電気通信大学 情報ネットワーク 利用ポリシー (在学生用)

2004/03/30

全学情報ネットワーク運用委員会

電気通信大学情報ネットワークを利用するためには、「利用に関するポリシー」と「情報セキュリティ維持に関するポリシー」の二つに掲げられた事項に反しないように十分注意しなければなりません。

これらのポリシーは全て「電気通信大学情報ネットワークの運用と利用に関する基本方針」の前文で述べられているように、我々利用者と管理者が、高度コミュニケーション科学の教育研究を標榜する本学に相応しい情報ネットワークの社会的責任のある模範的な運用と利用を行なうために定められています。

以下に二つのポリシー本文とその具体例や注釈を示します。利用者がポリシーに反した場合や、全学情報ネットワーク運用委員会または各学科の情報ネットワーク運用委員会が必要と認めた場合、学内ネットワークや情報機器の利用を警告なく終了させたり、当該利用者の所有する情報を消去・改変することがあります。

電気通信大学ネットワーク運用標準

(P1) 本学ネットワークの利用に関するポリシー(AUP)

(1) 基本的人権の保護

本学の情報ネットワークの上の活動やネットワーク上のコンテンツは、日本国憲法の条文に記されている基本的人権が保護されているものでなければならない。人種・性差・信条・信仰等への差別、人格やプライバシーへの攻撃等の他者の人権を侵害する行為を本学の情報ネットワークを通じて行なってはならない。具体的には差別的発言や誹謗中傷等の言論での暴力行為、実際の暴力行為や犯罪を助長する行為、性的虐待や性犯罪・幼児虐待を助長する行為、通信の盗聴や盗聴内容の公開等は禁止されている。

具体的な禁止事項

- 電子掲示板やネットニュース、メーリングリストに個人や団体が判明する形で名誉毀損に当たる発言や誹謗中傷が記された記事等を投稿すること。
- 電子掲示板やネットニュース、メーリングリストに暴力行為や犯罪行為を教唆する記事、それらを助長する記事等を投稿すること。
- 電子掲示板やネットニュース、メーリングリストに性犯罪や犯罪行為を教唆する記事、それらを助長する記事、児童ポルノ禁止法等に抵触する画像等を投稿すること。
- 電子メールやチャット等で個人や団体の名誉毀損に当たる発言したり、誹謗中傷を行なうこと。
- 電子メールやチャット等で児童ポルノ禁止法に抵触する画像を送信したり、青少年保護育成条例にて保護されるべき人物に対して同条例に抵触する発言を行なうこと。

(2) 商用利用の禁止

本学の情報ネットワークは、学術研究と教育利用のためのものであり、SINET の AUP も学術研究目的の利用のみと制限している。商用活動を目的とした利用を行なってはならない。

具体的な禁止事項

- **本学のメールアドレスを用いたネットワークオークションへの参加。**
- **本学のメールアドレスを用いた個人売買への参加。**
- **本学に設置されたサーバや学内のメールアドレスを用いた商業活動。・**

(3) 知的財産権の保護

著作権・意匠権・商標権等の知的財産権を尊重し、保護しなければならない。著作者に無断で著作物(またはその一部)の複製を作成・配布することは禁止する。また、大学の公共性に鑑み、著作権を侵害する恐れがあると考えられているソフトウェアの利用も禁止する。

具体的な禁止事項

- **本学のネットワークを用いて、著作権者の許可なく配布されている著作物(映像ファイル・楽曲ファイル・電子出版物・商用ソフトウェア・印刷物をスキャニングしたファイル)を発信・受信すること。**
- **違法ウェブサイトや違法 ftp サイトからダウンロードを行なうこと。ファイルのダウンロードする前に著作権侵害の可能性をよく吟味するべきである。**
- **研究用途以外で本学のネットワークでファイル共有・交換ソフトウェアを用いること。最近のファイル共有・交換ソフトウェアはファイル共有・交換ソフトウェアであることを意識させないようになっている。注意しなければならない。**

(4) 個人情報ならびにセキュリティ侵害の禁止

本学ならびに本学からアクセス可能な全ての学外組織の情報機器や情報資産およびその利用者のプライバシーは保護されなければならない。攻撃、盗聴等の情報セキュリティに対する侵害行為は禁止する。詳しくは「(P2) 本学ネットワークの情報セキュリティ維持に関するポリシー(ASP)」を参照せよ。

具体的な禁止事項

- **学内・学外を問わずネットワークに接続されているコンピュータやネットワーク機器に対して、攻撃を行なうこと。攻撃行為には電子掲示板にその規約違反の投稿を行なうこと、規約違反の利用を行なうこと等も含まれます。**
- **個人のコンピュータ、ファイルやフォルダー・ディレクトリに対して攻撃を行ない、個人情報を探り出すこと。またはその利用を妨害すること。**
- **利用者の定まっているコンピュータをその利用者の許可なく利用すること。**
- **コンピュータやネットワークを管理する中で知り得た個人情報を許可なく公開すること。**
- **アカウントとパスワードを他者と共有したり、一時的に貸与すること。**
- **本学のメールアドレスを、そのメールアドレスの利用者に許可なく他者に公開や販売を行なうこと。**
- **本学のメールアドレスを迷惑メールの発信者が利用する可能性のあるアンケート調査に記入すること。**

(5) 公共性の遵守

大学は公共の機関であり、公共から期待される活動を行なう義務を負う。本学情報ネットワークおよび本学情報機器の行き過ぎた個人的利用を禁止する。本学情報ネットワークから必要とされる以上の匿名性を持つ情報発信を行なってはならない。本学の成員は情報発信の内容に責任を持たなくてはならない。

具体的な禁止事項

- 本学ネットワークからネットワークゲームを遊ぶこと。研究に必要な場合は、申請が必要である。
- 本学ネットワークから猥褻画像や文書・他者を不快にさせる画像や文書等、教育研究機関に相応しくないと思われる情報を発信すること。
- 教育や研究用途に合致しない有料コンテンツを利用すること。
- 出会い系サイト等の教育研究機関に相応しくないサービスを利用すること。
- 個人的用途のために、楽曲ファイル・映像ファイル・商用ソフトウェア(試用版ではなく、CD-ROM等からコピーした製品そのものあるいはその一部)を本学ネットワークから発信・受信を行なうこと。本学ネットワークの過度の個人利用と見なします。
- ・情報発信(電子掲示板やメーリングリスト等への投稿)において、学外プロクシーサーバ等を利用しあたかも本学ネットワーク以外の箇所から発信したよう偽装する行為。情報発信を行なう場合は責任持って行なうべきである。

注釈

本学はSINETのノード校で、SINETとは1Gbpsで接続されています。実際は1Gbps全てを使えるわけではなく、20以上の他の研究機関と1Gbpsの帯域幅を共有しており、若干多めに利用してよいだけです。本学がネットワークの帯域幅を利用しすぎると、他の研究機関が利用可能な帯域幅が減少してしまいます。過度の私的利用は厳禁とします。

(6) 情報ネットワークと情報セキュリティの保護

情報ネットワークは産業から生活まであらゆる範囲に必須のインフラストラクチャである。本学ならびに学外の情報ネットワークの円滑なる運用を妨げる行為は禁止する。また、情報ネットワークは安全な場所ではない。利用者個人が情報セキュリティの保護に対して注意を怠らないようにしなければならない。個人情報や情報機器の情報セキュリティはその利用者が自ら進んで保護しなければならない。詳しくは「(P2) 本学ネットワークの情報セキュリティ維持に関するポリシー(ASP)」を参照せよ。
[後述]

(7) 教育の義務

本学の情報ネットワークと情報機器を利用あるいは管理する者は、情報ネットワークと情報機器、およびそれらの適切な運用に関する教育を受け、それらを理解しなければならない。全学情報ネットワーク委員会はネットワーク社会の現状や関連法規等を考慮した教育計画を立案し、実行しなければならない。

具体的な禁止事項

- コンピュータリテラシーの講義を受けずに本学ネットワーク及び本学内のコンピュータ等を利用すること。
- 無線 LAN 講習会を受けずに本学無線 LAN アクセスポイントを利用すること。
- 情報ネットワーク運用委員会からの広報やガイドラインを読まずに本学ネットワークを利用すること。
- 指導教官や講座・研究室教職員の指導を受けずに本学ネットワークを利用すること。

注釈

今後、本学ネットワークやコンピュータに関する講習会を定期的に行なうことを計画しています。これにはコンピュータの使い方から管理者になるための教育から、コンピュータセキュリティ等まで広い範囲に及びます。これらに参加するよう要請された場合は、必ず出席してください。

(8) 関係法規の遵守

AUP として定められる遵守事項の他に、情報ネットワーク上で行なわれるあらゆる活動は、関連法規に違反してはならない。

具体的な禁止事項

- ネットワークやコンピュータに関連した法律に抵触した活動を行なうこと。

注釈

ネットワークやコンピュータに関連した法律で代表的なものは

- *刑法・民法（実社会で違反とされる行為はネットワーク上でも違反行為です）*
- *不正アクセス禁止法（コンピュータやネットワークへの侵入・禁止等を規定しています）*
- *著作権法（ネットワーク上での著作権の扱いも規定しています）*
- *児童ポルノ法（ネット等での「児童ポルノ」の頒布等が禁止されています）*
- *個人情報保護法（個人情報の取り扱いを定めています）等があります。*

また、国際条約等ですと

- *ベルヌ条約（国際的な著作権に関する条約）*
- *WIPO 著作権条約（ベルヌ条約を包括する著作権に関する条約）*

等があります。

また、日本国以外のネットワーク上のコンテンツ等を利用する場合は、その国々の法律にも従わなければなりません。注意してください。

電気通信大学ネットワーク運用標準

(P2) 本学ネットワークの情報セキュリティ維持に関するポリシー(ASP)

(1) 情報機器の保護の義務

本学の情報ネットワークに接続されている全ての情報機器は、不正侵入・不正アクセス・サービス不能攻撃等に代表されるあらゆる情報ネットワークからの攻撃に対する対策を行なわなければならない。同時に全ての情報機器には潜在的脆弱性が存在するものと認識して、その対策を怠ってはならない。

具体的な禁止事項

- セキュリティホールが存在するパソコン等を、何の対策も取らずに本学ネットワークに接続すること。例をあげると
  - WindowsUpdate を行なわない Windows マシンの接続
  - ウイルスチェッカーのインストールされていない Windows マシンの接続。およびウイルス定義ファイルの更新を怠った Windows マシンの接続
  - セキュリティ勧告が発行されている OS を対策を行わずに利用すること。

  等を指す。

(2) 情報機器の情報漏洩防止の義務

本学の情報ネットワークに接続されている全ての情報機器は本学情報ネットワークとそれに接続されている情報機器の脆弱性の露呈に繋がる可能性のある情報の提供をしてはならない。本学の情報ネットワークとそれに接続されている全ての情報機器から提供される情報は、その波及範囲と影響を十分に考慮に入れたものでなければならない。

具体的な禁止事項

- 全学情報ネットワーク運用委員会等から広報されるセキュリティ情報やインシデント情報を本学外の電子掲示板やメーリングリスト、本学関係者以外の他者に送信すること。
- 本学ネットワークを利用して知り得た各ホストやネットワーク機器のセキュリティ情報を流布すること。これらの重要情報は各学科の情報ネットワーク運用委員会に直ちに届け、その指示に従わなければならない。

(3) 情報機器から提供されるサービスの管理義務

本学の情報ネットワークに接続されている全ての情報機器上で動作する各種サービスは、本学の情報ネットワークと情報機器の脆弱性の露呈や攻撃に利用される可能性を提供しないよう管理しなければならない。同様に、本学情報ネットワーク上で動作するサービスが学外組織の情報ネットワークに対する攻撃や情報漏洩に利用されないよう管理しなければならない。

具体的な禁止事項

- 学内学外を問わず、ネットワーク越しの攻撃や侵入の対策を怠ること。最近の Windows マシン等はデフォルトで利用すると攻撃に対して非常に脆弱となっていることがある。
- 研究用途以外でウェブコンテンツ等に本学あるいは他の組織のネットワークサービスのセキュリティホール等の脆弱性情報を掲載すること。

(4) 個人情報保護の義務

本学の情報ネットワークを利用する全ての者は、個人情報を管理するのは常に自分自身であることを認識しなければならない。その認識の元に学内外を問わず全ての情報ネットワークに流通する自分自身の個人情報を適切に管理しなければならない。本学の情報ネットワークとそれに接続される情報機器を管理する者は、それらの利用者の個人情報を可能な限り保護する措置を取らねばならない。また、管理作業を行なうときに知り得た利用者の個人情報の漏洩を行なってはならない。

具体的な禁止事項

- 自分の個人情報(氏名・住所・年齢・電話番号・メールアドレス等)を考えなしにアンケート等に書き入れること。自分自身の個人情報を管理するのは自分自身であることに留意すること。
- 本学ネットワークや本学のコンピュータを利用あるいは管理している途中で偶然知り得た他者の個人情報を公開・販売すること。

(5) 報告の義務

本学情報ネットワークの脆弱性を発見した場合やあるいは個人情報の漏洩を発見した場合等、本学情報ネットワークとその利用者の情報セキュリティが侵害されていると考えられる事態が起こった場合、発見者は速やかにそれを各部局の情報ネットワーク委員会あるいは全学情報ネットワーク委員会に報告しなければならない。報告を受けた各部局の情報ネットワーク委員会は速やかに全学情報ネットワーク委員会に報告しなければならない。

具体的な禁止事項

- 本学ネットワークや本学のコンピュータに脆弱性が存在しているのを知り得た場合に、それをシステム管理者や各学科の情報ネットワーク運用委員会に報告しないこと。
- ウイルス感染や攻撃・侵入等の被害にあったときに、それらをシステム管理者や各学科の情報ネットワーク運用委員会に報告しないこと。
- ポリシーに反した行為が行なわれていると知りながら、それをシステム管理者や各学科の情報ネットワーク運用委員会に報告しないこと。

(6) 対策の義務

本学情報ネットワークのセキュリティ・インシデントや個人情報の漏洩等の情報セキュリティの侵害行為に対して、全学情報ネットワーク委員会は即座に対策を行ない被害を最小にとどめなければならない。全学情報ネットワーク委員会は、情報セキュリティの侵害行為を分析し、必要な点検と対策の計画を立て指示を出さなければならない。本学の情報ネットワークとそれに接続される情報機器を管理する者は、その指示に従い点検と対策を行なわなければならない。

具体的な禁止事項

- ウイルスに感染したり侵入を受けた等の具体的な被害が発生しているのにも関わらず、そのコンピュータをそのまま利用し続けること。
- 全学情報ネットワーク運用委員会、各学科の情報ネットワーク運用委員会、システム管理者等からの指示や勧告に従わず、脆弱性の存在するコンピュータ等を利用し続けること。

(7) 教育の義務

本学の情報ネットワークと情報機器を利用あるいは管理する者は、情報セキュリティと個人情報の保護に関する教育を受け、それらを理解しなければならない。全学情報ネットワーク委員会はネットワーク社会の現状や関連法規等を考慮した教育計画を立案し、実行しなければならない。

[前述]