別紙１

静岡県立病院機構ネットワーク挙動監視用
ソフトウェア導入運用管理委託入札仕様書

○目次

１．調達の概要

本仕様書は、静岡県立病院機構情報システム（以下、「情報システム」という。）用として使用しているネットワークの挙動を監視するためのソフトウェアもしくはサービス（以下「本システム」という。）の調達及び保守作業に関するものである。

２．対象ネットワークと設置場所

ネットワーク名	設置場所	監視対象 IP 数
事務系ネットワーク	こころの医療センター	8
電子カルテネットワーク	こころの医療センター	77
部門システムネットワーク	こころの医療センター	73
画像系ネットワーク１	こころの医療センター	42
画像系ネットワーク２	こころの医療センター	10
画像系ネットワーク３	こころの医療センター	3

※上記はいずれも異なる VLAN である。

※上記構成は Catalyst9500（L3SW 相当 2 台）と Catalyst9300（L2SW 相当 6 台）から構成されている。

※監視方法については特段の定めはない。

３．製品仕様

（1）本入札において提案するソフトウェア又はサービスは、ネットワークトラフィックの振る舞い検知および対応機能（NDR 機能等）として、以下の要件をすべて満たすこと。

（ア）AI・機械学習による未知の脅威検知

従来のシグネチャ（パターンマッチング）方式のみに依存せず、AI（人工知能）や機械学習を活用したトラフィックの振る舞い分析を行うこと。これにより、既知の脅威だけでなく、未知の脅威、ゼロデイ攻撃、内部端末の不審な挙動などを検知できること 。

（イ）トラフィック（内部通信）の可視化と監視

境界防御（南北トラフィック）をすり抜けた脅威を捉えるため、組織内部のネットワーク間の通信（東西トラフィック）を含めて監視し、通信状況を可視化できること。

（ウ）既存ネットワーク機器からのトラフィック収集

当機構が指定する既存のスイッチ機器（Catalyst 9500 等）のミラーポートから SFP+等を経由してパケットデータを取得、又はフローデータを受信し、適切に解析できるアーキテクチャであること 。

（エ）迅速なレスポンスおよび自動・手動での遮断連携機能

不正な動作や異常を検知した際、管理コンソールへの速やかなアラート通知を行うこと 。また、製品単体での通信遮断、または既存のネットワーク機器（スイッチやファイアウォール等）と連携し、不審な端末の通信を論理的に隔離・遮断できる機能を備えること 。

（2）必要となるライセンス数は「２．対象ネットワークと設置場所」を参考にすること。

（3）管理コンソールを提供すること。提供方法はオンプレミス、クラウドどちらでも可。

（4）万が一管理コンソールに長期間接続出来ない事象が発生しても、導入時の設定情報が維持できること。

（5）当機構のシステム更新に伴い、当該サーバの一時的な運用並行期間中に追加ライセンスを必要としないこと。並行期間は 3 ヶ月から 6 ヶ月で監視対象は３－（２）で示した数量の 2 倍

を想定すること。
（6）パケットキャプチャにより制御を行う場合、Catalyst9500 と接続想定である。SFP+のポートから導入予定機器との接続に必要な機器を備えること。
（7）監視機器を設置する場合、当機構の指定するラック（河村電器産業の SKD42-1220W）にマウントできること。
（8）不正な動作を検知した時に製品単体での遮断、または速やかに遮断が必要と思われるアラートを通知する機能を備えること。ここでいう不正な動作は既知の脅威だけでなく、ネットワークの挙動から未知の脅威と思われる振る舞いを含めること。

４．納入期限及び運用管理期間

（1）導入期限（初期設定を含む）
令和８年８月 31 日(導入支援期間は令和８年６月１日から令和８年８月 31 日を想定する)

（2）運用管理期間
令和８年９月１日～令和 13 年８月 31 日

５．導入支援

（1）システムが正常に動作するよう設定を行うこと。導入においては運用中の機器類が再起動しないよう調整すること。ネットワーク通信の制御は当機構にて行うが、その他の作業については導入費用に全て含むこと。

（2）導入作業にあたっては必要に応じて打ち合わせを行い、当機構職員との円滑な協力体制を実現すること。打ち合わせの方法は WEB、対面どちらでも構わない。

（3）過去の事例を踏まえ推奨設定等がある場合は、滞りなく提案すること。

（4）管理コンソールがクラウドの場合、当機構から接続先へのネットワーク設定は機構職員が行うので、設定内容等を速やかに開示し必要に応じて支援を行うこと。

（5）導入時にシステム操作説明を行うこと。(最大 10 名程度)

６．保守要件

（1）導入に必要となった機器類については平日９時～17 時の受付窓口を有すること。
（2）機器類の保守はオンサイト保守とし、４営業時間以内に初動対応を行うこと。
（3）運用期間中の QA 対応について、簡易な問い合わせに対応できる連絡窓口を提示すること。
（4）契約書に付随する様式４号を毎月提出すること。障害があった場合は、指定した様式とともに障害報告書を添付すること。様式は問わない。

７．検査及び引き渡し

（1）検査及び引き渡しについては契約書の第 13 条のとおりとする。

（2）納品物として以下のもの電子媒体として納入すること。

・設定シート

・操作マニュアル

・保守連絡先

８．その他

（1）調達製品の稼動・保守については、落札者が最終責任を負うこととする。

（２）本仕様書に疑義がある場合は、本機構に質問し、その指示を受けること。なお、契約後の本仕様書の解釈は本機構によるものとする。

（３）本仕様書に対する質問は、入札説明書によるものとする。

（４）費用の請求については導入費用（設定費等）と管理費用（ライセンス料、利用料等）を明確にし、入札説明書４－（５）に記載している事項を熟読すること。