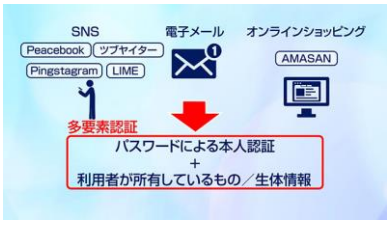
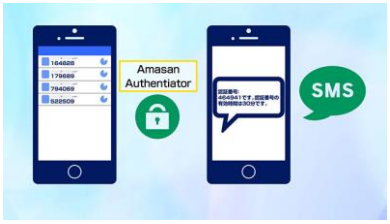
02_情報セキュリティ「あの手この手で乗っ取りを… ー多要素認証ー」

	■■■■■■■ 物語編 ■■■■■■■ ■カフェ 正樹と由依が話しているところに麗奈がやってくる	
由依	あれ？麗奈どうしたの？	
麗奈	麗奈、疲れきった顔 ピンスタ乗っ取られた件の対応でほぼ一日潰れた･･･疲れたー。	
由依	乗っ取りの原因ってわかったの？	
麗奈	私･･･ピンスタとツブヤイター、おんなじパスワード使っちゃっててさ･･･ それで、ツブヤイターの情報流出があって･･･	
由依	やっぱりツブヤイターのパスワード流出が原因だったんだね。	
麗奈	しかもしかも、ピンスタとピースブックはアカウント連携させてたし、アマサンのパスワードも同じの使っちゃってたから、結局、全部のパスワード換えなきゃいけなくなっちゃって、もういろいろ大変でさ･･･	
正樹	ピンスタのデータは復活できそう？	
麗奈	それが、いろいろ聞いてやってはみたけどダメそう･･･失ったものは大きいよ･･･	
由依	でも、金銭的な被害がなかっただけでも良かったって思わないとね！！	
麗奈	そうだよね･･･それでさーアマサンのサポートセンタ	

	ーの人に多要素認証っていうのをススメられちゃって・・・その設定もしてみたりしたんだけど、全然理解できなくてさ・・・二人は知ってる？	
正樹	多要素認証？　秘密の質問的な？	
麗奈	それが、ちょっと違うんだよね・・・ Web の説明通りに設定してみたんだけど、仕組みがわかんなくて・・・由依知ってる？	
由依	ん〜私もいくつか使ってるんだけど、実はあまりよくわかってないんだよねどうなってるんだろう。	
3 人で	誰か、教えてーーー	

	■■■■■■■ 解説・発展編 ■■■■■■■ ■カフェ	
天の声 （女性）	麗奈さん。とんだ災難でしたね！！ 良い機会なので多要素認証について学んでおきましょう。	
解説 （男性）	SNSや電子メール、オンラインショッピングなど様々なサービスを利用する際にはパスワードによる本人認証が用いられます。 パスワードに加え、利用者が所有しているものや生体情報を組み合わせて認証を行うことを多要素認証と呼びます。 まず、個人の認証に使うことができる「認証要素」について整理すると知識情報、生体情報、所有情報、の3つが挙げられます。 これらは「認証の3要素」と呼ばれています。 知識情報は、本人のみが記憶している情報で、パスワードや暗証番号などがこれにあたります。 生体情報は、本人の生体的な特徴に基づく情報で、指紋や静脈、声や顔などが使われています。 所有情報とは、本人のみが所有している物を使って表す情報のことで、暗号表、スマートフォンへのSMS 送信、トークンやアプリによるワンタイムパスワード生成などの方法があります。	  
由依	いろいろな方法で本人認証ができるんですね。	
麗奈	私がゆうべ設定したのもスマートフォンのアプリだったからきっと「所有情報」ってことですね。	
解説 （男性）	パスワードという「知識情報」に加え「生体情報」や「所有情報」を使うことで、多要素での認証が行われることになります。	

解説 （男性）	正樹君が言っていた「秘密の質問」は、パスワードと同じ「知識情報」の要素となりますので、多要素認証とはいえません。	
天の声 （女性）	秘密の質問は第三者に推測されやすいから、これからはあまり使われなくなるかもしれないわね。	
正樹	へー。確かに好きなスポーツチームとか、母親の旧姓って大して秘密の情報じゃないですよね。	
解説 （男性）	現在、二つ目の認証要素として用いられることが多いのは、スマートフォンのアプリで生成したり受信したりするワンタイムパスワードを使う方法です。	
麗奈	ワンタイムパスワードって、パスワードなのに所有情報なんですか？	
解説 （男性）	ワンタイムパスワードとは、一度限りしか有効でないパスワードのことです。ただし、スマートフォンなど個人が所有する特定の機器によって生成されたり、SMS などによって受信するパスワードなので、スマートフォン所有者だけが知りえる所有情報と考えることができます。一般に、ワンタイムパスワードは 6 桁くらいの数字が使われる場合が多いです。	
由依	6 桁の数字ってちょっと頼りない気がします。	
天の声 （女性）	ワンタイムパスワードの有効時間は 30 秒ほどと、とても短く設定されているの。6 桁の数字でも推測されにくいと考えられているわ。	
正樹	30 秒か・・・それっていったいどういう仕組みなんでしょうか？	
解説 （男性）	スマートフォンのアプリの場合、最初の設定で認証サーバーとアプリとで秘密の鍵を共有します。鍵と	

	いっても実際には何らかの数値で、画面に表示される QR コードを読み込むなどの方法でアプリに取り込むのです。	
麗奈	そういえば QR コード、やったな・・・。	
解説 （男性）	共通の鍵となる数値と現在時刻とを使った ある計算を行うことで、鍵を知るアプリと認証サーバーだけが知りうる共通のパスワードを生成できます。これがワンタイムパスワードの仕組みです。	
正樹	そうなんですね。	
麗奈	もし、多要素認証を設定していて、スマートフォンを無くしてしまった場合はどうなりますか？	
天の声 （女性）	大事なポイントね！　多要素認証には何らかのバックアップ手段が用意されているはずなので、確認して対策をとっておくことが重要よ。	
解説 （男性）	最近では多要素認証を使えるサービスが増えていますが、その一方で偽のサーバーに誘導するフィッシングメールや、本物そっくりの偽アプリといったものも確認されていますので注意してください。	
天の声 （女性）	仕組みをちゃんと理解して、本当の手段を正しく使っていく事が大事なの！ みんなも騙されないように！	
3 人	わかりました！！	