

ブロックチェーンとPKIの微妙な関係

セコム IS研究所/JNSA電子署名WG 佐藤雅史

～PKIとブロックチェーン(分散台帳)と私～

- ディレクトリサービス、PKI、ID連携、電子署名・タイムスタンプ（長期署名）、etc. これまで見てきた技術とアプローチは異なるが、ユースケースとしては共通点がある。
 - ブロックチェーン/分散台帳として大事な概念や要素は何か？
 - ソレでなければいけないユースケースが見えてくるとGood
- 仕組み（議論のネタ？）として面白そう
 - 様々な技術分野どうしの交流のきっかけに？
 - （電子署名の観点の場合）電子署名の生成と検証、そして台帳生成のフローが一貫しているのが興味深い。
- 一時のブームか？今後の技術の一分野となりえるか？
 - 実際の利用場面や周辺環境も含めた場合に適した解となりえるか？
 - 過去と同じ議論がループ？車輪の再発明？…にならないように…

データ・システム間連携の新たな時代を幕開けできるか？

スタンドアロン時代



個別のPCにあるデータと
アプリで完結していた世界

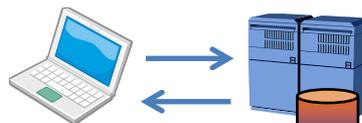
クラサーバ時代



クライアント

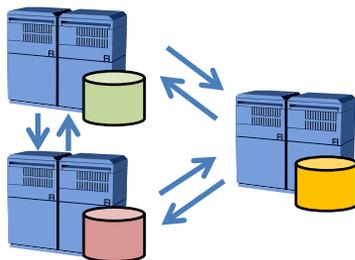


サーバ



シンクライアント

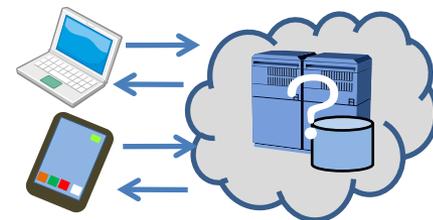
データ・機能連携時代



ディレクトリサービス、
Webサービス/SOA、
ID連携(SAML, OpenID)、
OAuth等々

必要に応じてデータや機能を
提供/利用する。
**(必要最小限のデータ・機能
提供とは何か?)**

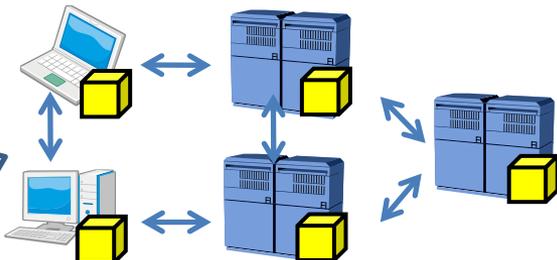
仮想化・クラウド時代



従来の試みが
直面してきた
組織間連携の
難しさ。

本気度は
いかほど？

データ共有・連携時代???



分散台帳・ブロックチェーン

同じデータを共有して利用する。
**(共有を前提としたうえで
アクセス制御やプライバシーを
どうしましょうか?とか)**

なかなか挑戦的にも見えるアプローチかも…