ネットワークセキュリティ詳説

PKI / TLS プロトコル

加藤 聰彦【著】

コロナ社

ま　え　が　き

今日インターネットは，電気や水道などと並んで，社会生活に欠くことのできないインフラストラクチャとなっている。その利用は，単なる情報検索や通信にとどまらず，ネットショッピングやネットバンキングなどの経済活動にまで広がっている。一般の利用者からは，インターネットは，「つねに側にあって利用できるもの」となっている。

一方，技術的な側面では，インターネットの機能は大規模化，複雑化を続けている。インターネット関連の標準化を進めている IETF では，2022 年 2 月の時点で，9 000 を超える標準文書（RFC）を定めている。また，無線 LAN の規格である IEEE 802.11 標準は，2020 年版が 4 000 ページを超えるサイズとなった。インターネットがインフラ化する裏で，その技術をフォローすることが困難となっている。

インターネットにおいて，技術更新が頻繁かつ注目されている分野の一つが，ネットワークセキュリティである。情報の流出や改ざんなどに対する多様な攻撃に対処するために，セキュリティ機能の改良，追加，大幅なバージョンアップなどが繰り返されている。本書では，ネットワークセキュリティ技術の中で，“https” で始まる URL を用いたセキュアなウェブサーバアクセスに使用される PKI（public key infrastructure：公開鍵基盤）と TLS（transport layer security：トランスポートレイヤセキュリティ）に関して解説する。

本書を作成するにあたっては，できるだけ詳細な技術内容を取り込み，かつわかりやすく説明することを心掛けた。具体的には，PKI と TLS に関連する 70 以上の RFC などの文書を対象とし，踏み込んだ説明を行った。その中には，2018 年に規格化された TLS バージョン 1.3 や，2021 年に規格化された QUIC などの最新情報も含まれる。PKI / TLS の最新の技術動向を広くカバーできていると自負している。

本書の構成はつぎのような三つに分けられる。

- 1 〜 3 章で，PKI / TLS で使用される情報セキュリティ技術の基礎を解説する。暗号化や認証の基本原理から，認証付き暗号（AEAD），RSASSA-PSS，楕円曲線暗号，エドワーズ曲線といった比較的新しい技術までを説明する。
- 4 章と 5 章が PKI に関する解説である。4 章で，認証局や証明書などに関して詳細に説明する。5 章では，証明書を検索・管理するための通信プロトコルを広く解説する。
- 6 〜 8 章が TLS に関する解説である。現在普及している TLS バージョン 1.2，新たに導入されたバージョン 1.3，Google 社が主導的に導入している QUIC のセキュリティなどについて詳しく説明する。

本書では，複数の読者層を想定している。まず，PKI / TLS について学習する読者である。全体を読み込むことにより，専門的な知識を得ることができると考えている。つぎは，セキュリティ初心者である読者である。各章・各節の説明は，概要から詳細に移行するよう努めている。概要の部分に着目することにより，大まかな内容を理解できると思う。最後が，ネットワーク技術者による辞典的な使い方である。PKI や TLS に関して特定のトピックを調べる場合，例えば，OCSP や TLS 1.3 について知りたい，証明書や TLS の特定のエクステンションの意味がわからない，などの場合は，それに関する部分を読むことで理解が進むと思う。このため，各章は独立して読めるように，また目次や索引が多くのキーワードを指定するように努めている。

本書がインターネットにおけるセキュリティの技術動向を理解する一助になればと願っている。

2022 年 7 月　　加藤　聰彦

本書の URL は，すべて 2022 年 8 月現在である。

目　　次

1. 情報セキュリティ技術の基本

2. 慣用系暗号のセキュリティ技術

3. 公開鍵暗号のセキュリティ技術

4. 公開鍵基盤：PKI

5. PKI のための通信プロトコル

6. トランスポートレイヤセキュリティ：TLS

7. TLS バージョン 1.3

8. QUIC セキュリティ

1 情報セキュリティ技術の基本

PKI / TLSプロトコルの解説の第一歩として，本章では情報セキュリティ技術の基本を紹介する。具体的には，慣用系暗号方式，公開鍵暗号方式，認証，鍵管理についての概要を説明する。

1.1 ウェブサーバアクセスのためのセキュリティ技術

今日，インターネットを介した情報通信は，社会のインフラストラクチャの一つとなっており，ウェブサーバアクセスによるオンラインショッピングやオンラインバンキングなども日常的に行われている。しかしこれらの通信では，クレジットカードの番号や銀行口座のID / パスワードなどの個人情報が盗まれ悪用されないように，細心の注意が必要となる。このようなウェブサーバアクセスを安全に実現するために，広く用いられている通信プロトコルがTLS（トランスポートレイヤセキュリティ）であり，ウェブサーバの正当性保証をサポートする仕組みがPKI（公開鍵基盤）である。現在では，多くのウェブサーバがPKI / TLSを使用している。

TLS通信の例として，ブラウザ（Microsoft Edge）を用いて電気通信大学のウェブサーバにアクセスした結果を**図1.1**に示す。アクセス先の**URL**（uniform resource locator）は“https://www.uec.ac.jp”（図中①）であり，プロトコルの種類を示す先頭の“https”が，TLSを用いて**HTTP**（hypertext transfer protocol）の通信を行うことを示す。またURLの表示の左側に鍵のマークがあるが（図中②），これはセキュリティ技術により安全な通信を行っていることを示す。実際，この部分をクリックすると，「接続がセキュリティで保護されています」と表示さ

図1.1 電気通信大学のウェブサーバへのアクセス結果

れる。

ウェブサーバアクセスの安全性を保障するためには，いくつかの要求条件がある。例えば，ウェブサーバにアクセスする利用者（クライアント）とサーバの間で転送されるデータは，悪意のある攻撃者が盗聴したとしても解読できないように暗号化されていなければならない。また，データが途中で改ざんされた場合は受信側で検知可能でなければならない。加えて，そもそも偽物でない正当なサーバと通信していることが保証されなければならない。これらを満足するために，TLS ではこれまでに情報セキュリティ技術として検討された多くのものを利用している。

そこで本書では，1 ～ 3 章で，PKI / TLS で使用される情報セキュリティ技術について解説する。この部分では情報セキュリティの基本から，AEAD や楕円曲線暗号といった比較的最近に使用されるようになった技術まで，一通り詳解する。なお，それらの解説では数学的な詳細については触れていない。本章ではまず，基本的な概念について解説する。

そもそも情報セキュリティとは，情報の機密性，完全性，可用性を維持することと定義されている。**機密性**（confidentiality）とは，許可されていない個人，エンティティまたはプロセスに対して，情報を使用不可または非公開にする特性である。**完全性**（integrity）とは，情報の正確さおよび完全さを保護する特性である。そして**可用性**（availability）とは，許可されたエンティティが要求したときに，情報のアクセスおよび使用が可能であるという特性である。本書では，PKI / TLS について詳細に解説するために，機密性と完全性に着目する。

暗号化（encryption）とは，情報を第三者に盗み見られないように，すなわち機密性を保証するように，決まった規則に従って変換することである。**図 1.2** に示すように，暗号化を行う前の情報を**平文**（plaintext）と呼び，暗号化された後の情報を**暗号文**（ciphertext）と呼ぶ。また，暗号文を平文に直す作業を**復号**（decryption）と呼ぶ。

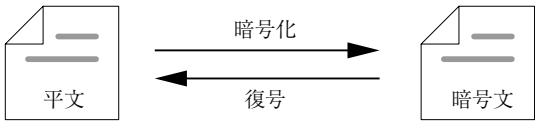


図 1.2　暗号化と復号

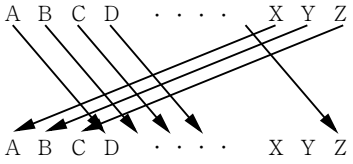


図 1.3　シーザー暗号

図 1.3 にジュリアス・シーザーが使用したといわれる**シーザー暗号**（Caesar cipher）の例を示す。これは，アルファベットを一定数だけずらすことにより暗号化し，逆に戻すことにより復号するというものである。図の例では，3 文字ずつずらしている。これにより，「TOSHIHIKO KATO」という平文は「WRVKLKLNR NDWR」という暗号文に変換される（ただしブランクの処理は省いている）。情報の送受信者が「3 文字ずらす」ということを知っている場合に，正確かつ安全な情報の伝達が可能となる。

これは非常に単純な方式であるが，現在の暗号方式につながる重要な性質を持っている。そ

れは，暗号化および復号のアルゴリズムは既知であり，「何文字ずらすか」という情報のみが秘密だということである。このような，暗号化および復号に使用する秘密の情報を**鍵**（key）と呼ぶ。アルゴリズムを公開し，鍵のみを秘密にすることにより，暗号のソフトウェアを誰もが開発できる，暗号の設計者が悪意のある仕掛けを施していないことを確認できる，などの利点が生じる。一方，鍵の情報が知られただけで暗号が破られる，という欠点もある。実際，シーザー暗号は鍵の種類が 26 個しかないため，容易に解読可能である。

シーザー暗号は機密性の保証のみを目的とするが，前述のように，現在の情報セキュリティにおいては，完全性の保証も重要な目的の一つとなっている。完全性の保証とは，具体的にはつぎの二つの攻撃への対応である（**図 1.4** 参照）。第一の攻撃は，正しい送信者 A が受信者に対して情報を送信した際に，攻撃者がその内容を改ざんするというものである。第二は，攻撃者 A′ が，送信者 A と偽って受信者に情報を送信するというものである。これらに対して，完全性の保証により，情報が正しい作成者によって作成され，かつその情報が悪意のある第三者によって改ざんされていないことが保証される。この完全性の保証を実現するための処理を**認証**（certification）と呼ぶ。認証では，対象となる情報を特徴づける付加情報を暗号技術により生成し，元の情報と付加情報の対により，情報の発信者が想定した者であること，元の情報（および付加情報）が改ざんされていないことの二つを保証する。

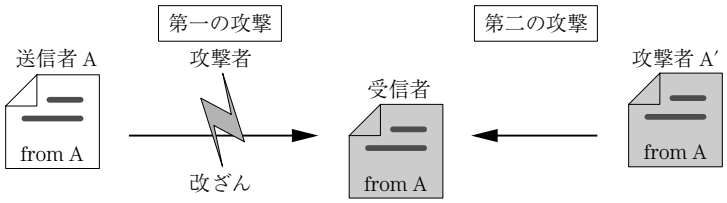


図 1.4　完全性の保証が想定する攻撃

また，前述のシーザー暗号では，暗号化と復号に同じ鍵「3 文字ずらす」を使用した。このような暗号方式を慣用系暗号方式と呼ぶ。これに対して，暗号化と復号に異なる鍵を使用し，そのうち一方のみを公開するという公開鍵暗号方式も存在する。

以下では，慣用系暗号方式と公開鍵暗号方式，認証，鍵の管理について順に概説する。

1.2　慣用系暗号方式

1.2.1　概　　要

慣用系暗号方式（conventional cryptosystem）とは，**図 1.5** に示すように，平文を暗号化する側と，暗号文を復号する側が，同一の鍵を用いる方式である。この方式は，**共通鍵暗号方式**（common key cryptosystem），**秘密鍵暗号方式**（secret key cryptosystem），**対称鍵暗号方式**（symmetric key cryptosystem）などとも呼ばれる。使用される鍵は，暗号化する側と復号する

図 1.5　慣用系暗号方式

側のみが保持しており，第三者には知らせてはならない。このため，**秘密鍵**（secret key）と呼ばれる。

この方式では，$\mathrm{E}(k, M)$ を暗号化の関数，$\mathrm{D}(k, M)$ を復号の関数とすると，暗号化と復号の関係は次式で与えられる。ただし，M は暗号化の対象となる情報（平文または暗号文），k は秘密鍵である。

$$M = \mathrm{D}(k, \mathrm{E}(k, M))$$

慣用系暗号方式は，ハードウェアによる実現を想定した方式であり，高速な暗号化・復号の処理が可能である。そこで，転送するパケットの暗号化など，比較的長いデータの処理を高速で行う場合などに用いられる。

1.2.2　ストリーム暗号とブロック暗号

転送するパケットの暗号化において，対象となる平文は可変長である。このような状況に対応するために，慣用系暗号方式ではつぎの二つのアプローチを採用している。第一は，平文と同じ長さのランダムなバイト列（乱数列）を生成し，その乱数列を用いて暗号化する**ストリー**

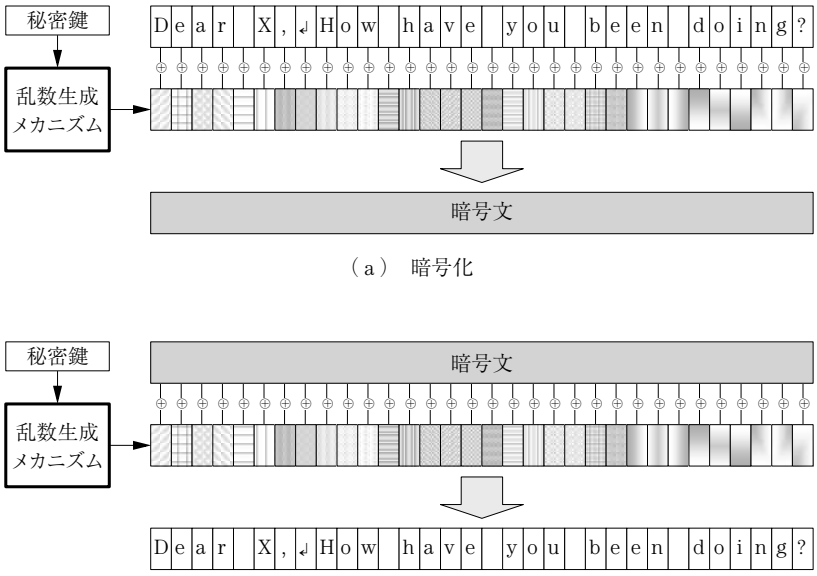
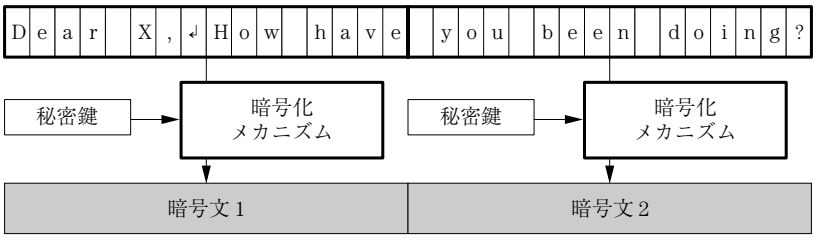


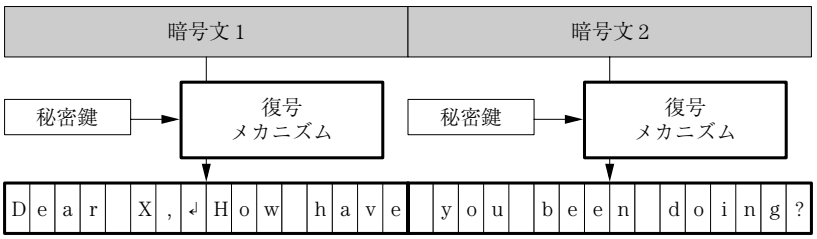
図 1.6　ストリーム暗号の概要

ム暗号（stream cipher）である。**図 1.6** にその概要を示す。図（a）の暗号化においては，秘密鍵に基づいて，平文と同じ長さの乱数列を生成し，平文のバイトと対応する乱数列のバイトとの排他的論理和を計算して暗号文とする。図（b）の復号においては，同じ乱数生成メカニズムと秘密鍵を用いて，暗号化と同一の乱数列を生成する。この乱数列と暗号文との各バイトの排他的論理和を計算することにより，平文を復元する。

第二のアプローチは，平文を固定長のブロックに分割し，ブロックごとに暗号化および復号を行う**ブロック暗号**（block cipher）である。その概要を**図 1.7** に示す。平文は固定長（図の例では 16 バイト）に分割され，ブロックごとに秘密鍵を用いて暗号化・復号される。なお，この例では平文がブロック長の整数倍であるが，平文の最後の部分はブロック長よりも短くなることが一般的である。そのような場合は，暗号化時に最後のブロックに追加の情報を埋め込む必要がある。



（a） 暗号化



（b） 復　号

図 1.7　ブロック暗号の概要

また，平文が複数のブロックに分割される場合は，連続したブロックをどのように関連付けるかを考慮する必要がある。このメカニズムをブロック暗号の利用モードと呼ぶ。図では各ブロックを独立に暗号化・復号しているが，より安全性を高めるために，多くの方法が提案されている。

ストリーム暗号の代表例としては，RC4 が挙げられる。またブロック暗号としては，かつては米国の国家暗号規格であった DES が代表例だった。しかし，その脆弱性が指摘され，現在は AES が広く用いられている。

索　　引

——著 者 略 歴——

1978 年　東京大学工学部電気工学科卒業
1983 年　東京大学大学院工学系研究科博士課程修了（電子工学専門課程）
　　工学博士
1983 年　国際電信電話株式会社研究所勤務
1991 年　国際電信電話株式会社研究所主任研究員
1995 年　国際電信電話株式会社研究所グループリーダ
2001 年　KDDI 研究所執行役員
2002 年　電気通信大学助教授
2007 年　電気通信大学教授
2021 年　電気通信大学名誉教授
2022 年　神奈川工科大学客員教授
　　現在に至る

ネットワークセキュリティ詳説　PKI / TLS プロトコル
PKI / TLS Protocols : Network Security Explicated

2022 年 10 月 3 日　初版第 1 刷発行　★

検印省略

著　者　加藤聰彦（かとう としひこ）
発行者　株式会社　コロナ社
　　代表者　牛来真也
印刷所　壮光舎印刷株式会社
製本所　株式会社　グリーン

112–0011　東京都文京区千石 4–46–10
発 行 所　株式会社　**コ ロ ナ 社**
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替00140–8–14844・電話(03)3941–3131(代)
ホームページ　https://www.coronasha.co.jp

ISBN 978-4-339-02929-1　C3055　Printed in Japan　（西村）