ブロックチェーンとPKIの微妙な関係
～JNSA電子署名WG、タイムビジネス協議会の立場から～

三菱電機　宮崎一哉

◆ JNSA電子署名WGの立場から
- ブロックチェーンで（電子署名法でいうところの）電子署名を実現できるか？
- 本人性が問題？・・・ビットコインは匿名性が、、取引所では身元確認が、、
- 何らかのコミットを行ったという記録は改ざんできずに共有できそうだが、、、

◆ タイムビジネス協議会の立場から
- ブロックチェーンで（日本の認定）タイムスタンプを実現できるか？
- 時刻のトレーサビリティが重要？・・・ハッシュのリンクだから順序性は説明できそう、、ビットコインでもいろんなところに時刻が記録されている、、
- リンキングプロトコルのタイムスタンプはブロックチェーン？
- 長期署名におけるPoE（Proof of Existence）には使えそう？

◆ PKIとブロックチェーンにおける「トラスト」とは？
- 第三者に対するトラストの提供：
  - 当事者が信用するのはいいが、第三者に対して信頼を与えられるの？
  - 「認定」するとして、何を認定するの？
- 長期にわたるトラストの維持：
  - 暗号アルゴリズムの脆弱化を乗り越えて、何十年もブロックチェーン全体をみんなで共有するの？