Jama software®

ホワイトペーパー

自動車開発に対するISO 26262の影響

IN PARTNERSHIP WITH

LHP®

コンプライアンスがトレーサビリティやリスクマネジメント、妥当性確認、検証に及ぼす影響

コンプライアンス標準、特に比較的新しい機能安全の要素に関わる標準によって、開発プロセスにさらなる要件が追加されます。

特に機能安全規格 ISO 26262 では、自動車のハードウェアおよびソフトウェアシステムの製品ライフサイクルに対してさらに多くの要件が追加されます。この機能安全規格は、V 字モデルライフサイクルのプロセスを設計するシステム全体を通じた統合要件のトレーサビリティ、リスクマネジメント、妥当性確認、検証、文書化および共同作業に影響するフレームワークとして機能します。また ISO 26262 では、自動車のシステムを作る際に用いるツールの認定も必要となります。

本文書では、この規格がカーエレクトロニクスの開発プロセスとサポートツールチェーンの両方に対して及ぼす影響について考察し、この規格に対して行われた最近のアップデートについても触れます。

自動車安全規格のコンプライアンスの簡略化

Jama Software は LHP Engineering Solutions（以下 LHP）の機能安全コンサルタントと提携関係を結び、当社の先見性のあるお客様が関連性のあるすべての機能安全規格およびサイバーセキュリティ規格（ISO 26262 や SAE J3061 など）に準拠できるよう、製品開発プロセスへのコンプライアンスのシームレスな組み込みを図っています。

詳しくは当社のブログ投稿をご覧ください

安全のための設計（DNS）では不十分

2011 年、カーエレクトロニクスシステムの複雑度と数の増加を受けて、ISO 26262 という機能安全規格とそれに続くアップデートが作成されました。

ISO 26262 は、より汎用的な工業向け機能安全規格である IEC 61508 を翻案したものです。他の産業にも類似の規則が多数存在します。たとえば、鉄道の CENELEC EN 501128 規格、航空宇宙の DO-178B/C 規格、医療の IEC 60601 規格などです。

ISO 26262 への合理的なアプローチ

ISO 26262 の採決に関わる委員会のメンバーという特殊なポジションにある LHP は、最新の改訂事項や、規格の方向性について、徹底的に把握しています。LHP では自動車関連企業が初めて規格に準拠するための支援体制を完備しており、初期段階から適切な体制を構築する際の実践ガイダンスを行っています。

詳細はこちら

これらすべての安全規格に共通するのは、システムの主要な機能に関連する重大度や潜在的な危険を判断する、リスク基準のアプローチです。機能がハードウェアとソフトウェアのサブシステムに切り分けられる前に、初期のアーキテクチャー設計段階でリスクの識別と割り当てが行われます。この規格の第一の目標は、システムやデバイスの不具合による怪我や危害、死亡の発生を防止することです。不具合が避けられないものであれば、そのシステムは潔く停止しなくてはなりません。

ISO 26262 は、製品ライフサイクル全体を通じてハードウェアとソフトウェアの安全性の懸念事項に対して体系的に対処し文書化することによって、システムエンジニアリングの基準を補完するものです。

この規格は、安全要件のトレーサビリティや妥当性確認、検証のほか、統合、テスト、生産、メンテナンス、生産終了に関する考慮事項も含まれています。

これまで、安全性の設計は要件に関する一般的な作業の一部と考えられていました。しかし、ソフトウェアチームとハードウェアチームで要件を特定および追跡するだけでは不十分です。

「この ISO 規格は他のリスク関連規格とは異なる。それは、この規格が、製品の不具合のリスクとは違い、EE システムの誤動作に起因する人間への危害に注目しているからである。責任やしかるべき注意を実現するため、そういったリスクの低減には、ドキュメントの中にこれまで一度も行われてこなかった厳密な記述がどうしても必要となる」

Mike Bucala, Lead Engineer for Vehicle Systems Quality, **Daimler Trucks NA**

隔離された環境で設計を行う（つまりハードウェアチームとソフトウェアチームがサイロ化されて作業を行う）一般的な慣習では、ISO 26262で要求されるタイプの安全性の対象範囲を保証できません。要件管理やモデリング、IDE、テスト用の最高のツールを使っても、ライフサイクルのうちの上位レベルの設計フェーズの部分と下位レベルのコンポーネント作成や統合、テストの部分の間には、やはりギャップが生じる可能性があります。この問題はどうすれば解決できるでしょうか。

要件への一般的なアプローチの中に欠けている主なものは、フェーズ間でのトレーサビリティのリンクです。多くのツールは、特定のフェーズにおける要件管理とトレーサビリティについては優れた機能を持っていますが、フェーズ間のトレーサビリティのための監査可能な証跡をほとんど残しません。プロジェクトが完了したところで、総合的で完全なライフサイクルトレーサビリティの活動が、後から思いついた形で監査として行われます。このような結果を、ISO 26262では開発と意思決定、サポートツールの選択プロセス全体を通じた注意事項を文書化することによって回避しようとしているのです。

ISO 26262が提案している、より幅広い総合的なアプローチの一例が、リスク分析を行う際の故障モードと危険の区別に表れています。この規格では、ユーザーが製品やコンポーネントを操作する際のシステムの状況や環境を考慮したトップダウン型のアプローチから危険を考えることを要求しています。

Jama Connect ™ for Automotive を活用した開発能力の向上

自動車向け製品の開発のトップ企業は、チーム全体の足並みを揃えつつ、より迅速な製品の定義付けや変更管理、機能安全の検証を可能にするために、Jama Software を活用しています。Jama Connect for Automotive を使用すれば、お客様は 1 つの強力なプラットフォームで要件とリスク、テストをより確実に管理し、機能安全規格と規制を遵守しやすくなります。また Live Traceability により、マーケティング上の要件や製品の要件、製品仕様、安全上の要件、検証と妥当性確認用アーティファクト、さらには不具合まで、チームが最初から最後までリンクさせることが可能です。

Jama Connect for Automotive の詳細はこちら

ISO 26262:2018のアップデート内容

常に進歩し続けるという自動車のテクノロジーの特性を受けて、ISO 26262 では 2011 年のリリース以来の公式なアップデートが必然的に行われました。このアップデートは最終的に 2018 年末に行われたため、ISO 26262:2018 と呼ばれています。

以前は、この規格は重量の総合計が 3,500kg 以下の四輪の車両のみに適用されていました。

2018 年のアップデートでは、ISO 26262 の対象範囲が、オートバイ、トラック、バス、トレーラーおよびセミトレーラーを含むすべての路面走行車に拡大されました。変更内容の一部を以下に記載します。

オートバイ、トラックおよびバス

乗用車は自動車安全水準（ASIL）に準拠する必要がありますが、その一方 ISO 26262 の最新版では二輪車安全水準（MSIL）を導入しています。またそれにより、その相違を考慮して、オートバイの危害分析とリスクアセスメントも改変されています。

トラックとバスは主にサイズと質量が大きいことが特徴であるため、そうした要素は車両の制御性につながり、したがってリスクにさらされることになります。たとえば、大型トラックに貨物を積んでいる場合、完全に空の場合よりも、急な坂でのホイールスピンなどの問題が起きやすくなります。

また、トラックやバス、セミトレーラーなど、異なる車両にはすべて特有の用途（たとえば長距離輸送用のセミトラックと都市型バスなど）があり、使用される条件や環境も一般的に異なるため、ISO 26262 の第 2 版では個々のベース車両タイプを区別しています。たとえば制御性の点では、コンクリートトラックは未舗装の建設現場などにも耐えられる必要がありますが、バスでは通常そのような路面に遭遇することはありません。

ホワイトペーパー：Functional Safety Considerations for Semiconductor Development on Road Vehicles（路面走行車の半導体開発に関する機能安全上の考慮事項）

最新版の ISO 26262 規格における半導体関連の考慮事項の主要なトピックについて考察し、航空宇宙分野の半導体開発に関する類似のガイダンス（RTCA DO-2543）とこれらのトピックを比較対照します。

ホワイトペーパーを読む

機能安全とサイバーセキュリティ

自動車内のコネクテッドデバイスに関するセキュリティ上の懸念の高まりに対応し、ISO 26262 では機能安全とサイバーセキュリティの間に効果的なコミュニケーションチャネルを組み込んだ管理計画を要求しています。これらの必要なチャネルは、機能安全管理のレベルと製品開発のシステムレベルの両面で特定されています。

半導体に関するガイドライン

ISO 26262 の第 1 版には、自動車の用途に使用される半導体に関する具体的なガイドラインの記載がありませんでした。そのためいくつか混乱が生じたことで、多くの自動車関連チームが自社の半導体サプライヤーに対する機能安全要件を独自に作成することとなりました。今回の第 2 版では、新しいセクションで自動車の用途に使用される半導体部品と半導体技術に関するガイドラインと定義を記載しています。これによって不確実な点がなくなるだけでなく、自動車業界での半導体の設計、検証および妥当性確認の点で統一性が生まれます。今回のアップデートでは、半導体部品をパーツとサブパーツに階層的に分割し、各種の半導体部品に関する具体的なガイダンスと例を示しています。

意図した機能の安全性（SOTIF）

完全自動運転車を目前に控え、第 2 版に盛り込まれなかったことは「ニューラルネットワークを使用した自動運転システムで発生すると予想される、非系統的で偶発的な安全上の問題」です。ISO 26262 の第 2 版は自動運転システムについて直接的には対応していない一方で、新しい SOTIF 規格は補完的に安全性を取り扱うことを目的としています。SOTIF が対象とする範囲には、自動運転機能がそのときの状況を正しく把握できないことや、センサーからの入力や多種多様な環境条件に対する機能の堅牢性が不足していることなどがあります。

SOTIF の主な目標は、既知または未知の安全でないシナリオのリスクを最小限に抑えるための十分な緩和措置を講じることです。これは、SOTIF の検証および妥当性確認の作業を反復的に定義付けて実践し、リスクと改善方法を評価することによって達成されます。その結果が機能安全ライフサイクルにフィードバックされます。

この先、特に自動運転技術によって業界が成長および変化するにつれて、ISO 26262 規格にさらなるアップデートが行われることは間違いありません。

ツールの影響

ISO 26262 では、ソフトウェアツール、さらにはツールチェーンが、安全性が最重要視されるシステムに適合していることを確認する認定プロセスについて述べています。

Jama Connect ™は ISO 26262 認証済

Jama Connect は、ISO 26262（ASIL D）に従って安全性に関連する製品を開発していることにより、国際的に認知されたテスト機関 TÜV SÜD の認証を受けています。

すなわち、Jama Software のお客様は、時間をかけて自社で認定を受けなくても、TÜV SÜD の認証をもって、プロジェクトにおいてソフトウェアソリューションの認定を受けていることを主張できます。Jama Software は、その認証を受けた最初の SaaS およびアジャイルベンダーです。

この認証のメリットについて、詳しくはこちらをご覧ください

ツールの認証はそのツールの使われ方によって決まり、その結果として、ツールが安全性にどのような影響を及ぼすかが明確になります。たとえば、ツールの用途次第で、そのツールがハードウェアの不具合やソフトウェアのバグをシステムに持ち込む可能性があるかどうかです。

ツールチェーンの中でのツールの使われ方によって、そのツールが持ち込んだエラーが検知されるかどうかの可能性が決まります。ツールがエラーを持ち込んだり引き起こしたりする可能性と、開発プロセス中にエラーが検出される可能性の兼ね合いに基づいて、ツールまたはツール内のフローに信頼度レベルが割り当てられます。以前は、誰がこの信頼度レベルを割り当てるのかというところに混乱が生じていました。

ソリューションやベンダーが自社でツール信頼レベル（TCL）を設定していることもよくありますが、最終的にはそのツールを使用する会社が自社の責任で、意図する用途に基づいて TCL を定義することになります。

この規格の 2018 バージョンに従い、自動車用システムの部品の製作に用いられる開発ソフトウェアは、機能安全設計環境においてその作業を行うための認証を受ける必要があります。認証および分類の要件については、ISO 26262 第 8 部の第 11 条に記載されています。ソフトウェアツールは、目的に適合していれば資格認証を受けられます。

実施の戦略

ツールとプロセスの認証はいずれも、ISO 26262 などの安全規格を完全に満たすように実施する必要があります。

ツール（およびツールスイート）の認証を受ける方法のひとつは、共通の利用モデルを設定することです。もちろん、要件作成かモデリングや構成の管理かなど、ツールの用途によって利用モデルはそれぞれ異なります。

たとえば、あるプロジェクトの安全要件を満たすには、不具合やエラーがツールに持ち込まれ、検出され、緩和された経緯と、そういった問題を組織が提起して設計チームに伝達する手順に注視する必要があります。

プロセス面では、ISO 26262 認証を受けようとする多くの企業が、「プロセス実証」のパイロットプロジェクトにこの規格を実施し始めると思われます。このアプローチでは、規格に準拠する上で開発プロセスとツールスイートの両方に必要となる変更を重点的に行います。安全は強化したドキュメントや監査のチェックリストだけでできるものではないため、組織の考え方にも変化が必要となるかもしれません。

ISO 26262 に準拠した開発を今すぐ開始する

自動車全体を作る会社でも、電子システムやソフトウェアコンポーネントを作る会社でも、Jama Connect for Automotive はお客様の機能安全プロセスの簡略化を以下でサポートします。

- ISO 26262:2018、ASPICE、SEBoKなどの主要な業界規格や規制に沿ったフレームワーク
- 自動車関連の製造活動向けの手順ガイドと構成ガイド
- すべての作業成果物に関するドキュメントのエクスポート用テンプレート
- プラットフォームの妥当性確認に要する時間を短縮する機能安全キット
- 自動車関連テクノロジーに関する製品開発プロセスにソリューションを適合させるためのコンサルティングとトレーニング

Jama Connect for Automotive のソリューション概要を読む

組織における ISO 26262 の実施

他の規格と同様、ISO 2626 のプロセスを実施するには、以下に挙げるいくつかの基本的なステップを反復的に行う必要があります。

01

既存のプロセスとツールを確認する、または「自分たちは今どこにいるのか」と自問する。

現在組み込まれているハードウェアおよびソフトウェア開発プロセスとツールチェーンを見直します。開発するアプリケーションをしっかり理解し、安全性の観点から信頼度を割り当てます。

02

ギャップ分析を行う、または「自分たちはどこへ行きたいのか」と自問する。

ギャップ分析またはインパクト分析を行って現状の課題をつきとめ、効率性の改善を進めます。この作業は多くの場合、モデルベースの設計テクニックを用いて行います。

03

トレーニングと教育の計画を立てる。

前のステップでつきとめたギャップに対応するための安全設計のトレーニングと教育を行います。

04

実践的なデプロイのサポートを実施する。

ここまでのステップで得た知識を、具体的なパイロットプロジェクトに活かします。そのためには、要件のトレーサビリティ、モデリング、シミュレーション、コード生成、検証、妥当性確認、ツールの認証、システム統合といった幅広い領域での支援が必要となります。

ベストプラクティスの遵守

ここで述べている機能安全への総合的なアプローチは、協働、トレーサビリティ、妥当性確認と検証（V&V）、リスク分析と緩和、ツールチェーン内での慎重な統合といった、優れたシステムエンジニアリングプロセスの主要な要素を具体的に示したものです。これらの要素についてひとつずつ検討してみましょう。

Rimac、Jama Connect™を活用して自動車業界に空前のイノベーションを実現

Rimac Automobili は、車両デザインにおいて世界のトップを走り続けています。同社の急速な勢いは、複雑な開発プロセスとも相まって、ベストプラクティスに準拠できない問題やコンプライアンスに関する悩みが生じる危険性を生んでいました。そんなときに、Jama Connect と出会ったのです。

顧客事例を読む

今日のカーエレクトロニクスシステムの共同開発における公式・非公式のやりとりや決定のポイントを記録しておくことが、ISO 26262 に関するドキュメント作成では重要です。しかし、チームのメンバーやサプライチェーン内の世界中のパートナーとのそういった共同作業は、できる限り通常のワークフローを邪魔しない形で行う必要があります。

機能安全を確保するためには、ライフサイクルプロセス全体を通じた要件や機能、実装、およびテストの明確なトレーサビリティが必要となります。ツールのベンダーにとっては、トレーサビリティがあることで、新バージョンのツールが顧客の既存のソフトウェアやハードウェアを壊さないことを確認できます。

トレーサビリティによって、当然のことながら要件の検証の道筋もできます。しかし、システムの妥当性確認も重要です。このふたつを合わせた V&V（妥当性確認と検証）によって、エンジニアが正しいものを作っていること、またそれを正しく作っていることを、それぞれ確認することができます。機能安全に注力するということは、V 字モデルライフサイクルの分解と統合のフロー全体を通じた V&V に、規格に準拠しない開発プロセスでは存在しないある一定レベルの厳密さと一貫性が要求される可能性があることを意味します。

機能安全は、リスクの危険性を判断、分析および緩和することによって達成されます。ISO 26262 では、許容可能なリスクレベルをシステムやコンポーネントに割り当てて、緩和プロセス全体を文書化する方法について詳しく述べています。この規格では、許容可能で統計的に受け入れられるレベルまでリスクを軽減する優れた設計の実践を通じた、潜在的な危険性の緩和策に取り組んでいます。

リスクの緩和策には、具体的なツールのプロセスと使用法の両方が含まれます。そのために、ツールスイートの安全機能を立証または証明することがツールのベンダーに求められる場合があります。一般的には、この規格に則って自社のツールを使用した場合に問題が起きないことをベンダーが顧客に納得させる必要があります。ISO 26262 で、安全性最重視のシステムにそのソフトウェアツール、さらにはツールチェーンが最適であることを確認する認定プロセスについて述べているのはそのためです。

機能安全を確保するためには、ライフサイクルプロセス全体を通じた要件や機能、実装、およびテストの明確なトレーサビリティが必要となります。ツールのベンダーにとっては、トレーサビリティがあることで、新バージョンのツールが顧客の既存のソフトウェアやハードウェアを壊さないことを確認できます。

自動車開発のスピードアップを図る

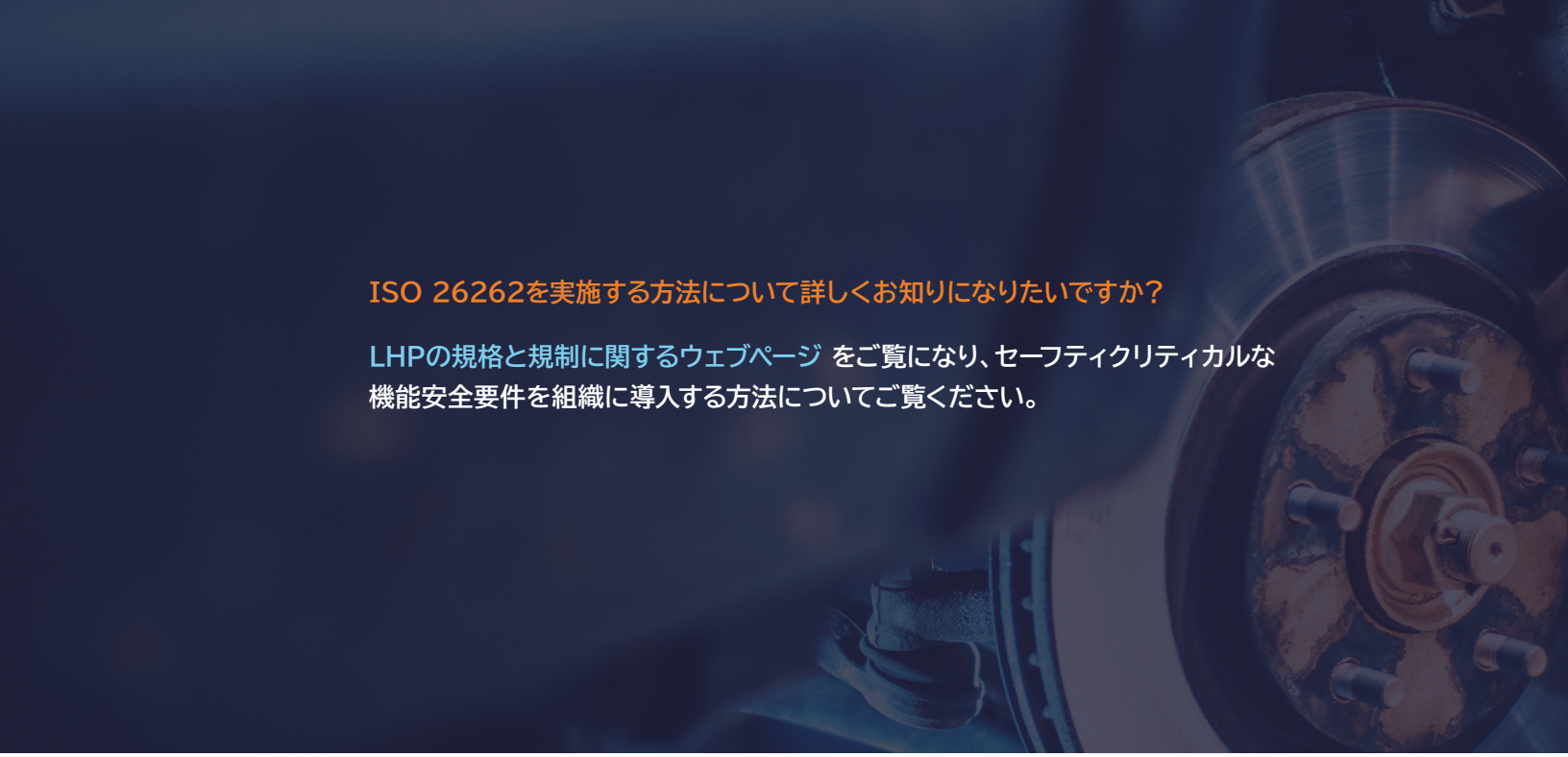
カーエレクトロニクスのハードウェアとソフトウェアの設計者は、自身の開発作業全体で ISO 26262 のプロセスをどのように実施するかを理解する必要があります。一方コンポーネント部品やツールのベンダーは、設計者の活動を支援するため、ISO 26262 で要求される認証作業を理解する必要があります。

Jama Connect for Automotive では、開発チームがひとつのプラットフォームで、安全性が最重要視される製品を製作しつつ、ISO 26262 と Automotive SPICE（ASPICE）という業界標準に準拠したフレームワークとテンプレートによって製品化までの時間を短縮することが可能となります。

当社のプラットフォームでは次のようなことが可能になります。

- 要件のスコープを明確に定め、要件を直接的に連携させることで、信頼度を向上して価値創出までの時間を短縮する
- 構成テンプレートとエクスポート用テンプレートを定義づけて合理化することで、導入にかかる時間を短縮する
- システムとテンプレートをフレキシブルに変更することで、組織に固有のニーズに Jama Connect を適合させる
- 人材やプロセスとデータに沿ったトレーニングを行うことで、導入を促し、チームへの変更の影響を抑える

自動車開発におけるチームの課題を解決する Jama Connect for Automotive の詳細については、当社のウェブサイトでご覧ください。



ISO 26262を実施する方法について詳しくお知りになりたいですか？

LHPの規格と規制に関するウェブページ をご覧になり、セーフティクリティカルな機能安全要件を組織に導入する方法についてご覧ください。

JAMA SOFTWARE について

Jama Software は、要件やリスク、テストの管理のための最先端のプラットフォームを提供します。Jama Connect をお使いいただければ、エンジニアリングチームのサイクルタイムの改善、品質の向上、コンプライアンスにかかる時間と商品化までの時間の短縮が実現します。Jama Software の顧客ベースは 30 か国 600 組織以上におよび、さらに増え続けています。航空宇宙・防衛、医療機器開発、自動車、半導体、ソフトウェア開発、金融サービス・保険、工業生産などの業界のお客様に採用いただいています。
詳細については、当社のウェブサイト jamasoftware.com. をご覧ください。

LHP について

2001 年に創立された LHP は、20 年近くにわたり、運輸業界にエンジニアリングサービスとテクノロジーインテグレーションを提供しています。LHP は、運輸業界のさらなる発展への寄与と、機能安全の実施を通じたより安全でスマートな、よりコネクテッドな世界の創出に取り組んでいることで、お客様の信頼感につながっています。LHP では、自動車業界の最新規格とベストプラクティスをベースに構築した、最先端のトレーニングと実践コンサルティングとインプリメンテーション、専用のオンサイトリソース、テクノロジーソリューション、エンジニアリングサービスを提供することで、安全な自動車業界の創出に取り組んでいます。
詳細については、LHP のウェブサイト lhpes.com をご覧ください。