NIST 内部文書

NIST IR 8498

スマートインバータのサイバーセキュリティ

住宅用および軽商業用太陽エネルギー・システムのガイドライン

最終

ジェームズ・マッカーシー

ジェフリー・マロン

ドン・ダニエル・レボリ＝

ジョナサン・ニク・ウルラウブ

本書は https://doi.org/10.6028/NIST.IR.8498 より無料で入手可能。

NIST 内部文書

NIST IR 8498

スマートインバータのサイバーセキュリティ

住宅用および軽商業用太陽エネルギー・システムのガイドライン

最終

ジェームズ・マッカーシー*

ジェフリー・マロン ダニエル・レボリ・カレテロ 応用サイバーセキュリティ部門 ジョナサン・ウィルトバーガー

インフォメーション・テクノロジー・ラボラトリー Nik Urlaub(#マサチューセッツ工科大学

*本書の執筆はすべて *NIST* 在職中に行われた。

#元 *MITRE* 職員。本書のすべての作業は *MITRE* 在籍中に行われた。

本書は より無料で入手可能。

2024 年 12 月

米国商務省 ジーナ・*M*・ライモンド長官

国立標準技術研究所理事兼標準技術担当商務次官 ローリー・*E*・ロカシオ

本論文では、実験手順を適切に特定するために、商用、非商用を問わず、特定の機器、装置、ソフトウェア、または材料を識別している。このような識別は、NIST によるいかなる製品またはサービスの推奨または保証を意味するものではなく、また識別された材料または装置が必ずしもその目的に対して利用可能な最良のものであることを意味するものでもありません。

本書には、NIST がその法定責任に従って現在開発中の他の出版物を参照する場合がある。概念や方法論を含め、本書に記載されている情報は、そのような関連出版物が完成する前であっても、連邦機関によって使用される可能性がある。従って、各出版物が完成するまでは、現行の要求事項、ガイドライン、手順が存在する場合は、それらが引き続き有効である。計画および移行の目的で、連邦機関は NIST によるこれらの新出版物の開発を注意深く見守ることが望ましい

各組織は、パブリックコメント期間中にすべての出版物のドラフトを検討し、NIST にフィードバックを提供することが推奨される。上記以外の多くの NIST サイバーセキュリティ出版物は、https://csrc.nist.gov/publications。

NIST テクニカルシリーズ方針

著作権、使用およびライセンスに関する

NIST 技術シリーズ出版識別子の構文

出版履歴

2024-12-10、NIST 編集審査委員会承認

この NIST テクニカルシリーズ出版物の引用方法

McCarthy J, Marron J, Faatz D, Rebori-Carretero D, Wiltberger J, Urlaub N (2024) Cybersecurity for Smart Inverters :

家庭および中小企業の太陽エネルギーシステムのためのガイドライン。(国立標準技術研究所,

Gaithersburg, MD）。NIST Interagency Report (IR) NIST IR 849828/NIST.IR.8498。

認可 ORCID iDs

ジェームズ・マッカーシー0000-0002-5559-733X

ジェフリー・マロン：0000-0002-7871-683X

連絡先

energy_nccoe@nist.gov

国立標準技術研究所
担当：国立サイバーセキュリティ・センター・オブ・エクセレンス、情報技術研究所
100 ビューロー・ドライブ（メール・ストップ 2002） メリーランド州ゲイサーズバーグ 20899-2002

追加情報

関連コンテンツ、更新の可能性、文書の履歴など、本書に関する追加情報は https://csrc.nist.gov/p
すべてのコメントは情報公開法（FOIA）に基づき公開される。

概要

本報告書は、一般家庭や小規模企業で使用される小規模太陽光インバータ実装のための実践的なサイバーセキュリティガイダンスを提供する。これらのガイドラインは、国家脆弱性データベース（NVD）に記録された既知のスマートインバータの脆弱性のレビュー、既知のスマートインバータサイバー攻撃に関する情報のレビュー、および 5 つのスマートインバータの例のテストによって得られたものである。また、この報告書は、7 つのガイドラインを実施するために製品に必要なサイバーセキュリティ機能について、スマートインバータの製造事業者に勧告を提示している。これらの勧告は、NIST IR 8259A および IR 8259B で定義されたモノのインターネット（IoT）サイバーセキュリティ能力のベースラインに基づいており、ベースライン・サイバーセキュリティ能力のいくつかについてスマートインバータ固有の情報を提供している。

キーワード

IoT サイバーセキュリティ機能、軽商用インバータ、住宅用インバータ、小規模太陽光発電システム、スマートインバータ・サイバーセキュリティ。

コンピュータ・システム技術報告書

国立標準技術研究所(NIST)の情報技術研究所(ITL)は、国家の測定および標準機構に技術的リーダーシップを提供することにより、米国の経済と公共の福祉を促進している。ITL は、情報技術の開発と生産的使用を促進するために、試験、試験方法、参照データ、概念実証実装、技術分析を開発している。ITL の責任には、連邦情報システムにおける国家安全保障関連情報以外のコスト効率の良いセキュリティとプライバシーのための管理、管理、技術、物理的標準とガイドラインの開発が含まれる。

特許開示通知

注意：ITL は、本出版物のガイダンスまたは要件に準拠するために使用が必要とされる特許請求の範囲の保有者に対し、当該特許請求の範囲を ITL に開示するよう要請している。ただし、特許権者は ITL の特許募集に応じる義務はなく、ITL は、本出版物に該当する特許があるとしても、それを特定するための特許調査は行っていません。

本書の発行日および、本書のガイダンスまたは要件に準拠するために使用が必要とされる可能性のある特許請求の範囲の識別を求めた後の時点で、そのような特許請求の範囲は ITL には識別されていません。

ITL は、本出版物の使用において特許侵害を回避するためのライセンスが不要であることを表明するものではなく、また示唆するものでもありません

目次

エグゼクティブサマリー 1
1. 序文 2
1.1. 想定読者 5
1.2. 報告組織 5
2. 所有者と設置者のためのサイバーセキュリティ・ガイドライン 7
2.1. ガイドラインその 1：デフォルトのパスワードと認証情報を変更する 8
2.2. ガイドライン 2：役割ベースのアクセス管理（RBAC）の使用 8
2.3. ガイドライン#3：ログにイベントを記録する設定 9
2.4. ガイドライン 4：ソフトウェアの定期的なアップデート 10
2.5. ガイドライン 5：システム情報のバックアップ 11
2.6. ガイドラインその 6：未使用の機能を無効にする 11
2.7. ガイドライン 7：通信の保護 12
3. スマートインバータ製造事業者に対するサイバーセキュリティの提言 14
3.1. 推奨されるベースライン・サイバーセキュリティ能力 14
4. 結論 21
参考文献 22
附属書 A. その他のリソース 24
附属書 B. 記号、略語、頭字語のリスト 25
附属書 C. 住宅用および軽商用太陽エネルギーシステム設置サイバーセキュリティチェックリスト 26
附属書 D. スマート・インバータの試験 27
D.1.ガイドライン#1: デフォルトパスワードと認証情報の変更に関するテスト結果 29
D.2.ガイドライン#2：役割ベースのアクセス管理の使用」のテスト結果 29
D.3.ガイドライン#3: ログにイベントを記録する設定」のテスト結果 30
D.4.ガイドライン#4: ソフトウェアの定期的なアップデート」のテスト結果 31
D.5.ガイドライン#5：システム情報のバックアップのテスト結果 32
D.6.ガイドライン#6: 未使用の機能を無効にする」のテスト結果 32
D.7.ガイドライン#7: 通信の保護」のテスト結果 33
附属書 E. 一般的なサイバーセキュリティガイダンスへのマッピング 35
E.1.ガイドラインに影響を与える一般的なサイバーセキュリティガイダンス 35
E.1.1.NIST サイバーセキュリティ枠組み 35
E.1.2. インターネットセキュリティセンター クリティカルセキュリティコントロール（CSC）バージョン 8 35
E.1.3.NIST SP 800-53r5 35

E.1.4.NIST SP 800-213A 36

E.1.5.MITRE ATT&CK フレームワーク 36

E.1.6.ISA/IEEC 62443-2-1 36

E.2.ガイドラインと一般的なサイバーセキュリティガイダンスとの関係 38

附属書 F. スマートインバータの脆弱性調査 41

表一覧

図 1.米国の発電量 2
図 2.住宅用または軽商用ソーラー・エネルギー・システムにおけるスマート・インバータの役割 4
図 3.ガイドライン#1 ライフサイクル・フェーズ 8
図 4.ガイドライン#2 ライフサイクル・フェーズ 9
図 5.ガイドライン#3 ライフサイクル・フェーズ 10
図 6.ガイドライン#4 ライフサイクル・フェーズ 10
図 7.ガイドライン#5 ライフサイクル・フェーズ 11
図 8.ガイドライン#6 ライフサイクル・フェーズ 12
図 9.ガイドライン#7 ライフサイクル・フェーズ 13
図 10.スマートインバータの機能要素 19
図 11.インバータの接続方法 28

図一覧

表 1.技術的サイバーセキュリティ能力に関する推奨事項 15
表 2.非技術的サイバーセキュリティ能力に関する推奨事項 19
表 3.試験したインバーターの特性 28
表 4.ガイドライン#1 のテスト結果 29
表 5.ガイドライン#2 のテスト結果 30
表 6.ガイドライン#3 のテスト結果 30
表 7.ガイドライン#4 のテスト結果 31
表 8.ガイドライン#5 のテスト結果 32
表 9 ガイドライン#6 試験結果 32
表 10.ガイドライン#7 のテスト結果 33
表 12.スマートインバータの脆弱性調査 41

謝辞

国立サイバーセキュリティ・センター・オブ・エクセレンス(NCCoE)は、このガイダンスを作成するにあたり、専門知識と設備を提供してくれたこのプロジェクトの協力者に感謝している。

Name	Organization	組織
Paul Abbazia	Bedrock Systems	ベッドロック システムズ
Adrian Beatty	Wunderlich-Malec Engineering	ワンダリッヒ-マレック エンジニアリング
Barbara B. Cuthill	NIST Applied Cybersecurity Division	NIST 応用サイバーセキュリティ部門
Eileen Division	The MIRTRE Corporation[1]	The MIRTRE Corporation
Joel Gil	Bedrock Systems	ベッドロック システムズ
Siv Hilde Houmb	Norwegian University of Science and Technology	ノルウェー科学技術大学
Ian Kittle	U.S. Department of Homeland Security	米国国土安全保障省
Trond Oines	Solar Technologies Scandinavia	Solar Technologies Scandinavia
Jeremy Panicker	Schneider Electric	シュナイダーエレクトリック
Sean Plankey	Bedrock Systems	ベッドロック システムズ
Aleksandr Rakitin	Schneider Electric	シュナイダーエレクトリック

[1]本書の執筆はすべて MITRE 在職中に行われた。

Chris Rezendes	Spherical Analytics	Spherical Analytics
Mark Rice	Pacific Northwest National Laboratory	パシフィック・ノースウエスト国立研究所
TJ Roe	Radiflow	Radiflow
Thomas P. Roth	NIST Smart Connected Systems Division	NIST スマートコネクテッドシステム部門
Arif Sarwat	Florida International University	フロリダ国際大学
Chris Rezendes	Spherical Analytics	Spherical Analytics
John Walsh	Bedrock Systems	ベッドロック システムズ
Don Wingate	Schneider Electric	シュナイダーエレクトリック
Tsion Yimer	Morgan State University	モーガン州立大学

エグゼクティブサマリー

本報告書は、配電網に接続され、電力会社が直接所有または運営していない小規模な住宅用および軽商用太陽光発電システムで使用されるスマートインバータのための実践的なサイバーセキュリティガイダンスを提供する。スマート・インバータは、家庭や小規模事業所と電力網との間のエネルギーの流れを管理する。送電網の状況を感知し、電力会社とコミュニケーションすることで、これらのデバイスは電力の可用性、安全性、送電網の安定性に貢献する。

スマートインバータは多くの場合、インターネットを使用してクラウドベースの管理機能と接続する。この接続性により、スマート・インバータはサイバー脅威にさらされ、安全で信頼性の高い運用を継続するための効果的なデバイス・サイバーセキュリティの必要性が高まる。

本報告書のセクション 2 では、住宅所有者、太陽エネルギーシステム設置者、太陽エネルギーシステム保守業者向けに、7 つのサイバーセキュリティガイドラインを提供している。これらのサイバーセキュリティ・ガイドラインは、住宅用または小規模事業用の太陽エネルギー・システムが安全かつ確実に設置、設定、運用されるようにするための行動を記述している。

本報告書のセクション 3 では、スマートインバータの製造事業者向けに 10 のサイバーセキュリティ能力を推奨する。これらのサイバーセキュリティ能力は、NIST Interagency Report（IR）8259A および 8259B に示された IoT サイバーセキュリティ能力コア・ベースラインから導き出されたものであり、セクション 2 ガイドラインの実施を可能にするものである。

附属書には、これらのガイドラインと推奨事項の作成と使用をサポートする情報が掲載されている。

附属書 A は、ガイドラインと勧告を作成する際に参照した出版物の書誌を提供する。

附属書 B は、略語と頭字語のリストである。

附属書 C は、システム設置者がセクション 2 のガイドラインで定義された措置を完了したことを検証する際に、独自に作成し使用することができるプロビジョニング・チェックリストのサンプルを提供する。

附属書 D は、設置された 5 台のスマートインバータをテストし、セクション 2 ガイドラインを実施する能力を判断した結果を記録している。

附属書 E は、セクション 2 のガイドラインを 6 つの一般的なサイバーセキュリティガイダンスソースにマッピングしている。

附属書 F は、国家脆弱性データベース（NVD）に記録された既知のスマートインバータのサイバーセキュリティ脆弱性に関する情報を示す。

1. 序文

本報告書は、配電網に接続され、電力会社が直接所有・運営せず、一般家庭や小規模企業で通常使用される小規模住宅用および軽商用インバータ向けの実践的なサイバーセキュリティ指針を提供するものである。このガイダンスは、現在のスマート・インバータの脅威の状況、現在利用可能なスマート・インバータのサイバーセキュリティ能力、およびシステム設置者、住宅所有者、小規模事業者が実施できる潜在的緩和策を調査することによって作成された。これらの機能と緩和策は、テストを通じて妥当性を確認し、その実用性を実証した。この報告書は、7 つのガイドラインを実施するために製品に必要なサイバーセキュリティ機能について、スマートインバータの製造事業者に提言を提供している。これらの勧告は、NIST Interagency Report (IR) 8259A [1]および IR 8259B [2]で定義されたモノのインターネット（IoT）サイバーセキュリティ能力のベースラインを基に、スマートインバータ固有の情報を提供するものである。

図 1 に示すように、米国エネルギー情報局[3]は、住宅用や軽商業用の太陽光発電システムのような小規模な太陽光発電を含め、太陽光発電の継続的な増加を予測している。

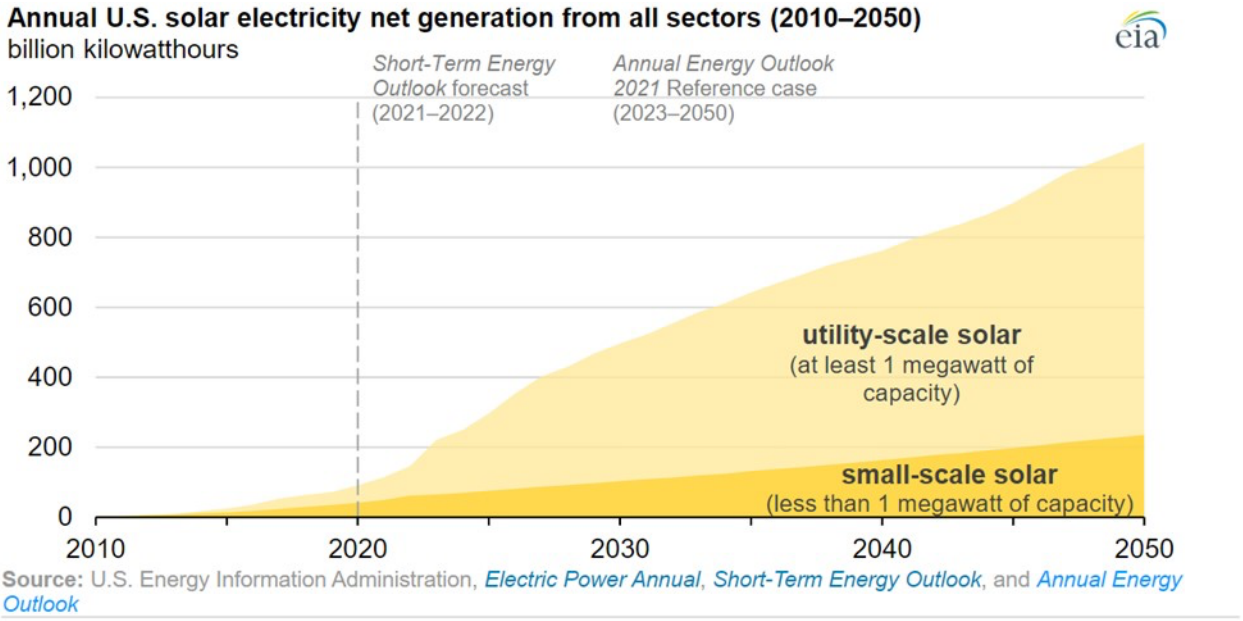

図 1.米国の発電量

送電網は、集中制御の少ない IoT やスマート・デバイス（スマート・インバーターなど）をより多く取り入れている。これらのデバイスは、クラウドベースの管理機能と接続するためにインターネットを使用することが多い。このようなインターネット接続はサイバー脅威へのエクスポージャーを高め、グリッドへの影響を防ぐための効果的なサイバーセキュリティの必要性を高めている。

配電網に接続された住宅用または軽商用のスマート・インバータ 1 台の妥協は、今日のグリッドに最小限の影響しか与えないだろう。しかし、太陽光エネルギー市場が成長するにつれて、電力会社は昼間の電力消費のピーク時に分散型再生可能エネルギー資源からの電力供給に依存するようになる可能性がある。このような変革

が起こると、複数の住宅用または軽商用のスマート・インバータを危険にさらすために開発された攻撃は、重大な影響を及ぼす可能性がある。インバータのセーフティ・クリティカルな機能は、電力フローを提供することが安全でない状態を常に検知できなければならない。

ベンダーが複数の製品ラインでソフトウェアを共有している場合、家庭用および軽商用のスマート・インバータで発見され悪用された弱点が、より大型の商用インバータを危険にさらすために活用される可能性がある。

電力網に影響を与えなくても、小規模な太陽光発電システムに対するサイバー攻撃は、住宅所有者や小規模事業主に次のような悪影響を及ぼす可能性がある：

- 経済的利益の損失：インバーターが系統から切り離されると、機器の設置によって期待された経済的利益が失われる。
- 家庭、事業所、または設置された機器への損害：インバータが攻撃されると、インバータが損傷したり、インバータの出力が安全な動作条件（高調波ひずみ、過電圧、周波数異常など）を超えてしまい、他の家庭や事業所の機器（AC、コンロ、電子機器など）が損傷する可能性がある
- 重要な必要時の機器の喪失：インバータが攻撃されると、必要なときにシステムが作動しなくなる可能性がある（停電など）。

小規模住宅や中小企業の太陽光発電システムで使用されるスマートインバータのサイバーセキュリティ防御は、サイバー攻撃が成功する可能性を減らすことができる。

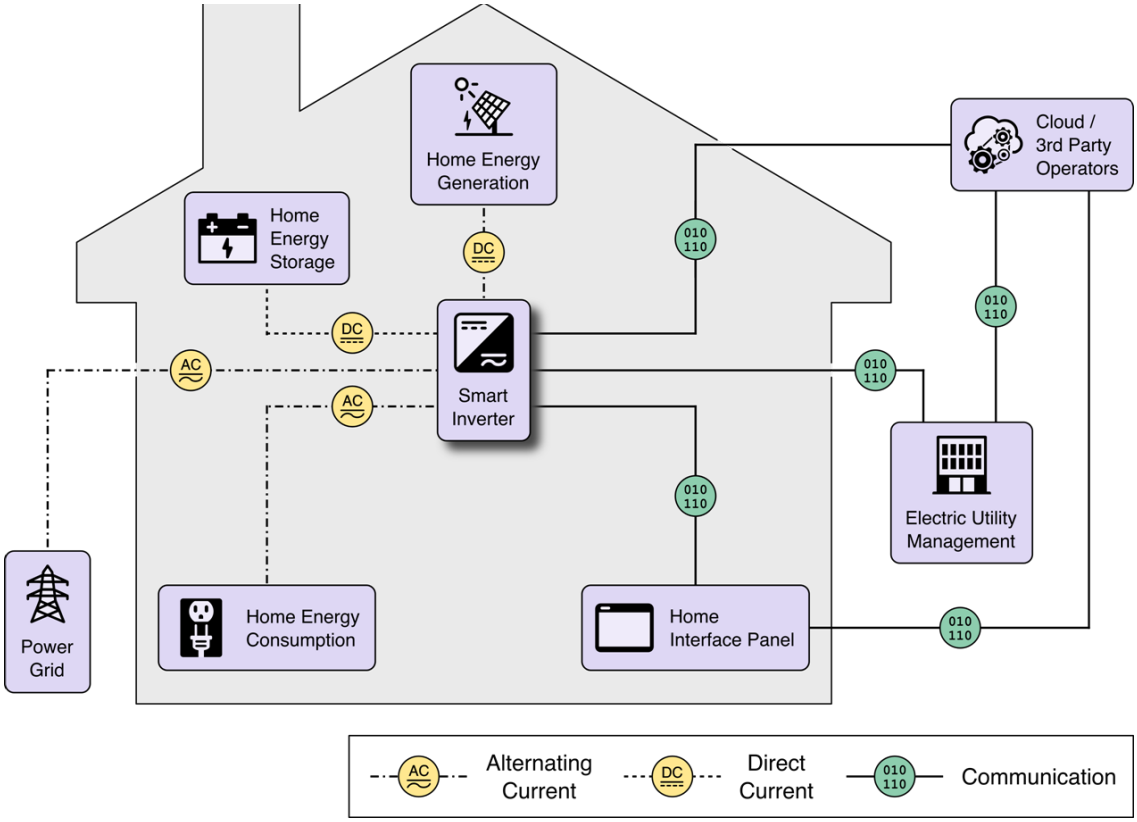

図 2.住宅用または軽商用ソーラー・エネルギー・システムにおけるスマート・インバータの役割

図 2 は、スマート・インバータが住宅用または軽商用の太陽エネルギー・システムで果たす中心的な役割を示している。スマート・インバータは、太陽エネルギー・システムの動作と電力網との相互作用を調整する。スマート・インバータは、システムのソーラー・パネルから直流（DC）電力を受け取り、そのエネルギーを 3 つの用途のいずれかに向ける

1. スマート・インバータは、直流電力を交流（AC）電力に変換し、すぐに使用できるように家庭や中小企業に供給することができる。

2. スマートインバータは、通信リンクを介して電気事業者またはサードパーティ事業者とコミュニケーションすることにより、余剰 AC 電力を電気事業者に供給することができる。

3. 家庭、事業所、または地域の電力会社で交流電力が必要ない場合、スマート・インバータは、ソーラー・パネルによって生成された直流電力を使用して、システムの家庭用エネルギー貯蔵コンポーネントのバッテリーを充電することができる。

さらに、スマート・インバーターは、家庭や企業がソーラーパネルが提供できる以上の電力を必要とする場合、家庭用蓄電コンポーネントからエネルギーを引き出すことができる。スマート・インバータはまた、需要が高い時に送電網をサポートするために家庭用蓄電装置から電力をプロバイダすることもできる。スマート・インバータは、通信リ

ンクを介して電気事業者またはサードパーティ・オペレーターと通信することにより、家庭用エネルギー貯蔵からの電力プロバイダを調整する。

電力会社やサードパーティとの連携に使用される通信リンクが防御されていない場合、スマートインバータは潜在的なサイバー攻撃にさらされる。正しいことが証明されたソフトウェアがない場合、スマートインバーターソフトウェアにはソフトウェアの欠陥が存在すると想定すべきである。いくつかの欠陥は、家庭、事業所、電力網に影響を及ぼす可能性のあるスマートインバー タの動作の操作を可能にすると想定すべきである。

1.1. 想定読者

本稿は、住宅用および小規模商業用スマートインバーター太陽光発電システムの所有者、設置者、保守事業者、および部品製造者のためのサイバーセキュリティガイダンスを提供する。

システム所有者、住宅所有者、中小企業のオーナーは、このガイダンスを使用して、システムに含めるべきサイバーセキュリティ機能を理解し、システムのサイバーセキュリティについてベンダー、設置業者、保守業者と話し合うことができる。システムの設置者は、このガイダンスを使用して設置手順とチェックリストを作成し、設置するシステムがシステム所有者に適切なサイバーセキュリティを提供することを確認することができる。システムの保守者は、このガイダンスを使用して、サイバーセキュリティ関連の保守（例えば、システ ムのパッチ適用）が実施されていることを確認する手順を定義し、システムが適切なセキュリティを継続 的に提供していることを検証することができる。製造事業者は、このガイダンスを使用して、自社の製品が安全な設置および運用をサポートするために必要なサイバーセキュリティ機能を提供していることを確認することができる。

1.2. 報告組織

サイバーセキュリティ・ガイダンスは 4 つの主要なセクションで構成されており、それぞれが特定の読者向けに調整されている。

- セクション 1 では、なぜサイバーセキュリティが住宅および中小企業の太陽光発電システムにとって重要なのか、なぜこのサイバーセキュリティガイダンスがスマートインバータに焦点を当てているのかを説明する。
- セクション 2 では、住宅用または小規模事業用の太陽光発電システムを確実に設置、設定、運用するための 7 つのガイドラインを示す。
- セクション 3 では、IR 8259A および IR 8259B に定義されているように、スマートインバータ製造事業者が製品に含めることを検討すべき 6 つの技術的および 4 つの非技術的サイバーセキュリティ能力を特定する。また、本セクションでは、スマートインバータが安全に設置、設定、運用されることを保証するために、IR 8259A および IR 8259B のサイバーセキュリティ能力に関する追加情報の形で、スマートインバータ固有の推奨事項を示す。
- セクション 4 では、このサイバーセキュリティ・ガイダンスの作成と発表について要約する。

このガイダンスは、ガイドラインや推奨事項の裏付けとなる情報を提供する附属書によって補強されている。

- 附属書 A は、このガイダンスを作成する際に参考にした出版物の書誌である。
- 附属書 B には、略語と頭字語のリストがある。
- 附属書 C は、太陽光発電システム設置者向けのプロビジョニング・チェックリストのサンプルを提供する。このチェックリストは、特定の製品や環境に必要な活動に合わせることができる。設置者は、ガイドラインで定義された行動を完了したことを確認するために、調整したチェックリストを使用することができる。完成したチェックリストは、設置に伴って完了したサイバーセキュリティ関連の活動の記録として、住宅所有者や中小企業所有者と共有することができる。
- 附属書 D は、設置された 5 台のスマートインバータをテストし、セクション 2 で示したガイドラインを実施する能力を測定した結果を記録したものである。
- 附属書 E は、ガイドラインを 6 つの一般的なサイバーセキュリティガイダンスの情報源にマッピングしている。製造事業者は、第 3 章の推奨事項および推奨事項を自社製品に実装する方法をよりよく理解するために、これらのマッピングを使用することができる。
- 附属書 F は、国家脆弱性データベース（NVD）に記録された既知のスマートインバー タのサイバーセキュリティ脆弱性に関する情報を示している。この情報はガイドラインの策定に使用された。

2. 所有者と設置者のためのサイバーセキュリティ・ガイドライン

本セクションでは、住宅所有者、太陽光発電システムの設置者および維持管理者向けに、7 つのガイドラインを示する。これらのガイドラインは、住宅用または小規模事業用の太陽光発電システムを確実に設置、設定、運用するために取るべき行動を定義している。このガイドラインには、設置者、保守者、および住宅所有者が太陽光発電システムのライフサイクル全体で実行すべきスマート・インバータ構成アクションが含まれている。また、これらのガイドラインは、安全な太陽エネルギーシステムの設置のために利用されるべきサイバーセキュリティ防御のコレクションを提供する。

本ガイドラインは、附属書 E に示された一般的なサイバーセキュリティのガイダンスに基づき、5 つのスマートインバー ターで利用可能なサイバーセキュリティ機能に対してテストされたものである。テスト結果は附属書 D に示されている。

各ガイドラインには以下の項目がある：

- ガイドラインの説明
- ガイドラインがれるべき太陽エネルギーシステムのライフサイクル段階の定義
    - 太陽光発電システムのライフサイクルには、製造事業者（[2] ）、設 置（設置）、運転、保守、廃炉（廃棄）の 5 つの段階がある。セクション 2 のガイドラインは、4 つのライフサイクルのうち 1 つ以上のフェーズで実施される：
        - セットアップ - スマート・インバータは、家庭または事業所に設置され、設定される
        - 機能 - 住宅所有者または事業主は、スマート・インバータを使用して、意図された機能を実行する。
        - 保守 - スマートインバータは、問題を修正したり、安全で信頼性の高い運転を継続するために保守を受けます。
        - 廃止措置 - スマート・インバータを家庭または事業所から撤去する。
- ガイドラインを実施するための構成例
    - 本ガイドラインは、製造事業者やスマートインバータのモデルによって実施方法が異なるため、例を高水準で説明している。具体的な手順については、製造事業者の説明書を参照すること。

[2]製造ライフサイクルの段階で実施されるサイバーセキュリティの推奨事項については、第 3 章で説明する。

2.1. ガイドラインその 1：デフォルトのパスワードと認証情報を変更する

デバイス製造事業者は多くの場合、デバイスのインストールとセットアップを簡素化するために、よく知られた、または簡単に発見できるデフォルトパスワード、個々のデバイス固有のパスワード、または他のアクセス認証情報を持つ、事前に構成されたアカウントを作成する。しかし、いったんインストールされ、コミュニケーション・ネットワークに接続されると、これらのパスワードや認証情報は、その値を知っている人なら誰でもデバイスにアクセスし、その構成を変更できるようにする可能性がある。

図 3.ガイドライン#1 ライフサイクル・フェーズ

図 3 に示すように、デバイスのセットアップとインストールプロセス中、事前設定された各アカウ ントには、新しい一意のパスワードまたはクレデンシャルが割り当てられるべきである。デバイスのインストールまたは操作の一部として作成される新しいアカウントには、一意のパスワー ドまたはクレデンシャルを割り当てるべきである。多要素認証[3] (MFA)は、特に特権のあるアカウント（第 2.2 節を参照）[4] のセキュリティを改善することもできる。

人との相互作用に加えて、スマート・インバータは他のシステムやデバイスとも相互作用する可能性がある。これらの相互作用は、強力な認証情報（デジタル証明書など）を使用して相互に認証する必要があり、セットアップ時に工場出荷時のデフォルトから変更する必要がある。

2.2. ガイドライン 2：役割ベースのアクセス管理（RBAC）の使用

責任を果たすために必要な機能のみにアクセスを制限することは、優れたサイバーセキュリティの重要な原則です。家庭や中小企業のソーラー・エネルギー・システムでは、さまざまな人や組織がスマート・インバータにアクセスする必要があるかもしれない。アクセス許可を各人や組織に直接割り当てるよりも、より管理しやすいアプローチは、役割と、特定のタスクを実行するために必要なアクセス許可を識別することでしょう。スマート・インバータには、設置者、保守者、電気事業者、サードパーティ・オペレーター、および住宅所有者の役割が定義されているかもしれない。個人または組織に対するアクセス許可の追加または削除は、1 つまたは複数のロールにアカウントを追加または削除することを含む。システム設置者にとっては、インターフェイスを変更し、システムのさまざまな側面に値を設定して、その環境で正しく機能するようにすることが重要かもしれません。住宅所有者は、代わりにモニターデータや過去の使用状況グラフを表示する機能を必要とするかもしれない。住宅所有者はスマート・インバータを再設定する必要はなく、また再設定できる必要もないでしょうし、システム設置者は過去のデータの一部を

[3]MFA は、以下の要素のうち 2 つ以上を使用する認証である：(i) あなたが知っているもの（パスワード／個人識別番号［PIN］など）、(ii) あなたが持っているもの（暗号化識別装置、トークンなど）、(iii) あなた自身であるもの（バイオメトリクスなど）。

[4]参考文献[4]では、MFA やパスワードなど、さまざまな認証技法における現在のベストプラクティスについて説明している。サイバーセキュリティ・インフラセキュリティ庁（CISA） [5]および連邦捜査局（FBI） [6]は、パスワードのベスト・プラクティスに関する追加ガイダンスを提供している。

必要としないかもしれません。このような役割と権限はさまざまですが、ユーザーに応じてデバイスへの安全なアクセスを確保するためには、役割を分けるというコンセプトが不可欠です。

図 4 に示すように、スマートインバータのライフサイクルのセットアップ段階で、適切なアクセス権限を持つロールの初期コレクションを定義する必要がある。保守段階では、ロールの作成、変更、削除が必要になることがある。たとえば、ソフトウェアの更新によってスマートインバータの機能が追加または削除され、役割定義の更新が必要になることがある。役割への人や組織の割り当ては、定期的に見直して、最新かつ適切であることを確認する必要がある。

図 4.ガイドライン#2 ライフサイクル・フェーズ

スマート・インバータの基本的な役割には、以下のようなものがある：

- スマートインバータの初期設定と構成を実行するために必要なアクセス権限を持つインストーラの役割。スマートインバータの製造事業者は、ガイドライン#1（セクション 2.1）に記載されているように、デフォルトのユーザーアカウントとともにデフォルトの役割としてこれを含めることができる。
- ソフトウェアアップデートのインストール、診断の実行、修理に必要なアクセス権限を持つ Maintainer ロール。
- スマートインバータの動作を監視し、アラートに対応するために必要なアクセス権限を持つホームオーナーロール。

2.3. ガイドライン#3：ログにイベントを記録する設定

サイバーセキュリティに関連する活動のログを別の場所に保存しておけば、予期せぬ事態を招いた要因を特定し、侵害から回復し、今後このような侵害を防ぐ方法を決定するのに役立つ。

検知ログは、イベントが検知されたときのスマートインバータの動作に関する情報（システムパラメータの正常値または異常値など）を含み、レビュアーがある程度忠実にイベントの連鎖を理解できるようにする。イベントロギングは、サイバーイベントへの対応と同様に、スマートインバータの問題のトラブルシューティングをサポートする。

ログには、システム・パラメータに加えて、以下のようなサイバーセキュリティに関連する情報も含まれていなければならない：

- ユーザーアカウントの作成と削除
- 認証に関連する ID を含む、ユーザー認証の成功と失敗。

- スマートインバータのコンフィギュレーション設定の変更（変更前と変更後の値、有効/無効の機能、割り当てられたユーザ・ロール、およびロール・パーミッションを変更したユーザまたはシステムの身元を含む
- 以前は無効だった機能を有効にする
- ソフトウェアおよびファームウェアのアップデートの記録。アップデートの開始方法（ユーザーによるもの、自動的なものなど）、アップデートのソース、アップデートの完全性情報（チェックサム、ハッシュなど）。
- ネットワーク接続や接続喪失などのコミュニケーションイベント
- スマートインバータのコントロールパネルから直接実行されるアクション

図 5 に示すように、ロギング機能は、太陽エネルギーシステムのセットアップ時に設置者が設定し、有効にする必要がある。運用と保守の間、所有者または保守技術者は、情報が意図した通りに収集され、ログに保存されていることを確認する必要がある。

図 5.ガイドライン#3 ライフサイクル・フェーズ

2.4. ガイドライン 4：ソフトウェアの定期的なアップデート

スマート・インバータは、その動作の「スマート」な要素を提供するソフトウェアに依存している。よく開発されたソフトウェアであっても、展開後に脆弱性が発見され、修正する必要がある。さらに、製造事業者はデバイスのソフトウェア機能を継続的に進化させている。したがって、インストール前にアップデートの妥当性、ソース、認証を確認する、スマートインバーター・ソフトウェアをアップデートする安全な手段を提供することが重要である。これにより、ソフトウェアが最新のセキュリティと機能を維持することができる。スマートインバータのセキュリティに影響を与えるアップデートは、できるだけ早く展開する必要がある。スマート・インバータ・ソフトウェアを常に更新しておくことは、デバイスが家庭や中小企業の太陽光発電システムに設置された後に発見された弱点から保護するのに役立ちます。

図 6.ガイドライン#4 ライフサイクル・フェーズ

図 6 に示すように、スマート・インバータのソフトウェアの更新は、機器の初期設定と継続的保守[5] の一環として行うべきである。製造事業者のサポート・ライフサイクルは一般に限られており、製造中止となったデバイスのパッチ

[5]インバーターは、安全な場合にのみ更新を許可するように設計されるべきである。

の開発は中止される。このような場合、所有者は製造中止となったデバイスをできるだけ早く最新モデルに交換する必要がある。

2.5. ガイドライン 5：システム情報のバックアップ

スマートインバータは、特定の家庭または中小企業の太陽エネルギーシステムの要件に基づいてカスタマイズできる構成パラメータまたは設定を有する。これらのパラメータは通常、構成ファイルに保存され、バッテリーの再充電電圧やセキュリティ設定（例えば、第 2.1 節で説明したユーザー認証情報、第 2.2 節で説明した権限やユーザー役割の割り当て）が含まれる。

構成バックアップの作成は、現在の構成情報を別の場所にコピーするプロセスです。スマートインバータの構成のバックアップを維持することで、サイバーまたは非サイバーのいずれかの事象が発生し、太陽エネルギーシステムが動作しない状態になった後、または正しく動作しない状態になった後に、動作を回復するのに役立ちます。構成のバックアップを復元するか、スマートインバータをデフォルト構成に戻す工場出荷時リセットを実行すると、問題が修正される可能性がある。設定復元機能は、セットアップ中にスマートインバーターにあらかじめ構築された設定をロードするためにも使用できる。

図 7 に示すように、スマートインバータのセットアップ時の初期設定後や保守時のパラメータ変更やアップグレード後にバックアップを作成する必要がある。

図 7.ガイドライン#5 ライフサイクル・フェーズ

バックアップは、フラッシュドライブやクラウドストレージなど、検索可能な場所に保存する必要がある。コンフィギュレーション・バックアップの作成方法は、製造事業者や製品によって異なる。

2.6. ガイドラインその 6：未使用の機能を無効にする

スマートインバータは、複数の展開シナリオやユーザー要件をサポートする機能や性能を備えて構築されることがある。このような特徴や機能を持つことで、展開に柔軟性がもたらされる一方で、有効化された各機能によって、デバイスがサイバーセキュリティの脅威にさらされる可能性が高まる。

特定のデバイス展開で使用されない機能や能力を無効にすることも、優れたサイバーセキュリティの重要な原則である。セキュリティを強化し、脅威へのエクスポージャーを減らすために、特定の展開に必要のない機能や能力はすべて無効にすべきである。

太陽光発電システムの運用に必要なスマート・インバータの機能および性能に加えて、あると便利な機能および性能、またはシステムを運用する上で便利な機能および性能があるかもしれない。その機能や性能を使用するかどうかを決定する際には、それらが提供するメリットがサイバーセキュリティの脅威へのエクスポージャーの増加を上回るかどうかを検討すること。

スマートインバータの機能と性能は、図 8 に示すように、セットアップと保守のライフサイクル段階で有効または無効にすることができる。

図 8.ガイドライン#6 ライフサイクル・フェーズ

スマートインバーターに含まれるかもしれないが、特定の展開では必要でないかもしれない特徴や機能には、以下のようなものがある：

- **リモートアクセスプロトコルとインターフェース**スマートインバータの運用や保守には、デバイスへのリモートアクセスが必要な場合がある。展開で使用されないリモートアクセスプロトコルまたはインターフェースは無効にすること。

- **ワイヤレスコミュニケーション。**スマートインバータは、有線と無線の両方のネットワーク接続をサポートしている場合がある。有線接続のみを使用する展開の場合は、ワイヤレスコミュニケーション機能を無効にする必要がある。

- **ゲストおよび/または匿名スマートインバータアクセス。**定義されたユーザーアカウントを持たずにスマートインバーターの機能や機能にアクセスできる Guest ロールは、読み取り専用とし、デバイスの設定や操作の変更を禁止すべきである。

2.7. ガイドライン 7：通信の保護

スマートインバータの重要な側面は、そのコミュニケーション能力である。スマートインバータのコミュニケーションは、電気事業者、第三者事業者、製造事業者、または地域環境の他のデバイスとのコミュニケーションを含む、さまざまな形態をとることができる。インバータは、運転情報を所有者や地域の電力会社に伝えることができる。また、ソフトウェア更新を受け取ったり、潜在的な問題を事前に検知するために操作情報を共有したりするために、装置製造事業者や装置の保守請負業者とコミュニケーションすることもある。しかし、このようなコミュニケーション機能は、サイバー攻撃の経路にもなる。そのため、スマート・インバータを脅威から保護しつつ、本来の目的に必要な通信を行う方法を検討することが重要である。

スマート・インバータの通信を悪意ある行為者から防御しつつ、必要な通信を可能にするには、多くのアプローチが考えられる。インバータは、インターネットのような公共ネットワークにさらされることなく、地域の電力会社とコミュニケーションするために、専用のセルラー接続を持つことができる。所有者とのコミュニケーションは、インバータに直

接接続されたコントロールパネルを使って行われる。更新は、USB「サムドライブようなポータブル記憶装置を使って行うことができる。[6]

スマートインバータは、既存の家庭のインターネット接続を利用して、所有者、電力会社、サードパーティ事業者、製造事業者とコミュニケーションすることができる。インバータが既存のインターネット接続を使用する場合、設置はインバータをネットワーク上の他の活動から分離するための措置を講じるべきである。この防御を提供するには、家庭用または業務用ルータによって作成された別の論理ネットワークなど、いくつかの方法がある。分離技術は、インターネットサービスプロバイダ（ISP）から利用可能な機能に依存する。地域の電力会社や製造事業者とのコミュニケーションに使用される接続は、ローカルネットワーク上の他のデバイスからアクセスできないようにする必要がある。サイバーセキュリティ機能は、電力会社または製造事業者間の仮想プライベート・ネットワーク（VPN）接続など、このような保護を提供することもできる。

図 9 に示すように、防御はセットアップのライフサイクルの段階で確立され、運用のライフサイクルの段階で監視され、効果を維持する必要がある。

図 9.ガイドライン#7 ライフサイクル・フェーズ

[6]一部の古いスマートインバータは、このアップデートメカニズムをプロバイダしている場合がある。スマートインバータのインストーラ/オペレータは、外部メディアを使用してソフトウェアアップデートを実行するリスクを認識する必要がある。また、インストーラ/オペレータは、メディアの出所と、メディアに悪意のあるソフトウェアが含まれていないことを確認する必要がある。

3. スマートインバータ製造事業者に対するサイバーセキュリティの提言

本節では、セクション 2 のガイドラインを実施するために必要なサイバーセキュリティ機能と、スマートイン バータの運用に対するサイバー脅威によりよく対処する機能を提供するために、スマートインバータ製造事 業者に対する推奨事項を示す。これらの勧告には、インバータ設計の変更、インバータソフトウェアとファームウェアの変更、またはインバータインタフェースを保護するための新しいフロントエンドデバイスの追加が含まれる。

3.1. 推奨されるベースライン・サイバーセキュリティ能力

家庭や中小企業の太陽光発電システムに使用されるスマートインバータは、IoT デバイスの一例である。IR 8259「*IoT* デバイス製造者のための基礎的サイバーセキュリティ活動」[7]は、そのガイダンスを「物理世界と直接相互作用するための少なくとも 1 つのトランスデューサ（センサまたはアクチュエータ）と、デジタル世界と相互作用するための少なくとも 1 つのネットワークインタフェース（イーサネット、Wi-Fi、Bluetooth、LTE、Zigbee、Ultra-Wideband [UWB]など）を有する」デバイスに適用すると説明している。スマート・インバータは、送電網の状態を感知し、送電網に電力をプロバイダし、この説明を満たすコミュニケーション・インターフェイスを通じて、送電網の所有者や送電網運用者とコミュニケーションする。新興のインバータ制御装置は、インバータ間の自律的な情報交換も必要とするかもしれない。したがって、IR 8259 [7]に示されている一般的なサイバーセキュリティガイダンスは、スマートインバータにも適用可能である。

IR 8259 シリーズの 2 つの出版物は、すべての IoT デバイスに推奨されるサイバーセキュリティの基本機能を提供している

1. IR 8259A「*IoT* デバイスサイバーセキュリティコアベースライン」[1]は、IoT デバイスが独自の技術的手段（すなわち、デバイスのハードウェアとソフトウェア）を通じて提供する 6 つの技術的サイバーセキュリティ能力のベースラインを定義している。

2. IR 8259B, *IoT Non-Technical Supporting Capability Core Baseline* [2]は、製造事業者またはサードパーティ組織が、IoT 機器のサイバーセキュリティを支援するために実施する 4 つの非技術的サイバーセキュリティ能力（例えば、ソフトウェア更新に関する情報、構成設定の指示、サプライチェーン情報の提供）のベースラインを定義している。

技術的なサイバーセキュリティ能力と非技術的なサポート能力を併用することで、IoT デバイスの使用に関連するサイバーセキュリティ・リスクを緩和しながら、顧客の目標達成を支援することができる。

スマートインバータは IoT 機器であるため、製造事業者は、所有者と設置者が 7 つの基本ガイドラインを実施できるように、ベースラインのサイバーセキュリティ機能をすべて製品に含めることを検討すべきである。表 1 と表 2 は、それぞれ IR 8259A [1]と IR 8259B [2]のベースラインのサイバーセキュリティ機能を各表の第 1 列に示している。さらに、各表の 2 列目と 3 列目には、スマートインバータのサイバーセキュリティ能力に特化したベースラインのサイバーセキュリティ能力に関する情報が含まれている。この追加情報は、附属書 D に示されたスマートインバータの試験と附属書 F に示されたスマートインバータの脆弱性調査から一部得られたものである。

表 1.技術的サイバーセキュリティ能力に関する推奨事項

IR 8259A 技術デバイスのサイバーセキュリティ能力	製造事業者向けスマートインバーターサイバーセキュリティ能力推奨追加情報	スマート・インバータ固有のサイバーセキュリティ能力の説明
デバイスの識別：IoT デバイスは、論理的にも物理的にも一意に識別できる。	スマート・インバータには、太陽エネルギー・システムの他のコンポーネントをインベントリ化する機能がある。この勧告はガイドライン#3 をサポートする。	太陽エネルギー・システムには、スマート・インバーターのほかにコンポーネントが含まれる場合がある（図 11 参照）。これらのコンポーネントには、特殊なゲートウェイ・デバイス、クラウドベースのサービス、あるいはモバイル・アプリが含まれることもある。これらのコンポーネントを識別し、インベントリ化する機能は、システムの活動を包括的に記録し、信頼できるシステム・コンポーネントを認識するのに役立つ。IR 8425 [8]は、IoT デバイスの一意な識別を拡張し、スマートインバータについてここで推奨されているように、IoT 製品のコンポーネント（例えば、クラウドベースのサービス、モバイルアプリ）のインベントリを含む。
デバイスの構成：IoT デバイスのソフトウェアの構成は変更可能であり、そのような変更は認可された事業体のみが実行できる。	スマートインバータは、その構成を外部にバックアップし、バックアップからその構成を復元することができる。この推奨はガイドライン#5 をサポートするものである。	スマートインバータの構成パラメータと設定のバックアップは、偶発的または悪意のある行為によって構成が変更された場合に、構成の迅速な復元を可能にする。スマートインバータは、動作に影響するすべてのパラメータと設定のバックアップを作成し、バックアップを外部記憶場所にエクスポートし、以前に作成したバックアップの整合性を確認し、バックアップから構成を復元できる必要がある
	スマートインバータは、展開において不要な機能を無効にしたり削除したりできるべきである。この勧告はガイドライン#6 をサポートする。	スマートインバータ製品は、さまざまな展開方法をサポートする必要がある。そのため、すべての展開で使用されない機能が含まれている可能性がある。有効であっても使用されていない機能は、悪意のある行為者がスマートインバータに不正にアクセスする機会を増加させる。すべての展開アプローチで使用されない機能は、デフォルトで無効とし、必要なときに設置者が積極的に有効にすることを求めるべきである。この推奨は、コミュニケーションプロトコルにも適用されるべきである。スマートインバータには、サードパーティから取得したソフトウェアが含まれる場合がある。そのようなソフトウェアでスマートインバー タが使用しない機能は、削除または無効にすべきである。
	スマートインバータは、その構成を工場出荷時のデフォルトにリセットすることができる。この推奨はガイドライン#5 をサポートする。	トラブルシューティングのために、スマートインバータをデフォルト設定に戻すことが有利な場合がある。さらに、スマートインバータを廃棄する場合は、工場出荷時のデフォルト設定にリセットし、悪意のある行為者を助ける可能性のある情報を削除する必要がある。
データ保護：IoT デバイスは、保存・送信するデータを不正アクセスや改ざんから保護することができる。	スマートインバータは、通信エンドポイントの相互認証を提供し、伝送中のデータの完全性を保護する安全な通信プロトコルを使用する。この勧告はガイドライン#7 をサポートする。	スマートインバータへの通信インタフェースは、通信路端点の相互認証、伝送中のデータの完全性保護、伝送中のデータの機密性保護を提供する通信プロトコルを使用すべきである。スマートインバータは、本質的にセキュリティ機能を提供するプロトコル（例えば、トランスポート・レイヤー・セキュリティなど）を使用するか、VPN などの技術を使用してセキュリティ機能を欠くプロトコルをラップすべきである。
インターフェースへの論理アクセス：IoT デバ	スマートインバータは、そのサービスにアクセスしようとする事業体の身元を決定す	インバータは、能力へのアクセスを管理するために、誰がその能力にアクセスしようとしているのか、また、どの能力の使用が認可されているの

IR 8259A 技術デバイスのサイバーセキュリティ能力	製造事業者向けスマートインバーターサイバーセキュリティ能力推奨追加情報	スマート・インバータ固有のサイバーセキュリティ能力の説明
イスは、そのローカルおよびネットワーク（ ）インターフェイス、ならびにそれらのインターフェイスで使用されるプロトコルおよびサービスへの論理アクセスを、認可された事業体のみに制限することができる。	るために MFA をサポートする。この勧告はガイドライン#1 をサポートする。	かを知る必要がある。インバータは、ユーザとシステムを認証して、そのアイデンティティを確立する。従来は、単一の認証要素であるパスワードが使用されてきた。しかし、パスワードは、重要なインフラストラクチャに影響を及ぼす可能性のある機能へのアクセスには、もはや適切な認証アプローチ（ ）ではない。スマート・インバータは、より強力な認証技法（MFA など）を使用してユーザを認証する必要がある。[7]スマート・インバータは、人以外の事業体（他のデバイスやシステムなど）ともコミュニケーションする。このような相互作用では、強力なシステム間認証（デジタル証明書など）を使用し、相互認証を提供する必要がある。
	スマートインバータは RBAC をサポートし、ロールを作成、変更、設定する能力を提供する。この推奨は、ガイドライン#2 をサポートする。	アクセス許可を各人に直接割り当てるよりも、より管理しやすいアプローチは、ロールのコレクションを定義し、各ロールが特定の責任を果たすために必要なアクセス許可を定義することである。適切なアクセス権限を持つロールの初期コレクションは、スマート・インバータのライフサイクルのセットアップ段階で定義する必要がある。運用や保守の段階では、ロールの作成、変更、削除が必要になることがある。
	スマートインバータは、認証されていないアクセスによって利用可能な情報の量と種類、およびサービスの種類を最小化する。この勧告はガイドライン#2 をサポートする。	スマートインバータやその動作に関する情報を、本人認証なしに個人やシステムにプロバイダとして提供することが必要になる場合がある。このようなアクセスを提供する場合、製造事業者は最小権限のサイバーセキュリティ原則に従うべきである。すなわち、スマートインバータは、認証されていないユーザに提供する情報の量を最小化すべきである。デバイスの「フィンガープリンティング」（すなわち、明示的にデバイスにアクセスすることなく、デバイスについて可能な限り多くを学習すること）は、悪意のある行為者が不正アクセスを得るために使用できる脆弱性や弱点を突き止めるのに役立ちます。 製造事業者は、非認証インターフェースで共有される情報を最小限に抑えるべきである。製品のバージョン、インストールされている特定のソフトウェアやファームウェア、 ネットワーク情報などの情報は、標的型サイバー攻撃から保護するために共有されるべきではない。
ソフトウェア更新： IoT デバイスのソフトウェアは、安全で設定可能なメカニズムを使用して、	スマートインバータのソフトウェアは、所有者の操作なしに自動的に更新できる。[8] この推奨は、ガイドライン#4 をサポートするものである。	悪用可能な脆弱性を生み出すソフトウェアの欠陥を修正するためにソフトウェア・アップデートをインストールすることは、スマート・インバータのサイバーセキュリティを維持するために非常に重要です。アップデートは、タイムリーにインストールすることが最も効果的である。しかし、アッ

[7]NIST 特別刊行物（SP）800-63 シリーズは、認証技法に関する詳細なガイダンスを提供している。

[8]この推奨は、将来を見据えたものであり、理想的なシナリオを示している。スマートインバータの中には、ソフトウェアを更新するためにユーザーによる操作が必要なものもある。

IR 8259A 技術デバイスのサイバーセキュリティ能力	製造事業者向けスマートインバーターサイバーセキュリティ能力推奨追加情報	スマート・インバータ固有のサイバーセキュリティ能力の説明
認可事業体によってのみ更新できる。		プデートのインストールが所有者や保守者の明示的なアクションに依存している場合、アップデートが十分に迅速にインストールされない可能性がある。自動更新は、更新が可能な限り迅速に適用されるようにすることができる。アップデートがインストールされると、所有者に通知されるべきである。意味のある通知であれば、更新によってどのようなインバータの機能およびサービスが影響を受けたかを特定すべきである。装置はまた、ソフトウェア更新の失敗を認識し、既知のソフトウェアに加えられた変更をロールバックし、更新の失敗を所有者に通知すべきである。自動更新の使用は、すべての展開シナリオにおいて適切であるとは限らないため、設定可能で あるべきである。自動更新機能は、更新をインストールすることが安全である場合、および現在の動作状 況が更新を延期する必要がある場合を認識するように設計されるべきである。 セーフティクリティカルな制御機能のソフトウェアアップデートは、スマートインバータのローカルプログラミングインタフェースを介してのみ実行してください。
サイバーセキュリティ状態の認識：IoT デバイスはサイバーセキュリティの状態を報告し、認可された事業体のみがその情報にアクセスできるようにすることができる。	スマートインバータは、サイバーセキュリティに関連するすべてのイベントのログを記録する。この勧告はガイドライン#3 をサポートする。	スマートインバータが期待通りに動作しなかったときに何が起こったかを判断するには、サイバーセキュリティインシデントを含む、障害につながった活動に関する情報が必要である。スマートインバータは、デバイスの健全性とサイバーセキュリティの両方に関連するイベントを監視し、ログに記録すべきである。スマートインバータの構成変更も含まれるべきである。この情報は、サイバーインシデントで漏洩しないように、リモートストレージにエクスポートされるべきである。
デバイス・セキュリティ[9] ：組織の要件を満たすために IoT デバイスを保護する能力	スマートインバータは、電力網と相互作用する、あるいは家庭や事業所への電力供給と相互作用するセンシングおよび制御機能を、サイバー攻撃にさらされる可能性のある他の機能から保護すべきである。この勧告はガイドライン#7 を支持する。	運用をより適切に保護するために、スマートインバータは、リアルタイム制御機能、セーフティクリティカル機能、およびパワーエレクトロニクスをデータ通信インターフェースから物理的またはソフトウェア的に保護するなど、デバイス内のさまざまな要素やサービス間の相互作用を制御する必要がある。この防御により、サイバーインシデントが物理世界との相互作用に及ぼす潜在的な影響を低減することができる。ローカルにホストされたウェブサーバを含むユーザ・インタラクション・インタフェースについては、仮想化や帯域外セキュリティ監視などの技術を採用すべきである。仮想化によって、ユーザ・インタラクション・インターフェースを、デバイスの安全な運用に不可欠な制御・監視機能から分離することができる。可能な限り、これらの機能はハードウェアレベルで分離

[9]デバイスセキュリティ機能は IR 8259A のベースラインには含まれていないが、SP 800-213A「*IoT Device Cybersecurity Guidance for the Federal Government*（連邦政府向け *IoT* デバイスサイバーセキュリティガイダンス）」で導入された：*IoT Device Cybersecurity Requirement Catalog* [9]で紹介されている。製造事業者に対するいくつかの推奨事項が、デバイスセキュリティ技術能力とよく一致しているため、ここに含まれている。

IR 8259A 技術デバイスのサイバーセキュリティ能力	製造事業者向けスマートインバーターサイバーセキュリティ能力推奨追加情報	スマート・インバータ固有のサイバーセキュリティ能力の説明
		されるべきである（例えば、制御機能には別の処理ユニットを使用し、制御システムハードウェアとユーザーインタラクションハードウェア間の信頼性をゼロと仮定する）。 図 10 は、スマートインバータの制御機能と、スマートインバータの他の機能要素との相互作用を示す。制御機能は、他の機能要素と異なる相互作用が必要な場合がある。これらの相互作用を防御することは、スマートインバータを正しく安全に動作させるために重要である。ソフトウェアの妥協が安全でない動作につながることは避けなければならない。これを確実にするために、電気機械的防御（過電圧サーキットブレーカ、過温度サーキットブレーカ、電気機械的アイランド検出など）が、ソフトウェアが危殆化した場合の安全運転の継続を保証するために必要となる場合がある。製造事業者は、インバーターソフトウェアが侵害されても、ハードウェアが物理的に安全でない状態になることができないようなスマートインバータを設計することが奨励される。
	スマートインバータは、身元が確認された信頼できるソースからのソフトウェアアップ デートのみを受け入れるべきである。この勧告はガイドライン#4 をサポートする。	不正または悪意のあるソフトウェア更新から保護するために、スマートインバータは、ソフトウェア更新 を受け入れる既知の信頼できるソースのリストを持つべきである。ソフトウェア更新を提供しようとするプロバイダの身元は認証されるべきであり、 認証された身元がソフトウェア更新のための既知の信頼できるソースである場合にのみ、更新が許可されるべきである。
	スマートインバータは、インストール前にソフトウェア更新の完全性を確認すべきである。この推奨はガイドライン#4 をサポートする。	スマートインバータは、受信したアップデートが信頼できるソースによって作成されたものであること、およびアップデートが作成された後に変更されていないことを確認する必要がある。ソフトウェア更新の完全性を検証するために、暗号ハッシュやデジタル署名などの技術を使用することができる

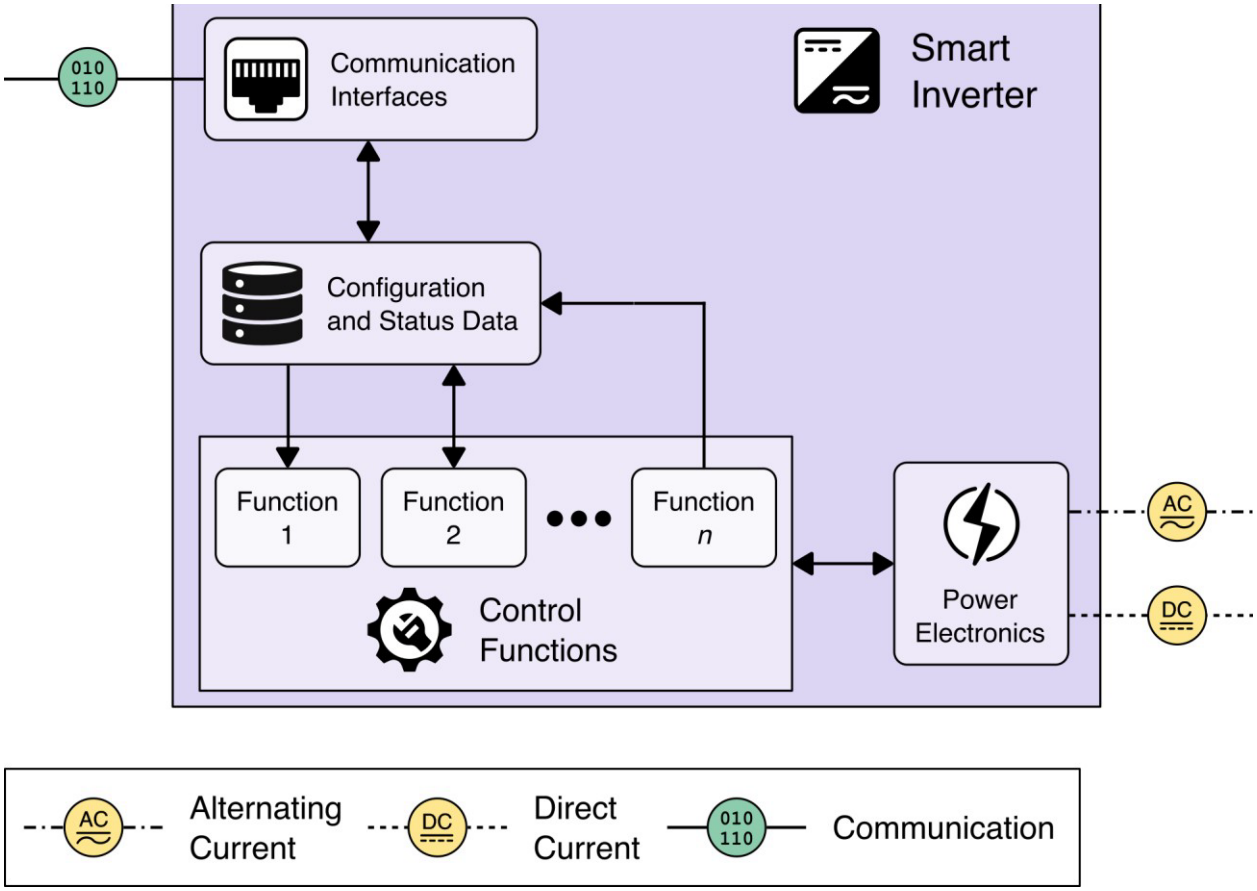

図 10.スマートインバータの機能要素

表 2.非技術的サイバーセキュリティ能力に関する推奨事項

IR 8259B 非技術機器のサイバーセキュリティ能力	製造事業者向け SmartInverter サイバーセキュリティ能力推奨追加情報	スマート・インバータ固有のサイバーセキュリティ能力の説明
文書化：製造事業者及び／又は製造事業者を支援する事業体（ ）が、顧客の購入前、デバイスの開発及びその後のライフサイクルを通じて、IoT デバイスのサイバーセキュリティに関連する情報を作成、収集、保管する能力。	製造事業者は、スマートインバータのソフトウェア部品表（SBOM）を提供し、維持する。この の推奨はガイドライン#4 をサポートする。	SBOM は、新たに発見された脆弱性が特定のデバイスのソフトウェアに適用されるかどうかを所有者と保守者が判断できるように、製品で使用されているライブラリとソフトウェアの詳細を提供する。 SBOM は、スマートインバータの寿命を通じて維持され、ソフトウェア更新による変更を含め、システムソフトウェアの現状を反映すべきである。
	製造事業者は、オーナーや設置者がガイドライン#1-7 を実行できるような文書を作成する。	所有者と設置者が推奨されるガイドラインをすべて実行できるようにするために、広範な文書が必要となる場合がある。この文書には、以下の方法が含まれる： • 認証技術の設定と変更 (例：MFA、パスワード) • ロールの作成と設定 • ソフトウェア・アップデートの

		• 機能の有効化と無効化 • ロギングの設定 • バックアップの有効化と設定 • コミュニケーションインターフェースの設定
情報と問い合わせの受信：製造事業者及び／又は支援事業体が、IoT 機器のサイバーセキュリティに関連する顧客等からの情報及び問合せを受信する能力。	製造事業者は、スマートインバータの脆弱性に関する情報を受け取る機能を開始する。この勧告はガイドライン#4 をサポートする。	製造事業者は、ソフトウェアの更新や改善を開発するために、スマートインバータの脆弱性や製品のその他の問題に関する情報を受け取る機能を持つ必要がある。
	製造事業者は、スマートインバーターに関する所有者や設置者からの質問を受け付け、対応する機能を開始する。この勧告はガイドライン#1-7 をサポートする。	所有者と設置者は、設置、初期設定、システム運転中の定期保守など、スマート・インバータのライフサイクルのすべての段階で問題に遭遇する可能性がある。製造事業者は、所有者や設置者からの質問を受け付け、タイムリーに対応する方法を持つべきである。
情報発信：製造事業者及び／又は支援事業体が、IoT 機器のサイバーセキュリティに関連する情報を（例えば、顧客又は IoT 機器のエコシステム内の他者に）ブロードキャストし、配布する能力。	製造事業者は、オーナーや設置者がガイドライン#1-7 を実施できるよう、最新の情報を発信する。	スマートインバータのサポートライフサイクルを通じて、サイバーセキュリティとガイドラインの実施に影響する関連する脅威、脆弱性、リスクに関する新しい情報が得られる可能性が高い。製造事業者は、所有者と設置者がすべての推奨ガイドラインを正常に実行できるように、更新された文書、速報、および/または通知を普及させる機能を備えるべきである。
教育と認識：製造事業者及び／又は支援事業体が、IoT 機器のエコシステムにおいて、サイバーセキュリ ティ関連の情報、考慮事項、機能などについて、顧客やその他の人々の認識を高め、教育する能力。	製造事業者は、所有者や設置者が理解しやすい形式で、関連情報や啓発資料を提供する。この勧告は、ガイドライン#1-7 を支持する。	スマート・インバータの確実で安全な設置と保守は、効果的な教育と認識にかかっている。製造事業者は、利用しやすく理解しやすい形式で情報、リソース、啓発資料を提供することで、所有者と設置者が推奨されるガイドラインをすべて確実に実行できるよう支援することができる。

住宅所有者、中小企業のオーナー、系統運用者、そして社会は、住宅用および軽商用の太陽光発電システムが安全かつ確実に動作することを合理的に期待している。スマート・インバータの製造事業者は、製品においてこれらの期待に十分に応えるべきである。

4. 結論

スマート・インバータは、潜在的なサイバーセキュリティの脅威にさらされ、その意図された動作に影響を及ぼすリスクを生み出している。これらのシステムの普及、依存、相互接続の拡大は、スマート・インバータに対するリスクが電力網に対するより広範なリスクを引き起こす可能性があることを意味する。

本報告書は、小規模住宅および中小企業向け太陽光発電システムの安全な設置と運用を改善するため、太陽光発電システムの所有者、設置者、保守業者向けに 7 つの基本的なサイバーセキュリティガイドラインを提供する。本報告書はまた、スマートインバータ製造業者に対するサイバーセキュリティ勧告も提供している。これらの勧告は、IR 8259A [1]および IR 8259B [2]の IoT サイバーセキュリティ能力ベースラインの一部について、スマートインバータ固有のガイダンスを提供するものである。製造事業者は、所有者と設置者が 7 つの基本ガイドラインを実施できるように、自社の製品にサイバーセキュリティ能力のベースラインをすべて含めることを検討すべきである。

これらのガイドラインと勧告は、いくつかの情報源から得られたものである。既存のスマート・イン バータの既知の脆弱性（附属書 F を参照）を特定するために NVD をレビューし、ガイドラインは、可能な限り、こ れらの脆弱性からのリスクを低減するための措置を提案した。一般的なサイバーセキュリティガイダンスの 6 つの情報源をレビューし、スマートインバータおよび太陽エネル ギーシステムコンポーネント製造事業者向けの具体的なガイドラインと推奨事項を特定した（附属書 E 参照）。ガイドラインの実用性は、既存の市販スマートインバーター5 機種に適用して検証したが、7 つのガイドラインをすべて実施できたのは 2 機種のみであった（附属書 D 参照）。製造事業者がこの勧告に従えば、将来のスマートインバータは 7 つのガイドラインをすべて実施できるようになるはずである。

参考文献

[1] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259A. https://doi.org/10.6028/NIST.IR.8259A.

[2] Fagan MJ, Marron JA, Brady KG, Jr., Cuthill BB, Megas K, Herold R (2021) IoT NonTechnical Supporting Capability Core Baseline.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259B. https://doi.org/10.6028/NIST.IR.8259B.

[3] 米国エネルギー情報局（2024 年）EIA は、2024 年に米国の年間太陽光発電量が水力発電量を上回ると予想している。https://www.eia.gov/todayinenergy/detail.php?id=60

[4] Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines : Authentication and Lifecycle Management.(National Institute of Standards and Technology, Gaithersburg, MD）、NIST 特別刊行物（SP）NIST SP 800-63B。

[5] CISA (2019) パスワードの選択と防御｜CISA.https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords。

[6] Brennan B, Smith K (2021) FBI Tech Tuesday：強力なパスフレーズとアカウント防御。連邦捜査局.https://www.fbi.gov/contactus/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-strong-passphrases-andaccount-protection。

[7] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259. https://doi.org/10.6028/NIST.IR.8259.

[8] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline for Consumer IoT Products.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425.https://doi.org/10.6028/NIST.IR.8425.

[9] Fagan MJ, Megas KN, Marron JA, Brady KG, Jr., Cuthill BB, Herold R, Lemire D, Hoehn B (2021) IoT Device Cybersecurity Guidance for the Federal Government：IoT デバイスのサイバーセキュリティ要件カタログ。(National Institute of

Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) NIST SP 800-213A. https://doi.org/10.6028/NIST.SP.800-213A.

[10] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.80053Ar5.

[11] 国立標準技術研究所（2024）NIST サイバーセキュリティ枠組み（CSF）2.0。(国立標準技術研究所、メリーランド州ゲイサーズバーグ） NIST サイバーセキュリティ白書（CSWP） NIST CSWP 29.

[12] CIS (2021) CIS Critical Security Controls® v8.https://www.cisecurity.o

[13] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD）、NIST 特別刊行物（SP） NIST SP 800-53r5。2020 年 12 月 10 日時点の更新を含む。

[14] mitre、mitre att&ck®。https://attack.mitre.org。

[15] International Society of Automation/International Electrotechnical Commission (2009) *ISA/IEC 62443-2-1-2009* 産業用オートメーション及び制御システムのセキュリティ *Part 2-1*：産業用オートメーションおよび制御システムのセキュリティプログラムの確立。Available at https://webstore.ansi.org/search/find?in=1&st=ANSI%2FISA-62443-21+%2899.02.01%29-2009

附属書 A. その他のリソース

- NERC (2023) Electric Vehicle Dynamic Charging Performance Characteristics during Bulk Power System Disturbances.https://www.nerc.com/comm/RSTC/Documents/Grid_Friendly_EV_Charging_Recomme ndations.で入手可能。
- Center for Internet Security CIS Controls Version 8.。
- National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6
- NIST (2019) National Vulnerability Database - Home.で利用可能。
- P.Ruggiero and M. Heckathorn (2012) Data Backup Options.。
- M.ウィルソン (2022) 太陽光発電の「トリップ」が自然エネルギーにとって送電網の脅威となる理由。E&E News.。
- 国家安全保障局（2023 年）Best Practices for Securing Your Home Network, Version 1.0.(国家安全保障局、フォート・ミード、メリーランド州）。で入手可能。
- 米国エネルギー情報局（2020 年） 太陽光発電は 2020 年には米国の電力の 3%であったが、2050 年には 50%になると予測している。米国エネルギーU.S. Energy 情報局（Information Administration） - EIA - 独立統計局（Independent Statistics and Analysis）で入手可能。
- 米国エネルギー省（2023 年）サイバー情報工学実施ガイド第 1.0 版。で入手可能。

附属書 B. 記号、略語、頭字語のリスト

AC	Alternating Current	交流
CIS	Center for Internet Security	インターネットセキュリティセンター
CISA	Cybersecurity and Infrastructure Security Agency	サイバーセキュリティ・インフラストラクチャセキュリティ機関
DC	Direct Current	直流
FBI	Federal Bureau of Investigation	連邦捜査局
IoT	Internet of Things	モノのインターネット
ISA/IEC	International Society of Automation/International Electrotechnical Commission	国際自動制御連盟/国際電気標準会議
ISP	Internet Service Provider	インターネットサービスプロバイダ
NCCoE	National Cybersecurity Center of Excellence	国家サイバーセキュリティセンター・オブ・エクセレンス
NIST	National Institute of Standards and Technology	国立標準技術研究所
NIST IR	NIST Interagency or Internal Report	NIST 政府機関間または内部報告書
NVD	National Vulnerability Database	国家脆弱性データベース
RBAC	Role-Based Access Control	役割ベースのアクセス制御
SBOM	Software Bill of Material	ソフトウェア部品表
USB	Universal Serial Bus	ユニバーサル・シリアル・バス
US-CERT	United States Computer Emergency Readiness Team	米国コンピュータ緊急対応チーム
VPN	Virtual Private Network	仮想プライベートネットワーク

附属書 C. 住宅用および軽商用太陽エネルギーシステム設置サイバーセキュリティチェックリスト

	アクション	備考
ガイドライン#1 - デフォルトのパスワードと認証情報を変更する	☐ デフォルトまたはデバイス固有のパスワードを、ユニークで安全なものに変更する。	
	☐ その他のデフォルトの認証情報をユニークで安全な値に変更する。	
	☐ 利用可能な場合は MFA を使用する	
ガイドライン#2 - 役割ベースのアクセス管理(RBAC)の使用	☐ ユーザーアカウントの作成	
	☐ ユーザー・ロールの作成	
	☐ ユーザーアカウントをロールに割り当てる	
	☐ 未使用のアカウントを無効にする	
ガイドライン#3 - ログにイベントを記録する設定	☐ ロギングの有効化と設定	
	☐ ログの外部保存場所を設定する	
ガイドライン 4 - ソフトウェアを定期的にアップデートする	☐ 最新のソフトウェア/ファームウェアバージョンをダウンロードして確認する	
	☐ 現在のソフトウェア/ファームウェアバージョンでデバイスをアップデートする	
ガイドライン#5 - システム情報のバックアップと復元	☐ 機器設定のダウンロード	
	☐ 利用可能なすべての構成をダウンロードする	
	☐ 検索可能な場所に設定を保存する	
ガイドラインその 6 - 未使用の機能を無効にする	☐ 使用していないインターフェースや機能などを無効にする。	
	☐ セキュリティ機能を有効にする	
ガイドライン#7 - 通信の保護	☐ デバイスがパーソナルネットワークから隔離されている	

附属書 D. スマート・インバータの試験

セクション 2 で示したサイバーセキュリティガイドラインをサポートする能力を判断するために、5 つのスマートイン バータを分析した。この試験は、2022 年秋に、当時市販されていたスマート・インバータを用いて実施された。テストは 2 つの方法のいずれかで実施された：試験」と「テスト」で

- レビューされた一般に入手可能な文書を調査し、勧告を実施することが可能かどうかを判断
- インバータの通信インタフェースを介したインバータとのコミュニケーションにより、ガイドラインが実施可能かどうかをテストした。[10]

テストされたインバーターはそれぞれ、3 つの接続方法のうちの 1 つを実施した

1. **インバータへの直接接続。**このインタフェース方式では、インバータ自体がサイバーセキュリティ・ガイドラインをすべて実装できる必要がある。
2. **ゲートウェイ装置とインバータの接続。**このインターフェース方式により、ゲートウェイ装置はサイバーセキュリティガイドラインの一部を実施することができる。
3. **インバータへのクラウドベースのサービス接続。**クラウドベースのサービスは通常、ゲートウェイ装置を介してインバータに接続される。このインタフェース方式では、サイバーセキュリティガイドラインの実装をインバータ、ゲートウェイ装置、クラウドベースサービスの間で分散できる。

ゲートウェイ機器接続とクラウドベースのサービス接続については、テストでは、接続のどのコンポーネントがサイバーセキュリティガイドラインを実装しているかは判断できなかった（以下を図 11 参照）。

[10]SP 800-53Ar5 [10]は、試験方法に関する追加情報を提供している。

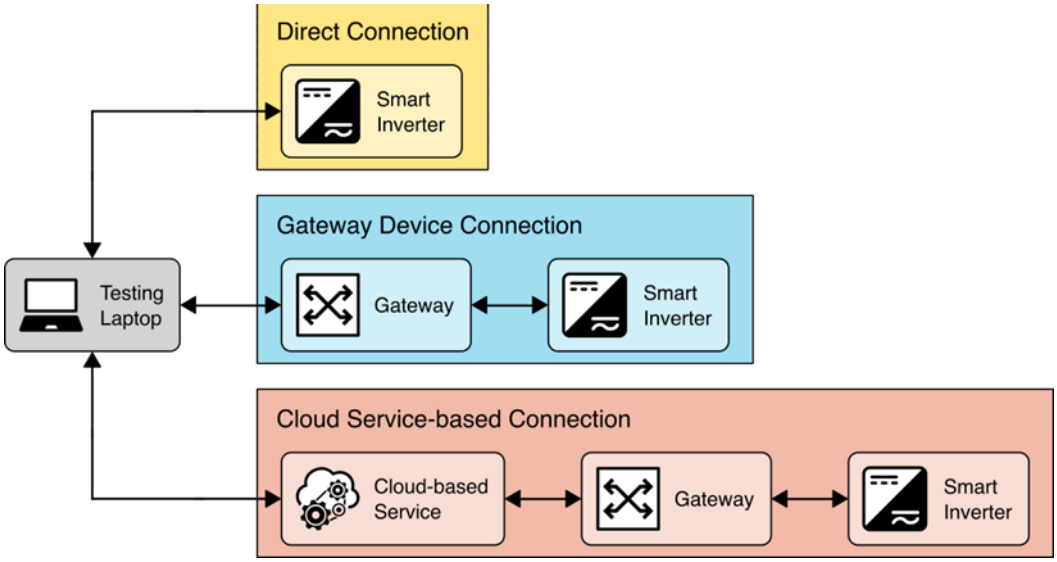

図 11.インバータの接続方法

表 3.試験したインバーターの特性

システム	インバータサイズ [11]	外部ゲートウェイ [12]	クラウド接続 [13][14]
インバーター	5.5 kW	はい	はい
インバーター	5.5 kW	はい	いいえ
インバーター	10.5 kW	はい	はい
インバーター	5 kW	はい	はい
インバーター	15 kW	いいえ	いいえ

[11]これはインバータの定格サイズを指す。

[12]インバータには、インバータにアクセスし、潜在的にインバータを管理するためのゲートウェイとして機能する外部システムがある。

[13]このシステムは、システムを監視し、潜在的に制御するためのクラウドサービスをサポートするように設計されている。

[14]「NA」は、スマートインバータが従来のアカウントを利用しないことを意味する。ワイヤレス・アクセス・ポイント経由で接続する携帯電話アプリケーションか、スマート・インバーターのフロント・パネルを使って設定する。

D.1.ガイドライン#1: デフォルトパスワードと認証情報の変更に関するテスト結果

このテストは、スマート・インバータがすべてのデフォルト・アカウントを識別し、それらのアカウ ントに関連付けられたデフォルト認証情報を一意の安全な認証情報に変更する能力を検証した。このテストは以下の場合に合格とみなされる：

- ベンダーの文書には、デフォルトのアカウント識別情報がすべて記載されていた。
- すべてのデフォルトアカウント認証情報を変更可能
- インバータは MFA をサポート

表 4.ガイドライン#1 のテスト結果

インバーター	デフォルトアカウントがベンダーのドキュメントに記載されている [#]	デバイスのデフォルトアカウントが特定されている [#]	資格情報の変更が可能 [はい/いいえ]	MFA の導入が可能 [はい/いいえ]
A	3	3	はい	いいえ
B	2	2	はい	いいえ
C	NA[14]	NA	はい	いいえ
D	NA	NA	はい	いいえ
E	2	2	はい	いいえ

D.2.ガイドライン#2：役割ベースのアクセス管理の使用」のテスト結果

このテストでは、スマートインバータが RBAC を使用して機能と能力へのアクセスを管理する能力を検証した。スマートインバータのアクセス管理には 3 つのレベルが識別された：

1. **レベル 1 - 基本。**スマートインバータはシングルユーザーアカウントを提供する。単一ユーザーアカウントにログインすることで、すべてのスマートインバータの機能と性能にアクセスできる。
2. **レベル 2 - 役割アカウント。**スマートインバータは、設置者、保守者、所有者などの定義された役割ごとに単一のアカウントをプロバイダする。役割アカウントのクレデンシャルは、その役割で行動することを認可された人たち（ ）と共有されます。役割アカウントにログインすると、その役割に関連するすべての機能と機能にアクセスできる。
3. **レベル 3 - RBAC。**スマートインバータは、役割と関連するアクセス許可のコレクションを定義する機能を提供する。ユーザは、定義されたロールにアカウントを割り当てることでアクセス権を付与されます

このテストでは、インバータがサポートするアクセス管理のレベルをアセスメントした。

表 5.ガイドライン#2 のテスト結果

インバーター	対応アクセス管理レベル
A	レベル
B	レベル 2
C	レベル 3
D	レベル 3
E	レベル 2

役割に基づくある程度のアクセス管理は、テストした 5 台のスマート・インバータすべてでサポートされていた。ほとんどのスマート・インバータは、「管理者／設置者」アカウント／ロールと「ユーザー」アカウント／ロールをサポートしていた。一部のスマート・インバータは、「ゲスト」アカウント／ロールもサポートしていた

D.3.ガイドライン#3: ログにイベントを記録する設定」のテスト結果

このテストでは、セキュリティに関連するイベントをログに記録し、定期的に外部ソースにエクスポートするスマート・インバータの機能を検証した

このテストは、デバイスが可能であれば合格とみなされた：

- 以下のセキュリティ関連イベントをログに記録する
    - o ログイン成功
    - o ログイン失敗
    - o コンフィギュレーションの変更
    - o ファームウェア・アップデート
    - o イベント（ネットワーク接続を含む
- ログを外部ソースにエクスポートする

表 6.ガイドライン#3 のテスト結果

インバーター	ロギングをサポート	セキュリティ関連のイベントログをサポート

A	はい	いいえ
B	はい	いいえ
C	はい	いいえ
D	はい	いいえ
E	はい	はい

テストされたデバイスはすべてロギングをサポートしていたが、そのロギング機能のほとんどは、インバータの動作に関連する機能（電力出力、グリッド接続など）に重点を置いており、セキュリティ関連の情報はほとんど提供されていなかった。テストしたスマート・インバータのうち、規準を完全にサポートしていたのは 1 台だけであった。

D.4.ガイドライン#4: ソフトウェアの定期的なアップデート」のテスト結果

このテストでは、セットアップと保守のライフサイクルの両方の段階で、スマートインバータがソフトウェアを更新する能力を検証した。

このテストは、以下の場合に合格とみなされた

- スマートインバータには、ソフトウェアのアップデートを実行する仕組みがあった
- スマートインバータの製造事業者は、ソフトウェアのアップデートを提供した。
- スマートインバータにプロバイダされたソフトウェア更新の完全性は保護され、検証可能であった。

表 7.ガイドライン#4 のテスト結果

イン	ソフトウェア・完全対応

テストしたスマートインバータのうち 5 台すべてが、ソフトウェアのアップデートを実行するための完全なメカニズムを提供していた。その仕組みはスマートインバーター・ベンダーによって異なり、ウェブベースのインターフェイス、カスタム・アップデート・アプリケーション、クラウド・サービスからのプッシュ・アップデートなどがあった。

D.5.ガイドライン#5：システム情報のバックアップのテスト結果

この試験では、スマートインバータの構成をバックアップして別の場所に保存し、事前に構築した構成をインストールしたり、バックアップから構成を復元したりするスマートインバータの能力を検証した。

このテストは、スマートインバータが可能であれば合格とみなされた

- 設定を別の場所にバックアップする
- バックアップから設定を復元する

表 8.ガイドライン#5 のテスト結果

インバーター	設定のバックアップをサポート	設定の復元をサポート
A	はい	はい
B	いいえ	いいえ
C	いいえ	いいえ
D	いいえ	いいえ
E	いいえ	いいえ

テストしたスマートインバータのうち、デバイス設定のバックアップと復元をサポートしていたのは 1 台だけだった。

D.6.ガイドライン#6: 未使用の機能を無効にする」のテスト結果

この試験は、特定の展開で必要とされる機能と能力だけを有効にするスマートインバータの能力を検証するものである。スマートインバータは、すべての運転条件で必要とされない機能や能力を有効または無効にできるべきである。

このテストは、以下の場合に合格とみなされた

- スマートインバータは、未使用のインターフェースを無効にする機能を備えている。
- スマート・インバータには、使用されていない機能や性能を無効にする機能がある。

表 9 ガイドライン#6 試験結果

インバーター	機能を無効にできる

A	Modbus インターフェース
B	Modbus および Web サーバー・インターフェース
C	いいえ
D	いいえ
E	いいえ

テストしたインバーターのうち、インターフェース、機能、能力を無効にする機能を備えていたのは 2 機種だけだった。

D.7.ガイドライン#7: 通信の保護」のテスト結果

このテストでは、スマートインバーターが個人用機器とは別のネットワーク上に設置できるかどうか（つまり、機器が専用ネットワーク上で動作できるかどうか）を検証した。

このテストは、スマートインバータがサポートしていれば合格とみなされた

- イーサネットまたは Wi-Fi 接続
- セカンダリーネットワーク（携帯電話など）接続

表 10.ガイドライン#7 のテスト結果

インバーター	接続タイプ
A	イーサネット
B	イーサネット
C	４G
D	４G
E	イーサネット

テストしたスマートインバータのうち 2 台だけがセルラーネットワーク接続をサポートしていたが、イーサネット接続はサポートしていなかった。むしろ、Wi-Fi アクセス・ポイントやスマート・インバータのコントロール・パネルを使ってセルラー接続を設定していた。イーサネット・ネットワークをセグメント化したり、スマート・インバータ接続用に専用の

Wi-Fi ネットワークを構築したりする機能は、ネットワーク・インフラの機能であり、スマート・インバータの能力に依存するものではない。

附属書 E. 一般的なサイバーセキュリティガイダンスへのマッピング

この附属書は、一般的なサイバーセキュリティガイダンスと、セクション 2 で示したスマートインバータの設置および運用のためのガイドラインとの間のマッピングを提供する。

E.1.ガイドラインに影響を与える一般的なサイバーセキュリティガイダンス

サイバーセキュリティに関する 6 つのガイダンスが、このガイドラインと推奨事項の策定に役立った

1. 重要インフラのサイバーセキュリティ改善のための NIST 枠組み（CSF）
2. センター・フォー・インターネット・セキュリティ クリティカル・セキュリティ・コントロール（CSC）8
3. SP 800-53r5（改訂 5 版）
4. SP 800-213A
5. MITRE ATT&CK フレームワーク
6. ISA/IEC

E.1.1.NIST サイバーセキュリティ枠組み

NIST サイバーセキュリティフレームワーク バージョン 2.0（CSF 2.0）[11] は、サイバーセキュリティリスクのマネジメントに役立つサイバーセキュリティ成果の分類法を提供している。この分類法の構成要素は、各成果の詳細を示す機能、カテゴリー、サブカテゴリーの階層である。本報告書のガイドラインは、サイバーセキュリティの成果を達成するための各ガイドラインの貢献を示すために、CSF のサブカテゴリーにマッピングされている。

E.1.2. インターネットセキュリティセンター クリティカルセキュリティコントロール（CSC）バージョン 8

Center for Internet Security (CIS) Critical Security Controls (CSC) version 8 [12]では、小規模から大規模のエンタープライズのセキュリティを確保するための、優先順位付けされた 18 の統制について記述している。各規制は、統制の概要、重要性、実施手順、および保護措置の説明だけでなく、さまざまな規模のエ ンタープライズに対する実施ガイドラインとともに提示されている。CSC バージョン 8

また、NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1 とのマッピングも含まれており、一致するコントロールに合わせることができる。

E.1.3.NIST SP 800-53r5

SP 800-53r5 [13]は、組織内のセキュリティとプライバシーのリスクに対処する 20 のコントロール・ファミリーを識別している。これらの統制には、監督責任を負う者が、連邦政府の情報システムには必須であり、連邦政府の領域外の組織にも適用可能な実施戦略を確立するのに役立つ潜在的な影響レベルが含まれている。

E.1.4.NIST SP 800-213A

NIST の「モノのインターネット（IoT）のためのサイバーセキュリティ」プログラムは、コネクテッドデバイスとそれらが展開される環境のサイバーセキュリティを改善するための標準、ガイドライン、関連ツールの開発と適用を支援している。政府、産業界、国際団体、学界のステークホルダーと協力することで、信頼を培い、世界規模でのイノベーションを可能にする環境を醸成することを目的としている。NIST の IoT 向けサイバーセキュリティ・プログラムは、製造事業者が IoT 機器への統合を検討し、消費者が機器の有効化/設定を検討すべき基本的な機能を IR 8259A[1]および IR 8259B[2]で定義している。

デバイスのサイバーセキュリティ機能とは、IoT デバイスが独自の技術的手段（すなわち、デバイスのハード ウェアとソフトウェア）を通じて提供するサイバーセキュリティ機能または特徴である。非技術的支援能力とは、製造事業者またはサードパーティ組織が、IoT デバイスのサイバーセキュリティを支援するために実行する行動である（例えば、ソフトウェア更新に関する情報、構成設定の指示、サプライチェーン情報のプロバイダ）。デバイスのサイバーセキュリティ能力と非技術的支援能力を併用することで、顧客の目標達成を支援しながら、IoT デバイスの使用に関連するサイバーセキュリティリスクを緩和することができる。

また、NIST の IoT 向けサイバーセキュリティチームは、SP 800-213A [9]において、デバイスのサイバーセキュリティ能力と非技術的なサポート能力の大規模なカタログを公表している。このカタログの能力は、SP 800-53r5 [13]のセキュリティ管理から派生したものであり、カタログ内で簡単に参照できるように標準識別子を含んでいる。

表 11 は、スマート・インバータのサイバーセキュリティ・ガイドラインを、SP 800-213A のデバイスのサイバーセキュリティ能力および非技術的支援能力に対応付けたものである。これらの能力を提供するデバイスとプロバイダを選択することで、ガイドラインの達成を支援することができる。

E.1.5.MITRE ATT&CK フレームワーク

MITRE の ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）枠組み[14]は、サイバーセキュリティ・イ ベントのライフサイクルにおける敵対的な手法と行動を記述している。ATT&CK フレームワークは、Microsoft Windows エンタープライズネットワークに対する高度な持続的脅威 （APT）から観察された戦術、技術、手順（TTP）に基づいて開発されました。ATT&CK は、戦術、技法、サブ技法、およびこれらの技法と手順の文書化された敵対者の使用という 4 つの中核的な構成要素で構成されている。ATT&CK マトリックスに示されている各手順には、戦術、テクニック、例、緩和戦略、検知戦略が記述されている。

E.1.6.ISA/IEEC 62443-2-1

ISA/IEC 62443「産業オートメーションと制御システムのためのセキュリティ（IACS）」[15]は、制御システムと運用技術のサイバーセキュリティを管理するための要件と方法を扱う標準のコレクションである。標準は 4 つの階層で構成されている：

一般、ポリシーと手順、システム、コンポーネント。ISA-62443-2-1 は、産業用オートメーション及び制御システム（IACS）のサイバーセキュリティリスクを低減する可能性のある、手続き、職員の能力、及び技術ベースの能力を実装し、維持することからなるセキュリティプログラムの要件を定義している。本文書のセキュリティプログラム要件は、脆弱性に対処することでリスクを緩和することを意図している。要件を満たさない場合、そのような脆弱性が存在する可能性がある。

E.2.ガイドラインと一般的なサイバーセキュリティガイダンスとの関係

表 11.サイバーセキュリティに関するガイダンス文書と設置・運用に関するガイドラインとのマッピング

CSF 2.0 サブカテゴリー	CSC v8	SP 800-53r5	SP 800-213A	MITRE ATT&CK 緩和	62443-2-1
ガイドライン 1：デフォルトのパスワードと認証情報を変更する					
PR.AA-05	4.7 5.2	アクセス・エンフォースメント［AC-3］	DC：PRV(1)、AUT(1)、INT(1)、CTL(4d) LA: AUN(1), AUN(2), ACF(2) DO：SMP(5b,c,e)、MNT(1g) EA: CSC(2c), CSC(3a,b,c), RSP(1, g)	アクセス管理 [M0801] パスワードポリシー [M0927]	USER 1.11
ガイドライン 2：役割ベースのアクセス管理を使用する					
PR.AA-05 PR.AA-03 PR.AT-02	5.1 5.4 6.8	アクセス・エンフォースメント［AC-3］	DC：prv(1)、aut(1)、 ラ：ロル(1)、ロル(2)、ロル(3)、ロル(4)、ロル(5)、ロル(6)、ロル(8)、ロル(9) DO：SMP(3b)、SMP(5j, k.l)、DSC(4b)、 MNT(1g) EA：CSC(2c)、CSC(3a,b,c)、RSP(1d,e,f,g,h)	特権アカウント管理 [M1026] ユーザーアカウント管理 [M1018]	USER 1.5 USER 1.8
ガイドライン 3：ログへのイベント記録の設定					

CSF 2.0 サブカテゴリー	CSC v8	SP 800-53r5	SP 800-213A	MITRE ATT&CK 緩和	62443-2-1
PR.PS-04	8.2	イベント・ロギング [AU-2]	DI: AID(2) CS：aei(2), eim(1), eim(2), eim(3), lct(1), rdl(1), rdl(2), rdl(3), rdl(4), rdl(5), rdl(6), lsr(1), lsr(2), lsr(3), lsr(4), srt(1), srt(2), srt(3), srt(4), aup(3), aup(4), aup(7) DS：OPS(1) DO: SMP(8) ID: CRI(7b)	リモート・データ・ストレージ [M1029]	イベント 1.1
ガイドライン 4：ソフトウェアを定期的にアップデートする					
PR.	7.3	欠陥の [SI-2]。	DI：AID(3) DP：クライ(3), クライ(4), クライ(5), ストックス(3) SU：UPD(1), UPD(6), APP(1).APP(2)、APP(3) DO：SMP(12)、 IQ：バグ(1a,b,c,d,e) ID：CRI(1a,b,c)、CRI(2a,c)、CRI(3a,b,c) EA：CSC(4a,b)、EOL(1a,b)、VMG(2a,b)	ソフトウェアの更新 [M0951]	COMP 3.1 COMP 3.2
ガイドライン 5：システム情報のバックアップ					

CSF 2.0 サブカテゴリー	CSC v8	SP 800-53r5	SP 800-213A	MITRE ATT&CK 緩和	62443-2-1
ID.AM-03 PR.IR-03 RC.RP-01	11.1 11.2	システム・バックアップ [CP-9] システム復旧 再構成 [CP-10]	DC: CTL(2) DPSTO(3) EA: BAK(1a,b,c)	データバックアップ [M0953]	AVAIL 1.1 AVAIL 2.5
ガイドライン 6：未使用の機能を無効にする					
ID.AM-01 ID.AM-02	2.1 4.8	ベースライン構成 [CM-2] 最小機能［CM-7］	DC：CTL(1)、CTL(2) ラ：IFC(2)、IFC(3)、IFC(6) DS：OPS(8) DO: SMP(10) EA: EXP(1)	ソフトウェア・コンフィギュレーション [M0954] 機能またはプログラムの無効化または削除 [M0942] ソフトウェアのインストールを制限する [M1033]	CM 1.1 COMP 1.1
ガイドライン 7：通信の防御					
PR.IR-01	12.2	境界防御［SC-7］	DS: COM(1) DO: SMP(5h)	ネットワーク・セグメンテーション [M0930]	NET 1.1

附属書 F. スマートインバータの脆弱性調査

スマートインバータで確認されている既知のサイバーセキュリティ脆弱性をよりよく理解するため、NVD は 2022 年初めに見直された。表 12 は、一般的なキーワード（例：ソーラー、インバータ、太陽光発電）と製造事業者固有のキーワードの両方を使用した NVD の複数のポイント・イン・タイム検索から作成された。表中の項目は、NVD から該当する共通脆弱性エクスポージャー（CVE）のサブセットである。この調査により、ガイドラインが対処すべきサイバーセキュリティ上の懸念が明らかになった。

表 12.スマートインバータの脆弱性調査

#	脆弱性#	概要	発効	CVSS v3 の度
1	CVE-2019-19229	3.14.1 (HM 1.12.1) より前の Fronius Solar Inverter デバイスの admincgi-bin/service.fcgi では、action=download&filename= ディレクトリトラバーサルが可能です。	2019 年 12 月 4 日	V3.1: 6.5 中
2	CVE-2019-19228	3.14.1 (HM 1.12.1) より前の Fronius Solar Inverter デバイスでは、today アカウントのパスワードが /tmp/web_users.conf ファイルに保存されているため、攻撃者は認証をバイパスすることができる。	2019 年 12 月 4 日	V3.1: 9.8 重要
3	CVE-2018-12927	Northern Electric & Power (NEP) 社のインバータ装置では、リモート攻撃者が nep/status/index/1 URI への直接リクエストを経由して、潜在的に機密性の高い情報を取得できる可能性がある。	2018 年 6 月 28 日	V3.0: 7.5 高
4	CVE-2018-12735	SAJ Solar Inverter は、リモートからの攻撃者が inverter_info.htm または english_main.htm URI への直接リクエストを経由して潜在的にセンシティブな情報を取得することを可能にする。	2018 年 6 月 25 日	V3.0: 7.5 高
5	CVE-2017-9863	** SMA Solar Technology 社の製品に問題が発見されました。ユーザーが同時に Sunny Explorer を実行し、悪意のあるホストにアクセスした場合、クロスサイトリクエストフォージェリーを使用してインバータの設定を変更することができる（たとえば、ユーザーパスワードを変更するために POST リクエストを発行する）。認証ユーザーが利用可能なすべての Sunny Explorer 設定は、攻撃者も利用可能です。(場合によっては、ユーザーがアクセスできない設定の変更も含まれます）。これにより、デバイスが完全に侵害される可能性がある。注：ベンダーは、Sunny Explorer は滅多に使用されないため、悪用される可能性は低いと報告している。また、Sunny Boy TLST-21 および TL-21、Sunny Tripower TL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 8.8 高

#	脆弱性#	概要	発効	CVSS v3 の度
6	CVE-2017-9860	** SMA Solar Technology 社の製品に問題が発見されました。攻撃者は、Sunny Explorer または SMAdata2+ ネットワークプロトコルを使用して、認証することなくデバイスのファームウェアを更新することができる。攻撃者がインバータに受け入れられるカスタム・ファームウェア・バージョンを作成することができれば、インバータは完全に侵害されます。これにより、攻撃者は、例えば、ローカル OS へのアクセス権を与えたり、ボットネットを作成したり、企業への踏み台としてインバータを使用したりなど、ほとんど何でもできるようになる。注：ベンダーによれば、この攻撃は常に "完全性と互換性の最終チェック "によってブロックされている。また、サニーボーイ TLST-21 および TL-21、サニートリパワーTL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 9.8 重要
7	CVE-2017-9859	** SMA Solar Technology 社の製品に問題が発見されました。インバータは、REGISTER 要求のパスワードを暗号化するために、弱いハッシュアルゴリズムを使用している。このハッシュアルゴリズムは、比較的簡単に解読することができる。攻撃者はオフラインのクラッカーを使ってパスワードをクラックできる可能性が高い。このクラックされたパスワードを使って、SMA サーバーに登録することができる。注: ベンダーの見解は、"このような 操作が成功する確率は極めて低いと考える "というものです。また、サニーボーイ TLST-21 および TL-21、サニートリパワーTL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 9.8 重要
8	CVE-2017-9858	** SMA Solar Technology 社の製品に問題が発見されました。インバータに細工したパケットを送信し、その応答を観察することで、アクティブなユーザーアカウントと非アクティブなユーザーアカウントを特定することができる。これにより、どのユーザーが存在し、どのユーザーが存在しないかを正確に知ることができるため、（ブルートフォース攻撃などの）更なる攻撃に役立ちます。注：ベンダーの見解は、これは「セキュリティ・ギャップそのものではない」というものである。また、サニーボーイ TLST-21 および TL-21、サニートリパワーTL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 7.5 高
9	CVE-2017-9855	** SMA Solar Technology 製品に問題が発見されました。インストーラーには、グリッドガードシステムと呼ばれる二次認証システムが用意されている。このシステムは予測可能なコードを使用し、1 つのグリッドガードコードをどの SMA インバータでも使用することができる。このようなコードをインストーラアカウントと組み合わせると、非常に機密性の高いパラメータを変更することができる。注意：グリッドガードは認証機能ではなく、単なるトレース機能であるとベンダーは報告している。また、サニーボーイ TLST-21 および TL-21、サニートリパワー TL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 9.8 重要
10	CVE-2017-9853	** SMA Solar Technology 製品に問題が発見されました。すべてのインバーターは、ユーザーとインストーラーのパスワードポリシーが非常に弱い。複雑さの要件も長さの要件も設定されていません。また、最大 12 文字と限られた文字数のため、強力なパスワードは不可能です。注：プロバイダは、12 文字の制限は "非常に高いセキュリティ標準" を提供すると報告している。また、サニーボーイ TLST21 および TL-21、サニートリパワー TL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 9.8 重要

#	脆弱性#	概要	発効	CVSS v3 の度
11	CVE-2012-5861	Sinapsi eSolar Light 太陽光発電システムモニター (別名 Schneider Electric Ezylog 太陽光発電 SCADA 管理サーバー)、Sinapsi eSolar、Sinapsi eSolar DUO のファームウェア 2.0.2870_2.2.12 より前のバージョンに複数の SQL インジェクション脆弱性があり、リモートの攻撃者に、(1) dettagliinverter.php の primo アクションの inverterselect パラメーター、または (2) changelanguagesession.php の lingua パラメーター経由で任意の SQL コマンドを実行される可能性がある。	2012 年 11 月 23 日	該当なし
12	CVE-2019-13529	攻撃者が認証済みのオペレータに悪意のあるリンクを送信することで、リモートの攻撃者が Sunny WebBox ファームウェアバージョン 1.6 以前のユーザの権限でアクションを実行できる可能性がある。このデバイスは、ログイン成功後のコミュニケーションを維持するために IP アドレスを使用するため、悪用されやすくなります。	2019 年 10 月 9 日	V3.1: 8.8 高
13	CVE-2017-9864	** SMA Solar Technology 社の製品に問題が発見されました。攻撃者は、認証されていない状態でもプラントの時刻を変更することができる。これによりシステム時刻が変更され、タイムスタンプに基づくロックアウトポリシーや乱数生成器に影響を与える可能性があり、データ分析のためのタイムスタンプが信頼できなくなります。注意 というのも、これはログ入力のタイムスタンプに影響するだけであり、プラントの時刻は後に NTP 経由でリセットされるからである。(ロックアウト・ポリシーや乱数発生器が影響を受けたことはない) 。また、サニーボーイ TLST-21 と TL-21、サニートリパワーTL-10 と TL-30 だけが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 7.5 高
14	CVE-2017-9862	** SMA Solar Technology 社製品に問題が発見されました。誤ったパスワードで Sunny Explorer にサインインすると、デバッグ報告書が作成され、アプリケーションに関する情報が開示され、攻撃者が自分の好きな内容の .txt ファイルを作成し保存できる可能性がある。攻撃者はこれを情報公開に利用したり、ローカルシステム上の通常利用できない場所にファイルを書き込んだりすることが可能です。注：ベンダーは、「デバッグ・報告書に含まれる 情報は、ほとんど重要ではない」と報告している。また、Sunny Boy TLST-21 および TL-21、Sunny Tripower TL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 7.5 高
15	CVE-2017-9861	** SMA Solar Technology 社の製品に問題が発見されました。セッション開始プロトコル(SIP)の実装では、暗号化を伴う認証が適切に使用されていないため、リプレイ攻撃、パケットインジェクション攻撃、中間者攻撃の脆弱性がある。攻撃者は、ローカルエリアネットワーク（LAN）内のどこからでも、SIP を使用してデバイスと正常にコミュニケーションすることができる。攻撃者はこれを利用して、デバイスをクラッシュさせたり、SMA サーバーとのコミュ ニケーションを停止させたり、既知の SIP 脆弱性を悪用したり、SIP コミュニケーション から機密情報を見つけたりすることができる。さらに、SIP コミュニケーションチャネルは暗号化されていないため、プロトコルを理解できる攻撃者はコミュニケーションを盗聴することができる。例えば、パスワードを抽	2017 年 8 月 5 日	V3.0: 9.8 重要

#	脆弱性#	概要	発効	CVSS v3 の度
		出することができる。注：ベンダーの見解では、隔離されたサブネットワークでは暗号化による認証は不要である。また、サニーボーイ TLST-21 および TL-21、サニートリパワー TL-10 および TL-30 のみが影響を受ける可能性がある。		
16	CVE-2017-9857	** SMA Solar Technology 社製品に問題が発見されました。SMAdata2+ 通信プロトコルは、暗号化された認証を適切に使用していないため、中間者攻撃、パケットインジェクション、リプレイ攻撃に対して脆弱性がある。設定変更、認証パケット、スカウティングパケットなどはすべて、リプレイ、インジェクション、中間者セッションに使用される可能性がある。Sunny Explorer で利用可能なすべての機能は、攻撃者がパケット設定を正しく行えば、ネットワーク内のどこからでも効果的に実行できる。これには、すべての(非表示を含む)アクセスレベルの認証プロセスや、獲得したアクセス権に応じた設定の変更が含まれます。さらに、SMAdata2+の通信チャネルは暗号化されていないため、プロトコルを理解できる攻撃者は、コミュニケーションを盗聴することができる。注意: ベンダーの見解では、隔離されたサブネットワークでは暗号化による認証は必要ありません。また、サニーボーイ TLST-21 および TL-21、サニートリパワー TL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 8.1 高
17	CVE-2017-9856	** SMA Solar Technology 社の製品に問題が発見されました。SMAdata2+のコミュニケーションから盗聴されたパスワードは、非常に簡単に解読することができる。パスワードは非常に単純な暗号化アルゴリズムを使って「暗号化」されている。このため、攻撃者は平文のパスワードを見つけ、デバイスを認証することができる。注意: ベンダーの報告によると、影響を受ける可能性があるのは Sunny Boy TLST-21 および TL-21 と Sunny Tripower TL-10 および TL-30 のみです。	2017 年 8 月 5 日	V3.0: 9.8 重要
18	CVE-2017-9854	** SMA Solar Technology 社の製品に問題が発見されました。ローカルホスト上の特定のパケットをスニッフィングすることで、ユーザが Sunny Explorer に入力した平文のパスワードを取得することができる。これらのパスワードは、デバイス全体を侵害するために使用することができる。注：ベンダーは、これらのパケットは通常インストール中に一度だけ送信されるため、悪用の可能性は低いと報告している。また、Sunny Boy TLST21 および TL-21、Sunny Tripower TL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 9.8 重要
19	CVE-2017-9852	** SMA Solar Technology 社の製品において、不正なパスワード管理の問題が発見されました。デフォルトのパスワードはほとんど変更されません。ユーザーパスワードはほぼ常にデフォルトです。インストーラーのパスワードは、同じ会社によってインストールされたインストーラーの間でデフォルトか類似していると予想される（しかし、変更されることもある）。隠しユーザアカウントは、(すべての隠しユーザアカウントについてテストするためにはさらなる調査が必要ですが、少なくともいくつかのケースでは)すべてのデバイスに対して固定パスワードを持っている。攻撃者がこれらの隠しユーザーアカウントのパスワードを取得できる脆弱性は他にも存在する。注: ベンダーは、 パスワードの割り当てに影響力はなく、グローバルにハードコードされたマスターパス	2017 年 8 月 5 日	V3.0: 9.8 重要

#	脆弱性#	概要	発効	CVSS v3 の度
		ワードは存在しないと報告している。また、Sunny Boy TLST-21 および TL-21、Sunny Tripower TL-10 および TL-30 のみが影響を受ける可能性がある。		
20	CVE-2017-9851	** SMA Solar Technology 製品に問題が発見されました。無意味なデータを送信したり、Sunny Explorer のデータベースポートに TELNET セッションを設定したりすると、アプリケーションがクラッシュする可能性がある。注意: ベンダーの報告によると、起こりうる最大の被害はコミュニケーション障害です。また、Sunny Boy TLST-21 および TL-21、Sunny Tripower TL-10 および TL-30 のみが影響を受ける可能性がある。	2017 年 8 月 5 日	V3.0: 7.5 高
21	CVE-2015-3964	SMA Solar Sunny WebBox にはハードコードされたパスワードがあり、リモートの攻撃者が不特定のベクター経由でアクセスを取得しやすくなっている。	2015 年 9 月 11 日	V3.x:(使用不可)
22	CVE-2018-7797	Power Monitoring Expert、Energy Expert (旧称 Power Manager) - EcoStruxure Power Monitoring Expert (PME) v8.2 (全エディション)、EcoStruxure Energy Expert 1.3 (旧称 Power Manager)、EcoStruxure Power SCADA Operation (PSO) 8.2 Advanced Reports およびダッシュボードモジュール、EcoStruxure Power Monitoring Expert (PME) v9.0、EcoStruxure Energy Expert v2.0、および EcoStruxure Power SCADA Operation (PSO) 9.0 アドバンスレポートおよびダッシュボードモジュールは、悪意のあるサイトにリダイレクトされた際にフィッシング攻撃を受ける可能性がある。	2018 年 12 月 17 日	V3.0: 6.1 中
23	CVE-2012-5864	ファームウェアバージョン 2.0.2870_2.2.12 以前の Sinapsi eSolar Light Photovoltaic System Monitor（別名 Schneider Electric Ezylog photovoltaic SCADA 管理サーバー）、Sinapsi eSolar、および Sinapsi eSolar DUO の管理ウェブページは認証を必要としないため、リモート攻撃者が直接リクエストを行うことで、ping.php へのリクエストで示されるように、管理者アクセス権を取得することが可能である。	2012 年 11 月 23 日	V3.x:(使用不可)
24	CVE-2012-5863	2.0.2870_2.2.12 以前のファームウェアを持つ Sinapsi eSolar Light 太陽光発電システムモニター（別名 Schneider Electric Ezylog 太陽光発電 SCADA 管理サーバー）、Sinapsi eSolar、および Sinapsi eSolar DUO の ping.php により、リモートの攻撃者が ip_dominio パラメータのシェルメタキャラクターを介して任意のコマンドを実行する可能性がある。	2012 年 11 月 23 日	V3.x:(使用不可)
25	CVE-2012-5862	2.0.2870_2.2.12 以前のファームウェアを持つ Sinapsi eSolar Light 太陽光発電システムモニター（別名 Schneider Electric Ezylog 太陽光発電 SCADA 管理サーバー）、Sinapsi eSolar、および Sinapsi eSolar DUO	2012 年 11 月 23 日	V3.x:(使用不可)

#	脆弱性#	概要	発効	CVSS v3 の度
		の login.php は、複数のハードコードされたアカウントを確立する。このため、リモート攻撃者は、このスクリプトに含まれる(1)平文のパスワード、または(2)パスワードハッシュを利用して、管理者アクセスを容易に取得できる。		
26	CVE-2012-5861	Sinapsi eSolar Light 太陽光発電システムモニター (別名 Schneider Electric Ezylog 太陽光発電 SCADA 管理サーバー)、Sinapsi eSolar、Sinapsi eSolar DUO のファームウェア 2.0.2870_2.2.12 より前のバージョンに複数の SQL インジェクション脆弱性があり、リモートの攻撃者に、(1) dettagliinverter.php の primo アクションの inverterselect パラメーター、または (2) changelanguagesession.php の lingua パラメーター経由で任意の SQL コマンドを実行される可能性がある。	2012 年 11 月 23 日	V3.x:(使用不可)
27	CVE-2017-6019	Schneider Electric Conext ComBox、モデル 865-1058、V3.03 BN 830 より前のすべてのファームウェアバージョンに問題が発見されました。デバイスへの一連の高速リクエストにより、デバイスが再起動する可能性がある。	2017 年 4 月 7 日	V3.0: 7.5
28	CVE-2021-33209	2.97.10 以前の Fimer Aurora Vision に問題が発見されました。ログインに失敗した際の応答で、ユーザー名とパスワードのどちらが間違っているかが公開され、攻撃者がユーザー名を列挙するのに役立ちます。これにより、ブルートフォース攻撃が容易になります。	2021 年 11 月 3 日	V3.1: 5.3 中
29	CVE-2021-33210	2.97.10 以前の Fimer Aurora Vision に問題が発見されました。攻撃者は（WebUI において）、プラントのキオスクビューから API のレスポンスを読み取ることで、認証なしでプラント情報を取得できる。	2021 年 11 月 3 日	V3.1: 4.3 中
30	CVE-2020-25755	Enphase Envoy R3.x および D4.x (およびその他の現行) デバイスで問題が発見されました。installer/upgrade_start の upgrade_start 機能により、リモートの認証ユーザーに force パラメーター経由で任意のコマンドを実行される可能性がある。	2021 年 6 月 16 日	V3.1: 8.8 高
31	CVE-2020-25754	Enphase Envoy R3.x および D4.x デバイスで問題が発見されました。従来のユーザー認証を回避するユーザー認証用のカスタム Pluggable Authentication Module (PAM)がある。このモジュールは、ユーザー名とシリアル番号の MD5 ハッシュから生成されるパスワードを使用する。シリアル番号は、認証されていないユーザーが/info.xml で取得できる。passwd やその他のツールを使ってユーザーパスワードを変更しようとしても、効果はありません。	2021 年 6 月 16 日	V3.1: 7.5 高

#	脆弱性#	概要	発効	CVSS v3 の度
32	CVE-2020-25753	v3 ソフトウェアを搭載した Enphase Envoy R3.x および D4.x デバイスで問題が発見されました。デフォルトの管理パスワードは、シリアル番号の下 6 桁に設定されている。シリアル番号は、認証されていないユーザーが /info.xml で取得できる。	2021 年 6 月 16 日	V3.1: 9.8 重要
33	CVE-2020-25752	Enphase Envoy R3.x および D4.x デバイスで問題が発見されました。インストーラと Enphase アカウント用のハードコードされたウェブパネルログインパスワードがある。これらのアカウントのパスワードは、ユーザー名とシリアル番号の MD5 ハッシュにいくつかの静的文字列を混ぜたハードコードされた値です。シリアル番号は、認証されていないユーザが /info.xml で取得できる。これらのパスワードは攻撃者が簡単に計算することができる。ユーザーはこれらのパスワードを変更することができません。	2021 年 6 月 16 日	V3.1: 5.3 中
34	CVE-2019-7678	Enphase Envoy R3.*.* に、images/、include/、include/js、または include/css を介した、TCP (Transmission Control Protocol) ポート 8888 におけるディレクトリトラバーサルの脆弱性が発見されました。	2 月 9 日 2019 年	V3.0: 9.8 重要
35	CVE-2019-7677	Enphase Envoy R3.*.*に、TCP ポート 8888 の/home URI の profileName パラメータを経由したクロスサイトスクリプティング（XSS）が存在する。	2 月 9 日 2019 年	V3.0: 6.1 中
36	CVE-2019-7676	Enphase Envoy R3.*.* に脆弱なパスワードが発見されました。管理者アカウントの admin パスワードで TCP ポート 8888 経由でログインできる。	2 月 9 日 2019 年	V3.0: 7.2 高
37	CVE-2021-20662	SolarView Compact SV-CPT-MC310 Ver.6.5 以前のバージョンにおいて、クリティカルな機能に対する認証が欠落しているため、攻撃者は不特定のベクターを経由して、アクセス権限なしに設定情報を変更することができる。	2021 年 2 月 24 日	V3.1: 7.5 高
38	CVE-2021-20661	Ver.6.5 以前の SolarView Compact SV-CPT-MC310 には、ディレクトリトラバーサルの脆弱性があり、認証された攻撃者は、指定されていないベクトルを介して、サーバー上の任意のファイルおよび/またはディレクトリを削除することができる。	2021 年 2 月 24 日	V3.1: 8.1 高
39	CVE-2021-20660	Ver.6.5 以前の SolarView Compact SV-CPT-MC310 には、クロスサイトスクリプティングの脆弱性があり、攻撃者は指定されていないベクトルを介して任意のスクリプトを注入することができる。	2021 年 2 月 24 日	V3.1: 6.1 中
40	CVE-2021-20659	Ver.6.5 より前の SolarView Compact SV-CPT-MC310 では、認証された攻撃者が不特定のベクターを 介して任意のファイルをアップロードする可能性がある。ファイルが PHP スクリプトの場合、攻撃者は任意のコードを実行する可能性がある。	2021 年 2 月 24 日	V3.1: 8.8 高

#	脆弱性#	概要	発効	CVSS v3 の度
41	CVE-2021-20658	SolarView Compact SV-CPT-MC310 Ver.6.5 より前のバージョンでは、攻撃者は、特定されていないベクトルを介して、ウェブサーバ特権で任意の OS コマンドを実行することができる。	2021 年 2 月 24 日	V3.1: 9.8 重要
42	CVE-2021-20657	SolarView Compact SV-CPT-MC310 Ver.6.5 以前のバージョンにアクセス管理の脆弱性が存在し、認証された攻撃者が、不特定のベクターを経由して、アクセス権限なしに設定情報を取得または変更される可能性がある。	2021 年 2 月 24 日	V3.1: 5.4 中
43	CVE-2021-20656	Ver.6.5 以前の SolarView Compact SV-CPT-MC310 において、ディレクトリの一覧表示による情報のエクスポージャーにより、認証された攻撃者がシステム内部のディレクトリやファイル構成などの情報を不特定のベクター経由で取得できる可能性がある。	2021 年 2 月 24 日	V3.1: 4.3 中
44	CVE-2021-34544	2.8.2 ビルド 52 2013.04.23 以前の Solar-Log 500 に問題が発見されました。/export.html、email.html、sms.html に、平文のパスワードが保存されている。これにより、デバイスにアクセスできる何者かによって機密情報が読み取られる可能性がある。	2021 年 12 月 7 日	V3.1: 6.5 中
45	CVE-2021-34543	2.8.2 Build 52 より前の Solar-Log 500 のウェブ管理サーバーは認証を必要としないため、リモートの攻撃者がサーバーに接続することで管理者権限を取得できる。その結果、攻撃者は設定ファイルを変更し、システムの状態を変更することができる。	2021 年 12 月 7 日	V3.1: 7.5 高