PKI（公開鍵インフラ）について

㈱アイティフォー

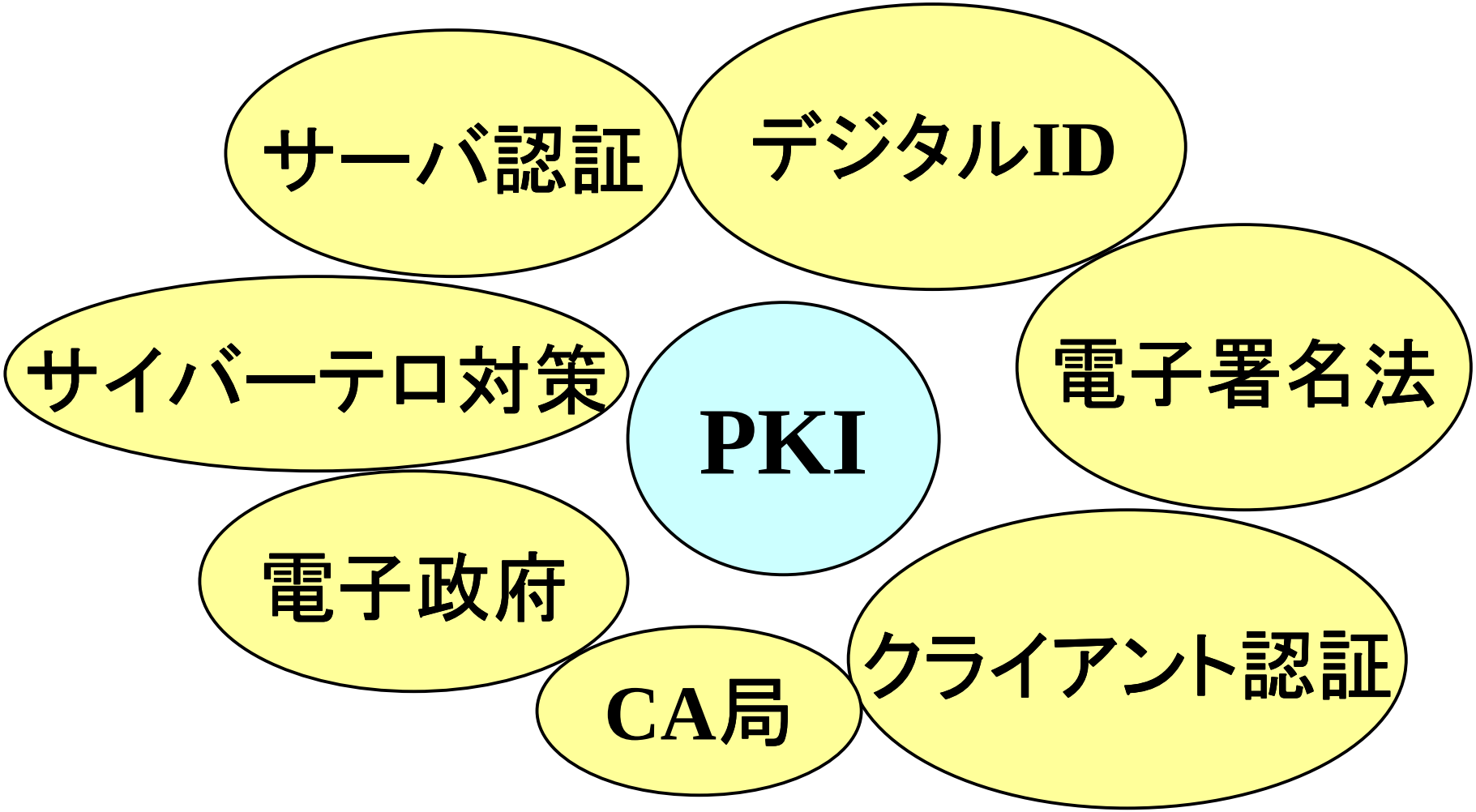
真田　勉

tsanada@itfor.co.jp

ITFOR™

■PKI

最近よく聞く･見る Keyword



ITFOR™

インターネットの問題点

- セキュリティの問題
  - 覗き見される。
  - 相手の認証ができない。「なりすまし」の危険
  - 差し替えられる危険性あり。
- 署名・印がない、(法的)効力がない。
  - 「相手側の事後否認に対し、有効な反論が出来ない。」
  - 結局、大事な書類は紙に印刷・押印している。

■PKI

インターネットは、このままでは
ビジネス（商取引）に使えない！

→PKIの導入へ

ITFOR™

PKI（公開鍵インフラ）の3側面

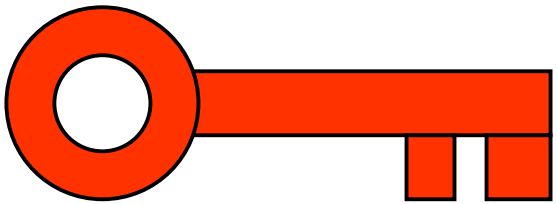
公開鍵方式を利用して、次のことを行なう。

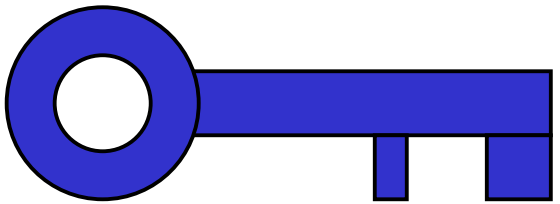
- 暗号化・復号
  - 鍵ペア（公開鍵，秘密鍵）方式
- 署名・検証
  - インターネット世界での（デジタル）署名
- 認証
  - ネット上での「なりすまし」防止

⇒すべて標準化へ

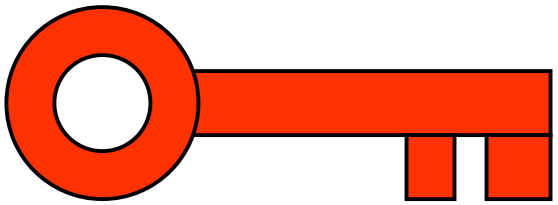
公開鍵による暗号化･復号

- 鍵ペアによる暗号化･復号
  - **Public key**で暗号化 → **Private key**で復号
  - **Private key**で暗号化 → **Public key**で復号
- 非対称性
  - **Private key** は、秘密にすべき
  - **Public key** は、広く公開しても良い



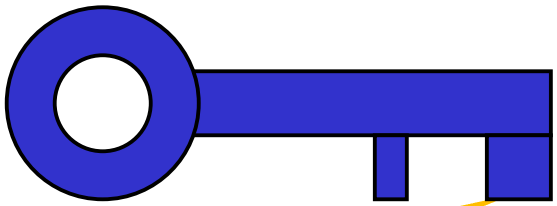


公開鍵暗号方式の特徴

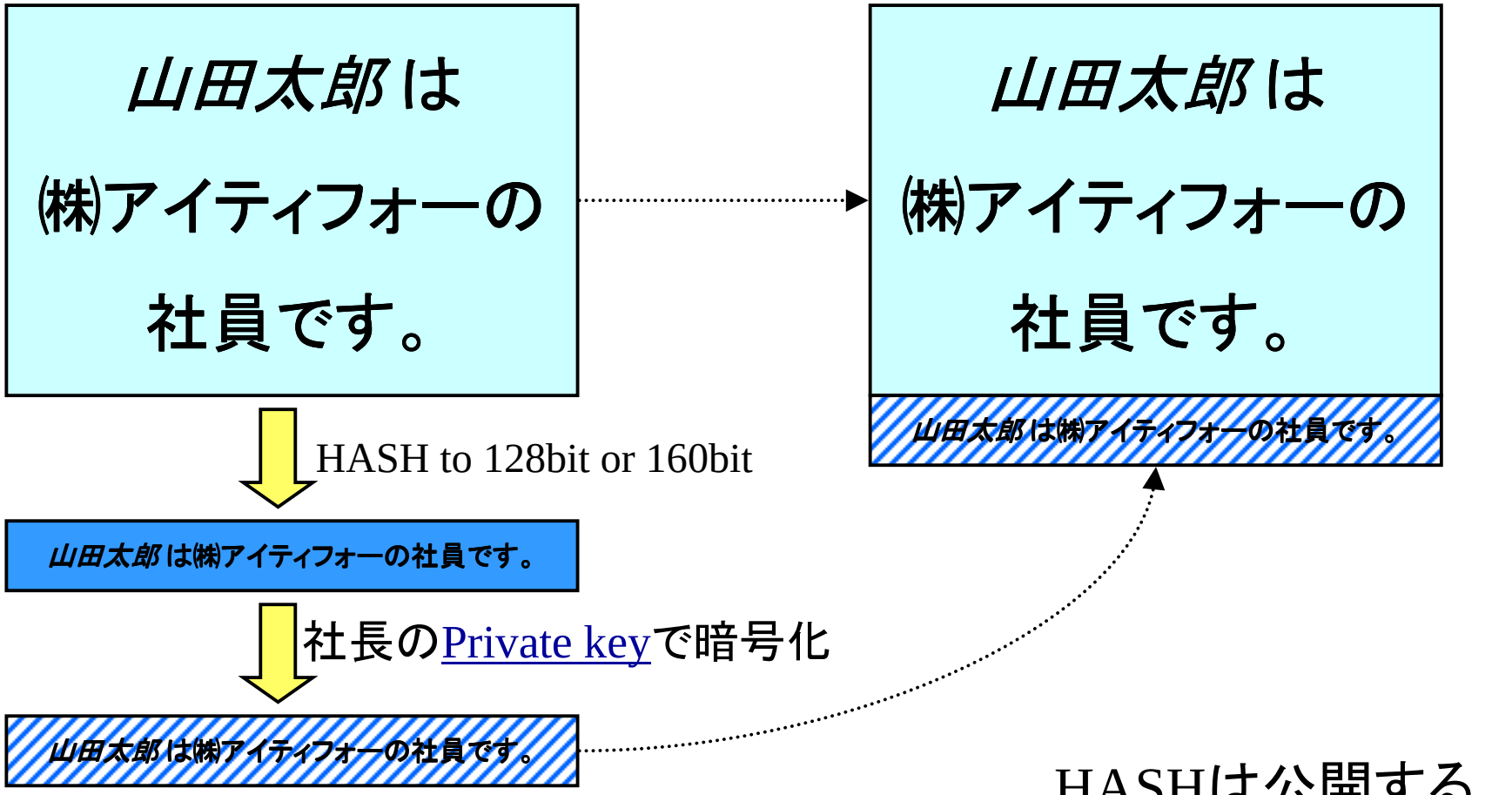


従来の暗号化との違い

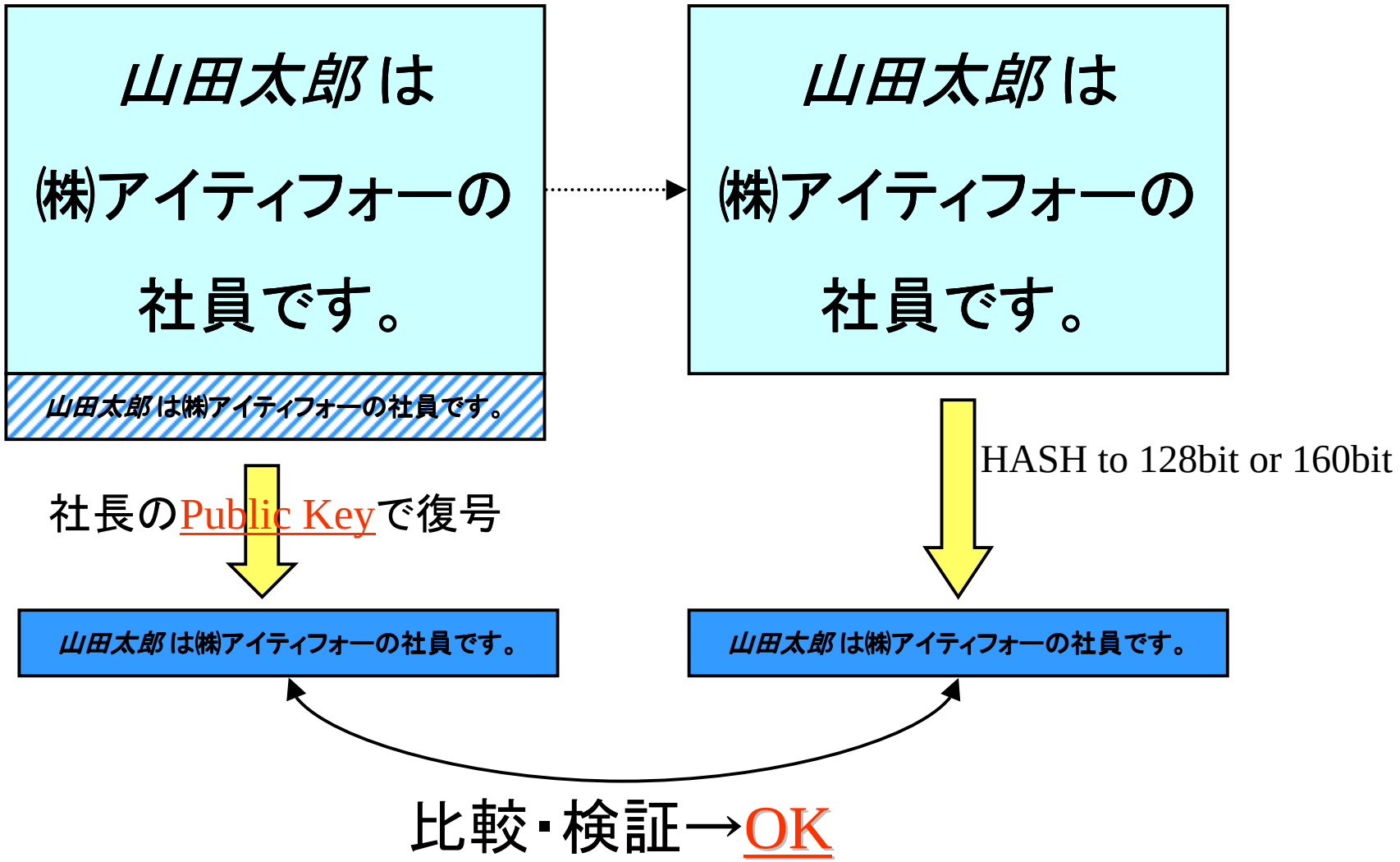
- 暗号用の鍵と復号用の鍵が別々。
- ひとり1ペアの鍵を持てば良い。
- 復号に必要な鍵は、一切インターネット上に流さない。（例外：バックアップ）



公開鍵方式による署名の原理



署名（印）の検証

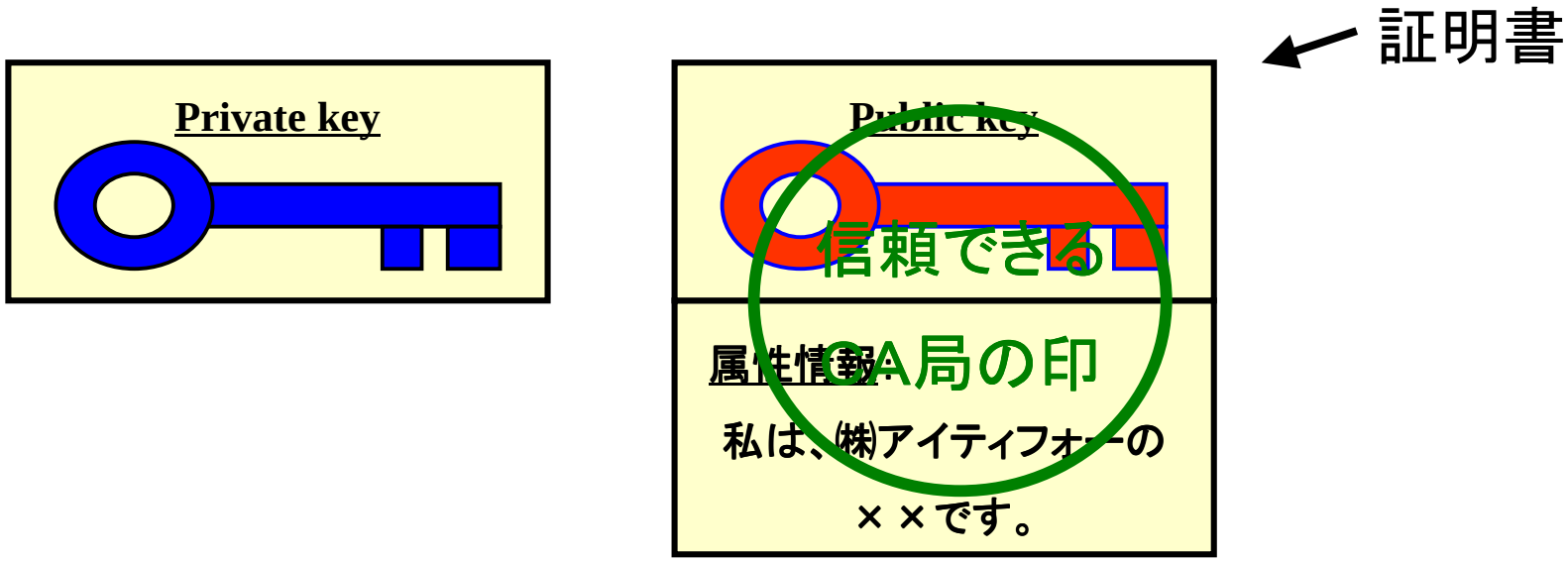

山田太郎は
㈱アイティフォーの
社員です。
山田太郎は㈱アイティフォーの社員です。
山田太郎は
㈱アイティフォーの
社員です。
HASH to 128bit or 160bit
社長のPublic Keyで復号
山田太郎は㈱アイティフォーの社員です。
山田太郎は㈱アイティフォーの社員です。
比較・検証→OK

インターネット世界での署名・押印の仕組み

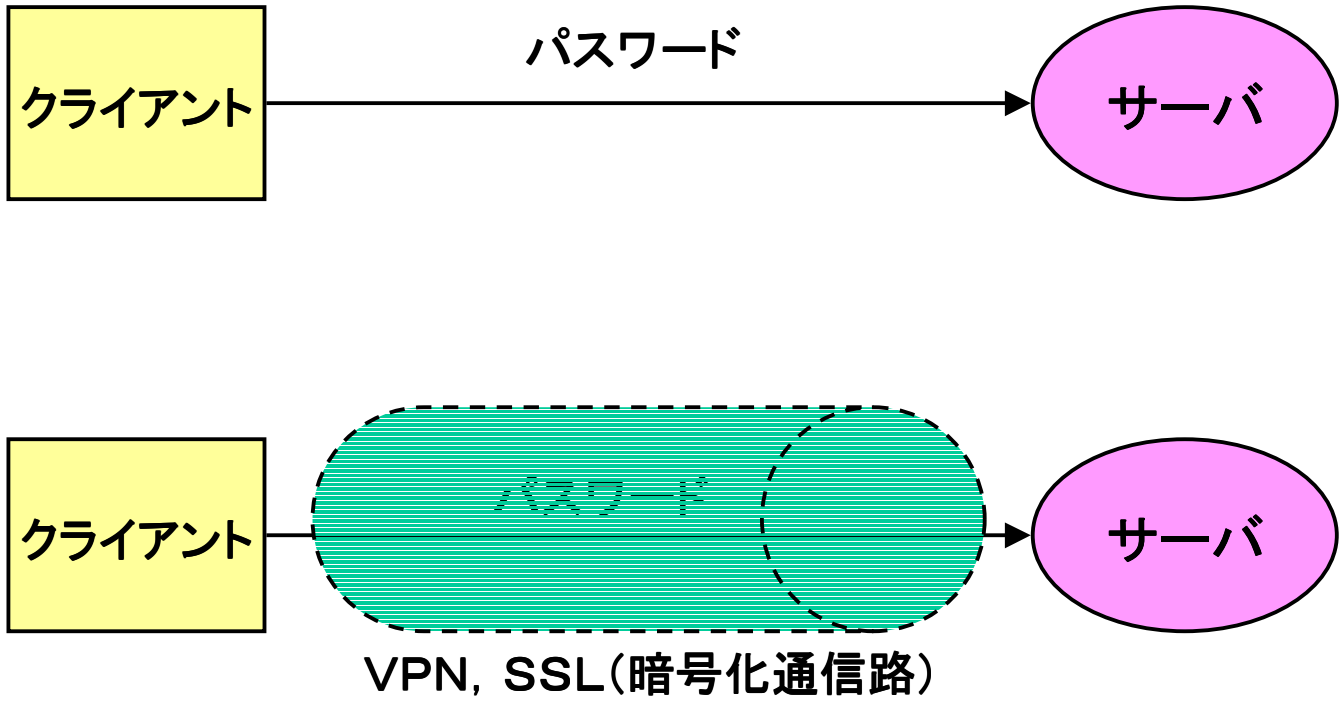
- 印鑑を作成または配布する仕組み
- 印鑑を登録する仕組み
- 署名する仕組み
- 署名を検証する仕組み
- 印鑑を有効期限前に失効させる仕組み
- 印鑑を更新する仕組み

公開鍵方式による認証

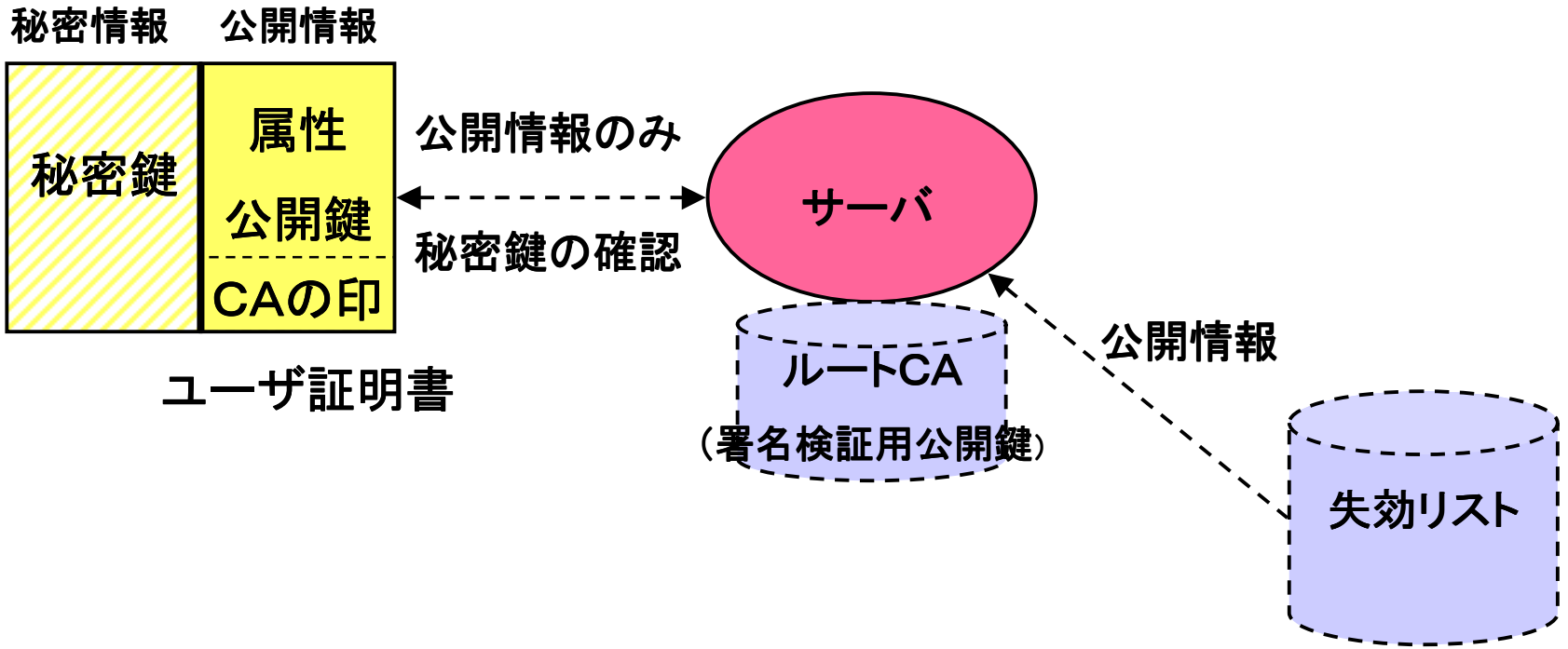
- インターネット世界のID
- 「なりすまし」を防ぐために、サーバ/クライアントは証明書を持つ。



パスワード（秘密情報）送信の安全性



CA局の印を信じれば，「公開情報」のみで相手を認証できる！



ITFOR™

PKIは何に利用されるか？

- 背景、展望、必要設備

「電子署名法」＊（2001年4月施行）

- デジタル署名がなされたものは、普通の紙の上の署名（印）と同じく法的効力を持つ。
  - デジタル“契約書” デジタル“領収書”
  - デジタル“住民票” デジタル“投票”
  - デジタル“入札” デジタル“申告”
  - デジタル“紙幣（マネー）”

ほとんどの書類は、実世界からインターネットの中へ移行できるはず。

＊正式には「電子署名及び認証業務に関する法律」

ITFOR™

IT書面一括法の施行（2001年4月）

- 電子メディアでの（金融機関）取引明細が可能となる。
- 紙の取引明細→（デジタル署名付き）電子メールなどへ移行。

インターネットバンキング・トレーディングは、
完全なペーパーレスへ

電子署名・認証技術の適用分野及び適用形態

（http://www.ipa.go.jp/security/enc/DigitalSignature/List.htmより）

- 電子メール

  S/MIMEを利用した電子メール

  PGPを利用した電子メール

  SSLサイトでのWebメール

- インターネットショッピング

  CyberCashを利用したインターネットショッピング

  PIN Based Debitプロトコルを利用したインターネットショッピング

  SECE銀行決済プロトコルを利用したインターネットショッピング

  SECE(SET)クレジット決済プロトコルを利用したインターネットショッピング

  SECE(SET)クレジット決済プロトコル（サーバウォレット方式）のインターネットショッピング

  SSLサーバ認証を利用したインターネットショッピング

  ISP仲介によるインターネットショッピング

  プリペイドカードを利用したインターネットショッピング

  電子マネーを利用したインターネットショッピング

  銀行口座引き落とし方式によるインターネットショッピング

ITFOR™

- インターネットバンキング

  SECEプロトコルを利用したインターネットバンキング
  SSL相互認証を利用したインターネットバンキング
  携帯電話を利用したインターネットバンキング
  ANSER-WEBを利用したインターネットバンキング
- インターネット株取引

  SECEプロトコルを利用したインターネット株取引
  SSLサーバ認証を利用したインターネット株取引
  SSL相互認証を利用したインターネット株取引
  携帯電話を利用したインターネット株取引
- 電子調達

  ネットオークション
  企業資材調達システム
  公共調達システム
- 電子申請

  電子申請システム
- VPN

  IPSECを利用したVPNシステム

ITFOR™

- コンテンツ配布、保管

  Adobe Acrobat採用方式の利用によるコンテンツ配布

  電子署名されたXMLファイルの配布

  コード署名を利用したアプリケーションの配布

  ディレクトリサービスを利用したコンテンツ配布

  電子文書証明サービスを利用した電子文書の配布
- インターネットEDI

  Identrus

  フィナンシャルEDI

  貿易金融EDI

  企業間EDI

  病院ネットワークシステム
- 認証基盤

  電子資格証明書

  電子社員証

  法人認証局

  法人向け与信システム
- その他

  ACES (Access Certificate for Electronic Services)

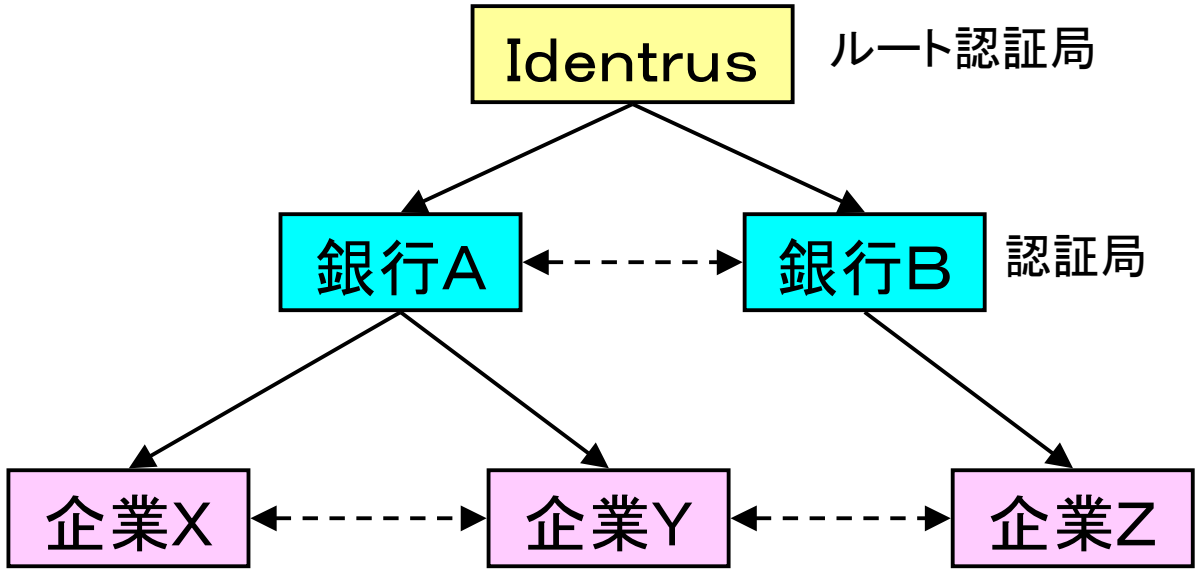
ITFOR™

GPKI
（日本電子政府構想2003年）

- 日本政府省庁・民間通信
- Bridge CA型信頼モデル
  - 複数の省がCA局を持ち、相互信頼する。
  - 省庁・民間(B2G)双方向相互認証
- 民間認証業務の認定
- GPKIパイロット事業の推進
  - 政府申請業務の９４％をオンライン化する予定
  - 電子署名ベースの申請、通知
  - 2000年度、政府認証機関を構築
    - 法務省、運輸省、通産省、郵政省
    - 民間認証機関との相互認証

Identrus計画

- （インターネットの世界で）金融機関によって企業の信用を保証する仕組みを作る。



☆企業Xは、企業Zと相互認証を行う。

ITFOR™

民間PKIの導入目的（短期的）

- SSL通信のクライアント認証
  - クライアント証明書の発行・配布
  - Webブラウザにクライアント証明書をインポートする。
  - サーバ側で、クライアント認証（含リボケーションチェック）を行う。

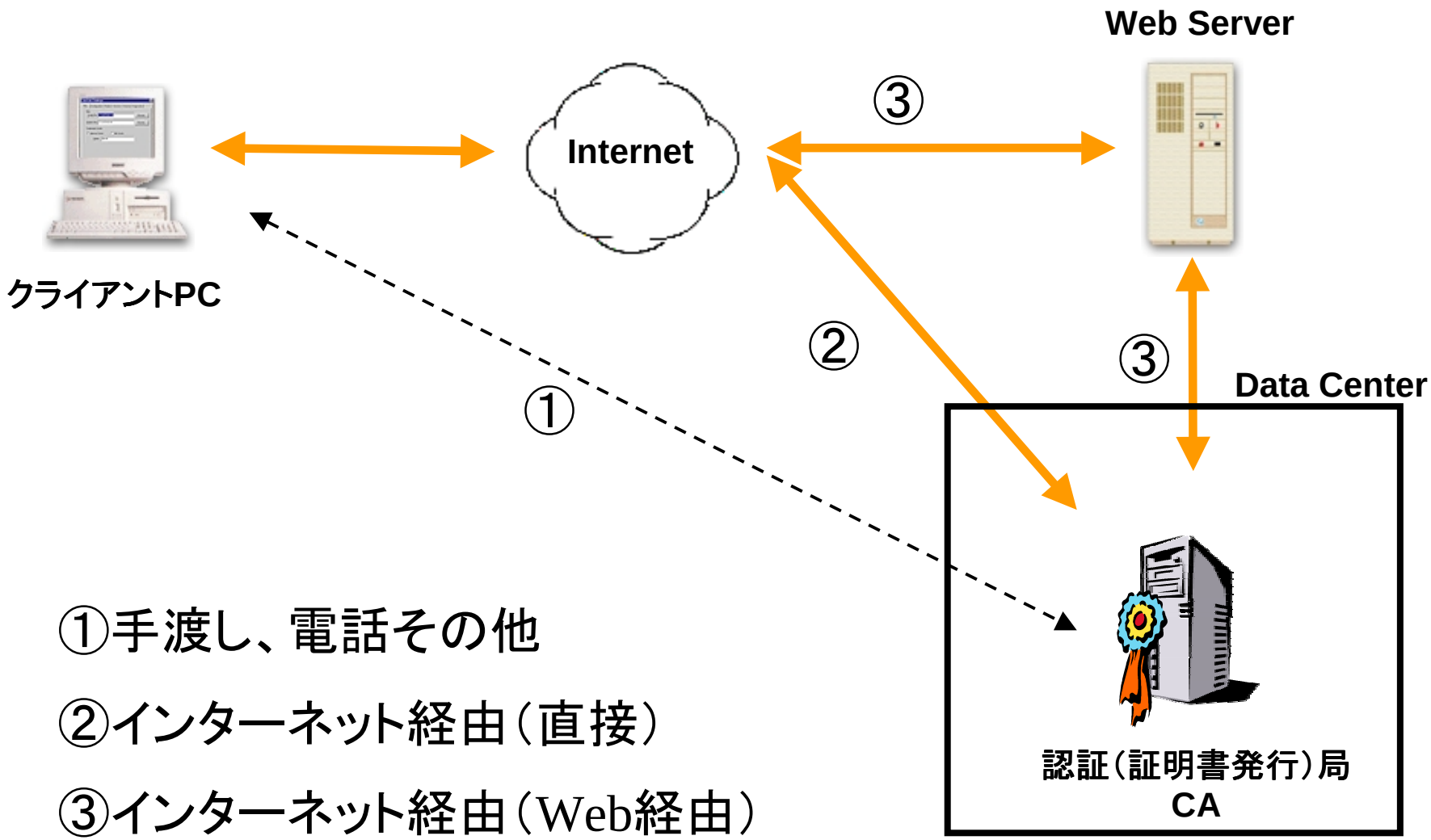
民間PKIの導入目的（長期的）

- インターネットセキュリティの基盤

  さまざまなPKIアプリの導入

  – 暗号化・復号
  – デジタル署名・検証
  – 認証

証明書の申請、発行、配布



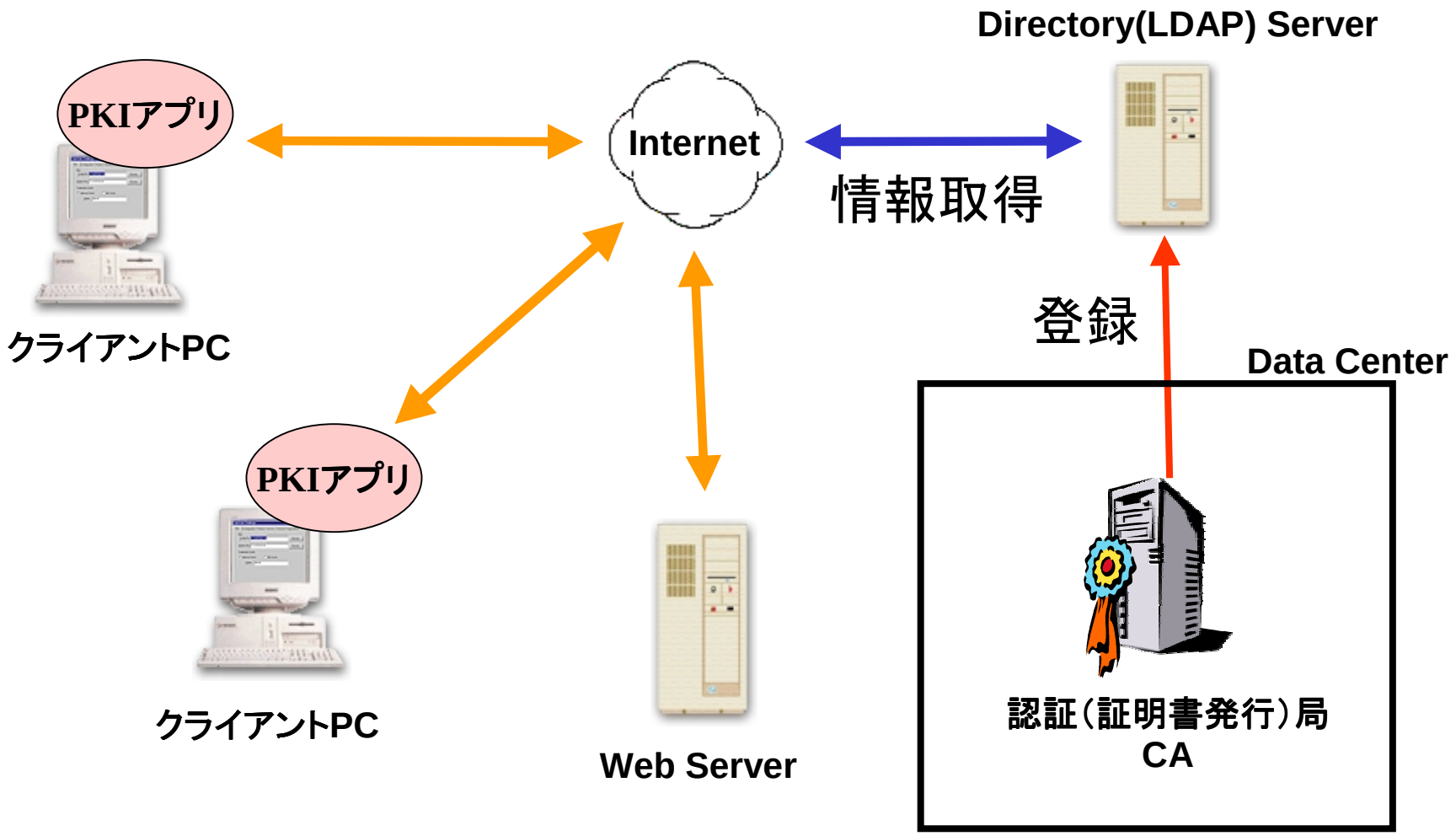
①手渡し、電話その他

②インターネット経由（直接）

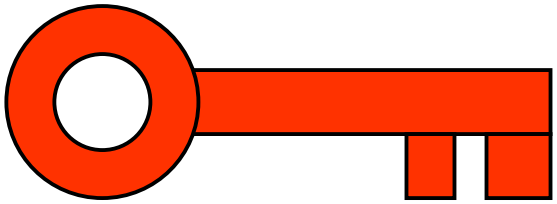
③インターネット経由（Web経由）

ITFOR™

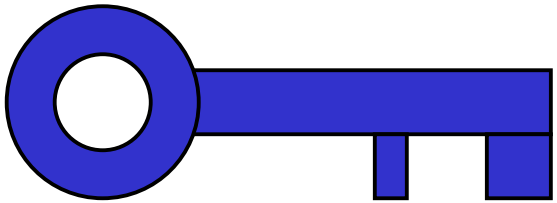
証明書失効情報の取得


Directory(LDAP) Server
PKIアプリ
Internet
情報取得
クライアントPC
登録
Data Center
PKIアプリ
クライアントPC
Web Server
認証（証明書発行）局
CA

■PKI



ありがとうございました。
㈱アイティフォー



ITFOR™