

IoT製品に対するセキュリティ 適合性評価制度に関する実証について

2023年 7月 19日

本日はご議論いただきたいこと

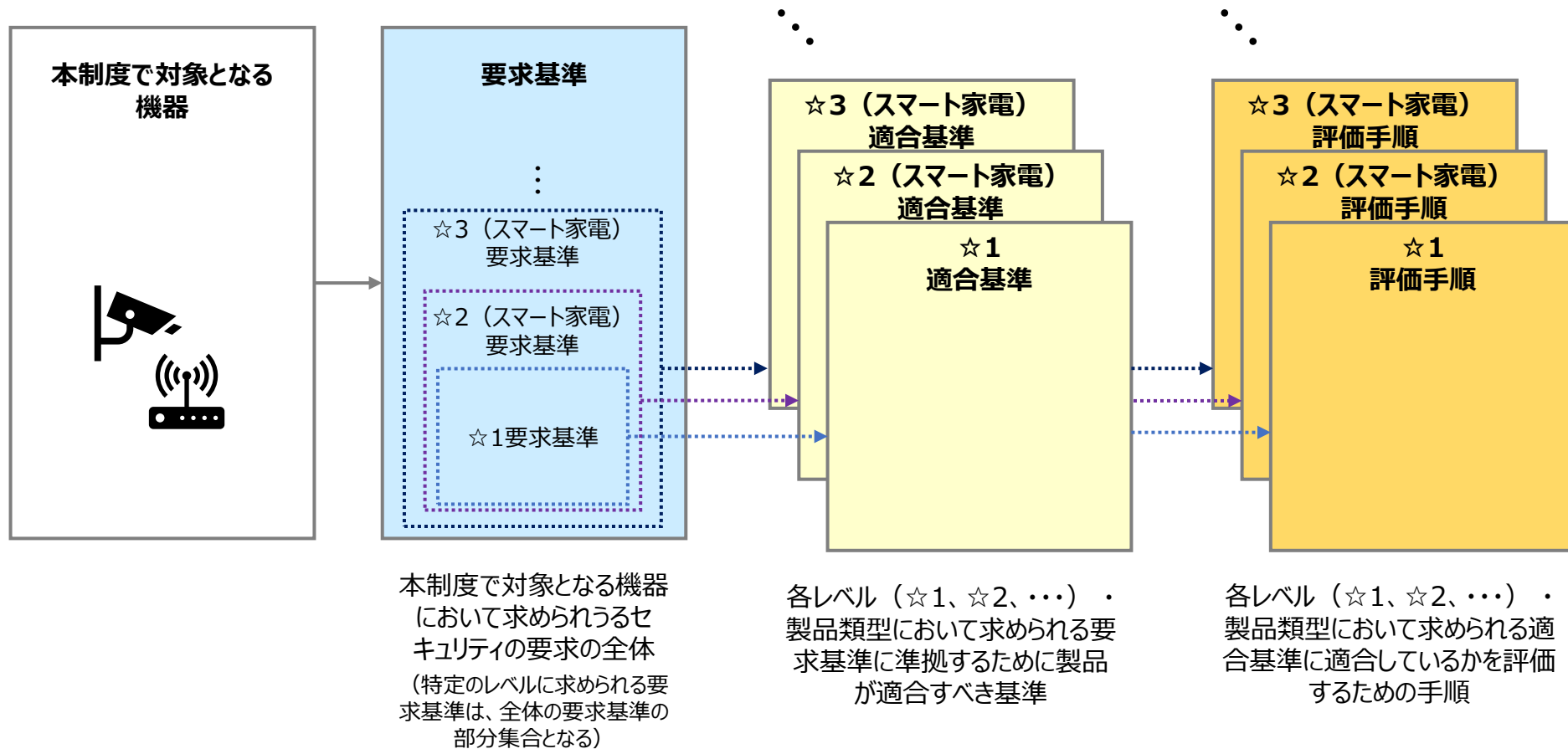
- 今年度の適合性評価の実証方針について【本資料】
- 検討を進める具体的な適合性評価スキームについて【資料 3 - 2】

適合性評価に関する実証の目的・進め方

中間とりまとめの記載事項

- どのような製品類型に対し、いかなる基準を適用することで、関係者にどの程度のコストが発生するかについて実証等を通じて検証する必要がある。

- 今年度、実際の製品に対する適合性評価の評価検証を行い、関係者にどの程度のコストが発生するかを検証する。
- プレ委員会を設置し主に☆1（最も低レベルの評価基準）の要求基準案・適合基準案・評価手順案を議論・策定し、これに基づき製品に対する適合性評価の評価検証を行う。



要求基準及び適合基準に関する検討体制（プレ委員会）

- ・ 制度開始以降、評価基準等を検討する委員会（検討委員会）においては、

(1)対象機器の定義や、IoT製品共通の要求基準を策定する機能

(2)製品・レベル毎の要求基準を満たしていることを示す適合基準及びそれに対する評価方法を策定する機能

の2つの機能が必要となる。

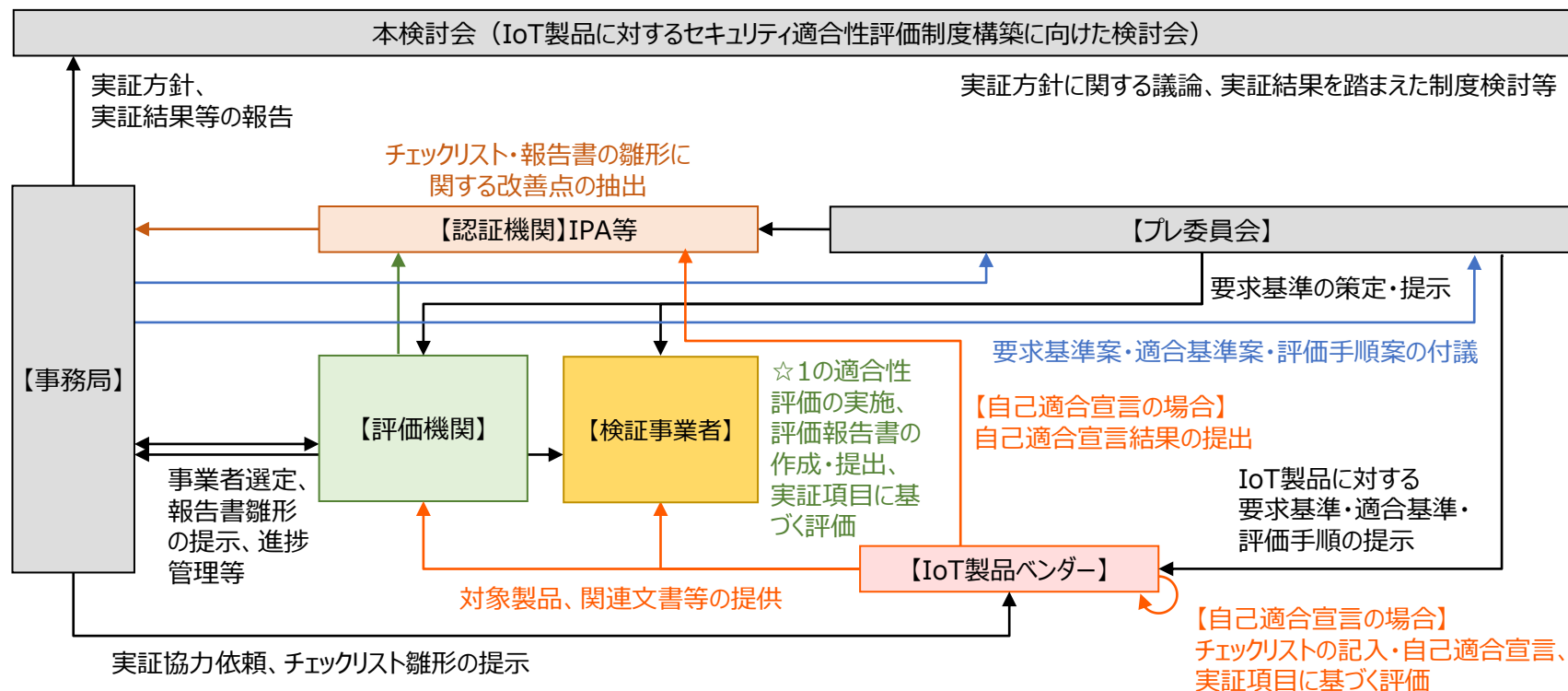
- ・ (1)では、対象機器の定義や本制度で対象とするIoT製品に想定される脅威に対して必要な「要求基準」を策定する。主に、評価機関や製品を利用・調達する側から望ましいセキュリティを考慮した意見を反映する。
- ・ (2)では、製品・レベル毎に、どの程度の安全性を実現すれば要求基準で求められる事項を満たすかを示す「適合基準」を策定するとともに、適合基準を評価するための「評価手順」を策定する。適合基準については、主に製品ベンダーから実装する機能についての技術面やコスト面を考慮した意見を反映するとともに、評価手順については、セキュリティ検証事業者の意見を反映する。

機能	目的	アウトプット	主なメンバー構成
機能 (1) 対象機器の定義や、適合基準策定WGが付議する要求基準案について議論し、制度で用いる要求基準を策定・更新する。	IoT製品の適合性評価の対象となる機器の定義、要求基準を議論・策定する。 主に、評価機関や製品を利用・調達する側の意見を反映する。	・ 本制度で対象とする機器の定義 ・ 本制度におけるレベル・製品類型で共通の要求基準	・ 学識者 ・ 評価機関 ・ IoT製品調達関連組織 ・ 既存適合性評価スキーム関係者 ・ 【オブザーバー】将来的に評価機関になり得る機関
機能 (2) 配下の適合基準策定WGが付議する適合基準案・評価手順案について議論し、制度で用いる適合基準・評価手順を策定する。	対象IoTの製品が、要求基準を満たしていることを示す適合基準、適合基準を評価するための評価手順を議論・策定する。 主に、製品ベンダー及びセキュリティ検証事業者からの意見を反映する。	・ 各レベル・製品類型における適合基準 ・ 各レベル・製品類型の適合基準に対する評価手順	・ 学識者 ・ 評価機関 ・ IoT製品ベンダー／ベンダー関連業界団体 ・ 既存適合性評価スキーム関係者 ・ 【オブザーバー】IoT製品に関する業界団体

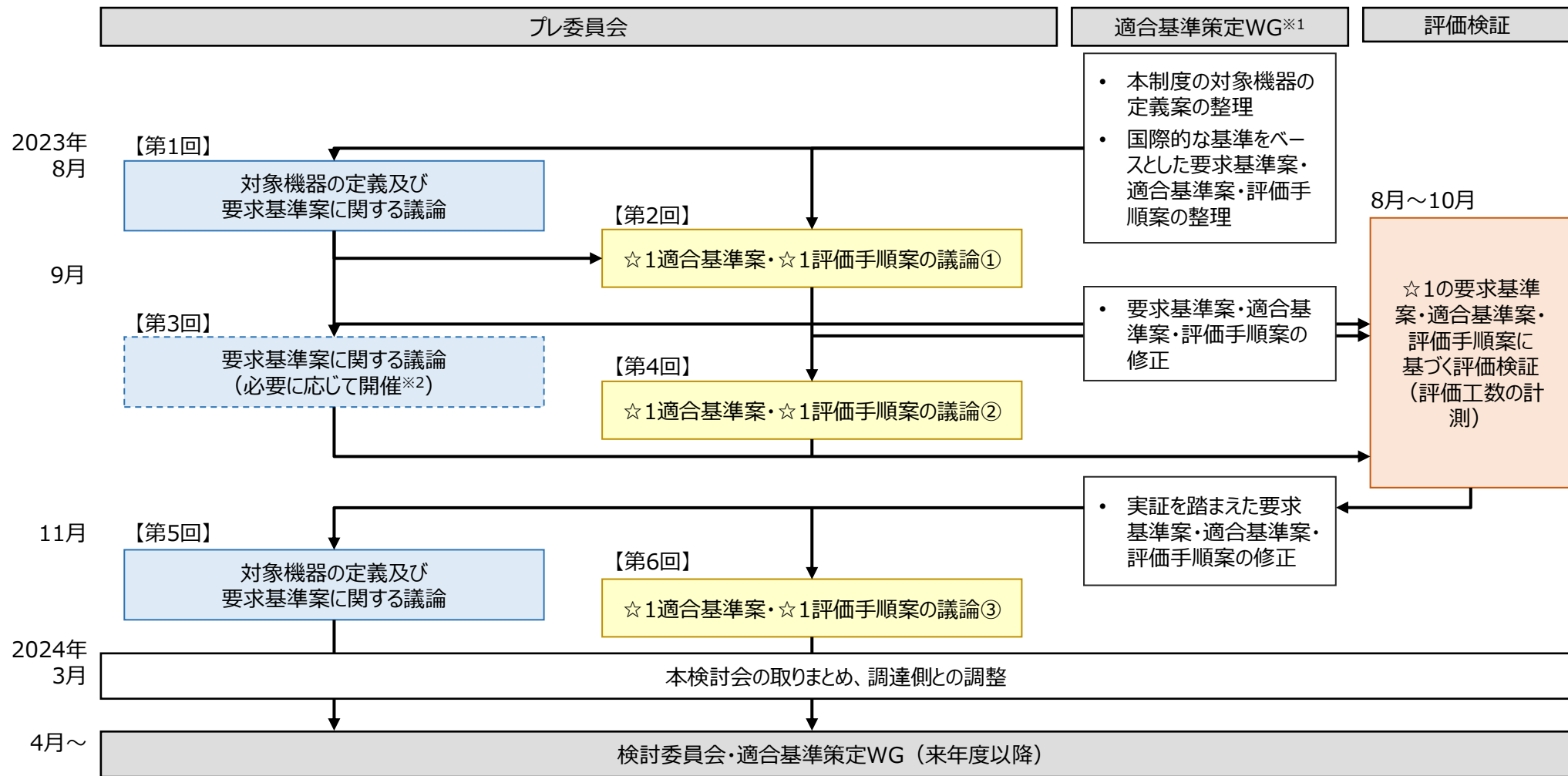
実証実施体制

- 自己適合宣言の場合、IoT製品ベンダー自身でチェックリストに基づく自己適合宣言を行い、実証項目に基づく評価を行う。また、検証事業者による評価を実施する。
- 第三者評価の場合、評価機関において、実証対象製品を開発するIoT製品ベンダーから提供される製品関連文書に基づき、☆1の適合性評価を行うとともに、評価報告書の作成及び実証項目に基づく評価を行う。
- 認証機関においては、IoT製品ベンダーや評価機関から提出されたチェックリストや報告書を確認し、それぞれの雛形に関する改善点を抽出する。
- 事務局においては、プレ委員会に対して、要求基準案・適合基準案・評価手順案を付議するとともに、評価機関及びIoT製品ベンダーの選定・協力依頼を行い、実証の進捗を管理する。

実証実施体制



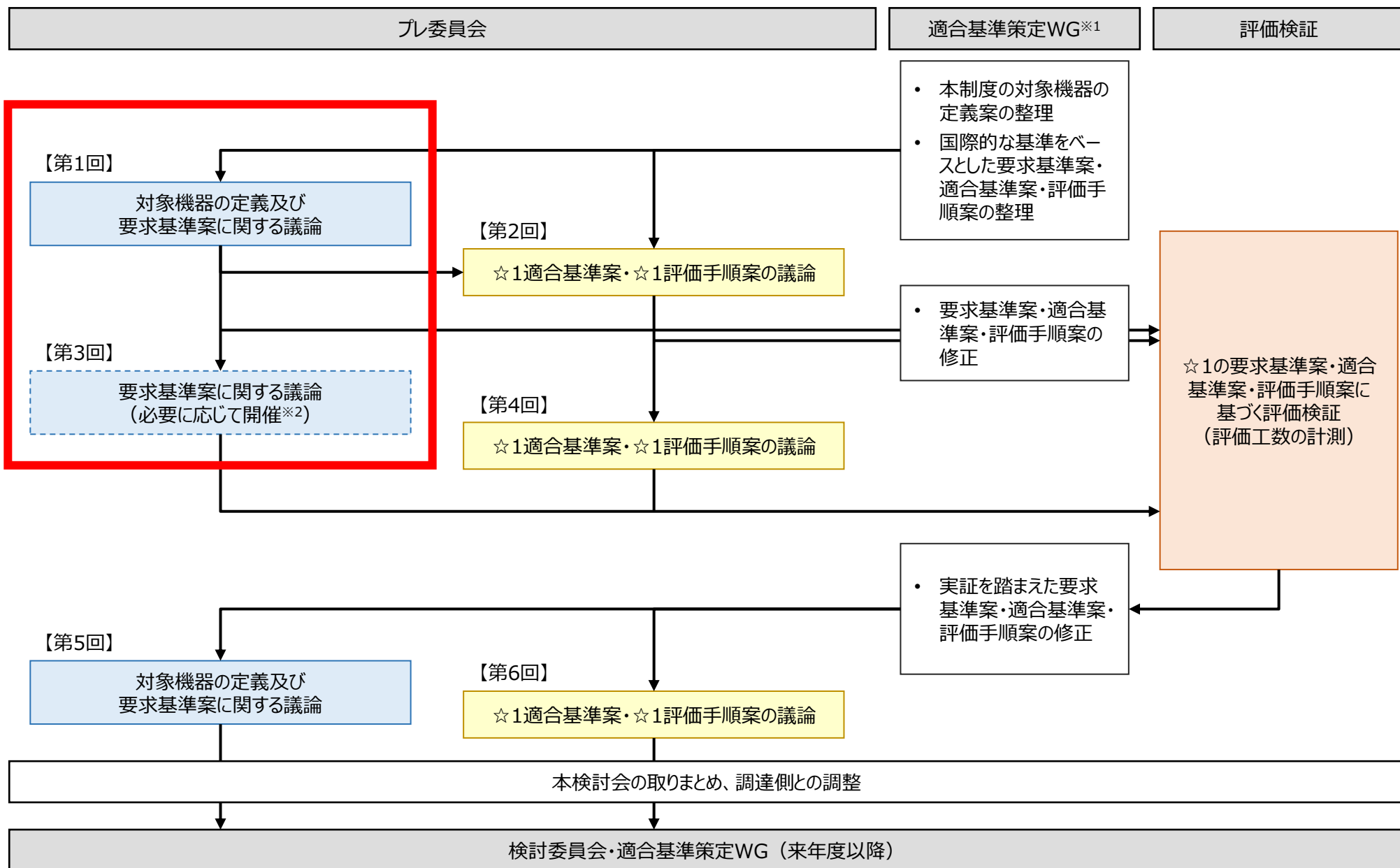
実証プロセス



※1 今年度は事務局が適合基準策定WGの役割を担い、事務局にて、要求基準案・適合基準案・評価手順案の検討・作成を行う。

※2 初回プレ委員会の議論で要求基準案が定まらなかった場合に開催する。

対象機器の定義及び要求基準案に関する議論 (1)



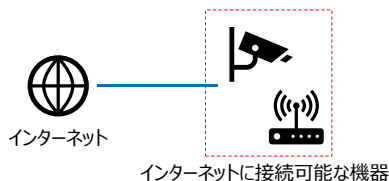
※1 今年度は事務局が適合基準策定WGの役割を担い、事務局にて、要求基準案・適合基準案・評価手順案の検討・作成を行う。

※2 初回プレ委員会の議論で要求基準案が定まらなかった場合に開催する。

対象機器の定義及び要求基準案に関する議論（2）

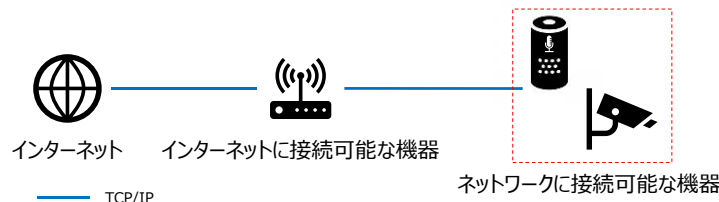
本制度の対象機器は、「インターネットに接続可能な機器」及び「ネットワークに接続可能な機器」である。

「インターネットに接続可能な機器」とは、TCP/IPの一部を構成する通信プロトコルを使用して、インターネット上でデータを送受信する機能を持つ機器である。



図「インターネットに接続可能な機器」のイメージ

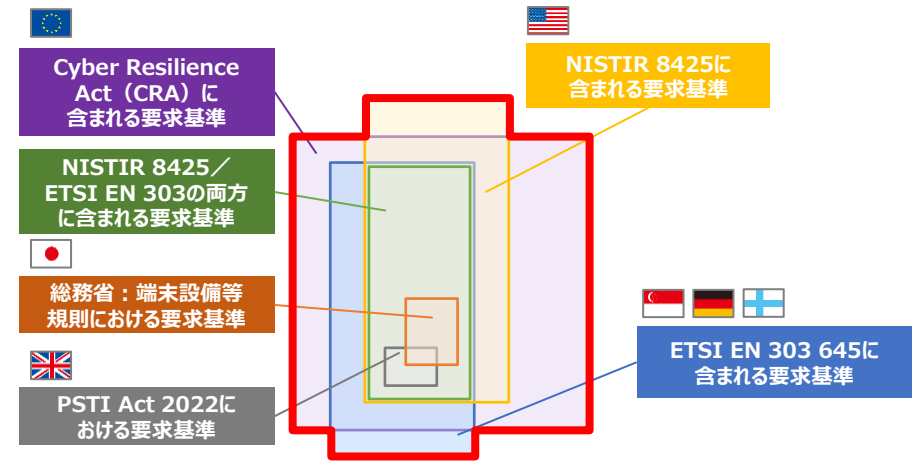
「ネットワークに接続可能な機器」とは、インターネットに接続可能でない機器のうち、電氣的又は電磁的エネルギーを伴う伝送により、データを送受信する機能を持つ機器であり、TCP/IPの一部を構成する通信プロトコルによって、「インターネットに接続可能な機器」に接続可能な機器である。



図「ネットワークに接続可能な機器」のイメージ

...

本制度で対象とする機器の技術的な定義案を議論・策定する。

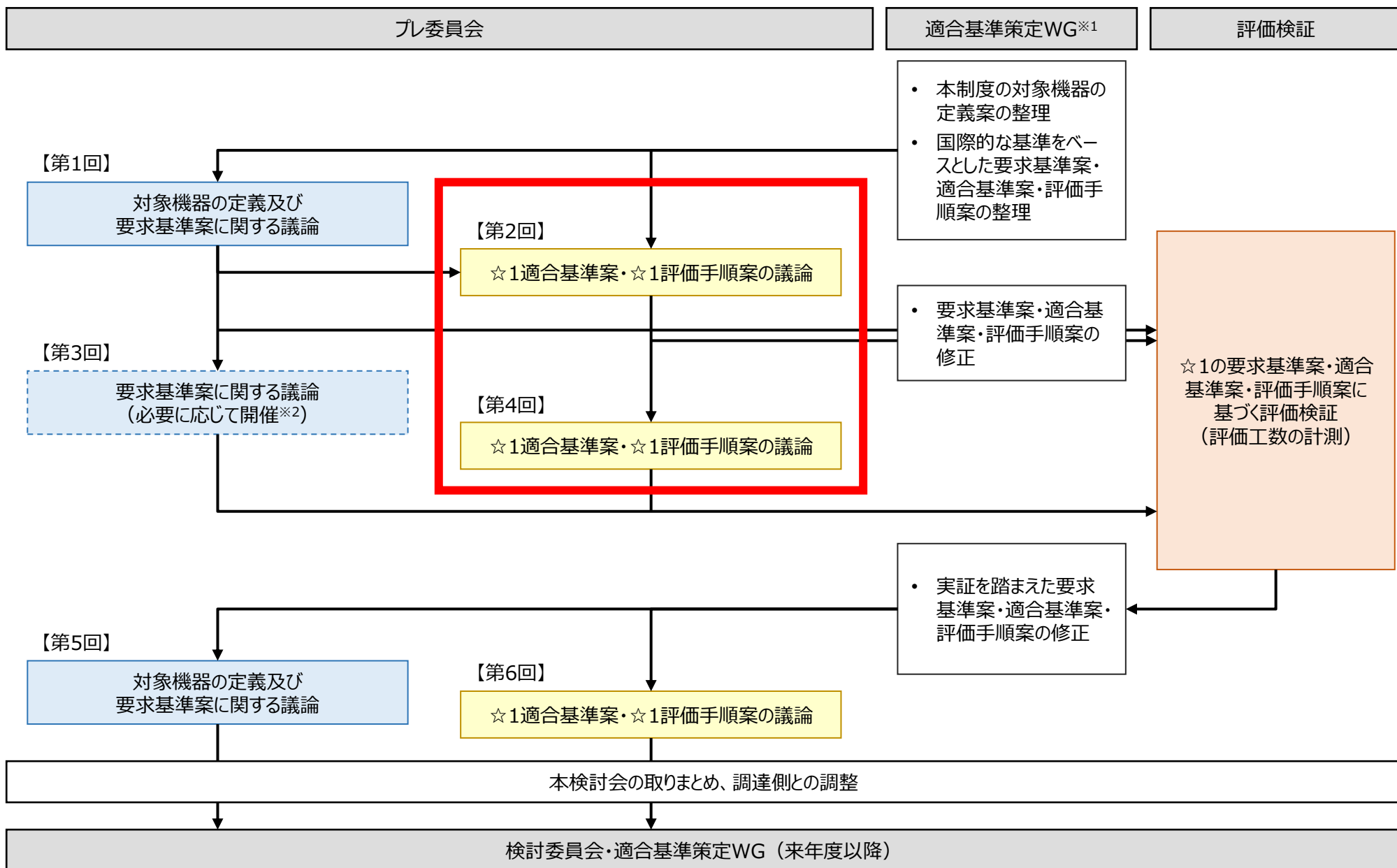


ETSI EN 303 645、NISTIR 8425、EU-CRA等の諸外国の要求基準の集合関係を整理し、重ね合わせの関係（ $\cup$ （カップ））にある要求事項を整理し、要求基準のロングリストを作成する（一部については、基準の取捨選択や独自基準の追加も検討する）。

要求基準のロングリスト（案）	
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用される機器において、定義された品質尺度に合ったパスワードが設定される、もしくは利用者によって設定できることを要求する。
	1-2. 製品導入時に固有のパスワードを使用する場合、定義された品質尺度に合ったメカニズムでパスワードが生成されることを要求する。
	1-3. 各認証メカニズムが、定義された品質尺度を満足する完全性、真正性及びセキュリティ保証であることを要求する。
	1-4. 各認証メカニズムについて、技術知識が限られる利用者が認証値を変更するためのメカニズムを提供することを要求する。
	1-5. 各認証メカニズムにおいて、失敗した認証試行が特定の数になった後、定義されたアクションが講じられることを要求する。
...	...

国際的な標準をベースに、本制度における要求基準案を議論・策定する。

☆ 1適合基準案・☆ 1評価手順案に関する議論 (1)



※1 今年度は事務局が適合基準策定WGの役割を担い、事務局にて、要求基準案・適合基準案・評価手順案の検討・作成を行う。

※2 初回プレ委員会の議論で要求基準案が定まらなかった場合に開催する。

☆ 1適合基準案・☆ 1評価手順案に関する議論 (2)

..... 来年度以降検討・策定を予定➡

要求基準のロングリスト（案の例）		☆ 1適合基準（案の例）	☆ 2適合基準（製品類型ごと）（案の例）	☆ 3適合基準（製品類型ごと）（案の例）
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用される機器において、定義された品質尺度に合ったパスワードが設定される、もしくは利用者によって設定できる。	製品導入時に初期パスワードを使用する場合、英数字からなる8桁以上の固有のパスワードを設定するか、利用者によって当該パスワードに設定ができる。	製品導入時に初期パスワードを使用する場合、容易に推測可能ではなく、英数字記号からなる16桁以上の固有のパスワードを設定するか、利用者によって当該パスワードに設定ができる。	...
	1-2. 製品導入時に固有のパスワードを使用する場合、定義された品質尺度に合ったメカニズムでパスワードが生成される。	- 生成されるパスワードは、容易に推測可能なパスワードではなく、英数字からなる8桁以上のパスワードである。容易に推測可能であるパスワードとは、以下のパスワードを意味する。 ✓ カウンタの増加により自動生成されるパスワード ✓ MACアドレス等の情報と同一もしくは関連したパスワード ✓ 共通した文字列や共通的なパターンを含むパスワード	生成されるパスワードは、容易に推測可能なパスワードではなく、英数字記号からなる16桁以上のパスワードである。	...
	1-3. 各認証メカニズムが、定義された品質尺度を満足する完全性、真正性及びセキュリティ保証である。	(適合基準設定せず)	- 認証情報は、TLS1.2以上の安全なチャネルを介して通信する。 - チャレンジ&レスポンスによる認証プロトコルにより検証する。	...
	1-4. 各認証メカニズムについて、技術知識が限られる利用者が認証値を変更するためのメカニズムを提供する。	- 認証に使用される手段（指紋、パスワード、その他トークン）に関わらず、利用者によって認証値を変更できる。 - 利用者が認証を変更する方法を、利用者がアクセスできるドキュメントリソースにて明記する。	- 認証に使用される手段（指紋、パスワード、その他トークン）に関わらず、利用者によって認証値を変更できる。 - 利用者が認証を変更する方法を、利用者がアクセスできるドキュメントリソースにて明記する。	...
	1-5. 各認証メカニズムにおいて、失敗した認証試行が特定の数になった後、定義されたアクションが講じられる。	(適合基準設定せず)	5回連続して認証に失敗した場合、5分間、アカウントをロックする。 - さらに5回連続して認証に失敗した場合、アカウントをロックする。	...
...	...	(適合基準設定せず)	...	...
...	...	...	...	...

☆ 1 では適合基準が設定されず、
☆ 2 では設定されるような要求基準も存在

☆ 1 でも☆ 2 でも適合基準が設定されるものの、
適合基準の要求内容はレベルに応じて異なるものも存在

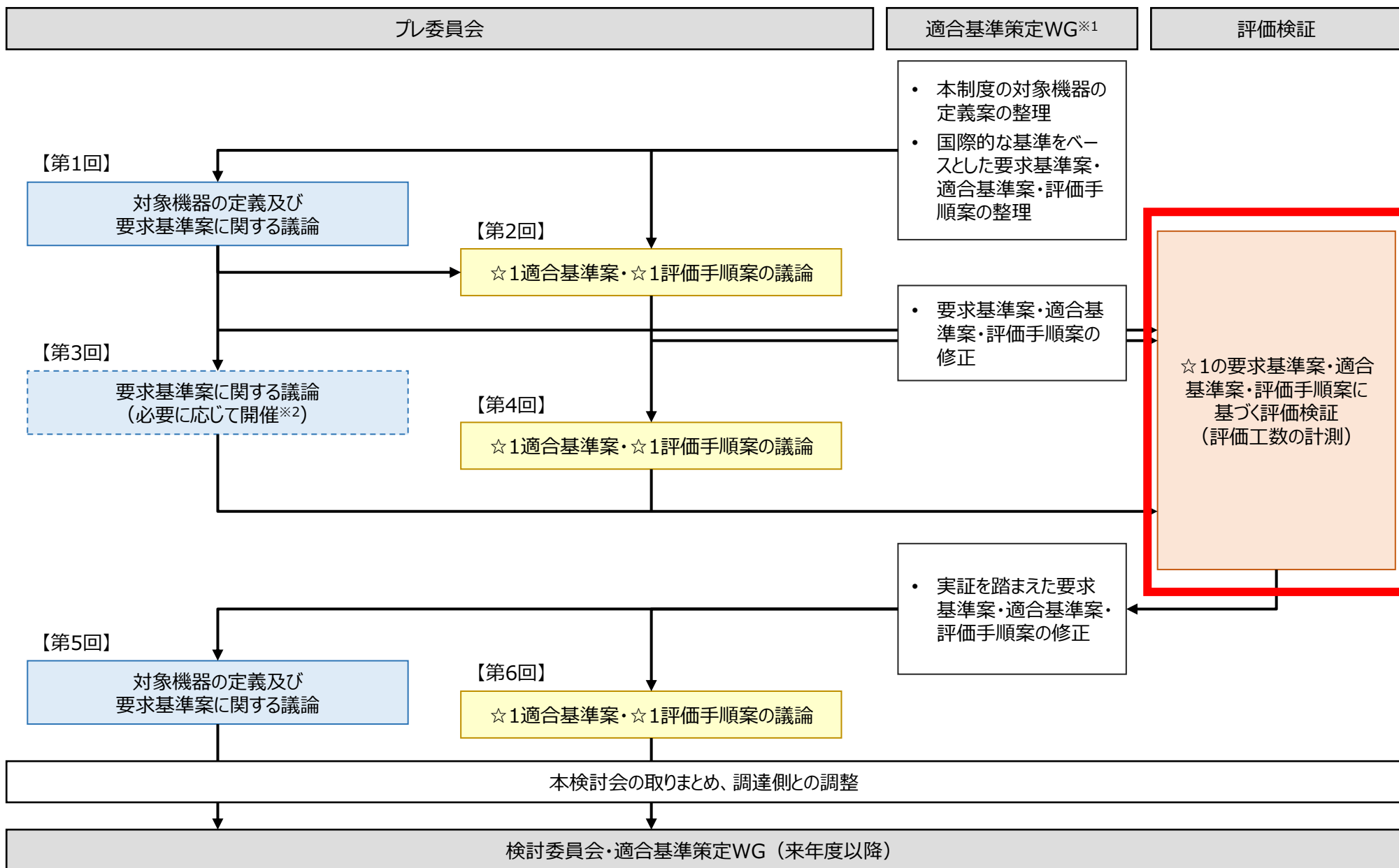
☆ 1レベルであれば、要求基準のロングリストのうち、どの基準が必要かを検討し、当該基準に準拠するために求められる適合基準案を策定する。

☆ 1適合基準案・☆ 1評価手順案に関する議論 (3)

要求基準（案の例）		☆ 1適合基準（案の例）	☆ 1評価手順（案の例）
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用される機器において、定義された品質尺度に合ったパスワードが設定される、もしくは利用者によって設定できる。	製品導入時に初期パスワードを使用する場合、英数字からなる8桁以上の固有のパスワードを設定するか、利用者によって当該パスワードに設定ができる。	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	1-2. 製品導入時に固有のパスワードを使用する場合、定義された品質尺度に合ったメカニズムでパスワードが生成される。	- 生成されるパスワードは、容易に推測可能なパスワードではなく、英数字からなる8桁以上のパスワードである。容易に推測可能であるパスワードとは、以下のパスワードを意味する。 ✓ カウンタの増加により自動生成されるパスワード ✓ MACアドレス等の情報と同一もしくは関連したパスワード ✓ 共通した文字列や共通的なパターンを含むパスワード	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	1-3. 各認証メカニズムが、定義された品質尺度を満足する完全性、真正性及びセキュリティ保証である。	認証情報は、TLS1.2以上の安全なチャネルを介して通信する。	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	1-4. 各認証メカニズムについて、技術知識が限られる利用者が認証値を変更するためのメカニズムを提供する。	- 認証に使用される手段（指紋、パスワード、その他トークン）に関わらず、利用者によって認証値を変更できる。 - 利用者が認証を変更する方法を、利用者がアクセスできるドキュメントリソースにて明記する。	- 実機に対する動作試行に基づき、対象製品が適合基準に適合していることを評価する。 - 製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	1-5. 各認証メカニズムにおいて、失敗した認証試行が特定の数になった後、定義されたアクションが講じられる。	5回連続して認証に失敗した場合、15秒間、アカウントをロックする。 - さらに5回連続して認証に失敗した場合、15分間、アカウントをロックする。 - さらに5回連続して認証に失敗した場合、60分間、アカウントをロックする。	実機に対する動作試行に基づき、対象製品が適合基準に適合していることを評価する。
	...	(適合基準なし)	—
...	...	...	...

☆ 1の各適合基準に適合しているかを評価するための手順を策定する。

実証の実施（1）



※1 今年度は事務局が適合基準策定WGの役割を担い、事務局にて、要求基準案・適合基準案・評価手順案の検討・作成を行う。

※2 初回プレ委員会の議論で要求基準案が定まらなかった場合に開催する。

実証の実施（2） | 実証内容・実証項目

- ・ プレ委員会を通じて策定した☆1の**要求基準案・適合基準案・評価手順案**に基づき、**対象製品に対する☆1の適合性評価の実証を行う**。
- ・ 実証では、**適合性評価に要する工数の確認や金銭的コストの算出、要求基準案・適合基準案・評価手順案の妥当性の確認、適合性評価に求められる知識・スキルに関する確認項目等**を検証する。
- ・ 実証結果を踏まえ、調達者、IoT製品ベンダー、評価機関等の全体の利益を考慮した制度を検討する。
- ・ ☆1ではIoT製品ベンダー自身による自己適合宣言も想定されるが、本実証では、IoT製品ベンダーによる自己適合宣言と評価機関による第三者評価のどちらも実証し、比較する。

実証項目	実証を通じて整理する事項
適合性評価に要する工数 (IoT製品ベンダー)	・ 【自己適合宣言の場合】 ・ ☆1の適合基準案・評価手順案ごとに適合性評価に要する工数を整理する。 ・ セキュリティ要件ごとの適合性評価工数を踏まえ、☆1の適合性評価にかかるベンダー負担コストを推計する。 ・ 【第三者評価の場合】 ・ IoT製品ベンダーが適合性評価を受ける際に要する工数（チェックリストの記入に要する工数、製品の提供に要する工数など）を整理する。
適合性評価に要する工数 (評価機関)	・ それぞれの実証対象製品について、☆1の適合基準案・評価手順案ごとに適合性評価に要する工数を整理する。 ・ セキュリティ要件ごとの適合性評価工数を踏まえ、第三者評価の場合のベンダー負担コスト及び評価機関の利益を推計する。
要求基準案・適合基準案・ 評価手順案の妥当性	・ それぞれの実証対象製品について、☆1の要求基準案・適合基準案・評価手順案の過不足を整理し、妥当性を評価する。
自己適合宣言による 評価の妥当性	・ IoT製品ベンダー自身による自己適合宣言と、評価機関による第三者評価で評価結果や評価コストにどの程度の差異が生じるかを整理する。
適合性評価に求められる 知識・スキル	・ ☆1の適合性評価にあたって、適合性評価実施者に求められる知識・スキルを整理する。 ・ 当該知識・スキルの獲得にあたって必要となる教育内容、実務内容等を整理する。

実証の実施 (3) | 適合性評価に要する工数の整理イメージ

要求基準 (案の例)		☆1適合基準 (案の例)	☆1評価手順 (案の例)	ルーターに関する評価工数	ロボット掃除機に関する評価工数	...
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用される機器において、定義された品質尺度に合ったパスワードが設定される、もしくは利用者によって設定できる。	製品導入時に初期パスワードを使用する場合、英数字からなる8桁以上の固有のパスワードを設定するか、利用者によって当該パスワードに設定ができる。	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。	0.2人時間	0.5人時間	...
	1-2. 製品導入時に固有のパスワードを使用する場合、定義された品質尺度に合ったメカニズムでパスワードが生成される。	- 生成されるパスワードは、容易に推測可能なパスワードではなく、英数字からなる8桁以上のパスワードである。容易に推測可能であるパスワードとは、以下のパスワードを意味する。 ✓ カウンタの増加により自動生成されるパスワード ✓ MACアドレス等の情報と同一もしくは関連したパスワード ✓ 共通した文字列や共通的なパターンを含むパスワード	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。	0.5人時間	0.5人時間	...
	1-3. 各認証メカニズムが、定義された品質尺度を満足する完全性、真正性及びセキュリティ保証である。	認証情報は、TLS1.2以上の安全なチャネルを介して通信する。	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。	0.2人時間	0.5人時間	...
	1-4. 各認証メカニズムについて、技術知識が限られる利用者が認証値を変更するためのメカニズムを提供する。	認証に使用される手段（指紋、パスワード、その他トークン）に関わらず、利用者によって認証値を変更できる。	実機に対する動作試行に基づき、対象製品が適合基準に適合していることを評価する。	0.2人時間	0.5人時間	...
		利用者が認証を変更する方法を、利用者がアクセスできるドキュメントリソースにて明記する。	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。	1.0人時間	0.5人時間	...
...	...	...	...	...	...	...
要求基準 計				●●人時間 (= ●●,000 円)	●●人時間 (= ●●,000 円)	...
...	...	...		...	...	...
合計				●●人時間 (= ●●,000 円)	●●人時間 (= ●●,000 円)	...

自己適合宣言及び第三者評価の両方において、適合基準・評価手順ごとに、評価に要する工数を確認する。
 全体の評価工数を踏まえ、☆1の評価にかかるコスト（自己適合宣言／第三者認証）を推計する。
 推計の結果、過大な金銭的コストがかかる場合は基準案の見直しを行う。

【参考】実証対象製品・評価機関の候補

- 効果的な実証結果を得るために、実証対象製品について、想定脅威、海外制度におけるラベリング取得状況、接続類型等を踏まえ、**ルーター、スマート家電、ネットワークカメラを主な候補**とし、今後、IoT製品ベンダーと調整の上で具体的な製品を選定する。
- これらの製品に対して、**IoT製品ベンダーによる自己適合宣言**のほか、ISO/IEC 17025に基づき認定機関より認定された**JISEC制度の評価機関による第三者評価の実証を行う**。

実証対象製品候補※

製品類型	選定理由
ルーター	- 直接的にインターネットに接続する可能性がある製品であり、脅威の度合いが高い - 現在検討されている米国のラベリング制度において、「一般的かつリスクの高い製品」として位置づけられているとおり、消費者の普及率が高い一方でリスクも高い製品類型である - シンガポールのCLS（Cybersecurity Labelling Scheme）で最もラベル取得数が多い類型であり、適合性評価のニーズが比較的高い - ヤマハ、NEC、バッファロー等、国内ベンダーの市場シェアが高い製品類型である
スマート家電 （ロボット掃除機、 スマートTV等）	- 間接的にインターネットに接続する消費者向けの製品であり、国内ベンダーの市場シェアが比較的高い - シンガポールのCLSで最もラベル取得数が二番目に多い類型であり、適合性評価のニーズが比較的高い
ネットワークカメラ	- 直接的にインターネットに接続する可能性がある製品であり、プライバシーに関わる情報を扱うなど、求められるセキュリティの度合いが相対的に高い - 現在検討されている米国のラベリング制度において、「一般的かつリスクの高い製品」として位置づけられているとおり、消費者の普及率が高い一方でリスクも高い製品類型である - 一方で、国内ベンダーの市場シェアが限定的であり、他の2製品と比較すると優先度はやや低い

自己適合宣言

製品ベンダー自身による対象製品に対する自己適合宣言を実施する。

また、検証事業者による評価を実施する。

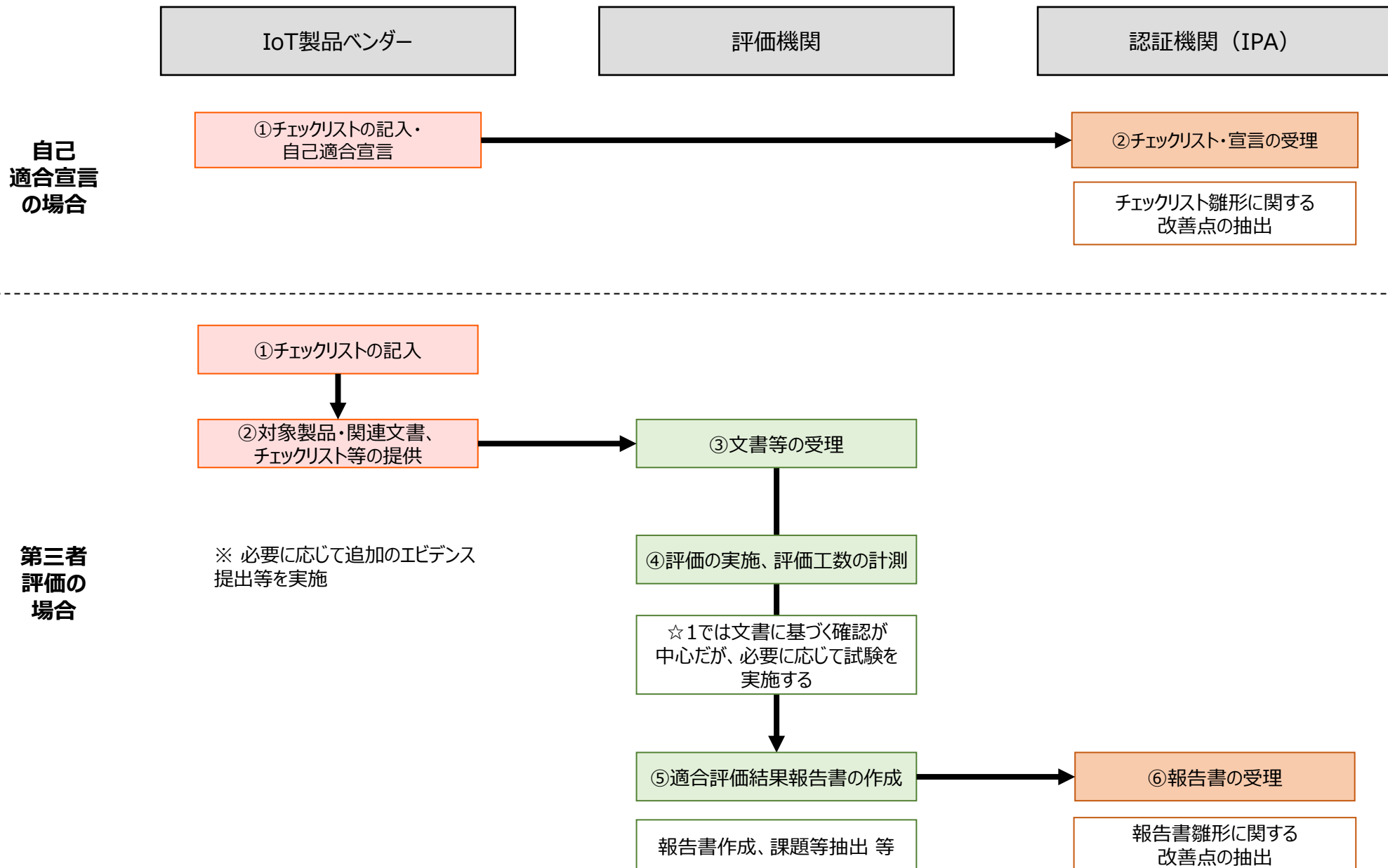
プレ委員会を通じて策定した、☆1の要求基準案・適合基準案・評価手順案案に基づき、適合性評価の実証を行う

評価機関による第三者評価

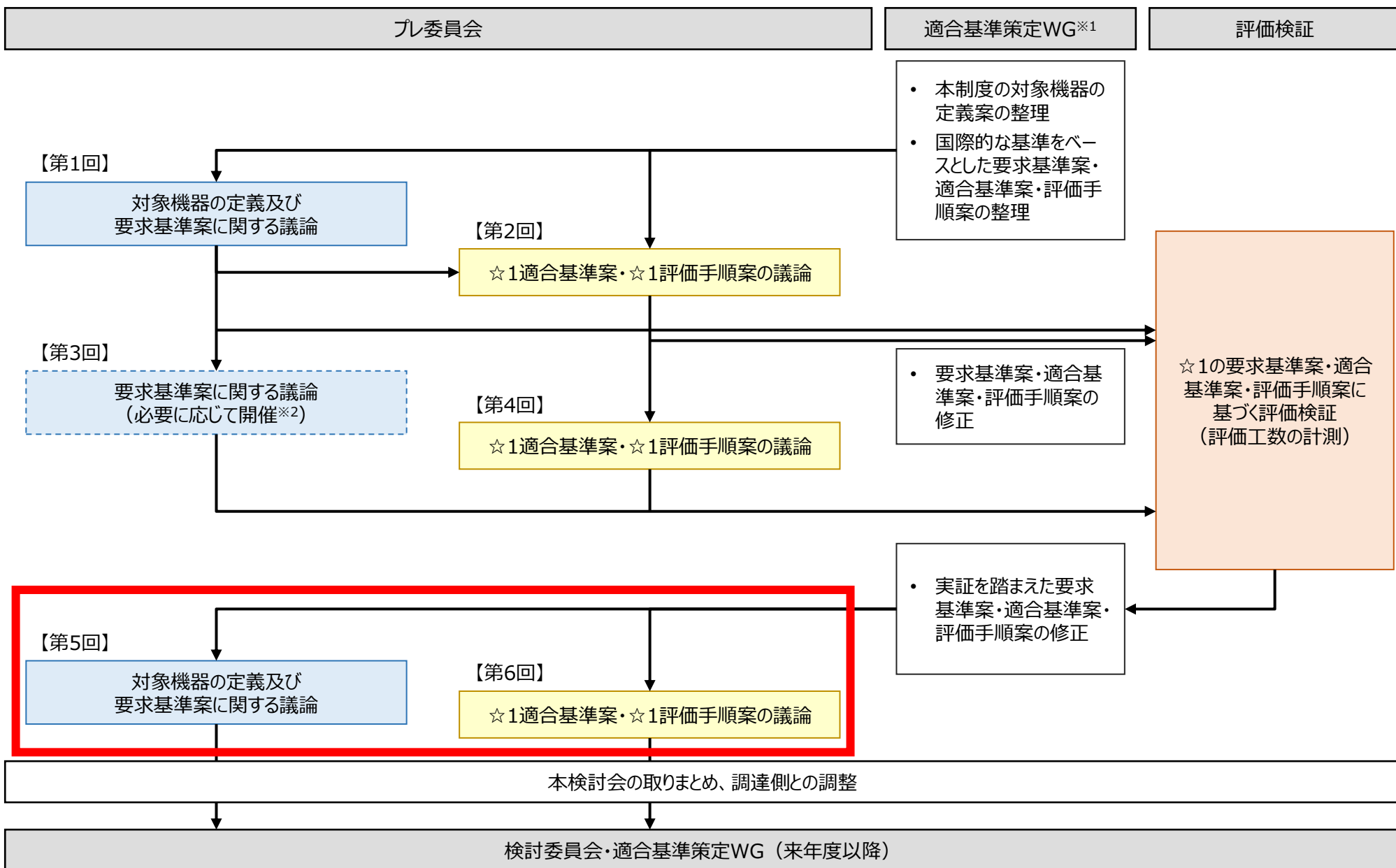
評価機関による第三者評価を実施する。実証では、ISO/IEC 17025に基づき認定されたJISEC制度の国内の評価機関に依頼する。

※ 各製品類型について、どの程度のスペックの製品を実証対象とするか、消費者向け／産業向けのどちらを対象とするか等の詳細については、製品ベンダーや評価機関と調整のうえで決定する。
また、いずれの製品に対して、自己適合宣言による実証を行うか、第三者評価による実証を行うかについても、製品ベンダーや評価機関と調整のうえで決定する。

【参考】評価検証のプロセス



実証結果を踏まえた要求基準案・適合基準案・評価手順案の議論（1）



※1 今年度は事務局が適合基準策定WGの役割を担い、事務局にて、要求基準案・適合基準案・評価手順案の検討・作成を行う。

※2 初回プレ委員会の議論で要求基準案が定まらなかった場合に開催する。

実証結果を踏まえた要求基準案・適合基準案・評価手順案の議論 (2)

要求基準 (案の例)		☆1適合基準 (案の例)	☆1評価手順 (案の例)
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用される機器において、定義された品質尺度に合ったパスワードが設定される、もしくは利用者によって設定できる。	製品導入時に初期パスワードを使用する場合、英数字からなる8桁以上の固有のパスワードを設定するか、利用者によって当該パスワードに設定ができる。	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	1-2. 製品導入時に固有のパスワードを使用する場合、定義された品質尺度に合ったメカニズムでパスワードが生成される。	- 生成されるパスワードは、容易に推測可能なパスワードではなく、英数字からなる8桁以上のパスワードである。容易に推測可能であるパスワードとは、以下のパスワードを意味する。 ✓ カウンタの増加により自動生成されるパスワード ✓ MACアドレスやシリアル番号等、製品識別子の情報と同一もしくは関連したパスワード ✓ 共通した文字列や共通的なパターンを含む	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	1-3. 各認証メカニズムが、定義された品質尺度を満足する完全性、真正性及びセキュリティ保証である。	認証情報は、TLS1.2以上の安全なチャネルを使用する。	製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	1-4. 各認証メカニズムについて、 技術知識が限られる 利用者が認証値を変更するためのメカニズムを提供する。	- 認証に使用される手段（指紋、パスワード、その他トークン）に関わらず、利用者によって認証値を変更できる。 - 利用者が認証を変更する方法を、利用者がアクセスできるドキュメントリソースにて明記する。	- 実機に対する動作試行に基づき、対象製品が適合基準に適合していることを評価する。 - 製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
	実証結果を踏まえ、要求基準案を具体化・追記・修正する	5回連続して認証に失敗した場合、15秒間、アカウントをロックする。 - さらに5回連続して認証に失敗した場合、15分間、アカウントをロックする。 - さらに5回連続して認証に失敗した場合、60分間、アカウントをロックする。	- 実機に対する動作試行に基づき、対象製品が適合基準に適合していることを評価する。 - 製品に関する文書（マニュアルや設計書等）に基づき、対象製品が適合基準に適合していることを評価する。
...	...	(適合基準案として過剰とされる基準は削除する)	...
...	...	...	...

実証結果を踏まえ、適合基準案を具体化・追記・修正する

実証結果を踏まえ、要求基準案を具体化・追記・修正する

各適合基準の評価に要する工数等を踏まえ、☆1の適合基準として過剰と考えられる基準は削除する

各適合基準の評価に要する工数等を踏まえ、過剰な工数がかかる評価手順については、修正又は削除する

実証の結果を踏まえ、要求基準案・適合基準案・評価手順案を修正する。