D3106 情報セキュリティ非常時行動計画に関する解説書

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  A2103 | 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 |
| 2013年7月5日  B2103 | 文書番号の変更のみ | － |
| 2015年10月9日  C2102 | 文書番号の変更のみ | － |
| 2016年2月5日  C2102 | 第一条の解説においてCSIRTに関する説明を追加 | 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 |
| 2021年3月25日  D3106 | 情報セキュリティ事象単独の非常時行動計画を策定することが想定されにくい実態を踏まえ、解説書の位置づけに変更するとともに、それに合わせた構成の見直しを実施 | 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。

1. 情報セキュリティインシデントに係る非常時行動計画の考え方

　非常時行動計画は、組織や事業に関わるインシデントのうち特に緊急性を要する事態が発生した場合の対応を定めるものである。本学における事業の継続に重大な支障をきたす可能性が想定される大規模な火災や地震その他の災害等の事態を特定し、当該事態への対応計画は、A大学業務継続計画（BCP：Business Continuity Plan）として策定されており、情報セキュリティに係る非常時行動計画についても、BCPの一部として統合して扱われることが望ましい。

　本書では、災害等による情報システムの大規模な物理的損壊、大規模障害、大規模セキュリティインシデント（マルウェア等による本学情報ネットワークの輻輳や停止）、及び重大な社会的影響や法的問題に発展する可能性のある本学関係者による情報発信や、本学に対する情報発信による事件・事故（コンテンツインシデント）に関してBCPに反映すべき内容について説明する。

　非常時行動計画とインシデント対応手順との扱う内容の線引きについては様々な整理の仕方が考えられる。一方、すべてのインシデントには一定の緊急性が認められるともいえるので、両者を一体化しても良いかもしれない。ただし、CSIRT（情報セキュリティインシデント対応チーム）が設置されている組織であっても、非常時対策本部は非常事態ごとに臨時に設置されるものであり、両者は区別して扱う必要がある。本サンプル例では、非常時連絡窓口の設置、非常時対策本部の設置などまでを非常時行動計画に書き、物理的インシデント、セキュリティインシデント、コンテンツインシデントそれぞれに対応する具体的緊急処置は「インシデント対応手順」にて示している。

　なお本書では、非常時対策本部設置後は、通常のインシデントの通報連絡体制がピラミッド構造だったとしても、それとは異なったフラットな連絡体制をとり、情報の集約と共有を一元化し、非常時対策本部による緊急な判断や行動を実現することを想定している。

2. 非常時行動計画において定めるべき内容

　(1)～(6)に示す内容をBCPにおいて情報セキュリティインシデントに係る非常時行動計画として定めることが望ましい。

(1) 非常事態の特定

　インシデントについての報告または通報を学内または学外から受けつけ、迅速に情報を集約する手段を全学実施責任者が整備し、学内に周知するとともに対外公表する。

　全学実施責任者が報告または通報を受けたインシデントのうち、非常事態の発生またはそのおそれがあると判断した場合には、全学総括責任者へ報告し、非常時対策本部の設置を提案する。

(2) 非常時対策本部の設置と体制

　非常時対策本部は、非常事態が発生しまたは発生するおそれが特に高いと認められる場合に、被害の拡大防止、被害からの早急な復旧その他非常事態の対策等を実施することを目的として、全学総括責任者によって設置される。全学総括責任者が非常時対策本部の本部長として全権をもち、関係者の間の緊急連絡網、情報共有体制を構築して、情報収集、証拠保全をした上で、対策を実施する。

　非常時対策本部は次の各号に定める委員をもって構成する。

一　全学総括責任者

二　全学実施責任者

三　関連する部局情報システムの部局総括責任者

このほか全学総括責任者が必要と認めたときは、委員以外の者を出席させて意見を聞くことができる。

(3) 非常時連絡窓口の設置と役割

　非常時対策本部には、緊急連絡及び情報共有等を行うために全学実施責任者が担当する非常時連絡窓口を設置し、関係者に周知徹底する。非常時連絡窓口は非常時対策本部長の指示に基づき、次の各号に定める役割を担う。

一　通報者や捜査当局、クレームの相手方、報道関係者等、外部との対応（連絡の受付と回答。場合によりヘルプラインの役割も含む）を直接または広報窓口を通じて行う。必要に応じて法律専門家とも相談する。

二　学内関係者からの情報の受付および収集、被害拡大防止や復旧のための緊急対策等の伝達を直接行う。必要に応じて全学情報システムについてCSIRT、情報メディアセンターや総務部と、部局情報システムについて部局技術責任者（及び同担当者）と連携する。

(4) 非常時連絡網の整備

　全学実施責任者は、非常時連絡窓口を中心とする非常時連絡網を整備する。非常時連絡網の連絡先には、非常時対策本部委員の他、全学情報システムについては情報メディアセンター、総務部、部局情報システムについては部局技術責任者及び部局技術担当者、必要に応じて法律専門家、広報部門を設定する。

(5) インシデント対応

　具体的なインシデント対応は、別途定める「インシデント対応手順」に基づき対処するが、非常事態においては非常時対策本部の指示がインシデント対応手順に優先する。

(6) 非常時対策本部の解散と再発防止策の検討

　全学総括責任者は、非常事態への対応が終了した場合、非常時対策本部から全学情報システム運用委員会への報告書の提出をもって、非常時対策本部を解散する。

　また全学総括責任者は、報告書をもとに再発防止策の実施を図る。