2017年度 春学期・（火Ⅱ）

情　報

第11回目「情報と社会」

27. 情報社会の概観
28. 情報社会の規範とセキュリティ

東京学芸大学 自然科学系
宇宙地球科学分野 講師
西浦 慎悟

● 最初に

講義資料は、http://astro.u-gakugei.ac.jp/~nishiura

→「西浦クンの講義室」に縮小版（PDFファイル）を置く予定

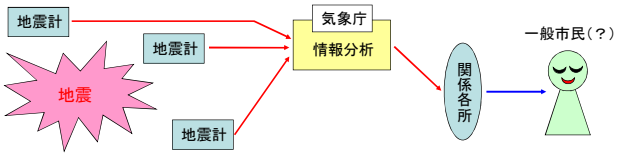
・国税電子申告・納税システム

「e-Tax」とも呼ばれる。インターネットを介した国税に関するオンライン・サービス。開発・運営は、国税庁から委託され、NTTデータが行っている。

→ 他にも様々な行政サービスがあるが、実際には、直接、役所などへ出向かなくてはならない事も少なくない（ただし、提出書類の書式は大抵DL可能）

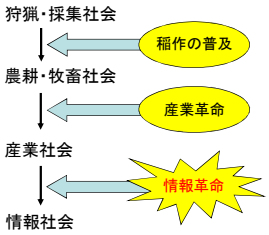
・緊急地震速報

気象庁が管理・運営する。地震発生直後に、各地の地震計の観測情報から地震の到達時刻・震度などを予想し、可能な限り迅速に、関係各所へ連絡するシステム。



● 情報社会・情報化社会

「情報」が、他の諸要素と同等かそれ以上の価値を持ち、これを中心に機能する社会を「情報社会」と呼ぶ。情報社会に向かって、現在進行形で変化している社会を「情報化社会」、より発展した情報社会を「高度情報社会」や「高度情報化社会」と呼ぶようだが、これらが厳密に区別されている訳では無さそうである（西浦私見）。



以前、社会の中心だったものが、新しいものに取って替わられる訳では無く、一般化・抱合化され、取り込まれて行く。

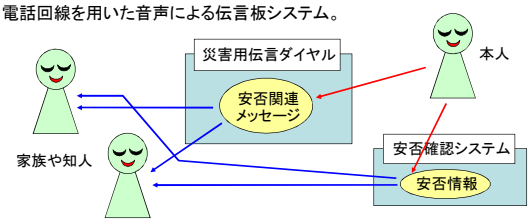
● 情報社会を象徴するその他のシステム

・安否確認システム

主にネットワークや通信に関連した企業が行う、災害時の家族・友人・社員の安否を確認するためのシステム。基本的には電子メールによる通知サービスである。

・災害用伝言ダイヤル

NTTコミュニケーションズが提供し、NTT東日本とNTT西日本が運営する、電話回線を用いた音声による伝言板システム。

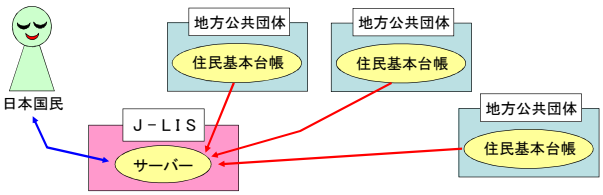


● 情報社会を象徴する行政システム

・住民基本台帳ネットワークシステム

住基ネットとも呼ばれる。各地方自治体が管理している住民基本台帳を電子化し、インターネットを介して、日本国民を特定する情報を行政機関で共有するシステム。回線にはIP-VPN（VPN = Virtual Private Network）が使用されている。地方共同法人地方公共団体情報システム機構（J-LIS）が運営する。

VPN = Virtual Private Network ： インターネット上の拠点間で、専用の接続方式や暗号化を用いることで構築される、仮想的な専用回線。特にISPが提供する専用IP網を使うものをIP-VPNと呼ぶ。



・販売時点情報管理システム

POSシステム（= Point of Sales System）とも呼ばれる。物品の売り上げを単品単位で集計・管理するためのシステム。バーコードとスキャナの普及によって、一般化した。

単なる売り上げ実績の蓄積に留まらず、数量や日時、場合によっては購入者の性別・年齢層、当日の天気などの情報とリンクして用いられることもある。

・ICカード

様々なデータを蓄積するために、集積回路（= IC）を、その内部組み込んだカード。携帯電話などのSIMカード、デジタル放送の視聴制御用のB-CASカード、決済用のICキャッシュカードなどで用いられている。電子マネーの普及に伴って、様々な機能を統合したICカードも登場している。

これ以前には、磁性体のテープを貼り付けた磁気ストライプ・カードが一般的だった。

● インターネットを介した経済/商業活動

・ネットショッピング / ネット通販

書籍、玩具、CD/DVD/BD、衣料品、装飾品、インテリア、各種ギフトなど

・ネットスーパー

食材、飲料、菓子、衣料品、日用品など

・ネット予約

コンサート、映画、航空機、鉄道、宿泊、レンタカー、診療など

・ネットオークション

各種グッズ、レアグッズ、新古品、中古品など

・ネットバンキング

上記に関連した支払い、各種振込・振替などなど

・アフィリエイト

成功報酬型広告。掲示広告を介して生じた利益を、実績に応じた報酬を広告掲示者に与える形式の広告。

→ 大抵のことは何でもできそう。

・知的財産権：

特許権（知財四権）

実用新案権（知財四権）

意匠権（知財四権）

商標権（知財四権）

著作権

・肖像権：他者から無断で撮影されたり、無断で公表・利用されない権利。

人格権(= 人格的利益を保護するための権利)

財産権

パブリシティ権 – 人に備わっている経済的価値などを保護する権利。

情報社会における様々な権利を心に留め、くれぐれも侵害することのないよう十分に注意すること。

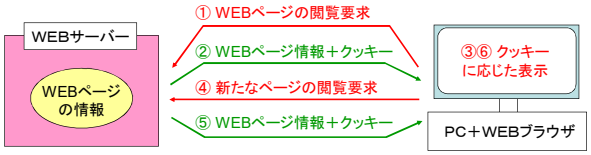
● Cookie（HTTP Cookie、クッキー）

WEBサイトが、閲覧者のWEBブラウザやPCに残す情報ファイル。
ユーザーの識別情報やセッションの管理情報などが記述されている。

・ログイン情報（ユーザーID、パスワードなど）の記憶

・ネットショッピング / ネットスーパーにおけるカートの内容物の保持

・サイトのアクセス記録



・セッション=ハイジャック：盗聴によってクッキーのセッションIDが第三者に知られると、ユーザーIDやパスワードが分らなくても、そのクッキーが有効な間は“なりすまし”を行うことが可能となる。→（設定）「クッキーを使用しない」設定にする

● よくある先生や研究者の勘違い

~~「商用目的で無く、教育や研究が目的であれば、著作権に抵触しない。」~~

~~→ だから、著作物に対して複製・改変などをやっても構わない~~

学校教員：「天文台が公開している天体画像を使って、教材を作りました」

（天文台のWEBページに「商用以外の研究・教育・普及活動には無許可で使ってOK」と記載）

→ 教材を、学校で児童相手に使ったら、評判が良かった！

→ 先生どうしの研究会で紹介・発表 → 違反

→ 専門機関で少年の更生目的で使用 → 違反

「先生同士の研究会」や「少年の更生目的の機関」は天文台のWEBページで示された目的・活動に合致しない。→ 事前に天文台に連絡を！

・共同利用で得た観測画像から作った天体のカラー画像の著作者は誰か？

オリジナルの観測データ → 観測所（？）、カラー画像 → 画像作成者（？）

28. 情報社会の規範とセキュリティ

● 情報社会における社会規範

・不正アクセス行為の禁止等に関する法律：

「不正アクセス禁止法」とも呼ばれる。

他者のアカウントの不正使用やセキュリティ・ホールを利用した認証の回避など。

→「不正アクセス行為」に対して、1年以下の懲役、または、50万円以下の罰金。

アカウントを、その所有者以外に提供するなど。

→「不正アクセス行為を助長する行為」に対して、30万円以下の罰金。

・個人情報の保護に関する法律：

「個人情報保護法」とも呼ばれる。「個人に関する情報」、「特定の個人を識別できる情報」、「他の情報と容易に照合できる情報」の保護。

対象は、5,000件以上の個人情報を扱う事業者。個人情報の適正管理、利用目的の通知と明確化。

● 情報社会におけるセキュリティ

・本人認証やアクセス権に関するセキュリティ意識を高める。

【 ユーザーとして 】

・他者に話さない、人目に晒さない。

・入力時に覗かれない。

・簡単に類推されるものにしない。

・なるべく長く、無意味なものにする。

・（困らない程度に）頻繁に変える。

【 システム管理者として 】

・試行回数を制限する。→ 例）銀行のATM

・試行速度を制限する。→ 例）次の入力まで一定時間の経過が必要

・ワンタイム・パスワードの使用 → ユーザーID、P.W.、使い捨てP.W.の併用

・乱数表を用いたマウス・クリックによる入力 → 例）ネットバンキングなど

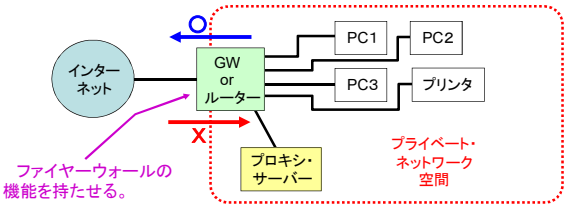
・セキュリティ性を意識してハードウェア / ソフトウェアを構築・使用する

【 システム管理者として 】

・プライベート・ネットワーク空間などによるファイヤーウォール（防火壁）を構築し、LAN内部のPCの保護を図る。

・プロキシ・サーバーを導入することで、外部アクセスへの安全性の向上化を図る。

・LANの内外を問わず、PCへのアクセスへは暗号化された通信を用いる。



・USBメモリは、パスワード設定できるものを使用し、これに保存するファイルにもパスワード設定や暗号化を施す。

→ これらの機能に対応したUSBメモリを使用する。

・内蔵型HDDにATAパスワードや暗号化を施す。
→ これらに対応した内蔵型HDDを使用する。

・PCを第三者に操作されないようにする。

ログイン認証（ユーザーID、パスワード）の設定

起動認証（BIOSパスワード）の設定

スクリーンセーバ復帰のためのパスワードの設定

・PCを紛失したり、盗難にあわないようにする。

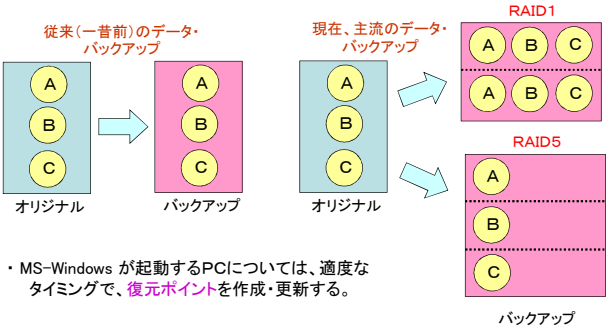
重要な情報の入ったPCはむやみに持ち歩かない。

重要なファイルは全てパスワード設定＆暗号化する。

持ち出されないようにワイヤーを用いて施錠する。

・重要なサーバーの情報などは、頻繁にバックアップを取る。

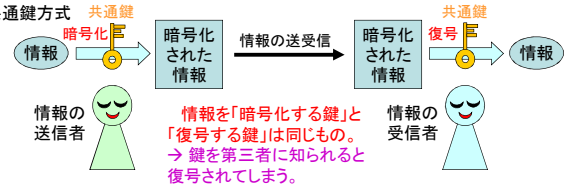
→ 手動による作業は不可能なケースが多いので、自動バックアップ・システムを構築することが必要。バックアップ先にはRAIDを用いるのが現在の主流。



・MS-Windows が起動するPCについては、適度なタイミングで、復元ポイントを作成・更新する。

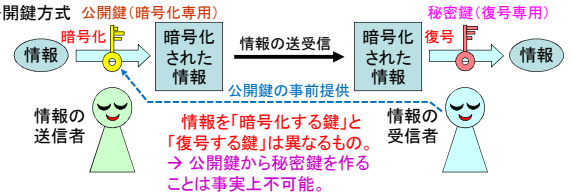
● 情報の暗号化

・共通鍵方式



情報を「暗号化する鍵」と「復号する鍵」は同じもの。
→ 鍵を第三者に知られると復号されてしまう。

・公開鍵方式



情報を「暗号化する鍵」と「復号する鍵」は異なるもの。
→ 公開鍵から秘密鍵を作ることは事実上不可能。

【 ユーザーとして 】

・他のPCやネットワークなどへのアクセスには、暗号化された通信を用いる。

→ 暗号化通信に対応した様々なクライアントが存在している。

・安全でないWEBサイトへはアクセスしない。

→ サイトが安全 or 危険の判断は難しいところだが・・・

・ウィルス対策ソフトなどのセキュリティ・ソフトウェアをインストールしておく。

・OSやアプリケーション、ウィルス定義ファイルなどのアップデートは頻繁に行う。

・MS-Windows の場合、適度なタイミングで復元ポイントを作成・更新する。

・漏洩した際に問題となるようなファイルには、パスワードを設定する、暗号化する、などの処理を施す（漏洩して困るファイルは持ち歩かないのがベスト）。

→ このためのセキュリティ・ソフトウェアは結構いろいろある。

・USBメモリは、パスワード設定できるものを使用し、これに保存するファイルにもパスワード設定や暗号化を施す。

本日の演習

インターネットを用いて、各班で以下の項目のいずれかについて調べ、代表者1名によって報告・発表せよ。なお、発表時間は一班あたり2分を目安とし、報告・発表は口頭のみで良い。

・テーマ1 ： 行政が行う情報サービスを1つ挙げて、その内容を簡潔に説明し、それに対して主張されている問題点や対策などを論ぜよ。

・テーマ2 ： ネットワークを介して、著作権や知的財産権が侵害されたケースを調べ、その概要と再発防止策・防衛策を論ぜよ。

・テーマ3 ： マルウェアによって引き起こされた実際の被害ケースを調べ、その概要と再発防止策・防衛策を論ぜよ。

・テーマ4 ： 教員や児童・生徒などを原因とし、ICT技術に関連した個人情報漏洩問題について調べ、その概要と再発防止策・防衛策を論ぜよ。

なお、各班で、本日中に（1）発表者の学籍番号・氏名、（2）本日の出席者の学籍番号・氏名、（3）本日の発表内容、をポータル/メセージにて、担当者まで提出すること。