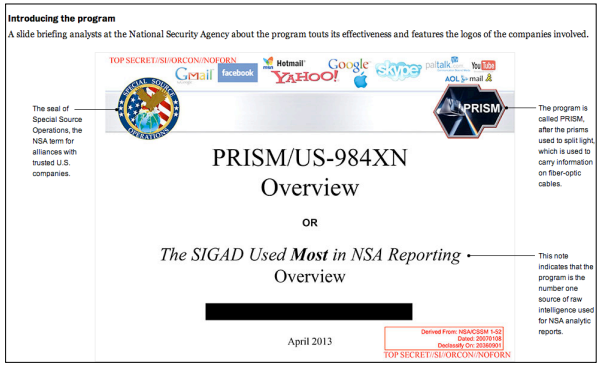
通信コンテンツの安全性

通信内容を守る
公開鍵暗号
暗号化の諸問題

大東文化大学
経営学部 水谷正大

http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

NSA Prism program



現在のIPv4の標準通信では

フツウのTCP/IPにはセキュリティ機構はない

- TCP/IP v4では、IPsec（IPパケット単位で安全性確保）などのセキュリティ機構は標準ではなく、まだ広く使われていない
- 心配事（･ω･）
  - 相手にメッセージは届いているか？誰かにメッセージを読まれていないか？
  - 届いたメッセージは改ざんされていないのか？
  - 受け取ったメッセージは誰が出したのか？.

ディープ・パケット・インスペクション

Deep Packet Inspection

メッセージが途中ルータを経由する通過する際に、パケットのヘッダ部だけでなくデータ部内を検査すること

コンピュータウイルス？、スパム？、侵入？とか、そのパケットを通過させるかや別の宛先に転送するかを勝手に判断したり、統計情報を収集する

一般企業、サービスプロバイダ、政府などが様々な用途で使用

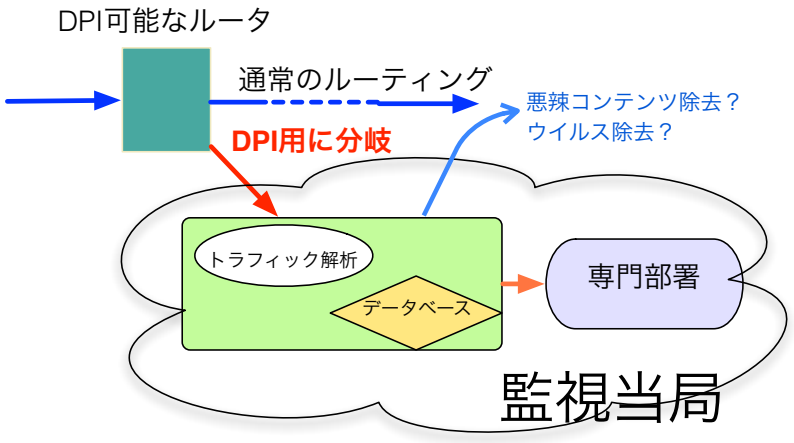
アメリカNSA、中国、イランなど。。

ユーザは途中で何が起ったかを知る手だてがない

DPIとネット中立性

インターネットのコンテンツ層の検査が不当に使われインターネットのオープン性を損なうようになるのではないかと懸念

DPIを使うと。。



通信の不正行為

盗聴

当事者以外の第三者が通信内容を知ること　DPIなどを含む

改ざん

作成した本人以外の第三者によってデータを勝手に書き換えること

成りすまし

不正な利益を得るために、他人のふりをすること

Phishing詐欺：偽造メールや偽装Webページにより不正に情報を得る

事後否認

当事者のどちらかが、情報をやりとりした事実を否定したり、情報の内容が改ざんされていると主張

安全な通信とは

不正行為がなされない通信

正しい通信相手と

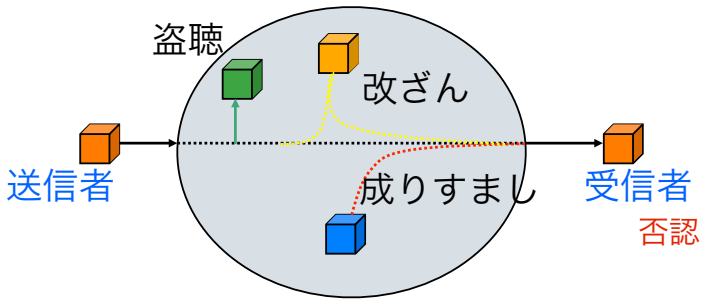
通信内容が他人に知られずに

本物（途中で改ざんされてない）で

読んだ・読まないと難癖なく

通信できること

ネットワーク回線上で何が起こり得るか



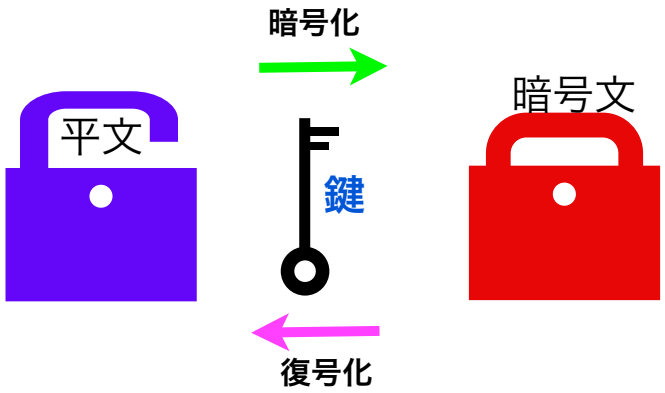
安全な通信の用語

- 暗号化
  - 通信にあずかる両者以外の第3者に交信内容を察知できないような通信
- 署名
  - 届いたメッセージが誰からのものかを確認できる通信
- 内容証明
  - 届いたメッセージが改ざんされていないことを確認できる通信

暗号学（Cryptography）

- 平文(ひらぶん) (Plain text)と暗号文(Cypher text)
- 暗号化(Encription, or Coding)
  - 平文から暗号文への変換
- 復号化(Decription, or Decording)
  - 暗号文から平文への変換
- 変換方法を固定
  - 平文と暗号文が1対1に対応
- 暗号化の鍵（Key）
  - 暗号化・復号化変換を具体的に定めるパラメータ

暗号化と復号化、鍵



シーザー（Caesar）暗号

- アルファベット文字を k 文字ずらす
  - 暗号化 c = e(p) = p + k (mod 26)
  - 復号化 p = d(c) = c - k (mod 26)
- k が暗号化キー
  - 暗号化と復号化とで共通鍵
- 例
  - ‘IBM’ を一文字前にシフトして’HAL’

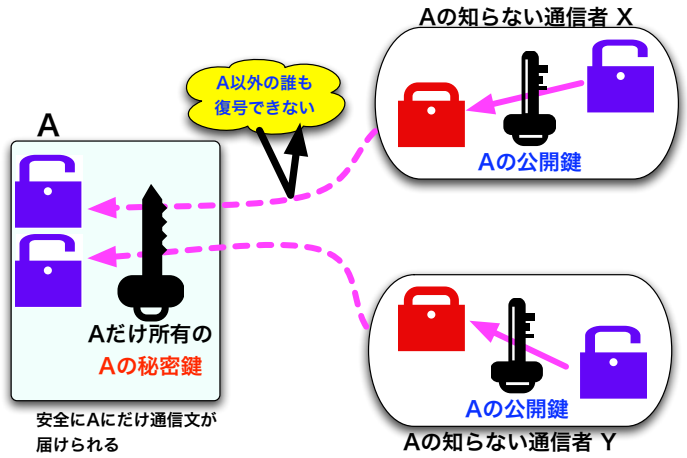
暗号の歴史

- 古典的暗号システム（ローマ時代から）
  - 共通鍵暗号システム（対称暗号システム）
  - 鍵の配送など運用上の欠点がある
- 公開鍵暗号システム: Diffie-Hellman(1976)
  - 公開鍵と秘密鍵の2つを使う
  - 不特定の相手と秘密の通信が可能
  - インターネット利用で必須な能力を備えている

公開鍵暗号方式の原理

- 計算量の理論に基づいた方式
  - 数学的には公開鍵から秘密鍵を見出すことが可能だが時間がかかりすぎ事実上不可能な作業
    - 例：電話番号から名前を見つけることはきわめて困難
- 一方向関数を使って文を変換する
  - 例：平文（名前）から暗号文（電話番号）
- 例）RSA方式（2006年9月まで米国特許だった）
  - 素因数分解の困難性を利用(1978年)

公開暗号方式--２つの鍵の役割

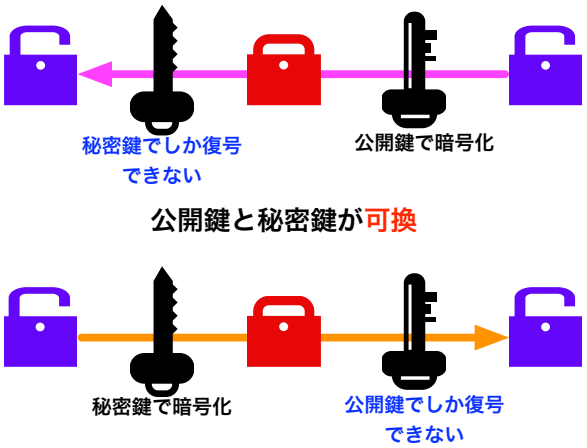


n人の間で秘密に通信する

鍵の配送の問題

- 古典暗号方式
  - 各人が(n-1)個の他人の暗号鍵を管理
  - 全体で n(n-1)/2 個の鍵を安全に管理する必要
  - 仲間が1人増えると n個の鍵を秘密裏に配送
- 公開暗号方式
  - 各人は1つの自分の秘密鍵だけを管理
  - 各人は自分の公開鍵を公開登録する
    - 人数は任意に増減できる

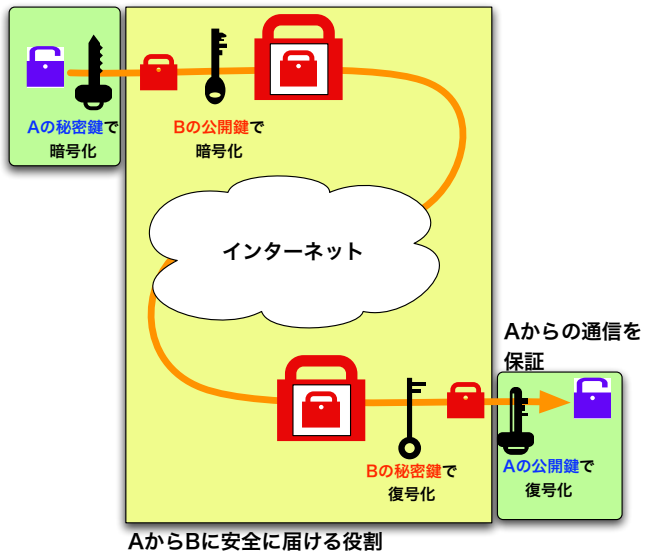
公開鍵暗号方式で望ましい鍵の性質



誰がメッセージを書いたのか

- メッセージの真偽を確かめる
  - 改ざんの防止
  - 内容証明通知
- 署名：本人でしか為し得ない印を付加する
  - 秘密鍵を使った電子署名

電子署名の仕組み



公開鍵暗号でも解決できない問題

公開鍵の認証

入手した公開鍵は本当に正しい相手の公開鍵なの？

公開鍵基盤（PKI）

公開鍵を真正に運用するための規格と仕組み

公開鍵の証明書と認証

広がる暗号化通信技術の利用（1）

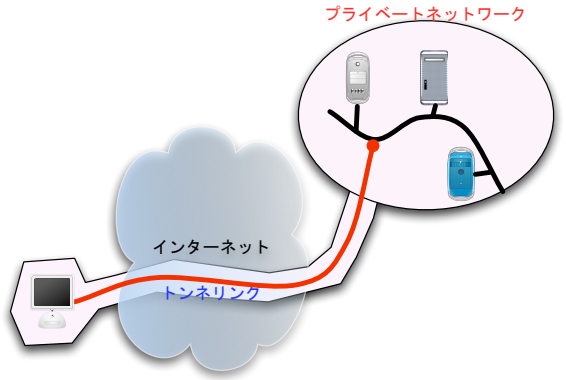
インターネットを利用する経済活動

HTTPS: SecureなHTTP

広がる暗号化通信技術の利用（2）

VPN (Virtual Private Network)

外出先からプライベートネットワークを利用する



Masahiro Mizutani

プライバシーと暗号化の問題

- 社会秩序と個人の自由をめぐる対立
- 相反する見解
  - 立場1: 誰でも使える暗号は脅威である
  - 立場2: 暗号は個人の尊厳に必要だ
- どのようにバランスするか？
  - 社会全体での合意が必要

Masahiro Mizutani

立場1:

法執行機関や国家にとって

誰でも使える暗号は脅威である

- 犯罪を助長する
- 警察の取り締まりの困難
  - FBIのデジタルテレフォニ（廃案）
  - NSAのクリッパーチップ（廃案）
    - 国家が復号鍵をもつ「安全な」暗号化
- 9.11以降、取り締まりの強化へ
  - 政府当局が法の執行のために通信を傍受することが許されている CALEA（通信傍受支援法）

Masahiro Mizutani

http://jp.techcrunch.com/2013/06/12/20130610survey-majority-of-americans-think-nsa-spying-is-more-important-than-privacy/

国家安全保障局（NSA）のインターネット詮索に対する発作的怒りが爆発する中、多くのアメリカ人は権力によるスパイ行為を全く問題なしと考えている。「アメリカ人の過半数 — 56% — はNSAによる通話記録の追跡を政府のテロ対策手段として受け入れている」

そのアメリカ人もメールの監視に関しては体質的にもう少し神経質のようだ。わずかの差ながら、過半数（52% 対 47%）が政府によるメール監視に反対している。

Released: June 10, 2013

Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic

Public Says Investigate Terrorism, Even If It Intrudes on Privacy

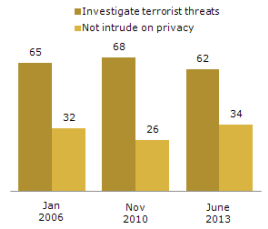
OVERVIEW

A majority of Americans – 56% – say the National Security Agency's (NSA) program tracking the telephone records of millions of Americans is an acceptable way for the government to investigate terrorism, though a substantial minority – 41% – say it is unacceptable. And while the public is more evenly divided over the government's monitoring of email and other online activities to prevent possible terrorism, these views are largely unchanged since 2002, shortly after the 9/11 terrorist attacks.

The latest national survey by the Pew Research Center and The Washington Post, conducted June 6-9 among 1,004 adults, finds no indications that last week's revelations of the government's collection of phone records and internet data have altered fundamental public views about the tradeoff between investigating possible terrorism and protecting personal privacy.

Public Says Investigate Terrorism, Even if it Intrudes on Privacy

Which is more important?



PEW RESEARCH CENTER/WASHINGTON POST June 6-9, 2013. Jan 2006 and Nov 2010 data from ABC/WP. Don't know responses not shown.

Most Back NSA Phone Monitoring

NSA getting secret court orders to track calls of millions of Americans to investigate terrorism ...	June 6-9 %
Acceptable	56
Not acceptable	41
Don't know	2
	100

Should the gov't be able to monitor everyone's email to prevent possible terrorism?	July 2002	June 7-9 2013
Yes	45	45
No	47	52
Don't know	8	3
	100	100

PEW RESEARCH CENTER/ WASHINGTON POST June 6-9, 2013. Figures may not add to 100% because of rounding.

http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

Masahiro Mizutani

立場2:

暗号は個人の尊厳に必要だ

- 盗聴の多くは国家によって行われてきた
- サイファーパンクという考え方
  - 自由な技術（強力な暗号）は全員で利用すべき
- 個人の自由
  - 基本的人権（自分のプライバシーを守る）
- PGP(Pretty Good Privacy)の普及と国家管理

Masahiro Mizutani

---

http://wired.jp/2013/06/12/private-conversations/

アメリカの事例

NEWS

2013.6.12 WED

あなたの通話や通信を傍受されないための方法

米国家安全保障局（NSA）がネットから個人データを収集し、携帯キャリアから膨大な量の通話記録を提出させていると報道されている。携帯での通話や電子メール、チャット、面と向かっての会話を傍受されないようにするための対策はあるのだろうか。

携帯電話

どれくらいの頻度で電話をかけているかというデータを政府はすでに収集している。互いに使い捨て電話を使わない限り盗聴される

電子メール

オンラインの使い捨てアカウントを使うだけでは不十分。電子メールのIPアドレスを追跡することで電子メールの送信元を特定できる。身元を本気で隠したいなら、「Hushmail」 https://www.hushmail.com の安全な電子メールサーヴィスを利用。ただし、添付文書は絶対に開かず、「Flash」や「Quicktime」は無効にし、ブラウザー用プラグインも無効化するかインストールしないことだ。

インスタントメッセージ

令状をもったNSAはすべての通信記録を手に入れ、精査することができ、OTR（Off The Record、オフレコ・メッセージング）機能を使うようにする必要がある。

リアルで会う

滝のそばか、ホワイトノイズのある場所で話すことだ

最大の危険ポイントがある。コミュニケーションの相手だ。相手はあなたとの会話の内容を、すべてネット上に公開してしまうかもしれないのだ。

Masahiro Mizutani