ネットワークに関するガイドライン

１．ネットワーク利用に関するガイドライン

平成１１年　２月２３日制定

ネットワークを利用した情報発信に関しては、そのマナーについての社会的問題が顕在化してきている。電子メールを使用し、ニュースグループ・掲示板等に投稿し、あるいはWWWページ（ホームページ）を公開する場合において、発信する者は自らの責任において情報公開を行うことが求められており、そのための指針として下記のガイドラインを作成する。なお、このガイドラインはあくまでも「例」であり、記入のない事項についても、発信者自身の責任において、マナーに反することのないよう留意すること。

【１．ネットワークの利用にあたって】

◆本学のメールサーバ・ウェブサーバ等のサーバ機器を利用するには，サーバ管理者からユーザIDと初期パスワードを交付してもらうこと。

使用するコンピュータによって管理者が異なります。一般学生が利用する総合情報処理センターのコンピュータは総合情報処理センターが，各学部等の部局（場合によっては学科）のサーバコンピュータは部局（あるいは学科）のネットワーク委員会が，各研究室のコンピュータはそれぞれの管理者が管理しています。

◆ノートパソコン等自分のコンピュータを学内のネットワークに接続するには，ネットワーク管理者の許可を得ること。

ネットワークは基幹ネットワークと部局ネットワークで管理者が異なります。基幹ネットワークはネットワーク運用委員会が，部局ネットワークは部局ネットワーク委員会が管理しています。一般ユーザが接続するのは部局ネットワークですから，利用方法については部局ネットワーク委員会にお尋ね下さい。

◆ユーザIDおよびパスワードの交付を受けた者はこれらを厳重に管理すること。

ユーザIDやパスワードが他人に漏れると，不正利用につながる恐れがあります。
交付されたユーザIDを他人に貸与してはなりません。
パスワードが漏れた場合は（本人の不注意だけでなく，学内外からのアタックによって盗まれた場合も），ユーザIDを一時停止してパスワードを変更していただきます。

【２．目的外利用の禁止】

◆情報ネットワークシステムの利用は、本学における教育、研究、学術情報サービス及び事務処理上必要と認められるものに限る。（神戸大学情報ネットワークシステム運用規程第十二条の二）

◆営利目的で使用することは認められない。

社会的には許される商行為であっても，本学に設置されているコンピュータ，ネットワーク機器，ネットワークを利用する場合は営利目的に使用しないこと。

◆社会通念上認められる範囲を逸脱した私的利用を禁止する。
就職活動やサークル活動は課外活動の一環として認められますが，私信のやりとりや趣味的な利用は節度をもって行うこと。

【３．犯罪行為に結びつく、あるいは結びつくおそれのある行為の禁止】

「犯罪行為をしてはいけない」というのは一般論として当然のことですが，著作権等に関しては何が犯罪行為か必ずしも正しく認識されていないようです。

◆国内の法律に抵触する行為，ならびにその手段として利用すること。
外国のコンピュータにアクセスする場合は，その国の法律も遵守して下さい。

◆著作権・著作隣接権を侵害する行為

- 市販のソフトウェアを違法にコピーすること。
ソフトウェアの使用にあたっては，使用許可条件（個人利用限定，サイトライセンス等）を守って下さい。 教育・研究に必要なソフトウェアにはしかるべき予算措置を講じて下さい。
- 印刷物（書籍，パンフレット，写真等）の一部または全部をスキャナやデジタルカメラ等で取り込み，著作権者の許可なくホームページ等で公開すること。
- 他のWWWページ等に掲載された画像等を無断で取得し，自分のWWWページ等で公開すること。
- 他人の著作物の全部の引用、又は（正当な目的外の・必要以上の・出所を明示しない・著作者名を表示しない）引用をすること。
- 他人の著作物を著作者に無断で改変することは，それ自体で著作権侵害になることがあります。
- 演奏者・編曲者・翻案者等の著作隣接権を侵害すること。
音声データも著作権で保護されています。

◆肖像権を侵害する行為

- 他人を撮影した写真を被写体本人に無断で公開すること。
被写体が美術品や有名な建築物等の場合も著作権侵害になる場合があります。

◆猥褻な文章・画像等を公開すること。

◆学内外のコンピュータへの不正なアクセス，また不正なアクセスを試みること。

◆学内外のコンピュータに 無意味な大量のデータを送り，意図的にネットワークやコンピュータを麻痺させること。

【４．公序良俗・社会的公正さに反することの禁止】

◆基本的人権を侵害する行為

- WWWページ等を使って他人を誹謗・中傷すること。
- 受信したメールの内容を発信人に無断で公開すること。
- 他人の個人情報を当人に無断で公開すること。
  WWWページや掲示板等は不特定多数の人に情報発信が可能です。中には悪意をもってそれらの情報を使う人がいるかも知れません。 他人の住所・電話番号・写真・誕生日等の個人情報の公開は行わないこと。自分自身の個人情報の開示も必要最小限にとどめて下さい。

◆ネットワーク利用のマナーに反する行為

- 不特定多数の人にダイレクトメールを送ること。
- 他人のアカウントを利用すること。
  本人が了承していてもこのような行為は避けて下さい。
- 学内共有の端末を占有すること。
  特に学生用の端末は数が十分ではないので、長時間占有することは避けて下さい。

【５．上記事項に違反している場合の措置】

◆不正利用が疑われる場合

- コンピュータまたはネットワークの不正利用が疑われる場合は，サーバ管理者がユーザIDを一時停止する。
- 疑義のあるホームページについては、サーバ管理者が公開を一時差し止める。

◆不正利用が確実な場合

- サーバ管理者によるデータの強制削除、アカウントの停止。

※附　則
このガイドラインは，平成１１年　２月２３日から実施する。

平成１１年２月２３日制定
平成１２年２月２５日改正

近年情報ネットワークの利用は飛躍的に増加し，本学においてもライフラインのひとつとなりつつある。 これに伴いシステムの安定性・安全性の確保が重要な課題となっている。ネットワークに接続された機器の不正使用の影響は， 不正使用者個人または不正使用された機器にとどまらず，他の利用者や機器へ波及する可能性が高い。管理者は日頃不正使用や不正アクセスに対する予防措置を 講じると共に，問題発生時には速やかに適切な対策をとらなければならない。このガイドラインはそれぞれの機器の管理責任を明らかにし，不正使用の予防措置， 障害発生時の対策等について，管理者がとるべき措置についてまとめたものである。

【１．基本的事項】

◆表現の自由・通信の自由

ネットワーク利用者の思想・信条の自由，表現の自由や通信の自由を最大限保証すること。

◆自己責任原則

ネットワークを利用する際には、その情報の内容については，それを発信した者が第一義的に責任を負う。

◆情報を受信する者の権利・利益の保証

情報を受信する者に対する権利・利益は最大限にこれを保証すること。

◆守秘義務

機器の管理上得た第三者に関する情報を他人に漏らしてはならない。

【２．機器の管理責任】

◆機器の定義

- 端末：パソコン・ワークステーション等，ネットワーク利用者が直接操作するネットワークに接続された機器
- サーバ機器等：メールサーバ，ウェブサーバ，ネームサーバ等情報を蓄積し発信する機器
- ネットワーク機器：ルータ，ネームサーバ等ネットワークの管理・運用に係る機器
- 部局ネットワーク各部局に設置された端末及びサーバ機器等を相互に接続するために部局に設置されたネットワーク
- 機関ネットワーク：KHAN-96で導入されたATM網等，部局ネットワークを相互に接続するための全学的なネットワークシステム

◆管理体制

「神戸大学情報ネットワークシステム運用規程」を参照のこと

情報ネットワークシステム委員会

- 機関ネットワーク及び機関ネットワーク機器の管理・運用方針を決定する。

情報ネットワーク運用委員会

- 基幹ネットワーク及び基幹ネットワーク機器の管理・運用方針を審議し，情報ネットワークシステム委員会へ提案する。
- 情報ネットワークシステム委員会の決定に基づいて，基幹ネットワーク及び基幹ネットワーク機器の管理・運用を実施する。
- 基幹ネットワーク及び基幹ネットワーク機器に係わる，新規機器の導入や設定の変更を決定する。

基幹ネットワーク運用者

- ネットワーク運用委員会の方針に基づいて，基幹ネットワーク及び基幹ネットワーク機器の日常的な管理・運用を行う。
- 基幹ネットワーク運用者の管理下にあるネットワーク機器・サーバ等機器・端末の不正使用に対して最大限の予防措置を講ずる。
- ネットワークの管理・運用に係わる情報を必要に応じて各部局のサーバ等管理者へ提供する

部局ネットワーク委員会

- 各部局の管理下にある部局ネットワーク及びネットワーク機器，サーバ等機器の管理・運用方針を決定し，実施する。
- 部局ネットワーク機器及びサーバ等機器の導入や設定の変更を決定する。
- 必要に応じてネットワーク機器の設定等を行う運用者をおき，その監督責任を負う。
- 部局の管理下にある各サーバ等機器及び端末の管理者を定める。
- 部局の管理下にあるサーバ等機器・端末の不正使用に対して最大限の予防措置を講ずる。
- 部局の管理下にあるサーバ等機器・端末の管理者に対して，適正な利用のための教育・広報を行う。
- 総合情報処理センターが発行する学生用IDの利用者については，総合情報処理センターの指導・助言を得て， 当該学生の所属する部局の部局ネットワーク委員長が適正な利用のための教育・広報に責任を負う。

サーバ等機器の管理者

- サーバ等機器の管理・運用を行う。
- 必要に応じてサーバ等機器の設定等にあたる運用者をおき，その監督責任を負う。
- 長期出張等、緊急対応に問題が生じることが予想される場合には、あらかじめ管理者権限を委任しておくこと。
- サーバ等機器の不正使用に対して最大限の予防措置を講ずる。

- サーバ等機器の利用者に対して，適正な利用のための教育・広報を行う。

端末管理者

- 端末の不正使用に対して最大限の予防措置を講ずる。
- 使用するソフトウェア等に不正なものがないよう十分配慮する。
- 正規のソフトウェア等が違法にコピーされることにないよう管理する。
- 長期出張等、緊急対応に問題が生じることが予想される場合には、あらかじめ管理者権限を委任しておくこと。

◆サーバ等管理者メーリングリスト

サーバ等機器の管理に有用な情報の共有をはかるため、部局ネットワーク委員会において、サーバ等管理者メーリングリスト （以下、部局MLという）を構築する。部局MLには，部局ネットワーク委員会メンバー，各部局のネットワーク運用委員， ならびにサーバ等機器及び端末の管理者及び運用者を登録する。必要に応じて，学科等のサーバ等管理者メーリングリストを構築する。
さらに、部局ＭＬを集約したメーリングリスト（以下、srvadm ML という）を基幹ネットワーク運用者が構築する。

【３．事件・事故への対応】
◆報告義務

- 各部局に設置されたネットワーク機器，サーバ等機器及び端末の管理者または運用者は、 管理下の利用者もしくは機器のネットワークに関連した事件・事故について、発生を確認した時点で速やかに当該機器の管理者及び部局ネットワーク委員長に 届け出ること。
- 他部局のネットワークまたは基幹ネットワークへの影響が懸念される場合は，部局ネットワーク委員長は基幹ネットワーク運用者へ速やかに報告すること。
- 当該機器の管理者は事件・事故についての詳細を文書により部局ネットワーク委員長に提出すること。
- 学外からのクラッキング等，他のサーバ等機器や端末においても緊急の対策が必要と考えられる場合は，速やかに部局MLやsrvadm MLへも報告すること。

◆不正利用に対する緊急対応

ネットワーク機器，サーバ等機器及び端末の管理者は、ネットワークにおける不正利用が確認された時点で、 すみやかに下記の処置をとるものとする。なお、不正利用により他の利用者（学内・学外を問わない）に損害や迷惑行為が認められた場合には、 利用者の所属部局、学生部、総合情報処理センター等、関連の部局と十分に連絡をとったうえで、誠意をもって対処すること。

- 利用者が電子メール等で不正行為を行った場合
  当該ＩＤの抹消等，当事者に対して適切な措置を行なう。また関連ログを採取するなどして、できるかぎり被害（影響）を調査し、 被害者等に対する連絡などの措置を行う。

- 利用者が不正なホームページを公開した場合
  当該ＩＤの抹消及びリンクの削除等当事者及び当該機器に対して適切な措置を行う。当該WWWページのデータ及び関連ログについては、 後日詳しい調査を行う場合に必要となることがあるのですべて保管すること。

- ソフトウェアの不正使用
  該当のソフトウェアを即刻削除し、不正使用の経緯を確認すること。

- ウィルスに感染した場合
  ワクチンソフトにより即刻除去すること。また、感染経路を特定し、再感染の防止に努めること。

◆不正アクセスに対する緊急対応

不正アクセスに対して、最も重要なことは、当該機器に対する対応だけでなく「他へ被害を広めない」ことに留意することである。 つまり、当該機器の防御を固めるだけでなく、周辺の機器の防御に対する対応を必ず行なうこと必要がある。このため、被害状況、 ならびに、侵入者や不正使用者の手口や行動状況などをできるかぎり把握し、周辺への影響を考慮した対応プロセスを検討すること。 状況によっては、「周辺を固めてから、最後に中心（自分の機器）を固める」方策をとった方が良い場合もありうる。
不正アクセスを受けた機器の管理者は、ネットワークにおける不正アクセスが確認された時点ですみやかに下記の措置をとるものとする。 また、基幹ネットワーク運用者は必要に応じ、危険性が回避されたことを確認できるまで、当該支線を切り離すことができる。
当該機器の管理者に連絡がとれない場合、部局ネットワーク委員会は当該機器の設置してある部屋への立ち入り、 及びネットワークからの切り離しを行うことができるが、可能な限り立会人を置くこととする。さらに、当該機器内部の調査が必要となる場合もあるので、あ らかじめ部局ネットワーク委員会で細部を取り決めておくことが望ましい。

- クラックされた場合
  - 「周辺への影響」に対する対応
    当該機気をネットワークから切り離し現有保存し、内部解析を行い周辺への影響の有無/可能性を調べる。
    - どのようなソフトが仕掛けられたかなどの調査
    - ログ解析などによる調査
    - 他のサーバへの rhostsの有無、同一パスワードによるIDの有無の確認
    - 関連する機器の管理者への連絡
    - 周辺への連絡

  - 「当該機器」に対する対応
    - 当該機器のネットワークからの切り離し
    - OS等のバージョンアップ
    - ID及びパスワードをすべて再構成すること
    - ハードディスクなどの２次記憶装置内の不審なデータの調査
      個人ファイル等に不正プログラムを隠している場合がある

- SPAMメール等、不正使用の足場にされた場合

速やかに当該機器を停止し、OS等のバージョンアップにより危険性を排除すること。

◆外部からのクレーム対応

- 外部からのクレームは、基幹ネットワーク運用者に届け出ること。
- 基幹ネットワーク運用者は、その対象となる利用者に関わる端末又はサーバ等機器の管理責任者、所属部局のネットワーク管理責任者、全学の場合は学生部、 それぞれに通知する。
- 学内利用者による違法行為等の場合、対応窓口は基本的に所属部局とする。
- サーバ等機器の予防措置不備の場合は、サーバ等機器の管理者が対応することを原則とする。

＊附 則　このガイドラインは、平成１１年２月２３日から実施する。
＊附 則　このガイドラインは、平成１２年２月２５日から実施する。