

セキュリティ対策及び迷惑メール対策の更なる強化について —「Outbound Port25 Blocking」を開始!—

WAKWAKでは、会員のセキュリティ対策及び迷惑メール対策の更なる強化に向けた取り組みを段階的に実施いたします。

その取り組みの第一弾として、Outbound Port25 Blocking(*1) (WAKWAK以外のメール送信サーバへの接続制限) を、平成17年3月1日(火)より実施いたします。具体的には、WAKWAKの動的IPアドレス(*2)から、WAKWAKのメールサーバ以外のSMTPポート (Port25)(*3)への通信をブロックいたします。

これにより、WAKWAKの動的IPアドレスを利用してインターネットに接続している会員がウイルスに感染した場合、パソコンから直接送信されるメールがブロックされるため、ウイルス感染による機密情報の漏洩や企業における顧客情報の流出、意図せずウイルス発信の加害者になってしまう等の危険性が低くなり、今まで以上に安心してインターネットをご利用いただくことができます。

また、WAKWAKの動的IPアドレスから発信される迷惑メールが大幅に削減されるため、社会問題化している迷惑メールの撲滅に大きく貢献できるものと考えており、更にこの取り組みがインターネット業界全体に広がることで、迷惑メール問題の完全撲滅に繋がっていくことを期待しています。

NTT-MEでは、これまでも「XePhionインターネット接続サービス」(*4)などの企業向けサービスを中心にセキュリティ対策の向上を積極的に推進してきましたが、今回はその一環として、コンシューマ向けサービスにおける更なるセキュリティ強化を実現するものです。

今後もセキュリティ対策や迷惑メール対策の更なる強化に積極的に取り組み、お客様への安全かつ安心なインターネット環境の提供及び迷惑メールの撲滅に努めてまいります。

1. 背景

現在、メールは重要な通信手段となり、企業活動及び一般生活において欠かせない存在になっています。一方で、ウイルス感染メール等の迷惑メールが社会問題となり、メールの利用に支障をきたしています。

昨今のウイルスは高度化、悪質化し、ウイルス感染したパソコン内の情報を破壊するだけでなく、パソコン内に含まれる機密情報や個人情報を含んだウイルス感染メールを不特定多数に送信するものも発生しています。また、ウイルス感染したパソコンが外部からコントロールされ、迷惑メール送信の基地として利用されるなど、知らぬ間に大量迷惑メール送信の加害者になる事例も発生しております。

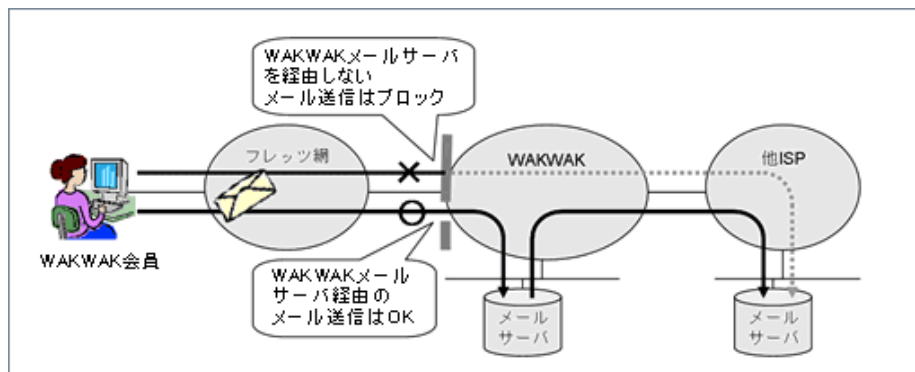
こうした状況に対し、迷惑メール問題の深刻化が著しい米国では、Outbound Port25 Blocking を実施するISPが増加してきており、日本においても同様の対策を実施する必要性が高まってきました。

2. Outbound Port25 Blocking について

(1) 概要

WAKWAKでは、ウイルス感染によるパソコンの機密情報や個人情報の流出、WAKWAKからの迷惑メール送信を防止するために、NTT東日本・NTT西日本が提供するフレッツ網経由でWAKWAKに接続している会員の動的IPアドレスから、WAKWAKのメールサーバ以外のSMTPポート (Port25) への通信をブロックいたします。

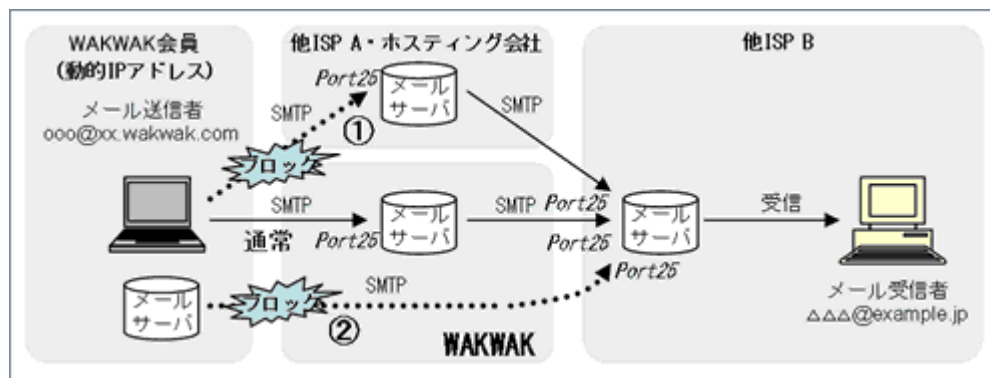
(2) 実施イメージ



(3) Outbound Port25 Blocking によって影響を受けるWAKWAK会員

以下の方法でメールを送信しているお客様については、従来の方法ではメールを送信できなくなる場合がありますので、該当のお客様はメーラーの設定変更等の対応を実施していただく必要があります。

他ISPまたはホスティング会社のメールサーバを利用してメールを送信しているWAKWAK会員、お客様自身でメールサーバを運用してメールを送信しているWAKWAK会員 (固定IPアドレスを利用しているお客様は影響を受けません)



(4) 影響の回避方法

上述の影響を受けるWAKWAK会員は、以下のいずれかを実施していただくことで、影響を回避することができます。他ISP、ホスティング会社のメールサーバを利用する際、SMTPポート(Port 25)を使用せずSubmissionポート(*5)やSMTP over SSL(*6)等を使用してメールを送信 (他ISP、ホスティング会社がSubmissionポートやSMTP over SSL等に対応している必要があります)。

WAKWAKのメールサーバ経由でメール送信を行うように設定を変更 (設定変更方法については後述の設定方法ページをご参照下さい)。

(5) ホームページ

- FAQ: <https://www.wakwak.com/prl/support/faq/op25b.html>
- 設定方法: https://www.wakwak.com/prl/support/g_mail/op25b_index.html

(6) 開始日

平成17年3月1日(火)

3.Submissionポートについて

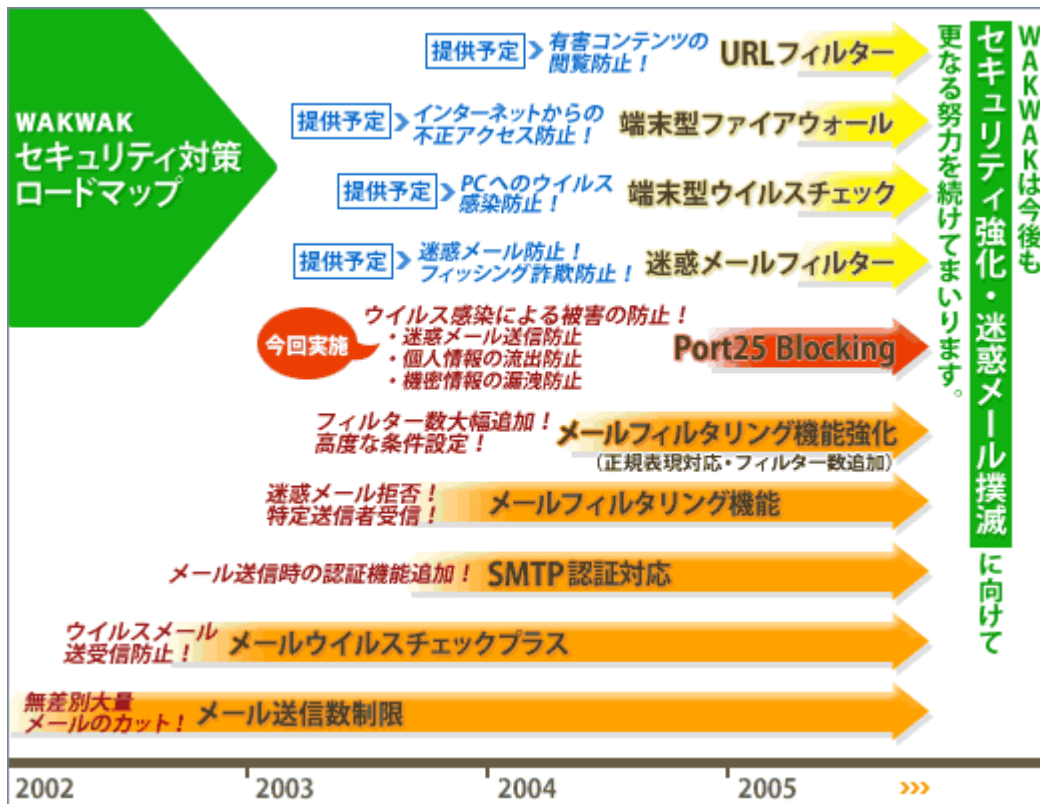
WAKWAKでは、すべてのメールサーバがSubmissionポートに対応しています。他ISPをご利用のお客様で、他ISPがOutbound Port25 Blockingを実施している場合、Submissionポートを利用することで他ISPからWAKWAKのメールサーバが利用できるようになります。

- [Submissionポートの設定方法](#)

4. WAKWAKのセキュリティポリシーについて

WAKWAKでは、これまでメール送受信時のウイルスチェックサービスや正規表現によるメールフィルタリングサービス(*7)の提供、1日あたりのメール送信数制限など、会員のセキュリティ対策及び迷惑メール対策の強化を積極的に推進してきましたが、今後もこれらのセキュリティ対策を更に強化し、会員に安全かつ安心なインターネット環境を提供してまいります。同時にインターネットの更なる発展に貢献するため、迷惑メールやウイルス等の完全撲滅を目指してまいります。

具体的には、今回実施するOutbound Port25 Blockingの他、迷惑メールフィルターサービスや端末型セキュリティサービスの提供などを予定しております。



*1Outbound Port25 Blocking: 近年、米国のISPで迷惑メール対策として実施されている対策で、ISPのメールサーバを利用しないメール送信 (Port25) をブロックするものです。ウイルス感染したPCから送信されるウイルス感染メールの大半は、ISPのメールサーバを経由せず、感染したPCより直接メール送信されます。また、迷惑メールの大半も同様にISPのメールサーバを経由せず、迷惑メール発信者のメールサーバから直接メール送信されます。このISPのメールサーバを経由しないメール送信をブロックすることにより、ウイルス感染メール、大量の迷惑メールの送信防止に大きな効果があると考えられています。

*2動的IPアドレス: ネットワークに接続するたびに、動的に割り当てられるIPアドレスのことです。インターネットの接続においては、一般的にISPから動的なIPアドレスを割り当てられます。これに対し、常に同じIPアドレスを取得するものを固定IPアドレスと呼びます。

*3SMTPポート (Port25): データ通信には、通信されるデータがメール送信なのかホームページ閲覧なのかを識別するために、識別番号が割り当てられています。その識別番号をポート番号といいます。メール送信には、一般に25番 (Port25) が割り当てられています。メール送信はSMTP (Simple Mail Transfer Protocol) というプロトコルで動作していることから、Port25はSMTPポートとも言われます。

*4XePhionインターネット接続サービス: NTT-MEが提供する企業向けインターネット接続サービスで、企業などのお客様収容ビルと、XePhionバックボーンとをメガデータネッツやEthernetなどの各種専用線で接続し、高品質で信頼性の高いインターネット環境を提供します。イントラネット/エクストラネットと連携した、トータルなネットワーク環境を実現します。

*5Submissionポート (Port587): メールクライアントからのメール送信に特化したメール送信用ポート (Port587) です。一般的に、Submissionポートを利用したメール送信には認証が必須となり、迷惑メール対策に効果があると言われていました。

*6SMTP over SSL: メール送信時、メールソフトとメールサーバの間の通信をSSLにより暗号化するメール送信手段です。暗号化されるため、メール送信時のセキュリティを高めることができます。

*7正規表現によるメールフィルタリングサービス: 正規表現とは、特定の文字列を用いて文字列のパターンを表現する方法です。WAKWAKのメールフィルタリングサービスは、正規表現によるフィルタリング条件指定に対応しています。詳しくは以下のURLをご参照下さい。

https://www.wakwak.com/prl/support/g_mail/filter_regexp.html

ご不明な点は [\[WAKWAKヘルプデスク\]](#) までお問合せください。