国立研究開発法人建築研究所情報セキュリティポリシー

令和５年１月20日
規 程 第 １ ８ 号

情報セキュリティ基本方針

当所における情報セキュリティに対する基本的な考え方を以下のとおり定める。

1.　リスク評価と対策

（１）　自組織の目的等を踏まえ、7. に定める自己点検の結果、8.に定める監査の結果、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）に基づきサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講じる。

（２）　前項の評価に変化が生じた場合には、情報セキュリティ対策を見直す。

2.　管理体制

（１）　情報セキュリティ対策を実施するための組織・体制を整備する。

（２）　最高情報セキュリティ責任者１人を置く。

（３）　本ポリシー等情報セキュリティ対策の重要事項の審議を行う組織は、建築研究所情報セキュリティ委員会とする。

（４）　最高情報セキュリティ責任者は、本ポリシーにて規定した当所における情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。

（５）　最高情報セキュリティ責任者は、自らの所掌する事務を本ポリシーに定める責任者に分掌させることができる。

3.　対策推進計画

（１）　情報セキュリティ委員会は、1.の評価の結果を踏まえた情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定める。

（２）　対策推進計画に基づき情報セキュリティ対策を実施する。

（３）　情報セキュリティ委員会は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行う。

4.　例外措置

（１）　本ポリシーに定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を定める。

5.　教育

（１）　役職員等が、自覚をもって本ポリシーに定めた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行う。

6.　情報セキュリティインシデントへの対応

（1）　情報セキュリティインシデントに対処するため、適正な体制を構築するとともに、必要な措置を定め、実施する。

（2）　情報セキュリティインシデントの可能性を認知した者は、本ポリシーに定める報告窓口に報告する。

（3）　本ポリシーに定める責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じる。

7.　自己点検

（1）　情報セキュリティ対策の自己点検を行う。

8.　監査

（1）　対策基準が統一基準等に準拠し、かつ実際の運用が対策基準に準拠していることを確認するため、情報セキュリティ監査を行う。

9.　情報の格付

（1）　取り扱う情報に、機密性、完全性及び可用性の観点に区別して、分類した格付を付す。

（2）　他機関との情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するかを明示等する。

10.　情報の取扱制限

（1）　情報の格付に応じた取扱制限を定める。

（2）　取り扱う情報に、前項で定めた取扱制限を付す。

（3）　他機関との情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等する。

11. 情報のライフサイクル管理

（1）　情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取扱いが損なわれることがないように、必要な措置を定め、実施する。

12. 情報を取り扱う区域

（1）　当所の管理下にある施設等において、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施する。

13. 外部委託

（1）　統一基準に準拠

14. 情報システムに係る文書及び台帳整備

（1）　所管する情報システムに係る文書及び台帳を整備する。

15. 情報システムのライフサイクル全般にわたる情報セキュリティの確保

（1）　所管する情報システムの企画、調達・構築、運用・保守、更改・廃棄及び見直しの各段階において情報セキュリティを確保するための措置を定め、実施する。

16. 情報システムの運用継続計画

（1）　所管する情報システムに係る運用継続のための計画（以下「情報システムの運用継続計画」という。）を整備する際には、非常時における情報セキュリティ対策についても、勘案する。

（2）　情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認する。

17. 暗号・電子署名

（1）　暗号及び電子署名の利用について、必要な措置を定め、実施する。

18. インターネット等を用いたサービスの提供

（1）　インターネット等を用いてサービスを提供する際には、利用者端末の情報セキュリティ水準の低下を招く行為を防止するために、必要な措置を定め、実施する。

19. 情報システムの利用

（1）　情報システムの利用に際して、情報セキュリティを確保するために役職員等が行わなければならない必要な措置を定め、実施させる。

20. サプライチェーン・リスク対応

（1）　サプライチェーン攻撃など巧妙化が加速するサイバー攻撃の脅威から当所の情報資産を守るための情報セキュリティ対策について、必要な措置を定め、実施する。