

平成 27 年度「マルウェア分析手法および分析環境に関する調査研究」  
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：マルウェア分析手法および分析環境に関する調査研究
- (2) 内 容 等：別紙 1 のとおり(マルウェア分析手法および分析環境に関する調査研究事業内容)
- (3) 履 行 期 限：別紙 1 のとおり(マルウェア分析手法および分析環境に関する調査研究事業内容)
- (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 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。
- (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、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 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 8 月 21 日（金） 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 20 日 17 時までに [aa-info@jpcert.or.jp](mailto: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 27 年 9 月 4 日（金） 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 27 年 9 月 11 日（金）

##### (4) 入札日

日時：平成 27 年 9 月 14 日（月） 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

#### 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

予令第 79 条の規定に参考で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る著しく不相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) / 椎木 (しいぎ)

E-mail : [aa-info@jpcert.or.jp](mailto: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 経理担当 加門 (かもん)

E-mail : [soumu@jpcert.or.jp](mailto: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)

## マルウェア分析手法および分析環境に関する調査研究概要

## 1. 件名

平成27年度 マルウェア分析手法および分析環境に関する調査研究

## 2. 目的

今日のサイバー攻撃に対応していくためには、攻撃で使用されるマルウェアの分析が必須であり、その手法は攻撃手法や環境の変化に応じて、随時更新していくとともに、分析手法や分析環境の高度化をすすめる必要がある。

マルウェアを詳細に分析するためには、マルウェアを分析環境上で動作させる動的分析手法や、マルウェア内のコードを読み解く静的分析を行う必要があるが、時間がかかるという問題がある。それに対して、マルウェアのハッシュ値や内部に含まれる文字列など、簡易に取得可能な情報から分析を行う表層分析は、動的分析や静的分析に比べて時間がかからないというメリットがある。

しかし、表層分析では、詳細な分析結果を得ることは難しいのが現状である。

日々、大量に発生するマルウェアすべてに動的分析や静的分析を実施することは難しいため、表層分析を高度化し、より多くの分析結果を得られるようにすることが求められている。

また、ユーザの利用する環境が、従来主流であった環境(Windows 7)から、より新しい環境(Windows 8.1, Windows 10)へ移行しつつある今、マルウェアも新しい環境で動作できるよう変化していくことが予想される。

新しい環境に対応したマルウェアに対抗するためには、新しい環境における、マルウェアの動作に関わる技術情報を理解すると共に、新しい環境へ適合した分析環境を構築する必要がある。

本調査研究では、上記の課題を解決することで、マルウェアの分析手法を高度化すること、または環境の変化に伴う技術情報を整理し分析環境を高度化することで、今後も増加・高度化すると考えられるサイバー攻撃に対抗するための、マルウェア分析体制強化を目指すことを目的とする。

## 3. 事業の内容及び実施方法

以下3つの事業内容からいずれかを選択し、JPCERTコーディネーションセンター（以下、「JPCERT/CC」という。）と協議しつつ、実施する。

## (1) 表層分析の高度化に関する調査研究

## ① 既存の表層分析手法に関する調査

既存の表層分析手法および分析ツールを調査し、調査結果を整理すること。

② 既存の表層分析手法の効果的な活用方法の検討

既存の表層分析手法のうち十分に活用しきれていない手法を、効果的に活用する方法を検討し、調査結果を整理すること。

③ 新しい表層分析手法の検討

既存技術ではカバーできていない分析結果を得るための新たな表層分析手法を検討、開発すること。また開発した表層分析手法をツールとして実装すること。

④ 表層分析手法の評価

②、③で、検討または開発した表層分析手法を実際のマルウェアを用いて評価すること。

⑤ 上記についての調査内容をとりまとめ、調査報告書を作成すること。

(2) 新しいWindows OSにおけるマルウェアの分析環境調査

① 新しい環境(64ビット版 Windows 8.1, Windows 10)に関する技術調査

新しい環境で導入・変更された技術について調査を行い、調査結果を整理すること。

② マルウェア分析ツールに関する技術調査

既存のマルウェア分析ツールの、新しい環境への対応状況を調査し、調査結果を整理すること。

③ マルウェアが使用するテクニックの検証

既存のマルウェアが使用する各種テクニックに関して、最新の環境で使用可能か調査し、調査結果を整理すること。

④ 上記についての調査内容をとりまとめ、調査報告書を作成すること。

(3) 上記二つ以外のテーマにおける、分析手法・分析環境の高度化に関する調査

①分析手法・分析環境の高度化に関するテーマを提案し、その内容について調査・研究を実施し報告書としてとりまとめること。なお、報告書の構成として、以下の項目を必ず含むこととする。

A) 既存技術および動向の調査

B) 既存技術の応用または新規技術を用いた、分析手法・分析環境の高度化の検討

C) マルウェアを用いた検討内容の評価

なお、調査期間中には、月に2回程度、JPCERT/CC において進捗および調査内容についての報告を行う。

4. 入札要件

(1) 過去に情報セキュリティに関する調査・研究の経験を有し、それを事業として請け負うことができる事業者であること。

- ① マルウェアに関わる調査研究の実施経験があることが望ましい。
- (2) マルウェア分析技術を有し、マルウェアを安全かつ適切に取り扱える環境を有しているまたは、整備できる事業者であること。
  - ① マルウェア分析業務の実施経験があることが望ましい。
5. 実施期間  
平成28年3月18日（金）までに納品し、検収を受けること。（契約締結日から5ヶ月間を目安とする。）
6. 成果物
  - ・ 調査報告書 正副各1部
  - ・ 調査報告書と、調査にあたり作成したデータ等を格納した電子媒体(CD-R 等) 正副各1部
7. 納入場所  
JPCERT コーディネーションセンター

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