FAQ

Frequently Asked Question

いまさら聞けない

いまだから聞きたい

このコーナーでは読者の皆さんのインターネットに関する疑問や質問にお答えします。「？」と感じたことはどのようなことでも構いませんので、下記のメールアドレスまでご質問ください。なお、ご質問へのメールでの回答はできませんのでご了承ください。

○ご質問はこちらまで
im-faq@impress.co.jp

今月のポイント

1 POP before SMTPとは？

2 ウェブサイトにクレジットカード番号や個人情報を登録しても本当に安全なのか？

Q

メールを送ろうとしても送れないときがあります。メールソフトを立ち上げた直後は送れるようです。どうすれば直りますか？（長野県 A・Kさん）

A

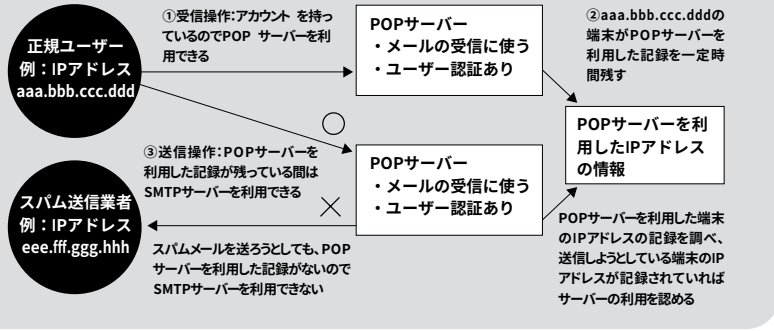
一度メールを受信する操作をすればメールを送れるはずです。これはメールサーバーの不正利用を防止する「POP before SMTP」という仕組みに関係しています。

メールサーバーには、ユーザー宛てに届いたメールを貯めておくPOPサーバーと、メール送信の処理をするSMTPサーバーの2種類の機能があります。POPサーバーへの接続にはユーザー認証の仕組みがあります。歴史的にSMTPサーバーは、正規ユーザー以外でも自由に利用できていました。しかし、第三者が勝手にSMTPサーバーを利用してスパムメールを送信する「メールの不正中継」URLが増えたために、現在は多くのプロバイダーが対策を施しています。その1つがPOP before SMTPで、これは文字どおり「送信（SMTP）前に受信（POP）する」方法です。具体的には、正規ユーザーがPOPでメールを受信するとそのIPアドレスが一定時間記録され、記録されているIPアドレス以外からはSMTPでメールを送れないというものです。この時間はサーバーごとに異なりますが、ほぼ10分前後です。この方法なら対応するPOPサーバーに正規のアカウントがないユーザーはSMTPサーバーを使ってメールを送信できません。メールソフトを起動した直後は自動的にメール受信操作をすることが多いため、最初はメールを送れるのです。

不正中継対策としては他にもRFC2554が定義するSMTP Auth（SMTP認証）という仕組みを使うこともあります。これはSMTPサーバーがユーザー認証を行う仕組みです。（山崎誠也）

メールの不正中継
URL http://www.jpcert.or.jp/ed/2001/ed010001.txt

●図1 POP before SMTPの仕組み



メール受信時の認証を利用して第三者のメール送信を防止する

Q ウェブショッピングなどで「通信が暗号化されます」「第三者に読まれることはありません」のように表示されますが、本当に安全なんでしょうか？（長野県　堀兼高志さん）

SSLによって通信経路上での盗聴を防ぎ、正しい相手と通信していることを確認

A

図2のような表示は、アクセスしようとしているウェブサイトが、サーバー証明書と呼ばれるセキュリティー技術を使用していることを示しています。このサーバー証明書は、ユーザーが正しいウェブサイトと安全な情報通信を行うために、2つのセキュリティー機能を提供するものです。

1つは、SSL（Secure Socket Layer）と呼ばれる暗号通信で、ウェブサーバーとの間でやり取りされるデータをすべて暗号化し、インターネット上で不正に盗聴されることを防ぎます。もちろん解読不能な暗号技術は存在しないので、絶対に安全だとは言い切れませんが、最新の汎用ブラウザーで使用される128ビットの強度を誇る暗号鍵は、ほぼ解読が不可能といわれています。

もう1つは、認証機能です。アクセスしているウェブサイトが実在する企業・組織のサイトであることを、第三者が証明するものです。実は、ウェブサイトの偽造は簡単で、著名なショッピングサイトをコピーして、そっくりそのまま別サーバーで運用するということは誰にもできます。これを防ぐために、しっかりとした審査機能を持つ第三者機関（認証局）が、実在する企業・組織が運営するウェブサイトであるということを認証する仕組みがあるのです。

通常、ブラウザーの右下に鍵がかけられた状態のアイコンが表示されている場合（図3）、SSL通信が開始されていることを表します。鍵アイコンをクリックすれば、そのSSL通信に使われている証明書を見ることができます。また、ウェブサイトによっては、サーバー証明書検証用シール（図4）を掲示しており、このシールをクリックすると、サーバー証明書の内容や有効性を簡単に知ることもできます。

ただし、テスト用のサーバー証明書は誰でも作れるので、誰が発行した証明書かが重要です。アクセスしたウェブサイトが使っているサーバー証明書が、一般的に信頼されているボルチモア社やベリサイン社などの認証局から発行されたものでない場合、「このセキュリティー証明書は、信頼する会社から発行されていません」と信頼性を問われることがあります。このようなメッセージが表示された場合は、アクセスしているウェブサイト自体が自分用に不正な証明書を発行し、他者になりすましている可能性があります。こういった場合は、ウェブサイトの安全性を疑う必要があります。

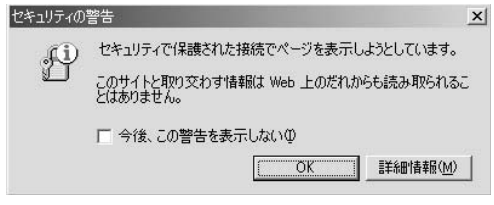
もう1つ大切なことは、SSLで守られるのは通信経路の安全性だけだということです。SSLでは、相手先のサーバーにデータが届いた後のセキュリティーは守られません。相手先の企業内でずさんな情報管理や内部犯行などがあれば、個人情報が流出する恐れがあります。個人情報の登録やクレジット決済などを行う際には、あたりまえのことなのですが、現実の世界と同様にウェブサイトの運営者つまり相手先を十分考慮するべきです。

（日本ボルチモアテクノロジーズ　河野真一）

SSLは当初Netscape Communications社で開発されたが、後にIETFで標準化され、TLS（Transport Layer Security）という名前になった（RFC 2246）。

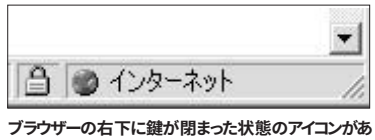
URL http://www.ietf.org/rfc/rfc2246.txt

●図2



SSL通信が開始されることを示すダイアログ

●図3



ブラウザーの右下に鍵が閉まった状態のアイコンがあればSSL通信中

●図4

サーバー証明書検証用シールがウェブサイトに貼られている場合もある

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp