TISAX
ENX ASSOCIATION

TISAX参加企業のためのハンドブック

TISAXアセスメントプロセスを実施し、結果をパートナー企業と共有する

発行

ENX協会
フランス1901年法に基づき設立
フランス ブローニュ＝ビヤンクール郡 登録番号 w923004198

所在地
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, France
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Germany

著者

Florian Gleich

連絡先

tisax@enx.com
+49 69 9866927-77

バージョン

日付:	2023-12-07
バージョン:	2.7
分類:	Public
ENX doc ID	602-JP

著作権表示

目次

1. 概要

1.1. 目的

TISAX（Trusted Information Security Assessment Exchange）へようこそ。

貴社のパートナー企業からの要請で、貴社の情報セキュリティ管理が、「情報セキュリティ審査」（ISA）の要求事項に従い定められた水準を満たしていることを証明するよう求められました。そして今、貴社はこの要請に応える方法を知りたいと考えています。

本資料は、貴社がパートナー企業からの要求を満たせるようにする、またはパートナー企業からの要求前にあらかじめ備えたりできるようにすることを目的としています。

本資料では、TISAX審査に合格するために必要な手順、および審査結果をパートナー企業と共有するにあたって必要な手順を解説します。

情報セキュリティマネジメントシステム（ISMS）は、構築・維持だけでも複雑なタスクが課されます。パートナー企業に対し、貴社の情報セキュリティマネジメントの適切性を証明するのは、より一層複雑なプロセスとなります。本資料は、貴社の情報セキュリティ管理を支援するためのものではありません。貴社による情報セキュリティ管理の取り組みを、パートナー企業に対して可能な限り簡単に証明できるようにすることを目的としています。

1.2. 対象範囲

本資料は、貴社が参加する可能性のあるすべてのTISAXプロセスに適用されます。

本資料には、TISAXプロセスを進めるにあたって必要な情報がすべて含まれています。

本資料には、審査の中核をなす情報セキュリティ要求事項への対処方法に関する、若干のアドバイスが記載されています。しかし、全体として、情報セキュリティ審査に合格するために何が必要かを伝えることを目的としているわけではありません。

1.3. 対象者

本資料の主な対象者は、「情報セキュリティ審査」（ISA）の要求事項に従い定められた情報セキュリティ管理水準を満たしていることを証明する必要のある企業、または証明したいと考えている企業です。

本資料に記載されている情報は、TISAXプロセスの積極的な取り組みの開始時点から活用できます。

また、サプライヤーに対し、定められた水準の情報セキュリティ管理の証明を求める企業にとっても有益です。本資料によって、貴社の要求を満たすために何をする必要があるかを、サプライヤーが把握できるためです。

1.4. 構成

まずはTISAXについて簡単に紹介した後、すぐに「どのようにすれば良いか」の解説に移ります。プロセスを進めるために必要なことすべてが、知るべき順序で記載されています。

本資料の所要時間の目安は、75分から90分です。

1.5. 本資料の使い方

いずれは、本資料の内容をすべて理解したいと考えるようになると思われます。適切な準備として、まず本資料全体をお読みになることをお勧めします。

本資料は、TISAXプロセスにおける三つの主要なステップに沿って構成されています。必要なセクションに進み、後で残りを読むことも可能です。

本資料は、理解を深めるためにイラストを使用しています。イラストの色には、意味が付与されている場合あります。そのため、本資料は、パソコン画面か、カラー印刷された状態でお読みになることをお勧めします。

ご意見をお聞かせください。本資料の内容に不足や、理解しにくい箇所がありましたら、ぜひお知らせください。皆様のご意見は、私たちにとっても、今後本資料を読む方たちにとっても大切です。

すでに旧版のTISAX参加企業ハンドブックをご利用の方は、本資料末尾の以下の箇所をご参照ください：セクション 8. 文書履歴。

1.6. お問い合わせ

以下の連絡先で、TISAXのプロセスに関するご案内や、ご質問への回答を行っています。

メールアドレス： tisax@enx.com
電話番号： +49 69 9866927-77

ドイツ国内での通常の営業時間（UTC+01:00）が、受付時間となります。

従業員は皆、英語とドイツ語を話します。イタリア語が母国語の従業員もいます。

以下のセクションもご確認ください：セクション 7.13. 附録：クレーム管理。

1.7. TISAX参加企業のためのハンドブックをご利用いただける他の言語および形式

TISAX参加企業のためのハンドブックは、以下の言語および形式でご利用いただけます：

言語	バージョン	形式	リンク
英語	2.7	オンライン	https://www.enx.com/handbook/tisax-participant-handbook.html
		オフライン	https://www.enx.com/handbook/tisax-participant-handbook-offline.html
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf
ドイツ語	2.7	オンライン	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
		オフライン	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf

言語	バージョン	形式	リンク
フランス語	2.7	オンライン	https://www.enx.com/handbook/tph-fr.html
		オフライン	https://www.enx.com/handbook/tph-fr-offline.html
		PDF	https://www.enx.com/handbook/tph-fr.pdf
中国語	2.7	オンライン	https://www.enx.com/handbook/tph-cn.html
		オフライン	https://www.enx.com/handbook/tph-cn-offline.html
		PDF	https://www.enx.com/handbook/tph-cn.pdf
スペイン語	2.7	オンライン	https://www.enx.com/handbook/tph-es.html
		オフライン	https://www.enx.com/handbook/tph-es-offline.html
		PDF	https://www.enx.com/handbook/tph-es.pdf
日本語	2.7	オンライン	https://www.enx.com/handbook/tph-jp.html
		オフライン	https://www.enx.com/handbook/tph-jp-offline.html
		PDF	https://www.enx.com/handbook/tph-jp.pdf
ブラジルポルトガル語	2.7	オンライン	https://www.enx.com/handbook/tph-pt.html
		オフライン	https://www.enx.com/handbook/tph-pt-offline.html
		PDF	https://www.enx.com/handbook/tph-pt.pdf
イタリア語	2.7	オンライン	https://www.enx.com/handbook/tph-it.html
		オフライン	https://www.enx.com/handbook/tph-it-offline.html
		PDF	https://www.enx.com/handbook/tph-it.pdf
韓国語	2.7	オンライン	https://www.enx.com/handbook/tph-kr.html
		オフライン	https://www.enx.com/handbook/tph-kr-offline.html
		PDF	https://www.enx.com/handbook/tph-kr.pdf

重要事項:

オリジナル版は英語です。
他言語版は、すべて英語版から翻訳されています。
内容が疑わしい場合は、英語版をご確認ください。

1.7.1. 邦訳について

本資料、TISAX参加企業のためのハンドブックは、英語版から翻訳されています。

TISAXの基礎となる資料は、すべて英語で作成されています（すべての契約書、TISAX審査機関に対する要求事項等）。そのため、貴社のパートナー企業や審査機関は、TISAX特有の用語について、英語版の用語を使用する可能性があります。

そこで、TISAX参加企業のためのハンドブックでは、翻訳にあたり、TISAXの用語は英語の原文のまま

記載するか、日本語訳の直後に括弧で英語の用語を併記しています。

1.7.2. オンライン版について

各セクションには、固有のID（「ID1234」形式）が割り当てられています。
IDは言語に関係なく、特定のセクションを参照します。

以下の方法で、特定のセクションにリンクできます。

- セクションのタイトルを右クリックして、リンクをコピー
- セクションのタイトルをクリックして、ブラウザのアドレスバーからリンクをコピー

ほとんどのイラストは、デフォルトの表示よりも大きなサイズで確認できます。図をクリックすると、拡大されたイラストが開きます。

1.7.3. オフライン版について

オフライン版では、オンライン版のほとんどの機能が使えます。特記事項として、イラストはHTMLファイルに埋め込まれています。オフライン版は、1ファイルだけで利用できます。

オンライン版にはあって、オフライン版で使えないのは以下の機能です。

- 拡大画像
- オンライン版オリジナルのフォント
  フォントは、ブラウザのデフォルト設定で表示されます

1.7.4. PDF版について

パソコンでPDF版を使用する場合でも、リファレンスはすべてクリックできます。しかし、PDF版を印刷した場合は、ページ番号などが印刷されないため、リファレンスのページはご自身で調べていただく必要があります。

2. 導入

以下のセクションでは、TISAXのコンセプトをご紹介します。

お急ぎの場合は、このセクションを飛ばして次のセクションから読むことも可能です。セクション 4.3. 登録準備。

2.1. なぜTISAXなのか?

なぜあなたはこの資料を読んでいるのでしょうか?

この問いに答えるために、まずはビジネス全般、特に情報保護について考えてみましょう。

パートナー企業の担当者を想像してみてください。担当者は機密情報を持っています。この担当者は、機密情報をサプライヤーである貴社と共有したいと考えています。貴社とパートナーが提携することで、価値が生まれます。この価値創出において、パートナー企業が貴社と共有する情報は、重要な役割を果たしています。だからこそ、パートナー企業はこの情報を適切に保護したいと考えています。貴社が、この機密情報を自社のものと同じように、細心の注意を払って扱っていることを確認したいと望んでいます。

しかし、自分たちの情報が適切に管理されていることを、どうすれば確認できるでしょうか。貴社を単に「信じる」だけでは不十分です。パートナー企業は、その証拠となるものを確認したいのです。

ここで二つの疑問が生じます。まず、情報の「安全な」取り扱いとは、誰が定義するのでしょうか?そして、どうすれば安全であることを証明できるのでしょうか?

2.2. 誰が「安全」を定義するのか?

この疑問に直面するのは、貴社とパートナー企業が初めてではありません。ほとんどの企業が答えを模索する必要に迫られ、そして得た結論の大半には、共通点が存在します。

問題の解決策が標準化されていれば、同じ解決策を毎回独自に考える必要はなくなり、すべてをゼロから作成する負担が軽減されます。規格の定義は大変な労力を要しますが、一度定義してしまえば、その後の利用者すべてが恩恵を受けられます。

情報保護の観点で何が正しいのかについては、確かにさまざまな見解があります。しかし、前述の利点から、ほとんどの企業は規格を定めています。規格とは、ある課題に対する、実績のあるベストプラクティスの結晶です。

貴社の場合、ISO/IEC 27001（情報セキュリティマネジメントシステム、ISMS）等の規格を導入し、実施することで、機密情報を安全に取り扱う最先端の方法を確立できます。このような規格があれば、毎回土台から作り直す必要がなくなります。さらに重要なのが、規格があれば、二社が機密情報を交換する必要がある際に共通の基盤を利用できるという点です。

2.3. 自動車業界の回答

あらゆる業界にあてはまる規格は、特定の業界を対象としないソリューションとして設計されている性質上、自動車会社に特有のニーズに合わせられているわけではありません。

一昔前、自動車業界は、より自動車業界特有のニーズに合った規格を調整し、定義することなどを目的とした団体を結成しました。VDA（Verband der Automobilindustrie）もその一つです。情報セキュリティを扱うワーキンググループで、複数の自動車企業が検討を重ねたところ、既存の情報セキュリティ管理規格にも同じような調整が必要であるという結論に達しました。

これらメンバー企業間の共同の取り組みにより、自動車業界で広く受け入れられている情報セキュリティ要求事項を網羅した質問票が作成されました。この質問票は「情報セキュリティ審査」（ISA）と名付けられました。

この取り組みによって、「『安全』を誰が定義するのか」という疑問に対する答えが得られました。自動車業界は、VDAを通じて、メンバー企業にこの疑問への回答を提示しています。

2.4. 安全であることの証明を効率的に行うために

ISAを社内目的のみに使用する企業もあれば、サプライヤーの情報セキュリティ管理の成熟度を審査するために使用する企業もあります。ビジネス関係の観点から、自己審査のみで十分な場合もあります。一方で、サプライヤーの情報セキュリティ管理について、完全な審査（オンサイト監査を含む）を実施する企業もあります。

情報セキュリティ管理の必要性に関する一般の認識が高まる中で、情報セキュリティを審査するためのツールとして、ISAが広く採用されるようになり、多くのサプライヤーがさまざまなパートナー企業から同様の要請を受けるようになりました。

しかし、パートナー企業間で適用基準は依然として異なっており、解釈もさまざまでした。その中でサプライヤーが証明すべきことは基本的に同じであり、証明方法が異なるだけでした。

そして、サプライヤーは、パートナー企業から情報セキュリティの管理水準の証明を求められるたびに対応を繰り返さなければならず、不満は大きくなってきました。監査人ごとに、同じ情報セキュリティ管理策を何度も提示しなければならないというのは、単純に非効率的だったのです。

では、効率化するためにはどうすればいいのでしょうか。ある監査人への報告書を、別のパートナーに再利用できるようにすれば、改善するのではないでしょうか?

ISAの維持を担当するENXワーキンググループに所属するOEMとサプライヤーは、自分たちのサプライヤーの不満に耳を傾けました。そのようにして、自分たちのサプライヤーだけでなく、自動車業界のあらゆる企業が利用できる形で、「安全であることをどうすれば証明できるか? 」という質問に対する回答が確立したのです。

この回答が、TISAX、“Trusted Information Security Assessment Exchange”（🇯🇵「情報セキュリティの審査基準」）です。

3. TISAXのプロセス

3.1. 概要

TISAXのプロセスは通常、[1]貴社のパートナー企業が、「情報セキュリティ審査」（ISA）の要求事項に従い定められた情報セキュリティ管理の水準を、貴社が満たしていることを証明するよう要請することで開始します。この要請に応えるには、3段階からなるTISAXプロセスを完了する必要があります。このセクションでは、貴社が実施することを求められる、これら三つのステップについての概要を説明します。

TISAXプロセスは、以下の3ステップで構成されています。

図 1. TISAXプロセスの概要

1. ステップ1
   登録
2. ステップ2
   審査
3. ステップ3
   共有

1. 登録
   我々が貴社に関する情報を収集し、審査を行う上で何が必要かを検討します。
2. 審査
   TISAX審査機関が実施する審査を受けます。
3. 共有
   審査結果をパートナーと共有します。

各ステップには、さらに細かい手順（サブステップ）が存在します。サブステップについては、後述の3セクションで解説します。

注意事項:

TISAXの審査結果が出るまでの期間については、お伝えしたいのですが、確実な予測は不可能であることをご理解ください。TISAXプロセス全体にかかる期間は、非常に多数の要因に左右されるためです。企業の規模や審査目的は多岐にわたり、情報セキュリティマネジメントシステムの準備状況もそれぞれ異なるため、確実な予測は不可能となっていることをご承知おきください。

3.2. 登録

最初のステップは、TISAXへの登録です。

TISAXへの登録の主な目的は、貴社に関する情報の収集です。TISAXでは、オンラインの登録プロセスを通じて、貴社から情報を提供していただきます。

この登録は、その後のすべてのステップの前提条件となります。登録には料金がかかります。

オンライン登録にあたって

- ご連絡先とご請求先情報をお伺いします。
- また、当社の利用規約に同意していただきます。
- 情報セキュリティ審査のスコープを定義できます。

このステップについては、以下を参照してください：セクション 4. 登録（ステップ 1）。

以下のセクションにオンライン登録プロセスの詳細が記載されています：セクション 4.5. オンライン登録プロセス。 すぐに開始する場合は、次のページをご利用ください：enx.com/en-US/TISAX/.

3.3. 審査

2番目のステップは、情報セキュリティ審査の実施です。

審査には、次の四つのサブステップが存在します。

a. 審査の準備
審査には準備が必要です。準備の範囲は、貴社の情報セキュリティマネジメントシステムの現在の成熟度によって異なります。準備は、ISAカタログに基づいて実施する必要があります。

b. 審査機関の選択
TISAX審査機関を選択する必要があります。

c. 情報セキュリティ審査
審査機関は、貴社のパートナー企業の要求事項に適合する審査スコープに基づいて、審査を実施します。審査プロセスは、最低でも初回監査が必要です。
貴社がすぐに審査に合格しない場合、審査プロセスで追加の手順が必要になる場合があります。

d. 審査結果
貴社が審査に合格すると、審査機関から正式なTISAX審査報告書が提供されます。審査結果に伴い、TISAXラベルも付与されます。[2]

このステップの詳細については、以下のセクションを参照してください：セクション 5. 審査（ステップ 2）。

3.4. 共有

三つ目の最後のステップは、審査結果のパートナーとの共有です。TISAX審査報告書の内容は、レベル別に構成されています。
パートナーがアクセスできるレベルは、貴社が決めることができます。

審査結果は3年間有効です。貴社がまだこのパートナーのサプライヤーである場合は、三つのステップを再度実施する必要があります。[3]

このステップの詳細については、以下のセクションを参照してください：セクション 6. 共有（ステップ 3）。

TISAXの基本的な流れはご理解いただけたと思いますので、次に各ステップの進め方についてご説明します。

4. 登録（ステップ 1）

この登録セクションを読むのにかかる時間は、およそ30分から40分です。

4.1. 概要

最初のステップは、TISAXの登録です。この登録は、その後のすべてのステップの前提条件となります。

以下のセクションで、登録の手順について説明します。

1. まず、重要な新しい用語について解説します。
2. 次に、オンライン登録の準備として、何をすべきかをアドバイスします。
3. 次に、オンライン登録の手順を説明します。

4.2. 貴社はTISAXの参加企業です

まず、理解しておくべき新しい用語を紹介します。貴社は「サプライヤー」という立場です。本資料を読んでいるのは、「顧客」の要求を満たすためです。しかし、TISAXは、「サプライヤー」と「顧客」という二つの役割を区別しません。TISAXにとっては、登録した全企業が「参加企業」となります。貴社と貴社のパートナー企業は、情報セキュリティ審査結果の共有に「参加」するのです。

図 2. TISAX参加企業になるための登録

1. 貴社
2. TISAX登録
3. TISAX参加企業

始めるにあたり、二つの役割を区別するため、サプライヤーである貴社を「アクティブ参加企業」と呼び、パートナーのことを「パッシブ参加企業」と呼びます。「アクティブ参加企業」は、TISAXの審査を受け、審査結果を他の参加企業と共有します。「パッシブ参加企業」は、貴社にTISAXの審査を受けるよう依頼した企業です。「パッシブ参加企業」は、審査結果を受け取ります。

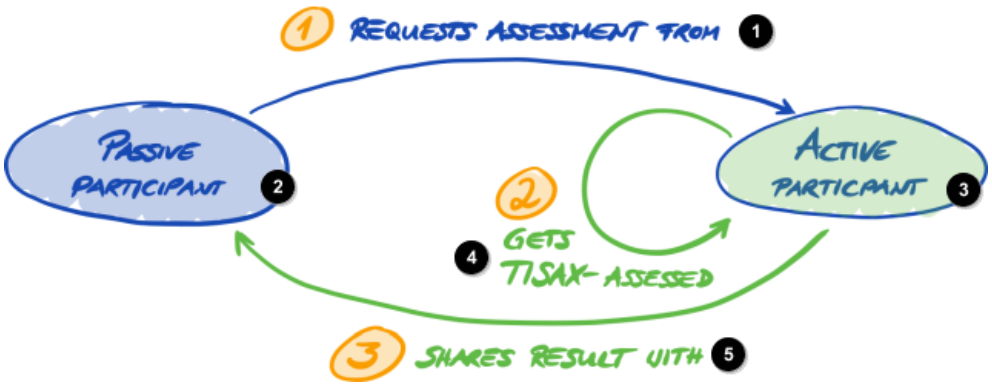


図 3. パッシブ参加企業とアクティブ参加企業

1. 1. 審査を要求
2. パッシブ参加企業
3. アクティブ参加企業
4. 2. TISAX審査を受ける
5. 3. 結果を共有

どの企業も、いずれの役割にもなることが可能です。審査結果をパートナー企業と共有すると同時に、自社のサプライヤーにTISAX審査を受けるよう要請することもできます。

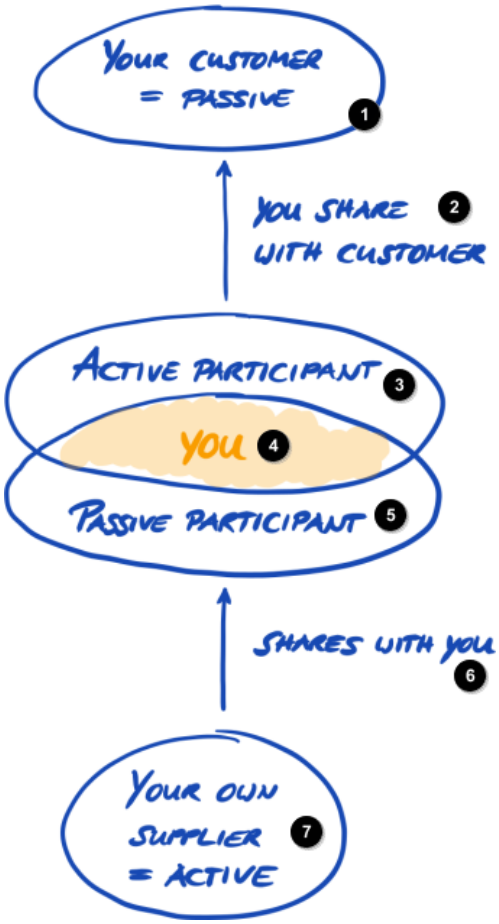


図 4. TISAXの参加企業は、アクティブ参加企業でありながら、同時にパッシブ参加企業にもなれます。

1. 貴社の顧客
= パッシブ
2. 顧客と共有
3. アクティブ参加企業
4. 貴社
5. パッシブ参加企業

6 貴社と共有

7 貴社のサプライヤー
= アクティブ

特に、保護を必要とする貴社のパートナー情報も扱っているサプライヤーに対しては、TISAX審査を要請することを強く推奨します。

4.3. 登録準備

このセクションでは、登録の準備に関する推奨事項について説明します。登録プロセスそのものについては、以下のセクションで詳しく説明します：セクション 4.5. オンライン登録プロセス。

オンライン登録プロセスを開始する前に、以下を実施することを強くお勧めします：

- 事前の情報収集
- それに基づく必要な決定

4.3.1. 法的基盤

通常、二つの契約を締結する必要があります。一つ目が、貴社とENX協会間で締結する契約「TISAX参加規約」（TISAX参加一般取引条件）です。二つ目が、貴社とTISAX審査機関の間で締結する契約です。登録プロセスでは、最初の契約のみを確認します。

TISAX参加一般取引条件は、貴社とENX協会の相互関係および、貴社と他のTISAX参加企業との関係を規定します。契約には、全員の権利と義務が規定されています。大半の契約書に見られる一般的な条項のほか、TISAXプロセスで共有、取得される情報の取り扱いについても詳細に規定されています。規則の主な目的は、TISAXの審査結果の機密保持です。すべてのTISAX参加企業が同じ規則に従うため、（パッシブ参加企業の）パートナー企業による、TISAX審査結果の適切な保護を期待できます。

オンライン登録のかなり早い段階で、TISAX参加一般取引条件に同意していただきます。これは実際の契約なため、オンライン登録プロセスを開始する前に、TISAX参加一般取引条件を読むことをお勧めします。その理由の一つとして、あなたの社内における役割によっては、社内または社外の弁護士からの許可が必要なことが挙げられます。

「TISAX参加規約」は、ENX協会ウェブサイトの以下のページからダウンロードできます：[4]
enx.com/en-US/TISAX/downloads/

PDFは、以下のリンクから直接ダウンロードできます。
enx.com/tisaxgtcen.pdf

オンライン登録にあたり、次の二つの必須チェックボックスにチェックを入れていただきます。

☒ We accept the TISAX Participation General Terms and Conditions （当社は、TISAX参加規約に同意します。）

☒ We confirm knowledge of Applicant’s release of Audit Providers’ professional duties of secrecy acc. to Sec. IX.5. and X.3 of the TISAX Participation General Terms and Conditions; （当社は、TISAX参加規約の第IX.5項および第X.3項に基づき、申請者が、審査機関の職業上の守秘義務を解除することに同意します。）

TISAX審査機関には公認会計士も存在するため、二つ目のチェックボックスを設けています。公認会計士には、職業上の守秘に関する特別な要求事項が課せられています。通常、この職業上の守秘に関する特別な要求事項により、審査機関の公認会計士が我々と情報を共有することは禁止されています。これにより、ENX協会がガバナンス面で必要とする、管理上の選択肢が取れなくなってしまうため、こ

の要求事項の解除を求めています。チェックボックスにチェックを入れる前に、条項をよくお読みください。

通常、機密情報を扱う人物との間で秘密保持契約（NDA）を必要としている場合は、一般取引条件の各セクションをご確認いただくことで、懸念はすべて解消できます。また、基本的に、ENX協会に機密情報を提供する必要はありません。

最後に、このシステムは、全員が同じルールを受け入れることを前提としていることをご理解ください。したがって、追加の規約を受け入れることはできません。[5]

4.3.2. TISAXの審査スコープ

TISAXプロセスの第2のステップでは、TISAX審査機関が情報セキュリティ審査を実施します。審査機関は、審査スコープを把握する必要があります。それに伴い、貴社による「審査スコープ」の定義が必要です。

「審査スコープ」では、情報セキュリティ審査の範囲を示します。簡単に言えば、審査スコープには、パートナー企業の機密情報を取り扱う、貴社の要素がすべて含まれます。審査スコープは、審査機関のタスクの、主な対象を示していると捉えることも可能です。審査機関の審査対象を規定するのが、審査スコープです。

審査スコープが重要な理由として、主に次の二つを挙げられます。

a. パートナー企業の要求を満たす審査結果を得るには、審査スコープに、パートナー企業の情報を扱う貴社の要素すべてが含まれている必要があります。
b. TISAX審査機関が意義のあるコスト計算を行うためには、審査スコープの正確な定義が不可欠です。

重要事項:

ISO/IEC 27001とTISAXの比較

まず、次の2種類のスコープを区別する必要があります。
1） 情報セキュリティマネジメントシステム（ISMS）のスコープ
2） 審査のスコープ
この二つは必ずしも同一ではありません。

ISO/IEC 27001認証では、ISMSの適用スコープを（「適用範囲定義書」で）定義します。ISMSのスコープ全体を、貴社が自由に決められます。ただし、審査スコープ（または「監査スコープ」）は、ISMSのスコープと同一でなければなりません。

TISAXでは、ISMSも定義していただく必要があります。しかし、異なる審査のスコープを定義することも可能です。

ISO/IEC 27001認証では、ISMSのスコープをどのように定義するかによって、審査のスコープを自由に定義できます。

対照的に、TISAXでは、審査のスコープはあらかじめ定義されています。 審査のスコープは、ISMSのスコープよりも狭めることができますが、ISMSのスコープを逸脱することはできません。

4.3.2.1. スコープの記述

スコープの記述では審査スコープを定義します。スコープの記述では、次の二つのスコープタイプから一つを選択する必要があります。

1. Standard scope （標準スコープ）
2. Custom scope （カスタムスコープ）
    a. Custom extended scope （カスタム拡張スコープ）
    b. Full custom scope （フルカスタムスコープ）

次のセクションでは、標準スコープについて解説します。99%以上の参加企業にとって、標準スコープが適切な選択です。したがって、カスタムスコープについては、以下のセクションでのみ説明します：セクション 7.8. 附録：カスタムスコープ。

4.3.2.2. 標準スコープ

標準スコープの記述は、TISAX審査の基礎となります。他のTISAX参加企業は、標準スコープの記述に基づく審査結果のみを受け入れます。

標準スコープの記述はあらかじめ定義されており、変更はできません。

標準スコープの大きなメリットは、自分で定義を考える必要がないことです。

以下が標準スコープの記述（バージョン2.0）です。

The TISAX assessment scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.
The assessment is conducted at least in the highest assessment level listed in any of the listed assessment objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

TISAXの審査スコープでは、審査のスコープが定義されます。審査の対象には、リストに記載された拠点の、審査を受ける組織の責任下にある、リスト内の審査目的で定められた、保護対象および保護目標のセキュリティに関するすべてのプロセス、手順およびリソースが含まれます。
リスト内の審査目的のいずれにおいても、記載された中で最も高い審査水準以上で審査は行われます。リスト内の審査目的に記載されたすべての審査基準が、審査の対象となります。

標準スコープを選択することを強く推奨します。TISAX参加企業はすべて、標準スコープに基づく情報セキュリティ審査結果を受け入れます。

4.3.2.3. スコープの設定

スコープタイプを定義したら、次に、どの拠点を審査スコープに含めるかを決定します。

貴社が小規模（1拠点）であれば、この作業は簡単です。審査スコープに、貴社の拠点を追加してください。

貴社の規模が大きい場合は、複数の審査スコープを登録することも可能です。

一つのスコープにすべての拠点を登録すると、次のようなメリットがあります。

- 審査報告書、審査結果、有効期限が一つになります。
- TISAX審査機関は、貴社の中心的なプロセス、手順、リソースを一度だけ審査すれば良いため、審査のコストを削減できます。

一方、スコープが一つだけの場合、以下のようなデメリットもあります。

- すべての拠点に同じ審査目的を設定する必要があります。
- TISAX審査機関が全拠点を審査するまで、審査結果は得られません。これは、審査結果を急いで必要としている場合などに問題となる可能性があります。
- 審査結果は、すべての拠点が審査に合格するかどうかで決まります。拠点の一つでも不合格だと、審査結果が合格になりません。これを回避するには、a） スコープからその拠点を削除し、b） 問題を解決して、c） スコープ拡張審査で後から拠点を追加する必要があります。

4.3.2.4. スコープの調整

スコープを一つだけにするか、複数にするかは、貴社だけが決められる選択です。ただし、決めかねている場合は、以下のフロ⊠ーチャートの質問が役に立つかもしれません。

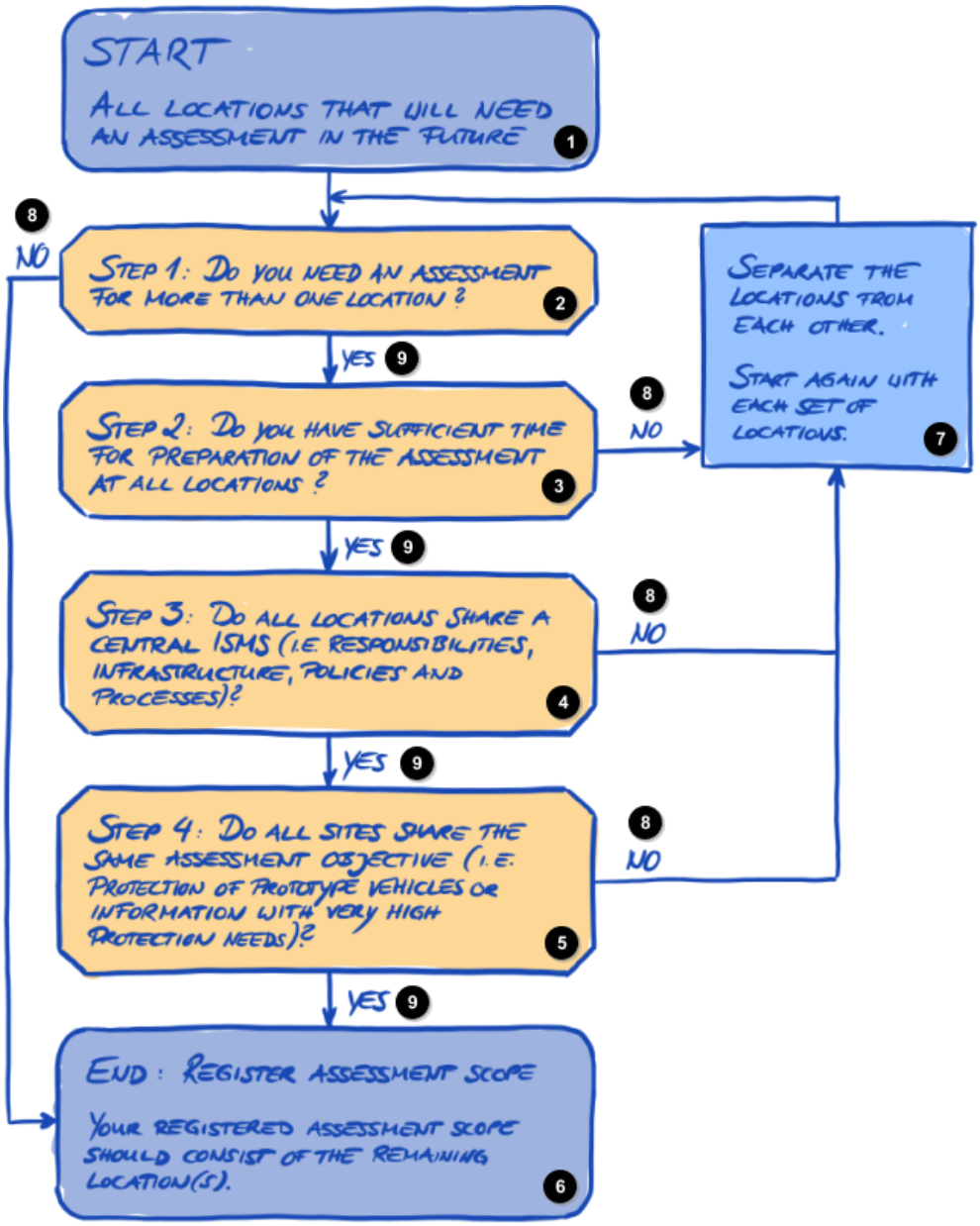


図 5. スコープを決めるためのフローチャート

1. 開始
   将来審査が必要になる全拠点
2. 1. 複数の拠点で審査が必要?
3. 2. すべての拠点で審査の準備をするのに十分な時間はある?
4. 3. すべての拠点で主要なISMS（責任、インフラ、方針、プロセスなど）を共有している?
5. 4. すべての拠点で、同じ審査目的（プロトタイプ車両や保護ニーズが非常に高い情報の保護）を共有している?
6. 終了。審査スコープを登録
   審査スコープには、残った拠点を登録することをお勧めします。
7. その拠点は切り離して、
   それぞれの拠点のセットで開始地点に戻ります。

8 いいえ

9 はい

注意事項:

この決定をあまり恐れる必要はありません。審査機関が審査を終了するまで、すべてのスコープは変更可能です。

例えば、審査の準備中にスコープが適切でないことに気づいた場合、変更することもできます。また、審査機関が、審査の初期段階においてスコープの変更を推奨する場合もあります。

追記事項:

- 正確には、ENXポータルへのオンライン登録時に定義された審査スコープは、変更できません。しかし、審査機関が審査結果をENXポータルにアップロードする際に、審査スコープを更新することは可能です。
- スコープを追加すると料金が増額され、スコープから拠点を削除しても返金はされません。審査機関は、元のスコープをベースにコストを算出しているため、コストが変わることを想定しておく必要があります。

4.3.2.5. 拠点のスコープを設定

どの拠点を審査スコープに含めるかを決めたら、次に拠点固有の情報を収集します。

各拠点について、社名や住所などの情報が求められます。また、TISAX審査機関が貴社の企業構造を把握するために必要な追加の情報もお聞きします。貴社の回答は、審査機関が必要とする労力を見積もる上での基礎となります。

各拠点に関し、以下の詳細情報を提供できるように準備してください（赤いアスタリスク *が付いた情報は、オンラインプロセスで必須です）。

項目	選択肢
拠点名 *	なし
D&B D-U-N-Sナンバー	なし
拠点の種類 *	自社所有の建物 会社が借りている建物 共有の建物の、会社が借りているフロアまたはオフィス 他社と共有しているオフィス 自社データセンター 共有データセンター
パッシブサイト保護 *	有り 無し
業界 （複数選択可）	情報技術 ☒ ITサービス ☒ 通信サービス ☒ ソフトウェア開発

項目	選択肢
	マネジメント ☒ コンサルティング
	メディア ☒ マーケティング ☒ 代理店 ☒ 印刷サービス ☒ 写真 ☒ 翻訳サービス
	研究開発 ☒ 車両テスト ☒ 車両シミュレーション ☒ プロトタイプ製作 ☒ ミニチュアカーモデル ☒ 開発サービス ☒ CAx開発サービス
	生産 ☒ 生産サービス ☒ 受託生産 ☒ ショップフロア ☒ ロジスティクス
	販売とアフターセールス ☒ 輸入、NSC ☒ ディーラー ☒ 金融サービス ☒ 保険 ☒ 保険金請求
	その他の業種 （記入してください）
拠点の総従業員数 *	0 1～10 11～100 101～1000 1001～5000 5000人以上

項目	選択肢
拠点の従業員数（IT） *	0 1〜10 11〜25 26〜50 50人以上
拠点の従業員数（ITセキュリティ） *	0 パートタイム 1〜5 6〜25 25人以上
拠点の従業員数（拠点セキュリティ） *	0 パートタイム 1〜3 4〜10 10人以上
この拠点の認証	ISO 27001 その他（記入してください） ISAE 3402 SOC2

表 1. 拠点ごとの詳細情報

注意事項:

「業種」は、分かる範囲で選んでください。上記の選択肢に、正解・不正解はありません。該当する業種がない場合は、「その他」を選択し、適切な業種を記入してください。

各拠点には“location name”（「拠点名」）を指定する必要があります。拠点名は、審査スコープへの拠点の割り当て時に、拠点を参照しやすくするための項目です。

拠点名は、以下の形式で割り当てることをお勧めします。

形式　[地理的な情報]

例:　架空の会社 「ACME」の場合

- フランクフルト
  （ドイツの都市フランクフルトの場合）

4.3.2.6. スコープ名

各スコープには“scope name”（「スコープ名」）を指定する必要があります。スコープ名の主な目的は、ENXポータルのスコープ一覧でスコープを識別しやすくすることです。見る人や同僚にとって有用な名称を割り当てることをお勧めします。外部とのコミュニケーションには、スコープIDを使う必要があります。

任意の名前を指定できます。ただし、複数のスコープに同じスコープ名を割り当てることはできません。

後でTISAX審査を更新する際は、スコープを新規作成する必要があります（内容は現在のスコープと同一になる場合もあります）。そのため、スコープ名には審査の年も記載することをお勧めします。

スコープ名は、以下の形式で割り当てることをお勧めします。

形式	[地理または機能に関する情報] [審査年]
例:	架空の会社 「ACME」の場合

- 2024
  （拠点が1か所のみの場合、地理情報なし）
- フランクフルト 2024
  （ドイツのフランクフルト市の複数拠点を対象とする場合）
- ニーダーザクセン州 2024
  （ニーダーザクセン州の全拠点を対象とする場合）
- ドイツ 2024
  （ドイツ国内の全拠点を対象とする場合）
- EMEA 2024
  （EMEA地域（ヨーロッパ、中東、アフリカ）の全拠点を対象とする場合）
- プロトタイプ開発 2024
  （プロトタイプ開発に関わる全拠点が対象となる場合の、機能に関する情報）

4.3.2.7. 連絡先

貴社と連絡を取るために、貴社の連絡先に関する情報を収集します。

TISAX参加企業全体で1名以上、審査スコープごとに1名以上の連絡先の提供をお願いしています。連絡先を追加することも可能です。

登録準備の段階で、貴社内で誰を連絡先にするかを決めてください。

連絡先について、以下の詳細情報をお知らせください。

	連絡先の詳細情報	必須かどうか	例
1.	挨拶文	必須	Mrs. / Mr.
2.	学位		博士 / 博士号 等
3.	名	必須	John
4.	姓	必須	Doe
5.	役職名	必須	IT部長
6.	部署名	必須	情報技術
7.	第一の電話連絡先	必須	+49 69 986692777
8.	第二の電話連絡先		
9.	メールアドレス	必須	john.doe@acme.com
10.	使用言語	必須	英語（デフォルト）
11.	その他の言語		ドイツ語、フランス語
12.	個人住所の識別子		HPC 1234
13.	番地	必須	Bockenheimer Landstraße 97-99
14.	郵便番号	必須	60325

	連絡先の詳細情報	必須かどうか	例
15.	都市名	必須	フランクフルト
16.	都道府県		
17.	国名	必須	ドイツ

表 2. 連絡先の詳細情報

重要事項:

それぞれの連絡先に、少なくとも1人の代理人を指定することをお勧めします。代理人を指定することで、連絡先を一時的に利用できない場合や退職時に、代理人が貴社の参加企業データを管理できます。
新しい連絡先の割り当ては（他に有効な連絡先がない場合）、複雑なプロセスを踏む必要があります。TISAXのプロセスにおいて、新たな主要連絡先の割り当てを承認できるのは、会社の代表資格を法的に証明できる人物のみです。

4.3.2.8. 公開と共有

TISAXの主な目的は、貴社の審査結果を他のTISAX参加企業に公表し、貴社の審査結果を貴社のパートナー企業と共有することです。

審査結果の公開と共有については、登録プロセス中でも、登録後でも、いつでも決定できます。

事前準備としてTISAXの手続きを進めている場合においても、TISAX参加企業のコミュニティに対する審査結果の公表の有無を、あらかじめ決めておくことが可能です。他には、この時点で準備することはありません。

パートナー企業からTISAXプロセスの実施を要請された場合は、最終的には審査結果を共有する必要があります。登録中でも、パートナー企業とステータス情報を共有できます。貴社の審査結果が利用可能になると、貴社のパートナー企業にはアクセス権限が自動的に付与されます。[6]

ステータス情報の共有には、以下の二つが必要です。

1. パートナー企業のTISAX参加企業ID

   TISAX参加企業IDは、パートナー企業を、TISAX参加企業として特定します。

   一般的に、パートナー企業は貴社に、TISAX参加企業IDを提供する必要があります。

   便宜上、TISAXの登録フォームには、審査結果の共有が頻繁に行われる企業について、参加企業IDのドロップダウンリストが用意されています。[7]

2. 必要な共有レベル

   共有レベルでは、パートナー企業が貴社の審査結果にどの程度までアクセスできるかを定義します。

   パートナー企業が特定の共有レベルを要求している場合や、パートナー企業に審査結果へのアクセスをどのレベルまで許可するかを定義する場合に使用します。

   共有レベルの詳細については、次のセクションを参照してください：セクション 6.5. 共有レベル。

次の情報を確認しておくことをお勧めします。

注意事項:

- 審査結果を公開するかどうかは、後からいつでも決めることができます。
- パートナー企業に対する共有の許可は、後からいつでも作成できます。

重要事項:

審査結果を公開しない場合や共有しない場合は、誰も貴社の審査結果を見ることはできません。

重要事項:

公開または共有を取り消すことはできません。

詳しくは以下のセクションを参照してください：セクション 6.4. 共有結果の永続性。

注意事項:

不思議に聞こえるかもしれませんが、実際に審査プロセスを開始していない段階でも、「審査結果」は共有できます。この初期段階では、貴社は「審査ステータス」を共有しているだけに過ぎません。貴社が「審査結果」を共有した参加企業は、貴社の審査プロセスがどの段階かを知ることができます。

TISAX参加企業の中には、貴社によるTISAXラベルの提示を求めているものの、審査プロセスが完了していない際に、特別な免除が必要となる場合があります。このようなケースで、パートナー企業はENXポータルのアカウントで貴社の「審査ステータス」を確認する必要があることも考えられます。

審査ステータスについては、次のセクションを参照してください：セクション 7.6. 附録：Assessment status（審査ステータス）。

審査結果の公開と共有については、次のセクションを参照してください：セクション 6. 共有（ステップ 3）。

4.3.3. 審査目的

登録プロセスでは、審査の目的を定義する必要があります。審査目的（assessment objective）では、情報セキュリティマネジメントシステム（ISMS）が満たすべき対象となる要求事項を決定します。審査目的は、パートナーに代わって取り扱うデータの種類によってのみ決まります。

以下のセクションでは、審査目的について解説し、適切な審査目的の選択方法についてアドバイスします。

審査目的を使用することで、パートナーやTISAX審査機関がTISAX審査プロセスで定義された内容を参照し、TISAX関連のコミュニケーションを取りやすくなります。

注意事項:

パートナーによっては、審査目的を指定する代わりに、特定の「審査レベル」（AL）でTISAX審査を受けるよう要求する場合があります。

審査レベルに関する詳細は、セクション 4.3.3.5. 保護ニーズと審査レベル（サブセ

クション「追加情報」）を参照してください。

4.3.3.1. 審査目的のリスト

現在、TISAXには12の審査目的があります。このうち、少なくとも一つの審査目的を選択する必要があります。審査目的は、複数選択できます。

審査目的は、情報セキュリティマネジメントシステムのベンチマークとして捉えることができます。審査目的は、TISAXプロセスにおける重要な項目です。すべてのTISAX審査機関は、主に審査目的に基づいて審査戦略を策定します。

現在、TISAXには、下表の審査目的が存在します。

番号	名前	説明
1.	Info high	Handling of information with high protection needs 保護ニーズの高い情報の取り扱い
2.	Info very high	Handling of information with very high protection needs 保護ニーズの 非常に高い情報の取り扱い
3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information) 機密性の観点から、保護ニーズの高い情報の取り扱い（機密情報へのアクセス）
4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information) 機密性の観点から、保護ニーズの 非常に高い情報の取り扱い（厳格な機密情報へのアクセス）
5.	High availability	Handling of information with high protection needs in the context of availability (high availability of information) 可用性の観点から、保護ニーズの高い情報の取り扱い（情報の可用性が高い）
6.	Very high availability	Handling of information with very high protection needs in the context of availability (very high availability of information) 可用性の観点から、保護ニーズの 非常に高い情報の取り扱い（情報の可用性が非常に高い）
7.	Proto parts	Protection of Prototype Parts and Components プロトタイプ部品・コンポーネントの保護
8.	Proto vehicles	Protection of Prototype Vehicles プロトタイプ車両の保護
9.	Test vehicles	Handling of Test Vehicles テスト車両の取り扱い
10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots イベントおよび動画・写真撮影時のプロトタイプの保護
11.	Data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) EU一般データ保護規則（GDPR）第28条（「処理者」）に基づくデータ保護

番号	名前	説明
12.	Special data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR EU一般データ保護規則（GDPR）第9条に規定された特別区分の個人データに関する、同第28条（「処理者」）に従ったデータの保護

表 3. TISAXの現行の審査目的

例：公道でテストドライブを実施する場合、審査目的には審査目的「Test vehicles」が含まれます。

注意事項：

審査目的「Info high」と「Info very high」を選択いただけるのは2024年5月31日までです。

審査目的「Confidential」と「Strictly confidential」を選択いただけるのは2024年4月1日までです。

この移行に関する詳細は、ENX協会ウェブサイトの以下のニュース記事をご確認ください：
CHANGES TO TISAX LABELS ACCOMPANYING ISA 6 RELEASE
enx.com/en-US/news/Changes-to-TISAX-Labels-ISA-six-Release/

重要事項：

TISAXでは、プロセスに「審査目的」が入力されるのが一般的です。ただし、パートナー企業によっては、特定の「審査レベル」（AL）でTISAXの審査を受けるよう要求する場合があります。

保護ニーズと審査レベルの関係については、次のセクションをご参照ください：セクション 4.3.3.5. 保護ニーズと審査レベル。

4.3.3.2. 審査目的とISA

ISAには、三つの基準カタログ（情報セキュリティ、プロトタイプ保護、データ保護）が存在します。各基準カタログは、「コントロール質問」と呼ばれる質問と、関連の要求事項からなります。

各審査目的は、以下を定義します。

- 適用されるISA基準カタログ（複数可）
- 回答が必須となるコントロール質問
- 貴社が満たすべき要求事項

一部の審査目的については、コントロール質問と要求事項のサブセットのみが適用されます。

TISAXの審査目的と、適用されるコントロール質問および要求事項に関する詳細は、以下のセクションをご参照ください：セクション 5.2.2. ISAドキュメントについて理解する。

4.3.3.3. 審査目的とTISAXラベル

貴社のパートナーから、「TISAXラベル」についての話があったかもしれません。「審査目的」と「TISAXラベル」はほぼ同じものです。違いは、貴社が「審査目的」をもって審査プロセスを開始し、審査に合格すれば、それに対応する「TISAXラベル」を受け取るという点です。

例：貴社は、パートナーからTISAXラベル「Info high」の取得を要請されました。そこで貴社は「Info high」を審査目的として選択しました。

次のイラストは、TISAXプロセスの入力と出力を示しています：

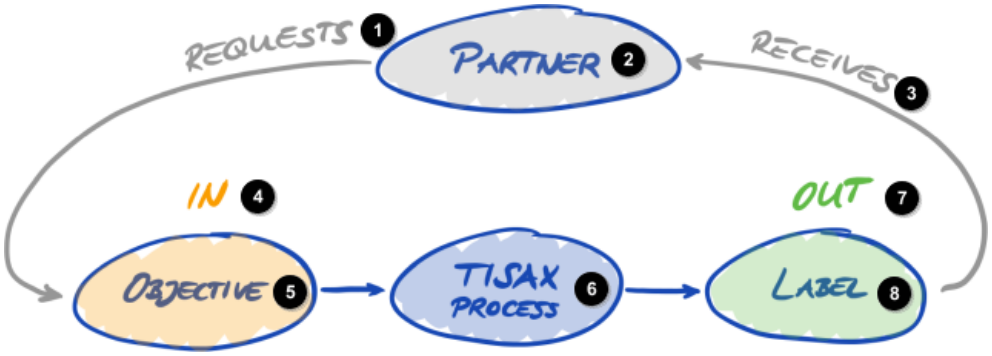


図 6. 審査目的とTISAXラベル

1. 要請
2. パートナー企業
3. 取得
4. 入力
5. 目的
6. TISAXプロセス
7. 出力
8. ラベル

TISAXラベルに関する詳細は、以下のセクションを参照してください：セクション 5.4.14. TISAXラベル。

4.3.3.4. 審査目的の選択

理想的なのは、貴社が達成しなければならない審査目的を、パートナーが正確に教えてくれることです。

以下の場合は、貴社の判断に基づいて審査目的を選択する必要があります。

a. パートナーからの要求前に、TISAXの審査を受けたい場合、または
b. 達成すべき審査目的について、パートナーが教えてくれない場合

重要事項：

> この時、他のパートナーも考慮した上で検討することを強くお勧めします。同等か、それ以上の要求事項を持つ既存のパートナーはいますか？ 将来的に、パートナーの要求事項が高くなると考えられますか？
>
> より高い保護ニーズの審査目的を選択することも検討すると良いかもしれません。そうすることで、他のパートナーの要求事項が高かった場合に生じる問題を防ぐことができます。

貴社の判断に基づいて審査目的を選択しなければならない場合、以下の点について考慮することも検討してください。

番号	審査目的	情報
1.	Info high	パートナーの文書の分類から、保護ニーズ（高い、非常に高い）を導き出せる場合があります。
2.	Info very high	
3.	Confidential	機密性の観点から保護ニーズの高い情報、または企業独自の分類スキーム（例：VDAホワイトペーパー「Harmonization of classification levels（分類レベルの調和）」）に従って一般的に機密として分類される情報を受け取り処理するすべての企業が対象です。 情報が不正に開示された場合、多大な損害（風評被害、刑事罰、金銭的損害など）が発生する可能性がある場合には、このTISAXラベルを選択する必要があります。
4.	Strictly confidential	機密性の観点から保護ニーズの非常に高い情報、または企業独自の分類スキーム（例：VDAホワイトペーパー「Harmonization of classification levels（分類レベルの調和）」）に従って一般的に厳格な機密または秘密として分類される情報を受け取り処理するすべての企業が対象です。 情報が不正に開示された場合、存続を脅かす、または壊滅的な損害（深刻な風評被害、深刻な刑事罰、非常に高額な金銭的損害など）が発生する可能性がある場合には、このTISAXラベルを選択する必要があります。
5.	High availability	顧客の生産・提供能力が、企業の製品・サービスの供給能力に依存しており、かつ、障害が発生した場合、短期間で顧客にかなりの損害が発生するおそれのある企業が対象です。 例：生産材料のジャストインタイムサプライヤー
6.	Very high availability	顧客の生産・提供能力が、企業の製品・サービスの短期的な供給能力に依存しており、かつ、障害が発生した場合、非常に短期間で顧客に著しく大きな損害が発生するおそれのある企業が対象です。 例：ジャストインタイムサプライヤーの場合、障害が発生すると、短期間で、再稼働までに非常に時間がかかる包括的な生産停止に陥るおそれがあります。
7.	Proto parts	顧客提供の、要保護に分類される部品またはコンポーネントを、自社で製造、保管、使用するすべての企業が対象です。 物理的な安全性、周囲を考慮した安全性、組織的な要求事項、プロトタイプの取り扱いに関する特定の要求事項が審査の対象となります。

番号	審査目的	情報
8.	Proto vehicles	要保護に分類される顧客提供の車両を、自社で製造、保管、使用するすべての企業が対象です。 物理的な安全性、周囲を考慮した安全性（保護されたガレージや作業エリアの有無など）、組織的な要求事項、プロトタイプの取り扱いに関する具体的な要求事項が審査の対象となります。 審査に合格すると、自動的にTISAXラベル「プロトタイプ部品・コンポーネントの保護」が発行されます。
9.	Test vehicles	要保護に分類された顧客提供の車両を使用して、試験やテスト走行（公道やテストコースでのテスト走行など）を実施するすべての企業が対象です。 組織的な要求事項やカモフラージュを含むプロトタイプの取り扱いに関する具体的な要求事項、および公道やテストコースでのテスト走行中の車両の取り扱いが審査の対象となります。 物理的な安全性および周囲を考慮した安全性に関する要求事項は、必ずしも審査に含まれません。貴社の拠点に相応の設備がある場合は、審査項目「プロトタイプ車両の保護」も選択することをお勧めします。
10.	Proto events	要保護に分類される顧客提供の車両、部品またはパーツを使用して、プレゼンテーションやイベント（市場調査、イベント、マーケティングイベントなど）、映画や写真撮影を実施するすべての企業が対象です。 プロトタイプの取り扱いに関する組織的な要求事項および具体的要求事項には、保護された部屋および公共の場におけるプレゼンテーション、イベント、映画・写真撮影に関する要求事項も含まれます。 物理的な安全性および周囲を考慮した安全性に関する要求事項は、必ずしも審査に含まれません。貴社の拠点に相応の設備がある場合は、審査項目「プロトタイプ車両の保護」も選択することをお勧めします。
11.	Data	EU一般データ保護規則の第28条に基づき、処理者として個人データを取り扱う場合は、「Data」の選択が必要になると思われます。
12.	Special data	EU一般データ保護規則の第28条に基づき、処理者として特別カテゴリーの個人データ（健康や宗教などのデータ）を取り扱う場合は、「Special data」の選択が必要になると思われます。

表 4. 審査目的の選択におけるアドバイス

さらに詳しく説明します。

- パートナーの要求事項を正確に把握している場合は、基本的に審査目的についてパートナーと話し合う必要はありません。一方、パートナーの要求事項を正確に把握していない場合は、審査プロセスを始める前に、パートナーに相談することを強くお勧めします。
- ISAには、各要求事項の「高い」保護ニーズと「非常に高い」保護ニーズ（もしあれば）で、実施

上でどのような差異があるかが記載されています。
詳細は、以下の画像を参照してください：
図 11. ISA基準カタログ「情報セキュリティ」の質問の主な要素のスクリーンショット。

4.3.3.5. 保護ニーズと審査レベル

貴社のパートナーは、さまざまな種類の情報を保有しています。その中には、特に保護レベルを高く設定すべき情報も存在する場合があります。ISAは、三つの「保護ニーズ」（“protection needs”）を区別することで、これに対応しています。パートナ⊠ーは自社の情報を分類して、通常は保護ニーズを割り当てます。

情報の保護ニーズが高くなるほど、パートナーは貴社にその情報を扱わせても安全か確証を得たいと考えます。そこで、TISAXは三つの「審査レベル」（AL）を設けています。審査レベルに応じて、審査機関がどの審査方法を適用する必要があるかが決まります。レベルが高いほど、審査に伴う労力は増加します。その結果、より慎重で正確な審査が行われます。

下の表は、TISAXの審査目的に適用される審査レベルを示しています。

番号	TISAX審査目的	審査レベル（AL）
1.	Info high	AL 2
2.	Info very high	AL 3
3.	Confidential	AL 2
4.	Strictly confidential	AL 3
5.	High availability	AL 2
6.	Very high availability	AL 3
7.	Proto parts	AL 3
8.	Proto vehicles	AL 3
9.	Test vehicles	AL 3
10.	Proto events	AL 3
11.	Data	AL 2
12.	Special data	AL 3

表 5. TISAX審査目的と審査レベルのマッピング

審査レベル 1（AL 1）：

審査レベル 1の審査は、本当の意味での自己評価（self-assessment）であり、主に社内目的で使われます。

審査レベル 1の審査では、監査人は、実施済みの自己評価が存在するかを確認します。監査人が、この自己評価の内容を審査することはありません。それ以上の証跡が必要となることもありません。

審査レベル 1の審査結果は信頼度が低いため、TISAXでは用いられません。ただし、貴社のパートナーがTISAXとは関係なく、こういった自己評価を要求する可能性はもちろんあります。

審査レベル 2（AL 2）：

審査レベル 2の審査では、審査機関が、貴社の自己評価（審査スコープ内の全拠点）の妥当性を確認します。審査機関は、証跡を確認し、[8]情報セキュリティ担当者と面談を行うことで、裏付けを行いま

す。

審査機関との面談は、通常、ウェブ会議を通じて行われます。また要望があれば、対面での面談も可能です。

審査機関に送りたくない証跡がある場合は、オンサイト調査を依頼することもできます。こうすることで、審査機関が持ち出し厳禁の証跡も確認できます。

注意事項:

審査レベル 2では、代替の審査方法が存在します。妥当性の確認の代わりに、審査機関が、完全なリモート審査を実施します。この方法は「審査レベル 2.5」と呼ばれることもあります。

審査レベル 2の審査との差異として、監査人により、貴社のISMSが要求事項を満たしているか検証が行われます。一方、審査レベル 3の審査とは異なり、監査人による、審査レベル 3のオンサイト調査（後述）は実施されません。

形式上、このような審査は審査レベル 2の審査として扱われます。

審査レベル 2.5の利点は、審査 3と互換性がある方法で審査される点です。したがって、比較的少ない手間で、後から審査レベル 3の本格的な審査にアップグレードすることも可能です。アップグレードする場合、監査人は、以下の審査レベル 3のセクションに記載されたオンサイト調査のみを実施します。

以下の場合には、審査レベル 2.5での審査を推奨します。

1. 現在必要なのは審査レベル 2のTISAXラベルのみだが、他のパートナーから、審査レベル 3のTISAXラベルを求められる可能性がある場合。審査レベル 2.5で審査することで、後から審査レベル 3にアップグレードという選択肢が生まれます。
2. 妥当性が十分な自己評価を作成することが困難な場合。妥当性を確認する上で、自己評価は疑う余地がなく、理解しやすく、裏付けが取れている必要があります。このような自己評価の作成は、基本的に安定した状況の企業であっても、社内で多大な労力を要する可能性があります。

審査レベルのアップグレードに関する詳細は、以下のセクションを参照してください：セクション 7.10. 附録：スコープ拡大審査。

これはあくまで任意で、審査レベル 2の要求事項を満ために必要な審査方法ではありません。審査レベル 2と審査レベル 2.5の違いは、審査結果を共有するパートナーには伝わりません。

審査レベル 3（AL 3）：

審査レベル 3の審査では、審査機関は、貴社が対象の要求事項に準拠しているか、包括的に検証します。監査員は、貴社の自己評価と、提出された文書を使用して、審査の準備を行います。審査レベル 2との相違点として、監査人はすべてを検証します。実施内容は以下の通りです。

- 文書と証跡の調査
- プロセスオーナーとの計画的な面談の実施
- 現地状況の確認
- プロセスの実行の確認
- プロセス参加者との抜き打ち面談の実施

注意事項:

以下は、本資料の後半で説明する内容について言及しています。

審査レベル 3では、審査機関は貴社の拠点に出向く必要があります。何らかの理由で、出向くことが一時的に不可能な場合や、不合理な労力を必要とする場合、審査機関は、動画を用いたリモート審査をもって、審査のオンサイト活動を実施できます。

審査機関は、このことを軽微な不適合としてTISAX審査報告書に記録する義務があります。 審査機関は、貴社の拠点に来訪できるようになり次第、それまでに不可能であったすべてのオンサイト活動を含めたフォローアップ審査を実施しなければなりません。さらに、他の是正処置が完了していない場合でも、フォローアップ審査の日程を決める必要があります。

審査機関がオンサイト活動を実施できるようになるのを待たず、この方法で審査を受けた場合は、TISAX仮ラベルをパートナーと共有できるようになります。

審査レベルと審査方法

各審査レベルにおける審査方法の概要を簡略化したものを、下表に示します。

審査方法	審査レベル 1 (AL1)	審査レベル 2 (AL2)	審査レベル 3 (AL3)
自己評価	○	○	○
証跡	☒	妥当性の確認	徹底的な検証
面談	☒	ウェブ会議[9]	オンサイトでの面談
オンサイト調査	☒	要望により実施可	○

表 6. 審査レベルに応じた審査方法の適用範囲

追加情報

- 審査レベル 2と審査レベル 3の違い
  審査方法の観点から、審査レベル2と3ではアプローチが大きく異なります。審査レベル2の審査では、監査員はすべての検証は行わず、妥当性のみを確認します。したがって、審査機関は、審査レベル 2の審査結果をもって、審査レベル 3へのアップグレードの根拠とすることはできません。そのため、審査レベル 3へのアップグレ☒ードは、基本的に新規の審査と同じ労力を必要とします。
- 妥当性の確認と検証の違い
  極めて簡単に言えば、妥当性の確認とは、確認対象の存在の有無と、それが正しいように見えるかを確認する作業です。これに対して、検証では、検証対象が主張通りのものであるかを、実際に確認します。
- 情報の分類と保護ニーズ
  情報の分類（機密や秘密など）と保護ニーズがどのように紐付けられるかは、パートナー企業によって異なる場合があります。そのため、残念ながら、パートナー企業の情報分類と保護ニーズが正確に対応しているような、シンプルな表を提供することはできません。
- 審査レベルを知っているだけでは不十分
  パートナー企業によっては、特定の審査レベルでTISAX審査を受けるよう要請してくる場合があります。この時、審査レベルを把握するだけでは、TISAXプロセスを開始するには不十分であることをご理解ください。審査レベルは、ISA基準カタログと、対応する保護ニーズを組み合わせることで、初めて意味を持ちます。パートナー企業はTISAXラベル（基準カタログおよび保護ニーズ）の

取得を要請するのが一般的です。しかし、保護ニーズは審査レベルと1対1で紐付けられているため、基準カタログと審査レベルを把握するだけで十分です。

- 審査レベルの階層
  どの審査レベルにも、必ずそれより低い審査レベルの要求事項が含まれます。例えば、審査レベル3に基づいた審査を実施した場合、審査レベル2のすべての要求事項は自動で満たされます。
- 審査レベルに関する推奨事項
  貴社の判断に基づいて審査目的（すなわちそれに伴う審査レベル）を選択しなければならない場合、審査レベル3にあたる審査目的を選択することを推奨します。審査レベル3のTISAX審査にかかる労力は、一般的に審査レベル 2よりも高くはありません。
  複数のパートナー企業を持つサプライヤーは、審査レベル3にあたる審査目的を選択するケースが少なくありません。こうすることで、将来的なあらゆる要求事項に備えることができ、審査レベルが異なることを気にする必要もなくなります。
- 商業面からの追加考察
  各審査レベルにおけるTISAX審査の総コストは、貴社の社内で必要とされる労力と、審査コストの合計として捉えられます。審査レベル2の場合、審査コストは低くなりますが、社内で必要な労力は大きくなる可能性があります。これは、審査レベル2の審査では、より包括的な自己評価と、より優れた内部文書が必要とされるためです。一方、審査レベル3の審査では、どのように業務が行われているかを示し、基本的な文書を示すだけでも、監査人にとって十分な証拠となることが少なくありません。一方、オンサイト調査を行わなければ、監査人は正確な文書を要求します。したがって、審査レベル2ではなく審査レベル3が選択されるのは珍しくありません。これは大企業よりも、むしろ中小企業によって取られる選択です。

4.3.3.6. 審査目的と貴社のサプライヤー

TISAXは、必ずしも貴社のすべてのサプライヤーに同じ要求事項を課すことを求めているわけではありません。貴社の審査目的が「保護ニーズが非常に高い情報の安全確保」であったとしても、貴社のすべてのサプライヤーが、同じ審査目的を達成しなければならないということにはなりません。さらに言えば、サプライヤーが、TISAXラベルを取得する必要があるということですらありません。

しかし、サプライヤーのサービスを利用することで、リスクが増加したり、新たなリスクが発生したりしないかどうかは、すべてのサプライヤーについて確認する必要があります。

以下に、非常に単純化した例を二つ挙げます。

1. 貴社には、非常に高度な保護が必要なデータの場合、通常のメールを使用できないというポリシーがあります。そのため、貴社のメールプロバイダーが、非常に高い保護ニーズのTISAXラベルを取得する必要はありません。
   貴社が暗号化されたメールのみを送信し、メールプロバイダーが非常に高い保護ニーズのデータを閲覧できない場合も、同様の結論となる可能性があります。
2. 貴社は、保護ニーズの非常に高い印刷データはシュレッダーで廃棄しています。この場合、もちろん廃棄物処理業者は貴社と同じ要求事項を満たす必要はありません。

しかし、リスクアセスメントの結果、サプライヤーも非常に高い保護ニーズを満たす必要があるという結論に達することがあります。この場合、TISAXラベルは、サプライヤーによるこの要求事項の達成を証明する手段になり得ます。

4.3.4. 料金

ENX協会は料金を徴収します。適用される料金、割引の可能性、支払い条件については、価格表からご確認いただけます。

価格表は、ENX協会ウェブサイトの以下のリンクからダウンロードできます。
enx.com/en-US/TISAX/downloads/
PDFは、以下のリンクから直接ダウンロードできます。

enx.com/pricelist.pdf

登録準備の際には、請求書に関し、以下の点についてご考慮ください。

- 請求書の送付先
  デフォルトでは、請求書は参加企業の所在地として登録された宛先に送付されます。しかし、請求書を受け取るための、別の送付先を選択するオプションがあります。

重要事項:

請求書の送付先が正しいことを、必ず確認してください。会計法上、請求書に記載される送付先は、貴社（請求書）の宛先と正確に一致する必要があります。コンプライアンス上の理由から、一度請求書を発行した後に、請求書の送付先を変更することはできません。

- 注文照会
  請求書に特定の発注書番号などを記載する必要がある場合は、発注書番号を記入してください。
- 付加価値税番号
  すべての料金には、ドイツの付加価値税（VAT）が適用されます。
  EU圏からの支払い処理には、この番号が必要です。請求書の送付先が以下の国にある場合は、VAT番号の提示が必須です。
  アイルランド、イギリス、イタリア、エストニア、オーストリア、オランダ、キプロス（ギリシャ領）、ギリシャ、クロアチア、スウェーデン、スペイン、スロバキア、スロベニア、チェコ共和国、デンマーク、ドイツ、ハンガリー、フランス、ブルガリア、フィンランド、ベルギー、ポーランド、ポルトガル、マルタ、ラトビア、リトアニア、ルクセンブルク
- サプライヤー管理

重要事項:

TISAXに参加する全企業の関係性の観点から、いかなる追加条件（一般購買条件、行動規範など）も受け入れることができないことをご了承ください。

請求書の発行プロセスに関する追加情報

- 個別の購買条件はお受けできません。
- 支払いは以下の方法をご利用ください。
  - 請求書に記載された銀行口座への振込み
  - クレジットカードによる支払い（弊社の決済サービスプロバイダー“Stripe”を経由した登録手続き中）
- 当社の請求書には、貴社の登録情報について以下の内容が記載されます。
  - 参加企業としての主要連絡先の氏名およびメールアドレス
  - 審査スコープ名

  以下の附録セクションに、請求書の例が記載されています：セクション 7.1. 附録：請求書の例。
- 請求書の処理に通常必要となるほとんどの情報は、請求書に直接記載されます。これらの情報およびその他の詳細情報は「Information for Members and Business Partners」（メンバーおよびビジネスパートナー向け情報）でご覧いただけます。メールでご連絡いただければ、最新版をお送りいたします。

注意事項:

一般的に、社内の支払い承認プロセスが長引く場合があることをENX協会は理解しています。そのため、TISAXプロセスにおける直後の手続きは、支払いをENX協会が受領したかどうかに関わらず実施されます。ただし、支払いを受領していない場合、審査結果を共有することはできませんのでご注意ください。
このため、適切な受取先に請求書を送付し、該当する場合は、注文照会が含まれていることを確認することをお勧めします。また、請求書が支払い済みかどうかも、内部で追跡できます。

重要事項:

ENX協会は料金を請求いたしますが、これは、TISAX審査の総費用の一部に過ぎません。TISAX審査機関は、審査にかかる費用を請求します。

審査機関にまつわる費用については、以下のセクションをご参照ください: セクション 5.3.4. オファーの評価。

重要事項:

料金は、以下の状況に関係なく発生します。

- TISAXプロセスの継続・中止
- TISAX審査の合格・不合格

そのため、初回審査の開始前に請求書が届く場合があります。

4.4. ENXポータル

このセクションでは、オンライン登録プロセスについて解説します。オンライン登録プロセスでは、前のセクションのアドバイスに従い貴社が収集したすべてのデータを入力してください。オンライン登録を開始する前に、ENXポータルの目的とメリットについて簡単に説明します。

ENXポータルは、TISAXに参加する全企業のデータベースを管理しており、TISAXの全プロセスにおいて重要な役割を果たします。TISAXの登録の際には、貴社が自社データを入力し、（貴社が同意した場合）TISAX審査機関は、そのデータを料金の算出や審査手順の立案に使用できます。TISAXの審査プロセスの完了後は、ENXポータルの共有プラットフォームを使って、審査結果をパートナーと共有します。

ポータルの名称は「TISAXポータル」ではなく「ENXポータル」となっていますが、これはENXポータルを他の事業活動（ENXネットワークなど）の管理にも使用しているためです。

4.5. オンライン登録プロセス

上記のアドバイス（セクション 4.3. 登録準備）に従って準備された方は、オンライン登録プロセスを始める準備は完了しています。

4.5.1. 所要時間

所要時間は、登録するスコープと拠点の数によって大きく異なります。スコープが一つ、拠点1か所での初回登録の場合で、20分以上はかかるとお考えください。

現在、途中から手続きを再開するのは容易ではないため、登録は1回で完了させることをお勧めします。それでも中断する必要がある場合は、不足データを要求するためにご連絡いたします。

4.5.2. 登録の開始

次のウェブサイトから登録を開始してください：
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

基本的には、画面の指示に従うだけで登録を進められます。念のため、以下に手順を簡単に記載します。

4.5.3. ポータルアカウント

最初の手順は、ENXポータルのアカウント作成です。ポータルアカウントは、貴社の「参加企業データ」の管理に必要です。

注意事項：

ENXポータルに、登録済みのメールアドレスと表示される場合は、ご連絡ください。このメッセージは、何らかの理由で貴社がすでにシステムに保存されている時に表示される場合があります。

注意事項：

記載の通り、ポータルアカウントは、必ずしも審査プロセスでアクティブな役割を付与されている「参加企業の連絡先」または「スコープ連絡先」（下記参照）とは限りません。

逆に、「参加企業の連絡先」または「スコープ連絡先」に、ポータルアカウントと同様の、参加企業データの管理権利が自動で与えられることもありません。そのため、「参加企業の連絡先」または「スコープ連絡先」に指定された同僚は、ENXポータルの参加企業データに自動的にアクセスすることはできません。

ENXポータルで作成済みの連絡先に、参加企業データの管理権限を付与する場合は（役割の付与の有無に関わらず）、その連絡先を招待する必要があります。詳細については、以下のセクション末尾の注記を参照してください：セクション 4.5.5. 参加企業の連絡先。

4.5.4. 参加企業の登録

2番目の手続きでは、貴社をTISAX参加企業として登録します。「TISAX参加企業」は、他の参加企業と審査結果を共有します。

4.5.5. 参加企業の連絡先

この連絡先の人物は、貴社の情報セキュリティ審査に関連する事柄全般の責任者です。これは、あなた自身でも、貴社の他の誰かでも構いません。

通常、必要とされるのは参加企業の主要連絡先のみです。ENX協会およびTISAX審査機関から送信される、登録関連のすべての連絡を他の人物にも送信したい場合は、参加企業の追加連絡先を追加してください。

重要事項：

それぞれの連絡先に、少なくとも1人の代理人を指定することをお勧めします。代理人を指定することで、連絡先を一時的に利用できない場合や退職時に、代理人が貴社の参加企業データを管理できます。

新しい連絡先の割り当ては（他に有効な連絡先がない場合）、複雑なプロセスを踏む必要があります。TISAXのプロセスにおいて、新たな主要連絡先の割り当てを承認できるのは、会社の代表資格を法的に証明できる人物のみです。

注意事項:

連絡先の追加や削除は、後からいつでも行うことができます（オンライン登録手続きの完了後でも、審査完了後でも可能です）。

注意事項:

参加企業の連絡先に、グループメールアドレスを使用することはできません（「info@acme.com」や「IT@acme.com」など）。

これは、ユーザーログインに関するISAの要求事項となっています。

注意事項:

各連絡先が、貴社の参加企業データにアクセスできるかどうかを選択できます。以下の手順のいずれかを実施します。

1. 連絡先を追加します。連絡先はENX協会のシステムに保存されますが、ログインしてデータを管理することはできません。
2. 連絡先を招待します。すると、ENXポータルから招待メールが送信されます。招待された連絡先は、メールに記載されている招待リンクに従ってください。連絡先がENXポータルの個人アカウントを作成すると、貴社の参加企業データを管理できるようになります。

新しい連絡先の作成方法： サインイン → MY TISAX → ADMINISTRATORS（管理者） → Create new TISAX Administrator（TISAX管理者の新規作成）

連絡先の招待方法： サインイン → MY TISAX → ADMINISTRATORS（管理者） → 連絡先の表の行の最後に移動し、下矢印のボタンをクリック → Edit TISAX Administrator（TISAX管理者を編集） → “ENX PORTAL ACCESS”（ENXポータルアクセス）セクションに移動 → “INVITE THIS CONTACT"（連絡先を招待）を「Yes（はい）」に設定 → “Save Contact”（連絡先を保存）をクリック

4.5.6. 参加規約

3番目の手続きは、「TISAX参加規約」への同意です。

以下のセクションの説明を参照してください：セクション 4.3.1. 法的基盤。

4.5.7. 審査スコープの登録

4番目の手続きでは、情報セキュリティ審査の審査スコープを登録します。

ここでは、以下の設定を行います。

1. 審査スコープ名を設定します。
   スコープ名の主な目的は、ENXポータルのスコープ一覧でスコープを識別しやすくすることです。
   以下のセクションの説明を参照してください：セクション 4.3.2.6. スコープ名
2. 審査スコープの種類を選択します。

（標準、カスタム）
以下のセクションの説明を参照してください：セクション 4.3.2. TISAXの審査スコープ。

3. スコープの主要連絡先を指定します。
特定のスコープにおける審査全般の責任者を指定します。これは、あなた自身でも、貴社の他の誰かでも構いません。
通常、必要とされるのはスコープの主要連絡先のみです。ENX協会から送信される、対象のスコープ関連のすべての連絡を他の人物にも送信したい場合は、参加企業の追加連絡先を追加できます。
4. 審査目的を選択します。
以下のセクションの説明を参照してください：セクション 4.3.3. 審査目的。
5. 審査スコープの拠点を追加します。
審査スコープに含まれる拠点をすべて指定してください。
以下のセクションの説明を参照してください：セクション 4.3.2. TISAXの審査スコープ。

注意事項：

一度作成した拠点は編集できません。軽微な変更（会社名の変更、番地、郵便番号、市町村のタイプミスなど）については、ENX協会までご連絡ください。 編集いたします。

重要事項：

この注意事項は、TISAXラベルの更新時にのみ関係します。

以前のスコープ登録時に作成・使用した、既存の拠点データを再使用してください。新しい拠点データを、同じ住所で作成しないでください。

これは、TISAX参加企業の中に、パートナーの審査結果を自動処理する企業が存在するためです。自動処理では、その企業のシステムとENXポータルが同期されるため、たとえわずかでも差異があると、同期が正常に完了しない可能性があります。また、不要な重複による、参加企業データの乱雑化を避けることにもつながります。

6. 公開レベルと共有レベルを選択します（オプション）。
審査結果を他のTISAX参加企業に公開するかどうか、また審査結果をパートナーと共有するかどうかを選択できます。一般的には、少なくとも貴社がTISAX参加企業であること、およびTISAXプロセスに合格したことの表示を許可します。
初回登録時には、この手続きを支障なく省略できます。審査結果へのアクセスは、後からいつでも定義可能です。
以下のセクションの説明を参照してください：セクション 4.3.2.8. 公開と共有。

重要事項：

公開や共有の許可を取り消すことはできません。
詳しくは以下のセクションを参照してください：セクション 6.4. 共有結果の永続性。

7. 請求書の受取人を指定します。
ENX協会からの請求書の受取人を指定してください。
以下のセクションの説明を参照してください：セクション 4.3.4. 料金。

注意事項：

ここで大きなミスが発生する可能性はあまりありません。多少異なるスコープを登録すべきだったことが後から分かっても（拠点を忘れていた、別の審査目的があった等）、審査機関は審査を実施できます。

例えば、貴社が当初スコープに追加しなかった追加の拠点をスコープに含める必要があると、監査人が判断したとします。その監査人は審査を進め、ENXポータルで審査結果をアップロードする際に、審査スコープを更新できます。

注意事項:

すべての審査スコープにはライフサイクルがあります。この段階では、審査スコープのステータスは「Incomplete（未完成）」、「Awaiting your order（貴社の依頼待ち）」、「Awaiting ENX approval（ENX承認待ち）」のいずれかです。

審査スコープのステータスの詳細については、以下のセクションを参照してください：セクション 7.5.1. 概要：Assessment scope status（「審査スコープのステータス」）。

注意事項:

拠点が多数ある大企業向けに、TISAXでは簡易グループ審査のオプションをご用意しています。簡易グループ審査は、以下の場合にご検討ください。

- スコープの拠点数が3以上あり、[10]かつ
- 貴社の情報セキュリティマネジメントシステムが万全であり、一元的に組織化されている場合。[11]

簡易グループ審査の場合、最初の労力が大きくなります。しかし、拠点数が増えるほど、このオプションの恩恵は大きくなります。

「簡易グループ審査」の詳細については、資料「TISAX Simplified Group Assessment」（TISAX簡易グループ審査）をご参照ください。

資料「TISAX簡易グループ審査」は、次の当社ウェブサイトの以下のページからダウンロードできます。
enx.com/en-US/TISAX/downloads/

PDFは、以下のリンクから直接ダウンロードできます。
enx.com/sga.pdf

注意事項:

貴社の審査スコープが登録された後は、貴社自身で審査スコープを変更することはできません。

まだ「TISAXスコープ抜粋」を審査機関に送付していないことを証明できる場合は、ご連絡ください。 こちらで変更いたします。

すでに「TISAXスコープ抜粋」を（いずれかの）審査機関に送付済みの場合は、ENXポータルで新しい拠点を作成し（該当する場合）、審査機関と変更について話し合ってください。審査機関が、変更内容に基づいて審査を実施し、ENXポータルのスコープ情報を更新します。

注意事項:

> ENXポータルで審査スコープを削除することはできません。誤って審査スコープを作成した場合は、ご連絡ください。 こちらで削除いたします。

4.5.8. 確認メール

上記の必須手続きがすべて完了した後、ENX協会がお申し込み内容を確認します。その後、確認メールをお送りします。

このメールには、次の二つの重要な内容が含まれています。

- すべてのTISAX審査機関の連絡先リスト
  リストの中から、貴社の審査スコープに対し審査を実施するTISAX審査機関を一つ選択してください。連絡先からオファーを依頼できます。
  審査機関の選定に関する詳細は、以下を参照してください：セクション 5.3. 審査機関の選択。
- 添付のPDFファイル「TISAX Scope Excerpt」（TISAXスコープ抜粋）

  ファイルには以下が含まれています。

  - データベースに保存されている情報
  - 貴社の参加企業ID
    以下のセクションを参照してください：セクション 4.5.8.1. Participant ID （参加企業ID）
  - 貴社のスコープID
    以下のセクションを参照してください：セクション 4.5.8.2. Scope ID （スコープID）

確認メールの例については、以下のセクションを参照してください：セクション 7.2. 附録：確認メールの例。

「TISAXスコープ抜粋」の例については、以下のセクションを参照してください：セクション 7.3. 附録：TISAXスコープ抜粋。

確認メールは通常3営業日以内にお送りします。

7営業日以内に連絡がない場合は、a） すべての情報を提供済みであること、b） 審査スコープのステータスが「ENXの承認待ち」であることをご確認ください。 登録の処理は、すべてが完了してから開始されます。すべてが完了したと思われるにもかかわらず、連絡がない場合は、こちらまでご連絡ください。

確認メールは、参加企業の主要連絡先に送信します。

> 注意事項:
>
> すべての審査スコープにはライフサイクルがあります。この段階では、審査スコープのステータスは「ENXの承認待ち」です。
>
> 審査スコープのステータスの詳細については、以下のセクションを参照してください：セクション 7.5.5. Assessment scope status “Awaiting your payment” （審査スコープステータス「支払い待ち」）。

次の二つのサブセクションでは、参加企業IDとスコープIDの目的について詳しく解説します。

4.5.8.1. Participant ID （参加企業ID）

参加企業IDは、

- TISAX参加企業を識別します。
- 参加企業ごとに一意です。
- 登録完了時に、ENX協会から付与されます。
- TISAX審査機関に情報セキュリティ審査を依頼するための前提条件です。
- 次のイラストのような形式です。

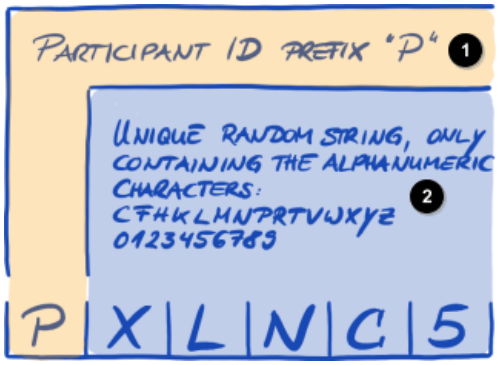


図 7. 参加企業IDの形式[12]

1. 参加企業IDの頭文字は「P」です。
2. 英数字のみからなる、一意のランダムな文字列です。
   CFHKLMNPRTVWXYZ
   0123456789

注意事項:

参加企業IDは、以下の二つの方法で調べられます。

1. 「TISAXスコープ抜粋」を確認します。
   上記セクション 4.5.8. 確認メールを参照してください。
2. ENXポータルにログインし、メインナビゲーションバーから“DASHBOARD”（「ダッシュボード」）を選択します。参加企業IDが表示されます。

4.5.8.2. Scope ID （スコープID）

スコープIDは、

- 審査スコープを識別します。
- 審査スコープごとに一意です。
- 登録完了時に、ENX協会から付与されます。
- TISAX審査機関に情報セキュリティ審査を依頼するための前提条件です。
- 次のイラストのような形式です。

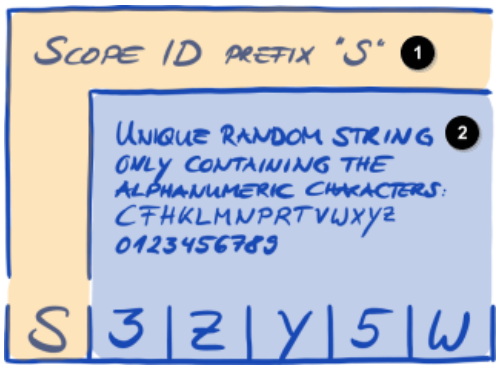


図 8. スコープIDの形式

1. スコープIDの頭文字は「S」です。
2. 英数字のみからなる、一意のランダムな文字列です。
   CFHKLMNPRTVWXYZ
   0123456789

注意事項:

スコープIDは、以下の二つの方法で調べられます。

1. 「TISAXスコープ抜粋」を確認します。
   上記セクション 4.5.8. 確認メールを参照してください。
2. ENXポータルにログインし、メインナビゲーションバーから「MY TISAX」、「SCOPES AND ASSESSMENTS（スコープと審査）」の順に選択します。スコープIDが表示されます。

注意事項:

すべての審査スコープ（スコープIDで識別）には、ライフサイクルが存在します。

審査スコープのステータスの詳細については、以下のセクションを参照してください：セクション 7.5. 附録：Assessment scope status（「審査スコープのステータス」）。

4.5.9. ステータス情報

この段階では、TISAXプロセスにおける貴社の状況を表す、二つの関連ステータスがあります:

1.参加企業ステータス
2.審査スコープステータス

次の図は、特定のステータスになるために満たさなければならない条件を示しています。

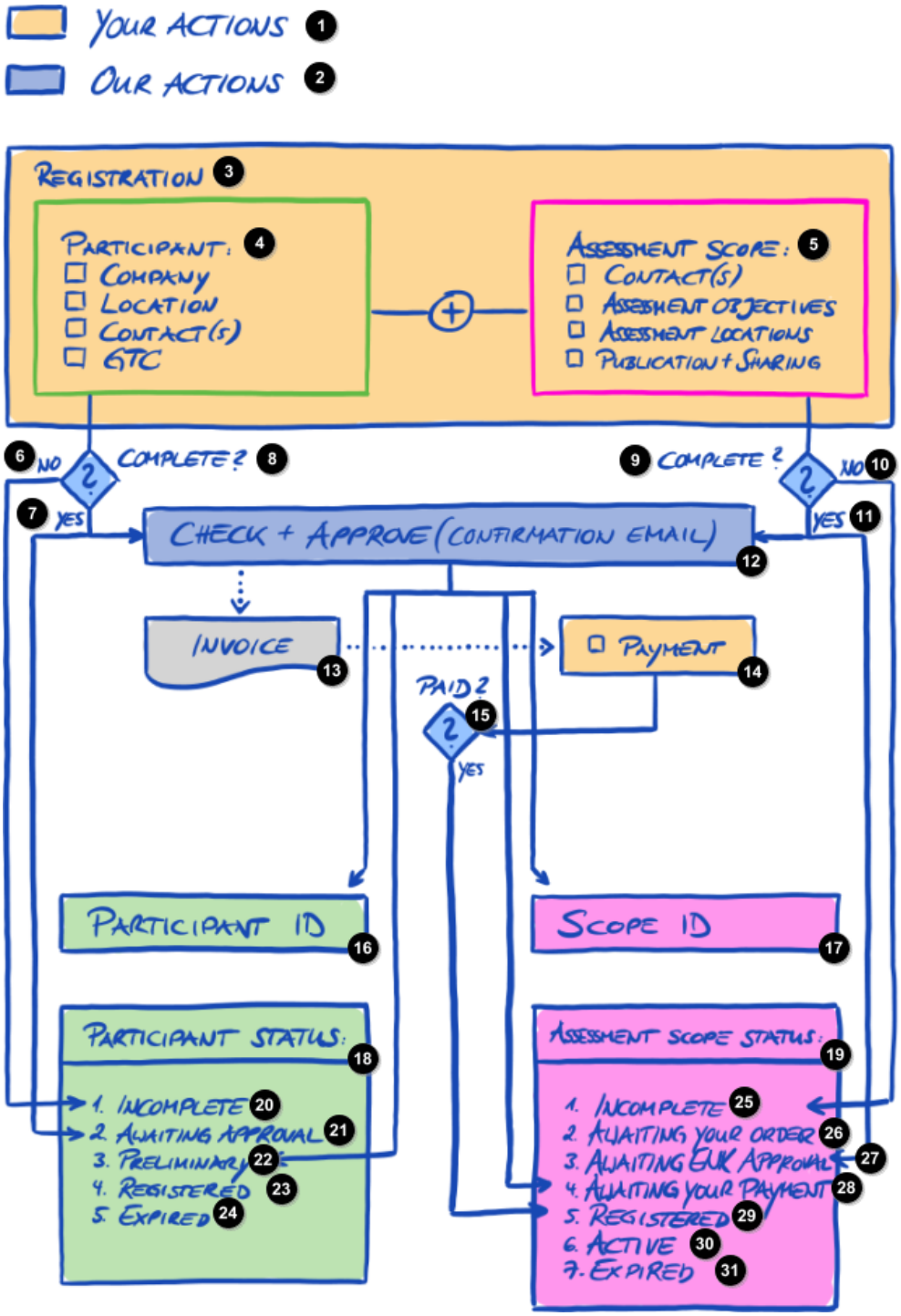


図 9. 参加企業ステータスと審査スコープステータスの条件

1. 貴社の行動
2. 我々の行動
3. 登録

4. 参加企業:
[ ] 企業
[ ] 拠点
[ ] 連絡先
[ ] 一般取引条件
5. 審査スコープ:
[ ] 連絡先
[ ] 審査目的
[ ] 審査拠点
[ ] 公開+共有
6. いいえ
7. はい
8. 完了?
9. 完了?
10. いいえ
11. はい
12. 確認+承認（確認メール）
13. 請求書
14. [ ] 支払い
15. 支払い済み?
16. 参加企業ID
17. スコープID
18. 参加企業ステータス:
19. 審査スコープステータス:
20. 1.未完了
21. 2.承認待ち
22. 3.予備
23. 登録済み
24. 期限切れ
25. 1.未完了
26. 2.貴社の依頼待ち
27. 3.ENXの承認待ち
28. 4.支払い待ち

29 5.登録済み

30 6.アクティブ

31 7.期限切れ

附録に、ステータスの定義および次のステータスに進むために必要なことが記載されています。

詳細は以下のセクションでご確認いただけます。

- 参加企業ステータスについては次を参照してください:
  セクション 7.4. 附録：Participant status（参加企業ステータス）。
- 審査スコープステータスについては次を参照してください:
  セクション 7.5. 附録：Assessment scope status（「審査スコープのステータス」）。

4.5.10. 登録情報の変更

注意事項:

以下のセクションに、データのライフサイクルに関するあらゆる疑問への回答が記載されています：セクション 7.9. 附録：参加企業データのライフサイクル管理。
企業名や連絡先などのデータを変更または更新したい場合の手順が記載されています。

これで、TISAX参加企業として登録されました。TISAXプロセスの次のステップに進む準備ができました。

5. 審査（ステップ2）

本資料の、審査セクションを読むのにかかる時間はおよそ30分から35分です。

5.1. 概要

第二のステップが、TISAX審査です。TISAX審査を受けるための大半の作業は、ここで行われます。

以下のセクションでは、審査について説明します:

1. まず、ISAの自己評価を利用して、TISAX審査の準備が整っているかを調べる方法について解説します。
2. 次に、TISAX審査機関の選び方について解説します。
3. 次に、審査プロセスがどのように進むかを解説します。
4. 最後に、「プロセスの結果」である審査結果と、それに伴うTISAXラベルについて解説します。

5.2. ISAに基づく自己評価

TISAX審査の準備を整えるには、まず情報セキュリティマネジメントシステム（ISMS）を最高の状態にする必要があります。貴社のISMSが求められる成熟度レベルに合致しているか把握するためには、ISAに基づく自己評価を実施する必要があります。

「情報セキュリティ審査」（ISA）は、「ドイツ自動車工業会」（Verband der Automobilindustrie e.V. 略称VDA）が発行する基準カタログです。ISAは、自動車業界における情報セキュリティ審査基準です。

以下のセクションでは、ISAに基づく自己評価を実施するための実践的な指示に重点を置いています。

本資料の説明や例、スクリーンショットは、ISAの第5版に基づいています。

注意事項:

ISAの旧版からの変更点については、Excelシートの「Change history」（変更履歴）をご覧ください。

注意事項:

VDAが新版を発行した際に、ISAのどのバージョンが貴社の審査に適用されるかについては、以下のセクションを参照してください: セクション 7.11. 附録: ISAのライフサイクル管理。

5.2.1. ISAドキュメントのダウンロード

ISAドキュメントをダウンロードして、自己評価を開始します。

ISAドキュメントは、以下のページからダウンロードできます。
enx.com/en-US/TISAX/downloads/

Excelファイルは、以下のページから直接ダウンロードできます。
portal.enx.com/isa5-en.xlsx

ISAドキュメントは、ドイツ語版もあります。
enx.com/de-de/TISAX/downloads/

5.2.2. ISAドキュメントについて理解する

自己評価を始める前に、役に立つ情報をご紹介します。主に、TISAX審査の利用を念頭に置いた、ISAドキュメントの公式な説明と定義について解説します。

5.2.2.1. 基準カタログ

ISAには、現在以下の三つの「基準カタログ」があります。[13]

1.	情報セキュリティ	Information Security
2.	プロトタイプの保護	Prototype Protection
3.	データ保護	Data Protection

各基準カタログには、それぞれ以下のようにExcelシートが割り当てられています。

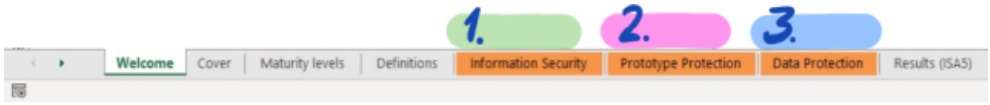


図 10. ISA基準カタログのExcelシートのスクリーンショット

貴社にとってどの基準カタログが適切かは、貴社の審査目的によって異なります。

どの基準カタログのどの要求事項が適用されるかは、審査目的ごとに定義されます。一つの基準カタログの要求事項のみが適用される審査目的もあれば、複数の基準カタログからの要求事項が適用される審査目的も存在します。

前述の審査目的は、各基準カタログに以下のように対応します。

番号	審査目的（Assessment objective）	ISA基準カタログ
1.	Info high	Information Security （情報セキュリティ）
2.	Info very high	Information Security （情報セキュリティ）
3.	Confidential	Information Security （情報セキュリティ）
4.	Strictly confidential	Information Security （情報セキュリティ）
5.	High availability	Information Security （情報セキュリティ）
6.	Very high availability	Information Security （情報セキュリティ）
7.	Proto parts	Prototype Protection （プロトタイプの保護）
8.	Proto vehicles	Prototype Protection （プロトタイプの保護）
9.	Test vehicles	Prototype Protection （プロトタイプの保護）
10.	Proto events	Prototype Protection （プロトタイプの保護）
11.	Data	Information Security （情報セキュリティ） Data Protection （データ保護）
12.	Special data	Information Security （情報セキュリティ） Data Protection （データ保護）

表 7. TISAX審査目的とISA基準カタログの対応関係

例えば、貴社が「データ保護」の審査目的を選択した場合、「情報セキュリティ」および「データ保護」の基準カタログの質問に答える必要があります。

上記のように、各基準カタログには、複数の審査目的が割り当てられています。それでは、要求事項と審査目的の対応関係はどうでしょうか?

次の表に、審査目的にどの要求事項が該当するか示します。

番号	審査目的（Assessment objective）	該当する要求事項
1.	Info high	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列
2.	Info very high	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列 ◦（「非常に高い保護ニーズの追加要求事項」）列
3.	Confidential	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列 （Confidentialityの「C」が付いているもののみ（Confidentiality = 機密性））

番号	審査目的（Assessment objective）	該当する要求事項
4.	Strictly confidential	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列 （Confidentialityの「C」が付いているもののみ（Confidentiality = 機密性）） ◦ （「非常に高い保護ニーズの追加要求事項」）列 （Confidentialityの「C」が付いているもののみ（Confidentiality = 機密性））
5.	High availability	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列 （Availabilityを意味する「A」が付いているもののみ（Availability = 可用性））
6.	Very high availability	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列 （Availabilityを意味する「A」が付いているもののみ（Availability = 可用性）） ◦ （「非常に高い保護ニーズの追加要求事項」）列 （Availabilityを意味する「A」が付いているもののみ（Availability = 可用性））

番号	審査目的（Assessment objective）	該当する要求事項
7.	Proto parts	▪ 基準カタログ“Prototype Protection”（「プロトタイプの保護」） ただし以下の章のみ： 8.1 Physical and Environmental Security（8.1 物理的・環境的セキュリティ） 8.2 Organizational Requirements（8.2 組織の要件） 8.3 Handling of vehicles, components and parts（8.3 車両、部品、コンポーネントの取り扱い） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列
8.	Proto vehicles	▪ 基準カタログ“Prototype Protection”（「プロトタイプの保護」） ただし以下の章のみ： 8.1 Physical and Environmental Security（8.1 物理的・環境的セキュリティ） 8.2 Organizational Requirements（8.2 組織の要件） 8.3 Handling of vehicles, components and parts（8.3 車両、部品、コンポーネントの取り扱い） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for vehicles classified as requiring protection”（「要保護車両に分類される車両の追加要求事項」）列
9.	Test vehicles	▪ 基準カタログ“Prototype Protection”（「プロトタイプの保護」） ただし以下の章のみ： 8.2 Organizational Requirements（8.2 組織の要件） 8.3 Handling of vehicles, components and parts（8.3 車両、部品、コンポーネントの取り扱い） 8.4 Requirements for trial vehicles（8.4 試乗車の要件） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列

番号	審査目的（Assessment objective）	該当する要求事項
10.	Proto events	▪ 基準カタログ“Prototype Protection”（「プロトタイプの保護」） ただし以下の章のみ： 8.2 Organizational Requirements（8.2 組織の要件） 8.3 Handling of vehicles, components and parts（8.3 車両、部品、コンポーネントの取り扱い） 8.5 Requirements for events and shootings（8.5 イベントおよび撮影に関する要件） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列
11.	Data	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列 （Confidentialityの「C」が付いているもののみ（Confidentiality = 機密性）） ▪ 基準カタログ“Data Protection”（「データ保護」） ◦ “Requirements (must)”（「要求事項（必須）」）列
12.	Special data	▪ 基準カタログ“Information Security”（「情報セキュリティ」） ◦ “Requirements (must)”（「要求事項（必須）」）列 ◦ “Requirements (should)”（「要求事項（推奨）」）列 ◦ “Additional requirements for high protection needs”（「高い保護ニーズの追加要求事項」）列 （Confidentialityの「C」が付いているもののみ（Confidentiality = 機密性）） ◦ （「非常に高い保護ニーズの追加要求事項」）列 （Confidentialityの「C」が付いているもののみ（Confidentiality = 機密性）） ▪ 基準カタログ“Data Protection”（「データ保護」） ◦ “Requirements (must)”（「要求事項（必須）」）列

表 8. 審査目的ごとに該当する要求事項

注意事項:

「高い保護ニーズの追加要求事項」および「非常に高い保護ニーズの追加要求事項」の2列の各要求事項には、Confidentiality（Confidentiality = 機密性）の「C」またはIntegrity（Integrity = 完全性）の「I」、あるいはAvailability（Availability = 可用性）の「A」、またはこれら3文字の組み合わせが付与されます。

上の表で、これらの2列の要求事項から前述の文字のうちの一つが記された要求事項に絞り込む場合、絞り込まれた要求事項には、その文字に加えて他の文字も記された要求事項も含まれます。

例えば上の表で「C」が指定されている場合、「（C）」、「（C、I、A）」または「（C、I）」が記されたすべての要求事項が適用されます（審査目的「Special data」など）。

下のスクリーンショットは、「情報セキュリティ」基準カタログのコントロール質問の主な要素を示しています（他の基準カタログには、これらの要素のサブセットのみ存在します）。すべての要素について、さらに下で解説します。

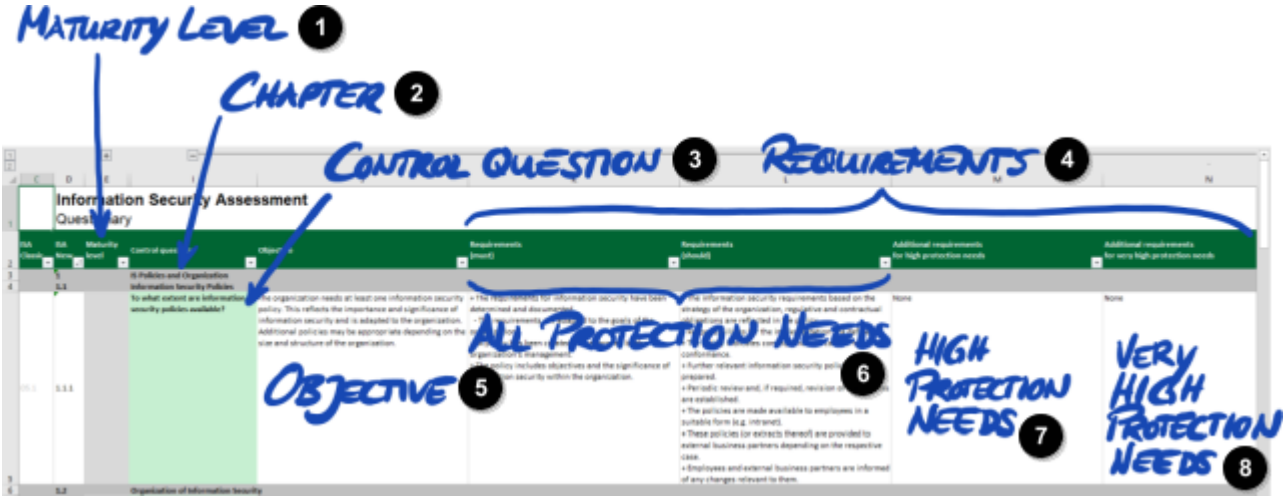


図 11. ISA基準カタログ「情報セキュリティ」の質問の主な要素のスクリーンショット

1. 成熟度レベル
2. 章
3. コントロール質問
4. 要求事項
5. 目的
6. すべての保護ニーズ
7. 高い保護ニーズ
8. 非常に高い保護ニーズ

5.2.2.2. 章立て

各基準のカタログは、質問を章立てて分類しています。

例：「2 人事部」

グループ分けは、企業における一般的な責任に基づいて行われます。各部門は、「Usual person responsible for process implementation」（プロセス実施に関する通常の責任者）（上記の例では「人事部」）の列で指定されます。

5.2.2.3. コントロール質問

各基準カタログの質問は、Excelの各シートに記載されています。

例：「4.1.2 ネットワークサービス、ITシステム、ITアプリケーションへのユーザーアクセスはどの程度安全か？」

コントロール質問は「コントロール」とも呼ばれます。これは監査人が用いる言葉です。ISAが基盤とするISO規格では、「コントロール」という用語を使用しています。

5.2.2.4. 自己評価フォームフィールド

“Maturity level”（「成熟度レベル」）と“Control question”（「コントロール質問」）列の間には、自己評価を実施する際に記入する必要のあるフォームフィールドがあります。

フォームフィールド	目的	必須かどうか
Implementation description（実施内容）（F列）	ここでは、貴社でこのコントロール質問に対処するために実施した内容を簡潔に記述します。	必須
Reference Documentation（参照ドキュメント）（G列）	実施を証明するためのドキュメントを指定します。	必須
Findings/Result （指摘事項/結果）（H列）	あるべき姿と現状の間にギャップがあると思われる分野について、指摘事項を記入します。	任意

表 9. 自己評価フォームフィールドとその目的

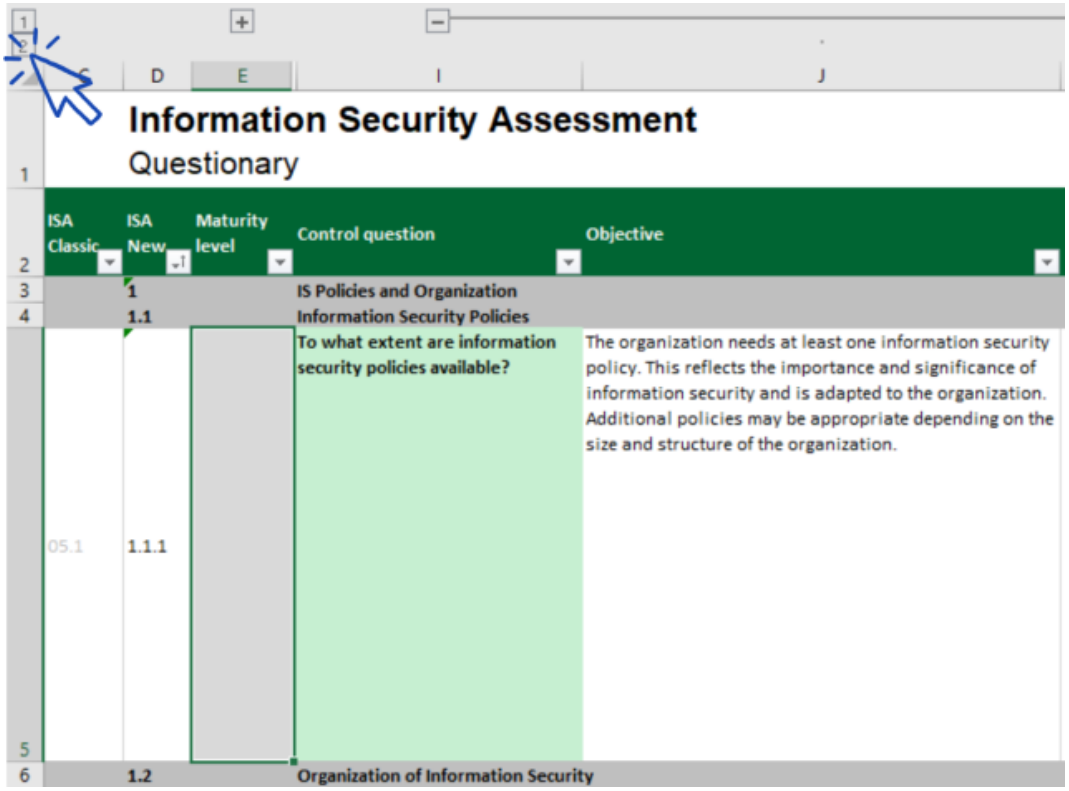
実施内容の簡単な記述とドキュメントの参照のみ必須です。この情報は、TISAXの審査機関が貴社をよりよく理解し、審査を準備する際に役立ちます。

以下は、自己評価をサポートするためのオプションの列です。

- Measures/recommendations （対策/推奨事項） （R列）
- Date of assessment （審査日） （S列）
- Date of completion （完了日） （T列）
- Responsible department （担当部署） （U列）
- Contact （連絡先） （V列）

重要事項:

ダウンロードしたExcelファイルを開き、基準カタログのワークシート（情報セキュリティ等）を選択しても、おそらく自己評価フォームフィールドはそのままでは表示されません。これを表示するには、レベル「2」[14]。 ボタンは、C1セルの左上にあります。これにより表示が拡大され、自己評価フォームフィールドが表示されます。



もう一つのアドバイスは、矢印キーを使って下にスクロールすることです。セルのサイズが大きいため、スクロ☒ールバーを使ったスクロールでは制御しにくい場合があります。マウス等のスクロール機能を使うと、誤って大きなセルをスキップしてしまう可能性もあります。

5.2.2.5. 目的

「コントロール質問」列の右側に「目的」列（J列）があります。ここには、情報セキュリティマネジメントの該当する側面から達成すべきことが記載されます。

例（コントロール質問4.1.2の場合）：「安全に識別された（認証された）ユーザーだけにITシステムへのアクセス権限を付与します。この目的のため、適切な手順により、利用者のIDを安全に決定します。」

5.2.2.6. 要求事項

要求事項は、目的を達成する上で満たすことが求められる事項です。

要求事項は以下の4列に分かれています。

1. Requirements (must) （要求事項（必須） （K列）
2. Requirements (should) （要求事項（推奨）） （L列）

3. Additional requirements for high protection needs （●高い保護ニーズの追加要求事項） （M列）
4. Additional requirements for very high protection needs （●非常に高い保護ニーズの追加要求事項） （N列）

達成すべき保護ニーズ（審査目的から導出）までのすべての要求事項を満たす必要があります。

審査目的によっては、要求事項のサブセットのみが適用されます。要求事項の適用スコープについては、セクション 5.2.2.1. 基準カタログの表 8. 審査目的ごとに該当する要求事項と、特にセクション末尾の注意事項をご参照ください。

要求水準「必須」と「推奨」のISA定義については、Excelシート“Definitions”（「定義」）の「重要な用語」を参照してください。

重要事項:

各要求事項は、目的の内容とその意図を正しく理解した上で満たすことが非常に重要です。要求事項を字面通りに満たしていても、貴社が目的（J列）の内容とその意図を正しく理解した上で、要求事項を満たしていると審査機関が判断するとは限りません。

要求事項とその表記は、規模を特定しない、架空の平均的な企業を想定して理論的に決められています。

審査機関は、必ず貴社における独自の実施内容を、貴社の目的に照らし合わせる必要があります。平均的な企業にとって適切であっても、貴社が置かれている特定の状況下では不十分な可能性があります。

詳細は以下のセクションを参照してください：セクション 5.2.5. 自己評価結果への対処。

5.2.2.7. 成熟度レベル

情報セキュリティマネジメントシステムのあらゆる側面における品質を審査するため、ISAは“maturity levels”（●「成熟度レベル」）の概念を採用しています。情報セキュリティマネジメントシステムが高度であればあるほど、成熟度レベルは高くなります。

ISAでは六つの成熟度レベルが設けられています。詳細な定義は、Excelシート“Maturity levels”（●「成熟度レベル」）に記載されています。成熟度レベルに関する統一的な理解を促すため、以下にISAで提供されている非公式な記述を引用します。

Maturity level （●成熟度レベル）	一言での表現	説明
0	Incomplete （●未完了）	プロセスが利用できない、プロセスに従っていない、またはプロセスが目的達成に適していない状態。
1	Performed （●実施済み）	文書化されていないか文書化が不完全なプロセスに従っており、その目的を達成する指標は存在する。
2	Managed （●管理済み）	目的を達成するプロセスに従っている。プロセスが文書化され、実施されたことを示す証跡がある。

Maturity level（●成熟度レベル）	一言での表現	説明
3	Established（●確立済み）	システム全体に統合された標準的なプロセスが適用されている。他のプロセスとの依存関係が文書化され、適切なインターフェースが作成されている。そのプロセスが、長期間にわたって持続的かつ積極的に使用されている証跡が存在する。
4	Predictable（●予測可能）	確立されたプロセスに従っている。プロセスの有効性は、主要データの収集を通じて継続的に監視されている。プロセスの有効性が不十分であると判断され、調整が必要とされる限界値が定義されている。（KPI）
5	Optimizing（●最適化）	継続的な改善を主目的とする予測可能なプロセスに従っている。改善は、専用のリソースによって積極的に進められている。

表 10. 成熟度レベルの非公式な記述

設問ごとに、貴社の情報セキュリティマネジメントシステムの成熟度レベルを評価してください。“Maturity level”（●「成熟度レベル」）（E列）に成熟度レベルを記入してください。

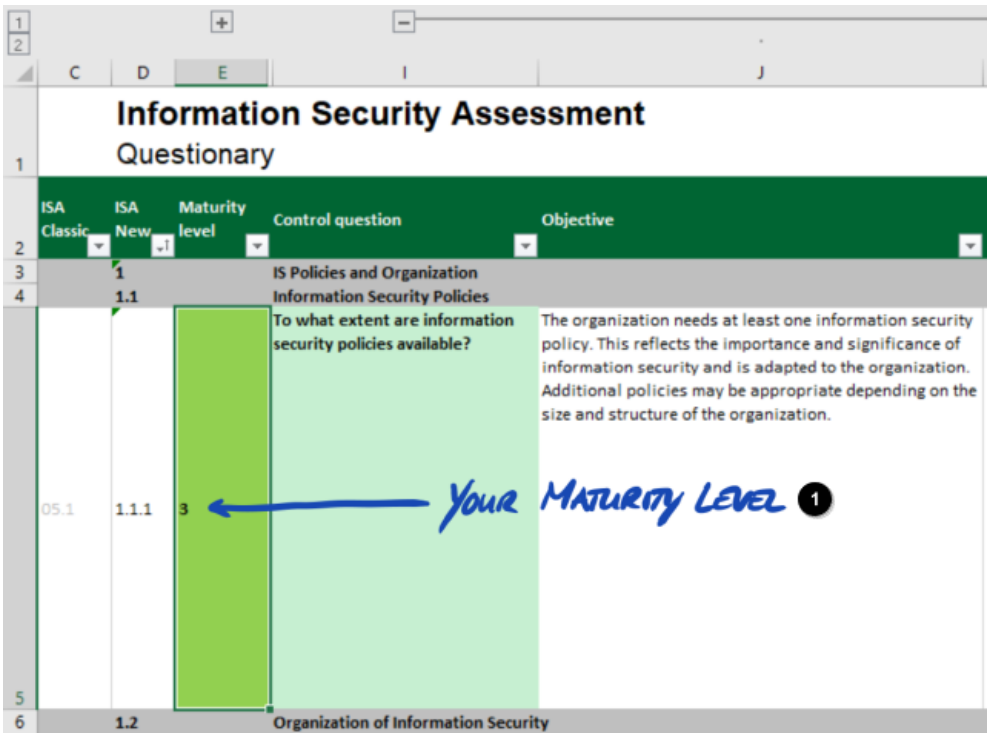


図 12. ISAドキュメント（Excelシート"Information Security"（「情報セキュリティ」））における成熟度レベルの選択例のスクリーンショット

1 貴社の成熟度レベル

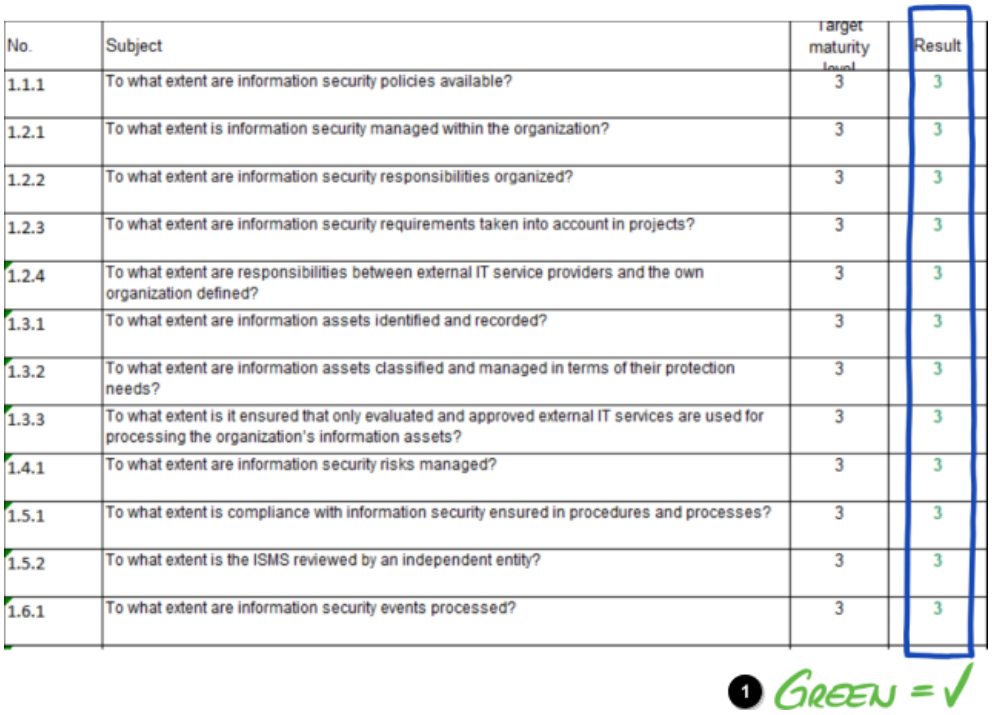
目標とする成熟度レベルと、それが審査結果に与える影響については、以下のセクションを参照してください：セクション 5.2.4. 自己評価結果の解釈。

以上で理解を深めた上で、自己評価を開始しましょう。

5.2.3. 自己評価の実施

Excelファイルを開き、審査目的に該当する各基準カタログのすべてのコントロール質問に目を通し、貴社の情報セキュリティマネジメントシステムの現状に適合する成熟度レベルを決定します。自身で最善と思われる判断を下してください。この段階では、正解・不正解はありません。

自己評価が完了したら、Excelシート「結果（ISA5）」の「結果」（H列）を、数字（0～5）または"n.a."（「該当なし」の意）で完全に埋めてください。



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

図 13. ISAドキュメント「結果（ISA5）」シートの例のスクリーンショット

1 緑

ISAに関する質問は、ENX協会までお問い合わせください。。

5.2.4. 自己評価結果の解釈

次の五つのサブセクションでは、自己評価結果の分析と解釈の方法について説明します。分析により、TISAX審査の準備が整っているか、まだ整っていないかが分かります。

5.2.4.1. 分析

自己評価結果の要約として、結果スコアを確認できます。

結果スコア（「目標成熟度レベルまでのカットバックを含む結果」）は、Excelシート「結果（ISA5）」（D6セル）にあります。「カットバック」については、すぐに説明します。

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE ❶ MAXIMUM RESULT SCORE

No.	Subject	Target maturity level	Result ❷
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

図 14. 結果スコアと最高結果スコア（Excelシート「結果（ISA5）」、D6およびG6セル）のスクリーンショット

❶ 結果スコア

❷ 最高結果スコア

自己評価の結果と結果スコアについて理解し、解釈する上で、以下の二つの分析レベルを区別する必要があります。

1. 質問レベル
   このレベルにはすべての質問が含まれます。質問ごとに、目標の成熟度レベルと、貴社の成熟度レベルが存在します。
2. スコアレベル
   このレベルには、すべての質問の結果をまとめた総合結果が含まれます。最高結果スコアと貴社の結果スコアが存在します。

下図は、分析レベルを表しています。

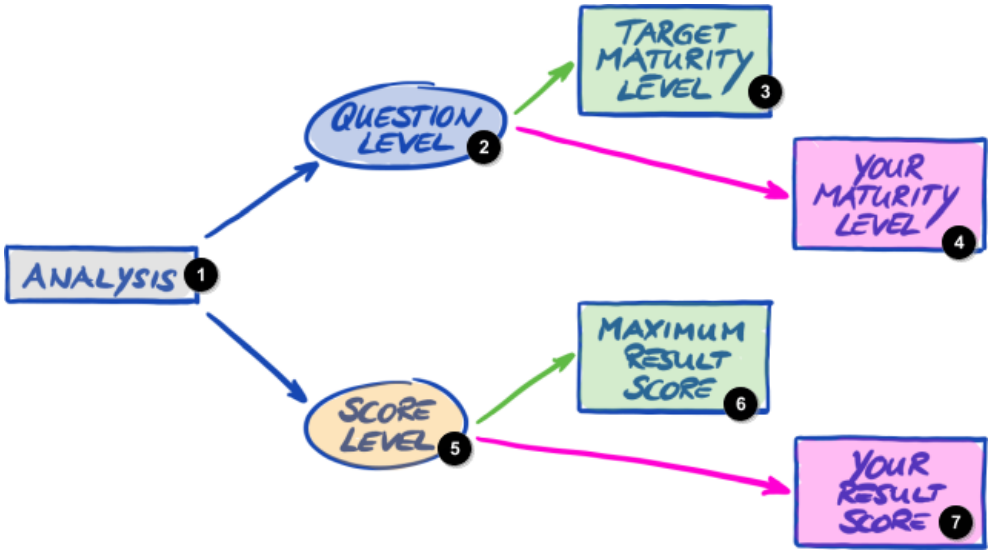


図 15. 質問レベルおよびスコアレベルでの自己評価結果の分析

❶ 分析

❷ 質問レベル

3. 目標の成熟度レベル
4. 貴社の成熟度レベル
5. スコアレベル
6. 最高結果スコア
7. 結果スコア

下図は、スコアレベルの結果と質問レベルの結果の場所を示しています。

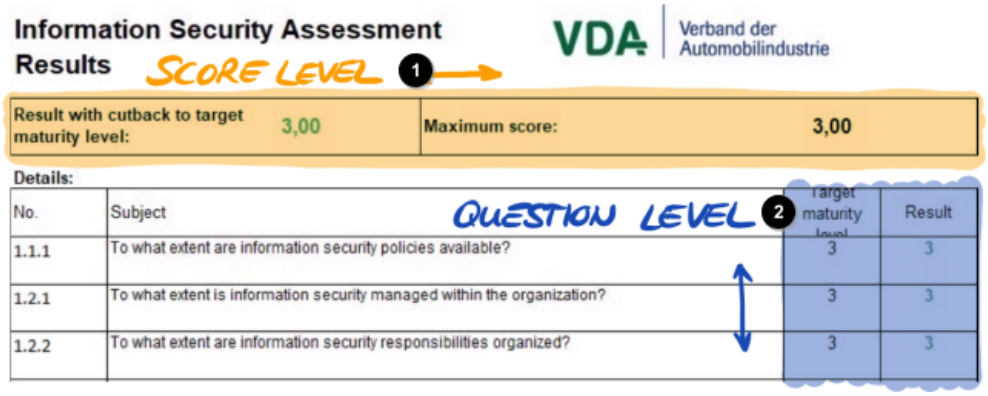


図 16. Excelシート「結果（ISA5）」のスコアレベルと質問レベル

1. スコアレベル
2. 質問レベル

次の図は、分析レベル、ISA目標定義、および貴社の結果を簡略化したものです。

図 17. 質問レベルおよびスコアレベルでの目標と貴社の結果

1. 目標の成熟度レベル
2. 貴社の成熟度レベル
3. 質問レベル
4. Q（質問）
5. TML（目標の成熟度レベル）
6. YML（貴社の成熟度レベル）
7. 最高結果スコア
8. 結果スコア
9. スコアレベル

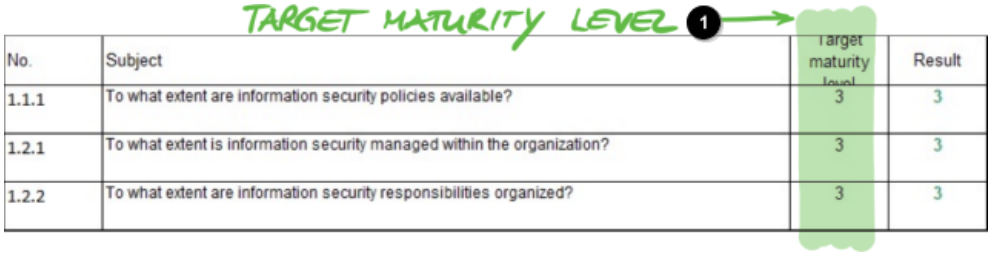
以下のセクションでは、結果と分析について詳しく説明します。

5.2.4.2. 目標成熟度（質問レベル）

ISAは、各質問の「目標成熟度レベル」を3に定義しています。

各成熟度レベルの定義については、以下を参照してください：セクション 5.2.2. ISAドキュメントについて理解する。

ISAは、Excelシート「結果（ISA5）」の中で目標成熟度レベルを定義しています（G列22行目以降、下図参照）。



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

図 18. Excelシート「結果（ISA5）」の目標成熟度レベルの定義

1 目標の成熟度レベル

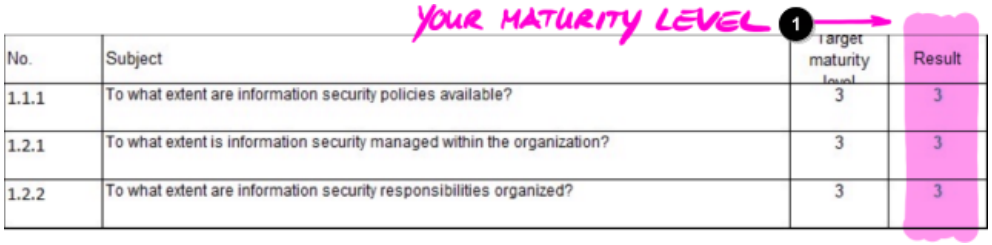
5.2.4.3. 貴社の結果（質問レベル）

TISAXラベルを取得するには、通常、各質問の成熟度レベルを目標成熟度レベル以上にする必要があります。

例えば、質問Xの目標成熟度レベルが「3」である場合、その質問に対する貴社の成熟度レベルは「3」以上でなければなりません。その質問の成熟度レベルが「3」未満である場合、TISAXラベルは取得できません。

これは、質問ごとに独立して達成する必要があります。二つの質問の目標成熟度レベルが「3」である場合、一つの質問の成熟度レベルが「2」であれば、もう一つの質問の成熟度レベルが「4」であっても、TISAXラベルは取得できません（過剰分で不足分を相殺することはできません）。

ISAドキュメントは、貴社の成熟度レベルをExcelシート「情報セキュリティ」（E列）からExcelシート「結果（ISA5）」に自動的に転送します（H列23行目以降）。



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

図 19. Excelシート「結果（ISA5）」の貴社の成熟度レベル

1 目標の成熟度レベル

貴社の成熟度は、ISAドキュメントで貴社の結果スコアが集約される前に、計算対象となります。基本的に、貴社の成熟度レベルは、目標成熟度レベルに「カットバック（減少）」されます。カットバックが行われるのは、成熟度レベルが目標成熟度レベルを上回っている質問と下回っている別の質問が同時に存在する時、二つの成熟度レベル間で相殺が発生しないようにするためです。

以下に、ISAがどのように質問レベルの結果を計算するかを説明します。

- 貴社の成熟度を、質問の目標成熟度と比較します。

- 貴社の成熟度レベルが目標成熟度レベルを上回っている場合、目標成熟度レベルまで「カットバック」します。
- 貴社の成熟度レベルが目標成熟度レベルを下回っている場合は、その質問では何も行われません。

例えば、下図のように目標成熟度レベルが「3」、貴社の成熟度レベルが「4」だとします。この質問に対する貴社の「カットバックされた結果」は「3」となります。

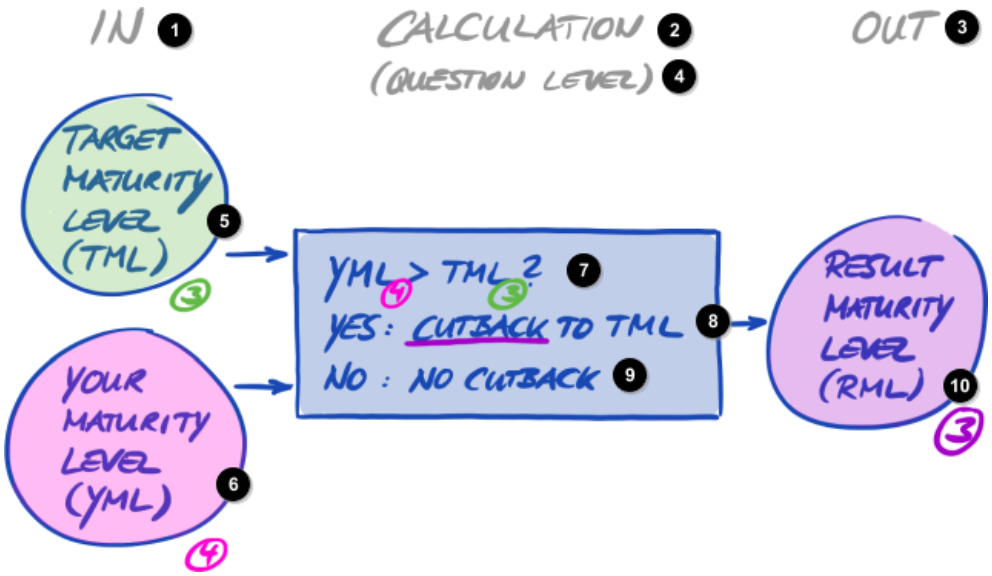


図 20. 結果成熟度レベルのカットバック計算

1. 入力
2. 計算
3. 出力
4. （質問レベル）
5. 目標の成熟度レベル（TML）
6. 貴社の成熟度レベル（YML）
7. YML > TML?
8. はい → TMLにカットバック
9. いいえ → カットバックなし
10. 結果成熟度レベル（RML）

下図は、貴社の成熟度レベルが目標の成熟度レベルより高ければ、ISAがそれをカットバックする様子を表しています（緑、オレンジ、赤の色は、「結果」列で使用されている色と一致します。以下を参照してください：図 19. Excelシート「結果（ISA5）」の貴社の成熟度レベル）。

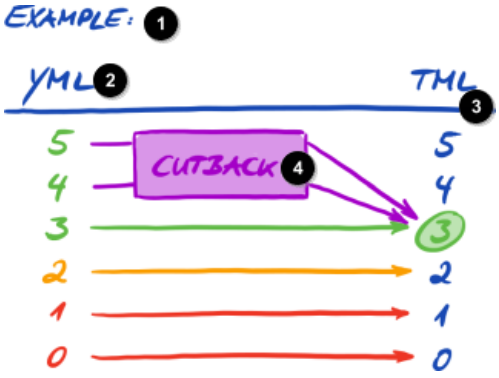


図 21. Excelシート「結果（ISA5）」で使用されている色を用いたカットバックの図解

1. 例:
2. YML
3. TML
4. カットバック

以下は、それぞれの質問レベルにおける成熟度レベルの別の表示方法です。丸の色は、目標成熟度、またはそこまでの「乖離」を示しています（例えば成熟度レベルが目標成熟度レベルより「-1」の場合、丸はオレンジ色になります）。チェックマークは、貴社の成熟度を示しています。

図 22. 質問レベルにおける成熟度レベル

1. 成熟度レベル
2. 質問
3. カットバック
4. 目標の成熟度レベル（TML）
5. TML +1以上

6 TML -1

7 TML -2以下

8 貴社の成熟度レベル（YML）

9 TMLへのカットバック

注意事項:

すべての質問で目標成熟度に達していなくても、TISAX審査に合格することは可能です。ここで主に問題とされるのは、関連するリスクがあるかどうかです。成熟度レベルが目標値を下回っていても、リスクがないのであれば、十分とみなされる場合があります。

5.2.4.4. 目標値（スコアレベル）

ISAでは、「理想的な」総合成熟度レベルを「最高結果スコア」（または「最高スコア」、G6セル）と定義しています。

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: MAXIMUM RESULT SCORE

No.	Subject	Target maturity level	Result 1
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

図 23. 最高結果スコア（Excelシート「結果（ISA5）」）

1 最高結果スコア

理論的に、この総合成熟度レベルは、（質問レベルの）すべての目標成熟度レベルの平均になります。すなわち、最高スコアは「3.0」です。

ただし、「3.0」となるのは、すべての質問が貴社の状況に適用される場合のみです。貴社の状況に適用されない質問があると、平均は変化し、最高結果スコアは「3.0」より低くなります。

さらに上に示した表示方法（図 22. 質問レベルにおける成熟度レベル）に基づき、最高結果スコアの平均に何が含まれるか、以下で確認できます。

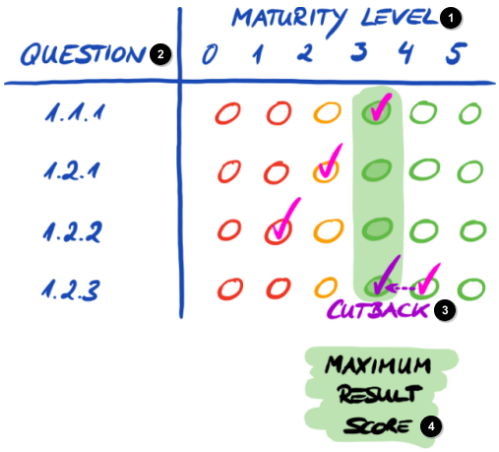


図 24. 最高結果スコア（スコアレベル）

1. 成熟度レベル
2. 質問
3. カットバック
4. 最高結果スコア

5.2.4.5. 貴社の結果（スコアレベル）

貴社の総合結果スコア（D6セル「目標成熟度レベルまでのカットバックを含む結果」）は、

- 貴社の情報セキュリティマネジメントシステムの全体的な成熟度レベルの概要を表します。
- 貴社のすべての成熟度レベル（質問レベル）の平均を表します。
- 最高結果スコア以下の値をとります。
- 可能な限り最高結果スコアに近づけることが望まれます。結果スコアが最高結果スコアを下回るほど、TISAXラベルが付与される可能性は低くなります。

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE 1

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

図 25. 貴社の結果スコア（Excelシート「結果（ISA5）」）

1. 結果スコア

上に示した表示方法（図 22. 質問レベルにおける成熟度レベル）を再度用いることで、最高結果スコアの平均に何が含まれるか、以下のように確認できます。

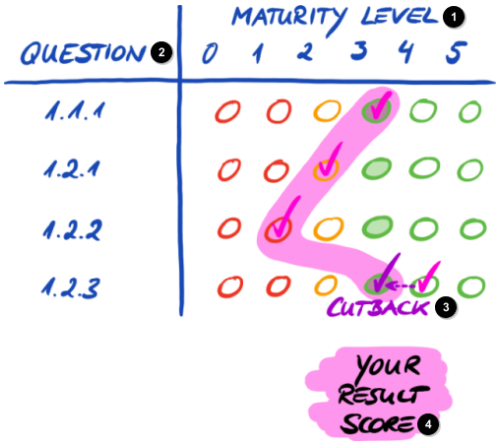


図 26. 貴社の結果スコア（スコアレベル）

1. 成熟度レベル
2. 質問
3. カットバック
4. 結果スコア

結果スコアにより、貴社について以下の事柄が分かります。

- TISAX審査を受ける準備ができているか。
- TISAXラベルの取得が期待できるか。

結果スコア（「目標成熟度レベルへのカットバックを行った値」）が「3.0」を下回っている場合、少なくとも一つの質問について成熟度レベルが目標成熟度レベルに一致していません。この場合、TISAX審査の準備を整える前に、情報セキュリティマネジメントシステムを改善する必要があると考えられます。

注意事項:

総合スコアの場合、結果スコアと最高結果スコア（「目標成熟度レベルまでカットバックした値」）間の許容可能な「乖離」には、公式の限界値が設定されています。

結果スコアが

- 10%下回る場合、総合審査結果は「軽微な不適合」となります。
- 30%下回る場合、総合審査結果は「重大な不適合」となります。

重要事項:

結果スコア（「目標成熟度レベルにカットバックした値」）が「3」であっても、TISAX審査で禁止事項が発見されず、必ず合格すると保証されるわけではありません。審査機関は、それぞれの側面で、貴社とは異なる見方をする可能性があることをご留意ください。

5.2.4.6. 準備は整いましたか?

上記の分析の目的は、貴社がTISAX審査を受ける準備ができているか把握することです。

結果スコア（「目標成熟度レベルまでカットバックした値」）が「3.0」（またはそれに近い値）の場合、貴社は間違いなくTISAX審査の準備ができています。この時、「結果」列（H）の値はすべて緑色になります（オレンジ色や赤色はありません）。

緑色でない場合は、自己評価結果に対処する必要があります（セクション 5.2.5. 自己評価結果への対処を参照）。

下図は、Excelシート「結果（ISA5）」に関するISAのレーダーチャートです。緑色の線は、章ごとの目標成熟度レベルを示しています。貴社の成熟度レベルがこの線上またはこれより上にあれば、TISAX審査を受ける準備ができています。この線より低い場合は、TISAXラベルを取得するには不十分な可能性があります。

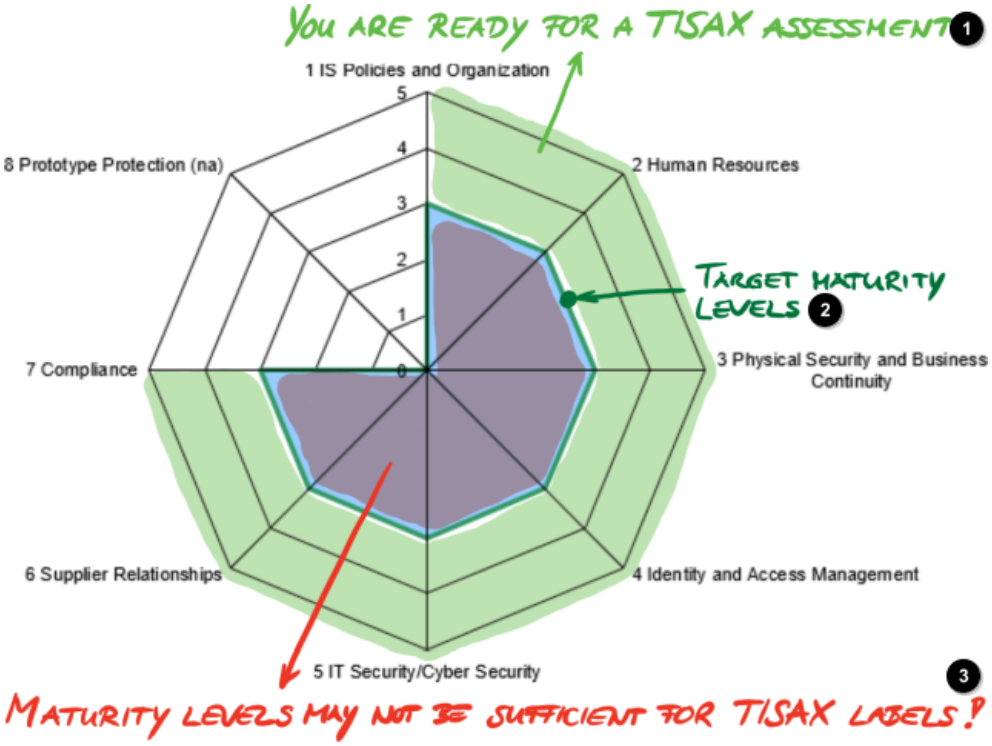


図 27. ISAレーダーチャートにおける目標成熟度レベルの達成度（Excelシート「結果（ISA5）」）のスクリーンショット

1. TISAX審査の準備が整った状態
2. 目標成熟度レベル
3. TISAXラベル取得には不十分な可能性のある成熟度レベル

ISAレーダーチャートを質問レベルに「変換」すると、質問レベルでも同様に緑・赤で表示されます。

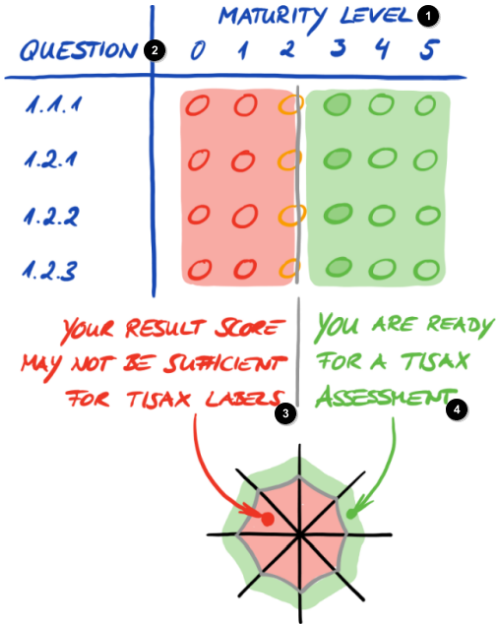


図 28. ISAレーダーチャートの「変換」

1. 成熟度レベル
2. 質問
3. 結果スコアがTISAXラベルの取得には不十分な可能性
4. TISAX審査の準備が整った状態

5.2.5. 自己評価結果への対処

自己評価の結果から、TISAXラベルの取得前に、情報セキュリティマネジメントシステムの改善が必要だと分かる場合があります。

成熟度レベルと目標成熟度レベル間にギャップがある場合、ギャップを埋める方法がすでに分かっていることもありますが、外部からのアドバイスが必要な場合もあります。この場合、TISAX審査機関にコンサルティングサービスを依頼できます。TISAXは、審査機関がコンサルティングを行うことを認めていますが、コンサルティングを義務付けているわけではありません。コンサルティングを行う審査機関は、TISAX審査を実施できませんのでご注意ください。

重要事項:

多くの企業がつまずく原因が、審査を受ける前に自己評価結果に適切に対処していないことです。
要求事項に従った情報セキュリティマネジメントシステム構築に必要な労力を、過小評価しないようご注意ください。多くの企業で、TISAX審査の準備のために大規模なプロジェクトを正式に立ち上げる必要があります。

注意事項:

TISAXの手続きを進めるために外部の支援をお探しの場合、さまざまな企業がコンサルティングやトレーニングのサービスを提供しています。いずれの企業も、ENX協会とは無関係です。

現在、ENX協会は

- 直接的に、あるいは第三者を通じて、公式なトレーニングを提供していません。
- したがって、第三者のサービスの質については一切言及しないため、ご注意ください。

注意事項:

「事前審査」や「ギャップ分析」等の項目に関する要求・依頼はお勧めしません。これらの手順を踏んだ上で審査に備えたいという考えは分かりますが、審査をそのまま開始する方が理にかなっているケースが大半です。

事前審査をお勧めしない理由に関する詳細は、以下をご参照ください。セクション 7.7. 附録: 「事前審査」と「ギャップ分析」が効果的ではない理由。

5.3. 審査機関の選択

TISAX審査を実施できるのは、ENX協会が契約した審査機関だけです。[15]。 TISAX審査機関は、貴社に対して過去にコンサル
ティング業務を行ったことがない場合に限り、貴社のTISAX審査を実施できます。

すべてのTISAX審査機関は、登録されたTISAX参加企業に対してのみTISAX審査を実施する義務があります。

重要事項:

TISAX審査スコープを登録したら、審査機関への連絡を開始することを推奨します。審査機関は、一定のリードタイムを必要とします。準備を終えてから連絡すると、不必要な遅れが生じる可能性があります。

注意事項:

すべての審査スコープにはライフサイクルがあります。この段階で、審査スコープは「承認済み」または「登録済み」のステータスでなければなりません。

審査スコープのステータスの詳細については、以下のセクションを参照してください: セクション 7.5.5. Assessment scope status “Awaiting your payment” （審査スコープステータス「支払い待ち」）。

5.3.1. 連絡先情報

TISAX審査スコープの登録後は、すべてのTISAX審査機関に連絡し、オファーを依頼できます。連絡先情報は、受信した登録確認メールに記載されています[16]（セクション 4.5.8. 確認メールを参照）。

注意事項:

TISAX審査機関へのオファーの依頼は、登録「後」に行ってください。審査機関は、登録を確認します。登録されていない場合、審査機関は依頼を拒否せざるを得ません。

審査機関の連絡先が登録確認メールにのみ記載され、公開ウェブサイトでは確認できないのもこのためです。

5.3.2. 国および地域

現在、審査機関の連絡先の多くはドイツに拠点を置いていますが、重要な点として、基本的にはどの審査機関も、世界中でTISAX審査を実施できます。審査機関の大半は、多くの国に自分たちの従業員を配置しています。

ENX協会のウェブサイトでは、国を選択することで、どの審査機関がその国に営業担当や監査人を展開しているかを確認できます（enx.com/en-US/TISAX/xap/）。

5.3.3. オファーの依頼

TISAXの審査機関が審査にかかる工数を正確に計算・予測できるように、必ず「TISAXスコープ抜粋」を添付してください。

図 29. スコープ抜粋のサムネイル（1ページ目）

詳細は以下のセクションを参照してください：セクション 4.5.8. 確認メール。

注意事項：

公平性は、TISAX審査機関にとって重要な特性です。TISAX審査機関は、利益相反関係がないことを確認します。審査機関に連絡する際には、この点を考慮することをお勧めします。貴社が審査機関と何らかの関係がある場合、その機関による審査は期待できません。

5.3.4. オファーの評価

TISAX審査機関は、貴社が自由に選択できます。すべての審査機関は、同じ契約を結んでいます。すべての審査機関は、同じ基準と同じ監査方法に基づいて審査を実施します。審査結果については、どの審査機関を選んでも違いはありません。貴社の審査結果は、すべてのTISAX参加企業が受け入れます。

オファーの際は、価格、評判、好ましさといった明らかな要因の他に、以下の要素についても検討できるでしょう。

- 予約状況
  審査をいつから開始できるかというのも、TISAX審査を急ぐ場合は重要かもしれません。
- オンサイトのアポイントメントにかかる出張費用
  貴社の国に事務所がある審査機関の方が、出張費用が安く済むかもしれません。
- 言語
  監査人は、あなたや貴社の他の面談対象者と母国語でコミュニケーションできるでしょうか。
- 審査の範囲
  どの審査が含まれているでしょうか。

審査の詳細については、以下のセクションを参照してください：セクション 5.4.3. TISAX審査の種類。
通常、オファーには初回審査と是正計画の審査が含まれます。フォローアップ審査は、工数の予測が困難なため、通常は他の審査の完了後にオファーされます。

最終的には、信頼関係が重要になります。審査機関は、貴社についてかなりの情報を得ることになるため、審査機関との信頼関係を構築する必要があります。

注意事項:

「事前審査」や「ギャップ分析」等の項目に関する要求・依頼はお勧めしません。これらの手順を踏んだ上で審査に備えたいという考えは分かりますが、審査をそのまま開始する方が理にかなっているケースが大半です。

事前審査をお勧めしない理由に関する詳細は、以下をご参照ください。セクション 7.7. 附録：「事前審査」と「ギャップ分析」が効果的ではない理由。

注意事項:

審査機関による審査の請求額をお伝えしたいところですが、この情報を提供するのは不可能であることをご理解ください。それは、費用があまりにも多くの要因に左右されるからです。また、TISAXの審査機関は、商業的な計算については自由に決定できます。

しかし、審査機関が貴社に請求する工数について、大まかな概算をいくつか挙げることはできます。一つの拠点を持つ平均的な中小企業の場合、審査レベル 2の審査には3.5〜4人日、審査レベル 3の審査には5〜6人日が必要となります。

注意事項:

すべての審査にはライフサイクルがあります。

審査のステータスの詳細については、以下を参照してください：セクション 7.6. 附録：Assessment status（審査ステータス）。

TISAX審査機関を選択したら、いよいよTISAX審査プロセスを開始できます。

5.4. TISAX審査プロセス

5.4.1. 概要

TISAXの審査プロセスは、いくつかの種類の審査から構成されています。ほとんどの場合、複数の審査が行われます。

審査プロセスは、以下のような一連の手順として捉えられます。

- 貴社が、情報セキュリティマネジメントシステムを最高の状態に整えます。
- 貴社の情報セキュリティマネジメントシステムが定められた要求事項を満たしているかどうかを、審査機関が確認します。要求事項と現状にギャップが見つかる場合があります。
- その際は、定められた期間内にギャップを解消します。
- ギャップが解消したかを、審査機関が再度確認します。

このような手順を交互に、すべてのギャップが解消するまで繰り返します。

審査プロセスにおいて、各サブステップを開始するのは貴社自身であることを理解することが重要です。審査プロセス全体は、貴社のコントロール下にあります。そしてもちろん、いつでも好きな時に査定プロセスを中断し、終了することも可能です。[17]

TISAXの審査プロセスは、以下のようなマクロ構造になっています。

- キックオフミーティング
  貴社と審査機関が、審査プロセスの詳細を計画します。
- 審査フェーズ1
  審査機関が、貴社の自己評価を確認します。
- 審査フェーズ2
  審査機関が、審査を実施します。

5.4.2. キックオフミーティング

TISAXの審査プロセスは、キックオフミーティングから始まります。キックオフミーティングは、審査プロセスの詳細を計画する場です。通常、キックオフミーティングは電話会議で行われます。審査機関が、会議を進行します。

とりわけ、以下の点が議題となります。

- ミーティングの参加者
- 審査を受ける企業について
- TISAXの審査プロセスがどのように行われるか
- 審査スコープの内容と、スコープが適切か
- 利益相反はないか
- 良い自己評価とはどのようなものか
- 誰が何に責任を持つか
- どのようにコミュニケーションを取るか
- 審査がいつ行われるか（およびその他の時間についての計画）
- 審査に誰が参加する必要があるか
- 苦情がある場合は誰に連絡すれば良いか

キックオフミーティングが終わってから、通常は1〜3か月後に自己評価を提出します。しかし、6か月後となる場合も珍しくありません。この期間は、準備状況によって異なります。TISAXは、提出期限を義務付けていません。自己評価の準備に必要なだけの時間をとって、審査に備えることができます。

5.4.3. TISAX審査の種類

TISAXの審査プロセスは、以下の3種類からなります。

- 初回審査（Initial assessment）
- 是正計画審査（Corrective action plan assessment）
- フォローアップ審査（Follow-up assessment）[18]

初回審査は必ず行われます。他の2種類のTISAX審査は、複数回にわたって行われることがあります。これらの審査は、以下のいずれかの状況になるまで行われます。

- すべてのギャップが解消される
- 貴社がTISAX審査プロセスを打ち切る
- 初回審査のクロージングミーティング終了後、最長期間の9か月が経過（この場合、再度の初回審査が必要）

すべてのTISAX審査について、以降のセクションで解説します。

注意事項:

すべての審査にはライフサイクルがあります。

審査のステータスの詳細については、以下を参照してください：セクション 7.6. 附録：Assessment status（審査ステータス）。

5.4.4. TISAX審査の要素

TISAXの各審査は、以下の要素で構成されます。

- 正式なオープニングミーティング[19][20]
  - 組織に関するすべての議題の網羅を目的としています。
  - 対面でのミーティングである必要はありません。
  - 議題についての話し合いは、1回の会議でまとめて行うことも、複数回の会議に分けることも可能です。
  - 組織に関する事前審査のあらゆる議題を「論理的に含める」ミーティングです。
- 審査手順
  - 審査機関は、すべての要求事項を確認します。
  - 審査方法は、それぞれの審査レベルに応じて選択されます。
- 正式なクロージングミーティング[21]
  - TISAX審査を締めくくります。
  - 審査機関が指摘事項を発表します。
  - 審査機関が審査結果を発表します。
  - 対面でのミーティングである必要はありません。
  - 組織に関する審査後のあらゆる議題を「論理的に含める」ミーティングです。

「クロージングミーティング」の後、審査機関は、「TISAX審査報告書」を更新してドラフト版を作成し、貴社に送付します。審査機関が何かを誤解していると思われる場合は、異議を申し立てることができます。[22]その後、審査機関が最終版の「TISAX審査報告書」を発行します。

上記の全要素について、以降のセクションで説明します。

5.4.5. 適合性について

TISAX審査プロセスの概要の説明を続ける前に、以降のセクションを理解するのに不可欠な、重要な概念について解説します。

TISAX審査の目的は、貴社の情報セキュリティマネジメントシステムが、定義された要求事項を満たしているか判断することです。審査機関は、貴社の情報セキュリティマネジメントシステムが要求事項に「適合」（“conforms”）しているかどうかを確認します。

ステップ1：該当する各要求事項について、個別に確認が行われます。

貴社のアプローチがすべての要求事項に「適合」していれば、審査に合格し、審査目的に対応するTISAXラベルを受け取ります。

要求事項への完全な適合または理想的な適合に至らないものは、すべて指摘事項（finding）と呼ばれます。TISAXでは、指摘事項を以下の4種類に区別しています。

番号	種類	定義	対応	例
1.	重大な不適合（Major non-conformity）	重大な不適合は ▪ 情報セキュリティに差し迫った重大なリスクをもたらします ◦ または、情報セキュリティマネジメントシステムの全体的な有効性に疑義を生じさせます	貴社がすべきことは ▪ 重大な不適合に対し、即座に適切な対抗措置を講じて対処します ▪ 是正措置を遅滞なく実施します	▪ 体系的な不適合 ▪ 機密情報のセキュリティに重大なリスクをもたらす、実施上の欠陥 ▪ 適切な是正処置で対処されていない実施上の欠陥
2.	軽微な不適合（Minor non-conformity）	軽微な不適合は ▪ 貴社の情報セキュリティに、差し迫った重大なリスクを生じさせず ◦ かつ情報セキュリティマネジメントシステムの全体的な有効性に疑義を生じさせない不適合です	貴社がすべきことは ▪ 是正措置を遅滞なく実施します	▪ 単発的または散発的なミス ▪ 要求事項または貴社の方針の実施における不遵守または欠陥
3.	観察事項（Observation）	情報セキュリティに対する直接的なリスクはないが、将来的にリスクを生じる可能性のある、要求事項または貴社の方針への不遵守を「観察事項」と呼びます。	貴社がすべきことは ▪ 生じうるリスクを注意深く調査し、監視し、評価します ▪ 観察事項をどのように取り扱うかを決定します	なし
4.	改善の機会（Room for improvement）	前述の種類にあてはまらず、情報セキュリティにリスクをもたらさないが、明らかな改善の余地がある逸脱を指します。	「改善の機会」に分類される指摘事項については、対処を実施するか、またどのように対処するかを、貴社が決定できます。	なし

表 11. 4種類の指摘事項

ステップ2：前述の「要求事項ごと」のステップにおけるすべての結果が、総合的な審査結果に集約されます。

総合審査結果は、以下のように分類されます。

a. 適合（Conform）
総合的な審査結果は「適合」です。すべての要求事項が満たされています。

b. 軽微な不適合（Minor non-conform）
要求事項に対して少なくとも一つの「軽微な不適合」がある場合、総合的な審査結果は「軽微な不適合」となります。

c. 重大な不適合（Major non-conform）
要求事項に対して少なくとも一つの「重大な不適合」がある場合、総合的な審査結果は「重大な不適合」となります。
（承認された是正計画がない場合は、どのような不適合でも、総合的な審査結果は「重大な不適合」となります）。

総合的な審査結果による違い

- 「軽微な不適合」の場合、すべての不適合が解消されるまで、TISAX仮ラベルを取得できます。
- 「重大な不適合」の場合、各問題を解決するまで、いかなるTISAXラベルも取得できません。
適切な対抗措置と是正処置を導入し、それが審査機関によって承認されれば、総合的な審査結果を「重大な不適合」から「軽微な不適合」に変更できます。これに伴い、TISAX仮ラベルを取得できます。

重要な点として、総合的な審査結果は、TISAX審査プロセス全体を通じて改善されていきます。

非常に単純な例ですが、初回審査の結果、総合的な審査結果が「重大な不適合」であったとしましょう。その後、貴社は指摘されたリスクを軽減します。その結果、総合的な審査結果が「重大な不適合」から「軽微な不適合」に変化します。さらにリスクが取り除かれれば、最終的には総合的な審査結果は「適合」となります。

これらに関する詳細は、以下で解説します。また、TISAXラベルの詳細については、以下のセクションを参照してください：
セクション 5.4.14. TISAXラベル。

5.4.6. TISAX審査プロセスの準備

審査機関は、貴社の自己評価に基づいて審査を準備します。そのため、自己評価を前もって審査機関に提出する必要があります。具体的な提出期限は、キックオフミーティングでの合意によって決定します。

審査機関は、十分に準備を整えることで、審査に要する時間を短縮できます。自己評価以外にも、審査機関は審査前に関連書類を要求します。要求されるのは、貴社が自己評価で参照した書類をはじめとする、審査機関が関連性があるとみなした書類です。

審査機関は、これらの情報に基づいて審査手順を計画します。

5.4.7. 初回審査

TISAXの初回審査をもって、TISAX審査プロセスは正式に開始します。

重要事項：

初回審査に伴い、次の二つの重要な期間が開始します。

1. TISAXラベルの最大有効期間は3年間です。
2. 不適合の解消には、最長9か月の猶予があります。この期間内にすべての不適合

を解消しなければ、TISAXラベルは発行されません。この期限を過ぎた場合、そのまま新たな初回審査を受けることができます。

どちらの期間も、初回審査のクロージングミーティングの日付をもって開始します。

注意事項:

上記の二つの期間以外に、時間的な制約はありません。例えば、オンライン登録の完了、審査機関への連絡、キックオフミーティングの実施などに期限はありません。初回審査の開始は、貴社の判断に委ねられます。

5.4.7.1. 最初の正式なオープニングミーティング

他のTISAX審査と同様に、初回審査は正式なオープニングミーティングから始まります。正式なオープニングミーティングは、通常、電話会議またはウェブ会議で行われます。小規模の企業や、他の監査の経験がある企業であれば、それほど時間はかかりません。

このミーティングの目的は以下の通りです。

- 審査の前提条件の確認
- 審査のプロジェクトリーダーと審査チームの紹介
- 審査計画の策定

5.4.7.2. 審査手順

準備された計画に従って、審査機関が初回審査を実施します。詳細は、審査の目的によって異なります。審査は主に、電話会議、オンサイトの面談、オンサイト調査で構成され、どれほど詳細に行われるかはさまざまです。[23]

審査機関は、初回審査で得られた指摘事項をすべて提示します。

5.4.7.3. クロージングミーティング

クロージングミーティングでは、審査機関がすべての指摘事項を再度まとめます。

5.4.7.4. TISAX審査報告書

「クロージングミーティング」の後、審査機関は「TISAX審査報告書」のドラフト版を作成し、貴社に送付します。審査機関が何かを誤解していると思われる場合は、異議を申し立てることができます。[24]その後、審査機関が「TISAX審査報告書」を発行します。

この段階における、現状の総合的な審査結果は以下のいずれかとなります。

- 適合
- 重大な不適合
  未対処の（軽微な）不適合がある場合、総合審査結果は常に「重大な不適合」となります。総合審査結果が「軽微な不適合」となるには、不適合への対応措置の実施に向けた処置を定義する必要があります。
  これを達成する方法については、次をご参照ください：セクション 5.4.9.4. 仮TISAXラベル。

初回審査で総合審査結果が「適合」であった場合、残りの審査セクションはスキップして、結果の共有に進むことができます。

総合審査結果が「重大な不適合」であった場合、次の課題は、指摘事項にどのように対処し、審査機関が指摘したギャップをどのように埋めるかについて計画を策定することです。この計画は、正式には「是正計画」（“corrective action plan”）と呼ばれます。

注意事項:

審査の開始前に、不適合となる状況を認識しており、審査までにそれを修正できない場合、あらかじめ是正処置（実施日を含む）を計画し、審査中に審査機関に提示できます。これにより、理論的には、総合審査結果が「軽微な不適合」となる可能性があります。ただし、実際にこのようになるケースはあまりないと思われます。

5.4.8. 是正計画の作成

初回審査で受けた指摘事項への対処方法を定めたものを、「是正計画」（“corrective action plan”）と呼びます。審査機関は、貴社の「是正計画」が適切であるか審査します（次のセクションを参照）。

「是正計画」の作成にあたっては、以下の要求事項を考慮する必要があります。

- 指摘事項
  - 是正措置が、どの指摘事項に対処するものかを明記する必要があります。
- 根本原因
  - 指摘事項の根本原因を特定し、記載する必要があります。
- 是正処置
  - それぞれの不適合について、対策を実施する「是正処置」を、一つ以上定義する必要があります。
- 実施日
  - それぞれの是正処置について、実施日を定める必要があります。
  - 実施期間として、対策を徹底的に実施するのに十分な時間を確保する必要があります。
- 対抗措置
  - 重大なリスクを引き起こす不適合については、是正処置が実施されるまでの間、不適合に対処するための対抗措置を定義する必要があります。
- 実施期間
  - 是正処置の実施に3か月以上かかる場合は、実施期間の正当性を説明する必要があります。
  - 6か月以上かかる是正処置については、それに加えて、より迅速な実施が不可能であることを示す証跡の提出も必要です。
  - いかなる是正措置も、実施期間が9か月を超えることはできません。

是正計画が完了したら、「是正計画審査」を要求できます。

重要事項:

できるだけ早く実施に着手することをお勧めします。「是正計画審査」の結果を待つ必要はありません。
「是正計画審査」は、通常、是正計画を審査機関に提出した後に行われます。

注意事項:

> TISAXは、是正処置計画の内容に関する要求事項のみを定めており、形式については定めていません。
> ほとんどの審査機関は、是正処置計画のテンプレートを提供しています。

5.4.9. 是正計画審査

「是正計画審査」の目的は、「是正計画」（上記参照）がTISAXの要求事項を満たしているかどうかを検証することです。

貴社は、「是正計画」を審査機関に提出します。審査機関は、要求事項（下記参照）に従って計画を審査します。貴社の計画が要求事項を満たしていれば、審査機関は「TISAX審査報告書」を更新して発行します。

この審査には通常、それほど時間はかかりません。電話会議やウェブ会議で実施されるケースが大半です。メールだけで行われることもあります。

5.4.9.1. 是正計画審査の実施理由

「是正計画審査」は、次の理由により行われます。

- 以下の審査後に不適合が残っている
  - 初回審査
  - フォローアップ審査
  - スコープ拡大審査
- 「是正計画」の審査を実施した結果、要求事項を満たしていなかった
- 是正計画の実施期間を算定する根拠となる影響因子が変更された

5.4.9.2. 初回審査との組み合わせ

「是正計画審査」は、個別に実施するよう義務付けられているわけではありません。初回審査のクロージングミーティングにおいても、「是正計画」を提示することは可能です。この時提出することで、審査機関はそのまま「是正計画審査」を実施できます。

もし「是正計画審査」を初回審査と組み合わせて実施し、「是正計画」が要求事項を満たしていれば、「初回審査報告書」は不要であると審査機関と合意することも可能です。その場合、審査機関は「是正計画審査報告書」を作成します。この報告書をもって、TISAX仮ラベルをそのまま取得できます。

5.4.9.3. 是正計画の要求事項

審査機関は、「是正計画」を以下の要求事項に照らして審査します。

- 対応が適切であること
  - 審査機関は、是正処置が不適合の根本原因を解決するかどうかに基づいて、是正処置の適切性を審査します。
- 重大なリスクは適切な対抗措置によって軽減されます。[25]
- 実施期間が適切であること
  - 実施期間は、初回審査の終了日から開始します
- 規定の実施期間を超えないこと
  - 正当性の説明を行うことなく、3か月を超えることはできません

- 正当性の説明を行い、かつ証跡を示すことなく、6か月を超えることはできません
- 9か月を超えることはできません

5.4.9.4. 仮TISAXラベル

総合審査結果が「軽微な不適合」の場合、TISAX仮ラベルが発行されます。

TISAX仮ラベルを取得する利点は、後から仮ではないTISAXラベルを取得するという条件の下で、受け入れるパートナーが多いことです。情報セキュリティマネジメントシステムの有効性をパートナーに証明することが急務である場合に効果的といえます。

TISAX仮ラベルの前提条件は、総合審査結果で「軽微な不適合」と判定された、是正計画審査報告書です。

TISAX仮ラベルは仮ではないTISAXラベルと基本的に同等です。 唯一の違いは、TISAX仮ラベルの有効期間が短いことです。

TISAX仮ラベルの有効期間は、初回審査のクロージングミーティング後から最長9か月間です。TISAX仮ラベルの有効期間は、是正措置の最長実施期間によって決定します。

例:

- 貴社の不適合が一つだけとします。ポリシーの見直しが必要で、それに伴う実施期間は2か月とします。
  この時、TISAX仮ラベルは2か月間有効となります。
- 前述のポリシーの見直しが必要な不適合があるとします。それに加えて、是正措置として、新しい外壁の構築を必要とする不適合があるとします。自治体から必要な承認を得るのに時間がかかるため、実施期間は8か月とします。
  この場合、TISAX仮ラベルは8か月間有効です。

実施期間の要求事項については、次を参照してください：セクション 5.4.9.3. 是正計画の要求事項

注意事項:

「是正計画審査」は任意です。

以下の場合は、そのままフォローアップ審査に進むことができます。

- TISAX仮ラベルを必要としない場合
- 審査機関の承認を得ることなく、是正措置を実施する自信がある場合

すべての是正措置が完了したら、「フォローアップ審査」を依頼する必要があります。

5.4.10. フォローアップ審査

「フォローアップ審査」の目的は、以前に指摘された不適合がすべて解消されているかを審査することです。通常は、すべての不適合が解消されたことを確認した時点で、フォローアップ審査を依頼します。

しかし、フォローアップ審査は必要なだけ受けることができます。フォローアップ審査において、審査機関から既存の、あるいは新たな不適合を指摘された場合は、是正計画を更新して、その箇所から審査プロセスを再度開始します。

この審査は、電話会議やウェブ会議だけでなく、対面の会議でも実施できます。

5.4.10.1. 実施時期

フォローアップ審査は、初回審査の終了から9か月以内に実施できます。[26]

5.4.10.2. 前提条件

TISAX仮ラベルが不要な場合は、直接フォローアップ審査を依頼できます。フォローアップ審査の前に「是正計画審査」を行う必要はありません。

5.4.10.3. TISAX仮ラベルの有効期限

TISAX仮ラベルが必要な場合は、仮ではないTISAXラベル取得までの期間が空かないようにしたいケースが多いかと思います。そのため、可能な限り早く、フォローアップ審査を依頼することをお勧めします。[27] その理由は、フォローアップ審査中に特定された軽微な指摘事項に対処できるように、時間に十分な余裕を持たせたいからです。

5.4.11. TISAX審査プロセス図

これまでのセクションをプロセス図にまとめると、次のようになります。

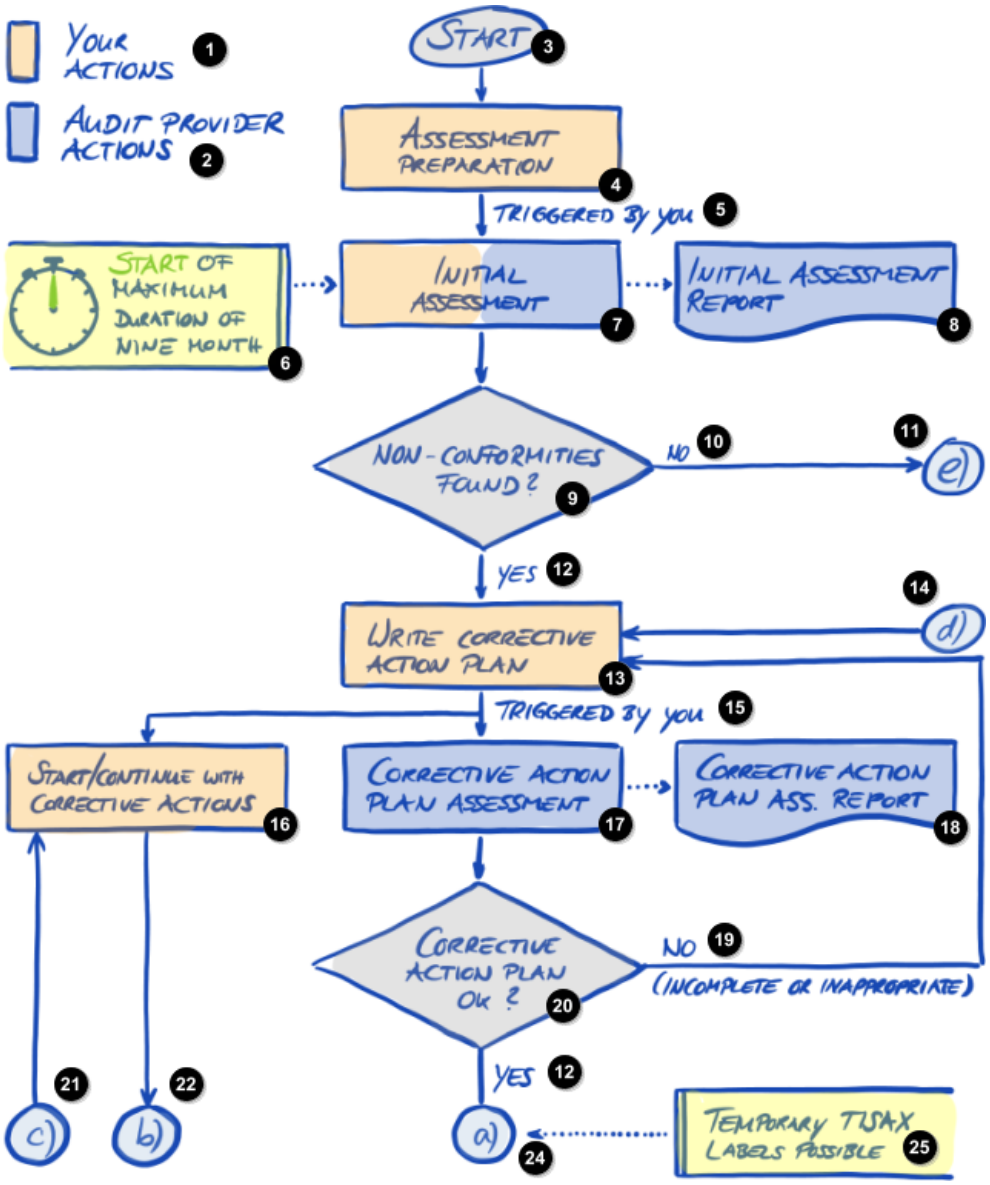


図 30. TISAX審査プロセス図（1/2）

1. 貴社の行動
2. 審査機関の行動
3. 開始
4. 審査の準備
5. 貴社によって開始
6. 最長9か月の審査期間の開始
7. 初回審査
8. 初回審査報告書
9. 不適合が見つかった?

10 いいえ

11 e)

12 はい

13 是正計画の作成

14 d)

15 貴社によって開始

16 是正措置の開始・継続

17 是正計画審査

18 是正計画審査報告書

19 いいえ（不完全または不適切）

20 是正計画は適切?

21 c)

22 b)

24 a)

25 TISAX仮ラベルを取得可能

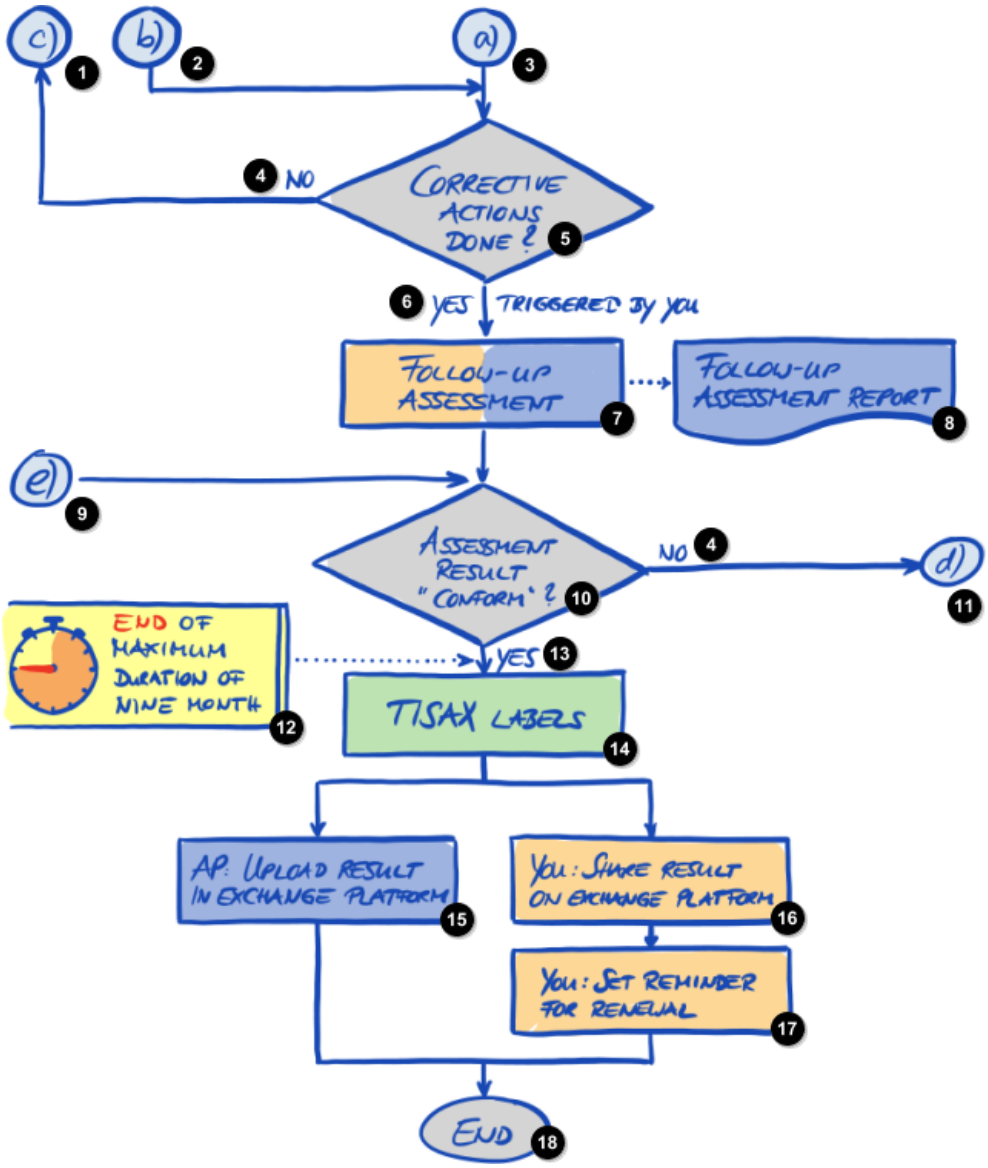


図 31. TISAX審査プロセス図（2/2）

1. c)
2. b)
3. a)
4. いいえ
5. 是正措置は実施済み?
6. はい、貴社によって開始
7. フォローアップ審査
8. フォローアップ審査報告書
9. e)

10. 審査結果は「適合」？
11. d）
12. 最長9か月の期間終了
13. はい
14. TISAXラベル
15. 審査機関：共有プラットフォームに結果をアップロード
16. 貴社：共有プラットフォームで結果を共有
17. 貴社：更新リマインダーを設定
18. 終了

5.4.12. Assessment ID （審査ID）

審査スコープの各TISAX審査は、「審査ID」によって識別されます。このIDは、貴社の審査結果と、対応するTISAX審査報告書を参照します。

審査IDは以下のようになっています。

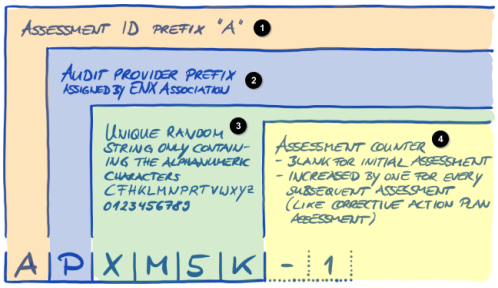


図 32. 審査IDの形式

1. 審査IDの頭文字は「A」
2. ENX協会が付与する審査機関の頭文字
3. 英数字のみからなる、一意のランダムな文字列です。
   CFHKLMNPRTVWXYZ
   0123456789
4. 審査カウンター
   - 初回審査時は空白
   - その後は（是正計画の審査のような）審査一つごとに1増加

審査IDは、通常、審査機関が貴社と連絡を取る際に使用されます。

5.4.13. TISAX審査報告書

「TISAX審査報告書」（“TISAX assessment report”）は

- 各TISAX審査後に（更新され）発行されます。

- 審査機関の指摘事項を文書化します。
- 総合審査結果（適合、軽微な不適合、重大な不適合）が含まれます。
- TISAX審査に関連するその他のすべての情報（審査目的、スコープ、関係者、拠点など）も記載されます。

「TISAX審査報告書」には、以下の種類があります（審査の種類によって異なります）。

- 初回審査報告書（Initial assessment report）
- 是正計画審査報告書（Corrective action plan assessment report）
- フォローアップ審査報告書（Follow-up assessment report）[28]

「TISAX審査報告書」は、すべて同じ構成となっています。[29] 審査機関は、各種の審査後に、報告書を拡張します。すなわち、「TISAX審査報告書」には必ず旧版の内容が含まれているため、貴社が扱う必要があるのは最終版のみとなります。

「TISAX審査報告書」の最初のセクションが、最終的にパートナーと共有する箇所になります。

TISAXの大きな特徴の一つとして、TISAX審査報告書のどの箇所をパートナーや他の参加企業と共有するかは、完全に貴社の判断に委ねられている点が挙げられます。TISAX審査報告書は、共有箇所を選択できるように構成されています。各セクション内では、より詳細な内容が展開されています。

「TISAX審査報告書」の構成は次のようになっています。

- A.審査関連情報
  企業名、審査スコープ、スコープID、審査ID、審査レベル、審査目的、審査日、審査機関
  このセクションには審査結果は含まれません。
- B.結果の要約
  審査結果の要旨（適合、軽微な不適合、重大な不適合）、指摘事項の数、結果のリスクの大まかな分類
- C.審査結果の要約
  章ごと（「9 アクセス管理」等）および基準カタログごと（「情報セキュリティ」等）の審査結果の要約
- D. VDA ISAの成熟度レベル（結果タブ）
  各要求事項の成熟度レベル
- E.詳しい審査結果
  すべての指摘事項の詳細な記述、対応するリスクアセスメントの結果、必要な対策、実施期間

「共有」ステップ（詳細は後述）では、パートナーがどのレベルまでTISAX審査報告書の内容にアクセスできるかを決定します。

5.4.14. TISAXラベル

登録準備のセクションで簡単に触れた要素です。 上述のように、かつては審査目的とされていたものが、現在ではTISAXラベルとなりました。

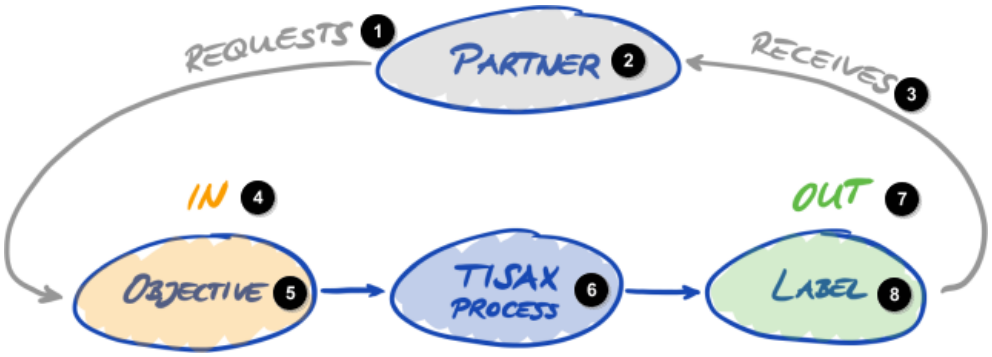


図 33. 審査目的とTISAXラベル

1. 要請
2. パートナー企業
3. 取得
4. 入力
5. 目的
6. TISAXプロセス
7. 出力
8. ラベル

TISAXラベルは

- TISAXの審査プロセスの結果です。
- 審査結果の概要として機能します。
- 貴社の情報セキュリティマネジメントシステムが、定義された要求事項を満たしていることを表します。

TISAXラベルは、TISAX審査プロセスのあらかじめ定められた出力です。そのため、TISAXラベルを使用することで、パートナー企業やTISAX審査機関とのTISAX関連のコミュニケーションが円滑になります。

5.4.14.1. TISAXラベルの階層

審査目的とTISAXラベルは、非常にシンプルな対応関係となっています。しかし、もう一つの重要な側面が、一部のTISAXラベルは階層的にリンクしていることです。すなわち、あるTISAXラベルを取得すると、自動的にその「下の」TISAXラベルも取得することになります。

例えば、貴社の審査目的が「Very high availability」であった場合、貴社は対応するTISAXラベル「Very high availability」を取得します。この時、審査目的「Very high availability」は「High availability」の上位集合なため、貴社は自動的にTISAXラベル「High availability」も取得します。

現在、TISAXラベルには次のような階層が存在します。

- 「Info high」は「Confidential」と「High availability」の上位集合
- 「Info very high」は「Strictly confidential」と「Very high availability」の上位集合

- 「Strictly confidential」は「Confidential」の上位集合
- 「Very high availability」は「High availability」の上位集合
- 「Special data」は「Data」の上位集合

注意事項:

過去にさかのぼってTISAXラベルを取得することもできます。貴社がすでに取得済みのTISAXラベルのサブセットとなるラベルをTISAXが新規に導入した場合、貴社は自動的にこの新しいラベルを取得します。

例：TISAXラベル「High availability」がまだ存在しない時に、貴社はTISAXラベル「Info high」を取得しました。TISAXがラベルHigh availabilityを導入すると、システムにより、自動的に貴社にこのラベルを割り当てられます。

対象の要求事項について、以下の表の指定を比較することで、階層関係を導き出すことができます: 表 8. 審査目的ごとに該当する要求事項。

これは、全参加企業にとっての重要事項ではないように思われるかもしれませんが、例えばあるパートナー企業が貴社にTISAXラベル「Very high availability」の提示を要求し、別のパートナー企業がTISAXラベル「High availability」の提示を要求したとします。その場合、両方のTISAXラベルを実際に保有していれば、「High availability」が「Very high availability」のサブセットであることを説明や理解する必要もなくなり、全員の手間が省けます。例えば、かなり厳格な購買プロセスを定めており、特定のTISAXラベルの取得を求めているパートナー企業を相手に、「Very high availability」は「High availability」よりも「良い」、などと説明したくはないかと思います。貴社はTISAXラベルをすべて提示して、担当者は「『High availability』のTISAXラベルが必要」という要求事項にチェックを入れる、というプロセスだけで済むに越したことはありません。

5.4.14.2. TISAXラベルの有効期間

TISAXラベルは通常3年間有効です。有効期間は、審査プロセスの終了時（TISAX審査報告書の発行前であっても）に開始します。

TISAX審査スコープに重要な変更があると、有効期間が短くなる場合があります。

例えば、会社の移転、新しい拠点の追加などです。（このような場合の対処法については、セクション 7.9.3.2. 拠点変更の申請方法およびセクション 7.9.3.4. 拠点の追加方法をご参照ください）

注意事項:

TISAXラベルはENXポータルのみで確認できます。TISAX審査報告書には記録されません。

5.4.14.3. TISAXラベルの更新

TISAXラベルを長期間維持するには、3年ごとに更新[30]が必要です。

そのためには、基本的にTISAXプロセスを再度実施する（審査スコープを登録し、再度TISAX審査を受け、審査結果を共有する）必要があります。TISAX参加企業として再作成する必要がないため、登録は初回よりも簡単です。もちろん、TISAXデータ
ベースに保存されているすべての連絡先や拠点データを再利用できます。

重要事項:

審査機関への連絡「前に」、「新しい」スコープを登録してください。審査機関

は、貴社が新しいスコープIDを提示できる場合にのみ、新しい審査プロセスを開始できます。

ほとんどの場合、新しいスコープの登録は簡単です。新しいスコープ名を割り当て、連絡先を追加し、審査目的を選択し、拠点を追加するだけ登録できます。すでにシステム内にある、以前に登録したスコープの連絡先と拠点データを再利用できます。

重要事項:

以前のスコープ登録時に作成・使用した、既存の拠点データを再使用してください。新しい拠点データを、同じ住所で作成しないでください。

これは、TISAX参加企業の中に、パートナーの審査結果を自動処理する企業が存在するためです。自動処理では、その企業のシステムとENXポータルが同期されるため、たとえわずかでも差異があると、同期が正常に完了しない可能性があります。また、不要な重複による、参加企業データの乱雑化を避けることにもつながります。

重要事項:

パートナー企業との取引期間中、継続的に有効なTISAXラベルが必要な場合は、カレンダーに、必要な更新プロセス開始のリマインダーを入れておくことを強くお勧めします。

TISAXラベルの有効期限が切れる少なくとも1年前に、更新手続きを開始することをお勧めします。

TISAXラベルを取得したら、最後のステップであるパートナー企業との共有に進みます。

6. 共有（ステップ3）

共有セクションの説明を読むのに必要な時間の目安は7分です。

TISAXプロセスをここまで進めてきましたが、貴社のパートナー企業は、貴社の情報セキュリティマネジメントシステムが機密データを保護できるという「証拠」を確認できていません。このセクションでは、貴社の審査結果をパートナー企業と共有し、要求された証拠を提示する方法について説明します。

6.1. 前提

TISAXの大きな特徴の一つが、貴社の審査結果が完全に貴社の管理下にあるということです。貴社の明示的な許可なしに、貴社の審査に関するいかなる情報も、誰とも共有されることはありません。

6.2. 共有プラットフォーム

ENXポータルは、共有プラットフォームを提供します。

審査機関は、TISAX審査報告書の最初の二つのセクション（AおよびB）をアップロードします。 この段階では、あなた以外は誰も情報を利用できません。

共有プラットフォームは、登録時に作成したアカウントでアクセスし、使用できます。

ポータルには、次のアドレスからアクセスできます。
enx.com/en-US/SignIn

6.3. 一般的な前提条件

審査結果をパートナー企業と共有するには、以下の二つの前提条件を満たす必要があります。

1. 審査機関が、審査結果を共有プラットフォームに提出している必要があります。
   審査結果は、TISAX審査報告書が発行されてから通常5〜10営業日後に、共有プラットフォームでアクセスできるようになります。
2. ENX協会が、貴社から支払われた料金を受領している必要があります（該当する場合）。

両方の前提条件が満たされると、審査スコープのステータスは「アクティブ」になります。

注意事項:

すべての審査スコープにはライフサイクルがあります。この段階では、審査スコープのステータスは「アクティブ」となっている必要があります。

審査スコープのステータスの詳細については、以下のセクションを参照してください：セクション 7.5.5. Assessment scope status “Awaiting your payment” （審査スコープステータス「支払い待ち」）。

審査結果が共有可能な状態（審査スコープのステータス=「アクティブ」）であるかどうかを確認するには、以下の手順に従ってください。

1. ENXポータルにログインします。
2. メインナビゲーションバーに移動し、 “MY TISAX” （「MY TISAX」）を選択します。

3. ドロップダウンメニューから“SCOPES AND ASSESSMENTS”（「スコープと審査」）を選択します。
4. 表に移動し、貴社の審査スコープが表示されている行を探します。
5. 貴社の審査スコープが審査スコープステータス“Active”（「アクティブ」）（“Scope Status”（「スコープステータス」）列）であることを確認します。

6.4. 共有結果の永続性

重要事項:

公開や共有の許可を取り消すことはできません。

これは、すべてのパッシブ参加企業が、受け取ったすべての審査結果へ、必ず継続的にアクセスできる環境を確保するためです。これが保証されていなければ、パッシブ参加企業は自分たちで審査結果を管理し、アーカイブしなければならなくなります。

このアクセス権限は、TISAX審査の有効期間中有効です。

誤って公開または共有許可を作成した場合は、直ちにENX協会までご連絡ください。

6.5. 共有レベル

共有レベルは、TISAX審査報告書の主要セクションのA～Eと1対1の対応関係にあります。

	TISAX審査報告書の主要セクション	共有プラットフォームにおける共有レベル
1	A.審査関連情報（Assessment Related Information）	
2	B.結果の要約（Summarized Results）	
3	C.審査結果の要約（Assessment result summary）	
4	D.VDA ISAの成熟度レベル（結果タブ）（Maturity Levels of VDA ISA (Result Tab)）	
5	E.詳しい審査結果（Detailed Assessment Results）	

表 12. TISAX審査報告書の主要セクションと共有プラットフォームにおける共有レベル

共有レベルが高ければ高いほど、各参加企業が、貴社のTISAX審査に関するより詳細な情報にアクセスできるようになります。

TISAX審査報告書の各セクションの内容の詳細については、以下を参照してください：セクション 5.4.7.4. TISAX審査報告書。

6.6. 審査結果を共有プラットフォームで公開する

共有プラットフォームで公開することで、審査結果を他の全TISAX参加企業と共有できます。これにより、他の全TISAX参加企業は、許可された共有レベルまで、貴社の審査結果にアクセスできるようになります。

審査結果を公開できるのは、総合審査結果が「適合」の場合のみです。

共有プラットフォーム上で審査結果を公開するための共有レベルとして、以下の選択肢からのみ選択できます。

- Do not publish (Default) （非公開（デフォルト））
- A. Assessment Related Information （A. 審査関連情報）
- A + Labels （A + ラベル）
- A + Labels + B. Summarized Results （A + ラベル + B. 結果の要約）

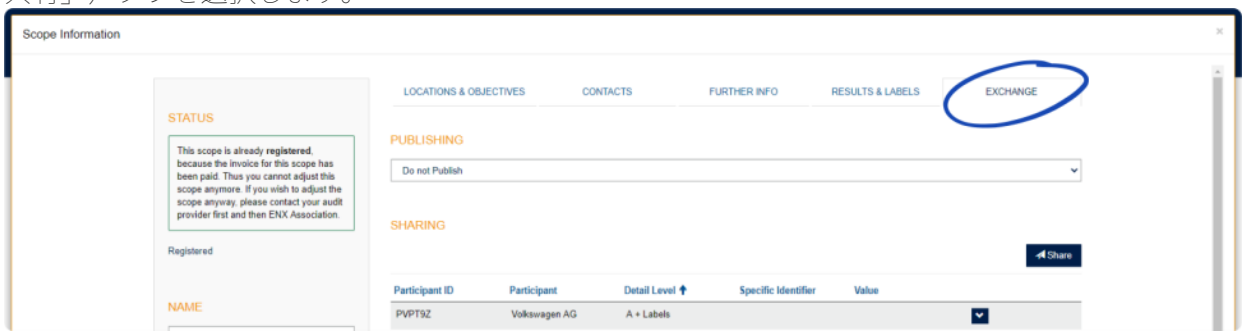
一般的な公開の場合は、共有レベル“A + Labels”（「A+ラベル」）をお勧めします。

重要事項:

審査結果を公開できるのは、セクション 6.3. 一般的な前提条件に記載された前提条件が満たされている場合のみです。

共有プラットフォームで審査結果を公開するには、以下の手順に従います。

1. ENXポータルにログインします。
2. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
3. ドロップダウンメニューから“SCOPES AND ASSESSMENTS”（「スコープと審査」）を選択します。
4. 表に移動し、貴社の審査スコープが表示されている行を探します。
5. 貴社の審査スコープが審査スコープステータス“Active”（「アクティブ」）（“Scope Status”（「スコープステータス」）列）であることを確認します。
6. 審査スコープの表の行の最後に移動し、下向き矢印のボタンをクリックします。
7. “Scope Information”（「スコープ情報」）を選択します。
8. 新しいウィンドウ（“Scope Information”（「スコープ情報」））で、“EXCHANGE”（「共有」）タブを選択します。



9. “PUBLISHING”（「公開」）セクションに移動し、ドロップダウンメニューを開き、希望する共有レベルを選択します（上記の推奨を参照）。

注意事項:

審査結果は共有プラットフォームでのみ公表されます。他のTISAX参加企業のみアクセスできます。TISAX参加企業をすべて記載したリストは公開されていません。公開されているTISAXウェブサイトには、TISAX参加企業の数のみ、記載される可能性があります。

6.7. 審査結果を特定の参加企業と共有する

前述のように、TISAXの審査結果を共有プラットフォームで公開する方法の他に、特定のTISAX参加企業と、選択的に高い共有レベルで共有することも可能です。

前述の公開方法とは異なり、この方法では、総合審査結果が（重大な、または軽微な）不適合であっても、審査結果を共有できます。

審査結果の共有は、TISAXに不可欠な要素です。情報セキュリティマネジメントシステムの審査は1回しか受けられませんが、審査結果の共有は、貴社が希望する限り何社でも、パートナー企業と共有できます。

共有プラットフォーム上での審査結果の共有は、以下の選択肢から選択できます。

1. A: Assessment Related Information （A：審査関連情報）
2. A + Labels （A + ラベル）
3. A + Labels + B: Assessment Summary （A + ラベル + B：審査の要約）
4. A + Labels + B + C: Summarized Results （A + ラベル + B + C：結果の要約）
5. A + Labels + B + C + D: Detailed Assessment Results （A + ラベル + B + C + D：詳しい審査結果）
6. A + Labels + B + C + D + E: Maturity Levels according to ISA （A + ラベル + B + C + D + E：ISAによる成熟度レベル）

共有する際は、“A + Labels”（「A+ ラベル」）をお勧めします。大半のパートナーの場合は、これで十分です。後からいつでも、より高い共有レベルを選択できます。

注意事項：

TISAX参加企業の中には、パートナーの審査結果を自動処理する企業が存在します。自動処理では、その企業のシステムとENXポータルが同期されます。対象の参加企業を指定して共有された審査結果のみが同期されます。セクション 6.6. 審査結果を共有プラットフォームで公開するに記載されている公開を行っただけで、同期されることはありません。

TISAXを使用しているOEMの一例がBMWです。BMWのパートナー企業の場合は、BMWと（公開だけでなく）審査結果を共有してください。

6.7.1. 前提条件

パートナー企業（または他のTISAX参加企業）と審査結果を共有するための前提条件は、以下の通りです。

- TISAXの審査結果は、他のTISAX参加企業にのみ共有できます。
- パートナー企業が、TISAX参加企業である必要があります。
- パートナー企業の参加企業IDが必要です。[31]
- 料金（該当する場合）の支払いが必要です。

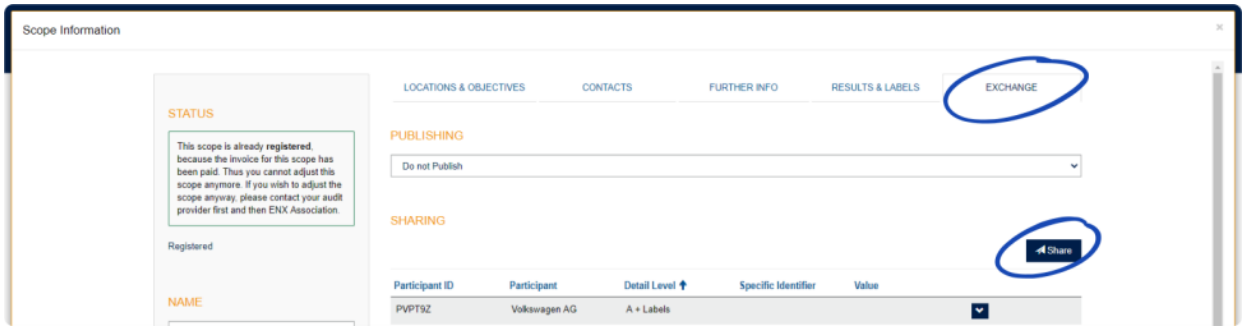
重要事項：

審査結果を共有できるのは、セクション 6.3. 一般的な前提条件に記載されている一般的な前提条件が満たされた場合のみです。

6.7.2. 共有権限の作成方法

審査結果を他のTISAX参加企業と共有するには、以下の手順に従ってください：

1. ENXポータルにログインします。
2. メインナビゲーションバーに移動し、“MY TISAX”（●「MY TISAX」）を選択します。
3. ドロップダウンメニューから“SCOPES AND ASSESSMENTS”（●「スコープと審査」）を選択します。
4. 表に移動し、貴社の審査スコープが表示されている表の行を探します。
5. 貴社の審査スコープが審査スコープステータス“Active”（●「アクティブ」）（“Scope Status”（●「スコープステータス」）列）であることを確認します。
6. 審査スコープの表の行の最後に移動し、下向き矢印のボタンをクリックします。
7. “Scope Information”（●「スコープ情報」）を選択します。
8. 新しいウィンドウ（“Scope Information”（●「スコープ情報」））で、“EXCHANGE”（●「共有」）タブを選択します。



9. “SHARING”（●「共有」）セクションに移動し、“Share”（●「共有」）ボタンをクリックします。
10. 新しいウィンドウ（“SHARE THIS SCOPE”（●「このスコープを共有」））で、パートナー企業の参加企業IDを入力します（または、隣の検索ボックスの参加企業リストからパートナー企業を選択します）。
11. 希望する共有レベルを選択します。
12. “Next”（●「次へ」）ボタンをクリックします。
13. 共有権限の永続性に関する説明を読み、理解してください。
14. 二つの“confirm”（●「確認」）チェックボックスに印を付けます。
15. “Submit”（●「送信」）ボタンをクリックします。

他はすべて共有プラットフォーム側で実行されます。レベルAとレベルBの共有の場合は、共有プラットフォームで情報を入手できます。パートナー企業がENXポータルにログインして、共有された審査結果を確認できるようになりました。[32]

より高い共有レベル（C～E）については、共有プラットフォームから審査機関に通知されます。その後、貴社の審査機関は、貴社のパートナー企業の主な参加企業の連絡先に（選択した共有レベルにあたる）情報を送信します。

6.8. TISAX外での審査結果の共有

TISAX共有プラットフォームを使用できるのは、他のTISAX参加企業に審査結果を知らせる場合に限られます。[33]

6.8.1. 共有が厳格に管理されている理由

TISAXでは、審査結果の共有メカニズムを標準化しています。他の認証（ISOなど）では結果がさまざまな方法で共有されており、全体像の把握に必要な情報がすべて含まれているとは限りません。それ

と比較して、TISAXの標準化された共有メカニズムがもたらす付加価値は大きく、特にOEMから高く評価されています。そして、他の企業にとっても、手順が明確に定義されていることはメリットとなります。

6.8.2. TISAXについて一般向けに書く際の手引き

審査結果については一般に公表できませんが、TISAXの取り組みについて言及できます。ENXポータルサイトでは、一般向けの発信方法に関するアドバイスを提供しています。また、使用できるTISAXロゴも提供しています。

ENXポータルへのログイン後、以下のリンクから情報にアクセスできます。
enx.com/en-US/myenxportal/marketing/
以下のリンクから直接ZIPアーカイブ（文書とロゴ）をダウンロードできます。
enx.com/en-US/myenxportal/marketing/TISAX-Trademark-and-Logos-Terms-and-Conditions.zip

壁に飾れるような証明書がほしいと思われる方もいるかもしれませんが、
上記のように共有プロセスは標準化されているため、そのいった証明書は発行しておりません。

6.8.3. TISAXに参加していないパートナー企業との共有

TISAXの審査結果を、a） TISAX参加企業でなく、b） TISAXラベルを（審査プロセスを経て）取得していない特定のパートナー企業と共有したい場合は、以下の手順に従ってください。

1. パートナー企業にTISAX参加企業として登録するよう指示します。
   TISAX参加企業として登録するだけで構いません。審査スコープの登録に進む必要はありません。
2. パートナー企業にTISAXに連絡するよう指示します。
   通常は、企業が審査スコープも登録する場合にのみ、新規登録は処理されますが、パートナー企業からの要請がある場合は、登録手続きが行われます。パートナー企業は、この手続きによってTISAXの参加企業となり、通常の共有プロセスを通じて、貴社のTISAX審査結果を受け取れるようになります。

この手続きは、TISAX審査結果の共有について規定する「TISAX参加規約」の遵守に関し、パートナー企業から同意を得ることを目的としています。

費用が発生するのは、審査スコープの登録のみであり、TISAX参加企業としての登録は無料なため、パートナー企業は貴社の審査結果を無料で受け取ることができます。ただし、自社の審査結果がないパートナー企業が受け取れる審査結果は最大5件までに制限され、公開データを見ることもできません。

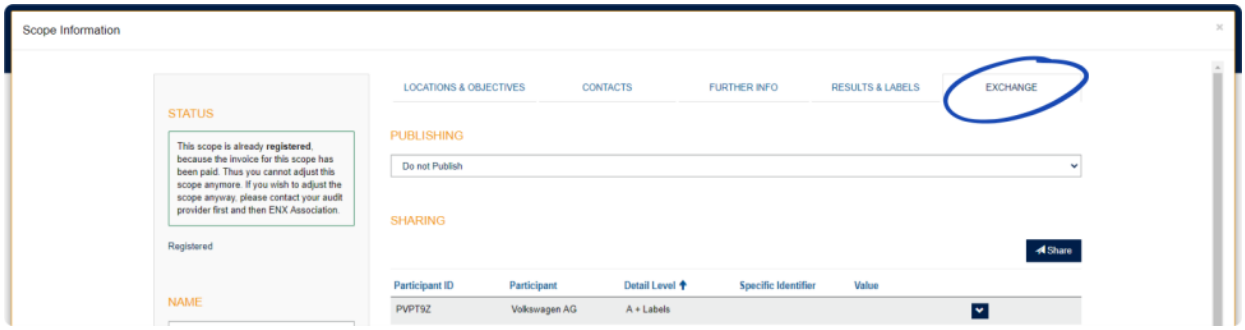
6.8.4. ENXポータルに直接アクセスできないパートナー企業の従業員との共有

審査結果を直接閲覧できるのは、ENXポータルのアカウントを持っているパートナー企業の従業員のみです。ポータルにアクセスできないパートナー企業の従業員に対し、TISAXラベルを提示する必要がある場合は、専用のPDFドキュメントをご利用ください。このドキュメントは、以下の手順で取得できます。

1. 以下のセクションの説明に従い、審査結果をパートナー企業と共有します：セクション 6.7. 審査結果を特定の参加企業と共有する。
2. ENXポータルにログインします。
3. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
4. ドロップダウンメニューから“SCOPES AND ASSESSMENTS”（「スコープと審査」）を選択します。
5. 表に移動し、貴社の審査スコープが表示されている行を探します。
6. 貴社の審査スコープが審査スコープステータス“Active”（「アクティブ」）（“Scope

Status”（「スコープステータス」）列）であることを確認します。

7. 審査スコープの表の行の最後に移動し、下向き矢印のボタンをクリックします。
8. “Scope Information”（「スコープ情報」）を選択します。
9. 新しいウィンドウ（“Scope Information”（「スコープ情報」））で、“EXCHANGE”（「共有」）タブを選択します。



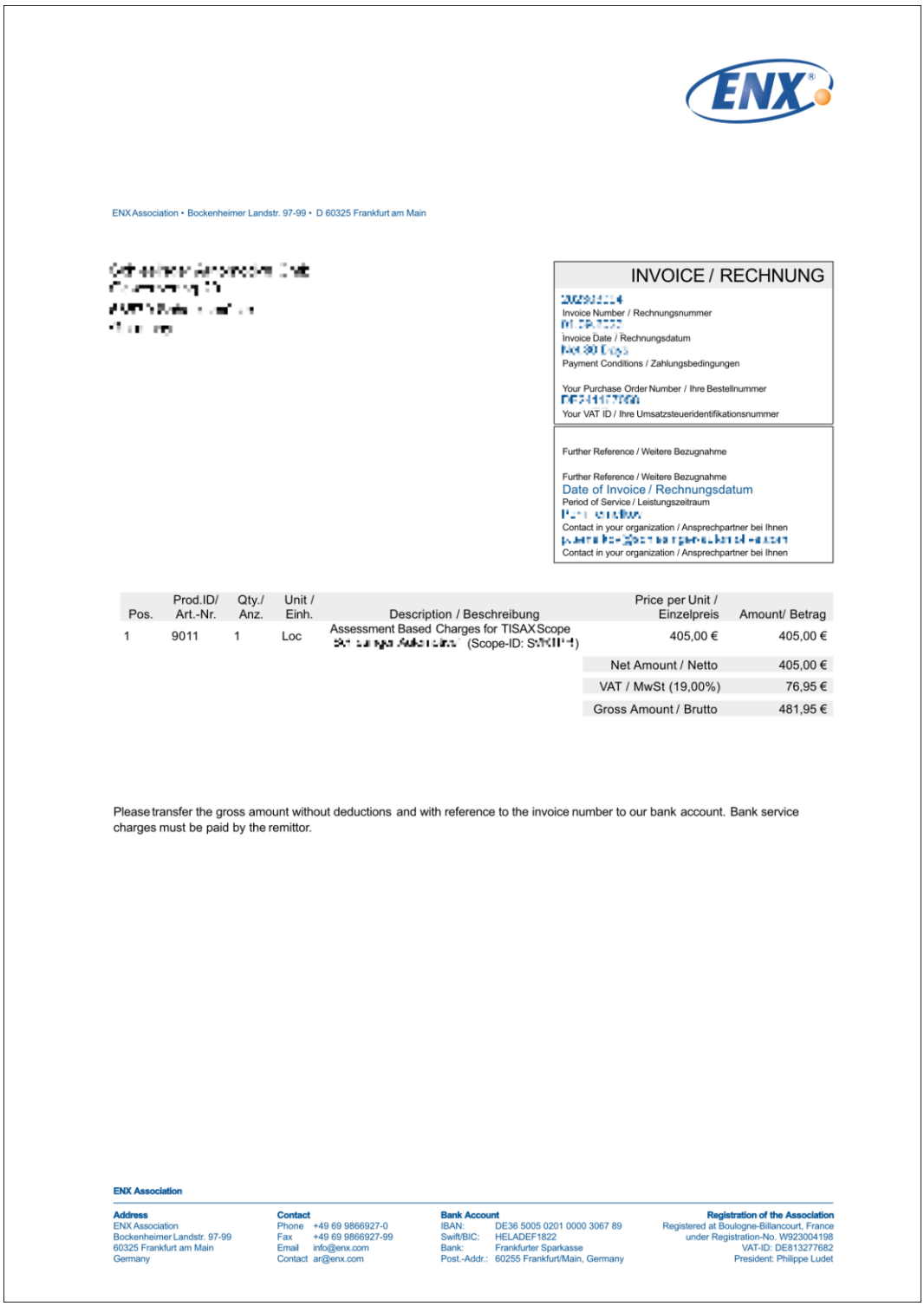
10. “SHARING”（「共有」）セクションに移動し、（ステップ1で作成した）共有権限の表の行を見つけます。
11. 共有権限の行の最後に移動し、下向き矢印のボタンをクリックします。
12. “Edit”（「編集」）を選択します。
13. 新しいウィンドウ（“SHARE THIS SCOPE”（「このスコープを共有」））で、一番下までスクロールし、“Request Shared Information as PDF”（「PDF形式で共有情報をリクエスト」）を選択します。
14. ドキュメントが生成されるまでしばらくお待ちください。
15. （“Copy of information shared with ACME.pdf (66.84 KB)”（「ACME.pdf共有情報のコピー（66.84 KB）」））ドキュメントをダウンロードします。

7. 附録

7.1. 附録：請求書の例

請求書の例を記載します。

詳細は以下のセクションを参照してください：セクション 4.3.4. 料金。



ENX Association • Bockenheimer Landstr. 97-99 • D 60325 Frankfurt am Main

[redacted]

INVOICE / RECHNUNG

[redacted]
Invoice Number / Rechnungsnummer
[redacted]
Invoice Date / Rechnungsdatum
[redacted]
Payment Conditions / Zahlungsbedingungen

Your Purchase Order Number / Ihre Bestellnummer
[redacted]
Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
Period of Service / Leistungszeitraum
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen

Pos.	Prod.ID/ Art.-Nr.	Qty./ Anz.	Unit / Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9011	1	Loc	Assessment Based Charges for TISAX Scope [redacted] (Scope-ID: [redacted])	405,00 €	405,00 €
					Net Amount / Netto	405,00 €
					VAT / MwSt (19,00%)	76,95 €
					Gross Amount / Brutto	481,95 €

Please transfer the gross amount without deductions and with reference to the invoice number to our bank account. Bank service charges must be paid by the remittor.

ENX Association

Address
ENX Association
Bockenheimer Landstr. 97-99
60325 Frankfurt am Main
Germany

Contact
Phone +49 69 9866927-0
Fax +49 69 9866927-99
Email info@enx.com
Contact ar@enx.com

Bank Account
IBAN: DE36 5005 0201 0000 3067 89
Swift/BIC: HELADEF1822
Bank: Frankfurter Sparkasse
Post.-Addr.: 60255 Frankfurt/Main, Germany

Registration of the Association
Registered at Boulogne-Billancourt, France
under Registration-No. W923004198
VAT-ID: DE813277682
President: Philippe Ludet

7.2. 附録：確認メールの例

オンライン登録の必須手続きがすべて完了すると、確認メールが送信されます。

この確認メールの送信についての詳細は、以下のセクションをご参照ください：セクション 4.5.8. 確認メール。

件名： [TISAX] スコープS3ZY5Vが承認されました

〇〇 様

TISAX審査スコープをご登録いただきありがとうございます。貴社のスコープ登録を実施し、スコープを承認いたしました。すべてのスコープ情報を含むTISAXスコープ抜粋と、現在のTISAX審査機関のリストを添付します。

次の手順

添付のTISAXスコープ抜粋を使って、貴社のスコープについて、すべてのTISAX審査機関に見積もりを依頼できます。

サポートが必要な場合

TISAXに関するご質問は、TISAXに関するよくある質問か、TISAX参加企業のためのハンドブックをご覧ください。TISAXに関してさらにサポートが必要な場合は、メール（tisax@enx.com）またはTISAXホットライン（+49 69 986692-777）まで電話でご連絡ください。

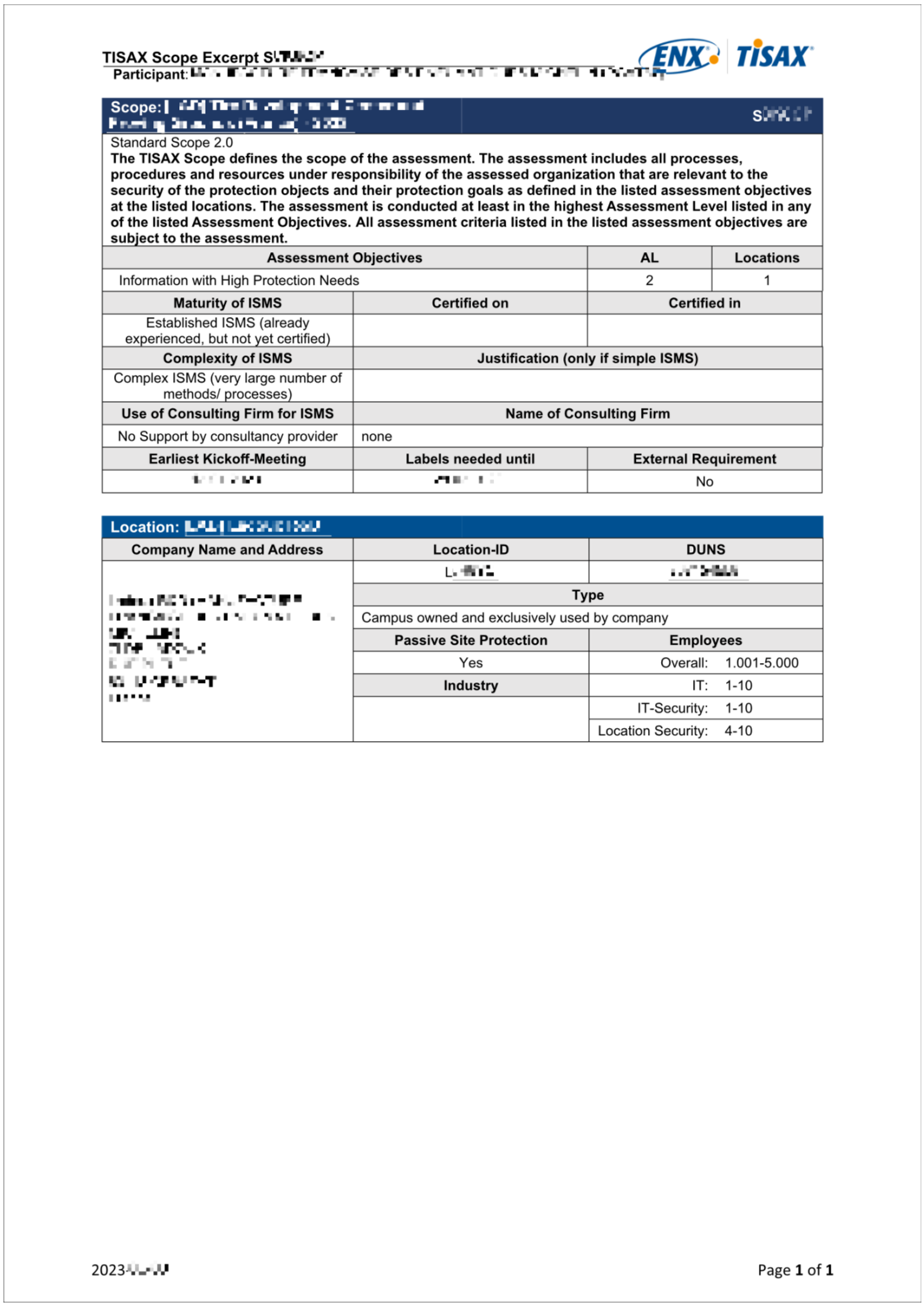
よろしくお願いいたします。

TISAXチーム

7.3. 附録：TISAXスコープ抜粋

確認メールには「TISAXスコープ抜粋」が添付されています。

詳細は以下のセクションを参照してください：セクション 4.5.8. 確認メール。



TISAX Scope Excerpt S[redacted]

Participant: [redacted]

Scope: [redacted] S[redacted]

Standard Scope 2.0

The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations. The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

Assessment Objectives	AL	Locations
Information with High Protection Needs	2	1

Maturity of ISMS	Certified on	Certified in
Established ISMS (already experienced, but not yet certified)		

Complexity of ISMS	Justification (only if simple ISMS)
Complex ISMS (very large number of methods/ processes)	

Use of Consulting Firm for ISMS	Name of Consulting Firm
No Support by consultancy provider	none

Earliest Kickoff-Meeting	Labels needed until	External Requirement
[redacted]	[redacted]	No

Location: [redacted]

Company Name and Address	Location-ID	DUNS
[redacted]	L[redacted]	[redacted]
	Type	
	Campus owned and exclusively used by company	
	Passive Site Protection	Employees
	Yes	Overall: 1.001-5.000
	Industry	IT: 1-10
		IT-Security: 1-10
		Location Security: 4-10

2023[redacted]

Page **1** of **1**

7.4. 附録：Participant status（参加企業ステータス）

7.4.1. 概要：Participant status（参加企業ステータス）

「参加企業ステータス」は、貴社がTISAXプロセスのどの段階にあるかを定義します。

「参加企業ステータス」には、以下の種類があります。

1. Incomplete （未完了）
2. Awaiting approval （承認待ち）
3. Preliminary （予備）
4. Registered （登録済み）
5. Expired （期限切れ）

下にある各ステータスに関するセクションの表には、以下の項目が記載されています。

- 貴社の状況
  （このステータスの時、どういった状態か）
- 貴社の次の行動
  （次のステータスがある場合、そのステータスに進むために必要なこと）
- ENX協会の次の行動
  （次のステータスがある場合、貴社のステータスを次に進めるために必要なこと）
- 次のステータス
  （存在する場合）

次のイラストは、あるステータスから次のステータスに進むための手続きを示しています。

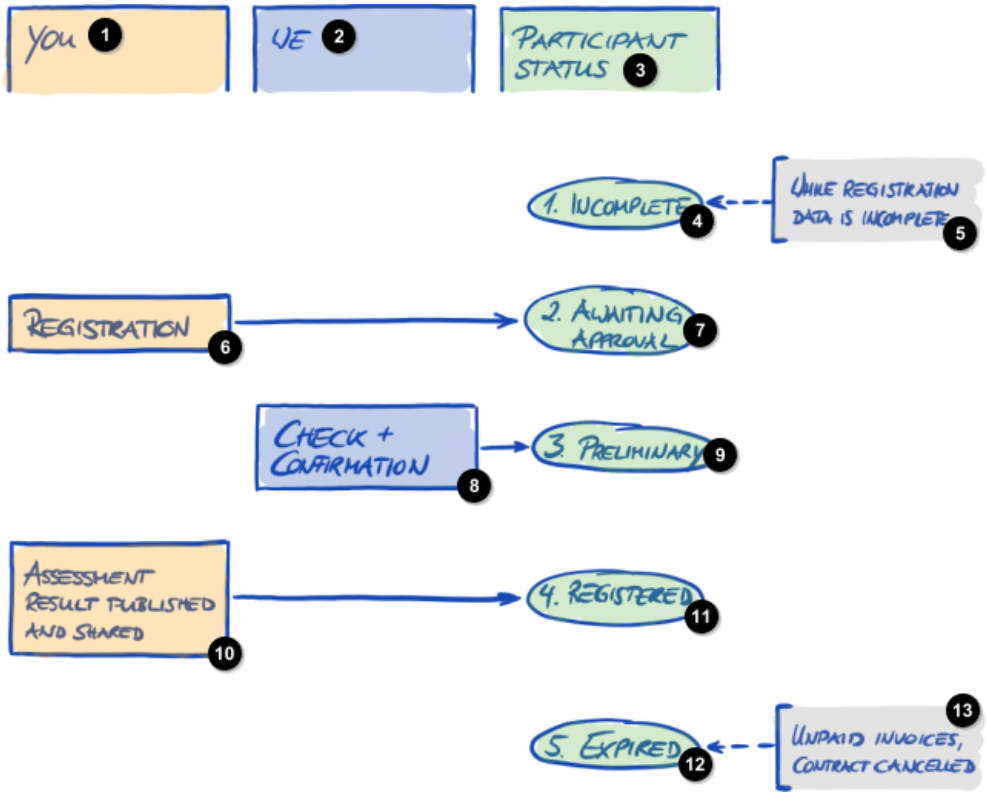


図 34. 参加企業ステータスの概要

1. 貴社
2. ENX協会
3. 参加企業ステータス
4. 1.未完了
5. 登録データが不完全な間
6. 登録
7. 2.承認待ち
8. 確認 + 確定
9. 3.予備
10. 審査結果の公表と共有
11. 4.登録済み
12. 5.期限切れ
13. 未払い請求書、契約解除

7.4.2. Participant status “Incomplete” （参加企業ステータス「未完了」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
未完了	TISAX登録が完了していません。 参加規約に同意していないか、 参加企業の主要拠点を指定していないか、 参加企業の主要連絡先が指定されていないか、 その他の必要な情報が不足しています。	以下のページから登録を進めてください： enx.com/en-US/SignIn	リマインダーメールをお送りします（通常数日以内）。	承認待ち

7.4.3. Participant status “Awaiting approval” （参加企業ステータス「承認待ち」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
承認待ち	TISAXの登録申請を完了しました。 審査スコープの登録は、完了しているか、未完了の状態です。	我々の次の行動をお待ちください。	貴社の申請を確認し、通常は承認します。 ただし、通常は、貴社が審査スコープを登録することでも、確認は開始します。 参加企業IDとスコープIDを割り当てます。 確認メールをお送りします。添付の「TISAXスコープ抜粋」（PDF）は、我々のデータベースに登録されている情報を要約したものです。	予備

7.4.4. Participant status “Preliminary” （参加企業ステータス「予備」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
予備	TISAXの登録に成功しました。	料金をお支払いください（該当する場合）。 TISAX審査プロセスを実施してください。 審査結果を公表・共有してください。	なし	登録済み

7.4.5. Participant status “Registered” （参加企業ステータス「登録済み」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
登録済み	TISAX審査プロセスを完了し、TISAXラベルを取得しました。 審査結果は公表・共有済みです。 TISAXラベルは、TISAX審査プロセスに合格した場合にのみ発行されます。ENXポータルでは、これを反映して審査スコープのステータスが「アクティブ」となっています。	なし	なし	（期限切れ）

注意事項:

パートナー企業の審査結果にアクセスしたい場合

他の参加企業の審査結果を受け取るには、以下のいずれかの前提条件を満たす必要があります。

- 貴社の審査結果を共有した場合（これにより、貴社によるTISAXへの参加が真剣なものであり、自動車コミ☒ユニティの一員であることが「証明」されたとみなされます）。
- 自動車業界（OEMやティア1サプライヤーなど）での評判に基づき、ENX協会が貴社を承認した場合。
- 他の参加企業から審査結果を受け取ることに、正当な関心があることを貴社が証明した場合。これは、入念なプロセスで検証する必要があり、多額の費用が発生する可能性があります。詳細についてはお問い合わせください。

7.4.6. Participant status “Expired” （参加企業ステータス「期限切れ」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
期限切れ	料金を支払っていないか、 貴社もしくはENX協会が相互契約（一般取引条件）を解除した場合。	なし	なし	なし

7.5. 附録：Assessment scope status（「審査スコープのステータス」）

7.5.1. 概要：Assessment scope status（「審査スコープのステータス」）

「審査スコープのステータス」は、貴社の審査スコープがライフサイクルのどの段階にあるかを定義します。

「審査スコープのステータス」は「審査ステータス」とは異なることに注意してください。「審査ステータス」の詳細については、以下を参照してください：セクション 7.6. 附録：Assessment status（審査ステータス）。

「審査スコープのステータス」には、以下の種類があります。

1. Incomplete （未完了）
2. Awaiting your order （貴社の依頼待ち）
3. Awaiting ENX approval （ENXの承認待ち）
4. Awaiting your payment （支払い待ち）
5. Registered （登録済み）
6. Active （アクティブ）
7. Expired （期限切れ）

下にある各ステータスに関するセクションの表には、以下の項目が記載されています。

- 貴社の状況
  （このステータスの時、どういった状態か）
- 貴社の次の行動
  （次のステータスがある場合、そのステータスに進むために必要なこと）
- ENX協会の次の行動
  （次のステータスがある場合、貴社のステータスを次に進めるために必要なこと）
- 次のステータス
  （存在する場合）

次のイラストは、あるステータスから次のステータスに進むための手続きを示しています。

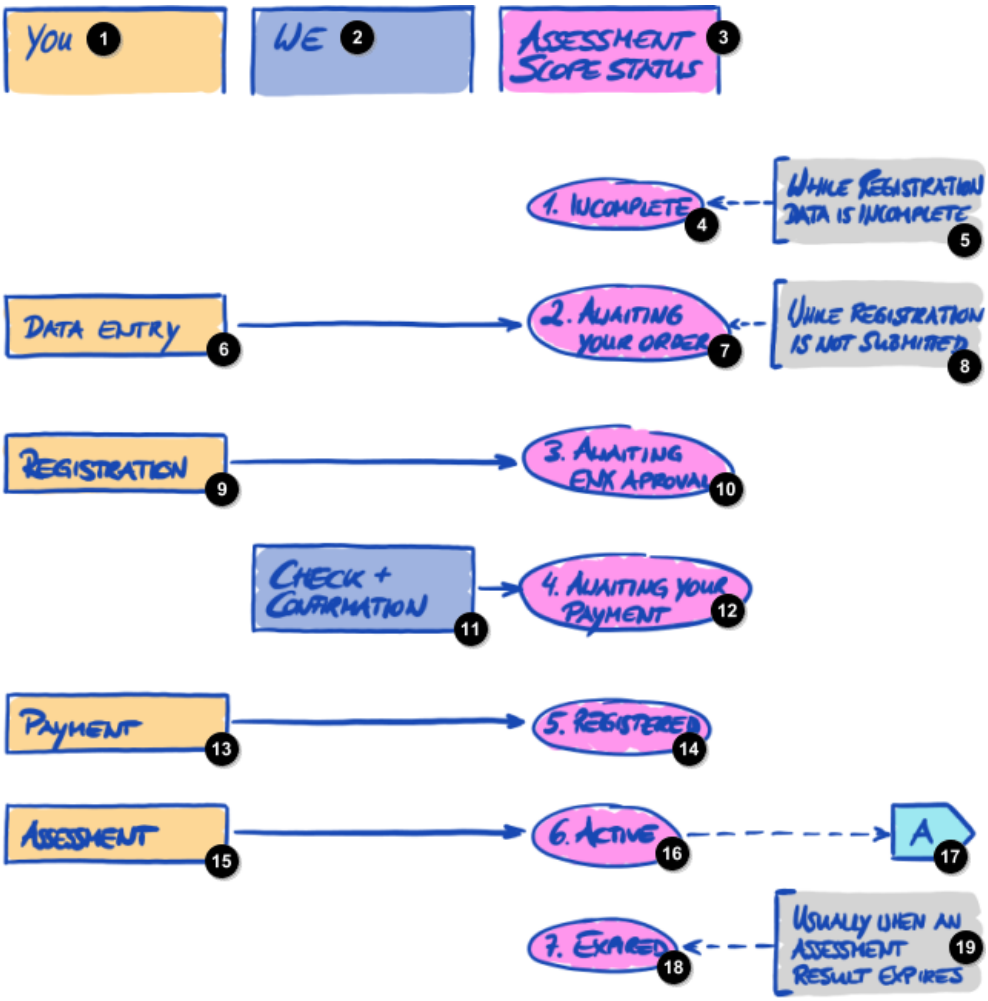


図 35. 審査スコープステータスの概要

1. 貴社
2. ENX協会
3. 審査スコープステータス
4. 1.未完了
5. 登録データが不完全な間
6. データ入力
7. 2.貴社の依頼待ち
8. 登録が未提出の期間
9. 登録
10. 3.ENXの承認待ち
11. 確認 + 確定
12. 4.支払い待ち

13. 支払い
14. 5.登録済み
15. 審査
16. 6.アクティブ
17. A
18. 7.期限切れ
19. 通常は、審査結果の期限切れ

上図のページ外へと向かう「A」は、審査スコープステータス「アクティブ」と「審査ステータス」をリンクしています。「審査ステータス」の詳細については、以下を参照してください：セクション 7.6. 附録：Assessment status（審査ステータス）。

7.5.2. Assessment scope status “Incomplete” （審査スコープステータス「未完了」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
未完了	審査スコープの登録が完了していないか、 必要な情報で提供されていないものがあります。	以下のページから登録を進めてください： enx.com/en-US/SignIn	リマインダーメールをお送りします（通常数日以内）。	貴社の依頼待ち

このステータスがどのような役割を果たしているかについては、以下を参照してください：セクション 4.5.7. 審査スコープの登録。

7.5.3. Assessment scope status “Awaiting your order” （審査スコープステータス「貴社の依頼待ち」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
貴社の依頼待ち	スコープの登録が完了していません。	以下のページから登録を進めてください： enx.com/en-US/SignIn	リマインダーメールをお送りします（通常数日以内）。	ENXの承認待ち

このステータスがどのような役割を果たしているかについては、以下を参照してください：セクション 4.5.7. 審査スコープの登録。

7.5.4. Assessment scope status “Awaiting ENX approval” （審査スコープステータス「ENXの承認待ち」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
ENXの承認待ち	審査スコープの登録申請が完了しました。	我々の次の行動をお待ちください。	貴社の申請を確認し、通常は承認します。 スコープIDを割り当てます。 確認メールをお送りします。 添付の「TISAXスコープ抜粋」（PDF）は、我々のデ⊠ータベースに登録されている情報を要約したものです。	支払い待ち

このステータスがどのような役割を果たしているかについては、以下を参照してください：セクション 4.5.7. 審査スコープの登録。

7.5.5. Assessment scope status “Awaiting your payment” （審査スコープステータス「支払い待ち」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
支払い待ち	審査スコープの登録が完了し、承認されました。 貴社は確認メールと「TISAXスコープ抜粋」を受け取っています。	料金をお支払いください（該当する場合）。 TISAX審査機関にオフ□ァ□ーを依頼します。 「支払い待ち」ステータス以降: ▪ パートナー企業と、審査に関する情報の共有を開始できます。[34] ▪ 審査結果の公開は事前に設定できます（この設定は、審査スコープのステータスが「アクティブ」に変更された時点で有効になります）。	貴社の支払いを待ちます。	登録済み

このステータスがどのような役割を果たしているかについては、以下を参照してください：セクション 4.5.8. 確認メール。

7.5.6. Assessment scope status “Registered” （審査スコープのステータス「登録済み」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
登録済み	審査スコープは登録済みです。 支払いが完了したか、その他の状況により、貴社の商業的ステータスが問題なしと判断されました。	TISAXの審査プロセスに進んでください。	なし	アクティブ

7.5.7. Assessment scope status “Active” （審査スコープステータス「アクティブ」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
アクティブ	TISAX審査プロセスを完了し、TISAXラベルを取得しました。	審査結果を公開および共有できます。 低いステータスの時点で設定していた公開と共有の権限が有効になります。	なし	期限切れ

公開と共有に関する詳細は、以下を参照してください：セクション 6. 共有（ステップ 3）。

7.5.8. Assessment scope status “Expired” （審査スコープステータス「期限切れ」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
期限切れ	以下のいずれかです。 ▪ 90日以内に審査スコープ登録を完了しなかった	審査スコープの登録を新しく開始してください。	なし	未完了 または 貴社の依頼待ち または ENXの承認待ち
	• 料金の支払いが不当に遅れた			
	• TISAXの手続きを打ち切った			
	• 審査結果の有効期限（3年間）が過ぎた			
	• 審査スコープに大きな変更があった（審査スコープに含まれる拠点が貴社に属さなくなった等）			

7.6. 附録：Assessment status（審査ステータス）

7.6.1. 概要：Assessment status（審査ステータス）

「審査ステータス」は、貴社が審査プロセスのどの段階にいるかを定義します。審査ステータスは、別の種類の審査に進む（「初回審査」から「是正計画審査」等）につれて変化します。

「審査ステータス」は「審査スコープステータス」とは異なることに注意してください。「審査スコープステータス」の詳細については、以下を参照してください：セクション 7.5. 附録：Assessment

scope status（「審査スコープのステータス」）。

「審査ステータス」には、以下の種類があります。

1. Initial assessment ordered （初回審査依頼済み）
2. Initial assessment ongoing （初回審査実施中）
3. Waiting for corrective action plan assessment （是正計画審査待ち）
4. Waiting for follow-up （フォローアップ待ち）
5. Finished （終了）

下にある各ステータスに関するセクションの表には、以下の項目が記載されています。

- 貴社の状況
  （このステータスの時、どういった状態か）
- 貴社の次の行動
  （次のステータスがある場合、そのステータスに進むために必要なこと）
- ENX協会の次の行動
  （次のステータスがある場合、貴社のステータスを次に進めるために必要なこと）
- 次のステータス
  （存在する場合）

次のイラストは、あるステータスから次のステータスに進むための手続きを示しています。

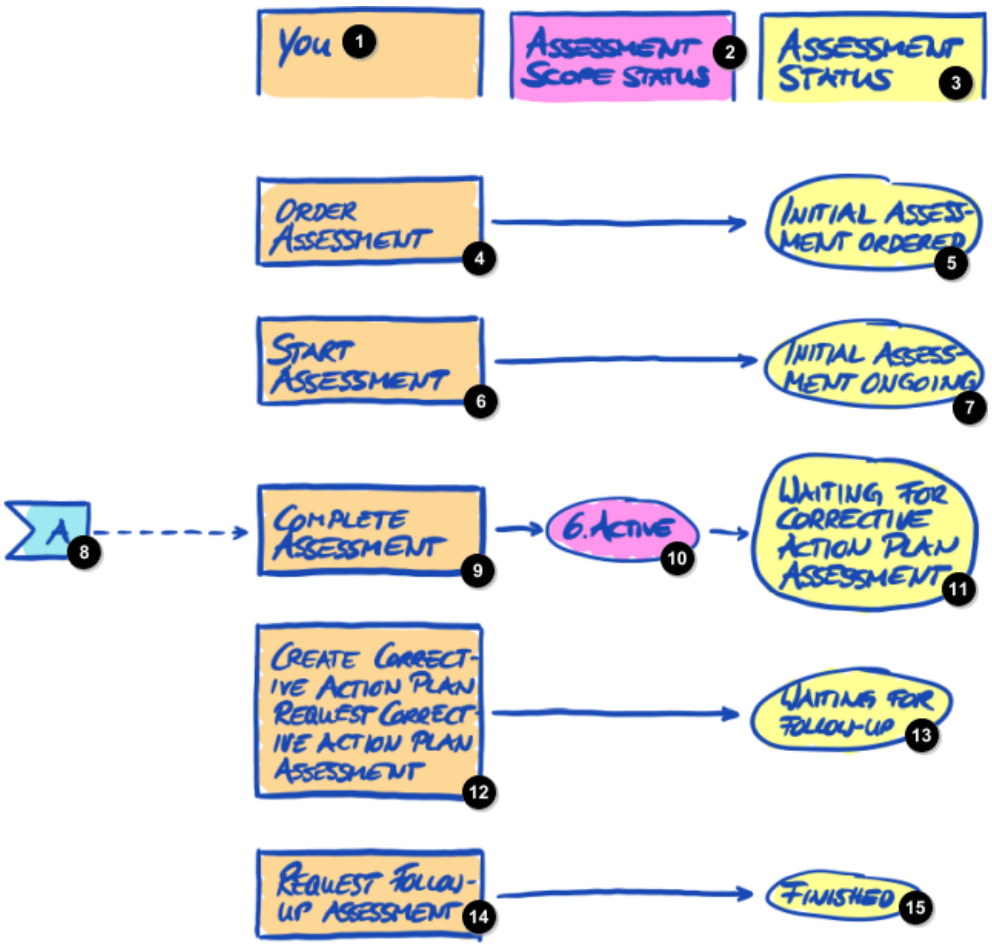


図 36. 審査ステータスの概要

1. 貴社
2. 審査スコープステータス
3. 審査ステータス
4. 審査依頼
5. 初回審査依頼済み
6. 審査開始
7. 初回審査実施中
8. A
9. 審査完了
10. 6.アクティブ
11. 是正計画審査待ち
12. 是正計画の作成
    是正計画審査を依頼
13. フォローアップ待ち
14. フォローアップ審査を依頼
15. 完了

上図のページ外へと向かう「A」は、審査スコープステータス「アクティブ」と審査ステータス「是正計画審査待ち」をリンクしています。「審査スコープステータス」の詳細については、以下を参照してください：セクション 7.5. 附録：Assessment scope status（「審査スコープのステータス」）。

7.6.2. Assessment status “Initial assessment ordered” （「審査ステータス「初回審査依頼済み」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
初回審査依頼済み	TISAX審査機関のいずれかを選択し、初回審査を依頼しました。	TISAX審査プロセスを続行します。	なし	初回審査実施中

7.6.3. Assessment status “Initial assessment ongoing” （審査ステータス「初回審査実施中」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
初回審査実施中	初回審査は次のいずれかの状態です。 ▪ 開始済み ▪ 完了したが、審査機関がTISAX審査報告書を未提出	なし	なし	是正計画審査待ち（該当する場合）

7.6.4. Assessment status “Waiting for corrective action plan assessment” （審査ステ☒ータス「是正計画審査待ち」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
是正計画審査待ち	貴社の審査機関が初回審査を実施しました。 貴社の審査機関が、ENX協会にTISAX審査報告書を提出しました。 審査結果は（重大な/軽微な）不適合です。	是正計画を作成してください。 是正処置を開始してください。 是正計画審査を依頼してください。	なし	フォローアップ待ち（該当する場合）

審査ステータスの「是正計画審査待ち」の最長期間は、9か月です。詳細は以下のセクションを参照してください：セクション 5.4.9.3. 是正計画の要求事項。

7.6.5. Assessment status “Waiting for follow-up” （審査ステータス「フォローアップ待ち」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
フォローアップ待ち	審査機関は、貴社の是正計画を承認しました。 貴社は是正処置を実施しました。	フォローアップ審査を依頼してください。	なし	完了

審査ステータスの「フォローアップ待ち」の最長期間は、9か月です。詳細は以下のセクションを参照してください：セクション 5.4.9.3. 是正計画の要求事項。

7.6.6. Assessment status “Finished” （審査ステータス「終了」）

ステータス	状況	貴社の次の行動	ENX協会の次の行動	次のステータス
完了	貴社の審査機関がフォローアップ審査を実施しました。 審査結果に不適合は含まれていません。 貴社の審査機関が、ENX協会にTISAX審査報告書を提出しました。	審査結果を公表・共有してください。	なし	なし

7.7. 附録：「事前審査」と「ギャップ分析」が効果的ではない理由

一般的に、審査機関に「事前審査」や「ギャップ分析」の実施を依頼しないことをお勧めします。TISAX審査プロセスをそのまま開始する方が理にかなっているケースが大半です。

このセクションでは、最もよく耳にする懸念事項について取り上げます。

以下の理由で事前審査を検討していますか?

1. 顧客が好ましくない審査結果を目にすることへの懸念がある方へ

   審査結果を誰が見られるかは、貴社が完全に管理できます。審査機関がENXポータルに何をアップロードするかは、貴社が決定します。誰にも見せないようにすることも可能です（当然、監査人は除きます）。

   また、審査機関は、TISAX審査報告書の最初の2セクションのみをアップロードし、詳細な審査結果をアップロードすることはありません。

2. 事前審査でコストを削減できるのではないかとお考えの方へ
   - 事前審査を行う場合
     - 事前審査の費用がかかります
     - 貴社内で不適合の修正に費用が発生する可能性があります
     - TISAX審査（「初回審査」）の全費用を支払う必要があります

     たとえ指摘事項がなくても、2回の審査の全費用を支払う必要があります

   - TISAX審査から開始した場合
     - 初回審査の費用がかかります
     - 貴社内で指摘事項の修正に費用が発生する可能性があります
     - いわゆる「フォローアップ審査」では、監査人は初回審査で指摘された不適合事項が修正されているかどうかにのみ注目するため、（初回審査に比べ）支払額が大幅に少なくなる可能性があります

     たとえ指摘事項があったとしても、支払うのは審査および短期間のフォローアップ審査の全費用のみです。

3. 審査に落ちると、永続的な影響があるとお考えの方へ

   審査は何度でも受けられるため、不合格の状態は変えることができます。審査結果が期待にそぐわなかったり、9か月の期限内に不適合を是正処置で修正できなかったりした場合は、失敗した審査を事前審査とみなし、新たにやり直せば良いだけです。そして、誰にも最初の結果を見せる必要はありません。合格した審査結果だけを共有すれば良いのです。

他にも以下の点を考慮する必要があります。

- 審査結果が予想よりも良かった場合、TISAX仮ラベルを取得できることがあります。 TISAX仮ラベルは、パートナー企業とそのまま共有できます。これは事前審査では不可能です。
- 事前審査を実施する機関にTISAX審査を依頼することを考えている場合、その機関は貴社のコンサルティングは行えません。コンサルティングを実施した場合、TISAX審査機関には別の機関を選ぶ必要があります。

事前審査を受けることがメリットとなる企業はほとんどありませんが、以下のような利点も存在します。

監査人が

- 貴社が確信を持てずにいる、ISMSの重要な側面に集中できます
- 通常よりも時間を費やして、より深い洞察を行えます
- 指摘事項を、異なる方法で文書化できます

TISAX審査プロセスに関するセクションを読むと、上記の内容をより理解しやすくなります。

7.8. 附録：カスタムスコープ

ほとんどのTISAX参加企業は、標準スコープを選択します。 しかし、稀にカスタムスコープを選択する必要があるケースも存在します。

カスタムスコープは2種類あります。

7.8.1. カスタム拡張スコープ

スコープを拡張できます。カスタム拡張スコープには、標準スコープよりも「多くの」内容が含まれます。審査機関による確認も多くなります。

目的：カスタム拡張スコープは、TISAX審査を社内または自動車業界外で使用したい場合に、必要となる可能性があります。

TISAXラベルと結果の共有：カスタム拡張スコープには、必ず標準スコープが含まれます。したがって、カスタム拡張スコープではTISAXラベルが付与されます。[35] 他のTISAX参加企業は、同様に審査結果を受け入れます。

記述：標準スコープにはあらかじめ定義された記述がありますが、カスタム拡張スコープの場合は、スコープに関する独自の記述が必要です。

7.8.2. フルカスタムスコープ

貴社独自のスコープを、完全に自由に定義できます。

目的：異なる審査スコープに属し、特定のサイト（データセンターなど）でサービスを使用する拠点がある場合に、それらの

サービスに対してフルカスタムスコープを使用できます。これにより、TISAX審査機関は、対象サービスのフルカスタムスコープの審査結果を簡単に再利用できます。

例えば、（異なるスコープに属する可能性もある）多くの拠点の中の一つに、中央IT部門があるとします。このIT部門に専用のフルカスタムスコープを定義することで、それ以外のスコープでそれぞれの審査結果を再利用しやすくなる場合があります。

TISAXラベルと結果の共有：フルカスタムスコープでは、TISAXラベルは付与されません。審査結果はENXポータルに記録され、日付、有効期間、総合審査結果の適合・不適合が記載されます。この審査結果を共有することは可能です。しかし、TISAXラベルのない審査結果を共有しても、ほとんどの場合、受け取った側は審査を「不合格」と捉えるでしょう。他のTISAX参加企業は、一般的にフルカスタムスコープの審査結果を受け入れません。

記述：カスタム拡張スコープについては、フルカスタムスコープが必要であれば独自のスコープ記述が必要です。

重要事項：

あくまでも、フルカスタムスコープは非常に稀な点にご注意ください。フルカスタムスコープを選択しても、98%の確率で審査機関によって標準スコープに戻されるでしょう。審査機関のアドバイスなしに、フルカスタムスコープを選択した参加企業はいません。

フルカスタムスコープの審査では、TISAXラベルを受け取ることができません。したがって、一般的に、フルカスタムスコープを選択しないことをお勧めします。なぜならば、他の参加企業がフルカスタムスコープの審査結果を受け入れることは、一般的にないからです。
パートナー企業が審査結果を受け入れ、貴社独自のスコープ記述に同意するという明確な保証がなければ、フルカスタムスコープは選択しないでください。

7.9. 附録：参加企業データのライフサイクル管理

以下のセクションでは、参加企業データ関連で何らかの変更が生じた場合の対処方法を解説します。

7.9.1. 参加企業データ（ENXポータル）にアクセスできなくなった場合

ENXポータルにアクセスできる人が社内におらず、参加企業データが残っていない場合は、ENX協会までご連絡ください。。 貴社の参加企業データへのアクセス回復のお手伝いをいたします。

7.9.2. 連絡先の管理

貴社の参加企業の主要連絡先、およびポータルアカウントを持つその他の「管理連絡先」は、いつでもENXポータルにアクセスして、以下の操作を行えます。

- 新しい連絡先の追加
- 既存の連絡先の削除
- 既存の連絡先に関する詳細の変更

7.9.2.1. 新しい連絡先の追加方法

新しい連絡先を追加するには、以下の手順に従ってください。

1. ENXポータルにログインします。

2. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
3. ドロップダウンメニューから“ADMINISTRATORS”（「管理者」）を選択します。
4. “Create new TISAX Administrator”（「TISAX管理者の新規作成」）ボタンをクリックします。
5. 連絡先のデータを入力します。
6. “Save Contact”（「連絡先を保存」）ボタンをクリックします。
7. 表に移動し、連絡先の表の行を見つけます。
8. 連絡先の行の末尾に移動し、下向き矢印のボタンをクリックします。
9. “Edit TISAX Administrator”（「TISAX管理者を編集」）を選択します。
10. 新しいウィンドウ（“Edit TISAX Contact”（「TISAX連絡先を編集」））で“ENX PORTAL ACCESS”（「ENXポータルアクセス」）までスクロールします。
11. “Yes”（「はい」）を選択します。
12. 表示されるセクション“WEB ROLES”（「ウェブ役割設定」）で“Add Role”（「役割を追加」）ボタンをクリックします。
13. 割り当てたい役割（“TISAX Administrator”（「TISAX管理者」）など）を選択します。
14. “Add Role”（「役割を追加」）ボタンをクリックします。
15. “Save Contact”（「連絡先を保存」）ボタンをクリックします。

7.9.2.2. 既存の連絡先の削除方法

既存の連絡先を削除するには、以下の手順に従ってください。

1. ENXポータルにログインします。
2. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
3. ドロップダウンメニューから“ADMINISTRATORS”（「管理者」）を選択します。
4. 表に移動し、連絡先の表の行を見つけます。
5. 連絡先の行の末尾に移動し、下向き矢印のボタンをクリックします。
6. “Delete TISAX Administrator”（「TISAX管理者を削除」）を選択します。
7. 確認画面が表示されるので、“Delete”（「削除」）ボタンをクリックしてください。

7.9.2.3. 既存の連絡先に関する詳細の更新方法

既存の連絡先の詳細を更新するには、以下の手順に従ってください。

1. ENXポータルにログインします。
2. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
3. ドロップダウンメニューから“ADMINISTRATORS”（「管理者」）を選択します。
4. 表に移動し、連絡先の表の行を見つけます。
5. 連絡先の行の末尾に移動し、下向き矢印のボタンをクリックします。
6. “Edit TISAX Administrator”（「TISAX管理者を編集」）を選択します。
7. 詳細を更新します。
8. “Save Contact”（「連絡先を保存」）ボタンをクリックします。

7.9.3. 拠点の管理

貴社の参加企業の主要連絡先、およびポータルアカウントを持つその他の「管理連絡先」は、いつでもENXポータルにアクセスして、以下について申請できます。

- 企業名の変更
- 拠点の変更（移転・移動）
- 市区町村等の名称の変更
- 新しい拠点の追加

必要な手順については、以降のセクションで説明します。

注意事項:

- TISAXでは、社名と所在地の組み合わせで「拠点」を定義します。
- 各拠点には「拠点ID」が割り当てられます（拠点IDは必ず「L」で始まり、6文字です。例：L1L3XY）。
- 貴社が現在の所在地から新しい所在地に移転した場合、古い所在地は有効な拠点ではなくなります。

重要事項:

ENXポータルで“Save Location”（「拠点を保存」）ボタンをクリックした後は、貴社による変更はできなくなります。以下のような場合は、変更を申請できます。

7.9.3.1. 社名の変更の申請方法

貴社の状況	社名の変更
例:	元の社名「ACME Tires Corporation」から 新しい社名「ACME Corporation」になった場合。

社名変更をご希望の方は、以下の手順で手続きしてください。

1. ENXポータルにログインします。
2. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
3. ドロップダウンメニューから“LOCATIONS”（「拠点」）を選択します。
4. 表に移動し、貴社の所在地が記載されている行を探します。
5. 所在地の行の末尾に移動し、下向き矢印のボタンをクリックします。
6. “Request Change”（「変更を申請」）を選択します。
7. 新しいウィンドウ（“Request Change”（「変更を申請」））で、フォームフィールド“Subject of the change”（「変更対象」）に移動し、ドロップダウンメニューを開いて“Company Name”（「社名」）を選択します。
8. フォームの入力を続けます。
9. フォームを送信します。

ENX協会が貴社の申請を確認し、可能であれば社名変更の申請を受理します。変更が完了次第お知らせいたします。

7.9.3.2. 拠点変更の申請方法

貴社の状況	新しい拠点への移転
例:	旧所在地「ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Germany」から 新所在地,「ACME Corporation Behrenstraße 35, 10117 Berlin, Germany」へ移転。

重要事項:

貴社の所在地の市区町村等の名称が、公的機関により変更された場合の対処方法は、セクション 7.9.3.3. 市区町村の名称等が変更された場合の申請方法を参照してください。

拠点が新しい所在地に移転した場合は、以下の手順に従ってください。

1. 新しい拠点を作成する
   a. ENXポータルにログインします。
   b. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
   c. ドロップダウンメニューから“Locations”（「拠点」）を選択します。
   d. “Create TISAX Location”（「TISAX拠点を作成」）ボタンをクリックします。
   e. 新しいウィンドウ（“CREATE TISAX LOCATION”（「TISAX拠点を作成」））で新しい拠点の詳細をフォームに入力します。
   f. “Save Location”（「拠点を保存」）ボタンをクリックします。
2. 新しく作成した拠点の“Location ID”（「拠点ID」）は把握しておく必要があります。「拠点ID」は、“MY LOCATIONS”（「自社拠点」）表の最初の列にあります。審査機関は、ENXポータルで審査スコープを更新する際に、この「拠点ID」を必要とします。
3. 審査機関に移転の旨を伝えてください（移転前と移転後の「拠点ID」の情報が必要です）。審査はもうお済みですか?
   a. まだであれば、拠点の変更に関して他にすることはありません。
   b. 審査が完了している場合は、審査機関に“scope extension assessment”（「スコープ拡大審査」）を依頼する必要があります。詳細は以下のセクションを参照してください: セクション 7.10. 附録: スコープ拡大審査。

審査機関は、貴社の依頼を確認し、ENXポータルで審査スコープを更新します。

注意事項:

貴社から審査を依頼された後にのみ、審査機関は貴社の審査スコープを更新できます。

7.9.3.3. 市区町村の名称等が変更された場合の申請方法

貴社の状況	貴社の拠点の市区町村等の名称が変更された場合。貴社の地理的な所在地に変化はありません。
例:	旧所在地「ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Germany」から 新所在地,「ACME Corporation Behrenstraße 97-99, 60325 Frankfurt, Germany」へ名称変更。

公的機関により、貴社の市区町村等の名称が変更された場合は、次の手順に従ってください。

1. ENXポータルにログインします。
2. メインナビゲーションバーに移動し、“MY TISAX”（「MY TISAX」）を選択します。
3. ドロップダウンメニューから“Locations”（「拠点」）を選択します。
4. 表に移動し、貴社の所在地が記載されている行を探します。
5. 所在地の行の末尾に移動し、下向き矢印のボタンをクリックします。
6. “Request Change”（「変更を申請」）を選択します。
7. 新しいウィンドウ（“Request Change”（「変更を申請」））で、フォームフィールド“Subject of the change”（「変更対象」）に移動し、ドロップダウンメニューを開き、“Address”（「所在地」）を選択します。
8. フォームの入力を続けます。
9. フォームを送信します。

ENX協会が貴社の申請を確認し、可能であれば市区町村等の名称変更の申請を受理します。変更が完了次第お知らせいたします。

重要事項:

これらの手順は、貴社の物理的な所在地は変わらないが、公的機関により市区町村等の名称が変更された場合にのみ適用されます。
新しい拠点に移転した場合は、セクション 7.9.3.2. 拠点変更の申請方法をご覧ください。

7.9.3.4. 拠点の追加方法

既存のTISAXラベルの有効期間中に新たに拠点を追加する場合は、審査機関に「スコープ拡大審査」（“scope extension assessment”）を依頼できます。

詳細は以下のセクションを参照してください：セクション 7.10. 附録：スコープ拡大審査。

7.10. 附録：スコープ拡大審査

セクション 5.4.3. TISAX審査の種類で記述されている標準的な種類の審査の他に、「スコープ拡大審査」（“scope extension assessment”）という特別な種類の審査があります。

以下を一つ以上追加したい場合に、既存のTISAX審査スコープを拡張できます。

- 審査目的、または
- 拠点

「スコープ拡大審査」を実施するにあたって、別の審査機関を選択することはできません。審査は標準的な審査と似ていますが、ほとんどの場合、審査機関は以前の審査から適用可能な結果を再利用することを検討します。

スコープ拡大審査を行い、不適合がなければ、審査機関は次のことを行います。

- ENXポータルで審査スコープを更新します。
- スコープ拡大審査報告書を発行します。

スコープ拡大審査によって、既存のTISAXラベルの有効期間が延長されることはありません。

注意事項:

移転または拠点の追加に伴ってスコープ拡大審査を実施する場合は、ENXポータルで新しい拠点を作成する必要があります。「拠点抜粋」または少なくとも「拠点ID」を審査機関に提供してください。
各拠点には「拠点ID」が割り当てられます（拠点IDは必ず「L」で始まり、6文字です。例：L1L3XY）。
ENXポータルの審査結果を更新するにあたって、審査機関は拠点IDを必要とします。

7.11. 附録：ISAのライフサイクル管理

ISAは、ENXワーキンググループが管理しています。

また、以下のような関連事項が存在します。

- VDAが、公式に新バージョンを発行しています。
- 審査機関は、貴社が初回審査を依頼した時点で有効なISAのバージョンを使用します。
- 依頼から初回審査の開始までの間に新しいISAバージョンが発行された場合、双方の合意に基づいて新バージョンを使用できます。
- ISAバージョンの公開日は、Excelシート“Cover”（「表紙」）で確認できます。
  - 例:
    バージョン：5.0 | 改訂4 | 2021-04-16

7.12. 附録：参考資料

このセクションでは、役立つと考えられる資料を記載します。

- ホワイトペーパー「Harmonization of classification levels（分類レベルの調和）」

  「本ホワイトペーパーでは、機密性保護の目的に主眼を置いたスキーム決定に関する、情報セキュリティワーキンググループからの提案を記述します。機密性保護とは、情報が権限のない個人、組織、またはプロセスにアクセスされないようにすることを指します。可用性、完全性、信頼性といった保護目的は、本ホワイトペーパーにおける焦点ではありません。」

  出版：ドイツ自動車工業会（Verband der Automobilindustrie e.V.）

  言語：英語版、ドイツ語版

  https://www.vda.de/en/news/publications/publication/harmonization-of-classification-levels
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--harmonisierung-der-klassifizierungsstufen-

- ホワイトペーパー「Information Security Risk Management」（情報セキュリティリスク管理）

  「本ホワイトペーパーの目的は、自動車業界の企業に対し、リスク志向の情報セキュリティ管理に関する情報を提供し、効果的な情報セキュリティリスク管理を確立できるようにすることにあります。本ホワイトペーパーは、VDA ISAのコントロール質問1.4.1の要求事項を満たせるように、TISAX審査を準備・実施する組織の支援を目的に作成されています。本ホワイトペーパーの内容は、実施上の推奨事項であり、必須の要求事項ではありません。」

  出版：ドイツ自動車工業会（Verband der Automobilindustrie e.V.）

言語：英語版、ドイツ語版

https://www.vda.de/en/news/publications/publication/white-paper--information-security-risk-management-
https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--risikomanagement-in-der-informationssicherheit-

7.13. 附録：クレーム管理

7.13.1. クレームの原因

TISAXに関するクレーム管理では、クレーム対象から以下の2分野に分類されます。

1. ENX協会（TISAXを統括する組織）
2. 審査機関（TISAX審査を実施する機関）

7.13.1.1. ENX協会に対するクレーム

ENX協会に対するクレームは、「TISAX管理責任者」（下記の連絡先を参照）までご連絡ください。

7.13.1.2. 審査機関に対するクレーム

まずは、監査人と直接問題の解決を図ってください。

解決しない場合は、次に審査機関のTISAX担当者にご連絡ください。

それでも解決しない場合は、審査機関の品質管理責任者にご連絡ください。

ここまでで問題が解決しない場合は、ENX協会の「TISAX管理責任者」（下記の連絡先を参照）までご連絡ください。

「TISAX管理責任者」より上の選択肢が必要な場合は、ENX協会の専務理事にご相談ください。

VDAは、クレーム管理には関与しません。

注意事項：

審査機関は、キックオフミーティングの際に、貴社がクレームを申し立てる権利について、貴社に通知する義務があります。 この通知がなかった場合、それ自体がクレームの事由となります。

7.13.1.3. クレーム申し立ての要求事項

ENX協会による対処が必要な場合は、以下の情報が必要です。

- クレームの申立人の情報
  - 社名
  - TISAX参加企業ID
  - 連絡先（名前、メールアドレス、電話番号）
- クレーム対象の審査の情報
  - 審査ID

- ENXポータルにまだ審査が記録されていない場合は、スコープID
- 審査機関の情報
  - 審査機関の社名
  - 監査人の氏名
- クレームの内容に関する情報
  1. 審査機関のパフォーマンスに関する一般的なクレーム
  2. 監査人の手法に関するクレーム
  3. 審査内容に関するクレーム
- 審査内容に関するクレームの場合、異議のある指摘事項
  - コントロール（例：1.6.1 "情報セキュリティに関する事項がどの程度処理されているか"）
  - 指摘事項（全文）
  - 異議の対象
    - コントロールの解釈
    - 内容に関する確認（入手可能な証跡が正しく審査されていない）
    - リスクアセスメント（適切性が考慮されていない）
  - 貴社による審査が異なる理由

7.13.2. クレーム窓口

「TISAX責任者」の連絡先は以下の通りです。

メールアドレス： tisax-complaints@enx.com
電話番号： +49 69 9866927-79

ドイツ国内での通常の営業時間内（UTC+01:00）にご連絡いただけます。

英語または🇩🇪ドイツ語でお話しいただけます。

8. 文書履歴

バージョン2.7

- 4言語（日本語、ブラジルポルトガル語、イタリア語、韓国語）を追加しました。
- HTML版用の言語スイッチャーを追加しました（右上に表示）。
- PDF版のレイアウトを改善しました。
- 機密性に関する二つの新しい審査目的に伴い、さまざまなセクションを更新しました。
- 「審査目的のリスト」のセクションを更新しました。（審査目的「Special data」の表現を修正し、ラベル移行に関する注記を追加しました。）
- タイプミスを修正しました。

バージョン2.6

- 審査目的とラベルに関する一般的な注意事項が追加されました。以前のバージョンでは、審査目的とラベルには、長い「正式名称」と「略称」がありました（例：「保護ニーズの高い情報の取り扱い」と「Info high（情報高）」）。ほとんどの人が略称しか使用しなかったため、これを「正式名称」に変更し、旧来の長い名称を「記述」に変更しました。 さらに、ENXポ⊠ータルおよびTISAX参加企業のためのハンドブックの翻訳版ではすべて、英語の正式名称のみが使用されています。
- 「審査目的のリスト」のセクションを更新し、「High availability」と「Very high availability」の二つの審査目的を追記し、「図6 TISAX審査目的（表形式、長形式および短形式）」を削除しました。
- 「審査目的とISA」のセクションを更新し、二つの審査目的「High availability」および「Very high availability」の適用対象が、基準カタログ「情報セキュリティ」のサブセットのみとなるように反映しました。
- 「審査目的とその依存関係」のセクションを削除しました。
- 「審査目的の選択」セクションを更新し、二つの審査目的「High availability」と「Very high availability」を追加しました。
- 「保護ニーズと審査レベル」セクションを更新し、二つの審査目的「High availability」と「Very high availability」、「表5 ISA基準カタログと保護ニーズのTISAX審査目的へのマッピング」を削除しました。
- 「基準カタログ」のセクションを更新し、二つの審査目的「High availability」と「Very high availability」を追加しました。
- 「要求事項」のセクションを更新し、二つの審査目的「High availability」および「Very high availability」の適用対象が、基準カタログ「情報セキュリティ」のサブセットのみとなるように反映しました。
- 「TISAXラベルの階層」のセクションを更新し、階層が存在するのは一部のみとなったことを反映し、「図36 TISAX審査目的とTISAXラベル（依存関係と階層構造）」を削除しました。
- 「附録：参考資料」セクションを更新し、リンク先の変更を反映しました。
- 複数箇所で細かい説明の追加や修正を行いました。
- タイプミスを修正しました。

バージョン2.5.1

- リンク切れを修正しました。

バージョン2.5

- 「拠点の管理」セクションを追加しました。
- 「附録：参考資料」セクションを更新し、リンク先の変更を反映しました。

バージョン2.4

- TISAX審査プロセスの最長期間に関する不明確な記述をセクション 3.1. 概要から削除しました。
- 「TISAX報告書」の名称を「TISAX審査報告書」に変更しました。
- ISO 27001とTISAXの相違点に関する注記を更新しました。
- 「スコープの記述」セクションを更新し、カスタムスコープのセクションを附録に移動しました。
- 「標準スコープの記述」をバージョン2.0に更新しました。
- 「公開と共有」のセクションを更新し、審査ステータスの共有に関する注記を更新しました。
- 「保護ニーズと審査レベル」のセクションを更新し、「審査レベル 2.5」、「動画に対応したリモート審査」、AL 2とAL 3の違い、妥当性チェックと検証の違いに関する内容を更新しました。
- 登録手続き開始へのリンクを更新しました。
- 変更された招待プロセスを反映するため、「ポータルアカウント」のセクションを更新しました。
- ISAドキュメントのダウンロードリンクを変更しました（enx.comでも入手可能になったことに伴う変更）。
- 「オファーの評価」のセクションを更新し、費用見積もりの根拠を追加しました。
- 「キックオフミーティング」のセクションを追加しました（「最初の正式なオープニングミーティング」のセクションから内容を移動）。
- 「適合性について」のセクションを更新し、4種類の指摘事項に関する新しい表を更新しました。
- 「初回審査」のセクションを更新し、時間的制約に関する注釈を更新しました。
- 「TISAX審査報告書」のセクションを更新し、積極的な是正計画に関する注記を更新しました。
- 「是正計画の作成」のセクションを更新し、「指摘事項」と「根本原因」の要求事項、および是正計画のテンプレートに関する注釈を更新しました。
- 「是正計画審査」のセクションを更新し、唯一の連絡手段としてのメールに関する注釈を更新しました。
- 「是正計画審査の前提条件」のセクションを「是正計画審査の実施理由」に改称し、二つの理由を追加しました。
- 「TISAX仮ラベル」のセクションの有効期間に関する例と説明を更新しました。
- 「TISAX報告書」のセクションの名称を「TISAX審査報告書」に変更しました。
- 「TISAXラベルの更新」のセクションで、ENXポータルの拠点データの再利用に関する注記を更新しました。
- 「附録：「事前審査」と「ギャップ分析」が効果的ではない理由」のセクションを追加しました。
- 「附録：カスタムスコープ」セクションを追加しました（「拡張スコープ」と「縮小スコープ」を「カスタム拡張スコープ」と「フルカスタムスコープ」に変更しました）。
- 「附録：スコープ拡大審査」セクションの、拠点データを参加企業のENXポータルアカウントに追加する理由と注記を更新しました。
- 「附録：ISAのライフサイクル管理」セクションを現状に合わせ更新しました。
- 「附録：参考資料」セクションを更新し、リンク先の変更を反映しました。

- 「附録：クレーム管理」セクションを追加しました。
- 電話番号をクリックできるように変更しました。
- 複数箇所で細かい説明の追加や修正を行いました。
- タイプミスを修正しました。
- TISAX審査機関への注記：この更新は、ENX doc ID 612 バージョン2.1に基づいています。

バージョン2.3

- 副題を変更しました。
- 本資料の主要形式を、WordやPDFからHTMLに変更しました。
- 翻訳版を追加しました（中国語版およびフランス語版、次の項目を参照）。
- 「TISAX参加企業のためのハンドブックをご利用いただける他の言語および形式」セクションを追加しました。
- ENXホームページへのリンクをすべて"https://portal.enx.com" から"https://enx.com"に変更しました（旧リンクも引き続き利用可能）。
- 「VDA ISA」を「ISA」に変更しました。
- ISAのバージョン5で導入された変更を反映するため、セクション 5.2. ISAに基づく自己評価を更新しました。
- 審査目的を記載したすべての表の行の順序を、ISAのバージョン5で変更された基準カタログの順序に合わせて変更しました。
- ISAバージョン5で変更された基準カタログの順序に合わせて、審査目的の一覧を記載した図を更新しました。
- 「スコープの調整」セクションを更新しました（図6、タイプミスの修正、審査目的の更新）。
- 「料金」セクションのクレジットカード決済に関する情報を更新しました。
- 「TISAX審査プロセス図」セクションを更新しました（図34、マネージドサービスプロバイダーに関する記述を削除）。
- 「附属：参考資料」セクションを更新しました（ホワイトペーパー「情報セキュリティリスク管理」を追加）。

バージョン2.2.1

- タイプミスを修正しました。

バージョン2.2

- 表紙の印刷上の問題を修正しました。
- ホームページおよびダウンロードのリンクをすべて変更しました。
- イタリア語での電話対応を追加しました。
- 「カスタムスコープ」セクションを拡張しました。
- 「拠点のスコープを設定」セクションを更新しました。
- 審査目的「第三者への接続」を削除、図7、9、38、表4、5、6、8を更新しました。
- 「審査レベルを伴う」を「審査レベルにおける」に変更しました。

- 「保護ニーズと審査レベル」セクションにおける「TISAX有効化リスト」への言及を削除しました。
  （該当しなくなったため）
- 「審査目的と貴社のサプライヤー」のセクションを追加しました。
- 「参加企業の連絡先」セクションを更新し、ENXポータルで参加企業データを管理できるように、グループのメールアドレスと連絡先の招待に関する情報を追加しました。
- 「審査スコープの登録」セクションの、審査スコープの変更に関する情報を更新しました。
- 「ステータス情報」セクションを更新しました（図12）。
- 「自己評価結果への対処」セクションを更新し、外部の第三者による支援に関する情報を追加しました。
- 「国および地域」セクションを更新し、審査機関の国および地域マトリックスへのリンクを更新しました。
- 「オファーの依頼」セクションを更新しました。
- 「オファーの評価」セクションで、「事前審査」に関する情報を更新しました。
- 「TISAXラベルの更新」セクションで、新しいスコープを登録する必要性に関する情報を更新しました。
- 「共有（ステップ3）」の各サブセクションで、ENXポータルのインターフェースの変更を反映しました。
- 「審査結果を特定の参加企業と共有する」セクションで、共有レベルに関する推奨事項と、共有された審査結果の自動処理に関する注記を更新しました。
- 「TISAX外での審査結果の共有」セクションを追加しました。
- 「ISAのライフサイクル管理」セクションを追加しました。
- 「附録：審査スコープステータス」を更新しました（「貴社の依頼待ち」ステータスを追加、「承認待ち」ステータスを「ENXの承認待ち」に、「承認済み」ステータスを「支払い待ち」に名称変更、図40）。
- 「附録：確認メールの例」セクションを更新しました。
- 「附録：TISAXスコープ抜粋例」セクションを更新しました。
- 「附録：審査ステータス」セクションを更新しました（「初回審査実施中」ステータスを追加、「フォローアップ審査待ち」ステータスの名称を「フォローアップ待ち」に変更、図41）。
- 「附録：フォルクスワーゲンのレガシー審査」（およびそれへの参照）を削除しました（関連性がなくなったため）。

バージョン2.1.2

- 「貴社の結果スコア」と「最高結果スコア」の間の「乖離」の公式の限界値を25%から30%に修正しました。

バージョン2.1.1

- タイプミスを修正しました。

バージョン2.1

- 「マネージドサービスプロバイダー」のセクションの削除しました。

- TISAX審査目的・ラベルを更新しました（EU一般データ保護規則に基づくデータ保護ラベル、プロトタイプラベルを二つから四つに追加、保護レベルから保護ニーズに名称変更、選択におけるアドバイスを更新）。
- ISA（バージョン4.0から4.1）の変更に伴い更新しました。
- 新たに資料「TISAX簡易グループ審査」（本資料の補遺）について言及しました。
- 拠点名とスコープ名の割り当てに関する提案を追加しました。
- 「登録料」の名称を「料金」に変更しました。
- 代理連絡先に関する推奨事項を追加しました。
- 料金モデルの選択を削除しました。

一番上に戻る。

[1] 先手を打ってTISAXのプロセスを進めることを検討しても良いでしょう。実際にそういった準備を進めている企業も存在します。あらかじめTISAXの審査を受けていれば、開始までの期間を大幅に短縮できるため、TISAXの審査を受けていない競合他社よりも優位に立てる可能性があります。

[2] 「TISAXラベル」は、TISAXプロセスの結果として得られ、審査結果を集約することをコンセプトとしています。詳細はセクション 5.4.14. TISAXラベルをご覧ください。

[3] TISAXに参加する際の登録ステップの大半は、1回のみ必要とされます。審査結果の更新時は、登録データの更新と確認のみ必要となります。

[4] 一般取引条件の変更はENXポータルで公表した上で、登録された連絡先に通知します。

[5] これは、他のすべての追加契約（行動規範など）についても同様です。

[6] 現在、パートナー企業に新しいアクセス権限について自動通知されることはないため、ご注意ください。貴社の審査結果にアクセスできる状態になったら、パートナー企業に通知することをお勧めします。

[7] ドロップダウンリストへの掲載を希望される方は、こちらまでご連絡ください。

[8] 証跡とは、ある要求事項を満たしているという貴社の主張を裏付けるものを指します。証跡は主に文書です。内部文書は必ず証跡として使用されます。

[9] 審査レベル2の審査のための面談は、通常ウェブ会議によって行われます。ご要望の場合は、オンサイトでの面談も可能です。

[10] 簡易グループ審査の理論最小値は3拠点です。

[11] 情報セキュリティマネジメントシステムの改善が必要であることを把握している場合は、最低でも拠点が12か所以上での利用を推奨します。

[12] 数字と文字（8とBなど）の混同を防ぐため、参加企業IDには、一部使用できない文字があります。ただし、一部の古い参加企業IDには「G」の文字が含まれている場合があります。

[13] ISAでこれらのカタログは「モジュール」とも呼ばれています。

[14] のグループ化ボタンをクリックする必要があります。グループ化機能には、Excelの「データ」リボンの「アウトライン」セクションからアクセスできます。

[15] 貴社に同様の審査（ISO 27001など）を実施している審査機関があり、その機関にTISAX審査も実施したいと考えていますか? その場合は、本資料を共有し、TISAX審査機関になるために何が必要かを確認するため、ENX協会に連絡するよう伝えてください。

[16] リストに記載されていない審査機関は、TISAX審査を実施できません。

[17] 審査プロセスを終了すると、TISAXラベルは取得できません。

[18] 実は4種類目として「スコープ拡大審査（Scope extension assessment）」もありますが、これは特殊なケースであるため、詳しくは以下のセクションの附録をご覧ください：セクション 7.10. 附録：スコープ拡大審査。

[19] 正式なオープニングミーティングの詳細な説明は、初回審査でのみ行われます。他のTISAX審査については、審査機関がスケジュールを立てて、ミーティングを実施します。

[20] 審査機関によっては「キックオフミーティング」の用語を、「正式なオープニングミーティング」と同義に使用する場合があります。

[21] 正式なクロージングミーティングの詳細な説明は、初回審査でのみ行われます。その他のTISAX審査については、担当の審査機関がこれらのミーティングの日程と形式を決定します。

[22] 紛争が解決できない場合は、問題をエスカレーションできます。より詳細な情報については、セクション 7.13. 附録：クレーム管理を参照してください。

[23] 審査方法と審査の厳密度に関する詳細は、次を参照してください：セクション 4.3.3.5. 保護ニーズと審査レベル。

[24] 紛争が解決できない場合は、問題をエスカレーションできます。詳細についてはENX協会までお問い合わせください。

[25] 適切な是正措置を定義していても、総合審査結果が「重大な不適合」となる可能性があることに注意してください。対策が即座に効果を発揮しない・できない場合がこれにあてはまります。

[26] もちろん、これは初回審査で不適合が指摘されたケースのみが対象です。審査結果が「適合」であった初回審査については、フォローアップ審査は必要ありません。

[27] 理論的には、初回審査の終了から9か月後となります。

[28] 実は4種類目として「スコープ拡大審査報告書（scope extension assessment report）」もありますが、これは特殊なケースであるため、詳しくは以下のセクションをご覧ください：セクション 7.10. 附録：スコープ拡大審査。

[29] 「TISAX審査報告書」は、すべてのTISAX審査機関に対し、使用が義務付けられたテンプレートに基づいて作成されます。

[30] 「更新」という言葉は誤解を招く可能性があります。TISAXラベルを3年以上維持するには、TISAXのプロセスを再度実施する必要があります。これは、新しい審査スコープの登録から始まります。

[31] TISAXは、参加企業IDの「TISAX公開」リストを管理していません。その理由は、似た社名の取り違え等の「人為的なミス」による、意図しない共有を防止するためです。したがって、パートナー企業の参加企業IDは、必ずパートナー企業に直接連絡して取得してください。

[32] 共有された審査結果は、パートナー企業がENXポータルにログインして、自ら確認する必要があります。新たに共有された審査結果について、パートナー企業へ自動的に通知されることはありません。

[33] この規則は、「TISAX参加規約」（https://enx.com/tisaxgtcen.pdf）に定義されています。

[34] 審査スコープのステ□ータスが「支払い待ち」または「登録済み」の間、「審査関連情報」には、審査スコ□ープの拠点、審査スコ□ープのステ□ータス、審査目的が含まれます。審査結果やTISAXラベルは含まれません。

[35] 「TISAXラベル」とは、審査結果を要約する概念で、TISAXプロセスの出力です。詳細はセクション 5.4.14. TISAXラベルをご覧ください。