UTM 設置・保守及び SOC 業務仕様書

１　業務基本要件

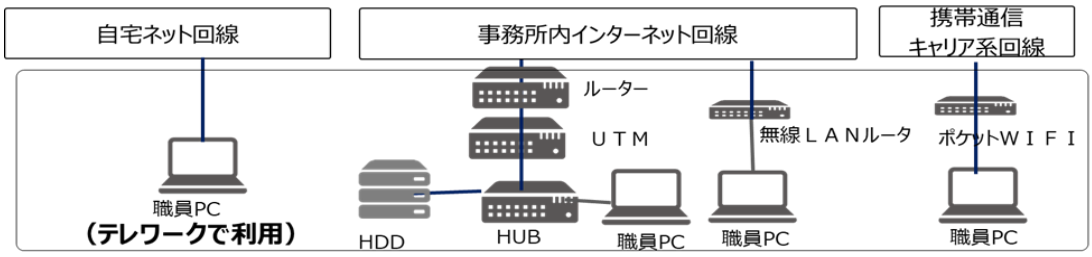
受注者は、組織委員会が LAN や WIFI 利用時のセキュリティ対策として導入する UTM（Unified Threat Management）機器の納入、初期設定、保守対応をおこなうこと。あわせて、設置した UTM が取得したログを SOC（Security Operation Center）にて収集・分析し、重要度の高いインシデントがあれば、メール等で組織委員会に通知すること。

受注者は契約締結後から 11 月 8 日までに機器の納入、初期設定を完了し、11 月 9 日から保守業務及び SOC 業務を開始すること。

２　UTM 設置・保守業務

(1) UTM の設置場所

組織委員会が運用する LAN 内（下図参照）



(2) UTM の台数

1 台

(3) 監視対象とする端末台数　同時接続目安 130 台前後

監視対象となる端末の OS：Windows10

(4) UTM の機能

ア　アンチウイルス機能

通信パケットをファイルに復元して検知可能（プロキシベース検査方式）であること。その他、ヒューリスティック検出エンジン等の機能を有し、亜種・新種のウイルス検知が可能であること。

イ　ＷＥＢフィルタリング機能

(ｱ) カテゴリごとにＷＥＢ閲覧制限が可能であること。

（カテゴリ例）違法性・犯罪性の高いサイト、ＷＥＢチャットサイト等

(ｲ) カテゴリごとの URL データベースは常時自動更新されること。

(ｳ) インターネット掲示板への書き込み禁止機能が利用可能であること。

ウ　アンチスパム機能

(ｱ) 以下プロトコルに対応していること。

○SMTP：POP3 IMAP　○SMTPS：POP3S IMAPS

(ｲ) 迷惑メールはメール設定（送信元 IP アドレス、ヘッダ情報等）により迷惑メ

ールフォルダへの自動振り分けが可能であること。

エ　アプリケーション制御

(ｱ)マルウェアに感染した端末（Botnet）に対してインターネット外部から攻撃指示や情報盗取をする目的で設置されたサーバ（C&C サーバ等）との危険な通信を制御することが可能であること。

(ｲ)ファイル共有ソフト・アプリケーションへの接続を制御することが可能であること。

オ　IPS（不正侵入検知・防御）機能

攻撃を検知した場合、送信元 IP などの条件を基にして当該トラフィックを遮断可能であること。

カ　アンチボットネット機能

C&C サーバの IP アドレスをブラックリスト登録する等により不正通信をブロックすることが可能であること。

キ　SSL-VPN 機能

クライアントソフトをインストールした職員 PC（P1 に記載した LAN 図参照）については、LAN 接続外（例:テレワーク環境や WIFI 接続時）であっても、SSL-VPN 機能を用いた安全なリモート接続が可能であること。

(5) ログの保管

組織委員会が通信ログを任意に照会・抽出できるように、クラウドストレージにログ保管できる仕組みを構築すること。クラウドストレージの容量については 8TB 以上とすること。

(6) UTM の保守

ア　24 時間 365 日体制でリモートにより稼働監視することが可能であること。

イ　障害発生時には電話にてサポートおよびオンサイト対応可能であること。

ウ　リモートによりファイアウオール設定変更等の支援が可能であること。

エ　機器にバグやセキュリティホールが生じた場合は、リモートにより必要に応じてファームウエアのバージョンアップをすること。

3　SOC について

(1) SOC 運営は JNSA（特定非営利活動法人　日本ネットワークセキュリティ協会）の会員企業により実施することとし、ログ分析等に専門性を有する職員が複数体制で業務をおこなう SOC 拠点を国内に設置・運用し、業務対応は日本語で実施すること。

(2) 24 時間 365 日体制で、本業務にて設置した UTM からログを収集・分析し、重要度の高いインシデントがあれば、メール等で発注者に通知すること。

(3) (2)に記載のインシデントに係る通知については以下項目を含むこと。

ア　検知内容

(ｱ)対象期間

(ｲ)対処状況（例：検知、駆除済）

(ｳ)送信元 IP アドレス、送信先 IP アドレス

(ｴ)マルウェア名称、アプリケーション名称等の対処に必要な情報

イ　対処手順

通知したインシデントに係る対処方法（例：IP アドレスから端末を特定し、ネットワークから切り離す。ウイルスソフトを利用してフルスキャンを推奨する　等）を示すこと。

また組織委員会から対処手順について問い合わせがあった場合は電話、メール等で回答をおこなうこと。

※SOC 監視用固定 IP アドレスは発注者にて手配する。