2022 特定課題研究計画書：太陽光発電インバータへのサイバー攻撃による電圧変動リスク評価

1　背景

DX（デジタルトランスフォーメーション）が我々の社会を根本的に変革させつつある．例えば，ZOOM や Google docs をはじめとする各種オンラインサービスは完全リモートワークを可能にし，働き方さえ変えてしまった．しかしながら DX が進むにつれて，サイバー攻撃が犯罪組織にとって魅力的なビジネスとなってしまっている．McAfee のレポート [1] によると，2020 年にはサイバー犯罪による金額的損失は年間１兆ドルにも達しつつあると推定されている上，今後もさらに上昇していく見込みである．この巨額の被害が示す通り，社会的観点からサイバーセキュリティがその重要性をますます増していくことは間違いないと思われる．

さらに，サイバー攻撃の脅威は我々の実世界にも及びつつある．計測装置の高性能化や深層学習に代表されるデータ処理技術の発展に伴う CPS（Cyber-Physical System）の普及により，エネルギー，製造，交通，都市，医療，農業等の基幹産業のスマート化に向けたパラダイムシフトが加速している．CPS では HMI（Human-Machine Interface，注：制御システムにおける基本的な構成要素）等の標準的な通信端末だけでなく，センサ，アクチュエータ，コントローラ等の物理的な作用を伴う装置がネットワークに直接繋がり，新たな攻撃対象領域（注：専門用語，Attack Surface）および脆弱性（注：専門用語，vulnerability）を生じる．実際，社会に深刻な影響を与えたインシデントとして，イランの核物質濃縮工場に対する攻撃 (Stuxnet) [2]，ウクライナの電力系統に対する攻撃 (BlackEnergy3) [3]，米国の石油パイプラインに対する攻撃 [4] 等の多くの実例が挙げられる．これらの事例が示すように，CPS のセキュリティは学術界と産業界を問わずその重要性が意識されている [5]．もちろん制御コミュニティも多くの貢献をしており，その成果は例えばサーベイ論文 [6] 等でまとめられている．日本語の解説としては例えば文献 [7] 等を参照すること．

2　先行研究

本研究では，基本的なインフラである電力系統を取り扱う．エネルギーは我々の生活の根幹を成しその影響力もきわめて大きいため標的として魅力的であり，実際にサイバー攻撃による停電も発生している [3]．現状の電力系統は，世界的な脱炭素（あるいはカーボンニュートラル）の流れに沿って，太陽光等の再生可能エネルギーをベースロード電源とする次世代電力系統（スマートグリッド）への転換が急速に進んでいる．スマートグリッドは典型的な CPS であり，そのセキュリティはきわめて重要な課題となる（参考：英語の文献 [8]，日本語の解説スライド [9]）．

以上の問題意識から，笹原は以下の研究

M. Lindsrtöm, H. Sasahara, X. He, H. Sandberg, and K. Johansson, “Power injection attacks in smart distribution grids with photovoltaics,” *European Control Conference,* 2021.

を行った．この研究は太陽光発電装置を大量導入した配電網，あるいはマイクログリッドを対

象としている．太陽光発電装置は DC/AC 変換および制御のためのインバータを備えており，インバータは将来的には無線ネットワークを介して効率的な分散制御を実現するための基幹装置として用いられると想定されている [10]．脅威シナリオとして，インバータへの通信端末の乗っ取りによる，発電指令値の改ざんを想定している．また等価なシナリオとして，大容量バッテリーを用いて作為的に追加電力を注入する攻撃を想定している．発電量が変化すれば背後の物理法則（Kirchhoff の法則）から系統の電圧が変化する．品質管理上電圧は一定範囲内に抑える必要があり，過度の電圧偏差は tripping（注：一部を分離すること）のための保護リレー装置の起動および地域の停電を招く．このシナリオでは，停電が起こり得るかどうかは実際に電圧が変動し得る範囲に依存するため，事前のリスク評価のために，攻撃の規模の大きさと電圧偏差の大きさの対応関係を調べた．具体的には『最も電圧変動の大きい電力注入時系列及び攻撃位置は何か？』という問題に解を与えた．

3　研究計画

しかしながら，前述の先行研究では，結果の証明に数学的に不明瞭であったり厳密でない部分があり，その正しさを改めて検証する必要がある．また，シミュレーションもやや小規模なものであり、十分に現実的な状況を模しているとは言い難い．これらを踏まえて，本研究課題では

- 先行研究の主張の精査および結果の補完的な検証
- 現実的なシミュレーションの実施とその結果の考察

を今後 12 週間の目標とする．

この目標に向けた具体的な研究計画として，以下のスケジュールを提案する．

- 第 1 週〜第 3 週：CPS および電力セキュリティに関する背景の理解（参考：[6, 7, 8]），本研究の数理的な問題の特殊ケースの計算
- 第 4 週〜第 6 週：電力系統の構成の理解（参考：[11, 12] の一部を後に指定，日本語の文献は知らないので，必要そうであれば一緒に探しましょう），一般ケースの証明，簡単なシミュレータの構築
- 第 7 週〜第 9 週：現実的なモデル（例えば [13] で用いられている 12 バスモデル）を用いたシミュレーション，発表の構成検討
- 第 10 週〜第 12 週：シミュレーション結果の考察，発表準備
- 第 13 週〜第 16 週：課題報告書執筆，院試勉強

また，一週間程度の間隔でミーティングを行う．簡単なものでいいので

- 一週間で目標としたこと
- 実際にやったこと
- 得られた知識・知見
- 目標とのズレ
- 次の一週間の計画

をまとめたスライドを作って話すこと．

参考文献

[1] Z. Smith, E. Lostri, and J. Lewis, "The hidden costs of cybercrime," McAfee, 2020, [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

[2] Cybersecurity & Infrastructure Security Agency, "Stuxnet malware mitigation," Tech. Rep. ICSA-10-238-01B, 2014, [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-10-238-01B.

[3] ——, "Cyber-attack against Ukrainian critical infrastructure," Tech. Rep. IR-ALERT-H-16-056-01, 2018, [Online]. Available: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.

[4] ——, "DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks," Tech. Rep. AA21-131A, 2021, [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa21-131a.

[5] 経済産業省, "サイバー・フィジカル・セキュリティ対策フレームワーク," 2019, [Online]. Available: https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf.

[6] S. Dibaji, *et al.,* "A systems and control perspective of CPS security," *Annual Reviews in Control,* Vol. 47, pp. 394-411 2019.

[7] 澤田 賢治, 細川 嵩, "制御システムとサイバーフィジカルセキュリティ, " 計測と制御, Vol. 58, No. 8, pp. 618–623, 2019.

[8] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE,* vol. 100, no. 1, pp. 210–224, 2012.

[9] 芹澤 善積, "電気エネルギーシステムにおけるサイバーセキュリティ," 2015, [Online]. Available: http://www.iee.jp/wp-content/uploads/honbu/03-conference/data-31/symp_150130/doc03.pdf.

[10] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics,* Vol. 9, No. 5, pp.5326-5340, 2021.

[11] P. Kundur, *Power System Stability and Control,* McGraw-Hill, 1994.

[12] A. Pabla, *Electrical Power Distribution,* McGraw-Hill, 2011.

[13] S. Civanlar, J. Grainger, H. Yin, and S. Lee, "Distribution feeder reconfiguration for loss reduction," Vol. 3, No. 3, pp. 1217–1223, 1988.