# 暗号化


**セカンドライフファクトリー**
**わいわいサロン（いつまでも勉強しよう！）**

208年4月15日

# 暗号化の利用

## 古典暗号から現代暗号へ



### 古典暗号の世界

暗号の歴史は人類の歴史と同じ長さ

軍事外交目的の非公開技術

参加者限定の1対1通信を前提

文字の置換を中心とする変換処理


### 現代暗号の世界

開かれた研究は1970年代から

プライバシー保護という動機付け

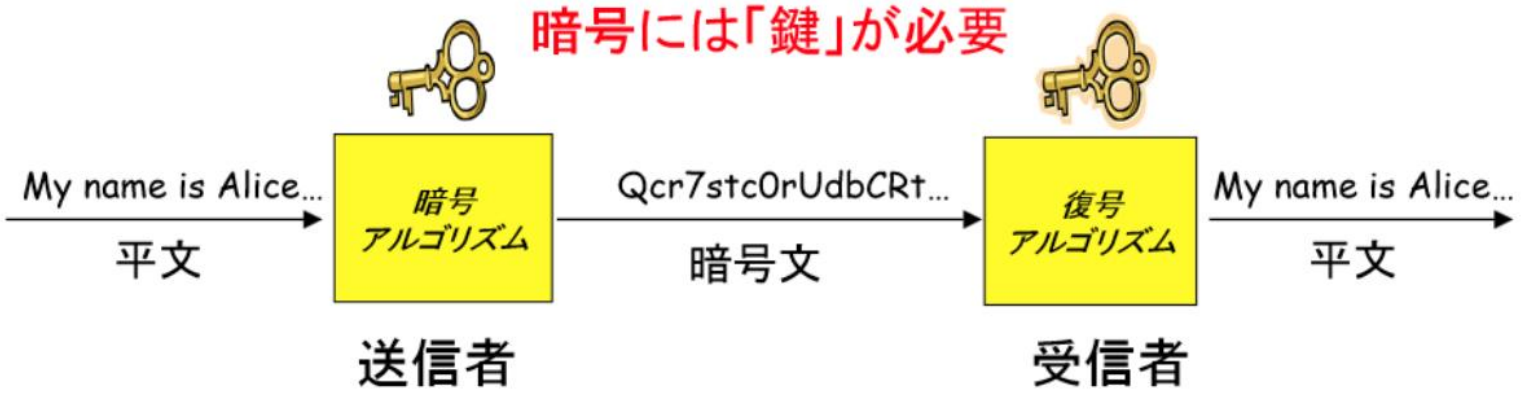
不特定多数が参加するネットワーク指向

ディジタル信号の変換処理

# 暗号化とは何か？

## 暗号技術でできること

- 秘匿　（Confidentiality）　盗聴の防止
- 認証　（Authentication）　なりすまし防止
- 完全性（Integrity）　情報の偽造防止



# 暗号化とは何か？

https://www.jp.websecurity.symantec.com/welcome/pdf/wp_encryption_history.pdf

現存する最古の暗号は、紀元前 3000 年頃の石碑に描かれているヒエログリフ（古代エジプトで使われた象形文字）であるとされています。ヒエログリフは長い間解読不能な暗号とされてきましたが、19 世紀にロゼッタ・ストーンの研究が大幅に進み、以降ヒエログラフ解読のきっかけになりました。

紀元前 6 世紀頃、古代ギリシャの都市国家・スパルタでは「スキュタレー暗号」が用いられました。この方式では、あらかじめある太さの棒（スキュタレー：図1）を持った暗号文の送り手がその棒に革紐を巻きつけて棒に沿って文字を書き、その革紐だけを受け手に送るというものです。受け手が同じ太さの棒を持っている場合は、革紐を巻きつけると解読できるという暗号の仕組みになっています。

このように、文字を読む順番を並べ替えることによって暗号化する方式を「転置式暗号方式」といいます。

# 暗号化とは何か？

紀元前１世紀に登場したシーザー暗号は、ユリウス・カエサル（英語読み：ジュリウス・シーザー）が頻繁に利用したことから名づけられ、暗号史で登場する幾多の方式の中でもとりわけ有名な暗号方式です。

シーザー暗号は、元の文章のアルファベットをある数だけずらして暗号化するもので、アルファベットを3文字ずらすということをあらかじめ送り手と受け手の間で決めておくものです。

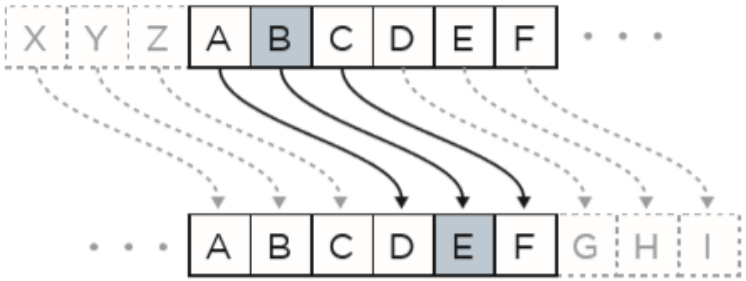


図2

シーザー暗号はその文字をずらすことから、「シフト暗号」とも言われ、シフト暗号をアルファベットで用いる場合最大 26 パターン試せば暗号が解読されてしまいますが、これを、均等にずらすのではなく文字をランダムに並べ替えれば、そのパターンは大きく増加（26×25×24×・・・・＝4000000000000000000000000000 通り!）し、解読は飛躍的に困難になります。

| | |
|---|---|
| 平文(暗号化されていない文)文字 | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| 暗号文字 | SMKRATNGQJUDZLPVYOCWIBXFEH |

# 暗号化とは何か？

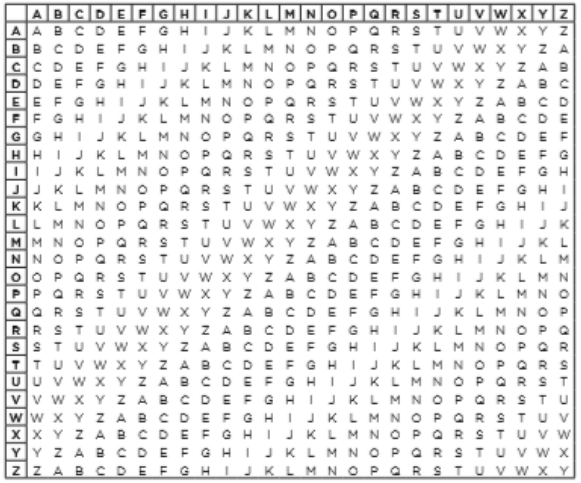
**ヴィジュネル暗号**

女王メアリの用いた暗号など、１つの文字ごとに文字を変えるパターンが１個の単一換字式暗号は解読されるようになります。また「ノーメンクラター」は、難点があり、膨大なコードブックの準備と、コードブックの共有が暗号利用者の悩みの種でした。この「鍵の受け渡し」に関する課題は、中世だけでなく暗号技術が進歩した近代以降の暗号においても利用者にとって課題になっています。

15 世紀になると、レオン・バッティスタ・アルベルティが、二つ以上の暗号アルファベットを使う「多表式」の暗号の原型を思いつき、その後脈々と引き継がれて発展を遂げました。16 世紀にはブレーズ・ド・ヴィジュネルが多表式の最終的な形として強力な暗号を考案したことから、ヴィジュネル暗号と呼ばれます。

ヴィジュネル暗号は、ヴィジュネル方陣（図 4）と呼ばれる表を用いる方式です。たとえば、GOLDMEDALIST という文章を OLYMPIC という鍵で暗号化する場合、原文の文字を表の上端に当てはめ、鍵の文字を表の左端に当てはめて交差するアルファベットが暗号文字ということになります。

| | |
|---|---|
| 平文 | GOLDMEDALIST |
| 鍵 | OLYMPICOLYMP |
| 暗号文 | UZJPBMFOWGEI |



# インターネット上で使用される暗号化（SSL)-01

**RSA暗号**は、インターネットでも広く利用されている話題の暗号です。
http://www.maitou.gr.jp/rsa/rsa10.php
この暗号をはじめとする現代の暗号は、かつて戦時中に一部組織でのみ使用われた暗号とは異なり、情報セキュリティを確保するための基盤技術として、情報ネットワーク社会に生きる我々に安心を与えてくれるものです。無意識のうちに利用しており、既にこの社会にとって必要不可欠なものとなっています。

共通鍵暗号→公開鍵暗号
1976年、2000年もの間、仕方がないこと考えられてきたこの問題を解決する、暗号界の革命とも言える概念が Diffie と Hellman という二人の研究者によって発表されました。
この暗号の概念では、A と B という2つの鍵を使用します。一方の鍵 ( A ) を使って暗号化した暗号文は、なんと暗号化に使った鍵 ( A ) では復号することができず、もう一方の鍵 ( B ) でのみ復号できるというのです。また、逆にもう一方の鍵 ( B ) で暗号化した暗号文も、もう一方の鍵 ( A ) でしか復号できないという考え方なのです。

**電子署名**
逆に自分だけの秘密の鍵 ( B ) を使って暗号化した場合です。そこで、ある文書を本当に自分が書いたものだとか、自分は本当に自分であることなどを周囲に証明（認証）したい時には、自分だけの秘密の鍵 ( B ) を使って暗号化し、この暗号文を公開します。周囲の人間は、公開されている鍵 ( A ) を使ってその暗号文を正しく復号できるか確かめ、それができれば本当に自分が書いたものだと証明されるのです。なぜなら、公開している鍵 ( A ) で復号できる暗号文を作れるのは、対応する秘密の鍵 ( B ) を持った本人だけだからです。これにより、暗号を印鑑のように使用することができます。

# インターネット上で使用される暗号化（SSL)-02

1．暗号化（SSL証明書） https://www.slogical.co.jp/ssl/
1）SSL証明書とは
SSL（Secure Sockets Layer）とは、インターネット上の通信を暗号化するための仕組み。
SSL証明書とは、SSL通信を行うサーバー側への設置が必要となる、認証局（CA、シマンテックやジオトラストなど）から発行される電子証明書です。

暗号化で使われる共通鍵をサーバーとクライアントが受け渡しする際、その信頼性を担保するためにSSL証明書が必要となり、次のような情報が含まれる。
- Webサイト運営者の組織情報
- 暗号化で使われる公開鍵
- SSL証明書の有効期限
- その他拡張情報
- 認証局による署名

# インターネット上で使用される暗号化（SSL)-03

① SSL証明書の種類
SSL証明書には、下記の3種類がある。
•DV（ドメイン認証）：組織実在性は審査せずに、ドメイン管理権限の確認のみで発行される
•OV（実在証明、企業認証）：組織実在性を審査して、電話確認（省略される場合もあり）を経てから発行される
•EV（EV証明書）：OV証明書よりも厳格な審査が行われる、ブラウザのアドレスバーに緑色で組織名を表示
※クライアント（PCやスマホなど）から信頼されていない認証局から発行された証明書（自己署名の証明書（＝オレオレ証明書）を含む）は、多くのブラウザで赤いバツマークが表示される。

# インターネット上で使用される暗号化（SSL)-04

② SSLのバージョン
SSLには以下のバージョンがあり、現在安全に利用できるものはTLS（Transport Layer Security）通信のみだが、SSLという名称が広く普及しているため、現在も、TLS1.0以降の通信がSSL通信と呼ばれることも多く、サーバー側に必要となる証明書も一般的には「SSL証明書」と呼ばれている。
•SSL 1.0　ネットスケープコミュニケーションズ社により設計される。脆弱性が見つかり、実用はされなかった。
•SSL 2.0　同社により再設計される。その後脆弱性が見つかり、現在は多くのブラウザがデフォルト設定では無効としている。
•SSL 3.0　同社により再設計される。脆弱性（POODLE）が発見されたため、現在は利用が推奨されない。
•TLS 1.0　IETFより公開されたバージョン。現在も利用可能。
•TLS 1.1　上記の改良版。共通鍵暗号としてAESも利用可能となる。
•TLS 1.2　上記の改良版。ハッシュアルゴリズムにSHA-256が追加される。
•TLS 1.3　策定中。HTTP/2の仕様を満たすもの。
Apacheであれば、例えば次のように設定してWebサーバーが提供するSSLのバージョンを定義する。

SSLProtocol all -SSLv2 -SSLv3

※将来的に、TLSの特定バージョンに脆弱性が発見された場合には、
そのバージョンをサーバー側で提供しないように設定変更する必要がある。

# インターネット上で使用される暗号化（SSL)-05

③ 暗号・鍵交換・改ざん検知のアルゴリズム
SSL通信のデータ暗号化は共通鍵暗号方式（AES・Camelliaなど）で行われるが、その暗号化で利用される共通鍵を、公開鍵暗号に基づく認証（RSA、DH、DSAなど）で事前に安全に交換します。
また、あわせて改ざん検知（SHA1、SHA-256などを利用）も行われる。
Apacheであれば、例えば次のように設定してWebサーバーが提供する暗号アルゴリズムのリストを定義する。クライアント（Webブラウザ）は、サーバーが提供できるアルゴリズム一覧の中から自身が使えるアルゴリズムを選択して、SSLのセッションが開始される。
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:.....

※将来的に、特定のアルゴリズムに脆弱性が発見された場合には、
そのアルゴリズムをサーバー側で提供しないように設定変更する必要がある。
※最近のIntelやAMDのCPUはAES-NIというAES暗号専用のハードウエア処理に対応していて、
また、ARMv8のCPUでもAES専用処理が可能なため、サーバー側でAESの優先度を上げたほうが効率がよいと思われる。
※現在策定中のTLS1.3ではChaCha20が採用される可能性もあるので、
SSLCipherSuiteの設定は、運用しながら時々見直しの必要がある。
常時SSL: 前述のとおり、SSL/TLS通信には改ざん防止機能もあるため、無線でのネット接続が多く行われるようになった現在、暗号化のみならず改ざん防止の点からもSSLの必要性が高まっている。
そのため、個人情報が送受信されるWEBページのみではなく、
Webサイト全体をSSL通信に対応させる「常時SSL」も実装され始めていて、
GoogleによるSEOの評価も、SSL対応しているサイトのほうが、若干ですが高い。
Apache で mod_headers が有効であれば、次のように設定して常時SSLに対応可能。
（HSTSを有効にして、httpへのアクセスをhttpsに強制リダイレクトする）
Header add Strict-Transport-Security "max-age=15768000"

# インターネット上で使用される暗号化（SSL)-06

④ どのSSL証明書を選べばよいのか？

暗号強度は、前述のSSLバージョンや暗号アルゴリズムで決定されるため、SSL証明書そのものによって盗聴・改ざんに強いSSL通信が担保されるわけではない。一般的には、次のような基準で選ばれる方が多い。

- httpsの通信ができればよい：RapidSSL
- サイトシールが必要：ジオトラスト QuickSSL Premium
- ECサイトなど企業認証を行いたい：トゥルービジネスID
- シマンテックのサイトシールで離脱率を抑えたい：シマンテック Secure Site
- EV証明書を使い、ブラウザアドレスバーに企業名を表示したい：シマンテック Secure Site with EV
- 迅速な企業審査を行いたい：サイバートラスト SureServer

# インターネット上で使用される暗号化（SSL)-07

2) SSL証明書の購入手順

1.キーペアとCSR（Certificate Signing Request）を作成する。
OpenSSL、Plesk、IISマネージャなどを使ってキーペアとCSRを作成する。

2.お申し込みﾌｫｰﾑから、CSRを送信して申し込む。申込み時にはCSRが必要で、ｷｰﾍﾟｱは必要ない。

3.入金する。銀行振込もしくはクレジットカード（PayPal）決済

4.認証局による、SSL証明書発行のための審査が行われる。
ドメイン認証型SSL（RapidSSL、QuickSSL Premiumなど）の場合
□承認メール送付先アドレス宛に届く承認URLをクリックする。
□承認URLのクリック後、認証局のクローラーが、WebサイトTOPページのコンテンツチェックを行う。
□その後、SSL証明書が即時発行されます。
□ただし、TOPページやドメイン名などが、即時発行の基準を満たさない場合は、認証局による
手動審　査後の発行となる。

5.SSL証明書が発行される
認証局からのメールでSSL証明書が送付されます。

6.SSL証明書をWebサーバーにインストールする。

※キーペアとSSL証明書がペアになりますため、手順1.で作成したキーペアは紛失しないようにバックアップを取る。

# 暗号化（SSL)とは？-01

日経WORKS：http://itpro.nikkeibp.co.jp/article/COLUMN/20071012/284384/

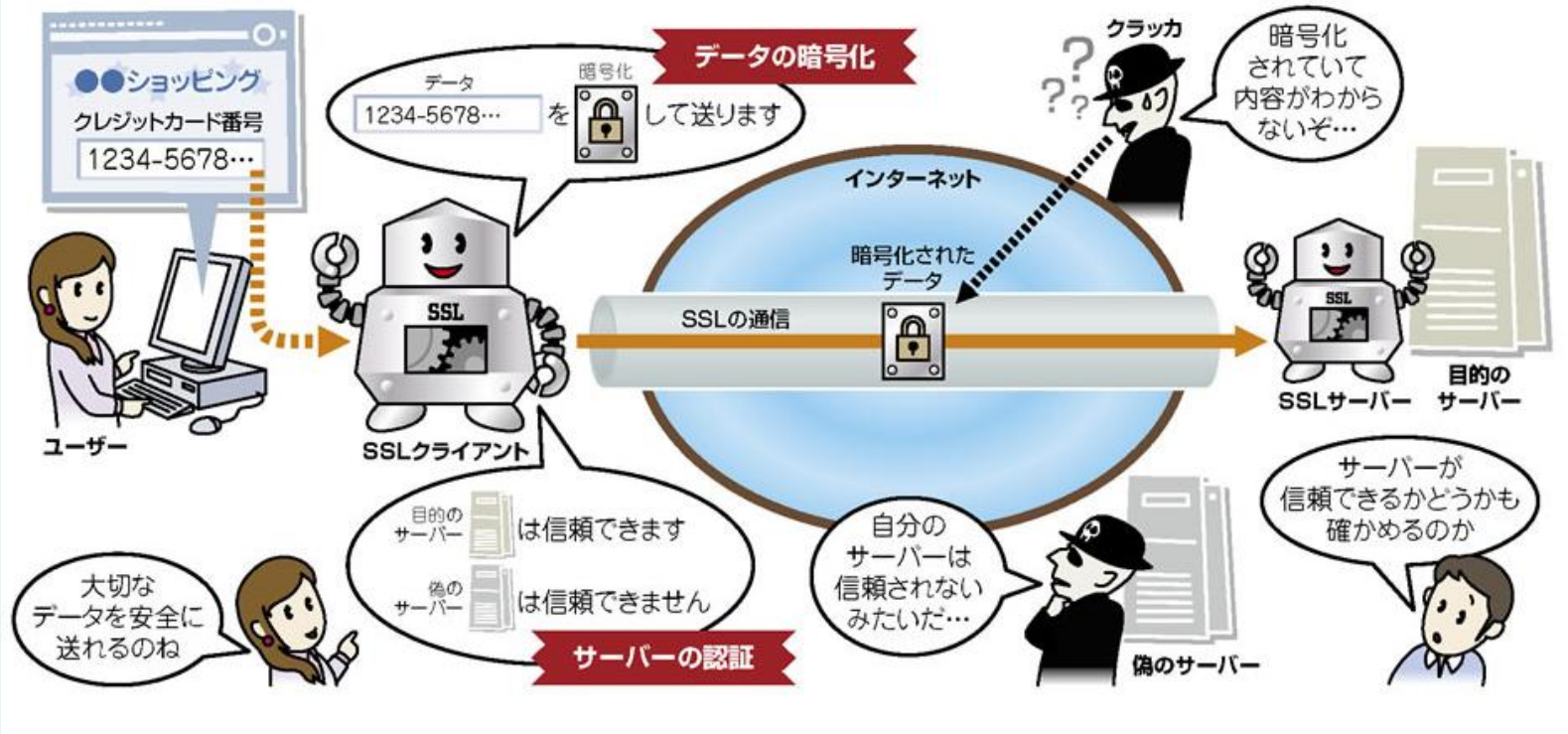



図1-1●SSLはインターネット上でデータを安全にやりとりするプロトコル
接続相手のサーバーが信頼できるかどうかを確かめたうえで，データを暗号化してやりとりする。クレジットカード情報などをやりとりするWebショッピングには欠かせない機能だ。

# 暗号化（SSL)とは？-02

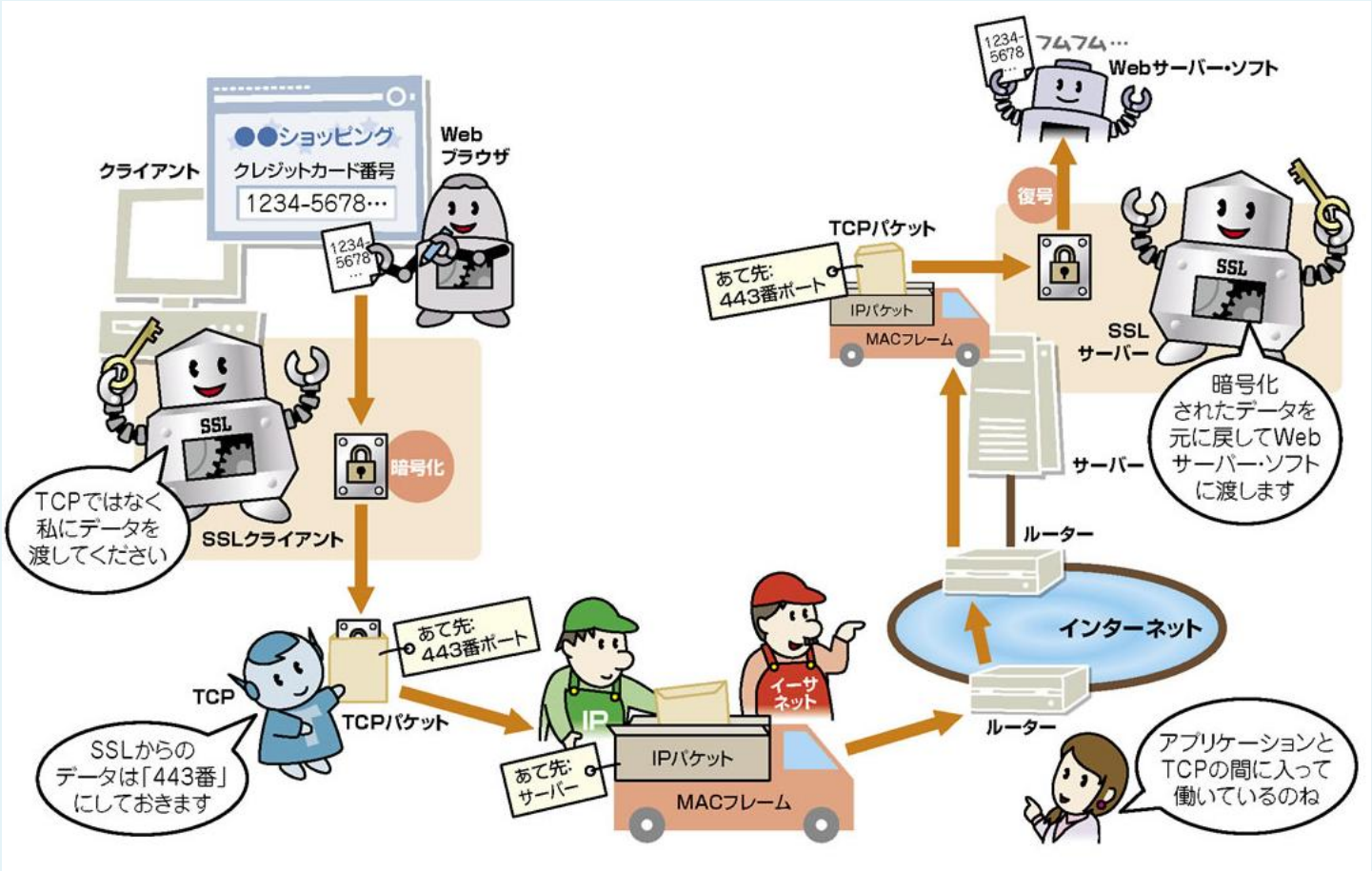



図1-2●TCPとアプリケーションの間で動作する
アプリケーションがTCPにデータを渡すところにSSLが介在して，データを暗号化する。

# 暗号化（SSL)とは？-03

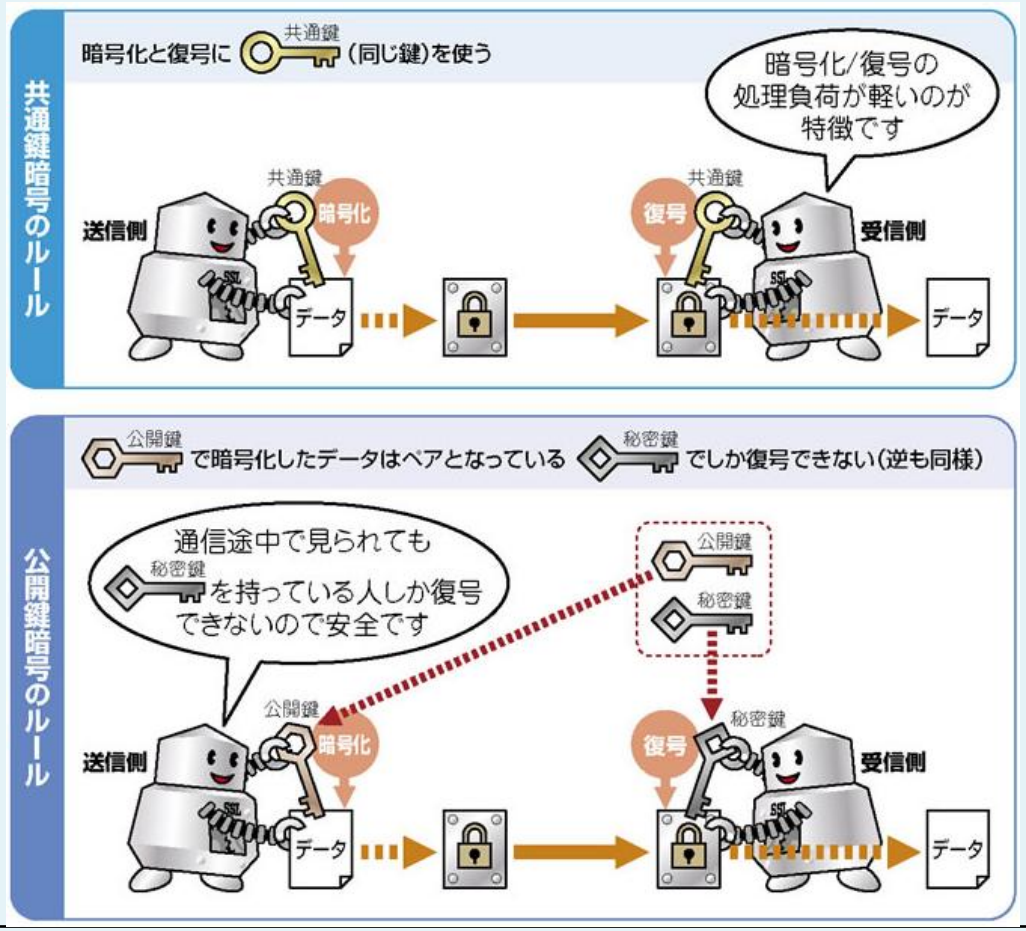



図2-1●SSLでは二つの暗号方式を使う
SSLは，共通鍵暗号方式と公開鍵暗号方式のそれぞれのメリットを組み合わせて実現する。

# 暗号化（SSL)とは？-04

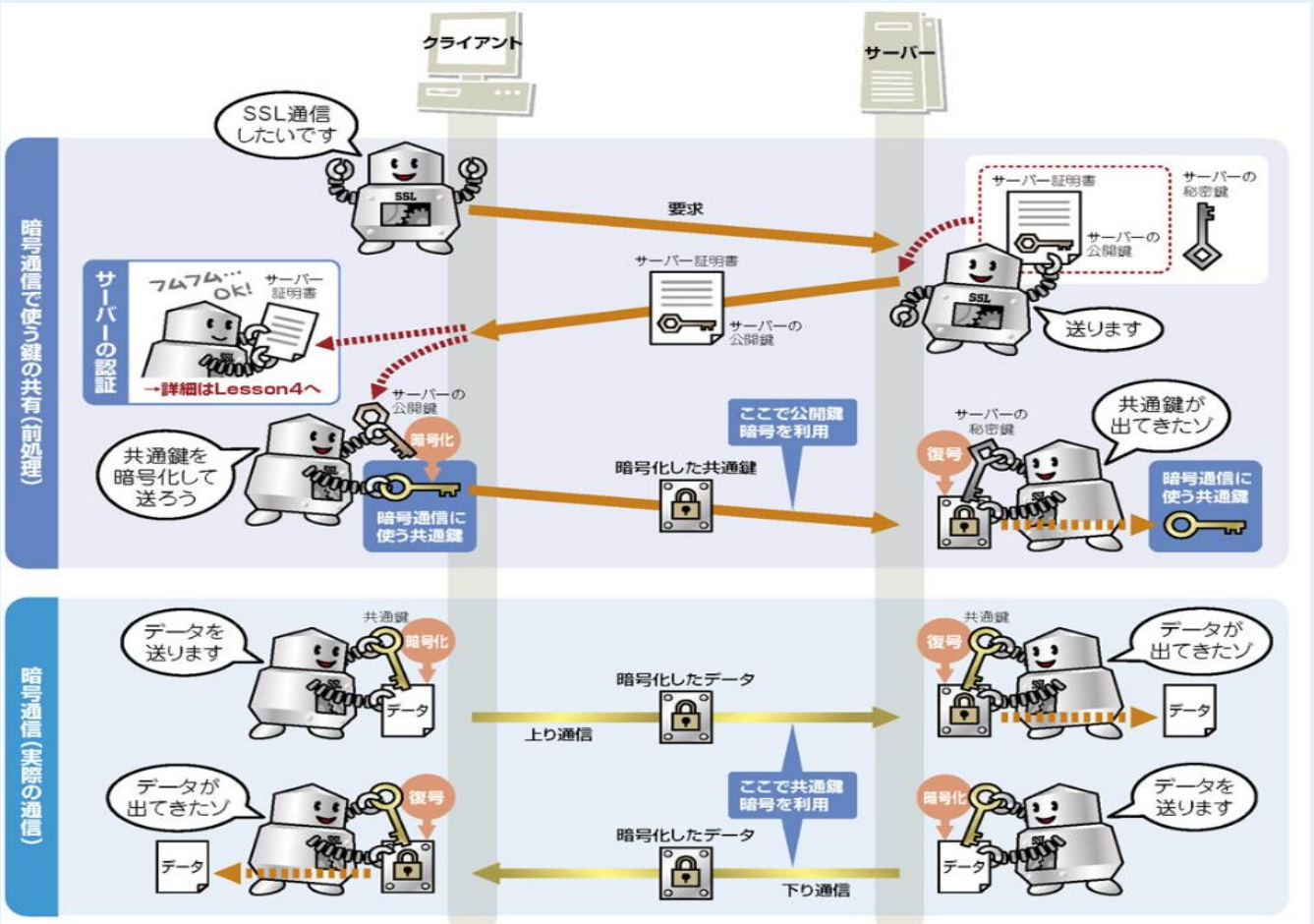



図2-2●SSL通信の概要
公開鍵暗号方式を使って「暗号通信で使う共通鍵」を安全に共有し，共有した共通鍵を使って暗号通信をする。

# 暗号

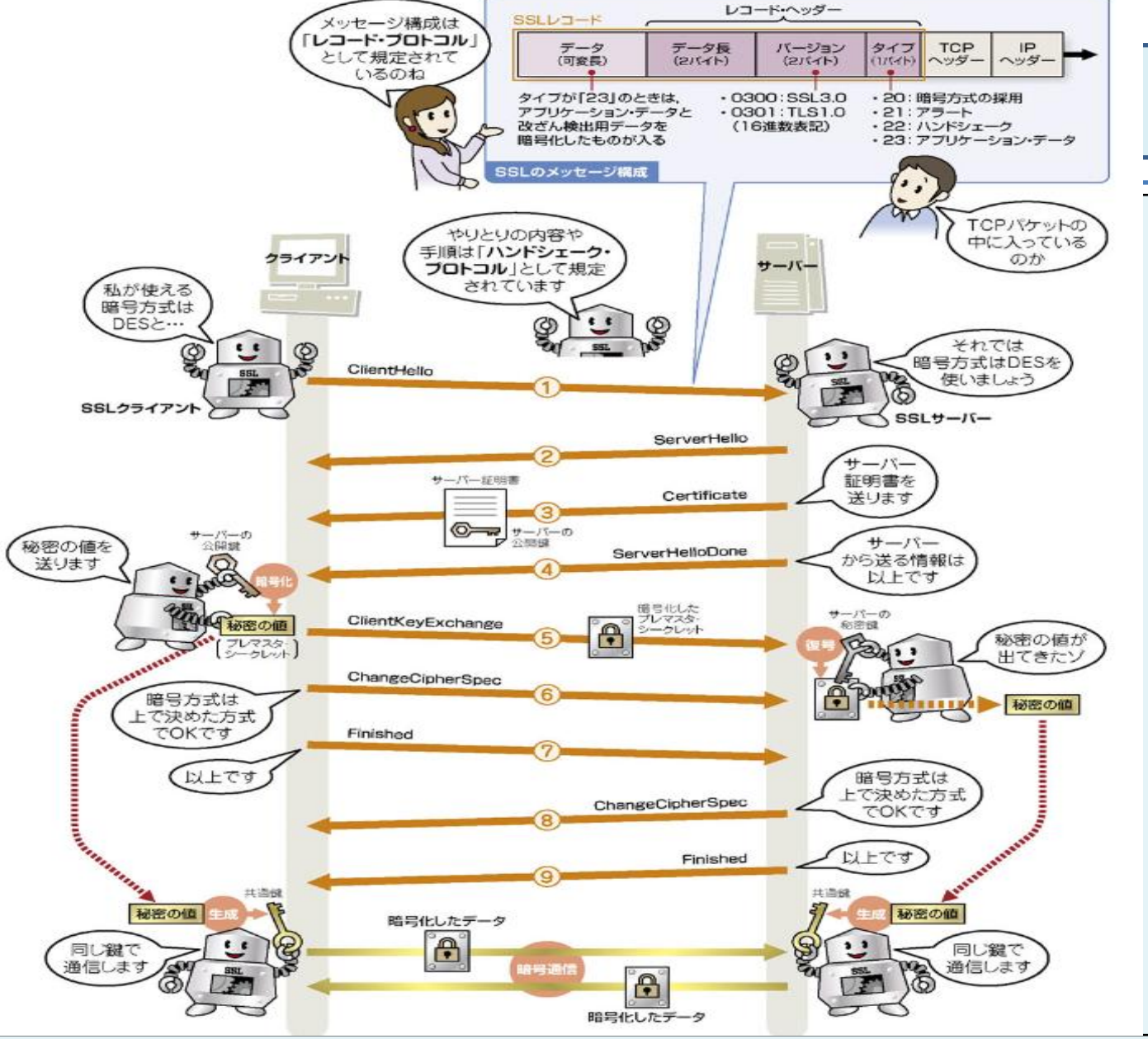



図3-1●SSLのメッセージ構成とやりとりの内容
メッセージの構成は「レコード・プロトコル」として，やりとりの手順は「ハンドシェーク・プロトコル」として規定されている。

# 暗号化（SSL)とは？-06

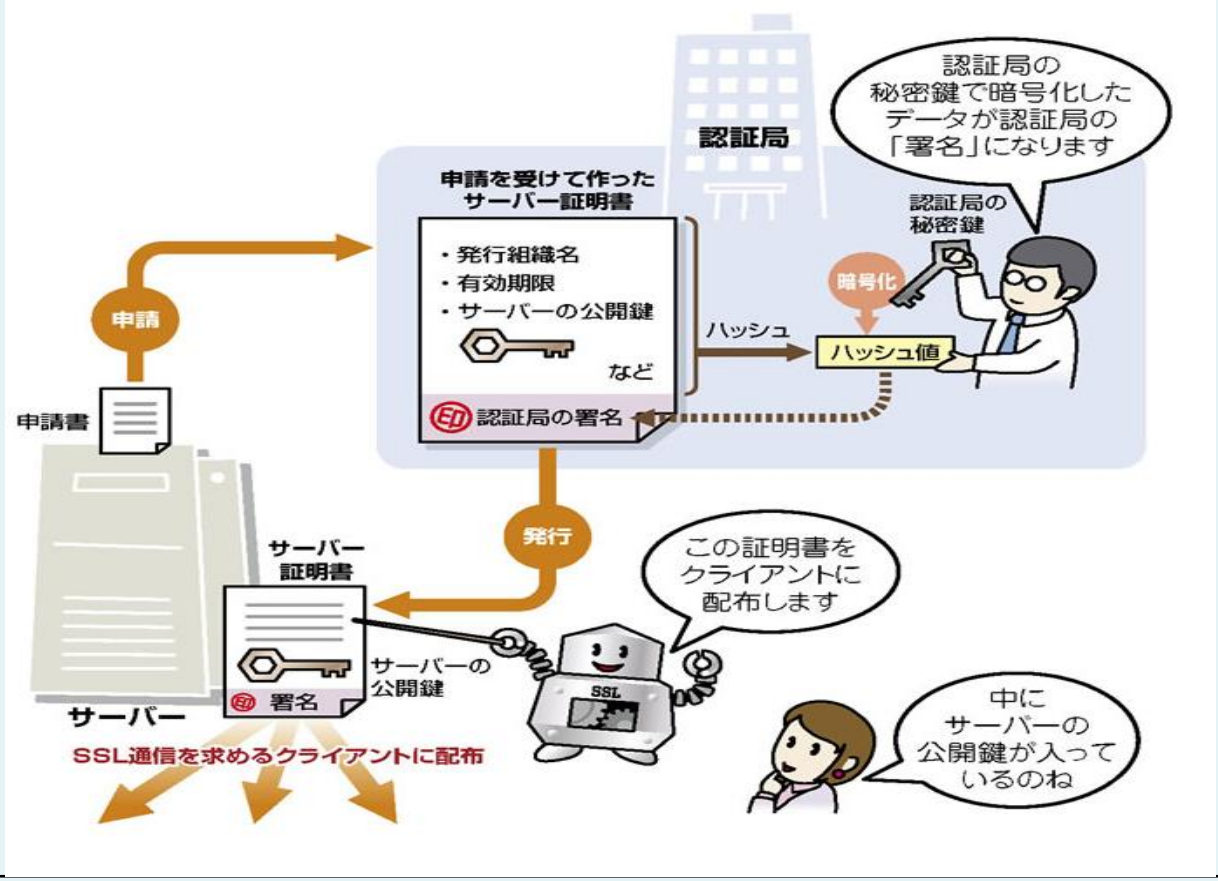



図4-1●「サーバー証明書」と「署名」とは？
サーバー証明書は，サーバーの各種情報が書き込まれた情報で，サーバーの公開鍵が含まれている。サーバー証明書には，認証局の署名（証明書を認証局の秘密鍵で暗号化したデータ）が付いている。

# 暗号化（SSL)とは？-07

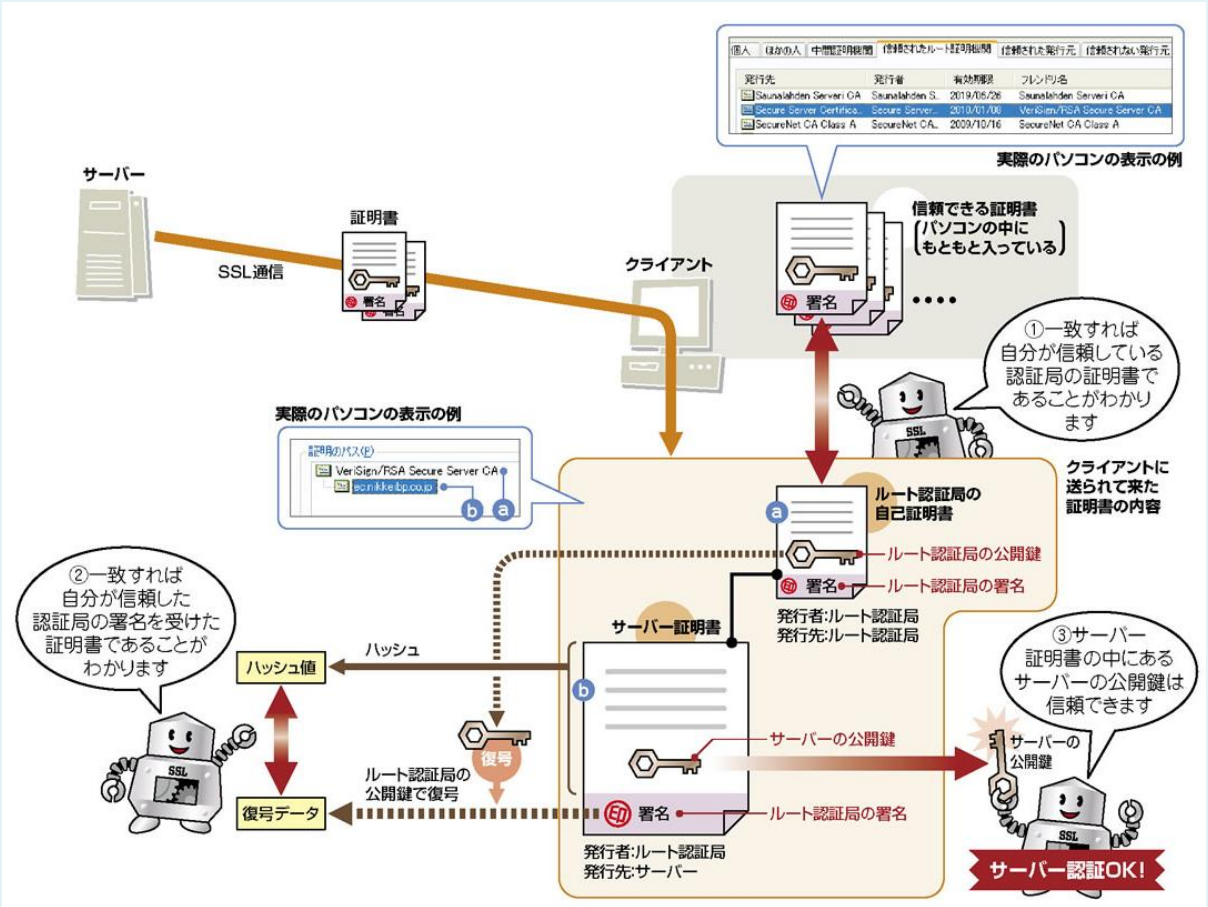



図4-2●サーバー認証のしくみ
クライアントには，「サーバー証明書」と「ルート認証局の自己証明書」が一緒に送られてくる。パソコンの中にもともと入っている証明書を使ってルート認証局の自己証明書の正当性をチェックし，その後，サーバー証明書の正当性をチェックする。

# 公開鍵？　素因数分解の困難さを利用

RSA暗号
2つの素数(P,Q(法＝PxQ))とべき乗世界
**n ×（P-1とQ-1の最小公倍数）+1**　で元の数値に戻る。
右図はP=3,Q=11(法=33)の例
公開鍵=X、秘密鍵=Y
（公開時はXとPxQを公開）
注：公開されたPxQからP,Qを求めることは現在のコンピュータでは時間的に不可能

$(A^X)^Y = A^{\{n \times (P-1) \times (Q-1)+1\}}$
であるので

$X \times Y = n \times (P-1) \times (Q-1) + 1$
↓
$7 \times Y = 1 \times (3-1) \times (11-1) + 1$
↓
$Y = (1 \times 2 \times 10 + 1) \div 7 = 3$

注)
①P,Qを知らなければ秘密鍵は得られない
②XはYが整数になるように選ぶ必要がある。

X　べき乗数　Y

| この世界の数 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 8 | 16 | 32 | 31 | 29 | 25 | 17 | 1 | 2 | 4 | 8 | 16 | 32 | 31 | 29 | 25 | 17 | 1 | 2 |
| 3 | 3 | 9 | 27 | 15 | 12 | 3 | 9 | 27 | 15 | 12 | 3 | 9 | 27 | 15 | 12 | 3 | 9 | 27 | 15 | 12 | 3 |
| 4 | 4 | 16 | 31 | 25 | 1 | 4 | 16 | 31 | 25 | 1 | 4 | 16 | 31 | 25 | 1 | 4 | 16 | 31 | 25 | 1 | 4 |
| 5 | 5 | 25 | 26 | 31 | 23 | 16 | 14 | 4 | 20 | 1 | 5 | 25 | 26 | 31 | 23 | 16 | 14 | 4 | 20 | 1 | 5 |
| 6 | 6 | 3 | 18 | 9 | 21 | 27 | 30 | 15 | 24 | 12 | 6 | 3 | 18 | 9 | 21 | 27 | 30 | 15 | 24 | 12 | 6 |
| 7 | 7 | 16 | 13 | 25 | 10 | 4 | 28 | 31 | 19 | 1 | 7 | 16 | 13 | 25 | 10 | 4 | 28 | 31 | 19 | 1 | 7 |
| 8 | 8 | 31 | 17 | 4 | 32 | 25 | 2 | 16 | 29 | 1 | 8 | 31 | 17 | 4 | 32 | 25 | 2 | 16 | 29 | 1 | 8 |
| 9 | 9 | 15 | 3 | 27 | 12 | 9 | 15 | 3 | 27 | 12 | 9 | 15 | 3 | 27 | 12 | 9 | 15 | 3 | 27 | 12 | 9 |
| 10 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 |
| 11 | 11 | 22 | 11 | 22 | 11 | 22 | 11 | 22 | 11 | 22 | 11 | 22 | 11 | 22 | 11 | 22 | 11 | 22 | 11 | 22 | 11 |
| 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 |
| 13 | 13 | 4 | 19 | 16 | 10 | 31 | 7 | 25 | 28 | 1 | 13 | 4 | 19 | 16 | 10 | 31 | 7 | 25 | 28 | 1 | 13 |
| 14 | 14 | 31 | 5 | 4 | 23 | 25 | 20 | 16 | 26 | 1 | 14 | 31 | 5 | 4 | 23 | 25 | 20 | 16 | 26 | 1 | 14 |
| 15 | 15 | 27 | 9 | 3 | 12 | 15 | 27 | 9 | 3 | 12 | 15 | 27 | 9 | 3 | 12 | 15 | 27 | 9 | 3 | 12 | 15 |
| 16 | 16 | 25 | 4 | 31 | 1 | 16 | 25 | 4 | 31 | 1 | 16 | 25 | 4 | 31 | 1 | 16 | 25 | 4 | 31 | 1 | 16 |
| 17 | 17 | 25 | 29 | 31 | 32 | 16 | 8 | 4 | 2 | 1 | 17 | 25 | 29 | 31 | 32 | 16 | 8 | 4 | 2 | 1 | 17 |
| 18 | 18 | 27 | 24 | 3 | 21 | 15 | 6 | 9 | 30 | 12 | 18 | 27 | 24 | 3 | 21 | 15 | 6 | 9 | 30 | 12 | 18 |
| 19 | 19 | 31 | 28 | 4 | 10 | 25 | 13 | 16 | 7 | 1 | 19 | 31 | 28 | 4 | 10 | 25 | 13 | 16 | 7 | 1 | 19 |
| 20 | 20 | 4 | 14 | 16 | 23 | 31 | 26 | 25 | 5 | 1 | 20 | 4 | 14 | 16 | 23 | 31 | 26 | 25 | 5 | 1 | 20 |
| 21 | 21 | 12 | 21 | 12 | 21 | 12 | 21 | 12 | 21 | 12 | 21 | 12 | 21 | 12 | 21 | 12 | 21 | 12 | 21 | 12 | 21 |
| 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 |
| 23 | 23 | 1 | 23 | 1 | 23 | 1 | 23 | 1 | 23 | 1 | 23 | 1 | 23 | 1 | 23 | 1 | 23 | 1 | 23 | 1 | 23 |
| 24 | 24 | 15 | 30 | 27 | 21 | 9 | 18 | 3 | 6 | 12 | 24 | 15 | 30 | 27 | 21 | 9 | 18 | 3 | 6 | 12 | 24 |
| 25 | 25 | 31 | 16 | 4 | 1 | 25 | 31 | 16 | 4 | 1 | 25 | 31 | 16 | 4 | 1 | 25 | 31 | 16 | 4 | 1 | 25 |
| 26 | 26 | 16 | 20 | 25 | 23 | 4 | 5 | 31 | 14 | 1 | 26 | 16 | 20 | 25 | 23 | 4 | 5 | 31 | 14 | 1 | 26 |
| 27 | 27 | 3 | 15 | 9 | 12 | 27 | 3 | 15 | 9 | 12 | 27 | 3 | 15 | 9 | 12 | 27 | 3 | 15 | 9 | 12 | 27 |
| 28 | 28 | 25 | 7 | 31 | 10 | 16 | 19 | 4 | 13 | 1 | 28 | 25 | 7 | 31 | 10 | 16 | 19 | 4 | 13 | 1 | 28 |
| 29 | 29 | 16 | 2 | 25 | 32 | 4 | 17 | 31 | 8 | 1 | 29 | 16 | 2 | 25 | 32 | 4 | 17 | 31 | 8 | 1 | 29 |
| 30 | 30 | 9 | 6 | 15 | 21 | 3 | 24 | 27 | 18 | 12 | 30 | 9 | 6 | 15 | 21 | 3 | 24 | 27 | 18 | 12 | 30 |
| 31 | 31 | 4 | 25 | 16 | 1 | 31 | 4 | 25 | 16 | 1 | 31 | 4 | 25 | 16 | 1 | 31 | 4 | 25 | 16 | 1 | 31 |
| 32 | 32 | 1 | 32 | 1 | 32 | 1 | 32 | 1 | 32 | 1 | 32 | 1 | 32 | 1 | 32 | 1 | 32 | 1 | 32 | 1 | 32 |

# 量子暗号

暗号を制す者は世界を制す。
ナチスの暗号をコンピューターで解読しナチスを破った。

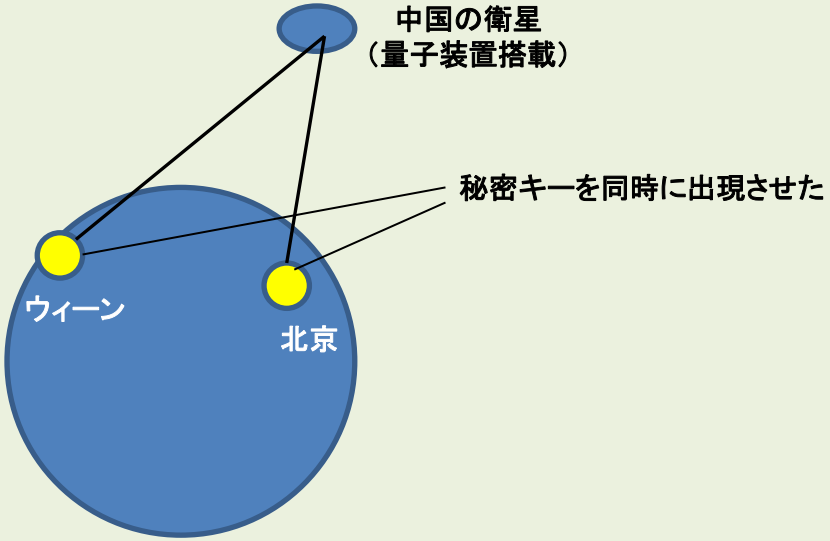
解読不能な暗号＝量子暗号
世界を変える最強の暗号　　基盤技術は欧米で生まれたが実用化では中国が先行している。

オンライン詐欺、ID盗難、ハッカー攻撃、電子的盗聴などから解放される。

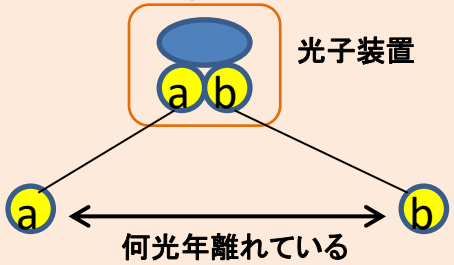
テロリストや犯罪組織が秘密に連絡を取り合ったり、政府が誰にも知られずに秘密を隠匿する可能性もある。

2017年9月に中国科学院の暗号学者と物理学者のチームが量子暗号を使用し北京とウィーンで30分に及ぶビデオ会議実験に成功。

量子のもつれ：1935年に発見、1984年に実験で確認された
　「同時に生み出された2つの光の粒子（光子）はどんなに遠く引き離されても双子のように同じ状態を維持し続ける」




## 量子からみあい（もつれ）




*光子aの影響が瞬時にb伝わる*

**アインシュタインの相対性理論に反しないか？**
**“情報は光速以上では伝わらない。影響が光速以上で伝わることは問題ない！！”**