人間文化研究機構
情報セキュリティインシデント対応チーム設置要項

平成29年3月13日

（令和元年7月22日改定）

人間文化研究機構

1．設置

人間文化研究機構情報セキュリティポリシーに基づき、情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため、人間文化研究機構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。）を設置する。

2．CSIRT の役割

CSIRT の役割は次のとおりとする。

（1）インシデント発生時の対応

ア）検知・連絡受付

インシデントの発生に関する予兆等の検知、発見、内部外部からのインシデントに関わる連絡・報告等の受付を行う。

イ）トリアージ

事実関係を確認の上、インシデントが発生したかどうかを検査・分析により判断し、被害状況や影響範囲等事態の全体像を把握した上で、インシデントの処理に優先順位を付ける。

ウ）インシデントレスポンス

初動対応（対応方針の検討、証拠の取得・保全・確保・記録、インシデントの封じ込め・根絶）の実施、復旧措置（暫定対策）の実施及び再発防止策（恒久対策）の検討を行う。

エ）報告

インシデントの発生について、速やかに情報セキュリティ責任者に報告する。情報セキュリティ責任者は、CSIRT から報告を受けた後、速やかに最高情報セキュリティ責任者（CISO）に報告する。

オ）事後対応

インシデントの収束後、報告書をまとめる。

（2）平常時の事前準備・予防等

ア）インシデント発生時の対応に必要な事前準備・予防

イ）その他 CSIRT 責任者が定めるもの

3．PoC

インシデントについて人間文化研究機構外の者からの連絡受付の役割を担う、情報セキュリティに関する統一的な窓口となる担当者 PoC（Point of Contact、ポック）を別に定め、機構外に周知、公表するものとする。

4. 対象インシデント

CSIRT が扱うインシデントは、本部及び機関が定めるインシデント対応に係る手順で定義するものとし、機構全体で共通するインシデントは次のものとする。

物理的インシデント	・地震等の天災、火災、事故等による物理的損壊 ・ネットワーク等の機能不全や障害等
セキュリティインシデント	・大量のスパムメールの送信 ・コンピュータウイルスの蔓延や意図的な頒布 ・不正アクセス行為の禁止等に関する法律に定められた特定電子計算機のアクセス制御を免れる行為 ・サービス不能攻撃、その他情報システム管理責任者の要請に基づかずに、管理権限のない情報システムのセキュリティ上の脆弱性を検知する行為 ・禁止された方法による外部からの接続 ・ネットワークへの侵入を許すようなアカウントを格納したPCの盗難・紛失
コンテンツインシデント	・電子掲示板、ブログやウェブサイト等での名誉・信用毀損にあたる情報の発信 ・他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信 ・通信の秘密を侵害する行為 ・他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信 ・秘密であるデータやプログラムの不正公開等守秘義務に違反する情報の発信 ・児童ポルノやわいせつ画像の公開 ・差別、侮辱、ハラスメントにあたる情報の発信

5. CSIRT 体制

CSIRT の体制は次のとおりとする。

(1)CSIRT は、本部及び機関に設置する。

(2)CSIRT に CSIRT 責任者を置き、情報セキュリティ責任者をもって充てる。

(3)CSIRT の構成は、CSIRT 副責任者、CSIRT 管理者、インシデントハンドラー、CSIRT 要員、外部委託事業者、外部の専門家等とし、本部及び機関の情報システム等の状況に応じて、改編することができる。CSIRT 責任者等の役割は CSIRT 構成表(別表)のとおりとする。

(4)外部委託事業者、外部の専門家等については、必要に応じ CSIRT 責任者が関係機関に依頼、要請等して定めるものとする。

6. CSIRT 連絡会の設置

（1）本部及び各機関に設置する CSIRT のインシデント対応水準の向上やインシデントを防止するため、最高情報セキュリティ責任者の下に、CSIRT 連絡会（NIHU CSIRT Liaison Group）を置く。

（2）CSIRT 連絡会の役割

ア）インシデント発生時における他機関 CSIRT への情報共有

イ）インシデント発生機関 CSIRT への情報提供及び助言

（当該情報提供及び助言を適用するか否かはインシデント発生機関 CSIRT の責に帰す）

ウ）インシデント発生に向けた事前準備

エ）インシデント再発防止策等の共有

オ）必要に応じて、国立大学法人・他大学共同利用機関法人等、関係機関との連携

（3） CSIRT 連絡会は、最高情報セキュリティ責任者が招集し、定期及び臨時に開催する。

別表　CSIRT 構成

構成		役割	設置の要否
CSIRT 責任者	情報セキュリティ責任者をもって充てる。	インシデント対応の責任者。インシデント対応の作業を監督し評価する責任を負う。また、CISO や本部その他の組織などとの調整役となり、危機を打開し、チームに必要な要員・リソース・技能を確保する。	必須
CSIRT 副責任者	情報システム管理責任者をもって充てる。	CSIRT 責任者が不在の場合に権限を引き継ぐ。	必須
CSIRT 管理者	情報システム管理責任者をもって充てる。	チームのリーダー。インシデントハンドラーの作業を調整し、インシデントハンドラーからの情報を収集し、インシデントに関する最新情報を必要な関係者に提供する。また、高い技術的な技能とインシデント対応経験を持ち、インシデント対応チーム全体の技術的な作業品質を監督して、その品質に最終的な責任を持つ。	必須（CSIRT 副責任者を兼ねることができる）
インシデントハンドラー	統括システム管理者若しくはシステム管理者をもって充てる。	インシデント発生時の、インシデント分析及び対処法の検討、関係部署との調整を行う等、インシデントに対応する CSIRT を、実務的な観点から中核として支え、対応方針を検討し、インシデントハンドリング全体に係るプロジェクトマネジメント等を行う。	必須
CSIRT 要員	システム管理者の中から CSIRT 責任者が指名する者	インシデントハンドラーを補助し、ともにインシデントハンドリングに当たる	必須（インシデントハンドラーを兼ねることができる）
外部委託事業者	システムベンダー（開発事業者、運用・保守事業者等）、ISP、ASP、クラウド事業者等契約関係のある外部の事業者に対し CSIRT 責任者が支援を依頼する者	検査・分析、証拠の取得・保全・確保・記録、インシデントの封じ込めと根絶、復旧措置、再発防止策の検討等に係る一部作業	任意

内部関係者	財政部門	インシデントハンドリングにおける予算対応等	任意
	法務部門	インシデントハンドリングにおける法的対応（契約を含む）等	必須
	広報部門	インシデントハンドリングにおけるマスコミ対応等	必須
外部の専門家	セキュリティベンダー、NISC、IPA、JPCERT／CC、警察等から CSIRT 責任者が支援を要請する者	検査・分析、証拠の取得・保全・確保・記録、インシデントの封じ込めと根絶、復旧措置、再発防止策の検討等に係る作業	任意
その他上記のほか CSIRT 責任者が支援を要請等する者		左記にて要請等された内容	任意

人間文化研究機構CSIRT体系図