第1回 ITBO 研究会議事録　追加 MEMO

★ 吉川さん加筆修正対応お願いします。

--------情報セキュリティ事故における BCP----------

ケース想定（事象例であり、こだわりはない）

・従業員端末が標的型攻撃で乗っ取られる

・従業員端末から社内重要サーバへアクセス、取引先情報を抜き取る

・従業員端末から、外部サーバに暗号化データ転送　HTTP　put、転送データ自体は端末から消去

→従業員本人も含め、気がついていない状態

・後日取引先より、データ漏洩に対する問合せ

・確認の結果、自社の取引先情報が、インタネット掲示板にさらされていることが判明

（これはたちがいいほう、実際にはデータが競合等に売られて、気がつかない状態）

→なんとなく入札に勝てないとか

さぁどうする？？

多分、やらなくては行けないこと例

1. 原因・影響範囲の特定

・被害拡大策の防止

・当該情報を格納しているサーバログの解析

・プロキシサーバ・FW のログ解析？

→攻撃された端末の特定ができるか？

・関連サーバのログ確認

→攻撃の範囲を特定できるか？

・証拠保全策の実施

2. 取引先への報告・メディア対応・当局への届け出

3. 再発防止策の決定

4. 再発防止策の実施

これらを実施する上で、予め準備していなくていけないこととは？

実際に行う上での、チェックシート的ななにか

そのためには各要素の要件を明確にする必要あり

★ 加藤さんからの追加情報及び情報ソース先情報

退職者の報復の部分のネタは次のところです。もしかすると、登録がいるかも。

http://www.keyman.or.jp/at/30006990/

＞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。

IPA の資料を漁りました。次の資料も追加してください。

情報漏えい発生時の対応ポイント集（第 3 版）
http://www.ipa.go.jp/security/awareness/johorouei/index.html

この資料には、吉川さんの書かれている「多分、やらなくては行けないこと例」が書かれております。加藤の言う「官庁提出」については、p.24 の 5. 通知・報告・公表等におけるポイント に書かれています。

この辺りの資料は、情報漏えい対策の観点での一般的な取り組みが書かれており、本年度の研究会の前提知識とするものと思います。
もちろん、情報漏えい事故でも、組織の事業継続に関わるダメージを受ける可能性はある訳ですが、BCAO でやるのだったら、最近のサイバー系の攻撃の過激化をにらんで、事業継続への重大影響があるよう場合をも含んだ対応の検討をするのかなと考えております。

＞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？
粗雑な方法については、次のニュースが元です。
http://www.justice.gov/usao/wvs/press_releases/May2014/attachments/0520143_Mitchell_Sentence.html

個人情報保護の取り組みについては、次のパーソナルデータに関する検討会がネタですが、ここまで研究会の範囲に入れると発散すると思いますので、この内容は参考程度で。
http://www.kantei.go.jp/jp/singi/it2/pd/

制御システムセキュリティも、入れるかどうか要検討です。

★ 大塚さんからの追加情報
くしくもベネッセの個人情報漏えい事案が発生したばかり
http://news.yahoo.co.jp/pickup/6122603

★ 岡さんからの追加コメント

サイバーリスクにたいしてのフォレンジックでのログ（履歴）ですが、今どきの手練れのハッカーなどは、ターゲットのサーバ、NW 機器のログはちゃんと始末していきます。では、形跡を残せるログは、なんなのかということになります。一部企業のように自社で常時監視でモニター上にリアルタイムにアラートが示せる仕組みを持っているところでさえ、抜けがあるくらいですから。また、ISMS（認証なのでなんだということもありますが）にも重なる部分でもあり、情報の機密種別と重要度を付け、システム構成（インフラ、運用含めて）を検討し、これから、インシデントのレベルによる対応策（対応フローなど）を検討し実施することが必要かと。また、情報漏えいのインシデントが発生し自社での追跡調査が難しいことも考慮し、専門企業への依頼とその企業への情報提供（ターゲットサーバ本体含む）も考慮し、代替環境（サーバ、ネットワーク機器）の準備も必要となるでしょう。

IPA の公開情報も役に立ちますが、現場がどのように動ける/動かせるかまでは、細かく記載されていないような過去の記憶あります。（最新の IPA も見てみます。）