第四回情報モラル・セキュリティ分科会（東京） 議事録
日時： 2009/05/21（木）15:00～18:00 会場： クオリティ 本社 6F 会議室
テーマ： 社内で守られる情報セキュリティルールを作ろう！
司会・進行： 情報モラル・セキュリティ分科会座長 富士フイルムコンピューターシステム株式会社 業務部 プロセス改革グループ 担当部長 橋本 純生 氏

※ 当分科会の運営方針により、個人/会社名を特定できる発言、および発表者から公開の許可を得られなかった内容は 議事録より削除されています。あらかじめご了承ください。

【第一部 前回までの成果発表】

●質疑・意見

○ここでいう「標準」とはスタンダードを意味しているのか、それともプロシージャか。

→スタンダードの意味で作成している。

○具体的な申請時の様式なども意識して作成しているのか。

→今回は作らないが、このセキュリティルールをもとに申請様式を作成することを意識してはいる。

○普通スタンダードはもっとぼかした表現で記述するものではないか。

→あまりに内容を曖昧にしすぎて、スタンダードよりもポリシーに近くなってしまうのは避けたい。

【第二部 グループワーク】

[媒体の取扱に関する標準]

●提案

○タイトルを「電子媒体の取扱に関する標準」に変える。

○対象者を「すべての従業員」→「すべての役員・従業員」に変える。

○対象システムに「すべてのコンピュータ」とあるが、これが何を指すかについては別の文書で規定されていることを前提に修正を進める。

○「媒体の保管・移動・再使用」の前に「媒体の使用」という項目を追加し、「媒体は、会社の指定したものを使用する」「相手先から要請があった場合、持ち出しの許可を得た PC、または社外で使用する場合は上長の許可を取った上でウイルスチェックをして使う」という内容にする。

○「生活マシン」が一般的な用語ではないため、「PC 等」に直す。

○データ出力制限には、ツールを使う以外にもレジストリを書き換える等の方法が考えられるため、「データ出力制限ツール」→「データ出力制限ツール等」変える。

○書き出し許可の期間は１ヶ月に固定せず、会社の判断によるものとする。

○媒体の移動はセキュリティが確保された手段とあるが、別途定義しておいたほうがよい。「社内便は鍵のかかるセキュリティ便にする」など。

○「従業員による媒体の持ち出し」の項目を新たに追加し、持ち出した媒体をどこに保存するかという

ことを規定する。持ち出しの際は上長の許可を得て、暗号化して鍵のかかる場所に保存する。

〇媒体の再使用については、同一部門内で機密レベルが同程度のデータを保存するのであれば再使用してよいものとする。

〇「媒体の廃棄」の項目を新たに追加し、「再生できない方法」とは何かをあらかじめ定義しておく。

●質疑・意見

〇「媒体の再使用」の本来の目的は、廃棄物が増えるのを避けるため。同一部門の同レベルで再使用という制限をすると、残りの媒体は結局廃棄物になってしまうのではないか。

→ハードディスクの消去の方法は確立されているが、USB メモリや携帯電話のメモリについては不確実である。消す方法が確実でないのなら再利用のほうが安全だと判断した。廃棄は物理的な破壊をする。

〇同一部門で同レベルの利用というのは、「再利用」というよりもただの「利用」ではないのか。

→同一部門内でいったん中身を消去してから別の使用者に回すことを再利用と定義する。

〇第 3 回大阪分科会で付け加えた定期バックアップの項目について言及されていないが、これはそのまま残すということか。

→特に議論の対象となっていない。

〇媒体の「持ち出し」と「移動」はどのように異なるのか。

→特に議論の対象となっていなかったが、「持ち出し」＝「出先での管理」（鍵のかかる場所に保管する等）、「移動」＝「運搬時の管理」を意味することを想定している。

［リモートアクセスサービスの標準］

●提案

〇「情報資産を外部から守る」とあるが、情報漏えいは内部者が原因となることも多いので、内外を問わず「情報資産を適切に守ることを目的とする」に変える。

〇機器の管理に関しては、「情報システム委員会が定める利用者」→「情報システム委員会が承認した利用者」に変える。

〇利用環境に関する事項が煩雑なため、16.4.3 は「利用できるサービス、接続方法、機器は情報セキュリティ委員会の定めるものでなければならない」のようにまとめる。

〇アカウント管理について、「リモートアクセスで利用するコンピュータ」の主語がわかりにくい。「社員がコンピュータをリモートアクセスで利用する場合は、情報システム部門の許可を得る。利用者は〇ヶ月ごとに利用許可を更新する」に直す。

〇アカウントは、一定期間にアクセスがなければ、期限内であってもアカウントを停止するものとする。アクセスしない間はアンチウイルスソフトウェアのデータベース更新等、セキュリティ対策ができていないことが理由である。

〇「申請時に許可された社員のみ」が分かりにくい。「許可された社員のみ」に直す。

〇接続記録については、「記録を蓄積して改変のできないように保管」とする。

○文末を「望ましい」→「なければならない」に変える。
○緊急時の対応は、「利用者はパスワードを忘れた場合、情報システム部に連絡をして所定の手順で仮パスワードを入手したのちすみやかに新たなパスワードにしなければいけない」に直す。
○障害が発生した場合、エンドユーザである一般社員がシステムの再構築をすることは難しい場合が多いため、「情報システム部門の指示を仰ぎながら再構築する」に直す。
○コンピュータの保管場所は、「定められた場所」→「鍵のかかる場所」に直す。

［電子メールサービス利用標準］

●提案

○想定されるリスクやサービス基盤といった前提をまず明確にすべき。
○対象者と対象システムの定義が曖昧。「従業員」の規定が別途必要。
○携帯電話のメールはここには含めないこととする。
○機密情報の送受信に際しては、別途文書管理規定で機密文書の定義をする。
○メールの到達確認が必要な場合とはどのようなときか。業務管理規定とリンクして規定しておくべき。
○添付ファイルをすべて暗号化する必要があるかどうかは、各企業の事情によるのではないか。
○メールが通信経路で傍受や改ざんされるリスクよりも、エクセルファイルなどの場合に仕切値や隠し文字等、意図しないものが見える状態で相手に送ってしまうリスクが大きいのではないか。重要なのは添付ファイルをすべて暗号化することではなく、「添付ファイルに相当するリスクを理解したうえで適切な対応を施す」ことである。個別のリスクについてはプロシージャに記載する。
○メーリングリストは情報がアーカイブとして残るため、当初のメンバーだけでなく途中参加のユーザにもすべてのやりとりが見えてしまうが、それは必ずしもメーリングリストだけのリスクだけではないので、特にメーリングリストについて言及すべき必要性を感じない。
○電子メールに付随するサービスについては、Web メールや SNS などに関する規定を「電子メールサービスとネットワークサービス」として項目を別個にくくり出す案が出た。
○HTML メールの送受信について具体的に想定したうえで制限の規定をすべき。ネットワークの負荷、ActiveX、フィッシング詐欺被害のリスクがあることを整理したほうがよい。
○退職社員のメールアドレスについては、出向者・転籍者もこれに準ずる。メールアドレスが代わった場合も同様に。
○電子メールの監視許可については、文面を直す必要はないが、監査を周知することが必要。
○宛先メールアドレスを直接入力せず共用アドレス帳から入力するというのは、望ましいが実際に運用するのは難しそう。これに近い運用をするためには、まず共用アドレス帳への登録が簡単にできなければいけない。あらかじめ申請が必要だと現実的な運用ができないため、登録の際に二次チェック、牽制ができるような仕組みにすればいい。共用アドレス帳に載っていないアドレス宛のメールには「本当に送っていいですか？」と注意を出すなど。
○「電話による到達確認」は電話に限らなくともよいのではないか。空メールを返す、FAX を利用する、など他にも手段はある。業務管理のレベルに応じて決めるのがよい。

●質疑・意見

〇機密情報を送っていいかどうか？という問題は、機密情報とは何か？ということに関わる。具体的な情報資産について判断したうえで決めて欲しい。

〇機密情報のレベル分けについては、「社外秘／関係者外秘」「機密度 1／2／3」といった分類ができる。

［携帯電話貸与・運用・返却の標準］

●提案

〇携帯電話は利用範囲があいまいで、セキュリティの議論ができる段階ではない。スタンダードに集約できない。

〇全体として何をリスクにしているのかを明確にすべき。想定できるリスクとしては、紛失時の情報漏えい、付随機能などがある。

〇個人利用と公的利用に対する考え方の整理をすべき。

以上