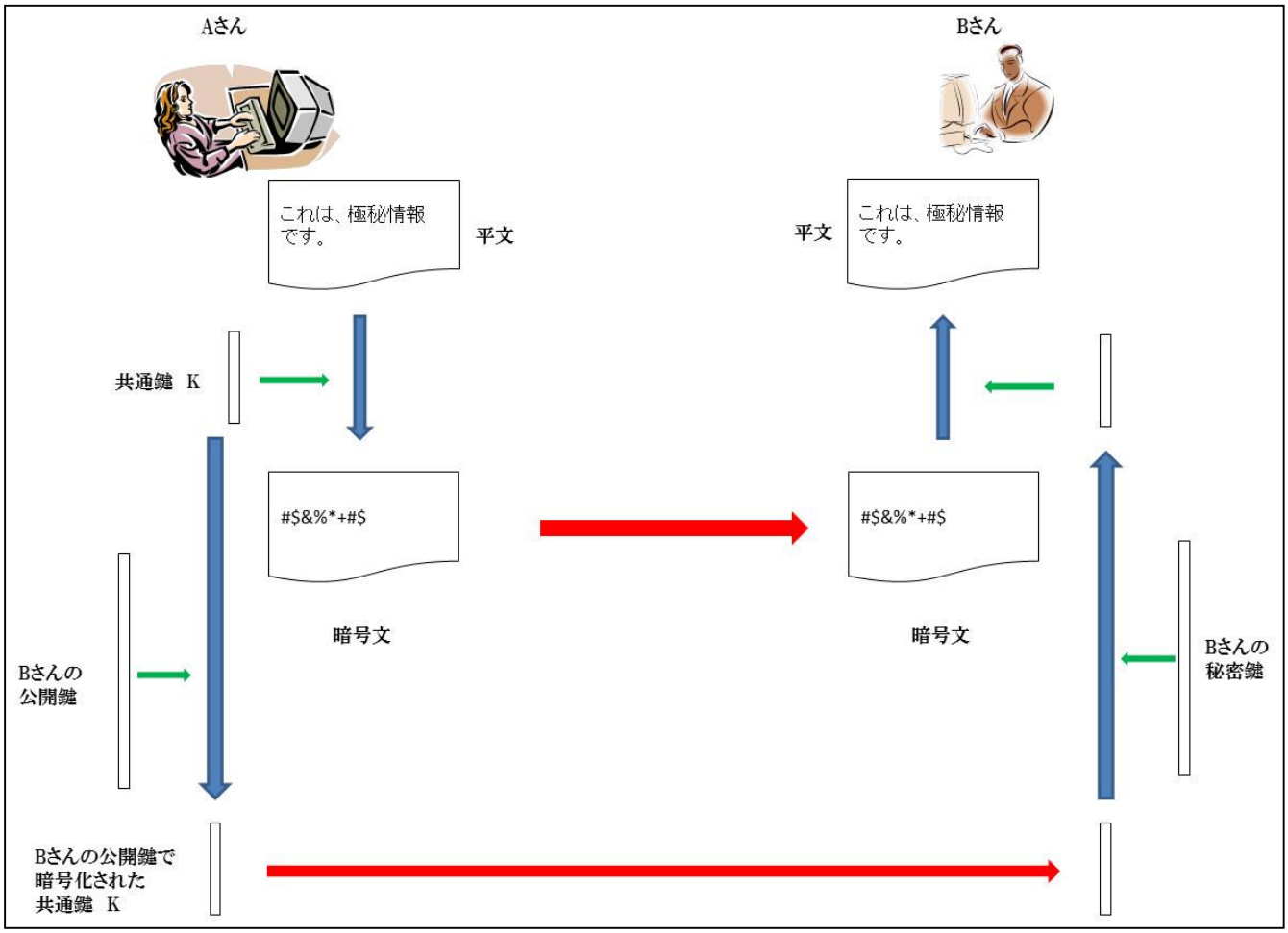
（1） 公開鍵暗号について

公開鍵暗号の説明をさらに進めます。その前に、公開鍵暗号と共通鍵暗号を用いた盗聴防止のデータ送受信の様子を図示したものを以下に示します。

送り手（A さん）は、まず共通鍵暗号で送りたい文（平文）を暗号化し、受け手（B さん）に送ります。この時の鍵は、乱数発生ソフトを用いて生成した規則性のない数値（乱数）を使います。この鍵を受け手（B さん）の公開鍵暗号の公開鍵で暗号化します。これも受け手に送ります。受け手側では、まず、送られてきた暗号化された鍵を自分の公開鍵暗号の秘密鍵で復号します。そして、その鍵で送られてきた暗号文を復号し、送り手からの平文を読むことができます。



さて、先々月（5 月）の紹介の中で、暗号によって「成りすまし」、「不正アクセス」、「改ざん」を防ぐことができると申し上げました。データを読めなくして、盗み見を防ぐという従来の暗号のイメージからは、少し異質なので、よくわからないという方も多いかと思います。まず「成りすまし」をどのように防ぐかを説明します。

そもそも「成りすまし」を防ぐというのは、「その人であることを証明する」ということにつきます。実際の生活の中でも、健康保険証や免許証で自分であることを証明しなければいけない場面がよくあると思います。でも、それを情報セキュリティ技術ではどのようにしたら実現できるのでしょうか？ごく単純に示すと以下の手順にようになります。

① 送り手は自分の公開鍵証明書を受け手に送る。

② 受け手は、送り手の公開鍵証明書についての第三者の証明を確認する。

しかしこれだけではあまりにも単純すぎて、具体的なことがよくわかりませんね。ただ、考え方としては、ある所有者の公開鍵暗号の秘密鍵はその所有者が持っており他人が使うことができないということを信頼の根拠とします。そしてその公開鍵暗号の所有者であることが、信頼できる第三者（認証局といいます）が発行した証明書によって証明され、受け手がその証明が間違いないことを確認できるしくみがあり、それを使うわけです。実際の生活においても、実印というのは本人しか使えませんし、その実印の証明書（印鑑証明書）を添付することによって、実印を押した文書が本人の作成した文書である（文書にその人の法的責任がある）ことが証明されますが、この役所が発行する印鑑証明書というしくみが「成りすまし」防止の機能に相当します。これにより、送り手が成りすましていないことが確認できるというわけです。実印を押すという行為に相当する機能はさらに後程「改ざん防止」として説明します。

具体例を見てみましょう。ネットショッピングは今や多くの方が経験していると思いますが、そのショッピングサイトで、クレジットカード番号を登録したり、利用状況の確認をしたりするときに、URL が https:// から始まるものに変わっていることが多いと思います。これは、上記の仕組みを使って、ショッピングサイトが成りすましではないことを利用者に示すための機能を使っているということを示しているものです。情報システムとして以下のようなことを行っています。

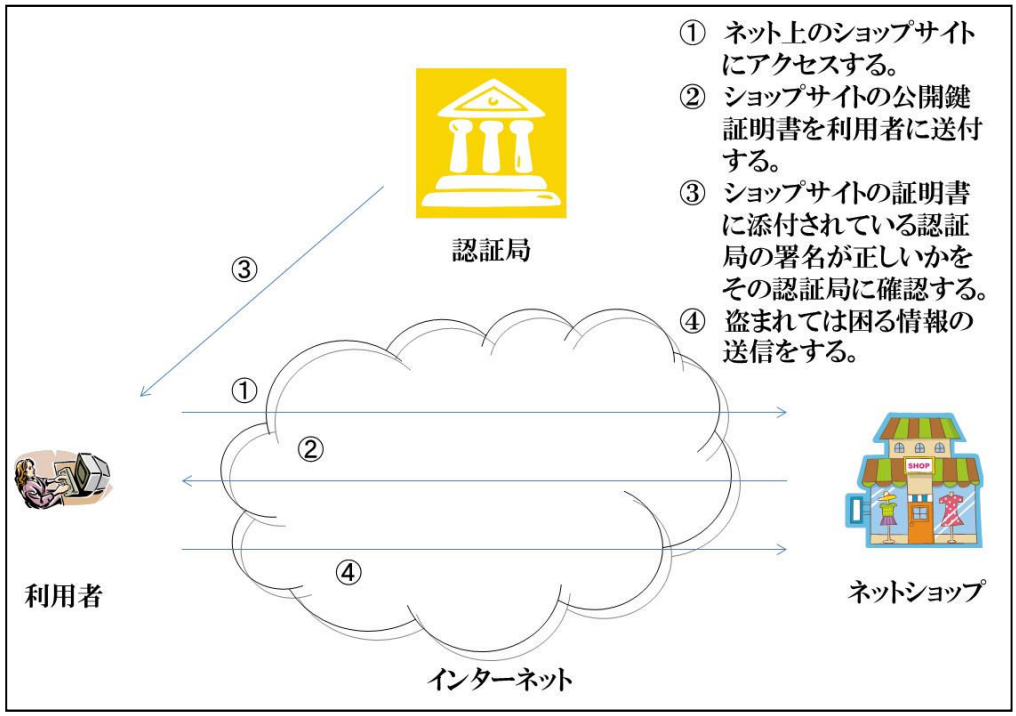
① 利用者がそのショッピングサイトにアクセスすると、サイトは自身の公開鍵証明書（中に自身の公開鍵も含んでいる）を利用者に送ります。その証明書はその公開鍵がサイトのものであることを示すものですが、その証明書には証明書がサイトのものであることを証明する認証局の署名が添付されています。

② 利用者側では、そのショッピングサイトの証明書に添付されている認証局の署名が正しいものであるかを、認証局の証明書を用いて確認します。

③ その後、例えばクレジットカード番号をサイトに送る際は、その証明されたサイトの公開鍵によって暗号化、実際は、前回も説明したように、クレジットカード番号

を共通鍵暗号で暗号化し、その鍵をその公開鍵によって暗号化し、サイトに送り、サイト側では、自身の秘密鍵で鍵を復号し、その鍵で暗号化されたクレジットカード番号を復号し登録します。

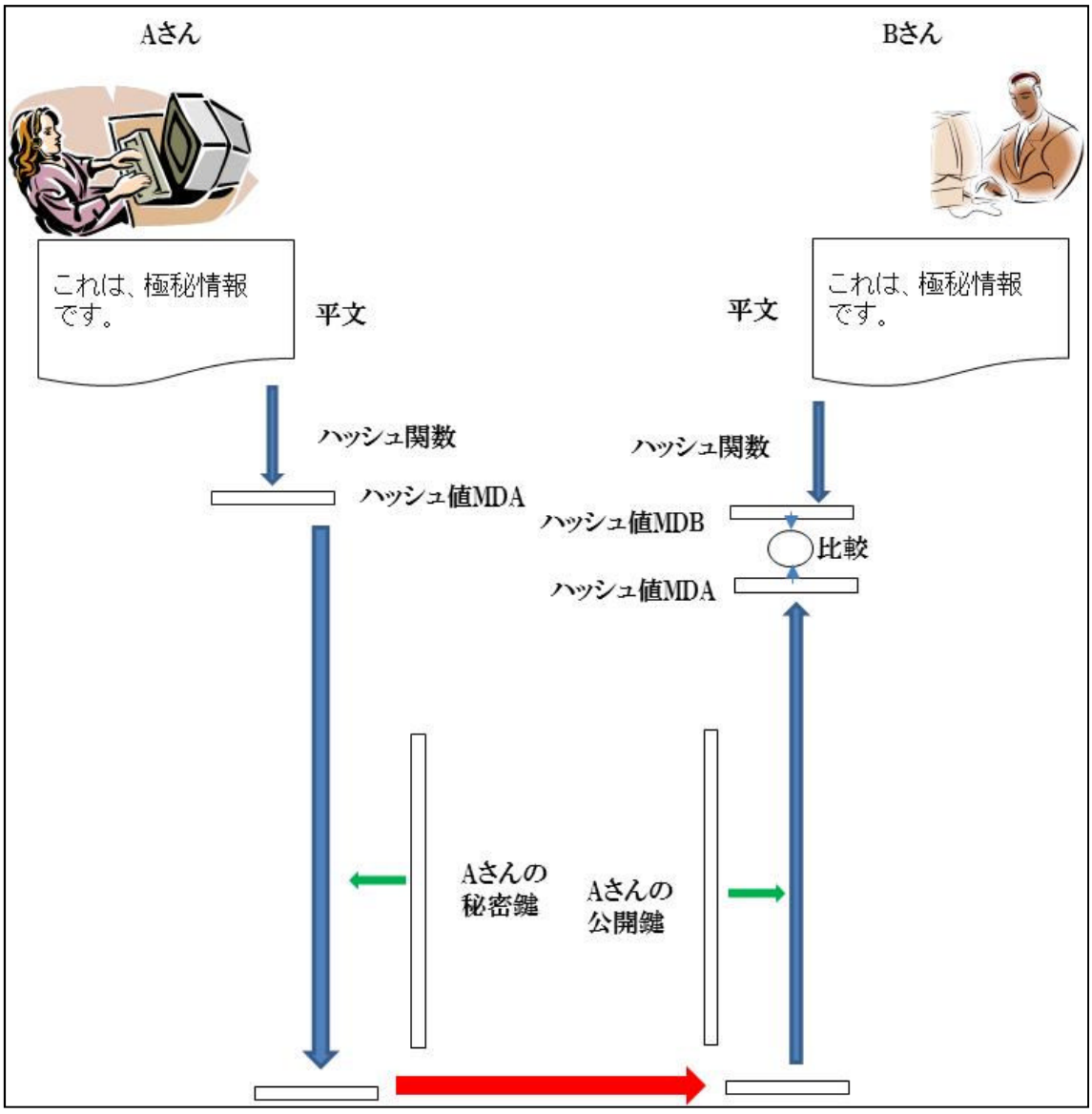
以上、言葉のみで説明しましたので、図示したものを以下に示します。



また、「成りすまし」防止とは表裏一体の機能で、「不正アクセス」の防止という機能がありますが、これは、単純には、パスワードによって利用者の確認をして、正しいパスワードを入力できない場合はアクセスを受け付けないということで実現はできますが、公開鍵暗号を用いた「不正アクセス防止」は、このショッピングサイトと利用者の関係の逆で、アクセスされるサイト側が利用者に対して、証明書の送付を要求し、その証明書を認証局に確認して、利用者本人に間違いないことを検証し、不正な者からのアクセスを受け付けないということです。具体的には所得税の確定申告などで e-Tax をご利用になろうと思った方もいらっしゃるかと思いますが、e-Tax を使うには準備として電子証明書の取得が必要です。この電子証明書というのが、自分の公開鍵証明書であり、市町村役場で発行してくれます。まさに印鑑証明書の電子版というものですね。自分自身の有効な電子証明書なしに e-Tax システムを利用すると不正アクセスとなります。公共のサービスですから個人情報などの保護のために、これだけ強力な「不正アクセス」防止が必要なわけです。

さて、話をもとに戻します。

「署名を添付する」とか「署名が正しいかを認証局の証明書を用いて確認する」などと言っていますが、それが公開鍵とどう関係してくるんだろう？と、まだ、具体的に説明できていません。ここで「改ざん」防止の説明をすることによって、この署名、証明書の確認などの意味をご理解いただこうと思います。さて、ここまで「署名」と言う言葉を使ってきましたが、情報セキュリティ技術での正式な呼び方は「デジタル署名」といいます。下の図は、その「デジタル署名」の仕組みを示したものです。



また、新しい言葉「ハッシュ関数」「ハッシュ値」という専門用語が出てきてしまいましたので、まずはこちらの説明をさせていただきます。ハッシュ関数というのは、データを変換する関数で、逆方向への変換が困難な関数が使われます。定義の言葉ではよく意味が分からないと思いますので、具体的な例で説明してみます。いろいろなアルゴリズム（演

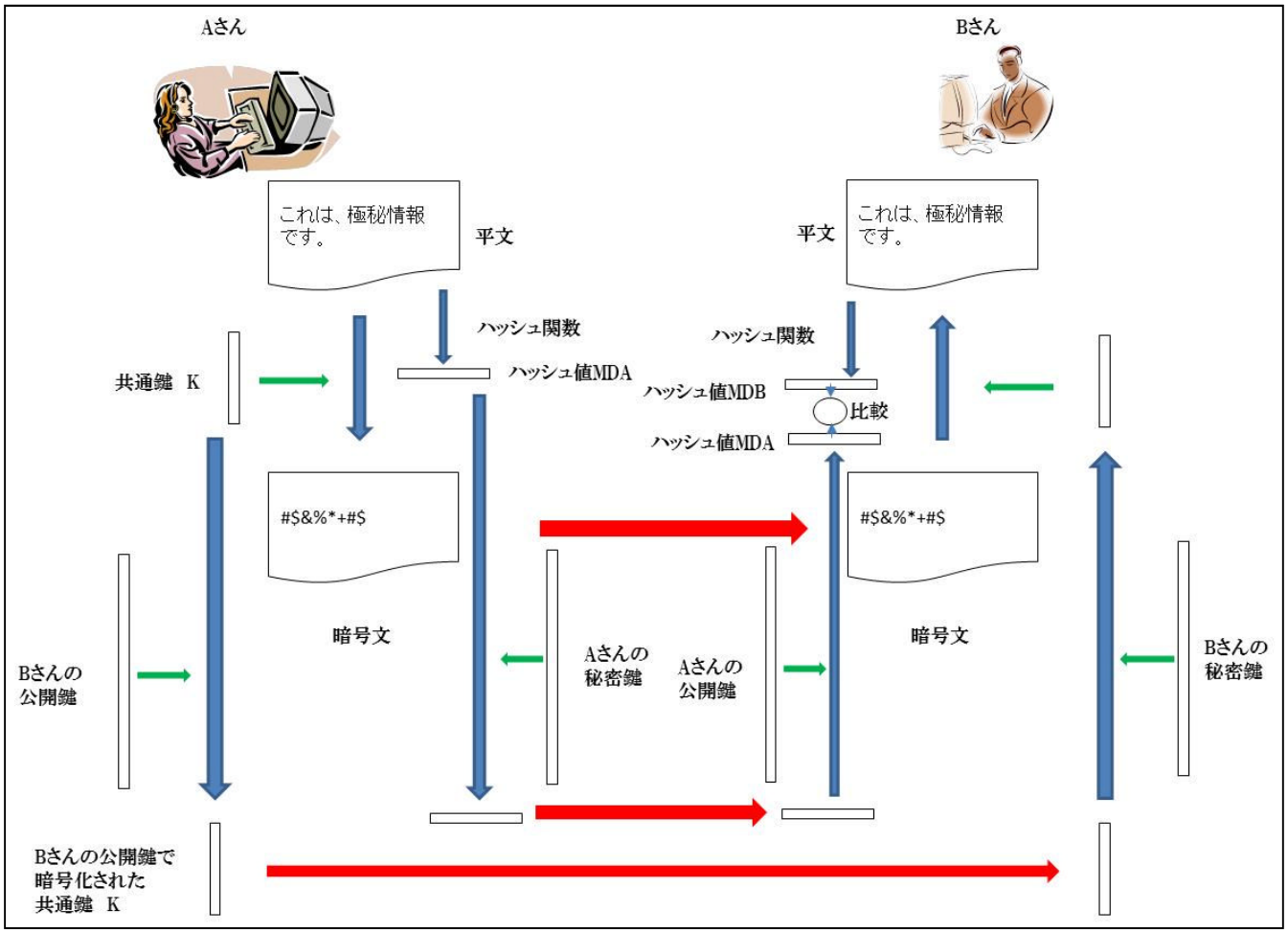
算方法）がありますが、例えば、共通鍵暗号の時に使った排他的論理和を使っても実現できます。例えば、データの先頭から 128 ビットずつ順に取り出してその 128 ビットと次の 128 ビットの排他的論理和を取ります。その結果と、次の 128 ビットの排他的論理和を取り、その結果と次、という具合にデータの最後まで演算し、最終的には 128 ビットの結果が残ります。この 128 ビットの値からはもとのデータを作り出すのは困難ですので、ハッシュ関数となりえます。つまり、この 128 ビットの演算結果が排他的論理和というハッシュ関数を施したハッシュ値となります。ただし、排他的論理和のような単純な演算ですと、同じハッシュ値を出す別の元データを簡単に作り出せてしまうので（例えば最初の 128 ビットだけハッシュ値と同じにして、残りのデータはすべてゼロとすれば、同じハッシュ値を出す元データとなります）このデジタル署名の仕組みに使うことはできません。ここでは、ハッシュ関数の説明のために単純演算を使用しただけですので、悪しからずご了承ください。

さて、デジタル署名の説明に移ります。この図では送り手 A さんがデジタル署名を付けて受け手 B さんに極秘文書を送ろうとしています。まず、A さんは極秘文書にハッシュ関数を施し、ハッシュ値 MDA（このハッシュ値のことをメッセージダイジェストと呼ぶため略称 MD とし、A さんが作ったハッシュ値なので MDA としました）を作ります。このハッシュ値 MDA に対して、A さんの秘密鍵で暗号化し、それを B さんに送ります。デジタル署名の基本的な考え方として、この自分の「秘密鍵で暗号化する」ことが、「署名をする」という行為に相当します。先ほど、「実印を文書に押す」という実際の生活での行為に当てはめて説明しましたが、まさにこの「実印を押す」に相当します。自分の秘密鍵を使うという行為を行えばいいので、A さんの秘密鍵で、平文全体を暗号化してもデジタル署名となりえます。しかし、公開鍵暗号は以前にも説明したとおり、処理時間がかかりすぎて、実用的ではないため、ハッシュ値のような短め（128 ビットとか 256 ビットとか）で、かつ元の文書のダイジェストになる（元のデータの特徴などをうまく表せるような）値を計算し、それに対して秘密鍵で暗号化するという方法を取ります。さて暗号化されたハッシュ値 MDA は受け手 B さんが A さんの公開鍵を使って復号します。これにより元のハッシュ値 MDA が得られます。B さんはさらにいっしょに送られてきた平文からハッシュ値を自分で計算します。これは当然同じハッシュ関数を用いますが、B さんが作ったのでハッシュ値 MDB と呼んでおきます。そして、ハッシュ値 MDA とハッシュ値 MDB を比較し、等しければ、極秘文書に改ざんがなかったことと同時に送り手が A さんであることが確認できるということです。先ほど、排他的論理和ではこのデジタル署名の仕組みとして利用できない

と言いましたが、B さんが受け取る平文を、悪意を持った人が先ほどの要領で、同じハッシュ値が出てくる偽データに置き換えたとしましょう。それでも、ハッシュ値 MDB と A さんから暗号化して送られてきたハッシュ値は等しくなり、改ざんされていないと判定できてしまいます。ですから、同じハッシュ値となる偽の元データが容易に作れるハッシュ関数はデジタル署名としては使われません。

このデジタル署名の仕組みを使って、先ほどの疑問を説明します。すなわち、ショッピングサイトの公開鍵証明書に認証局のデジタル署名が添付されているというのは、公開鍵証明書（公開鍵そのものと、公開鍵アルゴリズム、所有者の情報などが記載されてる電子文書です）のハッシュ値を認証局自身の秘密鍵で暗号化したものがデジタル署名です。利用者は、認証局の公開鍵でそのデジタル署名を復号し、証明書本体を自分でハッシュ関数を施し、復号した値と比較し、等しいかどうかを確認します。これにより、等しければ、認証局がデジタル署名を添付した証明書であることが確認できるというわけです。

さて、デジタル署名の仕組みの説明では図が複雑にならないように極秘文書は平文のまま送り手に送っているかのように書きましたが、一番盗聴されては困るデータですので、当然実際は暗号化して送ることは言うまでもありません。以上を加味し、デジタル署名の仕組みも追加したデータ通信の仕組み全体を図示したものが、下の図です。非常に細かくごみごみしていますが、通信路上を流れる情報はすべて暗号化されており、改ざんの防止も検知できる方式になっています。



公開鍵暗号という技術が発明されたことによって、いろいろな情報セキュリティの脅威から情報が保護できるようになりましたが、この公開鍵暗号を活用するためには、説明の中にもありましたように「認証局」という運用上の仕組みが必要なことがわかります。このように公開鍵暗号を用いてセキュアな情報サービス、システムを構築するための基盤のことを PKI（Public Key Infrastructure）と呼びます。

ということで、ここまでで暗号の技術的な説明を終了し、次回以降は、PKI や暗号技術の標準化など暗号を取り巻く仕組みや施策などの説明をしてみたいと思います。