

電子メール利用時の 危険対策のしおり

電子メールを介したトラブル
こんな対策が必要です!!



IPA

独立行政法人 情報処理推進機構
セキュリティセンター

<http://www.ipa.go.jp/security/>

はじめに

電子メールは企業活動のみならず、個人利用においてもなくてはならないものになっています。ウイルス対策ソフトやスパムメールフィルタリングソフトの普及により、電子メールを介したコンピュータウイルスや、迷惑(スパム)メールに対する対策は、効果的に実施されています。ところが、最近では、電子メールの扱いが不適切なために発生する情報漏えい事故や、標的型攻撃(後述)による不審メールの安易な扱いによるウイルス感染や情報漏えいが発生しています。特に、企業活動においては、これらの問題が、企業の信用問題にまで発展する場合があります。

こういった問題に対処するためには、電子メールを扱う側でのセキュリティ意識の向上および基本的な対策が重要になっています。

本対策のしおりでは、以下の内容について解説します。

- ❖ **電子メールの誤送信防止のために**
 - 誤送信防止のためのメーラーの設定
 - メール暗号化(添付ファイルの暗号化)
- ❖ **コンピュータウイルスや標的型攻撃から身を守るために**
 - メーラーのセキュアな設定
 - 標的型攻撃
 - 不審な電子メールの取り扱い



1. 電子メールの誤送信防止のために

電子メールの誤送信による主な情報漏えい事故は、以下に示す事例が多いようです。

- ❖ 宛先間違いにより発生する事故
- ❖ 同報メール*1の送信方法の誤りによるメールアドレス漏えい事故

*1) 同報メールとは、まったく同じ内容の電子メールを、複数の受信者に対して一斉に送信するメールのことです。

前者については、電子メール利用者の不注意が原因であることが多いようですが、後者は電子メールの扱いに関する不慣れが原因となることが多いようです。どちらの場合も、電子メールの宛先に関する問題であり、利用者が注意すれば防げる問題です。

- ❖ 電子メール送信前に、宛先や内容、添付ファイル有無の再確認を行う
- ❖ TO、CC および BCC の使い方を理解する(ルール化する)
- ❖ さらに、問題の発生を少なくするためにメールを暗号化する

こういった対策が効果的です。

💡 電子メール送信前の宛先などの再確認

■ Microsoft 社の Outlook Express の場合

例えば、Microsoft 社の Outlook Express を例にとって解説します。

電子メールを作成し、メール作成画面で送信ボタンを押下すると、即送信されるのが一般的な(初期)設定です。送信ボタンを押下する前に、宛先の再確認をすることが推奨されますが、心配な方は図1の設定をすることで、宛先の再確認にさらなるチャンスが生まれます。



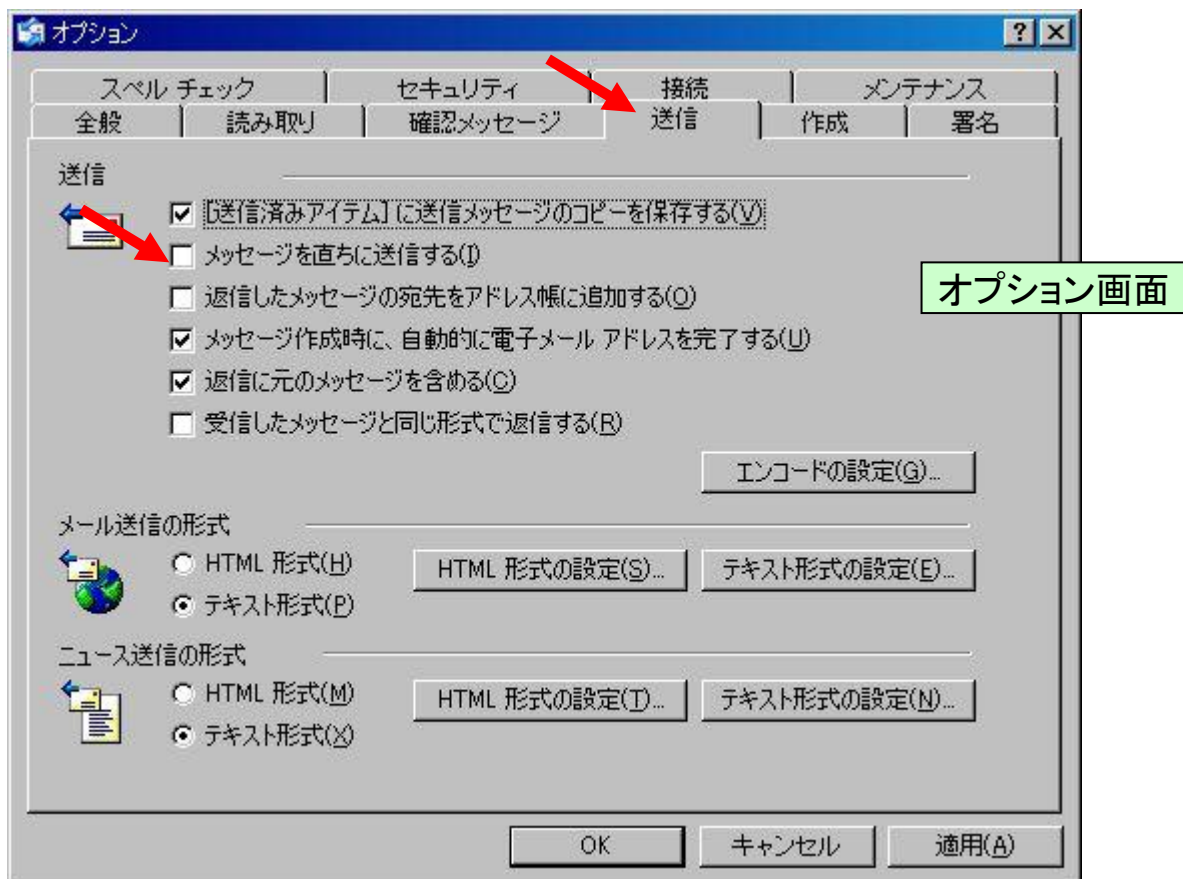
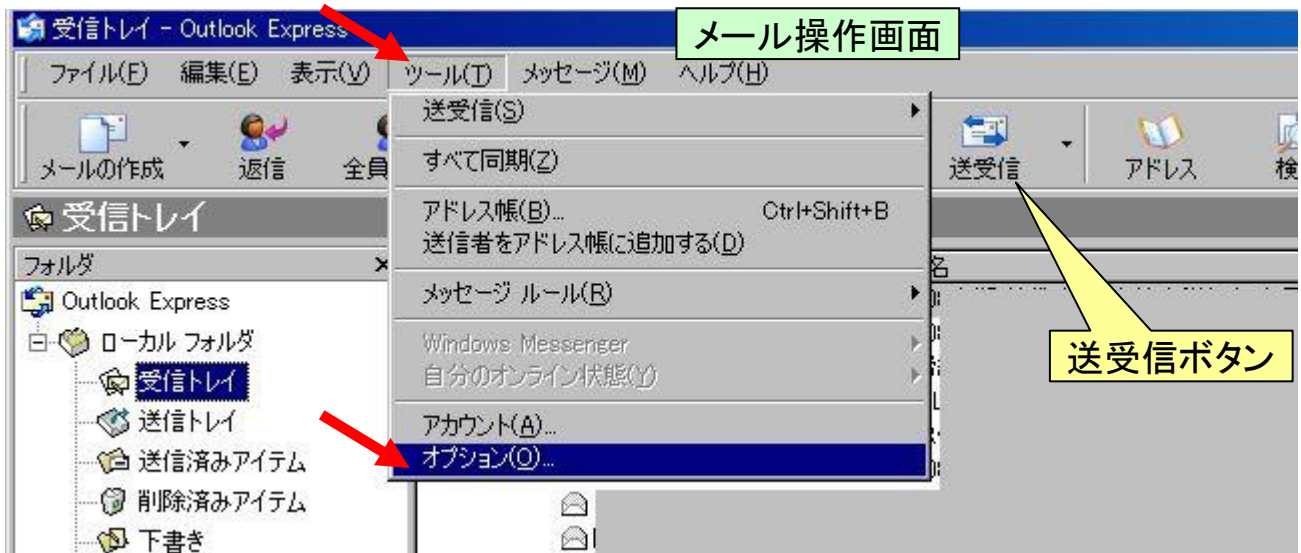


図1 宛先再確認のためのオプション設定

メール操作画面のツール→オプション→送信タブの「メッセージを直ちに送信する」のチェックをはずします(初期値はチェックされています)→OK ボタン(あるいは適用ボタン)。この設定により、メール作成画面で送信ボタンを押下しても、メールは即時送信されずに送信トレイに格納されます。つまり、送信トレイ上でメールの内容(宛先を含む)を再確認できることとなります。

実際のメール送信は、メール操作画面の送受信ボタンを押下することで実施されます。

■ Mozilla 社の Thunderbird の場合

Mozilla 社の Thunderbird の場合は、本体機能(設定)に即時送信を抑止するものではありませんが、送信前に内容の確認を促すアドオン*2が複数存在します。これらのアドオンを利用することで、送信前に宛先などの内容確認ができるので、再確認のチャンスが生まれます(アドオンの利用は自己責任となります)。

*2) アドオンとは、ソフトウェアに追加できる拡張機能のことです。Mozilla 社の Thunderbird は OSS(オープンソースソフトウェア)のため、多くの開発者によるアドオンが充実しています。

アドオンの例:

Check and Send : <https://addons.mozilla.org/ja/thunderbird/addon/2281>

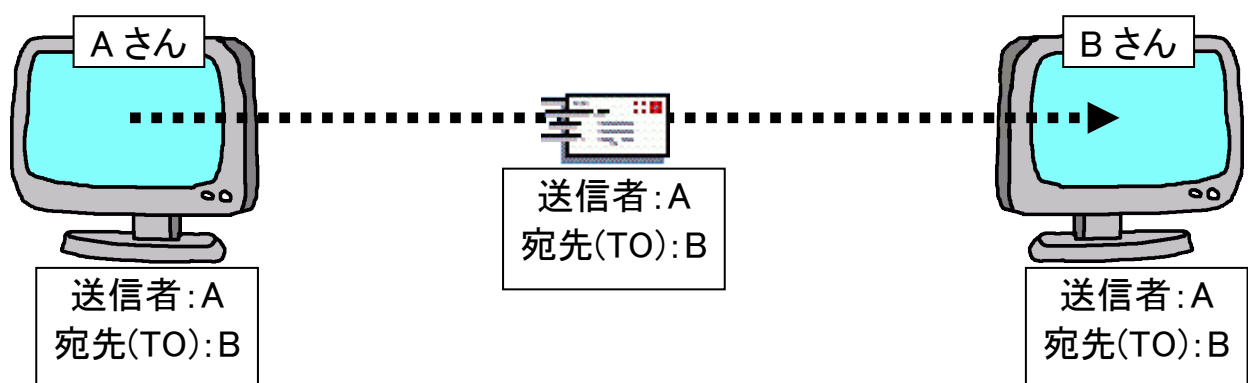
Confirm-Address : <https://addons.mozilla.org/ja/thunderbird/addon/5582>

など

💡 TO、CC および BCC の使い方

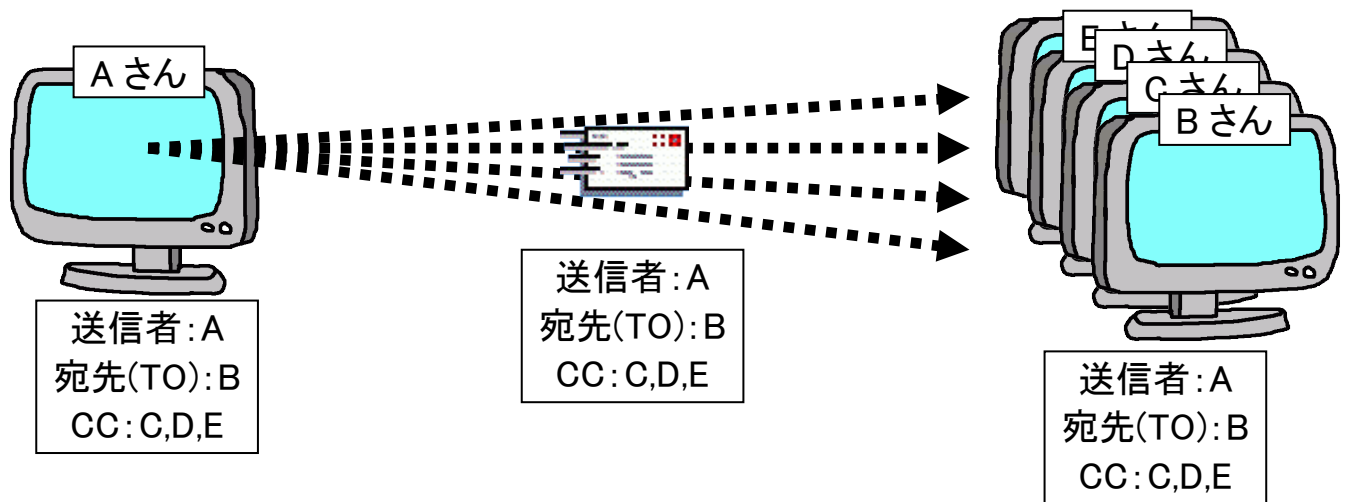
電子メールでの宛先指定には、TO 指定、CC 指定および BCC 指定があります。これも、Microsoft 社の Outlook Express を例にとって解説します。

TO による宛先指定は、電子メールの主宛先を指定するのが一般的です。特定の一人の宛先を指定する場合は、この TO 指定(Outlook Express では TO とは呼ばず、宛先と呼んでいます)を使います。



CC(カーボン・コピー)による宛先指定は、同一の電子メールを複数の宛先に同時に送信(同報メール)する場合に利用します。例えば、同じ企業内の複数の社員宛に、同じ内容の電子メールをそれぞれ送信するのは面倒なので、この CC 指定で複数の社員を指定することで、同じ内容の電子メールを一度で送信することができます。すべての送信先を TO に指定することもできますが、電子メールを送受信す

るメールサーバあるいはメールプロバイダーによっては宛先(TO/CC)の数に制限がある場合があるので注意してください。

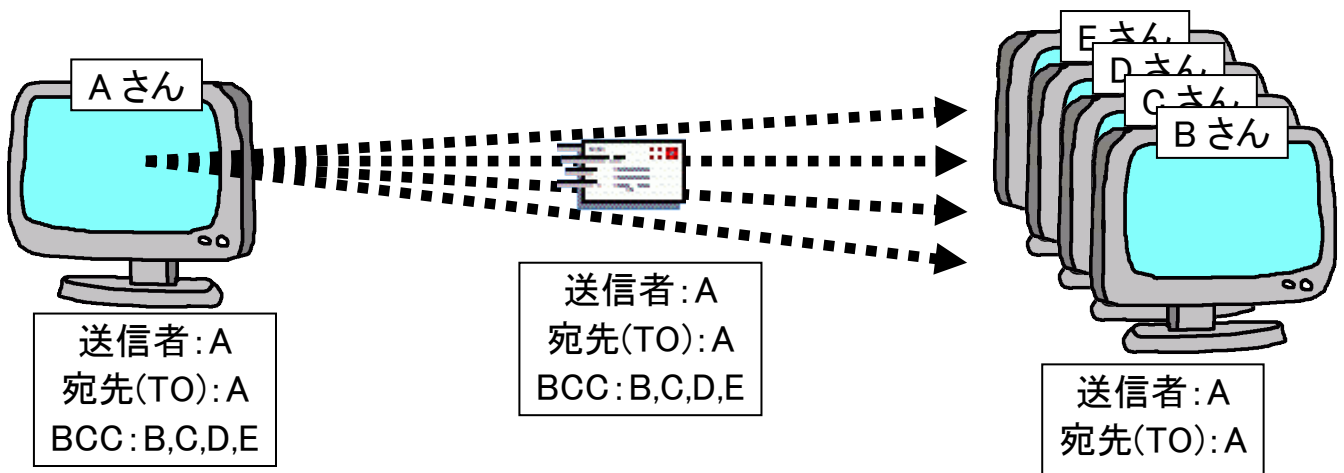


ここで、注意すべきは、Bさん、Cさん、Dさん、Eさんにはまったく同じ内容で、Bさん宛ての電子メールを、Cさん、Dさん、Eさんにも送信したことが、Bさん、Cさん、Dさん、Eさんすべてに分かるようになってきていることです(TOをBさんにした理由は、Bさんが主宛先のためですが、TO指定をしないとOutlook Express上で宛先なしとなるのでウイルスメールや迷惑メールと誤解されないために主宛先である誰かを指定[複数指定もOK]します)。

このケースで、Bさん、Cさん、Dさん、Eさんが、それぞれお互いを知らない場合は、このような電子メールを送られると戸惑うこととなります。CさんはAさんを除く他の人にメールアドレスを知られたくないかもしれません。結果的に、この場合はメールアドレスの漏えい(個人情報の漏えい)となってしまいます。

そこでBCC(ブラインド・カーボン・コピー)による宛先指定が有効になります。

BCCによる宛先指定は、同一の電子メールを複数の宛先に同時に送信(同報メール)する場合に利用します。例えば、複数の顧客宛に、同じ内容の電子メールをそれぞれ送信するのは面倒なので、このBCC指定で複数の顧客を指定することで、同じ内容の電子メールを一度で送信することができます。



この場合は、Bさん、Cさん、Dさん、Eさんには、宛先 Aさんの電子メールが送信されます。Bさん、Cさん、Dさん、Eさんには、この電子メールの宛先が自分以外にもあることは通知されません(自分宛なのかも通知されません)。

少なくとも本当の宛先となったメールアドレスが、他の受信者に通知されないの
で、本文や添付ファイルの内容を除いて、前述のような宛先指定による個人情報
漏えいとなることはありません。

宛先(TO)に送信者自身を指定しているのは、CCを使用する場合と同じ理由
(TO指定をしないと Outlook Express 上で宛先なしとなるのでウイルスメールや迷
惑メールと誤解されることがあります)です。宛先(TO)、CC、BCCを指定する場
合は、宛先情報(メールアドレス)が必須だからです。

ちょっと裏ワザになりますが、宛先(TO)を自分自身にするのであれば、自分自
身のメールアドレスをアドレス帳に登録して表示名を工夫すると、明示的な宛先表示
にすることができます。例えば、表示名：“BCCによる同報メール”など。

(注意 1) BCC が使えない？

Outlook Express で一度も BCC を使ったことがない場合、あるいは Outlook
Express を初期状態でお使いの場合は、メッセージ作成画面において BCC を入力
する入力欄が表示されていません。BCC 入力域を表示するには、[メッセージ作成
画面]で「表示」→「すべてのヘッダー」にチェックを入れてください。

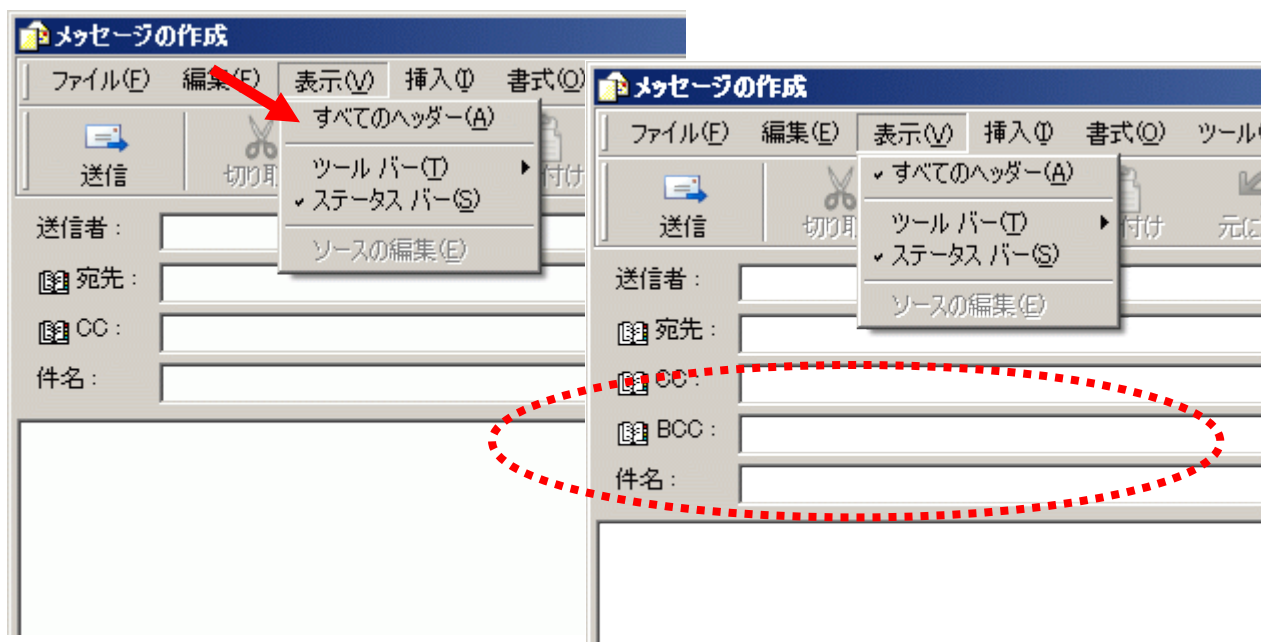


図 2 Outlook Express での BCC 入力域の表示

(注意 2) 送信済みフォルダのメールを見ても BCC の内容が見えない？

送信済みフォルダにある BCC を利用したメールを開いても BCC の内容は表示されません。BCC に指定したメールアドレスを確認したい場合は、[メール表示画面]で「ファイル」→「プロパティ」→[プロパティ画面]の手順にしたがって操作してください。ただし、プロパティ画面あるいはメッセージのソース画面で表示できる内容は、Base64 エンコード(符号化)されたものです。したがって、英語表記の部分(例えばメールアドレス部分)は読めますが、日本語表示の部分はデコード(復号)しないと読めません(どうしても日本語表示部分を見たい場合、デコードには圧縮・解凍ツールが利用できます)。

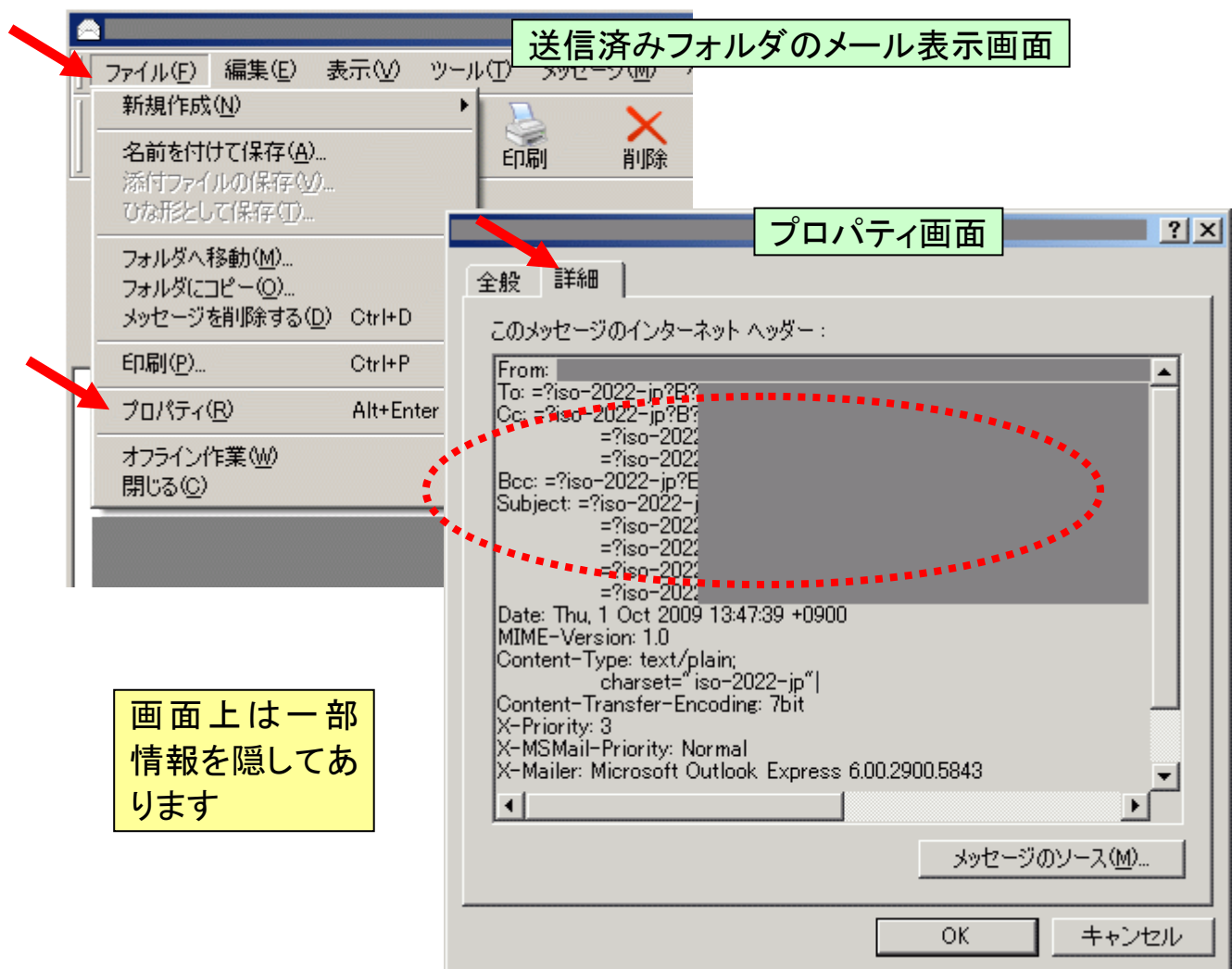


図 3 Outlook Express での送信済みメールの BCC 内容の確認

💡 メールの暗号化あるいは添付ファイルの暗号化

電子メールを安全に送受信するために、メールの本文や添付ファイルを暗号化することができます。

メール本文および添付ファイルを暗号化するには、暗号化のための専用ソフト (PGP^{*3}など) や環境 (暗号鍵) が必要となります。お手軽な方法として、添付ファイルのみをファイル暗号化ソフトやドキュメント作成ソフトに付属した暗号化機能、あるいは圧縮・解凍ソフトの暗号化機能によって暗号化する (パスワード保護する) ことも効果的です。

*3) PGP (Pretty Good Privacy) とは、アメリカの Philip R. Zimmermann を中心とした開発チームによって作られた暗号化ソフトで、世界的に標準化されているものです。

■ 公開鍵^{*4}を利用した暗号メール (高度な方法)

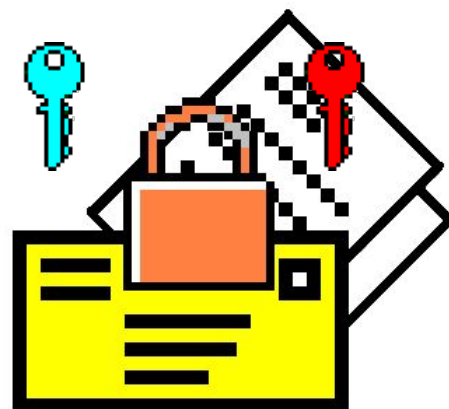
メールの宛先 (受信者) が暗号化のための公開鍵を公開している場合は、その公開鍵を利用してメールを暗号化します。公開鍵を公開している側にある秘密鍵 (公開鍵とペアのもの) がないと暗号メールは復号できません。つまり、受信者以外はメールの内容を見ることができないわけです。一般的には、PGP 機能として無償で提供されるソフトウェアを利用しますが、この方式を利用したメール暗号化ソフトも製品としてあります。

鍵管理が伴うので、あまり一般利用されていませんが、確実な方法であることは間違いありません。

*4) 公開鍵は暗号化のための鍵となるもので、ペアとして生成された秘密鍵とセットで利用されます。公開鍵で暗号化したものはペアとなる秘密鍵でしか復号できません。

■ パスワード (共通鍵) を利用した暗号メール

電子メールの送信側と受信側が、暗号化のための同じ鍵 (パスワード) を持っていれば、そのパスワードを利用して暗号化したメールをやり取りできます。一般的には暗号化の際に自動的に共通鍵とパスワード生成する方式のメール暗号化ソフトも市販されていますので、こういったものを利用することもできます。



■ 添付ファイルのみ暗号化したメール

メールそのものの暗号化とはいえない方法ですが、添付ファイルとするドキュメントを事前に暗号化しておき、メール送信で添付する方法が、お手軽です。

復号のためのパスワード等は、別の通信手段を利用して相手に伝えることが重要ですが、ドキュメントを暗号化する方法は、市販ソフトを利用したり、ドキュメント作成ソフトウェア (Office 製品等) や圧縮・解凍ソフトが用意している暗号化 (パスワード保護) 処理を利用することができます。

この方法でも、重要な情報を誤送信したとしても、復号のためのパスワードがなければ情報漏えいの被害を起こさないの、効果的です。

例えば、Microsoft 社の Office 2003 Word を利用しているならば、以下のように暗号化することができます。

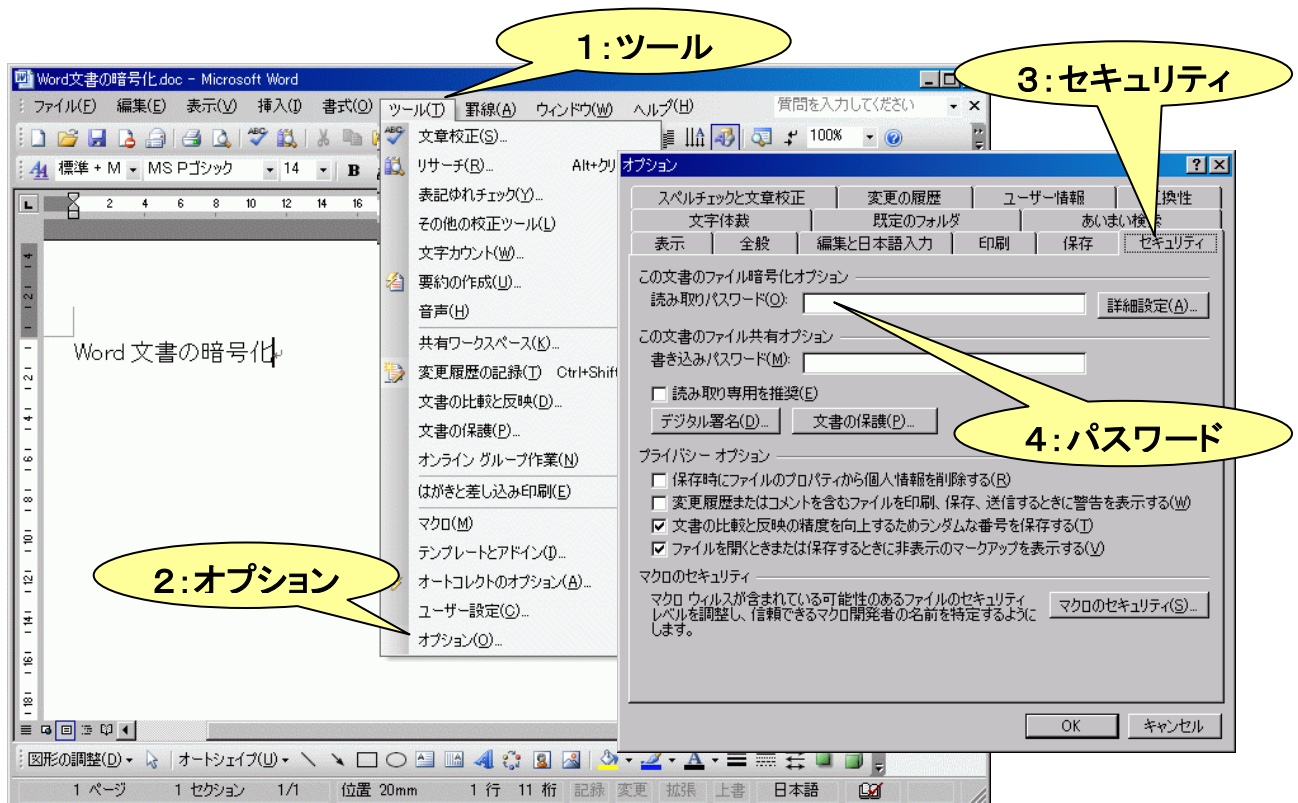


図 4 Office 2003 Word でのファイル暗号化

また、Microsoft 社の Office 2007 Word を利用しているならば、以下のように暗号化することができます。

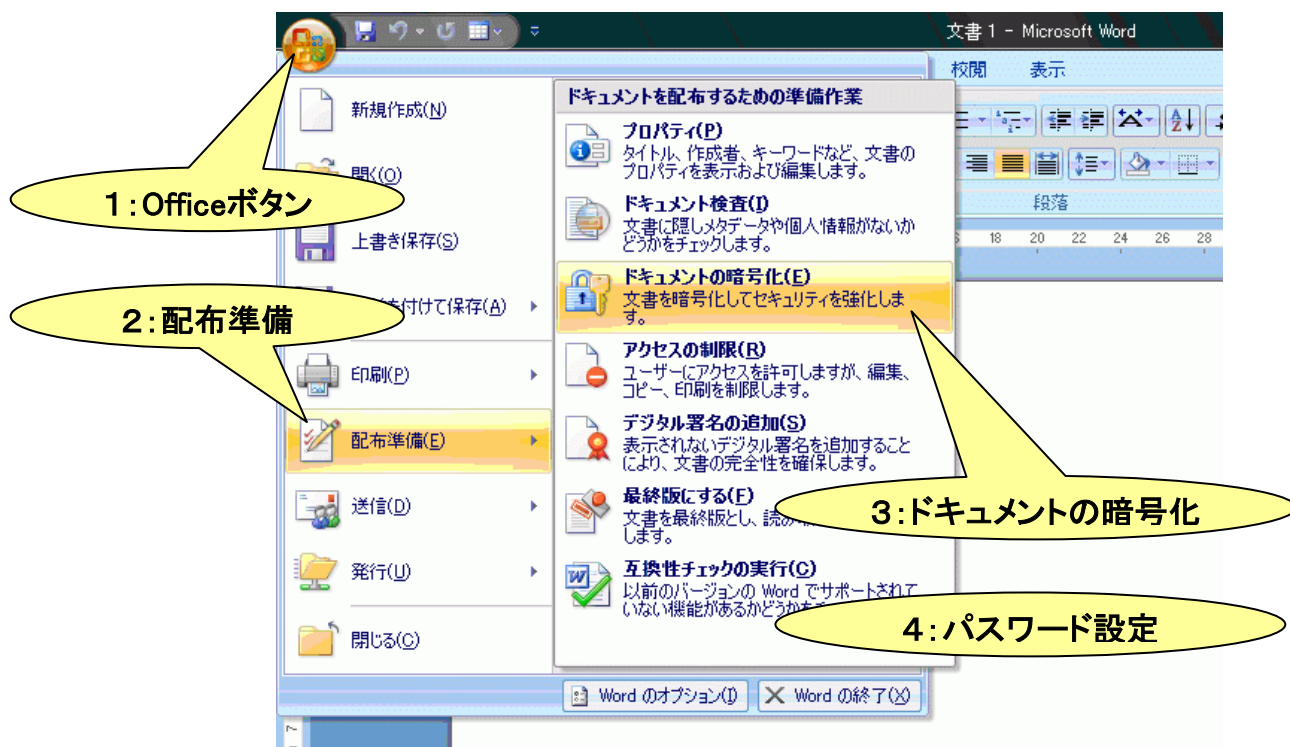


図 5 Office 2007 Word でのファイル暗号化

さらに、Windows OS を利用しているならば、Zip フォルダをパスワード保護する方法 (Zip フォルダ内のファイルをパスワード保護) もお手軽です。

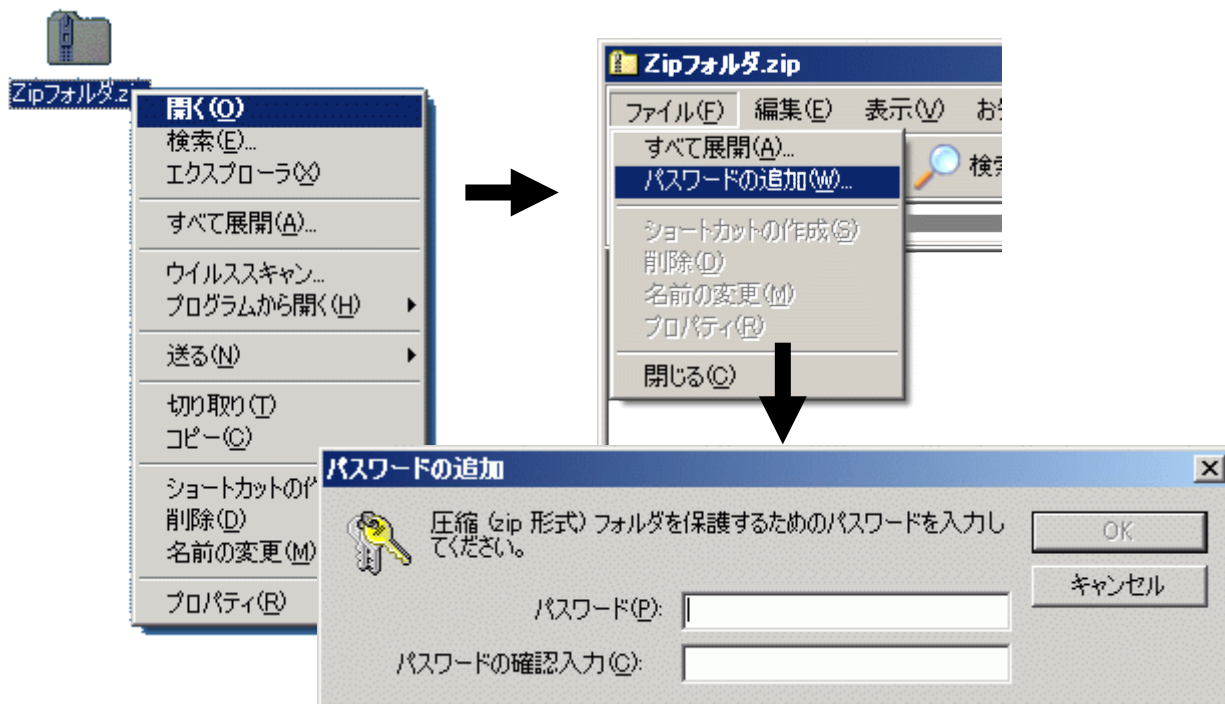


図 6 Zip フォルダ(フォルダ内のファイル)のパスワード保護

いずれの場合も、指定したパスワードを知らなければ、これらの文書ファイルや圧縮ファイル (Zip フォルダ) 内のファイルを開くことができません。

電子メールの暗号化は、誤送信防止のためというよりは、誤送信してしまった場合の防衛策となりますが、セキュリティ上は、電子メールや通信の盗聴などの不正アクセス対策にもなりますので、普段からいろいろ試しておくことが良いかもしれません。

さらに、ドキュメントや圧縮フォルダの暗号化(パスワード保護)は、電子メールの送受信のためだけでなく、ご自身のコンピュータ上の情報を守るための手段にもなります。お試しください。

2. Microsoft 社の Outlook Express のセキュアな設定

電子メールを安全に利用するために、Microsoft 社の Outlook Express を例にして、セキュアなオプション等の設定について解説します。また、Outlook Express は電子メールの内容を表示する際に、Internet Explorer の表示機能(エンジン)を使います。したがって、Internet Explorer のセキュリティ設定も強化することをお勧めします。

対象となるのは、インターネットオプション→セキュリティタブ→制限付きサイトで、このセキュリティゾーンのセキュリティレベルを**高**にすることです。関連項目については、後述の「**図 9 セキュリティオプションの設定**」を参照してください。

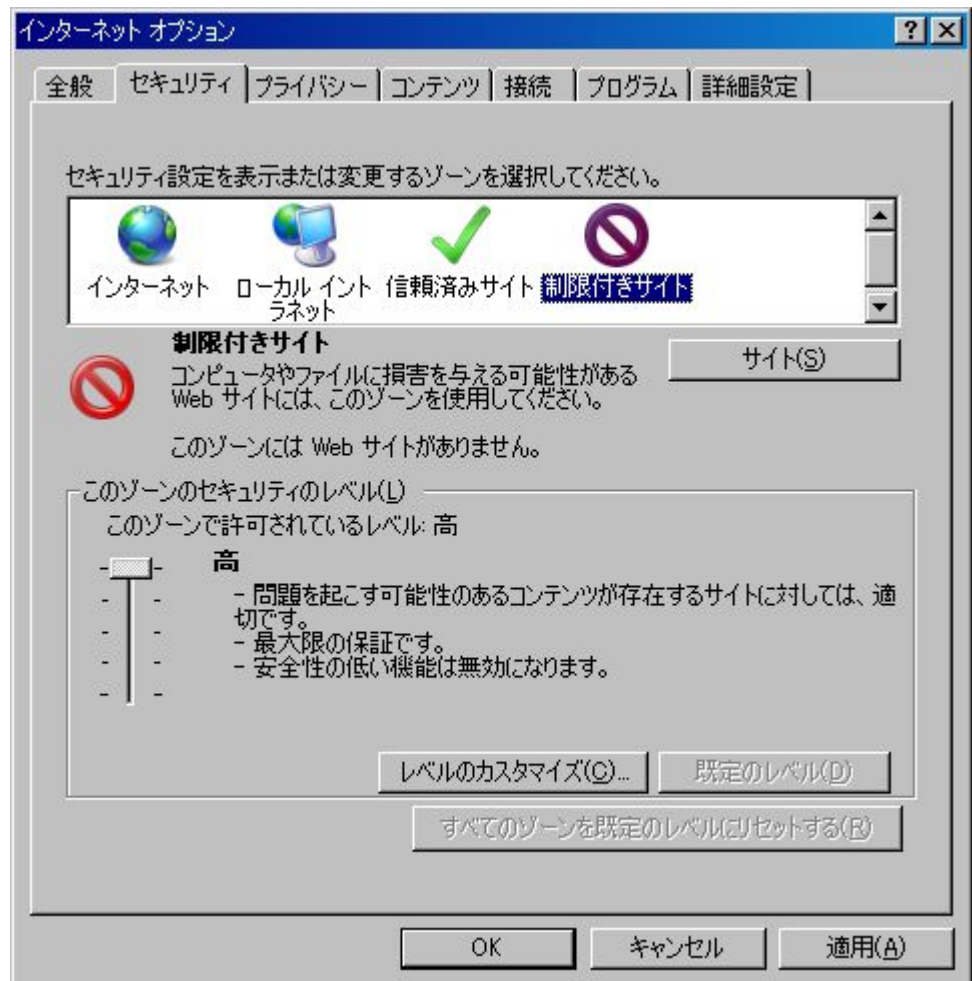


図 7 制限付きサイトのセキュリティレベルの設定

Outlook Express のオプション設定画面は、図 1 にも示してありますが、メール操作画面のツール→オプション(図 8)の通りです。

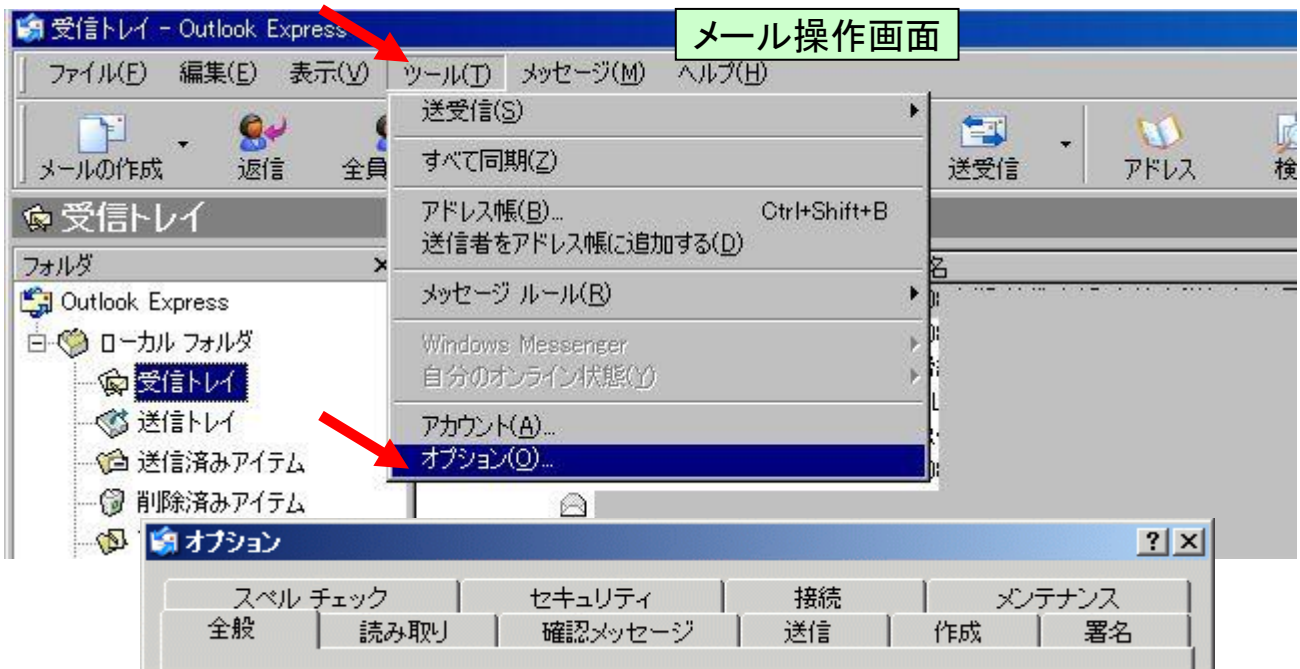


図 8 Outlook Express でのオプション設定画面の表示

オプション画面には複数のタブが用意されています(図 8)が、基本的なセキュア設定が必要なタブは以下の通りです。

- ❖ セキュリティ(オプション)
- ❖ 読み取り(オプション)
- ❖ 送信(オプション)

また、電子メールのプレビュー機能は抑止したほうが安全です。

- ❖ プレビューの抑止

(1) セキュアな設定のあらまし

Outlook Express を使用する場合のセキュアな設定のあらま시를以下に示します。

❖ プレビュー機能の抑止

受信した電子メールの安全性が保障されていない状態でのプレビュー機能はセキュリティ上好ましくはありません。そのため、プレビュー機能は抑止します。

❖ テキスト形式の送受信

メール本文をHTML形式にすると、メールの見栄えは格段に向上します。ところが、HTML形式の場合は、メール本文中にスクリプトを仕掛けることができます。このスクリプトが曲者で、悪意のあるスクリプトの場合は、メールを開いた際に、受信者の意図しない不正な処理が実行される恐れがあります。この脅威を少しでも緩和するために、メールの受信はテキスト形式で行う必要があります。また、メールを送信する際に、受信者が同じ設定をしていれば、受信者にとって安心できるテキスト形式で送信することがマナーと言えます。

スパムメールや広告メールでは、受信者の興味を引くためにHTML形式のものが多くあります。また、Outlook Expressには以前HTML形式のメールのプレビューや添付ファイルの処理で脆弱性があり、細工されたメールをプレビューしただけで、ウイルスに感染した事例もあります。このような危険性を未然に回避するためには、プレビュー機能を抑止するだけでなく、メールをテキスト形式で送受信することが重要になります。

見栄えがどうしても必要な場合は、伝えたい情報をドキュメント化し、受信者の同意の上、添付ファイル経由で行うことをお勧めします。

(2) セキュリティオプション

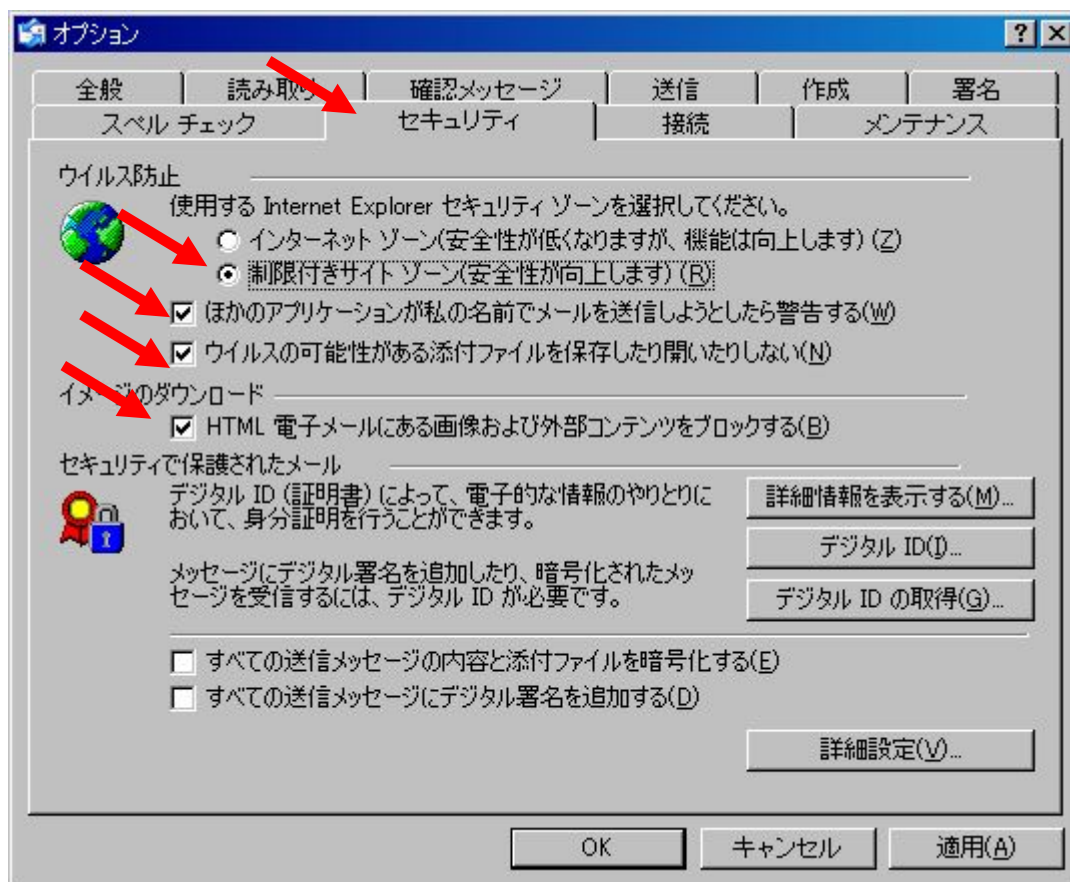


図 9 セキュリティオプションの設定

- ◆ セキュリティゾーンを選択は、『制限付きサイトゾーン』を選ぶ(詳細は後述)
- ◆ 『ほかのアプリケーションが私の名前でメールを送信しようとしたら警告する』にチェック
- ◆ 『ウイルスの可能性のある添付ファイルを保存したり開いたりしない』にチェック
- ◆ 『HTML 電子メールにある画像および外部コンテンツをブロックする』にチェック

(3) 読み取りオプション

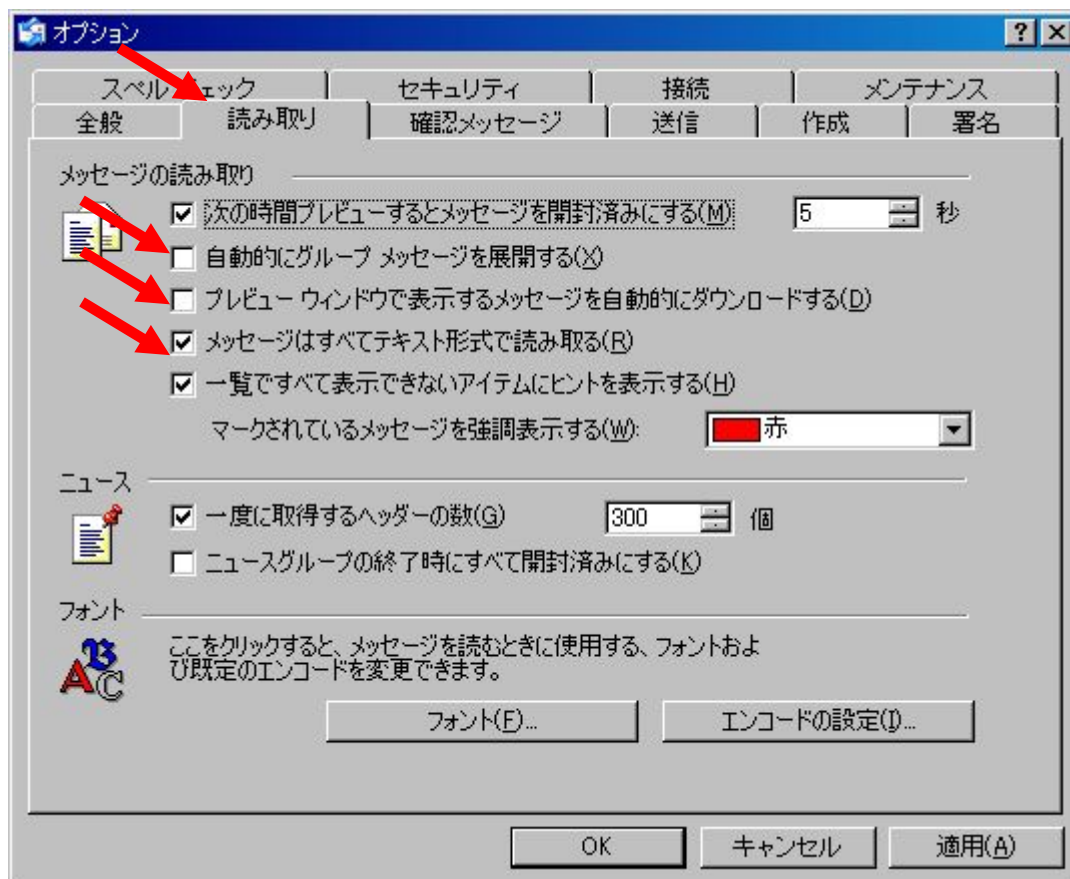


図 10 読み取りオプションの設定

Outlook Express のプレビュー機能はセキュリティ上利用しないほうが安全なので、関連する以下の設定を外しておきましょう。

- ◆ 『自動的にグループメッセージを展開する』のチェックは外す
- ◆ 『プレビューウィンドウで表示するメッセージを自動的にダウンロードする』のチェックは外す

また、メールの表示はテキスト形式が安全なので…

- ◆ 『メッセージはすべてテキスト形式で読み取る』にチェック

が有効です。

(4) 送信オプション

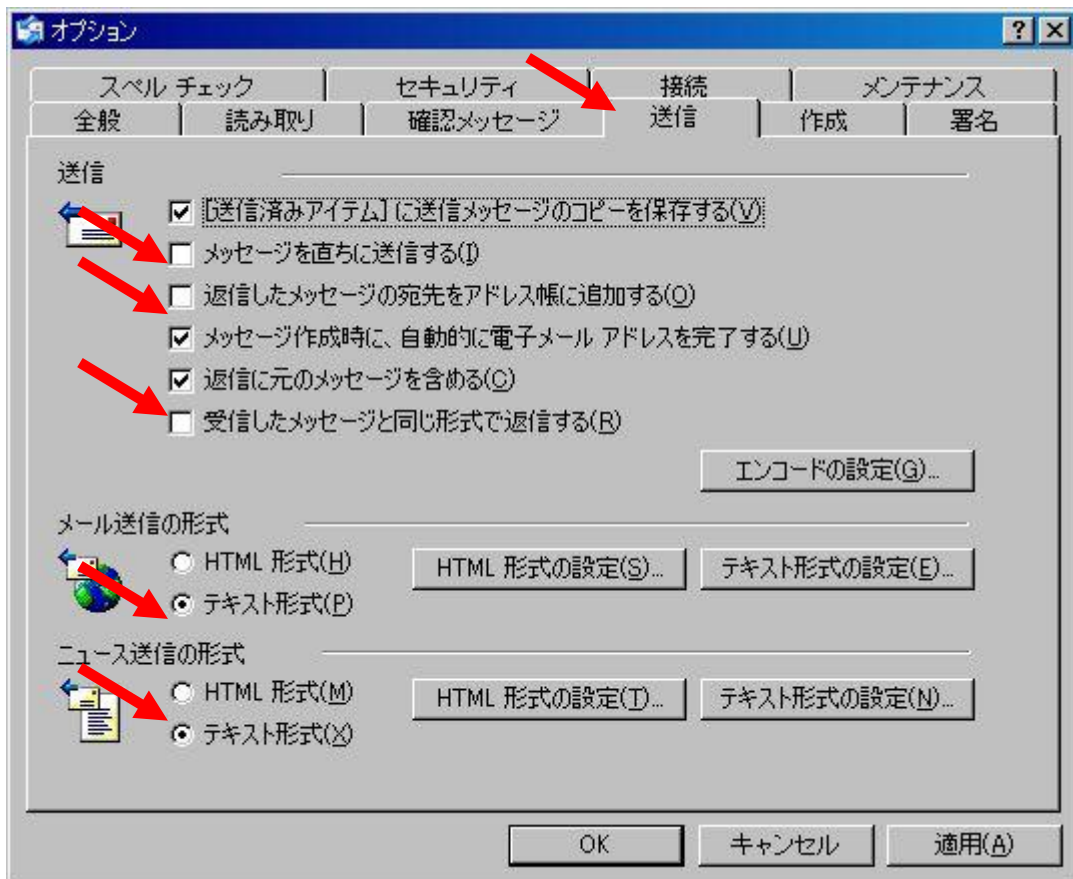


図 11 送信オプションの設定

まず、メールの誤送信を少しでも少なくするために…

- ◆ 『メッセージを直ちに送信する』のチェックは外す
- ◆ 『返信したメッセージの宛先をアドレス帳に追加する』のチェックは外す

また、メールの送信はテキスト形式で行うのがマナーなので…

- ◆ 『受信したメッセージと同じ形式で返信する』のチェックは外す
- ◆ メール送信の形式は『テキスト形式』を選択
- ◆ ついでにニュース送信の形式も『テキスト形式』を選択

(5) プレビューの抑止

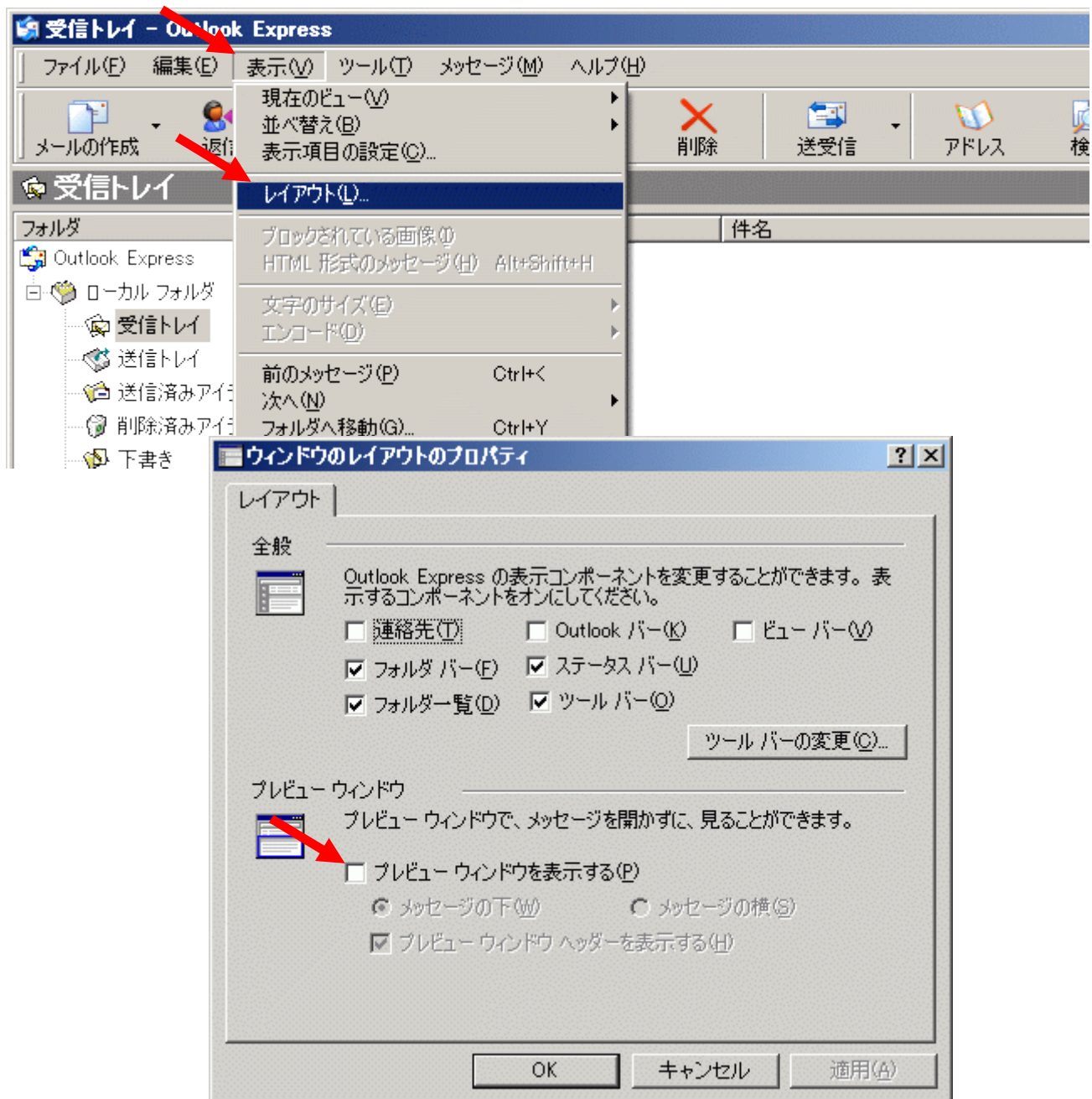


図 12 Outlook Express でのプレビューの抑止

前項でプレビューについて少し触れましたが、メーラーの脆弱性や出所不明のメールは開かないというメール受信の鉄則から、Outlook Express のプレビュー機能は抑止して下さい。

Outlook Express でプレビュー機能を抑止するには、表示→レイアウト→ウィンドウのレイアウトのプロパティで『プレビューウィンドウを表示する』のチェックを外します。

正直に言ってプレビュー機能は便利です。しかしながら、少しでも安全なメールの受信を心掛けるのであれば、機能を犠牲にするだけで安全性は向上します。世間では、Outlook Express は安全でない(新たな脆弱性の可能性)という言い方をする人もいますが、Outlook Express 以外のメーラーなら絶対に安全という保障があるわけではありません。しいて言えば、利用者が少ない分、狙われにくいという利点があるかも知れません。

Outlook Express 以外のメーラーを利用する場合は、Outlook Express の例を参考に、それぞれのセキュリティオプションの設定を実施してください。

締めくくりとしてはインパクトが弱いかも知れませんが、セキュリティ問題を意識し、以下に示す普段の警戒を怠らざれば、安全にメールを利用することができるでしょう。結局、普段の心掛けと言うことになるのでしょうか…

普段の警戒

- ➔ OS やアプリケーションの脆弱性に対するセキュリティ更新を常々確認し、必要なら適用する
- ➔ ウイルス対策ソフトによるウイルスの常駐監視を行う
- ➔ 出所不明のメールや怪しげなメールについては、開かない(プレビューもしない)

3. 標的型攻撃から身を守るために

標的型攻撃とは

標的型攻撃とは、主に電子メールを用いて特定の組織や個人を狙う悪意のある攻撃手法のことです。

典型的な例として、メール受信者の仕事に関係しそうな偽の話題等を含む本文や件名で騙し、添付ファイルのクリックを促すものが、数多く確認されています。

この場合の添付ファイルは、コンピュータウイルスそのものである場合や、脆弱性のあるアプリケーションを狙った悪意のあるコードが仕掛けられたファイルの場合が確認されています。このような添付ファイルを実行(開いて)してしまうと、ウイルスに感染したり、不正なコードが実行されることで、パソコンが乗っ取られたり、パソコン内の情報が漏えいする危険性があります。

標的型攻撃に利用された電子メールの事例を以下に紹介します。

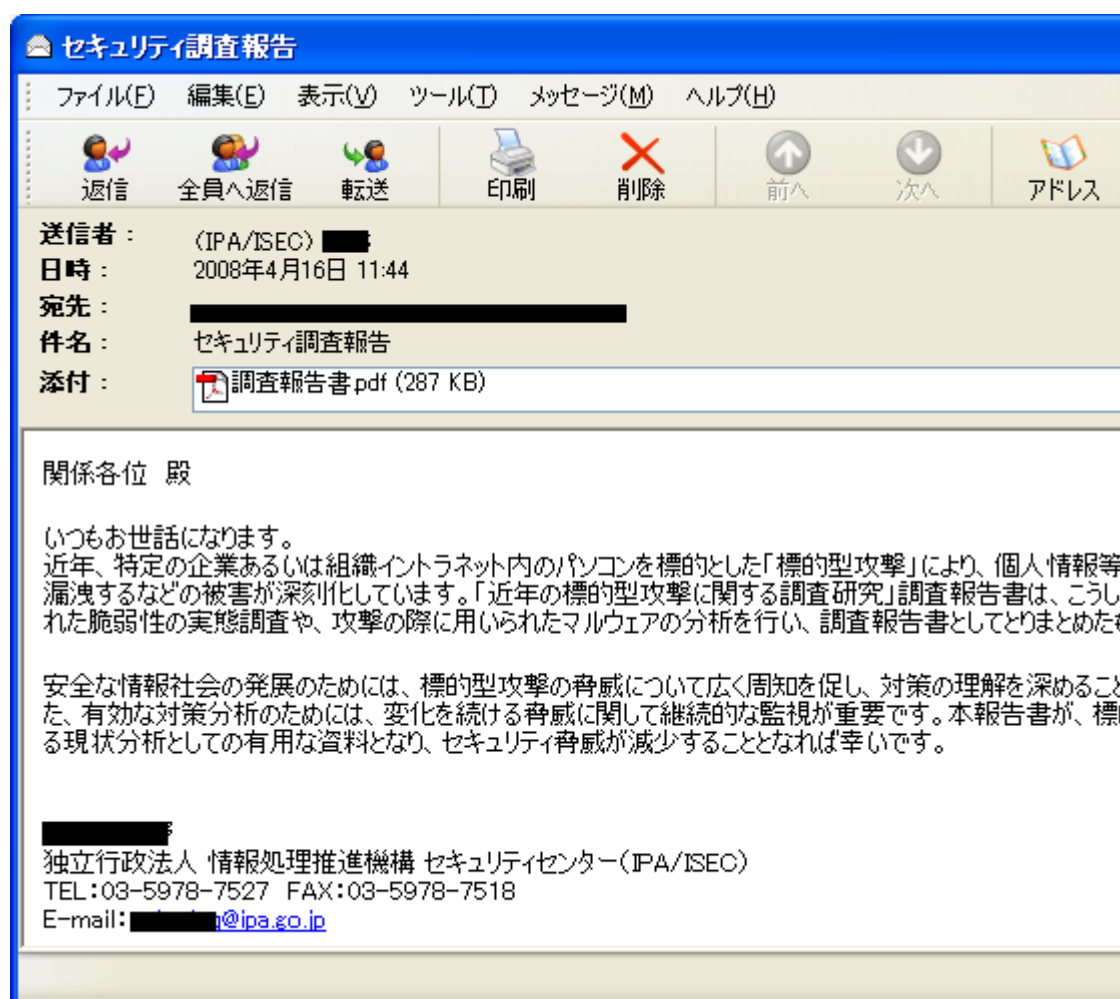


図 13 標的型攻撃に使われた電子メールの事例

この事例では、発信元として IPA を詐称しており、政府系のドメイン (go.jp) を持つ電子メールアドレスに対して発信されました。実際に、添付されていたファイルは古いバージョンの Adobe Reader で開くと不正なコードが実行される Adobe Reader の脆弱性を狙った PDF ファイルでした。

このように、相手を信用させて添付ファイルを開かせる手口ですが、セキュリティ意識の高い利用者でも信用させるほどの巧妙な騙しの方法といえます。

また、添付ファイルがないから安全かという、そうでもありません。HTML 形式を利用した電子メールや正規のウェブサイトの URL に見せかけた不正なウェブサイトに誘導する URL リンクをつけた電子メールにより、フィッシング行為を行うような標的型攻撃もありますので、注意が必要です。

標的型攻撃に対する予防策

企業や組織を狙った標的型攻撃に対する予防処置は…

- ◆ 不審なメールを開かない社員教育
- ◆ 不審なメールに関する情報共有
- ◆ ウイルス対策ソフトの正しい運用
- ◆ スпамメールのフィルタリング
- ◆ 何より OS やソフトウェアの脆弱性の解消

となりますが、不審なメールの見分け方としては…

- ◆ 日頃メールのやり取りのない企業からのメール
- ◆ 日頃メールのやり取りのない組織幹部からのメール
- ◆ 無料 Web メールアカウントからのメール
- ◆ 件名、本文、添付ファイル名の日本語が拙い、漢字の選び方が間違っているメール
- ◆ 本文中に部署や電話番号を記した署名がない(ここでの署名とは電子署名ではない) メール
- ◆ 件名に「緊急」など、ことさらに添付ファイル開封を促すメール
- ◆ 日頃メールでやり取りすることの無い種類のファイルが添付されているメール

一般社団法人 JPCERT コーディネーションセンター の
『標的型攻撃対策手法に関する調査報告書』より引用

http://www.jpCERT.or.jp/research/2008/inoculation_200808.pdf

が有効でしょう。

IPA では、最近増加していると言われている「情報詐取を目的として特定の組織に送られる不審なメール」に関して積極的に情報を収集し、予防・対処方法などの情報を提供することで、実被害が少なくなるよう、『情報セキュリティ安心相談窓口』を設置しています。

4. 情報セキュリティ安心相談窓口

<http://www.ipa.go.jp/security/anshin/>
コンピュータウイルスや不正アクセスの相談窓口

- ◆ 不審なメールを受信した場合は、送信者の組織に問合せで送信していないことを確認した上で、「情報セキュリティ安心相談窓口」にご連絡ください。
- ◆ IPA が当該不審メールを調査する必要があると判断した場合は、相談窓口の担当者が専用メールアドレスを連絡しますので、不審なメールを添付して送ってください。

☆電話による相談窓口

「情報セキュリティ安心相談窓口」の受付電話番号は
下記の URL をご参照ください。

<http://www.ipa.go.jp/security/anshin/>

※多くの方からご相談をいただく内容については、上記の「情報セキュリティ安心相談窓口」ページに「よくある相談と回答(FAQ)」の情報を掲載していますので、まずはそちらをご覧くださいませうお願いいたします。

その他、情報セキュリティに関して困った場合は、電子メールでもご相談を受け付けております。

E-mail : anshin@ipa.go.jp

※上記のメールアドレスは窓口専用となります。

このメールアドレス宛てに添付ファイル付きのメールを送られても、相談窓口側では安全確保のために添付ファイルを開きませんのでご了承ください。

(このメールアドレスに特定電子メールを送信しないでください)

不審なメールについて相談する場合は、把握できる範囲内で、次の項目を整理してからご連絡いただくと、すみやかに対応することができますので、ご協力をお願いします。

- (1) いつ届いたメールか
- (2) 送信者の組織名やメールアドレスと送信者への確認の結果
- (3) 使用しているウイルス対策ソフトと検知状況、ウイルス名
- (4) メール の 件名、添付ファイル名、本文
- (5) 同じメールが何人に届き、何人が添付ファイルを開いたか
- (6) 添付ファイルを開いた場合、どのような状態になったか
- (7) 実際にどのような被害が生じたか
- (8) 感染したパソコンのオペレーティングシステムとアプリケーションのバージョン
- (9) 当該メールのセキュリティ対策ソフトベンダ等への提供の可否について

5. 参考情報

■ 漏れたら大変！個人情報

<http://www.ipa.go.jp/security/kojinjoho/>

■ メール利用時のセキュリティ設定

<http://www.ipa.go.jp/security/personal/base/mail/>

■ 情報セキュリティ安心相談窓口

<http://www.ipa.go.jp/security/anshin/>

■ 近年の標的型攻撃に関する調査研究－調査報告書－

<http://www.ipa.go.jp/security/fy19/reports/sequential/>

■ 標的型攻撃対策手法に関する調査報告書

(一般社団法人 JPCERT コーディネーションセンター)

http://www.jpCERT.or.jp/research/2008/inoculation_200808.pdf

■ 情報セキュリティに関する新たな脅威に対する意識調査 2010 年版

<http://www.ipa.go.jp/security/fy22/reports/ishiki/>

■ 情報セキュリティ白書 2010 年版

<http://www.ipa.go.jp/security/publications/hakusyo/2010/hakusho2010.html>

■ 今月の呼びかけ

<http://www.ipa.go.jp/security/personal/yobikake/>

- 迷惑メールをはじめとした様々な経路で拡散する

新たなウイルスが出現！

<http://www.ipa.go.jp/security/txt/2010/10outline.html>

- 心当たりのないメールは、興味本位で開かずにはすぐ捨てよう！

迷惑メールから始まる様々な被害が増えています

<http://www.ipa.go.jp/security/txt/2008/09outline.html>

- 公的機関になりすましたメールに注意してください！！

<http://www.ipa.go.jp/security/txt/2008/05outline.html>

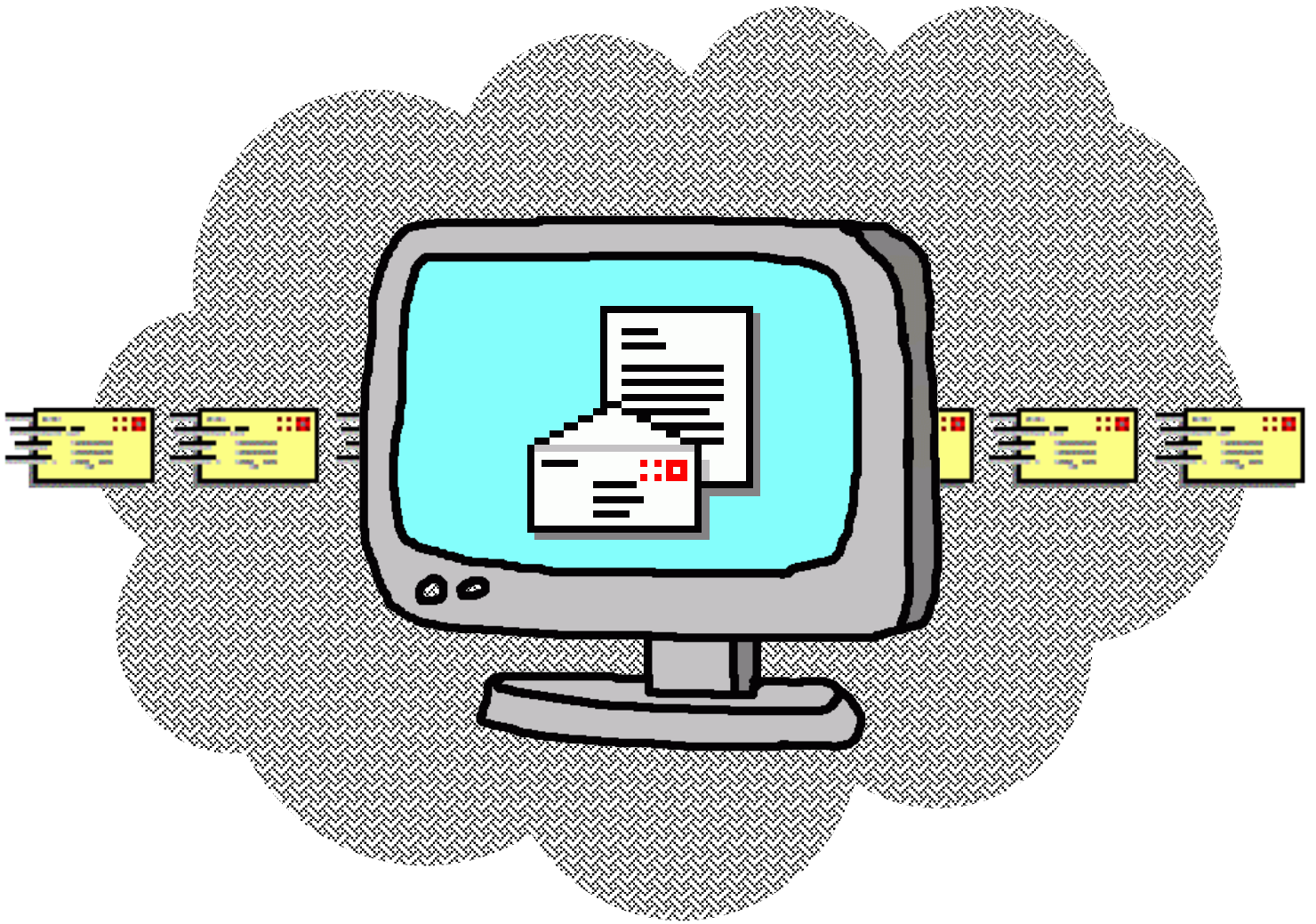
- 何かなあ？ 開いた時には、もう遅い

<http://www.ipa.go.jp/security/txt/2007/09outline.html>

IPA 対策のしおり シリーズ

<http://www.ipa.go.jp/security/antivirus/shiori.html>

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ対策のしおり



IPA

独立行政法人 情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
(文京グリーンコートセンターオフィス16階)

URL <http://www.ipa.go.jp/security/>

【情報セキュリティ安心相談窓口】(コンピュータウイルスおよび不正アクセス)

URL <http://www.ipa.go.jp/security/anshin/>

E-mail anshin@ipa.go.jp