2019 年度「専修学校による地域産業中核的人材養成」事業

成 果 報 告 書

本報告書は、文部科学省の生涯学習振興事業委託費による
委託事業として、一般社団法人全国専門学校情報教育協会
が実施した 2019 年度「専修学校による地域産業中核的
人材養成事業」の成果をとりまとめたものです。

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

１．事業概要

１　委託事業の内容

Society5.0 等対応カリキュラムの開発・実証

２．事業名

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

３．分野

工業分野(情報セキュリティ)

４．代表機関

法人名　　一般社団法人全国専門学校情報教育協会

所在地　　〒164-0003　東京都中野区東中野 1-57-8　辻沢ビル３F

５．構成機関・構成員等

（１）教育機関

1　学校法人岩崎学園　情報科学専門学校

2　学校法人桑園学園　札幌情報未来専門学校

3　学校法人中村学園　専門学校静岡電子情報カレッジ

4　学校法人龍澤学園　盛岡情報ビジネス専門学校

5　学校法人中央総合学園　専門学校中央情報大学校

6　学校法人三橋学園　船橋情報ビジネス専門学校

7　学校法人片柳学園　日本工学院専門学校

8　学校法人中央情報学園　早稲田文理専門学校

9　学校法人穴吹学園　専門学校穴吹コンピュータカレッジ

10　学校法人河原学園　河原電子ビジネス専門学校

11　学校法人龍馬学園　高知情報ビジネス＆フード専門学校

12　学校法人麻生塾　麻生情報ビジネス専門学校

13　学校法人 KBC 学園　国際電子ビジネス専門学校

（２）企業・団体

1　株式会社ディアイティ

2　株式会社ラック

3　株式会社ウチダ人材開発センタ

4　株式会社サンライズ・クリエイティブ

5　株式会社日本教育ネットワークコンソシアム

6　NPO 日本ネットワークセキュリティ協会

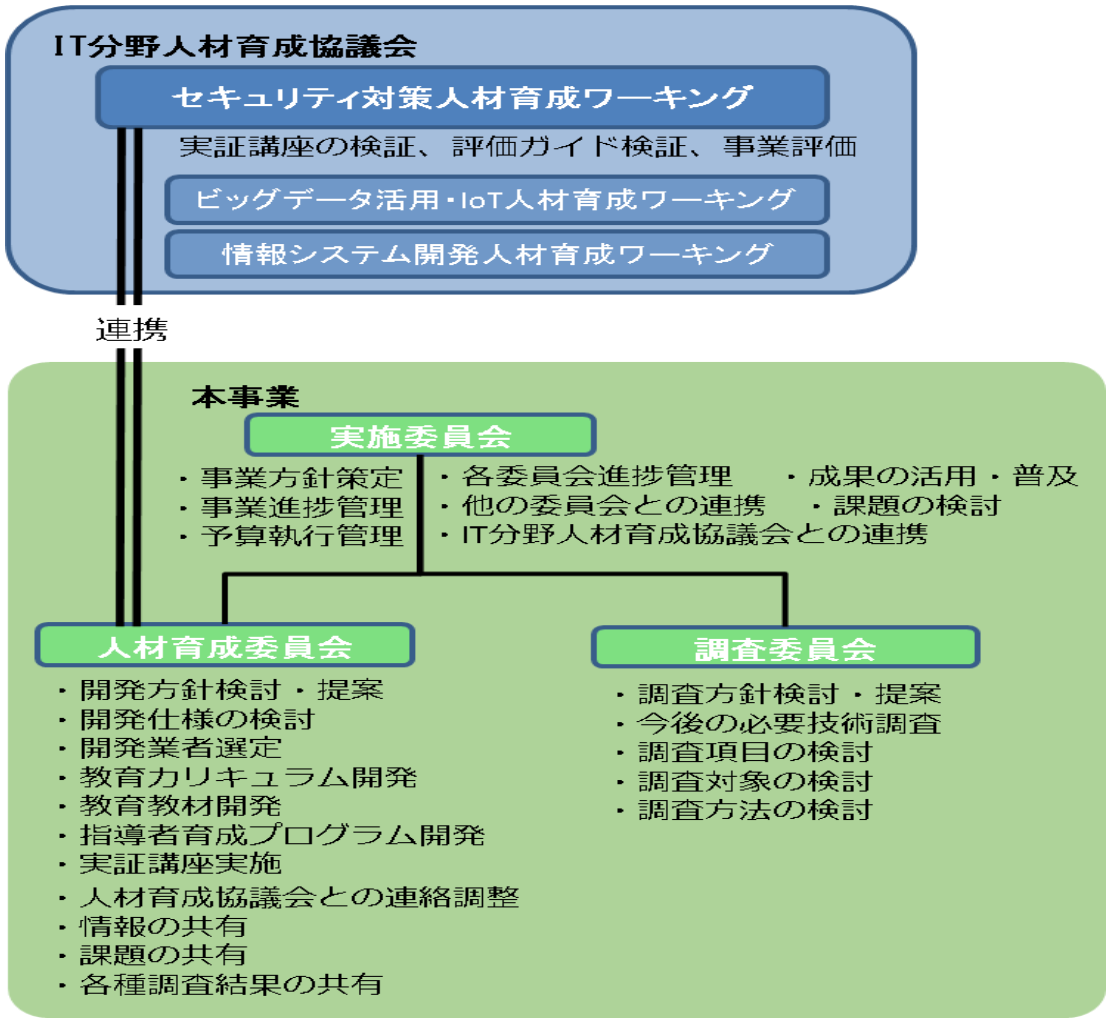
7　一般社団法人クラウド利用促進機構

8　一般社団法人全国専門学校情報教育協会

（３）行政機関

1　独立行政法人情報処理推進機構

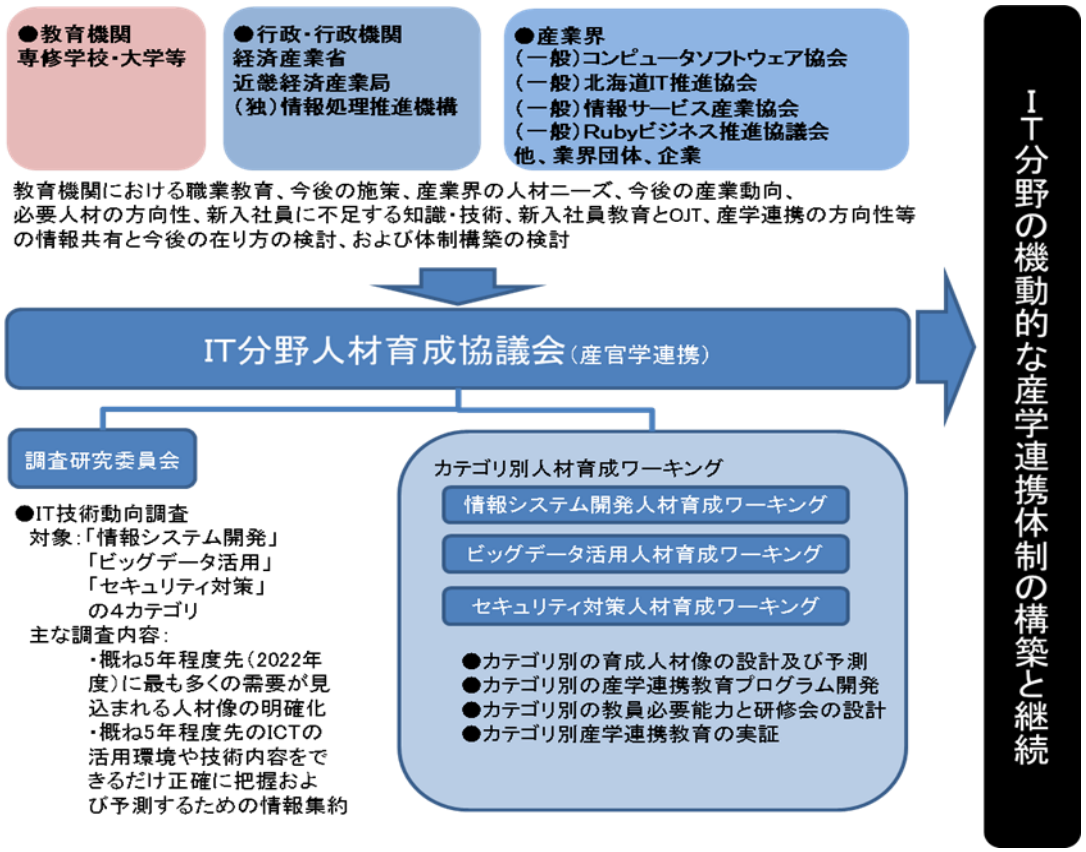
（４）事業の実施体制（イメージ）



IT 分野人材育成協議会との連携

IT 分野人材育成協議会の検討・協議する育成人材像の情報の提供を受けて、本事業で行う Society5.0 への対応実態調査等の情報と合わせて検討し、IT 人材育成協議会と情報共有するとともに、本事業では教育プログラム開発、実証を役割として担う。教育プログラム開発及び実証講座実施に対して、IT 分野人材育成協議会から産学連携方法の情報提供や連携先情報、専門人材の紹介、業界団体の協力等の支援で連携する。

IT 分野人材育成協議会（体制イメージ）



（５）各機関の役割・協力事項について

○教育機関

・育成人材像の明確化（専門学校の教育領域の検討）

・技術調査への協力（情報セキュリティの求人企業、学生就職先企業の紹介）

・教育プログラムの検討～作成協力（本事業で開発予定の教育カリキュラム原稿（案）の作成、シラバスの必要項目洗い出し、教育教材の必要項目洗い出しと参考資料の提供）

・現在実施されている関連教育カリキュラム・シラバス・使用教材の提供
・指導者育成プログラム作成協力
（本事業で開発予定の育成プログラム（案）の作成）
・実証講座実施協力（会場の提供、受講者募集（学生・OB への告知等）
・指導者育成研修会運営・実施協力（会場提供、受講講師募集）
・モデルカリキュラム実証協力と正規課程への導入検討
・成果の活用

○企業・団体
・産業界の Society5.0 への対応実態調査支援・協力（調査依頼先紹介、会員企業一覧の提供、調査項目の検討・助言）
・情報セキュリティ技術の最新情報提供（業界のトレンド、近年実用化の見込まれる技術情報等の提供）
・今後の情報セキュリティ技術者必要技術調査支援・協力（今後の情報セキュリティに関する企業としての方針や方向性と本事業の目指すべき方法への助言、業界団体等で行う調査資料の提供）
・産学連携教育カリキュラム作成支援・協力（産学連携における企業側のニーズ及び実施可能な連携に関する情報提供及び IT 分野人材育成協議会の作成する産学連携手法に関する情報セキュリティ企業からの意見集約と助言）
・企業内実習実証実施協力（企業内実習実施先の紹介、自社による企業内実習実施・運営）
・学内実習実証実施協力（講師派遣、課題（案）作成、学生評価、取組み所感）
・教育プログラムの評価、検証協力（実証講座の結果・成果に対する評価、改善の提案）

○IT 分野人材育成協議会
平成 29 年度より本会が受託している文部科学省の産学連携体制の整備事業で組織した産学官連携のコンソーシアム
教育機関　専門学校 27 校　企業　11 社、企業団体　5 団体、行政機関　2 機関が参加しています

企業団体では　一般社団法人コンピュータソフトウェア協会、一般社団法人Rubyビジネス推進協議会、一般社団法人東京都情報産業協会等が参加しています。

行政機関では、経済産業省近畿経済産業局地域経済部次世代産業・情報政策課、独立行政法人情報処理推進機構（IPA）が参加しています。

本事業は、上記事業と連携した、情報セキュリティ領域の人材育成についての取り組みとなります。

・セキュリティ対策分野育成人材像の共有
・教員の必要能力の情報共有
・産学連携教育の在り方に関する情報提供
・業界団体、行政からの意見集約と情報共有
・実証講座の検証結果確認
・評価ガイドの検証
・事業評価

６．事業の内容等

（１）本年度事業の趣旨・目的等について

ⅰ）事業の趣旨・目的

近年、携帯電話・スマートフォンをはじめ多くの機器がインターネットに接続され、便利なサービスが提供されるようになっている。Society5.0 では、あらゆる物がネットワークに接続し、双方向で情報の受渡を行い、サイバー空間とフィジカル空間を融合し、国民の生活を豊かにすることが想定されている。一方でネットワークに接続する機器の増加に伴い、情報セキュリティに関するリスクが増大し、重大な問題を引き起こすことが予測され、課題となっている。また、今後さらに増加するリスクに対応する情報セキュリティ人材の不足が指摘されている。

本事業では、IT 分野人材育成協議会と連携し、今後予測される情報セキュリティのリスクに対して、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を行うための教育プログラムを開発する。主にサイバー攻撃に対する対処、情報リスクに対応したセキュアなシステム開発技術を習得するための教育カリキュラム、教育教材を整備し、情報セキュリティ人材育成のモデルとして取りまとめる。情報系専門学校を中心にモデルカリキュラムの導入を促進し、Society5.0 時代に対応した情報セキュリティ技術者の育成を推進する。

ⅱ）目指すべき人材像・学習成果

情報システム開発技術者・情報セキュリティ技術者を目指す者を対象に、サイバー攻撃に対する対処技術とセキュアな情報システム開発技術を用い、情報システム・ネットワークシステムを開発できる情報セキュリティ技術者。

（２）当該教育カリキュラム・プログラムが必要な背景について

これまでパソコンによるインターネット通信が中心であった情報通信ネットワークは、スマートフォンや新たなデバイスの進展により、デバイス等の相互通信にも使用されるようになり、ネットワークに接続されている機器は、劇的に増加している。また、日本が今後目指す Society5.0 の社会では、すべての人を取り巻く機器がネットワークに接続され、情報を相互にやり取りすることが想定されているため、さらにネットワーク上の機器は増加が続くと予測される。（右上図は、IoT 機器数の推移と予測：５年で倍近くに増加している）

ネットワークに接続される機器の増加に伴い、それと比例して情報セキュリティのリスクも増加することとなり、 その対応と同時に情報システム設計の段階からセキュリティが確保されることが重要となっている。

従来の DDos 攻撃、リスト型攻撃等に加え、新種のコンピュータウィルスやランサムウェア等のリスクも増大している（右下図はランサムウェア増加の状況）。また、これまでパソコンを標的としていたウィルス等が、IoT 機器、スマートフォン等を新たに攻撃目標とし、感染を拡大させている。2017 年 11 月の調査結果によれば、他の IoT 機器への攻撃の観測結果に基づく、ウィルスに感染したと見られる IoT 機器の台数は、470,212 台（内日本国内の機器は 27,693 台）となっている。（平成 30 年度情報セキュリティ白書）　スマートフォンでは、不正アプリによる個人情報の抜き取り等の被害が増加している。

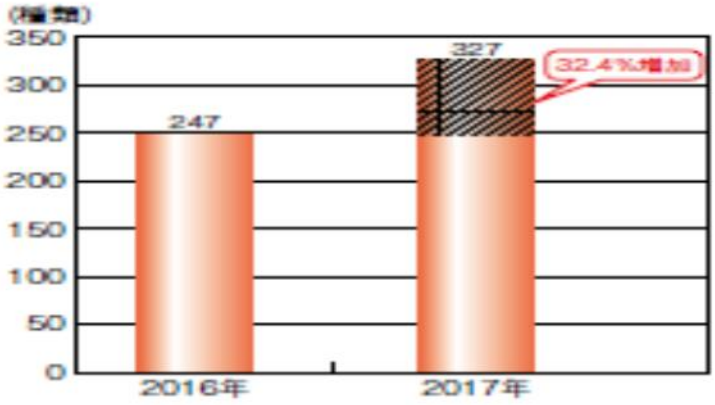
Society5.0 で目指す社会では、情報システムや情報通信ネットワークは、社会の根幹を支える基盤となり、情報リスクへの対応・情報セキュリティの確保は、最も重要な技術の一つである。

世界の IoT デバイス数の推移及び予測　　出展：平成 30 年度情報通信白書

	2014	2015	2016	2017	2018	2019	2020
合計	170.7	205.1	241.0	274.9	310.5	354.4	403.0
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.06	0.07	0.07
自動車	3.8	4.7	6.0	7.5	9.2	11.6	14.4
医療	2.0	2.3	2.8	3.4	4.1	5.0	6.1
産業用途	18.2	24.9	32.7	42.4	54.5	72.8	94.9
コンピューター	19.3	21.1	22.0	22.2	22.1	22.0	21.9
コンシューマー	33.8	38.9	45.3	52.0	59.3	67.2	76.3
通信	93.6	113.1	132.2	147.3	161.2	175.7	189.3

（出典）IHS Technology

ランサムウェア数の比較：情報セキュリティ白書 2018



■図 1-1-2　新たに確認されたランサムウェアファミリー数の年別比較
(出典)トレンドマイクロ社「2017 年年間セキュリティラウンドアップ」を基に IPA が編集

2012 年ディープラーニング技術の応用による AI（人工知能）の認識・判断率が飛躍的に向上し、実用化へ大きく前進した。既にいくつかの領域では、AI（人工知能）システムが実用化され、現実の社会で活用されている。クラウドコンピューティングが進展し、大容量のデータの分散管理、並列処理技術等により、大容量のデータの保存、分析処理が可能となるとともに、パソコンによるデータばかりでなく、組込み機器（センサー、位置情報、稼働等）をネットワークに接続し、取得できるデータの蓄積も行われ、そのデータを活用・分析し、社会の課題解決に利用できる状態になりつつある。Society5.0 実現に向けて、情報システムや IoT 機器、クラウドサービスが連携し、今後さらに多くの情報がネットワーク上を行きかう状況が予測される。

ネットワークに接続された機器の増加、流通する情報量の増加は、情報セキュリティに対してもリスク増加を招いている。しかしながら、急速に増大した IoT 機器のネットワークへの接続、情報流通量の増加等に情報セキュリティの対応が追付いていない状況にある。また、対応する情報セキュリティ人材の不足が大きな課題となっている（右下図）

情報セキュリティ技術について、新たな技術の進展や新たな機器のネットワークへの接続等により、従来の対策に加え、情報システム、ネットワークシステムの設計・開発段階から将来的なセキュリティリスクも踏まえた構築が必要となっている

これまで情報リスクへの対応は、問題が起こった後に対応する対処療法が中心であった。Society5.0 では、情報システム・ネットワークシステムは、社会を支える基盤として最も重要な位置づけであり、情報の流通が中断するようなことはあってはなら

ない。このため、サイバー攻撃・コンピュータウィルス等に対する対処療法は重要であり、今後も継続的に行うことが必要であるが、情報システムやネットワークシステムを設計・開発する段階から、既知の情報リスクへの対策を施し、今後起こりうるリスクに対応することが求められている。

Society5.0 実現と維持発展のため、技術的な観点から、既知のサイバーセキュリティ技術とセキュリティホールに対応したセキュアな情報システムの設計・開発技術、未知の脅威には、発生と同時に適切な対応が取れ、以降の情報システム設計・開発においては、経験から対策を講じることができる技術を有する情報セキュリティ人材育成が必要不可欠である。

出展：経済産業省「平成 26 年度補正先端課題に対応したベンチャー事業化支援等事業」　IT 人材の最新動向と将来推計に関する調査結果

今後、日本の目指す Society5.0 実現のためには、これまでに無い新たな情報セキュリティを確立することが、重要であり、安心・安全なサイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムが必要不可欠である。

本事業で開発をする教育プログラムは、情報システムの設計段階から安心・安全を設計し、今後拡大する IoT 機器の通信の脅威への対応、通信ネットワークのセキュリティ設計、サイバー攻撃の予防と対処技術、運用における安心・安全の確保技術等を

含めた情報セキュリティ・サイバーセキュリティを学習内容とする、これまでに行われていなかったSociety5.0に対応できる情報システム技術者の育成を目指ている。

（3）開発する教育カリキュラム・プログラムの概要

ⅰ）名称

情報セキュリティ対策エンジニア学科　教育プログラム

ⅱ）内容

本事業では、サイバー攻撃に対応するためのサイバーセキュリティ技術（攻撃を受けた際の対処法とシステムの脆弱性診断技術）と予防的に情報リスクに強い設計を用いて、攻撃等が行われにくい情報システム設計・開発技術を有する IT 技術者を養成するための教育カリキュラム・プログラムを開発する。

名称：情報セキュリティ対策エンジニア学科

ポリシー：既知のサイバーセキュリティ技術とセキュリティホールに対応したセキュアな情報システムの設計・開発を行うことができ、未知の脅威には、発生と同時に適切な対応が取れ、以降の情報システム設計・開発においては、経験から対策を講じることができる IT 技術者を育成する。 実践的な職業人育成のため、情報セキュリティ専門企業と連携し、セキュアな情報システム設計・開発および情報リスクに関する最新技術動向の情報提供を受けると共に産業界に求められる
技術習得のため、演習、企業内実習を取り入れた教育課程を設計する。

科目構成：

コンピュータシステム基礎	180 時間
セキュリティ基礎	240 時間
情報セキュリティの設計と構築	420 時間
産学連携教育	60 時間

各科目の目的：

■コンピュータシステム基礎（既存の教育プログラムを活用）
IT 技術者としてコンピュータを使用するための基本となる、ソフトウェア、ハードウェア、ネットワーク、データベース、プログラミング、運用・保守に関する基本知識及び技術を学習する

■セキュリティ基礎（既存の教育プログラムを活用）
情報セキュリティに携わる技術者として、セキュリティの基本技術、ネットワークの構造とセキュリティリスクとその対応、運用おけるセキュリティの確保等の専門知識と技術を学習する

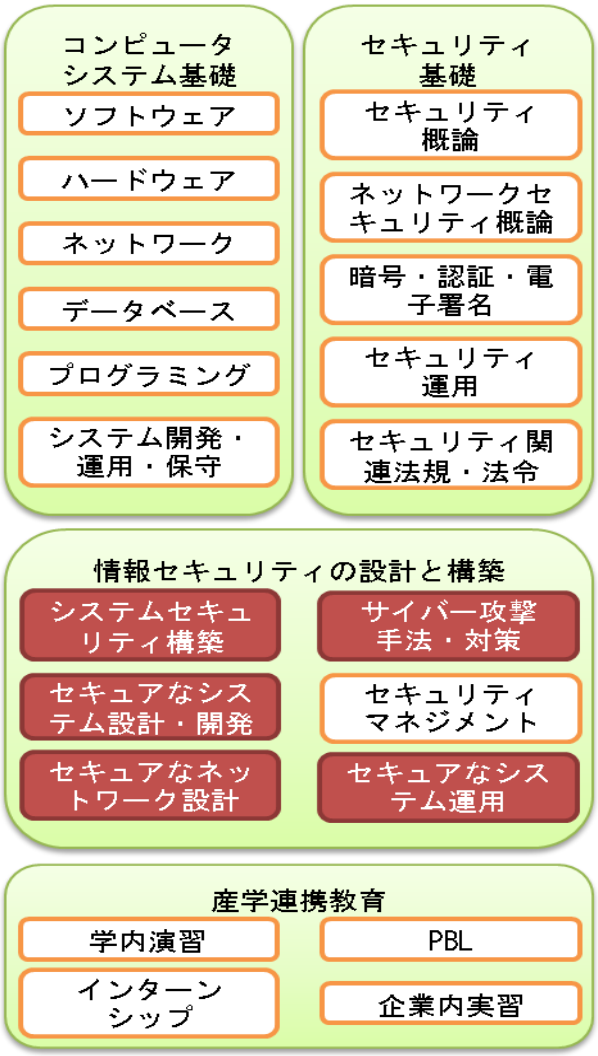
■情報セキュリティの設計と構築（本事業で開発する教育プログラム）

セキュアな情報システム設計・開発の専門知識・技術を学習する。
サイバー攻撃の手口と対応策及び攻撃リスクと脆弱性の診断に関する専門知識・技術を学習する

■産学連携教育（既存の教育プログラムを活用）

実践的職業教育のため、産学が連携した実習・演習を行い、実務で通用する技術習得を目指す。

教育カリキュラムのイメージ



●開発する教育カリキュラム・プログラム

・モデル・カリキュラム

・システムセキュリティ構築技術　教育カリキュラムと教材

情報システム設計・開発時点でのセキュリティ設計、不正アクセス防止対策、ウィルス感染予防対策、通信におけるセキュリティの確保、新たな脅威に対する対応の設計

・セキュアなネットワーク設計技術　教育カリキュラムと教材
ネットワークセキュリティの設計、安全な通信の確保、暗号化技術、ファイアーウォールの設計、IoT 機器のネットワークセキュリティと脅威の対応技術、インシデント発生時の対応と設計段階での予防と保守設定

・セキュアなシステム設計・開発技術　教育カリキュラムと教材
安全な情報システム開発、IoT 機器の脅威、通信規格と安全性の確保、セキュリティホールのふさぎ方、データ通信における暗号化の脅威と対処

・サイバー攻撃手法・対策技術　教育カリキュラムと教材
既知のサイバー攻撃の種類と対処技術、今後の脅威の予測と対応策の検討
ハッキング技術とクラックに対する対処、サイバー攻撃発生時の対応方法

・セキュアなシステム運用技術　教育カリキュラムと教材
セキュリティホールの認知と安全確保、システムメンテナンス、OS 等のアップデートとセキュリティパッチ、新たな脅威に対するシステム運用

・教員育成研修プログラム（カリキュラム・スケジュール・演習課題）
・指導書
・評価ガイド

昨年度調査の結果、

1．エントリーレベルの情報システム技術者については、情報セキュリティの技術は、特に必要は無い。
※情報システム開発においては、設計段階でセキュリティガイドライン等の仕様が組み込まれているため、個々人が保有している必要はない

2．エントリーレベルの情報システム技術者は、情報セキュリティについての知識と意識を持つことが重要である。

3．情報セキュリティの専門企業における技術者は、分析ツール等の技術が必要であり、習得している人材が求められている。

4．情報システム開発に携わる技術者は、情報セキュリティ領域に特有である情報倫理を学習する必要がある。

５．Society5.0 等の進展により、多くの機器や情報システムが接続し連携することが予測されるため、これまで教育されていなかったシステム間連携の教育プログラムの整備が急務である。

上記の結果から本事業では、①情報システム技術者に求められる情報セキュリティの知識・技術、②情報セキュリティ専門企業の技術者に必要な知識・技術、③情報セキュリティにおける情報倫理、④システム間連携の４つの領域の教育プログラムの整備を行うことを目指している。

①情報システム技術者に求められる情報セキュリティの知識・技術

現状は、「エントリーレベルの技術者が必要な技術は特に無く、情報セキュリティについての知識と意識が重要である」との調査結果であるが、今後、日本が目指す Society5.0 の社会では、爆発的に多くの機器がネットワークに接続されること、また、IoT 機器や情報システムが社会を支える基盤となり、不具合等が発生した場合の損害が膨大になること等の状況を踏まえ、全方位で情報リスクに対応し、セキュリティの確保ができる人材の育成を目標とする。

②情報セキュリティ専門企業の技術者に必要な知識・技術

情報セキュリティの専門企業における技術者が必要な知識・技術として、アクセスログ等の分析ツールの技術が重要である。また、既知の脅威に対応するディフェンス技術とともに新たな脅威に対する発見や予防的措置の対応能力が求められる。

特に、サイバー攻撃に対応する技術は、重要であり、今後の社会を支える基盤となる。

③情報セキュリティにおける情報倫理

情報を扱う技術者としての倫理（行動規範）を中心に、個人としての情報倫理、組織としての情報倫理からセキュリティマネジメントを学習し、情報システム開発における情報倫理を技術者個々人が理解することが情報セキュリティを確保する上で最も重要である。

④システム間連携

Society5.0 の目指す社会は、多くの機器や情報システムがネットワークを介して接続し連携することで実現をするが、情報システム同士の連携において、その信頼性の確保が重要である。システム A とシステム B が接続、連携するときに、システム A はどのようにシステム B を信頼するのか、また、逆の場合、システム B はどのように A の信頼を確認するのかが重要で

ある。システム間連携においては、連携するシステムにどのように信頼されるかを設計することが重要であり、情報セキュリティの確保は最低限の要件であり、その他の信頼確保の要素を学習する必要がある。

本事業では、上記状況を受けて、 Society5.0 実現と維持発展のため、技術的な観点から、既知のサイバーセキュリティ技術とセキュリティホールに対応したセキュアな情報システムの診断や既知の脅威に対する対応を行うことができ、未知の脅威には、発生と同時に適切な対応が取れ、以降の情報システム設計・開発においては、経験から対策を講じることができる IT 技術者を育成する。

情報セキュリティ確保の内容として、セキュリティポリシーの策定、製品仕様の標準化、情報通信のルール作成、一般企業・社員への啓発等の活動も含まれるが、IT 技術者育成を目的とするため、制度・ルール・啓発活動等の専門家育成は、専修学校の育成人材の対象とはしないこととし、セキュリティの技術を用いた情報システム開発技術者の育成を目指すこととする。

〇これまでの情報セキュリティ教材との違い

これまでの情報セキュリティでは、既知のリスクに対して、コスト、技術的な方法、影響などを分析して、対応策を講じる内容でセキュリティの確保を学習するが、今後、日本が目指す Society5.0 の社会では、既知のリスクに対応することも重要である。このことから、未知のリスクや不確実な要素を洗い出して、将来的な脅威に対応することが重要となる。未知のリスクや不確実な要素の洗い出し、将来的な脅威に対応する学習は、Society5.0 の実現を目指すためには必要不可欠であり、今後の人材育成が最も重要である。

（4）具体的な取組

ⅰ）計画の全体像

2018 年度

Society5.0 における情報セキュリティの対応実態の把握、情報セキュリティ専門科目の基礎部分の教育カリキュラム・教材開発、実証講座による教育プログラムの有用性の確認

●調査	情報セキュリティの Society5.0 対応実態調査	
●開発	カリキュラム・シラバス	・システムセキュリティ構築
		・セキュアなネットワーク設計
	教育教材	・システムセキュリティ構築教材
		・セキュアなネットワーク設計教材
●実証講座		・システムセキュリティ構築講座
		・セキュアなネットワーク設計講座

2019 年度

Society5.0 で必要な情報セキュリティ人材育成の専門科目の教育プログラム開発
実証講座により有用性の検証・確認

●開発	カリキュラム・シラバス	・サイバー攻撃手法・対策
		・セキュアなシステム設計・開発
	教育教材	・サイバー攻撃手法・対策教材
		・セキュアなシステム設計・開発教材
●実証講座		・サイバー攻撃手法・対策講座
		・セキュアなシステム設計・開発講座

2020 年度

Society5.0 で必要な運用領域における情報セキュリティ人材育成教育プログラムの開発と情報セキュリティ人材育成の為のモデルカリキュラムの取りまとめ
教育実施のための教員育成プログラムの構築・整備

●開発	カリキュラム・シラバス	・セキュアなシステム運用
	モデルカリキュラム	・情報セキュリティ対策エンジニア学科
	教育教材	・セキュアなシステム運用教材
	教員育成	・教員研修プログラム
		・指導書と評価ガイド
●実証講座		・セキュアなシステム運用講座
		・教員研修会

ⅱ）今年度の具体的活動

○実施事項

【調査】

●新通信技術における情報セキュリティ実態調査

目的：２０２０年に実用化予定の新たな情報通信技術である５G や IoT の進展により活用が進むことが予測される LPWA 等のネットワークにおける情報リスクに対するセキュリティ対策技術の現状及び技術の進展の情報を収集し、教育プログラムに反映する。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。

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

調査項目：５G 実用化で予測される脅威と対応、LPWA ネットワークにおける脅威と対応、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、サイバー攻撃における新技術動向と対応

分析内容：今後予測される新たな情報セキュリティの脅威と対応技術を明らかにする。情報セキュリティインシデント発生時の対応とその必要技術、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

※育成人材像については IT 分野人材育成協議会と連携して方向性を検討する。

【開発】

●教育カリキュラム・シラバス開発

本年度開発する教材部分のカリキュラム・シラバス開発　120 時間相当

・サイバー攻撃手法・対策　60 時間

・情報システム開発技術者のセキュリティ知識　30 時間

●教育教材開発

・サイバー攻撃手法・対策

サイバー攻撃及び対策を学習するための教材と演習用データ

・情報システム開発技術者のセキュリティ知識

情報システム技術者が必要な情報セキュリティ（情報倫理含む）を学習するための教材

・昨年度成果物

システムセキュリティ構築教材、セキュアなネットワーク設計教材について、実証講座の行い、検証の結果から見直しを行う

【実証講座】

●システムセキュリティ構築・ネットワーク設計講座

目的：開発したカリキュラム・教材を用いて講座を行い、内容・効果の検証を行う。

対象：専門学校学生、IT 技術者（卒業生等）

期間：２０１９年 7 月　3 日間（6 時間×３日　18 時間）

場所：東京

●サイバー攻撃手法・対策講座

目的：開発したカリキュラム・教材を用いて講座を行い、内容・効果の検証を行う。

対象：専門学校学生、IT 技術者（卒業生等）

期間：２０１９年 11 月　3 日間（6 時間×３日　18 時間）

場所：東京

●情報システム開発技術者のセキュリティ知識講座

目的：開発したカリキュラム・教材を用いて講座を行い、内容・効果の検証を行う。

対象：専門学校学生、IT 技術者（卒業生等）

期間：２０１９年 11 月　1 日間（6 時間×1 日　6 時間）

場所：東京

【成果の普及】

●成果物の配布

●成果報告会の実施

●成果のホームページでの公開

【委員会】

・実施委員会　3 回開催　9 名

事業開始時、事業の中間、成果報告時に開催する。

受託機関および協力専門学校・企業・団体、事務局の責任者で構成する。

事業計画の承認および全体の方向性の確認、事業の進捗状況の確認と予算執行管理。

・調査委員会　4 回開催　7 名

事業開始時、事業期間中の 2 回、成果報告時に開催する。

受託機関および協力専門学校・企業・団体、事務局の担当者で構成する。

情報セキュリティの Society5.0 対応実態調査の調査項目、対象、分析方法等を検討する。

・人材育成委員会　4 回開催　13 名

事業開始時、事業の中間、成果報告時に開催する。

受託機関および協力専門学校・企業・団体、事務局の担当者で構成する

教育カリキュラムの開発仕様・モデル化の関する検討・協議、教材開発仕様に関する検討協議、実証講座企画・運営、効果計測。

IT 分野人材育成協議会との連携、情報の共有

○事業を推進する上で設置する会議

会議名①　　実施委員会

目　的　　・事業目的および内容の承認、・事業の進捗管理、
・事業結果の確認
・事業会計の監査、IT 分野人材育成協議会との連携

検討の具体的内容　・事業方針策定
・事業進捗管理
・予算執行管理
・各委員会進捗管理
・成果の活用・普及
・他の委員会との連携
・課題の検討
・IT 分野人材育成協議会との連携

委員数　　８人

開催頻度　　年３回

実施委員会の構成員（委員）

1　飯塚　正成　一般社団法人全国専門学校情報教育協会　専務理事
2　川上　隆　情報科学専門学校
3　中村 健太郎　専門学校静岡電子情報カレッジ　教育改革室
4　吉野　忠男　大阪経済大学　経営学部　教授
5　山田　英史　株式会社ディアイティ　セキュリティサービス事業部 部長
6　長谷川 長一　株式会社ラック　サイバーセキュリティ本部　理事
7　吉田　雄哉　一般社団法人クラウド利用促進機構
8　菊嶋　正和　株式会社サンライズ・クリエイティブ　代表取締役

会議名②　　調査委員会

目　的　　・新通信技術における情報セキュリティ実態調査の企画、実施、考察

検討の具体的内容　・調査方針検討・提案
・今後の必要技術調査

・調査項目の検討

・調査対象の検討

・調査方法の検討

・IT 分野人材育成協議会との連絡・協議、情報共有

委員数　　７人

開催頻度　　年３回

調査委員会の構成員（委員）

1　鳥居　高之　船橋情報ビジネス専門学校　校長

2　海野　晴博　日本電子専門学校

3　大矢　政男　日本工学院専門学校　ＩＴカレッジ長

4　吉野　忠男　大阪経済大学　経営学部　教授

5　岡山　保美　株式会社ユニバーサル・サポート・システムズ取締役

6　菊嶋　正和　株式会社サンライズ・クリエイティブ　代表取締役

7　吉岡　正勝　一般社団法人全国専門学校情報教育協会

会議名③　　人材育成委員会

目　的　　・教育プログラム開発、教育領域・範囲・レベルの設計、検証の確認、成果の活用の設計、教育プログラムの実証、IT 分野人材育成協議会との連携

検討の具体的内容　・開発方針検討・提案

・開発仕様の検討

・開発業者選定

・教育カリキュラム開発

・教育教材開発

・指導者育成プログラム開発

・教育カリキュラム検証

・教育教材の検証

・指導者育成プログラム検証

・実証講座実施

・IT 分野人材育成協議会との連絡・協議、情報共有

委員数　　１２人

開催頻度　　年４回

1	吉岡　正勝	一般社団法人全国専門学校情報教育協会
2	中川　隆	高知情報ビジネス＆フード専門学校
3	樋口 正之	盛岡情報ビジネス専門学校
4	小澤　慎太郎	中央情報大学校
5	神馬　一博	河原電子ビジネス専門学校
6	上里　政光	国際電子ビジネス専門学校
7	稲垣　実	船橋情報ビジネス専門学校
8	川人 宏行	専門学校穴吹コンピュータカレッジ
9	木崎　悟	日本工学院専門学校
10	柳谷　博道	早稲田文理専門学校
11	北原　聡	麻生情報ビジネス専門学校
12	菊嶋　正和	株式会社サンライズ・クリエイティブ

○事業を推進する上で実施する調査

調査名　　新通信技術における情報セキュリティ実態調査

調査目的　　２０２０年に実用化予定の新たな情報通信技術である５GやIoTの進展により活用が進むことが予測されるLPWA等のネットワークにおける情報リスクに対するセキュリティ対策技術の現状及び技術の進展の情報を収集し、教育プログラムに反映する。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。

５G（第５世代移動通信規格）の実用化により、これまでの１０００倍のデータ通信が可能となり、ネットワークに接続する機器もこれまでの１００倍　５０億個のIoT機器が接続されることが予測されている。通信容量の増大、通信速度の高速化により、これまでにない情報システムの脅威が出現すると思われる。脅威に対応するためには、あらたな通信技術の理解や、新たな脅威対応する知識・技術が必要であり、５Gの通信技術や予測される脅威について調査し、従来の学習内容の更新を行うことが重要であると考える。

調査対象	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
調査項目	５G 実用化で予測される脅威と対応、LPWA ネットワーワークにおける脅威と対応、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、サイバー攻撃における新技術動向と対応
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。
活用手法	教育カリキュラム、科目・シラバスへの反映 時間数、領域・範囲・レベルの検討に活用、教育教材・演習教材の内容に反映、学習の事例や演習課題に活用 教員育成研修プログラムに反映 情報セキュリティの現状の把握と必要人材の理解に活用

○開発に際して実施する実証講座の概要

実証講座の対象者	専門学校学生、IT 技術者（卒業生等）
期間（日数・コマ数）	●システムセキュリティ構築・ネットワーク設計講座 ２０１９年7月　3日間（6時間×３日　18時間） ●サイバー攻撃手法・対策講座 ２０１９年11月　3日間（6時間×３日　18時間） ●情報システム開発技術者のセキュリティ知識講座 ２０１９年11月　1日間（6時間×1日　6時間）
実施手法	講義と演習・実習
想定される受講者数	システムセキュリティ構築・ネットワーク設計講座　１６名 サイバー攻撃手法・対策講座　　２０名 情報システム開発技術者のセキュリティ知識講座　１６名 合計　５２名（延べ）

ⅳ）開発する教育カリキュラム・プログラムの検証

●実証講座受講者からは、受講修了時のアンケートと演習課題の達成度により教育カリキュラム・教材の効果を計測する。

●実証講座受講者のアンケート結果及び演習課題の達成度の結果を教育カリキュラム・教材の開発に携わった企業・業界団体等と共有し、内容を時間数、受講者の技術の向上の観点から分析する。教育カリキュラムで設定する教育目標に到達している受講者の割合で、効果を検証し、内容、時間数、前提知識・技術について検討する。

●IT 人材育成協議会　セキュリティ対策人材育成ワーキングにおいて、実証講座の結果から標準化・モデル化に関する検討を行うとともに、専門学校への導入に関する協議を行う。

●事業に参画する企業が社員研修で活用するための改善や教育の設計（技術レベル・教育レベル・教育内容等）に関する意見を集約し、次年度以降の教育プログラムの設計に活用する。

（５）事業実施に伴うアウトプット（成果物）

【2018 年度】

●調査報告書

情報セキュリティの Society5.0 対応実態調査の結果および育成人材像を取りまとめた報告書

●教育カリキュラム・シラバス

・システムセキュリティ構築　コマシラバス　60 時間

・セキュアなネットワーク設計　コマシラバス　60 時間

●教育教材

・システムセキュリティ構築教材　　テキストと演習課題

・セキュアなネットワーク設計教材　　テキストと演習課題

【2019 年度】

●教育カリキュラム・シラバス

・サイバー攻撃手法・対策　　コマシラバス　60 時間

・情報システム開発技術者のセキュリティ知識　コマシラバス　30 時間

●教育教材

・サイバー攻撃手法・対策教材　テキストと演習課題

・情報システム開発技術者のセキュリティ知識　テキストと演習課題

・システムセキュリティ構築教材、セキュアネットワーク設計教材の見直し

【2020 年度】

●教育カリキュラム・シラバス

・セキュアなシステム運用　　コマシラバス　60 時間

・情報セキュリティ対策エンジニア学科　モデルカリキュラム　カリキュラム・学科構成・相関図　900 時間

●教育教材

・セキュアなシステム運用教材　テキストと演習課題

●教員育成

・教員研修プログラム

情報系専門学校教員を対象とした最新の情報セキュリティ技術とセキュアな情報システム開発技術の学習のための教材

・指導書及び評価ガイド

情報系専門学校教員を対象に、本事業で開発した教育プログラムを用いて、学習を進める指導方法と学習者の評価（教育の効果計測）をするためのガイド

（６）本事業終了後※の成果の活用方針・手法

●本事業に参加する専門学校に、教育カリキュラム・教材の利用及び学科の設置について調整を行い、導入を促進する。

●本事業に参加する企業に、開発した教育プログラムの社員教育への利用を検討していただき、成果の活用を促進する。

●本会会員校及び全国の情報系専門学校に成果を配布するとともに、モデルカリキュラム説明会を行い、教育カリキュラム・教材の活用および学科の設置を促進する。

●情報産業の業界団体を通して、成果物について、企業の研修等への利用を打診し、活用を促進する。

●教員の研修プログラムを用いて、本会の行う教職員研修を企画し、教員の育成を行い、教員研修プログラムの活用とともに教育カリキュラム・教材の専門学校への導入を促進する。

●情報セキュリティを取り巻く環境は、今後も大きく変化することが予測されるため、事業終了後も情報収集や教育プログラムの更新を行い、常に最新の状態で教育が実施できる継続的な体制を構築する。

●専門学校教員を対象とした「情報セキュリティ教育」に関する情報提供サイト・コミュニティサイトを整備し、教育実践の支援を行う。

２．事業の成果

１．調査

（１）新通信技術における情報セキュリティ実態調査

調査目的　　２０２０年に実用化予定の新たな情報通信技術である５GやIoTの進展により活用が進むことが予測されるLPWA等のネットワークにおける情報リスクに対するセキュリティ対策技術の現状及び技術の進展の情報を収集し、教育プログラムに反映する。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。

５G（第５世代移動通信規格）の実用化により、これまでの１０００倍のデータ通信が可能となり、ネットワークに接続する機器もこれまでの１００倍　５０億個のIoT機器が接続されることが予測されている。通信容量の増大、通信速度の高速化により、これまでにない情報システムの脅威が出現すると思われる。脅威に対応するためには、あらたな通信技術の理解や、新たな脅威対応する知識・技術が必要であり、５Gの通信技術や予測される脅威について調査し、従来の学習内容の更新を行うことが重要であると考える。

調査対象　　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

調査項目　　５G実用化で予測される脅威と対応、LPWAネットワーワークにおける脅威と対応、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、サイバー攻撃における新技術動向と対応

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。

活用手法　　教育カリキュラム、科目・シラバスへの反映

時間数、領域・範囲・レベルの検討に活用、教育教材・演習
教材の内容に反映、学習の事例や演習課題に活用
教員育成研修プログラムに反映
情報セキュリティの現状の把握と必要人材の理解に活用

ヒアリング先企業　トレンドマイクロ株式会社
フォーティネットジャパン株式会社
株式会社アルファネット
株式会社野村総合研究所
サービス＆セキュリティ株式会社　　計５社

調査結果

1. 今後予測される新たな情報セキュリティの脅威と対応技術

・5G ネットワークの通信スピード、拡張性、グローバル性は社会や人々の生活にメリットのある大きな進化をもたらすが、サイバー攻撃者にとっても不正収益などを拡大させる開拓地となる。

・あらゆるデバイスとアプリケーションをリアルタイムに可視化して、攻撃対象を包括的に保護する幅広さが求められている。

・5G、IoT ともに、それぞれの接続形態に脆弱性は少なからず存在し、攻撃経路となるネットワークトポロジーを起点に脅威が引き起こされる可能性がある。

・5G、IoT は膨大なデータを取り扱うことになり、パブリックまたはローカルな無線ネットワークの脆弱性をターゲットに攻撃が仕掛けられ、そこを起点にデータが狙われる。

・SIM ジャッキングマルウェアは進化し続けており、SIM カードをターゲットにした攻撃が行われ、最終的にネットワーク全体を乗っ取られる可能性がある。

・IoT においてはルーターの脆弱性を狙った攻撃が増え、ルーターを起点とした様々なサイバー攻撃が想定される。

・IoT の多くがオペレーションテクノロジー（OT）に根ざしたものであり、IT と OT の間にあるギャップがサイバーセキュリティの大きな課題となっている。IT では脆弱性を排除するために OS やセキュリティパッチのアップデートが頻繁に行われるが、OT ではそのアップデートによりアプリケーションが正常に動作しなくなる可能性もある。そのため、現在でも WindowsXP を OS にしている場合もあるが、ネットワークにつながることで、OT 側の脆弱性にも対処する必要性が出てくる。

・これまで信頼性が高いとされていたリアルタイムオペレーティングシステムに複数の脆弱性の存在が明らかになり、大混乱に陥ったという事例が出てきている。いま信頼性が高いものであっても明日はどうなるかわからないと考え、対処していく必要がある。

・リアルタイムでの保護は常に求められるが、サイバー攻撃の手法と対策はイタチごっこのようなものであり、定期的なセキュリティ診断は必要と思われる。そのため、ログを一元管理できるソフトやソリューションの需要は増していく。

・車に対するサイバー攻撃は今後増えていく。車も常にセキュリティ対策を行っていくメメンテナンスが必要となり、車のセキュリティを監視する仕組みは将来重要なインフラとなる。

2. 情報セキュリティインシデント発生時の対応と、その必要技術

・ハードウェアレベルで管理される SIM カードの ID は、アプリケーション側で認識する ID とのギャップがあり、そこをターゲットにされる可能性がある。IT ベースで認証する際、なりすましの SIM の ID を信用しないよう、可視化することが必要になる。

・SIM 内にアプリケーションとして搭載される分散型台帳を利用して実装することを可能にする、フェデレーテッド ID/アクセス管理（FIdAM：Federated Identity and Access Management）により、SIM ジャッキングや同様の IoT 攻撃による潜在的なハードウェアレベルの影響の検出と対処を行う。

・IoT により家庭用ネットワークに接続されたデバイスも急速に増えており、家庭用のルーターが狙われる場合もある。そのため、家庭用ネットワークに接続

されたすべてのデバイスに対するアクセス管理を可能にするセキュリティソリューションが必要となる。

・サイバー犯罪者などによる不正侵入やセキュリティ侵害は、実際に遭遇しないと理解できないことが多い。そのため、実際のインシデント発生を想定した演習による日常的な準備と改善が重要となる。そのようなセキュリティ対策を支援している企業もある。

・5G、IoT など技術は急速に進化しているが、人的なリスクは基本的なところで起きているところもまだまだ残っている。IoT 機器への攻撃として、初期設定値の ID とパスワードが単純なものであったため、そこからログインされているケースも存在している。情報セキュリティに携わるものだけでなく、運用する側も容易さばかりを求めるのではなく、セキュリティに対する意識を強める必要がある。

3. 情報セキュリティ人材の業務領域

・脆弱性に対するセキュリティ対策を行うのではなく、使いやすさなどを求める OT 側の要求にも対応していくため、今後は IT だけでなく、OT にも知見のある人材が必要になる。

・業界レベルで攻撃者の手法や戦術をもとに作られたフレームワークがこれまで以上に必要となり、脅威モデルやセキュリティ製品、組織リスクなどを評価できることが求められる。

・脅威インテリジェンスを用いた相関関係の分析や総合的な視点が重要となり、Security Operation Center（SOC）の分析チームのようなセキュリティ専門家の役割もより一層重要となってくる。

・セキュリティ人材は不足しており、サイバーセキュリティトレーニングなどを受講し、企業にとってのセキュリティ対策を理解する人材をそれぞれの企業が育成しているところもある。一方で、電話サポート代行のようにセキュリティに特化した代行会社も増えてくると想定される。そのため、情報セキュリティ人材には人を育てる力やコミュニケーション能力がこれまで以上に求められるようになってきている。

・コンサルティングを行う会社でも IT ソリューションの提案だけでなく、情報セキュリティの知見を深めているところがある。顧客に対し、コンサルティング的な提案力も必要になってきている。

4. 情報セキュリティ人材のシステム開発への関与

・セキュリティ部門及び開発部門の双方において、接続デバイスの可視化や制御を可能にし、それらのデバイスに関する問題点を対処しなければならなくなっている。

・セキュリティは、デジタル・トランスフォーメーションの障害物になるのではなく、デジタル・トランスフォーメーションの流れを推進するものでなくてはならない。そのため、情報セキュリティ人材もシステムが果たす役割を十分に理解する必要があり、開発時から関わることが求められる。

２．教育プログラム

（1）教育カリキュラム

以下の教育カリキュラム・コマシラバスを開発・整備した

・サイバー攻撃とその手法　　60 時間

●サイバー攻撃とその手法カリキュラム

学科：　情報セキュリティ	担当教員：
科目名：サイバー攻撃とその手法	対象年次：　　実施時期：
使用教材：セキュリティ教材	授業回数：60 (60 時間)

目標：

・サイバー攻撃の手法ごとに状況を把握し、原因を特定して対策をとることができる。

・情報セキュリティ・インシデント発生前の対策について説明できる。

・情報セキュリティ・インシデント発生後に被害を最小限にする手続きを説明できる。

・情報セキュリティに関連する倫理原則と法律について説明ができる。

前提知識：

・基本情報技術者試験の基本用語を説明できる。

回数	学習項目	備考
1	はじめに　Society 5.0 とは 第 1 章　ハードウェア（IoT）について把握する リスク分析、設計 理解度確認方法 　情報セキュリティにおける、IoT 機器固有の考慮事項を挙げられること。	IoT 機器の対策の基本は、通常のコンピュータの対策と同じです。ここでは極力 IoT 機器ならではの難しさと、それを考慮した設計をつたえる。セキュリティ・バイ・デザインについても改めて想起してもらう。
2	第 1 章　ハードウェア（IoT）について把握する ネットワーク分割 紛失、盗難 運用 理解度確認方法 　紛失、盗難に対し、物理的、論理	ここでは IoT 機器に限定せず、紛失、盗難にあいそうな情報機器全般に対し、ディスカッションによって対策を挙げてもらうとよい。

	的、人的セキュリティの観点で対策を提示できること。	
3	第 1 章　ハードウェア（IoT）について把握する 更新プログラムの適用 初期パスワードの変更 理解度確認方法 IoT 機器を提供する側として、どのような工夫をすれば IoT 機器を保護できるか自分なりの考えを説明できること。	IoT 機器の取り扱いでは、まず説明書をしっかり読むことが大事。IPA 資料も参考に、IoT 機器を提供する側、利用する側の対策をまとめてもらう。
4	第 2 章　ネットワークについて改めて学ぶ ネットワークを構成する IP アドレス、DNS ポート番号、TCP と UDP 理解度確認方法 ネットワーク構成エラーから原因を読み解けること。	仮想マシンを用い、ネットワークの基本的な設定を実際に行ってもらう。そのうえで、間違った設定を行ったときにどのような状況になるかを体験してもらう。
5	第 2 章　ネットワークについて改めて学ぶ VLAN 理解度確認方法 　VLAN スイッチによる 2 種類以上のネットワーク分割ができること	VLAN スイッチを用いたネットワーク分割の演習を実施。VLAN スイッチの実機を用意できない場合、VLAN を使った物理ネットワーク設計と論理ネットワーク設計を作ってもらう演習だけでもよい。
6	第 2 章　ネットワークについて改めて学ぶ プロキシサーバー, DMZ 理解度確認方法 　プロキシサーバーの役割、DMZ の役割について説明できること。	たとえば BlackJumboDog を使い、プロキシサーバーの動きや特徴、できることを確認。
7	第 2 章　ネットワークについて改めて学ぶ	OSI 参照モデルは暗記を推奨。 演習は Wireshark による各プロト

	プロトコルを知る HTTP, SMTP, POP, IMAP 理解度確認方法 　OSI 参照モデルにおいて、各層に流れている代表的な情報を提示できること。	コルの動作追跡で、各プロトコルのやり取りを確認し、OSI 参照モデルのどの層にどんな情報が流れているかを確認すする。Windows を想定しているが、Linux でも構わない。
8	第 3 章　ネットワークを狙った攻撃を知る 偵察、武器化 理解度確認方法 　nmap と netstat の目的の違いを説明できること。	外部から見えるポート番号を確認攻撃における調査する。そして内部的に提供しているポート番号を確認し、先に確認したポート番号と比較。両者の違いを説明できるようにする。
9	第 3 章　ネットワークを狙った攻撃を知る デリバリー、エクスプロイト 理解度確認方法 　エクスプロイトによってどんなことが可能か説明できること。	Metasploit Framework を用いて実際にエクスプロイトを行う。いくつかのコマンドにより、具体的にできることをいくつか体験する。
10	第 3 章　ネットワークを狙った攻撃を知る ポートを閉じる（対策） Windows ファイアウォール 理解度確認方法 　Windows ファイアウォールの役割を説明できること。	Windows ファイアウォールでポートを閉じた場合の結果の違いについて、nmap と netstat を比較する。
11	第 3 章　ネットワークを狙った攻撃を知る 　自動起動しているサーバーの終了（＋自動起動しない設定） 理解度確認方法 　代表的なポートとサービスの関係を提示できること。	物理的なサーバーとサービスとしてのサーバーについて違いを確認。サービスの終了と開放ポートの関係を確認。サービス終了の影響を nmap と netstat を使って確認する。演習は Windows を想定。
12	第 4 章　ネットワークの通信を把握する	ホスト OS 型仮想マシンを用い、監視対象の仮想マシンと Zabbix

	通信経路におけるログを確認する （状況把握） Zabbix 理解度確認方法 Web 監視ができる項目をいくつか提示できること。	サーバーを用意。Web 監視の最終的な設定と監視の様子を体験してもらう。
13	第 4 章 ネットワークの通信を把握する 通信内容を調査する（原因特定） Fiddler 理解度確認方法 HTTP 通信の解析結果の発表と共有をおこなう。	ホスト OS 型仮想マシンを用意。Fiddler については、インストールから通信のキャプチャと解析まで自由に操作してもらう。数人のグループで検討しつつ行えると望ましい。
14	第 4 章 ネットワークの通信を把握する 通信経路を流れるパケットを止める （対策） IPS, IDS (HIDS, NIDS) 理解度確認方法 IDS によってできることと、パケットフィルタによるファイアウォールとの違いを説明できること。	侵入検知システムとして Snort と SnortSnarf、脅威ベクターとして nmap をあらかじめ用意し、侵入検知システムの動作を体験する。
15	第 5 章　アクセス数を確認する Web サーバーへのアクセス数を分析する（状況把握） ログの分析（Log Parser、Google Analytics など） 理解度確認方法 Windows のログ情報をいくつか提示して、状況を説明できること。	ホスト OS 型仮想マシンを用意 (Windows)。あらかじめ Log Parser と Log Parser Studio を導入しておき、テーマを作ってログを分析してもらう。
16	第 5 章　アクセス数を確認する 様々なサーバーへのアクセス数を一元管理する（原因特定） ログの解析と可視化に役立つツール （原因特定） 理解度確認方法	各種サーバーのログを確認してもらい、そのサーバーの性格からどのような情報を知りたいか、その情報を知ることができるかを確認してもらう。

	サーバーへのアクセス数とログの解析の必要性を説明できること	
17	第 5 章　アクセス数を確認する syslog、Fluentd によるログの収集 理解度確認方法 　syslog と Fluentd について説明できること。	可能であれば、複数のサーバー上で Fluentd を動かし、ログを集約する体験を行う。
18	第 5 章　アクセス数を確認する Elasticsearch、Kibana 理解度確認方法 　Fluentd、Elasticsearch、Kibana の役割を区別できる	可能であれば、Fluentd、Elasticsearch、Kibana を構成し、デモンストレーションだけでもできるとよい。
19	第 5 章　アクセス数を確認する 負荷を分散する（対策） ロードバランサー、CDN の利用 理解度確認方法 　ロードバランサーや CDN のメリットを説明できる	CDN については構成を紹介できればよい。
20	第 6 章　脆弱性を狙った攻撃を知る ログインエラーを確認する（状況把握） ログイン履歴、ログイン失敗履歴 理解度確認方法 　ログイン履歴の確認で分かることを提示できる	Windows や Linux のログイン状況を確認する手法をいくつか試す。
21	第 6 章　脆弱性を狙った攻撃を知る SQL インジェクション 理解度確認方法 　SQL インジェクションでできることをいくつか挙げられる。	SQL について簡単な説明を補足として追加する。そのうえで、事前に構成した mutillidae (練習用脆弱 Web アプリ)を用い、SQL インジェクションやコマンドインジェクションを体験。IPA の『安全な SQL の呼び出し方』も参照
22	第 6 章　脆弱性を狙った攻撃を知る XSS, CSRF, …	OWASP Top 10 に列挙されている脆弱性をいくつか説明。可能な

	理解度確認方法 　ここで学んだ脆弱性を区別できること	らばデモンストレーションや実習を。
23	第 6 章　脆弱性を狙った攻撃を知る 脆弱性診断を実施する（原因特定） OWASP ZAP や ratproxy による診断 理解度確認方法 　ここで学んだ脆弱性を区別できること	OWASP ZAP と mutillidae (練習用脆弱 Web アプリ)を構成し、ZAP による脆弱性スキャンを体験。
24	第 6 章　脆弱性を狙った攻撃を知る Web アプリケーションの脆弱性に備える（対策） 理解度確認方法 　Web アプリの脆弱性をいくつか提示できること。セキュリティ・バイ・デザインの重要性を説明できること。	Web アプリケーションの脆弱性として OWASP Top 10 を提示し、どのような脅威、脆弱性、リスクがあるかを検討。
25	第 6 章　脆弱性を狙った攻撃を知る セキュアなシステム設計（セキュリティレビュー、コードレビュー、…） 理解度確認方法 　Web アプリの脆弱性をいくつか提示できること。セキュリティ・バイ・デザインの重要性を説明できること。	Web アプリケーションの脆弱性として OWASP Top 10 を提示し、どのような脅威、脆弱性、リスクがあるかを検討。
26	第 6 章　脆弱性を狙った攻撃を知る WAF (Web Application Firewall)の使用 理解度確認方 WAF の効果を説明できること。	可能であれば mutillidae に対し、WAF として ModSecurity を適用し、ZAP でスキャン。 ModSecurity の有無で応答がどう変わるかを体験。
27	第 6 章　脆弱性を狙った攻撃を知る プログラムの改修 理解度確認方法 　SQL インジェクションの脆弱性の対策をいくつか提示すること。	SQL インジェクションの脆弱性を持つ、受講者が修正可能な Web アプリを用意。そして WAF として ModSecurity を構成。SQL インジェクション攻撃に対し、プログラムの改修および ModSecurity の

		有無で応答がどう変わるかを体験。
28	第 7 章　高負荷の状況を検出する CPU 負荷を調べる（状況把握） top, uptime, dstat, ps コマンド 理解度確認方法 　CPU、メモリ、ディスクの負荷を確認する方法を提示できること。可能であれば、対策についても提示できること。	仮想マシンで Linux を用意。 Stress コマンドで負荷をかけつつ、各種コマンドの実行結果からどのようなコンポーネントに負荷がかかっているかを読み解いてもらう。
29	第 7 章　高負荷の状況を検出する メモリ使用量を調べる（状況把握） vmstat, free コマンド 理解度確認方法 　主にメモリの負荷を確認する方法を提示できること。可能であれば、対策についても提示できること。	引き続き Stress コマンドで負荷をかけつつ、各種コマンドの実行結果からどのようなコンポーネントに負荷がかかっているかを読み解いてもらう。
30	第 7 章　高負荷の状況を検出する 不明なプロセスを調査する（原因特定） コマンドログの調査 不要なプロセスを終了する（対策） kill コマンド 理解度確認方法 　プロセスやサービスを確認する方法を提示できること。可能であれば、対策についても提示できること。	仮想マシンで Linux を用意。プロセスを確認する ps コマンドや、デーモンの状況の確認で service や systemctl コマンドを使ってもらう。
31	第 8 章　暗号技術について改めて学ぶ 暗号と認証について知る 理解度確認方法 　暗号化と認証、電子署名について、その役割を説明できること。	暗号化と認証、デジタル署名を用いたいかにして通信内容を守るのか伝える。
32	第 8 章　暗号技術について改めて学ぶ 公開鍵暗号	公開鍵暗号について、DH 方式による暗号化と復号を、受講生同士

	理解度確認方法 　公開鍵の方式と特徴について説明できること。	ペアを作って実際に計算させてみる。
33	第 8 章　暗号技術について改めて学ぶ 共通鍵暗号 デジタル署名、認証 理解度確認方法 　図を使い、デジタル署名の仕組みを説明できること。	署名の持つ機能を 2 つ提示（本人確認、改ざんチェック）。デジタル署名でこの 2 つの機能をどうやって実現しているかを確認。この中で、認証局の役割を明確にする。
34	第 8 章　暗号技術について改めて学ぶ 暗号を使った技術について知る TLS(SSL), SSH, VPN 理解度確認方法 　TLS 通信における、CA、HTTPS サーバー、ブラウザのやり取りを説明できること。	TLS 通信の流れを確認します。可能ならば、Fiddler を用いて HTTPS 通信の解析を行ってください。
35	第 9 章　Web サイトなどの改ざんを検出する 管理者がサーバー上での改ざんを検出する（状況把握） Tripwire 理解度確認方法 ファイルの改ざんを検出する仕組みについて説明できること。	オープンソース版の Tripwire を用い、ファイルの改ざん検出を実際に行ってもらう。
36	第 9 章　Web サイトなどの改ざんを検出する ダウンロードしたファイルが改ざんされていないか利用者が確認する（状況把握） MD5 などのハッシュ値 管理者権限、更新権限でのログインを確認する（原因特定） ログイン履歴、IP アドレス 理解度確認方法	オープンソースソフトウェアのダウンロードを実際に行ってもらい、ハッシュ値の計算をしてもらう。ログイン履歴は Windows または Linux のイベントログを見てもらうことで、どのような情報がわかるかを確認してもらう。

	ハッシュ関数の特徴を説明できること。ログイン履歴からわかる不正なログインの例をいくつか提示できること。	
37	第 9 章　Web サイトなどの改ざんを検出する サーバー、管理用端末を管理する（対策） 修正パッチの適用 理解度確認方法 Web サーバーのバージョン確認から脆弱性の確認、パッチの適用までを実行できること。	Linux を用い、ディストリビューションが提供する初期バージョンの問題点を探させ、どうすれば問題を回避できるか調べたうえで適用してもらう
38	第 9 章　Web サイトなどの改ざんを検出する 脆弱性診断の実施 適切なアカウント設定 理解度確認方法 脆弱性診断のポイントをいくつか提示できること。	脆弱性診断として、IPA の提供する『Web 健康診断仕様』や、類するドキュメントを用意し、Mutillidae や適当な Web サイトの脆弱性診断を実施する。
39	第 10 章　情報の流出を調べる ディスクなどに残った痕跡を調べる（状況把握） フォレンジック 理解度確認方法 いくつか例示する情報に関し、揮発度の高い順番を説明できること。 ファーストレスポンダが行うべき行動を説明できること。	電子証跡をとるためには、セキュリティ・インシデント発生時の初動が大事であることを伝えます。そして、誰もがファーストレスポンダになりうることを確認します。
40	第 10 章　情報の流出を調べる USB での持ち出し、プリンタでの印刷を調べる（状況把握） 資産管理ツール 理解度確認方法	USB メモリによる情報の持ち出しに限らず、物理的に安全な外部との情報の受け渡し方法についてディスカッションしてもらう。

	物理的な手段による情報流出経路をいくつか提示できること。	
41	第 10 章　情報の流出を調べる メールでの流出を調べる（状況把握） メール監視ツール 理解度確認方法 メール本文の暗号化、添付ファイルの暗号化についてその方法をいくつか提示できること。 SMTP と POP3、IMAP の暗号化についていくつか手段を提示できること。	メールの添付ファイルを安全に保つにはどうすればよいかディスカッションしてもらう。暗号化添付ファイルや、メール本文の暗号化、Wireshark による通信キャプチャも併用して。
42	第 11 章　組織のセキュリティをマネジメントする 情報資産について知る（設計） 脅威(人的脅威、技術的脅威、物理的脅威) 理解度確認方法 脅威、脆弱性、リスク、管理策の違いについて明確に説明できること。	ワークショップで、情報資産の洗い出しから、その情報資産に対する脅威、そして脅威に対する脆弱性を洗い出してもらう。脅威と脆弱性の違いをしっかり認識してもらうこと。JIS Q 27000 の文言を説明するのもよい。観点としては、人的、論理的、物理的、運用を抑えておくとよい。
43	第 11 章　組織のセキュリティをマネジメントする 管理的対策、技術的対策 リスクマネジメント、リスクアセスメント 理解度確認方法 リスクを減らすための方法についていくつか説明できること。	前回洗い出した脆弱性をなくす（あるいは減じる）ための管理策をディスカッションし、発表してもらう。その後、リスクマネジメントとアセスメントについて解説。
44	第 11 章　組織のセキュリティをマネジメントする セキュリティ管理のルールを決める（開発） ISMS, 情報セキュリティポリシー 理解度確認方法	少なくとも JIS Q 27000, 27001, 27002 の概略はつかんでもらうようにします。

	ISMS 認証で要求される事項について、関連する工業規格とその概要を説明できること。	
45	第 11 章　組織のセキュリティをマネジメントする システム監査 委託先管理 運用体制を構築する（運用） インシデント管理(CSIRT) 理解度確認方法 システム監査について、助言型と保証型の特徴を説明できること。 インシデント管理の一連の流れを説明できること。	インシデント管理については、解説のみ先に行います。ワークショップは次のコマで実施します。
46	第 11 章　組織のセキュリティをマネジメントする インシデント管理(CSIRT) 理解度確認方法 インシデント管理において、CSIRT メンバーに必要とされるスキルにどのようなものがあるか、いくつか提示できること。	インシデントレスポンスの実例（の前半）を題材に、各段階でどのような検討を行うかをワークショップ形式で体験します。
47	第 12 章　日々の運用で対策を実施する 更新プログラムを適用する OS, Office 理解度確認方法 Windows Update と WSUS の違いについて説明できること。	WSUS の導入（時間がかかる場合、あらかじめ導入しておく）と、管理画面で、サーバーに関してどのような更新状況を取得できるか確認する。
48	第 12 章　日々の運用で対策を実施する ルーター、複合機、IoT 機器、… 理解度確認方法	情報を取り扱う電子機器を題材に、あんぜんな運用方法をディスカッション。

	様々な情報機器の脆弱性と管理策をいくつか提示できること。	
49	第 12 章　日々の運用で対策を実施する ウイルス対策ソフトを導入する 最新のパターンファイル更新状況の確認 理解度確認方法 　個人向けと企業向けのウィルス対策ソフトの違を提示できること。	企業向けウイルス対策ソフト（体験版が使えれば）を用い、パターンファイル適用状況の集中管理を体験
50	第 12 章　日々の運用で対策を実施する パスワードの管理を徹底する 使い回しの禁止 単純なパスワードの禁止 2 段階認証の使用 理解度確認方法 　安全なパスワードの作り方をいくつか提示できること。	John the Ripper や Cain を用い、簡単なパスワードの危険性を実演または体験。パスワードリスト攻撃とその対策、パスワードの定期的な更新についてのディスカッションなど。
51	第 13 章　従業員教育を徹底する 教育内容を考える 対象者 セキュリティポリシーの周知 理解度確認方法 　セキュリティポリシーの周知方法を提案できること	経営層、技術者、従業員、利用者など、対象者ごとに抑えるべきポイントが違うことを確認。内容としては、『割に合わない』ことを伝える。
52	第 13 章　従業員教育を徹底する 最新の動向、脅威と対策 理解度確認方法 　最新動向を追跡する方法をいくつか提示できること。	IPA では毎年 10 大脅威を提示。OSASP では 2014 年からは IoT Top 10 を数年ごとに提示。総務省や厚生労働省などの公的機関。民間によるセキュリティ・インシデントのまとめなどを紹介。特徴をつかんでもらう。

53	第 13 章　従業員教育を徹底する 教育方法の特徴を知る Web 研修 集合研修 実施タイミング 理解度確認方法 　各教育方法の特徴を提示できること。	集合教育の利点、毎日少しずつ提示する目標、電話対応の訓練など、場面ごとに効果的な手法を提示。
54	第 14 章　倫理を意識する 技術者倫理を学ぶ 公益の確保、企業の社会的責任 内部告発と公益通報 理解度確認方法 　なぜ技術者倫理が必要か、各自の考えを示せること。	情報処理学会による『情報処理学会倫理綱領』や『認定情報技術者倫理要綱・行動規範』を参照。技術者倫理の必要性をディスカッション。 https://www.ipsj.or.jp/ipsjcode.html https://www.ipsj.or.jp/CITPcode.html
55	第 14 章　倫理を意識する ハッキング技術の使用などの知識の悪用 知的財産権を保護する 著作権 理解度確認方法 　調査技術の利用が、悪用になるか否かの境目を自分なりに判断できること。 　知的財産権について、いくつか事例を提示できること。	調査技術は攻撃技術にもなります。知りえた知識を使って攻撃になるようなきわどい事例をできればディスカッションさせたい。
56	第 14 章　倫理を意識する 財産権 営業秘密 オープンソースのライセンス 理解度確認方法 　知的財産権のうち、知的創造物についての権利（特許、著作権、営業秘密	可能であれば、特許庁が管轄する特許権、実用新案権、意匠権そして商標権にも触れられるとよい。

	など）と営業上の標識についての権利（商標権や商品等表示）をいくつか提示して説明できること。	
57	第 15 章　法律などについて改めて学ぶ 個人情報の保護 個人情報保護法 理解度確認方法 　個人を識別する情報(PII)、個人情報の違いや、個人情報を扱う注意点を説明できること。	いくつかの例を提示し、それが個人情報保護法における個人情報か、個人を識別する情報かを考えてもらう。
58	第 15 章　法律などについて改めて学ぶ マイナンバー法 プライバシーマーク 理解度確認方法 　マイナンバー法の下で情報セキュリティシステムを構築するための注意点を挙げられること。	マイナンバーを適切に管理する方法について、基本的な対策を解説。そしてプライバシーマーク制度における特定個人情報と関連付ける。
59	第 15 章　法律などについて改めて学ぶ 法律 不正競争防止法 不正アクセス禁止法 理解度確認方法 　不正競争防止法、不正アクセス禁止法がどのような法律なのか概要を説明できること。	知的財産権と不正競争防止法と関連付ける。不正アクセス禁止法についてはどのような場合に罰則が適用されるか調べてもらうのもよい。
60	第 15 章　法律などについて改めて学ぶ ウイルス作成罪 サイバーセキュリティ基本法 プロバイダ責任制限法 電子計算機損壊等業務妨害罪	法律の説明ではなく、できるだけ多くの事例を集めてもらって分類してもらうとよい。

	理解度確認方法 　情報セキュリティにかかわる法律についていくつか提示できること。	

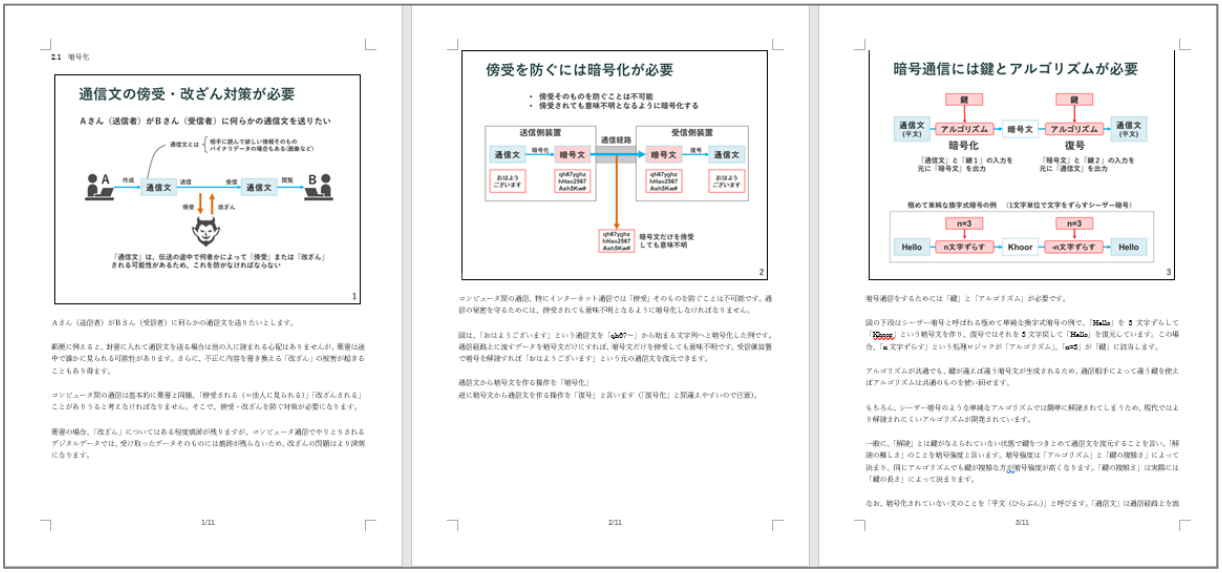
（２）教材

以下２点の教材を開発・整備した

・サイバー攻撃とその手法

・情報システム開発技術者のための情報セキュリティ基本知識

教材のイメージ



３．実証講座

システムセキュリティ構築実証講座①

■日　程：2019 年 10 月 28 日（月）9:00～13:00　　4 時間

2019 年 10 月 29 日（火）9:00～13:00　　4 時間

2019 年 10 月 30 日（水）9:00～13:00　　4 時間

■会　場：国際電子ビジネス専門学校

住所：〒900-0025 沖縄県那覇市壺川３丁目５－３

■受講者：国際電子ビジネス専門学校学生 25 名（１年次 15 名　２年次 5 名　４年次 5 名）

■目　標：システムセキュリティの知識・技術の習得

■講　師：鈴木　裕信

■実施内容：

○1 日目【10 月 28 日（月）】

時間	内容
9:00	●講座概要の説明 ●不正アタック対策（第 4 章） ユーザ認証 パスワードについて学ぼう パスワードとは知識 共有による認証 パスワードを使った認証の外観 パスワードを考えてみよう パスワードにまつわる誤解 定期的に変更することは安全か？ パスワードの現状 弱いパスワード 使い回すパスワード 盗まれるパスワード 個人のデバイスから サービスのサーバーから 顧客データ流出でサービス停止 盗まれたパスワード パスワードの処理フロー 暗号学的ハッシュ関数 クラック辞書を回避するためのパラメータ パスワード処理関数の実装の紹介

	多要素認証 Google 公式アプリ Google 認証システム まとめ ソフトウェアの脆弱性 ソフトウェアの脆弱性とは モリスワームの社会的影響 JVN 脆弱性の登録推移 国内の脆弱性管理サイト JVN iTerm2 における任意のコマンド実行が可能な脆弱性 複数の Apple 製品における脆弱性に対するアップデート LINE（Android 版）における複数の整数オーバーフローの脆弱性 OpenSSL に複数の脆弱性 Microsoft からのセキュリティ通知 完璧なソフトウェアは存在しない 脆弱性を放置するとどうなるのか？ Apache Struts2 CVE-2017-5638 脆弱性をもったコンピュータをみつける セキュリティ・アップデート 経営リスク管理として捉える ソフトウェアのライフサイクル まとめ マルウェア 用語の確認 マルウェア感染プロセス マルウェアの感染経路モデル C&C と感染端末（ボット）との関係 マルウェアの自律的感染拡大 感染拡大モデルの違い 蔓延するランサムウェア 急激にランサムウェアが増えた理由 公開鍵暗号法 ランサムウェアのモデル ダークウェブの登場 FBI も手を焼くマルウェア Gameover ZeuS

サイバー犯罪のためのマルウェア Zeus

FBI がおこなった 2010 年の壊滅作戦

サーバ・クライアントが P2P に進化

2014 年 6 月の撲滅作戦

スローガンを叫ぶのはむしろ危険

まとめ

TCP/IP とフィルタリング

TCP/IP

レイヤー化されているプロトコル

プロトコルは層になっている

パケットは入れ子になっている(TCP)

インターネット・プロトコル

IP アドレス

ローカルなネットワークで使うアドレス

NAT(Network Address Translation)

ルーターと NAT の違い

NAT (1 対多)

NAT (内部からの接続のみ)

トランスミッション・コントロール・プロトコル

ポート番号

TCP 3-ウェイ・ハンドシェイク

TCP 3-ウェイ・ハンドシェイクの脆弱性

SYN flood 攻撃

TCP/IP の接続開始

SYN flood への対応

UDP

ICMP

アプリケーションと TCP/IP

Web に使われるプロトコル

リモートログインで使われるプロトコル

アドレス管理に使われるプロトコル

メールに使われるプロトコル

ファイアウォールとパケット・フィルタリング

パケット・フィルタリング

	ルータを挟んだネットワークトポロジー ブリッジを挟んだネットワークトポロジー ルータ/ブリッジ上でフィルタリング ホストベースのフィルタリング フィルタリングのルールを考える フィルタリングのデフォルトは拒否 パケットフィルタの設定の考え方 ステートフルパケットフィルタリング ネットワーク・フィルタリングを動的に行うツールと併用パケット・インスペクション 実際のパケット・フィルタリング CentOS7 (GNU/Linux)の仕組み IDS（不正侵入検知システム） IPS（不正侵入防止システム） ネットワーク型とホスト型 シグニチャー方式とアノマリ方式 まとめ
13:00	終了

○2 日目【10 月 29 日（火）】

時間	内容
9:00	●情報セキュリティマネージメント（第 6 章） ISMS ISMS(Information Security ManagementSystem)とは C.I.A 情報セキュリティマネジメントシステム適合性評価制度 ISMS 適合性評価制度における認証基準 JIS Q 27001（ISO/IEC 27001）:2014 これまでの規格の流れ 規格の変化 物理的セキュリティも定義 ISMS 適合性評価制度の運用 ISMS クラウドセキュリティ認証 情報セキュリティマネジメントと PDCA サイクル 情報セキュリティポリシーの策定 リスクアセスメントとリスク対応 リスクへの対応・４つの考え方 脆弱性対策 日常的なセキュリティ監視と情報の収集 情報セキュリティ対策の評価 実務においての ISMS まとめ

インシデントと CSIRT
インシデントとは
標的型攻撃
標的型サイバー攻撃事例
マルウェアの進入経路
水飲み場攻撃
マルウェアの感染リスクは高い
マルウェアの挙動を理解する
マルウェア感染後
C&C とマルウェア
情報窃取のボット
スタックスネット Stuxnet
特定目標をターゲットとしたマルウェア
世界最初の兵器級マルウェア
大きく分類すると３つの機能
利用された脆弱性
ゼロデイ攻撃
バックドア・遠隔操作
LAN 内での感染拡大
rootkit
Rootkit 感染後のマルウェアは検知可能か？
高度化するマルウェア
ランサムウェア
フランチャイズ化したランサムウェア
CryptoLocker
CTB-Locker
DoS/DDoS 攻撃
日本国内の複数 EC サイトをターゲットとした DDoS 攻撃
DNS 水責め攻撃
NTP サーバを使った DDoS
トラフィック計測による管理サイトの確認
CSIRT
CERT/CC
JPCERT/CC
IPA
IPA 情報セキュリティ届出・相談・情報提供
CSIRT の重要性
インシデント対応が可能なチーム
日本シーサート協議会
まとめ
脆弱性流通とその仕組み
ソフトウェアの脆弱性とは
任意のコマンド実行
ソフトウェアのライフサイクル
脆弱性情報流通
脆弱性の発見
脆弱性情報ハンドリングの必要性
MITRE による脆弱性情報管理
NIST の運用する脆弱性データベース

	日本国内の脆弱性情報流通 ベンダーにとっての脆弱性情報流通 ユーザーにとっての脆弱性情報流通 Apache Struts2 の脆弱性を狙った攻撃 脆弱性の影響度指標 CVSS 脆弱性対応をめぐる議論 脆弱性をもつ IoT 機器を探索し警告する試み NOTICE / NICT とは 不正アクセス行為の禁止等に関する法律をめぐる議論 通称 NICT 法の改正 NOTICE・今度の予想と問題点 まとめ DDoS 攻撃と Mirai(第 4 章) DoS 攻撃とは アクセス量・データ量を極端に増やす Distributed(分散)DoS 攻撃 IoT ボットによる DDoS 攻撃 MIRAI インターネット史上最大級の DDoS 攻撃 IoT 機材が DDoS 攻撃ノードに 監視カメラ/ビデオレコーダーの乗っ取り DVR (Digital Video Recorder) CCTV(Closed-circuit Television) 中身は組み込み型 Linux 組み込み Linux システムを乗っ取る telnet をオープンにしている 外部から管理者権限でログイン Mirai が公開 HiSilicon IP Camera Root Password Mirai のアカウント・パスワード例 インターネットに接続する機器すべてを検索可能にする SHODAN 小型化する Linux 対応ハードウェア 360° を見渡せる知識？ DDoS 攻撃の対処 まとめ
13:00	終了

○3 日目【10 月 30 日（水）】

時間	内容
9:00	●セキュアプログラミング（第 11 章） セキュアプログラム概論 概論 コーディング・スタイル（規約） プログラムがリリースされるまで 今回のセキュア・プログラミングの範囲 バッファオーバフロー コード例 バッファサイズをはみ出すのを防ぐ 対策 メモリ境界を越えてのアクセス

	コード例 malloc は色々な問題を引き起こす SQL インジェクション コード例 テーブルをまるごと消す 文字列の検査 クロスサイト・スクリプティング XSS があるかどうかのチェック例 対応例 Apache Commons クロスサイトリクエストフォージェリ コード例 対応例 パス・トラバーサル コード例 対応例 Mitre による脆弱性の分類 まとめ Java セキュリティ（実習） 数値データの取り扱い 入力値の検査 Java の I/O の注意点 まとめ
13:00	終了

2018 年度に作成られた「システムセキュリティ構築」教材の実証検証のため、第 4 章、第 6 章、第 11 章を中心に講座を実施した。
事例等を紹介しながら、教材に記載されている内容の理解が深まるように講義を進め、各項目ごとにまとめと質疑応答の時間を設けた。
受講者は、専門学校　1 年次 15 名、2 年次 5 名、4 年次 5 名の 25 名であった。情報処理の基礎学習が途中である 1 年次には、レベルが高く、理解に時間がかかった。2 年次、4 年次の学生については、講義内容はおおむね理解できていた。教材のレベルとしては適切であると思われる。
最後に理解を深めるために行った実習については、講義中心の教材を補完するための試みであった。学生がこれまでに学習している内容と今回の講座の内容を踏まえ Java のセキュリティを取り入れたプログラム実習を実施した。講義内容・レベルが高かった 1 年次についても大きな滞りは無く実習を完了した。技術教育において、実際に自身で体験する実習・演習が理解を高めるために重要であると考えられる。

システムセキュリティ構築実証講座②

■日　程：2019 年 11 月 19 日（火）9:30～16:00　　6 時間　休憩 30 分
　　2019 年 11 月 20 日（火）9:30～16:00　　6 時間　休憩 30 分

■会　場：専門学校穴吹コンピュータカレッジ
　　住所：香川県高松市番町 2-4-14

■対象者：専門学校学生

■目　標：システムセキュリティの知識・技術の習得

■参加者：29 名

■講　師：鈴木　重毅　氏

■実施内容：

○1 日目【11 月 20 日（月）】

時間	内容
9:30	●講座概要の説明 ●不正アタック対策（第 4 章） ユーザ認証 パスワードについて学ぼう パスワードとは知識 共有による認証 パスワードを使った認証の外観 パスワードを考えてみよう パスワードにまつわる誤解 定期的に変更することは安全か？ パスワードの現状 弱いパスワード 使い回すパスワード 盗まれるパスワード 個人のデバイスから サービスのサーバーから 顧客データ流出でサービス停止 盗まれたパスワード パスワードの処理フロー 暗号学的ハッシュ関数 クラック辞書を回避するためのパラメータ パスワード処理関数の実装の紹介 多要素認証 Google公式アプリ Google認証システム まとめ ソフトウェアの脆弱性 ソフトウェアの脆弱性とは モリスワームの社会的影響 JVN 脆弱性の登録推移 国内の脆弱性管理サイト JVN iTerm2 における任意のコマンド実行が可能な脆弱性 複数のApple製品における脆弱性に対するアップデート LINE（Android版）における複数の整数オーバーフローの脆弱性 OpenSSLに複数の脆弱性 Microsoftからのセキュリティ通知

	完璧なソフトウェアは存在しない 脆弱性を放置するとどうなるのか？ Apache Struts2 CVE-2017-5638 脆弱性をもったコンピュータをみつける セキュリティ・アップデート 経営リスク管理として捉える ソフトウェアのライフサイクル まとめ マルウェア 用語の確認 マルウェア感染プロセス マルウェアの感染経路モデル C&Cと感染端末（ボット）との関係 マルウェアの自律的感染拡大 感染拡大モデルの違い 蔓延するランサムウェア 急激にランサムウェアが増えた理由 公開鍵暗号法 ランサムウェアのモデル ダークウェブの登場 FBIも手を焼くマルウェアGameover ZeuS サイバー犯罪のためのマルウェアZeus FBIがおこなった2010年の壊滅作戦 サーバ・クライアントがP2Pに進化 2014年6月の撲滅作戦 スローガンを叫ぶのはむしろ危険 まとめ
12:00	休憩
12:30	TCP/IPとフィルタリング TCP/IP レイヤー化されているプロトコル プロトコルは層になっている パケットは入れ子になっている(TCP) インターネット・プロトコル IPアドレス ローカルなネットワークで使うアドレス NAT(Network Address Translation) ルーターとNATの違い NAT（1対多） NAT（内部からの接続のみ） トランスミッション・コントロール・プロトコル ポート番号 TCP 3-ウェイ・ハンドシェイク TCP 3-ウェイ・ハンドシェイクの脆弱性 SYN flood攻撃 TCP/IPの接続開始 SYN floodへの対応 UDP ICMP

	アプリケーションとTCP/IP Webに使われるプロトコル リモートログインで使われるプロトコル アドレス管理に使われるプロトコル メールに使われるプロトコル ファイアウォールとパケット・フィルタリング パケット・フィルタリング ルータを挟んだネットワークトポロジー ブリッジを挟んだネットワークトポロジー ルータ/ブリッジ上でフィルタリング ホストベースのフィルタリング フィルタリングのルールを考える フィルタリングのデフォルトは拒否 パケットフィルタの設定の考え方 ステートフルパケットフィルタリング ネットワーク・フィルタリングを動的に行うツールと併用パケット・インスペクション 実際のパケット・フィルタリング CentOS7 (GNU/Linux)の仕組み IDS（不正侵入検知システム） IPS（不正侵入防止システム） ネットワーク型とホスト型 シグニチャー方式とアノマリ方式 まとめ ●情報セキュリティマネージメント（第6章） ISMS ISMS(Information Security ManagementSystem)とは C.I.A 情報セキュリティマネジメントシステム適合性評価制度 ISMS適合性評価制度における認証基準 JIS Q 27001（ISO/IEC 27001）:2014 これまでの規格の流れ 規格の変化 物理的セキュリティも定義 ISMS適合性評価制度の運用 ISMSクラウドセキュリティ認証 情報セキュリティマネジメントとPDCAサイクル 情報セキュリティポリシーの策定 リスクアセスメントとリスク対応 リスクへの対応・４つの考え方 脆弱性対策 日常的なセキュリティ監視と情報の収集 情報セキュリティ対策の評価 実務においてのISMS
16:00	まとめ インシデントとCSIRT インシデントとは 標的型攻撃 標的型サイバー攻撃事例 マルウェアの進入経路

	水飲み場攻撃 マルウェアの感染リスクは高い マルウェアの挙動を理解する マルウェア感染後 C&C とマルウェア 情報窃取のボット スタックスネット Stuxnet 特定目標をターゲットとしたマルウェア 世界最初の兵器級マルウェア 大きく分類すると３つの機能 利用された脆弱性 ゼロデイ攻撃 バックドア・遠隔操作 LAN 内での感染拡大 rootkit Rootkit 感染後のマルウェアは検知可能か？ 高度化するマルウェア ランサムウェア フランチャイズ化したランサムウェア CryptoLocker CTB-Locker DoS/DDoS 攻撃 日本国内の複数 EC サイトをターゲットとした DDoS 攻撃 DNS 水責め攻撃 NTP サーバを使った DDoS トラフィック計測による管理サイトの確認 CSIRT CERT/CC JPCERT/CC IPA IPA 情報セキュリティ届出・相談・情報提供 CSIRT の重要性 インシデント対応が可能なチーム 日本シーサート協議会 まとめ

○2 日目【11 月 20 日（火）】

時間	内容
9:00	●情報セキュリティマネージメント（第 6 章） 脆弱性流通とその仕組み ソフトウェアの脆弱性とは 任意のコマンド実行 ソフトウェアのライフサイクル 脆弱性情報流通 脆弱性の発見 脆弱性情報ハンドリングの必要性 MITRE による脆弱性情報管理 NIST の運用する脆弱性データベース 日本国内の脆弱性情報流通

	ベンダーにとっての脆弱性情報流通 ユーザーにとっての脆弱性情報流通 Apache Struts2 の脆弱性を狙った攻撃 脆弱性の影響度指標 CVSS 脆弱性対応をめぐる議論 脆弱性をもつ IoT 機器を探索し警告する試み NOTICE / NICT とは 不正アクセス行為の禁止等に関する法律をめぐる議論 通称 NICT 法の改正 NOTICE・今度の予想と問題点 まとめ DDoS 攻撃と Mirai(第 4 章) DoS 攻撃とは アクセス量・データ量を極端に増やす Distributed(分散)DoS 攻撃 IoT ボットによる DDoS 攻撃 MIRAI インターネット史上最大級の DDoS 攻撃 IoT 機材が DDoS 攻撃ノードに 監視カメラ/ビデオレコーダーの乗っ取り DVR (Digital Video Recorder) CCTV(Closed-circuit Television) 中身は組み込み型 Linux 組み込み Linux システムを乗っ取る telnet をオープンにしている 外部から管理者権限でログイン Mirai が公開 HiSilicon IP Camera Root Password Mirai のアカウント・パスワード例 インターネットに接続する機器すべてを検索可能にする SHODAN 小型化する Linux 対応ハードウェア 360° を見渡せる知識？ DDoS 攻撃の対処 まとめ
12:00	休憩
12:30	●セキュアプログラミング（第 11 章） セキュアプログラム概論 概論 コーディング・スタイル（規約） プログラムがリリースされるまで 今回のセキュア・プログラミングの範囲 バッファオーバフロー コード例 バッファサイズをはみ出すのを防ぐ 対策 メモリ境界を越えてのアクセス コード例 malloc は色々な問題を引き起こす SQL インジェクション コード例

	テーブルをまるごと消す 文字列の検査 クロスサイト・スクリプティング XSS があるかどうかのチェック例 対応例 Apache Commons クロスサイトリクエストフォージェリ コード例 対応例 パス・トラバーサル コード例 対応例 Mitre による脆弱性の分類 まとめ Java セキュリティ（実習） 数値データの取り扱い 入力値の検査 Java の I/O の注意点 まとめ
16:00	

2018 年度に作成られた「システムセキュリティ構築」教材の実証検証のため、第 4 章、第 6 章、第 11 章を中心に講座を実施した。

事例等を紹介しながら、教材に記載されている内容の理解が深まるように講義を進め、項目ごとにまとめと質疑応答の時間を設けた。

受講者は、専門学校　情報システム学科 1 年・ネットワークセキュリティ学科 1 年　２９名であった。情報処理の基礎学習が途中である 1 年次には、レベルが高く、理解に時間がかかった。

１年次であることを考慮し、講義中心の構成とした。最後に学生がこれまでに学習している内容と今回の講座の内容を踏まえ Java のセキュリティを取り入れたプログラム実習を実施したが、Java の学習がまだ基礎技術のみであったため、実習のレベルが高く、最後まで行うことができた受講者はいなかった。技術教育においは、実際に自身で体験する実習・演習が理解を高めるために重要

であるが、受講の前提となる知識・技術と実施する演習・実習のレベル的なバランスを考慮することが求められる。本講座で使用した教材は、情報セキュリティとしては基礎領域であるが、情報処理の基礎から応用の学習を習得した専門学校２年次の後期、３年次の教育カリキュラムに位置付けるレベルである。１年次を対象にした本講座で、座学レベルではついてこられる受講者も実習は、難しかったことにより、教材のレベルの検証ができた。

３．次年度計画概要

１．開発

カリキュラム・シラバス	・セキュアなシステム運用
モデルカリキュラム	・情報セキュリティ対策エンジニア学科
教育教材	・セキュアなシステム運用教材 （情報倫理、システム間連携含む）
教員育成	・教員研修プログラム ・指導書と評価ガイド

２．実証検証

（１）システムセキュリティ構築

実証講座の対象者	専門学校学生、IT 技術者（卒業生等）
期間（日数・コマ数）	システムセキュリティ構築講座 2020 年 9 月　3 日間（6 時間×３日　18 時間）
実施手法	講義と演習・実習
想定される受講者数	１６名

（２）サイバー攻撃手法・対策

実証講座の対象者	専門学校学生、IT 技術者（卒業生等）
期間（日数・コマ数）	サイバー攻撃手法・対策講座講座 2020 年 9 月　3 日間（6 時間×３日　18 時間）
実施手法	講義と演習・実習
想定される受講者数	１６名

（３）セキュアなシステム運用

実証講座の対象者	専門学校学生、IT 技術者（卒業生等）
期間（日数・コマ数）	・セキュアなシステム運用講座 2020 年 11 月　3 日間（6 時間×３日　18 時間）
実施手法	講義と演習・実習
想定される受講者数	１６名

（4）検証方法

●実証講座受講者からは、受講修了時のアンケートと演習課題の達成度により教育カリキュラム・教材の効果を計測する。

●実証講座受講者のアンケート結果及び演習課題の達成度の結果を教育カリキュラム・教材の開発に携わった企業・業界団体等と共有し、内容を時間数、受講者の技術の向上の観点から分析する。教育カリキュラムで設定する教育目標に到達している受講者の割合で、効果を検証し、内容、時間数、前提知識・技術について検討する。

●IT 人材育成協議会　セキュリティ対策人材育成ワーキングにおいて、実証講座の結果から標準化・モデル化に関する検討を行うとともに、専門学校への導入に関する協議を行う。

●事業に参画する企業が社員研修で活用するための改善や教育の設計（技術レベル・教育レベル・教育内容等）に関する意見を集約し、次年度以降の教育プログラムの設計に活用する。

３．事業成果普及と事業継続

●本事業に参加する専門学校に、教育カリキュラム・教材の利用及び学科の設置について調整を行い、導入を促進する。

●本事業に参加する企業に、開発した教育プログラムの社員教育への利用を検討していただき、成果の活用を促進する。

●本会会員校及び全国の情報系専門学校に成果を配布するとともに、モデルカリキュラム説明会を行い、教育カリキュラム・教材の活用および学科の設置を促進する。

●情報産業の業界団体を通して、成果物について、企業の研修等への利用を打診し、活用を促進する。

●教員の研修プログラムを用いて、本会の行う教職員研修を企画し、教員の育成を行い、教員研修プログラムの活用とともに教育カリキュラム・教材の専門学校への導入を促進する。

●情報セキュリティを取り巻く環境は、今後も大きく変化することが予測されるため、事業終了後も情報収集や教育プログラムの更新を行い、常に最新の状態で教育が実施できる継続的な体制を構築する。

●専門学校教員を対象とした「情報セキュリティ教育」に関する情報提供サイト・コミュニティサイトを整備し、教育実践の支援を行う。

2019 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

成 果 報 告 書

令和 2 年 2 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