2015 年度情報セキュリティ基盤論レポート講評

2015/09/14

佐藤周行

１．全体講評

今年の３題は以下のようなものでした。どうだったでしょうか。

I. 鉄道会社を例にとり、組織が保有する情報資産、特に個人情報を含むデータのリスク解析と対応策の策定を行う。

II. 実際のセキュリティインシデントを探してきてインシデントのシナリオを構築し、さらに多層防御を含む対応策策定の一環として「出口対策」とその有効性を論じる。

III. センサー系が我々の周りに張り巡らされ、それに基づいた 自律的なサービスが提供されるようになった今、引き起こされる社会制度的な問題を解析する。

詳細な論点は実際に採点に当たった先生による個別講評に譲ることにして、ここでは全体的なことを記します。

最初の問題 I は、情報セキュリティの問題としては標準的なものです。リスク解析と対応策の策定の流れとしては１．情報資産の特定と評価、２．脅威と脆弱性の列挙、３．前２つからのリスク値の算定、４．リスク分析に基づいたセキュリティ対策の策定となります。これらが一連の流れとしてきちんとつながっているレポートなら OK、どこかが切れているともう一度考え直しということになります。特に最後の４．が抜けていた人、画竜点睛を欠く形になったのは惜しい！

情報資産として個人情報を含むものがあり、個人情報の重要度は近年上がっています。変化する情報資産の評価値に応じて、１－４までを計算しなおすケースは今後増えていくと思います。将来の仕事の参考にしてください。

なお、例年「リスク」を「危険性」という一般用語で解釈してとんちんかんなレポートを書く人が例年何人かいるのですが、今年はこの点は大丈夫だったようです。

次の問題 II ですが、実際にあったセキュリティインシデントを読み解いたうえで、対応策を考えるというものです。社会的に話題になったインシデントは、報告書が公表されたり、報道である程度詳細な状況が明らかになったりします。それを時系列で読み解いて、実際の攻撃として何が起こったのか、どのようにして発見されたのかを理解するというのが最初のポイントです。実際に解析された例はいろいろなものがあげられていました。わかりやすい報告書があっても、そこからポイントを抽出することは依然として必要です。また、事件横断的に特定の攻撃手法を解析す

るレポートもありました。これでも Ok です。

攻撃を読み解いたら、次は防御策です。問題では「出口対策」を指定して対応策を考えてもらうことにしました。実は、標的型攻撃など、根治が難しいものに対しては多層防御で対応するという流れになってきています。出口対策はその重要な構成要素になります。最近の考え方の一端に触れてください。

最後の問題 III ですが、これは IoT の問題です。社会にセンサーが張り巡らされ、そこから上がってくるデータに基づいて社会活動に必要な意思決定が人間だけでなくプログラムによってなされるようになると、どのような社会的な問題が考えられるかを書いてもらうものです。

まずはセンサーネットワークが社会にどのように影響するかですが、ポジティブな面、ネガティブな面の両方に対して論じることが求められます。また、セキュリティ的な面からの解析も重要です。IoT の名のもとに、社会生活にセンサーが浸透している近未来（一部現在）を想像してください。

その次は、センサーから上がってくるデータをもとにプログラムが意思決定をするようになったら、それは従来人間が築き上げてきた法制度を含む社会制度とどのように整合性をとらなければならないのかという議論をしてもらうものです。論点は一部抽象的でしたが、きちんとブレークダウンした議論がなされたレポートに高い点数がついています。

２．最優秀賞

各問題に対して、１－２本、優秀なレポートが観察されました。優秀なレポートを書いた方には個別にメールでお知らせしました。おめでとうございます。その中で、優秀なレポートを 2 本そろえた真藤君に最優秀賞を送りたいと思います。

最優秀賞：真藤達也君

権威があるわけではないのですが、控えめにでもご自慢ください。

３．個別講評

【問題 I】

本課題では、企業における情報資産に対する「リスク分析」を実施し、その結果から採用すべきセキュリティ対策の優先度や具体的な対応をまとめる、というものでした。今年

は、情報セキュリティとしての「リスク分析」について、完全に外れているレポートがなかったという点で、全体感としては良好であったと考えます。ただ、今年は授業での説明前に課題を提示しており、検討の時間は十分にあったはずですから、一部の観点が欠けていると思われるものについては若干厳しめの再提出となっています。

まず始めに、リスク分析を実施するにあっては「情報資産」を洗い出す必要があります。課題中にも例示していますが、その形態は、紙であったり電子データであったり、さらには映像であったりもします。もし余裕があれば、自動改札や改札内の駅員用端末、非接触型カード自体（内臓チップ）などのハードウエアも挙げられるとよいでしょう。

情報資産が挙げられたら、次にそれらの状況を考えます。紙の申請書はどこに保存されているか、電子データはどこから入力されてどこに保存されどこで表示することができるか、などを確認します（実際の企業では現物を確認しますが、ここでは課題なので自分で定義します)。なお、最近の監視映像はサーバに電子データの形式で保存されていることが多いです。カードの利用履歴等を課題に挙げましたが、鉄道会社にとって本当はどこまで必要か？に踏み込んだ回答が見られなかったのは残念です。例えば、乗降駅は記録がないと鉄道運送業務が実行できませんが、駅の外のコンビニで買い物をした履歴は、どこまで鉄道会社で管理するものでしょうか。余計な情報を持たない、というのも 1 つのセキュリティ対策です。(購買履歴でも、駅ナカと駅の外を分ける、という案もありかと思います)

情報の資産価値については、一般的にはそれぞれの企業によって考え方が異なるため、一律にリスク値を定義することは困難です。そこで、自社の状況に応じてそれぞれリスク値を算出する基準と計算式を定義します。「セキュリティ」という言葉だけを聴くと、報道では某国家が盗聴したとかスマホからデータが抜かれるとか個人情報漏えいといった話が、すぐに思い起こされるかもしれませんが、情報セキュリティは 3 要素、機密性、完全性、可用性で考える、ということは授業でも何度か説明しています。例えば、IC カードを自動改札にタッチして、1 秒以内に反応がなかったらどうなるでしょうか。高い可用性を維持しているからこそ、自動改札にタッチしているあの短い時間（実際には 0.2 秒ほど）の中で、乗車経路を割り出して決済まで完了させることが可能となります。しかも、勝手に情報が改ざんできない完全性の対策も十分でなければなりません（カードは自分の手中に入手できるので、いくらでも悪意を持った解析が可能です)。そういった仕組みにまで言及している例が、極めて少ないのは惜しいところです

なお、利用者観点で「個人情報は、保護されなければならないから重要である」と、いきなり判定しているレポートがありましたが、それはあくまでも消費者側の「なんとなくそうであってほしい、という期待」であり、本レポートでは企業としての観点で客観的な判断を記載してほしいところです (企業はどちらかというと、ビッグデータを活用したい)。

脅威と脆弱性については、情報資産 1 つに対しては複数存在し、それぞれに対してリスク値（影響度や弱い点）を数値化することが必要です。本気でやると膨大になりすぎるので、レポートとしてはある程度省略してもかまいませんが、1 つの情報資産でも、どの脅威

から保護するか、によって対応は変わってきます。
以上のような検討を、リスク分析にて実施し、リスク値の高い情報資産、脅威、脆弱性の組を見つけて、軽減したり、移転したり、回避したりします。リスク値が低いものは受容でもかまわないでしょう。受容できる点数は、全体のバランスを見ながら定義します。リスクを軽減するなど、対策後の点数まで計算できていると、なお完璧です。
これらのような、一連の総合的な判定ができているものが、本課題にて期待される回答ということになります。

【問題 II】

問題 II では、実際のセキュリティインシデントを読み解いてもらい、その経過と対応策について考えてもらいました。
回答にあたってのキーポイントは 2 つあります。
１：公開情報をもとに、公開されていない部分を推測する
２：被害経過をもとに、実効性のある出口対策を検討する
まず 1 ですが、これは「公開情報」を「その時点で分かっている情報」と読み替えれば、自分がシステムオーナー、またはシステム管理者であった場合の被害範囲の見積りと対応検討のプロセスと同じです。単なる公開情報の整理ではなく、システム特性を考慮した攻撃手法や被害範囲の見積りがされているレポートを高評価としました。
２番目のポイントは、対策の「実効性」については、きちんとインシデントを理解した上で、「出口」で捉えるべき対象は何か？を考えるということです。今回、「外部向け通信を監視して、怪しい通信を遮断する」という趣旨の回答が複数ありましたが、これを実現するには、どうやって監視するのか？そもそも『怪しい通信』とはなにか？というところを検討する必要があります。
ここについて検討されている、または検討するためのプロセスを組み込んでいる回答は残念ながら多くはありませんでしたが、それらは高評価としています。

【問題 III】

－問題 1：IoT]普及が社会生活にどの様に影響するか出題した。難易は標準－
IoT の普及から社会生活への影響が幅広く問われた。問題は、技術進歩が或るとき飛躍的に進化する視点を含め利便性が生むマイナス面を例示してもらい、その課題対応策を出題した。セキュリティ技術の知識だけでなく社会インフラ全般の基本的なリスク認識が問われた、問題難易は、標準であった。

－問題 2：自動ソフトウェアが社会的な位置づけを出題した。難易はやや難－
問題数 2 問の内、自動プログラムの欠陥を誰が賠償責任を負うのか問われた。問題は、自動運転で交通事故が発生した際、運転者の責任か自動車メーカの責任か、依拠となる状況を述べる事を出題した。掃除ロボットが日本で開発されながら製品化が他国に大きく遅れた問題でもあり、複数分野からの検証が問われた。問題難易は、やや難または難解であった。

以上