神奈川大学 学長 殿

②記入例

| 受付者 | 受付日 | 整理番号 | 受付印 |
|---|---|---|---|
| | | | |

# 独立管理サブネット運用ガイドライン（見本）

制定日　2008年5月31日

サブネットの情報
- レンジ　133．72．21．0／25
- 所在　横浜1号館3階311室

責任者などの情報
- 責任者　情報システム推進部長
- 技術担当者　神奈川太郎
- 学生の参加　学生は管理を行わない

目的

本ガイドラインは、当該サブネットの管轄するサーバ上のコンテンツに起因するトラブルを回避し、サーバの安全性の向上を図り、ネットワークのセキュリティを維持することを目的とする。

適用範囲

本ガイドラインの適用範囲は、先に記載したサブネットレンジ内にあるサーバおよびネットワークである。またDNSで示された名前空間がサブネットレンジを越える場合においては、その名前空間も適用範囲とする。

日常の管理

見つかった場合にはその旨を学部・学科や情報システム推進部に通知し、緊急時の対応を行う。ウイルス対策が可能な機器があれば、可能なかぎり対策を講じる。JPCERT/CCなどが運営するセキュリティ情報のメーリングリストに加盟し、OSおよびサーバのソフトウェアセキュリティーホールを放置しない。ネットワークを利用できるユーザーを把握し、利用者の変更が発生した場合にはその都度サブネット内の登録情報を変更する。大量のアクセスが予想されるコンテンツを公開する場合は、あらかじめ接続先ネットワーク管理者（MNS)の了解を得る。無線LANやNATの利用には細心の注意を払い、不正利用が発生しないよう留意する。管理者パスワードについては、必要最小限の人員（管理者）に通知することとし、扱いには十分注意する。また、管理者権限の行使については記録をとる。

サーバ設置の届出

学外からアクセス可能なサーバを設置する場合は、接続先ネットワーク管理者（MNS）にサーバ設置届出書を提出する。

ログの保存

ログイン情報、サーバログなどのセキュリティー上必要な記録物については、過去1年分以上保管する。外部組織などからの問い合わせに際しては、ログを解析して必要に応じて回答を行う。ただし、ログの利用目的は不正行為の証拠保全と問題のあるコンテンツの配布先特定にのみ利用する。

緊急時の対応

障害発生時には直ちに原因となるPCや通信機器を速やかにネットワークから切り離し、報告の必要がある場合は学部・学科や情報システム推進部へ報告を行う。切り離した機器は障害解析のため現状保護し、原因を特定し除去した後に再度報告を行いネットワークに復帰させる。

監査

年1回以上、別途定める手順により、セキュリティスキャナなどを用いた監査を行い、接続先ネットワーク管理者（MNS）に提出する。