サイバーフィジカルシステムのクラウド型セキュリティ診断を設計する際の課題

松　崎　和　賢

On Challenges in the Cloud-based Security Diagnosis of Cybers-Physical Systems

Kazutaka MATSUZAKI

Abstract

Cyber-physical systems（CPS）contribute to the realization of Society 5.0, which is the society that Japan is aiming for, but there is a greater risk of cyber-attacks. Security measures are indispensable when infiltrating cyber-physical systems into critical infrastructure. However, even if there are no vulnerabilities with the system at the time of acceptance, new vulnerabilities may be discovered, or as the years go by, vulnerabilities may be embedded when a part of the system is updated or when operations vary. A mechanism that can carry out security diagnosis regularly would be required, and efficient implementation of diagnosis utilizing cloud computing environments is a candidate for its solution. In this paper, we clarify the issues when performing security diagnoses from the cloud and show two design patterns to deal with the emerging issues. Evaluation experiments were conducted after applying these two design patterns to the demonstration environment of CPS. As a result of the evaluation, we showed that the emerging issues could be handled by these two design patterns with cloud and cellular networks.

Key Words

Cyber physical system, cyber security, communication robustness test, industrial automation and control system

目　　次

1　サイバーフィジカルシステムとセキュリティ

我が国が目指す未来社会 Society 5.0 においてサイバー空間とフィジカル空間を高度に融合させたシステム（サイバーフィジカルシステム，以下 CPS とする.）が謳われている．実際にさまざまな産業分野で情報通信技術を活用した「スマート化」が進み，CPS が増加している．例えば分散電源として集中管理される太陽光発電所，クラウドから管理されるビルの空調・照明，スマート保安の対象となる工場が挙げられる．

しかし，CPS の増加によりサイバー攻撃のリスクは高まる．CPS ではサイバー攻撃による被害が物理世界に及ぶこともあり得る．関係する例として，パイプライン，浄水場，送電網といったインフラが情報系からサイバー攻撃を受けて操業停止に至るという事例が報告されている．時間の経過とともに新たな脆弱性の発見や攻撃者の能力の向上も見込まれるため，サイバーセキュリティ対策が妥当であるかの評価を継続的に行う必要があると考えられる．

セキュリティ評価の枠組みとしては，既存の制御システムや組み込み機器のセキュリティ認証制度で行われているセキュリティ試験が挙げられる．例えば，既知の脆弱性の存在を検査する試験や異常な通信データを送信した際の挙動を確認する試験（以下，通信ロバストネス試験とする.）がある．しかし，システムの受入を終え，稼働を始めた後にこうした試験を継続的に実施することは現在の慣行では難しい．

実際にセキュリティ試験をシステムの稼働後に行う場合，実施する時間と人と費用の制約がある．稼働しているシステムに対する現行の保安作業では，現地試験の時間を短くすることが求められる．現地試験の負担を減らすという観点では，セキュリティ試験を保安作業に追加することは逆行した取組となる．そのため，遠隔でできる試験をネットワーク越しに実施することで，現地試験を極力増やさないで済む可能性を追求することが本論文の動機となる．

本論文では，CPS のセキュリティ対策の状況を診断する負荷を低減する方式としてクラウド環境から遠隔で診断を実施する方式を検討する．遠隔から診断を実施しようとする際に，設計の工夫で解決できることをまずは明らかにする．その上でさらに解決しなくてはならない課題を明らかにする．

本論文の構成は以下のとおり．2 章で，CPS セキュリティ診断の課題を明確にする．3 章でクラウド型セキュリティ診断アーキテクチャを提示する．4 章で解決できている課題についての評価を行う．5 章で残された課題について考察し，6 章で結果をまとめる．

2　CPS セキュリティ診断の課題

2.1　想定する状況

想定する状況を明確にするため，**図 1** に CPS のセキュリティ診断を行う簡易的なモデルと課題を示す．

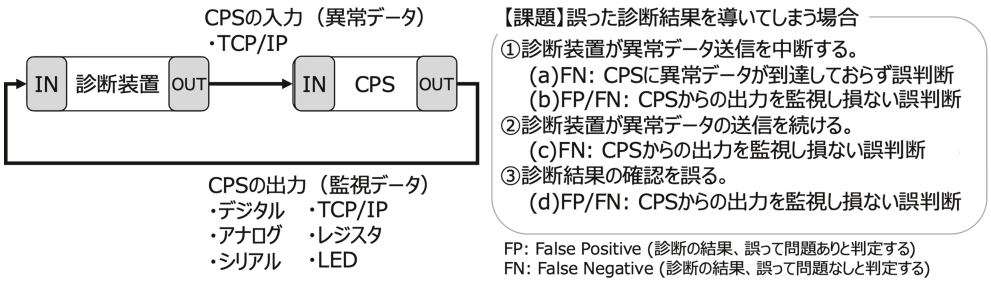


図 1　CPS のセキュリティ診断モデル及び現状の課題

診断装置はCPSの入力インターフェイス（IN）に対して異常データを診断のために送信する．どのようなデータを送るかは入力インターフェイスが受け付けるプロトコルに準じることになるが，本論文ではTCP/IPのプロトコルを想定する．

診断装置はCPSの出力（OUT）を監視することで，セキュリティ対策について診断を行う．監視の対象はあらゆる出力インターフェイスが候補となり，デジタル，アナログ，シリアル（RS－485等），TCP/IP，レジスタ（Modbus等），LED等が該当する．また，監視は以下の2つの段階において必要となる．

1. 診断のための異常データを送っている間に必須機能（essential functions）が維持されているかを監視する
2. 異常データを送った後で，通常の動作状態に復帰しているかを監視する

課題としては，誤った診断結果を導いてしまう場合が存在することである．これには以下の4通りの場合が考えられる．

(a) 異常データがCPSに到達しないため，無効なテストケースとして中断してしまう場合．実際にはセキュリティ対策に問題があるおそれもある．
(b) 監視データがCPSから観測できないため，異常ありと判定する場合と無効なテストケースとして中断してしまう場合とがある．
(c) 監視データがCPSから観測できないため，異常を見落としてテストケースを続行してしまう場合がある．
(d) 異常データを送った後で，通常の動作状態に復帰しているかを監視する際に，監視データがCPSから観測できないために，異常ありと誤判定する場合および異常なしと誤判定する場合がある．

2.2 関連研究

制御システムに対してネットワーク経由でのセキュリティ試験（ファジング等）を行う研究も近年様々な国際会議で報告されている．その中では，試験性能の向上の他，制御システム用の試験環境の要件も整理されている．例えば，試験対象となる機器を可能な限り網羅的に監視することと整理されている[i]．監視の対象はネットワークのインターフェイスや，デジタル入出力を指す．ソフトウェアに対するファジング試験との違いは必須機能が維持できているかどうかを通信やハードウェアの信号等を分析して監視することにある．ソフトウェアのファジングと異なり，デバッガで内部を把握することができず，外部から試験の際に起こっている現象で内部を類推する必要があるため，監視の精度を現実的なコストの中で高める工夫が求められる．

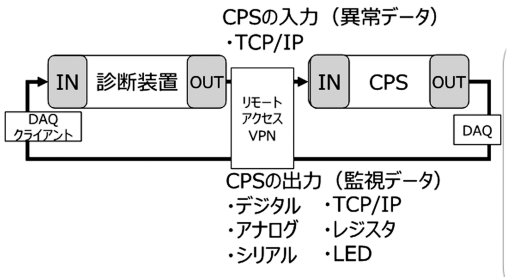
制御システムのファジングツールの性能自体を上げる研究も進められている．例えば，Polar[ii]では機械学習で制御の機能コードを特定し，異常データを少しずつ変えていく形のファジングを行う．これらのツールを地理的に離れたところにある試験対象に対して適用できるかどうかが本調査研究の関心事である．また，制御システム全体のセキュリティ対策をファジングにより評価する研究も注目を集めている[iii]．

---

i) Pfrang S., Meier D., Friedrich M. and Beyerer J., Advancing Protocol Fuzzing for Industrial Automation and Control Systems. DOI : 10.5220/0006755305700580, In Proceedings of the 4th International Conference on Information Systems Security and Privacy（ICISSP 2018）

ii) Zhengxiong Luo, Feilong Zuo, Yu Jiang, Jian Gao, Xun Jiao, and Jiaguang Sun. 2019. Polar : Function Code Aware Fuzz Testing of ICS Protocol. ACM Trans. Embed. Comput. Syst. 18, 5s, Article 93（October 2019）, 22 pages.

iii) Yuqi Chen, Christopher M. Poskitt, Jun Sun, Sridhar Adepu, and Fan Zhang. 2019. Learning-guided network fuzzing for testing cyber-physical system defences. In Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering（ASE '19）. IEEE Press, 962−973.
DOI : https : //doi.org/10.1109/ASE.2019.00093



【ナイーブ解】リモートアクセスVPNとDAQクライアントによる改善状況

	リモートアクセスVPN	DAQクライアント
①(a) 中断	△	無関係
①(b) 中断	△	△
②(c) 継続	無関係	△
③(d) 結果確認	○	△

△の理由：
・低レイヤーの異常データを送れない
・0.1msec程度の信号を取りこぼすおそれ
（異常、タッチパネル操作等）

図2　ナイーブな解による課題への対応状況

2.3　過年度の実証等におけるセキュリティ試験の取組

著者らは過年度に通信ロバストネス試験をリモートアクセス型 VPN（L2TPv2）で実施すること，及び拠点間 VPN（L2TPv3）で実施することを実証した[iv]．拠点間 VPN を用いる場合，双方のネットワークを同一 LAN における通信と同様に通信できるようになる．

前者では，DTLS を用いた VPN を経由して IEC 61580 プロトコルの通信ロバストネス試験を実施した．後者では携帯小型端末（Raspberry Pi）を試験対象の近くに持込み，L2TPv3 の LNS（サーバー）として動作させた上で仮想的なネットワークを構築し，通信ロバストネステストの実施可能性を確認した[v]．

図2に過年度に実証した方式も含むナイーブな方式による課題への対応状況を示す．ナイーブな解として追加した仕組みは以下の 3 点である．

1. リモートアクセス型 VPN
   診断装置と CPS をリモートアクセス型 VPN で接続した．具体的には CPS 側に DTLS を用いた VPN クライアント機器[1)]を持ち込み，診断装置側にコントローラ[2)]を設置した．
2. DAQ（データ取得）
   CPS 内の端子台接点からデジタル信号を分岐し，DAQ[3)]機器の入力とした．
3. DAQ クライアント
   TCP/IP 経由で DAQ にアクセスし，DAQ が保持するデータの値を定期的に入手してユーザに提示する．

対応状況としては部分的に対応できた項目が大半であった．

a）TCP/IP のプロトコルスタックに関する多くのテストケースを実行できたが，レイヤー 2（Ethernet 等）のデータやブロードキャストのデータの到達性に課題が残った．

b）DAQ クライアントを VPN 経由で使用して高頻度で現在値を取得し続けることはできたが，DAQ クライアントのアクセス頻度とネットワークレイテンシーの関係から短時間（0.1 秒程度）のパルスデータを検出できない課題が残った．

c）ネットワークレイテンシーの影響で，必須

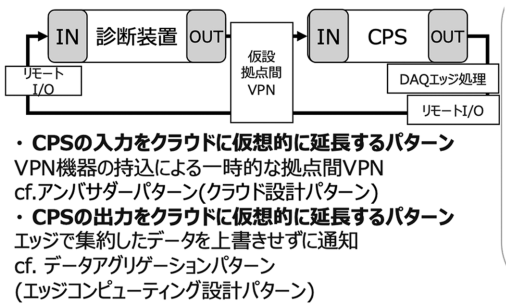
iv）Kazutaka Matsuzaki, Naota Sawabe, Ryo Maeda, Dai Suzuki, Takahiro Matsuura, Hiromu Hamada, Cybersecurity Evaluation Methodology for Distributed Energy Resources: Industrial Demonstration, IECON 2020-46th Annual Conference of the IEEE Industrial Electronics Society

v）松崎和賢，澤田賢治，再生可能エネルギーシステムの遠隔制御におけるセキュリティ評価環境の構築，電気学会電子・情報・システム部門大会，2019

1）Cisco OEAP（Office Extended Access Point）

2）Cisco Wireless LAN Controller

3）LabJack T4/T7



【提案手法】リモートアクセスVPNとDAQクライアントによる改善状況

	仮設拠点間VPN	DAQエッジ処理+リモートI/O
①(a) 中断	○	無関係
①(b) 中断	○	○
②(c) 継続	無関係	○
③(d) 結果確認	○	○

◎ではない理由：
・レイテンシーが高い場合、ジッタエラー対策が必要
・監視対象が多い場合、既存のSW/HWに限界
独自プロトコル等が必要

図 3　提案する入出力延長パターンと課題の改善状況

機能の監視が難しいことがあった．短時間ではあるが試験の要件よりは長い必須機能停止を見落とす場合があるという課題が残った．

d）異常データを送った後で，通常の動作状態に復帰しているかを監視する際に，ユーザのタッチパネル操作が可能であることを条件とした場合に検出できない場合があるという課題が残った．

3　遠隔セキュリティ診断のための設計パターン

図 3 に提案する入出力延長設計パターンと課題の改善状況を示す．提案手法では 2 つの設計パターンを同時に用いることでセキュリティ診断の課題に対応している．

1. CPS の入力インターフェイスをクラウドに仮想的に延長する設計パターン

このパターンでは，前章のリモートアクセス型 VPN に対して，拠点間 VPN を用いている．診断装置の OUT を CPS の IN と同一のネットワークセグメントに仮想的に存在させる．具体的には LAC/LNS 機器[4]を持ち込み，L2TPv3 の VPN を診断装置と CPS の間に一時的に構築する．クラウド設計パターンのアンバサダーパターン[5]の考え方に近い．アンバサダーパターンでは，リモートアクセスのためのプロキシを外部サービスとの通信のために導入する．そのため，提案方式は CPS 側に機器を持ち込むことにより実現する「派遣型」アンバサダーパターンとも言える．

2. CPS の出力をクラウドに仮想的に延長する設計パターン

このパターンでは，前章の DAQ クライアントによるプル型の方式で CPS の出力を確認するのではなく，DAQ に集約したデータをプッシュ型の方式で診断装置側に届ける．デジタル出力を例にすると，DAQ 上でデータの集約と条件判定を行った上で，リレーの ON/OFF を行い，リモート I/O の仕組みを用いて診断装置側にデジタル出力として伝えている．この方式により，DAQ 側で上書きをしてしまう短時間のパルスデータを診断装置側に伝えることができるようになる．エッジコンピューティング設計パターンのデータアグリゲーションパターン[6]の考え方を応用している．データアグリゲーションパターンでは，ネットワーク通信の安定しない環境でエッジコンピュータによりデータを一時的に集約して定期的に

4）　SoftEther VPN Server を動作させた Raspberry Pi

5）　https : //docs.microsoft.com/ja-jp/azure/architecture/patterns/

6）　https : //d1.awsstatic.com/events/jp/2017/summit/slide/D3T5-8.pdf

まとめて中央にデータを送る．提案方式では，データをアグリゲートして上書きされないように待避させたうえでプッシュ型配信により診断装置側に確実に送り出せるようにしている．

提案方式による対応状況としてはネットワークの安定した環境であれば実用に耐える．

a）レイヤー 2（Ethernet 等）やブロードキャストの異常データの到達性についても対応できている．

b）DAQ の性能にもよるが，0.1 秒程度の変化を監視して診断装置に伝えることができるため，短時間（0.1 秒程度）のパルスデータを検出できるようになっている．

c）上記と同様に，DAQ の性能にもよるが，必須機能の監視をミリ秒単位で実施することができる．短時間ではあるが試験としては見逃せない必須機能の停止も補足できるようになっている．

d）異常データを送った後で，通常の動作状態に復帰しているかを監視する際に，ユーザのタッチパネル操作が可能であることを条件とした場合にも，0.1 秒程度の操作でも検出できることを確認できた．

4 章で提案方式の対応状況を確認した実装と評価について詳細を記述する．

4 実装と評価

提案方式（3 章）で課題に一定の条件下で対応できることを，模擬環境にて評価した．評価は 3 通りの試験により実施した．

1. **ローカルネットワークでの試験と提案手法による試験による自動試験の件数比較**　比較のため試験装置の TCP/IP に関するテストスイートを実行する．ローカルの試験で自動実行するテストケースの数と，クラウド型の環境で行う際のテストケースの数を比較する．
2. **産業用プロトコルにおける自動試験の件数比較**　上記 1 の試験のうち，電力分野で導入の進む IEC　61850（MMS）に対するテストスイートに限定して同様の比較を実施した．IEC　61850 のソフトウェアを別のソフトウェアに変え，試験対象機器のデジタル出力も監視の対象とした．
3. **パルス信号の監視試験**　提案手法のクラウド型環境での監視試験を行った．試験用のアナログ出力を時系列に定常変化させ，条件を満たした際に 100 ミリ秒だけパルス出力を診断装置に送る試験を行った．このパルスを把握すると，診断装置側ではテストケースに「異常」として記録を残す．

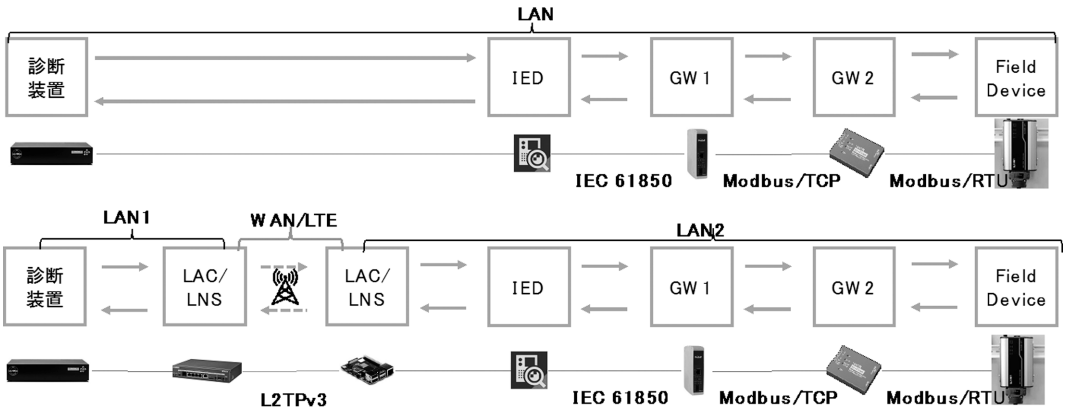


図 4　評価実験 1：IEC 61850 を用いて分散エネルギーリソースを模擬した環境において，ローカル試験と CPS の入力インターフェイスをクラウドに仮想的に延長するパターン適用時の試験との差を比較する．

診断装置としては，市販製品でプロトコルごとにテストスイート（テストケースの集合）を有した状態の Achilles Test Platform（ATP）を使用した．ATP では，試験対象の反応がないと判断すると実施中のテストケースを終えて次のテストケースに移るという動作をする．

4.1 評価実験 1

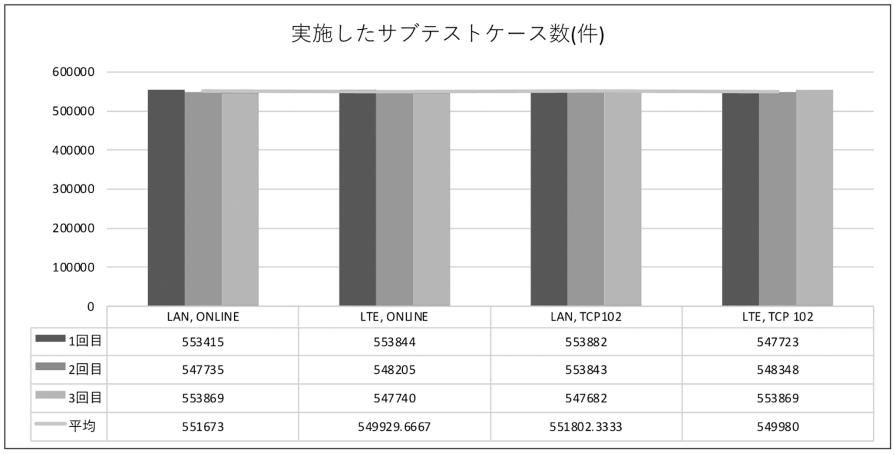
ローカルネットワークでの試験と提案手法による試験によるクラウド型の自動試験の件数比較を行った．

使用したテストスイートとしては，以下の通り．

- Ethernet，IP，TCP の主要な文法試験
- Ethernet の負荷試験
- IEC 61850（MMS）の試験

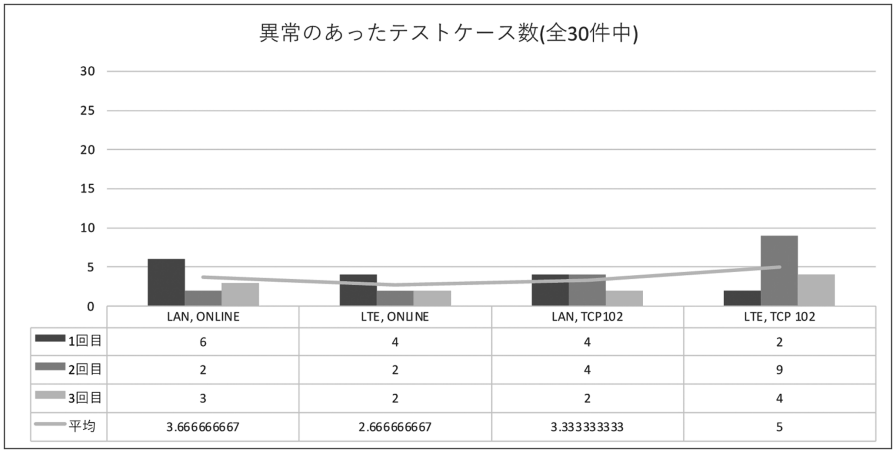
試験対象は Intelligent Electronic Device（以下 IED とする）シミュレータとして Omicron 社の IEDScout を用いた．試験入力は TCP 102 番ポートに限定し，監視は，ネットワークの疎通と TCP 102 番ポートの利用可能性を対象としている．

異常の判定条件として，テストケースを極力実施できるように監視対象が捕捉できなくなってから 30 秒で復帰すれば良いという緩い条件とした．この条件下で，ローカルネットワーク環境での直接接続，LTE 経由の接続で 3 回実施して比較を行った．



	LAN, ONLINE	LTE, ONLINE	LAN, TCP102	LTE, TCP 102
1回目	553415	553844	553882	547723
2回目	547735	548205	553843	548348
3回目	553869	547740	547682	553869
平均	551673	549929.6667	551802.3333	549980

図 5　実施したサブテストケース数



	LAN, ONLINE	LTE, ONLINE	LAN, TCP102	LTE, TCP 102
1回目	6	4	4	2
2回目	2	2	4	9
3回目	3	2	2	4
平均	3.666666667	2.666666667	3.333333333	5

図 6　異常のあったテストケース数

結果はいずれの場合も最後のテストケースまで実施してほぼ同じ結果を得た．実施したテストケースの数に統計有意な差はない（**図5　図6**）．

図6に異常のあったテストケース数を示す．監視条件にTCPポートを加えている方が異常の検出は平均して多い．これは，データを送付する先のポートと同じポートを使用して試験結果の判定を行うことの難しさを示す結果ともいえる．

4.2　評価実験2

産業用プロトコルにおける自動試験の件数比較を行った．評価実験1からの変更点として，IEC 61850を実装するソフトウェアを別の種類に変更し，試験対象機器の出力インターフェイスを監視条件に含めている．

使用テストセットとしては，以下の通り．

- IEC 61850（MMS）の試験

試験対象はlibiec61850(*)のサンプルプログラムを用いた．試験入力はTCP 102番ポートに限定し，監視はネットワークの疎通と，TCP 102番ポートの利用可能性と，IEDのデジタル出力（常時High）とした．その他の条件については，評価実験1と同様の設定とした．

図8に試験数と異常を含む割合を示す．いずれの試験でも最終的に異常という結果を残している．実際にソフトウェアも異常終了している．実施したテストの数は毎回同じであったが，発見した異常の数は若干異なった（35，30，33回）．これは評価実験1と同様に若干の判定誤差を含んでいると考えられる．

4.3　評価実験3

評価実験3では，パルス信号の監視試験を行った．これは，タッチパネル操作等の短い時間の通信・シグナルを正しく捕捉できることの確認を意図している．

診断装置を手動試験実施モードで動作をさせて，その間に監視が機能していることを判定することとした．DAQ内のLuaスクリプト実行環境で試験的な信号を生成し，10秒周期で100ミリ秒程度のパルス出力をCPSの出力として得る想

（*） https://github.com/mz-automation/libiec61850/

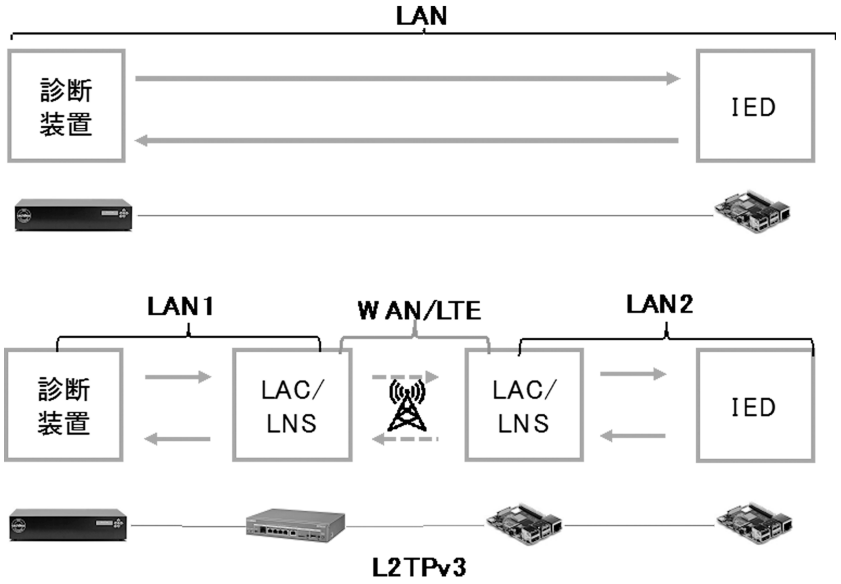


図7　評価実験2　IEC 61850環境

評価実験1との違いとしては，IEDのソフトウェアの種類を変更している．また，IEDのデジタル出力を監視している点も異なる．

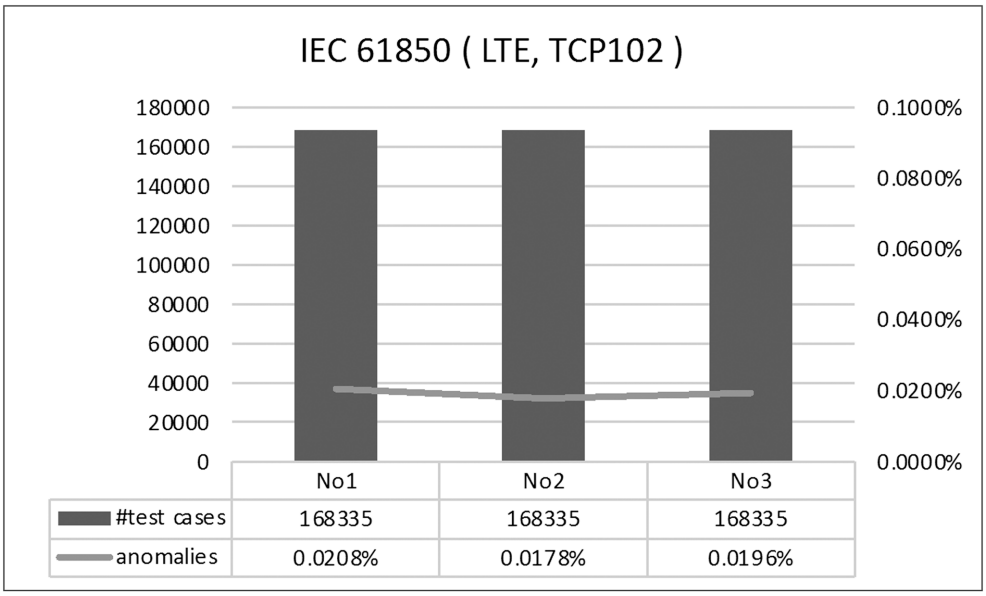


図 8　評価実験 2 における試験数と異常を含む割合

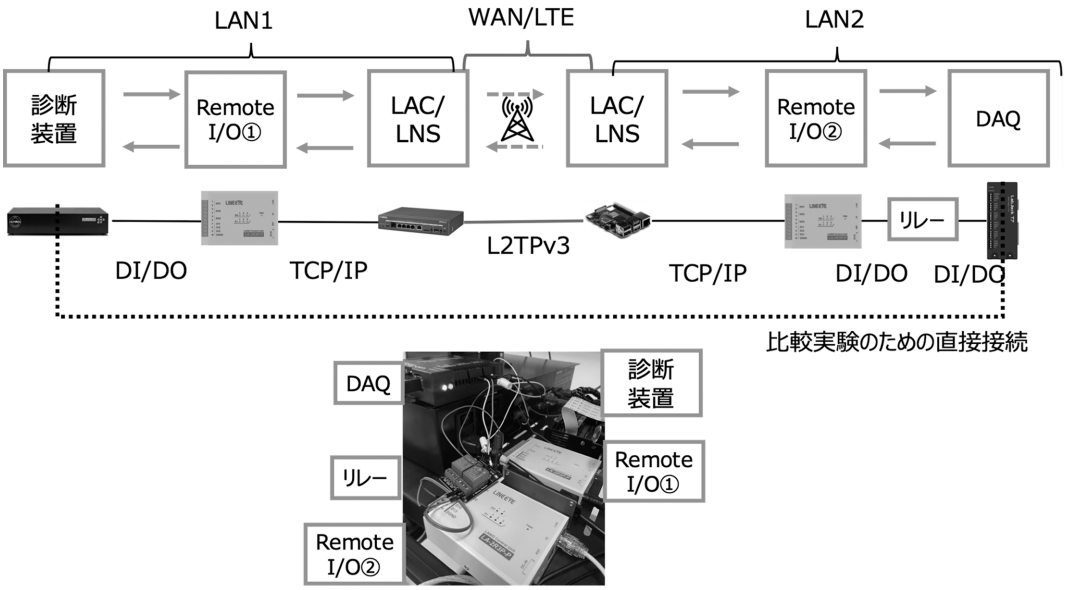


図 9　評価実験 3：監視に特化した環境であり，CPS の出力をクラウドに仮想的に延長するパターンの評価のための構成となっている．比較実験のために DAQ から直接診断装置に接続する経路も設定している．

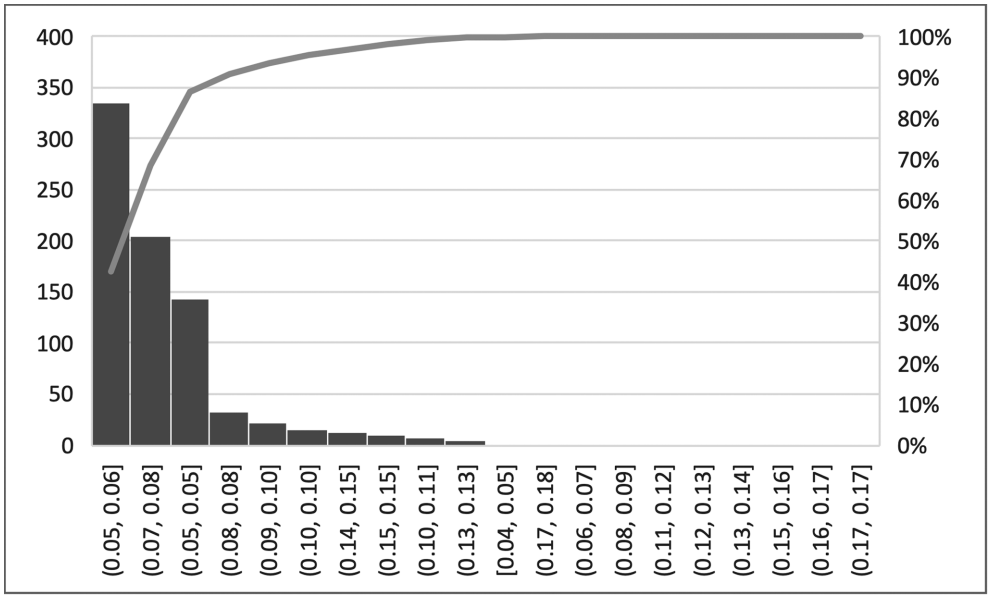


図 10　図 9 の環境におけるレイテンシー
棒グラフの一番左側は，0.05−0.06 秒の間で ICMP をやりとりした回数が 340 回程度（全体の 45% 程度）あったことを示す．

定とした．LTE 網経由で診断装置にこの出力を伝搬し，診断装置側で正しく異常として認識できることを確認した．

レイテンシーの平均値は 0.07 秒であった．最大で 0.18 秒（10 時間で 1 回のみ）を要した．分布は**図 10** の通りとなった．双方のパルス出力に対応の取れない場合はなく，100% 通知された．

5　考　　察

5.1　評価実験と課題の関係

(a) 送信データ未達により異常データの送信を中断してしまう事象については，評価実験 1 及び 2 から対応できているといえる．ただし，ネットワーク負荷試験については，今回の評価に含めていないが，負荷の再現性に関する評価は追加で必要である．

(b) 診断対象の出力の監視不調により異常データの送信を中断してしまう事象については，評価実験 2 及び 3 から対応できているといえる．ただし，監視する接点の数を増やす，送信側での TCP ポート監視等，より複雑な条件を扱う際には追加の評価が必要である．

(c) 診断対象の出力の監視不調により異常データの送信を中断してしまう場合も，(b) と同様に対応できていると言える．

(d) 診断対象の出力の監視不調により診断結果の判断を誤る場合も，オペレータの操作が正常にできている際に誤判定をするおそれについては該当しないことを示した．他の確認手法についても，基本的には (b) (c) と同様に送信側・監視側の双方で通常の操作確認であれば対応できると考えられる．

5.2　適 用 範 囲

ファジングの研究や認証制度における監視の要件は，「あらゆるアウトプットを対象とすること」である．現実的には，クラウド型でないローカルネットワークにおける試験の監視でも対象は限定されている．本提案手法におけるクラウドへの仮想的な拡張パターン適用時においても，リモート I/O や DAQ で機器の数を増やせばローカルエリ

表 1　評価実験と課題の関係

	評価 実験 1	評価 実験 2	評価 実験 3	
(a) 中断	○	○		(a−1) ローカルエリア内での試験と同様の試験を実施していた. (a−2) ローカルエリア内での試験と同件数の試験を実施していた.
(b) 中断		○	○	(b−2) 機器の出力の監視が適切にできていた. (b−3) 0.1 秒程度の異常も補足していた.
(c) 継続		○	○	(c−2) 機器の出力の監視が適切にできていた. (c−3) 0.1 秒程度の異常も捕捉していた.
(d) 結果確認			○	(d−3) 0.1 秒程度の操作も捕捉していた.

アネットワークにおける試験と同様の監視を再現することはできる．ただし，認証制度における認定ツールとなっている試験デバイスであっても，監視点数に GUI や物理的な制約がある．例えば ATP においてデジタル出力であれば物理的に 4 接点である．診断精度を高めるために多数の接点を監視する場合には何らかの符号化と監視表示機能の拡張が必要と考えられる．

今回の試験環境においては，レイテンシーも比較的小さく，ジッターの問題も結果には影響がなかった．電波の弱い地域での試験やネットワーク状態の悪い場合でのジッターエラーへの対応はさらなる実証研究が必要と考えられる．

診断の実際のユースケースを考えた時に，現地のシステムに DAQ 等を仮設する作業者の負担が増すことも考慮が必要である．作業者としては，監視機器の搬入，設置，設定，試験実施への立会があり，監視対象の規模に比例してコストがかかる．監視の条件となるパラメータを決める際に，現地環境に合わせて最適化をすると，その分現地の作業員の負担が増すため，試験コストの低減につながらないという問題も生じてしまう．作業者の負担を含めたトータルコストを低減するための方法論の確立も今後必要と考えられる．

6　ま　と　め

CPS の普及が進む Society 5.0 の時代におけるセキュリティ診断についてアーキテクチャを検討・評価した．特に，CPS の定期的な診断にサイバーセキュリティ対策の状況を含む場合を想定して，クラウド型のセキュリティ診断を実証対象とした．

クラウド型の診断を導入する理由は，診断作業コストの低減にある．ただし，診断の性能が低下しては本来の目的を果たせないため，診断結果に誤りを含みうる場合を列挙し，対策となる設計パターンを 2 つ提案した．それぞれ，評価対象 CPS の入力・出力をクラウドに仮想的に延長する方式である．この 2 つのパターンを適用した環境における評価実験の結果としては現行の課題への対応として十分であるといえる．ただし，拡張性，ジッターエラーへの対応に加え，セキュリティ診断の普及のためには診断の作業者負担を含めたトータルコストを下げるための方法論等今後の研究開発や制度面での支援が必要である．

謝辞

本論文中の実証実験は，電気通信大学 i−パワード・エネルギー・システム研究センター，技術研究組合制御システムセキュリティセンターの協力を得て実施した．試験環境及び有益なアドバイスを澤田賢治先生から提供いただきこの評価も可能となった．この場をお借りして感謝申し上げる．