C3104 情報システム運用リスク評価手順

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年10月31日  A3105 | 新規作成 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3104 | 情報システムの実態に合わなくなった箇所の修正 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |
| 2016年2月5日  C3104 | 添付１における項目の例示内容を更新 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

情報資産の管理者が行うリスク評価は、次に掲げる方法によるものとする。

1. 情報資産の洗い出し

　「リスク分析票」(添付１)の中項目ごとに関係する情報資産をすべて洗い出す。例えば、「6.6.1 コンピュータの取外し可能な付属媒体」の場合、USB媒体、メモリカード、CD/DVD/BD、磁気テープ等、保有するすべての可搬媒体が該当する。これら情報資産を一つのセルに一つずつ記入する[[1]](#footnote-1)。

1. 脆弱性分析

　「リスク分析票」(添付１)の安全対策項目と現状を比較し、脆弱性を数値で記入する。このとき、必要に応じ技術担当者の意見を取り入れ、現状を正確に把握する。脆弱性をあらわす数値は以下のとおりである。なお、未実施または即実施のものについては現在の状況を備考欄にメモしておくとよい。

|  |  |  |
| --- | --- | --- |
| 数値 | 意味 | 判断基準 |
| １ | 実施済み | 関連のドキュメントが整理され、それに則った運用がなされている。 |
| ２ | 一部実施 | 関連のドキュメントが不足しているか、または運用が正確に行われていない。 |
| ３ | 未実施 | ドキュメントもなく、運用もされていない。 |

1. 資産価値判断

　上記で洗い出した情報資産を機密性 (C)、完全性(I)、可用性(A)の観点で情報資産をリスク判断し、数値を記入する。判断基準は、これらの性格が損なわれたときに、その業務継続性に与える影響度から判断する。

* 機密性(C)

３：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が著しく下がる。その結果、利用者や社会、本学情報システムの継続性など広範囲に影響が出る。

２：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が下がる。その結果、利用者や社会、本学情報システムの継続性など一部に影響が出る。

１：情報資産に対し、基準となる安全性が確保されなかった場合、秘密性が下がる危険性が低い。また、利用者や社会、本学情報システムの継続性などに影響は出ない。

* 完全性(I)

３：情報資産に対し、基準となる安全性が確保されなかった場合、その情報の正確性または業務処理の正確な運用ができなくなる。その結果、利用者や社会、本学情報システムの継続性など広範囲に影響が出る。

２：情報資産に対し、基準となる安全性が確保されなかった場合、その情報の正確性または業務処理の正確な運用ができなくなる。その結果、利用者や社会、本学情報システムの継続性など一部に影響が出る。

１：情報資産に対し、基準となる安全性が確保されなくても、その情報の正確性または業務処理は継続可能である。その結果、利用者や社会または本学情報システム運用など、どの面にも影響が少ない。

* 可用性(A)

３：情報資産に対し、基準となる安全性が確保されなかった場合、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスできなくなり、利用者や社会または本学情報システム運用など、広範囲に影響がある。

２：情報資産に対し、基準となる安全性が確保されなかった場合、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスできなくなり、利用者や社会または本学情報システム運用などの一部に影響がある。

１：情報資産に対し、基準となる安全性が確保されなくても、利用すべき立場にある者が、必要なときに、情報及び関連する資産にアクセスでき、利用者や社会または本学情報システム運用など、どの面にも影響が少ない。

1. 脅威の判断

　上記(2)で洗い出した情報資産について、脅威を判断する。脅威の判断は、CIAが損なわれる頻度によって判断する。

* 機密性(C)

３：機密性が失われる危険が常にある。

２：機密性が失われる危険が週に一度程度ある。

１：機密性が失われる危険が年に一度程度ある。

* 完全性(I)

３：情報の正確性や円滑な運用が失われる危険が常にある。

２：情報の正確性や円滑な運用が失われる危険が週に一度程度ある。

１：情報の正確性や円滑な運用が失われる危険が年に一度程度ある。

* 可用性(A)

３：利用すべき立場にあるものが、利用不可能に陥る危険が常にある。

２：利用すべき立場にあるものが、利用不可能に陥る危険が週に一度程度ある。

１：利用すべき立場にあるものが、利用不可能に陥る危険が年に一度程度ある。

1. リスク値の算出

　脆弱性と資産価値と脅威の値を足しリスク値を算出する。

1. 対策の必要性判断

　上記5.の結果、リスク値が４以上のものについて、対策を実施する。対策を実施しないものについては、その理由を明確にし、全学総括責任者の承認を受ける。

添付１　リスク分析票（例）

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 大項目 | 中項目 | 安全対策項目 | 情報資産 | 脆弱性 | 資産価値 | | 脅威 | リスク値 | 備考 |
| Ｎｏ |
| 6.7 媒体の取扱い | | |  |  |  |  |  |  |  |
|  | 6.7.1 取外し可能な媒体の管理のための手順を備える | | |  |  |  |  |  |  |
| 6.7.1.1 |  | 不要となることで組織の管理外となる媒体が再利用可能なものであるときは、格納している内容を回復不能とすること |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |
|  |  |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |
| 6.7.1.2 |  | 組織の管理外とする媒体のすべてについて、認可を要求すること |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |
|  |  |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |
| 6.7.1.3 |  | 媒体を組織の管理外とする措置のすべてについて、監査証跡の維持のために記録を保管すること |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |
|  |  |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |
| 6.7.1.4 |  | すべての媒体を、製造者の仕様に従って、安全でセキュリティが保たれた環境に保管すること |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |
|  |  |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | A |  |  |  |
| 6.7.1.5 |  | 情報を媒体の寿命（製造者の仕様に従う。）よりも長く保管することが必要な場合、媒体の劣化による情報の消失を避けるために、その媒体に保管された情報を他の媒体に記録・保管すること |  |  | C |  |  |  |  |
|  |  | I |  |  |  |
|  |  | Ａ |  |  |  |
|  |  |  |  | Ｃ |  |  |  |  |
|  |  | Ｉ |  |  |  |
|  |  | Ａ |  |  |  |

1. リスク分析票の安全対策項目は次を参照されたい。http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS\_Audit\_Annex01\_2.xls [↑](#footnote-ref-1)