



# Isilon IQ スケールアウトNAS相互運用検証レポート 日本システムディベロップメント File Server Audit

---

ファイルサーバアクセスログ監視ソリューション 第二版

アイシロン・システムズ株式会社

最終更新日 2010 年 4 月

## 目次

1. はじめに .....	4
検証の目的.....	4
実施日.....	4
検証場所.....	4
2. 検証環境.....	5
システム構成.....	5
– File Server Audit 1.6.3.2.....	5
– Cisco Catalyst 2960.....	6
– Isilon IQ 1920.....	6
パターンマッチ検証環境.....	7
パターンマッチ検証環境(バージョンアップに伴う追加検証).....	8
負荷検証環境.....	8
3. パターンマッチ検証 .....	9
検証概略.....	9
検証結果.....	9
4. 負荷検証 .....	13
検証概略.....	13
検証結果.....	13
5. 考察 .....	15
6. その他のリソース .....	16
付録 A – Cisco Catalyst ポートミラー設定 .....	17
設定 .....	17

## 図表目次

図 1 : File Server Audit ログ検索.....	6
図 2 : Isilon IQ 1920 クラスタ・ストレージ.....	7
図 3 : パターンマッチ検証環境.....	7
図 4 : パターンマッチ検証環境 (追加検証) .....	8
図 5 : 負荷検証環境.....	8
図 6 : シングル ファイルシステムへCIFSアクセスした場合のWindowsエクスプローラ画面12	
図 7 : シングル ファイルシステムへCIFSアクセスした場合の「過去ログ検索」結果.....	12
図 8 : SMBパケット解析とパターン解析パフォーマンス.....	14
図 9 : ログ解析サーバのパフォーマンス.....	15

# 1. はじめに

## 検証の目的

アイシロン・システムズ(以下、アイシロン)が提供するスケールアウトNASストレージ環境である「Isilonクラスタ・ストレージ」と、株式会社日本システムディベロップメント(以下、NSD社)が提供するファイルサーバアクセスログ監視ツール「File Server Audit」との相互運用検証を実施しました。

「File Server Audit」は、ファイルサーバに対するアクセスをネットワークから監視する、ファイルサーバ専用ログ監視ツールです。

機密情報が格納されるファイルサーバは、万が一の情報漏えいに備えて、また情報漏えいを未然に抑止するため、“誰がどんな操作を行ったのか”というアクセスログを常に記録しておく必要があります。

今回、お客様にとってより最適なIT環境をご提供するために、NSD社とアイシロンの協力により、アイシロンのスケールアウトNASストレージをファイルサーバとして利用する場合のアクセスログ監視について、相互運用性を検証しました。

本検証では、パターンマッチ検証として一般的なオフィス環境を想定したファイル操作(Microsoft Office ファイルなどに対するファイルアクセスやフォルダアクセス)時のアクセスログ取得、および負荷検証として相応のネットワーク負荷が発生した環境におけるアクセスログ取得への影響を検証しました。

\*) 負荷検証結果については、本環境における実測結果を示したものであり、各製品としてなんら保証するものではありません。

## 実施日

2009年3月9日 ～ 2009年3月13日

2010年3月23日 ～ 2010年3月25日 (製品のバージョンアップに伴う追加検証を実施)

## 検証場所

アイシロン・システムズ株式会社「Isilon Smart Solution Center Tokyo」

## 2. 検証環境

### システム構成

今回の相互運用検証で利用したシステム環境(ハードウェアとソフトウェア)構成は、以下の通りです。

ハードウェア	OS	備考
DELL PowerEdge SC1435	Microsoft Windows Server 2003, Enterprise Edition SP2	File Server Audit 1.6 (アクセスログ監視)
Cisco Catalyst 2960	Cisco IOS Software, Version 12.2(25)	ポートミラースイッチ
Isilon IQ 1920	Isilon OneFS 5.0.3	監視対象ファイルサーバ
DELL ProLiant DL320 G3	Microsoft Windows Server 2003, Enterprise Edition SP2	Microsoft Active Directory (ドメインコントローラ)
DELL PowerEdge SC1435	Linux 2.6.18-92.el5 GNU/Linux	TCP Replay (ネットワーク負荷生成サーバ)
Panasonic Let'sNote CF-T1	Microsoft Windows XP SP3	クライアントPC

表 1: システム構成一覧

バージョンアップに伴う追加検証で利用したシステム環境(ハードウェアとソフトウェア)構成は、以下の通りです。

ハードウェア	OS	備考
DELL OptiPlex GX620	Microsoft Windows XP Professional SP2	File Server Audit 1.6.3.2 VISUACT-FX2 1.99.44 (アクセスログ監視)
Allied-Telesis CentreCOM GS908M	-	ポートミラースイッチ
Isilon IQ 1920	Isilon OneFS 5.5.4	監視対象ファイルサーバ
IBM ThinkPad X40	Microsoft Windows Server 2003, Standard Edition SP2	Microsoft Active Directory (ドメインコントローラ)
DELL LATITUDE D510	Microsoft Windows 7 Professional	クライアントPC

表 2: システム構成一覧(追加検証)

#### - File Server Audit 1.6.3..2

File Server Audit は、クライアントPCからファイルサーバへ流れるパケットをポートミラーリング機能付きのスイッチでミラーリングすることでアクセスログを監視します。その主な特長として、

- 1つのユーザ操作の情報が1行に集約されるので「いつ」「誰が」「どのファイルに」「どのような操作を行った」かが一目でわかる
- ファイルサーバからクライアントPCに“コピー”されたログが収集できる
- ファイルサーバとは独立してログが管理されるためセキュリティ強度が高い
- クライアントPCやファイルサーバに特別なソフトウェアのインストールが不要
- ネットワーク監視型のためファイルサーバに一切負荷がかからない

などがあります。「File Server Audit」の詳細は次のWebサイトをご参照ください。

<http://www.nsd.co.jp/service/fsa/>

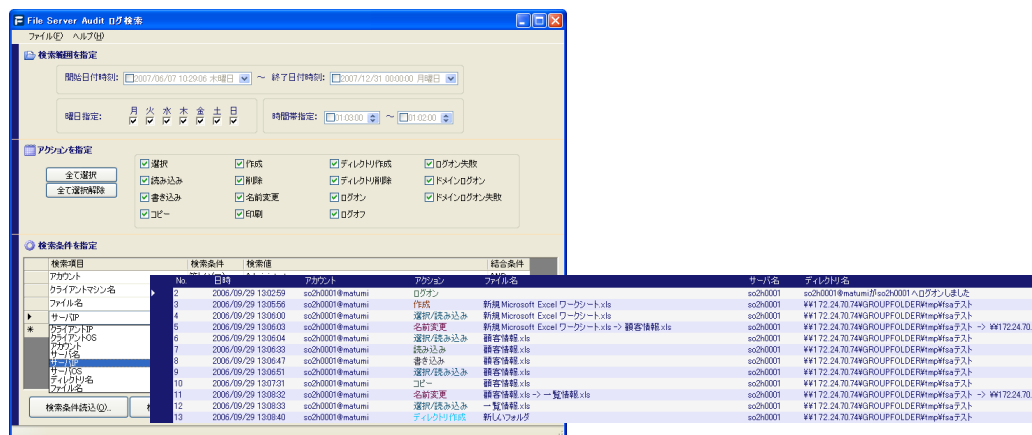


図 1: File Server Audit ログ検索

また、追加検証で利用した File Server Audit 1.6.3.2 のバージョンアップにおける主要な変更点は、

- ・ ファイルサーバを利用するクライアントPCのOSとして Windows Vista に対応したこと
- ・ Microsoft Office 2007 のパターンマッチに対応したこと

です。また、File Server Audit の動作環境として Windows Vista、Windows Server 2008 のサポートを開始しました。

なお、File Server Audit のアクセスログ収集機能を実現する内包製品セキュリティフ라이デー社「VISUACT(ビジュアクト)」は、Windows 7 に対応した VISUACT-FX2 を利用しました。「VISUACT」の詳細は次のWebサイトをご参照ください。

<http://www.visuact.jp/>

#### - Cisco Catalyst 2960

File Server Auditは、ネットワークスイッチのポートミラーリング機能を用いてファイルサーバのアクセスログを監視します。今回の検証では、Catalyst 2960 スイッチの Switched Port Analyzer (SPAN; スイッチドポートアナライザ)を利用して、ポートを通過するネットワークトラフィックをFile Server Auditが監視・解析するように構成しています。

なお、追加検証では、アライドテレシス社製 CentreCOM GS908M スイッチのポートミラーリング機能を利用して、ポートを通過するネットワークトラフィックを File Server Audit が監視・解析するように構成しました。

#### - Isilon IQ 1920

Isilon スケールアウト NAS ストレージは、高性能アプリケーションからエンタープライズアーカイブ、D2D(ディスクtoディスク)バックアップ、災害対策まで、企業の幅広いストレージニーズに対応します。Isilon IQ スケールアウトシリーズの主な特長として、

- ・ 業界初、完全対称型クラスタ・ストレージ・アーキテクチャ
- ・ 分散ファイルシステムにより単一の共有グローバル・ネームスペースを作成
- ・ ノード追加はわずか60秒、オンラインで容量や性能を拡張

- 単一ファイルシステムで6テラバイト(TB)～10.4ペタバイト(PB)までの容量拡張に対応
- 単一ファイルシステムで45 (GB)/秒の圧倒的なトータル・スループットを実現
- 業界初、ファイルやフォルダ毎のデータ保護を実現し、そのパリティ数を1～4まで設定可能
- 業界標準プロトコルの対応(NFS, CIFS, HTTP, FTP, iSCSI)
- ユーザ認証サポートプロトコル(LDAP, ADS, NIS)
- バックアップと監視 (NDMP, SNMP)

などがあります。詳細は、次のWebサイトをご参照ください。

<http://www.isilon.co.jp/products/>



図 2: Isilon IQ 1920 クラスタ・ストレージ

### パターンマッチ検証環境

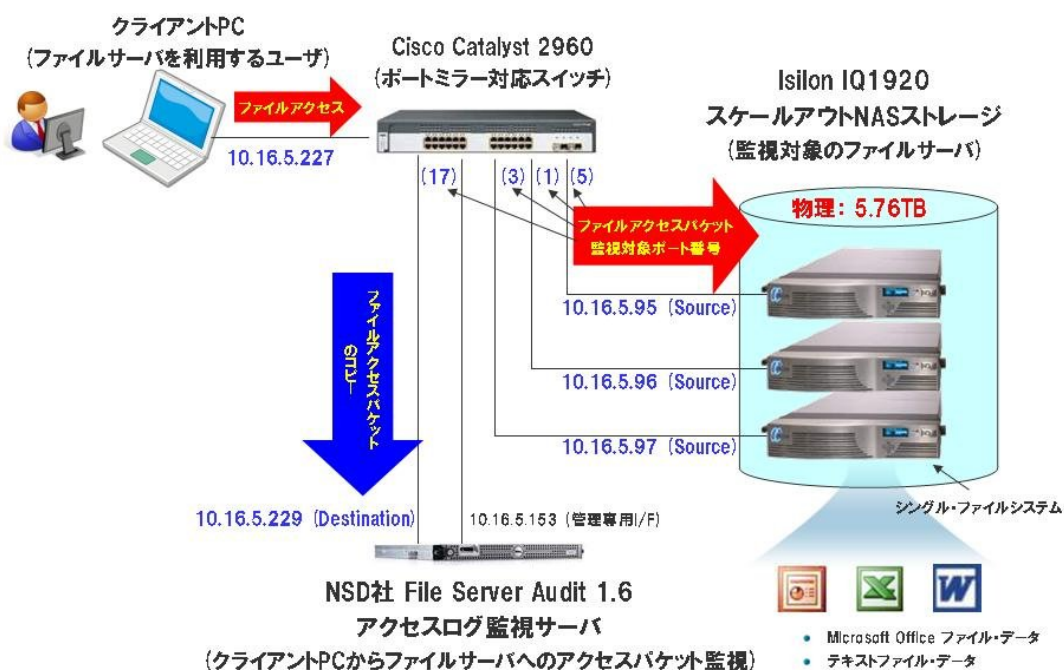


図 3: パターンマッチ検証環境

パターンマッチ検証環境(バージョンアップに伴う追加検証)

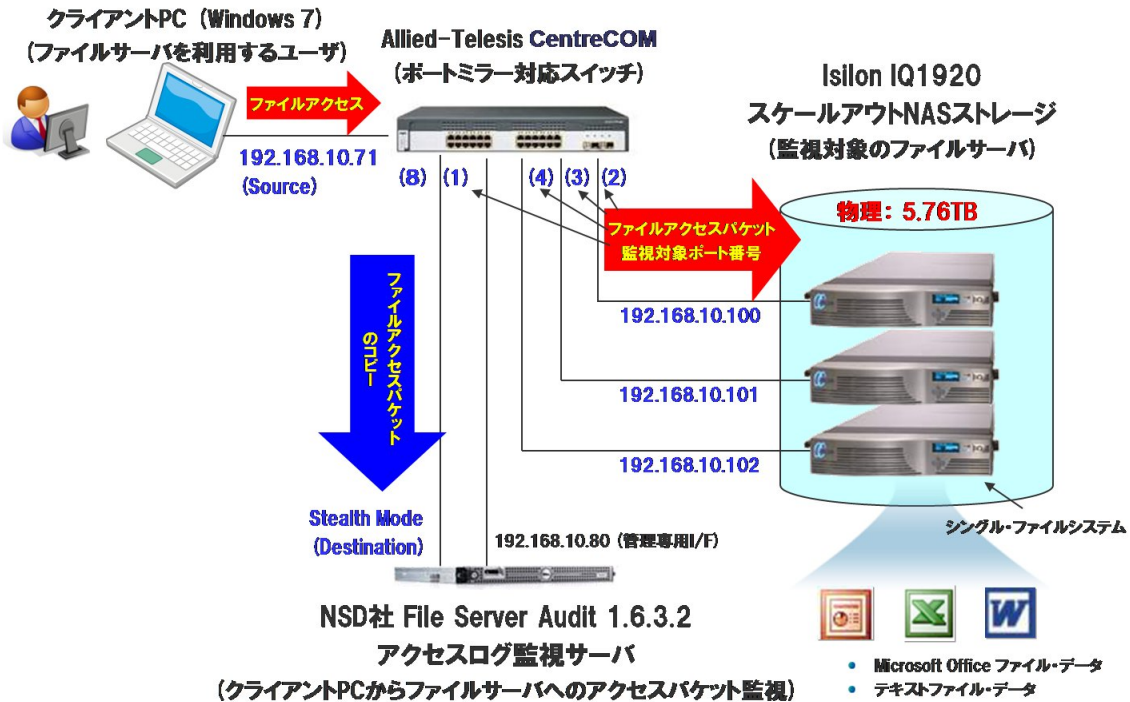


図 4: パターンマッチ検証環境(追加検証)

負荷検証環境

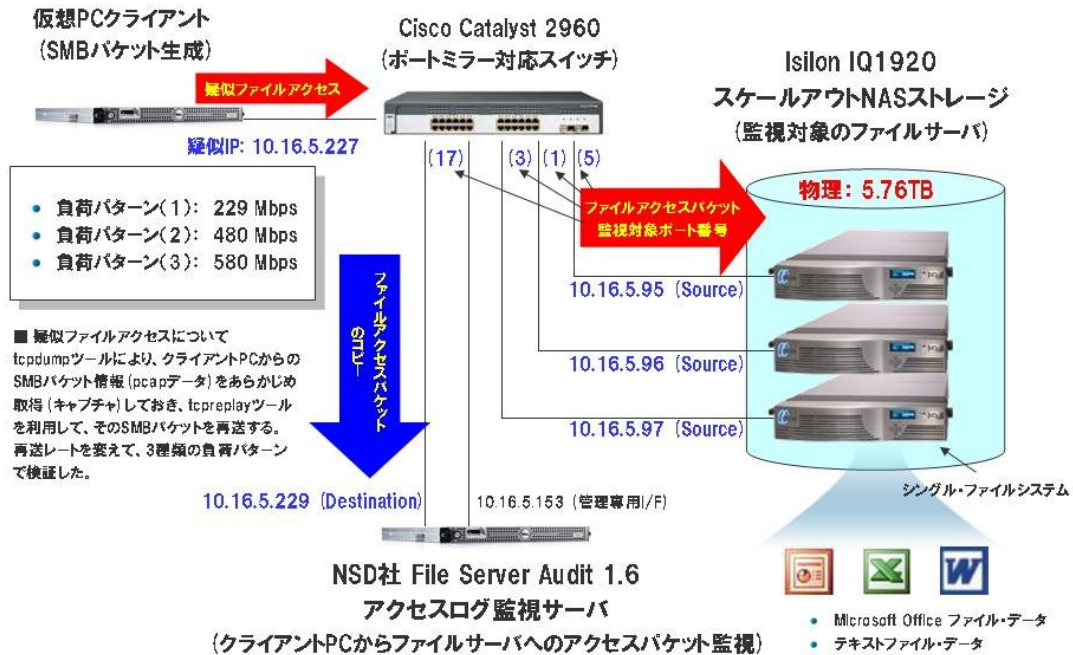


図 5: 負荷検証環境

### 3. パターンマッチ検証

ファイルサーバに対するアクセスを行った場合、1つのユーザ操作に対して、複数のトラフィックが発生しています。例えばExcelファイルを開いただけでも、実際にはテンポラリファイルの作成や削除などの処理が行われています。通常このような処理をAuditとして記録する場合、ユーザ操作に伴って発生する一連の動作が独立した・個別の操作として記録されてしまいます。

File Server Auditでは、このようなユーザ操作に伴う一連の処理パターンを解析する『パターンマッチ処理』を行うことにより、ある1つのユーザ操作を管理者の方がみてわかりやすい1つのログに集約しています。

#### 検証概略

Isilon IQは、従来のSANやNASストレージとは異なり、複数の筐体をクラスタリングしたシングル・ファイルシステムを提供しています。クライアントには、特別なソフトウェアやドライバなどを追加してインストールする必要がないにも関わらず、クラスタ内のどの筐体(ノード)を経由しても同一ファイルにアクセス可能な、グローバルネームスペースを実現しています。

パターンマッチ検証では、Isilon IQをファイルサーバとして運用した場合に、File Server Audit が、シングル・ファイルシステムの共有フォルダにあるファイル(Microsoft Officeファイル等)やフォルダを正しく認識して、アクセスログを取得することができるか検証しました。(図3)。

検証は、クライアントPCから、Isilon IQ上に作成した共有フォルダに対して、CIFSプロトコルでアクセスを行う方法で実施しました。共有フォルダへのアクセス方法と、主な操作は次の通りです。あわせて、アクセス方法と操作に応じてどのようなログが出力されるのか検証しました。

#### 【アクセス方法】

- Windows エクスプローラ
- コマンドプロンプト
- Microsoft Office アプリケーション (Word, Excel, PowerPoint, Access)

#### 【主な操作】

- フォルダの作成・名称変更・削除・ログオン・ログオフ
- ファイルの作成・名称変更・削除・コピー・移動

#### 検証結果

検証の結果、Isilon IQをファイルサーバとして利用する場合、クライアントPCからファイルサーバに対する全てのCIFSアクセスについて、ログが出力されることを確認しました。

#### 【フォルダ操作】

クライアントPCから『フォルダ』に対するアクセスを行った場合、全ての操作について正しくログを取得することを確認しました。クライアントPC上での操作内容とアクセスログの出力結果は(表3)の通りです。

アクセス方法	操作内容	ログ出力	出力結果評価
Windows エクスプローラ	フォルダ新規作成	ディレクトリ作成	○
	フォルダ名変更	名前変更	○
	フォルダ削除	ディレクトリ削除	○
コマンド プロンプト	フォルダ作成	ディレクトリ作成	○
	フォルダ名変更	名前変更	○
	フォルダ削除	ディレクトリ削除	○
ログオン	ログオン	ログオン	○
	ログオフ	ログオフ	○
	ログオン失敗	ログオン失敗	○
	ドメインログオン	ドメインログオン	○
	ドメインログオフ	ログオフ	○
	ドメインログオン失敗	ドメインログオン失敗	○

表 3: フォルダ操作のアクセスログ出力結果

【ファイル操作】

クライアントPCから『ファイル』に対するアクセスを行った場合、全ての操作について正しくログを取得することを確認しました。ファイルに対する操作内容とアクセスログの出力結果は(表4)の通りです。

	アクセス方法		操作内容	ログ出力	出力結果評価				
	From:	To:			Access	Excel	Power Point	Word	Text
Windows エクスプローラ			ファイル新規作成	作成	○	○	○	○	○
			ファイル名変更	名前変更	○	○	○	○	○
			ファイル削除	削除	○	○	○	○	○
	ファイルサーバ	ファイルサーバ	ファイルCTRL+C、CTRL+Vコピー	作成、コピー	(*2)	○	○	(*2)	○
	ファイルサーバ	ファイルサーバ	ファイル右クリックからコピー、貼り付け	作成、コピー	(*2)	○	○	(*2)	○
	ファイルサーバ	ファイルサーバ	ファイルドラッグアンドドロップコピー	作成、コピー	(*2)	○	○	(*2)	○
	ファイルサーバ	ファイルサーバ	ファイル移動	名前変更	○	○	○	○	○
	ファイルサーバ	クライアントPC	ファイルコピー	コピー	○	○	○	(*2)	○
	ファイルサーバ	クライアントPC	ファイル移動	コピー、削除	○	○	○	(*2)	○
	クライアントPC	ファイルサーバ	ファイルCTRL+C、CTRL+Vコピー	作成	○	○	(*2)	○	○
	クライアントPC	ファイルサーバ	ファイル右クリックからコピー、貼り付け	作成	○	○	(*2)	○	○
	クライアントPC	ファイルサーバ	ファイルドラッグアンドドロップコピー	作成	○	○	(*2)	○	○
	クライアントPC	ファイルサーバ	ファイル移動	作成	○	○	○	○	○
			ファイル選択	選択/読み込み	(*1)	○	(*1)	(*1)	(*1)
		ファイル内検索	選択/読み込み	(*1)	○	(*1)	○	(*2)	
コマンド プロンプト			ファイル名変更	名前変更	○	○	○	○	○
			ファイル削除	削除	○	○	○	○	○
	ファイルサーバ	ファイルサーバ	ファイルコピー	作成、コピー	(*2)	(*2)	(*2)	(*2)	(*2)
	ファイルサーバ	ファイルサーバ	ファイル移動	名前変更	○	○	○	○	○
	ファイルサーバ	クライアントPC	ファイルコピー	コピー	(*2)	(*2)	(*2)	(*2)	(*2)
	ファイルサーバ	クライアントPC	ファイル移動	コピー、削除	(*2)	(*2)	(*2)	(*2)	(*2)
	クライアントPC	ファイルサーバ	ファイルコピー	作成	○	○	○	○	○
クライアントPC	ファイルサーバ	ファイル移動	作成	○	○	○	○	○	

アクセス方法	操作内容	ログ出力	出力結果評価
Word	ファイル読み込み	選択/読み込み	(*2)
	名前をつけて保存	作成	(*2)
	上書き保存	書き込み	○
Excel	ファイル読み込み	選択/読み込み	(*2)
	名前をつけて保存	作成	(*2)
	上書き保存	書き込み	○
PowerPoint	ファイル読み込み	選択/読み込み	(*2)
	名前をつけて保存	作成	○
	上書き保存	書き込み	○
Access	ファイル読み込み	選択/読み込み	(*2)
	名前をつけて保存	作成	(*2)
	上書き保存	書き込み	(*1)

(\*1) NSD社の File Server Audit の仕様によりログの取得を行いません。

(\*2) NSD社によりパターンファイル定義の修正が予定されています。

表 4: フォルダ操作のアクセスログ出力結果

## 【シングル ファイルシステム】

クライアントPCから、クラスタ内の異なる筐体(ノード)を経由してIsilon IQ上の共有フォルダにアクセスしてファイル操作を行います。Isilon IQ/OneFSが実現するシングル ファイルシステムとは、クライアントが異なるノードにアクセスしても一貫したアクセス環境を実現します。(図6)

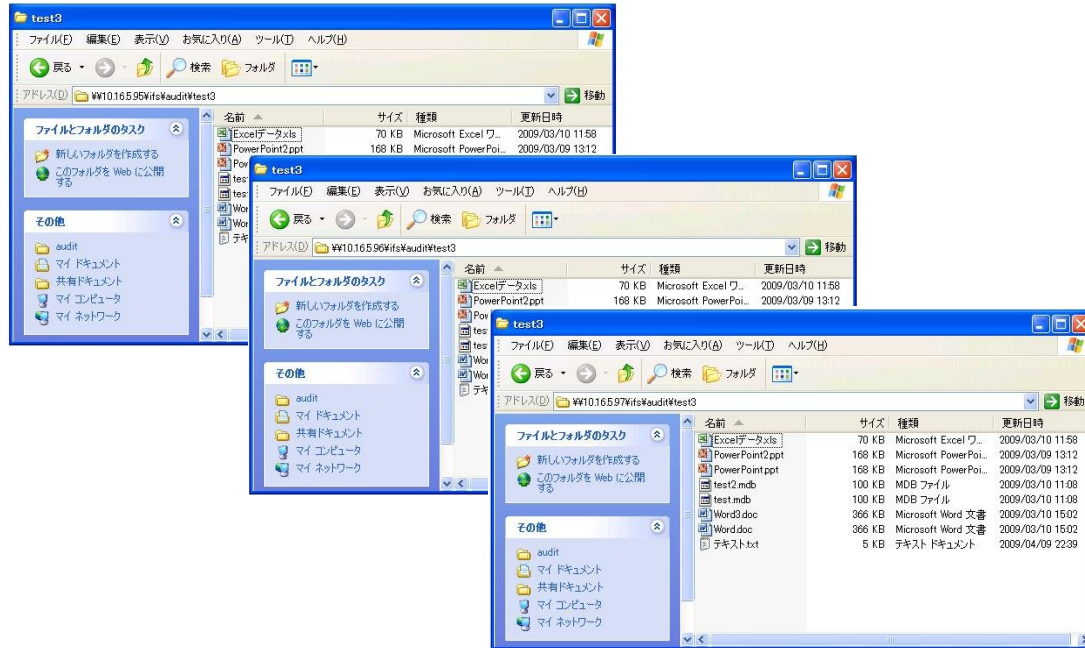


図 6: シングル ファイルシステムへCIFSアクセスした場合のWindowsエクスプローラ画面

今回の検証により、クライアントPCが異なるノード経由でシングル ファイルシステム上にある同一ファイルにアクセスした場合においても、アクセスログとして記録されることを確認しました。(図7)

日時	クライアントIP	アカウント	アクション	サーバ名	サーバIP	サーバOS	ディレクトリ名	ファイル名
2009/04/09 22:28	10.162.188	fsa-user2	ログオン	iq95-1	10.165.96	SAMBA	fsa-user2がiq95-1へログオンしました	
2009/04/09 22:29	10.162.188	fsa-user2	ログオン	iq95-2	10.165.96	SAMBA	fsa-user2がiq95-2へログオンしました	
2009/04/09 22:29	10.162.188	fsa-user2	ログオン	iq95-3	10.165.97	SAMBA	fsa-user2がiq95-3へログオンしました	
2009/04/09 22:30	10.162.188	fsa-user2	選択/読	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:30	10.162.188	fsa-user2	選択/読	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:30	10.162.188	fsa-user2	選択/読	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	テキスト.txt
2009/04/09 22:32	10.162.188	fsa-user2	作成	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	新規テキストドキュメント.txt
2009/04/09 22:32	10.162.188	fsa-user2	名前変更	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	新規テキストドキュメント.txt -> テキスト2.txt
2009/04/09 22:33	10.162.188	fsa-user2	作成	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	新規テキストドキュメント.txt
2009/04/09 22:33	10.162.188	fsa-user2	名前変更	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	新規テキストドキュメント.txt -> テキスト3.txt
2009/04/09 22:33	10.162.188	fsa-user2	作成	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	新規テキストドキュメント.txt
2009/04/09 22:33	10.162.188	fsa-user2	名前変更	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	新規テキストドキュメント.txt -> テキスト4.txt
2009/04/09 22:36	10.162.188	fsa-user2	書き込み	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト2.txt
2009/04/09 22:36	10.162.188	fsa-user2	書き込み	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト3.txt
2009/04/09 22:37	10.162.188	fsa-user2	書き込み	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	テキスト4.txt
2009/04/09 22:37	10.162.188	fsa-user2	選択/読	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:38	10.162.188	fsa-user2	選択/読	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:38	10.162.188	fsa-user2	選択/読	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	テキスト.txt
2009/04/09 22:38	10.162.188	fsa-user2	選択/読	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:39	10.162.188	fsa-user2	選択/読	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:39	10.162.188	fsa-user2	選択/読	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	テキスト.txt
2009/04/09 22:39	10.162.188	fsa-user2	書き込み	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:39	10.162.188	fsa-user2	書き込み	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト.txt
2009/04/09 22:39	10.162.188	fsa-user2	書き込み	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	テキスト.txt
2009/04/09 22:40	10.162.188	fsa-user2	削除	iq95-1	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト2.txt
2009/04/09 22:40	10.162.188	fsa-user2	削除	iq95-2	10.165.96	SAMBA	\\10.165.96\ifs\audit\test3	テキスト3.txt
2009/04/09 22:40	10.162.188	fsa-user2	削除	iq95-3	10.165.97	SAMBA	\\10.165.97\ifs\audit\test3	テキスト4.txt
2009/04/09 22:41	10.162.188	fsa-user2	ログオフ	iq95-1	10.165.96	SAMBA	fsa-user2がiq95-1からログオフしました	
2009/04/09 22:41	10.162.188	fsa-user2	ログオフ	iq95-2	10.165.96	SAMBA	fsa-user2がiq95-2からログオフしました	
2009/04/09 22:41	10.162.188	fsa-user2	ログオフ	iq95-3	10.165.97	SAMBA	fsa-user2がiq95-3からログオフしました	

図 7: シングル ファイルシステムへCIFSアクセスした場合の「過去ログ検索」結果

## 4. 負荷検証

Isilon IQは、シングル ファイルシステムに対する共有アクセス処理に優れたパフォーマンスを発揮します。Isilon IQをファイルサーバとして利用する場合、シングル ファイルシステムで膨大なデータを管理できるだけでなく、多くのクライアントアクセスを処理することができるため、そのアクセスログ取得についても高い処理性能が要求されます。

### 検証概略

負荷検証では、Isilon IQをファイルサーバとして運用した場合、一定のネットワーク負荷が発生した環境下でも、File Server Audit がIsilon IQに対するアクセスログを取得することができるかどうかを検証しました(図5)。

検証は、クライアントPCからIsilon IQ上の共有フォルダへアクセスしたパケットを取得、このパケット特定の負荷にあわせて再送した状況における、File Server Audit の処理性能を測定しました。あわせて、ネットワークの負荷状況に応じて、アクセスログが漏れなく取得できるかを検証しました。

### 【検証手順】

- クライアントPCからファイルサーバへのアクセスを tcpdump でパケットダンプする
- パケットファイルを tcpreplay で再送して大量のファイルアクセスを疑似的に発生する
- 高負荷な環境下で File Server Audit サーバの解析性能を確認する

### 【ネットワークの負荷パターン】

- ケース(1): 229 [Mbps] の CIFS ネットワーク・トラフィック
- ケース(2): 480 [Mbps] の CIFS ネットワーク・トラフィック
- ケース(3): 580 [Mbps] の CIFS ネットワーク・トラフィック

### 検証結果

検証の結果、Isilon IQをファイルサーバとして利用する場合、多数のクライアントからファイルサーバに対してCIFSアクセスが発生して、高負荷なトラフィックが発生した環境でも、File Server Audit の解析性能とアクセスログ監視サーバ性能ともに十分な性能を発揮していることを確認しました。

ネットワークの負荷パターン毎の解析パフォーマンス(図8)、およびアクセスログ解析サーバのパフォーマンス(図9)は次の通りです。

## 解析パフォーマンス

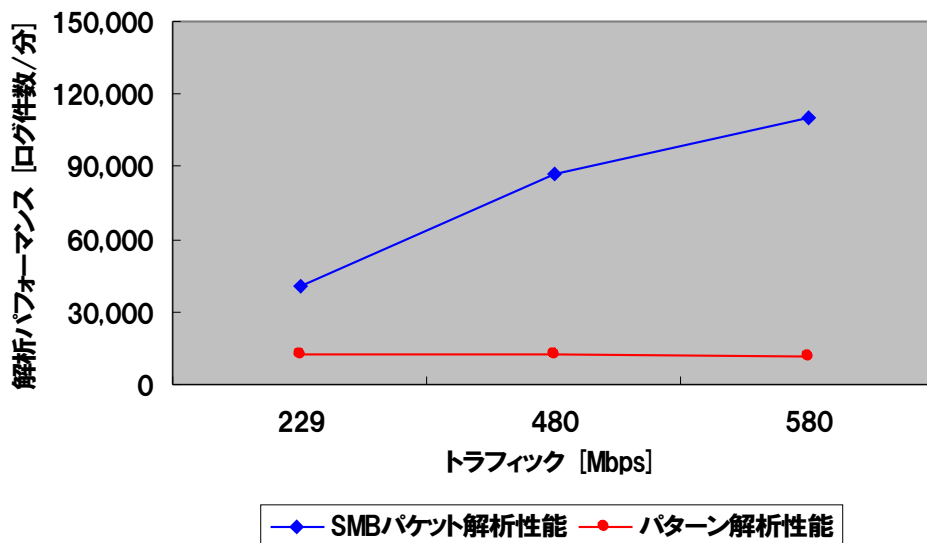


図 8: SMBパケット解析とパターン解析パフォーマンス

### 【SMBパケット解析パフォーマンス】

File Server Audit では、パケットをキャプチャしSMBパケットを解析した結果を、まずファイルに出力します。「SMBパケット解析パフォーマンス」とは、このSMBパケットを解析した結果のログが、一分間当たり何件生成されたかを示しています。この処理は、ネットワークを流れるパケットをリアルタイムでキャプチャする必要があるため、トラフィックに応じたスループットを出せることが要求されます。トラフィックが229Mbpsから580Mbpsへと増えるのに比例し、スループットも上がることを確認できました。

### 【パターン解析パフォーマンス】

前述の SMBパケット解析ログに対して、パターンマッチング処理を行った結果を、File Server Audit データベースに登録した件数です。580Mbpsの高負荷状態においても、処理性能が概ね維持されることを確認しました。

## ログ解析サーバのパフォーマンス

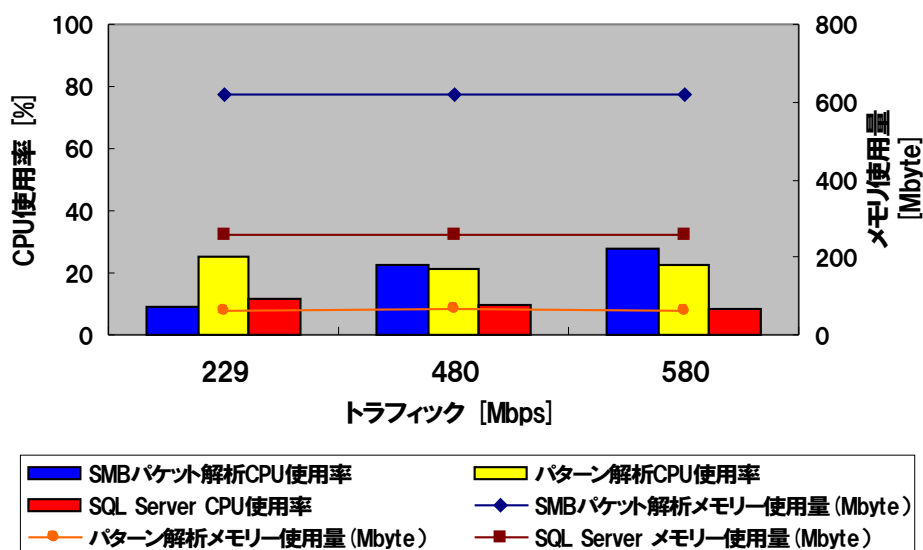


図 9: ログ解析サーバのパフォーマンス

### 【ログ解析サーバのパフォーマンス】

File Server Auditサーバの負荷状況を確認するため、Windows のパフォーマンスモニタを利用して CPU使用率とメモリ使用率を測定しました。SMBパケット解析の CPU使用率を除き、どのトラフィックにおいても、ほぼ一定の CPU使用率とメモリ使用率であり、安定的に稼働することが確認されました。SMBパケットの解析はトラフィックが増加すると、CPUへの負荷が少しずつではあるが高くなる傾向がありました。

## 5. 考察

検証結果より、File Server Audit および Isilon OneFS の最新バージョンでも、Isilon IQ をファイルサーバとして使用した際のCIFS アクセスログを、NSD社製 File Server Audit で問題なく取得することが確認できました。

Isilon IQとFile Server Auditを組み合わせることで、“スケーラビリティ”、“優れたパフォーマンス”、“高いセキュリティ”の全てを満たしたファイルサーバを実現できることが確認できました。

今回両社のプラットフォームが相互に利用可能なことを確認できたことにより、本ファイルサーバソリューションは、従来にはないITプラットフォームとしてお客様へご提案できることを確認しました。

## 6. その他のリソース

1

- 2・ 株式会社日本システムディベロップメント(<http://www.nsd.co.jp/>)
- 3・ セキュリティフライデー株式会社(<http://www.securityfriday.com/jp/>)
- 4・ File Server Audit 製品概要(<http://www.nsd.co.jp/service/fsa/>)
- 5・ VISUACT 製品概要([http://www.securityfriday.com/jp/product\\_1.html](http://www.securityfriday.com/jp/product_1.html))
- 6・ Isilon IQ 製品概要(<http://www.isilon.co.jp/products/>)

詳しい情報は <http://www.isilon.co.jp/> または <http://www.isilon.com/> をご覧ください。

### 謝辞

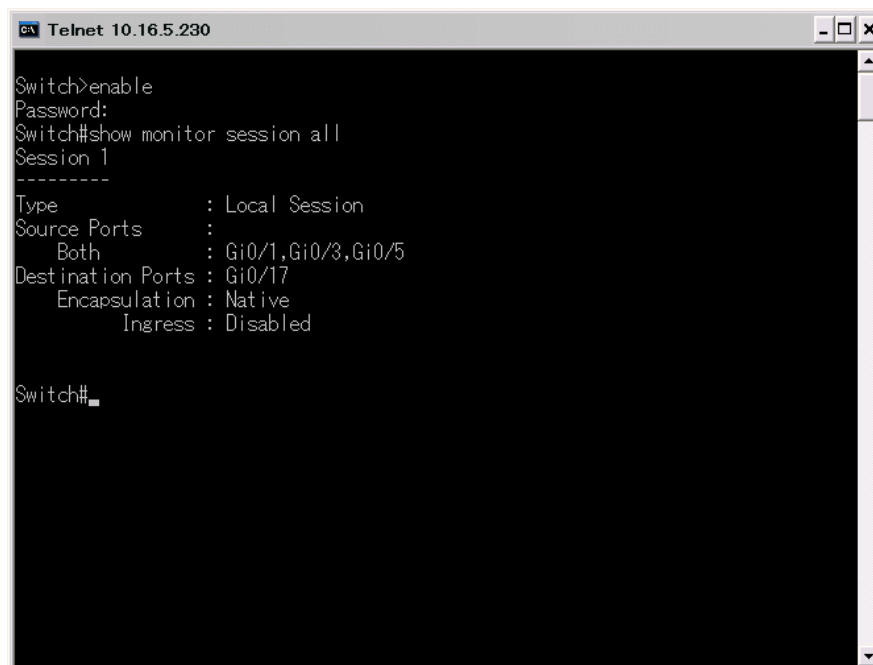
今回 Isilon IQとNSD社製 File Server Audit (セキュリティフライデー社製VISUACT)の検証にあたり、多大なるご協力を頂きました株式会社日本システムディベロップメント、セキュリティフライデー株式会社の皆様に、感謝いたします。

## 付録 A – Cisco Catalyst ポートミラー設定

ポートまたは VLAN を通過するネットワークトラフィックを解析するには、SPAN を使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。

### 設定

```
configure terminal
no monitor session 1
monitor session 1 source interface gigabitethernet 0/1
monitor session 1 source interface gigabitethernet 0/3
monitor session 1 source interface gigabitethernet 0/5
monitor session 1 destination interface gigabitethernet 0/17
end
```



```
Telnet 10.16.5.230
Switch>enable
Password:
Switch#show monitor session all
Session 1
-----
Type           : Local Session
Source Ports   :
  Both         : Gi0/1,Gi0/3,Gi0/5
Destination Ports : Gi0/17
  Encapsulation : Native
  Ingress       : Disabled

Switch#
```

詳しい情報は <http://www.isilon.co.jp/> または <http://www.isilon.com/> をご覧ください。

## アイシロン・システムズについて

Isilon Systems (NASDAQ: "ISLN")は、スケールアウト NAS ストレージ分野の世界的リーダーとして、お客様のミッションクリティカルなアプリケーションやワークフロー、業務プロセスのパフォーマンスを最大化し、ユニークなビジネスの価値をもたらすクラスター・ストレージとデータ管理ソリューションを提供しています。スケーラビリティの高さと容易な管理性を備え、コスト効率のよい Isilon IQ は、企業が大容量かつ急激に増大するファイルベースのデータを管理することを可能にします。

© 2001–2010 Isilon Systems, Inc. All rights reserved. 本資料の無断複製・転載を禁ず。Isilon、Isilon Systems、Isilon IQ、Isilon OneFS は、米国 Isilon Systems, Inc.の商標または登録商標です。その他、記載された会社および製品名などは該当する各社の商標または登録商標です。

お問い合わせ:

アイシロン・システムズ株式会社

〒151-0053

東京都渋谷区代々木 1-22-1 代々木1丁目ビル12F

電話: 03-5358-7188

FAX: 03-5333-4443

Email: [contact-jp@isilon.com](mailto:contact-jp@isilon.com)