パネルディスカッション②「ブロックチェーンの安全性と汎用性を考える」

【登壇者】

楠 正憲（くすのき・まさのり）
ヤフー株式会社 CISO-Board ／国際大学 GLOCOM 客員研究員

榊原 彰（さかきばら・あきら）
日本マイクロソフト株式会社 CTO

佐野究一郎（さの・きゅういちろう）
経済産業省商務情報政策局情報経済課長

高城勝信（たかぎ・まさのぶ）
日本 IBM 株式会社ブロックチェーン・アーキテクト

松尾真一郎（まつお・しんいちろう）
MIT メディアラボ研究員　※遠隔参加

【モデレータ】

高木聡一郎（たかぎ・そういちろう）
国際大学 GLOCOM 主幹研究員 / 准教授

【高木】このパネルディスカッション②では，ブロックチェーンの安全性と汎用性を考えます．最初に，安全性とか課題について議論していきたいと思います．次に，汎用性・可能性ということを議論して，最後に皆さんからの質問にお答えする形で Q&A のセッションを持たせていただきたいと思っておりますので，どうぞよろしくお願いいたします．

では最初に安全性・課題ということで議論をしていきたいと思うのですが，先ず松尾さんから話題提供をいただいて，そのあと楠さんから 5 分ほどお話をいただき，そのあとはディスカッションに入っていきたいと思います．それでは松尾さんから，お話をいただけますでしょうか．

【松尾】私はシリコンバレーに住んでいるんですが，MIT メディアラボの研究員をしております．MIT メディアラボは去年（2015 年）の 4 月にデジタル通貨イ

ニシアチブという，暗号通貨とブロックチェーンの研究をする部署を立ち上げたのですが，そこと一緒に仕事をしているというようなバックグラウンドを持っています．私自身はもともと暗号の研究者をずっと 20 年以上やっているという立場です．安全性について 5 分くらいで問題提起してほしいということを言われていたので，スライドは用意していないんですけれども，口頭で考えていることを説明したいと思います．

まず，安全性を含めて，ブロックチェーンって，何が技術的に整っていると本当に良いブロックチェーンなのかっていうことが，実はまだ定まっていないというのが実情だと思っています．非中央集権的に物事を決められるとか，セキュリティとか，プライバシーとか，スケーラビリティがこれくらいなきゃいけないよとか，いろんなことを実は満たしていかなきゃいけないんだけども，普通の情報システムでさえ，たとえばセキュリティと性能というのはトレードオフの関係にあります．ブロックチェーンに関していうと，非中央集権的にどれくらいしなきゃいけないのかといったようなことについて，トレードオフの関係が大体六つくらいあって，それのどれにすればいいのかということが実はよくわかっていないんですね．そのどの辺に，良いバランスをとっていけばいいのかということがユースケースによって異なっていて，たとえば取引所で実験をした時とビットコインだと，多分全然要件が違ったりするわけですね．多分，すべてを 100% 満たす解は存在しなくて，ユースケースによって異なり，条件に従ってチューニングをしていくというのが本当の使い方なんだと思うんですけれども，たとえば一番実績のあるビットコインのブロックチェーンでも，どこがブロックサイズの適切な落としどころなのかで 2 年以上もめている，というような状況があることを考えると，全然まだそれが理論的に見えていない．一つひとつのセキュリティとかプライバシーとか性能ということに関してどれくらいあればいいのかということを，まだまだこれから議論しなきゃいけないというところです．

私の専門分野のセキュリティについて考えてみると，たとえば，ブロックチェーンという暗号技術を使ったプロトコルなんですけど，暗号プロトコルの数学的な証明とか安全性の証明ってすごく難しくて，ブロックチェーンに関してもまだされていないんですね．ということは穴があるかもしれないというのが，まず言えるわけです．

個別の暗号技術についても実はまだ不安要素があって，たとえば，楕円曲線暗

写真左から，高木，榊原，松尾 (Skype 参加)

号を使っているんだけれども，そのパラメーターって本当にこれでいいのかとか，中期的に言うとハッシュ関数っていうのが 20 ～ 30 年すると結構破れる運命にあるんですけども，それが本当に良いのかとか．長期的に言うと量子計算機が出た時にどうするのかということを，誰も考えていなかったりとか．The DAO の件でもそうなんですが，たとえば実装は本当に安全なのかとか，鍵管理って本当にちゃんとされているのかというと，全然考えられていなかったり．ハードウェアのウォレットも，今，結構売られていたりしているんですけど，ああいうハードウェアセキュリティ製品は，たとえば ISO 15408 の認定とかを取ってるものが IC カードは多いんですが，それがちゃんと動くのかという意味では，まだまだ考えられていないということです．

もう一つのキーワードに，トラストということをここで挙げたいんですが，ブロックチェーンってトラストレスというキーワードが出てきます．これは信頼すべき第三者みたいなのがなくてもよいという意味で使っているんですけれども，実際は，それは多分ブロックチェーンでトラストっていうのを全ノードの過半数で分担しているので，トラストレスという言い方はちょっと誤解を招くんじゃないかなと思ったり．あるいは，行動とか運用をどう信頼するのかというところを，多分，考え直さなきゃいけないんだと思っています．

あとは，ビットコインも結構問題は複雑でして，オリジナルのサトシ・ナカモトの論文というのがあるんですが，たとえば中国の国内にいるマイニングをする人が，7，8 割のマイニングパワーを持っていて，それがグレートファイアウォー

ルの裏にあってなかなかその情報が洩れてこないっていうのは，想定外なんですね．もともとの論文からすると想定外なんだけどもこれは解けていないとか，あるいはもともとナカモト論文では，交換所を通じて円と交換するみたいなことは想定されていなかったと思うんですが，実は交換所というのは，そういう意味だとビットコインが想定していなかった単一障害点になり得るという意味だと，そういうことも含めて，実は，その信頼というのを考え直さないといけないなと思っているところです．

ということで，私が結構いろんな人に言っているのは，基本的には私自身はパブリックブロックチェーンについてもっと研究すべきだと思うんですが，これからまだまだ理論とか議論を積み上げていかなきゃいけないというのが現状かと思っています．

【楠】松尾さんの話を引き継ぐ前に簡単に自己紹介させていただきますと，もともと学生時代から電子マネーを研究していて，『日経デジタルマネーシステム』とかで書いていた時期もあって，卒論も電子マネー発行体の収益構造とかで，卒論では大きなシニョリッジ（seigniorage）は期待できないって書いたんですけど，どうもビットコインの作者は相当儲けているそうだと．これは一体どういうことだというので 2013 年くらいからだいぶ勉強して，マウントゴックスの事件の時とか最近だと The DAO のことでも解説の記事なんかを書かせていただきました．

すでに松尾さんからだいぶお話がありましたが，正直言ってビットコイン，ブロックチェーンの安全性というのは，まだ学問的にはあまり詰められていない状況にあるというふうに認識をしています．とはいえ，1 兆円近くの時価総額を持っていて，6，7 年の間も運用しているということは，ビットコインそのものは相当安全なんだろうなというような，経験的な知は持っていると．ただ，ビットコインの安全性が，すなわちブロックチェーンの安全性と言えるのかというと，私はかなり怪しいと思っています．

特に，なぜビットコインの安全性をなかなか学術的に説明できていないかというと，根深い哲学的な問題があると思っていて，ビットコインというのは運営者がいない脱中心的な貨幣システムを作っていこうという取り組みですけれども，暗号において追求されてきた安全性というのは，むしろ現実の権力構造をどうやって電子の上に持ち込んでいくか，現実のヒエラルキーをどうやって持ち込ん

でいくかというところからスタートしているので，これまでの学問上こうやれば安全だよと言われてきたことを意識してビットコインはやっていないという部分があると．それはつまり，選んでそうしていることなので，ここの上でどうやって安全性というのを新たに定義していくのかということを考える必要があるんだと思う．

同時に，逆に言うとパブリックチェーンとしてのビットコインの安全性というのは，先ほど説明があったように過半数の計算能力がある程度正しい目的で用いられているということに支えられているわけですが，裏を返すと後から同じ仕組みを作ったとしても安全ではない．なぜなら一番計算能力を持っている人が他にいるわけだから，簡単に乗っ取ることができる．ブロックチェーンのコンセンサスプロトコルのところなんかが一番問題になったり，何のためにコンソーシアムチェーンを作らなきゃいけないかというと，もう乗っ取られることはわかってるから乗っ取られないようにアクセス制御をしなきゃいけない．そういう話だというふうに理解をしていますし，ビットコイン以外のオルトコイン（Altcoin）なんかは，あまり安全性が検証されていないアルゴリズムをわざわざ使っているんですが，それはなぜかというと，同様にビットコイン用のマイニングの機械が持ち込まれると一瞬で乗っ取られてしまうから，それがないように実績はないけれどもアルゴリズムを ASIC（Application Specific Integrated Circuit）に載せることが難しい，SHA-2 とは別のメモリをいっぱい食うようなアルゴリズムを作らなきゃいけない．そういう現実の制約の中でやっている．

そういったなかで，やっぱりビットコインってすごく出来てるんですよ．もともとブロックチェーンはビットコインのために作られていて，逆にブロックチェーンを設計したサトシ・ナカモトは，ブロックチェーンは何が苦手かということをわかったうえでビットコインのいろんな周辺のルールを作っている．たとえば，プライバシー，アクセスコントロールは全くないということをわかっていて，「でもアドレスの持ち主がわからなければ匿名性は確保できますね」ということが論文で書かれていますし，あるいはファイナリティがない，つまり取引が完全には確定しないという問題に関しても，それでいいじゃないと．結局，ビットコインを，たとえばアンダーグラウンドの目的で使おうとしている人たちにとっては他に選択肢がないわけだから，別にファイナリティがないからブロックチェーンを選ばないということはないわけです．

写真左から，楠，佐野，高城

先日，The DAO の流出事件に対してハードフォークが決断されたということがありましたが，おそらく現実の銀行のシステムなんかでは，たとえば差し押さえであったりとか，間違った送金の組み戻しとか，いろんなことを実装していく必要が出てきますけれども，ビットコインにはそういう仕組みはないですし，あるいはきちっと安全性を担保しておくために鍵をちゃんと管理しなければなりませんが，その仕組みも用意されてないと．できるかできないかではなくて，ブロックチェーンという仕組みの外側であるということがある．多分ブロックチェーンを設計したサトシ・ナカモトは，ものすごくブロックチェーンの弱点を知り尽くして，それでも動く仕組みとしてビットコインを作っているというところが非常に面白いのかなと．

逆に言うと，運営者がいない世界を作ろうとするから難しいものがいっぱいある．たとえば，銀行とかいろんな機関で単に分散台帳として使いたい場合には，その鍵管理は従来通り集中型でやるとか，ビットコインとは別の選択がいろいろできるわけで，こうやってシンプルに考えていけば，ブロックチェーンの影響を受けた分散データベースというのはいろんな形で作っていけるでしょうし，今後そういったブロックチェーンにインスパイアされたデータ構造だとかシステムの作り方というのはいっぱい出てくるだろうと．それをブロックチェーンと呼ぶ人も出てくるとは思います．

特に，これまでの情報システムはデータ中心ではなく業務が中心で，業務を動かしていくためにどうやってデータやシステムを組み立てていくかという世界で

したけれども，ブロックチェーン，ビットコインの世界が先で，ビットコインのデータ構造とそれに繋がっていく情報システムがあって，最後に業務フローという順番．おそらくたくさんの異なるシステムを繋げていくうえでは，そういったビットコインのようなシステムの設計の順番がとても面白くて，テストの工数を減らしたり，信頼性を上げていくにも役に立つはずなので，そういった応用というのは今後増えてくる．おそらくそのブロックチェーンを取り巻くアーキテクチャがこれからの情報システムに与えてくる影響というのは大変大きいんじゃないかと思います．以上です．

【高木】ブロックチェーンそのものの安全性というのはなかなかまだ検証されていない，非常に未成熟なものだというお話がありましたが，未成熟なものとどういうふうに付き合っていくか，そこで何をしなければいけないのかという話と，またその未成熟であるとか完全に成熟するということはおそらくないでしょうから，何か問題が起こった時にどうやってそれをリカバリーできるのかという，そういった論点もあるのではないかというふうには思います．ここから二人のお話を受けて，自由に議論をしていきたいと思います．

【榊原】もうちょっと違うレイヤーの話をさせていただきたいんですけれども，スマート・コントラクトを書けるってこと自体が問題なんじゃないかという気もしておりまして，要は，すごく自由度が高いということが一つリスク含みであると．要は，チューリング完全がどうだとかよく言われますけれども，つまり何でもできちゃうということですから，チェーンが伸びて改ざんできるかどうかということはまた別としても，ブロックに瑕疵が含まれてしまうということは十分考えられると思うんですね．瑕疵が含まれたものがそのままずっと潜在的なバグとして残ったままチェーンが繋がっていって，ある何らかのタイミングでそれが顕在化するといった時に，「じゃあどうすればいいんだ？」ということって，その暗号化云々という基本的なアーキテクチャの上にある層のところで，もうそういった脆弱性が発生するっていう可能性，リスクはあるかな

というふうに考えています．

【松尾】おっしゃる通りで，The DAO の件とかも，あれからいろいろ指摘されている Solidity というスクリプトを書く仕組みがトランザクションを書くのには向いてない仕組みになっていて，そういう意味ではイーサリアムでいろんなトランザクションを書いていく時のプログラム言語のあり方をどうするべきかということを，もう少し練っておいたほうがよかったのではないかということが指摘されています．今，その改良も検討されていますし，その Solidity で書いたスクリプトをチェックするチェッカーみたいなものも最近出てきているので，多分そこは一つよくよく考えなきゃいけないところかなと思います．

つまり，前々からいろんなブロックチェーンのプロジェクトをやる時に，実践の金融システムを触ったことがない人がやっているのは危険だということを言われたことがあるんですけれども，今回そのトランザクション処理をどうするべきかという知見を持った人がもう少しこの世界に飛び込んでこないと，まだ危険かなという気はします．

【楠】おそらくブロックチェーンの持っているデータ構造の安全性と，その上で扱うデータの安全性の議論は，まず分けなくてはいけなくて，スマート・コントラクトが実際にイーサリアムとかハイパーレッジャーとかブロックチェーンとともに普及しつつあるなかで，ここの信頼性の問題は避けて通れないというふうに思います．一方で，契約書を起草した人間の書いた文言というのが，その起草した人の意図に常に合致しているかというと，紙の契約書でさえそうでない場合って結構あると思うんですね．契約した時にはこんなつもりじゃなかったということが現実にはいっぱい起こっている．だからその時に文言の「てにをは」を優先するのか，その両者の中でのコンセンサスを優先するのかは，最終的には裁判でこれまでの社会のルールでは決めてきたと．

おそらくそのスマート・コントラクトの問題の解き方っていろいろあって，できるだけ記述を厳密にしていったり，機能を減らすことによって，そういったギャップが起こることを防いでいくというのが一つのアプローチとしてあると思うんですけれども，社会システムとして考えていく場合には，最終的に意図と異なる契約が結ばれてしまって，それが何かの問題を起こした時の調停の仕組みと

いうのをどういうふうに考えていくかというのは非常に重要だと思いました．そういう意味では，ブロックチェーン自体は過去のある時点のスナップショットにデータを戻すには向いているデータ構造を持っているので，あらかじめ設計の中に，お互いの意図が異なっていた場合や事故が起こった場合の例外の処理の仕方についてきちっと組み込んでいくということが，将来必要になってくるのかなと思います．それは特に The DAO 事件でも非常に明確になったことの一つだと思います．

【榊原】そういうことを考えた場合のもう一つの問題点としては，そのスマート・コントラクトに携わる全員がそのスマート・コントラクトを理解できるかという問題になって，契約書は読んで文言を見ればわかるんですけれども，「Solidity を見るの？」という問題がある．大体，なぜスマート・コントラクトなのに「Hello World」と書けちゃうんだっていう，そういう変な問題があるんですが，それは機能を絞ったり制約をかけるとか，その事前事後の条件を何か作るとか，そういったことでかなりプロテクトはできると思うんですが，そもそもの内容理解ということに対するハードルをどう越えていくかというのは，すごく難しい問題だと思います．その辺は何か策があるのでしょうか？

【楠】多分，契約書も法律も読めた気になっていますが，たとえば『ワークブック法制執務』などを読むと，「及び」と「並びに」の違いのような日本語とかけ離れた記号論理っていっぱいあるので，契約そのものが内在しているその論理性と，いわゆる自然言語として読めてしまうことのギャップというのはあると思うんですが，それは昔のもともと文字が読めない人がいっぱいいた頃から法律であった識字率の問題とかとあまり変わらないと思っていて，社会システムとして契約書を書けない・読めない人であっても社会に参加できるように，代書屋の仕組みをはじめとしてきっちりと社会全体で支えていく必要があるんだと思いますし，スマート・コントラクト技術の競争の中でより可読性が高く，間違いが起こりにくいような文法やコーディング規約を作っていけるのか．あるいは，特殊で非常に高機能なスマート・コントラクトを使う人たちに対して，弁護士のような，あるいは司法書士のような国家資格が必要なのかどうか．そういうことは，将来ひょっとしたら議論になるのかもしれないと思います．

ただ，現実の契約というのも，各国の法律という異なるラグタイムの上でどう解釈するかとか十分に複雑な世界に入っていて，それがスマート・コントラクトによって著しく異なる状況になるかというと，その問題は，実はすでに生命保険の契約を結ぶ時にあの約款で自分がいくら貰えるのかを正確に計算できる人は多分いらっしゃらないし，実はあの紙の契約書に書かれていない保険会社のCOBOLのプログラムの金利の計算の仕方までを意識しなくても我々は現実には生命保険の契約をしているので，そういった情報の非対称ななかでの契約行為というのは今もあって，スマート・コントラクトの時代もあるのかなというふうに思います．

【佐野】最後は司法が介入するということですが，The DAOのケースでもありましたように，将来的には本当に必要が生じれば集団訴訟などの形で，ハードフォークを司法の決定で強制的にやるというようなことも考えられるのではないかと思ったのが一つです．

それから，高木さんが二つのアプローチとおっしゃいましたが，未成熟なものをどう高めていくかというのが一つ目でありますが，我々経産省が出したレポートの中では，暗号技術者とかそういったアカデミアとどう結びつけて，その中でどうコミュニティを作って高めていくかという話だと思っていまして，二つ目のアプローチとして，ある種そういうものとして割り切って使っていくということについては，スペックを明確化していくことによって，それを前提として利用者が気を付けて使っていくことだというふうに思っております．

【高城】The DAOの件が非常に衝撃的だったんですが，ものづくりの観点からいくと僕はスマート・コントラクトが書けるブロックチェーンに出会った時に，ITをやっている方だとわかると思うんですが，機能要件と非機能要件，インフラのセキュリティだとかパフォーマンスだとかそういうところを担う非機能要件だとか，その上につくる今言っているようなスマート・コントラクトの業務を担うようなところ，機能要件的なところを分離できているというのが非常に素敵だなというふうに思いました．

何を言っているかというと，前半の松尾さんの話だと，プラットフォームのセキュリティの問題を考えるということと，後半のスマート・コントラクトをどう

プログラミングするかということに分離できるので，そうやって分離して，たとえばプログラミングだったらアンチパターンをちゃんと研究するだとかですね．

The DAO の件は，もともとそのバグがわかっていたのに放置していたという話もありますが，あれで思ったのは，アセットが盗まれないような仕組みはちゃんと誰がプログラミングしても問題ないようにしましょうというような基本的なルールは，きちんと研究して，教育するというようなことが大事なのかなと思いました．

【高木】ありがとうございます．皆さんにお伺いしたいのですが，たとえば iPhone にアプリを提供する時にはアプリの審査を受けなければいけないということがあるわけですが，そのような感じでスマート・コントラクトをやるにもどこかに認証を得なければいけないみたいなことっていうのは，思想としてどうなのでしょうか．

【榊原】それだと全然 Decentralize されていないですね．現実社会をただデジタルにしただけという感じになってしまって，全然非効率．「その認証するところの信頼はどうなるの？」というところがある．最後まで解けない形で残ってしまうと思うので，あまり良い策とは思えないです．

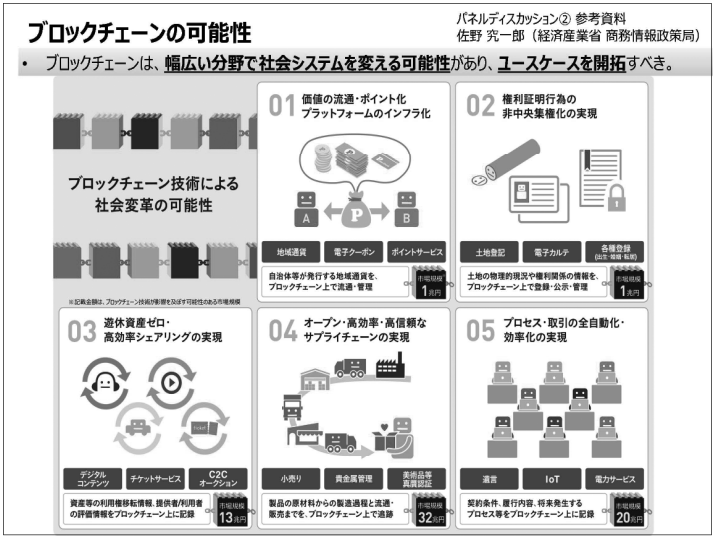
【楠】今の意見と全く同感で，契約の面白いところって，いくつもの読み方がある中で，それぞれの相手方に寄り添う人がいて，手続きの中で決めていくというところが大事なのであって，契約書の読み方を契約の相手方に聞くというのは日本だとよくあることですが，多分，契約社会の米国的な考え方で言うと，これは自分の弁護士と相談すべきことだと思うんですよね．ただ，日本ってたとえば法律の解釈もすぐその法律を所管している役所に聞いたり，ソフトウェアのライセンスをそのソフトウェアを作っているところに聞いたりという慣習があるので，気持ちとしてはわかるし，そういうサービスが出てくるのかもしれないですが，本質的には専門性を持ったエージェントをきちっとお願いできるような状況があって，それぞれの側に立った人たちの間できちっと衝突を解決していく仕組みというのがとても大事だと思います．

【松尾】同じだと思うんですが，多分そのエージェントにいろんな経験値を積み上げていく必要があって，The DAO の件は結構衝撃的に起きたんですけど，個人的に言うとそもそも 150 億円くらいを扱うというのは，実践投入するには早いわけですよ．インターネットの技術を作った時って，結局，10 年とか 20 年，お金と関係ないところでサンドボックスを作って遊んでて成熟させたというところが結構大きかったんですけれども，今，ブロックチェーンに関して言うと，そういうのを飛ばして実践投入されているのは若干不幸で，ただ，今，日本だけじゃなくて海外の金融規制当局とかもサンドボックスを作っていて，いろんな実験をしましょうと．日本の会社も実験をやっていますけど，そういうサンドボックスを使って実験しましょうというところから積み上げていって，最後にそういう専門家だったりとか判例だったりとか経験値みたいなものが出来上がってくる，というふうに考えて，あと数年それにみんないそしむというほうが，まっとうな進化をするんじゃないかという気がします．

【高木】まだまだ経験が必要だということですね．それではそろそろ後半の議論に移っていきたいと思います．後半ではブロックチェーンの汎用性・可能性ということで，どういったところに使っていけるのかということも議論していきたいと思います．経済産業省の佐野課長，それから日本 IBM の高城さんに 5 分ずつ簡単にお話をいただければと思います．

【佐野】今年（2016 年）の 4 月末に（経済産業省より）公表させていただいたものでございますが，（ブロックチェーンユースケースの可能性について）大きく五つに分けております．高木さんは（基調講演の中で）三つに分けていて，そっちのほうがわかりやすかったなと思ったんですが，これは五つの類型で，それぞれ重なり合う部分も当然あります．実用化が進んでいくのではないかという順番に意識的に並べております．

まずユースケースとして 1 点目ですが，価値の記録化，それが流通するというもので，ここに書いてあるように地域通貨とか電子クーポン，ポイント的な



ものです．これは比較的実用化が近いのではないかということです．それから２点目は，手続きコストが非常に低い形で証明行為がされるということで，登記とか船荷証券とか，こういったものの実用化が進んでいくんじゃないかというふうに思っております．それから３点目が，資産の移転を細かく管理ができるということで，シェアリングみたいな世界でもありますし，自律分散的なｎ対ｎの取引みたいなもので，エネルギーの世界でもアグリゲーターがいなくても（取引が）できるような仕組みを作るというものです．それから，４点目ですが，信頼できるトレーサビリティとか透明化ということで，サプライチェーンの管理ということであります．最近ちょっと注目しておりますのは，セキュリティが十分でないという議論もありますが，広い意味でのセキュリティ，トレーサビリティが管理されることによって，特に国家の文書管理みたいなもののなかで，広い意味でのセキュリティ確保というものにも貢献するんじゃないかということです．最後の５点目は，まさにイーサリアムとかスマート・コントラクトの世界で，プロセスが自動化されて，ここはまだ少し見えてない世界でありますけれども，IoT（Internet of Things）の世界で各デバイスがマイクロペイメントとセットで自律的に動いていくような世界．これは私も大きく期待をしておりまして，ADEPT（Autonomous Decentralized Peer-to-Peer Telemetry）みたいな話であり

ますが，大きくこの五つに期待をしているというところです．特にこの５点目はIoTの進展に伴って，どう転ぶかまだ正直見えない部分もありますけれども，私どもとしては期待をしているということでございます．ちなみにこの67兆円という数字が結構一人歩きしているのですが，実はもっと大きいかもしれないですが，関連する市場の数字ということで手持ちの数字であるものを計算すると，こういう数字になったということです．

【高城】 高城です．お手持ちの資料（当日配布資料）と大体同じ事が書いてあります．IBMのほうでまとめているものと，一般的にこういうところでユースケース適応できるだろうなというものをまとめているのと，経済産業省さんのまとめられた内容と，ゴールドマン・サックス（Goldman Sachs）がPDFで出している「Profiles in Innovation」★1というものと，その辺を見ながらジェネラルな形で，私の責任でこうまとめました．

三つくらいにまとめられるとわかりやすいのでしょうが，総花的に書いています．注目するところは，やはり仮想通貨です．今，本番でちゃんとビジネスができる市場になっているというのは，やっぱり両替所かなというふうに思っています．これは皆さんそう思っているとは思うんですが，ビットコインは国内取引高が大体今年（2016年）の７月で2,000億円を突破したと『日経新聞』にありましたけれど，そういう市場があります．さらに日本の場合，改正資金決済法が整備されていますので，他の国よりも安全というか，オフィシャルな形で，ビジネスができるような体制は整っているのかなと思って，このあたりはフォーカスを当てたいと思っています．

国際送金もリップル（Ripple）さんなどがもうすでにやられていますが，両替所が，たとえば地方銀行さんと共同化のシステムを作っています．そういうところに一つこの両替所を置くことによって，海外の両替所と連携して海外送金というのが簡単にサービスできると思います．私も夏休みでベトナムに行って，ビットコイン・ベトナムという２名でやっている会社があって，そこの人に頼んで海外送金をやってきました．本当にすぐに発行できて，すぐに送金ができて，す

ぐに口座にお金入ります．そういうようなものが結構簡単に作れる世界になってきています．あと証券取引ですね．弊社もJPX（日本取引所グループ）さんと実証をやらせていただきました．あと資産管理ですね．不動産登記の話は法的な話があるのかどうかよくわからないですが，世界的に実証が始まっていますねと．あと，契約管理．スマート・コントラクトですね．ただ，今のイーサリアムとかのSolidityに書くスマート・コントラクトだとかハイパーレッジャーのチェーンコードが契約書かというと違うと思うんです．たとえば，e文書法の判例ではサインされたPDFが裁判でエビデンスになっているわけで，ではビットコインにある台帳が裁判所でエビデンスになるかというところも，法整備だとか当局の意向を聞かなければいけない．技術以外のところです．

保険も契約のことなので同じような対応が必要です．貿易金融，サプライチェーンはIoTと絡んでいますが，先ほど話があったADEPTは，「デバイス・デモクラシー」[★2]という論文にまとまっています．IBMとしては実証実験で，サムスンさんとあれをやったのは2015年でしたかね．2016年は同じようにサムスンさんがマイクロペイメントについて出しています．ブロックチェーンに進化してないのかなというのが結論なんですが，IBMとしてはIoTとブロックチェーンを使ったシェアリングエコノミーだとか，限界費用ゼロ社会の実現みたいなところは，「デバイス・デモクラシー」という論文にまとめています．これはよくまとまっていると思うので，一読いただきたいと思います．

あと，本人確認．ソラミツさんのKYCの話と，自律分散組織の話と，あとトランザクティブ・グリッドの話がありましたが，そのあとスマートグリッドのところです．これも電力自由化が進んでいまして，送電網の自由化ですね．小売りは自由化されましたが，送電網が自由化されると1 to 1で売買できるようになります．そうなると，多分ブロックチェーンが使えるようになるということだと思います．

【高木】ありがとうございます．本当にたくさんの分野で可能性があるというお話でしたが，他の方々からコメントいかがですか？

【楠】3点ほどありまして，出てこなかった中でひょっとして応用の可能性があるかなと思うのは，企業間のデータ連携の中で，設備を持つ以外の形でデータ連

携したいものって結構あると思うんですね．責任分界点の関係とかの問題で．たとえば最近だと，ID を盗まれるケースが非常に増えていまして，盗まれた ID の情報って，たとえばヤフーならヤフーで気がついたものはヤフーで止めてるんですが，自分のところのお客さんで他社さんの ID が盗まれていることがあったりもしますし，たまたまそれに気が付いた時の情報をどうやって連携するかというのは，こちらからサーバを見ていても情報で対等な立場でデータ連携ができるメリットって結構大きいと思っていまして，この辺はニーズがあるのかなと思います．

それから，佐野課長のご報告の中でもあった，いわゆる公文書のところに関しては，よく紙のワークフローはなんだか非効率のように言われるんですが，紙って消すのは大変なので，基本的にはどんどん後から後から書いていく．これって実はブロックチェーンのデータ構造と非常に相性が良い面がありまして，公文書のデータの保存の仕方って RDB（Relational Database）みたいな表構造よりも，ブロックチェーンみたいな追記型でもってやっていったほうが良い部分が結構あるんじゃないかなというふうに思います．

最後に，先ほど e 文書法の話をされていて，これはむしろ電子署名法のほうが大きいのかなと思うんですが，特に海外で締結されたスマート・コントラクトに関して，日本国内で係争になるケースは今後増えてくる可能性があると思うので，これの有効性というのは早めに議論を始める必要があることだと思います．よく電子署名法について誤解がありまして，いわゆる民事訴訟法の 228 条にあるような，いわゆる文書の真正な成立を推定するというやつをその特定の PKI（Public Key Infrastructure）を使った環境に対して認めるのが電子署名法なんですけれども，じゃあ署名・捺印した文書やそういった特定認証局に行って認証局の証明書でサインしたやつだけが契約として有効かというと，そうではなくて，民法の考え方でいえば，基本的には口約束だって契約は契約で守らなければいけないものである．ただ立証というか挙証責任がどっち側に行くかみたいなものが，ハンコが押してあると基本的には押した人がちゃんと出したものだというふうに推定するというルールがあって，それを電子の世界

に持ち込んだわけですけれども，その文書が本当に成立をしているのかがITの時代にそんなに重要なのかというと，私はそうじゃないと思っています．なんでハンコの世界に2段の推定が重要かというと，現実には他人がハンコを勝手に押すケースも結構あって，それをどっちが立証するかというところが重たいからなんですね．ところがITの世界というのは，基本的にはあらゆるところにログが残るので，ある一つの契約が結ばれる過程で落ちてきたログをすべて改ざんするのは相当ハードルが高くて，単にブロックチェーン上での契約だけではなくて電子メール上で交わされたやりとりなんかにしても，その事実の立証はかなりハードルが下がってきていて，実はもっともっといろんなものが本来有効であるはずなのに，なかなか実社会での例がないからみんなおっかなびっくり今でも丸いハンコを契約書に押しているというのが実態．この辺はスマート・コントラクトだとか，ブロックチェーン上の公文書の有効性の議論をきちっとやっていくなかで，ひょっとしたら一気にIT化を進めるきっかけにできるんじゃないかと思っています．

【松尾】（直前，遠隔接続不良のため）詳細を聞いていないので，もしかしたらかぶるか，流れに沿っていないかもしれないんですが，多分，ブロックチェーンが生きる例としては，僕はパブリックブロックチェーンを念頭に置いているんですけれども，まずオープンデータであることと，もう一つは時系列的に変化するデータをずっと記録していて，それを後で何かと合わせ技で確認したいというケースだと思うんですね．

インターネットが我々に何をしてくれたかというと，キャプテンシステムみたいなものが昔あって，情報の提供は電電公社を通じて偉い人しかできなかったのが，末端からも情報が出てくるようになったということです．情報の交換という権利が末端にもくるようになって，そこでイノベーションが起きている．SNS（Social Networking Service）みたいなものができたというのが，インターネットが起こした革命だと思うんです．

改ざんされないで時系列で追えるようなデータに，誰でもアクセスできて，そこで新しいエコシステムを誰でも作れるというところが，やっぱりブロックチェーンのおいしいところだと思う．よくある例だと，たとえばUber（ウーバー）みたいなもの．実はUberみたいなものは誰でも作れるようになるので，末端の

人が自由に触れてエコシステムを作れるというところに妙味があるし，それで利便性が上がるデータは交換したほうがいいんじゃないかというインセンティブが働くんじゃないかなと思っています．

【高木】イノベーションを誰でも起こせるようになっていって，それには裏返しとしてデータがオープンになっていると．それを実現するにはブロックチェーンというのは非常に良い仕組みであるというようなことかと思いますが，先ほど楠さんのほうから公文書なんかも可能性があるんじゃないかとお話がありましたが，なにか政府の中で使っていくというような話はあるのでしょうか？

【佐野】そうですね．先ほどの 4 月の報告書の中で，政府自らがブロックチェーンを使っていこうと提言したわけですが，そういう意味で，楠さんがちょっとおっしゃいましたけども，今，この政府の中でどういったものがブロックチェーンとしてそのメリットを発揮しうるのかというのは検討しております．ただ，日本の行政システムの中でこういった新しい技術を採用するというのはハードルがいろいろあって，ブロックチェーンに限らないですが，こういった新しい技術の認証の仕組み自体を少し変えないと，なかなか変わらないかなと思っていまして，そこの仕組み自体から少し考えていこうというようなことを考えています．

【高木】ところで，今のところ，ビットコインのブロックチェーン，それからイーサリアムとかハイパーレッジャーとかあるわけですが，日本としてこれはどういうふうに付き合っていくのか．日本では，ブロックチェーンを使った実証実験は非常に盛んにやられていますし，ビットコインもかなり使っている人もいるような気もしますが，そのプラットフォームという意味では，海外のものを使う場合が多いというところがあるかと思います．それが国産でなければいけないということはないのかもしれませんが，どう日本として付き合っていくかというようなところは，何かありますか？

【楠】まだ出ていなかったテーマの一つとして，国際標準化の動きなんかがあると思うんですが，遅かれ早かれ ISO（国際標準化機構）でこういうことを議論すべきだという提案はオーストラリアからも出てきていて，その対応を迫られてい

る状況もあるなかで，ブロックチェーン自体がこれまでの延長線上で本当にいろんな方式がいっぱい提案されてそれぞれバラバラに発展していくものなのか，それともプロトコルとかあるレベルで共通化されて相互運用性が担保された状態になっていくのか，いろんな可能性が考えられると思うんですね.

私自身は，先ほどのスマート・コントラクトの安全性の問題にしてもテクニカルに解けていないところがいっぱいあるので，今はまだ様々な実装で競争し合いながらアイデアを出し合ってフィールドの中で白黒つけているフェーズだから，少なくとも実装の標準化はまだちょっと早いかもという気持ちを持ちつつも，国際的にどんどん議論が進んでいく以上，安全性に対する考え方であったり，言葉の取り方一つとってもまだ意識があってないところがいっぱいあって，ブロックチェーンの定義さえはっきりしていないため，こういったところの足並みをそろえていくというなかで，日本がプレゼンスを示していくのはとても大事なことだと思います. 日本は歴史的に非常に多くの暗号学者を抱えている国でもあるから，こういったところに対して非常に良い国際貢献をできると思っていまして，そこのプレゼンスというのはぜひ押していくべきだと思います.

【松尾】標準化は早いというのは楠さんと全く同感で，標準化に加わる時にいくつか視点があると思うんですけれども，国産の日本の強みがあるものを標準化にして世界にも使ってもらうというやり方と，日本には強みがないんだけれども外国からこんなことされてしまうと日本の産業にとって困るからそこは避けるように標準化して頑張るという，二つのやり方があって，ブロックチェーンに関して言うとまずどこが強みになるかがわからないので，今やらなきゃいけないのは，将来日本のいろんな企業がブロックチェーンを使って新しいビジネスを起こす時に障害にならないようにするのが，今やる必要があると．これがインターネットとのアナロジーでうまく成功しているかはわからないんですけども，多分ブロックチェーンの基礎技術を一生懸命やるというのは, そのルーティングの技術, ルータの作り方とか ISP の作り方を頑張るという話に近くて，インターネットができた当時はみんなが ISP をやりたがったり，最初のうちはドットコムバブルというのもあったり，広告媒体と一緒にインターネットを使って産業が起きて，それはビジネスとして全部失敗するわけですけれども，その次にいくつかの反省があって，インターネットの特性を生かして Facebook だとか SNS みたいなものが出て

きた．それが広告的に成功するわけですが，ブロックチェーンの特徴を生かした時にどこが人の注目を集めてマネタイズできるのかっていうところのほうが，本当は鍵になると思います．技術そのものは，日本は OS とかハードウェアのプラットフォームを持っていないので，そこはマイクロソフトさんだとかアップルだとかのを持っていく可能性はあるんですけれども，どうブロックチェーンの特徴っていうのを捉えるのかということに，一方で注力したほうが良いような気がします．

【高木】そこでどうブロックチェーンを使っていくかということは，結局はそのユースケースをどう見つけていくかっていうことになるんでしょうか？

【松尾】ユースケースって，たとえば 1996 年とか 1995 年とかそれくらいの時に，インターネットを使う Uber ができるなんて誰も思ってないわけですね．それは，メールがあってウェブがあってブログみたいなものができて，それが SNS になって，GPS（Global Positioning System）とスマホがあって，デバイスから物がとってこられるようになって，それを合わせて……っていうのを何段階か経て Uber が出てきている．多分，今わからないんだけれども何か確かな情報がブロックチェーン上に載ってそれを足し合わせるとこんなものができるっていうのは，段階を経て出てくるものなので，そういう特性をちょっと頭に入れつつ，何が必要なのか．それこそベンチャーができていく過程を支援していくようなことのほうが重要な気がします．

【高木】ありがとうございます．どういうふうに新しい使い方，ユースケースを探していくかというのはなかなか難しい．今，ベンチャーを育てていくような思想も必要だという話もありましたが，IBM さんもいろいろな実証実験をやられているかと思うんですが，ユースケースを見つけていく時の苦労とか，こういう観点で考えるといいんじゃないかというようなことは，何かありますか？

【高城】ユースケースを探し出すのは非常に苦労しています．何かやらなきゃということで，上から，「何か持ってきて」といわれるのが大半です．実証については，そんなに大きなお金じゃないですけれども，お金は出ているみたいなので，

ビジネスチャンスではある．弊社としてはデザインシンキングをやって，業務を知っているのはお客さんなので，お客さんと一緒に考えていくというモードでリスクも減らしながら，要は我々が持っていて動かないじゃないか，意味ないじゃないかと言われないようにする．逆に言うと，要は業務をやっているお客さんが考えなければいけないとは思っています．

【榊原】やはり日本の産業構造を考えますと，製造業にこれが適用されていかないとなかなか実感がわかないというところがありまして，金融の世界がブロックチェーンを使ってすごく効率化されましたとか言われても，金融の方にはすみませんが，ちょっと飛び道具的な，すごく実感がわかないところがあるんですけれども，プロセス系もディスクリート系も含めて製造業というのはすごく産業構造の層が深いわけですよね．それで関わっている人がすごく多くて，いろんなところがバリューチェーンで繋がっているわけですから，その製造業がブロックチェーンを採用して IoT でも何でもいいんですが，ものすごく業務のモデルが変わりました，ということになると，我々の社会も変わるっていう実感が出てくるのかなという気はします．

【楠】やっぱりたくさん失敗すると良いと思うんですよね．たとえば Facebook を途中から手伝っていたショーン・パーカー（Sean Parker）も，その前のナップスター（Napster）で失敗した後も何度もくり返し起業をしていますし．ブロックチェーン界隈がシリコンバレーだけのエコシステムじゃないところがとても面白いところだと思っていて，サトシ・ナカモトが本当に日本人かどうかはよくわかりませんけれども，最初に大きな事故を起こしたマウントゴックスは最近まで渋谷にあったわけですし，大きな問題を起こした The DAO も多分ドイツの Slock.it（スロックイット）を中心とした人たちですよね．

なんとなく，これまでのイノベーションは，非常に強い購買力を持った群とかいろんなところのエコシステムの上で成り立っていたものは西海岸とか限られた場所じゃないとなかなかスタートしにくかったんですけど，そういう意味で技術が民主化していて，世界のどこにいても面白いことを始められるという新しいパラダイムの時代が来ている．その中で東京って実は世界で最も大きな都市圏として非常に魅力のある街で，マウントゴックスをやっていたカルプレス（Mark

Marie Robert Karpelès）だけではなく，ノマドっぽく世界中をふらふらしていたビットコインの偉い人が日本人の奥さんに捕まって東京に住んでいるみたいな話は他にも結構あったりもするわけですね．日本にとっては，むしろ新しい動きを始めたり，何か失敗を繰り返しながら新しいものを生むチャンスが，実は増えているんじゃないかなという気もします．

【高木】その辺は松尾さん，シリコンバレーから日本を見ていてどうですか？

【松尾】多分，ブロックチェーンとかビットコインに関して，シリコンバレーのモデルは，開発では，フェイルファーストと言って，どんどん失敗してその中からうまくいくものを伸ばしていくというやり方をするんですが，The DAO の件でもそうだけど，フェイルファーストがうまくいかないわけですよ．つまりシリコンバレーのイケイケのモデルは，多分，通用しない．そこで日本．楠さんが日本に暗号の経験を持っている人がたくさんいるって言ってましたけど，その通りで，GPKI（政府認証基盤）にしろ今のマイナンバーにしろ，暗号を使って結構重厚長大なシステムをきっちり作り上げる力って日本にはたくさんあって，経験者もたくさんいて．綿密にものを作るっていうのは，日本ははるかに米国よりも優れているわけです．なので，その人たちをぜひ活用して，フェイルファーストはしないけどフェイルは認めるみたいな環境を整えてあげることがとっても重要なんだと思います．もう一つは，ビットコインのコアデベロッパーたちもちゃんと保護してあげないと，彼らも彼らで困っている．ある意味，今，日本に住んでいるコアデベロッパーたちもたくさんいるので，そういう人たちをうまく活用して，なんというか日本の精密に作るっていうところとその人たちのチャレンジャー精神みたいなのを合わせて，日本人だけじゃなくて育ててあげると，フェイルファーストだけではないベンチャーの新しいモデルみたいなものが作れるんじゃないかという気がしますけれどね．

【高木】今日もご登壇いただきました武宮さんのように，米国出身で日本に住んでブロックチェーンの開発をしているという人もいますので，日本という土地で様々な得意技を生かしながら開発をしていくというようなことができるような気がいたします．では，会場のみなさまからご質問等，ございますでしょうか．

【参加者】今日は貴重な情報をありがとうございました．チェーンとチェーンの間のインターフェイスの問題はどうなんでしょうか？

【松尾】異なるチェーンの間でどう情報をリンクするかとか合わせていくかという研究は昔から結構されていて，ハイパーレッジャーとかそういうところの議論で多分されているはずなので，そういったものが今後，より表に出てくるんじゃないかなという気がします．

【楠】ハッシュチェーンでしかないので，チェーンとチェーンを繋げること自体はそれほど難しくないんですね．問題は，それぞれのチェーンのデザインの中で一貫性を持っているので，チェーンを繋げた時に，チェーンをまたがったデータの一貫性をどう持っていくかというところには様々なチャレンジがあって，しばらく活発な開発が進むんだろうなという点．また，特にサイドチェーンの問題意識は，ちょっと触れさせていただいたパブリックチェーンにおいて，最も計算能力を持っている人以外のシステムの中でどうやって安全性を担保していくかというのが結構重要な議論としてあるので，おそらくチェーンをまたいだ一貫性以外のところでも，大きくないパブリックチェーンの安全性をどういうふうに担保していくかっていう点でも，チェーンとチェーンの間の関係というのは非常に重要になってきて，そこは多分，そのコンセンサスアルゴリズムの議論なんかと絡んでいきながら，作り方を間違えると大きなセキュリティホールが生まれてくる部分なのかなというふうに思います．

【高木】時間も来ておりますので，最後に一言ずついただければと思います．

【高城】さっきユースケースが大事と言ったんですが，やはり日本にいるエンジニアが世界に発信するようなものづくりというのは非常にエキサイティングなので．先ほど，製造系，ものづくりで，ブロックチェーンの適用が増えるといいっていうことでしたが，IoT と絡むと思うんですけど，たとえばインターネットに繋げるようなセットトップボックスに簡単に入るような，組み込みで入るようなブロックチェーンの仕組みを作るとか，そういうことが日本の技術者中心にできて，世界のオープンコミュニティでパブリッシュされるようになるといい．私は

ちょっとそこまで能力がないので，皆さんの中からか，この日本の中から，そういうものが生まれたら楽しいなと思って最後のお話を聞いていました．

【佐野】我々の政策の取り組みとしては，今日もお話がありましたが，どこが稼げるかよくわからないので，そこはユーザーサイドの活用，実証の中での競争を促すということかなと思います．あと，標準化の話が先ほどございましたが，確かに対外的に動きが出てきているので，一応それに向けて対応の準備を今進めてはいます．それから，これは今年度ですが，性能評価基準というものを整備していくということ．それと，政府としてどう扱っていくのか，どう仕掛けていくかということを今考えています．また，楠さんから話がありました電子署名法とか既存の法律の問題がありますが，それも少し整理をして考えていきたいと思っています．

【楠】技術のライフサイクルの中で発明されたものが社会で使われるまでって，結構平気で四半世紀くらいかかることが多いと思うんですが，ブロックチェーンは逆で，ビットコイン的なテクノロジーのもととなるアイデアって P2P が流行った 90 年代後半くらいからあったり，2000 年代初頭のハッシュキャッシュとか，一般対策の技術なんかも 2009 年にああいう形でインテグレートされていた．実装がポンと出てきて，それから一生懸命，安全性とかを議論し始めているという意味では，ちょっと珍しいパターンで，そういうダイナミズムの中で，これから何が起こってくるのかというところはとっても面白いと思います．

それと，もともとインターネットという分散のアーキテクチャで始まったはずのものが，実際にはテックジャイアントにデータもトラフィックも集まって，ピアリングの契約もそこ中心にまわっていくといったように非常に集中化していった．ウェブの世界は，本来データとデータは繋がっているはずの世界なのが，みんなそのシステムの下側に沈められてしまって，データベースの中身を見ることができないことが当たり前になった．ビットコインをはじめとして，ブロックチェーンのすべてのデータが公開されていて，そこの中でトランザクションが走るアイデアというのは，本来ティム・バーナーズ＝リー（Tim Berners-Lee）がウェブでやりたかったことがもう一度表に出てきているような気もしていて，そういう意味では大きなアーキテクチャの転換点になる可能性もあるのかなと期待をし

ています．

【松尾】今，楠さんからあったように，まさにそういう動きだと思っているのと，そういう意味で言うと，私はどちらかと言うとかなり中立性を持ってアカデミアの立場からどう成熟させていこうかということを今考えているので，MIT メディアラボというのが一つの足掛かりになったけれども，日本の大学も含めてアカデミアの中でそういうことを成熟させていくことを考えていますので，そういうことで貢献できればなと思っています．

【榊原】私にとってブロックチェーンというのは，テクノロジーの興味ももちろんなんですけども，それ以上に社会変革の可能性というところの興味が非常に大きい部分です．私は CTO という仕事をやっていまして，Chief Technology Officer なんですけど，真ん中の T はトランスフォーメーションの T で，Chief Transformation Officer でいきたいというふうに思っています．社会変革していけたらなと思っています．よろしくお願いします．

【高木】はい．それではお時間も過ぎてまいりましたので，このセッションはこの辺にしたいと思います．皆さんどうもありがとうございました．

（2016 年 9 月 8 日収録）

註

★ 1――Profiles in Innovation - May 24, 2016 (1) <https://ja.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1>

★ 2――Device democracy: Saving the future of the Internet of Things <https://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/>

日本語版「デバイス・デモクラシー：モノのインターネット（IoT）の未来のために」<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03620JPJA&attachment=GBE03620JPJA.PDF>