SSH対応UPS管理製品の開発

加藤 裕 *Yutaka Katoh*
近藤 真二 *Shinji Kondoh*
林 浩一 *Kouichi Hayashi*
荻原 博紀 *Hironori Ogihara*

1. まえがき

当社では，複雑化するネットワーク環境，ならびに多様化する市場のニーズに合わせLANインタフェースカード*1，SANUPS T*2など，さまざまなUPS管理製品を開発してきた。

LANインタフェースカードおよびSANUPS Tは，Telnetプロトコルを利用してコンピュータのシャットダウン，ならびに，それぞれの装置の各種設定やUPSの状態監視などができる。しかしながら，Telnetプロトコルは，ネットワーク上を流れる情報はすべて暗号化されていない平文であるため，悪意ある第三者によって以下のようなことがおこなわれる可能性がある。

・データ盗聴によるアカウント・パスワード漏洩
・なりすましによる情報漏洩

近年，これらの攻撃に対する防衛の必要性について重要視されるようになり，UNIX，Linuxコンピュータでは，Telnetプロトコルからセキュリティを十分考慮したSSH*3プロトコルに移行していく傾向にある。

このような動向を見据え，当社ではUPS管理製品にSSHプロトコルを導入し，SSHプロトコルを利用したコンピュータのシャットダウン，ならびにそれぞれの装置の各種設定やUPSの状態監視などができる製品の開発をおこなった。

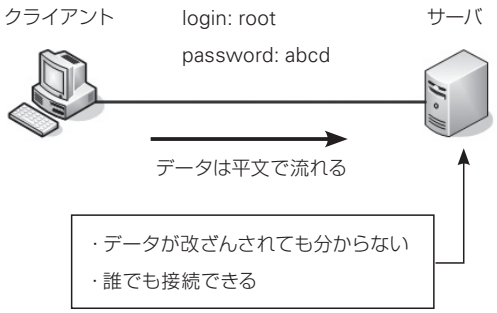
本稿では，SSHに対応したLANインタフェースカードとSANUPS Tの特長について紹介する。

*1: 加藤 裕ほか：LANインタフェースカード「SANUPS」PRASD04の開発 SANYODENKI Technical Report No.18参照。
*2: 加藤 裕ほか：電源管理ユニット「SANUPS T」の開発 SANYODENKI Technical Report No.20参照。
*3:Secure Shell（セキュアシェル）の略。

2. SSHとは何か

SSHとは，ネットワークを介して別のコンピュータにログインしたり，遠隔地のマシンでコマンドを実行するためのプログラム，または，プロトコルである。Telnetも同じ用途で使用するが，Telnetとの大きな違いは，ネットワーク上を流れるデータが暗号化されている，ということである(図1)。

＜Telnetの場合＞



＜SSHの場合＞

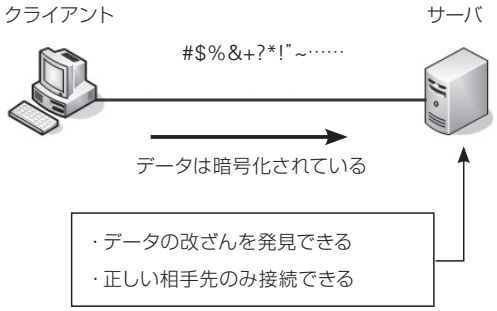


図1　TelnetとSSHの相違点

Telnetでは，ログインアカウントやパスワードがそのままネットワーク上を流れるため，第三者に傍受され，悪用される可能性がある。それに対しSSHでは，ログインアカウントやパスワード，ならびにネットワーク上を流れるすべてのデータを暗号化するため，情報の漏洩が防げる。

また，SSHでクライアントがサーバにログインするためには，サーバークライアント間で次の2種類の認証を行うため，より高度なセキュリティを保つことができる。

・ホスト認証：そのサーバが本当にユーザがログインしたいサーバであるかの確認。
・ユーザ認証：そのユーザがサーバにログインする資格があるかどうかの確認。

ホスト認証，あるいはユーザ認証(公開鍵認証の場合) では，“鍵”という数十ビットから2,000ビットほどのデータを利用する。鍵は，鍵生成プログラムによって，秘密鍵と公開鍵のペアで生成され，公開鍵で暗号化されたデータは，それに対応する秘密鍵によってのみ正しく復号化できる(図2)。

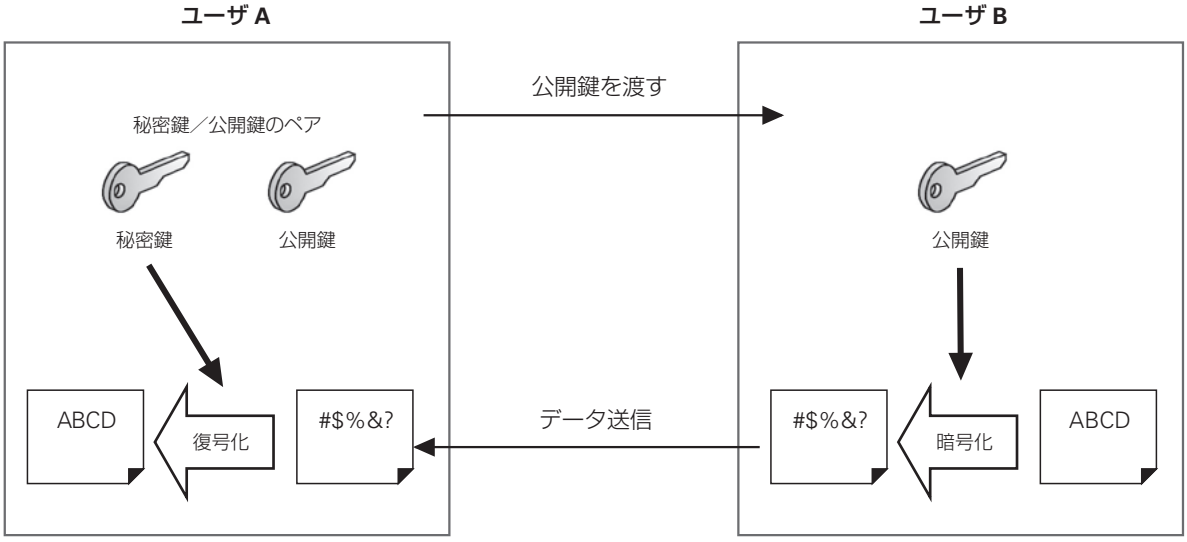


図2　公開鍵暗号化方式

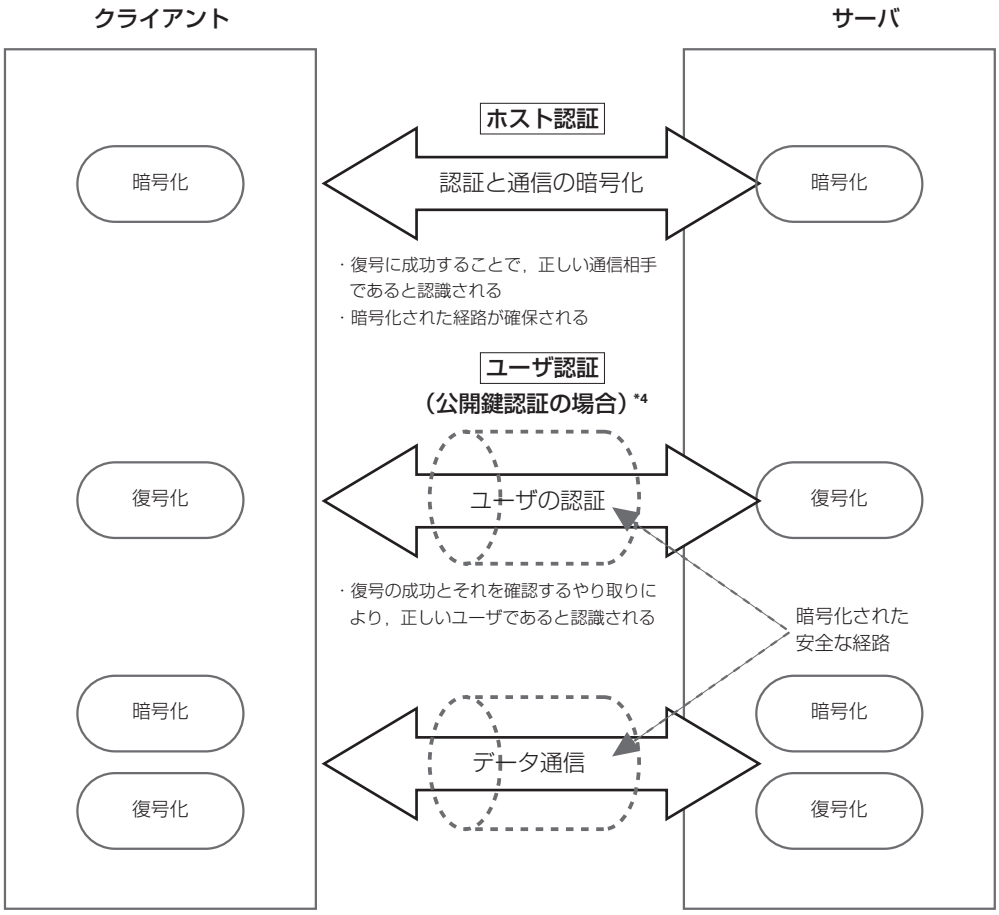


図3　SSH認証と暗号化通信の仕組み

*4: パスワード認証の場合は，暗号化された経路で，アカウントとパスワードの送受信を行う。

サーバマシンとクライアントマシンにおいて，一方のマシンに秘密鍵，もう一方のマシンにペアの公開鍵を登録しておくことで，鍵のペアを持っているクライアントのみがサーバにログインすることができる。

SSHの通信手順は以下のとおりである。また，SSHの一連の流れを図3に示す。

手順1．ホスト認証
　クライアント側において正しいサーバであることを確認する。また，暗号化された経路を確保する。
手順2．ユーザ認証
　サーバ側においてログインする資格があるユーザかどうかの確認をおこない，ログインが許可されたクライアントはサーバにログインすることができる。
手順3．データ通信
　暗号化された経路でデータの送受信をおこなう。

なお，本開発において対応したSSHの仕様を表1に示す。

3. システム構成

本開発でSSH対応をおこなったUPS管理製品は以下のとおりである。

・LANインタフェースカード（100Base-Tx）
・SANUPS T

それぞれのシステム構成例を図4，5に示す。

4. 特長

4.1 SSHプロトコルによるコンピュータのシャットダウン（SSHクライアント機能）

LANインタフェースカードおよびSANUPS Tからコンピュータのシャットダウンをおこなう際に，従来のTelnetプロトコルに加え，SSHプロトコルでコンピュータのシャットダウンができる。（図4，5の①）

SSHプロトコルでシャットダウンをする場合は，基本的にはTelnetプロトコルでシャットダウンをする場合と同じように，シャットダウンコマンドをスクリプトに記述することにより，シャットダウンができる。Telnetプロトコルでシャットダウンをする場合との違いは，SSH認証設定をする必要があるということである。なお，SSH認証設定においては，セキュリティのレベルや処理時間を考慮した上で，以下の方式を選択できる。

・ホスト認証の有無
・ユーザ認証方式（パスワード認証／公開鍵認証）の選択

Web画面におけるSSH認証設定の例を図6に示す。

なお，LANインタフェースカードの場合，SSHプロトコルでシャットダウンできる装置台数は，8台までである。

4.2 SSHプロトコルによる装置設定（SSHサーバ機能）

従来のターミナル機能では，シリアルあるいはTelnetプロトコルにより，装置の各種設定，UPSの状態監視などができたが，新たにSSHプロトコルでも同機能が使用できる（図4，5の②）。

これにより，セキュリティ上，SSHプロトコルしか許可されていない環境であっても，安全にLANインタフェースカードやSANUPS Tの各種設定やUPSの状態監視などができる。

表1　本開発におけるSSHの仕様

項目		仕様	備考
SSHバージョン		バージョン2	
ユーザ認証		パスワード認証	ユーザがあらかじめ登録したパスワードを使った認証
		公開鍵認証	ユーザがあらかじめ登録した秘密鍵・公開鍵ペアを使った認証
鍵の条件			
	鍵の形式	OpenSSH形式	
	公開鍵暗号方式	DSA	Digital Signature Algorithm。NIST（National Institute of Standards and Technology：米国国立標準技術研究所）によって公布された暗号方式
		RSA	Ronald Rivest，Adi Shamir，Leonard Adlemanの3名により開発された暗号方式
	パスフレーズ	なし	
	鍵コメント	なし	
	ビット数	1024	

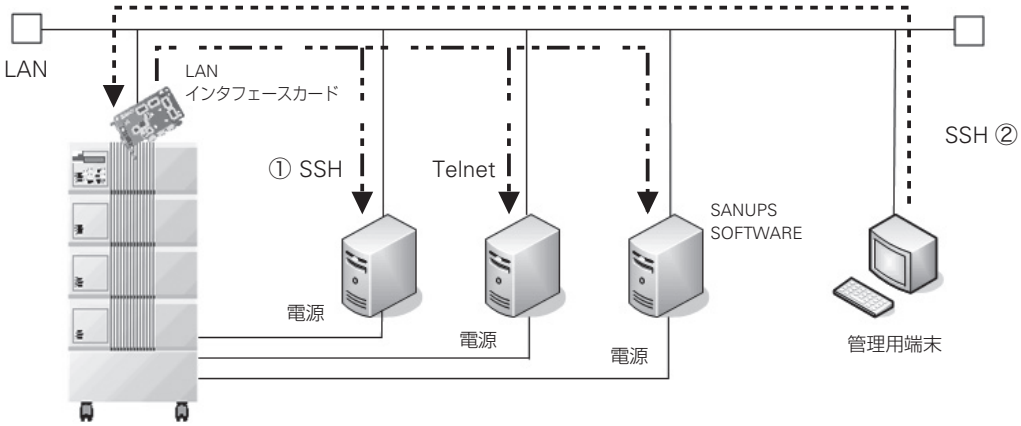


図4　LANインタフェースカードのシステム構成例

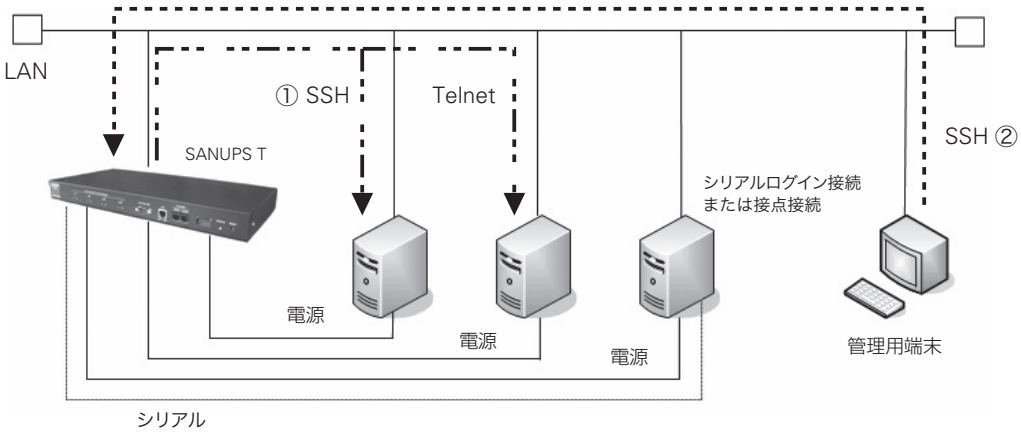


図5　SANUPS Tのシステム構成例

<パスワード認証の場合>

<公開鍵認証の場合>

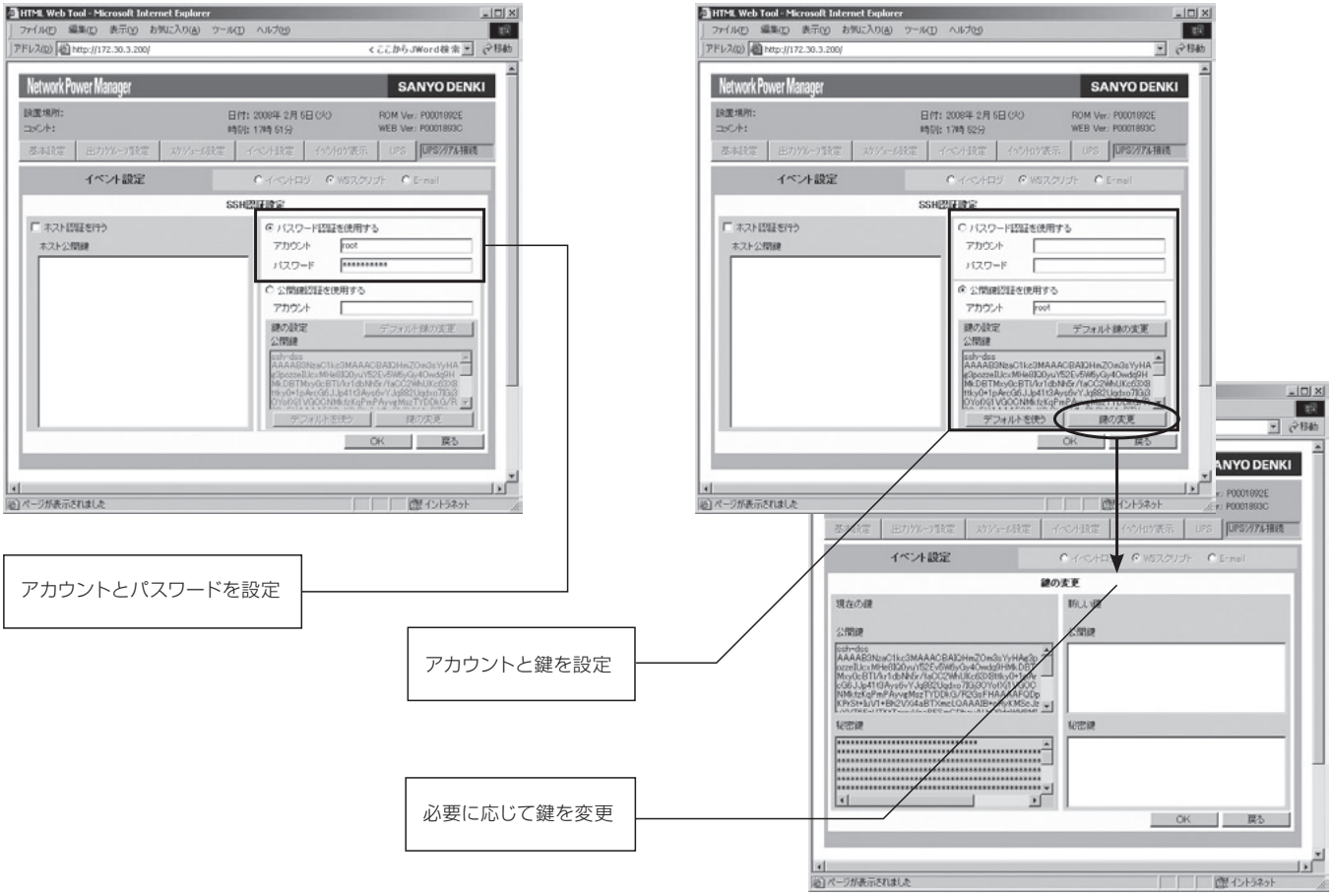


図6　SANUPS TにおけるWebでのSSH設定例

表2　一般ユーザアカウントの機能一覧

装置 / 項目	LANインタフェースカード	SANUPS T
接続装置／出力の状態表示	○	○
装置登録／変更／削除	×	×
ネットワーク情報設定	△	△
制御時間などの設定	△	△
サービス設定	×	×
アカウント設定	×	×
メール設定	×	×
スケジュール設定	△	△
時計設定	×	×
イベント設定	×	×
状態・計測値表示	○	○
イベントログ表示	○	○
制御	×	×
UPS情報表示	○	○
出力グループ設定		○

凡例　○：許可，△：表示のみ許可，×：禁止

4.3 その他の機能追加

4.3.1 一般ユーザアカウント対応

従来のUPS管理製品は，管理者用のアカウントしか用意しておらず，このアカウントでUPS管理製品にログインすることにより，それぞれの装置の各種設定や状態表示，制御などのすべての操作をおこなってきた(図4，5の②)。そのため，管理者以外の保守者などが，UPSの状態のみ監視したい場合は，保守者に管理者アカウントを知らせる必要があった。そのような場合には，ワークステーションへのログイン情報(アカウント，パスワード)なども保守者が見ることができてしまい，セキュリティ上問題があった。そのための対策として，一般ユーザアカウントを用意し，UPSの状態の監視など，機能を絞った形での管理ができるようにした。

一般ユーザアカウントでログインした場合の機能一覧を表2に示す。

4.3.2 メール受信機能の強化

メール受信機能においては，従来のUPSの状態や計測値に加えて，UPS形式，バッテリテスト結果，バッテリ寿命などの情報が取得可能である。

5．むすび

本開発は，セキュリティにポイントを絞った開発となった。他社に先駆けてSSHプロトコルのバージョン2を採用したことで，当社のセキュリティに対する姿勢を社会に発信することができたものと考える。

今回の開発をきっかけに，セキュリティに対する意識をより高め，より信頼される企業を目指して開発に従事していく所存である。

文献

(1) Daniel J. Barrettほか：実用SSH

(2) 新山祐介：入門OpenSSH

加藤 裕
1991年入社
パワーシステム事業部　設計第二部
電源機器，電源管理システムの開発，設計に従事。

近藤 真二
1985年入社
パワーシステム事業部　設計第二部
電源機器，電源管理システムの開発，設計に従事。

林 浩一
1997年入社
パワーシステム事業部　設計第二部
電源機器，電源管理システムの開発，設計に従事。

荻原 博紀
2005年入社
パワーシステム事業部　設計第二部
電源機器，電源管理システムの開発，設計に従事。