情報システム・バックアップオフィス研究会（ITBO 研）　２０１５年度　第７回　議事録

１．開催概要

●開催日　　：２０１５年１１月１０日（火）１６：３０～１８：３０
●開催場所　：BCAO 東京オフィス、（関西地区からのリモート参加はなし）
●進行役　　：大塚（座長）
●議事録作成：大塚（座長）
●出席者数　：５名（出席者名は末尾参照）
●配布資料　：ブロックチェーンへのサイバー攻撃の脅威とリスク_03.pdf（岡氏提供）

２．　議事内容

（１）　はじめに　（報告：大塚）

ITBO 研究会の定例会議も年度末まで残すところ（今回を入れて）5 回です。2016 年 3 月の最終成果のまとめに向け議論を集約して参りたいと思いますので、皆さんのご協力をお願いします。

本日は、特別ゲストとして露木千尋様をお招きしました。露木様は e-コマース関連事業で多くの業績を残されました。最初に簡単な自己紹介をお願いしました。

（露木様略歴）

・神奈川県小田原市出身。

・1995 年、e コマースソリューションプロバイダとして日本で初めてインターネットサービスプロバイダ向けにカード決済を利用した『リアルタイムサインアップシステム』を開発、国内コンビニでの e コマース決済のデファクトを確立した。e 革命に「陰の主役」ありと称される。

・その後 Web アプリケーションパッケージの開発、コンサルテイングを手掛け現在はベンチャー系企業の経営コンサルタントとして、「水道水」から発電機を回す技術の紹介や、スマホ、タブレット、ガラケーどこでも同時に 2 台急速充電可能な、非常にコンパクトな PowerUPS の販促等でご活躍。

インターネット黎明期でテクノロジーを使ったアイデアがどのようにビジネスに成長したかを最もよくご存知である方であるということで、ビットコイン 2.0 が今後どのように国内に普及し定着するかの議論に加わっていただくことにした。

次回、12 月は年末恒例の忘年会を計画するので、関山副座長にコーデイネートをお願いした。

（２）連絡事項（報告：大塚）

10 月の BCAO 運営会議が開催されなかったため、運営会議議事資料（案）からの抜粋を紹介します。

①　10/23 現在の BCAO 会員

個人正会員、法人正会員の活動者、法人賛助会員の活動者、学生会員、資格会員合計で、2,066 人。昨年比 120 人減。現在会員増加と法人会員の満足度向上のための対策を構築中。特に BCAO パンフレットの作成については高橋副理事長中心に案を固め早々にリリースできると聞いている。

② 月例会実績/予定

9 月 30 日 13:30-（参加 24 名）

「中小企業 BCP と組合 BCP の連携」高橋副理事長

「お互い様 BC 連携ネットワークを活用した成長戦略」細坪事務局長

10 月 30 日 13:30-（参加 名）

「BCP 策定手法の最新動向」伊藤副理事長

「サイバー対応や ERM などリスク管理統合の道筋」副島理事

11 月 18 日 13:30-

「リスクマネジメントと危機管理～想定内と想定外：原点に戻って考える～」指田副理事長

「地方公共団体 BCP の策定支援」丸谷副理事長

③ BCAO10 周年記念行事

⇒未議論

３．今月の ML の話題

（１）「ビットコイン」、「ブロクチェーン技術」が一般紙の記事や技術コラムに数多く取り上げられる（岡様、伊藤様、大塚）

・日経新聞（10/16）「エコノミックイトレンド（小林慶一郎氏）」「仮想通貨の技術的可能性」というタイトルと、「市場経済、構造変化も」というサブタイトルで、ビットコインの仕組みや、ネット上の仮想通貨に限らず、貨幣システムの設計と公共財的な意味での関連を語る。

・朝日新聞(11/1)朝刊一面にフィンテック 金融ＸIT=生活変える？というテーマで指紋決済や資産管理･･･ベンチャー続々という記事が特集。

・TechCrunch「ブロックチェーンの正体」

http://jp.techcrunch.com/2015/10/19/blockchain/?utm_source=tcdaily_20151020&utm_medium=email&ncid=tcdaily

この記事のキモは「許可制（Permissioned）ブロックチェーン」。許可制にすればするほど、取引（トランザクション）の実行（完了）に要する時間を短縮することが可能となる。反面、許可する管理者を置く(任命する)ことから、その信頼性や管理者が機能しなくなったときのダウンタイムの発生などの問題が発生。高信頼性を確保することと、トランザクション速度を高速化することの間には、一定のアンビバレントな関係（二律背反）があります。

（２）「そして未来へ」（岡様、大塚）

2015 年 10 月 21 日（水）午後 4 時 29 分、まさにその日その時間に開かれた、バック・トゥ・ザ・フューチャー パート２ 30 周年記念イベントには多くのファンが参加、テ

レビマスコミでも大きく報道され、注目を集めました。1985 年に想像した 2015 年の世界では、スマホ、ドローン、指紋認証技術、ApplePay などの決済技術、Google Glass などウエアラブル端末など数々の技術が現実となりました。では 30 年後の 2045 年に何が実現しているでしょうか？最近 20 代の若者に聞くと、全く想像出来ない、と答えます（というか思考停止しています）。今、2045 年に何が実現しているか、と想像するより「こんな世界を実現したい」というクリアーなイメージを描き、それを実現させるためのロードマップを作って、（今から）着々とステップバイステップで実現させていく、「逆算の発想」を持つことがとても重要です。ところで、未来人原田さんと言う方が「２ちゃんねる」で語ったスレが話題になっています。
http://harada2058.wiki.fc2.com/
真偽のほどは分かりませんが、あまりに明快に言い切っていることを見ると 30 年後の未来がクリアーにイメージできて、目が覚める思いがします。

４．本日のテーマ

IoT社会の100%セキュア環境の切り札か？ビットコイン２．０（前回に続き）

（参照）ブロックチェーンへのサイバー攻撃の脅威とリスク_03.pdf

（参考）Google Drive/定例会/20150908/ビットコイン2.0関連

前回に続き、分散型合意形成という考え方で単一障害点（Single Point of Failure）を作らないシステムであるビットコインテクノロジー(Bitcoin2.0)の可能性を議論。

（１）コアの技術は、ブロックチェーン技術と暗号化技術の２つ

コアの技術はおおまかには、ブロックチェーン技術と暗号化技術の２つから成る。

以下、ビットコインの例で説明する。

ＡさんからＢさんへP2Pで１ビットコインを送金する場合、デジタル署名技術を使う。これは、公開鍵暗号技術をベースにしたもの（本人しか知らない秘密鍵と誰にでもわかる公開鍵の組み合わせ。秘密鍵で暗号化したデータは公開鍵でしか複合できない。また、公開鍵で暗号化したデータは秘密鍵でしか複合できない特徴を持つ）Ａさんが秘密鍵で暗号化されたトランザクション（以下、TXと記述）は、Ｂさんが、Ａさんの公開鍵で複合することによって、送金はＡさんであること（なりすまし防止、否認拒否)、データ改ざんなしが保証される。

ＡさんからＢさんからの送金情報は瞬時に伝達されるが、同じ情報はブロックチェーン上にも公開される。

ブロックチェーンとは開始時点からのTXがすべて記述された完全なるログ＝記録簿（台帳とか言われる)。「ビットコイン」はブロックチェーン上にビットコインの所有権の移転の記録（誰から誰にいくら）がすべて記載されたもの。(誰から誰にいくらと言う情報はオープンになっている)「ビットコイン」のブロックチェーンは現在50GB程度ある。TXが発生するたび、あるいはマイニングが成功するたびにインターネット上のノードにブロードキャストされて追加される。(つまりインターネット上に同じものが数多く散らばっている）ビットコインのノード数は約10,000ある。現在新規のTXが発生するとすべてのノードにブロードキャストされるのに7秒かかると計算される。こ

のTXを数100から1000集めて１ブロックとする。１ブロックの最大は１Mbと決められている。ブロックが形成されると、非常に多数の人（マイナーと呼ぶ）の参加によるマイニングと呼ばれるハッシュ値を当てる競争（保有CPU量に比例し当選確率が上昇するのでProof of Workと言う）が行われる。この作業は、最大10分程度で終了するよう調整された作業。最初にハッシュ値を当てたマイナーに各TXに設定された手数料と報酬としてビットコイン（今は２５ビットコイン、今の相場で１００万円くらい）が支給される。常に特定のマイナーに集中しないように工夫されたしくみ。各ノードは発見されたハッシュ値と（nonceと言われる調整値）およびブロックのTXの内容（整合性）を検算して自分のブロックに追加する。

多数のマイナーの参加によりブロックチェーンの完全性（データのヌケモレやTX間の整合性や順序性を監視）していることから分散合意形成と言われる。これによってCIA（機密性、完全性、可用性）のうち完全性と可用性が保証される。

（２）　考えられるブロックチェーンのリスク

・秘密鍵の漏えい、喪失：個人で保管しなければならない秘密鍵が、人的ミスやウイルス、サイバー攻撃によって盗まれたり、またはなくしてしまったら、ビットコインを他人が自由に引出したり、または塩付けになって使えなくなる。取引所（両替所）に秘密鍵を預け、代わりにユーザーID、パスワードを支給されるサービスもある。（本来の個人管理の原則が崩れるので疑問であるが）

・サイバー攻撃、ウイルス：個人ばかりでなく、両替所やブロックチェーンそのものへのアタックも増えている。（ブロックチェーンへのサイバー攻撃の脅威とリスク_03.pdf,岡氏提供を参照）

・５１%乗っ取り:悪意をもったマイナーが全体の５１%を占め(総CPUパワーの５１%以上を持つということ)、結託して不正を行うと間違ったブロックチェーンが本物として扱われブロックチェーンの乗っ取りが可能に。仮に全体の１０%のマイナーが結託し不正を行う場合、6回ブロックチェーンがつながる成功率は０．１%以下となる。

・トランザクション展性：2011年に発見されたビットコイン、ブロックチェーンの脆弱性。デジタル署名の内容を変えずに署名スクリプト（操作命令）をいじることによって異なるTXID（ハッシュ値）が生成できてしまう現象。P2Pで送信者、受信者間で確認を行うので実害はないと思われる。

・量子コンピュータの出現：暗号化の解読、ハッシュ値の逆算に現在のCPU能力で、はるかに時間がかかるので実質的に解読不可能またはハッシュ値の逆算不可能と結論しこれが前提となっているが、量子コンピュータによりこの前提が覆る可能性がある。

（３）　ブロックチェーンの応用

2009年から様々なリスクに耐え、一度も停止することもなく稼働し続けているビットコイン、ブロックチェーンの利点を応用しいろいろなアイデアが生まれている。

・アルトコイン：ビットコインシステムのソースコードが100%公開されていることから、まったくそのままマネをした（コピペした）システムを立ち上げてしまった例。ライトコイン、モナコインなど数千ある。ビットコインで出来なかった変更を実施。

発行枚数(ビットコイン：21M枚、ライトコイン：84M枚、モナコイン：105M枚)ブロックタイム（ビットコイン：10分、ライトコイン：2.5分、モナコイン：90秒）マイニングアルゴリズム（ビットコイン：SHA-256、ライトコイン：Scrypt、モナコイン：Lyra2REV2(3)。結果ブロックチェーンの互換性はなく、それぞれマイナーが参加することが必要となりビットコインに比べ流通量的に劣る。

・オーバーレイヤー：オムニ（旧マスターコイン)、カラードコイン、カウンターパーティーなど、ビットコイン、ブロックチェーンの中に自分たちのウォレットしか読み込めないような暗号を紛れ込ませ、(紛れ込ませ方はオムニ、カラードコイン、カウンターパーティーそれぞれ３者３様で異なる）その情報をよみとって、自分たちの独自のコインの移動とみなして、ユーザーに表示するもの。TXとしてわずかなビットコイン（0.0001ビットコイン）を指定すれば通常のマイニングが行われる。ビットコイン、ブロックチェーンの安定性、堅牢性をそのまま利用した完全な「相乗りシステム」。地域通貨、ポイントなどの交換システムなど現実､適用の範囲が大きい｡(現在のやり方と違い､即時性、耐障害性、透明性、それに手数料が極端に少なくなるなどのユーザーへのメリットが多い）NASDAQが実験している、株式をブロックチェーンで発行するというものも、カラードコインの技術を採用しているらしい。ただし国内ではユーザーに多くの利益をもたらしても、このシステムを積極的に導入するリーダーが表れにくい（現在の交換システムの利益を消失させるため)。海外の先進国ではマーケットインの力が強く働くので、導入が促進される。

・ビットコイン2.0：ブロックチェーンを運用してみて、分かったビットコインではできなかったこと、なかなか解決できなかったことを出来るように全くゼロから設計されたブロックチェーン。これは、基本的にはブロックチェーンをつかったデータ構造を使っているが､これで多種多様な機能を提供することが可能になった(独自アセットの発行、マルチシグ、スマートコントラクトの生成、POSによるコンセンサスアルゴリズム、非中央集権型の取引所、秘匿トランザクションなど）新しいプラットフォーム。ブロックチェーン技術をベースにしているがビットコインとは全く別物。互換性なし。Bitshares、NXT、NEM（純国産)、Namecoin、Dashなど。

・許可型（Permissioned)：一企業内、またはコンソーシアム、グループの中だけで構築するブロックチェーン。(上記MLの話題を参照)

・万能化：Ethereum。Smart contractの決定版プラットフォーム。これからの発展が期待される。(今後、詳細研究調査)

（４）ブロックチェーン技術の将来

分散型合意形成という全く新しい概念で、セキュリテイの3要素（Confidentiality、Integrity、Availability）を実現するブロックチェーン技術の課題を議論。

・ブロックチェーンの安定性：ビットコインは6年間の実績があり、それなりに評価できるが、それ以外のものは歴史が短くまだ評価するに足らない。ブロックチェーンの安定性は多くのマイナーによるマイニング作業に依存する。不特定多数のマイナーが参加するためのインセンテイブはビットコインのケースでマイニング報酬（現在、10分で25ビ

ットコイン）とマイナー手数料。現在、マイニングリターン（ビットコイン相場）とのバランスでビジネスとして参入する業者によってマイニングの難しさが急激に高まった（2014年5月下旬時点、4年前と比べ100億倍）。今後、寡占化せず、偏りのない適切なマイナー数の確保ができるかが課題。

・機能拡張性：変化するユーザーニーズに対応するために、常にスムーズな機能変更、機能拡張を行っていかなければならない。機能変更、機能拡張の迅速な決定と周知、完璧な実行が欠かせない。しかしビットコインの例では、機能変更には非常に数多くの分散しているマイナーの総意での決定が必要になる。一方で機能変更、拡張の提案は一部のコアメンバーによってなされるが、このプロセスが不透明である疑いがある。MITラボに所属する専門家が実質な提案権を持っているようであるが、その詳細は不明。結局ビットコインとその他の派生システムとの競争になり、市場で選択されることになる。これからの国内のブロックチェーン技術の健全な発展のためには、強力な推進力を発揮するリーダーが必要と考える。官民学一体で協力し啓蒙、普及、拡大に尽力することを望む。

４．次回ＩＴＢＯ研究会

	開催日		時　間	場　所
		１２月８日（火）	１６：３０－１８：３０	ＢＣＡＯ 東京オフィス

今年の（東京地区、関西地区それぞれ）忘年会を予定します。
関西地区から参加される予定の方は、事前にご連絡ください。
ITBO 研究会メンバーのみなさん、奮ってご参加ください。

５．ＩＴＢＯ研究会会員（敬称　略）

No.		氏 名	参加	所属
1	座長	大塚　純一	○	-
2	副座長	伊藤　高信	○	FUN　Inc
3	副座長	関山　雄介	○	大成建設株式会社
4		岡　伸幸	○	ソフトバンク株式会社
5		海田　雅人		東京共同会計事務所
6		加藤　誠		株式会社日立コンサルティング
7		近藤　隆一		-
8		安齊　隆正		株式会社富士通エフサス
9		西出　三輝		損保ジャパン日本興亜リスクマネジメント株式会社
10		野原　英則		京セラ株式会社
11		宮島　正孝		セイコーエプソン株式会社
12		山口　孝一		株式会社インターネットイニシアティブ
13		吉川　明人		ＮＥＣネクサソリューションズ株式会社

14		木村　信弥		株式会社　ディー・オー・エス
15		後藤　富雄		バレイキャンパスジャパン
16		小尾　一介		Octave
17		岩崎　慎司		株式会社富士通総研
18		齊藤　公男		株式会社電通ワークス
19		佐々木志津香		パナソニックインフォメーションシステムズ株式会社
20	特別参加	露木　千尋	○	株式会社ホーキングジャパン

上記のほか、伊藤（嘉浩）様（キングフィッシュ）、日下様（住友電気工業)、斎藤様（IIJ)、小友様（富士通エフサス)、飯田様（江崎グリコ）が ML にて参加されています。　　（以上）