2017/09/15
佐藤周行

情報セキュリティ基盤論　2017　問題講評

情報セキュリティ基盤論では、レポートの採点と成績報告がすんでから、毎年レポート問題の講評と優秀賞の発表を行っています。今年（2017 年）は、レポート問題として必答問題と選択問題に分けました。必答問題は、すぐに答えが返ってくるだろう基礎的な問題、選択問題は少し調べ物をしないと解けない問題にしました。必答問題を下にあげてみましょう。

必須課題

1-A

(1) 情報資産の“資産価値” を構成する 3 要素について名称を挙げよ。

(2) 情報資産に対するリスクを考える際の 3 要素のうち 1 つは“資産価値”だが、残りの 2 つについて名称を挙げよ。

(3) 前問にて挙げた、2 つの要素は互いに対になる（ただし、1 対 1 とは限らない)。対になる組の例を、具体的に 3 つ以上挙げよ。

2-A

(1) 境界ベースの防御を実現するためのセキュリティ技術を 2 つ以上挙げよ

(2)　前項で示したセキュリティ技術を組み合わせた多層防御の構成を提示し、「どの技術が」「どのような攻撃を」防ぐための仕組みとなるか記述せよ

3-A

IoT におけるアイデンティティおよびアクセス管理（IAM）について考察せよ。以下の論点から想定される影響（事例が明示されるとよい)と、有効と思われる対策（根拠が明示されるとよい）を述べよ。

(1) 脅威の影響範囲が広いために、起こりうる情報セキュリティの影響と対策案を記載せよ。

(2)ライフサイクルが長いために、想定される情報セキュリティの影響と対策案を課題を記載せよ

1- A は、リスク分析に関するもので、(1)は CIA、(2)は脆弱性と脅威、(3)はいろいろありますが、最近私が影響を受けたものでは、SS7 の脆弱性とそれを狙った OTP 盗聴（のために、公衆網を使った SMS への OTP 送信サービスが廃止されたことがあって、さんざんで…）などがあるでしょう。

2- A は、授業でやったのがファイアウォールと EDR の組み合わせでした。「外部」の通信監視と、「内部」の異常検知を組み合わせて効果を高めるというものです。異なるセキ

ュリティ境界を想定してそこでの防御策をあげることが必要です。同じ境界上の防御策をあげると(2)でつまります。

3- A は、IoT ネットワークの統制に IAM（人の identity ではなく、機器の identity）をどう適用するか、その問題点をあげる問題です。IoT 機器は、通常の PC 等と異なり、数としては桁がちがうし、構成するネットワークも異質なので、管理の粒度とミドルウェアのアップデートに関係するセキュリティ上の脆弱性が無視できません。担当の先生からは、以下のような講評をもらっています。

例えば、現行法の製造物責任法で想定していなかった、オープンソース（無料のダウンロード・アプリなど）やオープンデータ（無料の地図データ）などを消費者が自らインストールできてしまう現行のドローンの脅威と過失責任問題や、海外に居るドローン製造業者やアプリ開発キット提供者と国内の消費者間における損害保証の枠組みなどが論点として望まれた。

必答問題に答えたうえでの選択問題ですが、今年は、題意の取り違えか、授業を聞かずにネットにころがっている情報を適当に取捨選択して解答を作ったからか、再提出をお願いしたレポートが例年になく多くありました。情報セキュリティという言葉自体は、社会的なインパクトが大きくなってしまい、結果として皆が知るようになり、それなりに事例研究なども与えられていますが、そういう表面的な知識だけではなく、考え方も含めて「授業を聞いて」勉強してもらいたかったと思います。

さて、B 問題の解説と講評に行く前に今年の優秀賞を発表します。今年は 4 名です。履歴書等には書けないとは思いますが、控えめにご自慢ください。

優秀賞：張 昊　君，大川 幸祐　君，友野良輔　君，曾　逸然　君

B 問題の講評

１－B：A 社は、企業向けのホスティング会社（※１）である。

・A 社は、ある日、ランサムウエアに感染し、顧客提供用のサーバ 150 台が暗号化された。その中には顧客が利用するデータベースや動画コンテンツなど、顧客にとってはかなりの価値のある情報が含まれていた。

・A 社のサービスとして、バックアップは取得していたものの、バックアップファイル自体がランサムウエアがアクセス可能なディレクトリ内に存在したため、暗号化されてしまった。

・暗号化解除費用として、5 億円を要求されるが、支払える金額は 5000 万円程度。

・やむなく、A 社は、B 社に買収される前提で、B 社に身代金を支払ってもらい、A 社自体は消滅することとった。

・この場合、A 社の情報セキュリティについて、

(1) A 社の CEO（最高経営責任者）として、ランサムウエアの被害に遭う前の時点における、リスク分析を実施せよ。

(2) 本来、どのような対応を取るべきであったが、リスク分析の結果に基づき具体的に述べよ。

全体としては、残念ながら課題が実際に発生した事件であり、結果が分かっていたこともあるのか、考察の幅が狭いレポートが目立ちました。
また、1-B の問題は、1-A にて検討すべきポイントのヒントを提示しているのですが、リスク分析において、資産価値（機密性、完全性、可用性）、脅威、脆弱性がうまく組み合わされていないレポートも多く、そのようなレポートでは「なんとなく重要な資産」「なんとなく脅威度が高い」「なんとなく脆弱性が高い」「だからセキュリティ対策が必要」、といった流れとなっており、リスク分析としてはほとんど意味のないものとなってしまっています。（おそらく、A 社の経営陣にとっても、「情報資産が重要」で、「セキュリティ対策が必要」なことは言われなくてもわかっていると思われます）

講義でも説明したように、リスク分析の評価値は絶対評価ではなく、相対的にリスクの高い情報資産を洗い出し、企業にとっての優先順位をつけるためのものです。
つまり、どんな基準を評価軸とするかは、A 社独自に検討する必要があります。今回の場合、顧客コンテンツは A 社管理下の情報資産ではあるものの、顧客によって閲覧や編集をする権限があるものであるため、5/17 の講義資料の評価軸をそのまま適用しようとすると、論理的に破綻する可能性があります（ただし実務的解釈は可能）。
例えば、A 社にとって、“CIA”については顧客企業を関連させ、以下のような評価軸を考えた方が、より正しくリスク分析ができると考えられます。

機密性のレベル	判定基準
5	A社のシステム管理者のみが閲覧可能
4	A社のシステム管理者と、当該情報の所有者である顧客企業のみが閲覧可能
3	A社のシステム管理者と、当該情報の所有者が許可設定したその他の者が閲覧可能
2	A社の社員が閲覧可能
1	公開情報

完全性のレベル	判定基準
5	A社のシステム管理者のみが編集可能
4	A社のシステム管理者と、当該情報の所有者である顧客企業のみが編集可能
3	A社のシステム管理者と、当該情報の所有者が許可設定したその他の者が編集可能
2	A社の社員が編集可能
1	誰でも自由に編集可能

可用性のレベル	判定基準
5	1ヶ月のうち停止が許されるのは、3時間（指定されたメンテナンス時間のみ）
4	1ヶ月のうち停止が許されるのは、24時間
3	1ヶ月のうち停止が許されるのは、4日間（概ね週に1日）
2	1ヶ月のうち停止が許されるのは、1週間
1	システム停止条件は特に指定なし

これによって、例えば、以下の４つの情報資産を評価してみます。

	機密性	完全性	可用性	資産価値(仮)
顧客提供用サーバ（HW）	5	5	5	15
サーバ用アプリケーション	5	5	5	15
顧客データ	3	3	5	13
顧客データのバックアップ	5	5	3	13

単純に列挙しただけでは、インフラ部分（サーバ HW＋アプリケーション）が重要な資産に見えます。ただし、A 社がホスティング事業を開始するにあたり、一般的なサーバ管理の環境を整えていたと仮定すると、注目するポイントが変わってきます。

仮に脅威と脆弱性の評価を以下のように仮定します。（脅威は講義資料から若干変更しています）

脅威のレベル			
脅威の発生頻度 / 脅威の影響度	高頻度 年間に数十回以上発生する可能性がある	中頻度 年に数回発生する可能性がある	低頻度 数年に1回発生する可能性がある
影響大 顧客向け業務の大部分が停止する可能性がある	脅威のレベル 高（3）	脅威のレベル 高（3）	脅威のレベル 中（2）
影響中 顧客向け業務の一部が停止する可能性がある	脅威のレベル 高（3）	脅威のレベル 中（2）	脅威のレベル 低（1）
影響小 業務にほとんど影響がない	脅威のレベル 中（2）	脅威のレベル 低（1）	脅威のレベル 低（1）

脆弱性のレベル		
脆弱性のレベル L（1）	脆弱性のレベル M（2）	脆弱性のレベル H（3）
十分なセキュリティ対策が実施されており、問題の発生は考えられない	セキュリティ対策が実施されているが、ある種の攻撃を受けると問題が発生する	セキュリティ対策が未実施のため、問題が発生しやすい

具体的な脅威と脆弱性の組は、それぞれの情報資産ごとに存在します。以下にそれらの組を挙げてみます。
もちろん、思考実験的なところがあり、すべてのリスクをカバーすることはできません。

詳細リスク分析（顧客提供用サーバ（HW））

属性及び重要性	脆弱性	脆弱性 Lv	脅威	脅威 Lv	総合リスク値
機密性 5	機器の不適切な設置場所、入退室管理の不備	L(1)	管理ポートへの直接アクセス	中(2)	10
			機器の盗難	中(2)	10
			盗聴デバイスの設置	中(2)	10
完全性 5	構成管理が厳格でない、作業時の複数名での確認なし	L(1)	部品の無断変更	低(1)	5
			意図しない設定変更	中(2)	10
可用性 5	電源設備が多重化されていない	L(1)	電源の供給停止	中(2)	10
	メンテナンス体制の不備	L(1)	部品故障による動作不可	中(2)	10

詳細リスク分析（サーバ用アプリケーション）

属性及び重要性	脆弱性	脆弱性 Lv	脅威	脅威 Lv	総合リスク値
機密性 5	管理領域アクセス制御の不備	L(1)	管理ファイルの無断閲覧	中(2)	10
	アプリケーションパッチ未適用	M(2)	認証情報の奪取	高(3)	30
	アプリケーションパッチ未適用	M(2)	サーバ内部情報の取得	中(2)	20
完全性 5	管理領域アクセス制御の不備	L(1)	設定ファイルの無断変更	高(3)	15
	アプリケーションパッチ未適用	M(2)	不正アカウントの追加	高(3)	30
	アプリケーションパッチ未適用	M(2)	不正モジュールの設置	高(3)	30
可用性 5	アプリケーションパッチ未適用	M(2)	アプリケーションの不具合	高(3)	30
	容量予測の不備	L(1)	キャパシティオーバー	中(2)	10

詳細リスク分析（顧客データ）

属性及び重要性	脆弱性	脆弱性 Lv	脅威	脅威 Lv	総合リスク値
機密性 3	アクセス管理機能の不備 ※顧客自身の設定ミスは除く	L(1)	非開示ファイルの無断閲覧	高(3)	9
	管理者による誤操作	M(2)	非開示ファイルの無断閲覧	高(3)	18
完全性 3	アクセス管理機能の不備 ※顧客自身の設定ミスは除く	L(1)	コンテンツの不正な改ざん	高(3)	9
	バックアップの不備	L(1)	コンテンツの消失・欠落	高(3)	9
可用性 5	多重化の不備	L(1)	コンテンツの消失・欠落	高(3)	15
	多重化の不備	L(1)	機器の不具合	高(3)	15

詳細リスク分析（顧客データのバックアップ）

属性及び重要性	脆弱性	脆弱性 Lv	脅威	脅威 Lv	総合リスク値
機密性 5	アクセス制御の不備	L(1)	非開示ファイルの無断閲覧	高(3)	15
	管理者による誤操作	M(2)	非開示ファイルの無断閲覧	高(3)	30
	不適切な保管場所	M(2)	非開示ファイルの無断閲覧	高(3)	30
完全性 5	アクセス制御の不備	L(1)	コンテンツの不正な改ざん	高(3)	15
	不適切な保管場所	M(2)	コンテンツの消失・欠落	高(3)	30
可用性 3	リカバリ手順の不備	M(2)	コンテンツの消失・欠落	高(3)	18

これらの結果から、以下のようなリスク分析ができるのではないでしょうか。

- ハードウエアに関しては、データセンター内で厳格に管理されていると想定し、全体として受容可能な低リスク領域である。
- サーバアプリケーションに関連し、アプリケーションパッチの未適用により、サービス提供に大きな影響を及ぼすような脅威が実際に発生する可能性が高い。ただし、アプリケーションパッチの提供されるタイミングは、A 社自体ではコントロールすることが難しい。この場合、「移転」として、サーバ管理の問題に起因した損害を補償する保

険（※注）への加入が検討できる。

- 顧客データ及びバックアップについて、管理者の誤操作による脅威の発生が考えらえる。操作前に、他の作業者と作業内容の確認をするなどの慎重な対応により、リスクの軽減が必要
- バックアップデータについて、不適切な保管場所による脅威の発生が考えらえる。オフライン媒体や、別サーバへの転送によりリスクの軽減が必要。
  また、リカバリ手順は、意外と忘れがちだが、本当にバックアップが必要になったときに問題が発覚することが多く、定期的な訓練等によりリスクの軽減が必要。

残念なことに A 社は、ランサムウエアによってバックアップファイルも含めて利用不可能になってしまいました。
おそらく、事業を始めるにあたっては、インフラ側（サーバハードウエア、アプリケーション）については、それなりの対応を取っていたと思われます。また、顧客データも「バックアップを取る」という対策により、完全性を確保したかのように見えていました。
しかし、日々の運用がうまく回っている限りにおいては、バックアップデータそのものを使う機会もなく、「(バックアップの）不適切な保管場所」という脆弱性が見逃されてしまったのではないかと予想されます。

なお、リスク分析は「1 回実施して終わり」ではないので、自社の情報資産の状況や、世の中のトレンド・技術動向などを見ながら、随時見直ししていくことも必要です。

（※注）ただし、保険が対象とする範囲については、その保険商品の諸条件を確認する必要があります。「保険に入っていれば、身代金を払えたのではないか（＝リスク移転)」という考え方もあるかもしれませんが、例えば 5 億円もの身代金を補償してくれるような保険は残念ながら存在しません。また、ランサムウエアは、身代金の支払いによりデータ復号をしてくれるかどうか、100%の保証はないので、一般的には身代金支払いによる解決は控える方が無難です。

２－B:

- 情報セキュリティインシデントへの対応にあたっては、①準備 ②検知 ③分析 ④封じ込め ⑤根絶 ⑥復旧 ⑦事後対応の 7 フェーズに基づく対応が求められる。
- 2016 年に発生した下記の情報セキュリティインシデントにおいて、上記②～⑦の各フェーズで行われた、または行うべきであった対応を挙げ、対応に先んじて必要となる①準備 を合わせて記述せよ。
- （公式報告）佐賀県：学校教育ネットワークの不正アクセス事案に係る個人情報関連ファイルの

調査結果についてお知らせします
http://www.pref.saga.lg.jp/kiji00349832/index.html

- （参考）piyolog：佐賀県の教育情報システム「SEI-NET」と校内 LAN への不正アクセス事案についてまとめてみた

http://d.hatena.ne.jp/Kango/20160627/1467041904

【評価について】
実際に起きたセキュリティインシデントをもとに考察して頂く課題でしたが、残念ながら優相当の回答はありませんでした。

【回答の傾向】
以下のような回答が多くありました。

・個別の事象に対する個別対応の提示
今回、インシデントについて時系列でまとめられていることもあり、個別事象についての個別対応の積み重ねになっている、結果論的な考察の回答が多く見られました。
インシデント対応の 7 フェーズを前提とした対応検討を求めていましたが、まとめて対策を提示するなど、インシデント対応をフェーズとしてみる観点が少なかったように思われます。

・インシデント対応の事前準備について
起こってしまった事象について、「被害拡大の抑止・事前予防のための準備」に関する考察はされていましたが、「インシデント対応のための準備」といった観点での考察は多くありませんでした。インシデントの発生を防ぐだけでなく、インシデントが発生した際の対応準備について考察が望まれます。

・多層防御の観点が不足
ひとつの事象について、ひとつの対応策のみ提示されているレポートが多く見られました。代替策・補完策や被害低減策といったものについて考慮が不足していると感じます。
実際にインシデントが発生している状況を考慮すると、ひとつの対応策で完全な封じ込めが期待できるとは限らず、また実現可能とも限りません。

・優秀なレポートに見られた共通点
情報資産の重要性を理解した上での準備や対応であったり、インシデント発生時の関係組織との連携も意識しており、そこに「なぜそれをする必要があるか」という自身の考察

も盛り込まれていました。

【講評】

本講義の中では、「攻撃者視点」「多層防御」など、セキュリティの基本的な考え方を解説してきましたが、実際のインシデント事例を前にするとこの考え方を適用する発想に至っておらず、一つ一つの脆弱性や侵害に対する対応策の列挙になってしまっているようです。

例：

パスワードが漏れた　→　全員のパスワードを変更しよう

ファイルが見られた　→　全てのファイルを暗号化しよう

例えば、攻撃者視点からみると、管理者 ID/パスワードを入手したあとは 裏口アカウントを発行する、バックドアプログラムを設置する、などの発想に至ります。こうなると、パスワード変更を実施したとしても封じ込めができない可能性を踏まえ、複数の対応策を適用する多層防御が必要ということになります。

興味深いことに、実際のセキュリティインシデントの現場においても、（セキュリティの知識があるはずの）組織がこのような場当たり的な対応を行っていることが少なくありません。

さらに、「自分がセキュリティインシデントの当事者である」場合に、どのようにすべきか、という点が考察できていれば優秀な回答として評価しています。自分がセキュリティインシデントの当事者として「リスク分析」や「システム・業務の性質」を把握してこそ、セキュリティ対策の優先度を考えた上で実効性を確保できる生きたセキュリティ対策となります。

【考え方の例】

自分が１教員であった場合・・・

「このシステムにはどのような情報が含まれているか」

→ 生徒の住所・氏名・電話番号・成績・評価・家庭環境（漏れたら大変なことに）

「自分のアカウントが盗用されると、被害範囲はどこまで考えられるか」

→ 少なくとも全校生徒　（もしかしたら他校も）

「取りうる対策はなにか」

→ 取り急ぎ自分のパスワードは変えられる。しかし自分の権限ではシステム停止や全

員のパスワード変更はできない。どうすべきか？
「自分のアカウントが盗用されないようにする準備はなにか」
→ 自分のログイン履歴を定期的に確認する
→ 気づいたときの連絡先を確認しておく

このような考え方は、組織としての準備を検討するにも活用できます。

セキュリティに関する技術的な知識が不足していたとしても、これらの基本的な考え方にもとづいた合理的・論理的な状況分析を行うことによりセキュリティ対策の選択肢を用意することができることを意識してください。

その上で、自分がセキュリティ対策の当事者として何を優先すべきか、何が有効かを考える事がセキュリティ対策の要点となります。

３－Ｂ：[Privacy by Design] 仮にロボット法があるなら、人との共生社会について考察せよ。

（背景）ロボット掃除機のような自律的動作から、ペッパー君や Google「Alpha_GO」 のように自ら学習し、自律的選択をする動作をする技術が急進している。 しかし、自律的選択が一人歩きすると、ロボットと人とが共生する社会において、人間社会を破壊する恐れがある。 例えば、アシモフの SF 小説や、手塚治虫の鉄腕アトムで宣言された、「人間への安全性、命令への服従、自己防衛」など、人とロボットが共存（けんかしないで共に生きる）でなく、共生（互いに助け合って生きる）するロボット法が求められている。

（設問） 以下の論点から、想定される影響と、有効と思われる対策を述べよ。

（論点１）人とロボットが共存するために、起こりうるコンプライアンス上の影響と対策案を記載せよ。

（論点２）人とロボットが共生するために、想定されるコンプライアンス上の影響と対策案を記載せよ。

講評結果は、対象 36 人中の内訳は、優が 8%、A が 25%、BB が 14%、B が 52%であった。

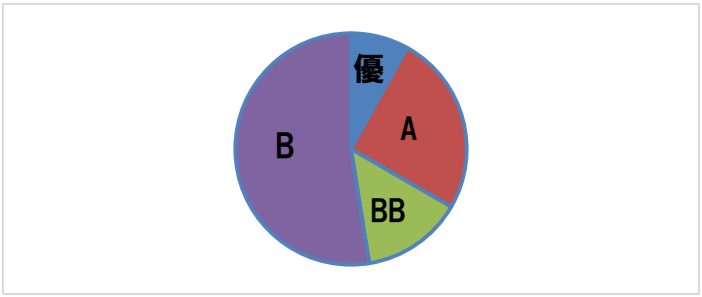
全体講評として、48%のレポートが講評に値すると考えます。優と A の合計 33%は自ら問いを抽出し仮説を明示し大変良いレポートであった。BB 評価の 14%は自ら問いを考察したが結果が同じものも散見された良いレポートであった。残り B 評価の 52%は間違った内容ではないが同様の文面が多く視られ、今後、自ら問いを考察することが望まれるものであった。

① 優を得たレポートは、課題を網羅的に抽出し、その課題解決策として仮説を立て有効性を明示した点が、大変良い評価であったと認識でききた。
② A を得たレポートは、課題を網羅的に抽出したまでは良かったが、その課題解決

策が何故有効かを明示するまでに至らない点があった。

③ BB を得たレポートは、課題を明示した点は良かったが網羅性に欠ける点があり、また、その課題解決策も何故有効かを明示するまでに至っていない点があった。

④ B を得たレポートは、間違いはないが、総じて同じ文面で有り、自ら問いを考察することを期待する。



３B の課題 （Privacy by Design）に望まれるレポート：

例えば、自動運転車が事故を起こした事例が海外で発生したなど、衝突事故の責任を誰が取るのか、所有者の操縦意思を越えたところの事故と所有者の因果関係をどのように示すのか、また海外でスマートスピーカの録音されてしまった殺人現場の音声録音が、現行法での証拠証跡能力の有無なだが仮設されることが望まれた。