# 制御システムのセキュリティ人材育成に関する調査

# 及びモデルカリキュラム等の作成

## － 調査実施報告書 －

2013 年 4 月

独立行政法人 情報処理推進機構
セキュリティセンター

目　　次

# 1. はじめに

## 1.1. 背景・目的

重要インフラや工場プラントで使用される制御システムに対するサイバー攻撃は、世界的に年々増加傾向にあり、その対策が急務となっている。平成23年度に実施された経済産業省の「制御システムセキュリティ検討タスクフォース」での議論においては、結果の1つとして制御システムのセキュリティ対策を行う人材の育成の必要性が挙げられている。また、独立行政法人情報処理推進機構（以下「IPA」という。）が、平成23年度に設置した「情報セキュリティ人材育成検討委員会」での議論において、制御システム分野の情報セキュリティ人材の育成についてIPAが貢献すべく平成24年度に事業を行うことが提言された。

このような状況を踏まえ、本調査では、制御システム分野の人材に必要な情報セキュリティに関する知識やスキルを調査するとともに、人材育成のためのモデルカリキュラム等の作成にあたった。これらの成果を基に我が国の制御システム分野の情報セキュリティ人材育成の促進を目的とするものである。

## 1.2. 検討の進め方

本調査の検討にあたり、制御システム分野の産業に属する企業に対し、インタビュー等の調査を行い、当該分野の産業に従事する者に求められる情報セキュリティに関する知識項目、スキルのとりまとめを行うとともに、当該知識項目、スキルを付与するために必要な研修のモデルカリキュラム等を作成した。さらに、本事業を遂行する上で必要な意見を有識者から得るため、IPA 内に「制御システムワーキンググループ」（以下「ワーキンググループ」という。）を設置した。

なお、本調査は、経済産業省の「制御システムセキュリティ検討タスクフォース」での議論の結果に基づき実施されるため、同タスクフォースの中間報告書とりまとめ（案）の内容を踏まえ、またタスクフォースの検討に基づき設立された技術研究組合制御システムセキュリティセンター（CSSC）の普及啓発・人材育成に係る活動とも密接な連携を行った。

具体的な検討の進め方を以下に示す。


**図 1.1　検討の進め方**

まず、制御システム分野の人材育成等に関する実態を知るために、制御システム分野の産業に関するインタビューを中心とした調査を行った。この調査にあたっては、特に制御システム関連分野において重要となる情報セキュリティに知識項目、スキルの明確化を意図した。また、調査に先立って作成した研修モデルカリキュラムのイメージ案についてコメントを集めることで、必要性の高い知識項目、スキルを抽出し、効果の高いカリキュラムを策定するための示唆が得られた。

実態調査の結果を踏まえ、知識項目、スキル、および研修モデルカリキュラムの案を作成し、有識者の意見を参考に検討を重ねて、これらをとりまとめた。

# 2. 制御システム分野の人材育成等に関する実態調査

## 2.1. 調査の概要

制御システムの開発、調達、運用、管理などの業務に携わる人材の育成の実態を調査するため、インタビュー調査を行った。

### (1)方針

制御システム分野における人材育成(特に情報セキュリティに関する教育)の実態、制御システム分野の情報セキュリティに関与する者に求められる知識項目・スキルについて実態を把握する。この実態把握を踏まえて、知識項目・スキル一覧、および研修のモデルカリキュラムの策定を行った。

制御システム分野のセキュリティに関する教育カリキュラムの整備が昨今強く要請されている点を考慮し、調査にあたっては、現場において必要とされる知識項目・スキルに関する意見や、具体的な研修を想定したカリキュラム作成に有用な意見を集めることとした。

制御システムに携わる業務毎に求められる能力等が異なることが想定されるため、インタビュー依頼時には、幅広い業務に対して回答可能な立場の方への依頼、もしくは異なる業務の複数担当者への対応を依頼した。

### (2)実施方法

調査に先立って､制御システムのセキュリティに関する文献を参考にして、研修モデルカリキュラムの原案（イメージ）を作成した。この原案の作成においては、特に制御システムに関わる情報セキュリティの知識項目、スキルのうち主要な項目と考えられるものを挙げた。

インタビュー調査対象者に対しては、事前にインタビューシート及び研修モデルカリキュラム原案（イメージ）を送付した上で、対面によるインタビュー調査において調査項目の詳細について聞き取りを行った。インタビューでは特に、制御システムのセキュリティを中心とした制御システム技術者における教育の実態、モデルカリキュラム原案において不足する項目や、教材を整備し活用する上で留意すべき点について意見を集めた。

### (3)調査項目

インタビュー調査においては、以下の調査項目について調査を実施した。

① 制御システムのセキュリティ確保への取組みの実態
- ・制御システムにおけるセキュリティ上の脅威やリスク
- ・制御システムにおけるセキュリティ確保のための取組み
- ・制御システムに特有のセキュリティ対策

② セキュリティ人材を中心とした人材育成の実態
- ・制御システムに関わる人材の育成状況について（教育の手法等）
- ・制御システムに関わる人材の育成状況について(推奨している資格等)
- ・制御システムに関わる人材に対するセキュリティ教育の状況について

③ モデルカリキュラム（案）への意見
- ・モデルカリキュラム（案）について
- ・体験型の学習について
- ・カリキュラムを利用した人材育成の実現方法について
- ・ベンダ技術者とその教育について
- ・ユーザ技術者とその教育について
- ・オペレータとその教育について

④ その他
- ・その他制御システム分野の人材育成等に関する問題意識・要望　等

## 2.2. 調査対象

調査対象は、制御システムを扱う分野に属し、制御システムの運用や開発を行う民間企業、または地方公共団体、公益法人等とした。調査対象を以下に示す。

**表 2.1　インタビュー対象の分野と対象者**

| 分野 | インタビュー実施対象者 |
|---|---|
| 化学分野 | ユーザ 1 社、エンジニアリング企業 1 社 |
| ガス分野 | 関連団体 1 組織、ユーザ 4 社(グループインタビュー) |
| 水道分野 | ユーザ 2 組織 |
| 電力分野 | 関連団体 2 組織 |
| 制御製品ベンダ | 大手ベンダ 4 社 |

計 5 分野 15 組織

## 2.3.調査結果

### (1)制御システムのセキュリティ確保への取組みの実態

①制御システムにおけるセキュリティ上の脅威やリスク

制御システムにおけるセキュリティ上の脅威やリスクについての主要なコメントを表 2.2に示す。

**表 2.2 主要なコメント**
**（制御システムにおけるセキュリティ上の脅威やリスク）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ リスクについては技術者や経営者に理解を促したい。<br>・ リスクを考えて対応を決める手法、リスク分析の教育が必要。<br>・ 脅威については未知の部分が多い。多様な脅威の全てをわかっていない。<br>・ 脅威のパスも多様だが、理解している人は少ない。<br>・ 具体的な脅威がわからないと対策はおろそかになりがちである。 |
| 化学分野ユーザおよびインテグレータ | ・ オフィス情報系から狙われるリスクの高さがよくわからない。<br>・ 情報漏洩でノウハウを取られる危機感はある。制御のレシピと設備データを抜かれると痛手にはなる。<br>・ 制御システム固有の脅威事例がないので特徴がわからずイメージが掴みにくい。制御の事例が少ない。<br>・ もし制御システムでの被害があれば危機感が高まるだろう。<br>・ 最近 2 年程で意識が大きく変化している。Stuxnet で危機感を持ち、教育や設備の補強を進めている。 |
| ガス分野ユーザ | ・ 想定すべき脅威が明確でないので誰かに示して欲しい。一般的なウイルス対策でよいのか、高度な Stuxnet 級の攻撃を想定した対策が必要なのか、想定脅威のレベルが定まらなければ動けない。<br>・ ハイレベル対策に経営層を動かすのは難しい。ここまで対策をやるべきという指標を示して欲しい。 |
| 水道分野ユーザ | ・ 基本的にコントロール室に厳格な入退室管理を導入しているが、導入が遅れている箇所も一部にある。<br>・ オペレータ業務を外部委託している場合もあり、必要に応じて職員が指導している。<br>・ 現在無人の浄配水場において、もし信号が途絶するような事態 |

| | |
|---|---|
| | が起きれば駆けつけて対応する。ただし、職員には対応経験が少ない者もいる。 |
| 電力分野ユーザ | ・ 実態としてこれまで脅威を経験したことがない。そのような中で事例の勉強は難しい。結局はモラルに関する教育になってしまう。<br>・ 脅威について教えた方がよい。脅威に晒される機会が少ないのでポイントを絞って教育してはどうか。<br>・ 更新周期が非常に長いため、独自仕様と国際標準の採用で今後各社が迷う所。 |

②制御システムにおけるセキュリティ確保のための取組み

制御システムにおけるセキュリティ確保のための取組みについての主要なコメントを表 2.3に示す。

**表 2.3 主要なコメント**
**（制御システムにおけるセキュリティ確保のための取組み）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ ログは取れるが解析の体制が整っていない。定期的に確認する人の確保が課題。<br>・ セキュリティに関して正常と異常の違いは一見しても分からない。技術的手段を入れて、アラームの自動化を試みている。システム監視サーバ自体が未だ認知されていない。もっと必要性を伝えるべき。<br>・ 脆弱性検出のツールは使いたい。ツールについて基礎から分かっている人は少ない。<br>・ セキュリティがわかる技術者は 10%ほど。社内の情報セキュリティの専門家は制御システムが分からない。<br>・ ウイルスに関する問題は運用・保守での接続時に事前確認して対応している。 |
| 化学分野ユーザおよびインテグレータ | ・ 前提として制御系は情報系とは切り離し入口を固く守る。他の分野、組立系や物流では前提としてつながらなければならないのでウイルス対策を入れてシステムを作っている。守り方が異なる。<br>・ メディア、CD-R、USB 等についてはウイルス対策として接続する前に最新パターンでチェックをしている。ベンダから受け取るときやユーザに渡す前にチェックしている。基本的にはつながないように保っている。 |

| | |
|---|---|
| | ・ 攻撃の兆候については情報収集をしている。<br>・ 運用でルールを定めている。情報系のルールを踏襲している。<br>・ 危険なことをできないようにする方向で対策を進めている（例：USB ポートをふさぐ）。<br>・ 被害を小さく復旧時間を短くするよう考えてシステムデザインしている（例：被害拡散を防ぐために区切る、ログを可能な限り出力し収集する）。<br>・ 異常に気付くのは感性、センスである。異常時にそれを言い出せるようにしておくことが大切である。 |
| ガス分野ユーザ | ・ オフィス系との境界のファイアウォール等のログチェック等を運用委託しており、異常や怪しい際にはベンダに連絡して確認している。 |
| 水道分野ユーザ | ・ 厚生労働省から水道事業所に特化した情報セキュリティポリシーのサンプルが配布されている。<br>・ 現在のシステムには USB によるデータ入出力が行えず、職員が手入力しているものもある。 |
| 電力分野ユーザ | ・ 満点を取るのは無理なので、及第点を取れるように、今できる対策を確実にすることが重要。<br>・ 制御システムセキュリティへの意識は高い。 |

③制御システムに特有のセキュリティ対策

制御システムに特有のセキュリティ対策についての主要なコメントを表2.4に示す。

**表 2.4　主要なコメント（制御システムに特有のセキュリティ対策）**

| **聴取先** | **コメント** |
|---|---|
| 制御製品ベンダ | ・ 技術面では基礎は情報系と同じ考え方。<br>・ 実現手法は多層防御が主（一方で境界ごとに対策を施すとコストが大きくなってしまう）<br>・ ウイルス対策ソフトウェアをあえて導入せず接続時等にチェックして運用で対応する場合もある。<br>・ 主に情報の層からの脅威を主に想定、HMI とコントローラの間やコントローラでどう守るかが重要。<br>・ 制御ネットワークは比較的閉じた環境になっている点が特徴。<br>・ HMI に注目しがちだがコントローラが大切。ベンダにより考え方や構成等が異なる。他社では手が出ない。 |

| | |
|---|---|
| | ・ 技術的に一番大事な部分が見えにくい。独自プロトコルの設計やコントローラの作り方は分からない。 |
| 化学分野ユーザおよびインテグレータ | ・ 情報系の事例と重複するのはやむを得ない。<br>・ 主にベンダが扱う制御機器のネットワークに独自性がある。無線計装などで作りこんでもいる。<br>・ 制御系では高速性が要求される。普通のウイルス対策は反応が遅くなるので入れられない。 |
| ガス分野ユーザ | ・ 一般的な対策、各社のシステムに特化されない汎用的知識は情報システムとあまり違いは無い。<br>・ 制御システムにはコントロール可能な機器類がつながっている点が特徴である。計装の部分が特徴。<br>・ 制御システムは作られるものが異なれば接続される機器が異なりシステムもセキュリティの手法も異なる。<br>・ 最後の砦が違う。安全側に倒れるような特徴が計装にはある。<br>・ 制御システムの一般化していないネットワークは特徴である。通信に特徴がある。<br>・ 情報システムには汎用的ソリューションがあるが、制御システムではユーザが自分で考える必要がある。<br>・ 制御システムの構築には典型的プロセスが無く、ユーザにより作り方が異なる。<br>・ 制御システムでは、クローズドなネットワーク、常に同じプロセスでシステムが動いていること等が特徴。 |
| 水道分野ユーザ | ・ 外部とウェブ系で繋がっているリモートメンテナンスがあるかどうかでセキュリティ対策上の条件は異なる。<br>・ 電源の問題。UPS を通していても、瞬低やパルス状の高電圧の影響を受けることがある。 |
| 電力分野ユーザ | ・ 結局、内容は情報系と同じになる。<br>・ 電力では、たとえば対策のトレードオフとして速度に影響が出る場合、考慮する必要がある。 |

### (2)セキュリティ人材を中心とした人材育成の実態

①制御システムに関わる人材の育成状況について（教育の手法等）

制御システムに関わる人材の育成状況についての主要なコメントを表 2.5 に示す。

**表 2.5　主要なコメント**
**（制御システムに関わる人材の育成状況について（教育の手法等））**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ 社内の研修所で製品や技術についてコースを受講。業務に必要なので自主的に研修を受ける。<br>・ 研修所では実機は扱っているが模擬プラントはない。大きなものはない。<br>・ 社内でカリキュラムや教育計画を考えている。職級とリンク付けして必要な知識と受ける教育を示す。<br>・ トレーニングセンターで自社製品の教育をしており、顧客向トレーニングカリキュラムを社員にも利用。 |
| 化学分野ユーザおよびインテグレータ | ・ エンジニアの教育ガイドラインと育成カリキュラムはある。工場別だが中身はほぼ共通。OJT と外部講習を利用している。<br>・ エンジニアにレベルを設定しレベル毎に受けて欲しい講習を示している。<br>・ エンジニアの導入教育はある。部署毎に作成。<br>・ 情報系の知識は個人差がある。外部講習会に参加して知識を吸収している。<br>・ IPA の基本情報くらいまでは取得していたい。 |
| ガス分野ユーザ | ・ 日々の実際の業務で叩き上げる。5 年か 10 年くらいで他の業務に移る。<br>・ 教育コンテンツはない。システムに特化したマニュアルと伝授。OJT 型。<br>・ 新人にベンダが提供する制御システムの基礎コースを受講させている。<br>・ ネットワークについての基礎も外部で受講している。OJT 中心の教育体系。<br>・ エンジニアを育てる基礎カリキュラムはある。訓練センターでは計装に関する講義はある。<br>・ 社内カリキュラムはない。入社時にメーカの研修を受けさせている。社内の OJT が中心。 |

| | |
|---|---|
| | ・ 教育は少なくベンダに教わることも無い。移動してきた際に基礎を数時間で教育する程度。後は OJT。<br>・ 訓練センターで基礎を教えている。ベンダの DCS 等の製品の講座と同様の内容を社内で実施している。 |
| 水道分野ユーザ | ・ オペレータは OJT で育成する。 |
| 電力分野ユーザ | ・ 制御分野では、教育カリキュラムやコースがない。<br>・ 会社によっては、基本的な教育を実施しているところもある。 |

②制御システムに関わる人材の育成状況について（推奨している資格等）

制御システムに関わる人材の育成状況についての主要なコメントを表 2.6 に示す。

**表 2.6　主要なコメント**
**（制御システムに関わる人材の育成状況について（推奨している資格等））**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ 制御に関する資格は無い。資格にしづらい。現場の経験とノウハウが大切。<br>・ SICE の計装エンジニア資格はハードルが高く取得している者は少ない。<br>・ 情報処理技術者のように制御の技術者について統一的な評価ができるかは疑問。制御システムの場合各社のシステムはそれぞれ違う。<br>・ 認定エンジニア的な資格制度を作るには対象人数が少ない。資格を取る人は全ベンダでも 70 人程度。制度が立ち行かなくなると想像される。<br>・ 資格に賞与等のインセンティブを用意している。給与が増える、一度限りの賞与が出る等。<br>・ 公的資格を取るように勧めてはいない。<br>・ 通信教育（外部教材）を活用している。<br>・ 製品開発でセキュリティに関係した場合でもプロジェクトが終わったら離れてしまう。資格を得ても続けられない。 |
| 化学分野ユーザおよびインテグレー | ・ 計装士、計量士など。<br>・ IT 系資格の給与への反映はない。昇格の要件に資格の取得によるポイントはある。受験料・受講への補助はある。 |

| | |
|---|---|
| タ | |
| ガス分野ユーザ | ・ 奨めている外部の資格のようなものは特にない。 |
| 水道分野ユーザ | ・ 特になし。 |
| 電力分野ユーザ | ・ 各社内で教育はしているが特に制御エンジニアの資格はない。<br>・ 資格や認定の制度を新たには必要としていない。<br>資格では通用しない。 |

③制御システムに関わる人材に対するセキュリティ教育の状況について

制御システムに関わる人材に対するセキュリティ教育の状況についての主要なコメントを表 2.7に示す。

**表 2.7 主要なコメント**
**（制御システムに関わる人材に対するセキュリティ教育の状況について）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ 社内で制御システムセキュリティに関する教育はなく、専門家も多くはない。<br>・ 制御セキュリティを専門とする人間が希少。自分の専門の中でセキュリティもカバーしなければならない。<br>・ 講師役の技術者が社内研修を行っている。その時の話題や趣旨に合わせてピンポイントに教えている。<br>・ 製品のセキュリティ担当者経由で教育を行っている。製品開発の各部署に担当がいる。<br>・ セキュリティ専門チームが各製品の開発部門に教育をしている。<br>・ 制御ではなく情報システムのセキュリティ教育を受けることはできる。カリキュラムも用意されている。<br>・ カリキュラムは手作り。体系化された教材は欲しい。自習するための教材、入門書が少ない。<br>・ セキュリティの基礎が技術者の常識になりつつあり基礎的教育をしづらい。<br>・ 社外セミナーや外部講師依頼を利用したい。開発でのセキュアプログラミングの講習等は検討段階。<br>・ 顧客向け製品トレーニングカリキュラムにはセキュリティに |

| | |
|---|---|
| | ついてはほとんど入っていない。 |
| 化学分野ユーザおよびインテグレータ | ・ 特に専門的な教育メニューはない。<br>・ 外部の講習会、ベンダの研修などを利用している。<br>・ セキュリティについてはシステムに関係するほぼ全員が勉強はしている。<br>・ 社内の IT 関連の教育でのウイルス対策等の教育はある。E ラーニング等。<br>・ 月例ミーティング等で牽引役から情報の展開をしている。 |
| ガス分野ユーザ | ・ 制御のセキュリティについては特に教育はしていない。<br>・ 一般社員向けの情報セキュリティ教育は制御系においても使える基本的なセキュリティ教育になっている。<br>・ してはいけないことについて注意点を教える程度（USB を挿してはいけない等）。 |
| 水道分野ユーザ | ・ オフィス系でのセキュリティの教育を見ながら制御系でも進めている。<br>・ 組織が実施する一般的なセキュリティ研修を受講する程度。 |
| 電力分野ユーザ | ・ 各社で独自の教育はしており一部に第三者が提供する教育を受ける会社もある。<br>・ 米国では、制御システムのセキュリティ教育の担当者が育成されている。 |

### (3)モデルカリキュラム（案）への意見

①モデルカリキュラム（案）について
制御システムのモデルカリキュラム（案）についての主要なコメントを
表 2.8に示す。

**表 2.8　主要なコメント（モデルカリキュラム（案）について）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ 基本的にはオフィス情報系とシナリオは同じ。<br>・ 内容は情報分野と同様だが、それらを基に制御システム全体のイメージを更新しセキュリティを入れる。<br>・ 制御システムの具体的なイメージの上で説明してセキュリティの必要性を理解させることが望ましい。<br>・ 身近な業務でセキュリティ脅威により被害を受けるという事例が欲しい。<br>・ 実施可能な範囲での運用面の対策、現場でどう考えて実施するかを重視してほしい。<br>・ 将来よりも現在の課題を重視してほしい。<br>・ 全体像を示してほしい。網羅的だが、不足部分は他の取組みと組み合わせる必要がある。<br>・ 詳しく知りたい人のために参照先を示すとよい。<br>・ 表現や用語が分野、立場、企業により異なるので難しい。<br>・ 教育を受ける視点が違うのでユーザとベンダでコースは分けた方がよい。 |
| 化学分野ユーザ/インテグレータ | ・ 検知や気付きの対応ができる人材の育成を重視したい。<br>・ まずは脅威と被害の実際を見せて伝えたい。 |
| ガス分野ユーザ | ・ 対策の表層的な記述よりも、対策が必要とされる理由やリスクの理解を促してほしい。<br>・ 情報システムと制御システムの性質の相違点や特徴を入れるべき。<br>・ インシデントやStuxnet等の脅威の動向を入れるべき。<br>・ 制御システムを設計、開発、運用する流れでセキュリティを取り扱い実現していくまとめ方がよい。 |
| 水道分野ユーザ | ・ 知識項目としては妥当。セキュリティの意義から教えるカリキュラムも必要である。 |

| | |
|---|---|
| | ・ ユーザが適切なベンダと製品を選択するための基礎知識をつけるためなら有用。<br>・ モデルカリキュラムは簡単なものがよい。<br>・ 制御系はオフィス系とどこが違うかという観点から入った方がわかりやすい。<br>・ 情報分野に特化している印象。たとえば、ループコントローラのような自動制御機器を想定しているか。 |
| 電力分野ユーザ | ・ 基礎的な項目としては案に示されたもので十分。<br>・ 模範的な対策が無理な際の代替策まで示してくれるとよりよい。<br>・ 経験年数で区切るより、持っているスキルや担当業務で区切るべき。<br>・ 基礎コースで注意喚起することが重要。<br>・ サードパーティリスクの管理についても採り上げるべき。 |

②体験型の学習について

体験型の学習についての主要なコメントを表 2.9に示す。

**表 2.9　主要なコメント（体験型の学習について）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ みせる演習を入れるべきである。脅威を認識し対策が必要と思うことが重要である。<br>・ 単なるデモではなく、セキュリティが強固な制御システムの設計を教育して欲しい。<br>・ デモシステム（模擬プラント）を構築・活用するには教育のシナリオを明確にしたい。<br>・ シナリオには無線 LAN から侵入され重要情報を奪われる場合、サーバに外部へのバックドアを埋め込まれる場合、エンジニアリングツールをUSB接続することを契機とする場合などが考えられる。<br>・ 体験型でなく講師のデモを見るだけでも有意義である。<br>・ 検査手法を整理したりツールの活用法を学び、各組織に知識を持ち帰れると良い。 |
| 化学分野ユーザおよびインテグレー | ・ 経営層に重要性をわかってもらうことは重要。デモを見てもらうのが良い。<br>・ デモと基礎知識をつける座学があると良い。 |

| | |
|---|---|
| タ | |
| ガス分野ユーザ | ・ 検知や対処の手法を教えて欲しい。 |
| 水道分野ユーザ | ・ 遠隔操作から現場操作に切り替えてポンプを手動で動かす等の切替え訓練は試みたい。職員には手動操作の経験が乏しい者もいる。 |
| 電力分野ユーザ | ・ 実習もできればよいが実現はかなり困難ではないか。<br>・ 情報系では、業界内でサイバー演習を実施している。制御系についても演習があるとよいという意見もある。<br>・ USB 接続をすると何が起きるのかを示すことは、個社では難しいので、注意喚起として意味がある。 |

③カリキュラムを利用した人材育成の実現方法について

カリキュラムを利用した人材育成の実現方法についての主要なコメントを表 2.10に示す。

**表 2.10 主要なコメント**
**（カリキュラムを利用した人材育成の実現方法について）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ 制御システムに根差したセキュリティについて他に類似する研修は無いので受講者は居るだろう。<br>・ テストベッド（模擬プラント）でのデモだけでなく、地方に出張して教える取組みと連携すべき。<br>・ HMI のセキュリティやフィールドのリスクの洗い出しのような課題には業界で一緒に取り組みたい。<br>・ コントローラで製品を差別化しており、技術は共通でなく自社研究している。セキュリティだけを切り出して他社と一緒には検討・対策をしにくい。<br>・ 長くて 1 週間くらい。必要ならば長期間でもよい。<br>・ SICE で認定している資格の保持者がテストベッドで研修受講してもよいだろう。 |
| 化学分野ユーザお | ・ 教育を受けるモチベーションが必要。制御での被害事例が少ない。 |

| | |
|---|---|
| よびインテグレータ | ・ 法的に強制されたり、被害発生で営業活動を制限されたり、工場が全停止したりという事態になれば必要性は高まるだろう。<br>・ 自発的に取るような資格は動機には弱すぎる。<br>・ 教える対象者のレベル差や要件の違いが大きい。どれも同じ内容では難しい。<br>・ セキュリティで悪事を教える印象を与える可能性はある。ブラックボックスにしておくのが安全という考え方もあるだろう。<br>・ 社員を研修に出しやすい環境にしてほしい（費用設定、期間等)。受講者には知識を社内や顧客に展開する役割を期待したい。 |
| ガス分野ユーザ | ・ テストベッド等を使いセキュリティ知識を教えたり、地方に勉強会への出張プレゼンをしてもらいたい。<br>・ 現段階ではセキュリティへの興味が無い。興味が無いため研修出張は不要である。<br>・ オペレータが現場を 2 日離れるのは難しい。 |
| 水道分野ユーザ | ・ 細かいことではなく、全般的なことと、取組の必要性をアピールしてほしい。 |
| 電力分野ユーザ | ・ 米国では、持ち運べる小さなデモシステムもあった。 |

④ベンダ技術者とその教育について

ベンダ技術者とその教育についての主要なコメントを表 2.11に示す。

**表 2.11　主要なコメント（ベンダ技術者とその教育について）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ ベンダの業務は製品開発と構築と保守の 3 つに分かれる。分けられずに重複する部分はある。<br>・ ベンダ向けカリキュラムは必要。最近の制御システムに関する知識（例：HMI のウィンドウズのセキュリティ）が遅れている、体系的な教育が求められる。<br>・ セキュリティと保守をうまく結び付けて、対応にコストが発生することをユーザに理解してもらうことが重要。<br>・ 脅威の現状や、技術の詳細については、セキュリティの基礎知識がないと理解が困難。 |

| | |
|---|---|
| | ・ 開発・構築におけるセキュリティの確保は重要。顧客に納める製品への感染が心配。<br>・ システムエンジニア（構築）向けにカリキュラムを用意したほうがよい。<br>・ セキュリティ要件にあわせて提案する能力を付ける必要がある。<br>・ 顧客分野によりエンジニアリングへの要求は異なる。<br>・ セキュアコーディングについては教育すべき。導入を示してより詳しい学習に誘導したい。<br>・ 製品開発者にはセキュアアプリケーション開発の手法が必要。 |
| 化学分野ユーザおよびインテグレータ | ・ エンジニアリングでは、構築を担当するがあまり深いところまでは入り込まない。要求をうけてどうするかを考える立場である。<br>・ ログをきちんと出力するアプリケーションの開発をしてほしい。トラブル解決し易くなる。<br>・ コントローラ以下の層は情報を持っているベンダが考えるべき。 |
| ガス分野ユーザ | ・ ベンダはセキュリティについて深く知っていて当然（特に自社の製品については）。<br>・ ベンダの技術者に標準的に教えることがあるかは疑問。ベンダ各社に既に教育体制がある。また各社で教えることは異なり共通化が難しいのではないか。 |
| 水道分野ユーザ | ・ ソフトウェアの変更等はベンダが行う。<br>・ インシデントについて判断がつかないならばベンダを呼ぶ。 |
| 電力分野ユーザ | ・ 更新周期が非常に長いため、ベンダの影響力が強い。プロトコルも独自仕様でオープンな規格になっていない。 |

⑤ユーザ技術者とその教育について

ユーザ技術者とその教育についての主要なコメントを表 2.12に示す。

**表 2.12　主要なコメント（ユーザ技術者とその教育について）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ 現場には、オペレータ、システム設計担当の技術者、システム保守担当の技術者がいるが、分野により役割の切り方は異なる。実際には１人ですべての役割を兼ねることも多い。<br>・ ユーザの技術者に身につけて欲しいのは脅威と問題意識。知識や経験を研修で持ち帰って、自社のシステムを見直し、考えて今後の対策を進めて欲しい。自分のことと思ってもらうことが重要。<br>・ 機器にセキュリティは作り付けで入っているからユーザが考える必要は無いという考え方では困る。<br>・ オペレータ、計装エンジニア（発注者）、保守エンジニアは別である。ベンダから提供する製品・システムでもアクセス権限を分けている。<br>・ ユーザの保守と設計のエンジニアは分けなくてもよい。仕様書作成や保守にそれぞれ対応する講座を作ればよい。 |
| 化学分野ユーザおよびインテグレータ | ・ ユーザ技術者向けの教育は重要である。<br>・ 保全担当者やエンジニア向けのカリキュラムは絶対に必要である。<br>・ セキュリティに関わる人は現場により異なりうる。オペレータ、技術部（保全）のいずれが関わるかは現場による。同じ会社でも工場により違うだろう。<br>・ ログはシステムエンジニアが見る。<br>・ プロセス異常についてはシミュレータがあるが、セキュリティについては想定外。ウイルスの場合のシミュレーションのシナリオがあるとよい。 |
| ガス分野ユーザ | ・ ユーザでも深く知っておく必要はある。<br>・ ユーザは基礎だけ習得すれば十分である。 |
| 水道分野ユーザ | ・ 初心者に受講してもらう形を考えてもよいのではないか。<br>・ ユーザはシステムについて専門知識はない。<br>・ 仕様や図案を用意するためには、ユーザにも知識が必要。 |
| 電力分野ユーザ | ・ ベンダの作り込みで直せる脆弱性についてユーザができることはないので事例として示す必要はない。 |

⑥オペレータとその教育について

オペレータとその教育についての主要なコメントを表 2.13に示す。

**表 2.13　主要なコメント（オペレータとその教育について）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ オペレータの位置づけ、定義は業種により異なる。それにより教育の要不要も異なる。<br>・ インシデントやトラブルの発生時には現場のオペレータに対応してもらうしかない。<br>・ 基本的にはオペレータには適切な担当者を呼ぶという対応を求める。<br>・ セキュリティのマニュアルを整備し、スキルと判断にまかせることが必要だろう。<br>・ マニュアル通りに行動する人だけでなく、設定等に触れるスキルを持つ人を想定する場合もある。<br>・ オペレータ教育は今後で良い。将来問題の切り分けが実行可能になればオペレータに教育が必要となる。<br>・ マニュアルを作り研修を行う上で、セキュリティについて整理するひな形があれば便利である。 |
| 化学分野ユーザおよびインテグレータ | ・ オペレータは基本的には言われたようにやる。ルールで禁止されていることはやらない。<br>・ エンジニア向け知識の基礎程度までは現場のオペレータには必要かもしれない。<br>・ エラーやログから現場のオペレータが発見することを考えた人材育成のカリキュラムがあっても良い。<br>・ オペレータによる不具合発生時の切り分けにおいてセキュリティが一項目になればよい。<br>・ 多くのオペレータはセキュリティを意識せず話しをしたがらない。<br>・ 様子がおかしいことに気付かせて相談させると良い。相談先の窓口を作っておけばトラブルは少ない。<br>・ オペレータのマニュアルは最終的には現場が作成している。<br>・ オペレータが出張して講習を受ける想定は無理。エンジニアに持ち帰らせる手法が良い。 |
| ガス分野ユーザ | ・ 難しい。教えるレベルは各社や規模により異なる。一概にはイメージできない。<br>・ オペレータに障害発生時の一時切り分けや、技術的な維持管理を求める場合もある。<br>・ セキュリティの基礎的教育・啓発は必要。 |

| | |
|---|---|
| 水道分野ユーザ | ・ オペレータは、基本的には技術員を呼ぶ対応だが、異常を発見する立場としてはカリキュラムが必要かもしれない。<br>・ 問題を最初に判断するには教育が必要。しかるべき対応をするためにルールや知識が要る。<br>・ オペレータに何を求めるかは、業態やルールによって異なる。<br>・ プラントの構成にもよるが、被害を広げない知識と、予防のための知識が必要。 |
| 電力分野ユーザ | ・ 脅威が現れたときにそれを把握できるかは重要である。 |

### (4)その他

その他（制御システム分野の人材育成等に関する問題意識・要望等）についての主要なコメントを表 2.14に示す。

**表 2.14　主要なコメント（その他）**

| 聴取先 | コメント |
|---|---|
| 制御製品ベンダ | ・ ユーザのトップ向けに啓発を行う必要性を感じる。経営層にセキュリティ対策の必要性について強く意識をもってほしい。必ずしも意識されていない。<br>・ エンジニアリングや保守の人について認証してはどうか。情報系では開発者や担当者に人の資格（例：CISSP）のようなものがあれば顧客は安心する。ある程度のセキュリティが実現できるものを作れると思えるものがある。 |
| 化学分野ユーザおよびインテグレータ | ・ パッチについては適用後に再起動が必要かどうかが分かりにくい。適用後に元に戻せるかどうかの情報があるとよい。 |
| ガス分野ユーザ | ・ セキュリティの教育を組織内でどう進めるのか。訓練方法を教えてほしい。<br>・ 普及啓発のために経営者への説明資料が欲しい。ビデオやパンフレットなど。現場へのセキュリティ予算増につながる。<br>・ 評価認証は規制をかけないと受けないところが出てくる。受けようという意識は弱い。規制が無ければ評価しようとしない。行政からの指導や通知でもよいから、国のアクションがないと自ら動き出すのは大変。<br>・ ユーザに対するセキュリティ認証のような制度は望んでいない。<br>・ 教科書が欲しい。モデルだけでなく実際のコンテンツをぜひ作っていただきたい。セキュリティ教育は教材が無い。カリキュラムがあれば是非利用したい。<br>・ カリキュラムの提供時期、対象者、利活用の方向性を定めるべきである。 |
| 水道分野ユーザ | ・ 制御システムの標準化は進められないだろうか。 |
| 電力分野ユーザ | ・ システムの認証を取得するかはユーザの判断なので強制はすべきではない。 |

## 2.4.分析

調査結果を踏まえ、得られた知見を以下にまとめる。

### (1)制御システムのセキュリティ確保への取組みの実態

制御システムにおけるセキュリティ上の脅威やリスクについて、技術者・経営者による更なる理解を促す必要があるとの意見が多かった。したがって、より明確に脅威・リスクを伝えるための工夫が必要である。たとえば、典型的な制御システムの構成図上でシナリオを示したり、具体的事例を示すといった形で、現実感を持ってもらう工夫が望まれている。

また、制御システムにおけるセキュリティ確保の取り組みとしては、「現場での気付き」「ログによる検知」「隔離し、機器の接続前にチェックする」といった運用上の対策が実施されており、今後はITセキュリティの技術を取り入れ、そうした対策を自動化することが望まれている。したがって、カリキュラムにおいては、現在実施されている取組みを踏まえた記載を行う必要がある。

さらに、制御システムのセキュリティ対策については、基礎的な技術・知識は情報システムと同様であるが、制御対象の周辺ではベンダの独自性が強いこと、技術的にも情報システムと異なる点があること、実装方法や運用上の要件や性質が情報システムとは異なること、制御システムごとに要件が異なるため考えながら対策を導入する必要があることが、特徴として挙げられた。したがって、ベースは情報システムにおけるセキュリティの知識項目や体系に置きながらも、制御システムとしての特徴的な点がより明らかになるよう記述を行う必要がある。

### (2)セキュリティ人材を中心とした人材育成の実態

制御システムに関わる人材育成については、大手ベンダでは教育計画に沿って制御システムエンジニア育成がなされている。手法としては現場でのOJT、外部の講習の利用が多い。また、訓練センターで制御製品に関する知識教育を行っている。したがって、そうした枠組みがあれば、既存の教育活動で利活用されることを考慮すべきである。

その一方、制御システムに関わる人材の大多数に勧められるような資格制度はないと考えられる。制御システム分野では、現場で経験を積みノウハウを習得することが重視される点、また、制御システム製品には各社の相違点

もあり､統一的な資格を作ることが難しい点も指摘されている｡したがって、資格取得をモチベーションとする方向は現状では適当ではなく、まずは現場で必要となるセキュリティに関する共通知識を整理して提示することに注力すべきであろう。

また、制御システムに関わる人材に対するセキュリティ教育については、ベンダ・ユーザのいずれにおいても、カリキュラムは整備されておらず、社内の少数の専門家の指導や社外講習が主である。ただし、情報システムのセキュリティに関する社員教育は全員になされており、共通の基礎知識となっていること、一部では、情報技術者向けカリキュラムも活用されていることから、モデルカリキュラムでは、情報セキュリティの一般知識（企業社員の常識程度のもの）については説明を省き、ある程度の知識はあるものとして記述を進めるものとする。

### (3)モデルカリキュラム（案）への意見

モデルカリキュラム（案）については、制御システムのイメージ上で実施可能なセキュリティの実装・運用を示すべき、脅威や被害の実際を伝えるべき、リスクや対策の必要性について理解を促すべき、といった意見が示された｡したがって､脅威やリスクについては導入部分の講座で重点的に取扱い、セキュリティの実装・運用に関しては、可能な限り制御システム上での適用を想定した書きぶりを行う。

体験型の学習については、模擬システム（模擬プラント）を用いたデモおよびトレーニングは有効でニーズもあることから、効果的な教育シナリオを策定すべきと考えられる。たとえば、いくつかの講座において実際に機器が動くところを見る、あるいは取り扱うような内容を盛り込む必要がある。

カリキュラムを利用した人材育成の実現方法については、研修（デモ／トレーニング、座学）と講演（地方出張）を組合せた取組みに期待する意見が得られた｡ただし､ベンダにおいては基礎的なカリキュラムの需要はあるが、ユーザにおいては受講へのモチベーションは高くない。 したがって､ユーザに対しては普及啓発を通じて脅威・リスクへの理解を促すことで、カリキュラムへの需要を高める展開が考えられる。

ベンダ技術者については、基礎知識を体系的に身につける手段が必要とされている。特に、構築担当者は提示されたセキュリティ要件に合わせ提案する能力が必要であり、開発担当者はセキュアコーディング／アプリケーション開発の知識が必要となる。したがって、カリキュラムにおいては、これらの指摘を意識して、項目および注釈を作成することが望まれる。

ユーザ技術者については、脅威の知識と問題意識を身につけ、現状のセキ

ュリティ対策の見直しができるようになることが期待されている。ただし、要求される知識の深さは、業務における役割により様々である。カリキュラムに沿った研修を受けたユーザ技術者が得た知識をもとに社内で普及啓発（教育）を担当する可能性も示唆された。したがって、モデルカリキュラムでは、脅威について理解を深めるだけでなく、現状の問題認識や改善も可能にする能力が得られることが望まれる。また、受講者が組織内でのオペレータ等を対象に、セキュリティについて指導する立場となることも視野に入れて、教育方針を記述する。

オペレータについては、期待される役割（必要な教育）が業種や規模により異なると考えられる。ただし、オペレータには現場で異常に気付き、担当者を呼ぶことが期待されるため、セキュリティに関する啓発と現場のマニュアル整備が必要とされている。しがたて、モデルカリキュラムにおいては、オペレータを主対象とはしないが、技術について知識をつけようとするオペレータが基礎的なコースを受講・参照することも想定する。特に「現場での気付き」の重要性には配慮する必要がある。

# 3. 制御システムのセキュリティに関する知識項目・スキルの策定

## 3.1. 策定の方針

知識項目･スキルについては､制御システム分野における実態に基づいて、同分野において重要度が高い知識項目・スキルを明確化し、これを含む一覧を作成することとした。

知識項目・スキルの一覧をとりまとめるにあたっては、以下の方針に基づくこととした。

・情報セキュリティの観点から網羅的・体系的に整理された知識項目・スキルをベースとする。

・特に制御システムのセキュリティにおいて重視される知識項目・スキルを明確化し、研修モデルカリキュラムの策定に資する。

## 3.2. 策定方法

知識項目・スキル一覧の策定にあたっては、まず、情報セキュリティにおける知識項目・スキルの体系を大枠として、これに制御システムのセキュリティに関する各種の文献から得た情報を加えて原案となるリストを作成した。

原案となるリストに、前述した制御システム分野関係者へのインタビュー調査を踏まえ、制御システム分野において重要度が高い知識項目・スキルについて修正を加えた。

このようにして作成したリスト案について、ワーキンググループにて集めた意見を参考に修正を行い､知識項目･スキルの一覧案としてとりまとめた。

知識項目・スキル一覧の策定にあたり参考とした文献とその扱いを以下に示す。

・情報セキュリティにおける知識項目・スキルの体系：

広い観点からは制御システムセキュリティは情報セキュリティに含まれうるものであるとの認識に基づき、知識項目・スキルの整理にあたって

は出発点として IPA の「共通キャリア・スキルフレームワーク 第 1 版」[1]を用いた。また、カリキュラムの具体例として IPA の「情報セキュリティ教本 改訂版」[2]を参考にした。

・制御システムのセキュリティに関する標準等：

制御システムにおいて実施すべき対策や制御システムに固有の観点について知見を得るために制御システムのセキュリティに関する標準やガイドライン等の文書を参考にした。具体的には、IEC 62443 シリーズ、CPNI「グッド・プラクティス・ガイド プロセス制御と SCADA セキュリティ」[3]、NIST SP800-82[4]を参照し、これらに示された知識項目・スキルを制御システムにおいて重要なものとして位置付けた。

・その他の制御システムのセキュリティに関係する報告書等：

制御システムのセキュリティ対策の実践において重視すべき知識項目・スキルを明らかにするために、特に現場に近い実践的な視点で取りまとめられた資料を参考とした。具体的には、経済産業省の「制御システムセキュリティ検討タスクフォース 人材ワーキンググループ」における検討[5] や、米国アイダホ国立研究所の Cyber Security Advanced Training のプログラムアジェンダ[6] を参考にしている。

これらの資料を参考に、知識項目・スキルの一覧案を作成し検討を加えた。検討では、一覧に記載された項目の妥当性だけでなく、制御システムに関わる者について、これらの知識項目・スキルに関して教育を必要とするかどう

---

[1] 情報処理推進機構「共通キャリア・スキルフレームワーク」
http://www.ipa.go.jp/jinzai/itss/csfv1.html

[2] 情報処理推進機構「情報セキュリティ教本 改訂版 - 組織の情報セキュリティ対策実践の手引き」 https://www.ipa.go.jp/security/publications/kyohon2/

[3] CPNI 「グッド・プラクティス・ガイド プロセス制御と SCADA セキュリティ（JPCERT/CC による和訳）」 https://www.jpcert.or.jp/ics/information02.html

[4] NIST 「Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security」 http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[5] 経済産業省 「制御システムセキュリティ検討タスクフォース報告書 中間とりまとめの公表について」
http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem_security/report01.html

[6] INL「2012 AGENDA Industrial Control Systems Cyber Security Advanced Training」https://secure.inl.gov/icsadv0213/includes/Agenda4Modules.pdf

かを検討し、研修モデルカリキュラムの策定における指針とした。これらの対象者の一覧を以下に示す。

・制御システムユーザ責任者
・制御システムユーザ技術者
・制御システムベンダ技術者（運用・保守サポート）
・制御システムベンダ技術者（システム構築）
・制御システムベンダ技術者（製品開発）

この案について､インタビューおよびワーキンググループにて意見を集め、修正を行い、本調査における成果として知識項目・スキルの一覧をとりまとめた。成果には各項目と研修モデルカリキュラムのコース・講座との対応付けを付記している。

# 4. 制御システムのセキュリティに関する研修モデルカリキュラムの策定

## 4.1. 策定の方針

制御システムのセキュリティに関する研修モデルカリキュラム（以下モデルカリキュラム）は、制御システムの運用や構築に従事する者に必要な情報セキュリティに関する知識項目・スキルについての整理を基に、研修カリキュラムを作成するための雛形をとりまとめたものである。

実際の研修にあたっては、このモデルカリキュラムを参考に、より詳細な研修コンテンツを作成することを想定している。

モデルカリキュラムの策定にあたっては、まず、前述したインタビュー調査に先立って原案（イメージ）を作成した。インタビューで得られたイメージに対する意見を踏まえて、あらためてモデルカリキュラムの設計を行うこととした。以下にその設計の方針を示す。

＜制御システムを対象とすることに対する基本方針＞

・ベースは情報システムにおけるセキュリティの知識項目や体系に置きながらも、制御システムとしての特徴的な点をより明確にする。
・現場で必要となるセキュリティに関する共通知識を整理して示す。
・制御システムにけるセキュリティ上の脅威・リスクを明確に伝えるための工夫を行う。

＜カリキュラムの作り方＞

・脅威やリスクについては導入部分の講座で重点的に取扱い、セキュリティの実装・運用に関しては、可能な限り制御システム上での適用を想定したものとする。
・「現場での気付き」「ログによる検知」「システムを隔離し、機器の接続前にチェックする」といった現在実施されている取組みを踏まえる。
・情報セキュリティの一般知識（企業社員の常識程度のもの）については説明を省き、ある程度の知識はあるものと想定し記述する。
・いくつかの講座において実際に機器が動くところを見る、あるいは取り扱うような内容を盛り込む。

＜想定される活用形態に対する配慮＞
・既存の教育活動で利活用されることを考慮する。
・ユーザに対し普及啓発を通じて脅威・リスクへの理解を促すことでカリキュラムへの需要を高めることも考慮する。

＜受講者について＞
・ベンダ技術者向けのカリキュラムにおいては、以下を意識し項目および注釈を作成する
  - 基礎知識を体系的に身につける
  - 構築担当者はセキュリティ要件に合わせ提案する能力を身につけることが重要である
  - 開発担当者にはセキュアコーディング/アプリケーション開発の知識が必要である
・ユーザ技術者向けのカリキュラムにおいては、以下を意識し項目および注釈を作成する
  - 脅威について理解を深めることが重要である
  - 自社のシステムにおいて対策を策定する能力を付けられるよう促す
  - 組織内でのオペレータ等を対象にセキュリティについて指導的な立場となることを想定し、教育の進め方について方針を示す
・カリキュラムにおいては、オペレータを主対象とはしない。技術について知識をつけようとするオペレータが基礎的なコースを受講・参照することも想定し、特に「現場での気付き」の重要性については記載する。

## 4.2. 策定方法

モデルカリキュラムの策定にあたっては、最初に、前述したインタビュー調査に先立って原案（イメージ）を作成した。この原案の作成にあたっては、主に経済産業省制御システムセキュリティ検討タスクフォース人材ワーキンググループでの検討結果[7]や既存のカリキュラム[8]を参考にした。

---

[7] 経済産業省 「制御システムセキュリティ検討タスクフォース報告書 中間とりまとめの公表について」
http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem_security/report01.html

[8] INL「2012 AGENDA Industrial Control Systems Cyber Security Advanced Training」https://secure.inl.gov/icsadv0213/includes/Agenda4Modules.pdf

前述したように、このイメージを見せながら制御システムに関する有識者にインタビューを行い、現場において必要とされる知識項目・スキルに関する意見や、効果的・具体的なカリキュラムの作成に有用な意見を聴取した。

インタビューで得られた意見、および知識項目・スキル一覧に関する検討を踏まえて、モデルカリキュラムの設計をあらためて行い、構成および内容を大幅に改めたモデルカリキュラム案を作成した。

このモデルカリキュラム案について､ワーキンググループにて意見を求め、修正を行って本調査における成果としてとりまとめた。

## 4.3. モデルカリキュラムの基本的な構成

### (1) 想定する対象者

特に重点的な教育が急務とされる、ユーザ企業の技術者とベンダ企業の技術者を対象にカリキュラムを作成することを念頭に置き、モデルカリキュラムには複数のコースを設定した。ユーザ企業におけるオペレータについては対象から外すこととした。[9]

### (2) コース

モデルカリキュラムは、制御システムユーザ企業の技術者と制御システムベンダ企業の技術者を主対象者に想定した。対象の立場と職務の内容を大掴みに捉えて、4 コース（基礎 1 コースおよび応用 3 コース）を一例として設定している。想定する対象者と各コースの対応を下図に示す。

[9] 制御システムセキュリティ（基礎）コースの冒頭の 3 講座は、制御システムをとりまく現状認識と脅威について取り扱うものである。これらの講座は経営層やオペレータに向けた普及啓発資料を作成する際に活用可能である。

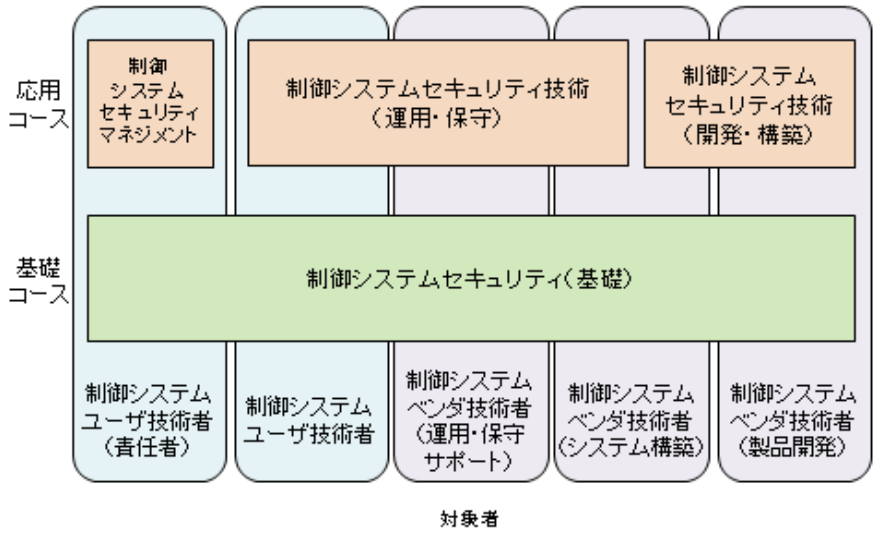


**図 4.1 モデルカリキュラムのコースと対象者**

制御システムセキュリティ技術（基礎）:

制御システムセキュリティに関する基礎的・全般的な知識やスキルの習得を狙うコース。他のコースの前提知識となる講座からなる。

制御システムセキュリティマネジメント:

応用コース。制御システムにおけるセキュリティマネジメントに関する講座からなる。

制御システムセキュリティ技術（保守・運用）:

応用コース。制御システムの保守・運用について、基礎コースでは扱えない、より詳細なセキュリティ関連技術知識を取り扱う。

制御システムセキュリティ技術（開発・構築）:

応用コース。制御システムの開発や構築を行う上で特に必要となるセキュリティ技術知識を取り扱う。

### (3) 留意点

・モデルカリキュラム全体の冒頭部分には、概要および使用方法を簡潔にまとめた説明をつけることとした。

・受講により、制御システム分野において現時点で特に実際に必要とされるセキュリティ関連知識を習得できることを目指した。情報セキュリティ分野における知識項目のすべてを完全に網羅するカリキュラムは意図していない。

・現在において必要と想定される知識項目のみを対象としている。このため、将来制御システム分野や脅威を含む情報環境が進展することで、これら以外の知識項目が必要となる可能性はある。

・講座の各回は 45～60 分で行うことを目安として検討した。各回の講座については講座内容の関連性を基に案として示した。実際のカリキュラムでの重点の置き方によって、回の構成や順番を変えることができる。

・各コースの内容の関連について各コースの冒頭に示すこととした。また、応用コースの学習にあたって基礎的な学習を済ませていることを前提とする場合に関しては講座内の該当箇所に「制御システムセキュリティ（基礎）」の関連講座について言及している。

## 4.4. 各コースの概要

以下にモデルカリキュラムの各コースの概要を示す。

### (1) 制御システムセキュリティ（基礎）

| 1. 制御システムセキュリティ（基礎） | |
|---|---|
| Ⅰ. 学習目標 | ・制御システムにおけるセキュリティリスクを理解する。<br>・制御システムの運用に必要なセキュリティ関連の基礎知識を理解する。<br>・制御システムに適したセキュリティ確保手法を理解する。 |
| Ⅱ. 概要 | 制御システム環境におけるセキュリティリスク、それに対応するセキュリティ要件、機能、構成について、制御システムの運用に必要な基礎知識を理解する。 |
| Ⅲ. 受講対象者 | ・制御システムに技術的に関わりうる全ての人。 |
| Ⅳ. 受講のメリット | ・制御システムユーザ企業の技術者（技術員、保守員等）：制御システムの運用、保守におけるセキュリティ問題に対処するために必要な知識が得られる。<br>・その他の者： 制御システムにおけるセキュリティ問題に関して基礎的な知識が得られる。 |
| Ⅴ. 受講者に前提として必要な知識等 | ・情報セキュリティについて一般常識程度のリテラシーを有すること。 |
| Ⅵ. このコースと他のコースの関係 | 本コースの講座のうち他のコースと内容に密接なつながりがある講座を以下に示す。本コースの内容についてより深く学習する場合にはこれらの上位のコースの講座を受講することが望ましい：<br><br>「制御システムセキュリティ（基礎）」<br>第 3 回<br>→ 「制御システムセキュリティマネジメント」<br><br>「制御システムセキュリティ（基礎）」<br>第 1 回、第 2 回、第 3 回、第 4 回、第 5 回、第 7 回<br>→ 「制御システムセキュリティ技術（運用・保守）」<br><br>「制御システムセキュリティ（基礎）」 |

| | |
|---|---|
| | 第 4 回、第 5 回<br>→ 「制御システムセキュリティ技術（開発・構築)」 |

| | 講座名 | 講座の概要 |
|---|---|---|
| 第 1 回 | 制御システムにおける脅威の現状 | 制御システムのセキュリティ上の脅威と対策に関する最新動向についてその概要を理解する。 |
| 第 2 回 | 攻撃のシナリオ | 制御システムへの攻撃を解説し、攻撃の具体的な再現を通じてセキュリティ上のリスクを理解する。 |
| 第 3 回 | 制御システムとビジネスリスク | 制御システムにおけるセキュリティマネジメント、リスク評価、インシデント対応等を理解する。 |
| 第 4 回 | セキュアな制御システムの構成 | セキュアな制御システムの構成方法について概要を理解する。 |
| 第 5 回 | セキュリティ対策 | パスワード／アカウント管理、マルウェア、機器接続、脆弱性対策について基礎を理解する。 |
| 第 6 回 | セキュリティ対策（続き） | 無線ネットワーク、リモート接続、バックアップ、物理的対策、人的対策について理解する。 |
| 第 7 回 | 攻撃の検知（基礎） | 監視の概要と手法のポイント、ログ管理について理解する。 |

## (2) 制御システムセキュリティマネジメント

| | |
|---|---|
| Ⅰ. 学習目標 | ・制御システムのセキュリティ維持に必要な管理手法を理解する。 |
| Ⅱ. 概要 | 制御システム環境におけるセキュリティリスク、制御システムのセキュリティ管理の手法に関して必要な知識を習得する。 |
| Ⅲ. 受講対象者 | ・主に制御システムユーザ企業における制御システム管理の責任者・現場の意思決定者を対象とする。 |
| Ⅳ. 受講のメリット | ・制御システムのセキュリティに関して、マネジメント、インシデント対応、人員や機材の管理、教育について必要な知識を身につけることができる。 |
| Ⅴ. 受講者に前提として必要な知識等 | 「制御システムセキュリティ（基礎)」の範囲の知識を有していること。<br>本コースのみを受講する想定であれば、以下の「このコースと他のコースの関係」の項に記載した「制御システムセキュリティ（基礎)」の各講座の内容について追加で学習しても良い。 |
| Ⅵ. このコースと他のコースの関係 | 本コースの講座と密接な関係のある「制御システムセキュリティ（基礎)」コースの講座を以下に示す：<br><br>「制御システムセキュリティマネジメント」第1回<br>←「制御システムセキュリティ（基礎)」第3回<br><br>「制御システムセキュリティマネジメント」第2回<br>←「制御システムセキュリティ（基礎)」第3回 |

| | 講座名 | 講座の概要 |
|---|---|---|
| 第1回 | セキュリティマネジメントと稼働の維持 | セキュリティマネジメント、リスク分析、規則等の整備について手法を理解するとともに、制御システムの稼働維持においてセキュリティを考慮することを学ぶ。 |
| 第2回 | インシデント対応と体制整備 | インシデント対応の概要と手順についてユーザ企業においてマネジメント層が果たす役割を中心に理解する。 |

※ 本コースの各講座は、それぞれ多くの重点項目を含む。必要に応じて1講座を単独で学習するカリキュラムを作成することも可能である。

## (3) 制御システムセキュリティ技術（運用・保守）

| | |
|---|---|
| Ⅰ. 学習目標 | ・制御システムに必要な情報セキュリティ関連知識をより深く理解する。<br>・制御システムに固有のセキュリティ確保手法をより深く理解する。 |
| Ⅱ. 概要 | 制御システム環境におけるセキュリティリスク、それに対応するセキュリティ要件、機能、構成について、制御システムの運用・保守の際に必要となる、より高度な知識を理解する。<br>（制御システムセキュリティ（基礎）よりも技術的に深い内容を含む） |
| Ⅲ. 受講対象者 | ・制御システムベンダ企業や制御システムエンジニアリング企業において、制御システムの運用・保守においてセキュリティ問題に対処する技術者を主な対象とする。<br>・ユーザ企業の技術者でより高度な知識の習得を目指す者も含む。<br>・制御システムベンダ企業や制御システムエンジニアリング企業においてシステム構築に関わる者を含む。 |
| Ⅳ. 受講のメリット | ・制御システムベンダ企業の技術者： 制御システムの運用、保守においてセキュリティ問題に対処するために必要な知識が得られる。また、制御システムベンダ企業の技術者が、システム導入・更新に際して提案を行うための知識をつけられる。<br>・制御システムユーザ企業の技術者： 運用や保守に関してより高度な知識を身につけられる。また、システム導入・更新時の仕様策定においてセキュリティ要件を定めることができるようになる。 |
| Ⅴ. 受講者に前提として必要な知識等 | 「制御システムセキュリティ（基礎）」コースの範囲の知識を有していること。<br>本コースのみを受講する想定であれば、以下の「このコースと他のコースの関係」の項に記載した「制御システムセキュリティ（基礎）」の各講座の内容について追加で学習しても良い。 |
| Ⅵ. このコースと他のコースの関係 | 本コースの講座と密接な関係のある「制御システムセキュリティ（基礎）」コースの講座を以下に示す：<br><br>「制御システムセキュリティ技術（運用・保守）」第1回<br>←「制御システムセキュリティ（基礎）」<br>第1回、第3回、第4回、第5回 |

| | |
|---|---|
| | 「制御システムセキュリティ技術（運用・保守)」第 2 回<br>←「制御システムセキュリティ（基礎)」 第 4 回<br><br>「制御システムセキュリティ技術（運用・保守)」第 3 回<br>←「制御システムセキュリティ（基礎)」 第 5 回 |

| | 講座名 | 講座の概要 |
|---|---|---|
| 第 1 回 | 制御システムへの脅威と対策手法 | 制御システムへの脅威、特にウイルス等のマルウェアとその対策手法の技術的詳細を理解する。 |
| 第 2 回 | 監視・防御とログ管理 | システムの防御や監視のための手法、ログ管理と分析について技術的詳細を理解する。 |
| 第 3 回 | 脆弱性と対策 | 脆弱性とその対策について手法と技術的詳細を理解する。 |

※ 本コースの各講座は、それぞれ多くの重点項目を含む。必要に応じて 1 講座を単独で学習するカリキュラムを作成することも可能である。

### (4) 制御システムセキュリティ技術（開発・構築）

| | |
|---|---|
| Ⅰ. 学習目標 | ・制御システム製品の開発・構築を行う上での要点を理解する。 |
| Ⅱ. 概要 | 制御システム環境におけるセキュリティリスク､それに対応するセキュリティ要件、機能、構成について、制御システムの開発・構築において必要な知識を理解する。<br>（制御システムセキュリティ（基礎）よりも技術的に深い内容を含む） |
| Ⅲ. 受講対象者 | ･制御システムベンダ企業やエンジニアリング企業において､制御システムの製品開発およびシステム構築を担当する技術者を対象に想定している |
| Ⅳ. 受講のメリット | ・制御システムベンダ企業の技術者： 制御システムの開発･構築において考慮すべきセキュリティについて必要な知識が得られる。 |
| Ⅴ. 受講者に前提として必要な知識等 | 「制御システムセキュリティ技術（基礎)」の範囲の知識を有していること。<br>本コースのみを受講する想定であれば、以下の「このコースと他のコースの関係」の項目に記載した「制御システムセキュリティ（基礎)」の各講座の内容について追加で学習しても良い。 |
| Ⅵ. このコースと他のコースの関係 | 本コースの講座と密接な関係のある「制御システムセキュリティ（基礎)」コースの講座を以下に示す：<br><br>「制御システムセキュリティ技術（開発・構築)」第 1 回<br>←「制御システムセキュリティ（基礎)」 第 4 回<br><br>「制御システムセキュリティ技術（開発・構築)」第 3 回<br>←「制御システムセキュリティ（基礎)」 第 5 回 |

| | 講座名 | 講座の概要 |
|---|---|---|
| 第 1 回 | セキュアな制御システムのデザイン | セキュアな制御システムを設計･計画するための手法と要点を理解する。 |
| 第 2 回 | セキュアなアプリケーションの実装 | セキュアなアプリケーションを実装する上で利用できる技術について要点を理解する。 |
| 第 3 回 | 制御システム製品ライフサイクルにおけるセキュリティ確保 | 制御システム製品のセキュリティ確保に関する要点を理解する。 |

※ 本コースの各講座は、それぞれ多くの重点項目を含む。必要に応じて１講座を単独で学習するカリキュラムを作成することも可能である。

## 4.5.カリキュラム作成において配慮すべき点

モデルカリキュラムの検討においては、モデルカリキュラムを用いたカリキュラムの作成において特に配慮すべき点について意見が示された。以下にこれらを整理して示す。

・応用的なコースについては、講座の各回だけを単独のコースとしてカリキュラムを作成することもできる。

・制御システムユーザにおけるセキュリティ対策の実現方法をより効率的・具体的に示す観点からは、セキュリティ関連標準への対応により重点を置いた内容とすることが有用である。特に ISO/IEC62443 に準拠した対策を制御システムに実装する方法をモデルで示す等の解説が効果的である。制御システム関連製品ベンダの技術者に対しては、これに加えて、コモンクライテリア相当の認証の取組みをモデルで解説すると良い。

本研修モデルカリキュラムは検討過程で制御システムのセキュリティに関連する標準として IEC 62443 シリーズを一部参考にしているが準拠を意図した策定は行っていない。参考のため IEC 62443-2-1 に示された要件項目と本モデルカリキュラムの講座項目との対応を別途作成することとした。

・機能安全とセキュリティの両立を図ることが、近い将来により重視される課題となる。教材でも簡単なモデルでの説明等から始めるべきである。

・各講座に示された事象や対策は、制御システムにおいてどのような位置・範囲におけるものであるかを理解することが重要である。カリキュラム作成においては、制御システムセキュリティ（基礎）コース 第 4 回に示したような制御システムのシステム構成のモデルを示し、これに照らし合わせて事象や対策について説明すると良い。

# 5. 考察

## 5.1. 制御システムセキュリティ教育に関する課題

本調査の過程で明らかになった、制御システムセキュリティの教育を推進する上での課題を以下に述べる。

### (1) 制御システムセキュリティの特徴的知識の継続的な抽出

本調査では、情報セキュリティの観点から網羅的・体系的に整理された知識項目・スキルをベースに、特に制御システムのセキュリティにおいて重視される知識項目・スキルを明確化することを目指したが、制御システムを扱うすべての分野の状況を網羅的に調査したものではない。制御システムセキュリティにおける特徴的な事項に関しては、今後も継続的に調査を行い、知識項目・スキルとして抽出し整理を続けていく必要がある。

また、本調査は現時点で必要と想定される知識項目・スキルのみを対象にしているため、制御システム分野や脅威を含む情報環境の進展に合わせて、継続的に内容の更新を行う必要もある。

### (2) 経営者層への普及啓発（理解の促進および危機意識の醸成）

今回作成した知識項目・スキル及び研修カリキュラムに基づいた教育を推進するには、組織の投資の権限を持つ経営者層の理解が最も重要となる。インタビュー調査の結果を見る限りにおいては、現時点で制御システム分野において制御システムセキュリティに関する自主的な研修の取り組みは殆どない。研修を新たに開始したり、既存の教育へ組み込んでいくことは、組織に一定のコストを負担させるものである。また、制御システムセキュリティの知識・スキルの習得は単発的な受講で実現できるものではなく、継続的に研修を受講することが重要である。

継続的な研修実施のための投資を組織内で確保するためには、経営者層が現在の制御システムのセキュリティに関し危機感を持ち教育の必要性を認識する必要がある。今回の知識項目・スキル及び研修のカリキュラムの普及に当たっても、まず経営者層に対してその有用性を理解してもらわなければならない。経営者層が危機意識を高めるためには、現状の制御システムのセキュリティ上の脅威を、自分の組織の制御システムにも起こりうる事態として

理解することが必要であり、そのためには脅威の実態を事例で示したり、自分の組織のチェックができる簡単なベンチマーク的なツールを活用した普及啓発策が効果的と考えられる。また、実際の研修の実施方法について具体的なイメージを持ってもらうためにも、研修の先行事例を紹介していくことも効果的である。

## 5.2.制御システムセキュリティ人材育成方策に関する課題

本調査では、インタビュー調査及び既存の情報セキュリティ及び制御システム関連の文献を基に制御システムセキュリティにかかわる知識項目・スキルを洗い出し、それらの項目をベースに制御システムセキュリティ（基礎）、制御システムマネジメント、制御システムセキュリティ技術（運用・保守）、制御システムセキュリティ技術（設計・開発）の 4 講座からなる研修のモデルカリキュラムを作成した。

これらの成果に基づいた人材育成の方策に関する課題を以下に述べる。

### (1)共有可能な知識に基づいた具体的なコンテンツ例の作成

今回の調査では研修のモデルカリキュラムを作成したが、実際に利用者が研修を行う際には、モデルカリキュラムを参考に独自のカリキュラムを作成し、さらにそれぞれの講座に適した教材(コンテンツ)を用意する必要がある。モデルカリキュラムの中でも、コンテンツの参考となる文献の例示は行ったものの、利用者自身がコンテンツを作成するのはややハードルが高い。また、知識項目・スキルの中には具体的に取り扱おうとすれば特定のシステムや製品に強く依存するためコンテンツ作成が難しい部分もある。

そこで、モデルカリキュラムの活用を推進する上でも、少なくとも必須講座については共有可能な知識を踏まえたモデルコンテンツを整備することが望ましいだろう。モデルコンテンツの作成に当たっては、単なる教科書的な内容ではなく、既に独自コンテンツを作成している組織等と連携しつつ、受講者のニーズを的確に取り込むことが望まれる。

### (2)より詳細かつ専門的な分野／業種／役割等への対応

モデルカリキュラムに基づいた教育を受講することで、受講者が制御システム分野において現時点で特に必要とされるセキュリティ関連知識を習得できることを目指したが、実際に制御システムを扱う分野・業種は非常に多岐にわたるため、内容としては制御システム全般に適用しうる汎用的なものと

なっている。モデルカリキュラムは、制御システムユーザ企業の技術者と制御システムベンダ企業の技術者を主な対象者としたうえで、対象の立場と職務の内容を大掴みに捉えており、基本的には利用者側が自身の組織の人材の業務内容・レベルに合わせてカリキュラムをアレンジして利用することを想定している。

一方、個別の分野や特定の制御システムに特化した研修に対するニーズも高いのであれば、より専門的な講座からなるモデルカリキュラム作成が必要となる。そのためには、各分野・業種・ユーザ/ベンダによって異なる組織の人材構成を調査したうえでモデル化し、各カテゴリで求められる知識項目・スキルを体系的に整理する必要がある。また、こうした取り組みは現在の制御システム分野におけるセキュリティ人材の過不足状況の実態を把握する上でも有効と考えられる。

### (3)制御システムセキュリティ人材ニーズの把握と発掘

制御システムの人材育成を継続的な取り組みとして実現するため、知識項目・スキル及び研修のモデルカリキュラムの継続的な更新と並行して、幅広く人材育成推進策を打ち出す必要がある。まずは、現状の制御システム分野におけるセキュリティ人材の不足状況を把握することが、具体的な施策の検討につながっていくものと考えられる。

一方で、根本的には制御システム分野において、セキュリティ人材のニーズが高まることが、人材の育成にもつながるため、前述の制御システムセキュリティセンター等の外部機関とも連携して、制御システムセキュリティへの意識向上について普及啓発を進めることが最重要課題である。

## 5.3.今後の展開

### (1)モデルカリキュラムの活用

今回策定した研修のモデルカリキュラムの利用形態として以下の 3 つを想定する。

1. 教育機関（ビジネス等含む）による教育事業／サービスへの利用
2. 制御システムユーザ／ベンダの社内教育への直接利用
3. 制御システムベンダやセキュリティベンダによる制御システムユーザ向けプログラムへの利用

1 つ目の形態として、教育機関による教育事業／サービスへの利用が考えられる。教育機関として具体的には制御システムのユーザ／ベンダの業界団体、教育ビジネスを展開する事業者及び大学・専門学校等が想定される。特に、制御システムのユーザ／ベンダの業界団体においては、既に団体内で制御システムに関する知見が蓄積されており、参加企業・組織とも密接な関係にあるため、比較的早期に研修を開始できる可能性がある。平成 24 年度に設置された技術研究組合制御システムセキュリティセンターでは、平成 25 年度から制御システムセキュリティに関する人材育成事業の開始を予定しており、ここでモデルカリキュラムが有効に活用されることが期待される。このような団体と積極的に情報共有をしていくことで、研修を実施した上での検証結果をモデルカリキュラムの更新にフィードバックすることも可能である。

一方、教育ビジネスや大学・専門学校における利用に関しては、サービスとして成立するかニーズを見極める必要があるため、先行する業界団体の動向をみながらの展開となることが予想される。

2 つ目の形態として制御システム分野のユーザ／ベンダの社内教育への直接利用が考えられる。制御システム分野のユーザ／ベンダが直接利用することで、自社が扱う制御システムに特化した形で内容を詳細化することが可能であり、より実践的な教育が行われることが期待される。ただし、各組織でカリキュラムやコンテンツを準備する負担がかかるため、活用方法のガイドやモデルコンテンツ等を提供するなどのサポートが必要と考えられる。

また、1 つ目の形態の例として挙げた制御システムのユーザ／ベンダの業

界団体が提供する研修をユーザ／ベンダの研修担当者が受講し、その内容を自社の組織に展開するという流れも想定される。

3 つ目の形態として、制御システムベンダやセキュリティベンダによる制御システムユーザ向けプログラムへの利用が想定される。制御システムにおけるセキュリティを直接製品・サービスという形で提供するベンダ自身が研修を行うことで、専門的で実践的な研修の実施が期待される。また、ベンダがユーザに対して通常行っている従来の制御システムの取扱説明等に、モデルカリキュラムに基づいたセキュリティの内容を取り込むことで、ユーザが自然にセキュリティの研修を受けるという流れが生まれることが期待される。

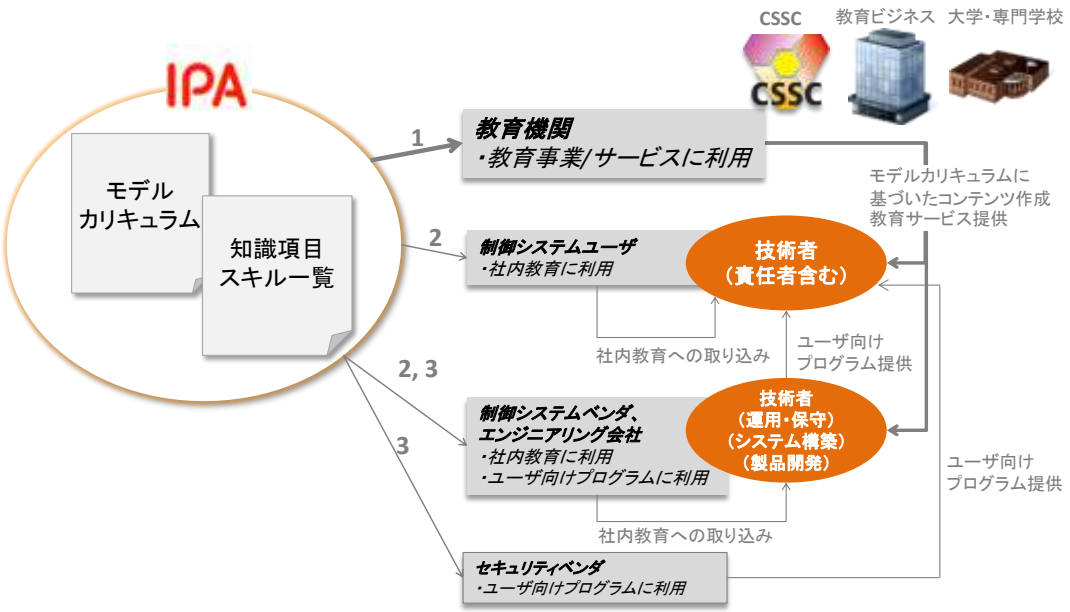


**図 5-1　成果物の活用イメージ**

### (2) 知識項目・スキルおよびモデルカリキュラムの継続的更新

制御システムを取り巻く技術やセキュリティ上の脅威は急速に変化しており、今回作成した研修のモデルカリキュラムもこのような環境の変化に合わせて継続的に更新していく必要がある。また、利用者自身もモデルカリキュラムにある内容だけを習得するのではなく、常に最新の情報を収集し、自主的に研修コンテンツを更新していくような柔軟な使い方が求められる。

今後のモデルカリキュラムの改訂にあたっては、利用者のニーズに応えたカリキュラムとするためにも、想定する利用者に実際にモデルカリキュラムを見て、使ってもらうことで、率直な評価を頂くことが第 1 歩となる。

今回のモデルカリキュラムは、制御システムセキュリティに特化した研修

カリキュラムとして、世界的にも前例の少ない先進的な取り組みである。近年日本と同様に制御システムセキュリティに取組む諸外国においても制御システムセキュリティの普及啓発及び人材育成は重要な課題として共通に認識されている。今回策定したモデルカリキュラムを国内のみならずに海外に対しても積極的に発信することで、国内外の制御システム関連団体と連携した教育の展開も模索していくべきである。