MS-IIS FTP Service5/6 の NLST コマンドの脆弱性について

ＮＴＴ コミュニケーションズ株式会社
ＩＴ マネジメントサービス事業部
セキュリティオペレーションセンタ

2009 年 09 月 14 日

Ver. 1.1

1. 調査概要

2009 年 08 月 31 日、Microsoft 社の IIS-FTP サーバ 5/6 系に関しての 0Day のセキュリティ脆弱性が公開された。
MS-Windows 2000 Server SP4 日本語版を対象に、この脆弱性の挙動について検証した結果をここに記す。

- 認証情報(匿名も含む)が必要である
- 特殊なディレクトリ名が必要であるため、ディレクトリ作成権限が必要である
  - 特殊なディレクトリ名が既に存在している場合は、ディレクトリ作成権限は不要であるが、特殊であるため、事前に存在する可能性はないと考えてよい
- インターネット上で公開された検証コードは、日本語版の MS-Windows 2000 Server SP4 でも動作する

さらに 2009 年 09 月 03 日に公開された IIS-FTP サーバの 0Day の DoS 攻撃に関して検証した結果をここに記す。

- 認証情報(匿名も含む)が必要である
- 攻撃時の他の接続を切断させることが可能である(DoS 攻撃)
- 待ちうけプロセス自体は終了しないため、再度接続することが可能である
- インターネット上で公開された検証コードは、日本語版の MS-Windows 2000 Server SP4 でも動作する

2. 検証結果

2.1. 検証環境

以下の環境で、検証を行った。

- Microsoft Windows2000 Server 日本語版 SP4 上の IIS5.0

2.2. 検証結果 (NLST の PoC)

以下、図のキャプションを参照されたい。

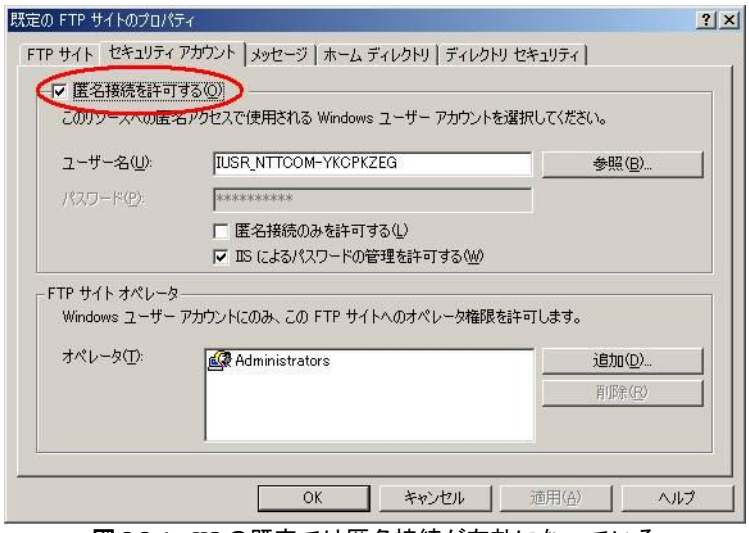

図 2.2-1 : IIS の既定では匿名接続が有効になっている

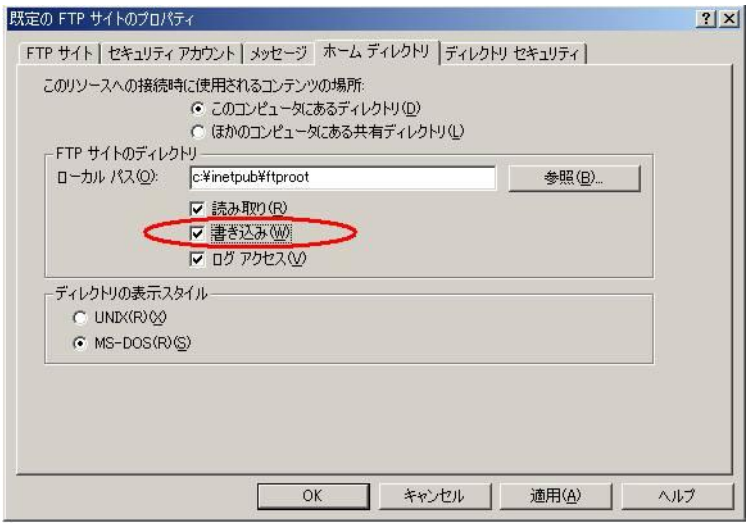

図 2.2-2 : IIS の既定では「書き込み」は有効ではないが、ここでは有効に設定する

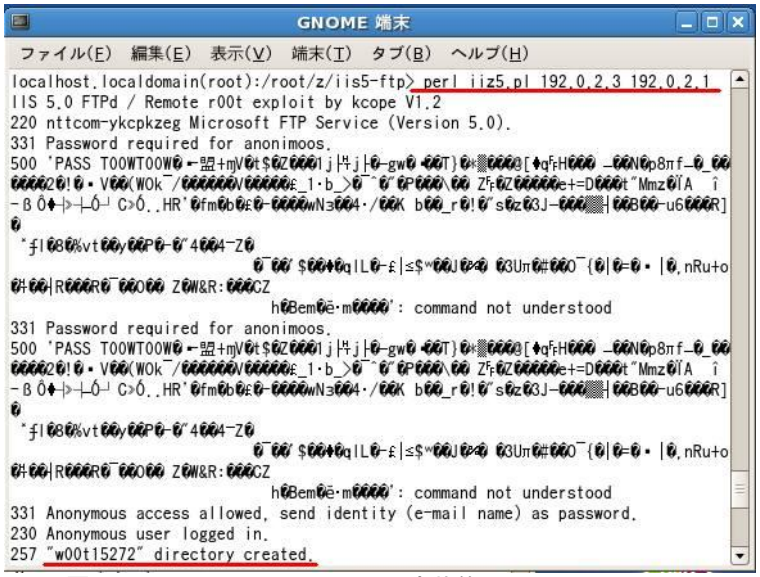

図 2.2-3 : 図 2.2-1 と図 2.2-2 の設定状態の IIS5.0 に対して、
インターネットで公開されている検証コードを実行する

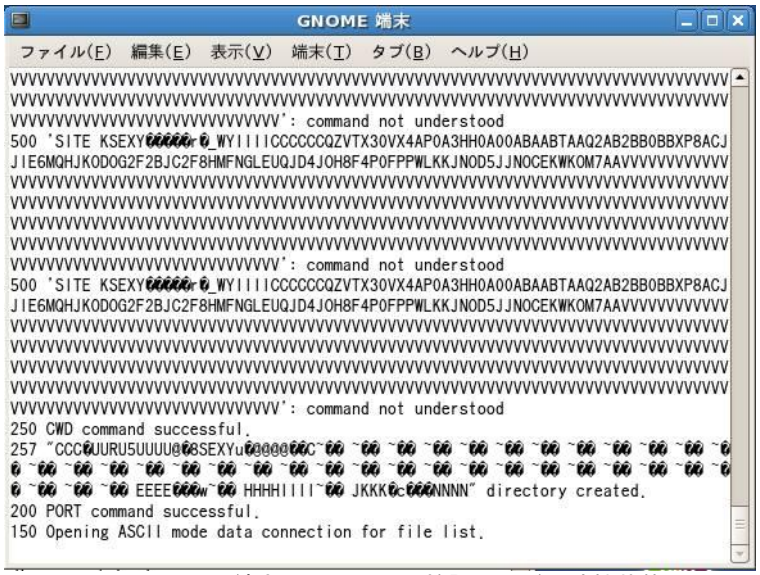

図 2.2-4 : 図 2.2-3 の続き。この画面で検証コードは待機状態に入る

図 2.2-5 : 図 2.2-4 の後、もう一つのシェルで 4444/tcp に接続することで、シェルを取得することが可能である

また、このシェルは「SYSTEM」権限で動作していることを確認した

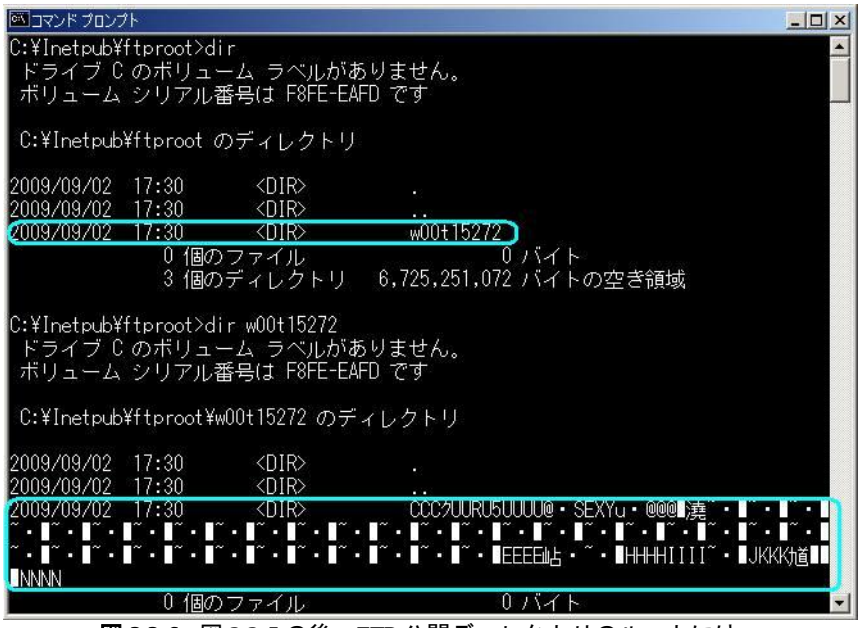

図 2.2-6 : 図 2.2-5 の後、FTP 公開ディレクトリのルートには、このようなディレクトリが作成されていた

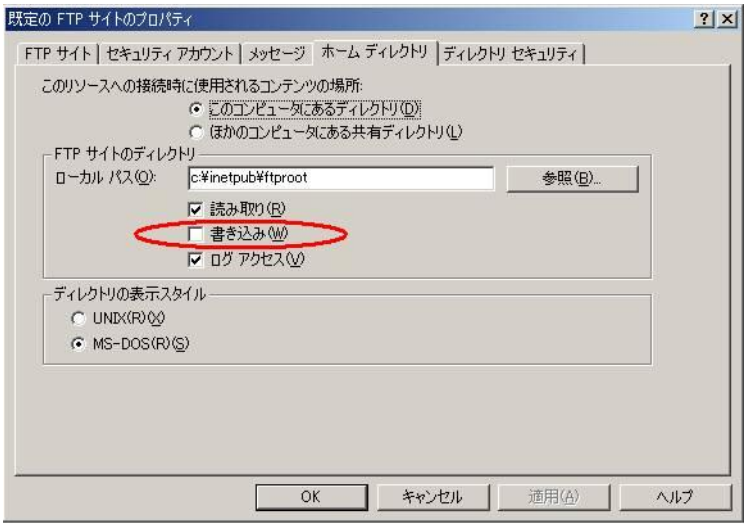

図 2.2-7 : 次は「書き込み」を禁止した。

IIS5.0 の既定の状態である

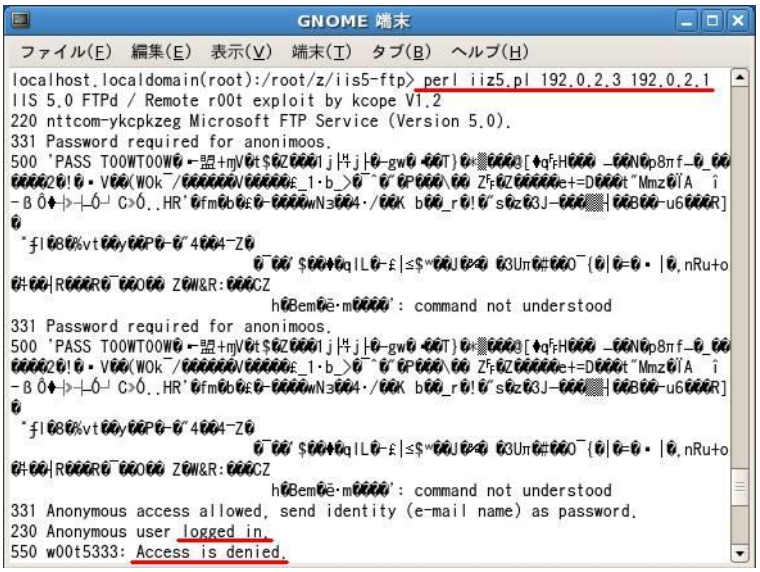

図 2.2-8 : 図 2.2-1 と図 2.2-7 の設定状態の IIS5.0 に対して、

インターネットで公開されている検証コードを実行する

(ログインは出来ているが、ディレクトリの作成に失敗している)

図 2.2-9 : 図 2.2-8 の続き。この画面で検証コードは待機状態に入る

図 2.2-10 : 図 2.2-9 の後にもう一つのシェルで 4444/tcp に接続することはできない

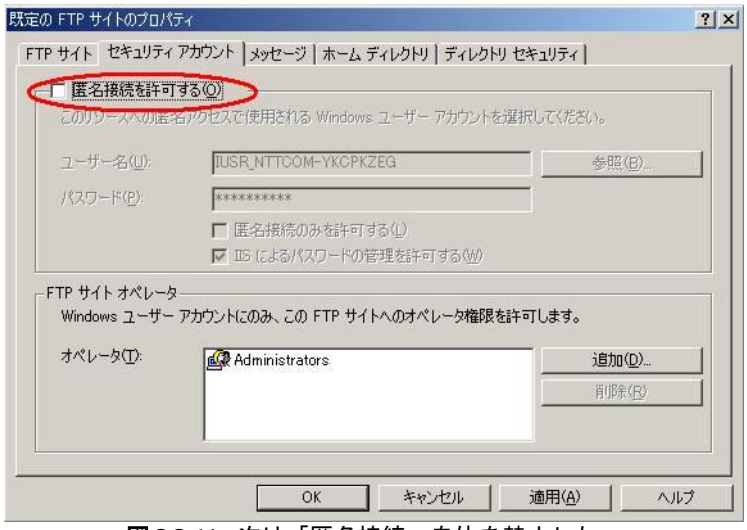

図 2.2-11 : 次は「匿名接続」自体を禁止した。

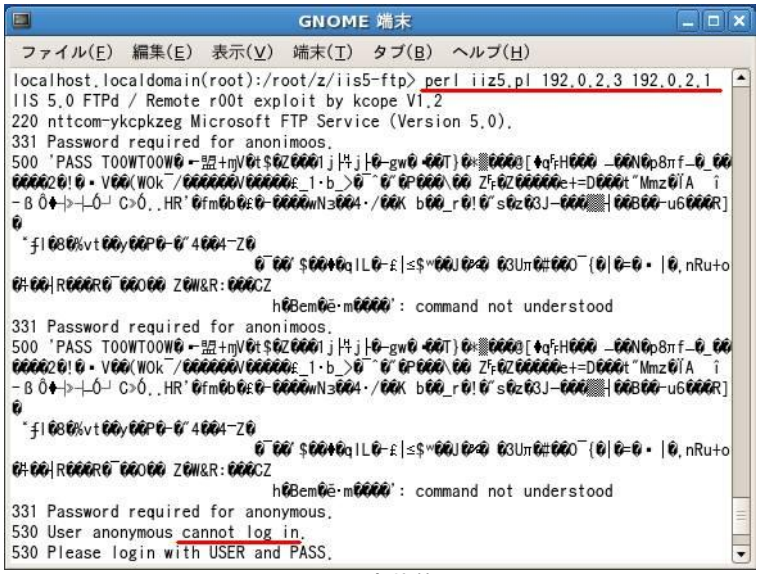

図 2.2-12 : 図 2.2-11 の設定状態の IIS5.0 に対して、

インターネットで公開されている検証コードを実行する

(ログイン自体に失敗している)

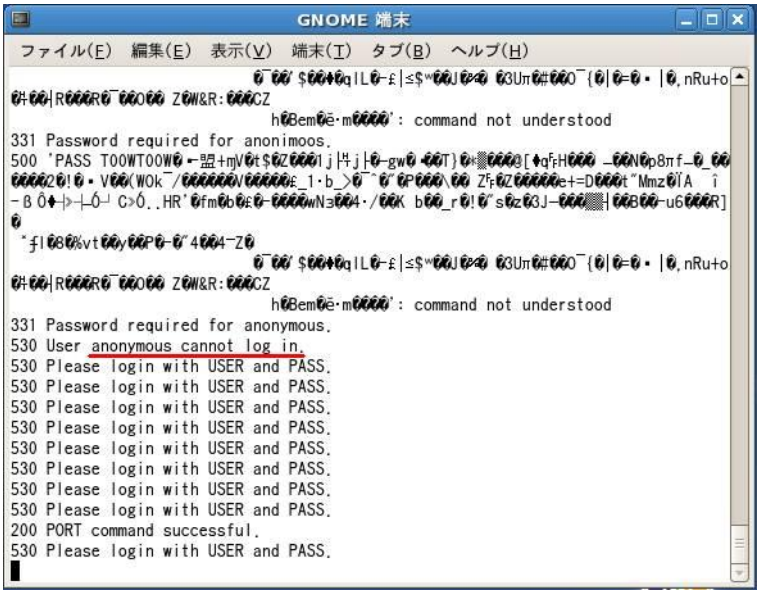

図 2.2-13 : 図 2.2-12 の続き。この画面で検証コードは待機状態に入る

図 2.2-14 : 図 2.2-13 の後にもう一つのシェルで 4444/tcp に接続することはできない

図 2.2-15 : 図 2.2-6 のようなディレクトリが既にあるので、「書き込み」禁止の状態で、図 2.2-6 で確認できるディレクトリを再利用するようにコードを修正し、それを実行してみた

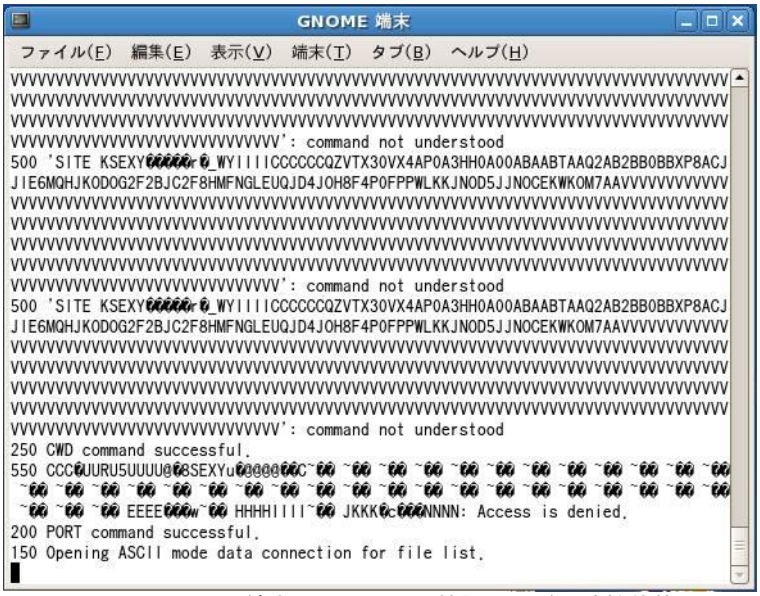

図 2.2-16 : 図 2.2-15 の続き。この画面で検証コードは待機状態に入る

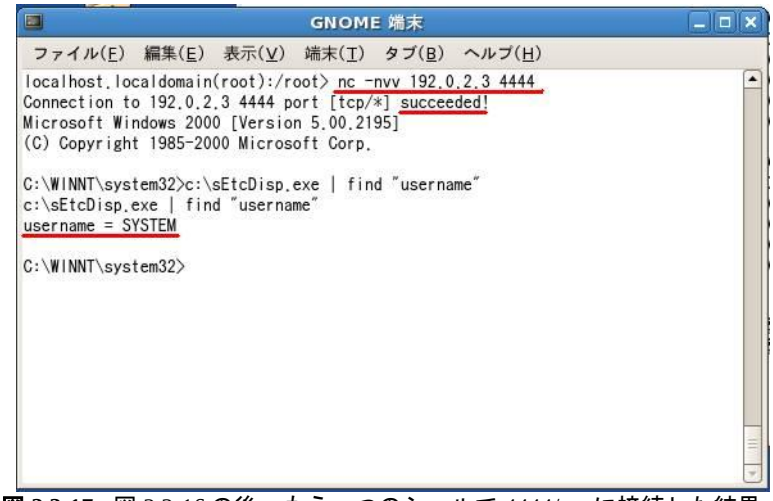

図 2.2-17 : 図 2.2-16 の後、もう一つのシェルで 4444/tcp に接続した結果。

つまり、事前に特殊な名前のディレクトリ名があれば「書き込み」権限は必要ないことが確認できる

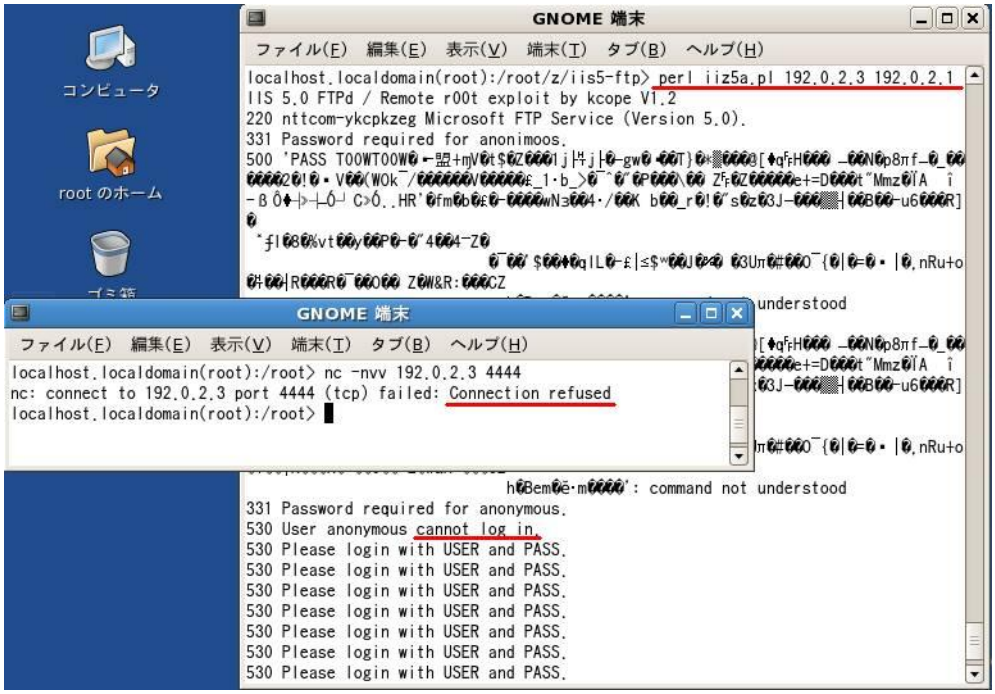

図 2.2-18 : さらに「匿名接続」を禁止してみた場合。

Exploit は成功していない。やはりログインしなければならないらしい

2.3. 検証結果 (DoS)

以下、図のキャプションを参照されたい。

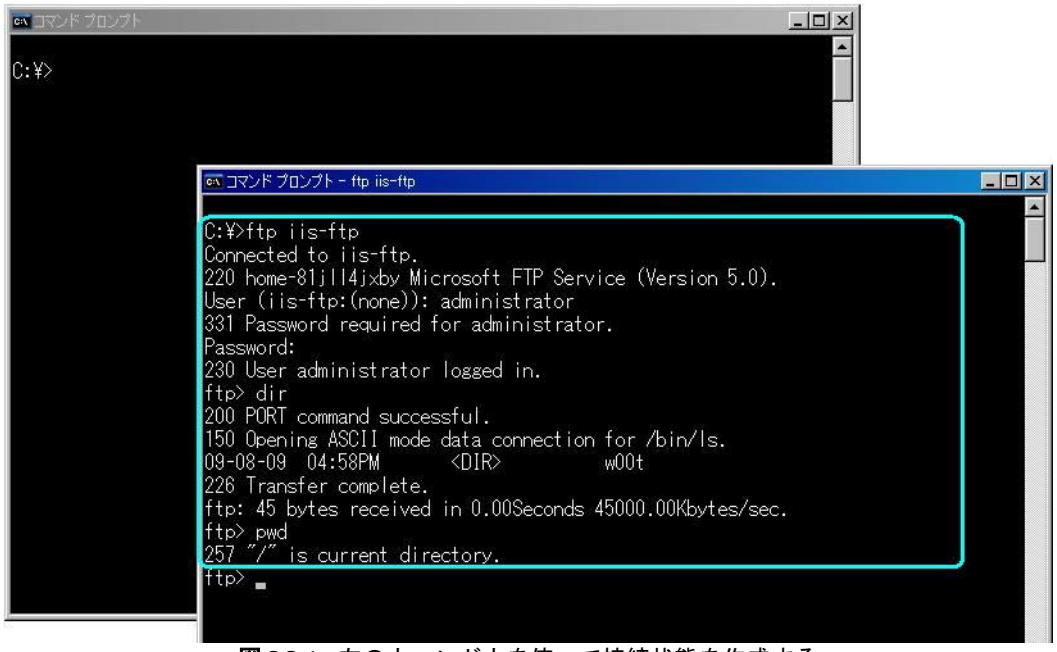

図 2.3-1 : 左のウィンドウを使って接続状態を作成する

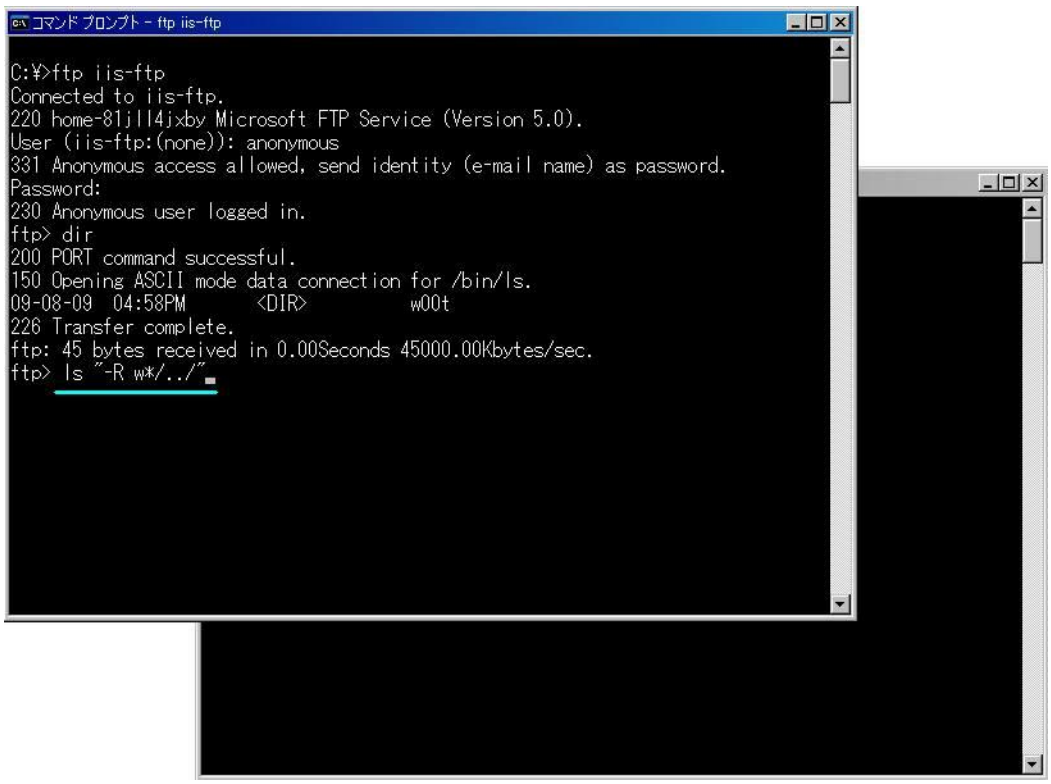

図 2.3-2 : 図 2.3-1 の状態のまま、今度は不正行為者が右のウィンドウを使って匿名ログインし、DoS 攻撃を実行する

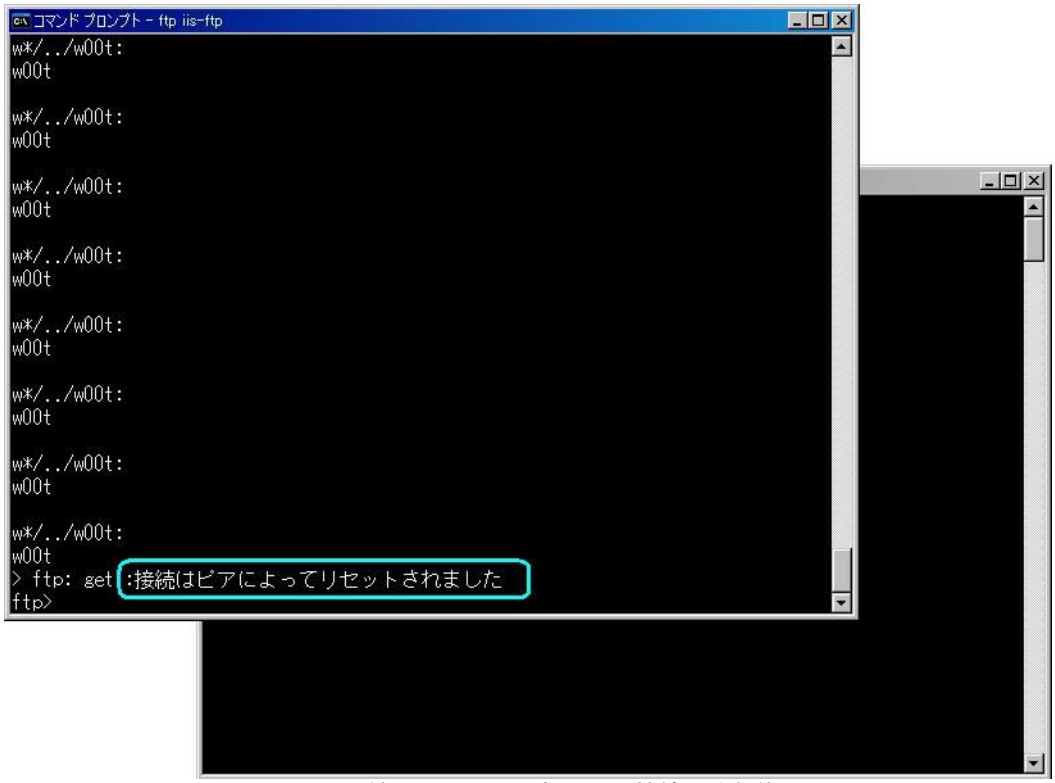

図 2.3-3 : 図 2.3-2 の結果。不正行為者の FTP 接続は強制終了している

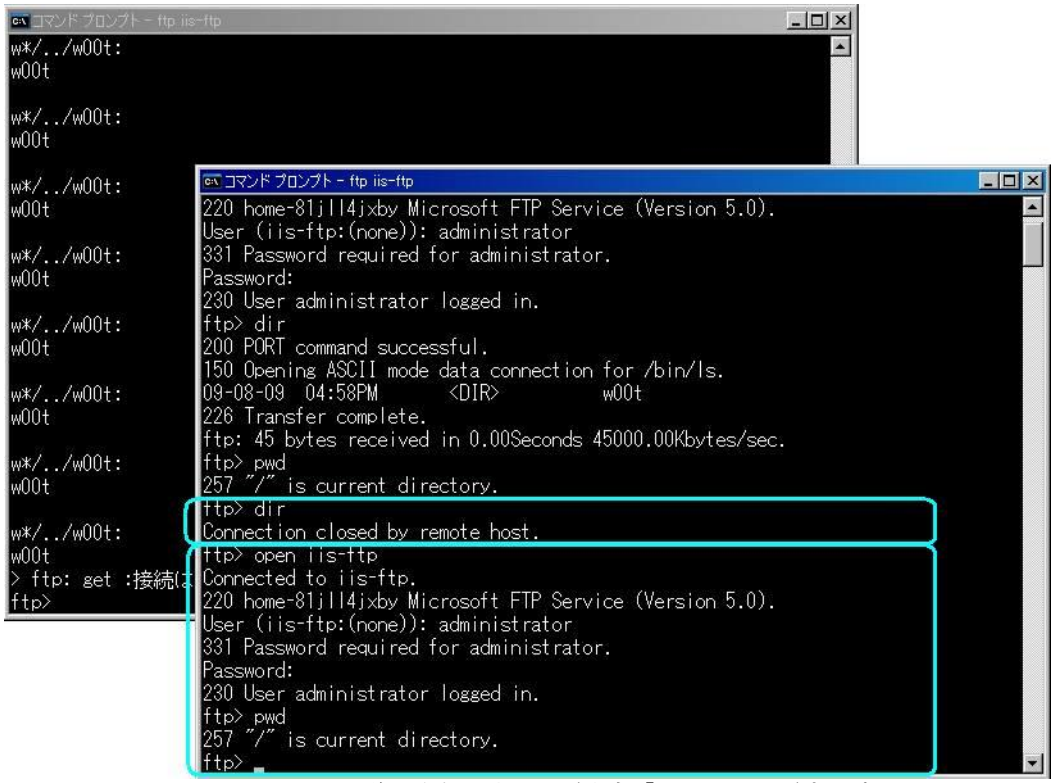

図 2.3-4 : 図 2.3-3 の後の右側のウィンドウも「dir」コマンド実行時に
切断されたことを確認した。
しかし、open コマンドで再度接続し、サービスを受けることが可能である

3. 検証作業者

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部ネットワークマネジメントサービス部
セキュリティオペレーションセンター
　佐名木 智貴

4. 参考

- SANS Microsoft IIS 5/6 FTP 0Day released
  http://isc.sans.org/diary.html?storyid=7039
- セキュリティホール memo
  http://www.st.ryukoku.ac.jp/~kjm/security/memo/#20090901_IIS
- インターネット インフォメーション サービスの FTP サービスの脆弱性により、リモートでコードが実行される (マイクロソフト セキュリティ アドバイザリ (975191)
  http://www.microsoft.com/japan/technet/security/advisory/975191.mspx
- milw0rm (Microsoft IIS 5.0/6.0 FTP Server (Stack Exhaustion) Denial of Service)
  http://www.milw0rm.com/exploits/9587
- CVE-2009-3023
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3023
- CVE-2009-2521
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2521

5. 履歴

- 2009 年 09 月 03 日 : ver1.0 最初の公開
- 2009 年 09 月 09 日 : ver1.1 DoS 攻撃に関する検証内容を追加、
  「2.3 検証結果 (DoS)」を追加
  「4 参考」の URL をいくつか追加

6. 最新版の公開 URL

http://www.icto.jp/security_report/index.html

7. 本レポートに関する問合せ先

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部ネットワークマネジメントサービス部
セキュリティオペレーションセンター

e-mail: scan@ntt.com

以 上