4D-6

モバイル端末向けオフラインアプリケーション統制システムの提案

森田　伸義　　礒川　弘実　　萱島　信　　梅澤　克之†

(株)日立製作所　横浜研究所†

1. はじめに

これまでに，報告者らはシンクライアントシステム(TCS)[1]向けオフラインアプリケーション統制システム(OAC：Offline Application Control system)を開発してきた[2]．本システムは，情報漏洩リスクを十分に低減した上でデータを持ち出すとともに，ネットワーク利用不可環境(以下オフライン環境)でも業務遂行を可能とする．

一方，近年，スマートフォンのようなモバイル端末が急激に普及してきている．このようなモバイル端末を用いて情報を組織外へ持出す場合，ネットワーク利用可能環境では TCS と同様に遠隔操作により安全に情報を利用できるが，オフライン環境への対応が十分とは言えない．

そこで本研究では，TCS 向けに開発した OAC をモバイル端末向けに拡張する．

2. モバイル端末向け OAC の要件

組織によって管理されていない端末(以下個人端末)の悪用による情報漏洩，およびモバイル端末の盗難/紛失による第三者への情報漏洩が問題になっている．このような問題に対して，TCS による解決が提案されているが，TCS はオフライン環境で利用できない．そこで，暗号化技術を利用することが効果的であると考えるが，暗号鍵が漏洩してしまうと暗号化された情報の漏洩リスクも高くなる．

上記課題を踏まえて，本研究では，OAC をモバイル端末向けに拡張するために，下記要件(1)から(3)を同時に満たすモバイル端末向け OAC を提案する．

(1) 端末の制限
　個人端末への漏洩を防止するために，端末ごとに持出情報の利用を制限できること．

(2) ユーザの制限
　第三者への漏洩を防止するために，情報ごとに利用可能なユーザを制限できること．

(3) 暗号鍵の盗難リスク低減
　暗号鍵の盗難を防止するために，第三者による暗号鍵の盗難リスクを低減できること．

3. モバイル端末向け OAC の提案

本提案システムの構成と基本的な動作フローを図 1 に示す．モバイル端末向け OAC は，使用者/承認者の PC，管理サーバ，使用者モバイル端末および IC チップを搭載した記録媒体から成る．使用者モバイル端末には，OAC クライアント(以下 Client)を搭載する．Client は，オフラインで利用するデータを管理サーバからダウンロードし，暗号化/復号を実行する．

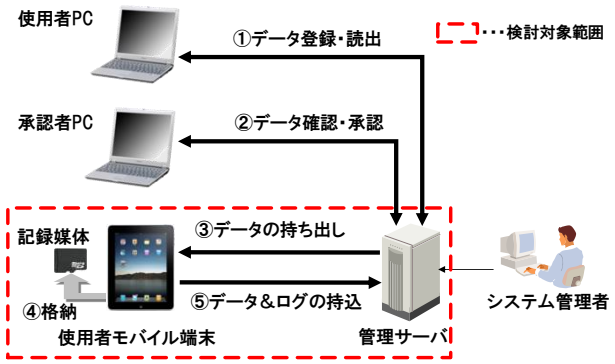

図 1 モバイル端末向け OAC のシステム構成

前節に示した要件(1)から(3)について，「端末の制限」を実現するためには，組織に登録されている端末のみが情報を利用できる必要がある．「ユーザの制限」を実現するためには，組織に登録されているユーザのみが情報を利用できる必要がある．「暗号鍵の盗難リスク低減」を実現するためには，第三者によって暗号鍵が容易に盗まれない必要がある．

以上より，前節に示した要件(1)から(3)を同時に満たすためには，下記(a)から(c)を同時に実現する必要がある．

(a)登録済みの端末でしか暗号化済み情報を復号できないこと．
(b)第三者が暗号化済み情報を復号できないこと．
(c)より安全な領域で暗号鍵を保管できること．

これらを同時に実現するにあたり，「ユーザパスワード」，「使用者モバイル端末の端末 ID」，「記録媒体の IC チップ領域に格納された

The proposal of Offline Application Control system for mobile terminals.

†Nobuyoshi MORITA, Hiromi ISOKAWA, Makoto KAYASHIMA, Katsuyuki UMEZAWA.
†Yokohama Research Laboratory, Hitachi, Ltd.

秘密鍵，およびそれに対応した公開鍵」を利用する．そして，これらを用いた多重の暗号化/復号により，上記(a)から(c)を同時に実現する．

以下，図 2 に暗号化/復号の処理概要(図 1 の破線部分の詳細)を示す．また，表 1 に図 2 の詳細を示す．

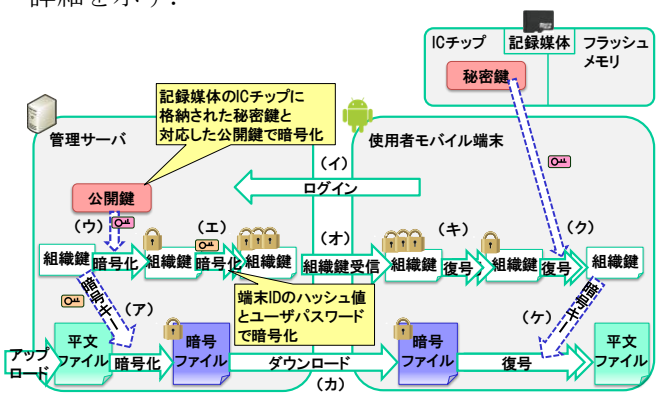

図 2 複数要素を用いた暗号化/復号の処理概要

表 1 複数要素を用いた暗号化/復号の処理詳細

#		実現方式
持ち出し時	ア	管理サーバはアップロードされた承認済みの平文ファイルを組織鍵で暗号化する．組織鍵とは，承認済みデータを暗号化/復号するための共通鍵のことである．
	イ	Client を立ち上げたときに，使用者モバイル端末はユーザ ID/パスワードを用いて管理サーバにログインする．また，使用者モバイル端末は，Client が起動している間，上記ユーザパスワードをアプリ領域に格納する．
	ウ	管理サーバは受信したユーザ ID を基に記録媒体(IC チップ)に格納されている秘密鍵に対応した公開鍵を用いて組織鍵を暗号化する．
	エ	管理サーバは受信したユーザ ID を基に，対応したモバイル端末 ID のハッシュ値を利用して上記(ウ)で暗号化された組織鍵を暗号化するとともに，受信したパスワードを利用して組織鍵をさらに暗号化する．
	オ	使用者モバイル端末は上記(エ)で暗号化された組織鍵を管理サーバから受信し，アプリ領域に格納する
	カ	使用者モバイル端末は上記(ア)で暗号化された暗号ファイルを管理サーバからダウンロードし，アプリ領域に格納する
利用時	キ	暗号化ファイルの復号時に，使用者モバイル端末はログイン時に格納したユーザパスワードを利用して組織鍵を復号する．また，使用者モバイル端末の端末 ID を取得するとともに，取得した端末 ID を基に組織鍵をさらに復号する．
	ク	使用者モバイル端末は上記(キ)で復号された組織鍵を記録媒体(IC チップ)に格納されている秘密鍵を利用して復号する
	ケ	使用者モバイル端末は上記(ク)で復号された組織鍵を利用して暗号ファイルを復号する

4. 評価

本研究で提案したモバイル端末向け OAC を評価する．本研究の適用先の一つとして考えている渉外業務におけるセキュリティリスクを，IT セキュリティのための基本テクニカルモデル[3]を参考に整理した．その中で，特に重要となるセキュリティリスクに対する効果を表 2 に示す．

表 2 より，提案するモバイル端末向け OAC が，情報持ち出し時に想定されるセキュリティリスクに対して有効であると言える．

表 2 セキュリティリスクに対する効果

項目	セキュリティリスク	モバイル OAC による効果
情報の不正取得	ユーザの成りすまし	暗号化に利用する複数要素の内，どれか一つでも守られていれば，情報を復号できない．
	不正アクセス	
情報の漏洩	モバイル端末の盗難/紛失	
	第三者による鍵情報の盗聴	管理サーバで暗号化された鍵情報をモバイル端末に配送しているため，盗聴しても情報を復号できない．
	ユーザによる誤操作	コピー&ペースト禁止，記録媒体使用禁止等のポリシーを強制することにより，誤操作による漏洩を防止できる．
	ユーザの故意による情報漏洩	ファイルを開くときに，ファイルハンドルを排他制御することにより，Client が起動中の間は，他のプログラムによる操作を防止できる．また，モバイルデバイスマネージャ(MDM)と連携することにより，モバイル端末が Jailbreak されているかどうかをチェックすることにより，ハックされた場合は直ちに情報を削除できる．
	ユーザによる誤った情報の持ち出し	承認者による持出情報の確認を実施することにより，持ち出せる情報の審査を厳格化できる．また，持ち出した情報に時限情報を付随しておき，モバイル端末が定められた期限になると自動的に情報を消去できる．

5. まとめ

本報告では，TCS 向けに開発した OAC をモバイル端末向けに拡張する提案を行った．また，提案方式を用いたモバイル端末向け OAC が，情報持ち出し時に想定されるセキュリティリスクに対して有効であることを示した．

今後の課題としては，モバイル端末と物理的に離れた状態で暗号鍵を所持できる IC カードを利用する方式も検討することが望ましい．

参考文献

[1] 中西，牧野，小高，杉山，石原:「セキュアクライアントソリューション」を支える「セキュリティ PC」と周辺装置，日立評論 Vol.88 No.05， p.p. 26-29，2006/5

[2] 礒川，アプリケーションとデータの管理方法，管理システム，それに用いられるシンクライアント端末，管理サーバ，およびリモート計算機，特開 2008-276723

[3] IT セキュリティのための基本テクニカルモデル:NIST，SP800-33 (2001)