

高等学校での事例

◆被害状況

- ・掲示板やチャットへのどのような書込みが、特定の個人を誹謗・中傷したり、公序良俗に反することなのかを理解していない生徒がいることが判明したため、モラル指導とともに、体験を通じてインターネットの技術的な仕組み等を理解させ、より適切に利用できるよう指導した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・パソコン教室は LAN 環境が整備されている。

ー校内のパソコン利用状況や利用形態ー

- ・パソコン教室は授業時以外の利用は禁止している。

ー校内のセキュリティ対策ー

- ・情報の授業時に掲示板やチャットの利用方法について指導している。

◆発見の経緯

- ・発見方法：ネチケットの授業中に具体的な質問が出た。
- ・発生日時：平成 16 年 11 月
- ・発見日：
- ・事実確認：実際に書込んでしまった内容で議論させた。

◆被害への対応

ー生徒への対応ー

- ・対応日：平成 16 年 11 月
- ・対応担当者：情報担当教員
- ・対応方法：

認識不足から誹謗・中傷する内容や公序良俗に反する内容を書込んでしまった生徒に対して、個別指導を実施した。

個別指導では、モラル指導とともに、インターネット利用は決して匿名ではなく、IP アドレスからパソコンが特定できることや、キーボードからの入力を監視して記録するソフトを利用して書込み内容を特定することができることなどを体験させ、インターネットの技術的な仕組みについても指導した。

◆今後の対策と効果

- ・モラル指導とともにインターネットの技術的な仕組みを理解させることにより、生徒が掲示板やチャットを利用する際、マナーを守るようになった。

体験学習による掲示板の利用指導

高等学校での事例

◆被害状況

- ・インターネットの掲示板を利用する際のマナーやモラルを生徒に指導した。
- ・実際にパソコン教室内のみで利用できる掲示板を設置し、生徒に自由に書込みをさせて後、指導を行った。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・校内 LAN が導入されている。

―校内のセキュリティ対策―

- ・生徒が利用するパソコンは、フィルタリングソフトにより掲示板の閲覧・書込みを禁止している。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 16 年度
- ・発見日：平成 16 年度
- ・事実確認：

◆被害への対応

―生徒への対応―

- ・対応日：平成 16 年度
- ・対応担当者：情報担当教員
- ・対応方法：

パソコン教室内のみで利用できる掲示板を設置し、生徒には実際の掲示板利用により近い形とするために生徒名が表示されないようにハンドルネームを配布後、生徒に自由に書込みをさせた。

教員もハンドルネームを利用し、掲示板の書込みに参加し、例として荒し行為や誹謗・中傷の書込みを煽るような書込みを行った。

教室内の体験実施後、生徒に掲示板を利用する際のルールやマナーについて指導を行った。

◆今後の対策と効果

- ・情報の授業を受けている 1 年生は、掲示板を閲覧する生徒は多いが書込みを実際に行う生徒は 2～3 割ぐらいである。授業においてはじめて掲示板への書込みを経験する生徒がほとんどなので、生徒にとってよい経験となっている。

掲示板サイトへの書込み巡回調査 1

高等学校での事例

◆被害状況

- ・有名な掲示板に当事者ならば特定可能な学校や個人についての書込みがあった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

－学校のコンピュータ環境・利用状況－

- ・休み時間や放課後にコンピュータ教室のパソコンは自由に利用できる。
- ・特に掲示板への書込みを禁止するなどの対策、措置を施しているわけではない。

◆発見の経緯

- ・発見方法：定期的な有名掲示板への巡回調査。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：
- ・対応担当者：担当教員
- ・対応方法：

実質的に被害があったわけではないが、掲示板への書込みが思わぬ事態を生み出す可能性があるため、有名な掲示板サイトなどを定期的に巡回し、学校や生徒にかかわる書込みの有無、内容を調査している。

◆今後の対策と効果

- ・今のところ被害やトラブルは発生していない。

掲示板サイトへの書込み巡回調査 2

高等学校での事例

◆状況

- ・過去に掲示板サイトで、生徒の個人名が書込まれたり、生徒や教員を誹謗・中傷する内容が書込まれたり、生徒の画像が無断で公開されたことがある。
- ・掲示板サイトに不適切な書込みがされるたびに、該当の掲示板サイトに削除依頼を実施している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

－掲示板への書込み巡回調査－

- ・対応日：毎朝授業が始まる前
- ・対応担当者：情報担当教員
- ・対応方法：

過去にトラブルがあった掲示板サイトをすべて記録している。

掲示板にいつ書込みが行われるかわからないので、情報担当教員が毎朝、過去にトラブルがあった掲示板サイトを巡回して、生徒や学校に関する書込みがされていないかの確認をしている。

掲示板は日々増えているので、1ヶ月に1回程度、検索サイトを利用して過去にトラブルがあった掲示板以外にも不適切な書込みが行われていないか調査している。

調査を行っている際に不適切な書込みがあった場合には、直ちに情報担当教員が掲示板の管理者に電子メールにより削除依頼を行っている。

◆今後の対策と効果

- ・調査は毎日実施しているので、過去に不適切な書込みが行われた掲示板サイトでの書込みは確実に減っている。しかし、すべての書込みに対して情報担当教員だけの調査・対応には限界もあるのでよい対応方法を模索している。

校内ネットワークフォルダの不正利用防止対策

高等学校での事例

◆状況

- ・各授業でパソコンを活用している。授業内容によっては、パソコンを利用した課題作成等があり、作成したデータはネットワークを通じて各授業の提出用のフォルダに提出させている。
- ・校内ネットワーク上にアクセス権限を設定せずに共有フォルダを作成しデータを提出させると、生徒の誤操作により他の生徒のデータが削除されたり、同じファイル名をつけたことにより上書きされたりすることが考えられる。また、他の生徒が作成したデータを閲覧したり、いたずら目的で書き換えたりすることも考えられる。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・生徒個々にユーザ ID とパスワードを付与している。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—生徒への対応—

- ・対応日：毎年4月
- ・対応担当者：情報担当教員
- ・対応方法：

各授業の課題提出用フォルダ並びにデータ配布用フォルダは、授業を選択している生徒以外がアクセスできないようにアクセス権限を設定している。

4月の履修登録終了後すぐに、ネットワークを管理している教員が履修登録のデータを基にフォルダのアクセス権限を設定している。

課題提出用フォルダは、授業を選択している他の生徒からの誤操作による削除や上書き、いたずら目的によるデータの書き換えを防ぐため、フォルダ内のファイルを開けないようにし、さらに上書き保存もできないような設定としている。

◆今後の対策と効果

- ・フォルダ内に提出されたデータが生徒の誤操作により削除されたり、上書きされたり、またいたずら目的によるデータの書き換えは発生していない。

校内パソコンのセキュリティ対策

高等学校での事例

◆状況

- ・校内で利用しているパソコンはインターネット利用が可能である。
- ・過去にウイルス感染や不正アクセスの被害に遭った経験はないが、OS のセキュリティパッチの未適用による被害事例が多くあるので、校内で利用しているパソコンの OS のセキュリティパッチを適用するようにしている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・校内に設置しているすべての生徒用パソコンと教員用パソコンから Web サイトの閲覧ができるようにしている。
- ・生徒が校内のネットワークを経由して教員用パソコンに接続することができないようにするために、生徒用と教員用のネットワークは分離している。
- ・教員が校務で使用するために学校に持ち込む私物パソコンは、校内ネットワークのセキュリティ確保のために接続を禁止している。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

ーセキュリティパッチの適用ー

- ・対応日：セキュリティパッチの情報が公開されたその日（1ヶ月に1回）
- ・対応担当者：情報担当教員
- ・対応方法：

職員室にあるパソコン 15 台と学校内のサーバ類は、セキュリティパッチの情報が公開されたその日のうちに情報担当教員が 1 台ずつ手動でセキュリティパッチをあてている。
生徒が利用しているパソコン 100 台は、ネットワークを利用して自動更新している。
セキュリティパッチの適用は授業の空き時間等を利用している。

◆今後の対策と効果

- ・OS のセキュリティパッチの未適用によるウイルス感染や不正アクセス等の被害は発生していないので、手間はかかるが今後も継続して実施していく。

生徒指導のためのアンケート調査

高等学校での事例

◆被害状況

- ・生徒が掲示板で構成された Web サイトを立ち上げたが、あるときから偽りの情報や誹謗中傷などが書き込まれるようになってしまい、さらには書込みをした個人を特定しようとする犯人探しの荒れ方に至った。
- ・個人に対する実名をあげた誹謗中傷や荒れ方から今後、書込みをした犯人を呼び出そうといった現実の暴力行為などを危惧し、対応を迫られることとなった。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：生徒の会話により判明した。
- ・発生日時：平成 17 年 5 月中旬
- ・発見日：平成 17 年 6 月
- ・事実確認：

6 月中旬頃、教員がたまたま耳にした生徒の会話から主に携帯電話からのアクセス利用による（PC 利用も可）生徒が運営していると思われる学校をテーマとした Web サイトの存在が明らかになった。Web サイトは 5 月中旬に作成されたようで、複数のフリー掲示板によって構成されており、誹謗中傷の書き込みや実名の書き込みも確認された。主に 1、2 年生の利用が中心となっており、口伝えで利用が広まっていったことが確認された。

◆被害への対応

ー生徒への対応ー

- ・対応日：平成 17 年 7～8 月
- ・対応担当者：
- ・対応方法：

掲示板削除へ向けた対応（別掲）と同時に、情報社会を生きてゆく生徒をどのように教育し、人権感覚やネット社会の特性などを理解させていくための基礎データを収集するためにアンケート調査を行うこととした。

調査内容は、

 - インターネットへのアクセス状況（利用有無、利用開始時期、利用サービス）
 - 電子メール利用状況（利用有無、送受信相手）
 - インターネット被害（精神的、金銭的）
 - 個人情報入力有無
 - インターネットにおける交友関係（有無）
 - メール・掲示板でのトラブル（有無）
 - トラブルの相談（有無、相手）
 - 個人特定の認識（メール、プロバイダ、IP）
 - なりすまし・盗聴の認識
 - トラブルの認識・損害請求の認識

◆今後の対策と効果

アンケート調査結果は、職員会議で報告し、教員全員で情報共有を行った。今後、生徒全員からの調査データをもとに指導方法等を検討し、実施していく。

生徒のインターネット被害状況の把握

高等学校での事例

◆被害状況

- ・生徒がインターネットを利用した犯罪等に巻き込まれた報告はないが、多くの生徒が携帯電話やパソコンを利用してインターネットを利用しており、また、携帯電話を利用した架空請求メールやワンクリック詐欺の被害が報道されている状況を踏まえ、生徒の携帯電話とインターネットの利用状況の把握を行った。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 17 年 6～7 月
- ・発見日：平成 17 年 6～7 月
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成 17 年 6～7 月
- ・対応担当者：情報担当教員
- ・対応方法：

情報の授業時に、情報セキュリティをテーマとした授業を実施し、生徒自身が被害にあった事例や新聞やテレビで報道されたセキュリティに関する事件・事故について、被害の状況とどのような対策が有効なのかを考えさせてレポートを提出させた。

提出されたレポートには、実際に金銭的な被害は発生していないものの、携帯電話における架空請求メールやワンクリック詐欺を経験したことがある生徒が多数いることが判明した。

また、パソコンや携帯電話の電子メールアドレスへのスパムメールについても多くの生徒が体験している状況が判明した。

◆今後の対策と効果

- ・生徒の状況をある程度把握できた点についてはよかったが、今後は、実際の被害に遭わないための指導を行っていく必要があり、効果的な授業内容を検討している。

常時接続環境によるインターネット利用への注意喚起

高等学校での事例

◆状況

- ・情報の授業を利用して生徒の自宅でのインターネット利用状況について確認したところ、ほとんどの生徒が自宅にあるパソコンでインターネットを利用している状況であった。また、多くの生徒のインターネットへの接続環境は ADSL 等を利用した常時接続であることも判った。
- ・学校のパソコンはセキュリティ対策が実施されていて、学校でパソコンを利用するときにはセキュリティ対策をほとんど意識することがない。同様の意識で生徒が自宅でインターネットを利用していると気づかぬうちに犯罪被害に巻き込まれる可能性があり、生徒が自宅でパソコンを利用するときにもセキュリティ対策を実施したうえで利用できるようにするための指導が必要と感じている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：生徒が自宅でインターネットを利用する際に不正アクセス等の被害に遭わないようにするための対策を生徒に指導する必要があると判断した。
- ・発生日時：平成 17 年 4 月
- ・発見日：
- ・事実確認：

◆対処方法

ー生徒への対応ー

- ・対応日：平成 17 年 5 月
- ・対応担当者：情報担当教員
- ・対応方法：
 - ネットワークを通じてパソコンが簡単に遠隔操作されてしまうことを理解してもらうために、学校のパソコン教室で生徒が利用するパソコンを教員が遠隔操作する様子を実際に見てもらっている。
 - 常時接続の環境では、インターネットを利用していないときでもパソコンと LAN ケーブルが常に繋がっているケースが多いので、インターネットを利用していない時には、インターネットに接続しないようにしておき、さらに LAN ケーブルも抜いておくと安全だということを指導している。あわせて、自宅のパソコンで利用している OS のセキュリティパッチをあてるように指導している。

◆今後の対策と効果

情報教育の依頼

小学校での事例

◆被害状況

- ・長崎県佐世保の小学校6年生児童殺傷事件により父兄より掲示板やWebサイトをはじめとするインターネットの使い方などを指導して欲しいという要望が寄せられた。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：父兄からの相談。
- ・発生日時：平成16年6月
- ・発見日：
- ・事実確認：

◆被害への対応

ー父兄・児童への対応ー

- ・対応日：
- ・対応担当者：教員
- ・対応方法：

小学校では、現在特定の児童が参加するパソコンクラブは存在するものの、すべての児童がパソコンを利用し、インターネットを活用するところまでには至っていない。そのため、情報教育が小学校の教育の範疇にあたるとは必ずしも考えられないところもあり、また正規の授業時間数との兼ね合いもあり、家庭で父兄から教育を行って欲しいということとなった。

◆今後の対策と効果

- ・パソコン利用などの安全面、モラル面での教育は、解決しなければならない課題であると認識している。

情報モラル指導 1

小学校での事例

◆被害状況

- ・長崎県佐世保の小学校 6 年生児童殺傷事件発生後、事件と同学年である 6 年生に対して、情報モラルの特別授業を実施した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：事件の影響を考慮し、児童に情報モラルの指導をする必要があると判断した。
- ・発生日時：事件報道から 2 週間後
- ・発見日：平成 16 年 6 月 1 日
- ・事実確認：

◆被害への対応

ー児童への対応ー

- ・対応日：
- ・対応担当者：担任教員
- ・対応方法：
事件を起こした同学年である 6 年生に対して、情報モラルについての授業を実施した。
報道されている内容をもとに、掲示板・チャット・電子メールなどネットワークでのコミュニケーションについての問題点や注意点を確認した。

◆今後の対策と効果

- ・特別授業を実施することで、児童のインターネットの利用状況が把握できた。
- ・今後も継続してモラル教育が実施できるよう検討している。

情報モラル指導 2

中学校での事例

◆状況

- ・インターネット利用者の低年齢化を鑑み、今までは中学2年生以上を対象に実施していた情報モラル指導を平成18年度からは中学1年生に対しても実施することとした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：インターネット利用者の低年齢化により中学1年生に対しても指導する必要性があると判断した。
- ・発生日時：平成18年4月
- ・発見日：
- ・事実確認：

◆対処方法

－生徒への対応－

- ・対応日：平成18年4月
- ・対応担当者：情報担当教員
- ・対応方法：

小学生の頃よりインターネットを利用している生徒が増えてきており、中学生であってもインターネットのトラブルに巻き込まれる可能性があるため、トラブルに巻き込まれないために入学して間もない中学1年生に情報モラル指導を実施することとした。

1年生全員を同じ教室に集め、Webサイトや電子メールを利用してトラブルに巻き込まれない指導を講義形式で行った。

最近は、ブログを利用して情報発信をしている生徒もいるので、特に個人情報や他人を誹謗・中傷するような情報を書込まないように指導した。

◆今後の対策と効果

- ・今後も、生徒がインターネットを利用したトラブルに巻き込まれないための知識を身につけるための指導を継続していく。

情報モラル指導 3

高等学校での事例

◆被害状況

- ・商業系に在籍している生徒は、授業時に情報機器を扱うことが多く、知識・技術の両面から情報モラルを習得する必要があるため、徹底して指導を行っている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・パソコン教室のパソコンはインターネットに接続できるが、教育委員会ネットワークのフィルタリングを通った Web サイトのみ閲覧できる。

―校内のセキュリティ対策―

- ・過去のシステムでは閲覧できる Web サイトを制限するため、フィルタリングソフトを導入していたが、現在はすべて教育委員会ネットワークのフィルタリングを通すシステムに変更された。
- ・ウイルス対策ソフトを導入している。
- ・過去にはログ管理を行い、アダルト系サイトなど学校からの閲覧には適さないサイトへ接続していないか定期的にチェックをしていたが、現在はすべて教育委員会ネットワークのフィルタリングを通すシステムに変更されたので、チェックは実施していない。

◆発見の経緯

◆被害への対応

―生徒への対応―

- ・対応日：
- ・対応担当者：教科担当教員
- ・対応方法：

商業系に在籍している生徒には、1年次に Web サイトの利用方法・電子メールの書き方・出会い系サイトなどの情報モラルに関する指導を行っている。

商業系に在籍している生徒で、情報処理関係の授業を選択している生徒には、3年次にネットビジネスに関する知識として、ネットオークションや電子商取引についての授業を実施している。しかし、現在では教育委員会ネットワークのフィルタリングがかかっているため、実際にネットオークションや電子商取引についての Web サイトを閲覧することができない。よって授業にさらなる工夫が必要となっている。Web サイトの利用にあたり、インターネットには影の部分があることを紹介し、アダルト系サイトなどの不適切な情報等が表示された場合の対処方法について事例を交えながら指導を行っている。

◆今後の対策と効果

情報モラル指導 4

高等学校での事例

◆被害状況

- ・生徒は授業時や放課後に学校のインターネットに接続しているパソコンを利用できるので、生徒一人一人がインターネット上のモラルやマナーを守って利用するように指導する必要がある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン利用状況や利用形態―

- ・パソコン教室のパソコンは放課後に生徒が自由に利用できる。

◆発見の経緯

- ・発見方法：
- ・発生日時：4月～5月
- ・発見日：
- ・事実確認：

◆被害への対応

―生徒への対応―

- ・対応日：4月～5月
- ・対応担当者：情報担当教員
- ・対応方法：

情報の授業において情報セキュリティや情報モラルについては、できるだけ早い指導が必要であるとの認識のもと、年度の早い時期の4月～5月にかけて実施している。

パソコン教室を放課後に開放しているので、パソコン教室の利用ルールと利用マニュアルを学校独自に作成し、生徒に配布し、ルールを守って利用するように指導している。

◆今後の対策と効果

インターネットの安全利用指導 1

高等学校での事例

◆被害状況

- ・架空請求メールやフィッシング詐欺などインターネットを利用した事件が多発している状況から生徒への安全教育を実施することとした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン環境ー

- ・パソコン教室は LAN 環境が整備されており、インターネットの利用は可能となっている。
- ・コンテンツフィルターをかけている。

ー校内のパソコン利用状況や利用形態ー

- ・パソコン教室の授業時以外の利用は禁止している。

◆発見の経緯

- ・発見方法：昨今の報道より、インターネットを安全に利用するための知識を習得させる必要があると判断した。
- ・発生日時：平成 16 年 11 月～12 月
- ・発見日：
- ・事実確認：

◆被害への対応

ー生徒への指導ー

- ・対応日：平成 17 年 1 月
- ・対応担当者：情報担当教員
- ・対応方法：

情報担当教員が外部機関主催の安全教育セミナー資料を用いて授業を実施した。

インターネットを安全に利用するための知識を確実なものにするために、生徒をいくつかのグループに分けたうえで利用した資料にある事例の問題点、注意点、対応策を討議させた後、教員が解説を行った。また、事前の知識と解説後の理解度を確認するための問題を解説の前後に実施した。

◆今後の対策と効果

- ・授業の実施前後に実施した確認問題の結果分析を行うことにより、生徒の現状を把握することができたうえ、生徒同士の討議により理解度が深まった。

インターネットの安全利用指導 2

高等学校での事例

◆状況

- ・架空請求メールやフィッシング詐欺などのインターネットを利用した事件が多発している状況から生徒への安全教育の必要性を感じ平成 17 年 1 月に外部機関主催の安全教育セミナー資料を用いて特別授業を実施した。
- ・授業時の生徒の反応もよく、生徒のリテラシー教育に効果のあるコンテンツだったので、平成 17 年度より必修となっている教科「情報」の年間スケジュールに組み込み、毎年実施することとした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：生徒のリテラシー教育に効果のあるコンテンツだったため。
- ・発生日時：平成 17 年 1 月
- ・発 見 日：
- ・事実確認：

◆対処方法

ー生徒への対応ー

- ・対 応 日：毎年 4 月
- ・対応担当者：情報担当教員
- ・対 応 方 法：

授業は生徒同士がお互いに情報交換を実施できるようにするために、グループでの学習としている。

まず、何の予備知識も与えない状況でクイズ学習を実施する。次に、映像プログラムを上映し、映像プログラムを見終わったところでもう一度クイズ学習を実施する。

全員がクイズ学習を終えたところで、教員がクイズ学習の解答並びに解説を実施する。

◆今後の対策と効果

- ・インターネット上に次々と発生する新手法の犯罪手口や攻撃手法にも生徒が対応できるようにするためにコンテンツの見直しを検討している。
- ・保護者向け講習会も予定している。

インターネットを利用した犯罪に巻き込まれないための指導 1

高等学校での事例

◆被害状況

- ・インターネットを利用した犯罪やトラブルなどの報道が多数されている。
- ・生徒がインターネットを利用する機会が増加しており、インターネットの利用に際して生徒自身の知識不足により犯罪の被害者にも加害者にもなる可能性があり、犯罪の手口やその対応方法を身につけておく必要がある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：最近の報道などから、生徒にインターネットを利用した最新の犯罪事例や対策方法を身につけさせる必要性を感じた。
- ・発生日時：
- ・発見日：
- ・事実確認：

◆被害への対応

－生徒への対応－

- ・対応日：平成17年6月
- ・対応担当者：情報担当教員
- ・対応方法：

インターネットを利用した最新の犯罪の手口とその対策を生徒に指導するために、雑誌や新聞、Webサイトなどから情報収集を行い、犯罪の手口・気をつけなければならない点・被害に遭わないための対策を学ぶ教材を作成している。

授業では使用する教材は、生徒が自宅に持ち帰っても利用できるように印刷して生徒に配布している。

今年度は、架空請求メールやワンクリック詐欺・フィッシング詐欺やオークション詐欺・出会いサイトについての具体的な手口とその対策を指導した。

◆今後の対策と効果

- ・生徒がインターネットオークション詐欺やワンクリック詐欺などで被害にあったという報告や犯罪の加害者になったという報告もない。

インターネットを利用した犯罪に巻き込まれないための指導2

高等学校での事例

◆状況

- ・自宅のパソコンや携帯電話を利用してインターネットを利用する生徒が増えている。また、犯罪に巻き込むための手口も巧妙化しており、年齢を問わず、インターネット上のトラブルに巻き込まれる可能性が高くなってきている。
- ・このような状況を鑑み、生徒にトラブルに巻き込まれないための情報をできるだけ早くかつ正確に伝える必要があると認識している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

—生徒への対応—

- ・対応日：情報の授業時（随時）
- ・対応担当者：情報担当教員
- ・対応方法：

年間の授業計画にとらわれず、随時、最新の情報を生徒に紹介している。

紹介する際には、警察や国民生活センターの Web サイトに掲載されているトラブル事例や教員が利用している携帯電話に届いた架空請求メールや教材研究で偶然発見したワンクリック請求の Web ページなど教員の体験に基づく事例について、その手口と対策を紹介し、トラブルに巻き込まれないように指導している。

◆今後の対策と効果

- ・指導の甲斐あって、生徒が架空請求メールやワンクリック請求などの不当な請求に応じてしまったなどのトラブル事例は発生していない。

インターネット安全利用の特別授業1

小学校での事例

◆被害状況

- ・携帯電話やインターネット利用についてのさまざまな事件・事故が社会問題化しつつあるなかで、児童への安全教育・指導が学校としての課題となっている。
- ・保護者からの関心も高く、安全教育実施の要望も寄せられている。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成17年9月
- ・発見日：
- ・対応方法：

◆被害への対応

—生徒への対応—

- ・対応日：平成17年9月
- ・対応担当者：
- ・対応方法：

総合学習の時間に安全教育を行った。

対象：4～6年生の全児童および保護者

実施形式：体育館における集合実施。保護者は希望者・参観形式。

時間：1時限45分間。保護者向けに児童向け安全教育終了後、20分程度最新の話題と安全のための考え方を講義。

内容

1. パソコンや携帯電話でインターネットを安全に活用するために
 - ①パソコンでできること 携帯電話でできること
 - ②インターネットでできること
 - ③インターネットでできないこと
 - ④注意しておくこと—インターネットの世界とは—
 - ⑤電子メールの注意事項
 - ⑥電子掲示板・チャットの注意事項
 - ⑦ホームページの注意事項
 - ⑧自分のホームページの注意事項
2. 最近の話題・質疑応答など

講師：NPO情報セキュリティフォーラム

◆今後の対策と効果

インターネット安全利用の特別授業2

中学校での事例

◆被害状況

- ・携帯電話やインターネット利用についてのさまざまな事件・事故が社会問題化しつつあるなかで、児童への安全教育・指導が学校としての課題となっている。
- ・保護者からの関心も高く、安全教育実施の要望も寄せられている。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成17年9月
- ・発見日：
- ・対応方法：

◆被害への対応

—生徒への対応—

- ・対応日：平成17年10月
- ・対応担当者：
- ・対応方法：

日曜日に学校にて安全教育を行った。

対象：1～3年生の希望生徒および希望保護者。

時間：生徒向け50分。保護者向け50分。

内容：

1. パソコンや携帯電話でインターネットを安全に活用するために
 - ①パソコンでできること 携帯電話でできること
 - ②インターネットでできること
 - ③インターネットでできないこと
 - ④注意しておくこと—インターネットの世界とは—
 - ⑤電子メールの注意事項
 - ⑥電子掲示板・チャットの注意事項
 - ⑦ホームページの注意事項
 - ⑧自分のホームページの注意事項
2. 最近の話題・質疑応答など

講師：NPO情報セキュリティフォーラム

◆今後の対策と効果

インターネット安全利用の特別授業3

中学校での事例

◆被害状況

- ・生徒が情報社会に主体的に参加できる力を養うため、通常の情報教育の授業とは別枠で、年間2回ほど特別講座を実施している。今年度はパソコンや携帯電話の普及に伴い中学生にとっても身近となったインターネットについて、インターネットを介したトラブルや犯罪の被害に巻き込まれないための対策や、生徒の認識不足によりトラブルや犯罪の加害者にならないための知識を身につける講座を実施した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成15年度より
- ・発見日：
- ・事実確認：

◆被害への対応

—生徒への対応—

- ・対応日：平成17年5月・10月
- ・対応担当者：情報担当教員・外部講師
- ・対応方法：

特別講座は2グループ（1年生と2・3年生）に分け、5月と10月に実施した。

1年生は、5月にインターネットの概要を紹介し、半年間の学校生活でパソコンの操作にも慣れてきた10月には、パソコンを使って実際にトラブルを疑似体験させ、トラブルに巻き込まれないための対策方法を指導した。

2・3年生は、5月に個人情報の扱い方について情報担当教員より講義形式で指導を行い、10月には外部講師を招き、外部講師がインターネットでトラブルや犯罪に巻き込まれないための対策についてビデオ教材と教材の解説を行った。

◆今後の対策と効果

- ・日常からの情報教育の授業と特別講座での指導の成果もあり、インターネットを介したトラブルや犯罪に対する意識が高まった。ただし、新たな脅威を防ぐ手段がないので、継続的に意識を高める取り組みを実施していく。

インターネット安全利用の特別授業4

高等学校での事例

◆被害状況

- ・インターネット利用に伴うさまざまなトラブルについて、従来から教科「情報」や教員の個別の対応を実施してきた。
- ・最近になって多くのトラブルが報道で取り沙汰され、生徒の安全確保の視点と教育効果の視点から外部の専門知識をもった講師に特別授業を依頼し実施した。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

◆被害への対応

ー生徒への対応ー

- ・対応日：平成16年12月
- ・対応担当者：教員、NPO 情報セキュリティフォーラム
- ・対応方法：

期末試験後の採点期間を利用し、高校2年生全員約200名を対象に外部講師によるインターネットを安全に利用するための特別授業を実施した。

内容は、ウイルスと不審なメール対策、個人情報の漏えい対策、ネットショッピングやオークションの注意点、掲示板・チャットのマナー、無線LANの注意、Webサイト公開時の注意点である。

◆今後の対策と効果

インターネット安全利用の特別授業5

高等学校での事例

◆被害状況

- ・生徒が授業や自宅でインターネットを利用する機会が増えているので、情報科の授業の一環として、生徒がインターネットを利用した犯罪に巻き込まれないようインターネットの安全利用について指導することとしている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・パソコン教室のパソコンは教育委員会が管理・運営しているネットワークに参加しており、教育委員会ネットワーク経由でインターネットが利用できる。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成15年～
- ・発見日：
- ・事実確認：

◆被害への対応

―生徒への対応―

- ・対応日：毎年秋
- ・対応担当者：情報セキュリティアドバイザー（神奈川県警察本部 ハイテク犯罪対策センター）・教員
- ・対応方法：

インターネット安全利用について、1年次生全員を対象とし、11月に特別授業を実施している。

特別授業は、サイバー犯罪等の実態・サイバー犯罪やインターネット上のトラブルに遭わないための対応などについて、神奈川県警察本部ハイテク犯罪対策センターに所属する情報セキュリティアドバイザーに依頼し、特別授業を実施している。

― 参考 ―

神奈川県警察本部ハイテク犯罪対策センター サイバー犯罪防止のための取組み
<http://www.police.pref.kanagawa.jp/mes/mesd0063.htm#bouhan>

◆今後の対策と効果

インターネット安全利用の特別授業6

高等学校での事例

◆状況

- ・生徒が学校内で利用するネットワークやパソコンはウイルス対策ソフトやフィルタリングなどのセキュリティ対策が実施されているため、生徒は校内でのパソコン利用にあたってはセキュリティ対策が実施されていることを日常的に体感している。したがって、校内での利用にあたって、セキュリティ上の大きなトラブルは発生していない。
- ・しかし、生徒が自宅で利用しているパソコンは、セキュリティ対策が実施されているものも実施されていないものもある。
- ・そこで、自宅のパソコンのセキュリティ対策を生徒自身が実施する、また、インターネットを利用する際にトラブルに巻き込まれないための知識を生徒が身につける必要があると認識している。
- ・情報の授業ではカリキュラムの都合もあり、セキュリティ対策のみの時間を設定することが難しい状況となっている。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- ・すべてのパソコンにウイルス対策ソフトを導入している。
- ・フィルタリングを利用して閲覧できる Web サイトに制限を設けている。

◆経緯

- ・発見方法：
- ・発生日時：
- ・発見日：
- ・事実確認：

◆対処方法

ー生徒への対応ー

- ・対応日：平成18年3月・4月
- ・対応担当者：情報担当教員、NPO 情報セキュリティフォーラム
- ・対応方法：

生徒がセキュリティ対策やインターネット上のトラブルに巻き込まれないための知識を身につけるための特別授業を実施することとした。

対象 高校2年生と3年生

実施形式 体育館での一斉授業

時間 1時限50分

内容 フィッシング詐欺やオークション詐欺、架空請求メールや不当請求、コンピュータウイルス対策などに関する内容のビデオ上映
上映したビデオの内容を確認するクイズ学習
情報漏えい事件等で昨今報道されているファイル交換ソフトについての注意喚起

◆今後の対策と効果

教員向けセキュリティ講習会の開催1

中学校での事例

◆被害状況

- ・以前から職員会議等で教職員の情報セキュリティに関する啓発を行っていたが、校内パソコンのOS更新を期に、情報セキュリティ・パソコンの操作・インターネットの利用方法などの啓発を図る講習会を開催することにした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン利用状況や利用形態―

- ・教員は職員用パソコンを自由に利用することができる。

―校内のセキュリティ対策―

- ・ウイルス対策ソフトを導入している。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成17年3月
- ・発見日：
- ・事実確認：

◆被害への対応

―教員向け講習会の開催―

- ・対応日：平成17年4月実施予定
- ・対応担当者：
- ・対応方法：
外部講師を招聘し、情報セキュリティ・パソコンの操作・インターネットの利用方法などについて、学校のパソコンを利用し、実習を交えながら講習会を実施する。

◆今後の対策と効果

教員向けセキュリティ講習会の開催2

高等学校での事例

◆被害状況

- ・年度始めに教員を対象としたネットワーク講習会を開催している。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

ー校内のパソコン利用状況や利用形態ー

- ・全教員にユーザ ID・パスワード・電子メールを付与している。

ー校内のセキュリティ対策ー

- ・校内のネットワークに個人所有パソコンを繋げる場合は、必ず学校に申請を行い、ウイルス対策ソフトの導入やセキュリティパッチが当てられている場合のみ接続を許可している。また、年度始めの講習会への参加を義務付けている。

◆発見の経緯

◆被害への対応

ー教員向け講習会の開催ー

- ・対応日：
- ・対応担当者：校内分掌で定められている管理部の教員
- ・対応方法：

校内パソコンを利用する際は、ユーザ ID とパスワードによる認証を行っているので、年度始めにネットワーク講習会を開催し、校内パソコンの利用方法、コンピュータウイルス対策、電子メールの扱い方などについての講習会を開催している。

校内ネットワークに個人所有パソコンを繋げる場合は、学校に申請を行い、セキュリティ要件を満たしているか確認している。また、ネットワーク講習会に参加することを義務付け、個人所有パソコンのウイルス対策ソフトの設定、インターネットや電子メールの設定、ネットワークの設定など、管理部の教員が指導を行っている。

◆今後の対策と効果

教員向けセキュリティ講習会の開催3

高等学校での事例

◆被害状況

- ・報道等で高校生が携帯電話・インターネット利用に関わるさまざまなトラブルに巻き込まれており、安全教育・生徒指導の必要性を認識しているが、カリキュラム上、授業のなかで情報モラルやマナーの指導に費やせる時間が十分にとれない状況にある。
- ・特別授業の実施、効果的な外部教材を利用するなど学校全体としての安全教育実施方法を模索しているが、教員間での携帯電話・インターネット利用における危険性の認識の差があり、今までのところ十分な安全教育・生徒指導ができていない。

◆学校のコンピュータ環境・利用状況・セキュリティ対策など

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 17 年
- ・発見日：
- ・対応方法：

◆被害への対応

—教員への対応—

- ・対応日：平成 17 年 10 月
- ・対応担当者：
- ・対応方法：

年 1 回実施の校内教員人権研修会において「情報モラル・マナー」をテーマ設定し、外部講師を招いて情報モラルやマナー、生徒が巻き込まれる事件や犯罪についての現状を教員間の情報として共有することとした。

研修資料として生徒向けに利用したい教材についても教員で評価を行った。

安全教育・生徒指導について一歩前進させることができた。

◆今後の対策と効果

- ・今回の対応については、生徒指導、教員の意識向上と情報共有を継続していく必要性があり、今後とも研修会などを実施していく。また、今後の対応に向けて校内の組織づくりについても検討していくこととなった。

教員向けコンピュータウイルス対策の講習会の開催

高等学校での事例

◆被害状況

- ・過去にコンピュータウイルス感染が発生しており、校内パソコンへのウイルス感染を防止するために、教員対象にウイルス対策の講習会を開催した。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

- 校内のセキュリティ対策—
- ・校内のすべてのパソコンにウイルス対策ソフトが導入されている。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 15 年 8 月
- ・発見日：
- ・事実確認：

◆被害への対応

- 教員向け講習会の開催—
- ・対応日：平成 15 年 8 月
- ・対応担当者：
- ・対応方法：
夏休み期間を利用して、ウイルスの概要・ウイルスがもたらす被害・ウイルス対策ソフトの利用方法・スパイウェアなどについて、教員向けにウイルス対策の講習会を実施した。

◆今後の対策と効果

- ・講習会の開催後、校内のパソコン・教員が校内に持ち込んでいる個人所有パソコンでのウイルス感染の報告はない。今後も、職員会議等を利用して、情報セキュリティの啓発を行っていく。

保護者・生徒向けインターネット教室の開催

中学校での事例

◆被害状況

- ・家庭や学校においてインターネットを利用できる環境が整備され、生徒はいつでもインターネットが利用できるようになった。生徒の保護者は子どものインターネットの利用状況を把握するために、インターネットの知識や利用方法について認識しておく必要がある。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

―校内のパソコン環境―

- ・パソコン教室のパソコンからインターネットの利用ができる。

―校内のセキュリティ対策―

- ・ウイルス対策ソフトを導入している。
- ・フィルタリングソフトを利用して、閲覧できる Web サイトを制限している。

◆発見の経緯

- ・発見方法：
- ・発生日時：平成 15 年
- ・発見日：平成 15 年
- ・事実確認：

◆被害への対応

―生徒・保護者への対応―

- ・対応日：
- ・対応担当者：情報担当教員
- ・対応方法：

学校が年 1 回実施している共学体験の 1 講座として、学校のパソコン教室を利用して生徒と保護者が一緒に学べるインターネット教室を開催した。

インターネットに詳しい保護者や地域住民を講師として迎え、インターネットの利用方法・コンピュータウイルス対策・情報モラルについて実習を交えながら体験学習を実施した。

◆今後の対策と効果

保護者向けセキュリティ教室の開催

高等学校での事例

◆状況

- ・生徒は自宅でも Web サイトの閲覧や電子メールの送受信などインターネットを利用しており、生徒がインターネットを利用する際にトラブルに巻き込まれないようにするためには、学校での指導とともに保護者からセキュリティ教育をする必要があると認識している。
- ・しかし、子どもを指導するための知識やスキルを保有していない保護者も多いと認識しているので、指導できる知識やスキルを身につけるための安全教室を開催することとした。

◆学校のコンピュータ環境の状況・利用状況・セキュリティ対策など

◆経緯

- ・発見方法：生徒へのセキュリティ教育は学校と保護者の両方からの指導が必要であり、そのためにも保護者の知識やスキルを高める必要があると考えている。
- ・発生日時：平成 18 年 6 月
- ・発見日：
- ・事実確認：

◆対処方法

ーセキュリティ教室の内容ー

- ・対応日：平成 18 年 6 月
- ・対応担当者：情報担当教員、NPO 情報セキュリティフォーラム
- ・対応方法：

保護者向けの安全教室の開催を周知し、参加希望者を募り、安全教室を開催した。

Windows アップデートやフィルタリングソフトなどについて、実際にパソコンを利用し設定方法などを体験する内容とした。

場所：相鉄岩崎学園ビル（横浜市神奈川区鶴屋町 2-17）

時間：9:00～12:00 3 時間

- 内容：
1. インターネットの基礎知識
 2. セキュリティについて
 - ・ユーザ ID とパスワードについて
 - ・プライバシーの守り方
 - ・コンピュータウイルスについて
 3. 電子メールの基礎知識
 4. ブラウザの設定
 - ・コンテンツアダプタイザ
 - ・プロバイダのフィルタリングサービス
 - ・市販のフィルタリングソフト
 - ・検索エンジンの検討
 - ・Web のアクセス履歴を見る
 5. インターネットによる情報発信
 - ・ブログ
 - ・掲示板

講師：NPO 情報セキュリティフォーラム

◆今後の対策と効果

謝 辞

本事例集の作成にあたっては、神奈川県高等学校教科研究会情報部会の先生の皆様をはじめ、匿名を条件とした取材のため学校名、お名前を書き記すことができませんが、個別に事例提供にご協力して下さった小学校、中学校、高等学校、専門学校の多くの先生、職員の皆様に感謝申し上げます。

皆様のお力添えによりまして教育現場における情報セキュリティ事故・対応事例の研究を実施させていただくことができ、事例集として取りまとめることができましたことを深く感謝申し上げます。

また、今後につきましても事故・対応事例の収集を継続して行ってまいります。何卒変わらぬご協力いただけますよう宜しくお願い申し上げます。

特定非営利活動法人 NPO 情報セキュリティフォーラム

この事例集は、NPO 情報セキュリティフォーラムが独立行政法人福祉医療機構
(子育て支援基金) の助成金を受けて作成したものです。

無断転載禁止

教育現場における情報セキュリティ事故・対応事例の研究
事例集

平成 19 年 2 月発行

特定非営利活動法人 NPO 情報セキュリティフォーラム

横浜市神奈川区鶴屋町 2-17 相鉄岩崎学園ビル 8 階

TEL : 045-311-8777 FAX : 045-311-8747

E-mail: isef@isef.or.jp

<http://www.isef.or.jp/>