セコム IS研究所
Intelligent Systems Laboratory

PKI day 2017
ブロックチェーンとは何か？

2017年4月19日

セコム株式会社 IS研究所
主任研究員
(JNSA電子署名WGサブリーダー)
佐藤　雅史

セコムIS研究所
Intelligent Systems Laboratory

この講演では…

- 30分でブロックチェーンを理解する？
  かなり無茶！
- パネルディスカッションで必要な
  キーワードを共有することを目指します
  - ブロックチェーン？スマートコントラクト？
  - PKI？
    etc.

ブロックチェーンって何？

セコム IS 研究所
Intelligent Systems Laboratory

正直なところ、一言で表しにくい…

よくあるイメージ
- 非中央集権的？(or 分散？)で、
- データの真正性を担保して？
- データを共有する？

ブロックチェーン？分散台帳？

パブリック？プライベート？

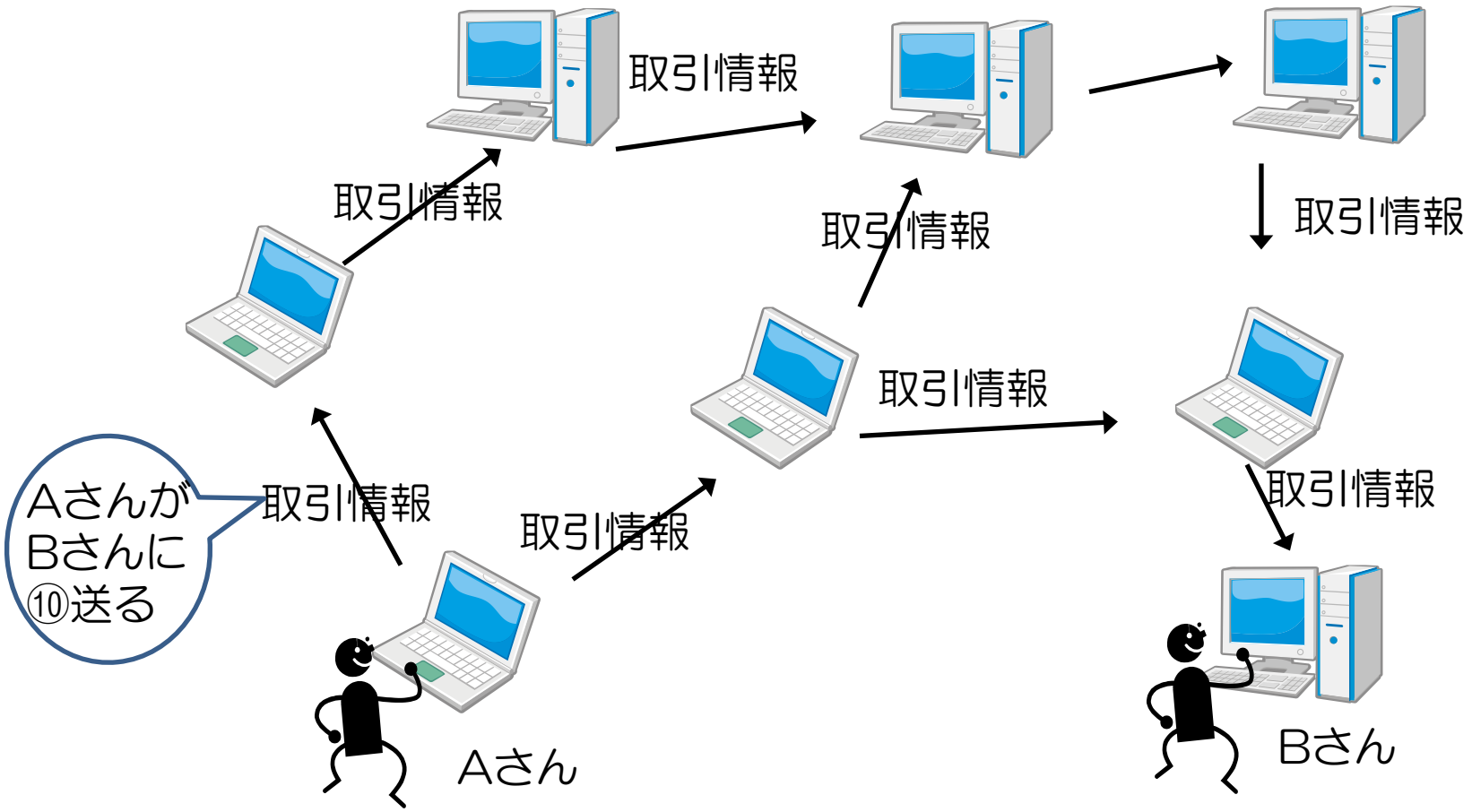
Permissonless? Permissioned?

- 定義も色々
  - 英国政府レポート、JBA、etc.
- 実装も色々
  - Bitcoin/OpenAssets, Ethereum, Hyperledger(fabric, iroha, sawtooth lake), R3 Corda, Ripple, etc.
- ISO/TC 307(Blockchain and electronic distributed ledger technologies)で定義の議論が始まりそうではあるが…

ブロックチェーン/分散台帳でしたい事

セコム IS研究所
Intelligent Systems Laboratory

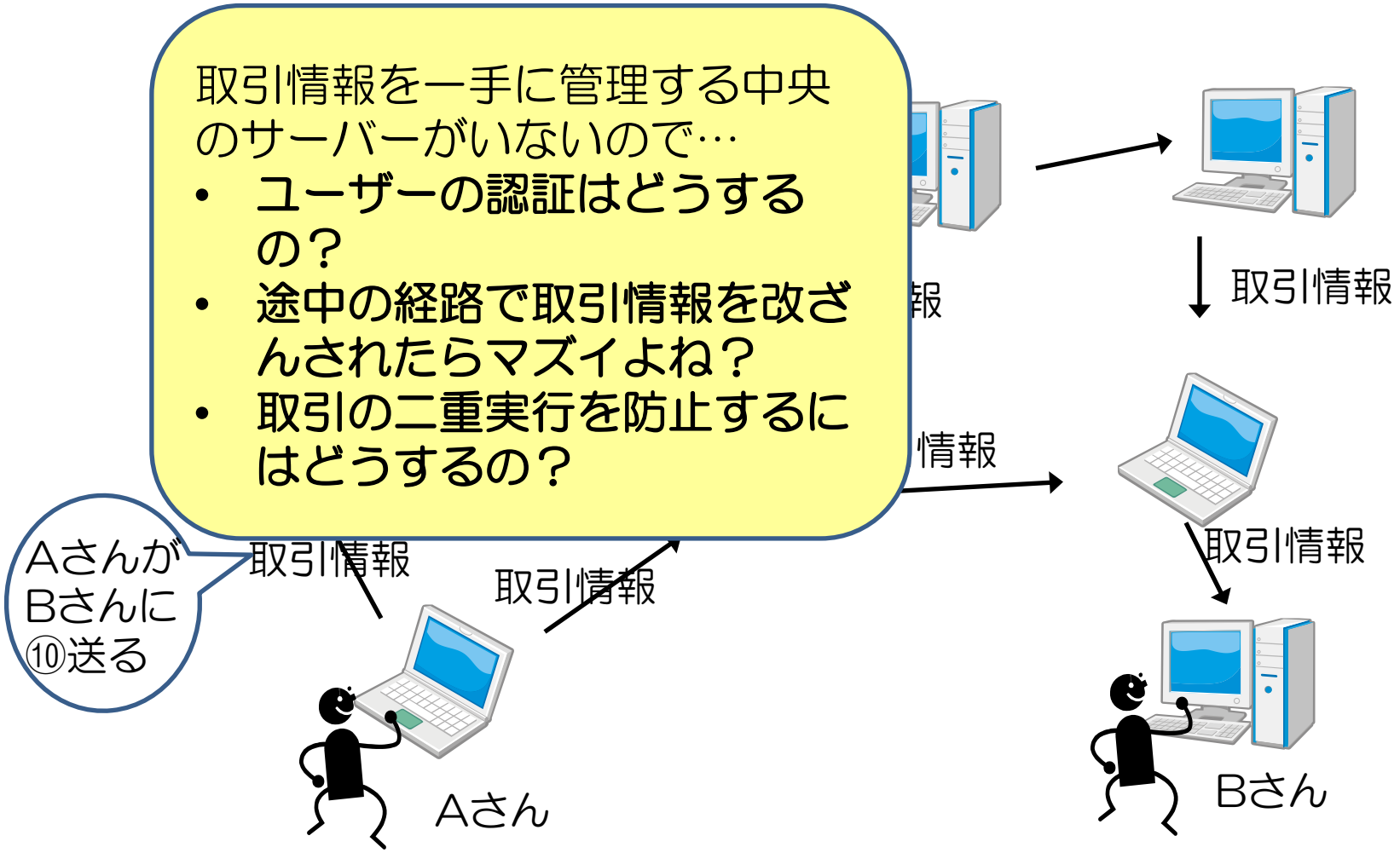
特定の中央のサーバーを介さずに、取引（送金、資産移転等）を実行したい



ブロックチェーン/分散台帳でしたい事

セコムIS研究所
Intelligent Systems Laboratory

特定の中央のサーバーを介さずに、取引（送金、資産移転等）を実行したい



ブロックチェーン/分散台帳でしたい事

セコムIS研究所
Intelligent Systems Laboratory

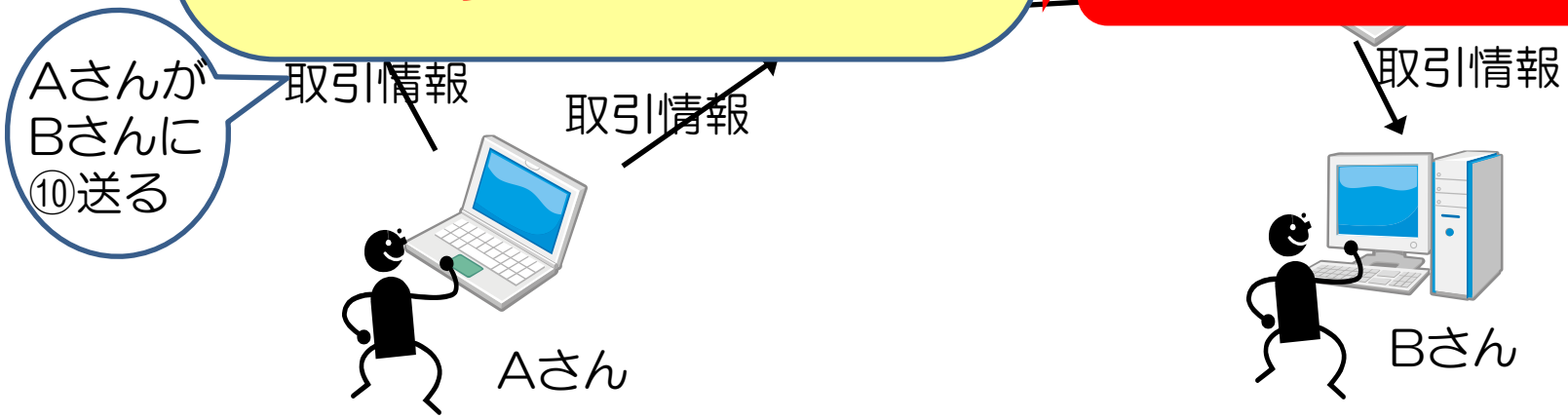
特定の中央のサーバーを介さずに、取引（送金、資産移転等）を実行したい

取引情報を一手に管理する中央のサーバーがいないので…

- ユーザーの認証はどうするの？
- 途中の経路で取引情報を改ざんされたらマズイよね？
- 取引の二重実行を防止するにはどうするの？

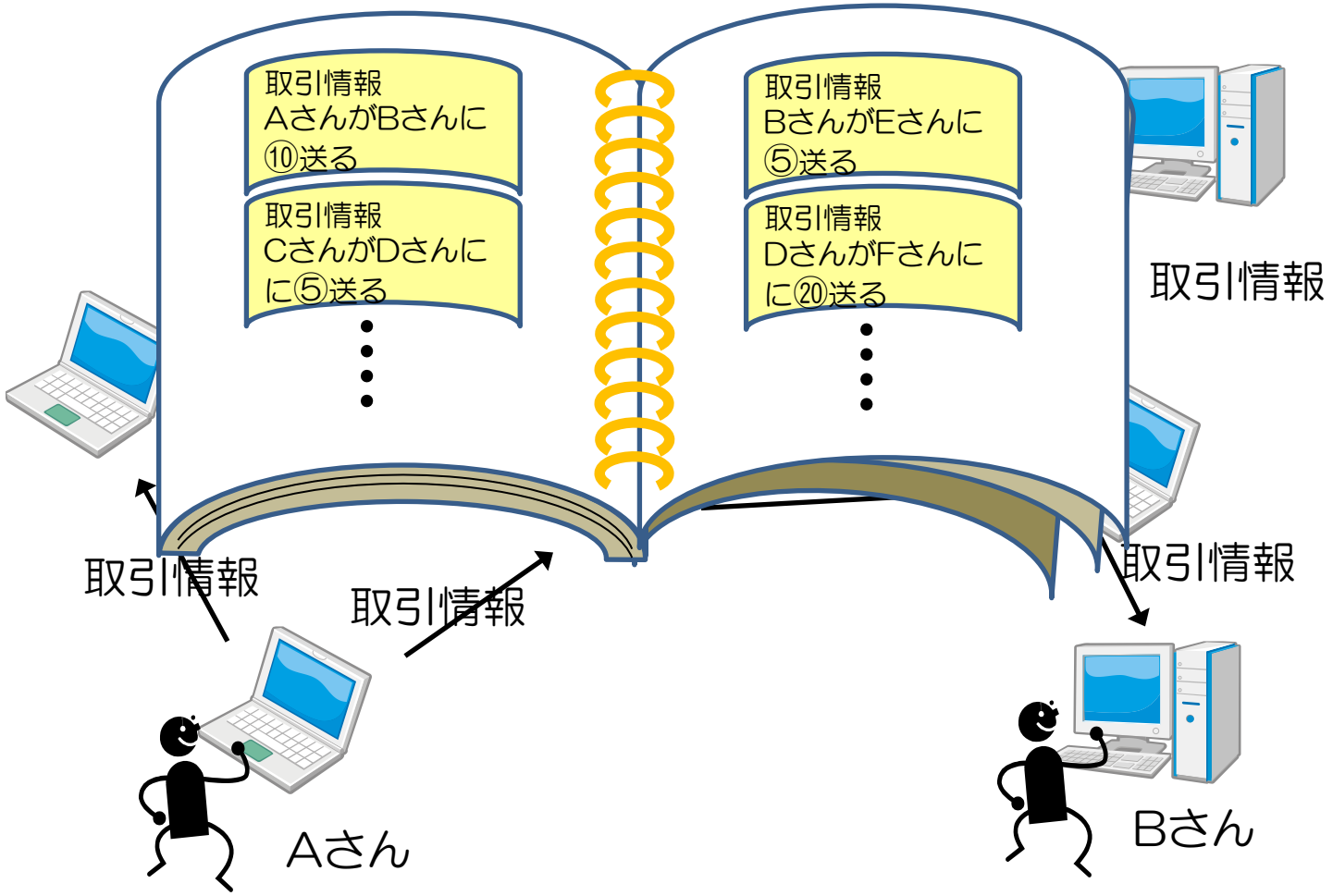
ユーザーが署名鍵を管理してデジタル署名

台帳の生成と共有のメカニズム
（コンセンサスアルゴリズムと呼ばれている）



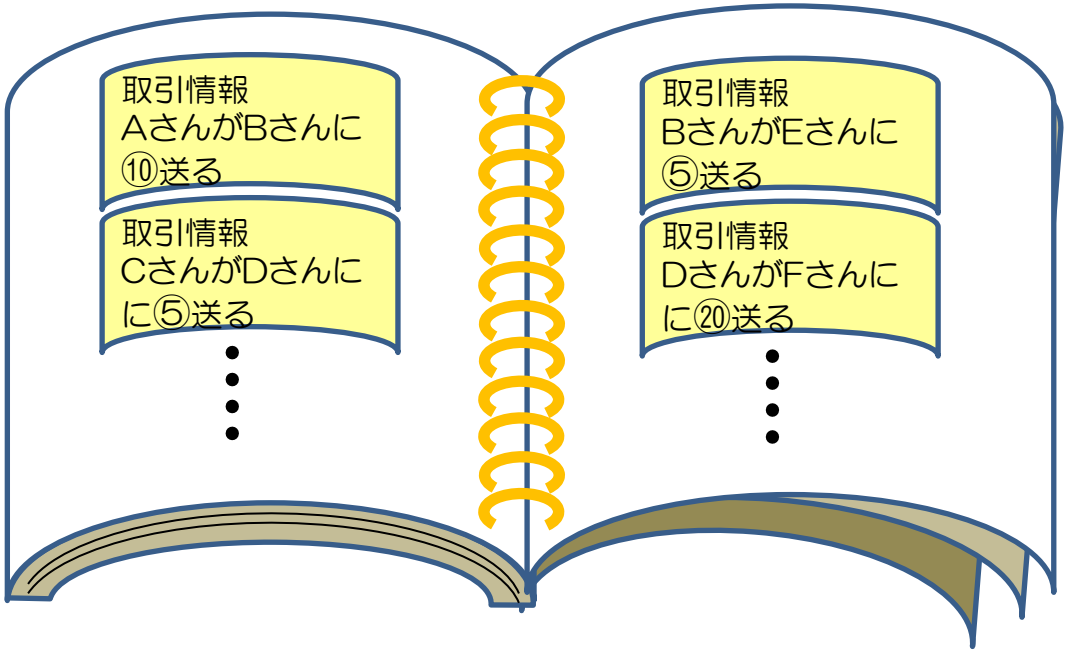
台帳の生成と共有

矛盾なく取引を実行するために、
参加者で一意な取引情報の履歴（= 台帳）を共有する（ことをめざす）



台帳の生成と共有に必要な要素は？

セコムIS研究所
Intelligent Systems Laboratory

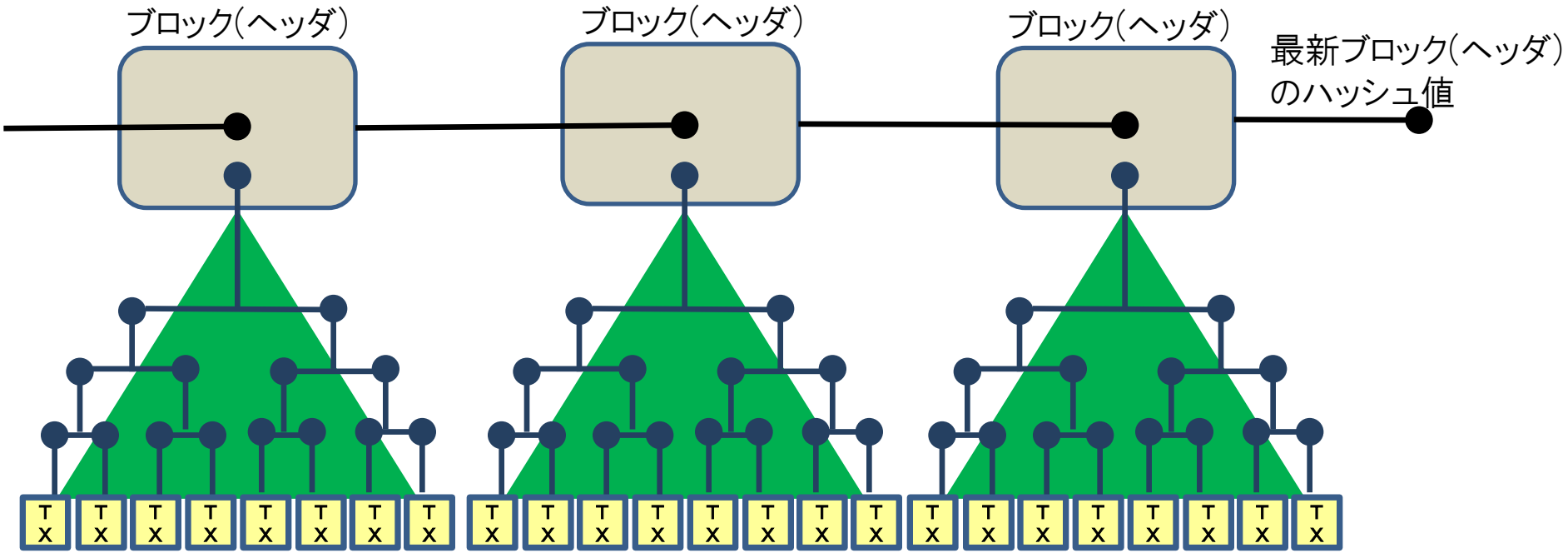


- 一度、台帳に載った取引情報は改ざん（順序の入れ替えなど）されないこと
  - ➢ ハッシュ値の連鎖などによる存在証明を行う
- 台帳や、その各ページ（＝ブロック）の作成が特定の者に支配されない（偏らない）こと
  - ➢ ブロック生成者の決定や、載せる取引情報の決め方（コンセンサスアルゴリズムと呼ばれている）
    - 仕組みはネットワーク参加方法により前提が異なる

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）



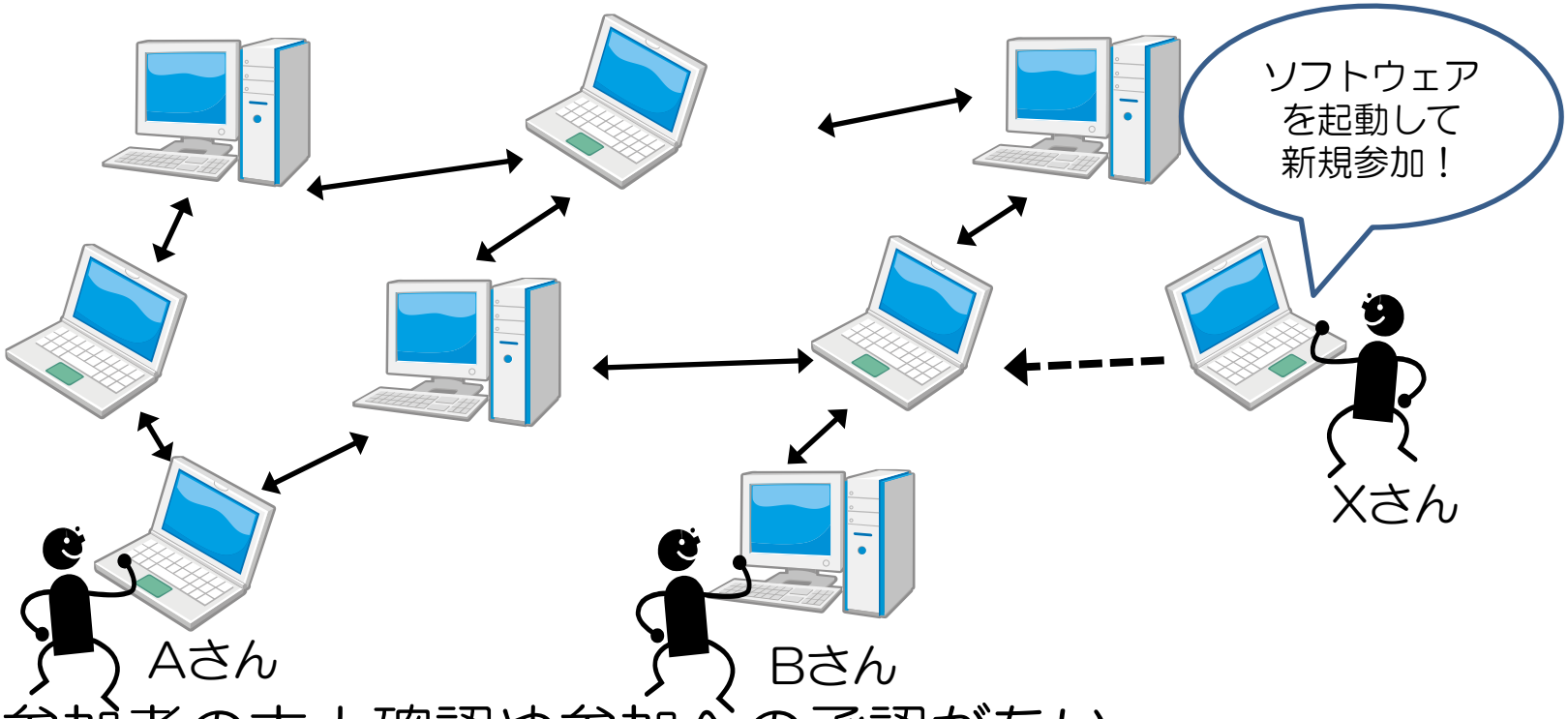
T X 取引情報のデータ

ある周期的なタイミングで各ブロックが生成される

パブリックブロックチェーン？ (permissionless?)

セコムIS研究所 Intelligent Systems Laboratory

ネットワークへの参加/離脱が自由な世界(Bitcoin, Ethereum, etc.)

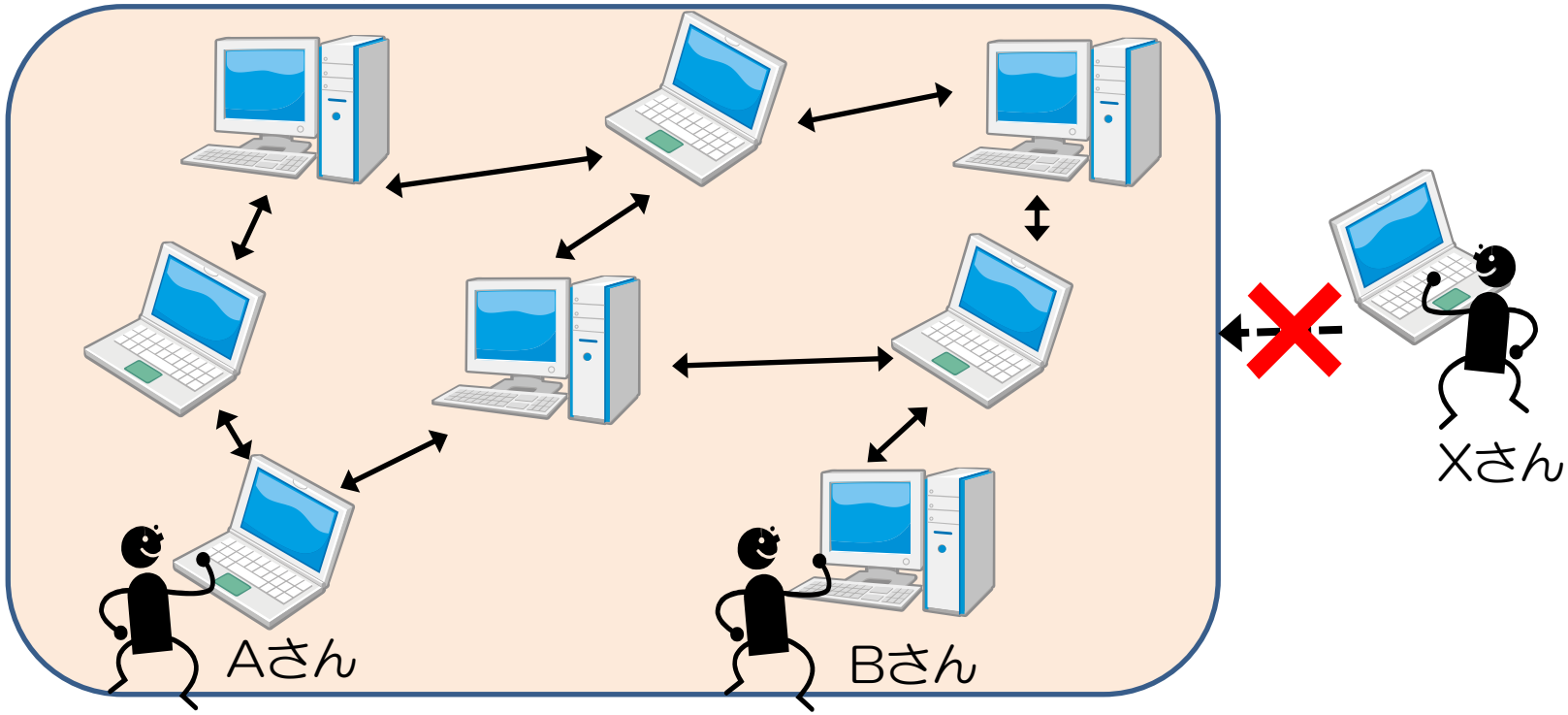


- 参加者の本人確認や参加への承認がない
  - デジタル署名の鍵ペアを自身で作る程度
- 誰が参加しているか分からないことを前提とした設計
  - 競争原理に基づくブロック生成アルゴリズム (proof of work, proof of stake, etc.)など

プライベート/コンソーシアム ブロックチェーン？ (permissioned?)

セコム IS研究所 Intelligent Systems Laboratory

ある組織や業界、用途で閉じた世界



- 参加への承認が必要（身元や資格の確認など）
- ある程度のガバナンスは前提としうる？
  - 参加者間での責任や役割の分担（ブロック/台帳の生成や検証など）
  - 障害対策としてのコンセンサスアルゴリズム？

セコムIS研究所
Intelligent Systems Laboratory

で、何に使うんでしょう？

（暗号通貨や送金、決済などの議論はありますが…）

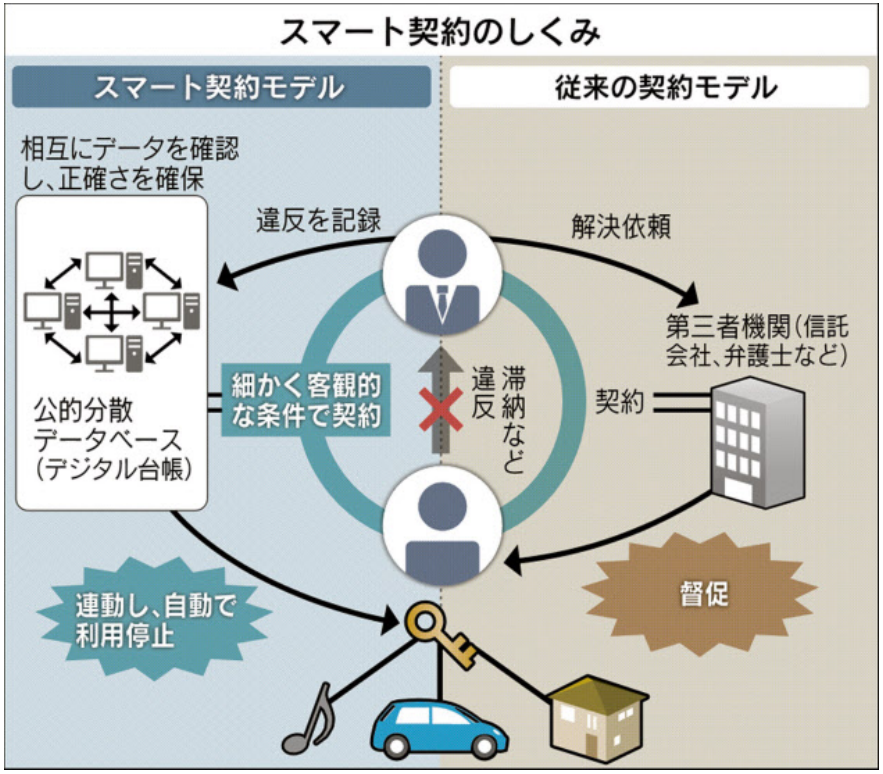
スマートコントラクト？ (smart contract)

セコムIS研究所 Intelligent Systems Laboratory

- ブロックチェーンと一緒に語られることもあるが、もともとは独立した概念
- スマートな契約(コントラクト)の実行
  - コンピュータ上で自動的に検証され履行される契約(DRMなどもその一種)
  - Nick Szabo氏が1994年に提唱したとされる
- ブロックチェーンの文脈では、取引情報の実行だけでなく小さなプログラムコードも実行できるというもの
- ブロックチェーンを基盤としてスマートコントラクトを実現しようという風潮？

スマートコントラクトの例?

セコムIS研究所
Intelligent Systems Laboratory



スマート契約で可能になる有力な新サービス

業界	予想される新たなサービス
通販	商品が届いた瞬間に支払えることで、信託機関の仲介が不要に
不動産	賃貸住宅の入退室の厳密な管理が可能に。個人の自宅の貸し出しもしやすく
自動車	遠隔操作できるカギと連動し、ローンを滞納すれば開かなくなる仕組みが可能に
音楽	コンテンツの購入者を登録。個別の口座に暗号のカギを割り振り、その口座の持ち主のみが音楽配信を受けられるサービス。コピー、海賊版問題の解決策に
選挙	有権者の登録、認証が低コストで可能に
遺言	信託サービスなしでも高い信頼性をもって記録でき、随時更新も可能
建設	工程管理を細かく設定し、それに合わせた支払いも可能に

日経産業新聞 2014年12月15日付”金融紛争なくなる？プログラムが契約管理する未来　「スマート契約」の衝撃”より
http://www.nikkei.com/article/DGXMZO80840720S4A211C1X13000/

スマートコントラクトによる自動化の例？

セコムIS研究所
Intelligent Systems Laboratory

InsureETH

http://dapps.oraclize.it/insureth
http://mkvd.s3.amazonaws.com/apps/InsurEth.pdf

Dynamis

http://www.dynamisapp.com/

この例で実現しようとするものは？

- 保険金や返金などの支払い条件をコード化した自動実行
  - 外部ソースからの情報（例えば飛行機の遅延やキャンセル等の状態）と連動して実行される
  - 人的ミスの排除、支払い判断の不公正さの解消
- 受取人を台帳に記載・共有して詐欺対策など
- 保険業者の透明性確保（支払い能力に関する情報など）

ブロックチェーン/分散台帳のユースケースって？？？

セコム IS研究所
Intelligent Systems Laboratory

ブロックチェーン技術の展開が有望な事例とその市場規模

• 幅広い分野へ影響を与える可能性がある

経済産業省 「ブロックチェーン技術を活用したサービスに関する国内外動向調査報告書」（2016/4/28）
http://www.meti.go.jp/press/2016/04/20160428003/20160428003.html

セコムIS研究所
Intelligent Systems Laboratory

電子契約、保険、融資、電子カルテ、
資金移転、サプライチェーン、電子申請、
登記、オークション、etc.

あれ？デジャヴ？

ECOM(電子商取引推進協議会) 報告書
https://www.jipdec.or.jp/library/archives_ecom.html

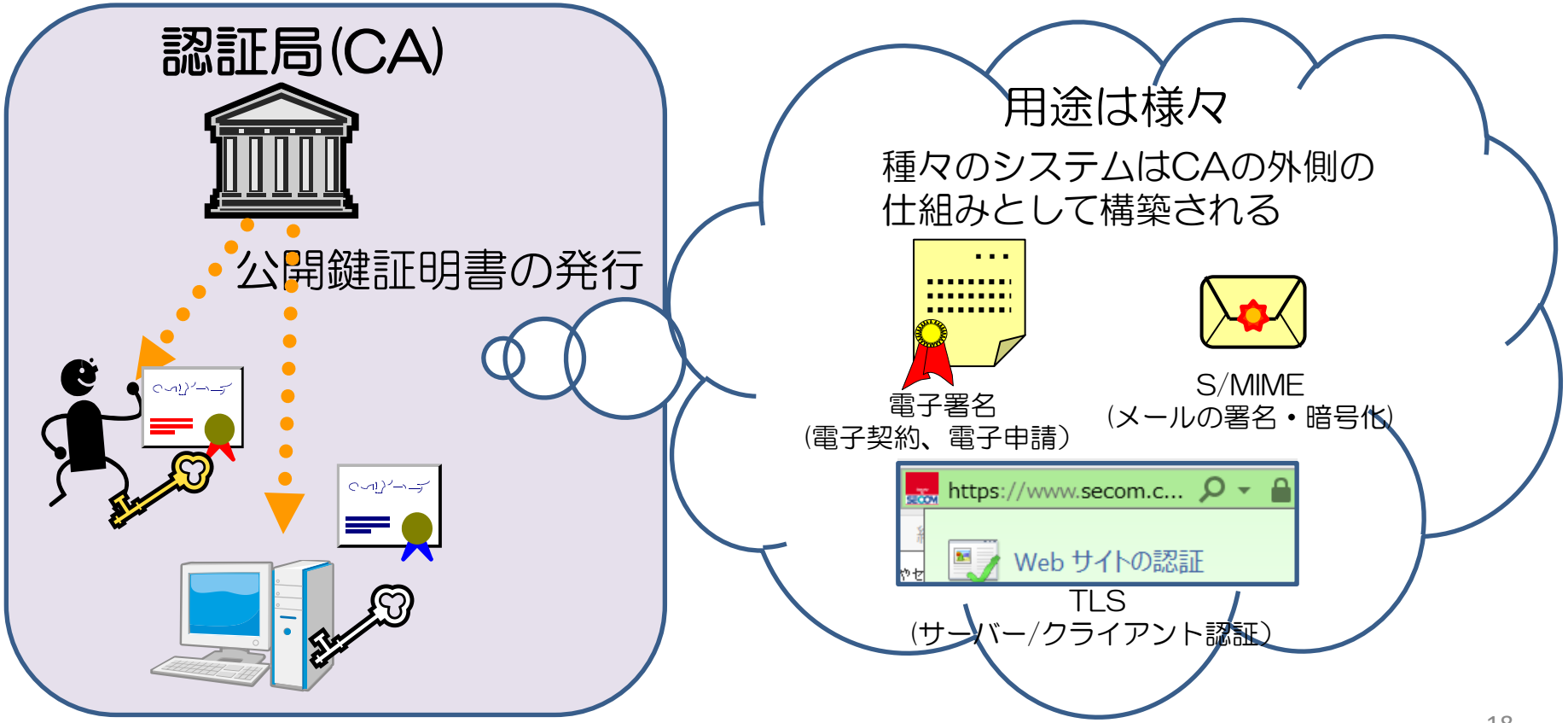
- 平成13年度 電子署名・認証の利用状況調査
- 平成15年度ＥＣ技術基盤の相互運用性に関する調査研究事業（電子署名生成・検証システムのセキュリティ環境の標準化等調査）署名ポリシー調査報告書［経産省委託調査］
- 平成15年度ＥＣ技術基盤の相互運用性に関する調査研究事業（取引相手先の属性認証技術等の調査）ＳＡＭＬ利用検討報告書［経産省委託調査］

PKI(Public Key Infrastructure)って、なんだっけ？

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

個々のエンティティ同士ではなく、第三者機関（CA）を信頼するモデル

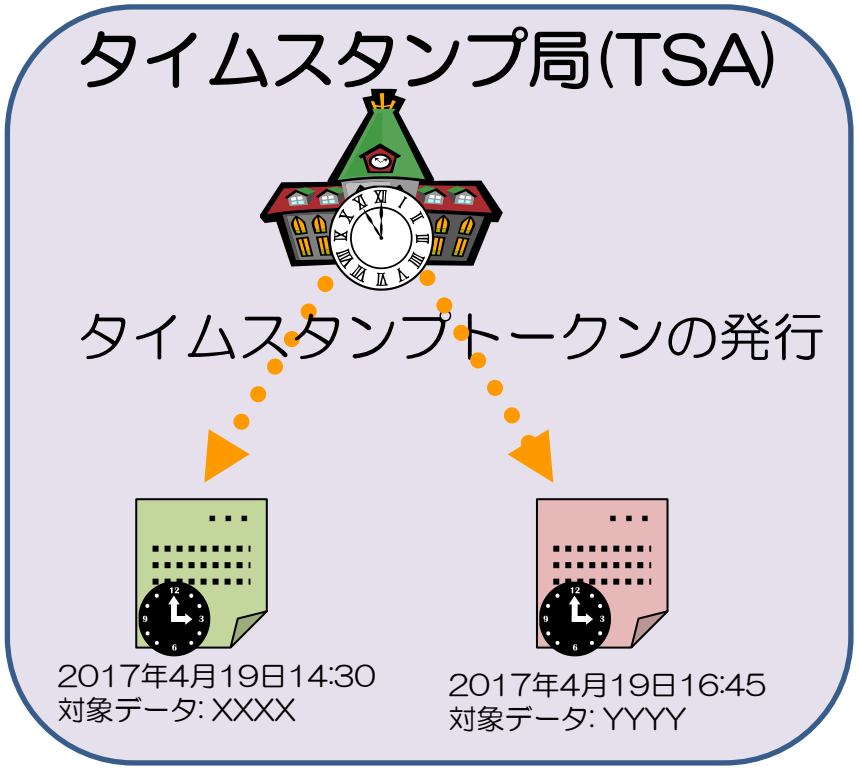


タイムスタンプ技術って、なんだっけ？

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



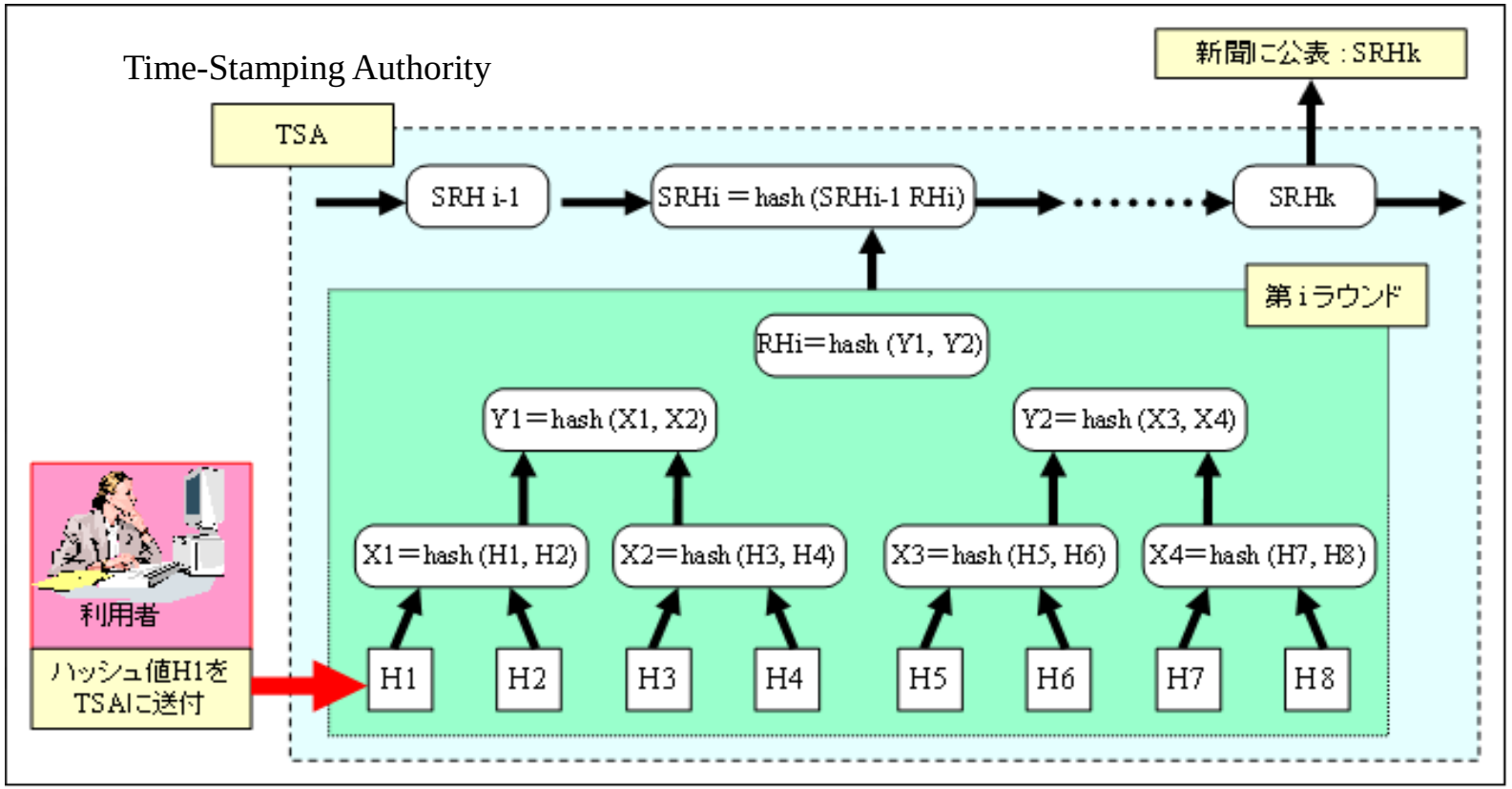
- 日本では2005年に事業者の認定制度が始まった。
  (http://www.dekyo.or.jp/tb/index.html)
- タイムスタンプ生成の仕組みとして、
  PKIベースのもの(RFC 3161)や、
  ハッシュツリーを使うもの(ISO/IEC 18014-3, etc.)
  等のバリエーションがある。

【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)

参考：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。

ブロックチェーンと従来技術（PKI＆タイムスタンプ）の違いって？

セコムIS研究所
Intelligent Systems Laboratory

ブロックチェーンに期待されている
要素の例

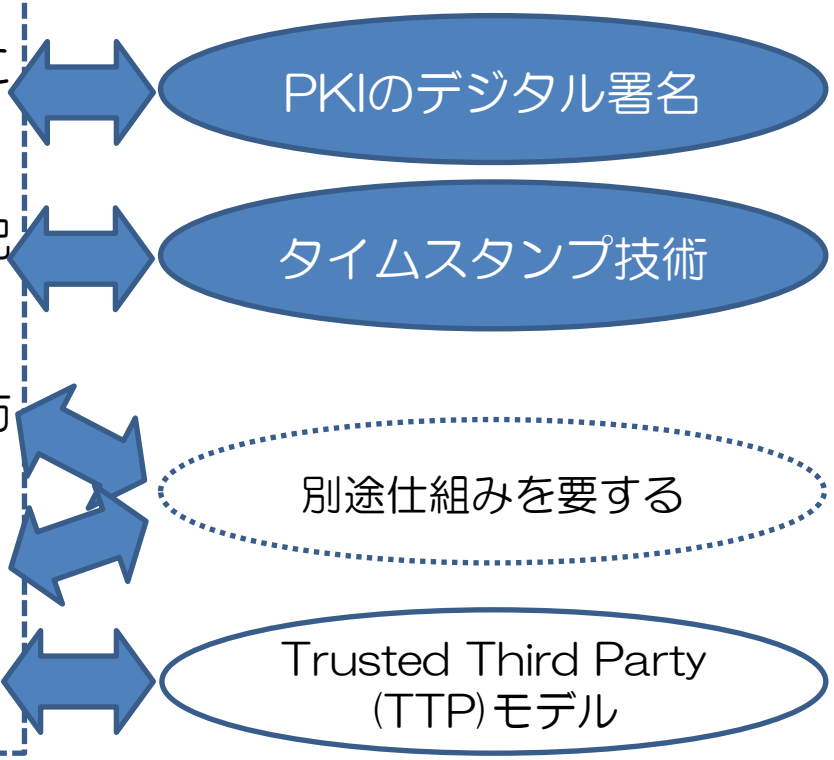
① データ（取引情報など）の作成者以外によるデータ改ざんの困難性

② データが過去に存在したことの証明（記録の順序等に対する改ざん困難性）

③ データ処理の整合化（例：二重実行の防止）

④ データの保存や共有

⑤ P2P/分散/非中央集権的モデル



適用しようとする利用場面ではどの要素が重要か？

ブロックチェーンとPKIのスコープとは？
～処理フロー（電子契約/電子申請等のイメージ）の観点で～

セコムIS研究所
Intelligent Systems Laboratory

	パブリック ブロックチェーン	プライベート/コンソーシアム ブロックチェーン	PKI （署名+タイムスタンプ）
⓪　利用者の登録（利用者の本人確認と署名鍵との紐づけ）	ブロックチェーン上の仕組みは持たない	仕組みが提供されるものもある	認証局による証明書発行
①　データの作成（＋デジタル署名）と送信	トランザクション(取引情報)生成の仕組みが含まれている	左に同じ	各アプリによる。署名データに関する標準規格がある。
②　受信側でのデータの検証	トランザクション(取引情報)検証の仕組みが含まれている	左に同じ	各アプリによる。署名データに関する標準規格がある。
③　データに応じた処理の実行	処理内容によってはチェーン外の仕組みが必要となる	左に同じ	各アプリによって提供される
④　データの保存	台帳生成と共有の仕組みが含まれている	左に同じ	各アプリによる。署名の保存に関する標準規格がある。
⑤　保存データの事後検証	検証は可能であるが、検証処理のための実装は別途必要か	左に同じ	各アプリによる。署名の保存に関する標準規格がある。

アプリ側等で構築が必要なもの
カバーしようとしている機能

※厳密な分類ではありません（利用目的や実装によって差異があります）

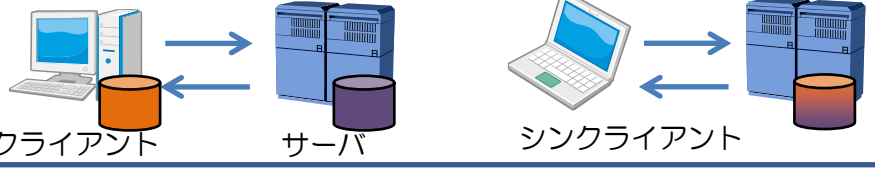
データ・システム間連携の新たな時代を幕開けできるか？

セコム IS研究所
Intelligent Systems Laboratory

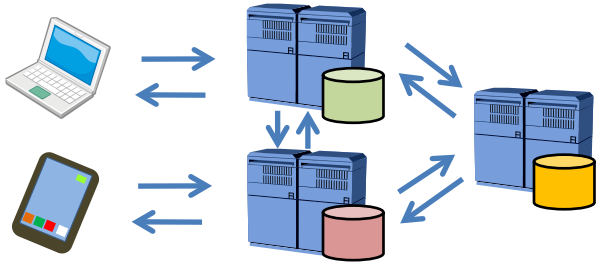
スタンドアロン時代

個別のPCにあるデータと
アプリで完結していた世界

クラサバ時代



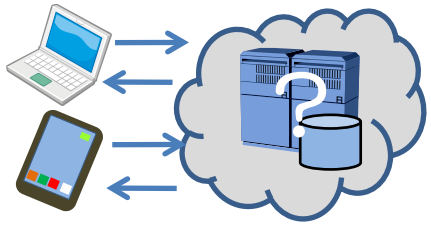
データ・機能連携時代



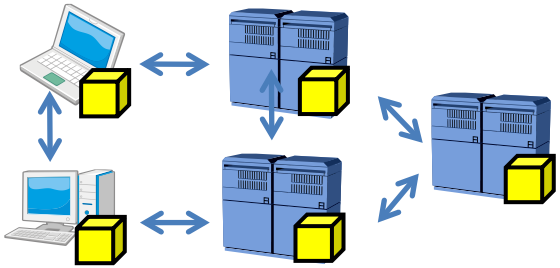
ディレクトリサービス、
Webサービス/SOA、
ID連携(SAML,OpenID)、
OAuth等々

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



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…

ブロックチェーンに期待されているものは何でしょう？（期待は人それぞれ？）

セコム IS研究所 Intelligent Systems Laboratory

- 暗号通貨？
- データ改ざんの困難性？データの存在証明？
- 複数のサーバ/組織間でのデータの共有？
- データの公開や共有を前提とした透明性？
- 非中央集権的モデル？
  - 従来の中央機関型サービスに対する反動？
  - 何に対して非中央集権を求めるのか？
- 非中央集権というより分散や冗長性？耐障害性？
- ローコストへの期待？
- 何でも良いので凝り固まった既存のシステムから脱却したい？

セコムIS研究所
Intelligent Systems Laboratory

パネルディスカッションに続く