

第二回 調査技術ゼミ

2005年9月5日

**『暗号化と回復』
WindowsのEFSを使って**

ネットエージェント株式会社

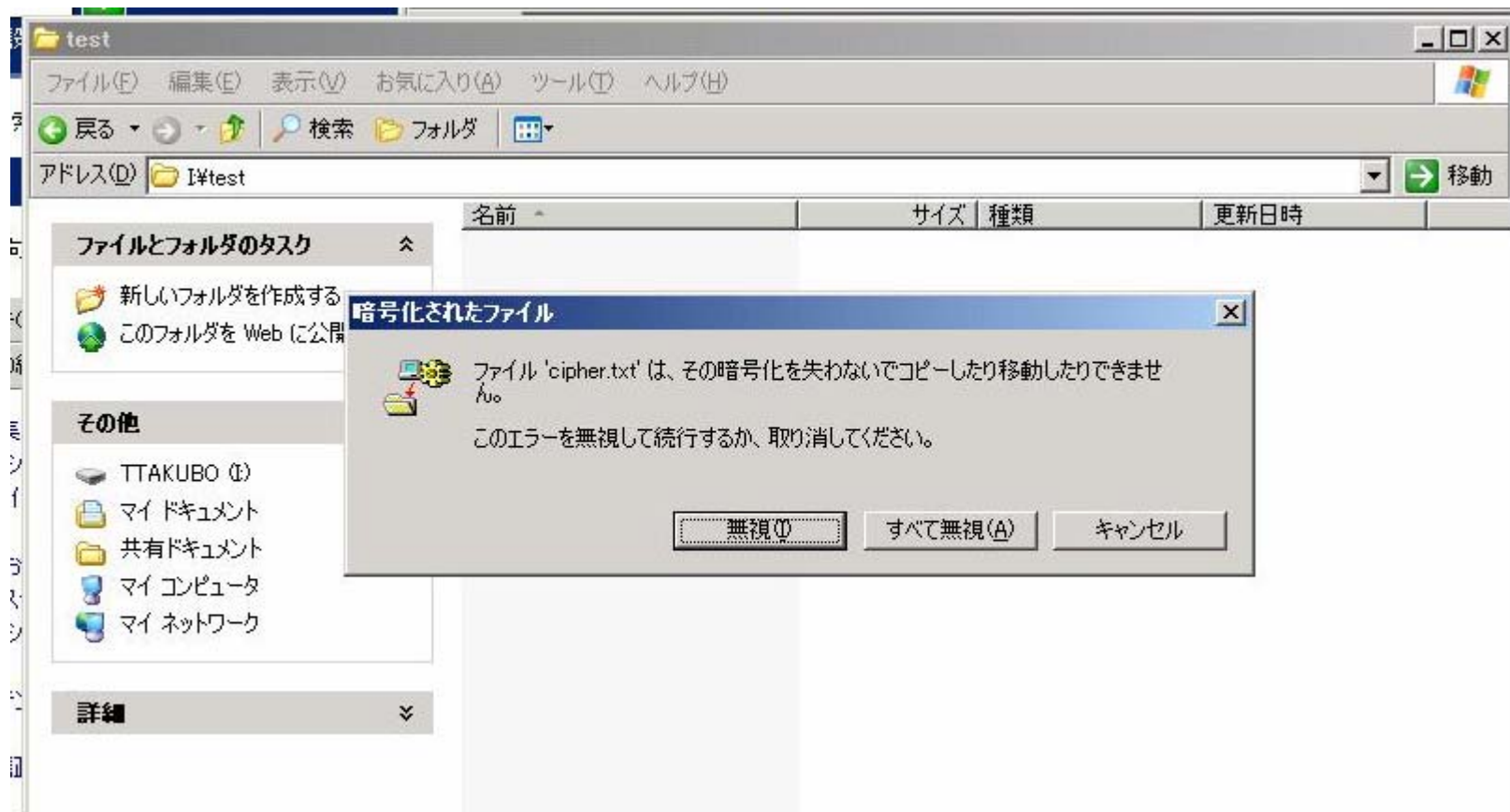
EFSの概要

- 暗号化方式
 - AES (XP SP1、2003Server以降)
 - DESX、3DESの使用も可 (レジストリ、GPOにて指定)
- ファイルの中身の暗号化
 - 権限があれば削除や移動は可能
 - ACEとの併用が必要
 - OPENに失敗してもアクセスタイムは更新
- ネットワークの移動は暗号化されない
 - WebDAVやIPSec、PPTPの併用が必要

EFSの使用

- ユーザーレベルで使用可能
 - 管理者の設定不要(ドメイン環境含む)
 - 証明書はEFSが自動作成(CAを構成して管理の簡略化も可能)
 - 証明書はEKU(Enhanced Key Usage)に[ファイル回復]フィールドが必要。[ファイル回復]はMicrosoftPKIの一部として定義
- 暗号化の解除
 - 明示的な解除(プロパティのチェックを外す)
 - NTFSボリューム以外への移動(ダイアログあり)
 - desktop.iniで除外の指定も可能
- EFSの無効化
 - ドメイン:グループポリシー
 - Windows2000 回復エージェントを削除
 - Windows2003 EFSのプロパティで無効化をチェック
 - ローカル:レジストリ

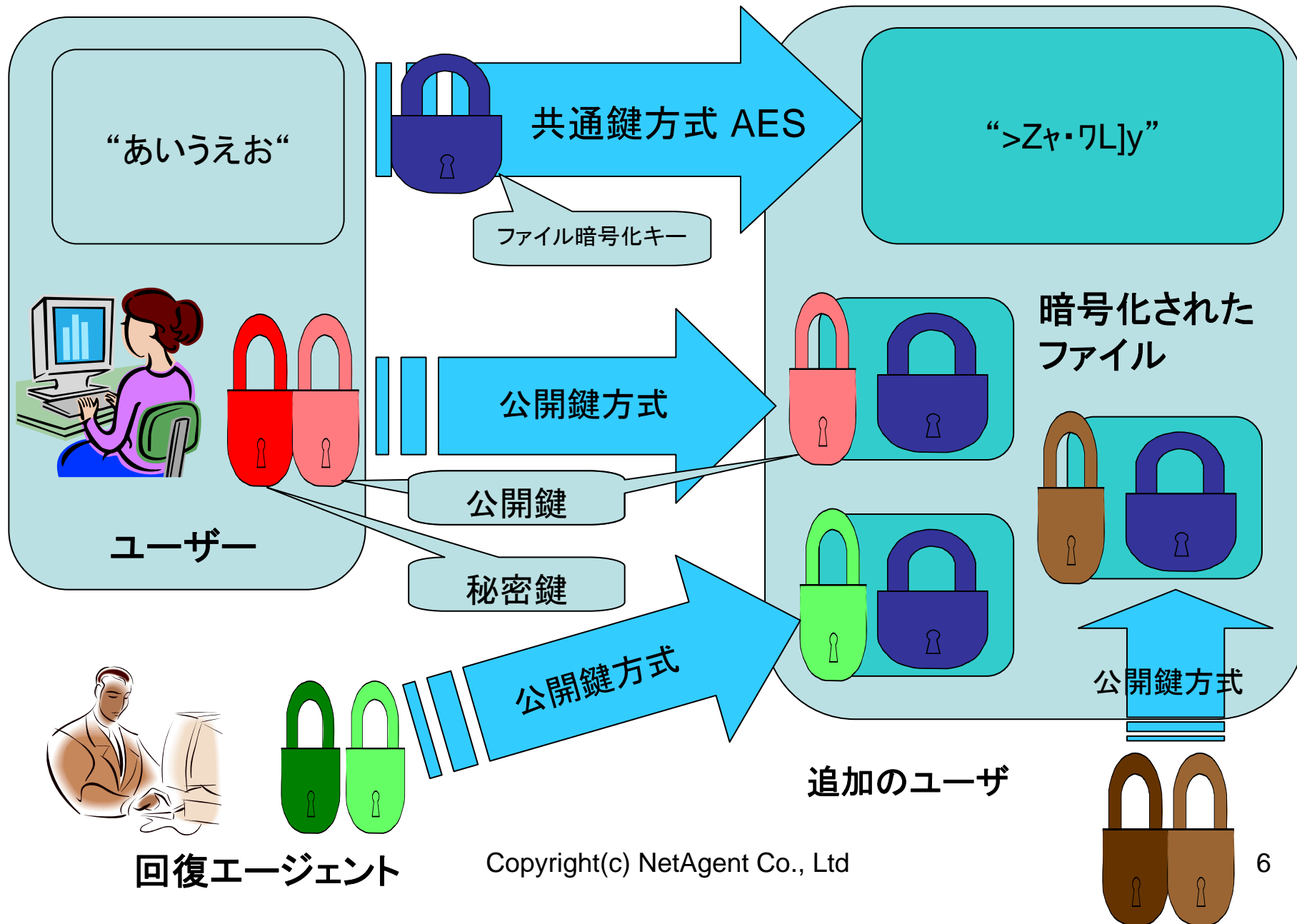
例：FATボリュームへの移動



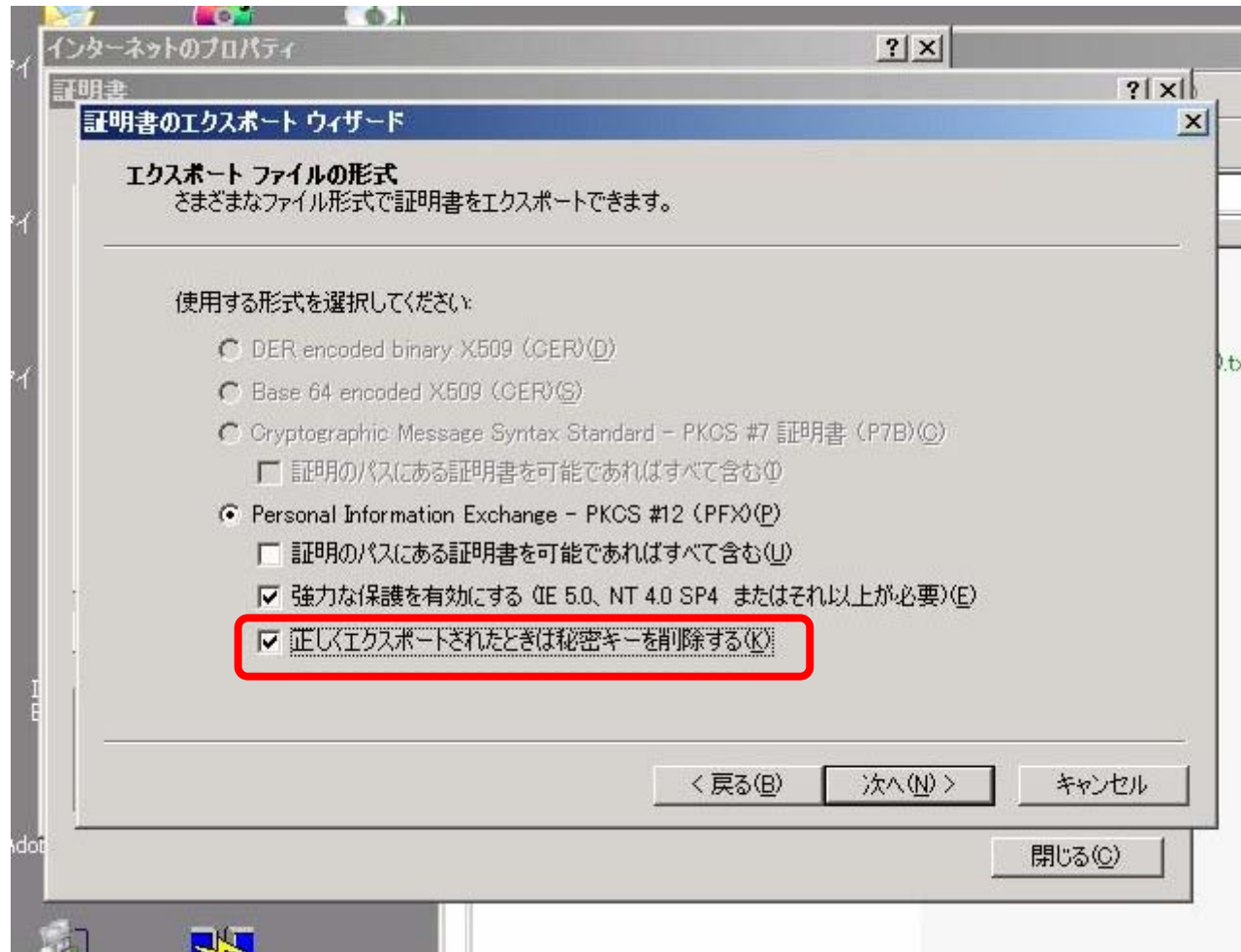
EFSによるファイルの暗号化手順

1. 「ファイル暗号化キー」によるファイルの暗号化
2. EFS証明書の公開鍵による「ファイル暗号化キー」の暗号化
3. 追加のEFSユーザーやEFS回復エージェントの公開鍵による「ファイル暗号化キー」の暗号化
4. 公開キーに対応する秘密キーは「保護されたキー格納領域」に格納される
 - 証明書と秘密キーをエクスポートする際、システムから削除することも可能

EFS暗号化の流れ



例：証明書のエクスポート



EFSの暗号化解除の手順

1. 「ファイル暗号化キー」の暗号化解除
 - ユーザー、追加のEFSユーザー、EFS回復エージェントの**いずれか**の秘密鍵による
 - EFS回復エージェントは回復ポリシーのスコープ内を**すべて**回復可能
2. 「ファイル暗号化キー」によるファイルの暗号化解除

EFS回復エージェント

「暗号化されているユーザーデータを回復するために、公開キー証明書が与えられている人」

– 「データの回復」とは、ファイルを暗号化したユーザーの秘密キーを使わずに、そのファイルの暗号化を解除する処理のこと

- ユーザーが会社を退職した場合
- ユーザーが秘密キーをなくした場合
- 捜査機関からの要請があった場合

Windows2003Severヘルプファイルより

回復ポリシー

1つまたは複数のユーザーアカウントを回復エージェントに指定できる、公開キーポリシーの一種

- スタンドアロンではローカルに構成される
 - Win2000: Administratorが既定の回復エージェントに
 - XP以降: 既定の回復エージェントはないので、cipher.exe /rを実行し証明書を作成後、回復ポリシーに追加する
- ネットワークでは、ドメイン、OU、個別のコンピュータのいずれかに構成される
 - 最初のドメインコントローラ設定時に既定のポリシーとして、ドメイン管理者に自己署名付き証明書が発行される

回復エージェントの追加

- 回復エージェントは個々の暗号化されたファイルに保存される
 - ⇒暗号化された後に追加された回復エージェントは反映されない
 - cipher.exe /uの実行 or Reopenしてから再度保存
- 「efsinfo.exe /r ファイル名」で確認可能
 - [NT]Efsinfo.exe を使用して暗号化されたファイルの情報を調べる方法 <http://support.microsoft.com/kb/243026/>
 - バージョンによる差異に注意(常に最新版を使用する)

回復エージェントでの回復手順

1. 回復対象ファイルのバックアップ
2. バックアップを安全なシステムへの移動
3. 証明書と秘密キーをインポート
4. バックアップファイルを回復
5. ファイルの暗号化を解除

Windows2003Severヘルプファイルより

Advanced EFS Data Recovery

- ElcomSoft Co.Ltd.製
- システムが起動しないときやログオンできないときに使用可能
- 動作条件
 - システム内に暗号化キーが残っていること
 - 暗号化したユーザーのパスワード
 - 対象ディスクへの管理者権限

予期せぬ回復

- アプリケーションが作成する一時ファイル
⇒フォルダを暗号化して、新規にファイルを作成することを推奨
- 平文ファイルの暗号化フォルダへの移動
⇒MTF (Master File Table)領域の消毒が必要な場合もある
- ページファイル内の情報
⇒仮想メモリのページ ファイルをクリアする」ポリシー
<http://go.microsoft.com/fwlink/?LinkId=51312>
- システムの復元
⇒復元を無効⇒ファイルを暗号化⇒復元を有効

参考

- 情報漏えい対策ガイド (Windows 編)
 - <http://www.microsoft.com/japan/windowsserver2003/activedirectory/kinko/default.msp>
 - Microsoft文書
- The Windows Server 2003 Family Encrypting File System
 - <http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/WinNETSrvr-EncryptedFileSystem.asp>
 - Microsoft文書
- Windowsにおける物理アクセス対策 – EFSとSYSKEY
 - <http://www.st.rim.or.jp/~shio/csm/efs/>
 - 塩月 誠人 氏 (ネットワークセキュリティコンサルタント、中央大学 研究開発機構 研究員)

**解き明かす力、今すぐにでも。
フォレンジック・サービス**

NetAgent

The Forensics Company

<http://forensic.netagent.co.jp/>