# 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８回　議事録

１．開催概要

●開催日　　：２０１５年１２月８日（火）１６：３０～１８：３０

●開催場所　：BCAO 東京オフィス、関西オフィス

●進行役　　：大塚（座長）

●議事録作成：大塚（座長）

●出席者数　：８名（出席者名は末尾参照）

●配布資料　：なし

２．議事内容

（１）　はじめに　（報告：大塚）

2015 年今年最後の研究会になりました。今日はいつもの研究会後に忘年会を企画しています。皆さん奮ってご参加ください。ITBO 研活動も残すところ後、4 回（今回を入れて）。来年は 2 年間の活動の集大成に向けて議論を収束させるとともに、来年度（2016 年 4 月以降）の活動について皆さんのご意見をお聞かせいただきたいと思う。

ITBO 研活動資料（アジェンダ、議事録、添付資料他）は Google Drive に保管して共有しています。ITBO 研の皆さんのユーザー登録は済んでいますが、もしドライブにアクセスできない場合はこちらを利用してください。

・アカウント名：itbobcao@gmail.com

・パスワード　：itbo2012

（２）連絡事項（報告：大塚）

11 月の運営会議に参加できなかったため、BCAO 事務局による議事録から抜粋してご紹介します。

① BCAO会員勧誘促進パンフレット

12月の運営委員会までにパンフレット(案)を準備する予定。(実際、年明けにずれ込んだ)

来年1月完成をめざす。(高橋副理事長報告)

外部委託費用として10万円を予定。

② 経済産業省受託事業「平成27年度製造基盤議技術実態等調査」

訓練の取り組み状況アンケート、セミナー＆演習の実施:2016年1月22日(大阪)25日(名古屋)、26日(東京)

以上の結果をもとに事業継続能力向上に必要な訓練・演習手法を整理。

BCAO専門家委員会＆名和教授で実施する。

当受託案件の報告結果は経産省より公報される。今後BCAO新規会員獲得につながるものと期待。

上記により、2016年1月25日の運営委員会は1月27日に日程変更

③ BCAO関西地区　10周年記念イベント

関西地区、萩原理事より報告あり。(詳細は略)

当日セミナー会場内にて記念パーテイーを予定（外部ケータリングを利用）

３．今月の ML の話題

●IIJ Technical WEEK 2015 TOPIC（岡様）

IIJ Technical WEEKが開催されました。

2日目にITBO研にもお呼びしたことのあるIIJ斎藤　衛氏の

「セキュリティ動向2015」のセッションがあり、その中にビットコイン関連のレポートがありました。

”DD4BC”（DDos For BitCoin）：emailなどで脅迫状を送りつける、Bitcoinを払わないとDDoS攻撃（400Gbps）するものですが、実際には、10Gbps～40Gbpsぐらいの攻撃力しかなかったようです。

宛先表示名は”DD4BC Term”だったので、複数名のグループ犯行なのでしょう。

http://www.iij.ad.jp/company/development/tech/techweek/pdf/151112_1.pdf

●　Safety 2.0について（これって、BCのキーワード？）

IoTの進展とともに、企業の安心・安全活動が新たなステージに入ります。人の注意力に頼る時代を「Safety 0.0」、安全を組み込んだモノを提供する時代が「Safety 1.0」とすれば、これからの時代の安全は「Safety 2.0」だと言われます。「Safety 2.0」が従来の安全活動と大きく違うのは、技術的なアプローチだけでなく、その推進役が経営層であるという点だそうです。「Safety 2.0」は企業に高次元の安全に加え、生産性の向上や従業員の安全、また新産業の創出といった多くの便益を生み出すとのことです。http://kenplatz.nikkeibp.co.jp/cp/Safety2015/（岡様）

Safety 2.0は日経BPの造語（Industry4.0をもじって）ではないか。

昨今のCSRの取り組みや企業の行動規範、ガバナンスコード等の取り組みから行くと、企業におけるすべての活動について、経営層の推進（関与）が求められます。

HPの説明では、

・人の注意力に頼る時代「Safety 0.0」→これは、従来の労働安全衛生（OHSAS等）ではないかと

・安全を組み込んだモノを提供する時代　「Safety 1.0」→セキュリテイ・バイ・デザインです。

・「Safety 1.0」に加え”生産性の向上” ”従業員の安全” ”新産業の創出”を生み出す時代、

「Safety 2.0」→講演を見る限り”生産性の向上” ”従業員の安全” ”新産業の創出（IoT）”をキーワードに集められていますがいまいち、すっきりしません。”従業員の安全”はSafety 0.0に含まれるし・・。多分に憶測ですが、日経BPにだまされる（マーケット創造に乗せられる）ことも多いので新しい言葉には要注意です。（野原様）

●VVVランサムウェアの流行のきざし（吉川様）

ランサム（身代金）＋ウエア（ソフトウエア）の造語。感染したPCのファイルを勝手に暗号化、戻したければ身代金を払えと脅迫する。支払期限を過ぎると身代金を釣り上げる。ファイル拡張子にvvvが付くことが特徴。身代金を払っても元に戻れない。身代金は払うべきでない。犯罪を助長することになる。

Malvertising（Malware/Malicious Advertising：広告配信ネットワークを悪用して感染する）や改ざんされた正規のWebサイト経由でのドライブ・バイ・ダウンロード（見ただけで感染する、IEやFlash Playerの脆弱性を利用した攻撃が多い）または、スパムメールの添付ファイルやWebリンクのクリックで感染。（大部分の攻撃はソフトウエアの最新化で防げる。）5月に初めて日本語版ランサムウエアが登場（Crypt0L0cker）。11-12月で被害が急増。びっくりすることにランサムウエアビジネ

スが存在する。ウラウドで提供されランサムウエア作成サービスで身代金の一部を徴収するビジネスモデル。身代金はビットコインで要求されることも。大事なファイルは定期的にバックアップが必要。DVD/ブルーレイ/オンラインストレージ、複数世代のバックアップを取得する。オンラインリアルタイムバックアップ方式だと暗号化された状態でバックアップされてしまうので注意すること。

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）Google Drive/定例会/20150908/bitcoinの基本_SB岡20150828.pdf

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

● 前回の復習

IoT社会を支える100%セキュアなインターネット環境は作れるか？

100%セキュアなネット環境とは、機密性（Confidentiality)完全性、(Integrity)可用性、（Availability）が保証されていること。ビットコイン2.0では暗号化技術（共通鍵暗号、公開鍵暗号技術、ハッシュ関数他）とブロックチェーン技術を組み合わせて実現する。

以下、ビットコイン　アプリケーションを例に説明する。

機密性とは、アクセスを認可された者だけが情報にアクセスできるようにすることであるが、ビットコインではブロックチェーン上に取引き（トランザクション、以下TXと表記）である送金者、受取者のID（ブロックチェーンアドレス、各個人の公開鍵暗号から作られたもの）とビットコイン数量がすべて一般公開されているルール。従って誰でも取引き履歴（General　Ledger）を閲覧することができる。しかし、各個人が管理する秘密鍵（公開鍵のペアー）をばらさない限り、書き込まれたTXの本人特定はできない。万が一秘密鍵がばれてしまったり、盗まれた場合、本人になりすまして不正送金が行われる可能性がある。（秘密鍵→公開鍵の生成→ビットコインアドレスの生成が可能）

完全性とは、TXの内容が正確かつ完全である（改ざんされていない）ことを保証することである。送金者、受取者の間（2者間）の送金については、デジタル署名を用いるので本人なりすまし、本人否認、改ざんは防止できる。一方で送金者の不正な二重送金の防止は、ブロックチェーンのマイニングによって担保される。マイニングとは、開闢以来の取引履歴が完全に正しいものであることを保証する作業。もし送金者が二重送金を行ってもブロックチェーン上にブロックチェーンアドレス、数量がすべて記録されているので、保持しているビットコイン数、送金数が衆目にさらされているので簡単にばれてしまう。マイニング作業中に不正TXは落とされる。また、送金者が同時に２人の異なる受取者にビットコインを送った場合、いったん、両方のTXがブロックチェーンに追加されるが、その後マイニングが繰り返されブロックチェーンが伸びて行くとき、早く伸びた方（長い方）が「正」とされる。つまりマイニングを行う多数のマイナーが支持した方が「正」となる。

可用性とは、インターネット上にノードと呼ばれるブロックチェーンのコピーが多数存在し、どこからでも、だれでもアクセスできることから実現される。現在、世界中に数万のノードが存在する。

機密性（Confidentiality)完全性、(Integrity)可用性、（Availability）を未来永劫維持するための条件は、将来のネットワークのキャパシテイ（の拡張性）が十分であること、個人の秘密鍵は個人で管理することなどのルールを守ることのほかに、ブロックチェーンを維持するマイニングが偏りのない不特定多数のマイナーによって実行されることが必須。

● 多数の善意のマイナーをどうやって確保するのか

マイナーのインセンテイブは、マイニング報酬とトランザクションフィーの2つ。マイニング報酬は、最初に発見したマイナーが、新しいブロックを繋げるときに報酬として受け取るビットコイン。（今は25BTC（対円為替相場で100万円くらい））トランザクションフィーは、送金者がチップとして（お礼）渡すビットコイン。これは決まりがなく、一般的には0.0001～0.0005BTC(6～30円)ぐらい。また ゼロ（0）BTCで手数料を払わない人もいる。これはウォレットクライアントで自由に設定できる。

一方でマイナーのコストはマイニングに必要なシステム資源の準備と運用費。高性能のCPUを積んだマイニングシステムと電気代を中心としたランニングコストが主。マイニングは確率論であるが、マイニングパワー（言わばCPU資源）に比例し確率が高くなる。マイニングパワーの増減（マイナー数の増減）に関わらず、一定量、2週間2016ブロック（10分以内に1ブロック）が得られるように、マイニング計算の難易度が自動調整される。つまり直近2週間のブロックの生成時間のポアッソン分布を取り、2週間で2016ブロック（10分で1ブロック）が生成されるように、求めるハッシュ値がある値以下であることという条件を設定する。（実際は求める64ケタのハッシュ値の頭から連続したOゼロを埋めてこの数を多くしたり少なくしたりして調整する）今は数年前に比べ100億倍、難しくなっている。現在、対ドル為替相場が上昇基調なので、マイナー（実際には多くのマイナーを束ねたマイニングプール）の確保は順調に推移している。多数の（善意の）マイナーのマイニングのお陰で2009年から今日まで、何度かビットコインブロックチェーンに対する深刻な攻撃が繰り返されたが、（一時的にスローダウンしたものの）止まらず、完全性を維持し続け、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）が証明された。

● スマートコントラクトとは？

スマートコントラクトとは、契約行動をプログラム化し、自動的に実行しようとするものとされる。この利点は、ビットコインと同様に、契約の相手方を信用する必要がなくなること(trust-free、トラストフリー)とコストが極端に低下すること、の二つ。これによりマイクロペイメントに活用できるようになる。「契約の相手方を信用する必要がなくなる」とは、ブロックチェーン技術により過去の契約の実行履歴がすべて記録・公開されているため、完全に透明性があり、また契約内容がプログラム化され人が介在せず機械的に実行されるため、詐欺をする余地が極端に少なくなるということ。「コストが極端に低下する」とは、第三者機関などを必要としないこと。従来では契約が確実に履行されるためにエスクロー(商品の注文後、買い手は第三者に料金を渡し、商品が買い手に到着した後、第三者は売り手に料金を渡す)のようなサービスが必要になるが、スマートコントラクトではプログラムの中にエスクロー機能が実現される。これを実現させる万能プラットフォームがEthereum（イサリアム）である。応用アプリとして考えられているのが、シェアード・エコノミー（Air bnb、UBERまたは、空きストレージ領域の賃貸サービスのSTORJなど）そしてIoT領域。具体例としては、イサリアムブロックチェーンに連結された鍵であるスマートロック、Slockがある。まず所有者がSlock上に貸出すための価格と保証金の額を設定する。利用者はイサリアムブロックチェーンを介してそれを支払い、スマートフォンを使って鍵の開け閉めをする。利用者はTXをイサリアムに送信するまで保証金はプログラムでブロックチェーン上に保持される。つまりレンタル料金は自動的にSlockの所有者に送られ利用者には保証金からレンタル料金を差し引かれ返還される。これらはすべて第三者の介入なしに行われる。Slock(スマートロック)はほかにデジタルコンテンツの配信にも応用できる。IoTの例で

はドローンの飛行についての許可、否認をブロックチェーン上に明記することができる。同様にIoTデバイスのさまざまなアクセス制御（機密性）を可能にする。IoTが悪意のもった第三者にのっとられたり、不正を働くことが完全に防止できる。

● スマートコントラクトとの比較

マイナンバー対応ソリューションで使われている「Final Code」と DRM とを比較した。

（1） Final Code ; http://www.marubeni-sys.com/sec/finalcode/index.html

「Final Code」は、重要なファイルを暗号化して、ファイルの開封状況などの利用状況を追跡し、あとから遠隔で削除もできるファイル暗号化・追跡ソリューションである。 利用者情報、利用者権限をクラウドに上げて、ファイルをオープンするとき必ずクラウドに問い合わせるというしくみ。ファイルの所有者（管理責任者）が誰にいつまで、何を見せる、最後は削除するところまでセットする。

以下の特徴がある。1. ファイルにパスワードがないため、流出しても心配ありません。2. ファイルの作成者が許可した相手以外は開封できません。3. 手元を離れたファイルでも、遠隔で“あとから”削除できます。4. アクセスログによりファイルの行方や操作をしっかり管理できます。5. 手軽に導入できるクラウドサービス。複雑な設定は不要です。6. 有償なのは暗号化するユーザーだけ。閲覧に必要なソフトは無償。

Smart contract と違うところは、クラウドがないところ。クラウドも「中央集権的管理」が行われていると見ると、単一障害点（Single Point of Failure）になりうる。Smart contract で使うパブリックブロックチェーンは完全な分散合意形成で維持されるため、安全である。

（2） DRM（Digital Rights Management デジタル著作権管理）

Microsoft 社マルチメデイアプレーヤに実装された暗号化されたコンテンツを解く鍵を使って復合化しながら再生するしくみ。ソフトウェアがユーザーのコンテンツ利用を管理するため、利用期間の切れた後には再生不能にするなどの処置が可能になる。この方法の問題点として、暗号方式や再生ソフトウェアの内部構造がリバースエンジニアリングによって知られてしまうこと。初期の DRM 技術として知られているものに、DVD の映像信号を暗号化する CSS がある。CSS では再生ソフトウェアに埋め込んだ固定鍵を用いる単純な暗号化を使っていたため、リバースエンジニアリングにより鍵が一般に知られてしまってからは、ほとんどその実効性が失われている。また、懸念点として、第一に DRM 技術のほとんどが特定のメーカーによって定められ、その技術的詳細が一般に公開されていないことから、そのメーカーやサービスが活動を停止した際に、購入したコンテンツが将来にわたっても利用可能なのかが必ずしも担保されていないこと。また、再生機器を買い換えた場合にデータの移行が出来ず、それまでに購入したコンテンツが利用できなくなる場合もあること。第二に DRM はその技術的特性により、理由を問わず複製そのものを制限している。そのため、一般的な著作物では、著作権法によって認められている範囲での私的複製、抜粋、データの編集などの行為も、複製を伴う行為であれば制限されている。第三に各種の DRM 技術は特定のソフトウェアに依存し互換性が無いことから、消費者は特定のソフトウェアを選択せざるを得なくなる。また再生や閲覧のためのソフトウェアを利用できる環境についても同様の制限があり、例えば iTunes や Windows Media Player の DRM 技術を使用するコンテンツが、OS として Linux 等を用いるコンピュータ上で再生できないといった課題がある。

● 今後の見通しは？

以下の課題を考える。

**(1) 将来のユーザーニーズの変化にどう対応するか**

プラットフォームとしてのビットコイン 2.0 のニーズとしてはブロックチェーンスケーラビリテイ確保である。ビットコインブロックチェーンでは、ブロックサイズ　1Mb、マイニング間隔 10 分、認証の確定までの回数　なし（一般に 6 回以上と言われる）、という規定がある。スマートコントラクトやマイクロペイメントへの応用を広げるためにはこれらの要求に対応する必要がある。なお、SDK、API 等の提供はユーザー側の担当である。

選択肢は3つ。1．ビットコインブロックチェーンの仕様の拡張。2．ビットコインブロックチェーンに繋げるサイドチェーンの活用。3．Ethereum など他のブロックチェーンでの実現。1．についてはもともとの設計思想を大きく変えることから制約がある。仕様を変更するとホークと呼ばれるブロックチェーンの分岐が発生しブロックチェーン自体の価値が薄れてしまう。2．は一番実現性が高い方法。しかしマイニング間隔 10 分が変わらないためパブリックに認証される項目について考慮が必要。3．についてはいろいろなアイデアがある。Ethereum（イサリウム）のようなパブリックブロックチェーンで構築するもの。Mijin,ORB のように許可型ブロックチェーンで実現する方法などがある。

**(2) 分散合意形成を支える、多数の善意のマイナーをどう増やし確保するか**

マイナーがちゃんとマイニングを続けてくれるモチベーションがあるかどうかということ。マイナーのインセンテイブは上記記述のとおり。マイナーはブロックチェーンに何が書かれているかは気にしない。マイニング報酬は現在25ビットコインだが、2017 年中に半減する（12．5ビットコイン）。そして将来ゼロになる。（2040 年頃と予想）。そうなるとトランザクションフィーだけがインセンテイブになる。他方で、ビットコインブロックチェーンを使ったアプリが増えることにより TX が多くなると思われる。その場合、10 分間で発生する TX が 1 ブロックで収まりきれないため、ユーザーはトランザクションフィーを高くして認証優先順位を上げるようとします。トランザクションフィーが少ないといつまでも未承認のままの状態になるからである。以上さまざまな要因によって、ブロックチェーンのマイナー数が変動する。マイナー数が減ると、悪意を持ったマイナーが不正なブロックをブロックチェーンに繋げる、のっとり（51%攻撃）がしやすくなるリスクが増大する。

**(3) インターネット資源の限界をどう考える**

現在ビットコインブロックチェーンのマイニングプールの 90%、マイナーの 50%以上を China が占めている。China には Great Firewall が存在し、ネットワークトラフィックの制限（最悪、遮断）を実施。これによりノード間のマルチキャスト時間に影響を与えているためブロックサイズの拡張、マイニング間隔の短縮が容易ではない。今年 12 月に香港で行われた会議において、ブロックサイズを 2 倍（1 Mb→2Mb）にしかつ、圧縮ロジックによって TX 数を 4 倍にし、合計現在の 8 倍の TX 量を処理できる案が提案され概ね受け入れられた。（最終決定ではない）。ビットコイン以外のブロックチェーンの構築にも同様の課題が存在する。

● まとめにかえて

従来の中央集権的で行われた、機密性（Confidentiality)完全性、(Integrity)可用性、（Availability）の確保のための管理コストを、分散合意にしたら本当に安くなるのか？そして未来永劫保証されるのか？

いろいろな条件があり、まだ結論できない。

まず、全員が（日本国民があるいは全世界が）分散合意形成という全く新しい考え方に積極的に参加していけるかが問題。すでに（日本のように先進国では）サービスが完成しており中央集権型管理体制に慣れてしまっていると、心情的になかなか納得いかないと思う。

ビットコイン 2.0 はインフラである。従って、その上に稼働するアプリケーションがどんな価値を生み出すかが重要である。現在金融を中心に進められている「Fin Tech」の流れで活用しようと検討が進んでいるが、ビットコイン 2.0 でなければ出来ないというものでもないため、むしろ金融以外のさまざまな領域（流通とかサービスとか、あるいは IoT 活用全般）での検討を期待する。

５．次回ＩＴＢＯ研究会

| | 開催日 | | 時　間 | 場　所 |
|---|---|---|---|---|
| | | １月１３日（水） | １６：３０－１８：３０ | ＢＣＡＯ 東京オフィス |

次回、祝日を挟むため開催曜日が変わっています。ご注意ください。

関西地区から参加される予定の方は、会議通話を用意しますので事前にご連絡ください。

６．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 |

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）、露木様（ホーキングジャパン）、徳永様が ML にて参加されています。

（以上）