# マイクロソフトのセキュリティへの取り組み

2002／03／14

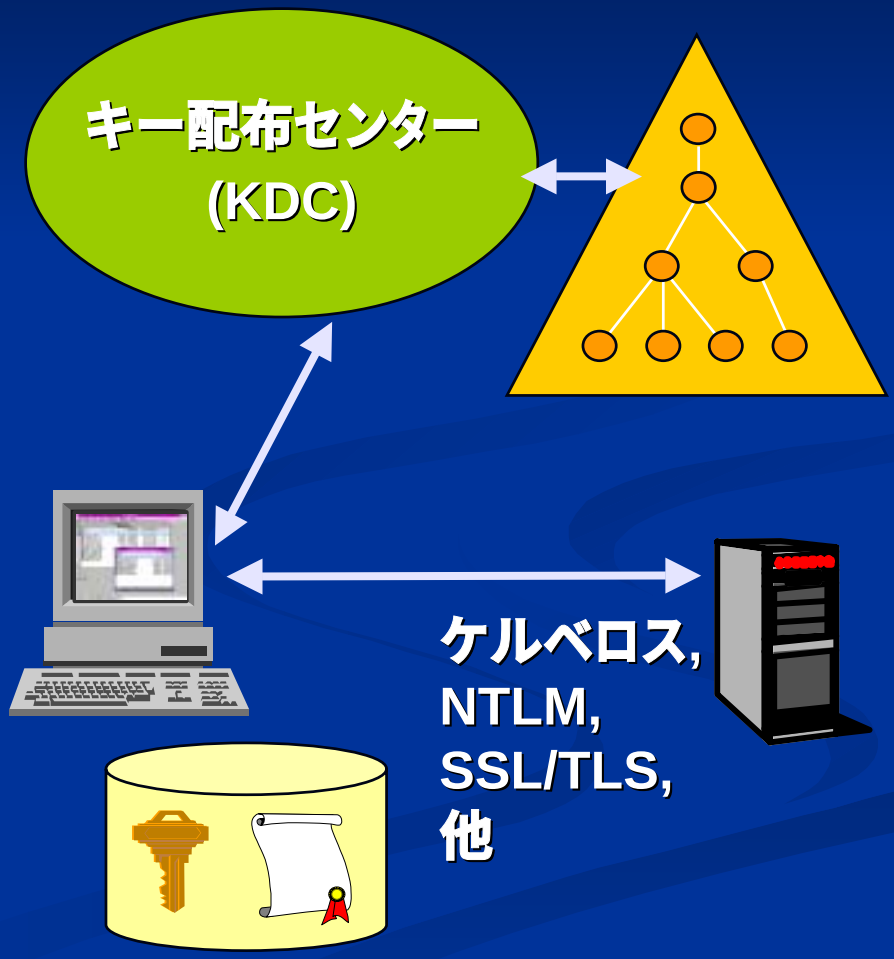
マイクロソフト株式会社
デベロッパー・マーケティング本部
.NETテクノロジー部
加藤健二

# 目次

- ***提供するセキュリティ技術***
  - ***アクティブディレクトリ***
  - ***セキュリティプロトコル***
  - ***ケルベロス***
  - ***スマートカード***
  - ***SSLクライアント認証***
  - ***PKI***
  - ***EFS***
- **セキュリティ強化への体制作り**
  - STPP

# Windowsにおけるセキュリティのテーマ

- シングル サインオン
- 標準プロトコルによる認証
  - ケルベロス認証
  - NTLM認証
  - SSL/TLS認証
- クレデンシャル情報
  - スマートカード
  - 公開鍵
- 管理
  - ポリシーベース
- アクティブ ディレクトリ統合
  - アカウントの格納
  - 公開鍵の格納
  - ポリシーの格納



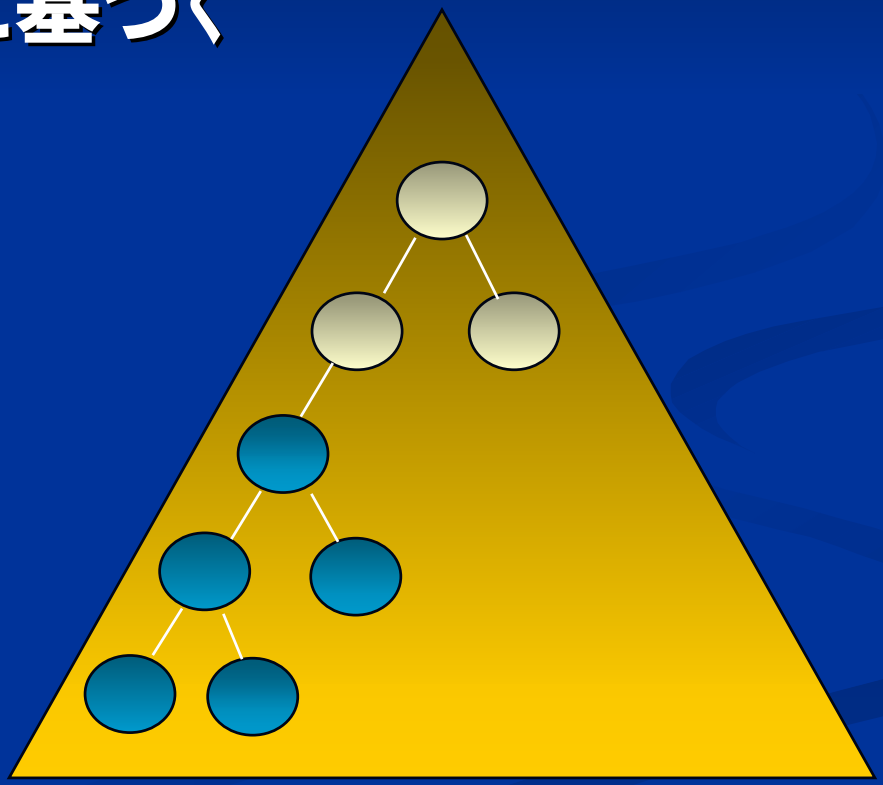
# セキュリティ サービス アーキテクチャ

| | |
|---|---|
| Active Directory 統合 | 階層化したアカウントとポリシーの格納<br>信頼された認証局<br>PKI証明書とCRLの発行 |
| 柔軟な認証メカニズム | 多様な認証メカニズム ( NTLM, バイオメトリックス, PKI, スマートカード ) |
| 一貫した承認モデル | 唯一無二のアイデンティティ<br>インターネット ベースのDNSを統合<br>ケルベロス チケットとWindowsのACL |

# アクティブディレクトリ セキュリティ

# セキュリティ モデル

- Active Directory (AD) を利用した認証と承認の簡単なモデルに基づく



# ADによるアカウント管理の利点

- 組織単位と呼ばれるコンテナでの分類整理
- 多くのオブジェクトのサポート
- 簡単で多様な管理方法
  - GUI
  - スクリプト
- ディレクトリ複製
  - LDAP
  - ディレクトリ同期

# 管理の委任

- 特定コンテナへのプロパティ変更許可を委任
- あるOU下の特定タイプの子オブジェクトの作成や削除の許可を委任
  - ユーザー、グループ、プリンタ
- あるOU下の特定タイプの子オブジェクトの特定プロパティの更新許可を委任
  - ユーザーオブジェクトのパスワード設定

# アクセス権の設定と継承

- アクセス権のレベル設定
  - オブジェクト全体
  - オブジェクト内のプロパティセットで定義するグループに適用
  - オブジェクトの個別プロパティに適用
- アクセス権の継承
  - 上位コンテナで定義されたアクセス権情報の下位への反映

# ADとPKIの統合

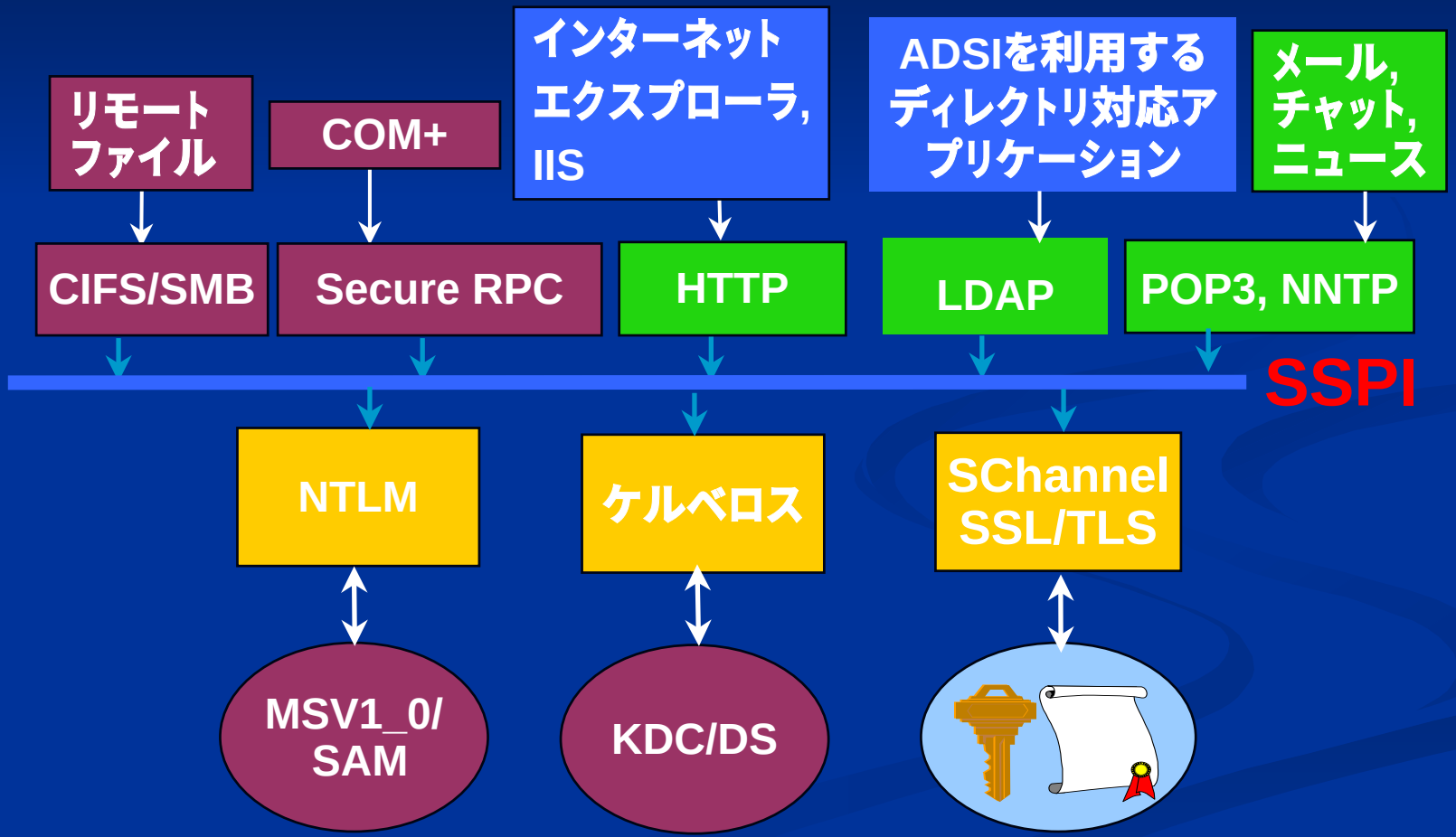
- エンタープライズCAで必須
- ACLによる証明書の管理
- コンピュータへの証明書の自動発行
- (ユーザー証明書の自動発行)
- 証明書、CRL、CTLの公開場所
- 証明書マッピング

# セキュリティプロトコル

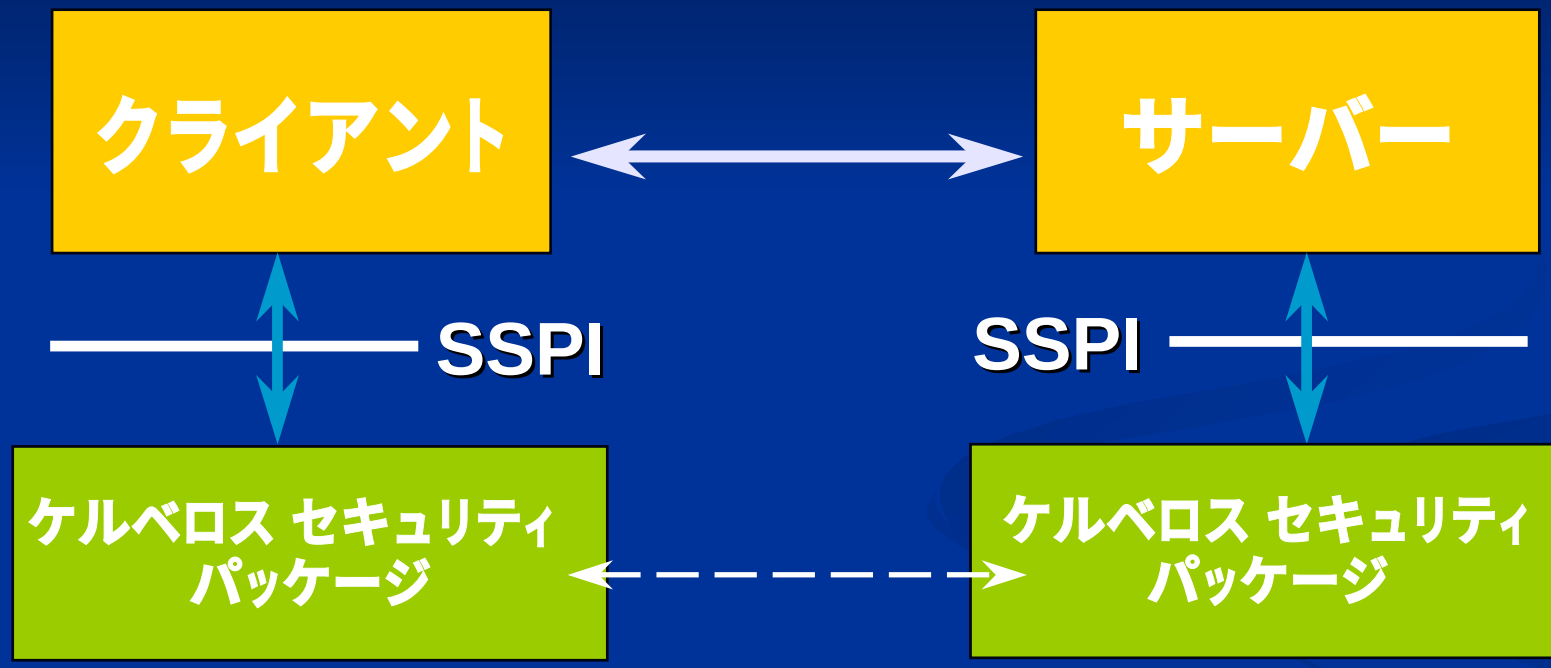
# 複数のセキュリティ プロトコル

- NTLM 認証プロトコル
- Kerberos Version 5 認証プロトコル
- セキュア チャネル サービス

# 複数セキュリティ認証のための アーキテクチャ



# SSPI( Security Support Provider Interface )



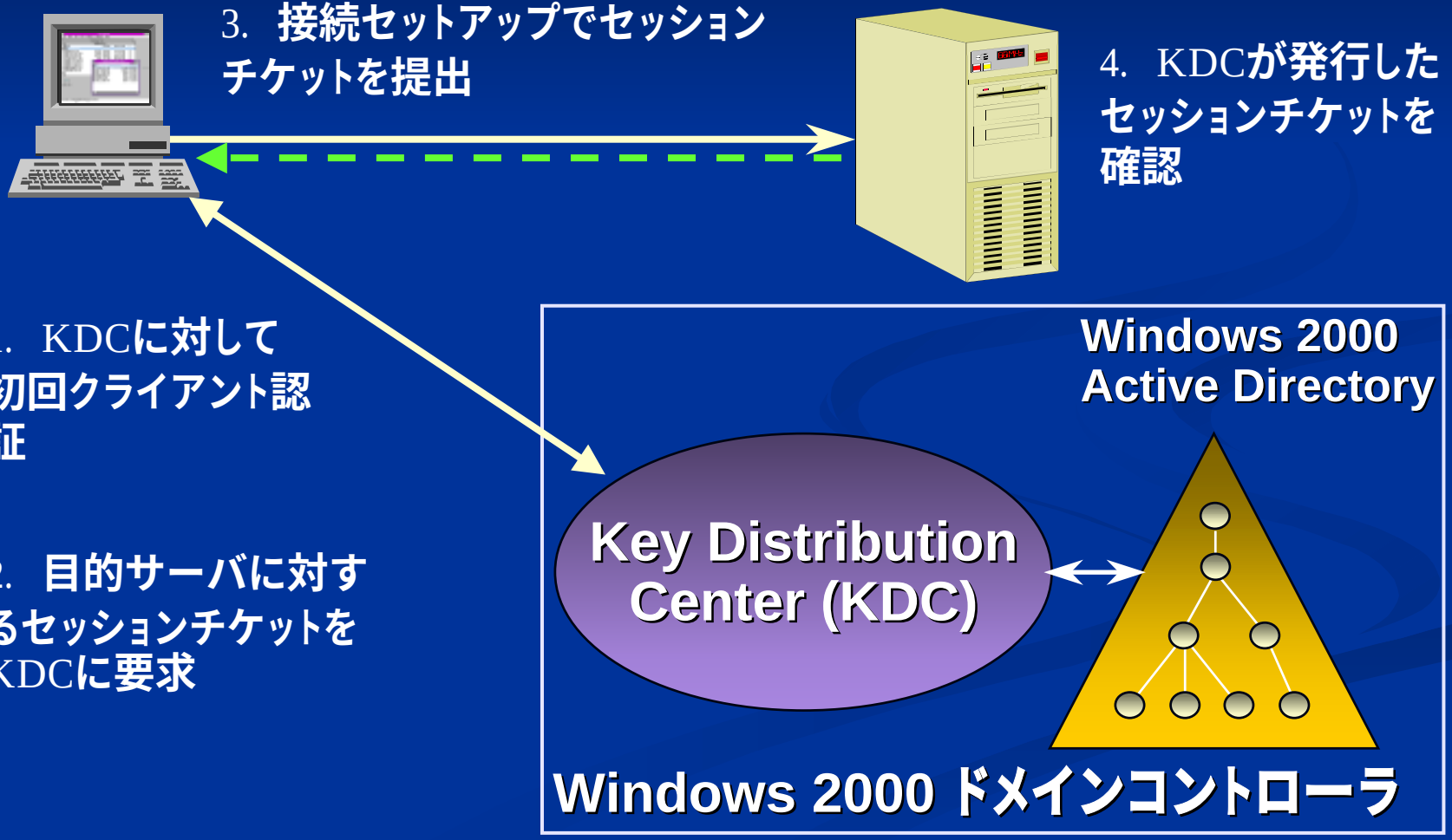

- アプリケーションプロトコル：すべてのデータを運搬
- ケルベロス SSP：セキュリティコンテキストの管理

# ケルベロス

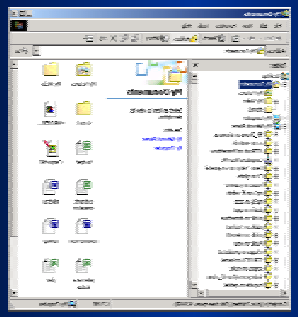
# ケルベロス認証

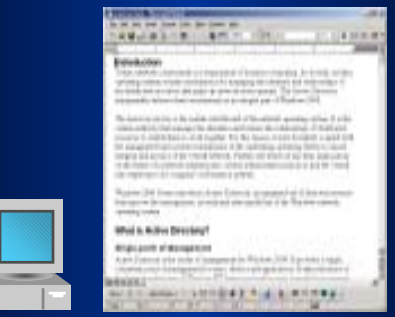
- サーバーに対する認証効率の向上
- 相互認証
- 認証の委任
- 信頼管理の簡略化
- 相互運用

# ケルベロスに関する予備知識



# Windows 2000 ケルベロスの基本

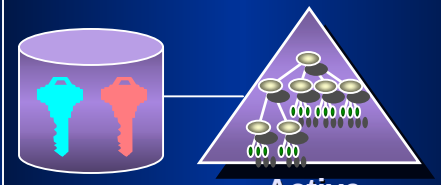





Client Machine

① (Authentication)

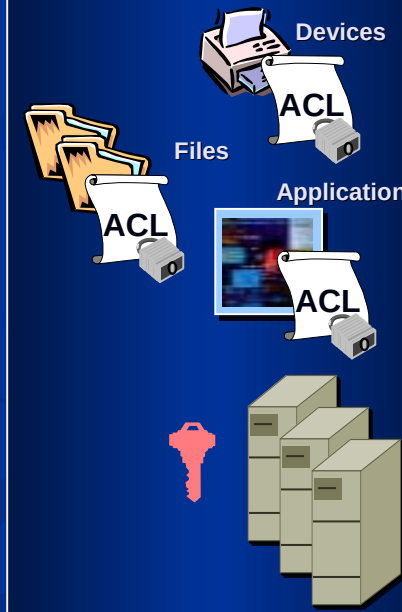
② Ticket




Windows 2000
Domain Controller

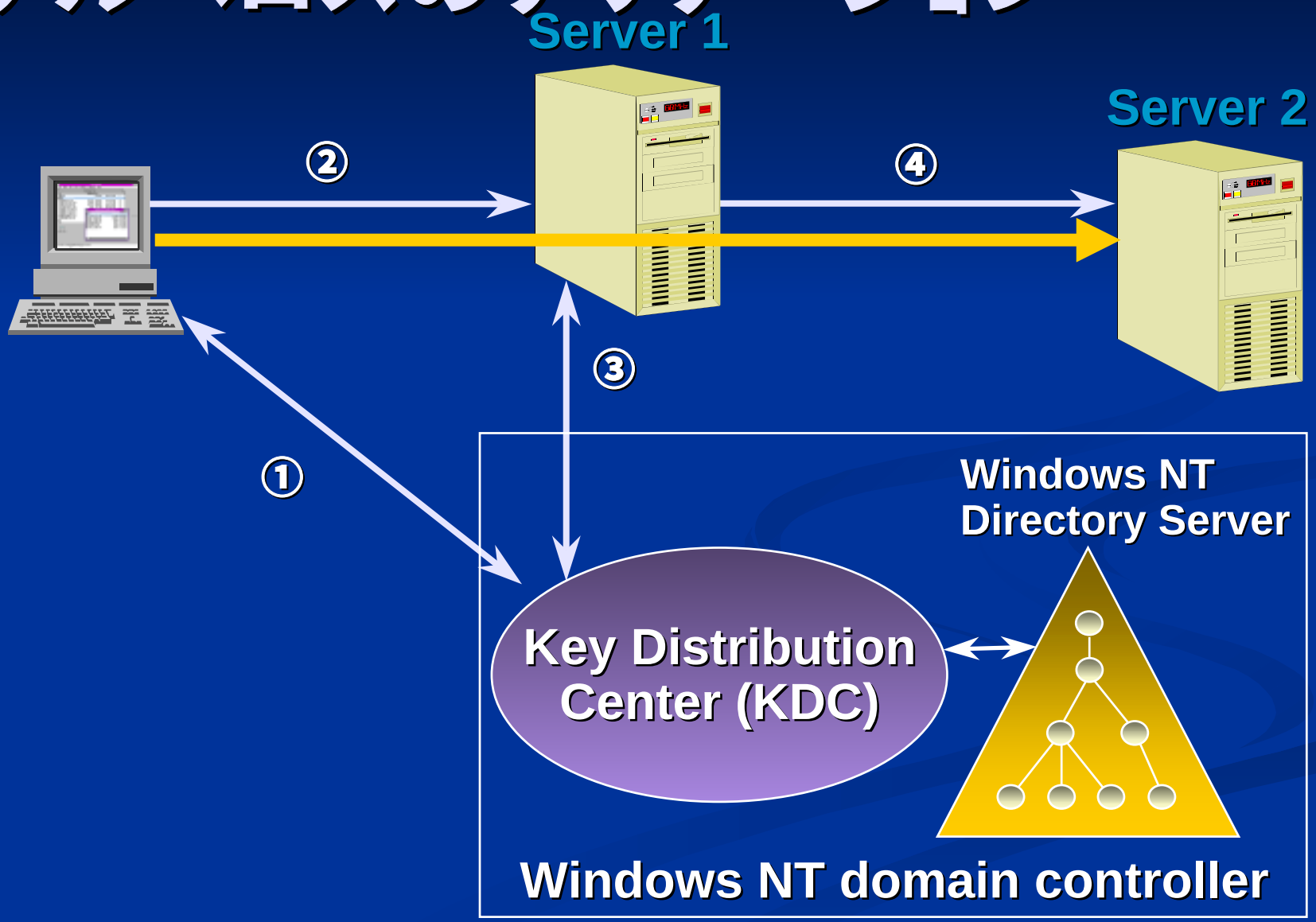
③ (Authorization) Request Ticket

④ 4. Resource



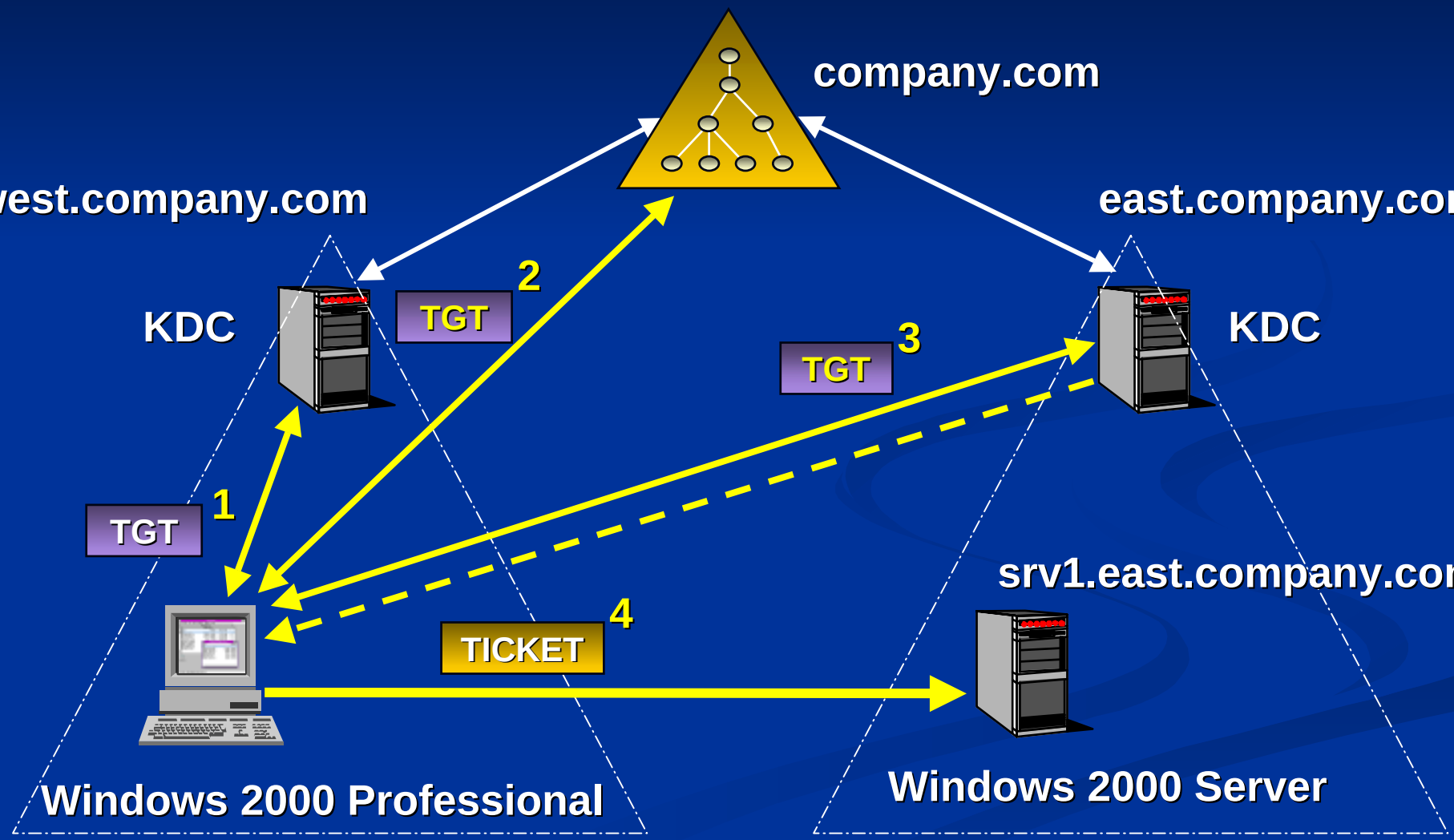

Windows 2000
Server(s)

# ケルベロスのデリゲーション



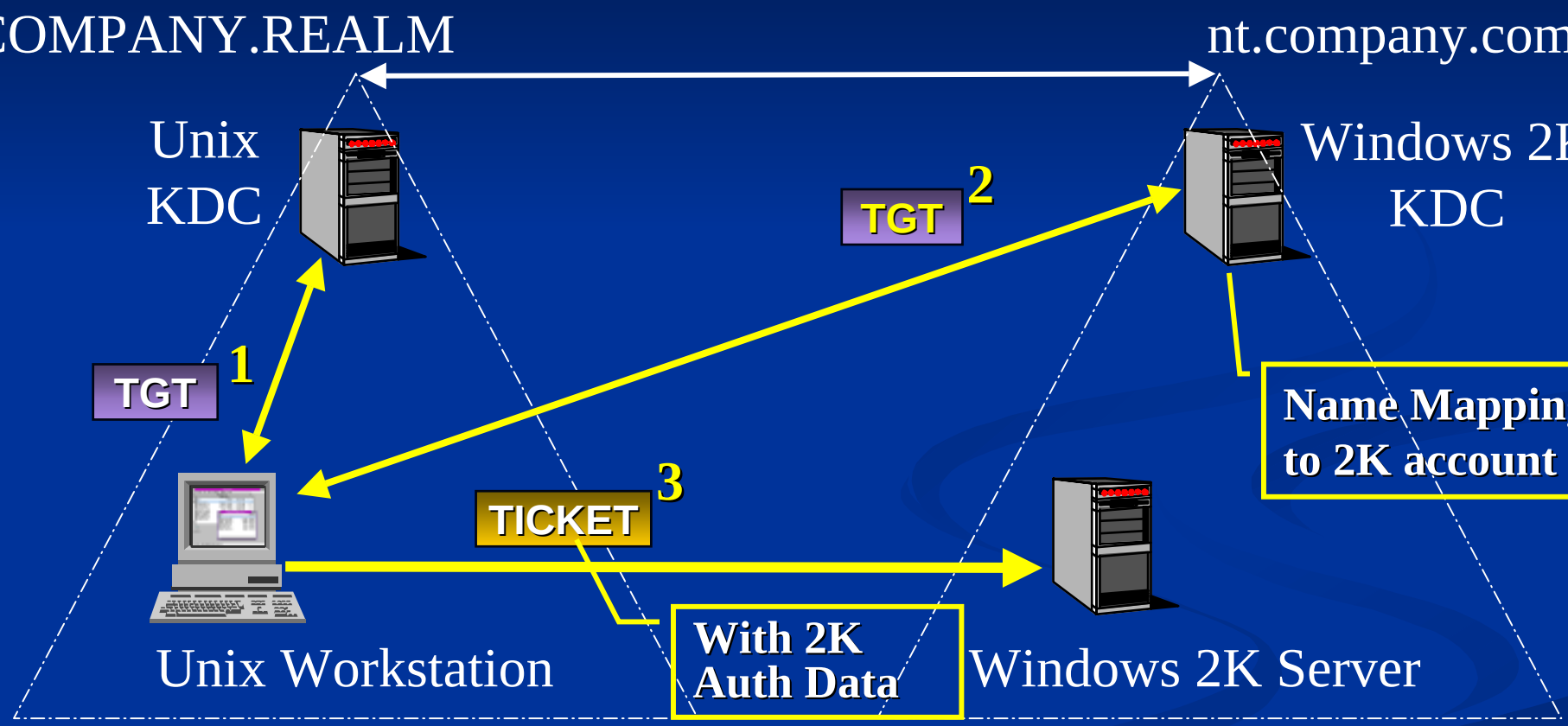
# Windows 2000 ケルベロス

## クロス-ドメイン 承認



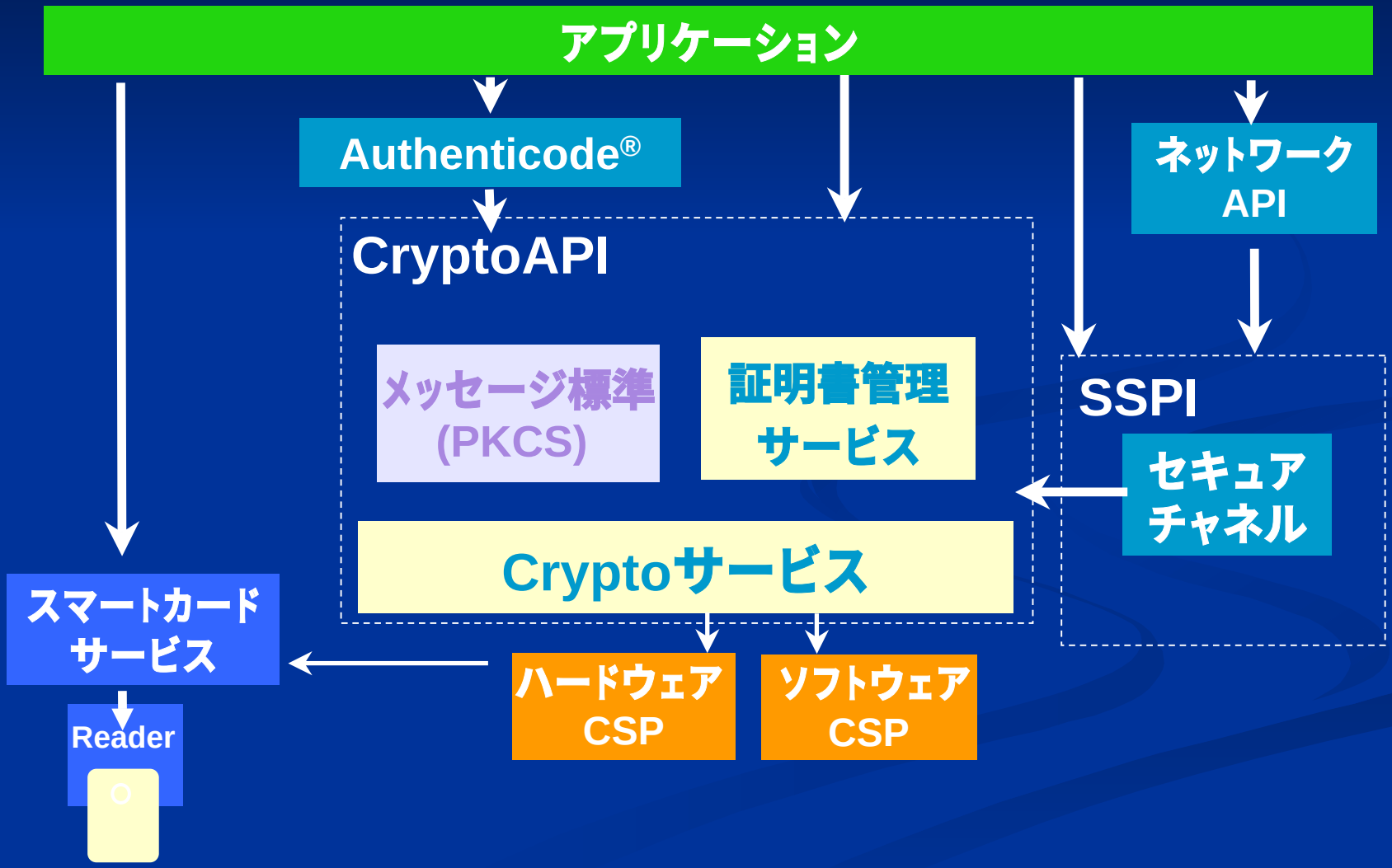
# Windows 2000 ケルベロス

## Unix KDC との認証

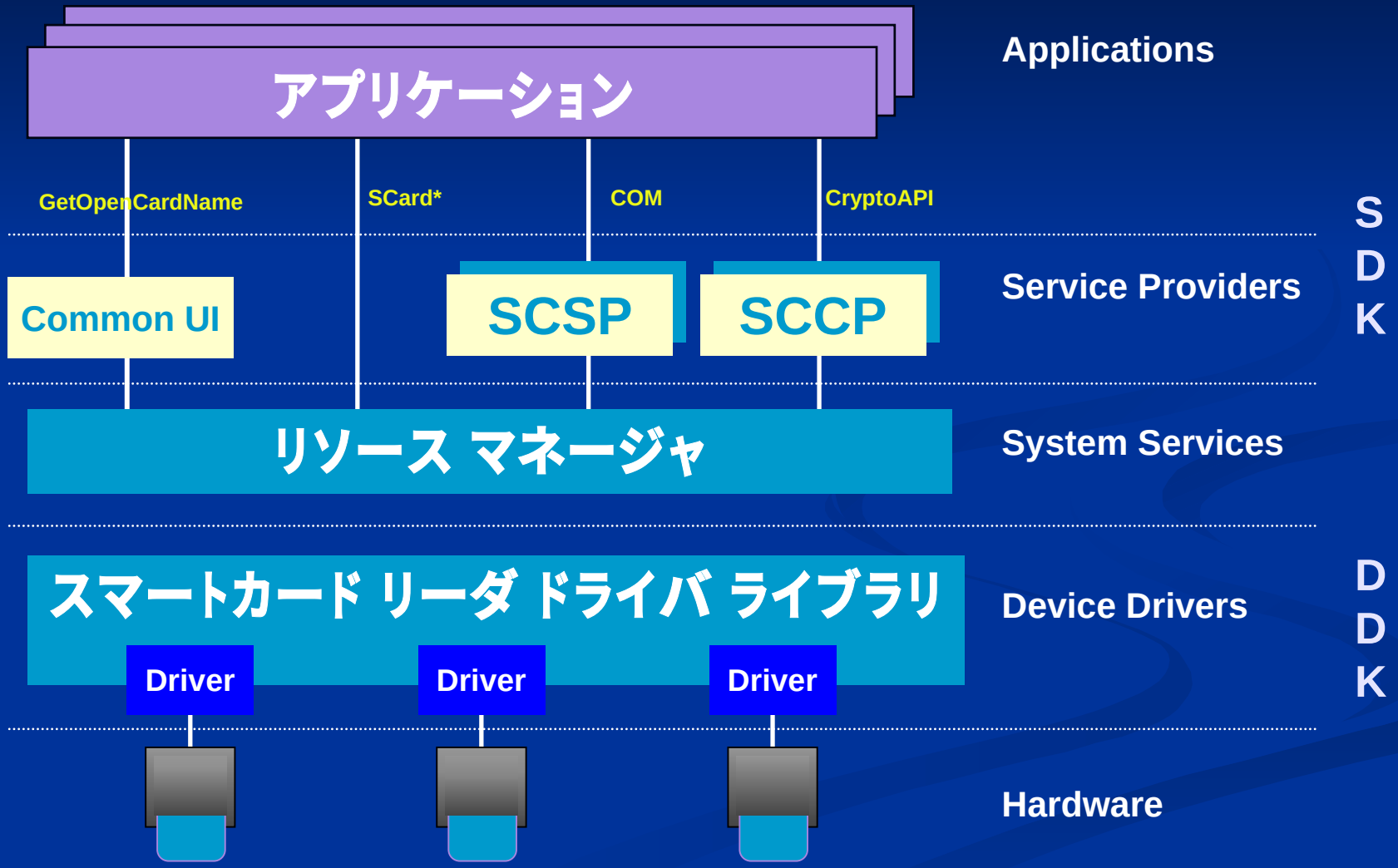


# スマートカード

# CryptoAPI


アプリケーション
Authenticode®
ネットワーク API
CryptoAPI
メッセージ標準 (PKCS)
証明書管理サービス
SSPI
セキュアチャネル
Cryptoサービス
スマートカードサービス
Reader
ハードウェア CSP
ソフトウェア CSP

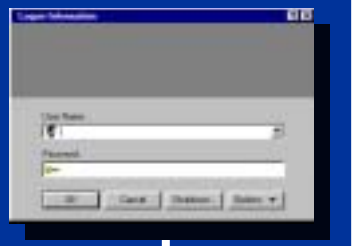
# スマートカード サービス



# Windows 2000 スマートカード

## スマート カード ログオン

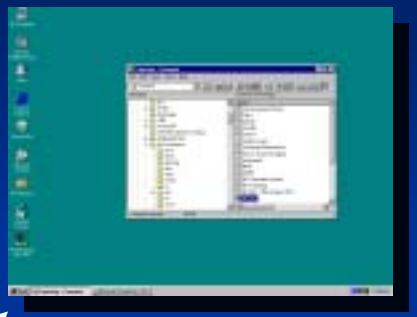

1 Card insertion causes Winlogon to display GINA



2 User inputs PIN

3 GINA passes PIN to LSA

4 LSA accesses smart card and retrieves cert from card



8 Smart card decrypts the TGT using private key allowing LSA to log user on

6 KDC verifies certificate ther looks up principal in DS

5 Kerberos sends certificate in a PKINIT login request to the KDC

7 KDC returns TGT, encrypted with a session key which is in turn encrypted using user's public key


# スマートカードを必要とする理由

クライアント認証、ログオン、電子メールの
利用におけるセキュリティ確保

- 秘密鍵および個人情報に関するフォームを保護するために、改ざんされにくい記憶域を提供する
- 認証、デジタル署名、キー交換などを含むセキュリティ上の重要な演算処理を、システム内の関係のない部分と切り離す
- 勤務先、自宅、または出張先のコンピュータ間で、資格情報やその他の機密情報の移植を可能とする

Windowsプラットフォームに統合している
公開鍵インフラの主要な要素

# スマートカードの利便性

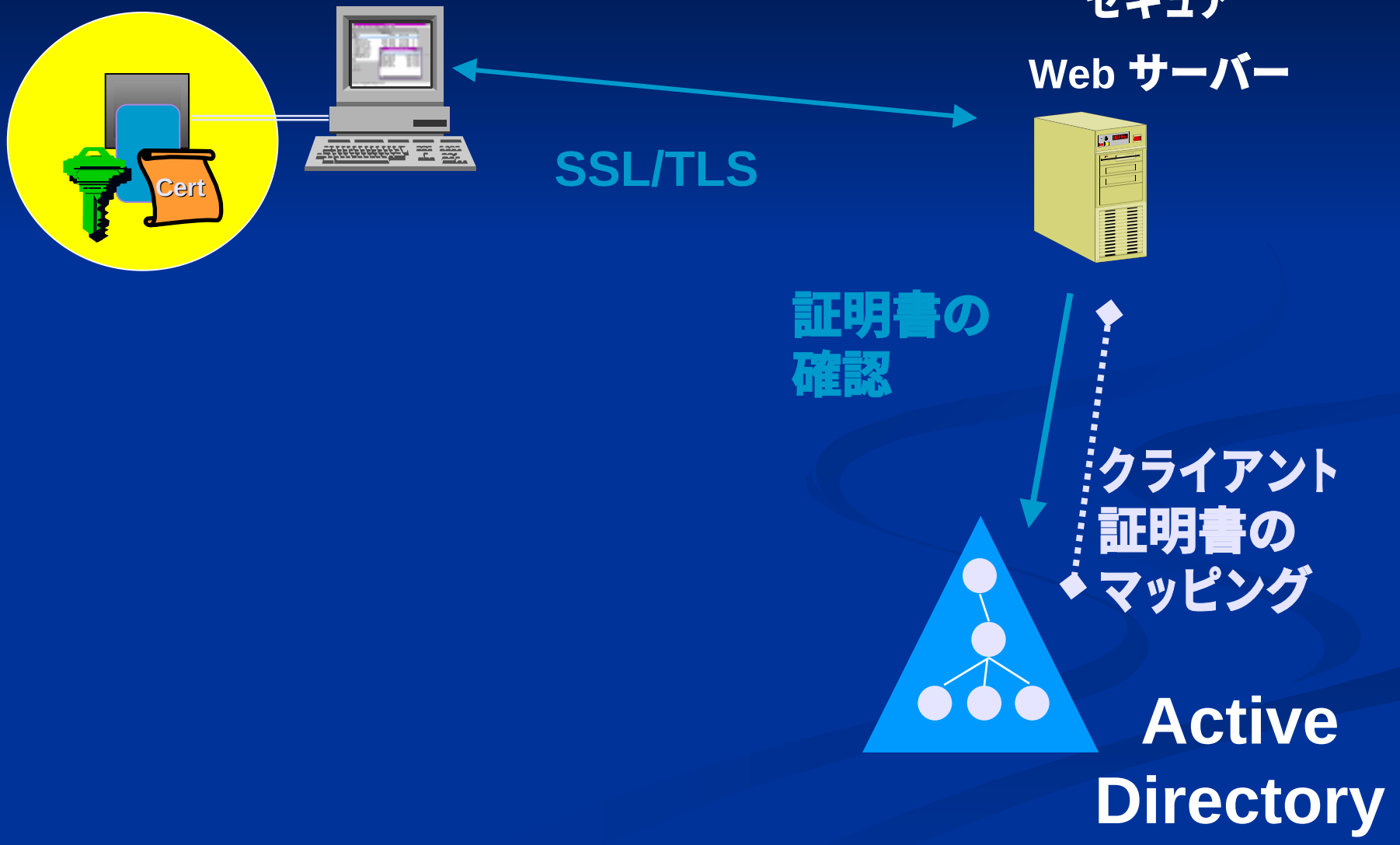
- スマートカード読み取り装置およびカードとコンピュータ間の標準インターフェースモデル
- スマートカードを認識するアプリケーションを作成するためのデバイスに依存しないAPI
- ソフトウェア開発用の使いやすいツール
- すべてのWindowsプラットフォームとの統合

# SSLクライアント認証

# IIS での証明書マッピング

- クライアント証明書をWindowsアカウントにマッピング
- DSマッピング
  - [サブジェクトの別名]のUPNからユーザーを識別
  - エンタープライズCAで自動的に実行
- 1対1マッピング
  - 個別の証明書とアカウントをマップ
- 多対1マッピング
  - 証明書の属性とアカウントをマップ

# DSマッピングによるクライアント認証



# PKI

# PKI – 提供する機能

- プライバシー
- 認証
- 否認不可性

# PKI – 構成要素

- 認証機関
- 証明書公開ポイント
- キーと証明書管理ツール
- 公開キー対応アプリケーション
- ハードウェアサポート

# Windows 2000 PKI – 概要

- 相互運用性
  - PKI標準に準拠したメッセージ、証明書、サービスの交換
- セキュリティ
  - 堅牢なセキュリティアルゴリズムの利用
- 柔軟性
  - 最小限の作業でPKIを構成
- 使いやすさ
  - エンドユーザー、管理者、開発者に使いやすい

# Windows 2000 PKI – 使いやすさ

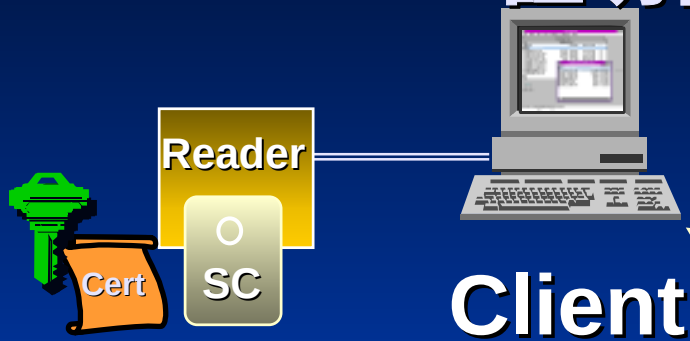
- エンドユーザー
  - 自分の証明書の管理
    - MMCの証明書マネージャ
    - IEのセキュリティの設定ダイアログボックス
- 管理者
  - 既存のMMCを利用
    - 必要に応じて、証明書を無効にできる
    - 証明書やCRLのプロパティの表示
    - 証明書の属性テンプレートを定義できる
    - グループポリシー作成による設定変更

# Windows 2000 PKI – 使いやすさ

- 開発者
  - 3つのセキュリティサービスのセットを提供
    - CryptoAPI 1.0
    - CryptoAPI 2.0
    - SSPI

# Windows 2000 PKI

## 証明書の登録フロー




Client

Root CA

Certificate Request
and Authentication

Subordinate CA

Active
Directory

Publish Certificate?

# Windows 2000 PKI

## SSLクライアント認証

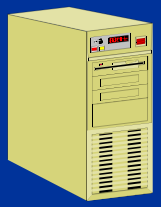

Client

HTTP with SSL/TLS

Secure Web Server

Certificate Enrollment

Subject Lookup



Certification Authority

Active Directory

# Windows 2000 PKI

## セキュアな電子メール (S/MIME)

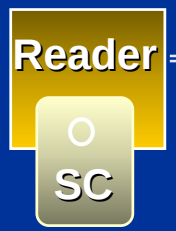
Outlook™ Express

Active Directory

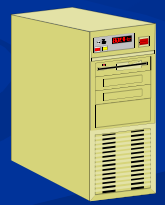
Internet

Retrieve user's certificate (LDAP)

S/MIME

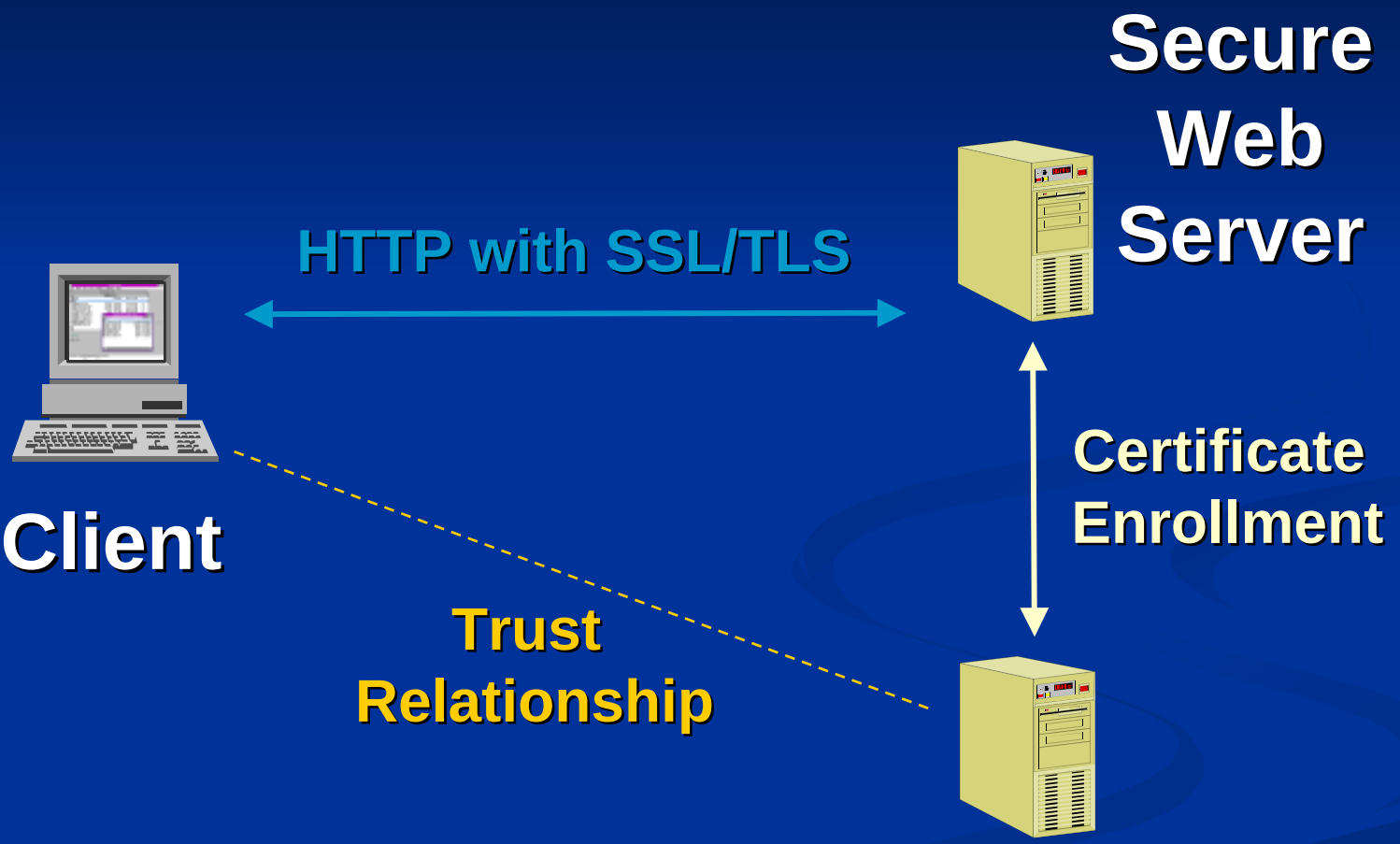

Outlook



Exchange サーバー

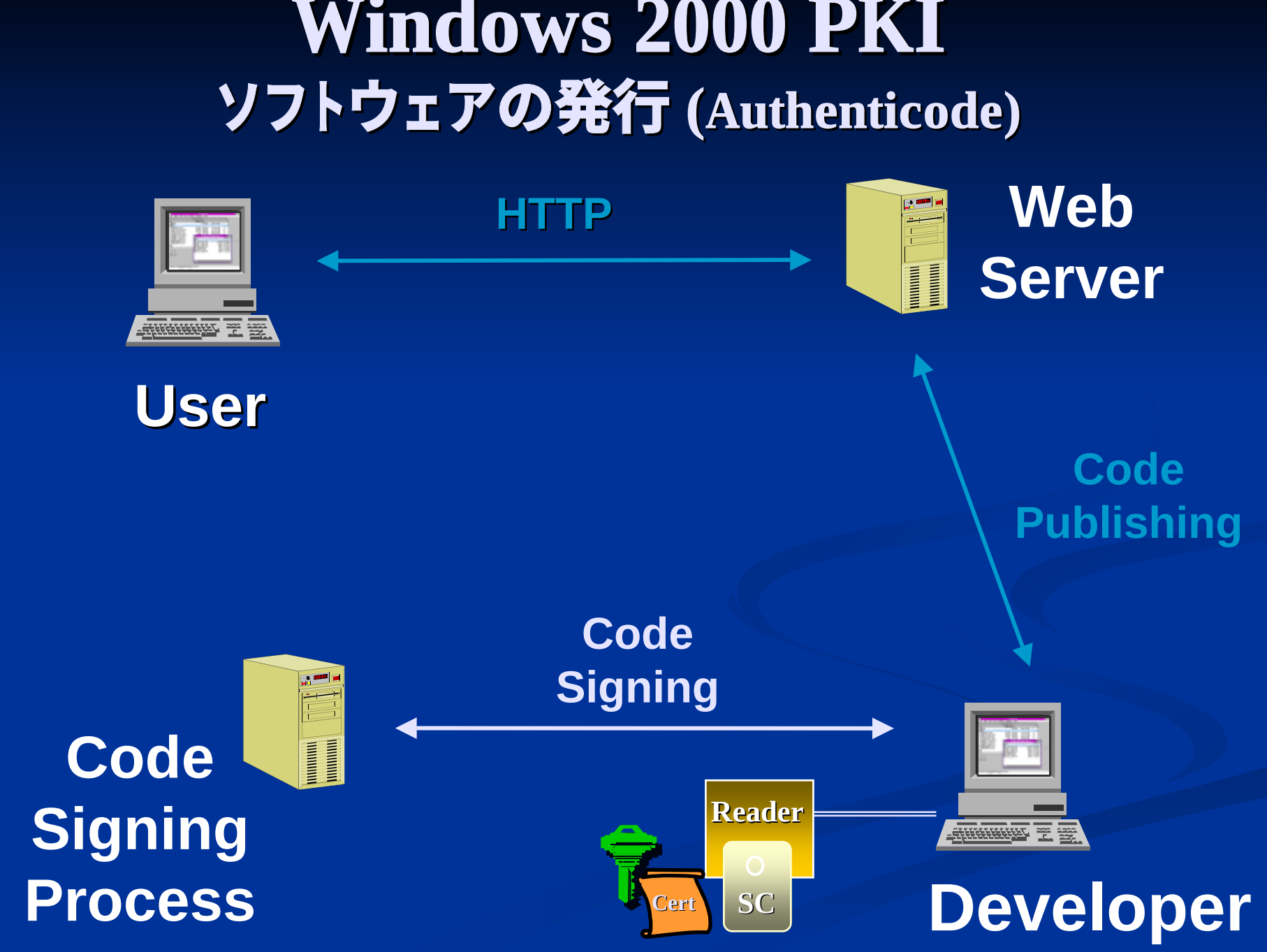
# Windows 2000 PKI

## Eコマース (SSLサーバー認証)



# Windows 2000 PKI

## ソフトウェアの発行 (Authenticode)

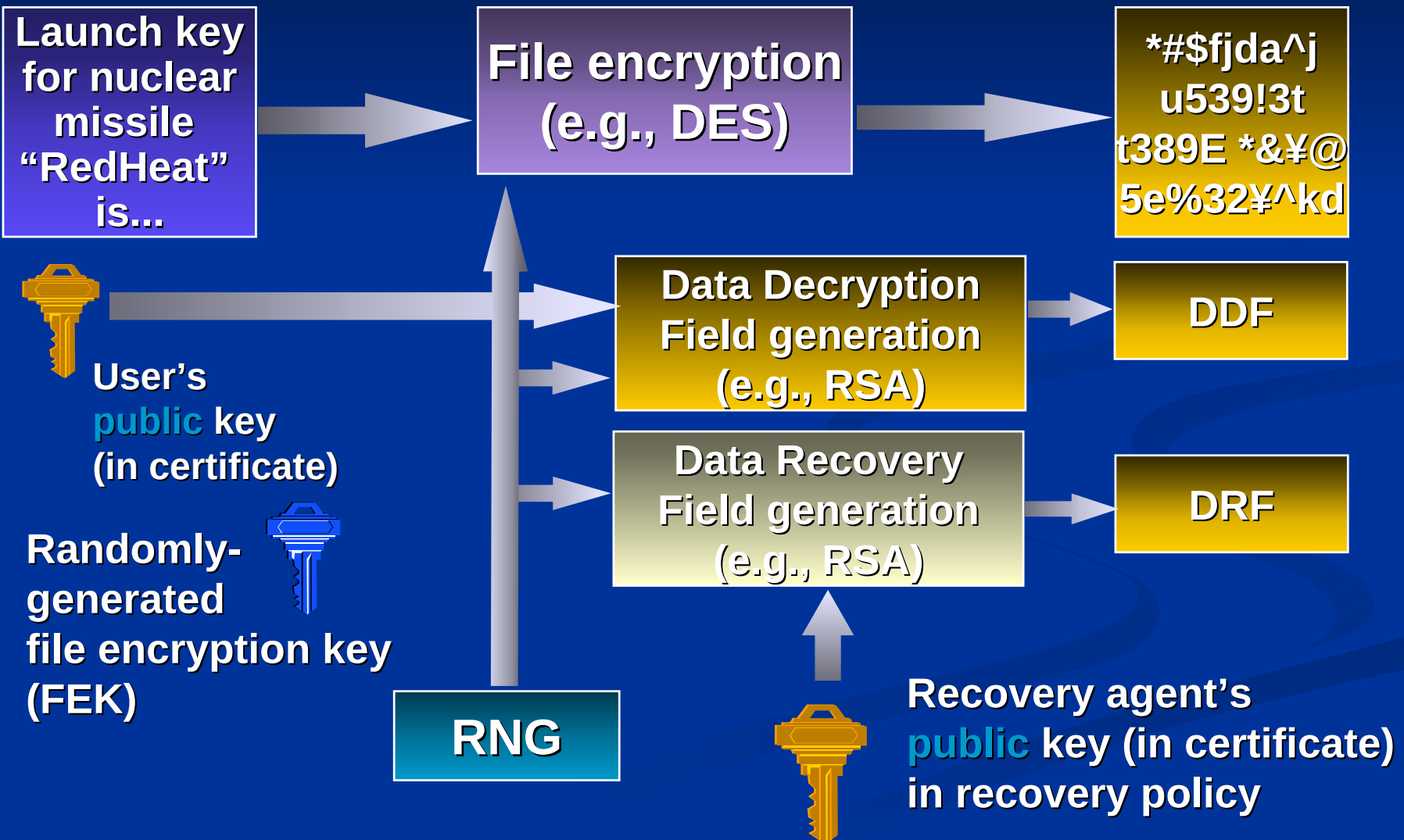


# EFS

# 暗号化ファイルシステム

- ローカルコンピュータ内の指定ファイルまたは、フォルダを暗号化
- 使用時に自動解読、保存時に再暗号化
- NTFSファイルシステムに保存
- 暗号鍵は、ユーザーの公開暗号鍵
- 解読は、ユーザーの持つ秘密鍵
- 管理者は、EFSデータ回復証明書を所有

# データ暗号プロセス


Launch key for nuclear missile “RedHeat” is...
File encryption (e.g., DES)
*#$fjda^j u539!3t t389E *&¥@ 5e%32¥^kd
User’s public key (in certificate)
Data Decryption Field generation (e.g., RSA)
DDF
Data Recovery Field generation (e.g., RSA)
DRF
Randomly-generated file encryption key (FEK)
RNG
Recovery agent’s public key (in certificate) in recovery policy

# データ復号プロセス

*#$fjda^j
u539!3t
t389E *&¥@
5e%32¥^kd

File decryption
(e.g., DES)

Launch key
for nuclear
missile
“RedHeat”
is...

User’s private
key

File encryption
key (FEK)

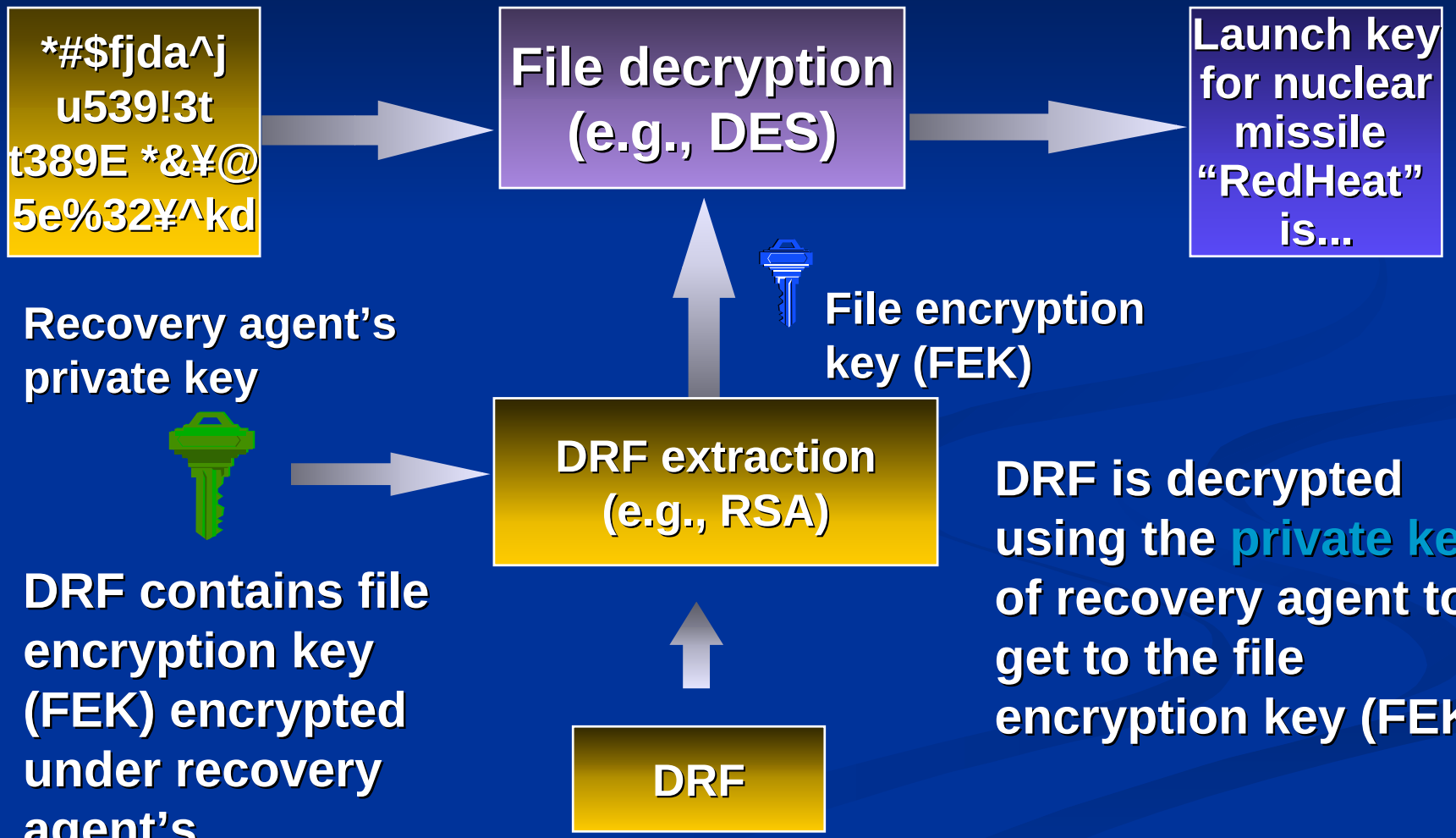
DDF extraction
(e.g., RSA)

DDF contains file
encryption key
(FEK) encrypted
under user’s
public key

DDF

DDF is decrypted
using the private key
to get to the file
encryption key (FEK)

# データ回復プロセス


*#$fjda^j
u539!3t
t389E *&¥@
5e%32¥^kd
File decryption
(e.g., DES)
Launch key for nuclear missile “RedHeat” is...
File encryption key (FEK)
Recovery agent’s private key
DRF extraction
(e.g., RSA)
DRF is decrypted using the private key of recovery agent to get to the file encryption key (FEK)
DRF contains file encryption key (FEK) encrypted under recovery agent’s public key
DRF

# サードパーティCAとのPKI運用

# サポート技術情報：JP273856

- 暗号化ファイルシステムでのサードパーティ認証機関のサポートに関する文書
- 証明書内の[キー使用法]
  - キーの暗号化
  - データの暗号化
- 証明書内の[拡張キー使用法]
  - EFSの識別子(1.3.6.1.4.1.311.10.3.4)

# サポート技術情報：JP281245

- サードパーティCAを用いたスマートカードログオンに関する文書
- 証明書内の[キー使用法]
  - デジタル署名
  - キーの暗号化
- 証明書内の[拡張キー使用法]
  - クライアント認証(1.3.6.1.5.5.7.3.2)
  - スマートカード ログオン(1.3.6.1.4.1.311.20.2.2)

# 目次

- 提供するセキュリティ技術
  - アクティブディレクトリ
  - セキュリティプロトコル
  - ケルベロス
  - スマートカード
  - SSLクライアント認証
  - PKI
  - EFS
- *セキュリティ強化への体制作り*
  - *STPP*

# STPP

## Strategic Technology Protection Program

1. プロダクトの強化とセキュリティ対策ツールの提供
2. セキュリティ情報とサービスの提供
3. パートナープログラム

Get Secure. Stay Secure.

# ストラテジック テクノロジー プロテクション プログラム（STPP）

- セキュリティ問題へのワールドワイドレベルでの取り組み
- セキュリティ アセスメントサービスと対策ツールの提供

| | |
|---|---|
| サービスの提供 | ■ ウィルス問題に対する無償相談・サポート窓口の常設<br>■ プレミアサポート、MCS によるセキュリティ アセスメント |
| オンラインでの情報提供 | ■ セキュリティに関するポータルサイトの開設<br>■ セキュリティ 情報 E-mail 通知サービス<br>■ セキュリティ情報 Rating System |
| プロダクト強化とツールの提供 | ■ Microsoft Security Tool Kit<br>■ セキュリティ メンテナンス ツールと技術資料<br>■ 製品の開発プロセスの強化 |

# セキュリティ関連機能の強化と対策

- Secure Windows Initiative（SWI）
  - マイクロソフト製品のセキュリティ強化を目的とするセキュリティ専任メンバーからなる社内組織
  - マイクロソフト製品の設計、開発、テストフェーズにフォーカス
  - セキュリティ教育、各種ツール、プロセス改善、テスト方法 等に関する指導
  - セキュリティ機能の実装と強化に関して製品開発部門と密接に連携

# Security Tool Kit（日本語版）

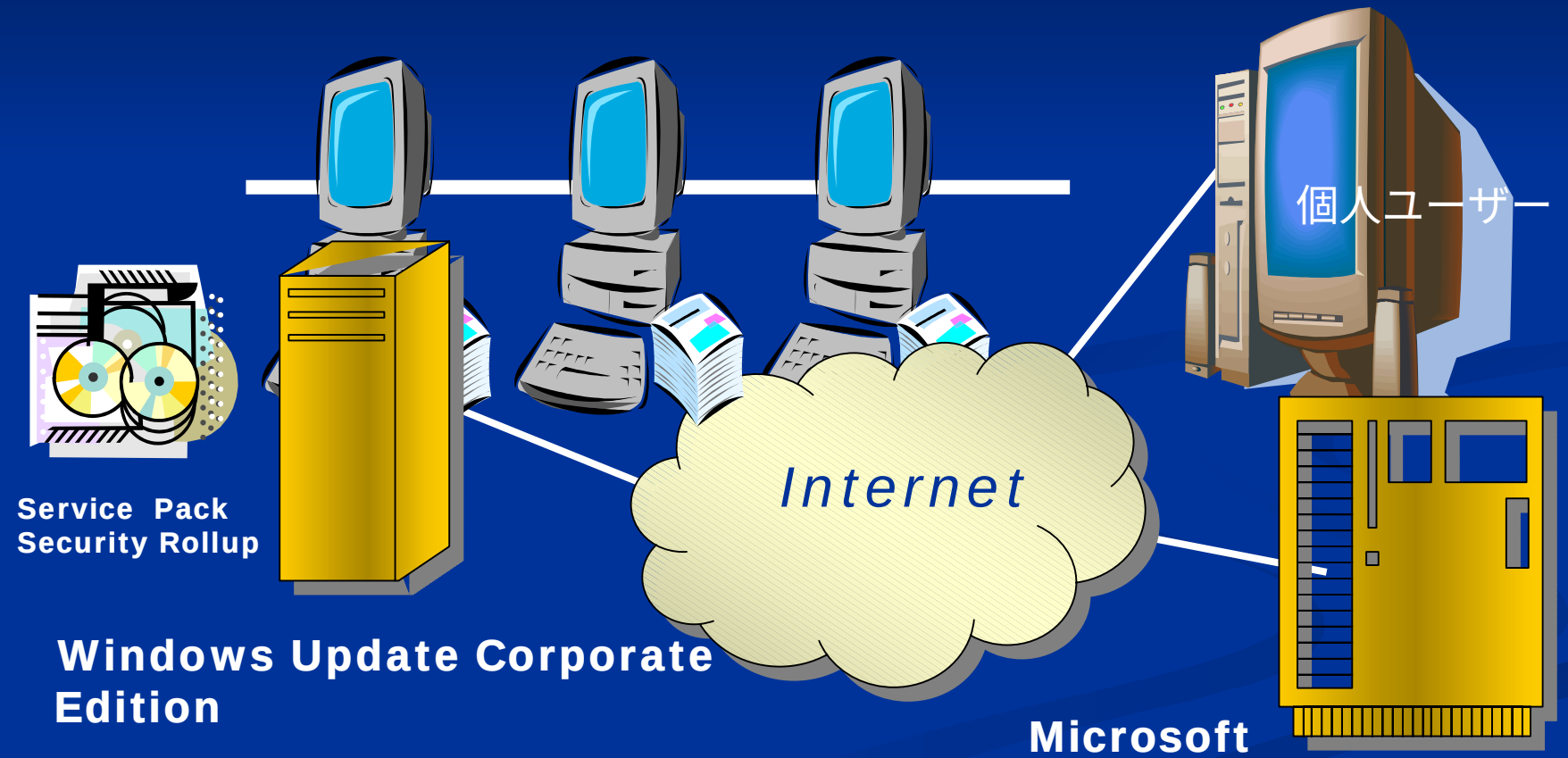
- システム管理者向けのセキュリティリソースを提供
  - Guide
    - セキュアな Windows を構成するための方法
    - 対象：Windows 2000, Windows NT 4.0, Windows NT 4.0 TSE
    - 新規インストールと既存インストール, Step by Step Guide
  - Software Updates
    - 各製品の最新 Service Pack およびセキュリティ ロールアップ
    - Windows 2000 Service Pack 2, Windows NT 4.0 SRP 等
  - Deployment and Management Tools
    - セキュアな Windows を構成するために使用する各種ツール
    - HFNetChk, IIS Lockdown Wizard 等
  - Online Resources
    - TechNet をはじめとする、マイクロソフトがオンライン上で提供するセキュリティ関連情報のご紹介

# サービス／ツールのご利用方法

- **システムの導入時に**
  - Security Tool Kit のSoftware Update で最新のシステムレベルにアップデート
  - IIS Lockdown Tool で利用しないサービスの停止とセキュアな設定を実現
- **運用時のメンテナンス作業に**
  - HFNetChk Tool でセキュリティ修正プログラムの適用状態を把握
  - セキュリティ情報 Rating System でセキュリティ修正プログラムの重要度を確認
  - Security Rollup Patches でセキュリティ修正プログラムを一括して適用可能

# Windows Update- 維持管理の基盤 -

企業ユーザー



# Windows Update
## Windows のオンライン拡張


- 修正プログラムの配信
- セキュリティ修正プログラムの提供
- 新機能の提供
- ドライバーの更新

- 3rd パーティ ドライバの提供

# サービスの提供

- 非契約ユーザー様向けサポート
  - 常設のセキュリティ相談窓口（無償の電話サポート）
    - 「マイクロソフトセキュリティ情報センター」

      0120-69-0196 (月～金　9:30-12:00,13:00-19:00)
  - Security Tool Kit の技術サポート
  - セットアップ、オペレーションについてお答えします。

    （個別の環境への適用はアセスメントサービスにて）

# 日本におけるセキュリティへの取り組み

- ワールドワイドの活動に加え、業界パートナーとの取り組み！

**オンラインでの情報提供**

- セキュリティに関するポータルサイトの開設
  → www.microsoft.com/japan/security
- セキュリティ 情報 E-mail 通知サービス 日本語版
- セキュリティ情報 深刻性評価システム

**プロダクト強化とツールの提供**

- Microsoft Security Tool Kit 日本語版
- セキュリティ メンテナンス ツールと技術資料
- 製品の開発プロセスの強化 － SWI －

**サービスの提供**

- ウィルス問題に対する無償相談サポート窓口の常設
- プレミアサポート、MCS によるセキュリティ アセスメント

＋

**パートナーとの取り組み**

- 継続的なセキュリティ対策の啓蒙活動
- 業界連絡網と緊急告知フレームワークの構築

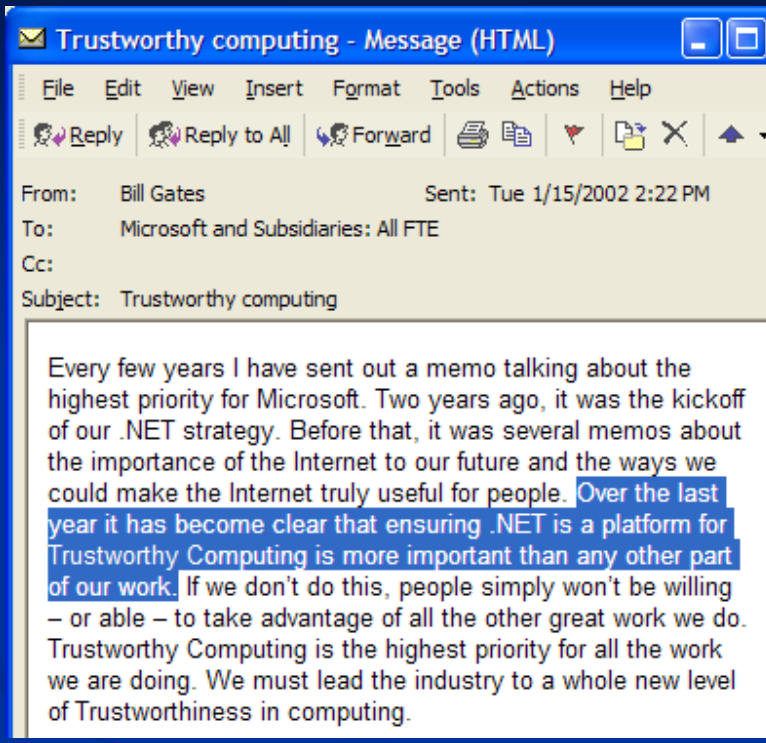
# パートナープログラムの内容

| | | |
|---|---|---|
| 啓蒙活動 | 定期的な<br>連絡会の開催 | 業界内のセキュリティ情報の共有<br>プログラムの継続した改善活動 |
| | 継続的<br>セキュリティ<br>啓蒙活動 | イベントやセミナーなどを通じて、セキュリティ<br>対策の徹底と運用を継続的に啓蒙 |
| | セキュリティ<br>関連サービス<br>の充実 | セキュリティ関連の保守サービスや運用管理<br>コンサルティングメニューの充実 |
| 緊急時への備え | 業界連絡網<br>の構築 | 通常時の情報共有と初動に向けた体制準備<br>緊急時の業界をあげた協調作業 |
| | 緊急告知体制<br>の構築 | 一般ユーザー、企業ユーザーへの<br>警告・対策情報の早期提供のしくみ作り |

# 設計段階のセキュリティ対策

現在

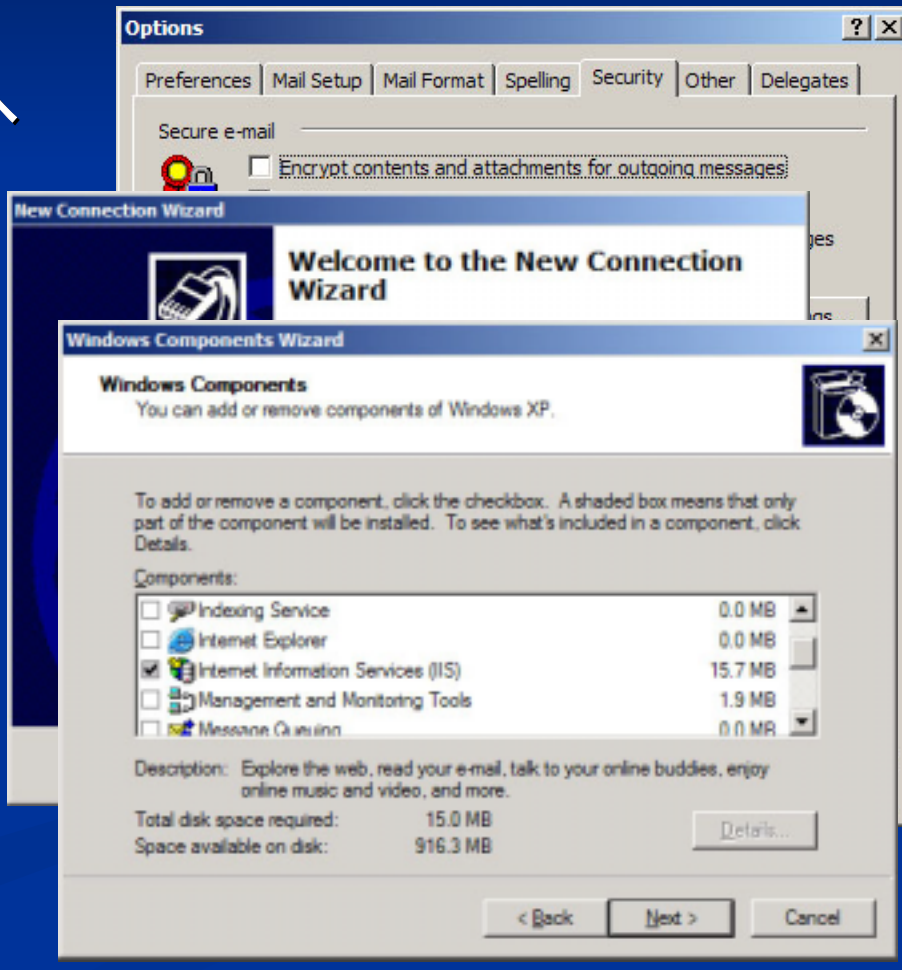
- Windows, VS.NETのセキュリティコードレビュー
  - 出荷前工程の改善：
    コーディング手段、出荷時設定の見直し
  - 出荷後作業の改善：
    CD制作会社による規定遵守の強化
- 9000人以上のWindows,ISA, .NET開発者教育
- 第三者機関によるWindows, ISA, .NETフレームワークの検証



# 初期設定におけるセキュリティ対策

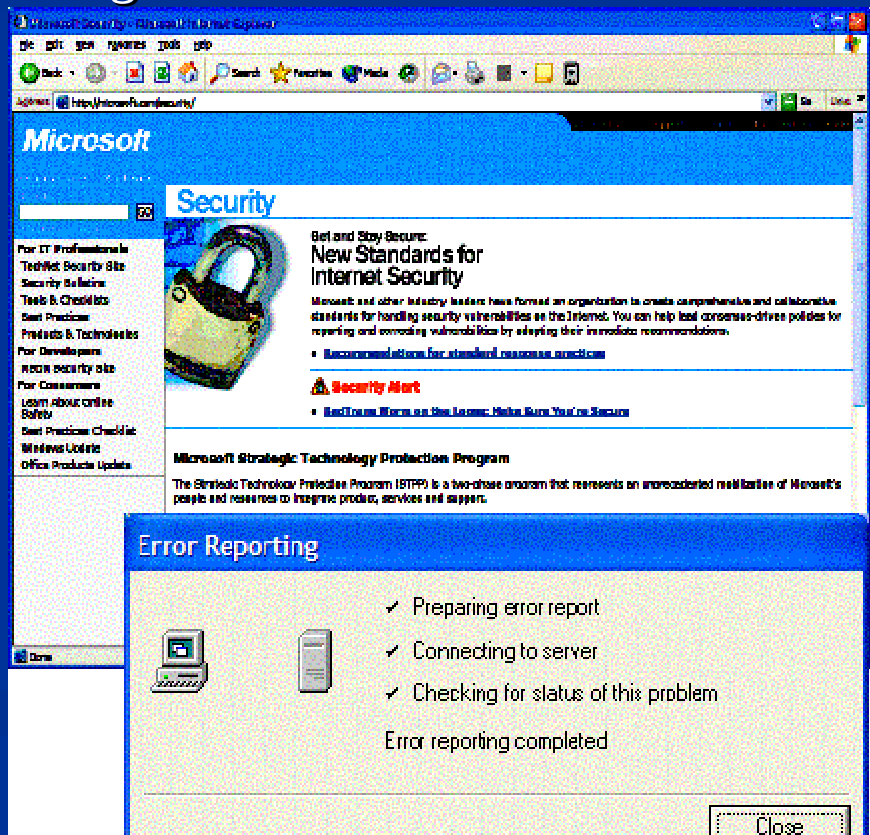
Microsoft Office xp　Microsoft Windows xp　Microsoft Windows.net Server Family

- Office：.exeの受取、scriptへのアクセス無効
- XP：インターネット接続にファイアウォールを設定
- Windows .NET Server：
  **初期設定でIIS6を無効化**
  - **ウィザードによる不要なサービスの無効化**



# 導入段階でのセキュリティ対策

- “Get Secure. Stay Secure.”（セキュリティの確保と維持）を実現する
  STPP（ストラテジック テクノロジー プロテクション プログラム）、
  MSRC（マイクロソフト セキュリティ レスポンス センター）
- Windows 2000 Security Rollup Packageの提供
- 企業向けセキュリティ
  アセスメントや各種ツール
- セキュリティを重視した
  Windows 2000 SP3
- VS.NET の自動更新
- 企業向けWindows Update



# マイクロソフトの個人情報保護に関する昨今の取組み

## 業界との取組み

- オンライン プライバシー アライアンスに加盟
- TRUSTe、BBBOnline

## 第三者機関による監査

- Deloitte、Price Waterhouse、Foundstone

## ビジネス手法

- 1997年に、GLBに準拠した公平な情報交換のための実施手順を採用
- MSNは業界で初めて、保管されている個人データをユーザー自身に公表
- ヨーロッパ セーフ ハーバー条約に調印
- XPのライセンス認証における匿名性：個人情報は不必要
- 社内における個人情報保護の推進

## 製品設計

- Kids Passport：親が子供のデータ共有を管理（pre-COPPA）
- .NET My Services：ユーザーが自身のデータを管理

# 企業＆利用者全体での取り組みが必要

- セキュリティ問題についてIT業界団体が主導
  - セキュリティの脅威について報告
  - ベストプラクティスを共有
  - 問題発生時に迅速なソリューションを提供
- 技術の相互運用性を推進
- 個人情報保護やセキュリティの適格基準、法整備の明確化
- ITインフラの提供者はセキュリティ対策を念頭に
- 利用者にもセキュリティの意識改革を

# Get Secure. Stay Secure.

セキュリティを“確保”し、そして“維持”する