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

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」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 5

１　委託事業の内容 5

２．事業名 5

３．分野 5

４．代表機関 5

５．構成機関・構成員等 5

（１）教育機関 5
（２）企業・団体 6
（３）行政機関 6
（４）事業の実施体制（イメージ） 6

（５）各機関の役割・協力事項について 7

６．事業の内容等 10

（１）本年度事業の趣旨・目的等について 10
（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 10
（３）開発する教育カリキュラム・プログラムの概要 15
（４）具体的な取組 19
（５）事業実施に伴うアウトプット（成果物） 26
（６）本事業終了後※の成果の活用方針・手法 27

２．事業の成果 29

１．調査 29

（１）情報セキュリティの Society5.0 対応実態調査 29

２．教育プログラム 34

（１）教育カリキュラム 34
（２）教材 43

３．実証講座 43

３．次年度以降の活動 44

１．実証検証 44

（１）システムセキュリティ構築教育プログラム 44
（２）セキュアなネットワーク設計教育プログラム 44
（３）平成３１年度開発教材の実証検証 44
（４）検証方法 44

２．事業成果普及と事業継続 45

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　学校法人中央穴吹学園　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

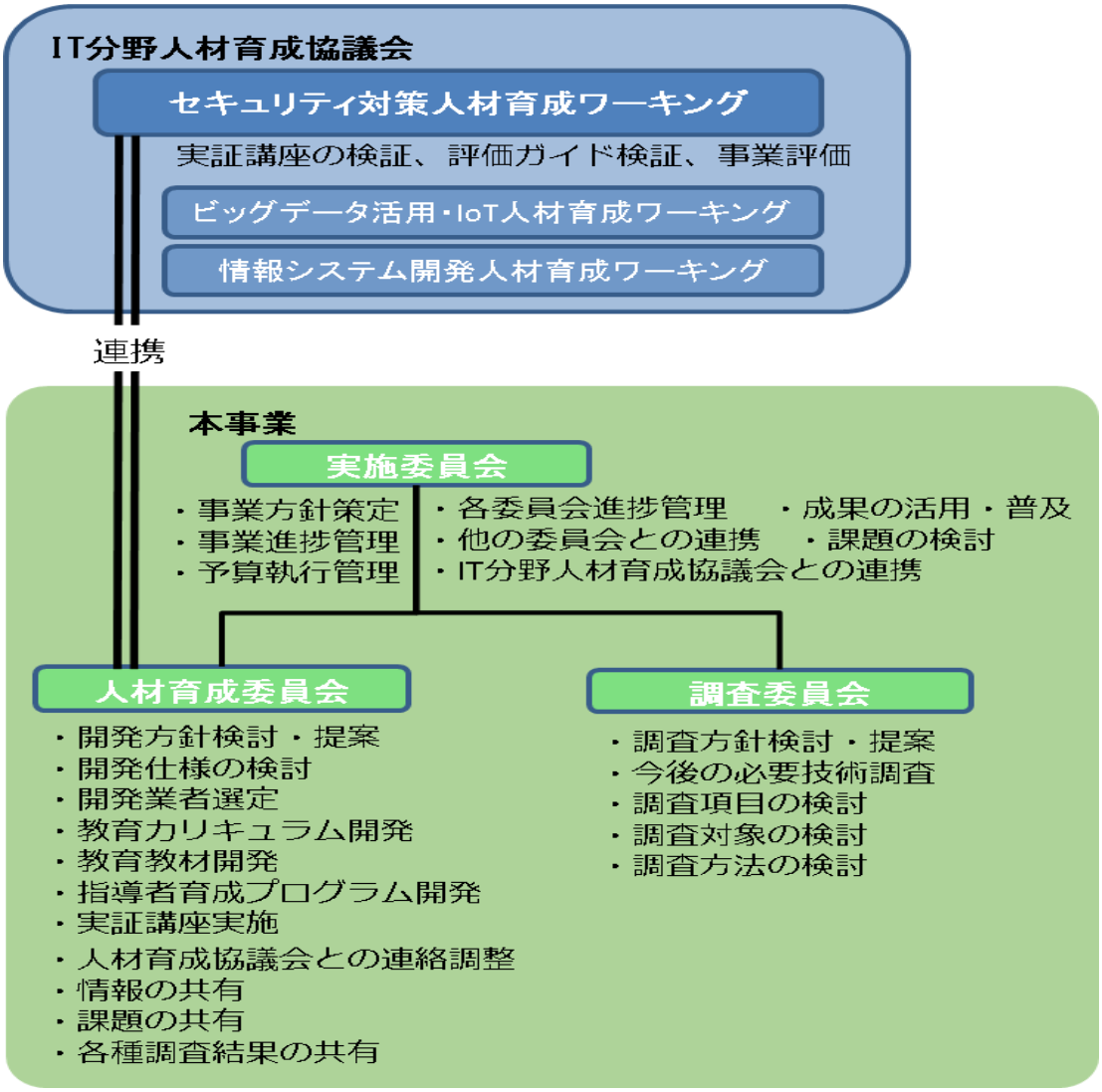
7　一般社団法人クラウド利用促進機構

8　一般社団法人全国専門学校情報教育協会

（３）行政機関

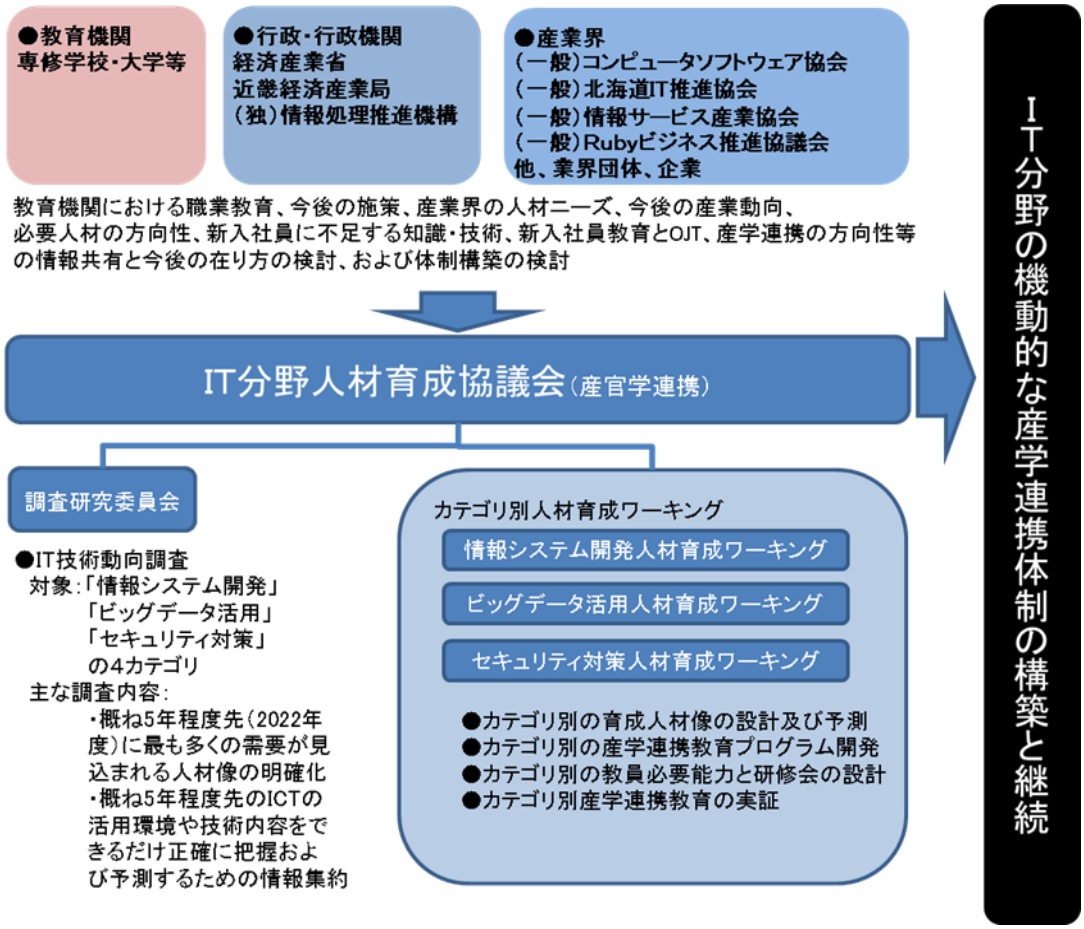
1　独立行政法人情報処理推進機構

（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。



（５）各機関の役割・協力事項について

〇教育機関

・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

〇企業・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）

〇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。

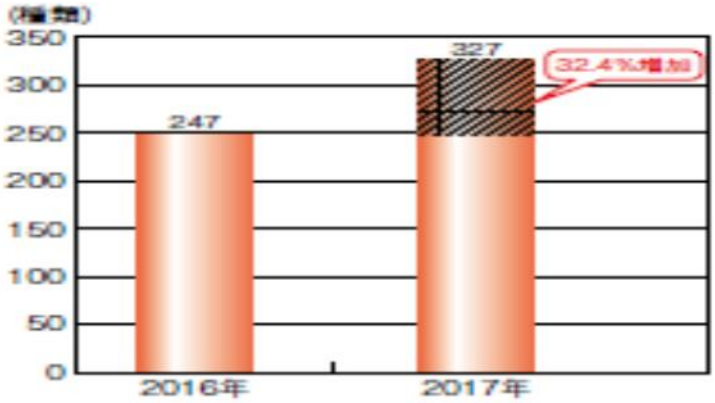
Society5.0 で目指す社会では、情報システムや情報通信ネットワークは、社会の根幹を支える基盤となり、情報リスクへの対応・情報セキュリティの確保は、最も重要な技術の一つである。

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）

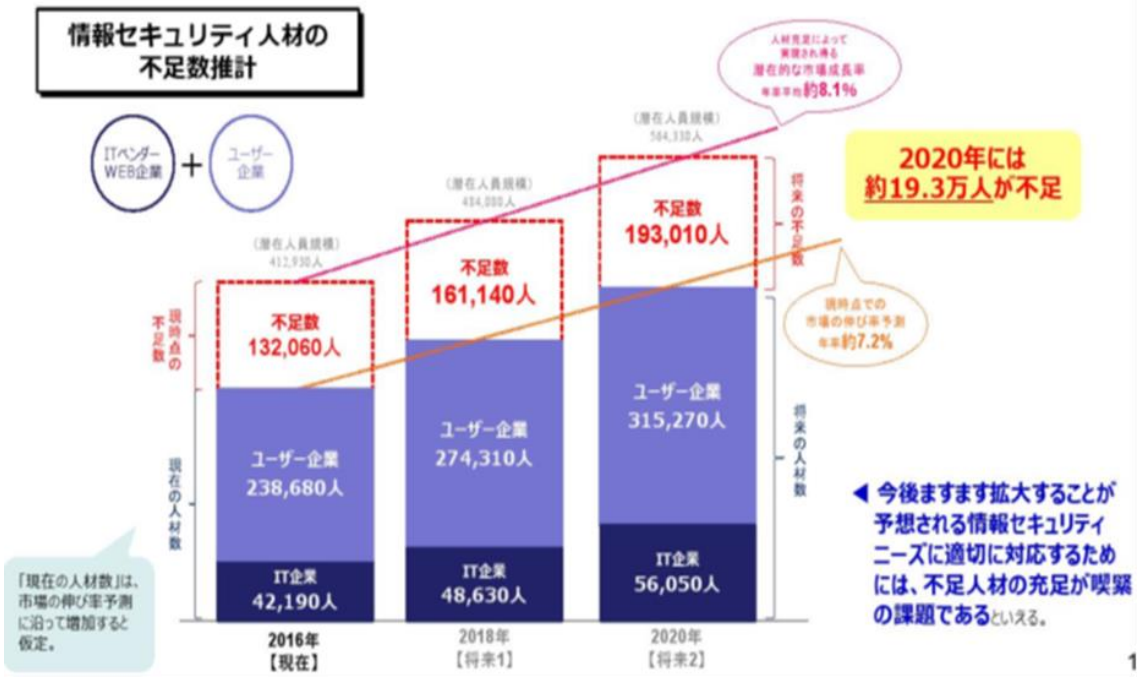
情報セキュリティ技術について、新たな技術の進展や新たな機器のネットワークへの接続等により、従来の対策に加え、情報システム、ネットワークシステムの設計・開発段階から将来的なセキュリティリスクも踏まえた構築が必要となっている

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

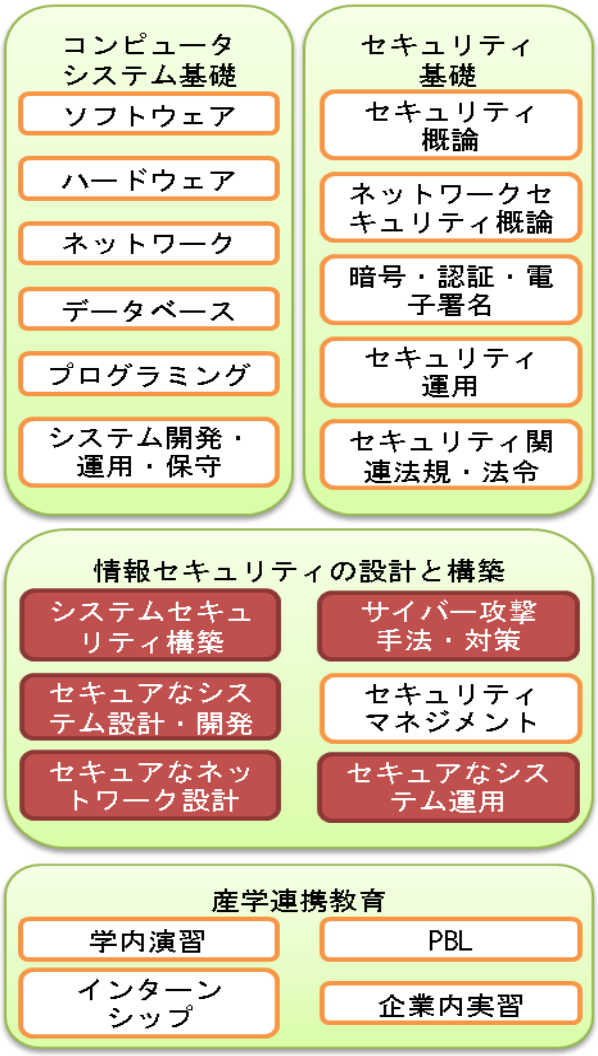
■情報セキュリティの設計と構築（本事業で開発する教育プログラム）

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

これまでの情報セキュリティの技術教育は、コンピュータネットワークセキュリティが中心のカリキュラムが実施されて、情報システムそのもののセキュアな設計・開発を学習するものはほとんどなかった。情報セキュリティの確保は、企業においてコストとして認識されており、これまでの情報システム設計・開発においては、後回しにされたり、開発費削減のために手が付けられていない領域であった。情報システム開発にとっては、優先順位の高い技術とは認識されず、教育プログラムは未整備の状態である。「当該教育カリキュラム・プログラムが必要な背景①」に記載されているように、この数年でネットワークに接続する機器が爆発的に増加したこと、今後日本が目指す Society5.0 の社会ではさら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により、全方位で情報リス

クに対応し、セキュリティの確保が求められるようになっている。しかしながら、ネットワークに接続する機器の爆発的な増加や情報技術の発展のスピードに人材育成が追付いていない状態である。

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。

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が、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ります。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

平成３０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

平成３１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

平成３２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

〇実施事項

【調査】

●情報セキュリティの Society5.0 対応実態調査

目的：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。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：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

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

※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

・システムセキュリティ構築　　60 時間

・セキュアなネットワーク設計　　60 時間

●教育教材開発

・システムセキュリティ構築

情報システムのセキュリティを構築するための教材と演習用データ

・セキュアなネットワーク設計

ネットワークシステムの情報セキュリティを設計するための知識・技術を学習するための教材

【実証講座】

●システムセキュリティ構築講座

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：平成 31 年 1 月　3 日間（6 時間×３日　18 時間）

場所：東京

●セキュアな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：平成 31 年 1 月　3 日間（6 時間×３日　18 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

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　大花　学　札幌情報未来専門学校　マネジャー
4　中村 健太郎　専門学校静岡電子情報カレッジ　教育改革室
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　　・情報セキュリティの Society5.0 対応実態調査の企画、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　　６人

開催頻度　　年４回

1　川上　隆　　情報科学専門学校
2　中村 健太郎　専門学校静岡電子情報カレッジ　教育改革室
3　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
4　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／NPO 日本ネットワークセキュリティ協会　セキュリティ啓発 WG　リーダー
5　吉田　雄哉　一般社団法人クラウド利用促進機構
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

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　株式会社日本教育ネットワークコンソシアム

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　中央情報経理専門学校高崎校

5　神馬　一博　河原電子ビジネス専門学校

6　上里　政光　専修学校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　代表取締役

○事業を推進する上で実施する調査

調査名　　情報セキュリティの Society5.0 対応実態調査

調査目的　　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。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。

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　　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

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講座
平成 31 年 1 月　3 日間（6 時間×３日　18 時間）
セキュアなネットワーク設計講座
平成 31 年 1 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　システムセキュリティ構築講座　１６名
セキュアなネットワーク設計講座　１６名
合計　３２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）

【平成 30 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

【平成 31 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

・セキュアなシステム設計・開発　コマシラバス　60 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

・セキュアなシステム設計・開発教材　テキストと演習課題

【平成 32 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）情報セキュリティの Society5.0 対応実態調査

調査目的	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。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。
調査対象	情報セキュリティ専門企業 株式会社ディアイティ　株式会社ラック
調査手法	訪問によるヒアリング
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
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
調査結果	IoT 機器のネットワーク接続による新たな脅威について ・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。

・ネットワークの部分は共通することもあるが、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。
・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。

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
・基本となる設計や開発の原理原則は変わらない
・一方で、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。
・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性がある

サイバー攻撃における新技術動向と対応について
・サイバー攻撃のトレンドを追う方法としては、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。
・同時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。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。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。
・演習や実践を行った方が良い。

専門学校の育成人材の領域の設計

1　情報システム開発企業（ベンダー）の人材について
新卒新入社員の段階で情報セキュリティの知識や技術を持っている必要はない
情報システム設計・開発におけるセキュリティは、ガイドライン等に従って設計段階で組込まれているので、個人がその技術・知識を持っている必要はない

2　ユーザー企業の情報セキュリティ人材
ユーザー企業のセキュリティは主に人的リスクに対する対応となるのでリスクマネジメント分野となる

3　情報セキュリティ専門企業の人材

サイバー攻撃に対して分析ツール等を使える人材が不足している

今後、さらに高度になるサイバー攻撃に対して対応できる人材の育成が急務である。

1.調査内容とその結果①

1. **情報セキュリティに対する脅威について**
   1. 「情報セキュリティ 10 大脅威」の項目の中で、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。
   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。

【結果】

- 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の窃取」「内部不正」という脅威が挙げられる。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。
- 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』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。

8

1.調査内容とその結果②

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**
   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収拾すれば良いと考えますか。
   2. 今後（もしくは現在）情報セキュリティ専門企業として、どういった対策をお考えですか（とられていますか）。
   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。

【結果】

- 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。
- ネットワークの部分は共通することもあるが、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。
- 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。
- 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、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。

9

1.調査内容とその結果③

3. 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
   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。

【結果】

- 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
- 一方で、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。
- 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性がある

10

1.調査内容とその結果④

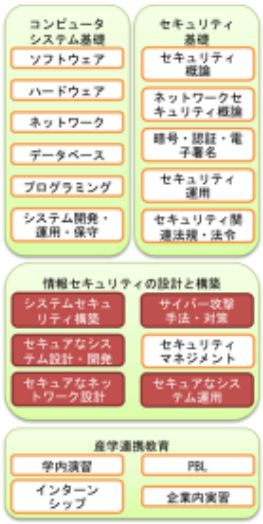
4. サイバー攻撃における新技術動向と対応について
   1. 開発者が所属する企業にとって、重要なサイバー攻撃における新技術動向と対応策を知るために、開発者はどのように情報収拾するべきだと考えますか。（上記のサイト表1で特に追うべき重要なサイトはどれですか。）
   2. 最近のサイバー技術動向で、特に重要と考えるトピックは何ですか。

【結果】

- サイバー攻撃のトレンドを追う方法としては、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。
- 同時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。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。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。
- 演習や実践を行った方が良い。

11

1.調査内容とその結果⑤



5. カリキュラムにある項目の順位づけについて
   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。

【結果】

- 「設計と構築」が重要である
- 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。
- 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。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、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。
- 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。

12

総論

- 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性
  - ✓ 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性
- 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。
  - ✓ 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るべき項目として、「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。
- 「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。
- 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を促すこと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。

13

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

・システムセキュリティ構築　　60 時間

・セキュアなネットワーク設計　　60 時間

●システムセキュリティ構築カリキュラム

学科：Society5.0 に向けたシステムセキュリティ構築	担当教員：	
科目名：	対象年次：　　実施時期：	
使用教材：	授業回数：15	
目標：Society5.0 時代のシステムセキュリティ構築ができる。		
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	第 1 章　現在・近未来 　狩猟社会、農耕社会、工業社会、情報社会、そして新たな世界へ 　Society5.0 で実現する社会 　Society5.0 の仕組み 　経済発展と社会的課題の解決を両立 　各分野における新たな価値の事例 　Society 5.0 による人間中心の社会 理解度確認方法　ペーパーテスト	
2	第 2 章　暗号化・認証 　暗号の用語 　暗号アルゴリズム、鍵、暗号強度 　暗号解読と安全性 　電子政府推奨暗号リスト 　共通鍵暗号	

	公開鍵暗号 演習「公開鍵暗号方式による暗号化と復号」 ハッシュ関数とメッセージ認証コード デジタル署名 認証局とデジタル署名 認証技術 セキュリティチップ 理解度確認方法	
3	第3章　セキュリティプロトコル 認証プロトコル SSL/TLS HTTPS IPSec S/MIME PGP VPN 演習「認証局の構築とサーバ証明書の発行」 演習「S/MIME を用いた暗号化メールの送受信」 理解度確認方法　ペーパーテスト	
4	第4章　不正アタック対策 リスクとは何か 管理策とは何か システム管理者向け対策 利用者向け対策 家庭における対策 ウィルス対策 不正アクセス対策 脆弱性対策 標的型攻撃対策 IoT	

	制御システム 演習「Microsoft Security Baselinesによるセキュリティ構成の確認」 理解度確認方法　ペーパーテスト	
5	第5章　可用性、物理的セキュリティ 機密性、完全性、可用性 論理的セキュリティ、人的セキュリティ、物理的セキュリティ、運用 二重化とバックアップ 単一ポイント障害 ディスクの冗長構成 コンピュータの冗長構成 冗長ネットワーク 業務拠点喪失からの復旧 警備員、マントラップ 記憶媒体 情報の消去 理解度確認方法　ペーパーテスト	
6	第6章　情報セキュリティマネジメント 情報資産管理の計画 リスク評価とリスク対応 情報資産に関する情報セキュリティ要求事項の提示 情報セキュリティ要求事項 情報資産管理 情報セキュリティの確保 インシデントの管理 情報セキュリティの意識向上 コンプライアンス 情報セキュリティマネジメントの継続的改善	

	情報セキュリティに関する動向・事例情報の収集と評価 PDCA サイクル ISMS 認証 システム監査制度、プライバシマーク制度 理解度確認方法　ペーパーテスト	
7	第 7 章　サーバとシステム基盤 機密性、完全性、可用性を実現する土台 機密性 完全性 可用性 演習「パスワードクラッキング」 理解度確認方法　ペーパーテスト	
8	第 8 章　Web システム Web システムの 3 階層構造 Web サーバのセキュリティ対策 Web アプリケーションのセキュリティ対策 ネットワークのセキュリティ対策 その他のセキュリティ対策 演習「SQL インジェクションの体験と対策」 理解度確認方法　ペーパーテスト	
9	第 9 章　VPN VPN の基本技術構成 インターネット VPN IP-VPN 理解度確認方法　ペーパーテスト	
10	第 10 章 無線 LAN	

	無線 LAN の規格 暗号化と認証の仕組み セキュリティ対策 無線 LAN の物理特性 インシデント事例 理解度確認方法　ペーパーテスト	
11	第 11 章 セキュアプログラミング セキュリティ・バイ・デザイン 既知の脆弱性への対応 未知の攻撃および対応漏れを意識した対応 設計原則 実装原則 脅威モデリング 開発プロセス 計画すべきセキュリティ機能 情報の収集 理解度確認方法　ペーパーテスト	
12	第 12 章 個人を対象としたもの 基本的な対策 インターネット 電子メール 情報機器 演習「身近な脅威の例と対策」 理解度確認方法　ペーパーテスト	
13	第 13 章 組織や不特定多数を対象としたもの 社員・職員 組織幹部 情報管理担当者	

	理解度確認方法　ペーパーテスト	
14	第 14 章 セキュリティインシデントへの対応 情報セキュリティインシデントとは 組織の取り組み（CSIRT） 社会全体の取り組みや制度 セキュリティ関連法案 インシデント管理と対応チーム インシデント発生前の備え インシデント対応ポリシーの作成 インシデントハンドリング インシデント対応計画 標準運用手順書 事後処理 演習「インシデントの例と初期対応の検討」 理解度確認方法　ペーパーテスト	
15	第 15 章 Socity5.0 の担い手として Society 5.0 の社会像 これまでの振り返り 求められる人材像 Society 5.0 の主役たれ 理解度確認方法　学習内容のグループディスカッション	

●セキュアネットワーク設計カリキュラム

学科：Society5.0 に向けたセキュア・ネットワーク設計	担当教員：
科目名：	対象年次：　　実施時期：
使用教材：	授業回数：60 分×4 回×15 コマ
目標：Society5.0 時代のネットワークセキュリティ設計ができる。	

前提知識： ・ネットワークの基本用語を説明できる(TCP/IP, OSI 参照モデル, IPSec など) ・情報セキュリティについて学習済みである。		
回数	学習項目	備考
1	1. 第 1 章　Society5.0 とネットワーク 2. 第 2 章　ネットワークセキュリティとは 3.　守りたいものは何ですか 4.　演習「情報資産の洗い出しとリスクの検討」 理解度確認方法　演習の相互評価	
2	1.　避けられないセキュリティ侵害 2.　立場によって違う対策 理解度確認方法 ペーパーテスト	各内容とも 2 コマ（2 時間）。
3	1. 第 3 章　プロトコルのセキュリティ 2.　演習「中間者攻撃の体験」 3.　演習「ポートスキャンによるサーバ探索」 4.　演習「ネットワークスニファによる通信傍受と暗号化」 理解度確認方法　演習結果の相互評価	プロトコルのセキュリティで 2 時間。演習は 3 種類で 2 時間分。
4	1.　ネットワークサーバのセキュリティ 2. 第 4 章　ネットワークセキュリティ設計（概要） 3. 第 5 章　OSI 参照モデルとファイアウォール（L1～L4） 理解度確認方法　ペーパーテスト	ネットワークサーバのセキュリティで 2 時間。
5	1.　演習「フィルタリングルールの設計と実践」 2. 第 5 章　OSI 参照モデルとファイアウォール（L5～L7） 3.　アンチマルウェア 4. 第 6 章　ネットワークの分離（スイッチ） 理解度確認方法　ペーパーテスト	

6	1. 第 6 章　ネットワークの分離（VLAN、ルーター、DMZ） 2.　演習「（VLAN によるネットワーク分割と）ルーターによるネットワーク分割」 理解度確認方法	ネットワークの分離で 3 時間。
7	1. 第 7 章　アカウントセキュリティ（認証、認可、ログと監査） 2.　演習「Windows ローカルグループとセキュリティグループ」 3.　特権アカウントの制限 理解度確認方法　アカウントセキュリティと演習の関係性の説明	アカウントセキュリティおよび特権アカウントの制限で 3 時間
8	1.　アカウントの統合管理 2. 第 8 章　アクセス制御 理解度確認方法　ペーパーテスト	それぞれ 2 時間ずつ
9	1. 第 9 章　侵入検知と防御（概要、IDS/IPS、動的解析、ハニーポット） 2.　演習「侵入検知システムの構築」 理解度確認方法　演習結果の相互評価	侵入検知と防御で 3 時間
10	1. 第 9 章　侵入検知と防御（L7 ファイアウォール） 2.　演習「Web プロキシーの構築とコンテンツフィルタリング」 3.　セキュリティイベント情報の管理 4. 第 10 章　裏口をふさぐ（概要） 理解度確認方法　ペーパーテスト	
11	1. 第 10 章　裏口をふさぐ（RAS、Bluetooth、携帯端末） 2. 第 11 章　無線 LAN（脅威、認証、暗号化、物理特性） 3.　演習「RADIUS サーバ構築と無線 LAN 環境構築」 理解度確認方法　ペーパーテスト	無線 LAN で 2 時間

12	1. 第 12 章　検疫ネットワーク 2. 第 13 章　セキュリティ情報の管理 3.　脆弱性情報の管理（CVE、NVD、JVN） 4.　演習「NSE、OpenVAS による脆弱性検査、Metasploit」 理解度確認方法　ペーパーテスト	
13	1.　脆弱性情報の管理（ベンダー公開情報、最新情報の収集） 2.　資産情報の管理 3. 第 14 章　暗号による情報の保護と暗号化通信（データの暗号化） 理解度確認方法　ペーパーテスト	資産情報の管理で、Society5.0 と絡めて 2 時間ほど。
14	1. 第 14 章　暗号による情報の保護と暗号化通信（電子署名の仕組み） 2.　暗号化通信 3.　演習「グループポリシーによる、特定通信経路の IPSec 暗号化」 理解度確認方法　演習内容の説明	暗号化通信で 3 時間
15	1.　ファイル、ディスクの暗号化 2. 第 15 章　信頼の創出、証明、チェーンの構築と維持 3.　演習「IoT ネットワーク導入計画シミュレーション」 理解度確認方法 導入計画の相互評価	少なくとも演習で 2 時間はとる。ファイル、ディスクの暗号化は前倒ししてもよい。

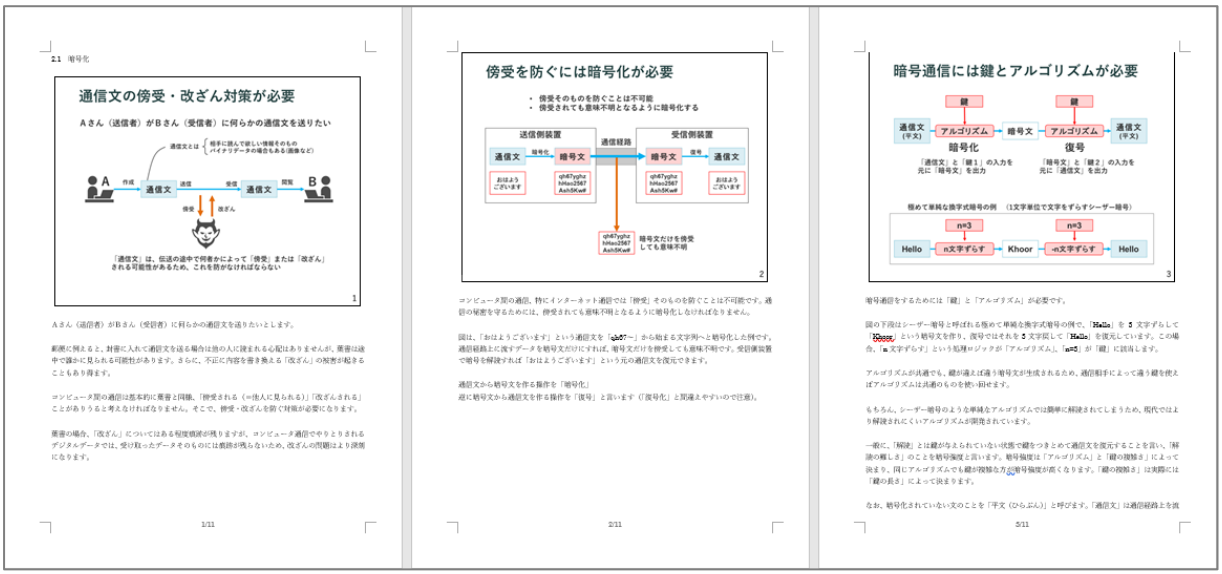
（２）教材

以下２点の教材を開発・整備した

・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

教材のイメージ



３．実証講座

本年度、実証講座の実施は見送りとした。

※教育カリキュラム・教材開発スケジュール遅れおよび実証実施を予定していた専門学校の実施期間の調整ができなかったため

３．次年度以降の活動

１．実証検証

（１）システムセキュリティ構築教育プログラム

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
平成 31 年 8 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　　システムセキュリティ構築講座　１６名

（２）セキュアなネットワーク設計教育プログラム

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）　セキュアなネットワーク設計講座
平成 31 年 8 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　　セキュアなネットワーク設計講座　１６名

（３）平成３１年度開発教材の実証検証

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
平成 31 年 11 月　3 日間（6 時間×３日　18 時間）
・セキュアなシステム設計・開発講座
平成 31 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　　３０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。

２．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。

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

成 果 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。