

入札説明書

ネットワーク不正通信対策業務

- | | | |
|----|-------|---------------|
| 1. | 入札説明書 | P 1 ~ P 6 |
| 2. | 別紙様式 | P 7 ~ P 1 1 |
| 3. | 記入例 | P 1 2 ~ P 1 4 |
| 4. | 仕様書 | P 1 5 ~ P 1 8 |

平成 2 9 年 1 2 月

法人企画部総務課

入札説明書

ネットワーク不正通信対策業務に係る一般競争入札については、関係法令に定めるもののほか、この入札説明書によるものとします。

1. 公告日

平成29年12月13日（水）

2. 入札に関する内容

(1) 入札物件

ネットワーク不正通信対策業務

(詳細は、仕様書のとおりとします。)

(2) 完了期限

平成30年3月31日（土）

(3) 作業場所

奈良県橿原市四条町840番地 公立大学法人奈良県立医科大学

3. 入札参加資格

次に掲げる条件のすべてに該当する者が、この入札に参加することができます。

- (1) 公立大学法人奈良県立医科大学物品購入等の契約に係る取引停止等措置要領に基づく取引停止等の措置(奈良県の入札参加資格停止の措置を含む。)期間中でないこと。
- (2) 奈良県における物品購入等に係る競争入札の参加資格者で、営業種目がB1⑤の「コンピュータ、周辺機器」、Q2の「電算業務」またはQ7⑯の「その他サービス」に登録されている者であること。奈良県(会計局総務課調達契約係)へ届けた印章について、受付されたことを証するため、受付印が押された届けの控えの写しを提出すること。
- (3) 仕様書に示した仕様と同等以上の業務実績(国、地方公共団体または独立行政法人と、2件以上の契約実績)があることを証明できる者であること。
- (4) 会社更生法(平成14年法律第154号)第17条の規定による更正手続開始の申立て同法附則第2条の規定によりなお従前の例によることとされる更正事件(以下「旧更正事件」。)に係る同法による改正前の会社更生法(昭和27年法律第172号。以下「旧法」。)第30条に規定する更正手続開始の申立てを含む。)をしていない者または申立てをなされていない者であること。ただし、会社更生法に基づく更正手続開始の決定(旧更正事件に係る旧法に基づく更正手続開始の決定を含む。)を受けた者については、更正手続開始の申立てをしなかった者または申立てをなされなかった者とみなす。
- (5) 平成12年3月31日以前に民事再生法(平成11年法律第225号)附則第2条の

規定による廃止前の和議法(大正11年法律第72号)第12号第1項の規程による和議開始の申立てをしていない者であること。

- (6) 平成12年4月1日以後に民事再生法第21条に規定する再生手続開始の申立てをしていない者または申立てをなされていない者であること。ただし、同法に基づく再生手続開始の決定を受けた者であって、再生計画の認可の決定を受けた場合は、再生手続開始の申立てをしなかった者または申立てをなされなかった者とみなす。
- (7) 情報セキュリティ対策に関する24時間対応のSOCを有し、本業務に関する不正通信監視に24時間対応出来ること。
- (8) 本業務に関し、本学への支援を適切かつ遅滞なく行うためのチーム体制を整備すること。なお、チームメンバー構成においては、情報セキュリティアドミニストレータ試験合格者およびネットワークスペシャリスト有資格者をそれぞれ1名以上含むこと。

4. 入札参加申込

(1) 申込(申請)受付場所

〒634-8521 奈良県橿原市四条町840番地

公立大学法人奈良県立医科大学

法人企画部 総務課情報推進係 那須、熊谷

TEL: 0744-22-3051 (内線: 2162)

FAX: 0744-29-8815

E-Mail: ictwork@naramed-u.ac.jp

(2) 提出期限

提出期限 平成30年1月11日(木)午後3時まで

郵送不可

(3) 提出書類

- ① 入札参加資格審査結果通知書の写し
- ② 業務実績報告書(別紙様式1)
- ③ 3. 入札参加資格の(7)、(8)について確認できる資料
(様式自由、代表者印必要、なお個人名は含めないこと)

5. 入札参加資格の確認

入札参加資格の有無については、4.(3)に示した提出書類に基づいて確認し、その結果を平成30年1月17日(水)までに入札参加申込者に対し、FAXにより通知します。

6. 入札説明会

入札説明会は行いません。

7. 仕様書等に関する質問方法

入札説明書、仕様書等に関して質問がある場合は、質問票（別紙様式5）を作成し、平成29年12月20日(水)午後3時までに4.(1)の場所まで電子メールで提出して下さい。尚、質問票を提出する場合は、必ず事前にその旨電話下さい。

（電話による質問および土・日・祝日は不可とします。）

質問に対する回答は、平成29年12月25日（月）までに全員にメールで回答します。

8. 入札、開札の日時および場所

平成30年1月23日（火） 午後2時00分から

公立大学法人奈良県立医科大学 大学本部棟3階 小会議室

9. 入札書の提出方法

(1) 入札書は、入札日時に入札箱に投入してください。その際、封筒に入れ密封し、かつ、封書の表面に氏名（法人の場合はその名称または商号）および「ネットワーク不正通信対策業務」の入札書である旨を記入してください。（記入例を参照）

(2) 郵便による入札は不可とします。

(3) 入札参加者は、その提出した入札書の引換え、変更または取消しをすることはできません。

(4) 入札参加者が相連合し、または不穏な挙動をする等の場合で競争入札を公正に執行することができない状態にあると認めるときは、当該入札を延期し、またはこれを中止することができます。

(5) 入札執行回数は、2回を限度とします。

10. 入札書の作成方法等

(1) 入札書は<別紙様式2>によることとします。

(2) 入札書は日本語で記載し、金額については日本国通貨とします。

(3) 入札書の記載にあたっては、下記の点に注意してください。

ア. 件名は、「ネットワーク不正通信対策業務」とします。

イ. 年月日は入札書の提出日とします。

ウ. あて名は、公立大学法人奈良県立医科大学 理事長 細井 裕司 とします。

エ. 入札者氏名および押印は、法人にあつては法人の名称または商号および代表者の氏名とし、また印章にあつては奈良県（会計局総務課調達契約係）に届出済みのものとします。

オ. 代理人が入札する場合は、入札者の氏名および当該代理人の氏名を記載して押印しておくとともに、<別紙様式3>の委任状を提出してください。

カ. 入札書に記載する金額は、仕様書に明記する一切の諸経費を含んだ額を記入してください。

- (4) 入札参加者は、入札書の記載事項を訂正した場合は、当該訂正部分について入札書に押印したものと同一印を押印しておかなければなりません。ただし、入札書記載の価格を加除訂正することはできません。
- (5) 落札決定に当たっては、入札書に記載された金額に、当該金額の100分の8に相当する額を加算した額（当該金額に1円未満の端数があるときは、その端数を切り捨てた金額とする。）をもって落札価格としますので、競争入札に参加しようとする者は、消費税および地方消費税に係る課税業者であるか免税業者であるかを問わず、見積もった契約金額の108分の100に相当する金額を入札書に記載してください。
- (6) 記載した金額を提出前に変更するときは、新しい入札書を使用してください。

1 1. 入札保証金

業務実績が過去2年以内に2件以上ある場合は免除します。

ただし、落札者が落札後契約を締結しない場合は、公立大学法人奈良県立医科大学契約規程第17条第2項の規定に基づき、損害賠償を請求する場合があります。

1 2. 契約保証金

公立大学法人奈良県立医科大学契約規程の定めによります。

1 3. 開札

開札は、入札執行後直ちに入札に参加する者またはその代理人が必ず出席（1社1名）して行うものとします。この場合において、入札に参加する者またはその代理人が立ち会わないときは、入札執行事務に関係ない職員を立ち会わせてこれを行うこととします。

1 4. 入札の無効

次の各号のいずれかに該当する入札は、無効とします。

なお、無効の入札をした者については、再度の入札に加わることはできません。

- (1) 所定の入札条件に違反した入札
- (2) 入札書に記名押印を欠く入札
- (3) 入札書の重要な文字の誤脱等により必要な事項を確認できない入札
- (4) 入札書記載の価格を加除訂正した入札
- (5) 同一入札者がなした同一事項についての2以上の入札
- (6) 入札に際して公正な入札の執行を害する行為があったと認められる入札

1 5. 当該入札に関する事務を担当する部局の名称

〒634-8521 奈良県橿原市四条町840番地
公立大学法人奈良県立医科大学

法人企画部 総務課情報係 那須、熊谷

TEL : 0744-22-3051 (内線 : 2162)

FAX : 0744-29-8815

E-Mail : ictwork@naramed-u.ac.jp

16. 落札者の決定方法

- (1) 有効な入札書を提出した者であって、予定価格の制限の範囲内の最低価格をもって入札をした者を落札者とします。
- (2) 落札となるべき同価の入札をした者がいるときは、直ちに当該入札者にくじを引いていただき、落札者を決定するものとします。
- (3) 落札者となるべき者が、予定価格よりも異常に低い価格をもって入札したときは、当該入札者が参加の条件を満たし、かつ契約の条件を確実に履行できるかを照会するために、当該落札者の決定を保留する場合があります。
- (4) 再度の入札をしても、落札者がいないときまたは落札者が契約を締結しない場合は、随意契約に移行する場合があります。

17. 入札の中止等およびこれによる損害に関する事項

天災等やむを得ない理由により入札の執行を行うことができないときは、これを中止します。また、入札者の連合の疑い、不正不穏行動等をなすことにより入札を公正に執行できないと認められるときは、入札を取り消すことがあります。これらの場合における損害は入札者の負担とします。

18. 調達手続きの停止等

この調達に関する苦情申し立てに係る処理手続きにおいて、契約を停止しまたは解除する場合があります。

19. 契約書の作成

- (1) 契約書を2通作成し、各自1通を保有することとします。
- (2) 契約書の作成に要する費用は、落札者の負担とします。ただし、契約書用紙は交付します。

20. その他の事項

- (1) 落札決定後、契約締結までの間に、落札者が入札参加資格を失ったりまたは指名停止を受けたりした場合は契約を締結しません。
- (2) 入札に参加しようとする者は、関係法令を遵守し、信義誠実の原則を守り県民の信頼を失うことのないよう注意してください。
- (3) 落札者は落札決定後、契約締結までに落札額の内訳として本業務の初期費用、月額運用経費記載した内訳書（様式自由）を提出してください。

なお、本調達で構築したシステム一式は、次年度以降も継続して使用するものとします。ただし、予定している月額運用経費については、執行予定額(月額) 300,000円(消費税及び地方消費税を含む。)を上限とします。

<別紙様式1>

業務実績報告書

平成 年 月 日

公立大学法人奈良県立医科大学理事長 細井 裕司 殿

住所（所在地）
名称または商号
代表者名

印

項 目	内 容
1. 契約名称	
2. 契約年月日、契約期間	
3. 契約相手方	
4. 契約金額	
5. 業務内容	
1. 契約名称	
2. 契約年月日、契約期間	
3. 契約相手方	
4. 契約金額	
5. 業務内容	
1. 契約名称	
2. 契約年月日、契約期間	
3. 契約相手方	
4. 契約金額	
5. 業務内容	

※注意

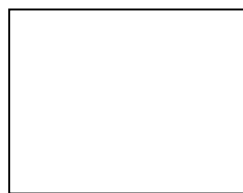
1. 国、地方公共団体または独立行政法人と、2件以上の業務実績を複数回記載して下さい。過去2年以内に2件以上の業務実績がある場合は、入札保証金を免除します。
2. 複数頁に分かれる場合は、ページ番号を記載して下さい。
3. 別業務の一環として実施した場合は、その旨が分かるように記載して下さい。

<別紙様式3>

委 任 状

私は、(受任者名) _____ を代理人と定め、
次の事項を委任します。

1. 入札物件名 ネットワーク不正通信対策業務
2. 作業場所 奈良県橿原市四条町840番地
 公立大学法人奈良県立医科大学



(受任者使用印)

上記の入札および見積もりに関する一切の権限を委任します。

平成 年 月 日

公立大学法人奈良県立医科大学
理事長 細井 裕司 殿

委任者 住所 (所在地)
 氏名 (名称または商号)

印

<別紙様式4>

入 札 辞 退 届

入札年月日 平成 年 月 日 ()

調達物件名 ネットワーク不正通信対策業務

下記の理由により入札を辞退します。

記

入札辞退理由

平成 年 月 日

公立大学法人奈良県立医科大学
理事長 細井 裕司 殿

住所 (所在地)
氏名 (名称または商号)

印

〈別紙様式5〉

ネットワーク不正通信対策業務に関する 質問票

事業者名:

電話番号:

担当者部署:

メールアドレス:

質問年月日: 平成 年 月 日

担当者役職:

担当者氏名:

	質問項目	質問の内容
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

※ 「質問項目」には、何のどの項目に関する質問か記載すること。

※ 「質問の内容」には、質問内容を簡潔に記載すること。

図1．入札書記載例

<別紙様式2>

入札書

												円
--	--	--	--	--	--	--	--	--	--	--	--	---

※消費税抜きの金額を記入

- ① 見積もった金額の108分の100に相当する金額(消費税および地方消費税抜きの金額)を記入してください。
- ② 予定数量に対する総額を記入してください。
- ③ 金額の前に¥マークを記入してください。

ただし、

1. 入札物件名 ネットワーク不正通信対策業務
2. 作業場所 奈良県橿原市四条町840番地
公立大学法人奈良県立医科大学

入札説明書および仕様書を承諾のうえ、上記のとおり入札します。

平成29年〇〇月〇〇日

← 入札書提出日の日付を記載してください。

公立大学法人奈良県立医科大学

理事長 細井 裕司 殿

県に登録している登録印を押印してください。

入札者 住所（所在地） △△市□□町1丁目10番地
氏名（名称または商号） 〇〇〇〇〇株式会社
代表取締役 大和 太郎 印
(代理人 鈴木 一郎 印)

↑ 代理人が入札する場合は、会社名・代表者名の下に代理人氏名を記入のうえ、受任者使用印を押印してください。

※ 入札に際しての所持品について

- ・委任状（代理人が入札に参加する場合）
- ・印鑑（代理人が入札に参加する場合、委任状に押印されたもの）
- ・入札書（2部）
- ・封筒、のり、赤色のペン等入札書の作成に必要なもの

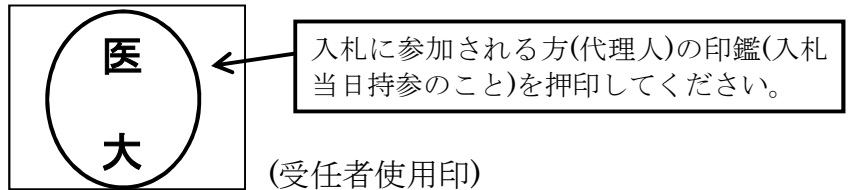
図 2. 委任状記載例

<別紙様式 3 >

委 任 状

私は、(受任者名) 医大 太郎 を代理人と定め、
次の事項を委任します。

1. 入札物件名 ネットワーク不正通信対策業務
2. 作業場所 奈良県橿原市四条町 8 4 0 番地
 公立大学法人奈良県立医科大学



上記の入札および見積もりに関する一切の権限を委任します。

平成 2 9 年 ○ ○ 月 ○ ○ 日

公立大学法人奈良県立医科大学
理事長 細井 裕司 殿

会社などの代表者印(県指名登録での使用印)を
押印してください。

委任者 住所(所在地) △△市□□町 1 丁目 1 0 番地
 氏名(名称または商号) ◎◎◎◎◎株式会社
 代表取締役 大和 太郎

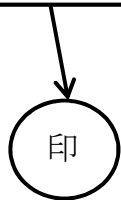
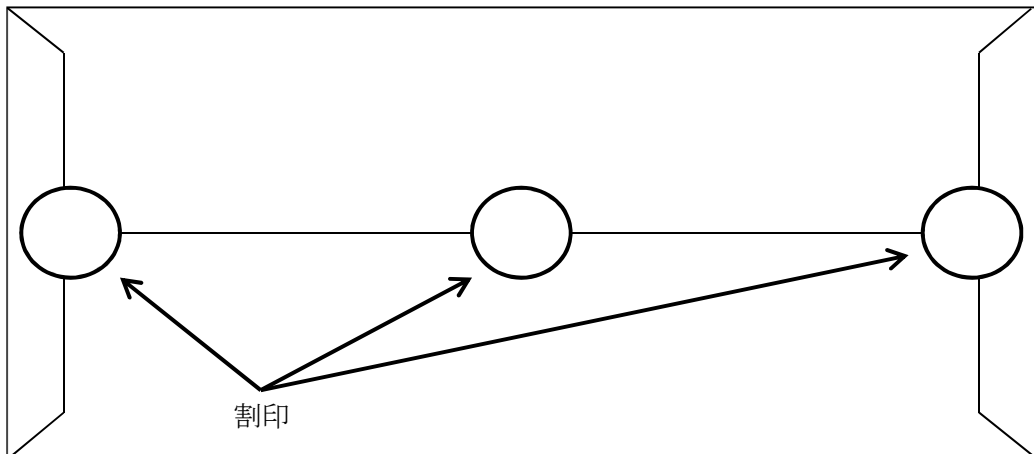


図3. 入札書に係る封書の記載例

封書表面

入札書在中		平成29年〇〇月〇〇日
公立大学法人奈良県立医科大学理事長 細井 裕司 様		
入札物件名	ネットワーク不正通信対策業務	
作業場所	奈良県橿原市四条町840番地 公立大学法人奈良県立医科大学	
入札者	住所(所在地)	△△市□□町1丁目10番地
	氏名(名称または商号)	◎◎◎◎◎株式会社
	代表取締役	大和 太郎

封書裏面



ネットワーク不正通信対策業務 仕様書

(主旨)

インターネットは、本学の教育、研究、診療等の業務に欠かせない。

しかし、近年インターネットを経由したサイバー攻撃が激化している。

特にメールやUSBメモリ等からのマルウェア感染などにより不正なプログラムが学内のパソコン等に感染すると、学内で保有している個人情報等が外部に流出する恐れがある。しかし、完全なセキュリティ対策は存在しないことから、多重的な対策により情報流出等の可能性を出来るだけ少なくすることが現在の対策と考えている。

現在、インターネットからの入り口対策としてはメールからのマルウェア感染やスパムメール対策を行っている。

今回のネットワークセキュリティ監視業務では主に出口対策として、内部から不正な通信が行われた場合や不審な挙動等を出来るだけ迅速に検出することを目的として導入するものである。これにより、本学においても異常時の速やかな対応を図ることとする。

(基本事項)

- ・業務の遂行にあたる管理体制を明確化すること。
- ・作業に当たって事故（情報セキュリティ事故を含む）が発生した場合、速やかに報告すること。また、本学の調査に協力する義務を負うこと。
- ・業務の遂行にあたり、稼働しているネットワークやシステムに影響を与えないこと。なお、業務の履行のため影響をあたえることが予想される場合は本学担当者と協議のうえ進めること。
- ・業務遂行にあたり必要な情報の本学からの提供については、本学担当者と協議すること。
- ・業務遂行にあたっては、本学の現状について本学担当者から詳細なヒアリングを実施し、その結果を構築に反映させること。
- ・本業務で得られたデータに個人情報や本学の機密情報が含まれている場合は、直ちに本学担当者に連絡しその対処についての指示に従うこと。

(法令等の遵守)

本業務に関する諸法令を遵守し、業務の円滑な進捗を図ると共に諸法令の適用運用は、請負業者の責任と費用負担において行わなければならない。

(SOCの体制)

ネットワーク監視部門であるSOC（Security Operation Center）については、本業務に係る次の事項を実施するための体制を構築すること。

○監視業務

- ・リアルタイム監視

攻撃者の特性、攻撃パターン、環境特性等を考慮し、SIEMによるインシデントのリアルタイム監視

- ・ 定点観測

正常状態把握、不審な兆候の検出等のため、時間軸や量的な観点を加味した統計的な手法による定点分析を行い、観測潜在的な脅威を可能な限り網羅する

- 調査・情報収集

脅威情報（攻撃者/組織、攻撃活動、攻撃手法）及び脆弱性情報（脆弱性、悪用可否、被害有無）、シグネチャ情報等について、研究者のブログやニュース、公式機関からの収集

- チューニング/分析手法開発

監視・調査/情報収集の結果を踏まえ、リアルタイム監視の拡充に向けた SIEM のチューニングや分析手法の開発の実施。

- リアルタイム監視の体制

リアルタイム監視については、24 時間体制で対応。
その他については、平日（9:00～17:00）で対応。

（業務内容）

- セキュリティ監視全般

- ・ ネットワークの出口（ファイアーウォール内で本学内からファイアーウォール向け）の不正通信を監視し、インシデント発生を迅速に検知するためのネットワーク監視が出来るネットワーク不正通信監視装置等を設置すること。なお、この仕様書で予定しているネットワーク不正通信監視装置のセキュリティ検知のための機能について、同等以上の機能を有している装置・ソフトウェア等の組み合わせで、ネットワーク不正通信監視装置と同等以上のセキュリティ検知が出来る場合はそれでも対応可とする。
- ・ 学内の設置しているハード、セキュリティ製品などに対して定期的に脆弱性診断を行うことが可能であること。重大なリスクとなりうるインシデントを SIEM 等の手法を用いて検知できること。

- ネットワーク不正通信監視装置

- ・ ネットワーク不正通信監視機器は、インシデントの分析を早期に行うために、次のような検知を可能とし、アラートを通知できること。
 - ユーザによる不正操作を可能とする不正なアプリケーションや攻撃者に狙われやすい脆弱なアプリケーションの使用の検知
 - 攻撃者が攻撃対象や攻撃手法を選定するために行うシステム構成や潜在する脆弱性を探索するようなツールの実行の検知
 - マルウェアを侵入させるような外部からの脆弱性をつく攻撃やエクスプロイトによる攻撃の検知
 - 特権昇格やアクセス権取得の内部探索を実施する RAT のインストールなど、攻撃が成功したことの検知
 - 外部への情報漏洩やシステム破壊など目的実行のためのマルウェアの内部拡散や C&C サーバとの外部通信の検知

- ・脆弱性診断を実施し、診断結果と攻撃イベントの相関分析により、対処済みの脆弱性をついた攻撃と未対処の脆弱性をついた攻撃を分類して、アラートを通知できること
- ・ネットワーク不正通信監視機器自体が VPN 機能を有し、学内ネットワーク外からリモートで監視ができること。
- ・検知イベントの緊急度判定を早期に行えるように、ネットワーク不正通信監視機器自体が相関分析ルールを有し、相関分析手法により攻撃種別および危険度の自動判別が可能であること。
- ・検知に問題がない程度の相関分析ルールがあること。
- ・最新の脅威へ迅速に対応するため、検知ルール及び相関分析ルールを自動でアップデートできること
- ・カスタムシグネチャを作成できること
- ・通信量の特性や通信状況の分析が可能であること
- ・IP レピュテーション情報に基づいた不正通信の検知ができること
- ・セキュリティ監視機器の物理仕様は次によること。
 - 19 インチラックに収容し高さを 2U 以内とすること。
 - 電源：100V で動作すること。
 - 室温：10℃～35℃の間で問題なく動作すること。
 - 湿度：10%～85%の間(ただし結露していない状態)で問題なく動作すること。

○インシデントの監視

契約期間内では、SOC において以下のインシデントの監視を行うこと。なお、契約終了後も継続的に不正通信の監視を行うため、本学と契約を締結し業務を継続出来ること。

- ・ネットワーク不正通信監視機器からの検知イベントのログ分析について、リアルタイム監視により 24 時間 365 日有人の侵入検知・分析・評価を行い、インシデント発生時には緊急度を判定して 2 時間以内を目標に対処案を提示すること
- ・ネットワーク不正通信監視機器による脅威検出だけでなく、単純には検出できない脅威の予見・兆候などを含め、以下に上げるような非定型の分析例による対策を講じること。
 - 不正アクセスが疑われる特定イベントに関する分析
 - 通信量の特定や通信状況の分析
 - 検知したアラートの影響度合の分析
 - 脆弱性やマルウェアの流行情報を元にした分析
 - セキュリティ関連ニュース、トピックを基にした分析
- ・対処が必要と判断したアラートだけを通知できること
- ・対処が必要と判断した不正通信に対して、本学内に設置しているアクセス制御装置（ファイアウォール）により不正通信の遮断措置を行うこと。ただし、遮断措置方法については本学担当者と事前に協議し決定しておくこと。
- ・定期的な監視結果を総括した月次報告書を提供できること
- ・アラート情報等に関する QA 対応を実施すること

- ・IPA、JPCERT/US-CERT、メーカー等からの脆弱性情報、脅威情報の定期的な情報提供を実施できること
- ・ネットワーク不正通信監視機器の稼働監視を行うこと。
- ・ネットワーク不正通信監視装置の稼働監視で異常を検知し故障と判断できる場合は、センドバックによる交換を行うこと。
- ・監視業務の詳細は、本学担当者と十分調整すること。

(構築)

- ・ネットワーク不正通信監視装置の設置については本学担当者と協議のうえ、設置計画書を提出すること。
- ・ネットワーク不正通信監視装置の設置については、本学担当者が立ち会いし実施すること。
- ・運用開始に当たってはネットワーク不正通信管理装置の操作等運用上の説明を書面で作成し、本学担当者に説明を行うこと。
- ・インシデントの監視のための体制を明確にし、体制関係（連絡体制、インシデント種別毎の対応等）の資料を提出すること。
- ・本学との協議の結果は書面にまとめて本学担当者の承認を得ること。
- ・運用開始は、平成 30 年 2 月 1 日とする。

(成果物)

○運用開始前

次の書類等を書面（1部）及びデータで提出すること。

原則として、データは、CD-ROM等に格納し、提出すること。

- ・インシデント監視体制資料
- ・ネットワーク不正通信監視装置取扱説明書
- ・ネットワーク不正通信監視装置仕様書
- ・本業務での各種設定資料
- ・ネットワーク不正監視運用マニュアル（本学担当者向け）

○運用開始後

- ・インシデント発生等本学担当者に連絡が必要な場合は速やかに電話・メール等で行い、その後、書面で報告を行うこと。
- ・重大なインシデント発生がない場合は、毎月 10 日までに前月の監視状況を書面で報告すること。
- ・本学担当者が今回の業務に係る事項に疑義が生じた場合は、問い合わせが出来る体制を構築すること。
- ・IPA、JPCERT/US-CERT、メーカー等からの脆弱性情報、脅威情報の定期的な情報提供を随時実施すること