全体講評（情報セキュリティ基盤論 2012）

2012/08/31

佐藤周行

今回の情報セキュリティ基盤論のレポートはどうだったでしょうか。問題１(A, B)がいわゆる「文系」ということで事象の解析をしてもらうもの、問題 2(A,B)がいわゆる「理系」ということで技術に関係するものを答えてもらいました。一見面倒な 1-A を解答した人が極端に少なかったということと、2-B にトライして結局砕け散った人が多数いたということが今年の特徴でしょうか。

昨年の講評で「素人考えはいかん。リスクというのは技術用語だ」と言い、今年の授業でも強調したこともあり、問題 1 では比較的まじめに解析・解答した人が多かったように思われます。一般用語の延長で「リスク」や「監査」を語っても業界の人は相手にしてくれません。問題１にきびしめのコメントがついた人はそこらあたりを反省しましょう。

問題２については玉石混交といった感じでしょうか。A の方は、リスク分析も併せてする必要があるという意味で総合問題でした。セキュリティ技術の持つ効果を評価したうえで制度設計をする必要がありました。B の方は、手を動かして S/MIME のブラックボックスの中身をこじ開けてみろという問題でしたが、完全にトランスペアレントにしか考えられず「openssl smime –verify で successful と出るからＯＫで一っす」というのは、理工系の専攻に在籍する学生としていかがなものかと。

今回は MANABA による双方向のレポートの評価を本格的にやりました。まずは e-Learning システムである MANABA を使う機会をくださった朝日ネットさんに御礼を申し上げたいと思います。どうもありがとうございました。レポートを提出して、少し経ったらコメントがつけられて戻ってきたと思います（「少し」の程度は問題によって差がありましたけど)。面食らったであろうことは一部に「再提出」の指示があったことだと思います。GPA とか何とか言って評価の世界も世知辛くなってきますから、できるだけ良い点を上げたいのですが「いくらなんでも」というレポートに出会ったときはやはり再提出してもらわないといけません。実際、複数回「再提出」を食らった人もいました。e-Learning システムというのは、「出したレポートを一発評価」という従来型の評価に代わって、「できるまでやってもらう」というある意味「理想的な」評価方法を支援するということが今回はっきりわかりました。教師にとっては喜ばしいことです。学生にとってどうなのかは、来年以降レポートを出す人数が評価してくれるでしょう。

さて、例年、素晴らしいレポートに出会えます（このために教師をやっているようなも

のです)。今回単位を出した 50 人強の中で、以下の 3 人を最優秀賞に選びました。履歴書に書けるほどの権威があるかどうかはわかりませんが（ないです)、控えめにご自慢ください。

最優秀賞：　伊藤悠貴　君
　　木下僚　　君
　　多田和弘　君
（50 音順）

個別講評

問題は http://www-sato.cc.u-tokyo.ac.jp/PKI-project/ISECINF2012Problems.pdf におかれています。問題を見直したい人、また授業を受けていず、講評だけを見て興味を持った方はご参照ください。個々人の講評は MANABA を見てください。

１－Ａ：

本設問はある程度自由に回答可能なものですので、以下の考え方は、一例です。

情報資産を「財務諸表」（あるいはその元となる「財務データ」）と考えて、4/24 資料の P. 83 のような表を作成することが、本講義でのリスク分析になります。（そこに至るまでの説明は、資料全体を参照してください。また、脅威やぜい弱性は、本設問の条件に合わせて　考え直す必要があります。）

A 氏は、財務諸表に関する重要性の理解として、株主総会前と株主総会後で重視する点が異なっていたと思われます。（同じ情報資産でも、時間軸でリスクが変化する可能性を理解することも重要です。これはパスモの履歴の不正利用を例として説明しました）

表では、機密性、完全性、可用性が、すべて同じ数値で評価されていますが、もし企業が必要とするならばそれらの数値に係数をかけることが可能です。（教科書 P. 36、第１部の問題９あたり）

例えば、株主総会前では、機密性についてリスク値を高めに設定し、情報漏えいに考慮したような対策（システムの完全分離、財務諸表の金庫への保管）を行ったと思われます。また、株主総会後では、可用性を重視し、自社システムで管理するのはリスクが高いと判断し、クラウド業者にリスクを移転しているものと考えられます。

A 氏は、残念ながら、完全性についてはリスク値を低く評価したか、あるいは、脅威やぜい弱性の洗い出しが十分でなかった可能性があります。

その結果、起こりうる事件としては、財務諸表への不適切な情報記載です。ぜい弱性のある可能性としては、営業部と経理部との間の発注書のやり取りの中で、確認作業がない（→単独の意思で改ざん可能）などの考慮漏れがあったものと考えられます。

本設問は、結果を見て、リスク分析を想定しますので、上記に合うように、リスク値（情報資産の機密性、完全性、可用性、及び、脅威とぜい弱性のレベル）をうまく定義してリスク値に応じた対策の導入状況等を説明することが求められています。

１－Ｂ：

この設問は、組織のセキュリティレベルの評価（監査）を行う場合によく採用される「成熟度モデル」を実際に適用してみようとする問題です。「成熟度モデル」に基づく監査が他の、例えば準拠性監査と異なるのは、評価の結果をフィードバックして、レベルの改善につながるという点です。PDCA サイクルと相性が良いということも期待されています。監査における成熟度モデルというと COBIT や NIST のものが有名ですが、成熟度モデルそのものは他にも適用されています。ソフトウェアの品質管理における Capability Maturity Model なんていうのはその典型ですね。

さて、解答の前に意識しておくことは、問題となっているのは一義的には組織のセキュリティ管理の方法であるということです。ＡさんとＢさんの属している部署は違いますから、それぞれに課されているセキュリティに関する義務も異なるでしょう。ＡさんとＢさんの振る舞いから、その組織の成熟度をまずは評価しましょう。営業支店よりデータセンターの方が成熟度の点で高いのは当然です。営業支店が L1、データセンターが L3 くらいで運用されているようですね。できたばかりの部署だからまだ手探りなのかもしれません（本当は親会社のセキュリティポリシーにまずは従うとは思うのですが）。また、データセンターでは、教育や訓練の機会が提供されています。このためには関連する規則くらいはあると考えるのが普通です。それを超えてレベルを定量的に評価して何か対策を練っているかと言われれば、それは少し仮定が必要になるかもしれません。一般にレベル付けの根拠は規則、訓練の存在や従業員の習熟度等に求められるわけです（問題はヒントにあふれていましたね）。その検討をした上で、個人のスキルの評価をすればよいと思います。本当に監査（学生さんに監査といってもピンと来ないとは思いますが）をするのだったら、組織の評価をした上で、それをあげる方法の提案、特に個人を対象にした組織的なスキルアップの提案をすればよいと思います。

２－Ａ：

本設問は、（技術的な|個別の）脅威への対応策について、実際の業務や組織におけるリスク低減とどのような関係にあるか検討するというものです。

どれだけ高度な対策であっても、「金銭的コスト」「手続きが煩雑」「ユーザーの知識が必要」「業務フローとあっていない」といった理由により実際のリスク低減に結び付かないケ

ースは少なくありません。(「安易な技術的対策」が失敗する大きな理由の一つです)

この事を踏まえると、脅威・脆弱性への対策については、期待される効果やコストだけでなく、実際の運用環境に適用しやすいかどうか、また効果を発揮する上での阻害要因がないか、といったことについても検討が必要ということになります。(残念ながら、個別の技術要素に対する説明を出ない回答が一定数ありました。)

今回は、「ログイン情報盗用」という脅威に対し実際に採用されている対策を評価することになります。回答にあたってポイントとなるのは、銀行という様々なユーザーが多数想定される状況において、対策の実効性確保のために何が必要か意識されているか、という所です。

例えば、セキュリティソフトウェア（マルウェア対策ソフト）は、導入すればユーザーのスキルに依存せず、一定のリスク低減効果が見込めます。この対策に関しては、各種製品の検知率を比較選定するよりも、まずソフトウェアの導入とパターンファイルのアップデートの必要性を認識し、実施する ～金融機関から見れば、「してもらう」～ 事が、リスク低減のための主要なコスト、あるいは実効性を確保するために対応/受容すべき欠点・制約である事を分析・記述されていることが求められます。

本設問にあるように、情報システムのセキュリティリスク低減のためには、個別の技術要素だけでなく、システムをその一部として成立している組織・業務の理解に基づくセキュリティ設計が必要です。

２－Ｂ：

この設問は、S/MIME の具体的な処理手順をごく基本的な構成要素から構築しなおしてくださいという趣旨の問題です。S/MIME はもはやメールの基本的なツールになっていますから、今更、処理手順など気にしなくてもよくなっているとは思いますが、ブラックボックスをこじあけて、動作の基本原理を暗号の基本的なツールから理解しなおすことは決して無駄にはならないと思います。その意味で 「openssl smime -verify とすると成功する」以上のことを書いていないレポートが一定数見られたのは残念でした。ブラックボックスのままじゃん。また、実際のデータで検証することなく「a.txt のハッシュ値を暗号化する」と書いているレポートも多く見られました。ハッシュ値を取る対象は a.txt ではない、と補習の場でも強調したと思います。認証属性がハッシュ値の対象になっていることは RFC を見ればわかるし、実験すれば確かめられます。きっと、大雑把なブロック図を見て「こうなっているに違いない」と実験もしないで思い込んだのですね。追試の重要さは勉強しませんでしたか？

なお、暗号が RSA になっていることにより、署名と暗号化が同じルーチンで実装されているので、今回は復号もできましたが、一般の公開鍵暗号では署名アルゴリズムと暗号化アルゴリズムは異なっており、復号も一般にはできません。RSA に限ったトリックだとここで念を押しておきましょう。

この問題を解くときに基本となるのは署名データの ASN.1 パース（openssl asn1parse）ですが、そこまでは自作しなくてもよいです。ただ、署名部分の復号を行った結果が認証属性のハッシュ値と一致することを確認してください。

正解にいたる道筋は以下のようになります。

１． MIME形式のa.mimeからmime.p7sを取り出す(エディタでも、openssl smime -pk7outでも)

２． mime.p7s の ASN.1 構造をみて、認証属性を取り出す。(openssl asn1parse -strparse XXX -noout) 今回は位置 911 以降が認証属性になっていたはず。認証属性には a.txt のハッシュ値が入っている。9925…のデータが相当する。

３． 認証属性に続けて署名データが置かれているのでそれを取り出す（openssl asn1parse -strparse YYY -noout -out signed) 今回は mime.p7s 中の位置 1106 以降がそれに対応したはず。ファイルはとりあえず signed とでもしておく。

４． signed を復号すると、8a3c…ではじまるハッシュ値がでてくる。これが 2. で取り出した認証属性のハッシュ値と一致することを確認する。

ここまでできると、S/MIME の処理系（の署名部分）が作れるようになります。