JPCERT CC®

平成 29 年 8 月 17 日

平成 29 年度 「Sysmonログの簡易分析Webアプリケーションシステムの開発業務」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：平成 29 年度「Sysmon ログの簡易分析 Web アプリケーションシステム」開発業務

(2) 内　容　等：別紙 1 のとおり(平成 29 年度「Sysmon ログの簡易分析 Web アプリケーションシステム」開発業務仕様書)

(3) 履 行 期 限：別紙 1 のとおり(平成 29 年度「Sysmon ログの簡易分析 Web アプリケーションシステム」開発業務仕様書)

(4) 入札方法等：

本件は、JPCERT コーディネーションセンターが経済産業省より委託されている平成 29 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。

(5) 入札説明会に参加し、入札説明書の交付を受けた者であること。

3. 入札者の義務

この一般競争に参加を希望する者は、JPCERT コーディネーションセンターが配布する仕様書に基づいて提案書を作成し、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 JPCERT コーディネーション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者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 29 年 9 月 4 日（月） 16 時 00 分～17 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 8 月 31 日 17 時までに aa-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) 提案書の受領期限及び受領場所

期限：平成 29 年 9 月 19 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) 入札者決定の通知日

平成 29 年 9 月 20 日（水）

(4) 入札日

日時：平成 29 年 9 月 22 日（金）16 時 00 分～ （落札者が決定するまで）

場所：「4.契約事項を示す場所等」(1)に同じ

持参：入札書

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 JPCERT コーディネーション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 条の規定に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
分析センター　朝長（ともなが）/ 竹田（たけだ）
E-mail ：**aa-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　小島（こじま）
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）

JPCERT CC®

別紙 1

Sysmonログの簡易分析Webアプリケーションシステムの開発業務（仕様書）

1. 件名

平成29年度　Sysmonログの簡易分析Webアプリケーションシステムの開発業務

2. 目的

近年のサイバー攻撃では、マルウエアに感染した端末起点として、他の端末への感染拡大や、内部サーバーへの侵入など、ネットワーク内に侵害が拡大する事例が増加している。侵害を受けた端末の調査には、影響・被害範囲などの特定のため、フォレンジック調査が行われる。しかし、フォレンジック調査には多くの時間が必要なため、調査対象が多岐にわたる場合、網羅的に調査を行うのは困難である。

一方で、端末内で動作したアプリケーションや通信などの詳細なログを日頃から取得しておくことで、インシデント調査が必要な場合にフォレンジック調査を行わずにログの調査だけで被害状況を把握する調査方法も存在する。このような用途に使用できるツールとしてマイクロソフト社からSysmon というツールが無償公開されている。Sysmon は、端末上で動作したアプリケーションの情報やレジストリエントリの作成、通信など Windows OS の様々な動作をイベントログに記録するツールである。

このSysmonのログを調査する最も一般的な方法は、イベントログをテキストなどの形式に変換し、検索などを行う方法である。しかし、このような方法では多数の端末を同時に調査することは困難である。

そこで本事業では、Sysmon のログを一元管理し、ログ分析を迅速かつ正確に行うことのできる簡易分析システムを開発し、インシデント調査のスピード、正確性を向上させ、工数を削減することを目的とする。

3. 事業の内容及び実施方法

以下に関し、JPCERT コーディネーションセンターと協議しつつ、実施する。

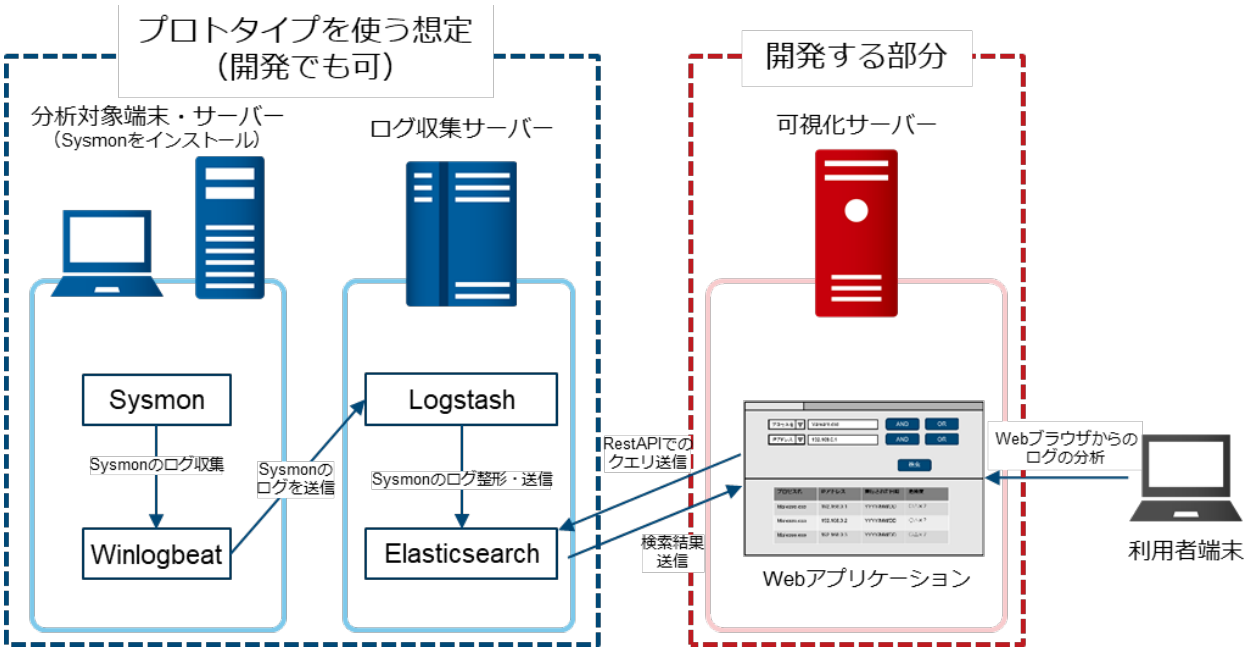
(1) Sysmon のログを収集、保存、分析するためのシステム構築

Sysmon をインストールした端末からログを収集し、データベース等に格納する仕組みを構築すること。後述する Web アプリケーションから当該データへアクセスできること。

なお、本システムのプロトタイプは作成済みであり、基本的にプロトタイプでの構築を推奨するが、後述する Web アプリケーションの開発にあたり、実装が困難である等の問題が発生した場合、独自開発を行うことも可能である。

図 1 はプロトタイプのイメージである。端末の Sysmon のログを収集するツールとして、Winlogbeat を使用する。収集されたログを保存する基盤として、ログ収集ツールである Logstash

と検索エンジンツールである Elasticsearch を使用する。



[図 1　Sysmon ログの簡易分析 Web アプリケーションシステム]

(2) ログを分析するための Web アプリケーションの開発

以下の機能を有する Web アプリケーションを開発すること。

1. データベースなどに格納されているログを入力として、以下の項目について分析結果を可視化する機能
   - プロセス情報
     - プロセスの親子関係
     - 各プロセスに関連する動作（レジストリエントリの操作、ファイル作成、通信など）
   - 通信情報
     - 端末間通信
     - 端末から外部への通信

2. データベースなどに格納されているログを STIX(Structured Threat Information eXpression)、IoC(Indicator of Compromise) 形式での検知ルールにより検索する機能

3. 2. 検索機能を使用した定期的なログの監視機能

(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。

4. 入札要件
   - システム構築、Webアプリケーション開発を行った経験を有すること。

5. 履行期間
   平成30年3月16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、以下すべての電子データを納品すること。
   - システム構築手順書
   - Webアプリケーション仕様書およびソースコード
   - 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

JPCERT CC®

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った者

六　前各号の一に該当する事実があっ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