

平成30年度「専修学校による地域産業中核的人材養成事業」

情報セキュリティの Society5.0対応実態調査報告書



Society5.0に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

平成 30 年度「専修学校による地域産業中核的人材養成事業」

情報セキュリティの Society5.0 対応実態調査報告書

Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

目次

目次.....	3
実施概要.....	5
ヒアリング内容.....	7
質問と各社の回答.....	9
1 情報セキュリティに対する脅威について.....	9
1.1 背景.....	9
1.2 ヒアリング内容.....	10
1.3 回答.....	11
1.4 結論.....	12
2 IoT 機器のネットワーク接続による新たな脅威について.....	14
2.1 背景.....	14
2.2 ヒアリング内容.....	14
2.3 回答.....	15
2.4 結論.....	18
3 今後の情報セキュリティの観点からのシステム設計と開発について.....	19
3.1 背景.....	19
3.2 ヒアリング内容.....	19
3.3 回答.....	19
3.4 結論.....	20
4 サイバー攻撃の最新の動向について.....	21
4.1 背景.....	21
4.2 ヒアリング内容.....	21
4.3 回答.....	22
4.4 結論.....	23
5 カリキュラムの順位づけについて.....	24
5.1 前提.....	24
5.2 ヒアリング内容.....	25
5.3 回答.....	25
5.4 結論.....	26
全体の考察と結論.....	27
文献目録.....	28
付録「ヒアリングシート」.....	29

実施概要

本調査は、平成 30 年度「専修学校による地域産業中核的人材養成事業」における情報セキュリティの Society 5.0 対応実態調査である。本調査の目的は大きく分けて二つある。一つは今後、増加する情報リスクに対するセキュリティ対策技術の現状と将来的な予想及び Society5.0 で予測される情報リスクへの対応と技術の進展の情報を収集し、教育プログラムに反映すること、もう一つはセキュアな情報システム設計・開発技術を明らかにし、教育教材開発に活用することである。調査は情報セキュリティ専門企業 2 社（株式会社ディアイティ様、株式会社ラック様）に対して、ヒアリング方式で実施された。ヒアリングした内容は、情報セキュリティの脅威と対応技術(既知の対策)、情報セキュリティインシデント発生時の対応と必要技術、情報セキュリティの観点からのシステム設計・開発技術、情報セキュリティ人材の業務領域・システム開発への関与状況と必要技術等である。

対象：情報セキュリティ専門企業

調査手法： 訪問によるヒアリング （2 社）

1. 株式会社ディアイティ

セキュリティサービス事業部 事業部長 山田英史 氏

実施日：平成 30 年 12 月 18 日（火）14 時～15 時 30 分（90 分間）

2. 株式会社ラック

サイバーセキュリティ本部 理事 長谷川 長一 氏

実施日：平成 30 年 12 月 27 日（木）10 時～11 時 30 分（90 分間）

調査項目： 情報セキュリティに対する脅威、IoT 機器のネットワーク接続による新たな脅威、今後の情報セキュリティ技術、情報セキュリティの観点からのシステム設計・開発、サイバー攻撃における新技術動向と対応

※ヒアリングシートについては、本報告書の末尾に添付する。

分析内容： 情報セキュリティの脅威と対応技術（既知の対策）の明らかにする。情報セキュリティインシデント発生時の対応と必要技術、情報セキュリティの観点からのシステム設計・開発技術を明らかにし、情報セキュリティ人材の業務領域・システム開発への関与状況とともに必要技術を分析する。

成果の活用： 教育カリキュラム、科目・シラバスへの反映、教育教材・演習教材の内容に反映、教員育成研修プログラムに反映をそれぞれ検討する。

ヒアリング内容

Q1. 情報セキュリティに対する脅威についてお伺いします。

Q1.1 上記項目の中で、もしくはこれ以外で、セキュリティを考慮する必要のある開発者（以下開発者）が特に詳細まで知っておいた方がいいと考えることは何ですか。

Q1.2 上記項目の中で、もしくはこれ以外で、開発者が忘れがち、ミスをしがち、軽視しがちなものは何ですか。

Q2. IoT 機器のネットワーク接続による新たな脅威についてお伺いします。

Q2.1 IoT デバイスのセキュリティ対策は非常に多岐にわたっており、今後もその種類は増えていく中で、開発者はどのように知識を收拾すれば良いと考えますか。

Q2.2 今後（もしくは現在）情報セキュリティ専門企業として、こういった対策をお考えですか（とられていますか）。

Q2.3 IoT デバイスの新たな脅威において特に重要と考えるトピックは何ですか。

Q3. 今後の情報セキュリティ技術/情報セキュリティの観点からのシステム設計・開発についてお伺いします。

Q3.1 今後システム設計や開発において、意識するセキュリティはどう変化していくか、またどう変化していくべきだと考えますか。何が基本的なものとして残り、何が新しく出てくることが考えられますか。

Q4. サイバー攻撃における新技術動向と対応についてお伺いします。

Q4.1 開発者が所属する企業にとって、重要なサイバー攻撃における新技術動向と対応策を知るために、開発者はどのように情報收拾するべきだと考えますか。（上記のサイト表 1 で特に追うべき重要なサイトはどれですか。）

Q4.2 最近のサイバー技術動向で、特に重要と考えるトピックは何ですか。

Q5. カリキュラムにある項目（別紙参照）の順位づけについてお伺いします。

Q5.1 これらの中で特に重要なものは何だと考えますか。
足りないものや不要なものがありますか。もしありましたら、具体的に教えてください。

質問と各社の回答

本調査では、情報セキュリティ専門企業として、株式会社ディアイティ様（以下D社）、株式会社ラック様（以下L社）の2社の担当者からヒアリングを行なった。この章ではそのヒアリング項目と各社の回答の要約について記述する。

1 情報セキュリティに対する脅威について

1.1 背景

情報セキュリティに対する脅威については、既存の標準的な指標について、独立行政法人 情報処理推進機構（以下IPA）から毎年出版されている『情報セキュリティ 10 大脅威』[1]がある。各年に発生した、情報セキュリティにおける事案の中で、比較的社会的に影響の大きかったものを約100名の有識者らの議論と投票によって決め、それを発表しているものである。専修学校の学生らのカリキュラムを整えるにあたって、これらの情報が基本となると考え、この資料をベースとしてヒアリングを行った。

表 1. 情報セキュリティ 10 大脅威 2018 [1]

順位	組織	昨年順位
1 位	標的型攻撃による被害	1 位
2 位	ランサムウェアによる被害	2 位
3 位	ビジネスメール詐欺による被害	ランク外
4 位	脆弱性対策情報の公開に伴う悪用増加	ランク外
5 位	脅威に対応するためのセキュリティ人材の不足	ランク外
6 位	ウェブサービスからの個人情報の窃取	3 位
7 位	IoT 機器の脆弱性の顕在化	8 位
8 位	内部不正による情報漏えい	5 位
9 位	サービス妨害攻撃によるサービスの停止	4 位
10 位	犯罪のビジネス（アンダーグラウンドサービス）	9 位

1.2 ヒアリング内容

表1における『情報セキュリティ 10 大脅威 2018』を元に、この中、あるいはこの他にもセキュリティ専門企業として、専修学校の学生が特に知っておいた方が良い、学んでおくべきと考えられることは何か、また、開発者が忘れがち、ミスをしがち、軽視しがちなことは何かについて、ヒアリングを行った。

1.3 回答

1.3.1 D 社の回答

世の中の参考資料（リファレンス）は知っておくことが望まれる。

1 位 標的型攻撃による被害

IPA 『「高度標的型攻撃」対策に向けたシステム設計ガイド』

<https://www.ipa.go.jp/files/000046236.pdf>

6 位 ウェブサービスからの個人情報の窃取

IPA 『安全なウェブサイトの作り方』

<https://www.ipa.go.jp/files/000017316.pdf>

8 位 内部不正による情報漏えい

IPA 『組織における内部不正防止ガイドライン』

<https://www.ipa.go.jp/files/000057060.pdf>

攻撃のパターンとしては外部からの攻撃と内部からの攻撃がある。外部からの攻撃としては「標的型攻撃」、内部からの攻撃は「内部不正」として挙げている。また、やはりウェブサイトへの攻撃が普遍的に非常に多いため、「ウェブサービスからの個人情報の窃取」を挙げている。

トレンドとしては、ランサムウェアやビジネスメール詐欺といった情報を奪うのではなく、お金をとるような攻撃が起きている。情報を奪うのは多くの場合は企業に対して行われるが、お金は誰からでもとれるため、個人がターゲットになる。

学生が常にトレンドを追うのは難しいかもしれないが、そういうものがあるということは伝えた方が良い。

「開発者のミス」について、開発者の種類によって発生するミスが変わってくる。

専門学校の学生はプログラマーとして就職することが多い。

プログラマーがセキュリティ上の判断をする機会は少ない、仕様が正しく読めることが重要。

学生自身の開発者としてのキャリアの方向性で求められるものは変わってくる。

1.3.2 L 社の回答

10 大脅威は 100 人の産官学の人間によって投票で決まっているため、これはインパクトの大きいものが選ばれているだけであり、社会への影響を表したものではない。たとえば、SQL インジェクションは 10 大脅威が発表され始めた 2006 年にはあるが、今は出ていない。しかし、実際に世の中で起きる脅威としては依然存在しており、重要な脅威である。

また、10 大脅威で注目されているのは「結果」であり、その「原因」を考えることが重要。なぜ攻撃されたのかを考える。

10 大脅威というよりももっと基本となるものをちゃんと学んでおくべきである。

上位にあるから自分が知らなくてもいいわけではない。自分が開発するアプリや言語において、脆弱性の原因になる要素を学ぶべきであり、それは忘れがちなところである。

同じ IPA からの資料として『セキュア・プログラミング講座』が発表されている [2]。その内容やチェックリストを確認し、結びつけて押さえておく必要がある。

1.4 結論

10 大脅威 2018 のなかでは「標的型攻撃」「ウェブサービスからの個人情報窃取」「内部不正」という脅威が D 社からあげられたが、L 社のいうように、これは実際に重要なものを反映しているというよりは、その年に話題になった結果に注目したものである。

その上で気にするべきは基本となるようなガイドライン（例えば、『セキュア・プログラミング講座』[2]や『安全なウェブサイトの作り方』『組織における内部不正防止ガイドライン』『組織における内部不正防止ガイドライン』）を読み込み、脆弱性という「原因」と結果を結びつけて考えられるようになることであると言える。

2 IoT 機器のネットワーク接続による新たな脅威について

2.1 背景

IoT 機器における脅威についても 1.1 と同様に、IPA から『IoT 開発におけるセキュリティ設計の手引き』[3]が出版されている。昨今注目を浴びている IoT について、IPA が 2006 から続けてきた組み込み機器のセキュリティの調査を元に、それらの機器やサービスがネットワークに繋がることで生じる様々な脅威や、それらを原因とするリスクや被害を予防するために、必要な情報を記載したものである。その手引きにおいて、IoT の構成要素を「サービス提供サーバ・クラウド」「中継機器」「システム」「デバイス」「直接相互通信するデバイス」の 5 つに分類して定義している（図 1）。

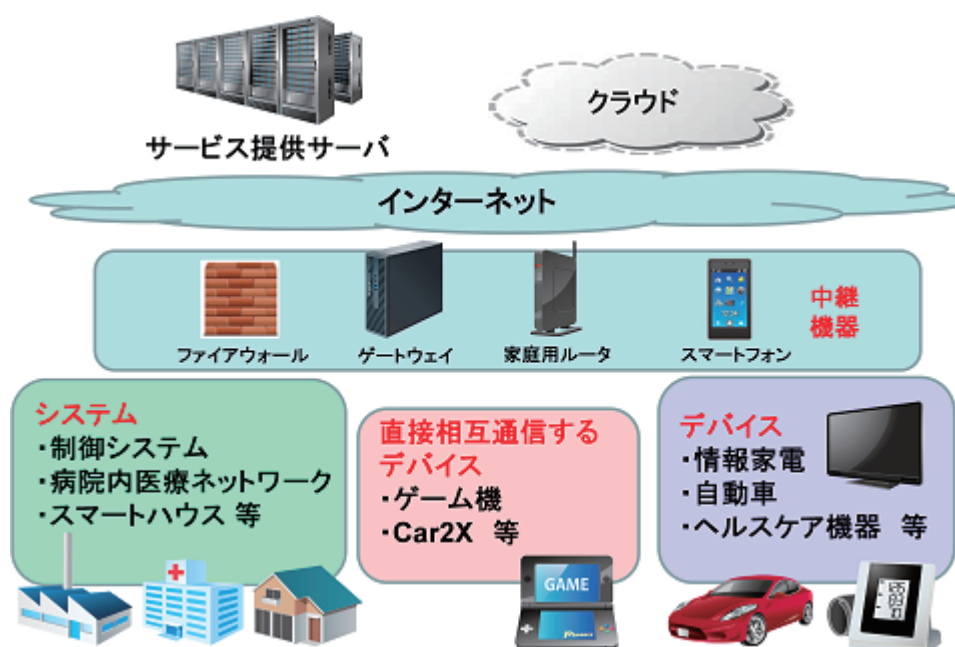


図 1 . IoT の全体像 [3]

2.2 ヒアリング内容

図 1 に示されるように、IoT には様々な形態の機器が含まれており、デバイスごとに求められるセキュリティの知識は変わってくるため、IoT のセキュリティ対策は非常に多岐にわたるといっても過言ではない。そのような知識の更新が頻繁かつ広範囲に求められる状況で、開発者はいかにして知識を収集すべきなのか、現在どのような取り組みをおこなっているのか、特に重要なトピックはなににかについてなどをヒアリングを行った。

2.3 回答

2.3.1 D 社の回答

「センサー」「アクチュエーター(制動部)」等、現実世界とサイバー世界が接する部分のリスクとその対策。コネクティッドカー、スマートビルディング、医療デバイス等利用分野によりリスクも対策も異なり、それぞれに専門性を要求される。各分野でのガイドラインの理解が求められる。

(例)自動車部品メーカーに関連するカイトライン

ドイツ自動車産業のセキュリティカイトライン TISAX

・ Volkswagen 社等のドイツメーカと取引する際に TISAX 準拠が求められる

・ サプライチェーンのセキュリティ統制の一環

IoT に共通するのはセンサーと制動部があり、それがインターネットで制御されたり、センサーの情報を吸い上げたりするところ。

今までと変わらず、ネットワーク上でのセキュリティが大事。

ハードウェアレベルでのセキュリティまで統一的にカバーしてるものは今はないと認識している。ただ、各分野でガイドラインが出ていることがあるので、それがあればそういうものを使う。そのようなガイドラインが出ていることがあるということを学生には伝えておくといい。

日本でも経済産業省がざっくりとした大きなフレームワークとして

「サイバー・フィジカル・セキュリティ対策フレームワーク」の作成を進めている。

会社としての取り組みについて、IoT のセキュリティに直接携わる業務を行っていないか、最新動向を知る機会として「一般社団法人スマートフォンセキュリティ協議会」や「経済産業省産業サイバーセキュリティ研究会」等に参加している。

最新の情報を手にいれる上で、スマートフォンセキュリティ協議会等の協議会に参加するという方法もある。学生でも参加できるものもあるし、参加できなくても情報は公開されている。

IoT の新たな脅威については、現実世界とサイバー空間が接することによって、サイバー空間のリスクが現実世界に影響を与え、現実世界のリスクがサイバー空間へ影響を与えること。

IoT では、セキュリティ機能は部品に組み込まれるケースが多く、実装に失敗しても修正が難しい。したがって、部品調達から始まり製品製造、サービス開発までのサプライチェーン全体のセキュリティ品質が保証されなければ、IoT 機器やそれを使ったサービスのセキュリティが担保できない。運用面の脅威では、制動部への攻撃、フレイハジィの問題がある。

いままでサプライチェーンの品質管理はしっかり行ってきたが、その品質管理にセキュリティ要件が含まれるようになる。

2.3.2 L 社の回答

IoT の開発をする上で、デバイス（ハードウェア）の特性の知識は重要である。

今一番狙われているのは防犯カメラや、複合機、家庭にあるルータなど。

サイバーフィジカルシステム（ビルや駐車場の管理システムなど）もある。

PC やスマホのライフサイクルは 2,3 年であるが、IoT のライフサイクルは数十年になることがある。家電は 6,7 年くらい、車なら 10 年、ビルの管理システムなどは 40 年くらいになる。それを意識して開発をしなければいけない。

また、家庭用 IoT システムであれば TCP で通信を行なっているため、普通にウェブのセキュリティと同様に暗号化されるが、サイバーフィ

ジカルシステムなどは独自のプロトコル、独自の OS を用いており、暗号化もされていないことがある。

また、IoT 機器であるのに、アップデートが難しい仕様になっていることがある。たとえば、ある掃除機ではアップデートの際に蓋をあけて PC からダウンロードしてきたアップデートパッチを USB 経由で適用する必要がある。多くの人にはできないし、やらない。そのような特性を知ることと、設計をする際にそういったところを気にして欲しい。

PC やスマホ、タブレットの考えをそのまま当てはめていってはいけない。

IoT のセキュリティの学び方は、ハードウェアの開発を知っている人と、ソフトウェアの開発を知っている人それぞれで学び方は変わってくる。

今回対象となるような専修学校の学生であれば、どちらかというソフトウェアの開発側かと思う。高専等ではハードウェア側も知っていることが多いため、学び方を変えるべき。

情報系の学生が IoT 機器のセキュリティを学ぶうえでは、まずはハードウェア側の特性を知るための勉強が必要である。

昔はゲートウェイセキュリティといって、持ち出しされることを想定しておらず、建物の出入りのセキュリティを高めることがセキュリティの基本であった。いまは持ち出されることもある。

また、情報システムの管理は情報システム部が行っており、それなりに知識のある人が行っているが、IoT 機器の管理は総務が行っている。総務は基本的に知識のあるとは限らない、普通の人であり、そういった人たちでも扱えるような設計をしていく必要がある。

PC やスマホであれば、問い合わせ先が存在するが、IoT 機器や組み込み系デバイスであれば問い合わせ先が存在しないことがある。問題が

起きた時に脆弱性ポータルサイトに対応策が載るが、IoT 機器や組み込み系は海外の信頼できないベンダーなどもあり、そういったところの脆弱性は載らないことも多い。

調達する際に機器選定をしっかりとする必要がある。

その機器が持っている機能が狙われる。カメラであれば映像を見たいという動機から狙われる。

2.4 結論

IoT 機器に関しては PC やスマホデバイスでのセキュリティとはある程度分けて考える必要がある。D 社のいうように、ネットワークの部分は共通することもあるが、L 社のいうように、サイバーフィジカルシステムなどは通信プロトコルに独自の暗号化されていない通信プロトコルを持っていることがあるため、注意が必要である。また、IoT のセキュリティ対策は特に、デバイスの特性を知らなければいけない。IoT の開発に関わる上では、ソフトウェア側の知識だけでなく、実際に関わるハードウェア側について詳しくなるための基礎的な勉強を行っておく必要がある。

新たな情報の収集元としては研究会や協議会に参加するということが考えられる。学生の参加を受け付けていることもあり、可能であればそういったものをカリキュラムに組み込むことを検討する価値がある。

トピックとしては、家電やサイバーフィジカルシステム、車などが挙げられた。それぞれに対して、異なった学習が必要であり、共通して学ぶことは難しいが、それぞれ学ぶ参考になるガイドラインや研究会があるため、実際に必要になった時にアクセスできるように、そのリファレンスを学ぶことは重要であると考えられる。

3 今後の情報セキュリティの観点からのシステム設計と開発について

3.1 背景

情報セキュリティの脅威は常に変化し続けている。例えば、2 節に書かれたように、IoT 機器は非常に多岐にわたり、デバイスごとに新しい情報セキュリティ上の脅威が考えられる。そのように変化の激しい分野において、求められるのはいかに知識を更新するか、また、その中でも普遍的なものは何かについてである。

3.2 ヒアリング内容

前節で説明したように、変化の激しい分野において、専修学校の学生が知っておくべきことは何かをヒアリングを行った。具体的には「どのように変化していくか」や、「どう変化していくべきか」、新しい技術が生まれてくるなかで、基本として残るものはなにか、これからはどんな知識が新しく要求されるようになるのかについて、ヒアリングを行った。

3.3 回答

3.3.1 D 社の回答

開発プロセスの各段階におけるセキュリティ評価は基本であり重要。要件定義、設計を行う者は、プロフェッショナルとして、各種カイト、ライン等を理解することか求められる。(理解不足による訴訟の例あり) システム環境の複雑さか開発/運用の複雑さにつなかり(利用者、Sler、Cloud 事業者)システムの利用者(社内ユーサ、顧客等)とシステム開発・運用者の役割・責任の明確化か強く求められる。

要件定義、基本設計、詳細設計という段階が基本としてあるが、その段階が移行するタイミングでセキュリティのチェックをする必要があるが、それが行われていないことが多い。例えば、詳細設計になった時点で基本設計にあったセキュリティ要件が消えてしまっていることがある。

IPA などから出ているガイドラインを読んでいないと訴訟の問題になることがある。

こういった基本は今後も変わっていかない。

変わっていくのは細かいところであって、大きなところは変わっていかない。

3.3.2 L 社の回答

セキュリティ対策の変化の原因には二つある。一つは技術の変化である。攻撃側も防衛側も技術の変化は共通して起きるので、技術が変化すればその状況は変化する。もう一つは IT を取り巻く環境の変化である。具体的にはランサムウェアなどは 16 年前から存在しているが、仮想通貨の普及によって近年急激に増加している。

IT 機器は昔は全員が使ってるわけではなかったが、全ての人が使うようになったことでヒューマンエラーは増加している。

タッチパネルが増えてきたので誤操作が起きることも。

開発のあとのテストで、ユーザーの動きをどこまで予測できるかが大事。例えば、アルファベットと数字以外を入れると誤作動が起きるようなシステムを作ってしまった会社があり、それがシステムの的に制限されていなかったため、誤作動を起こしてしまった。「想定外」をなくしていくことが重要である。

変わらないものとして、設計や開発の原理原則などの大きな枠組みはだいたい長い期間残っていく。

3.4 結論

両者とも基本となる設計や開発の原理原則は変わらないという回答であった。一方で、L 社の回答にあるように、技術の変化や IT を取り巻く環境の変化によって重要な脅威は変わってくる。また、PC やスマートフォンが普及したことで、IT リテラシーに差があり、ヒューマンエラーも発生することを考慮したシステムを設計する必要があるが出てきている。

4 サイバー攻撃の最新の動向について

4.1 背景

サイバー攻撃はセキュリティ対策とのいたちごっこが続けている。セキュリティ対策に対し、サイバー攻撃手法はそれを突破するために、様々な試行錯誤の中で高度に変化していく。そういった変化の中では最新の動向を追うことは非常に重要である。例えば、[4]にはサイバー攻撃のトレンドを収集するウェブサイト/書籍として、下記の表 2 のように候補をあげている。

表 2. サイバー攻撃手法のトレンドを確認するためのウェブサイトや書籍 [4]

サイバーレスキュー隊 J-CRAT(ジェイ・クラート)	標的型サイバー攻撃の被害拡大防止のため、組織の被害低減と攻撃の連鎖の遮断を支援する活動を行う。定期的なレポートを確認可能。
サイバー情報共有イニシアティブ(J-CSIP(ジェイシップ))	サイバー攻撃による被害拡大防止のため、サイバー攻撃に関する情報共有の実運用を行う。定期的なレポートを確認可能。本仕組みは午前試験でも何度か出題されている。
情報セキュリティ白書	情報セキュリティ全般に関する状況をまとめた書籍。
ScanNetSecurity	サイバーセキュリティ専門ポータルサイト
Security NEXT	最新情報セキュリティニュースサイト

4.2 ヒアリング内容

追うべきウェブサイトや書籍は表 2 にあげたようなもの以外にも多数存在し、それぞれの企業にとって追うべき内容は異なっていると考えられる。その中で、開発者がその企業にとって重要なサイバー攻撃における新技術の動向と対応策を知るために、どのように情報収集を行えばよいか。特に上記のサイトのなかでどのサイトが重要であるかについてヒアリングを行った。

4.3 回答

4.3.1 D 社の回答

自組織の学習用モデルとして世の中の事故事例を収集するなら、
「ScanNetSecurity」の「不正アクセス事件関連記事の一覧」「個人情報漏洩事件・事故関連記事の一覧」が参考になる。事例を掘り下げて研究するのであれば「J-CSIP」が適している。一覧には無いが、脆弱性情報の情報源としては JPCERT/CC のメーリングリスト
「JPCERT/CCAlert」や IPA 「JVN」等が定番である。

攻撃手法は日々変化しているが、実際のインシデント現場で見られるのは今まで繰り返し警告されていたことが実行できていないことによるものが多い。

- ・ 弱いパスワード
- ・ 既知の脆弱性の放置
- ・ ファイアウォール設定不備

D 社ではトレンドを追うために人をセミナーに派遣したりしている学生も先端の技術に触れるという意味で、そういったことをしていく意義がある。

そういったセミナーの情報は、セキュリティ関係の NPO とか著名な組織のホームページやメーリスで得ることができる。

学生であれば DEFCON や SECCON のようなコンテストに出るとするのはよくある。

カリキュラムという意味では世の中の事例を演習形式でやってみるのが良いのではないか。

4.3.2 L 社の回答

セキュリティ企業はだいたいセキュリティの情報を公開しているので、それを収集する。しかし、そこでは基本的に「結果」に注目されることが多いので、原因をちゃんと追求することをしなければいけない。

原因を追うには脆弱性ポータルサイトで脆弱性情報にちゃんと目を通しておく必要がある。

大学や大学院生、高専生は資格をとる人が少ない。専修学校の学生は資格を重視して、単位等の学校の勉強を軽視している傾向を個人的に感じる。

大学や大学院生は研究を通して、考えながら実践的なところを結構やっているが、専修学校の学生は考えるより先に手を動かしていることが多い。内容を理解せずにやり方だけ覚えてしまっていることが多いため、表面的になりがちである。単純な知識として覚えるだけでなく、実践的な勉強をしたほうがよい。

インターンシップなどによってより実践的な勉強をするべき。

また、講師を外部から呼ぶにしても、引退後の人が呼ばれることも多いが、実際に現場を知っている若手を起用したほうが良い。
また、とくにその学校の OBOG などがいくと、学生の目の色が変わる。

専修学校では学生同士の学び合いがない。そういったことはやっていくべき。

4.4 結論

サイバー攻撃のトレンドを追う方法として、表 2 にあるように、セキュリティ団体が公開しているウェブサイトや書籍が良いことがわかった。しかし、L 社の回答にあるように、結果に注目されがちであるため、原因を追求するためには脆弱性ポータルサイトなどを追うようにした方が良いことがわかった。また、セミナーや研究会に参加することもトレンドを追う助けになるようである。学生であれば DEFCON や、SECCON への参加を促すのことも助けになると考えられる。

両者に共通して、演習や実践を行った方が良いということがわかった。

5 カリキュラムの順位づけについて

5.1 前提

すでにカリキュラム案として、企画提案書に図 2 にあるような項目を挙げている。



図 2. 教育カリキュラムのイメージ

5.2 ヒアリング内容

図2のカリキュラムのイメージの中で、専修学校の学生が学ぶ上で、特に重要だと考えるものはなにか、足りないものや不要と考えられるものは何かについてヒアリングを行った。

5.3 回答

5.3.1 D 社の回答

どんなシステムでも共通なのはネットワーク

プログラマーのセキュリティという意味ではセキュアなシステム設計・開発が重要。ガイドラインにも目を通していない会社が結構あり、問題になっている。

セキュリティにおいて割と重要なのはモニタリング（監視）。侵入をいかに早く検知するかが重要。そこにお金をかけていない会社が多い。どういう攻撃を受けたか、どういう情報が漏れたかというログが取れていない。軽視されがちなので、分野としてもあったほうがいいのではないか。

5.3.2 L 社の回答

大学生は時間があるので、自主的にインターンシップや勉強会に出ることがあるが、高専や専門学校は時間がないので、インターンシップや実践の時間を自主的に取ることができない。それをカリキュラムの中に入れてしまった方がいい。

教員にも教育が必要である。大学では Faculty Development(FD)をやっているが、とくに専修学校の教員にはほとんどFDがない。カリキュラムを決めて欲しいというだけであって、FDをしなければ意味がない。

FDをやっていったって、先生が実践的な教育をできるようにしないとけない。

大学の場合は教員は専門分野を持っていて、それ以外の分野に関しては外部の非常勤講師を手配していることが多い。

順位づけとしては基礎は普通にやっていると思うので、それでいいのではないか。「情報セキュリティの設計と構築」のほうがりていないことが多い。

システム開発ライフサイクルの中で考慮すべきセキュリティ、開発技法を教える必要がある。その上で、演習を行う。

実機演習と実機学習は分けて考えて欲しい。例えばサーバーの脆弱性の調査を依頼されました。どのようにやりますか？みたいな実際のプログラムをみて、それができるようにならなきゃいけない。

5.4 結論

2社で共通して、「設計と構築」が重要であるという回答であった。基礎的なところを網羅しておくことは当然重要ではあるが、「設計と構築」の時間を増やすことを検討することが良いと考えられる。また、前節でも回答があったように、インターンや演習を通して、より実践的な技術を学ぶことが企業からは求められているようである。インターンをカリキュラムに組み込むことがもし難しければ、L社のいうように、実際に現場で働いている若手を非常勤講師として採用することや教員の実践教育としてFDを行うことも検討の価値がある。

また、足りない項目として、D社からは「監視（モニタリング）」が挙げられた。

全体の考察と結論

本ヒアリングでは「今後、増加する情報リスクに対するセキュリティ対策技術の現状と将来的な予想及び Society5.0 で予測される 情報リスクへの対応と技術の進展の情報を収集し、専門学校の学生を対象とした教育プログラムに反映する」という目的の元、「セキュアな情報システム設計・開発技術を明らかにし、教育教材開発に活用する」という目標を持って、2 社にヒアリングを行った。

2 社の回答に共通して言えるのは、ネットワークの知識や設計の知識は普遍的かつ重要であり、これを重点的に学んでいく必要はあると考えられる。そのために IPA などから出版されている業界標準のガイドラインを網羅しておく必要がある。一方で、変化の激しい部分や、IoT などの新しい技術に関しては研究会、セミナー、セキュリティ関係のコンテスト等に参加し、能動的に情報収集する必要がある。また、最新の脆弱性情報に注目する上で、学生が「脆弱性ポータルサイト」の脆弱性情報を追えるようになることも重要であるといえる。

カリキュラムに追加すべき項目として、「監視（モニタリング）」と、「インターンシップや外部講師の招聘などの実践演習」があげられた。とくに「インターンシップ」は企業からの要請も強く、大学に比べ自由な時間の少ない専修学校の学生にはカリキュラムに組み込むことは検討する価値があると考えられる。

また、学生のカリキュラムではないが、「教員の教育（FD）」の重要性も指摘された。知識の更新の早い分野であるほど、FD が重要であるが、大学や高専に比べて専修学校の教員にはそれが足りていないとの指摘があった。

以上より、教育教材開発の際には、「ネットワーク」や「設計」の技術を基礎として重点的に教えたうえで、知識の更新のためのセミナーや研究集会等への参加や脆弱性ポータルサイトの読み方を教え、インターンシップ等の実践演習も組み込んでいくことが重要であると結論づける。

文献目録

- [1] 独立行政法人情報処理推進機構, “情報セキュリティ 10 大脅威 2018,” 27 4 2018. [オンライン]. Available:
<https://www.ipa.go.jp/security/vuln/10threats2018.html>.
- [2] 独立行政法人情報処理推進機構, “IPA セキュア・プログラミング講座,” 9 6 2017. [オンライン]. Available:
<https://www.ipa.go.jp/security/awareness/vendor/programming/>. [アクセス日: 20 1 2019].
- [3] 独立行政法人情報処理推進機構, “「IoT 開発におけるセキュリティ設計の手引き」を公開,” 2 4 2018. [オンライン]. Available:
<https://www.ipa.go.jp/security/iot/iotguide.html>. [アクセス日: 20 1 2019].
- [4] 棚. 英之, “最新動向から学ぶサイバー攻撃の手法と対策,” 15 8 2018. [オンライン]. Available: <https://thinkit.co.jp/article/14843>. [アクセス日: 20 1 2019].

付録「ヒアリングシート」

ヒアリングシート

情報セキュリティに関するリスクが増大する昨今、技術的な視点からリスク対策を構築できる情報セキュリティ人材の育成が喫緊の課題となっています。そこで専門学校を学生を対象とした教育プログラムの開発に向け、情報リスクへの対応と技術の進展についてヒアリングを行いたいと考えております。ヒアリング項目は5項目、計10問ございます。ご協力のほどよろしくお願いいたします。

Q6. 情報セキュリティに対する脅威についてお伺いします。

IPA から毎年発表されている『情報セキュリティ 10 大脅威』には、その前年に発生した社会的に影響の大きい事案がまとめられています。

Q6.1 上記項目の中で、もしくはこれ以外で、セキュリティを考慮する必要のある開発者（以下開発者）が特に詳細まで知っておいた方がいいと考えることは何ですか。

Q6.2 上記項目の中で、もしくはこれ以外で、開発者が忘れがち、ミスをしがち、軽視しがちなものは何ですか。

Q7. IoT 機器のネットワーク接続による新たな脅威についてお伺いします。

IPA から出版されている『IoT 開発におけるセキュリティ設計の手引き』には、様々な IoT 情報セキュリティの脅威と対策が記載されています。

Q7.1 IoT デバイスのセキュリティ対策は非常に多岐にわたっており、今後もその種類は増えていく中で、開発者はどのように知識を收拾すれば良いと考えますか。

Q7.2 今後（もしくは現在）情報セキュリティ専門企業として、こういった対策をお考えですか（とられていますか）。

Q7.3 IoT デバイスの新たな脅威において特に重要と考えるトピックは何ですか。

Q8. 今後の情報セキュリティ技術/情報セキュリティの観点からのシステム設計・開発についてお伺いします。

情報セキュリティの脅威は常に変化し続けており、今までの常識がそもそも通用しないこともあります。

Q8.1 今後システム設計や開発において、意識するセキュリティはどう変化していくか、またどう変化していくべきだと考えますか。何が基本的なものとして残り、何が新しく出てくることが考えられますか。

Q9. サイバー攻撃における新技術動向と対応についてお伺いします。

様々なサイト（例えば[こちらのサイトの表 1](#)）で最新のサイバー攻撃のトレンドを追うことができるようになっています。

Q9.1 開発者が所属する企業にとって、重要なサイバー攻撃における新技術動向と対応策を知るために、開発者はどのように情報収拾するべきだと考えますか。（上記のサイト表 1 で特に追うべき重要なサイトはどれですか。）

Q9.2 最近のサイバー技術動向で、特に重要と考えるトピックは何ですか。

Q10. カリキュラムにある項目（別紙参照）の順位づけについてお伺いします。

専門学校の学生向けに教育カリキュラムの案として、すでにいくつか挙がっているものがあります。

Q10.1 これらの中で特に重要なものは何だと考えますか。

Q10.2 足りないものや不要なものはありますか。もしありましたら、具体的に教えてください。

平成 30 年度「専修学校による地域産業中核的人材養成事業」
Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

情報セキュリティの Society5.0 対応実態調査報告書

平成 31 年 3 月

一般社団法人全国専門学校情報教育協会
〒164-0003 東京都中野区東中野 1-57-8 辻沢ビル 3F
電話：03-5332-5081 FAX 03-5332-5083

●本書の内容を無断で転記、掲載することは禁じます。