CCDS
～攻撃者視点IoTハッキングコースのご紹介～

一般社団法人 重要生活機器連携セキュリティ協議会
株式会社マストトップ

１．攻撃者視点IoTハッキングコース実施概要

攻撃者視点IoTハッキングコース概要

　これまでに実施した「CCDS指定検査資格講習」のプログラムメニューを見直し、名称を「攻撃者視点IoTハッキングコース」へと変更致しました。IoT機器に対するハッキング技術を基礎から学ぶことが可能なプログラムとなっております。

また従来の「CCDS指定検査資格講習」の内容も、本プログラムには含まれておりますので、本コースを修了することで、従来通りCCDS指定資格試験の受験資格も得られます。

1）各講習プログラムは講義＋実習をセットとした演習形式で構成しており、受講後も継続的に実践可能なプログラム内容となっております。
2）製品・サービスの脅威分析や、対策立案、リスク評価等が包括的に含まれるプログラムであり、CCDSのマーク取得に留まらず、対策すべきセキュリティ課題を総合的に検討することが可能です。
3）オープンソースのセキュリティ検証ツールを使用し、ハッキングの実施手順や結果の分析方法など、基礎的な内容を理解することが可能です。
4）Wi-Fi無線ルータや疑似スマートホーム環境を使用し、非常にリアルな環境でハッキングの実践を行うことが可能です。
5）講義、実習のいずれもオンライン環境を利用し、リモートでの受講や、受講後の復習が可能です。

実施要項

・募集期間：別紙、募集要項参照

・講習開催予定：別紙、募集要項参照

・講習プログラム
　－90分×１２コマの講習プログラムを実施（詳細後述）

・開催場所：
　－オンライン受講（詳細は別途ご案内致します）

・募集人数：１０名（上限）、最小開催人数：６名

・受講費用：
①CCDS幹事・正会員 割引価格
　・幹事会員：20万円／1名
　・正会員　：25万円／1名
　・一般会員：30万円／1名（検査資格登録不可）
②2名セット割引価格
　・幹事会員：35万円／2名
　・正会員　：45万円／2名

プログラム概要

・脅威分析＞基礎＞実践と、段階を追って修得していくプログラム構成。
・ツールや実機を使った実習と、講義がワンセットとなった実践的な演習スタイル

1日目　脅威分析コース：90分×４講座

・脅威分析や対策立案、リスク分析の実践：講義＋実習
・セキュリティ検証環境の環境構築：講義

2日目　ハッキング基礎コース：90分×４講座

・セキュリティ検証環境の環境構築：講義
・セキュリティ検証ツールのオペレーション演習：講義＋実習
・セキュリティ検査のポイント：講義

3日目　ハッキング実践コース：90分×４講座

・疑似スマートホーム環境に対する演習（１）～（４）：実習

今後の講習実施スケジュール

・今後の講習計画は以下を予定。
※開催最小人数に応募が満たない場合、次回の開催予定に
　繰り越して実施する。
※各コースはセットでの受講が前提であり、個別受講は不可。

■2022年の講習実施スケジュール

実施計画	講習実施日	募集上限	開催最小人数
2022年7月	・脅威分析コース：7/8(金)※ ・ハッキング基礎コース：7/15(金) ※ ・ハッキング実践コース：7/22(金) ※	１０名	６名
2022年11月	・脅威分析コース：11/4(金) ※ ・ハッキング基礎コース：11/11(金) ※ ・ハッキング実践コース：11/25(金) ※	１０名	６名

※11月の日程については当会イベントの状況に応じて変更の可能性がございます。

プログラムメニュー①

：１日目　：2日目　：３日目

No.	講習テーマ	形式	時間
P1	**【ステップ1】IoT機器に対する脅威分析の実践** ～脅威の抽出やCCDS-STRDEモデルによる分類方法の理解	講義・実習	90分
P2	**【ステップ1】想定脅威に対するセキュリティ対策の立案** ～セキュリティ対策の概要と対策フレームワークの活用	講義・実習	90分
P3	**【ステップ２】リスク値の算定とリスク対応の原則** ～CVSSを用いたリスク値の算定とリスク対応方針の検討	講義・実習	90分
P4	**【ステップ３】検査環境の構築** ～Linux環境によるセキュリティ検査ツールの環境構築方法	講義	90分
P5	**【ステップ３】OSS検証ツールのオペレーション手順と結果分析①** **～**OSS検証ツール４種を対象に、使用手順や解析手法の理解	講義	90分
P6	**【ステップ３】OSS検証ツールのオペレーション手順と結果分析②** **～**OSS検証ツール４種を対象に、使用手順や解析手法の理解	講義・実習	90分
P7	**【ステップ３】OSS検証ツールのオペレーション手順と結果分析③** **～**OSS検証ツール４種を対象に、使用手順や解析手法の理解	講義・実習	90分
P8	**【特別講習】セキュリティ検査の実施におけるポイント** ～CCDSサーティフィケーションプログラムの概要 ～CCDSが定義するIoT機器セキュリティ要件と国内外セキュリティ基準の対応	講義	90分

プログラムメニュー②

No.	講習テーマ	形式	時間
P9	**【ハッキング演習】** **疑似スマートホーム環境に対する演習と実践（1）** ～侵入・攻撃経路のプラン策定	講義・実習	90分
P10	**【ハッキング演習】** **疑似スマートホーム環境に対する演習と実践（2）** ～CTFによるハッキングトレーニング①	講義・実習	90分
P11	**【ハッキング演習】** **疑似スマートホーム環境に対する演習と実践（3）** ～CTFによるハッキングトレーニング②	講義・実習	90分
P12	**【ハッキング演習】** **疑似スマートホーム環境に対する演習と実践（4）** ～CTFによるハッキングトレーニング③ ～ハッキングトレーニングの総括	講義・実習	90分

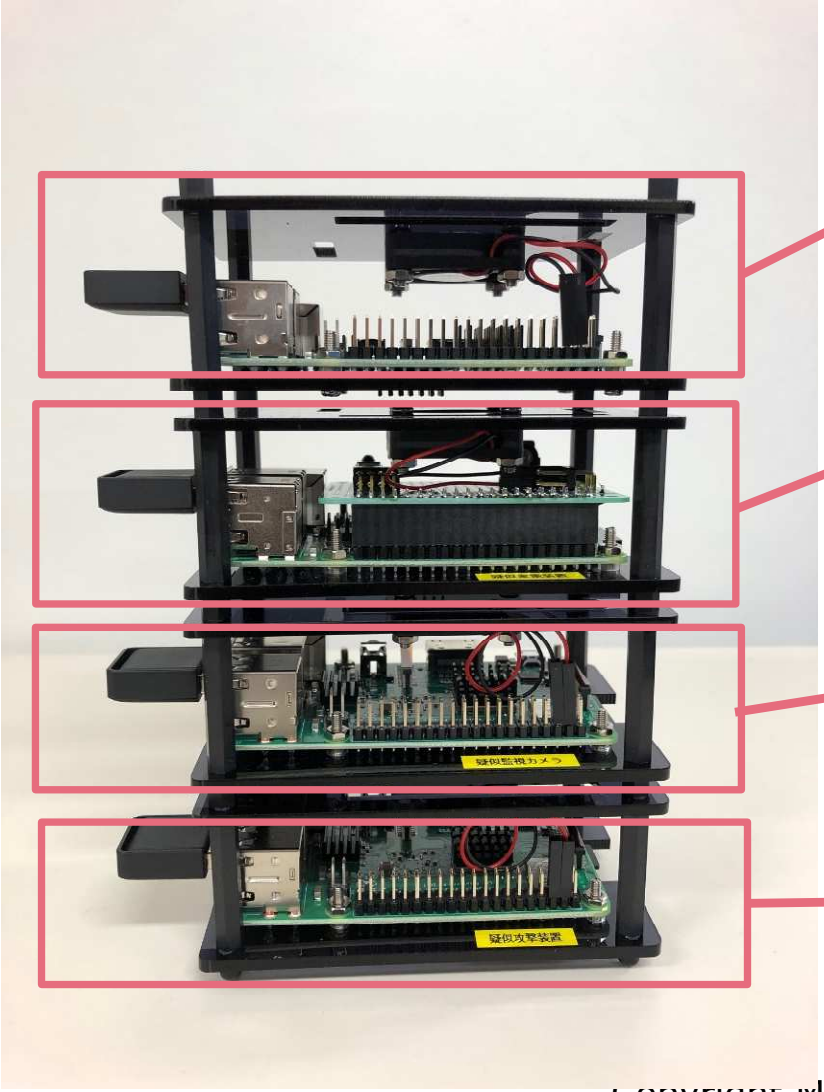
プログラムメニュー③

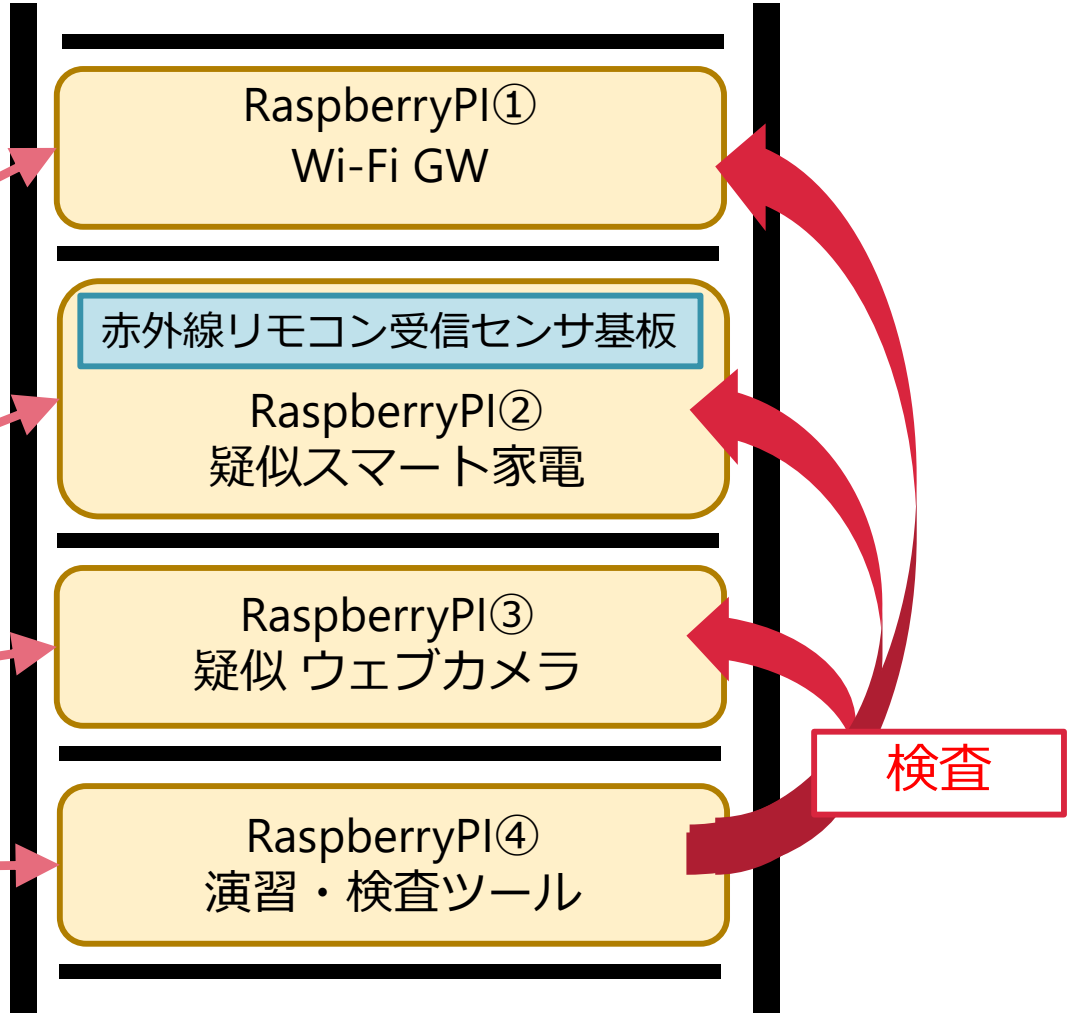
- 下記のプログラムメニューについては、オンラインによる自習形式にて受講可能となります。

No.	講習テーマ	形式	時間
SP1	**共通要件の内容説明と検査手法の解説と実践** ～共通要件11項目の内容と、検査手法や合格基準の理解	オンライン 講義（自習）	–
SP2	**リモート演習環境によるP5～P7、P9～P12の実習の復習** ～講習日から１ヵ月間は、リモート環境を使用したツールのオペレーションや、ハッキング演習の復習が可能（予約制）	オンライン 実習（自習）	–

演習環境のご紹介

・演習/検査ツールと、検査対象となる疑似IoT機器を
RaspberryPIにより、一体化した構成。
・各受講者にリモート環境を開放し、ツールを使った実習が可能。





2．CCDS指定検査資格試験　実施概要

CCDSが提供する講習の役割

CCDSサーティフィケーションプログラム

メーカによる自主検査

専門業者による第三者検査

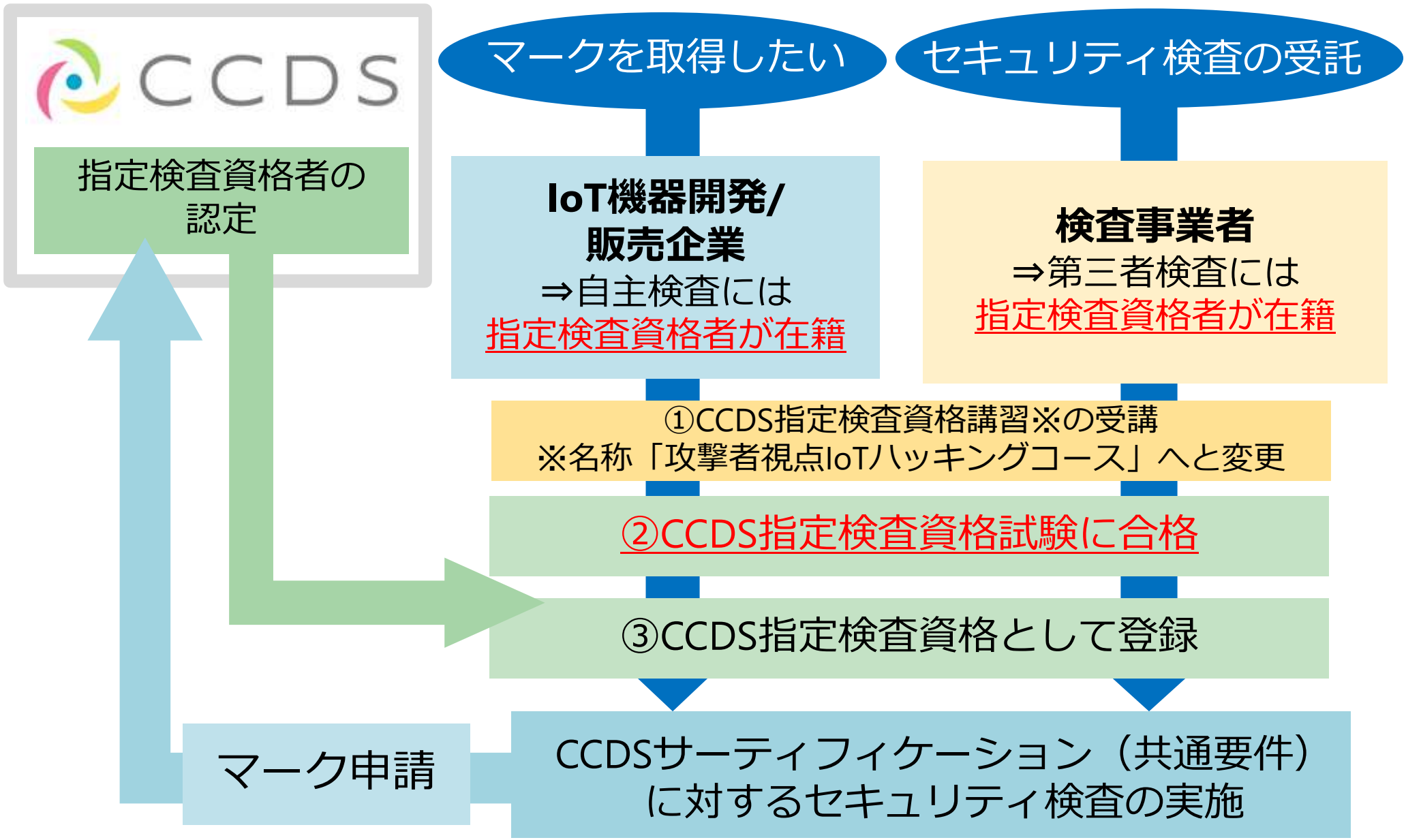
セキュリティ要件に対する適合検査が必要

■課題
・IoTセキュリティ人材の不足
・適合検査基準・手順の共通認識

CCDS人材育成プログラム
～攻撃者視点IoTハッキングコース～

CCDSとして、検査基準の共有とスキル修得を支援

資格取得とマーク申請までのフロー



IoTハッキングコースの位置づけ

・攻撃者視点IoTハッキングコースは、CCDSの認定を受けたセキュリティ人材育成プログラムであり、CCDSサーティフィケーションマークの取得申請に必要な検査手順・手法の知見や技術についても習得できる内容です。
・検査資格に有効期限はありませんが、毎年のサーティフィケーションのセキュリティ要件の改定に伴い、別途追加講習の受講による更新が必要となります。

①攻撃者視点IoTハッキングコース
（効果測定で全教科70点以上の取得）

⇒検証に必要な知識の習得と確認
自動車免許で言えば…　学科試験

②CCDS指定検査資格試験

⇒実際に検査を実行することができるか
自動車免許で言えば…　路上試験

両方揃ってはじめて資格登録となります

試験の目的

- CCDSサーティフィケーションプログラムにおける、IoT機器共通のセキュリティの11要件（以降、CCDS11要件）を検証できるスキルを持ち合わせているかどうかを確認する

- 試験方針
  - CCDS11要件を理解していること
  - CCDS11要件をチェックする手段を理解していること
  - 実際に脆弱性検証ツールの操作ができること（nmap, aircrack-ng, THC-Hydra, OpenVAS, Wireshark等）
  - 脆弱性検証手法を理解していること（脅威分析、検証内容策定、検証の実施、報告書作成）

受験申請から検査資格登録までの流れ

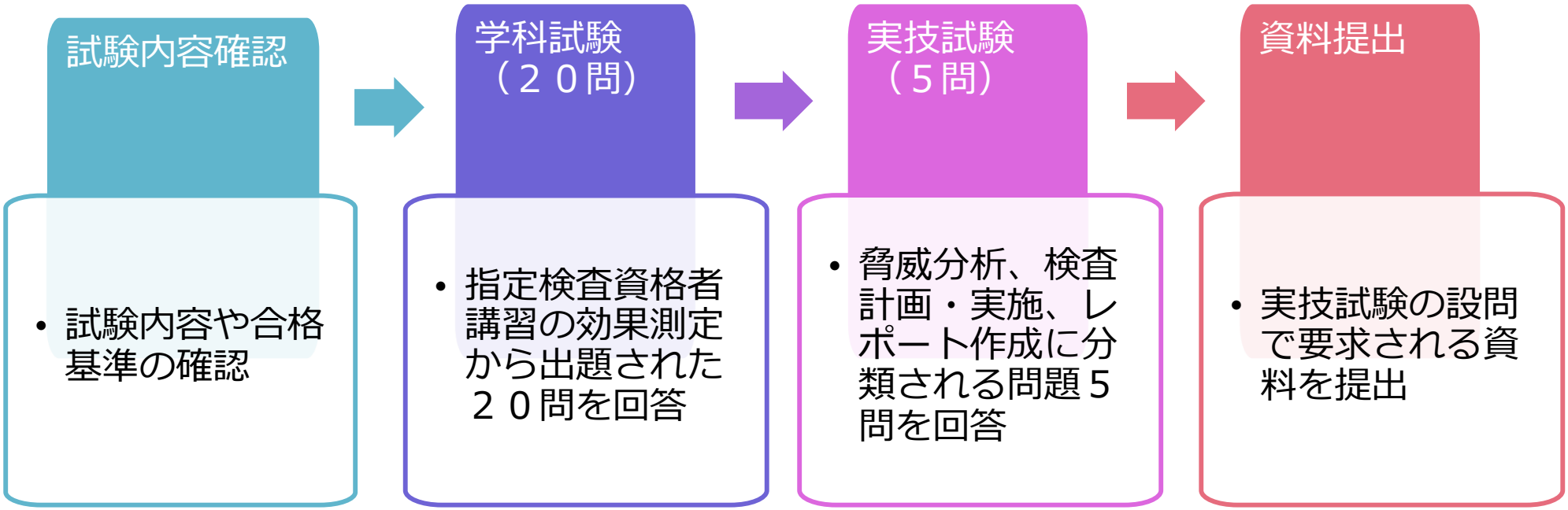
資格講習の受講	受験の申請	試験の受験	合否発表・登録
• 資格講習の受講が当試験受験の要件です	• 受験申請シートに記入の上、CCDS事務局までお申し込みください	• CCDS目黒事務所にて試験を受験します	• 合否は2週間以内を目処に受験者へ通知します • 合格者には、登録番号を発行し、登録証を作成・発送します

実施日程・受験手数料・申し込み方法等

- 実施日程：順次開催中（事前予約性）
  ※CCDSから対応可能なスケジュールを告知しますので、受験者の方がご希望の日程を選択いただける形となります。
- 試験時間：時間制限240分　※完了した時点で退席可能です
- 受験手数料：1回 5,000円
- 試験会場：CCDS東京事務所
  (東京都品川区上大崎2-12-1 野田ビル3F)
- 申し込み方法：CCDS会員向けに別途アナウンスします

★詳細については後日アナウンス致します。
★過去に資格講習を受講された方へのフォローアップ講習も開催しています。

試験の流れ



※１．受講生が使用する検証実施用機器として、検査資格講習で使用した機器を提供します
※２．試験時間は最大240分としていますが、学科試験・実技試験の時間配分は自由です

試験時の受講生への配布資料

- 試験概要
  - 配布資料１）試験概要・設問
  - 配布資料２）検証対象機器の取扱説明書（簡易版）

- 各種テンプレート
  - 検査用様式１）IoT分野共通セキュリティ要件検査ガイドライン_ヒアリングシート
    ※ヒアリング結果を記載済み
  - 検査用様式２）CCDS_共通セキュリティ要件検査手順書・結果表
  - 試験用様式１）脅威分析表・検証計画
  - 試験用様式２）脆弱性レポート

試験内容・合格基準

- 試験内容
  - （学科試験）CCDS指定検査資格者講習の効果測定テストの中から20問を出題
  - （実技試験）CCDS11要件に関する5問の問題を出題
    - 受験者は、ツールを用いた検証を通して回答を作成

- 合格基準
  - **学科試験、実技試験共に９割以上**正解すること
  - 各書類を提出すること
    - 実技試験の各設問で要求される回答資料
      ※提出資料は設問ごとに異なります

試験に関するFAQ

■この試験に合格すると何ができるようになりますか？

◆合格者はCCDS共通要件のマーク申請に伴う検査（メーカによる自主検査、メーカから委託を受けての第三者検査）およびマーク申請の代行ができるようになります

■資格講習を受講してから要件等の変更があった場合はどうなりますか？

◆前回受講時からの変更部分・差分については適宜フォローアップします

◆フォローアップの方法については以下を予定しています

- 資格講習受講者専用のメーリングリスト、情報公開ページ
- 資格講習受講者に向けたオンライン説明会の実施

■資格講習の受講が受験の要件とありますが、受験資格の有効期限はありますか？

◆当試験制度開始から1年間とし、それ以降は受講から1年間とする予定です。

■受験時には資料を持ち込んだり参照してもいいでしょうか？

◆はい、資料の持ち込みやWeb検索は可能です。
ただし、他の人への相談等は許可していません。