



**「NEDO懸賞金活用型プログラム
「課題①新たなサイバーセキュリティの技術」
「課題②量子計算機時代のブロックチェーンシステムの安全性確保技術」
に係る周辺動向調査及び事業運営支援業務」に関するご説明**

2026年3月18日

国立研究開発法人 新エネルギー・産業技術総合開発機構

半導体・情報インフラ部

目次

1. 全体スケジュール 15:00~15:05(5分)
2. 懸賞金課題およびスケジュール
15:15~15:30(25分)
3. 応募における注意点 15:30~15:40(5分)
4. Q&A 15:40~16:00(15分)

新たなサイバーセキュリティの技術

- 1 中小企業を含めた様々な企業のセキュリティ強化に資する**安価な国産ツールの開発**
- 2 懸賞金型により**有望な技術力・競争力を有する製品・サービスの実績形成と認知拡大を促進**
- 3 **スタートアップ企業等の市場参入**（政府調達やSIerとのマッチング等）を後押し

今後の成長に向けた課題（As-Is）

導入実績が重視される商慣習

- 新規製品が販売されても、実績が重視されるため、調達先が存在せず、事業として成り立たないため、企業が育たない

十分な開発投資が行われにくい事業環境

- 安定的な収益基盤が見通しづらいため、製品開発・研究開発への投資が限られる
- セキュリティ製品の販売はSIerが商流を担っており、製品ベンダーで対応できる余地は限られている

目指すべき方向性（To-Be）と実現のための主な政策対応

スタートアップ等が実績を作りやすくなる／有望な製品・サービスが認知される

- 政府機関等が有望なスタートアップ等の製品・サービスを試行的に活用
- 有望な製品・サービス・企業の情報を集約・リスト化し、政府機関等へ情報展開する／業界団体とも連携して審査・表彰を実施

有望な技術力・競争力を有する製品・サービスが創出され、発掘されやすくなる

- セキュリティ関連の技術・社会課題解決に貢献する技術・事業を発掘するための「コンテスト形式」による**懸賞金事業**等を実施
- 我が国商流の中心である**SIerと国産製品・サービスベンダーとのマッチング**の場を創出

AI, SBOM, SSDFについて、汎用的かつ高度なセキュリティソリューションを募集

第9回産業サイバーセキュリティ研究会事務局説明資料を参考に作成

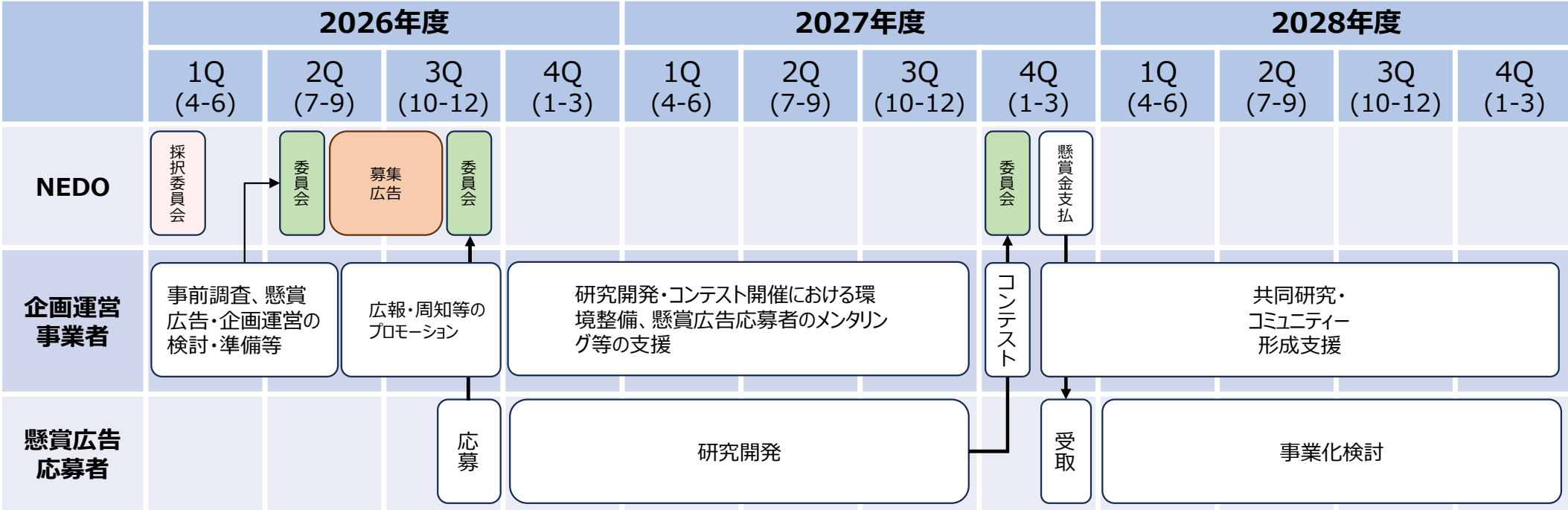
懸賞金事業（課題）の目的・狙い：サイバーセキュリティを取り巻く技術・政策動向を踏まえた上で、国内のサイバーセキュリティの対応力向上

想定する非金銭的支援の内容：伴奏支援（マッチングイベントなど）

想定される参加者像：日本の法人格を有する民間企業、大学・公的研究機関等（スタートアップ等を含む）

コンテスト終了後の展開【P】：ビジネスマッチング／有望な製品・サービス・企業の情報を集約・リスト化し、政府機関等へ情報展開する／業界団体とも連携して審査・表彰を実施／政府調達等

懸賞金事業スケジュール 新たなサイバーセキュリティの技術



課題名:量子計算機時代のブロックチェーンシステムの安全性確保技術



METI イノベーション政策課
NEDO 半導体情報インフラ部

- 1 暗号資産等で広く用いられているブロックチェーン技術に関する耐量子計算機暗号への移行技術の提供
- 2 多様化するブロックチェーンの鍵管理方式について標準化に資する安全かつ効率的な方式の開発

今後の成長に向けた課題 (As-Is)

ブロックチェーンの耐量子化が必要

- 社会生活の基盤として広くブロックチェーンが使われる中、量子計算機の発展により、当初想定されていた安全性が確保できない(危殆化)が懸念されている

乱立した多様な鍵管理方式

- ブロックチェーンでは、暗号の有効期限に基づく鍵管理が難しく、セキュリティインシデントの原因となっている

目指すべき方向性 (To-Be) と実現のための主な政策対応

耐量子 (PQC) ブロックチェーンへの移行技術の確立

- 広く使われているブロックチェーンの耐量子化のための移行技術の創出
- 懸賞金事業により現在提案されている移行技術よりも効率的な技術を開発

標準化に資する多様かつ安全なブロックチェーン鍵管理技術の確立

- 多様化した鍵管理技術を評価し、ブロックチェーンを安全に活用する基盤となる方式を開発
- 多様な方式からより安全かつ効率的な技術を発掘するために懸賞金事業を実施

重点分野 耐量子計算機暗号への移行技術 多様かつ高度な鍵管理技術

懸賞金事業(課題)の目的・狙い:安全かつ柔軟なブロックチェーン活用基盤技術を確立を目的とする。単体の暗号技術の安全性の確保においては、国際的なコンペティション等のプロセスを通じ、安全な技術の選定が行われている。ブロックチェーンのような応用技術においても、多様な安全技術を創出しつつも、標準化を見据えた技術選定を行うためには、コンペティション等を通じた技術開発が有効である。また、ブロックチェーンの応用(暗号資産等)に関しては、フィンテックなどの比較的小さな企業が単独で課題解決することが難しく、政府が技術開発を支援する必要がある。

想定する非金銭的支援の内容:伴走支援(マッチングイベント、教育プログラム、テストベッドの提供など)

想定される参加者像:日本の法人格を有する民間企業、大学・公的研究機関等(スタートアップ等を含む)

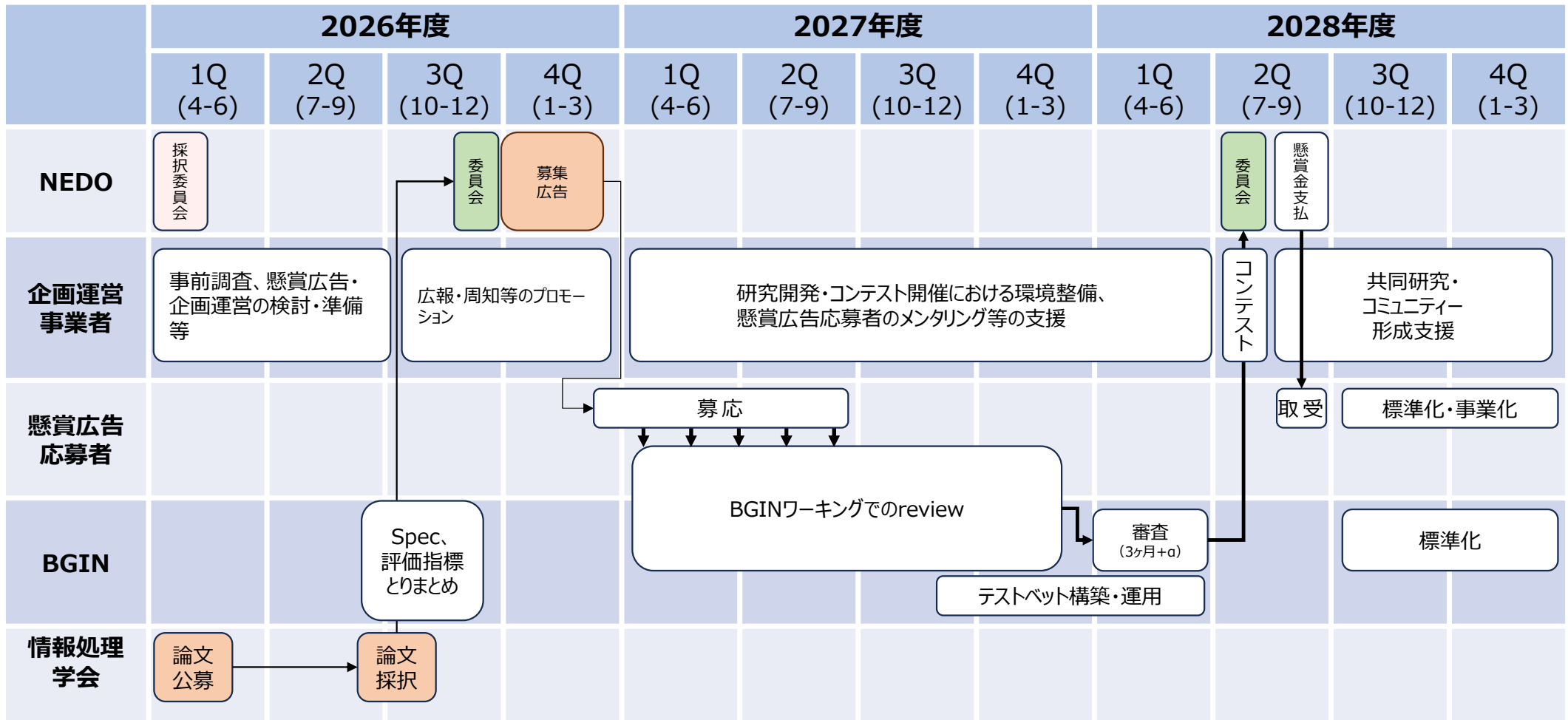
コンテスト終了後の展開:他のNEDOプロへの橋渡し等、ISO標準化、BGIN標準化

CONFIDENTIAL

PQC: Post-Quantum Cryptography(量子コンピュータ時代に耐性を持つ暗号技術)
ECDSA: Elliptic Curve Digital Signature Algorithm(楕円曲線暗号によるデジタル署名方式)
BGIN: Blockchain Governance Initiative Network(ブロックチェーンの国際標準化団体)

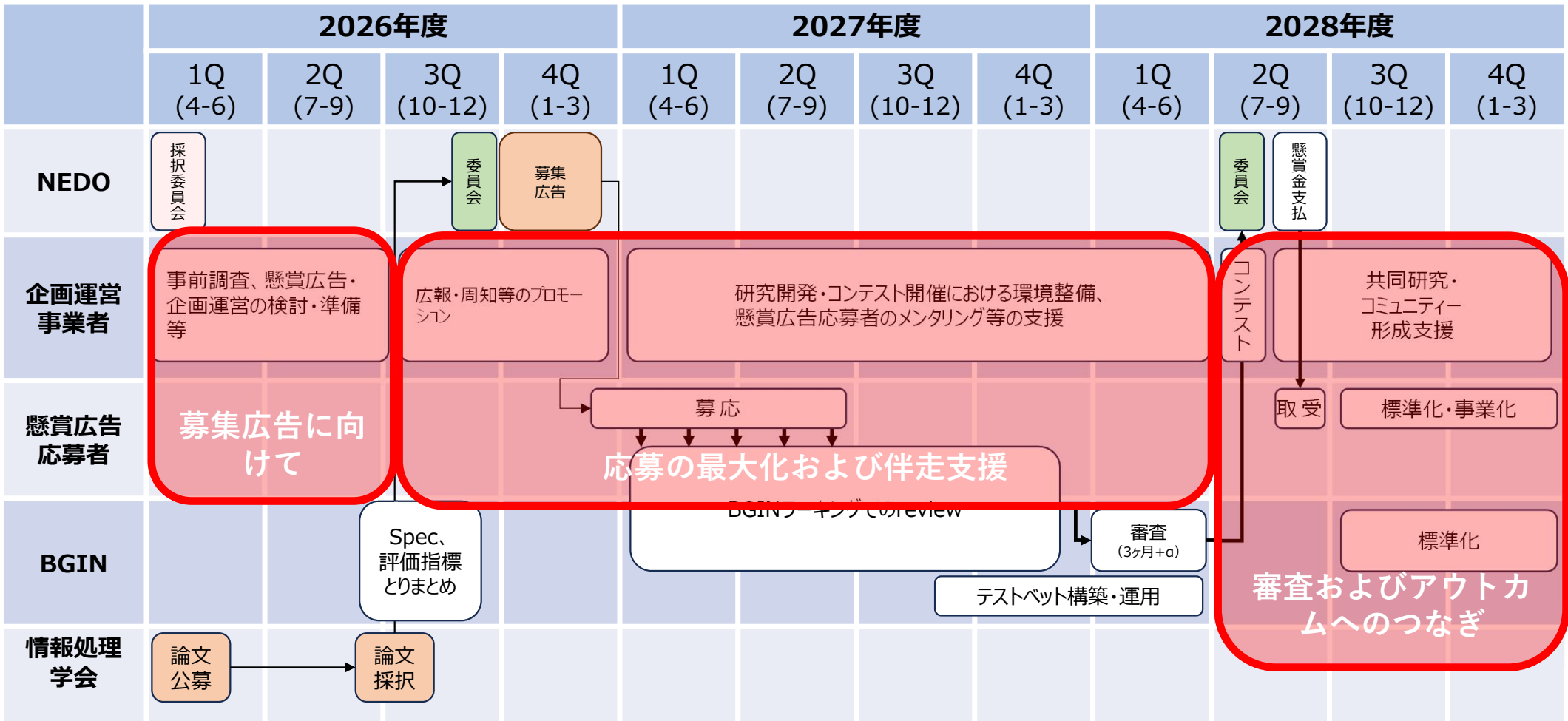
懸賞金事業スケジュール

量子計算機時代のブロックチェーンシステムの安全性確保技術



企画運営としてお願いしたいこと

懸賞金交付等審査委員会



本事業の概要と公募

- 調査の目的
 - 「課題①新たなサイバーセキュリティの技術」：
サイバー攻撃の高度化・複雑化、脆弱性対応の迅速化、及び、開発段階からのセキュリティ品質確保の重要性の高まり等の課題が生じており、並びに、これらの課題に対して、従来の人手による運用やルールベースの対策では、攻撃手法の変化やシステム構成の複雑化に十分に追従することが困難であり、またコスト面や運用面の制約から導入が進まないケースも多くなっています。
 - 「課題②量子計算機時代のブロックチェーンシステムの安全性確保技術」：
社会生活の基盤として広くブロックチェーンが使われる中、量子計算機の発展により、当初想定されていた安全性が確保できない（危殆化）が懸念されている。また、ブロックチェーンでは暗号の有効期限に基づく鍵管理が難しく、セキュリティインシデントの原因となっています。
 - 本事業では、これら課題に関する調査を実施し、コンテスト等の企画運営を実施する。
- 事業期間：2026年度～2028年度（NEDOが指定する日から2028年3月31日まで）
- 事業規模
 - 懸賞金総額：3.8億円程度（予算額は変動する可能性がある）
 - 事業予算額：3.0億円以内の委託（懸賞金を含まない、予算額は変動する可能性がある）
- 公募期間：2026年3月13日(金)～4月13日(月) 正午締切

※詳細は公募要領・仕様書をご参照ください。

提出期限および提出先

本公募要領に従って「提案書」を作成し、その他提出書類とともに以下の提出期限までにアップロードを完了させてください。なお、持参、郵送、FAX又は電子メールによる提出は受け付けません。必要なすべての書類をPDFにし、1つのZipファイルにまとめてアップロードしてください（パスワード禁止）。提案書はヒアリング審査準備の便宜上、横長の形式（パワーポイントを含む）でご用意いただいても結構です。

1. 提出期限：2026年4月13日（月）正午アップロード完了
2. 提出先：J Grants

<https://www.jgrants-portal.go.jp/subsidy/a0WJ200000CDXJuMAP?wfid=a0XJ2000006ex5EMAQ>

※ 応募状況等により、公募期間を延長する場合があります。
公募期間を延長する場合は、N E D Oウェブサイトでお知らせいたします。

審査方法・基準、スケジュール

【審査方法】

外部有識者による「採択審査委員会」とNEDO内の「契約・交付審査委員会」の二段階で審査します。契約・交付審査委員会では、採択審査委員会の結果を踏まえ、NEDOが定める基準等に基づき、最終的に実施者を決定します。必要に応じてヒアリング審査（4/13-5/7を予定、日時はNEDO指定）や資料の追加等をお願いする場合があります。なお、委託先の選定は非公開で行われ、審査の経過等、審査に関する問い合わせには応じられませんのであらかじめ御了承ください。

【審査基準】

「採択審査委員会」および「契約・助成審査委員会」の審査基準につきましては、公募要領をご確認ください。

【スケジュール】

- 公募締切：2026年4月13日（月）正午
- 採択審査委員会：2026年5月上旬（予定）
- 契約・交付審査委員会：2026年5月中旬（予定）
- 委託先決定：2026年5月下旬（予定）

契約について

本事業の契約におきましては、「調査委託契約標準契約書」を使用します。
以下のサイトよりダウンロードしてください。

https://www.nedo.go.jp/itaku-gyomu/2025_3yakkan_chousa.html

問い合わせ

本公募に関するお問い合わせは、以下のE-mailにて受付けます。

国立研究開発法人新エネルギー・産業技術総合開発機構

半導体・情報インフラ部

担当者：田中（俊）、卯川、齊藤

E-mail：cyber-bounty[*]ml.nedo.go.jp

E-mailは上記アドレスの[*]を@に変えて使用してください。

審査の経過等に関するお問い合わせには応じられません。

お問い合わせ頂いた内容で、応募検討者全員に公開すべきと判断される情報につきましては、

NEDOホームページの公募情報のページに掲載致します



ニュースリリースや公募、イベント情報等、様々な最新情報を発信しています。
ぜひフォロー・ご登録をお願いします！



NEDO
(@nedo_info)



NEDO【英語版】
(@nedo_info_en)



NEDO



スタートアップクラブ



NEDO Channel



NEDO PR Channel



質疑

Q：提案資料の枚数制限はありますか？

A：枚数の制限はありません。ただし、審査の効率を考慮し、要点を絞った資料をご用意いただけますと幸いです。

Q：フォーマットの指定はありますか？

A：公募ページのWordテンプレートを用意してありますが、記載された項目を網羅していただければppt等でも大丈夫です。

Q：予算について、NEDOで想定している割振りを、概算でよいので教えてください。

A：各社で独自のご提案を期待しております。そのため、回答は控えさせていただきます。

Q：NEDOの懸賞金事業の場合、懸賞広告案が別途提供されることが多いのですが、本件の懸賞広告（案）はありますか。

A：懸賞広告（案）は用意していません。