

# 検証報告書

文書番号:SEET160045-01 検証実施者:白坂 健一郎 検証期間:2016/7/11 - 2016/7/25

富士通製ストレージ ETERNUS NR1000 F2552 (clustered Data ONTAP 8.3.2)

と PowerChute Network Shutdown を用いた電源連動検証

備考

本検証作業時に使用した機器の部品及び、仕様は予告なしに変更される場合がございます。 機器仕様変更後の動作可否については、本ドキュメントをもって保障しないことをご承知おき下さい。

Data ONTAP は、米国 NetApp 社の米国およびその他の国における登録商標または商標です。

Microsoft, および Windows は、米国 Microsoft Corporation の、米国およびその他の国における 登録商標または商標です。 Windows の正式名称は、Microsoft Windows Operating System です。 本ドキュメントでは以下の通り省略して記載しております。 Microsoft® Windows® Server 2012 R2 ⇒ Windows Server 2012 R2

Red Hat、Red Hat Enterprise Linux は米国およびその他の国において登録された Red Hat, Inc. の商標です。

# 目次

1.		検証の背景	4
2.		検証内容概要	4
3.		検証期間および検証実施場所	4
4.		検証機器構成	4
	4.	1 ハードウェア構成	4
	4.	2 ネットワーク構成	5
	4.	3 SSH, RSH 実行環境	5
		4.3.1 Windows Server 2012 R2 Standard Update 環境	5
		4.3.2 Red Hat Enterprise Linux 7.0 (for Intel64)環境	5
5.		検証結果	6
6.		富士通製ストレージ ETERNUS NR1000 シャットダウン方法	7
7.		作業全体の流れ	8
8.		シャットダウン環境構築(RSHの場合)	9
	8.	1 NR1000の設定(Windows/Linux 共通)	9
		8.1.1 管理ファイアーウォール設定の確認1	0
		8.1.2 管理ファイアーウォールポリシーのコピー1	0
		8.1.3 管理ファイアーウォールポリシーの編集1	0
		8.1.4 管理ファイアーウォールポリシーの有効化 1	1
		8.1.5 PCNS 用ユーザーの追加1	1
	8.	2 RSH 実行環境の構築(Windows の場合) 1	2
		8.2.1 Cygwin のインストール1	2
		8.2.2 NR1000 への接続確認 (RSH)1	3
	8.	3 RSH 実行環境の構築(Linux の場合)1	4
9.		シャットダウン環境構築(SSHの場合) 1	5
	9.	1 NR1000の設定(Window/Linux 共通)1	5
	9.	2 SSH 実行環境の構築(Windows の場合) 1	5
		9.2.1 Cygwin のインストール1	5
		9.2.2 NR1000 へのログイン1	6
		9.2.3 SSH-RSA 鍵の作成1	7
		9.2.4 PCNS 用ユーザーの追加 (SSH) 1	8
		9.2.5 PCNS 用ユーザーへ公開鍵を登録1	9
		9.2.6 公開鍵の確認1	9
		9.2.7 NR1000 への接続確認(SSH-RSA 鍵認証) 2	20
	9.	3 SSH 実行環境の構築(Linux の場合) 2	!1
		9.3.1 NR1000 へのログイン 2	21
		9.3.2 SSH-RSA 鍵の作成	22
		9.3.3 PCNS 用ユーザーの追加 (SSH) 2	23

9.3.4 PCNS 用ユーザーへ公開鍵を登録	
9.3.5 登録公開鍵の確認	
9.3.6 NR1000 への接続確認(SSH-RSA 鍵認証)	
10. PCNS のインストール	
10.1 Windows の場合	
10.2 Linux の場合	
10.3 PCNS のインストールマニュアルについて	
11. NR1000 シャットダウン命令発行用スクリプトの作成	
11.1 RSH 用スクリプトの作成- <windows></windows>	
11.2 SSH 用スクリプトの作成- <windows></windows>	
11.3 RSH 用スクリプトの作成- <linux></linux>	
11.4 SSH 用スクリプトの作成- <linux></linux>	
12. PCNSの設定	
12.1 Windows の場合	
12.1.1 イベントの設定	
12.1.2 UPS シャットダウンの設定	
12.1.3 コマンド実行の設定	
12.2 Linux の場合	
12.2.1 イベントの設定	
12.2.2 UPS シャットダウンの設定	
12.2.3 コマンド実行の設定	
13. シャットダウンシーケンス	
13.1 シーケンス概要	
13.2 電源障害発生時におけるシステム全体のシャットダウンシーケンス	
13.3 PowerChute Network Shutdown のイベントログ	
13.4 UPS のイベントログ	
14. お問い合わせ先	

# 1. 検証の背景

富士通グループとの共同提案実施時に富士通製ストレージ ETERNUS NR1000 を含めた構成が増加 傾向にあり、且つ、電源障害発生時における弊社製 UPS を用いた電源連動の要望が増加してい るため、今回の検証を行いました。

### 2. 検証内容概要

富士通製サーバ、富士通製ストレージ ETERNUS NR1000 を含む IT 機器に給電している APC Smart-UPS が電源障害を検出した際に、弊社電源管理ソフトウェア PowerChute Network Shutdown®を用いて安全にシステム全体のシャットダウンが行える環境を構築・動作検証を実施しま す。

# 3. 検証期間および検証実施場所

検証期間:2016 年 7 月 11 日~2016 年 7 月 25 日 検証場所:富士通検証センター(東京・浜松町)

#### 4. 検証機器構成

4.1 ハードウェア構成

No	機器名	OS / Version情報
1	富士通製PCサーバ PRIMERGY RX2540 M1	Windows Server 2012 R2 Standard Update
2	富士通製PCサーバ PRIMERGY RX2540 M1	Red Hat Enterprise Linux 7.0 (for Intel64)
3	富士通製ストレージ ETERNUS NR1000 F2552	clustered Data ONTAP 8.3.2
4	富士通製セキュアスイッチ SR-S308TL1	
5	PowerChute Network Shutdown	v4. 1. 0
6	APC Network Management Card 2	AOS v6.4.0, sumx v6.4.0
7	APC Smart-UPS 1500 LCD	
8	Cygwin	2.5.2-1, 64-bit installation

表1. 使用機器一覧

# 4.2 ネットワーク構成

図1. 機器接続構成



### 4.3 SSH, RSH 実行環境

# 4.3.1 Windows Server 2012 R2 Standard Update 環境

表 2. SSH. RSH バージョン情報

Application	Version		
Open SSH	7. 2p2-1		
RSH	0. 17-2		

4. 3. 2	<b>Red Hat</b>	Enterprise	Linux 7.0	(for	Intel64)環境
---------	----------------	------------	-----------	------	------------

表 3. SSH. RSH バージョン情報

Application	Version
Open SSH	6. 4p1-8
RSH	0. 17–75

# 5. 検証結果

弊社電源管理ソフトウェア PowerChute Network Shutdown (以下 PCNS と記載) を用いて ETERNUS NR1000 F2552(以下 NR1000 と記載)を含めたシステム全体のシャットダウン環境の構 築、および、シャットダウン動作が正常に行われることを確認しました。 概要は下記となります。

- > RSH もしくは SSH を使用し、Windows Server 2012 R2 Standard Update (以下 Windows と記載)、Red Hat Enterprise Linux 7.0 (for Intel64) (以下 Linux と記載)共に正常 にシャットダウン可能
- クラスタ環境の NR1000 もシャットダウン可能

#### ※環境構築時のポイント

PCNS を用いて NR1000 をシャットダウンするためには予め以下準備が必要です。

- > Windows の場合は、SSH、もしくは、RSH のコマンドを実行する環境を別途構築する
- > RSH の場合は、NR1000 側で管理ファイアーウォールポリシーの設定、及び、ログイン ユーザーの設定を行う
- > SSH の場合は、サーバ、及び、NR1000 にてログインユーザーの設定、及び、SSH 公開 鍵認証の設定を行う

【注意】

今回は UPS からの停電信号を受信し、システム全体がシャットダウンされることの確認のみ実施したため、全ての機器は UPS から給電されておりません。 実際の環境では、ネットワーク機器を含めたシステム全体の最大消費電力を考慮に入れた上で、

適切な VA 容量、並び、バッテリバックアップ時間が確保される UPS をご選択下さい。

### 6. 富士通製ストレージ ETERNUS NR1000 シャットダウン方法

NR1000 をシャットダウンするには、当該機器の Data ONTAP (ストレージ OS) 管理インターフ ェースにてシャットダウンを実行する必要があります。 管理インターフェースへのアクセス方法は下記4通りとなります。

- > シリアルコンソール
- > SSH (SSHv2)
- > RSH
- ▶ Telnet

予め用意したスクリプトを PCNS 経由で実行させるため、今回は SSH、及び、RSH を用いた方法 を検証しました。

SSHでは、パスワード認証による対話型ログインはスクリプトの利用が困難であることから、 今回は鍵認証方式を採用しました。

本ドキュメントでは、RSH と SSH、双方の検証結果を記載いたしましたが、RSH はセキュアなプロトコルではないため、SSH を使用することをお勧めします。

PCNS を用いたシャットダウン実施時の信号の流れを以下に記載しております。

図 2. シャットダウンシーケンス



# 7. 作業全体の流れ

本ドキュメントにおける作業の流れは下記の通りとなります。

- > NR1000の設定(Windows/Linux共通)
- NR1000へのRSH、もしくは、SSHログイン環境の構築
   ※ NR1000をシャットダウンするスクリプトを実行するサーバにて、RSH、もしくは
  - SSHでNR1000ヘログインできる環境を構築します。
- ➢ PCNSのインストール
- ▶ NR1000シャットダウン用スクリプトの作成
- PCNSシャットダウン設定

- 8. シャットダウン環境構築(RSHの場合)
  - 8.1 NR1000の設定(Windows/Linux 共通)

NR1000の場合、デフォルトでは RSH は無効です。 RSH 接続を使用する場合は、RSH 要求がファイアーウォールを通過できるように、管理ファイア ーウォールポリシーで RSH を有効とする必要があります。 今回は以下を実施しました。

- > 管理ファイアーウォール設定の確認
- 管理ファイアーウォールポリシーのコピー
- ▶ 管理ファイアーウォールポリシーの編集
- > 管理ファイアーウォールポリシーの有効化
- ※ 管理ファイアーウォールポリシーの編集方法については、NetApp clustered Data ONTAP 8.3 システムアドミニストレーションガイド(クラスタ管理) 部品番号: 215-09540\_A0 に記載され ております。

ドキュメントリンク:https://library.netapp.com/ecm/ecm\_download\_file/ECMP1719718

#### 8.1.1 管理ファイアーウォール設定の確認

SSH、または、シリアルコンソールから NR1000 の Data ONTAP 管理インターフェースへ ログインし、下記コマンドを入力して現在の管理ファイアーウォールポリシーを確認 します。

例)

>>system services firewall policy show

# 8.1.2 管理ファイアーウォールポリシーのコピー

Data ONTAP では、事前定義されているファイアーウォールポリシーの変更が出来ない ため、事前定義された管理ファイアーウォールポリシーをコピーし、コピーしたポリ シーで RSH を有効にします。

下記コマンドを使用して新しい管理ファイアーウォールポリシーを作成します。

例)

- vserver : cluster\_mgmt
- ポリシー:mgmt
- 保存先 vserver : cluster\_mgmt
- 新規ポリシー:mgmt\_pcns

>>system services firewall policy clone -vserver cluster\_mgmt -policy mgmt -destinationvserver cluster\_mgmt -destination-policy mgmt\_pcns

# 8.1.3 管理ファイアーウォールポリシーの編集

下記コマンドを使用して、管理ファイアーウォールポリシーに RSH アクセスを有効に する定義を追加します。

例)

- vserver : cluster\_mgmt
- ポリシー:mgmt\_pcns
- サービス:rsh

>>system services firewall policy create -vserver cluster\_mgmt -policy mgmt\_pcns -service rsh -allow-list 0.0.0/0

### 8.1.4 管理ファイアーウォールポリシーの有効化

下記コマンドを使用して、編集した新しい管理ファイアーウォールポリシーを有効に します。

例)

- vserver : cluster\_mgmt
- LIF : cluster\_mgmt
- ファイアーウォールポリシー:mgmt\_pcns

>>network interface modify -vserver cluster\_mgmt -lif cluster\_mgmt -firewall-policy mgmt\_pcns

### 8.1.5 PCNS 用ユーザーの追加

PCNS から NR1000 へ RSH ログインを行う、PCNS 用のユーザー(管理者権限)を作成し ます。

例)

- ユーザー名 : adminpcns
- 認証方式:RSH
- 認証手順:パスワード

>>security login create -username adminpcns -application rsh -authmethod password

ユーザーが問題なく作成されたことを確認するため、以下のコマンドを実行してユー ザー情報を確認します。

>>security login show

#### 8.2 RSH 実行環境の構築(Windows の場合)

# 8.2.1 Cygwin のインストール

Windows Server 2012 R2 上で RSH コマンドが実行可能な環境を構築するため、Cygwin をインストールします。今回は以下の内容でインストールしました。

- Cygwin のインストールパス: C:¥Cygwin64
- インストールしたパッケージ名:表4に記載
- 表 4. インストールパッケージー覧(RSH 実行環境構築時)

#	パッケージ名
1	inetutils-server Common networking clients and servers
2	openssh: The Open SSH server and client programs
3	openssl: A general purpose cryptography toolkit with TLS imple-
	mentation
4	rsh: Clients for remote access commands

インストール後、Windows 環境変数 Path に "<u>C:¥cygwin64¥bin</u>"を追加します。 スタートボタンからコンピューターを選択、右クリックで "<u>プロパティ</u>"を選択しま す。次に、システムの詳細設定を選択し、システムのプロパティ画面を開きます。"<u>詳</u> <u>細設定</u>"画面内の "<u>環境変数</u>"ボタンを押すことで環境変数の設定画面が表示されま す。環境変数画面を表示させたら Path 項目に "<u>C:¥cygwin64¥bin</u>"のパスを 編集ボ タンを押して追加します。

#### 図 3. 環境変数設定画面

Administrator のユーザー環境変数( <u>U</u> )						
	値					
TEMP	%USERPROFILE%¥AppData¥Local¥Temp					
ТМР	%USERPROFILE%¥AppData¥Local¥Temp					
	新規( <u>N</u> ) 編集( <u>E</u> ) 削除( <u>D</u> )					
ステム環境変数( <u>S</u> ) 変数	(fi )					
ステム環境変数( <u>S)</u> 変数 NUMBER OF PR	值 64					
ステム環境変数( <u>S)</u> 変数 NUMBER_OF_PR OS	値 64 Windows NT					
ステム環境変数( <u>S</u> ) 変数 NUMBER_OF_PR OS Path	値 64 Windows NT C:¥ProgramData¥Oracle¥Java¥javapat					
ステム環境変数( <u>S</u> ) 変数 NUMBER_OF_PR OS Path PATHEXT DPOCESSOD_AP	値 64 Windows NT C:¥ProgramData¥Oracle¥Java¥javapat .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.J					
ステム環境変数( <u>S</u> ) 変数 NUMBER_OF_PR OS Path PATHEXT DPOCESSOD AD	值 64 Windows NT C:¥ProgramData¥Oracle¥Java¥javapat .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.J AMD64 新規( <u>W</u> ) 編集(I) 削除(L)					

# 8.2.2 NR1000 への接続確認 (RSH)

以下のコマンドを使用して、PCNS 用ユーザーにて NR1000 へ RSH でログインし、ユー ザー情報が表示できることを確認します。ユーザー情報が表示されれば問題ありません。

>>rsh <ONTAP IP Address> -| <PCNS 用ユーザー名>:<設定した Password> security login show adminpcns

### 図 4. RSH を用いた NR1000 への接続確認コマンド入力結果 (Windows)

G4.		管理者: コマンド	プロンプト		-		x		
licrosoft Windows [Version 6.3.9600] c) 2013 Microsoft Corporation. All rights reserved.									
C:¥Users¥Administ 10.20.111.20:513:	rator>rsh 10 Connection	).20.111.20 -1 a refused	adminpens:Root0000	)					
C:¥Users¥Administ w adminpcns	rator>rsh 10	).20.111.20 -l a	adminpens:Root0000	) security	loa	sin s	sho		
Vserver: cluster_	_mgmt	A+L+ :+ :		<b>≬</b> +					
User/Group Name	Application	Method	Role Name	ACCT Locked					
adminpcns adminpcns 2 entries were di	rsh ssh splayed.	password publickey	admin admin	no -					
C:¥Users¥Administ	:rator> <mark>_</mark>								

#### 8.3 RSH 実行環境の構築(Linux の場合)

Linux の場合は、OS の RSH 機能を使用します。

「8.1 NR1000 の設定 (Window/Linux 共通)」を行った後、以下のコマンドを使用して、 PCNS 用ユーザーにて NR1000 へ RSH ログインし、ユーザー情報が表示できることを確 認します。ユーザー情報が表示されれば問題ありません。

>>rsh <ONTAP IP Address> -| <PCNS 用ユーザー名>:<設定した Password> security login show adminpcns

図 5. RSH を用いた NR1000 への接続確認コマンド入力結果 (Linux)

[root@rx2540m1-15 デスクトップ]# rsh 10.20.111.20 -l adminpons:Root0000 security login show adminpcns Vserver: cluster\_mgmt Authentication Acct User/Group Name Application Method Role Name Locked . - - - - - password adminpcns rsh admin no publickey admin adminpcns ssh -2 entries were displayed.

# 9. シャットダウン環境構築(SSHの場合)

9.1 NR1000の設定(Window/Linux 共通)
 NR1000では、SSH(v2)はデフォルトで有効となっているため、NR1000側でのSSHに関する設定変更(管理ファイアーウォールポリシーの変更等)は不要です。

### 9.2 SSH 実行環境の構築(Windows の場合)

#### 9.2.1 Cygwinのインストール

Windows Server 2012 R2 上で SSH コマンドが実行可能な環境を構築するため、Cygwin をインストールします。今回は以下の内容でインストールしました。

Cygwin のインストールパス:C:¥Cygwin64

表 5. インストールパッケージ名 (SSH 実行環境構築時)

#	パッケージ名
1	inetutils-server Common networking clients and servers
2	openssh: The Open SSH server and client programs
3	openssl: A general purpose cryptography toolkit with TLS imple-
	mentation
4	rsh: Clients for remote access commands

インストール後、Windows 環境変数 Path に "<u>C:¥cygwin64¥bin</u>"を追加します。 スタートボタンからコンピューターを選択、右クリックで "<u>プロパティ</u>"を選択しま す。次に、システムの詳細設定を選択し、システムのプロパティ画面を開きます。"<u>詳</u> <u>細設定</u>"画面内の "<u>環境変数</u>"ボタンを押すことで環境変数の設定画面が表示されま す。環境変数画面を表示させたら Path 項目に "<u>C:¥cygwin64¥bin</u>"のパスを 編集ボ タンを押して追加します。

図 6. システム環境変数編集画面

	環境変数	x					
Administratorのフーザー環境亦数(II)							
Administration のユージー 泉沢送太( <u>ロ</u> )							
変数 1世 TEMD %LISERDROETLE%¥AppData¥Local¥Temp							
TMP %USERPROFILE%#AppData#Local#Temp %USERPROFILE%#AppData#Local#Temp							
新規( <u>N</u> ) 編集( <u>E</u> ) 削除( <u>D</u> )							
システム環境変数( <u>S</u> ) 変数	値 ^						
NUMBER_OF_PR	. 64						
OS	Windows NT						
Path	C:¥ProgramData¥Oracle¥Java¥javapat						
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.J						
DDOCECCOD AD		]					
新規( <u>₩</u> ) 編集( <u>I</u> ) 削除( <u>L</u> )							
OK         キャンセル							

### 9.2.2 NR1000 へのログイン

コマンドプロンプトを開き、既存ユーザー(管理者権限)で NR1000 に SSH でログイン 出来ることを確認します。

>>ssh <ONTAP IP Address> -| <userID>

図 7. SSH を用いた NR1000 へのログインコマンド入力結果 (Windows)



ログインできることを確認したら、一旦ログオフします。 ※ログオフのコマンドは "<u>exit</u>"です。

### 9.2.3 SSH-RSA 鍵の作成

Cygwinの機能を使用して SSH-RSA 鍵を作成します。以下のコマンドを実行します。

>>ssh-keygen -t rsa

### [指定項目]

- 鍵の名前:\*\*\*\*\_rsa
- パスフレーズ: 空白のまま(何も入力しない)
- 保存先/鍵名称: C:¥Program Files¥APC¥PowerChute¥PCNSScript¥\*\*\*\*\_rsa

以下の SSH-RSA の公開鍵および秘密鍵が生成されます。

公開鍵:\*\*\*\*\_rsa.pub ② 秘密鍵:\*\*\*\*\_rsa

#### 図 8. SSH-RSA 鍵作成コマンド入力結果(Windows)

C:¥Users¥Administrator>ssh-keygen -t rsa -Generating public/private rsa key pair. Enter file in which to save the key (/home/Administrator/.ssh/id\_rsa): C:¥Progra m Files¥APC¥PowerChute¥PCNSScript¥pcns\_rsa Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in C:¥Program Files¥APC¥PowerChute¥PCNSScript ¥pcns\_rsa. Your public key has been saved in C:¥Program Files¥APC¥PowerChute¥PCNSScript¥pcr \_rsa.pub. The key fingerprint is: SHA256:rmJbBRGW67kBZtK80+fHRvzWcPi90tv166tpxjbvamQ\_Administrator@rx2540m1-03\_ The key's randomart image is: ---[RSA 2048]----+ o =o. o oE. =.0 .+=.. o.... + <u>o</u>O+.= .o. o .=+00B FSHA2567----

### 9.2.4 PCNS 用ユーザーの追加 (SSH)

NR1000 にすでに存在する既存のユーザー(管理者権限)にて、NR1000 へ SSH でログイ ンします。 NR1000 上で、PCNS 用のユーザー(管理者権限)を作成します。

- PCNS 用ユーザー名: xxx
- 認証方式: publickey

>>security login create -username <PCNS 用ユーザー名> -application ssh -authmethod publickey

図 9. PCNS 用ユーザー作成コマンド入力 (Windows)

C:¥Users¥Administrator>ssh admin@10.20.111.20 Password: cluster\_mgmt::> security login create -username adminpcns -application ssh -auth method publickey\_

以下の警告が表示されますが、問題ございません。

Warning: To use public-key authentication, you must create a public key for user "<PCNS 用ユーザー名>".

図 10. コマンド入力後の警告表示 (Windows)

C:¥Users¥Administrator>ssh admin@10.20.111.20

<sup>D</sup>assword:

cluster\_mgmt::> security login create -username adminpons -application ssh -auth method publickey

Marning: To use public-key authentication, you must create a public key for user ″adminpons″.

cluster\_mgmt::> 🛓

# 9.2.5 PCNS 用ユーザーへ公開鍵を登録

PCNS 用ユーザーへ「SSH-RSA 鍵の作成」で作成した公開鍵を登録します。 下記コマンドを実行します。

※public-key(赤字で表示している部分)は「SSH-RSA 鍵の作成」で作成したものを利 用して下さい。

>>security login publickey create -username <PCNS 用ユーザー名> -index 5 -publickey "sshrsa …"

#### 図 11. PCNS 用ユーザーへの公開鍵登録画面(Windows)

# ;¥Users¥Administrator>ssh admin@10.20.111.20

<sup>D</sup>assword:

cluster\_mgmt::> security login create -username adminpons -application ssh -auth method publickey

Marning: To use public-key authentication, you must create a public key for user ″adminpens″.

### 9.2.6 公開鍵の確認

PCNS 用ユーザーに公開鍵が登録されたか確認します。 下記コマンドを実行し、設定した公開鍵が表示されれば問題ありません。 >>security login publickey show -username <PCNS 用ユーザー名>

図 12. 公開鍵確認コマンドの入力(Windows)

cluster\_mgmt::> security login publickey show -username adminpcns\_

### 9.2.7 NR1000 への接続確認(SSH-RSA 鍵認証)

SSH 鍵認証によるログインが行えるか確認します。 パスワードを聞かれずに、NR1000 ヘログインできれば問題ありません。

例)

- ユーザー名:\*\*\*\*
- 秘密鍵保存先/名称:C:\Program Files\APC\PowerChute\PCNSScript\\*\*\*\*\_rsa
- 接続先:\*\*\*.\*\*\*.\*\*\*.\*\*\*

使用コマンド:

>>ssh -| <UserID> -i "<秘密鍵保存先および名称>" <ONTAP IP Address>

図 13. SSH-RSA 鍵認証方式を使ったログイン動作の確認(Windows)

C:¥Users¥Administrator>ssh -I adminpons -i "C:¥Program Files¥APC¥PowerChute¥PCNS Script¥adminpons\_rsa" 10.20.111.20 cluster\_mgmt::> \_

# 9.3 SSH 実行環境の構築(Linux の場合)

# 9.3.1 NR1000 へのログイン

既存ユーザー(管理者権限)でNR1000にSSHでログイン出来ることを確認します。

>ssh <ONTAP IP Address> -| <userID>

図 14. SSH-RSA 鍵認証方式を使ったログイン動作の確認 (Linux)

[root@rx2540m1-15	デスクトップ]#	ssh	10.20.111.20	-l	admin
Password:					
cluster_mgmt::>					

ログインができることを確認したら、一旦ログオフします。 ※ログオフのコマンドは "<u>exit</u>"です。

# 9.3.2 SSH-RSA 鍵の作成

SSH-RSA 鍵を作成するため、以下のコマンドを実行します。 >ssh-keygen -t rsa

[指定項目]

- 鍵の名前:\*\*\*\*\_rsa
- パスフレーズ: 空白のまま(何も入力しない)
- 保存先/鍵名称: C:¥Program Files¥APC¥PowerChute¥PCNSScript¥\*\*\*\*\_rsa

以下の SSH-RSA の公開鍵および秘密鍵が生成されます。

公開鍵:\*\*\*\*\_rsa.pub

② 秘密鍵:\*\*\*\*\_rsa

図 15. SSH-RSA 鍵作成コマンド入力結果 (Linux)

[root@rx2540m1-15 デスクトップ]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
1a:f8:b3:a5:7f:d6:f9:01:26:04:2a:6f:5a:0f:f4:d6 root@rx2540m1-15.linux.tcs
The key's randomart image is:
+[ RSA 2048]+
· · · · · ·
=. 0
. * S E O
= * 0.
. + o
= 0 0 .
00
++

#### 9.3.3 PCNS 用ユーザーの追加 (SSH)

NR1000 にすでに存在する既存のユーザー(管理者権限)にて、NR1000 へ SSH でログイ ンします。

NR1000上で、PCNS 用のユーザー(管理者権限)を作成します。

- PCNS 用ユーザー名:xxx
- 認証方式: publickey

>security login create -username <PCNS 用ユーザー名> -application ssh -authmethod publickey

図 16. PCNS 用ユーザー作成コマンド入力 (Linux)

```
[root@rx2540m1-15 デスクトップ]# ssh 10.20.111.20 -l admin
Password:
cluster_mgmt::> security login create -username kshirasa -application ssh -authm
ethod publickey
Warning: To use public-key authentication, you must create a public key for user
"kshirasa".
cluster_mgmt::>
```

以下の警告が表示されますが、問題ございません。

Warning: To use public-key authentication, you must create a public key for user "<PCNS 用ユーザー名>".

#### 9.3.4 PCNS 用ユーザーへ公開鍵を登録

PCNS 用ユーザーへ「SSH-RSA 鍵の作成」で作成した公開鍵を登録します。

下記コマンドを実行します。

※public-key(赤字で表示している部分)は「SSH-RSA 鍵の作成」で作成したものを利 用して下さい。

>security login publickey create -username <PCNS 用ユーザー名> -index 5 -publickey "sshrsa …"

図 17. PCNS 用ユーザーへの公開鍵登録画面 (Linux)

[root@rx2540m1-15 デスクトップ]# ssh 10.20.111.20 -l admin Password: cluster\_mgmt::> security login create -username kshirasa -application ssh -authm ethod publickey Warning: To use public-key authentication, you must create a public key for user "kshirasa".

cluster\_mgmt::> security login publickey create -username kshirasa -index 5 -pub lickey "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCtlCo9sCHluvqOvt8KSxPLiQv4YBeNRKIf G+hi2oXUfvsEGiri2bWiBSFBioXUEE7aDd+eZFujH7/l75tjtt8xzmMAl8siMb3wYw5xHsucmy8nRrJL HxIH96LLEKGCTHQ+YLAZfWx3TytVS9B2XHlc/LKpwKb51ioOaNewYgVF+Q+YiXMm4ysUdIa0TOQe3yEi XVqQjX/7mh6bzJBWAE3j1SHaT8RiwUfSmTjkIZDFN5jbWtPAMhtZ+0wn6Wh0dNiQLu24vm6w2Zs3C/f3 D6PI45U/RWL0XP1IKEC5RNoxqIe56EQMxQ/SalBKNaWk7RUh47208FRC692T8W4Z0+z7 root@rx2540 m1-15.linux.tcs"

cluster\_mgmt::>

### 9.3.5 登録公開鍵の確認

PCNS 用ユーザーに公開鍵が登録されたか確認します。下記コマンドを実行します。 >security login publickey show -username <PCNS 用ユーザー名>

図 18. PCNS 用ユーザー公開鍵確認画面 (Linux)

[root@rx2540m1-15 デスクトップ]# ssh 10.20.111.20 -l admin Password: cluster_mgmt::> security login publickey show -username adminpcns
Vserver: cluster_mgmt UserName: adminpcns Index: 5 Public Kev:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCmJEmZKYSGQsZf8FMpesyoGDcMKznLpQ0zflJo3GvN 7RdE5KR2L/0wdjPlo00Bt2dfBXANkV4yBGc0JwZ7C6a5BG6wh1XKwHlITGzUYQDPUq30pCRPVec+Gl1E +WBW8yRRuz4hwl1u0X656ptfeUZz8M77spCJLsQuHEm0+Cu6YZEowTnb4wKXXBolS0rfNd0P+xTCytgJ ZDsxQPRTu3+NTT2T+Jo+b2ZqQ8G/JM23SqKh45PLMqa92ysXqrhXbyyhb8ZuwpUmRU01DtyYlZQkag40 +u/CjT9FY8vtuQv0BdH0Bgk/PppfCaW7PEhJerc2e8XF0mkkUbxuzlWN0Jxh Administrator@rx254 0m1-03
Fingerprint: 1c:30:63:f5:a3:c9:b6:3b:24:c5:97:6f:fe:6c:82:b2 Bubblebabble fingerprint: xugar-hydug-mokid-vynoc-vazed-pisup-tidyb-zapat-tymoc-pacok-hexex Comment:

設定した公開鍵が表示されれば問題ありません。

### 9.3.6 NR1000 への接続確認(SSH-RSA 鍵認証)

SSH 鍵認証によるログインが行えるか確認します。 パスワードを聞かれずに、NR1000 ヘログインできれば問題ありません。

例)

- ユーザー名:\*\*\*\*
- 秘密鍵保存先/名称:C:\Program Files\APC\PowerChute\PCNSScript\\*\*\*\*\_rsa
- 接続先:\*\*\*.\*\*\*.\*\*\*.\*\*\*

使用コマンド:

>ssh -| <UserID> -i "<秘密鍵保存先および名称>" <ONTAP IP Address>

図 19. SSH-RSA 鍵認証方式を使ったログイン動作の確認(Linux)

```
[root@rx2540m1-15 デスクトップ]# ssh -l adminpcns -i "/opt/APC/PowerChute/PCNSSc
ript/adminpcns_rsa" 10.20.111.20
cluster_mgmt::>
```

## 10. PCNS のインストール

### 10.1 Windows の場合

PCNS をインストールします。インストール先は下記となります。 C:¥Program Files¥APC¥PowerChute

NR1000 シャットダウン用スクリプトファイルは下記に保存します。 ※PCNS インストール後に下記フォルダーを手動で作成下さい。 C:¥Program Files¥APC¥PowerChute¥PCNSScript

尚、PCNS のインストールマニュアルについては 後述する 10.3 の項目を参照願い ます。

#### 10.2 Linux の場合

PCNS をインストールします。インストール先は下記となります。 /opt/APC/PowerChute

NR1000 シャットダウン用スクリプトは下記に保存します。 ※PCNS インストール後に下記フォルダーを手動で作成下さい。 /opt/APC/PowerChute/PCNSScript

尚、PCNS のインストールマニュアルについては 後述する 10.3 の項目を参照願い ます。

# 10.3 PCNS のインストールマニュアルについて

PCNS のインストールマニュアルは下記 URL からダウンロード可能です。 下記 URL から以下の検索条件を選択頂き、PCNS のインストールマニュアルをダウン ロードして下さい。

- 製品カテゴリー:無停電電源装置(UPS)
- ・ 製品サブカテゴリー: UPS Management
- ・ 製品群 : PowerChute Network Shutdown

http://www.schneider-electric.com/jp/ja/download/

# 11. NR1000 シャットダウン命令発行用スクリプトの作成

#### 11.1 RSH 用スクリプトの作成-<Windows>

PCNS が実行する NR1000 シャットダウン命令用のバッチファイルを作成します。 バッチファイル保存先:C:¥Program Files¥APC¥PowerChute¥PCNSScript

NR1000 シャットダウン命令発行用バッチファイルは以下の3個から構成されます。 名称: PCNSUtil.bat (NetAppShut.bat 実行用)

名称: PCNSS leep.vbs (NR1000 シャットダウン命令発行待機用)

名称: NetAppShut. bat (NR1000 シャットダウン命令発行用)

記述例: PCNSUtil.bat

@start /d "C:¥Program Files¥APC¥PowerChute¥PCNSScript" NetAppShut.bat ※PCNS の制限により、NetAppShut.bat を直接実行しないようにしています。

記述例:PCNSSleep.vbs

WScript.Sleep 1000 \* 10 ※NR1000 へのシャットダウン命令発行待機時間:10 秒を想定した記述です。 10 秒と設定する場合は1000 [ミリ秒] \* 10 = 10 [秒] ※実際の運用環境では、NR1000 を利用しているサーバのシャットダウンに要す る時間を確認し、NR1000 シャットダウン命令発行待機時間を調整して下さい。

記述例:NetAppShut.bat

@echo off call cscript "C:¥Program Files¥APC¥PowerChute¥PCNSSleep.vbs" start /d "C:¥Program Files¥APC¥PowerChute¥PCNSScript" rsh.exe 10.20.111.20 -I adminpcns:Root0000 system node halt -node all

※管理インターフェース IP アドレス: 10.20.111.20
※ログイン ID: adminpcns
※パスワード: Root0000

## 11.2 SSH 用スクリプトの作成-<Windows>

PCNS が実行する NR1000 シャットダウン命令用のバッチファイルを作成します。 バッチファイル保存先:C:¥Program Files¥APC¥PowerChute¥PCNSScript

NR1000 シャットダウン命令発行用バッチファイルは以下の3個から構成されます。

名称: PCNSUtil.bat (NetAppShut.bat 実行用)

名称: PCNSS leep.vbs (NR1000 シャットダウン命令発行待機用)

名称: NetAppShut. bat (NR1000 シャットダウン命令発行用)

記述例: PCNSUtil.bat

@start /d "C:¥Program Files¥APC¥PowerChute¥PCNSScript" NetAppShut.bat

※PCNS の制限により、NetAppShut. bat を直接実行しないようにしています。

記述例:PCNSSleep.vbs

WScript.Sleep 1000 \* 10

※NR1000 へのシャットダウン命令発行待機時間:10 秒を想定した記述です。
 10 秒と設定する場合は1000 ミリ秒 x 10 = 10 秒
 ※実際の運用環境では、NR1000 を利用しているサーバのシャットダウンに要する時間を確認し、NR1000 シャットダウン命令発行待機時間を調整して下さい。

記述例:NetAppShut.bat

@echo off

call cscript "C:\Program Files\APC\PowerChute\PCNSSleep.vbs"

start /d "C:¥Program Files¥APC¥PowerChute¥PCNSScript" ssh.exe 10.20.111.20 -o StrictHostKeyChecking=no -l PCNSCygwin -i "C:¥Program Files¥APC¥PowerChute¥PCNSScript¥adminpcns\_rsa" system node halt -node all

※管理インターフェース IP アドレス: 10.20.111.20
 ※ログイン ID: adminpens
 ※初回認証時の通過確認を不要にするため、Host Key Checking を無効にします。

# 11.3 RSH 用スクリプトの作成-<Linux>

PCNS が実行する NR1000 シャットダウン命令用のシェルスクリプトを作成します。 シェルスクリプト保存先:/opt/APC/PowerChute/PCNSScript

NR1000 シャットダウン命令発行用シェルスクリプトは下記となります。 名称: NetAppShut. sh (NR1000 シャットダウン命令発行用)

記述内容: NetAppShut.sh

#!/bin/sh

sleep 10s

rsh 10.20.111.20 - I adminpcns:Root0000 system node halt -node all

※管理インターフェース IP アドレス: 10.20.111.20
 ※ログイン ID: adminpens
 ※パスワード: Root0000
 ※NR1000 へのシャットダウン命令発行待機時間:10 秒を想定した記述です。
 ※実際の運用環境では、NR1000 を利用しているサーバのシャットダウンに要する時間を確認し、NR1000 シャットダウン命令発行待機時間を調整して下さい。

# 11.4 SSH 用スクリプトの作成-<Linux>

PCNS が実行する NR1000 シャットダウン命令用のシェルスクリプトを作成します。 シェルスクリプト保存先:/opt/APC/PowerChute/PCNSScript

NR1000 シャットダウン命令発行用シェルスクリプトは下記となります。 名称: NetAppShut. sh (NR1000 シャットダウン命令発行用)

記述例:NetAppShut.sh

#!/bin/sh

sleep 10s

ssh 10.20.111.20 - I adminpcns -o StrictHostKeyChecking=no -i

/opt/APC/PowerChute/PCNSScript/adminpcns\_rsa system node halt -node all

※管理インターフェース IP アドレス: 10.20.111.20

※ログイン ID: adminpcns

※秘密鍵保存先: /opt/APC/PowerChute/PCNSScript/adminpcns\_rsa

備考:秘密鍵作成後、上記フォルダーに秘密鍵の保存先を変更します。 ※初回認証時の通過確認を不要にするため、Host Key Checking を無効にします。 ※NR1000 へのシャットダウン命令発行待機時間:10 秒を想定した記述です。 ※実際の運用環境では、NR1000 を利用しているサーバのシャットダウンに要す る時間を確認し、NR1000 シャットダウン命令発行待機時間を調整して下さい。

# 12. PCNS の設定

- 12.1 Windows の場合
  - 12.1.1 イベントの設定

UPS オンバッテリ イベントのシャットダウンを有効にします。

シャットダウン開始までの待機時間(復電待機時間):120秒

※待機時間"120秒"は PCNS のデフォルト値となります。運用環境に合わせて適宜調 整して下さい。

PowerChute				rx2540m1-03	3
<ul> <li>► R2540m1-03</li> <li>Tペントログの表示</li> <li>イペントの設定</li> <li>シャットダウン設定</li> <li>通信設定</li> </ul>	イベントの設定 アイコンをクリックし、UPSイベントに応答するPowerの イベント1~16/16 イベント	Chuteイベ)	ントを設定します。 <u>コマンドファイル</u>	<u>シャットダウン</u>	?
PowerChuteセットアッ: > UPSの構成 > ヘルプ ログアウト	<ul> <li>プ 入力電力回復</li> <li>⑦ ランタイム超過</li> <li>⑦ 使用可能なランタイムが+分</li> <li>⑦ ランタイム残り時間がしきい値を下回る</li> </ul>	© © ©	0 0 0	0	
	シャットダウンの設定     イベント名     UPSオンバッテリ       シャットダウンの有効化     ・     ・       待機時間     120     秒	]	適用 =	? *	

図 20. PCNS イベント設定画面

12.1.2 UPS シャットダウンの設定

"<u>UPS の電源をオフにする</u>"を選択します。

当該設定を選択することで、UPS はネットワークマネジメントカードの設定に基づいてサーバシャットダウン完了後に停止します。

図 21. PCNS シャットダウン設定画面(UPS シャットダウン設定)

PowerChute		rx2540m1-03	)
✓ rx2540m1-03	シャットダウン設定		?
イベントログの表示	PowerChuteがシャットダウンシーケンスを開始するとき、以下の設定が使用されます。		_
イベントの設定	▼ UPSシャットダウン	2	
シャットダウン設定		· ·	
通信設定	○ UPSの電源をオフにしない		1
PowerChuteセットアップ	● UPSの電源をオフにする		L
▶ UPSの構成	○ UPSコンセントグループの電源をオフにする		1
▶ ヘルプ	→ コマンド実行	?	
ログアウト			

# 12.1.3 コマンド実行の設定

コマンドファイルのフルパス欄に実行させるコマンドファイル名を入力します。 名称: C:¥Program Files¥APC¥PowerChute¥PCNSScript¥PCNSUtil.bat 所要時間(コマンドファイル実行完了までに必要とされる時間):60秒 ※コマンドファイル実行所要時間は運用環境に合わせて調整して下さい。

図 22. PCNS シャットダウン設定画面 (NR1000 シャットダウンコマンドの登録)

- NETWORK SHUTDOWN		rx2540m1-03	3
▼ rx2540m1-03	シャットダウン設定		?
イベントログの表示	PowerChuteがシャットダウンシーケンスを開始するとき、以下の設定が使用されます。		
イベントの設定	▶ UPSシャットダウン	?	
シャットダウン設定	<ul> <li>マコマンド実行</li> </ul>	?	
通信設定 PowerChuteセットアップ	コマンドファイルのフルパス C:\Program Files\APC\PowerChute\PCNSS	5	
▶ UPSの構成			
▶ ヘルプ ログアウト			

# 12.2 Linux の場合

# 12.2.1 イベントの設定

UPS オンバッテリ イベントのシャットダウンを有効にします。 シャットダウン開始までの待機時間(復電待機時間): 120 秒

ノイクトラウノ開始よどの特徴時间(後电特徴時间)、120 移

※待機時間"120秒"は PCNS のデフォルト値となります。運用環境に合わせて適宜調 整して下さい。

- NETWORK SHUTDOWN						
rx2540m1-15	イベントの設定					?
イベントログの 表示	アイコンをクリックし、UPSイベントに応答する	るPowerChuteイベントを	設定します	-		
イベントの設定	イベント1~16 / 16					
シャットダウン設定		ПŐ	通知	コマンドファイル	シャットダウン	
通信設定	🕑 UPSオンバッテリ	<b>Q</b>	0	Ô	<b>e</b>	_
PowerChuteセットアップ	🕑 入力電力回復	0	0	Ô		
UPSの 構成	● ランタイム超過	9	0	0	0	
ヘルプ	使用可能なランタイムが十分	0	0	Ô		
ログアウト 		-	-	-		_
<u>ې</u>	ヤットダウンの設定				2.36	
	イベント名 U シャットダウンの有効化 待機時間 (	JPSオンバッテリ <b>ヹ</b> 120 秒				

図 23. PCNS イベント設定画面

12.2.2 UPS シャットダウンの設定

"UPS の電源をオフにする"を選択します。

ネットワークマネジメントカードの設定に基づいて、サーバシャットダウン完了後に UPS が停止します。

PowerChute		rx2540m1-15	5
rx2540m1-15	シャットダウン設定		?
イベントログの 表示	PowerChuteがシャットダウンシーケンスを開始するとき、以下の設定が使用されます。		
イベントの設定	▼ UPSシャットダウン	?	
シャットダウン設定	○ UPSの電源をオフにしない		
通信設定 PowerChuteセットアップ	● UPSの電源をオフにする		
▶ UPSの 構成	○ UPSコンセントグルーブの電源をオフにする		
▶ヘルプ	▶ コマンド実行	?	
ログアウト	▶ ユーザへの通知	?	

# 12.2.3 コマンド実行の設定

コマンドファイルのフルパス欄に実行させるコマンドファイル名を入力します。 名称: /opt/APC/PowerChute/PCNSScript/NetAppShut.sh 所要時間(コマンドファイル実行完了までに必要とされる時間):60秒 ※コマンドファイル実行所要時間は運用環境に合わせて調整して下さい。

図 25. PCNS シャットダウン設定画面 (NR1000 シャットダウンコマンドの登録)

イベントログの 表示		始するとき、以下の設定が使用されます。	
イベントの設定	▶ UPSシャットダウン		?
シャットダウン設定	<ul> <li>コマンド実行</li> </ul>		2
通信設定			<b>-</b>
PowerChuteセットアップ	コマンドファイルのフルバス	/opt/APC/PowerChute/PCNSScript/NetAppSI	
▶ UPSの 構成	所罢時間	60 秒 7	

以上で設定は終了です。

13. シャットダウンシーケンス

停電時、以下のシーケンスに基づいて動作することを確認いたしました。

13.1 シーケンス概要

PCNSが停電(UPSバッテリ運転)を検知

②設定した復電待機時間経過後 PCNSによるシャットダウンが開始される

③PCNSがコマンドファイルを実行

④コマンドファイルにてSSHもしくはRSHにてNR1000にログイン、NR1000のシャットダウン実行

※電源復旧時は、NR1000と各サーバは手動で起動させるものとします。

※NR1000 はデフォルトでは給電開始と同時に自動起動します。

# 13.2 電源障害発生時におけるシステム全体のシャットダウンシーケンス

#### 表 6. 電源障害発生時のシステム全体のシャットダウンシーケンス表

機器情報		-								シャ	ットダウン	シーケ	シス											
機架名	のの情報		停電経過時間													-								
1成台口		▲ 停	停電			🕨 停電 👥 📥			▲ UPS停止命令受付				A Outlet Group 1出力停止					▲ UPS出力停止 (Main Outlet				<u>、Group含む)</u>		
		0min		1min	2r	min	3min	4n	nin		5min		6min		7min	8min		9min		10min				
APC Smart-UPS 1500 LCD	AOS v6.4.0	120秒		180秒				180秒				出力傳	亭止											
					1	)UPSに対し	Gracef	ıl Shutdowr	命令	を発行	ř													
FUJITSU PC Server PRIMERGY RX2540 M1	Windows Server 2012 R2 Standard					2)2721	@0S	シャットタ・ウン																
FUJITSU PC Server PRIMERGY RX2540 M1	Red Hat Enterprise Linux 7.0 (for Intel64)		復電待	機時間		2)2721	@0S	ノャットタ゛ウン																
			12	0秒																				
FUJITSU Storage ETERNUS NR1000 F2552	Clusterd DATA ONTAP 8.3.2					3NR10003	シャットタ゛	レ レ																

※NR1000へのシャットダウン命令発行まで設定時間分(10秒)待機

13.3 PowerChute Network Shutdown のイベントログ

2分の復電待機時間経過後、NR1000に対し、シャットダウンコマンドが発行されました。

NR1000 に対するシャットダウンコマンドを発行してから1分経過した時点で OS に対しシャットダウンコマンドが発行されました。 Windows、Linux から同時にシャットダウンコマンドが発行されても、NR1000 は最初に受け付けたシャットダウンコマンドのみ受け付けます。 ※バッテリ運転から2分経過後、"<u>Linux(もしくは Windows)はまもなくシャットダウンする。</u>" 旨イベントログに記録されます。

(以下、表7、表8参照願います。)

※イベントログに記載されている IP アドレス: 10.20.111.100 は今回検証に用いた UPS に搭載されている APC Network Management Card 2 の IP アドレスになります。

表 7. PCNS イベントログ (本ログは Linux の場合)

経過時間	イベント
0分	UPSがバッテリ電力に切り換わりました。
2分	UPS重大イベント: オンバッテリ。
	シャットダウンプロセスが開始されました。Linuxはまもなくシャットダウンします。
	PowerChuteはUPS 10.20.111.100の電源をオフにしています
	シャットダウンコマンドファイルの実行。
っくいい	UPSコンセントグループ(UPS Outlets)の電源オフが開始されました。
ረጋጋ ኃላታ	UPS重大イベント: コンセントグループの電源オフ開始。
3分	シャットダウンコマンドファイルは完了しました。
	PowerChuteが実行中の物理マシンをシャットダウンしています。

表 8. PCNS イベントログ (本ログは Windows の場合)

経過時間	イベント
0分	UPSがバッテリ電力に切り換わりました。
	UPS重大イベント:オンバッテリ。
2分	シャットダウンプロセスが開始されました。Windowsはまもなくシャットダウンします。
	PowerChuteはUPS 10.20.111.100の 電源をオフにしています
	シャットダウンコマンドファイルの実行。
2分5秒	UPSコンセントグループ(UPS Outlets)の電源オフが開始されました。
	UPS重大イベント:コンセントグループの電源オフ開始
24	シャットダウンコマンドファイルは完了しました。
37)	PowerChuteが実行中の物理マシンをシャットダウンしています。

13.4 UPS のイベントログ

停電発生から約2分経過後、PCNSから UPS に対しシャットダウンプロセス移行命令が発行されました。

停電発生から約5分経過後、アウトレットグループ1の出力が停止しました。

停電発生から約8分経過後、メインアウトレットグループおよびUPS本体の出力が停止しました。

※アウトレットグループ、メインアウトレットグループの Power Off Delay の値は PCNS のコマンドファイル実行時間の設定値によっては変動する場合があります。

※イベントログ上に記載されている IP アドレス: 10.20.111.12 は検証に使用したサーバの IP アドレスです。

表 9. UPS イベントログ

経過時間	イベントログ
0分	UPS: On battery power in response to rapid change of input.
	入力電源の急速な変化に伴い、UPSはバッテリ運転に切り替わりました
2分6秒	UPS: A graceful shutdown process is being used to shut down the load equipment before the UPS turns off. Initiated by PowerChute ns from 10.20.111.12.
	10.20.111.12のPowerChuteの命令により、UPSはシャットダウンプロセスに移行しました。
	UPS: Started a reboot process.
	リブートプロセスが開始されました。
2分7秒	UPS: Switched outlet group 1, Outlet Group 1, has been commanded to shutdown, sequenced.
	アウトレットグループ1にシャットダウンコマンドが送信されました。
	UPS: Main outlet group, UPS Outlets, has been commanded to shutdown, sequenced.
	メインアウトレットグループ、UPSにシャットダウンコマンドが送信されました。
5分8秒	UPS: The power for switched outlet group 1, Outlet Group 1, is now turned off.
	アウトレットグループ1の出力が停止しました。
8分8秒	UPS: The output power is turned off.
	UPS出力が停止しました。
	UPS: The graceful shutdown period has ended.
	シャットダウンプロセスは終了しました。
	UPS: No longer on battery power.
	バッテリ運転は終了しました。
	UPS: The power for the main outlet group, UPS Outlets, is now turned off.
	メインアウトレットグループ、UPS出力停止が停止しました。
	UPS: The graceful shutdown period has ended.
	シャットダウンプロセスが終了しました。

# 14. お問い合わせ先

本検証報告書にて記載されている製品の使用方法及び、製品仕様に関するご不明点については、 以下記載の連絡先にお問い合わせ下さい。

※弊社製品以外のお問い合わせについては回答出来ない場合がございます。

シュナイダーエレクトリック株式会社

白坂 健一郎

E-mail: <u>kenichiro.shirasaka@schneider-electric.com</u>, <u>jinfo@schneider-electric.com</u> Webサイト:\_http://www.apc.com/