PKI Day 2017

セコムIS研究所
Intelligent Systems Laboratory

IoT・ブロックチェーン時代のPKI

2017年　4月　19日

松本　泰　　セコムＩＳ研究所

© 2017　SECOM CO.,LTD.

PKI Day 2017
IoT・ブロックチェーン時代のPKI

セコムIS研究所
Intelligent Systems Laboratory

- 今回のPKI day 2017では、現在、世の中で注目されているIoT・ブロックチェーンの技術とPKIの関係をテーマに取り上げます。
- IoTに関して、500億個以上にもなると言われているIoTデバイスは、単純に繋がることで価値を生むわけではありません。何らかのIoTデバイス間等のTRUST（信頼関係）が、IoTに価値を与えることになります。その際、多様な信頼関係を形成するためには、公開鍵暗号、更には標準化された公開鍵暗号技術であるPKIが大きな役割を果たすべきだと考えられます。その一方、リソースやコスト制約のあるIoTデバイスにおいて、PKIはどのように実装させるか等に大きな課題があります。
- ブロックチェーンに関して、非中央集権システムを実現する技術として注目されています。同じ暗号技術であるPKIは、ブロックチェーンにとって代わられるものなのか、共存して行くものなのか。棲み分けられるものなのか。
- PKIやブロックチェーンのような暗号技術によるプラットフォームが、社会基盤としての機能するためには、暗号技術と複雑な社会の双方の理解が必要になります。
- PKI day 2017では、以上を踏まえ「IoT・ブロックチェーン時代のPKI」をテーマに、今後の社会におけるPKIの在り方を議論します。

© 2017 SECOM CO.,LTD.

PKI day 2017 までの歩み

セコム IS研究所
Intelligent Systems Laboratory

回	年	PKI day テーマ
1	2005	PKI技術最新事情
2	2006	PKIの展開と最新技術動向
3	2007	PKIの過去・現在・未来
4	2008	PKIの標準から実装まで 最新動向
5	2009	さまざまな分野に展開されるPKIの最新動向
6	2010	社会基盤としてのPKI／PKIの10年
7	2011	番号制度時代のPKI
8	2012	・我が国における信頼基盤の連携に向けて ・PKIへの攻撃とその対応
9	2014	・公開鍵暗号に関連する周辺技術動向の共有 ・デジタル社会のための「電子署名を見直す」
10	2015	サイバーセキュリティの要となるPKIを見直す
11	2016	マイナンバー時代のPKI
12	2017	IoT・ブロックチェーン時代のPKI

© 2017 SECOM CO.,LTD.

PKI day 2017 プログラム

セコム IS研究所 Intelligent Systems Laboratory

- 午前
  - 「PKI Day 2017のオーバービュー」 セコム株式会社 IS研究所／PKI相互運用技術WGリーダー　松本　泰 氏
  - 「どこでも公開鍵暗号」　横浜国立大学　教授　松本　勉 氏
  - 「自律するIoTのためのセキュリティ技術の取り組み」 ルネサスエレクトロニクス株式会社　シニアスペシャリスト　高比良 賢一 氏
  - 「IETFにおけるIoT/暗号技術に関する標準化動向」　株式会社レピダム　取締役　菅野　哲 氏
- 午後の前半
  - 「OpenSCによるJPKIカードドライバ」 オープンソース・ソリューション・テクノロジ株式会社 エキスパート 濱野　司 氏
  - 「FIDO認証と公開鍵暗号」　ヤフー株式会社 Yahoo! JAPAN 研究所 上席研究員 五味 秀仁 氏
  - 「ブロックチェーンとは何なのか？」 セコム株式会社 IS研究所/電子署名WGサブリーダー 佐藤 雅史 氏
- 午後の後半
  - パネルディスカッション「PKIとブロックチェーンの微妙な関係」

© 2017　SECOM CO.,LTD.

2017年バズワード・ランキング？？
IoT、BD、AI、Fintech、ブロックチェーンとトラスト

セコムIS研究所 Intelligent Systems Laboratory

- IoT
  - IoTの価値は、IoTデバイスが出力するデータに信頼に大きく依存するのでは？
- BigData
  - （人が入力するデータではなく）IoTデバイスから出力されるデータにより形成
  - IoTデバイスに信頼がなければ、BigDataも単なるゴミデータになる
  - 信頼のおけるBigDataのためのデジタル署名、タイムスタンプ、ブロックチェーン？が必要？？？
- AI
  - 信頼のおけるBigDataなしに信頼のおけるAIは、あり得ない（と思う）
- Fintech　***
  - 「ICTを駆使した革新的（innovative）、あるいは破壊的（disruptive）な金融商品・サービスの潮流」***
  - 新しい技術の話ではない。金融分野におけるスマート社会への移行？？
  - 金融分野における新たなエコシステム／トラストモデル
- ブロックチェーン（技術）
  - Fintechの中で、数少ない新しい技術を思われている節がある。
  - 多くの場合、ブロックチェーン（技術）の何が新しいのか理解されていない。

*** 出典：フィンテック（Fintech）と http://www.fujitsu.com/jp/group/fri/businesstopics/fintech/definition/

© 2017 SECOM CO.,LTD.

Society 5.0的世界観におけるトラスト（≒PKI）

セコム IS研究所 Intelligent Systems Laboratory

- Society 5.0とは　　***
  - 狩猟社会、農耕社会、工業社会、情報社会に続く、以下のような新たな経済社会をいう。(1) サイバー空間とフィジカルカル空間を高度に融合させることにより、(2) 地域、年齢、性別、言語等による格差なく、多様なニーズ、潜在的なニーズにきめ細かに対応したモノやサービスを提供することで経済的発展と社会的課題の解決を両立し、(3) 人々かが快適で活力に満ちた質の高い生活を送ることのできる、人間中心の社会
- 松本の考える？？Society 5.0的世界観におけるトラスト（妄想？？）
  - フィジカルカル空間に広くIoTデバイスを配置し、サイバー空間と高度に融合
    - ⇒　　このIoTデバイス・サービスのためのトラスト
  - 広く配置したIoTデバイスが出力するデータは、BigDataを形成し、そのBigDataをAIが解析し、さらにその解析結果をフィジカルカル空間に反映するといったスマート社会
    - ⇒　　このスマート社会のためのトラスト
    - ⇒　　IoT、BigData（、AI）が価値をもたらすためのトラスト
- 「人々かが快適で活力に満ちた質の高い生活を送る」ために、マルチステークホルダー（多様なステークホルダー）の連携により「モノやサービスを提供」したい。
  - マルチステークホルダーのためのトラスト≒公開鍵暗号、PKIによるトラスト

*** 総合科学技術・イノベーション会議　科学技術基本計画 2016年1月22日 http://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf

© 2017　SECOM CO.,LTD.

IoTデバイス・サービスが価値を産むためには

セコムIS研究所 Intelligent Systems Laboratory

IoTデバイスが出力するデータで、価値を生む多くがパーソナルデータ

脆弱性対応としてのセキュリティ対策

- 製品サイクルを考慮したセキュリティ・バイ・デザイン
- PDCAサイクル
- 緊急対応体制(CSIRT)の確立

暗号技術によるトラスト

- IoTデバイスへの暗号技術の組み込み
- ハードウェアセキュリティ
- IoTデバイス の Root of Trust

プライバシー保護

- IoT利活用のためのプライバシー・バイ・デザイン

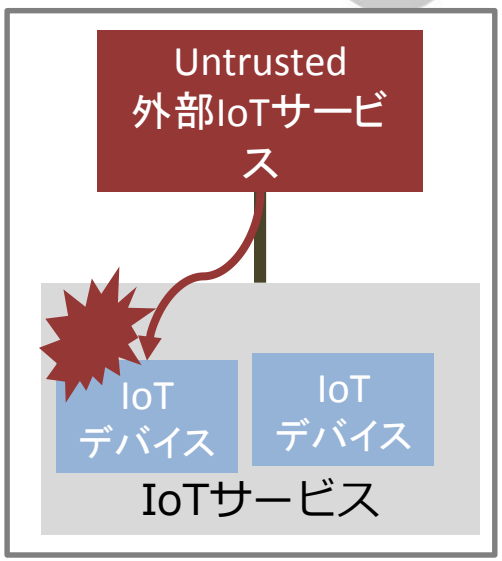
- IoTデバイスが価値を生むためには、IoTデバイス・IoTデバイスが出力するデータが、信頼のおけるものである必要がある。
- 更に、多様な信頼関係（トラスト）が、多様な価値を産み、それがイノベーションに繋がる？？

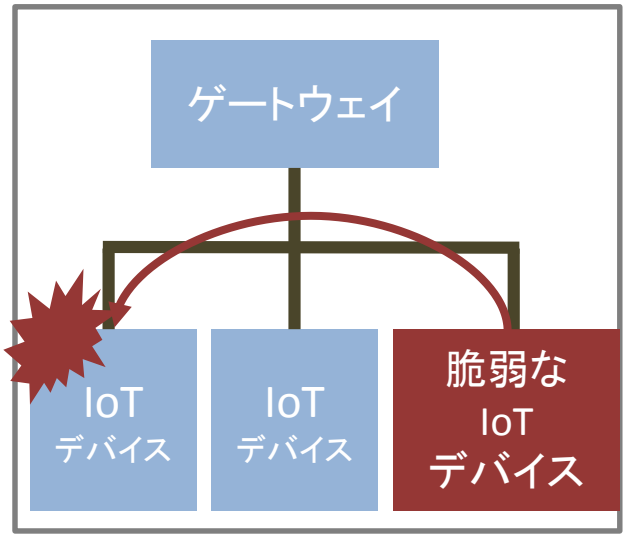
© 2017 SECOM CO.,LTD.

IoTにおける攻撃と対策（トラストの関係）

セコムIS研究所
Intelligent Systems Laboratory

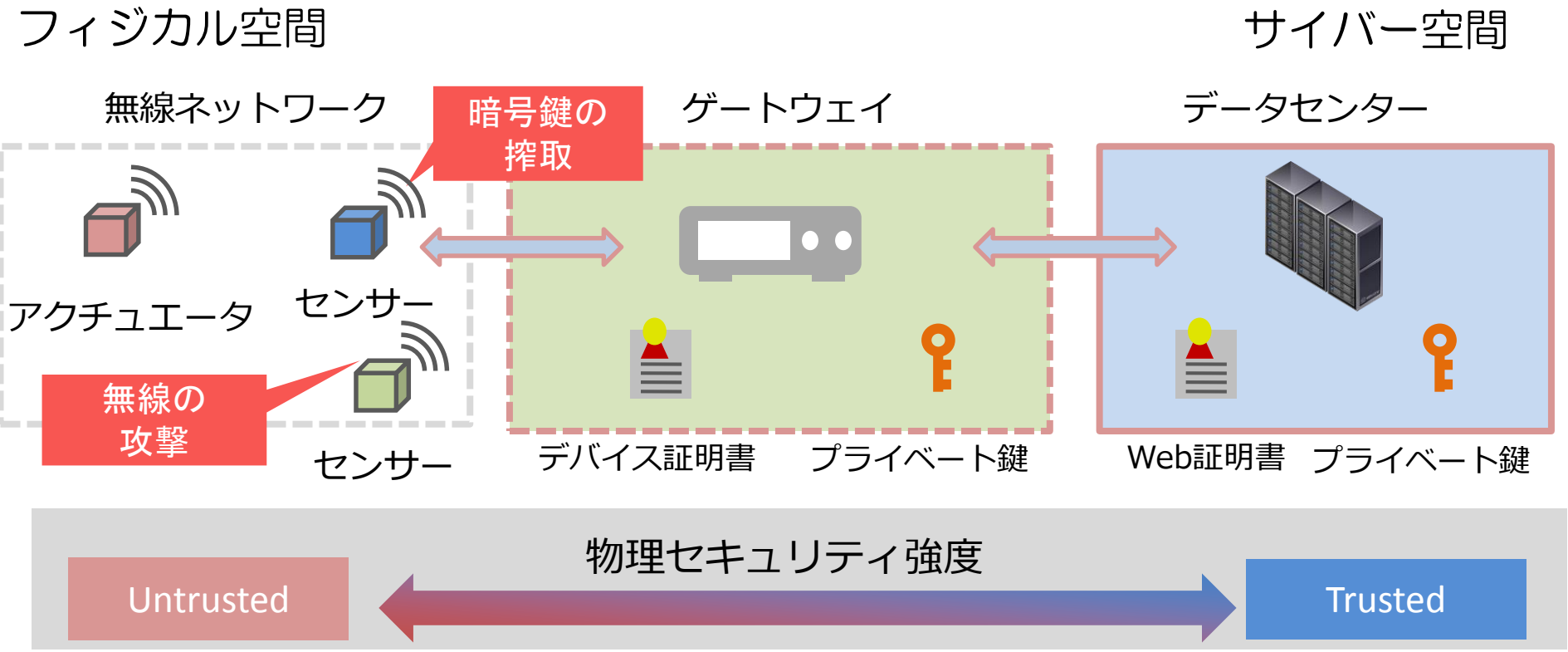
- IoTデバイスとサービスの信頼（Trust）
  - IoTデバイスが、信頼関係ない外部のサービスと接続されてしまう問題
  - ⇒ 外部のサービスとの間のトラストの確立
- 外部のネットワークから脆弱なデバイス・プログラムへの攻撃（乗っ取り）
  - ⇒脆弱性をなるべく作らない（セキュリティ・バイ・デサイン）
  - ⇒脆弱性対応　⇒　セキュアなプログラムコードの更新
    - ⇒信頼できるコードの検証（コード署名）
    - ⇒ そのためのRoot of Trust （信頼の起点）組込み
- IoTデバイス間の信頼(Trust)
  - 脆弱なIoT機器から、重要な制御を行うIoTデバイスへの攻撃
  - ⇒IoT機器の認証（ Certification ）
    - 認証（ Certification ）されたIoT機器のみ接続
    - ⇒IoT信頼のおけるデバイスの証明





© 2017 SECOM CO.,LTD.

「何処でもIoT」のためのセキュリティ



- IoTデバイスは弱い物理的環境に置かれることが想定されるため、「**物理的環境に依存しないセキュリティ**」が求められる。
- 物理的環境による保護に代わる「**ハードウェアセキュリティ**」が必要
- 広く配置されるIoTデバイスを収容するための無線＋無線セキュリティ技術

→　必然的に「**暗号技術によるトラスト**」が重要になる

© 2017 SECOM CO.,LTD.

マルチステークホルダー環境におけるトラスト
自動運転時代における
ECUに係るステークホルダーと権限管理への要求

セコムIS研究所
Intelligent Systems Laboratory

番号	ロール	権限レベル	権限
ユーザロール1	ECU製造者	高い	ECU自体へのアクセスとアップデート
ユーザロール2	自動車メーカー		各装置へのアクセスとアップデート
ユーザロール3	修理工場		自動車メーカーから配布されたツールをもとに各装置へのアクセスとアップデート
ユーザロール4	検査機関/警察		OBDポートから各装置の状態の読み込み
ユーザロール5	オーナー/運転手	低い	アクセス権なし

Horizon 2020 Program, SHARCS(Secure Hardware-Software Architectures for Robust Computing Systems), Deliverable D2.1, “SHARCS Applications and framework requirements for secure-by-design systems”から抜粋・訳

- こうした、マルチステークホルダーによる権限管理の理想モデルとして、PKI（公開鍵基盤）による各エンティティを証明する公開鍵証明書と、証明された各エンティティの権限を証明する属性証明書を使うモデルがある。
- しかし、すべてのECUにおいて公開鍵を扱うことは難しく、公開鍵と共通鍵のハイブリッドモデルを考える必要がある　→これが簡単ではない！！

© 2017 SECOM CO.,LTD.

IoTにおける暗号技術の役割（コネクテッド・カーの場合）

セコム IS研究所 Intelligent Systems Laboratory

- 認証 – 機器の認証、サービスの認証等
  - CANに接続されたECU-ECU間の双方向の認証
    - 乗っ取られたECUから別の（無関係な）ECUへの攻撃を防ぐ
  - TCU(Telematics Control Unit) と外部サービス間の双方向の認証
- デジタル署名による証明、及び、証明書
  - コード署名 – プログラムコードの正当性の検証 – OTAでは非常に重要
  - 車のビジネスに係る様々なステークホルダー・エンティティ（人、組織、機器）の電子証明書と、そのエンティティによるデジタル署名による様々な証明 。
  - サプライチェーンにおける電子証明によるトラストチェーン
    - ex. 正当な保守ツールの証明書、認定された修理工場の証明書、検査機関の証明書、検査機関により検査されたことの証明書、etc.
  - -> マルチステークホルダー下において、様々なモノとサービスの連携を行うためのトラストチェーン　⇒　スマート社会？
  - -> ビジネス的に要求される信頼関係を暗号技術・PKIにより実装？？
- 暗号化
  - TCUと外部のサービス間や、車に格納されたプライバシー情報の暗号化

© 2017 SECOM CO.,LTD.

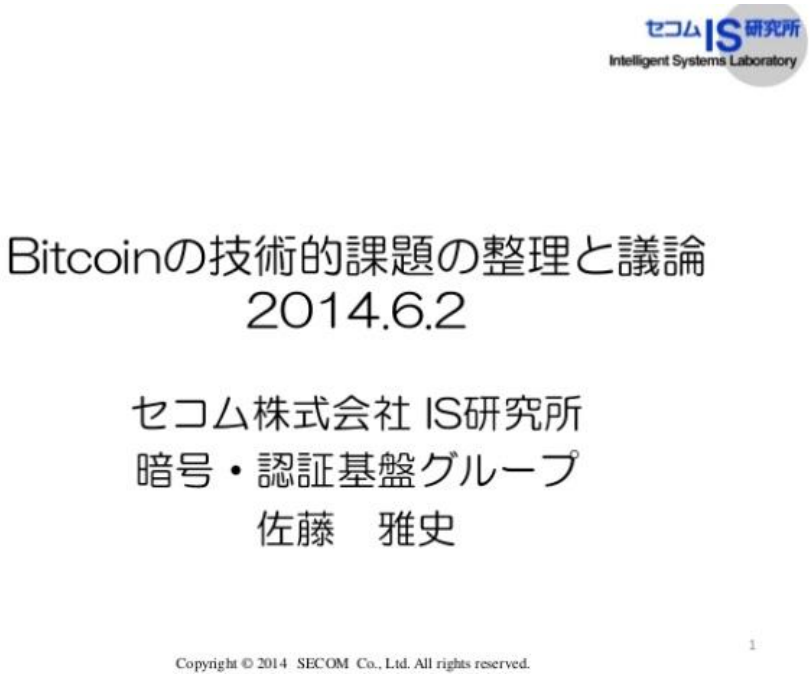
IoTデバイス・サービスにおけるPKIの課題

セコムIS研究所 Intelligent Systems Laboratory

- IoTデバイスにおける暗号技術の要求
  - 物理的環境に依存しないためのハードウェアセキュリティ
  - 限られたリソースにおける公開鍵暗号技術の実装
  - 様々なトレードオフが必要な環境下での実装
    デバイスコスト、省電力無線+省電力暗号、低遅延暗号等の要求
- IoTサービスにおける暗号技術の要求
  - サービスにおけるイニシャルコスト・設置コスト
    - クレデンシャル発行のサプライチェーン
    - 設置の容易性とセキュリティ
  - 長期の信頼のおける運用
    - 大量のIoTデバイス・暗号鍵の管理、信頼のおける鍵配布、失効
    - 信頼のおける暗号鍵の運用と運用コストの最適化
- IoTデバイス・サービスのための標準化
  - 信頼がおける効率的なクレデンシャル発行とか
    - Trust provisioning、Device provisioning etc…
  - Etc….

© 2017 SECOM CO.,LTD.

ブロックチェーンに関連する活動
JNSA Bitcoin 勉強会　2014年6月2日
PKI相互運用WG・電子署名WGの共催



この頃：Bitcoinは、（技術的に）よー分からん。⇒　技術的には、よー分かった。⇒　興味喪失？？？

出典：
Bitcoinを技術的に理解する　https://www.slideshare.net/kenjiurushima/20140602-bitcoin1-201406031222
Bitcpoinの技術的課題の整理と議論 https://www.slideshare.net/MasashiSatoJP/jnsa-bitcoin-20140602

© 2017 SECOM CO.,LTD.

ブロックチェーンは本当に世界を変えるのか

2016/07/01　日経FinTech

まだまだ未成熟なブロックチェーン、実用には四つの課題

2015年来、ブロックチェーンはFinTech（金融とテクノロジーの融合領域）の文脈のみならず、そこを飛び越えた領域でも、インターネット革命と近いレベルの「ディスラプティブ（破壊的）」な技術と喧伝されている。ブロックチェーンの現状の課題を四つの問題提起で解説する。（2016/7/1）

ブロックチェーンは、結局のところ何が新しいのか

一口に「ブロックチェーン」といっても、その利用形態はプラットフォームやサービスごとに大きく異なる。「ブロックチェーン」と呼ばれる技術の代表的なメカニズムから共通的な要素を抽出し、その意味するところを改めて探りたい。（2016/7/14）

国際的な存在感が希薄すぎる日本のブロックチェーン業界

ビットコインを端緒としたブロックチェーン技術の応用は、国内外を問わず大きな熱量を持って広まっている。今回はブロックチェーンを取り巻く世界の潮流と、それを踏まえた国内の状況に関して、その渦中からではなく第三者からの視点で俯瞰してみたい。（2016/9/9）

出典：　ブロックチェーンは本当に世界を変えるのか
http://itpro.nikkeibp.co.jp/atcl/column/16/062400138/

セコムIS研究所
Intelligent Systems Laboratory

- 2015年12月
  秘密会合？？
- 2016年7月1日
  連載開始
- 2017年2月13日
  最終回

松尾 真一郎 氏
MITメディアラボ、
東京大学生産技術研究所

佐藤 雅史 氏
セコムIS研究所

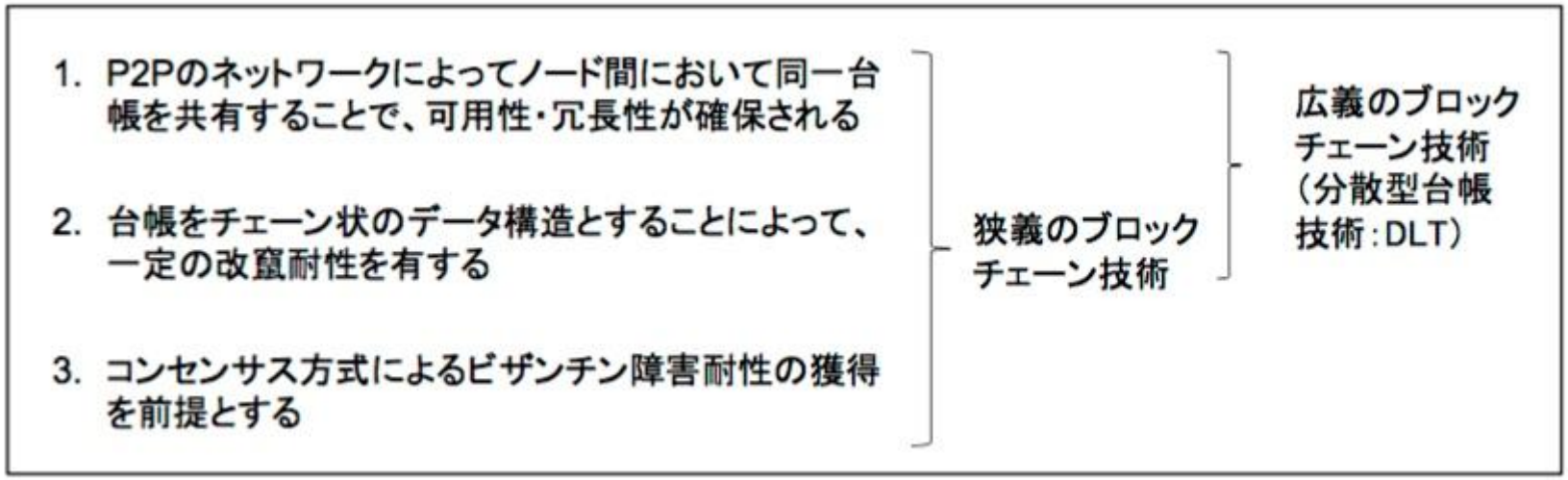
林 達也 氏
レピダム
代表取締役

© 2017 SECOM CO.,LTD.

ブロックチェーン技術と既存技術？？

セコムIS研究所
Intelligent Systems Laboratory

「ブロックチェーン技術の活用可能性と課題 に関する検討会報告書」***におけるブロックチェーン技術



- 2. 改竄耐性、完全性
  - 従来からのタイムスタンプ技術 との関係？
- 3. 可用性・冗長性
  - 署名されたデータであれば、分散配置可能であり　⇒　可用性確保
  - 例えば「証明書失効リスト」「CT(Certificate Transparency)」
    - #CRL は、「公開された失効台帳」

出典：ブロックチェーン技術の活用可能性と課題 に関する検討会報告書
- フロックチェーン技術か銀行業務に変革をもたらす可能性を見据えて -
https://www.zenginkyo.or.jp/fileadmin/res/news/news290346.pdf

© 2017　SECOM CO.,LTD.

タイムスタンプ・プロトコルに関する技術調査

最終更新日　2004年 2月18日

独立行政法人 情報処理推進機構
セキュリティセンター
isec-info@ipa.go.jp

実施者

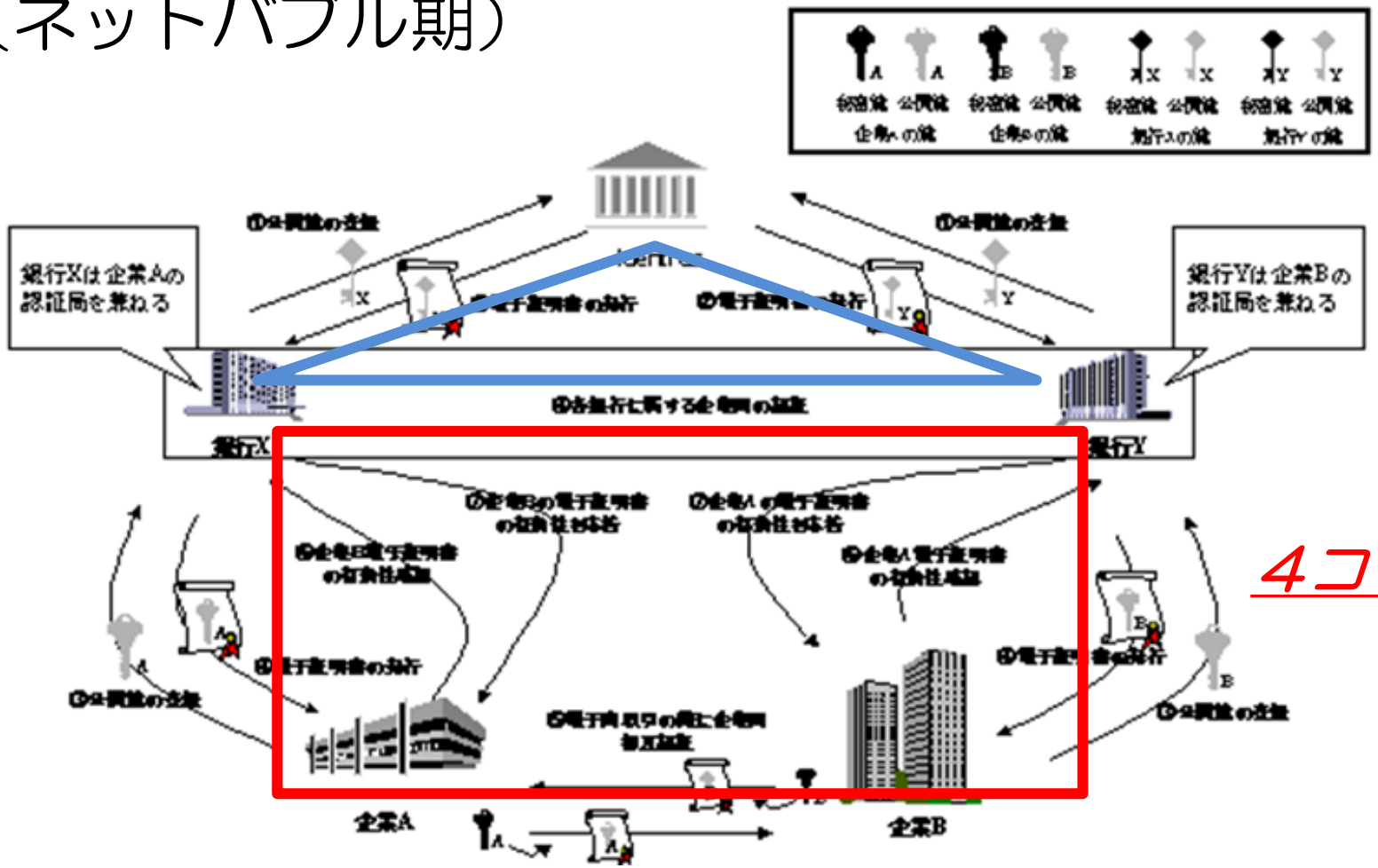
- NPO 日本ネットワークセキュリティ協会
「2003年度 情報セキュリティ関連の調査に関する公募」において採択。

- タイムスタンプの利用が想定される分野は、幅広い。公開文書(約款、技術報 告書、IR 情報)、知的財産(実験データ、設計図、写真)、業務文書(契約書、議 事録)、記録(作業・検査報告、監査記録)等の電子文書にタイムスタンプを適正 なコストで施すことができれば、その文書の信頼性、証拠性としての価値を飛躍 的に高めることが可能になる。
- タイムスタンプによって完全性を確保した電子文書の保存は、監査等の作業効率と精度を高める可能性がある。このように、透明 性があり効率的な電子社会の誕生のためにも、電子署名やタイムスタンプについ ての基盤整備は有意義である。

出典:　https://www.ipa.go.jp/security/fy15/reports/tsp/index.html

© 2017 SECOM CO.,LTD.

2000年頃のFintech??　Identrus
（ネットバブル期）



HAT

4コーナー

４コーナーモデル　--　トランザクションに信頼を与える仕組み

HAT　--　信頼のおける（ポリシが整合した）金融機関を追加する仕組み

→デジタルデータのみで自動的にトランザクションを検証する

出典：　Identrusのイメージ https://www.ipa.go.jp/security/enc/digitalsignature/32_ED.htm

© 2017 SECOM CO.,LTD.

2017年度版「4コーナモデル+ HAT」の妄想？

セコムIS研究所 Intelligent Systems Laboratory

- 2000年頃のIdentrusの 「4コーナモデル+ HAT」
  - 4コーナモデルの顧客の取引（異なるパーティ間の取引の仕組み）
    - 当時、４コーナモデルは成功せず、3コーナモデルで利用
    - #ブロックチェーンによる金融機関間の海外送金等と類似
  - HAT:I　dentrusのポリシーに整合した金融機関へCA証明書を発行
- では、2017年現在における「 4コーナモデル+ HAT 」を実装を妄想
  - 各金融機関のクレデンシャル管理
    - 犯罪収益移転防止法、KYC（Know Your Customer）対応
    - リモート認証は、JPK利用者認証用証明書、または、FIDOトークン？？
    - 本人と結びつきを保証したリモート署名のための仮名証明書の発行
      - 仮名証明書は、何枚でも発行
      - 仮名証明書に対応したオンライン・ウォレットの秘密鍵管理
  - HATの実装
    - ポリシーを満足していることを示すCA証明書を金融機関のへ発行
  - 4コーナモデルの実装
    - 顧客は、仮名証明書を使い分けることができる。
    - リモート署名サーバで署名したトランザクション(送金データ等）をブロックチェーン？？に書き出し

© 2017 SECOM CO.,LTD.

「OpenSCによるJPKIカードドライバ」
オープンソース・ソリューション・テクノロジ株式会社
エキスパート　　濱野　司 氏

セコムIS研究所
Intelligent Systems Laboratory

IC・ID カードの相互運用可能性の向上に係る基礎調査 報告書

掲載日　2007年　1月11日

独立行政法人 情報処理推進機構
セキュリティセンター

概要

ICカードを利用し個人等を識別するIC・IDカードは、今後オンラインでの各種サービ等をセキュリティ面で支える社会インフラに成長する兆しを見せている。　しかし、そのためには、クライアント環境や製造ベンダー等の違いによりサービス分野等をまたがっての利用に技術的な制約を受けない、相互運用可能性の確保が必要である。

シーズ調査では相互運用可能性を実現する標準化動向や海外の取組みにおける技術体系の事例を、またニーズ調査では現在のIC・IDカードにおける相互運用可能性の実態と今後への展望を調査し、今後国内でIC・IDカードの相互運用可能性の向上に必要になる、国際標準を活用した関連技術の標準化やツール開発、普及方策の検討を行った。

実施者

- NPO 日本ネットワークセキュリティ協会（JNSA）

出典：http://www.ipa.go.jp/security/fy18/reports/ICID/

© 2017 SECOM CO.,LTD.

セコムIS研究所
Intelligent Systems Laboratory

パネルディスカション
ブロックチェーンとPKIの微妙な関係

© 2017 SECOM CO.,LTD.

パネリスト

- 宮崎 一哉 氏
  - 三菱電機・生産システム本部/電子署名WGリーダー
  - タイムスタンプ協議会
- 満塩 尚史 氏
  - 経済産業省　CIO補佐官
- 宮内 宏 氏
  - 宮内・水町IT法律事務所　弁護士
  - 電子契約
- 松尾 真一郎 氏
  - MITメディアラボ、東京大学生産技術研究所
- 林 達也 氏
  - レピダム　代表取締役
- 佐藤 雅史 氏
  - セコムIS研究所

© 2017 SECOM CO.,LTD.

パネルディスカヨンのお題目？？

セコムIS研究所
Intelligent Systems Laboratory

- そもそもブロックチェーンの分類、定義
  - パブリックブロックチェーン
  - 「プライベートブロックチェーン」は、新しい技術なのか？
- 仮想通貨、仮想通貨交換業者にとってのブロックチェーンの課題は？
  - パブリックブロックチェーンの議論
  - 規制との関係
- スマートコントラクトは、本当に可能なのか？
  - パブリックブロックチェーンの議論
  - そもそも契約とは
- プライベートブロックチェーンの意義はどこにあるのか？
  - 金融分野以外のブロックチェーンの意味するところは？
  - 金融分野以外においてパブリックブロックチェーンは成立するのか？
  - 「プライベートブロックチェーン」は、そもそも意味があるのか？
- etc….

© 2017 SECOM CO.,LTD.

過去のPKI day の参考スライド

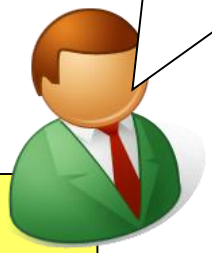
© 2017 SECOM CO.,LTD.

２０１１年現在の状況？

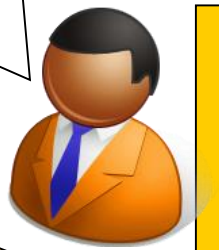
セコムIS研究所
Intelligent Systems Laboratory

"Rough consensus and running code"

法制度等から
ニュートラルな
技術標準



民事訴訟法は228条4項 「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立。。」



ギャップ
噛み合わない会話
共有されないビジョン

技術標準

・既存のレガシーな法制度
・様々な管轄官庁の様々な業法

デファクト標準
としての実装

対極の実装

紙前提の制度
（の電子化）

強い影響

「電子署名法」、「e文書法」、「電子公証人制度」、「商業登記に基づく電子認証制度」、「住民基本台帳制度」、etc….

現実の実務からの乖離という問題

既存の慣習、権益が強すぎる問題

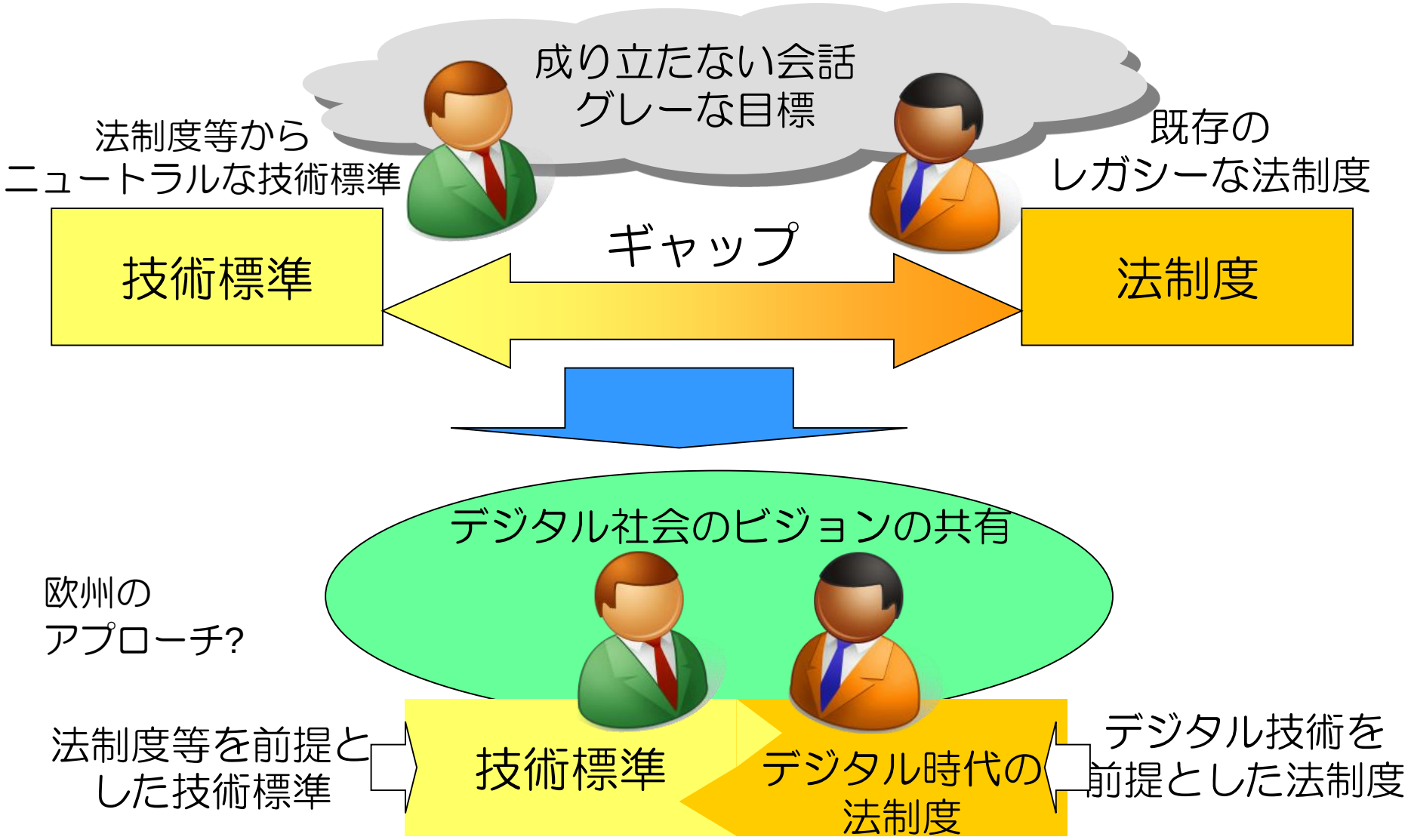
「光の道」で医療問題も教育問題も解決する？

番外編

現在の医療の問題点は、デジタル化以前の問題

© 2017 SECOM CO.,LTD.

技術と制度をかみ合わせるためには



© 2017 SECOM CO.,LTD.

PKI day 2015のオーバビュー

セコムIS研究所
Intelligent Systems Laboratory

3部　広がるサイバー空間に対応するPKIの新しい応用領域

時代の要請

マイナンバー制度の時代

ビッグデータ時代

IoT時代

サービスレイヤー

行政サービス
医療サービス
金融サービス
Webサービス

電子契約書
医療記録
電子領収書
プログラム（コード署名）

オープン化する制御システム
医療機器
ITS
車の車載器
IPルーティング

信頼が必要な情報連携サービス

信頼が必要なデジタルコンテンツ

数百億個のデバイスの多様な信頼関係

トラストレイヤー

eIDAS
電子署名
タイムスタンプ
電子シール
電子配布
Webサイト認証

Web trust for CA
Webサイト認証
DNSSEC
RPKI

（広義の）トラストサービス

トラストを構成する要素

デジタル社会のための法制度

法制度と整合性のある標準化

信頼のおける運用

セキュアな実装技術

暗号技術等のコア技術

1部 新しい時代の電子署名

2部 SSL/TLS実装の今とこれから

PKI day 2015

© 2017 SECOM CO.,LTD.

欧州・米国・日本

セコムIS研究所
Intelligent Systems Laboratory

欧州
規制モデル

米国
市場モデル

トラストが必要なサービス

一般データ
保護規則

個人情報の連携・個人情報の利活用と保護

eIDAS規則

トラストサービス・レイヤー

ハイパー
ジャアアント
による支配？

アイデンティティ管理（自然人、法人）
日本におけるマイナンバー制度等

大陸法的
アプローチ

英米法的
アプローチ

日本の立ち位置は？？

© 2017 SECOM CO.,LTD.