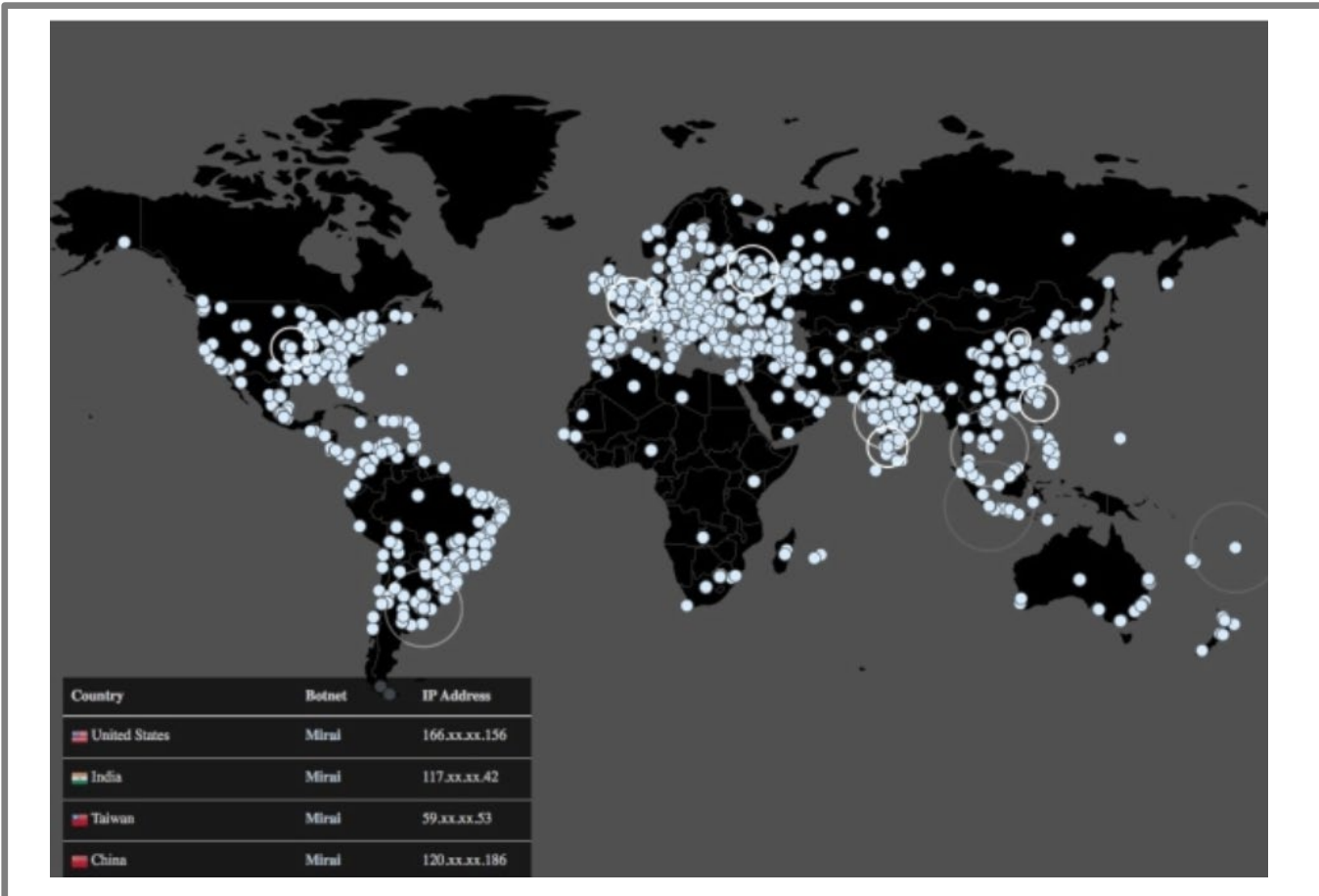


1 IoT機器をとりまくセキュリティの背景

■IoT機器におけるセキュリティ対策が企業にとって重要な命題に！

- ・Mirai、ランサムウェア（Wanna Cry）による攻撃が、グローバルな脅威となる
- ・アメリカにおいて、IoT製品におけるセキュリティ上の脆弱性が訴訟に発展

【マルウェア「Mirai」による攻撃の分布】



出典：https://cybersecurity-index.com

【アメリカにおけるWi-Fiルータの訴訟事例】

2-1. 事例紹介～メーカーの責任が問われる時代 CCDS

■ASUS製ルータにおける脆弱性事例

⇒メーカ企業にとって、セキュリティの脆弱性が、訴訟問題に発展する時代になった！

【概要】

・米FEDERAL TRADE COMMISSION (FTC) は、台湾のコンピュータ・ハードウェアメーカーASUS Tek Computer, inc.のホームルータに脆弱性があり、2014年2月には、脆弱性を悪用した不正アクセスにより12,900件の個人データが流出したと報告。

・この問題は米FTCとASUSの間で訴訟に発展し、ASUSは今後20年間、独立監査の対象となる他、ソフトウェアのアップデートやユーザーへの注意喚起など、包括的なセキュリティプログラムを確立し、維持していく必要がある。

Copyright 2018 Connected Consumer Device Security Council Proprietary 8

出典：CCDS講義資料より

■各省庁の動き

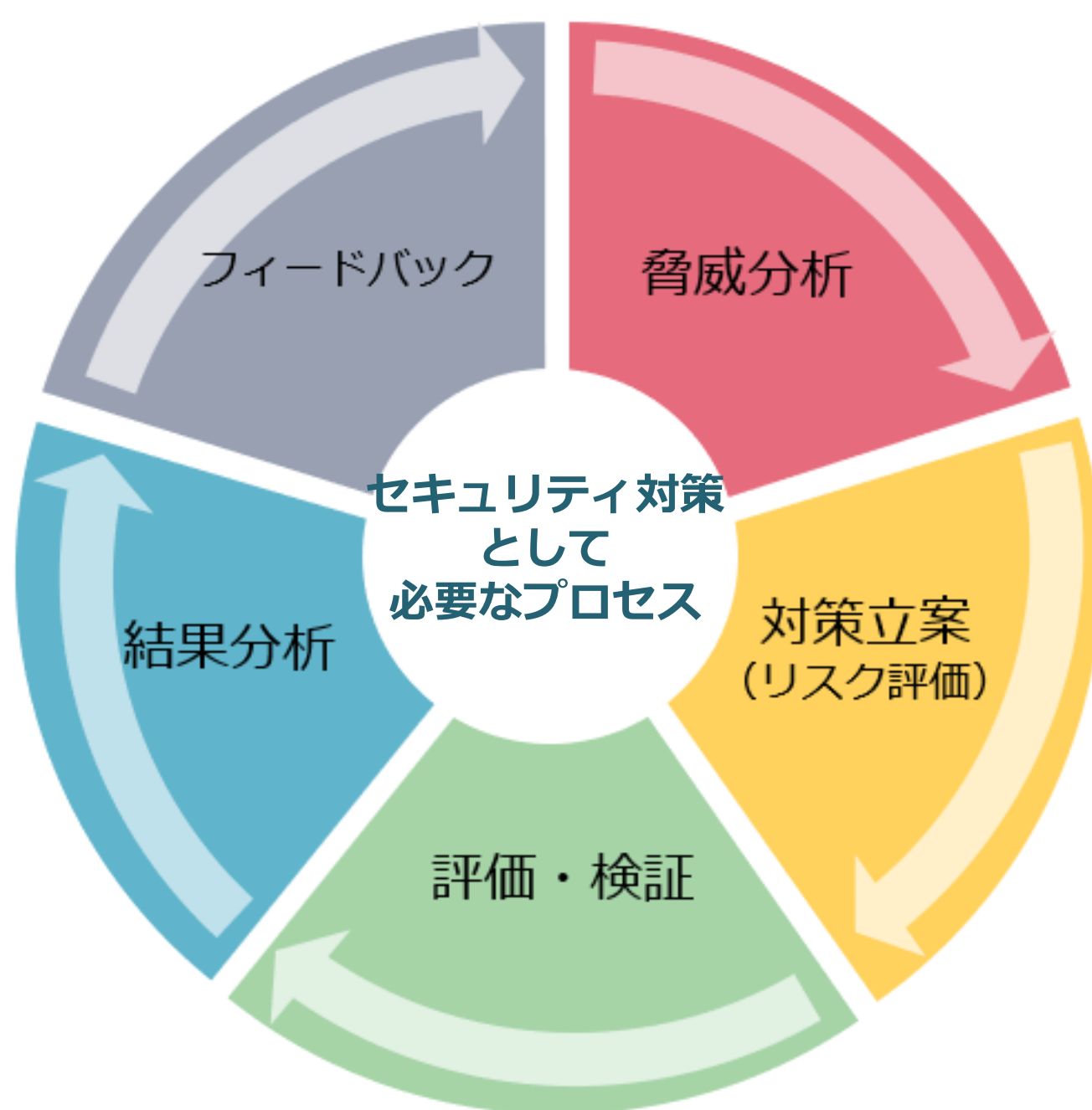
総務省・経産省は、IoT推進コンソーシアムによる活動を通じて、IoT機器のセキュリティに関する認証制度や法整備を視野入れた検討を開始。

IoT機器開発を行う企業にとって、セキュリティ対策は不可避の状況

2 プログラムの構成

■プログラムの特徴

- ・IoT機器のセキュリティ対策を、脅威分析から結果分析までオールインワンで実施可能
- ・基礎＞実践＞応用コースと、段階的にレベルアップしていくプログラム構成
- ・検証ツールや実機を使用し、実習と講義がワンセットとなった演習スタイル



MASTTOP セミナープログラム

脅威分析：

⇒どこがどのように危険なのか？

対策立案

⇒何をどう対策すれば良いのか？

評価・検証：

⇒対策の結果、実際に問題はないか？

結果分析：

⇒問題があった場合の解決策は？

1日目 基礎コース：90分×5講座

- ・IoT機器を取り巻く脅威
- ・情報セキュリティ基礎講座(1)～(3)
- ・検証環境の構築実習

2日目 実践コース：90分×5講座

- ・セキュリティ検証ツールのオペレーション実習
- ・脅威分析～対策立案～リスク評価
- ・セキュリティ課題レポートの作成実習

3日目 応用コース：90分×5講座

- ・IoT機器へのアタック実習
- ・スマートホームへのアタック実習

3 CCDS指定検査資格の取得について

■本プログラムの終了により取得可能な資格

- ・本セキュリティ人材育成プログラムは、CCDSの認定を受けたセキュリティ人材プログラムであり、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証手順・手法の知見や技術を習得できる内容となっています。

- ・IoT機器開発/販売企業がマーク取得のための検査を行う場合や、マーク取得のためのセキュリティ検査を受託する場合には、指定検査資格者としてCCDSの認定を受ける必要があります。
- ・本プログラムの修了により、CCDSに認定された指定検査資格者の資格を得ることが可能です。
- ⇒全教科で効果測定70点以上取得することで、受講修了者として登録されます。

4 プログラムのコース内容

■オールインワンコース：3日間集中講座

- ・対象者：現場のエンジニア（IoT機器の開発者、品質保証担当者、SE、テストエンジニア等）
- ・受講人数：1回10名
- ・開催時期：2019年10月11日、18日、25日開催

【基礎コース】	演習No.	講習テーマ	形式	時間
	F 1	IoT機器をとりまくセキュリティ上の脅威（概況）	講義	90分
	F 2	情報セキュリティ基礎講座（1）～ネットワークセキュリティ編	講義・実習	90分
	F 3	情報セキュリティ基礎講座（2）～サーバセキュリティ編	講義・実習	90分
	F 4	情報セキュリティ基礎講座（3）～Webアプリケーション編	講義・実習	90分
	F 5	CCDSサーティフィケーションマーク共通要件の説明	実習	90分
【実践コース】	演習No.	講習テーマ	形式	時間
	F 6	OSSツールによるセキュリティの検証手法とは ～4つの検証ツールを事例に、使用手順や解析手法を学ぶ	講義・実習	90分
	F 7	OSSツールによるセキュリティ検証のオペレーション実習 ～4ツールを使用した検証の実習	講義・実習	90分
	F 8	システム構成図を用いた脅威分析の実践 ～守るべき資産や想定される脅威の分析～	講義・実習	90分
	F 9	セキュリティ対策フレームワークの活用、リスク評価の実践 ～フレームワークを用いたセキュリティ対策の立案～ ～CVSSv3を使用したリスク評価の実践～	講義・実習	90分
【応用コース】	F 1 0	セキュリティ課題レポートによる課題報告の実践 ～セキュリティ課題の報告レポート作成実習～	講義・実習	90分
	演習No.	講習テーマ	形式	時間
	F 1 1	アタック実習Part. 1～IoT機器単体（1）	実習	90分
	F 1 2	アタック実習Part. 1～IoT機器単体（2）	講義・実習	90分
	F 1 3	アタック実習Part.2～スマートホームシステム（1）	実習	90分
	F 1 4	アタック実習Part.2～スマートホームシステム（2）	実習	90分
	F 1 5	アタック実習Part.2～スマートホームシステム（3）	講義・実習	90分

5 お問い合わせ先

■株式会社マストトップ

担当： 田久保 順<takubo@mast-top.com>
松本 潤<j-matsumoto@mast-top.com>