THE DOCUMENT COMPANY
FUJI XEROX

IW2003 PKI応用編

富士ゼロックス株式会社
稲田 龍
<Ryu.Inada@fujixerox.co.jp>

THE DOCUMENT COMPANY
FUJI XEROX

PKIアプリケーション

アプリケーションの動向

THE DOCUMENT COMPANY FUJI XEROX

- HTTPS
- S/MIME
- 電子署名アプリケーション
- 無線LANでの認証(802.1X認証)

HTTPS

THE DOCUMENT COMPANY FUJI XEROX

- SSLを使い通信路の暗号化と接続先(元)の認証を行う
- Internet Explorer/Netscape Navigatorなどが標準でサポート

- 多くの場合、サイト側の認証と暗号化のみが行われているが、クライアント側の認証も使われつつある
  - うまく使えば、Single Sign Onとなる
  - パスワードベースの認証に比べユーザの負担小

- Windows Update/Windows Activateにも利用されている。

SSL/TLSとは…

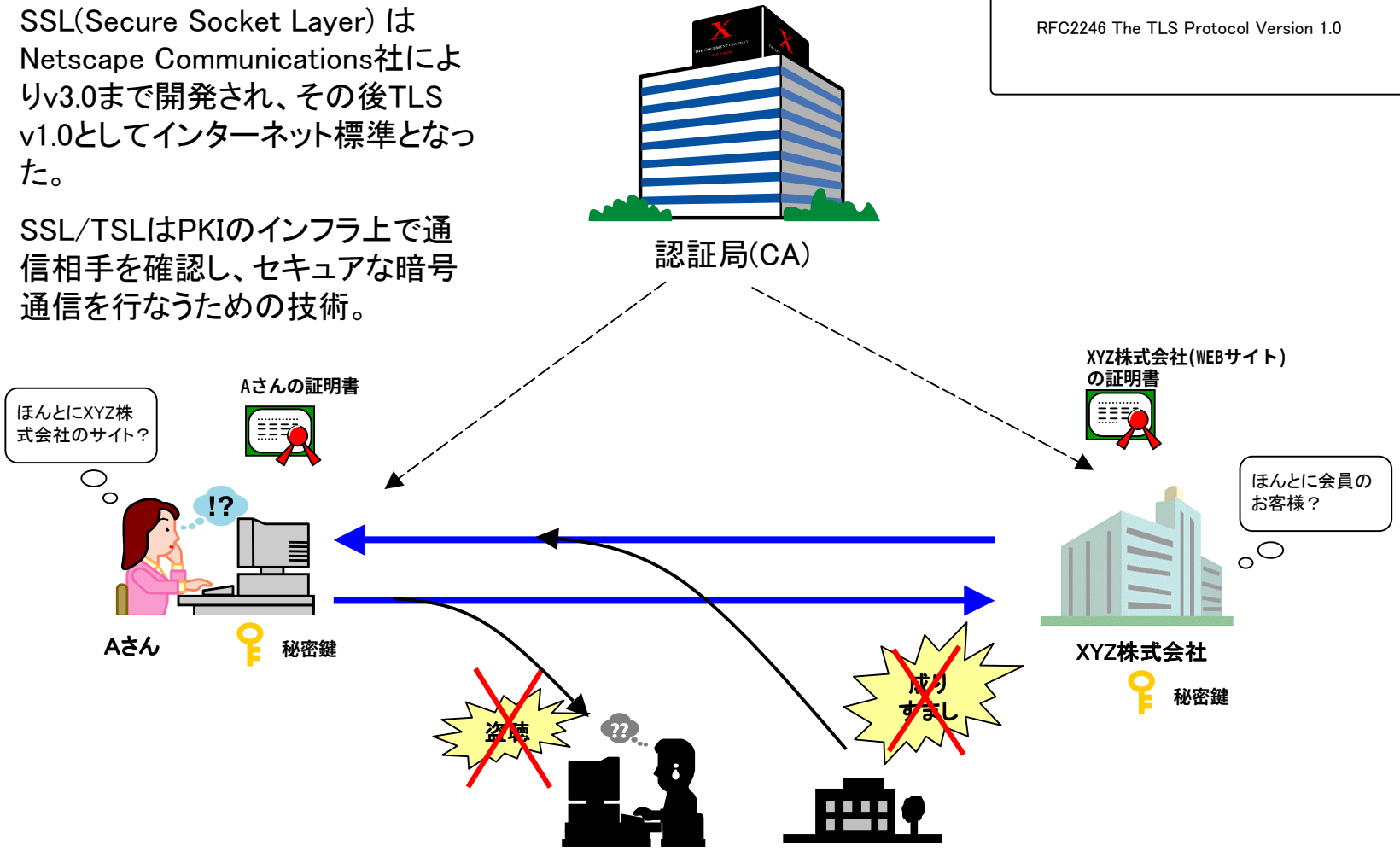
SSL/TLSとは…

SSL(Secure Socket Layer) は Netscape Communications社により v3.0まで開発され、その後TLS v1.0としてインターネット標準となった。

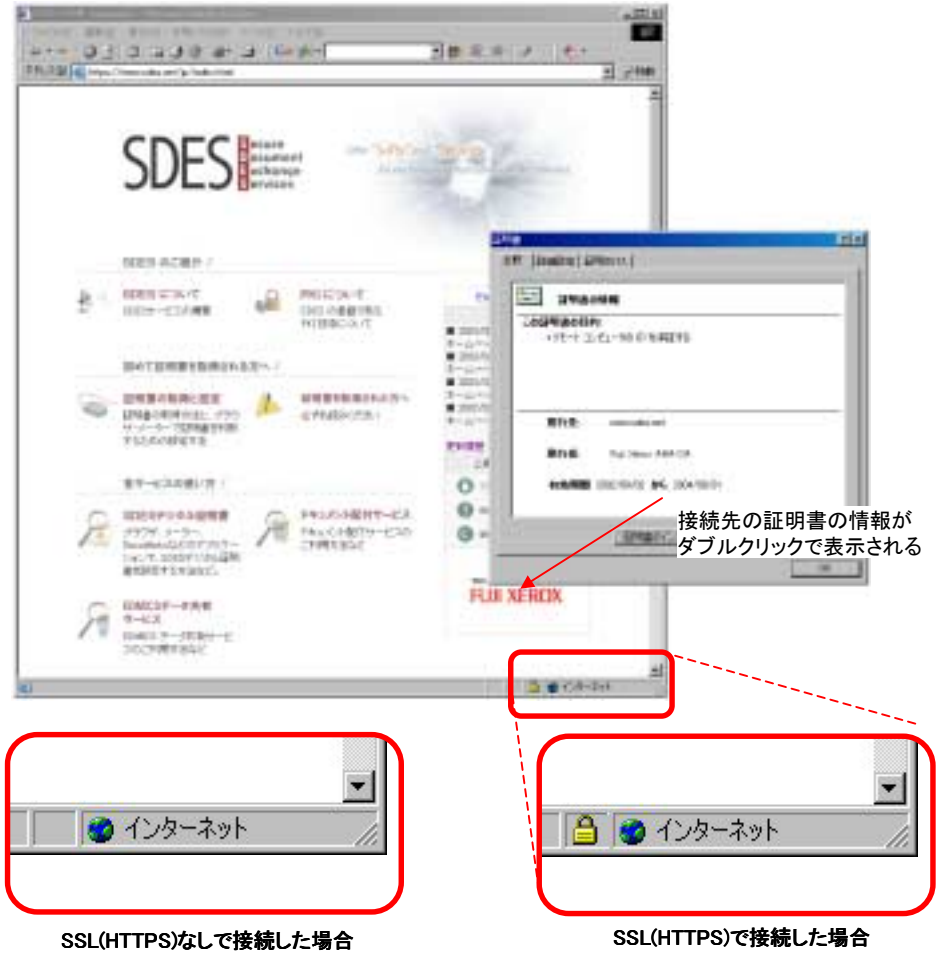
SSL/TLSはPKIのインフラ上で通信相手を確認し、セキュアな暗号通信を行なうための技術。

SSL/TLS 関連RFC

RFC2246 The TLS Protocol Version 1.0

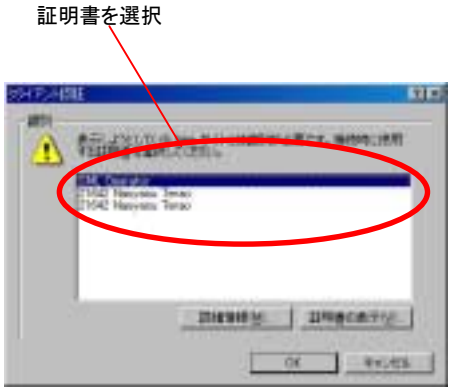


SSL対応ブラウザ（Internet Explorer 6）



SSL(HTTPS)なしで接続した場合

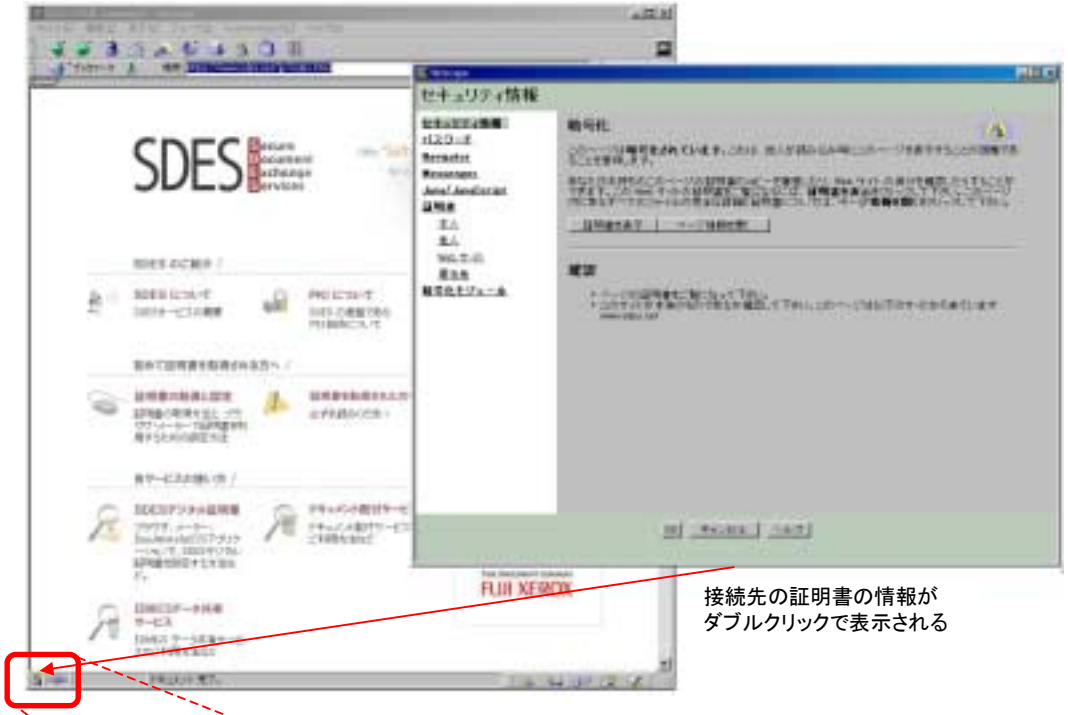
SSL(HTTPS)で接続した場合



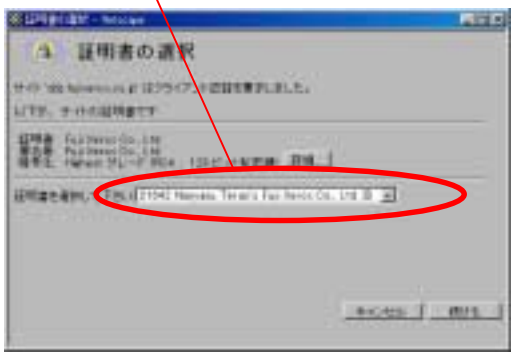
SSL(HTTPS)クライアント認証が要求された場合

Internet Explorer 6でのSSL(HTTPS)

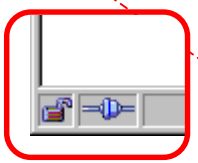
SSL対応ブラウザ（NetscapeNavigator 4.78）



接続先の証明書の情報が
ダブルクリックで表示される



SSL(HTTPS)クライアント認証が要求された場合



SSL(HTTPS)なしで接続した場合

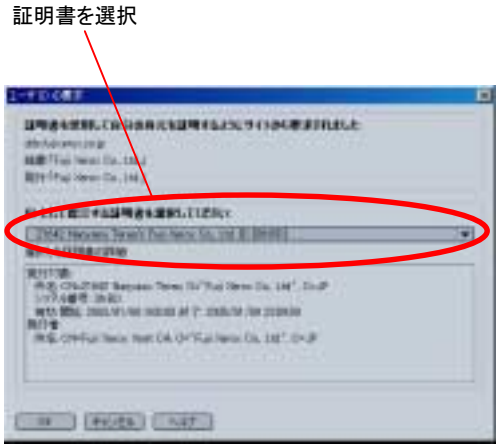
SSL(HTTPS)で接続した場合

NetscapeNavigator 4.78でのSSL(HTTPS)

SSL対応ブラウザ（Netscape 7.1）

SSL(HTTPS)なしで接続した場合

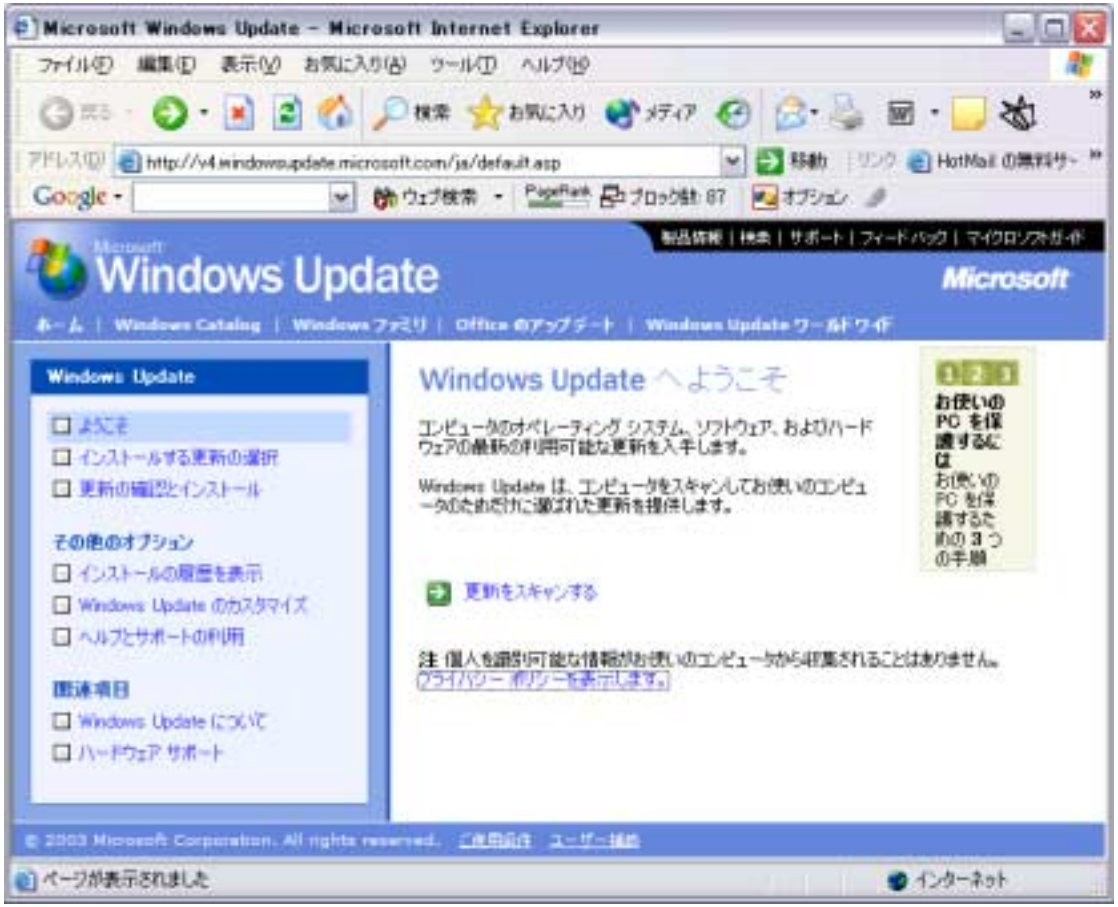
SSL(HTTPS)で接続した場合



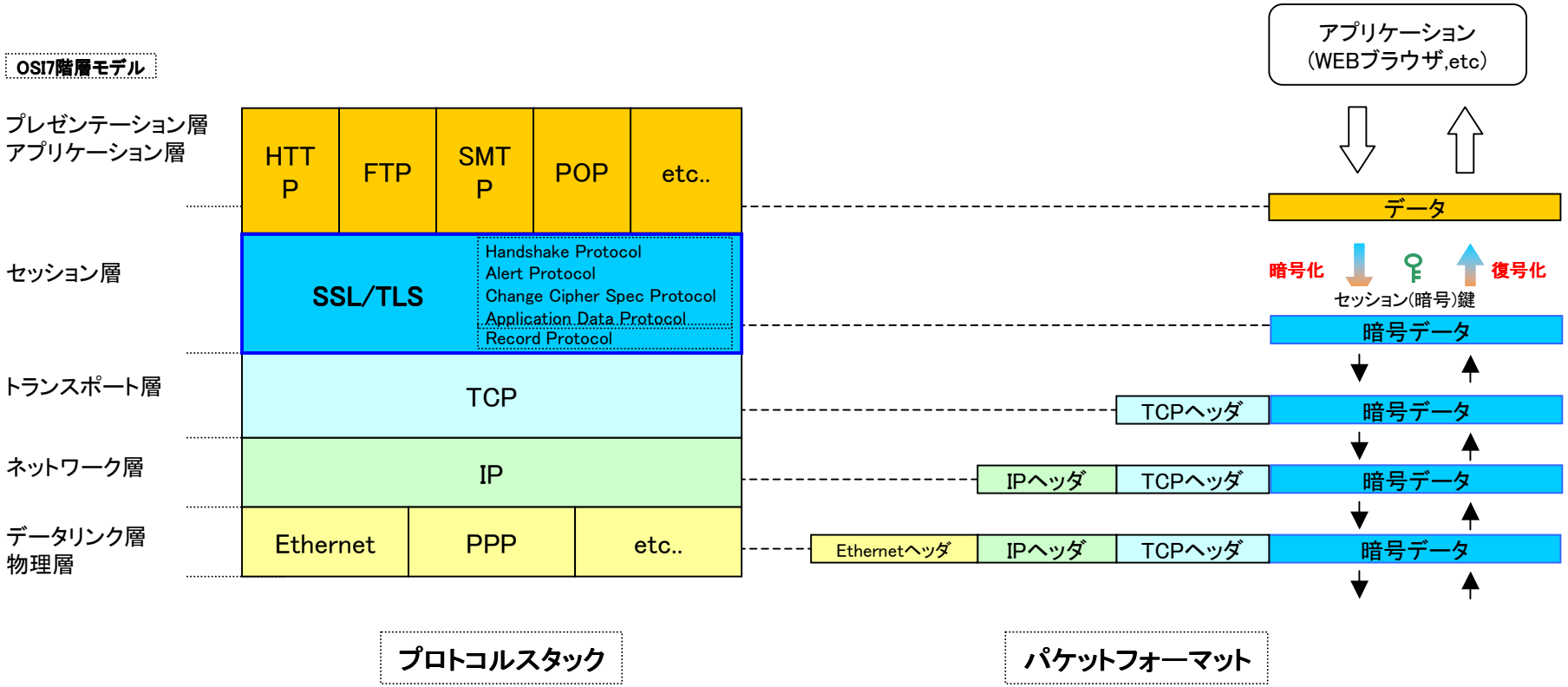
SSL(HTTPS)クライアント認証が要求された場合

Netscape 4.71でのSSL(HTTPS)

Windows Update



SSL/TLSプロトコル(1) – プロトコルスタック



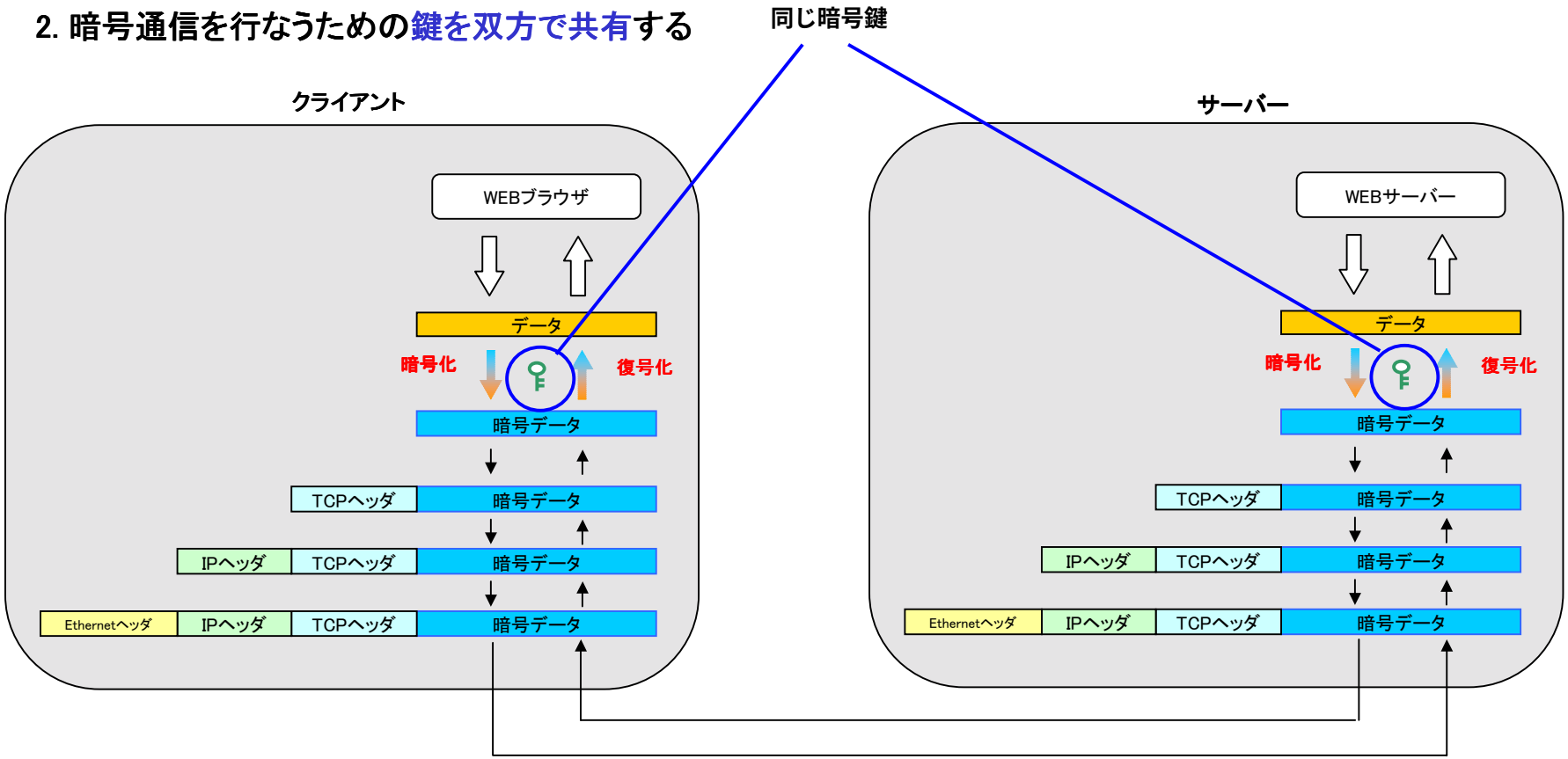
SSL/TLSはアプリーケーションとトランスポートの中間に位置するため、
利用するアプリケーションに依存せずにセキュアな通信が行なうことができる。

SSL/TLSプロトコル(2) – 鍵共有

THE DOCUMENT COMPANY FUJI XEROX

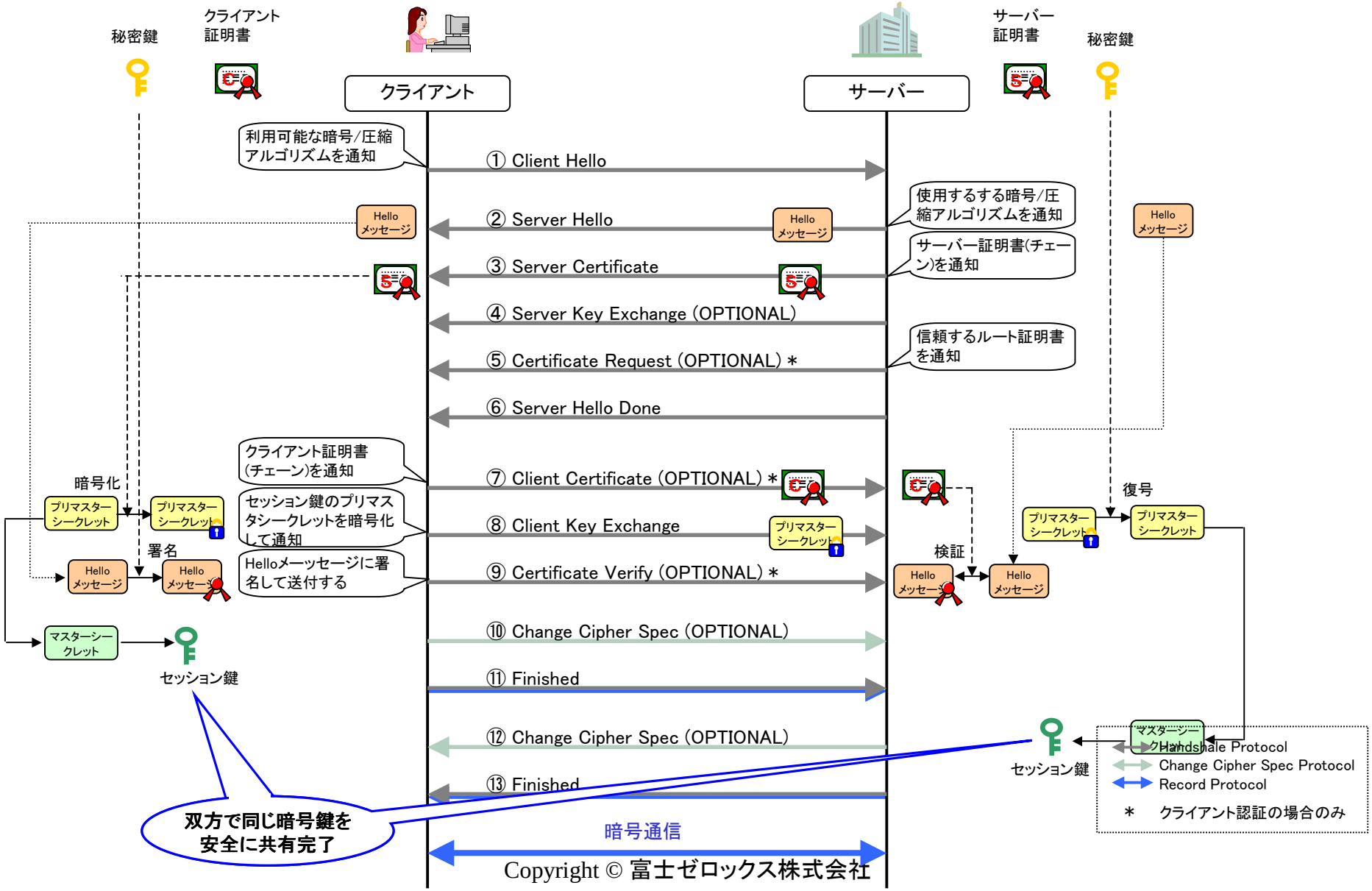
暗号通信を行なうためには…

1. 通信相手が正しい通信相手なのか認証する
2. 暗号通信を行なうための鍵を双方で共有する



SSL/TLSプロトコル(3) – ハンドシェイク

THE DOCUMENT COMPANY FUJI XEROX



S/MIME

THE DOCUMENT COMPANY FUJI XEROX

- MIMEを使い電子メールの暗号化と電子署名
  - メジャーではないが、そろそろ使われ始めている

- Microsoft Outlook/Outlook Express
- Netscape Navigator
- Orangesoft Winbiff
- Becky!
- MEW(電子署名のみ)
- Gnu PG

S/MIMEとは…

THE DOCUMENT COMPANY FUJI XEROX

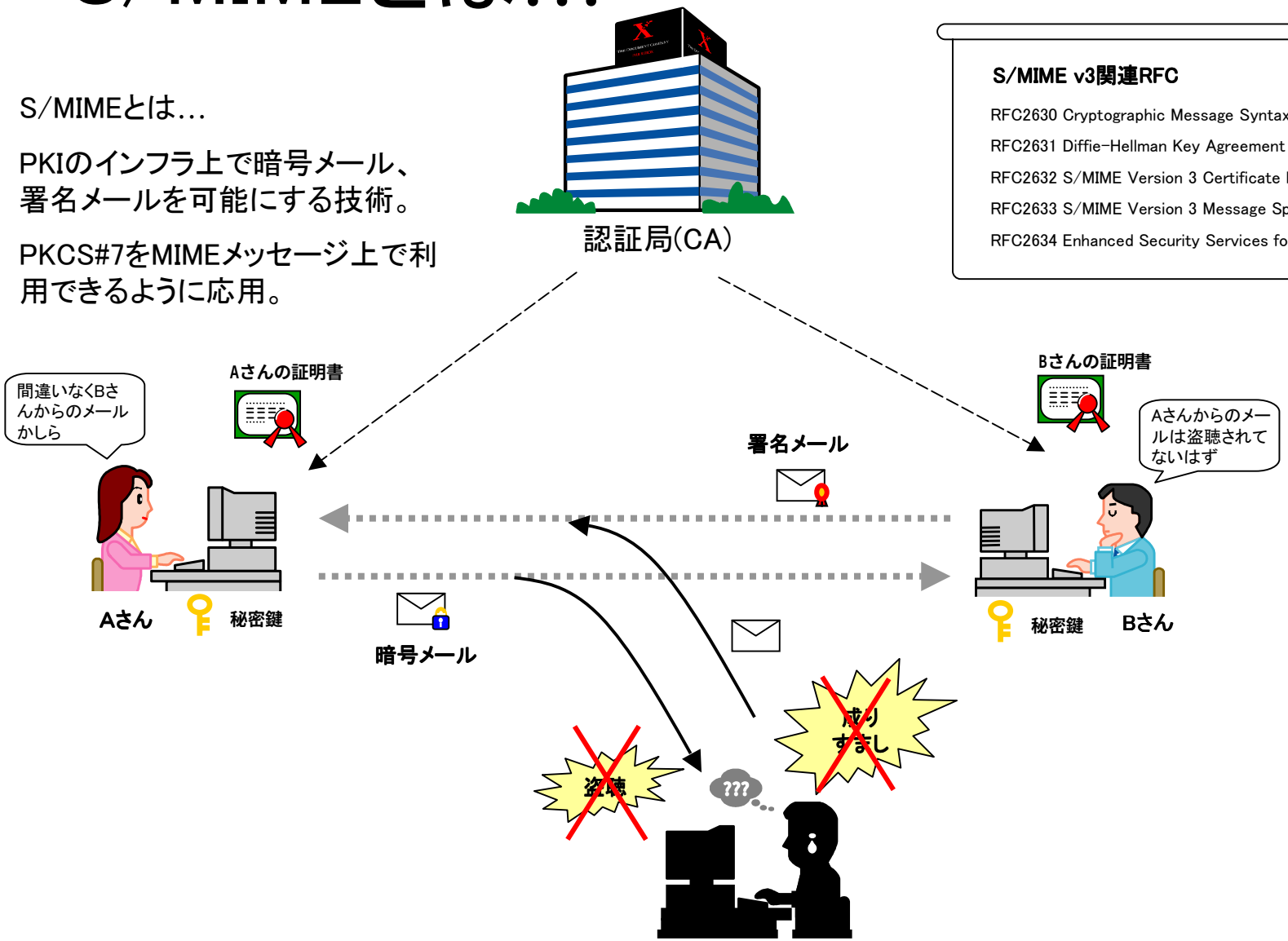
S/MIMEとは…

PKIのインフラ上で暗号メール、署名メールを可能にする技術。

PKCS#7をMIMEメッセージ上で利用できるように応用。

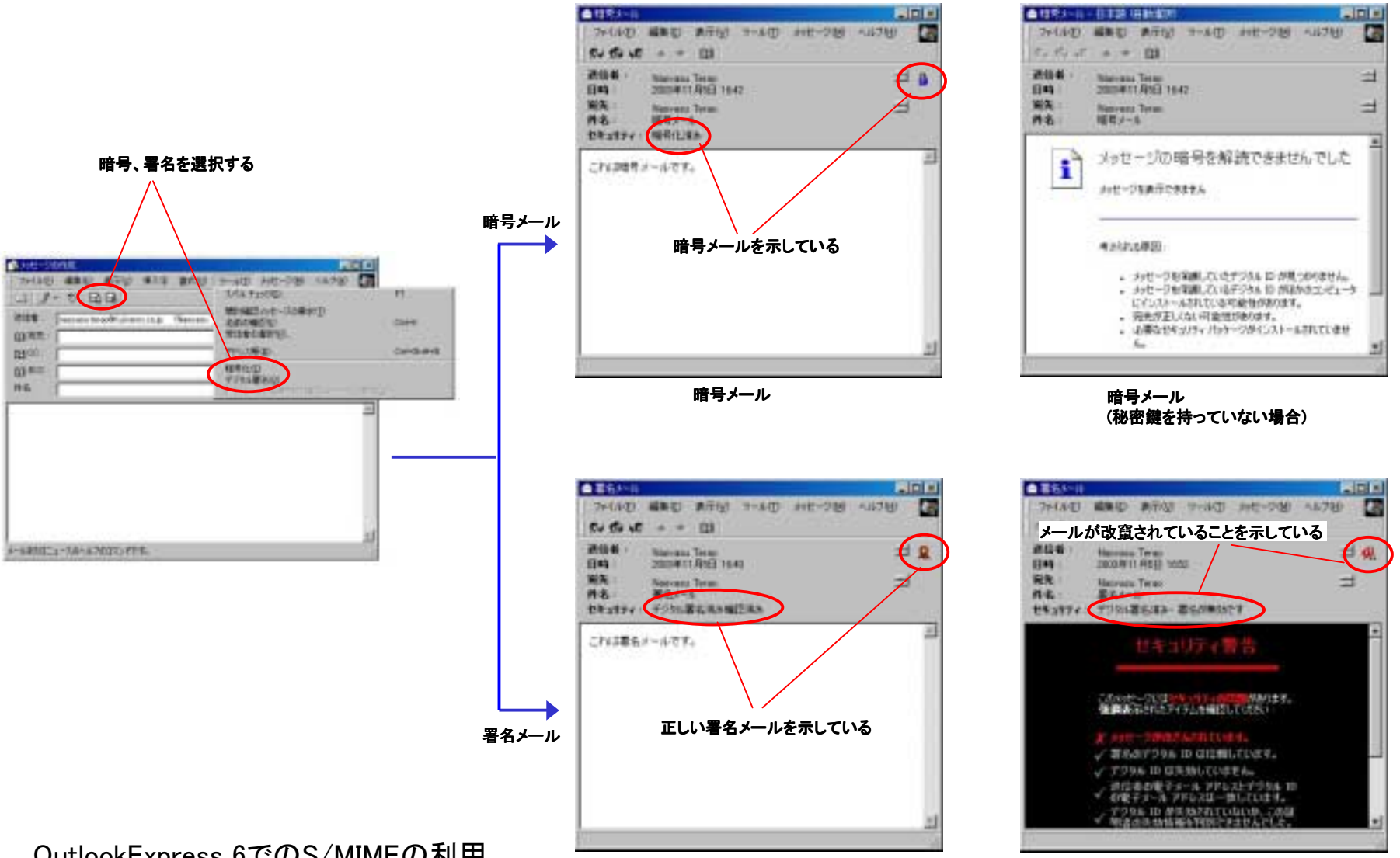
S/MIME v3関連RFC

RFC2630 Cryptographic Message Syntax
RFC2631 Diffie-Hellman Key Agreement Method
RFC2632 S/MIME Version 3 Certificate Handling
RFC2633 S/MIME Version 3 Message Specification
RFC2634 Enhanced Security Services for S/MIME



S/MIME対応メーラー（OutlookExpress 6）

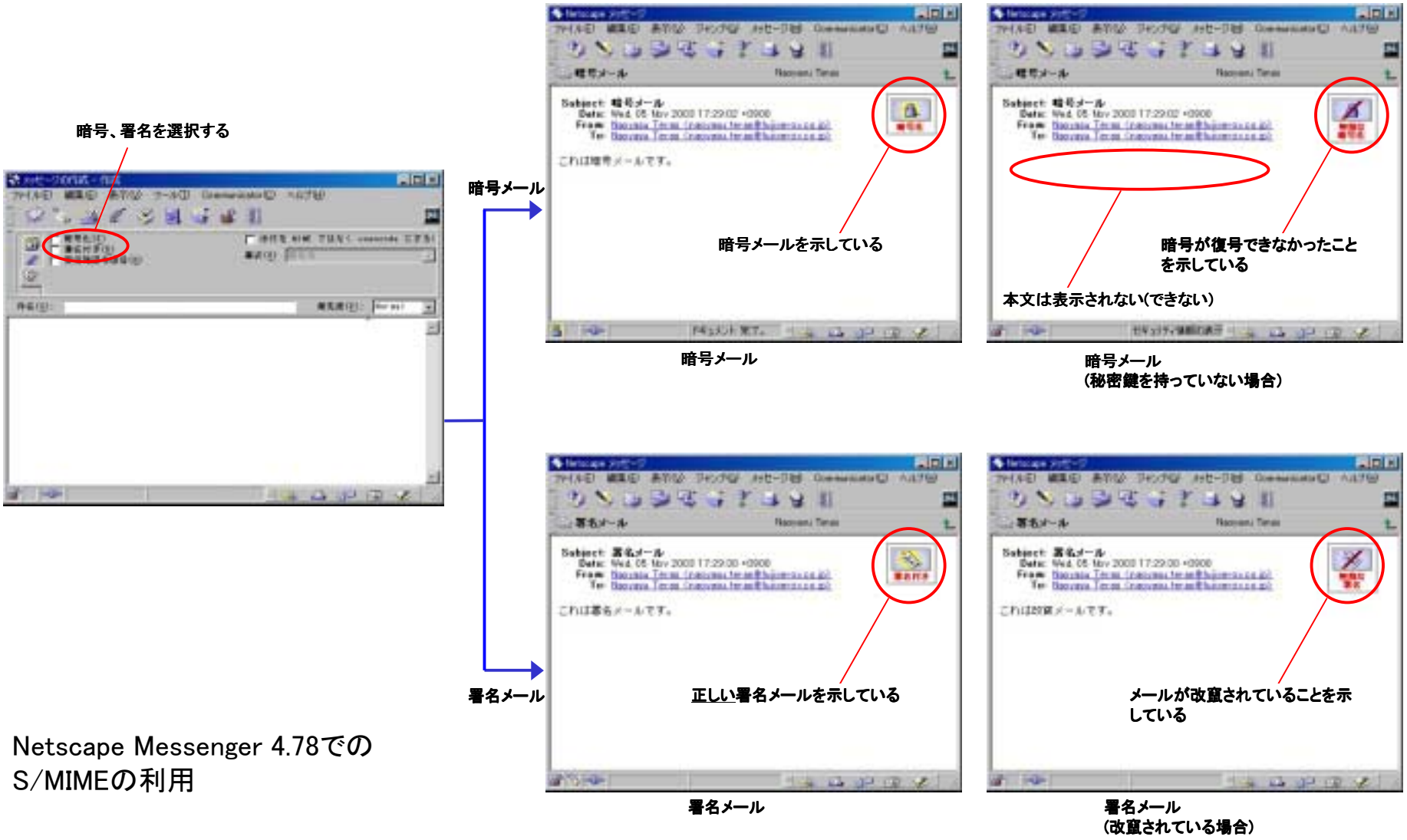
THE DOCUMENT COMPANY FUJI XEROX



OutlookExpress 6でのS/MIMEの利用

S/MIME対応メーラー（Netscape Messenger 4.78）

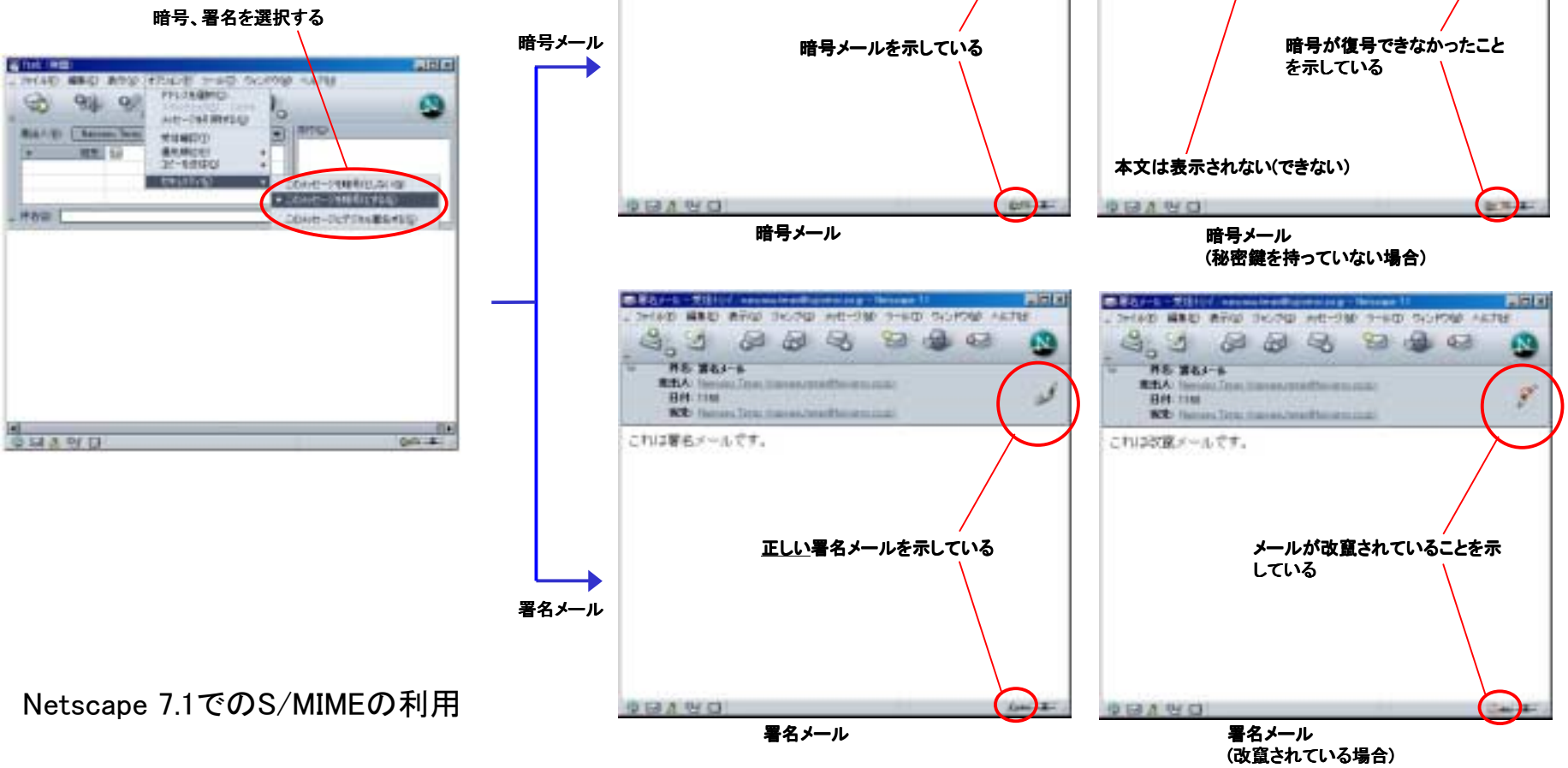
THE DOCUMENT COMPANY FUJI XEROX



Netscape Messenger 4.78での
S/MIMEの利用

S/MIME対応メーラー（Netscape 7.1）

THE DOCUMENT COMPANY FUJI XEROX



Netscape 7.1でのS/MIMEの利用

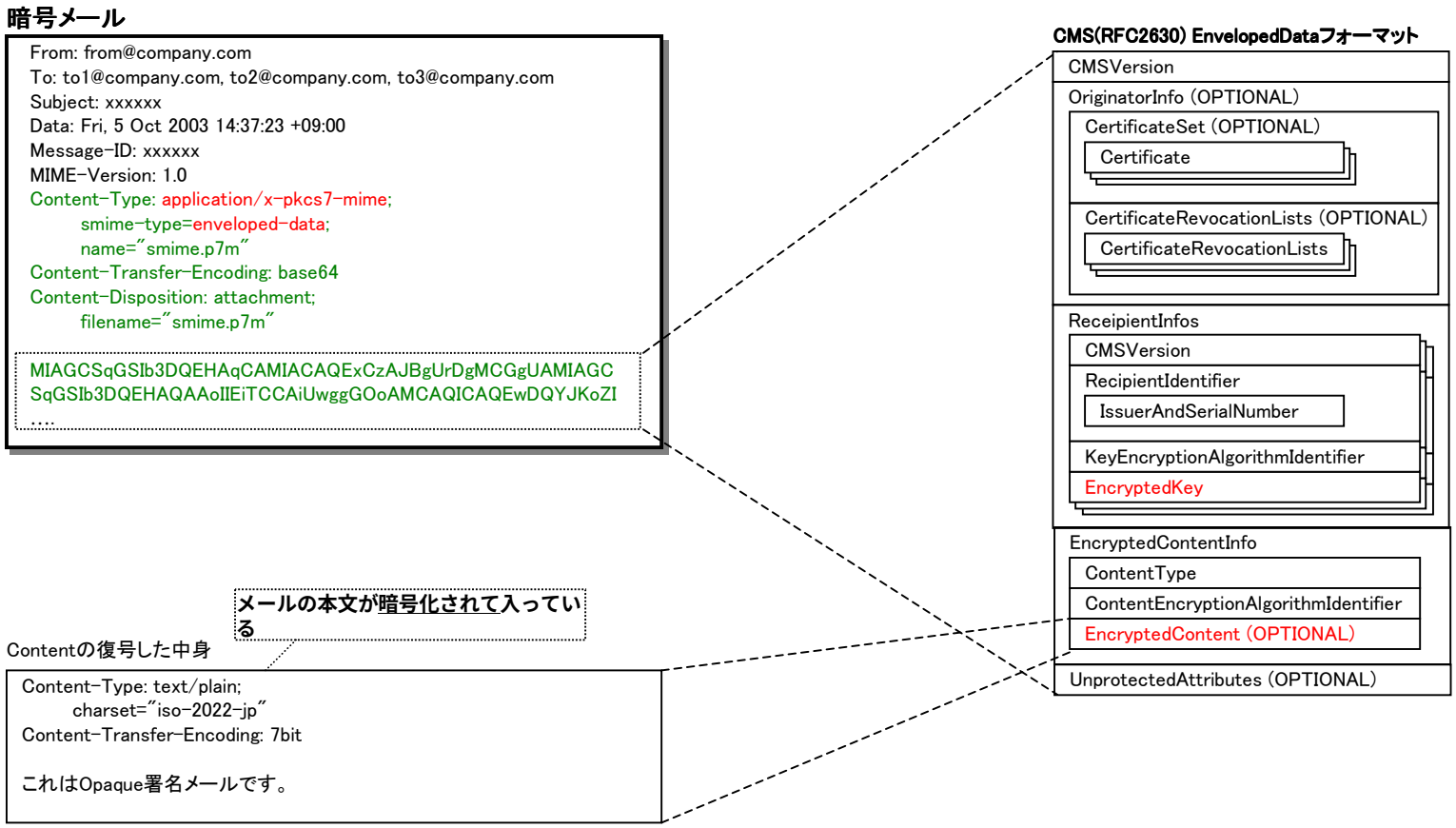
S/MIMEのメールメッセージ

THE DOCUMENT COMPANY FUJI XEROX

- 本文や添付ファイルをメールの形式(MIME)に
- MIME化したメッセージを入力として署名データまたは暗号文を作成
- PKCS#7形式にエンコード
  - RFC2315
    PKCS #7 : Cryptographic Message Syntax Version 1.5
  - フォーマットはASN.1で表記される。
  - エンコードのルールはBERまたはDERに従う。
- BASE64変換して、規定のMIMEヘッダを付ける
  - RFC2311
    S/MIME Version 2 Message Specification
  - RFC2633
    S/MIME Version 3 Message Specification

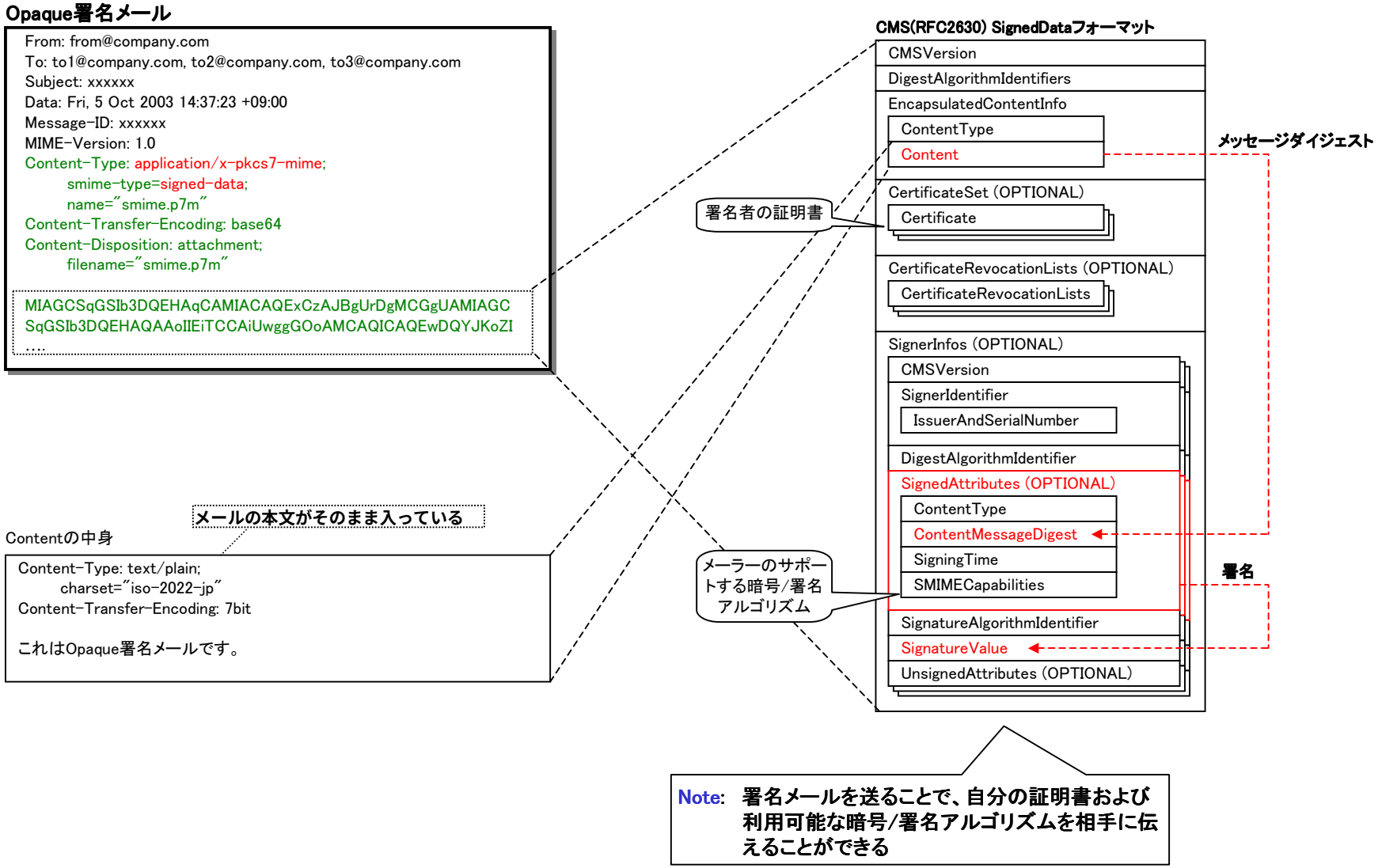
S/MIMEメッセージ内部構造（暗号）

THE DOCUMENT COMPANY FUJI XEROX

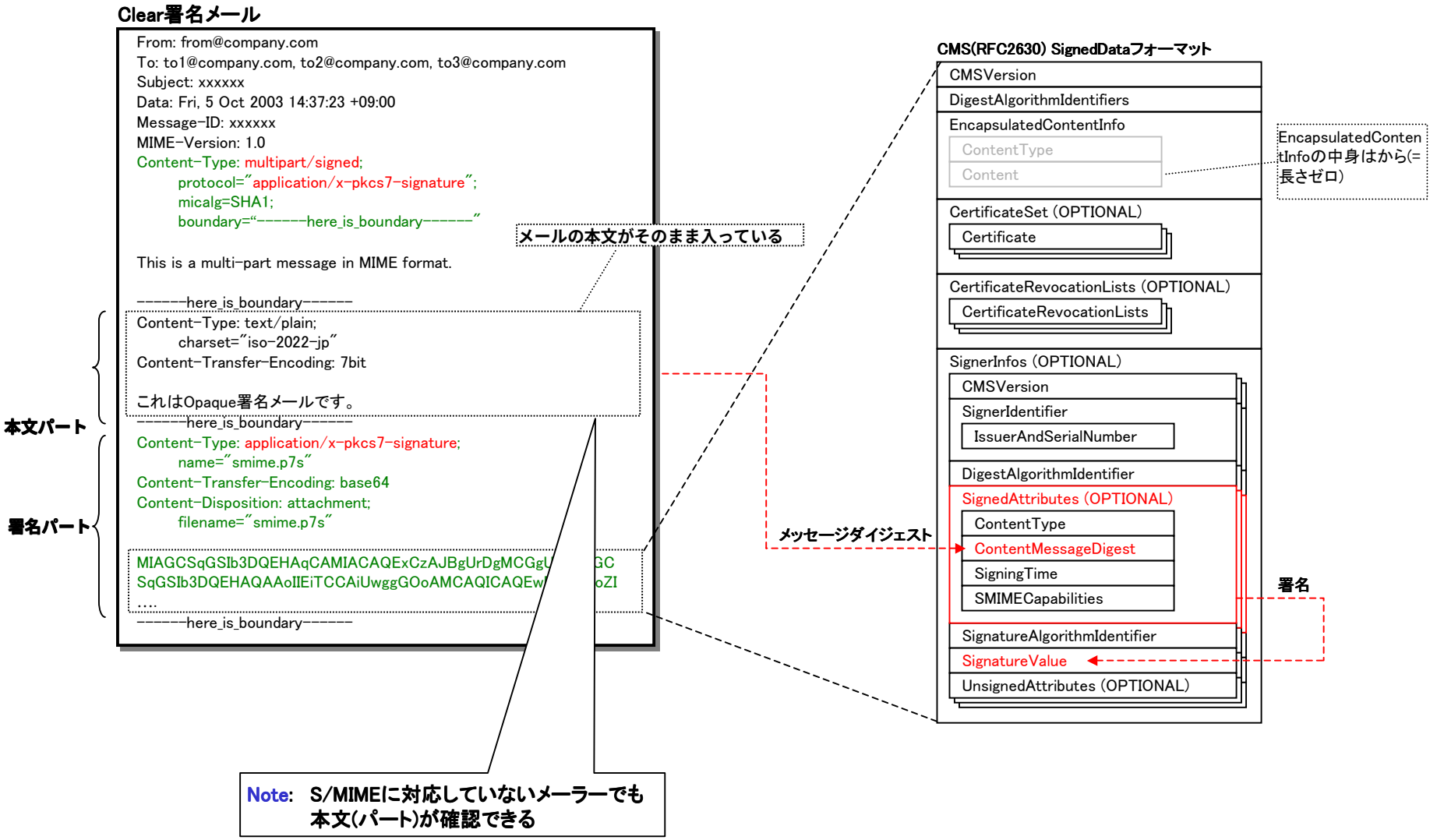


S/MIMEメッセージ内部構造（Opaque署名）

THE DOCUMENT COMPANY FUJI XEROX



S/MIMEメッセージ内部構造（Clear署名）



電子署名アプリケーション

THE DOCUMENT COMPANY FUJI XEROX

- ファイル/データ等に対して電子署名
  - 文書などのデータに署名する
  - コード署名といわれるプログラムへの署名

- 電子署名法の施行/電子政府での採用
- 専用アプリケーション
  - 電子申請など
- 汎用アプリケーション
  - Acrobat
  - Microsoft Office XP
  - DocuWorks

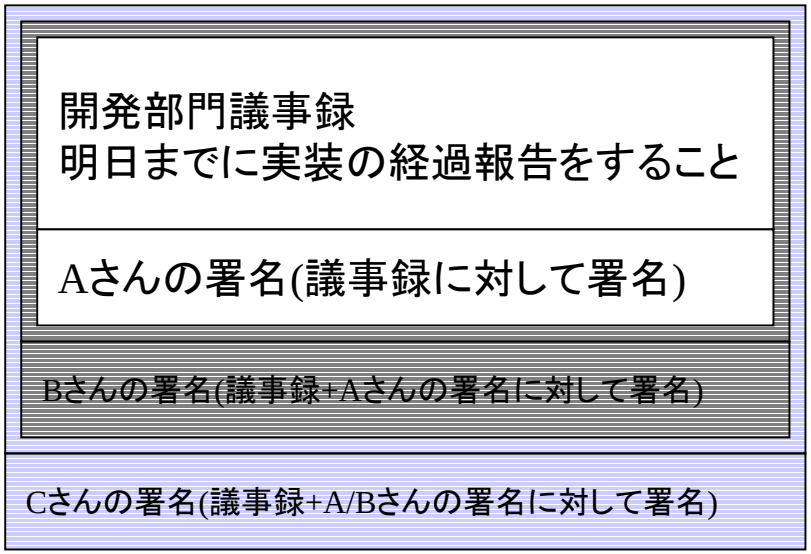
シリアル署名とパラレル署名

THE DOCUMENT COMPANY FUJI XEROX

- 署名をどの部分に行うかの違い
- 用途により使い分けが必要
- Acrobat/Office XP/DocuWorksともにシリアル署名を実装

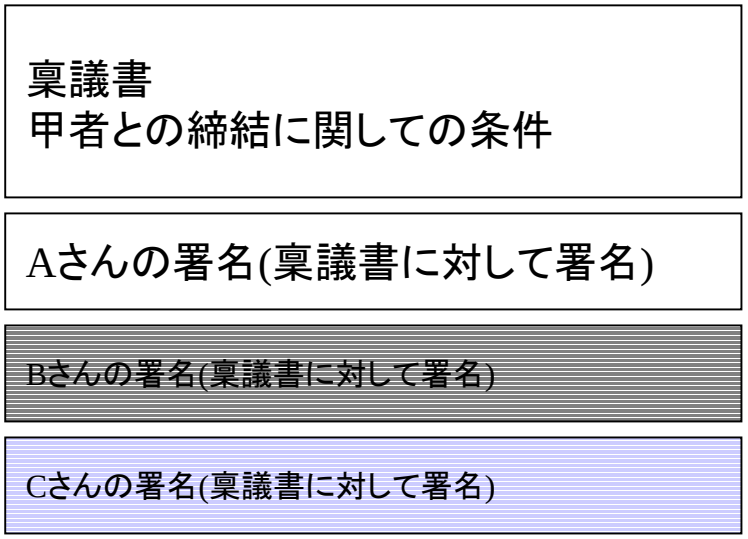
シリアル署名

- 署名を「追加」していくイメージ
- 長所
  - 署名の順番がわかる
- 短所
  - オリジナルの文書に対しての署名



パラレル署名

- 署名対象に対してのみ署名を行う
- 順番に関係なく署名検証可能

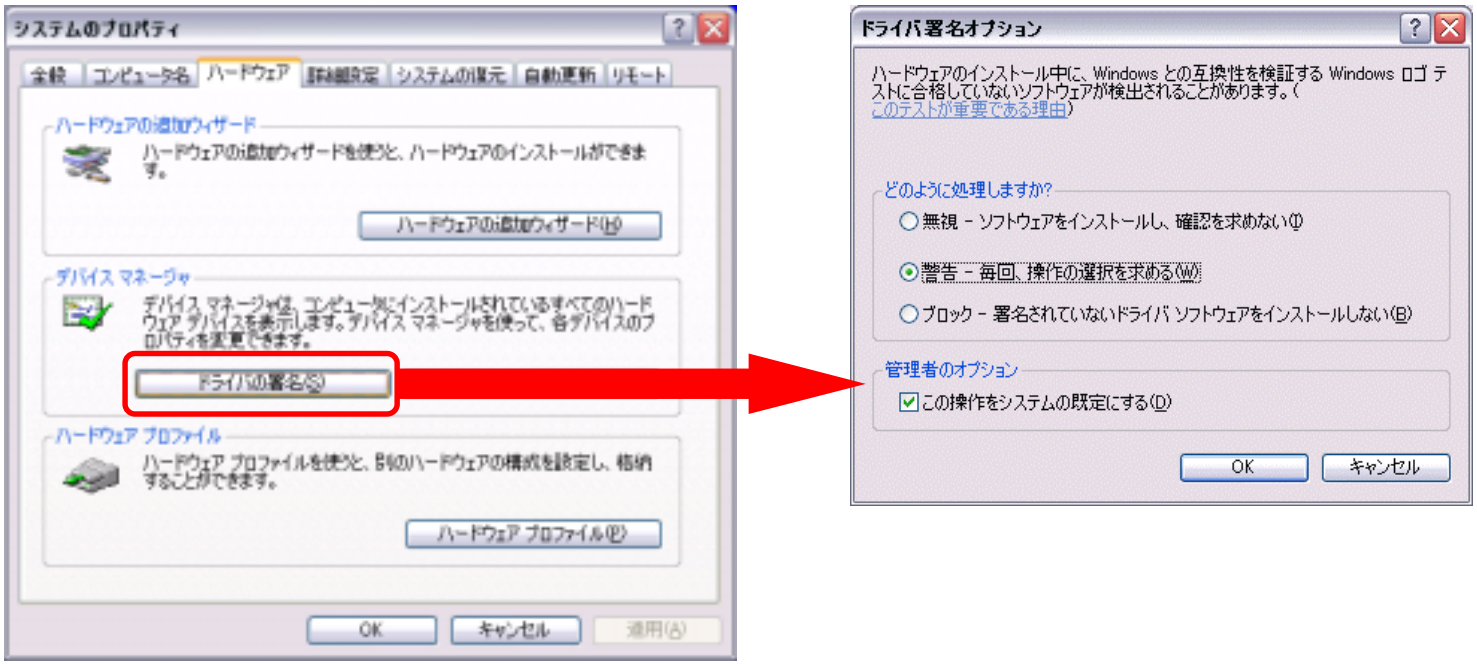


コード署名

THE DOCUMENT COMPANY FUJI XEROX

- ダウンロードしたプログラムが正しいかどうかをどう確認するか?
  - 悪意のあるプログラム/ウィルスの排除
  - 正当なデバイスドライバであるかどうかの確認

Windowsのドライバの署名

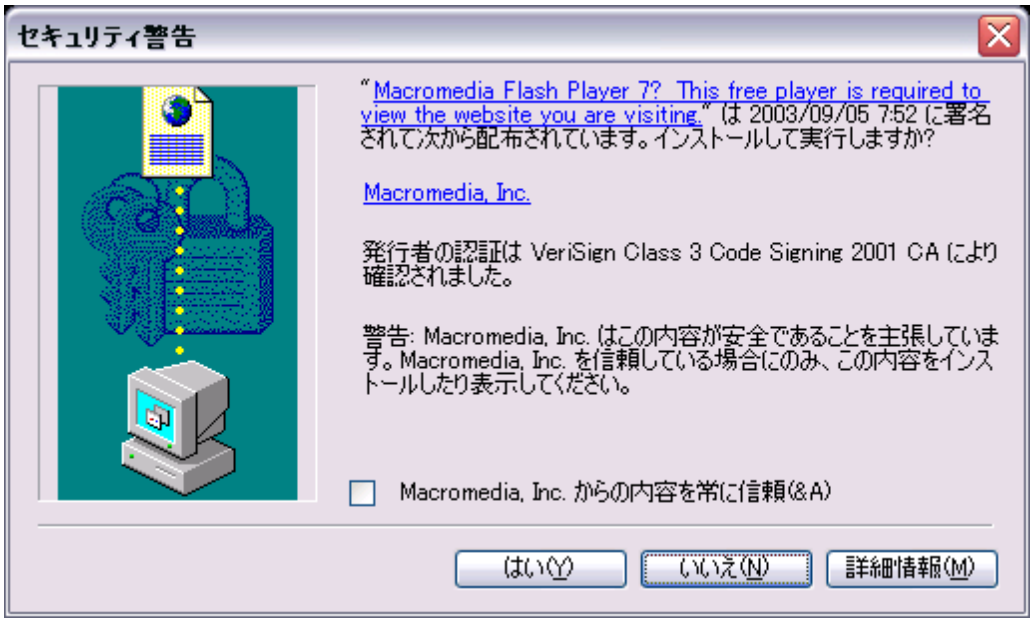


マイクロソフトはWindowsのドライバに対して署名をすることにより、互換性の保障を行っている

Active-Xのコード署名

THE DOCUMENT COMPANY FUJI XEROX

- IEの機能拡張を行うActive-Xモジュールに関してもコード署名を提供している



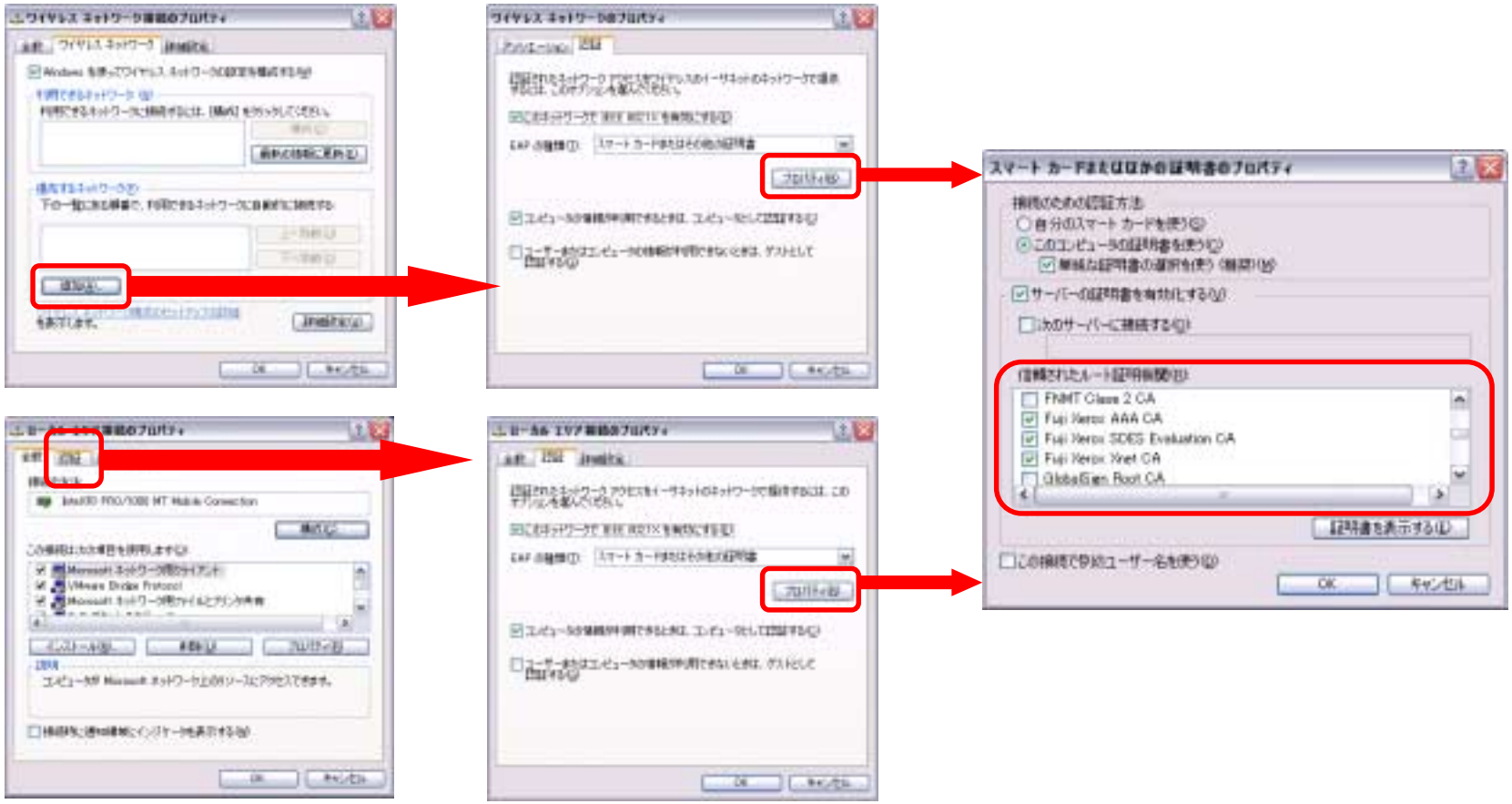
無線LANでの応用(802.1X)

THE DOCUMENT COMPANY FUJI XEROX

- 無線LANが広く使われているが…有線LANに比べ
  - 盗聴
  - 盗用

  が容易に行われている
    - SSID/WEPが広く使われているが、ないよりましな程度
    - IPA(情報処理振興事業協会)が注意を喚起している
- ダイアルアップ接続で認証に広く使われているRADIS認証/EAPを無線でも利用できる

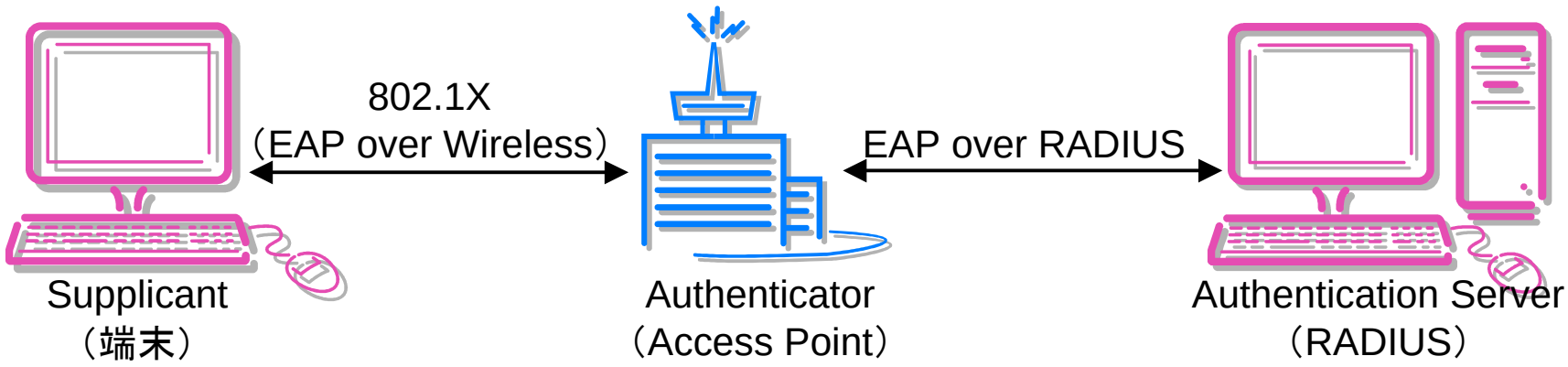
Windows XPでの802.1Xの設定



無線LANベンダがドライバとして提供している場合もあるが、Windows XPでは
ネットワーク接続の機能として有線/無線の区別なくサポートをしている

IEEE802.1x

- 無線/有線LANにおけるユーザ認証の規格
- 認証フレームワークにはPPPの認証機能の部分を拡張したEAPを利用する
- EAPを利用することで、ID/パスワードによる認証だけでなく、ワンタイム・パスワードやセキュリティトークンカード、電子証明書などによる認証が可能



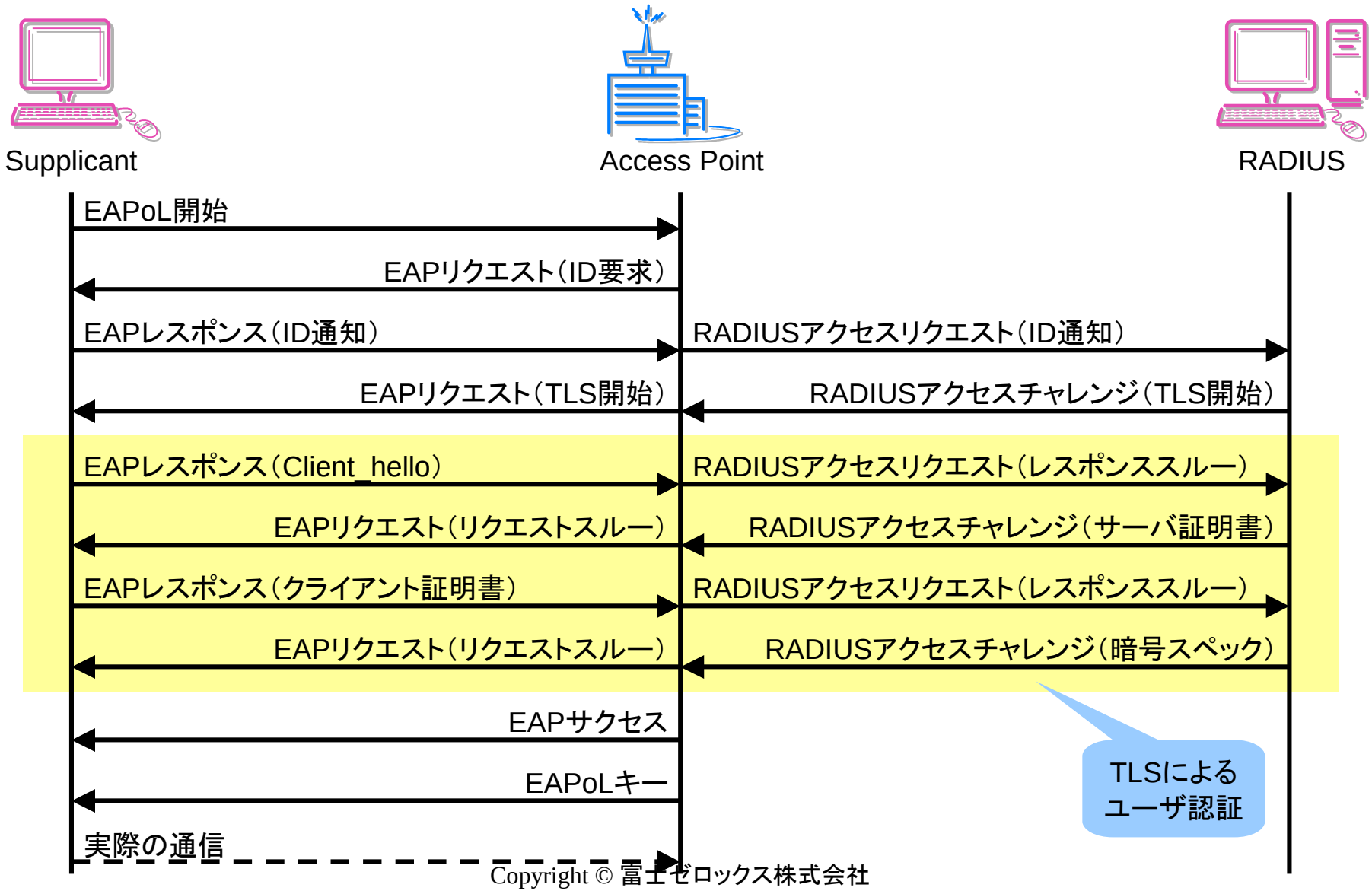
EAP

- EAP-TLS
  - TLSのハンドシェイクプロトコルを利用する認証方式
  - クライアント/サーバ双方の証明書を利用した相互認証
  - 暗号アルゴリズムの選択
  - 暗号鍵を安全に共有するための階層的な鍵生成

- EAP-TTLS
  - TLSのハンドシェイクプロトコルを利用する認証方式
  - クライアント証明書はオプション（サーバ認証のみ）
  - TLSトンネル内で様々なクライアント認証方式が利用可能（例えばID/パスワードの認証）

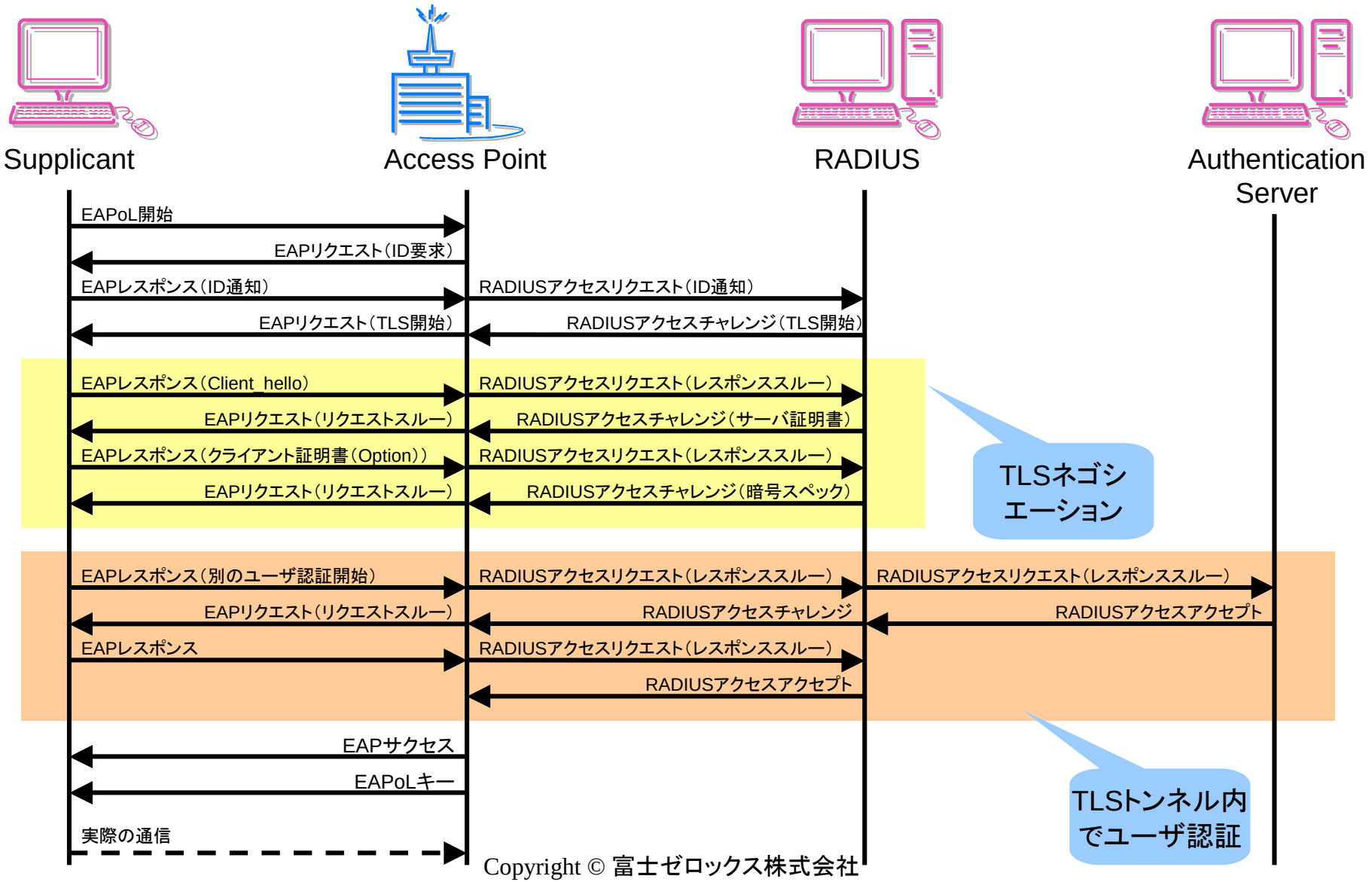
- PEAP
  - TLSのハンドシェイクプロトコルを利用する認証方式
  - クライアント証明書はオプション（サーバ認証のみ）
  - TLSトンネル内で別のEAPを利用して認証を行う

EAP-TLSの認証シーケンス



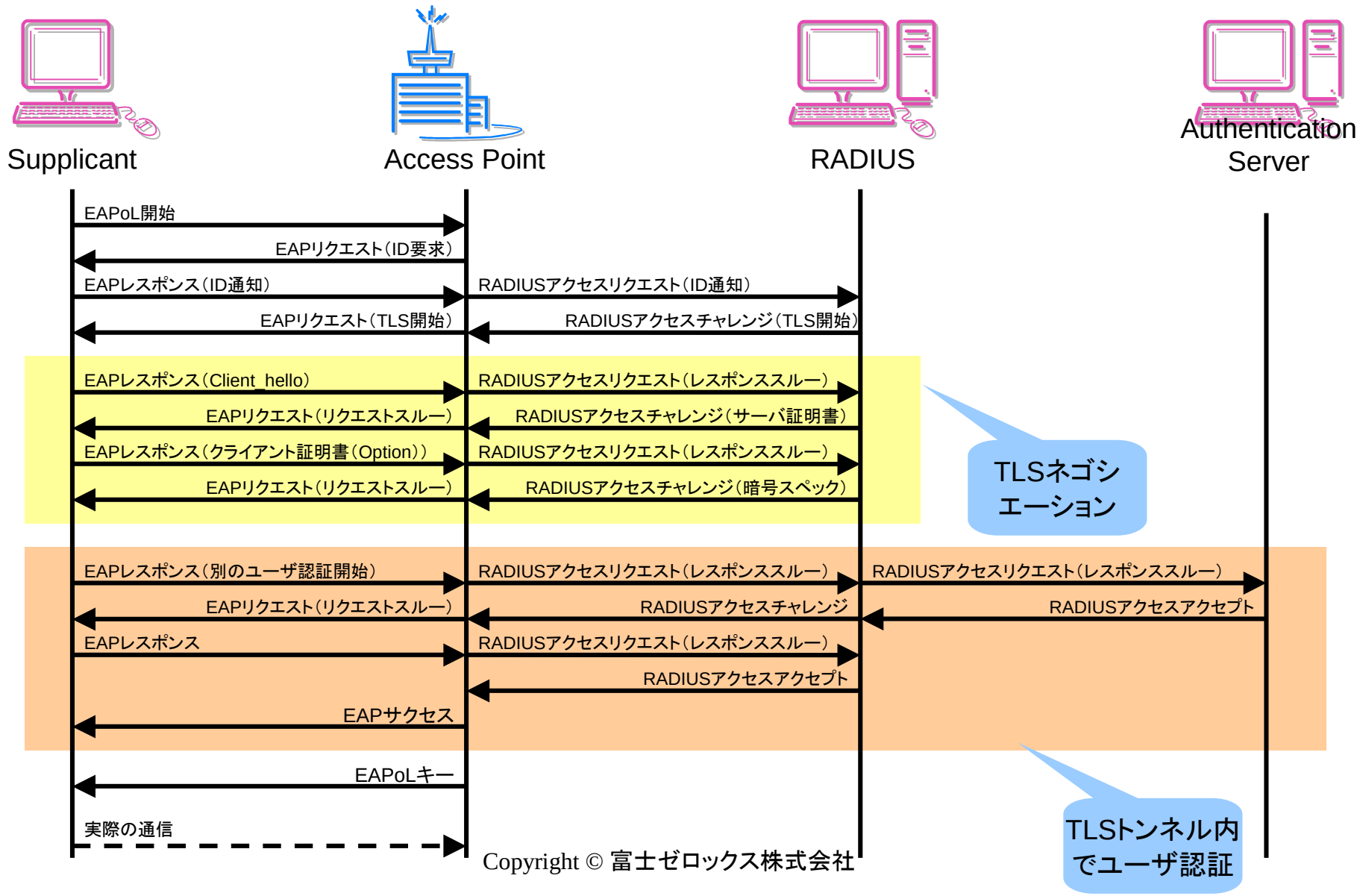
EAP-TTLSの認証シーケンス

THE DOCUMENT COMPANY FUJI XEROX



PEAPの認証シーケンス

THE DOCUMENT COMPANY FUJI XEROX



THE DOCUMENT COMPANY
FUJI XEROX

PKI実装

PKI実装面

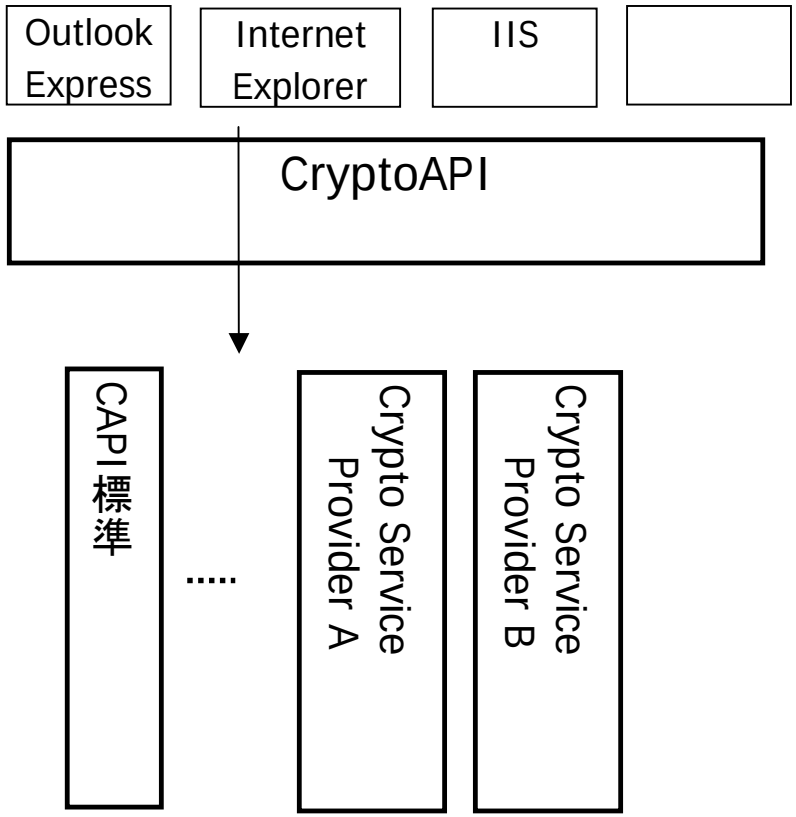
THE DOCUMENT COMPANY FUJI XEROX

- Windows系
  - Crypto API(Microsoft)
  - OpenSSL
- JAVA系
  - JDK/JCE
- UNIX系
  - OpenSSL

Windows Crypto API

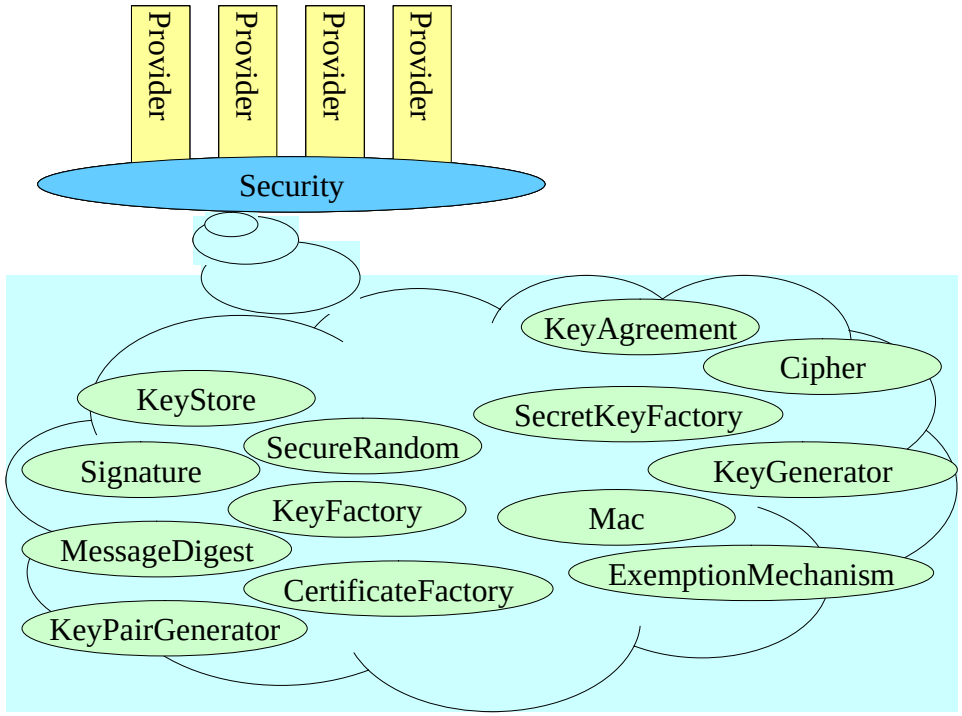
THE DOCUMENT COMPANY FUJI XEROX

- CSP(Crypto Service Provider)モデル
- IE 4.0以降から提供
- 暗号エンジンをモジュール化
- 複数の暗号エンジンを保持
- Third Party提供のCPSを利用可能
- 証明書の検証に関しても良く考えられている
- 暗号エンジンを作る場合、Microsoftにコード署名をしてもらう必要あり



JAVA/JCE

- JAVAの機能拡張モジュールとしてProviderモデルで実装されていた
  - 1.4より標準機能として実装されている
- 暗号機能/Hash機能/X509証明書操作機能を実装



JDK/JCE

THE DOCUMENT COMPANY FUJI XEROX

- java.security.cert以下に実装されている。
- クライアントとして使う面では十二分な実装
  - JDK本体で証明書の基本的なハンドリングが可能
  - JCE(Java Cryptographic Extensions)で暗号周りの機能を提供
    - Windows同様Third PartyのJCEに差し替えることが可能
    - Sunより証明書を発行してもらい、その証明書でコード署名を行う必要あり
  - JSSE(Java Secure Socket Extensions)でSSL/TLSを提供

- RFC3280の証明書検証アルゴリズム相当のメカニズムを実装
- CertPathBulder/CertPathValidator/CertStoreの3つに仮想化
  - CertPathBulder
  - CertPathValidator
  - CertStore

OpenSSL

- 多くのUNIX系プラットフォームのデファクト実装
  - Linux/*BSD*に採用
- Windowsプラットフォームでも動作
- ApacheのSSL/TLSのエンジンとして広く使われている
  - Apache 1.X+mod_ssl+OpenSSL
  - Apache 1.X+Apache_SSL+OpenSSL
  - Apache 2.X(標準でSSL/TLSをサポート)

今後の方向性

今後

THE DOCUMENT COMPANY FUJI XEROX

- 長期署名の話
- 証明書の実効性をあげる
- 楕円関数
- マルチドメイン
- 証明書検証
  - DPD/DPV

長期署名

長期署名

THE DOCUMENT COMPANY FUJI XEROX

- PKIの電子署名の検証では…
  - トップCAからEEまでの有効期間のANDの期間のみ検証可能
- 実社会の契約では…
  - 契約時から3ヶ月以内に発行された印鑑証明があれば有効
- 定期的に署名のしなおしをするなどの対処が必要
- 欧州で活発に議論が行われている
- 58th IETFで新たにLTANS-WGが活動を開始

証明書の実効性/有効性

証明書の実効性/有効性

THE DOCUMENT COMPANY FUJI XEROX

- 昨年の4月にいわゆる「電子署名法」が施行
  - 特定認証局が発行した電子証明書に実印と同様の権限を与えた
- 商業登記法の改正
  - 商業登記局が会社代表者に対して証明書を発行
    - 会社代表者に対しての印鑑証明に相当する
- 欧米では、バイオメトリックス情報を証明書に入れる動きもある
  - 身分証明書の代わりに使える証明書
  - 署名のイメージを入れる動きもある

THE DOCUMENT COMPANY
FUJI XEROX

楕円関数

楕円関数

THE DOCUMENT COMPANY FUJI XEROX

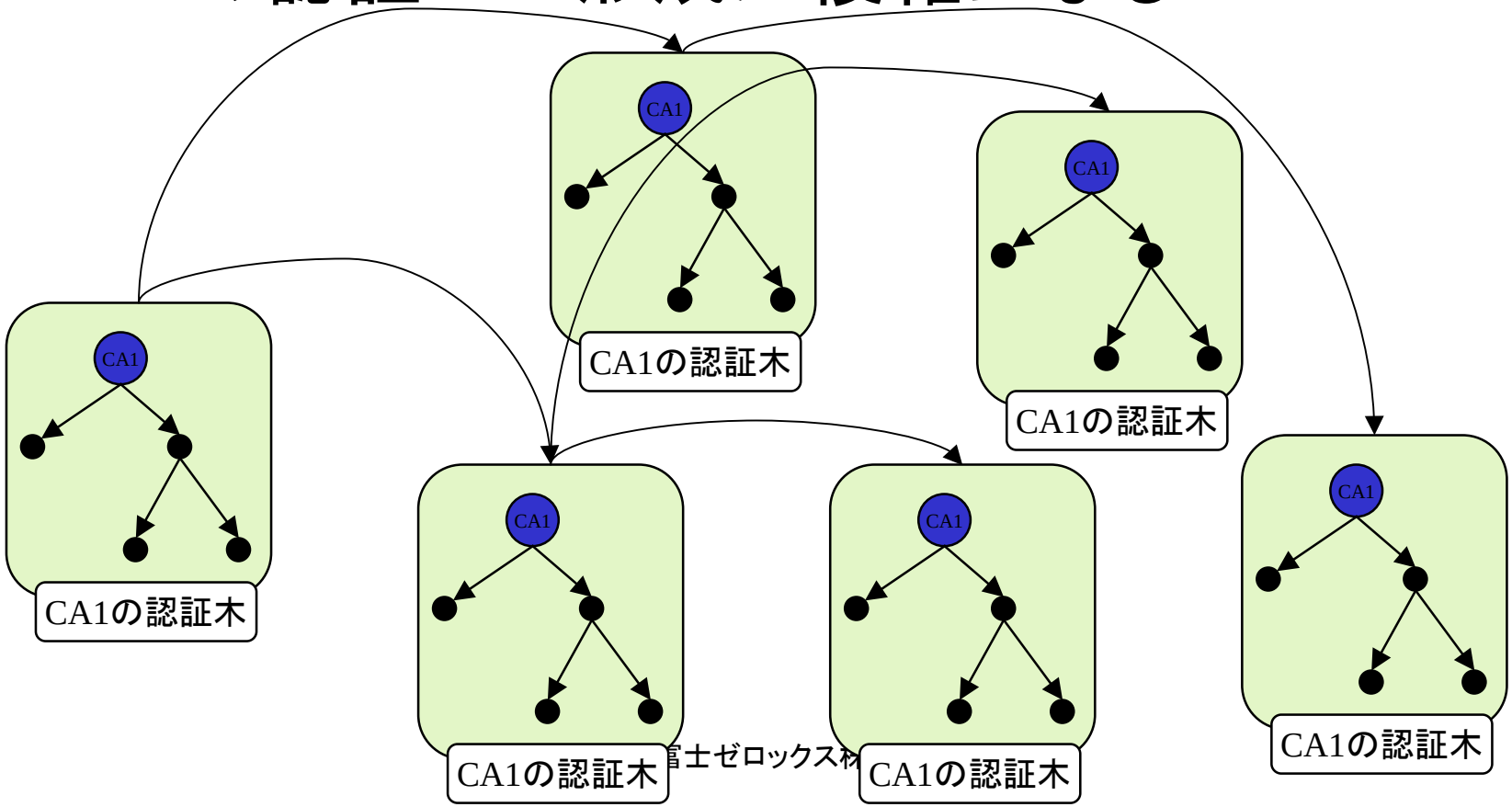
- 楕円曲線の一部を利用して公開鍵として使う
- 証明書の電子署名のアルゴリズムとして RSA/DSAのかわりに楕円関数を使う動きもある
  - 検証がRSAに比べ計算量が少なく、PDA/携帯電話などCPUパワーに限りがある場合に有利
    - とはいえ、このごろのPDA/携帯電話のCPUパワーは馬鹿にできない
  - RSAの1024bit相当の強度を300bit程度で実現
    - 証明書を小さくできる
- OpenSSLにSunが実装を提供

マルチドメイン/BCA

マルチドメイン

THE DOCUMENT COMPANY FUJI XEROX

- 複数のPKIドメインが互いに連携して存在
- PKIの認証パス形成が複雑になる



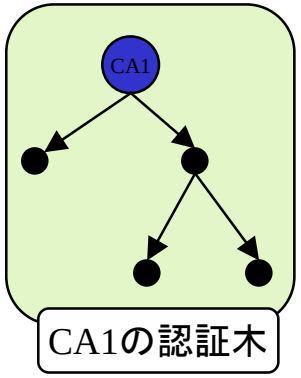
THE DOCUMENT COMPANY
FUJI XEROX

証明書検証

証明書の検証

THE DOCUMENT COMPANY FUJI XEROX

- 木構造の検証でさえ…
  - 証明書の検証プロセス
    - 署名の連鎖の電子署名のチェック
    - 有効期限のチェック
    - CRLのチェック
    - ポリシーのチェック
    - …

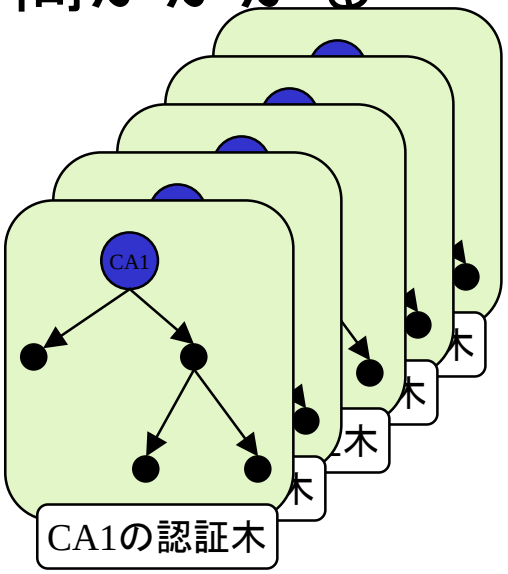


- 複雑で煩雑な処理が必要

証明書の検証

THE DOCUMENT COMPANY FUJI XEROX

- マルチドメイン環境では…
  - パスが長くなるため検証に時間がかかる
  - 木構造での検証に加え
  - ポリシーマップ
  - 相互認証証明書の検証
  - 複数のパスの可能性



- 果たしてすべてのEEが検証できるか?

証明書の検証

THE DOCUMENT COMPANY FUJI XEROX

- 証明書検証を委任
  - EEでは荷が重い
  - サーバに証明書検証を依頼
  - サーバには十分な資源とネットワークコネクティビティを提供
- RFC 3379

  Delegated Path Validation and Delegated Path Discovery Protocol Requirements
  - DPD(Delegated Path Discovery)
    - パス構築を依頼
  - DPV(Delegated Path Verification)
    - パス検証を依頼

証明書の検証

THE DOCUMENT COMPANY FUJI XEROX

- CVS(Certificate Validation Protocol)
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-cvp-01.txt
- SCVP
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-10.txt
- DPD/DPV using OCSP with extensions
- DVCS(Data Validation and Certification Server Protocols)
  - RFC 3029

- GPKI 証明書検証サーバ
  - OCSP v1の独自拡張