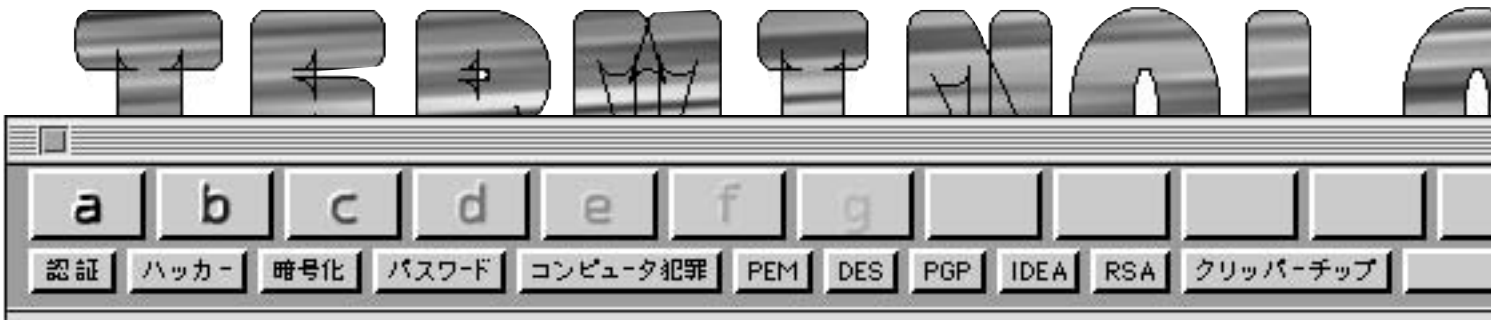
TERMINOLOGY of Internet



暗号化（encryption）

数理アルゴリズムを使用して、文章だけでなく音声や画像も含めたディジタル情報を第三者に判読できない形式に変換すること。暗号化には、共有鍵暗号化と公開鍵暗号化の2つの方式がある。

共有鍵暗号化（private key encryption）は、同じ1つの鍵をお互いが内密に所有してデータの暗号化と復号化を行う方式。DESなどがこれにあたる。この方式の欠点としては、鍵（合鍵）を配布中に盗聴された場合に用をなさないこと、大勢と交信する場合はその人数だけ鍵を用意しなければならないことなどがある。

公開鍵暗号化（public key encryption）では、秘密鍵（secret key）と公開鍵の2つのデータ暗号化鍵を使用して、データの暗号化と復号化を行う。秘密鍵は公開しないで内密に所有し、公開鍵は誰でも使用できるように一般に広く配布する。共有鍵暗号化とは異なり、この方式では、送信側と受信側で別々の秘密鍵と公開鍵を持つことになる。送信側では受信側が配布した公開鍵を入手し、それを使用してデータを暗号化して転送する。受信側では自分だけしか持っていない秘密鍵を使用して、それを暗号化する前のデータに復元する。このため、送信者であっても暗号化した後はそのデータを解読することはできない。また秘密鍵は公開されていないので受信者だけが復号化できる。Martin E.Hellman、Ralph Merkle、Whitfield Diffieによって考案された。RSAなどがこの方式にあたる。

DES【デス】

Data Encryption Standard（データ暗号化基準）の略。1960年代後半にIBMが開発した数理アルゴリズムの1つであり、1977年に米政府によって連邦情報処理基準として採用された。クレジットカードや銀行の自動預け払い機など、非軍事アプリケーションの共有鍵暗号化アルゴリズムとして、広く使用されている。

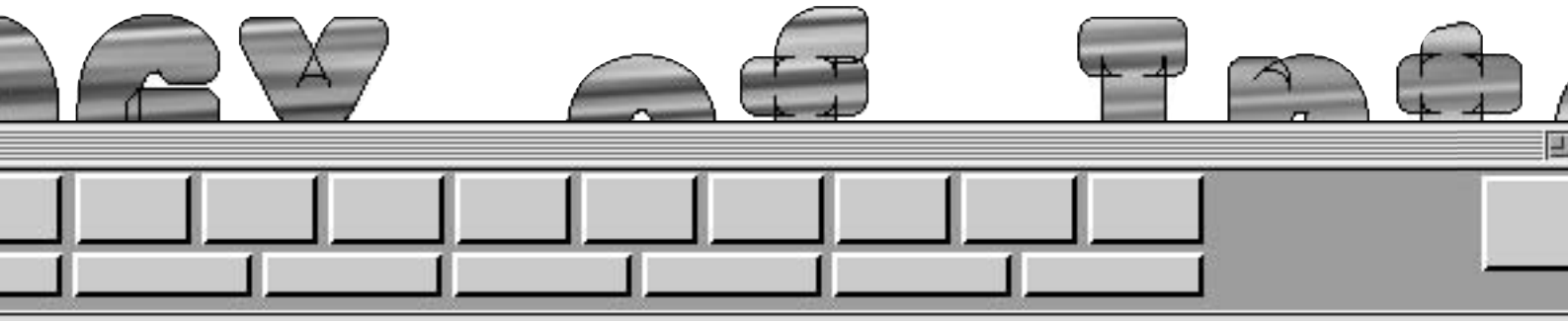
コンピュータ犯罪（computer crimes）

コンピュータの不正操作、不正利用、破壊行為などをコンピュータ犯罪と呼ぶ。具体的には、権限を与えられていない不正アクセス、クレジット番号などの個人情報の不正入手、データの改ざん、ウイルス（virus）やトロイの木馬によるプログラムの損傷などを指す。ウイルスとは、オペレーティングシステムやアプリケーションに取り付いて、それらに損害を与えるプログラムのこと。自分自身で複製を作り、他のシステムに「感染」することからコンピュータウイルスと呼ばれる。また、トロイの木馬（Trojan Horse）とは、データの不正入手、改変、破壊を行うためにコンピュータシステムに忍び込ませたプログラムのことで、表面上はシステムに必要な機能を提供しているように見せかけている。トロイ戦争で、ギリシャ軍が木馬に兵をひそませて敵地に侵入し、敵軍を破った故事にちなんでいる。

認証（authentication）

個人や法人を、「本人」であると相手側が確認する手続きのこと。通常は、入力されたユーザー識別番号やパスワードなどのログオン情報によって行う。日常生活とは違い、ネットワーク上では電子化されたデータから本人であることを確認しなければならないため、認証が必要になる。信頼できる第三者機関の設立も含めた認証システムとデータの機密性を保証する暗号化システムの確立がインターネットでの電子商取り引きを促すことになる。（先日、あるラジオ番組のパーソナリティがカナダのクレティエン首相の声色をまねて、エリザベス女王との電話インタビューに成功した事件があったが、これも本人認証に失敗した例の1つ）。

CIAの盗聴事件が話題になりましたので、今回はセキュリティ関係の用語を取り上げました。ご意見、情報などお待ちしております。E-mail to：**ip-term@impress.co.jp**



クリッパーチップ（Clipper Chip）

暗号化アルゴリズムを埋め込んだコンピュータチップのこと。米政府が標準化を提案している。チップには暗号化鍵も埋め込まれ、その親鍵（マスターキー）は政府が保持する計画になっている。犯罪情報が暗号化された場合、それを傍受することが事実上不可能になるため、コンピュータをはじめ通信機器への搭載を義務づけて、これを防止することが目的とされている。反面、あらゆる通信が政府に盗聴されるおそれがあることから、市民や産業界の反対にあっている。

PGP【ピージーピー】

Pretty Good Privacyの略。Philip Zimmermannによって開発された暗号化ソフトウェア。電子メールの暗号化だけでなく、秘話機能を提供するため、インターネット電話（例：PGPfone™）にも応用されている。暗号化アルゴリズムにはRSAとIDEAが使用されている。PGPとPretty GoodはPhil's Pretty Good Software社の商標。

パスワード（password）

コンピュータシステムやデータへのアクセスを制限するために使用されているユーザー固有の文字列のこと。正しく入力したときにのみアクセスが許可される。パスワードによるセキュリティを確実にするために、最小文字数、有効期間、変更禁止期間などを決めているシステムもある。パスワードに関してユーザーが留意する点としては、許可されている最大文字数まで使うこと、頻繁に変更すること、英字と数字と記号を混在させる（無意味な文字列にする）ことなどが挙げられる。

PEM【ペム】

Privacy Enhanced Mail（プライバシーを強化したメール）の略。電子メール暗号化方式の1つであり、インターネット標準として提案されている。暗号化アルゴリズムにはRSAとDESを使用している。

IDEA【アイディーイーエー】

Improved Data Encryption Algorithm（改良型データ暗号化アルゴリズム）の略。DESと同様の共有鍵暗号化アルゴリズムの1つ。James L. MasseyとXuejia Laiによって開発され、1990年に発表された。

RSA【アールエスエー】

Rivest-Shamir-Adlemanの略。公開鍵暗号化アルゴリズムの1つであり、開発者の名前（Ronald Rivest、Adi Shamir、Leonard Adleman）を取ってRSAと名付けられており、現在、最も広く支持されている。RSAは米国で特許が成立していること、また暗号化システムは武器であるとの認識からフルセット版の輸出は禁止されているため、海外ではサブセット版の使用のみが許可されている。

ハッカー（hacker）

悪意を持ってコンピュータシステムに不正侵入し、コンピュータを悪用して詐欺を行ったり、システムに損害を与えたりする者のこと。米国の法曹界ではコンピュータ犯罪に及ぶ行為全般をハッキング（hacking）と呼んでいることから、この用語が一般的に使用されている。

After care

デレゲートサーバー　前号の「delegate」を「DeleGate」に、「デレゲート」を「デリゲート」に訂正します。（村上昌文さんからご指摘いただきました）。

POPメール　前号の「電子メールを読み書きする方法の1つ」を「電子メールを読み書きするプログラムの1つ」に訂正します。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp