仕　様　書

1. 件 名 マルウェア対策ソフトウェアライセンスの利用契約

2. 数 量　1 式

3. 目 的

QSTnet における端末向けコンピュータマルウェア対策として、ユーザ端末に ISMAP 登録がある不正プログラム対策ソフトウェアを導入することで、振る舞い検知の導入による脅威の可視化を実現する。

4. 使用期間　令和 8 年 10 月 1 日～令和 9 年 9 月 30 日
（納入期限は使用期間前日の令和 8 年 9 月 30 日までとする）

5. 納入場所
国立研究開発法人量子科学技術研究開発機構　本部
〒263-8555 千葉県千葉市稲毛区穴川 4-9-1

6. 仕様・性能
(1) 構成及び規格
別紙の通り。
(2) ソフトウェア仕様
a) クライアントのオペレーティングシステムは Windows11,Windows Education ,Windows Workstation,Windows Server,macOS, Linux に対応していること。
b) スケジューリングによるローカルハードディスク内のマルウェア検索が可能なこと。
c) マルウェア検査用のプログラムをメモリ内に常駐することができ、実行されたプログラム及びオープンされたデータファイルのリアルタイム検査が可能なこと。
d) 発見したマルウェアに対して、「マルウェアの削除」及び「マルウェアの駆除」の処理が可能なこと。
e) クラウド上の管理サーバでの集中管理に対応していること。
f) 攻撃を検知した場合には、原因、不正振舞の分析、感染した端末の特定、影響範囲を把握できること。
g) 検知した結果に対する評価及び対応、復旧を実施すること。

h）インシデント関連に対し、アラートが出力された際、端末を自動的にネットワークから隔離することができること。
i）隔離された端末の脅威分析などを完了し、問題が解消した後、元の通信状態に戻すことができること。
j）検出した脅威をリモートで除去するための機能を有すること。
k）管理可能なセキュリティ対策製品のログ収集を行うことができ、複数条件によるログの検索、集計、レポート機能を有すること。また、CSV 形式で出力可能であること。
l）収集したログファイルを元に、マルウェア及び脅威の詳細情報（オブジェクト情報、マルウェアが生成したプロセス情報、マルウェアの通信先情報など）などのトラッキングに関することを可視化する機能を有すること。
m）攻撃の一環として、マルウェアによりファイルが生成された場合を踏まえ、ファイルの操作履歴を取得し、検索を可能とすること。
n）利用されたマルウェアに関する情報の可視化が可能であること。（感染経路、配布範囲、実行の有無等）
o）内部から外部への不正発信に関する情報の可視化が可能であること。（発信の有無、宛先等）
p）マルウェア感染状況や脅威情報等をマッピング表示又はダッシュボードに表示し、マルウェア拡大範囲の特定機能を有すること。
q）マルウェアに感染した経緯を確認可能とし、ドリルダウン等によるプロセス特定等の分析機能を有すること。
r）指定した条件(例:ファイル名、ドメイン、IP アドレスなど)で EDR ログの検索を行うことで、管理しているエージェントの中から条件に関連した影響端末を特定できること。
s）標的型攻撃の進行状況(攻撃段階)と影響を受けた端末が管理コンソールで確認できること。
t）クラウド上に構築された管理サーバの利用ライセンスが含まれており、マルウェア対策ソフトが導入された端末に対して、以下の管理が可能なこと。
・パターンファイル及び検索エンジンのアップデート状況の確認
・マルウェア検知状況の確認
・各種パラメータの変更
u)過検知によるファイル駆除が認められた場合、駆除されたファイルを駆除時点に復元する機能を持つこと（Windows、Windows Server、Linux)。
v)管理画面の問い合わせ専用ポータルから問い合わせを起票、もしくはチャットや電話での問い合わせが可能なこと。
w)ISMAP に登録のある製品であること。

7. 検 査

当機構職員が、所定の要件を満たしていることを確認したことをもって検査合格とする。

8. その他

(1) 受注者は、量研の情報セキュリティポリシーを遵守すること。

(2) 受注者は、本件で取得した当機構の情報を、当機構の許可なしに本件の目的以外に利用してはならない。本件の終了後においても同様とする。

(3) 受注者は、本件で取得した当機構の情報を、当機構の許可なしに第三者に開示してはならない。本件の終了後においても同様とする。

(4) 本件の履行に当たり、受注者は従業員又はその他の者によって、当機構が意図しない変更が加えられることのない管理体制を整えること。

(5) 本件の履行に当たり、情報セキュリティ確保の観点で、受注者の資本関係・役員等の情報、本件の実施場所、業務を行う担当者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報を求める場合がある。受注者は、これらの要求に応じること。

(6) 本件に係る情報漏えいなどの情報セキュリティインシデントが発生した際には、速やかに当機構担当者に連絡し、その指示の元で被害拡大防止・原因調査などを行うこと。

(7) 受注者は、当機構から本件で求められる情報セキュリティ対策の履行状況を当機構からの求めに応じて確認・報告を行うこと。またその履行が不十分である旨の指摘を受けた場合、速やかに改善すること。

(8) 受注者は、機器、コンピュータプログラム、データ及び文書等について、当機構の許可無く当機構外部に持ち出してはならない。

(9) 受注者は、本件の終了時に、本件で取得した情報を削除または返却すること。また、取得した情報が不要となった場合も同様とする。

(10) 本件で作成された著作物（マニュアル、コンピュータプログラム等）の所有権は、当機構に帰属するものとする。

(11) 本件の履行に当たり、その業務の一部を再委託するときは、軽微なものを除き、あらかじめ再委託の相手側の住所、氏名、再委託を行う業務範囲、再委託の必要性及び金額等について記載した書面を当機構に提出し、承諾を得ること。その際受注者は、再委託した業務に伴う当該相手方の行為について、当機構に対しすべての責任を負うこと。

(12) 本件を実施するために必要な当機構の情報は、本件の契約後、当機構が定めた方法により開示する。

(13) 仕様書上疑義が生じた場合は、当機構担当者と協議の上決定するものとする。

（要 求 者）
部課名： 情報基盤管理部 IT 運用・学術情報課
氏　名： 小畑　欣也