情報システム・バックアップオフィス研究会（ITBO 研）　２０１４年度　第５回　議事録

１．開催概要

●開催日　　：２０１４年１２月９日（火）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　：６名（出席者名は末尾参照）

●配布資料　：［IPA「新しいタイプの攻撃」の対策に向けた設計・運用ガイド　改定第二版］
［情報セキュリテイ 対策実施チェックリスト］(前回配布物と同じもの)

２．議事内容

（１） はじめに　（報告：大塚）

早いもので今年最後の研究会となりました。今日は研究会終了後に忘年会があります。
幹事は関山さん、今日は姫路から忘年会に間に合うよう駆けつけてくれます。
師走の忙しい日々ですが、今晩だけは少しだけ楽しみましょう。

（２） ご連絡事項（報告：大塚）

① BCAO 運営会議（11/25 開催）で各運営部門担当理事から進捗・課題を報告。BCAO 会員増加問題について意見交換。
これについての ITBO 研メンバーからのコメント、
- 会員増加にあたり、まずタイムリーな情報公開が必要だ。BCAO 活動（月例勉強会、講演会、研究会活動成果など）をコンテンツとして BCAO ポータルにアップしオンデマンドで簡単に入手できる仕組みを考えて欲しい。（最近は講演動画など、金をかけなくても安く簡単に作成できるツールが利用できる）
- もはや、世間は“BC とは”という情報を求めていない。Needs がどこにあるかもっと Marketing 調査を行うことが必要。

② BCAO 12 月度勉強会；12/18 14:00-17:10「サプライチェーンと BCM」（山口さん/インターリスク総研）「取引先の事業継続能力評価手法について」（伊藤さん/富士通総研）@国立オリンピック総合センター。引き続き意見交換会があります。17:10-19:00。出席者が少人数で固定化しているので皆さんもぜひご参加ください。

③ ITBO 研会員拡大、およびデイスカッションを深めるために、一部部外者との ITBO 研 ML によるメール交換を行う。ただし、一時的に ML に追加登録するのではなく、Bcc としてメールを転送する。逆に意見を発信する場合は座長経由で ML に流す。部外者名は議事録にてオブザーバーとして明記する。現在、伊藤（嘉）氏、日下氏、斎藤氏と情報連携している。今後小友氏が加わる予定。（下記名簿参照）

３．本日のプレゼンテーション・意見交換

（１）昨日までの ML デイスカッションから　（報告：大塚）

①　ドローン（Drone）の商用利用の期待。

もともとは、米軍など軍事無人偵察機。技術的には「火星探査機（キュリオシテイ）」とか「はやぶさ」でも目にするもの。
当初、災害現場で人が近付けない場所に空から偵察し情報をリアルタイムで収集する活用を議論したが、最近 TV やネットで盛んに紹介されている。NHK TV「さきどり 11/30(日)8:25-8:57 http://www.nhk.or.jp/sakidori/backnumber/141130.html
（以下デイスカッション概要）
・セコムが警備利用での技術開発中。先進国（米国）ではアマゾン、グーグルが積極的。
・ドローンで収集した Big Data を分析し意味のある情報を取り出すソフトウエア（物体、人物認識、デジタルサーベイランス）が必要となる。今後新技術が開発されるだろう。
・グーグルは、IoT からの BigData を収集し価値あるデータ解析をすることにある。グーグルが取り組んでいる車の自動運転技術と同様と想像する。
・欧州では、ドローン飛行を規制。米国は来年 FAA が商用ドローンを飛ばすガイドラインを発表。日本では、まだ法整備が十分でない。（空港周辺および 150M 以上、有人で飛ばすときだけ航空法が適用される）。まだラジコン飛行機の領域で止まっている。
・ドローンは事前に目的地情報をセットすれば自動で飛行し空中で停止する。ラジコン機に比べ、はるかにインテリジエンスがあり操縦者は熟練した飛行テクニックが不要。
・現在のコモデイテイ技術を利用して安価に高性能な機器を作ることが可能になっている（ここで、Raspberry PI の紹介、CPU 本体で¥4,700.-ナリ）。
・コモデイテイ通信手段として既存の Internet（Wifi 網,携帯電話網）を使う。しかるべき人がしかるべき指示をしかるべき機器に送信し、収集した（映像）データを正しく受信するために Trusted Network が必須。ここでもサイバーセキュリテイを確保するテクノロジー＆ルール作りが必要。
・我が国にはまだ、商用ドローンを取り巻くさまざまな課題を包括して検討するコンソーシアムがない。New Business として育成するために早急のアクションが求められる。
（参考）ドローンを経験することで、リーダーはどんな気づきを得ることができるか
http://diamond.jp/articles/-/48075

② 首都圏大停電にどう立ち向かう？
もし、24 時間を越える停電が発生した場合オフィス（高層ビル、インテリジェントビル）には留まれない。照明、通信機器のみならずエレベータ、空調、給排水が使えなくなるため。
現在電力会社 1 社だけに頼った電力供給を複線化できないかを議論。
電力もＩＴシステムと同じ歴史をたどる？
かつて、メインフレームによる一極集中システムで発展。その後、クラサバシステムが出現、分散処理で EUC がブームに。電力もＩＴシステムのように安価で安定的に品質のよい電力供給が実現するだろうか。
（以下デイスカッション概要）
・先日の徳島県豪雪による大規模停電では電話（IP 電話）が不通となった。
防災電話は電池稼働のため使えた。一般の電話機（黒電話、ISDN 電話）は交換機から

電力が供給されるため交換機が稼働していれば使える。

・ソーラーや風力など自然エネルギー利用は発電効率にムラが発生する。多い時は捨てられ、少ないときは（原発など）ベースロード電源から供給しなければならない。結局、蓄電技術の成功（蓄電効率の向上）に依存する。蓄電効率を向上させると蓄電池の（爆発）危険性が高まる。常に効率性と安全性を天秤にかけている。

・電気の地産地消について。初代プリウスがソーラーパネルを積んでいた。しかしこれは社内空調の一部の電力に使うためのもの。実用性を考えたものではなし。

・3.11以降、カセットコンロボンベで発電する機器が発売された。

・電気の地産地消をすすめるには、現在の固定概念、つまりいつでもどこでも品質のいい電気が手に入って、電気代が単一料金で使い放題という考えをやめる必要がある。地域、家庭、（車などの単一）機器で電気をいつどのように使うのか、地域、家庭、個人でコンセンサスを形成し用途にあったエネルギーの活用を考える。たとえば、EV（電気自動車）であればガソリン車のあたりのガソリン代と電気代を比較する。１KM走行するための電気代<<ガソリン代であれば、今の電気代（単一料金）より高くてもよし。

有限な資源としての電気を大事に使う利用者のマインドを醸成することが大事。

・水素エネルギーへの転換も候補となる。トヨタ　FCV-Miraiの発表。水を電気分解して水素を作るとは、大量の電気が必要ということ？

http://www.itmedia.co.jp/smartjapan/articles/1411/25/news045.html

水素ステーション建設は東京オリンピックを目標に国も後押し。ただし現在水素エネルギーはコモデイテイ化していない。コストダウンにはこれからの普及が鍵となる。

③　最新話題本：新刊書、久世浩司著「なぜ、一流の人はハードワークでも心が折れないのか？　実践版 レジリエンス・トレーニング」

「レジリエンス」という言葉に気が引かれて、つい買ってしまった。ここでは心理学上のレジリエンス。「回復力」、「緩衝力」、「適応力」で定義される。「ストレスの多い働き方」を「レジリエンスのある働き方」に変えるにはどうすればよいかについてレジリエンス・トレーニングを説明。

（２）「標的型メール攻撃～皆さんの会社ではどう備えている？」（報告：大塚）

前回、時間切れとなったテーマ。次回（2015/1/13）、IIJ 斎藤氏の講演を予定。

その下地のデイスカッションを行い次回議論のポイント、方向性の共通認識を持ちたい。

（参考）「対策実施チェックリスト」※前回配布した資料

「新しいタイプの攻撃」の対策に向けた設計・運用ガイド改訂第2版

https://www.ipa.go.jp/files/000017306.pdf

・Google,Yahoo を狙った攻撃（Operation Aurola）イランの原子力施設を狙った攻撃（Stuxnet）米国中央軍ネットワークにおけるウイルス感染（2008 年）、三菱重工業の軍事情報を狙った戦略的多段階攻撃（2011 年 3 月-5 月）など重要インフラを標的にした高度で悪質なサイバー攻撃が発生している。

・「新しいタイプの攻撃」とは、複数の攻撃パターン（ソーシャルエンジニアリング、ゼロデイ攻撃、USB デバイス、外部指令サーバ（C&C サーバ）との通信、個別システムに特化

した攻撃）を組み合わせた特定企業、個人をねらった攻撃。
個々の防御システムをたくみに回避するように組み合わせてあり、あらかじめ目標に合わせて攻撃が設計されている。
・政府は、今年5月に情報セキュリテイ政策会議で「重要インフラの情報セキュリテイ対策に係る第3次行動計画」を決定。障害体制の強化の中で重要インフラ業者に対し、「IT-BCP」本体の実効性検証、「IT-BCP」発動の際の連絡、対応体制等の検証、以上CHECK(確認)、実効性検証を踏まえた改善点の抽出・分析、以上ACT(是正)、演習から得た改善点に基づく「IT-BCP」等関係規定の整備・見直し、以上PAN(準備)を明記。
具体的に国は重要インフラ業者に何を求め、重要インフラ業者はどこまで対応できているか？まさか、国はセプター（CEPTOR）セプターカウンシルだけ作って何もしていないことはないよね。BCMを回すだけでなく、中身のある議論をしてるのか？
・同じく今年5月、情報セキュリテイ政策会議で決定された、「新・情報セキュリテイ人材育成プログラム」で、人材の質的・量的不足、情報セキュリテイ従事者役26.5万人のうち約16万人が質的に不足、さらに約8万人が量的に不足とし供給側の対策として、IT技術者等に、情報セキュリテイを必須能力として位置付け、訓練/演習教材等の作成や能力基準・資格のあり方の検討を進めるとしているが、この中にIT-BCPの能力アップについてどこまで考慮されているか？IT-BCPもビジネス要件から構築されるのでビジネス-ITの視点が必須。IT技術者には十分ではない方も多い。
なお、重要インフラとは、情報通信、金融、航空、鉄道、電力、ガス、政府行政サービス、医療、水道、物流、化学、クレジット、石油 の１３の業種
・重要インフラの事業継続を達成するには企業として標的型攻撃にどう対応するか議論
（以下デイスカッション概要）
・情報通信業者の場合、「通信の秘密」は、憲法と通信保護法で守られている。
それが故に仮にDDoSなどの攻撃だとわかっていても通信を止めることができない。
法曹界を含む研究会にて仮に通信停止した場合、攻撃の防止以外の用途で利用しないならば、「正当業務行為」として違法性が阻却されるとの意見があり。
・遠隔ウイルス操作事件（いわゆる誤認逮捕事件）はサイバー事件でありながら
逮捕・立件は偽計業務妨害罪、ハイジャック防止法違反とならざるを得なかった
法整備が急務である。
・特に重要な社員向けセキュリテイリテラシー教育について。
KYT(危険予知トレーニング、製造現場で古くから使われている手法)のeLearningを
全員に実施している。
・ネットワークポリシーとして、社内から安易にインターネットを閲覧できないようにしている。
・ProxyでGlobal　IPがネットに流れ込まない設計としているほか、万が一Global　IPが流れていることを発見した場合、ただちにウイルス感染を疑い厳密な調査を行っている。
・上記以外にネットワーク設計で出口対策を行い、バックドア検知、ウイルス拡散を防止する方法がある。

-サービス通信経路設計（F/W の外向き通信遮断ルール設定、F/W の遮断ログ監視）
-ブラウザ通信パターンを模紡する http 通信検知機能の設計
（http メソッド利用バックドア通信の遮断）
-RAT の内部 proxy 通信（CONNECT 接続）の検知遮断設計
-最重要部のインターネット直接接続の分離設計（VLAN で設計）
-重要攻撃目標サーバの防護(ActiveDirectory を管理するセグメントを分離)
-SW 等での VLAN ネットワーク分離設計（利用セグメントと管理セグメントの分離）
-容量負荷監視による感染活動の検出（SW の異常値、負荷やログ容量の検知）
-P2P 到達範囲の限定設計(不要な RPC 通信の排除)
・しかし、上記の対策をとっても完全に防護することは不可能。従って事故発生前提の対策計画が重要。危機管理体制と手順の確立。ケーススタデイによる演習を繰り返し行い全社的な対応能力を向上させる。
・攻撃による組織への損失を見極め、コスト vs 効果を考慮した対策立案とすること

・現状課題として情シス部門の各担当者（専門家）間の連携が出来ておらず、システム全体の脅威の把握、コントロールが出来ていない。

- プロジェクトマネジャー（開発、運用）
- セキュリテイアドバイザー
- 各製品担当

・Sony　Pictures Entertainment社の報復攻撃。これってアリ！？
http://jp.reuters.com/article/topNews/idJPKBN0JP2LM20141211

４．これからのＩＴＢＯ研究会の日程

	開催日		時　間	場　所
次回	2015 年	１月１３日（火）	１６：３０～１８：３０	ＢＣＡＯ 東京オフィス
		２月１０日（火）	１６：３０～１８：３０	ＢＣＡＯ 東京オフィス
		３月１０日（火）	１６:３０-１８:３０	ＢＣＡＯ東京オフィス

以前お配りしたアジェンダの中の１月の開催日が間違っていました。正しい日時は、1 月 13 日（火）16:30 からです。お詫びして訂正いたします。どうぞお間違え無いようお願いいたします。

５．お願い

ITBO 研は日々の ML での情報交換＆デイスカッション活動が中心です。月例会は、それまでの ML のやりとりの整理と発信者からのコメントと追加のデイスカッションです。
ML でのやりとりは座長にて交通整理を行うので、みなさん、積極的に課題を提言し、どしどしデイスカッションに参加してください。
次回は斎藤氏（IIJ 政府情報セキュリテイ有識者）をお招きしての月例会です。今回たいへん良い機会ですので多数の方の参加をお願いいたします。ご質問、ご意見は事前に ML にてお願いいたします。
また、前回定例会にて、IIJ 斎藤氏の講演を次回 12/9 と発表しましたが、都合により 2015/1/13

に変更になりました。お詫びして訂正いたします。

６．２０１４年度　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	関山　雄介		大成建設
3	副座長	伊藤　高信	○	FUN Inc.
4		近藤　隆一	○	富士通エフサス
5		岡　伸幸		ソフトバンク BB
6		吉川　明人	○	ＮＥＣネクサソリューションズ
7		安齊 隆正		富士通エフサス
8		海田　雅人		東京共同会計事務所
9		西出　三輝		損保ジャパン日本興亜リスクマネジメント
10	BCAO 大阪オフィスから参加	野原　英則	○	京セラ
11		宮島　正孝		セイコーエプソン
12		山口　孝一	○	IIJ
13		森口　泰樹		AIG
14		加藤　誠		日立コンサルティング
15		後藤　富雄		イマジネーションテクノロジーズ
16		木村　信弥		株式会社　ディー・オー・エス
17	オブザーバー	伊藤　嘉浩		キングフィッシュコミュニケーション
18	オブザーバー	日下　太一		住友電気工業
19	オブザーバー	斎藤　衛		IIJ
20	オブザーバー	小友　修		富士通エフサス
21	オブザーバー			

（以上）