D3252 電子メール、メッセージング利用ガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A3202 | 新規作成（電子メール手順） | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2007年10月31日  A3202 | 「電子メール利用ガイドライン」として、書式や表現を見直し | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3252 | 電子メールの利用実態に合わなくなった箇所の修正 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |
| 2019年12月27日  D3252 | 大幅改定及び文書名の変更 | 長谷川明生（中京大学） |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

**1. 本書の目的**

電子メールやメッセージング・サービスは日常生活において必要不可欠なものになっている。そのため、安全な方法で使用しなければ、ウイルス感染や情報漏洩等の原因となり得る。誤った方法による使用は学習・教育・研究活動の停止や社会的信用を失わせる要因となる可能性もある。

本書は、このようなリスクを軽減し、情報資産を保護し、電子メール等を安全に利用するための手引きである。

1. **2. 本書の対象者**

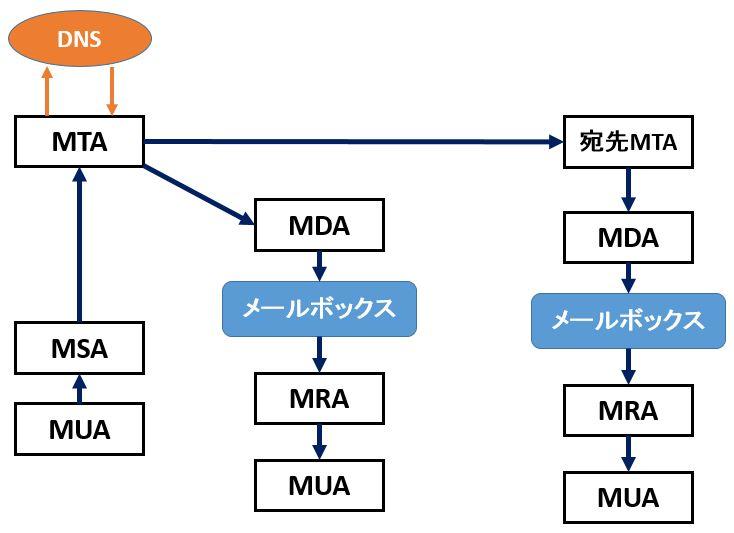
本書は、学内のすべての利用者を対象とする。

1. **3. 電子メールとメッセージング・サービス**

電子メールと各種メッセージング・サービスの大きな違いは、電子メールがインターネットでの汎用サービスなのに対して各種のメッセージング・サービスはサービス提供企業や企業団体の提供するサービスだという点である。メッセージング・サービスの多くでは、アカウントは専用ソフトウェアや機器の電話番号に結びついている。また、サービス提供業者をまたがってのメッセージのやり取りは保障されていない。それに対して、電子メールでは、インターネット接続提供業者のアカウントを利用するが、ソフトウェアも好きなものが選べ、相手に到達可能であれば世界中のインターネット利用者とメールをやり取りすることが可能である。

1. 3.1 電子メールの仕組み

インターネットで使われている電子メールシステムでは、利用者の使っているアプリやソフトウェアから送り出されたメールは複数の電子メールサーバを経由して、バケツリレー式に相手に届けられる。図1[[1]](#footnote-1)に、電子メールの送受信に関わるソフトウェアの関係を示す。



1. 図1　電子メールの伝送の概略
2. 表1 メール配送にかかわるサーバ

|  |  |  |
| --- | --- | --- |
| 略称 | 名称 | 機能 |
| DNS | Domain Name System | 名前からIPアドレスを検索する。 |
| MTA | Mail Transfer Agent | メールを相手のMTAに転送する。 |
| MDA | Mail Delivery Agent | MTAから利用者の郵便受けにメールを配送する。 |
| MRA | Mail Retrieval Agent | 郵便受けからMUAにメールを渡す。認証機能も持つ。 |
| MUA | Mail User Agent | メールを読み書きするソフトウェアやアプリケーションのこと |
| MSA | Message Submission Agent | MUAで作成されたメールを受け取りMTAに送り出す。 |

大学で電子メールを利用する場合には、メールの送信者や宛先としてのメールアドレスは、たとえば、user-id@example.ac.jpかuser-id@example.jpのような形式のことが多い。user-idの部分には職員番号や学籍番号が使われたりする。@マーク以降はメールを受け取るMTAの名前と思ってよい。

A大学の学生がB大学の友だちにメールを送ろうとしたとする。友だちのメールアドレスがt403212@example.ac.jpの場合、電子メール・アプリケーション(MUA、メーラー)でt403212@example.ac.jpを宛先としたメールを作成し「送信ボタン」を押すと友だちのアドレスの@以降のexample.ac.jpをキーにしてDNSでB大学のMTAのネットワーク上のアドレス(IPアドレス)を得る。MSAが宛先の最も近いMTAを選んで、そのMTAに中継を依頼する。友だちの大学のMTAはアドレスからt403212用のメールボックスにMDAを用いて受け取ったメールを書き込む。

メールを読む場合は、メーラーを起動すると、MRAを介して利用者を認証した上でサーバのメールボックスのメールを読む。

メールをウェブサービスとして扱える場合には、間にウェブサーバが必要となる。現在ではMTA-MRA-MSA-MUAの間の通信は暗号化されていることが普通であるが、MTAとMTAの間の通信の暗号化については期待できない。この場合、どこかで盗み見られる可能性があるので、重要なメールについてはメール本文を暗号化するといった必要がある。そのような手段としてS/MIME、PGPやGPGがあるが広く使われているとは言えない。

1. 3.2 電子メール・ソフトウェアの設定

メーラーの設定については以下の手順で実施する。

(1) 大学のサービスでは情報センターの指示にしたがって実施すること。ISPのサービスにおいては、ISPの指示に従うこと。

(2) メーラーの設定時に、必ず署名がメールに添付されるようにすること。また、表示名が付けられる場合には表示名を設定すること。

(3) 可能な場合には、ウイルス感染防止対策ソフトウェアを端末に導入し適切に設定しておくこと。

(4) 電子メールの自動転送設定を不用意に行わないこと。誤転送は情報漏洩につながる。また、転送先でメールの容量が大きすぎるといった問題で受け取れないといった問題がある。

1. 3.3 電子メール利用上の注意点

電子メールの利用にあたっては以下の事項に注意すること。

(1) メーラーには通常メールを送受信するためのidとパスワードを設定するが、その情報を漏洩しないこと。漏洩した場合、迷惑メールのばらまきに使われる可能性が高い。

(2) 差出時に宛先を間違えないように注意すること。アプリケーションの補完機能による宛先間違いが多く発生している。宛先間違いは情報の漏洩につながる。

(3) 心当たりのない差出人からのメールや、宛先が不審なメールは原則無視するか、注意して開封すること。

(4) 添付ファイルやURLは、ウイルス対策ソフト等で安全性が確認できなければクリックしたり開いたりしないこと。

(5) 大容量のファイルをメールに添付しないこと。

(6) 不用意にメールの転送をしないこと。情報漏洩につながる可能性がある。安易にメールの自動転送を設定しないこと。

(7) 同報メールについてはメールアドレスの漏洩をしないように注意すること。送信者のアドレスを宛先にし、BCCを利用するのが望ましい。CCの利用には細心の注意が必要である。必要に応じてIn-Reply-Toヘッダを活用すること。

(8) ファイルを添付する必要がある場合には、そのファイルが正しいものか、繰り返し確認すること。また、大きなファイルはクラウドストレージに置き、そのURLを送るといった配慮が必要である。

(9) 機密を要する情報のやり取りには電子メールは不向きな手段であるが、必要な場合には、機密を要する内容が含まれる添付ファイルに適切な暗号化処理を行うこと。暗号化せずに機密を要するファイルをメールやメッセージング・サービスで扱うことは不適切である。このとき、添付ファイルを暗号化するのに用いた暗号キーやパスワードを別のメールで送る方法は、両方のメールを盗聴された場合に情報漏洩につながるので推奨しない。対案として、あらかじめ送受信者で暗号化キーを決めておき、暗号化したファイルのみをクラウドストレージにおいて、メールでURLを伝える方法がある。

解説：メールアカウントの漏洩は、なりすまし、迷惑メール送信やパスワードリスト攻撃に利用される恐れがある。また、漏洩していなくても、迷惑メールの差出アドレスに利用されることもある。  
ウイルス感染防止と情報漏洩防止は強調しすぎることはない。電子メールでは、差出人等はソフトウェアで設定できるので、なりすましが可能である。受信者のアドレスを差出人と偽装した迷惑メールを送って金銭を要求するとか、受信者の電子メールのアカウント情報を詐取しようとする迷惑メールが後をたたない。

1. 3.4 電子メールの監視

電子メールシステムの適正な利用のため、その利用状況（あて先、内容、添付ファイル等）について、証跡の取得、保存、点検及び分析が行われる可能性がある。利用者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を実施していることを認識すること。

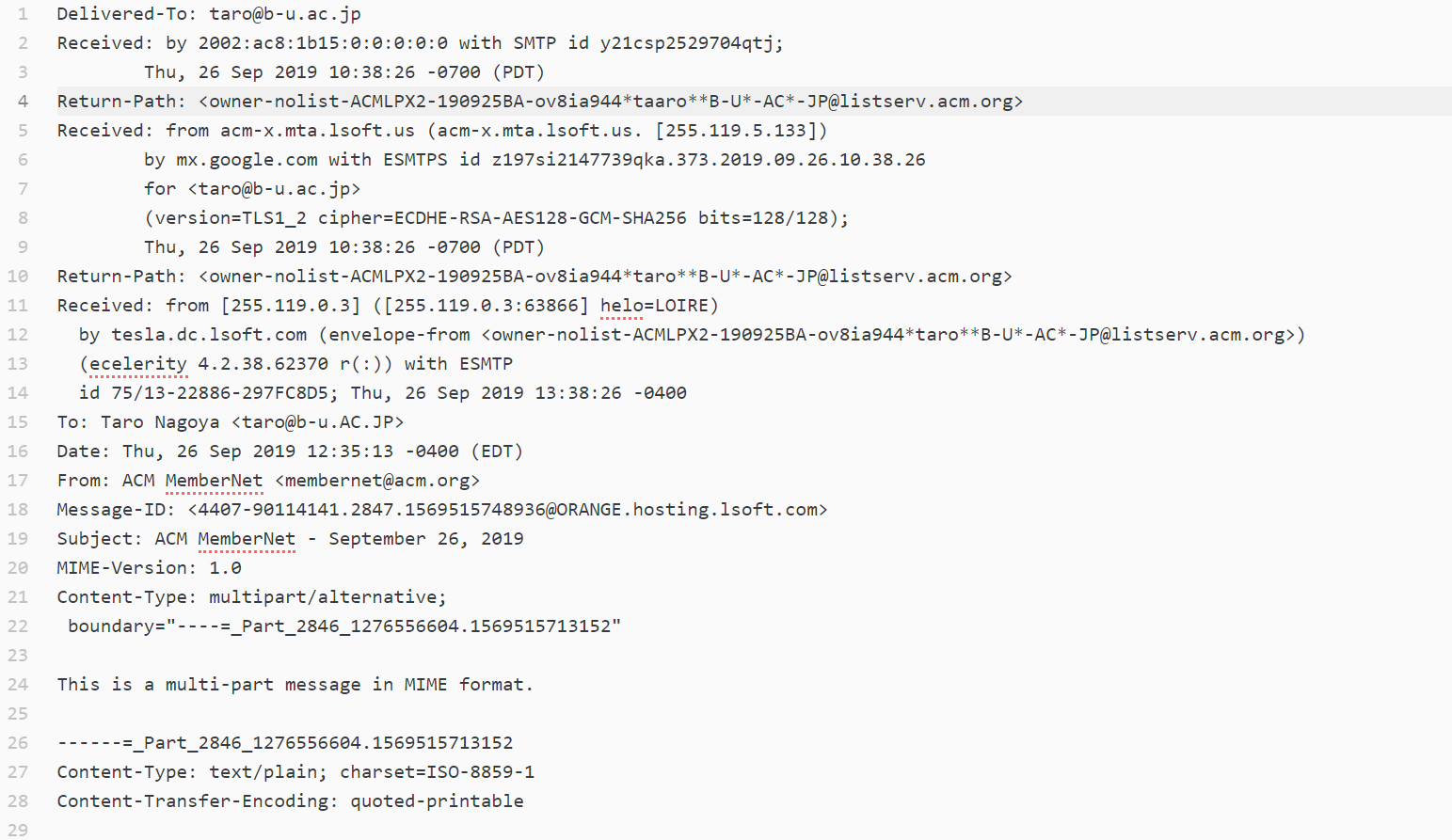
1. 3.4 電子メールのデータの読み方

現在では、電子メールをブラウザで読み書きすることが多くなっている。スマートフォンやタブレットでメールを読む場合には、差出人情報（From:）、宛先（To:）とメールの表題（Subject:）およびメール本文を見られる。これらの情報は、メーラーの設定で変更可能なもので、しばしば詐称されるので注意が必要である。

メールの送受信に関する詳細な情報は、パソコンのメーラーを使うと得られる場合がある。

以下の図に、あるメールのソースを示す。

スマートフォンやメーラーで表示される情報は以下の図の15行目から17行目と19行目のみのことが多い。本文は最初の空行（23行目）の後ろにある。



1. 図2　電子メールの例（冒頭部分の抜粋）[[2]](#footnote-2)
2. **4. 電子メールおよびメッセージング・サービスの脅威**

最近は電子メールやメッセージング・サービスを利用して詐欺や問題のあるホームページへの誘導しようとする案件が増えている。また、裁判所からの簡易裁判を装ったメールでの詐欺もある。電子メールを用いたものをフィッシング（phishing）、メッセージング・サービスのショート・メッセージを使う詐欺をスミッシング(smishing)と呼ぶ。以下によくあるものを紹介する。

1. 宅配業者の再配達通知を装い詐欺サイトやマルウェアのサイトに誘導するもの。出会い系サービスへの誘導もある。

2. 利用しているネットワーク・サービスを装い、不正侵入されたといって脅して、ID、パスワードや課金に関する登録情報の変更を促すもの。

3. 裁判所や架空の役所を名乗り、金銭を詐取しようとするもの。

4. 2段階認証用のキーコードをメッセージング・サービスで送り付け、偽のサイトに誘導し認証情報を窃取しようとするもの。

5. 宛先間違いメールをよそおったメールを多数回おくりつけて、間違い指摘メールを待って出会い系サイト等に誘導するもの。

このようなメールやメッセージは無視し、絶対に本文中のリンクをクリックしないことが肝心である。

1. 図1におけるMUA等はソフトウェアの略称である。表１にそれらについて簡単にまとめた。  
   詳細は次のページ等を参照されたい。http://www.denet.ad.jp/technology/2018/07/mailserverwords.html [↑](#footnote-ref-1)
2. メールデータの詳細な読み方については、迷惑メール相談センターのホームページに解説記事がある。URLは次の通り。

   https://www.dekyo.or.jp/soudan/contents/ihan/header.html [↑](#footnote-ref-2)