JPCERT CC®

電子メールソフトのセキュリティ設定について

第 1 分冊

- はじめに
- 本文書がカバーする電子メールソフト
- 電子メールソフトの設定に関する説明

一般社団法人**JPCERT**コーディネーションセンター
2011 年 **2** 月 **1** 日

本資料は、一般社団法人 JPCERT コーディネーションセンターのウエブサイトにて公開している「電子メールのセキュリティ設定」をPDFファイルにまとめたものです。
最新の情報に関しては、以下の URL を参照してください。

一般社団法人 JPCERT コーディネーションセンター
電子メールソフトのセキュリティ設定について
https://www.jpcert.or.jp/magazine/security/mail/index.html

1 はじめに

インターネットが一般に普及した現在、電子メールはインターネット利用者の大半が使うコミュニケーションツールとなりました。それに伴い迷惑メールが増加し、更にウイルスを配布するような攻撃にもしばしば利用されるようになってきました。

加えて近年では、今までの迷惑メールのような無差別な配布ではなく、特定少数を標的とした標的型メール攻撃と呼ばれる攻撃も散見されるようになってきています。

標的型メール攻撃において攻撃者は、企業情報、個人の Web ページや ブログ、メーリングリスト等から特定の個人情報等を入手し、知り得た情報をもとに標的とされた特定の組織向けにメール文面などをカスタマイズし、その会社の幹部社員などからの社内文書や、組織が関連している分野の資料を装ったメールを作成します。

攻撃者は、標的となったユーザがつい開いてしまうような電子メールを送付することによって、ユーザにメールに添付した文書ファイルなどを開かせ、そこに仕込んだウイルスを感染させることによって、情報を窃取したり、利用者の PC を乗っ取ったりするといった手法を用いるものが多く見られます。

このように電子メールが攻撃に利用される背景としては、電子メールには偽造されたり、内容を改ざんすることが比較的容易にできてしまう規格上の問題があります。このような問題を解決するための技術やサービスが提供されていますが、そもそもこのような事実が広く知られていないことから、対策が浸透していない状況にあります。

電子メールが広く利用されていることから、電子メールの偽造、改ざんといった問題や、迷惑メールへの対策が必要なことは言うまでもありません。特に、送信者の偽造や内容の改ざんは、電子メールを用いたコミュニケーションの根本的な信頼性にかかわる問題と言えます。

この問題に対処するために、例えば PKI や PGP を用いた電子署名を利用するなどのユーザ側での対策や、SMTP 認証を利用したサービス提供者側での対策などがあります。できる限りこれらの対策をとり、不正な電子メールに騙されないようにすることが重要です。

しかしながら、電子署名は導入の難しさからか比較的敬遠されやすく、また、あまり一般的でもないため、この対策を採用している組織は非常に少ないのが現実です。

このような現状の中で、ユーザとして「何に注意をして」、「どのように設定すればよいのか」を知ることは非常に重要です。 特に標的型メール攻撃は、突き詰めれば個人の傾向を理解した上での攻撃手法であることから、システムだけで完全に保護することはできません。 従って、電子メールの利用者側でも自分の身を護るために対策を行っていくことが重要です。

以上のような状況から、JPCERT/CC では電子メールの利用者が自分の身を護るための最低限の設定や確認事項を調査し、公開することにいたしました。

本文書を参考にして、皆さんが電子メールを用いた詐欺や攻撃を受ける可能性を少しでも減らすことができればと願っております。

2　本文書がカバーする電子メールソフト

本文書では以下の電子メールソフトを取り上げました。

電子メールソフト	バージョン
Apple Mail.app	3.5 (930.3)
Becky! Internet Mail	2.50.01
Microsoft Outlook Express	6.00.2900.5512 (xpsp.080413-2105)
Microsoft Outlook 2003	(11.8217.8221) SP3
Microsoft Outlook 2007	(12.0.6316.5000) SP1 MSO (12.0.6320.500)
Microsoft Windows Live Mail	2008 (Build 12.0.1606)
Mozilla Thunderbird	3.1.6
Gmail	-
Yahoo! メール	-

これらの電子メールソフトは、一般的に利用されており、特に Microsoft Outlook Express/Microsoft Windows Live Mail/Apple Mail.app は OS に標準で添付されているため、利用者が多い電子メールソフトとなっています。

※各電子メールソフトの手順中に使用している画像には、一部上記と異なるバージョンで取得した画像が含まれています。
その場合の該当箇所には、画像を取得した電子メールソフトのバージョン情報を記載しています。

3　電子メールソフトの設定に関する説明

電子メールソフトは利用者が頻繁に利用するものであるため、各電子メールソフトには様々な機能が実装されています。

ここでは、安全に電子メールを利用するための必要最低限の機能に関して簡単に説明を行います。

3.1　受信メール一覧で表示される情報の拡張

電子メールを取り扱うにあたり、受信したメール一覧の表示項目には、最低限以下を表示するべきです。

- 送信者の電子メールアドレス (From)
- 受信者の電子メールアドレス (To)
- 表題 (Subject)
- 送信日時 (Date)

これらの項目は、自分に届いた電子メールが迷惑メールや攻撃メールであるかどうかを判断する上で、基礎となる情報です。これらの情報を詐称する事も可能ですが、まずはこれらの情報を確認することが電子メールを安全に使用するための第一歩となります。

「受信メール一覧で表示される情報の拡張」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.2　送信者のアドレス表示

電子メールには本文の他に、「送信者」、「受信者」、「配送経路」等を含む、ヘッダと呼ばれる項目があります。

一般に、電子メールを利用する上で送信者の情報を確認することは重要です。

攻撃を目的とした電子メールでは、送信者情報を詐称することが多いため、送信者を確認したから安全とは言えませんが、攻撃を検知するための一助となることは間違いありません。

また、現在の電子メール規格では、送信者のメールアドレスの他に、「表示名」(display name)と呼ばれる付加情報を追加することができます。 多くの場合、表示名には本名やニックネームなどが使われていますが、表示名は送信者が任意で設定できることが出来るため、送信者を確認する際にこの「表示名」に頼り切ると、送信者の詐称を受けやすくなるという意味で両刃の剣と言えます。

送信者情報が詐称されている可能性を踏まえた上で、確認してください。

「送信者のアドレス表示」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.3 S/MIME 及び PGP 対応

電子メールは通常、暗号化や電子署名を行わずにやりとりされています。これは、電子メールを何らかの方法で、不正に受信し、内容を読んだり（盗聴）、書き換えたりする（改竄）することが可能であると言うことを意味し、盗聴による個人情報の窃取や、改ざんによる攻撃などが比較的簡単に行えてしまいます。

IETF では、このような状況に対応するために、S/MIME(RFC5750, RFC5751)及び、MIME の PGP 対応(RFC2015, RFC3156, RFC4880)に関する規格を制定しています。

S/MIME は PKI を利用した電子証明書を用いる手法で、公的個人認証基盤(いわゆる住基ネット)等で配られている個人証明書や、様々な証明書発行機関によって発行された個人証明書を利用して電子メールの暗号化や電子署名を行うことができます。

今回調査した電子メールソフトは、Becky!を除き全ての電子メールソフトがインストール直後から S/MIME を利用できます。また、Becky!も標準で添付されている Plug-In をインストールすることで S/MIME に対応できます。

一方、PGP 対応については、いずれの電子メールソフトでも標準では利用できません。実際には Windows Live Mail 以外の電子メールソフトは、Plug-In を導入することで PGP に対応できますが、本文書では取り扱いません。

本文書では、S/MIME、PGP 対応のどちらを採用すべきかに関しては論じませんが、電子メールを通じた被害を減らすためには、電子署名や暗号化を活用することが重要であると考えています。

「S/MIME 及び PGP 対応」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.4 迷惑メールフィルタ機能

迷惑メールの増加に伴い、一部の電子メールソフトでは、迷惑メール対策のためのフィルタ機能が組み込まれています。

この迷惑メールフィルタ機能は、受信した電子メールをふるいにかけ、迷惑メールを分離する機能です。

昨今、流通する電子メールの大半が迷惑メールであるとの報告があり、大量の迷惑メールを受信することによる作業効率の低下が問題となっています。迷惑メールフィルタ機能を利用することで、迷惑メールの処理時間の低減が期待出来ます。

なお、迷惑メールフィルタ機能は、迷惑メールを「完全に」分離してくれるわけではなく、迷惑メールと疑わしいと判定された電子メールを分離するものです。 従って、利用の際には、

- 迷惑メールではない電子メールが迷惑メールに分類されてしまう
- 迷惑メールが認識されない

という状況が発生することを認識した上で使用する必要があります。

「迷惑メールフィルタ機能」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.5 HTML メールの取り扱い

3.5.1 HTML メールとは

HTML メールとは、電子メールの本文が HTML（Hyper-text Markup Language）で記述された電子メールです。「HTML 形式のメール」とも呼ばれます。

HTML メールは、HTML の特徴である多彩な表現力を使用して、文字に装飾を施したり、文章に図や写真などの画像を組み込んだりすることが出来ます。HTML メールは、クリスマスカードやバースデーメールなどの個人間の社交的なコミュニケーションのために利用される他、企業からの広告案内や商品通知などにおいて、積極的に利用されています。

3.5.2 HTML メールを表示する仕組み

電子メールソフトは、一般的に HTML メールを表示するために HTML レンダリングエンジンを実装しています。電子メールソフトは、受信した電子メールのヘッダを解析し、HTML メールと判定した場合に HTML レンダリングエンジンを使用して HTML で記述された内容に従い、メールの内容を表示します。

主な HTML レンダリングエンジンと、各エンジンを搭載している Web ブラウザや電子メールを次に掲げます。

- Trident(MSHTML)：Internet Explorer、Outlook など
- Webkit：Safari、Apple Mail など
- Gecko：Firefox、Thunderbird など

例えば、Gecko と呼ばれる HTML レンダリングエンジンは、Web ブラウザである Firefox にも、電子メールソフトである Thunderbird にも、共通して使用されています。したがって、HTML レンダリングエンジンに起因する Web ブラウザの脆弱性が発見された場合、脆弱性の影響を受ける範囲は、同系の電子メールソフトにまで広がる可能性があります。

3.5.3 HTML メールの危険性

HTML メールには、以下のような問題があります。

一つは、これまでに電子メールソフトの HTML 表示機能に多数の脆弱性が見つかっていることです。

これまで、電子メールソフトの HTML メール表示関連処理には多くの脆弱性が発見されてきました。メールを閲覧するだけで PC がウイルスなどに感染してしまうため、HTML メールの表示（プレビュー）に関する脆弱性は特に危険度が高いのです。攻撃者が送信した HTML メールを閲覧したユーザの PC がウイルスに感染したという事例も過去に発生しています。

もう一つは、リンクが偽装されやすいことです。

HTML では、悪意をもった発信者が、もっともらしく見える表示に対して、まったく無関係なリンク先を対応付けることが出来ます。このため、HTML メール上では銀行の URL だと信じてクリックした受信者が、実際には攻撃者が用意したフィッシングサイトに誘導される可能性が高まります。

また、直接的な危険性ではありませんが、HTML メールを表示する際に Web サーバへのアクセスが生ずる場合（画像の読み込みなど）には、ユーザがメールを開いた事を Web サーバの運用者が確認出来るため、電子メール・アカウントが利用されていることや、ユーザの行動がトラッキングされてしまう可能性もあります。

<リンク偽装の事例>
以下の事例では、フィッシング対策協議会の URL が表示されているが、実際にクリックしたときにジャンプする先は、JPCERT/CC の Web サイトとなっています。

フィッシング対策協議会のサイトはこちら。
http://www.antiphishing.jp/

3.5.4 HTML メールの取り扱い

このように HTML メールは攻撃手段として使用される可能性があります。セキュリティを重視するのであれば HTML メールの受け取りは控えたほうがよいでしょう。 HTML メールを受け取った場合にも、以下のように電子メールソフトを設定して HTML メールとしての表示を抑制しておくことで、攻撃されるリスクを減らすことができます。

1) 電子メールソフトで HTML メールをプレビューしないようにする。

2) 電子メールソフトで HTML メールを送信しないようにする。

各電子メールソフトの設定は、以下を参考に実施してください。

もし、HTML メールを使用する場合は、その危険性を理解した上で、電子メールソフトのみならず OS、Web ブラウザの修正プログラムを適宜更新した上で利用してください。

3.6 添付ファイルの取り扱い

3.6.1 添付ファイルとは

添付ファイルとは、電子メールの本文に添付して送受信されるファイルです。

電子メールは、単体のテキスト・メッセージだけの送受信を前提として設計され、画像データや音声データなどのバイナリデータはテキストに変換して本文中に埋め込まない限り、電子メールで送受信することができませんでした。

電子メールの利用が拡大するのに伴い、そうした不便さを解消するため、1 つの電子メールのメッセージを複数の要素から構成できるような拡張が定義され、構成要素がバイナリデータである場合には、BASE64 や uuencode、Quoted Printable などといった方式に従って文字データに変換（エンコード）および復元（デコード）する方法が採用されて、画像やドキュメントファイルなど様々なファイルを手軽に送受信することができるようになりました。

3.6.2 添付ファイルの危険性

電子メールの添付ファイルは便利な機能ですが、ウイルスなどマルウエアの感染経路の一つともなっています。スパムメールにマルウエアが添付されている場合もあります。発信元に知人のアドレスが記載された電子メールのように見えても、第三者が知人のアドレスを騙って発信した可能性や、知人の PC がウイルスに感染していて添付ファイルも汚染されている可能性が否定できません。

添付ファイルにウイルスが含まれている場合、添付ファイルを開くことは、ウイルスが起動する契機を与えることになるため、添付ファイルの取り扱いには注意が必要です。

ウイルス等のマルウエアは、.exe や .scr などの実行形式ファイルだけでなく、Adobe Reader/Acrobat や Microsoft Office のデータ形式のファイルに埋め込まれていて、それらのアプリケーションの脆弱性を悪用して感染させようとする可能性があります。

また、安全なファイル形式とされている .txt などに拡張子を偽装した（電子メールソフトが認識する実際の拡張子とは異なる拡張子のように見せかけた）ファイル名が攻撃に利用されたケースもあります。

3.6.3 添付ファイルの取り扱い

添付ファイルをもつ電子メールを受け取った場合は、次の点に注意することが重要です。

- 知らない相手からの添付ファイルを開かない、もしくはメールを削除する

  知らない相手からの電子メールに添付されたファイルの安全性を確認することは容易ではありません。不審なメールにはウイルスが添付されていることが多いため、不用意に添付ファイルを開かないことが望まれます。

- 知り合いからの添付ファイルも不用意に開かないようにする

  電子メールの差出人は詐称することが可能であることやウイルス感染により意図せずメールが送信されている場合があるため、差出人が知り合いであっても、添付ファイルは不用意に開かず、メール本文や添付ファイル名を確認の上、少しでも不審に感じた場合は、添付ファイルを開く前に送信者に確認することが望まれます。

- ウイルス対策ソフトを最新の状態に保つ

  添付ファイルに既知のウイルスが含まれていた場合、ウイルス対策ソフトの定義ファイルが最新の状態であれば、誤って添付ファイルを開いてしまった場合でも感染を防げる可能性があります。このため、常に定義ファイルを最新の状態に保つことが望まれます。

- 使用している OS やアプリケーションを常に最新の状態に保つ

  添付ファイルに含まれるウイルスには、OS やアプリケーションの脆弱性を利用して感染を広げるものがあります。パッチなどが公開された既知の脆弱性を利用したウイルスの場合、基本的には OS やアプリケーションを最新の状態することで感染を防ぐことが可能です。このため、OS やアプリケーションは常に最新の状態に保つことが望まれます。

3.6.4 送信メールの形式

現在、様々な形式で電子メールを送付することが可能となっています。(例として、HTML、リッチテキスト等)

しかし、HTML メールの取り扱いで説明したとおり、この種の拡張されたメール形式は、場合によって攻撃に利用されることがあります。従って、受信者によってはこの種の電子メールに対し「受け取らない」・「読まずに捨てる」という扱いをする可能性があります。

ですから、特別なことがない限り、HTML メールやリッチテキストメールは送らないことが望ましいと言えます。

「送信メールの形式」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.6.5 開封確認機能

もともとの電子メールの規格では、電子メールを送信した後、受信者が配送された電子メールを読んだことを確認する術がありませんでした。 しかし、電子メールがビジネスなどでも利用されるようになり、受信者が電子メールを開封した事を確認したいという要望が増えたため、受信者が電子メールを開封したことを通知する開封確認機能が追加されました。

しかし、この開封確認機能は、「メールを読んだ（開封した）」という情報だけでなく、どこで読んだかなどの情報が漏洩してしまう可能性があり、セキュリティ的にはリスクを伴う物でもあります。

以上の理由により、どうしても必要な人を除いて、この機能は利用しないことが（現時点では）望ましいと考えられます。

「開封確認機能」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。