



電子文書の公平な公開を保証する 暗号化システム (1)

明治大学 理工学部
情報科学科 中所研究室

| | |
|------------------|--|
| 概要 | <ul style="list-style-type: none">●略称: タイムロックメッセージ●機能: 「後で見て欲しい」メッセージを, 暗号化して渡し, 指定時刻に達すると復号化 |
| 特徴 | <ul style="list-style-type: none">●指定時刻に達するまで, 電子文書の内容を 閲覧できないことを完全に保証●サーバの管理者の操作ミスや 意図的な不正行為を完全に防ぐ |
| 用途 | <ul style="list-style-type: none">●公共分野<ul style="list-style-type: none">* 競争入札の公告や開札* 選挙の投票の開票* 全国共通試験問題●遊び・生活分野<ul style="list-style-type: none">* 囲碁、将棋の封じ手* Mr. マリック的な予言* 年賀状、誕生日のメッセージ (配達日指定) |
| 関連 企業 | <ul style="list-style-type: none">●電子政府・電子自治体・政府認証基盤 GPKI (Government Public Key Infrastructure)●グリーティングカードサービス提供サイト |

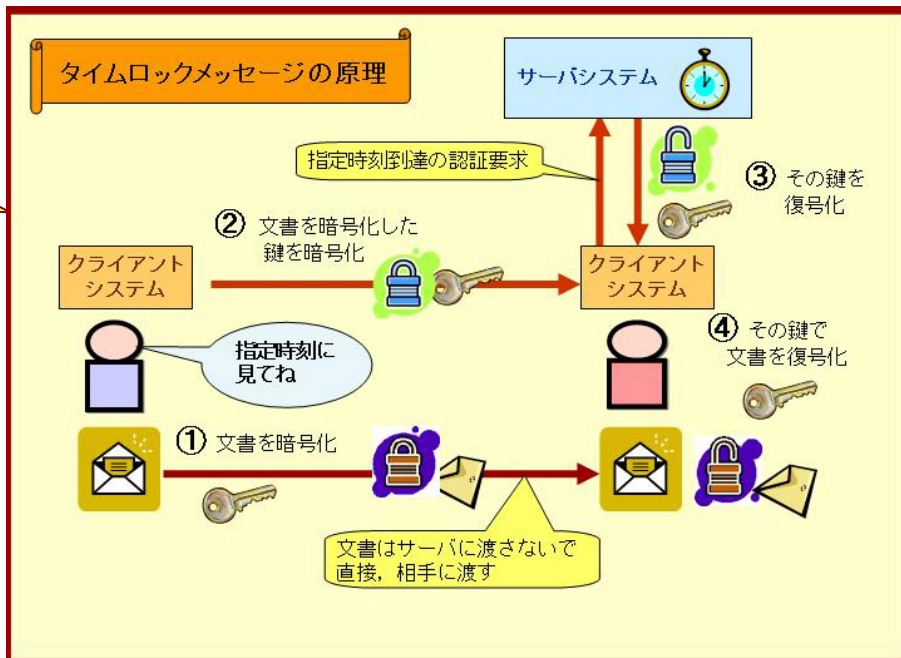


電子文書の公平な公開を保証する 暗号化システム (2)

明治大学 理工学部
情報科学科 中所研究室

特許第3572576号

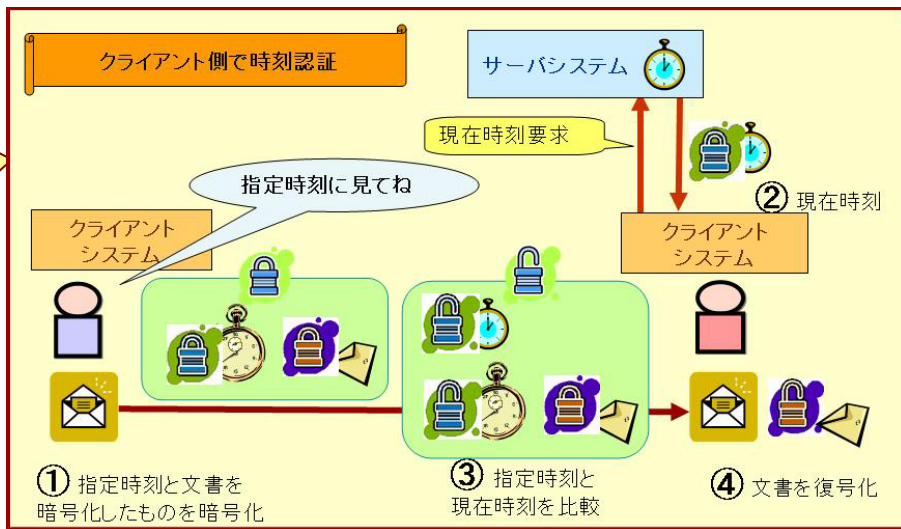
サーバ側で
時刻認証



特許第3577704号

クライアント側
で時刻認証

- サーバの負荷軽減で、応答遅延解消
- ×時刻認証の手順が複雑化





電子文書の公平な公開を保証する 暗号化システム (3)

明治大学 理工学部
情報科学科 中所研究室

