4D-5

シンクライアント向けオフラインアプリケーション統制システムの開発

礒川 弘実† 森田 伸義† 梅澤 克之† 萱島 信†

(株)日立製作所 横浜研究所†

1. はじめに

企業などの組織内でデータとデータ処理アプリケーション(以下アプリ)を集中管理し，ネットワーク経由の画面操作で遠隔からデータとアプリを活用可能とするシンクライアントシステム(TCS)がある[1]。TCS を使用することで，(1)場所と時間を選ばずいつも同じ環境で業務遂行できる，(2)出先や移動中などのモバイル環境で業務する際にもデータを組織内から持ち出す必要が無く機密データの紛失・盗難のリスクが低減される，というメリットがある。

しかし，TCS には，ネットワークが利用不可または低品質な状態(以下オフライン状態)ではデータとアプリを快適に操作できず，業務遂行困難な場合があるという問題がある。

そこで，本稿では，情報漏洩リスクを十分に制御可能とした上でデータを持ち出してオフライン状態でも利用可能とする，TCS をベースとしたオフラインアプリケーション統制システム(OAC：Offline Application Control system)を提案する。

2. OAC の提案

組織内から持ち出したデータ(以下持出データ)の漏洩リスクを低減する施策は，下記の２つに大別される。

(1) 持出データ最小化と組織外存在時間最短化

持出データを必要最小限に抑える。また，持ち出し後も不要になった時点ですぐ消去するなど組織外に存在する時間を短くする。

(2) 持出データ処理フロー中の漏洩防止

組織内からの持ち出しから組織外での活用，組織内への持ち込みまで，持出データの処理に関わる一連の処理で漏洩を防止する対策を施す。

そこで，上記施策をシステムで実現する OAC を提案する。OAC が提供する機能を表 1に示す。

Development of Offline Application Control System for Thin-client.
†Hiromi ISOKAWA, Nobuyoshi MORITA, Katsuyuki UMEZAWA, Makoto KAYASHIMA
†Yokohama Research Laboratory, Hitachi, Ltd.

表 1 OAC の機能

目的	機能	機能内容
データの持出抑制	承認機能	承認者に許可されたデータのみ持ち出し可能とする。また，許可された操作(閲覧，編集，複製，印刷等)のみオフライン状態で実施可能とする。
	時限機能	承認期限切れデータを自動消去する。
持出データの管理	計算機制限機能	持出データの使用可能計算機を制限する。
	暗号化機能	使用時以外は持出データを暗号化する。
	複製抑止機能	持出データ使用時(データ復号状態)に他への複製を防止する。
	ログ機能	持出ログ，使用時の操作ログを取得する。

3. OAC の開発

上記機能を持った OAC のプロトタイプシステム(以下プロト)を開発した。プロトは TCS をベースとしている。プロトのシステム構成と基本的な動作フローを，図 1に示す。

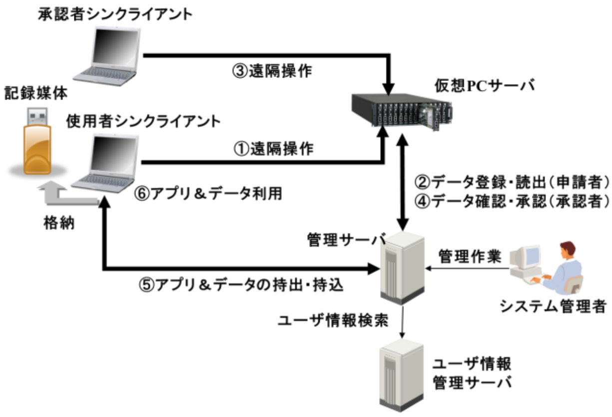

図 1 OAC のシステム構成

データ持出の管理を行う OAC サーバソフトウェア(以下 Server)の入った管理サーバを設置す

る。Server は，オフラインで使用するデータを管理し，使用者からのデータの持出・持込依頼と承認者からの承認依頼を受け付ける。

使用者シンクライアントには，データ処理に使用するアプリと OAC クライアントソフトウェア(以下 Client)を搭載する。Client は，オフラインで使用するデータを Server からダウンロードし，記憶媒体に暗号化して格納する。また，オフライン状態で記憶媒体のデータを復号し，データに指定されたアプリを実行する。

プロトにおける機能の実現方式を表 2に示す。

表 2 プロトの機能実現方式

機能	実現方式
承認機能	Server に登録されたデータは，承認者の許可が得られないと記憶媒体にダウンロードできないようにする。データにはオフライン状態で実行できる操作(閲覧，編集，複製，印刷)を設定可能とし，Client では許可された操作のみ実施可能とする。
時限機能	データには利用開始時刻と終了時刻を設定可能とする。Client で時刻を確認し，利用開始時刻前のデータは使用不可に，利用終了時刻後のデータは消去する。
計算機制限機能	持出データの記録媒体としてパスワードロック可能なデバイス[2]を使用し，パスワードを Client に登録する。利用者シンクライアントのみ Client を搭載することで，持出データを使用可能な計算機を制限する。
暗号化機能	Client は，持出データを記録媒体に暗号化して保存する。使用時にはシンクライアントの揮発メモリ上にデータを復号する。(シンクライアントの電源 OFF で復号データは全て消去される。)
複製抑止機能	Client は，持出データを復号する際に，持出データを処理するアプリ以外のアプリの起動，ネットワーク送信，記憶媒体書込み，コピー&ペースト，画面キャプチャ，印刷を禁止する。
ログ機能	Server への持出・持込に関するログは全て保存する。また，Client は，シンクライアント上での操作を記録し，オンライン状態になった際に，Server に操作ログを送信する。Server はログを管理し，システム管理者及び利用者に提供する。

4. OAC の試用

開発したプロトを約 380 人の組織で試用した。システムは２年間問題なく稼動した。アプリは，テキスト編集アプリと，プレゼンテーション(以下プレゼン)アプリ２つ(A)(B)の計３つを使用可能とした。初年度の利用実績を，表 3に示す。

表 3 OAC の利用実績(初年度)

ユーザ数	データ登録ユーザ	39 人(10.8%)
持出データ数	テキストデータ	27(ユーザ数:11)
	プレゼン(A)データ	223(ユーザ数:31)
	プレゼン(B)データ	30(ユーザ数:12)
データ利用数	テキストデータ	168(ユーザ数:16)
	プレゼン(A)データ	296(ユーザ数:18)
	プレゼン(B)データ	181(ユーザ数:8)
	データ新規作成	83(ユーザ数:17)
承認処理数	許可	339
	却下	0

プレゼン(A)データのデータ利用ユーザ数(18 人)が持出ユーザ数(31 人)の約半分であることから，TCS が使用不可の場合に備えてのバックアップとしても多く使用されたことが分かった。

5. まとめ

オフライン状態では業務遂行が困難となるシンクライアントシステムの問題を解決するため，情報漏洩リスクを十分に制御可能にした上でデータを社外に持ち出し，オフライン状態で使用可能とするオフラインアプリケーション統制システムを提案した。また，本システムのプロトタイプを開発し，組織内で試用することで，本システムの実現可能性と有効性を確認した。

今後の課題としては，現システムでは必須となっている事前のシンクライアントへのアプリのインストールを不要にすること等がある。

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] T. Kato, T. Tsunehiro, M. Tsunoda and J. Miyake: A Secure Flash Card Solution for Remote Access for Mobile Workforce: IEEE Trans. on Consumer Electronics, Vol. 49, Issue 3, pp. 561 -566, Aug. 2003.