2016 年 5 月 13 日

匿名 FTP サーバで重要情報が公開されていることへの注意喚起

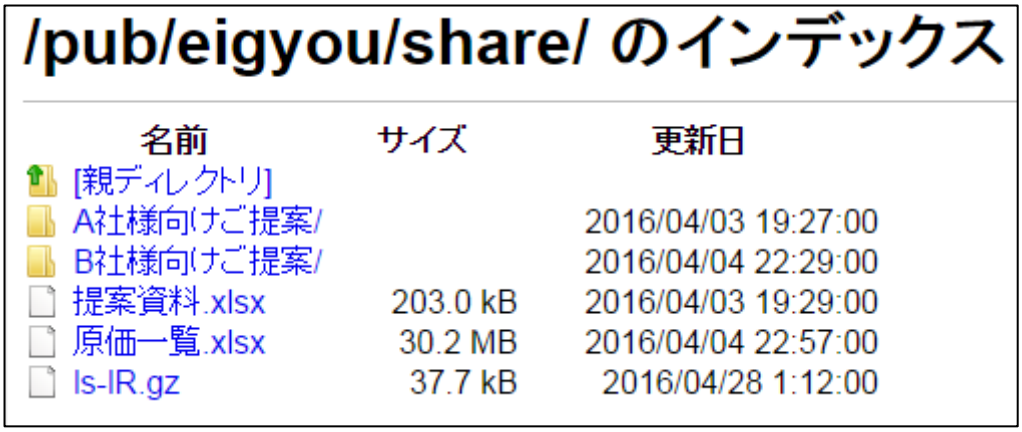
株式会社ラック

ラックではこのほど、インターネットに接続されたサーバから、取引先情報や社員の個人情報などが意図せず公開されているとみられるケースを複数確認しました。情報管理のあり方が厳しく問われる昨今、組織の内部情報に外部の誰もがアクセスできる状態を放置すれば、取引の縮小や停止、社会的信用の低下を招き、経営危機に直結する事態にも発展しかねません。経営層の方々は以下の情報を参考に、自組織でアクセス管理が不十分なサーバが公開状態になっていないか早急に確認することをお勧めします。

◇

内部情報が公開状態となっているのは、ファイルをやり取りするための「ファイル転送サーバ（FTP サーバ）」のうち、パスワードを入力せずに外部からアクセスできる「匿名 FTP サーバ(anonymous FTP サーバ)」です。匿名 FTP サーバ自体はインターネット黎明期から存在する情報共有手段の一つですが、近年は他の手段の多様化により利用されなくなりつつあります。

情報が公開状態となっていたのは国内の約 3400 組織・個人で、大部分は公開しても差し支えないとみられる情報でしたが、中には営業秘密に該当し得る請求書や見積書のほか、年賀状送り先一覧、従業員名簿、メールのバックアップといった個人情報も含まれていました。



内部情報を公開している匿名 FTP サーバのイメージ

なお、管理が不十分なまま匿名 FTP サーバを使っているのは、個人以外では中小企業がほとんどで、大企業や政府系機関の使用は目的があって情報を公開しているもの以外には確認できませんでした。ただ、意図せず公開されている情報の中には、請求書や見積書の宛名などに大企業やよく知られた組織の名前が確認できるケースも多く、取引の内容や金額が第三者から容易に閲覧できる状況となっています。

意図せず内部情報が公開される直接的な原因はアクセス権限の設定不備です。背景として以下のようなケースが考えられます。

- 不特定多数に対して公開しているサーバであるとの認識がない
- 過去に使った FTP サーバが利用者のいなくなった今も停止されずに放置されている
- 社員が自宅などで作業するため個人で FTP サーバを設置しており、組織としてサーバの存在を認識していない

内部情報が外部に公開されていると、次のような問題が生じる恐れがあります。

- 取引先から情報管理の責任を問われるおそれがある
- 取引先とのやり取りが標的型攻撃に悪用されるおそれがある
- 取引先名が漏れることにより、取引先自身の情報管理が不十分だという風評被害を生じさせる恐れがある

さらに、匿名 FTP サーバでファイルの書き込みも自由にできる状態になっている場合には、コンピュータウイルスや違法コピーした映画やアニメなどの「ファイル置き場」に使われる危険性もあります。

情報漏洩を防ぐには、まず、FTP サーバの設置・運用状況を確認する必要があります。FTP サーバは専用のサーバ機に限らず、Windows の機能として通常のパソコンに、LAN 接続型の外付けハードディスク（NAS）に、あるいはクラウド上にでも設置できますので、情報システム部門だけでなく、個々の社員がそのようなことをしていないかも確認する必要があります。組織内に FTP サーバが存在する、または社員が個人で FTP サーバを設置したことがあると判明したら、さらに次の点を確認し、対策をご検討ください。

- 意図せず外部の誰もがアクセスできる状態（匿名 FTP サーバ）になっていないか
- 意図して外部に公開している場合でも、誰もが書き込みできる状態になっていないか
  →そのような状態になっている場合は、直ちに書き込み権限を制限するとともに、不審なファイルが置かれていないか確認する

- FTP サーバは今後も業務に必要か
  →業務に必要な場合はアクセスできる範囲を制御する
  →必要でない場合は FTP サーバを停止する。さらに、社内で勝手に匿名 FTP サーバが設置されないよう、ファイアウォールで外から内への通信を遮断する

FTP サーバのアクセス管理不備による問題は古くて新しいテーマです。ラックは 2006 年にも、アクセス権限の制御が不十分（パスワードを設定していない、ID とパスワードが同一など）な FTP サーバに対する攻撃が増加していることに関し、注意喚起情報を発表しました。今回判明した匿名 FTP サーバからの意図しない内部情報の公開は、この注意喚起から 10 年経過した現在もなお、情報セキュリティの基本であるアクセス管理が徹底できていない事実を示しています。

今や、インターネットに接続した機器には世界のどこからでもアクセスされる可能性があります。2016 年 1 月には、ネットワークカメラの映像が意図しないまま公開されていることが報じられ、話題となりました。これと同様に、ファイル転送サービス（FTP）により公開されている情報を探し出す検索サービスも存在します。利用者、特に経営トップは、インターネットで公開状態にしている情報は容易に発見され得ることを今一度認識し、適切なアクセス管理がなされているかを確認してください。

Q&A

Q1: なぜこの注意喚起情報を公開したのですか？

A1: インターネットのように、あらゆる人やデバイスがつながるネットワークに対して、重要な情報が管理されない状況で公開される危険性について、具体的な事例を用いて認知を広めるために公開しました。

Q2: 「匿名 FTP サーバ(アノニマス FTP サーバ)」とは何ですか？

A2: 関係者がアクセスする際に使うユーザーID の代わりに、不特定多数の者がアクセスする際には「匿名」を意味する「anonymous」と入力することから、英語で「anonymous FTP server」と呼ばれ、日本語では「匿名 FTP サーバ」と訳されます。パスワードなどの認証を行わず誰にでもアクセスを許可する設定となっており、このアクセスは、不正アクセス禁止法で禁止された不正アクセス行為に当たらないと考えられます。

Q3: 国内約 3400 の匿名 FTP サーバは、ラックが独自に調査したものですか？

A3: 匿名 FTP サーバの検索サイトに、日本国内の約 3400 の FTP サーバがインデックスされているのを確認したもので、ラックが自ら FTP サーバを探査したものではありません。

Q4: 問題のある情報を公開していたと分かったサーバに関し、ラックはどう対応しましたか？

A4: 明らかに問題がある情報を公開していたサーバについて、ラックから JPCERT/CC に対し、「インシデントの報告」を行いました。

Q5: 国内の約 3400 組織・個人の詳細は調査しましたか？

A5: その調査のためには、ファイルの内容を詳細に分析する必要がありますが、公開を意図していない重要情報も含まれていると考えられることから、そのような調査は行っておりません。

以上