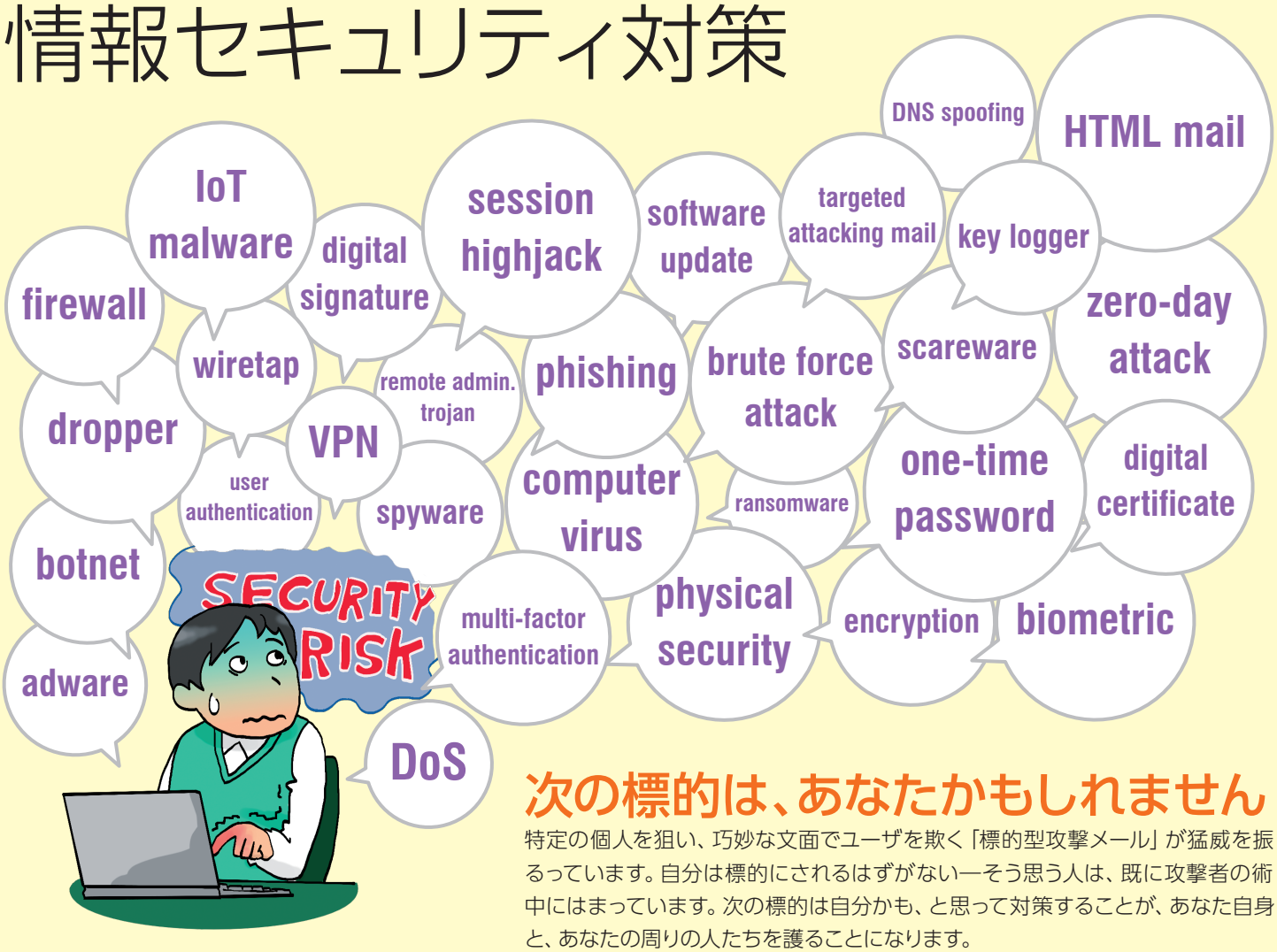
情報セキュリティ対策



次の標的は、あなたかもしれません

特定の個人を狙い、巧妙な文面でユーザを欺く「標的型攻撃メール」が猛威を振るっています。自分は標的にされるはずがない―そう思う人は、既に攻撃者の術中にはまっています。次の標的は自分かも、と思って対策することが、あなた自身と、あなたの周りの人たちを護ることになります。

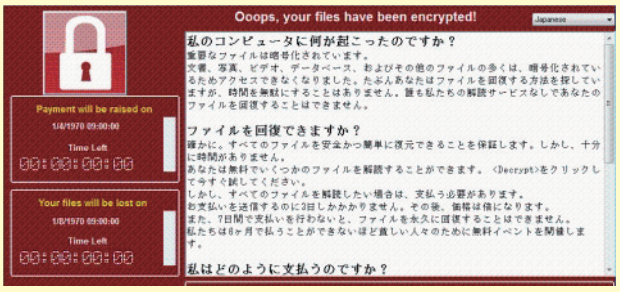
どうして自分の情報が漏れるの？

論文発表や社会的な活動は、自分の立場や興味を世間に広言しているようなものです。他の人のSNSに自分のことが書かれることもありますし、攻撃の被害にあった他人のコンピュータやスマートフォンから、あなたの情報が漏えいする可能性もあります。これら断片的な情報があれば、あなたが普段どのようなメールを送受信しているかも想像できてしまいます。

SNSからの漏洩イメージ

攻撃の被害に遭うとどうなるの？

大切なデータが消去されたり、あなたのアカウントから迷惑メールが発信されたりします。データを暗号化して人質に取り、元に戻すための身代金を要求する「ランサムウェア」の被害も問題になっています。その一方、表面的には何の変化も起こさず、長期間にわたって、ユーザの行動を逐一監視するようなコンピュータ・ウィルスもあります。どのような被害が発生するか、予想できないというのが実際のところです。

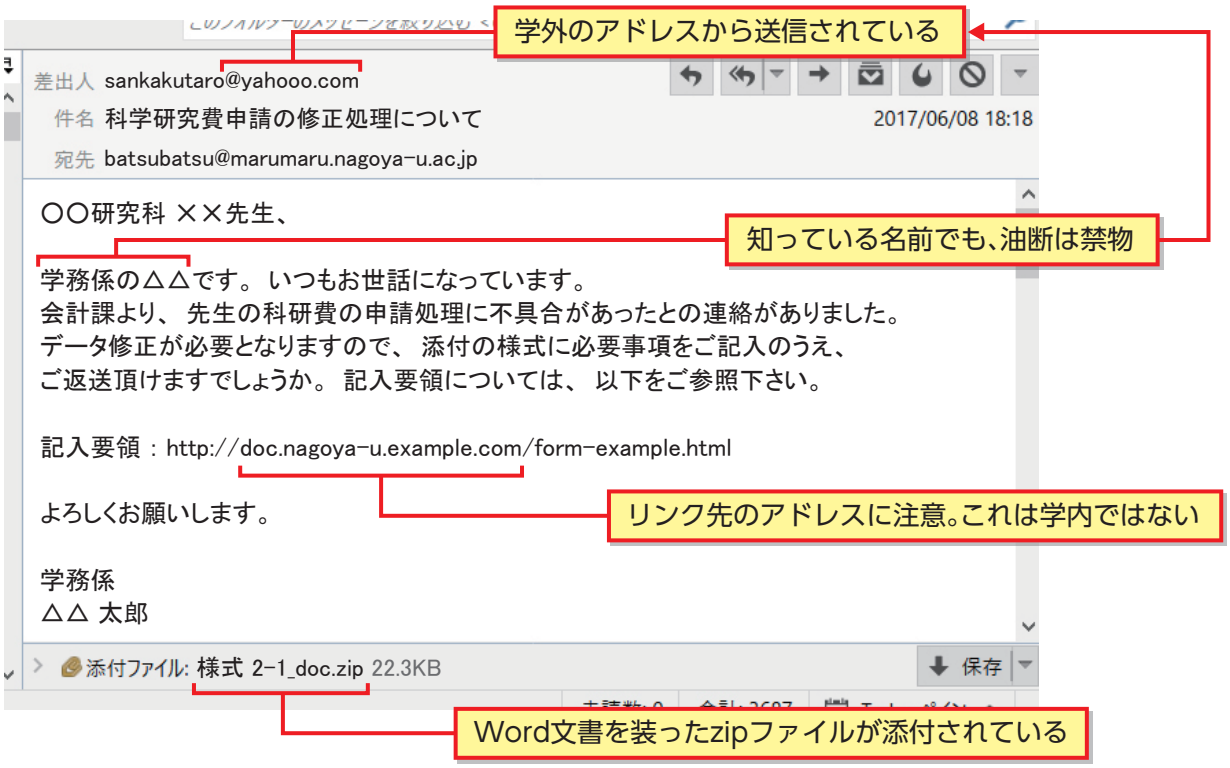


情報処理推進機構（IPA）Webページより ※一部加工しています
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

対策法は裏面へ

メールの中の怪しそうな部分を見抜く

攻撃の典型的な手口を知っておけば、多くの（全てではありません）不正メールを見抜くことができます。
メールを受け取ったら、以下のような点に注意して確認してみてください。



可能であれば、以下のような対策も有効です。

- ☐ HTMLメールの使用は避ける（メールの偽装工作を抑止する）
- ☐ メールヘッダの詳細を表示させ、配送経路を確認する（送信アドレス偽装を見抜くのに役立つ）
- ☐ メール以外の手段で、送信者に確認を取る

万一に備え、多重の対策を

万一の事態に備え、セキュリティ対策を多重に施しておくことが重要です。
以下は、比較的簡単に実行でき、効果の高い対策法です。

ソフトウェア・アップデートは自動設定に

ソフトウェアの不具合が悪用されるのを防ぐため、メーカーは定期的に修正用プログラムを配布し、ソフトウェアを更新（アップデート）することを呼びかけています。アップデートが速やかに適用されるよう、自動でアップデートを行う設定にすることを強くお奨めします。アップデートの仕組みのないソフトウェアや、メーカーがサポートを終了した古いソフトウェアでは、致命的な不具合が放置される可能性もあります。そのようなソフトウェアの使用は危険ですので、絶対にやめてください。

定期的なバックアップを

コンピュータウィルスに感染すると、データが消去されたり、使えなくなったりする可能性があります。たとえ「身代金」を払っても、データが帰ってくる保証はありません。あなたの作ったデータは、どこにも売っていません。定期的に、自分自身でデータのバックアップを取るようにしてください。

セキュリティ対策ソフトウェアの利用を

セキュリティ対策ソフトウェアにより、既知の攻撃の多くを防ぐことができます。名古屋大学はシマンテック社のセキュリティ対策ソフトのサイトライセンスを保有しており、本学の所有の機器（レンタル品も含む）であれば、無料で利用することができます。
詳しくは、情報連携統括本部のホームページ http://www.icts.nagoya-u.ac.jp/ja/services/sitelicense/ を参照して下さい。

発行・編集：名古屋大学情報連携統括本部広報委員会
〒464-8601 名古屋市千種区不老町
TEL:052-789-4352 FAX:052-789-4385
2017年7月