内閣府 政策統括官（経済安全保障担当）御中

# 令和７年度経済安全保障に関するリスク分析についての調査

# 調査報告書

令和８年３月

株式会社 NTT データ経営研究所

# 目 次

## 1 諸外国におけるリスク分析に関する比較調査

### 1.1 主要国における国家リスク評価（NRA）のポイント整理

各国の国家リスク評価（National Risk Assessment: NRA）は、自然災害、事故、悪意ある脅威など多様なリスクを対象として実施されているが、その制度設計や評価手法、結果の活用方法は一様ではない。 本調査では、OECD レポート（National Risk Assessments -A CROSS COUNTRY PERSPECTIVE-）において整理された比較観点を参照しつつ、

- A 軸 リスクの分析手法（分析の頻度や手順、評価の考え方、ステークホルダーの巻き込みなど）
- B 軸 分析対象とするリスクの内容

の二点に対応する形で、各国 NRA のポイントを整理した。

本章ではまず、A/B 各軸について、各国制度の差異が現れる主要な観点について、以下に抽出・整理した。

#### 1.1.1 分析手法軸（A 軸）の整理

各国の制度を横断的に確認すると、リスク分析の設計に関して、以下の観点が確認できた。

**A-1 整理単位**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| リスクの整理単位 | 発生要因起点型 | ドイツ、フランス、米国 |
| | 影響起点型 | 英国、フィンランド、オランダ、スウェーデン |

各国の NRA においては、リスクの整理単位に明確な差異が確認された。

一類型は、自然災害、事故、外的脅威等の **発生要因（ハザード／脅威）** を単位として整理する方式である。この方式では、リスク項目は原因別に体系化される傾向がみられる。ドイツおよびフランスに加え、米国においても SNRA におけるハザード／脅威ベースの整理が確認された。

他方、社会機能や重要サービスへの影響を基準とする **影響（社会機能）** を単位として整理する方式も確認された。英国は社会機能への影響を基準とした整理する傾向がみられ、フィンランドおよびオランダにおいても社会機能への影響を基準とした整理が確認された。

**A-2 評価手法**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| 評価手法 | シナリオ前提の定性中心型 | 英国、フィンランド、スウェーデン、米国 |
| | 評価マトリクスを用いた半定量型 | ドイツ、オランダ、フランス |

各国の NRA では、**発生可能性（Likelihood）と影響度（Impact）の二軸**によりリスクを整理する枠組みが広く用いられている。ただし、その評価の具体的手法には差異が見られた。

英国やフィンランドでは、合理的最悪シナリオ（Reasonable Worst Case Scenario）等のシナリオを前提とし、専門家による評価や政府横断のワークショップを通じて発生可能性と影響を整理する方式が採られている。評価結果は段階区分やマトリクスとして整理されるものの、その評価は機械的に算出されるものではなく、シナリオに基づき**専門家の判断に依拠**することが多い。また米国では、同様に**発生可能性と影響の評価を行う枠組み**が用いられているが、**評価は主として脅威・ハザードごとのシナリオ評価として整理**されるとともに、評価結果は能力評価等と組み合わせて運用される。

一方、ドイツやオランダでは、発生可能性や影響度について**事前に設定された評価基準や段階区分に基づきリスク**

**を評価し**、評価マトリクス上で比較する方式が採られている。半定量型とは、厳密な確率計算ではないものの、あらかじめ定められた評価基準とスコアに基づき、複数のリスクを一定の基準で比較可能に整理する方式である。

**A-3 分析プロセス・時間軸**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| 評価射程（Horizon） | 5 年程度の期間に発生する可能性のあるリスクを評価 | 英国、ドイツ、オランダ、スウェーデン |
| | 5 年程度の評価射程に加えて、長期的リスクを別枠で設定 | オランダ |
| | 明示的な評価射程を設定しない | 米国、フィンランド |
| 更新サイクル（Cycle） | 制度的な周期で定期的に更新 | 米国、フィンランド、スウェーデン |
| | 制度的な周期は設定していないが、上位の戦略・政策見直しと連動 | オランダ |
| | 明示的な更新周期なし | 英国、ドイツ |

各国のリスク分析制度を比較すると、**「評価射程（Horizon）」と「更新サイクル（Cycle）」の設計に差異**が確認された。すなわち、一定期間に発生する可能性のあるリスクの評価と、評価を更新する周期は異なる概念であり、各国は制度目的に応じてこれらを異なる形で設定している。

評価射程については、**一定期間に発生する可能性のあるリスク」を評価**する方式（英国、ドイツ、オランダ、スウェーデン）が確認された一方で、長期的なリスクを別枠で整理する方式（オランダ）や、**明示的な射程を設定しない制度**（米国、フィンランド）も把握した。

また、更新サイクルについても、**制度的な周期に基づき定期的に評価を更新**する方式（米国、フィンランド、スウェーデン）や、**戦略・政策の見直しと連動**する方式（オランダ）が見られた一方、**明示的な更新周期を設定せず**状況変化等の随時に更新する制度（英国、ドイツ）も確認された。

**A-4 リスク間関係の扱い**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| リスク間関係の扱い | 単一リスク単位で評価する傾向 | 米国、ドイツ |
| | リスク間の影響を考慮したシナリオ分析がみられる | 英国、フィンランド |

リスク間の関係の扱いにも差異が見られた。

米国やドイツでは、個別のリスクシナリオを単位として評価が行われるのに対し、英国やノルウェーの事例では、社会機能間の依存関係を踏まえた影響の波及や連鎖がシナリオ分析の中で考慮されている。すなわち、リスクを独立した事象として評価するアプローチと、リスク間の関係性を前提に影響の広がりを捉えるアプローチが確認された。

なお、B-4 でも複合リスクに言及するが、A-4 は**分析方法の観点**から、リスク間の関係を分析の中でどのように捉えるかに着目するものである。一方、B-4 は**リスク体系の表現の観点から**、複数のリスクの関係がリスクの整理や提示の中でどのように現れるかに着目するものである。

**A-5 ステークホルダー関与**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| 関与主体・関与構造 | 複数行政による分散入力（連邦・地方の制度的関与） | 米国、ドイツ |
| | 外部主体が制度的に位置付けられ関与（専門家・インフラ事業者等） | 英国、オランダ、フィンランド、スウェーデン |
| 関与するプロセス・役割 | 情報提供・入力を中心とした関与 | 米国、ドイツ |
| | シナリオ作成を中心とした関与 | 英国、フィンランド、スウェーデン |
| | シナリオ作成から分析までを実質的に担う主体としての関与（専門家ネットワーク等） | オランダ |

**リスク分析プロセスへの外部関与**の範囲および関与構造にも差異が確認された。

米国やドイツでは連邦・州レベルの行政主体からの入力を制度的に組み込まれ**分散入力**を行う。また、英国やオランダ、フィンランド、スウェーデンでは、専門家やインフラ事業者などの**外部主体を制度内に位置づけ関与**させる構造が見られた。

このような関与構造の違いに加え、**関与の段階および役割にも差異**が見られた。すなわち、外部主体が**情報提供や入力にとどまる**場合（米国、ドイツ）、**シナリオ作成を中心とした関与**（英国、北欧諸国）、シナリオ作成に留まらず**分析プロセスを実質的に担う主体として関与する**場合（オランダ）など関与する範囲や役割・大きさの違いがあり、この違いは分析に取り込まれる知見の範囲やリスクの把握の仕方に影響を与える。

**A-6 分析結果の制度接続**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| 制度への接続 | 計画の前提・状況認識共有を重視 | 英国、ドイツ、スウェーデン |
| | 政策優先順位付けを重視 | 英国、オランダ、フィンランド |
| | 能力整備・資源配分接続を重視 | 米国 |

**分析結果の活用範囲**にも差異が確認された。

NRA を公開し**社会全体でのリスク認識共有を重視**する制度がある一方、英国やオランダのように分析結果を**政策の優先順位付けや計画の前提**として用いることを重視する制度も存在する。米国では、NRA が国家安全保障戦略などの上位戦略と密接に連動し、**能力整備や資源配分の優先順位付けに直接接続**されることを重視する点が特徴である。

このように、分析結果の制度への接続は、状況認識の共有から政策優先順位付け、さらには能力整備への直接的な反映まで、段階的な違いとして整理することができる。

### 1.1.2 対象リスク軸（B 軸）の整理

ここでは、各国の NRA が「どのようなリスクをどのような構造で対象としているか」について、設計上の差異を整理した。

**B-1 リスクの概念構造**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| リスクの概念構造 | ハザード／脅威をリスクと捉える整理 | ドイツ、米国 |
| | 社会機能への影響をリスクと捉える整理 | 英国、フィンランド、オランダ |

| | | |
|---|---|---|
| | 備えるべき能力とのギャップをリスクと捉える整理 | 米国 |

各国の NRA では、何を「リスク」として捉えるかという概念構造に差異が確認された。

一つは、自然災害や事故、外的脅威などの**ハザード／脅威そのものをリスクとして整理する方式**であり、ドイツや米国に代表される。

これに対し、**社会機能への影響を基準としてリスクを整理する方式**も確認され、英国、フィンランド、オランダなどで採用されている。

米国ではハザード／脅威ベースの整理が採用されている一方、リスク評価は National Preparedness System の中で位置づけられており、**リスクが国家の対応能力に与える影響**という観点が強く意識されている。このため、事**象ベースの整理と能力接続の両側面が併存**する構造が確認された。

**B-2 経済安全保障関連リスクの扱い**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| 経済安全保障関連リスクの扱い | 社会機能のリスクとして整理<br>（例：医療・食料供給・金融サービスの機能停止） | 英国、オランダ、フィンランド、スウェーデン |
| | 個別ハザードのシナリオの影響として扱う<br>（例：サイバー攻撃等のシナリオにおける経済影響） | ドイツ、米国 |

各国の NRA では、**経済安全保障に関連するリスクをどのような形で制度の中に位置づけるか**に差異が確認された。英国やフィンランド等では、社会機能への影響を起点としてリスクが整理されるため、供給網や経済活動に関わるリスクも、医療、食料供給、金融サービス等の社会機能への影響の一部としてその**機能低下がリスク**と整理される。

これに対しドイツでは、ハザード事象ごとのシナリオ分析が中心であり、経済安全保障に関連するリスクは、サイバー攻撃等の**個別ハザードの影響評価の中で扱われる**傾向が見られた。

このように、各国制度においては、経済安全保障関連リスクを独立した分析対象として整理するというよりも、既存の分析枠組の中で定義している点は共通している。その定義単位は、社会機能の低下、あるいはハザード事象の発生といった形で整理される傾向にある。

**B-3 リスク分類の粒度**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| リスク分類の粒度 | 比較可能性を重視し、一定の粒度でリスクを整理 | 英国 |
| | 個別ハザードごとに詳細なシナリオを設定 | ドイツ、米国 |
| | 社会機能単位で比較的粗い粒度で整理 | フィンランド、スウェーデン |

各国の NRA では、**リスクをどの程度の細かさ（粒度）で整理するか**にも差異が確認された。

英国では、Generic Risk と呼ばれる単位でリスクが整理されており、自然災害、事故、サイバー攻撃等の異なる種類のリスクが同一の単位で提示される。一方、ドイツではハザード事象ごとに具体的なシナリオを設定した上で評価が行われるため、分析単位は比較的詳細である。フィンランドでは社会の重要機能への影響を基準としてリスクが整理されており、社会機能単位で比較的粗い粒度で整理されている。

**B-4 複合リスクの扱い**

| 観点 | 確認された差異の例 | 対象国の例 |
|---|---|---|
| 複合的影響の現れ方 | シナリオの中で複数分野に影響につ | 英国、 |

| | | |
|---|---|---|
| | いて取り扱い | |
| | 単一の事象ごとに整理 | ドイツ、米国 |

各国の NRA では、複数のリスクが相互に影響し合う関係についての扱いにも差異が見られた。
多くの制度では、リスクは個別の事象単位で整理されるが、特定の事象が複数分野に影響を及ぼす形でリスクが捉えられる事例も確認された。英国では、単一シナリオの中で複数分野への波及（cascading effects）を評価している点が特徴といえる。
なお、B-4 同様に「複合リスク」に言及する A-4 との違いについては、A-4 の項に記載した。

### 1.2 分析手法および対象リスクの具体的整理

本節では、前節で整理した分析視点に基づき、各国の制度における具体的な記述および運用実態を確認した。

#### 1.2.1 分析手法軸（A 軸）の整理

各国の制度を横断的に確認すると、リスクの整理単位に関しても明確な差異が確認された。本節では、1.1 で整理した観点に基づき、各国における整理単位の具体的な設計を確認した。

**A-1 整理単位**

**（1）基本構造**

各国の NRA は、まず「何を単位としてリスクを整理するか」を定める。OECD レポートでは、各国の整理単位は大きく分けて以下の 2 通りに整理されている。

- **発生要因（ハザード／脅威）起点型**：地震、洪水、テロ等の発生事象そのものを単位とする。
- **影響（社会機能）起点型**：電力供給、医療提供、物流等の社会機能への影響を単位とする。

発生要因（ハザード／脅威）起点型では、リスク項目は原因別に体系化される。ドイツおよびフランスに加え、米国の SNRA においても脅威およびハザードを基礎とした整理が確認された。ただし、米国は、リスク評価は国家の対応能力（Preparedness）との関係の中で位置づけられており、単純なハザード分類にとどまらない構造を有している。
他方、社会機能や重要サービスへの影響を基準とする影響（社会機能）起点型では、社会機能への影響を基準としてリスクが整理される。英国では社会機能への影響を基準とした整理が採用されており、フィンランドおよびオランダにおいても社会機能への影響を基準とした整理が確認された。

以下に、**発生要因起点型**の代表例としてドイツ、**影響起点型**の代表例として英国を取り上げた。

**■発生要因起点型の事例（ドイツ）**

OECD レポートでは、ドイツのリスク分析（Risk Analysis in Civil Protection）は、明確に**ハザード起点**で整理されていることが紹介されている。ドイツでは、

- Flood（洪水）／Pandemic（感染症）／Storm surge（高潮）／Earthquake（地震）

など、**具体的な自然ハザードを単位**として分析が実施され、各ハザードごとに、

- 想定シナリオ／発生規模／地理的範囲／影響対象

が個別に設定される。

**■影響起点型の事例（英国）**

OECD レポートでは、英国の NRA について次のように記述している。

"The assessment identifies generic risks that could have a significant impact on the United Kingdom."

英国では、地震や洪水といった物理的原因そのものではなく、「国家に重大な影響を及ぼす Generic Risk（汎用的リスク）」を整理単位とする。例えば、OECD が紹介する英国のリスクには、

- Coastal flooding／Pandemic influenza／Terrorist attack

が含まれる。これらは発生原因は異なるが、抽象化されたリスク単位として横並びに整理される。

**（2）制度的含意**

このように、各国の NRA ではリスクの整理単位において異なる整理思想が採用されている。発生要因起点型では個別リスクの原因分析が中心となるのに対し、影響起点型では異なる種類のリスクについて社会機能への影響という共通の観点で並べて評価することが可能となる。そのため、例えばパンデミック、サイバー攻撃、大規模洪水といった性質の異なるリスクについて、医療提供体制や物流機能への影響の程度というを同一の基準で比較し、政策上の優先順位付けに活用することが可能となる。したがって、**整理単位の設計はリスク分析の対象範囲や比較の枠組みを規定する重要な制度要素**となる。

**A-2 評価手法**

**（1）基本構造**

各国の NRA では、リスク評価は**発生可能性（Likelihood）と影響度（Impact）の二軸**により整理されることが多い。この枠組み自体は多くの国で共通しているが、その評価の方法や制度設計には差異が見られた。

一般的な評価の構造は、以下の要素から構成される。

- **影響（Impact）の設計**
  人命、経済、社会機能等の観点で評価軸を設定し、段階区分により整理する。
- **発生可能性（Likelihood）の評価**
  絶対確率ではなく、発生頻度のレンジや段階区分による相対評価が用いられることが多い。
- **可視化（Risk Matrix）**
  Impact × Likelihood の二軸マトリクス上に配置し、リスクの相対的位置関係として提示する。

ただし、この枠組みを **どのように適用し、結果をどのように整理するか**には制度設計上の違いが見られた。以下に、定性中心型の代表例として英国、半定量型の代表例としてドイツを取り上げた。

**■定性中心型の事例（英国）**

OECD レポートでは、英国の影響評価について次のように整理されている。

"an assessment of the impact of these risks is carried out via cross-government workshops, including predefined scoring scales…"

英国では、政府横断のワークショップ等を通じて専門家が評価を行い、影響および発生可能性を整理する方式が採用されている。

影響項目には以下が含まれる（OECD Table 24.1）。

- Human impact（死亡・負傷）／Economic impact／Disruption of essential services／

Psychological impact

評価は段階区分により整理されるが、評価基準に基づく機械的な算定ではなく、ワークショップ等における**専門家判断を踏まえて評価区分に割り当てる形で行われる**点に特徴がある。評価結果は **National Risk Matrix** として提示され、Impact × Likelihood のマトリクス上でリスクの相対的位置関係が示される。

**■半定量型の事例（ドイツ）**

これに対し、ドイツのリスク分析（Risk Analysis in Civil Protection）では、影響および発生可能性について**事前に設定された評価基準**に基づき整理が行われる。

各ハザードシナリオについて、

- 想定される影響の規模／発生可能性／影響対象

などを評価基準に基づき段階区分で整理し、それらをマトリクス上で比較する。

この方式では、厳密な確率計算を行うわけではないものの、評価基準と段階区分を制度として明示し、複数のリスクを**一定の基準で比較可能な形で整理する**点に特徴がある。

**（2）構造的含意**

以上のとおり、各国の NRA における差異は **Likelihood × Impact の枠組みそのものではなく、その評価処理の運用方法に現れる**といえる。すなわち、枠組みは共通していても、評価基準を参照しつつ専門家判断により区分へ割り当てる方式と、評価基準やスコアリングを制度的に明確化する方式といった運用上の違いがみられる。

### A-3 分析プロセス・時間軸

**（1）基本構造**

各国の NRA では、リスク評価の時間軸設計に関して、「評価射程（Horizon）」と「更新サイクル（Cycle）」の関係に明確な差異が確認された。**評価射程とは、リスクをどの程度先まで見通して評価するかという時間的範囲**のことであり、**更新サイクルとは、制度としてリスク評価を見直す周期**を意味する。

多くの国において、この両者は必ずしも一致しておらず、制度目的に応じて異なる形で組み合わせて設計されている。

評価射程について、英国やドイツでは一定期間内の発生可能性を評価する方式が採られている。英国では、合理的最悪シナリオ（Reasonable Worst Case Scenario）を前提に、**悪意あるリスクは約 2 年、非悪意リスクは約 5 年の期間を対象として評価**が行われる。ドイツにおいては、発生可能性（plausibility）は**今後 5〜10 年の期間を前提**として、統計データおよび専門家判断に基づき区分される。

一方、オランダでは**通常のリスク評価を約 5 年の期間で実施しつつ、潜在的な脅威については 10〜20 年の長期的視点で別途整理**するなど、時間軸を分離した設計が採られている。これに対し、米国やフィンランド、スウェーデンでは、**評価射程を明示的に設定せず、制度運用上の枠組みの中で評価**が実施される。

更新サイクルについては、米国、フィンランドおよびスウェーデンにおいて**制度的な周期に基づく定期更新**が確認される。米国では、THIRA および SPR を通じて**概ね 3 年を単位として評価および能力の見直し**が行われる。フィンランドにおいても、**EU の報告義務に基づき概ね 3 年ごとにリスク評価が実施**される。

他方、オランダでは**明示的な更新周期は設定されていない**ものの、**国家安全保障戦略等の見直しと連動して評価が更新**される。英国やドイツにおいては、**明示的な更新サイクルを制度として固定していない**点が特徴といえる。

| 国名 | 評価射程 | 更新サイクル | 設定の論理 |
|---|---|---|---|
| US | 明示なし | 3 年 | THIRA/SPR により 3 年ごとにリスク評価と能力評価を更新し、能 |

| | | | |
|---|---|---|---|
| | | | 力の変化把握と目標（Capability Targets）の見直しを行う。評価射程は明示せず、制度的な更新周期で運用。 |
| UK | 2 年／5 年 | 明示なし（随時更新） | 合理的最悪シナリオを前提に、悪意あるリスクは 2 年、非悪意リスクは 5 年の評価期間を設定し、その期間内の発生可能性を評価。 |
| ドイツ | 5～10 年 | 明示なし | 発生可能性（plausibility）は今後 5～10 年の期間を前提に、統計的頻度を参照しつつ専門家判断で区分。 |
| オランダ | 5 年／長期 10–20 年 | 明示なし（戦略更新と連動） | 通常シナリオは約 5 年を対象としつつ、潜在的脅威は 10～20 年の長期枠で別途整理し、時間軸を分けて評価。 |
| フィンランド | 明示なし | 3 年（EU 義務） | EU の報告義務に基づき 3 年ごとにリスク評価を実施し、備え（preparedness）の見直しに接続。評価射程は明示せず。 |
| スウェーデン | 5 年 | 2 年 | 各機関は継続的にリスク・脆弱性の分析を実施するとともに、少なくとも 2 年ごとにその結果をリスク・脆弱性分析（RSA）として取りまとめ、政府に報告する。国家リスク評価（NRSB）は約 5 年の中期的視点で実施される。 |

**（2）制度的含意**

以上のとおり、各国の NRA における差異は、評価射程および更新サイクルのいずれか一方にあるのではなく、両者をどのように組み合わせて制度設計しているかに現れるといえる。すなわち、評価射程とは独立に**更新サイクルを設定**する方式や、**評価射程と更新サイクルを対応させて運用**する方式、さらに**短期と長期の評価射程を併用**する方式などが確認された。

このような時間軸設計の違いは、制度目的の違いを反映したものであるだろう。すなわち、リスクを横断的に比較し優先順位付けに用いる場合には、一定の評価射程を設定した上で複数のリスクを同一の時間枠で評価する設計が採られることが多い。一方、能力整備や備えの管理に接続する場合には、制度としての更新サイクルに合わせて評価を実施し、定期的な見直しを前提とする設計が採られることが多い。また、不確実性の高いリスクに対応する観点から、短期と長期の評価射程を分けて設定する方式も見られる。

**A-4 リスク間関係の扱い**

**（1）基本構造**

各国の NRA では、個別のリスクを評価するだけでなく、リスク同士の関係にも着目した分析が行われており、**複数分野への影響の波及や相互依存関係が考慮**される傾向が見られた。

従来型のリスク分析では、自然災害や事故等のリスクを**単一の事象単位**で評価する方法が一般的であり、各リスクは基本的に独立した分析対象として扱われる。

これに対し、近年の NRA では、複数のリスクが相互に影響し合う構造を前提とし、

- 複数のリスクが時間的・因果的に連鎖する**複合リスク（compound risk）**
- 社会機能やインフラの相互依存を通じて影響が拡大する**システム的リスク（systemic risk）**

といったリスク間関係をシナリオの中に組み込む形で分析するアプローチが見られた。

このように、NRA におけるリスク分析は、個別のリスク単位での評価を基本としつつ、その影響の評価の中で他分野へ

の波及や相互依存関係を考慮する形で発展しているとみることができるだろう。

**■リスク連鎖分析の事例（英国）**

英国の National Risk Assessment では、個別のリスクシナリオを評価するだけでなく、**社会機能間の相互依存関係を踏まえた影響拡大**が分析の中で考慮されている。

OECD レポートでは、英国のリスク分析について次のように整理されている。

"Risks are assessed in terms of their impacts on people, the economy and the environment, including **the potential for cascading effects** across systems."

このように英国の NRA では、リスクを単独の事象として評価するだけでなく、社会システム内での波及や連鎖（cascading effects）を考慮した分析が行われている。

**■システム的リスク分析の事例（ノルウェー）**

ノルウェーの国家リスク分析（National Risk Analysis）では、**社会機能間の相互依存を前提としたシナリオ分析**が行われている。例えば、**異常気象により広域的な停電が発生した場合、電力供給の停止が通信、交通、医療等の重要サービスに波及し、社会機能全体に影響が拡大する可能性が想定**されている。このようにノルウェーの NRA では、単一の事象による直接的影響だけでなく、重要インフラ間の依存関係を通じた**影響連鎖（cascading effects）**が分析の中で扱われている。

**■複合リスク分析の事例（フィンランド）**

フィンランドの国家リスク評価においても、**社会機能の相互依存性を前提とした分析**が行われている。例えば、サイバー攻撃や電力障害等が発生した場合に、**通信、金融、物流など複数の社会機能に影響が波及する可能性**が想定されている。フィンランドの分析では、このような複数の事象の連鎖や同時発生を前提とした**複合リスク（compound risk）**が分析対象として取り入れられている。

### （2）制度的含意

以上のとおり、各国の NRA では、単一の事象を個別に評価する分析を基本としつつ、その影響評価の中でリスク間の相互作用や影響連鎖を考慮する形で分析が発展している。この結果、評価の対象は**個別の事象そのものに留まらず、社会システム全体の脆弱性や依存構造にも及ぶ**。

## A-5 ステークホルダー関与

### （1）基本構造

各国の NRA では、リスク分析に対するステークホルダーの関与の在り方について、関与主体の構造と関与の段階の双方に差異が見られ、それによって分析の性格そのものに影響を与えていると考えられる。

例えば、米国やドイツでは、連邦・州レベルの行政主体からの情報入力を制度的に組み込むことで、広範な情報収集を前提とした分析が行われるようである。一方、英国では中央政府が分析を統括しつつ、専門家等がシナリオ作成に参加することで、分析過程における判断の質を高める設計が採られているとみられる。また、オランダでは専門家やインフラ事業者が継続的に関与することで、特定分野の実務的知見が分析に反映されやすい構造といえるだろう。

このように、関与のあり方は、情報の収集範囲、分析過程への関与の程度、知見の専門性といった側面において異なる影響を持つといえる。

以下に、分散入力型の代表例として米国およびドイツ、外部制度化型の代表例としてオランダおよびスイスを取り上

げる。

**複数行政が分散入力を行う事例（米国・ドイツ）**

米国およびドイツでは、リスク分析に複数の行政主体が制度的に関与する**分散入力型の構造**が採用されている。中央政府が分析の枠組みを設計する点は共通するが、実際のリスク情報や評価には**州政府や関係機関からの入力**が組み込まれる。

米国では、国土安全保障省（DHS）が中心となり **Strategic National Risk Assessment（SNRA）** が実施される。分析には連邦政府機関に加え、州政府や専門家の知見が反映される。

> "The Strategic National Risk Assessment draws on expertise from across the federal government and other partners."

このように、米国の制度では連邦政府が分析を統括しつつ、**複数の行政主体の知見を接続する形でリスク評価**が行われる。

ドイツの **Risk Analysis in Civil Protection** でも同様に、連邦政府が分析枠組みを設計しつつ、州政府や専門機関の知見を踏まえて分析が実施される。ドイツは連邦制国家であり、**危機管理の多くの権限が州に属する**ため、リスク分析においても複数の行政主体の関与が制度的に前提とされている。

**外部主体が制度的に位置付けられる事例（オランダ・スイス）**

オランダやスイスでは、政府機関に加え、重要インフラ事業者や専門家などの**外部主体を制度内に位置づける**外部制度化型の構造が確認される。

オランダの **National Risk Assessment** では、政府機関だけでなく、重要インフラ事業者や専門家がリスク評価のプロセスに参加する。OECD レポートでは次のように整理されている。

> "Experts from government, academia and the private sector participate in the assessment process."

この制度では、政府が分析枠組みを設計しつつ、民間事業者や専門家の知見を制度的に組み込みながらリスク評価が行われる。

スイスのリスク分析でも、政府機関に加えてインフラ事業者や専門家が関与する形で分析が実施される。特に重要インフラ分野では民間主体の役割が大きいため、分析プロセスに外部主体を制度的に組み込む構造が採用されている。

### （2）構造的含意

ステークホルダー関与の設計は、リスク分析に取り込まれる情報の範囲と性質を規定し、結果として**何がリスクとして認識されるかに影響**を与える。行政主体からの入力を中心とする制度では、制度的に把握可能なリスクや政策判断に直結するリスクが中心となる傾向があるのに対し、外部の専門家やインフラ事業者が関与する制度では、社会システムの依存関係や運用上の脆弱性といった、現場に根差したリスクが分析に現れやすくなるといえる。

したがって、ステークホルダー関与は単なる体制上の違いではなく、**リスクの把握範囲や整理のされ方を規定**する分析設計上の重要な要素であるといえるだろう。

## A-6 分析結果の制度接続

### （1）基本構造

OECD レポートでは、制度接続の方向として次の類型が確認された。

- **計画の前提・状況認識共有を重視**：危機対応計画やレジリエンス計画の共通の前提条件として使用する。
- **政策優先順位付けを重視**：リスク評価結果を分野横断的に比較し、重点的に対応すべきリスクを選定する。
- **能力整備・資源配分接続を重視**：必要な対応能力（Capability）の特定やギャップ分析と直接結び付ける。

以下に、英国および米国の事例を通じて、制度接続の違いを確認した。なお、各国の制度は必ずしも単一の類型に対応するものではなく、複数の接続の仕方を併せ持ちながら、その中でどの機能を重視するかに違いが見られた。

**■ 計画の前提・状況認識共有／政策優先順位付けを重視の具体的事例（英国）**

OECD レポートでは、英国の NRA について次のように整理されている。

“The National Risk Assessment underpins emergency planning and preparedness activity across government.”

評価結果は National Resilience Planning Assumptions として整理され、**政府全体の計画策定の共通前提**として用いられる。また、リスクマトリクスによりリスクの相対的な位置関係が可視化されることで、政策対応の重点領域を示す機能も併せ持っている。

**■ 能力整備接続型の具体的事例（米国）**

OECD レポートでは、米国では、THIRA/SPR プロセスを通じて、**リスク評価、必要能力の特定、能力ギャップ分析が一体的に設計**されていること、評価結果は**直接的に能力整備や予算優先順位に接続**されることが指摘されている。

**（2）制度的含意**

このように、分析結果の制度接続は、状況認識の共有、政策対応の優先順位付け、能力整備への接続といった複数の機能を持ちうるが、各国制度ではその中でどの機能に重心を置くかに違いが見られる。すなわち、計画の前提としての活用を重視する制度、リスクの相対的な位置付けを通じて政策対応の重点を示す制度、能力整備や資源配分に直接接続する制度といった違いとして整理することができるだろう。

### 1.2.2 対象リスク軸（B軸）の整理

各国の NRA が「どのようなリスクをどのような構造で対象としているか」について、設計上の差異が確認された。本節では、1.2 で整理した観点に基づき、各国における整理単位の具体的な設計を確認した。

#### B-1 リスクの概念構造

**（1）基本構造**

各国の NRA では、何をリスクとして捉えるかという概念構造の違いが、その後の分析の進め方や評価の対象範囲に直接的な影響を与えていると考えられる。

例えば、ドイツのようにハザード／脅威をリスクとして捉える場合には、個別事象ごとの発生可能性や影響を積み上げる形で分析が構成される。一方、英国やフィンランド、オランダのように社会機能への影響をリスクとして捉える場合には、異なる事象を同一の影響単位で整理し、分野横断的に把握することが可能となる。また、米国のように能力体系との関係でリスクを捉える場合には、評価結果がそのまま必要能力やギャップの特定に接続される構造となる。

このように、リスクの定義の仕方は、分析の単位、比較の枠組み、さらには評価結果の接続先を規定する基礎的な設計要素として機能しているといえる。

**■発生要因起点型の事例（ドイツ）**

OECD レポートでは、ドイツのリスク分析について次のように整理されている。

"Risk analysis … is an objective-dispassionate inventory of what would have to be reckoned with upon the onset of a hazardous incident in Germany."

ドイツでは、ハザード事象の発生を前提としてリスクを把握する方式が採用されており、自然災害、事故、人為的脅威等の発生事象を基礎として分析が実施されている。

**■影響起点型（Generic risk）の事例（英国）**

OECD レポートでは、英国の NRA について次のように整理されている。

"The assessment identifies generic risks that could have a significant impact on the United Kingdom."

英国では、個別ハザードの分類ではなく、国家に重大な影響を及ぼし得るリスク（Generic risk）を単位として整理している。

**■ハイブリッド型（発生要因＋能力接続）の事例（米国）**

OECD レポートでは、米国の SNRA について次のように整理されている。

"The SNRA evaluates risks in terms of the potential consequences and likelihood of occurrence of hazards."

また、SNRA は National Preparedness System の中で位置づけられている。

米国では発生要因（ハザード／脅威）ベースの整理が採用されている一方、リスク評価は Preparedness 体系の中で位置づけられており、リスクが国家の対応能力に与える影響という観点が強く意識されている。

### （2）構造的含意

リスクの概念構造の違いは、単なる分類の違いではなく、制度として何を分析対象として切り出し、どのように比較・評価するかを規定するといえる。発生要因起点の整理では個別事象ごとの特性や発生メカニズムの把握が可能となる一方で、異なるリスク同士を直接比較することは難しい。これに対し、影響起点の整理では、異なる事象であっても社会機能への影響という共通の観点で並べて把握することが可能となる。また、能力接続型では、リスク評価がそのまま必要能力やギャップの特定に接続されるため、分析結果を直接的に備えや資源配分の検討に結び付けることが可能となる。

したがって、リスクをどの単位で定義するかは、分析手法の違いにとどまらず、比較の可能性や政策への接続の仕方を規定する制度設計上の論点となるだろう。

## B-2 経済安全保障関連リスクの扱い

### （1）基本構造

各国の NRA では、経済安全保障に関連するリスクは独立した項目として整理されるのではなく、既存のリスク枠組の中で位置づけられる。そのため、同一のリスクであっても、制度によって分析対象としての切り出され方が異なる。

例えば、英国やオランダ、フィンランド、スウェーデンでは、供給網や経済活動に関わるリスクは、医療・食料供給・金融

サービスといった社会機能の低下として提示される。一方、ドイツや米国では、個別ハザードのシナリオの中でその影響として扱われる。

**■社会機能のリスクとして整理する事例（英国・フィンランド）**

OECD レポートでは、英国の NRA について次のように整理されている。

"The assessment identifies generic risks that could have a significant impact on the United Kingdom."

英国では、個別ハザードではなく、国家に重大な影響を及ぼし得る **Generic risks** を単位としてリスクが整理されている。このため、**供給網や経済活動に関わるリスクも**、医療、食料供給、金融サービス等の**社会機能への影響の一部**として扱われる。フィンランドの NRA においても、社会の重要機能（vital societal functions）への影響を基準とした整理が採用されている。

**■個別ハザードのシナリオの影響として整理する事例（ドイツ）**

OECD レポートでは、ドイツのリスク分析について次のように説明されている。

"Risk analysis … is an objective-dispassionate inventory of what would have to be reckoned with upon the onset of a hazardous incident in Germany."

ドイツではハザード事象ごとのシナリオ分析が中心となっており、洪水や感染症等の個別ハザードごとに影響評価が実施される。このため、経済安全保障に関連するリスクは独立した政策領域として整理されるというよりも、個別ハザードの影響評価の中で扱われる構造となっている。

### （2）構造的含意

経済安全保障関連リスクの扱いの違いは、当該リスクをどの単位で把握し、どのように比較・評価できるかに影響を与える。社会機能として提示される場合には、異なるリスクを分野横断的に並べて把握することが可能となる一方、個別の機能の内部構造や依存関係の詳細な把握は限定される。これに対し、社会基盤として整理される場合には、インフラ単位での脆弱性や依存関係を具体的に把握することが可能となるが、分野横断的な比較は相対的に難しくなる。また、ハザード影響として扱われる場合には、個別事象ごとの影響の内訳として経済的側面を把握することは可能であるが、経済安全保障リスクとして横断的に位置づけることは難しいといえる。

したがって、経済安全保障関連リスクの扱いの違いは、**リスクの重要性の差ではなく**、どの単位で把握し、どの範囲で比較し、どの政策領域に接続されるかを規定する制度設計上の論点となるだろう。

## B-3 リスク分類の粒度

### （1）基本構造

各国の NRA では、リスクをどの程度の細かさ（粒度）で整理するかにも制度設計上の差異が確認された。例えば、英国では Generic Risk という単位でリスクが整理され、異なる種類のリスクであっても国家レベルで横並びに提示される。一方、ドイツでは洪水や感染症等の個別ハザードごとに具体的なシナリオが設定され、それぞれについて発生可能性と影響が個別に評価される。また、フィンランドやスウェーデンでは、社会機能単位でリスクが整理され、機能ごとの影響として把握される。

このように、リスクの粒度は、比較可能性を重視する整理から、個別事象の詳細分析を重視する整理まで幅を持って設計されているとみられる。

**■比較可能性重視型の事例（英国）**

OECD レポートでは、英国の NRA について次のように説明されている。

"The assessment identifies generic risks that could have a significant impact on the United Kingdom."

英国では、異なる性質のリスクを横断的に比較することを目的として、一定の粒度でリスクが整理されている。個別事象を細分化するというよりも、国家レベルで比較可能な単位として **Generic Risk** が設定され、評価が行われている。

**■詳細シナリオ型の事例（ドイツ）**

OECD レポートでは、ドイツのリスク分析について次のように整理されている。

"Risk analysis … is an objective-dispassionate inventory of what would have to be reckoned with upon the onset of a hazardous incident in Germany."

ドイツでは、ハザード事象ごとに具体的なシナリオを設定した上で評価が行われる。感染症、洪水、停電など、個別ハザードに基づくシナリオが設定され、それぞれについて発生可能性および影響の評価が実施される。

**（2）制度的含意**

この違いは、リスク分析において何を把握できるかと何を比較できるかに直接的な影響を与えると考えられる。粒度を粗く設定し共通単位で整理する場合には、**異なるリスクを横断的に比較し、相対的な重要性を把握**することが可能となる一方、個別事象の具体的な発生過程や影響の内訳を詳細に把握することは難しくなる可能性がある。これに対し、粒度を細かく設定しハザードごとにシナリオ分析を行う場合には、**個別リスクの詳細な影響や発生メカニズムを把握することが可能**となるが、異なるリスク同士を同一の尺度で比較することは難しくなると想定される。また、社会機能単位で整理される場合には、機能ごとの脆弱性や影響の広がりを把握することが可能となるが、個別事象の違いは相対的に抽象化される。

したがって、リスク分類の粒度は、**詳細な分析と横断的な比較のいずれを重視するかという設計上の選択を反映**していると想定され、リスク評価の使い方そのものを規定する制度的な要素といえる。

**B-4 複合リスクの扱い**

**（1）基本構造**

各国の NRA では、複数分野にまたがる影響がどのような形で評価結果の中に現れるかに違いが見られた。

英国の NRA では、単一の事象を評価するだけでなく、その影響が電力、通信、交通等の複数分野に波及する過程がシナリオの中で扱われている。このように、分野間の連鎖的影響を分析の中で扱うことにより、一つのリスクが複数分野にまたがる形で提示される。

これに対し、ドイツや米国では、リスクは主として個別のハザード事象ごとに整理され、それぞれの事象について発生可能性と影響が評価される構造となっている。

**■複合リスク分析の事例（英国）**

英国の NRA では、複数分野にまたがる波及効果を考慮した分析が行われている。

OECD レポートでは次のように説明されている。

"Risks are assessed not only individually but also in terms of cascading impacts across sectors."

電力供給、通信、交通などの社会基盤の相互依存性を踏まえ、一つの事象が他分野へ連鎖する影響が分析の中で扱われている。

**■システムリスク分析の事例（オランダ・ノルウェー）**

オランダおよびノルウェーの NRA では、社会システム全体の安定性に着目した分析が行われており、複数の事象が同時または連続して発生する状況がシナリオとして扱われている。

OECD では、これらの制度について

“interdependencies between critical sectors are explicitly considered”

と整理されている。

### （2）制度的含意

個別事象ごとの評価を基礎としつつ、複数分野への波及をシナリオの中で扱うかどうかの違いは、評価結果において影響の広がりをどの程度明示的に捉えるかに関わるといえる。複数分野への波及を扱う場合には、単一の事象がもたらす影響の広がりや連鎖が一体の現象として提示される一方、個別事象ごとに整理される場合には、影響は各事象の評価の中で把握されるにとどまる。

このように、複合的影響の扱いは、個別事象の評価を基礎としつつ、その影響の広がりをどの程度明示的に取り込むかという設計の違いとして現れるといえる。

## 2 我が国におけるリスク分析手法に関する示唆の抽出

### 2.1 本章の目的と整理の考え方

本章では、第 1 章で整理した各国の国家リスク評価（NRA）の制度設計を踏まえ、我が国のリスク分析手法に対する示唆を抽出した。

各国制度を比較すると、リスク分析は単なる評価手法の違いではなく、①何をリスクとして捉えるか、②どのように分析するか、③分析結果をどのように政策に接続するか、という三つの設計要素の組み合わせとして構成されているといえる。ここでは、この三つの観点から各国制度の設計思想を整理し、我が国の経済安全保障リスク分析に適用可能な考え方を抽出した。

### 2.2 リスク概念の設計に関する示唆

**① 分析単位は、個別ハザードではなく「社会機能への影響」が適切**

経済安全保障リスクは、洪水や感染症のように単一のハザード事象として把握されるというよりも、供給網断絶、技術依存、重要インフラ機能停止、データ流通制約等を通じて、社会システムへの影響として顕在化する場合が多いといえる。したがって、分析単位（A1）は個別ハザードではなく、**社会機能への影響を基準とする整理**が一つの考え方として位置づけられるだろう。

個別ハザードを単位とする整理では、供給網や技術依存のように複数の要因が重なって顕在化するリスクを一体として把握することが難しく、その結果、分野横断的な比較や優先順位付けが難しくなる場合がある。

このため、個別事象は、社会機能への影響をもたらす契機・経路として位置づけつつ、分析の基礎単位をどこに置くかについては、目的に応じて整理することが考えられる。

**② 分析プロセスは、「横断比較」と「重点分析」を分けて設計**

各国の制度を比較すると、リスク分析のプロセス設計においては、**「異なる分野のリスクを比較する機能」と「個別リスクの構造を詳細に理解する機能」**が、必ずしも同一の方法では両立しないことが確認された。

例えば、英国のように社会機能への影響を基準としてリスクを整理する制度では、**異なる分野のリスクを同一の枠組みで比較し、優先順位付けを行うことが可能**となる。他方、このような整理では、**個別リスクの発生構造や依存関係の詳細は簡略化**される。一方、ドイツのようにハザード単位で分析を行う制度では、**個別事象の発生構造や影響の詳細な理解が可能**となるが、**異なる分野のリスクを横断的に比較することは難しく**なる。

このように、リスク分析においては、**「比較可能性」と「構造理解」という二つの機能がトレードオフ**の関係にあるといえる。経済安全保障分野のリスクは、供給網、技術、インフラ、データなど複数分野にまたがるため、分野横断的な比較に基づく優先順位付けが不可欠といえる。一方で、実際の政策対応においては、依存関係や波及経路といった個別リスクの構造を把握しなければ有効な対応は困難と想定される。

このため、これら二つの機能を単一の分析プロセスで同時に満たそうとするのではなく、**分析プロセスを明確に二段階に分けて設計することが有用**ではないだろうか。

すなわち、

・第一段階では、社会機能への影響を基準にリスクを整理し、**分野横断の比較**を行う

・第二段階では、重要性の高いリスクに絞り、**依存関係・波及経路・発生構造を詳細に分析**する

という構造を採ることが適切ではないか。

これにより、国家レベルの優先順位付けに必要な比較可能性と、政策検討に必要な具体性の双方を確保することが期待される。

**③ 評価は、単一リスクの点数化ではなく「比較のための共通軸」として設計**

評価手法（A2）の目的は、精緻な確率評価そのものではなく、**異なる分野のリスクを比較可能な形で整理**し、重点的に分析すべきリスクを選定することにあるだろう。したがって、評価は厳密な数量化を追求するよりも、比較に耐える共通評価軸を設定し、**リスクの相対的な重要性を把握するための手段として設計**することが適切と考えられる。これは、個別リスクごとに精緻な確率評価を行う場合であっても、分野ごとに前提やデータの性質が異なるため、評価結果をそのまま横断的に比較することが難しい場合があるためである。

経済安全保障リスク分析においては、少なくとも以下の観点を共通軸として持つことが妥当ではないか。

- 社会機能への影響の大きさ
- 発生可能性または顕在化蓋然性
- 他分野への波及性・連鎖性
- 政策対応の緊急性・重要性

重要なのは、評価をリスクの精緻な記述の代替とするのではなく、重点分析すべきリスクを絞り込むための装置として位置づけることと考えられる。

**④ 複合リスクは「重点分析の中で扱う」ことを基本としつつ、構造的把握への対応が必要**

経済安全保障分野では、リスクの本質は単一事象そのものよりも、供給網、技術、インフラ、データ等の依存関係を通じた波及構造にある。このため、リスク間関係（A4）は補論として後から付け加えるのではなく、重点分析の中で扱うべき論点である。

各国の制度においても、複合リスクは独立した分析対象として体系的に整理されているわけではなく、**個別リスクのシナリオの中で、社会機能間の波及や連鎖として分析**されている。これは、複合リスクを独立の項目として整理しようとすると、リスクの組合せが過度に増大し、分析の実効性が低下することが理由の一つである。

一方で、近年では、**社会システム全体の相互依存性に着目し、複数分野にまたがる影響を構造的に捉える「システミックリスク（systemic risk）」**の重要性が指摘されている。これは、個別リスクの連鎖として影響を把握するだけでなく、社会システム全体の脆弱性や相互依存構造そのものに着目する考え方であり、シナリオベースの分析の中でも、個別事象の連鎖ではなく、分野間の依存関係や構造的な脆弱性に着目する分析の視点と位置付けることができる。

したがって、経済安全保障リスク分析においては、複合リスクを個別リスクのシナリオの中で波及構造として扱うことを基本としつつ、複数のリスクに共通して現れる分野間の依存関係やボトルネックを横断的に把握する視点を併せて持つことも重要ではないか。

**⑤ 外部主体は「最初から広く入れる」のではなく、段階に応じて関与**

ステークホルダー関与（A5）については、単に「官民連携が重要」で終えるのでは不十分である。論点は、**誰を、どの段階で、何の目的で関与させるか**であるといえる。

各国の制度を比較すると、外部主体の関与は広く見られるものの、その関与の仕方は一様ではない。特に、分析初期の段階から外部主体を広く参加させる場合、知見の多様性は確保される一方で、評価軸や整理単位の設定が困難となり、分野横断的な比較の枠組みが不明確になる傾向がある。他方、外部主体の関与を後段に限定しすぎると、供給網や技術、インフラの実態に関する情報が不足し、リスクの構造把握が不十分となる。

リスク分析プロセスは、一般に①リスクの特定（評価対象の選定）と②リスクの評価（シナリオ分析・影響評価）から構成されると整理できる。このうち、外部主体の関与の在り方は、主として評価プロセスの中でどのように設計するか

が論点となる。
このため、経済安全保障リスク分析においては、外部主体の関与を一律に広げるのではなく、分析プロセスに応じて段階的に設計するという考え方が位置づけられる。具体的には、少なくとも以下のような段階分けが考えられる。
このため、経済安全保障リスク分析においては、外部主体の関与を一律に広げるのではなく、分析プロセスに応じて段階的に設計することも一案である。具体的には、少なくとも以下のような段階分けが考えられる。

- **分析初期（比較段階：リスクの特定・評価枠組みの設定）**
  政府主導により評価軸や整理単位を設定し、分野横断的な比較が可能となる前提を整える
- **重点分析段階（評価段階：シナリオ分析）**
  その上で、重要インフラ事業者、業界関係者、技術専門家等を関与させ、依存関係・脆弱性・波及経路を具体化する
- **妥当性確認段階（評価段階：検証）**
  外部有識者等により、シナリオや評価の妥当性を検証する

このように、比較段階では政府主導により分析の枠組みを安定させ、重点分析段階において外部知見を集中的に投入するという設計も一つの考え方である。これは、英国やオランダにおける実務的な運用にみられる事例である。

### 2.3 リスク分析結果の政策接続に関する示唆

各国制度の比較から確認されるのは、リスク分析制度の実効性は分析の制度そのものではなく、**それが政府の意思決定プロセスにどの程度接続されているか**によって決まるという点である。実務上、リスク分析は調査研究として実施されるものの、政策形成や資源配分の意思決定と接続されない場合には、制度として十分に機能しない可能性がある。
第一に、リスク分析を政策サイクルの中に組み込むことで、**継続的に更新される政策基盤として位置づける**ことが有用であるだろう。英国では国家リスク評価が定期的に更新され、その結果が National Risk Register として公表されることで、政府、地方自治体、重要インフラ事業者等が同一の前提の下で備えを検討する仕組みが構築されている。このように、リスク分析を単発の調査として実施するのではなく、**定期的に更新される政策基盤として制度化すること**が重要である。政策サイクルの中に位置づけられない場合、分析は一度限りの報告書として終わり、政策運用に反映されない可能性がある。
第二に、その分析を支えるために、関係省庁が参加し、リスク評価のインプットを提供する**政府横断の仕組みを構築**することが有用といえるだろう。多くの国では、リスク分析に必要な情報は特定の部局に集約されているわけではなく、各省庁や関係機関に分散している。そのため、英国の NRA では関係省庁が評価ワークショップに参加し、オランダの国家安全保障リスク評価でも関係機関や専門家が分析プロセスに関与する仕組みが設けられている。このように、リスク分析を特定の担当部局のみで実施するのではなく、**関係省庁が評価プロセスに参加し、分析のインプットを提供する仕組み**を設けることで、リスク分析は政府全体の共通認識として機能する可能性がある。また、このような参加プロセスは、関係機関にとって当該リスクへの当事者意識を形成する効果も持つ。
第三に、こうして得られた**分析結果を、政策課題の整理および政策優先順位の検討に接続**することで、意思決定に直接反映させることが有用であるだろう。米国では SNRA が National Preparedness System の中に位置づけられ、THIRA を通じて必要能力の検討や能力ギャップ分析に接続されている。このように、リスク分析は単なる状況整理ではなく、**政府としてどの分野に重点的に対応する必要があるかを検討する政策判断の基礎情報**として制度化されている。分析結果が政策優先順位の検討に接続されない場合、リスク分析は政策形成に影響を与えない独立した分析活動にとどまる可能性がある。
以上を踏まえると、経済安全保障リスク分析制度を実効性のある制度として設計するためには、少なくとも以下の制

度要素を確立することが考えられる。

- リスク分析を政府の政策検討サイクルの中で定期的に実施すること
- 関係省庁が分析プロセスに参加し、リスク評価のインプットを提供する政府横断の仕組みを設けること
- 分析結果を政策課題の整理および政策優先順位の検討に活用すること

すなわち、経済安全保障リスク分析は、単発の調査研究として実施するのではなく、**関係省庁が継続的にインプットを提供し、その結果が政策優先順位の検討に反映される政府横断の政策サイクルとして制度化すること**が考えられる。

## Appendix Ⅰ 各国 NRA の詳細

### 1.1 英国

#### 1.1.1 英国 NRA 制度の概要

英国の NRA 制度は、

- Generic Risk により抽象化されたリスク単位で整理し
- 合理的最悪想定（RWCS）に基づくシナリオ評価を行い
- Likelihood × Impact によりリスクを比較し
- その結果を計画前提および政策優先順位付けに活用する

という構造を有する。

この点において、英国の NRA は、能力整備を直接駆動する制度というよりも、**政府および社会全体におけるリスク認識の共有と計画前提の設定を支える評価プロセス**として位置づけられる。

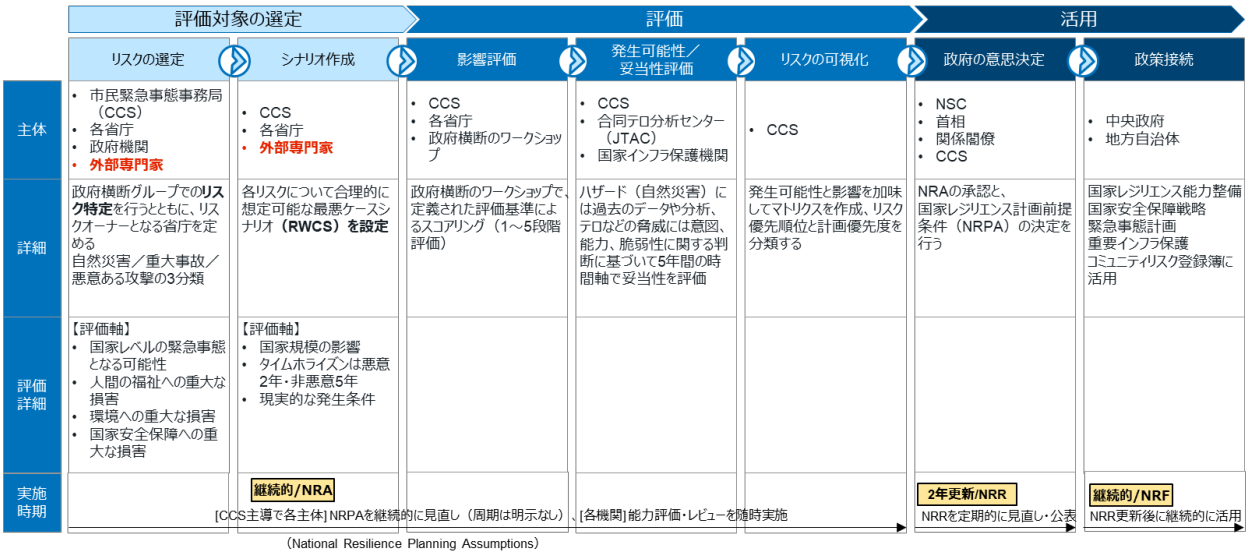
項目別の特徴について、下表に整理した。

| 項目 | 内容 |
|---|---|
| 制度の位置づけ（Positioning） | 英国においては、国家リスク評価（NRA）は**内閣府（Cabinet Office）の Civil Contingencies Secretariat（CCS）が統括**する制度として位置づけられており、政府全体の緊急事態対応計画の基盤となる分析プロセスとして運用されている。<br>NRA は、各政府機関および地方対応機関が計画前提（planning assumptions）を設定するための共通参照点として機能し、その要約版である National Risk Register（NRR）が公表されることで、社会全体でのリスク認識の共有にも活用される。 |
| リスクの範囲・対象（Scope） | 対象は、自然事象、大規模事故、悪意ある攻撃を含むオールハザードであり、国土全体またはその相当部分に重大な影響を及ぼし得る緊急事態が対象とされる。<br>さらに、個別の具体事象ではなく、特定の場所・主体・事象に依存しない「Generic Risk（汎用的リスク）」として整理される点が特徴である。 |
| リスクの概念（Concept） | 英国におけるリスクは、<br>• 発生可能性（Likelihood / plausibility）<br>• 影響（Impact）<br>の組み合わせにより評価される。<br>リスクは、専門家が総合的に判断し、以下を満たすものとして選定される。<br>• 緊急事態に該当すること<br>• 今後 5 年間に発生する可能性があること<br>• 政府の対応・復旧において課題となること<br>また、各リスクは**「合理的最悪想定（Reasonable Worst Case Scenario: RWCS）」に基づき評価**される。これは、極端な最悪ケースではなく、現実的な範囲内で最大の影響を想定するものであり、リスク間の比較可能性を確保する役割を持つ。 |
| 評価手法 | 評価はシナリオベース分析に基づき、Generic Risk ごとに RWCS を設定して |

| | |
|---|---|
| （Methodology） | 実施される。<br>各リスクについて、<br>• 発生可能性（専門家判断＋データ）<br>• 影響（複数の評価基準）<br>を評価し、Likelihood × Impact の二軸マトリクス上で整理される。<br>発生可能性は、自然災害等については統計データと専門家判断の組み合わせにより評価され、悪意ある脅威については、脅威主体の意図・能力および対象の脆弱性を踏まえて評価される。<br>評価結果はリスクマトリクスとして可視化され、リスク間の相対的な優先度の判断に用いられる。 |
| 実施体制（Process & Governance） | NRA は**内閣府（CCS）が中央集中的に統括し、政府各省庁および関係機関が関与する形**で実施される。<br>評価プロセスには、<br>• 政府機関<br>• 学術機関<br>• 外部専門家<br>が関与し、専門家の知見を基礎とした評価が行われる。 また、専門家はシナリオ作成および評価プロセスに直接関与し、政府横断的なワークショップ等を通じてリスク評価が実施される。 |
| 時間軸・更新（Horizon & Cycle） | 評価射程（Horizon）は 5 年間と明示的に設定されている。<br>この時間軸は、<br>• 発生可能性の評価の現実性<br>• 政策・計画への活用可能性<br>の観点から設定されている。<br>一方で、更新サイクル（Cycle）は制度として明確に固定されておらず、状況変化や政策見直しに応じて随時更新される。 |
| 評価結果の活用（Use） | NRA の結果は、主として以下に活用される：<br>• 政府および関係機関における計画前提（planning assumptions）の設定<br>• 緊急事態対応および復旧計画の基礎<br>• リスクの優先順位付け<br>• National Risk Register（NRR）を通じた社会へのリスク情報の共有<br>すなわち、英国の NRA は、能力整備や資源配分に直接接続するというよりも、**政策・計画の前提となるリスク認識の共有および優先順位付けに重点を置いた制度**として機能する。 |

### 1.1.2 英国 NRA の実施フロー

英国におけるリスク評価から能力整備・政策接続に至る一連のフローを整理した。




### 1.1.3 外部専門家等の関与

外部専門家について下表に整理した。

| 項目 | 説明 |
|---|---|
| リスク評価の体制 | • 内閣府市民緊急事態事務局（CCS）が国家リスク評価 および国家レジリエンス計画前提条件（NRPA）の作成を調整する<br>• 国家安全保障会議（NSC）が最終的な評価と計画を承認し、各省庁がそれぞれ「リスク・オーナー」として責任を負う |
| 専門家<br>参加組織 | • 大学<br>• 業界パートナー<br>• 民間セクターの重要インフラ所有者・運営者 等 |
| 専門家<br>専門領域 | • 行動科学／気象学（Met Office）／地質学（BGS）／火山学／大気科学／航空宇宙工学／リスク・証拠コミュニケーション 等 |
| 専門家<br>参加形態 | • エキスパート・チャレンジ・グループ：アカデミックや専門家が、作成された評価に対して異議申し立てや検証を行う<br>• 行動科学専門家グループ：独立したパネルとして CCS に助言を行う<br>• 自然ハザード・パートナーシップ（NHP）：17 の公的機関によるコンソーシアムが、自然災害に関する専門的助言や科学ノートを提供する<br>• SAGE (緊急時科学助言グループ)：大規模事案発生時に、科学的情報を解釈し政府に助言を行う |
| 官側詳細<br>（政府横断 WS・分析チーム等） | • リスク・オーナー省庁：各リスクに特定の省庁が指定され、証拠収集の責任を負う<br>• 政府主席科学顧問（GCSA）ネットワーク：各部門の科学顧問が手法を承認し、評価結果に科学的・技術的証拠が適切に考慮されているかを判断する独立した裁定者の役割を果たす |

### 1.1.4 評価対象とするリスク

英国では National Risk Register（NRR）において対象リスクシナリオが公表されている。以下に NRR 2025 年版におけるリスクシナリオの設定を掲載する。一方、NRR は機密扱いで実施される National Security Risk Assessment の一部を公開したものであり、NRA では**これ以外にも非公開のリスクシナリオ**が設定されている。

## Contents

### 1.2 US

#### 1.2.1 米国 NRA 制度の概要

米国の NRA 制度は、

- ハザード／シナリオ起点でリスクを整理しつつ
- Likelihood × Impact により比較評価を行い
- その結果を Preparedness 体系に組み込み
- 能力整備・資源配分へ直接接続する

という構造を有する。

この点において、米国の NRA は、独立したリスク評価制度というよりも、**国家の備え（Preparedness）を駆動するための統合的な評価プロセス**として位置づけられる。

項目別の特徴について、下表に整理した。

| 項目 | 内容 |
|---|---|
| 制度の位置づけ（Positioning） | 米国においては、単一の国家リスク評価（NRA）文書が独立して存在するのではなく、**Strategic National Risk Assessment（SNRA）を中核とする評価プロセスが、National Preparedness System（NPS）の中に組み込まれた制度構造**として設計されている。<br>SNRA は、国家防災目標（National Preparedness Goal）の策定および中核能力（core capabilities）の特定に資する基盤として位置づけられ、**リスク評価は能力整備・資源配分に接続される前提で運用される**。 |
| リスクの範囲・対象（Scope） | 対象は、テロ、サイバー攻撃、パンデミック、大規模自然災害等を含む**オールハザード**であるが、<br>• 明確な開始と終了を持つイベント<br>• 国土安全保障任務に直接関連する事象<br>に限定される。<br>一方で、<br>• 移民問題等の慢性的社会課題<br>• がんや交通事故等の一般的リスク<br>• 人口動態・経済動向等の構造的トレンド<br>は対象外とされる。 また、一定の閾値（例：1 億ドル超の経済損失）により、**国家レベルのリスクとして扱う範囲が定義される**。 |
| リスクの概念（Concept） | SNRA におけるリスクは、<br>• 発生可能性（Likelihood：年間発生頻度）<br>• 影響（Consequence）<br>の組み合わせとして評価され、加えて不確実性が考慮される。<br>影響は以下の 6 側面で多面的に評価される：<br>• 生命損失<br>• 負傷・疾病<br>• 経済損失<br>• 社会的避難 |

| | |
|---|---|
| | • 心理的影響<br>• 環境影響<br>また制度上は、ハザード評価に加え、**Preparedness（備え）および能力との関係でリスクを捉える構造**が採られている点が特徴である。 |
| 評価手法<br>（Methodology） | 評価は**シナリオベース分析**を基礎として実施される。SNRA では、国家安全保障上重大な影響を与え得るリスクとして **23 の代表的シナリオ**が設定される。<br>各シナリオについて、<br>• 発生可能性（頻度ベース）<br>• 影響（複数指標）<br>を評価し、**Likelihood × Impact による比較**が行われる。 なお、評価は網羅的リストではなく、**継続的に見直される反復的プロセス**として設計されている。 |
| 実施体制（Process & Governance） | SNRA は、**国土安全保障省（DHS）および FEMA を中心に実施**される。<br>その上で、<br>• 連邦政府内の複数機関<br>• 州・地方政府<br>• 部族・準州<br>が関与する**分散入力型（連邦型）プロセス**が採用される。 さらに、国家の preparedness は、政府のみならず民間・非営利・市民を含む“Whole of Community”の共同責任とされ、分析は多層的主体の関与の下で統合される。 |
| 時間軸・更新<br>（Horizon & Cycle） | 評価射程（Horizon）は制度上明示されていない。<br>一方、更新については、PPD-8 に基づき定期的更新が求められ、実務上は**約 2 年程度での見直しが適当**とされている。<br>また、THIRA および SPR 等のプロセスを通じて、能力評価と連動した周期的見直し（概ね数年単位）が行われる。 |
| 評価結果の活用<br>（Use） | SNRA の結果は、主として以下に活用される：<br>• 国家 Preparedness 計画の基盤形成<br>• 中核能力（core capabilities）の特定<br>• 能力投資および資源配分の優先順位付け<br>• 政府横断でのリスク認識の共有<br>すなわち、SNRA は単なる分析ではなく、**能力ベースの計画策定および政策意思決定を支える基盤情報として機能**する。 |
| 制度的特徴（総括） | 米国の NRA 制度は、ハザード／シナリオ起点でリスクを整理しつつ、Likelihood × Impact により比較評価を行い、その結果を Preparedness 体系に組み込み、能力整備・資源配分へ直接接続するという構造を有する。この点において、米国の NRA は、独立したリスク評価制度というよりも、国家の備え（Preparedness）を駆動するための統合的な評価プロセスとして位置づけられる。 |

### 1.2.2 米国 NRA の実施フロー

米国における SNRA を中核としたリスク評価から能力整備・政策接続に至る一連のフローを整理した。


### 1.2.3 外部専門家等の関与

外部専門家について下表に整理した。

| 項目 | 説明 |
|---|---|
| リスク評価の体制 | • 国土安全保障省（DHS）および 連邦緊急事態管理庁（FEMA）が「戦略的国家リスク評価（SNRA）」の開発を主導する<br>• 大統領指令第 8 号（PPD-8）に基づき、連邦政府内の省庁間コミュニティが参加する |
| 専門家<br>参加組織 | • 民間セクター<br>• 非営利セクター<br>• 大学の「センター・オブ・エクセレンス（COE）」等 |
| 専門家<br>専門領域 | • 工学／社会科学／物理科学／公衆衛生／公共政策／インテリジェンス脅威分析／心理的影響／社会的な避難 等 |
| 専門家<br>参加形態 | • **センター・オブ・エクセレンス（START, CREATE）**：テロリズムのリスクや経済分析に関する学術的専門知識を提供する<br>• **民間コントラクター**：モデルの開発、テスト、データ収集、リスク分析の作成を支援する |
| 官側詳細<br>（政府横断WS・分析チーム等） | • **リスク管理分析局（RMA）**：DHS 内で SNRA の主導的な調整を担い、科学的根拠に基づいた分析アプローチをとる<br>• **常設ワーキンググループ**：予防、保護、緩和、対応、復旧の各領域にワーキンググループが存在する<br>• **SNRA ワーキンググループ**：自然災害、技術的/偶発的ハザード、敵対的・人為的脅威に焦点を当てた専門グループがステークホルダーの意見を集約する<br>• **インテリジェンス・コミュニティ**：国家情報長官や司法長官が、テロ関連のインテリジェンス情報を DHS に提供する |

### 1.2.4 評価対象とするリスク

米国では、Threat/Hazard が設定されており、定期的にリスク分析が行われているものの、その内容は 2011 年の Strategic National Risk Assessment（SNRA）以降公開されていない。

**Table 25.1. SNRA National-Level Events**

| Hazard Group | Hazard Type | National-level Event Description |
|---|---|---|
| Natural | Animal Disease Outbreak | An unintentional introduction of the foot-and-mouth disease virus into the domestic livestock population in a U.S. state |
| | Earthquake | An earthquake occurs within the U.S. resulting in direct economic losses greater than $100 Million |
| | Flood | A flood occurs within the U.S. resulting in direct economic losses greater than $100 Million |
| | Human Pandemic Outbreak | A severe outbreak of pandemic influenza with a 25% gross clinical attack rate spreads across the U.S. populace |
| | Hurricane | A tropical storm or hurricane impacts the U.S. resulting in direct economic losses of greater than $100 Million |
| | Space Weather | The sun emits bursts of electromagnetic radiation and energetic particles causing utility outages and damage to infrastructure |
| | Tsunami | A tsunami with a wave of approximately 50 feet impacts the Pacific Coast of the U.S. |
| | Volcanic Eruption | A volcano in the Pacific Northwest erupts impacting the surrounding areas with lava flows and ash and areas east with smoke and ash |
| | Wildfire | A wildfire occurs within the U.S. resulting in direct economic losses greater than $100 Million |
| Technological/ Accidental | Biological Food Contamination | Accidental conditions where introduction of a biological agent (e.g., Salmonella, E. coli, botulinum toxin) into the food supply results in 100 hospitalisations or greater and a multi-state response |
| | Chemical Substance Spill or Release | Accidental conditions where a release of a large volume of a chemical acutely toxic to human beings (a toxic inhalation hazard, or TIH) from a chemical plant, storage facility, or transportation mode results in either one or more offsite fatalities, or one or more fatalities (either on- or offsite) with offsite evacuations/shelter-in-place |
| | Dam Failure | Accidental conditions where dam failure and inundation results in one fatality or greater |
| | Radiological Substance Release | Accidental conditions where reactor core damage causes release of radiation |
| Adversarial/ Human-Caused | Aircraft as a Weapon | A hostile non-state actor(s) crashes a commercial or general aviation aircraft into a physical target within the U.S. |
| | Armed Assault | A hostile non-state actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the U.S. resulting in at least one fatality or injury |
| | Biological Terrorism Attack (non-food) | A hostile non-state actor(s) acquires, weaponised, and releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the U.S. |
| | Chemical/Biological Food Contamination Terrorism Attack | A hostile non-state actor(s) acquires, weaponized, and disperses a biological or chemical agent into food supplies within the U.S. supply chain |
| | Chemical Terrorism Attack (non-food) | A hostile non-state actor(s) acquires, weaponised, and releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure |
| | Cyber Attack against Data | A cyber-attack which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes resulting in economic losses of a Billion dollars or greater |
| | Cyber Attack against Physical Infrastructure | An incident in which a cyber-attack is used as a vector to achieve effects which are —beyond the computer‖ (i.e., kinetic or other effects) resulting in one fatality or greater or economic losses of $100 Million or greater |
| | Explosives Terrorism Attack | A hostile non-state actor(s) deploys a man-portable improvised explosive device (IED), Vehicle-borne IED, or Vessel IED in the U.S. against a concentration of people, and/or structures such as critical commercial or government facilities, transportation targets, or critical infrastructure sites, etc., resulting in at least one fatality or injury |
| | Nuclear Terrorism Attack | A hostile non-state actor(s) acquires an improvised nuclear weapon through manufacture from fissile material, purchase, or theft and detonates it within a major U.S. population centre |
| | Radiological Terrorism Attack | A hostile non-state actor(s) acquires radiological materials and disperses them through explosive or other means (e.g.,, a radiological dispersal device or RDD) or creates a radiation exposure device (RED) |

*Source:* The Strategic National Risk Assessment in Support of PPD 8 (2011): A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation.

### 1.3 ドイツ

#### 1.3.1 ドイツ NRA 制度の概要

ドイツの NRA 制度は、

- ハザード起点でリスクを整理し
- 参照地域を明示した具体的シナリオを設定し
- 発生可能性と影響を段階的に評価し
- リスクマトリクスにより可視化し
- その結果を連邦レベルの政策判断および州・地方を含む統合的な市民保護計画に接続する

という構造を有する。

この点において、ドイツの NRA は、英国のような抽象化された汎用リスク比較とも、米国のような能力整備・資源配分への直接接続とも異なり、**ハザードごとの具体的シナリオ分析を基礎として、連邦国家全体の市民保護と政策判断を支える制度**として位置づけられる。

項目別の特徴について、下表に整理した。

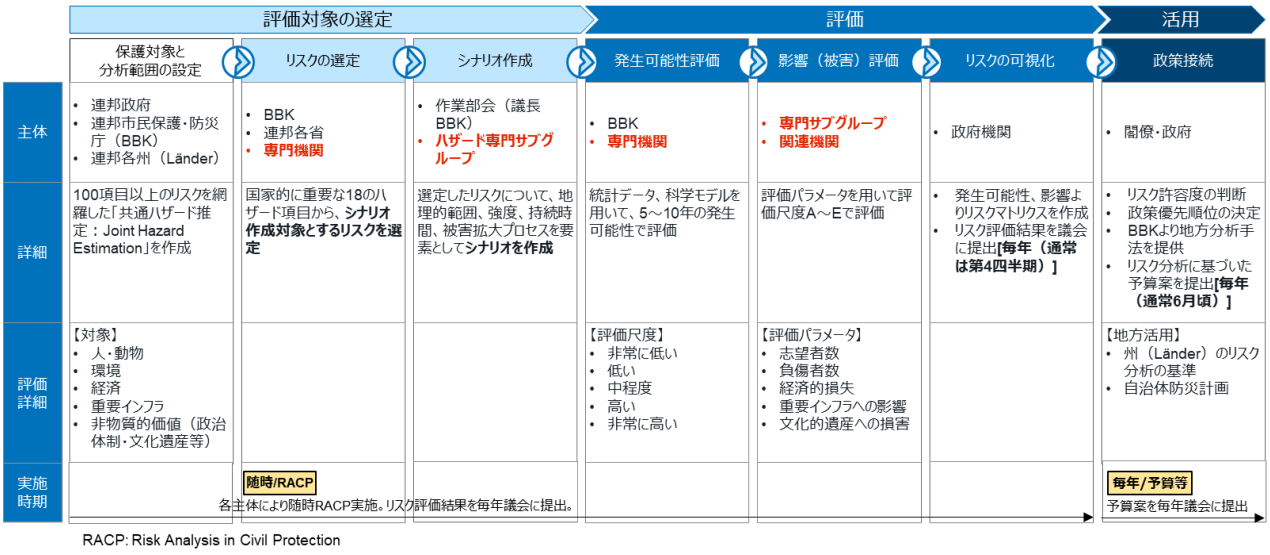
| 項目 | 内容 |
|---|---|
| 制度の位置づけ<br>（Positioning） | ドイツにおいては、国家リスク評価は**市民保護（civil protection）のための連邦レベルのリスク評価プロセス**の中に位置づけられており、連邦レベルの政策判断および州・地方自治体レベルのリスク分析に情報を提供する制度として設計されている。<br>その目的は、政府の憲法上および法律上の責任に従い、**連邦レベルのリスク評価および政策決定に資するリスク分析を提供すること**、あわせて、ドイツにおける相互接続されたリスク評価システムの一部として、州および地方自治体レベルのリスク分析に情報を提供することにある。 |
| リスクの範囲・対象<br>（Scope） | 対象は、**自然的、技術的、人為的ハザードを含むオールハザード**であり、**連邦全体に影響を及ぼし得る主要ハザード・事象**が評価対象とされる。<br>また、ドイツのリスク分析は、ハザード事象の発生を前提として、その際に何が想定されるかを整理する**客観的分析**として位置づけられている。加えて、分析に当たっては「参照地域（reference area）」を設定することが重視されており、ドイツ連邦共和国、州、行政区、農村地域、コミュニティ等の地理的範囲を定めた上で、当該地域にハザードが生じた場合の影響が評価される。<br>保護対象としては、**人・動物、経済・環境、重要インフラ・施設、政治システムや文化遺産等の非物質的対象**を含む国家的価値が念頭に置かれている。 |
| リスクの概念<br>（Concept） | ドイツでは、リスク概念が独立した理論枠組として整理されているというより、**ハザードシナリオに基づく分析手順の中で、発生可能性と影響を評価する構造**として位置づけられている。すなわち、リスクは、ハザード事象の発生を前提に、<br>• 発生可能性（Likelihood）<br>• 影響（Impact）<br>を評価することで把握される。<br>また、影響は、基本法上の保護対象とされる国家的価値への影響という観点から捉えられており、分析対象に含めるか除外するかは、**合理的に想定される最悪** |

| | |
|---|---|
| | **のシナリオにおいて国益にどのような影響を及ぼすか**を基準として判断される。この点で、ドイツの NRA は、**ハザード起点でリスクを把握し、その結果を保護対象への影響として整理する構造**を有している。 |
| 評価手法<br>（Methodology） | 評価は、**ハザード事象に基づく構造化された分析手順**として実施される。<br>作業プロセスは、<br>1．参照地域の記述<br>2．ハザードの選定とシナリオの記述<br>3．発生可能性の評価<br>4．影響の評価<br>5．リスクの可視化<br>という段階で構成される。<br>発生可能性は、1（非常に可能性が低い）から 5（非常に可能性が高い）までの **5 段階スケール**で評価され、対応する統計的発生可能性が割り当てられる。また、ハザードごとのワーキンググループが**合理的な最悪シナリオ**を設定し、10 年に 1 回以上発生し得る事象を「非常に可能性が高い」、10,000 年以上に 1 回程度の事象を最も低い可能性水準として扱う。<br>このように、ドイツの NRA は、ハザードごとの具体的シナリオを前提に、**Likelihood × Impact によって比較可能な形でリスクを可視化する評価手法**として設計されている。 |
| 実施体制（Process & Governance） | ドイツでは、国家リスク評価は**連邦レベルで中央調整**されつつ、州・地方レベルと接続された制度として運用されている。<br>また、比較整理上は、関与構造として分散入力型（連邦・地方の制度的関与）に位置づけられている。加えて、外部主体の関与は、シナリオ作成の中核参加というよりも、**情報提供・入力を中心とした関与**として整理されており、専門機関等が分科会・ワーキンググループを通じて参加する構造が確認される。<br>連邦内務省は、最新のリスク分析結果および関連動向を**毎年連邦議会に報告**しており、報告書は公表・公開される。 |
| 時間軸・更新<br>（Horizon & Cycle） | 評価射程（Horizon）については、ドイツでは **5～10 年の期間を前提に発生可能性を評価する構造**として整理されている。<br>具体的には、発生可能性は対数スケールに基づき評価され、10 年に 1 回以上の事象から、10,000 年以上に 1 回程度の事象までを範囲として扱う。<br>一方で、更新サイクル（Cycle）は制度として明示的に固定されておらず、比較整理上も**明示的な更新周期なし**とされている。ただし、連邦内務省による議会への年次報告という形で、最新の分析結果と動向が継続的に共有される制度運用が確認される。 |
| 評価結果の活用<br>（Use） | ドイツの NRA 結果は、主として以下に活用される。<br>• 連邦レベルのリスク評価および政策判断への情報提供<br>• 州・地方自治体レベルのリスク分析への接続<br>• リスク管理、緊急時計画、危機管理における判断基盤 |

| | |
|---|---|
| | • リスク低減措置の優先順位付け<br>• 不可避の事象への備えと対処の準備<br>• 議会報告を通じた戦略的意思決定支援<br>すなわち、ドイツの NRA は、能力整備・資源配分へ直接つなぐ制度というよりも、**連邦・州・地方を接続するリスク分析基盤として、政策判断と危機管理計画に情報を提供する制度**として機能している。 |

### 1.3.2 ドイツ NRA の実施フロー

ドイツにおけるリスク評価から能力整備・政策接続に至る一連のフローを整理した。




RACP: Risk Analysis in Civil Protection

### 1.3.3 外部専門家等の関与

外部専門家について下表に整理した。

| 項目 | 説明 |
|---|---|
| リスク評価の体制 | • 連邦市民保護・防災庁（BBK）が、連邦政府および州（Länder）と協力して全国的なリスク分析を編纂する<br>• 連邦と州の共同責任として、2006 年から「共通ハザード推定」を基盤に実施されている |
| 専門家<br>参加組織 | • 民間の重要インフラ運営者<br>• 民間救助団体（赤十字、ヨハニター等）<br>• 保険業界<br>• 科学<br>• 学術機関 等 |
| 専門家<br>専門領域 | • 気象（DWD）／環境／経済／統計／地質学（BGR）等 |
| 専門家<br>参加形態 | • **ラウンドテーブル（Round Table）**：行政、政治、民間（CI 運営者等）、消防、医療など、事案に関わる全アクターが協力し、既存計画の補完やインターフェースの欠落を議論する |

| | |
|---|---|
| | • **分析ワークショップ**：専門家が一堂に会し、シナリオに基づく被害想定や cascade（連鎖）効果、対応能力の「目標と現状の比較 (TARGET-ACTUAL)」を議論・決定する |
| 官側詳細（政府横断 WS・分析チーム等） | • **運営委員会 (Steering Committee)**：連邦省庁の代表で構成され、内務省が調整する。手法の枠組み決定やハザード選定を行う<br>• **作業委員会 (Working Committee)**：連邦機関の代表で構成され、具体的なシナリオ作成や報告書作成を行う<br>• **ハザード専門サブグループ**：専門機関が主導し、個別のシナリオ分析を実施する |

### 1.3.4 評価対象とするリスク

ドイツでは以下のリスクを評価対象としている。

**自然災害・人為的環境影響（Naturereignisse / Anthropogene Umwelteinflüsse）**

| 番号 | ドイツ語（Überschrift/Beschreibung） | 日本語訳 |
|---|---|---|
| **3100** | **Gefahren und Anforderungen auf Grund von Naturereignissen und anthropogenen Umwelteinflüssen** | **自然災害および人為的環境影響による危険と要求事項** |
| **3110** | **Extremwetterlagen** | **極端な気象状況** |
| 3111 | Sturm/Orkan/Tornado | 嵐／暴風／竜巻 |
| 3112 | Starkregen, Hagel, Eisregen, Blitzeis | 豪雨、雹、氷雨、ブラックアイス |
| 3113 | Langanhaltender Schneefall/Schneeverwehungen | 長期にわたる大雪／吹雪 |
| 3114 | Langanhaltender Starkfrost | 長期にわたる強い霜 |
| 3115 | Lawinengefahren | 雪崩の危険 |
| 3116 | Schwere Gewitter mit massiven Blitzeinschlägen | 大規模な落雷を伴う激しい雷雨 |
| 3117 | Hitze- und Dürreperioden mit Missernten und/oder Trinkwassermangel | 不作および／または飲料水不足を伴う猛暑・干ばつ期 |
| 3118 | SMOG | スモッグ |
| **3120** | **Erdbeben** | **地震** |
| **3130** | **Erdbewegungen** | **地盤変動** |
| 3131 | Bergschäden/Erdsenkungen/Erdrutsche/Muren/Hangrutschungen | 鉱山被害／地盤沈下／地滑り／土石流／斜面崩壊 |
| **3140** | **Flächenbrände (Waldbrand, Heidebrand, Moorbrand)** | **面的火災（山林火災、荒野火災、泥炭地火災）** |
| **3150** | **Hochwasser/Sturmfluten** | 洪水／高潮 |
| 3151 | Hochwasser durch Staudammbrüche | ダム決壊による洪水 |
| 3152 | Örtliche Hochwasser durch starke Regenfälle | 強雨による局地的洪水 |
| 3153 | Hochwasser in Bächen, Flüssen und Stromtälern | 小川・河川・川谷における洪水 |
| 3154 | Sturmfluten/Hochwasser an Meeresküsten und Binnenseen | 海岸・内陸湖における高潮／洪水 |
| **3160** | **Meteoriteneinschläge** | **隕石衝突** |

ABC 災害・技術・交通事故・大火災（ABC-Lagen / Technologie- und Transportunfälle / Großbrände）

| 番号 | ドイツ語（Überschrift/Beschreibung） | 日本語訳 |
|---|---|---|
| **3200** | **Gefahren und Anforderungen auf Grund von ABC-Lagen, Technologie- und Transportunfällen und Großbränden** | **ABC 災害、技術事故・交通事故および大火災による危険と要求事項** |
| **3210** | **A-Gefahren** | **A（放射線）危険** |
| 3211 | Gefahrstofffreisetzungen aus Kernkraftwerken des eigenen Landes | 自国の原子力発電所からの危険物質放出 |

| | | |
|---|---|---|
| 3212 | Gefahrstofffreisetzungen aus Kernkraftwerken der Nachbarländer | 隣国の原子力発電所からの危険物質放出 |
| 3213 | Gefahrstofffreisetzungen aus Kernkraftwerken anderer Staaten | 他国の原子力発電所からの危険物質放出 |
| 3214 | Gefahrstofffreisetzungen aus sonstigen kerntechnischen Anlagen (Forschungsreaktoren, Wiederaufarbeitungsanlagen oder anderen Anlagen mit radioaktiven Stoffen) | その他の原子力施設（研究用原子炉、再処理施設、または放射性物質を扱うその他の施設）からの危険物質放出 |
| 3215 | Freisetzung sonstiger radioaktiver Stoffe | その他の放射性物質の放出 |
| **3220** | **B-Gefahren** | **B（生物）危険** |
| 3221 | Seuchen (Epidemien, z. B. Influenza und Pandemien) | 感染症（流行病、例：インフルエンザおよびパンデミック） |
| 3222 | Tierseuchen (Epizootien) | 家畜伝染病（エピズーティ） |
| 3223 | Großflächige Pflanzenkrankheiten (Epiphytien) | 広域植物病（エピフィティ） |
| 3224 | Freisetzung pathogener Stoffe oder Mikroorganismen aus biologischen/gentechnischen Anlagen | 生物工学・遺伝子工学施設からの病原性物質または微生物の放出 |
| 3225 | Freisetzung sonstiger pathogener (biologischer) Stoffe oder Mikroorganismen | その他の病原性（生物学的）物質または微生物の放出 |
| **3230** | **C-Gefahren** | **C（化学）危険** |
| 3231 | Freisetzung toxischer Stoffe (nicht-Seveso-Betriebe) | 有毒物質の放出（セベソ指令非対象事業所） |
| 3235 | Gefahrstofffreisetzungen aus ortsfesten Objekten mit bekanntem Gefahrenpotenzial (Seveso-Betriebe, z.<br>B. Freisetzung bestimmter ungefährlicher Stoffe, die<br>erst durch die Freisetzung selbst brennen, explodieren, verpuffen oder durch Verbindung mit anderen Stoffen pathogen oder toxisch werden) | 既知の危険可能性を持つ固定施設からの危険物質放出（セベソ指令対象事業所。例：放出によって燃焼・爆発・爆燃が生じる、または他の物質との結合により病原性・毒性を持つ特定の無害物質の放出） |
| 3240 | Gefahrstofffreisetzungen bei Transportunfällen (Straße, Schiene, Wasserstrassen einschließlich Küstenmeer und hohe See, Luft) ※ Ausführungen zu Pipelines entweder unter dieser Kennziffer oder unter 3260 | 交通事故時の危険物質放出（道路、鉄道、沿岸海域・公海を含む水路、航空）※パイプラインに関する記述はこの番号または 3260 で扱う |
| 3241 | Straße, Schiene, Luft | 道路、鉄道、航空 |
| 3242 | Binnenwasserstraßen | 内陸水路 |

交通事故・多数傷病者・重要インフラ（供給）

| **番号** | **ドイツ語（Überschrift/Beschreibung）** | **日本語訳** |
|---|---|---|
| 3243 | Küstenmeer/hohe See | 沿岸海域／公海 |
| 3245 | Großbrände, Explosionen, Zerknalle, Verpuffungen | 大規模火災、爆発、爆裂、爆燃 |
| **3250** | **Massenanfall von Betroffenen** | **多数傷病者発生（マスカジュアリティ）** |
| 3251 | Straße einschließlich Übergänge und Tunnels | 道路（踏切・トンネルを含む） |
| 3252 | Schiene einschließlich Übergänge und Tunnels | 鉄道（踏切・トンネルを含む） |
| 3253 | Wasserstrassen einschließlich Küstenmeer und hohe See sowie Binnengewässer | 沿岸海域・公海・内陸水域を含む水路 |
| 3254 | Luft | 航空 |
| 3255 | Massenanfall von Betroffenen durch sonstige Ursachen | その他の原因による多数傷病者発生 |
| **3260** | **Schwere Störungen und Schäden in Einrichtungen der Versorgung und Ernährung (Kritische Infrastruktur – Versorgung)** ※ Ausführungen zu Pipelines entweder unter dieser Kennziffer oder unter 3240 | **供給・食料施設における重大な障害・損害（重要インフラ－供給）** ※パイプラインに関する記述はこの番号または 3240 で扱う |
| 3261 | Wasser | 水 |
| 3262 | Lebensmittel | 食料品 |
| 3263 | Gas (Erdgas, Flüssiggas) | ガス（天然ガス、液化ガス） |

| | | |
|---|---|---|
| 3264 | Elektrizität | 電力 |
| 3265 | Fernwärme | 地域暖房 |
| 3266 | Mineralöl | 鉱物油 |
| 3267 | Kohle | 石炭 |
| 3269 | Gesundheit (Krankenhäuser/Klinika, zentrale Arzneimittellager, …) | 保健医療（病院・クリニック、中央薬品倉庫など） |

廃棄処理・情報インフラ・テロ・戦争

| 番号 | ドイツ語（Überschrift/Beschreibung） | 日本語訳 |
|---|---|---|
| **3270** | **Schwere Störungen und Schäden in Einrichtungen der Entsorgung (Kritische Infrastruktur – Entsorgung)** | **廃棄処理施設における重大な障害・損害（重要インフラ－廃棄処理）** |
| 3271 | Abwassernetz, Klärwerke | 下水道ネットワーク、下水処理場 |
| 3272 | Abfallentsorgung allgemein, Mülldeponien, Müllverbrennungsanlagen | 一般廃棄物処理、廃棄物処分場、廃棄物焼却施設 |
| 3273 | Sondermüll-Verbrennungsanlagen | 産業廃棄物焼却施設 |
| **3280** | **Langanhaltende Störungen/großflächiger Ausfall der Informations-, Kommunikations- und Warnsysteme unter Berücksichtigung von Interdependenzen und Dominoeffekten (Kritische Infrastruktur – Informationstechnik)** | **相互依存性・連鎖効果を考慮した情報・通信・警報システムの長期的障害／広域停止（重要インフラ－情報技術）** |
| 3281 | Telefonnetze, Funknetze, EDV-Netze | 電話網、無線網、コンピューターネットワーク |
| 3282 | Satellitengestützte Systeme | 衛星利用システム |
| 3283 | Rundfunk und Fernsehen | ラジオ・テレビ放送 |
| **3290** | **Absturz kosmischer Flugkörper** | **宇宙飛行体の墜落** |
| **3295** | **Gefährdung durch Kampfmittel als Altlasten** | **遺棄爆発物・旧軍需品による危険** |
| **3300** | **Gefahren und Anforderungen durch Terrorismus/Anschläge/Attentate/Sabotage** | **テロリズム・攻撃・暗殺・妨害行為による危険と要求事項** |
| **3400** | **Kriegshandlungen auf oder über deutschem Boden oder in Grenzgebieten benachbarter Staaten zu Deutschland** | **ドイツ領土上・上空または隣国との国境地域における戦闘行為** |

出典）Methode für die Risikoanalyse im Bevölkerungsschutz

### 1.4 オランダ

#### 1.4.1 オランダ NRA 制度の概要

オランダの NRA 制度は、

- 国家安全保障利益への影響を基準としてリスクを整理し
- 脅威シナリオごとに発生可能性と影響を評価し
- 同一手法により幅広いリスクを比較可能な形で整理し
- その結果を国家安全保障戦略、レジリエンス評価、危機管理に接続する

という構造を有する。加えて、オランダでは、**重要分野間の相互依存性を明示的に考慮するシステム的・複合的リスク分析**が行われており、複数事象が同時又は連続して発生する状況をシナリオとして扱う点にも特徴がある。

この点において、オランダの NRA は、**国家安全保障利益への影響評価を軸としつつ、比較可能性とシステム的把握を両立させ、政策優先順位付けに接続する制度**として位置づけられる。

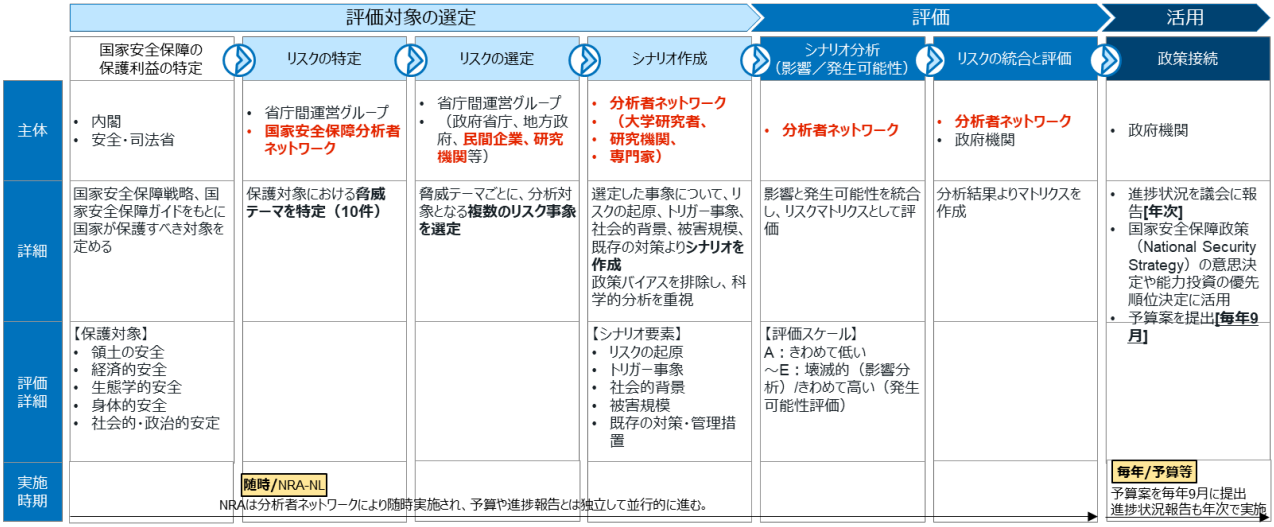
項目別の特徴について、下表に整理した。

| 項目 | 内容 |
|---|---|
| 制度の位置づけ<br>（Positioning） | オランダにおいては、国家リスク評価（NRA）は、**国家安全保障に影響を及ぼし得る脅威を特定し、その影響および発生可能性を評価する枠組**として位置づけられている。<br>また、NRA は**国家安全保障戦略（National Security Strategy）の基盤**とされ、評価結果は同戦略のインプットとして活用され得る。さらに、レジリエンス評価や危機管理にも活用される制度として整理されている。 |
| リスクの範囲・対象<br>（Scope） | 対象は、**非意図的脅威と意図的脅威の双方を含むオールハザード**であり、国内外の災害、危機、脅威を幅広く含む。<br>その上で、評価の目的は、**今後 5 年間におけるオランダの国家安全保障上の主要リスクを把握すること**に置かれている。<br>また、リスクはハザードそのものではなく、**国家安全保障利益に対する脅威と、それが社会的混乱をもたらすかどうか**という観点で捉えられている。 |
| リスクの概念<br>（Concept） | オランダでは、国家安全保障が危機に晒されるのは、**一つまたは複数の国家安全保障利益が脅かされ、その結果として社会的混乱が生じる、又は生じ得る場合**と定義されている。評価は以下の組み合わせによって行われる。<br>• 発生可能性（Likelihood）<br>• 6 つの国家安全保障利益への影響（Impact）<br>影響の基準となる国家安全保障利益は、従来の<br>• 領土の安全保障<br>• 身体の安全<br>• 経済安全保障<br>• 生態系の安全保障<br>• 社会的・政治的安定<br>に加え、**国際法秩序**が追加されている。さらに、領土の安全保障の中に**デジタル領域**および**同盟国の領土保全**という評価基準が組み込まれている。<br>この点で、オランダの NRA は、**国家安全保障利益への影響を基準にリスクを把** |

| | |
|---|---|
| | **握する構造**を有している。 |
| 評価手法<br>（Methodology） | 評価は、**脅威シナリオに基づくシナリオ分析**として実施される。その際、オールハザード・アプローチの下で、異なる災害、危機、脅威を**同一の評価手法**で分析することにより、相互比較を可能としている。<br>各シナリオについては、<br>• 6 つの国家安全保障利益への影響<br>• 発生可能性<br>を評価し、**Impact × Likelihood** の枠組みで比較評価が行われる。<br>このように、オランダの NRA は、**幅広いリスクを比較可能な形で整理し、政策判断に資する比較的・体系的な評価手法**として設計されている。 |
| 実施体制（Process & Governance） | 比較整理上、オランダは関与構造として**外部制度化型**に位置づけられており、関与の段階・役割としても、**分析の中核主体として専門家ネットワーク等が関与する構造**が確認されている。すなわち、政府内部だけで完結するのではなく、外部の専門的知見を制度的に取り込みながら、リスクのシナリオ分析および評価を行う構造が特徴である。 |
| 時間軸・更新<br>（Horizon & Cycle） | 評価射程（Horizon）は、通常のリスク評価について**約 5 年**が設定されている。その一方で、オランダでは**潜在的脅威について 10～20 年の長期的視点で別途整理する**など、時間軸を分離した設計が採られている。<br>また、更新サイクル（Cycle）については、**明示的な固定周期は設けられていないが、国家安全保障戦略等の見直しと連動して更新される**制度として整理されている。 |
| 評価結果の活用<br>（Use） | NRA の結果は、主として以下に活用される。<br>• 国家安全保障戦略の基盤・インプット<br>• レジリエンス評価<br>• 危機管理<br>• 戦略的政策形成<br>• 国家安全保障に関する戦略的議論<br>したがって、オランダの NRA は、単なるリスク一覧ではなく、**国家安全保障政策の方向付けと優先順位付けを支える基礎資料**として機能している。 |

### 1.4.2 オランダ NRA の実施フロー

オランダにおけるリスク評価から能力整備・政策接続に至る一連のフローを整理した。




### 1.4.3 外部専門家等の関与

外部専門家について下表に整理した。

| 項目 | 説明 |
|---|---|
| リスク評価の体制 | • 安全・司法省が「国家安全保障戦略」および NRA の調整責任を負う<br>• 内閣が戦略の実施に責任を負い、他省庁や民間、学術界と協力する |
| 専門家<br>参加組織 | • 知識機関<br>• 科学的基盤の専門家<br>• ビジネス界、民間セクター |
| 専門家<br>専門領域 | • 公衆衛生（RIVM）／情報・安全（AIVD/MIVD）／応用科学（TNO）／国際関係（クリンゲンダール研究所）／経済学（SEO）／法学（WODC）等 |
| 専門家<br>参加形態 | • **国家安全保障分析者ネットワーク (ANV/ANNN)**：政府機関、学術界、民間セクターの専門家からなる公式なネットワークで、シナリオの開発とリスク評価を実質的に担当する。これにより科学に基づいた分析を担保する<br>• **klankbordgroep (響板グループ/諮問グループ)**：科学、民間セクター、地方自治体などの専門家が、戦略の内容について意見交換を行う |
| 官側詳細<br>（政府横断<br>WS・分析チーム<br>等） | • **国家安全保障運営グループ (Steering Group)**：省庁間の組織で、評価のサイクル開始時にどのシナリオを詳細化するかを決定する。<br>• **地方レベルの関与**：安全地域 (safety/security regions) がシナリオ開発に参加し、現場の知見を取り入れる |

### 1.4.4 評価対象とするリスク

オランダでは以下のカテゴリー・個別リスクを評価対象としている。

| Threat Theme | Category | Scenario |
|---|---|---|
| Climate and natural disasters | Extreme weather events | Snow storm |
| | | Hurricane |
| | | Heat/drought |
| | Flood | Flooding from the sea |
| | | River flood |
| | Wildfire | Wildfires |
| | Earthquake | Induced earthquake |
| | | Naturally occurring earthquake |
| Infectious diseases | Human infectious diseases and zoonoses | Pandemic caused by a respiratory virus transmissible from human to human |
| | | Flu pandemic |
| | | Flu epidemic |
| | Animal and plant diseases | Outbreak of foot and mouth disease among cows |
| | | Outbreak of a zoonotic variant of avian flu |
| Major accidents | Radiation accidents | Borssele nuclear plant |
| | | Radiation accident in Europe |
| | Chemical accidents | Failure of an ammonia storage tank |
| | Transport accidents | Train disaster with flash fire |
| Social polarisation , extremism and terrorism | Social polarisation | Social polarisation surrounding conspiracy theories |
| | Non-violent extremism | Infiltration of public administration |
| | | Subversive enclaves |
| | | Anti-government extremism |
| | Violent extremism | Anarcho-extremism |
| | | Escalation of violence by right-wing extremists |
| | | Attack on pride event |
| | Terrorism | Multiple terrorist attacks |
| | | Assault on and hostage-taking in parliament |
| | | Lone actor |
| Foreign subversion of the democratic constitutional system | Espionage | Cyber espionage targeted at public authorities |
| | | Traditional state espionage |
| | Foreign interference | Foreign interference diaspora communities |
| | Foreign influencing (hybrid operations) | (Covert) influencing by China |
| | | Hybrid operations by Russia - exploiting societal debate (migration) |
| | Organised crime | Criminal violence towards media and government |
| | | Organised crime throughout the Netherlands |
| | | Criminal interference in business |
| International and military threats | Pressure on multilateral security institutions | Disintegration of NATO |
| | | Disintegration of the OSCE |
| | | Rift within the EU |
| | Fragility in the vicinity of the Netherlands and/or the EU | IS seizes power in Morocco |
| | | Collapse of the Venezuelan state |
| | | Break-up of Bosnia-Herzegovina |
| | Armed conflict between centres of power | Deployment of nuclear weapons in the Iran and Saudi Arabia conflict |
| | | Reunification of China and Taiwan |
| | | Temporary occupation of an EU Member State |
| | | Crisis in the South China Sea |
| | Proliferation of weapons of mass destruction | Terrorist attack using a biological weapon |
| | | Innovation of nuclear delivery systems |
| Economic threats | Threats to the Netherlands' role as an important logistical hub | (No standalone scenario in Figure 8; scenarios incorporated into Figure 7 and Figure 2) |
| | Foreign interference in industry | Foreign state acquiring a minority interest in a major telecommunications provider |
| | | Foreign venture capital investment in health and biotech start-ups |
| | | Covert acquisition of an unlisted company whose products include dual-use goods |
| | Contraction or distortion of international trade | Trade war involving Europe |
| | | Trade disruption due to production issues abroad |

| | | |
|---|---|---|
| | | Foreign regulation of tech companies |
| | Unwanted strategic dependencies | Import of fossil-based energy |
| | | Shortages of key raw materials |
| | Destabilisation of the financial system | Systemic actor in the finance sector facing great difficulty |
| | | New European debt crisis |
| | | Disruption of payments |
| | | Adjustment of the value of financial assets as a result of expectations not being realised |
| Cyber threats | Disruption of the internet | Attack on a cloud service provider |
| | | Misconfiguration at a major internet service provider |
| | Disruption of cyber-physical systems | ICS cyber attack - chemical industry |
| | Cybercrime | Ransomware attack in the healthcare sector |
| | | Collateral damage |
| | (Cross-ref: Intentional threat against vital processes) | Ransomware attack on telecommunications provider |
| | (Cross-ref: Espionage ) | Cyber espionage targeted at public authorities |
| Threats to critical infrastructure | Intentional threat against vital processes | Ransomware attack on telecommunications provider |
| | Disruption of vital processes due to technical or human failure | Nationwide blackout |
| | | Chain effects of a power outage |
| | Natural event disrupting vital processes | River flood |
| | | Wildfires |

出典）National Risk Assessment of the Kingdom of the Netherlands 2022

### 1.5 フィンランド

#### 1.5.1 フィンランド NRA 制度の概要

フィンランドの NRA 制度は、

- 社会の根幹機能を基準としてリスクを整理し
- オールハザードの事象を対象に
- 合理的最悪ケースシナリオに基づく分析を行い
- 5 つの主要影響基準と比較可能な尺度によって評価し
- その結果をリスク管理戦略、能力開発、資源配分に接続する

という構造を有する。

この点において、フィンランドの NRA は、ハザード事象そのものを起点とする制度というよりも、**社会の重要機能の維持と供給保障を軸に、国家・地域・民間をつなぐ影響起点型のリスク評価プロセス**として位置づけられる。

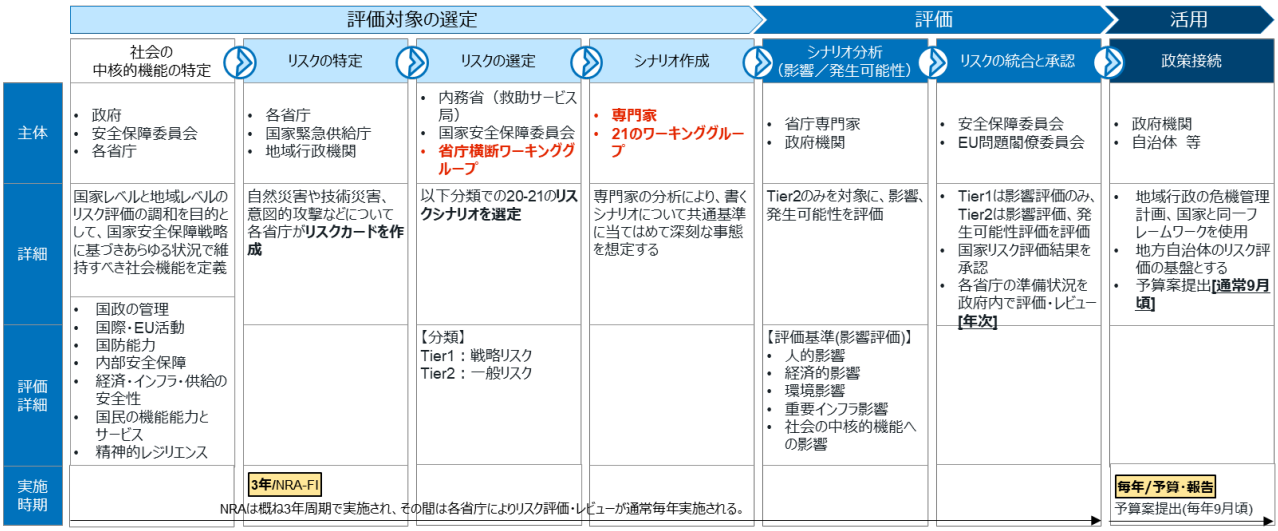
項目別の特徴について、下表に整理した。

| 項目 | 内容 |
|---|---|
| 制度の位置づけ<br>（Positioning） | フィンランドにおいては、国家リスク評価（NRA）は、**社会の根幹機能（core vital functions）を確保するための国家的なリスク把握プロセス**として位置づけられている。<br>その制度設計は、2010 年の「社会のための国家安全保障戦略」に見られるように、**あらゆる状況で確保されるべき社会の根幹機能の定義と高度なリスク特定プロセスを結びつけた構造**を有する。<br>また、最初の NRA は、EU 市民保護メカニズムに対するフィンランド政府の対応としても位置づけられており、国家レベルから地方レベルまでを含むリスク管理政策の改善および統合の一環として設計されている。 |
| リスクの範囲・対象<br>（Scope） | 対象は、**テロやサイバー攻撃を含むオールハザード**である。その上で、フィンランドの NRA は、ハザードそのものを起点とするというより、**社会の根幹機能にどのような影響を与えるか**という機能起点の整理を採用している。<br>また、リスクの定義には、緊急事態の発生可能性に加えて、**人的、経済的、環境的、社会的・政治的影響**が組み込まれており、それらの分野における資産の堅牢性や脆弱性も考慮される。 |
| リスクの概念<br>（Concept） | フィンランドにおけるリスクは、以下の組み合わせとして把握される。<br>• 発生可能性（Likelihood）<br>• 影響（Impact）<br>ただし、概念上の特徴は、単なるハザード評価ではなく、**社会の重要機能の維持および供給保障の確保を中核視点とすること**にある。<br>影響評価については、以下の **5 つの主要基準**が設定されている。<br>• 人的影響<br>• 経済的影響<br>• 環境への影響<br>• 重要インフラへの影響 |

| | |
|---|---|
| | • 社会の根幹機能への影響<br>この点で、フィンランドの NRA は、**社会機能への影響を基準としてリスクを捉える構造**を有している。 |
| 評価手法<br>（Methodology） | 評価は、**合理的最悪ケースシナリオ（reasonable worst case scenarios）に基づくシナリオ分析**を基礎として実施される。<br>詳細分析は **21 のワーキンググループ**で行われ、それぞれがリスクの歴史的背景、起こりうる結果の概要、ならびに既に講じられている準備・対応措置を含むシナリオを策定した。<br>また、フィンランドの NRA は、<br>• すべてのリスクについて影響分析<br>• tier 2 リスクについて発生可能性分析<br>を行うよう設計されている。<br>影響の測定は **5 段階スケール**で行われ、例えば人的被害については、少数の死傷者を低影響、1,000 人超を高影響とするような閾値設計が採用されている。さらに、内務省の調整の下で、国家レベルおよび地域レベルの評価手法の整合が図られ、**比較可能な基準による評価**が志向されている。 |
| 実施体制（Process & Governance） | フィンランドの NRA は、**首相府に始まる政府上級レベルのリーダーシップ**の下で実施される。実務面では、緊急対応に責任を持つ各省庁の危機管理準備担当秘書官から成る**ワーキンググループ**が設置され、民間部門については**国家緊急供給庁**および**地域国家行政機関**を通じて参加する。<br>また、作業は**内務省（救助サービス局）が調整**し、**保安委員会（Security Committee）が運営**する。合意された NRA は、その後、事務次官レベルの保安委員会および大臣級委員会に提出され、最終承認を受けるプロセスとなっている。<br>このように、フィンランドでは、政府主導の枠組みの下で、民間・地域主体を制度的に取り込む構造が採られている。 |
| 時間軸・更新<br>（Horizon & Cycle） | 評価射程（Horizon）については、**制度上明示されていない**。<br>一方で、更新サイクル（Cycle）については、比較整理上、**制度的な周期で定期的に更新する方式**に分類されており、EU の報告義務に基づく**概ね 3 年ごとの実施**として整理されている。 |
| 評価結果の活用<br>（Use） | フィンランドの NRA 結果は、主として以下に活用される。<br>• リスク管理戦略の支援<br>• 能力開発の支援<br>• 意識向上<br>• リスクに基づく資源配分のための共通根拠資料<br>• 国家レベルおよび地方レベルのリスク管理の改善<br>すなわち、フィンランドの NRA は、単なる分析資料ではなく、**社会の重要機能の維持を前提に、政策優先順位付け、能力整備、資源配分を支える基盤情報**として機能する。 |

### 1.5.2 フィンランド NRA の実施フロー

フィンランドにおけるリスク評価から能力整備・政策接続に至る一連のフローを整理した。




### 1.5.3 外部専門家等の関与

外部専門家について下表に整理した。

| 項目 | 説明 |
|---|---|
| リスク評価の体制 | • 内務省（救助サービス局）が作業を調整し、安全保障委員会が全体を運営する。<br>• 2015 年から NRA を導入し、国家レベルの「Tier1 リスク」と「Tier2 リスク」を特定している |
| 専門家<br>参加組織 | • 民間セクター（国家緊急供給庁/NESA 経由）<br>• 地域当局（地域州行政局、環境センター等）<br>• NGO（赤十字等）<br>• 学術界 等 |
| 専門家<br>専門領域 | • 気象（FMI）／放射線／医療／食料安全／物流／通信／サイバーセキュリティ等 |
| 専門家<br>参加形態 | • **マルチセクター・ワーキンググループ**：各省庁の準備秘書官や、民間・地域レベルの代表者で構成される。各省庁が作成した「リスクカード」を評価し、全政府的な対話を行う。<br>• **21 のワーキンググループ**：具体的なリスク分析は、各シナリオごとに設置された専門グループで実施される |
| 官側詳細<br>（政府横断<br>WS・分析チーム<br>等） | • **省庁間の協力**：首相府、外務、内務、保健社会、農林、運輸通信、雇用経済、環境、教育文化、国防の各省庁が横断的に関与する。<br>• **閣僚委員会 (EU 問題担当)**：最終的な NRA の承認を行い、政治的レベルでの合意を形成する |

### 1.5.4 評価対象とするリスク

フィンランドでは National risk assessment(NRA) 2023 において、対象リスクシナリオが公表されている。以下に NRA 2023 年版におけるリスクシナリオの設定を掲載する。

| Threat scenarios and disruptions |
|---|
| Information influence activities |
| Political, financial and military pressure |
| Use of military force |
| Mass influx of migrants and instrumentalisation of migration |
| Terrorist act or another violent act targeting the structures of society or large crowds |
| Violent civil disturbances involving large crowds, groups or communities or actions compromising social order |
| Disruption of the public economy |
| Disruption of the financial system |
| Disruptions in energy supply |
| Major disruption in power supply |
| Severe disruption in the availability of fuels |
| Disruptions in information and communications networks and services |
| Disruptions in the continuity of transport |
| Disruptions in health security |
| Antimicrobial drug resistance |
| Pandemic or similar widespread epidemic |
| Animal disease epidemics |
| Disruptions in water supply |
| Disruptions in food supply and deterioration of food and nutrition security |
| Large-scale or long-lasting accidents |
| Maritime multi-sector accident |
| Severe nuclear power plant accident in Finland or Finland’s neighbouring areas |
| Several simultaneous extensive wildfires |
| Extremely strong space weather storm |

### 1.6 スウェーデン

#### 1.6.1 スウェーデン NRA 制度の概要

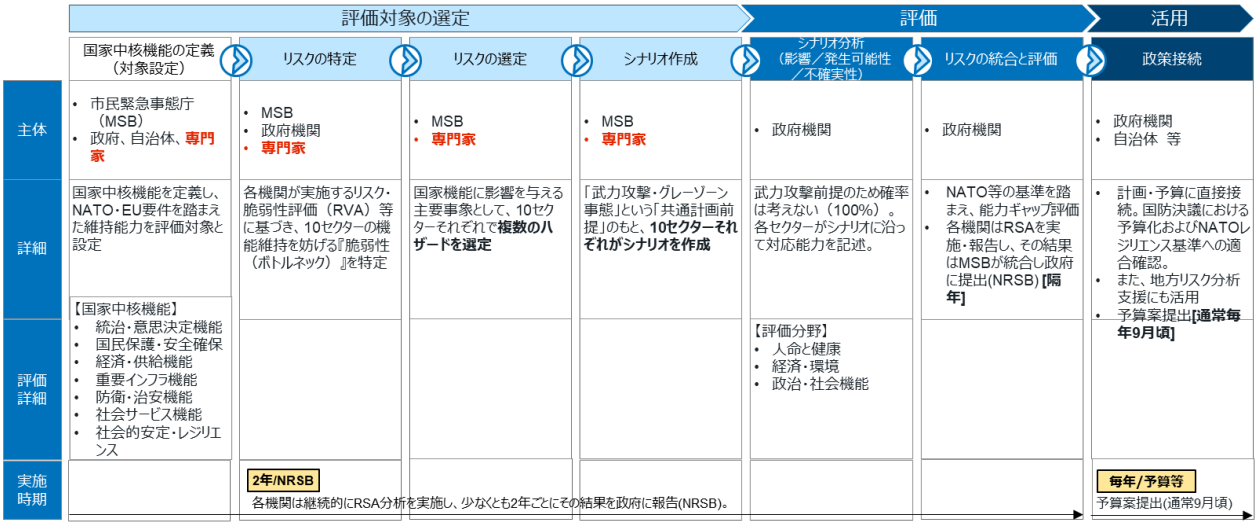
項目別の特徴について、下表に整理した。

| 項目 | 内容 |
|---|---|
| 制度の位置づけ（Positioning） | スウェーデンにおいては、国家リスク評価は国家的リスク・脆弱性評価（NRSB）として制度化されており、**スウェーデン市民保護・緊急事態庁（MSB）が隔年で政府に提出する国家レベルの評価プロセス**として位置づけられている。<br>MSB は、備えを所管する各機関が提出するリスク・脆弱性評価（RSB）を考慮しつつ、**社会全体レベルと備えセクター別の双方で評価を実施**する。また、NRSB は、特に重大な脅威・リスク・脆弱性と、講じられた又は計画中の措置を示すものとして位置づけられている。 |
| リスクの範囲・対象（Scope） | 対象は、**スウェーデン社会の保護価値に対して特に重大な影響を及ぼし得るリスク**であり、発生した場合に平時の危機事象又は警戒態勢につながる可能性のあるものが対象とされる。<br>2025 年版 NRSB では、**平時の危機から戦争までを含む広範な脅威像**を対象としており、**26 の特に重大な脅威**が整理されている。加えて、スウェーデンの評価では、急性リスクのみならず、社会の保護価値を継続的に脅かし、急性リスクの発現を助長し得る慢性的リスク（chronic risks）も補完的に含めている点が特徴である。<br>また、重大性の判断に当たっては、脅威が①特定可能な単一の有害現象であり、②直接的損害をもたらし、③社会の保護価値に特に重大な影響を及ぼし得て、④平時の危機又は警戒態勢への移行を引き起こし得ること、という 4 基準が用いられている。 |
| リスクの概念（Concept） | スウェーデンでは、脅威（hot）とリスク（risk）を区別して捉えている。脅威とは、個人又は社会に損害を与え得る潜在的原因であり、リスクとは、**脅威が現実化する可能性と、その結果生じる負の影響の組み合わせ**として定義される。<br>評価において検討されるのは、<br>• 脅威そのもの<br>• 事象としての具体的な姿（シナリオ）<br>• その結果として生じる影響<br>• 発生可能性<br>である。<br>また、MSB は、脅威が現実化する際の**深刻かつ信頼性の高い単一のシナリオ**を用いて分析する。さらに、スウェーデンでは脆弱性が明示的に統合されており、**有害事象の発生可能性を下げる能力又は影響を抑制・管理する能力に欠陥がある場合に脆弱性が生じる**とされる。脆弱性は、社会全体レベルと備えセクター別の双方で把握される。 |
| 評価手法（Methodology） | 評価は、**脅威起点のシナリオ分析**を基礎として実施される。MSB は、脅威の現れ方を**強度、持続時間、影響範囲**の観点から記述し、それに基づいて想定される影 |

| | |
|---|---|
| | 響を評価する。<br>影響評価は、**死者数、負傷者数、社会経済的コスト、自然・文化環境への被害**など複数の影響変数を用いて行われ、これらには**操作化された測定値**が設定されている。一方、発生可能性については、脅威の性質が複雑であることを踏まえ、**確率的要因、決定論的要因、敵対的・人為的要因**を踏まえた論理的推論により導かれる。また、評価作業は本質的に探索的であり、**国家レベルのリスク評価には大きな不確実性が内在する**ことも明示されている。<br>比較整理上は、分析手法は**シナリオ記述→影響評価→発生可能性評価**という段階的な構造として整理されている。 |
| 実施体制<br>（Process & Governance） | NRSB は、**MSB が制度上の実施主体**として作成する。作業に当たっては、**約 70 の政府機関**が 2024 年中に MSB へ提出したリスク・脆弱性評価（RSB）が、特にセクター別脆弱性評価の基礎資料として用いられる。<br>さらに、**26 の専門機関**（備え当局及びその他の当局）が、国家リスク評価の各部分について専門家として関与している。また、リスク評価に含まれる脅威記述、影響評価、発生可能性評価は、**専門機関によるコメントとソース確認を通じて品質保証**されている。<br>このように、スウェーデンでは、MSB を中核にしつつ、各備え当局・専門機関の知見を取り込む**外部制度化型かつ多主体参加型の評価体制**が採られている。 |
| 時間軸・更新<br>（Horizon & Cycle） | 評価射程（Horizon）は、**今後 5 年間**と明示されている。すなわち、NRSB は、社会が今後 5 年の間に直面し得る特に重大な脅威とリスクを対象としている。<br>一方、更新サイクル（Cycle）は、**隔年**である。MSB は、奇数年ごとに NRSB を作成・提出する任務を負っており、比較整理上も、スウェーデンは**制度的な周期で定期更新する方式**に位置づけられている。 |
| 評価結果の活用<br>（Use） | NRSB の結果は、主として以下に活用される。<br>• 国家レベルの関係機関に対する統制・フォローアップの基盤資料<br>• リスク意識や責任関係が不十分な領域における政策形成の基礎資料<br>• スウェーデンの備えの強化に向けた、**dimensionerande typsituationer**（備えを設計するための典型事態）の明確化<br>• 可能な事象展開に関する前提の精緻化<br>• リスク状況ごとの社会的影響の可視化<br>• **国家的調整が必要な事前計画や大規模演習の対象リスクの選定**<br>したがって、スウェーデンの NRSB は、単なる状況認識の整理にとどまらず、**政策形成、備え・レジリエンス計画、国家的調整の優先付けを支える基盤情報**として機能している。一方で、提示ファイル中には**資源配分への直接接続の明示的記述はない**。 |

### 1.6.2 スウェーデン NRA の実施フロー

スウェーデンにおけるリスク評価から能力整備・政策接続に至る一連のフローを整理した。




### 1.6.3 外部専門家等の関与

外部専門家について下表に整理した。

| 項目 | 説明 |
|---|---|
| リスク評価の体制 | • スウェーデン市民緊急事態庁（MSB）が内閣からの負託を受け、主導する<br>• 地方の「リスク・脆弱性分析（RVA）」を国家レベルで統合する「国家リスク・能力分析」として運用されている |
| 専門家<br>参加組織 | • 16 の市町村<br>• 3 つの郡議会<br>• 14 の民間、非営利等機関 等 |
| 専門家<br>専門領域 | • 個別の専門り領域についての詳細情報なし<br>• （MSB はカナダ等の他国とも協力し、標準化された能力アセスメント手法を開発している） |
| 専門家<br>参加形態 | • **専門家ワークショップ**：50 名規模の専門家やキーマンが集まり、リスク特定やシナリオ分析を共同で行う。これにより異分野間のネットワークを形成し、危機の複雑さを理解する。<br>• **品質レビューパネル**：評価の後に、利害関係者による品質チェックを行い、不確実性の高い箇所を特定する |
| 官側詳細<br>（政府横断<br>WS・分析チーム<br>等） | • **56 の政府機関**：広範な国家機関がリスク特定や品質レビューのプロセスに関与する。<br>• **ボトムアップの統合：**義務化されている地方レベルの RVA の結果を、国家レベルの「トップダウン」評価で補完する体制をとっている |

### 1.6.4 評価対象とするリスク

NRSB2025 では、２６の特に重大な脅威・リスクが公表されている。一方、脆弱性評価については、対象セクターは公表されているが内容は機密扱いとなっている。

国家リスク像 ― NRSB 2025 における特に重大な脅威・リスク
Nationell riskbild – särskilt allvarliga hot och risker i NRSB 25）

**生物学的脅威（Biologiska hot）**

- ✓ 感染症（Epidemi）
- ✓ 動物感染症（Epizooti）

**自然・環境リスク（Natur- och miljöhot）**

- ✓ 森林火災・植生火災（Skogs- och vegetationsbrand）
- ✓ 集中豪雨（Skyfall）
- ✓ 太陽嵐（Solstorm）
- ✓ 暴風（Storm）
- ✓ 熱波・干ばつ（Värmebölja och torka）

**技術的脅威（Teknologiska hot）**

- ✓ ダム決壊（Dammhaveri）
- ✓ IT インシデント（It-incident）
- ✓ 化学物質事故（Kemikalieolycka）
- ✓ 海上事故（Maritim olycka）
- ✓ 電力系統のネットワーク障害（Nätsammanbrott i elsystemet）
- ✓ 原子力事故（Kärnteknisk olycka）

**社会的・経済的脅威（Sociala och ekonomiska hot）**

- ✓ 国外で発生する重大事象（Händelse utomlands）
- ✓ 制御不能な人口移動（Okontrollerade befolkningsrörelser）
- ✓ 国際的な物流・貿易フローの混乱（Störning i internationella handelsflöden）
- ✓ 暴動・大規模騒乱（Våldsamt upplopp）

**安全保障上の脅威（Säkerhetshot）**

- ✓ CBRN テロ（CBRN-attentat）
- ✓ サイバー攻撃（Cyberangrepp）
- ✓ 不正な情報操作（Otillbörlig informationspåverkan）
- ✓ テロ攻撃（Terrorattentat）
- ✓ 重要インフラへの破壊工作（Sabotage mot kritisk infrastruktur）

**軍事的脅威（Militära hot）**

- ✓ 武力攻撃 ― NATO 枠組内でのスウェーデン国外における戦闘
（Väpnat angrepp – Strid utanför Sverige inom ramen för Nato）
- ✓ 武力攻撃 ― 遠隔攻撃（Fjärrangrepp）
（Väpnat angrepp – Fjärrangrepp）
- ✓ 武力攻撃 ― スウェーデン領域内での戦闘
（Väpnat angrepp – Strid på svenskt territorium）
- ✓ 武力攻撃 ― 核兵器による攻撃
（Väpnat angrepp – Kärnvapenangrepp）

**慢性的リスク （Kroniska risker）**

- ✓ 気候変動 Klimatförändringar
- ✓ ハイブリッド影響（複合的脅威） Hybridpåverkan
- ✓ 体制を脅かす組織犯罪 Systemhotande organiserad brottslighet
- ✓ 不安定化する国際情勢 En instabilare omvärld

【セクター別脆弱性評価】＊機密扱い
経済安全保障（Ekonomisk säkerhet）
電子通信・郵便（Elektroniska kommunikationer och post）
エネルギー供給（Energiförsörjning）
金融サービス（Finansiella tjänster）
基盤データ供給（Försörjning av grunddata）
保健・医療・介護（Hälsa, vård och omsorg）
食料供給・飲料水（Livsmedelsförsörjning och dricksvatten）
治安・公共の安全（Ordning och säkerhet）
消防・救助および民間防護（Räddningstjänst och skydd av civilbefolkningen）

交通・輸送（Transporter）
【社会全体レベルの脆弱性評価】
社会全体レベル（Övergripande samhällsnivå）

出典）NRSB2025

## Appendix II 国家リスク分析に関する予兆・可能性・潮流の把握・分析（海外主要国における事例）

ここでは、国家リスク分析に関する予兆、可能性、潮流の把握・分析の手法・プロセスについて、本調査における調査対象６か国に加えて、シンガポールを加えて、７か国を対象に、各国の取り組みを調査・整理した。特に以下の３か国については、積極的な取組みが認められる。

**イギリス**：政府科学局（Government Office for Science）が主導する「ホライズンスキャニング・プログラム」を実施している。

**シンガポール**：首相府直轄の「戦略先見センター（Centre for Strategic Futures: CSF）」を有し、世界で最も先進的な取り組みの一つとされる。

**フィンランド**：議会に「将来委員会（Committee for the Future）」、政府に「先見グループ」を置き、4 年ごとに「将来に関する政府報告書」を提出している。

### 2.1 各国活動比較サマリー

| 国名 | 主要実施機関 | フォーサイト体制の特徴 | NRA 接続強度 |
|---|---|---|---|
| 英国 | 政府科学局（GO-Science）、内閣府 | 科学トップと政治が法制化・組織化されたハイブリッド体制 | ◎ 強い（直接的・制度的統合） |
| シンガポール | 首相府、戦略先見センター（CSF） | 首相府直轄による「政府一体」の強力なトップダウン体制 | ◎ 強い（完全統合型） |
| フィンランド | 議会将来委員会、Sitra、政府先見グループ | 議会・政府・独立機関の三層による民主的・協調的体制 | ○ 中程度（包括的安全保障経由） |
| オランダ | PBL、WRR、CPB、NCTV | 独立した専門評価機関による科学的勧告重視の体制 | ○ 中程度（補完的・間接的） |
| 米国 | NIC、DHS、FEMA、FFCOI 等 | 各省庁が独自の手法を確立する分散型・省庁横断体制 | △ 弱い（部分的・分散的） |
| ドイツ | 連邦教育研究省（BMBF）、Fraunhofer ISI | 厳格な品質管理による技術・イノベーション重視の体制 | △ 弱い（制度的連携は限定的） |
| スウェーデン | Vinnova、MSB、FOI | イノベーション機関主導・先端技術（AI 等）活用の体制 | △ 弱い（現状では間接的・部分的） |

イギリス・シンガポールは、フォーサイト（先見活動）が国家の公式なリスク評価（NRA）プロセスに直接的に統合されており、政策立案や予算配分への強力な反映メカニズムを持つ。

オランダ・フィンランドは、独立性の高い研究機関や議会がフォーサイトを担い、その長期的な知見が包括的な安全保障フレームワークを通じて間接的に NRA を補完している。

アメリカ・ドイツ・スウェーデンは、特定分野（イノベーションや諜報など）における先見活動は世界最高水準であるが、それらを政府全体を覆う単一の国家リスク評価として統合する制度的メカニズムは発展途上または分散型である。

### 2.2 将来の不確実性・リスク把握の主要手法

将来予測の手法は、大きく以下の 3 種類に分類される。各手法は独立して用いられるのではなく、相互補完的に組み合わせて使用されることが一般的である。

| 手法 | 焦点 | 問いの形 |
|---|---|---|
| ホライズン・スキャニング | 予兆・断片 | 「何か新しいことが起きていないか？」 |
| シナリオ・プランニング | 可能性・幅 | 「もし A ではなく B という世界になったらどうするか？」 |
| メガトレンド分析 | 必然・潮流 | 「避けて通れない巨大な変化は何か？」 |

#### 2.2.1 ホライズン・スキャニング

**「兆しの探索」：変化の初期微動を捉える**

目的：既存の枠組みにとらわれず、組織にとっての「未知の未知（知らないことすら知らない事象）」を減らすことにある。まだ顕在化していないが、将来的に大きな影響を及ぼす可能性のある「弱い信号（Weak Signals）」を特定する活動である。

具体的な実施内容:

- **STEEP 分析:** 社会（Social）、技術（Technological）、経済（Economic）、環境（Environmental）、政治（Political）の 5 つの切り口で、通常のニュースには掲載されないような専門論文、特許、SNS の局所的な動向、スタートアップの動きなどを網羅的に収集する。
- **継続的モニタリング:** 一過性の調査にとどまらず、専門家チームが日々「通常とは異なる動き」「新しい変化の兆候」と判断した情報をデータベース化し、共有する体制を構築している。

#### 2.2.2 シナリオ・プランニング

**「複数未来の構築」：あり得る未来の幅を描く**

目的：特定の未来に賭けるのではなく、いかなる未来が訪れても「致命的打撃を回避できる（レジリエンスを確保する）」ための戦略を構築することにある。「未来はこうなる」という単一の予測（Forecast）に依拠するのではなく、「未来はこうなり得る」という複数の分岐を論理的に構築する手法である。

具体的な実施内容:

- **不確実性の軸の設定:** ホライズン・スキャニングで得られた情報をもとに、将来を大きく左右し、かつ結果が予測不可能な「2 つの重要軸」を選定する（例：「国際協力 vs 保護主義」×「技術革新の加速 vs 停滞」）。
- **4 つの世界観の構築:** この 2 軸を交差させ、4 つの異なる未来の物語（シナリオ）を作成する。各シナリオにおいて、自国の社会保障や教育がどのように変化するかを具体的に記述する。

#### 2.2.3 メガトレンド分析

**「長期潮流の把握」：抗えない大きなうねりを知る**

目的：短期的な変動に惑わされることなく、国家や組織が長期的・構造的に取り組むべき優先事項を明確化することにある。個別の事象ではなく、今後 10～30 年にわたって社会の基盤を規定する、不可逆かつ巨大な変化を分析する手法である。

具体的な実施内容:

- **相互作用の分析:**「少子高齢化（人口動態）」と「デジタル化（技術）」が交差した場合に医療システムに何が生じるかというように、「メガトレンド同士の衝突」が生む社会的課題を予測する。

- **構造的脆弱性の特定:** これらの巨大な潮流に対し、現在の法制度や産業構造がどこで「無理を来すか」を特定する。

### 2.3 調査対象国における実施事例 1（英国）

英国のリスク評価は、政治的な意思決定機関と科学的な専門家組織が密接に連携する「ハイブリッド体制」で実施されている。

#### 2.3.1 英国 フォーサイト制度の概要

| 項目 | 説明 |
|---|---|
| 制度タイプと制度位置づけ | 内閣府（Cabinet Office）レジリエンス局（Resilience Directorate）と政府科学局（GO-Science）の連携による法制化・組織化されたハイブリッド体制。UK 政府レジリエンス・フレームワーク（2022 年）において、フォーサイトと NRA の制度的接続が明示されている。 |
| フォーサイトの整理思想 | STEEP（社会・技術・経済・環境・政治）の観点から「弱い信号（Weak Signals）」を探索するホライズン・スキャニングを中核に置く。合理的最悪ケース・シナリオ（RWCS）を評価の基礎とし、主幹省庁（LGD）が担当領域のリスクを特定する方式を採用している。 |
| 実施枠組みと体制 | 内閣府レジリエンス局が全体統括を担う。GO-Science のホライズン・スキャニング・チームが新興リスクを探索し、その成果を内閣府に直接報告する。各省庁の LGD が担当領域のリスクを特定・報告する義務を負い、政府主席科学顧問（GCSA）がリスク評価全体の科学的妥当性を担保する。 |
| NRA との接続 | ◎ 強い。GO-Science のホライズン・スキャニングが国家安全保障リスク評価（NSRA）プロセスの上流工程として明確に位置付けられている。NSRA の結果は、国家レジリエンス計画前提（NRPA）の基礎として用いられる。 |
| 主要参照文書 | 国家リスク登録簿（NRR 2023）、国家安全保障リスク評価（NSRA、機密版）、UK 政府レジリエンス・フレームワーク（2022 年）、コミュニティ・リスク登録簿（CRR）、GO-Science Foresight Toolkit |

#### 2.3.2 英国 フォーサイトの実施フロー

リスク評価は、2～3 年周期（NSRA）及び継続的なモニタリングを通じて実施されている。以下のプロセスが確認される。

**評価射程と更新サイクル:**

- 悪意あるリスク（テロ・攻撃等）：2 年サイクルで評価
- 非悪意リスク（自然災害・感染症等）：5 年サイクルで評価
- ホライズン・スキャニング：常時継続的に実施

**プロセス詳細フロー:**

1. GO-Science が STEEP 観点によるホライズン・スキャニングを継続的に実施し、5～20 年先の新興リスクを特定する。
2. スキャニング成果を「ホライズン・スキャニング・プログラム・チーム」（内閣府と GO-Science 合同）が評価・選別し、NSRA の「新興リスク候補」として内閣府に提出する。

3. 各省庁の LGD が担当領域のリスクについて「妥当な最悪のケース・シナリオ（RWCS）」を構築し、内閣府に報告する（2～3 年周期）。
4. 内閣府レジリエンス局が全省庁からの報告を統合し、影響度（7 次元の Harm 指標）と発生確率のマトリクスにマッピングして NSRA を作成する。
5. GCSA が NSRA の科学的妥当性レビューを行い、必要に応じて SAGE 等の専門家委員会に諮問する。
6. 完成した NSRA は機密指定の上、閣僚・省庁幹部に共有される。一般公開版として「国家リスク登録簿（NRR）」が公表される（直近版：2023 年）。
7. 地方レジリエンス・フォーラム（LRF）が NRR に基づく「コミュニティ・リスク登録簿（CRR）」を作成・公開する。

**参加主体:**

- 緊急時科学助言グループ（SAGE 等）：重大な危機が発生した際に招集
- エキスパート・チャレンジ・グループ、行動科学専門家グループ
- 自然ハザード・パートナーシップ（NHP）
- 王立アカデミー、大学研究者、産業界専門家

### 2.3.3 関係文書等

| 文書名 | 種別 | 概要 |
|---|---|---|
| 国家リスク登録簿（NRR 2023） | 公開文書 | 89 リスクを 4 カテゴリ（自然ハザード・人為的脅威・技術的ハザード・複合ハザード）に分類。発生確率・影響度のマトリクスで可視化。 |
| 国家安全保障リスク評価（NSRA） | 機密文書 | 各リスクの RWCS・政府の備え状況・対応計画を含む詳細版。内閣・省庁幹部のみ閲覧可能。 |
| UK 政府レジリエンス・フレームワーク（2022 年） | 公開戦略文書 | リスクへの対処方針、官民連携、地方自治体との役割分担等を定める。 |
| コミュニティ・リスク登録簿（CRR） | 公開文書 | 地方レジリエンス・フォーラム（LRF）が地域版 NRA として作成・公開。 |
| GO-Science Foresight Toolkit | 公開ツールキット | 公務員や専門家が将来予測を実践するためのマニュアル。 |

### 2.3.4 英国 フォーサイトの記載内容（参照・補足）

| 手法 | 根拠文書と詳細 |
|---|---|
| ① ホライズン・スキャニング（予兆の探索） | **根拠文書:** GO-Science "Foresight projects and toolkit" / Cabinet Office "National Risk Register 2023" (Methodology section)。<br>**詳細:** 内閣府と政府科学局が共同で「Horizon Scanning Programme Team」を組織。STEEP 分析のフレームワークを用い、5 年～20 年先の「弱い信号」を探索することが明記されている。政策立案者がスキャニングを行うための具体的なワークフローが「Futures Toolkit」に掲載されている。 |

| | |
|---|---|
| ② リスクの特定（LGD 方式） | **根拠文書:** Cabinet Office "The Roles of Lead Government Departments..." (2023) / UK Government Resilience Framework (2022)。<br>**詳細:**「主幹省庁（LGD）モデル」が採用されており、特定のリスクごとに責任を持つ省庁が割り当てられている（例：感染症リスクは保健社会福祉省（DHSC）、サイバー攻撃は科学・イノベーション・技術省（DSIT））。 |
| ③ 最悪想定の構築（RWCS） | **根拠文書:** Cabinet Office "National Risk Register 2023" (Technical Annex) / House of Lords: "Preparing for Extreme Risks" (2021)。<br>**詳細:**「妥当な最悪のケース・シナリオ（RWCS）」を用いることが特徴である。これは「起こり得る範囲内で最も過酷な事態（Worst plausible）」を想定するものであり、各リスクは RWCS に基づき一貫した基準で比較可能とされる。 |
| ④ 評価とマッピング（マトリックス） | **根拠文書:** Cabinet Office "National Risk Register 2023" (The Risk Matrix, p.10-15)。<br>**詳細:** 特定された RWCS は、「発生確率（Likelihood）」と「影響度（Impact）」の 2 軸で評価される。影響度は以下の 7 つの次元（Dimensions of Harm）でスコアリングされる：①死亡者数、②負傷・疾病者数、③社会的混乱（市民の不安）、④心理的影響、⑤経済的損失、⑥環境的ダメージ、⑦インフラへの影響。 |

### 2.4 調査対象国における実施事例 2 （シンガポール）

シンガポールの「戦略的先見性（Strategic Foresight）」への取り組みは国家の生存戦略の中核に据えられている。首相府（PMO）が強力な主導権を握り、官庁の縦割りを排した「政府一体（Whole-of-Government）」のアプローチを徹底している点が特徴である。

#### 2.4.1 シンガポール フォーサイト制度の概要

| 項目 | 説明 |
|---|---|
| 制度タイプと制度位置づけ | 首相府（PMO）直轄の戦略先見センター（CSF：Centre for Strategic Futures）を核とする「政府一体（Whole-of-Government）」体制。公共部門ガバナンス法（Public Sector (Governance) Act 2018）が省庁間の情報共有・横断的政策調整の法的根拠を整備している。 |
| フォーサイトの整理思想 | 単なる予測ではなく、政府全体の「先見能力」を向上させ、盲点を減らすことをミッションとする。「探索（Scanning）→深掘り（Sense-making）→戦略化（Acting）」のサイクルで運用される。「不都合な未来（Uncomfortable Futures）」シナリオを意図的に作成し、政策立案者の盲点を解消する機能を持つ。 |
| 実施枠組みと体制 | 首相府戦略グループが国家の長期的優先事項を策定する司令塔を担う。CSF が実務を担い、各省庁に配置された先見担当官（Foresight Officers）とネットワークを構築している。RAHS システムにより弱い信号の自動検知・早期警戒が行われる。 |

| 項目 | 説明 |
| --- | --- |
| NRA との接続 | ◎ 強い。NRA は「トータル・ディフェンス（Total Defence）」フレームワーク（6 要素：軍事・民間・経済・社会・デジタル・心理的防衛）の中に組み込まれている。政府リスク管理フレームワーク（Government Risk Management Framework）により、CSF の活動が「中長期リスク識別」機能として制度的に位置付けられている。 |
| 主要参照文書 | 『Foresight』レポート（CSF 発行、年次）、国家シナリオ集（内部限定）、RAHS システム、"Conversations on the Future"（PMO 発行） |

### 2.4.2 シンガポール フォーサイトの実施フロー

**プロセスの評価射程と更新サイクル:**

- 継続的スキャニング：RAHS システム及び各省庁担当官による常時モニタリング
- 駆動力分析：数年おきに更新
- 国家シナリオ：数十年先を見据えた複数シナリオ、数年ごとのサイクルで更新

**プロセス詳細フロー:**

1. RAHS システム及び各省庁の先見担当官が、継続的に「弱い信号（Weak Signals）」を収集・分類して CSF のデータベースに入力する。
2. CSF が定期的に「駆動力（Driving Forces）分析」を実施し、技術革新・地政学・人口動態など、シンガポールの将来を左右する主要要因を特定する。
3. 数十年先を見据えた「国家シナリオ（National Scenarios）」を複数構築し、閣僚・上級官僚と共有する。これが各省庁のリスク評価の前提条件（基礎シナリオ）となる。
4. CSF が「不都合な未来（Uncomfortable Futures）」シナリオを意図的に作成し、政策立案者の盲点を解消する機能を果たす。これが各省庁のリスク評価における「見落としリスク」の識別に直結する。
5. 各省庁は CSF のシナリオを前提として、所管領域の具体的リスク評価を実施し、首相府の政府リスク管理フレームワークに報告する。
6. RAHS の早期警戒データが新興リスクの早期識別を支援し、リスク評価の随時更新に貢献する。

**専門家連携:**

- 国際アドバイザリー・パネル（IAP）：世界的な思想家・技術者・元外交官等で構成。定期的にシンガポールに招かれ政府高官と議論を行う。
- CSF フェロー：学術界・民間セクターから選ばれた専門家。客観的な視点を提供する。
- RAHS プログラム：国内外の研究機関・IT 企業と連携し、データ分析・AI を用いた「兆しの自動検知」システムを共同開発・運用している。

### 2.4.3 関係文書等

- **『Foresight』レポート（CSF 発行、年次・公開）**： メガトレンド・新興技術・地政学的変化に関する分析。2024 年版は AI・気候・地政学的分断をテーマとして取り上げた。
- **国家シナリオ集（内部限定・複数年更新）**： 閣僚・上級官僚が長期戦略策定に使用する「教科書」として共有される。
- **RAHS システム（継続的・内部）**： 弱い信号の早期警戒データベースとして機能し、常時リスク分析の基盤となる。

- **政策実装事例**：食料安全保障「30 by 30」目標（国内生産 30%を 2030 年までに達成）、サイバーセキュリティ庁（CSA）設立、デジタル経済協定（DEA）推進等がフォーサイト活動の直接的成果として記録されている。

### 2.5 調査対象国における実施事例 3（フィンランド）

フィンランドは、議会・政府・独立機関の三層構造によるフォーサイト体制を世界に先駆けて制度化した国である。4 年ごとに「将来に関する政府報告書」を議会に提出することが慣行として定着しており、将来予測を政治サイクルに組み込む独自のモデルを形成している。

#### 2.5.1 フィンランド フォーサイト制度の概要

| 項目 | 説明 |
|---|---|
| 制度タイプと制度位置づけ | 議会（将来委員会）・政府（首相府先見グループ）・独立機関（Sitra）の三層構造。危機管理法、総合安全保障に関する政府決議（YTS）、安全保障委員会設置根拠法令が法的根拠を構成する。 |
| フォーサイトの整理思想 | 政治サイクル（4 年）にフォーサイトを組み込む独自モデル。Sitra のメガトレンド分析（2～3 年周期）と VTT 技術フォーサイトを共通プラットフォームとして活用し、政府・民間・市民社会が共有する将来認識を形成する。 |
| 実施枠組みと体制 | 議会将来委員会（世界唯一の常設議会将来委員会、1993 年設置）が政府報告書を審議・評価する。首相府先見グループが 4 年ごとの「将来に関する政府報告書」の起草を主導する。Sitra が「メガトレンド（Megatrendit）」報告書を 2～3 年周期で更新し、共通プラットフォームとして機能する。 |
| NRA との接続 | ○ 中程度。内務省が主導し、安全保障委員会が調整する NRA プロセスに対し、Sitra や VTT の知見が「長期リスクの文脈情報」として提供される。包括的安全保障戦略（YTS）への統合プロセスが確立している。 |
| 主要参照文書 | 将来に関する政府報告書（4 年周期）、Sitra メガトレンド報告書（Megatrendit）、国家リスクアセスメント（Kansallinen riskiarvio）、社会の安全保障戦略（YTS） |

#### 2.5.2 フィンランド フォーサイトの実施フロー

フィンランドのフォーサイト・プロセスは、4 年周期の「政府フォーサイト・サイクル」と継続的なスキャニング活動が並行して運用されている。

**評価射程と更新サイクル:**

- メガトレンド分析（Sitra）：2～3 年周期で更新
- 技術フォーサイト（VTT）：継続的に実施
- 将来に関する政府報告書：4 年周期（政治サイクルに同期）
- 国家リスクアセスメント（NRA）：内務省が定期的に策定

**プロセス詳細フロー:**

1. Sitra のメガトレンド分析・VTT の技術フォーサイト等を活用した常時トレンド収集・環境スキャニングを実施する。
2. 首相府先見グループが省庁横断的な分析セッションを開催し、各省庁の長期課題を統合する。

3. 市民参加、専門家ヒアリング、シナリオ・プランニングを組み合わせ、4 年ごとの「将来に関する政府報告書」を起草する。
4. 議会将来委員会が報告書を審議・評価し、「将来委員会の報告書」として回答する（年間 100 件以上の将来調査・評価を実施）。
5. 審議結果が政府の中期プログラム・戦略・予算に反映され、モニタリングが継続される。
6. 内務省の NRA に対し、Sitra や VTT の長期リスク分析が背景情報として提供される。その後、総合安全保障戦略（YTS）に統合される。

### 2.5.3 関係文書等

- **将来に関する政府報告書（Government Foresight Report）**：4 年ごとに首相府が起草し議会に提出する政府全体の将来展望文書。
- **Sitra メガトレンド報告書（Megatrendit）**：2～3 年周期で更新。2023 年版では「生態系の危機」等 5 つのトレンドを特定。
- **国家リスクアセスメント（Kansallinen riskiarvio）**：内務省が策定する公開文書。
- **社会の安全保障戦略（Yhteiskunnan turvallisuusstrategia : YTS）**：政府横断的な包括戦略。

## 2.6 調査対象国における実施事例 4（オランダ）

オランダは、独立性の高い複数の専門評価機関がフォーサイトを担い、長期的な知見を通じて国家リスク評価（NRA）を補完する体制を構築している。

### 2.6.1 オランダ フォーサイト制度の概要

| 項目 | 説明 |
|---|---|
| 制度タイプと制度位置づけ | 独立した専門評価機関複数体制。安全地域法（Wet veiligheidsregio's 2010）および国家安全保障戦略が法的根拠を構成する。NRA（国家リスクアセスメント：NRB）は NCTV（国家テロ・治安調整官）が 2～3 年周期で実施する。 |
| フォーサイトの整理思想 | 独立機関の科学的勧告を重視する体制。DESTEP フレームワーク（社会・経済・文化・技術・環境・政治の 6 軸）による駆動力分析と、「重要不確実性」の選定を組み合わせたシナリオ構築アプローチが採用されている。 |
| 実施枠組みと体制 | オランダ環境評価庁（PBL）が環境・空間計画分野のシナリオ構築を担う。オランダ科学評議会（WRR）が長期横断的な政策課題に関する勧告報告書を作成する。オランダ科学・技術未来研究所（STT）が「ホライズン・スキャン 2050」を実施する。 |
| NRA との接続 | ○ 中程度。NCTV が実施する NRB（2～3 年周期）に対し、独立機関の長期シナリオ（2030/2050 年）が背景文脈として参照される。直接統合ではなく補完的・間接的な接続関係にある。 |
| 主要参照文書 | PBL「Netherlands in 2030」、WRR 政策勧告報告書、NCTV NRB、STT「Horizon Scan 2050」 |

### 2.6.2 オランダ フォーサイトの実施フロー

**評価射程と更新サイクル:**

- シナリオ分析（PBL）：2030 年・2050 年を対象とした長期シナリオ
- ホライズン・スキャン（STT）：2050 年を対象
- NRB（NCTV）：2～3 年周期で更新

**プロセス詳細フロー（PBL 事例）:**

1. 準備フェーズ：範囲・目的の設定とステークホルダー協議を実施する。
2. DESTEP 分析：社会・経済・文化・技術・環境・政治の 6 軸で駆動力を幅広く収集する。
3. 重要不確実性の選定：影響度と不確実性が高い要素を選び、2 軸のマトリクスを構築する。
4. シナリオ・ナラティブ構築：定性的ストーリーを作成し、定量的裏付けを付加する。
5. ホライズン・スキャン：文献調査やワークショップで「未知の未知」を含む信号を収集する。
6. 政府・議会・社会に対して勧告・公表し、NRB の長期文脈として参照される。

### 2.7.3 関係文書等

- **PBL「Netherlands in 2030」**: 環境・空間計画分野の長期シナリオ分析報告書。
- **WRR 政策勧告**: デジタル化・気候変動等の横断的政策課題に関する勧告。
- **NCTV 国家リスクアセスメント（NRB）**：2～3 年周期で更新されるオランダの公式 NRA 文書。
- **STT「Horizon Scan 2050」**: グランド・チャレンジを特定するホライズン・スキャン報告書。

## 2.7 調査対象国における実施事例 5（米国）

米国は、各省庁が独自の手法を確立する分散型・省庁横断体制でフォーサイト活動を実施しており、政府全体を覆う単一の国家フォーサイト制度は存在しない。特定分野（諜報、技術、防衛等）における先見活動は世界最高水準にある一方、それらを統合する制度的メカニズムは発展途上・分散型の段階にある。

### 2.7.1 米国 フォーサイト制度の概要

| 項目 | 説明 |
|---|---|
| 制度タイプと制度位置づけ | 分散型・省庁横断体制。国土安全保障法（2002 年）、情報改革・テロ防止法（2004 年）、大統領政策指令第 8 号（PPD-8）が関連法的根拠を構成する。 |
| フォーサイトの整理思想 | 機関ごとに手法が異なる。NIC は 4 年周期の「Global Trends」報告書を通じた長期地政学的先見。USCG は「プロジェクト・エバーグリーン」による 20 年先の戦略的先見。FFCOI が省庁間の知見共有ハブとして機能する。 |
| 実施枠組みと体制 | 国家情報会議（NIC）が 4 年ごとに「Global Trends」を刊行。沿岸警備隊（USCG）が「プロジェクト・エバーグリーン」を実施。疾病対策センター（CDC）が「4 アーキタイプ・フューチャーズ手法」による新興リスク探知を担当。陸軍 TRADOC（戦力近代化司令部）がクラウドソーシング型「マッド・サイエンティスト・ラボラトリー」を運用する。連邦フォーサイト・コミュニティ・オブ・インタレスト（FFCOI）が省庁間の知見共有ハブとして機能する。 |
| NRA との接続 | △ 弱い。統一 NRA は存在せず、FEMA の THIRA（能力目標設定・資源評価）、DHS の NRCA（国家リスク能力評価）、ODNI/NIC の NIE（国家情報評価）が並立する体制となっている。 |

| 項目 | 説明 |
|---|---|
| 主要参照文書 | NIC「Global Trends 2040」、FFCOI 公式サイト、DHS NRCA、CDC 戦略的先見報告書 |

### 2.7.2 米国 フォーサイトの実施フロー

**評価射程と更新サイクル:**

- NIC「Global Trends」：4 年周期で更新（大統領選挙サイクルに対応）
- USCG「プロジェクト・エバーグリーン」：4 年周期で実施

**プロセス詳細フロー（NIC 事例）：**

1. 構造的な力（Structural Forces）の分析：長期にわたり世界を形成する人口・経済・環境・技術的な基盤的要因を分析する。
2. 新興ダイナミクス（Emerging Dynamics）の特定：短～中期に重要性を増す新たな潮流や変化を特定する。
3. 代替シナリオの構築：上記要因の組み合わせに基づき、複数の代替的な未来シナリオを構築する。
4. 主要な不確実性の整理：シナリオを左右する分岐点となる重要な不確実性を整理・提示する。

**プロセス詳細フロー（USCG「プロジェクト・エバーグリーン」）：**

1. センシング（Sensing）：世界的な変化の兆候を幅広く収集する。
2. エンビジョニング（Envisioning）：複数の未来像を構築する。
3. ワークショップ（Gaming）：シナリオに基づく演習・ゲームを実施し、組織の対応能力を検証する。
4. ストラテジャイジング（Strategizing）：演習結果をもとに戦略的優先事項を策定する。

### 2.7.3 関係文書等

- **NIC「Global Trends 2040」（公開文書）**：4 年ごとに刊行される長期地政学的展望報告書。
- **DHS 国家リスク能力評価（NRCA）**：DHS が実施するリスク評価文書。
- **FEMA THIRA（能力目標設定・資源評価）**：FEMA が実施する地域・国家レベルの能力評価。
- **CDC 戦略的先見報告書**：公衆衛生分野の長期リスク予測。
- **FFCOI 公式サイト**：省庁横断的な先見活動のコミュニティ・オブ・インタレスト。

## 2.8 調査対象国における実施事例６（ドイツ）

ドイツのフォーサイト活動は、連邦教育研究省（BMBF）とフラウンホーファーISI（Fraunhofer ISI）による厳格な品質管理・技術・イノベーション重視の体制が特徴である。安全保障リスク分析（BBK 所管）とフォーサイト活動の制度的連携は限定的な段階にある。

### 2.8.1 ドイツ フォーサイト制度の概要

| 項目 | 説明 |
|---|---|
| 制度タイプと制度位置づけ | 技術・イノベーション重視の体制。民間保護・災害支援法（ZSKG）が安全保障リスク分析の法的根拠を構成する。フォーサイトは連邦教育研究省（BMBF）が政策的主体として監督し、フラウンホーファーISI（Fraunhofer-Institut für System- und Innovationsforschung）が実務機関として実施する。 |
| フォーサイトの整理思想 | 厳格な品質管理による「弱い信号（Weak Signals）」の検出を重視する。収集データから専門家が約 2%を有効信号として認定し、月約 30 件のトップ信号を選定・ |

| 項目 | 説明 |
| --- | --- |
| | 深掘りするプロセスを採用している。 |
| 実施枠組みと体制 | BMBF フォーサイト・プロセスはサイクル I（専門家調査・デルファイ調査・発明家スカウティング・サイエンス・マップ）とサイクル II（社会トレンドのプロファイル分析・「未来からの物語」構築）から構成される。 |
| NRA との接続 | △ 弱い。連邦市民保護・災害支援局（BBK）が民間保護リスク分析を担当するが、BMBF の技術フォーサイトと BBK のリスク分析は行政的に独立した別プロセスとして運用されている。技術フォーサイト成果が新興技術リスク評価で参照されることはあるが、制度的連携は限定的である。 |
| 主要参照文書 | BMBF フォーサイト報告書、BBK 民間保護リスク分析、Fraunhofer ISI 月次弱い信号レポート |

### 2.8.2 ドイツ フォーサイトの実施フロー

**評価射程と更新サイクル:**

- BMBF フォーサイト・サイクル I・II：複数年サイクルで実施
- 弱い信号選定：月次（月約 30 件のトップ信号を選定）

**プロセス詳細フロー（BMBF フォーサイト・プロセス）:**

1. サイクル I - 情報収集：専門家調査、デルファイ調査（Delphi Survey）、発明家スカウティング（新興技術の特定）、サイエンス・マップ（論文引用分析による研究動向可視化）を実施する。
2. サイクル I - バリデーション：収集データから専門家が一次バリデーションを行い、約 2%を有効な「弱い信号」として認定する。
3. 月次選定：月次でトップ信号（約 30 件）を選定し、ISI 内部データベースに格納する。
4. 専門家ワークショップ：選定された信号について専門家ワークショップを開催し、社会的インパクトの文脈に落とし込む。
5. サイクル II - シナリオ統合：社会トレンドのプロファイル分析を行い、「未来からの物語（Stories from the Future）」を構築する。
6. BBK への参照：新興技術に関連するリスクが特定された場合、BBK の民間保護リスク分析において参照されることがある（制度的義務ではなく任意の参照）。

### 2.8.3 関係文書等

- **BMBF フォーサイト報告書（BMBF Foresight）**： 連邦教育研究省が刊行する技術・イノベーション先見報告書。
- **BBK 民間保護リスク分析（Risikoanalyse im Bevölkerungsschutz）**： 連邦市民保護・災害支援局が実施するリスク分析報告書。
- **Fraunhofer ISI 月次弱い信号レポート**: ISI が内部的に整理・共有する月次信号選定レポート。

## 2.9 調査対象国における実施事例 7 （スウェーデン）

スウェーデンのフォーサイト活動は、イノベーション機関主導・先端技術（AI 等）活用の体制が特徴であり、民間緊急事態庁（MSB）による国家リスク・脆弱性分析（RVA）との接続強化が現在の課題となっている。

### 2.9.1 スウェーデン フォーサイト制度の概要

| 項目 | 説明 |
|---|---|
| ① 制度タイプと制度位置づけ | イノベーション機関主導型。総合防衛法（LSO 2003:778）および国家安全保障戦略（2017 年）が関連法的根拠を構成する。 |
| ② フォーサイトの整理思想 | AI を活用した大規模環境スキャニング、エッジ・ケース観察（統計的外れ値を将来の前触れとして分析）、スペキュラティブ・デザイン、SESTA フレームワーク（システム思考・環境スキャニング・トレンド分析の統合）などの先端技術を積極的に活用する。 |
| ③ 実施枠組みと体制 | Vinnova（イノベーション庁）が 10～20 年先の技術・イノベーション方向性の探索を担う。MSB（民間緊急事態庁）が国家リスク・脆弱性分析（RVA）を策定する。FOI（防衛研究所）が地政学・新興軍事技術の先見的分析を担当する。SIPA（スウェーデン未来研究所）がスペキュラティブ・デザインを活用したシナリオ可視化を担当する。 |
| ④ NRA との接続（接続強度：△） | MSB が国レベルの RVA を策定する。各機関のフォーサイトが個別 NRA を経て MSB へ統合される経路はあるが、体系的な反映メカニズムは整備途上である。近年、長期新興リスクの組み込みを強化中。 |
| ⑤ 主要参照文書 | Vinnova イノベーション・フォーサイト報告書（「技術の将来」シリーズ）、MSB 国家リスク・脆弱性分析（RVA）、FOI Memo シリーズ、国家安全保障戦略（2017 年） |

### 2.9.2 スウェーデン フォーサイトの実施フロー

**評価射程と更新サイクル:**

- Vinnova イノベーション・フォーサイト：10～20 年先を対象
- MSB RVA：定期的に更新

**プロセス詳細フロー:**

1. AI 活用スキャニング：Vinnova が自動テキスト解析等の AI ツールを活用し、大規模な兆候探索を実施する。
2. エッジ・ケース観察：統計的外れ値を将来の前触れとして分析し、通常の予測手法では見落とされるリスクを特定する。
3. SESTA フレームワーク適用：システム思考、環境スキャニング、トレンド分析を統合したフレームワークを活用して分析を行う。
4. スペキュラティブ・デザイン（SIPA）：不確実な未来を視覚的に描写し、政策立案者の思考を刺激するシナリオを作成する。
5. RVA への統合：MSB が各機関のフォーサイト成果を収集し、国家リスク・脆弱性分析（RVA）に反映する（現状では体系的メカニズムは整備途上）。

### 2.9.3 関係文書等

- **Vinnova イノベーション・フォーサイト報告書（「技術の将来」シリーズ）**：イノベーション庁が刊行する技術先見報告書。

- **MSB 国家リスク・脆弱性分析（RVA）**： 民間緊急事態庁が策定する国家レベルのリスク・脆弱性分析文書。
- **FOI Memo シリーズ**: 防衛研究所が刊行する地政学・安全保障に関する先見的分析文書。
- **国家安全保障戦略（2017 年）**： スウェーデンの安全保障政策の基本戦略文書。

以上