C2102 情報システム非常時行動計画に関する規程

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 |

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。

C2102-01（目的）

第一条 この規程は、Ａ大学情報システムの運用において非常事態が発生した場合の行動を非常時行動計画として事前に定め、早期発見・早期対応により、事件・事故の影響を最小限に抑え、早急な情報システムの復旧と再発防止に努めるために必要な措置を講じることを定めることを目的とする。

解説：非常時行動計画は、情報システム運用に関す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。本学の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、業務継続計画（BCP：Business Continuity Plan）として策定されるべきであるが、BCPが策定されている場合には、本計画はBCPの一部として統合されるべきである。  
BCPが未整備である場合を想定し、本計画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（ワーム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）に関する部分を扱う。  
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「C3102 インシデント対応手順」にて示している。

C2102-02（定義）

第二条 この規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　運用基本方針　本学が定めるＡ大学情報システム運用基本方針をいう。

二　運用基本規程　本学が定めるＡ大学情報システム運用基本規程をいう。

三　非常事態　本学情報システムの運用に関するインシデントのうち特に緊急性を要するものをいう。

四　その他の用語の定義は、運用基本方針及び運用基本規程で定めるところによる。

C2102-03（非常事態の報告）

第三条　全学実施責任者は、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整備し、周知・公表する。

２　全学実施責任者は、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。

C2102-04（非常時対策本部）

第四条　全学総括責任者は、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ために非常時対策本部を設置する。

２　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

３　全学総括責任者は、非常時対策本部の本部長となる。

４　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。

解説：非常時対策本部は、全学総括責任者が設置し、全学総括責任者、全学実施責任者、関連する部局情報システムの部局総括責任者で構成する。全学総括責任者が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。

C2102-05（非常時連絡網）

第五条　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。

２　非常時連絡窓口は、非常時対策本部長の指示に基づき、通報者や捜査当局、クレームの相手方、報道関係者等、外部との対応を直接または広報窓口を通じて行う。

３　非常時連絡窓口は、非常時対策本部長の指示に基づき、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。

４　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。

５　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。

解説：連絡窓口は、全学実施責任者が担当し、通報者や捜査当局、弁護士、報道等の内外からの連絡の受付と回答（あるいはヘルプラインの役割も）を行う。連絡窓口は、全学情報システムについて情報メディアセンター（設置されている場合はCSIRT）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）と連携し、法律専門家とも相談する。  
本計画では、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。

C2102-06（インシデント対応手順）

第六条　具体的なインシデント対応は、別途定める「C3102 インシデント対応手順」に基づき対処する。

２　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。

C2102-07（再発防止策の検討）

第七条　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。

２ 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。