事務用電子メール利用ガイドライン

趣旨

このガイドラインは，「金沢大学情報セキュリティポリシー」に基づき，金沢大学事務用電子メール(@adm.kanazawa-u.ac.jp，以下「電子メール」という。)を安全に利用するために必要な事項を定める。

電子メール利用の原則

利用者は，教育，研究，社会貢献，運営及びその支援以外の目的に電子メールを利用しないこと。

電子メールの利用環境

利用者は，必ずセキュリティ対策を施した情報機器から電子メールを利用すること。

電子メールの監視

利用者は，金沢大学情報セキュリティ対策基準「21．システム監視に関する基準」に基づいた監視が行われていることを了承した上で電子メールを利用すること。

電子メール登録の制限

利用者は，ニュースグループ，メーリングリスト等(メールマガジン，Web マガジン)への電子メール登録は，学習・教育・研究活動上必要なものに限定すること。

電子メールの作成と送信

To，Cc 及び Bcc の利用

- メールアドレスを To(あて先)，Cc(カーボン・コピー)に列記すると，当該電子メールを受信した者に他の受信者のメールアドレスが漏洩することになるため，学外の複数のあて先に電子メールを送信する際は，受信者各自に個別送信するか，他の受信者にメールアドレスが見えない Bcc(ブラインド・カーボン・コピー)により一斉送信すること。

電子メールの誤送信防止

- 電子メールを送信する際は，送信先メールアドレス，送信元メールアドレス，メール本文及び添付ファイルについて確認し，誤って送信しないように十分注意すること。
- メッセージ送信前に確認画面を表示する設定が可能な場合は，設定を行うこと。

添付ファイルの暗号化

- 添付ファイルを送信する場合には，ファイルにパスワード等の暗号化を行う必要性の有無を検討したうえで送信すること。

送信メールの形式の制限

- HTML 形式の電子メールを送信した場合，それを受信した側の情報セキュリティ水準の低下を招くおそれがあるため，原則として HTML 形式の電子メールを送信しないこと。

平成 29 年 5 月 29 日作成

電子メール 1 件当たりのファイル容量制限

- 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。
- 10M バイトを超える場合は，別の手段による情報提供（ファイル送信サービス※1 など）やファイル分割送信などの方法を検討すること。

その他，電子メール作成と送信時の注意事項

- 受信した電子メールを転送する際は，第三者へ公開すべきではない情報が含まれている場合があるため，内容及び相手先に十分注意すること。

電子メールの受信

受信メールの形式の制限

- 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ぎ，情報セキュリティ水準を高めるため，受信した電子メールをテキストとして表示することとし，特に HTML メールのプレビュー機能は使用しないこと。

不審な電子メールを受信したときの対処

- 日本語の言い回しが不自然であったり，送信元メールアドレスのドメインとメール本文に記載されたリンク先のドメインが異なっているなど，不審な電子メールを受信した場合は，パソコンリーダー若しくは情報化推進室に連絡・相談すること。

迷惑メールの対処

- 受信した迷惑メールに対しては，これを無視すること。送信者へメールの停止要求を出した場合，その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ること。

添付ファイルの対処

- 受信した電子メールの添付ファイルは，その機器に情報が保存されている場合があることを認識のうえ，適切に対処すること。

学外からのメールアクセス

- 原則として，公衆無線 LAN 環境からの利用はしないこと。
- 無線 LAN から接続する必要がある場合は，安全確保(VPN 接続サービス※2 など)に留意して利用すること。

※1 ファイル送信サービスは，総合メディア基盤センターがサービス（http://www.imc.kanazawa-u.ac.jp/service/sendfile/）を提供している。
※2 VPN 接続サービスは，総合メディア基盤センターがサービス(http://www.imc.kanazawa-u.ac.jp/service/vpn/)を提供している。

平成 29 年 5 月 29 日作成