



今年度の技術戦略の検討課題について

2009年8月28日

内閣官房情報セキュリティセンター(NISC)

<http://www.nisc.go.jp/>

資料2

第2次基本計画における技術戦略の進め方について

第2次情報セキュリティ基本計画(技術戦略関係部分)



第2次計画では、(ア)情報セキュリティ技術開発の重点化と多様性の維持、(イ)「グランドチャレンジ型」研究開発・技術開発の推進、(ウ)研究開発・技術開発の効率的な実施体制の構築と基盤の整備を技術戦略における重点政策に掲げている。

(ア) 情報セキュリティ技術開発の重点化と多様性の維持

基盤としてのITの強化、および国民が安心してITを利用できるような環境の実現を目標とした、研究開発・技術開発を重点的に促進する。経済環境が厳しさを増す中で、ITを利用して生産性向上を図ることと、その分野における将来にわたる主導的かつ優位な地位を確保するという視点を持って、研究開発・技術開発を推進することが、従来以上に求められる。具体的には、利用者に対策への過度の負担を強いない、事前に情報セキュリティ対策が埋め込まれた、安全・安心な機器の実現や利用者環境の提供を、重点的に取り組むべき課題として取り組みを推進する。

一方で、研究開発・技術開発の多様性を確保するため、市場として成立していないために企業が取り組まない分野や将来的なリスクに対抗するための先行的な開発、開発コストが巨大な分野、および基礎研究など、我が国として戦略的に維持すべき分野に対しては、政府が積極的に取り組むこととする。

(イ) 「グランドチャレンジ型」研究開発・技術開発の推進

情報セキュリティ対策においては、喫緊の対応が必要でありながら対策が十分でない課題や、中長期的な視野で抜本的な技術革新等の実現が求められる課題が存在する。これらの対策が困難な課題に対応するため、「グランドチャレンジ型」の研究開発・技術開発を推進する。

喫緊の課題の解決に向けては、要素技術の統合化・実装化で迅速な対応を図る。

また、既に開発済みであっても、制度や教育が追いついていないなどの理由から技術成果が利用されていない場合があり、組織・人間系の管理手法の高度化や利用者の啓発と並行して、統合的な対策を推進することが有効となる。

中長期的な研究開発の推進のためには、将来の社会像を予測し、そこで必要となる情報セキュリティ技術を検討することで、研究開発・技術開発テーマの開拓を行なう。具体的には、設計段階から製品にセキュリティを作り込むための手法の確立や、開発ノウハウの蓄積は短期的に実現できるものではなく、また多くの知見を集約する必要があるため、中長期的なビジョンと実施体制、および支援環境をもって当たることが望ましい。

(ウ) 研究開発・技術開発の効率的な実施体制の構築と基盤の整備

国が支援するプロジェクトにおいては、その投資効果を最大化するために、研究開発・技術開発の計画策定時にプロジェクトの途中で得られた成果を活用する手順(プロセス)を組み込むとともに、プロジェクトの内容および実施状況の公開を促進する。また、情報セキュリティを取りまく環境の移り変わりが激しい中で、社会情勢変化や技術革新の影響を評価し、必要性が高い場合には計画変更が可能な、柔軟なプロジェクト管理の仕組みを導入し、新たな脅威への迅速な対応を可能とする。

さらに、直接的な研究開発・技術開発の取組みに加え、情報セキュリティ分野の特殊性にかんがみ、研究開発支援の環境整備を官民の連携によって積極的に推進する。具体的には、リスクの表記法や評価方式の共通化、情報セキュリティに関するデータベースの整備と共有、及び隔離ワークベンチの構築などによって、研究開発の支援と加速を図る。

SJ2009に掲げられている施策(1)(内閣官房 技術戦略関連部分)



第2次情報セキュリティ基本計画

SJ2009関連施策

(ア) 情報セキュリティ技術開発の重点化と多様性の維持

① 萌芽的研究開発に係る基本方針等の策定

民間での技術開発が行われている領域については民間の自主性に任せ、民間の取組みが乏しい萌芽的な研究については公的資金を投入する等のポートフォリオに関する分析を実施する。2009年度においては、特に技術開発領域に対する投資対効果の精度を高めるための手法の見直しについて検討する。

② 中長期的目標に対する研究開発・技術開発の促進

基盤としてのITを強化することに直結する中長期的目標に対して、公的研究資金を重点的に投入するための方策に関する検討を2008年度に引き続き実施する。

③ 短期的目標設定のなされている研究開発・技術開発の投資バランスの改善検討

既存技術の改良や運用技術の開発等、短期的目標設定のなされている研究開発・技術開発について、官民での取組みの状況を把握し、さまざまな領域において過小投資、過大投資が発生しないよう投資ポートフォリオに関する分析を2008年度に引き続き実施する。

④ 高セキュリティ機能を実現する次世代OS環境の評価及び性能向上

2008年度にプロトタイプ版の開発が完了した「セキュアVM」の内閣官房での試用および政府機関内での利用を想定した実証実験を実施し、実運用に向けた課題の整理を実施する。また、産学官の連携により、セキュアVMの性能向上及び利用環境の拡大を図る。

(イ) 「グランドチャレンジ型」研究開発・技術開発の推進

⑤ 「グランドチャレンジ型」のテーマ及び推進の枠組み検討

総合科学技術会議と情報セキュリティ政策会議の連携の下、2009年度では、プロジェクトのより詳細なテーマ及びグランドチャレンジ型研究を推進するための枠組みについて、検討を実施する

SJ2009に掲げられている施策(2)(内閣官房 技術戦略関連部分)



第2次情報セキュリティ基本計画

(ウ) 研究開発・技術開発の効率的な実施体制の構築と基盤の整備

SJ2009関連施策

⑥公的な競争的資金制度におけるプロジェクト管理・評価の検討

研究開発プロジェクトについて、開発期間中の新たな状況変化に応じた柔軟な計画変更を可能とするとともに、研究開発の中間成果の利用を促進するための制度の改善を検討する。

⑦実施状況の把握及び継続的な見直しの実施

情報セキュリティ政策会議は、総合科学技術会議との連携の下に、産官学を通じた我が国における情報セキュリティに関連する研究開発・技術開発の実施状況の把握を2008年度に引き続き実施する。

⑧投資効果に係る継続的評価プロセスの導入

情報セキュリティ政策会議は、総合科学技術会議との連携の下に、情報セキュリティ技術に関する研究開発・技術開発の投資効果について、1)事前、2)中間、3)事後の各段階における評価を2008年度に引き続き実施し、その結果については速やかに公表する。

⑨政府調達における成果利用の方策の検討

情報セキュリティ研究開発・技術開発における成果を、調達を通じ、最大限、直接政府が活用するための方策について、その検討を2009年度も引き続き行う。

①-③, ⑤, ⑦-⑨を纏めて検討する。

具体的には、情報セキュリティに係わる技術開発の進捗状況を目的別に評価し、現在の技術における本質的問題を調査する。その上で、政府が推進すべき研究分野の検討、「グランドチャレンジ型」研究テーマの選定等を行う。

④については、政府機関でのセキュアVMの導入・運用に向けた課題整理を行う。

⑥については、研究開発プロジェクトの管理・評価に係わる改善施策を具体化し、これらの施策を特定の研究開発事業で関係者とともに試行する。

政府が促進すべき技術開発分野に関する過去の検討内容(1)



- 情報セキュリティ技術戦略の基本的な考え方(2005, 2006)
 - ITの安心利用環境実現のための技術開発を「技術戦略」と定義
- 技術戦略に関する全体俯瞰の把握(2005、2006)
 - 重点化分野の設定(情報セキュリティ技術の高度化及び組織・人間系の管理手法の高度化を実現するための取組み、情報セキュリティ技術を支える環境整備としての取組み)
 - グランド・チャレンジの考え方の提示(長期的、根本的な課題を解決するための大目標を設定し、各要素技術の統合的開発を行うもの)

報告書で示されたグランド・チャレンジ型テーマの例

- コンピュータウイルスなどの悪意を持ったプログラムによる脅威を根絶できるような情報処理環境の構築。
- 情報システムを運用する回避不可能な人為的ミス等から発生するトラブルやエラーを根絶する、「情報セキュリティ・ユニバーサルデザイン」の確立。
- 情報サービス、ネットワークサービスにおいて、利用者側が情報セキュリティサービスの品質グレードを指定し、利用できる環境の構築。例えば、電気通信事業者やプロバイダーが指定するのではなく、利用者がグレードをコントロールし、かつユーザブルに利用可能な「迷惑電話・迷惑メール防止サービス」の提供など。
- 認証等の基礎となるトラストポイントの国際化とネットワーク化。例えば、日本が先導してトラストポイントに求められる要件と検証を行い、各国が持つトラストポイントについて相互互換性を保証する「グローバルトラストネットワーク」を形成する取組み。
- 通信障害等を自律的に検知し、回復することのできる高信頼性のあるインターネット環境の構築。

- グランドチャレンジの方向性を提示(2008)

- 将来的な社会ビジョンの検討・・・実現すると望ましいと考えられる特徴的な要素(ニーズ)を抽出
- 情報セキュリティ技術の潮流予測・・・現在の技術とその動向に基づき演繹的にシーズを予測
- 「ニーズ」「シーズ」「最先端性」を満たす技術を抽出し、グランドチャレンジ型研究開発・技術開発の方向性を提示

昨年度の報告書には4つの研究分野の方向性が示されている。

- 「安全・安心な生活、社会経済活動」や「グローバル・ユビキタス」を実現するべく、日常の生活、社会経済活動に浸透したIT機器の情報セキュリティ確保に係る技術。
 - 「当然化」を実現するべく、一定の情報セキュリティ水準が確保されたプロダクトを設計開発する手法および技術。
 - 「適切性」を実現するべく、利用シーンに応じて動的に情報セキュリティ水準を最適化するような技術・システム。
 - 「マネージャビリティ(可管理性)」を実現するべく、人間がリスクをコントロールできることで安心して情報を管理できるような技術。
- なお、テーマ検討においては、目に見える具体物「New Secure Product」の開発を実現するものとする。

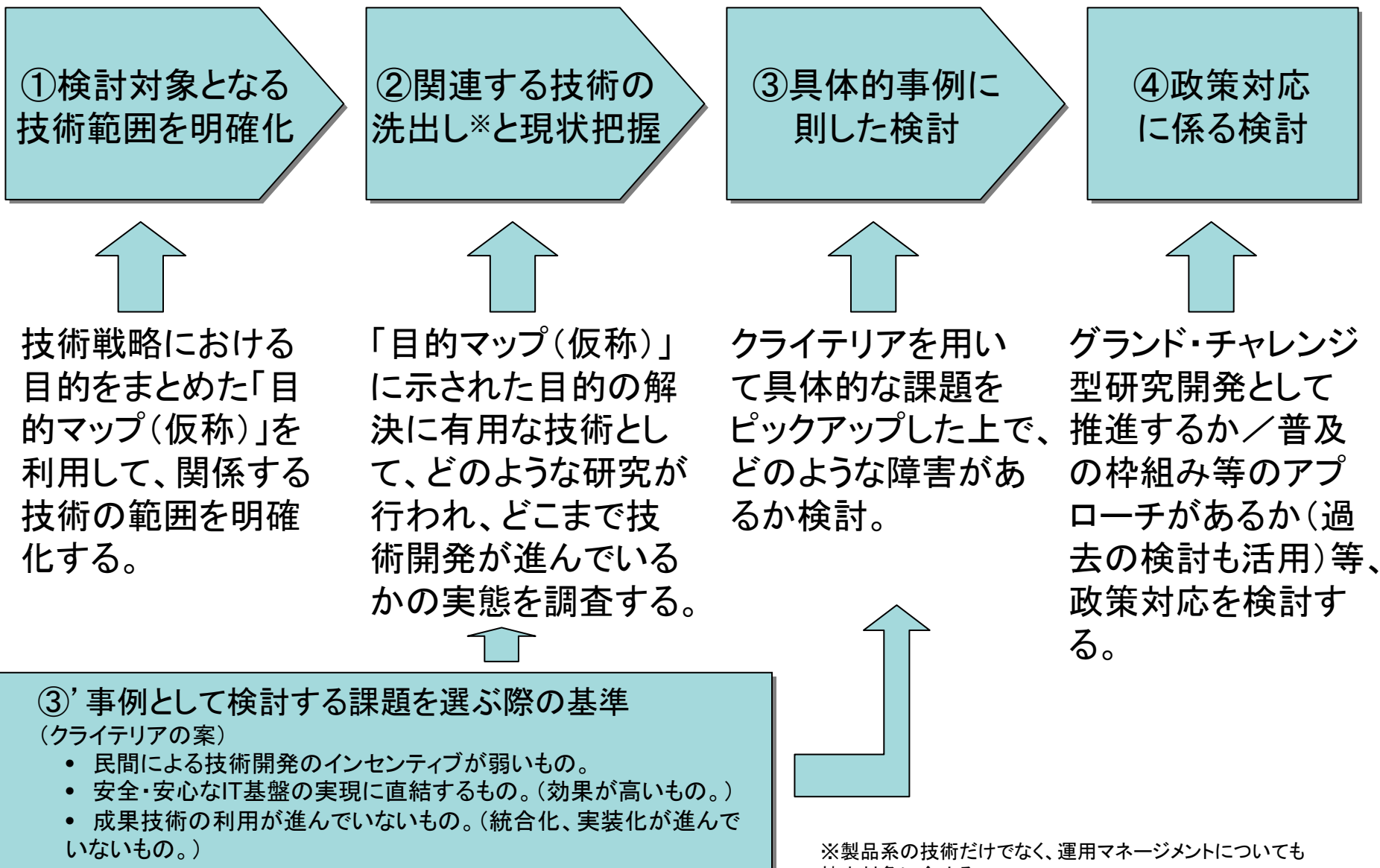
昨年度までの検討内容を踏まえ、テーマを具体化するため、今年度は研究・開発プロジェクトの推進に係わる下記の点について検討を深めたい。

- **グランドチャレンジ型研究開発のテーマ及び推進枠組み検討**
 - グランドチャレンジ型研究開発を推進するための方法論、具体的な枠組みの検討
[第2次基本計画(イ), (ウ)、SJ2009施策⑤と関連]

- **情報セキュリティ技術の研究・開発における政府関与の在り方**
 - 研究・開発促進ツール(補助金、減税、融資、産学連携スキーム等)の活用検討
 - 萌芽的研究開発における公的資金投入の在り方(対象等)について検討
[第2次基本計画(ア)、SJ2009施策①, ②, ③と関連]

- **研究・開発成果の利用・普及推進の在り方**
 - 要素技術の統合化・実装化をどのように進めるべきか
 - 技術の普及等の枠組みをどのように構築すれば良いか
 - 組織・人間系の管理手法の高度化をどのように進めれば良いか
[第2次基本計画(イ)、SJ2009施策⑥, ⑨と関連]

政府が促進すべき技術開発分野に係る検討の進め方(案)



「目的マップ(仮称)」のイメージ



	ITの安心・安全利用環境の実現		
	「機密性」 情報・アプリケーションの 不正利用を防止する	「可用性」 サービス継続ができる	「完全性」 正しい情報が利用できる
未然防止 (事前対策)	<ul style="list-style-type: none"> 第三者に情報が渡らない サービスを利用するための認証情報を第三者が不正に利用できない 	<ul style="list-style-type: none"> システムダウンを防ぐことができる バグや誤操作による間違った動きを防止できる 	<ul style="list-style-type: none"> 情報の改ざんを防止できる(改ざんされた情報であることが容易に分かる)
被害拡大防止 (初動対応)	<ul style="list-style-type: none"> 情報が第三者に漏洩した場合は、漏洩したことが分かる 第三者に漏洩した情報を削除する(認証情報は無効化する)ことができる 	<ul style="list-style-type: none"> システムがダウンしても直ぐに復旧することができる 誤操作を検知して、被害の拡大を防止する 	<ul style="list-style-type: none"> ネットワーク上に拡散している改ざんした情報を削除することができる
再発防止 (事後対策)	<ul style="list-style-type: none"> 漏洩経路・漏洩先を特定することができる 漏洩した要因を技術的な観点から特定し、対応手段を取ることができる 	<ul style="list-style-type: none"> サービスが停止した原因を特定し、対応手段を取ることができる 	<ul style="list-style-type: none"> 改ざんした情報の発信者を特定することができる

- 検討を深めるべき事項及び政府の促進すべき技術開発分野に係る「検討の進め方」について
- 「目的マップ(仮称)」の作成方法
 - 技術戦略の目的の解決に有用な技術を網羅的に洗い出す手段として適切であるか。
- 技術開発の進捗状況に係わる実態調査の調査項目
 - 政府として取り組むべき技術開発分野を選ぶ際の基準として、下記の要素を調査すれば良いか。
 - 民間による技術開発のインセンティブが弱いもの。
 - 安全・安心なIT基盤の実現に直結するもの。(効果が高いもの。)
 - 成果技術の利用が進んでいないもの。(統合化、実装化が進んでいないもの。)

高セキュリティ機能を実現する次世代OS環境の評価

- 平成18年度から平成20年度まで、文部科学省科学技術振興調整費の重要課題解決型研究「高セキュリティ機能を実現する次世代OS環境の開発」にて、仮想化技術を利用してセキュアなOS環境を実現するセキュアVMの開発を推進。平成21年3月にプロトタイプ版の開発が完了し、オープンソースソフトウェア「BitVisor」として一般に公開 (<http://www.securevm.org/>)。
- 今年度は、政府機関でのセキュアVMの導入・運用に向けた課題整理を行う予定
 - BitVisorについて、政府機関での利用を想定した実証評価を実施し、実運用上の問題点や改善点などの課題を検討
 - 仮想化技術によりOSのセキュリティ向上を図るソフトウェアについて調査を実施。BitVisorとの比較評価や運用上の問題点などの課題を検討

研究開発プロジェクトの管理・評価体制の改善

昨年度の報告書では、研究開発プロジェクトの管理・評価体制の改善施策として、以下の方向性を示している。本年度は、これらの施策を幾つかの研究開発事業で関係者ととともに試行することが取組み方針として示されている。

【1】 計画変更の柔軟化とリファクタリングの必要性

- ・年次計画は、研究者及び資金配分機関で、当初計画の見直しを行い、常に精度の高いものとしておくこと。或いは、複数年の研究計画は粗い粒度で立て、詳細計画は毎年設定できる形態とすること
- ・資金配分機関において、処遇等の改善を通じて、できるだけ対象研究領域に知見を有し、評価、資金の使用状況の審査を適切に行える人材を確保すること
- ・PO(Program Officer)等の担当者に対して計画変更の要望があった際は、それを判断するための場(有識者委員会等)を組織するなど、研究の進展等に応じて柔軟に計画変更するための仕組みを、資金配分機関内に設けること

【2】 途中段階で得た成果利用プロセスの独立

- ・中間成果の扱いについて、研究開発計画等で定めるようにルール化を検討すること
- ・データベースなどを活用し、中間成果を公表できる体制を整備すること
- ・知的財産権上の扱い等、中間成果を活用する際の開発者と利用者の権利についてのルールの明確化を検討すること
- ・成果を活用する側との連携、成果の実装へのつなぎ部分についても、支援の強化の方策を検討すること

取り組み方針

- 「計画変更」については、幾つかの研究制度で認められている。そこで、ベストプラクティスを共有するために、各制度の目的を加味したうえで各制度の規定、実施手順の整備状況等を調査する。
 - 研究開発プロジェクトの計画変更に関する規定例：
科学研究費補助金(科研費)の場合は、「経費の使用内訳の変更」、「研究費の一部の繰越し」を一定の条件下で認めている。この条件を超える場合は、事前承認が必要となるが、承認ルールについては明確には示されていない(ハンドブック等の公開資料には示されていない)。
- 変更ルールや実施手順に「あいまいさ」が残る部分について検討する。
 - 審査・評価委員会(計画変更の妥当性を評価する委員会)の満たすべき要件
 - 承認ルール(審査・評価委員会、財務省や会計検査院の了解を得るためには、どういう点に着目し、どんな手順で話を進めて、どんな基準で許可すれば良いかなど)
 - 情報セキュリティ研究の特性を考慮した承認ルール(研究過程で発見した脆弱性を公表することが、リスクに繋がるようなケース)
- 関係者(計画変更に伴って説明責任が生じるとされる組織への(審査・評価委員会、財務省、会計検査院など))ヒアリング結果を踏まえ、「計画変更」の実施手順のガイドラインを作成する。

「計画変更」に係わる規定



補助金等適正化法※ ¹ (第7条)における規定	ある研究制度における「計画変更」の規定
<p>一 補助事業等に要する経費の配分の変更(各省各庁の長の定める軽微な変更を除く。)をする場合には、各省各庁の長の承認を受けなければならないこと。</p>	<p>【交付申請書の記載内容の変更に係る手続き】 直説明費の使用内訳の変更 研究代表者は、各費目の額を、交付された直接経費の総額の**%未満(直接経費の総額の**%の額が…(以下省略))</p>
<p>三 補助事業等の内容の変更(各省各庁の長の定める軽微な変更を除く。)をする場合には、各省各庁の長の承認を受けなければならないこと。</p>	<p>該当する手続きの記載が見当たらない</p>
<p>四 補助事業等を中止し、又は廃止する場合には、各省各庁の長の承認を受けなければならないこと。</p>	<p>【交付申請書の記載内容の変更に係る手続き】 補助事業の廃止 研究者が、補助事業を廃止しようとする場合に、当該研究代表者が作成する「補助事業廃止承認申請書」により申請を行い、〇〇大臣の承認を得るとともに、未使用の補助金を返還し、…(以下、省略)</p>
<p>五 補助事業等が予定の期間内に完了しない場合又は補助事業等の遂行が困難となった場合には、すみやかに各省各庁の長に報告してその指示を受けなければならないこと。(第2項以降省略)</p>	<p>【交付申請書の記載内容の変更に係る手続き】 翌年度における直接経費の使用 当該年度の補助事業が、交付決定時には予想し得なかったやむを得ない事由に基づき、補助事業が予定の期間内に完了しない見込みとなった場合であって、研究代表者が、補助事業の期間を延長するとともに、補助金の全部又は一部を翌年度に使用することを希望する場合には、…(以下、省略)</p>

※1: 補助金等に係る予算の執行の適正化に関する法律(昭和30年法律第179号)

【仮説】ある研究制度では、(1)補助事業の変更等(補助事業の廃止、直接経費の使用内訳の変更)、(2)研究代表者の変更、(3)研究分担者の変更に関する規定のみが記載されている。「内容の変更」についても、軽微な変更を規定することで計画変更が柔軟に行えるようになるのではないか。

取り組み方針

- 研究の進捗を確認するために、中間成果を報告するように規定した制度は多数あるが、中間成果の活用に関する記述は見当たらない。
 - ▶ 例えば、科学研究費補助金の場合、年度が終了した時には「実績報告」、研究が終了した時には「研究成果報告書」を提出し、これらは「科研費データベース」を通じて公開されることになっている。また、4年以上の研究開発については、3年目に中間目標を達成しているか否かについての中間評価を行い、評価結果に基づいて継続の可否を決めることになっている。
- 中間成果の公表/活用を進めてもらうには、公表/活用ルールを明確化する必要がある。すなわち、開発者と利用者の知的財産権などを整理する必要があるが、これには研究支援機関の果たすべき役割が大きい。そこで、新設される研究プログラムのなかに、グランドチャレンジのプロジェクト管理の改善「採択後の成果を最大化するための取り組みなど」を入れ込む活動を進める。
 - ▶ 例えば、最先端研究開発支援プログラムの公募要領によると、中心研究者が研究支援担当機関を選定する(公募の可能性があり)。支援担当機関を公募方式で選定する場合、「研究成果が適時適切に公開され、外部研究機関や民間事業者が利用しやすいものとなるよう環境が整備されているか」を審査の項目に追加することで、中間成果の公表や活用が促進されるのではないか。