大規模情報漏えいにおける セキュリティマネジメントからの考察

2016年03月11日
情報処理学会・全国大会

内田　勝也

情報セキュリティ大学院大学
uchidak@gol.com

はじめに

セキュリティマネジメント／心理学からの考察

- 標的型攻撃を始めとするソーシャルエンジニアリング攻撃は、技術的対策だけで対応できず、セキュリティ教育・訓練の重要性が高まってきた
  しかし、従来のセキュリティ教育・訓練に疑問を呈する(海外の)専門家・実務家もでてきた
- 「内部犯行の90%は，技術でなく，人を考える必要がある」とFBI(前CISO)は言っている
- 国内では、まだ、セキュリティ対策は技術中心で、人材育成も技術者育成が中心であると感じる
  その理由として，
  - セキュリティ技術を教える教員は多いが，セキュリティマネジメント／リスクマネジメントを教える教員（実務経験者）が少ない
  - 教育・訓練が重要視されていない感じを受ける．　教育・研修で、参加者全員に高い効果を与えられないが、ウイルス対策等を始めとする技術的対策も完璧でない
- 最近の大量情報漏えいから感じるのは、
  - インシデント対応は、プロジェクトマネジメントやリスクマネジメントが欠落している
  - PDCA(計画，実行，評価，改善)が大切といわれているが、運用ができていないことが多い
    実行されているか確認／評価が行われていない。 また、評価者(内部監査)の権限が低い／ない
  - 責任が明確でないため、規程／ルールがないと先送りになる傾向がある
  - 過去のインシデント情報収集や訓練が行われないのは、「正常化バイアス」が働いているのでは？
  - セキュリティ専門家(有識者)は「セキュリティマネジメントの指摘は後知恵バイアス（Hindsight bias）／後出しジャンケン」と言う

大規模情報漏えいにおける セキュリティマネジメントからの考察

セキュリティマネジメントからの考察

公開された資料から読み解く（ベネッセ事件報告書）

- この報告書を読んで筆者は，ベネッセはセキュリティ対策を結構きちんとやっていたと感じた
- 端末のデバイス規制や入退室管理を行い，ログの取得や社員教育などもやっていた
- ベネッセよりセキュリティ対策が甘い企業のほうが多い

[第4回]ベネッセを襲った個人情報漏洩事件
http://itpro.nikkeibp.co.jp/atcl/column/15/082000196/082000004/

監査／事故調査で何を確認するのか？

- 制度と運用の乖離を確認
- 監視カメラは常時監視か？　録画は？
- ログ対象は？ チェックは？　保存期間は？
- セキュリティ研修の内容の確認／評価方法は？ 行動変容の確認は？　子会社も
- セキュリティ監査項目と過去の指摘事項及びその改善は行われているか？
- システムPWの利用者数は？
- PWは利用者別だったのか？
- システムPWのログチェック間隔は？

物理的セキュリティ
- 入館許可証による入退室管理
- 監視カメラ
- クライアントPCへのワイヤーロック

人的・組織的対策
- セキュリティ研修
- セキュリティ監査

技術的セキュリティ
- システムへのパスワード設定
- ログの取得とアラート設定
- ソフトのインストール制限
- URLフィルタリング
- 外部デバイスへの書き出し制御
- データベースへのアクセス制御

社長等の記者会見（2014.07.17）で、「アクセス権限」及び「アクセスログ」の質問については捜査理由で回答なし【9:37より】
https://www.youtube.com/watch?v=RaQfv5_MQ0

第2回公判：弁護側は冒頭陳述 【産経ニュース 2014.11.13】
- 顧客情報のデータベースにアクセスするIDとパスワードは共有で、多くの従業員が利用できたと指摘

大規模情報漏えいにおける セキュリティマネジメントからの考察

セキュリティマネジメントからの考察

公開された資料から読み解く（ベネッセ事件報告書）

- 子会社はISMS認証取得をしていたが，何ら記述がない
- ISMS関連では，リスク評価，適用宣言書等作成文書の確認，重要項目（職務の分割，開発施設／試験施設及び運用施設の分離等）の確認，内部監査結果，審査機関の審査内容の確認を行う
- これらを総合的に判断して，セキュリティ対策が適切かの判断が必要だが，ISMS関連の調査報告がない．報告書は重大な課題を評価していない

同種の事件・事故が発生し、大きく取り上げられたが対応していない。「正常化バイアス」では？

- 三菱UFJ証券・情報漏えい事件：2009年4月発覚．「調査報告書（抜粋）」は、職務の分離、施設環境の分離などに問題があったと述べている
  http://www.sc.mufg.jp/company/news/apology/index.html
- ファーストサーバ事故：2012年6月に発生．ISMSは、ベネッセと同一の審査機関が担当
- 職務の分離や施設環境（開発、テスト、本番）の分離の問題（未実施）は、ベネッセと同じ

- ウィーケストリンク（Weakest link）：鎖の強さはその環の一番弱い所で決まる
- ベネッセの個人情報は最も重要な情報資産のはず

この様な状況でも、ベネッセの「セキュリティ対策は適切」だっただろうか？

大規模情報漏えいにおける
セキュリティマネジメントからの考察

ISMS 管理目的及び管理策

JIS Q 27001:2006 管理目的及び管理策（133項目）環境に応じ取捨選択・追加 可能

1．情報セキュリティ基本方針
（1）情報セキュリティ基本方針
2．情報セキュリティのための組織
（1）内部組織
（2）外部組織
3．資産の管理
（1）資産に対する責任
（2）情報の分類
4．人的資源のセキュリティ
（1）雇用前
（2）雇用期間中
（3）雇用の終了又は変更
5．物理的及び環境的セキュリティ
（1）セキュリティを保つべき領域
（2）装置のセキュリティ
6．通信及び運用管理
（1）運用手順及び責任
（2）第三者が提供するサービスの管理
（3）システムの計画作成及び受入れ
（4）悪意のあるコード及びモバイルコードからの保護
（5）バックアップ
（6）ネットワークセキュリティ管理
（7）媒体の取扱い
（8）情報の交換
（9）電子商取引サービス
（10）監視

- 職務の分離
- 開発・試験・運用施設の分離

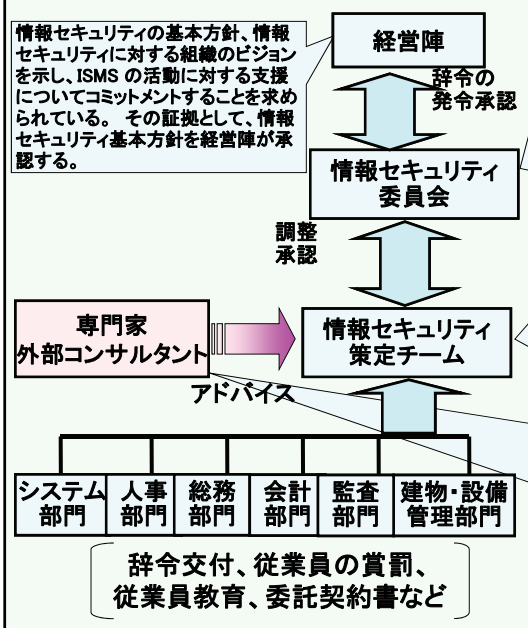
7．アクセス制御
（1）アクセス制御に対する業務上の要求事項
（2）利用者のアクセス管理
（3）利用者の責任
（4）ネットワークのアクセス制御
（5）オペレーティングシステムのアクセス制御
（6）業務用ソフトウェアのアクセス制御
（7）モバイルコンピューティング及びテレワーキング
8．情報システムの取得，開発及び保守
（1）情報システムのセキュリティ要求事項
（2）業務用システムでの正確な処理
（3）暗号による管理策
（4）システムファイルのセキュリティ
（5）開発及びサポートプロセスにおけるセキュリティ
（6）技術的ぜい弱性管理
9．情報セキュリティインシデントの管理
（1）情報セキュリティの事象及び弱点の報告
（2）情報セキュリティインシデントの管理及びその改善
10．事業継続管理
（1）事業継続管理における情報セキュリティの側面
11．順守
（1）法的要求事項の順守
（2）セキュリティ方針及び標準の順守，並びに技術的順守
（3）情報システムの監査に対する考慮事項

Katsuya Uchida uchidak@gol.com

大規模情報漏えいにおける
セキュリティマネジメントからの考察

ISMS構築のための組織体制

ISMS 構築のための組織体制例



情報セキュリティ委員会を中心とした体制で策定されるISMS 関連文書は、委員会だけでなく組織の経営陣により承認された規程として必要に応じて関係者に周知し、定期的に見直しを行う。
この委員会は、組織の保有する情報資産の取り扱いに責任を持ち、情報セキュリティの方向性を提言できるだけの情報セキュリティに関する理解と実行力をもった組織であるべきです。
情報セキュリティ委員会は、組織においてISMS の中心的役割を負う。以下は情報セキュリティ委員会の役割の例示です。

- リスクマネジメントのための環境整備について検討機関となる
- ISMS 関連文書の策定時には内容について実質的な決定機関となる
- 導入段階のISMS を推進する各種施策や改訂を検討する
- 運用段階でセキュリティ問題等が発生した場合の検討機関となる
- ISMS 運営の評価結果に基づいた改善について検討機関となる

ISMSの構築実務を担当する。適用範囲内の重要な情報資産を広く現状把握し、その取り扱いを検討するのに十分な知見を持つメンバーで構成されるべきです。例えば、情報資産の取り扱い方法の決定に当り、適用範囲内の部署間での見解の相違や、利害関係の調整が必要になる場合があり、そのような摩擦の調整役として、部門間の枠をこえて当事者に対してうまく働きかけが求められる。この場合は、高いセキュリティ知識も当然必要ですが、調整能力や経験に基づくコミュニケーションのスキルも重要になる。

ISMSの構築作業は、組織が自前で（できれば専任の）要員を確保した上で進めるべきです。しかし、「情報セキュリティ」の対象とする範囲は「IT 技術」、「経営的な判断」や「ビジネスへの理解」など、求められる知識や経験は多岐にわたり、これらの領域をバランスよく俯瞰的に見通す力量が求められる。
組織の主要な業務はその業務に携わっている人が一番知っているが、時としてミクロな視点での判断に終始してしまう。「外部の専門家・コンサルタントの登用」は、この判断にマクロな視点を与え、また最新の情報を提供してくれる窓口機能が期待される。情報セキュリティ委員会へのオブザーバ参加、規定文書のレビューや監査計画策定など、必要な局面で彼らの持つ専門知識を効果的に活用することも良いと思う。しかし、外部の専門家やコンサルタントはISMS構築支援を行うもので、当事者ではないので、意思決定を含めた丸投げは避けなければならない。

Katsuya Uchida uchidak@gol.com

Katsuya Uchida（uchidak@gol.com）

大規模情報漏えいにおける
セキュリティマネジメントからの考察

厚労省 セキュリティ対応組織

1. セキュリティ対応組織（厚労省）

(1) CIO補佐官：非常勤 5名（週3日勤務）がおり，1名は「セキュリティ担当」

- 非常勤補佐官は，緊急時「蚊帳の外」になることが多いが，それで問題ないのか？
  非勤務時での対応をセキュリティ担当の場合の対応を考える必要があるのではないか？
- 政府CIO補佐官（各府省担当）は，各省庁での勤務時間も短い？
- CIO補佐官（セキュリティ担当）の役割はどうなっているのだろうか（施策推進とあるが）？
  今回の事案では，厚労省で 4月22日に同様事案が発生しており，5月8日まで約2週間（連休があるが）の間に，CIO補佐官を含めた対応があったのか？
- セキュリティ教育・訓練施策の推進もCIO補佐官の役割になるが，
  - 標的型攻撃をはじめとしたサイバーセキュリティや
  - セキュリティ関連の情報収集などが行われていたのか？

政府CIO等へ専門的・技術的見地から支援等を行う（政府CIO補佐官 募集要項より） 政府CIO補佐官（各府省担当）
① 府省における電子行政に関する戦略の支援・評価
② 業務・システム最適化の企画・実施・評価
③ 電子行政に係る予算に関する評価等
④ 府省の情報システムの調達に関する支援・評価
⑤ 府省の情報システムの開発・運用・保守に関する支援・評価
⑥ 府省の情報セキュリティの向上に関する施策の推進
⑦ 府省における情報通信技術人材の育成
※ 政府CIO補佐官（各府省担当）は、情報セキュリティに関する素養を確認の上、各府省で最高情報セキュリティアドバイザーを兼務する場合がある
http://www.cas.go.jp/jp/saiyou/pdf/20150114-hijoukin.pdf

大規模情報漏えいにおける
セキュリティマネジメントからの考察

厚労省 セキュリティ対応組織

1. セキュリティ対応組織（厚労省）

(2) CSIRT：Computer Security Incident Response Team

CSIRTは何ら役割を果たしていない

- NISCは，各省庁に2012年 CSIRTの設置を求めた
- 2013年4月にCISO(官房長)が，以下のように述べている
  障害・事故等が発生した際に、これまでも迅速かつ適切に対処するための体制確保等に努めてきたが、政府機関全体の方針を踏まえ、必要な機能等を備えた厚生労働省CSIRTを設置し、緊急対応態勢の強化を図った
  NISC，政府機関における情報セキュリティに係る年次報告（平成24 年度）
  http://www.soumu.go.jp/main_content/000235220.pdf
- CSIRTが適切な運用されてきたかの検証を果たす組織は？
- 2015年9月11日サイバーセキュリティ戦略本部長（官房長官）が「サイバーセキュリティ基本法第27条第3項に基づく勧告」（下枠内）を行った

⇒ 9月18日「情報セキュリティ強化等に向けた組織・業務改革 ―日本年金機構への不正アクセスによる情報流出事案を踏まえて―」を厚労省は公開した

勧告：サイバーセキュリティ基本法第25条第1項第3号の規定に基づく「日本年金機構における個人情報流出事案に関する原因究明調査結果」、「検証報告書」等を踏まえ、同法第27条第3項の規定に基づき、下記の所要の措置を講じるよう勧告する

1. 体制整備 ①厚労省の体制 ②機構の体制 ③機構のCSIRT ④厚労省と機構の連絡・連携体制
2. 技術的対策 ①厚労省と機構の情報システム等 ②機構の情報セキュリティ対策 ③機構の運用管理対策 ④機構の外部情報セキュリティ監査
3. 教育・訓練 ①厚労省の教育研修・訓練 ②機構の教育研修 ③機構の訓練 ④職員の認識と所管法人等監督
4. 成果の評価と報告 ①機構の成果評価と報告 ② 厚労省の報告： 厚労省は、上記の評価終了後速やかに、評価結果を含む本勧告の履行状況について、サイバーセキュリティ戦略本部長に報告すること

大規模情報漏えいにおける
セキュリティマネジメントからの考察

厚労省 セキュリティ対応組織

● サイバーセキュリティ基本法第27 条第3項に基づく勧告 2015年9月11日

⇒ 情報セキュリティ強化等に向けた組織・業務改革 ―日本年金機構への不正アクセスによる情報流出事案を踏まえて―

http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150918-02.pdf

第1 日本年金機構における情報流出事案に関する総括
＜はじめに＞
＜今回の事案についての主な反省点＞
1. 情報セキュリティの重要性に関する意識の欠如
2. 組織的な危機管理対応の欠如
3. 組織横断的、有機的な連携の欠如
＜再発防止に向けた基本的考え方＞
第2 今回の事案を踏まえた再発防止策
1. 厚生労働省における情報セキュリティ対策の強化
(1) 組織的対策（体制強化、情報共有）
① 情報セキュリティ対策室（仮称）の設置
② CISO、CSIRT 体制の見直しについて
(2) 人的対策（意識改革、人材育成）
① 職員の意識改革
② マネジメント面の意識改革
③ 実践的な訓練の実施
④ 専門人材の確保
⑤ 教訓や知識の蓄積と継続性の確保
(3) 業務運営対策（ルールの見直し、徹底）
① 報告及び連絡体制の確立、責任の明確化
② 保有する情報を適切にリスク評価した上での情報管理の徹底
(4) 技術的対策（情報システムの強化）
① 高度な標的型攻撃を想定した入口、内部、出口のセキュリティの強化
② 情報セキュリティの運用設計の見直しと改善
③ 調達時の契約内容の見直し
2. 厚生労働省と機構の関係の強化
(1) 厚生労働省の機構に対する指導監督の強化
① システムに対する監督部署の明確化
② モニタリング機能の強化
③ 業務運営上定める内規等の共有のルール化
④ 報告、連絡の徹底
⑤ 情報共有の徹底
⑥ 年金局と機構の連携の強化
(2) 年金局の体制強化
3. 厚生労働省所管法人等に対する監督と情報セキュリティ対策の強化
(1) 教育訓練の実施
(2) 報告、連絡体制の確保
(3) リスク評価を踏まえた情報管理の徹底と監査（助言）の実施

2015年9月18日 作成

大規模情報漏えいにおける
セキュリティマネジメントからの考察

厚労省 セキュリティ対応組織

1. セキュリティ対応組織（厚労省）

(3) 情参室（正式には，「情報政策担当参事官室」）等

- 情参室は，室長補佐以下4名で、一般的な人事ローテーションの中での任用で、高度な専門性に基づく対応が要請される情報セキュリティインシデントに対処できる知識や経験を持つ専門家とは言えない。 更に，職員1名が兼務で，省全体のサイバーセキュリティ対策を中心的に担う状況であった．
  結局，情参室を始め，厚労省全体が今回事案の重大性認識が欠如していた
- また，セキュリティ担当の非常勤CIO補佐官との連携も取れていない
- 情報連絡遅延：過去3年間で、ホームページ改ざん等のサイバー攻撃が複数回発生し，事案は厚労省内部・外局，独法から情参室に報告される．しかし、多くの報告は事案収束後で，情参室やCIO補佐官が適時・適切な役割を果たせる連絡体制でなかった． 本事案でも、責任者らへの報告は、最初の攻撃発生後2週間以上が経過してからであった

大規模情報漏えいにおける
セキュリティマネジメントからの考察

年金機構 セキュリティ対応組織

2. セキュリティ対応組織（年金機構）

(1) 情セ担当部（情報セキュリティ担当部署）

- 緊急時対応が文書化（ルール化）されていても，ルール通りにいかないのが緊急時対応では？
- 対応すべき事柄が文書化（ルール化）されていないと，それ以上のことを考えない
  - 5月8日，2通の不審メールが届いたが、メール受信確認ルールがないため，メール受信者の個別確認をしなかった
  - インターネット遮断ルール（判断者、判断基準）がないため、統合ネットワークを通じたインターネット接続の一部又は全部やメール送受信回線の遮断を実施しなかった.
- 緊急時対応の未熟さ
  - NISCの不審通信指摘は，機構内セキュリティ機能が役立たなかったとの認識があったのか？
  - 5月8日のメールは，業務用メールアドレス（公開メールアドレス）宛で，この段階で他職員に確認していれば、業務用メールアドレスが狙われている旨の注意喚起がで きた
  - 5月15日 運用委託会社から「新種ウィルスは情報漏洩タイプでない」との解析結果報告は，5月8日のNISCの不審通信検知との矛盾を感じていない

- 情報セキュリティ以前に，組織での基本的業務遂行ができていない
- 緊急時に対応ルールがなければ，組織内／上級管理者の判断を仰ぎ，決定しないと問題を大きくするだけ

Katsuya Uchida uchidak@gol.com

大規模情報漏えいにおける
セキュリティマネジメントからの考察

年金機構 セキュリティ対応組織

2. セキュリティ対応組織（年金機構）

(2) インシデント対応体制

- サイバー攻撃等のインシデント発生時対応は、機構にCSIRT制度が設けられていない
- 緊急事態を想定した厚労省との連絡体制も定められていないため組織的対応ができなかった
- 具体的対処が明示されたマニュアルも存在していなかった
- インシデントの発生に直面し、厚労省への報告.連絡.相談は、場当たり的であった
- リスクに備えた人員配置がなかった。情報セキュリティアドバイザーは、情報セキュリティスペシャリスト等の有資格者が1名いたが、役員・管理職等の判断権者に進言できる職位でなく，当時は，職務から事実上外れており、事案発生後，業務に戻る指示等はなかった． また，サィバー攻撃等のインシデント対応経験者もいなかった．しかし，情報セキュリティ専門人材を外部から補うこともなかった

- CSIRT制度があった厚労省も機能しなかった． 制度構築でなく，制度運用の重要性への無理解
- 連絡体制やマニュアル不在は緊急時にしばしば発生する． それを想定した教育・訓練が必要
- 年金機構で保有している情報のリスクを考慮した体制構築ができていない

◆ 厚労省だけではないが、官庁等は、「起きた問題」にしか対応しない
起こりうるリスクに対しては、動かない

Katsuya Uchida uchidak@gol.com

Katsuya Uchida（uchidak@gol.com ）

大規模情報漏えいにおける
セキュリティマネジメントからの考察

標的型メール訓練について

標的型添付メール訓練について

（1）国内での訓練結果　　クリック割合

1. 事前の情報提供せず訓練を実施. . . . . 約４０　%
2. 事前に情報提供を行って訓練を実施. . . . . 約１０　%
3. 訓練実施２年後、事前の情報提供をせず実施. 約１２．５%
4. 訓練実施２年後、事前に情報提供し実施. . . 約　６．３%

1. ３自治体（横浜、豊島区、藤沢）の結果
2. 中央官庁（NISC）
3. １自治体での結果（豊島区）
4. １自治体での結果（豊島区）

（2）米国：Lance Spitzner（SANS.org　RSA Conf. 2014）

- 訓練間隔を短くすればするほど、効果はある・・・
  - 四半期　19%
  - 2ヶ月毎　12%
  - 毎月　4%
- 毎回、内容を難しくして行く必要がある

- 訓練を行っても、クリックを完全になくせないが、訓練をやる意味はある
- 技術的な対応（例：DMARC等）を否定しない

- 標的型メール攻撃だけが，情報漏えいの問題ではない
- 標的型電話攻撃（逗子市ストーカー事件）もある
- マルウェアがリモート攻撃だけではない
- 対話型の標的型メール攻撃もある

人的セキュリティの誤解？

- 標的型訓練で、完璧な防御ができないので、やる意味がない！
- 100%対応と 10%以下対応は同じでない。人的対策で、100%対応は不可能
- クリックした／しないでなく、おかしいと思ったら、職員間での注意喚起や対応部門への連絡するリテラシーの醸成
- 技術的対策（F/W，IDS，ウイルス対策ソフト等）で 100%完璧な防御は可能？

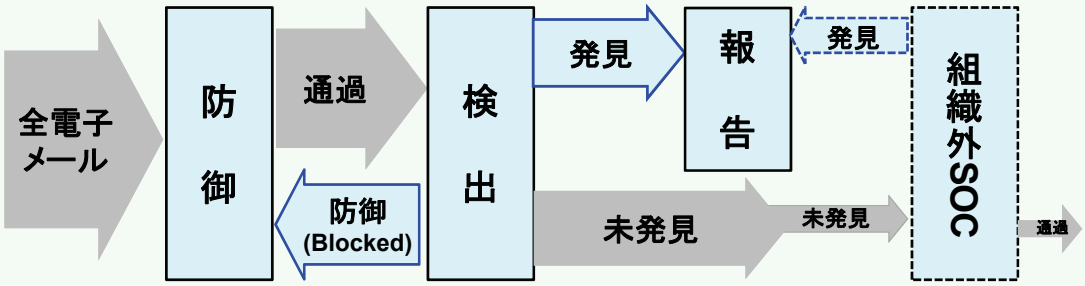
- これからも，サイバー攻撃は遙かに多彩な形で人間を攻撃対象にする

大規模情報漏えいにおける
セキュリティマネジメントからの考察

標的型メール対応

標的型メール 対応評価図

- 標的型メール攻撃では、標的型メールだけが送付される訳ではなく、その組織に関係する全てのメールが送付されることを念頭に対応する必要がある



防御 ： 標的型メールを通さない仕組み（① 添付ファイル形式のメールは認めない　② DMARC）

検出 ： 利用者への教育・訓練（組織対応の重要性も）

報告 ： 報告体制を確立することが大切（緊急時体制の確立、訓練も）

組織外SOC ： どれだけの権限を持ち、どの様な報告を行うか等を考える必要がある

送信元詐称迷惑メールへの対策に有効な送信ドメイン認証技術のひとつで、既に標準化されている

標的型メール攻撃について

今回の標的型メールは、リモートアクセス機能を利用して、大量の情報盗取を行ったものだが、大量情報の削除・改ざん、システム業務を不能 にするものを考えることも必要では？

大規模情報漏えいにおける
セキュリティマネジメントからの考察

個人情報保護の認識不足

- 個人情報について
  - 原則として基幹系システムに保管
  - 一定条件下で機構LANに接続する共有フォルダに保管
  - 機構LANシステムの共有フォルダへの保管ルール（経営企画部総務室作成 最終更新日平成27年3月23日「日本年金機構共有フォルダ運用要領」）
    - 共有フォルダのアクセス権を関係者のみに制限、又は ファイルにパスワードを設定
    - 保管不要ファイルは、速やかに削除する
- システム／セキュリティ監査等の機能不全
  - 情報セキュリティや個人情報保護に関する自己点検が毎月実施
    - 自己点検の内容は、主に事務ミスや内部不正を想定したもの
    - 課題があれば、回答者本人が改善施策を記入し、回答結果の組織対応はなかった
  - 情報セキュリティ監査は、平成24年度まで年金局事業企画課監査室が実施、平成25年度以降は機構の内部監査で実施
  - 外部からの攻撃を想定した情報セキュリティ対策は監査対象外であった
  - 監査部実施のリスク・アセスメント手順にインターネット接続状況等の標的型攻撃を想定した評価項目がなく、リスク・アセスメントに標的型攻撃を想定した取り組みとなっていなかった
- 現場に対するガバナンス不足
  - 数千件/年の指示依頼が全国に発出、現場での理解・徹底に負荷に。過去の重複も
  - ルールは本部策定、遵守管理は執行部門に。 ルール遵守状況を本部が把握できない

- この運用要領は守れるか？ 確認は？
- 守れない要領はないのと同じ

- 誰が監査項目の見直しをするのか？
- 年金局と機構での相違が問題なのか？

大規模情報漏えいにおける
セキュリティマネジメントからの考察

どの様に対応するのか？

オープン質問とクローズド質問（Open question & Closed question）

- オープンな質問：相手に答えを自由に考えさせる質問
- クローズドな質問：「はい／いいえ」等、制限された選択肢内の言葉で回答できる質問

ピラミッドストラクチャー（Pyramid structure）

- 最初は，「はい／いいえ」等で回答でき，限定された質問から始め，少しずつ幅を広げていき，オープンな回答で幅広い内容を聞いていく

コミュニケーションスキル講座：聴く力と話す力を磨く！
http://itpro.nikkeibp.co.jp/article/COLUMN/20070529/272792/

内部／外部監査での質問方法

- 外部監査等で「最新のOSを使っていますか？」と言った質問をする監査人がいる． これに対し，一部の人たち（報告者も含め）は，XPを使っていても，「はい」と回答する． 監査人に指摘されたら，「XPが最新のOSだと思っていた」という． 正しい回答を得るには，「現在使っているOSは？」と聞く必要がある
- また，優れた質問者（悪者とは限らない）は，対象者から求める情報を意識させることなく聞きだす技術，誘導質問術（Elicitation Techniques）を使うこともある

内田勝也「誘導質問術からみた個人情報漏えいの考察」情報処理学会論文誌 2015.12

- ベネッセのISMS審査員（英語は Auditorで監査人）、内部監査や年金機構のセキュリティ担当者は適切な質問をしていたのだろうか？
  質問が悪ければ、正しい回答を得られない可能性も高い

大規模情報漏えいにおける
セキュリティマネジメントからの考察

終わりに

- 良い制度・仕組みでも，機能していなければないとの同じだが，しばしば制度だけをみて，問題を見逃すケースが多い
- 聞き方で，正しい結果が得られなかったり，再度，質問をやり直すことになる
- オープンな質問とクローズドな質問をうまく利用することにより，会話が継続し，親しい関係を短時間で築くことも可能になる
- 「誘導質問術（Elicitation Techniques）」という言葉を知らなくても，多くの場面で利用されていることがわかると，悪意の利用への対処方法，間接的な情報収集で人間関係を円滑にすることも可能になる

- 制度と運用を明確にし、PDCAを確実に回す仕組みが必要
- 「監査」の英語は Audit で「聴く」という意味であるが、「監」は、上から目線を感じる。むしろ、「岡目八目」[1]の考えが、本来の監査ではないだろうか？
- 年金機構 「定期点検で個人情報が流出拠点から【共有ファイルサーバの整理及び個人情報のパスワード設定等は本年4月末までにすべて対応済】との報告がされていた」
  ⇒ この報告を信じられる組織かを判断できる（専門能力のある）内部監査部門であれば、共有ファイルサーバを確認したのでは・・・

1) 囲碁を傍から見ている人は、対局者より八目先の手が見えるから転じ、第三者は局面全体を見る余裕があり、的確に判断できるという意味

大規模情報漏えいにおける
セキュリティマネジメントからの考察

参考：年金機構インシデント概要

インシデント概要

5月08日(金)	内閣サイバーセキュリティセンター(NISC)より情参室、年金局を通じ、「不審通信を検知」との通報を受領。該当端末を特定し、抜線した. メールは，2通（開封 1通）
5月15日(金)	運用委託会社より「新種ウイルスは情報を漏えいタイプでない」との解析結果を受領し、一旦収束したと判断
5月18日(月)	不審メール受信(99通)
5月19日(火)	高井戸警察署に相談及び捜査依頼。不審メール受信（18日から20通）
5月20日(水)	不審メール受信(3通)
5月21日(木)	NISCより情参室を通じ、不審メールの解析結果受領。同日から端末よy個人情報流出が始まる
5月22日(金)	NISCより情参室を通じ「不審な通信を検知」との通報受領。 該当端末を特定し、抜線。 同日中に該当拠点の統合ネットワークを通じたインターネット接続を遮断
5月23日(土)	運用委託会社より、「不審な通信を検知」との連絡を受領。 該当端末を特定し、抜線。同日中に該当拠点の統合ネットワークを通じたインターネット接続を遮断。個人情報流出が止まる
5月28日(木)	警察より、「機構から流出したと考えられるデータを発見した」との連絡を受領
5月29日(金)	機構全体の統合ネットワークを通じたインターネット接続を遮断
6月01日(月)	事案公表
6月04日(木)	メール送受信回線を遮断

厚労省で、インシデントが事前に発生していた
- 4月22日 攻撃：厚労省 年金局／地方厚生局
  職員が受信メールの添付ファイルの開封で、端末が感染し、C&Cサーバに不正通信が発生。
  この通信のアクセスログから、不明な文字列が付加されているなどの特徴があった
- NISCから通知を受けた厚労省はURLブロックを行い、通信発生の約2時間後に遮断された

流出した情報	件数
２情報（基礎年金番号、氏名）	約 ３．１万件
３情報（２情報 ＋ 生月日）	約 １１６．７万件
４情報（３情報 ＋ 住所）	約 ５．２万件
合　　計	約 １２５．０万件

大規模情報漏えいにおける
セキュリティマネジメントからの考察

参 考 資 料

- 日経IT Pro，コミュニケーションスキル講座：聴く力と話す力を磨く！ http://itpro.nikkeibp.co.jp/article/COLUMN/20070529/272792/
- クリス・ハドナジー， ソーシャル・エンジニアリング， 日経BP社
- 日経IT Pro， セスペ試験で学ぶ セキュリティ事件簿 [第4回]ベネッセを襲った個人情報漏洩事件 http://itpro.nikkeibp.co.jp/atcl/column/15/082000196/082000004/
- 三菱UFJ証券，調査報告書（抜粋）平成21年（2009年）7月2日， http://www.sc.mufg.jp/company/news/apology/investigation.html
- ロバート・チャルディーニ，影響力の武器，誠信書房
- 日本経済新聞，続報オンライン犯罪，1981 年10 月18 日朝刊，13 版
- 内田勝也，誘導質問術からみた個人情報漏えいの考察，情報処理学会論文誌 2015.12

大規模情報漏えいにおける
セキュリティマネジメントからの考察

ありがとうございました

情報セキュリティ大学院大学
内 田 勝 也
e-mail: uchidak@gol.com
Twitter: @woodytokyo
Facebook: woodytokyo
http://www.uchidak.com/