D2103 情報セキュリティインシデント対応チーム（CSIRT）設置規程

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 |
| 2021年3月25日  D2103 | 統一基準の改定内容を踏まえ、CSIRTの設置と役割を規定する内容に修正 | 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：CSIRTの運用に関する遵守事項は、「D1001 情報セキュリティ対策基本規程」第十八条で規定されており、本規程はCSIRTの役割明確化ならびに体制に関する具体的な遵守事項を定めるものである。  
A大学においては、CSIRTは全学CSIRT（A大学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、全学総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。  
なお、A大学CSIRTは、監視機能を外部SOCに委託している。また、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。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。

D2103-01　（目的）

第一条　本規程は、Ａ大学（以下、「本学」という。）における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。）の設置に必要な事項を定め、本学に関わる情報セキュリティインシデントへの適切な対応のための体制の構築を行うことを目的とする。

解説：本文書では、「D1001 情報セキュリティ対策基本規程」の遵守事項を「政府機関等の情報セキュリティ対策のための統一基準群」に極力一致させる観点から、同規程第十八条で役割を明確化することを求められている内容について別文書として規定しているが、D1001の第十八条に相当する内容を本規程に移行し、CSIRTの構築及び運用に関する遵守事項を本規程でまとめて扱うことでも問題ない。

D2103-02　（適用範囲）

第二条　本規程は、Ａ大学CSIRT（以下「本学CSIRT」という。）を対象とする。

D2103-03　（用語）

第三条　本規程で用いる用語は、「D1001 情報セキュリティ対策基本規程」第三条に定めるところによる。

D2103-04　（本学CSIRTの設置）

第四条　全学総括責任者は、本学CSIRT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備すること。

２　部局総括責任者は、本学CSIRTと連携して、情報セキュリティインシデントの発生に備えた連絡、報告、情報集約及び被害拡大防止のための緊急対応に必要な体制を整備すること。

解説：情報セキュリティインシデントへの対応にあたっては、CSIRTのみでなく、インシデント関連部局（インシデントの原因となったり、被害が生じたりしている機器やユーザーの在籍部局等）の部局技術責任者を中心とする担当者の協力が必要になる場合が多い。CSIRT責任者は、あらかじめ各部局総括責任者に対し、第２項に定めるような連絡、報告、情報集約及び被害拡大防止のための緊急対応に必要な体制整備に関して、CSIRTへの協力の義務を負う旨を周知しておくべきである。

D2103-05　（本学CSIRTの役割）

第四条　全学実施責任者は、情報セキュリティインシデントに備えた体制における本学CSIRTの役割として、次に示す各項を含む業務内容を規定すること。

一　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の正確な把握に努める。

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。

二　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。

三　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。

解説：各号のほか、必要に応じて学内情報ネットワークの緊急遮断措置（もしくはその支援）を役割として規定することで、CSIRTの権限を明確化することも考えられる。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が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ことは一般に困難であるため、各部局が自らの責任のもとで行うことが想定される。

D2103-06　（CSIRT業務の外部委託）

第六条　全学実施責任者は、本学CSIRTの業務の一部を外部委託する場合は、調達にあたりD2101（情報セキュリティ対策基準）第60条及び第61条に加えて、次に示す事項が本学の要求水準を上回ることを確実にすること。

一　定期報告の頻度と報告内容

二　夜間及び休日におけるサービス内容

三　インシデント発生時の初動対応として実施する内容

解説：民間事業者が提供するセキュリティ監視・運用サービスのうち、一定の品質が確保されていることを審査機関にて確認したものを掲載したリストが、独立行政法人情報処理推進機構（IPA）より公表されている。委託先の選定に際しては、当該リストに掲載されているサービスであることを要件とすることも考えられる。  
「情報セキュリティサービス基準適合サービスリスト」（IPA）  
https://www.ipa.go.jp/security/it-service/service\_list.html

２　CSIRT責任者は、外部委託先からの報告内容を本学CSIRT内で共有すること。

解説：外部委託を行う場合、委託先に「丸投げ」状態になり、CSIRT要員が実態を把握できていない状況が生じがちである。インシデント発生時に慌てて委託先に照会するようなことのないよう、定常的な共有の仕組みを運用しておくことが望ましい。