2016 年情報セキュリティ基盤論講評

2016/08/29

佐藤周行

1. 全体講評

今回は必答の A 問題と選択の B 問題を出しました。従来は B 問題に相当するものを選択問題の形で出していたのですが、いろいろつまみ食いして覚えると、あまり健全でない形でセキュリティを論じる人が出てきそうな感じだったので、今回は必答問題をもうけました。特に I-A をおろそかにするとすべてにおいてふわふわした議論しかできなくなります。再提出や警告を受けた人は復習しましょう。

A 問題は、リスク分析の用語、セキュリティの防御における境界の設定と、防御方法の組み合わせによる多層防御、IoT の IAM に関する問題になります。

I-A : CIA と脅威、脆弱性の用語と具体例をあげることを求めていますが、具体例をあげることができない人が何人かいました。こちら、再提出に関し、似たような解答があったのですが、まぁ、偶然の一致かもしれませんね。

II-A : 防御方法を複数あげ、その組み合わせとして多層防御を組むことを求めるものでしたが、これも防御方法をあげるだけで組み合わせられない解答が見受けられました。多層防御（Security in Depth）はバズワードですが、実感がないと正しい運用ができません。

III-A: IoT のアイデンティティ＆アクセス管理についての問題です。デバイス数が膨大になることを前提とせよということを問題の中に書いているのですが、それを読み取れない解答がありました。というか、一部に似たような解答があってそれが再提出行きになったりしていました。

学生ということで、セキュリティに関係する分野の最前線にいるわけではないということはわかりますが、せっかく現場にいる方が講師として授業をしてくれているのですから、もう少しがんばれないかな、という感じのレポートが見受けられたことを正直に書いておきたいと思います。

B 問題は、少し調べ物が必要な問題です。調べ物をせずに、自分の直感で書くとあさっての方向の解答を書きかねません。特に I-B は、いろいろ言いたいことがある人もいるとは思いますが、それを抑えて、冷静に問題を解くことが求められます。いろいろ資料を読み込んで解答してきた（参考資料がきちんと refer されていた）ものはいろいろ評価が高いと思います。

I-B：生体情報、位置情報という個人情報の中でよりセンシティブな情報を扱うシナリオでのリスク分析です。話題がホットということで、めくらましにあった人がいました。

II-B: Cyber Kill-Chain を脅威のフレームワークとして考え、セキュリティインシデントの検知にどう適用するかを問う問題です。Kill Chain の各フェーズでの対応を考えることが求められます。

III-B: ICT 環境の中にロボットが入ってきたときに、人間とどう共生するかを考える問題です。ロボットが自律的に行動し、しばしば判断において人間を超えるようになるとき、どのような体制を作っておくべきかということを解答として求めます。自動運転をはじめとして自律型の機械は今後どんどん出てきますから、SF のようで SF でない近未来の検討課題です。

2. 表彰

例年、優秀なレポートを書いてきた人を講評の中で表彰しています。今回は A 問題をきちんと解いたうえで、B 問題についても頑張った

橋爪　崇弘　君
池内　尚史　君

に優秀賞をさしあげたいと思います。役に立つとは思えませんが、控えめにご自慢ください。

3. 個別講評

A 問題

授業のスライドを見たり、参考書を見れば答えがそのまま書いてあるような問題のつもりで出しました。

[I-A]

リスク分析の初歩中の初歩の問題です。情報資産に対して (3) であげた脆弱性と脅威を、資産価値と併せて考えて、リスク値を計算することができます。そこから後はリスク対応ということになりますが、I-B で現代的な問題設定をしているので、それを解いてみてください。授業の最初に言ったと思いますが、リスク対応は「決断して前に進む」ためのビジネス側の視点から論じることが必要です。

解答

(1) 機密性、完全性、可用性

(2) 脅威　脆弱性

(3) （例）認証に弱いパスワード（よく知られているもの、語数の短いもの）を使っていているという脆弱性を持っている場合、脅威としてのリスト攻撃、ブルートフォース攻撃が考えられる。

[II-A]

2-A 講評

2-A、2-B 共通の傾向として、各技術要素については記述されているものの、それらの組み合わせを意識されていない回答が多く見受けられました。[1]

さて、2-A の出題内容は、個別の防御技術を組み合わせることにより、どのような攻撃を防ぐことができるか、というものです。

回答にあたっては、それぞれの技術で防げるものだけでなく、「防げないもの」を意識する、というところがポイントとなります。

考え方の例

ネットワークレベルの防御策（たとえば、ファイアウォール）で防げないものは？

→ 例えば、暗号化された通信

⇒ どのような対策がある？

優秀な回答の多くには、「～されたとしても」という表現が多くみられました。多層防御の概念に通じる考え方だと思います。

2-A 解答例

セキュリティ技術

✧ ファイアウォール （ネットワークレベルでの境界防御）

✧ OS のユーザー権限設定 （メモリ/ファイルシステム）

組み合わせによる防御例

上記技術を適用しているウェブサーバにおいて、外部からの攻撃が行われたシナリオを想定する

1. サービスの停止や総当たり攻撃が目的と思われる外部からの通信について、ファイアウォールで通信を遮断する
2. 公開されているウェブサーバ・ウェブアプリケーションの脆弱性をついて侵入された場合でも、OS のユーザー権限設定により、以下の攻撃を防止する

---

[1]「煙報知器」や「防火扉」について説明できているのに、「火災対策」については説明できていない、という感じでしょうか。

- 管理者など、他ユーザー権限によるプログラム実行
- システムメモリ領域への悪意あるコード混入
- システムファイルの書き換えや、他ユーザーのデータ閲覧

[III-A]

IoT デバイスの IAM について考察せよということですが、問題には背景として「桁違いに多いアイデンティティを取り扱う環境が生まれる」「長期間にわたる様々な認証・認可が要求される」と書いてありますから、それを踏まえた解答をしてほしかったと思います。

	IoT 機器特有の性質	想定される影響 （解答例）	有効と思われる対策 （解答例）
論点1	IoT 機器は、脅威の影響範囲・影響度合いが大きい。	自動運転車へのハッキングは、自車の CAN、信号機システム、対向車の CAN、歩行者情報など繋がる全てから侵入の恐れが高い。	＜主体者の対策＞ 運転者、所有者、自動車メーカ、グローバルな業界標準、行政と国際連携による横断的なセキュリティ対策を行う。
論点2	IoT 機器は、ライフサイクルが長い。	消費者が所有する IoT への攻撃は､マンション IoT60 年、住宅 IoT30 年、自家用車 IoT20 年、家電 IoT10 年の長期間において認証やセキュリティアップデートが行われない恐れがある。	＜設計者の対策＞ 転売、譲渡、修理交換が有っても暗号鍵やセキュリティ・アップデートを継承する仕組みを確立する。同じメーカ以外と繋げられても秘密情報が漏えいしないように対策を行う。
論点3	IoT 機器に対する監視が行き届き難い。	事件事故が発生した際、所有者の機器および所有者本人への監視や事故調査が行えず、責任追及性を失う恐れがある。	＜法や規制による対策＞ 被害発生時の責任の在り方、法規制と罰則の整備、業界検証制度の対応を行う。また機器メーカによる相互監視やログ取集を許容する社会制度を整備する。
論点4	小さく軽い IoT 機器は、機能・性能が限られている。	機器が小さいとセキュリティ機能がインストールされるスペースが無かったり、アップデートを提供する運用者が	＜運用者の対策＞ 機器やネットの脆弱性診断、システム全体の脅威分析､IC チップを含むハードウェアの真正性の検証等に

		維持されなかい危険性がある。	必要なサービスを提供し続ける。またＩｏＴ専用ＧWや多段階ネットレイヤーごとに認証が有る。
論点5	IoT 機器メーカやサービス開発者が想定していなかった接続が行われる。	自動運転車が事故を避ける場合、運転者または歩行者のどちらを保護すべきか、利用者の関与が不在となる恐れがある。	＜利用者の対策＞ フェールセーフへの同意、緊急停止の権限セキュリティ 119 番の設置など、ユーザを巻き込んだ対策を行う。また未使用機器の電源 OFF、手放す時のデータ消去が有る。

B 問題

B 問題は、少し掘って考えてほしい問題を並べていますが、設問の趣旨を理解しきれていない解答が若干みられました。考えるポイントと、一部解答例をあげます。

[I-B]

全体として､情報セキュリティとしてのリスク分析への理解が不足していました｡1A にて、リスク分析に必要な項目を挙げているにもかかわらず、1B においてその内容が活かしきれていないレポートも多く見られました。

基本的には、企業がビジネスを行うのは利益のためであり、決して“個人情報の保護”それ自体を目的としているわけではありません。したがって、企業がセキュリティ対策を行うには、そのサービスにおいて取り扱う情報資産（個人情報とは限らない）にどのくらいの価値があり、その価値を損なう可能性のある脅威や脆弱性がどのくらいあるか、これらを（ある程度）客観的に数値化することにより、実際にコストをかけるべき対策を選択していきます。
そのために、資産価値、脅威、脆弱性を組み合わせて、“リスク値”を算出します。ここで、資産価値は、機密性、完全性、可用性の観点から算出します。これらの数値の算出には、一般的、絶対的基準はありません。自分で定義するか講義資料を引用するなど、何か具体的な基準を作成する必要があるのですが、多くのレポートで「高」「中」「低」等を定義せずに使っており、感覚的になりすぎていました。

情報資産の選び方についても、生体情報、位置情報といった具体的に示されたもの以外にも、スマートフォンのアプリケーション（ソフトウエア）とか、サーバ側の Web アプリケーションやデータベースといったものも出てくるはずなのですが、これらの考察も多くはありませんでした。（折しも、位置情報を活用する「ポケモン Go」では偽物アプリケーションが出回りました）
さらに、リスク分析を実施するにあたっては、企業の観点で行います。一部で「個人情報だから守ってほしい」といった、消費者側の観点で考えているものもありましたが、対策への優先順位は企業が最終的に判断するものです。（実際のところ、個人情報が漏えいしても、賠償しないケースは多数あります）

一方で、脅威と脆弱性の組み合わせについては、多くのレポートにおいて、よく考えているものが見られましたので、これは良い点だったと考えられます。

[II-B]

この設問は外部からの攻撃について、Lockheed Martin 社による Cyber Kill Chain の考え方をあてはめ、攻撃に気づくためにはどのような監視を行うべきか、という設問です。
解答にあたっては、以下を意識する必要があります。

① 攻撃者が各フェーズでどのような行動をするか
② 通常のアクセスと、攻撃者によるアクセスにどんな違いがあるか

このうち、①についてはほとんどの方が正しく理解されているようです。いっぽう、②については「怪しい通信を監視する」といったような解答が多くみられました。
例えば通信を監視するのであれば、“通信量” “通信元” “通信先”などなど、観測（監視）可能な要素を洗い出し、想定される特徴について掘り下げることで、「怪しい」を定義することができ、おのずと監視方法も記述可能となります。

2-B 解答例

以下、Cyber Kill Chain のフェーズごとに解答する

1: Reconnaissance（偵察・予兆）

検知すべき兆候例 公開システムにおけるアクセスの急増 / 普段アクセスされないアクセス元からの通信発生

監視方法 ログ分析ツールにより、公開サーバへのアクセスログを分析（拒否されたアクセスを含む）

検知時の対応策 アクセス元の IP アドレス情報を記録しておき、以後の重点監視対象とするなど
このフェーズでの通信遮断などは正規ユーザーへの影響も考えられるため、積極的な対策は慎重に行う

2: Weaponization（武器化）

（このフェーズの多くは、攻撃者の環境（端末）において行われ監視困難である。以下に、内部に攻撃者が存在していた場合の監視方法を示す）

検知すべき兆候例　内部ユーザーによる、攻撃ツールのダウンロードサイトへのアクセス

監視方法　ファイアウォールやプロキシのアクセスログから、ドメイン名や IP アドレスでの探索

検知時の対応策　攻撃者（ユーザー）および利用端末の特定とネットワーク接続遮断

3: Delivery（配送）

検知すべき兆候例　マルウェアの添付されたメール受信

多数のメールアドレスにおいて同一の添付ファイルを受信[2]

監視方法　メール添付ファイルのウイルススキャン

メールサーバにおける添付ファイル受信記録の分析

検知時の対応策　検知されたメール（ファイル）の隔離とセキュリティベンダーへの検体送付

送信元アドレスの受信拒否

ユーザーへの注意喚起

4: Exploitation（エクスプロイト）

検知すべき兆候例　プログラム実行権限の変更（権限昇格）

プログラム実行エラー（メモリアクセスエラーなど）

監視方法　ホストベース IDS による OS 動作監視

アンチウイルスソフトウェアによるふるまい検知

検知時の対応策　プログラム実行内容とエラーメッセージの調査

システム挙動の継続監視

5: Instllation（インストール）

検知すべき兆候例　システムファイルの書き換え

レジストリの変更

システムユーザー追加

監視方法　ファイアウォール/プロキシログの監視

ホストベース IDS によるファイル/レジストリの変更監視

検知時の対応策　インストール/変更されたファイルの削除

バックアップからの復元

侵入経路の調査

6: Command & Control（遠隔操作）

検知すべき兆候例　クライアントから遠隔操作サーバーとの通信

業務時間外のシステム利用や通信の発生

監視方法　ファイアウォール/プロキシログによる内部→外部通信の監視

検知時の対応策　通信内容の分析

---

[2] マルウェアのばらまきを想定

通信元端末の特定

通信の遮断

7: Actions on Objectives（目的実行）

検知すべき兆候例　内部から外部への大量のデータ通信（アップロード）

外部への攻撃実行（踏み台）

監視方法　ファイアウォールによる外部への通信量の変化を監視

ネットワーク IDS による内部から外部への通信

検知時の対応策　通信の遮断

関連システムやデータなど、被害範囲の調査

ユーザー・顧客・攻撃先への連絡と謝罪

[III-B]

ロボットが「意思をもって」存在し、人間と共存していく世の中にだんだんなっていっていますが、そのときに、機械としてのロボットのコントロールと、人間とかかわりをもつエンティティとしてのコントロールが混在します。そのような状況を考えて、法というか、体制をどう整備すべきかというのが問題です。

	ロボット法・条文	想定される影響 （解答例）	有効と思われる対策 （解答例）
論点1	ロボットは人を傷つけたり殺したりしてはいけない。	人の労働の代替的存在から、感受性を与えられることで、ロボットによる殺傷や支配が起きる恐れがある。	＜他の人権との衝突＞ 事後の措置でなく、問題が発生する前に審議や事件を解決する救済策を提供する。また危害を加えない制限機能がある。
論点2	ロボットはお金だけは作ってはいけない。	3,500 兆円の貨幣経済の流動性の停止し、世界経済が破綻する恐れがある。	＜保護機能のデフォルト設定＞ 社会制度の維持向上の仕組みやプライバシーの保護をロボットにデフォルトで組み込む必要がある。また、道徳・倫理・躾の育成機能がある。
論点3	男が女のロボットに、大人が子供のロボットに、入れ替わってはいけない	愛犬に家族愛や人格を見出し始めている現状において、ロボットが勝手に私生活に関与する恐れがある。未来のイブ	＜一人にしておかれる権利＞ 人間と話すことを許可しても、人間の私生活を尊重し、どう付き合っていけるのか人間側に選択権を与える。また対人安全機能が有る。

論点4	人間が分解したロボットを別のロボットが組み立ててはならない。	危険な感受性を持ったロボットの解体や、暴走したロボットの破壊したにも拘わらず、勝手に再組立てられたっ場合、侵害や事件が再発する恐れがある。	＜プライバシーライフサイクルの保証＞ ロボットのライフサイクル全体に対応する、情報管理を保証する。また緊急電源停止機能多ある。
論点5	ロボットは無断で海外に行ってはいけない。	ロボット兵器を大量に製造する国が、持たざる国に侵略する恐れがある。	＜プライバシー尊重の可視化＞ 国家や社会基盤の継続に影響する行動を可視化し、その理念や目標に対して検証する権限を有する。また、ロボットIDなど個体識別認証の機能が有る。

以上