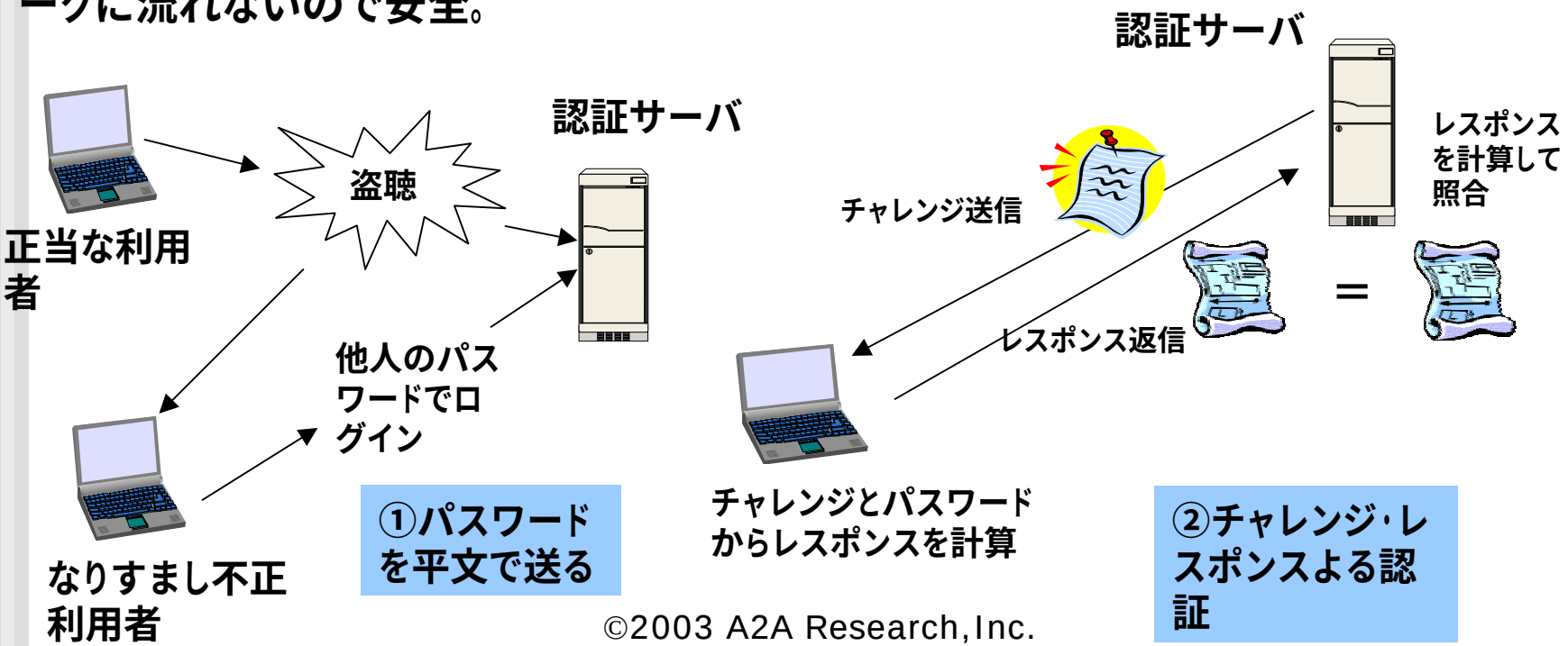
テレワーカのリモートアクセス法

- テレワーカが会社のネットワークにアクセスし、自宅に会社のデスクと同等の環境を作るには、情報セキュリティを配慮したリモートアクセス法を採用する必要がある。
- 安全なリモートアクセスのために、テレワーカの認証（本人であることの確認）と情報の盗難、改ざんを防ぐため、暗号化や通信路のトンネル化などを行う。
- 安全なリモートアクセスには以下のような方法がある。
  - メールの交換のみで十分であれば、暗号メールを使うのが簡単。
    暗号メールはファイルそのものが暗号化されるのでサーバ上での盗難も防げる。
  - ＳＳＬによりＷｅｂ形式でのファイル交換とＷｅｂメールを導入する手もある。
    社内データのＷｅｂ形式化とＷｅｂメールを導入すれば、携帯端末からのメールアクセスも安全に行える。
  - インターネットＶＰＮではより多くのアプリケーションに対応できる。

リモートアクセスの実際（目次）

(1) パスワードによる認証 (テレワーカ本人の確認)

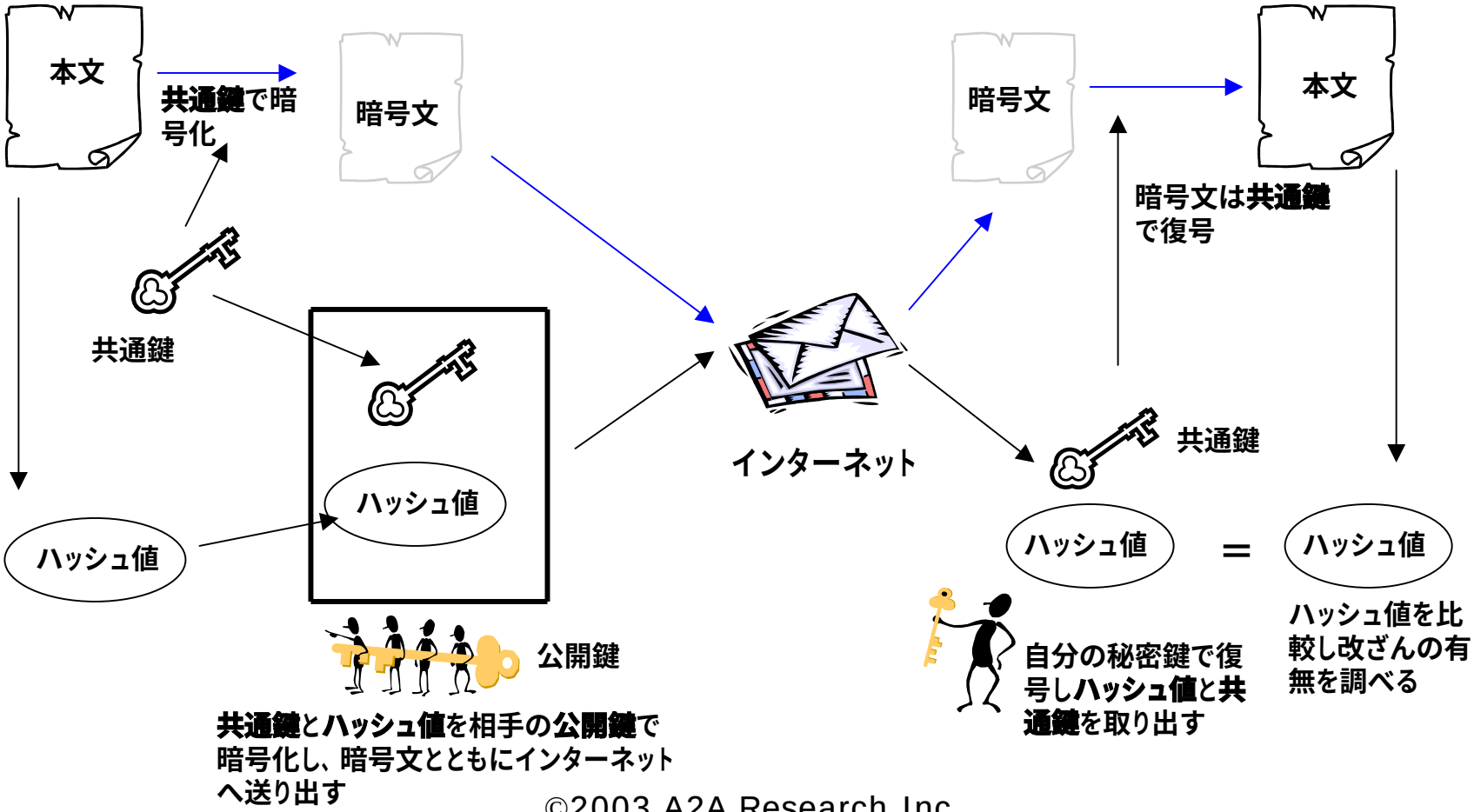
パスワードには固定パスワードとワンタイム・パスワード (ハード、ソフト) があるが、固定パスワードをネットワーク上で**平文**で送るのは盗聴の危険が大きい。**チャレンジレスポンス**によればパスワードそのものはネットワークに流れないので安全。



(2) メールの暗号化

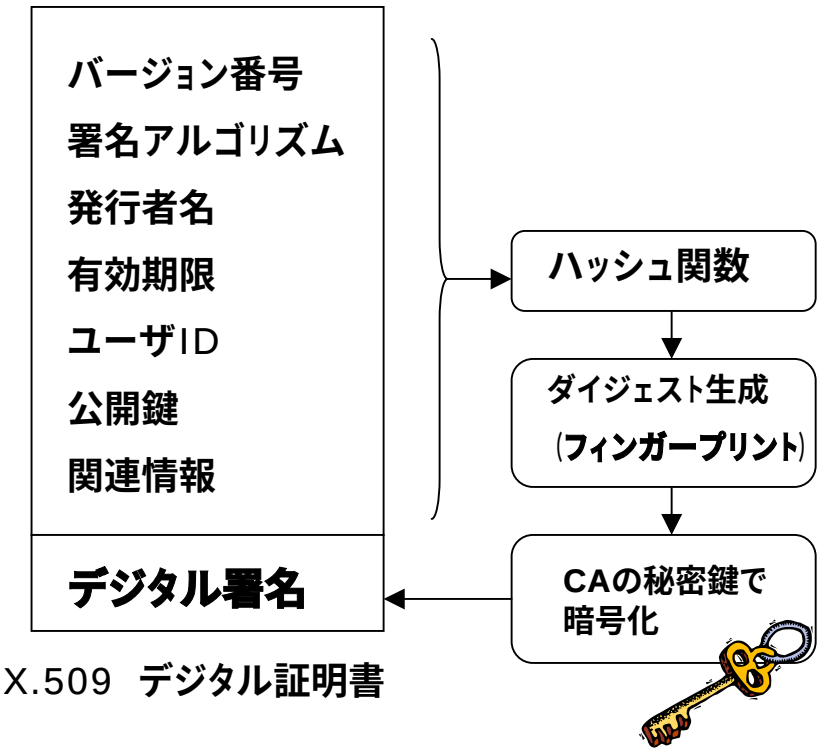
- S／MIMEはデジタル証明書により公開鍵の持ち主の身元を確認する。
- PGPはデジタル証明書を使わないため、クライアントソフトをインストールするだけで簡単に使える。ただし、米国の輸出規制で商用ライセンスの問題がある。
- フリーの互換ソフトGnuPGが使える。ドイツで開発されたため米国の輸出規制を受けない。
- テレワーカが本社とメール交換する場合には、他の簡便な方法で添付ファイルのみ暗号化するという方法もある。

暗号メールの仕組み
(S／MIME，PGPの例)



デジタル証明書

- デジタル証明書は米ベリサインなどのＣＡサービスを提供している企業から有料で発行してもらう。
- 発行の際は登記簿などで会社を確認し、その情報はデジタル証明書に記載される。
- 個人の認証にも利用できる。
- ＳＳＬの現在のフォーマットは Ｘ．５０９　Ｖｅｒ．３
- Ｓ／ＭＩＭＥやＩＰＳｅｃ／ＩＫＥでも利用される。



X.509　デジタル証明書

(3) Webアクセスによる方法
SSLによるセキュリティ対策

Webアクセスに潜む脅威

①Webサーバへの不正アクセス(攻撃)

②通信途中で奪われたデータの解読

③Webブラウザでの危険なプログラムのダウンロード
ウイルス感染や
危険なスクリプトの実行など

SSLはWWWにおける暗号化の事実上の標準で

①通信の暗号化

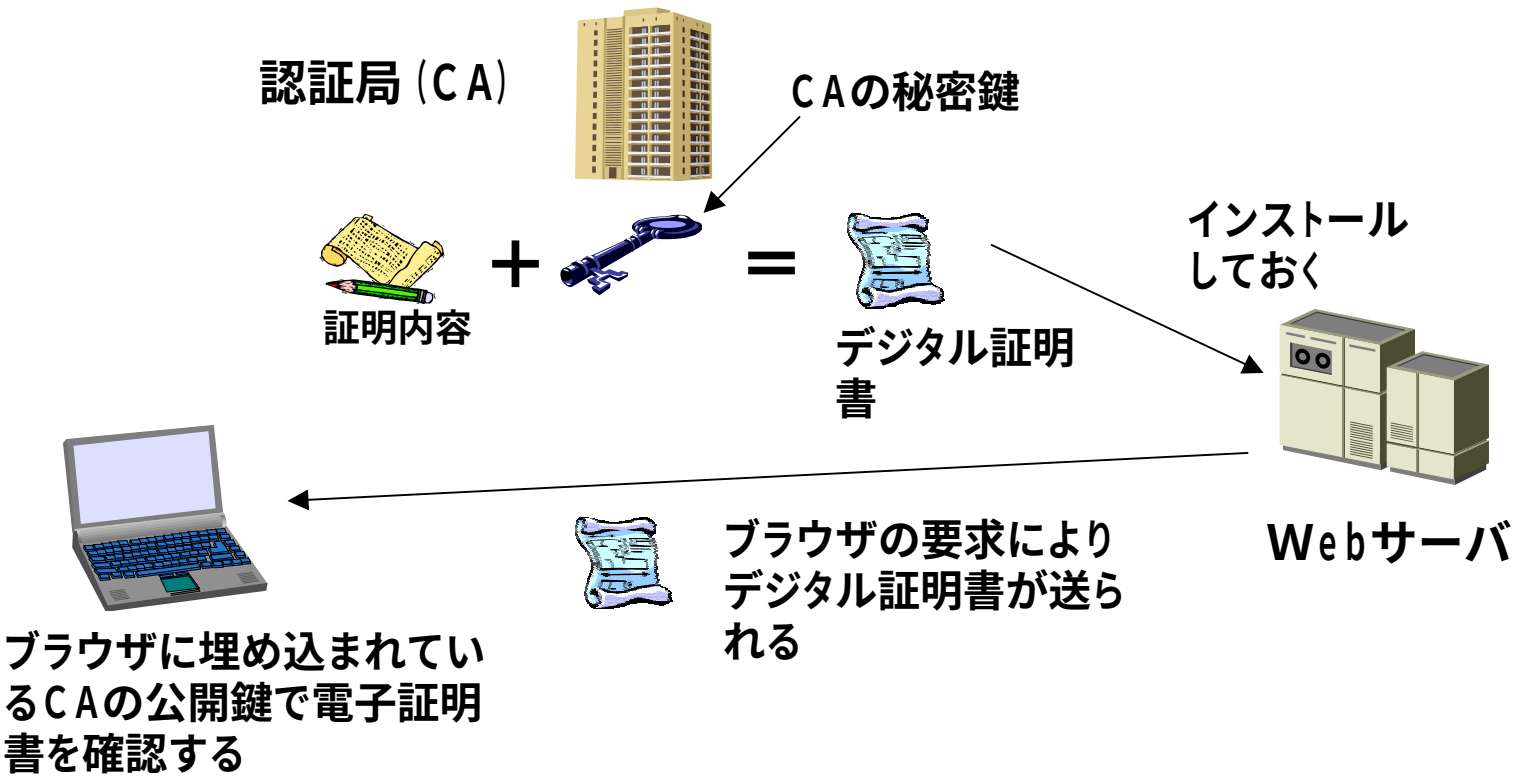
②データの完全性の保証(改ざん防止)

③サーバの認証(なりすまし防止)

④クライアントの認証(不正アクセス防止)

の機能がある

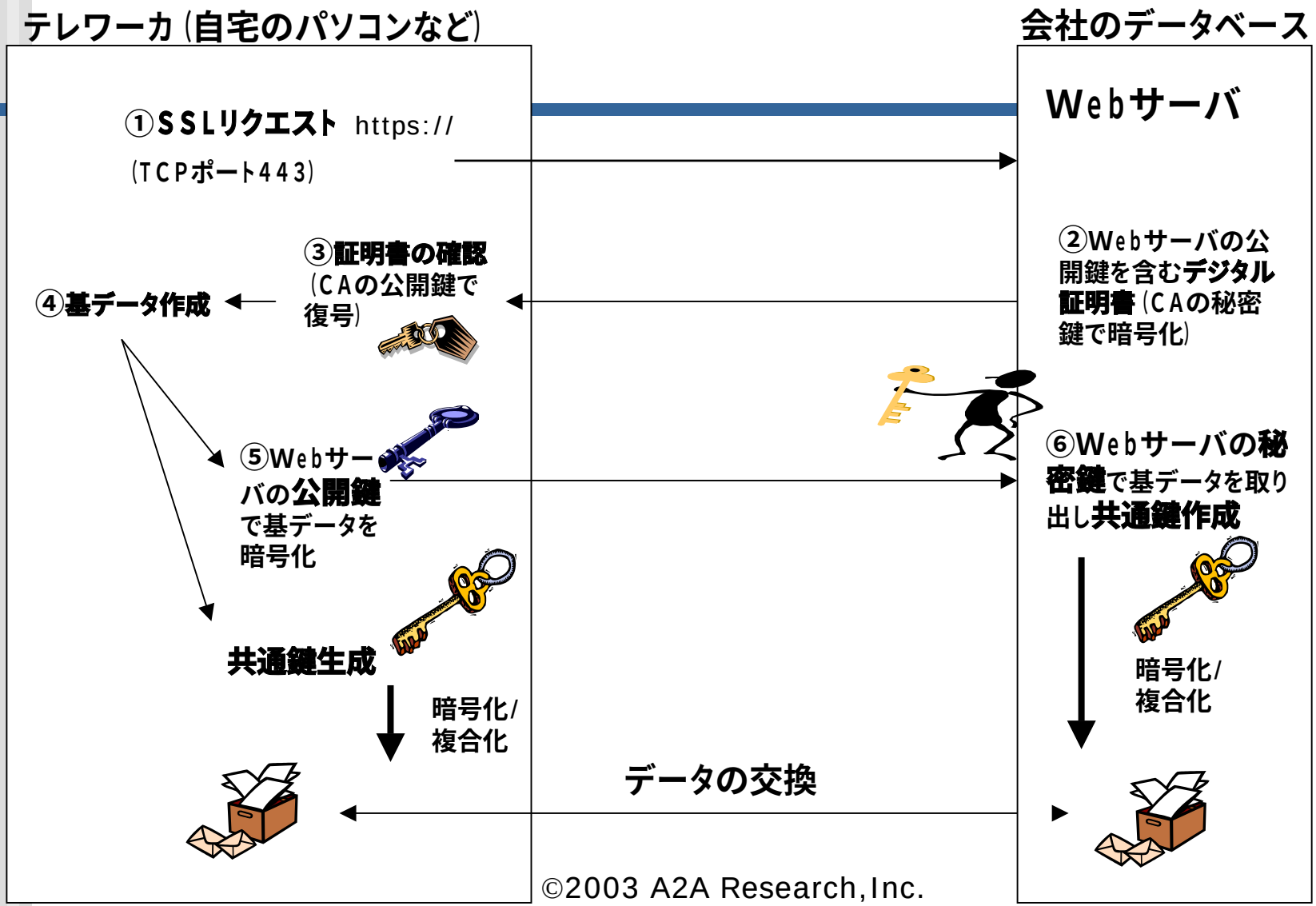
ＳＳＬサーバ認証
(サーバが本物であるかどうか確認する)



ＳＳＬクライアント認証

- サーバ認証と同様にクライアントの認証も可能
- テレワーカが会社のＷｅｂにアクセスするケースでは第3者認証機関を利用するまでもない。
- 会社自身で社員の認証をすればよい。（自社でＣＡ設立）
- ただし、デジタル証明書がパソコンにインストールされるので盗難や紛失が大きな脅威になる。
- テレワーカなどのクライアントの認証は「ユーザＩＤ＋パスワード」のほうが実用的かもしれない。

ＳＳＬ暗号化処理の例

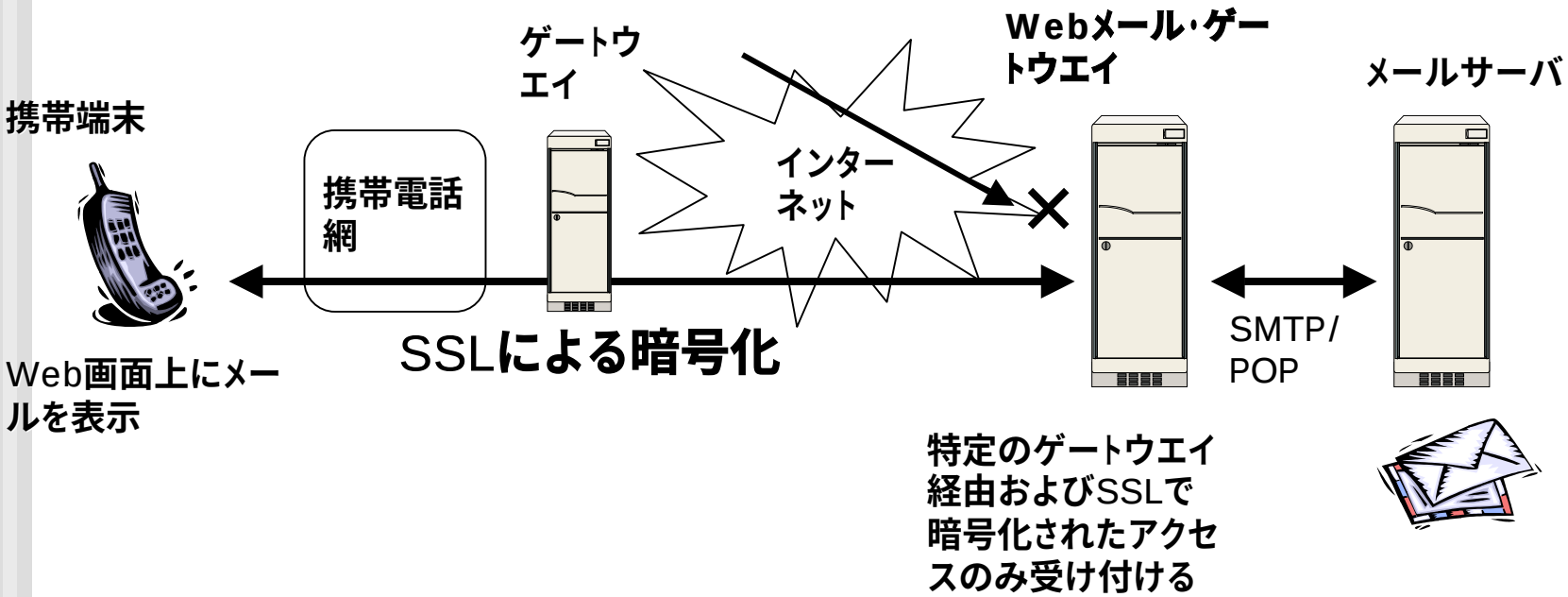


携帯端末から社内のメールサーバにアクセス
Webメールの導入が現実的

- 携帯電話機はIPSecなどのVPN機能は持っていない。
- 最近の携帯端末はSSLに対応している。

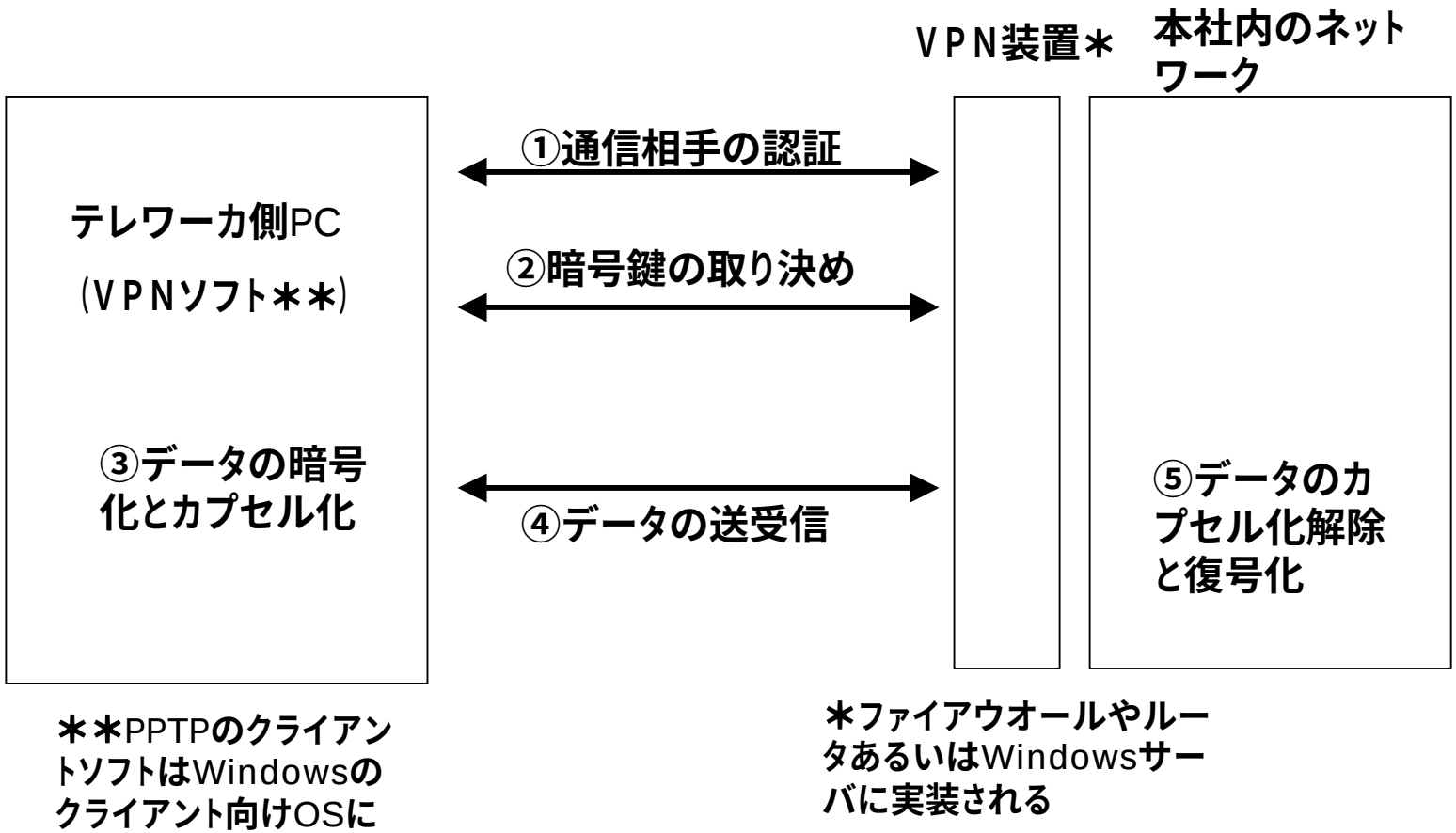
  そこで
- Webメール･ゲートウエイ（ソフト）を利用したWebメールを導入
- 電話番号による認証は番号の転送に問題
- クライアントの認証にはJava で作成されたワンタイム･パスワードなどを利用
- 携帯網とインターネットの境界のゲート･ウエイ（IPアドレス）でアクセス制限をする
- SSLによりWebブラウザとWebサーバ間を暗号化する

Webメール･ゲートウエイの導入



(4) インターネットVPNによる方法

(PPTPの基本的な手順の例)



インターネットVPNの設定手順
(PPTPの例)

①**認証行程**：任意の変数をやり取りし、変数とパスワードを基にハッシュ値を生成。双方でハッシュ値が一致することを確認する。

②**暗号鍵の決定**：鍵を作り出す基になるデータをやり取りし、双方で共通鍵を生成する。

③**暗号化**：共通鍵で（IPヘッダー）＋（データ）を暗号化

④**トンネル化**：PPPヘッダーを付けて1対1の仮想的な通信路を確保。

⑤**送出**：あて先グローバル・アドレス等を付けてインターネットに送り出す。

(5) 最適なリモートアクセスは何か

在宅での業務内容とセキュリティポリシーおよびコストとの兼ね合いになる。テレワーカの自宅で利用可能なアクセス回線の速度も考慮する必要がある。情報セキュリティの観点からは会社のセキュリティポリシーに基づいたセキュリティ対策が求められるが、リモートアクセスの導入により会社のイントラネットにセキュリティホールのような弱点を造ってはならない。電子メールのやり取りだけなら添付文書の暗号化で十分かもしれない。SSLによるWebアクセスであれば、容易にファイルの共有ができる。テレワーカ側は普段使っているWebブラウザで会社のWebサーバにアクセスし、社内のファイルへのアクセスやメールシステムも利用できる。また、携帯端末から社内のメールシステムの利用も容易に実現できる。インターネットVPNがLAN間接続のみならず、リモートアクセスの手段としても注目されているが、導入の容易さという面では難点がある。最近話題になっている、SSLによるWebアクセス方式「SSL-VPN」に注目したい。

END