情報セキュリティの基礎2

テキストP59–99

http://cobayasi.com/koza/security/2_basic2.pdf

守りたい対象を整理し、セキュリティの適切なコストを算定する

暗号

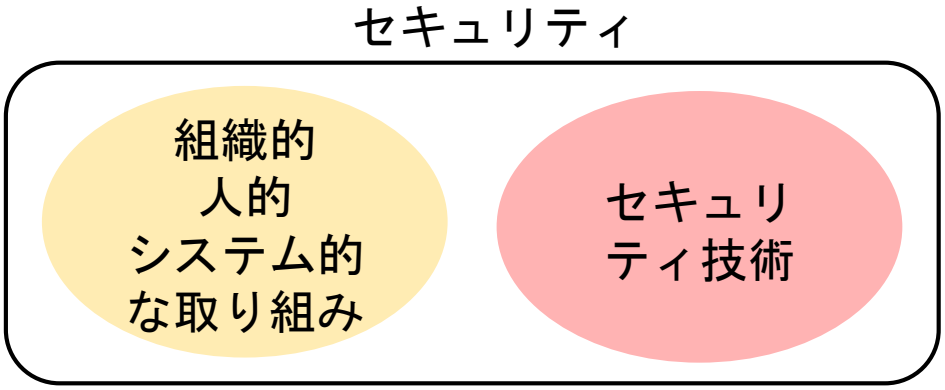
1. セキュリティ技術の広がり
2. 暗号の基本
3. 共通鍵暗号
4. 公開鍵暗号

セキュリティ技術の広がり

テキストP59-61

セキュリティ技術とは

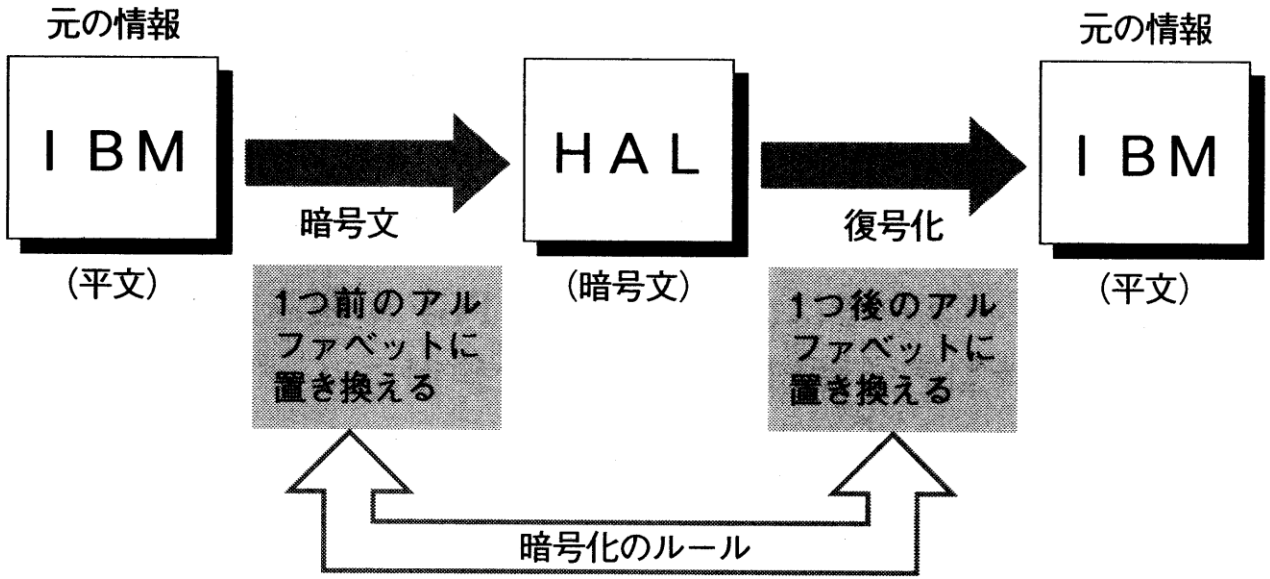
安全に仕事を進めるために行う、継続的な組織的・人的・システム的な取り組み(セキュリティ)を、効率的に行うための技術



セキュリティ技術の種類

暗号化

データの内容を第三者に分からなくする方法



Ｉ Ｂ Ｍ
↓ ↓ ↓ 1つ前のアルファベットに置き換える
Ｈ Ａ Ｌ
↓ ↓ ↓ 1つ後のアルファベットに置き換える
Ｉ Ｂ Ｍ

認証

正当性を検証すること。ユーザ名とパスワードの組み合わせを使って、コンピュータを利用しようとしている人に、その権利があるかどうか(ユーザ認証)や、その人が名乗っている本人かどうかなどを確認する(本人認証)こと。

マルウェア対策

ウィルスなどの「悪意のあるソフトウェア」(マルウェア:Malicious Software)に対して、有効な手段を講じる

フィルタリング

一定の条件に基づいてデータなどを選別・排除する仕組み

信頼性の向上

使用しているシステムが壊れないように対策を取る。「自動的にデータを二重に保存する」「システムが故障した際の代替機を用意する」

暗号の基本

テキストP62-63

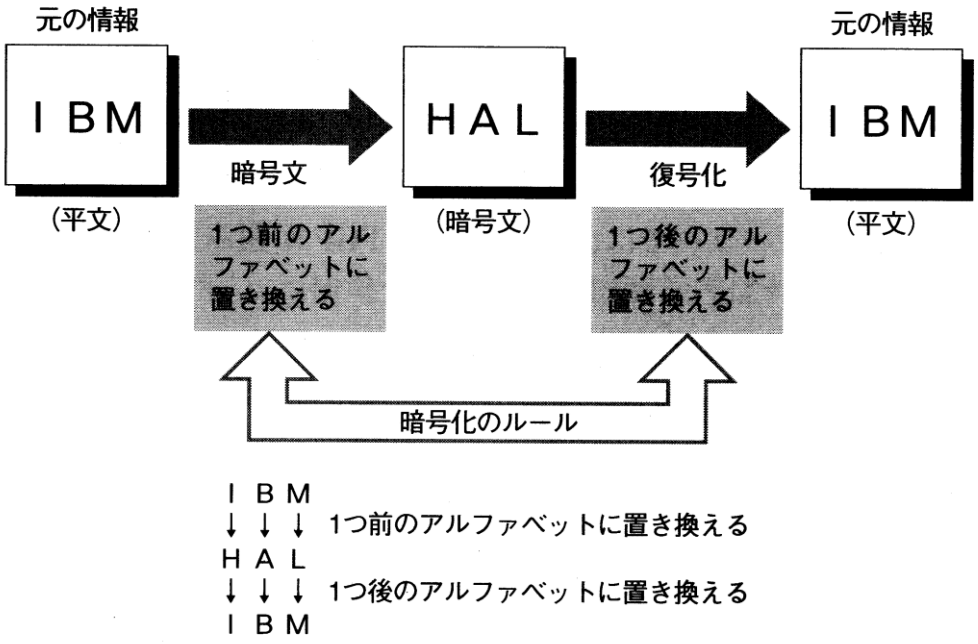
盗聴リスクと暗号化

ネットワークシステムの運用では、常に盗聴のリスクがあり、このリスクを許容可能範囲に留める対策として、暗号化がある

- **暗号化**
  情報(平文)を特定の条件のみ、復元可能な一定の規則で変換し、一見して無意味な情報とする
- **復号**
  暗号化した暗号文を、元の情報に戻す

暗号の基本と種類

暗号化アルゴリズムでは、暗号化や復号するための特定の条件を鍵（キー）と呼び、ビット列で表現する。この鍵を、情報にアクセスすることを許可されている人だけが保持することで、許可されていない人への情報漏えいを防ぐことができる。



暗号化では、鍵の取扱いが非常に重要な問題となるので、暗号化の種類は、鍵の取扱い方の違いよって、二種類に分かれる

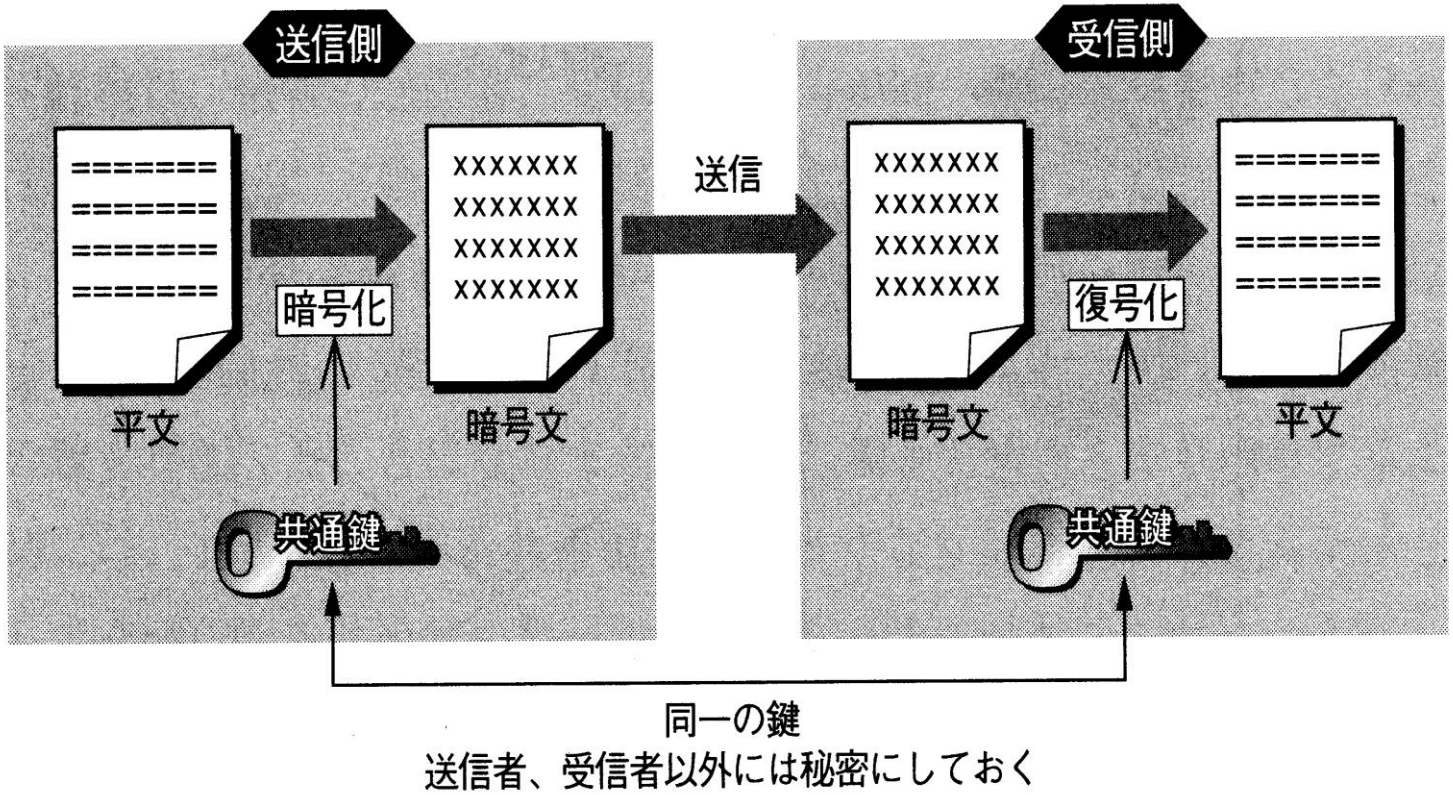
- **共通鍵暗号化方式**
- **公開鍵暗号化方式**

共通鍵暗号　テキストP64-67

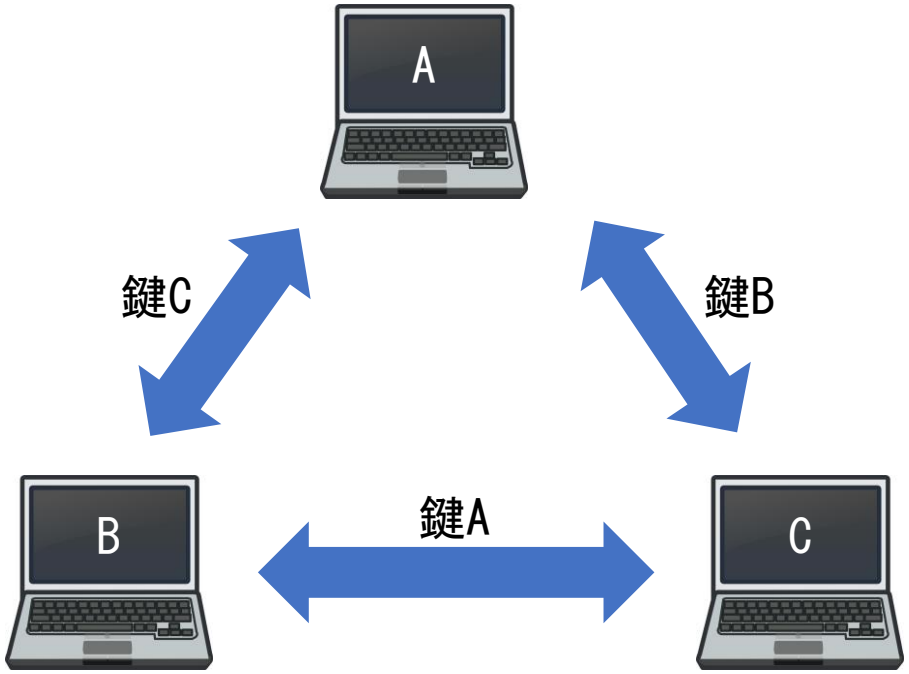
共通鍵暗号化方式(Common key cryptosystem)

共通鍵(秘密鍵)

送信者と受信者が共通の鍵(キー)で本文を暗号化するが、鍵の交換に問題がある



共通(秘密)鍵の数



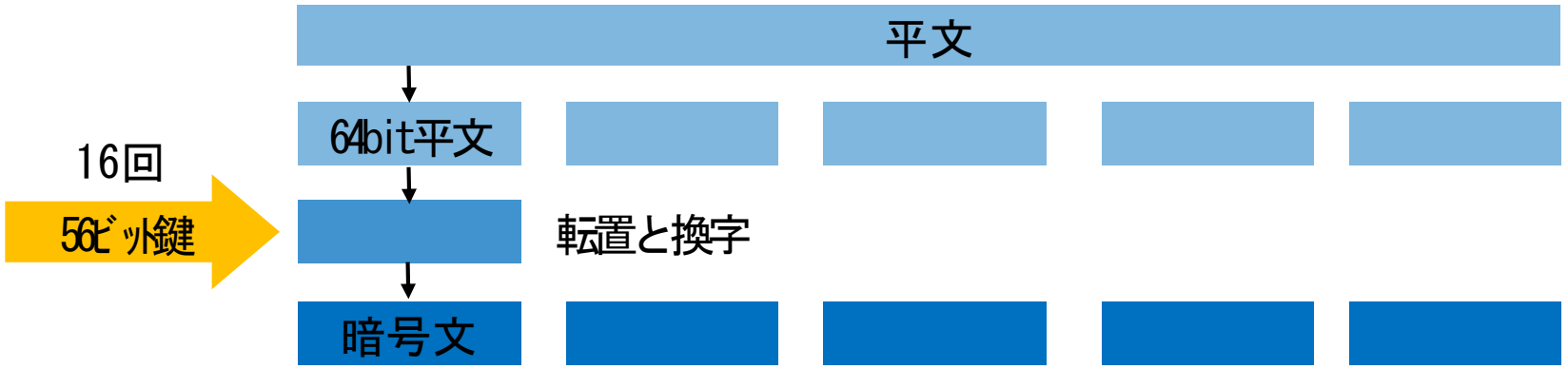
通信ペアごとに異なる鍵が必要となるので、通信する人数がn人の場合は、$\frac{n(n-1)}{2}$個の鍵が必要となる

共通鍵暗号化方式の実装技術(種類)

DES(Data Encryption Standard)

1977年にIBMが開発し、アメリカ連邦政府標準の暗号方式として採用された、共通鍵(秘密鍵)暗号方式の一つ

データを64ビット単位(ブロック)に区切り、さらに、ブロックを32ビットごとに分割する。これらを、鍵を使って転置と換字を16回繰り返して暗号文にする。鍵の長さは、56ビットである。



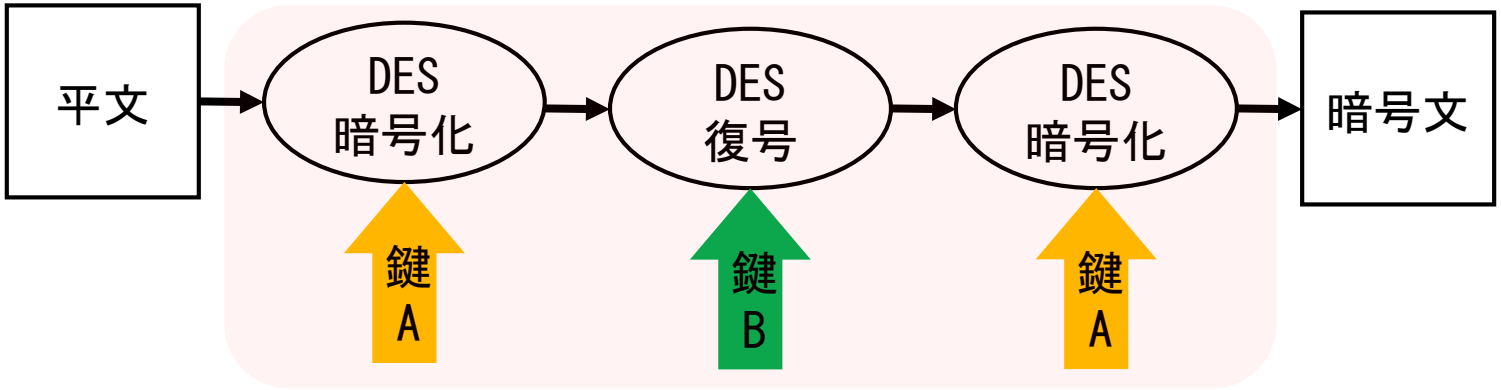
- 鍵の数と危殆化

鍵の数=2^{56} ＝ 約7京(7×10^{16})

危殆化(きたいか)：技術の進歩により暗号化の強度が低下すること

TripleDES

異なる2つの暗号鍵を用いて、DESによる暗号化と復号の処理を3回繰り返すことにより解読されにくくしたもの



AES(Advanced Encryption Standard)

アメリカ国立標準技術研究所(NIST:National Institute of Standards and Technology)が2001年に、DESに代わる標準暗号化方式として公募によって定めた。

AESもブロック暗号で、ブロック長は128ビット、鍵長は128ビット・192ビット・256ビットの3つが利用できる。

共通(秘密)鍵の管理

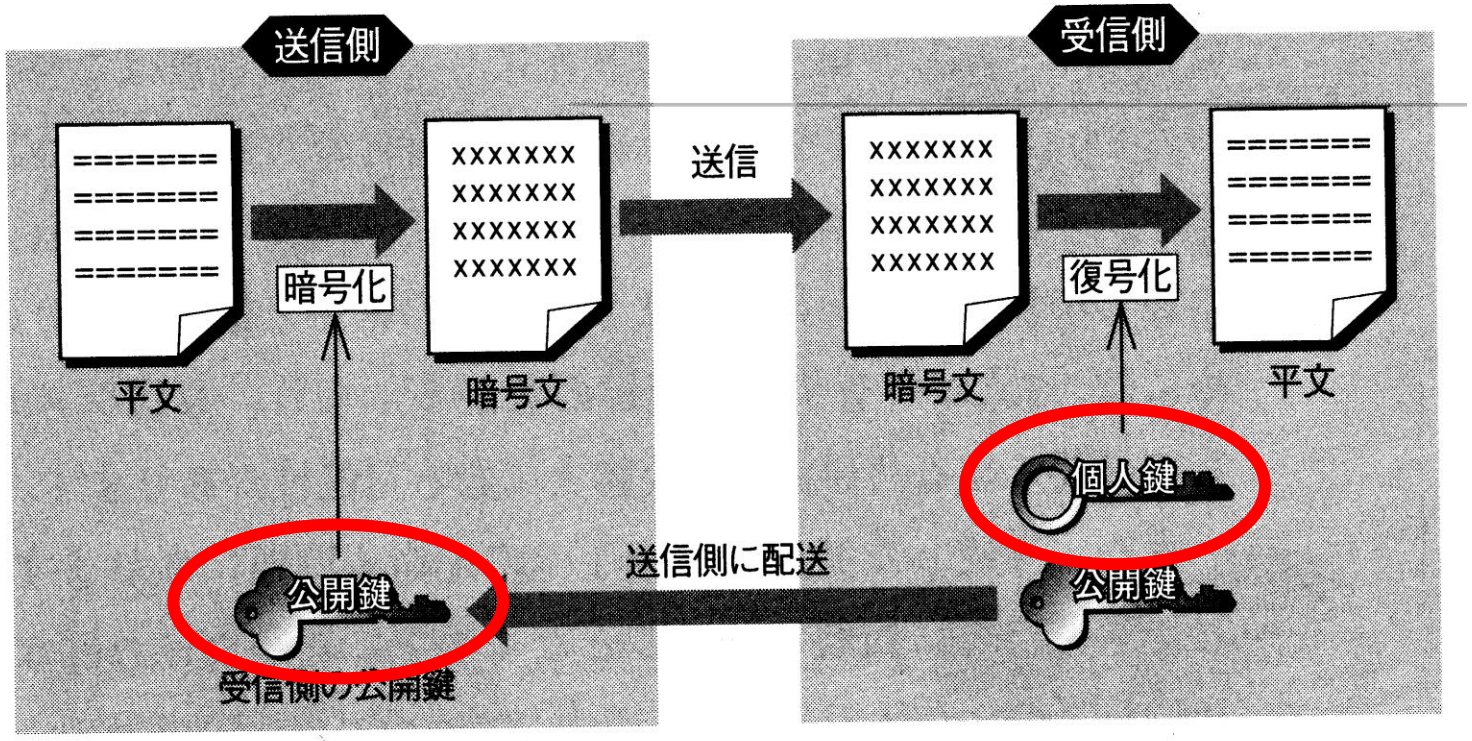
共通鍵の管理は、原則は「プライバシー保護」「真正性の確保」の観点から、ユーザ本人に任せるべきではあるが、取り扱いの不備(紛失など)から業務継続に重大な障害となる場合がある。

ユーザのセキュリティリテラシが充分に備わるまで、セキュリティ管理部門で鍵を一括管理する必要がある。

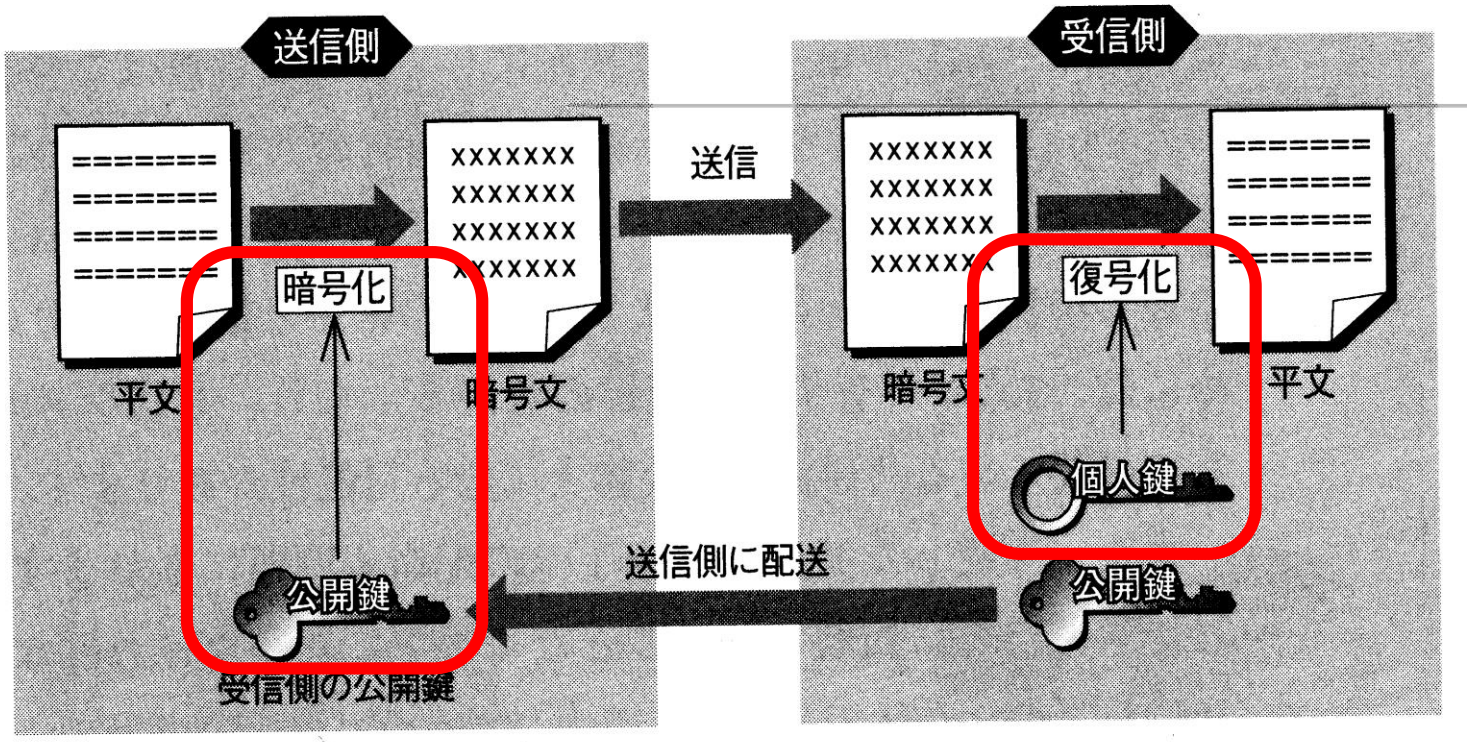
公開鍵暗号　テキストP62-63

公開鍵暗号化方式(public key encryption system)

対になる2つの鍵(公開鍵,秘密鍵(個人鍵))を使ってデータの暗号化・復号を行う



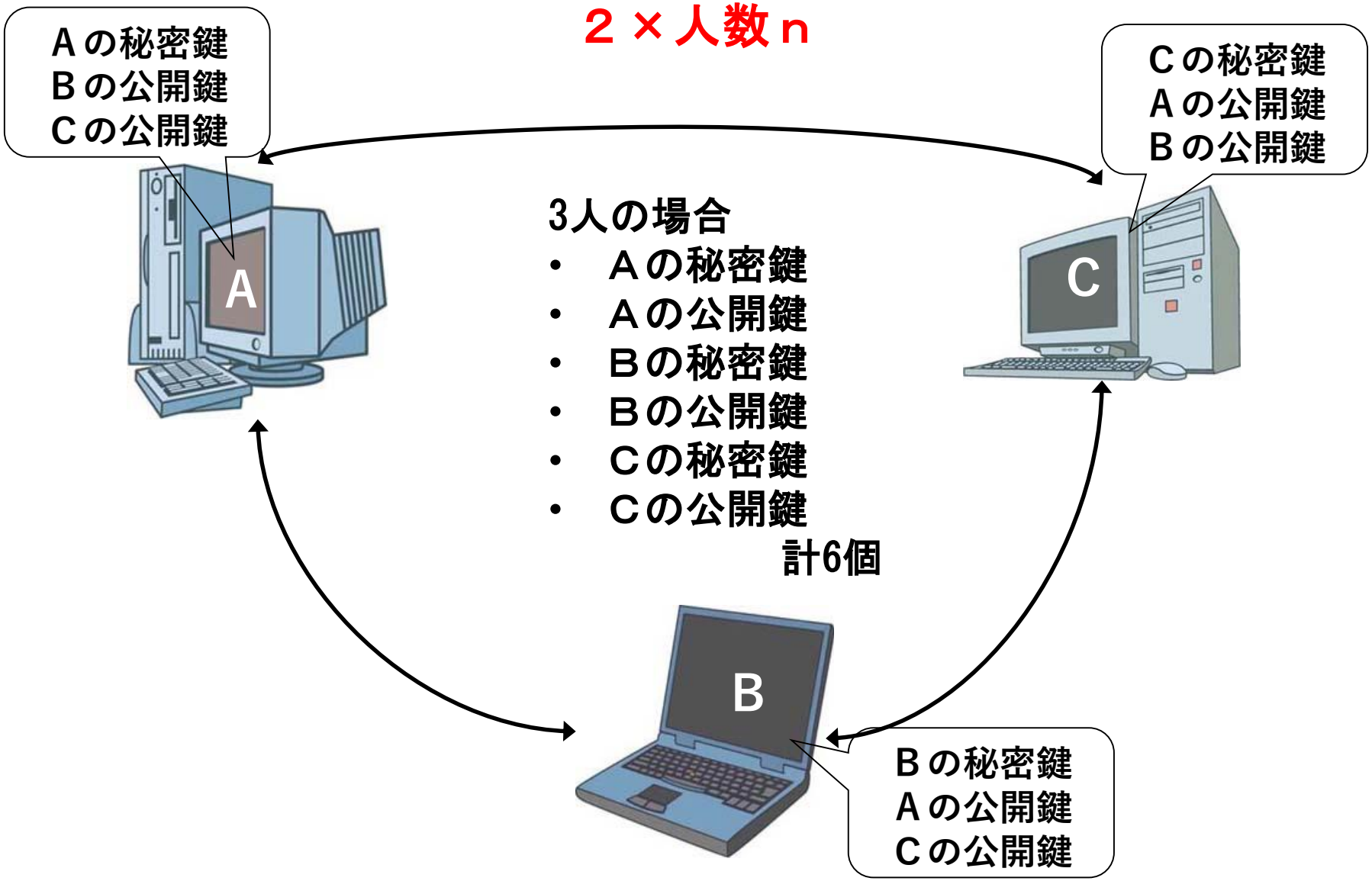
公開鍵暗号化方式の仕組み



一般に公開されている鍵（公開鍵）を使って平文を暗号化し、公開鍵を基にして作成した秘密（個人）鍵を使って復号する

公開鍵暗号化方式の管理鍵数

２×人数ｎ



公開鍵暗号化方式の実装技術(種類)

RSA(Rivest-Shamir-Adleman cryptosystem)

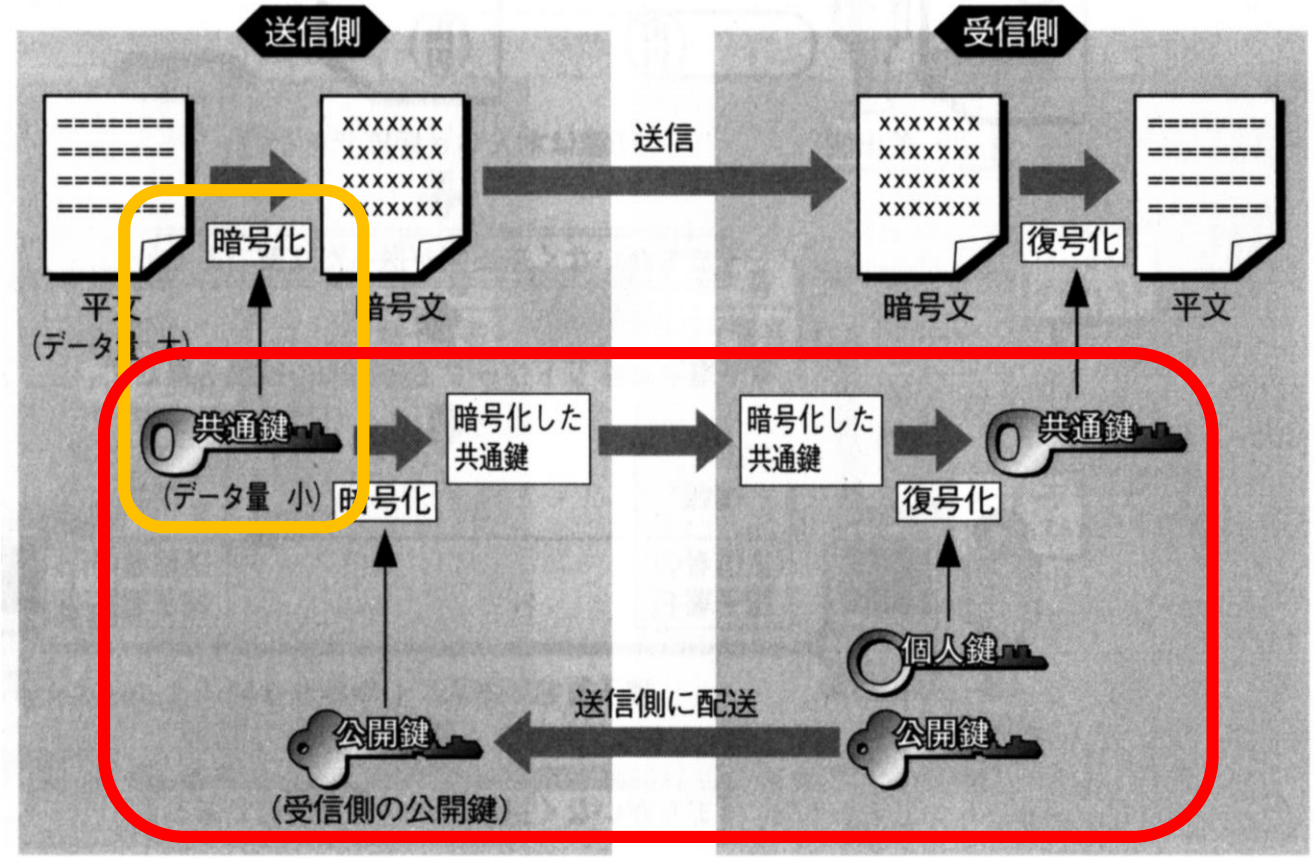
大きな素数同士をかけ合わせた整数を素因数分解するのが困難であることを利用した公開鍵暗号の一つ

楕円曲線暗号(ECC:Elliptic Curve Cryptosystem)

1985年にKoblitz氏とMiller氏が、ほぼ同時に独立に考案した公開鍵型の暗号方式で、楕円曲線と呼ばれる数式によって定義される特殊な加算法に基づいて暗号化・復号を行う

ハイブリッド方式

平文を共通鍵暗号化方式で暗号化し、暗号化するために使用する共通鍵を公開鍵暗号化方式で暗号化して受け渡す



認証

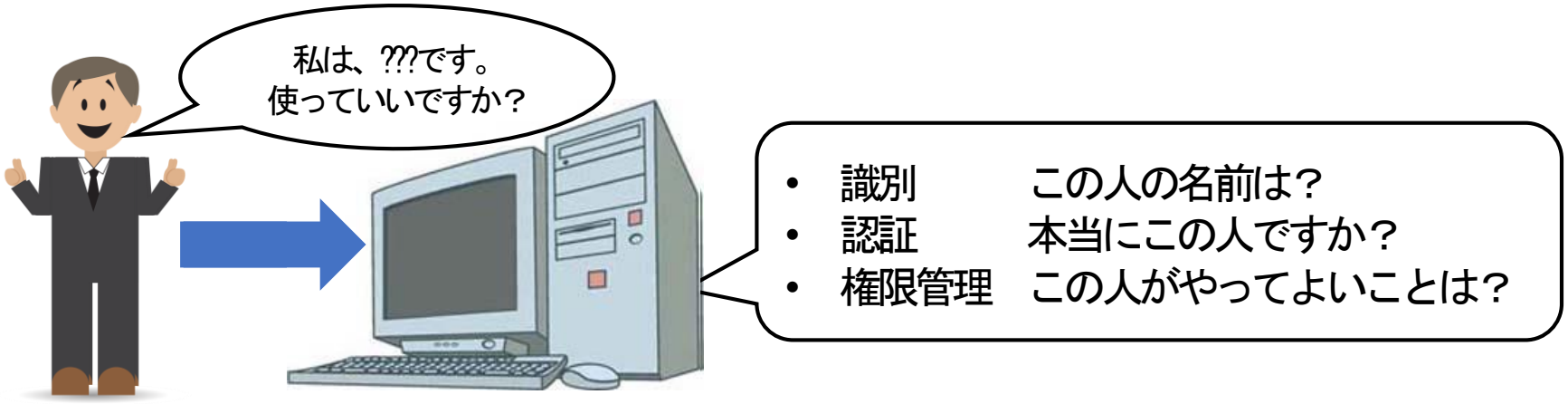
1. 認証の基本
2. ワンタイムパスワード
3. パスワードの欠点
4. バイオメトリクス
5. ディジタル署名
6. PKI

認証の基本

テキストP74-78

アクセスコントロールと認証システム

ユーザの識別、認証、権限管理を行うことを、アクセスコントロールと呼び、アクセスコントロールを実現するシステムを、認証システムと呼ぶ



識別

どのユーザがアクセスしようとしているか？を認識する

ユーザのシステムの利用可否、機能やデータの使用に関する権限を判断でき、通常ユーザIDを用いて、確認する

認証

システムを利用するユーザが、確かに本人であるか？正当な利用権限を持っているか？を確認する

認証方法

- 知識による認証(知識情報(ユーザID, パスワードなど)による認証)
- バイオメトリクス認証(生体情報(指紋, 声紋など)による認証)

権限管理

アクセスを許可していないデータに対して、むやみにアクセスできないように、ユーザの権限（アクセス権）を設定してコントロールする

ディレクトリ＼ユーザ	営業部員	総務部員	管理者
営業部	読可，書可	権限無	読可，書可，消可
総務部	権限無	読可，書可	読可，書可，消可
社内掲示板	読可，書可	読可，書可	読可，書可，消可

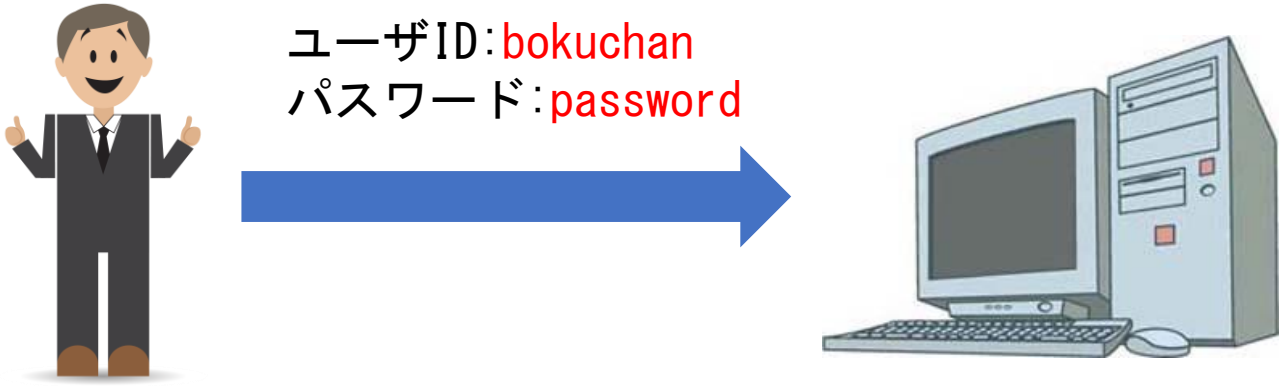
個々のユーザについての権限や所属グループについての権限も設定できる

パスワード認証

クリアテキスト(パスワード)認証

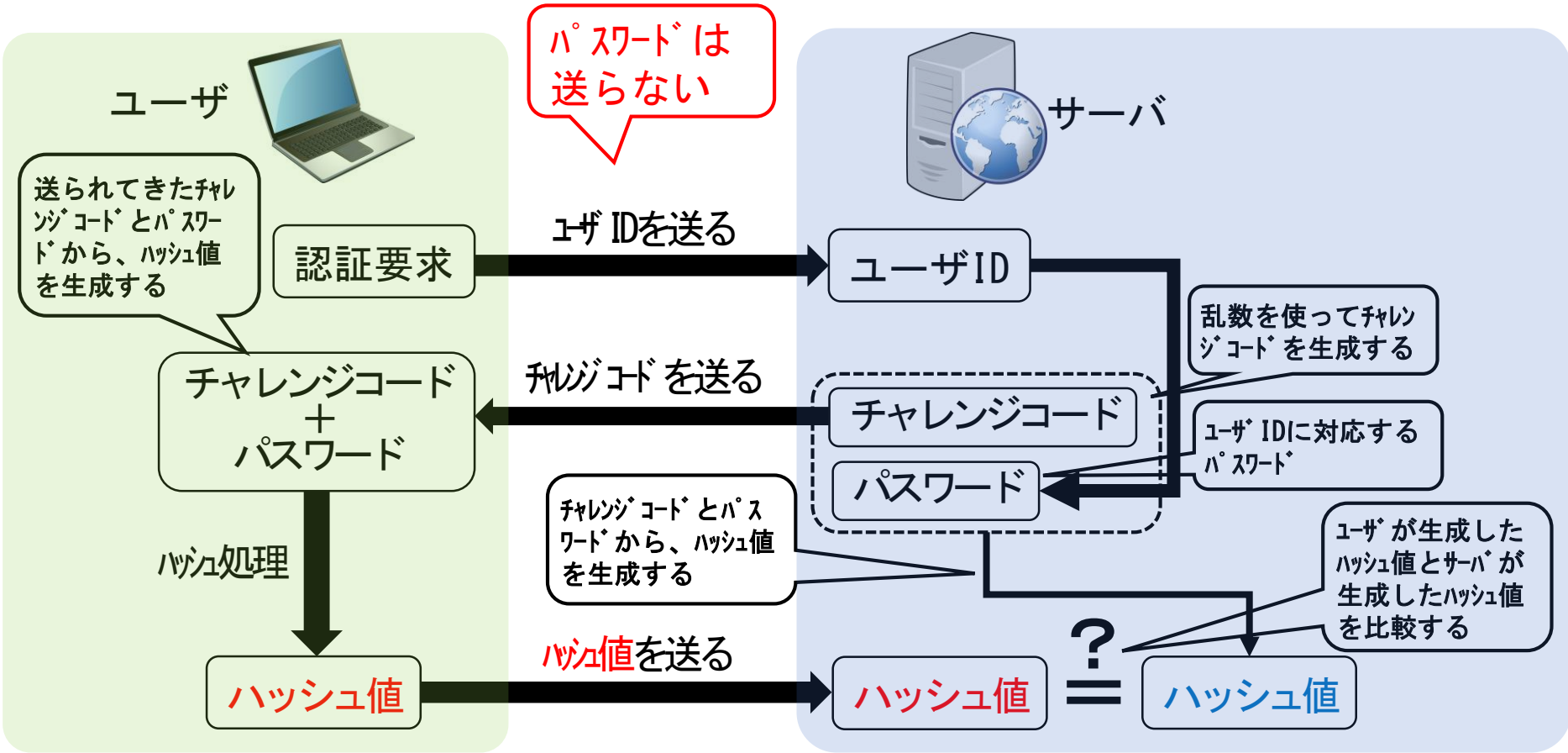
ログインするときに、サーバへ平文(暗号化しない)でユーザIDやパスワードを送る

ユーザIDとパスワードで認証する方式であるPPP(Point to Point Protocol)の一種のPAP(Password Authentication Protocol)などの認証方式で採用されている



チャレンジレスポンス認証

① クライアントからサーバに対して、ユーザIDを送信する
② サーバが、チャレンジコードをクライアントに返信する
③ クライアントは、ハッシュ値をサーバに返信する



チャレンジレスポンス認証の利点

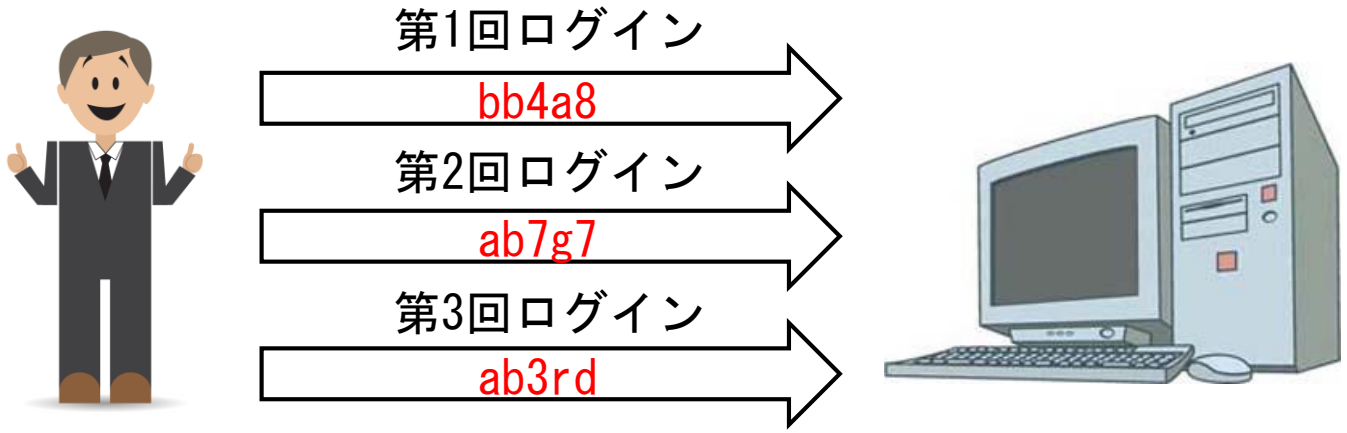
　ネットワーク上にはパスワードが流れず、また、チャレンジコードは使捨てなので、クラッカーは不正アクセスすることができない。この認証方法を採用したCHAP(Challenge Handshake Authentication Protocol)がある。

ワンタイムパスワード

テキストP79-81

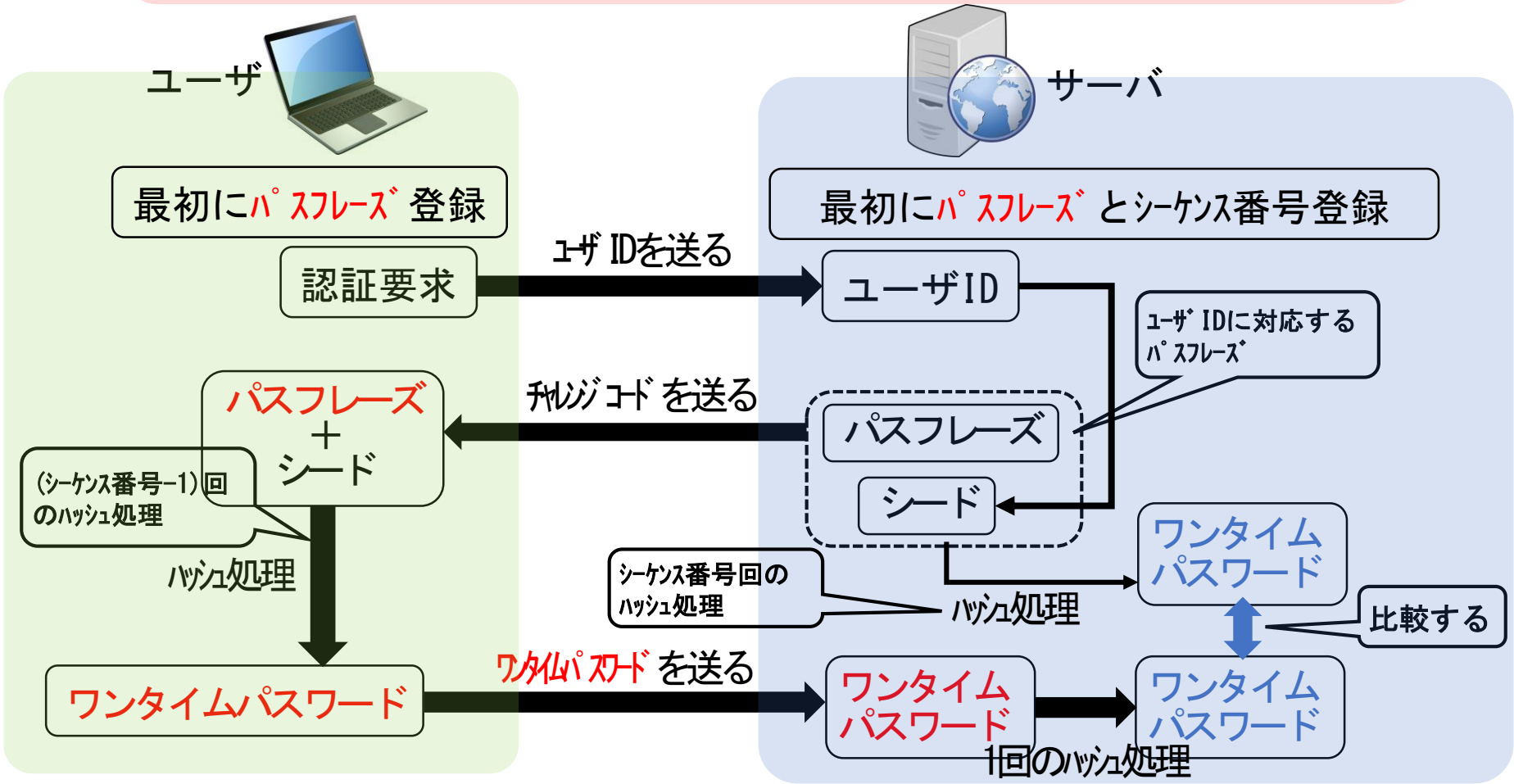
ワンタイムパスワード

ログインするたびに新しいパスワードを使う



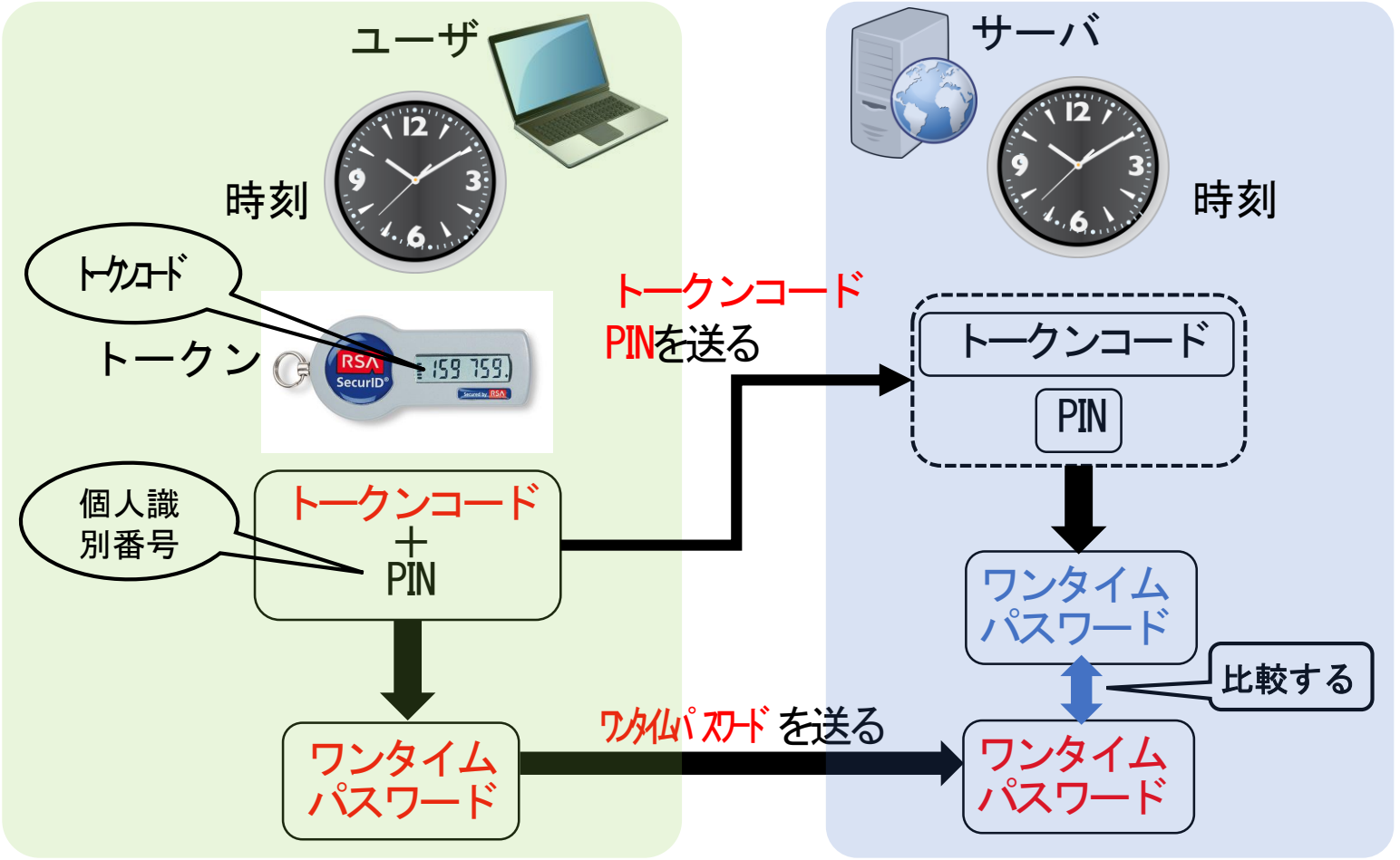
S/KEY

「チャレンジレスポンス認証」と類似した方式で、ユーザとサーバの間で、シード（チャレンジコードと同じ、使い捨て乱数）とパスフレーズ及びシーケンス番号（やり取りの回数）を利用して認証する



時刻同期方式

チャレンジコードの代わりに、時刻をトリガとして使用して認証する



パスワードの欠点

テキストP82-85

パスワード認証の運用

パスワードは実体がないものなので、認証に使うためには、以下の点に注意が必要である。

* ユーザの不注意でパスワードが漏えいする
* 辞書攻撃などにより、利用されやすいパスワードが推定される
* 総当たり攻撃により、すべてのパスワードがチェックされる

パスワード作成上の要件

パスワード認証は、様々なリスクに対応するため、以下の要件を満たして運用する必要がある。

* 漏えいを防ぐため、メモなどに書き残さない
* 漏えいや盗聴の被害を最小限度に留めるため、頻繁に変更する
* 辞書攻撃などの対象になりそうなパスワードは使用せず、できる限り複雑で長いものを用いる
* 総当たり攻撃に対処するため、数回の入力ミスで、該当ユーザIDを利用不可にする
* ショルダーハッキングに対処するため、タイプ入力時間は短くする

パスワード作成要件の矛盾

強力なパスワードの基準(Windowsの場合)

対象	内容
文字数	少なくとも8文字以上
文字	以下のものをすべて含む • 文字(大文字):A,B,C,・・・ • 文字(小文字):a,b,c,・・・ • 数字:0,1,2,・・・ • 記号:’ ~ ! @ # $・・・
その他	• 以前使っていたパスワードと異なる • 名前またはユーザ名を含まない • 一般的な単語または名前でない

パスワード管理ツール

近年、多くの人達が、多くのパスワードを保持し、利用することが多くなってきた。これに伴って、パスワードの管理負担やリスクが大きくなった。

パスワード管理ツール（アプリ）は、パスワードの「保存」「自動入力」「強度のチェック」や「強制変更」などの機能がある。

パスワードリマインダ

パスワードを忘れたときに、復旧するための機能。

復旧するためには、「秘密の質問」などのユーザしか知らない情報を入力させるなどして、ユーザに代替認証を促した後、パスワードをリセットするなどの処置を施す。

ユーザID発行上の注意

ユーザIDの決め方

通常、ユーザIDは管理し易さから、一定の規則に従って作成されている。ランダムな規則で作成すれば、クラッカーは、ユーザIDを特定しにくい。

また、管理者権限を持つもののユーザIDは、adminやrootは使うべきではない。

ユーザIDの管理

ユーザIDは、適切にライフサイクルコントロールする。異動や退職など、システムの利用権限を失ったときには、速やかにかつ確実に回収する必要がある。また、一度利用権限を失ったユーザIDは、再度利用することは避ける。

ログインの状態(成功や失敗)は、ログで記録を取り、一定回数以上のログイン失敗には、該当ユーザIDを使用不可にする。

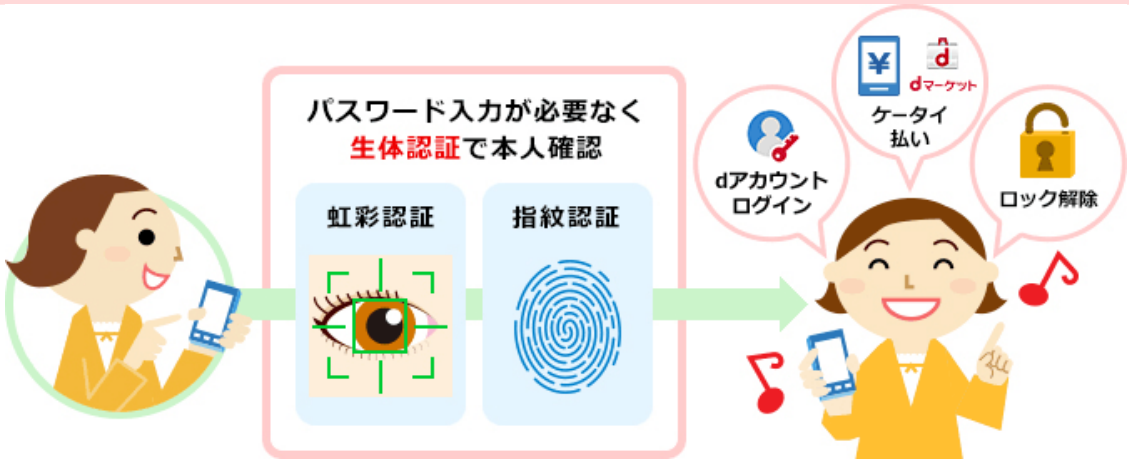
バイオメトリクス

テキストP86-87

バイオメトリクス認証

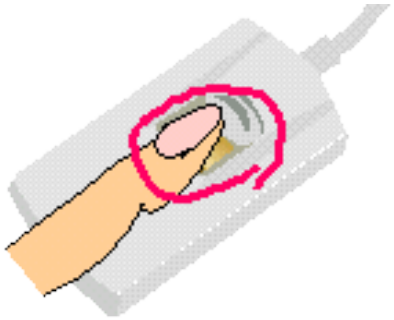
人間の生体情報（指紋や虹彩など）を使って本人認証する。

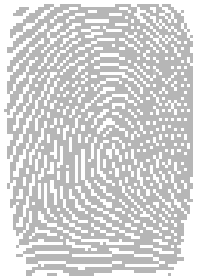
人間の生体情報（指紋や虹彩など）は、個体によって特徴があり、本人を正確に識別できる。また、この情報は、盗難や置き忘れなどの心配がない。

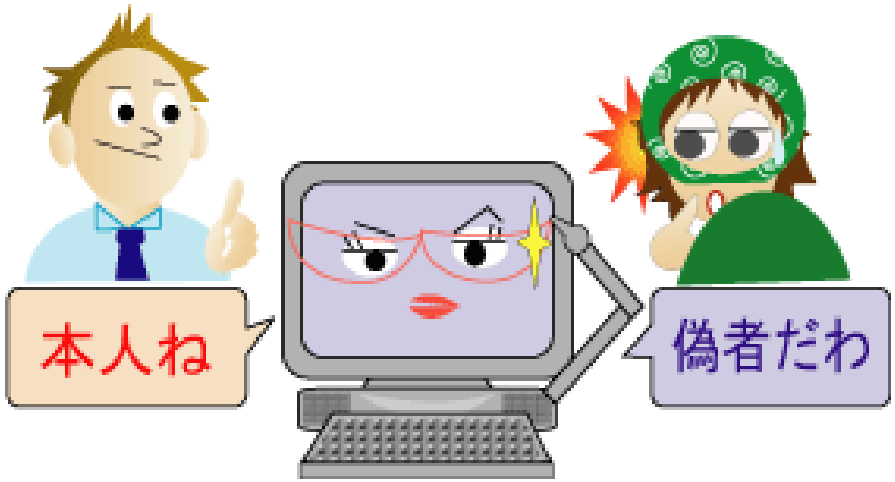


指紋(認証)

指紋の形をトポロジ(位相)として認識する。
古くから犯罪捜査などで、本人認証として使用され、近年、コンピュータによって精度の高い識別が可能となったが、コピー可能なことから、他の生体情報(体温や皮脂成分など)と併用して使用することが多い。



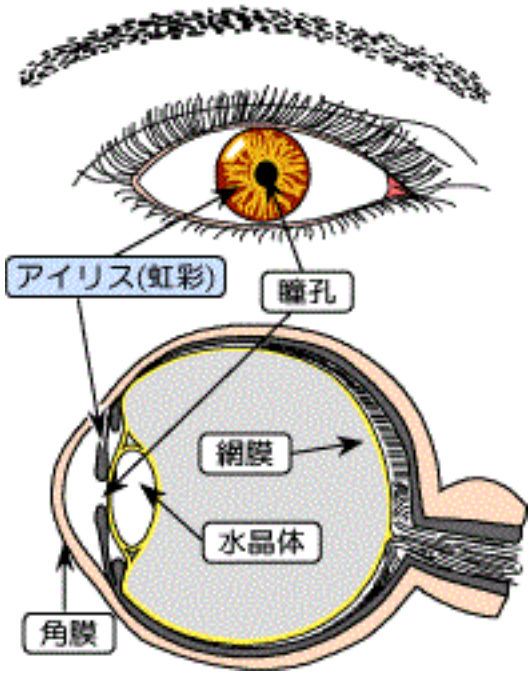




虹彩(認証)

眼球の角膜と水晶体の間にある輪状の薄い膜(虹彩:アイリス)を使って認識する。

虹彩は、コピーし難いことから、指紋認証よりも優れている。



声紋(認証)

人間から得られる個体特有な音声波形の特徴を使って認識する。
声紋は、生体の状態(病気や加齢など)によって大きく変化するので、認識誤りが発生することがある。

静脈パターン認証

手のひらや指先の静脈パターンにより本人確認を行う。
静脈内を流れる血液中の還元ヘモグロビンが吸収する近赤外線をあてて指を撮像し、静脈パターンを抽出し、予め登録された静脈パターンとマッチングすることで、認証を行なう。

多要素認証

ユーザの本人認証時に複数の要素を用いて確認する。
認識時の正確性・安全性を高めるため、知識による認証や所持品による認証、生体認証を組み合わせて、本人認証する。

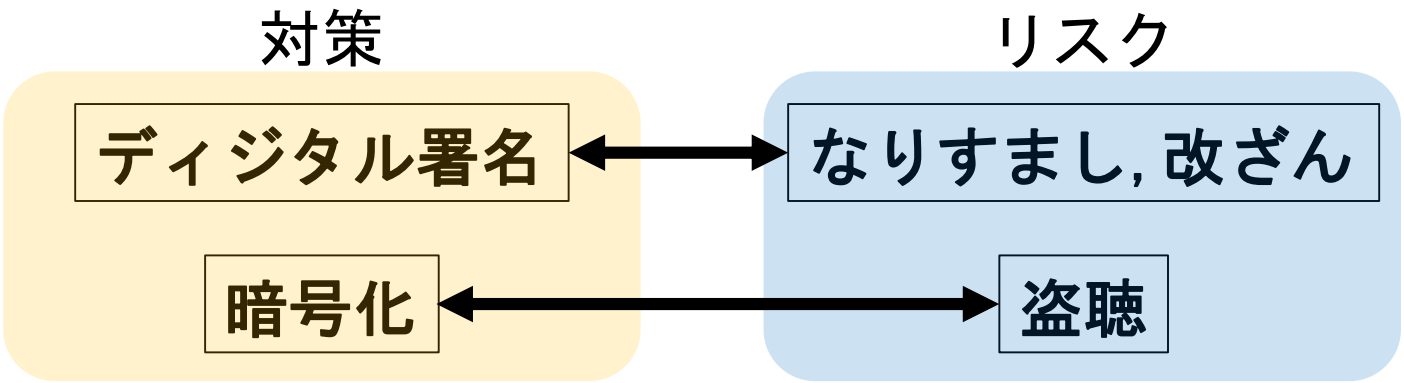
ディジタル署名

テキストP88-92

ディジタル署名とは

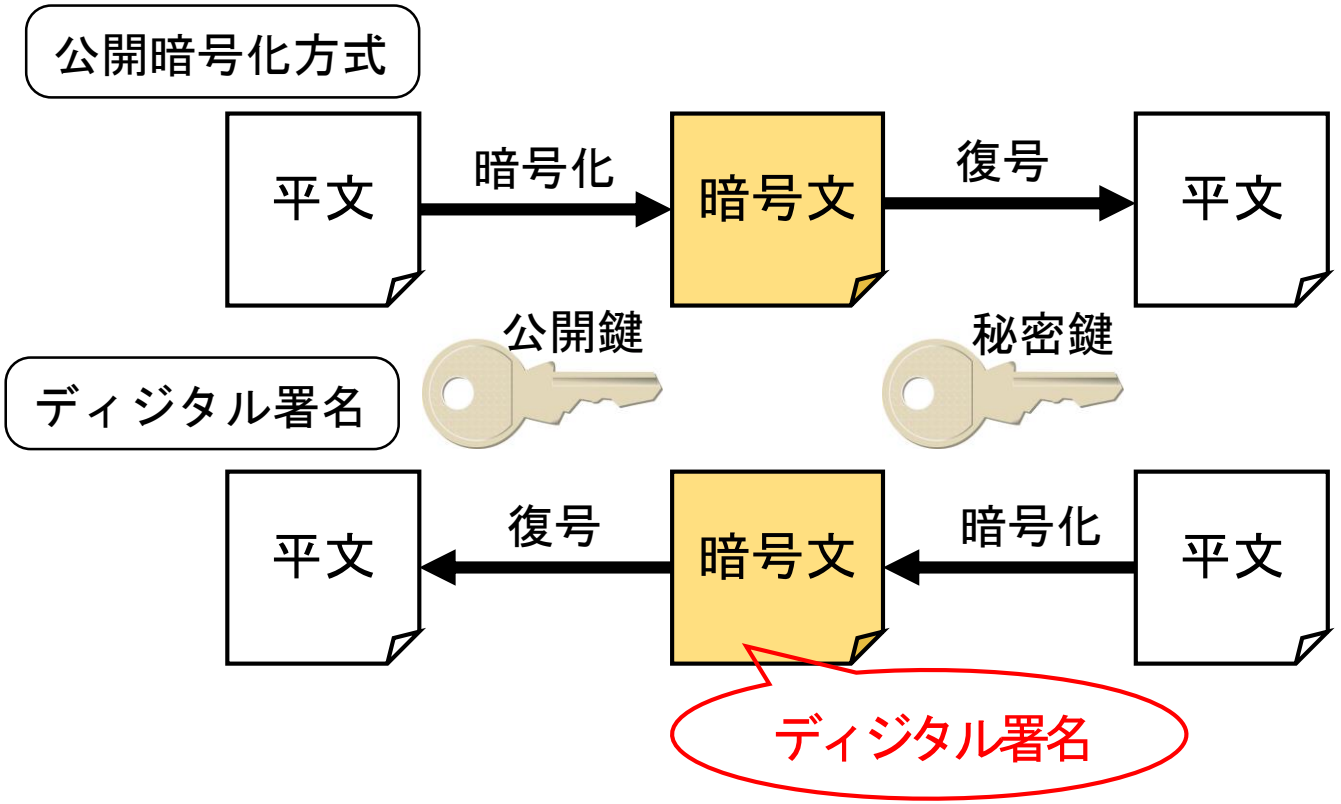
送られてきたデータの送信元データが間違いないか、送る途中でデータが改ざんされていないかを確認する。

ディジタル署名は、「なりすまし」と「改ざん」の対策に用いられる。

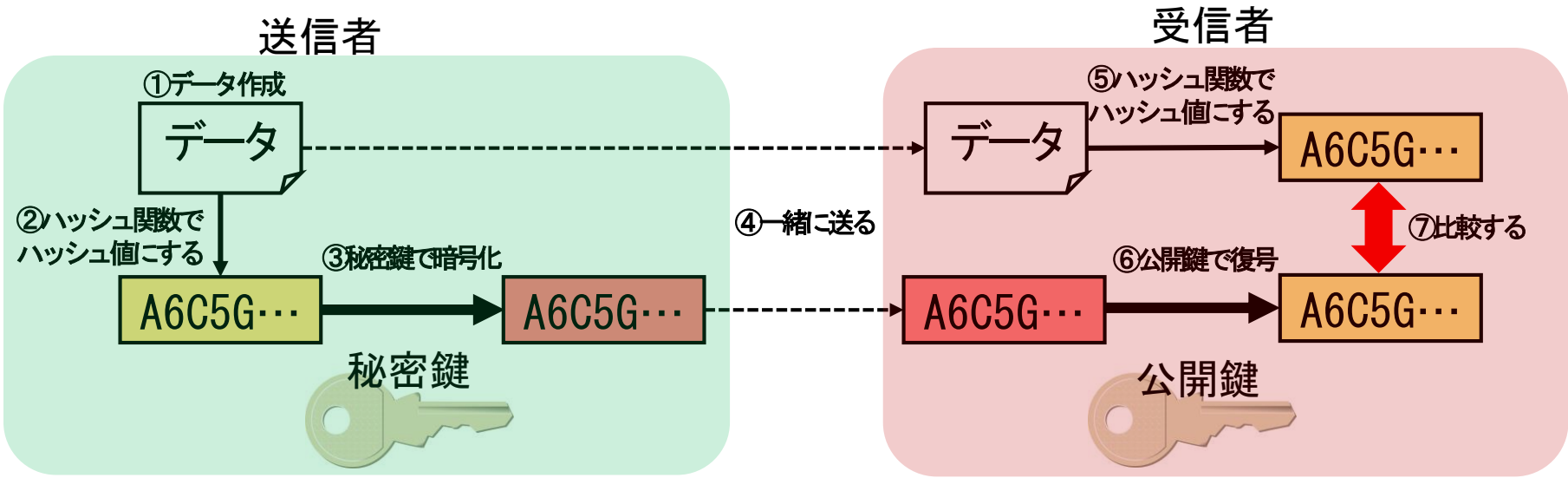


公開鍵暗号方式では、送信者は、暗号化の鍵として公開鍵を用い、復号の鍵として秘密鍵を用いる。

これに対して、ディジタル署名では、平文に秘密鍵を用いて暗号化して、ディジタル署名を作成する。



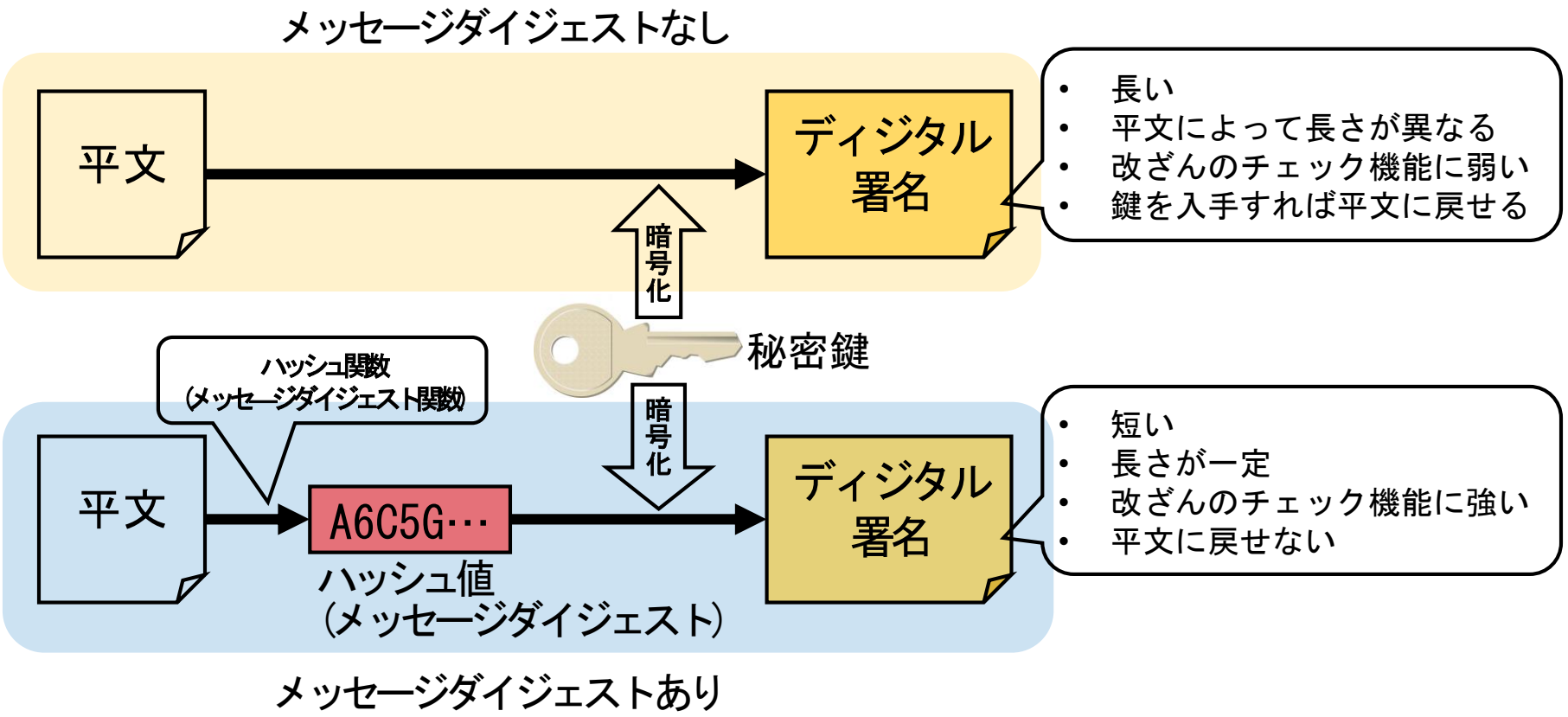
ディジタル署名の仕組み



① 送信者は送信するデータを作成する
② 作成したデータを基にハッシュ関数を使ってハッシュ値を算出する
③ ハッシュ値を送信者の秘密鍵を使って暗号化する。このときに利用するのは公開鍵暗号方式。
④ ①で作成したデータと③で作成した「送信者の秘密鍵で暗号化したハッシュ値」を一緒に受信者に送る
⑤ 受信者は、受信データを基に、送信者が使ったものと同じハッシュ関数を使ってハッシュ値を算出する
⑥ 送信者が送った「送信者の秘密鍵で暗号化されたハッシュ値」を、あらかじめ入手していた送信者の公開鍵で復号する
⑦ ⑤で算出したハッシュ値と、⑥で復号したハッシュ値を比較する。
⑧ 両者が一致すれば、「送る途中でデータが改ざんされていない」「送信者が正しい」ということを確認できる

メッセージダイジェスト

ディジタル署名を作成する際に、平文をハッシュ関数で規則性のない固定長の値(ハッシュ値)にして、作成した、メッセージの要約(メッセージダイジェスト)



MD5(Message Digest 5)

任意の長さの平文を元に、128ビットの値を生成するハッシュ関数(要約関数)

SHA-1(Secure Hash Algorithm 1)

任意の長さの平文を元に、160ビットの値を生成するハッシュ関数(要約関数)

SHA-2(Secure Hash Algorithm 2)

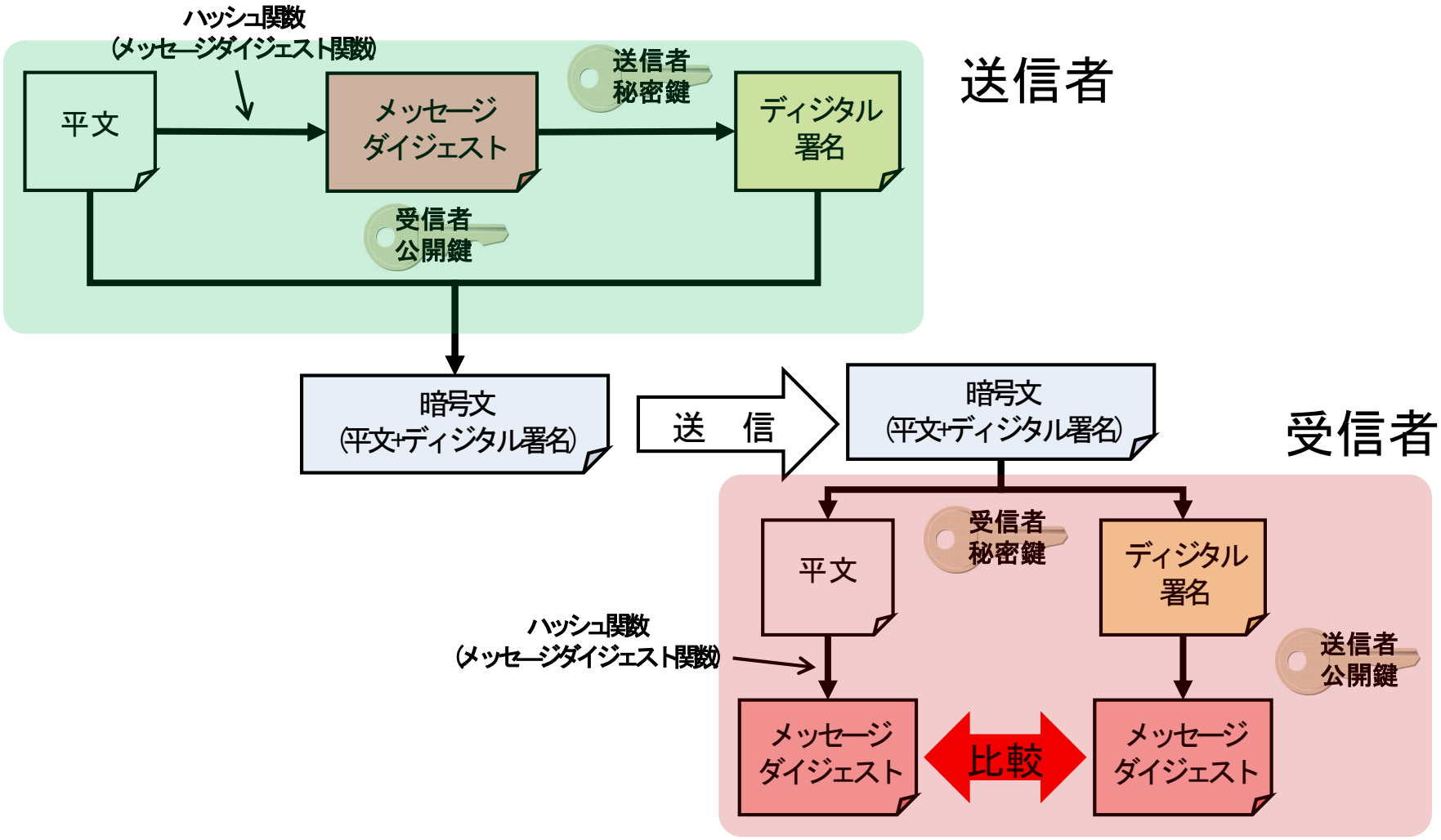
任意の長さの平文を元に、224ビット、256ビット、384ビット、512ビットの値を生成するハッシュ関数(要約関数)

MAC(Message Authentication Code)

メッセージダイジェストを作る時に、平文とMAC鍵を足したデータを対象にする

ディジタル署名と公開鍵暗号方式の複合

セキュリティを強固にするため、ディジタル署名を公開鍵暗号方式で暗号化してから送信する

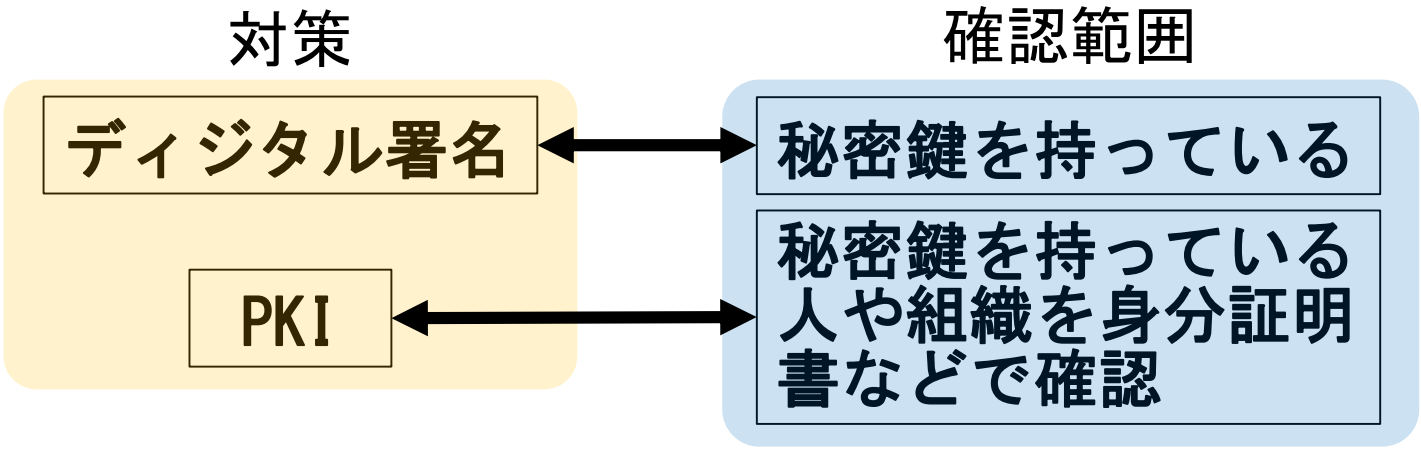


公開鍵基盤
(PKI:Public Key Infrastructure)

テキストP93-96

ディジタル署名の弱点

　ディジタル署名は、メッセージ送信者が秘密鍵を持っていることを証明するものだが、この秘密鍵を持っている人が必ずしも、本人(メッセージ送信者本人)とは限らない。
　また、秘密鍵やこの鍵とペアとなる公開鍵も、偽造された場合もある。



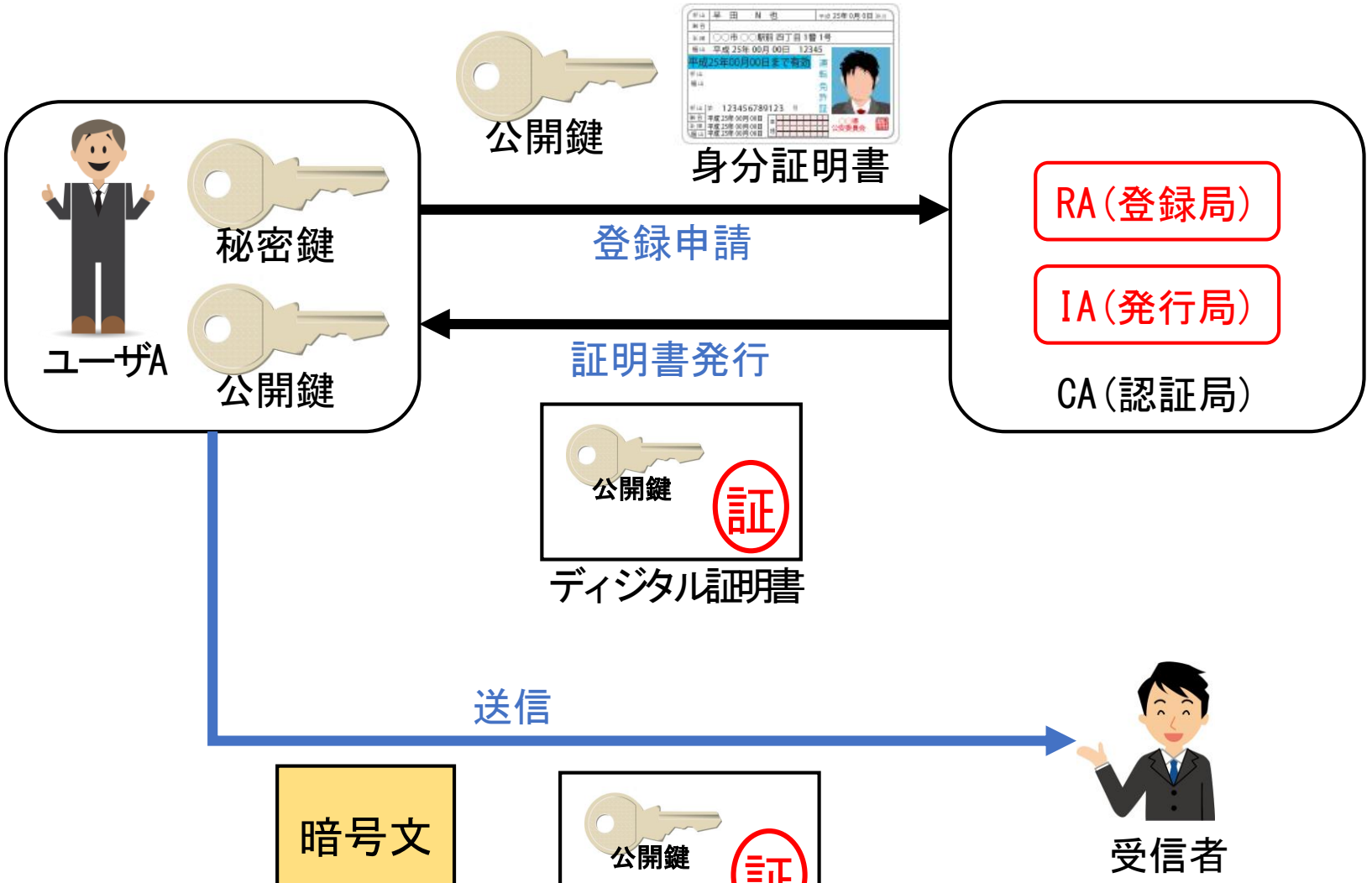
PKI

PKI(公開鍵基盤)とは、公開鍵や秘密鍵が確実に本人のものであることを、第三者機関の介入により証明すること

ディジタル証明書の発行

公開鍵と本人を結び付けるためには、第三者機関が証明書(ディジタル証明書)を発行する。

証明書の発行元を認証局(CA:Certificate Authority)と呼び、ディジタル署名を登録する登録局(RA:Registration Authority)と発行する発行局(IA:Issuing Authority)がある。


公開鍵
身分証明書
秘密鍵
登録申請
RA（登録局）
IA（発行局）
ユーザA
公開鍵
証明書発行
CA（認証局）
公開鍵
証
ディジタル証明書
送信
暗号文
公開鍵
証
受信者
秘密鍵で暗号化
した文書
ディジタル証明書
ディジタル証明書の公開鍵で文書を開く
（認証局の発行したディジタル証明書の
公開鍵で文書を開くことができたので、
ユーザAからであることがわかる）

ブラウザに登録されているディジタル証明書