［ゼミ室外秘］

# 「Mr.マリック風予言の管理システム」の試作について
## （別名：電子文書の公平な公開を保証する暗号化システム）

2007.4.？ 中所

１．研究目的

近年，Web アプリケーションを短期間で構築する必要性が高まっている．そのアプローチとして、Web サービスとして実現した（している）要素機能（サブシステム）をネットワーク上で相互に連携して，より大規模なスーパーアプリケーションを形成する方法が注目されている。

そこで，本研究では，近未来の社会的ニーズが高いと思われる例題を取り上げ、その試作を通して Web サービス連携の有効性を検証する。

２．例題

仮名１：「Mr.マリック風予言の管理システム」

仮名２：「電子文書の公平な公開を保証する暗号化システム」

概要：

競争入札の公告や開札，選挙の電子投票の開票，試験問題や結果の公表など，電子文書の公平な公開を必要とすることは多い．その実現のために，あらかじめ暗号化された電子文書が将来の指定時刻まで復号化されないことを保証するシステムを開発する．特に，システム管理者などの内部の関与者からも閲覧ができないことを保証するために，時刻認証と暗号技術を組み合わせたソフトウェアシステムとして実現する．

主要な分野としては，公平性が重視される電子政府，電子自治体がある．公平に公開されるべき文書の内容が事前に漏れないことや，締切前に提出した文書が締切前には閲覧できないようにすることなどである．このような行政サービスの普及のためには，インタフェースはインターネットを前提にしたＷｅｂサービス機能として実現する必要がある．このほか，グリーティングカードサービスのような個人向けサイトで，文書の秘密性を完全に保証するサービスがある．

参考資料：「タイムロックメッセージ」

３．試作の内容

・時間に余裕のある範囲で、できるところまで、プログラムを作ってみる。
・ビジュアルな部分を優先する。機能はサブセットの基本機能のみでもよい。
・途中で、適宜、打ち合わせ実施。（不明な点は、早めに問い合わせること。）

以上