

令和7年度 情報セキュリティリスク診断業務

仕 様 書

令和7年4月

東日本高速道路株式会社

1. 総則.....	1
1-1. 適用の範囲.....	1
1-2. 用語の定義.....	1
1-3. 契約書類の解釈.....	2
1-4. 日数等の解釈.....	2
1-5. 監督員、主任補助監督員及び補助監督員.....	2
1-5-1. 監督員.....	2
1-5-2. 主任補助監督員.....	2
1-5-3. 補助監督員.....	2
1-6. 受注者の要件及び責任者等.....	3
1-6-1. 受注者の要件.....	3
1-6-2. 履行責任者の要件.....	3
1-6-3. 作業責任者.....	3
1-7. 提出書類.....	4
1-7-1. 監督員を経由しない提出書類.....	4
1-7-2. 提出書類の様式.....	4
1-7-3. 契約金額内訳明細書.....	5
1-8. 業務計画書.....	5
1-8-1. 業務計画書の提出.....	5
1-8-2. 変更業務計画書.....	5
1-9. 資料の貸与及び返却.....	5
1-9-1. 資料の貸与.....	5
1-9-2. 資料の保管及び返却.....	5
1-9-3. 資料の修復.....	5
1-9-4. 資料の守秘義務.....	5
1-10. 業務の再委任等.....	5
1-10-1. 指定した主たる部分の再委任.....	5
1-10-2. 軽微な部分の再委任.....	6
1-10-3. その他の再委任.....	6
1-10-4. 再委任等の要件.....	6
1-10-5. 再委任等者の管理等.....	6
1-11. 打合せ.....	6
1-12. 履行状況報告.....	6

1-13. 業務の変更.....	6
1-13-1. 業務の変更指示 .....	6
1-13-2. 変更業務の施行 .....	6
1-14. 業務の一時中止に伴う増加費用の協議.....	7
1-15. 契約変更.....	7
1-15-1. 契約変更.....	7
1-15-2. 契約変更書類の作成.....	7
1-16. 履行期間の変更 .....	7
1-16-1. 事前協議.....	7
1-16-2. 事前協議の手続き .....	7
1-16-3. 受注者からの履行期間延長の請求 .....	7
1-17. 完了検査.....	8
1-17-1. 完了届 .....	8
1-17-2. 完了届提出の要件 .....	8
1-17-3. 検査日及び完了検査員名の通知.....	8
1-17-4. 検査の立会 .....	8
1-17-5. 完了検査の内容 .....	8
1-17-6. 軽微な修補の取扱い .....	8
1-17-7. 受渡書の提出.....	9
1-17-8. 部分引き渡し・一部完了検査 .....	9
1-18. 代金の支払い .....	9
1-19. 遅延日数の算定 .....	9
1-20. 成果品 .....	9
1-21. 契約不適合責任.....	9
1-21-1. 欠陥の調査 .....	9
1-21-2. 欠陥の原因の調査に要する費用の負担.....	9
1-22. 秘密の保持.....	10
1-22-1. 目的.....	10
1-22-2. 定義.....	10
1-22-3. 情報管理体制の確保.....	10
1-22-4. 情報の明示 .....	10
1-22-5. 目的外の使用.....	10
1-22-6. 取得の制限 .....	10
1-22-7. 適切な管理 .....	10
1-22-8. 利用者の制限.....	10
1-22-9. 資料の持ち出しの禁止 .....	11

1-22-10. 複写又は複製の禁止 .....	11
1-22-11. 守秘義務 .....	11
1-22-12. 履行期間完了後の取扱い .....	11
1-22-13. 第三者への委任等について .....	11
1-22-14. 調査及び報告 .....	11
1-22-15. 事故時の対応 .....	11
1-22-16. 事故時の責任分担 .....	11
1-23. 紛争中における発注者、受注者の義務 .....	12
1-24. 関係法令及び条例の遵守 .....	12
1-25. 著作権の譲渡等 .....	12
2. 業務の概要 .....	13
2-1. 目的 .....	13
2-2. 履行期間 .....	13
2-3. スケジュール .....	13
2-4. 履行場所 .....	14
2-5. 業務の実施概要 .....	14
3. 業務細部 .....	17
3-1. 通信調査 .....	17
3-2. ペネトレーションテスト .....	18
3-3. 実施結果の分析及び評価 .....	21
3-4. その他 .....	23
3-5. 成果品の作成 .....	23

# 1. 総則

## 1-1. 適用の範囲

本仕様書は、東日本高速道路株式会社(以下「発注者」という。)が行う「令和7年度 情報セキュリティリスク診断業務」(以下「本業務」という。)に適用するものとし、本業務に係る「役務契約書」(以下「契約書」という。)について統一的な解釈及び運用を図るとともに、本業務に係る必要事項を定め、契約の適正な履行の確保を図るものとする。

## 1-2. 用語の定義

契約書類に使用する用語の定義は、次の各号に定めるところによる。

- (1)「契約書類」とは、契約書第1条に規定する契約書及び仕様書等をいう。
- (2)「仕様書等」とは、仕様書、入札(見積)者に対する指示書及びこれらを補足する書類をいう。また、発注者がその都度提示した変更仕様書若しくは追加仕様書を含むものとする。
- (3)「契約金額内訳明細書」とは、契約書第3条第1項の規定に基づき、契約金額の内訳を示したものをいう。
- (4)「監督員」とは、契約書第8条第1項の規定に基づき、発注者が定め受注者に通知した者をいう。
- (5)「主任補助監督員」及び「補助監督員」とは、本仕様書 1-5-2 及び 1-5-3 の規定に基づき、監督員が定め受注者に通知した者をいう。
- (6)「履行責任者」とは、契約書第9条第1項の規定に基づく履行責任者として、受注者が配置し発注者に通知した者をいう。
- (7)「完了検査」とは、契約書第25条第2項の規定に基づき、業務の完了を確認するために行う検査をいう。
- (8)「検査員」とは、契約書第25条第2項の規定に基づき、「完了検査」を行うために発注者が定めたものをいう。
- (9)「指示」とは、監督員が受注者に対し、業務の実施に必要な方針、事項等について書面により示し、実施させることをいう。
- (10)「承諾」とは、契約書類で明示した事項について、発注者若しくは監督員又は受注者が書面により同意することをいう。
- (11)「協議」とは、書面により業務の内容又は取扱い等について、発注者又は監督員と受注者が対等の立場で合議し、結論を得ることをいう。
- (12)「提出」とは、監督員が受注者に対し、又は受注者が監督員に対し業務の実施等に係わる書面又はその他の資料を説明し、差し出すことをいう。
- (13)「提示」とは、監督員が受注者に対し、又は受注者が監督員に対し業務の実施等に係わる書面又はその他の資料を示し、説明することをいう。
- (14)「報告」とは、受注者が監督員に対し、業務の進行状況等を必要に応じて書面により知らせることをいう。
- (15)「通知」とは、監督員が受注者に対し、又は受注者が監督員に対し業務の実施等に関する事項について、書面をもって知らせることをいう。
- (16)「書面」とは、手書き、印刷物等の伝達物をいい、発行年月日を記載し、署名又は捺印したものを有効とする。緊急を要する場合は、ファクシミリ又は電子メールにより伝達できるものとするが、速やかに有効な書面を作成するものとする。

(17)「参考」とは、契約書類に含まれない図書で、発注者及び受注者を拘束するものではない。

### 1-3. 契約書類の解釈

契約書類は、相互に補完し合うものとし、そのいずれか一つによって定められている事項は、契約の履行を拘束するものとする。

### 1-4. 日数等の解釈

契約書類における期間の定めは契約書第1条第10項の規定によるものとするが、履行期間以外の日数の算出に当たっては、12月29日から翌年1月3日までの期間、5月3日から5月5日までの期間及び8月13日から8月15日までの期間の日数は算入しないものとする。

### 1-5. 監督員、主任補助監督員及び補助監督員

#### 1-5-1. 監督員

契約書第8条第1項第5号の規定に基づき監督員に委任した権限は次の各号に掲げるものをいう。

- (1) 契約書第11条の規定に基づき行う報告の受理及び確認
- (2) 契約書第12条の規定に基づき行う報告の受理、調査若しくは検査及び指示
- (3) 契約書第13条の規定に基づき行う貸与品等の取扱い
- (4) 契約書第14条の規定に基づく仕様書等の変更
- (5) 契約書第15条の規定に基づき行う業務の全部又は一部の一時中止の指示
- (6) 契約書第17条の規定に基づき行う履行期間の変更の請求
- (7) 契約書第20条第2項の規定に基づき行う通知の受理及び第3項の規定に基づき行う臨機の措置の請求書面の提出は、仕様書等に定めるものを除き、監督員を経由して行うものとする。この場合においては、監督員に到達した日をもって発注者に到達したものとみなす。

#### 1-5-2. 主任補助監督員

監督員は、自己を補助させるために主任補助監督員を定め、自己の権限とされる事項のうち監督員が必要と認めた権限を委任することができるものとする。この場合において、監督員は主任補助監督員の氏名を受注者に通知するものとし、委任した権限の内容は下記に示すものとする。なお、主任補助監督員を変更したときも同様とする。

仕様書の条項	項 目	内 容
1-8-1	業務計画書の提出	業務計画書の提出先及び修正の請求
1-8-2	変更業務計画書	変更業務計画書の提出先
1-9-1	資料の貸与	図書及び関係資料の貸与
1-9-2	資料の保管及び返却	図書及び関係返却資料の提出先
1-11	打合せ	打合せ、業務等打合簿の提出先
1-20	成果品	成果品に関する指示

#### 1-5-3. 補助監督員

監督員は、自己又は主任補助監督員を補助させるために補助監督員を定め、自己の権限とされる事項のうち

監督員が必要と認めた権限を委任することができるものとする。この場合において、監督員は補助監督員の氏名を受注者に通知するものとし、委任した権限の内容は下記に示すものとする。なお、補助監督員を変更したときも同様とする。

仕様書の条項	項 目	内 容
1-11	打合せ	打合せ、業務等打合簿の提出先

## 1-6. 受注者の要件及び責任者等

### 1-6-1. 受注者の要件

受注者は経済産業省が定める「情報セキュリティサービス基準」に適合する企業を記載した「情報セキュリティサービス基準適合サービスリスト」(うち脆弱性診断サービス)に登録されていること。

### 1-6-2. 履行責任者の要件

本業務の遂行にあたり、契約書第9条第1項の規定に基づき配置する履行責任者は、受注者に所属し、下表1-6-2に示す要件に該当するものかつ日本語に堪能(日本語通訳が確保できれば可)で、原則として履行期間を通して配置しなければならない。

なお、配置する履行責任者の通知は、履行責任者届(様式第1-1(1)号)によるものとし、履行責任者を変更したときも、同様とする。

表1-6-2 履行責任者の要件

要件
<p>1. 次のうちいずれかの資格を有すること。</p> <ul style="list-style-type: none"> <li>● 情報処理安全確保支援士</li> <li>● CISSP(Certified Information Systems Security Professional)</li> <li>● CISA(Certified Information Systems Auditor)</li> <li>● CISM(Certified Information Security Manager)</li> <li>● GIAC(Global Information Assurance Certification)</li> <li>● CEH(Certified Ethical Hacker)</li> <li>● OSCP(Offensive SECURITY Certified Professional)</li> </ul> <p>2. 次のいずれかの事業において、令和4年度以降に合計で5件(契約件数。包括的な契約の場合は各診断につき、1年間分で1件とみなす。)以上の実績(診断方法は問わない。)を有すること</p> <ul style="list-style-type: none"> <li>● ウェブアプリケーション診断</li> <li>● プラットフォーム脆弱性診断</li> <li>● スマートフォン／タブレット端末アプリケーション脆弱性診断</li> <li>● その他ソフトウェアやシステムの脆弱性対策を目的とした診断又はテスト</li> </ul>

### 1-6-3. 作業責任者

受注者は、本業務の実施において、業務の管理を行う作業責任者を定めなければならない。

作業責任者は受注者に所属する者とし、下表1-6-3に示す要件に該当するものかつ日本語に堪能(日本語通訳が確保できれば可)で、本業務において、現場業務が発生する場合は、立ち会わなければならない。

作業責任者の通知は、作業責任者届(様式第 1-1(2)号)によるものとし、作業責任者を変更したときも、同様とする。

なお、履行責任者が作業責任者を兼ねることができるものとする。

表1-6-3 作業責任者の要件

要件
1. 次のうちいずれかの資格を有すること。 <ul style="list-style-type: none"><li>● 情報処理安全確保支援士</li><li>● CISSP(Certified Information Systems Security Professional)</li><li>● CISA(Certified Information Systems Auditor)</li><li>● CISM(Certified Information Security Manager)</li><li>● GIAC(Global Information Assurance Certification)</li><li>● CEH(Certified Ethical Hacker)</li><li>● OSCP(Offensive SECURITY Certified Professional)</li></ul>
2. 次のいずれかの事業において、令和4年度以降に合計で5件(契約件数。包括的な契約の場合は各診断につき、1年間分で1件とみなす。)以上の実績(診断方法は問わない。)を有すること <ul style="list-style-type: none"><li>● ウェブアプリケーション診断</li><li>● プラットフォーム脆弱性診断</li><li>● スマートフォン／タブレット端末アプリケーション脆弱性診断</li><li>● その他ソフトウェアやシステムの脆弱性対策を目的とした診断又はテスト</li></ul>

## 1-7. 提出書類

### 1-7-1. 監督員を経由しない提出書類

契約書第 8 条第 5 項に規定する「仕様書等に特別の定めが置かれているもの」とは、次の書類をいう。

- (1) 契約書第 3 条の規定による内訳明細書
- (2) 契約書第 4 条の規定による承諾願
- (3) 契約書第 10 条第 3 項の規定による監督員又は補助監督員に対する措置請求
- (4) 契約書第 25 条の規定による業務完了による受渡書
- (5) 契約書第 26 条第 1 項の規定による代金の支払いに係る請求書
- (6) 契約書第 28 条第 1 項の規定による第三者による代理受理による承諾願
- (7) 契約書第 40 条第 2 項の規定による遅延利息の請求書
- (8) その他発注者の指定した書類

### 1-7-2. 提出書類の様式

受注者が発注者に提出する書類で様式が定められていないものは、受注者において様式を定め提出するもの



とする。ただし、発注者又は監督員がその様式を指示した場合は、これに従わなければならない。

### 1-7-3. 契約金額内訳明細書

契約書第3条に規定する契約金額内訳明細書は、契約金額内訳明細書(様式第1-2(1)号及び(2)号)により提出するものとする。

## 1-8. 業務計画書

### 1-8-1. 業務計画書の提出

受注者は、業務着手前に、次の各号に掲げる本業務の計画に関する事項を記載した業務計画書を監督員に提出しなければならない。ただし、業務着手前に提出することが困難なものについては、後日、別途提出できるものとする。

なお、仕様書等の規定により業務計画書に記載すべき事項と同様な書類がある場合、又は監督員が必要でないと認めた場合は、この限りではない。

また、監督員は、提出された業務計画書を検討の上、必要と認めた場合には、受注者に対して修正を求めることができるものとする。

- |                 |                  |
|-----------------|------------------|
| (1) 業務概要        | (5) 連絡体制         |
| (2) 工程表         | (6) 仕様書等に定められた事項 |
| (3) 業務組織表(実施体制) | (7) その他必要事項      |
| (4) 基本的な業務実施方法  |                  |

### 1-8-2. 変更業務計画書

受注者は、業務計画書の内容を変更する場合は、その都度監督員に変更業務計画書を提出しなければならない。

## 1-9. 資料の貸与及び返却

### 1-9-1. 資料の貸与

監督員は、仕様書に定める図書及びその他関係資料を、受注者に貸与するものとする。

### 1-9-2. 資料の保管及び返却

受注者は、貸与された図書及びその他関係資料の必要がなくなった場合は、ただちに監督員に返却するものとする。

### 1-9-3. 資料の修復

受注者は貸与された図書及びその他関係資料を丁寧に扱い、損傷してはならない。万一、損傷した場合には、受注者の責任と費用負担において修復するものとする。

### 1-9-4. 資料の守秘義務

受注者は、仕様書等に定める守秘義務が求められる資料については複製してはならない。

## 1-10. 業務の再委任等

### 1-10-1. 指定した主たる部分の再委任

契約書第6条第1項に規定する「指定した主たる部分」とは、次の各号に掲げるものをいい、受注者は、これを再委任することはできない。

(1) 計画、調査又はテストにおける総合的企画、業務遂行管理、手法の決定及び技術的判断

(2) 分析、解析又は評価における手法の決定及び技術的判断

#### 1-10-2. 軽微な部分の再委任

契約書第 6 条第 3 項に規定する「軽微な部分」とは、コピー、ワープロ、印刷、製本、計算処理(単純な電算処理に限る)、データ入力、電子納品の作成補助、消耗品購入及び資料整理作成業務等をいう。

#### 1-10-3. その他の再委任

受注者は、前記 1-10-1 に規定する主たる業務以外の業務の一部を第三者に委任する場合は、契約書第 6 条第 3 項の規定に基づき、発注者に再委任等承諾願(様式第 1-3 号)を提出し、その承諾を得なければならない。ただし、発注者の承諾により受注者は契約上のいかなる責任又は義務を免れるものではない。

#### 1-10-4. 再委任等の要件

受注者は、業務の一部を第三者に委任する場合、発注者から「地域 3(関東支社が所掌する区域)」において、取引停止措置を受けている期間中であってはならない。

#### 1-10-5. 再委任等者の管理等

受注者は、業務の一部を第三者に委任する場合、書面により契約関係を明確にしておくとともに、受注者の責任において業務を実施しなければならない。

#### 1-11. 打合せ

受注者は、業務を適正かつ円滑に実施するため、監督員と常に密接な連絡をとり、必要な段階で、十分な打合せを行うものとし、その内容を業務等打合簿(様式第 1-4 号)により監督員に提出するとともに相互に記載事項について確認しなければならない。打合せ場所は、原則として以下のとおりとするが、監督員が指定する Web 会議ツールで開催することも可能とする。なお、打合せに関する費用については、関連する業務に含まれるものとし、別途計上しない。また、後述される説明や報告にかかる開催形式も、原則本項に基づき実施するものとする。

【打合せ場所】東日本高速道路株式会社 本社

(東京都千代田区霞が関3-3-2 新霞が関ビルディング内)

#### 1-12. 履行状況報告

受注者は、契約書第 11 条の規定に基づく履行状況報告において、発注者が求めた場合は速やかに応じるものとする。

#### 1-13. 業務の変更

##### 1-13-1. 業務の変更指示

監督員が、契約書第 14 条の規定に基づく業務内容の変更又は仕様書等の訂正(以下「業務の変更」という。)の指示を行う場合は、業務等指示簿(様式第 1-5 号)によるものとする。

##### 1-13-2. 変更業務の施行

受注者は、業務の変更指示が行われた場合は、その指示に従って業務を実施しなければならない。

#### 1-14. 業務の一時中止に伴う増加費用の協議

受注者は、契約書第 15 条の規定に基づき、監督員が業務の全部又は一部を一時中止させた場合に伴う増加費用については、次のとおり協議し、決定するものとする。

- (1) 受注者は、業務の一時中止に伴い増加費用が生じた場合は、請求額を記した増加費用の請求書を発注者に提出するものとする。
- (2) 受注者から請求があった場合においては、発注者が算定した増加費用の額を記した増加費用の協議書をもって、受注者と協議するものとする。
- (3) 増加費用の額について、発注者からの協議書により受注者は同意書(様式第 1-6 号)を発注者に提出するものとする。なお、協議開始の日から 14 日以内に協議が整わない場合には、発注者が定め受注者に通知するものとする。

#### 1-15. 契約変更

##### 1-15-1. 契約変更

発注者と受注者は、次の各号に掲げる場合において、契約の変更を行うものとする。

- (1) 業務内容の変更により著しく契約金額に変更が生じる場合
- (2) 履行期間の変更を行う場合
- (3) 発注者と受注者が協議し、業務の履行上必要があると認める場合

##### 1-15-2. 契約変更書類の作成

契約変更を行う場合において、受注者は変更する契約書類を発注者所定の書式により作成し、記名押印の上、発注者に提出しなければならない。なお、変更する契約書類は、次の各号に基づき作成するものとする。

- (1) 本仕様書 1-13-1 の規定に基づき監督員が受注者に指示した事項
- (2) 業務の一時中止に伴う増加費用及び履行期間の変更等決定済みの事項
- (3) その他発注者又は監督員と受注者との協議で決定された事項

#### 1-16. 履行期間の変更

##### 1-16-1. 事前協議

事前協議とは、契約書第 16 条の規定に基づく履行期間の変更において、当該変更が履行期間変更協議の対象であるか否かを監督員と受注者で確認する作業をいう。

##### 1-16-2. 事前協議の手続き

監督員は、業務の変更指示を行う場合において、履行期間変更協議の対象であるか否かを併せて通知するものとし、受注者はこれを確認するものとする。なお、受注者は、監督員からの通知に不服がある場合には、7 日以内に異議を申し立てることができる。

また、受注者は、事前協議において履行期間変更協議の対象であると確認された事項及び契約書第 15 条の規定に基づき業務の一時中止を行ったものについて、延長日数の算出根拠、変更工程表その他必要な資料を監督員に提出するものとする。

##### 1-16-3. 受注者からの履行期間延長の請求

受注者は、契約書第 16 条の規定に基づき、履行期間の延長が必要と判断した場合には、必要とする延長日数の算出根拠、変更工程表その他必要な資料を添付の上、速やかに履行期間延長協議書(様式第 1-7 号)

を発注者に提出するものとする。

## 1-17. 完了検査

### 1-17-1. 完了届

契約書第 25 条第 1 項の規定に基づく完了通知は、完了届(様式第 1-8 号)により行うものとする。

### 1-17-2. 完了届提出の要件

受注者は、完了届を発注者に提出する際には、次の各号に掲げる要件をすべて満たさなければならない。

- (1) 仕様書等(追加、変更指示も含む)に示す全ての業務が完了していること。
  - (2) 仕様書等により義務付けられた資料の整備が全て完了していること。
  - (3) 変更契約を行う必要が生じた場合においては最終変更契約書を発注者と締結していること。ただし契約書第 19 条の規定に基づき契約金額の変更、増加費用、損害額について協議中のため、この変更契約を締結できない場合で、契約期間に達した場合は、その部分を除く最終変更契約書が準備されていること。
- また本仕様書 1-17-8 に記載する部分的な完了については、その部分が完了した時点の最新の契約書と読み替えるものとする。

### 1-17-3. 検査日及び完了検査員名の通知

監督員は、業務の完了検査に先立って受注者に対して書面をもって、検査日等を通知するものとする。この場合において、受注者は検査に必要な書類及び資料等を整備するとともに、必要な人員及び機材を準備し、提供しなければならない。

### 1-17-4. 検査の立会

契約書第 25 条第 2 項の規定に基づく受注者の検査の立会については、発注者が必要と認めた場合のみ立会を行うものとし、立ち合いの有無については、前項の検査日等の通知に併せて行うものとする。

### 1-17-5. 完了検査の内容

完了検査は、業務の実施に当たって発注者に提出した書類を対象として契約書類と対比し、検査員が検査を行うものとする。

### 1-17-6. 軽微な修補の取扱い

#### (1) 修補の指示

検査員は、修補の必要があると認めた場合においても、その修補が軽微であると判断した場合には、受注者に対して、期限を定めて修補の指示を行うことができるものとする。ただし、受注者がその指示に異議を申し出た場合はこの限りではない。

#### (2) 修補の完了の確認

検査員が、修補の指示をした場合において、修補の完了の確認は監督員が行うものとする。監督員は、検査員の指示どおり修補が完了したと認めた場合には、受注者に対して完了確認の通知書を交付するものとする。

#### (3) 修補が完了しない場合

検査員が指示した期間内に修補が完了しなかった場合は、軽微な修補としての取扱いをやめ、発注者は契約書第 25 条第 2 項の規定に基づき、検査の結果を通知するものとする。

#### (4) 検査完了期間の取扱い

前(2)により修補の完了が確認された場合は、その指示の日から修補完了の確認の日までの期間を、また

前(3)により取扱いをやめた場合は、その指示の日から期限の日までの期間を、それぞれ契約書第 25 条第 2 項に規定する期間に含めないものとする。

#### (5) 検査結果の通知

監督員が、この軽微な修補の取扱いに基づき、検査員の指示した修補の完了を認め、受注者に完了確認の通知書を交付した場合においても、契約書第 25 条第 2 項の規定に基づいて発注者が行う検査結果の通知において、不合格とすることを妨げるものではない。

#### 1-17-7. 受渡書の提出

受注者は、完了検査に合格し完了認定の通知を受けたときは、速やかに受渡書(様式第 1-9 号)を発注者へ提出しなければならない。

#### 1-17-8. 部分引き渡し・一部完了検査

(1) 成果品について、「3.業務細部」に示す各業務が完了したときについては、前項までの各項を準用して、一部完了検査を行うものとする。この場合において、「業務」とあるのは「部分引渡しにかかる業務」、「完了検査」とあるのは「一部完了検査」、「代金」とあるのは「部分引渡しに係る代金」とそれぞれ読み替えて、これらの規定を準用する。

(2) 受注者は、一部完了検査に合格した場合には、部分引渡しに係る代金の支払を請求することができる。

#### 1-18. 代金の支払い

発注者は、契約書第 26 条第 1 項の規定に基づき代金の支払請求を行う場合には、消費税法に基づく消費税及び地方消費税率を適用するものとし、発注者は契約書第 26 条第 1 項に規定された代金を受注者が指定する金融機関(日本国内の本支店)の口座に振り込むものとする。

#### 1-19. 遅延日数の算定

契約書第 39 条第 5 項に規定する「遅延日数」は、次式により算定するものとする。

遅延日数=(完了届受領日ー契約履行期間日)+(修補の完了届受領日ー不合格の通知日)

なお、不合格の通知日及び修補の完了届受領日は、それぞれ契約書第 25 条第 2 項及び第 5 項に規定するものをいい、本仕様書 1-17-6 に規定するものは含めないものとする。

#### 1-20. 成果品

成果品の作成及び提出に当たっては、本仕様書3-5に示す事項及び監督員の指示に従って行うものとする。

#### 1-21. 契約不適合責任

##### 1-21-1. 欠陥の調査

受注者は契約書第 41 条に規定する契約不適合責任期間に欠陥が出現した場合において、発注者からその欠陥の原因の調査をすることを指示されたときは、これに従わなければならない。

##### 1-21-2. 欠陥の原因の調査に要する費用の負担

前記 1-21-1 に示す欠陥の原因の調査に要する費用は、契約書第 30 条、第 32 条又は第 39 条の規定に基づき受注者の費用で成果品を修補する場合、受注者が代替物の引渡しをする場合、再履行等をする場合、受注者が損害賠償を負担する場合、受注者が契約金額を減額する場合又は発注者が契約解除した場合を除

き、発注者の負担とする。

## 1-22. 秘密の保持

### 1-22-1. 目的

業務の実施のため、知り得た秘密情報及び個人情報の取扱いに関して、以下のとおり定めるものとする。

### 1-22-2. 定義

秘密保持に関する定義は、下記の各項目の定めるところによる。

- (1) 「秘密情報」とは、業務の実施上知り得た情報で、公知でないものをいう。
- (2) 「個人情報」とは、個人情報の保護に関する法律(平成 15 年 5 月 30 日法律第 57 号、最終改正令和 2 年 6 月 12 日法律第 44 号)第 2 条第 1 項に規定されたものをいう。
- (3) 「秘密情報」及び「個人情報」は文書・図画・電磁的記録等の保存媒体の如何を問わない。

### 1-22-3. 情報管理体制の確保

受注者は、秘密情報及び個人情報の取扱者を必要最小限の人数とした管理体制を監督員が確認するため、「情報取扱者名簿及び情報管理体制図(様式 1-10 及び 1-10-1)」を、契約締結日の翌日から14日以内に監督員に文書にて提出しなければならない。ただし、契約締結日の翌日から14日以内に提出することが困難な場合は、後日速やかに提出するものとする。当該名簿は所属部署や氏名を明示し、情報管理体制図にてその関係を図示すること。明示した内容に変更があった場合は変更内容を速やかに監督員へ通知する。また、受注者は情報管理体制図と情報取扱者名簿の記載内容に矛盾のないようにし、記載していない者に個人情報を開示・漏えいすることのないよう厳重に管理すること。秘密情報においても必要に応じて、この取扱いに準ずるものとする。

### 1-22-4. 情報の明示

発注者及び受注者は、秘密情報及び個人情報を業務遂行のために相手方に提供する場合は、当該情報を特定し、秘密情報又は個人情報であることを明示しなければならない。

### 1-22-5. 目的外の使用

業務の実施のために提供された秘密情報及び個人情報を業務の目的以外に使用してはならない。

### 1-22-6. 取得の制限

受注者は、業務を遂行するに当たり個人情報を取得するときは、あらかじめ、本人に対しその利用目的を明示しなければならない。また、利用目的の達成に必要な範囲内で、適正かつ公正な手段で個人情報を取得しなければならない。

### 1-22-7. 適切な管理

- (1) 業務を遂行するに当たり知り得た秘密情報及び個人情報について、善良なる管理者の注意をもって、漏えい、滅失又は毀損の防止その他の適切な管理に必要な措置を講じるものとする。
- (2) 受注者は、業務に従事している者(以下「従事者」という。)に対し、(1)の措置を遵守させるための必要な措置を講じるものとする。
- (3) 監督員が求めた場合、受注者は、「管理に必要な措置」について定めた文書を発注者に提示するものとする。

### 1-22-8. 利用者の制限

受注者は、業務の実施のために開示又は提供された秘密情報及び個人情報について、業務の実施に必要と認められる従事者以外に開示又は提供してはならない。

#### 1-22-9. 資料の持ち出しの禁止

秘密情報及び個人情報、物的移動（複製物を作成し、複製物を移動させる場合も含む）や磁氣的・電子的・ネットワーク的移動等の方法を問わず、無断で持ち出してはならない。

#### 1-22-10. 複写又は複製の禁止

受注者は、業務を実施するために、発注者から引き渡された秘密情報及び個人情報が記録された資料等を複写、複製又は加工してはならない。ただし、あらかじめ監督員の承諾を受けたときは、この限りではない。

#### 1-22-11. 守秘義務

業務の遂行上知り得た秘密情報及び個人情報を他に開示・漏洩してはならない。ただし、下記の項目に該当するものは、この限りではない。

- (1) この契約への違反によらず公知であるか、又は入手後公知となった情報
- (2) 相手方より受領する以前から当事者が知っていた情報
- (3) 本業務と無関係に、当事者が知っていた情報
- (4) 相手方の書面による同意を事前に得て開示された情報
- (5) 法的手続き、あるいは公認会計士による監査等により当事者が開示を求められる情報

#### 1-22-12. 履行期間完了後の取扱い

業務の履行期間終了後、速やかに、秘密情報及び個人情報が記載又は記録された文書、図画、電磁的記録等の媒体（複写物及び複製物を含む。）を返還するとともに、返還が不可能又は困難な媒体及び受注者の記録装置に複写された電磁氣的記録は、監督員の指示に従って、当該媒体を再生不可能な状態に消去又は廃棄する。

秘密保持に係る規定は、法令の定めにあるものを除き、履行期間終了後もなお、有効とする。

#### 1-22-13. 第三者への委任等について

受注者は、発注者の承諾がない限り、秘密情報又は個人情報の処理に係る本業務の一部を第三者に委任又は請け負わせてはならない。なお、発注者の承諾を得て本業務の一部を第三者に委任又は請け負わせた場合には、受注者は当該第三者に対して、秘密情報及び個人情報に係る秘密保持について、本契約における受注者の義務と同様の義務を負わせるものとする。

#### 1-22-14. 調査及び報告

発注者は受注者に対し、秘密情報及び個人情報の管理状況の調査を目的として、必要な範囲で業務の履行場所に立ち入り、調査を行うことができる。

受注者は、監督員から秘密情報及び個人情報の管理状況について報告を求められたときは、速やかに監督員に必要事項を報告しなければならない。

#### 1-22-15. 事故時の対応

受注者は、秘密情報及び個人情報の不正使用、漏洩、滅失又は毀損その他の事故が発生した場合には、直ちに監督員に報告し、その対応について協議するものとする。なお、監督員は、受注者に対し問題の対処に必要な措置を求めることができる。

#### 1-22-16. 事故時の責任分担

受注者の責に帰すべき事由により、秘密情報及び個人情報の不正使用、漏洩、滅失又は毀損その他の事故が発生し、これにより発注者又は第三者への損害が生じた場合は、受注者は、発注者又は第三者に対し、その損害について賠償の責を負うものとする。

#### 1-23. 紛争中における発注者、受注者の義務

- (1) 受注者は、契約書第 43 条の規定に基づく手続きを行った場合においても、業務を継続しなければならない。
- (2) 前記の場合、契約変更を必要とするときは、発注者及び受注者は発注者が定めた規定に従い、受注者は不服がある旨を明記して契約変更の締結を行うものとする。
- (3) 業務が完了した場合、前記変更契約書に基づき、契約書第 25 条の規定に基づく検査及び契約書第 26 条に基づく代金の支払を行うものとする。

#### 1-24. 関係法令及び条例の遵守

- (1) 受注者は、業務の実施に当たっては、すべての関係諸法令及び条例等を遵守しなければならない。
- (2) 受注者は、仕様書等が関係諸法令及び条例に不相当である場合や、矛盾していることが判明した場合は、直ちに書面にて監督員に報告し、その確認を求めなければならない。

#### 1-25. 著作権の譲渡等

著作権等については、契約書第 5 条及び第 7 条の各項によるもののほか、下記のとおりとする。

- (1) 受注者は、発注者の権利を確保するため、成果品の制作に関連する一切の所有権、著作権(著作者人格権を含む)、著作隣接権、制作関係者の権利等についてのすべての権利処理を自己の責任と負担において行うものとする。
- (2) 受注者は、成果品の制作業務に関わった者(以下「制作関係者」という。)に対して、成果品に関し著作者として著作者人格権を行使しない旨を明示した「制作関係者誓約書(様式第 1-11 号)」に署名させ、発注者に提出しなければならない。
- (3) 成果品中に既存の著作物(以下「既存著作物」という。)が含まれる場合には、受注者は速やかに発注者に申し出るものとし、その権利処理について前項と同様の義務を負うものとする。本項にいう既存著作物に関する「権利処理」とは、以下の事項について権利者の書面による合意を得ることをいう。
  - 1) 成果品に含まれる既存著作物の著作権その他一切の権利は発注者に完全かつ単独に帰属すること。
  - 2) 1)の場合において単独に帰属させることができない場合は、無償で使用許諾を受けること。
  - 3) 既存著作物の著作者は、成果品において既存著作物が使用される限りにおいては、発注者(発注者から著作物使用許諾を受けた者を含む。)に対し著作者人格権を主張しないこと。
- (4) 受注者は、成果品が第三者の知的財産権を侵害していないことを保証する。
- (5) 成果品につき第三者との間で知的財産権に関するクレーム・紛争が生じた場合は、受注者は自己の責任と費用においてこれを解決するものとし、また発注者が被った被害を補償する。
- (6) 受注者は、発注者が成果品の内容を二次使用するときはこれに同意するものとする。



## 2. 業務の概要

### 2-1. 目的

本業務は、発注者の情報システムに対して、高度サイバー攻撃の流れに沿った攻撃者の活動痕跡を調査する「通信調査」と、情報システム内部への侵入可否及び侵入後の被害状況について、攻撃者が実際に行う最新の攻撃手法を用いて客観的に検証する「ペネトレーションテスト」を行い、その結果に基づき、セキュリティ対策上の問題点について評価及び助言等を受け、発注者の情報セキュリティ水準を向上させる目的とし実施する。なお、「ペネトレーションテスト」にはシステムに存在する脆弱性やセキュリティ的な不備を網羅的に検査する「脆弱性診断」を含むものとする。本仕様書中では「通信調査」及び「ペネトレーションテスト」を「調査」又は「テスト」と表記する場合がある。

### 2-2. 履行期間

本業務の履行期間は、契約締結日の翌日から令和8年2月27日までとする。

### 2-3. スケジュール

契約締結後の主な作業スケジュールは次のとおり想定しているが、具体的なスケジュールについては、本仕様書の業務内容を踏まえ、本仕様書1-8に示す業務計画書に含めること。

なお、以下のスケジュールは参考であり、発注者及び受注者を拘束するものではない。

《想定するスケジュール》

	令和7年						令和8年	
	7月	8月	9月	10月	11月	12月	1月	2月
マイルストーン	★キックオフ	★事前説明会					★個別調査結果の説明	★報告会
通信調査	<div>ログ採取※</div>		<div>調査</div>				<div>問合せ期間</div>	
	<div>事前準備</div>							
ペネトレーションテスト	<div>事前準備</div>		<div>テスト</div>					

※ログ採取については、発注者の作業工程とする。

## 2-4. 履行場所

ペネトレーションテストの履行は、以下の場所にて実施するものとする。なお、作業場所の詳細については、契約締結後に発注者より連絡するものとする。

作業場所	住所
東日本高速道路株式会社 本社	東京都千代田区霞が関3-3-2 新霞が関ビルディング

## 2-5. 業務の実施概要

### (1) 通信調査の対象と方法

#### ① 調査対象ログ

通信調査の調査対象は発注者が指定するログ(表2-1)を調査対象とし、それぞれ1週間分(約1300GB相当)の調査・解析を実施する。なお、発注者は対象機器及びサービスの情報等、詳細について、契約締結後に提示するものとし、契約締結前の提示は行わない。

表2-1 通信調査対象ログ

ログファイル		収集量(想定)
1	メールサーバログ	約1GB
2	プロキシログ(Antivirus ログを含む)	約480GB
3	DNS サーバログ	約50GB
4	Firewall ログ	約75GB
5	認証サーバログ	約690GB
合計		約1300GB

#### ② 調査の手法

受注者は、高度サイバー攻撃におけるキルチェーンモデル(表2-2、表2-3)を参考に、発注者が指定した各種ログに対して、攻撃段階毎に該当する痕跡及び活動の疑いについて通信調査を実施すること。なお、分析を通じてセキュリティインシデントを発見した場合には、速やかに監督員に報告を行うものとする。また、監督員からの求めに応じ、対策について助言及び支援を行うものとする。

表2-2 サイバーキルチェーンモデル

攻撃段階		説明
1	偵察	インターネットなどから組織や人物を調査し、対象組織に関する情報を取得する
2	武器化	エクスプロイトやマルウェアを作成する
3	配送	なりすましメール(マルウェアを添付)を送付するためのなりすましメール

		(マルウェア設置サイトに誘導)を送付し、ユーザにクリックするように誘導する
4	攻撃	マルウェア添付ファイルを実行させるユーザをマルウェア設置サイトに誘導し、脆弱性を使用したエクスプロイトコードを実行させる
5	インストール	エクスプロイトやマルウェアの侵入の成功により、標的がマルウェアに感染する
6	遠隔制御	マルウェアと C&C サーバを通信させて、感染 PC を遠隔操作する新たなマルウェアやツールのダウンロード等により、感染拡大や内部情報の探索を試みる
7	目的達成	探し出した内部情報について、改ざん・破壊、加工(圧縮や暗号化等)した後の情報の持ち出し等を実行

表2-3 攻撃段階と取得対象ログの関係

攻撃段階		メールサーバログ	Firewall ログ	プロキシログ	認証サーバログ	DNS サーバログ
1	偵察	-	-	-	-	-
2	武器化	-	-	-	-	-
3	配送	○	-	○	-	○
4	攻撃	-	○	○	-	○
5	インストール	-	-	-	-	-
6	遠隔制御	-	○	○	○	○
7	目的達成	○	○	○	-	○

## (2) ペネトレーションテストの対象と方法

### ① テスト対象システム

発注者が運用するIP通信が可能な情報システムのうち、約 120IPをテスト対象 IP とする。対象の詳細については、契約締結後に別途発注者より指示する。なお、ここで言うIPとは、テスト対象とする情報システムの各種サーバ、端末、通信回線装置等(以下「ホスト」という。)に付与され、テストを実施する対象として選定したものとする。また、テスト対象は全て発注者の社内ネットワーク内に存在しており、グローバルネットワークに公開されているものは含まない。

### ② テストの種類、手法、形式

ペネトレーションテストの種類は内部ペネトレーションテストとし、手法はブラックボックステスト、テスト形式はシナリオ型とする。表2-4に従ってテストの実施内容を取り纏め、本仕様書3-1(1)に基づき作成する個別業務計画書に含めること。なお、シナリオについては契約書第14条に基づき変更する場合

がある。

表2-4 テストシナリオ概要

項目	
1	システム情報、脆弱性情報等の収集 <ul style="list-style-type: none"><li>● ネットワーク情報の収集</li><li>● システム情報の収集</li><li>● 脆弱性情報の収集</li><li>● ユーザ情報の収集</li></ul>
2	対象ホストへの侵入可否の調査・分析 <ul style="list-style-type: none"><li>● OS、ミドルウェアに内在する脆弱性の調査</li><li>● 認証サービスの稼働状況の調査</li><li>● ユーザ情報の調査</li><li>● プロダクト固有のデフォルトユーザ情報の調査</li></ul>
3	侵入可能な攻撃の実行 <ul style="list-style-type: none"><li>● ユーザID、パスワードを使用したログイン試行</li><li>● OS、ミドルウェアの脆弱性を利用したコマンドの実行</li><li>● OS、ミドルウェアの脆弱性を利用した情報の窃取</li></ul>
4	侵入後の活動 <ul style="list-style-type: none"><li>● 一般ユーザから管理者への権限昇格の実行</li><li>● システム内部の情報収集</li><li>● 侵入に成功したホストと同様の手法で他ホストへの侵入</li><li>● 侵入に成功したホストを踏み台にした他ホストへの侵入</li></ul>

### ③ 攻撃手法について

テストにおいて使用する攻撃手法が、稼働中のサービスに支障を与える可能性がある場合、その影響を取りまとめたうえで事前に提出し、監督員の承認が得られた場合のみ実施すること。

攻撃手法はテスト対象とするホストに対し、侵入を達成できる可能性のある攻撃手法をすべて実施すること。ただし、攻撃手法が膨大にあるなど、実施期間内にすべての攻撃手法を実施することが困難であると想定される場合には、監督員との協議の上、実施する攻撃手法数を調整することができるものとする。

なお、調整により実施しないこととなった攻撃手法のうち、脆弱性が確認されたものについては、個別調査結果報告書に脆弱性に関する情報として記載すること。

## 3. 業務細部

### 3-1. 通信調査

#### (1) 個別業務計画書の作成

受注者は、以下の事項を含めた個別業務計画書を作成すること。

- ① 採取対象ログの詳細(取得元、ファイル名等)と採取予定日※
- ② 調査スケジュール
- ③ 調査ログ毎の調査と解析対象
- ④ 調査ログ毎の調査方針と調査観点
- ⑤ 調査結果報告書に記載予定となる報告内容の一覧

※ログ採取は発注者が実施するため、監督員と調整、確認すること

#### (2) 調査の実施

受注者は、通信調査の実施にあたり、表3-1の各項目に従って調査を実施すること。なお、調査に際し本仕様書2-5(1)①に示す調査対象ログの他、関連するログファイルの採取が必要となった場合は、採取の必要性等において監督員と協議し、適宜、監督員からログの提供を受け、調査を継続するものとする。

表3-1 攻撃段階毎の調査内容

攻撃段階		調査内容	調査対象ログ
1	偵察	-	-
2	武器化	-	-
3	配送	攻撃者によるマルウェア添付メールの送信	メールサーバログ
		攻撃者によるマルウェア設置サイトへの誘導メールの送信と誘導	メールサーバログ プロキシログ DNS サーバログ
4	攻撃	コールバック(Web プロキシサーバを介さない外部への通信)	Firewall ログ DNS サーバログ
		コールバック(HTTP, HTTPS 等のプロトコルによる外部への通信)	プロキシログ DNS サーバログ
5	インストール	-	-
6	遠隔制御	コールバック(Web プロキシサーバを介さない外部への通信)	Firewall ログ DNS サーバログ
		コールバック(HTTP, HTTPS 等のプロトコルによる外部への通信)	プロキシログ DNS サーバログ

		ファイルサーバなどへのアクセスや権限の奪取	認証サーバログ
7	目的達成	コールバック(Web プロキシサーバを介さない外部への通信)	Firewall ログ DNS サーバログ
		コールバック(HTTP, HTTPS 等のプロトコルによる外部への通信)	プロキシログ DNS サーバログ

### 3-2. ペネトレーションテスト

受注者は、ペネトレーションテストの実施に当たっては、以下の各項目に従うものとする。

#### (1) 事前説明会及びヒアリングの実施

- ① 受注者は、監督員と協議の上、事前説明会及びヒアリングの時期について調整すること。
- ② 事前説明会は原則として1回開催すること。
- ③ 事前説明会では、テスト及びその調査にかかる日程、内容、依頼事項、実施における注意点等について説明すること。
- ④ 事前説明会実施後、テスト対象システム毎にペネトレーションテストで必要な情報を収集するためのヒアリングを行うこと。
- ⑤ ヒアリング時は、受注者のこれまでの経験や知見を活用し効果的なペネトレーションテストが実施できるよう、必要な資料の閲覧(例えば、ネットワーク構成図等)や確認、助言等を行うこと。
- ⑥ 受注者は、テスト対象システム側で必要となる事前準備・確認事項(例えば、データのバックアップの取得や、通信監視を委託している業者をはじめとする関係先への連絡、テスト及びその調査実施時においてサービス障害等が発生した場合の技術的な対応、必要に応じた復旧支援体制等)について、テスト対象システム担当者及び監督員へ説明すること。
- ⑦ 事前説明会及びヒアリング終了後、3営業日を目途に業務打合簿を作成し提出すること。
- ⑧ 事前ヒアリング及びヒアリングは仕様書 2-4 に定める場所にて実施すること。

#### (2) 個別業務計画書の作成

- ① 受注者は、テスト対象システム毎に、以下の事項を含めた個別業務計画書を作成すること。
  - (ア) ペネトレーションテストの概要
  - (イ) ペネトレーションテストの実施方法(攻撃方法、使用するツール等の内容を含む。)
  - (ウ) テストシナリオ
  - (エ) ペネトレーションテスト期間中の作業スケジュール
  - (オ) 業務体制、システム管理者およびテスト対象システムのテストに従事する担当者の役割、所属、氏名の一覧表
  - (カ) ペネトレーションテスト実施中に不測の事態が発生した際の連絡、対応体制
- ② ペネトレーションテストの実施経路(外部からの攻撃を想定したインターネット経由からの攻撃など)及

びテスト実施中に留意すべき事項(例えば帯域の圧迫やシステムへの負荷)を取り纏め、個別業務計画書に含めること。

- ③ 個別業務計画書については、テスト対象システム担当者と協議の上で作成し、調査実施までに監督員の承認を得ること。承認が得られなかった場合は、個別業務計画書の問題点について意見聴取した上で再作成し再協議すること。
- ④ テストシナリオを作成する上で、事前に調査対象ホストへのポートスキャン等が必要な場合は、対象ホスト、実施方法、実施希望日についてテスト対象システムの担当者と協議のうえ、事前に監督員の承認を得ること。

### (3) 診断の実施

受注者は、ペネトレーションテストの実施に当たっては、表3-2の診断内容を含むものとし、承認が得られた個別業務計画書及び以下①～⑦の事項に基づきペネトレーションテストを実施すること。

表3-2 ペネトレーションテストの診断内容

項目		診断内容
1	TCP スキャン	詳細な TCP スキャンを行い、診断対象ホスト上で動作しているサービスを検出する。各サービスのプロトコルに応じてアクセスを行い、情報収集を行う。スキャンの実施対象はオープンポートおよび提供サービスを確認の上決定するものとし、well-known ポートに代表的なポートを加えた範囲とする。
2	UDP スキャン	TCP スキャンと同様 UDP スキャンを行い、システム情報の抽出を実施する。また、各サービスのプロトコルに応じた手順でアクセスし情報収集を行う。スキャンの実施対象はオープンポートおよび提供サービスを確認の上決定するものとし、well-known ポートに代表的なポートを加えた範囲とする。
3	セキュリティホールチェック	最新のセキュリティパッチが適用されているか、OS や Web サーバなどが適切に設定されているかを調査し、既知のセキュリティホールへの対策が適切に行われているか診断する。
4	アプリケーションバナーのチェック	OS や Web サーバなどの製品名・バージョンが外部から取得でき、それらが攻撃に悪用される危険性がないか診断する。

5	認証試行	推測可能なアカウントや、簡易的なユーザ・パスワードによる認証試行を行い、OS、アプリケーションや、管理コンソール等の利用可否を検出する。  実施対象は OS、FTP、Telnet、SSH、HTTP、SMB、DNS、各種 Database、ネットワーク機器・サーバ機器等の管理コンソールとする。
6	アクセス権限奪取	サービスやアプリケーションの設定不備や仕様上の脆弱性を検出し、ホストへの侵入や機微な情報の入手、情報システムの不正利用を試みる。
7	既知の脆弱性に対する攻撃	既知の脆弱性及びバグに対する影響確認を試行する。実施対象は OS、DNS、AD、各種 Database、LDAP とする。
8	中間者攻撃	診断用端末から対象ホストやネットワーク機器に対し、通信内容を傍受する為の特殊なフレームを送信し、受信可能となったデータを確認し侵入につながる内容の存在有無確認を実施する。
9	侵入後の攻撃	侵入したホスト上のアカウント情報や設定情報を取得・解析し、他のホストに対する影響確認を実施する。また、ホストを踏み台とし直接には到達不可能なネットワークやデータベースへの侵入を試行する。

- ① テスト実施期間の各日の作業開始時及び作業終了時には、テスト対象システム担当者及び監督員へ連絡すること。また、各日の作業終了後、作業進捗報告書(実施した作業内容及び調査対象ホストがわかるもの)を作成し、テスト対象システム担当者及び監督員に提出すること。
- ② 脆弱性等を利用して攻撃するためのツール等を利用する場合は、当該ツール等を利用することによる影響の有無等含め、対象システム担当者に説明し承諾を得ること。
- ③ 検出した問題を利用して侵入できた場合、監督員及びテスト対象システム担当者に対して、その旨を速やかに連絡すること。その後、監督員またはテスト対象システム担当者から情報提供依頼や状況の再現を求められた場合は協力すること。
- ④ 作業中は、テスト対象システムを含む発注者が運用するシステム及びサービスを停止させたり、又は阻害したりしていないか常に状況を確認すること。
- ⑤ テスト対象システムを含む発注者が運用しているシステム及びサービスを停止させ、又は阻害した場合は、直ちに作業を中止し、監督員及びテスト対象システム担当者へ連絡すること。また、サービス復旧の際に協力を求められた場合には、監督員及びテスト対象システム担当者監督員の指示に従うこと。なお、中止した調査の再開にあたっては、テスト対象システム担当者と再会に伴う影響も



含め、十分に調整し、サービスへの影響が生じない対策を講じること。

- ⑥ テスト対象システム担当者からの指示及び問い合わせに速やかに対応できる体制を整備すること。
- ⑦ テスト対象システムがクラウド上で稼働するシステムである場合、発注者が契約する各クラウドサービスのペネトレーションテスト実施における注意事項及び制約事項等を十分理解した上で実施すること。

### 3-3. 実施結果の分析及び評価

受注者は、通信調査及びペネトレーションテストの実施結果に関して、以下の通り報告書に取り纏めテスト対象システム担当者及び監督員へ説明すること。

#### (1) 個別調査結果報告書の作成

##### ① 記載内容

受注者は、通信調査及びペネトレーションテストの結果からセキュリティ対策の実施状況の分析・評価を行い、その結果について以下の項目を含めた個別調査結果報告書を作成すること。また、IPアドレス等の機密情報をマスクしたバージョンも作成すること。

(ア) 個別調査結果報告書の内容は、図表やイメージ等を用いるなど、テスト対象システム担当者が理解し、調査の再現が可能となるよう読みやすさについて工夫すること。また、テスト対象システム担当者がセキュリティ対策水準の向上に努められるよう、必要に応じて受注者の知見、助言等を適宜追加すること。

##### i. 調査・テストの内容

- 調査・テストで用いた実施手順、実施観点
- 調査・テスト対象システムについて調査を実施した範囲

##### ii. 調査・テストの実施結果

- 検出した問題の内容及び危険度(深刻度のレベル)の一覧  
診断により発見された脆弱性については、表3-3の例を参考に、報告レベルを定義(3～4レベル程度)すること。

表3-3 報告レベルの参考

レベル	判断指標	CVSS(※)
高	緊急性が高く、早急に対策が必要。	7.0～10.0
中	間接的に攻撃に利用される可能性があり複数組み合わせることで実害へと発展する問題点。	4.0～6.9
低	直接的な被害に発展する可能性は低い、対策することで潜在的なリスクを回避可能な問題点。	0.1～3.9
参考	脆弱性という程のレベルではないものの、セキュリティ上好ましくないと考えられる事項。	0.0

(※)CVSS…共通脆弱性評価システム (Common Vulnerability Scoring System)

検出した問題を再現する方法(ペネトレーションテストに限る)

- 検出した問題に対して推奨する具体的な対策方法  
(なお、根本的な対策方法が、期間もしくはコスト等の面から早期の実施が現実的に困難と想定される場合は、暫定対応策についても併せて示すこと)

iii. 調査・テスト結果全体の評価

- 全体的な調査・テスト結果のまとめ、総論

iv. 問い合わせ窓口

- 質問対応連絡先(メールアドレス、電話番号)

(イ) ペネトレーションテストにおいて、侵入できた問題については、問題点の重要性の認識が容易となるよう危険度のレベルを用いて説明すること。また、侵入できた問題点については侵入が成功するまでの攻撃の流れが把握できるように、利用した脆弱性や設定の不備も含めて記載すること。

② 報告期限

受注者は、通信調査及びペネトレーションテストの終了後、それぞれ、おおむね3週間以内に個別結果報告書を作成し報告すること。なお、個別調査結果報告書は業務完了時に成果品として納入すること。

(2) 個別調査結果の説明

受注者は、監督員及びテスト対象システム担当者と調整のうえ、個別調査結果報告書について説明すること。また、質疑応答を含む業務打合簿を作成し、説明会終了後1週間以内を目途に報告すること。なお、業務打合簿は業務完了時に成果品として納入すること。なお、個別調査結果の説明後、当該内容及びその後に実施する報告会にかかる問い合わせ対応を行うこと。

(3) 全体調査結果報告書の作成

受注者は、次の事項を含む全体調査結果報告書を作成し報告すること。なお、全体調査結果報告書は業務完了時に成果品として納入すること。

① 記載内容

(ア) 個別結果報告書を取り纏めたもの

(イ) 通信調査及びペネトレーションテスト結果の全体を俯瞰し、国内外のサイバー攻撃の動向等を考慮したうえで、発注者のセキュリティ水準を向上させるための助言や改善案

(ウ) 今後の通信調査及びペネトレーションテストを実施するにあたっての助言やあり方についての提言

(エ) 総評

② 提出期限

受注者は、個別結果報告書の提出からおおむね1週間以内に、全体調査結果報告書を作成し報告すること。なお、全体調査結果報告書は業務完了時に成果品として納入すること。

#### (4) 報告会の開催

受注者は、全体調査結果報告書の提出後、速やかに調査結果の報告会を開催すること。また、報告会前に報告内容について、監督員と協議すること。さらに、質疑応答を含む業務打合簿を作成し、報告会終了後1週間以内を目途に提出すること。

### 3-4. その他

#### (1) 進捗管理

受注者は、作業の実施に当たり、監督員と密に連絡を取るとともに、進捗管理表を作成すること。また、1か月に1回以上の頻度で情報を集約し、作業の進捗状況について報告を行うこと。なお、本業務の実施に当たって、疑義が生じた場合は、速やかに監督員と協議すること。

#### (2) 問い合わせ等への対応

受注者は、本業務に係る監督員及びテスト対象システム担当者からの問い合わせについて、速やかに対応すること。なお、問い合わせ内容のうち協議が必要である場合は、速やかに監督員と協議すること。

#### (3) 業務実施に当たっての留意事項

受注者は、本業務の実施に当たっては、内閣官房内閣サイバーセキュリティセンター「政府機関等の情報セキュリティ対策のための統一基準群(令和5年度版)」及び不正アクセス行為の禁止等に関する法律を把握した上で実施すること。

### 3-5. 成果品の作成

受注者は、本業務の成果品として以下を取りまとめ、納入の少なくとも7日前までに監督員へ提示したうえで、電磁記録媒体(DVD-R)を2部作製するものとする。なお、DVDメディアは受注者が用意するものとする。

受注者は、本業務の成果品である電磁記録媒体(DVD-R)をあらかじめウィルスチェック等の実施により、マルウェア等の感染対策を実施しなければならない。また、ウィルスチェックに使用した製品及びバージョンについて、DVDの盤面等に記録すること。なお、チェックに使用する製品の指定はない。

表3-4 成果品一式

成果品名		形式
1	打合簿	PDF 形式、A4サイズとする
2	計画書	PDF 形式、A4サイズとする
3	報告書	PDF 形式、A4サイズとする

## 提出書類の様式

様式第 1-1(1)号	履行責任者届
様式第 1-1(2)号	作業責任者届
様式第 1-2(1)号	契約金額内訳明細書
様式第 1-2(2)号	契約金額内訳明細書
様式第 1-3 号	再委任等承諾願
様式第 1-4 号	業務等打合簿
様式第 1-5 号	業務等指示簿
様式第 1-6 号	同意書
様式第 1-7 号	履行期間延長協議書
様式第 1-8 号	(一部)完了届
様式第 1-9 号	受渡書
様式第 1-10 号	情報取扱者名簿及び情報管理体制図の提出について
様式第 1-11 号	制作関係者誓約書

※提出書類の様式は、すべてA4 サイズとする。

様式第 1-1(1)号

令和 年 月 日

東日本高速道路株式会社

代表取締役社長 ○○ ○○ 殿

住 所

会社名

代表者

履 行 責 任 者 届

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、下記の者を履行責任者としますので、当人の経歴書を添えてお届けします。

記

職名

氏名

(注) 経歴書には当人の生年月日、現住所、最終学歴、取得資格、職歴、本業務に関する経歴等を記載すること。

様式第 1-1(2)号

令和 年 月 日

東日本高速道路株式会社

代表取締役社長 ○○ ○○ 殿

住 所

会社名

代表者

作 業 責 任 者 届

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、下記の者を作業責任者としますので、当人の経歴書を添えてお届けします。

記

職名

氏名

(注) 経歴書には当人の生年月日、現住所、最終学歴、取得資格、職歴、本業務に関する経歴等を記載すること。

様式第 1-2(1)号

令和 年 月 日

東日本高速道路株式会社

代表取締役社長 ○○ ○○ 殿

住 所

会社名

代表者

契約金額(変更)内訳明細書(第○回)

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、別添契約金額(変更)内訳明細書を提出します。

以 上





令和 年 月 日

東日本高速道路株式会社  
代表取締役社長 ○○ ○○ 殿

住 所  
会社名  
代表者

再 委 任 等 承 諾 願

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、下記のとおり再委任等に付したいので、承諾願います。

記

1. 再委任等に付する内容
2. 期 間
3. 金 額
4. 再委任等する必要性及び再委任等予定者を選定した理由
5. 再委任等者に関する事項
  - (1)住 所
  - (2)商 号 また は 名 称
  - (3)代 表 者 名
  - (4)東日本高速道路株式会社
- 取引停止措置の有無 有 ・ 無
6. 再委任等に係る履行体制に関する書面
7. 添 付 書 類
- 再委任等者との契約書等の案

業務等打合簿

[illegible]

(注1)電子メールによる伝達とする。

(注2)電子メールの場合、受領者は受領日を記載したうえで、発議者に電子メールで返送のうえ、保管するものとする。

(注3)内容欄には、下記事項毎に整理して記載すること。

当社側：請求、通知、協議、回答、承諾

受注者側：請求、報告、申出、質問、協議、提出

(注4) 打合簿作成者側の受領表示は、取消し線により削除すること。

業務等指示簿

(件名) 令和7年度 情報セキュリティリスク診断業務

指示年月日 令和 年 月 日

No. \_\_\_\_\_

<p style="text-align: center;">監督員</p> <p>指示者 ○○ ○○</p>	
<p>下記のとおり指示する。</p>	
<p>なお、本件は別途変更契約を締結する。</p>	
<p>(指示内容)</p>	
<p>令和 年 月 日</p> <p>上記の指示書を受領しました。</p>	<p style="text-align: right;">履行責任者 ○○ ○○</p>

(注1)電子メールによる伝達とする。

(注2)電子メールの場合、受理者は受領日を記載したうえで、発議者に電子メールで返送のうえ、保管するものとする。

(注3)変更契約の記載について、該当しない場合は取り消し線により削除すること。

様式第 1-6 号

令和 年 月 日

監督員

\_\_\_\_\_  
殿

会社名

履行責任者

〇 〇※ 同 意 書

(件名) 令和7年度 情報セキュリティリスク診断業務

令和 年 月 日付けで協議のありました〇〇※については、同意します。

※協議のあった内容を記載すること。

令和 年 月 日

東日本高速道路株式会社

代表取締役社長 ○○ ○○ 殿

住 所

会社名

代表者

履行期間延長協議書

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、契約書16条の規定に基づき下記のとおり履行期間の延長を協議いたします。

記

1. 当初履行期間      令和 年 月 日から  
                         令和 年 月 日まで      (当初履行日数      日間)
2. 変更履行期間      令和 年 月 日から  
                         令和 年 月 日まで      (変更履行日数      日間)  
                         (延長日数      日)
3. 延長理由

以 上

(注)変更工程表を添付すること

様式第 1-8 号

令和 年 月 日

東日本高速道路株式会社

代表取締役社長 ○○ ○○ 殿

住 所  
会社名  
代表者

(一 部) 完 了 届

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、業務を(一部)完了しましたので、届け出ます。

以 上

様式第 1-9 号

令和 年 月 日

東日本高速道路株式会社

代表取締役社長 ○○ ○○ 殿

住 所

会社名

代表者

受 渡 書

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、(一部)完了検査に合格しましたので、引渡します。

以 上

様式 1-10

令和 年 月 日

東日本高速道路株式会社

(部署名)

監督員 ○○ ○○

(受注者名)

履行責任者 ○○ ○○

情報取扱者名簿及び情報管理体制図の提出について

(件名) 令和7年度 情報セキュリティリスク診断業務

標記について、別添のとおり提出します。

【添付書類】

様式第 1-10-1 号 情報取扱者名簿及び情報管理体制図

以 上



情報取扱者名簿及び情報管理体制図

(件名) 令和7年度 情報セキュリティリスク診断業務

1. 情報取扱者名簿

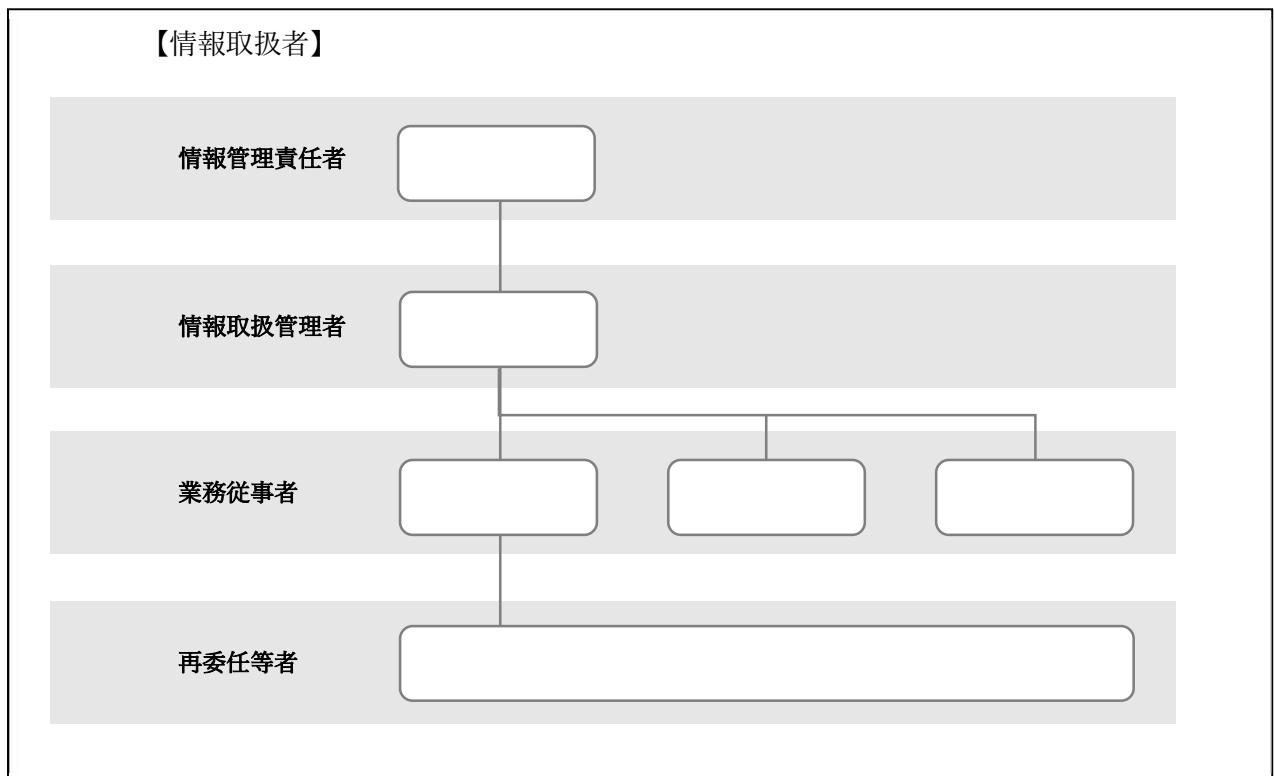
	氏名	所属部署	役職
情報管理責任者※1			
情報取扱管理者※2			
業務従事者※3			
業務従事者※3			
業務従事者※3			
再委任等者※3			

※1 本業務における情報の取り扱いについて、すべての責任を有する者

※2 本業務の進捗状況等の管理を行う者であり、本業務で知り得た保護すべき情報を取り扱う可能性のある者

※3 本業務で知り得た保護すべき情報を取り扱う可能性のある者

2. 情報管理体制図



## 制作関係者誓約書

私、●●(以下「制作関係者」という。)は、令和 年 月 日に東日本高速道路株式会社(以下「発注者」という。)及び○○(受注者)との間で締結された令和7年度 情報セキュリティリスク診断業務に係る「役務契約書」に基づき、○○に関する制作業務に従事していました。

私は、本成果品にかかわる下記の権利が発注者に帰属することを了解し、同意します。私は、ここに、本成果品にかかわることにより生じる著作権(翻訳・翻案権、二次的著作物の利用に関する原著作者の権利を除き、著作隣接権、貸借権、ロイヤリティ請求権を含む。)を発注者に無償譲渡します。

私が、本成果品に関し、著作者としての権利を有するとみなされる場合には、本書において、公表権を行使せず、発注者(発注者から著作物使用許諾を受けた者を含む。以下同じ。)の裁量により本成果品を公表する権利を認めます。私は、発注者に対して本成果品の著作者としての氏名表示権及び同一性保持権を行使しません。私は、成果品に関し、発注者が商標登録出願することを了解し、同意します。

私は自己の実績を表す等非営利的な使用を除き、本成果品を不正に開示又は使用しないことに同意します。

令和 年 月 日

制作関係者: ○ ○ ○ ○ 印

肩書き

住所