第 1 回 ITBO 研究会議事録

日　時：7 月 8 日（火）　16:30-18:00

参加者：大塚、近藤、加藤、西出、吉川、伊藤(敬称略)

場　所：BCAO 日本橋事務所

① はじめに：

-13 名の登録を得て 26 年度研究会として正式スタート（7 月 15 日現在 14 名）

-岡さん（前座長）手術療養のため当面月例会に参加できず

-伊藤さんが代わりに 26 年度研究会の準備をいただいた

② ITBO 研究会の運営：

-議事録、各種資料等の共有⇒昨年どおり Google Drive の利用で検討する

★　Google アカウントの登録を進めたいが会員で問題があるというご意見の方はコメントいただきたい

★　利便性（容量制限の問題、アクセス制御の問題）を考慮し、他のファイル共用サービスでよいものがあればご提案いただきたい

★　BCAO 事務局（平吾さん）に BCAO としての資料の共有ポリシーの確認を行います

-議事録は、メモとして翌日メールで当日参加者に配信し、加筆・修正を依頼（期間 1 週間）後、議事録として ML メンバーに配信する

可能な限り、ライブ感を以て当該メモを作る（可能な限りメモ取りを行うが、出席者の加筆・修正（期間 1 週間）は前向き対応）

伊藤（高）氏が出席時は伊藤氏がメモ取り、いない時はボランティアで前向きに対応！

-資料を見ての質問はどうか。⇒遠隔参加（リモート）のメンバーとの意識・内容の共有促進したい

-月例の会合は集合いただくことを基本とする。この場合リモート参加の方が難しいか

　⇒ Skype その他のツール利用等今までに色々考えたが、各会社様での社内ネットワーク利用規定含め勤務時間内の参加は色々の意味で難しいという意見多数。

★　特にリモートの会員の方でご意見があればお願いしたい

-開催時間設定　4 時半スタートに関して、いろいろ意見があったが結果、いままでどおりとなった。

女性メンバーからの意見も考慮しての対応であったが今回はいない。

6 時に繰り下げたらよいとの事では無く、会社的(東京ベース)には、夕方に会議等が有れば 4 時も 6 時も同じとの意見多数。

　オプションとしては 5 時半スタートもあり？（これも中途半端な気がする、終了後の懇親会も当会のポイント/完全自由参加にもなっている方もおり、終わりの時間からの逆算）

★　新規会員の方でご意見があればお願いしたい

-開催日：原則第二火曜日とするただし、事務所使用の都合により変更

26 年度は下記（他の意見ある方は ML にて悩み共有し、調整しましょう）

8 月はお休みで、オプションで納涼会を企画(お盆後、ML 連絡)
9 月 16 日（火）16 時半
10 月 14 日（火）16 時半
11 月 18 日（火）16 時半
12 月 9 日（火） 16 時半
1 月 13 日（火） 16 時半
2 月 10 日（火）16 時半
3 月 10 日（火）16 時半

-東京以外から参加いただく方々には、
月例会の出席も是非お願いしたいが、可能な限り ML での皆さんと意見交換、議論していただき仲間感、一体感（出席感）を目指す。
それらのメール文書も議事録、又は共有情報とすることで、研究会活動報告書の材料とする。

資料共有の提案：ML 最大限利用（添付資料含め）
資料共有の方法：グーグルドライブで今までは資料を共有してきた。
運用形態　　：グーグルアカウント必要ですがいかがですか？（資料=pdf,pp,excel,wd:PW は不要で良いでしょうか？）
⇒ML にてメンバーに確認。
⇒前年度は岡座長が当該アカウントの管理されていたが、何でも容量制限があり、古いファイルから自動消去されると言っていた覚えがある。
：研究会の成果として集約させたいとの思いです。

③ 研究会テーマ
-いままでの経緯
（山口さんの昨年度最後の ML メールから）
『なお昨日も有志で意見交換会を行いましたが、今期どういったテーマを扱うかは
未定です。
とはいっても、昨日の参加者では主にサイバー攻撃を受けた後の事業継続をどう
考えるかといった点に関心を持たれた方が少なくありませんでしたのでこちらを
しばらく研究していこうかと検討しております。
具体的には IT セキュリティは予防が主で語られていますが、実際に被害にあった、
情報が漏えいした、といった際にどのように対応すべきなのか、実際の現場では
どうなのかといったところを専門家を招いて講演、議論を行うことを検討してお

ります。
しばらくは IT 絡みの話があるかと思いますが、こういったテーマにご興味のある
方、もしくは BO 方面からこういった研究を行いたいといったことも歓迎ですので
是非ともご参加をご検討くださいませ。』

-上記を受けての議論、発言者：（敬称略）
吉川：外部サーバから情報漏えい事案（例）を紹介しつつ説明。(吉川さん資料リンク参照)
★　吉川さん加筆修正対応お願いします。
大塚：そもそものサイバーリスクって何だっけ？
加藤：（別途 IPA 資料リンク参照）
情報システム部門だと官庁提出の義務あり、そのフォーマットを見る。
システム側の対応はシンプルで、下記のとおり
・被害にあった PC,サーバのスクラッチインストール
・攻撃の「気配」があった時は止める。ただし自社システムだと止めれば良いが、お客先のシステムだと簡単に止める訳には行かない。
西出：フォレンジック（予防）⇒ログをどうとっているかどうか？　等々
加藤；運用対応者はピリピリ状態、攻撃されているか否か「気配」感の中での判断になる場合がある。
大塚：データの外部漏えい、改ざん、喪失した場合のビジネスインパクトを評価しているのか。事後対応がいつもきまって同じような気がする。
加藤：情報の内容による？　個人情報？
吉川：お客見込み情報の漏えい？
加藤：BIA の結果はベンダー側の謝罪する人間が、部長レベル、事業部長レベル、役員レベルになるだけ。どのポジションの人間が謝りに行く程度の話。
大塚：情報漏えい等を生じるリスクって具体的には…？
吉川：SQL インジェクション、web からの侵入事故はかなりあったが・・・
大塚：昔は（個人の）愉快犯だったが、今は国家レベル或いはプロの（集団の）世界となっている。これはもう戦争！国民全員が共通認識し危機感をもたなければならない。
吉川：銀行決済端末をとられて、勝手に振り込まれる等：IPA の資料参照　pos 端末が xp ベースかもしれない。
加藤：制御系システムもクローズドでは無いので、入り込まれる可能性がる。
吉川：上半期は OPENSSL でしょ？　xp 端末の存在がリスク
大塚：すでにネット上にある情報を組み合わせ類推することによる個人情報の特定化ができる。（振り込め詐欺で使われている事例あり）もはや情報漏えいを完全に防ぐ方法はないね。ネット上に拡散した（個人）情報がどういう悪いことに使われるか、結果どういう影響が起きるのか自分でしっかり理解したうえの対策（起きちゃったときどうするか）を考

えなくちゃだめだね。
加藤：米国：粗雑な方法によるアタックも範疇、個人情報の匿名化？
　　個人情報法、法律との解釈、（厳しすぎるのではないの？）
　　どこでシステム止めて、誰が謝りに行ってという事が現行のベースだが、「気配」「とられつつある」状況についての判断にかかっているのは事実。
吉川：埋め込み型 OS/責任は機器メーカー、OS はサポートされる
　　リスク共有は有りだが、結果事象での対応ではないか（笑）
近藤：やり方それなりに・・・
　　情報整理：盗まれる、使われ方等、情報の内容の整理。

PS:17 時 37 分に野原さん（京セラ）と個人携帯のスピーカーモードで自己紹介や、メールで言われている事を参加者で確認した。

④　当研究会の活動を行った結果最終的に何が出来ているかの議論
-世界はまだしも日本ではまだこのような研究が遅れていると言わざるを得ないので、大きな提言だったりするのも良いのではないか。（ネット）利用者や会社の人たちへのメッセージ含めて。
-自分だけなら良いが、他の事象との絡みからすると、何とも言えない。
-ガイドライン、チェックリストの作成。会員の皆様のお仕事に関連し有効に使えるものがいいね。
・ファイルを取られた時、それに入っていた中身の精査や影響の確認（何が取られたのか、どこまで取られたのか）⇒自然災害だったら被害内容は明らかだが、これは最終的にわかるのか否か？そのリスクは何か？
・対応はどうするのか？　ログが有れば全部わかるのか、他のサーバとの関連でどこまでわかるのか？　⇒何をログで残すのか？　とか色々あるだろう。何を取られたか特定するのは大変でしょう。
・セグメント別の提言まで持って行ければ、指針、チェックリスト等の提言をゴールとする。

関連サイト・情報・文献等（前述の論議にもあり）
セキュリティ本山、NIST　SP800, 内閣情報セキュリティセンター、
東京法令出版　サイバー犯罪捜査入門　基礎編、操作実戦編、捜査応用編

宿題：次回まで下記サイト内からの情報を各自チェックしてみよう！
十大脅威
http://www.ipa.go.jp/security/vuln/10threats2014.html

被害状況調査
http://www.ipa.go.jp/security/fy25/reports/isec-survey/index.html

⑤　おまけ。重要な懇親での協議（何を飲みながら協議したか？）
-ITBO 研究座長をどうする？
⇒大塚さん(2 代目座長であったが再登板)にお願する。岡前座長へ意見招請を行う。
⇒但し、この先 2 年間どうなるかわからないので(皆そうだが)、変更がある時は又皆で前向きに話し合おう。
（大塚コメント）座長の選出は研究会会員皆様全員の意思の確認が必要です。今回は非公式な打診と認識しております。正式には、全員に対し公示、選挙、同意を行うものとなります。