

2015 年 1 月 30 日
CIO 賢人倶楽部事務局担当 高橋

第 22 回 CIO 賢人倶楽部 議事メモ

1. 日 時：2015 年 1 月 20 日 15 時~18 時 30 分
2. 場 所：大手町フィナンシャルシティノースタワー22 階会議室
3. 出席者：以下 15 名、順不同、敬称略
木内（オラン）、有吉（アドバイザー）、柏原（ホンダ）、沼（アドバイザー）、岩本（ノバルティス）、深作（ノバルティス）、磯村（東京ガス）、寺嶋（積水化学）、小河原（アスクル）、河崎（福岡 BK）、中村（福岡 BK）、田口（インプレス）、重松（東レシステム）、幸重（ANA）、荒牧（ANA）
他オブザーバー9 名 [KPMG8 名（事務局：西崎・立川・高橋・板垣・山本）、土田、三浦、伊藤]、オラン 1 名（速水）
4. 議事メモ：下記の通り

【議事内容】

木内：昨年 9 月より事務局を KPMG にお願いしてから順調に進んでおり、今後もより良い形で進めていきたいので協力をお願いします。本日のテーマはメディアでも話題となっており少々難しいテーマではあるが、サイバーセキュリティー。活発な議論をお願いします。

【1】 プレゼンテーション：リスクシナリオに基づく SIEM 導入事例（山下・小野）

沼：大凡いくらくらいかかるのか？

山下：最近フリーソフトの活用もある。また、リアルタイム性をどこまで追求するかにより変わってくるが、数千万円規模。金融機関であれば 1 億円を投じる例もあるが、範囲によって変わる。導入にあたっては少しずつスパイラルアップしていく形が望ましい。製品を選択する場合には拡張性も大事になる。

沼：オペレーションコストは？

山下：セキュリティーオペレーションセンターや CSIRT に人をどれだけ配置するかによって変わる。

沼：KPMG としてのサービスはあるか？

山下：CSIRT の立上に関わる支援は行うが、オペレーションセンターについては 24 時間 365 日運用の形になるので支援はしていない。

沼：ノウハウの継承が難しい。新しい分野なのでこの分野のサービス拡充はよいのではないか。

山下：監視については外部へ任せる事が多いが、SOC がやってくれるのは怪しい事象のアラートであり、それを判断するのは会社の役目となる。CSIRT チームについては社内に作られた方が良い。

田口：欧米の普及率はどのくらいか？

山下：かなり導入している。欧米では自社の中に SOC や CSIRT を置いている会社が多い。

田口：従業員数規模は 1 万人規模のようなところが多いのか？

山下：多いが、サービスの体系によるところが多い。

重松：リスクマネジメントのサービスを提供されているので、KPMG 内にリスクシナリオ等を作られるサービスはないか？

山下：リスクシナリオを使ってセキュリティー対策を強化する支援を行うことはよくある。

重松：おそらく気付かない弱点は多く、かなり前の段階で事象を捉えないといけない。リスクアセスメントの重要性がかなりの比重をしめるのではないか。また、ベンダーの売込みはあるが実際の機能強化は難しい。どういうリスクシナリオがあるか分かっていないといけないし、ルールが分からないので、よっぽどのアドバイスがないと難しい。また、プロダクトによっては使いやすいインターフェイスはあるものの、使いこなす事が難しい。

山下：インターフェイスは分かり易くなっているが、結局は社内のルールが大事。機能についても集約されてきている。IBM、ユニシス等が出している製品も使いやすい。国内の事例も多くなっている。

柏原：8ページのシステム毎の重要度評価のうち、標的と成り得る資産の分析の対象となる部分についてはわかるが、対象外のところを踏み台にされて攻撃される脅威がある。

小野：狙われやすい部分については気をつける必要がある。

柏原：対象外部分を蔑ろにするにはいかなものか？

小野：対象外部分についてもリスクの高いものについてはケア必要。

柏原：誰がどこを狙うかが判らないので、対象外のログを取るべきなのでは？

小野：各サーバのデータは膨大なため、効果を考えた上で優先順位付が必要。

柏原：記述は無いが、対象外部分についても踏み台にされるかされないかの判断も必要ということで理解した。

深作：大量アラートの対処について、導入にあたりどのように進めていくのか？

山下：初期導入の一部として、どういう体制が必要かを考えていく必要がある。当初設定後にログをため込んでいくと、引っかかる案件が出てくるが、問題の無い場合もあるため、その際はホワイトリストとして異常値を正常値化していく処理も必要。導入直後はアラートの分類作業も必要。

深作：同じく、社内の体制をどのように作る必要があるのか？

山下：導入時に必要な体制は、監視体制の構築、発見後のリカバリーをやる体制の構築が必要。

磯村：関連会社を含めたグループ全体の事例はあるか？

山下：規模が大きくなれば CSIRT に人員を配置するのはコストがかかるので、限られた会社になる。例えば大きな金融機関グループであれば持株でこのような機能を持つところも

ある。配下各社をまとめてサポートする体制を作っている。個別のシステム導入については各グループ会社各自で行っているが、インシデントが発生した際の対応については持株会社で行っている。

寺嶋：同じインフラで標準化しないと、監視機能が変わった場合等、関係会社間の調整をしないと運用が難しいのではないかな？

山下：プロセスと技術のところは各社、一番上の組織のところはグループ全体で集約できるのであればした方がよい。

寺嶋：プロセスとルール策定に加え、カスタマイズが必要なのでは？

山下：各社の環境によりカスタマイズが必要。

岩本：技術対応はいいレベルに来ているので、数千万円の予算があれば予防に回す方がよいのでは？

山下：各社の状況による。穴だらけの仕組みではハンドリングできない。

岩本：予防のレベルは **KPMG** としてはどのような形にすべきと考えるか？

山下：予防的部分の対策は情報量としては多くのものがある。ただし経営者がどのように捉え、投資の意思決定をするかが大事であり過去にはそこが問題になっていたこともある。最近事例も多く、投資マインドも醸成されてきている。

岩本：導入はタイムラインで大体1年から1年半かかるが、その間にネットワーク環境も変わる。**BPO** をやり続けなければならないのでは？

山下：ルールのメンテナンス、システムの構成に合わせて変更することは、導入した後も継続する必要があるので、その度合いが激しければ導入が続くようなケースとなる。

木内：セキュリティーインフォメーションマネジメントとセキュリティーリスクマネジメントをしっかりチューニングする必要がある。製品によって相関分析ができるのか？

山下：ロジックは大体がかなり簡易な言語でカスタマイズできるので、チューニング・検索の精緻化が可能。

寺嶋：相関分析は難しい。

深作：相関分析の範囲は相当広い。

河崎：導入は金融機関が多いのでは？

山下：金融機関は多い。カード決済、不正送金等の例の検出等で取り組みが進んでいる。

中村：守りの部分、不正取引対応はやっている。攻めの部分、イベント・マーケティング分野において発見のログ分析はできていない。いろいろな仕掛けがあるが分析はスキルも人もいないのが現状。何かあった時のために必要。

立川：疑わしい取引の監視をする部門は？

沼　：ビッグデータの分析ということだが中々難しい。

河崎：特に外資は予防に重点がおかれているが、発見が難しいのなら持ちだされても意味のない情報についてはクラウドを使おうと思っている。クラウド業者もしっかり暗号化している。守りたいデータだけ徹底的にしっかりとやる方向。

小河原：当社は個人情報だけ。暗号化、データ分散化については自前主義を辞めた。共通ロジックは一緒に考え、暗号化とデータ分散化を行った。EC 企業はこのような形が多い。物流含めて個人情報が多い。また MA を行った際のセキュリティーレイヤーがばらばらでどう統合するのも課題。その間にアタックされたら終わり。水平統合の場合は仕組みが使えない。時間とお金の戦いになるので、ビジネスデューデューリもまともにできないのにセキュリティーデューデューリはまず難しい。

【2】プレゼンテーション：最新セキュリティー事情「T-SIRT」の視点から（北村）

河崎：毎日 150~200 件の問合せと伺ったが、普段どのような対応をされている？

北村：作業所 1000 か所、利用者 13,000 人、PC15,000 台で PC のセッティング、プリンター接続対応も行っている。マニュアルに挙げても見ない。まずはこれを裁く。放棄率が 5% 程度で回している。

荒牧：防災演習にはどのくらいの頻度で何人参加？

北村：年に数回、海外も含めて実施している。

木内：協力会社のサーバ等はどのように管理している？

北村：三菱商事さん系の業者をお願いしている。将来的には情報そのものにリスク度合いを設定したい。

重松：情報が重要な産業なので、経営者との距離、情報共有が大事。どういう工夫をされているか？

北村：経営との距離を縮めるやり方は、適当なサイズの事故が必要、これが一番よい。一番真剣に話ができる。いきなり致命的な問題では困る。

沼　：6名は専任？医療業界は品質が一番重要。マニュアル同様に品質担保の仕組み作ると良い。

木内：セキュリティーポリシーが重要となる。

北村：セキュリティー、向上の安全性は会社の中で一番理解が得やすいと思っている。

重松：セキュリティーは工場の安全性と同じ。

沼　：品質の作り込みはガバナンスではない。

礒村：安全は全てに優先する。セキュリティーは最優先事項。

北村：セキュリティーは、事故を起こさなければそれで良いとなりがちであるが、これが問題。TV等で毎日のようにメディアによる吊るし上げが起きている。

小河原：新しい取引先と契約を結ぶ際、セキュリティーチェックをするが甘いとビジネススピード遅くなる。足元は基準を守る必要があるが、物流会社経由でPCを盗まれた事もある。それを機にパートナーに対するセキュリティー体制を強化した。

沼　：どこまでやるかも重要。

北村：PC セキュリティー診断サイトをトレンドマイクロに作ってもらった。これにより末端にまで重要性を分らせる事が必要。情報管理体制台帳を運用している。ただ、現在はスマホを持っている人がほとんどとなってきたので、書き込みや写真投稿は問題となりやすい。

小河原：大手のパートナーについては一緒に教育をすることもある。いい技術もっている中小企業を取り込む際、その場合は委託社員として常駐させ、PC 貸与、研修も社員と同一の形でやっている。

北村：秘密守るべき範囲を分類し、その範囲について顧客と合意をした上で、我々の責任の及ぶ範囲をできるだけ小さくしておく事も重要。

【3】「メディアから見たトレンド」についてプレゼンテーション（田口、資料無し）

田口：Google Trend によれば「サイバーセキュリティー」に関する情報は 2006 年をピークに減少している。日本では「情報漏えい」、米国では「Data Breach」という言葉が直近トレンドでは多くなっている。日本では「ウィルス」より「情報漏えい」の Key Word が多く、TBC が問題になった事がある。

2006 年の日本の「情報漏えい事件」は日産が 538 万人、富士ゼロックスが 400 万件。2005 年、Yahoo BB が 450 万人の顧客情報流出した際、一人 500 円の金券を支払ったケースがあり、今回ベネッセもこれをベースに支払った。金券には電子マネー、図書券、また、今回は自社運営財団への寄付とするケースがあったが、これがなければダメージはそれ程大きくはならなかったと言われている。

直近では件数自体減ってはいるが、2013 年のヤフーの不正アクセス 2200 万件、2014 年のベネッセは 3000 万件の顧客データが話題となったが実害は大きくなっている。

一方米国では、事情が違っている。以下 TOP5 の事件を挙げる。

- ・5 位は 450 万件の患者データ漏えいを起こした 206 病院を運営する大手医療チェーンの CHS 社。社会保障番号も盗まれた。米国では病院が狙われやすい。
- ・4 位は大手ホームセンターの Home Depot。5600 万件の顧客カード情報と 5300 万件のメールアドレスが漏えい。対策費は 6200 万ドルにも上り、現在 EMV 技術を全店に適用中。他の小売りチェーンにもばら撒かれている説がある。

- ・番外編は大手小売チェーンの **TARGET**。POS からクレジットカード、デビットカード情報を盗み、1 億 1000 万人に影響が及んだ。出入の空調事業者のコードを利用し、2013 年のクリスマスシーズンにウィルスが一斉に起動。CEO、CFO、CIO の首が飛んだ。ウクライナのオデッサ拠点の可能性あり。同地は 2000 年頃からハッキングの基地となっている。
- ・3 位は **JP Morgan Chase**。7600 万世帯、700 万社の中小企業の顧客情報が漏えい。幸いな事に口座番号、PW、社会保障番号等が漏えいした証拠は無い。米国最大級の金融機関の事件としてインパクトが大きかった。**Bloomberg** により、ロシアのハッカーが **Chase** 等の米金融機関を攻撃したという声明を出したという報道で発覚。
- ・2 位は **eBay**。社員のアカウントで中枢の DB に侵入され、ユーザ ID・PW、メールアドレス、住所、電話番号、生年月日等の個人情報が流出。1 億 4500 万人のユーザに注意喚起がなされた。10%の減収見込み。
- ・1 位はご存じのように **Sony Pictures Entertainment**。100TB の多様な情報が流出。映画コンテンツ、社員のメール情報、タレントの報酬等各種情報が流出。**GOP** によるハッキングで全社員の PC に犯行声明。アンジェリーナ・ジョリーがバカ女優、大根役者だと誹謗した社員のメール情報が流出。現在進行形で被害が起きている。

オバマ大統領が今年の所信表明演説でサイバーセキュリティ対策を表明。政府として本腰を入れて対応する事を表明。ハッキングを受けた企業を守るための法律を検討している。被害を受けた企業の損失額が昔と違う。企業を守らないと経済が立ち行かなくなる可能性があるレベルになってきている。

100 テラバイトの情報漏えいで、米国のメディアは散々な事を書いている。**SONY** はかわいそうだが、それだけ致命的な打撃となった。

沼　：メールは読まれるものとして対応の必要あり。

田口：これだけの形で報道されると、かなり深刻でリカバーすることは難しくなる。事件に巻き込まれないようにしましょう。

【4】今後の運営について（立川）

- ・3 月 19 日の第 24 回賢人倶楽部公開セミナーアジェンダの確認
- ・セミナー集客は各会員が 2~3 名ずつ CIO ならびにそれに準ずる方を勧誘する。
- ・4 月 21 日に羽田クロノゲートの見学日程が確定。ここで新年度運営に関するディスカッション、懇親会を実施予定。

- ・新メンバーの勧誘も検討。

荒牧：人数的にはどのくらいまで増やすのか？倍増した場合に、見のある議論ができるかは検討が必要。

立川：一度には増やせないなので、1年がかりで声をかけて徐々に増やしていく形。

沼：声かけて良いか？

立川：一旦ご紹介頂き、メンバーで検討した上で決める形。

【5】新サイトお披露目（木内）

沼：英文サイトを検討してはどうか？海外からの注目も高まる。

木内：海外の業者を使うことも検討できる。

沼：メンバーが、参考になる書籍を紹介することも面白い。

了