施行　2003 年 11 月 1 日
改定　2010 年 4 月 1 日

セキュリティ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、セキュリティ管理に必要な事項を定めるものとする。

本ガイドラインは、該当する部門により次のように分類する。

Ⅰ　トップドメイン管理部門編
Ⅱ　ネットワーク管理部門編

Ⅰ　トップドメイン管理部門編

１．入退室管理

①サーバやネットワーク機器が設置されているマシンルームは通常は施錠しておかなければならない。
②入退室状況を記録するよう努める。

２．サーバ管理

①サーバ管理をリモートで行う場合は、接続元のＩＰアドレスを限定しなければならない。
②サーバへログインする端末も十分な安全対策がなされたものを用いなければならない。業者には確認書を提出させる。
③不必要なサービスについては停止しなければならない。
④ＯＳやアプリケーションについては、常に脆弱性情報を収集し、高いセキュリティを確保しなければならない。
⑤重要性の高いサーバには無停電電源装置を設置しなければならない。
⑥利用可能なアカウントには必ず安全なパスワードを設定しなければならない。
⑦サーバから一時的に離れるときにもログアウト等の操作防止措置をしなければならない。
⑧Windows 系サーバはウィルス情報の更新は頻繁に行い、日常的にアンチウィルスソフトを稼動させなければならない。
⑨サーバでクライアントアプリケーションを実行することは極力避けなければならない。
⑩ウィルスやワームに感染した怖れがあるときには、まず、ネットワークから切り離さなければならない。
⑪機密性が高いサーバを廃棄するときには OS、ソフトウェア、データとも完全に消去しなければならない。

３．DNS 管理

①マスターとスレーブの同期を定期的にチェックしなければならない。
②DNS コンテンツサーバと DNS キャッシュサーバは分離して運用するほうが好ましい。
③対障害性を確保するため、DNS は異なるネットワークに分散配置するほうが好ましい。

４．アカウント管理

①パスワードの安全性を定期的に検証する。
②不要なアカウントは速やかに削除しなければならない。
③アカウント毎のアクセス数の統計を定期的（例　年１回）にとり、利用状況を把握しなければならない。

５．ファイアウォール管理

①基本ルールを変更するときは、情報センター長の許可を得なければならない。また、変更された基本ルールは情報センター委員会にて報告しなければならない。軽微な変更はこの限りではない。
②基本ルールは学内関係者といえどもむやみに公表してはならない。
③ファイアウォールの適用外となるホスト、サブネットワークについては「ファイアウォール適用外申請書」を情報センター長宛てに提出しなければならない。
④ファイアウォール適用外となったホスト、サブネットワークについては、セキュリティ上で堅牢であること

を確認するために不定期にセキュリティ診断するよう努める。
⑤ログについては、一定期間（例　一年間）保存しなければならない。

6．侵入検知システム管理
①最新の侵入方法にも対処できるように運用しなければならない。
②侵入が検知されたならば、必要な対処をとらなければならない。

7．メールゲートウェイウィルス駆逐システム管理
①最新のメール添付型ウィルスにも対処できるように運用しなければならない。
②駆逐の記録を、定期的（例　年１回）に集計しなければならない。

8．不正アクセス対策
①サーバなどのアクセスログを定期的（例　月１回）に分析し、不正アクセスを検知できるよう努める。
②セキュリティホールなどの情報収集に努め、ネットワーク管理者に対して適切な対処をするよう勧告しなければならない。
③学内にて不正アクセスなどの被害が発生した場合、学外の関係機関（JPCERT 等）に報告するよう努める。

9．トラフィック監視
基幹ネットワークのトラフィックを日常的に監視し、不正アクセスを示すような異常な状態があれば、原因を調査し、対処しなければならない。

１０．バックアップ管理
①データのバックアップは定期的（例　日１回）に取得しなければならない。
②システムのバックアップはシステム変更時には必ず取得しなければならない。
③バックアップは３世代以上を保持するよう努める。
④復旧作業については、年１回確認テストを行うよう努める。

１１．データ保管
①電子媒体には、第三者が重要性を容易に認識できるようにラベルに必要事項を記載しなければならない。
②利用しない時間帯（例　昼休み）は電子媒体などを机上に放置してはならない。
③秘密情報をパソコン内に保管するときには、暗号化を行うよう努める。
④秘密情報を記録した電子媒体は施錠可能な場所に保管しなければならない。

１２．データ破棄
秘密情報を記録した電子媒体を廃棄あるいは再利用するときは、情報を復元できないように完全に消去しなければならない。

Ⅱ　ネットワーク管理部門編

1．入退室管理
①サーバやネットワーク機器が設置されているマシンルームは通常は施錠しておかなければならない。
②入退室状況を記録するよう努める。

2．電子媒体配送
秘密情報、個人情報が記録された電子媒体は原則的に学外（自宅を含む）へ持ち出さない。持ち出さなければならないときは、暗号化しておく。

3．個人情報保護
①個人情報を当事者が参照するときには、当事者外の情報を参照されないように留意しなければならない。

例　学生に登録電話番号を確認するときに、他の学生の情報が参照できないよう配慮する。

②業務と直接関連しない用途に、電話番号や住所などの個人情報を利用してはならない。

③個人情報を電子媒体などで学内の部署に提供する場合は、所属長の許可を得なければならない。
また、所属長は個人情報の提供記録を保持しなければならない。
④個人情報を学外者に電子媒体などで提供する場合は、文書にて情報センター長の許可を得なければならない。
⑤個人情報が記載された帳票類が不要になったときは、シュレッダーなどにかけて廃棄しなければければならない。
⑥個人情報が記載された電子媒体のデータが不要になったときは、データを消去しなければならない。

4．サーバ管理
①サーバ管理をリモートで行う場合は、接続元のＩＰアドレスを限定しなければならない。
②サーバへログインする端末も十分な安全対策がなされたものを用いなければならない。業者には確認書を提出させる。
③不必要なサービスについては停止しなければならない。
④ＯＳやアプリケーションについては、常に脆弱性情報を収集し、高いセキュリティを確保しなければならない。
⑤重要性の高いサーバには無停電電源装置を設置しなければならない。
⑥利用可能なアカウントには必ず安全なパスワードを設定しなければならない。
⑦サーバから一時的に離れるときにもログアウト等の操作防止措置をしなければならない。
⑧Windows 系サーバはウィルス情報の更新は頻繁に行い、日常的にアンチウィルスソフトを稼動させなければならない。
⑨サーバでクライアントアプリケーションを実行することは極力避けなければならない。
⑩ウィルスやワームに感染した怖れがあるときには、まず、ネットワークから切り離さなければならない。
⑪機密性が高いサーバを廃棄するときにはOS、ソフトウェア、データとも完全に消去しなければならない。

5．アカウント管理
①パスワードの安全性を定期的に検証する。
②パスワード忘れに関する利用者からの問い合わせには、本人特定を必要とする。
メールや、電話による問い合わせには原則的には応じない。
パスワード通知に関しては問い合わせ者氏名、日時を記録しておく。
③不要なアカウントは速やかに削除しなければならない。
④アカウント毎のアクセス数の統計を定期的（例　年１回）にとり、利用状況を把握しなければならない。
⑤ネットワーク利用者のパスワード管理が不適切な場合は、厳しく指導しなければならない。

6．不正アクセス対策
①サーバなどのアクセスログを定期的（例　月１回）に分析し、不正アクセスを検知できるよう努める。
②セキュリティホールなどの情報収集に努め、ネットワーク利用者に対して適切な対処をするよう勧告しなければならない。

7．バックアップ管理
①データのバックアップは定期的（例　日１回）に取得しなければならない。
②システムのバックアップはシステム変更時には必ず取得しなければならない。
③バックアップは３世代以上を保持するよう努める。
④復旧作業については、年１回確認テストを行うよう努める。

8．データ保管
①電子媒体には、第三者が重要性を容易に認識できるようにラベルに必要事項を記載しなければならない。
②利用しない時間帯（例　昼休み）は電子媒体などを机上に放置してはならない。
③秘密情報をパソコン内に保管するときには、暗号化を行うよう努める。
④秘密情報を記録した電子媒体は施錠可能な場所に保管しなければならない。

9．データ破棄
秘密情報を記録した電子媒体を廃棄あるいは再利用するときは、情報を復元できないように完全に消去しなければならない。