

情報システムの受注者における情報セキュリティ対策基準

令和6年8月2日 最高情報セキュリティ責任者裁定

(趣旨)

奈良先端科学技術大学院大学(以下、「本学」という。)の情報システムの開発、運用等を委託された受注者が、情報システムのセキュリティを維持するために必要となる対策を定めるものである。

(委託事業実施前の情報セキュリティ対策)

1. 受注者は、委託元となる本学情報システム担当者(以下、「本学担当者」という。)に対し、以下の情報セキュリティ対策を明示すること。また、変更があった場合は速やかに本学担当者に報告すること。
 - ① 本学担当者より提供された情報の目的外利用の禁止
 - ② 受注者における情報セキュリティ対策の実施内容及び管理体制
 - ③ 受注者における情報セキュリティインシデントへの対処方法
 - ④ 受注者における情報セキュリティ対策の履行状況の確認方法
 - ⑤ 受注者における情報セキュリティ対策の履行が不十分な場合の対処方法
 - ⑥ 委託事業の実施に当たり、受注者又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制
 - ⑦ 受注者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報
 - ⑧ 本学担当者との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順
2. 受注者において以下の情報セキュリティに係るサプライチェーン・リスクを低減する対策が行われていること。
 - ① 各工程において信頼できる品質保証体制が確立されていること。
 - ② 不正な変更が発見された場合に、本学担当者と受注者が連携して原因を調査・排除できる体制を整備していること。
 - ③ 機器等に不正がないことを担保することができる事業者が製造した機器等を用いてシステム構築等を行うこと。
3. 受注者がその役務内容を第三者に再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、再委託先の第1条の情報と共に第2条の実施状況を本学担当者に明示し、了承を得ること。また、再委託した業務に伴う再委託者の行為について、全ての責任を

負うこと。

（委託事業実施時の情報セキュリティ対策）

4. 本学が実施する情報セキュリティ対策について、本学担当者の指示に従い協力すること。
5. 本学ネットワークへ接続する場合等、本学の情報資源を使用する際は、本学が定める「ゲストユーザ向け奈良先端科学技術大学院大学 IT リソース利用に関するガイドライン」を遵守すること。
6. 受注者における情報セキュリティ対策の履行状況を確認すること。
7. 本学情報システムに対し本学の意図しない変更が行われた場合や、情報の目的外利用が認知された場合等の情報セキュリティインシデントが発生した際は、受注者は速やかに本学担当者に連絡し、本学担当者の指示に基づき委託事業を一時中断するなどの必要な緊急措置を講じた上で、契約に基づく必要な措置を講じること。また、本学CSIRT（サイバーセキュリティインシデント対応チーム）からの調査依頼に協力すること。

（委託事業における情報の取扱い）

8. 本学担当者等から提供された情報において、以下の事項を遵守すること。
 - ① 提供される情報は必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。
 - ② 提供された情報が受注者において不要になった場合は、これを確実に返却又は抹消し、本学担当者の確認を得ること。
 - ③ 提供された情報において情報セキュリティインシデントの発生を認知した場合は、速やかに本学担当者に報告すること。

（委託事業終了時の情報セキュリティ対策）

9. 委託事業終了時において、以下の事項を遵守すること。
 - ① 本学から提供された情報を本学担当者の指定した方法で処理し、本学担当者的了承を得ること。
 - ② 委託事業用に作成したアカウントやパスワード、各種設定等を含むシステム情報と、生成された情報を確実に返却又は抹消し、本学担当者的了承を得ること。