

仕様書

1. 件名

令和2年度補正持続化給付金事務事業

2. 目的

新型コロナウイルス感染症の拡大により、休業を余儀なくされるなど、中堅企業、中小企業、小規模事業者、個人事業者、フリーランスの方々の業況に大きな影響が出ているところ。

こうした事業者は、我が国経済の基盤を支える存在であり、事業の継続は極めて重要。

このため、感染症拡大により、特に大きな影響を受けている事業者の事業継続を支援するため、事業全般に幅広く使える給付金を支給するもの。

3. 事業内容

上記の目的に照らし、次に掲げる事業を実施する。

(1) 新型コロナウイルスの影響を受けた中堅・中小法人、個人事業主への給付金の支給

① 給付対象

詳細は経済産業省から指示するが、中堅・中小法人、個人事業主等最大200万者程度が対象となることも予想されるため、十分な体制を構築すること。

② 給付額

中堅・中小法人が200万円、個人事業主（フリーランスを含む。）が100万円を上限とする。計算式等の詳細は経済産業省の指示に従うこと。

③ 事務局の設置

(1) ①からの申請を受け付けるため、

i) 電子受付

ii) 電子申請に支障がある申請者のための受付を確実に実施できる体制を構築すること。なお、ii)の体制は窓口など提案によることとする。

なお、従業員等（窓口等で申請者と接する場合は申請者に対するものも含む。）への新型コロナウイルス感染症対策を徹底し、万が一新型コロナウイルス感染症に罹患した者が生じた場合も事業継続可能な体制とすること。

また、本事業に従事する者との間で秘密保持などの遵守事項を定め取り交わすこと。また、不特定多数の者が氏名・住所・口座番号・振込金額などの情報に同時に触れることのできない対策を講じること。

④ 申請書類

以下の書類を念頭においているが、必要な書類や様式等は経済産業省と協

議の上決定する。

- 前年度の確定申告書
- 売上台帳
- 虚偽の申請でないことの宣誓書
- 実在確認書類
 - 中堅・中小法人：原則として法人番号
 - 個人事業主（フリーランスを含む）：本人確認書類（パスポート、運転免許証等）

⑤ 二重取り等不正防止のための必要な措置

二重取り等不正な手段による支給を防止するため、最低限以下の措置を講じることとするが、詳細は経済産業省と協議の上決定する。

- 事後的に申請内容に虚偽が明らかとなった場合には返納を求めるところを明示。また、その場合には返納を求めるところ。
- 虚偽内容が特に重大又は悪質な場合には事業者名等を公表すること。更に特に悪質なものについては刑事告発等を行う可能性があることを示した上で申請させること。
- 確定申告書により、代表者氏名、事業所所在地等を確認。その情報を事務局においてデータベース化して名寄せを行い、二重取りを防止すること。その他、二重取りを防止するために必要な措置を講じること。

⑥ 給付金の支給

上記（１）①への給付金の給付（贈与）については、別途経済産業省が交付する資金（２兆円程度）を原資に行うものとする。なお、受給者への給付金の給付は、以下により行うものとする。

- i) 受給者は事務局に給付申請書等を提出。
- ii) 事務局は給付申請の内容について適格性等の確認を実施。また、給付金の受領に係る委任について委任状の提出を受け、受給者と合意すること。
- iii) 事務局は給付に必要な額を都度経済産業省に請求（受給者の代理で受給する旨も併せて申請）。
- iv) 経済産業省は事務局に対して給付金の支給のために必要な金額を支払。なお、給付金の支払に要しなかった金額は経済産業省に返還すること。
- v) 事務局は受給者に給付金を速やかに給付（銀行口座のみ）。
- vi) 交付通知書の送付。

上記の他、受給者への給付金の給付に関する事務の詳細については契約結後、経済産業省と協議の上決定することとする。

⑦ 反社会的勢力の排除

上記⑥v) 以外に反社会的勢力などからの申請及び振込を防止するために必要な措置を講じること。

(2) HP等による広報

上記(1)①を広く周知するため、以下を実施すること。

① HPの設置

制度の概要、FAQ、申請の動画解説などを掲載すること。詳細は提案による。

② 広報

新聞、Web等の手段より広報を行う。詳細は提案によることとするが、掲載先等については経済産業省と相談の上決定することとする。

(3) コールセンターの設置

上記(1)及び(2)に対応するため、電話による問合せ窓口を以下により設置すること。

- 複数拠点(国内に2カ所程度)に設置
- 開設期間: 契約締結日~2020年12月28日まで
- 窓口時間: 8:30~17:00(5~6月については上記時間帯は常に開設すること。7月以降は土祝除く日~金。)
- 1日に最大5,000件程度の相談を受けられる体制を構築すること。
(契約締結後直ちに体制を整える必要はないが、問合せ件数に応じて適時体制を構築すること。)
- 不正受給等の内部通報にも対応していることを明示すること。

4. 事業を実施する上での補足事項: 注意点

本仕様書に記述していない事項であっても、仕様書の目的を達成するために提案があれば行う。

上記3(1)~(3)を、別紙1「情報セキュリティに関する事項」を踏まえて実施すること。

5. 事業期間

委託契約締結日から令和3年2月28日まで

6. 成果物

3.(2)②に用いた資料 1式

7. 納入場所

中小企業庁長官官房総務課

8. 情報管理体制

(1) 受託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、委託者に対し「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、住所、生年月日、所属部署、役職等が記載されたもの)別紙2を契約時に提出し、担当課室の同意を得ること。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。

(2) 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し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
- 経済産業省が個別に承認した場合を除き、契約相手方に係る親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の契約相手方に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の契約相手方以外の者に対して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

(3) 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。

(4) (1) 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。

9. 業務従事者の経歴

業務従事者の経歴(氏名、所属、役職、職歴・業務経験がわかる資料)を提出すること。

※経歴提出のない業務従事者の人件費は計上不可。

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を定めたものを含み、以下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、契約期間中に、担当職員の要請により、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、本事業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事業にかかわる従事者に対し実施すること。
- 3) 受託者は、本事業遂行中に得た本事業に関する情報（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、本事業遂行中に得た本事業に関する情報（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、本事業を終了又は契約解除する場合には、受託者において本事業遂行中に得た本事業に関する情報（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又は廃棄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、本事業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。ただし、担当職員の承認を得た場合は、この限りではない。
- 7) 受託者は、本事業の遂行において、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「政府機関等の情報セキュリティ対策のための統一基準群（平成30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、当省が実施する情報セキュリティ監査又はシステム監査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、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（事業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。）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、既知の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。
- 11) 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、構築又は改修したウェブアプリケーションのサービス開始前に、「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。

12) 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ずること。

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。

13) 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、原則、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」（以下「政府ドメイン名」という。）を使用すること。なお、政府ドメイン名を使用しない場合には、第三者による悪用等を防止するため、事業完了後、一定期間ドメイン名の使用权を保持すること。

14) 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。そ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事業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。

15) 受託者は、本事業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、本事業の実施場所、本事業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、本事業の実施期間中に従事者を変更等する場合は、事前にこれらの情報を担当職員に再提示すること。

16) 受託者は、本事業を実施するに当たり、約款による外部サービスやソーシャルメディアサービスを利用する場合には、それらサービスで要機密情報を扱わないことや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。

17) 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、経済産業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や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やソフトウェア等の利用者に要求することがないように、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経済産業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に開発すること。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、経済産業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が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。
- 18) 受託者は、本事業を再委託する場合は、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)～17)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。

情報取扱者名簿及び情報管理体制図

①情報取扱者名簿

		氏名	住所	生年月日	所属部署	役職	パスポート 番号(※4)
情報管理責任者(※1)	A						
情報取扱管理者(※2)	B						
	C						
業務従事者(※3)	D						
	E						
再委託先	F						

(※1) 受託事業者としての情報取扱の全ての責任を有する者。必ず明記すること。

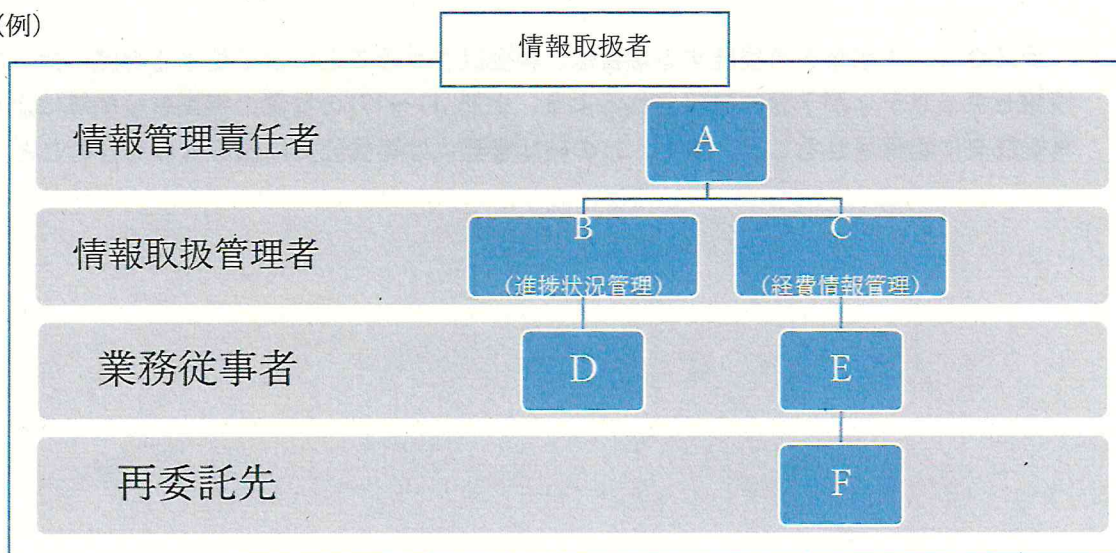
(※2) 本事業の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本事業の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。

(※3) 本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

(※4) 日本国籍を有する者及び法務大臣から永住の許可を受けた者(入管特例法の「特別永住者」を除く。)以外の者は、パスポート番号等を記載。

②情報管理体制図

(例)



【情報管理体制図に記載すべき事項】

- ・ 本事業の遂行にあたって保護すべき情報を取り扱う全ての者。(再委託先も含む。)
- ・ 本事業の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。
- ・ 情報管理規則等を有している場合で上記例を満たす情報については、情報管理規則等の内規の添付で代用可能。

③その他

- ・ 情報管理規則等の内規を別途添付すること