3D-01

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*

内田　勝也†

所　属†　情報セキュリティ大学院大学

1　はじめに

大量の情報漏えいが発生後における「第三者による事故調査報告」の多くは技術的な対策課題に関連した記述が多く，セキュリティマネジメントからの考察が非常に少ない．この原因が何に依拠しているかは明確でないが，

① キュリティ専門家も，技術者中心でセキュリティマネジメント等は専門外である．
② セキュリティマネジメントを調査対象にすると，他分野の課題が浮き彫りになる．

との話もあるが，憶測の範囲を超えない．

セキュリティマネジメントやリスクマネジメント，セキュリティ心理学を長年，調査研究してきた立場から，公開情報を基に考察を試みた．

2　セキュリティマネジメントの考察

セキュリティマネジメントの観点からは，

① 当該組織の情報資産を洗い出し，どの様なリスクがあるかを評価（リスクアセスメント）し，管理目的や管理策を選択する．
② リスクアセスメントにより，そのリスク対応計画を策定し，必要な管理策を実施し，セキュリティ事件・事故等に対応する．
③ 適切なセキュリティマネジメントが実施されているかを監視・レビューする．
④ 継続的な改善を行うために，内部監査やレビュー結果等に基づき，是正ソチ及び予防措置を行う．

という手順を考える必要があるが，この①から④を，PDCA(計画，実行，評価，改善)と呼んでいる．

3　セキュリティマネジメントの課題

セキュリティマネジメントでは，技術的な対策と異なり，実施した対策が必ずしも明確に見えず，体制があっても適切に運用されていなければ，やっていないのと同じである．

実際，年金機構では，「共有ファイルサーバ内の個人情報へのパスワード設定やアクセス制限等」があり，定期点検時の確認は，「全て対応済み」回答であったが，一部は非対応であった［1］．

実施すべき処理ができているかは，単に聞くだけでは十分でない場合もあり，実行されているかの調査も必要になる．

監査人の質問で，「最新の OS を使っていますか？」と言った質問だと，Windows XP を使っていても，「はい」と回答する被監査者がいる．単に，「はい／いいえ」が返ってくる質問では不十分で，「OS の名前は？」という質問を追加しないと，正しい結果が得られないことがある．

「**オープン質問／クローズド質問**」を必要に応じ，組みあわせることが大切である．

更に，年金機構の監督官庁である厚労省は，「CSIRT」体制が求められていた｛2｝．しかし，年金機構の事件で CSIRT は，機能しなかった．他省庁の CSIRT は，適切に機能しているだろうか？

PDCA を適切に回すことの重要性が言われているが，年金機構や一般企業であれば，内部監査部門が，評価（Check）を担う必要があるが，中央省庁でも，いずれかの組織が評価を行う必要がある．

4　セキュリティ監査について

適切にセキュリティ対策の実行を確認するための重要なものの１つは監査である．

監査は，英語で「Audit」であり，「聴講する」との意味もあり，「監：上から下を見下ろす，見はりをし，善悪を判断する」意味ではない．四文字熟語の「岡目八目」と同じ目線である．

監査に近い言葉に「検査」があるが，

- 検査：決まったルールに基づいて事務手続きが行われているか確認する．
- 監査：内部統制上から，ルールにリスクがあるかも確認し，リスクがあれば指摘する．

と考える［3］．

ISMS（情報セキュリティマネジメントシステム）認証制度では，審査機関の審査員が審査を行うが，この審査は，「Audit」である．

5　実例から考えるセキュリティマネジメント及びセキュリティ監査

2014 年 7 月に発覚した通信教育企業での大量情報漏えい事件をセキュリティマネジメントの立場から考える．情報処理子会社は，ISMS 認証を取得しており，コンピュータ関係の雑誌でも，図１に示す対策を行っており，セキュリティ対策はきちんとやっていたと述べている［4］．

セキュリティマネジメントからの最大の疑問は，

---

* Research of Security Management from Mass Personal Information Leak

† Katsuya Uchida, Institute of Information Security

これらの対策が適切に機能（運用）されていたかの検証である．

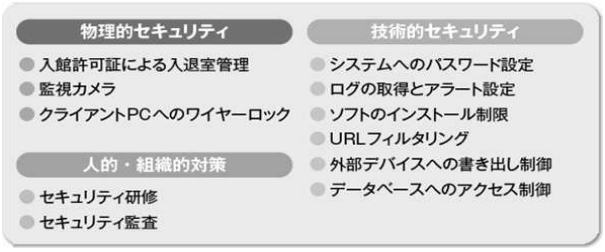

図１ 主なセキュリティ対策

例えば，パスワード設定について，2014 年 11 月の公判時に「データベースにアクセスできる ID が他の従業員と共同利用だった」と弁護側は主張している［5］．

この事件は，業務委託先職員による内部犯行だが，正規職員（部長代理）による内部犯行が 2009 年に発覚し，約 5 万人の顧客情報が名簿業者に売却された「三菱 UFJ 証券」事件がある．

この事件の調査報告書（抜粋）が公開されており，今回の事件にも示唆に富む内容がある［6］．

① (元)職員は，顧客情報等の検索ツールの開発・運用等の実質的責任者で，本件委託先職員を指導する立場で，顧客情報の不正持出が可能な一連の権限等が分断されていなかった．
② (元)職員への管理・牽制も十分でなく，隠蔽行為もできた． システム部は，内部者の不正行為の潜在的なリスクを認識していたが，監視の強化等の対応は途上で，本件行為者の不正行為は監視対象外だった
③ 職員の教育・研修は，意図的不正行為を防止する観点が希薄で，顧客情報等を取り扱うシステム部職員は より高い倫理観が求められるが，そうした点に着目した対応が不足しており，情報セキュリティ管理に関する外部委託先職員の教育・研修も不足していた．
④ 情報セキュリティ管理の総合的な運営のために「情報セキュリティ委員会」を設置し，経営陣も参加して議論を行っていたが，リスク管理上の問題を深く検討したことがない． また，情報セキュリティ管理の統括部署があるが，情報システム管理はシステム部自身の所管で，牽制が働きにくい態勢であった．

と述べている．この様な課題への対応として，

① 情報セキュリティ管理室への情報セキュリティ統括機能の一元化した
② システム部における開発・運用・監視機能の分離を明確化
③ 高権限者に対するモニタリングと牽制
④ 重要なシステムと出口のモニタリング強化
⑤ 利用者の識別が可能な ID 管理の徹底

を行うと述べている．

同様の管理策は，ISMS にもあり，①職務の分離（開発と運用機能等の役割を分離する），②開発環境，テスト環境，運用環境の分離等は，大量の個人情報や知財などの重要情報を扱う場合には，十分に配慮する必要がある．

三菱 UFJ 証券（現 三菱 UFJ モルガン・スタンレー証券）も ISMS 認証を取得していたが，事件当時，十分機能していなかった可能性がある［7］．

６ 終わりに

必要な体制構築しても，機能していなければ，体制がないのと何ら変わりはない． セキュリティマネジメントでは，体制の構築だけでなく，その体制が適切に機能しているかを確認し，大きなリスクがあれば是正措置を求める．

時間の経過や環境の変化があれば，リスクも変わる．そのため，PDCA を回すことが大切になる．

単に，セキュリティ対策を行っているかの質問だけでは，必ずしも的確な状況を把握できないこともある．

本論文は，当該組織の発表（調査報告）やニュースリリースからセキュリティマネジメント的観点から考察を行った． このため，誤解などが含まれている可能性を否定しない．

大量の個人情報漏えいや重要インフラ等でのセキュリティ事故・事件に対して，セキュリティマネジメントからの考察を含め，真の「第三者」が調査し，報告をすべき時代になってきたのではないだろうか？

参考文献

［1］日本年金機構，不正アクセスによる情報流出事案に関する 調査結果報告について，2015 年 8 月
［2］情報セキュリティ対策推進会議 官民連携強化のための分科会，情報セキュリティ対策に関する官民連携の在り方について，2012 年 1 月
［3］先端内部監査研究会，これが金融機関の内部監査だ(第 1 版)，金融財政事情研究会
［4］左門 至峰，セスペ試験で学ぶセキュリティ事件簿，ITPro ，2015 年 9 月，http://itpro.nikkeibp.co.jp/atcl/column
［5］朝日新聞，ベネッセ情報流出、元Ｓ Ｅ 側が無罪主張 第２ 回公判，2014 年 11 月 13 日
［6］三菱 UFJ 証券，調査報告書（抜粋），2009 年 7 月，http://www.sc.mufg.jp/company/news/apology/investigation.html
［7］日本情報経済社会推進協会，ISMS 認証取得組織(三菱 UFJ モルガン・スタンレー証券：初回登録日： 2008 年 3 月 27 日），http://www.isms.jipdec.or.jp/lst/ind/CR_IS_x0020_531963.html