参考資料 2-2

「プラス・セキュリティ」知識の補充のためのモデルカリキュラム
セキュリティ・IT に関する基礎知識の整理

2020.11 NISC 基本戦略第 1 グループ

「プラス・セキュリティ」知識の補充のためのモデルカリキュラムにおいて、「DX を推進する部門の責任者あるいは主要な役割を担う管理職（DX 経営推進者・DX 事業推進者等、部課長級を念頭)」であって、必ずしも IT やセキュリティに関する専門知識や業務経験を有していない方々に、専門家と協働するにあたり最低限必要で役に立つと考えられるセキュリティ・IT 基礎知識（専門的な知識そのものの習得というより基礎概念として理解すべきと言えるもの）として、どこまで身に付けることが望ましいか、以下のとおり第 1 段階的な試みとして整理を行った。

（1）「サイバーセキュリティの要素技術」に係る基礎概念

◆**目標：**サイバーセキュリティの基本的な考え方や用語について正しく理解し、セキュリティ対策の状況や不明点を確認できる。

（参考) IT パスポート試験シラバスにおける対応要素（【】内は項目番号）
・情報の収集や活用を安全に行うために情報セキュリティが必要であることを理解する。【61】
・情報セキュリティを確保するために必要な、暗号、認証、公開鍵基盤などの技術の役割を理解する。【63】

→上記の目標に当たり、以下の項目は、概念なりとも理解することが望ましいと考えられる。

- 情報セキュリティ対策の基礎（9 か条など）
- 情報セキュリティの基礎
  （3 要素(機密性、完全性、可用性）／脅威、脆弱性、リスク／ドベネックの桶、多層防御、最小権限）
- 代表的な暗号方式、認証方式（共通鍵暗号方式 ／ 公開鍵暗号方式 ／ 認証方式）
- デジタル署名、PKI
- ユーザ認証（多要素認証、二段階認証）

上記習得に当たって前提となる IT に関する基礎概念

（2）「コンピュータ理論」に係る基礎概念

◆**目標：**コンピュータの基本的な仕組やソフトウェアの階層等について正しく理解し、DX の推進に関連してこれらについて考えを伝えあえる。

（参考) IT パスポート試験シラバスにおける対応要素（【】内は項目番号）
・コンピュータを構成する基本的な構成要素と仕組を理解する。【40】
・OS、アプリケーション、ファームウェア等の機能やソフトウェアの階層を理解し、PC、サーバ、モバイル端末で利用される主な OS の種類について理解する。【45】
・ネットワークを介した分散処理を実現する為に用いられるサーバ、データセンタ、クラウドコンピューティングの基本を理解する。【20】

→上記の目標に当たり、以下の項目は、概念なりとも理解することが望ましいと考えられる。

- コンピュータの基本構成（5 大要素）
- ソフトウェアの階層（アプリ、OS、ファームウェア等）
- 主な OS の種類（PC、サーバ：Windows(Microsoft)、macOS(Apple)、Linux／
  モバイル端末（スマホ等）：Android(Google)、iOS(Apple)））
- サーバ、データセンタ、クラウドコンピューティング

≈

≈（3）「情報通信ネットワーク理論」、「インターネットの基本原理」に係る基礎概念

◆目標：ネットワーク上で発生する通信について正しく理解し、必要なネットワーク機器やインターネットのプロトコル等について判断ができる。

（参考）IT パスポート試験シラバスにおける対応要素（【】内は項目番号）
- ネットワークは企業などの活動において必要不可欠な基盤であることを認識し、代表的なネットワークの構成要素について、役割の概要を理解する。【58】
- ネットワーク経由で通信するためには，通信プロトコルが必要であることを理解し、代表的なプロトコルの役割を理解する。【59】
- インターネットの基本的な仕組とそれを応用したシステムについて理解する。【60】

→上記の目標に当たり、以下の項目は、概念なりとも理解することが望ましいと考えられる。

- インターネットにおける通信の仕組
  （インターネットについての基本的な概念（分散型）／
  OSI 参照モデル、TCP/IP の階層、通信プロトコルの階層／IP アドレス／MAC アドレス／
  ドメイン名、DNS）
- ネットワーク機器（ハブ、ルータ、スイッチ）
- インターネットのプロトコルとそれを利用したシステム（電子メール／WWW）

（注）上記の項目については、基礎概念についての認識が共有されるよう、実際の試行カリキュラム実施にあたっては NISC から講師に別途資料を提示している。（関心がある場合は、お問い合わせください。）

＜参考１＞整理作業の考え方

作業①：DX 事業推進に際し活用が想定される場面（★）から逆算し、どのような状態を目指すかを整理。

★DX 推進のシナリオ例：

国内主要都市を中心に店舗を構え、デザイン性の高い日用品を販売していた A 社は、新型コロナウィルス感染症の影響で実店舗における販売が落ち込んだことから、ネット販売による B2C 事業を開始することとなった。これまで、セールス部門の部長を務めていた D 氏は、DX 推進部長に抜擢され、ネット販売のサービス立ち上げに向けた検討プロジェクトをスタートさせた。

プロジェクトの主要メンバーは、社内の情報システム構築を担当していた I 氏、そしてシステム開発業務を委託していた付き合いのある IT ベンダーの V 社が加わった。ある日、プロジェクトの定例ミーティングで次のようなやり取りがあった。

I 氏「今回 V 社さんに開発して頂くネット販売のサービスは、***クラウド***上で運用する予定です。クラウド業者としては、運用コストの一番安価な Z 社が良いと考えています。」

D 氏「運用コストは当社の利益に大きく影響するので、安価であることに越したことはないが、Z 社のセキュリティ対策は大丈夫か？」

I 氏「Z 社はクラウド分野では後発組ですが、***OS*** を含めた ***PaaS*** のクラウド環境を提供する業者として国内企業の利用実績も多く、***Linux*** の脆弱性対応もしっかりしています。また、クラウド環境の保守用のアカウントには***強力なパスワード***を設定しており、接続する PC も ***MAC アドレス***により制限しています。」

D 氏「基本的な対策は出来ているようで安心した。クラウドの上で運用する、当社のネット販売サービスの方はどうか？」

V 社「サービス全体の***セキュリティ分析***を行い、必要なセキュリティ対策を導入しています。」

D 氏「お客様はスマホや PC を使いインターネット経由でネットショッピングをされるが、***なりすまし***等の対策はどうか？」

I 氏「お客様がサービスにログインする際に、***二要素認証***で不正利用を防ぎます。」

D 氏「お客様の***個人情報***はどこに保管しておくのか？　流出の心配はないのか？」

V 社「クラウド上に保管されますが、個人情報や注文情報は***暗号化***されます。また、注文情報には***電子署名***を付けるので、不正な書き換えも出来ません。電子署名のための***証明書***は P 社から発行する予定です。」

D 氏「なるほど、P 社は公的な認定をうけた***認証局***なので安心だ。お客様に安心してネットショッピングを楽しんで頂く為に、何かアピールはできないか？」

V 社「それであれば、プライバシーマーク制度を活用してはいかがでしょうか。個人情報の取り扱いを適切に行う体制等が整備されていることを証明できます。」

D 氏「よし、プライバシーマークを取得しよう。次回までに、必要な体制・費用等の見積りをして、役員会で承認を得ることにしよう。」

（注）文中、***下線付き斜体太字部分***が、本試行カリキュラムで補充する基礎知識に該当する。

作業②：実務目線から IT 初心者に必要な知識が整理された「IT パスポートシラバス」を参照し、ⅰ：詳細な目標（以下参照）とⅱ：理解が望ましい基礎概念を整理。

（1）「サイバーセキュリティの要素技術」に係る目標：
- 情報の収集や活用を安全に行うために情報セキュリティが必要であることを理解する。【61】
- 情報セキュリティを確保するために必要な、暗号、認証、公開鍵基盤などの技術の役割を理解する。【63】

（2）「コンピュータ理論」に係る目標：
- コンピュータを構成する基本的な構成要素と仕組を理解する。【40】
- OS、アプリケーション、ファームウェア等の機能やソフトウェアの階層を理解し、PC、サーバ、モバイル端末で利用される主な OS の種類について理解する。【45】
- ネットワークを介した分散処理を実現する為に用いられるサーバ、データセンタ、クラウドコンピューティングの基本を理解する。【20】

（3）「情報通信ネットワーク理論」、「インターネットの基本原理」に係る目標：
- ネットワークは企業などの活動において必要不可欠な基盤であることを認識し、代表的なネットワークの構成要素について、役割の概要を理解する。【58】
- ネットワーク経由で通信するためには，通信プロトコルが必要であることを理解し、代表的なプロトコルの役割を理解する。【59】
- インターネットの基本的な仕組とそれを応用したシステムについて理解する。【60】

（注）【】内は「IT パスポートシラバス」の項目番号に対応。

＜参考２＞セキュリティ・IT に関する基礎知識を問う設問例

「プラス・セキュリティ」知識の補充のためのモデルカリキュラム
セキュリティ・IT に関する基礎知識を問う設問例

2020.11 NISC 基本戦略第 1 グループ

モデルカリキュラムでは、「必ずしも IT やセキュリティに関する専門知識や業務経験を有していない方々」を対象としているところ、受講者の知識・経験を把握し、それに応じた実施上の工夫を行った方がよいと考えられるが、必ずしもこれまで、セキュリティ・IT に関する基礎知識に係る経験や習得状況等を問う設問が見当たらなかったところ、以下のとおり試みに設問例を作成した。

（設問例）

Q. IT の知識や経験について、該当するもの全てに【〇】をご記入ください。

No. 1 【 】 インターネットで注文したり手続きを行ったことがある。

No. 2 【 】 IP アドレスと呼ばれる数字列を見たことがある。

No. 3 【 】 Facebook、Twitter、Instagram 等の SNS を３つ以上使っている。

No. 4 【 】 自宅のインターネット環境の一部又は全部を自分で整えたことがある。

No. 5 【 】 パソコンの周辺機器（例えば、USB 接続の外付けハードディスクドライブ）を自分で選んで購入したことがある。

No. 6 【 】 パソコンの使い方を他の人に教えたことがある。

No. 7 【 】 学生時代（学部講義含む）を含めて、プログラム（C、Java、Python 等）を作成し実行ファイルを実行したことがある。

No. 8 【 】 コマンドプロンプト等で、コマンドの入力によるパソコンの操作をしたことがある。

No. 9 【 】 IT 関係の業務に従事したことがある。

Q. セキュリティの知識や経験について、該当するもの全てに【〇】をご記入ください。

No. 1 【 】 パソコンにインストールされているウィルス対策ソフトの名称を知っている。

No. 2 【 】 必要に応じてOSやアプリケーションのセキュリティパッチ（修正プログラム）を適用している。

No. 3 【 】 セキュリティ事故のニュースや報道をみて、パソコンやアカウントの設定を変更したことがある。

No. 4 【 】 ファイルを暗号化（例えば、ファイルの圧縮時にパスワードで保護）したことがある。

No. 5 【 】 セキュリティ関係の業務に従事したことがある。