

# 仕様書

## 1. 契約件名

自動車リサイクルシステムのセキュリティ診断業務役務請負

## 2. 目的

自動車リサイクルシステムは、「使用済自動車の再資源化等に関する法律（以下、「自動車リサイクル法」という。）」に基づき、平成17年1月からサービスを開始しており、9万以上のリサイクル関連業者だけでなく、自動車メーカー、自動車の所有者及び国、自治体がインターネット経由で利用している。まさに、自動車リサイクル業務の円滑な遂行に必要不可欠なものである。

しかしながら、昨今のインターネットを取り巻く環境は、不正アクセス又はそれを試みる行為やウィルス等（以下「不正アクセス手法等」という。）によりシステムにダメージを与えるなどの被害が、後を絶たないのが現状である。

これら、不正アクセス手法等による被害の大きな要因としては、各種の脆弱点（セキュリティホール：情報システムを構成する各種OS、アプリケーションソフトウェア、通信手段等におけるセキュリティ上の問題を惹起させるソフトウェア上の欠陥）があり、日々、新たな報告がされているところである。情報システムの安全性を高めるためには、最新情報に基づいた各種の脆弱点のセキュリティ診断を定期的に行うことが重要である。

本年5月のサーバ入替えに際して、各種OSやミドルウェアは最新情報に基づく対策を行ったが、アプリケーションソフトウェアはそのまま継続使用しているため、アプリケーションソフトウェアのセキュリティ診断を実施するものである。

## 3. 業務内容

自動車リサイクルシステムについて、受注者は以下に従いセキュリティ診断を実施すること。

なお、セキュリティ診断対象アプリケーションソフトウェアは、別紙の通り。

### (1) 実施計画書の作成

受注者は、契約締結後、速やかにセキュリティ診断の実施に関する計画書を策定し、公益財団法人 自動車リサイクル促進センター システム部担当職員（以下、「担当職員」という。）の了解を得ること。

なお、実施計画書には、診断実施日時、セキュリティ診断対象アプリケーションソフトウェア、診断手法及び診断項目の概要、診断を実施する者、診断実施によるシステムテスト環境（以下、「ST環境」という。）運用上のリスク及びその回避方法、中間報告書及び診断結果報告書の構成と記入例を記載すること。

(2) 外部からのセキュリティ診断

セキュリティ診断対象アプリケーションソフトウェアに対し、事前に届け出たIPアドレスより当センター外部（インターネット側）からST環境にツール及び専門家による疑似攻撃を実施し、独立行政法人 情報処理推進機構（IPA）発行の「Webアプリケーション脆弱性対策チェックリスト」(2010年4月掲載)にある脆弱性を網羅したセキュリティ診断を行うこと。

なお、診断項目の詳細については、実施計画書策定時に担当職員と協議すること。

(3) 中間報告書の提出

上記(2)の結果をもとに問題点とその再現手順及びリスクを一次判定した中間報告書を作成し提出すること。記載項目等については、担当職員と協議の上決定すること。

(4) 診断結果報告書の作成及び報告会の開催

上記(2)の結果をもとに問題点とその原因を特定するとともに、それら进行分析し、アプリケーション面だけでなく、インフラ面からの改善策等についても考察を行った診断結果報告書を作成すること。診断結果報告書には、必要に応じ関連データを添付することとし、記載項目等については、担当職員と協議の上決定すること。

診断結果報告書は担当職員に予め検査を受け、合格すること。検査の結果不合格のものについては、担当職員の指示に従い、遅滞なく手直しをし、再検査を受けた上で担当職員等を対象とした報告会を実施すること。

4. 業務実施場所

特に指定しない。

但し、報告会は公益財団法人 自動車リサイクル促進センターで実施のこと。

5. 納入物品

診断結果報告書 2部(正1部、副1部)

上記の納入物品については、紙媒体で納入するとともに、Microsoft PowerPoint 2003又はOpenOffice.org 3.2.0でレイアウトの崩れなく読み取れるように作成されたファイル及び当該ファイルをISO 26300 (ODF)形式で保存したファイルをISO 9660形式にフォーマットされたCD-R又はDVD-Rのいずれか1枚に格納すること。

なお、関連データは、Microsoft Excel 2003又はMicrosoft Word 2003でレイアウトの崩れなく読み取ることが可能なファイルを用いることができるものとする。

6. 納入期限

平成22年10月29日(金)

## 7. 納入場所

公益財団法人 自動車リサイクル促進センター システム部

## 8. 実施要件

- (1) 受注者は、診断及び結果の分析を行うときには、自動車リサイクルシステムのネットワーク構成及び運用上の規制・習慣等に関して、十分理解の上、与えられた環境下において実施すること。

なお、既存のネットワークの運用形態を崩さないよう十分に留意すること。

- (2) 診断に際して、自動車リサイクルシステムに異常が発生した場合は、その責任を負うとともに、状況や対処方法等について、担当職員に直ちに報告の上、必要な対処を行う。また、担当職員と協議の上、当該事案に係る一連の経緯、対処等に加え、原因などについての考察を含めた報告書を早急に作成し、提出すること。
- (3) 自動車リサイクルシステムへ調査・分析のための装置等を設置する場合は、事前に担当職員と十分協議を行った上で実施することとし、自動車リサイクルシステムへの影響を最小限に留める様、留意すること。

## 9. 情報セキュリティに関する事項

- (1) 契約期間中及び契約終了後においても、業務に関して知り得た当センターの業務上の内容について、他に漏らし又は他の目的に利用してはならない。
- (2) 当センター内で取り扱うデータ及び情報システムの取扱いには十分注意を払い、担当職員の許可なく当センター外に持ち出すことのないようにすること。
- (3) 受注者は、業務実施期間中において、セキュリティ診断関係書類（診断結果報告書、関係資料、関連メモの原本及びコピー等（媒体を問わず）を指し、当センターより貸与したものも含む。）を機密扱いとして整理・保管すること。また、セキュリティ診断業務完了後又は契約解除する場合には、セキュリティ診断関係書類を速やかに当センターに提出又は機密管理の上破棄し、その旨を担当職員に書面で報告すること。
- (4) 受注者は、当センター内に複製が可能な電子計算機等の機器を持ち込んで業務を行う必要がある場合には、事前に担当職員の許可を得ること。

なお、この場合であっても、担当職員の許可なく複製してはならない。

- (5) 受注者は、貸与された紙媒体、電子媒体であっても、担当職員の許可なく当センター外で複製してはならない。また、業務終了後には、複製した情報等が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。
- (6) 受注者は、業務の遂行において、当センターの情報セキュリティが侵害され又はその恐れがある場合には、速やかに担当職員に報告を行い、原因究明及びその対処方法等について担当職員と協議すること。

## 10. その他

- (1) 納入物品に関する所有権、著作権及びその他の権利は、原則として、当センターを含む4法人に帰属するものとする。受注者は予め4法人の受託を得た場合のみ、業務の成果物を基に二次的著作物を製作し、譲渡、貸与等を行うことができる。

納入物品に、受注者が従前から保有する知的財産権が含まれていた場合は、権利は受注者に留保されるが、4法人及び4法人の指定した機関等は、納入物品を利用するために必要な範囲において、これを無償で利用できるものとする。

受注者は4法人に対し、著作者人格権を行使しないものとする。第三者から納入物品に対し権利侵害に関する訴えが生じた場合は、受注者の責めにおいて解決するものとする。

- (2) 業務における体制表（以下「実施体制表」という。）を契約後、速やかに担当職員に提出すること。実施体制表には、責任者及び業務に従事させる主担当者の氏名及び所属、担当業務、指揮命令系統並びに連絡先を記載すること。

なお、実施体制表を変更する場合は、事前に、変更後の体制表を担当職員に提出すること。

- (3) 業務に際して発生した不明な点は、担当職員に確認の上、指示に従うこと。  
(4) 業務に関して緊急に是正すべき点が明らかになった場合は、診断の最中であっても、直ちに担当職員に報告すること。

- (5) 担当職員が受注者に対し、常時契約履行に関する調査を行える体制とすること。

- (6) 業務に係る診断ツール及び通信費等の一切の費用は、受注者の負担とする。

- (7) 受注者は、役務の全部若しくは大部分を一括して第三者に委任し、又は請負わせてはならない。ただし、当センターの承諾を得た場合は、この限りではない。

受注者は、第三者に委任し、又は請負わせる場合には、委任又は請負寄せた業務に伴う当該第三者の行為について、当センターに対しすべての責任を負うものとする。

受注者は、第三者に委任し、又は請負わせる場合には、受注者がこの契約を遵守する為に必要な事項について、当該第三者と約定しなければならない。

なお、当該第三者がさらに別の第三者に委任し、又は請負わせてはならない。

(別紙)

セキュリティ診断対象アプリケーションソフトウェア画面数

203画面

なお、画面情報の詳細は「秘密保持誓約書」の受領後に開示する。