

I²CNERへの研究提案

時刻ずれと実際の水素損失の区別に関する、対象を限定したシミュレーション研究
— 2～3か月の短期研究滞在・1つの問い・1つのシステム・1件の報告書 —

時刻ずれ（時計の誤り）は、どの条件で実際の水素損失（漏えい）と区別できるか。時刻の不確かさを考慮する判定法は、誤警報率をそろえた場合に検知をどの程度改善するか。否定的な結果も結論として認める。

申請者	テオドル・ディモフ トラキア大学（ブルガリア、スタラ・ザゴラ）サイバーセキュリティ専攻 学生
受入れ希望先（協議中）	九州大学 カーボンニュートラル・エネルギー国際研究所 (I ² CNER)、伊都キャンパス（福岡市）
形式と期間	短期研究滞在、2～3か月。滞在中に約束するのは対象を限定したシミュレーション研究1件（8週間または12週間の計画、提案書 第6章）。実験は受入れ先との協議により実施を検討する発展課題
ステータス	計画中・調整中（未確定）。v1.4（2026年10月21日）

目次

第I部 研究提案（要旨、研究課題、方法、予備結果と限界、先行研究、作業計画〔8週間・12週間〕、お願い
したいご支援、参考文献、付録A～C、付記：水素レジリエンス観測室）

第II部 プロジェクト文書全文（長期的な研究プログラムの構想・以前の版）：水素インフラのサイバーリス
クとレジリエンス（1～10、出典90件）

版：v1.4（2026年10月21日）。研究滞在は計画中・調整中であり、確定したものではありません。本サイトは提案者による研究構想の紹介であり、九州大学またはI²CNERの公式見解、承認済みの共同研究、支援の決定を示すものではありません。

1. 要旨

水素ステーション（HRS）の漏えい検知は、流量・圧力・温度の計測値と、その時刻情報に依存しています。流出側の時計がずれると、充填流量の立ち上がり・立ち下がりの間に質量収支の残差が生じ、実際の漏えいと区別しにくくなります。本提案は、2〜3か月の短期研究滞在で、**1つの問い・1つのシステム・1件の報告書**に限定した、**対象を限定したシミュレーション研究**です。

対象は、蓄圧器からディスペンサーまでの1つの供給区間とその計測・判定ロジックです。公開した再現可能なベンチマーク（v1.4：ラインインベントリ込みの質量収支、模擬漏えい、誤警報率をそろえた比較）を出発点とし、受入れ先の専門家に前提を確認いただいた上で、時刻ずれと漏えいがどの条件で区別できるかを評価します。主要成果物は、コード・データ・不確かさの分析を含む技術報告書1件です。利用できる計測では区別できない、という否定的な結果も結論として認めます。

実設備への接続や試験は行いません。ガス品質と値の固定に関する検討、および単セル試験などの実験は、受入れ先との協議により実施を検討する発展課題（付録A）として記載し、本計画には含めません。本提案は計画中・調整中（未確定）であり、受入れ、共同研究の合意、費用負担などが決定したことを示すものではありません。

本サイトにある G1〜G7 の広い構想（プロジェクト文書）は、長期的な研究プログラムの構想、または以前の版として位置付けます。今回ご提案するのは、本書（v1.4）の範囲のみです。

2. 研究課題

研究課題（1件）：時刻ずれ（時計の誤り）は、どの条件で実際の水素損失（漏えい）と区別できるか。また、時刻の不確かさを考慮する判定法は、誤警報率を等しくそろえた場合に、検知をどの程度改善するか。

項目	内容
対象システム（1つ）	蓄圧器 → ディスペンサー配管の供給区間と、その流量・圧力・温度の計測および漏えい判定ロジック（シミュレーション）
主要成果物（1つ）	再現可能なベンチマークを拡張した技術報告書（コード、パラメータの根拠、不確かさの分析、失敗事例を含む）
本研究の貢献	時計の誤り・遅れて届くパケット・物理的な計器の遅れを区別し、漏えい検知の性能（見逃し、検知までの時間、損失質量、不要な停止）を誤警報率をそろえて定量化する、前提と限界を明示した評価手順
認める結論	区別できる条件の特定、または、利用できる計測では区別できないという否定的な結果
対象外	実設備・実車両への接続、特定製品の脆弱性、攻撃手順の詳細、事業者の機密データ

3. 方法

- **物理モデル：**配管内の保有量（ラインインベントリ）を含む質量収支 R_W を、配管容積 V 、圧力 P 、温度 T と実在気体の密度式（Abel-Noble 式、NIST の値との差は約1%以内）で表します^{[88][89][90]}。流量計・温度計の応答遅れ（一次遅れ）を含めます。
- **時刻の不具合の区別：**時計の誤り（オフセット・ドリフト）、遅れて届くパケット（タイムスタンプは正しい）、物理的な計器の遅れを別々にモデル化します。正・負のオフセット、ドリフト、ジッター、通常の故障（計測値の固定、計量器の誤差の段階変化）も扱います。

- **判定法**：流量のみの単純な基準（A0）、インベントリ補正（A）、時刻の不確かさの上限を考慮する判定（B）を比較します。しきい値は、別の乱数の種・別のステーションの漏えいのない充填で、誤警報率が同じ値（例：1%）になるよう**事前に**較正します。計量器の誤差は計器ごとに固定し、同じステーションの充填間で変えません。
- **評価指標**：模擬漏えいを注入し、見逃し、検知までの時間、損失質量、不要な停止（漏えい開始前の停止を含む）を、誤警報率をそろえて比較します。検知確率と誤警報率の関係（ROC）も示します。
- **区別可能性マップ（仮説・方法）**：漏えいの大きさ × 時刻ずれの格子で、各充填を「漏えい」「漏えいなし」「情報不足」に分類し、圧力・温度や独立した時刻参照を加えると何がかわるかを示します。
- **受入れ先が条件を定めるブラインドテスト（計画）**：判定アルゴリズムとしきい値を凍結し（コードのハッシュ値を記録）、受入れ先が提案者に知らせずに設定した充填プロファイル（漏えいの有無・大きさ・開始時刻、時刻ずれ、故障）で評価します。各手法を、事前に較正した等しい誤警報率で比較し、失敗した条件も含めてすべて報告します。実施の可否と担当者は受入れ先と協議します。
- **不確かさ**：Wilson の95%信頼区間は有限回の試行による統計的な不確かさのみを表し、モデルの誤りは含みません。感度分析（1因子ずつ、OFAT）は因子間の相互作用を評価しないため、主要な組合せを追加で確認します。
- **再現性**：乱数の種、パラメータ、コード、期待される出力を公開し、Python版とJavaScript版で同一の結果が得られることを確認します（v1.4で確認済み）。

4. 予備結果（例示モデル）と限界

公開したベンチマーク v1.4 の結果です（各条件400回の充填、50ステーション、すべての手法を誤警報率1%以下に事前較正）。実設備の性能を示すものではなく、研究の出発点として位置付けます。

- **時刻ずれなし**：誤警報は A0・A 0.75%、B 0%。2%の漏えいの検知は A 280/400、時刻の不確かさを考慮する B2 は 66/400 で、時刻ずれがなければインベントリ補正（A）が最も良い結果でした。誤警報率1%での検知確率（ROC）は、2%漏えいで A 70.8%、B2 16.5%、5%漏えいで A 100%、B2 80.8%。
- **時刻ずれあり**：+0.1 s で A の誤警報は 77%、B2 は 0%。+0.3 s では A は 400回中386回で漏えい開始前に停止し（不要な停止）、B2 は 5%の漏えいを 318/400 検知しました。
- **区別できない条件**：宣言した上限を超えるずれ（0.5 s 以上）、ドリフト、物理的な計器の遅れ（時定数 1.0 s）では、どの手法も誤警報がほぼ100%で、流量だけでは時刻ずれと区別できませんでした。圧力計の値の固定では、インベントリ補正を使う手法の誤警報が 97~100%に増えます。
- **区別可能性マップ**：流量のみでは漏えいがなくても 10~23%が「漏えい」と判定され、圧力・温度を加えると 0.2 s 以上の時刻ずれはほぼ常に識別されましたが、漏えいのない充填の 3~15%は依然として「漏えい」と判定されました。独立した時刻参照の追加効果は、この例示モデルでは小さい結果でした。
- **流量の大きさは打ち消し合うか**：厳密には打ち消し合いません（インベントリ項と絶対雑音が流量に比例しないため）。ただし、影響は小さい結果でした。
- **限界**：計量器の最大許容誤差 1.5%は OIML R 139-1 のクラス2の計量器の値で、計量システム全体では検定時 2%、使用中検査時 3%です^[76]（感度分析で使用）。誤差と雑音の分布は本モデルの仮定です。出典 [65] は電力系統における時刻同期攻撃の研究であり、水素設備で 0.2 s などの閾値を示すものではありません。時刻ずれの値はシナリオとして与えたものです。

5. 先行研究との比較と根拠

文献	対象	主な内容	本研究で加える点
^[20] Touhiduzzaman ほか (PNNL/Sandia, 2024)	大規模水素貯蔵	サイバーリスク評価	1つの計測・判定ロジックについて、時刻の不確かさを検知性能として定量化する
^[21] Rivera・Koleva (NREL, 2025)	水素長期貯蔵の実証設備	脅威の経路とシナリオ	シナリオの1つ（時刻の不具合）を、再現可能な数値評価に落とし込む
^[23] IEEE SPIES 2024	交通・電力系統と統合された HRS	DoS 攻撃の影響	通信の遮断ではなく、時刻情報の誤りによる誤判定を扱う
^[24] IEEE T-ITS 2025	配電系統と統合された電解式 HRS	偽データ注入に対する実行可能領域の推定	偽のデータではなく、本物の計測値に付いた誤った時刻を扱う
^[25] IEEE PES GM 2025	水素インフラ	サイバー脅威に対する感受性の評価	設備単位の評価を、充填ごとの検知性能（誤警報率をそろえた比較）で補う
^[65] Han・Crossley (IEEE PES GM 2019)	電力系統 (IEEE 1588)	時刻同期攻撃の脆弱性	時刻誤差の影響を水素の質量収支に適用する（閾値は引き継がない）

- **計測と充填：** 軽量車両の充填の最大流量は 60 g/s です^[74]。充填プロファイルの前提は SAE J2601 と公開資料に基づきます^{[73][75]}。
- **実在気体の密度：** NIST Chemistry WebBook（Leachman ほかの状態方程式）を基準とし、Abel–Noble 式との差を確認しました^{[88][89][90]}。

6. 作業計画

報告書を第8週に完成させる **8週間の計画** と、同じ問いをより丁寧に検証する **12週間の計画** を示します。どちらも主要成果物は技術報告書1件です。

8週間の計画（報告書は第8週）

期間	作業	成果・判断点
着任前	受入れ条件、指導体制、データと公表のルール、安全教育の確認	滞在計画
第1週	前提の確認（対象区間、計測構成、パラメータの範囲）、ベンチマーク v1.4 の再現	前提の記録
第2～3週	前提に合わせたモデルの修正、時刻の不具合と通常の故障の注入	コードと検証用テスト
第4週	判定アルゴリズムとしきい値の凍結（等しい誤警報率で事前校正）	凍結版（ハッシュ値を記録）
第5週	受入れ先が条件を定めるブラインドテスト	ブラインドテストの結果（失敗を含む）
第6週	区別可能性マップ、感度分析、失敗事例の整理	不確かさの報告
第7週	執筆	報告書の草稿
第8週	修正とセミナー	主要成果物：技術報告書、セミナー資料

12週間の計画

期間	作業	成果・判断点
着任前	受入れ条件、指導体制、データと公表のルール、安全教育の確認	滞在計画

期間	作業	成果・判断点
第1～2週	前提の確認とベースラインの再現	前提の記録、再現結果
第3～5週	モデルの修正（計器の動特性、ジッター、通常の故障）、判定法の実装	コードと検証用テスト
第6週	判定アルゴリズムとしきい値の凍結	凍結版（ハッシュ値を記録）
第7～8週	受入れ先が条件を定めるブラインドテスト	ブラインドテストの結果（失敗を含む）
第9～10週	区別可能性マップ、感度分析（主要な組合せを含む）、失敗事例	不確かさの報告
第11～12週	執筆、修正、セミナー	主要成果物：技術報告書、セミナー資料

論文：学術誌または国際会議への投稿は、結果が十分な場合に限り、受入れ先と協議の上で判断します（条件付き）。

- **提案者の役割：** モデルとコードの実装、ベンチマークの拡張、時刻の不具合と脅威の整理、結果の文書化（サイバーセキュリティの側面を担当）。NIS2指令とブルガリアのサイバーセキュリティ法を日本の制度と比較する視点も提供できます。
- **データの必要性：** 公開資料と合成データで実施できます。受入れ先が公開可能な範囲で、充填プロファイルや計量器の仕様に関する一般的な情報を共有いただける場合は、前提の妥当性を高めるために使用します。事業者の機密データは扱いません。

7. お願いしたいご支援

石原所長ご自身に、水素ステーションの計量についてのご専門を前提とするものではありません。お願いしたいのは次の点です。

- **前提の確認：** 計測構成、充填プロファイル、計器の応答時間、配管容積の範囲について確認いただける研究者（所内、または所外の専門家）のご紹介。
- **ブラインドテスト：** 提案者に知らせずに評価条件を設定いただける担当者（研究室の学生・研究員でも可）。
- **報告書の確認：** 公表前に、前提と結論の書き方について確認いただくこと。
- **滞在の条件：** 受入れ上の身分、指導体制、期間についてのご相談。

8. 参考文献

本提案で引用した番号は、プロジェクト文書の出典一覧（全90件、「前提・限界・参考資料」に掲載）に対応します。90件は独立した90の証拠ではありません。同じ機関・同じ規格・同じ研究グループによる資料や、背景説明のための資料を含みます。

- サイバーリスクと先行研究：[\[20\]\[21\]\[23\]\[24\]\[25\]](#)
- 時刻同期：[\[65\]](#)
- 計測と充填：[\[70\]\[71\]\[72\]\[73\]\[74\]\[75\]\[76\]](#)
- 実在気体の密度：[\[88\]\[89\]\[90\]](#)
- 品質と試料採取（付録A）：[\[66\]\[67\]\[68\]\[69\]](#)
- PEM形水電解の透過（付録A）：[\[86\]\[87\]](#)
- 材料と水素脆化（観測室の水素脆化レイヤー）：[\[50\]\[81\]\[82\]\[83\]\[84\]\[85\]](#)
- 供給回復時の配分（研究シナリオ）：[\[77\]\[78\]\[79\]\[80\]](#)

付録A 受入れ先との協議により実施を検討する発展課題

以下は本計画（第6章）には含めません。受入れ先との協議により実施を検討する発展課題であり、試験装置、分析計、試験範囲は現時点で決定したものではありません。新たな発見を主張するものでもありません。

A1. ガス品質と値の固定（シミュレーション）：「値の固定」を次の2つに分けて扱います。(1) **表示画面の値の固定**：画面に表示される値だけが固定され、判定処理には実際の計測値が入力される場合。運転員の判断には影響しますが、自動判定には影響しません。(2) **判定処理に入力される計測値の固定**：判定処理そのものが固定された値を使う場合。自動判定の見逃しや誤警報に直接影響します。ベンチマーク v1.4 は (2) を通常の故障として含みます（流量計・圧力計）。品質の判定では、試料の代表性も前提となります^{[66][67][68][69]}。

A2. PEM形水電解の単セル試験（実験）：電流密度と差圧の組合せにより水素の透過が変化する一方で、判定処理に入力される分析計の値が固定された場合に、独立した参照測定がその不一致をどの程度の時間で検知できるかを検討します。SOECを対象とする場合は、仕組みと運転条件が異なるため、別の前提として扱います。

- **透過量と濃度の区別**：水素の透過量（絶対量）は電流密度と圧力とともに増加すると報告されています^[86]^[87]。一方、酸素中の水素濃度は、酸素の生成量が少ない低電流密度で高くなります。Bernt ほかは、低電流密度では陽極側で爆発性の混合気が生じ得るため、追加の対策が必要であると報告しています^[87]。
- **安全**：試験範囲（特に低電流密度・高差圧の条件）と停止条件は、受入れ先の安全基準と安全審査に従って定めます。

段階	主な活動	受入れ先と確認する事項
準備	文献の整理、試験装置と分析計の確認、安全審査	使用できるセル、分析計の種類、安全手順
基準測定	主分析計と独立した分析計による基準測定	電流密度・差圧の試験範囲、測定間隔
制御試験	主分析計の値を判定処理の入力で固定した条件で、電流と圧力を段階的に変える	安全上の上限値（陽極側の水素濃度を含む）、停止条件
試験後評価	電圧低下、インピーダンス、可能であれば顕微鏡観察	利用できる評価装置

付録B 研究仮説（観測室の例示シナリオ）

以下は、観測室の例示シナリオに対応する研究仮説です。いずれも検証前の仮説であり、実測値や事故事例を示すものではありません。

- **純度表示と物理条件の乖離**：判定処理に入力される分析計の値が固定され、正常範囲を示したまま、運転点が透過の増加しやすい領域に移動する条件があり得る（PEM形を前提）。独立した参照測定により、この不一致を早期に検知できるかを検証する（付録A2）。
- **圧力サイクルの操作**：圧力が警報範囲内に留まっても、サイクル数と振幅の増加は疲労の観点で別の評価を必要とし得る。水素ガス環境では鋼の疲労き裂進展が加速することが知られている^{[81][82]}。サイクル速度の制限や独立した計数が評価を支援できるかを検討する。観測室の疲労指標・き裂表示は例示であり、工学上の限界値や寿命を示すものではない。
- **液体水素のオルト・パラ転換**：通常の水素はオルト水素約75%、パラ水素約25%からなり、液化時に転換が完了しない場合、転換に伴う発熱が輸送・貯蔵中の気化要因になり得る^{[61][62]}。サイバー事象との因果関係は研究仮説として扱う。
- **本物の測定値によるデジタルツインの汚染**：本物の観測の削除と複製によってベイズ推論の結果を誘導できることが示されている^{[63][64]}。水素研究のモデルにどの程度当てはまるかは、対象ごとに検証が必要である。

- **時刻のずれによる質量収支の誤判定：** 流出側の時刻ずれ δ による残差の誤差は、一次近似で δ と流量の変化率の積として現れる。本提案の研究課題であり、再現可能なベンチマーク（v1.4）で予備的に評価した（ただし、ラインインベントリと計器の遅れを含めると一次近似だけでは説明できない）。
- **本物の測定、代表性のない試料：** 採取ワークフローの記録が、分析結果の代表性の事後検証を支援できるかを検討する^{[66][67][68][69]}。意図的な操作の可能性は推測的である。
- **正しい部品、不適合な充填構成：** SAE J2799 と J2601 の版・設定の組合せをソフトウェアのみで網羅的に確認するテストベンチの有用性を検討する^{[70][71][72][73]}。悪用可能性は推測的である。
- **供給は回復した——誰のために：** 供給回復時の配分規則と公平性の指標を、総供給量と併せて評価する^{[77][78][79][80]}。信頼や社会受容性への影響は推測的である。

付録C 安全・情報管理・協議事項

- 攻撃と対策はシミュレーション上でのみ検証します。実設備への接続、能動的な試験、運転条件の変更は本計画に含めません。
- 特定製品を標的とする 익스プロイトは作成せず、事業者の機密データは扱いません。公表前には受入れ先による確認を受け、責任ある開示を行います。
- 情報の持出し、公開範囲、知的財産の取扱いは、受入れ先の規程に従って協議します。参加者を伴う調査を行う場合は、九州大学の規程に基づく倫理審査を受けます。
- 協議事項：研究訪問の時期・期間、受入れ上の身分、指導体制、設備・情報へのアクセス、旅費・滞在費等の条件。エラスムス・プラス（Erasmus+）による資金支援の受給資格は未確認であり、トラキア大学の国際交流担当部署に確認します。日本の水素事業者が指定された重要インフラ分野に含まれるか否かは、滞在中に調査します。九州大学サイバーセキュリティセンターとの協力の可能性については、現時点で接触はありません。

まずは対象を限定した検討から始め、得られた知見をもとに、継続的な共同研究の可能性をご相談できれば幸いです。どうぞよろしくお願いいたします。

付記. 水素レジリエンス観測室（例示モデル）

本提案に付属するウェブサイトには、研究の考え方を説明するための例示モデル「水素レジリエンス観測室」を収録しています。1つの水素設備群（水素製造、圧縮・貯蔵、輸送、水素ステーション、燃料電池、制御システム）を、分割線の左側では基準構成（A）、右側では対策変更後（B）の状態で表示し、同じ初期状態・同じ事象列を共通の時間軸で比較します。

- シナリオと対策の対応は、文書 第4章の弱点（W1～W9）と第5章の対策（M1～M9）の対応表に従います。比較対照として、攻撃によらない故障のシナリオも含めています。
- サイバーセキュリティ上の状態、運転上の状態、安全上の評価状況を分けて扱います。隔離は修復を意味せず、監視だけでは侵害は除去されません。安全上の評価が「未評価」の場合、自動的な再起動は行いません。
- v1.3で追加：A/B観測室（1本の水素チェーンに同じ外乱を与え、モデル化した対策のない状態Aと対策のある状態Bを共通の時間軸で比較する例示）、水素脆化レイヤー（累積圧力変動指標に比例させた微小き裂の概念表示、例示）、再現可能なベンチマーク（時刻ずれのある質量収支、Python版・JavaScript版のコードを公開。v1.4でラインインベントリ、模擬漏えい、誤警報率をそろえた比較、ROC、区別可能性マップを追加）、新たな研究シナリオ3件（付録B）。研究仮説の一覧は付録Bを参照してください。
- 計器の値、運転点、クロスオーバー指標、疲労指標（工学上の限界値ではありません）、時間のステップ、比較結果はすべて例示です。実測値、発生確率、性能保証として扱うことはできません。計器値は状態を説明する

ための例示です。物質収支・熱収支を計算した結果ではありません。

前提と限界

本モデルは研究上の議論を支援するためのものであり、実設備を再現・検証したデジタルツインではありません。流体・熱・電気化学の詳細な挙動、設備ごとの保護機能、および実運用における人の判断は再現できません。物理的な安全性や対策の実効性については、専門家による検討と追加の検証が必要です。参考資料の確認日：2026年10月20日（出典61～90は10月21日）。

水素インフラのサイバーリスクとレジリエンス

1. 概要

水素は、日本および欧州連合（EU）の脱炭素戦略における主要なエネルギーキャリアである^{[41][53]}。水素サプライチェーン、すなわち水電解装置、圧縮機、高圧貯蔵設備、パイプライン、水素ステーション（HRS）、燃料電池、およびそれらと電力系統との接続は、制御技術（OT）によって運用されている。具体的には、産業制御システム（ICS）、SCADA、プログラマブルロジックコントローラ（PLC）、安全計装システム（SIS）である。これらのシステムのデジタル化が進み、ITネットワーク、ベンダー、系統運用者との接続が増えるほど、サイバー・フィジカルなリスクにさらされる度合いは高まる。

このテーマについては、すでに研究が進められている。2024年には米国のパシフィック・ノースウェスト国立研究所（PNNL）とサンディア国立研究所が大規模水素貯蔵のサイバーリスク評価を公表し^[20]、米国国立再生可能エネルギー研究所（NREL）は長期エネルギー貯蔵用の水素システム（水電解装置、貯蔵設備、燃料電池）に対する脅威を分析した^[21]。また、査読付き論文では、系統と連系したHRSに対するサービス妨害（DoS）攻撃および偽データ注入（FDI）攻撃がモデル化されている^{[23][24][25]}。しかし、技術的な脆弱性を安全性、経済性および社会の信頼への影響と結び付け、サプライチェーン全体を体系的に評価する研究は、依然として十分ではない。

本プロジェクトは、次の5点を提案する。(1) 水素サプライチェーンにおけるサイバー・フィジカルな弱点のマップ、(2) 安全面への影響を含むシナリオベースのリスク評価、(3) IEC 62443、NIST SP 800-82r3、NIST CSF 2.0、ISO/IEC 27001/27019、ならびに日本およびEUの規制に対応付けた防護対策の枠組み、(4) 模擬プロセスデータを用いた異常検知のプロトタイプ、(5) サイバーインシデントが水素技術への信頼と社会受容性にどのような影響を及ぼし得るかの分析。最後の点が、I²CNERのアンドリュー・チャップマン准教授の研究（エネルギー政策、水素社会のモデリング、社会受容性）との接点となる^{[3][6][7]}。

連絡の経緯。 提案者は、I²CNERのアンドリュー・チャップマン准教授と面談の機会をいただいた^{[3][4]}。受入れの可否、時期および条件は協議中である。

2. 目的

2.1. 全体目的

水素インフラのサイバーリスクとレジリエンスを評価する手法を開発し、シミュレーションのレベルで検証することを目的とする。本手法は、OT/ICSにおける技術的な脆弱性を、安全性、供給の継続性、経済性および社会の信頼への影響と結び付けるものでなければならない。

2.2. 具体的かつ測定可能な目標

番号	具体的目標	測定指標
G1	文献および規格の体系的レビュー	40件以上の出典からなる注釈付きカタログ（うち10件以上は水素に特化したもの）
G2	水素サプライチェーンの参照アーキテクチャ	サプライチェーンの4つ以上のセグメントを対象とした、ゾーンとコンジット（IEC 62443-3-2）のモデル
G3	攻撃シナリオのカタログ	MITRE ATT&CK for ICSの戦術に対応付けた10件以上のシナリオ（うち3件以上は、過圧、漏えい、SISの無効化といったサイバー・フィジカルな影響を伴うもの）

番号	具体的目標	測定指標
G4	防護対策マトリクス	IEC 62443-3-3、NIST SP 800-82r3、NIST CSF 2.0の各機能、ならびに日本およびEUの要件に対応付けた30項目以上の管理策
G5	異常検知のプロトタイプ	模擬データまたは公開データ上で動作するコード。適合率、再現率、F1値および検知時間を報告し、1つ以上のベースライン手法と比較する
G6	社会経済的側面（チャップマン准教授のグループとの共同）	「サイバーインシデント → 信頼 → 受容」の概念的枠組みと、将来の調査に向けた質問票・シナリオの案
G7	成果の発信	技術報告書1件、学術誌または国際会議向け論文原稿1件、I ² CNERでのセミナー1回

3. 対象範囲：水素サプライチェーン

セグメント	主な設備	主要なデジタル構成要素とインターフェース
製造	水電解装置（固体高分子形〔PEM〕、アルカリ形、固体酸化物形）、整流器、水処理設備	PLC、SCADA/HMI、電力量計、再生可能エネルギーおよび電力系統との接続 ^[21]
圧縮・貯蔵	圧縮機、バッファ容器および高压容器、大規模貯蔵設備	圧力・温度・漏えいセンサ、SIS、データヒストリアン ^{[20][21]}
パイプライン・輸送	パイプライン、チューブトレーラー、分配拠点	SCADA、遠隔監視制御装置（RTU）、テレメトリ、漏えい検知システム
水素ステーション（HRS）	ディスペンサー、プレクーラー、ステーション内蓄圧設備	ステーション制御装置、ステーションと車両間の通信、運営・決済システム、遠隔監視 ^{[22][23][51]}
燃料電池・系統連系	定置用燃料電池、マイクログリッド、非常用電源	エネルギー管理システム（EMS）、アグリゲーター、系統サービス用の信号 ^{[21][23][24]}

対象外： 書面による許可のない実設備での試験、特定製品を標的とするエクスプロイトの開発、および事業者の機密データの取り扱いの対象外とする。福岡で公開されている設備（6.3参照）は、背景情報としてのみ扱う。

4. サイバーセキュリティ上の弱点

4.1. 水素に特別な注意が必要な理由

水素システムは、高压、可燃性ガス、自動制御という3つの要素を併せ持つ。NRELの分析では、圧力、温度、純度および漏えいの計測機器が攻撃対象として挙げられており、偽の計測値によって過圧などの危険な状態が隠蔽されるおそれがある^[21]。PNNLとサンディア国立研究所は、水素貯蔵設備へのサイバー攻撃が、作業員、周辺住民および所有者に物理的・経済的損害をもたらし得ることを指摘し、イベントツリー解析を用いてシナリオを記述している^[20]。LUT大学のHYGCELプロジェクトは、水素関連の82件の事象を分析し、サプライチェーンにおける事故の多くが貯蔵および供給の段階で発生していることを明らかにした^[26]。これらは、デジタル監視が最も重要となるセグメントでもある。

4.2. 主な弱点

W1. OT/ICS/SCADA/PLCとIT/OTの融合 企業のITネットワークに侵入した攻撃者は、OTに向けて横展開（ラテラルムーブメント）を行い得る。米国のCISA、NSAおよびFBIは、Volt Typhoonと呼ばれるグループが、OT資産に到達する目的で、エネルギー分野を含む重要インフラのITネットワーク内にあらかじめ潜伏していると高い確度で評価している。一部の被害組織では、少なくとも5年間にわたりアクセスが維持されていた^[19]。

W2. 安全計装システム（SIS） SISは、過圧時の緊急停止など、最後の自動防護バリアである。マルウェア TRITON/TRISIS（HatMan）は、Triconex安全コントローラのファームウェアを改ざんする目的で作成された。その狙いは、プロセスの安全な停止を妨げることにある^{[13][14]}。

W3. リモートアクセスとベンダーアクセス 水電解装置、圧縮機およびHRSの遠隔保守は、恒常的な侵入口を生み出す。Volt Typhoonは、正規アカウント、RDPおよび環境寄生型（Living off the Land）の手法を用いる^[19]。NRELのシナリオには、水電解装置および貯蔵設備へのRDPのバックドアが含まれている^[21]。

W4. IIoTセンサ（漏えい、圧力、温度、流量） 圧力センサや漏えいセンサに対するデータ注入や信号妨害は、運転員や制御アルゴリズムを誤認させるおそれがある^[21]。水電解型HRSに関する研究では、やり取りされる運転パラメータに対するFDI攻撃が、技術面と経済面の双方に影響を及ぼすことが示されている^[24]。

W5. レガシープロトコルと設定不備のあるプロトコル 従来のModbusやDNP3には、認証および暗号化の機能が組み込まれていない。セキュアな派生方式（Secure Modbus/TLS、DNP3 Secure Authentication）を利用するには、意図的な導入が必要である^[28]。OPC UAを採用するだけでは安全性は保証されない。2020年のインターネット全体を対象とした調査では、インターネットから到達可能なOPC UA環境1,114件のうち92%に、セキュリティ機能の無効化や旧式の暗号方式といった設定上の不備が確認された^[27]。また、Industroyerは、IEC 60870-5-104などのプロトコルの正規機能を悪用し、変電所に制御コマンドを送信する^{[16][17][18]}。

W6. サプライチェーン 水電解装置、ステーション制御装置およびセンサには、多数のベンダーによるファームウェアとソフトウェアが組み込まれている。NRELは、水素システムにおける電力量計への脅威として、サプライチェーンの侵害を挙げている^[21]。ブルガリアのNIS2関連の新たな法制度では、EU域外の高リスクな技術およびサプライヤーを制限できる可能性が規定されている^[56]。

W7. HRSの運営と決済 HRSは、OT（ディスペンサー、冷却設備、蓄圧設備）を、予約、決済、遠隔監視などのITサービスと結び付けている。例えば、福岡市の水素ステーションは事前予約制とキャッシュレス決済で運営されている^[51]。米国エネルギー省（DOE）のHyRIGHTプロジェクトは、大型車両への水素充填時の通信における潜在的なサイバー脆弱性を研究上の課題として挙げている^[22]。DoS攻撃のモデルによれば、タンクの充填状態、需要、システムサービスなどの信号が遮断されると、ステーションの収益性が許容水準を下回るおそれがある^[23]。

W8. 電力系統・再生可能エネルギーとの連系 水電解装置やHRSは系統に柔軟性を提供し得るが、それに伴い電力システムのリスクも引き継ぐことになる。ウクライナの電力網に対する攻撃（Industroyer、2016年／Industroyer2、2022年）は、特化型マルウェアが開閉装置を直接操作し得ることを示している^{[16][18]}。EMSやアグリゲーターからの信号が改ざんされると、水素設備が最適でない、あるいは危険な状態で運転されるおそれがある^{[23][24][25]}。

W9. サイバー・フィジカルな影響 最も深刻なシナリオは、制御の操作（例：圧力設定値や圧縮機の運転の改ざん）、監視の無力化（偽のセンサデータ）およびSISの無効化を組み合わせたものである。その結果、過圧、漏えい、さらには火災や爆発のリスクが生じ得る^{[20][21]}。物理的な損傷がなくても、ITインシデントによって操業が停止することがある。Colonial Pipelineの事例がそれに当たる（4.3参照）。

4.3. 記録されたインシデントと研究

インシデント／研究	記録されている内容	水素インフラへの教訓
Colonial Pipeline （米国、2021年5月）	ITネットワークにおけるランサムウェアDarkSideの感染。2021年5月7日、同社は予防措置としてパイプライン全体の運用を停止し、5月13日にシステムを再稼働した ^{[10][11][12]}	ITインシデントが物理的な供給を停止させ得る。ネットワーク分離、手動運転計画および復旧計画が必要である

インシデント／研究	記録されている内容	水素インフラへの教訓
TRITON/TRISIS (中東、2017年)	Triconex SISを標的としたマルウェア。CISAによれば、この攻撃により製油所が数日間停止し、攻撃者はロシアの研究機関TsNIIKhMと関連付けられている ^{[13][14]} 。Schneider Electricは、コントローラのキースイッチが正しい位置（「PROGRAM」以外）にあれば不正なプログラムの注入は成功しなかったであろうと指摘している ^[15]	水素設備のSISには、ネットワークからの隔離、プログラミングモードの物理的な管理、および安全とセキュリティの協調設計が求められる
Industroyer/CrashOverride（ウクライナ、2016年）およびIndustroyer2（2022年）	IEC 101/104、IEC 61850およびOPC DAに対応した、ICS攻撃用のモジュール型プラットフォームであり、電力網への攻撃に使用された ^[16] ^[17] 。2022年には、IEC-104のみに対応した派生型がウクライナのエネルギー分野のOTを標的とした ^[18]	サイバー脅威が想定される以前に設計されたプロトコルでは、「正規の」悪意あるコマンドが通ってしまう。系統と連系したHRSや水電解装置にも関係する
Volt Typhoon（共同勧告AA24-038A、2024年2月）	重要インフラ（通信、エネルギー、運輸、上下水道）への事前潜伏。ベンダーの初期パスワードを用いたOTへのアクセス試行 ^[19]	新たな水素事業者においても、多要素認証（MFA）、ログの一元管理および脅威ハンティングが必要である
水素に特化した分析	PNNL／サンディア国立研究所：大規模水素貯蔵のサイバーリスク評価 ^[20] 、NREL：H2 LDESに対する脅威ベクトル ^[21] 、DOE HyRIGHT ^[22] 、HRSに関する論文 ^{[23][24][25]} 、LUT HYGCEL ^[26]	本プロジェクトにおける参照アーキテクチャおよびシナリオの基礎となる

注：本文書の作成にあたって調査した範囲では、水素設備そのものを標的とし、公に記録されたサイバーインシデントは確認されなかった。上記の水素に特化した出典は、リスク分析およびシミュレーション研究であり、実際の攻撃の報告ではない。

5. 防護対策

番号	対策	主な枠組みと出典	対応する弱点
M1	リスクガバナンス 方針、役割、リスク評価、サプライヤー管理	新たにGovern（統治）機能が加わったNIST CSF 2.0 ^[30] 、ISO/IEC 27001に基づく情報セキュリティマネジメントシステム ^[33] 、およびISO/IEC 27019:2024のエネルギー分野固有の管理策（プロセス制御システム、レガシーシステム、安全機能の可用性に関するものを含む） ^[32]	W1–W9
M2	IEC 62443：ゾーン、コンジット、セキュリティレベル システムのゾーンとコンジットへの分割、目標セキュリティレベル（SL 0～4）の設定、62443-3-2に基づくリスク評価、62443-3-3に基づくシステム要件	ISA/IEC 62443 ^[31]	W1, W3, W5, W6
M3	Purdueモデルに基づくネットワーク分離と産業用DMZ IT⇔OT間の通信の厳格な制御、SIS専用ネットワークの分離	NIST SP 800-82r3 ^[29] 、日本も支持するOTサイバーセキュリティの原則 ^[37]	W1, W2, W8
M4	セキュアリモートアクセス 踏み台サーバ、フィッシング耐性のあるMFA、ベンダー向けのオンデマンドかつ時間制限付きのアクセス、セッションの記録	CISA AA24-038A ^[19] 、NIST SP 800-82r3 ^[29]	W3
M5	プロトコルの堅牢化 DNP3 Secure Authentication、Secure Modbus/TLS、署名と暗号化（SignAndEncrypt）を有効にしたOPC UA、証明書管理	RADIANCE ^[28] 、Dahlmannsら ^[27]	W5

番号	対策	主な枠組みと出典	対応する弱点
M6	監視と異常検知（プロセスデータへの機械学習の適用） OTネットワークの監視、物理的な妥当性チェック（例：圧力・温度・流量の整合性）、FDI検知モデル	ENISA：エネルギー事業者の32%は、重要なOTプロセスを1つもSOCで監視していない ^[57] 、HRSにおけるFDI検知 ^[24] 、ICSのテストベッドとデータセット ^[39]	W1, W4, W8
M7	サプライチェーンとSBOM ソフトウェア部品表（SBOM）、署名付きファームウェア、サプライヤー契約におけるセキュリティ要件	NTIA：SBOMの最小要素 ^[38] 、「サプライチェーンを保護する」原則 ^[37] 、IEC 62443 ^[31]	W6
M8	インシデント対応と復旧 OTに特化した対応シナリオ、オフラインバックアップ、手動による安全運転の確保、演習	Colonial Pipelineの教訓 ^{[10][11]} 、NIS2指令およびブルガリアのサイバーセキュリティ法に基づく報告義務（24時間／72時間） ^[56] 、日本の能動的サイバー防御に関する法律（サイバー対処能力強化法） ^{[45][46]}	W1, W7, W9
M9	安全とセキュリティの協調設計 SISのセキュリティリスク評価、CyberPHA、サイバー・インフォームド・エンジニアリング	IEC 61511-1:2016の8.2.4項はSISのセキュリティリスク評価を求めている ^{[35][36]} 、ISA-TR84.00.09-2024はサイバーセキュリティを安全ライフサイクルに統合している ^[34] 、DOEのサイバー・インフォームド・エンジニアリング国家戦略 ^[40] 、TRITONの教訓 ^[15]	W2, W9
M10	デジタルツインとテストベッドによる検証 攻撃と対策はシミュレーション上でのみ検証し、稼働中のシステムでは決して行わない	ICSのテストベッドとデータセットに関するサーベイ ^[39] 、NRELのH2 LDESシミュレーションモデル ^[21]	W1-W9

6. 日本および国際的な背景

6.1. 日本の水素政策

- **水素基本戦略（2023年6月6日改定）** 水素（アンモニアを含む）の導入量を、2030年に年300万トン、2040年に年1,200万トン程度、2050年に年2,000万トン程度とすることを目標としている。2030年までに、日本企業による水電解装置の導入を15GW程度とすることを目指し、15年間で官民合わせて15兆円を超えるサプライチェーン投資を見込んでいる^[41]。
- **水素社会推進法** 正式名称は「脱炭素成長型経済構造への円滑な移行のための低炭素水素等の供給及び利用の促進に関する法律」（令和6年法律第37号）であり、2024年5月24日に公布され、同年10月23日に施行された^[42]。同法により事業計画の認定制度が導入され、独立行政法人エネルギー・金属鉱物資源機構（JOGMEC）を通じて、既存燃料との価格差に着目した支援と拠点整備支援が行われる^[43]。
- **第7次エネルギー基本計画（日本語版で追加）** 2025年2月18日に閣議決定された^[59]。

6.2. ICSおよび重要インフラに関する日本のサイバーセキュリティ

- **経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」（英語版1.1）** 産業制御システムを対象とし、資産およびゾーンの分析、対策の立案、継続的な見直しという手順に沿って構成されている^[44]。
- **能動的サイバー防御に関する法律** 「重要電子計算機に対する不正な行為による被害の防止に関する法律」（令和7年法律第42号。通称：サイバー対処能力強化法）であり、2025年5月23日に公布された^[45]。内閣府による2026年10月1日付の解説によれば、指定された重要インフラ事業者（特別社会基盤事業者）は、重要な電子計算機を届け出るとともに、一定のインシデントを報告しなければならない^[46]。

- **国家サイバー統括室（NCO）** 2025年7月、内閣サイバーセキュリティセンター（NISC）を改組して設置された。「重要インフラのサイバーセキュリティ対策のための統一基準」は2026年10月1日に施行され、「重要インフラのサイバーセキュリティに係る行動計画」を補完するものとなっている^[47]。
- **本プロジェクトにおける未解決の論点：** 水素事業者が日本の重要インフラ分野に含まれるか否か、また含まれる場合にどのような形で含まれるか（例：「ガス」分野や「電力」分野を通じて）。この点は未確認であり、滞在中に調査する予定である。

6.3. 福岡市および九州大学における水素の取り組み

- **九州大学の水素ステーション（伊都キャンパス）** 九州電力と共同で実施されているNEDO（国立研究開発法人新エネルギー・産業技術総合開発機構）の事業の一部である。ゼロエミッション電源の電力を用いて水素を製造しており、2023年11月15日からは、九州初の大型燃料電池バスが伊都キャンパスとJR九大学研都市駅の間で乗客を運んでいる。運行は2025年度までの予定とされている^{[48][49]}。
- **サステナブル水素研究所（HYDROGENIUS）** 2026年4月1日、次世代燃料電池産学連携研究センターを含む学内の水素関連3センターを統合して設立された。I²CNERとの緊密な連携が予定されている^[50]。
- **福岡市「水素リーダー都市プロジェクト」** 福岡市は2015年、中部水処理センターにおいて、下水バイオガスから水素を製造する世界初の水素ステーションを開設した。同ステーションは2022年に商用ステーションとしてリニューアルされ、九州大学はその運営を担う協議会のパートナーとなっている。さらに同市は、九州大学箱崎キャンパス跡地において、水素供給パイプラインを備えた水素ステーションの整備も計画している^{[51][52]}。
- **キャンパスにおけるサイバーセキュリティの専門性** 九州大学サイバーセキュリティセンターも伊都キャンパスに所在する^[9]。同センターとの協力の可能性は今後検討する予定であり、現時点で接触はない。
- **水素エネルギー製品研究試験センター（HyTReC）（日本語版で追加）** 福岡水素戦略（Hy-Lifeプロジェクト）の一環として、福岡県が中心となって設立した公益財団法人である。水素ガス環境下で使用するバルブやセンサなど、水素関連製品の耐久試験や圧力サイクル試験を行っている^[60]。地域の研究・試験基盤を理解するための背景として参照するものであり、同センターとの接触や連携はない。

6.4. I²CNERおよびチャップマン准教授の研究との適合性

I²CNERは、2010年から世界トップレベル研究拠点プログラム（WPI）の拠点であり、2020年からはWPIアカデミーの一員である。水素の製造と利用、ならびに再生可能エネルギーを基盤とする社会システムの設計に取り組んでいる^{[1][58]}。チャップマン准教授は、エネルギー経済・政策、エネルギーシステム分析、および持続可能性の総合的評価を専門とする^[3]。主な業績には、将来のエネルギーシステムにおける水素普及の可能性を評価した4つの事例研究のレビュー^[6]、日本を対象とした「電化か水素か」の戦略分析^[7]、デジタル経済とエネルギー安全保障に関する研究^[8]がある。また、2026～2029年度の科学研究費助成事業（基盤研究(B)）「Energy system design for a green hydrogen circular economy」の研究代表者を務め^[5]、エネルギーシステムの設計に機械学習を応用している^[3]。

チャップマン准教授の研究分野はエネルギー政策、エネルギーシステム分析および社会的受容性であり、サイバーセキュリティの側面は提案者が担う。両分野の接点は、**サイバーインシデントが水素インフラに対する信頼、安全性、経済性および受容性にどのような影響を及ぼすか**という問いにある。技術的なサイバーシナリオ（例：HRSにおける偽の漏えいデータ）は、リスク認知、コスト、導入のペースへの影響として捉え直すことができる。こうした影響は、水素社会のモデルに組み込むことが可能である。

6.5. EUおよびブルガリアの状況

- **EU水素戦略（COM(2020) 301）** 再生可能水素向けの水電解装置を2024年までに少なくとも6GW、2030年までに40GW導入し、再生可能水素を最大1,000万トン生産することを目標としている^[53]。

- **NIS2指令（EU）2022/2555** 附属書Iの「エネルギー」部門において、「水素」サブセクターは水素の製造、貯蔵および輸送を行う事業者を対象としている^[54]。**ブルガリア**は、サイバーセキュリティ法の改正法（官報第17号、2026年2月13日）によりNIS2指令を国内法化し、水素事業者を明示的に対象に含めた^[55]。重大なインシデントは24時間以内に通知し、72時間以内に続報を提出しなければならない^[56]。
- **ENISA（欧州連合サイバーセキュリティ庁）** 2024年のサイバー演習「Cyber Europe 2024」はエネルギー分野をテーマとした。ENISAはまた、エネルギー分野の事業者の32%が、重要なOTプロセスを1つもSOCで監視していないと報告している^[57]。
- **資金：** エラスムス・プラス（Erasmus+）による資金支援（例：実習を目的とするモビリティ）の可能性については、トラキア大学の国際交流担当部署に確認する必要がある。受給資格は未確認である。

7. 研究方法と作業パッケージ（構想）

研究方法： 体系的レビュー、アーキテクチャのモデリング（IEC 62443-3-2、ゾーンとコンジット）、NRELの手法に倣ったMITRE ATT&CK for ICSおよびサイバーキルチェーンによる脅威モデリング^[21]、イベントツリー^[20]およびCyberPHA^[36]による影響評価、合成データまたは公開データを用いたシミュレーションと機械学習^[39]、チャップマン准教授のグループと共同で行う社会経済的影響の概念モデリング。

作業計画： 日程は、提案書 第5章の12週間計画（第1～2週：前提の合意とベースラインの再現、第3～6週：実装、第7～8週：不確かさと失敗事例の分析、第9～12週：改良と執筆）に一本化した。滞在中に約束する成果は、1つの研究課題・1つの対象システム・1つの主要成果物（シミュレーション研究と技術報告書）である。以下の作業パッケージは、滞在中も含むプロジェクト全体の構想であり、滞在中の約束ではない。

- **WP0（着任前）：** 条件、指導体制、データおよび公表に関するルールの調整、安全教育。
- **WP1：** 文献および規格のレビュー、サプライチェーンの参照アーキテクチャ（ゾーン／コンジット）。
- **WP2：** 脅威モデリング、シナリオの作成、発生可能性と影響の評価。
- **WP3：** シミュレーションモデルの構築と異常検知（滞在中のシミュレーション研究の中心）。
- **WP4：** 対策マトリクスと、IEC 62443、NIST、経済産業省ガイドライン、NIS2指令／ブルガリアのサイバーセキュリティ法への対応付け。
- **WP5：** 「サイバーインシデント → 信頼 → 受容 → 経済」の概念的枠組み（合意が得られた場合は共同で実施）。
- **WP6：** 総括、セミナー、論文原稿（結果に応じた条件付き）。

期間： 滞在中は2～3か月を想定し、提案書 第6章に8週間の計画（報告書は第8週）と12週間の計画を示す。単セル試験、分析計による測定、試験後の特性評価などの実験は、受入れ先との協議により実施を検討する発展課題として提案書の付録Aに記載し、本計画には含まない。

8. 期待される成果と発表

1. 水素サプライチェーンにおける参照アーキテクチャと、サイバー・フィジカルな弱点のカタログ（D1、D2）。
2. IEC 62443、NIST SP 800-82r3、NIST CSF 2.0、ISO/IEC 27019、経済産業省ガイドライン、NIS2指令およびブルガリアのサイバーセキュリティ法に対応付けた対策マトリクス（D4）。日本およびEUの事業者が活用できるものとする。
3. 模擬データを用いた、オープンな異常検知プロトタイプ（D3）。攻撃に悪用され得る詳細は公開しない。
4. サイバーセキュリティと水素の社会受容性との関係を扱う学際的な枠組み（D5）。
5. 発表（結果に応じた条件付き）：

- 水素エネルギーまたはエネルギー政策分野の学術誌への論文投稿（例：チャップマン准教授のグループも論文を発表しているInternational Journal of Hydrogen Energy^{[6][7]}）
- および／または電力システム分野のIEEE国際会議での発表（例：関連研究が発表されたIEEE PES General Meeting^[25]）

著者構成は、受入れ先のグループと協議のうえ決定する。

6. I²CNERでのセミナーおよびトラキア大学での成果報告。将来の学位論文および継続的な共同研究の基盤とする。

9. リスクとその軽減策

リスク	発生可能性	軽減策
滞在が確定しない、または延期される（条件、ビザ、資金）	中	条件の早期確認、WP1～WP2の遠隔実施の検討、代替となる資金源の確保
実データや実システムにアクセスできない	高	シミュレーションモデルと公開データセットを用いる。実システムでの試験は行わない
成果の機微性（デュアルユース）	中	汎用的なアーキテクチャを用いる。特定製品を標的とするエクスプロイトは作成しない。公表前に受入れ先による確認を受け、責任ある開示を行う
学際的な隔たり（サイバーセキュリティ ↔ エネルギー政策）	中	WP5における明確な役割分担、定期的な打ち合わせ、学内のサイバーセキュリティ専門家の協力の検討（今後確認）
3か月に対して対象範囲が広すぎる	中	HRSおよび水電解装置・貯蔵設備を優先し、その他のセグメントはより概括的なレベルで扱う
一部の出典が日本語のみで提供されている	中	公式の英語版がある場合はそれを用い、受入れ先のグループの協力を得る
参加者を伴う調査に関する倫理上の要件	低～中	九州大学の規程に基づく承認を得た後にのみ調査を実施する

10. 出典

1. Kyushu University, I²CNER — About. <https://i2cner.kyushu-u.ac.jp/en/about/>
2. I²CNER — “Prof. Tatsumi Ishihara appointed as the New Director of I²CNER”. <https://i2cner.kyushu-u.ac.jp/news/9468/>
3. Kyushu University Faculty Profiles — Chapman John Andrew (Associate Professor, I²CNER). https://hyoka.ofc.kyushu-u.ac.jp/html/100025407_en.html
4. Chapman Lab. <https://chapman-lab.com/>
5. KAKEN — Chapman Andrew; “Energy system design for a green hydrogen circular economy”, Grant-in-Aid for Scientific Research (B), FY2026–2029. <https://nrid.nii.ac.jp/en/nrid/1000060795293/>
6. Chapman A. et al. (2019). A review of four case studies assessing the potential for hydrogen penetration of the future energy system. *International Journal of Hydrogen Energy*, 44. <https://doi.org/10.1016/j.ijhydene.2019.01.168>
7. Karmaker S.C., Chapman A.J., Sen K.K., Saha B.B. (2026). Electrification or Hydrogen? A strategic pathway for Japan's energy transition. *International Journal of Hydrogen Energy*, 201. <https://doi.org/10.1016/j.ijhydene.2025.152989>
8. Sen K.K., Karmaker S.C., Chapman A.J., Saha B.B. (2025). Digital economy in reducing energy inequality and enhancing energy security for environmental sustainability. *Journal of Cleaner Production*, 522. <https://doi.org/10.1016/j.jclepro.2025.146344>
9. Cybersecurity Center, Kyushu University — Access. <https://cs.kyushu-u.ac.jp/en/access/>
10. U.S. DOE CESER — Colonial Pipeline Cyber Incident. <https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>
11. Testimony of Joseph Blount, CEO Colonial Pipeline, U.S. Senate HSGAC, 8 June 2021. <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Blount-2021-06-08.pdf>
12. CISA/FBI — AA21-131A: DarkSide Ransomware. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a>

13. CISA — MAR-17-352-01 HatMan: Safety System Targeted Malware (Update B), 2019. <https://www.cisa.gov/sites/default/files/document%20s/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf>
14. CISA — AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a>
15. Schneider Electric — Security Notification SEVD-2017-347-01, EcoStruxure Triconex Tricon V3. https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2017-347-01&p_File_Name=SEVD-2017-347-01+Triconex+V3.pdf&p_enDocType=Technical+leaflet
16. CISA — CrashOverride Malware (Alert, rev. 2021). <https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware>
17. ESET — Win32/Industroyer: A new threat for industrial control systems. https://web-assets.esetstatic.com/wls/en/papers/white-papers/Win32_Industroyer.pdf
18. Mandiant (Google Cloud) — INDUSTROYER.V2: Old Malware Learns New Tricks, 2022. <https://cloud.google.com/blog/topics/threat-intelligence/industroyer-v2-old-malware-new-tricks/>
19. CISA/NSA/FBI et al. — AA24-038A: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, 7 Feb 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
20. Touhiduzzaman M., Louie M., Veeramany A., Ehrhart B. (2024). Large-Scale Hydrogen Storage Cyber Risk Assessment. PNNL/Sandia, SAND-2024-13301R. <https://doi.org/10.2172/2480226>
21. Rivera J., Koleva M. (2025). Hydrogen Long Duration Energy Storage for Resilience (H2 LDES Demo) Project: Threat Vectors and Scenarios. NREL/PR-5700-92485. <https://docs.nrel.gov/docs/fy25osti/92485.pdf>
22. U.S. DOE Hydrogen Program AMR 2024 — The HyRIGHT Project (IN040). https://www.hydrogen.energy.gov/docs/hydrogenprogramlibraries/pdfs/review24/in040_james_2024_o.pdf
23. Impact of Denial-of-Service Cyberattacks on Hydrogen Refueling Stations in an Integrated Transportation and Electric Power System. IEEE SPIES 2024. <https://doi.org/10.1109/spies63782.2024.10983559>
24. Adaptive Feasibility Area Estimation to Enhance Cybersecurity of Electrolysis-Based Hydrogen Refueling Stations Integrated With Power Distribution Systems. *IEEE Trans. Intelligent Transportation Systems*, 2025. <https://doi.org/10.1109/tits.2025.3592630>
25. Cyber Threat Susceptibility Assessment of Hydrogen Infrastructure. IEEE PES General Meeting 2025. <https://doi.org/10.1109/pesgm52009.2025.11225809>
26. LUT University, HYGCEL WP6 T3 — Operational risks and cybersecurity. https://www.lut.fi/sites/default/files/media/documents/HYGCEL-WP6T3_Operational%20risks%20and%20cybersecurity.pdf
27. Dahlmanns M. et al. (2020). Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments. ACM IMC 2020. <https://doi.org/10.1145/3419394.3423666>
28. RADIANCE: Cyber Vulnerabilities and Mitigations Related to Communication Protocols Found in Energy Delivery Systems (OSTI). <https://doi.org/10.2172/1999671>
29. NIST SP 800-82 Rev. 3 — Guide to Operational Technology (OT) Security, Sept 2023. <https://doi.org/10.6028/NIST.SP.800-82r3>
30. NIST — The NIST Cybersecurity Framework (CSF) 2.0, Feb 2024. <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.29.pdf>
31. ISA — ISA/IEC 62443 Series of Standards. <https://www.iso.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
32. ISO/IEC 27019:2024 — Information security controls for the energy utility industry. <https://www.iso.org/standard/85056.html>
33. ISO/IEC 27001:2022 — Information security management systems. <https://www.iso.org/standard/27001>
34. ISA-TR84.00.09-2024 Part 1 — Cybersecurity Related to the Safety Lifecycle. <https://www.iso.org/products/isa-tr84-00-09-2024-part-1-cybersecurity-related-t>
35. Addressing the Security Requirements in Functional Safety Standard IEC 61511-1:2016 (Texas A&M University). <https://hdl.handle.net/1969.1/193441>
36. RVS Bielefeld — Security in IEC 61508/61511 (book chapter). <https://rvs-bi.de/publications/books/RVS-Bk-17-01/Ch13-SecurityIn61508-61511.pdf>
37. ASD's ACSC, CISA et al. — Principles of Operational Technology Cyber Security, Oct 2024. <https://www.cisa.gov/resources-tools/resource/s/principles-operational-technology-cyber-security>
38. NTIA — The Minimum Elements for a Software Bill of Materials (SBOM), 2021. https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
39. A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Communications Surveys & Tutorials*, 2021. <https://doi.org/10.1109/comst.2021.3094360>
40. U.S. DOE — National Cyber-Informed Engineering Strategy, June 2022. https://www.energy.gov/sites/default/files/2022-06/FINAL%20OE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf
41. METI — Basic Hydrogen Strategy (English, 6 June 2023). https://www.meti.go.jp/shingikai/enecho/shoene_shinene/suiso_seisaku/pdf/20230606_5.pdf
42. e-Gov — 脱炭素成長型経済構造への円滑な移行のための低炭素水素等の供給及び利用の促進に関する法律（令和6年法律第37号）. <https://law.s.e-gov.go.jp/law/506AC0000000037>
43. JOGMEC — Support focusing on the price gap and support for the development of hubs, 23 Oct 2024. https://www.jogmec.go.jp/english/news/release/release_00275.html
44. METI — The Cyber/Physical Security Guidelines for Factory Systems, Ver. 1.1 (English). https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.1_eng.pdf

45. e-Gov — 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和7年法律第42号）. <https://laws.e-gov.go.jp/law/507AC0000000042>
46. Cabinet Office of Japan — サイバー対処能力強化法に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する制度の解説. https://www.cao.go.jp/cybersecurity/pdf/cyber_kaisetsu_202610.pdf
47. National Cybersecurity Office (NCO), Japan. <https://www.cyber.go.jp/eng/>
48. Kyushu University — Students combine art and science to design Kyushu's first large hydrogen bus, 20 Sept 2023. <https://www.kyushu-u.ac.jp/en/topics/view/534/>
49. Kyushu Electric Power & Kyushu University — press release, 14 Nov 2023. <https://www.kyuden.co.jp/press/2023/h231114-1.html>
50. Kyushu University — Hydrogen Institute for Sustainability (HYDROGENIUS). <https://sustainable.hydrogenius.kyushu-u.ac.jp/en/>
51. Fukuoka City — 水素リーダー都市プロジェクト (Hydrogen Leader City Project). <https://www.city.fukuoka.lg.jp/keizai/suiso/business/suisoleader.html>
52. Fukuoka Facts — World's first hydrogen refueling station producing hydrogen from sewage. <https://facts.city.fukuoka.lg.jp/en/data/hydrogen-from-sewage/>
53. European Commission — A hydrogen strategy for a climate-neutral Europe, COM(2020) 301. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0301>
54. Directive (EU) 2022/2555 (NIS2), Annex I. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
55. ブルガリア官報 第17号（2026年2月13日） — サイバーセキュリティ法の一部を改正する法律（原文ブルガリア語）. <https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=241234>
56. BTA（ブルガリア通信） — Parliament Adopts Conclusive Amendments to Cybersecurity Act to Align with Updated EU Standards, 05.02.2026. <https://www.bta.bg/en/news/bulgaria/1058489-parliament-adopts-conclusive-amendments-to-cybersecurity-act-to-align-with-updat>
57. ENISA — Cyber Europe tests the EU Cyber Preparedness in the Energy Sector, 20 June 2024. <https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector>
58. 九州大学 カーボンニュートラル・エネルギー国際研究所（I²CNER） — 研究所について（日本語版で追加）. <https://i2cner.kyushu-u.ac.jp/ja/about/>
59. 経済産業省 — 「第7次エネルギー基本計画」が閣議決定されました（2025年2月18日、日本語版で追加）. <https://www.meti.go.jp/press/2024/02/20250218001/20250218001.html>
60. 公益財団法人 水素エネルギー製品研究試験センター（HyTReC） — ウェブサイト（日本語版で追加）. <https://www.hytrec.jp/>
61. R. Drnevich (Praxair) — Hydrogen Delivery: Liquefaction & Compression. Strategic Initiatives for Hydrogen Delivery Workshop, U.S. DOE, 2003年5月7日（日本語版で追加）. https://www1.eere.energy.gov/hydrogenandfuelcells/pdfs/liquefaction_comp_pres_praxair.pdf
62. da Silva Falcão ほか — Ortho- to para-hydrogen catalytic conversion kinetics. *International Journal of Hydrogen Energy* 62 (2024) 345–351（日本語版で追加）. <https://doi.org/10.1016/j.ijhydene.2024.02.380>
63. M. Carreau, R. Naveiro, W. N. Caballero — Poisoning Bayesian Inference via Data Deletion and Replication. *AISTATS 2025*, PMLR 258, 883–891（日本語版で追加）. <https://proceedings.mlr.press/v258/carreau25a.html>
64. NIST — AI 100-2e2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations（2025年3月、日本語版で追加）. <https://doi.org/10.6028/NIST.AI.100-2e2025>
65. M. Han, P. Crossley — Vulnerability of IEEE 1588 under Time Synchronization Attacks. *IEEE PES General Meeting 2019*（電力系統を対象、日本語版で追加）. <https://doi.org/10.1109/PESGM40551.2019.8973494>
66. NPL（英国国立物理学研究所） — Environmental hydrogen purity for fuel cell vehicles（試料採取の代表性、v1.3で追加）. <https://www.npl.co.uk/products-services/environmental/hydrogen-fuel-cell-car>
67. T. Bacquart ほか — First Hydrogen Fuel Sampling from a Fuel Cell Hydrogen Electrical Vehicle–Validation of Hydrogen Fuel Sampling System to Investigate FCEV Performance. *Processes* 10 (2022) 1709（NPL、v1.3で追加）. <https://doi.org/10.3390/pr10091709>
68. A. S. O. Morris ほか — Challenges in hydrogen fuel sampling due to contaminant behaviour in different gas cylinders. *International Journal of Hydrogen Energy* 46 (2021) 18167–18178（NPL、v1.3で追加）. <https://doi.org/10.1016/j.ijhydene.2021.02.220>
69. ISO 19880-9:2024 — Gaseous hydrogen — Fuelling stations — Part 9: Sampling for fuel quality analysis（v1.3で追加）. <https://www.iso.org/standard/82251.html>
70. SAE J2601_202005 — Fueling Protocols for Light Duty Gaseous Hydrogen Surface Vehicles（v1.3で追加）. https://doi.org/10.4271/j2601_202005
71. SAE J2799_202603 — Hydrogen Surface Vehicle to Station Communications Hardware and Software（v1.3で追加）. https://doi.org/10.4271/j2799_202603
72. UNECE GTR No. 13 フェーズ2 TF5 — L. Interoperability Considerations（前文第I節の草案、2019年6月4日、v1.3で追加）. https://wiki.unec.org/download/attachments/81888831/GTR13-6-11%20TF5%20Interoperability_4-Jun-2019_clean.pdf?api=v2
73. V. Mattelaer (CEP) — SAE J2601-5 Training Session（講習資料、2025年、v1.3で追加）. https://cep.expert/wp-content/uploads/2025/09/CEP-REC_SAE-J2601-5-Training-Session-Vincent-Mattelaer_EN.pdf
74. U.S. DOE 燃料電池技術室（FCTO） — An Introduction to SAE Hydrogen Fueling Standardization（ウェビナー資料、2014年9月11日、v1.3で追加）. https://www.energy.gov/sites/prod/files/2014/09/f18/fcto_webinarslides_intro_sae_h2_fueling_standardization_091114.pdf
75. California Air Resources Board — Existing Light-Duty Hydrogen Refueling Stations In-Use Study Report（2024年12月、v1.3で追加）. <https://www2.arb.ca.gov/sites/default/files/2024-12/Existing%20Light-Duty%20Hydrogen%20Refueling%20Stations%20In-Use%20Study%20Report%20ADA%20AL.pdf>

76. OIML R 139-1:2018 (2022年再確認) — Compressed gaseous fuel measuring systems for vehicles. Part 1: Metrological and technical requirements (v1.3で追加) . https://www.oiml.org/en/files/pdf_r/r139-1-e18-reconfirmed-2022.pdf
77. Regulation (EU) 2017/1938 — concerning measures to safeguard the security of gas supply (v1.3で追加) . <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32017R1938>
78. R. Fleming — A legal perspective on gas solidarity. *Energy Policy* 124 (2019) 102–110 (v1.3で追加) . <https://doi.org/10.1016/j.enpol.2018.09.037>
79. X. Rui ほか — An Optimal Flow Allocation Model of the Natural Gas Pipeline Network Considering User Characteristics. *Journal of Pipeline Systems Engineering and Practice* 13(3) (2022) (v1.3で追加) . [https://doi.org/10.1061/\(ASCE\)PS.1949-1204.0000665](https://doi.org/10.1061/(ASCE)PS.1949-1204.0000665)
80. M. Alnakhlhi, P. Dehghanian ほか — Equity-Aware Load Shedding Optimization in Interdependent Power and Gas Networks Against Rising Temperatures. *IEEE TPEC* 2025 (v1.3で追加) . <https://doi.org/10.1109/tpec63981.2025.10906984>
81. Y. Murakami, S. Matsuoka — Effect of hydrogen on fatigue crack growth of metals. *Engineering Fracture Mechanics* 77 (2010) 1926–1940 (九州大学、v1.3で追加) . <https://doi.org/10.1016/j.engfracmech.2010.04.012>
82. B. P. Somerday, P. Sofronis, K. A. Nibur, C. San Marchi, R. Kirchheim — Elucidating the variables affecting accelerated fatigue crack growth of steels in hydrogen gas with low oxygen concentrations. *Acta Materialia* 61 (2013) 6153–6170 (I²CNER、v1.3で追加) . <https://doi.org/10.1016/j.actamat.2013.07.001>
83. I²CNER — Elucidating the variables affecting accelerated fatigue crack growth of steels in hydrogen gas with low oxygen concentrations (研究紹介、2013年10月2日、v1.3で追加) . <https://i2cner.kyushu-u.ac.jp/news/2843/>
84. KAKEN20K04161 — 高桑脩 (九州大学) : 熱活性化過程として解釈する水素ガス環境中の水素助長疲労き裂進展 (2020～2022年度、v1.3で追加) . <https://kaken.nii.ac.jp/grant/KAKENHI-PROJECT-20K04161/>
85. I²CNER (イリノイ大学サテライト) — Hydrogen Materials Compatibility (部門紹介、v1.3で追加) . <https://i2cner.illinois.edu/hydrogen-materials-compatibility/>
86. P. Trinke, B. Bensmann, R. Hanke-Rauschenbach — Current density effect on hydrogen permeation in PEM water electrolyzers. *International Journal of Hydrogen Energy* 42 (2017) 14355–14366 (v1.3で追加) . <https://doi.org/10.1016/j.ijhydene.2017.03.231>
87. M. Bernt ほか — Analysis of Gas Permeation Phenomena in a PEM Water Electrolyzer Operated at High Pressure and High Current Density. *Journal of The Electrochemical Society* 167 (2020) 124502 (v1.3で追加) . <https://doi.org/10.1149/1945-7111/abaa68>
88. NIST Chemistry WebBook, SRD 69 — Thermophysical Properties of Fluid Systems (水素、233.15 K と 288.15 K の等温線、2026年10月21日取得、v1.4で追加) . <https://webbook.nist.gov/chemistry/fluid/>
89. J. W. Leachman, R. T. Jacobsen, S. G. Penoncello, E. W. Lemmon — Fundamental Equations of State for Parahydrogen, Normal Hydrogen, and Orthohydrogen. *J. Phys. Chem. Ref. Data* 38 (2009) 721–748 (v1.4で追加) . <https://doi.org/10.1063/1.3160306>
90. R. W. Schefer, W. G. Houf, T. C. Williams, B. Bourne, J. Colton — Characterization of high-pressure, underexpanded hydrogen-jet flames. *International Journal of Hydrogen Energy* 32 (2007) 2081–2093 (Abel–Noble 式の係数、v1.4で追加) . <https://doi.org/10.1016/j.ijhydene.2006.08.037>

検証に関する注記：本文書における事実に関する記述は、該当する出典により確認した（出典1～60は2026年10月20日、61～90は10月21日）。出典90件は独立した90の証拠ではなく、同じ機関・同じ規格・同じ研究グループによる資料や、背景説明のための資料を含む。未確認または未解決として明記した事項：(a) 日本の水素事業者が指定された重要インフラ分野に含まれるか否か、(b) エラスムス・プラスによる資金支援の受給資格、(c) 九州大学サイバーセキュリティセンターとの協力の可能性。