ソフトウェア事業協同組合セミナー

 1

ブロックチェーンの活用展開に向けて

ー基本的仕組みの理解から応用パターンの把握までー

2019年9月27日
才所敏明
（株）IT企画・代表取締役社長
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

（注）本セミナーの資料全体は、セミナー終了後1週間程度で当社Webサイトに登録し、
同時にFacebookでも登録URLを公開します。

 2

自己紹介

1966年　東京大学・工学部・計数工学科・数理コース
1970年　東芝入社
　社内計算機利用環境企画・構築・活用指導・支援
　　スーパコン～PCを利用した技術開発環境構築・活用推進（1969UNIX）
　　インターネットの企業活動への活用推進
　　（1974Internet　1984JUNET　1987InetClub　1992商用サービス）
　情報セキュリティ研究開発企画・推進、事業支援（1995）
　　暗号・認証技術等の事業への活用推進　（1999IoT）
2007年　（株）IT企画設立
　事業支援活動（顧問・相談役）：2社（日、米）
　大学教育活動（情報セキュリティ）：九大、慶応
　研究開発活動（研究員）：中央大学研究開発機構
　　暗号・認証、秘密分散、バイオメトリクス、電子メールセキュリティ、
　　IoTシステムセキュリティ、FinTech（仮想通貨、ブロックチェーン）
　　ビッグデータ、AI

本日のご説明内容

［1］暗号技術の発展の歴史と
現代暗号の基本的仕組み

［2］ブロックチェーンの特徴および
暗号技術が支えるブロックチェーンの仕組み

［3］ブロックチェーンの分類とそれぞれの特徴

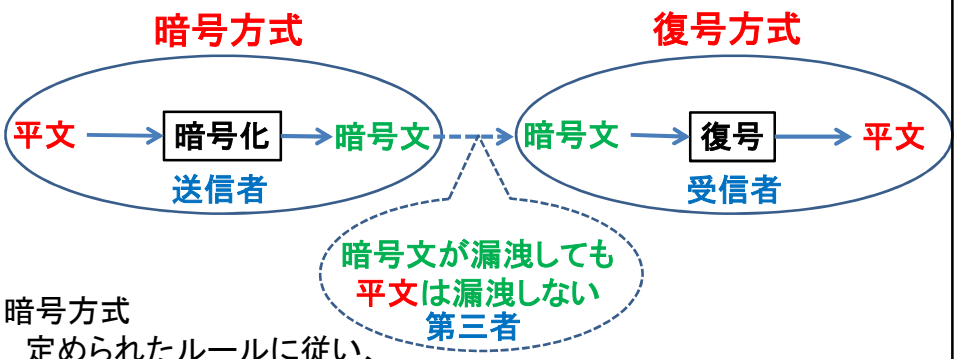
［4］ブロックチェーンの応用分野および
活用に向けた取組み

［5］ブロックチェーンの技術・応用に関する最新動向

［1］

暗号技術の発展の歴史
と
現代暗号の基本的仕組み

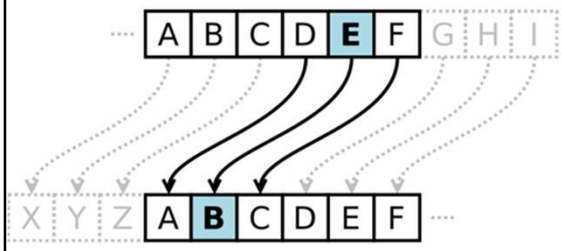
暗号技術とは

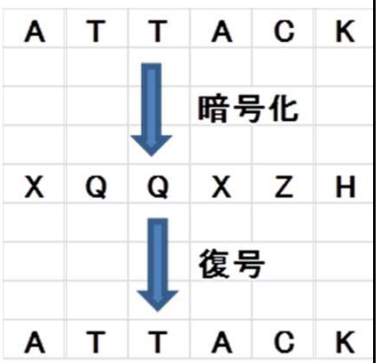


暗号方式
　定められたルールに従い、
　内容が分かる文章（平文）を、内容の分からない文章（暗号文）へ
　変換する方式
復号方式
　暗号文を元の平文へ戻す方式（それぞれの暗号方式に対応）
暗号技術
　平文を暗号化でき、また復号できる、暗号方式および復号方式の対

暗号技術発展の歴史　古代暗号

（例1）シーザー暗号（紀元前100年頃）





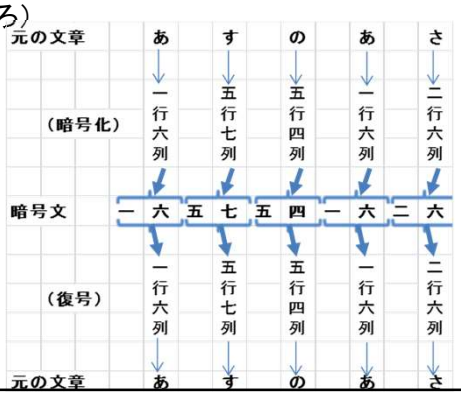
暗号技術発展の歴史　古典暗号

外交活動の活発化による暗号の普及期へ

（例1）ノーメンクラター暗号、16世紀ごろ（スコットランド女王メアリ）
イングランド女王エリザベス暗殺をたくらみ仲間と暗号通信
側近ウオルシンガムの部下が解読、証拠確保、関係者処刑

（例2）上杉暗号（戦国時代、16世紀ごろ）

七	六	五	四	三	二	一	
ゑ	あ	や	ら	よ	ち	い	一
ひ	さ	ま	む	た	り	ろ	二
も	き	け	う	れ	ぬ	は	三
せ	ゆ	ふ	ゐ	そ	る	に	四
す	め	こ	の	つ	を	ほ	五
ん	み	え	お	ね	わ	へ	六
	し	て	く	な	か	と	七



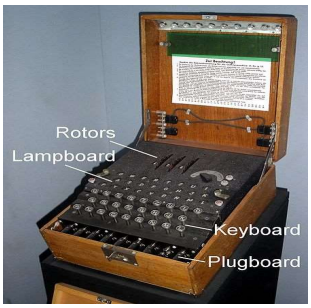
暗号技術発展の歴史　近代暗号

暗号の作成・解読は、手作業から機械へ

（例1）エニグマ暗号（第2次世界大戦でドイツ使用）

英国の数学者アラン・チューリング
のチームが解読
＜映画「イミテーションゲーム/
エニグマと天才数学者の秘密」＞

（チューリング賞：コンピュータ科学の
ノーベル賞）



エニグマ暗号機

（例2）パープル暗号（第2次世界大戦で外務省が使用）
ニューヨーク総領事館から句読点コードが盗まれ、米国が解読

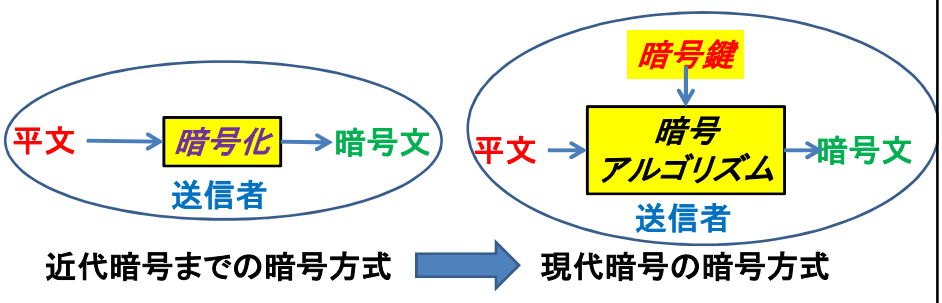
暗号技術発展の歴史　現代暗号
暗号の作成・解読は、計算機利用へ

計算機開発の歴史：1946ENIAC、暗号専用機としては1943コロッサス

現代暗号の特徴：コンピュータ/ネットワークの発展により、
軍事的・政治的利用から、産業活動・生活活動での利用へ
多くのベンダによる開発競争、相互運用性の保証
➔暗号化/復号ソフト開発に必要な暗号方式の公開が必要に

従来は“暗号方式を公開しない”ことで安全性を確保
➔従来とは異なる仕組みで
暗号文の安全性を確保することが必要に！

暗号技術発展の歴史　現代暗号
暗号方式を暗号アルゴリズムと暗号鍵に分離

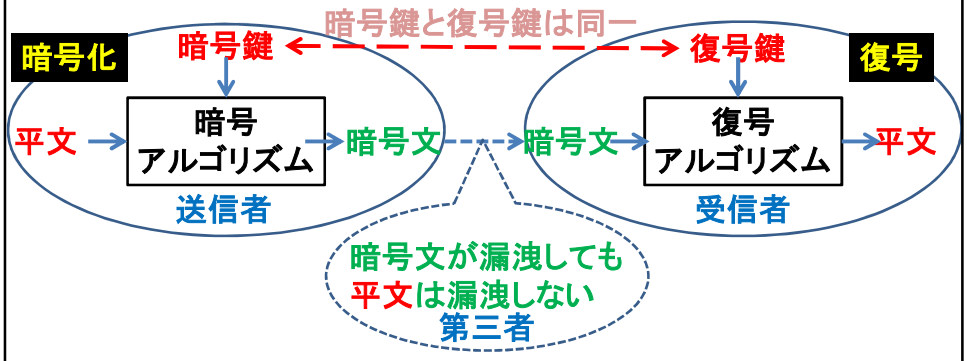


近代暗号までの暗号方式 ⇒ **現代暗号の暗号方式**

現代暗号は、暗号アルゴリズムを公開しても
暗号鍵を公開しなければ安全性が確保できるよう、
暗号アルゴリズムが設計されている

現代暗号　共通鍵暗号方式

暗号鍵と復号鍵が同一



共通鍵暗号方式の課題

あらかじめ、通信相手と暗号鍵（復号鍵）を共有しておく必要がある

現代暗号　共通鍵暗号方式

代表的な暗号方式と活用事例

米国

DES：鍵長56ビット、1976年米国連邦標準、2005年標準から除外

AES：鍵長128、192、256ビット、2001年米国連邦標準

日本

NTT：1985年FEAL（64ビット）

三菱：1995年MISTY（128ビット）

東芝：1999年Triplo（128ビット）、2003年Hierocrypt-3（128ビット）

2003年Camellia（128ビット）

日本での活用事例

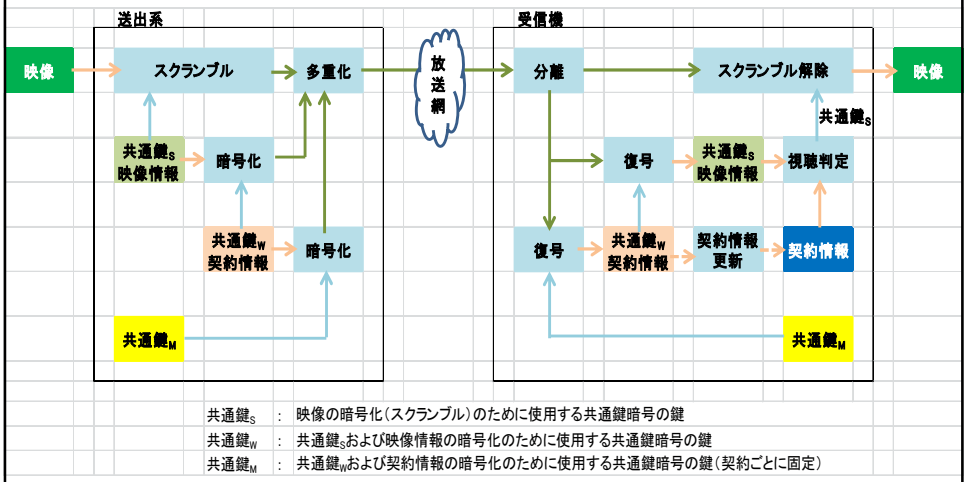
有料放送（1991年）：限定受信システム
（CAS：Conditional Access System）

ノンストップ料金収受（1997年）：高速道路料金収受システム
（ETC：Electronic Toll Collection System）、

 13

限定受信システム

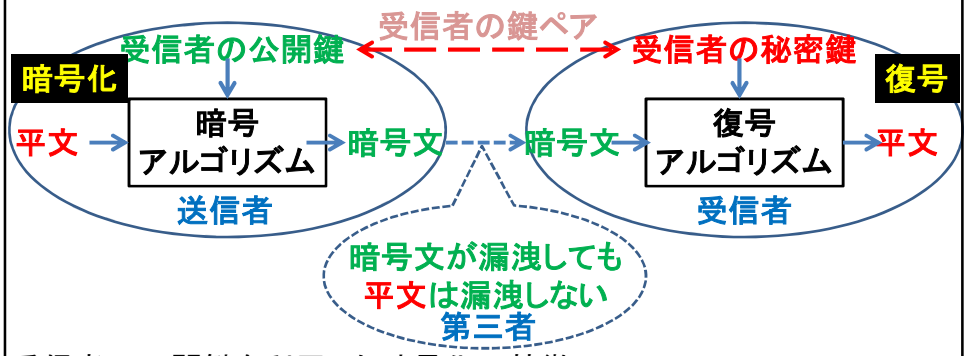
CAS：Conditional Access System



 14

現代暗号　公開鍵暗号方式

暗号鍵と復号鍵が異なる



受信者の公開鍵を利用した暗号化の特徴

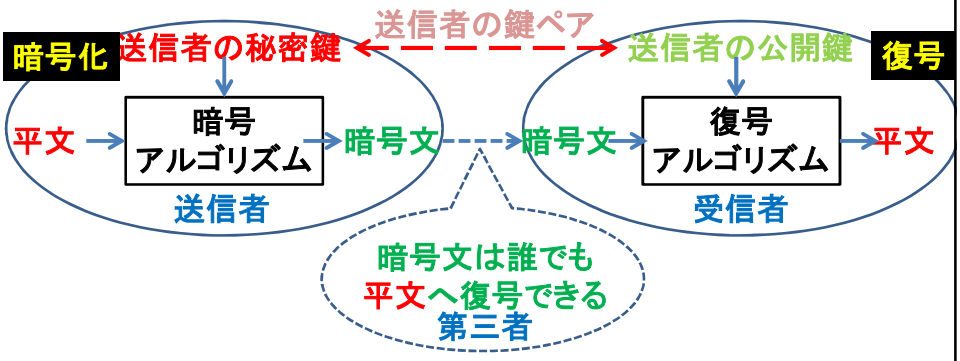
　公開されている公開鍵により暗号化された暗号文は、
　　対応する秘密鍵を所有する受信者しか復号できない

受信者の公開鍵を利用した暗号化の課題

　公開されている受信者の公開鍵が正しいことを確認する必要がある

現代暗号　公開鍵暗号方式

暗号鍵と復号鍵が異なる

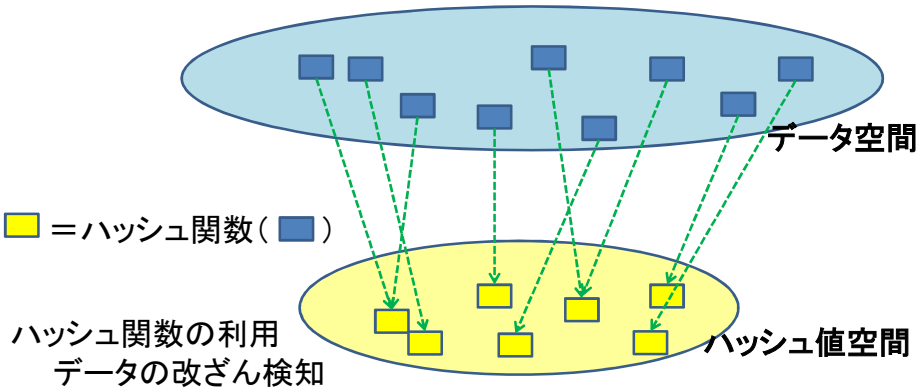


送信者の秘密鍵を利用した暗号化の特徴
　暗号文は送信者の公開鍵でのみ復号可能である

送信者の秘密鍵を利用した暗号化の課題
　暗号文は誰でも復号でき、平文の情報は保護されない

ハッシュ関数

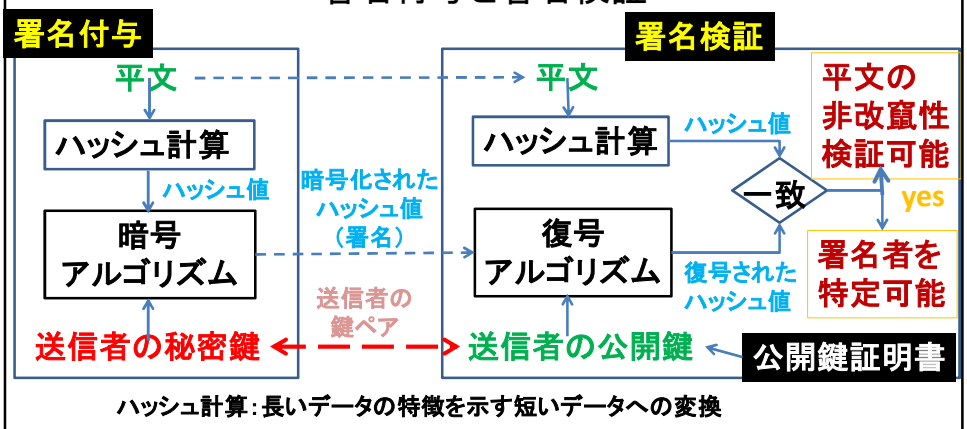
入力したデータを一定の短い長さのデータへ変換



ハッシュ関数の利用
　データの改ざん検知
　　あらかじめデータのハッシュ値を計算し安全に格納しておく
　　必要に応じ、データのハッシュ値を再計算し、
　　格納していたハッシュ値と同一であれば
　　改ざんや変更が無いことを確認

現代暗号　公開鍵暗号方式

署名付与と署名検証



ハッシュ計算：長いデータの特徴を示す短いデータへの変換

署名検証により、
　平文が改ざん（変更）されていないことの確認、
　　および署名者（送信者）の特定が可能
前提として、送信者の正しい公開鍵の入手が必要（公開鍵証明書）

現代暗号　公開鍵暗号方式

代表的な暗号方式と活用事例

主要な公開鍵暗号方式

1978年RSA暗号：大きな素数の積の
　　素因数分解問題の難しさを利用

1985年楕円曲線暗号：楕円曲線上の
　　離散対数問題の難しさを利用

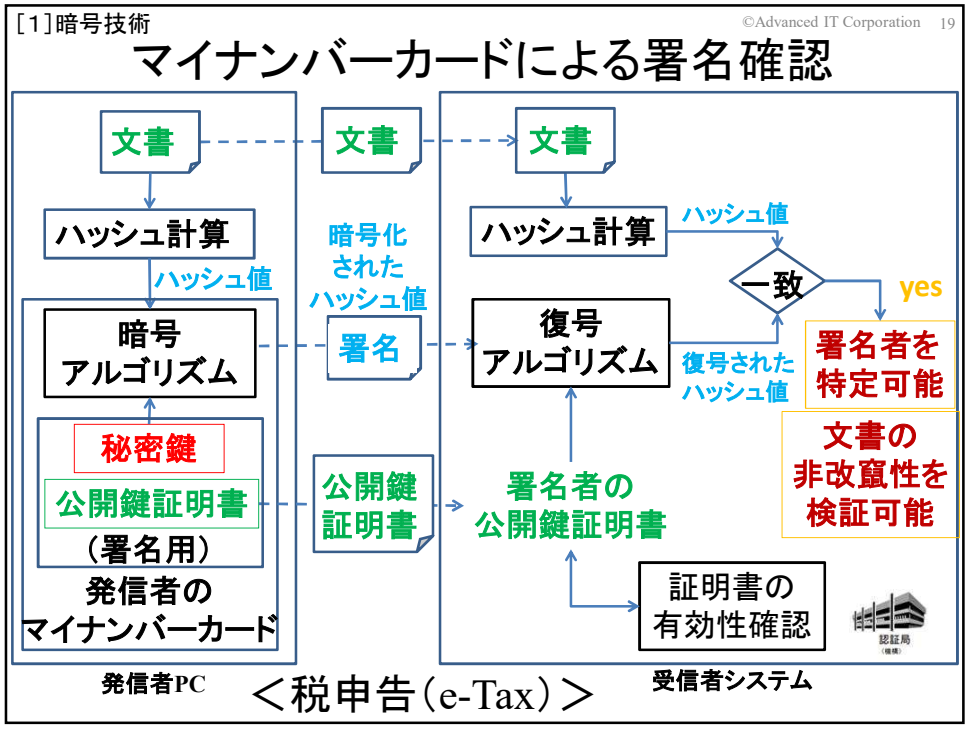
日本での活用事例

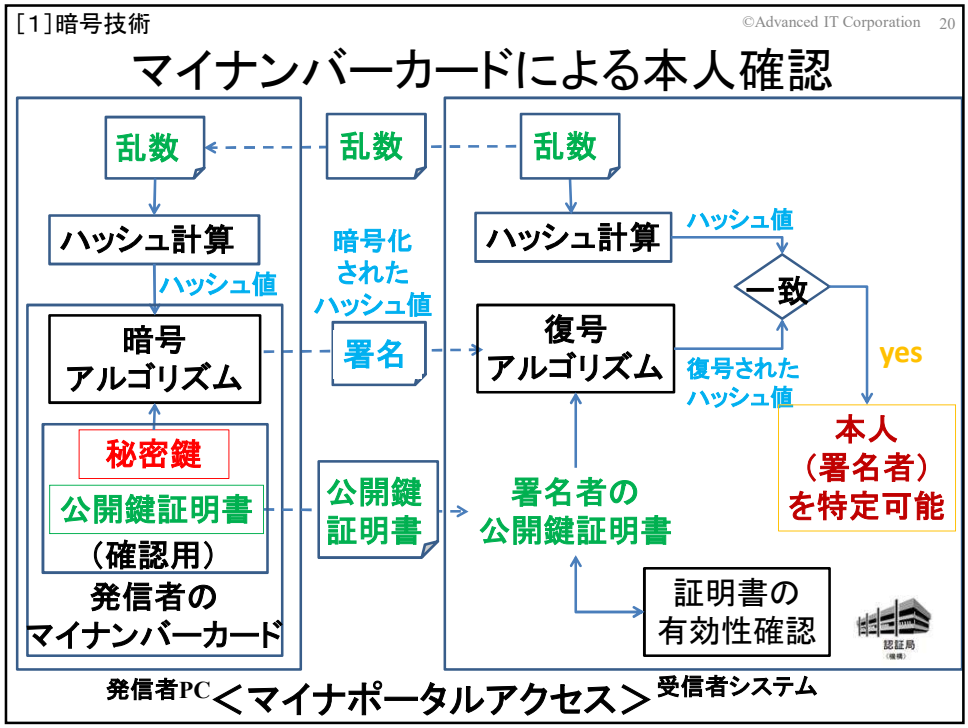
1998年PCでDVD視聴
（DTCP：Digital Transmission Content Protection、楕円曲線暗号他）

2001年クレジットカード（EMV仕様、RSA暗号）

2006年ICパスポート（ICAO準拠、RSA暗号、楕円曲線暗号）

2016年マイナンバーカード（RSA暗号）


[1]暗号技術
©Advanced IT Corporation 19
マイナンバーカードによる署名確認
文書
文書
文書
ハッシュ計算
ハッシュ値
暗号化
された
ハッシュ値
ハッシュ計算
ハッシュ値
一致
yes
暗号
アルゴリズム
署名
復号
アルゴリズム
復号された
ハッシュ値
署名者を
特定可能
秘密鍵
公開鍵証明書
（署名用）
発信者の
マイナンバーカード
公開鍵
証明書
署名者の
公開鍵証明書
文書の
非改竄性を
検証可能
証明書の
有効性確認
発信者PC
＜税申告（e-Tax）＞
受信者システム


[1]暗号技術
©Advanced IT Corporation 20
マイナンバーカードによる本人確認
乱数
乱数
乱数
ハッシュ計算
ハッシュ値
暗号化
された
ハッシュ値
ハッシュ計算
ハッシュ値
一致
yes
暗号
アルゴリズム
署名
復号
アルゴリズム
復号された
ハッシュ値
本人
（署名者）
を特定可能
秘密鍵
公開鍵証明書
（確認用）
発信者の
マイナンバーカード
公開鍵
証明書
署名者の
公開鍵証明書
証明書の
有効性確認
発信者PC
＜マイナポータルアクセス＞
受信者システム

まとめ

（1）暗号技術は、戦いの道具として発展（古代～近代暗号）

人類の歴史は紛争の歴史：
人類・社会の歴史の陰に、暗号に関する熾烈な戦いが存在、
その勝敗が人類・社会の歴史を形作ってきた

（2）暗号技術は、社会活動・生活活動の道具へ（現代暗号）

計算機・ネットワークの発展により暗号技術が身近な技術へ：
産業の発展、国民生活の利便性向上に大きく貢献

（3）現代暗号は、共通鍵暗号方式、公開鍵暗号方式に分類可能

共通鍵暗号方式：通信相手と暗号化および復号に使用する鍵の
共有および安全な管理が必要
公開鍵暗号方式：公開鍵は公開可能、秘密裏に管理すべきは秘密鍵のみ

（4）現代暗号は、様々の用途で利用可能

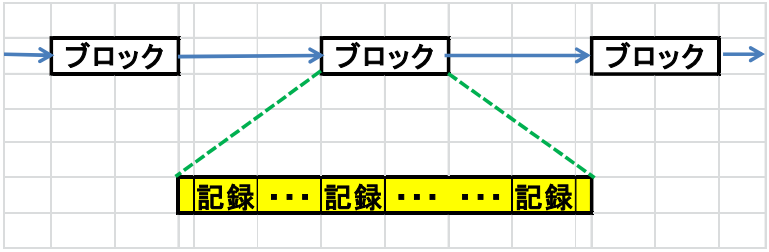
（共通鍵・公開鍵暗号方式）保有データ・通信データの秘匿
（ハッシュ関数）保有データ、通信データの非改ざん性確認
（公開鍵暗号方式）データへの署名者の確認（秘密鍵保有の確認） 16:00

[2]

ブロックチェーンの特徴
および
暗号技術が支える
ブロックチェーンの仕組み

ブロックチェーン

記録（支払等）を（複数）格納しているブロックの連鎖



ブロックチェーンの特徴

（1）中央管理組織の無い記録技術

（2）記録消失の危険性が極めて低い記録技術

（3）過去の記録の改ざんが難しい記録技術

ブロックチェーンの特徴（1）
中央管理組織の無い記録技術

コンセンサスアルゴリズムの必要性

専門の管理組織が無いため、
ブロックチェーンに追加する人・組織の選定方法を
あらかじめ決めておくことが必要

コンセンサスアルゴリズムの例

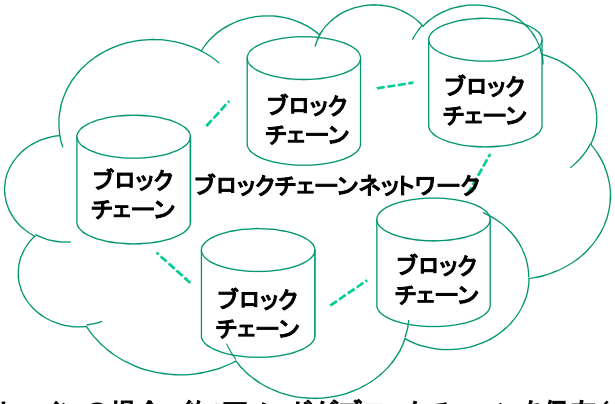
PoW（Proof of Work）：定められた作業を
最初に完了した人・組織に承認権と報酬

PoS（Proof of Stake）：資産の保有量に応じた確率で、
所有者に承認権と報酬

PoI（Proof of Importance）：資産の保有量に加えて、
資産の使用量に応じた確率で、利用者に承認権と報酬

ブロックチェーンの特徴（2）
記録消失の危険性が極めて低い記録技術

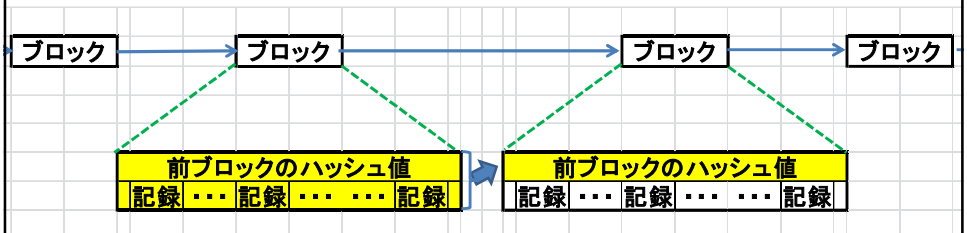
記録が多数のノードで保管・管理されているため



参考：ビットコインの場合、約1万ノードがブロックチェーンを保有（2019年2月時点）
データ量：210GB＋5～10GB/month

ブロックチェーンの特徴（3）
過去の記録の改ざんが難しい記録技術

過去の記録の情報（ハッシュ値）が
以降の記録に反映されているため



ハッシュ値：対象となるデータの特徴を一定の長さのデータに変換したもの。
対象となるデータが1ビットでも変われば、ハッシュ値も変わる。
ハッシュ値から元のデータの復元は不可。ハッシュ関数は一方向性関数。
参考：ビットコインのブロック高は、58321（2019年7月1日頃）

■

ブロックチェーンの例としての ビットコインブロックチェーンの紹介

ブロックチェーン技術を 最初に具現化したのがビットコイン！

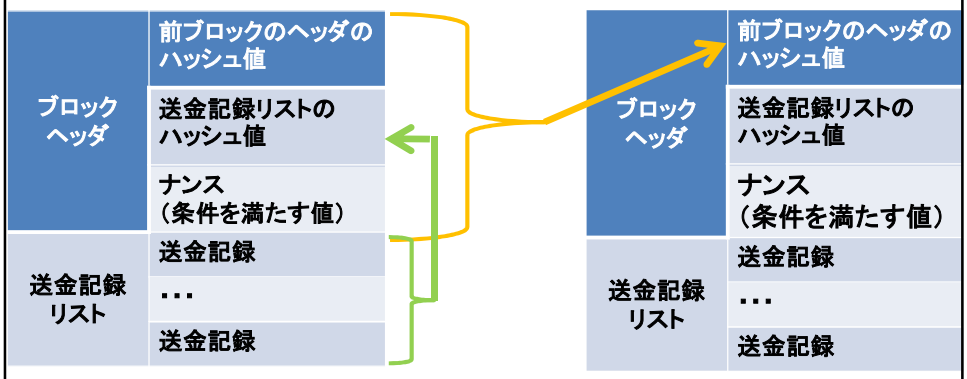
ビットコインの歴史

2008年10月　サトシ・ナカモトがインターネット上で論文発表

2009年1月　ビットコインソフトウェアが開発され運用開始
（その直後に、最初のトランザクションが発行された）

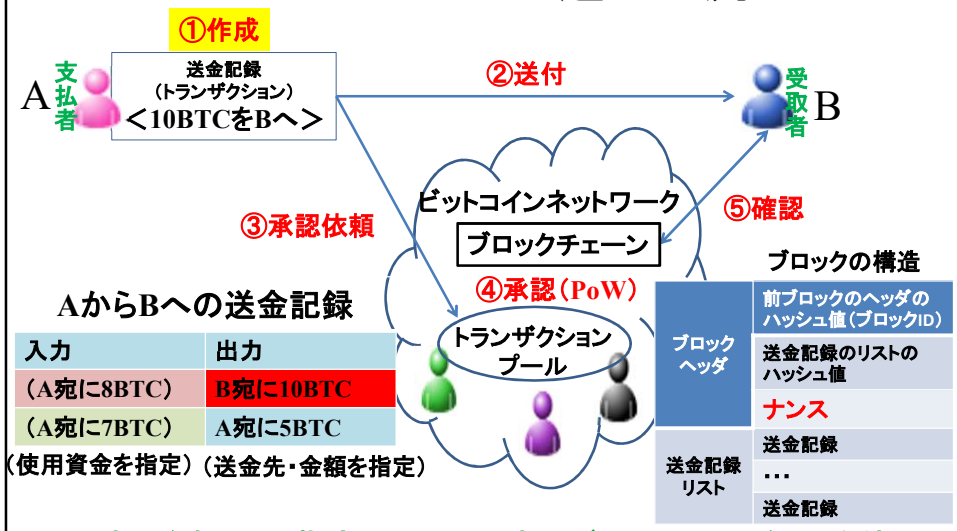
2010年5月　現実世界で初めて決済に使用された
「ピザ2枚（約25ドル）＝1万BTC」で取引が成立（1BTC≒0.2円）
（1BTC≒107.5万円：2019年9月21日）➔ ピザ1枚　約54億円！）

ビットコインにおけるブロックの連鎖



ハッシュ値：対象となるデータの特徴を一定の長さのデータに変換したもの。
対象となるデータが1ビットでも変われば、ハッシュ値も変わる。
（データが変更されていなければ、ハッシュ値は同一となる。）

AからBへの10BTC送金の流れ



AからBへの送金記録

入力	出力
(A宛に8BTC)	B宛に10BTC
(A宛に7BTC)	A宛に5BTC

(使用資金を指定) (送金先・金額を指定)

受取者(送金先)の指定には、受取者のビットコインアドレスを使用
支払者の使用資金は過去の送金記録内の自分宛の出力の未使用分

①支払者によるビットコイン送金記録の作成

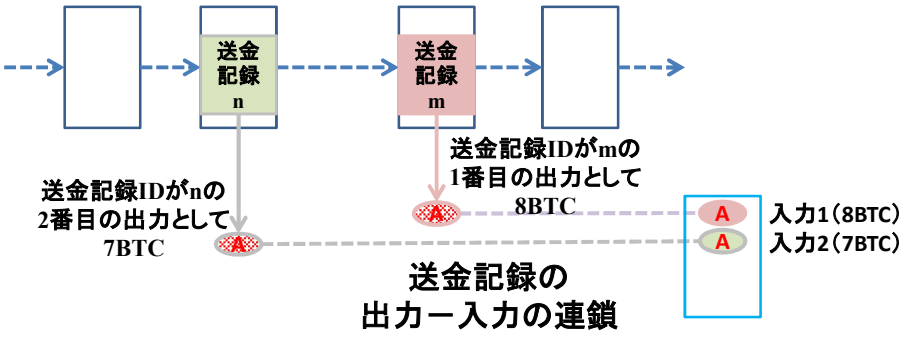
<ビットコインワレット>

利用者A,Bは、あらかじめワレット(財布)を保有
公開鍵暗号方式の楕円暗号の公開鍵・秘密鍵および、
公開鍵から生成されるビットコインアドレス(27～34文字)を管理

(1)支払者Aは、送金に使用する資金を確認
受取者として支払者Aのビットコインアドレスが
指定されている(自分宛の)未使用の送金記録を確認

(2)支払者Aは、B宛の送金記録を作成
使用する資金、送金先(受取者Bのビットコインアドレス)、
送金額により、送金記録を作成

(1)送金に使用する資金を確認



送金記録ID:送金記録のハッシュ値
入力の指定:送金記録IDと何番目の出力かで指定

(2)送金記録の作成

XからAへの送金記録(ID=m)

入力	出力
	A宛に8BTC

YからAへの送金記録(ID=n)

入力	出力
	A宛に7BTC

新規に作成する
AからBへの送金記録

入力	出力
(A宛に8BTC)	B宛に10BTC
(A宛に7BTC)	A宛に5BTC

注1:送金記録IDは、
送金記録のハッシュ値
注2:使用資金は、送金記録IDおよび
何番目の出力かにより指定

ハッシュ値:対象となるデータの特徴を一定の長さのデータに変換したもの

作成された送金記録

使用する送金記録ID=m

入力		出力	
入力元	所有権	出力金額	出力先
		8	Aのアドレス

使用する送金記録ID=n

入力		出力	
入力元	所有権	出力金額	出力先
		7	Aのアドレス

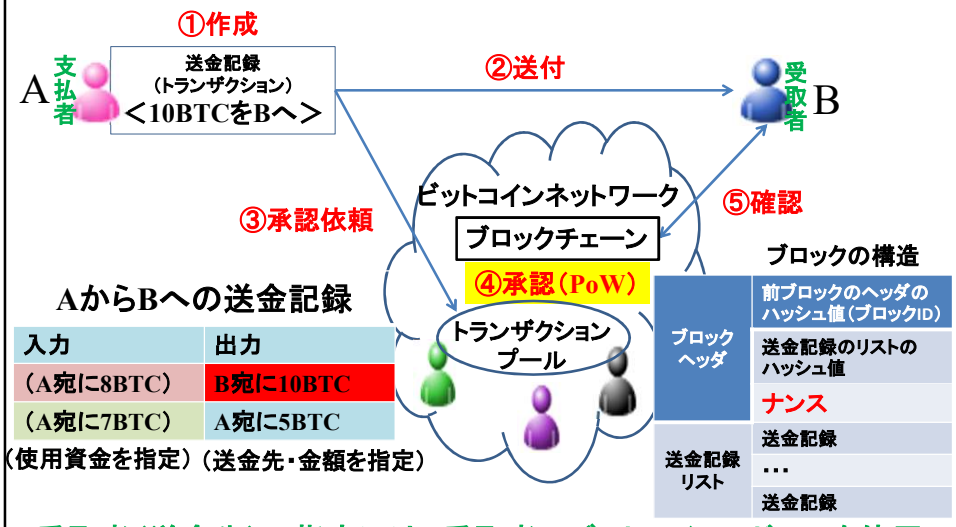
出力先（送金先）は、
新たな受取者（B、A）の公開鍵から生成される
ビットコインアドレス（27～34文字）で指定

Aが新たに作成する送金記録

入力		出力	
入力元	所有権	出力金額	出力先
ID=m Out=1	公開鍵（256ビット）、署名	10	B
ID=n Out=2	公開鍵（256ビット）、署名	5	A

署名は受取者だけが保有する秘密鍵
により作成（楕円曲線暗号の利用）

AからBへの10BTC送金の流れ



AからBへの送金記録

入力	出力
（A宛に8BTC）	B宛に10BTC
（A宛に7BTC）	A宛に5BTC

（使用資金を指定）（送金先・金額を指定）

受取者（送金先）の指定には、受取者のビットコインアドレスを使用
支払者の使用資金は過去の送金記録内の自分宛の出力の未使用分

④検証者によるブロックの構成（承認）
（送金記録の検証およびナンスの計算）

＜トランザクションプール＞
ブロックチェーン未登録の送金記録の集まり

(1)未登録の送金記録の妥当性を検証し、
ブロック構成する記録（トランザクション）を選定
使用する資金（入力資金）は未使用か？
使用する資金（入力資金）の使用権はあるか？➔㋐
使用する資金（入力資金）の合計と
支払う資金（出力資金）の合計は一致するか？

(2)**ブロック構成条件を満たす数値（ナンス）の計算➔㋑**

作成された送金記録

使用する送金記録ID=m			
入力		出力	
入力元	所有権	出力金額	出力先
		8	Aのアドレス

使用する送金記録ID=n			
入力		出力	
入力元	所有権	出力金額	出力先
		7	Aのアドレス

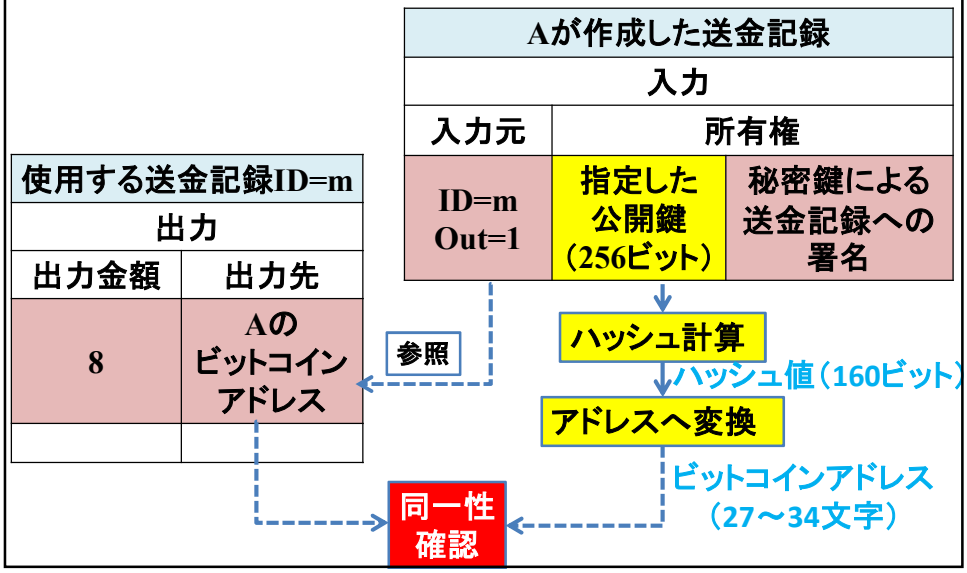
出力先（送金先）は、
新たな受取者（B、A）の公開鍵から生成される
ビットコインアドレス（27～34文字）で指定

Aが新たに作成する送金記録			
入力		出力	
入力元	所有権	出力金額	出力先
ID=m Out=1	公開鍵（256ビット）、署名	10	B
ID=n Out=2	公開鍵（256ビット）、署名	5	A

署名は受取者だけが保有する秘密鍵
により作成（楕円曲線暗号の利用）

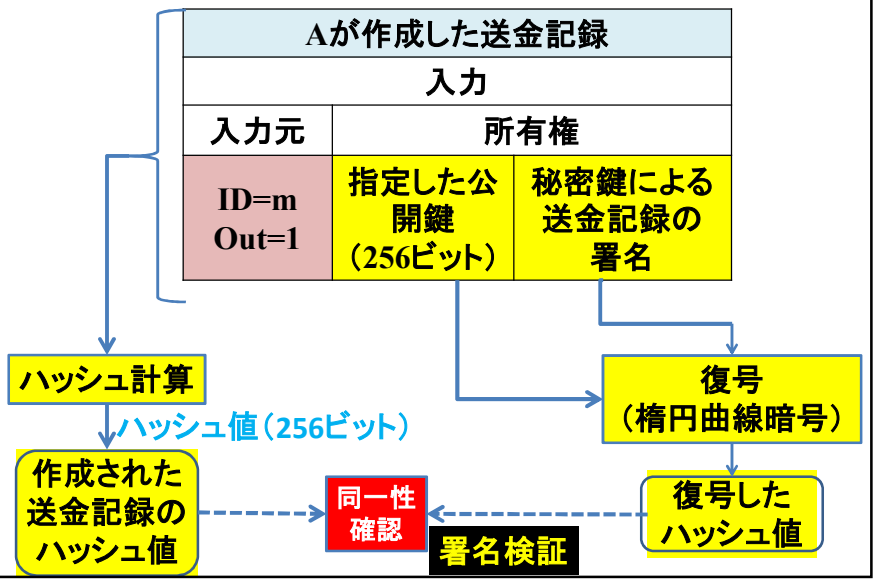
㋐作成された送金記録の検証　その1

ビットコインアドレスと公開鍵が一致するかどうか



㋐作成された送金記録の検証　その2

公開鍵に対応する秘密鍵で署名されているかどうか



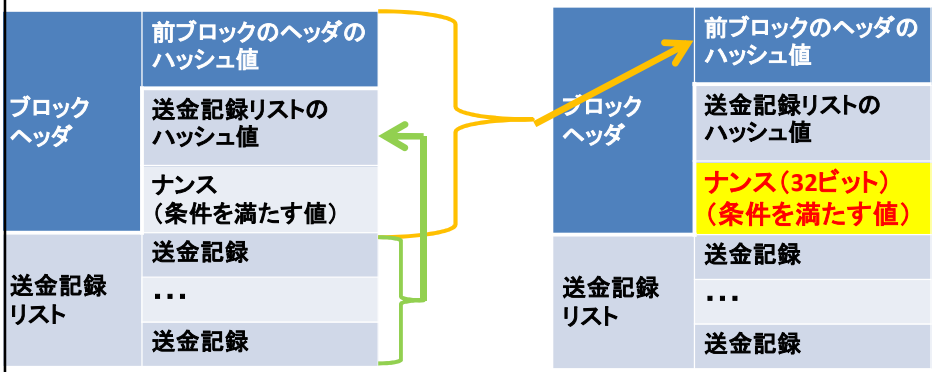
④検証者によるブロックの構成（承認）
（送金記録の検証およびナンスの計算）

＜トランザクションプール＞
ブロックチェーン未登録の送金記録の集まり

(1)未登録の送金記録の妥当性を検証し、
ブロック構成する記録（トランザクション）を選定
使用する資金（入力資金）は未使用か？
使用する資金（入力資金）の使用権はあるか？➔㋐
使用する資金（入力資金）の合計と
支払う資金（出力資金）の合計は一致するか？

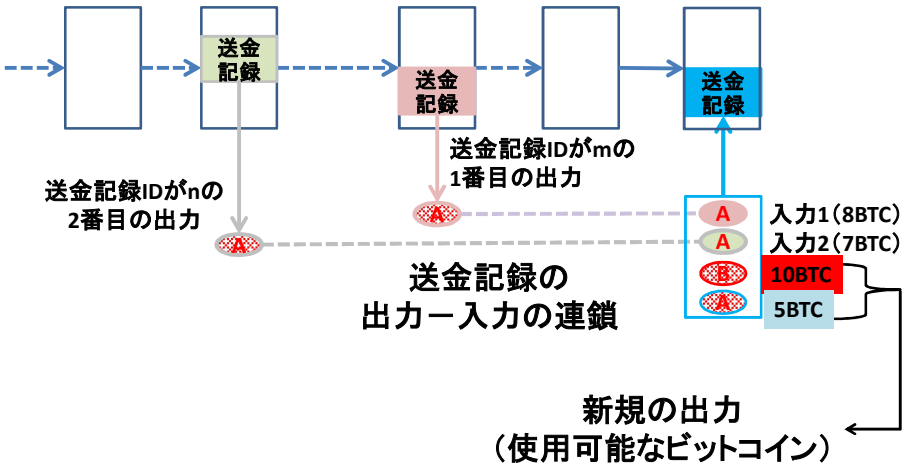
(2)**ブロック構成条件を満たす数値（ナンス）の計算➔㋑**

㋑ブロック構成条件を満たすナンスの計算



検証者は、それぞれ自分で構成したブロックに対しハッシュ値を計算、
条件を満たすナンス探索作業を実施する必要がある（マイニング）
条件：ブロックのハッシュ値（256ビット）の先頭に16個の0が並ぶこと
ハッシュ関数は一方向性のため、ナンスを次々と変えて
ハッシュ値を計算して探索する方法しかない➔膨大な計算量/電力消費
（ビットコイン1トランザクションの電力消費量：VISAの32万倍
年間電力消費量は世界4位の日本の1/13、チリやフィリピンと同等）

送金記録の承認後



まとめ

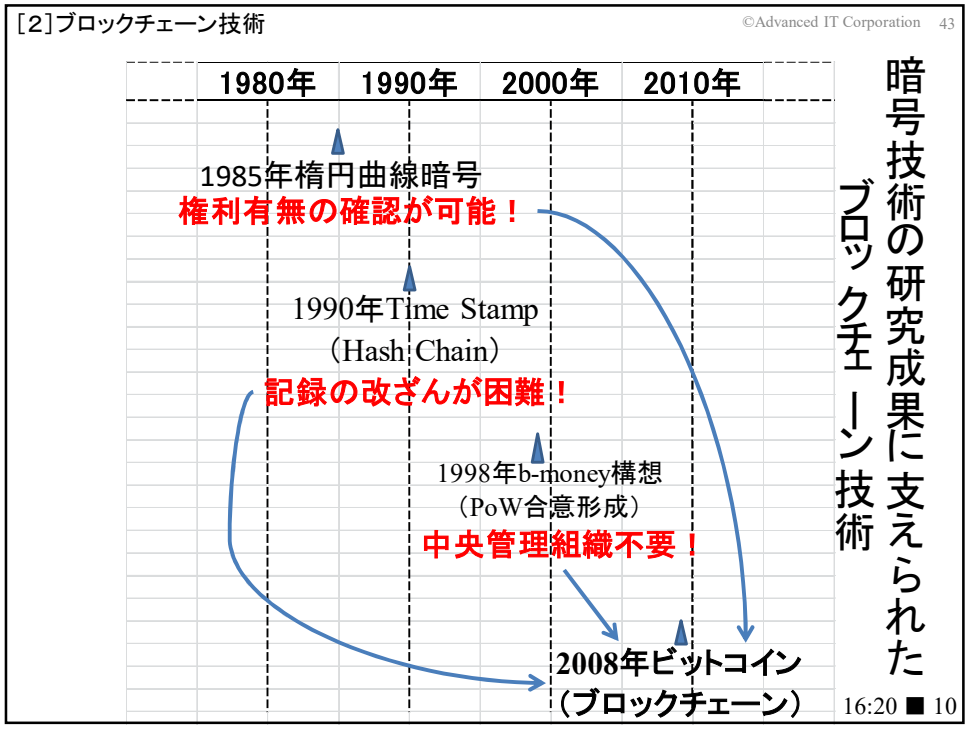
（1）ブロックチェーンの特徴機能

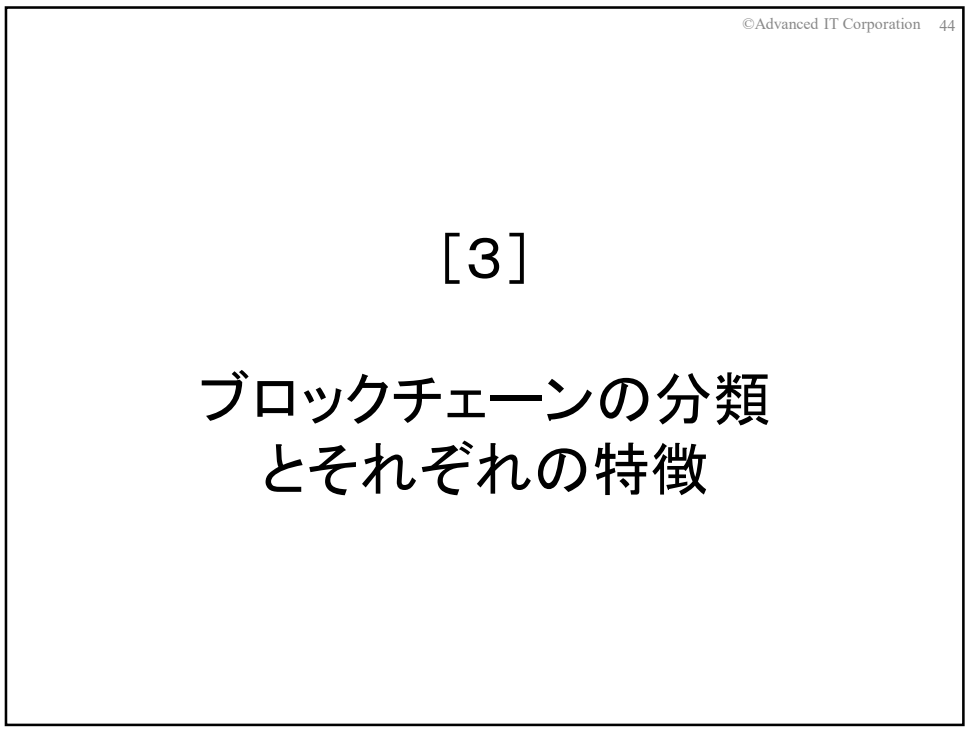
- 中央管理組織の無い記録技術
- 記録消失の危険性が極めて低い記録技術
- 過去の記録の改ざんが難しい記録技術

（2）ビットコインのブロックチェーン

- ブロックチェーン技術を最初に具現化したのがビットコイン！
- ビットコインシステムの
  - 機能概要、送金の仕組み、ブロック構成の仕組みを紹介
- ビットコインブロックチェーンにおける暗号技術の活用場面
  - ハッシュ計算：ブロックID、送金記録（トランザクション）ID
    - ブロック（トランザクション）の改ざん検知
    - 公開鍵からのビットコインアドレスの生成
  - 署名（ハッシュ値の秘密鍵による暗号化）：入力（資金）の所有権証明

（3）暗号技術の研究成果に支えられたブロックチェーン


[2]ブロックチェーン技術
©Advanced IT Corporation 43
1980年
1990年
2000年
2010年
1985年楕円曲線暗号
権利有無の確認が可能！
1990年Time Stamp
（Hash Chain）
記録の改ざんが困難！
1998年b-money構想
（PoW合意形成）
中央管理組織不要！
2008年ビットコイン
（ブロックチェーン）
暗号技術の研究成果に支えられた
ブロックチェーン技術
16:20 ■ 10


©Advanced IT Corporation 44
[3]
ブロックチェーンの分類
とそれぞれの特徴

ブロックチェーンシステム構成エンティティ

主要なブロックチェーンシステムを構成するエンティティ

①情報登録申請エンティティ:
新たなトランザクション(情報)を作成・申請するエンティティ

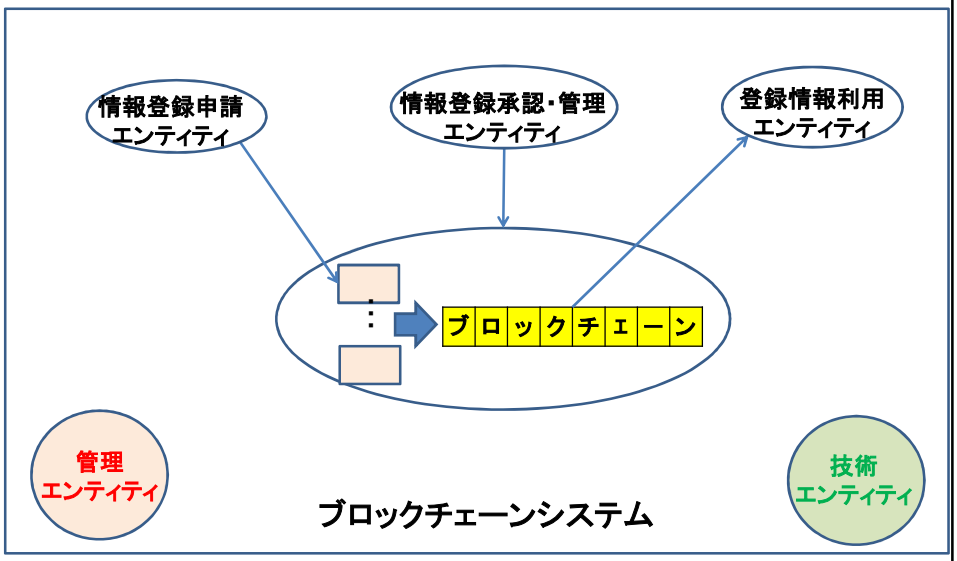
②情報登録承認・管理エンティティ:
申請されたトランザクションを検証し、
ブロックチェーンへ登録・管理するエンティティ

③登録情報利用エンティティ:
登録されているトランザクションを参照し利用するエンティティ

④管理エンティティ:
ブロックチェーンシステムの運用方針を決定するエンティティ

⑤技術エンティティ:
ブロックチェーンの技術・システムを開発するエンティティ

ブロックチェーンシステムの基本構成



ブロックチェーンシステムの一般的分類（1）
＜パブリック、プライベート、コンソーシアム＞

ブロックチェーンシステムの情報登録承認・管理エンティティによる分類

①パブリックブロックチェーン
情報登録承認・管理エンティティとして自由に参加できる
ブロックチェーンシステム
一般ユーザ向けサービス（ビットコイン等の暗号資産システム）

②プライベートブロックチェーン
情報登録承認・管理エンティティが単一であるブロックチェーン
企業・組織内サービス（分散DBシステム等の代替、HyperLedger）

③コンソーシアムブロックチェーン
情報登録承認・管理エンティティが複数であるブロックチェーン
契約関係に基づく企業間サービス
（EWF（エネルギー分野）、R3（金融分野））

各ブロックチェーンのメリット
パブリック、プライベート、コンソーシアム

①パブリックブロックチェーンのメリット
中央管理組織による改ざんのリスクが無い
データの永続性や可用性が高い

②プライベートブロックチェーンのメリット
プライバシー・秘密情報の保護が容易
第三者による改ざんは困難
速やかな取引承認が可能（マイニング競争は不要）
マイニング報酬などのインセンティブが不要
プロトコルの変更が容易

③コンソーシアムブロックチェーンのメリット
パブリック/プライベートブロックチェーンの
それぞれの特徴を一定程度保有 ■

ブロックチェーンシステムの一般的分類（2）
＜Permissionless、Permissioned＞

ブロックチェーンシステムの
情報登録承認・管理エンティティの参加要件による分類

①Permissionlessブロックチェーンシステム
誰でも情報登録承認・管理エンティティとして参加可能
情報登録承認・管理エンティティは匿名可能で、
信頼できない場合もある

②Permissionedブロックチェーンシステム
情報登録承認・管理エンティティとして参加するには、
管理エンティティの承認が必要
情報登録承認・管理エンティティは特定可能で、信頼できる

■

ブロックチェーンシステムの分類（1）
ブロックチェーンの各エンティティの参加要件による分類

①情報登録申請エンティティ：＜参加自由、承認必要＞
新たなトランザクションを
作成・申請するエンティティとしての参加要件

②情報登録承認・管理エンティティ：＜参加自由、承認必要＞
申請されたトランザクションを検証し、ブロックチェーンへ
登録・管理するエンティティとしての参加要件

③登録情報利用エンティティ：＜参加自由、承認必要＞
登録されているトランザクションを
参照し利用するエンティティとしての参加要件

■

ブロックチェーンシステムの分類（2）
＜真正性保証型、データ保全型、プロセス実行型＞

ブロックチェーンの管理（登録）対象情報による分類

①真正性保証型：ハッシュ値のみの管理
　データはブロックチェーン外のシステムで管理
　データの真正性保証が目的

②データ保全型：データそのものも管理
　データはブロックチェーン外のシステムで処理（利用）
　データの保全も目的

③プロセス実行型：ビジネスロジック（スマートコントラクト）も含め管理
　ブロックチェーン機能としてビジネスロジックを実行
　プロセスの自動実行も目的

真正性保証型ブロックチェーンシステム
＜データのハッシュ値のみブロックチェーンで管理＞

（1）応用例：
　既存のシステムで管理するデータ/DBの真正性保証
　個人情報を扱わず、別途管理する個人情報の真正性保証

（2）事例：エストニアのKSI（Keyless Signature Infrastructure）
　2007年に大規模なサイバー攻撃を受け、国家機能が一時マヒ
　その経験を踏まえ、信頼できる第三者機関に依存せず、
　　ハッシュ関数にのみ依存するデータの真正性保証の仕組み
　　ガードタイム社のKSI（Keyless Signature Infrastructure）
　今では、サイバー攻撃防衛先進国に。
　　NATOサイバー攻撃防衛協力センターがエストニアに。
　　（防衛省も昨年、職員を派遣することを発表）

［3］ブロックチェーン分類

 53

エストニア共和国

首都タリン
人口132万

IT立国を目指すIT先進国。安定した経済成長、政府主導のデジタル戦略、スタートアップ環境の整備等により、優秀な起業家・エンジニアの誘致に成功、欧州圏のIT市場のオフショア開発拠点へ。

e-Government構想：エストニア国民はICチップ入りの国民カード1枚で、投票から医療、教育、納税、銀行、警察関連など全ての手続がオンライン上で完結。

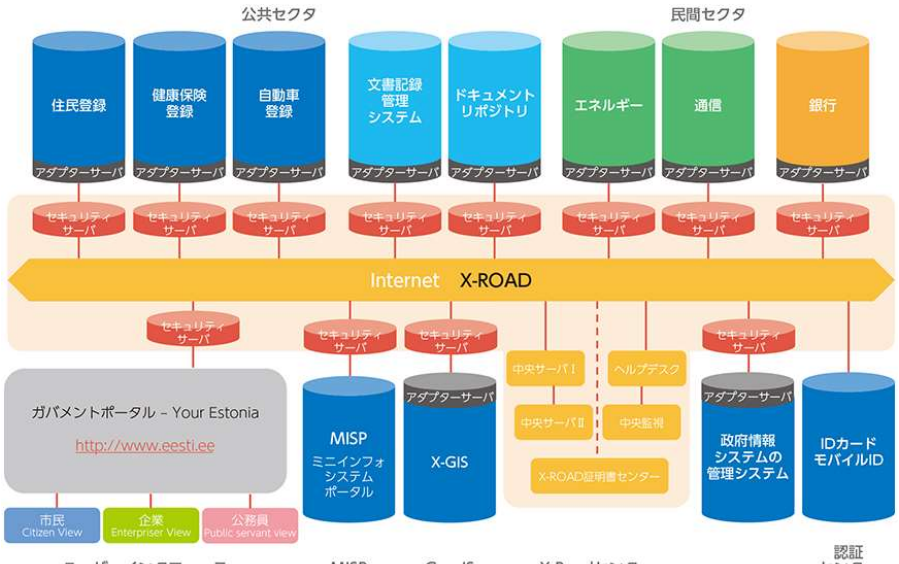
e-Resident構想：外国人もエストニアのデジタル市民となり、オンラインで行政サービスを利用したり、起業したり等が可能。（約165か国の5万人以上が登録済み（日本人も約2500人））。

Estcoin構想：国の公式通貨としての計画はとん挫
（欧州中央銀行総裁：ユーロ圏の通貨はユーロのみと発言）
エストニア大統領が”e-Residency2.0”構想2018年12月発表
（e-Residencyコミュニティ内での利用を目指す模様）

［3］ブロックチェーン分類

 54

エストニアの電子政府アーキテクチャ



出典：平成27年版　情報通信白書（総務省）

[3]ブロックチェーン分類

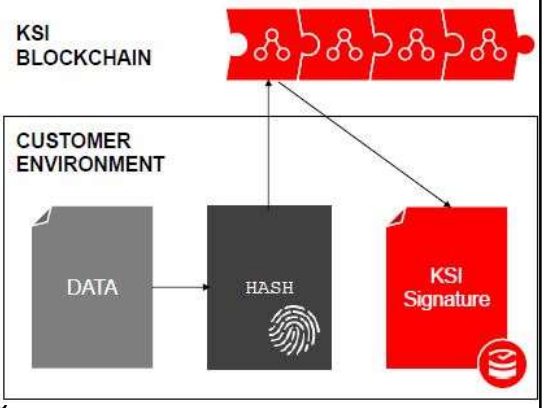
KSI：Keyless Signature Infrastructure

開発元：guardtime（エストニア）　試験：2008年　2012年：実運用

概要：キーレス署名は従来のPKI署名とは異なる代替方式で、
暗号鍵を使わないため、鍵の安全な管理を必要としない署名方式

実現方式：
過去からのデータの要約
をチェーンで結び、
改ざんを検知できる仕組み
（hash-linked time-stamping）

現状：
エストニアのe-Governmentを
支えるX-Roadプラットフォーム
で扱う政府の記録（データ）は
全てKSI署名で保護されている



出典：Guardtimeの資料”Securing Public Services with Blockchain”

[3]ブロックチェーン分類

データ保全型ブロックチェーンシステム
＜データそのものもブロックチェーンで管理＞

（1）応用例
取引の記録
資産のトレーサビリティを保証

（2）事例：Tracr（デビアス社のダイヤモンド追跡システム）
今まで不透明だったダイヤモンドの流通を完全に可視化
ダイヤモンドが発掘鉱山から小売り業者までの追跡が可能に
1：ダイヤモンドにカラット、クラリティ、カラーといった
個々のダイヤモンドの特性を記録する
固有の「グローバル・ダイヤモンドID」を割り当て
ブロックチェーンへ登録
2：発掘鉱山から小売業者へのダイヤモンドの移動の
各チェックポイントでトランザクションとして記録

プロセス実行型ブロックチェーンシステム
＜ビジネスロジック（スマートコントラクト）も含め管理＞

（1）応用例

金や不動産等の売買契約の処理

各種配信サービスの自動実行

（2）事例：ujo MUSIC（音楽配信サービス）

1. 配信された音楽のロイヤリティの配分をアーティスト間であらかじめ決めておく。
2. 取り決めに基づき、音楽配信の対価が各アーティストへ自動的に送金するスマートコントラクトを登録

スマートコントラクト

ブロックチェーンに実装するビジネスロジック

（ビジネスロジックに応じたリアクションを実装可能）

スマートコントラクトは2013年に19歳のロシア人青年

Vitalik Buterinが発表したイーサリアムで初めて実装

スマートコントラクトという考え方は

暗号学者Nick Szaboが1996年に発表

Ethereum

代表的なスマートコントラクト記述言語：Solidity

代表的なSolidity開発環境：Remix

Hyperledger Fabric

チェーンコード（スマートコントラクト）記述言語：

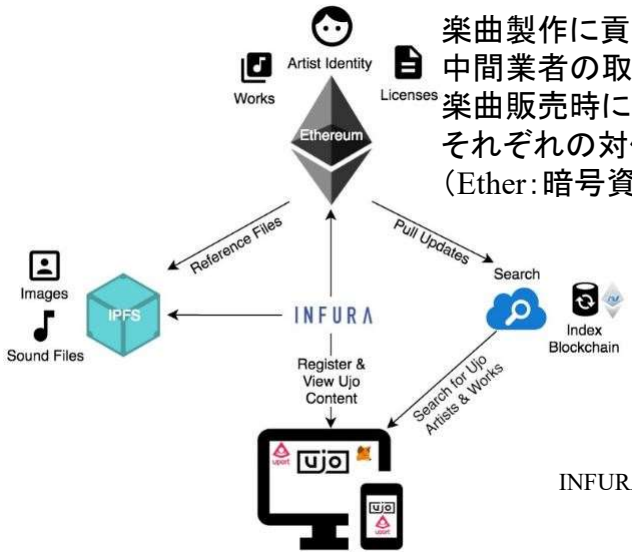
プログラミング言語Go、Node.js、Java

代表的な開発環境： Hyperledger Composer

[3]ブロックチェーン分類

 59

ujo MUSIC：音楽配信サービス



楽曲製作に貢献したアーティスト、
中間業者の取り分をあらかじめ登録、
楽曲販売時には、登録情報に従って
それぞれの対価をEtherにより配分
（Ether：暗号資産Etereum上の通貨）

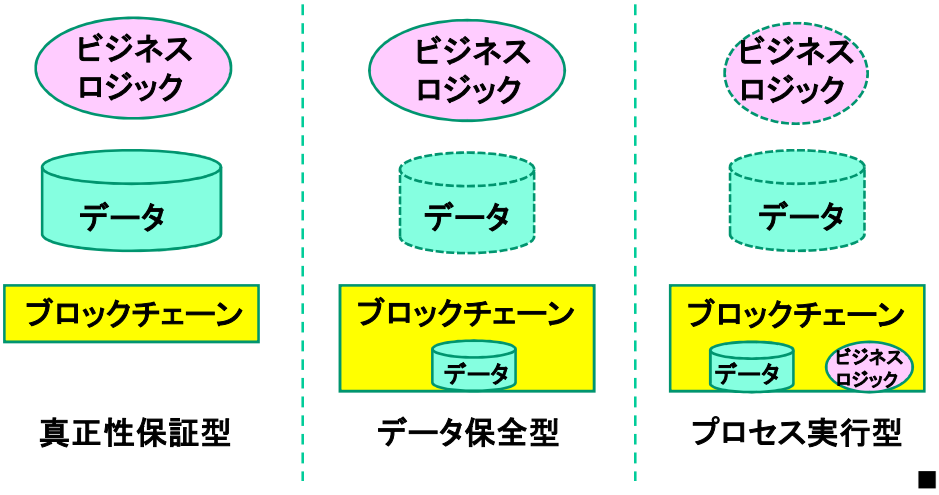
INFURA：Ethereum and IPFS networks
へのAPIアクセス を可能とする
サービスを提供

出典：https://blog.ujomusic.com/building-ujo-1-from-the-technical-underground-to-the-future-a39e825612ef

[3]ブロックチェーン分類

 60

ブロックチェーンシステムと
従来システムとの役割分担



■

分散型台帳技術とは
Distributed Ledger Technology（DLT）

DLTの特徴

（1）台帳の共有 （2）台帳の分散管理 （3）台帳の同期

その実現技術の一つにブロックチェーンがある、という関係

ブロックチェーンを利用していない分散台帳の例

リップル社のXRP Ledger

XRP Ledgerは承認者の8割が認めた取引を台帳に記録する
という方法で非常に速いスピードで取引承認が可能

（2018年現在：UNL全体：23、リップル社：9）

決済や外国為替送金などをインターネット上で行うシステム
主に銀行などの金融機関や法人向けの台帳

まとめ

（1）一般的なブロックチェーンシステムの分類名称
パブリック、プライベート、コンソーシアム
Permissionless、Permissioned

（2）ブロックチェーンシステムの各エンティティの参加要件による分類
エンティティ：情報登録申請、情報登録承認・管理、
登録情報利用

（3）ブロックチェーンの管理（登録）対象情報による分類
真正性保証型、データ保全型、プロセス実行型

（4）分散型台帳技術とブロックチェーンの関係

16:50 ■

［4］

ブロックチェーンの応用分野および活用に向けた取組み

4．1　活用が期待される応用分野・市場規模見通し

4．2　日本における活用可能性・取組事例
＊農業　＊建設　＊製造　＊電力
＊著作権管理　＊物流　＊医療
＊その他

4．1　応用分野・市場規模

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

ブロックチェーン技術を利用したサービスに関する国内外動向調査　経済産業省　平成28年3月

4．1　応用分野・市場規模

 65

ブロックチェーンの ユースケースとサービス事例

ブロックチェーン技術を利用したサービスに関する国内外動向調査　経済産業省　平成28年3月

4．1　応用分野・市場規模

 66

ブロックチェーン技術の 活用が期待される主な分野

分類（注）		分野・テーマの特徴	ブロックチェーン活用の意義	活用検討事例（一部）
活用が期待される分野	医療・ヘルスケア	• センシティブデータでありかつ改竄された場合の影響が多大	• データが改ざん不可能	• 治験データ管理プラットフォーム • 医療機関カルテ共有システム
	物流・サプライチェーン・モビリティ等	• 多様なステークホルダーが関与しているため、データが改ざんされる可能性あり	• 多数のステークホルダーが関与する中で改ざん防止可能	• 製造業におけるトレーサビリティ • 食品のトレーサビリティ
活用が期待される分野横断的テーマ	IoT	• 今後、通信端末・トランザクションの増大が想定 • セキュリティの確保	• デバイス間での直接取引可能 • アクセス権限が改ざん不可能	• M to M 少額取引 • IoT デバイス管理・アクセス制御
	スマートプロパティ	• 権利やモノの流通の促進	• 権利のトークン化による流通の促進 • 中央集権的なデータベースが不要なことによる低コストな権利管理の実現	• コンテンツの利益分配・利用許諾管理 • 不動産の権利処理 • データ流通プラットフォーム
	シェアリングエコノミー	• 透明性の高いシェアリングの実現	• プロシューマーによる非中央集権的なサービスの実現によるプラットフォーマーの恣意的な運営の廃除	• 民泊、ライドシェア、カーシェア

分散型システムに対応した技術・制度等に係る調査報告書　経済産業省　平成30年3月

4．1　応用分野・市場規模

 67

国内ブロックチェーン市場 支出額予測 2017年～2022年

IDC Worldwide Semiannual Blockchain Spending Guide 2017H2, 9/2018

4．1　応用分野・市場規模

 68

国内ブロックチェーン活用サービス市場 規模推移予測

2019 ブロックチェーン活用サービス市場の実態と将来展望　矢野経済研究所　2019年4月

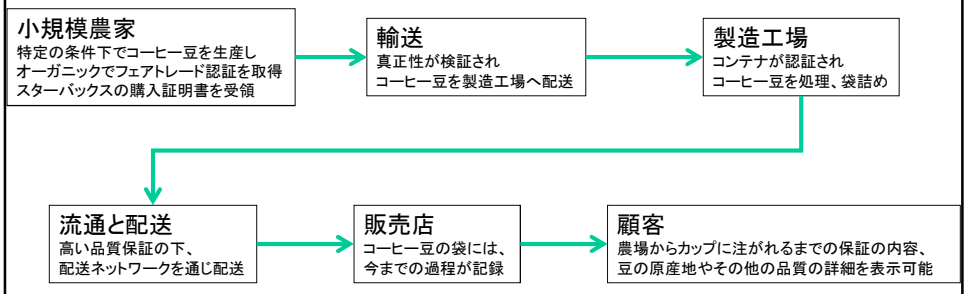
農業分野での活用可能性・取組事例

（1）活用可能性：
　農産物のトレーサビリティ（産地偽装対策等）
　生産過程・輸送過程の可視化
　　（生産・輸送工程の改善、消費者への情報提供）

（2）取組事例：
　①スターバックス（米国）が、フェアトレード証明のための
　　コーヒー豆のトレーサビリティへ適用中
　②ブロックチェーンにより農業の付加価値を高める実証実験を
　　ワイン、野菜を対象に有機農業の先進地・宮崎県綾町と
　　電通国際情報サービス（ISID）が実施中

①スターバックス（米国）：
フェアトレード証明のためのコーヒー豆のトレーサビリティ

コーヒー豆は生産農家から加工・流通プロセスを経て、
販売店経由、顧客へ、
その過程をブロックチェーンに記録、顧客がその記録を確認可能に！



下記URLの資料を参考に作成
https://www.slideshare.net/kazumihirose/decode-2019-cd09-build-2019-blockchain-as-a-service

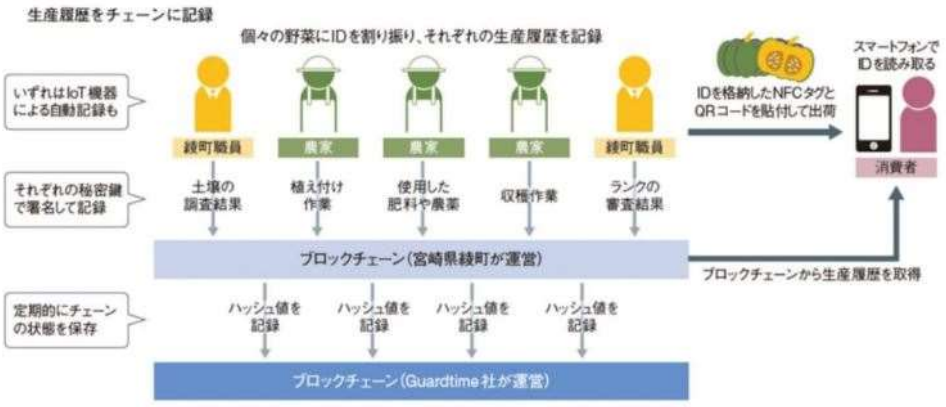
②宮崎県綾町とISIDによる農業の付加価値を高める実証実験

ブロックチェーンと農業を掛け合わせ付加価値を高める実証実験を
ワイン、野菜を対象に有機農業の先進地・宮崎県綾町と
電通国際情報サービス（ISID）が実施中
（ブロックチェーン技術については、guardtimeおよびシビラ社が協力）

生産過程をブロックチェーンに記録し、消費者がQRコードにより確認
ワイン：ぶどうの栽培や収穫、発酵などの過程を記録
野菜：作付された土壌や時期を記録（次ページに構成図）

輸送過程をブロックチェーンに記録、流通品質管理・産地偽装検知
野菜：NFCタグ付き箱の内部にセンサーを同梱し、
振動、温度、照度を記録

宮崎県綾町とISIDによる実装実験構成図
野菜の生産過程の記録と消費者への情報提供



https://www.coindeskjapan.com/6834/

■

建設分野での活用可能性・取組事例

（1）活用可能性：
契約行為・資材調達の自動化
建設工事の透明性
工事の内容と資金の流れの記録
（建設業界の汚職や不正を撲滅し、信頼性を向上）

（2）取組事例：
①設計図などの機密データの建設現場でのセキュアな管理を
前田建設がTRIART等の協力を得、「XCOA」(クロスコア)で実現
（XCOAはブロックチェーンを応用した暗号データ分散技術）

■

製造分野での活用可能性

製品への信頼性付与（偽造品流通検知）
：原材料、生産国、検査結果、流通経路などの情報の非改ざん性

トラッキング機能強化：問題発生時にも信頼できる情報により
問題点の把握、問題個所の発見が容易

プロセス自動化：センサーデータに基づく自動処理
（業者間の契約や支払いの自動化（製品の出荷と配送が
確認されてから支払いを自動的に実施等））

契約データ管理：契約書等の重要な書類の確実な保存、非改ざん性

需要予測：製品のトラッキングから得られたデータの統計的処理

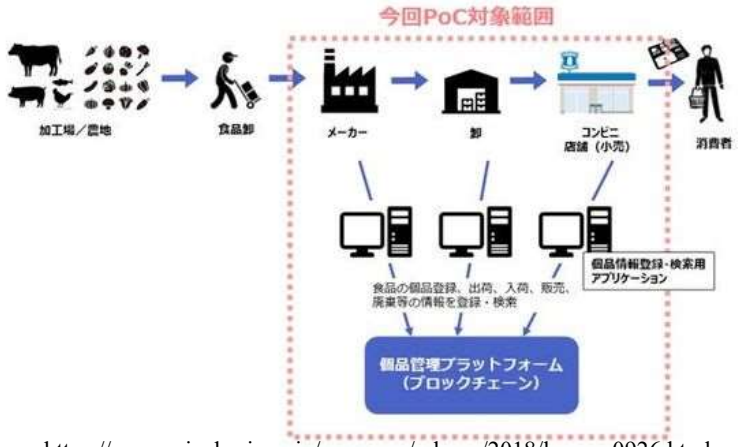
製造分野での取組事例

①食品メーカーから消費者までの一連の経路を個品単位で可視化のPoCを、ブロックチェーン基盤「Hyperledger Fabric」を利用し、みずほ情報総研とローソンが実施

②天然ゴムの原料の安定的な調達・供給・流通の透明性確保のため、トレーサビリティ・システムの構築に向けた実証実験を開始
天然ゴム加工会社PT. Aneka Bumi Pratama（本社：インドネシア）の天然ゴム原料調達サプライチェーンを活用し、
CTCが実証実験用のトレーサビリティ・システムを構築

①みずほ情報総研とローソンによる食品流通における可視化の実証実験

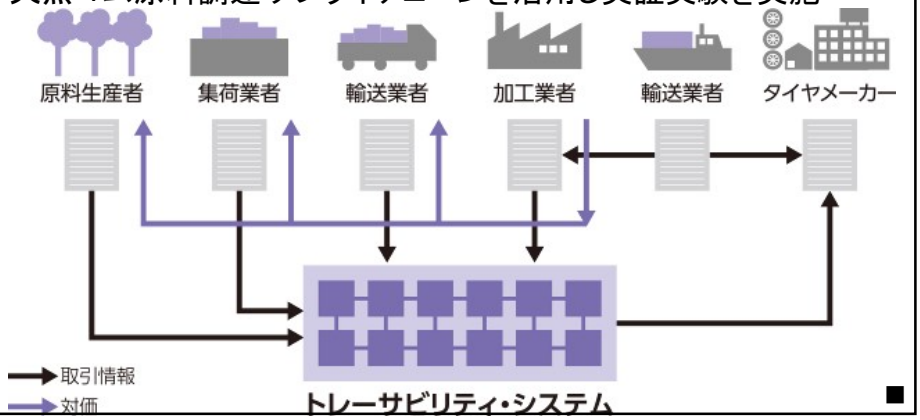
食品メーカーから消費者までの一連の経路を個品単位で可視化
ブロックチェーン基盤「Hyperledger Fabric」を利用



https://www.mizuho-ir.co.jp/company/release/2018/lowson0926.html

②PT. Aneka Bumi PratamaとCTCによる天然ゴム原料トレーサビリティ実証実験

天然ゴムの原料の安定的な調達・供給・流通の透明性確保が目的
天然ゴム加工会社PT. Aneka Bumi Pratama（本社：インドネシア）の天然ゴム原料調達サプライチェーンを活用し実証実験を実施



電力分野での活用可能性・取組事例

（1）活用可能性：
再生可能エネルギーを中心とした分散型電源の拡大に伴い、P2P 取引の実装に向けた機運が高まり、P2P 取引を実現する上で鍵となる技術としてブロックチェーンへ期待

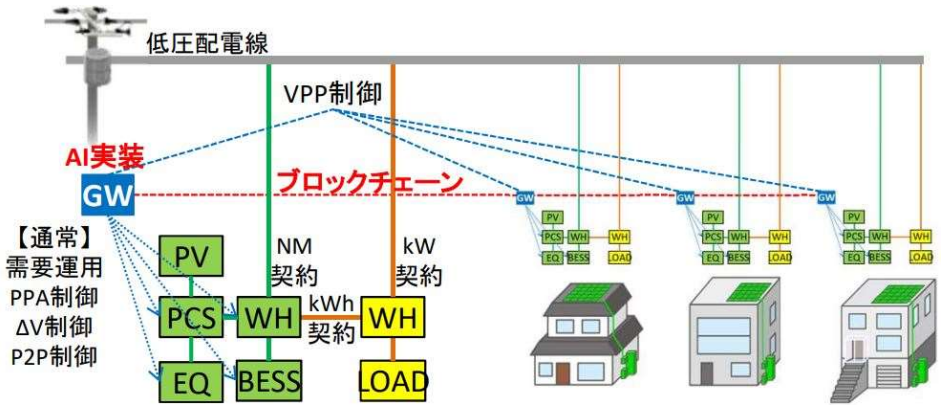
（2）取組事例：
①宮古島市島嶼型スマートコミュニティ実証事業の目標は、需要家メリットを最大化し、電力供給コストを低減し、社会コストを最小化するエネルギー供給モデルの追求
②みんな電力は、低炭素価値取引へのブロックチェーン適用を目指し電源を指定した取引を可能とする P2P 電力取引システムを構築
③太陽光発電パネルの電気を住戸間や住戸・店舗間で電力融通を行うための実証事業で、Ethereumのプライベートチェーンを利用し構築（浦和美園等で実証実験中）

4．2　活用可能性・取組事例

 79

①宮古島市
島嶼型スマートコミュニティ実証事業

需要家メリットを最大化し、電力供給コストを低減し、社会コストを最小化するエネルギー供給モデルが目標。ローカル制御/精算にブロックチェーン等を活用。プライベート型分散台帳技術である「BBc-1」を利用。



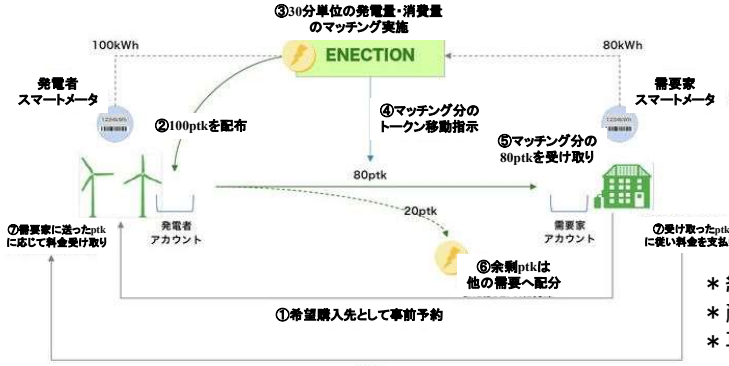
http://smaeco.co.jp/wp-content/uploads/2018/02/miyakojima-rc-65.pdf

4．2　活用可能性・取組事例

 80

②みんな電力による
P2P 電力取引システム「ENECTION2.0」

みんな電力株式会社は、株式会社AerialLabIndustriesと協同で、電源を指定した取引を可能とする P2P 電力取引システム「ENECTION2.0」の開発を完了し、2018年 9 月より先行利用試験を実施、2018年12月に商用化。NEMのパブリックブロックチェーンを採用して実現。

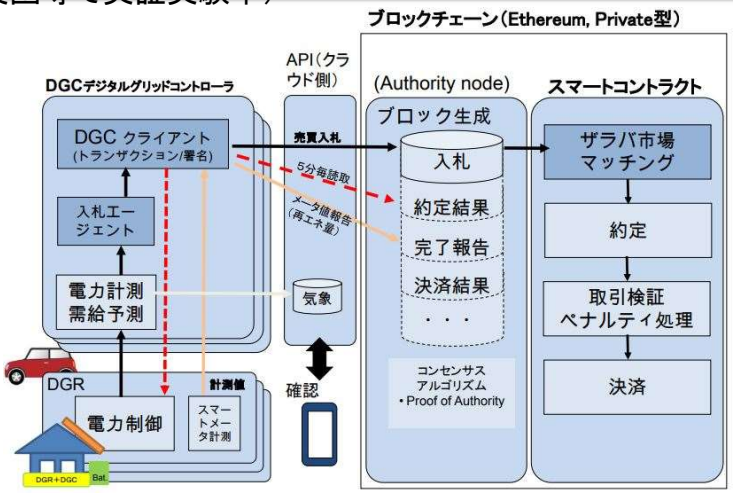


＊結果をBCへ登録
＊顔の見える電力
＊再生可能エネルギーであることの証明

https://crypto.watch.impress.co.jp/docs/interview/1181811.html

③電力融通決済システム

太陽光発電パネルの電気を住戸間や住戸・店舗間で電力融通を行うための実証事業で、Ethereumのプライベートチェーンを利用し構築（浦和美園等で実証実験中）



https://www.meti.go.jp/committee/kenkyukai/energy_environment/e-tech/pdf/007_03_00.pdf

著作権管理分野での活用可能性・取組事例

（1）活用可能性：

著作権・著作物の登録・公開（著作物の無断利用への迅速な対応）
著作権比率の登録、自動的な著作権料配分（透明、確実な利益配分）
著作物配信システムとの連動により、自動配信
中間者を排した、著作権者と利用者の直接取引

（2）取組事例：

①ブロックチェーン技術を使った音楽権利情報処理システム基盤構築
クリエイターの権利情報処理に関する作業効率と信頼性を高めるのを目的とし、「Amazon Managed Blockchain」のコンソーシアムチェーンの「Hyperledger Fabric」を利用し、以下を目標にソニーミュージックが構築。
「電子データの作成時期の証明」
「改ざんできない事実情報の登録」
「過去に登録済みの著作物との照合・判別」
「データの生成日および生成者を参加者間で共有・証明」

物流分野での活用可能性・取組事例

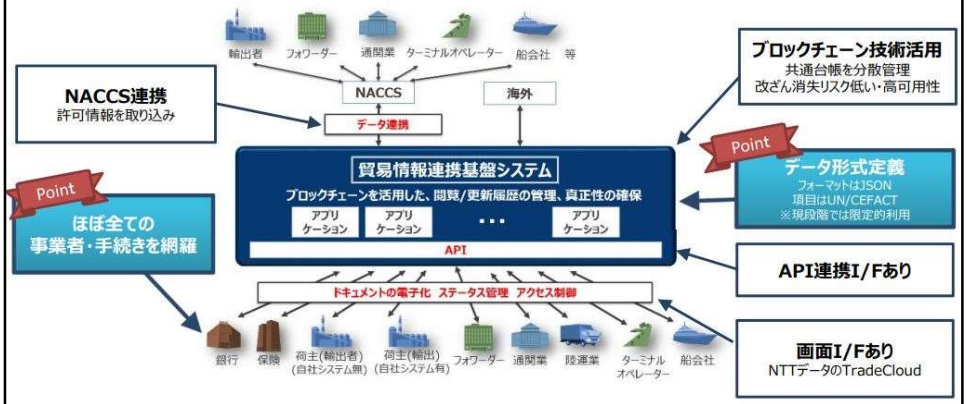
（1）活用可能性：

個々の対象製品の物流データを（自動的に）記録することにより、
生産者から消費者に届くまでの過程がすべて記録
改ざんが困難な透明性のある物流プロセスの記録情報
配送トラブルへの迅速な対応が可能

（2）取組事例：

①ブロックチェーン技術を活用した貿易情報連携基盤の実証事業
官民連携でグローバルサプライチェーンにおける
貿易手続きの効率化へ
ブロックチェーンを活用したデータ連携システムを構築し、
輸出入者・フォワーダー・通関業・陸運業・ターミナルオペレーター・船会社
・銀行・保険等を含めた貿易手続きに関わる事業者間で、
貨物や手続きなどに関する正確なデータをセキュリティーが担保された形で
共有できる仕組みを提供し、生産性向上と輸出リードタイムの短縮を目指す
（NTTデータ）

①ブロックチェーン技術を活用した貿易情報連携基盤の実証事業



https://www.jpca.or.jp/cedi/event/pdf/28/GSCM-WG.pdf

医療分野での活用可能性および取組事例

（1）活用可能性：
医薬品のサプライチェーン（偽薬監視、リコール）
薬事申請における治験データの認証、電子申請
医療機器運用時のデータ認証、保守の管理
患者情報の管理（個人情報、同意情報、遺伝情報）
支払い業務効率化（保険請求）
医療情報（電子カルテ等）の他業種連携・共有

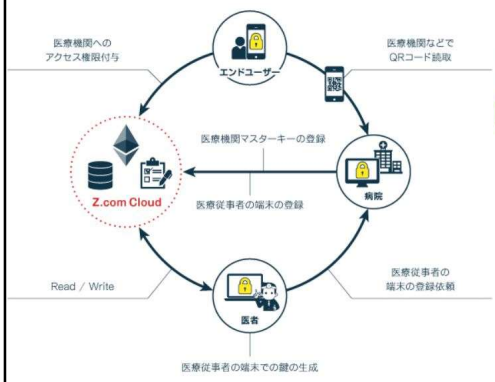
（2）取組事例：
①3M（米国）：偽造品の流通課題への対策として、
医薬品の真正性の証明
②GMOブロックチェーンオープンソース提供プロジェクトによる
医療カルテ共有システム
アクセス制御処理の自動化（スマートコントラクト）

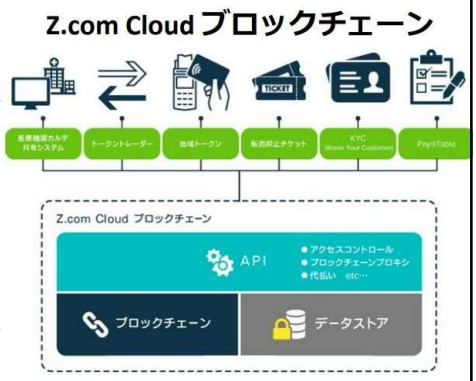
①3M（米国）：医薬品の真正性の証明
偽造品の流通課題への対策

https://www.slideshare.net/kazumihirose/decode-2019-cd09-build-2019-blockchain-as-a-service

②医療カルテ共有システム

GMOブロックチェーンオープンソース提供プロジェクト





特長1）データのアクセスコントロールが可能
特長2）トランザクション手数料（Gas）の代払い機能
特長3）冗長化による高い耐障害性
特長4）ブロックチェーン基盤をAPIでラッピング

https://guide.blockchain.z.com/ja/docs/oss/medical-record/　　http://jami.jp/about/documents/Blockchain2.pdf

■

その他の取組事例

＊ブロックチェーン活用したインターネット投票
つくば市は、インターネット投票の実証実験を2019年8月28日に実施
すると発表。VOTE FOR、ユニバーサルコムピューターシステム、NECが協力。
狙い:「投票内容の改ざん防止」、「秘匿性の確保」、「場所にとらわれない投票」、
「マイナンバーカードに登録されている顔写真による確実な本人確認」
https://japan.zdnet.com/article/35139201/
https://www3.nhk.or.jp/lnews/mito/20190829/1070007203.html

＊ブロックチェーンを応用した野生鳥獣の食肉のトレーサビリティの管理
長野県茅野市を本拠とする「日本ジビエ振興協会」は、
ジビエのトレーサビリティの管理に、プライベートチェーンMijinを
利用したシステムの試験運用を2017年から実施
https://gentosha-go.com/articles/-/18256

＊ブロックチェーン活用の不動産情報共有が始動
ブロックチェーン技術を活用した不動産情報共有プラットフォームの
実証プロジェクトが、2018年11月、不動産情報コンソーシアムを設立
https://crypto.watch.impress.co.jp/docs/event/1151951.html

＊保険・貿易取引のデータ共有の実証実験（2017年11月～2018年11月）
東京海上日動はNTTデータと協同し、海外クレーム代理店が、世界中に点在する貿易関連書類と最新の保険証券書類の収集、関係者との情報共有の迅速・正確に実施し、迅速な保険金支払い手続きを実現できる見通しを得た。
https://economies2.com/feature/insurance_blockchain2/

＊大学の学位証明書のオンライン発行へ
経済産業省は文部科学省と連携し、2018年度中に設計を決め、
2019年度以降の実用化を目指している。
https://www.nikkei.com/article/DGXMZO32259480W8A620C1EE8000/

＊外国人留学生の日本語講座の受講履歴や成績証明管理にブロックチェーンを活用する実証実験を開始（2019年2月）
ソニー、富士通および富士通総研は、外国人留学生の受入・育成を行う教育機関であるヒューマンアカデミー株式会社の協力のもと、講座受講履歴や成績データの管理においてブロックチェーン技術の有用性を確認する実証実験を開始。
https://www.sony.co.jp/SonyInfo/News/Press/201902/19-0227/

＊ブロックチェーンを利用した電子地域通貨「さるぼぼコイン」、2017年12月発行開始
地域通貨では我が国で初めて「ブロックチェーン」の技術が導入された。
http://www.chukeiren.or.jp/magazine/pdf/chuybudayori%20201805.pdf

まとめ

（1）今回紹介した
ブロックチェーンの活用に向けた取組事例
における主な機能・目的は以下の通り。

<機能>
＊情報の記録・管理
＊情報の提供・共有
＊情報に基づく処理の自動化

＜目的＞
＊作業効率化およびトラブル対応の迅速化・正確化
＊役割・責任の明確化
＊顧客・パートナーへの安心感付与（説明責任）

（2）ブロックチェーンの広範囲な応用可能性は確実で、
市場も成長するものと思われる。
（過大な期待への反動からか失望の意見もある）

（3）現状、ブロックチェーンの実用化フェーズの応用は
暗号資産以外にない。
（ほとんど、実証レベルか検討レベルにとどまっている）

Hype Cycle for Blockchain Business（2018, Gartner）

安定期到達までの想定期間

○ less than 2 years　● 2 to 5 years　● 5 to 10 years　▲ more than 10 years

（４）ブロックチェーンの応用の現状と今後の取組について

①多くの場合、ビジネスソリューションを実現するのに
ブロックチェーンを使わなくとも、既存技術で対応可能。

2018年末までのブロックチェーンプロジェクトの85%が、実際にはブロックチェーンを使うことなく既存技術で同等の効果を上げ得たとガートナーは予想。

（現状のブロックチェーンプロジェクトの多くは、技術習得（技術者育成）、対象業務への適用可能性検証（PoC）・課題抽出が目的のため。）

②ブロックチェーンをよく理解することが大変重要。

ソリューションベンダーのセールストークに惑わされず、自社・客先の課題解決・目標達成に適切な技術・パートナーの選択が重要。

③ブロックチェーンの可能性をよく理解し、果敢なトライを。

金融サービスを超えてブロックチェーン導入が進んでいるのは事実。

多くの企業で、事業・業務のブロックチェーン時代の将来像を描き、果敢なトライを期待したい。 17:10 ■

［５］

ブロックチェーンの技術・応用に関する最新動向

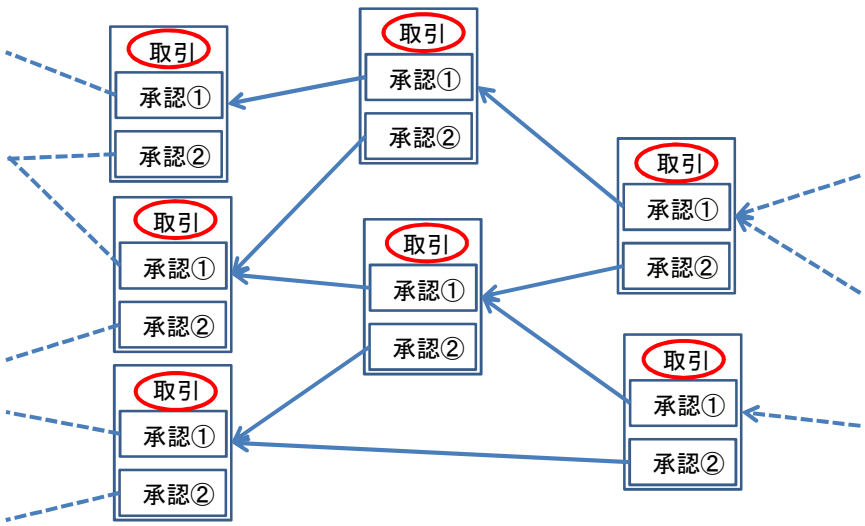
５．１ ブロックチェーン関連技術の最新動向

５．２ IoT/ビッグデータ/AIにおける
ブロックチェーン活用・連携の視点

ブロックチェーンに変わる新技術　DAG
IOTA

開発元：IOTA Foundation（ドイツ）　発表：2016年7月
概要：機械と機械が直接取引を行うことを想定した、
IoT向けの仮想通貨/決済プロトコル
特徴は、マイナーが不要で、取引手数料がかからないこと
実現方式：既存のブロックチェーンとは少し異なり、
Tangle（DAG：Directed acyclic graph：有向非巡回グラフ）を使用
現状：オープンソースとして公開（機能強化は継続中）
2017年11月、IOTA上で分散型データ販売市場確立のため
20社以上とパートナーシップ契約
（マイクロソフト、富士通、シスコ、フォルクスワーゲン、サムスン等）
2018年8月、富士通は「IOTAを新たな標準プロトコルにする
準備が整った」と発表

Tangle（イメージ）



ブロックチェーンに変わる新技術　Hashgraph
Hedera　Hashgraph

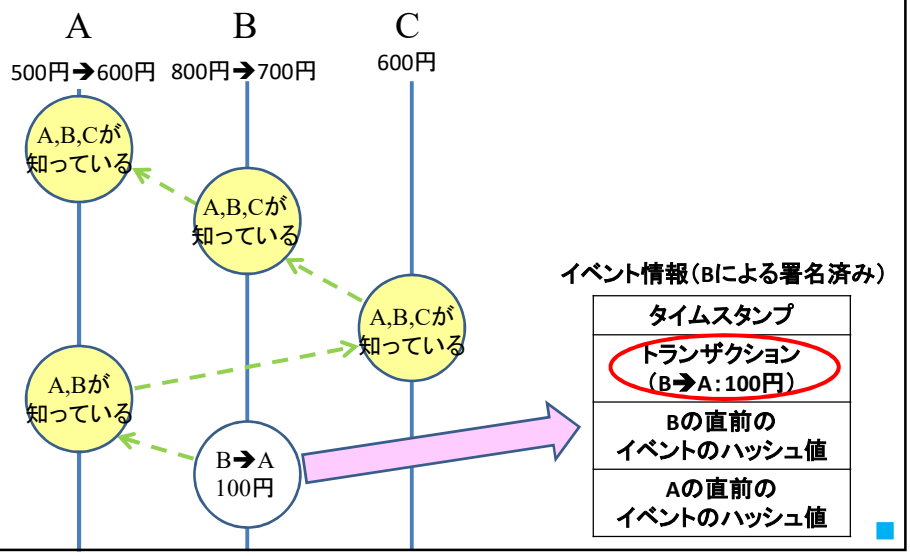
開発元：Hedera Hashgraph LLC（米国）　発表：2017年9月
（Hashgraph技術は、SwirldsのCTOであるLeemon Bairdが2016年に開発）

概要：高速処理（1秒当たり数十万トランザクション）が可能
各業界の専門知識を持つ企業の委員会でガバナンス、安定性を維持
（ドイツテレコム、IBM、野村ホールディングス、Swirlds、TATA等）
各国政府が求めるKYCやAMLに関する規制の遵守が可能

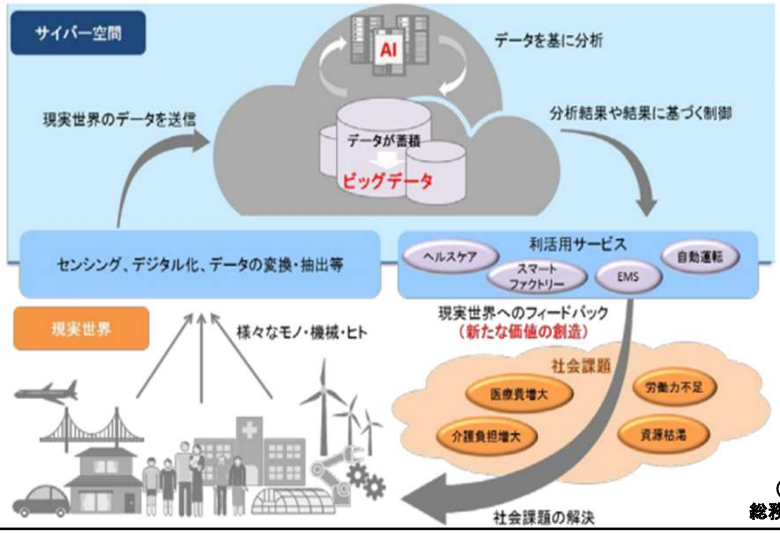
実現方式：既存のブロックチェーンとは少し異なり、
Hashchain（DAGの一種）を使用

現状：Hederaのソースコードは委員会で統制
Hederaプラットフォーム上での応用開発は自由
Hashgraphコンセンサスアルゴリズムのパテントは Swirldsが保有

Hashgraph（イメージ）
3人（A，B，C）のコミュニティの例

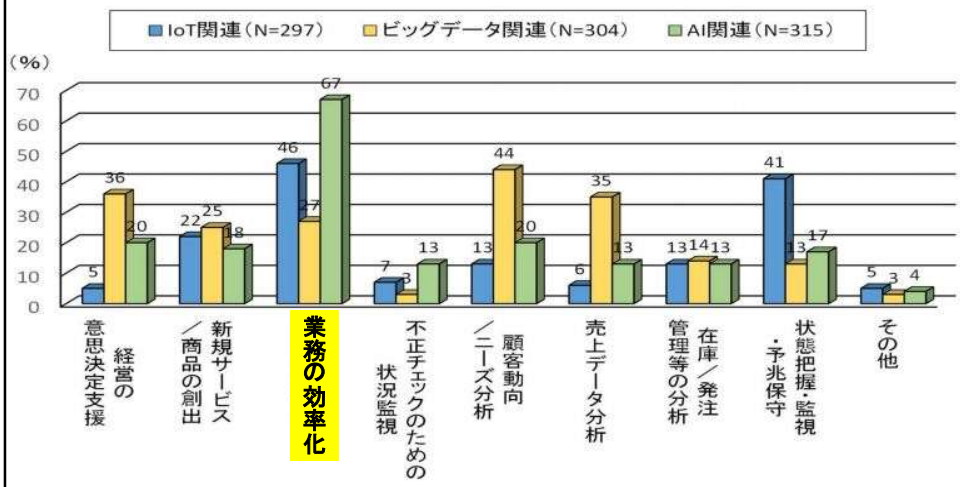


データ駆動型・主導社会に向けて IoT/ビッグデータ/AI



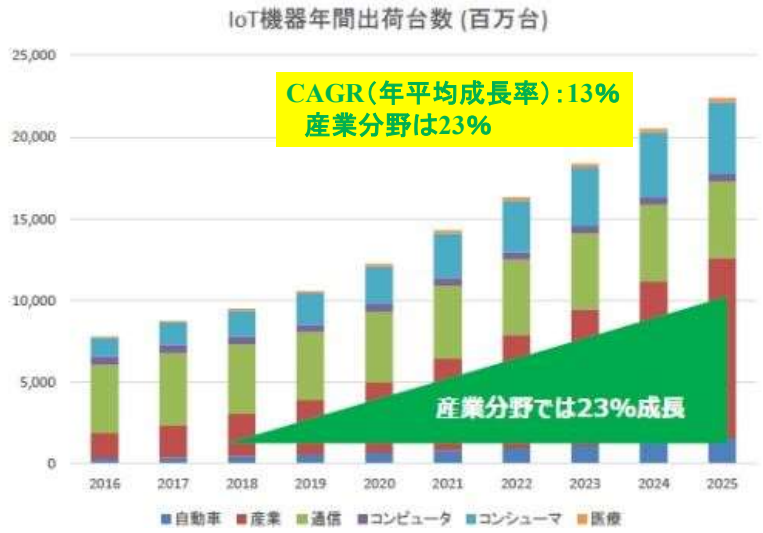
（平成28年
総務省資料より）

IoT/ビッグデータ/AIの活用目的



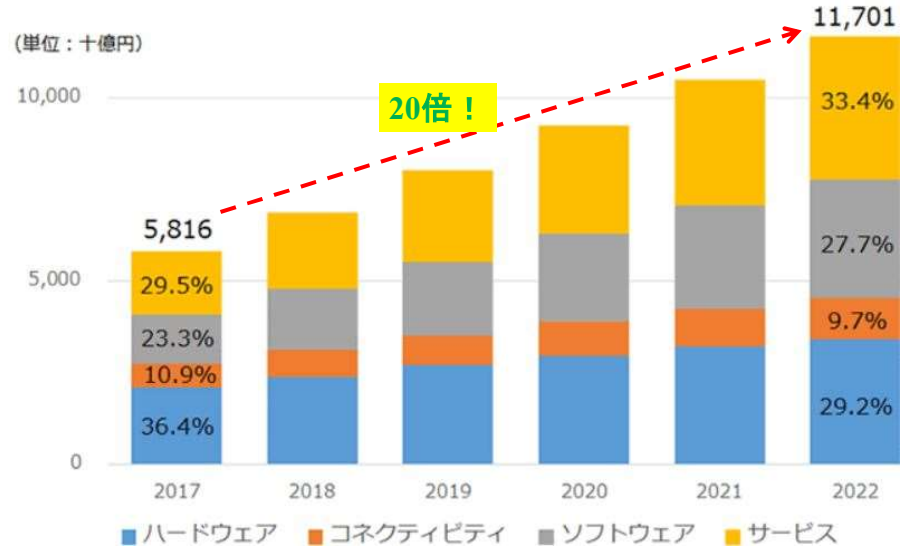
ビッグデータは、「経営の意思決定支援」、「顧客動向/ニーズ分析」、「売上分析」、IoTは、「業務の効率化」、「状態把握・監視」、AIは、「業務の効率化」への活用が期待されている。（JEITAの情報システム部門への2019年のアンケート結果より）

（世界）IoT機器普及の動向



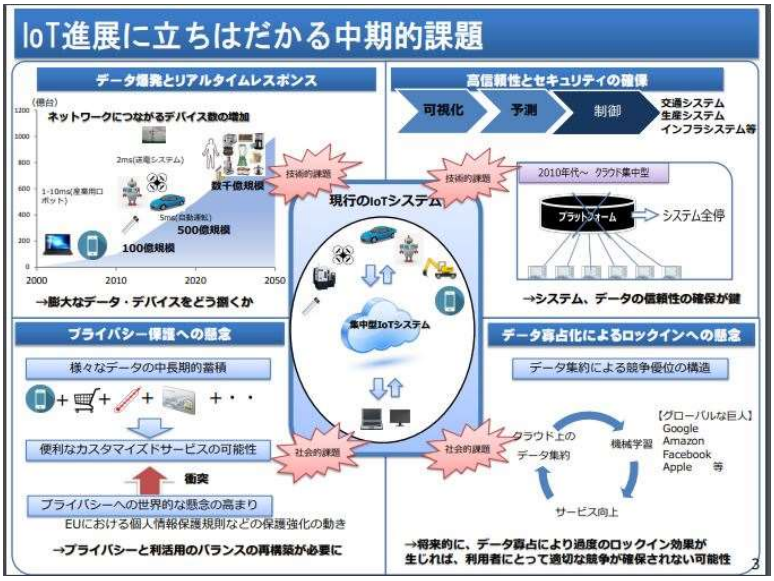
世界の分野別IoT機器出荷実績・予測（IHS Marketの資料より）

（国内）IoT市場動向



支出額予測と技術グループ別支出割合推移（IDC Japanの資料より）

IoTの課題



IoT進展に立ちはだかる中期的課題への新たなアプローチ（METI資料）より

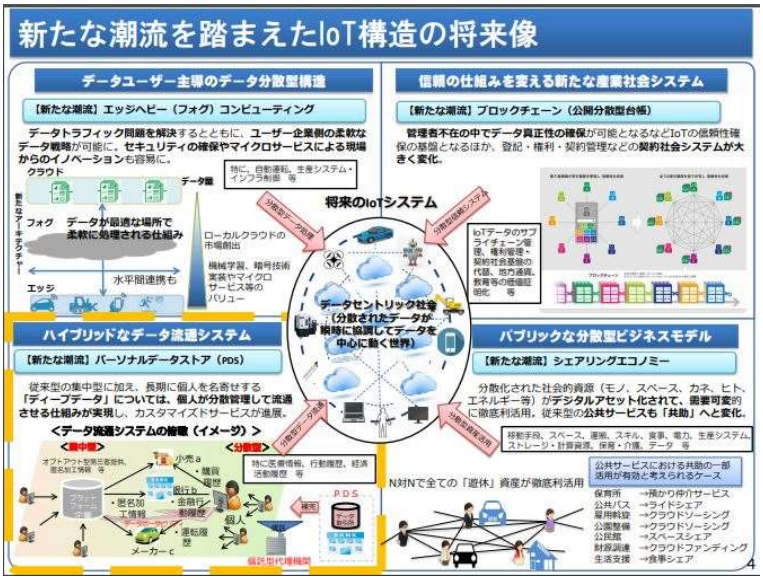
IoTの課題克服に向けて

データ爆発とリアルタイムレスポンス

プライバシー保護への懸念

高信頼性とセキュリティの確保

データ寡占化によるロックインへの懸念



IoT進展に立ちはだかる中期的課題への新たなアプローチ（METI資料）より

IoT＊ブロックチェーンの取組

（１）GMOインターネット（株）他：ブロックチェーンとIoTを活用した
宅配ボックスの実証実験
複数の宅配ボックスにIoTデバイスを配置、ブロックチェーンとIoTをうまく組み合わせて複数の利用者で使用可能に

（２）Nayuta：ブロックチェーンを活用した、
使用権をコントロールできる電源ソケットの開発
電源ソケットの持ち主は、指定した時間帯に何時間使用できるという使用権トークンをユーザへ提供（使用権をコントロールでき、第三者による不正利用（盗電など）がなくなる）

IoTにおけるブロックチェーン活用の可能性（トレーサビリティ）

①組織内で分散発生するデータの維持管理
作業プロセスの可視化、改良・最適化への活用
トラブルへの迅速な対応
データの確実な管理➔複数の分散ノードによる管理
データの真正性の保証➔非改竄性の保証

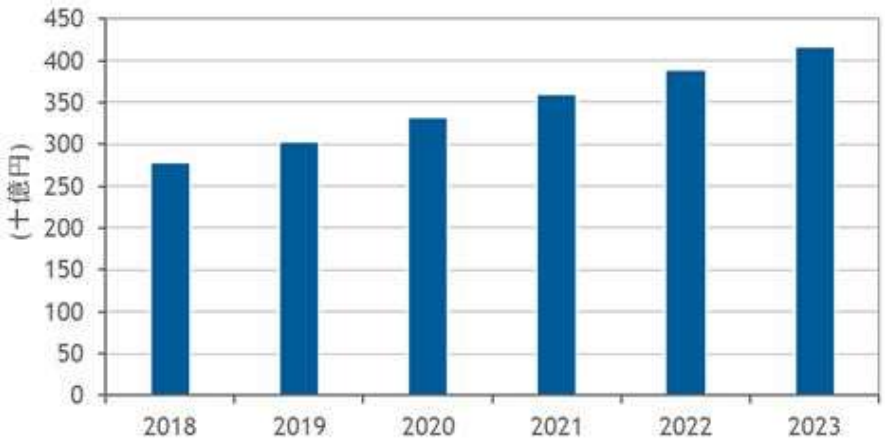
②組織間でのタイムリーな情報共有
全体工程のスムーズな遂行（作業の並列化）
トラブル、クレーム原因の迅速な追求・対処
組織間でのデータの共有➔相互運用性、安価性

③顧客への情報提供（信頼、安心感）、第三者への説明責任

ビッグデータの動向

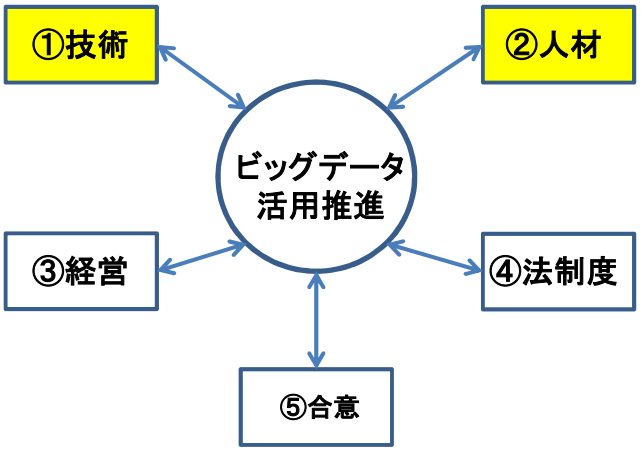
ビッグデータを構成する各種データ（例） 平成24年版 情報通信白書

（国内）ビッグデータ関連市場の動向

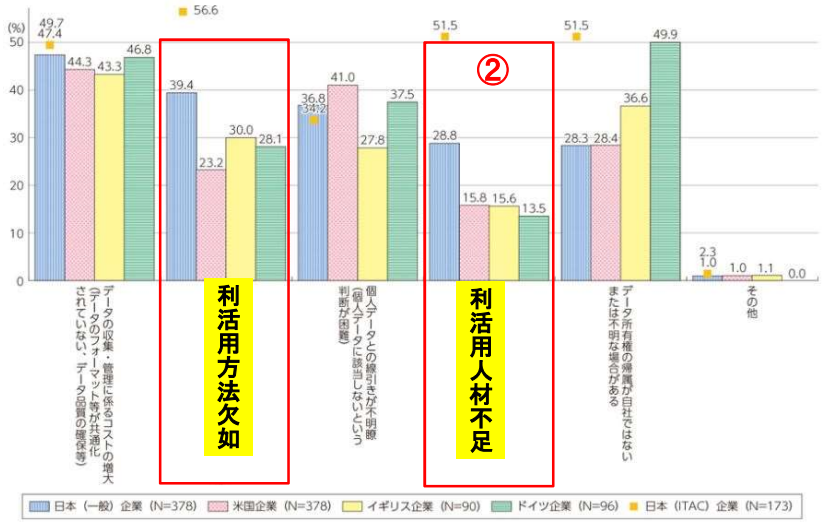


国内BDAソフトウェア市場2018年の実績と2019年～2023年の予測（作成：IDC Japan）

ビッグデータ活用推進を支える基盤・環境



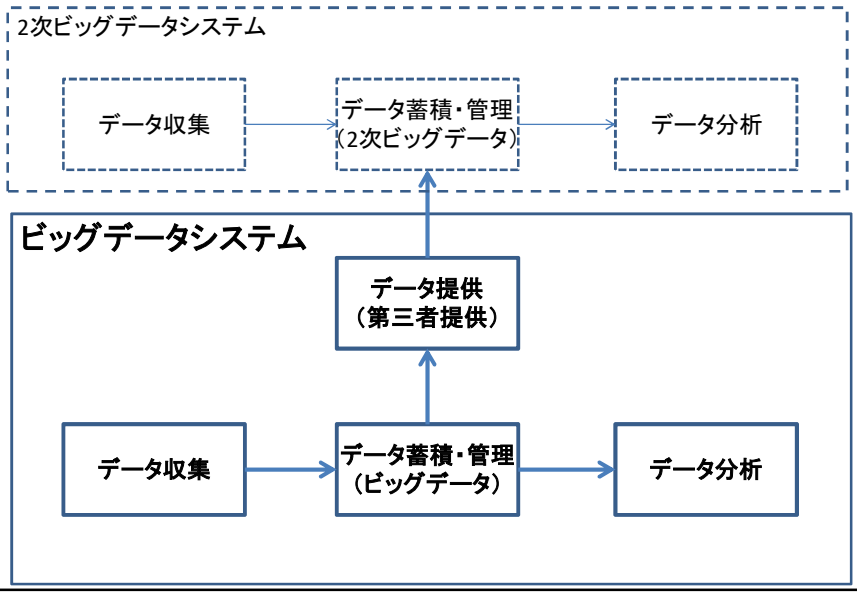
産業データの取扱いや利活用の現在または今後想定される課題や障壁



（出典）総務省「安心・安全なデータ流通・利活用に関する調査研究」（平成29年）

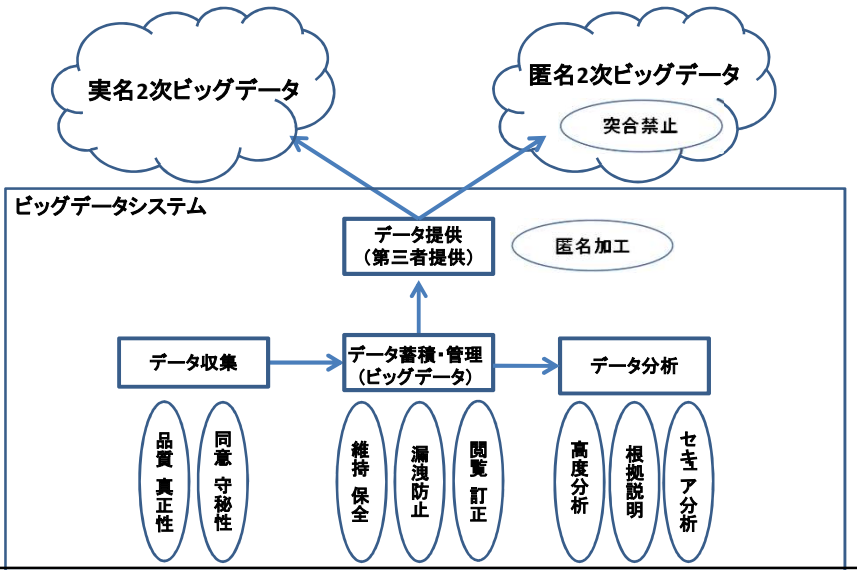
 111

ビッグデータシステム構成モデル



 112

ビッグデータシステムを構成する サブシステムの主要技術課題一覧



ビッグデータ活用推進のための技術

（１）人工知能等による高度分析技術
　　および分析結果の根拠提示技術

（２）暗号化状態処理等によるセキュア分析技術

（３）個人データの第三者提供のための匿名加工技術

（４）集めないビッグデータに関する技術
　　個人のデータは個人の管理下へ（PDS）
　　情報銀行：個人のデータの管理・運用代行

（５）ブロックチェーンに関する技術
　　BigchainDB：分散型DB（MongoDB)に
　　ブロックチェーンの特徴的機能を実装
　　Keyless Signature Infrastructure（KSI）：
　　ハッシュを利用してデータを繋ぐブロックチェーン

BigchainDB（BigData+Blockchain）

開発元：BigchainDB GmbH（ベルリン）　発表：2016年2月
概要：大企業が求める処理能力、大容量、多様な検索・アクセス制御等の
　データ管理機能に加え、ブロックチェーンの特徴機能
　（記録データの不変性、分散コントロール、資産の登録・移転等）を提供
実現方式：ビッグデータ管理システム（MongoDB：NoSQL DBMS）へ
　ブロックチェーンの特徴機能を付加
現状：オープンソースとして公開（機能強化は継続中）
　世界で20社以上がパートナー企業となり、
　　応用PJが進行中（日本企業：リクルート、トヨタ）
　トヨタは、MITのメディア・ラボ、ブロックチェーン技術企業と提携
　　具体的には、TRI（Toyota Research Institute）が主導
　　BigchainDBは、自動運転や自動運転テストの
　　データの安全な共有にための分散暗号化DBとして利用

Keyless Signature Infrastructure(KSI)

開発元：Guardtime（エストニア）
開発：2007年
開発目標：完全性、透明性、監査性を重視
　　ドキュメントのハッシュ値による
　　ドキュメントの非改ざん性の検証が可能
　　（ドキュメントの署名者の検証は別途）
開発事例：エストニアの100万人規模の
　　非改ざん性を検証可能な医療情報DB
開発アプローチ：OracleDBへのKSI add-onの開発

ビッグデータ＊ブロックチェーンの取組

（１）札幌市：ICT活用プラットフォーム『DATA-SMART CITY SAPPORO』
での実証実験
　課題：情報の電子データ化は進んでいるものの、
　　蓄積されたデータの正当性は管理者に委ねられていること
　結果：オープンデータの登録・利用における透明性や、
　　活用時に正しいデータが取り扱われていることを保証する
　　真正性の確保において、ブロックチェーン技術が
　　効果的であることを確認

（２）(株)インサイト：居住用賃貸物件に関する家賃収納代行業務のための
個人信用情報基盤の構築
　目標：学歴、職歴やクレジット情報の利用記録、ローンの返済記録、
　光熱費の利用状況など、個人の住に関するあらゆる情報を記録し、
　新しい個人の信用情報のプラットフォームをブロックチェーンで実現

ビッグデータにおける ブロックチェーン活用の可能性（リライアビリティ）

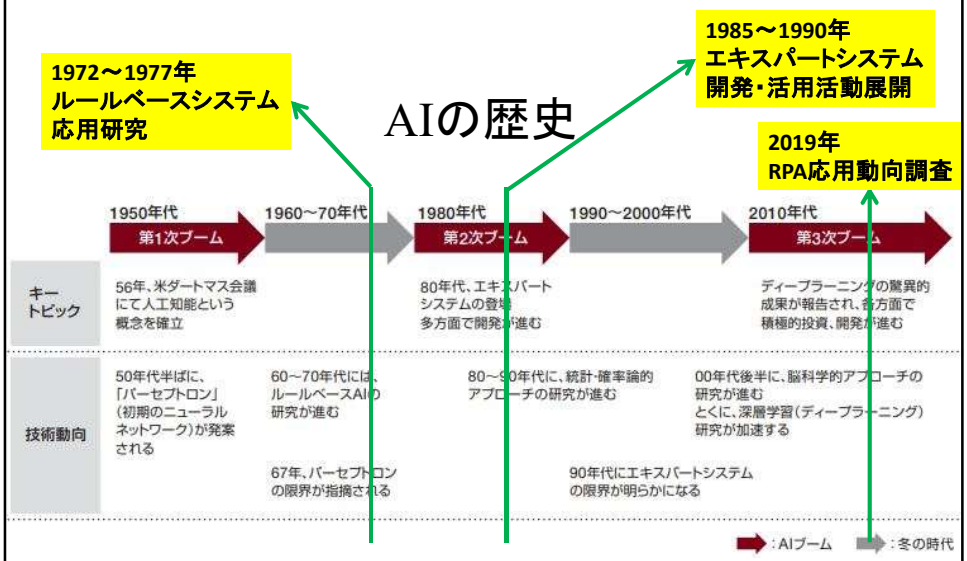
社会及び社会を支えるシステムのデータドリブン化対応
➔誤ったデータの混入による
社会・組織のミスリードや、システムの誤動作の回避

①IoT等で収集されるデータの真正性確認
➔IoT等で収集されるデータの
送信元のなりすまし、受信データの改ざん検知

②サービス中のビッグデータの真正性保証
➔ビッグデータの改ざん検知

③ビッグデータの適切な更新の保証、トラブル対応
➔更新の確実な記録（非改ざん性）

④ビッグデータとしてのブロックチェーン活用



PwCコンサルティング合同会社　Strategy& Foresight Vol.15 2018 Spring

技術レベル・機能によるAIの分類

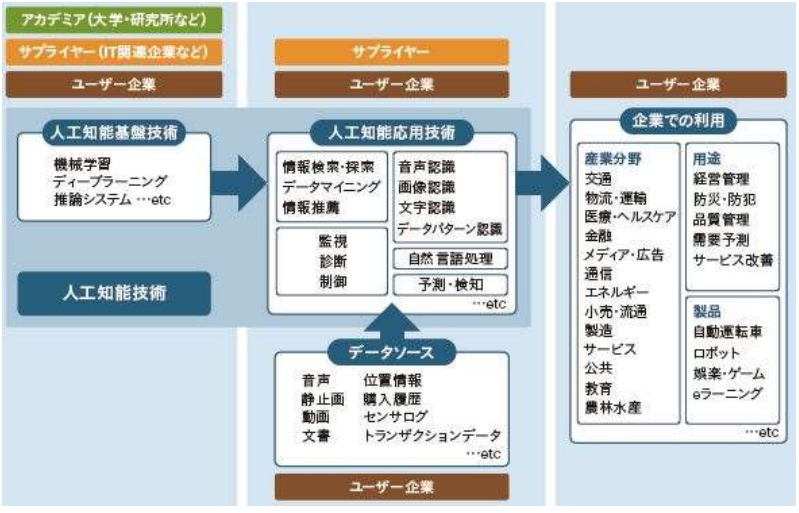
	どのような技術か	実現される機能	事例
レベル1（制御）	従来の制御工学に基づく制御システム	制御システム（厳格なルール）に基づく単純なアウトプット	●"AI搭載"と称される家電製品
レベル2（推論）	「知識」を使ったAI →推論・探索が可能に	インプットされたデータとあらかじめ決められたルールに基づく多様なアウトプット	●質問応答システム ●エキスパートシステム
レベル3（機械学習）	機械学習を取り入れたAI	サンプルとなるデータを基にルールや知識を学習し、新たなインプット（データ）について自動的に判断してアウトプット	●インターネットの検索エンジン ●将棋やチェスのプログラム ●画像認識システム ●音声認識システム ●自然言語処理システム ●ロボット・機械の自律化 ●囲碁のプログラム
レベル4（ディープラーニング）	ディープラーニングを取り入れたAI	人間が介在したりルールを設定しなくても、自律的に特徴やルールを学習し、自動的に判断してアウトプット	

機械学習技術の一種であるディープラーニングの発展により、精度の向上や用途の拡大が見込まれる

- ●画像認識システム → カメラの顔認識・医療機器の画像診断など
- ●音声認識システム → 音声入力など
- ●自然言語処理システム → 自動翻訳など

みずほ情報綜研　[特集] 人工知能の可能性とビジネスへの活用

AIの活用プロセス



みずほ情報綜研　[特集] 人工知能の可能性とビジネスへの活用

AI実現のアプローチ

分類	概要	活用事例	課題
ルールベース アプローチ	人間がルール(条件と答え)を整理し、それをコンピュータに移植する	• 医療診断 • LSI設計 • 金融信用査定	• 例外に対応できない • 新しい事象に対応できない • 0 or 1 で答えを出せないような曖昧な問題に対応できない
統計・確率論的 アプローチ	大量のデータの観測を通じデータに内在する相関関係を統計的手法で分析し、確率として表現する	• Web翻訳 • スマートフォン音声認識 • 車載カメラ画像認識	• AIが真に因果関係を理解していない(データを統計・確率論的に処理しているに過ぎない) • 性能の限界がある(統計・確率論的処理のため、原理的に精度100%は実現しえない)
脳科学的 アプローチ	脳の神経活動を再現する数学モデル(ニューラル・ネットワーク)を使い、データ処理する	• 音声検索、画像検索 • 同時通訳 • 囲碁対局	• 判断の根拠がブラックボックス化する • コントロールが難しい(思いもよらない判断をすることもある) • 膨大なデータが必要となる

PwCコンサルティング合同会社 Strategy& Foresight Vol.15 2018 Spring

AI応用：検知・識別

適用分野	AI導入事例	
画像の意味理解・判別・仕分け・検索	ウェブ画像検索	検索ページに画像をアップロードすることで、類似画像や関連するWebページの検索結果を表示
	画像の仕分け・整理	写真を自動的にカテゴリー分類
	医療画像診断	胃生検、大腸生検等の画像から癌と疑われる領域を自動的に抽出
音声の意味理解・判別・仕分け・検索	音声入力	音声を認識してWeb検索したり、装置の操作を実施
	曲検索	膨大な量の楽曲の学習に基づき、ヒット曲の予測やアーティスト、レコード会社やファンのマッチングを提供

PwCコンサルティング合同会社 Strategy& Foresight Vol.15 2018 Spring

AI応用：予測・判断

適用分野	AI導入事例	
異常検知	クレジットカードの不正利用検知	カードの利用場所、時刻、金額のデータに基づいて不正の有無を検知
定量的予測	タクシー売上・需要予測	人口統計データ、タクシー車両運行データ、気象データ、施設データを分析して、時間帯別にタクシー乗客の多い場所を予測
	与信スコアリング	ユーザーのオンライン行動データをマシンラーニングを利用して分析し、与信判断
定性的予測	商品の自動レコメンド	ECサイトにおいて顧客の「興味や購買意欲が高まる動き」をリアルタイムで予測し、商品をレコメンド
	運転手感情把握	人の表情やハンドル操作、脈拍から運転者の感情、疲労度を把握し、車内の音楽やエアコンを調整
	婚活サイト自動マッチング	婚活行動などの情報に基づき、漠然とした好みを可視化し、成婚率の高い相手をマッチング

PwCコンサルティング合同会社　Strategy& Foresight Vol.15 2018 Spring

AI応用：実行・制御

適用分野	AI導入事例	
表現生成	要約・文章作成	キーワードを指定することにより、インターネット上の情報を参考に、オリジナルの記事を作成
	ロゴデザイン	ロゴを作りたい組織（モノ）の名前やアイコン、色などを選択することで条件に合うロゴを作成
	チャットボット	社内外の問い合わせに対応
行動／作業	柔軟な手作業	ボトルの形状を認識して、自動でキャップ締め作業実施
	乗用車の自動運転	モード切替により自動運転が可能な電気自動車（EV）が登場

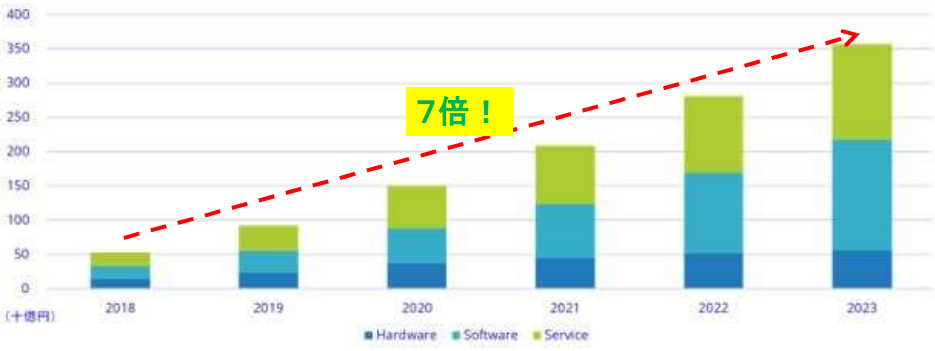
PwCコンサルティング合同会社　Strategy& Foresight Vol.15 2018 Spring

AIで代替しやすい業務要件

視点	業務要件
AI導入による経済効果	業務量が多い／労働単価が高い
	スキル／ノウハウのある人材が不足している
データの存在／入手性	関連データが既に蓄積されている
	データ収集のためのコストが低い
現在のAI技術レベルとの親和性	判断に人間的／社会的常識を必要としない
	対人コミュニケーション能力を必要としない
	感性（芸術的センス）を必要としない
	100％の精度を求められない（結果に対する責任が深刻ではない）

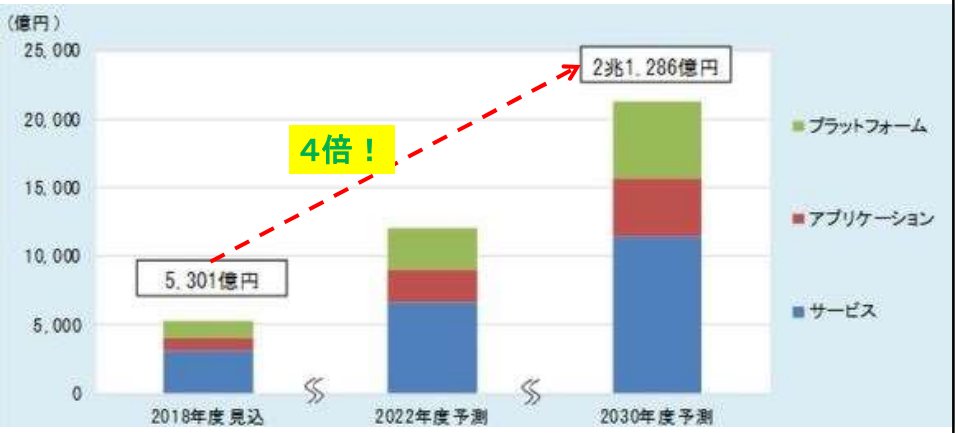
PwCコンサルティング合同会社　Strategy& Foresight Vol.15 2018 Spring

（国内）AIシステム市場予測（2019年～2023年）



「国内AIシステム市場予測、2019年～2023年」（IDC Japan2019年5月21日発表資料）

（国内）AI応用市場動向



「2019 人工知能ビジネス総調査」（富士キメラ総研2019年6月7日発表資料）

AI＊ブロックチェーンの取組み

（1）医療分野：Doc.ai
＊医療情報を暗号化し個人情報と切り離し、
ブロックチェーンを使って医療機関で共有
＊医療情報の分散管理により改ざんが困難（高い信頼性の医療情報）
＊AIを使った診察も目指す、セカンドオピニオンとしての活用も

（2）医療分野：DeepMindと英国民保健サービス（NHS）と病院の連携による取組み
＊DeepMindに大量のスキャン画像と症状を学習させ、
スキャンデータのみから疾患を特定することを目指している
＊個人情報を扱う医療プラットフォームとしての信頼を得るために、
DeepMindはブロックチェーンを活用して暗号化した患者の個人情報をリアルタイムで追跡できる「Verifiable Data Audit」を2017年中に導入すると発表

AIにおけるブロックチェーン活用の可能性

①AI応用におけるブロックチェーン活用

ブロックチェーンによるデータの真正性保証

➔AI応用結果の信頼性

AIの意思決定プロセスの確実な記録・分析過程の説明

➔人によるAI分析結果の追跡・理解支援

②ブロックチェーンにおけるAI応用

ブロックチェーンの分析へのAI応用

ブロックチェーンのスマートコントラクトへのAI応用

➔推論エンジン等のAI技術を応用した
スマートコントラクトの可能性

17:30

おわりに

おわりに

DX：Digital Transformation

①2015年、WEF（World Economic Forum）が
DTI（Digital Transformation Initiative）を発足

②2018年、経済産業省がD X レポート
～ITシステム「2025年の崖」の克服とDXの本格的な展開～を発表

・**既存システムが**、事業部門ごとに構築されて、全社横断的なデータ活用ができなかったり、過剰なカスタマイズがなされているなどにより、**複雑化・ブラックボックス化**

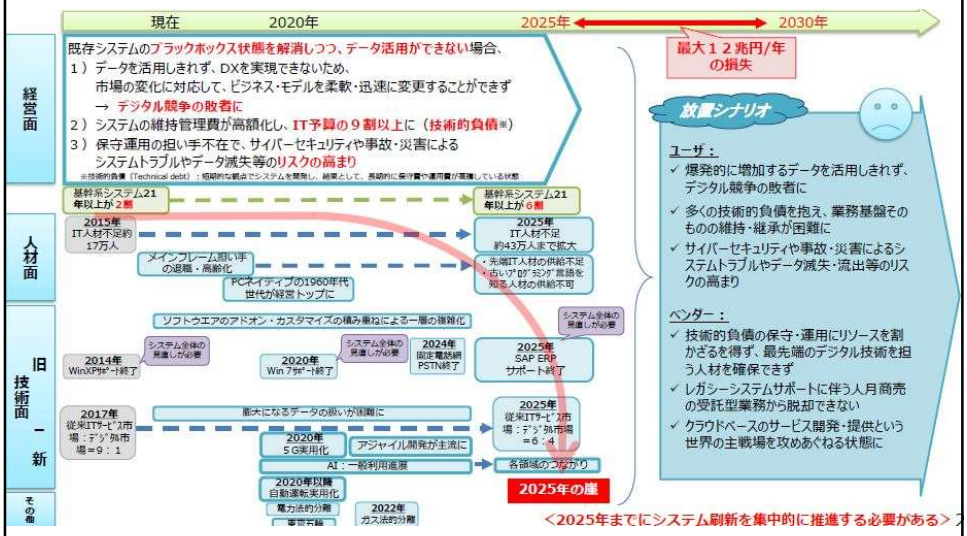
・経営者がDXを望んでも、データ活用のために上記のような既存システムの問題を解決し、そのためには**業務自体の見直しも求められる中、現場サイドの抵抗も大きく**、いかにこれを実行するかが課題

→ この課題を克服できない場合、DXが実現できないのみでなく、2025年以降、最大12兆円／年（現在の約3倍）の経済損失が生じる可能性（2025年の崖）

おわりに

2025年の崖

2025年までにシステム刷新が必要！



経済産業省のDXレポートより

おわりに

 133

日本のDX阻害要因

	グローバル	日本
1	データのプライバシーとサイバーセキュリティに関する不安(34%)(2016 年は 5 位)	**予算およびリソース不足(42%)**
2	予算およびリソース不足(33%)	組織内のスキルおよびノウハウの不足(31%)
3	組織内のスキルおよびノウハウの不足(27%)	**一貫したデジタル戦略とビジョンの不足(24%)**
4	規制および法律の変化(27%)(2016 年は 9 位)	データのプライバシーとサイバーセキュリティに関する不安(23%)
5	デジタル カルチャーの成熟度の低さ(24%)	ビジネスのスピードに見合う適切なテクノロジーの不足(22%)

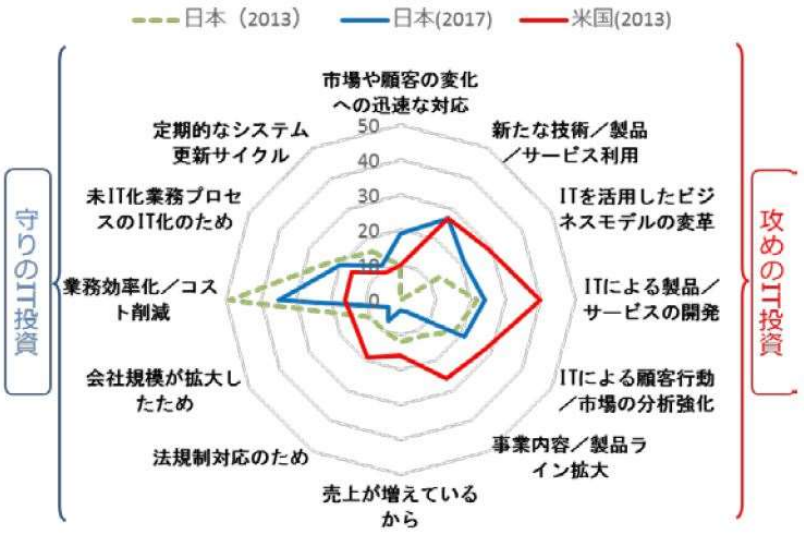
Dellが発表したデジタル変革の状況に関する調査結果

おわりに

 134

IT投資における日米比較

日本は攻めのIT投資へのシフトが必要



JEITAの2017 年 国内企業の「IT 経営」に関する調査結果

おわりに

 135

IT化関連テーマの取組度（10年間の推移）

（JEITAの情報システム部門への2019年のアンケート結果より）

おわりに

 136

DX実現に向けて

①METIの警鐘「2025年の崖」は
システム刷新の壁を乗り越えるチャンス！
ユーザ企業：情報システム刷新PJ立ち上げのチャンス
SI企業：情報システム刷新ビジネス提案のチャンス

②「2025年の崖」を乗り超えるデジタル戦略の策定を！
新たな「事業・業務の現状」把握し
「事業・業務の将来像」（ビジョン）を描き、
「ブロックチェーンを含む新技術」の詳細
およびその動向を把握の上、
デジタル戦略を策定・推進へ

 137

終

（ご清聴、ありがとうございました）

 138

話題：暗号の危殆化

考案された当時の暗号研究の水準やコンピュータの処理能力では容易に解読できなかった暗号アルゴリズムが、新しい攻撃手法の発見やコンピュータ性能の飛躍的な向上により、十分に安全とは言えなくなること

		安全性指標に相当する鍵長・パラメータ（bit）				
		～2010年	2011～2030年	2031年～	2031年～	2031年～
暗号の安全性指標		80 bit セキュリティ	112 bit セキュリティ	128 bit セキュリティ	192 bit セキュリティ	256 bit セキュリティ
共通鍵暗号（AESなど）		80	112	128	192	256
公開鍵暗号 デジタル署名	素因数分解問題に基づく方式（RSAなど）	1024	2048	3072	7680	15360
	離散対数問題に基づく方式（DSA, DHなど）	1024	2048	3072	7680	15360
	楕円曲線上の離散対数問題に基づく方式（ECDSA, ECDHなど）	160	224	256	384	512
ハッシュ関数（SHA-2など）		160	224	256	384	512

https://www.nict.go.jp/publication/NICT-News/1303/01.html

 139

話題：暗号資産（仮想通貨）

順位	名称	記号	時価総額
1	Bitcoin	BTC	$230,770,507,812
2	Ethereum	ETH	$33,345,412,861
3	XRP	XRP	$16,777,509,982
4	Bitcoin Cash	BCH	$7,510,707,733
5	Litecoin	LTC	$7,487,246,142
6	EOS	EOS	$5,423,812,688
7	Binance Coin	BNB	$4,591,788,731
8	Tether	USDT	$3,826,998,216
9	Bitcoin SV	BSV	$3,672,528,567
10	TRON	TRX	$2,269,181,081
11	Cardano	ADA	$1,993,993,065
12	Stellar	XLM	$1,964,580,608
13	Monero	XMR	$1,707,086,953
14	UNUS SED LEO	LEO	$1,575,243,676
15	Dash	DASH	$1,398,306,872
16	NEO	NEO	$1,209,104,010
17	IOTA	MIOTA	$1,095,114,011
18	Chainlink	LINK	$1,089,556,852
19	Cosmos	ATOM	$918,969,744
20	Ethereum Classic	ETC	$875,490,153

2019年7月10日現在2264通貨（資産総額 $355.45 B　約15兆円）

出典：All Cryptocurrencies　https://coinmarketcap.com/all/views/all/

 140

話題：暗号資産（仮想通貨）の課題

匿名性と特定・追跡性の両立が必要だが・・・

匿名性：誰が誰にいくら送金したか、の情報は公開したくない
　一般に、暗号資産（仮想通貨）は一定の匿名性がある：Bitcoin
　匿名性を強化した暗号資産（仮想通貨）も存在：Monero, Zcash
特定・追跡性：犯罪捜査や公平な徴税のためには必要

現状：各国政府で対応が異なる　国際的なルール作りの議論？
　日本：改正資金決済法（2017年）により、「仮想通貨交換業」として
　　のマネロン対策の義務化（KYC）、取引所は登録制
　　匿名性の強い暗号資産（仮想通貨）を取り扱う取引所は未登録

Libra：Facebookが発表した新たな暗号資産（仮想通貨）　2020年発行予定
　各国政府は懸念を表明
　　匿名性の問題、膨大な利用者数（27億人）の問題
　Facebookは、発行を強行しない、と発表したが、開発は続行強いる模様

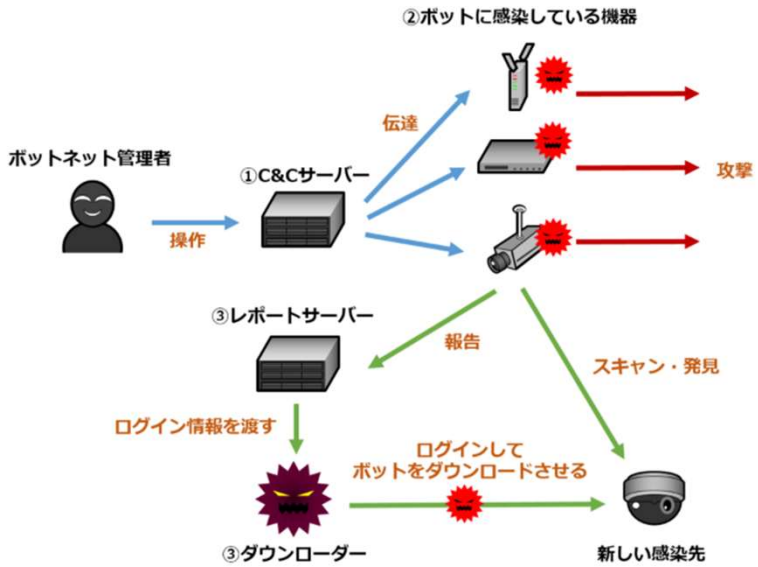
話題：IoTのセキュリティ

Miraiマルウェア（2016年10月ソース公開）
　亜種や新種が次々と蔓延
　初期設定パスワードで使用しているIoTが乗っ取られDDOS攻撃へ加担させられる

カリフォルニア州でIoTを対象とするサイバーセキュリティが成立（2018年9月）
　各IoTに固有のパスワードを事前にプログラムしておくか、初めて
　　アクセスするとき新しい認証コードを発行できるようにすること

日本
「電気通信事業法及び国立研究開発法人情報通信研究機構法の
　一部を改正する法律」が平成30年11月1日（木）に施行
　NOTICE：IoT機器に設定されているパスワードが容易に推測されるもの
　かどうかを確認し、該当する場合、利用者への注意喚起
総務省は「IoT」の普及を踏まえ、端末機器に不正アクセスを防ぐ機能を設けること
　を義務付ける（2020年4月から適用）
　電気通信事業法に基づく端末機器の基準認証に関するガイドライン（2019年4月）

話題：IoT向けマルウェアMiraiの動き



出典：http://www.atmarkit.co.jp/ait/articles/1611/08/news028.html

話題：ビッグデータ活用促進を促す法制度

＊改正個人情報保護法（平成29年5月30日施行）
　個人情報の事前の本人の同意を得なくとも
　　オプトアウト方式による第三者提供が可能
　匿名加工情報の利活用に関する規定を新設
　　個人を識別できないように個人情報を加工し、
　　当該個人情報を復元できないようにした情報
　　第三者提供に
　　本人の同意、オプトアウトの仕組みは不要
＊次世代医療基盤法（平成29年4月成立）
　要配慮個人情報に該当する医療情報も
　　オプトアウト方式により第三者提供可能

話題：データの独占・寡占の弊害を防ぐ法制度（自由な競争環境の確保）

データが大きな価値を持つようになりデータの独占や寡占が企業の競争を制限することにもなりかねないことが懸念

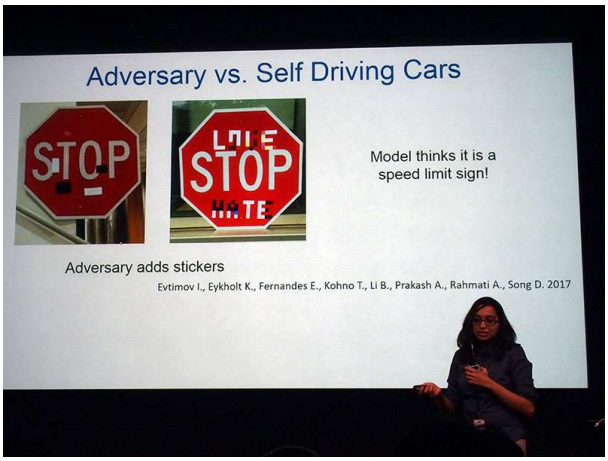
＊OECD：
　「Big Data：Bringing Competition Policy to the Digital Era」
　（2016年10月）

＊公正取引委員会：
　「データと競争政策に関する検討会報告書」
　（2017年6月）
　　＝＞市場での支配的立場を使ってのデータ収集や
　　不当なデータの囲い込みは、独占禁止法の適用を検討

 145

話題：敵対的攻撃 (Adversarial Attack)

画像認識モデルに対して敵対的に生成された摂動が画像に加えられることによって、誤識別が誘発されるというディープラーニングの問題



交通標識に細工をしたステッカーをはり付けるだけで
「停止」の交通標識を「速度規制」の交通標識に誤認識させられた
https://business.nikkei.com/atcl/report/15/061700004/111400232/

 146

話題：ディープフェイク

ディープフェイクとはAIの技術を応用した偽のビデオやオーディオ
「敵対的生成ネットワーク」
（GAN：Generative Adversarial Networks）を利用し生成

GAN：２つのニューラル・ネットワークに訓練データをたくさん与え学習させる。
生成器（generator）と呼ばれる最初のネットワークは、訓練データを見て模倣し手書き文字や動画、音声といった人工的な出力を生成する。
次に、識別器（discriminator ）と呼ばれる第2のネットワークは、各出力を生成ネットワークと同じ訓練データと比較し、出力が本物がどうかを判定。
識別器が生成器の出力を却下するたびに、生成器は最初からやり直す。
最終的に識別器は出力と訓練データとの違いが分からなくなる状態へ。
（模倣と現実の見分けがつかなくなる）

本人と見分けがつかない偽動画「ディープフェイク」がSNS経由拡散し問題
CEOになりすましたディープフェイクの音声で約2600万円の詐欺被害（9月5日）
➔AIによって、高度な改竄技術がより簡単に利用可能となってきた！

講演テーマ：ブロックチェーンの活用展開に向けて
－基本的仕組みの理解から応用パターンの把握まで－
講演者：（株）IT企画　代表取締役社長　才所敏明

講演概要：

新たなデジタル技術を活用して新たなビジネスモデルを創出するDXの必要性が叫ばれている中、新たなデジタル技術としてIoT、ビッグデータ、AIと並び注目されているブロックチェーンについて、その活用展開を進めるにあたり必要な、ブロックチェーン技術の基本的仕組み・特徴、応用パターン・活用事例、IoT/ビッグデータ/AIとの融合等の最新動向を紹介する。

＊暗号技術の発展の歴史と現代暗号の基本的仕組み
＊ブロックチェーンの特徴と暗号技術が支えるブロックチェーンの仕組み
＊ブロックチェーンの分類とそれぞれの特徴
＊ブロックチェーンの応用分野および活用事例
＊ブロックチェーンおよびIoT/ビッグデータ/AIとの融合に関する取組み（最新動向）