

IoT機器・システムの品質課題とその対策！

～「つながる世界の品質確保に向けた手引き」の活用～

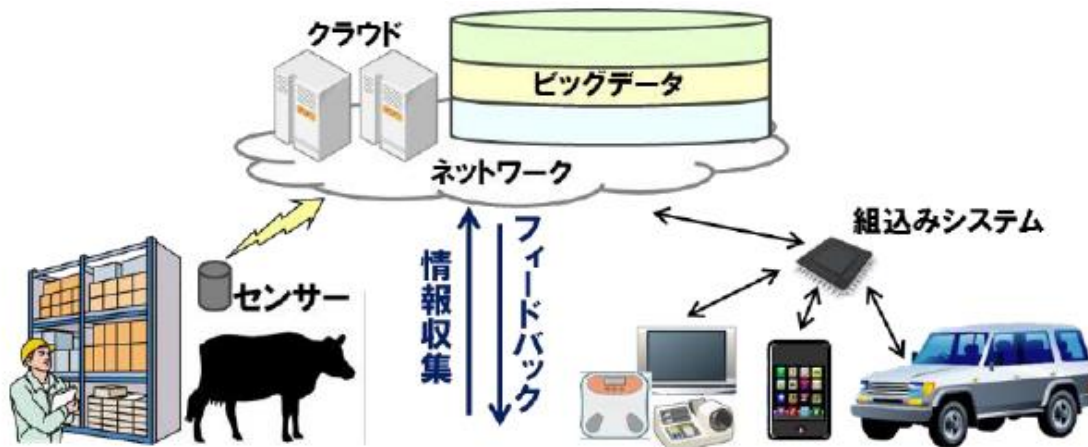
独立行政法人情報処理推進機構（IPA）
社会基盤センター 産業プラットフォーム部
研究員 宮崎義昭

IoT (Internet of Things) :

「コンピュータがRFIDやセンサーを用いて“モノ(Things)”から迅速かつ正確に情報収集を行うことで、省力化とともに、**自らが世界を観察、特定、理解**するようになる概念」

K. Ashton, “That ‘Internet of Things’ Thing,” 1999
<http://www.rfidjournal.com/articles/view?4986>.

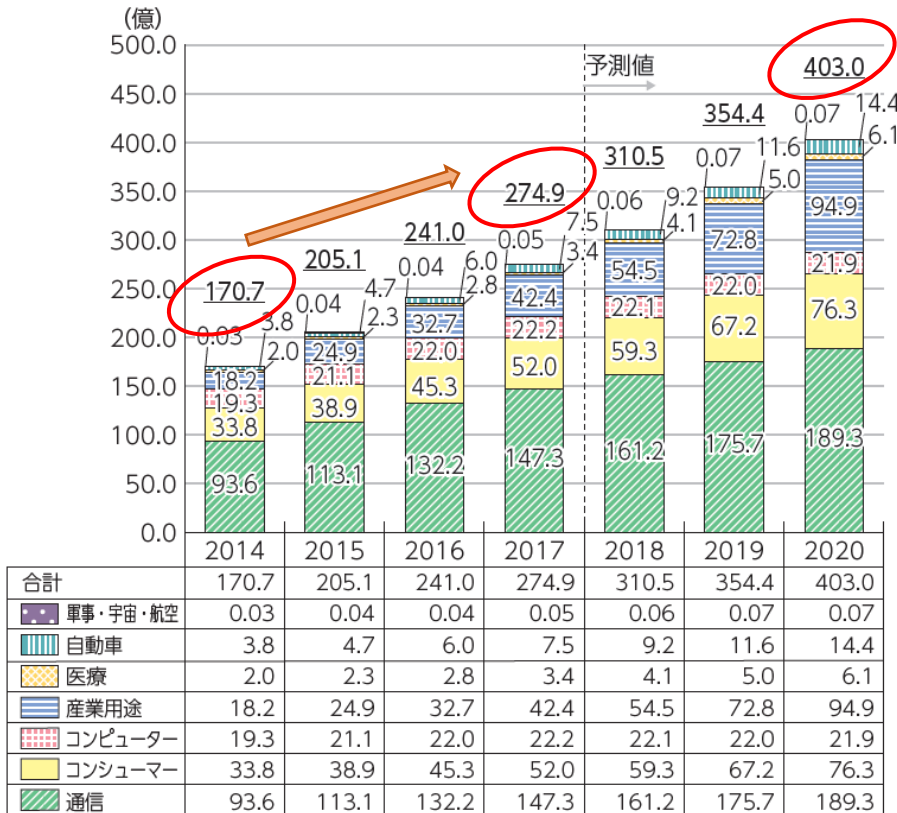
⇒ 現在のIoTは、収集した莫大なデータ（ビッグデータ）を用いて**新しい知見**を得たり、リアルタイムに**機器やシステムを制御**することも重要な特長



IoTデバイスの増加

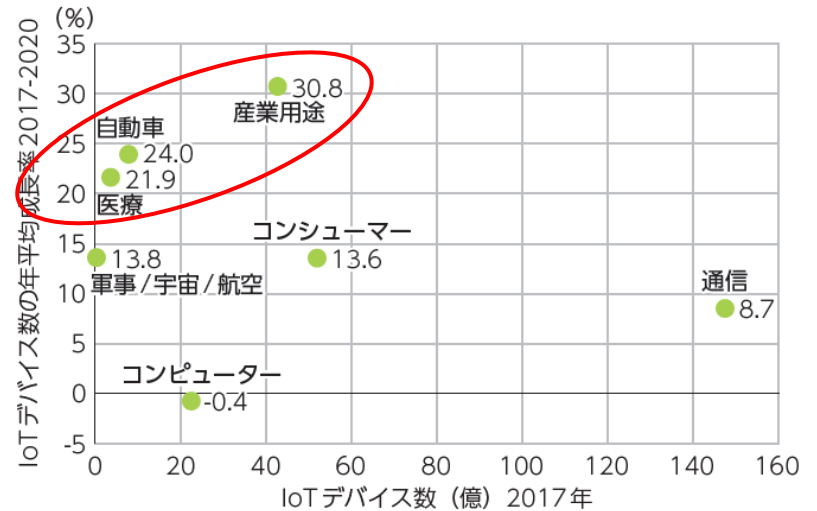
- IoTデバイス数：171億個（2014年）⇒ 275億個（2017年）1.6倍
- 伸び率：産業用途／自動車／医療 20%超

図表 1-1-2-1 世界のIoTデバイス^{*2}数の推移及び予測



(出典) IHS Technology

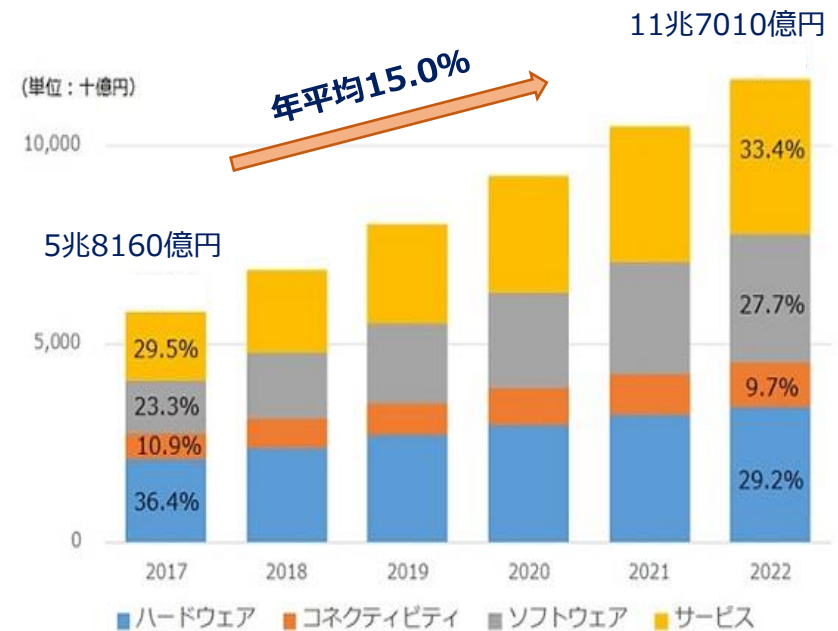
図表 1-1-2-2 分野・産業別のIoTデバイス数及び成長率予測



(出典) IHS Technology

【出典】総務省 情報通信白書（2018年度版）

- 個人から社会基盤まで幅広い分野に適用
 - スマートフォン、ネット家電、ウェアラブル端末
 - 工場設備の見える化、物流トラッキング、農作業の省力化
 - 橋梁、トンネルなどインフラ設備の老朽化監視
 - 自動運転、遠隔医療、他
- 製品・サービスの環境整備が進む
 - IoT向け通信環境の整備
 - クラウドサービスの普及
 - デバイスの低価格化、他
- 他技術との融合による高度化
 - ビッグデータ
 - AI（人工知能）、他



国内IoT市場のテクノロジー別支出額予測 (IDC Japan)

一方で、IoT機器・システムの欠陥が社会問題化する懸念も！

監視カメラの映像がインターネット上に公開

利用者が気づかないまま、WiFi等を通じてインターネットに接続



攻撃者



セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開。**
(ID、パスワードなどの初期設定が必要)

自動車へのハッキングによる遠隔操作

携帯電話網経由で遠隔地からハッキング



攻撃者

カーナビ経由でハンドル、ブレーキを含む制御全体を奪取。



人命にも関わる事故が起こせることが証明され、自動車会社は**140万台にも及ぶリコール**を実施。

【出典】「経済産業省の取組とIoTセキュリティガイドラインVer1.0の概要」、経済産業省

大量に拡散したデバイスやシステムの脆弱性は修復が困難！

IoT機器・システムの特徴	品質リスク
多くの種類のモノやシステムがつながる	1箇所の不具合による影響が、広い範囲に波及する
接続機器の種類や個数の増加など、システム構成が柔軟に変化する	機器の更新による非互換や、想定を超える接続数による性能低下などが発生
様々な利用者に様々な利用環境で使われ、接続の自由度が高い	開発者が想定しない使われ方をされ、動作が保証できない
長期利用中に環境や技術が変化する	利用するOSSに脆弱性が見つかるなど、稼働中に安全安心のレベルが低下する

OSS : オープンソースソフトウェア

従来の製品・サービス開発のノウハウだけでは、
想定できない品質リスクがあり、事前の対策が難しい！

- IoTの特徴を捉えて、IoT製品・システムの品質を確保し維持するために、考慮すべき事項を13の視点として整理
- 開発者、保守者、品質保証者、運用者など品質に携わるすべての担当者が対象

つながる世界の 開発指針



2016年3月 公開
2017年6月 改版



品質確保の観点で
具体化

つながる世界の 品質確保に に向けた手引き



2018年3月 公開

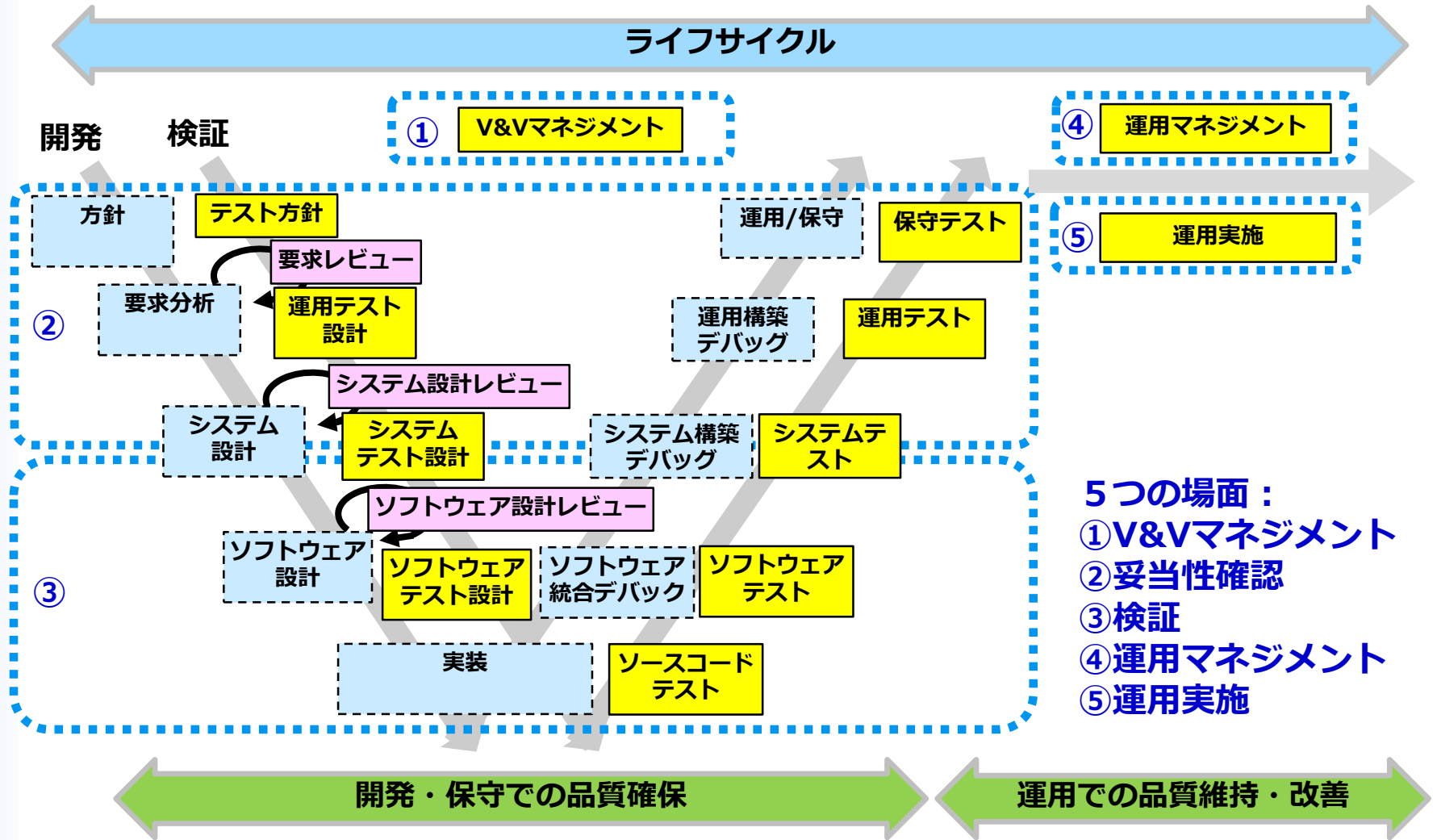
①IoTのライフサイクル全般で、品質を確保する活動を「V&Vマネジメント」「妥当性確認」「検証」「運用マネジメント」「運用実施」の5つに整理し、品質確保のための考慮事項を解説

②IoTで実際に起こり得るIoTシステムの制御競合のケースを事例として、品質確保のための「13の視点」に基づき、適用検討事例を紹介

③開発・運用の現場で活用できる品質確保チェックリストを同時公開

※V&V : Verification and Validation (検証と評価)

■ 品質確保の5つの場面を想定し、そこで考慮すべき重点事項を整理



IoTの品質確保、維持・改善の13の視点

■ IoTの開発・保守から運用までライフサイクルで品質を確保、維持・改善

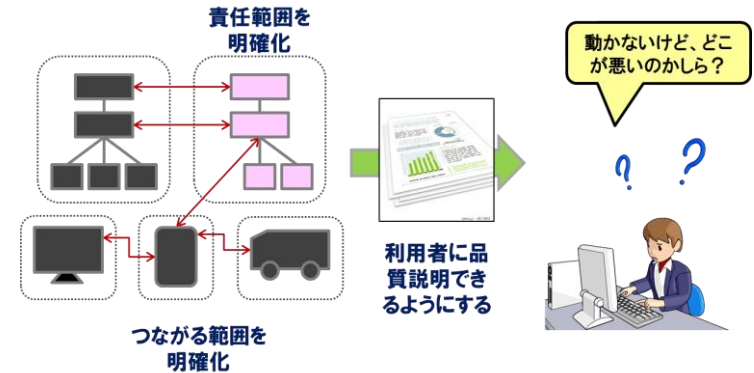
	活動		品質の確保、維持・改善の視点
開発・保守	V&V マネジメント	IoTの品質確保のための検証・評価計画立案	【視点1】 IoTの社会的影響やリスクを想定する
	妥当性確認	利用者視点での要求の妥当性確認	【視点2】 つながる機能の要求仕様が利用者を満足させるか確認する
			【視点3】 実装した機能が利用者の要求を満たしているか評価する
	検証	IoTの特徴に着目したテスト設計	【視点4】 多種多様なつながり方での動作と性能に着目する
			【視点5】 多種多様な利用環境や使い方に着目する
			【視点6】 障害や故障、セキュリティ異常の検知と回復に着目する
			【視点7】 長期安定稼働の維持に着目する
			【視点8】 大規模・大量データのテスト環境構築とテスト効率化を検討する
			【視点9】 テストのし易さと実施可能性を検討する
		IoTの効率的なテスト実施	【視点10】 テストを効率的に実施し、エビデンスを残す
運用	運用マネジメント	IoTの品質を維持・改善するための運用計画立案	【視点11】 運用中の環境変化による影響やリスクを想定する
	運用実施	長期利用での品質維持と改善	【視点12】 運用中の環境変化を捉え、品質が維持されているか確認する
			【視点13】 ソフトウェアの更新時はつながる相手への影響を確認する

V&Vマネジメント（検証方針・計画立案）

【視点1】IoTの社会的影響やリスクを想定する

概要

- IoTでは障害が発生すると影響が拡散し、甚大な被害となる可能性がある
 （例）マルウェア「Mirai」（注1）の事例では大規模なDDoS（注2）攻撃による被害が発生
- ⇒ 問題が発生したときの社会的な影響やリスクを考慮し、品質の説明責任が果たせる検証・評価計画の策定が重要



（注1） <https://www.ipa.go.jp/files/000057382.pdf>

（注2） DDoS : Distributed Denial of Service attack（分散型サービス妨害攻撃）

考慮ポイント

【1-1】IoTの特徴を考慮した検証・評価の方針を策定する

- 適用分野/社会的影響、法規制、プロジェクト自体のリスク、調達品の品質などを考慮

【1-2】つながる範囲を明確化してリスク・コストを意識しながら検証・評価計画を策定する

- 検証評価の範囲、要員、スケジュール、評価基準、予算などを考慮

【1-3】つなぐ相手や利用者に対して品質を説明できるようにする

- 調達品を含めた検証結果のエビデンスを残し、利用者や関係者に対する説明責任を考慮

【1-4】検証・評価の範囲を明確化し、関係者間の合意を促す

- 依頼元や調達品の提供元などの関係者と合意を得るための仕組みを考慮

妥当性確認（要求仕様のレビュー）

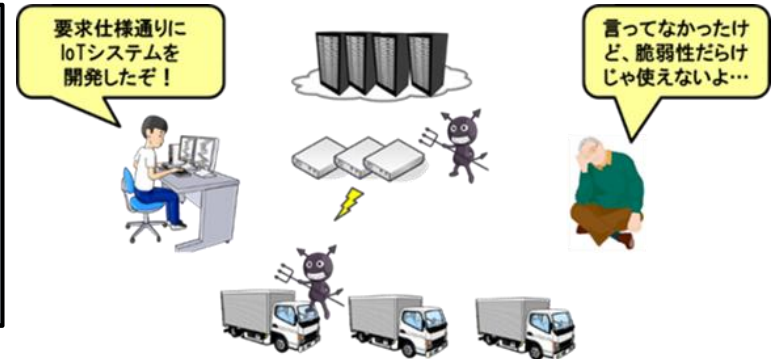
【視点2】 つながる機能の要求仕様が利用者を満足させるか確認する

概要

■ IoTでは利用者や利用環境の想定が難しい

⇒ 多様な利用者や利用環境の変化に対して、本来提供したい価値を継続して提供できるか、要求仕様そのものの妥当性を確認する

- 要求仕様に明確に書かれていない暗黙的な要求も対象とする



考慮ポイント

【2-1】 IoT特有の機能や性能、互換性や拡張性に着目する

- つながる機器の種類、性能差、取り扱うデータ、将来的な拡張性に関する要件を確認

【2-2】 利用環境や利用者の使い方に着目する

- 利用者や利用場面、利用者の役割などを想定しているか確認

【2-3】 IoTのライフサイクルでの安全安心^(注)に着目する

- 機器の障害や劣化、セキュリティなどの要件を確認

【2-4】 長期利用のための保守・運用に着目する

- リリース後の不具合や脆弱性対策、システムの正常稼働を確認する機能などの要件を確認

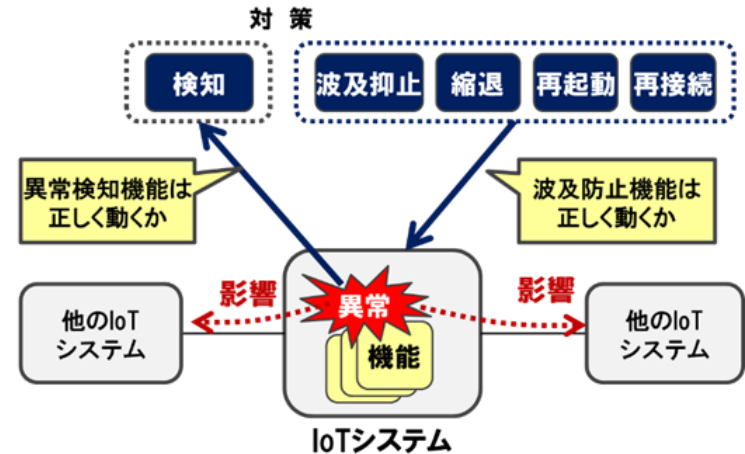
(注) 本書における定義：対象とする機器やシステムのセーフティ、セキュリティ、リライアビリティが確保されていること

検証（テスト設計）

【視点6】 障害や故障、セキュリティ異常の検知と回復に着目する

概要

- 機器・システムとの接続が行われるため、障害/故障が波及したり、セキュリティ攻撃を受ける可能性がある
- ⇒ 障害/故障が発生しても意図された機能が維持できるか確認する
- ⇒ セキュリティについて、セーフティに与える影響を含めて確認する



考慮ポイント

【6-1】 障害/故障や異常の検知、復旧などの異常処理や長期利用に係わるテストを設計する

- 設計範囲外の機器接続や異常データ発生時の処理
- 機器の障害/故障、通信の障害発生時の処理
- 長期間利用時、複数システムによる競合時の処理

【6-2】 つながることによるセキュリティの脅威やそれがセーフティに及ぼす影響を考慮したテストを設計する

- セキュリティ攻撃の検知、セキュリティ/セーフティ規格による要求事項への準拠の確認
- レベルが異なるシステム間の接続、セキュリティがセーフティに与える影響の確認

運用実施（長期利用での品質維持）

【視点12】 運用中の環境変化を捉え、品質が維持されているか確認する

概要

- リリース後に想定外のIoT機器接続やセキュリティ劣化が発生する可能性がある
 - 「BlackEnergy」^(注)では、復旧活動を妨害する補助的攻撃が行われ、遠隔操作や監視機能を無効化された。何が起きているかの把握が遅れ、復旧までに6時間を要し40～70万人に影響が出た
- ⇒ 機器の故障やセキュリティ異常を検知するための機能が正常に動作していることの確認が重要



(注) https://www.jpCERT.or.jp/present/2016/20160217_CSC-JPCERT01.pdf

考慮ポイント

【12-1】 リリース後の利用環境の変化と脆弱性などの技術情報を把握する

- 利用環境の変化の把握（想定外の利用者、機器の故障やセキュリティの異常、等）
- 技術方法の変化の把握（脆弱性情報、OSSなどの更新情報、法規制の変化、等）

【12-2】 利用者が直接利用する機能と安全安心に係わる機能が維持されているかを確認する

- 利用者に約束している機能や性能の状況を確認し利用者へ情報提供
- 安全安心に係わる機能の定期的な確認（障害監視、ウイルス対策、縮退・停止機能、等）

つながる世界の品質確保チェックリスト

- 「品質確保の手引き」に記載した考慮事項について、開発・保守や運用の現場で確認するためのチェックリストを公開
 - 事業内容や開発の実態に合わせてカスタマイズしてご利用ください！

URL : <https://www.ipa.go.jp/files/000064878.xlsx>

チェック項目について、対象とどうかを検討

対象とした項目について、実施状況を記入

計画書やテスト結果などのエビデンスを記載

考慮ポイントとチェック項目	対象の検討	実施状況(対象と決めた場合)	エビデンス(対象と決めた場合)	確認日
【4-1】多数の機器の接続や性能を考慮したテストを設計する				
① テスト設計時の考慮項目				
4-1-1-1 最大接続数、データの最大量に関するテストが考慮されているか？	対象	検討中		
4-1-1-2 想定外のデータを取り扱う機能に関するテストが考慮されているか？	対象	未着手		
4-1-1-3 様々なつながり方でつながる相手も含めた機能の充足性に関するテストが考慮されているか？	対象	未着手		
4-1-1-4 動作寿命や消費電力に関するテストが考慮されているか？	対象外			
4-1-1-5 IoT全体としての性能の満足性や性能のボトルネック、性能バランスに関するテストが考慮されているか？	対象	未着手		
② テストの実行性・効率性確認				
4-1-2-1 実行性に関して、接続性や性能の確認に必要なテスト環境の条件や仕様が明確であるか？				
4-1-2-2 効率性に関して、つながるパターンやデータパターンなどの組み合わせテストの実行時間を予測しているか？				
【4-2】多種類の機器との接続やシステム連携を考慮したテストを設計する				
① テスト設計時の考慮項目				
4-2-1-1 同一機種の各種バージョンでの機能の互換性に関するテストが考慮されているか？				
4-2-1-2 同一仕様の各種メーカーでの機能の互換性に関するテストが考慮されているか？				
4-2-1-3 システム連携などでの相互の情報の交換に関するテスト(異常データも含む)が考慮されているか？				
② テストの実行性・効率性確認				
4-2-2-1 実行性に関して、機能や情報の互換性の確認に必要なテスト環境の条件や仕様が明確であるか？				
4-2-2-2 効率性に関して、テスト対象機種やバージョンの組み合わせテストの実行時間を予測しているか？				
【5-1】利用者、利用状況、利用環境などを考慮したテストを設計する				
① テスト設計時の考慮項目				
5-1-1-1 利用者の特性・スキル、利用場所、利用シーンなどを想定したテストが考慮されているか？				
5-1-1-2 利用状況把握機能とプライバシー保護機能に係わるテストが考慮されているか？				
② テストの実行性・効率性確認				
5-1-2-1 実行性に関して、実利用に関する確認に必要なテスト環境の条件や仕様が明確であるか？				
5-1-2-2 効率性に関して、実利用を想定したシーンの組み合わせテストの実行期間を予測しているか？				

品質確保の手引き／チェックリストの具体的な用途

- IoT製品・システム開発の品質確認に適用
 - 新規製品開発やエンハンス時の品質確認
 - PoC（Proof of Concept：概念実証）の要件の確認
 - 障害発生時の原因分析と対策後の品質確認
- IoT製品・システムの発注/調達時の確認に適用
 - 発注時の購入仕様の品質確認条件や受入検査事項
 - 調達品の品質確認
- 品質コンサルや第三者検証の確認に適用
 - お客様への検証/評価コンサルの素材
 - 検証業務の受託案件の品質確認

関連団体様などを通して実案件への適用を推進中！

⇒ 「考慮不足の洗い出しに役立った」「組織の品質保証の課題が見つかった」などのご意見あり。

中小規模IoTの品質確認チェックリスト

- 中小規模の製品・サービスを想定した簡易版のチェックリストを新たに作成（2018年11月公開）
- 従来のチェックリストは、“規模が小さい案件への適用には確認項目が多すぎて使いづらい”とのご意見に対応したもの

中小規模向けIoTの品質確認
- 自己診断チェックリスト -

独立行政法人情報処理推進機構
社会基盤センター

IoTの特徴を捉えた品質確認の
ポイントが簡単に分かります！！

IoTの特徴

- 様々なモノやシステムがつながる
- 接続される機器の種類や個数など、システムが柔軟に変化する
- 様々な利用者が様々な利用環境で使う
- 自動車・家電製品・工場のシステムなど長期に利用される

自己診断チェックリスト		
No.	チェック内容	チェック欄
(1)	IoT機器・システムとしての特徴や産業分野の規則など守らなければならない事項などの観点から検証・評価方針を策定していますか？	
(2)	つながる範囲を明確化して、リスクとコストを認識しながら、検証・評価計画を策定していますか？	
(3)	検証・評価の結果として残すべき記録（テストの実施環境、実施項目、テスト結果、実行ログなど）が明確になっていますか？	
(4)	検証・評価計画書やテスト設計書、テストの合否判定の結果に対する倉庫方法や、トラブルシューティングに関する協力について、関係者間で決めていますか？	
(5)	IoT特有の機能、性能、将来の拡張を考慮して、要求仕様の妥当性をレビューしていますか？	
(6)	利用者や利用環境を網羅的に考慮して、要求仕様の妥当性をレビューしていますか？	
(7)	IoT機器の障害や劣化による影響、セキュリティ対策など、安全安心を考慮して、要求仕様の妥当性をレビューしていますか？	
(8)	IoT機器・システムを長期的に安定して稼働させるための保守・運用を考慮して、要求仕様の妥当性をレビューしていますか？	
(9)	接続する機器の最大数や最大データ量を考慮したテストや、性能テストを設計していますか？	
(10)	メーカーやバージョンが異なる機器と接続するときの機能の互換性や、システム連携の情報の互換性を考慮したテストを設計していますか？	
(11)	利用者の特性・スキル、利用場所、利用シーンなどを想定したテストを設計していますか？	
(12)	機器の故障やシステム障害の発生を想定したテストを設計していますか？	
(13)	つながることによるセキュリティの脅威やそれがセーフティに及ぼす影響を考慮したテストを設計していますか？	
(14)	障害解析に必要なログの収集や転送を行う機能、アップデートに関する機能（セキュリティな転送、失敗時の回復、負回・性能など）のテストを設計していますか？	
(15)	テスト設計で抽出したテストを確実に実施するために必要なテスト環境は準備できていますか？	
(16)	テスト設計で抽出したテストを効率化するための手段を検討していますか？	
(17)	テストの実行順序や組み合わせを考慮してテストをしていますか？	
(18)	合否判断の根拠となるエビデンスを採し、テスト実施結果を開発チームと確認していますか？	
(19)	IoTの機能が当初の要求を満足しているか総合評価し、評価結果を開発者と合意していますか？	
(20)	運用中に起こり得るシステムの機能や性能が劣化する事項を予測し、それらの発生を把握するような監視方法と発生時の対応プロセスを決定していますか？	
(21)	機能や性能が利用者の期待を達成できているか評価し、評価結果を開発者と共有し、開業にフィードバックするプロセスを決定していますか？	
(22)	リリース後の利用環境の変化や最新の技術情報を把握し、対応していますか？	
(23)	利用者が利用する機能と安全安心に関する機能が正常に維持できていることを、確認していますか？	
(24)	ソフトウェアの更新時は、接続先システムに影響を与えないことを確認していますか？	

従来の考え方を踏襲しつつ、チェック項目を
24項目に集約。分かりやすい解説付き！

ダウンロードURL：

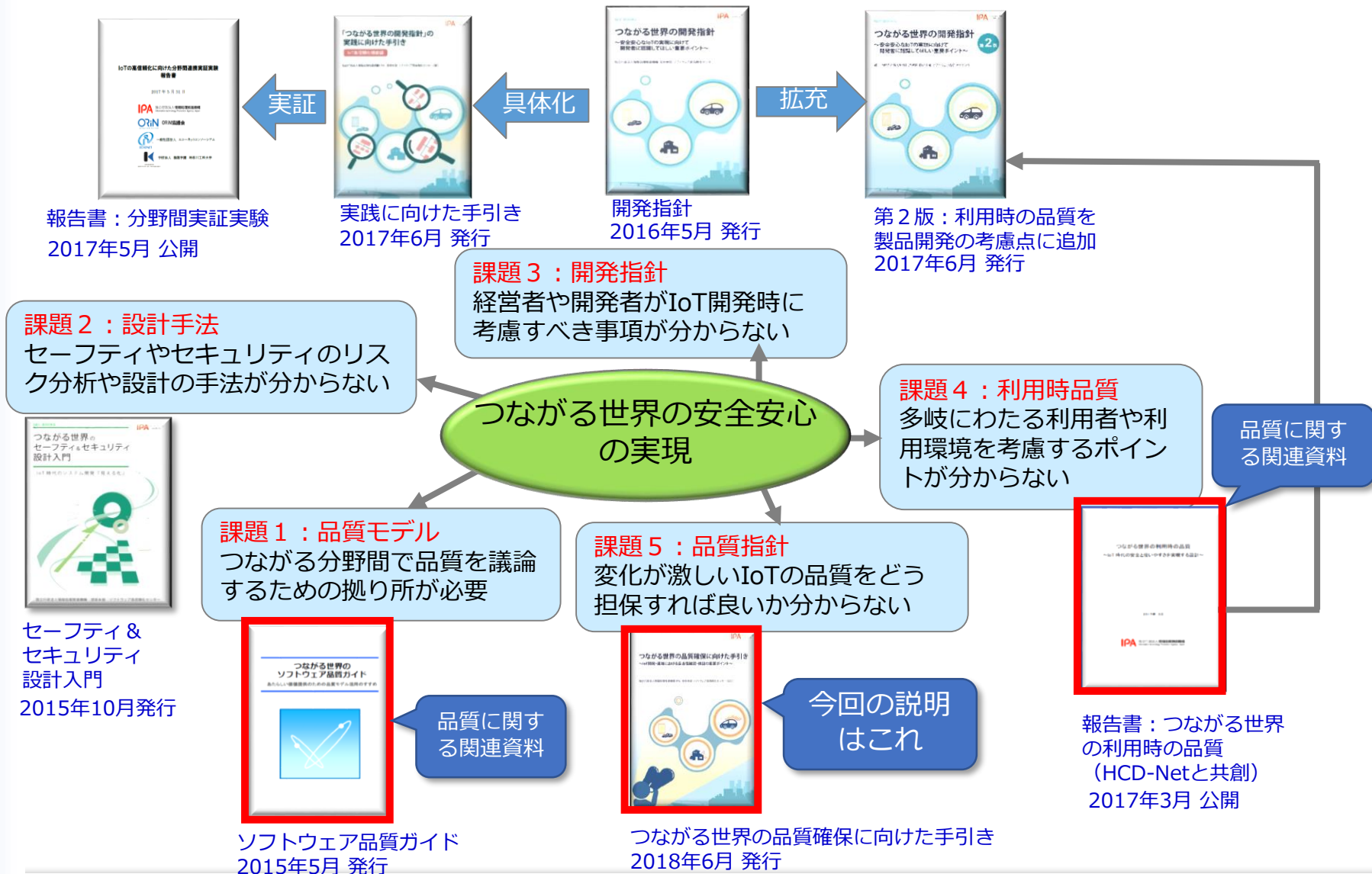
- <https://www.ipa.go.jp/sec/publish/tn18-001.html>
- <https://www.ipa.go.jp/files/000069673.xls>

- 早い段階で様々な視点から品質リスクを洗い出す
 - 守るべき対象を明確にしたうえで、障害による被害を想定する
- その上で、いま対処すべき品質リスクへの対策を検討
 - 当面の利用者や利用場面において必要な対応範囲を決定する
- 将来の拡張に合わせて、品質リスク対策も順次強化
 - 機能や利用者の広がりに伴い、リスクは必ず増えることを認識する

優先度やコストも考慮しバランスが取れた品質リスク対策を！

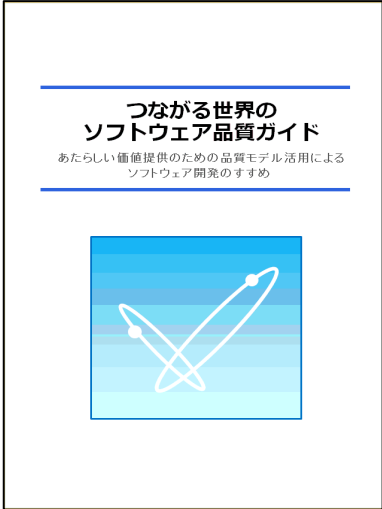
(参考) 関連資料

(参考) つながる世界の安全安心に向けたIPAの取組み IPA



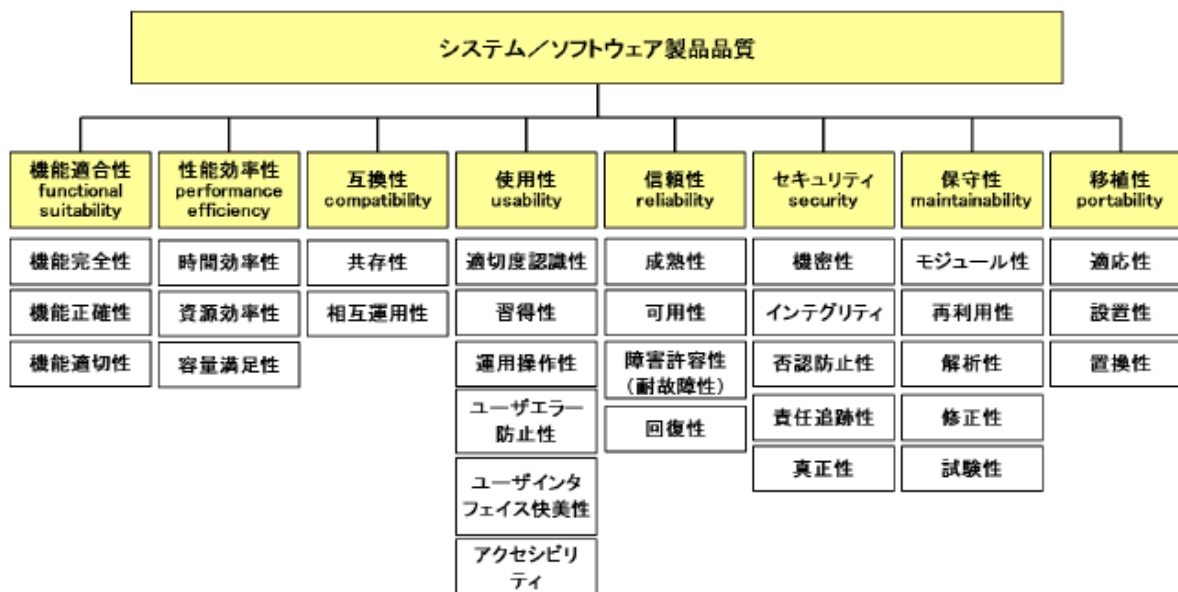
- 製品・サービスを提供する事業者が理解しておくべき品質に関する基本的な知識をIoT機器・サービスの事例を交えて紹介
- 国際規格SQuaRE※の活用についてわかりやすく解説

(※) SQuaRE：ソフトウェア製品の品質要求及び評価に関する国際規格。
ISO/IEC 25000シリーズ、JIS X 25000シリーズ。

	ソフトウェア 品質ガイド編 (約100頁)	品質をあらためて考える背景、国際規格SQuaREの概要、ユーザビリティ/セーフティ/セキュリティなど重要な品質に関する解説、品質向上に向けた改善ポイント、品質説明と第三者評価、などについて分かりやすく説明。
SQuaRE品質 モデル活用リ ファレンス編 (約110頁)	国際規格SQuaREで規定された品質モデル（製品品質、利用時の品質、データ品質）について、品質特性/品質副特性の各項目について、説明/ニーズ例/測定量の例等を記載。実際に品質要件の洗い出しや評価計画を作成する場面で、作業効率を期待。	

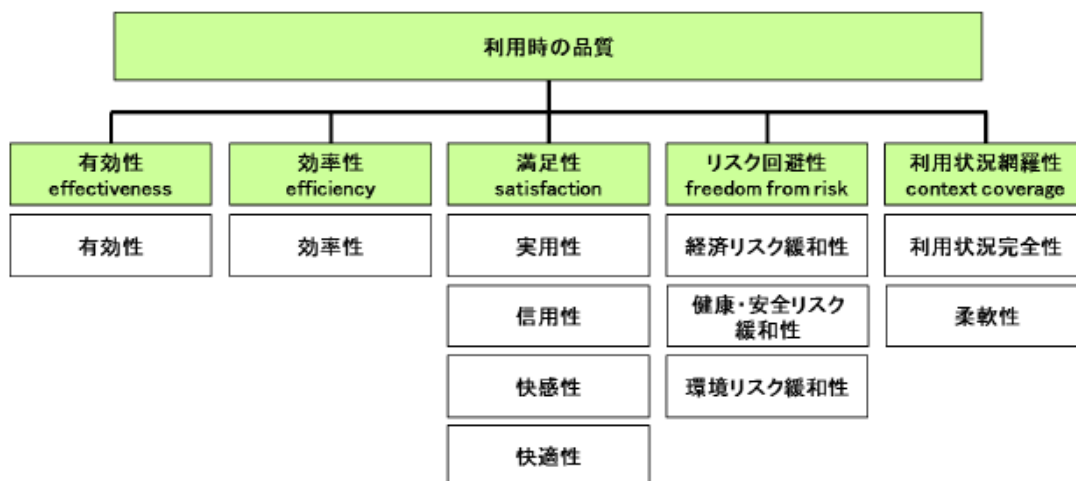
公開URL <https://www.ipa.go.jp/sec/reports/20150609.html>

(参考) SQuaREの品質モデル



JIS X 25010:2013
システム/ソフトウェア
製品品質

機能の豊富さ、操作のしやすさなど、製品自体が備えている特徴から見た品質



JIS X 25010:2013
利用時の品質

作業効率の向上、使った時の満足感など、その製品の利用者に対する影響から見た品質

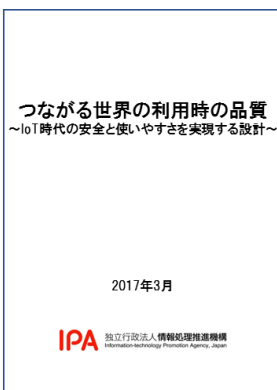
つながる世界の利用時の品質～IoT時代の安全と使いやすさを実現する設計～

利用時の品質：利用者がある利用状況において、利用者のニーズに照らして、製品・システムを利用できる度合い
ISO/IEC 25000シリーズ (SQuaRE)

➡ 性能や耐久性といった製品品質に対して、実際にユーザが利用する際の有効性、効率性、満足度、危険な状況を招かないリスク回避性を指す

「つながる世界」において、すでにネットワークにつながっている、または今後つながる可能性がある機器やシステムを開発・利用する際の「利用時の品質」について、主に以下の事項を報告

- 一般的な利用時の品質の考え方、**設計への反映プロセス**などの整理
- つながる世界を含めた**失敗・成功事例の収集と課題の整理**
- つながる世界に向けた利用時の品質向上のための**15の視点**を提示



利用時の品質を向上することによる効果

- ① ユーザの満足度が高まる
- ② 市場に出たからの失敗が減る
- ③ 新しい「ユーザ経験」を生み出す

報告書公開URL <https://www.ipa.go.jp/sec/reports/20170330.html>

つながる世界の利用時の品質～IoT時代の安全と使いやすさを実現する設計～

報告書公開URL <https://www.ipa.go.jp/sec/reports/20170330.html>

利用時の品質向上のための15の視点

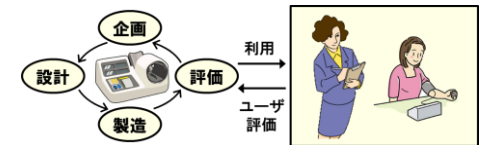
区分	視点
組織文化	1 つながる世界の利用時の品質を意識する
	2 他部門と連携して取り組む文化を作る
	3 自社や顧客の責任者の意識を変える
	4 利用時の品質向上に関わる人材を育成する
把握・分析	5 ユーザの特性や経験、文化、利用環境を考慮する
	6 ユーザ経験を収集・分析・評価する
	7 間接・受動的ユーザやプライバシーにも配慮する
	8 利用状況や利用環境の変化の影響を考慮する
設計	9 企画・設計段階からユーザを巻き込む
	10 ユーザを安全な操作に導く設計をする
	11 第三者に機能や情報を使わせない設計をする
	12 操作結果やメッセージを確実に伝える設計をする
保守・運用	13 ユーザや関係者からフィードバックを得る仕組みを作る
	14 知見を開発時及び出荷後の利用時の品質向上に活用する
	15 つながるリスクの周知と安全設定の仕組みを作る



組織文化の醸成



ユーザ経験の把握・分析



ユーザを巻き込んだ設計



知見をまとめる保守・運用

つながる世界シリーズの書籍、及びチェックリストのご活用を宜しくお願い致します。

ご清聴ありがとうございました。