情報セキュリティ基盤論（２０１４年）全体講評と優秀者の発表

2014/09/05

佐藤周行

今回のレポート課題はどうだったでしょうか。今回のレポートのテーマは（問題１）リスク分析をシナリオを決めてやってみる（問題２）標的型攻撃を解析する。攻撃者のシナリオを考慮したうえで防御側の対応を決める（問題３）ビットコインを社会制度に対するインパクトという観点から解析する、でした。詳細な解析や解答例は、実際に採点を担当した先生に寄せていただいたので、それをこの講評の後半に載せておくことにして、前半では、概略を述べることにします。レポートを出して、再提出等、特にコメントをもらわなかった人は、以下のコメントを参考にして自分のレポートを見直してください。

問題１は、ビジネス環境によってリスク分析の基準や結果が異なることを実感してください、という問題です。この問題の評価ポイントは次のようになります。

１．情報資産を具体的に挙げているか。
２．CIA を評価しているか。
３．脅威脆弱性を評価しているか。
４．オープンソースと非オープンソースで、異なるリスク値を算出しているか。

実は「オープンソース vs.非オープンソース」という文言は、システムソフトウェアの評価軸を設定しやすくするためのサービスです。それよりも、そのシステムソフトウェアがビジネスでどういう位置づけで動いているかを想像することが大切です。Web 上の小売をしているか、基幹業務でスクラッチから業務ソフトを作っているか、基幹業務でアプリケーションソフトウェアを作っているか等、シナリオ設定にはいろいろなバリエーションがあります。まずはそれを一つ固定しましょう（問題を解き終わったら、別のシナリオを設定して解きなおすとよいと思います。結論が多分変わります)。ビジネスのシナリオが決まったら、ビジネスの観点から資産の評価をしましょう。アプリケーションソフトウェア資産よりは、ビジネスに必要な名簿やロジスティクスの情報の方が大切です。ここで、いわゆる「CIA」による点数付けをします。**この「定量的解析」をさぼった人が相当数いました。この解析プロセスはリスク分析の第一歩です。ゆめゆめ忘れることなかれ。**資産とその価値が同定できたら、それに対するセキュリティ上の「脅威と脆弱性」の解析をします。その上でどう対応するか（受容=放置を含め）を決定します。ここまでくるとビジネスの意思決定のプロセスのひとつになることがわかると思います。リスク分析そのものはセキュリティのレベルを上げるものではなく、ビジネス上の意思決定をサポートするものであることを理解してください。

問題２は、標的型攻撃についての問題です。標的型攻撃はたいていの場合ステルスで動

くので、対策の取り方も難しいです。まずは標的型攻撃の最大公約数的な定義をあげておきましょう。

１．　メールや USB メモリ、または特定の Web サイトへの誘導などで、組織のスタッフまたはスタッフが持っている情報端末へマルウェアを仕込む。
２．　マルウェアを働かせることでターゲットとなっている組織の情報を盗む。

１．については、サーバシステムへの攻撃は普通試みられないことに注意してください。サーバシステムへの攻撃は目立つので気づかれやすくなります。視点を変えていうと、攻撃のシナリオが明白でないし、人に対する汎用性もないので、解析が難しいという特徴があります。ということで、評価ポイントは以下の４つになります。

１．標的型攻撃として正しい題材を選択できたか。
２．発表された資料の「語られない」部分を推測して合理的な攻撃シナリオを作ることができたか。
３．入口対策と出口対策として正しいものをあげることができたか。
４．さらに、その対策の実効性を評価できているか。

今回は、１．はクリアできたとして、２．について、合理的なシナリオ作りの時に発表資料をなぞることに終わっているレポートが見当たりました。３．と４．はよくできている人が多かったと思います。人的対策とともに技術的な対策をきちんと講じることが基本です。

なお、事例として PlayStationNetwork をあげている人が相当数いて、きっと Wikepedia を踏んだんですね。PSN のケースはもしかしたら標的型攻撃（が端緒）だったかもしれません。それは可能性としてありだと思うのですが、それなら上の評価ポイント（特に２.）に従って記述することが大切です。なお、模範解答例を採点を行った先生から寄せていただいています（この稿の後半部分)。参考にしてください。

問題３は、ビットコインの評価の問題です。セキュリティの問題というよりは（もちろん Mt. Gox のような重大なインシデントは記憶に新しいところですが)、社会制度に対して、ディジタルのもたらした新技術がどのようなインパクトを持つか、それをどう評価して今後付き合うべきか、という点からのレポートを求めました。ということで、評価ポイントは以下の２つです。

１．　現状の法制度で評価して（日本では）通貨と言えないと判断した根拠を述べている
２．　「通貨」のあるべき姿まで立ち戻って、将来的に通貨として社会制度に組み込まれる可能性があるかを評価する。

１．について言えば、実体があるか、信用はだれが与えているか、有価証券足り得るか、
２．について言えば、たとえば迅速性、安全性、効率性の観点から、ビットコインに用

意されるべき地位があるか、たとえば決済の手段として従来のものより優れているかどうかについて解析がなされていることが必要です。記述が具体的であればなおよし、という感じでしょうか。

ビットコインはそのほかにもセキュリティまたは運用の観点から現在でも脆弱性と脅威の存在が指摘されています。しかし、現状、それら技術的脅威とは無関係に取引所の閉鎖等、強権的な政策で圧力をかけている国もあります。「通貨として有望」で「国家の主権を侵害する」可能性がある、「通貨としては脆弱で」「国の経済に悪影響を与える要因になる」等の理由が正当なのか、新技術に対するよくあるラッダイト運動なのかは今後のビットコインの使われ方が証明することになると思います。

さて、この講義は成績をつけるのが甘いのですが、その代わり、優秀なレポートを書いた人を表彰することで差をつけさせてもらっています。今回は、受講人数が多かったこともあり、以下の５人に差し上げることにしました。

最優秀：杉田　祐樹　君
優秀：　上中谷　健　君
　　小沢真理奈　君
　　黄　　宇陽　君
　　千田　拓矢　君

履歴書に書いてどのくらい効果があるかわかりませんが、控えめにご自慢ください。

詳細講評：問題１

問題１では、企業がシステムを導入する際に、「オープンソース」あるいは「非オープンソース（ベンダー提供製品)」のいずれかを選択するとしたら、情報セキュリティの観点からはどのような評価が可能か？を問うものです。

企業の形態や、情報資産、対象となる製品等を詳細に定義すれば、それだけ詳細に「リスク分析」ができます。(レポート中で、「オープンソース」対「非オープンソース」の比較は意味がない、といった主旨のコメントもありましたが、その通りです。本課題では、本当に比較したいのではなく、比較のプロセスそのものをどう形成するか、を見ています。)

企業における情報セキュリティの観点で、「リスク分析」といったときには、まず３つの要素を検討します。

・情報資産の価値（重要性）
・脅威
・ぜい弱性

です。

今回、ソフトウェアのバグとしての「ぜい弱性」と、企業の情報セキュリティマネジメントの「ぜい弱性」を混同している例が見られました。リスク分析で評価するのは、企業の管理体制にどのような弱点があるか、の「ぜい弱性」です。

また、情報資産の価値は、さらに詳細に、機密性、完全性、可用性の 3 つの要素を数値化することで、大きさを比較します。

企業が、なんらかのアプリケーションを利用するということは、そこに「脅威」が発生します。通常は、外部からの不正な情報取得等を挙げます。

ここまでは、オープンソース・非オープンソース共に同じ評価になることが予想されます。

外部からの不正な情報取得を実施するためには、ソフトウェアのバグ等を利用しますが、これらを防ぐための企業側の管理体制を検討します。

ここで、企業の業態等が影響します。もし、ソフトウェアの開発企業で、ソースコードを精査できるエンジニアが豊富にいる企業であれば、オープンソースであっても未然にバグを見つけて、対抗策を導入できる能力が高い（＝企業としてのぜい弱性が低い）といえるでしょう。

一方で、販売店チェーンの企業が、単純にオンラインショッピングサイトを開設したいだけで、システム開発部門を持たないのであれば、オープンソースをチェックする能力が低く、企業から提供される製品（非オープンソース）のアップデートを適時に導入する方が安全となる可能性が高いと考えることができます。

（これ以外の観点で、別の評価ができる可能性も、もちろんあります）

このような違いを、情報資産を具体的に例示した上で、「リスク値」として評価し、その大きさの差からどちらを選択するかの結論が導出できればよい、ということになります。

問題２：

特定の企業や組織等を標的として、内部へ侵入し、重要システムを狙う標的型攻撃が深刻な問題となっている。攻撃者側は、長期にわたりシステムに侵入し、重要なシステムに対する存在を与えている。

これら標的型攻撃への対策として、既存の対策である「入口対策」に加え、「出口対策」を行う事が有効とされている。

過去に、実際に標的型攻撃により発生したと報告または報道されているセキュリティインシデントを挙げ、以下の視点から論ぜよ。

問１． 報告または報道の内容をもとに、攻撃→被害発生→発見 に至るまでのシナリオを作成せよ。（報告や報道に記載のない部分は合理的な範囲で推定/仮定/想定すること）

実際に日本の公的機関に対して行われ、被害が発生した事例として、2013 年 5 月に報告（最初の報道は 2013 年 1 月）された、農林水産省（以下、農水省）に対するサイバー攻撃（標的型攻撃）を対象としてシナリオを作成する。

なお、基本的な情報については以下に拠るものとし、発表内容を時系列で整理の上、考察した内容を表 1 に示す。

農林水産省： 農林水産省へのサイバー攻撃に関する調査結果（中間報告）の公表について

http://www.maff.go.jp/j/press/kanbo/hisyo/130524_1.html

piyolog： 農林水産省の TPP 情報等の窃取を目的にしたと思われるウィルス感染(サイバー攻撃)事案をまとめてみた

http://d.hatena.ne.jp/Kango/20130107/1357582614

表 1 農水省に対するサイバー攻撃に関するインシデントシナリオ

No.	日付	公表事項	考察・推察
1	2012 年	農水省職員を装った標的型メールによる攻撃が行われている事が内閣官房情報セキュリティセンター(NISC)より報告され、マルウェア感染の調査・対応を行うよう指示される。	当時点ですでに農水省の PC が乗っ取られ、メール送信されていると考えられる。
2	2012 年 2 月～4 月	1 を受け、農水省のネットワークに関するセキュリティ調査①が行われる。	
3	2012 年 3 月	セキュリティ調査①(1 回目)により不審な通信が発見されたが、以下の理由から、「情報流出は発生しなかった」と認識され、調査・対応が行われなかった ・「対策」のみに注力し、詳細な調査を行わなかった ・発見されたデータの一部サンプルを、「不審な通信の全てである」と誤解した。	
4	2012 年 4 月	ネットワークシステム管理運用担当者の全員が部署移動により交代した。	
5	2012 年 5 月	セキュリティ調査①(2 回目)により、マルウェアが検出される。 不審な通信についても調査が行われたが、セキュリティ調査①(1 回目)の誤解および引き継ぎの不備等もあり、通信量が少ないと認識された。 以上の事から、引き続き「情報流出は発生しなかった」と認識された。 なお、ここまでの調査で、本来は制限されている外部媒体の接続や各種 PC の利用ルールについてユーザーへの周知・遵守がされていない事が確認されている。	マルウェアだけでなく、ユーザーのルール遵守に関する問題への対応が行われなかったため、外部媒体経由でのマルウェアの拡散・被害拡大が発生している可能性がある。(自宅 PC 等が感染していた場合、2014 年現在も対応されないままとなっている可能性がある)
6	2013/1/1～	農水省に対しサイバー攻撃が行われ、2011 年 10 月から 2012 年 4 月に作成された内部文書が漏えいしていた恐れがあると読売新聞により報道される。 含まれるデータ： 2011 年 11 月の APEC 首脳会議関連情報：	読売新聞の取材ソースは明らかにされていないが、その後の推移をみても、ほぼこの報道通りであったと考えられる。

		TPP 関連事項 等 2012 年 4 月の日米首脳会談関連情報：TPP 関連事項、要人の行動予定 等 ● 内部文書データは各 PC から別の PC に集約されていた ● データが集約されていた PC は外部サーバと繰り返し通信していた ● 外部サーバは何者かが操作を行っていた ● [1]財務省や RSA における問題発生時にも使用された HTran と呼ばれる通信ツールが利用されていた[2][3] ● 「TPP」等のキーワードでデータ検索されていた	公表された（確定している）情報漏えいは 2012 年 1 月以降となっているが、それ以前から恒常的に不正な通信が行われていたと考えるのが妥当。 関連事象として、同ツール(HTran)を使用した財務省への不正アクセスの場合、2012 年 11 月までの「2 年間」にわたり感染していた事が判明している。[4]
7	2013/1/4	農水省責任者は、情報流出の有無を確認するため、セキュリティ調査①の対象とならなかった PC も含め、セキュリティ調査②の実施を指示した。 セキュリティ調査②の結果、セキュリティ調査①の対象とならなかった PC から、少なくとも 1 件の不審な通信が発見された。 しかし、指示を受けた農水省担当者は、確認対象を「セキュリティ調査①の対象となっていた PC」と限定して解釈し、発見された不審な通信について責任者に報告を行わなかった。	常識的に考えれば、本来調査対象外であったとしても、不審な通信が発見されれば即時報告されるべきである。
8	2013/1/7	7 を受け、農水省責任者は報道機関に対し、情報流出の可能性は低いと回答。	
9	2013/1/7	8 の報道対応後、実際には不審な通信が行われた事が（担当者と別の作業実施部署から）責任者に説明される。	作業実施部署も、問題発生をこの時点まで報告していない。

[1] 財務省：財務省におけるウイルス感染事案について
http://www.mof.go.jp/about_mof/other/other/press_20120720.html
[2] 日経新聞：財務省の情報流出、ＰＣ123 台で確認　ウイルス感染
http://www.nikkei.com/article/DGXNASFL200DS_Q2A720C1000000/
[3] Chinese HTran Root To RSA Hack Revealed By Dell
http://www.techweekeurope.co.uk/news/chinese-htran-root-to-rsa-hack-revealed-by-dell-36043
[4] 財務省にサイバー攻撃、パソコン 123 台が感染
http://itpro.nikkeibp.co.jp/article/NEWS/20120720/410429/

10	2013/1/8	農水大臣は報道内容を肯定する会見を行い、詳細なセキュリティ調査③を行うと発表。	
11	2013 年 1 月～	報道されたインシデントに関し、2010 年 12 月 31 日以降の状況に関するセキュリティ調査③が行われる。調査対象は以下の通り。 ● PC 103 台(全 PC 約 5,500 台より選定) ● 関係者 50 人 ● PC を使用していたユーザー 283 人	調査対象は報道までの 2 年のみ、かつ通信の記録に欠落があると報告されていることから、実際の被害はより大きいものである可能性がある。
12	2013/5/24	調査により、インシデントの発生とその被害状況が公表された。 公表された被害は以下の通り。 ● 39 台の PC による不審な通信が行われた ● 2012 年 1 月～4 月に、5 台の PC から個人情報・業務情報を含む 124 文書が流出	

問 2. システムへの侵入に利用された経路と、攻撃者がその経路を選択した理由（得られたメリット）を考察せよ。

調査報告および報道からはシステムへの侵入経路や侵入時期について確認されていないが、標的型メール攻撃によるものと推定される。この推定の補強材料として、以下の点が挙げられる。

1. 農水省職員を騙った標的型メールが確認されている(問 1 回答 No.1 部分)
2. 農水省に対しては、以前にも同様の標的型メール攻撃が行われており、その際には少なくとも 1 台で被害が発生している

   農林水産省における標的型メール事案について

   http://www.maff.go.jp/j/press/kanbo/hyoka/120202.html

システムへの侵入経路としてメールを利用することには、攻撃者にとって以下のようなメリットがある。

1. 標的とするユーザーや組織や端末を特定・限定しやすい

   マルウェアを添付したメールは、「送信先メールアドレス」にしか到達しない。これは、発見を遅らせる上で大きなメリットである。この事案においても、「農水省あて」ではなく、「農水省から」不審なメールがあったとの報告が発見の起点である。
2. 標的とするユーザー・システム・ネットワークに届く確率が高い

   通常、メールアドレスは実際に存在するユーザー・端末に関連づけられており、メールアドレスを選定すれば、送信した内容が誰にもアクセスされないという可能性は比較的低いと考えられる。特に当事案のように、官公庁であれば、使われていないメールアドレス（いわゆる死にアカウント）は非常に少ないと言ってよい。
3. プログラムが実行される可能性が高い

   メリット 2 とも関連するが、メールの文面や添付ファイルの形態により、ユーザー自身にマルウェアを展開させる事ができる可能性が高い。今回の場合、TPP には複数の省庁や外部機関が関係することから、職員は外部からのメールを一律に無視する事が出来るとは考え難く、メール添付ファイルを開く、リンク先 Web ページを確認する、等の操作を行う事になる。

問 3. 発生した被害を低減、もしくは回避できたと考えられる対策手法案を、入口対策、出口対策のそれぞれ１つ以上挙げ、期待できる効果とその理由を述べよ。

入口対策について：

問 2 の回答に記載した通り、調査報告および報道からはシステムへの侵入経路は明らかになっていないため、標的型メールによるマルウェア感染であるものとして、対策例を２つ挙げる。

対策１： クライアント PC のソフトウェアアップデート

通常、標的型攻撃はメールの添付ファイルや、HTML ベースでのメール、Web へのリンク等を通じ、PC の脆弱性を利用してマルウェアを送りこもうとする。

今回の場合、対象はプログラマーやシステム管理者ではなく、特殊なプログラムが実行可能である可能性は低いことから、使用された脆弱性は一般的なソフトウェアに存在していたものであり、これらソフトウェアのアップデートにより多くの攻撃が防止できた可能性が高い。

以下に、アップデート対象とするソフトウェアの典型例を例示する。

- Windows および Internet Explorer
- Office ソフトウェア（MS Office）
- Adobe Acrobat / Adobe Reader
- Flash
- Java 実行環境
- アーカイバソフト(データ圧縮/展開ソフト)

対策２： S/MIME によるメール署名および暗号化

問 2 の回答 3 に示したように、標的型メールによる攻撃の防止が難しい理由の１つとして、受信したメールの正当性を確認することが難しいという事が挙げられる。

S/MIME によるメールの電子署名と暗号化は、メール送信元およびメール内容の正当性をある程度保証することができる。(送信元端末が乗っ取られ、署名用パスワードまで漏えいしているような場合は例外)

これにより、例えば署名されていないメールについてはリンクを開かない、添付ファイルは別途セキュリティ担当者の管理下で確認するといった対応を行う事により、メール経由でのマルウェア侵入のリスクを低減できるものと考えられる。

出口対策について

問 1 に記載の通り、当事例は多くの要因が関連したことにより、「侵入後の発見の遅れ」と、「発見後の対応の遅れ」が複合している。このそれぞれについて対策を 1 つずつ挙げる。

対策１： 恒常的な通信の分析監視

今回の問題に関する調査は、農水省自身ではなく、内閣官房情報セキュリティセンター(NISC)からの指摘や報道がきっかけとなっており、また行われている調査も、問題が確認されてから「都度」行われている。そのため、農水省は被害が顕在化しない限り攻撃に気づかない状態にあったといえる。

これに対応するためには、メール・Web を含む外部および内部への通信を監視し、マルウェアによって行われるような不審な通信を発見できる状態を常に保つ事が有効と考えられる。たとえば、以下のような製品によるネットワークの監視やフィルタリングである。

- IDS/IPS：ネットワークを通る各種通信の監視
- SIEM：IDS/IPS ほか ファイアウォール、各種サーバ、ネットワーク機器のログの統合監視)
- Web コンテンツフィルタリング：アクセス先 Web ページの監視

対策２：インシデントの報告・対応体制の整備

当インシデントは、少なくとも 3 回は対応の機会を逃したものと考察される。具体的には、問 1 の回答に記述の下記タイミングである。

- No.3 2012 年 3 月
- No.5 2012 年 5 月
- No.7 2013 年 1 月

これらはいずれも「不審な通信」を確認しながらも連絡・報告の不備により十分な対応に至らなかったものであり、対策 1 を取ったとしても、これが改善されないままであれば発見された問題への対応の遅れと被害拡大が予想される。農水省の報告でも、同様の指摘がなされており、以下の改善案を提示している。(以下報告書より抜粋)

① 危機意識を持って業務に取り組むよう、一連の対応の具体的な問題点を全職員に周知
② サイバー攻撃がさらに多様化・巧妙化することを前提としたシステム・ネットワークの構築
③ セキュリティとシステムの担当の連絡・相談の円滑化、幹部への迅速な報告を可能とする体制の整備
④ 専門家への相談・報告のルール化など、外部専門家の更なる活用
⑤ セキュリティ・システム業務に十分な知識・経験等を有する人材の育成・確保
⑥ 職員によるＰＣの不適切利用の禁止をシステム面でも担保、ＰＣ利用ルールに係る十分な指導の実施
⑦ 全職員への研修及び攻撃訓練の継続によるセキュリティ意識の定着
⑧ ＣＳＩＲＴの活用による担当職員の知見の蓄積、意識の向上とインシデント対応能力の向上

しかい、問 1 回答 No.4 にあるような大規模な人事異動が定期的に発生する組織環境において、ユーザーの教育も含め、上記に抜粋したような継続的な体制の維持整備を自組織単独で行うのは非常に難しいと考えられる。この組織体制において有効な対策を行うためには、上記⑧に記載の外部機関の活用をさらに広げ、セキュリティ組織への権限の委譲（場合によってはネットワークの停止権限等も含む）が必要と考える。

レポート３　ｅコンプライアンスについて
問題①　日本の通貨制度から通貨と呼べない依拠を挙げて、違法性を考察せよ

以下の課題について 1 つ以上調査し、分析できた事実から評価を交えた意見を断定的に記載されていることが望ましい。複数課題に考察が有る場合は、より良いレポート評価ができる。

Ａ．実物通貨でないと課題認識した
Ｂ．銀行行為でないと課題認識した
Ｃ．有価証券でないと課題認識した

Ａ．実物通貨でないと課題認識した場合、「通貨の単位および貨幣の発行等に関する法律（通貨法）」や「日本銀行法」などから実物通貨か否かを考察している。また、各国政府造幣局・中央銀行などの信頼貨幣か否かを考察している。
Ｂ．銀行行為でないと課題認識した場合、「日本銀行法」や「紙幣類証券取締法などの法律」などから造幣局が発行した硬貨と日銀が発行した紙幣の通貨発行権の有効性を考察している。
Ｃ．有価証券でないと課題認識した場合、「金融商品取引法」や「紙幣類証券取締法などの法律」などから財産的価値や支払手段として銀行や証券会社が売買の仲介などの本業で取り扱う事が可能か否かを考察している。

問題②　米 FRB 議長などの理解から将来期待される点を挙げて、有効性を考察せよ

以下の課題について 1 つ以上調査し、分析できた事実から評価を交えた意見を断定的に記載されていることが望ましい。複数課題に考察が有る場合は、より良いレポート評価ができる。

Ａ．迅速性があると課題認識した
Ｂ．安全性があると課題認識した
Ｃ．効率性があると課題認識した

Ａ．迅速性があると課題認識した場合、国際決済やグローバルな証券取引ルール（例えば、海底・光ケーブルの遅延も含め各国の証券取引上において 3 秒以内であれば同時取引とみなすルールを考察する）などから「迅速性」が確保できるか否かを考察している。かつ、信頼されている「交換の手段」があるか否かを考察している。
Ｂ．安全性があると課題認識した場合、国家財政の危機や政府転覆および第三国間取引など

「安全性」が確保できるか否かを考察している。かつ、信頼されている「偽造難易度」や国籍を持たない「価値尺度」があるか否かを考察している。
C．効率性があると課題認識した場合、実物通貨に比べ、「効率性」が確保できるか否かを考察している。かつ、信頼されている「価値保存」があるか否かを考察している。