フュージョンシス電子文書管理システムの仕様概略

株式会社フュージョンシス

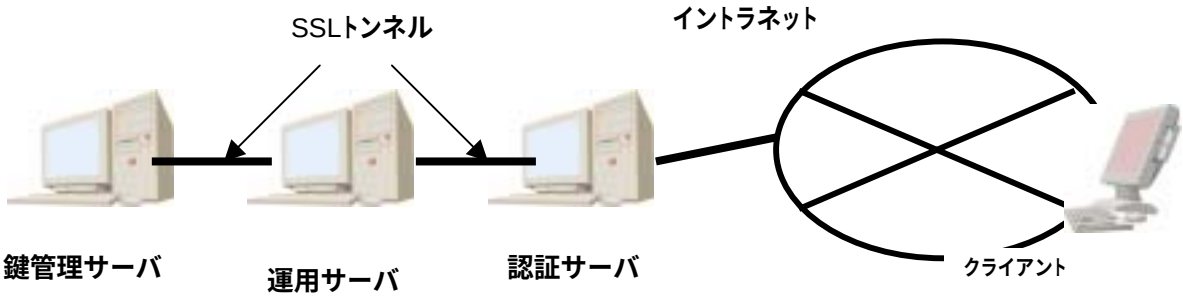
文書バージョン	日付	変更点
ver0.1	2003 年 11 月 25 日	作成
ver0.5	2003 年 12 月 9 日	修正
ver0.6	2003 年 12 月 28 日	修正
ver0.6	2004 年 2 月 14 日	修正

目次

概要

電子文書を暗号化し、権限の存在する人やグループに対してのみ、暗号の鍵を使うことを許可し、文書を閲覧させるシステムです。文書自体が元から暗号化されているので、従来の方法に比べて遙かに機密性が高く、ハッカーや第三者の攻撃に対して安全です。

全体のイメージ

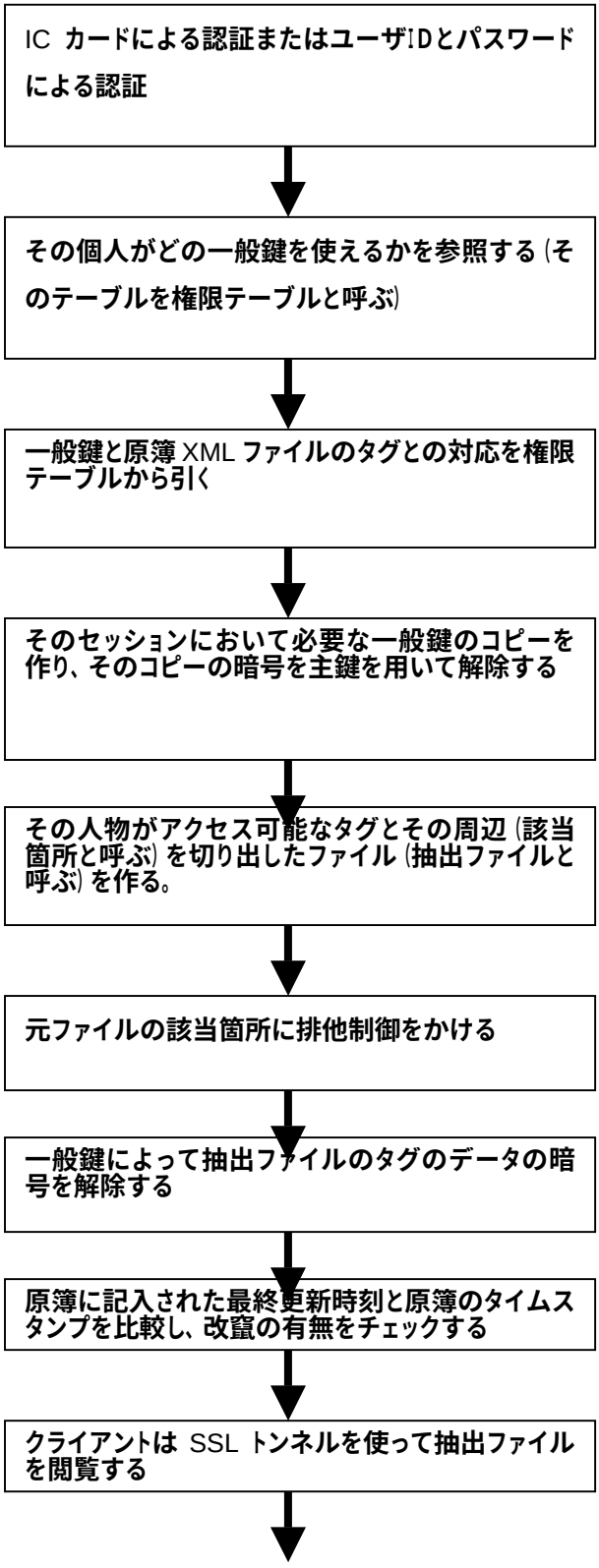


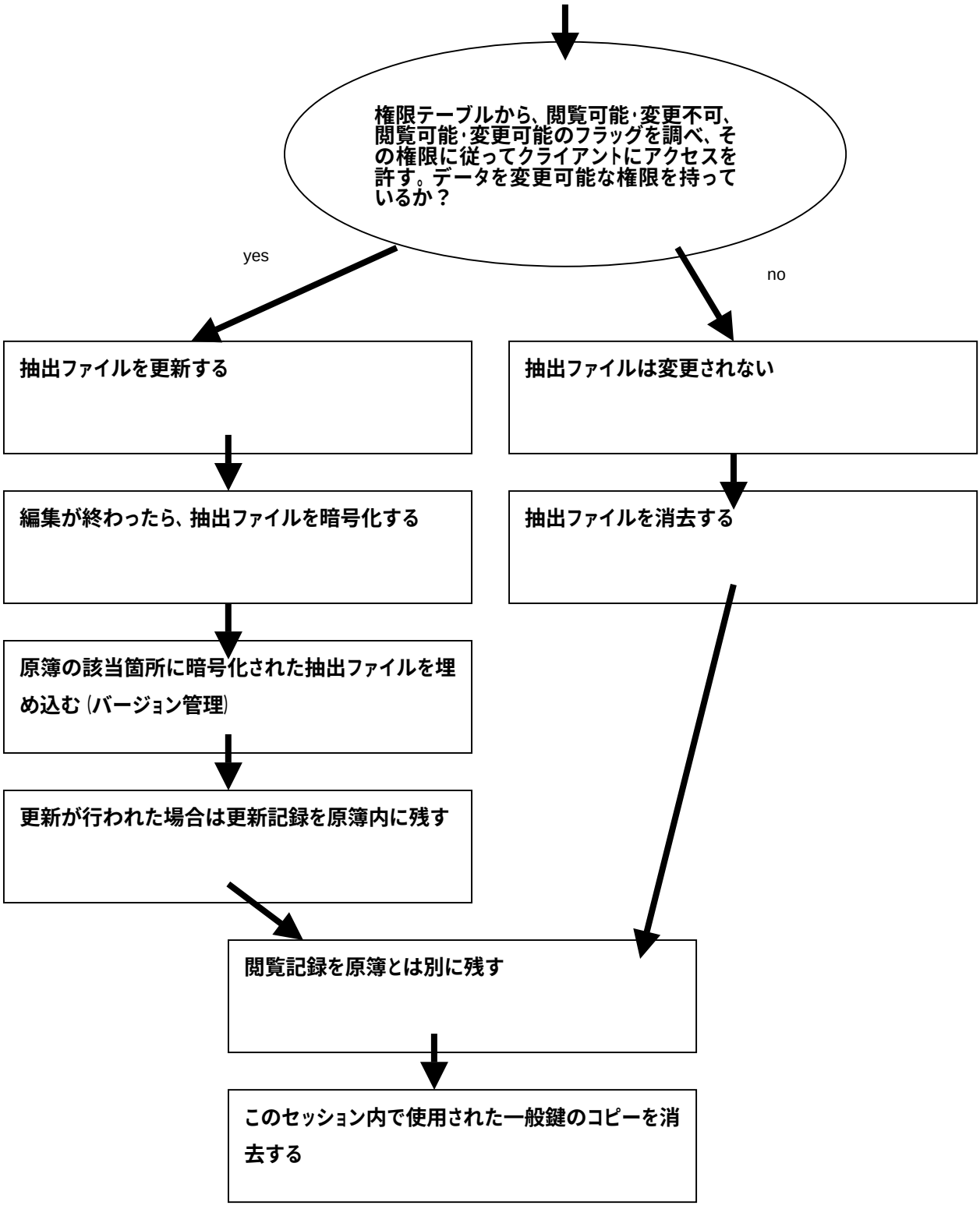
鍵管理サーバは、クライアント PC 群から直接にアクセスされることはありません。

用語

言葉	意味	備考
原簿	個人情報など非常に重要性の高い情報を含む XML ファイル	
権限テーブル	あるユーザがどの一般鍵を使えるかを決めたテーブル	管理者だけがレコードの変更権限を持つ。
一般鍵	原簿のデータを暗号化するための鍵	普通ディスク上にあり、使用されるときメモリ上に置かれる。変更はされない。原簿の XML の1個のタグに対して1個の一般鍵が割り当てられる。従って個数はタグの個数だけ存在する。
主鍵	一般鍵を暗号化そして暗号解除するための鍵	常にメモリ上にある。定期的に変更される。主鍵は鍵管理サーバに対して1個だけ存在する。
該当箇所	あるユーザが参照または変更することが許される原簿の中の箇所	

処理の流れ


IC カードによる認証またはユーザIDとパスワードによる認証
その個人がどの一般鍵を使えるかを参照する（そのテーブルを権限テーブルと呼ぶ）
一般鍵と原簿 XML ファイルのタグとの対応を権限テーブルから引く
そのセッションにおいて必要な一般鍵のコピーを作り、そのコピーの暗号を主鍵を用いて解除する
その人物がアクセス可能なタグとその周辺（該当箇所と呼ぶ）を切り出したファイル（抽出ファイルと呼ぶ）を作る。
元ファイルの該当箇所に排他制御をかける
一般鍵によって抽出ファイルのタグのデータの暗号を解除する
原簿に記入された最終更新時刻と原簿のタイムスタンプを比較し、改竄の有無をチェックする
クライアントは SSL トンネルを使って抽出ファイルを閲覧する


権限テーブルから、閲覧可能･変更不可、閲覧可能･変更可能のフラッグを調べ、その権限に従ってクライアントにアクセスを許す。データを変更可能な権限を持っているか？
yes
no
抽出ファイルを更新する
抽出ファイルは変更されない
編集が終わったら、抽出ファイルを暗号化する
抽出ファイルを消去する
原簿の該当箇所に暗号化された抽出ファイルを埋め込む（バージョン管理）
更新が行われた場合は更新記録を原簿内に残す
閲覧記録を原簿とは別に残す
このセッション内で使用された一般鍵のコピーを消去する

システム構成

- OS　LINUX　AIX HP-UX SOLARIS IRIX などからご自由に選べます。
- 開発言語　JAVA
- データベース　DB2　ORACLE　INFOMIX　SYBASE　POSTGRESQL　MYSQL などからご自由に選べます。
- アプリケーションサーバ　TOMCAT などからご自由に選べます。

使われる暗号

鍵サーバが使う暗号は特定のものに限定されない。従って AES, DES, Rijndael などを使うことができる。もちろん階層的暗号化法も使うことができる。

権限テーブルの実装

- 権限テーブルは POSTGRESQL 内に実装する。
- 各レコードは暗号化しない。
- 1個のタグに1個の鍵を対応させる (従って鍵とタグは同一視できる)。

権限テーブルのイメージ

名前	所属	ユーザ ID	パスワード	IC カード内の ID	暗号を解除することの許されるタグ	用いることが許される鍵の ID
小山	保険課	FG00001	*****	plfg06789	<名前><生年月日><学歴>	k678920，k6834，k89803
中村	納税課	HJ9086	******	hjhu*999	<収入><住所>	k44446，khhhhh0，k34346

元文書の履歴の管理

履歴は原簿の中に書かれる。原簿の更新が終わり、主鍵で原簿が暗号化される直前の時刻を書き込み、さらにその時刻を表す文字列を暗号化する。この文字列は改竄の有無のチェックに使われる。

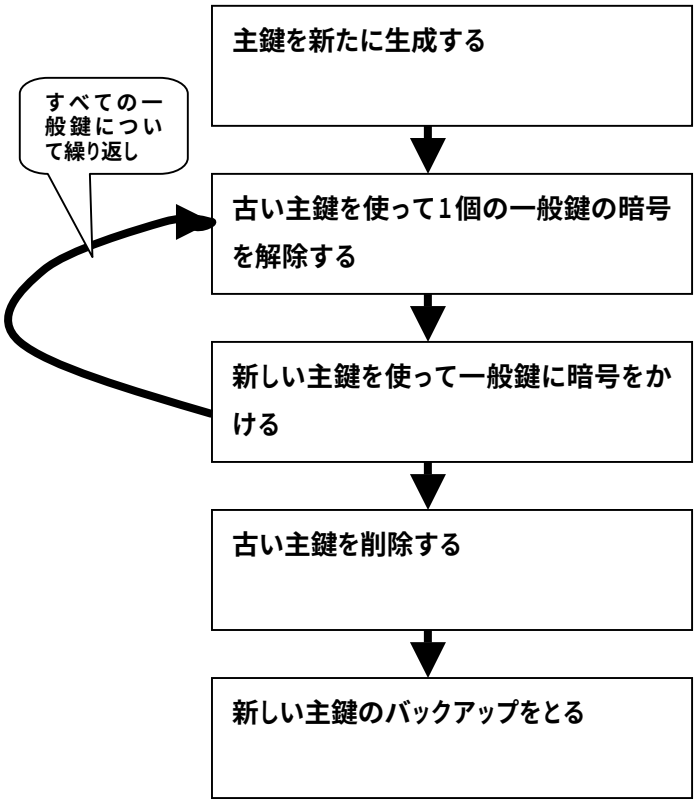
履歴のフォーマット

userID	閲覧 or 更新	更新（閲覧）開始日時	更新（閲覧）終了日時	更新したタグ

主鍵の管理および定期的な変更

主鍵はメモリ上に置く。バックアップはサーバ内には残さず、フロッピーディスクなどに保存する。また1ヶ月に一度主鍵は変更される。

主鍵の更新の処理の流れ



改竄の有無のチェック

原簿内のタイムコードと原簿のタイムスタンプを比較することにより、改竄の有無をチェックする。

階層的暗号化法を一般鍵の隠蔽に使う場合

この場合、HES 以外の暗号を異なるのはマスターキーの扱いである。マスターキーは、2枚の異なる IC カードを読み取り機に差し込むことによって使えるようになる（したがって読み取り機は2台必要になる）。

実装するプログラムの機能

カテゴリー	機能	説明または備考
認証	ICカード読み取り	LINUX 用の読み取りプログラムの市販品があるか不明で、現在調査中。
	ユーザIDとパスワードによる認証	
主鍵関連	主鍵生成	管理者が行うモードと cron が行うモードの2つがある
	主鍵の floppy disk などへの保存	管理者が行う。
	主鍵のメモリ上へ載せる	主鍵自体をデーモン化する
	主鍵の定期的な更新	cron を用いる
一般鍵関連	一般鍵生成	
	一般鍵によって原簿のタグ内のデータを隠蔽	
	主鍵による一般鍵の隠蔽	
	主鍵による一般鍵の暗号の解除	
	一般鍵によって抽出ファイルの暗号を解除	
抽出ファイル関連	権限テーブルを参照して原簿からそのクライアントが参照または変更できる部分を抽出する	
	閲覧権限保有者には SSL トンネルを通じて抽出ファイルの内容を送る	
	変更権限保有者の従って抽出ファイルの内容を変更する	
	変更した抽出ファイルを原簿に埋め込む	
	閲覧権限保有者が閲覧した抽出ファイルを消去する	
改竄関連	改竄チェック	
履歴関連	履歴を原簿に記録する	
HES 関係（オプション）	階層的暗号化法の構成を決め（段数、子鍵の数、孫鍵の数など）	
	階層的暗号鍵のマスターキーを生成する	
	マスターキーを使えるようにするためのプログラム	読み取り機は2台必要。LINUX 用の読み取りプログラムの市販品があるか不明で、現在調査中。
	子鍵（一般鍵）で原簿のタグ内のデータを隠蔽	
	主鍵によって子鍵（一般鍵）を隠蔽	
	主鍵によって子鍵（一般鍵）の暗号を解除	
	子鍵（一般鍵）で原簿のタグ内のデータの暗号を解除	