通信の安全性

安全な通信
公開鍵暗号
暗号化の諸問題

水谷正大

Gmail 送信時のメールの暗号化

https://support.google.com/mail/answer/6330403?hl=ja

暗号化されていないメールが個人情報漏洩を引きおこさないように

受信したメールが暗号化されているかどうかを確認

送信先のメールプロバイダが暗号化技術TLSをサポートしているか確認

機能をGmailに実装（2016年2月9日）

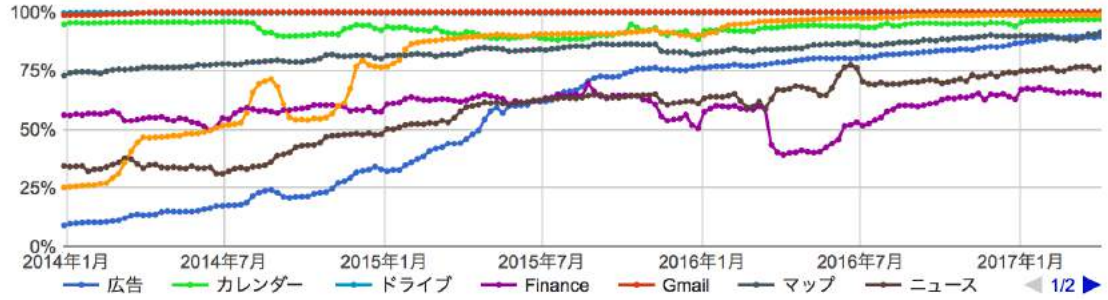
Google 全体

このグラフは、Google のサーバーに対するリクエストのうち、暗号化された接続を使用したものの割合を表しています。

これは、Google トラフィックの大半を表す概数です。

https://www.google.com/transparencyreport/https/

サービス別



これは、特定のサービスについて Google トラフィックの大半を表す概数です。

Google は、Google のサービスすべてに HTTPS を導入できるよう努めています。2014 年 3 月には、Gmail で HTTPS のみを使用することを発表しました。引き続き Google では、暗号化への対応が難航している一部の Google サービスについて、その原因となっている技術的な障壁に対処していき

セキュリティが
なぜ
こんなに
話題になるのか？

国家による通信監視が長期にわたり実施

NSA（アメリカ合衆国国家安全保障局）元職員 **Edward Snowden**の内部告発によると、NSAは国内だけでなく海外要人の通信記録まで後半に収集。全容の多くはいまだ不明。

http://www.newsweekjapan.jp/stories/world/2017/04/post-7339.php

米入国審査の厳格化、日本など同盟国も対象に

米国がすべての入国者に対して、SNSのパスワードなどの提示を要求する可能性

中東諸国だけでなく西側諸国でも監視が行われていた事実が次ぐ次と発覚。。。。

金盾（インターネット情報検閲システム）

中国政府の情報化・電子政府化に向けた「**金字工程**」と称する国家戦略（1993年）。Great Firewallはその一部

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

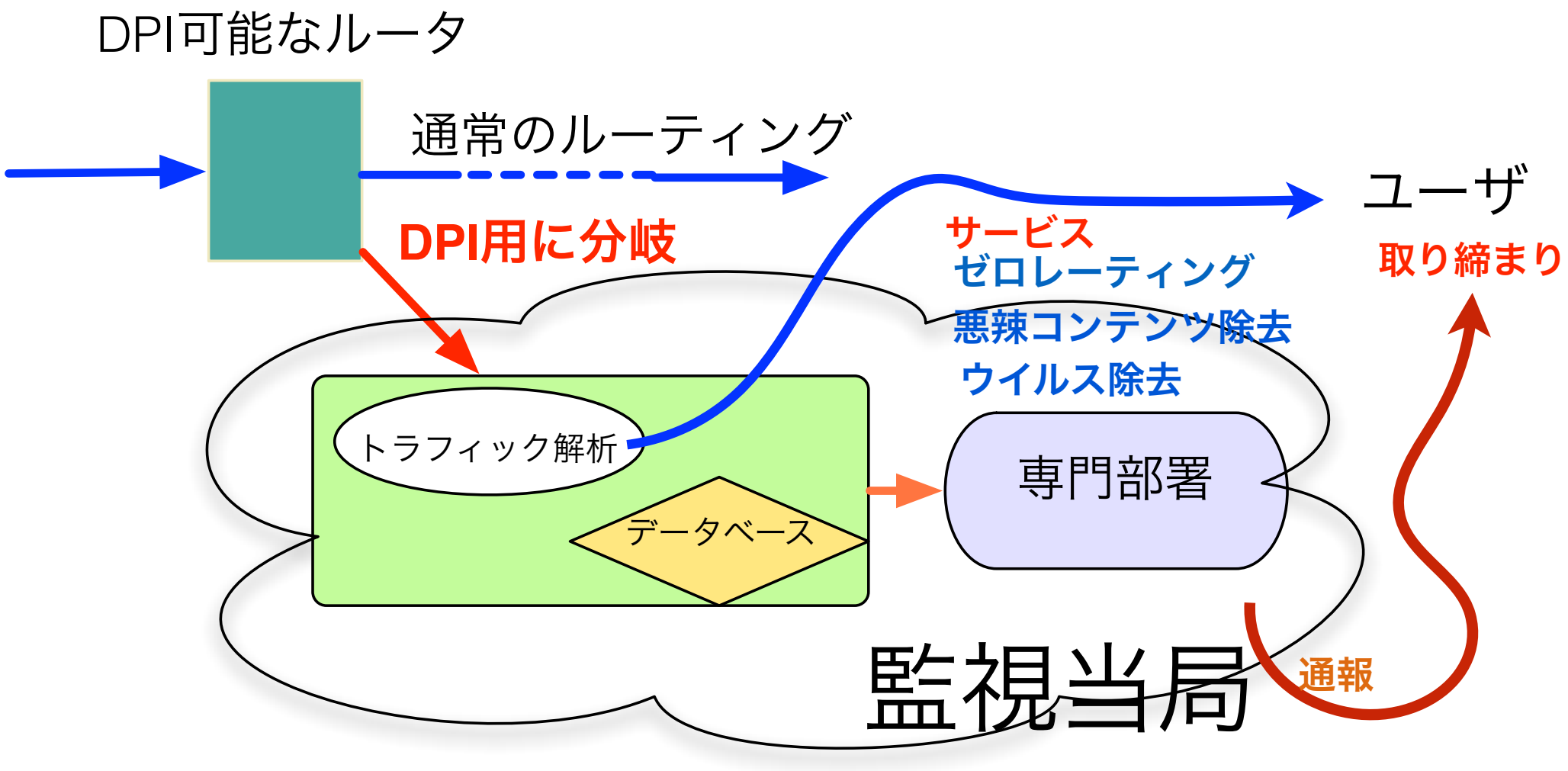
一般企業、サービスプロバイダ、政府などが様々な用途で使用

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。。


DPI可能なルータ
通常のルーティング
DPI用に分岐
ユーザ
サービス
ゼロレーティング
悪辣コンテンツ除去
ウイルス除去
取り締まり
トラフィック解析
データベース
専門部署
監視当局
通報

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は IPパケット単位でのセキュリティ機構は非標準

あり得る懸念

誰かにメッセージを読まれていないか？

メッセージ誰が出したのか？

メッセージは改ざんされていないのか？

しらばっくれたり内容が改ざんされたと主張されたら?

通信の不正行為

盗聴 wiretap/phone hack

当事者以外の第三者が通信内容を知ること

改ざん falsification/manipulation

作成した本人以外の第三者によってデータを書き換える

成りすまし impersonation/masquerad

不正な利益を得るために、他人のふりをする

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 deny a fact

やりとりの事実の否定・内容改ざんを主張

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

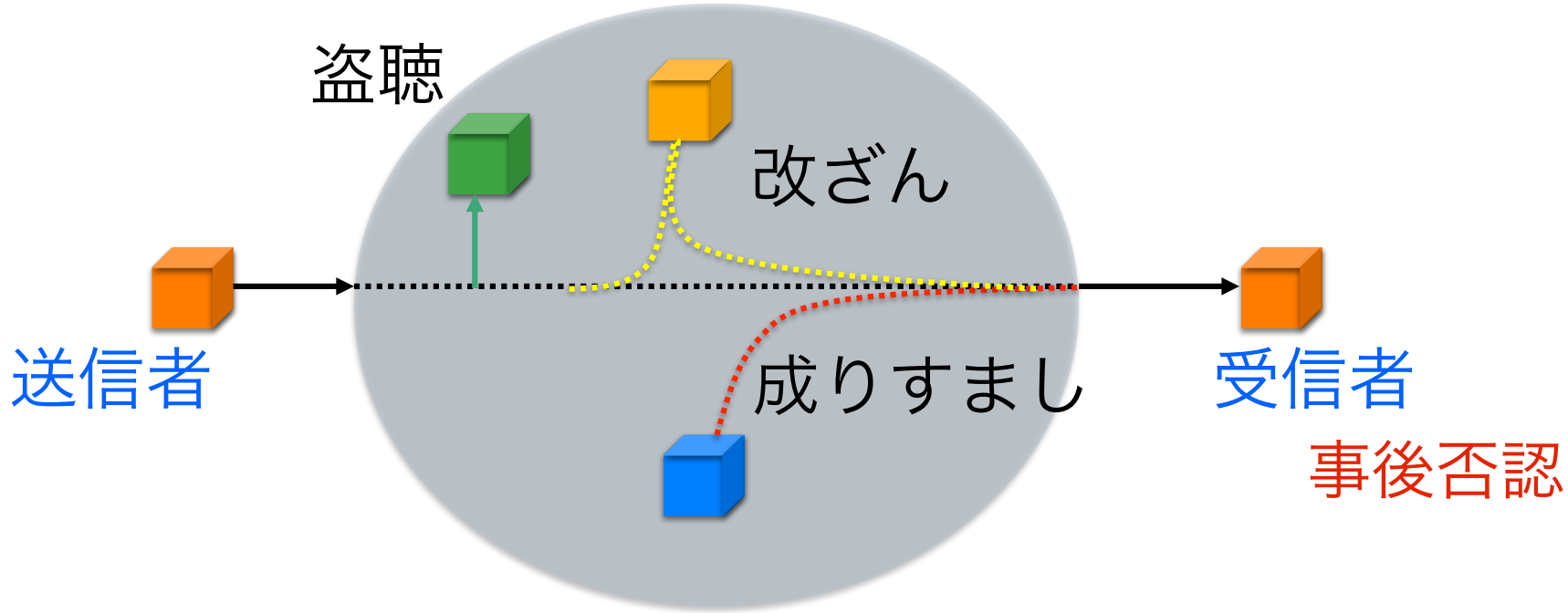
通信内容が他人に知られずに

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起こり得ること



安全な通信の用語

暗号化

　第3者に交信内容を察知できないようにする

署名

　メッセージが誰からのものかを確認できる

内容証明

　メッセージが改ざんされていないことを確認できる

暗号学（Cryptography）

ひらぶん
平文(Plain text)と暗号文(Cypher text)

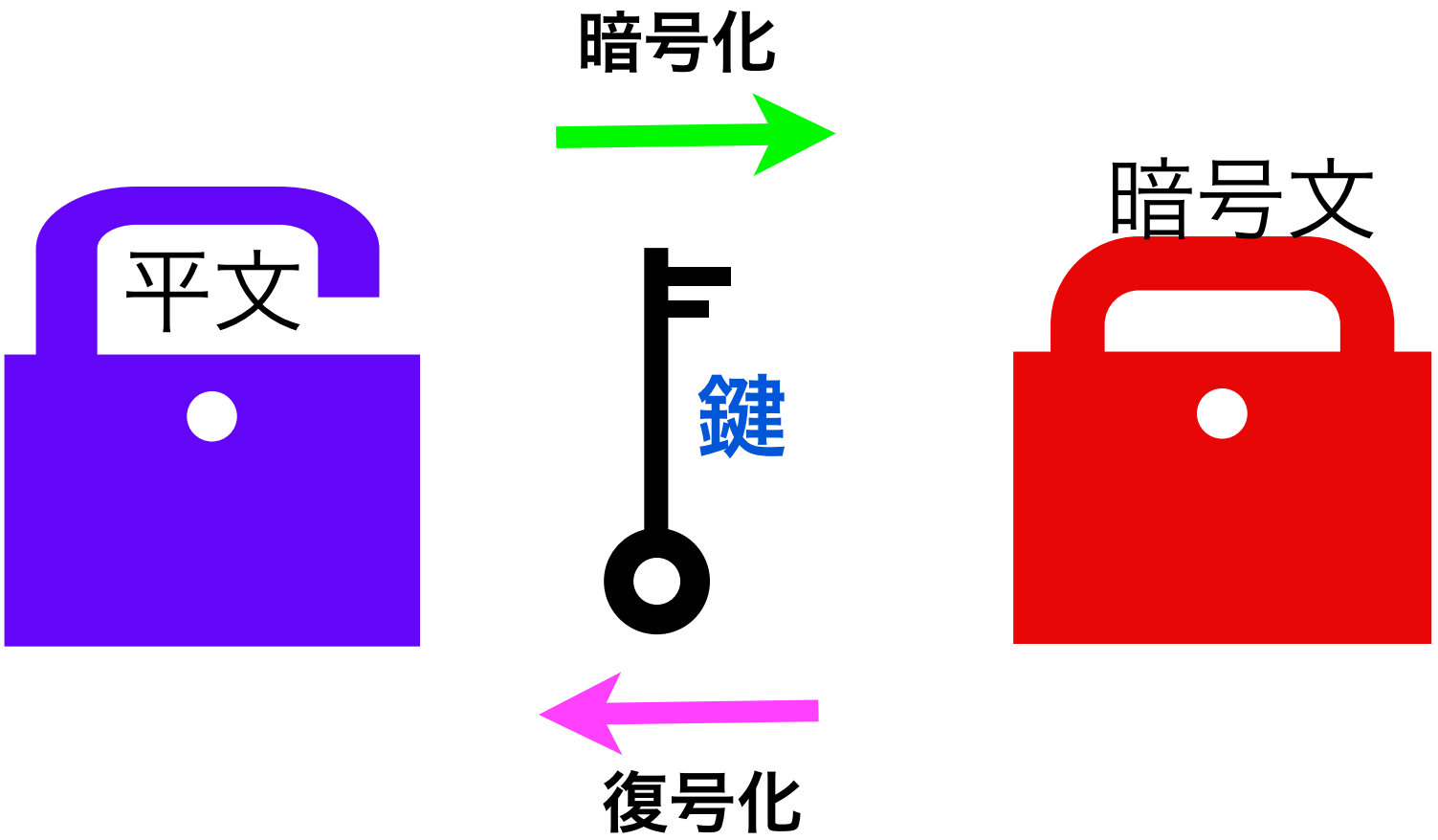
暗号化(Encription/Coding)
　　平文から暗号文への変換

復号化(Decription/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 $c = e(p) = p + k \pmod{26}$

復号化 $p = d(c) = c - k \pmod{26}$

k が暗号化キー

暗号化と復号化とで**共通鍵**

‘IBM’ を一文字前にシフトして’HAL’

暗号の歴史

古典暗号システム（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)

2015チューリング賞　https://awards.acm.org/about/2015-turing

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

インターネットで安全な通信を可能

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

時間がかかりすぎ事実上不可能とみなされる作業

一方向関数を使って文を変換する

例：電話番号から名前を見つけることは困難

平文（名前）⟷ 暗号文（電話番号）

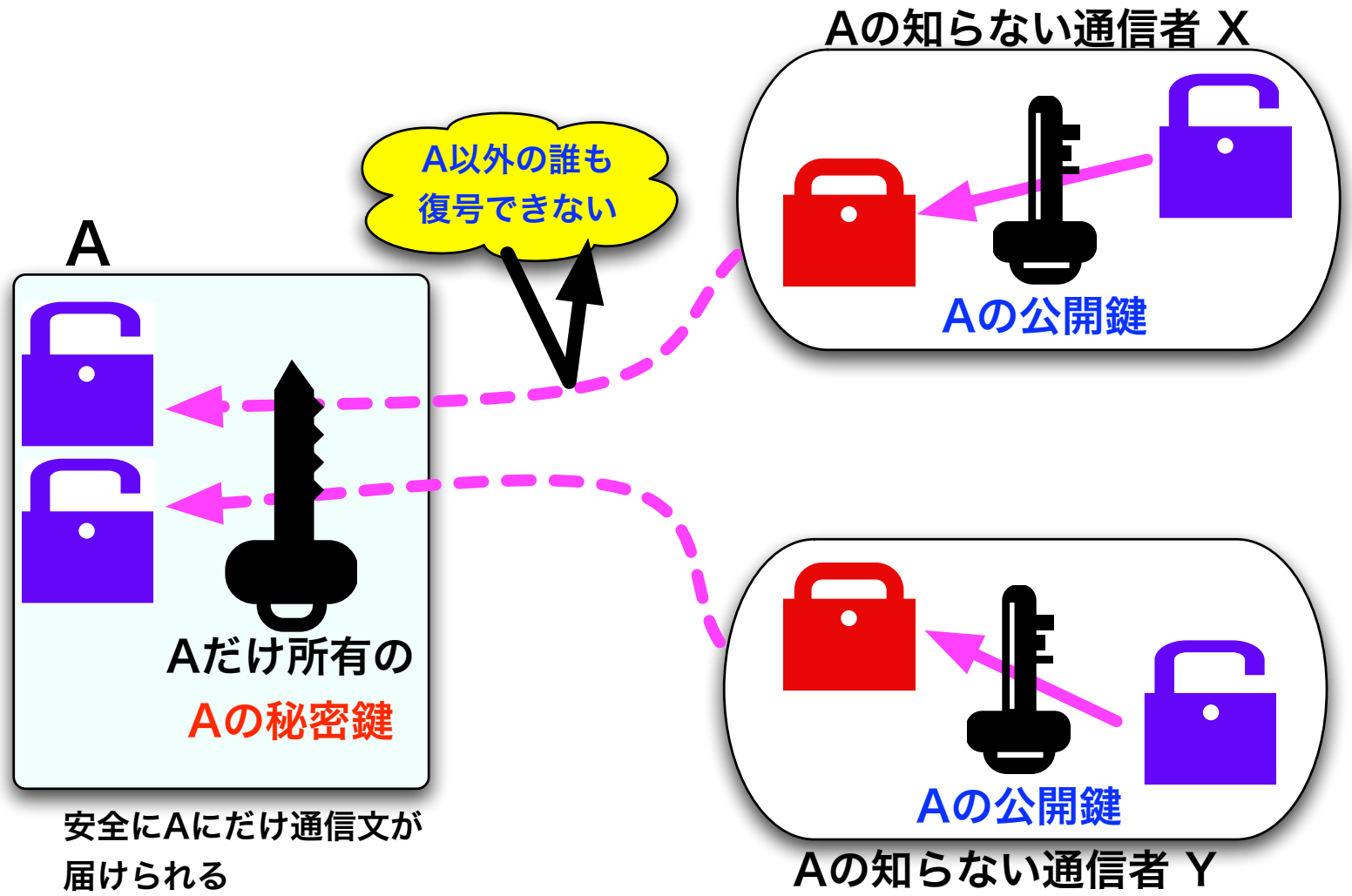
RSA方式(1978年) Rivest, Shamir, and Adleman

2015チューリング賞 http://www.ams.org/notices/200307/comm-turing.pdf

素因数分解の困難性を利用

2006年9月まで米国特許だった

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

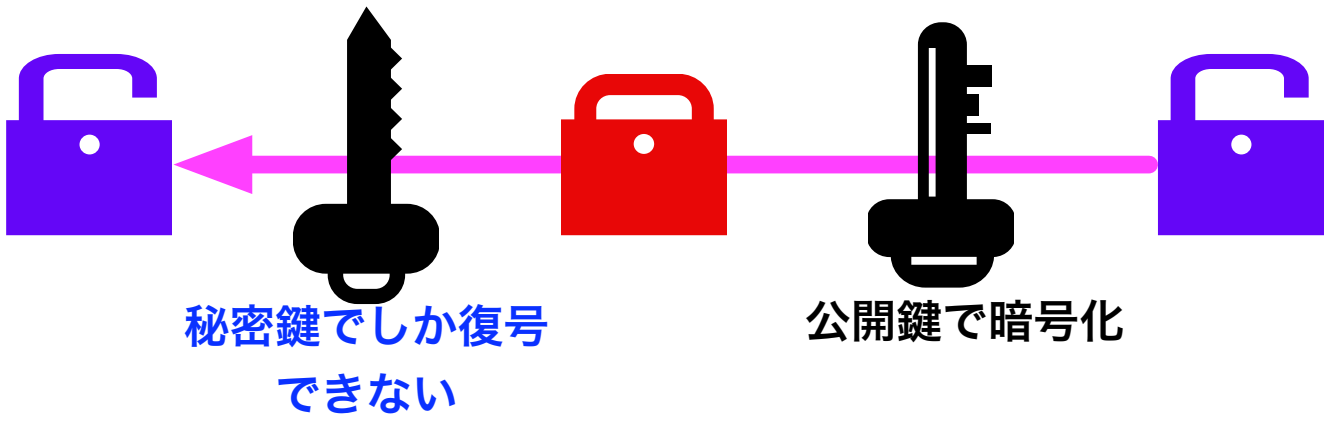
公開暗号方式

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

公開鍵暗号方式の望ましい性質



公開鍵と秘密鍵が可換

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

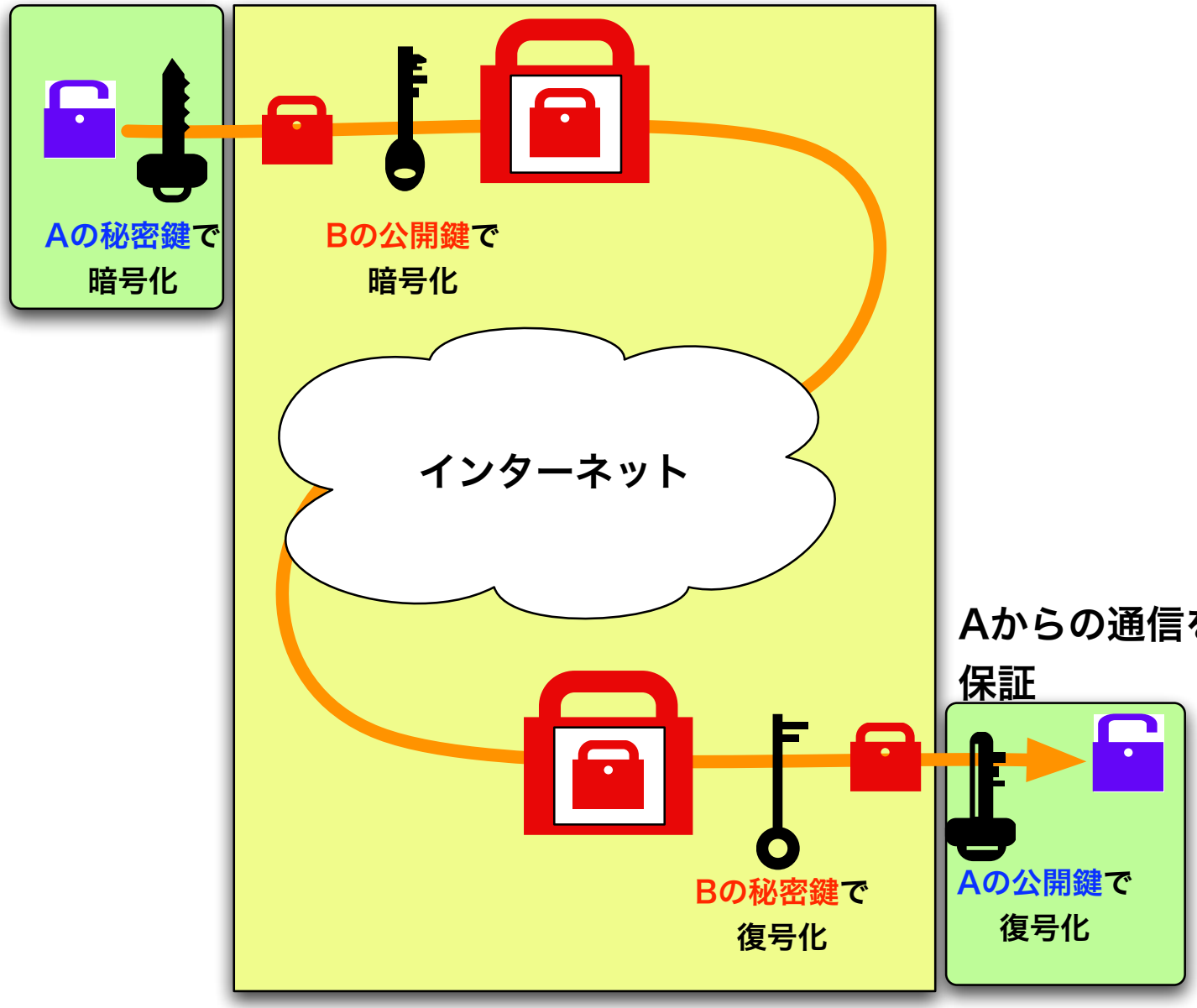
改ざんの防止

内容証明通知

署名：本人でしか為し得ない印を付加

秘密鍵を使った**電子署名**

電子署名の仕組み



AからBに安全に届ける役割

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

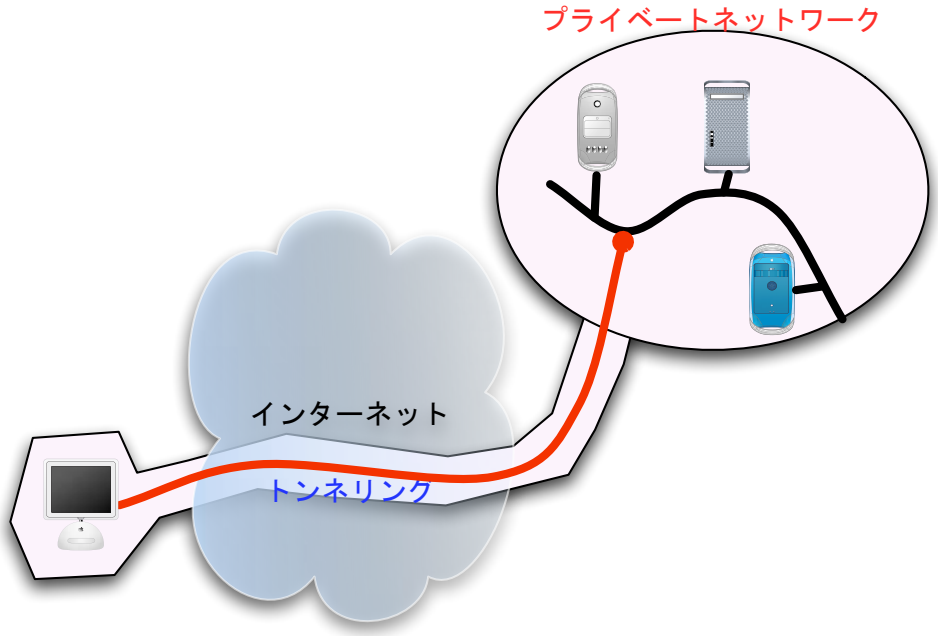
暗号化通信技術の利用（１）

HTTPS: SecureなHTTP

暗号化通信技術の利用（2）

VPN (Virtual Private Network)

閉じたネットワークへの仮想ネットワーク経路



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

問われていること

どのようにバランスするか？

社会全体での合意が必要

立場I:

誰でも使える暗号は脅威である

犯罪を助長する

治安維持・警察取り締まりを困難にする

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

政府は法の執行のために通信傍受が許されてるか

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

基本的人権（自分のプライバシーを守る）

http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138

国連の人権委員会もAppleを支持する声明

NEWS

2013.6.12 WED

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

あなたの通話や通信を傍受されないための方法

アメリカの事例

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は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