# 電気通信機器のMRA -

# サイバーセキュリティに関する米国の最新動向

2022年3月10日

ラモナ・ザー

米国国立標準技術研究所（NIST）

米国商務省

米国

- US TEL MRA参加
- MRAの範囲とサイバーセキュリティの追加
- サイバーセキュリティに関する米国の最新動向
- 消費者向けIoT製品の自主的なラベル付け基準

# 米国TEL MRA パートナー

## APEC TEL MRA

オーストラリア
カナダ
台湾
香港
韓国
マレーシア
ニュージーランド
シンガポール
ベトナム

## 二国間MRA

イスラエル
日本
メキシコ
欧州連合
イギリス

# 米国 **FCC** - 機器認証手続き
# 47 CFR

**1.サプライヤーの適合性宣言（SDoC）について**

**2.認証**

FCC認定の試験所の利用が必要

FCC認定の電気通信認証機関の利用が必要

資料： https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization

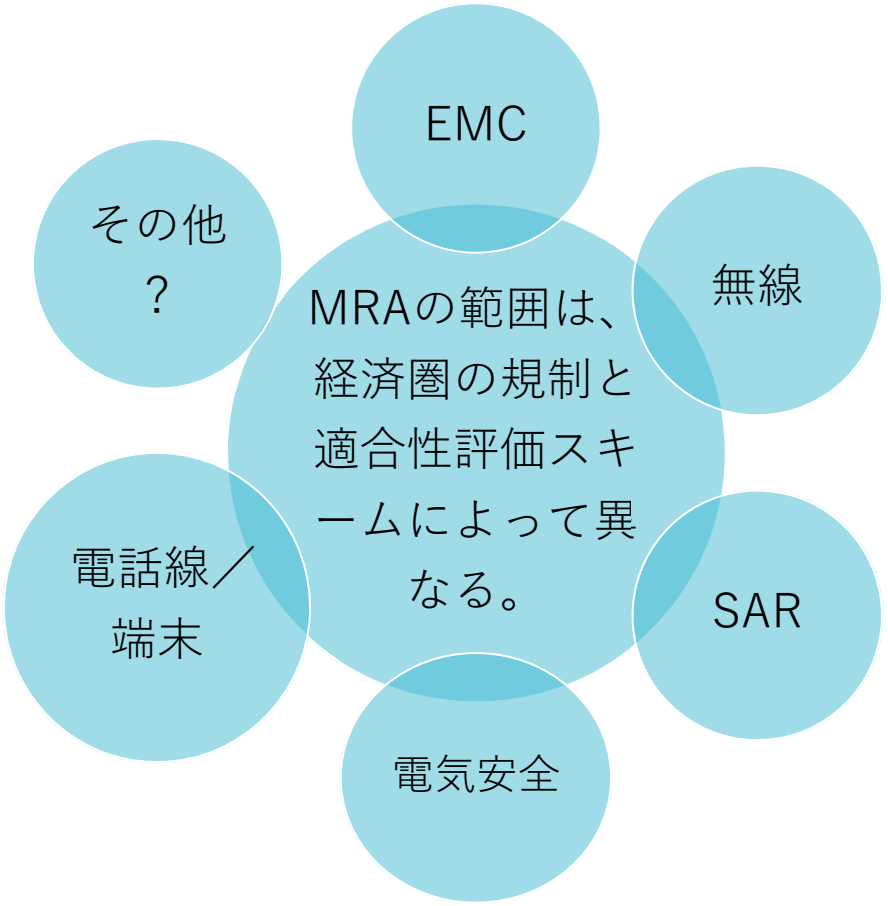
# 米国**NIST**の指定機関としての役割

1.**米国のCABをMRAパートナーの電気通信規制当局に対して指定する**

2.**米国のTCBをFCCに対して指定する**

資料： https://www.nist.gov/mutual-recognition-agreements-mras

# TEL MRAの範囲は技術や規制に対応して変化を遂げた



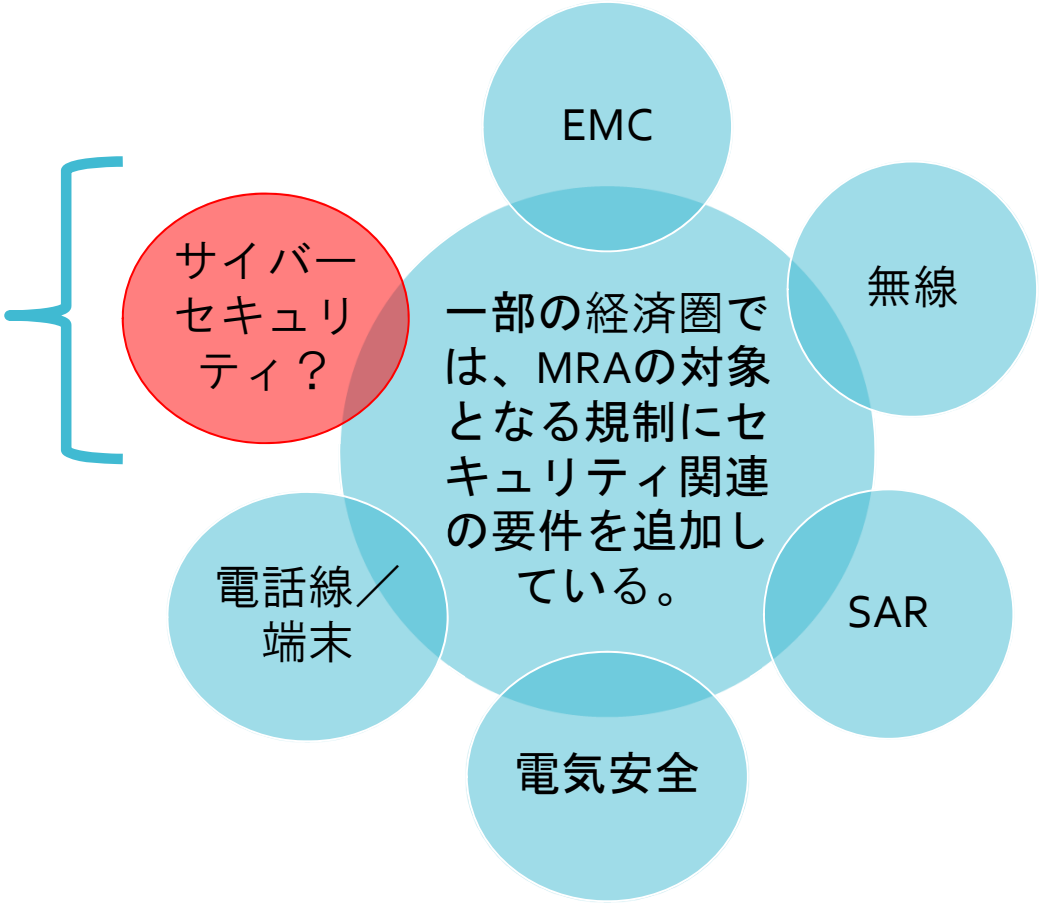

各規制当局は、それぞれの規制に含まれる要素とMRAでカバーされる要素を決定する。

# 最近の動き：サイバーセキュリティの要件の導入

日本

EU

その他？




CABは、関連するMRAパートナー規制スキームに参加するために、サイバーセキュリティ適合性評価活動における能力を証明しなければならない。

各規制当局は、それぞれの規制に含まれる要素とMRAでカバーされる要素を決定する。

# 無線／IoT機器の**サイバーセキュリティ**に関する最近の動向
# 米国 - FCC

2021年8月19日 FCC 21-73 **規制作成の通知**(NPRM) および**照会の通知(NOI)**の公開について

NPRM：機器認証手続の具体的な変更を提案
NOI：FCCの機器認可プログラムが、適切な基準やガイドラインを通じて機器のサイバーセキュリティを向上させるためにどのように利用できるかについてのパブリックコメントの募集。

FCC 21-73に関するコメント期間およびFCC回答コメント期間が終了。

FCCはコメントを検討し、今後の方針を決定する。

# 無線／IoT機器の**サイバーセキュリティ**に関する最近の動向
# 米国-**ホワイトハウスの大統領令（EO）について**

*米国のサイバーセキュリティの向上*に関するホワイトハウスの大統領令14028号の発行（2021年5月12日）

> EOの第4節では、次の項目に係るサイバーセキュリティのラベル付け基準の策定に関する具体的なタスクをNISTに割り当てている。
>
> **消費者向けIoT機器**
>
> 消費者向けソフトウェア

与えられた時間は 1年

# **米国大統領令14028 -** 消費者向けIoT製品のラベル付け基準

## 現在の状況

モノのインターネット（IoT）機器には、**顧客**である組織や個人がサイバーセキュリティ・リスクを軽減するために利用できる**機器サイバーセキュリティ機能を備えていないことが多い。**

*資料：NISTIR 8259*


ラベルの目標

メーカーが**自主的に**IoT製品のサイバーセキュリティを向上させる動機を与える。

**消費者を教育し**、サイバーセキュリティの問題に対する**意識を高める。**

# 推奨基準が**公開された**

2021年、NISTは公開ワークショップを開催し、関係者の意見を聞き、推奨基準を策定。

2022年2月4日、NISTは「***消費者向けモノのインターネット（IoT）製品のサイバーセキュリティ・ラベル付けに関する推奨基準***」を発表（NISTホワイト・ペーパー）

- 消費者向けIoT製品の基準を参照

注：NISTは、「消費者向けソフトウェアのサイバーセキュリティ・ラベル付けに関する推奨基準」も発表。 ここでは取り上げていないが、これも重要な文書。

# 基準について

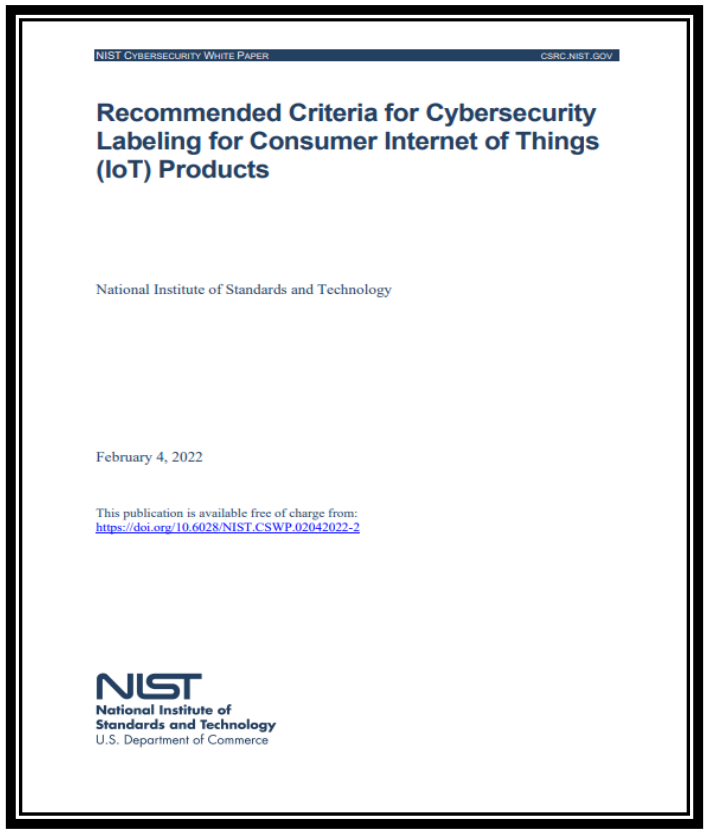
これらは、**消費者向けIoT製品の**サイバーセキュリティに関する**自主的な**ラベル付けのための、技術基準および非技術基準のベースライン（最低基準）。

この基準は、**スキームの所有者が**独自のラベル付けプログラムの一部として**使用する**ためのもの。

NISTは独自のラベル付けプログラムを確立しておらず、ラベルのデザインも行っていない。

基準は**望ましい結果**で表現されており、具体的な技術基準／適合性評価手法ではない。

技術的なアプローチは、**製品の種類**と機能、および利用可能な技術基準に基づいて、**スキームの所有者**が決定する。




# 主な推奨事項

範囲

技術的ラベルの基準

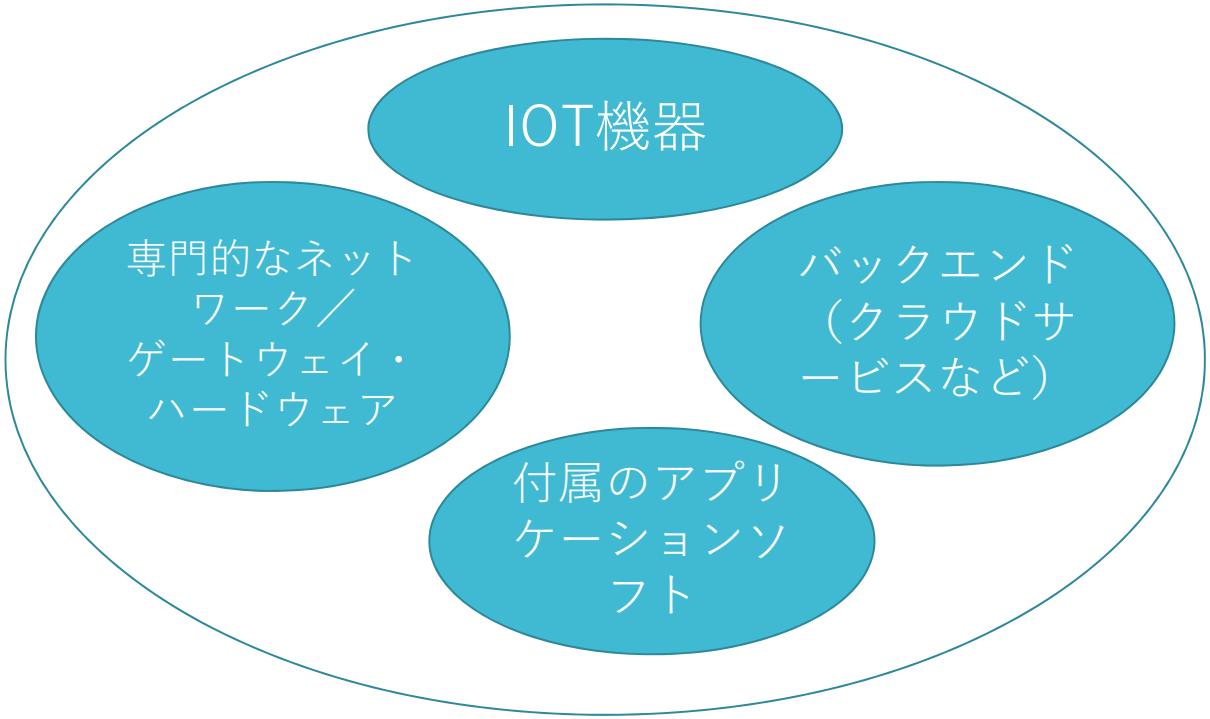
非技術的なラベルの基準

ラベルのタイプ

消費者教育

*この他にも多くの詳細情報や考慮事項を記載している。*

推奨されるラベル付け基準の範囲　**消費者向けIoT製品全体**




*NISTのホワイト・ペーパー：　IoT機器のコンポーネントは、IoT機器や、IoT機器が作成・使用するデータにアクセスすることができる。これらのコンポーネントは、IoT機器やお客様などに影響を与える可能性のある潜在的な攻撃ベクターとなる....これらの**補助的なコンポーネントは、IoT製品に新たなリスクや固有のリスクをもたらす可能性があるため、補助的なコンポーネントを含めたIoT製品全体をセキュリティで保護する必要がある。***

# ラベルの推奨ベースライン（最低）**技術基準**

**技術基準 (6)**

- 資産の識別
- 製品構成
- データ保護
- インターフェイスのアクセス・コントロール
- ソフトウェア・アップデート
- サイバーセキュリティの現状認識

NISTIR 8529A - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf も参照のこと

# ラベルの推奨ベースライン（最低）**非技術基準**

**非技術基準(4)**

- 文書化
- 情報・問い合わせ受付
- 情報発信
- 製品の教育と認知度

- NISTIR 8259B:
  https://csrc.nist.gov/publications/detail/nistir/8259b/final
  も参照のこと

# 推奨**ラベルタイプ**

## NISTが推奨するバイナリー・ラベル

- これは、製品が基準となる規格を満たしていることを示す単一のラベルを意味する。
  - *製品にはラベルが付いているか、付いていないかのどちらかである。*
- URLやQRコードによる付加情報の提供
- 物理的とデジタルの両フォーマットに対応

## 一般消費者にも使える

- このラベルは、サイバーセキュリティの専門知識を持たず、ラベル基準の技術的メリットを判断できない可能性のある一般消費者にとっても使用可能なものでなければならない。

# 推奨される**消費者教育の取り組み**

NISTは、ラベル・スキームの所有者に対して、強力な**消費者教育キャンペーン**を実施することを推奨している。

- ラベル認知度の確立と向上
- プログラムの重要な側面に関する消費者への透明性の提供
- IoT製品関係者がラベルについて話すための共通の方法を確保する

また、スキーム所有者は、ラベルが何を意味し、何を意味しないかなどの詳細を含む、**ラベル付けスキームに関する主要な情報に**消費者が**オンラインでアクセスできるようにする**必要がある。

.

# 次（現在）のステップ **試験段階**

NISTは現在、以下のような質問に対する関係者の意見を求めている。

- 一部またはすべての基準に対応する既存のラベル付けスキームはあるか？
- この基準に基づいて新しいプログラムを立ち上げることに興味のある組織はあるか？
- 基準に基づいた消費者向けIoT製品ラベル付け制度の潜在的な動機とは？

関心のある方は、**2022年3月15日**までに labeling-eo@nist.gov にコメントをお送りください。

資料：*https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots-approach*

# 最終ステップ　NIST**概略報告**の発行

EOで与えられたタスクを完了するために、NISTは試験段階で得られた情報を考慮して、2022年5月12日までに**概略報告**を作成し、発行しなければならない。

これにより、EOで要求されているアクションが完了する。

**この取り組みに関する今後のアクションは、まだ定義されておらず、決定もされていない。**

[例えば、*消費者向けIoT製品や消費者向けソフトウェアのラベル付けプログラムの**義務化を開始するような**指示や要請はない*]。

# 本日のトピックのおさらい

MRAパートナー規制当局の中には、MRAの対象となる規制に**サイバーセキュリティ**を含めているところもある。 CABは、関連するサイバーセキュリティの適合性評価活動のための**能力**を実証しなければならない。

FCCの機器認可プログラムの現在の範囲には、サイバーセキュリティは含まれていない。 FCCは、機器のサイバーセキュリティを向上させるために、このプログラムを利用できるかどうか、あるいはどのように利用できるかを判断するために、**NOI**を発行した。FCCは、今後の方針を決定するために、関係者のコメントを検討している。

USG（NIST）は、**消費者向けIoT製品**および**消費者向けソフトウェア**に対する推奨サイバーセキュリティ・ラベル付け基準を策定した。スキームの所有者がこの基準を採用し、（1）**サイバーセキュリティの改善を動機とし**、（2）サイバーセキュリティの問題に対する消費者の**意識**を高めるために、**自主的な**ラベル付けプログラムの提供を開始することが期待されている。

ご清聴ありがとうございました。

質問
mra@nist.gov

連絡先
Ramona.saar@nist.gov