第31回諜報研究会



# 暗号と社会のかかわり史

2020年5月23日

（株）IT企画　才所敏明

Mail：toshiaki.saisho@advanced-it.co.jp
Web：http://www.advanced-it.co.jp/
Facebook：https://www.facebook.com/toshiaki.saisho



## 自己紹介

1970年4月～1994年12月　東京芝浦電気（東芝）・情報システム部門
　　東芝Gの技術・研究部門の研究開発環境の整備・高度化推進
1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門
　　東芝のセキュリティ技術センター発足と同時にセンター長就任
　　東芝Gのセキュリティ技術開発・事業支援活動推進
2007年10月　(株)IT企画を設立
　　情報技術および情報セキュリティ技術分野の研究開発や
　　その応用事業に対するプロフェッショナルサービスを開始
［現職］
　(株)IT企画　代表取締役社長
　事業支援活動（顧問・相談役）：2社（日、米）
　大学教育活動（情報セキュリティ）：九大、目白大
　研究開発活動：中央大学研究開発機構、九州大学大学院
　　暗号・認証、秘密分散、バイオメトリクス、電子メールセキュリティ、
　　IoTシステムセキュリティ、FinTech（仮想通貨、ブロックチェーン）
　　ビッグデータ、AI

## 暗号（文）とは

第三者に公開したくないデータを、
　特別な知識なしでは理解できない形へ変換したデータ

暗号化：不特定の第三者にも理解できるデータ（平文）を
　特別な知識を有する特定の人しか理解できないデータ
　（暗号文）へ変換すること

復号：特別な知識を有する特定の人が、
　その知識を利用し暗号文を平文へ変換すること

解読：特別な知識を有しない人が、
　何らかの方法で暗号文を平文に変換すること

暗号技術：暗号化に使用する技術
　および復号に使用する技術の総称



## 人類・社会の歴史は紛争の歴史

紛争：敵対する勢力間の争い

紛争当事者は、連携する勢力間での協議・連絡により
　敵対する勢力に対し優位に立つことを目指す
➔ 協議・連絡の内容の漏洩は、敵対する勢力を優位に

敵対する勢力への情報漏洩を防ぎたい ➔ 暗号を利用
敵対する勢力は、対立する勢力の動きを把握したい
➔ 暗号を解読

＜暗号技術の開発と解読技術の開発の繰り返しの歴史＞

暗号に関する熾烈な戦いの勝敗が、
人類・社会の歴史を形作ってきた！

# 本日のお話

（1）古代暗号　暗号の歴史の始まり

（2）古典暗号　外交活動の活発化による暗号の普及　**紛争の道具としての暗号**

（3）近代暗号　暗号の作成・解読は手作業から機械へ

（4）現代暗号　暗号方式の暗号アルゴリズムと暗号鍵への分離

（5）現代暗号（共通鍵暗号方式）
特徴、開発の歴史、社会での活用例

（6）現代暗号（公開鍵暗号方式）　**産業・生活を支える暗号**
特徴、開発の歴史、社会での活用例

（7）これからの暗号応用と課題
拡大する暗号応用・暗号の悪用・新たな課題と対応状況



# （１）古代暗号

## 暗号の歴史の始まり

＊ヒエログリフ（紀元前3000年頃、エジプト）
＊スキュタレー暗号（紀元前600年頃、ギリシャ）
＊シーザー暗号（紀元前100年ごろ、ローマ）

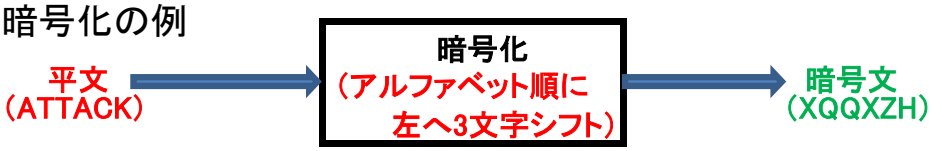
# 古代暗号：シーザー暗号

紀元前100年頃、古代ローマの軍事的指導者
ユリウス・カエサル（ジュリアス・シーザー）が使用
（シェイクスピアの『ジュリアス・シーザー』の「ブルータス、お前もか」）

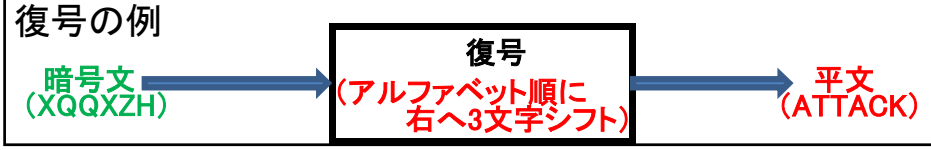
暗号化：アルファベットをある数だけずらす
復号　：アルファベットを逆順に同じ数だけずらす

ABCDEFGHIJKLMNOPQRSTUVWXYZ

暗号化の例




復号の例






# （２）古典暗号

## 外交活動の活発化による暗号の普及

＊ノーメンクラタ暗号
（15世紀から18世紀、スコットランド）
＊ヴィジュネル暗号（16世紀頃、フランス）
＊上杉暗号（16世紀頃、日本）

# 古典暗号：ノーメンクラタ暗号

15世紀から18世紀にかけ使用

暗号化：シーザー暗号のように1文字の換字だけではなく、
フレーズを記号などへ置換え（置換ルールはコードブック）

復号　：コードブックを利用し、元の文字列を復元

**16世紀、スコットランド女王メアリ・スチュアートがイングランドのエリザベス女王暗殺を企て、共謀者とのやり取りに利用した暗号。**

エリザベス女王の側近のウォルシンガム配下のスパイ組織網により暗号文が入手され暗号解読の名人に解読され、女王メアリは処刑された。（女王メアリ暗号とも呼ばれている）
なお、ウォルシンガムは解読の事実を伏せ、メアリにはしばらく手紙のやり取りを行わせ、メアリがエリザベスの暗殺を手紙に記したのを見計らって（確実な証拠を確保の上）メアリと共謀者を一網打尽にし、全員を処刑した。

**敵対勢力の暗号化された通信から情報を継続入手するため、暗号解読の事実を伏せることは、以降の歴史でも良く採られた方法**



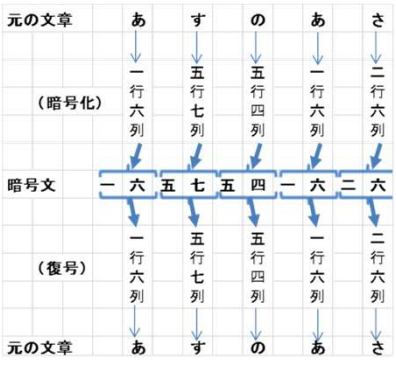
# 古典暗号：上杉暗号

16世紀頃、戦国時代の武将・上杉謙信の軍師だった宇佐美定行の著書、兵法書に暗号の作り方が記載

暗号化：7×7のマス目（方陣）に“いろは48文字”を埋め、
1文字を行と列に割り当てられた数字へ置換

復号　：行と列の数字、および方陣を利用し復元

| 七 | 六 | 五 | 四 | 三 | 二 | 一 | |
|---|---|---|---|---|---|---|---|
| ゑ | あ | や | ら | よ | ち | い | 一 |
| ひ | さ | ま | む | た | り | ろ | 二 |
| も | き | け | う | れ | ぬ | は | 三 |
| せ | ゆ | ふ | ゐ | そ | る | に | 四 |
| す | め | こ | の | つ | を | ほ | 五 |
| ん | み | え | お | ね | わ | へ | 六 |
| | し | て | く | な | か | と | 七 |



# （３）近代暗号

## 暗号の作成・解読は
## 手作業から機械へ

＊ツインマーマン暗号（第一次世界大戦、ドイツ）
＊ADFGX暗号（第一次世界大戦、ドイツ）
＊エニグマ暗号（第二次世界大戦、ドイツ）
＊パープル暗号（第二次世界大戦、日本）
＊ミッドウェー暗号（第二次世界大戦、日本）

（第一次世界大戦：1914年～1918年　　第二次世界大戦：1939年～1945年）

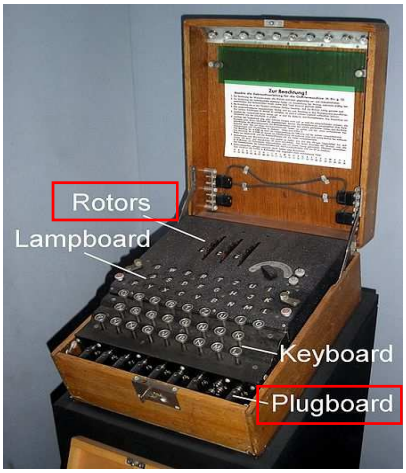


## 近代暗号：エニグマ暗号

第一次世界大戦（1914年～1918年）終盤の1918年、ドイツの発明家アルトゥール・シェルビウスによって発明された機械式暗号機

ドイツ軍は第一次世界大戦で使用していた暗号が解読されていた事実を知らず、より強力な暗号が必要という意識は低く採用せず。

しかしその後、イギリスによって暗号が解読されていたことで第一次世界大戦に敗れたと知ったドイツは、暗号が国家の存亡を左右するという危機感から、エニグマ採用を決定。



ポーランドはローターとプラグボードの初期設定と文字の出現パターンの対応表を作成し、解読機「ボンブ」開発に成功。しかし、ドイツがエニグマを改良することによって増大する暗号パターンにポーランドが対応できず、資金的にも人材的にも充実しているイギリスにその研究情報を渡し解読を託した。
（その2 週間後に、ドイツはポーランドへ侵攻、
第二次世界大戦（1939年～1945年）が始まった）

イギリスの解読グループに集められた精鋭の中でも、
ひときわ才能を発揮したのが**数学者のアラン・チューリング！**
**1940年には「ボンブ」を改良しエニグマの暗号解読に成功**

**エニグマ暗号解読の事実は極秘事項として扱われ、ドイツは終戦までエニグマを信頼して使用し続けていた。エニグマ暗号が解読されていたという事実が公表されたのは、1974 年のことであった。**



## アラン・チューリング（1912年～1954年）

フォン・ノイマン（von Neumann）と並ぶ
電子計算機実用化/計算機科学の元祖とされている

①1937年、今日のコンピュータの
数学的モデルと評されるチューリング・マシンを考案
②1942年、第二次大戦中、ドイツはエニグマよりも強力な
ローレンツSZ40暗号機を利用していたが、
チューリングがローレンツ暗号解読技法を考案、
それに基づいて暗号解読用コンピュータ、コロッサス
が開発され、1943年に稼働（汎用計算機：1946年ENIAC）
③1954年、没。計算機科学の世界では最高の栄誉である
チューリング賞（1966年より）にその名を残している

2014年：イミテーション・ゲーム/エニグマと天才数学者の秘密
映画は第二次世界大戦中にエニグマ暗号の解読に取り組み、
のちに同性間性行為のかどで訴追を受けた
イギリスの暗号解読者アラン・チューリングを描く

# （１）古代暗号～（３）近代暗号まとめ

民間利用は無く
もっぱら
国家や組織の勢力争いの道具として利用



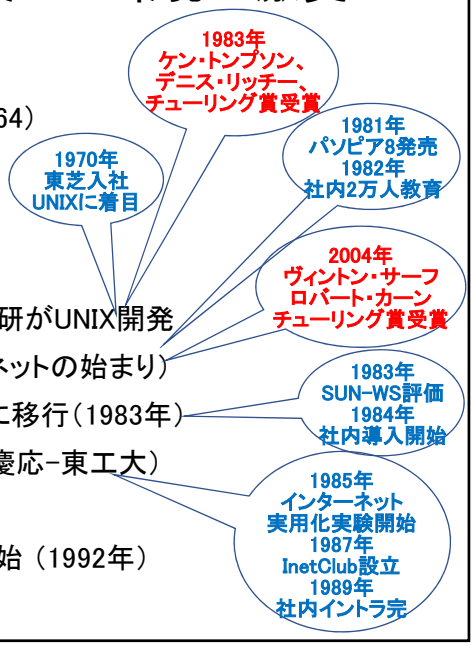
# （４）現代暗号

暗号方式の
暗号アルゴリズムと暗号鍵への分離

# 第二次世界大戦後のIT環境の激変

コンピュータの発展
- 第一世代: 真空管（1950 ～ 1959）
- 第二世代: トランジスタ（1959 ～ 1964）
- 第三世代: IC（1964 ～ 1970）
- 第三.五世代: LSI（1970 ～ 1980）
- 第四世代: VLSI（1980 ～1993 ）

コンピュータネットワークの発展
- ARPANET 実験開始（1969年）ベル研がUNIX開発
- TCP/IP の開発（1982年、インターネットの始まり）
- ARPANET がTCP/IP ネットワークに移行（1983年）
- JUNET 実験開始（1984年、東大-慶応-東工大）
- 米国で商用ISP登場（1990年）
- AT&T Jens 商用ISP (Spin) 営業開始（1992年）
- IIJ営業開始（1993年）





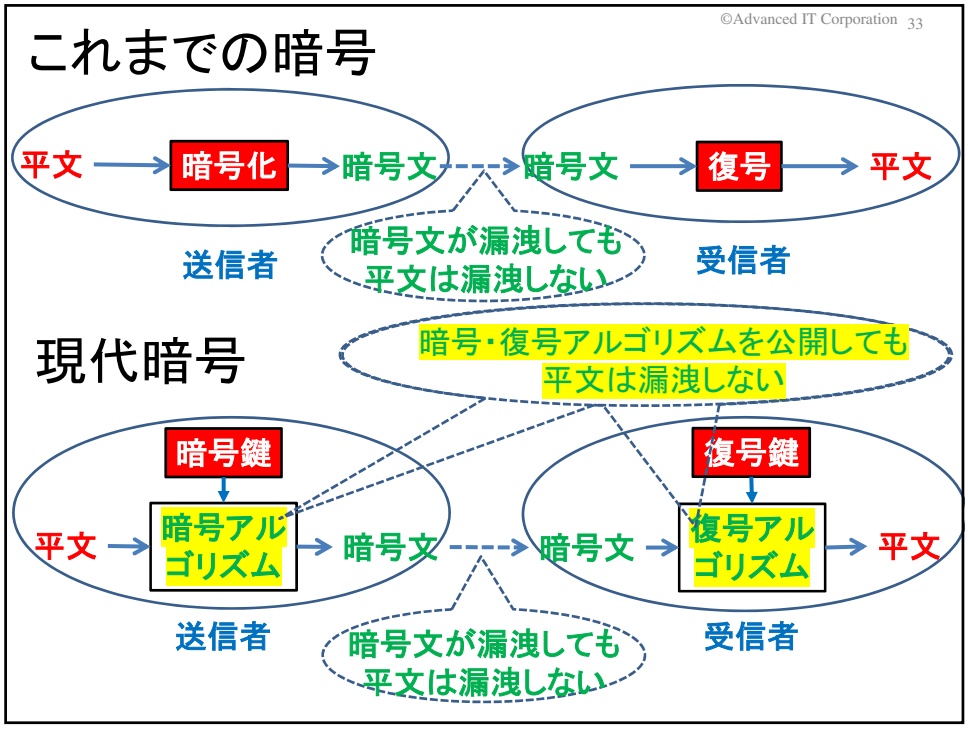

# 近代暗号から現代暗号へ

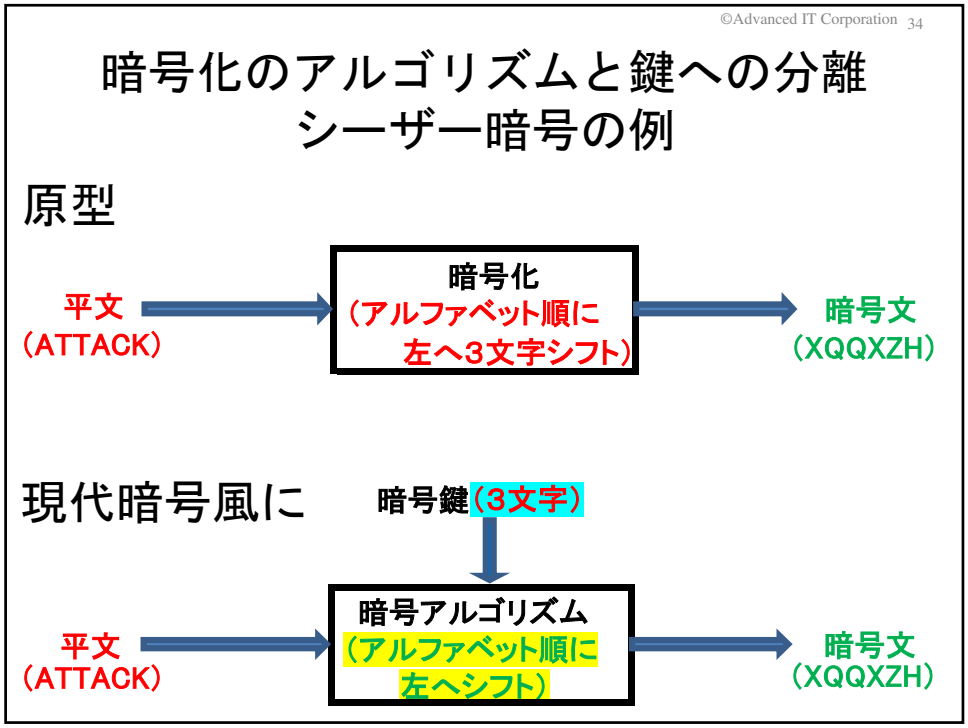
コンピュータ/ネットワークの発展により、
軍事的・政治的利用から、産業活動・生活活動での利用へ

多くのベンダによる開発競争、相互運用性へのニーズ
➔暗号化/復号ソフト開発に必要な暗号方式の公開が必要に

従来は“暗号方式を公開しない”ことで暗号の安全性を確保
➔従来とは異なる仕組みで
暗号の安全性を確保することが必要に！

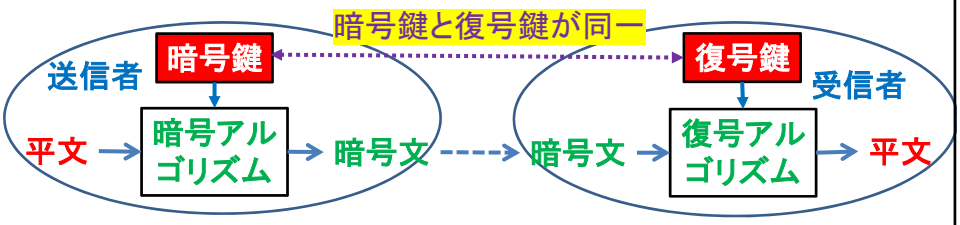
現代暗号では暗号方式を暗号アルゴリズムと暗号鍵に分離
現代暗号は、暗号アルゴリズムを公開しても
暗号鍵を公開しなければ安全性が確保できるよう、
暗号アルゴリズムが設計されている


©Advanced IT Corporation 33
これまでの暗号
平文
暗号化
暗号文
暗号文
復号
平文
送信者
暗号文が漏洩しても
平文は漏洩しない
受信者
現代暗号
暗号・復号アルゴリズムを公開しても
平文は漏洩しない
暗号鍵
復号鍵
平文
暗号アル
ゴリズム
暗号文
暗号文
復号アル
ゴリズム
平文
送信者
暗号文が漏洩しても
平文は漏洩しない
受信者

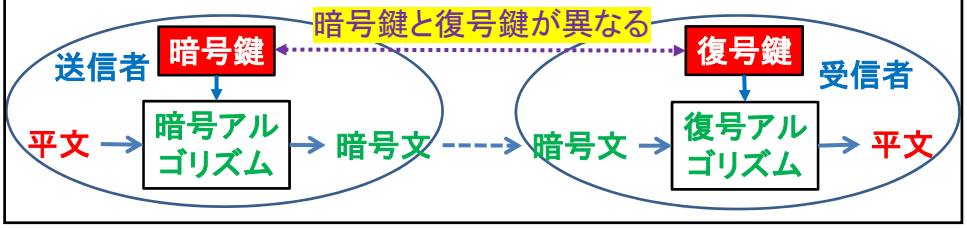

©Advanced IT Corporation 34
暗号化のアルゴリズムと鍵への分離
シーザー暗号の例
原型
平文
(ATTACK)
暗号化
(アルファベット順に
左へ3文字シフト)
暗号文
(XQQXZH)
現代暗号風に
暗号鍵(3文字)
平文
(ATTACK)
暗号アルゴリズム
(アルファベット順に
左へシフト)
暗号文
(XQQXZH)

# 現代暗号の二つの暗号方式

## 共通鍵暗号方式

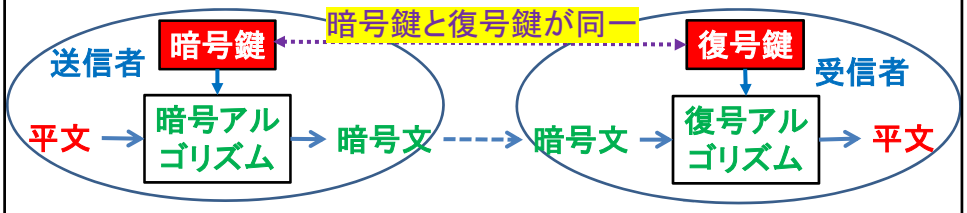



## 公開鍵暗号方式






# 共通鍵暗号方式の特徴



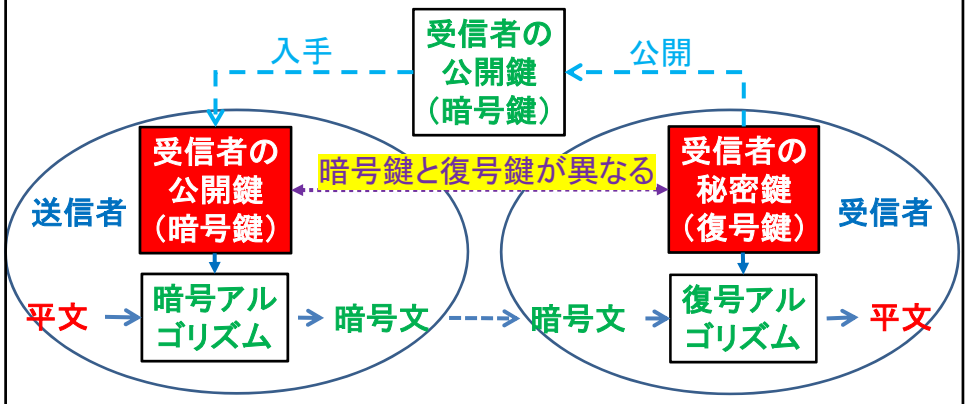

①暗号鍵と復号鍵が同一（共通鍵）

②送信者と受信者は秘密の共通鍵を
安全に保管しておくことが必要

③送信者と受信者で秘密の共通鍵を共有しておくことが必要

共通鍵暗号の鍵共有問題 ➔ Diffie-Hellmanの鍵共有方式

# 公開鍵暗号方式の特徴




①利用者は異なる二つの鍵、
公開鍵（暗号鍵）と秘密鍵（復号鍵）、を保有
②公開鍵から秘密鍵を計算できない
③秘密鍵は秘密に管理することが必要だが、公開鍵は公開可能
④公開鍵が受信者の正しい公開鍵であることの確認が必要
公開鍵の所有者確認 ➔ 公開鍵証明書、PKI



# （５）現代暗号（共通鍵暗号方式）

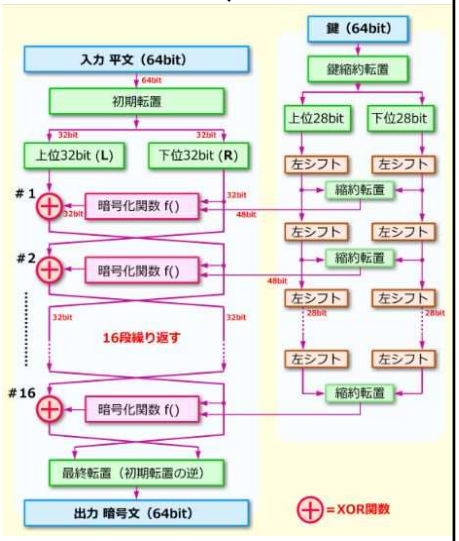
## 開発の歴史および社会での活用例

# 第1世代共通鍵暗号の代表：DES（Data Encryption Standard）

1976年に米国初の
データ暗号化標準として採用された
共通鍵暗号方式の暗号

世界で広範に利用された
最初の現代暗号

DESの暗号鍵（復号鍵）の鍵長は、
56ビット （$2^{56}$の鍵パターン）




鍵の例
1 0 0 1 1 0 0 0 1 0 1 1 1 0 0 0 0 1 1 1 0 0 1 0 0 1 1 0 0 0 1 0 1 1 1 0 0 0 0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 1 0 1

http://www.atmarkit.co.jp/ait/articles/1505/21/news030.html



# DES開発経緯

1960年代後半：IBMが暗号方式の研究に着手
1968年：米国標準局（NBS、現在のNIST）は調査の結果、
　統一された相互運用可能なデータ暗号化の標準規格が必要との結論
1971年：英国のロイズ銀行は、現金自動支払装置のデータ保護のために
　IBM考案の「Lucifer」を採用（IBMはLuciferを製品として提供開始）
1975年：NBSが標準案として改良版Luciferを公表
　**諜報機関である米国国家安全保障局（NSA）の不適切な干渉の疑惑**
**（NSAだけが暗号化データを容易に解読できるようにしたのではないか、**
**という疑惑に対し、米国上院諜報特別委員会による調査が実施された）**
1976年：米国連邦標準（FIPS）として承認
1981年：米国国家標準協会（ANSI）が定める標準として制定

**＜DESは、ビジネス分野（特に金融業界）で広範に利用された＞**

# DES解読の歴史
# 理論的手法による暗号解読

**差分解読法：解読者にとって都合の良い**
**平文と暗号文のペアが入手可能である場合の解読手法**

①平文とその暗号文、その平文の一部分を変更した暗号文など、
入手した平文と暗号文の多数の組合せから平文間の差分、
暗号文間の差分を利用し、秘密の鍵を推定する方法

②**1989年にイスラエルのBiham とShamirによって考案**

③差分解読法は、DESには有効では無かった

**線形解読法：平文とそれを暗号化した暗号文がペアで入手できるが、**
**攻撃者は平文を選ぶことができない場合を想定した解読手法**

①暗号化の関数を、より簡単な関数に近似（線形近似）させて置換え、
この線形近似させた関数を解読することにより、
少ない計算量で鍵を見つけようという方法

②**1993年に三菱電機の松井充氏によって考案**

③松井氏は線形解読法により、
$2^{43}$の平文と暗号文のペアが必要であるが、DES攻撃に成功



# DES解読の歴史
# 全数探索による暗号解読

復号鍵（暗号鍵）の鍵長がnビットの場合、$2^n$種のビットパターンの中に鍵は必ずある。全てのビットパターンをチェックすることにより鍵を見出そうとする解読手法。ブルートフォース解読とも呼ばれ、コンピュータの急速な高速化・廉価化に伴い、活発化。

DES Challenge：RSA Data Security社が1997年より毎年開催している暗号解読コンテスト（DESの安全性はコンピュータの高速化・廉価化により急速に低下）

| DES Challenge | DES Challenge の結果 | | |
|---|---|---|---|
| | 解読年月 | 解読時間 | 解読に使用した機器 |
| Ⅰ | 1997年6月 | 140日 | 約7万台のPC |
| Ⅱ－1 | 1998年2月 | 40日 | 約5万台のPC |
| Ⅱ－2 | 1998年7月 | 56時間 | 約25万ドルで作成した解読専用マシン |
| Ⅲ | 1999年1月 | 22時間15分 | DES専用解読マシン＋ 約10万台のPC |

DESの延命策として、DESで3回暗号化することにより安全性を高めた暗号アルゴリズムTripleDES（鍵長112ビット）がIBMにより考案され、1999年には米国連邦標準（FIPS）にも加えられ利用されてきたが、2005年には遂にDESが米国連邦標準から外された

# 日本の第1世代共通鍵暗号

日本企業も米国連邦標準DESを実装、製品・機器への組込み利用

日本独自の共通鍵暗号の開発は、DESの開発から10年の遅れ
1985年：NTTが鍵長64ビットのFEAL
1987年：NTTが安全性を高めたFEAL-8（鍵長64ビット）を開発
（ICカード等の8ビットマイクロプロセッサ上の
ソフトウェア向きに設計）
1988年：日立が鍵長64ビットのMULTI2を開発

また、鍵長の短さがDESの安全性を脅かしている状況から、
1990年：NTTはさらに安全性を高めた
鍵長128ビットのFEAL-N(X)を開発
1995年：三菱電機は、DES解読の経験を生かし、
鍵長128ビットのMISTYを開発
1999年：東芝も、DES/TripleDESとの互換モードを有する
TripleDESの改良版Triplo（鍵長128ビット）を発表



# 日本社会に大きなインパクトを与えた応用

（1）限定受信システムCAS（Conditional Access System）
1991年：BS有料放送「WOWOW」開始、2000年：BSデジタル放送が開始
多様なコンテンツが少額の費用で自宅のTVで楽しむことが可能

（2）不正コピー防止システムDTCP
（Digital Transmission Content Protection）
東芝とインテルが仕様策定推進
1998年：専用機器でしか視聴できなかった映画等のDVDがPCで視聴可能

（3）高速道路料金収受システムETC
（Electronic Toll Collection System）
2001年：自動車が料金所で停車する必要も無く高速道路を快適に走行可能

（4）ICカード乗車券（交通系ICカード）Suica
2001年：Suicaによる出改札システム導入（電子マネーEdyも同時期に）
駅の出改札の自動化・効率化、店舗での支払いも可能

## 暗号利用に対する規制・制度化の動き

（1）暗号技術に関する規制

対共産圏輸出統制委員会（ココム）（1950年～1994年）

鍵長が40ビットを超える暗号を組み込んだ製品の輸出は規制

ワッセナー・アレンジメント（1996年～）

大量破壊兵器等の開発等を行っている国、テロリストへの

軍事転用が可能な高度な貨物や技術の移転の防止（暗号技術も対象）

（2）米国のキーエスクロー（Key Escrow）政策

1993年：米国がキーエスクロー構想を発表（スキップジャック、クリッパーチップ）

通信暗号方式の統一、復号鍵の第三者機関への寄託（escrow）により、

捜査当局は裁判所の許可の下で暗号化された通信内容の解読が可能

（3）キーリカバリー（Key Recovery）政策

1996年：ゴア副大統領はキーリカバリー構想への転換を発表

米国民間企業11社がKRA発足、技術の開発・標準化活動着手

1997年：欧州や日本企業も参加し、70社以上の国際的な連合に発展

1999年：キーリカバリーの仕組みの有無に関係なく暗号技術・暗号製品の

輸出規制の緩和が進んだため、KRAは自然消滅

東芝も参加
3か月に1度の
欧米での会合に出席

東芝も、1998年、
通産省からの委託で
鍵回復システムを開発

最後の会合はハワイ
（日本メンバ主催）



## 第１世代共通鍵暗号の終焉・・・第2世代へ

（1）新たな米国連邦標準暗号の策定　AES（Advanced Encryption Standard）

1997年1月：米国国立標準技術研究所（NIST）がAES選定プロジェクト開始

2001年11月：Rijndael（ベルギーの暗号学者提案）をAESとして米国連邦標準登録

（AESは、鍵長が128ビット、196ビット、256ビットを選択できる共通鍵暗号）

（2）欧州の暗号技術推奨リスト策定活動　NESSIE

（New European Schemes for Signature, Integrity, and Encryption）

2000年1月：NESSIEプロジェクトを開始

2003年3月：暗号技術推奨リストを含む最終報告書を公表

推奨共通鍵暗号：MISTY1（64ビット）、Camellia（128ビット）、SHACAL-2（256ビット）、AES

（3）日本の電子政府推奨暗号策定活動　CRYPTREC

（Cryptography Research & Evaluation Committee）

2000年7月：CRYPTRECが、暗号技術の公募開始

2003年2月：「電子政府推奨暗号リスト」を決定

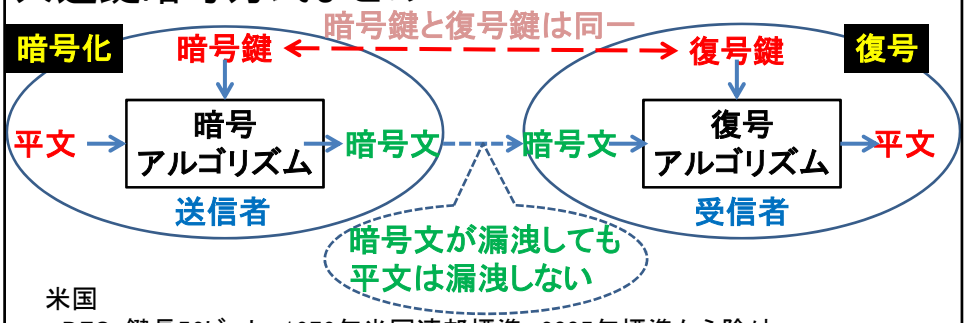
推奨共通鍵暗号（128ビット）：Camellia、CIPHERUNICORN-A、Hierocrypt-3、SC2000、AES

2013年3月：改訂版「電子政府推奨暗号リスト」を公表

推奨共通鍵暗号としては、Camellia、AESとなり、その他は推奨候補の位置づけに

## 共通鍵暗号方式まとめ

 64




米国
- DES：鍵長56ビット、1976年米国連邦標準、2005年標準から除外
- AES：鍵長128,192,256ビット、2001年米国連邦標準

日本
- NTT：1985年FEAL（64ビット）
- 三菱：1995年MISTY（128ビット）
- 東芝：1999年Triplo（128ビット）
- 2003年Camellia（128,192,256ビット）
- 2003年Hierocrypt-3（128,192,256ビット）

日本での活用事例
- 有料放送（1991年）：限定受信システム（CAS：Conditional Access System）
- PCでDVD視聴（1998年）：DTCP（Digital Transmission Content Protection）
- ノンストップ高速道路(2001年)：ETC（Electronic Toll Collection System）
- ICカード乗車券/電子マネーカード（2001年）：Suica,Edy

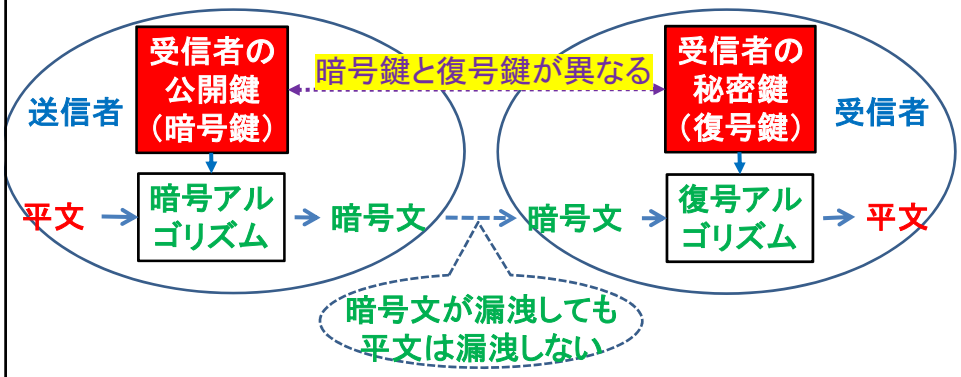
 65

# （６）現代暗号（公開鍵暗号方式）

## 開発の歴史および社会での活用例

 66

# 公開鍵暗号方式の特徴




①公開鍵（暗号鍵）と秘密鍵（復号鍵）が異なる

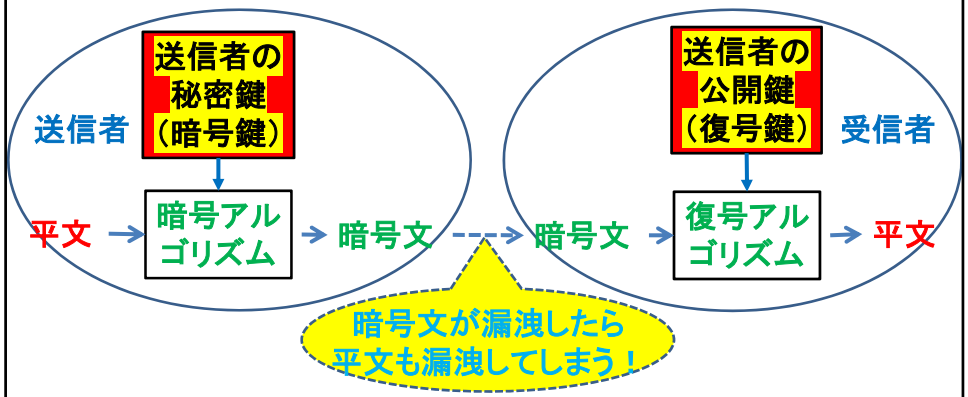
②公開鍵から秘密鍵を計算できない

③秘密鍵は秘密に管理することが必要だが、公開鍵は公開可能

④公開鍵が受信者の正しい公開鍵であることの確認が必要

 67

# 公開鍵暗号方式のもう一つの特徴




送信者の秘密鍵で暗号化したら・・・

受信者以外でも、送信者の公開鍵を入手し復号できるので、
平文は漏洩してしまう！ ➔ 情報の秘匿には使用不可

誰かの公開鍵で復号できたら、
その人が暗号化したことを確認できる ➔ 電子署名への応用

# 主要な公開鍵暗号方式

（1）Diffie-Hellmanの鍵共有方式

1976年：スタンフォード大学マーティン・ヘルマン教授が2人の
大学院生と、共通鍵暗号の鍵共有問題を解決する方法として発表

Diffie-Hellmanの鍵共有方式は、公開鍵暗号方式の概念を包含

（2）RSA暗号

1978年：アメリカのマサチューセッツ工科大学の
ロナルド・リベスト(Rivest)，アディ・シャミア(Shamir)，
レオナルド・エーデルマン(Adelman)が発表

2002年：3名はチューリング賞を受賞

（3）楕円曲線暗号

1985年頃：IBM トーマス・J・ワトソン研究所のビクタ・ミラーと
ワシントン大学のニール・コブリッツ が各々発明した暗号



# 日本社会の安心・安全強化のための応用

（1）セキュアなインターネットメール（S/MIME）

1982年：インターネットが稼働すると同時にインターネットメールも利用開始
セキュリティ機能は不十分（考慮されず）、でも急速な拡大

1995年：S/MIME（Secure / Multipurpose Internet Mail）開発
メール内容の秘匿（暗号化）、送信者の認証（署名）、
メール内容の改ざん検知（署名）

S/MIMEは残念ながら
社会での活用は限定的
S/MIMEの課題を克服する
SSMAX仕様を提案中

（2）セキュアなWebブラウザ（SSL/TLS）

1989年：WWW（World Wide Web）の提案　欧州原子力機構CERNのTim Berners-Lee

1993年：NCSA Mosaicを提供開始　画像も扱える画期的なブラウザ

1995年：Mosaic CommunicationsがSSLを開発
Netscape Navigator 1.1へ組み込み（https://・・・）
サーバ認証・クライアント認証（署名）、通信内容の秘匿（暗号化）

スーパコン応用拡大
を目的とした海外調査
イリノイ大学のNCSAを訪問
Mosaicに注目

（3）クレジットカード（EMV仕様）

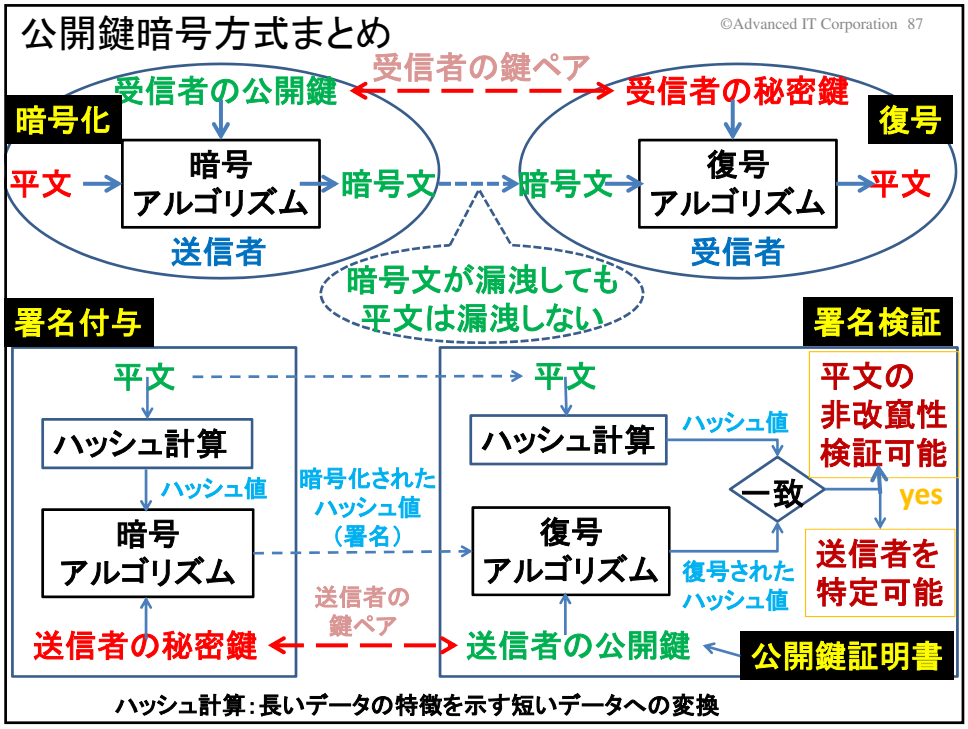
1993年：ICチップ搭載クレジットカード統一規格（EMV仕様）策定（日本導入:2001年）
公開鍵暗号としてRSA　共通鍵暗号としてTripleDES/AES

（4）マイナンバーカード

2016年1月：マイナンバーカード発行開始
公開鍵暗号としてRSA　共通鍵暗号としてAES

2021年3月：健康保険証としての機能付加予定

コロナウイルス感染症
緊急経済対策
特別定額給付金10万円
マイナンバーカードの活用




©Advanced IT Corporation 88

主要な公開鍵暗号方式

1976年：Diffie-Hellmanの鍵共有方式

1978年：RSA暗号
大きな素数の積の素因数分解問題の難しさを利用

1985年：楕円曲線暗号
楕円曲線上の離散対数問題の難しさを利用

日本での活用事例

1992年：商用インターネットサービス開始
1995年：セキュアインターネットメール（S/MIME）
1995年：セキュアWebブラウザ（SSL/TLS）

2001年：クレジットカード（EMV仕様） RSA、AES/TripleDES

2016年：マイナンバーカード RSA、AES

# （４）～（６）現代暗号 まとめ

犯罪への悪用も含め
暗号利用は民間中心へ

国や組織の諜報活動の道具
としての利用も水面下で活発



# （７） これからの暗号応用と課題

暗号の応用拡大
　＊ブロックチェーン/ビットコイン

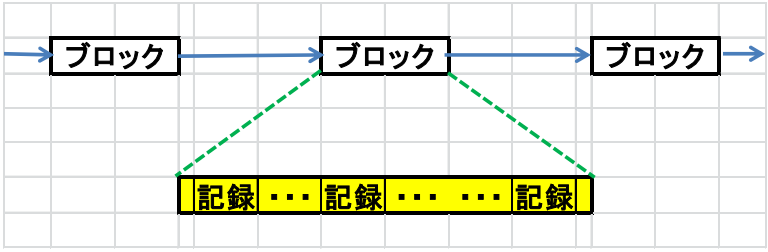
暗号の悪用
　＊ランサムウェア（コンピュータウイルス）

新たな課題と対応状況
　＊量子コンピュータの動向

# 暗号の応用拡大

## ブロックチェーン

取引・支払等の記録を（複数）格納しているブロックの連鎖




## ブロックチェーンの特徴

（1）中央管理組織の無い記録技術
　　ブロックの登録者はルールに従い希望者から選定

（2）記録消失の危険性が極めて低い記録技術
　　ブロックチェーンを多数のノードで重複管理

（3）過去の記録の改ざんが難しい記録技術（ビットコインを例に説明）



# ビットコインブロックチェーン

**ブロックチェーン技術を**
**最初に具現化したのがビットコイン！**

**ビットコインでは、ブロックチェーンに送金記録を格納**

## ビットコインの歴史

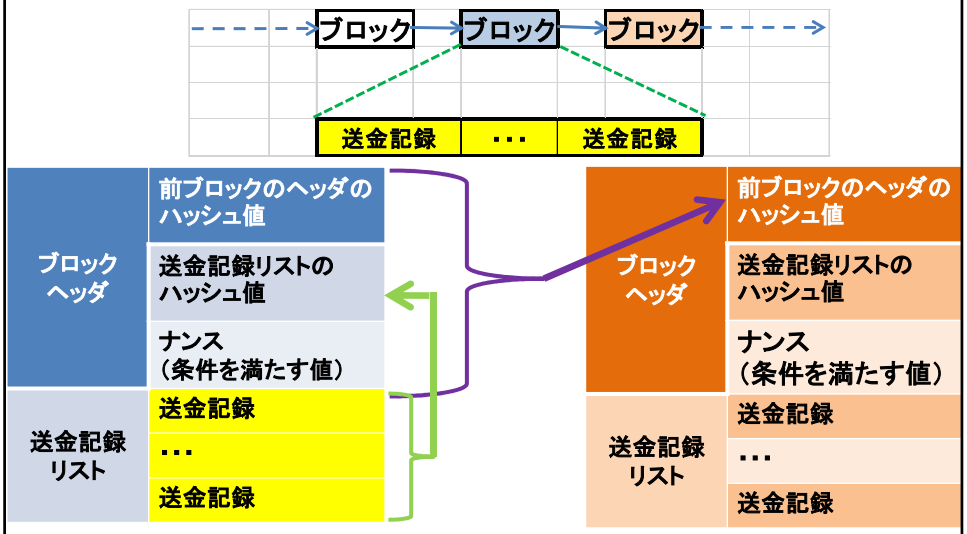
2008年10月　サトシ・ナカモトがインターネット上で論文発表

2009年1月　ビットコインソフトウェアが開発され運用開始
　（その直後に、最初のトランザクションが発行された）

2010年5月　現実世界で初めて決済に使用された
「ピザ2枚（約25ドル）=1万BTC」で取引が成立（1BTC≒0.2円）
1BTC≒98万円：2020年5月6日 ➔ ピザ1枚　約49億円！

 103

## ビットコインブロックチェーンにおけるブロックの連鎖




ハッシュ値：対象となるデータの特徴を一定の長さのデータに変換したもの。
対象となるデータが1ビットでも変われば、ハッシュ値も変わる。

 105

## 暗号資産（仮想通貨） 最近の動向

現状　暗号資産の数：2564　　資産総額：¥27,141,714,792,875
https://coinmarketcap.com/ja/all/views/all/ （2020年5月6日）
世界の通貨供給量（現金＋預金）：9465兆円（2016年）
(日本：現金104.3兆円、現金+預金818.0兆円 2019年12月）

動向
- 国家の暗号通貨発行（法定暗号通貨）の可能性
  - ベネズエラの官製暗号通貨「Petro」
  - ロシアの官製暗号通貨「CryptoRuble」
  - 中国の官製暗号通貨「デジタル人民元」
  - その他：UAEとサウジアラビア、スウェーデン、エストニア
- StableCoin（価格が安定した暗号通貨）の可能性
  - Tether,TrueUSD,他約80存在　Libraも2020年発行予定

課題
- 犯罪・不正目的の利用増大　暗号技術による匿名性の悪用
  - マネーロンダリング、違法取引サイトでの決済
  - ➔ 匿名性と共に確実な特定・追跡性が必要
- 各国中央銀行の金融政策による経済活動への影響力低下

# 社会を脅かす暗号の悪用
# ランサムウェア（ウイルス）

ランサムウェアとは
- 暗号化による恐喝ソフトウェア:
  「データを暗号化した」「復活するには身代金を支払え」
- 主要な感染経路:メール、Webサイト、可搬記憶媒体

現状:（1989年　最初のランサムウェアAIDS）
- 個人向けの少額（数万円程度）の身代金
- 医療機関、自治体を対象に高額）身代金
  - Hollywood Presbyterian Medical Center（＄40万）
  - Kansas Heart Hospital（＄40万）
  - Riviera Beach City（＄60万）、Lake City（＄50万）

氾濫の背景
- 暗号化データの復号鍵無しの復号は困難（暗号技術の悪用）
- 暗号化によるウイルス検知ソフトの無効化
- 暗号資産（ビットコイン）による支払いのため
  受取者の特定・追跡は困難（暗号資産の悪用）
- RaaS（Ransomware as a Service）の出現（2016年）　SATAN



# 新たな課題と対応状況
# 量子コンピュータ

従来のコンピュータの性能向上の限界（ムーアの法則は終焉？）

➔ 量子力学の重ね合わせ現象を利用した同時並列計算

現在のスーパコンの性能の、15億倍？　9000兆倍？

| | 量子コンピュータ | | | |
|---|---|---|---|---|
| 方式 | 量子ゲート | 量子アニーリング | デジタル回路によるアニーリング | レーザーネットワーク |
| 対象 | 通常のコンピュータと同じ | 組合せ最適化問題 | | |
| 特徴 | 汎用型の量子コンピュータ（高速に解ける問題は限定的） | 組合せ最適化問題に特化した量子コンピュータ | デジタル回路の設計を工夫 | レーザーの量子力学的な特性を利用 |
| 最大ビット数（注） | 20ビット（IBM） | 2,048ビット（D-Wave） | 102,400ビット（日立） | 2,048ビット |
| 主要企業 | IBM、グーグル、インテル、IonQ | D-Wave、グーグル、ノースロップグラマン、NEC | 富士通、日立 | NTT |

https://www.sbbit.jp/article/cont1/36552

量子アニーリング：「組合せ最適化処理」を高速かつ高精度に実行すると期待されている計算技術

# 量子コンピュータ（量子ゲート方式）の暗号技術への影響

共通鍵暗号

現状、2030年までは、鍵長は112ビットで安全とされている

（一般に128ビット、一部192ビット,256ビットも利用されている）

➔グローバーのアルゴリズム　計算量減少例　$2^{100}$➔$2^{50}$

➔サイモンのアルゴリズム　計算量減少例　$2^{100}$➔100

公開鍵暗号

現状、2030年までは、鍵長は2048ビットで安全とされている

➔ショアのアルゴリズム

RSA（素因数分解の困難性）　計算量減少例　$2^{2048}$➔2048

（楕円曲線暗号でも計算量が大幅に減少可能）



# 耐量子コンピュータ暗号

量子コンピュータへの対応策

共通鍵暗号　　鍵長を増大（現在の2～3倍）

公開鍵暗号　　耐量子コンピュータ暗号への移行

主要な耐量子コンピュータ暗号方式

格子に基づく暗号: 格子問題（LWE 問題等）

符号に基づく暗号: LPN 問題

多変数多項式に基づく暗号: MP 問題, IP 問題

同種写像に基づく暗号: 同種写像問題

各国の動き

米国：NISTによる標準化（2017年公募開始）

2019年1月：公開鍵暗号17候補、デジタル署名9候補

日本：CRYPTRECにて2019年6月より検討開始

第48回総合科学技術・イノベーション会議（2020年1月23日）

量子技術イノベーション戦略報告

＜主要技術領域＞

i）量子コンピュータ・量子シミュレーション　ii）量子計測・センシング

iii）量子通信・暗号　iv）量子マテリアル（量子物性・材料）

# （７）これからの暗号応用と課題

## まとめ

**暗号応用拡大による新たなサービスでは課題も発生**

ブロックチェーン/ビットコイン

➔不正・不法取引、マネーロンダリング、脱税等への対策

**暗号の悪用も活発化**

ランサムウェア（コンピュータウイルス）

➔インターネット利用者の匿名性と特定・追跡性の両立対策

➔暗号技術は諸刃の剣！

暗号技術の活用による社会の発展を促進しつつも、
社会の安心・安全を維持する仕組みの実装も必要

**情報技術の発展・普及は暗号技術へのチャレンジ**

IoTの爆発的社会実装 ➔ 軽量暗号

量子コンピュータ実用化 ➔ 耐量子コンピュータ暗号

➔暗号技術が社会の更なる発展を阻害しないよう
要素技術の研究、社会実装方式の研究開発が必要



# 本日のお話

（1）古代暗号　暗号の歴史の始まり
（2）古典暗号　外交活動の活発化による暗号の普及
（3）近代暗号　暗号の作成･解読は手作業から機械へ

紛争の道具としての暗号

（4）現代暗号　暗号方式の
暗号アルゴリズムと暗号鍵への分離
（5）現代暗号（共通鍵暗号方式）
特徴、開発の歴史、社会での活用例
（6）現代暗号（公開鍵暗号方式）
特徴、開発の歴史、社会での活用例

産業・生活を支える暗号

（7）これからの暗号応用と課題
拡大する暗号応用･暗号の悪用･新たな課題と対応状況

インターネット依存社会の発展を支える暗号

ご清聴、ありがとうございました。

先頭へ