ソフォス株式会社
2013 年 10 月 04 日

FUJITSU Server PRIMERGY / FUJITSU Storage ETERNUS NR1000 F2240 と Sophos Anti-Virus for NetApp の連携におけるウイルス検知の動作検証報告

本レポートは 2013 年 9 月 11 日～13 日に貴社トラステッド・クラウド・スクエアで実施した ETERNUS NR1000 F2240 上の CIFS サーバと連携した Sophos Anti-Virus for NetApp におけるウイルス検知の動作検証の方法および結果をまとめた書です。

1. はじめに

当社製品 Sophos Anti-Virus for NetApp は Network Appliance 社 Data ONTAP 7 および 8.x 7-MODE の CIFS 共有に対するウイルス検知機能に対応しております。今回は Network Appliance 社の OEM 製品である ETERNUS NR1000 F2240 と Sophos Anti-Virus for NetApp を連携し、ウイルス検知の動作検証を行った結果を報告いたします。

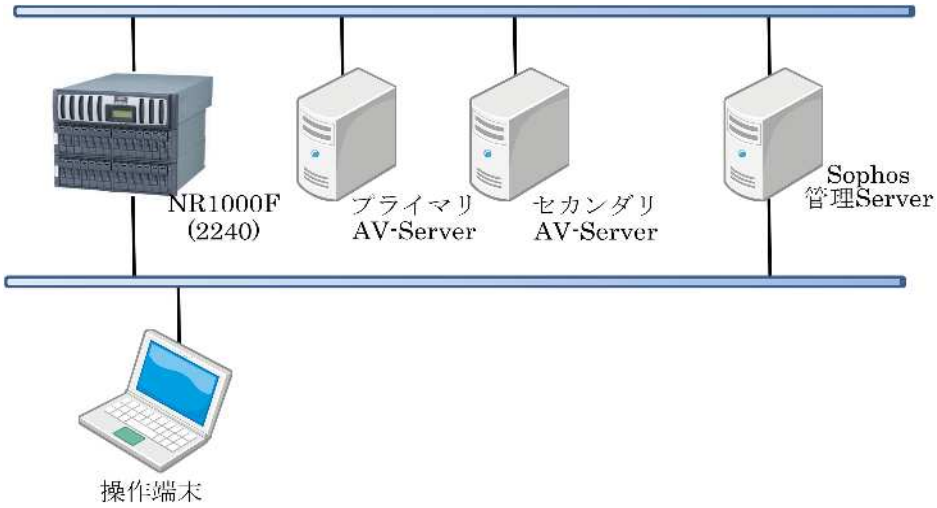
2. 検証概要

次の操作を、WORKGROUP 環境と Active Directory 環境で行い、機能の動作状況を確認します。（NR1000F サーバ（Data ONTAP）と AV サーバ（Anti-Virus サーバ）間の CIFS アクセスでは WORKGROUP 環境と Active Directory 環境で、ユーザ認証（ローカルユーザ、ドメインユーザ等）および設定方法が異なるため、各々の環境で検証を実施します）

- インストール
- AV-Server のプライマリ／セカンダリ設定
- AV-Server の再起動
- MS Office ファイルのファイル操作
- 複数ファイルのコピー操作
- 擬似ウイルスファイルの検知
- AV-Server のプライマリ／セカンダリ切り替え

3. **検証環境**

(ア) 検証環境１（WORKGROUP 環境）



① ETERNUS NR1000F

HW:	2240
OS:	Data ONTAP　8.1.2 7-Mode　（CIFS）
MEM:	12GB
HDD:	600GB(10Krpm)×24 本

② プライマリ AV-Server

HW:	PRIMERGY RX300 S6 (F250)
OS:	Windows 2008 R2 Standard
CPU:	Xeon X5690 3.46GHz/6 コア/12MB コア×2
MEM:	16GB
HDD:	600GB(SAS/10Krpm)×3 [RAID5] ×1
SW:	Sophos Anti-Virus for Windows Ver10.2 Sophos Anti-Virus for NetApp Ver1.01

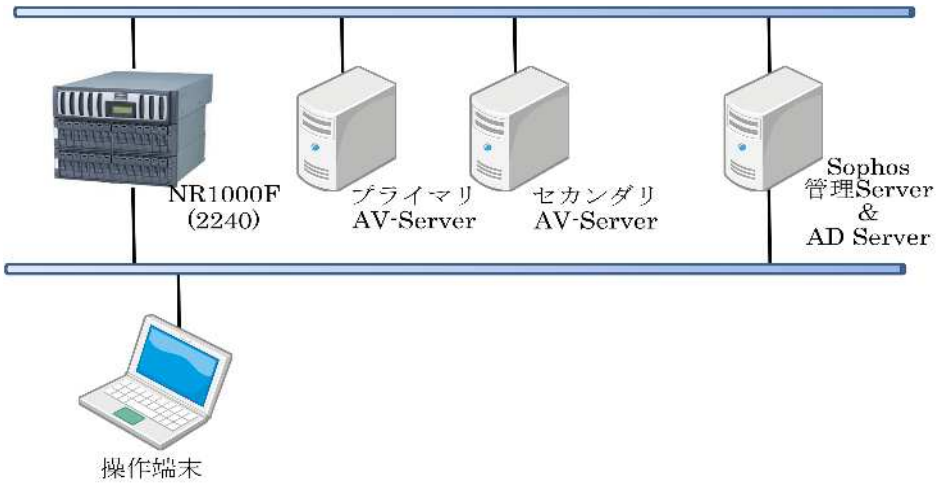
③ セカンダリ AV-Server

HW:	PRIMERGY RX300 S7(F240)
OS:	Windows 2008 R2 Standard
CPU:	Xeon E5-2603 1.8GHz/4 コア/10MB　×2
MEM:	16GB
HDD:	600GB(SAS/10Krpm)×3 [RAID5] ×1
SW:	Sophos Anti-Virus for Windows Ver10.2 Sophos Anti-Virus for NetApp Ver1.01

④ Sophos 管理 Server

HW:	PRIMERGY RX300 S6 (F250)
OS:	Windows 2008 R2 Standard
CPU:	Xeon X5690 3.46GHz/6 コア/12MB コア×2
MEM:	16GB
HDD:	600GB(SAS/10Krpm)×3 [RAID5] ×1
SW:	Sophos Enterprise Console 5.2 NetApp SystemManager

(イ) 検証環境２（Active Directory 環境）



① ETERNAUS NR1000F

HW:	2240
OS:	Data ONTAP　8.1.2 7-Mode　（CIFS）
MEM:	12GB
HDD:	600GB(10Krpm)×24 本

② プライマリ AV-Server

HW:	PRIMERGY RX300 S6 (F250)
OS:	Windows 2008 R2 Standard
CPU:	Xeon X5690 3.46GHz/6 コア/12MB コア×2
MEM:	16GB
HDD:	600GB(SAS/10Krpm)×3 [RAID5] ×1
SW:	Sophos Anti-Virus for Windows Ver10.2 Sophos Anti-Virus for NetApp Ver1.01

③ セカンダリ AV-Server

HW:	PRIMERGY RX300 S7(F240)
OS:	Windows 2008 R2 Standard
CPU:	Xeon E5-2603 1.8GHz/4 コア/10MB　×2
MEM:	16GB
HDD:	600GB(SAS/10Krpm)×3 [RAID5] ×1
SW:	Sophos Anti-Virus for Windows Ver10.2 Sophos Anti-Virus for NetApp Ver1.01

④ Sophos 管理 Server & AD Server

HW:	PRIMERGY RX300 S6 (F250)
OS:	Windows 2008 R2 Standard
CPU:	Xeon X5690 3.46GHz/6 コア/12MB コア×2
MEM:	16GB
HDD:	600GB(SAS/10Krpm)×3 [RAID5] ×1
SW:	Sophos Enterprise Console 5.2 NetApp SystemManager Active Directory

4. **検証結果**

	検索項目数		結果
	設定数	実施数	
検証環境１（WORKGROUP 環境）	7	7	良好
検証環境２（Active Directory 環境）	7	7	良好

5. **検証詳細**

(ア) 検証環境１（WORKGROUP 環境）

	検証項目	検証内容	確認方法	結果
1	インストール	インストール後の AV-Server と ETERNUS NR1000F 間の通信確立を確認する。	・ETERNUS NR1000F に CIFS の共有領域及び CIFS の共有領域にアクセスするためのローカルユーザを作成する。 ・2 台の AV-Server に Sophos Anti-Virus for Windows と Sophos Anti-Virus for NetApp をインストールする（ローカルユーザにて接続するように設定）。 ・ETERNUS NR1000F にて vscan コマンドを実行し、プライマリ／セカンダリ AV-Server の 2 台が表示されたことを確認する。 ・プライマリ／セカンダリ AV-Server の管理画面を表示し、信号機アイコンが緑色になっていることにより通信確立を確認する	良好
2	AV-Server のプライマリ／セカンダリ設定	2 台の AV-Server でプライマリ／セカンダリ構成後、AV-Server と ETERNUS NR1000F 間の通信確立を確認する。	・ETERNUS NR1000F にて「vscan scanners secondary_scanners」コマンドを実行する。 ・2 台の AV-Server の内、セカンダリ AV-Server の「P/S」項目が「Sec」と表示されることを vscan コマンドを実行して確認する。 ・プライマリ／セカンダリ AV-Server の管理画面を表示し、信号機アイコンが緑色になっていることにより通信確立を確認する	良好
3	AV-Server の再起動	プライマリ／セカンダリ AV-Server の再起動後、AV-Server と ETERNUS NR1000F と通信確立を確認する	・ETERNUS NR1000F にて vscan コマンドを実行し、プライマリ／セカンダリ AV-Server の 2 台が表示されたことを確認する。 ・プライマリ／セカンダリ AV-Server の管理画面を表示し、信号機アイコンが緑色になっていることにより通信確立を確認する	良好
4	MS Office ファイルのファイル操作	MS Word の「新規文書作成」、「上書き保存」、「別ファイル名保存」のの各々の操作を行った時に、ウイルス検索が実行されていることを確認する。 本検証は、ETERNUS NR1000F の共有フォルダ上で MS Word の操作により確認する。	・AV-Server の管理画面にて「Ctrl + Alt + D」キーを押し、デバッグモードに変更する。 ・操作端末にローカルユーザでログインし ETERNUS NR1000F の共有フォルダを開く。 ・ETERNUS NR1000F の共有フォルダに MS Word にて新規文書を作成後、ウイルス検索されたことをログファイルで確認する。 ・MS Word で作成したファイルを編集後、上書き保存後、ウイルス検索されたことをログファイルで確認する。	良好

			・MS Word で作成したファイルを編集後、別のファイル名で保存後、ウイルス検索されたことをログファイルで確認する	
5	複数ファイルのコピー操作	複数のファイルのコピーでの書込み／読み込み動作時に、ウイルス検索が実行されていることを確認する。 本検証は検証用に用意した複数のファイルを使用し、ETERNUS NR1000F の共有フォルダにコピーすることで確認する。	・AV-Server の管理画面にて「Ctrl + Alt + D」キーを押し、デバッグモードに変更する。 ・操作端末にローカルユーザでログインする。 ・複数のファイルを操作端末より ETERNUS NR1000F の共有フォルダにコピー後、ウイルス検索されたことをログファイルで確認する。 ・複数のファイルを操作端末より ETERNUS NR1000F の共有フォルダにコピー後、ウイルス検索されたことをログファイルで確認する	良好
6	擬似ウイルスファイルの検知	ウイルスが検知／クリーンアップ処理が行われることを、擬似ウイルスファイル（eicar）を使用して確認する。	・操作端末にローカルユーザでログインする。 ・擬似ウイルスファイル（eicar）を操作端末より ETERNUS NR1000F の共有フォルダにコピーする。 ・ログファイルに、ウイルス検知のメッセージが出力されたこと確認する。 ・ETERNUS NR1000F の共有フォルダよりファイルが削除されていること、クリーンアップ設定したフォルダへの移動処理をログファイルで確認する。	良好
7	AV-Server のプライマリ／セカンダリ切り替え	プライマリ AV-Server に障害（ハード、ネットワーク、アプリケーションなど）が発生した時に、セカンダリ AV-Server への切り替えが行われるかの確認。 本検証では、アプリケーション障害を想定し、オンアクセス検索を停止させることで、擬似的にアプリケーション障害を発生させ、ウイルス検知／クリーンアップ処理がセカンダリ AV-Server で行われるかを確認する。	・プライマリ AV-Server のオンアクセス検索を停止する。 ・操作端末にローカルユーザでログインする。 ・擬似ウイルスファイル（eicar）を操作端末より ETERNUS NR1000F の共有フォルダにコピーする。 ・セカンダリ AV-Server のログファイルに、ウイルス検知のメッセージが出力されたこと確認する。 ・ETERNUS NR1000F の共有フォルダよりファイルが削除されていること、クリーンアップ設定したフォルダへの移動処理をセカンダリ AV-Server のログファイルで確認する。	良好

(イ) 検証環境２（Active Directory 環境）

	検証項目	検証内容	確認方法	結果
1	インストール	インストール後の AV-Server と ETERNUS NR1000F 間の通信確立を確認する。	・ETERNUS NR1000F に CIFS の共有領域にアクセスするためのドメインユーザを作成する。 ・2 台の AV-Server に SAV for Windows/SAV for NetApp をインストールする（ドメインユーザで接続するように設定）。 ・ETERNUS NR1000F にて vscan コマンドを実行し、プライマリ／セカンダリ AV-Server の 2 台が表示されたことを確認する。 ・プライマリ／セカンダリ AV-Server の管理画面を表示し、信号機アイコンが緑色になっていることにより通信確立を確認する	良好
2	AV-Server のプライマリ／セカンダリ設定	2 台の AV-Server でプライマリ／セカンダリ構成後、AV-Server と ETERNUS NR1000F 間の通信確立を確認する。	・ETERNUS NR1000F にて「vscan scanners secondary_scanners」コマンドを実行する。 ・2 台の AV-Server の内、セカンダリ AV-Server の「P/S」項目が「Sec」と表示されることを vscan コマンドを実行して確認する。 ・プライマリ／セカンダリ AV-Server の管理画面を表示し、信号機アイコンが緑色になっていることにより通信確立を確認する	良好
3	AV-Server の再起動	プライマリ／セカンダリ AV-Server の再起動後、AV-Server と ETERNUS NR1000F と通信確立を確認する	・ETERNUS NR1000F にて vscan コマンドを実行し、プライマリ／セカンダリ AV-Server の 2 台が表示されたことを確認する。 ・プライマリ／セカンダリ AV-Server の管理画面を表示し、信号機アイコンが緑色になっていることにより通信確立を確認する	良好
4	MS Office ファイルのファイル操作	MS Word の「新規文書作成」、「上書き保存」、「別ファイル名保存」のの各々の操作を行った時に、ウイルス検索が実行されていることを確認する。 本検証は、ETERNUS NR1000F の共有フォルダ上で MS Word の操作により確認する。	・AV-Server の管理画面にて「Ctrl + Alt + D」キーを押し、デバッグモードに変更する。 ・操作端末にドメインユーザでログインする。 ・ETERNUS NR1000F の共有フォルダに MS Word にて新規文書を作成後、ウイルス検索されたことをログファイルで確認する。 ・MS Word で作成したファイルを編集後、上書き保存後、ウイルス検索されたことをログファイルで確認する。 ・MS Word で作成したファイルを編集後、別のファイル名で保存後、ウイルス検索されたことをログファイルで確認する	良好
5	複数ファイルのコピー操作	複数のファイルのコピーでの書込み／読み込み動作時に、ウイルス検索が実行されていることを確認する。 本検証は検証用に用意した複数のファイルを使用し、ETERNUS NR1000F の共有フォルダにコピーすることで確認する。	・AV-Server の管理画面にて「Ctrl + Alt + D」キーを押し、デバッグモードに変更する。 ・操作端末にドメインユーザでログインする。 ・複数のファイルを操作端末より ETERNUS NR1000F の共有フォルダにコピー後、ウイルス検索されたことをログファイルで確認する。 ・複数のファイルを操作端末より ETERNUS NR1000F の共有フォルダにコピー後、ウイルス検索されたことをログファイルで確認する	良好

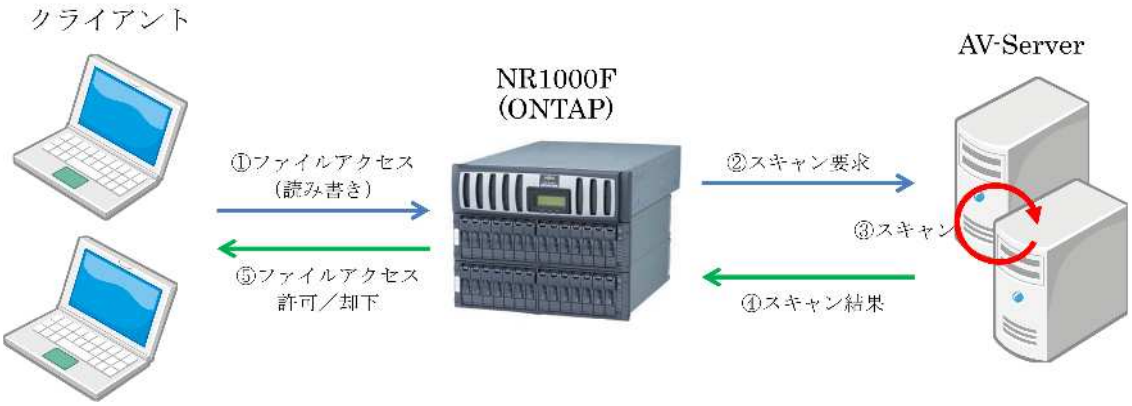
6	擬似ウイルスファイルの検知	ウイルスが検知／クリーンアップ処理が行われることを、擬似ウイルスファイル（eicar）を使用して確認する。	・ドメインユーザでログインする ・擬似ウイルスファイル（eicar）を操作端末よりETERNUS NR1000F の共有フォルダにコピーする。 ・ログファイルに、ウイルス検知のメッセージが出力されたこと確認する。 ・ETERNUS NR1000F の共有フォルダよりファイルが削除されていること、クリーンアップ設定したフォルダへの移動処理をログファイルで確認する。	良好
7	AV-Server のプライマリ／セカンダリ切り替え	プライマリ AV-Server に障害（ハード、ネットワーク、アプリケーションなど）が発生した時に、セカンダリ AV-Server への切り替えが行われるかの確認。 本検証では、アプリケーション障害を想定し、オンアクセス検索を停止させることで、擬似的にアプリケーション障害を発生させ、ウイルス検知／クリーンアップ処理がセカンダリ AV-Server で行われるかを確認する。	・プライマリ AV-Server のオンアクセス検索を停止する。 ・操作端末にドメインユーザでログインする ・擬似ウイルスファイル（eicar）を操作端末よりETERNUS NR1000F の共有フォルダにコピーする。 ・セカンダリ AV-Server のログファイルに、ウイルス検知のメッセージが出力されたこと確認する。 ・ETERNUS NR1000F の共有フォルダよりファイルが削除されていること、クリーンアップ設定したフォルダへの移動処理をセカンダリ AV-Server のログファイルで確認する。	良好

6. システム構成について（参考）

- 最小のサーバ構成として、管理サーバ×1 台、AV サーバ×２台の専用サーバを推奨します。
  ※本番の Active Directory 環境では、管理サーバと AD サーバは共存しない構成を推奨します。
  ※検証環境の AV サーバでは、メモリ２GB、ディスク４０GB（OS 含む）のリソースを使用していました。
- ネットワーク構成として、クライアント⇔ETERNUS NR1000F、ETERNUS NR1000F⇔AV サーバの接続は別セグメントでの接続を推奨します。
- ETERNUS NR1000F サーバへのアクセスが多い環境での AV サーバ構成の検討では、高性能な AV サーバを使用するより、通常スペックの AV サーバ台数を増やしたほうが効果的です。
- ETERNUS NR1000F サーバ移行時に CIFS 領域をフルスキャンする場合、ディスク容量よりファイル数が多い構成の方が、ウイルス検索時間が長くなる傾向があります。（ウイルス検索では、ファイルタイプにより異なりますが、ファイル内のウイルスに感染していると想定している部分のみを検索します）

7. **ウイルス検索の処理フロー（参考）**

クライアントから ETERNUS NR1000F にアクセスした時の、ウイルス検索の簡単な処理フローを記載します。



※ETERNUS NR1000F（ONTAP）のウイルス検索（vscan）では、CIFS のみをサポートしています。（ETERNUS NR1000F サーバへのデータ復旧で ONTAP のバックアップ／リストア機能を利用する場合、ウイルス検索は実行されません）

8. **まとめ**

本検証のすべての項目において、結果は良好であり、問題となる事象は確認されませんでした。

9. **問い合わせ先**

ソフォス株式会社

電話番号　：03-3568-7550（代表）

Email　　：salse@sophos.co.jp