

原子力エネルギー協議会(ATENA)について

平成31年1月10日

主要原子力施設設置者

(北海道電力等9社、日本原電、日本原燃及び電源開発)

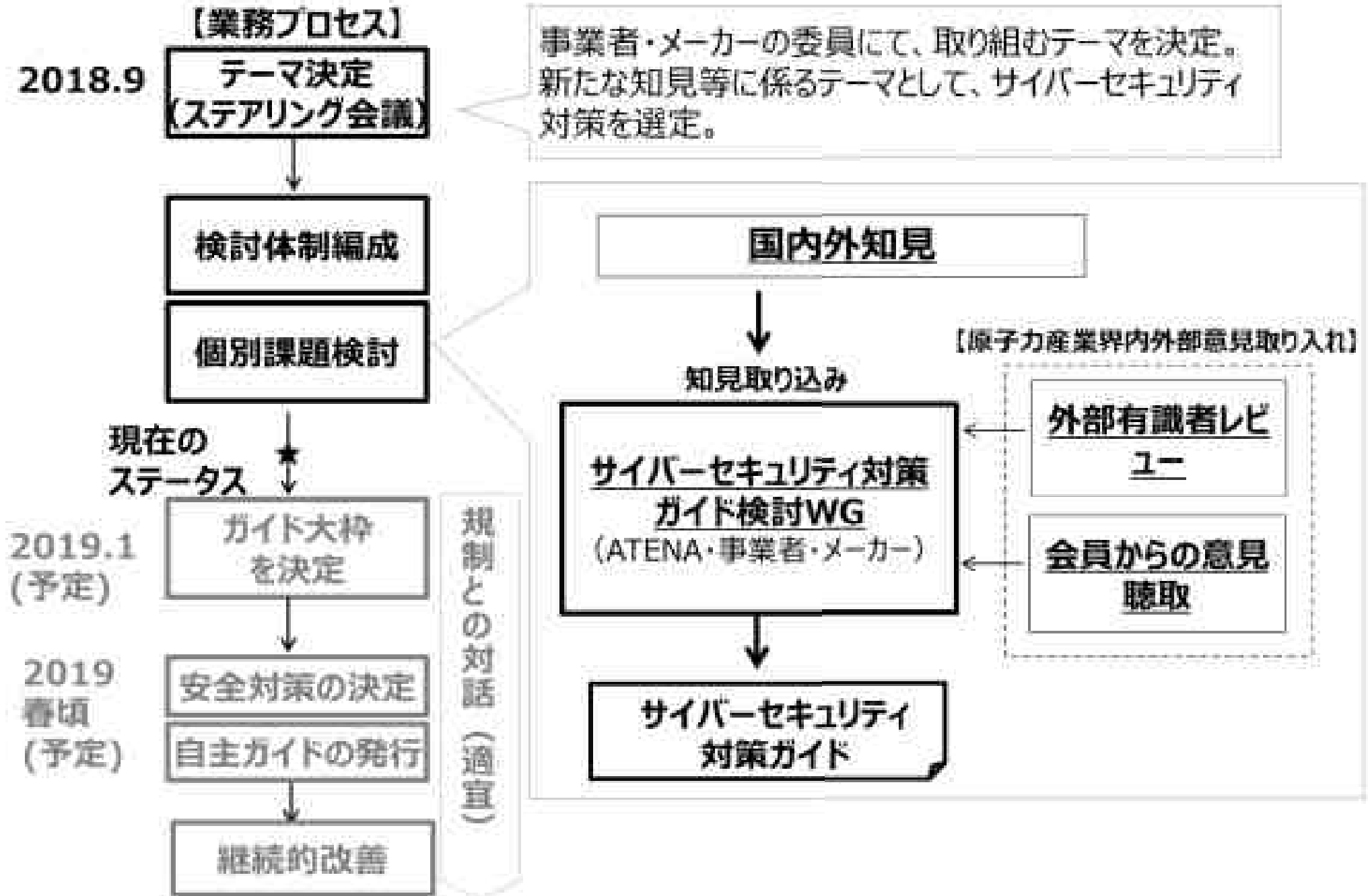
- ATENAは、原子力産業界の共通的な技術課題に、原子力産業界全体で取り組むために、事業者・メーカーで設立した組織。
- ATENAは、原子力発電所の安全性に関する共通的な技術課題を特定するとともに、技術検討を行い、安全対策を立案し、事業者に導入を促す。
- ATENAが立案する安全対策は、事業者の8割以上の投票が得られた場合に決定する。事業者は、ATENAの決定事項にコミットし、自らの事業活動に確実に反映する。
- ATENAには、今後、事業者及びメーカーの代表者として規制当局と対話してもらおう。
また、原子力産業界全体の課題としてATENAが優先的に取り組んでいる課題に限らず、規制当局から原子力産業界へ確認を求める課題についても、ATENAが一元的に取り扱う。
- なお、個社課題への対応については、今後も各事業者の責任にて行う。

ATENAにおいては、以下の技術課題に着目し、取り組むことにより効果的な安全性向上が期待される個別課題をテーマとして取り上げ、それぞれに対し技術検討を行うこととしている。

技術課題	説明	テーマ（例）
①新知見・新技術の積極活用	国内外の新知見や運転経験から個別課題を取り上げ、最も効果的なリスク低減策を検討する	・サイバーセキュリティ対策導入ガイドラインの立案
②外的事象への備え	人為事象を含む外部事象においてさらなる取り組みが必要な事象を検討する	・不確実さの大きい自然現象への対応
③自主的安全向上の取り組みを促進するしくみ	原子力産業界全体の安全性向上のスパイラルアップに繋がれるようなしくみを検討する	・原子力規制検査において活用する安全実績指標（PI）に関するガイドラインの検討

<p>テーマ</p>	<p>サイバーセキュリティ対策導入ガイドラインの立案</p>
<p>概要</p>	<p>欧米原子力業界や国内一般産業界のサイバーセキュリティに関する最新の動向を元に、原子力発電所の安全性に関わる情報システムに対するサイバー攻撃への対応方針をまとめ、自主ガイドを発行する。</p>
<p>検討の必要性</p>	<p>国内原子力発電所のサイバーセキュリティ対策は、情報システムのスタンドアロン運用や外部メディアへのアクセス時のチェックを行っているが、事業者の自主対策として、国内外の最新の動向を踏まえた以下のようなマネジメントシステムや対策系の要件をとりまとめてもらうことが、事業者のセキュリティ対策の更なる向上に資するため、ATENAにて対策系をガイドとしてとりまとめるもの。</p> <ul style="list-style-type: none"> ・サイバーセキュリティマネジメント（必要な組織、責任者、システムや構成図等のインフラ管理、定期レビュー等）の確立 ・セキュリティ要件の定義（多重防護（検知・防護・運用管理・対処）の採用） ・運用管理、異常時対処 等

具体的な対応例(サイバーセキュリティ対策の場合)



- ATENAは、原子力産業界の自律的かつ継続的な安全性向上の取り組みを定着させるため、原子力の安全性に関する共通的な技術課題に原子力産業界全体で取り組む組織として、事業者・メーカーで設立した。
- ATENAにおいては、今後、原子力産業界側で自主で取り組む必要があると判断したテーマ等を対象に、安全対策として、安全性向上に資する自主ガイド等を順次まとめて頂く。
- 我々事業者としては、今後ATENAが決定した安全対策については、自らの事業活動に確実に反映する。
- 規制委員会においても、技術的な論点について、ATENAとの議論をお願いしたい。