仕　様　書

1　案件名称

2019 年G20 大阪サミット関西推進協力協議会の情報セキュリティ対策にかかるコンサルティング業務委託

2　目的

2019 年G20 大阪サミット会議（以下「G20 大阪サミット」という。）が、2019 年６月 28 日及び 29 日に大阪で開催される。2019 年G20 大阪サミット関西推進協力協議会事務局（以下「事務局」という。）では、会議の開催成功に向けた取組みを進めているところであるが、G20 大阪サミットは各国首脳が一堂に会する国際会議であることから、より一層厳格なサイバーセキュリティ対策が求められている。

そのような状況の下、事務局の情報セキュリティ対策を早急により確実なものにするために必要となる各種情報セキュリティ対策への支援、情報提供、相談窓口の設置、インシデント発生時の迅速な対応等、情報セキュリティに関するコンサルティング業務を行うものである。

3　履行期間

2019 年４月１日から 2019 年７月５日まで

なお、仕様書６に定める業務については次の期間とする。

（１）2019 年４月１日～2019 年６月 26 日　…　仕様書６（１）及び（２）

（２）2019 年６月 27 日、28 日及び 29 日　…　仕様書６（３）

（３）2019 年６月 30 日～2019 年７月５日　…　仕様書６（２）

4　成果物

（１）　本件仕様書６（１）（２）における成果物

・問合せ管理表

（２）　本件仕様書６（３）における成果物

・緊急時対処に係る議事録

・調査結果報告書

5　構成

事務局における構成は以下のとおり。なお、構成の詳細については、セキュリティ保持の関係上、契約締結後に情報を提供する。

・事務局職員用端末　　40 台程度

・ネットワークプリンタ　　２台

・クラウドファイルサーバー

・クラウドメールサーバー

6　業務内容

（１） 現状確認

事務局で利用するネットワークにかかる情報（ネットワーク構成、プロセス情報、接続情報、ファイル情報、ドライバ情報、マシン、ユーザ情報等）の収集を行い、インシデント発生時にすぐに対応できるよう、事務局が利用するネットワークの現状を把握する。

（２） 緊急時対応（メール問合せ対応）

事務局で利用するネットワークについて、メール対応により助言を行うことで、インシデントレスポンスを支援する。なお、調査を効率的に行うために必要な場合は、協議のうえ機材等を利活用することも可とする。

事務局が提供するウイルス検知等情報への対応方法、内閣サイバーセキュリティセンター（NISC）を始め他機関からの検知情報への対応、質問への対応、その他情報セキュリティの問題等について、事務局からの問い合わせ窓口を設置し、メールによる質問を24時間受け付けること。(最大で週に１回まで、問い合わせ１回に対する調査及び回答に要する工数は最大で８時間を想定。)

受注者は、メールにより、その問合せ・相談に対して専門的見地から回答、解説、助言を行うこと。

また、午前９時から午後６時までに受け付けたメールについては原則３時間以内に調査・ 分析に着手し、適切な助言、提案及び情報提供を行うこと。

「３　委託期間　（１）仕様書６（１）（２）における委託期間」におけるログ等の分析、リバースエンジニアリング作業及び端末のフォレンジック作業は、双方協議のうえ別途取り扱いを決定する。

（３） 緊急時対応（オンサイト対応）への参画

サミット開催前日である2019年６月27日並びに開催当日である2019年６月28日及び29日の計３日間（夜間も含む）において、サイバー攻撃や不正侵入等、事務局の情報システム運用に重大な影響を及ぼすインシデントが発生した場合は、確実に参集できる体制を整備し、オンサイトにより対応を支援すること。なお、緊急時の参集については、緊急時連絡網及び参集手順要領を策定し、事務局からの連絡後１時間以内に担当者が事務局に参集すること。ただし、天災や特殊な交通状況などの影響を受ける場合はこの限りではない。

事務局が緊急時に対応体制を設置した場合、事務局の招集に基づき緊急時の対処に参画し、関係者への連絡、拡大防止のための応急措置（ログ等の分析、リバースエンジニアリング作業及び端末のフォレンジック作業に応じること)、対応方針の策定、復旧、再発防止策の策定等について、適切な助言、提案及び情報提供を行うとともに、当該緊急時対処に係る議事録を作成し、原則翌日までに送付すること。サミット開催期間の終了後に引き続き調査を行う必要がある場合は、緊急時対応（メール問合せ対応）の調査範囲で対応すること。

７　受注者等に求める要件

本件業務を実施するにあたり求める要件は以下のとおりとする。なお、各要件について別紙

に基づき必要書類等を事務局あて提出すること。

（１） 直近５年の間に、政府機関等が主催する国際会議等（サミット、G7 等）におけるオンサイトでの政府機関又は地方自治体等へのインシデントレスポンス支援業務実績があること。

（２） 本件業務を実施する部門は、情報セキュリティ対策、各種脆弱性等に関する調査、情報セキュリティ監査業務等のコンサルティング業務を専門としていること。（少なくとも 10 名以上の要員がいること。）また、本件業務を含む業務について、ISMS 認証または同等のものを取得していること。

（３） 本件業務の業務責任者については、以下の資格を１つ以上所有するとともに、情報セキュリティもしくはサイバーセキュリティコンサルティング業務の経験が５年以上あること。

- 情報システムセキュリティ専門家(CISSP/SSCP)
- 情報セキュリティマネージャ(CISM)
- 情報セキュリティ監査人(CAIS)
- 情報システム監査人(CISA)
- 情報処理安全確保支援士
- 情報セキュリティスペシャリスト
- 情報処理技術者(テクニカルエンジニア(情報セキュリティ))

（４） 本件業務を実施する者に、インシデントレスポンス業務の経験を５年以上有している者を含めた体制を構築すること。

（５） G20 大阪サミットは世界的な会議であり、世界各国から多種多様なサイバー攻撃を受ける可能性があるため、少なくとも 10 か国語での調査が可能な体制を構築すること。

（６） 本件業務を実施する部門は、常に最新の脅威情報（ネットワーク攻撃情報、マルウェア情報、脆弱性情報、標的型メール、スパムメール、なりすまし情報等）を、世界各地に設置した 300 万以上のセンサーから収集する仕組み及び体制を持っていること。

８　その他

本件業務の遂行上知り得た個人情報及びG20 大阪サミットに関する機密事項については、本業務のみに利用するものとし、契約期間中又は契約終了後を問わず第三者に漏洩しないこと。

（別紙）

仕様書７に関する必要書類及び提出期限

要件	必要書類	提出期限
（１）	次の事項を明らかにする文書（契約書、仕様書の写し等） ・業務名称及び概要 ・業務の相手方 ・業務実施年月日 ・政府機関等が主催する国際会議等の名称及び概要	平成 31 年３月 22 日
（２）	業務実施部門に関する次の文書 ・部門の体制を明らかにするもの（体制図等） ・ISMS 認証または同等の認証の取得を証明するもの	平成 31 年４月１日
（３）	各種資格の取得を証明するもの	
（４） （５） （６）	業務実施体制を明らかにするもの（体制図等）	