令和２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
が実施した令和２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

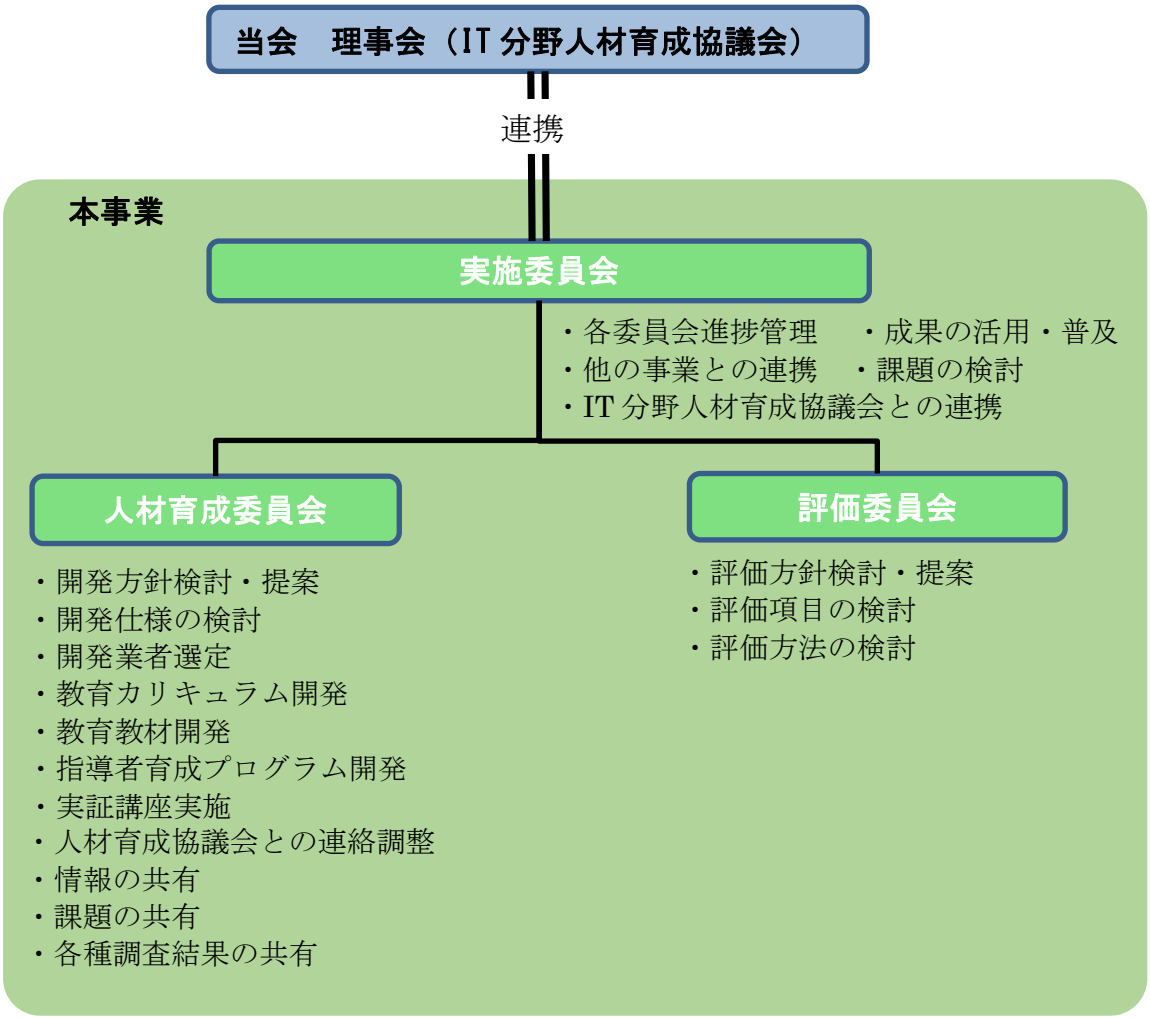
7　一般社団法人クラウド利用促進機構

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）



（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

・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）

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

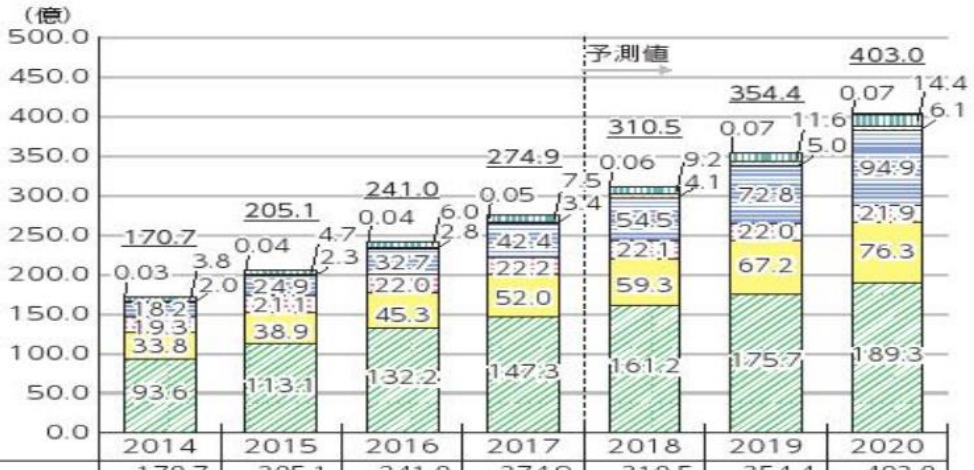
これまでパソコンによるインターネット通信が中心であった情報通信ネットワークは、スマートフォンや新たなデバイスの進展により、デバイス等の相互通信にも使用されるようになり、ネットワークに接続されている機器は、劇的に増加している。また、日本が今後目指す Society5.0 の社会では、すべての人を取り巻く機器がネットワークに接続され、情報を相互にやり取りすることが想定されているため、さらにネットワーク上の機器は増加が続くと予測される。（右上図は、IoT 機器数の推移と予測：５年で倍近くに増加している）

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。

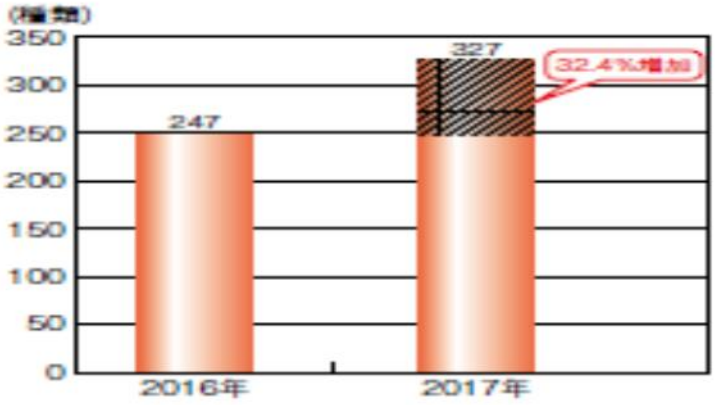
世界の IoT デバイス数の推移及び予測　　出展：平成 30 年度情報通信白書



	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

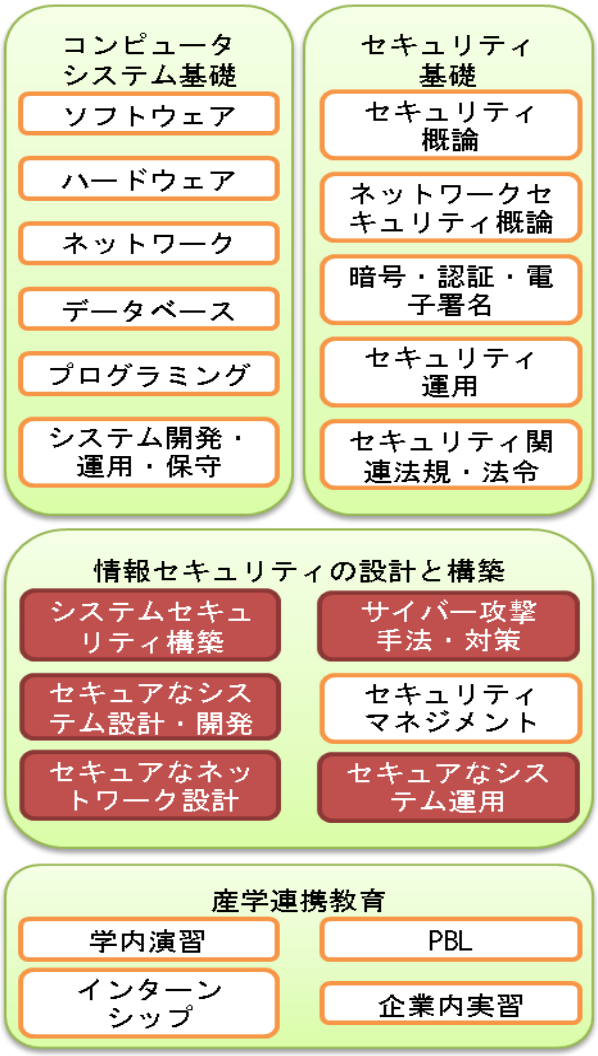
■情報セキュリティの設計と構築（本事業で開発する教育プログラム）

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

平成３０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
　　・情報システム開発技術者のセキュリティ知識
　教育教材　・セキュアなネットワーク設計の見直し
　　・サイバー攻撃手法・対策教材
　　・情報システム開発者に必要な情報セキュリティ

●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

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 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）
　教員教材　　・映像教材（サイバー攻撃手法・対策）と指導書

●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運用講座

ⅱ）今年度の具体的活動

○実施事項

【開発】

●教育カリキュラム・シラバス開発

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

●教育教材開発

・セキュアなシステム運用教材

情報セキュリティを確保して、システム運用を行う技術と知識の教材

●教員用教材

・映像教材（サイバー攻撃手法・対策）と指導書

【実証講座】

●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：2020 年 9 月　　3 日間（6 時間×３日　18 時間）

定員：20 名

●セキュアなシステム運用講座

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：2020 年 12 月　　3 日間（6 時間×３日　18 時間）

定員：20 名

●教員研修会

目的：情報セキュリティの科目を担当するための知識と授業の運用を開発した映像教材をもとに解説し、内容・効果の検証を行う。

対象：情報系専門学校教員

期間：2020 年 12 月　　2 日間（6 時間×２日　12 時間）

定員：２０名

【成果の普及】

●成果物の配布　　情報系専門学校、情報系企業団体に配布

●成果報告会の実施　　2021 年 2 月　場所：東京

●成果のホームページでの公開

【委員会】

・実施委員会　4 回開催　8 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。

・人材育成委員会　4 回開催　12 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・モデル化に関する検討・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

・評価委員会　4 回開催　８名

事業開始時、事業期間中の 1 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。

実証検証の評価（方法・基準の設計）、評価者の選定、

○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４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　　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　　１１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	専門学校中央情報大学校
5	上里　政光	国際電子ビジネス専門学校
6	稲垣　実	船橋情報ビジネス専門学校
7	川人 宏行	専門学校穴吹コンピュータカレッジ
8	菊池　一路	日本工学院専門学校
9	柳谷　博道	早稲田文理専門学校
10	北原　聡	麻生情報ビジネス専門学校
11	菊嶋　正和	株式会社サンライズ・クリエイティブ

会議名③　　評価委員会

目　的　　・情報セキュリティ教育の専修学校が担う領域・範囲・レベルの検討と協議

・本事業の開発カリキュラム・教材の評価

・実証講座、教員育成の評価

・成果の活用・普及に関する評価

検討の具体的内容　・専修学校の情報セキュリティ教育の在り方の検討（人材需要等を踏まえ、産業界に供給する人材を明確化）
・本事業の教育プログラム（カリキュラム・教材、他）が育成すべき人材に一致しているかを検討・協議～評価
・教員の研修プログラムの評価
・実証講座の結果検証と評価
・成果の活用（利用できるのもかどうか）や普及（方法や対象）に関する評価
・評価項目、評価方法、評価手法の検討・協議
・評価者の選定と評価の依頼

委員数　８人

開催頻度　年４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	菅原　一博	学校法人管原学園 理事長
3	山本　匡	学校法人小山学園 理事長
4	武田　結幸	学校法人武田学園 理事長
5	秋葉　英一	学校法人秋葉学園 理事長
6	黒木　雄太	学校法人黒木学園
7	柏尾　典秀	学校法人栗原学園北見情報ビジネス専門学校
8	飯塚　久仁子	一般社団法人全国専門学校情報教育協会

○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）●サイバー攻撃手法・対策講座

3 日間（6 時間×３日　18 時間）

●セキュアなシステム運用講座

3 日間（6 時間×３日　18 時間）

実施手法　　実証講座実施協力校の学生・卒業生に対して募集を行う。

実習を通して技術が定着するよう講義４　実習６の割合で講座を設計する

受講者の達成度を計測する

想定される受講者数　各２０名　計４０名

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。

●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

・情報システム開発技術者のセキュリティ知識　テキスト

【2020 年度】

●教育カリキュラム・シラバス

・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

●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「サイバー攻撃手法・対策」の知識・技術を学習し、講義するための映像教材と指導書

・評価手法

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、学習した学習者の評価（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。

●「情報セキュリティ教育」に関する情報提供を本会 Web サイトを利用して行い、専門学校教員の教育実践を支援する。

２．事業の成果

１．教育プログラムの開発

（１）モデル・カリキュラム

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した。

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、運用に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。

○カリキュラム表（抜粋）

学科：コンピュータシステム基礎	担当講師：
科目名：ハードウェアの基本	授業回数：23 コマ（回）
科目概要：コンピュータを構成するハードウェアの基本について学ぶ。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	コンピュータの種類と構成	
2	ハードウェアとは	
3	プロセッサの基本①種類と特徴	
4	プロセッサの基本②アーキテクチャ	
5	プロセッサの基本③制御装置・演算装置の役割	
6	プロセッサの基本④動作原理―演算の仕組み	
7	プロセッサの基本⑤動作原理―命令とアドレッシング	
8	プロセッサの基本⑥動作原理―割込み	
9	プロセッサの基本⑦クロック周波数、CPI、MIPS	
10	プロセッサの基本⑧高速化技術	
11	プロセッサの基本⑨並列処理	
12	プロセッサの基本⑩マルチプロセッサシステム	
13	メモリの基本①種類と特徴	
14	メモリの基本②主記憶装置	
15	メモリの基本③記憶階層	
16	メモリの基本④アクセス方式	
17	メモリの基本⑤メモリの容量と性能	
18	メモリの基本⑥記録媒体の種類と特徴	
19	バスの種類と特徴	
20	入出力インターフェイスの種類と特徴	
21	入力装置の種類と特徴	
22	出力装置の種類と特徴	
23	補助記憶装置の種類と特徴	

学科：コンピュータシステム基礎	担当講師：
科目名：ソフトウェアの基本	授業回数：11 コマ（回）
科目概要：コンピュータを構成するソフトウェアの基本について学ぶ。	
評価方法：	
前提知識：特になし。	

回数	学習項目	備考
1	ソフトウェアとは	
2	オペレーティングシステムの種類と特徴	
3	オペレーティングシステムの基本機能と構成	
4	オペレーティングシステムにおける管理の仕組み①（ジョブ管理、タスク管理、データ管理、入出力管理、記憶管理）	
5	オペレーティングシステムにおける管理の仕組み②（ネットワーク制御、運用管理、ユーザ管理、セキュリティ制御、障害管理）	
6	アプリケーションとは	
7	ミドルウェアの役割と機能	
8	ファイルシステムの種類と特徴	
9	開発ツールの種類と特徴、機能	
10	オープンソースソフトウェアの種類と特徴	
11	オープンソースソフトウェアの活用と最新動向	

学科：情報セキュリティの設計と構築	担当講師：
科目名：サイバー攻撃手法	授業回数：22 コマ（回）
科目概要：サイバー攻撃に関する詳細な攻撃手法について学習する。	
評価方法：	
前提知識：「セキュリティ基礎」で学んだ知識。	

回数	学習項目	備考
1	サイバー攻撃対策の考え方	
2	サイバー攻撃対策の種類①入口・出口対策	
3	サイバー攻撃対策の種類②多層防御	
4	マルウェアの動作内容と種類	
5	マルウェアへの対策	
6	不正アクセスの攻撃手法	
7	不正アクセスへの対策	
8	アプリケーションに対する攻撃手法	
9	アプリケーションへの攻撃対策	
10	主な攻撃手法①辞書攻撃、総当たり攻撃、パスワードリスト攻撃	
11	主な攻撃手法②クロスサイトスクリプティング、クロスサイトリクエストフォージェリ、クリックジャッキング	
12	主な攻撃手法③ドライブバイダウンロード、SQL インジェクション、ディレクトリトラバーサル	
13	主な攻撃手法④レインボーテーブル、サイドチャネル攻撃、ディレクトリリスティング、OS コマンドインジェクション	
14	主な攻撃手法⑤中間者攻撃、MITB 攻撃、第三者中継	
15	主な攻撃手法⑥DNS キャッシュポイズニング、DNS 水責め攻撃、IP スプーフィング	
16	主な攻撃手法⑦セッションハイジャック、セッション ID 固定化攻撃、リプレイ攻撃	
17	主な攻撃手法⑧DoS 攻撃、DDoS 攻撃、EDoS 攻撃、電子メール爆弾	
18	主な攻撃手法⑨標的型攻撃、APT、水飲み場型攻撃	
19	主な攻撃手法⑩フィッシング、ワンクリック詐欺、スミッシング	
20	主な攻撃手法⑪ゼロデイ攻撃、サイドチャネル攻撃	
21	主な攻撃手法⑫テンペスト攻撃、ポートスキャン	

22	主な攻撃手法⑬ダウングレード攻撃、フットプリンティング、SEO ポイズニング	

（２）セキュアなシステム運用教材

情報セキュリティを確保して、システム運用を行う技術と知識の教材を開発した

第１章　セキュリティ構築

1-1　情報システムにおける脅威と脆弱性

1-2　サイバー攻撃対策の考え方

1-3　主なセキュリティ技術

1-4　セキュアプロトコル

1-5　ハードウェアへの実装

第２章　セキュアなシステム設計

2-1　セキュリティアーキテクチャ

2-2　CC の概要と構成

2-3　テレワークに必須なゼロトラストセキュリティ

第３章　セキュリティマネジメント

3-1　リスクマネジメント

3-2　情報セキュリティマネジメントシステム（ISMS）

3-3　セキュリティポリシーの策定

3-4　ISMS の規格

第４章　セキュアなシステム運用

4-1　情報セキュリティ監査

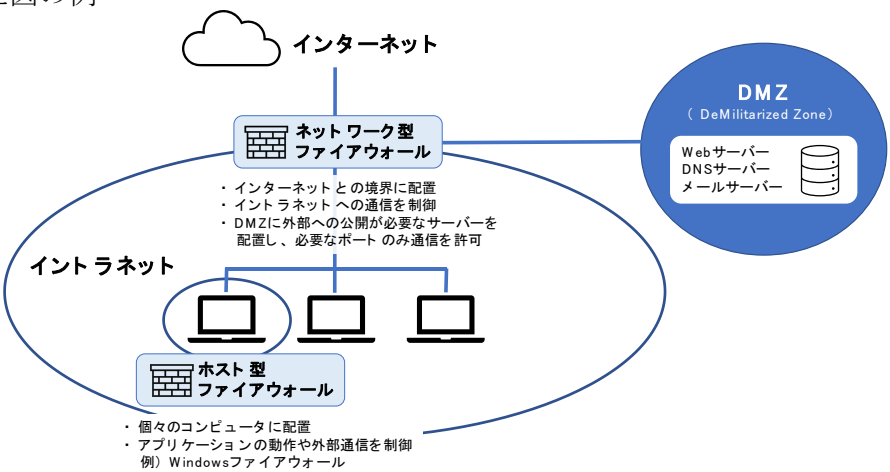
4-2　インシデント対応の基本

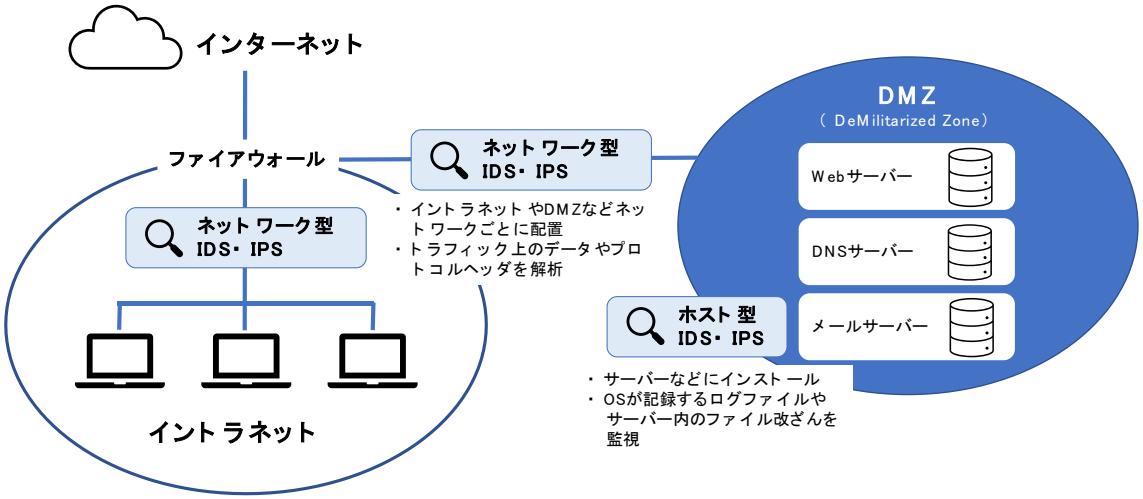
4-3　デジタルフォレンジックのプロセス

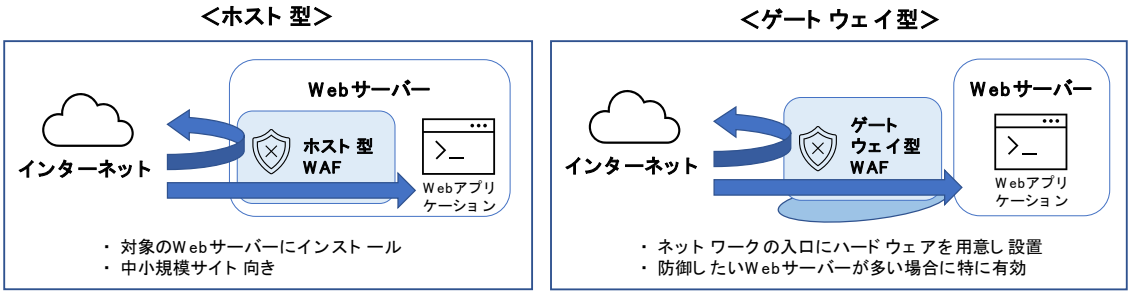
4-4　デジタルフォレンジックの実践

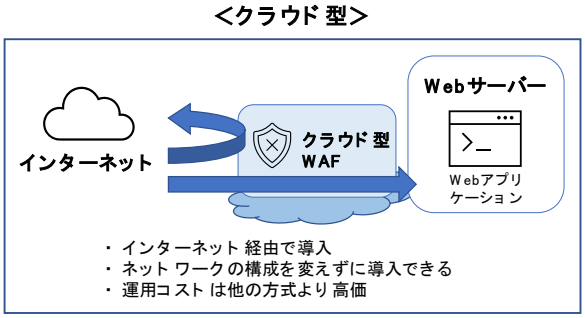
図を多く差し込み、ビジュアル的にわかりやすくまとめた

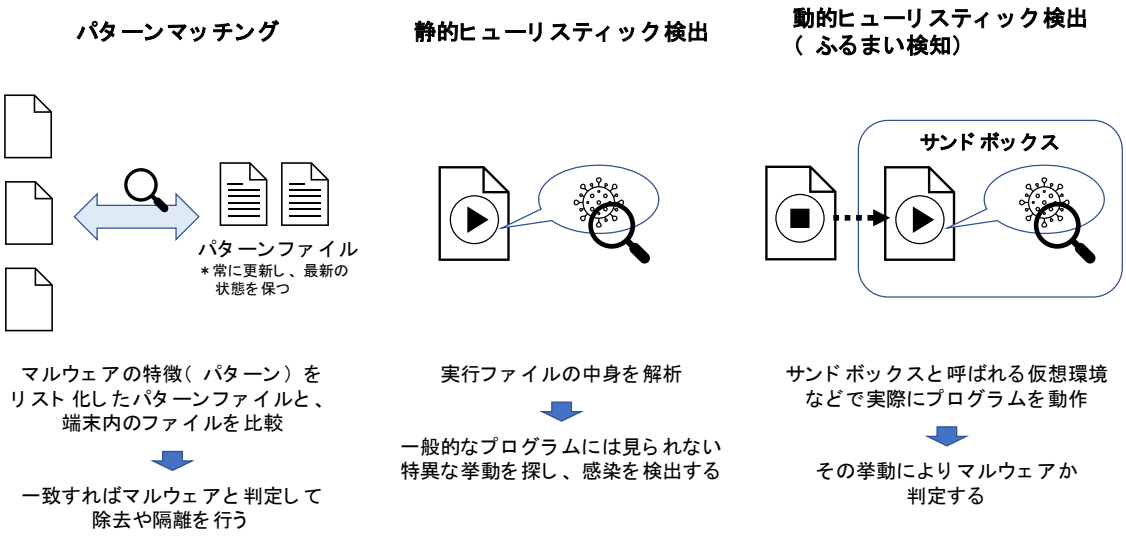
用いた図の例




インターネット
ファイアウォール
ネットワーク型
IDS・IPS
・イントラネットやDMZなどネットワークごとに配置
・トラフィック上のデータやプロトコルヘッダを解析
DMZ
（DeMilitarized Zone）
Webサーバー
DNSサーバー
メールサーバー
ホスト型
IDS・IPS
・サーバーなどにインストール
・OSが記録するログファイルやサーバー内のファイル改ざんを監視
ネットワーク型
IDS・IPS
イントラネット


<ホスト型>
Webサーバー
インターネット
ホスト型
WAF
Webアプリケーション
・対象のWebサーバーにインストール
・中小規模サイト向き
<ゲートウェイ型>
Webサーバー
インターネット
ゲートウェイ型
WAF
Webアプリケーション
・ネットワークの入口にハードウェアを用意し設置
・防御したいWebサーバーが多い場合に特に有効


<クラウド型>
Webサーバー
インターネット
クラウド型
WAF
Webアプリケーション
・インターネット経由で導入
・ネットワークの構成を変えずに導入できる
・運用コストは他の方式より高価


パターンマッチング
静的ヒューリスティック検出
動的ヒューリスティック検出
（ふるまい検知）
パターンファイル
＊常に更新し、最新の状態を保つ
サンドボックス
マルウェアの特徴（パターン）をリスト化したパターンファイルと、端末内のファイルを比較
一致すればマルウェアと判定して除去や隔離を行う
実行ファイルの中身を解析
一般的なプログラムには見られない特異な挙動を探し、感染を検出する
サンドボックスと呼ばれる仮想環境などで実際にプログラムを動作
その挙動によりマルウェアか判定する

（3）サイバー攻撃　ビデオ教材と演習手順書

教員用にビデオ・指導書を作成予定であったが、新型コロナウイルス感染症拡大防止、緊急事態宣言等により、休校せざるを得ない状況であった教育機関では、遠隔授業やｅラーニングを通して非接触形式の授業・講座実施の要望が多くあった。実施員会等の意見から、教員用のビデオではなく、遠隔授業やｅラーニングに活用できるビデオ教材を整備した。

実習環境の構築や遠隔での実習・演習を適切に進めることができるよう手順書という形式で解説を取りまとめた。

ビデオ教材の作成範囲は、昨年度開発した「サイバー攻撃手法・対策」の遠隔教育や演習のバランスを考慮し、一部を抜粋して作成した。また、学習効果を計測するための確認テストを整備した。

■ビデオ化した項目

サイバー攻撃手法・対策

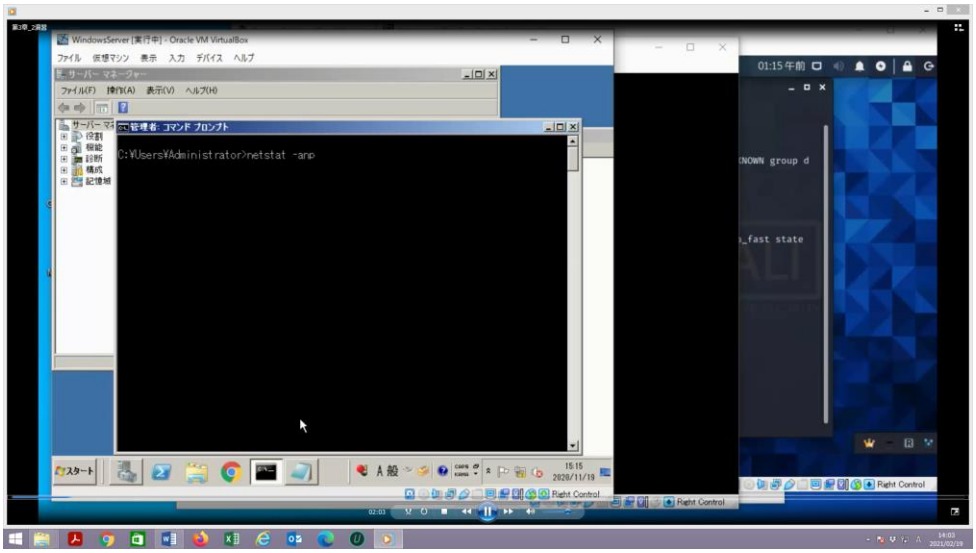
第 3 章　　ネットワークを狙った攻撃を知る

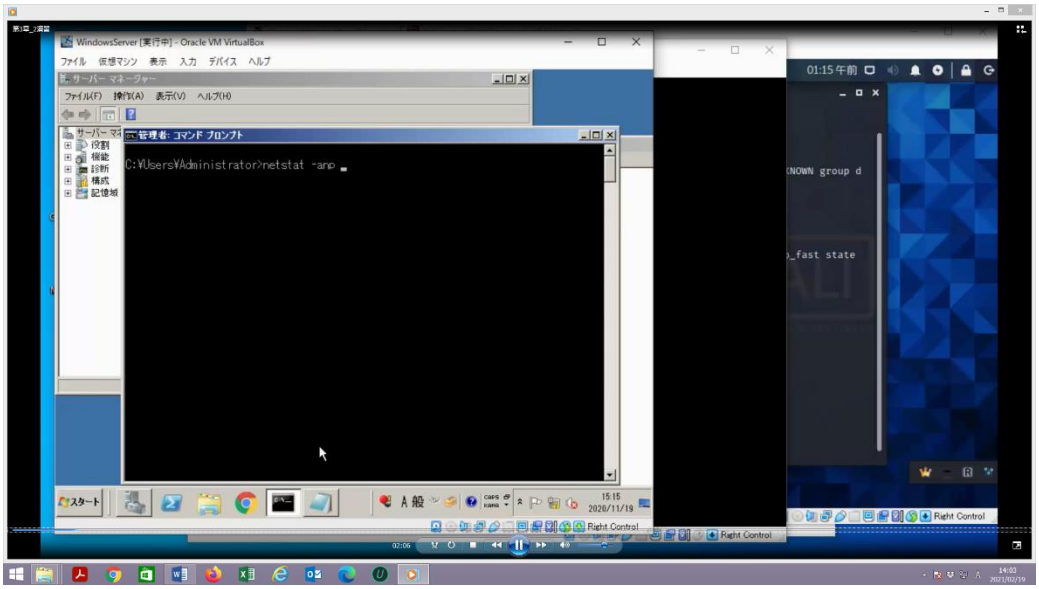
第 4 章　　ネットワークの通信を把握する

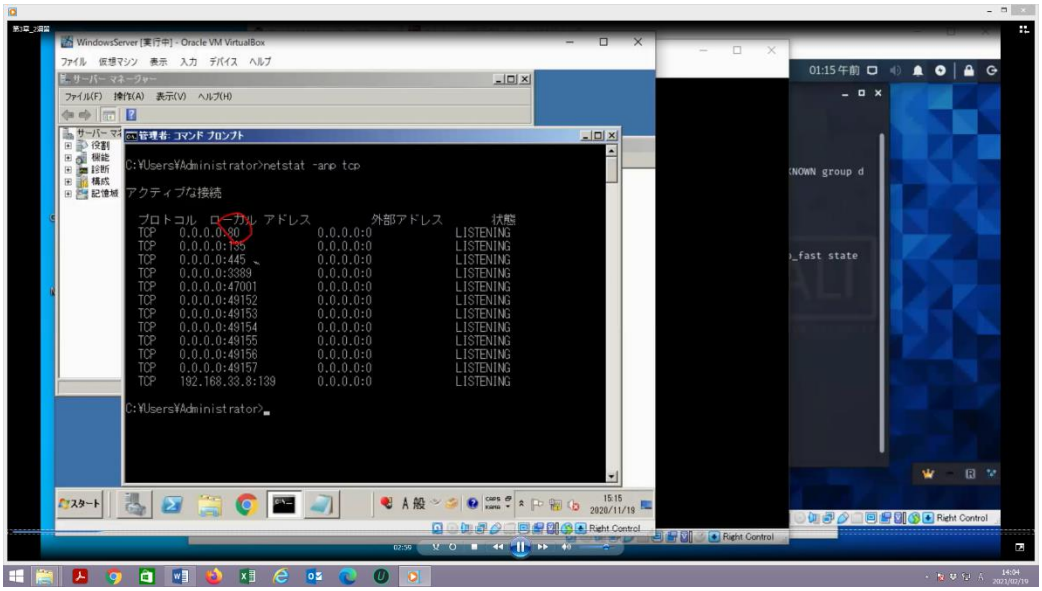
第 6 章　　脆弱性を狙った攻撃を知る

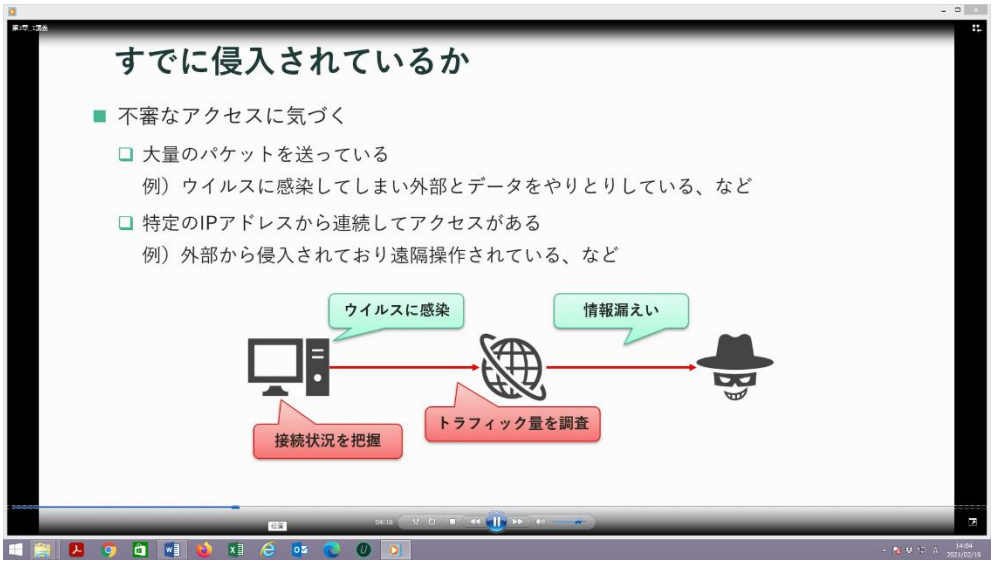
第 8 章　　暗号技術について改めて学ぶ

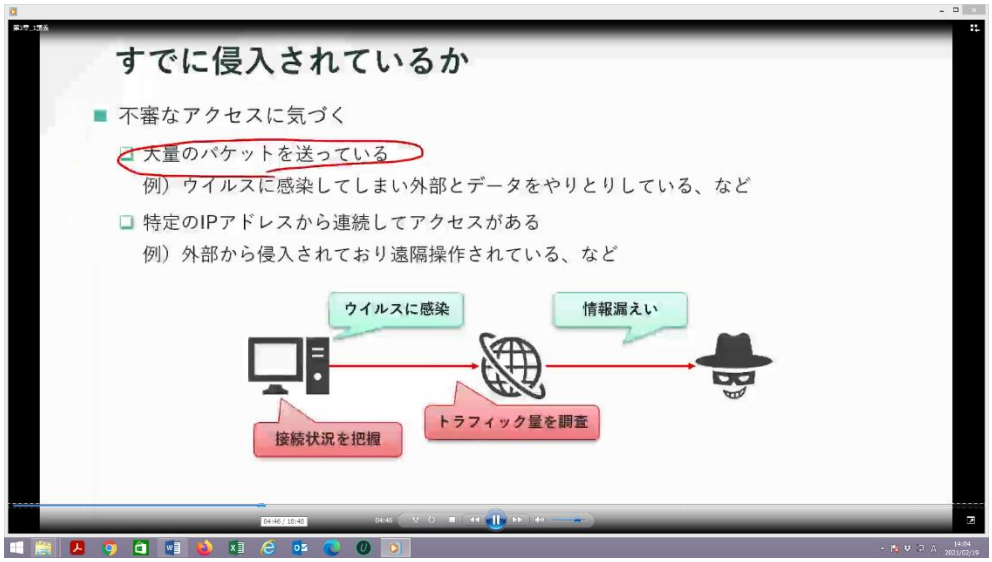
第 11 章　　組織のセキュリティをマネジメントする

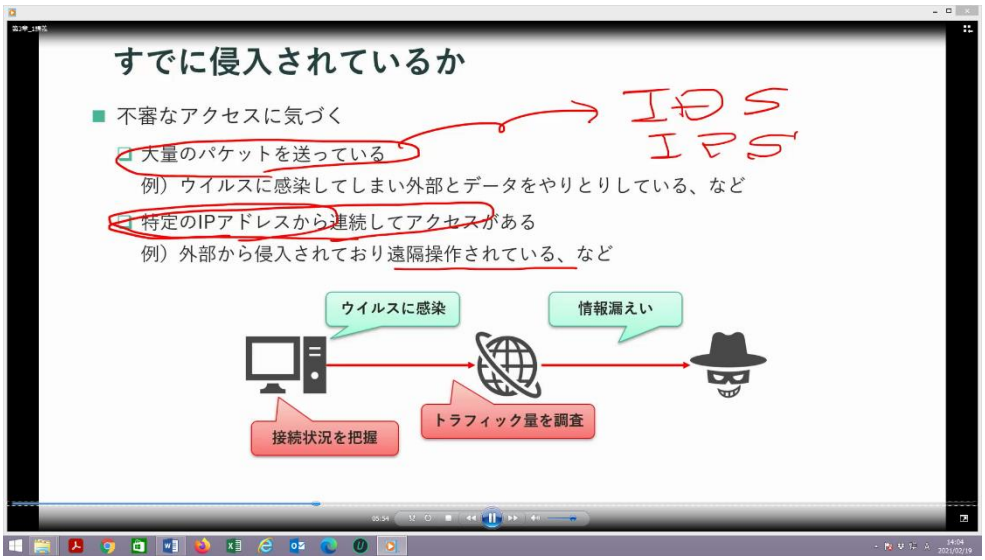


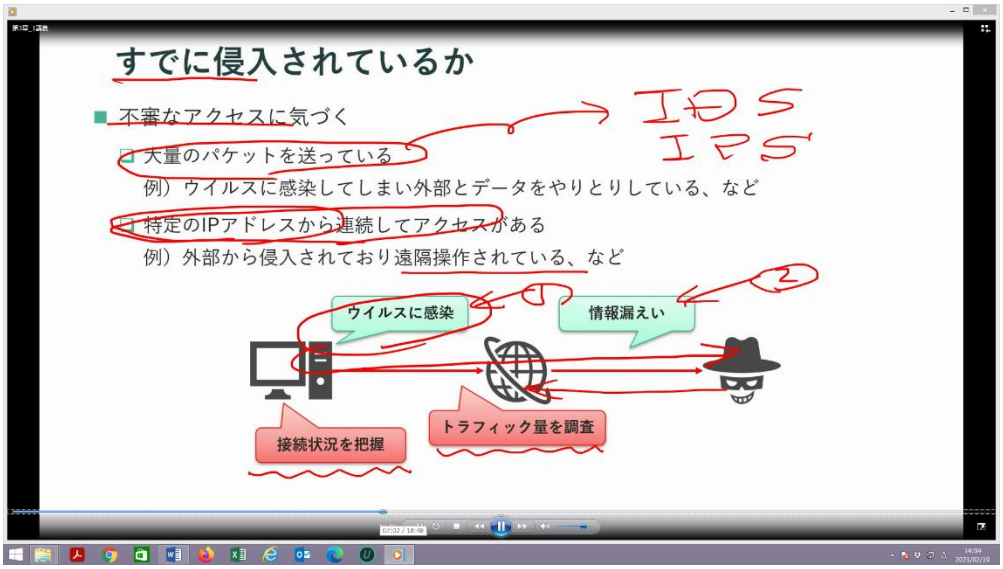

WindowsServer [実行中] - Oracle VM VirtualBox
ファイル 仮想マシン 表示 入力 デバイス ヘルプ
サーバー マネージャー
ファイル(F) 操作(A) 表示(V) ヘルプ(H)
管理者: コマンド プロンプト
C:¥Users¥Administrator>netstat -anp
01:15 午前
Right Control


WindowsServer [実行中] - Oracle VM VirtualBox
ファイル 仮想マシン 表示 入力 デバイス ヘルプ
サーバー マネージャー
ファイル(F) 操作(A) 表示(V) ヘルプ(H)
管理者: コマンド プロンプト
C:¥Users¥Administrator>netstat -anp tcp
アクティブな接続
プロトコル ローカル アドレス 外部アドレス 状態
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING
TCP 192.168.33.8:139 0.0.0.0:0 LISTENING
C:¥Users¥Administrator>
01:15 午前
Right Control


すでに侵入されているか
不審なアクセスに気づく
大量のパケットを送っている
例）ウイルスに感染してしまい外部とデータをやりとりしている、など
特定のIPアドレスから連続してアクセスがある
例）外部から侵入されており遠隔操作されている、など
ウイルスに感染
情報漏えい
接続状況を把握
トラフィック量を調査


すでに侵入されているか
不審なアクセスに気づく
大量のパケットを送っている
例）ウイルスに感染してしまい外部とデータをやりとりしている、など
特定のIPアドレスから連続してアクセスがある
例）外部から侵入されており遠隔操作されている、など
ウイルスに感染
情報漏えい
接続状況を把握
トラフィック量を調査


すでに侵入されているか
不審なアクセスに気づく
大量のパケットを送っている
例）ウイルスに感染してしまい外部とデータをやりとりしている、など
特定のIPアドレスから連続してアクセスがある
例）外部から侵入されており遠隔操作されている、など
IDS
IPS
ウイルスに感染
情報漏えい
接続状況を把握
トラフィック量を調査



確認テスト 設問と選択肢

章	問題番号	
3	設問1	新規に構築したサーバー上で、空いているポートを確認したい。以下の手法のうち、最も適切な手法はどれか。
		選択肢1：ポートスキャン 選択肢2：netstatコマンド 選択肢3：ファイアウォール 選択肢4：サービスの一覧
	設問2	新規に構築したサーバーで、利用者から確認できる空きポートを確認したい。以下の手法のうち、最も適切な手法はどれか。
		選択肢1：ポートスキャン 選択肢2：netstatコマンド 選択肢3：ファイアウォール 選択肢4：サービスの一覧
	設問3	以下の説明のうち、正しい説明はどれか。
		選択肢1：サービスに脆弱性があれば、ポートが閉じていてもネットワーク経由で該当するサービスに直接侵入できる。 選択肢2：必要なポート以外が閉じていれば、不要なサービスが原因で攻撃されることはない。 選択肢3：ランダムなポートに対する連続アクセスがあれば、攻撃を受けている可能性がある。 選択肢4：ファイアウォールでポート設定する場合、すべてのポートを開いた上で、侵入される可能性のあるポートを閉じる。
	設問4	サーバーにおけるnetstatの結果とnmapの結果で、検出されたポートが異なっていました。この状況に対する適切な理解は次のどれですか（複数選択）。
		選択肢1：netstatの実行結果にはファイアウォールの設定が反映されることがあるため、問題は無い 選択肢2：通信経路にファイアウォールが設置されていない可能性が高い 選択肢3：nmapでは脆弱なポートのみが表示される 選択肢4：サーバーを利用するために必要なポートのみがnmapで検出できれば操作に支障は無い。
	設問5	あるWebサーバーで開放中のポートを調べたところ、TCP 20と21が開放されていました。この状況に対してとるべきアクションがあるとすれば以下のどれですか。なお変更する場合、利用者に対しては適切な通知がなされるものとします。
		選択肢1：Webコンテンツをアップロードするために必要なので、この状況で問題は無い。 選択肢2：Telnetによる外部からの操作が有効なままなので、ポートを閉じる必要がある。 選択肢3：ファイル転送にSSHを使うべきなので、SSH接続を有効にした上で2つのポートを閉じる。 選択肢4：TCP 20と21は暗号化されていないため、暗号化プロトコルであるHTTPSを有効にする必要がある。

２．実証講座

●サイバー攻撃手法・対策講座(3 日間)、●セキュアなシステム運用講座(3 日間)を計画していたが、新型コロナウイルス感染症拡大防止の観点から、実施を見送ることとした。

次年度以降、協力専門学校等の授業への活用を通して、内容の検証、精査等を行う予定である。

３．次年度以降の取組み

１．今後の展開

●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、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。

●本会の行う教職員研修を企画し、教員の育成を行い、成果物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。

２．事業期間終了後の活動

●成果物のダウンロードが可能なように、Web サイトへ掲載し活用を促進する。

●次年度以降、正規課程への導入や、成果を活用している協力校、他の専門学校と連携して、教育プログラムの検証、精査を行うとともに、情報・技術など内容の更新を継続する。

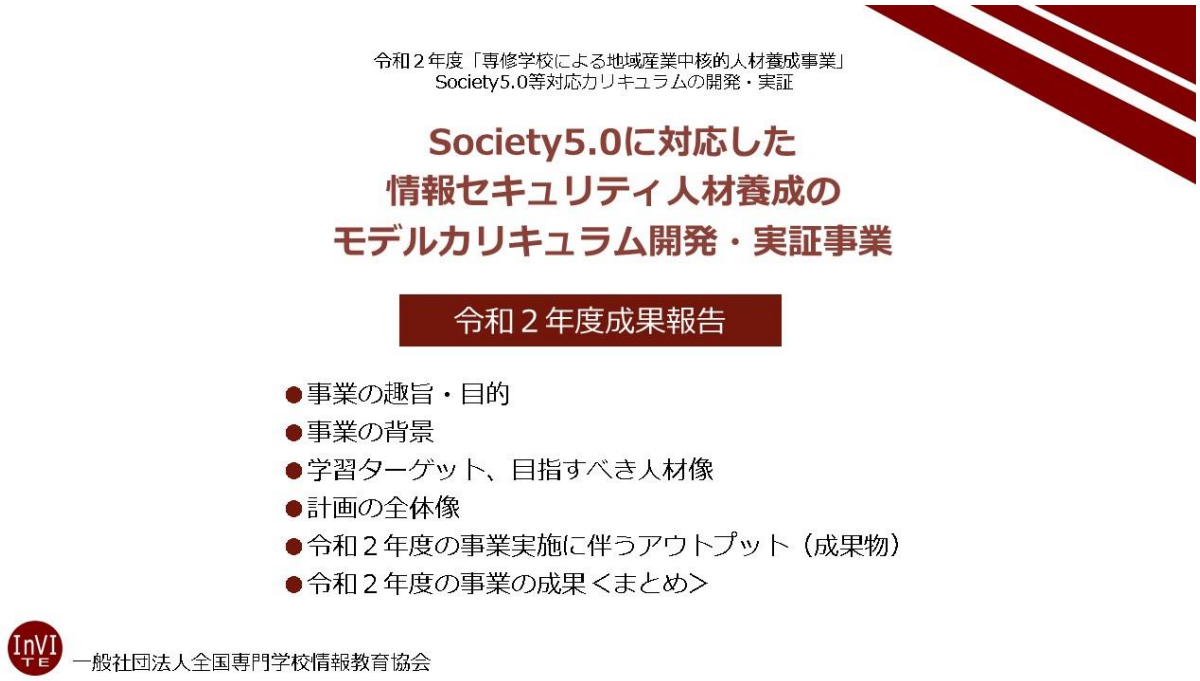
３．事業成果普及と事業継続

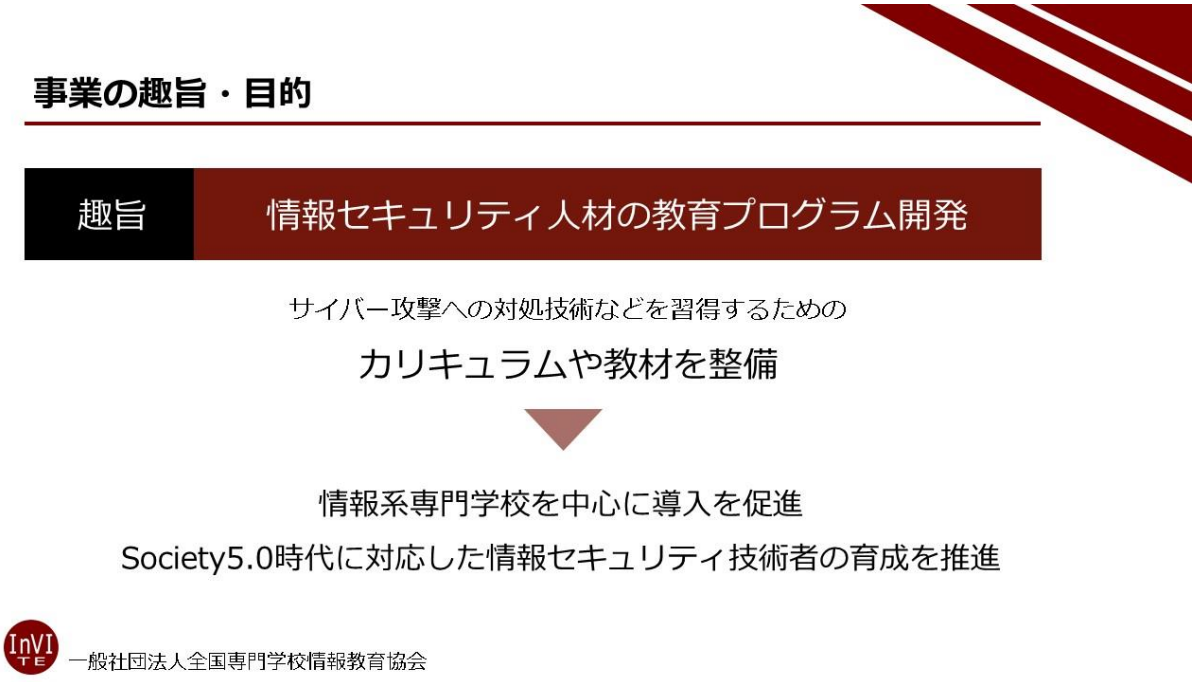
●情報セキュリティを取り巻く環境は、今後も大きく変化することが予測されるため、事業終了後も情報収集や教育プログラムの更新を行い、常に最新の状態で教育が実施できる継続的な体制を構築する。

●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。

資料

成果報告動画のスライド





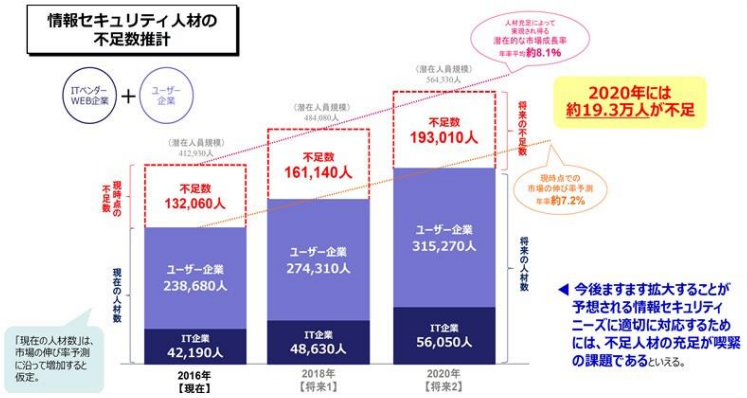
事業の背景

IoTの進展などにより
ネットワークに
接続される機器が増加

▼

情報セキュリティの
リスクも増加

課題
対応する情報セキュリティ人材が不足

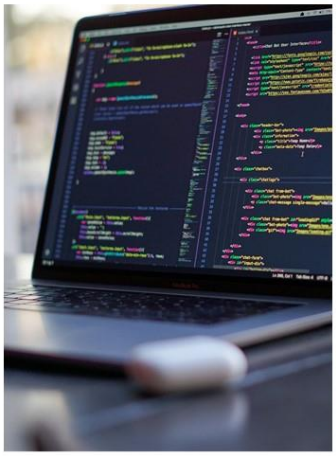


一般社団法人全国専門学校情報教育協会

学習ターゲット、目指すべき人材像

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、
情報セキュリティを担保できるIT技術者
の育成を目指す



一般社団法人全国専門学校情報教育協会

計画の全体像

平成30年度

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	

令和元年度

開発	カリキュラム・シラバス	・サイバー攻撃手法・対策 ・情報システム開発技術者のセキュリティ知識
	教育教材	・セキュアなネットワーク設計の見直し ・サイバー攻撃手法・対策教材 ・情報システム開発者に必要な情報セキュリティ
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	

令和２年度　今年度実施

開発	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）
	教員教材	・映像教材（サイバー攻撃手法・対策）と指導書 ・評価手法
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運用講座 ・教員研修会	

令和２年度の事業実施に伴うアウトプット（成果物）

①教育カリキュラム・シラバス

・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 900時間

②教育教材

・セキュアなシステム運用教材　テキスト

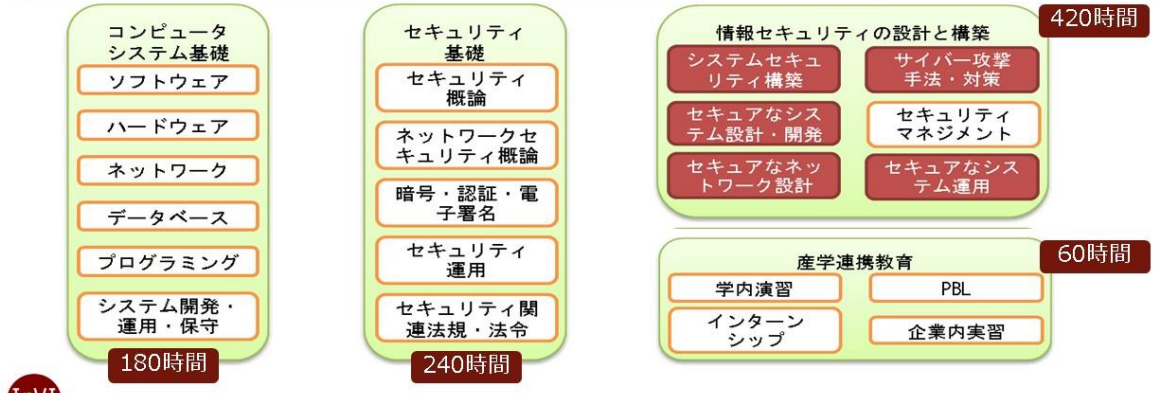
③映像教材

・映像教材と演習手順書
当初教員用の映像教材作成を予定していたが、委員会での検討の結果、
遠隔教育にも活用できる学生を対象とした映像教材の作成を優先して実施した

令和２年度の事業実施に伴うアウトプット（成果物）

①教育カリキュラム・シラバス

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



一般社団法人全国専門学校情報教育協会

令和２年度の事業実施に伴うアウトプット（成果物）

②教育教材

セキュアなシステム運用教材　テキスト

情報セキュリティを確保して、システム運用を行うための技術と知識の教材

③映像教材

サイバー攻撃・対策の映像教材

遠隔教育にも活用できる「サイバー攻撃手法・対策」の映像教材

演習手順書

「サイバー攻撃手法・対策」映像教材の演習を進めるための解説書

一般社団法人全国専門学校情報教育協会

令和２年度の事業の成果＜まとめ＞

教育カリキュラム、教材を整備 → 期待される人材の育成が可能に

＜成果の活用＞

- 本事業に参加する専門学校・企業に、開発したカリキュラム・プログラムの導入を促進
- 本会会員校及び全国の情報系専門学校に教育カリキュラム・教材の活用および学科の設置を促進
- 情報産業の業界団体を通して、成果物の企業研修等への利用を促進
- 遠隔教育実施のためのコンテンツ・教育手法・効果測定に関する研究とプログラム整備に活用

▶ 専門学校等への導入により人材不足の解消に貢献

一般社団法人全国専門学校情報教育協会

演習環境の下準備

新規に演習環境を作成する手順を以下に示します。作成する仮想マシンは以下の通りです。

仮想マシン	WindowsServer	MutillidaeII	Kali-Linux
OS	Windows Server 2008 R2 試用版	Linux (CentOS 8)	Linux (Debian ベース)
ホスト名	victim08	mutillidae	kali
IP アドレス	192.168.33.8/24	192.168.33.10/24	192.168.33.13/24
役割	脆弱性チェックやツールの練習	脆弱 Web アプリとツールの練習	ペネトレーションテスト集
アカウント	Administrator	admin	kali
パスワード	P@ssw0rd	admin	kali

本セットアップ手順は、Linux や Windows の操作がある程度できる方を対象にして作成してあります。不明点があれば、自力解決してセットアップを行ってください。

準備1. VirtualBox のインストール

作業1. Virtual Box インストール

__1. VirtualBox の platform packages と Extension Pack の最新版をダウンロードします。
https://www.virtualbox.org/wiki/Downloads
例：
platform packages: VirtualBox-6.1.12-139181-Win.exe
Extension Pack: Oracle_VM_VirtualBox_Extension_Pack-6.1.12.vbox-extpack

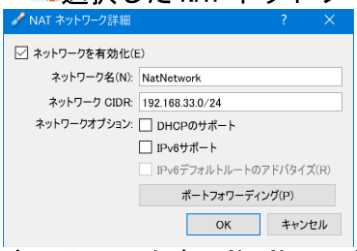
__2. Oracle VirtualBox を、標準設定のままインストールします。

__3. VirtualBox を起動し、以下の手順で、拡張機能(Extension Pack)をインストールします。
ファイル > 環境設定 > 機能拡張, 新しいパッケージを追加
ダウンロードした Extension Pack 最新版を指定。

__4. 必要ならば再起動します。

作業2. 仮想ネットワーク構築

__1. 以下の手順で NatNetwork を編集または作成します。この仮想ネットワークはセットアップ時に使用します。
・ファイル > 環境設定 > ネットワーク
・新しい NAT ネットワークを追加します。
・選択した NAT ネットワークを編集します。



ネットワーク名: NatNetwork
ネットワーク CIDR: 192.168.33.0/24
ネットワークオプション: ☐ DHCP のサポート

__2. 以下の手順で Host-Only Ethernet Adapter を編集または作成します。この仮想ネットワークは演習時に使用します。

・ファイル > ホストネットワークマネージャー, プロパティ （または作成）
・アダプター > ◉アダプターを手動で設定
IPv4 アドレス: 192.168.33.20
IPv4 ネットマスク: 255.255.255.0
・DHCP サーバー > □サーバーを有効化 ←チェックを外す
・[適用]

__3. デフォルトの仮想マシンフォルダーを指定しておきます。

・ファイル > 環境設定 > 一般
・デフォルトの仮想マシンフォルダー: 任意（例: D:¥VirtualBox VMs）

準備2. Kali Linux のセットアップ

作業1. OVA ファイルのインポート

__1. セットアップキットから、以下の手順で Kali-Linux.ova をインポートします。

・ファイル > 仮想アプライアンスのインポート, （前手順の OVA ファイル）
・仮想アプライアンスの設定（下記以外は既定値を使用）

準備3. Mutillidae II のセットアップ

作業1. OVA ファイルのインポート

__1. セットアップキットから、以下の手順で MutillidaeII.ova をインポートします。

・ファイル > 仮想アプライアンスのインポート, （前手順の OVA ファイル）
・仮想アプライアンスの設定（下記以外は既定値を使用）

準備4. Windows Server 2008 R2 評価版のセットアップ

脆弱性を評価する犠牲マシンとして用意するので、あえて旧バージョンの Windows を使用します。ライセンスがあれば、製品版の Windows Server 2008 R2 でもセットアップは同様です。

作業1. （OVA ファイルを使う場合）OVA ファイルのインポート

サンプルとして、セットアップ済みの OVA ファイル WindowsServer.ova が用意されていますが、配布時には有効期限が切れています。ライセンス関係が不明瞭な場合、こちらの OVA ファイルは使わないでください。OVA ファイルを使用する場合、slmgr /rearm で有効期限をリセットしてから使用してください。

__1. セットアップキットから、以下の手順で WindowsServer.ova をインポートします。

・ファイル > 仮想アプライアンスのインポート，（前手順の OVA ファイル）
・仮想アプライアンスの設定（下記以外は既定値を使用）

__2. インポートが終われば事前準備は終了です。

作業2. （OVA ファイルを使わない場合）Windows Server 2008 R2 評価版のセットアップ

__1. 以下のリンクをたどり、Windows Server 2008 R2 評価版の ISO ファイルを入手します。
https://www.microsoft.com/ja-JP/download/details.aspx?id=11093

__2. 以下の手順で新規仮想マシンを作成します。

・仮想マシン > 新規
・名前とオペレーティングシステム
名前: WindowsServer
マシンフォルダー: （既定値）
タイプ: Microsoft Windows
バージョン: Windows 2008 (64-bit)
・メモリーサイズ
（既定値）
・ハードディスク
（既定値）
・ハードディスクのファイルタイプ
（既定値）
・物理ハードディスクにあるストレージ
（既定値）
・ファイルの場所とサイズ
（既定値）

__3. 仮想マシン WindowsServer の設定(S)で、以下を設定します。

・設定 > 一般 > 高度，クリップボードの共有: 双方向
・設定 > ストレージ，コントローラー: SATA - 空，
光学ドライブ: > 仮想光学ディスクの選択/作成
ダウンロードした ISO ファイルを選択
・設定 > ネットワーク
☑ネットワークアダプターを有効化
割り当て: NAT ネットワーク

名前: NatNetwork

__4. WindowsServer を起動し、Windows Server 2008 R2 評価版をセットアップします。
既定値以外の設定は以下の通り。

・起動ハードディスクを選択:（ダウンロードした ISO ファイル）
・インストールの種類: 新規インストール（カスタム）
・パスワード: P@sswOrd

作業3. VirtualBox Guest Additions の導入

__1. Guest Additions CD イメージの挿入を実施します。

・Oracle VM VirtualBox > デバイス > Guest Additions CD イメージの挿入

__2. Guest Additions を導入します。

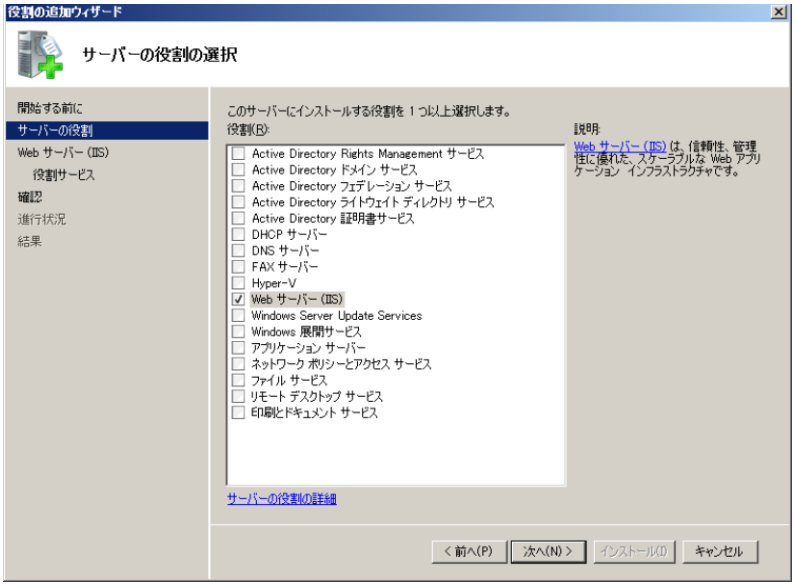
・D:¥VBoxWindowsAdditions.exe を実行。既定値のままでインストール。
・再起動

作業4. 初期設定

__1. 仮想マシン WindowsServer に Administrator でログオン後、以下の手順で初期構成タスクを実施します。

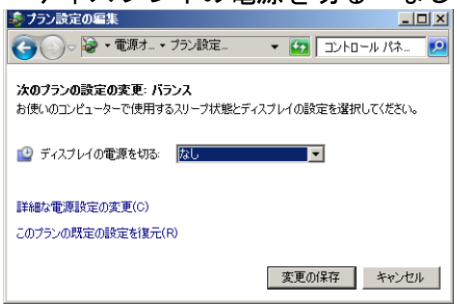
・ネットワークの構成, ローカル エリア接続, プロパティ,
インターネット プロトコル バージョン 4
IP アドレス: 192.168.33.8
サブネットマスク: 255.255.255.0
デフォルト ゲートウェイ: 192.168.33.1
優先 DNS サーバー: 1.1.1.1
代替 DNS サーバー: 8.8.8.8
・Windows ファイアウォールの構成,
Windows ファイアウォールの有効化または無効化
ホームまたは社内（プライベート)ネットワーク: 無効にする
パブリック ネットワーク: 無効にする
・リモート デスクトップを有効にする
◉リモートデスクトップを実行しているコンピューターからの
接続を許可する。
・自動更新とフィードバックを有効にする > 手動で設定を構成する
Windows 自動更新 > 更新プログラムを確認しない
Windows エラー報告 >
レポートを送信せず、この確認画面も今後表示しません
・コンピュータ名とドメインの入力 > 変更
コンピューター名: victim08
・今すぐ再起動する

__2. 初期構成タスクの役割の追加で、演習用に Web サーバーを追加します。



__3. 電源オプションで、ディスプレイの電源を切らないようにします。

・コントロールパネル > ハードウェア > 電源オプション > プラン設定の編集
・ディスプレイの電源を切る: なし



__4. パスワード複雑さを無効化します。

・ gpedit.msc 実行
・ コンピュータの構成 >Windows の設定 > セキュリティの設定 > アカウントポリシー > パスワードのポリシー
・ 複雑さの要件を満たす必要があるパスワード : 無効
・ 全ウィンドウを閉じる。

__5. 以下のアカウントを作成します。

アカウント名　　victim1
パスワード　　ryougoku　　←間違えて ryogoku にしないように

```
net user /add victim1 ryougoku
```

__6. その他の設定を変更します（初期構成タスクが開いていない場合、[Windows]キー + [R], oobe で実行)。

・初期構成タスク > ☑ログオン時にこのウィンドウを表示しない > 閉じる
・VirtualBox > デバイス > 光学ドライブ > 仮想ドライブからディスクを除去
・エクスプローラー > Alt + T, O > 表示タブ >
☐登録されている拡張子は表示しない

作業5. Chrome 導入

__1. 以下の手順で Internet Explorer の 「IE セキュリティ強化の構成」を解除します。
サーバーマネージャー > セキュリティ情報 > IE ESC の構成, 全てオフ

__2. Internet Explorer を起動し、以下の URL を開きます。
https://www.google.com/chrome/

__3. Chrome をダウンロードし、インストーラーを実行します。

__4. インストール後に Chrome が開いたら、そのまま閉じます。

作業6. サクラエディタ導入

__1. 以下の 2 ファイルをダウンロードし、C:¥Lab フォルダー（作成）に移動します。
7z1900-x64.exe（64 ビット x64）
https://sevenzip.osdn.jp/
sakura-tag-v2.4.1-build2849-ee8234f-Win32-Release-Installer.zip
https://github.com/sakura-editor/sakura/releases

__2. 以下のファイル(7-Zip インストーラ)を実行し、既定値でインストールします。
7z1900-x64.exe

__3. 以下のファイルを 7-Zip で展開します。
sakura-tag-v2.4.1-build2849-ee8234f-Win32-Release-Installer.zip
右クリック > 7-Zip > ここに展開

__4. 生成された以下のインストーラを実行します。
sakura_install2-4-1-2849-x86.exe
・追加タスクの選択
☑「SAKURA Editor で開く」メニューの追加 ←ここだけ変更

__5. サクラエディタへのパスを指定します。
・[Windows]キー + [Pause] （または[Windows]キー + [R],sysdm.cpl 実行）
・システムの詳細設定 > 詳細設定 > 環境変数
・ユーザー環境変数 > 新規
変数名: PATH
変数値: C:¥Program Files (x86)¥sakura

作業7. Wireshark 導入

__1. 以下の URL からインストーラーをダウンロードします。
https://www.wireshark.org/download.html
Windows Installer (64-bit)
ダウンロード先: C:¥Lab

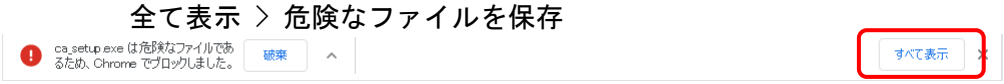
__2. インストーラーを実行します。
Npcap 1.00 Setup - Installation Options
☑Install Npcap in WinPcap API-compatible Mode ← チェックする

作業8. Cain & Abel 導入

__1. WindowsServer で Chrome を使って以下のファイルをダウンロードし、C:¥Lab フォルダーにコピーします。

ca_setup.exe

※ ダウンロードはブロックされるので、以下の手順で回避します。
全て表示 > 危険なファイルを保存



本家アーカイブ：
https://web.archive.org/web/20190603235413/http://www.oxid.it/downloads/ca_setup.exe

参考：
https://web.archive.org/web/20190603235413if_/http://www.oxid.it/cain.html

__2. インストーラーが改ざんされていないことを確認します。

```
certutil -hashfile ca_setup.exe MD5
certutil -hashfile ca_setup.exe SHA1
```

ハッシュ値：
MD5 - EA2EF30C99ECECB1EDA9AA128631FF31
SHA1 - 82407EAF6437D6956F63E85B28C0EC6CA58D298A

__3. ca_setup.exe を実行し、Cain & Abel をインストールします。

WinPcap は Wireshark でインストール済みなので、
ここでは[Don't Install]を選択

__4. 以下の URL から日本版ワードリストを取得します。

lower.gz
https://download.openwall.net/pub/wordlists/languages/Japanese/

__5. ファイルを 7-zip で解凍し、生成した lower.lst ファイルを以下にコピーし、ファイル名を変更します。

C:¥Lab¥lower.txt

__6. Cain を実行し、以下の手順でパスワードクラックの動作確認をします。

Cracker タブ > LM & NTLM Hashes > [+]ツールボタン , Next
victim1 右クリック > Dictionary Attack > NTML Hashes
Dicrionary 欄 右クリック > Add to List > C:¥Lab¥lower.txt, Start

__7. 動作確認後、以下の手順で設定をリセットします。

Dictionary 欄 右クリック > Reset initial file position

Dictionary 欄 右クリック > Remove All , Exit
victim1 右クリック > Remove All
Cain 終了

作業9. 仮想マシン WindowsServer への Snort 導入

__1. 以下の 3 ファイルをダウンロードし、C:¥Lab フォルダにコピーします。

Microsoft Visual C++ 2008 再頒布可能パッケージ (x64)
vcredist_x64.exe
https://www.microsoft.com/ja-jp/download/details.aspx?id=15336
Snort_2_9_16_1_Installer.x64.exe https://www.snort.org/downloads
snortrules-snapshot-29161.tar.gz https://www.snort.org/downloads
※ snortrules のダウンロードには Sign In が必要。ダウンロード後に logout を忘れずに。以下を確認。
Google Chrome の設定 >
自動入力 > パスワード
プライバシーとセキュリティ > 閲覧履歴データの削除

※Wireshark 導入時に下記ファイルはインストール済みだが、必要に応じてダウンロード。
Visual Studio 2015 の Visual C++ 再頒布可能パッケージ
vc_redist.x64.exe
https://www.microsoft.com/ja-jp/download/details.aspx?id=48145
Npcap 0.9997 installer
npcap-0.9997.exe https://nmap.org/npcap/

__2. 以下の 2 ファイルを実行し、既定値のままインストールします。

vcredist_x64.exe
Snort_2_9_16_1_Installer.x64.exe

※以下は Wireshark と同時に導入済み。必要に応じてインストール。
npcap-0.9997.exe
vc_redist.x64.exe

__3. 以下のファイルを展開。出来上がった tar ファイルをさらに展開します。

snortrules-snapshot-29161.tar.gz
右クリック, 7-Zip > ここに展開

snortrules-snapshot-29161.tar
右クリック, 7-Zip > ここに展開

__4. 出来上がった以下の 2 つのフォルダーを、C:¥Snort に上書きコピー (統合、置換) します。

preproc_rules
rules
※残り 2 つはコピーしない (etc, so_rules はコピーしない)

__5. コマンドプロンプトから、Snort 導入確認をします。

```
cd ¥Snort¥bin
snort -V
```

実行結果の例

```
  ,,_      -*> Snort! <*-
 o"  )~    Version 2.9.16.1-WIN64 GRE (Build 140)
  ''''     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11
```

作業10. Snort 設定と動作確認

__1. サクラエディタで C:¥Snort¥etc¥snort.conf を開き、修正します。

```
cd ¥Snort¥etc
sakura snort.conf
```

[C:¥Snort¥etc¥snort.conf]
※行番号は参考です。セットアップの時期によって設定ファイルの内容が変わり、行番号が前後することがあります。

```
...
 45 ipvar HOME_NET 192.168.33.0/24
...
104 var RULE_PATH c:¥snort¥rules
105 var SO_RULE_PATH c:¥snort¥so_rules
106 var PREPROC_RULE_PATH c:¥snort¥preproc_rules
...
113 var WHITE_LIST_PATH c:¥snort¥rules
114 var BLACK_LIST_PATH c:¥snort¥rules
...
247 dynamicpreprocessor directory c:¥snort¥lib¥snort_dynamicpreprocessor
...
250 dynamicengine c:¥snort¥lib¥snort_dynamicengine¥sf_engine.dll
...
253 # dynamicdetection directory /usr/local/lib/snort_dynamicrules
...
265 # preprocessor normalize_ip4
266 # preprocessor normalize_tcp: ips ecn stream
267 # preprocessor normalize_icmp4
268 # preprocessor normalize_ip6
269 # preprocessor normalize_icmp6
...
525 output log_unified2: filename ../../../snort/log/snort.log, limit 128, nostamp
...                                  ↑
        先頭に強制的に log/が付加されるので、UNIX 風の相対パス指定が必要
```

__2. ダミーファイルを３つ作成します。

```
cd ¥Snort
copy nul rules¥white_list.rules
copy nul rules¥black_list.rules
copy nul log¥snort.log
```

__3. 動作確認用のルールを作成します。

```
cd ¥Snort¥rules
sakura local.rules
```

[C:¥Snort¥rules¥local.rules]

```
...
 22 alert icmp any any -> any any (msg:"ICMP Testing Rule"; sid:1000001; rev:1;)
```

__1. 動作確認のため、仮想マシン WindowsServer の設定で以下を設定します。

・設定 > ネットワーク
☑ネットワークアダプターを有効化
割り当て: ホストオンリーアダプター
名前: VirtualBox Host-Only Ethernet Adapter

__2. 監視対象のネットワークインターフェースを確認します。

¥Device¥NPF_... の存在する Index 番号を控える。

```
cd ¥Snort¥bin
snort -W
...
Index   Physical Address    IP Address    Device Name     Description
-----   ----------------    ----------    -----------     -----------
    1   00:00:00:00:00:00   disabled      ¥Device¥NPF_NdisWanIp   NdisWan Adapter
    2   00:00:00:00:00:00   disabled      ¥Device¥NPF_NdisWanBh   NdisWan Adapter
    3   00:00:00:00:00:00   disabled      ¥Device¥NPF_NdisWanIpv6 NdisWan Adapter
    4   08:00:27:D9:F5:49   0000:0000:fe80:0000:0000:0000:f52c:9c64 ¥Device¥NPF_{FDA2692A-6A7A-4
BCA-A09F-FFC15AFB01C7}  Intel(R) PRO/1000 MT Desktop Adapter
    5   00:00:00:00:00:00   disabled      ¥Device¥NPF_Loopback    Adapter for loopback traffic
 capture
```

上記の例では Index 番号は 4 となる。

__3. コマンドプロンプトから Snort を起動します。

-i オプションで指定する数字は、上記で控えた Index 番号（例: 4）

```
snort -i 4 -c c:¥Snort¥etc¥snort.conf -A console -E
...
Commencing packet processing (pid=****)    ←これが出れば起動している。
```

WARNING が大量に出るが、起動さえすれば無視してかまわない。

__4. 仮想マシン Kali-Linux から ping を打ち、ping が検出されるか確認します。

Kali-Linux のターミナルから：

```
ping 192.168.33.8
```

WindowsServer のコマンドプロンプト上

```
**/27-**:36:02.769733  [**] [1:1000001:1] ICMP Testing Rule [**] [Priority: 0]
{ICMP} 192.168.33.13 -> 192.168.33.8
```

__5. Ctrl + C で Snort を終了します。

__6. イベントビューアにログが取られているか確認します。

[Windows] + R, eventvwr
カスタム ビュー > 管理イベント

__7. コマンドプロンプト、イベントビューア、その他開いているウィンドウを閉じます。

作業11. 仮想マシン WindowsServer へのルート証明書インポート

__1. 仮想マシン Mutillidaell が起動していない場合は起動します（ログイン不要）。

__2. 仮想マシン WindowsServer の  で、以下が設定されていることを確認します。

・設定 > ネットワーク
☑ネットワークアダプターを有効化
割り当て: ホストオンリーアダプター
名前: VirtualBox Host-Only Ethernet Adapter

__3. ログオンしていない場合は仮想マシン WindowsServer に Administrator でログオンします。

__4. ブラウザで以下の URL を開き、localCA.pem をダウンロードフォルダにダウンロードします。
http://192.168.33.10/

__5. ブラウザ右上の「Google Chrome の設定」から、以下を開きます。
設定 > プライバシーとセキュリティ > セキュリティ > 証明書の管理 > 信頼されたルート証明機関，インポート

__6. ダウンロードフォルダの「全てのファイル(*.*)」から localCA.pem を開き、ルート証明書をインポートします。

__7. 動作確認で以下の URL を開き、エラーが無いことを確認します。
https://192.168.33.10/ **←スキーマを https にして確認**

作業12. セットダウン

__1. ダウンロードフォルダの全ファイルを C:¥Lab に移動します。

__2. ゴミ箱を空にします。

__3. C:¥Lab フォルダの以下のファイルとフォルダを削除します。
lower.gz
sakura-tag-v2.4.1-build2849-ee8234f-Win32-Release-Installer.zip
snortrules-snapshot-29161.tar
warning.txt
etc¥
so_rules¥

令和２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３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