

(^_^) アカウント

コンピュータやネットワーク上の資源を利用できる権利のことをアカウントといいます。コンピュータを起動し、ネットワークに接続（ログイン）し、コンピュータやネットワーク上の資源を利用する権利を、ユーザーアカウントやログインアカウントといい、電子メールを送受信する権利をメールアカウントといいます。また、利用する際には、ユーザーID（IDはidentificationを略したもの、ユーザー名ともいう）と呼ばれるものが必要なため、ユーザーIDをアカウントという場合もあります。

ユーザーIDは、単にIDとも呼ばれ、あらかじめサーバなどに登録をしておかなければなりません。この作業をアカウントの発行といいます。登録されていないIDではコンピュータやインターネットを使うことができません。

さらに、ID所有者本人であるかどうかを確認するためにパスワードが必要です。パスワードもアカウント発行時にサーバなどに登録されます。IDとパスワードを正しく入力した人だけがコンピュータやインターネットを使うことができるように、セキュリティを二重に施しています。

IDとパスワードは、個人を特定する作業である個人認証に使われるものですが、文字と数字の組み合わせであり、他人に知られてしまうと本人になりすまして不正に使用される危険性があるため、現在では、さまざまな個人認証のシステムが開発されています。

プラスチック製のカードに、CPUやメモリ、セキュリティ回路を組み込んだスマートカード（smart card）やICカードと呼ばれるものにIDとパスワードを記録し、カード読み取り装置で個人認証を行う方法があります。カードの利用には暗証番号を必要とし、暗証番号を知っているカードの所有者のみが使える仕組みです。

カードによる個人認証の方法は、カードの紛失や盗難の危険性があります。現在、指紋や網膜、静脈、声紋といった固有の身体的な

特徴をもとに個人認証を行う生体認証技術が研究、開発されています。生体認証はなりすましが困難とされ、パスワードの必要がないなどの特長があります。

(T-T) 個人情報の漏洩

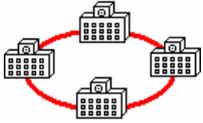
住所、氏名、電話番号、誕生日、学校名などとともに、携帯電話番号、クレジットカード番号、メールアドレス、ID、パスワードなども個人情報です。

メールアドレスやIDは他人に知られることはありますが、これらとともにそのパスワードを知られると、本人になりすましてコンピュータやネットワークを不正に使用され、さまざまな個人情報の盗難にあうことがあります。

ある大学では本人の知らないところで就職内定を辞退する電子メールを出され、就職ができなくなったという事件が起きました。デジタル化された情報がやり取りされるネットワーク社会では、対面によるやり取り、電話による連絡、自筆の手紙などと異なり、なりすましが容易です。IDとパスワードは自己責任として厳重に管理しなければなりません。

また、メールアドレスを不用意に他人に知らせ利用されると迷惑メールや宣伝メール、コンピュータウイルスが送信されてきたりします。他人のメールアドレスやIDを本人の同意を得ずに、第三者に伝えないこともネットワーク社会でのマナーです。

パスワードは、主に半角のアルファベットや数字を用いて本人が作ります。電話番号や誕生日、メールアドレス、IDに関連するものなどを避けることが推測されにくいパスワードを作る方法として推奨されています。また、パスワードは、メモなどをせずに本人が記憶することにより管理することが漏洩を防ぐ方法として推奨されています。



セキュリティ

セキュリティ (security) とは、安全、保全、保障、安心という意味ですが、コンピュータ関連で用いたときは、コンピュータやネットワーク上の資源を活用する権利をもたない第三者からこれらの資源を守ることをいいます。

セキュリティのレベルを高くすると安全性は高まりますが、コンピュータの活用における制限が増えます。逆にレベルを低くすると、コンピュータは使いやすくなりますが、安全性の面で問題が増えます。

企業や学校などのネットワークでは、情報の読み取りについて、どのような情報を誰に許可するのか、ネットワーク上のさまざまな操作についてどのような操作を誰に許可するのかなど、情報の目的外使用や外部からの侵入、機密漏洩などを防止するために定めたセキュリティに関する基本方針として、セキュリティポリシーを作成し、運用を行う必要があります。セキュリティポリシーはコンピュータウィルスの感染によるデータやシステムの破壊やさまざまなトラブルによるシステムの停止、データの喪失などに対する対処についても含めます。

学校情報ネットワークは、すでに二万台以上の端末パソコンが接続された大規模なネットワークであり、学校の中で生徒や教職員が安心して自由に使えることを保障しながら、セキュリティレベルの高いポリシーを策定し、運用されています。

各学校においてネットワーク管理を担当する教職員の負担軽減を考慮した全校共通の学校教育用のネットワーク管理ツールを組み込み、教職員や生徒のアカウントの発行などが容易に行えます。しかし、アカウントが容易に発行できることは、セキュリティの面からは、不安要素となります。従って、管理ツールを操作できる権限をもったアカウント (管理者権限) については、各学校で厳重に管理されなくてはなりません。

また、府教育センターのサーバ群には、外部ネットワークであるインターネットとの間に、どのような情報のやり取りをするかについての

セキュリティポリシーがあります。インターネット上に存在するコンピュータウィルスを送信するようなサイトや不正侵入を試みるサイトなどからはファイアウォール技術により内部ネットワークを守っています。また、どのような情報 (パケットと呼ばれる) を通過させ、どのような情報を遮断するのかについては、学校教育利用の観点からセキュリティポリシーを定め、ファイアウォールユニットに設定されています。

セキュリティポリシーは、ネットワークの利用目的に照らし、必要とする利用方法や使用時の操作性とセキュリティレベルとのバランスを考え、コンピュータやネットワークの資源の量や質、利用内容への影響など、複雑な要素を総合的に判断して策定されます。このポリシーに基づいて、サーバや端末パソコンのそれぞれの設定を行い、ネットワークを維持、管理、運用しています。また、セキュリティポリシーは、固定したものではなく、新たなネットワーク技術やセキュリティ侵害方法の登場などを受け、その都度検討が行われ、変化するものでもあります。

Q . 端末パソコンにインストールされているリアルプレイヤー (RealPlayer) で、インターネット上の番組を見ることはできないのですか。

A . 学校情報ネットワークのセキュリティポリシーでは、不正サイトからの侵入防止やネットワークの負荷軽減を図るため、外部ネットワーク (インターネット) からのストリーミングデータと呼ばれる動画や音声などの情報を遮断しています。リアルプレイヤーは、内部ネットワーク上に用意された教材ビデオなどを視聴するためにお使いください。



セキュリティの学習

- 1 本時の位置 Web ページの閲覧や電子メールなどのネットワーク利用の学習を開始する前に行う。
- 2 指導目標 情報通信ネットワークのセキュリティについて理解させ、自己のアカウントの管理やパスワードに変更などセキュリティを確保する方法を習得させる。
- 3 目標行動 ネットワークを利用するためのアカウントを適切に管理できる。また、個人情報の保護やセキュリティの確保を理解して、暗証番号など実生活で使うさまざまなパスワードの自己管理ができる。
- 4 留意点 情報モラルの育成の観点から、次の事項を理解させる。
 - ・ アカウント
 - ・ ID
 - ・ パスワード
 - ・ セキュリティ
- 5 準備 パスワードをランダムに発生させて、生徒全員のアカウントを発行する。

6 展開

	学習内容	学習活動	留意事項	評価規準
導入	暗証番号	銀行のキャッシュカードの暗証番号や、携帯電話の電源入力時の暗証番号などの例を発表する。	暗証番号の役割について考えさせるが、ここでは深入りはしない。	
展開	個人認証 アカウント	個人認証の方法について学習する。 アカウントの意味を理解する。 <ul style="list-style-type: none">・ ログインアカウント・ メールアカウント	カードと暗証番号、携帯電話本体と暗証番号のように組み合わせたもので個人認証が行われることに気付かせる。 アカウントはコンピュータやネットワーク上の資源を利用できる権利であることを理解させる。	個人の権利と利益を守るための個人認証について説明できるか。

展 開	パスワード	<p>アカウントの発行について理解する。</p> <p>適切なパスワードを考える。</p>	<p>アカウントはサーバで発行され認証が行われることを理解させる。</p> <p>アカウントを発行すると、IDとパスワードが渡されることを説明する。</p> <p>IDは、端末パソコンを使用する時の利用者の名前に当たることを理解させる。</p> <p>どのようなパスワードがよいかを考えて作るよう教示する。</p> <p>電話番号や住所、誕生日、メールアドレスに関連するものは避けたほうがいいことに気付かせる。</p> <p>準備したIDとパスワードを生徒一人ひとりに渡す。</p>	<p>IDとパスワードが個人認証の方法として有効であることが説明できるか。</p> <p>自分には覚えやすく、他人には想像がつかないものを作ることができるか。</p>
	セキュリティ	<p>ネットワークにログイン(接続)し、パスワードの変更を行う。</p> <p>パスワードを自己管理することの重要性を考える。</p> <p>ネットワークのセキュリティ確保について学習する。</p>	<p>ネットワークの資源は自分自身と他人の財産であり、これを守るための責任について考えさせる。</p> <p>ネットワークの不正使用を許すことがどのような影響を与えるかを考えさせる。</p>	<p>パスワードの変更ができたか。</p> <p>ネットワーク資源や利用者一人ひとりの権利と利益を守るための個人認証について説明できるか。</p>
ま と め	まとめ	ネットワークの不正使用の防止について考える。	セキュリティの確保には不断の努力が必要であることを気付かせる。	セキュリティ確保の大切さとパスワードの自己管理の必要性を説明できるか。