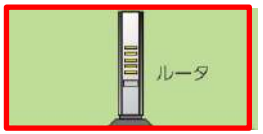
| 図書の記号・番号 | 情Ｉ７０５ |
|---|---|

| 番号 | 訂正箇所 ページ | 訂正箇所 行 | 原　　文 | 訂　　正　　文 |
|---|---|---|---|---|
| 1 | 67 | 例題２の図 |  |  |
| 2 | 110<br>-<br>111 | | 別添１ | 別添１ |
| 3 | 112 | 18行 | 符号 check digit（チェックディジット） | （削除） |
| 4 | 39 | 24行 | 規定されおり， | 規定されており， |

## 2 デジタル署名と電子認証

電子メールを受け取ったとしても，それが本当に本人からのものであるのかどうかを判断することは難しい。誰かがその人になりすまして送信したものである恐れもある。

そこで，発信者が本人であることを証明する方法として，公開鍵暗号方式の公開鍵と秘密鍵のどちらの鍵でも暗号化できるという性質を応用したデジタル署名がある。

公開鍵暗号方式は，公開鍵で暗号化したものを秘密鍵で復号するが，デジタル署名はこの逆を行う。つまり，送信者は本人しかもっていない秘密鍵で要約文を暗号化したデジタル署名を文書に添付する。そして，受信者は公開鍵で要約文へ復号する。プログラムで文書から作成された要約文と復号された要約文を比較することで，その文書が本人からのものかどうか確認することができる。

❶秘密鍵をもっている人しかデジタル署名はできない。秘密鍵を格納したICカードなどをコンピュータにセットしてデジタル署名するため，コンピュータに秘密鍵の情報が残らない。

❷ダイジェストメッセージまたはハッシュ値ともいい，プログラムにより平文の特徴的な部分を生成した文のこと。要約文から平文に戻すことはできない。


①送信者は，公開鍵をあらかじめ認証局（認証する機関）に届ける。
②認証局は，公開鍵が申請者（送信者）のものであることを証明する電子証明書を発行する。
③送信者は，あるプログラムにより，送信する平文から要約文（ダイジェスト）を作成する。
④送信者は，署名（デジタル署名）を行う（秘密鍵を用いて要約文を暗号化）。
⑤デジタル署名と送信者の公開鍵が添付された電子証明書を，平文とともに送信する。
⑥受信者は，認証を行う（電子証明書から送信者の公開鍵を取り出し，デジタル署名を復号し，要約文を取り出す。復号に成功すれば，送信者本人であることが認証される）。
⑦受信者は，平文から③と同じプログラムにより要約文を作成する。
⑧上記⑥と⑦の要約文を比較し，一致すれば送信者本人によりデジタル署名されたことが証明される。もとの文が少しでも改竄されていると異なる要約文が作られ，一致しない。
⑨受信者は認証局に問合し，電子証明書が有効であるかを確認する。

●図４　デジタル署名・電子認証の方法

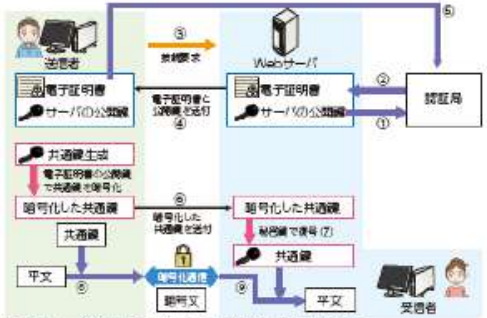
電子証明書は，公開鍵の持ち主を証明する電子データである。平文を送信する際に，送信者が公開鍵を信頼できる認証局に登録し，電子証明書の発行を受け，平文やデジタル署名とともに公開鍵を添付した電子証明書を送信する。公開鍵が送信者本人のものかどうかは，認証局に照会することで確認できる。なお，デジタル署名と電子証明書は，従来の印鑑と印鑑証明書に相当する。デジタル署名が本人のものかどうかを電子証明書により第三者が証明する技術を電子認証という。

## 3 SSL/TLS

Webページ上で情報をやり取りする際に用いられる暗号化技術にSSL（Secure Sockets Layer）がある。SSLで暗号化されたWebページのURLは「https://」で始まっていて，このプロトコルをHTTPSという。ブラウザに鍵（錠）のマークを表示することによって，データがSSLによって暗号化されていることを示している。また，暗号化はセッション鍵方式が利用されており，鍵のやり取りは，Webサーバと利用者のブラウザ間で自動的に行われる。

❶デジタル署名だけではなりすましを防げない。公開鍵は誰でも利用できるので，電子証明書が必要になる。

❷🔒や🔐のようにブラウザの一部に鍵のマークが付く。




①受信者は，公開鍵をあらかじめ認証局（認証する機関）に届ける。
②認証局は，公開鍵が申請者（受信者）のものであることを証明する電子証明書を発行する。
③送信者は，受信者に協調要求をする。
④受信者は，送信者に受信者の公開鍵が添付された電子証明書を送信する。
⑤送信者は，認証局に照会し，電子証明書が正しく有効であるかを確認する。
⑥送信者は，送信者が作成した共通鍵を，受信者の公開鍵で暗号化して送信する。
⑦受信者は，受信者の秘密鍵で復号して共通鍵を取り出す。
⑧送信者は，平文を共通鍵で暗号化して送信する。
⑨受信者は，暗号化された平文を共通鍵で復号する。

●図５　SSLの処理の流れの例

**+α**

電証では，SSLのセキュリティをさらに高めた暗号化方式としてTLS（Transport Layer Security）が多く使用されているが，SSLの名称が普及していることから総称としてSSLということもある。

| 別添 No. | 訂　　正　　文 |
|---|---|
| 1 | |

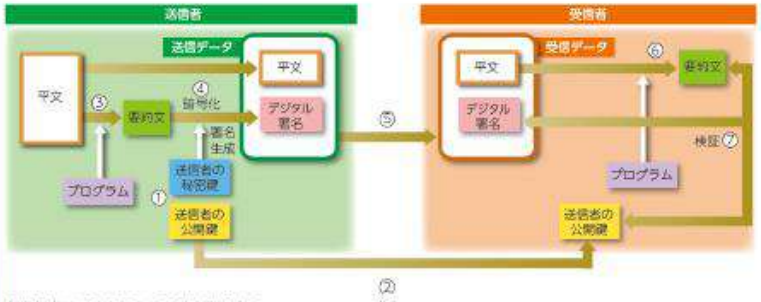
## 2 デジタル署名と電子認証

電子メールを受け取ったとしても，それが本当に本人からのものであるのかどうかを判断することは難しい。誰かがその人になりすまして送信したものである恐れもある。

発信者が本人であることを証明する方法として，**デジタル署名**❶がある。送信者は本人しかもっていない秘密鍵で要約文❷を暗号化したデジタル署名を文書に添付する。そして，受信者は平文から得られた要約文と送信者から送られた公開鍵，およびデジタル署名の3つが，ある検査式を満たしているかを検証することで，その文書が本人からのものかどうか確認することができる。

❶秘密鍵をもっている人しかデジタル署名はできない。

❷ダイジェストメッセージまたはハッシュ値ともいい，プログラムにより平文の特徴的な部分を生成した文のこと。要約文から平文に戻すことはできない。




①送信者は，秘密鍵と公開鍵を作成する。
②送信者は，公開鍵を受信者へ送信する。
③送信者は，あるプログラムにより，送信する平文から要約文を作成する。
④送信者は，送信者の秘密鍵で署名（デジタル署名）生成を行う。
⑤デジタル署名と平文とともに送信する。
⑥受信者は，平文から③と同じプログラムにより要約文を作成する。
⑦②の公開鍵と⑥の要約文，④のデジタル署名の三つが，ある検査式を満たしているかを検証し，満たしていれば，本人から受信した平文であると確認できる。
●図4　デジタル署名の方法

❸デジタル署名だけではなりすましを防げない。公開鍵は誰でも利用できるので，電子証明書が必要になる。

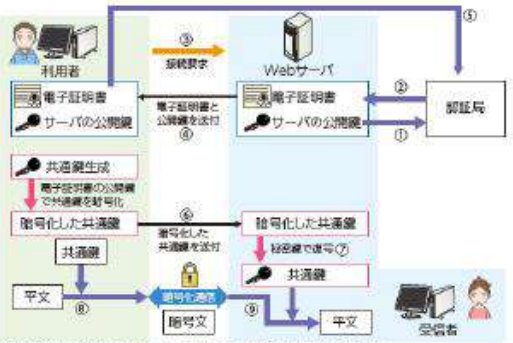
**電子証明書**❸は，公開鍵の持ち主を証明する電子データである。平文を送信する際に，送信者が公開鍵を信頼できる認証局に登録し，電子証明書の発行を受け，平文やデジタル署名とともに電子証明書を添付した公開鍵を送信する。公開鍵が送信者本人のものかどうかは，認証局に照会することで確認できる。デジタル署名が本人のものかどうかを電子証明書により第三者が証明する技術を**電子認証**という。


①送信者は，公開鍵をあらかじめ認証局（認証する機関）に届ける。
②認証局は，公開鍵が申請者（送信者）のものであることを証明する電子証明書を発行する。
③送信者は，デジタル署名と公開鍵が添付された電子証明書を平文とともに送信する。
④受信者は，認証局に照会し電子証明書が有効であるかを確認する。
●図5　電子認証の方法

## 3 SSL/TLS

Webページ上で情報をやり取りする際に用いられる暗号化技術にSecure Sockets Layer/Transport Layer Security SSL/TLSがある。SSL/TLSで暗号化されたWebページのURLは「https://」で始まっていて，このプロトコルをHTTPSという。ブラウザに鍵（錠）のマークを表示することによって，データがSSL/TLSによって暗号化されていることを示している。❶また，暗号化はセッション鍵方式が利用されており，鍵のやり取りは，Webサーバと利用者のブラウザ間で自動的に行われる。

❶🔒や🔐のようにブラウザの一部に鍵のマークが付く。




①受信者は，公開鍵をあらかじめ認証局（認証する機関）に届ける。
②認証局は，公開鍵が申請者（受信者）のものであることを証明する電子証明書を発行する。
③利用者は，受信者に接続要求をする。
④受信者は，利用者に受信者の公開鍵が添付された電子証明書を送信する。
⑤利用者は，認証局に照会し，電子証明書が正しく有効であるかを確認する。
⑥利用者は，利用者が作成した共通鍵を，受信者の公開鍵で暗号化して送信する。
⑦利用者は，受信者の秘密鍵で復号して共通鍵を取り出す。
⑧利用者は，平文を共通鍵で暗号化して送信する。
⑨受信者は，暗号化された平文を共通鍵で復号する。
●図6　SSL/TLSの処理の流れの例