情報セキュリティと情報倫理

第10回
暗号技術とセキュリティ

（参考書：11 情報セキュリティの基盤技術「暗号」
12 暗号と認証を支える制度）

2022/12/09

暗号技術とセキュリティ

- 議論
  - 暗号の原理ならびに公開鍵暗号をはじめとする代表的な暗号方式，電子署名 （シラバスより）
  - 盗聴に対する暗号化と政府の介入
- 教科書
  - 11.情報セキュリティの基盤技術「暗号」
  - 12.暗号と認証を支える制度
- 参考書
  - IT 社会の法と倫理　第二版　第三章

通信に対する攻撃

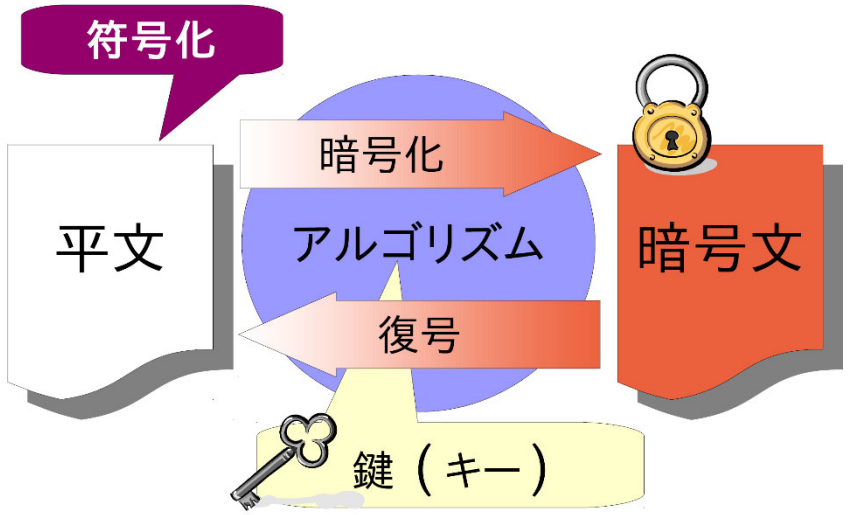
- 盗聴
  - 送信者の通信文を、受信者以外の第三者が受信する
- 妨害
  - 送信者の通信文を、第三者が妨害して受信者に届かないようにする
- 受信者へのなりすまし
  - 第三者が正規の受信者と偽って、送信者の通信文を受信する
- 送信者へのなりすまし
  - 第三者が正規の送信者と偽って、受信者に通信文を受信させる
- 改竄
  - 第三者が、送信者の通信文を通信中に書き換えてから受信者に受信させる

データと数

- 文字コード
  - 自然言語における文字に対して、適切なデータを付番
- 固定長方式
  - 現在のコンピュータには8ビットを採用
  - 文字「A」の場合
    - 文字コードは「65」→　二進数で「1000001」
    - 左に1つ“0”を追加して「01000001」

暗号とは

- 一見では分からないようにデータを隠す技術
  - 平文(plaintext), 暗号文(ciphertext)
  - 暗号化(encryption), 復号(decryption)
- 暗号化手法:
  符号化技術、暗号化アルゴリズム、鍵
  - 共通鍵暗号方式
  - 公開鍵暗号方式

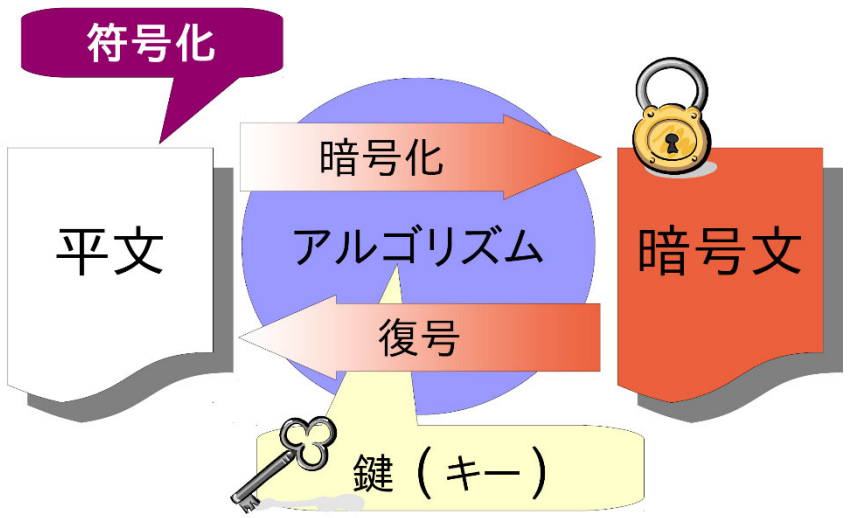


暗号の使用

- 通信データは盗聴されうる
  - 金融システム
  - 有償コンテンツ(衛星放送、CATV 等)
  - 電子メール、Web
- 情報伝達、許可の無いアクセス防止、改竄防止、盗用防止にも暗号が使われる
  - 暗号化されていれば（解読されない限り）安全

暗号の用途

- 機密性
  - 盗聴されない
- 完全性
  - 改竄されない
- 認証
  - なりすましを防ぐ
- 否認防止
  - 送った・受け取ったことを否認できない



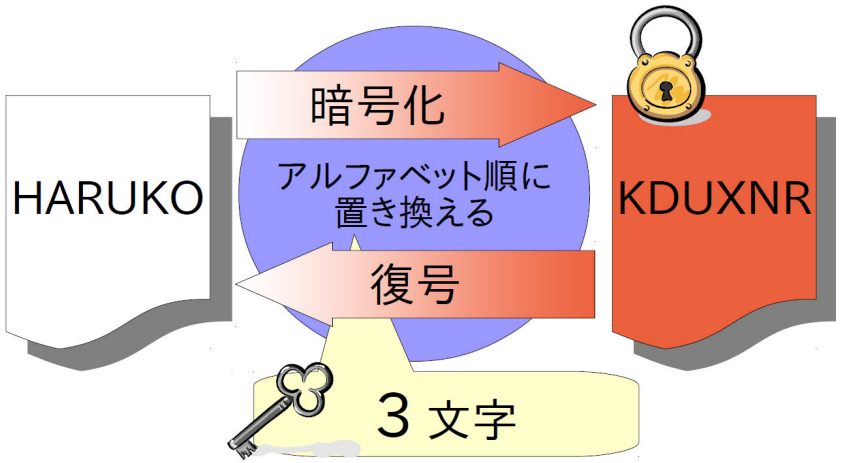
暗号の使用例

- 消費者の買い物、ATMでの暗証番号
- インターネット上での買物時のクレジットカード番号
- 銀行の記録や金融データ
- ビジネスに関わる秘密通信
- 病院などのデータベース上の機密データ
- 教師の保管している学生の答案や成績ファイル
- 映像データの移動制限
  - SeeQVault
    - 著作権保護のための暗号化。映像データの移動制限。SeeQVaultの対応外付けHDDは同じくSeeQVaultの対応機器でないと再生できない。
  - CPRM（Content Protection for Recordable Media）
    - デジタル放送の「1回のみ録画可」である映像をDVDに録画した後に、別の記録メディアにデジタルコピーできなくする著作権保護技術。

暗号化手法

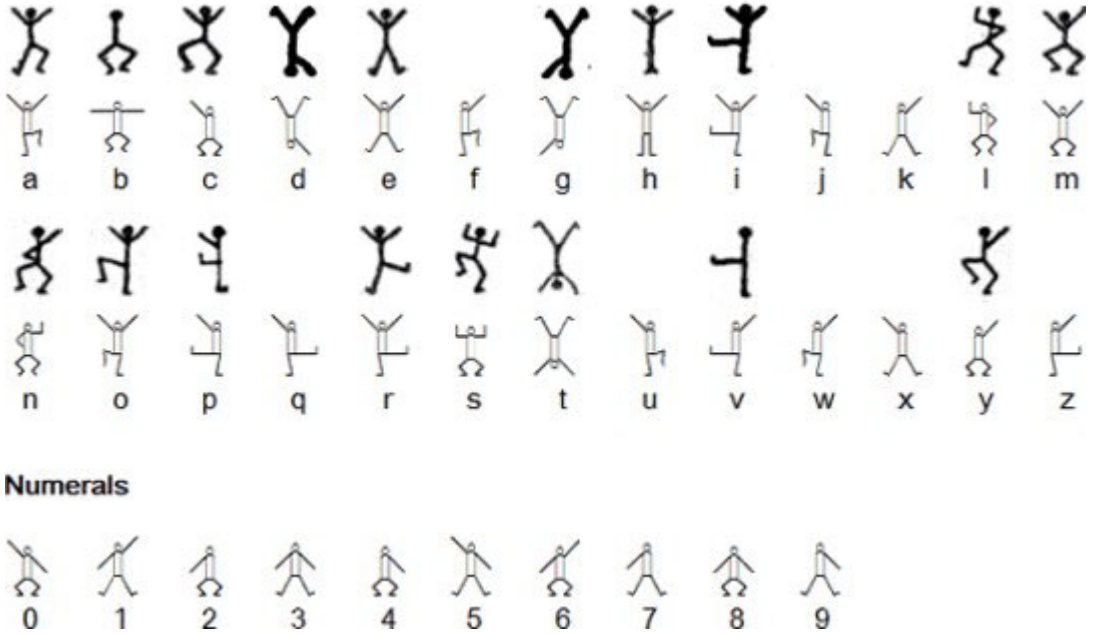
共通鍵暗号

- 暗号化と復号で同じ鍵を使う
  - シーザー暗号
    - アルファベット順を置き換える
    - 鍵：3文字
  - スキュタレー方式
    - 丸い棒に細長いテープを巻く
    - 鍵：棒の太さ



共通鍵暗号

– 踊る人形
  - 「シャーロックホームズ」シリーズの作品から
  - 多数の人の形をしたシンボル
    – それぞれアルファベット1文字に対応



共通鍵暗号の特徴

- 公開鍵暗号と比較して変換が簡易で高速
- 鍵の配送・保管が問題
  - 相手によって鍵を使い分ける必要がある
  - 鍵の事前受け渡しが必要
  - 換字式暗号は頻度分析攻撃に弱い
    - 一般的な英文では「e」がもっとも使われているなど

共通鍵暗号方式

- ブロック暗号
  - 平文をブロック単位に分割して暗号化を行う
  - 実現が比較的容易
    - DES (Data Encryption Standard) 鍵長56bit
      - 1975 年アメリカ商務省標準局で公表
      - 1999年1月、22時間15分でDESの鍵がやぶられた。総当たり攻撃
  - Triple DES (3DES) → AES（Advanced Encryption Standard）
  - FEAL　NTT が開発
  - MULTI　日立製作所が開発。デジタル衛星放送等
  - IDEA　PGP などで使われる
  - RC5　Ronald Rivest が開発。SSL など。
  - MISTY　三菱電機が開発。W-CDMA など

共通鍵暗号方式(2)

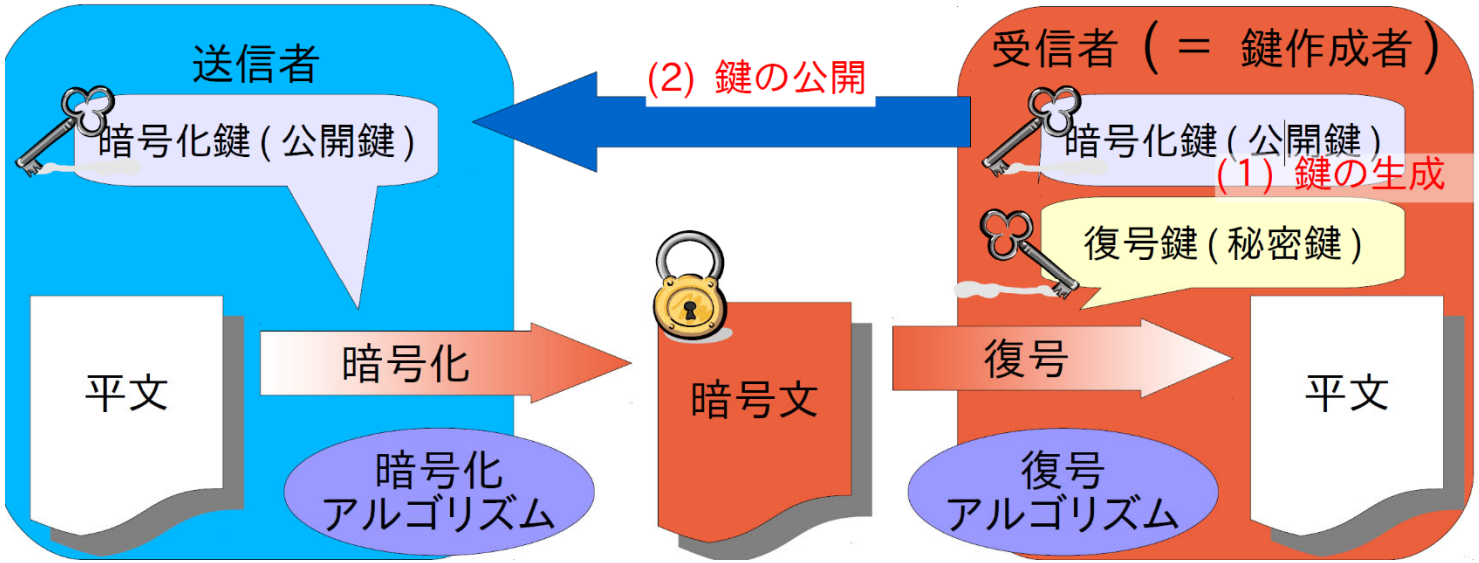
- ストリーム暗号（逐次暗号）
  - 平文の1 文字毎に順次暗号化
    - 通信に向く
  - RC4 Ronald Rivest が開発。SSL 、無線LAN など
    - 脆弱性が見つかっている。現在使用禁止
  - A5 GSM(Global System for Mobile Communications)
  - SEAL　　IBM が開発。
  - MULTI-S01　　日立製作所が開発

暗号の脆弱性:
暗号が、暗号化されたものから、鍵を知ることなく
復号できてしまう方法が見つかること

公開鍵暗号

公開鍵暗号

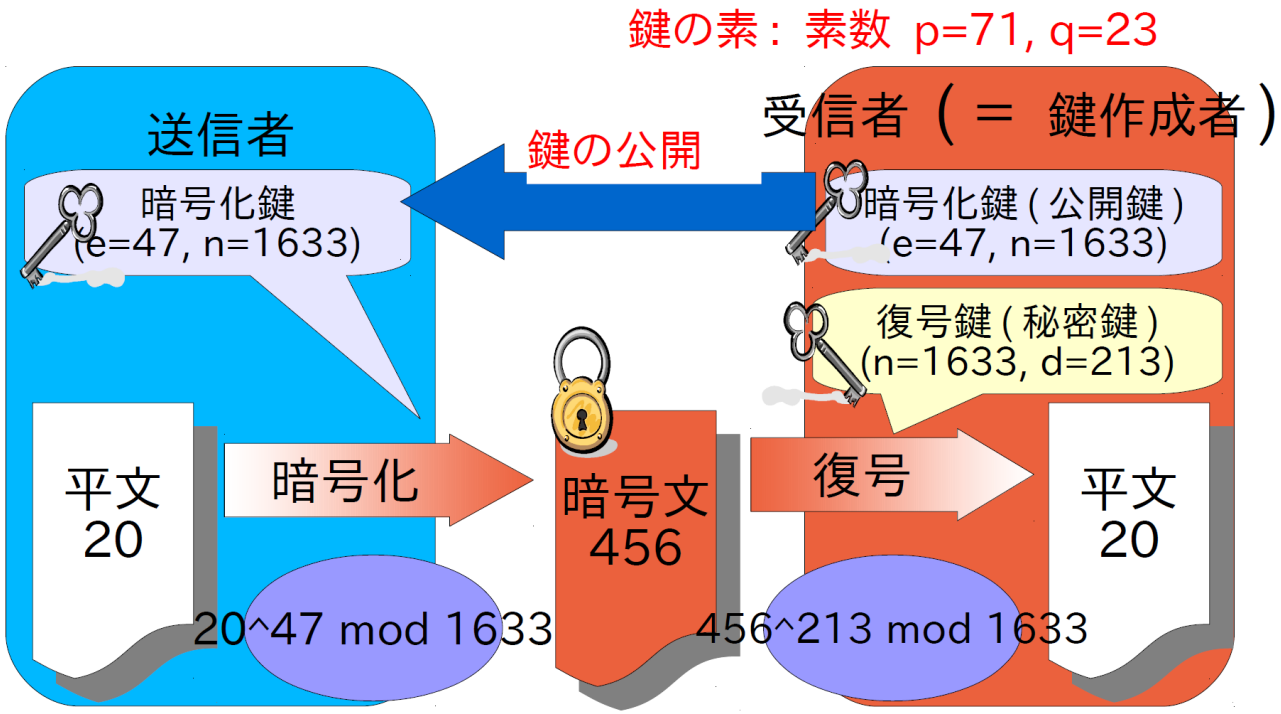
- Stanford 大学Whitfield Diffie, Martin Hellman が提案 (1976 年)
  - ペアになる鍵を作成、一方を公開、他方を保管
  - 一方の鍵から他方を推測できない



RSA暗号

Ron Rivest, Adi Shamir, Len Adleman (1977)

- 公開鍵暗号　→　数学的な一方向性に基づいて実装
  - 素数と素数の掛け算は簡単
  - 素因数分解は難しい
    - 71 x 23 = 1633 → 1633=X x Y
- 素数として150 ～ 300 桁以上を使用



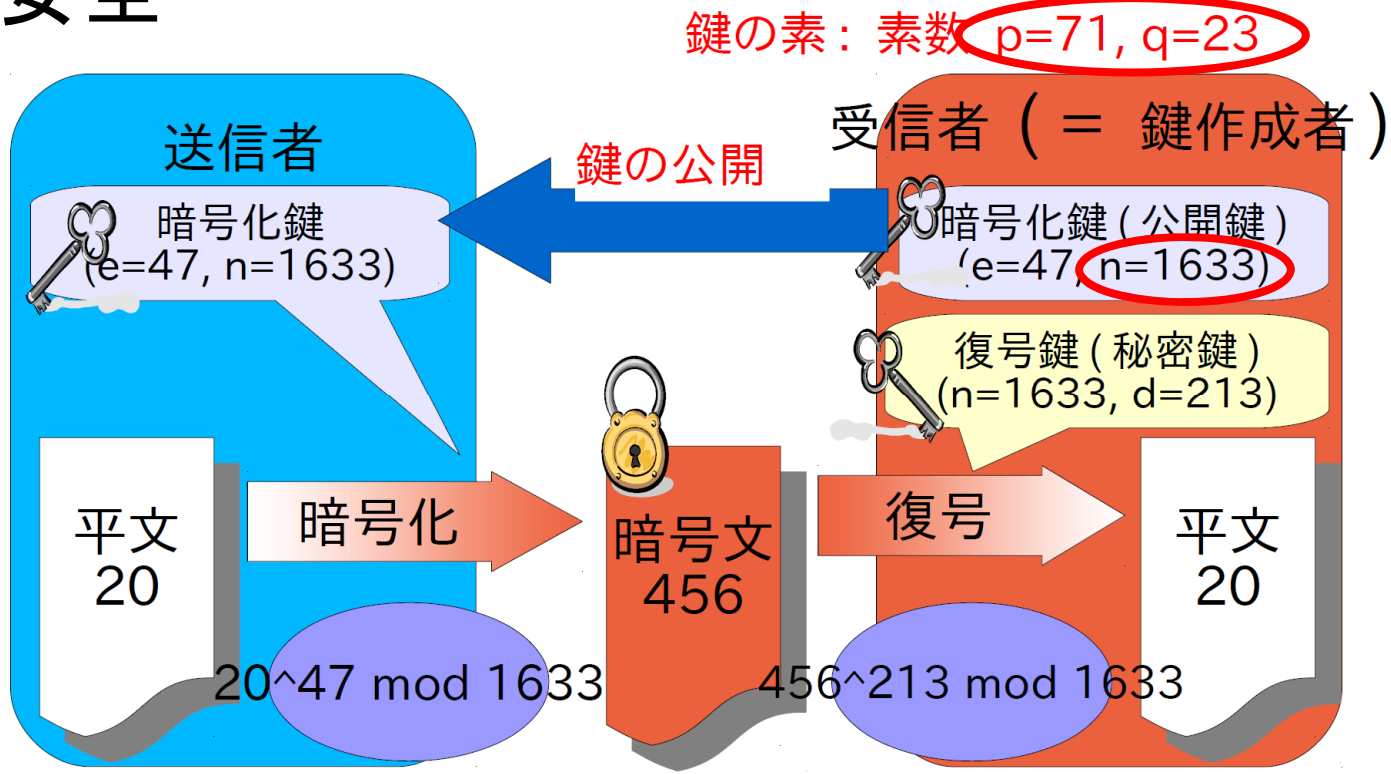
(1)2つの大きな素数p とqを決める
　例：p=71,　q=23
(2)p × q= n を計算する
　例：n=71 × 23=1633
(3)(p-1) と(q-1)の最小公倍数Lを計算する
　例：70 と22の最小公倍数
　　L=770
(4)L と互いに素で、Lより小さい任意の整数 e を選ぶ
　例：e = 47
(5) e × d≡1 mod L となる正の整数 d (eのモジュラ逆数) を計算する
　d=213

RSAを破る

- 公開されている n から n=pq と素因数分解できればRSAを攻撃可能
- RSAでは p と q の値は数百桁程度の大きな素数であるため素因数分解に膨大な時間がかかる

  → 計算量的安全

教科書p181に
計算時間の変化の例

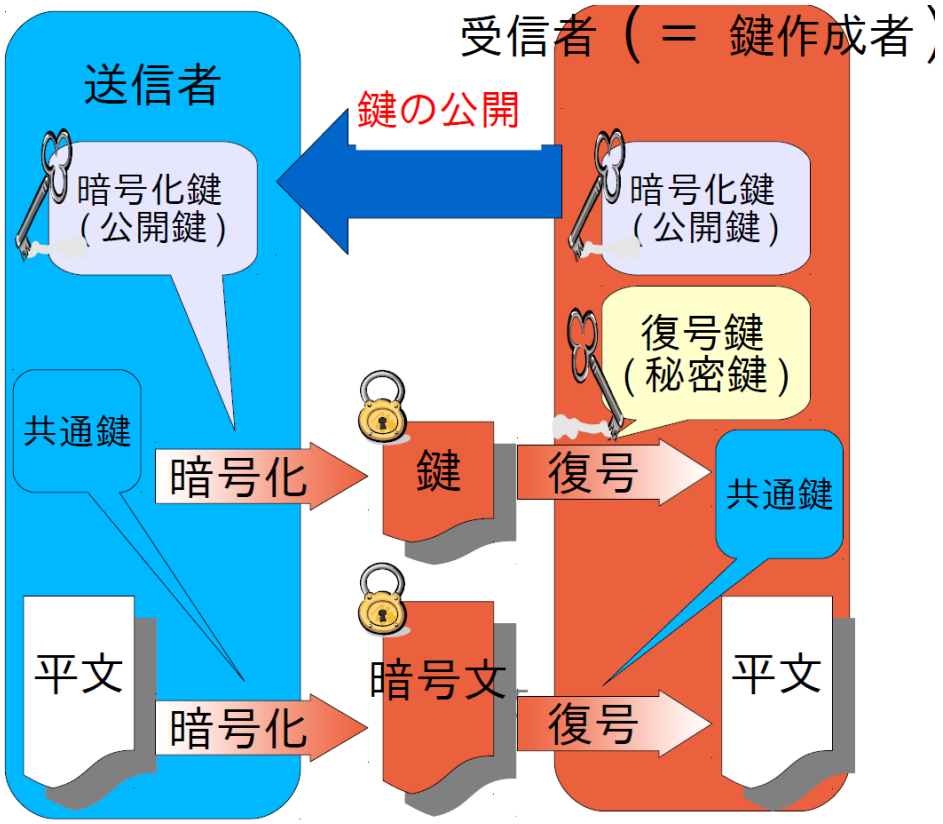


共通鍵暗号と公開鍵暗号

- 公開鍵暗号は低速
  - 計算処理が難しい
  - 共通鍵暗号の1000 倍ぐらい遅い

→　組み合わせて使用

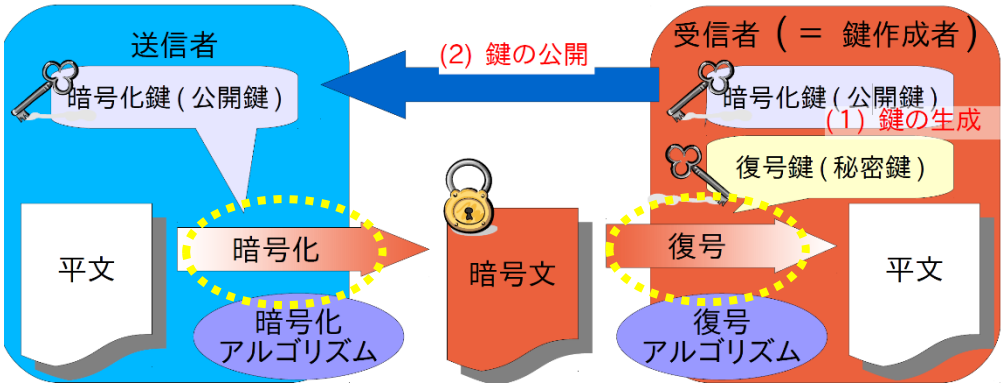
  - 公開鍵暗号で、共通鍵暗号の鍵を送付する
  - 送付された鍵を使って共通鍵暗号を使用する
    - 鍵の配送問題を解決

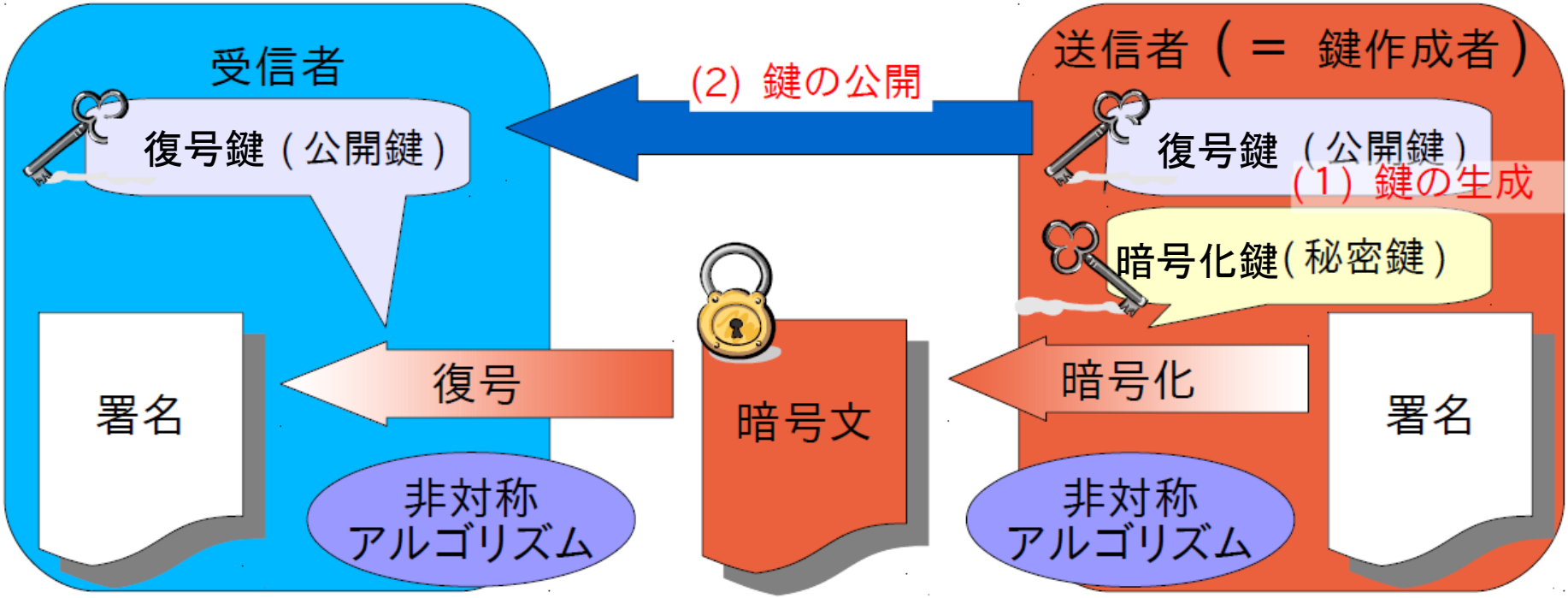


電子署名

電子署名のしくみ

- 公開鍵暗号の(逆向き) 使用
  - 秘密鍵で暗号化
  - 公開鍵で復号
    - 組み合わせが不正なら復号不能



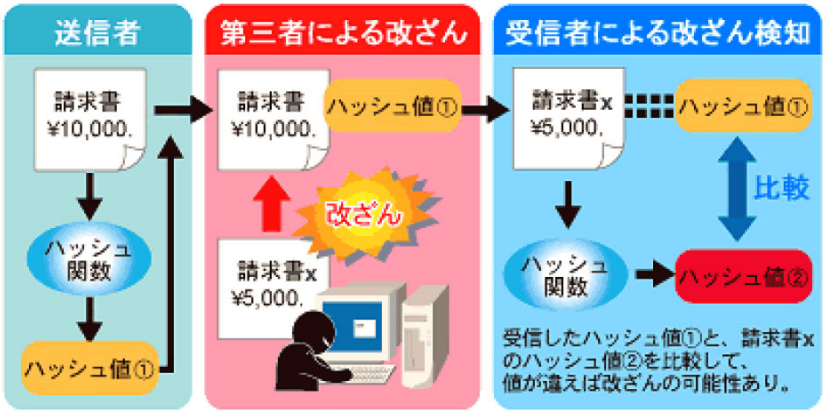


セキュアハッシュ関数

- 元データ全体に電子署名せずにダイジェスト化
  - 任意の桁数のデータから、一定の桁数のデータを出力する事が出来る。（ハッシュ値）
  - 出力されたハッシュ値から、元のデータを取り出す事は出来ない。（復元出来ない、一方向性関数）
  - 元データのごく一部だけが変更された場合でも、出力されるハッシュ値は大きく変化する。
  - 違う元データから同じハッシュ値が出力される可能性がごく低い。

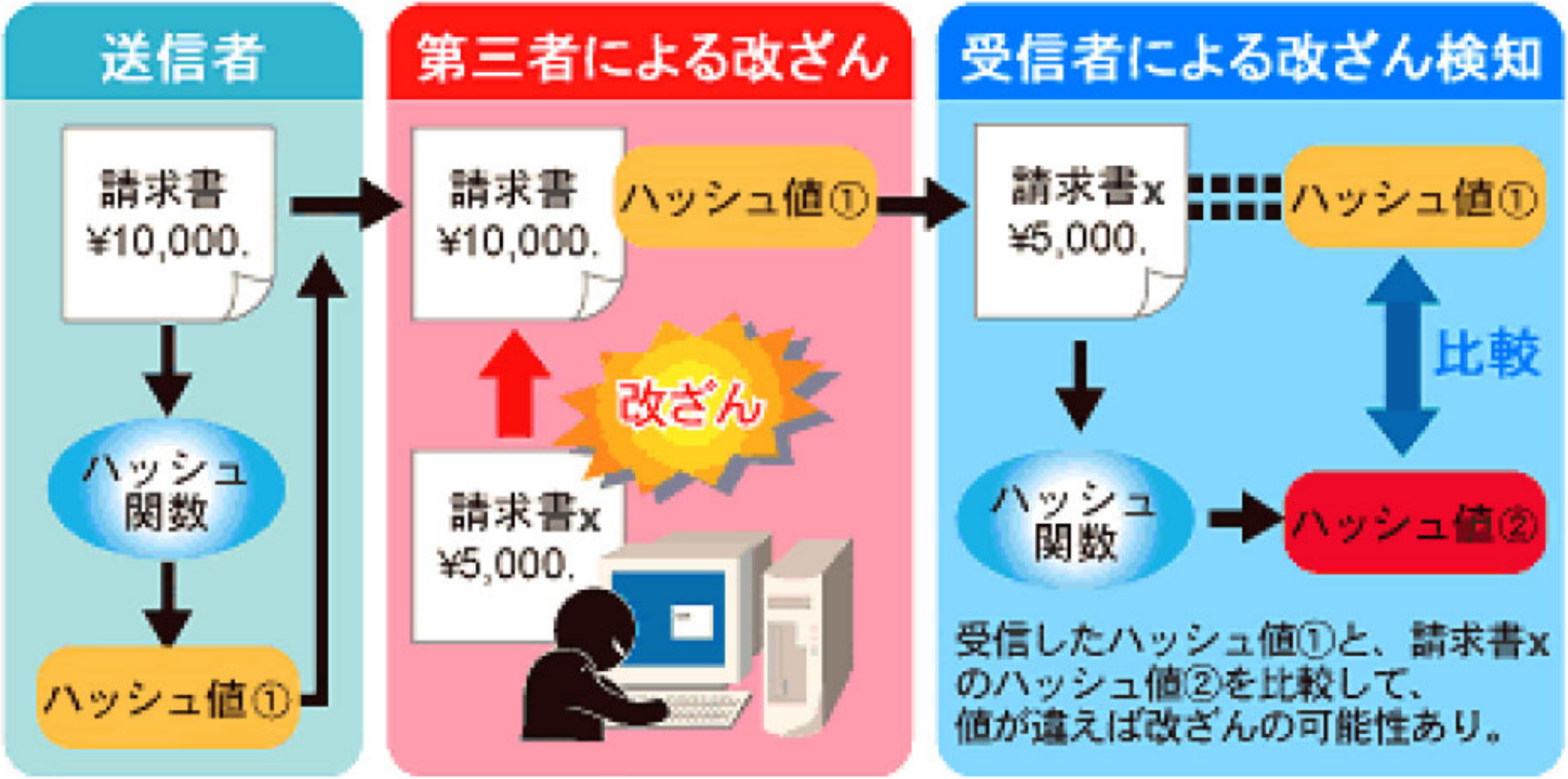
→ ダイジェストに電子署名してやれば良い

- MD5　　RSA Security 社
- SHA-2　　米国標準
- RIPEMD160　ヨーロッパ標準　など



セキュアハッシュ関数

- 元データ全体に電子署名せずにダイジェスト化
  - 任意の桁数のデータから、一定の桁数のデータを出力する事が出来る。（ハッシュ値）



セキュアハッシュの脆弱性

- ハッシュ := 様々な大きさのファイルから、
  (小さな) 固定長のデータに変換する。
  - 異なるファイルが、偶然同じハッシュ値を持つことがありえる。
    (ハッシュ・コリジョン)
- 2004 年 8 月 MD5 の強衝突耐性に理論的な脆弱性
  - 同じハッシュ値を持つ2つのファイルが生成できる
  - ファイルに意味があるかどうかは別
- 2007 年11 月 MD5 の弱衝突耐性に対する脆弱性に関する発表 (Vulnerability of software integrity and code signing applications to chosen-prefix collisions for MD5)
  - あるファイルと同じハッシュ値を持つファイルが生成できる

公開鍵の正当性保証

PGP (Pretty Good Privacy)

問題:「その公開鍵は、本当に想定した人のものなのか？」

- 解のひとつ　→　PGP

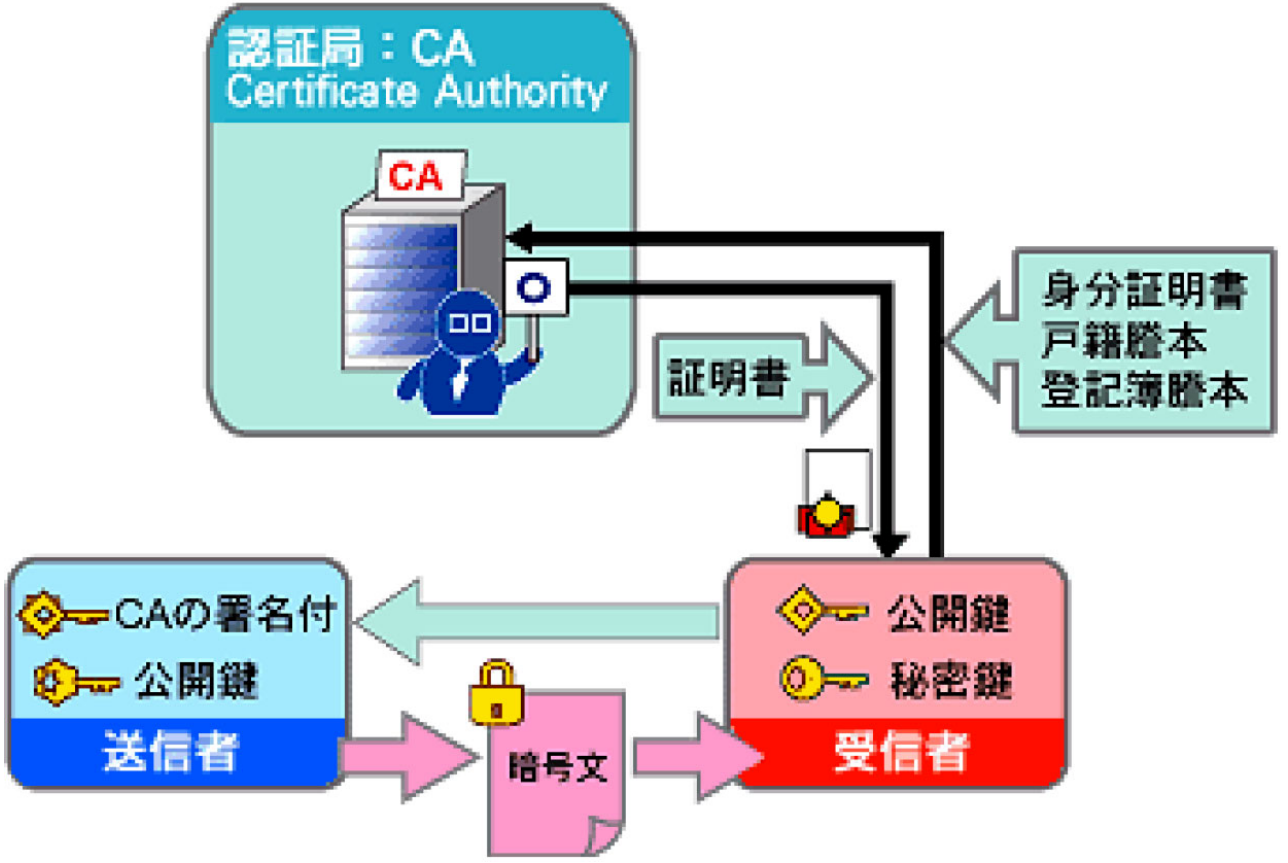
- Philip Zimmermann が開発 (1991 年)
- 電子メール用に開発　→　電子文書一般に適用可能
- 信頼の輪(public key ring) 受け手の公開鍵を持つ
  - 内容を秘密にして送りたい
    - 相手の公開鍵で暗号化して送信
  - 署名をつけたい
    - 自分の秘密鍵で暗号化して送信
  - 署名をつけた上で内容を秘密にしたい
    - 自分の秘密鍵で暗号化した上で相手の公開鍵で暗号化

CA (Certificate Authority)

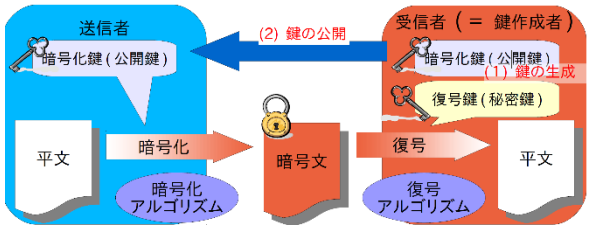
問題:「その公開鍵は、本当に想定した人のものなのか？」

→　公開鍵の正当性を保証する機関（認証局）を設置

- 公開鍵とその所有者を保証する証明書を発行



PGP では信頼の輪で実現



PKI (Public Key Infrastructure)

- 公開鍵暗号基盤
  - CA 同士の連携方法
    - Root CA , 中間CA
  - CA の仕事の分担
    - RA　Registration Authority (登録局)
    - VA　Validation Authority (検査局)
- GPKI (Government PKI)
  - 電子政府

SSL/TLS 技術

（ Secure Socket Layer / Transport Layer Security ）

- 公開鍵暗号方式に基づく方式
  - Web (https) などで利用
  - 通信相手の公開鍵を基に暗号化した通信を開始
    - デジタル署名を基に、公開鍵の正当性を確認
    - CA (RootCA) による確認　→ PKI
  - その通信専用の秘密鍵を交換して、以降の通信を行う
  - 通信には、ハッシュによる改竄検知を併用する
- デジタル署名が正しくない場合 (オレオレ証明書)
  - 偽の通信相手の可能性あり (man-in-the-middle attach など)

通信と盗聴

無線LAN

- IEEE802.11　無線LAN関連規格
  - IEEE 802.11b　　最大11Mbps
  - IEEE 802.11a　　最大54Mbps
  - IEEE 802.11g　　最大54Mbps
  - IEEE 802.11n　　最大300Mbps
  - IEEE 802.11ac　　最大6.9Gbps
  - IEEE802.11ax　　最大9.6Gbps　（Wi-Fi 6）
- 暗号化されていない場合は極めて容易に盗聴可能
  - 暗号化でない以下の方法はほぼ無意味
    - MACアドレスによる接続制限
    - SSIDの隠蔽

無線LANで使われる暗号技術

規格名	暗号化方式	パスフレーズ長(ビット)	備考
WEP	RC4	40～104	すでに解読されている
WPA	RC4またはAES	104	セキュリティー強度に不安
WPA2	RC4またはAES	128	AESを標準で使うことで安全性向上
WPA3	AESまたはCNSA	256	現在最も高い安全性

2017年10月16日、WPA2の脆弱性が報告される。

各無線LANベンダーは該当製品の対策ファームウェアへのアップデートを推奨。

その後2018年6月ごろから新規格WPA3

盗聴

- 電話が電話交換手による接続の時代から
- 現在：電気通信事業法、電波法等により規制
  - 警察力による盗聴はある
    - 犯罪捜査のための通信傍受に関する法律
      - http://www.moj.go.jp/HOUAN/SOSHIKIHO/MONITOR/refer01.html
  - 違法行為として
    - 武富士の事件 (ジャーナリスト宅盗聴事件　２００１年)
- 情報のやりとりの盗聴
  - 交信履歴だけでもプライバシーが漏れ出す
  - プッシュホンの音　→　暗証番号が分かるかも
  - 携帯電話を持つ　→　現在の居場所が絞れる

暗号化と盗聴

- 通信が暗号化される　→　盗聴が難しくなる
  - 一般市民のプライバシーの確保
  - 犯罪者にも有利に？

アメリカの暗号化と盗聴に関する政策

傍受のための通信システム（ USA ）

- Federal Communications Act (1934)
  - 情報の送り主が認めた人以外の人が盗聴、外部への漏洩を禁止
- Omnibus Crime Control and Safe Streets Act (1968)
  - 裁判所の令状をとれば政府は盗聴してよい（盗聴と電子的監視）
- Electronic Communication Privacy Act (1986)
  - 盗聴法の電子的通信への拡張
- Communications Assistance for Law Enforcement Act (1994)
  - 通信の傍受ができるシステムでなければならない
  - 電子通信サービスの提供者、および電子通信機器の製造者は、法律に基づいた根拠のある場合には、通信システムから声、データ、および他の通信形態での（暗号化されていない）平文の内容を政府機関が手に入れることができるよう、保証しなければならない。

盗聴に関する論点

- テロリストや犯罪者からの防衛
  - 電気通信技術が発達しても警察機関の裁判所命令による電子諜報活動能力が失われないこと
- 盗聴は必要なのか？
  - 1990 年代でも500 件/ 年
  - 捜査手段としての盗聴の有用性は低い？
- 経費
  - 盗聴可能にするシステムの導入に18 億ドル！
- 技術革新と世界競争
  - 通信サービス･装置開発の足枷になりかねない

1990 年代中頃のアメリカの暗号政策

- 秘密性
  - NSA (National Security Agency, 国家安全保障局)
    - 他国が絶対解読できない暗号システムの開発
    - 他国が使った暗号をすべて解読する
  - 研究者や技術者の囲い込み
- 暗号標準
  - DES (1976 年)
  - DES は本当に安全か？ (Trap doors はないのか)
  - より強固な暗号標準には政府が反対
    - NSA のスパコンでも解くことが難しいから！

アメリカの暗号政策(1990 年代中頃)

- 輸出制限
  - 暗号は軍需品
  - 米国製の暗号製品は、国内用と国際用
    - 国際用の方がセキュリティが弱い(鍵長が短い等)
  - 国際的なビジネスマンも困る
  - 強力な暗号化ツールが米国外で開発
    - カナダ、オーストラリア、ヨーロッパ等
    - PGP
      - 書籍にプログラムが印刷されてやりとり
- 情報の禁止
  - 何が暗号か分からない
    - 落書き、並べる順序、解説書、曲のリクエスト等々

鍵預託方式

- クリッパーチップ (Skipjack)
  - 強力な暗号とプライバシーを確保。かつ、
    政府はどんなメッセージでも解読可能
    → 政府がアルゴリズムを作成
- 鍵供託 (key escrow)
  - 解読時の鍵を2つに分割
  - 2つの異なる預託機関で保管→政府の暴走を防ぐ
- 問題点が多い
  - 暗号アルゴリズムは秘密
    - 品質が不明
  - 鍵供託に頼らずに解読できるのでは？という疑惑

鍵預託方式についての議論

- プライバシーと防衛
  - 警察機関が犯罪からの防御に盗聴が利用可能か否か
  - 法的根拠のある電子調査
  - 犯罪者が強力な暗号化を使った事例は提示される
  - 国家の危険性の具体例はほとんど提示されない
- 自発的な採用
  - クリッパーチップがあっても、その上でPGP が使われては意味が無い
    - 他の暗号化方式は違法化するのか？？

鍵預託方式についての議論（2）

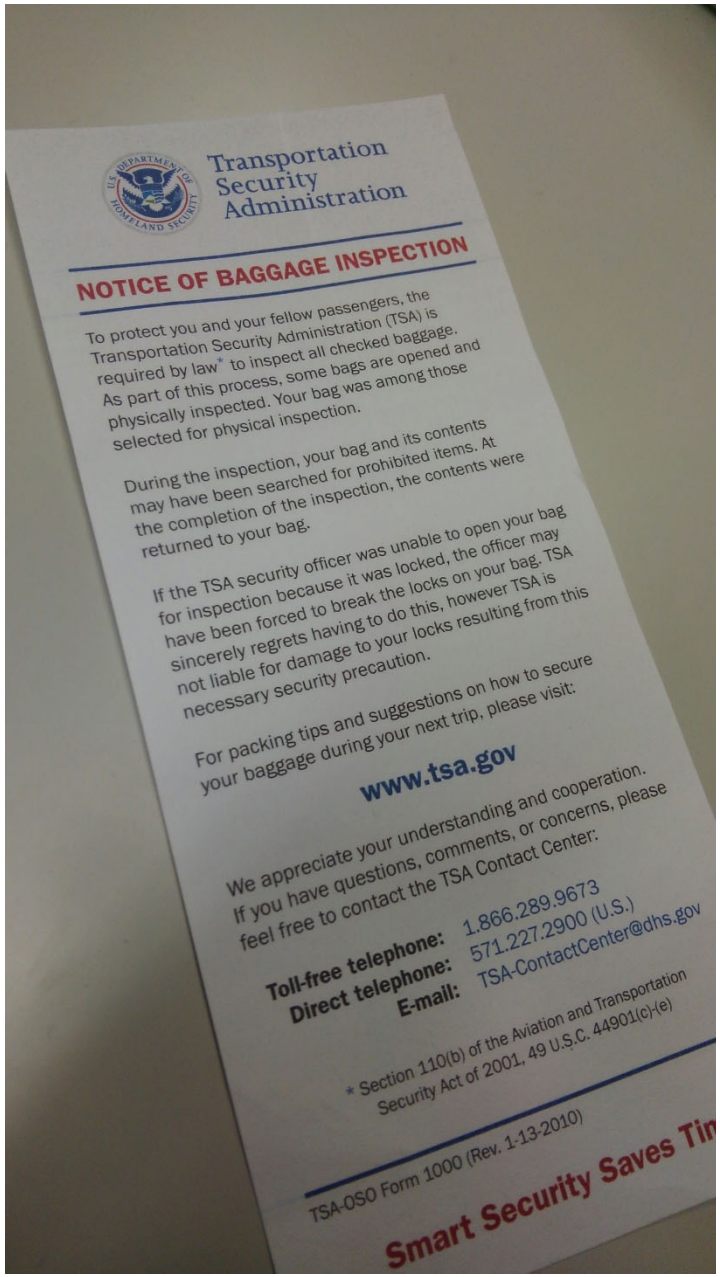
- 自由とのトレードオフ
  - 例えば、州を跨るハイウェイ網は犯罪者の逃亡に利用されている、という見方と同じ
    - 結局はトレードオフ
- 国際貿易
  - クリッパーチップ入りの製品は競争能力が低い
    - 米国政府に弱み(?) を握られたくない
    - 米国以外の製品を買えば済む

TSA ロック

- TSA (アメリカ運輸保安局)
- (Transport Security Agency)
- アメリカの空港での預入荷物
- 本人と専用鍵で開く
  - TSA しか保有しない
- プライバシー

vs

(政府機関の) モラル



暗号と盗聴に関する問題点

プライベートで安全な通信を求める側

– 政府がその権力を濫用するかもしれない心配

vs

政府が容易にアクセスできるように求める側

– 合法的な警察活動のもとでのアクセスは当たり前

- 恐ろしい犯罪やテロリストから身を守ってくれるのと同じ警察機関が、反対意見や慣習的でない行為を押さえつけようとしている限り、この対立は消えないだろう。