施行　2003 年 11 月 1 日
改定　2007 年 10 月 31 日

基幹ネットワーク管理に関するガイドライン

このガイドラインは、中京大学キャンパスネットワークの運用に関し必要な事項のうち、基幹ネットワークの管理に必要な事項を定めるものとする。

１．対象

以下を基幹ネットワークとし、本ガイドラインの対象とする。

(1)「chukyo-u.ac.jp」ドメインのネットワーク
　(外部接続ネットワーク、キャンパス間接続ネットワークを含む)
(2)レジストリのデータベースに登録された情報

２．目的

(1)基幹ネットワークの維持・管理
(2)サブネットワーク(別途規定)の接続・管理

３．基幹ネットワークの維持・管理

情報センターが以下を維持・管理する。

(1)外部ネットワーク(インターネットを含む)およびサブネットワークの接続に関する構成を設計、維持・管理し、必要組織との調整、指導を行う。
(2)ネットワークの配線および機器
　基幹ネットワーク機器、配線の安定的な作動状態を維持・管理する。
(3)経路制御
　基幹ネットワークの安定的な経路制御を維持・管理する。
(4)ネットワークの監視
　①ネットワークの動作状態を監視し、異常がある場合は速やかに対処する。
　②基幹ネットワークおよび他組織の安定運用あるいは公共の福祉に対し、重大な影響を与える通信が発見された場合の状況調査及び証拠保全のために学外との通信を定常的に採取することが出来る。採取した通信の内容は、公的機関または情報センター長からの調査要請にのみ解析または参照可能とする。採取のためのシステム及び採取後の情報は厳重に管理し、保管期間は 3 ヶ月間とする。
　③基幹ネットワークおよび他組織の安定運用あるいは公共の福祉に対し、重大な影響を与える通信が発見された場合、被害の拡大を防止するために、必要に応じてその通信元を発見するため、パケットモニタリング等の適切な手段をとることができる。該当する機器を発見した場合は、当該機器の管理者に対して是正するよう勧告をおこなえる。また、必要に応じて該当するパケットを遮断することができる。これらの措置の判断の基準および手順は、「セキュリティ管理に関するガイドライン」に従うものとする。
(5)帯域制御
　基幹ネットワークの適切な位置に帯域制御装置を設置し、適切なネットワーク環境を構成し、運用する。また、基幹ネットワークの構成、運用に変更が生じた場合は、速やかに帯域制御を再構成することができる。
(6)侵入検知システムの運用
　「セキュリティ管理に関するガイドライン」に基づき、侵入検知システムを構築し、運用する。
(7)ファイアウォールの運用
　「セキュリティ管理に関するガイドライン」に基づき、ファイアウォールを構築し、運用する。
(8)ネームサーバの運用
　「トップドメイン管理に関するガイドライン」に基づき、レジストリ・データベースの登録情報の管理、トップドメイン情報の管理、サブドメイン委譲の管理、必要なドメインネームサーバの構築、運用を行う。
(9)メールサーバの運用
　「トップドメイン管理に関するガイドライン」に基づき、メールサーバを構築し、運用する。
(10)WWW サーバの運用
　「トップドメイン管理に関するガイドライン」に基づき、WWW サーバの運用を支援する。
(11)キャッシュサーバの運用

インターネットアクセスでのセキュリティを強化するため、また、アクセス時間を短縮するため、キャンパスネットワーク最上位キャッシュサーバを構築し、運用する。

(12)IP アドレスの管理

①サブネットワークに対して、別途定めるサブネット空間(プレフィックス)を割り当てる。

②原則的に DHCP サーバにて IP アドレスを動的に配布する。また、利用者より「固定 IP アドレス申請書」が提出された場合、適切な固定 IP アドレスを割り当てる。

③サブネットワークへ割り当てた IP アドレスの利用状況に変更が生じた場合、サブネットワーク運用担当者から変更を届けてもらわなければならない。

(13)連絡体制について

基幹ネットワークに障害が発生したときなど、サブネットワーク利用者へ連絡をする場合には、情報センターよりサブネットワーク運用担当者へ連絡し、サブネットワーク運用担当者がサブネットワーク利用者へ連絡するものとする。

(14)必要に応じて情報センター長は、サブネットワーク接続のため以下のメンバーを招集できる。

①情報センター員

②情報センター事務室スタッフ

③サブネットワーク運用担当者

(15)基幹ネットワーク運用に関する調整は、情報センターおよびサブネットワーク運用担当者にて行い、情報センター長の決定に従う。

4．サブネットワークの接続・管理

(1)「サブネットワーク接続申請書」による申請に対し、情報センター委員会で審議し、接続の許可および非許可を決定しなければならない。

(2)サブネットワークに対し、適切な回線・ネットワーク機器を設置し、安定したネットワークを提供しなければならい。

(3)サブネットワークに対して、「サブネットワーク管理に関するガイドライン」および「セキュリティ管理に関するガイドライン」を遵守するよう指導する。

(4)サブネットワークの利用停止、使用許可の取り消しについて

上記責任を遵守されずサブネットワークの運用が適切に行われない場合は、情報センター長が以下の措置をとることができる。

①サブネットワーク運用担当者への警告

②一定期間のサブネットワーク運用停止

③サブネットワーク設置許可の取り消し

(5)サブネットワークに対するトラブル処置

サブネットワーク下のネットワークまたはサーバによるトラブルにより、基幹ネットワークおよび他組織の安定運用あるいは公共の福祉に対し、重大な影響を与える通信が発見された場合、被害の拡大を防止するために、必要に応じてその通信元を発見するため、パケットモニタリング等の適切な手段をとることができる。該当するサブネットワークを発見した場合は、当該サブネットワークの管理者に対して是正するよう勧告をおこなえる。また、必要に応じて該当するパケットを遮断することができる。これらの措置の判断の基準、および手順は「セキュリティ管理に関するガイドライン」に従うものとする。

(6)必要に応じて情報センター長は、サブネットワーク接続のため以下のメンバーを招集できる。

①情報センター員

②情報センター事務室スタッフ

③サブネットワーク運用担当者