SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

PMBus のセキュリティに関する一考察
A study of Security Issue about PMBus

岡田 悠聖 * 塩原 孝弘 † 加藤 雅彦 *
Chikase Okada Takahiro Shiohara Masahiko Kato

キーワード PMBus, IoT 電源, IoT セキュリティ

あらまし

近年，再生可能エネルギーの需要が高まっている．太陽光発電を使ったスマートグリッドなど，自然エネルギーを電力に変える方式は，従来型の発電所から末端へ一方向に送電するという仕組みと異なり，需給に応じて双方向に電力が流れる．そのため，精密な電力制御を行う必要があり，電力変動の調整機能として蓄電池システムが期待される．そこで，バッテリー管理機能を持つ IoT 電源が着目されている．IoT 電源とは，バッテリーの充放電を細かく制御したり，遠隔からバッテリー残量を確認したりすることができる IoT 機器である．一方，IoT 機器は遠隔操作を行うためにネットワーク接続されており，攻撃の対象となっている．IoT 電源が攻撃されると，電源がダウンし機器が動作しなくなるなど重大な事故につながる恐れがある．

そこで本研究では，攻撃が行われた際の IoT 電源に特有なリスクを明らかにし，対策を検討する．

検証環境として，制御用に PMBus (Power Management Bus)を用いた電源装置と，操作や表示，ネットワーク通信を行う管理用の小型コンピュータが一体となった装置を IoT 電源として用いる．

PMBus とは，電源制御用の 2 線式シリアルバスである．各電源を操作する機器をマスターデバイス，ネットワーク経由で操作される電源をスレーブデバイスと呼び，1 つのマスターデバイスにつき，複数のスレーブデバイスを同時に制御することが可能である．スレーブデバイスごとに 7 ビットのアドレスが振られ，そのアドレスを指定してコマンドを送信することで制御を行う．電源回路はデジタル電源制御プロトコルである PMBus を使ってデジタル制御でリアルタイムに出力電圧などを制御でき，バスライン上に複数の電源接続が可能である．

攻撃シナリオとして，Mirai などの IoT 機器に対する攻撃を参考に，攻撃対象となるスレーブデバイスのアドレス特定から PMBus に対する DoS 攻撃までを想定し，検証を行う．検証環境は，管理用コンピュータへの初期侵入が完了した状態とし，本来動作しているプログラムの改ざんは行わないものとする．管理用コンピュータには Raspberry Pi，PMBus コントローラとして市販の工業用 AC/DC 電源を使用し，Raspberry Pi とコントローラの間を PMBus で接続する．Raspberry Pi は，PMBus から電圧情報を読み取り，Web 上で表示を行う簡易的なプログラムを作成し，実行する（図 1）．

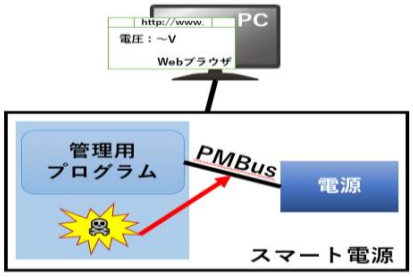

図 1 検証環境

調査ではまず，スレーブデバイスのアドレスを入手するために PMBus 通信の盗聴を試みる．次に，入手したデバイスのアドレスを使用して大量の読み込みを発生させ，PMBus に対する DoS 攻撃を行う．

その結果，本来動作しているプログラムに手を加えることなくスレーブデバイスのアドレスを取得し，電源の電圧表示に異常が発生した．

侵入後の対策として，PMBus コントローラの冗長化や PMBus 上で通信相手を認証する拡張機能の導入，PMBus コントローラの異常動作を検知する仕組みの導入，攻撃に利用されるコマンドの削除などが考えられる．

さらに，攻撃が成功した場合を想定し，攻撃されることを前提とした機器設計を行うことなどについても，今後検討を行う．

* 長崎県立大学，〒851-2130 長崎県西彼杵郡長与町まなび野 1-1-1,
University Of Nagasaki, 1-1-1 Manabino, Nagayo, Nishisonogi, Nagasaki, 851-2130, Japan .
† TDK 株式会社，〒272-8558 千葉県市川市東大和田 2-15-7,
TDK Corporation, 2-15-7 Higashi-Ohwada, Ichikawa-shi, Chiba, 272-8558, Japan .