C1101 情報セキュリティインシデント対応チーム（CSIRT）運営規程

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 |
| 2015年10月9日  C1101 | 新規作成 | 上原哲太郎（立命館大学） |
| 2016年2月5日  C1101 | PoCに関する記述を一部修正 | 上原哲太郎（立命館大学） |
| 2017年10月17日  C1101 | CSIRT及びその構成員の役割の明確化及び他規程等との整合確保のための修正 | 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 |

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。

解説：　A大学においては、CSIRTは全学CSIRTのみが単独で設置されている。大学の事情によっては、拠点や部局単位で複数のCSIRTを設置するほうが適切な場合も想定される。例えば附属大学病院が、教育・研究系部局とは高い独立性を有する形で運用され、情報セキュリティ対策に関しても独立した体制にて実施されている場合に、附属大学病院向けに別のCSIRTを設置・運用することが考えられる。また、学外へのインターネット接続を拠点ごとに行っているような場合も、接続単位でCSIRTを設置するほうが効率的なこともある。一方で、学内で複数のCSIRTを階層的に組織すると緊急時にCSIRT間での相互連絡等が必要となるため、全学統括責任者等への報告により多くの手間や時間を要するなどの弊害もあり、大学の事情に応じて最適な体制を検討することが望ましい。また、CSIRTの運用を少人数で行わざるを得ない場合、夜間や長期休暇中にCSIRTが十分に機能しない可能性があり、こうした状況において情報セキュリティインシデントが発生したときの扱いについても定めておく必要がある（A大学では外部委託にて対応している）。

１．設置

1. 全学統括責任者は、情報セキュリティインシデント対応チーム（以下「CSIRT」という。）の活動が円滑に行えるよう、予算措置や適切な権限委譲を含めた環境を整えるとともに、必要に応じて活動内容について助言または指導を行うものとする。
2. 部局統括責任者は情報セキュリティインシデントの発生に備え、CSIRTと連携して、連絡、報告、情報集約および被害拡大防止のための緊急対応に必要な体制を整える。

２．組織

解説：　A大学CSIRTは、監視機能を外部SOCに委託している。また、情報ネットワークに関する実務については、メディアセンタースタッフがCSIRT構成員を支援することを想定している。また、(4)の対象者は学内教職員に限定されず、学外の専門家等をあてることも可能である。

1. CSIRTは、情報セキュリティインシデント対応チーム責任者（以下、「CSIRT責任者」という。）及び担当者で組織する。
2. CSIRT責任者は、CSIRTの業務を統括するとともに、学内外の関係機関と、必要に応じて情報セキュリティインシデントに関する情報共有に関する活動の責任者を務め、全学総括責任者が指名する。
3. 担当者は、各部局総括責任者が本学教職員から1名以上を推薦し、全学総括責任者が委嘱する。このとき、自部局の教職員を推薦することを原則とするが、教職員の所属部局の部局総括責任者及びCSIRT責任者の承認のもとで、他部局の教職員を推薦することも認める。
4. CSIRT責任者は、必要があると認めるときは、全学統括責任者の承認を得た上で、(3)に掲げた以外の者を指名して担当者に加えることができる。
5. CSIRT責任者はCSIRTの構成員の中から1名以上の情報セキュリティインシデント対応チーム副責任者（以下、「CSIRT副責任者」という。）を指名する。CSIRT副責任者はCSIRT責任者から委譲を受けた場合にCSIRT責任者の業務を代行することができる。

３．活動

解説：　A大学CSIRTでは、夜間・休日における情報セキュリティインシデント及びその他の連絡の受付と初動対応を、民間サービスに外部委託している。

　担当者は、次に掲げる活動を行うものとする。このうち活動の一部について、CSIRT責任者は予め全学統括責任者の承認を得た上で、外部委託を行うことができる。

1. 本学における情報セキュリティインシデントの報告窓口として、学内からの情報セキュリティインシデントの可能性のある事象に関する情報を受け付けるとともに、本学情報ネットワークの監視に関する情報も活用することにより、情報セキュリティインシデントに関する事象を正確に把握すること。

解説：　学内利用者（教職員、学生等）に情報セキュリティインシデントであることを判断した上で報告させることは、判断誤りによる報告漏れにつながるため、その可能性を認知した段階で報告を求める必要がある。ただしこうした可能性を含めると端末やアプリケーションの不具合や混雑による応答低下なども含めた膨大な報告を受け付けざるを得なくなり、CSIRTにおける対応負荷も増えるため、ウェブによる報告記入画面を設けたり、トラブル相談窓口を別に設けたりするなどにより、CSIRTの機能を持続的に維持できるような仕組みを検討することが必要である。

1. 情報セキュリティインシデントに関する外部機関との連絡窓口（PoC：Point of Contact）機能を、本学の総務部門や広報部門と連携して提供すること。

解説：　この場合の外部機関としては、監視業務を委託している外部SOCや他大学CSIRT等が該当する。なお、情報セキュリティインシデントが発生した際に文部科学省への報告を行うのは、CSIRTではなく本学総務部門である。

1. 情報セキュリティインシデントの発生時に、必要に応じて被害の拡大防止、復旧及び再発の防止にかかる技術的支援や助言を行うこと。
2. 情報セキュリティインシデントの発生時に、予め全学統括責任者による承認を得た条件を満たす場合には、CSIRT責任者による判断に従って本学情報ネットワークの緊急遮断措置を行うこと。これ以外の権限については、必要な場合はあらかじめ全学統括責任者から委譲を受けた措置について、全学統括責任者の承認を都度受けることなく行うことができる。

解説：　CSIRTが本学情報ネットワークを緊急遮断する権限は、情報セキュリティインシデント対応に関する責任を全うするために必要な手段として全学統括責任者からCSIRTにあらかじめ与えられており、遮断を行う場合に全学統括責任者等に許可を求める必要はない。なお、情報セキュリティインシデントが解消した場合の本学情報ネットワークの復元については、CSIRTには部局情報システムやネットワークに問題がないことを確認する権限がないことから、CSIRTが復元の可否を判断することはできず、各部局が自らの責任のもとで行うこととしている。

　　　　なお、A大学では遮断に際してCSIRT責任者（CSIRT副責任者による代行を含む）が実施を判断することを前提としているが、これが不適切と考えられる場合は、各担当者に対応の優先順位を設定し、情報セキュリティインシデント発生時に対応可能な最上位の担当者が判断を行うことと定めてもよい。

1. 学内の情報セキュリティインシデントの発生状況を定期的に取りまとめ、全学統括責任者に報告するとともに、対策に関する意思決定を支援すること。
2. 情報セキュリティインシデントへの対処能力を向上させるため、必要に応じてCSIRT構成員を対象とする研修や訓練などを実施すること。

４．雑則

　この規程に定めるほか、CSIRTの運営に関して必要な事項は、別に定める。

解説：　A大学におけるCSIRTによるインシデント対応等の具体的な運用手順については、「C3102 インシデント対応手順」にて規定しているので、あわせて参照のこと。

　　附　則

この規程は、平成XX年X月X日から施行する。