新製品紹介

小容量 UPS「GX シリーズ」用ネットワークカード「Web/SNMP カードⅡ」

"Web/SNMP Card II" Network Cards for "GX Series" Small Capacity UPSs

森藤 裕治郎 * MORITO, Yujiro　初見 博 ‡ HATSUMI, Hiroshi　畠中 伸治 ⁂ HATAKENAKA, Shinji

近年，突発的な落雷や豪雨による電源異常（停電や瞬低）が増加してきている[(1), (2)]。こうした電源異常に備えるために，無停電電源装置（UPS：Uninterruptible Power System）の導入が必要不可欠である。UPS は，停電が発生すると UPS に接続されているバッテリを供給源に切り替えて，負荷機器に安定した電力を供給する。

UPS は産業分野では半導体製造装置やデジタルプリンタなどの電源保護として利用され，IT 分野ではデータセンターなどのサーバ機器やネットワーク機器などの電算機器を電源保護として利用される。特に IT 分野では，電源が遮断される前にデータを退避したり，基本ソフト（OS：Operating System）を適切な処理で安全に停止する OS シャットダウン処理を行ったりすることが必要である。UPS に UPS 管理システムを連携させることで，バッテリの電力が残っている間に OS シャットダウン処理を自動で実行させることができ，無人化されたサーバルームなどの IT 機器を電源異常から守ることができる（**図 1**）。

UPS 管理システムには，サーバや PC などのコンピュータにインストールして動作させるアプリケーションソフトウェアと，UPS に直接実装してネットワーク経由で管理が可能なネットワークカードによるものがある。前者では UPS 管理用として専用のコンピュータが必要になるのに対し，後者では UPS に組み込むので専用コンピュータは不要となる。データセンターなどの IT 分野では限られたスペースに多くのサーバを配置するため，後者の省スペースタイプのニーズが高い。また，昨今の IT 分野では，ネットワークの暗号化や仮想化技術を取り込んだ技術への対応が重要視されるようになってきている。

本稿では，これらの機能に対応した小容量 UPS「GX シリーズ」用ネットワークカード「Web/SNMP カードⅡ」について述べる。

1 特　徴

今回開発した Web/SNMP カード II を**図 2** に，Web/SNMP カード II と既存品（Web/SNMP カード）の機能比較を**表 1** に示す。

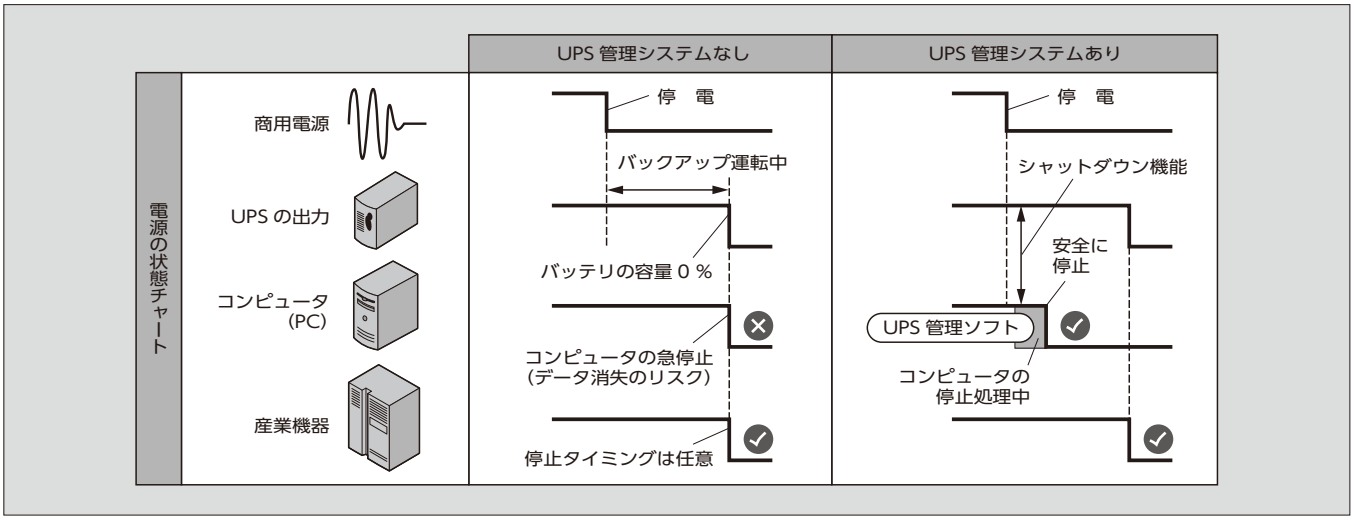

図 1　UPS 管理システムの役割

＊ 富士電機株式会社パワエレシステムエネルギー事業本部開発統括部電源機器開発部
‡ 富士電機株式会社営業本部ファクトリーオートメーション統括部営業第四部
⁂ 富士電機株式会社パワエレシステムインダストリー事業本部オートメーション事業部業務第一部

図 2　「Web/SNMP カードⅡ」

表 1　新旧機能比較表

項　目		開発品	既存品
呼　称		Web/SNMPカードⅡ	Web/SNMPカード
ハードウェア仕様		Cortex-A9/M4 マルチコアCPU	V850 シングルCPU
Ethernet*通信		10M/100M/1,000M （ギガビット対応）	10M/100M
IPアドレス		IPv4，IPv6，IP自動設定	IPv4
Web接続		HTTP，HTTPS	HTTP
セキュリティ接続		SSH2.0（制約なし）	SSH（制約あり）
SNMP		v1，v2c，v3 （暗号化対応）	v1，v2c
メール通知	認　証	PLAIN，LOGIN，MD5	なし
	暗号化	SMTPS	なし
ロ　グ	イベント	1,000件	800件
	計　測	30日間	2日間
瞬停通知		メール&ログ	なし
マルチ言語		リアルタイム切替（日英）	言語ファイルで切換

＊Ethernet：富士ゼロックス株式会社の商標または登録商標

1.1　セキュリティ

従来，データセンターなどで管理用に使用される閉域ネットワークは，インターネットのような広域ネットワークほどのセキュリティは必要なかった。しかし，近年では，ワイヤレス通信や USB（Universal Serial Bus）通信などの一時的な利用を目的とした接続や，仮想ネットワーク（VPN：Virtual Private Network）などの物理的に接続された状態でソフトウェアによって回線を分離する仕組みが普及してきている。そのため，従来のように独立して構成することは困難になってきているため，閉域ネットワークにおいてもセキュリティを確保することが課題になっている。

暗号化による通信データの盗聴防止や改ざん防止，接続元のデジタル証明書などを使ったなりすまし防止などのセキュリティの実装には，暗号化処理で高速演算が必要である。

本開発品では，既存品ではできなかった高速演算を可能としたプロセッサ（ARM：Advanced RISC Machines）を搭載し，暗号化通信（TLS1.2：Transport Layer Security）で標準化されているハッシュアルゴリズム SHA−256（Secure Hash Algorithm）を実装しており，高度な暗号化によってセキュリティを実装することで，安全なネットワーク通信に対応している（**図 3**）。

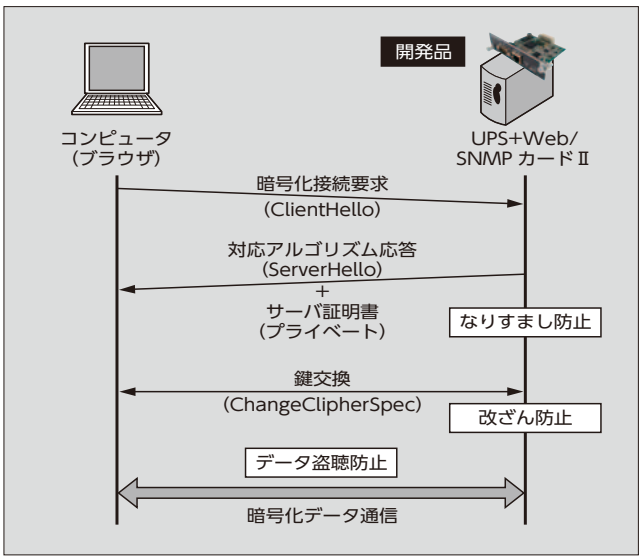

図 3　TLS 接続のしくみ

1.2　Internet Protocol Version6（IPv6）

2001 年 1 月施行の「高度情報通信ネットワーク社会形成基本法」による“e−Japan 重点計画”に明記されたことで，わが国においても IPv6 の利用は拡大している。OS やスマートフォンなどのネットワーク接続機器には IPv6 が実装されていてユーザが意識することなく使える環境が整備されてきた。

産業分野では，IPv6 はこれまでニーズとしては少なかったため実装は遅れていた。しかし，IT 分野のネットワークインフラにおいて IPv6 は一般的となっているため，従来の IPv4 と IPv6 が混在した環境が産業分野で増加している。

本開発品では，IPv4 と IPv6 が混在した環境にも対応できるように，IPv4 と IPv6 の両方を搭載したデュアル

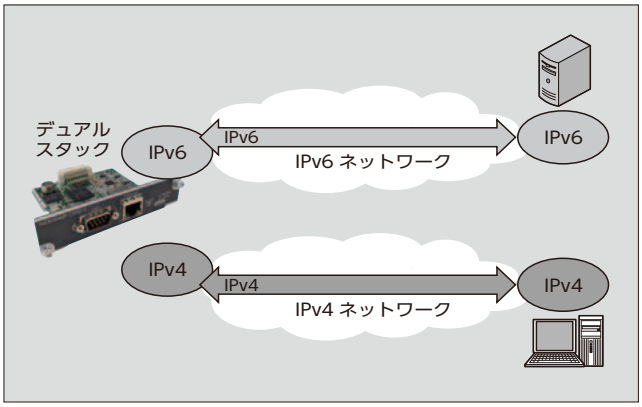

図 4　IPv4 と IPv6 のデュアルスタックの構成

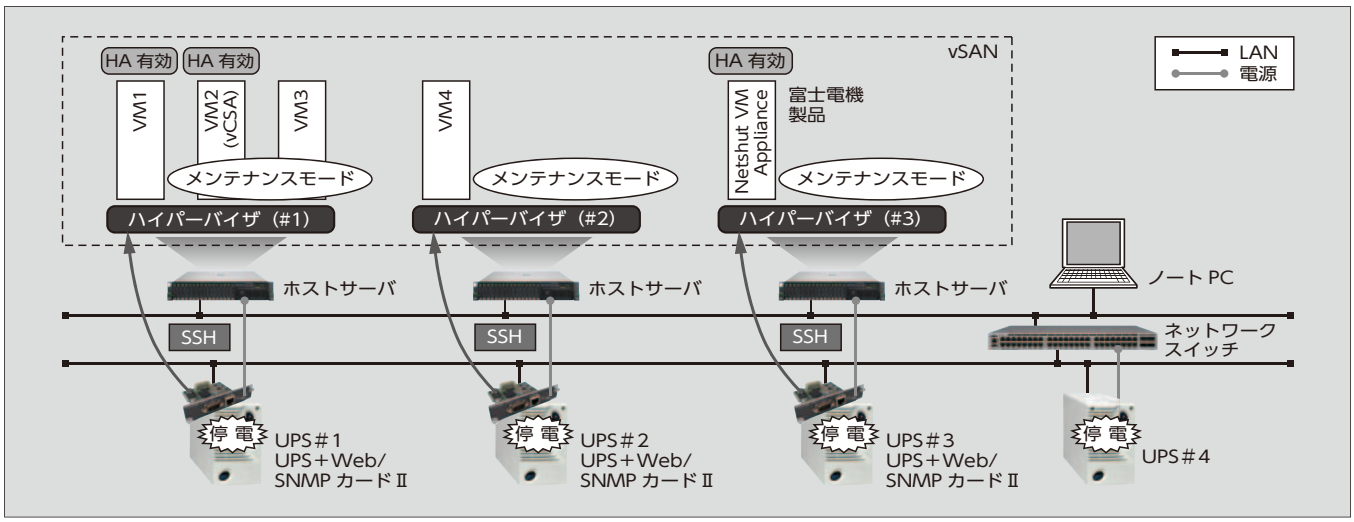

図 5　SSH 通信を使った仮想化システムとの連携

スタック（**図 4**）を備えている。IPv6 ではアドレス長が 128 bit に拡張されているため，手動でアドレスを設定することが困難である。そこで，ホスト名で置き換えるシステム（DNS：Domain Name System）や自動でアドレスを設定するシステム（DHCPv6：Dynamic Host Configuration Protocol version 6）も備えている。

1.3　仮想化システムへの対応

コンピュータの高度化が進むにつれて，1 台の高性能なサーバ上で，複数の仮想的なサーバを運用する仮想化システムが普及している。仮想化システムは，仮想サーバを管理する物理サーバ（ハイパーバイザ）とストレージで分散構成され，故障などの異常が発生してもクラスタ構成のような冗長化により高可用性（HA：High Availability）を持っている。こうしたシステムに UPS を導入した場合，電源異常時の動作やシステム停止のタイミングを判断することが難しい。

本開発品が実装しているハイパーバイザと直接通信が行える機能（SSH2.0：Secure Shell）によって，最大 8 台までのハイパーバイザをシャットダウンさせることができる。これにより，これまで難しかった大規模な仮想化システム（HCI：Hyper−Converged Infrastructure）にも対応できる（**図 5**）。

参考文献

⑴　国土交通省.“最近の自然災害と防災・減災の取り組みについて”. 2018. http://www.zenkokubousai.or.jp/download/reiwa_nittei01.pdf,（参照 2019−06−13）.
⑵　電気事業連合会. IEEJ. 2018−10−15. https://eneken.ieej.or.jp/data/8119.pdf,（参照 2019−06−13）.

発売時期

2019 年 9 月

お問い合わせ先

富士電機株式会社
パワエレシステムインダストリー事業本部オートメーション事業部業務第一部
電話（03）5435−7091

（2019 年 9 月 26 日 Web 公開）

富士電機

Innovating Energy Technology