セコムIS研究所
Intelligent Systems Laboratory

MWE 2019
Blockchainの技術的現状とその応用
ブロックチェーンとデータ真正性

2019年11月29日

セコム株式会社 IS研究所
主任研究員
佐藤　雅史

自己紹介

セコムIS研究所
Intelligent Systems Laboratory

発表者

佐藤　雅史

- 情報セキュリティ、特に電子認証や電子署名応用などが専門
- 日本ネットワークセキュリティ協会(JNSA)、日本トラストテクノロジー協会(JT2A)、日本トラストサービス推進フォーラムなどに参画。
- 仮想通貨セキュリティ検討会(CGTF)メンバー
  仮想通貨交換所セキュリティ検討担当
  https://vcgtf.github.io
- ブロックチェーンに関する国際標準 (ISO/TC 307) 国内委員会 セキュリティWG 主査

自己紹介

セコムIS研究所
Intelligent Systems Laboratory

発表者

佐藤　雅史

- 情報セ… …子署名応用な…
- 日本… …SA)、日本… …、日本トラ… …に参画。
- 仮想… …ンバー仮想… … http…
- ブロ… …O/TC 307) …

http://www.nikkeibp.co.jp/atclpubmkt/book/18/265180/

http://www.c-r.com/book/detail/1222

真正性(Authenticity)

※和訳は佐藤によるもの

セコムIS研究所 Intelligent Systems Laboratory

ISO (International Organization for Standardization)	
property that an entity is what it claims to be エンティティが主張している通りのものであるという特性	ISO/IEC 27000:2018
degree to which the identity of a subject or resource can be proved to be the one claimed サブジェクトやリソースのアイデンティティが主張されているものであることを証明できる度合い	ISO/IEC 25010:2011
ITU-T (International Telecommunication Union Telecommunication Standardization Sector)	
The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information. 与えられた情報に改ざんや偽造がないことと、実際に与えたと主張するエンティティによって提供された情報であることを保証できること	J.160 (02)
NIST (National Institute of Standards and Technology)	
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. 本物であり、さらに、検証でき信頼できるという：伝達、メッセージ、またはメッセージ発信者の有効性に対する確実性	SP 800-30 SP-800-53 など
The property that data originated from its purported source データがその発信元から発信されたという特性	SP 800-63-3 SP 800-38B など

データの真正性

- 誰が作った/送った？
- いつ作った/送った？
- どんな内容で？（内容の妥当性ではなく、完全性）

ブロックチェーンとデータ真正性

セコムIS研究所
Intelligent Systems Laboratory

- 誰が作った/送った？
- いつ作った/送った？
- どんな内容で？（内容の妥当性ではなく、完全性）

ブロックチェーンとデータ真正性

セコム IS 研究所
Intelligent Systems Laboratory

- 誰が作った/送った？
- いつ作った/送った？
- どんな内容で？（内容の妥当性ではなく、完全性）
  - デジタル署名によるトランザクションの改ざん対策
  - ハッシュ値のチェーンによるブロック（トランザクションの履歴）の改ざん対策

ブロックチェーンとデータ真正性

セコムIS研究所
Intelligent Systems Laboratory

- 誰が作った/送った？

- いつ作った/送った？
  - ブロックのチェーンによるトランザクションの存在証明（順序性の担保）
- どんな内容で？（内容の妥当性ではなく、完全性）
  - デジタル署名によるトランザクションの改ざん対策
  - ハッシュ値のチェーンによるブロック（トランザクションの履歴）の改ざん対策

ブロックチェーンとデータ真正性

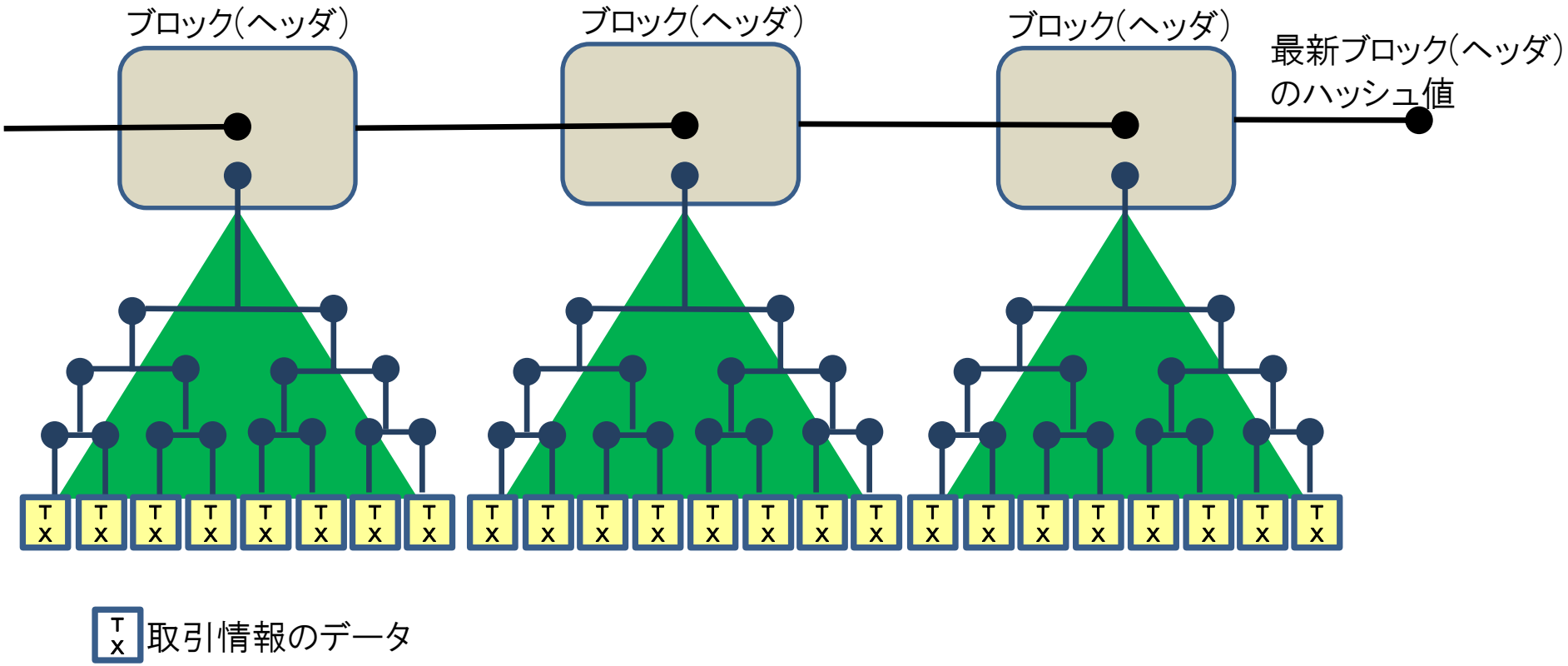
セコムIS研究所
Intelligent Systems Laboratory

- 誰が作った/送った？
  - 証明可能かどうかはケースバイケース
  - デジタル署名に使う署名鍵とエンティティ（実際の送信者など）との紐づけが必要。
- いつ作った/送った？
  - ブロックのチェーンによるトランザクションの存在証明（順序性の担保）
- どんな内容で？（内容の妥当性ではなく、完全性）
  - デジタル署名によるトランザクションの改ざん対策
  - ハッシュ値のチェーンによるブロック（トランザクションの履歴）の改ざん対策

参考：ブロックチェーンの例（Bitcoinのイメージ）

セコム IS 研究所
Intelligent Systems Laboratory

トランザクションとブロックのハッシュ値の連鎖（イメージ）



T X 取引情報のデータ

ある周期的なタイミングで各ブロックが生成される

ブロックチェーン以外のデータ真正性

セコムIS研究所
Intelligent Systems Laboratory

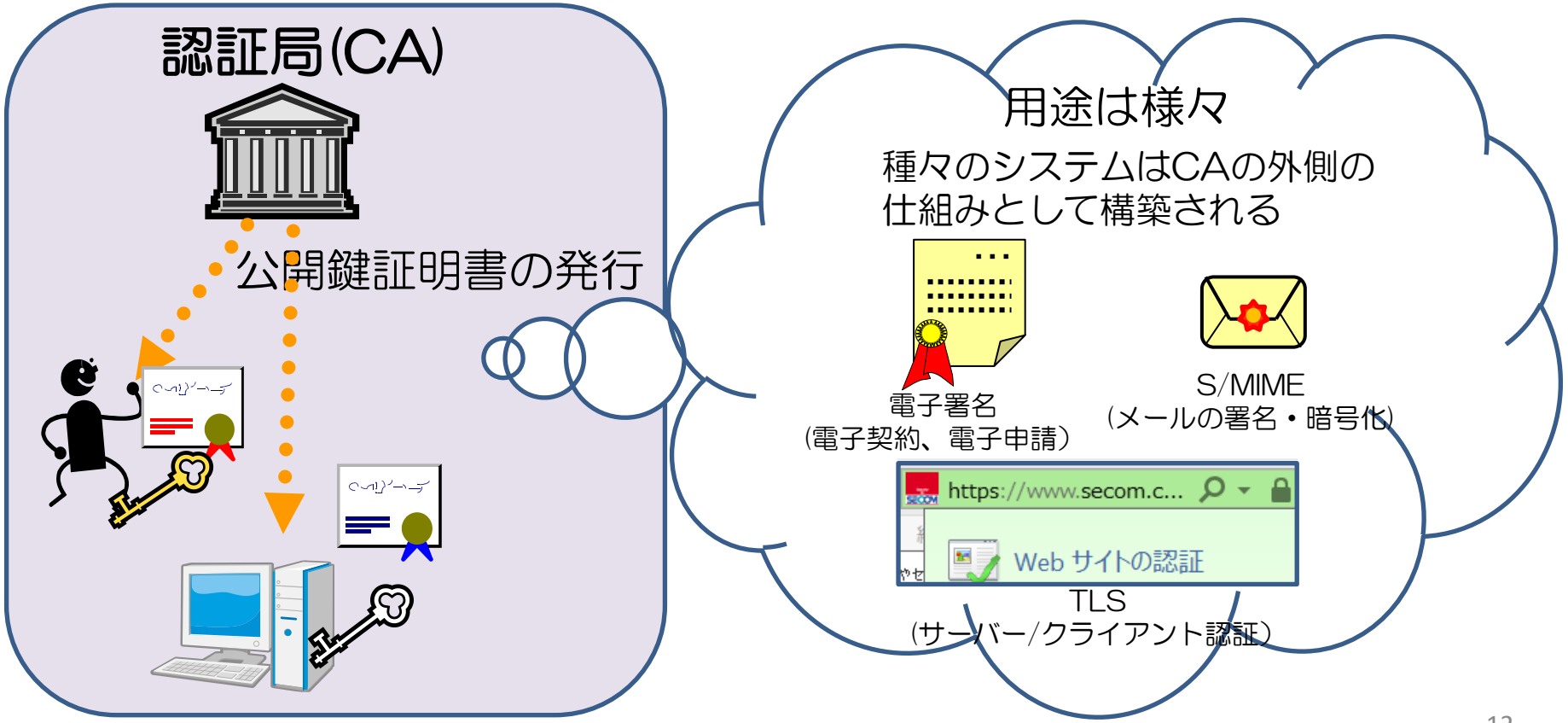
- システムへのアクセスコントロールとログ保全
- 暗号技術応用
  - PKIによるデジタル署名
  - タイムスタンプ技術

PKI(Public Key Infrastructure)って？

セコム IS研究所 Intelligent Systems Laboratory

非常にざっくりと乱暴に言ってしまえば…
信頼される第三者機関がエンティティ(人、組織、デバイス、etc.)の存在(公開鍵との紐づけ)を証明する仕組み

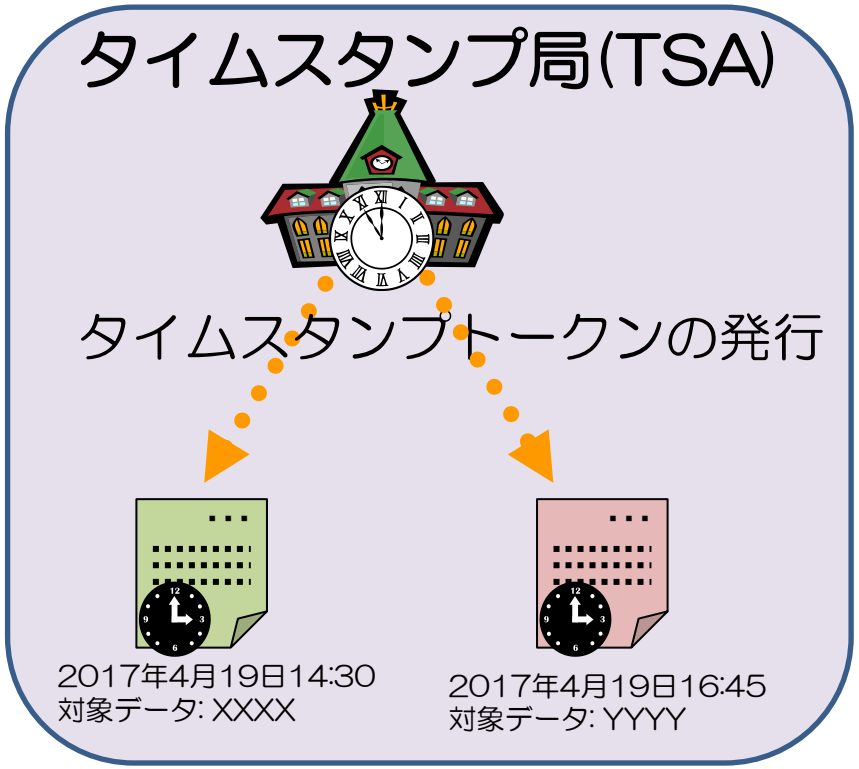
第三者機関（CA）を信頼するモデル



タイムスタンプ技術って？

非常にざっくりと乱暴に言ってしまえば…
信頼される第三者機関がデータに対する時刻証明（存在証明）を行うもの

データに改ざんがないこと、当時存在したことを証明する



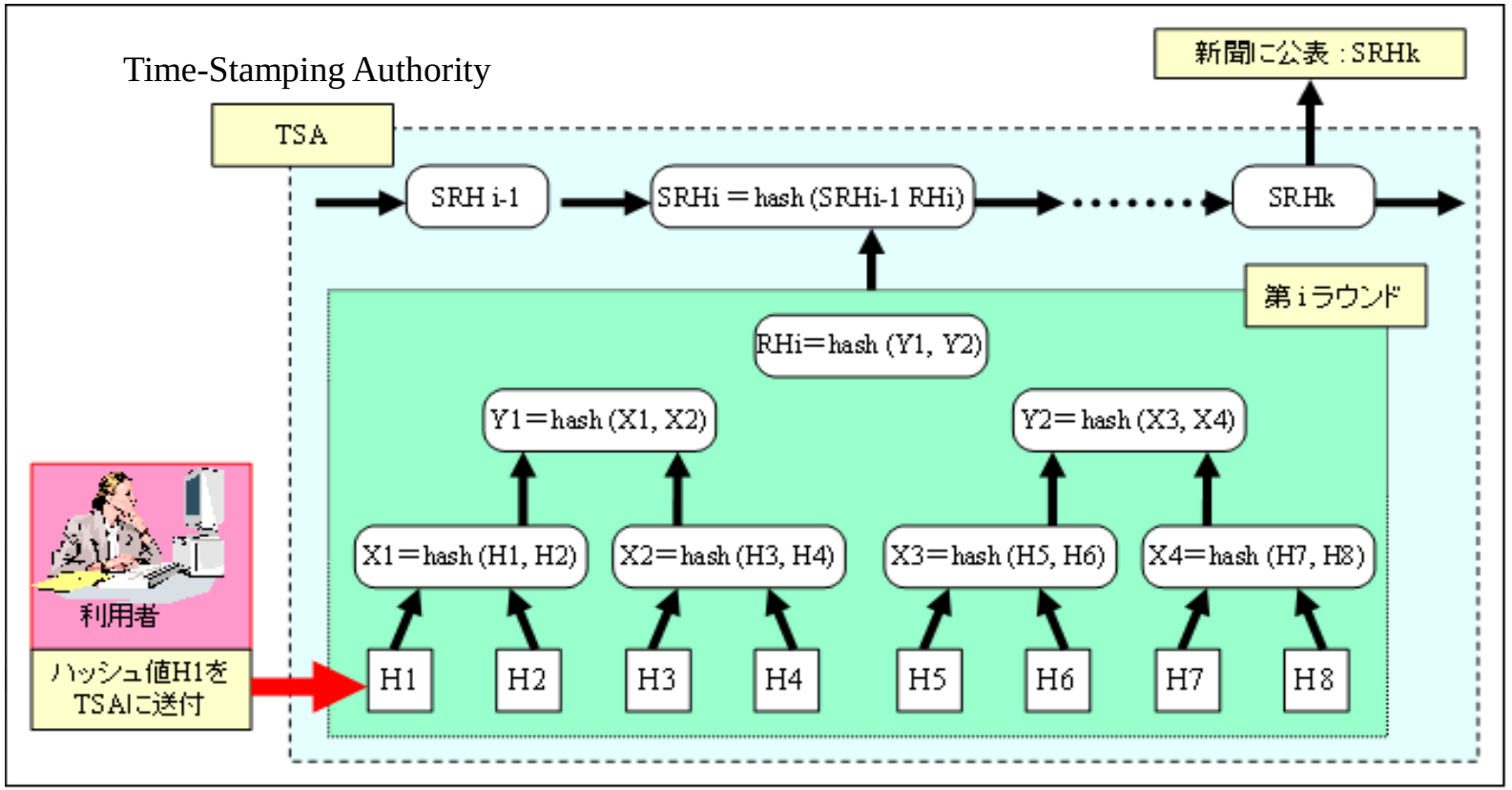
- 日本では2005年に事業者の認定制度が始まった。
  (http://www.dekyo.or.jp/tb/index.html)
- タイムスタンプ生成の仕組みとして、
  PKIベースのもの(RFC 3161)や、
  ハッシュツリーを使うもの(ISO/IEC 18014-3, etc.)
  等のバリエーションがある。

【参考】
- タイムスタンプ・プロトコルに関する技術調査
  (IPA, 2004年2月)
- タイムスタンプ技術に関する調査報告書
  (IPA, 2004年4月)

リンキング方式のタイムスタンプ

セコム IS 研究所
Intelligent Systems Laboratory

標準規格：ISO/IEC 18014-3



https://www.ipa.go.jp/security/pki/093.html より

その他、ハッシュツリーを使う仕組みとして、Surety社やGuardtime社の実装や
Evidence Record Syntax（RFC 4998, RFC 6283）がある。

従来技術とブロックチェーンの違いとは？

セコムIS研究所
Intelligent Systems Laboratory

- データの真正性を証明する機能を提供する機関や組織の存在
  - パーミッションレス型は特定の機関や組織による管理ではなく分散したノードを仮定
- 真正性の検証
  - ブロックチェーンの場合は人手を介さない機械的な処理が中心。データだけで検証できることが求められる。
- 匿名性(仮名性) vs エンティティの証明
  - 複数のノードでデータを共有するブロックチェーンでは顕著となる