

情報システム・バックアップオフィス研究会（ITB0 研） 2014年度 第4回 議事録

1. 開催概要

- 開催日 : 2014年11月18日（火） 16:30～18:30
- 開催場所 : BCA0 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 標的型攻撃メールの傾向と事例分析 <2013 年>]
[情報セキュリティ 対策実施チェックリスト]

2. 議事内容

（1） はじめに （報告：全員）

皆さんの近況を一言お願いします

- ・ 京都の秋は公私ともイベントがいろいろあり多忙の毎日。来週は高松にてお茶会のお手伝いがある（高）
- ・ 子供の受験を控え、家じゅう落ち着かない（雄）
- ・ 仲間と非接触タイプの小型心拍数計測機のプロトタイプを開発した（実機デモを拝見）
24/365 データを計測しサーバに転送することにより健康 Big Data として活用。
高齢者医療への展開が期待できる。（富）
- ・ 業務目標達成の号令のもと全社一丸となって奮闘中。（明）
- ・ 鈴鹿 4 耐に参加。ただし、自転車です。バイクレースと違って逆コース。下りは 6-70km 出ることも。全参加者中ほぼ真ん中でゴール。楽しい一日でした。（孝）
- ・ 42 年ぶりの高校同窓会に参加。還暦同窓会！卒業後初めて再会する友人もあり名前を聞いてびっくりすることも。それぞれの人生を経て今元気であることに感謝。（純）

（2） ご連絡事項（報告：大塚）

- ① BCA0 運営会議（10/28 開催）で BCA0 会員数問題についての高橋副理事長から報告。（資料回覧）。現会員のモチベーションアップと新規会員獲得のための宣伝プロモーションの 2 つについて議論。
- ② BCA0 11 月度勉強会；11/20 「BCMS/ISO/訓練等々取組実態調査・分析でわかったこと大公開！」（副島さん/ニュートンコンサルティング）「首都圏における本社機能の継続について」（伊藤さん/富士通総研）@国立オリンピック総合センター
- ③ BCA0 アワード 2014 イン仙台の会場決定。2015 年 3 月 16 日（月）13:00 @AER TKP ガーデンシティ仙台 ホール C。この期間に BC/DR 関連企業、団体のイベントが多数企画されている。ITB0 研参加メンバーの企業も参加の予定あり。機会があれば参加してみたいか。
- ④ 12 月の研究会では終了後忘年会を企画します。奮ってご参加ください。

会場はBCAO 東京オフィス近辺。

⑤ 関西支部 日下さんとのコラボについて。

最初はテーマに応じて ITB0 研 ML で参加していただく。ゆるいつながりから始めて、状況を見て定期研究会に参加するなど徐々に深めていく感じでいきたい。

(3) 本日のご議論事項 (報告: 大塚)

① ITB0 研究会のメンバー以外の方への ML 配信について

現在、ITB0 研のメンバーになる予定の方に ITB0 研活動を理解してもらうために 1 名 ML のメールを転送している。また特定のテーマに対し専門家の方にディスカッションに参加してもらうために 1 名を予定。今後 ITB0 研のメンバーの拡大のため加入してくれそうな方に ITB0 研の活動を紹介するために ML 内容を配信することも想定される。

以上より ITB0 研としてディスカッションした結果、以下合意した。

-ML の利用はオープンで自由な意見交換の場という原則で柔軟に運用する

-転送するかどうかはテーマごとにケースバイケースで判断し座長に一任する

-個人メールアドレスを ML に組み込むことはせず、CC で配信する

-Read Only になるため、発言する場合は座長へ依頼していただき転送するものとする

-メールの内容が残ったり転送されたりすることもありうるため、機密情報のやり取りは禁止する

-基本的に ITB0 研に加入していただき、ML に登録されるのが望ましいが当面は柔軟な運用で様子を見る

3. 本日のプレゼンテーション・意見交換

(1) 昨日までの ML ディスカッションから (報告: 大塚)

- ① ドローン (Drone) とは小型無人航空機のこと。目的地までの自動飛行・姿勢制御技術、遠隔操作技術、高性能カメラ撮影技術、情報伝送技術の発展により、映像産業のみならず、災害時の情報収集活動、建築建造物の構造体躯体健康調査、密漁船監視など多方面の利活用が期待されており、米国では今後 10 年で 8 兆円規模と見込まれている。

(参考) ドローンを”斜め上に行く発想”で使う

<http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/100800080/>

伊藤氏、2 トントラック 2 台分にもおよぶ機材のコレクション収集の経験あり。

趣味としてのラジコン、ビジネスとしてのドローン技術についてさわりを語っていただいた。

普及にあたって、自動・自律的に目的地に到達する飛行体の安全性信頼性の確保、遠隔制御技術の向上にかかわる情報セキュリティ技術に関する各種法整備が必要になる。

現在は航空法、電波法その他関連法規でも明確に規定されていない。

先行している米国では来年から本格的な商業利用の許可が下りる予定。

(参考) NASA がドローンの交通整理を検討中か

<http://nge.jp/2014/09/10/post-5299>

(参考) ドローンの交通整理がいよいよ本格化

<http://nge.jp/2014/10/23/post-86621>

(2) 欧米の重要インフラのレジリエンス対策から学ぶ日本の対応について (報告: 伊藤)

加藤さんから紹介いただいた2つの資料をきっかけにMLにてディスカッションが展開された。今回、伊藤副座長さんから議論のポイントを整理し解説いただいた。

(参考)「重要インフラ防護におけるレジリエンス・マネジメントについて 平成24年度」
2013.2 CSMI研究所

(参考) Presidential Policy Directive大統領政策指令 -- Critical Infrastructure Security and Resilience. February 12, 2013

- ・ Resilienceという言葉は2005年ころから広まった。
- ・ ASIS SPC. 1-2009 「組織のレジリエンス: セキュリティ、準備態勢及び継続マネジメント・システム—要求事項と利用ガイダンス」米国規格協会、2009年3月、でレジリエンス・マネジメント・システム (CERT-RMM) の標準ガイダンスが初めて出版された。
- ・ CERT-RMMはレジリエンス活動に実際に取り組む際の組織としてのマネジメントのあり方について規定したもの。その後、ISO22323に取り組みされたが、変遷ののちISO 31000、ISO 22301へと引き継がれている。
- ・ 組織でレジリエンス・マネジメントを実施するには、セキュリティ、事業継続、災害復旧、IT運用に係るマネジメントについての知識と理解力が必要となる。
- ・ CERT-RMMの詳細については上記資料を参照のこと。
- ・ Resilienceという言葉の定義は実は一つではない。それぞれの国、団体、組織で微妙に食い違う。米国では、歴史的にFloodが業務リスクとして重視された。その後9.11、Hurricane被害を経験しこれらを想定した検討が進んだ。

以下、参加者コメントサマリー:

- ・ Resilience がSecurity/BC、DR/IT運用管理の3つの領域をカバーするということはITガバナンスの概念と同じだ。JIPDECさんの扱うSecurity Management・BC Management・IT運用管理の3つの認証サービスの世界だね。
- ・ サイバー軍隊の設立はここ10年くらいの話。日本は、「サイバー防衛隊」を今年(2014年3月26日)発足した。

(参考) 自衛隊の「サイバー防衛隊」発足、防衛大臣直轄で脅威に対処

<http://itpro.nikkeibp.co.jp/article/NEWS/20140326/546344/>

- ・ 大企業であってもレジリエンス(減災対策の視点)への投資は他社の動向を見ながら判断しているのが現状。保険的な概念であるという捉え方が有力。これではリスク対策投資が景気に左右され増減してしまう!
 - ・ 2003年経産省の「情報セキュリティ総合戦略」(部会長 寺島実郎)で、[しなやかな「事故前提社会システム」の構築(高回復力・被害局限化の確保)の実現]が提唱された。その、戦略1: しなやかな「事故前提社会システム」の構築(高回復力・被害局限化の確保)の実現(2)~事故対応策の、抜本的強化の具体策として、企業・個人におけるリスクに対する定量的評価手法の開発とあったが、いまだに実現していない。
- なお、この戦略の中に重要インフラ業者のサービス継続・復旧計画ガイドラインの整備

が明記されている

- ・ 攻撃者（ハッカー集団）と被害者（ユーザ）のスキルを比べるとダントツに攻撃者が上手（うわて）。結果、被害者が攻撃を受けた場合CERT（インシデント対応の専門家集団）への依頼と対応（復旧も含めて）が必須となる。
- ・ 霞が関は各府省にそれぞれCERTを置いているのに、人材は2年でローテーションする。これではノウハウが蓄積されないし、専門人材が育たない。
- ・ リスクマネジメントは経営の責任だが、経営者はサイバー攻撃のリスクが何かを理解していない。
- ・ 米国はサイバーテロ対策とは誰が何のためにやるかがはっきりしているが、日本はやもやした感じである。
- ・ 日本においては最悪の事態（国の存続のために誰を選び、残すのか）の定義がなされていない。つまり、危機管理意識が余りにも欠落している。

（３）（予告：2015/1/13ゲスト講演会）重要インフラ業者のサイバー攻撃への対策について
（報告：大塚、山口）

以前ITB0研でお話いただいたサイバーセキュリティの第一人者で内閣府情報セキュリティセンターでも活躍されているIIJの斎藤氏にITB0研での講演をお願いしています。重要インフラ業者が直面するサイバーテロの現状と政府の取組み、企業での対策のポイントをお聞きしたいと思います。

多くの方の参加していただき、ディスカッションしたいと思いますので、是非日程の確保をお願いします！！

（背景）

- ・ 今年5月に情報セキュリティ政策会議で「重要インフラの情報セキュリティ対策に係る第3次行動計画」が決定された。

<http://www.nisc.go.jp/conference/seisaku/ciip/dai37/pdf/37siryou02.pdf>

- ・ 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の業種です。

- ・ 毎日のようにサイバーセキュリティ関連のニュースが流れている。

－ 衆院議員にサイバー攻撃 標的メール、海外発信か 解散情報狙う？

<http://headlines.yahoo.co.jp/hl?a=20141123-00000054-san-soci>

－ 国内大手サイトでハッキング？報告相次ぐ 「シリア電子軍」が 世界的に影響

http://headlines.yahoo.co.jp/hl?a=20141128-00000006-zdn_n-sci

- ・ 例えば情報通信業者は電気通信放送事業の2つですが、事業者および国は、P（予防抑制）D（検知回復）C（確認）A（是正）の各フェーズでどのような対応をしているのか？裏話を含めてお聞かせください。

- ・ リスクベースの進め方、（たら、れば=What if ?）の例や具体的な話をしていきたい。

・ 国の進めようとしている重要インフラ業者に対する具体的な政策案は？その、実効性について議論したい。

- ・ 東京オリンピックに係る具体的な取組み、動向について。今どうなっている？

以下、山口氏からのコメント

- ・対策実施チェックリスト（本日配布資料）ベースで考えると社員セキュリティ教育、社内エスカレーション対策など十分対応できている。
- ・また、外部提供サービスに係わるものは別。サービス品質に対するセキュリティ上の取り組みは、さらに高度になる。
- ・「サイバーセキュリティ基本法」に関する話として、国としては、お金（補助金、助成金など）を出して、最低限ルールを守らせたいと思っている。
- ・IoTに代表される課題で検討する重要性が増している。特にホームセキュリティについては、危険性が高い。
- ・「通信の秘密」は、憲法と通信保護法で守られているが、それが故に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場合がある。
- ・法曹界を含む研究会にて攻撃の防止以外の用途で利用しない場合に、「正当業務行為」として違法性が阻却されるとの意見があった。今後、議論を加速できないか考えたい→重大インシデントが起きない限りダメなのじゃないか（別コメント）

4. 2014年度 ITBO研究会の日程

	開催日		時 間	場 所
次回		12月9日（火）	16:30～18:30	BCAO 東京オフィス
	2015 年	1月13日（火）	16:30～18:30	BCAO 東京オフィス
		2月19日（火）	16:30～18:30	BCAO 東京オフィス

5. お願い

ITBO 研は日々の ML での情報交換とディスカッションを中心に活動します。月例会は、前日までの ML のやりとりの整理と発信者からの補足コメントが中心です。

交通整理は座長にて行うので、ITBO 研のみなさんはどしどし ML のディスカッションに参加してください。

次回、今年最後ですので忘年会を企画しています。是非多くの方々の参加を期待します。あらかじめスケジュールの確保をお願いします。さらに皆さまへの質問や新たな話題の提供、ご意見をお待ちしています。どうぞよろしくお願いいたします。

なお、すでにお配りした11月アジェンダの中の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うようお願いいたします。

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		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
	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

以上