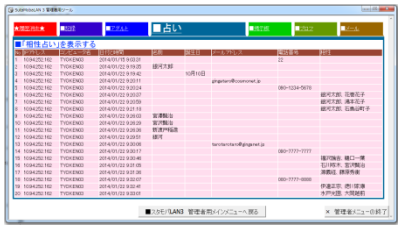
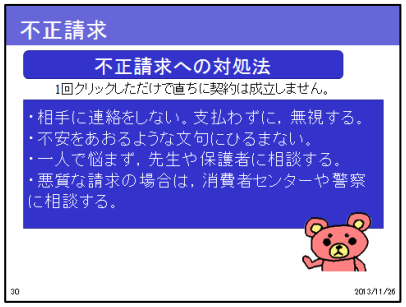
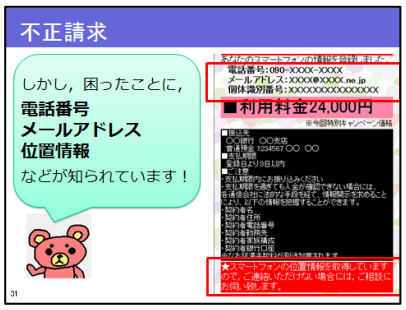
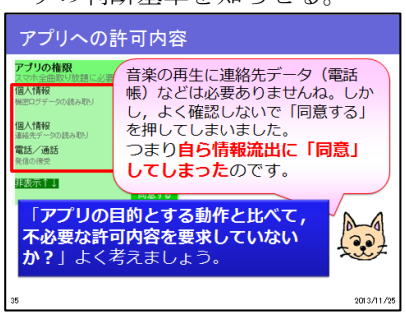
「アプリをインストールするときの注意点」についての展開例

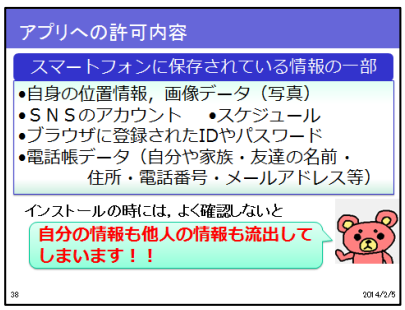
1　題材のねらい

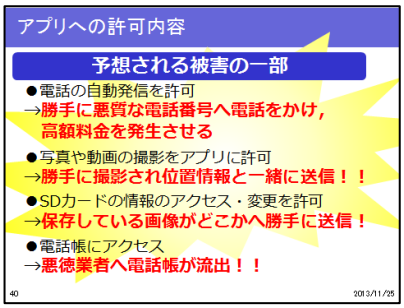
スマートフォンから個人情報を抜き取ったり機能を乗っ取ったりする危険なアプリが存在していることを知らせ，アプリへの許可内容を確認しないまま安易にインストールすることはこれらに同意していることと等しいことに気付かせる。セキュリティ確保のための知識を学ばせ，適切な判断をすることがスマートフォンからの情報流出を防ぎ，自他を危険から守ることができるようにする。

2　展開例

過程	学習活動	教師の指導・支援	指導上の留意点等 ◎ポイント　※留意点　・解説　■用語解説
導入 10分	1. アプリに情報を入力することの危険性について知る。	・管理者用ソフトウェアから，前時の「占いの館」で入力した内容が，サーバに送信され全て記録されていることを示す。 	◎「スマートフォンで情報を入力するということは，情報が出ていくことに等しい」ことに気付かせる。 ◎入力されたデータと IP アドレスから，氏名・電話番号・メールアドレス等の情報が紐づけされてしまい，個人が特定されてしまうことに気付かせる。 ・スマートフォンは電源が入っていると，インターネットにつながったままになる。アプリの中には，電話帳など個人情報にアクセスして他所へ送信するものがある。送信されたデータは蓄積され，業者に販売され商用利用される。 ■IP アドレス…インターネット上でパソコンに割り振られた識別番号。重複することがない。インターネット上でのパソコンの住所にあたる。
	2. 学習内容の把握をする。	・スライドで本時の目標を示し，確認させる。	
	アプリをインストールするときの注意点を学ぼう		
	3.「アプリ SHOP」からアプリをインストールし，危険なアプリの存在を知る。	・スライドで操作方法を説明し，実際の操作についても一斉送信で確認してから体験させる。 	※スタモバ「アプリ SHOP」 →「スマホ全曲取り放題」アプリ →不正請求サイトへ誘導される。

展開 30分	4. 不正請求への対処法について学ぶ。 (1) 不正請求への対処法を考える。	・スライドを示し，このような請求画面が表示されたらどうするか考えさせる。 	◎パソコンや携帯電話でも同様にワンクリック詐欺があったが，スマートフォンでは，電話帳や位置情報も同時に流出する可能性があり，携帯電話やパソコンの場合より被害リスクが大きくなることをおさえさせる。 ・IP アドレスからは発信者の使っているプロバイダや携帯電話会社とアクセスポイント（市町村）は分かるが，個人情報は分からない。警察からの開示請求があれば公表することはあるが，このような業者には公表しない。しかし，スマートフォンの場合は，危険なアプリによって，電話帳等の個人情報を抜き取られる場合がある。
	(2) 不正請求への対処法を知る。	・スライドを使って対処法について解説する。 	◎登録画面が出た場合，保護者や教師など信頼できる大人に相談する。無視をするのが良いが，相手業者から料金請求の電話がかかってきたり、メールが送られてきたりした場合は、電話の着信拒否やメールの受信拒否等で対応する。悪質な場合は，消費者センターや警察に相談する。 ・このようなサイトでは，お年玉等で何とか払える金額を提示してくることが多く，相談できない生徒が被害に遭ってしまうことがある。
	5. アプリをインストールする際に確認すべき事項を学ぶ。 (1) なぜ情報が流出したか考える。	・個人情報が流出した理由を考えさせる。 	
	(2) 何を確認すればよいか知る。	・スライドを使って，危険なアプリの判断基準を知らせる。 	◎「アプリの動作から考えると不必要な許可内容を求められていないか」が判断の基準となることを知らせる。 ・アプリをインストールするとき，アプリの権限として，スマートフォンに保存されている情報や機能にアクセスするか，許可内容を確認する画面が表示される。これをよく確認しないと，アプリをインストールするときに，自ら情報の送信を許可してしまうことになる。

	(3) 「アプリ SHOP」を起動し，それぞれのアプリについて，許可内容が適切かどうかを考え，安全と思ったものについてインストールする。	・画面を一斉送信しながら，手順を説明する。 ・学習プリントのチェック項目に，○×をつけて，安全かどうか判断させる。 	※１つは例として教師が説明しながら全員で考えさせ，残り３つを各自判断させる。
	(4) インストールしても安全だと思ったアプリと，その理由を発言する。	・画面を一斉送信しながら，それぞれのアプリについて解説を行う。	◎少しでも怪しいと思う項目があれば，類似の別のアプリを使うように指導する。 ・Google Play（Android）や App Store（iPhone）など公式のページからアプリをダウンロードさせる。広告メール等に記載された URL からダウンロードするのは危険が生じる場合がある。また，公式サイトにも危険なアプリが存在しているので注意が必要である。 ・インターネット＋SD カードへのアクセス許可は，ネットゲーム等で，ダウンロードしたデータを保存するというアプリの動作が予想される。しかし悪質な場合には，SD カードに保存された情報を他所へ送信する権限を与えたことにもなる。アプリへのユーザーレビューも参考にしたい。しかし，アプリの機能を有効にするためによいレビューを書くように強要するアプリもある。
	6.収集された情報がどのような被害につながるのかを知る。 (1) スマートフォンに，どんな情報が保存されているかを知る。	・スマートフォンに保存されている情報を知らせる。 	◎スマートフォンの中には，自分の個人情報だけではなく，他人の個人情報も多く含まれていることを確認する。

	(2) 情報が流出すると，どんな被害が予想されるか知る。	・情報流出した場合の被害について質問し，許可内容とそれを許可した場合の被害についてスライドでまとめる。 	◎アプリをインストールするときには，許可内容をよく確認しないと，情報が流出し，自分だけではなく周囲にも被害が及ぶことに気付かせる。許可内容をしっかり確認することが自他の身の安全につながることを確認する。
終末 10分	7. まとめる。 (1) 授業を振り返り，アプリをインストールするときの注意点について学習プリントにまとめ，発表する。	・授業を振り返り，スマートフォンから情報流出を防ぐにはどうしたらよいか，「アプリの許可内容」というキーワードを使って学習プリントにまとめさせる。 ・まとめた内容を発表させる。	

3　評価

十分満足できると判断される生徒の姿（A）	アプリをインストールするときに気を付けることについて答えることができ，またその理由についても適切に理解している。
本時の評価規準（B）	アプリをインストールするときに気を付けることについて答えることができる。
支援が必要とされる生徒への支援方法（C）	記述できない生徒に対して，机間指導を行う。