文化フォーラム

暗号と社会のかかわり史

（1）暗号って、どんなもの？
（2）人類の歴史の中で、暗号はどのように使われてきたの？
（3）現在の私たちの生活で、どのように使われているの？

2024年5月24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）
　研究開発活動：中央大学研究開発機構、九州大学大学院
　技術分野：暗号・認証、秘密分散、本人確認技術（バイオメトリクス）、
　　電子メールセキュリティ、IoTシステム、ビッグデータ、AI、
　　暗号資産セキュリティ、ブロックチェーン技術

暗号とは？

暗号（文）：秘密にしておきたい情報を
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：誰にでも情報を理解できる形で表現されたデータ（平文）を
特別な知識を有する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人が、
その知識を利用し暗号文を平文へ変換すること

暗号技術：暗号化および復号に使用する技術の総称

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

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]新たな課題と対応動向（主要なトピック紹介）

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！

［１］古代暗号

暗号の歴史の始まり

(1) スキュタレー暗号
（紀元前600年頃、ギリシャ）

(2) シーザー暗号
（紀元前100年ごろ、ローマ）

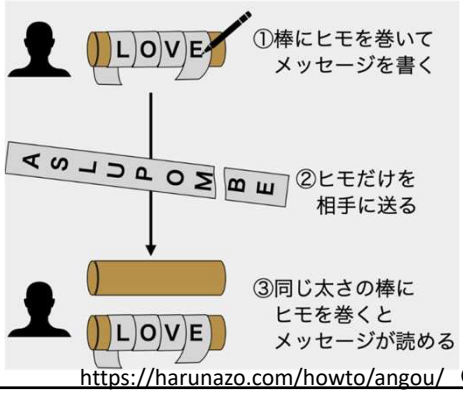
(1) 古代暗号：スキュタレー暗号

紀元前600年頃、古代ギリシャの都市国家・スパルタで使用

暗号化：ある太さの棒（スキュタレー）に革紐を巻きつけて
棒に沿って革紐に文字列（平文）を書く

復号　：同じ太さの棒にその革紐を巻きつけることにより
送り手が書いた文字列が棒に沿って現れる

https://commons.wikimedia.org/wiki/File:Skytale.png



https://harunazo.com/howto/angou/

平文の文字の順番を入れ替えることによって暗号化する方式を「転置式暗号方式」という。

(2) 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

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）

復号の例

暗号文（XQQXZH） → 復号（アルファベット順に右へ3文字シフト） → 平文（ATTACK）

1文字または数文字単位で別の文字や記号等に変換することによって暗号化する方式を「換字式暗号方式」という。

余談

古代暗号：ヒエログリフ

https://commons.wikimedia.org/wiki/File:Egypt_Hieroglyphe2.jpg

紀元前3000年頃の、現存する最古の暗号（？）

ヒエログリフは、ヒエラティック、デモティックと並ぶエジプト語の表記体系の一つで、象形文字の一種。

機密情報の秘匿を目的としたいわゆる「暗号」とは異なる。

太平洋戦争の時には、暗号として鹿児島弁が使われた

ドイツと日本の情報交換は、無線通信による暗号電報のみ。
しかし、その暗号はすべて連合国側に筒抜けで、
盗聴されても理解できない言葉で会話することに。
そこで選ばれた言葉が標準語に最も遠い鹿児島弁。

暗号化前の平文
「カジキさん、カジキさん、ノムラの親爺は早く発たせなくてはいけないが、もう発ちましたか？」
「ヨシトシさん、ヨシトシさん。ヨシトシの親爺はもうすぐ発ちます」
「カジキさん、ヨシトシの親爺は、もう潜って行かれましたか」
「潜水艦で行きました」

『深海の使者』吉村昭　https://www.yama-mikasa.com/entry/2017/05/11/060554

［２］古典暗号

外交活動の活発化による暗号の普及

(1) ノーメンクラタ暗号
（15世紀から18世紀、スコットランド）

(2) 上杉暗号
（16世紀頃、日本）

(1) 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

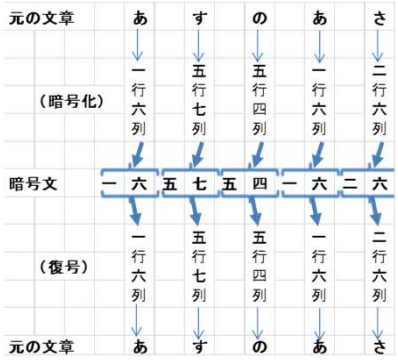
(2) 古典暗号：上杉暗号

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



座標式暗号方式：発明者はポリュビオス
ギリシャ人（紀元前203～120年）

［３］近代暗号

暗号の作成・解読は
手作業から機械へ

(1)エニグマ暗号
（第二次世界大戦、ドイツ）

(2)ミッドウェー暗号
（第二次世界大戦、日本）

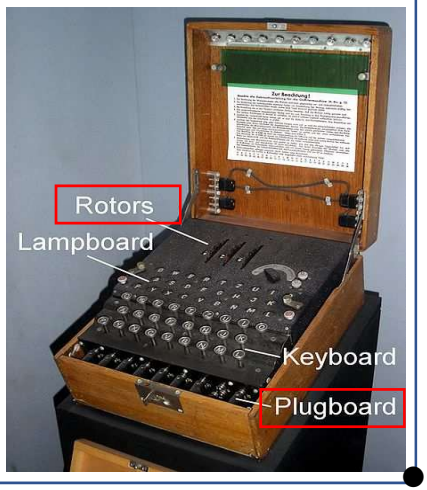
（第一次世界大戦：1914年～1918年　　第二次世界大戦：1939年～1945年）

(1)近代暗号：エニグマ暗号

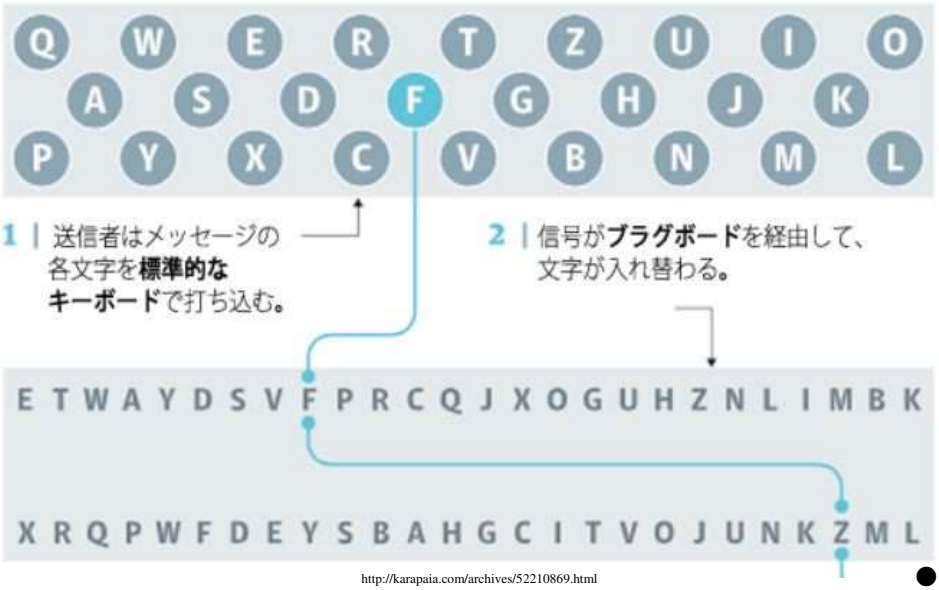
第一次世界大戦（1914年～1918年）終盤の1918年、ドイツの発明家アルトゥール・シェルビウスによって発明された機械式暗号機

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。

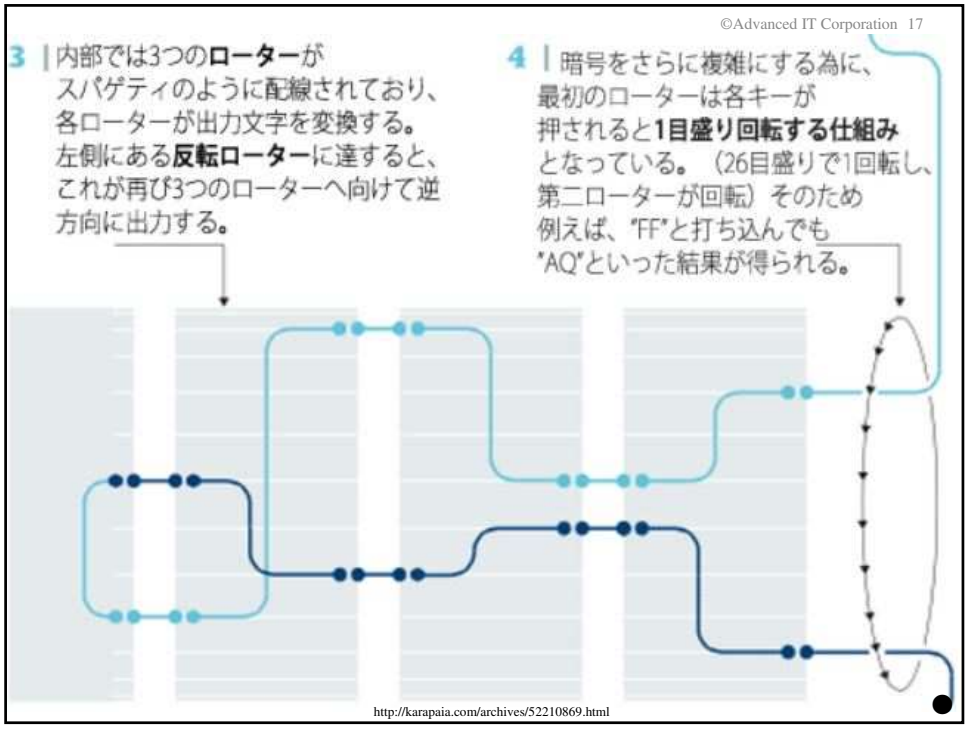
しかしその後、イギリスによって暗号が解読されていたことで第一次世界大戦に敗れたと知ったドイツは、暗号が国家の存亡を左右するという危機感から、エニグマ採用を決定。

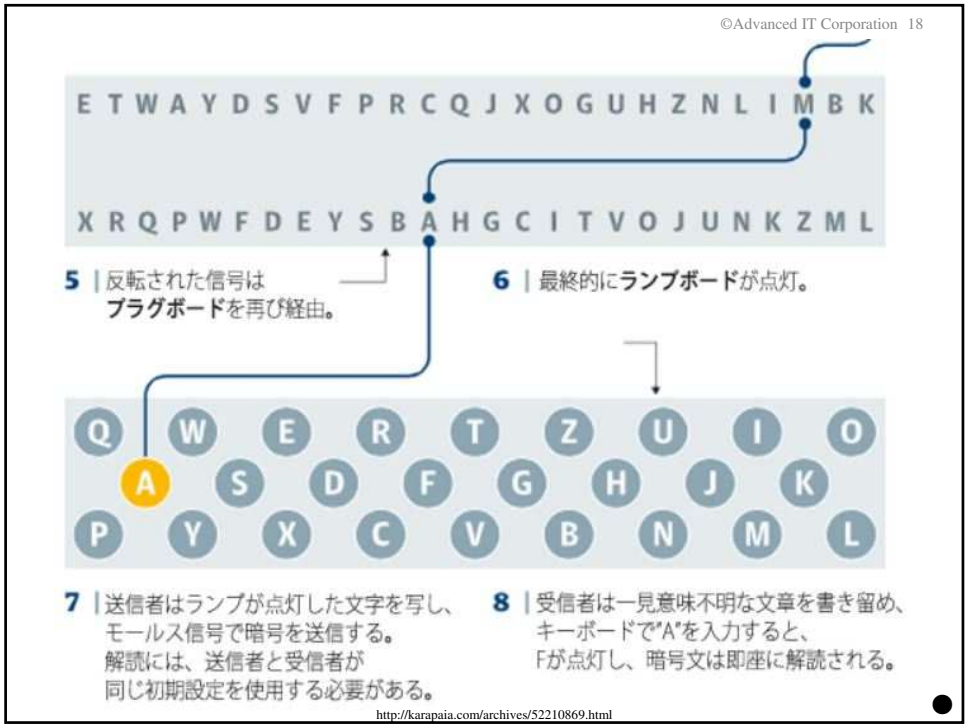


Enigma エニグマの仕組み



http://karapaia.com/archives/52210869.html


©Advanced IT Corporation 17
3 | 内部では3つのローターがスパゲティのように配線されており、各ローターが出力文字を変換する。左側にある反転ローターに達すると、これが再び3つのローターへ向けて逆方向に出力する。
4 | 暗号をさらに複雑にする為に、最初のローターは各キーが押されると1目盛り回転する仕組みとなっている。（26目盛りで1回転し、第二ローターが回転）そのため例えば、"FF"と打ち込んでも"AQ"といった結果が得られる。
http://karapaia.com/archives/52210869.html


©Advanced IT Corporation 18
E T W A Y D S V F P R C Q J X O G U H Z N L I M B K
X R Q P W F D E Y S B A H G C I T V O J U N K Z M L
5 | 反転された信号はプラグボードを再び経由。
6 | 最終的にランプボードが点灯。
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
7 | 送信者はランプが点灯した文字を写し、モールス信号で暗号を送信する。解読には、送信者と受信者が同じ初期設定を使用する必要がある。
8 | 受信者は一見意味不明な文章を書き留め、キーボードで"A"を入力すると、Fが点灯し、暗号文は即座に解読される。
http://karapaia.com/archives/52210869.html

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。

(2)近代暗号：ミッドウェー暗号（海軍D暗号）

第二次世界大戦のターニング・ポイントとなった、
ミッドウェー海戦当時に海軍が使用していた暗号

D暗号は、エニグマ暗号のような1文字ごとの変換ではなく、コード式を採用した語句暗号とも呼ばれる方式

具体的には、一つの語句・文章に対して、あらかじめ対応する文字や数字を対応付ける方式で、対応一覧を「暗号書（コードブック）」に記載しておき、発信者はこれを参照して変換後、更に乱数表を使い加工する方式

昭和17年に連合軍が撃沈した日本海軍の潜水艦から暗号書・乱数表が回収されたことにより、日本海軍の暗号がだんだん読まれるようになった

ミッドウェー海戦についても、アメリカが日本海軍の暗号を解読し待ち伏せをしていた

［１］古代暗号～［３］近代暗号まとめ

［1］古代暗号　暗号の歴史の始まり
　　(1)スキュタレー暗号（紀元前600年頃） (2)シーザー暗号（紀元前100年頃）

［2］古典暗号　外交活動の活発化による暗号の普及
　　(1)ノーメンクラタ暗号（15世紀から18世紀） (2)上杉暗号（16世紀頃）

［3］近代暗号　暗号の作成・解読は手作業から機械へ
　　(1)エニグマ暗号（第二次世界大戦） (2)ミッドウェー暗号（第二次世界大戦）

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

余談

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

［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

(1)近代暗号から現代暗号へ

(2)現代暗号の二つの暗号方式

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） 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）（➔1988年WIDE）
- 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）

1983年 ケン・トンプソン、デニス・リッチー、チューリング賞受賞

1981年 パソピア8発売 1982年 社内2万人教育

2004年 ヴィントン・サーフ ロバート・カーン チューリング賞受賞

1983年 SUN-WS評価 1984年 社内標準へ

1985年 インターネット実用化実験開始 1987年 InetClub設立

(1) 近代暗号から現代暗号へ

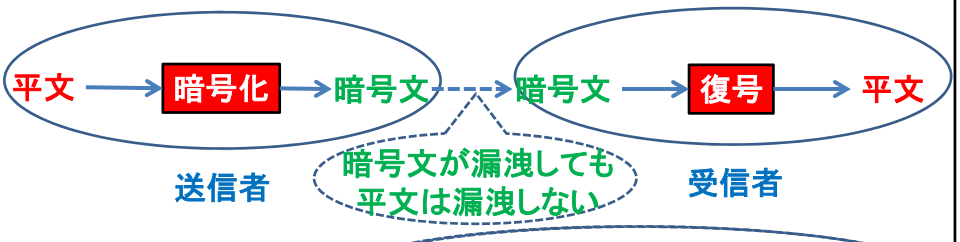
コンピュータ/ネットワークの発展により、
軍事的・政治的利用から、産業活動・生活活動での利用へ

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

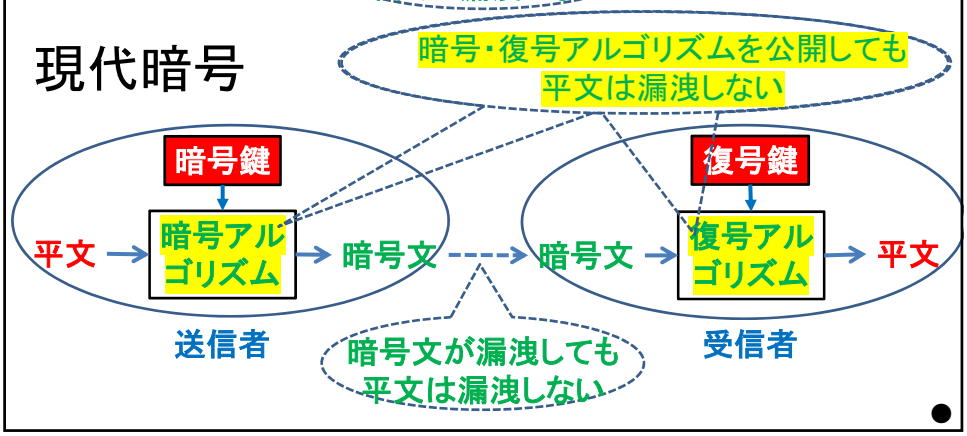
従来は“暗号方式を公開しない”ことで暗号の安全性を確保
➔従来とは異なる仕組みで
暗号の安全性を確保することが必要に！

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

これまでの暗号

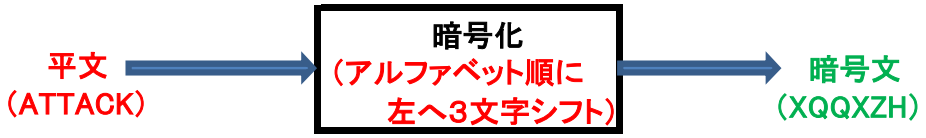


現代暗号

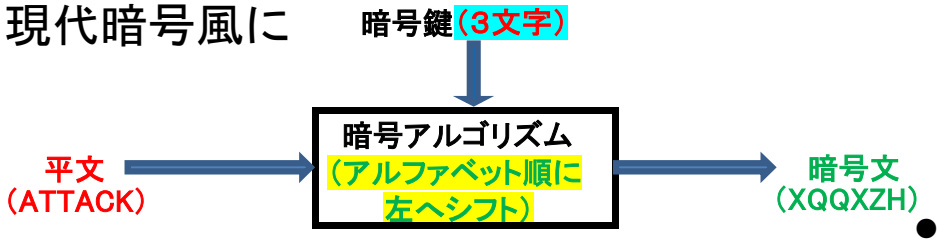


暗号化のアルゴリズムと鍵への分離
シーザー暗号の例

原型

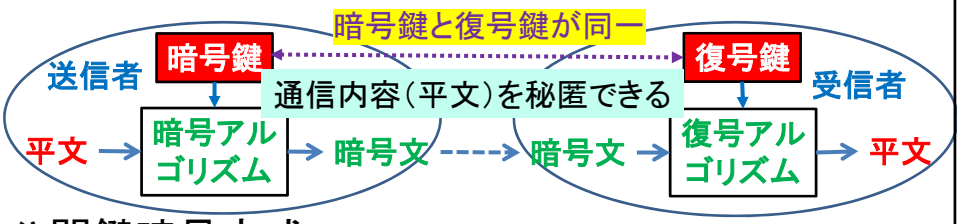


現代暗号風に

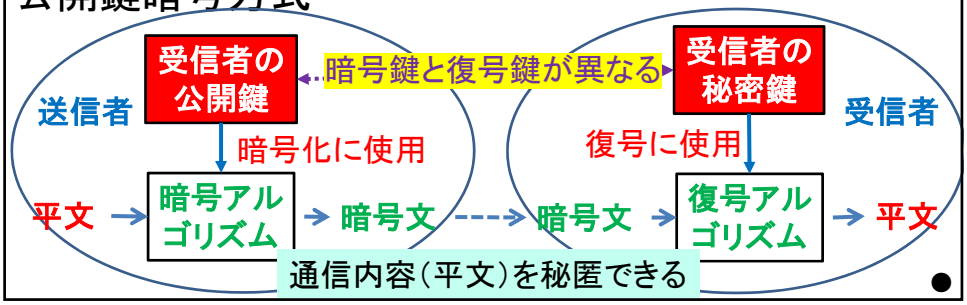


(2)現代暗号の二つの暗号方式

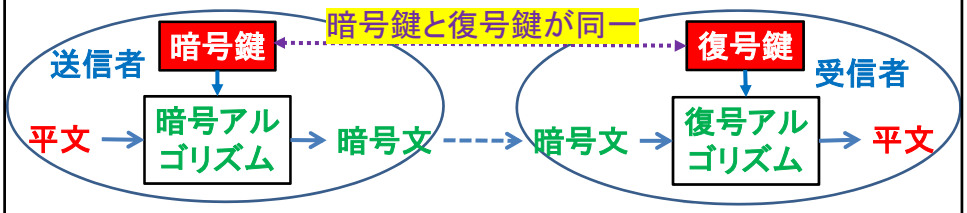
共通鍵暗号方式



公開鍵暗号方式



共通鍵暗号方式の特徴



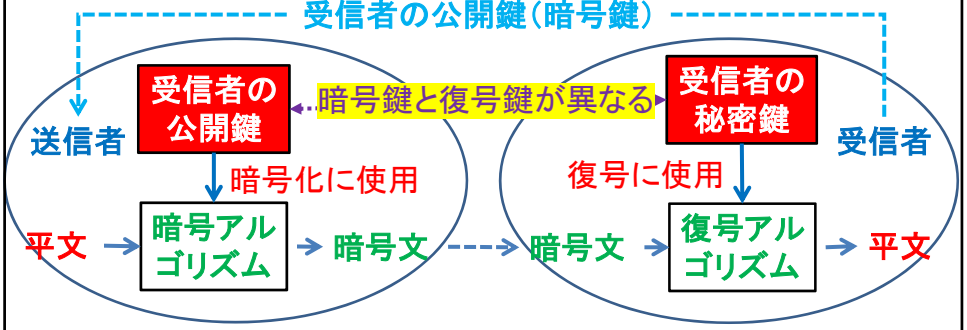
①暗号鍵と復号鍵が同一（共通鍵）

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

(1)第1世代共通鍵暗号の代表：DES
(2)日本の第1世代共通鍵暗号
(3)日本社会に大きなインパクトを与えた応用
(4)暗号利用に対する規制・制度化の動き
(5)第１世代共通鍵暗号の終焉・・・第2世代へ

(1)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

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、
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：IBMが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・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疑惑。
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**1989年にイスラエルのBiham とShamirによって考案**
②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**1993年に三菱電機の松井充氏によって考案**
②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

(2)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

(3)日本社会に大きな影響を与えた応用

①限定受信システムCAS　1991年
BS有料放送「WOWOW」、2000年にはBSデジタル放送開始
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　1998年
東芝とインテルが仕様策定推進
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　2001年
自動車が料金所で停車する必要も無く道路を快適に走行可能

④ICカード乗車券（交通系ICカード）　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

(4)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

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
（Clipper Chipと呼ばれるハードウェアとSkipjackと呼ばれる非公開の暗号アルゴリズム）

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

(5)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

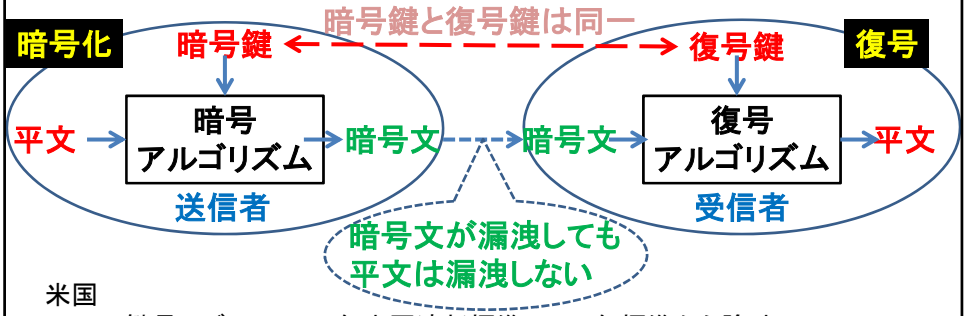
2003年2月：「電子政府推奨暗号リスト」を決定　推奨共通鍵暗号(128ビット)：

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



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)

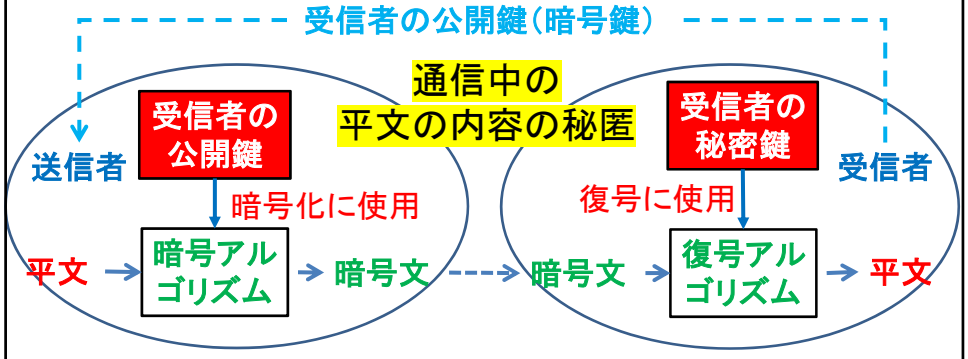
ノンストップ高速道路(2001年)：ETC(Electronic Toll Collection System)

ICカード乗車券/電子マネーカード(2001年)：Suica,Edy

［６］現代暗号（公開鍵暗号方式）

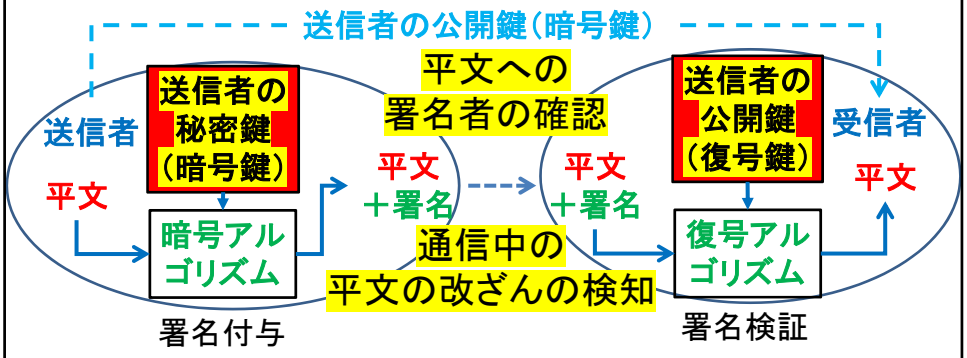
(1) 主要な公開鍵暗号方式
(2) 日本社会の安心・安全強化のための応用

公開鍵暗号の暗号化への利用



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

公開鍵暗号のもう一つの利用形態：署名



署名付与：平文の特徴データ（ハッシュ値）を
送信者（署名者）の暗号鍵で暗号化し生成

署名検証：署名を復号したものが、
受信した平文の特徴データと一致するかどうかの確認

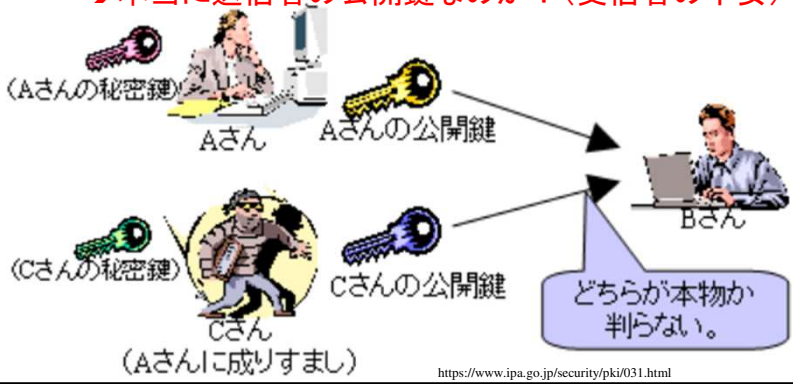
公開鍵暗号の利用の課題
公開鍵の正しさをどうやって確認？

送信者による暗号化：受信者の公開鍵を使用

➔本当に受信者の公開鍵なのか？（送信者の不安）

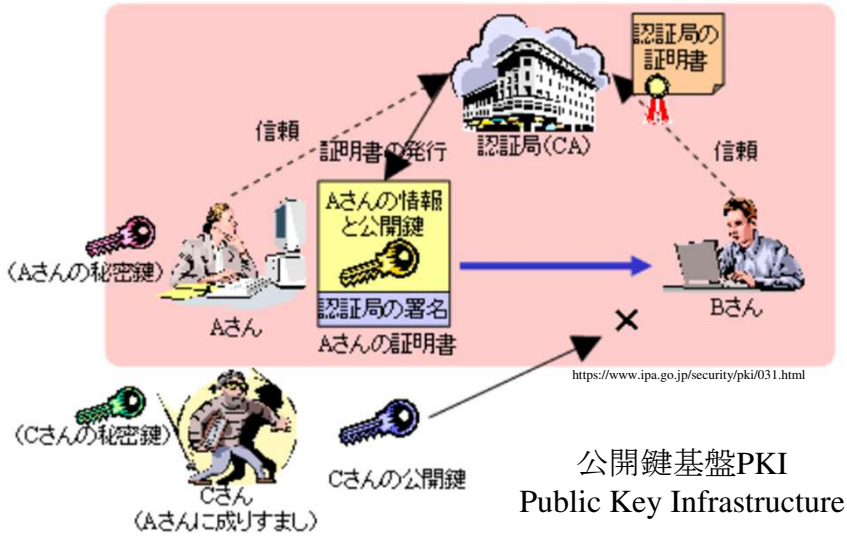
受信者による署名確認：送信者の公開鍵を使用

➔本当に送信者の公開鍵なのか？（受信者の不安）



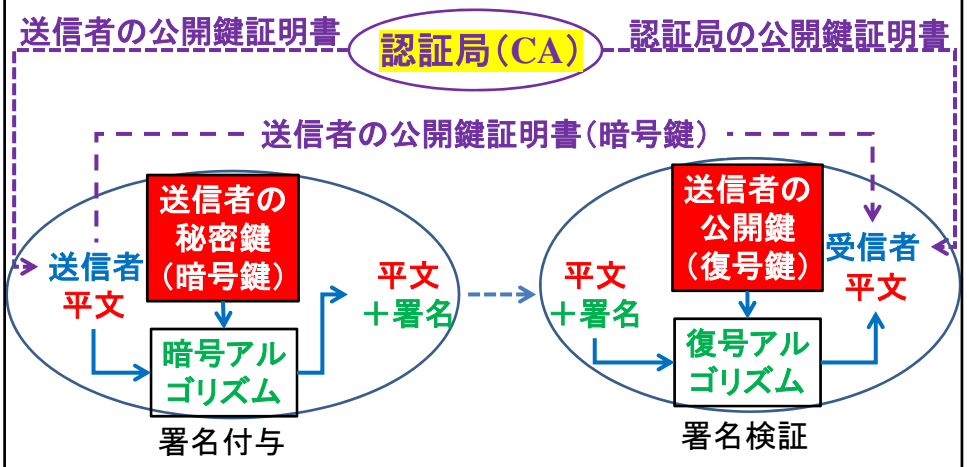
https://www.ipa.go.jp/security/pki/031.html

公開鍵証明書
公開鍵の正しさを信頼できる第三者が証明



公開鍵基盤PKI
Public Key Infrastructure

公開鍵暗号による署名の確認方法



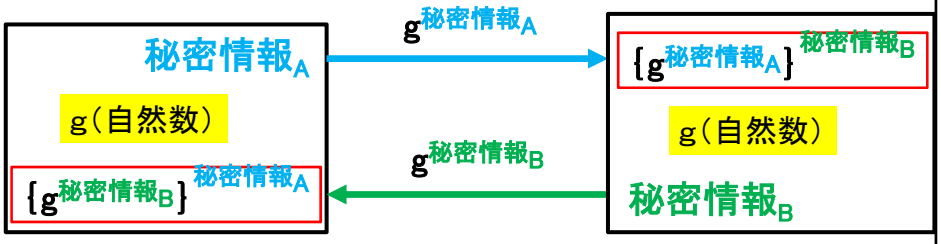
送信者の公開鍵証明書:認証局が送信者の公開鍵であることを保証

認証局の公開鍵証明書:上位の認証局が、
信頼できる認証局の公開鍵であることを保証

(1)主要な公開鍵暗号方式

①Diffie-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



Aさんと Bさんで安全に鍵を共有する方法

根拠1：$\{g^{\alpha}\}^{\beta}=g^{\alpha\times\beta}=g^{\beta\times\alpha}=\{g^{\beta}\}^{\alpha}$

根拠2：gとαからg^{α}を計算するのは簡単だが、
gとg^{α}からαを計算するのは困難
（通信情報は盗聴されても問題ない：離散対数問題の一方向性）●

②RSA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年ごろ

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

●

(2)日本社会に大きなインパクトを与えた応用

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

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)

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

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)

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暗号資産(ビットコインブロックチェーン)

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)

暗号資産の悪用を
抑止・防止可能な
安心・安全な
暗号資産移転基盤
SSVATFを提案中

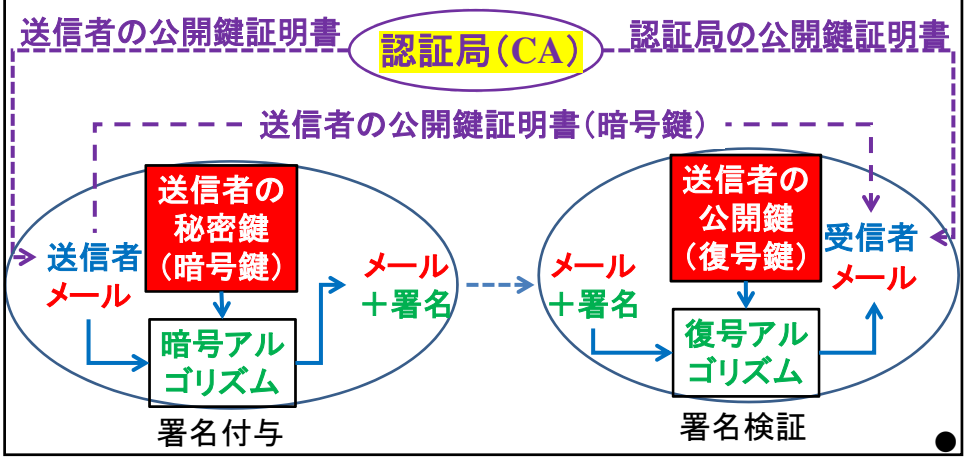
⑤マイナンバーカード

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

①日本社会の安心・安全のための応用
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
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



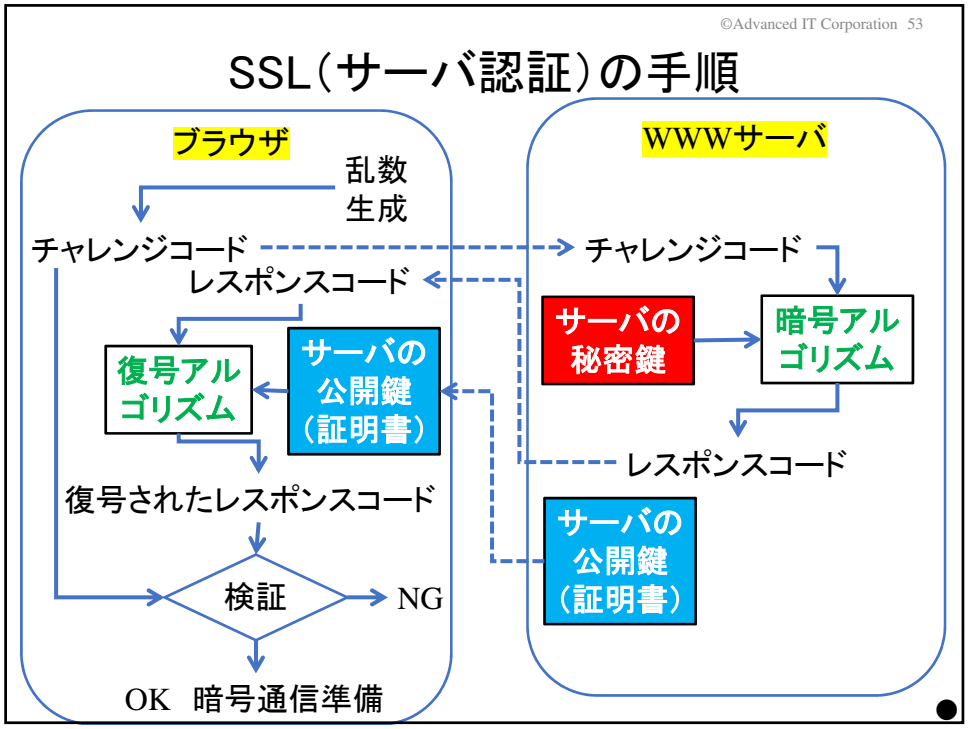
②日本社会の安心・安全のための応用
セキュアなWebブラウザ（SSL/TLS）

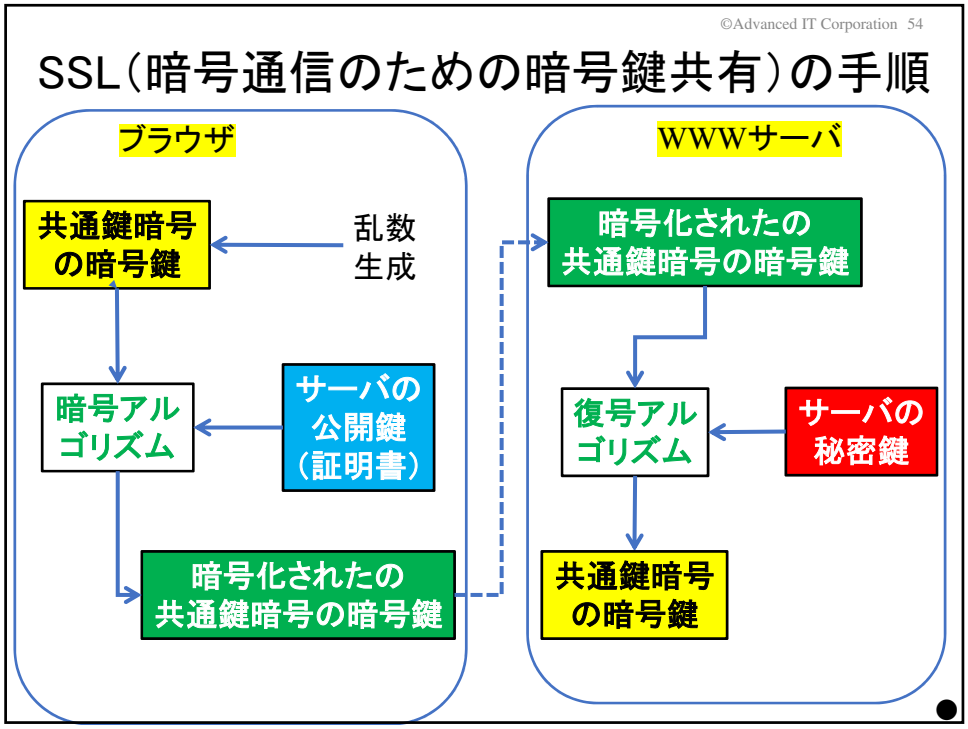
1989年：WWW（World Wide Web）の提案
欧州原子力機構CERNのTim Berners-Lee
1990年：WWWおよびエディタ（テキストベース）を実装
世界初のウェブページが公開
1993年：NCSA（米国立スーパーコンピュータ応用研究所）
がMosaicを提供開始、画像も扱える画期的なブラウザ
1994年：Mosaic Communications社設立（Marc Andreessen）
Netscape Navigator 1.0を提供開始
1995年：Mosaic Communications社が
SSL（Secure Socket Layer）を開発
Netscape Navigator 1.1へ組み込み
1996年：SSLの標準化は、国際標準仕様提案機関の一つ、
IETFへ移管され、名称もTLSへ変更し議論継続

テキストベース
であったが
有用性を実感

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

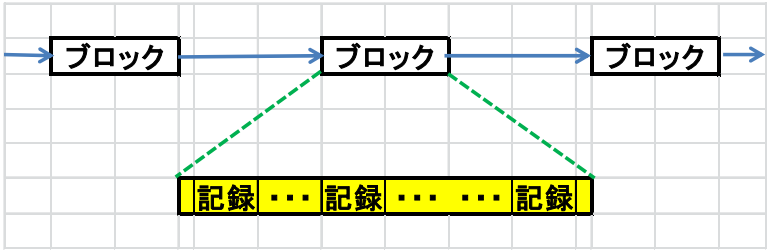
クライアントPC側に専用ソフトのインストールが不要なため、
インターネット上のほとんどのサービスは、Webベースで提供！


©Advanced IT Corporation 53
SSL（サーバ認証）の手順
ブラウザ
WWWサーバ
乱数
生成
チャレンジコード
チャレンジコード
レスポンスコード
サーバの
秘密鍵
暗号アル
ゴリズム
復号アル
ゴリズム
サーバの
公開鍵
（証明書）
レスポンスコード
復号されたレスポンスコード
サーバの
公開鍵
（証明書）
検証
NG
OK 暗号通信準備


©Advanced IT Corporation 54
SSL（暗号通信のための暗号鍵共有）の手順
ブラウザ
WWWサーバ
共通鍵暗号
の暗号鍵
乱数
生成
暗号化された
共通鍵暗号の暗号鍵
暗号アル
ゴリズム
サーバの
公開鍵
（証明書）
復号アル
ゴリズム
サーバの
秘密鍵
暗号化された
共通鍵暗号の暗号鍵
共通鍵暗号
の暗号鍵

④日本社会の安心・安全のための応用
暗号資産（ビットコインブロックチェーン）

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

AからBへの10BTCのビットコイン送金記録

使用する送金記録ID=m

入力		出力	
入力元	所有権	出力金額	出力先
		8	Aのアドレス1（公開鍵1に対応）

使用する送金記録ID=n

入力		出力	
入力元	所有権	出力金額	出力先
		7	Aのアドレス2（公開鍵2に対応）

出力先（送金先）
新たな受取者（B、A）の公開鍵から生成されるビットコインアドレス（27～34文字）で指定

Aが新たに作成する送金記録

入力		出力	
入力元	所有権	出力金額	出力先
ID=m Out=1	公開鍵1（256ビット）、署名1	10	Bのアドレス
ID=n Out=2	公開鍵2（256ビット）、署名2	5	Aのアドレス3

署名1：公開鍵1に対応する秘密鍵1による署名
署名2：公開鍵2に対応する秘密鍵2による署名

 57

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！

 58

暗号資産（仮想通貨） の動向

現状　暗号資産の数：8884
資産総額：約230兆円
https://coinmarketcap.com/ja/all/views/all/ （2023年12月12日）
（日本の2023年度予算は、114兆円余り（一般会計の総額）

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

対策
利用者の匿名性と共に確実な特定・追跡性が必要

➔SSVATF（安心・安全な暗号資産流通基盤）を提案中

社会・経済の健全な発展に資する
社会的責任を果たしうる暗号資産業界へ

⑤日本社会の安心・安全のための応用 マイナンバーカード

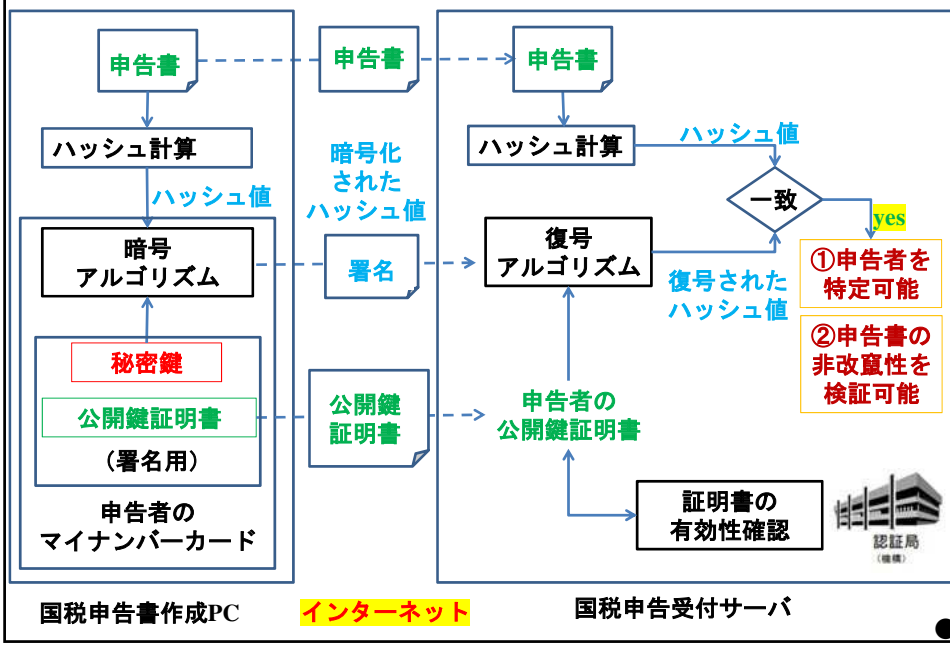
社会保障・税番号制度（2013年5月マイナンバー関連4法案成立）
行政を効率化し、国民の利便性を高め、
公平・公正な社会を実現する社会基盤

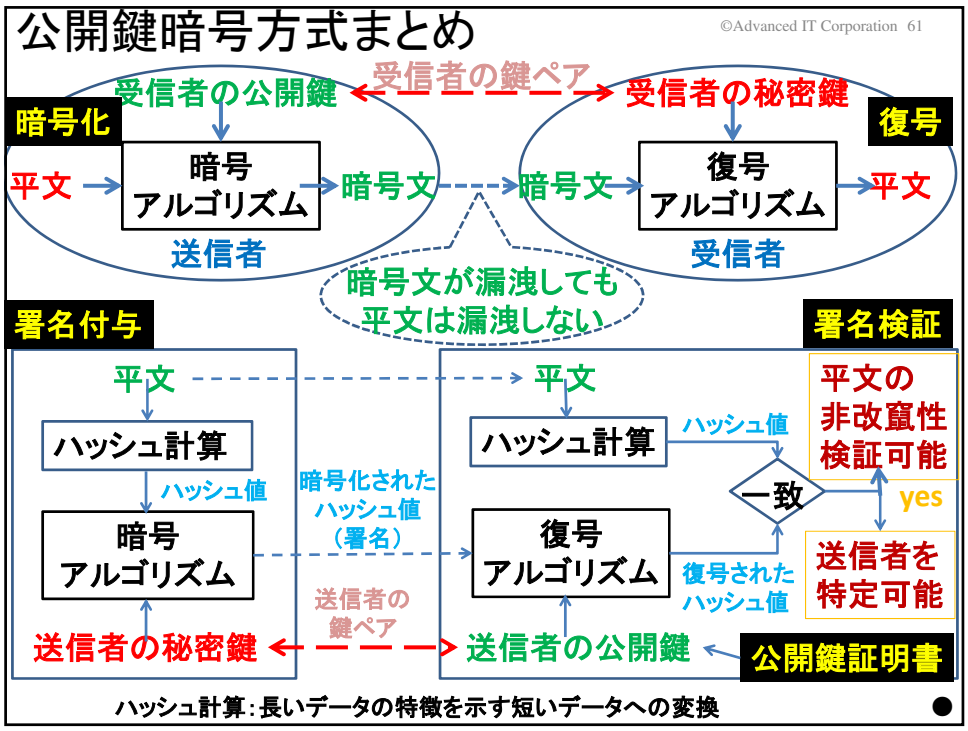
マイナンバーカード（2016年1月発行開始）
番号確認と身元確認が可能な唯一の書類
行政手続きのためのインターネット経由の本人確認基盤

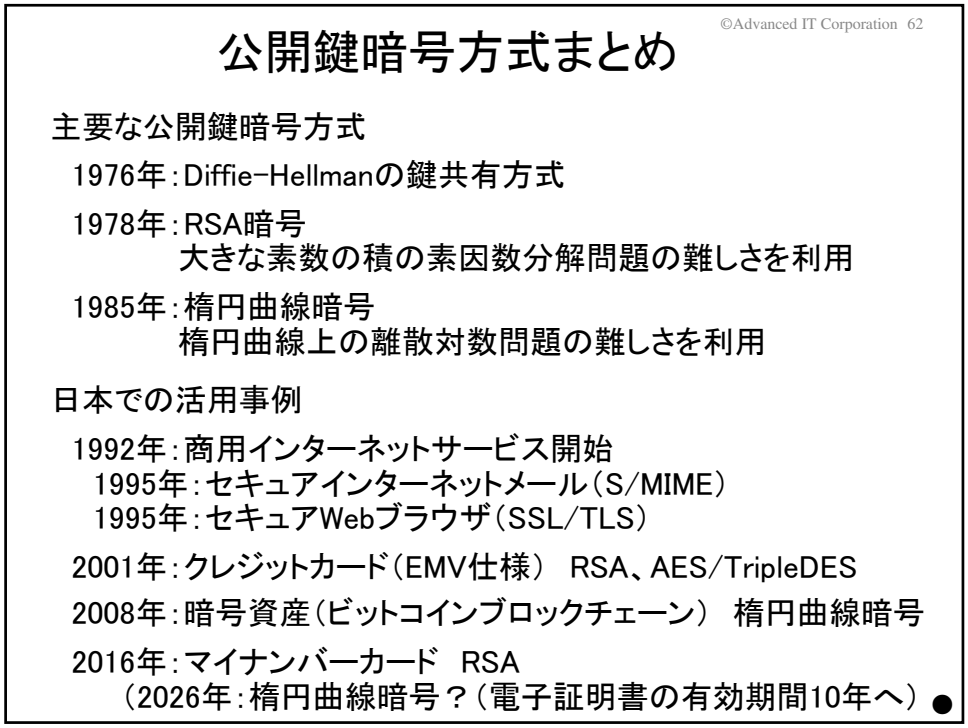
デジタルファースト法案（2019年5月成立）
地方自治体を含め、デジタル化、
インターネット経由の行政手続きの導入・普及の加速

健康保険証としての機能付加（2021年3月）
マイナンバーカードを健康保険証として利用可能

マイナンバーカードによる国税申告（e-Tax）




公開鍵暗号方式まとめ
©Advanced IT Corporation 61
受信者の鍵ペア
受信者の公開鍵
受信者の秘密鍵
暗号化
復号
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
受信者
暗号文が漏洩しても
平文は漏洩しない
署名付与
署名検証
平文
平文
ハッシュ計算
ハッシュ値
ハッシュ計算
ハッシュ値
平文の
非改竄性
検証可能
一致
yes
暗号化された
ハッシュ値
（署名）
暗号
アルゴリズム
復号
アルゴリズム
復号された
ハッシュ値
送信者を
特定可能
送信者の
鍵ペア
送信者の秘密鍵
送信者の公開鍵
公開鍵証明書
ハッシュ計算：長いデータの特徴を示す短いデータへの変換


©Advanced IT Corporation 62
公開鍵暗号方式まとめ
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
2008年：暗号資産（ビットコインブロックチェーン） 楕円曲線暗号
2016年：マイナンバーカード RSA
（2026年：楕円曲線暗号？（電子証明書の有効期間10年へ）

［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

●

余談

暗号資産（仮想通貨） の動向

現状　暗号資産の数：8884
　　資産総額：約230兆円
　　https://coinmarketcap.com/ja/all/views/all/ （2023年12月12日）
（日本の2023年度予算は、114兆円余り（一般会計の総額）

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

対策
　利用者の匿名性と共に確実な特定・追跡性が必要

➔SSVATF（安心・安全な暗号資産流通基盤）を提案中

社会・経済の健全な発展に資する
社会的責任を果たしうる暗号資産業界へ

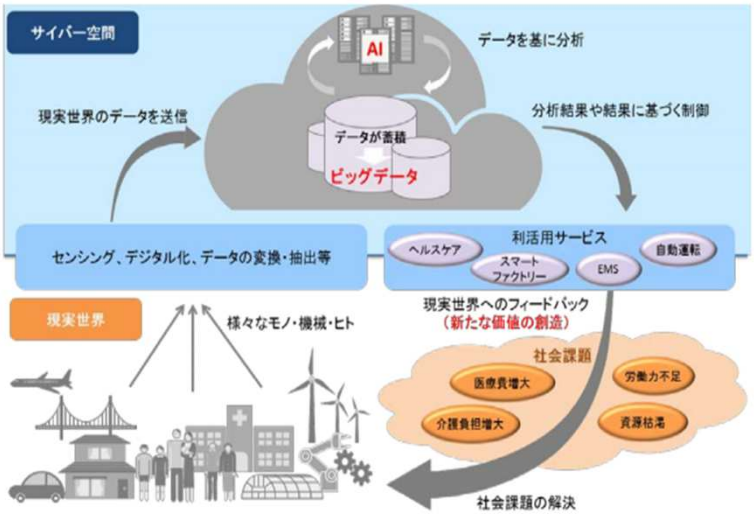
●

［７］新たな課題と対応状況（主要なトピック紹介）

(1)IoTデバイスの急速な活用・普及

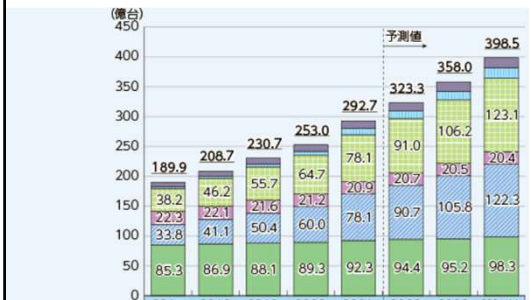
(2)量子コンピュータ実用化の可能性

(1)新たな課題と対応状況
データドリブン社会へ：IoTデバイスの活用
IoT：Internet of Thing



https://www.jnsa.org/seminar/nsf/2018/data/NSF2018_S1.pdf

IoTデバイスの急速な活用・普及



	2017	2018	2019	2020	2021	2022	2023	2024(年)
合計	189.9	208.7	230.7	253.0	292.7	323.3	358.0	398.5
自動車・宇宙航空	7.1	8.5	9.8	11.3	12.7	14.2	15.7	17.3
医療	3.3	4.0	5.1	6.5	10.7	12.5	14.6	17.2
産業用途	38.2	46.2	55.7	64.7	78.1	91.0	106.2	123.1
コンピューター	22.3	22.1	21.6	21.2	20.9	20.7	20.5	20.4
コンシューマー	33.8	41.1	50.4	60.0	78.1	90.7	105.8	122.3
通信	85.3	86.9	88.1	89.3	92.3	94.4	95.2	98.3

情報通信白書(令和4年版)
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nf3r1000.html

IoTデバイスの急増！

2021年 300億個程度
➔ 2024年 400億個程度へ

世界の人口
2020年 78億人程度
➔2040年 85億程度へ

国連人口基金(UNFPA)
「世界人口白書2023」
https://eleminist.com/article/2728?page=2

IoTデバイスのリスクと必要な対策

IoTデバイスがDDoS攻撃に参加させられるリスク
DDOS:Distributed Denial of Service
ボットネット(IoTデバイスで構成)による使用不能攻撃
2016年:KrebsOnSecurityサイトへの攻撃(60万台以上)
MIRAI ソースコード公開 亜種の氾濫 新種も次々と出現
booter/stresser(DDoS攻撃請負業者) $20から
➔ IoTデバイスがボットネットに組み込まれない対策

データドリブン社会を支えるIoTシステムが攻撃を受けるリスク
なりすましIoTデバイスによる偽データの送信
IoTデバイスが収集したデータの改ざん
(データに強く依存する社会への直接的な影響・被害)
➔ IoTデバイス、送信データの真正性を確認できる仕組み

➔ アクセス元、データ送信元のIoTデバイスを
特定・追跡できる仕組み

IoTデバイス向け軽量暗号

IoT向け暗号の必要性
- IoTデバイスへのアクセス制御：暗号技術による権限確認
- IoTデバイスの真正性：暗号技術によるIoTデバイスの認証
- 送信データの真正性：暗号技術による送信データの認証

IoT向け暗号の軽量性の必要性
- IoTデバイスの処理能力：十分なセキュリティ機能搭載が困難

性能指標	アプリケーションの例
回路規模 (消費電力, コスト)	RFID、低コストセンサー
消費電力量	医療機器、バッテリ駆動デバイス
レイテンシ（リアルタイム性能）	メモリ暗号化、車載機器、産業向けI/Oデバイス制御
メモリサイズ (ROM/RAM)	家電機器、センサー、車載機器

https://www.cryptrec.go.jp/symposium/20171218_cryptrec-lw.pdf

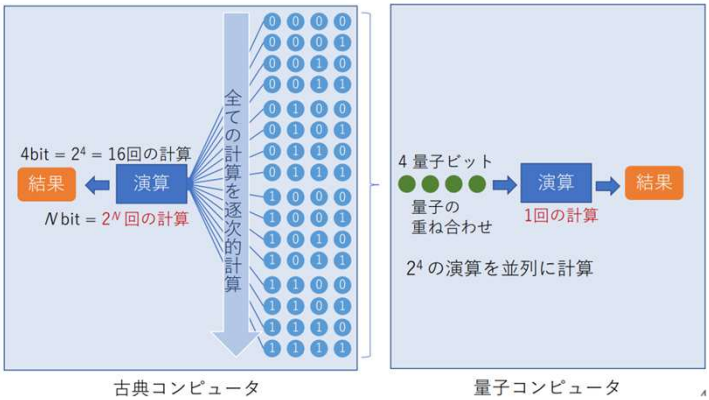
軽量暗号の開発・標準化
- 国際：ISO 29192（Lightweight cryptography）2012～
  - ➔米国NISTも 2015 年より軽量暗号の標準化の検討を開始、2023年2月、最終候補としてAsconファミリを選定）
- 日本：CRYPTREC 暗号技術ガイドライン（軽量暗号）2017/03
  - ➔2023年度更新予定

(2) 新たな課題と対応状況
量子コンピュータの実用化間近？

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？



https://www.soumu.go.jp/main_content/000655118.pdf

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による計算量減少の可能性

2^{128}（10 進数で 38 桁程度）➔2^{64}（10 進数で 19 桁程度）

➔サイモンのアルゴリズム　計算量減少の可能性

2^{128}（10 進数で 38 桁程度）➔128程度

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）　計算量減少の可能性

2^{2048}（10 進数で 76桁程度）➔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）

2022年7月：標準技術の候補として4つの暗号アルゴリズムを選定

日本：CRYPTRECにて2019年6月より検討開始

2023年3月：暗号技術ガイドライン（耐量子計算機暗号）

[7]新たな課題と対応状況
まとめ

技術の発展による、新たなサービスの出現
➔新たな課題（犯罪者/悪意のある人が活用）

(1)IoTデバイスの急速な活用・普及

技術の発展の、既存サービスへの影響
➔暗号技術の破綻

(2)量子コンピュータ実用化の可能性

終わりに

＜暗号技術の利用＞
[1]古代暗号～[3]近代暗号
　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]～[6]現代暗号
　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に利用
[7]新たな課題と対応状況
　技術の発展、新たなサービスによる課題への対応継続中

＜暗号技術と社会の相互作用＞
（1）暗号技術は、時代時代の社会の要請により開発され発展！
（2）暗号技術の発展が、時代時代の社会を形作ってきた！

 75

終

ご清聴、ありがとうございました。