# 京都大学情報システムログ管理ガイドライン

（平成２９年４月１日 情報環境機構長裁定）

## １　目的

1　本ガイドラインは、京都大学情報セキュリティ対策基準（以下「対策基準」という。）第８５条、第８６条及び第８９条並びに京都大学全学情報システム利用規則（以下「利用規則」という。）第２３条に基づき、情報システムから取得した証跡及び採取した利用記録並びに情報システムで発生するイベントの記録（以下「ログ」と総称する。）の取り扱いについて、部局情報セキュリティ技術責任者及び部局情報システム技術担当者が遵守すべき事項を明確にすることを目的とする。

2　ログ管理は次の各号に掲げることを目的とする。

⑴ 情報セキュリティ上での不正な通信及び活動の検出・監視のため

⑵ 情報システムの障害など異常検出、異常プロセスの特定及び状態監視のため

⑶ 情報システムに発生したトラブルの事後の原因究明及び調査のため

⑷ 情報システムの利用統計(報告も含む)及び利用状況分析のため

⑸ 情報システムにて発生した事象の証明のため

3　本ガイドラインでは、対策基準第８９条第２項ただし書きについては扱わない。

## ２　定義

本ガイドラインにおいて、次の各号に掲げる用語は、京都大学の情報セキュリティに関する規程（以下「規程」という。）、対策基準及び利用規則に定めるもののほか、次の各号の定めるところによる。

⑴ イベント　情報システム又はネットワーク内で発生する事象をいう。

⑵ ログ管理　ログ取得又は採取（以下「収集」という。）、保管、利用及び廃棄といったログのライフサイクル管理をいう。

⑶ ログの保管　標準的な運用活動の一環として定期的にログをアーカイブすることをいう。

## ３　対象機器とログ種別

1　本ガイドラインは、次の各号の情報システムを対象とする。

⑴ 全学情報システム

⑵ 特定部局情報システム

2　部局情報システム技術担当者は、ログ収集にあたり、次のログ種別と第１第２項に示す目的を明確にしなければならない。

⑴ セキュリティソフトウェアログ

マルウェア対策、侵入検知、リモートアクセス、Web プロキシ、脆弱性管理、認証、ルータ、ファイアウォール、ネットワーク検疫など

⑵ オペレーティングシステムログ
　システムイベント、監査記録など
⑶ アプリケーションログ
　クライアント要求とサーバ応答、アカウント情報、使用状況の情報、重要な運用上でのイベントなど

４　体制

1　全学情報システム及び特定部局情報システムについて、部局情報システム技術担当者は、第１条第２項の各号に掲げる目的に則ったログ管理を行う。

2　部局情報セキュリティ技術責任者は、部局情報システム技術担当者に対して、ログ管理に係る監査や改善の指示行うことができる。

５　ログ収集と保管

1　部局情報システム技術担当者は、ログ収集を行うにあたり、次の各号に掲げる事項を実施しなければならない。

⑴ ログ収集については、管理する当該情報システムの機能、あるいは連携した情報システムで行うこと。

⑵ 収集したログは、最低限９０日間、当該情報システムの機能、あるいは連携した情報システムで保管しなければならない。また、システムバックアップの際、ログも含めること。

⑶ ログ収集について、当該情報システムの運用手順書に、ログ種別、利用目的、保管期間及び保管場所などをあらかじめ記載しておくこと。

⑷ 情報システムの容量制限など、技術的な理由でログの保管ができない場合は、部局情報セキュリティ技術責任者に報告し、その承認を得なければならない。

2　部局情報システム技術担当者が、重要度などに配意し、９０日以上の保管が必要と判断したログについては、保管期間、その保管方法及び保管場所を部局情報セキュリティ技術責任者に申告し、保管期間の延長を行うことができる。

3　部局情報セキュリティ技術責任者は、各部局の情報システムについて、システム名、ログ種別、利用目的、保管期間及び保管場所などを記載した管理簿を作成し、部局情報セキュリティ責任者に報告しなければならない。

4　部局情報セキュリティ責任者又は部局情報セキュリティ技術責任者は、対策基準第８７条及び第８９条第７項に示されるログ収集に関する利用者への周知については、第３項で示される管理簿に記載された項目のうち、システム名、ログ種別、利用目的を利用者に公開することで実施してもよい。

６　収集したログの利用

1　収集したログについて、部局情報システム技術担当者は、第１第２項に示す目的の範

囲において利用することができるほか、次の各号に掲げる事項を遵守しなければならない。

⑴収集したログを分析し、利用統計及び利用促進施策の一環として公表する場合、部局情報システム技術担当者は、個人の特定ができないように匿名化処理を施さなければならない。

⑵規程第２条第６号に示されるインシデント及び京都大学情報資産利用のためのルール第７に示される被疑行為に対する調査（以下「インシデント等調査」という。」の際に必要となるログについて、当該の部局情報システム技術担当者は、部局情報セキュリティ技術責任者へ収集したログを伝達しなければならない。

⑶ 部局情報セキュリティ技術責任者は、インシデント等調査に関し、最高情報セキュリティ責任者又は情報ネットワーク危機管理委員会もしくは情報ネットワーク倫理委員会の求めに応じて、部局情報セキュリティ責任者の指示の下、ログをこれらの要求元に伝達しなければならない。

⑷ 部局情報セキュリティ技術責任者は、学外の機関等（個人及び法的機関を含む。以下同じ。）からインシデント等調査に関するログの照会があった際には、部局情報セキュリティ責任者の指示の下、京都大学情報セキュリティインシデント対応手順に従って対応するものとする。

⑸ 情報システム障害及び障害などが予見される事象の際に必要となるログについて、部局情報システム技術担当者は、部局情報セキュリティ技術責任者へ収集したログを伝達しなければならない。

⑹ 部局情報システム技術担当者は、第１第２項第１号から第３号に示す目的の範囲において、当該情報システムの管理を委託する業者に対し、ログを伝達することができる。

2　部局情報セキュリティ責任者、部局情報セキュリティ技術責任者及び部局情報システム技術担当者は、第１項の場合を除き、ログを第三者に伝達してはならない。

7　収集したログの保護

1　部局情報システム技術担当者は、情報システムから収集したログの機密性、完全性及び可用性が損なわれないよう保護しなければならない。

2　部局情報システム技術担当者は、収集したログ及び保管したログの保護にあたっては、アクセス制限、物理的セキュリティ対策あるいは暗号化処理などを設定しなければならない。

3　部局情報セキュリティ技術責任者は、最高情報セキュリティ責任者又は情報ネットワーク危機管理委員会もしくは情報ネットワーク倫理委員会により、又は学外の機関等からの正当な手続きにより、インシデント等調査に関するログを保護するよう依頼があった際には、部局情報セキュリティ責任者指示の下、京都大学情報セキュリティインシデント対応手順に従い、適切に当該ログを保護しなければならない。この場合、保護

するよう依頼した者に対し、保護を要する期間を明確にするよう求めるものとする。

4　部局情報セキュリティ技術責任者は、ログの保護状態を監査でき、必要と認めれば改善勧告ができる。

８　収集したログの廃棄

1　部局情報システム技術担当者は、情報システムから収集したログの保管期間が満了し、かつ保管期間を延長する必要性がない場合は、速やかにこれを廃棄するものとする。

2　部局情報セキュリティ技術責任者は、前条第３項の保護するよう依頼のあったインシデント等調査に関するログについて、指定された保護を要する期間が満了し、かつ保護期間を延長する依頼がない場合には、速やかにこれを廃棄するものとする。

3　部局情報セキュリティ技術責任者は、ログの廃棄状態を監査でき、必要と認めれば改善の指示ができる。

９　雑則

本ガイドラインに定めるもののほか、ログ管理に関し必要な事項は情報環境機構長が定める。

附 則

本ガイドラインは、平成２９年４月１日から施行する。