仕様書（案）

１．件名

令和５年度化学物質安全対策（ナノ材料等に関する国内外の安全情報及び規制動向等に関する調査）

２．背景と目的

ナノ材料を含む先端材料（アドバンストマテリアル。以下、「AdMa」という。）は、様々な社会課題の解決に資するものとして、我が国産業においても一層の利用拡大が見込まれている一方、AdMa はその複雑で革新的な構造と組成のために、人の健康や環境への影響が懸念されている。経済協力開発機構（OECD）の工業ナノ材料作業部会（以下、「WPMN」という。）では、2021-2024 年の新たなアクションプランにおいて AdMa に関する新たな化学物質管理について議論を加速化することを決定している。また、国際標準化機構（ISO）においても、TC229（ナノテクノロジー）において、AdMa について検討が開始されている。他方、ナノ材料に関しては、米国の有害物質規制法（TSCA）では 2017 年にナノスケール材料の報告制度が開始され、欧州においても REACH 制度において 2020 年よりナノフォームの登録が開始されている。

内分泌かく乱物質は、人及び野生動物の内分泌機能を阻害又は活性化させることで健康に有害な影響を及ぼすものであるが、わずかなばく露量で健康に多大な影響を与えうる。一方で、作用機序等に係る科学的知見・根拠が明確にはなっていないが、欧州等において規制のあり方等に関する議論が進められている。

このような国際的な潮流の中で、我が国としても国内産業への影響も考慮しつつ、AdMa や内分泌かく乱物質に関して、迅速かつ適切に対応していく必要がある。

本事業では、AdMa について、国内における製造・輸入・使用等の状況、安全管理として必要とされる情報等の調査、化学物質管理及び規制の動向について国外の規制機関における対応状況についての情報収集・分析、国際会議に参画する我が国専門家の活動の支援や関連会合への対応等を行うとともに、内分泌かく乱物質について、国内外の新たな化学物質管理、規制措置等に関する情報収集等を行うことを目的とする。

３．調査内容及び調査方法

３－１．ナノ材料の安全管理に関する調査

OECD や欧米等の動向を踏まえて、ナノ材料やその安全管理に必要とされる情報を調査する。

具体的には、国内におけるナノ材料の製造・輸入・使用等の状況、安全管理に必要とされる情報等を調査する。この結果を踏まえ、ナノマテリアル情報収集・

発信プログラムで収集・公表している情報の妥当性を検討するとともに、対象とすべきナノ材料や収集すべき情報の有無や情報発信方法などの課題について検討を行う。
　なお、原則、OECD における定義や勧告等を踏まえた範囲を対象とするが、ナノマテリアル情報収集・発信プログラムにおける情報収集内容との重複を除く 。

３－２．工業ナノ材料作業部会（WPMN）等の国際会議に係る対応支援等
　以下に記載の国際会議に対応するため、過去の議論等の経緯を整理するとともに、必要な情報収集、分析を行い、国際会議等での支援を行う。各会議の終了後は議論の概要を整理する。

＜対応する国際会議＞
・第 23 回 WPMN 会合（フランス・パリ）
　2 名程度参加し、その議事・議論等について準備・情報収集・分析を行うなど必要なサポートを行う。また、必要なコメント等を英文にて作成する。
・WPMN 配下の作業グループである SG8（ばく露関連）、SGTA（テストガイドライン関連）、SIA（Safe-by-design 関連）、AdMa を含めた専門家会合
　国内専門家の派遣や電話会議への参加等（４回程度を想定）により、テストガイドラインの改定・作成の進捗、試験プログラムの作成状況、各国の取組状況等の情報収集を行い整理する。また、必要なコメント等を英文にて作成する。
・必要に応じ、上記会合以外にも、AdMa、Safe-by-design に関するテーマ会議・ワークショップ等について、その議事・議論等の情報収集・分析を行うなど、WPMN 対応に必要なサポートを行う。

　なお、関連する会合の場においては、質問・意見等を受けたり技術的な内容の説明を行うことも想定されるため、対応者は英語の議論の参加に加えて当該会合に関係する専門用語も理解できる者とする。
　また、会合への参加、作成する資料、関連資料の翻訳等の対応については、派遣される国内専門家、化学物質管理課と相談の上、決定する。
　さらに、現地開催における会議への参加や国内専門家の派遣については、コロナの蔓延状況や主催機関の方針等をよく見極め、経済産業省化学物質管理課と相談の上、参加の可否について判断する。

３－３．AdMa 及び化学物質の内分泌かく乱作用に関する対応
　３－２．の対応に係る情報等を収集するため、OECD 等で議論されている AdMa 及び化学物質の内分泌かく乱物質に関する化学物質管理、規制等の動向及び安全性情報を収集・整理する。収集した情報は、既知見の情報を踏まえて内容毎に整理し直し、調査報告書に取りまとめること。

（１）AdMa に関する調査

AdMa(混合物・複合材を含む)における下記１）～３）の情報について、米国及び EU（欧州連合）の他、ドイツ、フランス、オランダ、英国、カナダ、アジア諸国（中国・韓国等）等を中心に情報収集を行う。また、日本国内および他国においても大きな規制等の動きがあった場合には情報を収集する。整理にあたっては、適宜図表を盛り込むこととする。

情報の収集にあたっては、インターネット及び文献による調査等を中心に行う。調査結果は、３ヶ月毎に取りまとめ、経済産業省に報告を行うこととする。

なお、経済産業省化学物質管理課から AdMa に関して特定の規制動向について情報収集の要望があった際は、それに応じること。

１）ナノ材料及び AdMa の定義、規制やガイダンスの制定・改廃動向について

ナノ材料及び AdMa の定義、また人健康・環境安全に係る規制等について、米国及び EU を中心に、現状及び今後の方向性について情報収集・分析を行い、整理する。

国際的な定義の確立は各国の規制の方向性を大きく左右するものであり、幅広い製品分野のグローバルな取引にも影響することから、ナノ材料及び AdMa の定義や安全性に関する情報を収集する。

欧州においては、欧州化学品庁（ECHA）で各種ガイダンスの更新等が進められており、今後の規制動向や WPMN の各種プロジェクトの進捗等に特に注目して情報収集を行う。

また、米国においては、米国環境保護庁（EPA）が提案した、多層カーボンナノチューブ（CNT）に関する重要新規利用規則（SNUR）の結果など、ナノ材料に対する規制の動向について注目して情報収集を行う。

あわせて、より短期間に試験法導入が可能と見込まれる ISO 等の取組状況についても把握していく。

なお、国内についても、ナノ材料を中心に AdMa に関係する規制の動きがあった場合には情報を収集する。

２）AdMa の安全性に関する検討状況

欧州、米国及び国内における AdMa の安全性に係る文献や研究機関等が発表した報告書等について、特にインパクトが大きい案件について情報を収集し、その内容を要約して整理する。特にナノ材料に関しては計測方法・定義・カテゴリー化等に着目する。

有害性情報については、特に日本での製造量が多い CNT、シリカ、二酸化チタン等やその他 OECD で議論されているナノ材料について注目し情報収集する。CNT については、研究により物理化学的性状ごとに毒性が異なることが指摘される一方、共通の毒性を指摘する声もあり、CNT の安全性に関する研究は依然として活発である。日本では CNT の製品化が進んでいるが、欧州では規制の動きもあり、安全性に関する最新情報の収集にも努

める。

３）AdMa に関連した設計段階からの安全性確保（safe-by- design）に関する取組状況

OECD やドイツ、オランダ、英国、カナダ等を中心に AdMa に対する規制での取り扱い、なかでも安全性に対応するための safe-by-design に対する取組み等の議論が活発化している。この点を中心に AdMa の規制動向について情報収集を行う。

（２）化学物質の内分泌かく乱作用に関する調査

化学物質の内分泌かく乱作用については、欧州及び米国を中心に規制動向の情報収集し、欧米での報告制度等について比較する等の整理を行う。

情報の収集にあたっては、独立行政法人製品評価技術基盤機構（NITE）のケミマガ（https://www.nite.go.jp/chem/shiryo/chemimaga.html）等を利用してトピックを抽出し、既知見の情報を踏まえて年１回（年度末）体系的に整理する。整理にあたっては、適宜図表を盛り込むこと。

なお、経済産業省化学物質管理課から特定の規制動向について情報収集の要望があった際は、それに応じること。

４．調査実施期間

委託契約締結日から令和６年３月１５日までとする。

５．納入物

・調査報告書電子媒体（CD-R）　１式

➢調査報告書、調査で得られた元データ、委託調査報告書公表用書誌情報（様式１）、二次利用未承諾リスト（様式２）を納入すること。

➢調査報告書については、PDF 形式に加え、機械判読可能な形式のファイルも納入すること。

➢調査で得られた元データについては、機械判読可能な形式のファイルで納入することとし、特に図表・グラフに係るデータ（以下「EXCEL 等データ」という。）については、EXCEL 形式等により納入すること。

なお、様式１及び様式２は EXCEL 形式とする。

・調査報告書電子媒体（CD-R）　２式（公表用）

➢調査報告書及び様式２（該当がある場合のみ）を一つの PDF ファイル（透明テキスト付）に統合したもの、並びに公開可能かつ二次利用可能な EXCEL 等データを納入すること。

➢セキュリティ等の観点から、経済産業省と協議の上、非公開とするべき部分については、削除するなどの適切な処置を講ずること。

➢調査報告書は、オープンデータ（二次利用可能な状態）として公開されることを前提とし、経済産業省以外の第三者の知的財産権が関与する内容を報告書に

盛り込む場合は、①事前に当該権利保有者の了承を得、②報告書内に出典を明記し、③当該権利保有者に二次利用の了承を得ること。二次利用の了承を得ることが困難な場合等は、下記の様式２に当該箇所を記述し、提出すること。
➢公開可能かつ二次利用可能な EXCEL 等データが複数ファイルにわたる場合、１つのフォルダに格納した上で納入すること。
◆各データのファイル名については、調査報告書の図表名と整合をとること。
◆Excel 等データは、オープンデータとして公開されることを前提とし、経済産業省以外の第三者の知的財産権が関与する内容を含まないものとすること。

※調査報告書電子媒体の具体的な作成方法の確認及び様式１・様式２のダウンロードは、下記 URL から行うこと。
https://www.meti.go.jp/topic/data/e90622aj.html

６．納入先
経済産業省製造産業局化学物質管理課化学物質リスク評価室

７．不開示情報の取り扱い
（１）情報管理体制
①受注者は本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報セキュリティを確保するための体制を定めた書面（情報管理体制図）」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職等が記載されたもの）別紙様式を契約前に提出し、担当課室の同意を得ること（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。）。なお、情報取扱者名簿は、委託業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。
（確保すべき履行体制）
契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、経済産業省が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。
②本事業で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならないものとする。ただし、担当課室の承認を得た場合は、この限りではない。
③①の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め担当課室へ届出を行い、同意を得なければならない。

（２）履行完了後の情報の取扱い
国から提供した資料又は国が指定した資料の取扱い（返却・削除等）については、担当職員の指示に従うこと。業務日誌を始めとする経理処理に関する資料については適切に保管すること。

８．情報セキュリティに関する事項

業務情報を取り扱う場合又は業務情報を取り扱う情報システムやウェブサイトの構築・運用等を行う場合、別記１「情報セキュリティに関する事項」を遵守し、情報セキュリティ対策を実施すること。

（別記１）

情報セキュリティに関する事項

以下の事項について遵守すること。

1)　受託者は、契約締結後速やかに、情報セキュリティを確保するための体制並びに以下 2)～18)に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、経済産業省（以下「当省」という。）の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、定期的に、情報セキュリティを確保するための体制等及び対策に係る実施状況を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。
なお、報告の内容について、担当職員と受託者が協議し不十分であると認めた場合、受託者は、速やかに担当職員と協議し対策を講ずること。

2)　受託者は、本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施すること。

3)　受託者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、当省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

4)　受託者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく当省外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。

5)　受託者は、本業務を終了又は契約解除する場合には、受託者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去すること。その際、担当職員の確認を必ず受けること。

6)　受託者は、契約期間中及び契約終了後においても、本業務に関して知り得た当省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。なお、当省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供すること。

7)　受託者は、本業務の遂行において、情報セキュリティが侵害され、又はそのおそれがある場合の対処方法について担当職員に提示すること。また、情報セキュリティが侵害され、又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

8)　受託者は、「経済産業省情報セキュリティ管理規程（平成 18･03･22 シ第 1 号）」、「経済産業省情報セキュリティ対策基準（平成 18･03･24 シ第 1 号）」及び「政府機関等のサイバーセキュリティ対策のための統一基準群（令和３年度版）」（以下「規程等」と総称する。）を遵守すること。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

9)　受託者は、当省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行うこと。

10)　受託者は、本業務に従事する者を限定すること。また、受託者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報を担当職員に提示すること。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示すること。

11)　受託者は、本業務を再委託（業務の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記 1)から 10)まで及び 12)から 18)までの措置の実施を契約等により再委託先に担保させること。また、1)の確認書類には再委託先に係るものも含むこと。

12)　受託者は、外部公開ウェブサイト（以下「ウェブサイト」という。）を構築又は運用するプラットフォームとして、受託者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。また、ウェブサ

イト構築時においてはサービス開始前に、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。

13)　受託者は、ウェブサイトを構築又は運用する場合には、インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。
なお、必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

14)　受託者は、ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に基づくこと。また、ウェブアプリケーションの構築又は更改時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施すること。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出すること。なお、チェックリストの結果に基づき、担当職員から指示があった場合は、それに従うこと。

15)　受託者は、ウェブサイト又は電子メール送受信機能を含むシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「.go.jp」を使用すること。

16)　受託者は、情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施すること。
①各工程において、当省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

②情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当省と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。

③不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。

④情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。

⑤サポート期限が切れた又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。

⑥電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）等のなりすましの防止策を講ずるとともにSMTPによるサーバ間通信のTLS（SSL）化やS/MIME 等の電子メールにおける暗号化及び電子署名等により保護すること。

17)　受託者は、本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ソーシャルメディアサービスを含む）を利用する場合には、これらのサービスで要機密情報を扱ってはならず、8）に掲げる規程等に定める不正アクセス対策を実施するなど規程等を遵守すること。なお、受託者は、委託業務を実施するに当たり、クラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）」において登録されたサービスから調達することを原則とすること。

18)　受託者は、ウェブサイトの構築又はアプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行うこと。
①提供するウェブサイト又はアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。
（a）ウェブサイト又はアプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。
（b）アプリケーションプログラムを提供する場合には、当該アプリケーション

の仕様に反するプログラムコードが含まれていないことを確認すること。
（c）提供するウェブサイト又はアプリケーション・コンテンツにおいて、当省外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させるなどして確認すること。

②提供するウェブサイト又はアプリケーションが脆弱性を含まないこと。

③実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。

④電子証明書を用いた署名等、提供するウェブサイト又はアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをウェブサイト又はアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

⑤提供するウェブサイト又はアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、ウェブサイト又はアプリケーション・コンテンツの提供方式を定めて開発すること。

⑥当省外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がウェブサイト又はアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をウェブサイト又はアプリケーション・コンテンツに組み込む場合は、当省外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該ウェブサイト又はアプリケーション・コンテンツに掲載すること。