A3202 電子メール利用ガイドライン

２００９年2月１２日制定

1. 目的

このガイドラインは、同志社大学情報システム利用内規に基づき、情報資産を保護し、電子メールの安全な利用に資することを目的とする。

2. 対象者

このガイドラインは、同志社大学ドメイン（doshisha.ac.jp）に属するメールドメインにて電子メールを利用するすべての利用者（以下「利用者」という。）を対象とする。 ＩＴサポートオフィスが提供する電子メールシステム（以下「本学提供電子メール」という。）のほか、外部プロバイダ、学部・研究科・センター等、及び教員個人が運用する電子メールの利用者についても、本ガイドラインに準じることとする。

3. 電子メールソフトウェアの設定

3.1 電子メール受信に係る設定

(1) ウイルス対策ソフトウェア等を利用し、ウイルス対策を行うこと。

(2) 偽のホームページへの誘導や、不正なスクリプトの実行を未然に防ぐために、受信した電子メールはテキストとして表示すること。やむを得ず HTML 形式を利用する場合は、HTML 形式のプレビュー機能を停止させること。

3.2 電子メール送信に係る設定

受信者側のセキュリティ水準低下を防止するために、HTML 形式の電子メールを作成しない設定とすること。

4. 電子メールに係る全般的な注意事項

4.1 利用目的

利用者は、電子メールシステムを、教育研究活動のために使用すること。

4.2 電子メールの自動転送

本学提供電子メールでは自動転送を認めている。要機密情報を送信する場合は暗号化すること。

4.3 証跡の取得

本学では、本学提供電子メールの他、電子メール全般の利用について、証跡を取得及び保存し、必要に応じて点検及び分析を行うことがある。

4.4 ウイルス対策、迷惑メール対策

本学では、電子メールに対して、ウイルス対策及び迷惑メール対策を行っている。これにより、電子メールの送受信に支障がある場合は、ＩＴサポートオフィスに相談すること。

4.5 ユーザ ID 及び電子メールアドレスの管理

(1) 他人のアカウント及び電子メールアドレスを使用してはならない。

(2) アカウント及び電子メールアドレスを他人と共用しないこと。

(3) 利用者は、電子メールを利用する必要がなくなった場合は、その管理者に届け出ること。

(4) 特定のサービス、職位、部門単位に付与されるアカウント及び電子メールアドレスのように、複数の関係者で共用したり、担当者が引き継いで使用する必要がある場合は、利用者は、許可及び設定についてその管理者に相談すること。

5. パスワードの管理

利用者は、パスワードを電子メールソフトウェアに永続的に保存しないこと。ただし、受信の都度パスワード入力を行うことが煩雑である場合は、電子メールソフトウェアに一時保存し、PC 起動後のみパスワード入力とする仕組みを利用してもよい。

6. 電子メールの受信

6.1 電子メールの受信確認

利用者は、定期的に電子メールの受信確認を行うこと。

6.2 電子メールのウイルスチェック

(1) ウイルス対策ソフトウェアによる自動ウイルスチェックを実施すること。
(2) 受信済電子メールの添付ファイルに対し、定期的にウイルスチェックを行うこと。これは、新種のウイルスに対応したパターンファイルの提供が間に合わなかった可能性を考慮し、最新のパターンファイルを用いて過去に受信した添付ファイルに対してもウイルスの有無を確認するための対策である。
(3) 電子メール利用によって、ウイルスに感染又は感染の疑いがある場合は、直ちに当該 PC をネットワークから切り離した後、ＩＴサポートオフィスに連絡すること。
(4) その他、電子メールに関連したウイルス対策で緊急対応が必要な場合は、当該電子メールシステムの管理者の指示に従うこと。

6.3 あて先間違いの電子メールを受信したときの対処

あて先間違いの電子メールを受信し、その内容から、送信者から正しい受信者へ再度送信する必要があると判断した場合は、可能な範囲で、送信者へあて先が間違っていたことを通知すること。通知した後は当該メールを削除すること。

6.4 不審な電子メールを受信したときの対処

(1) 不審な電子メールを受信した場合は、開かずに削除することが望ましい。
(2) 電子メールに不審なファイルが添付されていた場合は、当該ファイルを開かずに削除することが望ましい。
(3) (1)(2)に関わらず、受信した不審な電子メール又は添付ファイルの参照が必要な場合は、削除する前にＩＴサポートオフィスに相談すること。

6.5 迷惑メールの対処

(1) 必要以上に電子メールアドレスを公表又は通知しないことが望ましい。
(2) 電子メールアドレスを開示又は通知する場合は、自動収集されないように、工夫を施すことが望ましい。（画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等）
(3) 受信した迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性もあることに留意すべきである。

7. 電子メールの作成と送信

7.1 To、Cc 及び Bcc の利用

(1) To（あて先）、Cc（カーボンコピー）及び Bcc（ブラインドカーボンコピー）の総あて先件数は必要最小限とすること。
(2) 意図せず他人の電子メールアドレスを公開してしまうことを避けるため、同時に多数の人へ電子メールを送信する場合は、Bcc を利用するか、各自に個別送信すること。

7.2 電子メール１件当たりのファイル容量の制限

(1) 電子メール本文と添付ファイルを含めた総容量が 10M バイトを超えないこと。
(2) 電子メール本文と添付ファイルを含めた総容量が 10M バイトを超える場合は、別手段による提供や分割送信などの方法を採ること。

7.3 自動分割送信の禁止

自動分割送信された電子メールについては、ウイルスチェックが十分に機能せず、学内外のセキュリティ水準の低下の原因となるため、自動分割送信機能の使用は禁止する。

7.4 受信確認機能の使用制限

トラフィック増を防止するため、受信確認機能はやむを得ない場合を除き使用しないこと。

7.5 誤送信時の対応

電子メールを誤って送信した場合は、相手先（受信者）への対応は発信者が責任をもって行うこと。

7.6 ウイルスを送信したときの対処

誤ってウイルスを送信したことが判明した場合は、直ちにＩＴサポートオフィスへ連絡すること。

7.7 その他、電子メール作成及び送信時の留意事項

(1) 要保護情報を電子メールを用いて送信する場合は、「情報取扱ガイドライン」に定められた安全措置を講じること。
(2) 電子署名の付与、暗号化及び復号化に使用する鍵を適切に管理すること。
(3) 他人になりすまして電子メールを送信しないこと。
(4) 電子メールを転送する際に、作成者の許可なく内容の変更をしないこと。
(5) 個人情報やプライバシーの保護に配慮すること。

7.8 ネチケット

(1) チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。
(2) スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、ジャンクメール（役に立たない情報が書かれている電子メール）等を送信しないこと。
(3) 電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。
(4) 俗語的表現やあらかじめ定められていない省略語を使用しないこと。
(5) 機種依存文字を使用しないこと。
(6) 電子メールを作成する際、各行とも全角 30～35 文字程度で改行を入れること。
(7) To、Cc 及び BCC の使い分けを意識し、送信する電子メールに対する返事を要求する時には、To（あて先）を使用すること。

8. 電子メールの保存・削除

8.1 メールボックス（サーバ側）における電子メールの保存・削除

サーバの個人別メールボックスに格納される電子メールの保存期限、最大容量及びバックアップ状況等を考慮の上、不要な電子メールを削除し、必要に応じて PC へ保存すること。

8.2 メールボックス（PC 側）における電子メールの保存・削除

(1) 本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合は、暗号化等の措置を講じること。
(2) 本文や添付ファイルに要完全性保持情報及び要可用性保持情報が含まれている電子メールについては、適宜バックアップすること。
(3) 不要な電子メールは速やかに PC から削除すること。
(4) 本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合は、復元が困難な状態にすること。

9. 相談窓口

(1) 緊急時の対応が必要とされる場合は、ＩＴサポートオフィスに連絡し、指示に従うこと。
(2) このガイドラインの内容について不明な点がある場合は、ＩＴサポートオフィスに相談すること。

10. 事務

このガイドラインに関する事務は、企画部企画室情報企画課及び総務部庶務課が取り扱う。

附　則

このガイドラインは、２００９年４月１日から施行する。