平成 27 年 5 月 27 日

平成 27 年度「高度サイバー攻撃への対応のためのログ分析ツールの開発」に関する入札のご案内

一般社団法人 JPCERT コーディネーションセンター
(入札管理責任者　総務部長　村上憲二)

次のとおり一般競争入札に付します。

1. 入札に付する事項

(1) 名　　称：高度サイバー攻撃への対応のためのログ分析ツールの開発
(2) 内　容　等：別紙 1 のとおり(高度サイバー攻撃への対応のためのログ分析ツールの開発概要)
(3) 履行期限　：別紙 1 のとおり(高度サイバー攻撃への対応のためのログ分析ツールの開発概要)
(4) 入札方法等：
本件は、JPCERT コーディネーションセンター（以下「当センター」という。）が経済産業省より委託されている平成 27 年度サイバーセキュリティ経済基盤構築事業（サイバー攻撃等国際連携対応調整事業）で実施されるプロジェクトの一つとして実施し、総合評価落札方式で行う。
したがって、入札の際には提案書を提出し、技術審査を受けなければならない。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 8 パーセントに相当する額を加算した金額（当該金額に 1 円未満の端数が生じたときは、その端数金額を切捨てるものとする。）をもって落札価格とするので、入札者は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にかかわらず、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すること。

2. 入札要件

(1) 予算決算及び会計令（以下「予決令」という。）第 70 条の規定に該当しない者であること。ただし、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、参加することを認める。
(2) 予決令第 71 条の規定に該当しない者であること。
(3) 経済産業省から補助金交付等停止措置又は指名停止措置が講じられている者ではないこと。
(4) 経営の状況、信用度が極度に悪化していないと認められる者であり、適正な契約の履行が確保される者であること。

3. 入札者の義務

この一般競争に参加を希望する者は、当センターが配布する仕様書に基づいて提案書を作成し、これを入札書に添付して入札書の受領期限内に提出しなければならない。また、落札者の決定日前日までの間

において当センターから当該書類に関して説明を求められた場合は、これに応じなければならない。
なお、採用し得ると判断した提案書を添付した入札書のみを落札決定の対象とする。

4. 契約事項を示す場所等

(1)入札説明会の日時及び場所

日時：平成 27 年 6 月 4 日（木） 13 時 00 分～14 時 00 分(1 時間程度を予定)

場所：〒101-0054 東京都千代田区神田錦町 3-17 廣瀬ビル 11 階

一般社団法人 JPCERT コーディネーションセンター

TEL ：03-3518-4600

FAX ：03-3518-4602

※説明会参加希望者は 6 月 2 日 17 時までに ww-info@jpcert.or.jp に必要事項 (法人名、部署名、参加者氏名、連絡先) を記載のうえ、メールにて参加希望の事前申し込みをすること

(2) 入札書・提案書の受領期限及び受領場所

期限：平成 27 年 6 月 16 日（火）17 時 00 分（必着）

場所：「4.契約事項を示す場所等」(1)に同じ

方法：持参、郵便(簡易書留による)

(3) 落札者の決定日

平成 27 年 6 月 22 日（月）

(4) 入札結果の通知

入札結果は、落札者を含め入札者全員に対して、落札者の決定日にメールその他の手段により通知するものとし、当センターの Web サイトにて公表する。

5. その他

(1) 入札保証金及び契約保証金

全額免除

(2) 入札書の変更及び取消し

入札者は、提出した入札書等の変更及び取消しをすることができない。

(3) 入札の無効

本公告の 2.入札要件に示す入札参加資格のない者による入札及び各項に定めた諸条件について、その条件に違反した場合は入札を無効とする。

(4) 契約書の作成

落札者が当センターと契約を締結する際には、契約書の作成を必要とする。

(5) 落札者の決定方法

予決令第 79 条の規定を参考に作成された予定価格の制限の範囲内で、入札管理責任者が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、入札管理責任者が定める総合評価の方法をもって落札者を定めるものとする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の範囲内の価格をもって入

札をした他の者のうち、評価の最も高い者を落札者とすることがある。

6. 問合せ先(メールでの問い合わせを原則とする)

(1) 入札説明書等に関する問い合わせ

一般社団法人 JPCERT コーディネーションセンター
早期警戒グループ　藤本（ふじもと）/ 満永（みつなが）
E-mail ：ww-info@jpcert.or.jp

(2) 入札行為に関する問い合わせ先

一般社団法人 JPCERT コーディネーションセンター
総務部　経理担当　加門（かもん）
E-mail ：soumu@jpcert.or.jp

※緊急を要する場合に限り、電話による問合せ可
9:00～18：00（12:00～13:00 は除く）月～金曜日（祝・休日を除く）

別紙 1

「高度サイバー攻撃への対応のためのログ分析ツールの開発概要」

1. 件名

平成27年度 高度サイバー攻撃への対応のためのログ分析ツールの開発（統合ログ分析ツール）

2. 目的

本件調達においては、「特定組織に対して明確な攻撃意図を持ち、国家や企業等の情報窃取やシステム破壊を行う巧妙で執拗な計画された攻撃」を「高度サイバー攻撃」という。

近年、高度サイバー攻撃による被害が国内企業において継続的に発生している。高度サイバー攻撃では、入念な攻撃計画が立てられていることが多く、侵入自体を防ぐことは難しい。しかし、侵入を早期に発見することで、攻撃者の横断的移動を防ぎ、被害を最小化することが可能となる場合がある。加えて、攻撃者の痕跡を確認することで、攻撃の状況を把握し、必要な対策を立てることが可能となる。侵入検知や、攻撃の痕跡を確認する上で非常に重要となるのが、様々なログに対する相関的かつ総合的な分析である。JPCERTコーディネーションセンター(以下「JPCERT/CC」という。)では、高度サイバー攻撃の対応支援において、各種ログに対して相関的な分析を行い、影響範囲の洗い出しを実施しているが、膨大なログから必要な情報を抽出し、分析を行うには、専門知識と多くの工数が必要となる。そこで、高度サイバー攻撃の対応支援に即したログ分析ツールの開発を行うことで、ログ分析を迅速かつ正確に行い、対応支援のスピード、正確性を向上させ、対象組織における被害拡大抑止を図る。併せて、JPCERT/CCのログ分析対応者の工数削減に資することを目的とする。

また、本ツールで、サイバー攻撃の対応で活用できる標準仕様 STIX(Structured Threat Information eXpression)形式の入出力を可能とすることで、他システム、他組織との情報の共有性を高める。

3. 事業の内容及び実施方法

以下に関し、JPCERT/CCと協議しつつ、実施する。

(1) 各種ログを分析用に変換するためのCLI形式のアプリケーション（以下「ログ変換ツール」という。）の開発

フォーマットが異なる各種ログから必要なデータを抽出し、csv等の統一フォーマットに変換できること。ログ取得元機器にて取得したログを入力とし、正規表現等を利用して変換を行い、後述する統合ログ分析ツールへの入力データを出力すること。

分析で利用するログは、以下とする。

- プロキシサーバのログ
- Active Directoryのログ（Domain Controllerのイベントログ）
- ファイヤウォールのログ
- ファイルサーバのログ
- その他、JPCERT/CCとの間で協議の上、決定したログ

(2) ログを分析するためのWebアプリケーション（以下「統合ログ分析ツール」という。）の開発

ログ変換ツールで変換済みのデータを入力とし、各種ログの分析結果、相関を可視化できるアプリケーションを開発すること。また、STIX形式の入出力機能を実装すること。ツールの要件は以下のとおり。

- 各種ログの検索結果や分析結果を、表などの可読性が高い形式で表示できること。
- ログの相関分析結果を、表などの可読性が高い形式で表示できること。
- ログを様々な条件で横断検索し、検索結果を表などの可読性が高い形式で表示できること。
- ログの相関分析結果をSTIX形式で出力できること。
- STIX形式の入力データを解析した結果を、表などの可読性が高い形式で表示できること。

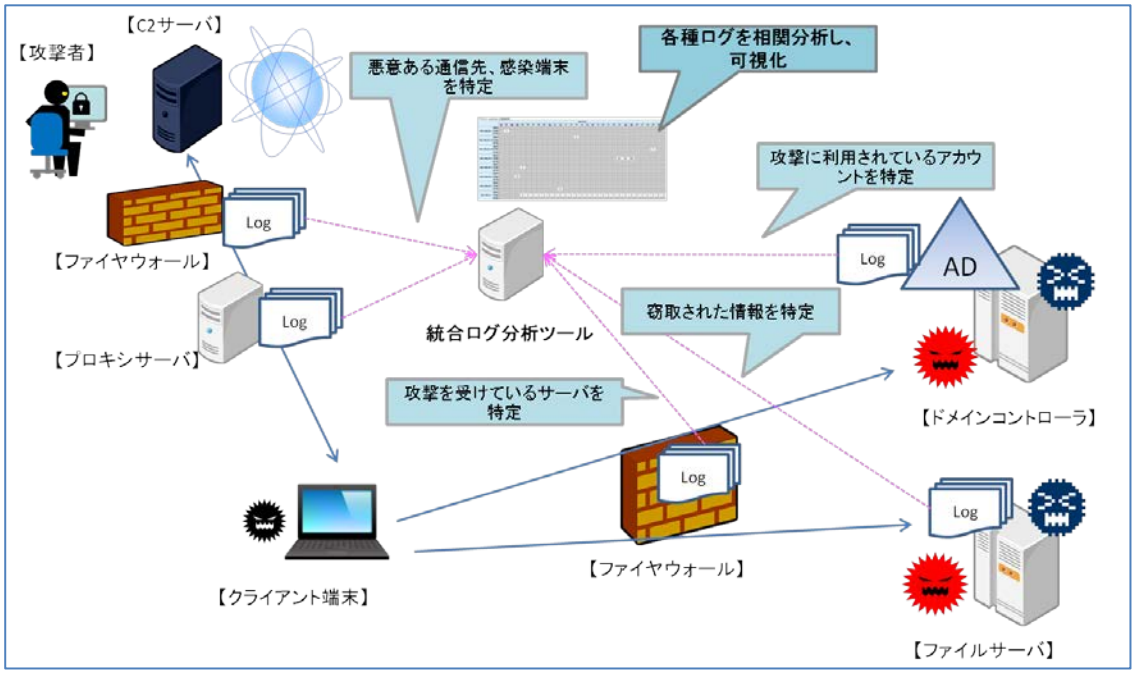
(3) アプリケーションが動作するシステムのVMイメージ作成

VMWare Esxiで動作する(1)、(2)を評価済みのイメージファイルを提出すること。

(4) アプリケーションに関わる脆弱性対応

受託事業者は、以下を実施すること。

- 請負期間中、アプリケーションの開発に利用するOSSの脆弱性情報を確認すること。影響度の高い脆弱性が公開された場合は、JPCERT/CCと協議した上で、必要に応じてアップデートを行うこと。



[図 1. 統合ログ分析ツール実現予想図]

4. 入札要件
   - 高度サイバー攻撃 に対して対応支援業務を行った経験を有すること。
   - プロキシサーバ、Active Directory、ファイヤウォール等の各種ログを分析した実績を有すること。
   - Active Directory環境におけるセキュリティを考慮した構築および開発（仮想システム環境を含む）実績を有すること。
   - STIX(Structured Threat Information eXpression)およびAPIに精通していること。

5. 履行期限

   平成28年3月18日（金）までに納品し、検収を受けること。

6. 成果物

   以下の完成図書と、以下全ての電子データを納品すること。
   - ツールの仕様書、ソースコード及び実行形式のファイル
   - ツールの開発、ビルドに使用した開発ツールのプロジェクトファイル
   - VMWare社Esxiで動作する形式のイメージファイル
   - 事業報告書（プロジェクト計画、打ち合わせ議事録、テスト結果など）

7. 納入場所

   一般社団法人 JPCERT コーディネーションセンター

別紙2

JPCERTコーディネーションセンターにおける入札は当該箇所に付き以下の予算決算及び会計令（国による歳入徴収、支出、支出負担行為、契約等について規定したもの）を準用して行うこととする。

予算決算及び会計令（抜粋）

（昭和２２年４月３０日勅令第１６５号）

（一般競争に参加させることができない者）

第７０条　契約担当官等は、売買、貸借、請負その他の契約につき会計法第２９条の３第１項の競争（以下「一般競争」という。）に付するときは、特別の理由がある場合を除くほか、当該契約を締結する能力を有しない者及び破産者で復権を得ない者を参加させることができない。

（一般競争に参加させないことができる者）

第７１条　契約担当官等は、次の各号の一に該当すると認められる者を、その事実があった後二年間一般競争に参加させないことができる。これを代理人、
支配人その他の使用人として使用する者についても、また同様とする。

一　契約の履行に当たり故意に工事若しくは製造を粗雑にし、又は物件の
品質若しくは数量に関して不正の行為をした者

二　公正な競争の執行を妨げた者又は公正な価格を害し若しくは不正の利益を得るために連合した者

三　落札者が契約を結ぶこと又は契約者が契約を履行することを妨げた者

四　監督又は検査の実施に当たり職員の職務の執行を妨げた者

五　正当な理由がなくて契約を履行しなかつた者

六　前各号の一に該当する事実があつた後二年を経過しない者を、契約の履行に当たり、代理人、支配人その他の使用人として使用した者

２　契約担当官等は、前項の規定に該当する者を入札代理人として使用する者を一般競争に参加させないことができる