

# 情報科学概論

名古屋大学における  
情報セキュリティについて

情報基盤センター

小川 泰弘

# 情報セキュリティとは？

- 計算機の利用
- ネットワークの利用
  - 以前は専門家だけ
  - 最近は、利用が広がり犯罪者も利用
- 様々なセキュリティを考える必要がある

情報系の学生は、より専門的な理解を！

# 名古屋大学 情報セキュリティガイドライン

- 名古屋大学では、全構成員が守るべきガイドラインを作成
- 情報連携統括本部のサイトに掲載

[http://www.icts.nagoya-u.ac.jp/  
ja/security/guideline.html](http://www.icts.nagoya-u.ac.jp/ja/security/guideline.html)

# 情報セキュリティの概念

- 利用者は誰か？  
    認証: Authentication
- 何ができるか？  
    権限・権利管理: Authorization
- 安全に通信しているか？  
    暗号化通信: Encryption
- 機器は安全か？  
    機器の完全性(ウィルス対策): Anti-Virus

# 利用者は誰か？

- 利用者認証： ユーザID、パスワード
  - 「名古屋大学ID」
- 名古屋大学IDは、すべての基盤
  - 絶対に他人・友人等には貸さないこと
- 他人が利用すると、大きな問題が生じる
  - 問題の責任を問われる場合も

# 何ができるか？

- 名古屋大学IDは、多様に利用
  - 履修登録
  - 電子メール
  - 情報メディア教育センターの端末
  - NUCT (WebCT)
  - その他、多様な情報システム

# 何ができるか？

- 名古屋大学IDは、多様に利用
  - 履修登録
  - 電子メール
  - 情報メディア教育センターの端末
  - NUCT (WebCT)
  - その他、多様な情報システム

してはいけないことも！

# 何をしてはいけないか

- 他人の権利を侵すこと
  - 著作権・プライバシーなどを侵す
  - 誹謗・中傷などをインターネットなどへ記載
- 権限のないシステムを利用すること
  - パスワードを盗む・推測する、クラックツールを使う
  - 不正アクセス防止法によって処罰
- 目的外の利用
  - 大学のシステムをバイトに利用
- 過剰利用
  - 大量のメール送信など



# 著作権侵害

- 違法なファイル共有
  - Gnutella, WinMX, Winny, Share, 迅雷(Xunlei)
  - 学内ネットワークは監視対象
- ソフトウェアのライセンス違反
  - 違法コピー
    - ◇ 研究室内でライセンス数以上に使用
    - ◇ 研究室のソフトを自宅で使用

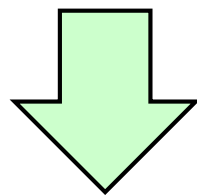
# 著作権侵害違反事例1

- 一昨年度は名古屋大学で3件発生
  - BitTorrent で映画ファイルを交換
  - 米国著作権管理団体から計算機(IP)を特定して指摘
  - 学生もしくは所属研究室が判明
  - 学生および指導教員が研究科長から嚴重注意

訴訟問題に発展する可能性もありうるので注意

# 著作権侵害違反事例2

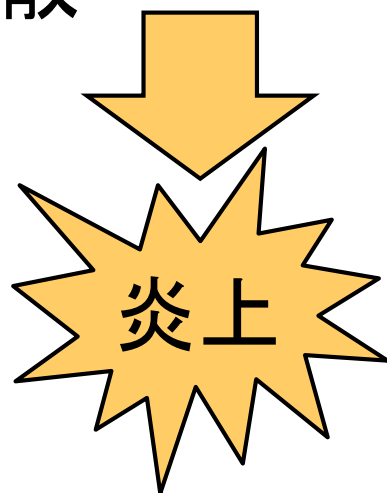
- 大学での Winny の利用
  - 2ちゃんねる に FQDN が掲載される
  - 2研究室が該当
  - 大学関係者が発見し、センターへ通報



大学でのネットワーク監視へ

# 不適切な情報の拡散

- 掲示板などでの誹謗・中傷
- Twitter などでの飲酒・犯罪の告白
- デマの拡散



インターネットは世界中と繋がっている

# インターネット上の匿名性

- 基本的にはない
  - その気になれば特定可能



[PR]

発信元を匿名化するソフトを使い、出版

アクセス禁止法違反な  
認めているという。

サイバー犯罪対策課  
ようにするソフト「T  
パーに侵入、同社のサイト

自分が特定されても問題ない  
発言・行動を行う

少年は、サーバー会社を装ったメールを出版社の社員に送信。偽サイトに誘導して社員  
のIDやパスワードを盗み、出版社のサーバーに侵入した、と同課は説明している。

少年はツイッター上で「Ochiaki」と名乗り、様々なサイバー攻撃に関わったと  
書き込んでいた。同課が押収した記録媒体からは、他人のツイッターアカウントを乗っ取  
り、都内の弁護士への殺害予告ツイートを大量にさせた痕跡も見つかったといい、同庁は  
同法違反などの疑いで調べる。

# 安全な通信

- インターネット上の通信は他人から傍受される可能性
  - 安易にパスワードなどを入力しない
- 暗号化されているか可能な限り確認
  - SSL(ブラウザの鍵マーク)

# SSLのマークの一例



# SSLマークが無い例



The screenshot shows a web browser window with the address bar displaying `https://www.west-frc.com/webs/W714100S`. The browser's address bar and toolbar do not show a lock icon, indicating a lack of SSL certification. The page content includes a navigation menu with items like "CLUB NTT-West", "約款ご確認", "お申し込み", "詳細情報", "内容確認", and "お申し込み完了". Below this is a table with two columns: "お申し込みサービス" and "クレジットカード支払い(新規)". A notice states: "契約約款 クレジットカード支払規約 プライバシーポリシーをご確認のうえ、お申し込みフォームへお進みください。". A list of bullet points follows, detailing requirements for credit card payments. Below the text are logos for "NTT Group Card", "MasterCard", "VISA", "JCB", "AMERICAN EXPRESS", and "Diners Club INTERNATIONAL". Further down, more bullet points provide information about payment terms and card validity. A green callout box on the right side of the page contains the text "SHA-1署名が原因".

クレジットカード支払い

← → ↻ `https://www.west-frc.com/webs/W714100S` ☆

## クレジット

CLUB NTT-West ○ 約款ご確認 ○ お申し込み ○ 詳細情報 ○ 内容確認 ○ お申し込み完了 ○

お申し込みサービス	クレジットカード支払い(新規)
-----------	-----------------

契約約款 クレジットカード支払規約 プライバシーポリシーをご確認のうえ、お申し込みフォームへお進みください。

- クレジットカード支払いをお申し込みいただけるお客様  
電話ご契約者、電話ご契約者の家族(配偶者、同居親族、父母、子等) または電話料金等のお支払い者
- 取り扱いクレジットカード  
以下のマークのあるクレジットカードをご利用いただけます。



- 口座引落とし日  
お客様のご指定のカード会社の規約に基づく口座引落とし日
- ご利用料金のお知らせ  
クレジットカードによるお支払い開始後は、書面によるご利用料金のお知らせ等の送付はなくなり、ご利用料金のお知らせ等の確認は、インターネットでご覧いただく「Myビルング」のご案内となります。  
※複数の電話回線をお持ちで、それぞれの請求書の金額を1枚の請求書でお支払いいただいているお客様には、ご利用料金内訳書を送付させていただきます。(なお、インターネットのアクセス回線とひかり電話を一枚の請求書でお支払いいただいているお客様は、電話番号単位で既にご利用料金がまとめられている為、上記のご利用料金内訳書を送付いたしません。)
- ご利用カードの有効期限等について  
ご登録のクレジットカードのカード番号や有効期限が変更になった際は、書面またはインターネットで再度お申し込みが必要となりますのでご注意ください。

※上記の内容でご不明な点がございましたら料金お問合せセンターへ連絡をお願いします。  
料金お問合せセンターの連絡先は [こちら](#)

**SHA-1署名が原因**



# セキュリティ上のリスク

- マルウェア
  - ウィルス
  - トロイの木馬
  - スパイウェア
- フィッシング
- ファーミング

# マルウェア (malware)

- 悪意のあるソフトウェアの総称
- 「不正プログラム」とも呼ばれる
  - ウィルス
  - トロイの木馬
  - スパイウェア
  - バックドア
  - 悪質なアドウェア などなど
- 悪戯から金儲け、犯罪行為へ

# コンピュータ・ウイルス (virus)

- ファイルからファイルに感染
- 当初は実行ファイル、  
現在はWord, Excel, 画像など何でもアリ
- 報道では他のマルウェアと混同される
- 多種多様な感染経路

# トロイの木馬 (Trojan horse)

- コンピュータ内に潜み悪質な動作をする
  - ファイルの削除・改変
  - アンチウィルスソフトの無効化
  - バックドアの設置
  - 他のプログラムのダウンロード  
(スパイウェアなど)
- 他のファイルに偽装して実行→感染

# スパイウェア (spyware)

- ユーザの情報を秘密裡に収集・送信
  - キーロギング
  - パスワードの奪取
  - ファイルの転送
  - ブラウザハイジャック
  - 偽の警告メッセージ
- 他のファイルに偽装して実行→感染
- 他のプログラムとセットになっていることも

# フィッシング (phishing)

- 本来とは異なるウェブページを表示
  - メール本文のURLをクリック別ページへ
  - 短縮URL
- 事例
  - UFJ銀行のHPを模したサイト
    - ◇ ユーザIDとパスワードを入力させる
    - 口座の認証情報が盗まれる
  - 学内にフィッシングサイトが構築されたことも

# ファームィング (pharming)

- DNSの設定を書き換える
  - ↳ URLをIPアドレスに変換
- 偽のサイトへ誘導
- 偽装手口
  - ブロードバンド・ルータの設定変更
  - PCの hosts ファイルの変更  
(トロイの木馬などによる)

# 様々な感染事例

- ウェブサイトを見るだけで感染
  - 信頼できないサイトを閲覧しない
  - 信頼できないリンクをクリックしない(掲示板)
  - **Java Scriptの無効化**で防げることも
- 短縮URLの悪用
- メールを開くだけで感染(添付ファイル、HTML)
  - **メールを受け取るだけで攻撃を受ける場合も**
- ネットに接続するだけで感染
- USBメモリを通じて感染



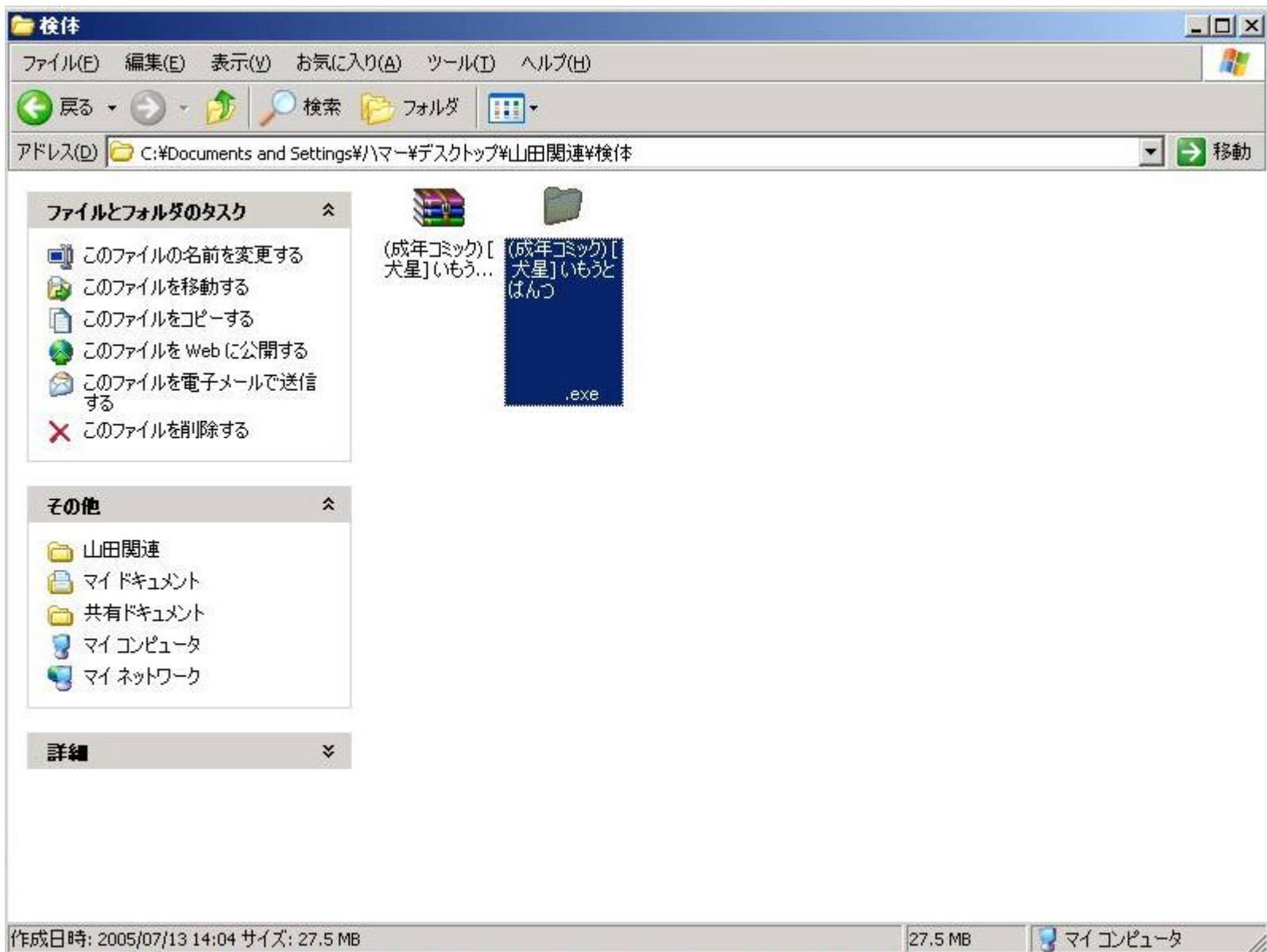
# Winnyの危険性

- 通常ファイルやフォルダを偽装した実行ファイルが存在
- 誤ってファイルを実行すると、
  - ウィルスが動作 (例: 山田オルタナティブ)
  - コンピュータ内のファイルをインターネットに公開
  - 画面をキャプチャ

学内でも感染事例あり！

# ファイル名の偽装


- アイコンの偽装




編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)



C:\Documents and Settings#\ユーザー#\デスクトップ#\山田関連#\検体

- ファイルとフォルダのタスク** 
- ファイルの名前を変更する
  - ファイルを移動する
  - ファイルをコピーする
  - ファイルを Web に公開する
  - ファイルを電子メールで送信する
  - ファイルを削除する

- 場所** 
- 山田関連
  - マイドキュメント
  - 共有ドキュメント
  - マイコンピュータ
  - マイネットワーク



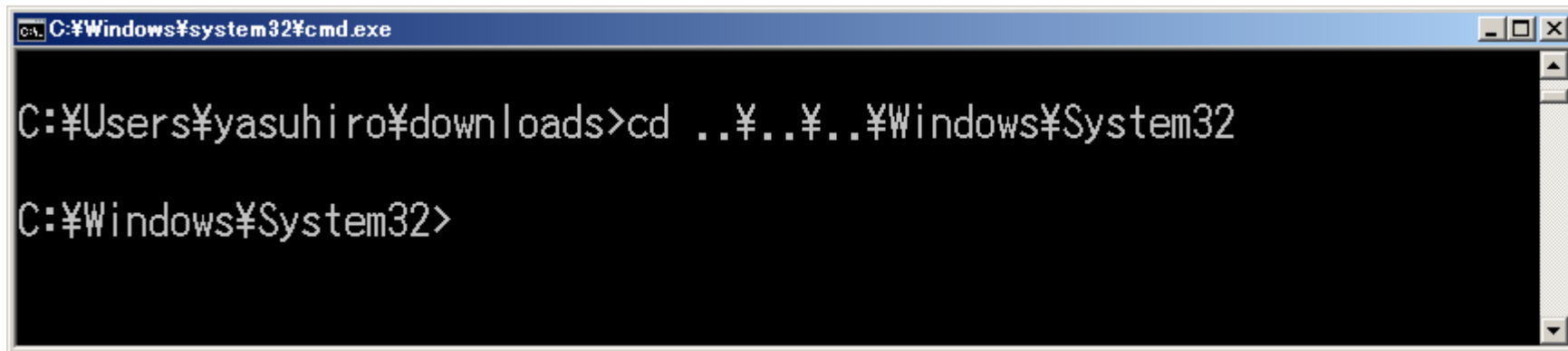
# ファイル名の偽装

- アイコンの偽装
- RLTrap
  - Unicodeの制御文字 RLO を利用し exe を隠す



# 圧縮・解凍ソフトの脆弱性

- 予期せぬディレクトリへファイルを解凍
  - 相対パスの悪用



```
C:\Windows\system32\cmd.exe

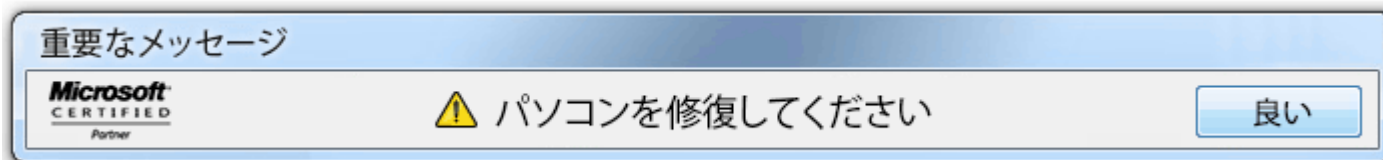
C:\Users\yasuhiro\downloads>cd ..\..\..\Windows\System32

C:\Windows\System32>
```

- 同じライブラリの利用による脆弱性の拡大

# ユーザの誘導

- 怪しげな広告バナー



- 「ウイルスに感染しています」と  
虚偽のメッセージが出ることも

# 怪しげなソフトのインストール

RegClean Pro

Systweak 社製品

## Windows Vista PC 修理



Microsoft Partner  
Gold Application Development



### システム情報:

現在マシンが起動中です: **Windows Vista**

Registry Cleaner アプリケーションは、お使いのオペレーティングシステムと互換性があります。

ダウンロードを開始

ファイルサイズ: 3.10 MB(ブロードバンド接続において約 10 秒間)  
要件: Windows XP/Vista/7/8(32/64 ビット)  
ダウンロード:

RegClean Pro は **5 つ星評価**を数多く受けた製品であり、これまで世界中で **1,000 万人**を超える方々に使用していただいています。無償版では、レジストリの問題をスキャンし、エラーを最大で **15 個**まで修復します。利点として、以下が挙げられます:

- ✓ コンピューターのパフォーマンスが高速化
- ✓ コンピューターの起動時間が短縮
- ✓ アプリケーションのエラーメッセージの数が減少
- ✓ コンピューターが安定化

### ステップ1

ダウンロードを開始

### ステップ2

「実行」または「保存」ボタンが表示されたら、これをクリックします

### ステップ3

システムの稼働が遅くなる原因となっているエラーを修復します!



# パソコン遠隔操作

- ウェブサイトの脆弱性
- トロイの木馬 `iesys.exe`
- バックドアからの侵入
  
- 犯罪予告の書き込み

# ブルートフォースアタック

- パスワードを総当たりで試す
  - ログイン回数の制限で防げる
- リバースブルートフォースアタック
  - パスワードを固定して、ユーザIDを変更
  - JAL と ANA が侵入される
  - ユーザ側では対策できない

# パスワード

- 頑健なパスワードの使用
  - ID・名前・誕生日・電話番号はダメ
  - 短いものはダメ(最低8文字)
  - 数字・記号を混ぜる
  - 使いまわしをしない
- 他人に教えない

定期的な変更は一長一短

# 解けない暗号

- ワンタイムパッド(one time pad)
  - 暗号鍵として平文と同じ長さの乱数を使用
  - 理論上、解読不能
  - 類似: バーナム暗号

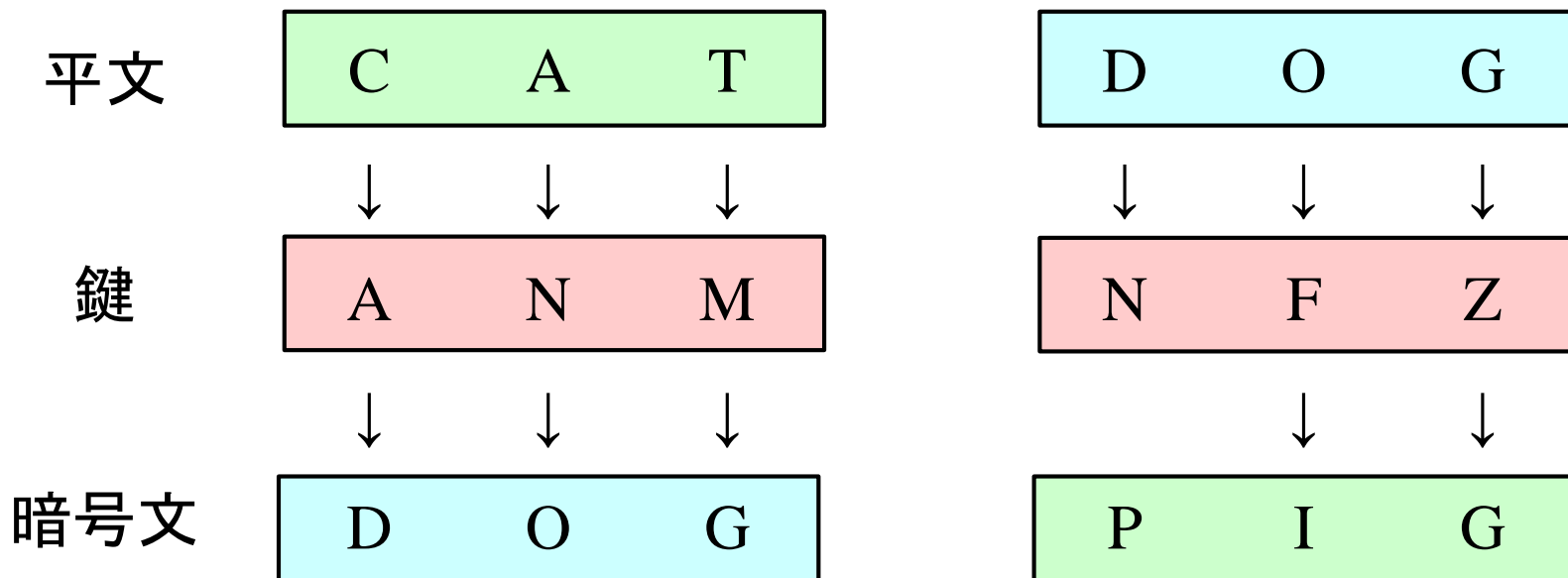
鍵が変わると  
全く別の文

平文	C	A	T	D	O	G
	↓	↓	↓	↓	↓	↓
鍵	+1	+14	+13	-14	-6	-26
	↓	↓	↓	↓	↓	↓
暗号文	D	O	G	P	I	G

# 解けない暗号

- ワンタイムパッド(one time pad)
  - 暗号鍵として平文と同じ長さの乱数を使用
  - 理論上、解読不能
  - 類似: バーナム暗号

鍵を文字列にすることも可能



# ワンタイムパッドの鍵

- 毎回変更する
  - 異なる平文に同じ鍵を使用しない
  - 平文より短くして繰り返さない
- 生成に疑似乱数を使わない
- 安全に配送する

実用性は高くない

# 自分だけは安全？

- いつ被害者になるか
- いつ加害者になるか

# 対策

- Windows Update などのソフトの更新
- セキュリティパッチの適用
- アンチウィルスソフトの導入
  - <http://w3serv.itc.nagoya-u.ac.jp/sitelicense/antivirus/>
- 信用できないファイルをクリックしない
  - 知人からのメールの添付ファイルにも注意
- Windows XPの使用禁止
- 頑健なパスワード



# 対策の限界

最大のセキュリティホールは人間

- 単純なパスワード
- セキュリティ対策の不備
  - パスワードなどが初期設定のまま
- 情報機器の紛失
- 無線LANの盗聴・ただ乗り
- 電子メールによるパスワードの問合せ
- パスワードの盗み見
- 振り込め詐欺

ソーシャルハッキング

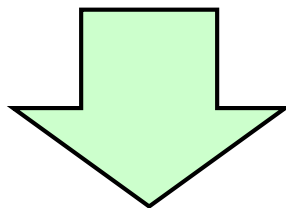
# インターネット空間

- 「仮想空間」？
  - 仮想でもあり、現実でもある
  - “virtual”の誤訳。本来の意味は「実質上の」
- ネットは現実社会の一部であり、  
現実社会の写像でもある
  - 現実社会に無いものはネットにも無い
  - 現実社会とネットは相互に影響を与え合う

# 「ネットde真実」

- 「ネットで真実を知った」
- 「マスコミは隠している」

ネットには正しい情報も間違った情報も存在



たいていの「真実」に辿りつける

# 名大の情報セキュリティ窓口

## □ITヘルプデスク

- 電話: 052-747-6389
- E-mail: [it-helpdesk@icts.nagoya-u.ac.jp](mailto:it-helpdesk@icts.nagoya-u.ac.jp)

## □情報連携統括本部

<http://www.icts.nagoya-u.ac.jp/>

名古屋大学 情報連携統括本部 - Windows Internet Explorer

http://www.icts.nagoya-u.ac.jp/ja/

名古屋大学 情報連携統括本部

一般の方 教職員 / 学生の方 情報システム管理者 日本語 English

ITヘルプデスク  
電話でのお問い合わせは 052-747-6389

情報連携統括本部 情報基盤センター 情報戦略室 情報メディア教育システム



Information インフォメーション

イベント 2015年07月07日 平成27年度第4回名古屋大学情報連携統括本部公開講演会・研究会のご案内

イベント 2015年05月28日 平成27年度第3回名古屋大学情報連携統括本部公開講演会・研究会のご案内

# レポート

今回の講義内容について、どの程度事前に知っていたか、感想と合わせて記述

- 提出形式：PDF
- 提出先： yasuhiro@is.nagoya-u.ac.jp  
Subject は「**情報科学概論レポート**」
- 締め切り： 5月31日