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9回 議事録

1. 開催概要

●開催日 ：2016年1月13日（水）16：30～18：30

●開催場所 ：BCAO 東京オフィス

●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）

2 年間の ITBO 研究会活動、残すところあと 3 回になった。今日の話しの中心は ITBO 研究会活動を振り返り、どうまとめていくかである。

今日は具体的なアウトプットと言うよりも自由にみなさんのご意見お考えを述べていただき、次回以降じょじょに集約させていく。

また今日は年初第一回なので、おひとりずつ、新年の抱負プラス最近の出来事をご紹介いただきたい。

K氏：退職して1年経った。現在シニア学校で勉強中。

N氏：昨年はマイナンバー施行関連で全国を飛び回った。「サイバーセキュリティ 経営ガイドライン」が昨年末経産省等から発表されたことを契機にセキュリティがもっと経営にアピールでき投資が行われるようになることを期待。

O氏：昨年ITBO研で取り上げたビットコイン 2.0 とその基礎技術であるブロックチェーン関連の議論があったが、これと時期を同じくして社内でも研究検討が進み、年初にプレスリリースができた。

S氏：IoT社会が実現するとビル設計、施工もこれを避けて通れない。間違いなくIoTが分からなければ設計できなくなる。今から勉強しつつ、将来のインテリジェントビルのあり方を考えている。

I氏：昨年末からいろいろバタバタしていたが、やっと落ち着いた。ITBO研で取り上げてきたビットコイン、ブロックチェーン、スマートコントラクト、というテーマが面白い。突き詰めて考えていくとぐるりと回ってインターネットとはなんだという命題にぶち当たる。最近アップル社のスマホに乗り換えて、ネットとは結構セキュアじゃないことが理解できた。ただ家族と会話すると、当然だと言われショックを受けている。

Y氏：昨今のセキュリティ事情を見るにつけ、中小企業においては（サイバー）セキュリティを担保することは所詮ムリだという意識を持った。セキュリティ会社のサーバがハッキングされ顧客情報が漏えいした事案も報道された。もう、すべて情報は流失するのが前提と考えておかないといけない。

O 氏：年初から電力自由化が話題に。今年 4 月から開始される。自由化されることによってコストが下がりサービスが向上すると期待される。一方で供給元が複数になるだけでなく自分で発電し売電もできるので電気の売り買いのやりとりが東電をトップにしたツリー型から Any-to-Any になり全体の管理が複雑化する。これを「見える化」し安く管理するシクミが求められる。電力の安定供給と自由競争によるサービス向上のふたつをどうやって達成するかが大きな課題となる。

T氏：約 25 年前に金融で第三次オンラインがあった時、各銀行ファームバンキングのフォーマットが全銀手順により統一された。これはネットワークのレイヤーレベルの統一ではなく金融業界で電文フォーマットが決まったということ。この結果、IT不況期、不動産賃貸管理で銀行からデータの消込みが半自動化され急激に効率化ができ、IT 業界も一息つくことができた。今 Fintech の世界で決済データの複線化（銀行、カード、プリペイドカード、ポイントカード、地域振興券その他異業種間のまとめ割引き決済などなど）のオムニ化に対応するためにブロックチェーン技術が活用できるのではないかと見ている。（しかも同時に安くサービス向上可能）この議論は業種、業態、ビジネスシーンに応じて変わるので我々はビジネスケース（ユースケース）で語らなければならない。

（2）連絡事項（報告：大塚）

略、1 月研究会アジェンダをご覧ください。

3．今月の ML の話題

MLで話題になったテーマについて振り返ります

●サイバーセキュリティに関する国家資格について

「情報処理安全確保支援士」の設置。一般企業に対して「情報処理安全確保支援士」の設置が、義務付けられるという新聞報道。どういうところで使うのか、また何ができないのかなど詳細は不明。政府のIT人材育成の施策の一貫か。試験合格+CPD（継続的研鑽）+3 年ごとの資格更新が必要となる。ITSS の技術レベル4相当なのでかなり高い。一方で2016年4月から「情報セキュリティマネジメント試験」が開始される、これは ITSS の技術レベル2相当（HP では 2 と書いているが実際は 1.5 程度）。これはユーザの立場の試験。

●政府の企業向けサイバーセキュリテイガイド

12/7 に「IoT 社会に向けたデータ利活用施策及びサイバーセキュリティに関する対応」が発表。12/28 にIPA、経産省が「サイバーセキュリティ経営ガイドライン」を公開。

経営者における3原則と CISO へ指示すべき重要 10 項目を提示している。10項目の内容はハードル高い。対象は大企業及び中小企業（小規模事業者を除く）のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業という。つまりECサイトは必須ということ。従って規模の大小にかかわらずかなりの民間企業が対象になると思われる。内容をよく見ると、ECなどの業務委託契約に付随した内容に似ている。しかし、NDA を結んでいるとしても再委託先までの関係者への徹底は難しく、また契約先が倒産していることも多い。監査権を担保しても実質監査をやれる状況ではない。

これを解決するアイデアの一つとしてブロックチェーン技術の応用があると思う。（ブロックチェーン技術とは暗号化技術とP2Pによる分散型合意形成から成り立つしくみ）

4．本日のテーマ

2年間におよぶITBO研究会の総まとめを議論する。今日は細かな話しより、結論をどんな方向にするかについて皆さんの自由なご意見、感想を聞く。各回のテーマ、議論のキーワードを1月研究会のアジェンダに入れた。

a.（総論として）今までの活動を振り返り、その時どきさまざまなテーマで議論が行われてきている。われわれで問題を共有した後で世の中でも同じような議論が出てきており、その意味で未来が少しずつ現在に近づいてきていると言える。（K）※例えば、マイナンバー制度施行にともなうマイナンバーの漏えい問題。金銭目的のID・パスワードを盗むサイバー犯罪の増加。2020年東京オリンピックを見据えた対策など。

b. 議論したFact/Findingはリスクでもあるがチャンスとも捉えられるものもあった。
その軸で整理してみたらどうか？　（まだ全然そうなっていないが）国としても費用から投資へといっている。われわれとして、これから起こるであろうことを予言しているみたいなこともあるのでそれを言ってあげるだけでもいい。（N）

c. ITの世界には必ずセキュリティの話しが出てくる。しかし、個人と企業や国のレベルでは対応は異なる、これを分けて考える。例えば企業や国が管理する知的財産情報の漏えい事件は表に出てこない。恐らくこれによる損害のほうが個人情報漏えいよりはるかに大きいのではないか。また企業業績や株価に影響する情報は瞬時に世界をめぐり、相場の変動を誘発経済活動にも影響を与えていることは事実である。これは過去とは大きく違った状況（現象）である。一方で「サイバーセキュリティ経営ガイドライン」の冒頭に、「セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。」とある。こう書かれたら、手の打ちようがない。これを読んだ経営者はここで止まる！攻めのIT投資に向かわせる書き方の工夫が必要と考える。安全工学の教科書の冒頭に、超スーパーカーでもブレーキがちゃんと効くという安心がないとアクセルが踏み込めない。経営も同じ、経営のアクセルが踏めるためにサイバーセキュリティのリスクが正しく認識されコントロールされていることが必須。（ＯＹＩ）

d. セキュリティとは、どういう意味なのかもう一度整理しなおすべきである。例えば、一般人のイメージするセキュリテイとは、自分のPCの情報が知らない人に渡ってしまうことのリスクである。個人情報すべてが完全にクローズでなければならないという盲目的な考えが蔓延、また隠せば隠すほど、これを破ろうとする悪意のある人や組織とのいたちごっこになっているセキュリティリテラシーを向上させセキュリティ管理する情報のメリハリをつけるべきである。（その人それぞれの立場によって全然違うのでどうやってやるかは難しいが）（O）

e. サイバーセキュリティはテーマとしては面白いと思う。マイナンバーは「分散保管」という仕組みで管理されている。いわゆる割符。全部合わせると地図になる。マイナンバーがその一個のパーツとして考えると理解しやすい。個人認証に関して、従来のパスワード管理に加え生体認証（指紋や光彩、あるいは全身認証のしくみ）が取り入れられている。セキュリティを

破ろうとするのはその先にメリットがあるからである。（つまり、個人のカードのIDとパスワードを盗もうとするのは多額の金をうばうことができるから）（T）

f. サイバーセキュリテイは極論を語らなければならないので気持ちが落ちる。99.99%防御したとしても1回漏えいするとダメ。しかし、明るい未来をめざしたい。米国のプロスポーツの世界で、戦略はディフェンスにありという言葉がある。オフェンス（攻め）はその場のマグレで決まることが多い。ディフェンスは事前に入念に計画され実施されるものであるらしい。ベッキーのライン画面が漏えいした事件。10年間築いてきた信頼が一日でなくなってしまったのもラインのIDパスワードのディフェンスの戦略が無かったことが原因だ。ラインの画面が動かぬ証拠になって一発で決定的なダメージを受けてしまう。昔も同じことはいっぱいあったが、言い逃れができていた、今はできない。

g. いろんなリスクの話題が出て、これが顕在化することを考えたら個人や一企業で完全にまっとうすることはできない。サイバーセキュリティはインターネットの繋ぎ口を守るしかないのではないか。ASPの入口出口にしっかり対策をしてもらって、これを自賠責保険のようにして強制的に費用を払うようにするしかない。

h. 攻撃が最大の防御という考えがある。オトリ（ハニーポット）に爆弾を仕込んでこれを取っていった相手にバクダンをブチ込む。ただしDDoSの相手だと難しいが。他にFinal Codeみたいなソリューションは面白いと感じている。究極、ファイル一個一個にセキュリティを仕込むことをしないとダメである。

5. 次回ITBO研究会

	開催日		時　間	場　所
		2月9日（水）	16:30－18:30	BCAO　東京オフィス

関西地区から参加される方は、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、露木様（ホーキングジャパン）が参加されました。

さらに、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）、徳永様が ML にて参加されています。

（以上）