

マルウェア対策・WAF 機器の運用管理業務に関する
民間競争入札実施要項（案）

国立研究開発法人理化学研究所

目次

1	趣旨.....	1
2	マルウェア対策・WAF 機器の運用管理業務の詳細な内容及びその実施に当たり確保されるべき質に関する事項.....	1
3	実施期間に関する事項	3
4	入札参加資格に関する事項.....	3
5	入札に参加する者の募集に関する事項.....	4
6	マルウェア対策・WAF 機器の運用管理業務を実施する者を決定するための評価の基準その他本業務を実施 する者の決定に関する事項	5
7	マルウェア対策・WAF 機器の運用管理業務に関する従来の実施状況に関する情報の開示に関する事項.....	6
8	マルウェア対策・WAF 機器の運用管理業務の請負業者に使用させることができる国有財産に関する事項	7
9	マルウェア対策・WAF 機器の運用管理業務請負者が、理研に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の本業務の適正かつ確実な実施の確保のために本業務請負者が講じるべき措置に関する事項	7
10	マルウェア対策・WAF 機器の運用管理業務請負者が本業務を実施するに当たり第三者に損害を加えた場 合において、その損害の賠償に関し契約により本業務請負者が負うべき責任に関する事項.....	10
11	マルウェア対策・WAF 機器の運用管理業務に係る法第 7 条第 8 項に規定する評価に関する事項	10
12	その他業務の実施に関し必要な事項	11
	別紙 1 従来の実施状況に関する情報の開示	
	別添 1 調達仕様書	

1. 趣旨

競争の導入による公共サービスの改革に関する法律（平成 18 年法律第 51 号。以下「法」という。）に基づく競争の導入による公共サービスの改革については、公共サービスによる利益を享受する国民の立場に立って、公共サービスの全般について不断の見直しを行い、その実施について、透明かつ公正な競争の下で民間事業者の創意と工夫を適切に反映させることにより、国民のため、より良質かつ低廉な公共サービスを実現することを目指すものである。

上記を踏まえ、国立研究開発法人理化学研究所（以下「理研」という。）は「公共サービス改革基本方針」（令和元年 7 月 9 日閣議決定）別表において民間競争入札の対象として選定された「マルウェア対策・WAF 機器の運用管理」について、公共サービス改革基本方針に従って、民間競争入札実施要項を定めるものとする。

2. マルウェア対策・WAF 機器の運用管理業務における運用要件の大枠（詳細は別紙 1 参照）及びその実施に当たり確保されるべき質に関する事項

(1) マルウェア対策・WAF機器の運用管理業務の概要

ア 対象となるマルウェア対策・WAF機器の運用管理業務の概要

(ア) 導入の経緯

昨今の我が国を取り巻くサイバーセキュリティ環境を鑑み、理研においても、サイバーセキュリティ対策の維持・強化をコスト効率を鑑みつつ、実施することを目的として、マルウェア対策の向上およびWebサーバのセキュリティ監視環境の強化を行うために本業務を実施している。

(イ) マルウェア対策・WAF機器の構成

・マルウェア対策システム

A. 標的型攻撃監視機能部

FireEye NX

B. 通信遮断機能部

IXIA ThreatARMOR

IXIA iBypass

・WAF システム

A. WAF 本体

Imperva X4510(SS-WAF-X451-H1)

Imperva M160(SS-M16-H1)

B. SSL 暗号／復号機

A10 Thunder3040S(TH3040-010-N1SSL-CFW)

イ 対象業務の内容

(ア) セキュリティ運用業務

- 「リアルタイム分析結果」および下記「月次レポート」を参照できる専用ポータルサイトを提供すること。
- 月末締め翌月第10営業日を目安に月次レポートを郵送で提出し、ポータルサイト上で提示すること。
- 監視機器から出力されるログを用い、24時間365日ログ分析を行うこと。
- 分析の結果、緊急性が高いと認められた場合、分析完了から 15 分以内に電話通知、調査結果から理研の指示により通信遮断を行うこと。また、後述するポータルサイト上に別途情報を提示すること。

(イ) 機器運用業務

- 機器の正常性を平日9時から17時にて監視し、異常がある場合は同時間帯内にて

障害対応を行うこと。

(ウ) 支援業務

- 理研における情報システム運用に必要とされる情報セキュリティに関する情報があれば適宜提供すること。
- 研究所のネットワーク、サーバ管理者からのマルウェア対策システム、Webサーバやコンテンツ・マネジメント、コンピュータセキュリティに関する問い合わせに対応すること。対応可能時間は、平日9時から17時とすること。

ウ 請負業務の引継ぎ

(ア) 現行請負者又は理研からの引継ぎ

理研は、当該引継ぎが円滑に実施されるよう、現行請負者及び請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務を新たに実施することとなった請負者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行請負者から業務の引継ぎを受けるものとする。なお、その際の事務引継ぎに必要な経費は、現行請負者の負担となる。

(イ) 請負期間満了の際の引継ぎ

理研は、当該引継ぎが円滑に実施されるよう、請負者及び次回請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務の終了に伴い請負者が変更となる場合には、本業務を受注した請負者は、当該業務の開始日までに、業務内容を明らかにした書類等により、次回請負者に対し、引継ぎを行うものとする。

なお、その際の事務引継ぎに必要な経費は、本業務を受注した請負者の負担となる。

(2) 確保されるべき対象業務の質

ア 業務内容

「マルウェア対策・WAF機器の運用管理業務に係る業務」に示す運用業務を適切に実施すること。

イ セキュリティ上の重大障害件数

個人情報、施設等に関する情報その他の契約履行に際し知り得た情報漏えいの件数は0件であること。

ウ マルウェア対策・WAF機器の運用管理業務上の重大障害件数

長期にわたり正常に稼働できない事態・状況及び保有するデータの喪失等により、業務に多大な支障が生じるような重大障害の件数は0件であること。

エ 基準時間完了率

メール（電話）による問い合わせがあった時点から、15分以内に問題が解決できた件数が、全問い合わせ件数のうち90%以上であること。

オ 問題解決率

全問い合わせの件数のうち、問題が解決できた問い合わせ件数の割合は、90%以上であること。

(3) 契約の形態及び支払

ア 契約の形態は、業務請負契約とする。

イ 理研は、業務請負契約に基づき、請負者が実施する本業務について、契約の履行に関し、マルウェア対策・WAF機器の運用管理業務の調達仕様書に定めた内容に基づく監督・検査を実施するなどして適正に実施されていることを確認した上で、適正な支払請求書を受領した日から30日以内に、毎月、契約金額を支払うものとする。確認の結果、確保されるべき対象業務の質が達成されていないと認められる場合、

又は達成できないおそれがある場合、理研は、確保されるべき対象業務の質の達成に必要な限りで、請負者に対して本業務の実施方法の改善を行うよう指示することができる。請負者は、当該指示を受けて業務の実施方法を改善し、業務改善報告書を速やかに理研に提出するものとする。なお、請負費は、本件業務開始以降のサービス提供に対して支払われるものであり、請負者が行う準備行為等に対して、請負者に発生した費用は、請負者の負担とする。

(5) 法令変更による増加費用及び損害の負担

法令の変更により事業者に生じた合理的な増加費用及び損害は、アからウに該当する場合には理研が負担し、それ以外の法令変更については請負者が負担する。

ア 本業務に類型的又は特別に影響を及ぼす法令変更及び税制度の新設

イ 消費税その他類似の税制度の新設・変更（税率の変更含む）

ウ 上記ア及びイのほか、法人税その他類似の税制度の新設・変更以外の税制度の新設・変更（税率の変更含む）

3. 実施期間に関する事項

業務請負契約の契約期間は、2020年4月1日から2022年3月31日までとする。

4. 入札参加資格に関する事項

(1) 法第15条において準用する法第10条各号（第11号を除く。）に該当する者でないこと。

(2) 予算決算及び会計令（昭和22年勅令第165号）第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別な理由がある場合に該当する。

(3) 予算決算及び会計令第71条の規定に該当しない者であること。

(4) 理研の競争契約参加資格又は国の競争参加資格（全省庁統一資格）のどちらかにおいて、2019年度に「役務の提供等」のA、B及びCのいずれかの等級に格付されている者であること。

(5) 法人税並びに消費税及び地方消費税の滞納がないこと。

(6) 労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。

(7) 理研及び府省等における物品等の契約に係る指名停止措置要領に基づく指名停止を受けている期間中でないこと。

(8) 調査研究や各工程の調達仕様書の作成に直接関与した事業者及びその関連事業者（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和38年大蔵省令第59号）第8条に規定する親会社及び子会社、同一の親会社をもつ会社並びに委託先事業者等の緊密な利害関係を有する事業者をいう。）でないこと。

(9) 調達計画書及び調達仕様書の妥当性確認並びに入札事業者の審査に関する業務を行うCIO補佐官及びその支援スタッフ等の属する又は過去2年間に属していた事業者でないこと。または、CIO補佐官等がその職を辞職した後に所属する事業者の所属部門（辞職後の期間が2年に満たない場合に限る。）でないこと。

(10) 単独で対象業務を行えない場合は、又は、単独で実施するより業務上の優位性があると判断する場合は、適正に業務を実施できる入札参加グループを結成し、入札に参加することができる。その場合、入札書類提出時までに入札参加グループを結成し、入札参加資格の全てを満たす者の中から代表者を定め、他の者は構成員として参加するものとする。また、入札参加グループの構成員は、上記(1)から(9)までの資格を満たす必要があり、他の入札参加グループの構成員となり、又は、単独で参加することはできない。なお、入札参加グループの代表者及び構成員は、入札参

加グループの結成に関する協定書（又はこれに類する書類）を作成し、提出すること。

（注）入札参加グループとは

本業務の実施を目的に複数の事業者が組織体を構成し、本業務の入札に参加することを指す。

- (11) 過去5年以内に中央府省庁、一部上場企業からSIEM基盤とセキュリティアナリストを用いたログの分析を受託した実績を有する者がプロジェクトに参画し、その者の実名で提示できること。
- (12) 過去5年以内に中央府省庁、一部上場企業から受託した情報セキュリティ監査業務を行った者が2名以上参加し、監査対象および実施者を実名で提示できること。
- (13) マルウェア対策システムから得られるセキュリティ情報から、予想される脅威を正確に、適切に分析できること。
- (14) 本業務を行う上での請負者の体制に、ITILエキスパート以上の資格を有する要員が参画していること。
- (15) 本業務を主管する組織（会社全体あるいは所属部門）が、ISO/IEC20000認証を取得していること。
- (16) 本業務を主管する組織（会社全体あるいは所属部門）が、JISQ27001 認証あるいは、ISO/IEC27001 認証を取得していること。
- (17) 本業務を主管する組織（会社全体あるいは所属部門）が、プライバシーマーク付与認定を取得していること。
- (18) 本業務を主管する組織（会社全体あるいは所属部門）が、ISO14001の認証を取得していること。
- (19) 現在、理研と同規模以上のシステムの監視実績を有し、かつ10Gbps以上のインターネット回線を有するシステムにおいて、不正侵入検知装置の監視実績を有すること。
- (20) CISSP(Certified Information Systems Security Professional)、あるいはCISSPとSSCP(Systems Security Certified Practitioner)が在籍し、セキュリティ監視作業に従事していること。
- (21) 10年以上のセキュリティ監視センター運営実績を持ち、1000センサー以上の監視実績を有すること。
- (22) 経済産業省の情報セキュリティ監査企業台帳に登録されている事業者であること。
- (23) プロジェクト管理者内には、情報セキュリティ監査業務の経験を3年以上、累計10件以上の情報システムをペネトレーション方式で監査した実績を有する者が存在すること。
- (24) プロジェクトメンバーは情報セキュリティに関する最新の脆弱性情報について収集・調査研究し、情報セキュリティに関し最新の知識を有しており、IPAやJPCERT/CCなどに対して脆弱性の報告を行っている実績を有すること。
- (25) 過去5年以内においてセキュリティ分野でGartner社またはIDC社などの外部評価機関の評価を受け、その評価結果が評価機関より公開されている企業であること。

5. 入札に参加する者の募集に関する事項

(1) スケジュール

入札公示：官報公示	2019年 11月中旬
入札説明会	11月下旬
質問受付期限	11月下旬

資料閲覧期限	2020年 1月上旬
提案書提出期限	1月上旬
提案書の審査	1月中旬頃
入札書提出期限	1月上旬頃
開札及び落札予定者の決定	1月下旬頃
契約締結	1月下旬頃

(2) 入札書類

入札参加者は、次に掲げる書類を別に定める入札説明書に記載された期日及び方法により提出すること。

ア 入札説明後の質問受付

入札公告以降、理研において入札説明書の交付を受けた者は、本実施要項の内容や入札に係る事項について、入札説明会後に、理研に対して質問を行うことができる。質問は原則として電子メールにより行い、質問内容及び理研からの回答は原則として入札説明書の交付を受けたすべての者に公開することとする。ただし、民間事業者の権利や競争上の地位等を害するおそれがあると判断される場合には、質問者の意向を聴取した上で公開しないよう配慮する。

イ 技術審査のための提案書等

別添1「マルウェア対策・WAF機器の運用管理仕様書」の各要求項目を満たすことができることを証明する書類を提出すること。理研は、これを用いて技術審査をおこなう。

ウ 定価見積書（見積原価内訳書）

人件費の単価証明書及び物件費の価格証明書を含んだ定価見積書
ただし、契約後に発生する経費のみとする。

エ 入札書

入札金額（入札参加者が消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、契約期間内の全ての請負業務に対する報酬の総額の110分の100に相当する金額）を記載した書類

オ 委任状

代理人に委任したことを証明する書類
ただし、代理人による入札を行う場合に限る。

カ 競争参加資格審査結果通知書の写し

理研の競争契約参加資格又は国の競争参加資格（全省庁統一資格）のどちらかにおいて、2019年度に「役務の提供等」のA、B及びCのいずれかの等級に格付されている者であることを証明する審査結果通知書の写し

キ 暴力団排除に関する書類（落札予定者となった者のみ提出。）

法第15条において準用する法第10条に規定する欠格事由のうち、暴力団排除に関する規定について評価するために必要な書類

6. マルウェア対策・WAF 機器の運用管理業務を実施する者を決定するための評価の基準その他本業務を実施する者の決定に関する事項

以下に本業務を実施する者の決定に関する事項を示す。

(1) 評価方法

本業務を実施する者の決定は、最低価格落札方式によるものとする。

(2) 落札者の決定

ア 別添1「マルウェア対策・WAF機器の運用管理仕様書」に示す全ての要求要件を満たし、かつ、入札価格が予算決算及び会計令第79条の規定に基づいて作成された

予定価格の制限の範囲内で最も低い者を落札者とする。ただし、予算決算及び会計令第84条の規定に該当する場合は、予算決算及び会計令第85条の基準を適用するので、基準に該当する入札が行われた場合は入札の結果を保留する。この場合、入札参加者は理研の行う事情聴取等の調査に協力しなければならない。

イ 調査の結果、会計法（昭和22年法律第35号）第29条の6第1項ただし書きの規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内で次順位の者を落札者とすることがある。

ウ 落札者となるべき者が2人以上あるときは、直ちに当該入札者にくじを引かせ、落札者を決定するものとする。また、入札者又は代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わってくじを引き、落札者を決定するものとする。

エ 契約担当官等は、落札者を決定したときに入札者にその氏名（法人の場合はその名称）及び金額を口頭で通知する。ただし、上記イにより落札者を決定する場合には別に書面で通知する。また、落札できなかった入札者は、落札の相対的な利点に関する情報（当該入札者と落札者のそれぞれの入札価格及び性能等の得点）の提供を要請することができる。

(3) 落札決定の取消し

次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、契約担当官等が、正当な理由があると認めたときはこの限りでない。

ア 落札者が、契約担当官等から求められたにもかかわらず契約書の取り交わしを行わない場合

イ 入札書の内訳金額と合計金額が符合しない場合

落札後、入札者に内訳書を記載させる場合がある。内訳金額が合計金額と符合しないときは、合計金額で入札したものとみなすため、内訳金額の補正を求められた入札者は、直ちに合計金額に基づいてこれを補正しなければならない。

(4) 落札者が決定しなかった場合の措置

初回の入札において入札参加者がなかった場合、必須項目を全て満たす入札参加者がなかった場合又は再度の入札を行ってもなお落札者が決定しなかった場合は、原則として、入札条件等を見直した後、再度公告を行う。

なお、再度の入札によっても落札者となるべき者が決定しない場合又は本業務の実施に必要な期間が確保できないなどやむを得ない場合は、自ら実施する等とし、その理由を官民競争入札等監理委員会（以下、「監理委員会」という。）に報告するとともに公表するものとする。

7. マルウェア対策・WAF 機器の運用管理業務に関する従来の実施状況に関する情報の開示に関する事項

(1) 開示情報

対象業務に関して、以下の情報は別紙1「従来の実施状況に関する情報の開示」のとおり開示する。

ア 従来の実施に要した経費

イ 従来の実施に要した施設及び設備

ウ 従来の実施方法等

(2) 資料の閲覧

前項ウ「従来の実施方法等」の詳細な情報は、民間競争入札に参加する予定の者から要望があった場合、月次レポート・リアルタイム分析結果等について、所定の手続を踏まえた上で閲覧可能とする。ホームページ等のウェブ上で閲覧可能な情報が

ある場合、リンク先を貼るなど閲覧が容易になるような工夫をするものとする。

また、民間競争入札に参加する予定の者から追加の資料の開示について要望があった場合は、理研は法令及び機密性等に問題のない範囲で適切に対応するよう努めるものとする。

8. マルウェア対策・WAF 機器の運用管理業務の請負業者に使用させることができる理研の施設・設備等に関する事項

(1) 理研の施設・設備等の使用

請負者は、本業務の遂行に必要な施設、設備等として、次に掲げる施設、設備等を適切な管理の下、無償で使用する事ができる。

ア 業務に必要な電気設備

イ その他、理研と協議し承認された業務に必要な施設、設備等

(2) 使用制限

ア 請負者は、本業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。

イ 請負者は、あらかじめ理研と協議した上で、理研の業務に支障を来さない範囲内において、施設内に運用管理業務の実施に必要な設備等を持ち込むことができる。

ウ 請負者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに、必要な原状回復を行う。

エ 請負者は、既存の建築物及び工作物等に汚損・損傷等を与えないよう十分に注意し、損傷（機器の故障等を含む。）が生じるおそれのある場合は、養生を行う。万一損傷が生じた場合は、請負者の責任と負担において速やかに復旧するものとする。

9. マルウェア対策・WAF 機器の運用管理業務請負者が、理研に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の本業務の適正かつ確実な実施の確保のために本業務請負者が講じるべき措置に関する事項

(1) 本業務請負者が理研に報告すべき事項、理研の指示により講じるべき措置

ア 報告等

(ア) 請負者は、仕様書に規定する業務を実施したときは、当該仕様書に基づく各種報告書を理研に提出しなければならない。

(イ) 請負者は、請負業務を実施したとき、又は完了に影響を及ぼす重要な事項の変更が生じたときは、直ちに理研に報告するものとし、理研と請負者が協議するものとする。

(ウ) 請負者は、契約期間中において、(イ)以外であっても、必要に応じて理研から報告を求められた場合は、適宜、報告を行うものとする。

イ 調査

(ア) 理研は、請負業務の適正かつ確実な実施を確保するために必要であると認めるときは、法第26条第1項に基づき、請負者に対し必要な報告を求め、又は理研の職員が事務所に立ち入り、当該業務の実施の状況若しくは記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

(イ) 立入検査をする理研の職員は、検査等を行う際には、当該検査が法第26条第1項に基づくものであることを請負者に明示するとともに、その身分を示す証明書を携帯し、関係者に提示するものとする。

ウ 指示

理研は、請負業務の適正かつ確実な実施を確保するために必要と認めるときは、請負者に対し、必要な措置を採るべきことを指示することができる。

(2) 秘密を適正に取り扱うために必要な措置

- ア 請負者は、本業務の実施に際して知り得た理研の情報等（公知の事実等を除く）を、第三者に漏らし、盗用し、又は請負業務以外の目的のために利用してはならない。これらの者が秘密を漏らし、又は盗用した場合は、法第54条により罰則の適用がある。
- イ 請負者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、請負者からの文書による申出を理研が認めた場合に限り、第三者へ開示できるものとする。
- ウ 請負者は、理研から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律（平成15年法律第57号）に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。
- エ アからウまでのほか、理研は、請負者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

(3) 契約に基づき請負者が講じるべき措置

ア 請負業務開始

請負者は、本業務の開始日から確実に業務を開始すること。

イ 権利の譲渡

請負者は、債務の履行を第三者に引き受けさせ、又は契約から生じる一切の権利若しくは義務を第三者に譲渡し、承継せしめ、若しくは担保に供してはならない。ただし、書面による理研の事前の承認を得たときは、この限りではない。

ウ 権利義務の帰属等

- (ア) 本業務の実施が第三者の特許権、著作権その他の権利と抵触するときは、請負者は、その責任において、必要な措置を講じなくてはならない。
- (イ) 請負者は、本業務の実施状況を公表しようとするときは、あらかじめ、理研の承認を受けなければならない。

エ 瑕疵担保責任

- (ア) 理研は、成果物の引渡し後に発見された瑕疵について、引渡し後1年間は、請負者に補修を請求できるものとし、補修に必要な費用は、全て請負者の負担とする。
- (イ) 成果物の瑕疵が請負者の責に帰すべき事由によるものである場合は、理研は、前項の請求に際し、これによって生じた損害の賠償を併せて請求することができる。

オ 再委託

- (ア) 請負者は、本業務の実施に当たり、その全部を一括して再委託してはならない。
- (イ) 請負者は、本業務の実施に当たり、その一部について再委託を行う場合には、原則として、あらかじめ機能証明書において、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法（以下「再委託先等」という。）について記載しなければならない。
- (ウ) 請負者は、契約締結後やむを得ない事情により再委託を行う場合には、再委託先等を明らかにした上で、理研の承認を受けなければならない。
- (エ) 請負者は、(イ)又は(ウ)により再委託を行う場合には、請負者が理研に対して負う義務を適切に履行するため、再委託先の事業者に対し前項「(2)秘密を適正に取り扱うために必要な措置」及び本項「(3)契約に基づき請負者が講じるべ

き措置」に規定する事項その他の事項について、必要な措置を講じさせるとともに、再委託先から必要な報告を聴取することとする。

- (オ) (イ)から(エ)までに基づき、請負者が再委託先の事業者に義務を実施させる場合は、全て請負者の責任において行うものとし、再委託先の事業者の責に帰すべき事由については、請負者の責に帰すべき事由とみなして、請負者が責任を負うものとする。

カ 契約内容の変更

理研及び請負者は、本業務の質の確保の推進、またはその他やむをえない事由により本契約の内容を変更しようとする場合は、あらかじめ変更の理由を提出し、それぞれの相手方の承認を受けるとともに法第21条の規定に基づく手続を適切に行わなければならない。

キ 契約の解除

理研は、請負者が次のいずれかに該当するときは、請負者に対し請負費の支払を停止し、又は契約を解除若しくは変更することができる。この場合、請負者は理研に対して、契約金額の100分の10に相当する金額を違約金として支払わなければならない。その場合の算定方法については、理研の定めるところによる。ただし、同額の超過する増加費用及び損害が発生したときは、超過分の請求を妨げるものではない。

また、請負者は、理研との協議に基づき、本業務の処理が完了するまでの間、責任を持って当該処理を行わなければならない。

- (ア) 法第22条第1項イからチまで又は同項第2号に該当するとき。

- (イ) 暴力団員を、業務を統括する者又は従業員としていることが明らかになった場合。

- (ウ) 暴力団員と社会的に非難されるべき関係を有していることが明らかになった場合。

- (エ) 再委託先が、暴力団若しくは暴力団員により実質的に経営を支配される事業を行う者又はこれに準ずる者に該当する旨の通知を、警察当局から受けたとき。

- (オ) 再委託先が暴力団又は暴力団関係者と知りながらそれを容認して再委託契約を継続させているとき。

ク 談合等不正行為

請負者は、談合等の不正行為に関して、理研が定める「談合等の不正行為に関する特約条項」に従うものとする。

ケ 損害賠償

請負者は、請負者の故意又は過失により理研に損害を与えたときは、理研に対し、その損害について賠償する責任を負う。また、理研は、契約の解除及び違約金の徴収をしてもなお損害賠償の請求をすることができる。なお、理研から請負者に損害賠償を請求する場合において、原因を同じくする支払済の違約金がある場合には、当該違約金は原因を同じくする損害賠償について、支払済額とみなす。

コ 不可抗力免責・危険負担

民間事業者は、上記事項にかかわらず、不可抗力により請負事業の全部若しくは一部の履行が遅延又は不能となった場合は当該責任を負わないものとする。

理研及び請負者の責に帰すことのできない事由により契約期間中に物件が滅失し、又は毀損し、その結果、理研が物件を使用することができなくなったときは、請負者は、当該事由が生じた日の翌日以後の契約期間に係る代金の支払を請求することができない。

サ 金品等の授受の禁止

請負者は、本業務の実施において、金品等を受け取ること、又は、与えることをしてはならない。

シ 宣伝行為の禁止

請負者及び本業務に従事する者は、本業務の実施に当たっては、自ら行う事業の宣伝を行ってはならない。また、本業務の実施をもって、第三者に対し誤解を与えるような行為をしてはならない。

ス 法令の遵守

請負者は、本業務を実施するに当たり適用を受ける関係法令等を遵守しなくてはならない。

セ 安全衛生

請負者は、本業務に従事する者の労働安全衛生に関する労務管理については、責任者を定め、関係法令に従って行わなければならない。

ソ 記録及び帳簿類の保管

請負者は、本業務に関して作成した記録及び帳簿類を、本業務実施中は厳重に管理し、本業務を終了した場合には、理研が要求する記録及び帳簿類を理研に納品すること。

タ 契約の解釈

契約に定めのない事項及び契約に関して生じた疑義は、理研と請負者との間で協議して解決する。

10. マルウェア対策・WAF 機器の運用管理業務請負者が本業務を実施するに当たり第三者に損害を加えた場合において、その損害の賠償に関し契約により本業務請負者が負うべき責任に関する事項

本業務を実施するに当たり、請負者又はその職員その他の本業務に従事する者が、故意又は過失により、本業務の受益者等の第三者に損害を加えた場合は、次のとおりとする。

- (1) 理研が国家賠償法第1条第1項等の規定に基づき当該第三者に対する賠償を行ったときは、理研は請負者に対し、当該第三者に支払った損害賠償額（当該損害の発生について理研の責めに帰すべき理由が存する場合は、理研が自ら賠償の責めに任ずべき金額を超える部分に限る。）について求償することができる。
- (2) 請負者が民法（明治29年法律第89号）第709条等の規定に基づき当該第三者に対する賠償を行った場合であって、当該損害の発生について理研の責めに帰すべき理由が存するときは、請負者は理研に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責めに任ずべき金額を超える部分を求償することができる。

11. マルウェア対策・WAF 機器の運用管理業務に係る法第7条第8項に規定する評価に関する事項

(1) 本業務の実施状況に関する調査の時期

理研は、本業務の実施状況について、総務大臣が行う評価の時期（2021年5月を予定）を踏まえ、本業務開始後、毎年3月に状況を調査する。

(2) 調査項目及び実施方法

ア システム運用上の重大障害の件数

マルウェア対策・WAF機器の運用管理業務報告書等により調査

(3) 意見聴取等

理研は、必要に応じ、本業務請負者から意見の聴取を行うことができるものとする。

(4) 実施状況等の提出時期

理研は、2021年4月を目途として、本業務の実施状況等を総務大臣及び監理委員会へ提出する。

なお、調査報告を総務大臣及び監理委員会に提出するに当たり、CIO補佐官及び外部有識者の意見を聴くものとする。

12. その他業務の実施に関し必要な事項

(1) マルウェア対策・WAF機器の運用管理業務の実施状況等の監理委員会への報告

理研は、法第26条及び第27条に基づく報告徴収、立入検査、指示等を行った場合には、その都度、措置の内容及び理由並びに結果の概要を監理委員会へ報告することとする。

(2) 理研の監督体制

本契約に係る監督は、主管係自ら立会い、指示その他の適切な方法によって行うものとする。

本業務の実施状況に係る監督は以下のとおり。

監督職員：情報システム部 情報化戦略・基盤課 技師 古沢 秀明

検査職員：情報システム部 部長

(3) 本業務請負者の責務等

ア 本業務に従事する請負者は、刑法（明治40年法律第45号）その他の罰則の適用については、法令により公務に従事する職員とみなされる。

イ 請負者は、法第54条の規定に該当する場合は、1年以下の懲役又は50万円以下の罰金に処される。

ウ 請負者は、法第55条の規定に該当する場合は、30万円以下の罰金に処されることとなる。なお、法第56条により、法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、法第55条の規定に違反したときは、行為者を罰するほか、その法人又は人に対して同条の刑を科する。

エ 請負者は、会計検査院法（昭和22年法律第73号）第23条第1項第7号に規定する者に該当し、会計検査院が必要と認めるときには、同法第25条及び第26条により、同院の実地の検査を受けたり、同院から直接又は理研を通じて、資料又は報告等の提出を求められたり、質問を受けたりすることがある。

(4) 著作権

ア 請負者は、本業務の目的として作成される成果物に関し、著作権法第27条及び第28条を含む著作権の全てを理研に無償で譲渡するものとする。

イ 請負者は、成果物に関する著作権者人格権（著作権法第18条から第20条までに規定された権利をいう。）を行使しないものとする。ただし、理研が承認した場合は、この限りではない。

ウ ア及びイに関わらず、成果物に請負者が既に著作権を保有しているもの（以下「請負者著作物」という。）が組み込まれている場合は、当該請負者著作物の著作権についてのみ、請負者に帰属する。

エ 提出される成果物に第三者が権利を有する著作物が含まれる場合には、請負者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行うものとする。

(5) マルウェア対策・WAF機器の運用管理業務の調達仕様書

本業務を実施する際に必要な仕様は、別添1「マルウェア対策・WAF機器の運用管理仕様書」に示すとおりである。

別紙 1

従来の実施状況に関する情報の開示

1 従来の実施に要した経費		(単位：千円) (税抜き)		
		2017年度	2018年度	2019年度
人件費	常勤職員	—	—	—
	非常勤職員	—	—	—
物件		—	—	—
請負費 等	役務	45,100	35,100	39,990
	機器・回線等			
	その他			
計(a)		45,100	35,100	39,990
参 考 値	減価償却費	—	—	—
	退職給付費用	—	—	—
(b)	間接部門費	—	—	—
(a) + (b)		45,100	35,100	39,990
<p>(注記事項)</p> <p>理研では、民間競争入札の対象であるマルウェア対策・WAF機器の運用管理業務の全部を請負契約により実施している。</p> <p>なお、支払い金額は、一般競争入札の落札額である。</p> <p>2018年の金額の減額理由は、監視項目を重要度によって絞り込んだためである。</p> <p>2019年の金額の増加理由は、管理業務の内容を追加したためである。</p> <p>※ 請負契約のため、費用の詳細な内訳の開示は受けられない。</p>				

2 従来の実施に要した施設及び設備

理研

【施設】

施設名称: SINET埼玉データセンター

使用場所: 非公開

【設備】

運用対象

マルウェア対策機器 2 台、通信遮断器 2 台、WAF機器 3 台、SSL機器 2 台

請負者所有

VPNルータ1台、SOC、SEAM

外部拠点

なし

3 従来の実施方法等

従来の実施方法（業務フロー図等）

（セキュリティ監視）請負者によるログ監視→インシデント・重大判定→理研に通報

（機器監視）請負者による機器監視→異常判定→保守業者に連絡し保守対応→対応完了、

↓理研に連絡

理研

に連絡

（注記事項）

メール通知件数：2018年度6件、2019年度（8月まで）3件

→メール通知の内容：インシデント発生時の連絡（メール通知後電話連絡）

問い合わせ件数：2018年度11件、2019年度（8月まで）6件

→問い合わせの内容：理研からおこなった機器の挙動や作業内容の問合せ

作業件数：2018年度6件、2019年度（8月まで）9件

→作業件数：理研からおこなった設定変更等の作業依頼

2019年度は作業要件を追加した。

別添 1 調達仕様書

マルウェア対策・WAF 機器の運用管理
Audit and support to protect network and computer security
仕様書

国立研究開発法人理化学研究所

1. 業務の目的

情報漏えいや計算機への不正侵入等、サイバーセキュリティの事故は、被害の対象となった情報システムや個人端末だけでなく、それらを管理する個人、組織に深刻なダメージを与える。国立研究開発法人理化学研究所（以下「研究所」という。）においても例外でなく、情報漏えい事故等が発生すれば研究所の社会的信用を著しく損ない、組織運営に大きな影響を及ぼす恐れがある。したがって、これらのサイバーセキュリティ上の事故は絶対に防がなければならない、そのためには適切な情報システムの運用とセキュリティ管理が必要となる。

本業務は、利用者端末からの通信状況から研究所の情報および情報システム等に対するセキュリティ管理を行い、サイバーセキュリティ上の事故から守る事を目的とする。

2. 概要

本業務は、研究所のサイバーセキュリティ対策等によりインターネットからの脅威、特にマルウェアと WAF(Web Application Firewall)による監視する「セキュリティ監視・対応」から構成される。受注者は契約期間内において以下に述べる仕様を満たした業務を提供し、研究所の情報セキュリティ管理業務を補助する。

3. 契約期間

2020年4月1日から2022年3月31日までとする。

4. 装置設置場所

NTT 東日本埼玉データセンター内国立研究開発法人理化学研究所ラック
埼玉県和光市広沢 2-1 国立研究開発法人理化学研究所研究本館

研究所のネットワーク環境の将来の変更などにより本契約期間中に装置の設置場所変更の必要が生じた場合は別途協議するものとする。

5. 監督員および検査員

監督員 情報システム部情報化戦略・基盤課 技師 古沢 秀明
検査員 情報システム部 部長

6. 秘密保持等

(ア) 受注者は研究所で見たもの、および研究所から開示された作業資料等の秘密情報(以下「情報」という。)については秘密を保持し、研究所の書面(電子メール含む)による事前の同意を得た場合を除きこれを第三者に開示または漏洩してはならない。但し、次の各号のいずれかに該当する情報についてはこの限りではない。

A) 研究所から開示を受ける前に公知であったかまたは開示を受けた後、受注者の責

によらず公知となった情報

- B) 受注者が開示を受ける前に保有していたことを証明できる情報
 - C) 受注者が独自に開発したことを証明できる情報
 - D) 正当な権限を有する第三者から開示を受けた情報
- (イ) 受注者は情報を本作業のためにのみ使用し、他の目的に使用しないものとする。
- (ウ) 受注者は本作業の実施にあたって、研究所の機密に属する事項は秘匿を厳守するものとする。
- (エ) 受注者は本作業の終了に当たり、研究所から開示された作業資料等の処分につき研究所担当者の指示に従うものとする。

7. 構成機能部とシステム構成

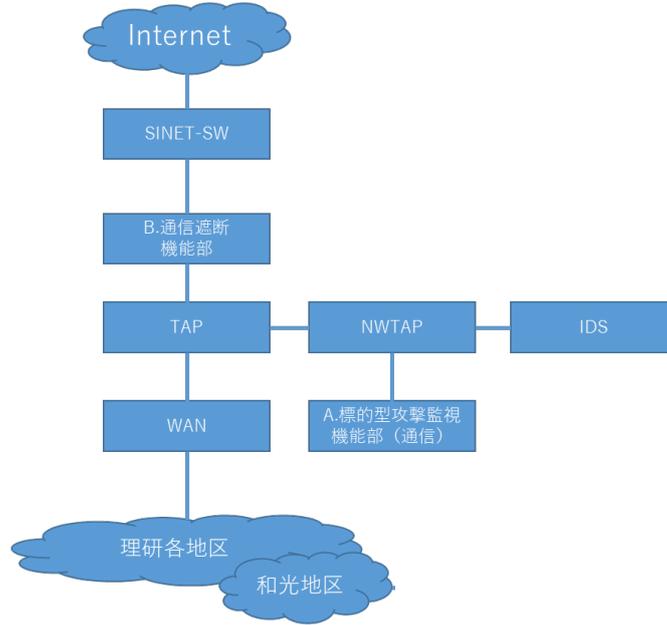
マルウェア対策システム

- A. 標的型攻撃監視機能部 一式
FireEye NX
- B. 通信遮断機能部 一式
IXIA ThreatARMOR
IXIA iBypass

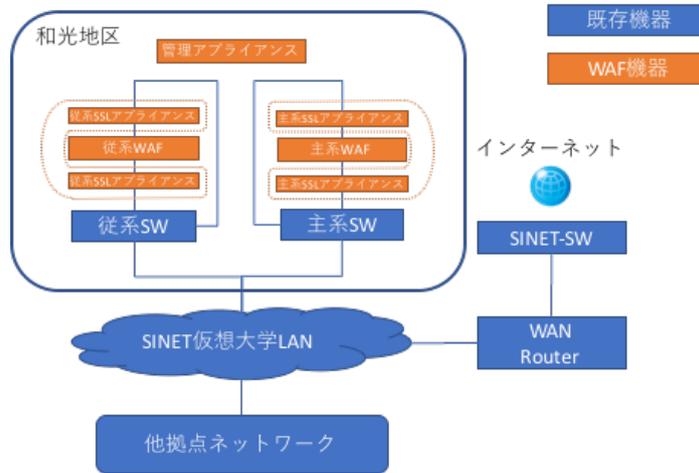
WAF システム

- WAF 本体 一式
Imperva X4510(SS-WAF-X451-H1)
Imperva M160(SS-M16-H1)
- SSL 暗号／復号機 一式
A10 Thunder3040S(TH3040-010-N1SSL-CFW)

マルウェア対策システム構成



WAF システム構成



8. 業務内容

以下に記載する「セキュリティ監視(ア)」「業務支援(イ)」の2つのサービス及びそれらに必要な環境(ウ、エ、オ)を提供すること。

(ア) セキュリティ監視要件

- ✓ 下記の「月次レポート」を参照できる専用ポータルサイトを提供すること。
- ✓ 月末締め翌月第10営業日を目安に月次レポートを郵送で提出し、ポータルサイト上で提示すること。
- 標的型攻撃監視機能部
 - 全体
 - 標的型攻撃監視機能部を用い、24時間365日ログ分析を行うこと。
 - 「リアルタイム分析結果」が参照可能であること。
 - 監視機能
 - (1) マルウェア対策システムの標的型攻撃監視機能部と通信遮断機能部を自動および手動にて適宜連携させること。
 - (2) 時系列分析、攻撃プロセスのロジック化など、複数の独自検知ルールを保有していること。
 - (3) C&C サーバ等について独自のブラックリストを保有し不審な通信を検知することが可能なこと。
 - 機器監視・復旧対応
 - (1) 標的型攻撃監視機能部の機器の正常性を平日9時から17時にて監視し異常がある場合は同時間帯内にて障害対応を行うこと。
 - (2) 通信を処理するインターフェイスのリンクダウンは、ポーリングとTrapによる監視をすること。
 - (3) 障害発生時は一次切り分けを実施し、機器故障の場合は復旧まで対応すること。なお、各機器の保守契約は研究所にて別途締結する。
 - 運用・解析体制
 - (1) SIEM (Security Information and Event Management) 基盤を用いて標的型攻撃監視機能部からのログの分析を実施すること。
 - (2) 分析の結果、緊急性が高いと認められた場合、分析完了から15分以内に電話通知、調査結果から研究所からの指示により通信遮断を行うこと。また、後述するポータルサイト上に別途情報を提示すること。
 - (3) SIEM 基盤は常に最新の脅威についての情報収集を行い、ロジック

をアップデートし、最適なものへ更新すること。

- (4) SIEM 基盤には AI を含む常時 500 以上のロジックが存在していること。
- (5) 機器から研究所の SIEM に対してもログ転送が行えること。
- (6) 検知されたアラートは、SIEM を用いた自動分析に加え、標的型攻撃対策機能部が 検知したログ (PCAP データを含む) をアナリストがリアルタイムに分析を行い、予め定められた 4 段階の重要度に判別してリアルタイムに通知すること。また、月次で検知件数などを報告すること。
- (7) 通知内容には、該当端末の IP アドレス、マルウェアの接続先 IP アドレス、URL 等、アナリストが脅威と判定した理由等および、推奨する対応策が記載されていること。
- (8) コンフィグバックアップ、各種バージョンアップ作業やパッチの適用などを行い、標的型攻撃監視機能部を適切な状態に保持できること。検証や手順書作成が必要な場合は別途調達とする。
- (9) 原則、既に設定済みのポリシーを踏襲すること。新たにポリシーチューニングが必要な場合は別途調達とする。但し、運用過程において、特定シグネチャに対する設定変更 (非通知設定等) の必要性が判明した場合、研究所からの指示に基づき月 5 件までを目安に対応すること。

- 通信遮断機能部

- 機器運用・監視・復旧対応

- (1) 通信遮断機能部の正常性を平日 9 時から 17 時にて監視し異常がある場合は同時間帯内にて障害対応を行うこと。
- (2) 通信を処理するインターフェイスのリンクダウンは、ポーリングと Trap による監視をすること。
- (3) 障害発生時は一次切り分けを実施し、機器故障の場合は復旧まで対応すること。なお、各機器の保守契約は研究所にて別途締結する。
- (4) マルウェア対策システムの標的型攻撃監視機能部と通信遮断機能部を自動または手動にて適宜連携させること。
- (5) 自動更新される定義リストに加えて、任意の遮断/許可のブロックリスト設定作業を実施すること。
- (6) コンフィグバックアップ、各種バージョンアップ作業やパッチの適用などを行い、通信遮断機能部を適切な状態に保持できること。検証や手順書作成が必要な場合は別途調達とする。

- (7) 受注者からの一方的な連絡通知だけではなく、研究所の担当者がセキュリティ状況を確認できること。
- (8) ブロックした不正 IP アドレスに関して、PDF 形式の月次レポートとして出力すること。

- WAF システム部

- 機器運用・監視・復旧対応

- (1) WAF 部の正常性を平日 9 時から 17 時にて監視し、異常がある場合は同時間帯内にて障害対応を行うこと。
- (2) SSL 暗号復号機の証明書の管理、切り替え作業を行うこと。年に数件程度を想定すること。
- (3) SSL 暗号復号機/WAF 配下に設置されるサーバの登録／削除／変更などの管理を行うこと。月に数件程度を想定すること。
- (4) 通信を処理するインターフェイスのリンクダウンは、ポーリングと Trap による監視をすること。
- (5) 障害発生時は一次切り分けを実施し、機器故障の場合は復旧まで対応すること。なお、各機器の保守契約は研究所にて別途締結する。
- (6) WAF は、自動更新される定義に加えて、任意の遮断/許可のブロックリスト設定作業を実施すること。
- (7) コンフィグバックアップ、各種バージョンアップ作業やパッチの適用などを行い、適切な状態に保持できること。検証や手順書作成が必要な場合は別途調達とする。
- (8) 受注者からの一方的な連絡通知だけではなく、研究所の担当者がセキュリティ状況を確認できること。
- (9) ブロックした不正 IP アドレスに関して、PDF 形式の月次レポートおよび CSV ファイルとして出力すること。
- (10) 原則、既に設定済みのポリシーを踏襲すること。新たにポリシーチューニングが必要な場合は別途調達とする。但し、運用過程において、特定シグネチャに対する設定変更（ブロック設定/非通知設定等）の必要性が判明した場合、研究所からの指示に基づき月 5 件までを目安に対応すること。

(イ) 業務支援

- (1) 研究所における情報システム運用に必要とされる情報セキュリティに関する情報があれば適宜提供すること。
- (2) 研究所のネットワーク、サーバ管理者からのマルウェア対策システム、Web サーバやコ

ンテンツ・マネジメント、コンピュータセキュリティに関する問い合わせに対応すること。
対応可能時間は、平日 9 時から17時とすること。

(ウ) 受注者に求める要件（応札時に証する資料を提出すること）

- (1) 監視センター等に常時セキュリティ監視の専門技術者を配置し、本業務を実施すること。なお監視センターは、平日 9 時から 17 時半の間で有人監視が可能な設備、人数規模を持つこと。
- (2) 過去 5 年以内に中央府省庁、一部上場企業から SIEM 基盤とセキュリティアナリストを用いたログの分析を受託した実績を有する者がプロジェクトに参画し、その者の実名で提示できること。
- (3) 過去 5 年以内に中央府省庁、一部上場企業から受託した情報セキュリティ監査業務を行った者が 2 名以上参加し、監査対象および実施者を実名で提示できること。
- (4) マルウェア対策システムから得られるセキュリティ情報から、予想される脅威を正確に、適切に分析すること。
- (5) 本業務を行う上での受注者の体制に、ITIL エキスパート以上の資格を有する要員が参画していること。
- (6) 本業務を主管する組織（会社全体あるいは所属部門）が、ISO/IEC20000 認証を取得していること。
- (7) 本業務を主管する組織（会社全体あるいは所属部門）が、JISQ27001 認証あるいは、ISO/IEC27001 認証を取得していること。
- (8) 本業務を主管する組織（会社全体あるいは所属部門）が、プライバシーマーク付与認定を取得していること。
- (9) 本業務を主管する組織（会社全体あるいは所属部門）が、ISO14001 の認証を取得していること。
- (10) 現在、研究所と同規模以上のシステムの監視実績を有し、かつ 10Gbps 以上のインターネット回線を有するシステムにおいて、不正侵入検知装置の監視実績を有すること。
- (11) CISSP(Certified Information Systems Security Professional)、あるいは CISSP と SSCP(Systems Security Certified Practitioner)が在籍し、セキュリティ監視作業に従事していること。
- (12) 10 年以上のセキュリティ監視センター運営実績を持ち、1000 センサー以上の監視実績を有すること。
- (13) 経済産業省の情報セキュリティ監査企業台帳に登録されている事業者であること。
- (14) プロジェクト管理者内には、情報セキュリティ監査業務の経験を 3 年以上、累

計 10 件以上の情報システムをペネトレーション方式で監査した実績を有する者が存在すること。

- (15) プロジェクトメンバーは情報セキュリティに関する最新の脆弱性情報について収集・調査研究し、情報セキュリティに関し最新の知識を有しており、IPA や JPCERT/CC などに対して脆弱性の報告を行っている実績を有すること。
- (16) 過去 5 年以内においてセキュリティ分野で Gartner 社または IDC 社などの外部評価機関の評価を受け、その評価結果が評価機関より公開されている企業であること。

(エ) 必要機材等

- (1) 機材等を設置する場合は、研究所が指定する設置場所、電源の仕様に収めること。設置場所は 42U の 19 インチラック内とし、電源は 100V 2A までとする。
- (2) 本業務の実施にあたって必要な機材や回線は、受注者にて準備すること。

(オ) その他

- (1) 本業務を通じて、取り扱う情報、通信、設備その他のセキュリティを確保すること。また、その事実を客観的に証明すること。
- (2) 受注者(再委託がある場合は再委託先を含む。以下同様。)は、適切なセキュリティポリシー、セキュリティガイドラインを元に本業務を実施し、下記の研究所のセキュリティポリシー、ガイドラインを遵守すること。
- (3) 本業務において、受注者の責により事故、業務中断を発生させた場合は、都度原因究明と再発防止策を実施し、研究所に書面にて報告すること。
- (4) 本業務で作成する報告書について、研究所と協議の上で適宜見直すこと。
- (5) 本業務にて発生する情報は、必要に応じて暗号化、認証等を行い、情報漏えい、盗難等に備えること。
- (6) 受注者は本業務において得られた各種情報等について守秘義務を負い、研究所の許可なく第三者に対して開示してはならない。本業務に携わる全ての者に遵守させること。ただし、既に公知であった情報についてはこれに該当しない。
- (7) 本業務の運用に必要な情報は、研究所よりすべて提供する。

9. ドキュメント

本運用業務により以下の書類の記述内容が変更になった際は修正を行うこと。

- (1) 「連絡体制図」
- (2) 「システム構成図」
- (3) 「運用手順書」

10. 運用

ISO27001 を踏まえたセキュリティ対応の PDCA を構築し、ISO20000 に準拠した IT サービス提供を行うマネジメントを実施するため、以下を踏まえた運用を行うこと。

1. ITサービス管理プロセス全体の体系およびPDCA サイクルを定義し、連絡体制を含めた実フローを明示すること。
2. 本業務の適用範囲を明確に定義すること。
3. 本業務で用いる用語を定義すること。
4. 本仕様書での要求要件を踏まえたマネジメントシステムの要求事項を整理すること。
5. 本業務を実施するにあたって必要となるサービスマネジメントの計画・実施を行うこと。
6. 本業務で必要となる各プロセスが明確に定義されていること。
7. 本業務を実施するために必要となる運用指標 (KPI) が定義されていること。
8. 研究所と受注者の間で KPI を踏まえた SLA が定義出来る状態であること。

11. 運用ドキュメントフォーマット

本仕様にて作成される各種運用ドキュメントは研究所にて修正可能なフォーマットにて提出すること。各ドキュメント内で使用されている構成図等においても、作成したアプリケーションで修正可能な形式で別途提出すること。

研究所にて対応可能ソフトウェアは以下のとおりである。提出用書類に最適なソフトウェアを選択し使用すること。

- マイクロソフト社製 Word
- マイクロソフト社製 Excel
- マイクロソフト社製 PowerPoint
- マイクロソフト社製 Visio

12. セキュリティ基準の遵守

- (1) 本業務に関連して研究所内で計算機、ネットワーク等を扱う場合は、原則として研究所の定める情報セキュリティポリシー、ガイドラインを遵守すること。
- (2) 作業用計算機等を管理する担当者を定め、緊急時の連絡先とともに研究所に報告すること。
- (3) 作業用計算機等を研究所に持ち込む際は、あらかじめ研究所の許可を得ること。
- (4) 作業用計算機等においては、かならずウィルス対策を実施すること。
- (5) 作業用計算機等上でファイル交換ソフトウェアを使用しないこと。
- (6) 本業務において著作権の侵害行為を行わないこと。
- (7) 本業務に関するネットワーク構成図、システム情報、機器設定情報等を研究所

外に持ち出さないこと。持ち出す必要がある場合はあらかじめ研究所の許可を得ること。

- (8) その他業務実施上、情報セキュリティに関連する対策等について研究所の求めがある時は、これに協力すること。

13. サービス品質保証

研究所は必要に応じて作業の進捗状況、不具合処理に関して監督を行う。受注者は必要に応じ本契約が履行された事が確認可能な書類を作成提出すること。受注者は「品質マネジメントシステム(ISO9001:2015)」の認証を取得すること。

14. その他

- (1) 作業の実施に際しては、誠意をもって行うものとし、上記資格保持者などが事前に十分に教育を受けた技術力を有する者を派遣すること。教育を受けたことを証明すること。
- (2) 研究所の事前の了承が無い作業遅延、受注者の瑕疵責任による障害、先に述べたセキュリティ基準を遵守せずセキュリティ事故等を発生させた場合は、都度研究所に始末書を提出すること。
- (3) 受注者の瑕疵責任によるシステム障害、先に述べたセキュリティ基準を遵守せずセキュリティ事故を発生させた場合は、受注者の責において全ての対応、修復等を行うこと。
- (4) 受注者の業務遂行能力が著しく劣ると研究所が判断した場合は、契約期間中であっても契約解除に応じること。
- (5) 上記の契約解除において、研究所に損害が発生したと認める場合には損害賠償に応じること。
- (6) 本業務を履行する上で事故、異常等を認めた場合は、速やかに当研究所担当者に連絡すること。

15. 仕様書の疑義

本仕様書に対する疑義または本仕様により解決出来ない問題が発生した場合は、研究所監督員と協議の上決定すること。

以 上