2022 年 8 月 18 日

2022年度「ネットワークログ分析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：2022 年度「ネットワークログ分析システムの開発業務」
(2) 内　容　等：別紙 1 のとおり（2022 年度「ネットワークログ分析システムの開発業務」仕様書）
(3) 履 行 期 限：別紙 1 のとおり（2022 年度「ネットワークログ分析システムの開発業務」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令和 4 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、税抜き金額をもって落札価格とするので、入札者は消費税およ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関わらず、入札書には税抜きの金額を記載すること。

2. 入札要件

(1) 予算決算および会計令（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、被保佐人また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また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) 入札案件に対して原則、再委託を行わないこと。ただし、やむを得ない場合はあらかじめ JPCERT コーディネーションセンターにあらかじめ申し出ること。
(6) 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もとづいて提案書を作成し、これを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)入札説明会の日時および場所

日時：2022 年 9 月 5 日（月） 16 時 00 分～17 時 00 分（1 時間程度を予定）

場所：Web 会議システムによるオンライン開催

Web 会議システムを使用できない場合は、以下の場所での参加を認める

東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階

TEL ：03-6271-8901

FAX ：03-6271-8908

※説明会参加希望者は 9 月 2 日（金）17 時までに ir-info@jpcert.or.jp に必要事項（法人名、部署名、参加者氏名（2 名まで）、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。なお、9 月 2 日（金）に通信状態の事前確認を実施する（別途連絡）

(2) 提案書の受領期限および受領場所

期限：2022 年 9 月 12 日（月）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：郵便（簡易書留による）

(3) 入札者決定の通知日

2022 年 9 月 16 日（金）

(4) 入札日

日時：2022 年 9 月 20 日（火）10 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) 入札保証金および契約保証金

全額免除

(2) 入札書の変更および取消し

入札者は、提出した入札書等の変更およ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およ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恐れがあると認められるとき、また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恐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. 問い合わせ先（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
インシデントレスポンスグループ　朝長（ともなが）／ 水野（みずの）
Email ：**ir-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） ／ 神山（かみやま）
Email ：**soumu@jpcert.or.jp**

※緊急を要する場合に限り、電話による問い合わせ可
9:00～18：00（12:00～13:00は除く）月～金曜日（祝・休日を除く）
TEL：03-6271-8901（※留守番電話対応中のため、録音いただけましたら折り返します）

JPCERT CC®

別紙1

2022年度「ネットワークログ分析システム」開発業務仕様書

1. 件名

2022年度「ネットワークログ分析システム」開発業務

2. 目的

JPCERT/CCでは、セキュリティインシデントが発生した組織の被害状況調査をサポートしており、被害組織のログ分析やディスクフォレンジック調査業務を行っている。
本開発システムは、Webサーバー、プロキシサーバーなどのネットワーク機器のログを参照可能なフォーマットでデータベースに格納し、検索および可視化による分析を可能とするシステムの開発を行う。昨今の在宅ワークの定着や侵入型ランサムウェア攻撃などの多様な業種へのセキュリティインシデントの被害が拡大するに伴い、セキュリティインシデント調査をスムーズにスタートさせることが難しくなっている。このような背景を踏まえて、現状の問題を解決するためのシステムの構築を行う。本システムは、セキュリティインシデント発生時のログ分析の際に発生する、以下の問題点を解決することを目的とする。

(1) 大量のログデータを調査依頼者と調査担当者（JPCERT/CC）の間での受け渡しを安全に行う必要性
(2) 受け取ったデータを素早く分析可能な状態（検索・可視化できる）にする
(3) ログデータの安全な管理
(4) 複数人での同時分析
(5) 分析結果（エビデンス）の保存

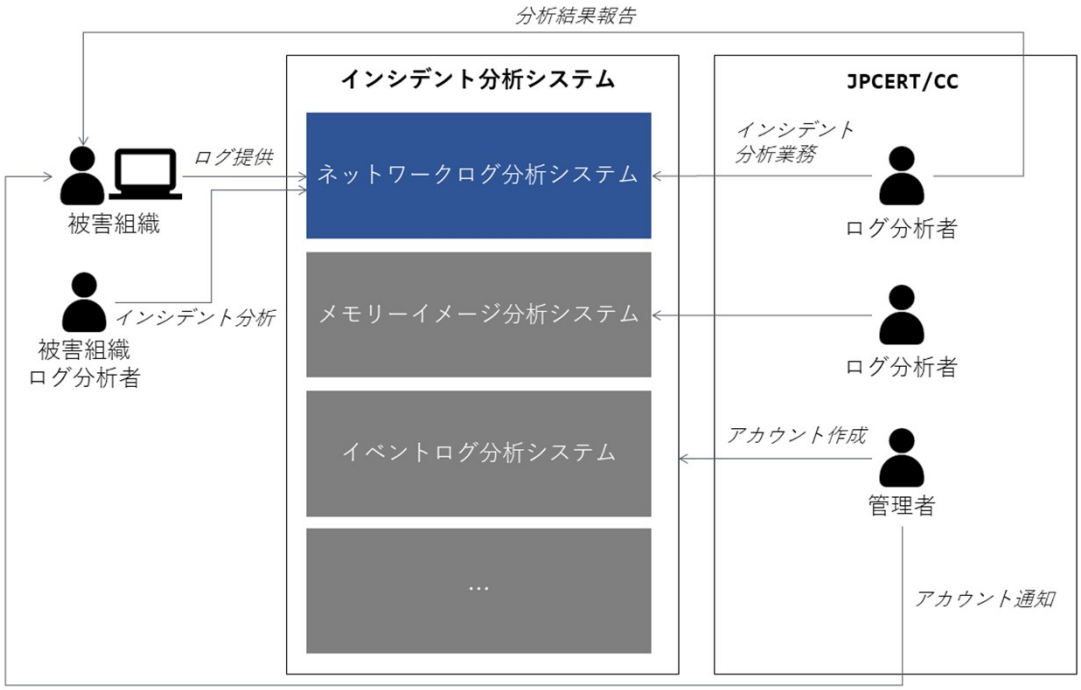
2.1 用語の定義

用語	説明
被害組織	セキュリティインシデント発生時のログを提供する組織
ログ分析者	ログ分析を担当するJPCERT/CC担当者および被害組織の担当者
管理者	本システムを管理するJPCERT/CC担当者
インシデント分析業務	セキュリティインシデント調査時の各種アーティファクトを分析する業務（本システムを使用する業務）
インシデント分析システム	セキュリティインシデント調査時の各種アーティファクトを分析するシステム全体
ネットワークログ分析システム	インシデント分析システム内でネットワーク分析を担当するシステム（本入札の開発範囲）
ログ	Webサーバー、プロキシサーバーなどのネットワーク機器のログ
ログアップロード機能	ログファイルをアップロードするためのWeb GUI
ログパース機能	受信したログをパースして、データベースに格納

ログデータベース	アップロードしたログをユーザーごとに管理および参照可能なデータ
ログ分析機能	データベースのログを検索および可視化可能なWeb GUI
ログ管理機能	データベースに格納されたログを削除する機能
ユーザー管理機能	本システムを使用するユーザーを管理
ユーザー認証	本システム使用時のユーザー認証機能およびWeb GUI
アクセス制御機能	ユーザーごとにアクセス可能な機能およびデータベース（ログ）を制限する

2.2 用語の定義

「ネットワークログ分析システム」の業務範囲を［図 1］に示す。



［図 1: 「ネットワークログ分析システム」の業務範囲］

「ネットワークログ分析システム」を使用した業務フローは以下のとおりである。

［0.］ 管理者が本システムを使用する被害組織のアカウントを作成し、通知
［1.］ 被害組織が本システムにログをアップロード
［2.］ 本システムにてログを分析可能な状態に処理し、保存
［3.］ ログ分析者が本システムを使用し、インシデント分析業務を行う
［4.］ 被害組織にてログ分析者が所属している場合は、本システムを使用してインシデント分析
［5.］ ログ分析者（JPCERT/CC）が分析結果を被害組織にレポート
［6.］ インシデント分析業務終了後、管理者がシステム上のログを削除

3. 本システム開発の前提条件

3.1 開発方針

- システムの構築はAWS上に行う
- システムはTerraformで構築・管理可能にする
- 各機能について既存のクラウドサービスを使用できる場合は、そのサービスをなるべく使用する
- クラウドサービスのアップデート（仕様変更）に伴うシステムの不具合を最小限に抑える
- 開発プロセス内でプロトタイプを作成し、仕様の相違が発生しないように、随時JPCERT/CCとプロトタイプの確認を行いながら進める
- インシデント分析システム内の他のシステムとの連携を考慮する
- システム内で使用するアプリケーション管理（脆弱性対策）のコストを削減するためにサーバーレスサービスの使用を検討する
- JPCERT/CCが準備するバージョン管理システム（GitLab）を使用し、コード管理、課題管理を行う
- 委託先が準備するAWSアカウントを使用して開発を行う

3.2 スケジュール

詳細なスケジュールは、JPCERT/CCと協議のうえ、決定する。以下にスケジュール概要を示す。

スケジュール	内容
2022年10月	開発プロジェクト開始
2022年10月~2023年1月	設計 & プロトタイプ開発 & テスト
2023年2月	受け入れテスト & 脆弱性診断（JPCERT/CCにて実施）
2023年3月	問題箇所および脆弱性の修正・納品
納品後から2023年3月31日	検収

3.3 実施期間および納期

- 実施期間：契約締結日から2023年3月31日（金）まで
- 納期：2023年3月20日（月）

3.4 成果物

- 詳細設計書
- テスト計画書およびテスト結果報告書
- 本システムを構築する際のTerraformコード
- テストコード
- 利用マニュアル
  - ✓ 管理者向け
  - ✓ 被害組織向け
- 構築手順書
- 作業報告書（プロジェクト計画、打ち合わせ議事録、テスト結果など）

なお、Terraformコードや利用マニュアルは原則として公開を前提とした（機密情報など一般公開された際にシステムへの影響が及ばない）整備が行われていること。

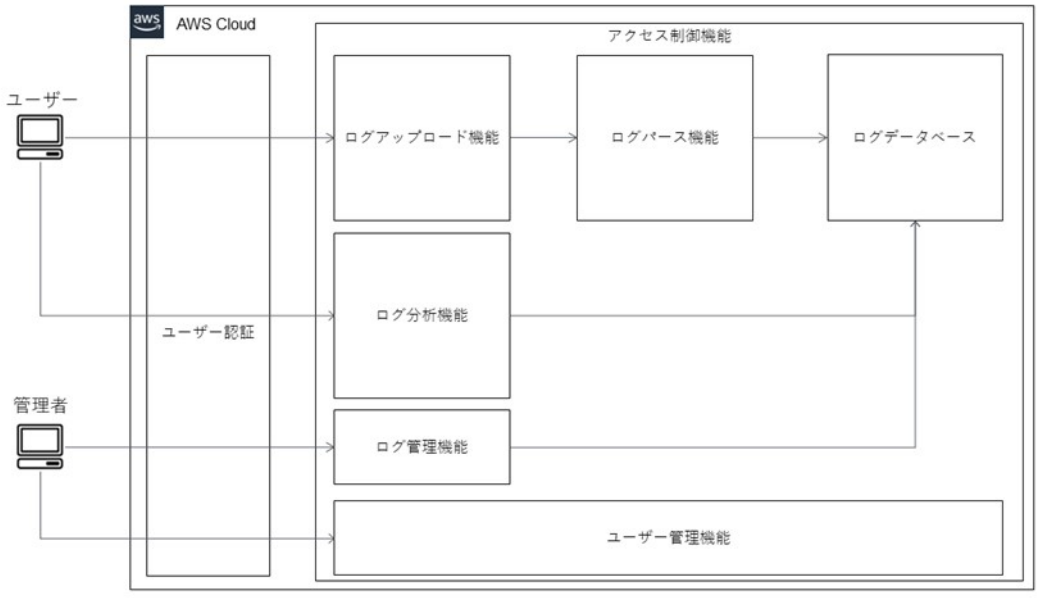
3.5 納入場所

一般社団法人 JPCERT コーディネーションセンター

4. システム概要

4.1 システム概要図

「ネットワークログ分析システム」の機能と各機能の関係を［図 2］に示す。



［図 2: システム概要図］

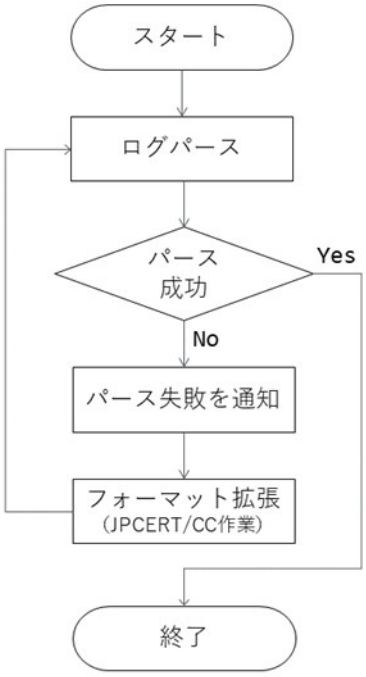
4.2 機能要件

4.2.1 ログアップロード機能

- Web GUIからファイルとしてログをシステムにアップロード可能にする
- アップロードされたログは、一時的に保管し、ログパース機能にてパース処理を行う
- アップロード可能なファイルの最大サイズ
  - 5G（ブラウザー、AWSサービスにおけるタイムアウトを考慮する）
- 同時に複数のファイルをアップロード可能
- 受信対象のファイル形式は以下のとおり
  - テキスト形式
  - ZIP形式
  - tar.gz形式
- ログがアップロードされたことを指定したメールアドレスに通知する

4.2.2 ログパース機能

- ログ受信機能からログを受信し、ログをパースしてデータベースに格納する
- パースするログのフォーマット形式は以下のとおり（プロキシサーバーやその他のネットワーク機器のパース機能は、JPCERT/CCにて後ほど拡張予定）
  - Apache（Common Log Format）
  - Nginx（デフォルトフォーマット）
- パースするログのフォーマットは、拡張可能にする
  - フォーマットを追加定義可能
- ファイルのフォーマットが異なるためにパースするような場合に備えて、パース失敗時に再度パース処理を行えるようにする（図 3を参照）
- 本機能は動作ごとにインスタンスとして起動する



［図 3: ログパース機能失敗時のフロー］

4.2.3 ログデータベース

- ログパース機能から受信したログを格納する
- ログデータはユーザーごとに管理可能なように保存する
- ログデータは案件ごと（ケース）に管理可能なように保存する
- ログデータは削除可能なように管理する
- データベースはELKスタックまたは、それと同等の機能を有するものを使用する
- 本機能はユーザーごとにインスタンスとして起動する

4.2.4 ログ分析機能

- Web GUIにてログデータベースに格納されたデータを検索および可視化する
- ログの検索はユーザーに紐づくデータのみに制限する
- 検索クエリは保存可能にする
- ログ分析機能はELKスタックまたは、それと同等の機能を有するものを使用する
- 本機能はユーザーごとにインスタンスとして起動する

4.2.5 ログ管理機能

- Web GUIにてログデータベースのデータを削除可能にする

- 削除するデータの指定方式は以下のとおり
  - ユーザー
  - ケース
  - 日時

4.2.6 ユーザー管理機能

- Web GUIにて本システムを使用するユーザーを作成、削除、使用停止を可能にする
- ユーザーに付与可能な権限は3つ準備する

使用可能機能	一般ユーザー	分析ユーザー	管理者
ログアップロード機能	○	○	○
ログ分析機能	-	○	○※1
ログ管理機能	-	-	○
ユーザー管理機能	-	-	○

※1 すべてのユーザーのログを検索可能

- 本機能は、インシデント分析システム内の他のシステムにも適用可能にする

4.2.7 ユーザー認証

- Web GUIにてSSOによる認証を行う
- 本機能は、インシデント分析システム内の他のシステムにも適用可能にする

4.2.8 アクセス制御機能

- ユーザーごとに使用可能な機能を制限する
  - ユーザーごとのアクセス制御は「ユーザー管理機能」に記載
- ユーザーごとにアクセス可能なデータベースを制限する

4.2.9 その他機能に含める要件

- 以下の機能はスケールアウト可能な構成にする
  - ログパース機能
  - ログデータベース

4.3 性能要件

- システムの同時利用者想定数
  - 5人
- 1カ月の想定システム使用件数
  - 4件
- アップロード可能なファイルの最大サイズ
  - 5G
- ログパース機能の最大待ち時間
  - 2時間

4.4 テスト要件

- 単体テスト、結合テスト、総合テストおよびJPCERT/CCによる受入テストを実施する（各テストの方針について提案書に記載する）
- Google Chrome、Firefoxのテスト時の最新バージョンにおいて動作確認を行う
- テスト結果はJPCERT/CCに報告し、確認された問題は、修正の上で納入する

4.5 セキュリティ機能要件

- システムの可用性確保
  - システムの異常停止を監視し、障害発生時に迅速な復旧を行う方法または機能を備えること
- 不正通信の遮断
  - 許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること
- システムログの蓄積・管理
  - システムへの不正行為の検知、発生原因の特定に用いるために、システムの利用記録、例外的事象の発生に関するシステムログを蓄積し、1年間の期間保管するとともに、不正の検知、原因特定に有効な管理機能（システムログの検索機能、システムログの蓄積不能時の対処機能等）を備えること。
  - システムログの改ざんや消去に備えて、定期的なバックアップを取得する。
- ログの保護
  - ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能および消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失および破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。
- 管理者権限の保護
  - 特権を有する管理者による不正を防止するため、管理者でアクセスできるネットワークを制限する機能を備えること
- 保存情報の機密性確保
  - ログへ直接アクセスできるネットワークを制限する機能を備えること

- システムの構成管理
  - システム構築時のソフトウェアおよびサービス構成に関する詳細情報が記載された文書を提出するとともに文書どおりの構成とし、脆弱性の発生が想定されるソフトウェアに関するアップデート方法を備えること
  - システムおよびクラウドサービスの設定を管理し、意図しない変更を検知できる機能を備えること
- Webアプリケーションのセキュリティ対策
  - 独立行政法人情報処理推進機構「安全なWebサイトの作り方改訂第7版（https://www.ipa.go.jp/files/000017316.pdf）」に基づいてセキュリティを意識した設計、開発を行うこと
- 構築時の脆弱性対策
  - JPCERT/CCにて実施した脆弱性診断の結果をもとに、対処が必要な脆弱性は修正の上で納入すること

4.6 入札要件

- AWSおよびTerraformを使用した開発経験を有すること
- Webアプリケーションおよびデータベースを伴うシステム開発経験を有すること
- ネットワークログ分析業務について知識または経験があること
- CIツール、バージョン管理システム（Git）を使用した開発経験を有すること

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および会計令（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。

予算決算および会計令（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　当該契約を締結する能力を有しない者

二　破産手続開始の決定を受けて復権を得ない者

三　暴力団員による不当な行為の防止等に関する法律（平成三年法律第七十七号）第三十二条第一項各号に掲げる者

（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ときは、その者について三年以内の期間を定めて一般競争に参加させないことができる。その者を代理人、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、製造その他の役務を粗雑に行い、または物件の品質若しくは数量に関して不正の行為をしたとき。

二　公正な競争の執行を妨げたときまた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とき。

三　落札者が契約を結ぶことまたは契約者が契約を履行することを妨げたとき。

四　監督または検査の実施に当たり職員の職務の執行を妨げたとき。

五　正当な理由がなくて契約を履行しなかつたとき。

六　契約により、契約の後に代価の額を確定する場合において、当該代価の請求を故意に虚偽の事実に基づき過大な額で行つたとき。

七　この項（この号を除く。）の規定により一般競争に参加できないこととされている者を契約の締結または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とき。

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。