2018/09/12
佐藤周行

情報セキュリティ基盤論（2018）講評

1. 表彰

   佐藤の成績のつけ方はとても甘いのですが、それではインセンティブが働かないこともあり、優秀なレポートを提出した人を講評時に表彰することで差をつけています。評価基準はB問題での解析の深さおよびA問題の解答の正確さです。

   最優秀賞　李東池君　水木祐哉君　　田中大揮君　品川大樹君　船曳敦漠君
   優秀賞　　林田淳一郎君　邵文君　朱傑君　Song Jungmin 君

   履歴書に書いて威張れるかどうかはよくわかりませんが、適当にご自慢ください。

2. 全体講評

   問題はA（必須）問題で、基本的な事項を聞き、B（任意）問題で、ミニプロジェクトの形で、少し大きい問題を解いてもらうものです。

   １Aは情報資産のCIA（AICという言い方もバズっているようですが）の理解です。授業を聞いていれば一発なんですけどねぇ。例年頓珍漢な答えが一定数見られるのはいかがなものか、と。２Aは多層防御を指定して、攻撃に対する防御策を立案させるものです。授業で典型例としてあげたんですけどね。３Aはアイデンティティ管理に関する問題です。様々なフェーズにおいて、想定される脅威とそれへの対応例をあげるものです。A問題の通奏底音は「情報資産の管理方法」です。１は評価について、１－３は、脅威とそれへの対応の仕方を問うています。これが情報セキュリティの基本中の基本ですから、がんばって理解してください。
   続いてB問題です。
   １Bはシステム構築のやり方として標準的なものとして考えられるオンプレミス、クラウドに加えてブロックチェーンを考え、それぞれのリスク評価をし、最後に対応策を決断する（この経営判断のためにリスク評価をするのだという事実を忘れて暴走してはいけません）という問題です。簡単化されていますが、通るべき道は基本的にすべて踏んでいることに注意してください。
   ２Bは2018年に発生した実際のセキュリティインシデントのレポートを元に、授業でやった(Cyber) Kill Chainの考え方を当てはめて、レポートを「再」解析してみよとい

う問題です。「再」解析によって、新たな視点でインシデントを見ることができます。はっきり言って難しいのですが、果敢にチャレンジした人が多数見られました。

３B はロボットに関し、脅威とそれへの対応の例をあげてもらう問題です。ロボットや AI（機械学習）については、法学その他さまざまな観点からいろいろな問題が提起されてきましたが、この問題は、現場においてのセキュリティ対策の観点からロボットを理解するというものです。

3. 個別問題の解説

以下、採点者の各先生からの B 問題の解説をあげておきます。今後の勉強の参考にしてください。

１－B：

基本的には提出者の方の理解度は概ね高かったと言えると思います。今年の出題では、３つの異なった方式のシステムを比較するということで、例年からすると若干挑戦するハードルが高くなってはいるかと思います。

ただし、情報資産を１つ（取引記録（データ））と限定したことで、評価すべき資産価値は１組（機密性、完全性、可用性の１セット）になりますので、結果として最終的な脅威・脆弱性の組の数はそんなには多くないとは思います。

（それぞれのシステム方式のリスク値算出がちょっと手間でしょうか）

今回は情報資産固定なので情報資産の資産価値も固定なのですが、一部、システムの特性によって資産価値が変化するリスク評価のレポートも見られました。資産価値は、企業としてその情報をどのくらい重要とみなすか、の指標ですので、先に資産価値を固定しそのあとシステム側の評価を行う流れを想定していました。

脅威と脆弱性ですが、全方式に対応する組み合わせを一括で網羅的に洗い出すことも可能ですが、リスク分析では優先順位を洗い出すことが目的ですので、その方式においてリスクとならないようなことは除外し、各方式にあった組のみを選び出して効率的に行うことができます。例えば、クラウド方式やブロックチェーン方式では、自社でのハードウエア管理はほとんど想定しなくてもよいので、列記しなくても問題ありません。

オンプレミス方式→クラウド方式→ブロックチェーン方式と進むにつれて、自社でコントロールできる脆弱性が少なくなってきます。今回は出題に含めませんでしたが、脆弱性がコントロールできない場合は、リスク対応のうち、軽減ではなく移転（他にリスクを負担、保証させる）を採用する必要があります。通常は契約上の制約や保険などを利用します。

世の中では、セキュリティ上のリスクを被害金額等の数値化により、可視化する試みはいくつかありますが、情報資産の企業にとっての価値というものはなかなか評価しにくいものです。（漏洩前提で被害金額を計算しても、それが客観的な資

産価値かというとそうではないですね。そもそも最近は、例えば個人情報が漏洩したとしても、何も保証しないことが多いし裁判例もほとんど増えていない状況です）

現実的に情報資産にどんな価値があるか（＝企業としてどこまでコストをかけられるか）は、数値化しようとすると非常に難しいため、リスク分析ではある程度大まかなリスク値を算出することにより、優先順位を定め、企業にとって一番問題となるリスクから対策を導入していく（＝通常は、脆弱性の数値を下げる）ということは、理解しておいてください。

２－B:

【全体の評価】

実際に起きたセキュリティインシデントをもとに考察する課題です。難易度としてはかなり高いかと思いますが、優秀な回答が複数ありました。一方で、単純な報告書記載事項の後追いとなってしまっている回答も少なくありません。

【回答のポイント】

この設問は、実際のインシデント報告書をもとに事実をフェーズに分けて理解（設問 1a）し、改善案を提示（設問 1b）する必要があります。「体制の問題」「手順の不備」のようにフェーズ分けをせず、不足点の指摘にとどまっている回答が見られました。報告書はインシデントの経過についてよくまとめられているので、全体を俯瞰して、単一の出来事としてとらえがちですが、きちんとセキュリティインシデントのフェーズとして分解する必要があります。実際のインシデント対応においても、原因が特定・対応されないまま復旧が行われ、インシデントが再発に至るケースがあります。無理に俯瞰しようとせず、今何ができているか、何をするべきかという検討が必要です。

また、この課題では報告書には書かれていない、準備できていたであろう事柄を記述する必要があります。（設問 2）推定した内容が、マイネットが行った対応の裏付けとなっていることを、矛盾なく説明できる解答が求められます。ここでは、いわゆる「セキュリティ対策」だけを目的としていないことも記述可能なことがポイントとなります。例えば、インシデント知得から 2 時間未満で 13 のサービスに対し「緊急メンテナンス」をアナウンスできるという点は、ゲームサービス事業者におけるシステム特性が生かされた場面であるといえるでしょう。準備はすべてのフェーズに関連する段階であり、準備をしていない事への対応は困難であるということ、またシステムや業務の特性にかなった対策が有効に機能していることを認識してもらえればと思います。

３－B:

＜全体講評＞

３B 任意の課題は、登録学生 108 名中、提出者 52 名（48%）と半数が提出していました。成績は、提出者 52 名中、最優 4 名（8%）、優 5 名（9%）、良 31 名（60%）と、こちらも例年とあまり相違ない比率でした。ただし、可 12 名（23%）の内 4 割が、レポートの文脈が同じである事、レポート提出日が同じ 31 日である事、かつ時間帯も同様である事から、誰かの回答をコピーした感があります。ただし３B のレポートも、丸写しは視られず、各自、それなりに課題解決策を記述していた事は、課題に興味が有ったと考えられます。

＜特異な講評点＞

特筆すべき点は、最優と優の学生 9 名（計 17%）が、かなりロボット法に興味を示したと思われる点です。人の命令は「言った事と期待する事」が異なる事を明示し、それに反し、ロボットは自己学習するもルールに基づくと捉え、ロボットと人間社会が共存する社会的なセキュリティ基盤について述べている点は、優れていると判断できます。