ENISA サイバーセキュリティ脅威状況の評価方法

2025 年 8 月

ENISA について

欧州サイバーセキュリティ機関（ENISA）は、欧州全域で高度なサイバーセキュリティの共通レベルを達成することを目的とした、欧州連合（EU）の機関だ。2004 年に設立され、EU サイバーセキュリティ法によって強化された欧州サイバーセキュリティ機関は、EU のサイバー政策に貢献し、サイバーセキュリティ認証制度を通じて ICT 製品、サービス、プロセスの信頼性を高め、加盟国や EU 団体と協力し、欧州が将来のサイバー課題に備える支援を行っている。知識の共有、能力開発、意識向上を通じて、同機関は主要なステークホルダーと協力し、ネットワーク化された経済に対する信頼を強化し、EU のインフラのレジリエンスを高め、最終的にはヨーロッパの社会と市民のデジタルセキュリティを確保している。ENISA およびその活動に関する詳細情報は、www.enisa.europa.eu。 をご覧ください

お問い合わせ

著者へのお問い合わせは、etl@enisa.europa.eu までお願いする。

この報告書に関するメディアからの問い合わせは、press@enisa.europa.eu までお願いする。

編集者

ジャミラ・ブテメール、イリアス・バカティス、イフィゲニア・レラ - ENISA

寄稿者

アポストロス・マラトラス、ラズヴァン・ガブリラ、ステファノ・デ・クレセンツォ - ENISA

法的通知

この出版物は、特に明記されていない限り、ENISA の見解および解釈を反映したものだ。これは、規則 (EU) No 2019/881 に基づく ENISA または ENISA 団体の規制上の義務を保証するものではない。

ENISA は、この出版物またはその内容を変更、更新、または削除する権利を有する。この出版物は情報提供を目的としており、無料でアクセス可能でなければならない。この出版物またはその一部を引用する場合、または使用する場合、ENISA を出典として明示しなければならない。

サードパーティの情報源は、必要に応じて引用する。ENISA は、本出版物で参照されている外部ウェブサイトを含む、外部情報源の内容について一切の責任を負わない。

ENISA またはその代理人として行動するいかなる者も、本出版物に含まれる情報の利用について責任を負わない。

ENISA は、本出版物に関する知的財産権を保有している。

著作権表示

© 欧州サイバーセキュリティ機関（ENISA）、2025

特に明記されていない限り、この文書の再利用は、クリエイティブ・コモンズ・アトリビューション 4.0 インターナショナル (CC BY 4.0) ライセンス (https://creativecommons.org/licenses/by/4.0/) の下で許可されています。これは、適切な出典を明記し、変更点を明示する限り、再利用が許可されることを意味します。

欧州サイバーセキュリティ機関が所有していない要素の使用または複製については、それぞれの権利者に直接許可を求める必要がある場合がある。

ISBN 978-92-9204-719-1、DOI 10.2824/1888892

目次

1.序論 4

1.1CTL の範囲と基本原則 4

2.CTL の方法論 6

2.1 方法論的アプローチの概要 6

2.2 方向性 7

2.2.1CTL の目的を確立する 7

2.2.2 対象者を定義する 7

2.2.3 インテリジェンス要件の定義 8

2.3 収集 9

2.3.1 収集計画を定義する 9

2.3.2 情報源の妥当性確認 10

2.3.3 収集データの入力 11

2.4 処理 12

2.4.1 処理の準備 12

2.4.2 言語処理 12

2.4.3 サイバー脅威の分類 12

2.4.4CTI 枠組み 12

2.4.5 処理済みコンテンツの統合 13

2.4.6 処理済みコンテンツの相関付けと充実 13

2.5 分析と作成 14

2.5.1 分析の準備 14

2.5.2 分析の実施 15

2.5.3CTL の妥当性確認 15

2.5.4 配信媒体の妥当性確認 15

2.5.5 成果物の制作 16

2.6 配布 16

2.6.1 配布の準備 16

2.6.2CTL 成果物の配布 16

2.7 フィードバック 17

2.7.1 フィードバックの受領 17

2.7.2 フィードバックに基づく対応 17

3.今後の作業 18

3.1 自動化された情報処理への移行 18

1. 序論

政策立案者、リスクマネージャー、情報セキュリティ実務者は、状況認識と脅威分析に裏打ちされた、現在の脅威の状況に関する最新かつ正確な情報を必要としている。EU サイバーセキュリティ機関（ENISA）のサイバー脅威の状況（CTL）報告書は、2013 年から毎年発行されている。この報告書は、公開されているデータを使用し、EU の脅威の状況に焦点を当て、観察された脅威エージェント、傾向、攻撃ベクトルに関する独立した見解を提供している。

ENISA は、その専門知識を活用し、この活動を強化することで、政策立案や意思決定に必要な関連情報をステークホルダーに提供するとともに、サイバーセキュリティの専門コミュニティの知識と情報を増進し、サイバーセキュリティの課題について確固たる理解を確立することを目指している。絶えず変化し続けるサイバー脅威の状況を把握することで、ENISA のサイバー脅威分析活動は付加価値を生み出している。 中長期的な傾向を識別することで、これらの取り組みは状況認識と将来の困難を予測する能力の向上に貢献している。

ENISA は、明確で公開されている方法論に基づいて、脅威の状況に関する的を絞った報告、勧告、分析、その他の措置を提供することを目指している。ENISA CTL 方法論の確立により、ENISA は、水平的、主題別、および分野別のサイバーセキュリティ脅威の状況に関する透明かつ体系的な情報の提供のための基準を設定することを目指している。この方法論的枠組みの全体的な焦点は、CTL を構成するプロセス、手法、利害関係者、ツール、および内容的な要素の特定と定義にある。

ENISA 脅威状況報告書 2021[1] の改訂版および ENISA 脅威状況報告書 2022 の方法論[2] に従い、ENISA はこの取り組みのさらなる発展と文書化を進めている。この更新された方法論は、文書をより実用的なものにし、CTL 作成プロセスの各段階に関する詳細情報を提供することを目的としている。

1.1 CTL の範囲と基本原則

この手法は、ENISA の年次（ENISA Threat Landscape、ETL）、セクター別（STL）、およびその他のテーマ別（TTL）の脅威状況、ならびに状況認識を目的として ENISA の脅威分析サービス（TAS）が作成するその他すべての報告書に適用される。

CTL をドラフトする際には、以下の考慮事項および原則が重要であると考える。

- **正確性：**報告書の正確性は、収集、処理、相関分析、および分析された情報に依存する。TAS チームは、情報入力戦略を検討し、情報源の正確性、関連性、網羅性、提示形式の種類（例：報告書または機械可読形式）、および重点分野（例：セクター、EU 被害者分析、攻撃者関連性、脅威グループ、脅威の種類）に基づいて情報源の品質を評価する。これは、ENISA がセクター別脅威状況（STL）を公開する場合にも特に重要だ。その場合は、情報入力戦略を適宜改良する必要があるからだ。さらに、報告書の正確性は、分析の品質およびそこから導き出された推論に直接影響される。
- **適時性：**時間は、特に報告書が戦術的または運用上の情報も記載している場合、その実行可能性に影響を与える。報告書の発行頻度は、その範囲、重要度、および対応すべき利害関係者の要件によって決まる。これらの規準に基づき、報告書は、発生時、毎月、四半期、半年、または毎年発行することができる。
- **実行可能性：**CTL は、サイバー領域における脅威に対するステークホルダーの認識を高め、意思決定プロセスを支援し、サイバー脅威に対する予防的、積極的、事後対応的な姿勢を改善すべきだ。これは、戦略レベルと運用レベルの両方で達成できる。ENISA は、運用レベルと戦略レベルの両方で、さまざまなカテゴリーの脅威に関するサイバーセキュリティの推奨事項を報告書に記載することで、CTL のこの側面に重点を置

[1] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

いている。運用面については、特定の脅威の予防および対応のための緩和戦略の策定の基礎を提供することでカバーしている。戦略的な高レベルな側面については、脅威の動向に関する年次レビューでカバーしている。テーマ別またはセクター別の脅威の動向を報告する場合、提案される対策は、分析対象のセクターまたはテーマの特性を反映したものとなる。

2. CTL 方法論

2.1 方法論的アプローチの概要

CTL の生産手法は、以下の質問に対応することを目的としている：

- どのような種類のデータが収集されるか？
- 対象者は誰か？
- データはどのように収集され、処理されるか？
- データはどのように分析されるか？
- CTL の構造（構成要素と内容）はどのようなものか？
- CTL はどのように配布されますか？
- フィードバックの収集プロセスは？

この方法論の目的のため、ENISA のアプローチは、情報の収集と処理、分析の実施、主要な利害関係者との対話、CTL の改善に関する明確な提言の提供から始まる協力に重点を置いている。

図 *1* に示すように、ENISA の社内アナリストが、報告書のコンテンツを継続的に評価している。以下の図は、CTL 手法の開発プロセスと、その各ステップで重点的に取り組む分野を示す。このプロセスには、脅威の状況に関する要件（範囲、対象読者）の計画、社内外の利害関係者からの情報源の種類と形式の識別および妥当性確認が含まれる。収集したデータを処理・分析し、最終的な報告書草案を ENISA の関連ステークホルダーと検討・協議した後、サイバーセキュリティの脅威の全体像を確定し、公表する。

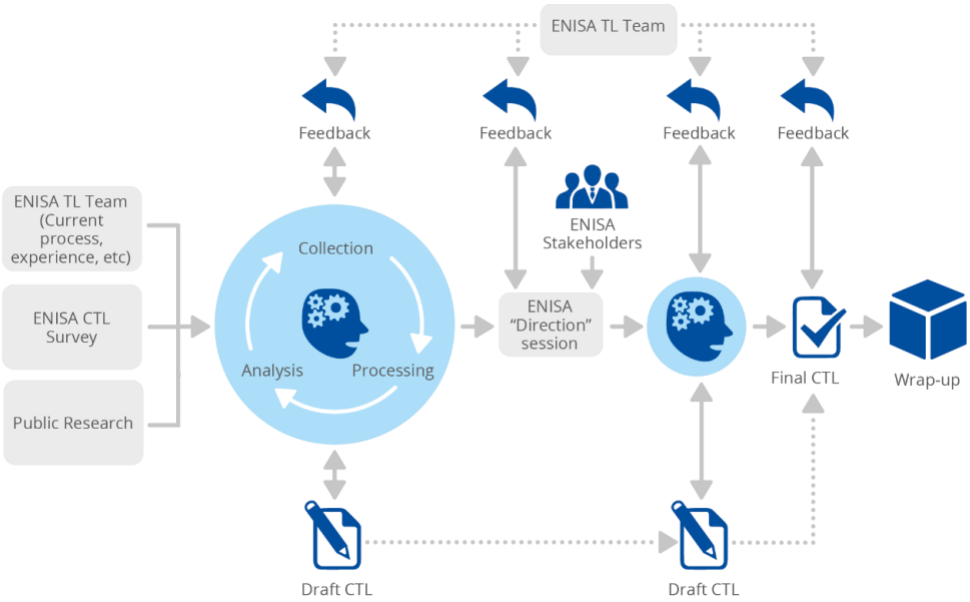

図 1：ENISA CTL 方法論の全体像

CTL は、過去および現在の出来事に関する情報や分析を表しており、読者は、直面する可能性が高い**脅威を文脈に沿って理解することができる**。CTL にどのような内容を含めるべきか、どのような分類法を使用すべきかを理解するには、まず CTL の作成方法を理解する必要がある。インテリジェンス主導のアプローチでは、インテリジェンス・コミュニティの実用的かつ有用な教訓を CTL の作成に採用する。例えば、作成者は、読者や関係者が CTL から理解したいこと（インテリジェンス要件など）を、それぞれの答え（分析結果など）に明確に翻訳することができる。

以下の図は、ENISA におけるこのようなプロセスの高レベルな構造を、インテリジェンスライフサイクル[3] に基づいて詳細に示したものだ。

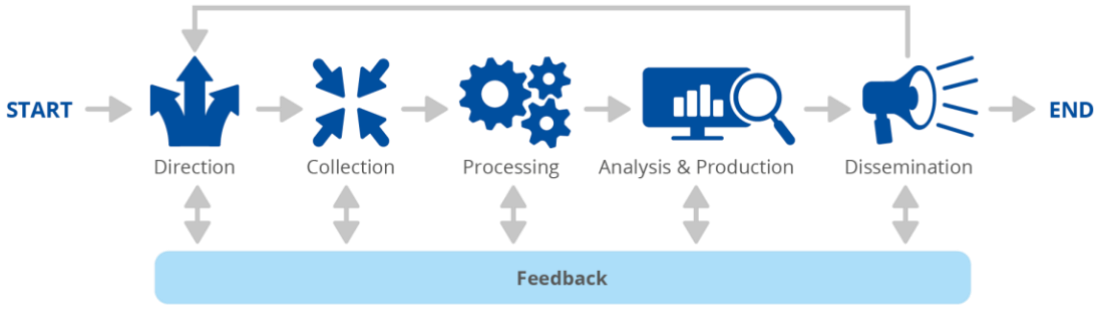

図 2：ENISA CTL 作成プロセスの概要

以降の章では、上記の図で強調された各要素を詳細に説明し、各章で ENISA CTL の文脈において方法論がどのように満たされているかを明示的に参照する。

2.2 方向性

この最初のステップの目的は、CTL の目的、範囲、および対象者を確立することです。これらの要件を確立し、**ENISA の法的権限**を考慮することで、報告書に必要な情報要件、必要な情報の種類、情報を提供する利害関係者、および報告書の対象者を定義することができます。

図 3：CTL の方向性定義プロセス

2.2.1 CTL の目的の確立

すべての CTL は、以下の目的のために**脅威分析の強化**に貢献する情報を共有することを目指している。

- EU レベルでの正確なサイバー脅威の概要の提供

- 意識向上、

- リスクマネジメントへの貢献

- 研修、演習、能力開発の機会の識別 - 戦略的意思決定への貢献 - 政策立案への貢献

2.2.2 対象者を定義する

CTL の目的が確立され、成果物が委託されたら、対象者を検討する。CTL の対象者は、以下の通りとする。

- **戦略的**：脅威に関連する動向に関する情報で、高レベルの戦略を推進するために活用できる。セキュリティ戦略担当者や他の上級意思決定者が利用し、経営陣レベルまで共有される場合もある。
- **戦術的**：侵入セットが悪意のあるサイバー活動を行うために使用する最も一般的な戦術、手法、手順（TTP）に関する情報。この情報は通常、アーキテクト（ネットワーク、システム、製品、プロセス）、セキュリティ管理責任者、人事関連担当者、レッドチーム、ブルーチーム、パープルチーム、インシデント対応者、脅威ハンター、デジタルフォレンジック担当者によって利用される。

[3]https://filigran.io/understanding-cyber-threat-intelligence-lifecycle/

- **運用**：差し迫った攻撃の前兆や兆候に関する情報。通常、脅威環境を監視して生成され、可能であればコンテキスト化され、インシデント対応担当者やセキュリティマネージャーなどの上級セキュリティスタッフによって利用される。

CTL の内容および共有またはマークのレベルは、定義された対象者によって異なり、その逆も同様であるため、対象者を明確に定義することの重要性を強調することが不可欠だ。戦略的な対象者には、要約および主要な調査アセスメントへの参照を提供すべきだ。さらに、CTL の各セクションは、異なるレベルで取り扱うべきだ。例えば、検出エンジニアがより効果的に調査できるように、TTP[4] への参照をグラフィカルに詳細に説明した別個の附属書を用意することができる。文書構造は、対象読者へのシグナルを送るためにも使用できる。したがって、CTL の構造と分析の深さを対象読者のニーズに合わせて調整し、その選択を明示的に示すことで、文書の関連性、実行可能性、および影響力が向上する。

2.2.3 インテリジェンス要件の定義

インテリジェンス要件とは、情報収集またはインテリジェンスの生成が必要とされる、一般的または特定のあらゆる対象を意味する。[5]

インテリジェンス報告書を作成するために必要なもの（生産要件）と、生産要件を満たすために収集する必要がある情報（インテリジェンス要件）には区別がある。生産要件はステークホルダーから提示され、より抽象的な質問の形をとる。この生産要件は、複数の インテリジェンス要件に翻訳され、主要な質問を生産チームが回答可能な個別の要素に分解される。

ENISA の主な作成要件は、EU 加盟国（EU MS）**が直面するサイバー脅威だ**。

情報要件には、特に、NIS2 セクターを標的とした、国家と関連のある侵入セット、サイバー犯罪グループ、およびハクティビストによるサイバー攻撃[6] が含まれる。収集した各インシデントまたはイベントについて、以下の質問に対処する必要がある。

- このインシデントは、少なくとも 1 つの EU 加盟国を標的としているか、または影響を与えているか？
- これは国境を越えたインシデントか？
- どのセクターが影響を受けているか？
- このインシデントの影響を受けるシステムおよび/または資産はどれか？
- このインシデントの影響は？
- 関連する侵入セットは攻撃をどのように実行したか（TTPs）？
- 侵入セットの推定動機は？
- このインシデントに関連する特定の状況はあるか？
- この脅威に対抗するために適用できる緩和策は？

収集したインシデントを分析することで、傾向やアセスメントを導き出し、それを脅威状況レポートに統合して記載する。

[4] https://www.sekoia.io/en/glossary/ttp-cyber-tactics-techniques-and-procedures/

[5] https://intel471.com/blog/cyber-threat-intelligence-requirements-what-are-they-what-are-they-for-and-how-do-they-fit-in-the

[6] 不正なアクセスや悪意のある行動により、デジタル資産、システム、またはネットワークを妨害、侵害、または損傷する意図的な行為（ENISA）

収集したデータを考慮すべき期間も定義する。通常、これはデータを収集する期間を指定するものだ。なお、CTL のドラフト作成のために選択、分析されたインシデントの大部分は、定義された期間に発生したものだが、この期間に報告された、それ以前に発生したインシデントが CTL に含まれる場合もある。

特定のイベントが EU の脅威状況と関連性があるかどうかを評価するために、ENISA のアナリストは、EU 関連性スコアというシンプルなスコアリングシステムを使用している。このシステムは、以下の値で特徴付けられる。

高：欧州連合のサイバー脅威に対するレジリエンス、および欧州の市民や企業向けのサービスやデジタルツールの信頼性および信頼性に重大な影響を及ぼす可能性のあるサイバーセキュリティイベント。

中：欧州連合のサイバー脅威に対するレジリエンス、および欧州の市民や企業向けのサービスやデジタルツールの信頼性および信頼性に中程度の影響を与える可能性のあるサイバーセキュリティイベント。

低：欧州連合のサイバー脅威に対するレジリエンス、および欧州の市民や企業向けのサービスやデジタルツールの信頼性および信頼性に軽微な影響またはまったく影響を与えないサイバーセキュリティイベント。

2.3 収集

収集プロセスには、収集計画、特定された情報源の継続的な評価など、正確な実用的な情報を確保するためのさまざまな業務の調整が含まれる[7]。データは、複数の情報源（公開報告書、購読サービス、EU 加盟国および民間パートナーが ENISA と共有する情報など）から収集される。この方法論のステップでは、データ収集計画と情報源の評価を行う。また、次の段階で処理され、実用的な情報に変換される前に、情報源から実際にデータを収集することも含まれる。

図 4：CTL データ収集プロセス

2.3.1 収集計画の定義

プロセスの次のステップは、情報要件を満たすために収集する必要のある情報を識別および分類し、その情報を収集する場所を特定して、データ収集要件を明確に定義することだ。これは、オープンソース情報、サイバー脅威情報（CTI）プロバイダ、知識共有グループ、EU 加盟国や民間パートナーが共有する情報など、外部からの収集である場合もある。

このプロセスが実践でどのように機能するかの例は、以下の表に示されている。

インテリジェンス要件	収集要件
報告期間において、EU 組織に対して最も多く展開されたランサムウェアの亜種は何ですか？	• ランサムウェアグループを参照してくださいデータ漏洩サイト（DLS） • ENISA の知識ベースを参照する • ENISA の利害関係者に相談する

表 1：データ収集要件の定義例

データ収集要件は通常、インテリジェンス収集計画（ICP）に格納され、すべてのインテリジェンス要件を列挙し、ソースの種類にマッピングし、TAS アナリストが毎日データを収集できるようにする。表 2 に示されるような指標的なインテリジェンス収集計画が提示されている。このリストにより、アナリストは重複、欠落、または不一致を特定し、適切に対応することができる。データに基づく分析には、スキルと関連ツールおよびサービスが必要だ。2025 年 1 月以来、ENISA

[7] https://www.first.org/global/sigs/cti/curriculum/pir

CTL は ENISA 脅威分析サービス (TAS) のプロセスおよびカタログに統合され、特定の時点における EU のサイバー脅威の状況の正確性を確保するため、データ収集段階に重点が置かれている。

ENISA の daily data collection は、生産要件、インテリジェンス要件、および CTL の時間枠に基づいて精緻化される。データ収集は反復的なタスクだが、情報資産が故障した場合に、確立された収集要件を満たすことができる重複または補完的な資産（ ）で置き換えられるよう、適切なレベルの継続的な評価と冗長性を確保することが不可欠だ。[8] ほとんどのソースは、オープンソースインテリジェンス（OSINT）に基づいており、理論的には、インテリジェンスの目的や収集要件を満たすために、公開されているデータから収集、処理され、適切な対象者にタイムリーに配信されるインテリジェンスと定義されている[9] 。情報過多を回避し、CTL にとってこの豊富な情報の価値を最大限に引き出すためには、ソースの正確性および関連性を構造的に継続的にアセスメントすることが、優れた収集計画の策定に役立つ。

CTL の方向性に基づき、必要な情報源の種類を定義する。異なる種類のデータには、以下の特徴がある。

- **オペレーショナル** – 侵害の指標（IoCs）などの技術的な詳細を含む傾向がある。
- **戦術的** – 特定のインシデント、マルウェア、または侵入セットに関連する戦術、手法、手順 (TTP) に関する情報が含まれる。
- **戦略的** – 主に PESTEL 手法[10] に基づいて、動機、関連する脅威アクター、コンテキスト情報を評価したもの。

ソース	データの種類	収集時期
民間ベンダー	運用、戦術	通年
機関関係者	運用、戦略	通年
ソーシャルメディア	業務、戦略、戦術	通年
脆弱性の開示	運用、戦術	通年
調査	運用、戦略、戦術	通年

表 2：TAS 指標情報収集計画

2.3.2 情報源の妥当性確認

欧州連合のサイバーセキュリティのエコシステムは複雑かつ多層的で、司法・内務、デジタル単一市場、研究政策など、さまざまな国家および EU の政策分野にまたがっている[11] 。さらに、EU は、さまざまな協力形態で構築された官民連携に多額の投資を行っている。この複雑な構造、および視点や可視性の違いは、確かにいくつかの課題をもたらすものの、**CTL の観点からは、さまざまな信頼できる情報源から情報収集を行うことができるというユニークな機会も提供している。**

内部情報源には、情報要件への情報を提供する内部の人員、プロセス、技術資産など、あらゆるものが含まれる。これは、ENISA が状況認識および脅威情報レポートを作成するために CTL を作成する場合に、主に重要になる。

[8] J. AMMONS、「MITRE ATT&CK を使用して脅威の検知能力を向上させる方法」Gartner (2021)。

[9] https://www.bercynumerique.finances.gouv.fr/roso-osint-lexploitation-des-sources-ouvertes-sur-internet

[10] https://wikis.ec.europa.eu/spaces/ExactExternalWiki/pages/50109048/Context+analysis+–+PESTEL

[11] X.、「効果的な EU サイバーセキュリティ政策の課題」、欧州会計監査院 (2019)

機関情報源 – サイバーセキュリティ分野における EU の数多くの機関および ENISA との想定される相互関係を表す。これには、CSIRT ネットワーク（CERT-EU を含む）、EUROPOL/EC3、EEAS の STRATCOM、ネットワークおよび情報セキュリティ指令協力グループ（NIS-CG）などが含まれるが、これらに限定されない。

外部情報源には、ENISA が外部から収集したあらゆる情報が含まれる。例えば、技術指標リポジトリ、ソーシャルメディア、フォーラムなどだ。外部情報源は、オープンソースとクローズドソースに分類できる。外部情報源は、以下を提供する。

- **生データまたは処理済みデータ**：データソースは、大きく異なる場合がある。例えば、要求に応じて出力を提供するデータプロバイダ、手動でクエリを実行できるツール、手動でアクセスして操作する必要があるフォーラムなどが挙げられる。
- **自ら収集および/または処理したデータに基づく情報**：エンドポイントベンダーなど、広範なテレメトリにアクセスできるプロバイダは、定期的に分析を行い、潜在顧客や顧客にとって興味深い洞察を確立している。この情報は定期報告書として公開されており、その一部は CTL 自体となっている。
- **収集、処理、分析、配信されたデータと情報に基づく完成したインテリジェンス製品**：情報からインテリジェンスへの移行は、少なくとも概念的には、それを生産する方法を知る企業によって主に実施される。

文脈化は、次のセクションで説明するソースの信頼レベルと共に、収集時に実施すべきだ。文脈化は通常、報告書の目的と方向性から導かれる。

2.3.2.1 ソースの信頼性レベル

データ収集のこの段階では、情報源の信頼度を確立する必要があります。これは、情報源の信頼性と情報の信頼性を表す、アドミラルティシステムの 2 文字表記（[12]）に基づいています。

情報源の信頼性	情報の信頼性
A - 完全に信頼できる	1 - 他の情報源によって確認済み
B - 通常信頼できる	2 - おそらく真実
C - かなり信頼できる	3 - 可能性あり
D - 通常信頼できない	4 - 疑わしい
E – 信頼できない	5 - 不可能
F - 信頼性を判断できない	6 - 真偽を判断できない

2.3.3 入力データの収集

TAS アナリストは、毎日データを収集し、ソースの信頼度と EU 関連性スコアに基づいて、前のフェーズで設定された要件に従って初期選別を行い、選択されたデータの処理に進む。

[12]https://www.threat-intelligence.eu/methodologies/#the-admiralty-scale-also-called-the-nato-system

2.4 処理

データ処理は、取得したデータを人間中心の分析やインテリジェンスの出力に適した形式に変換するプロセスだ。この段階では、**収集したデータを、TAS アナリストがより効率的にレポートやアセスメントを作成するために使用できる形式に変換する。**この処理には、収集したデータの半手動による相関分析も含まれる。

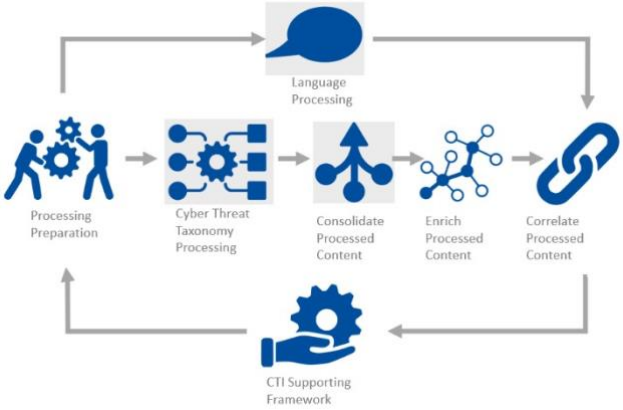

図 4：CTL データ処理プロセス

2.4.1 処理の準備

収集したすべての情報のデータ処理は、定義された優先情報要件に従って準備および計画される。CTL の処理段階と分析段階は密接に関連しており、分析段階から処理段階にフィードバックを行う必要がある。

2.4.2 言語処理

CTL を開発する際、アナリストは使用する言語を決定する必要がある。これは単純に聞こえるかもしれないが、対応が必要な課題を引き起こす可能性がある。たとえば、公開されているオープンソースの脅威レポートから英語でレポートを収集する場合、他の言語で書かれた情報源が除外されるリスクがある。同様に、さまざまな言語の一次情報源を監視する場合、分析のニーズと目的に合わせて、それらを単一の首尾一貫した言語に処理する必要がある。**CTL は、ヨーロッパ言語および英語の情報源を使用し、英語で公開されている**[13] 。

2.4.3 サイバー脅威の分類

CTL を提供するための方法論のもう 1 つの重要な要素は、サイバー脅威のエコシステムを構造化するために使用する分類である「コンテンツ分類」の定義だ。これは、収集したデータの整理方法や履歴データセットの作成方法を決定するため、処理に不可欠だ。この段階では、信頼性が高く一貫性のある出力を生成するために、一貫性のある分類と枠組みを持つことが非常に重要であることがわかる。

2021 年 3 月、ENISA は、ステークホルダーの要件やニーズを収集し、ENISA の年次 CTL の改善を目的とした調査を実施した。この 調査の結果、関連ステークホルダーから、追加の分類を検討すべきという提案がいくつか寄せられた。

ENISA 脅威分類：2016 年に初めて策定され（[14] ）、2022 年に更新された（[15] ）、ENISA 脅威分類は、CTL の指針および ENISA 内で参照される脅威の標準となった。**この分類は、より成熟した実用的な枠組みを開発することを目的として、現在改訂中だ。**

2.4.4 CTI 枠組み

現在、サイバー脅威を構造化するための CTI フレームワークがいくつか存在している。それぞれ重点分野が異なり、したがって具体的な用途も異なるが、最終的には、使用される脅威分類および CTL プロセスの指示および計画段階で設定された要件に基づいて、情報を効率的に収集し、整理することができる。TAS レポート（ENISA CTL を含む）の場合、このプロセスの一部は、データや情報を共通言語（STIX2.1）に翻訳し、大量のデータを実用可能な形式に変換するか、MITRE ATT&CK（® ）に従って TTP（戦術、技術、手順）データセットを構造化することに焦点を当てている。

---

[13] https://style-guide.europa.eu/en/content/-/isg/topic?identifier=part-four-publications-in-a-specific-language

[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[15] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

- **OASIS サイバー脅威インテリジェンス (CTI) STIX™[16]** ：OASIS サイバー脅威インテリジェンステクニカル委員会 (OASIS CTI TC) によって開発された脅威インテリジェンスの表現および共有の標準規格は、構造化脅威情報表現 (STIX™) およびその対応リレーメカニズムである信頼された自動情報交換 (TAXII) だ。2021 年、STIX™ は OASIS 標準としてリリースされた。STIX™ は、サイバー脅威および観測可能な情報を記述するオントロジーおよび言語だ。これにより、組織はサイバー脅威インテリジェンスを一貫した、機械で読み取り可能な形式で共有することができ、発生の可能性が最も高いコンピュータベースの攻撃をよりよく理解し、それらの攻撃をより迅速かつ効果的に予測および対応することが可能になる。STIX™ は、脅威インテリジェンスのさまざまなプラットフォームの表現の基盤となるフォーマットに影響を与えている。
- **STIX 2.1 は、MITRE ATT&CK® などの他の枠組みも統合している。**これは、現実の世界での観察結果に基づく、敵の戦術や手法に関する世界中からアクセス可能な知識ベースだ。ATT&CK 知識ベースは、民間企業、政府、サイバーセキュリティ製品およびサービスコミュニティにおける、特定の脅威モデルや方法論の開発の基礎として活用されている。
- **サイバーキルチェーン®[17]** ：ロッキード・マーティン社が開発したサイバーキルチェーン® 枠組みは、サイバー侵入に関連する活動を識別および防止するためのインテリジェンス主導の防御® モデルの一部だ。このモデルは、敵が目標を達成するために完了しなければならないことを識別する。サイバーキルチェーンの 7 つのステップ® は、攻撃の可視性を高め、アナリストの敵の戦術、手法、手順に関する理解を深める。
- **欧州連合脆弱性データベース（EUVD）[18] ：**EUVD は、加盟国間の脆弱性報告の断片化に対する懸念の高まりに対応し、NIS2 指令の遵守を支援するために、2025 年に欧州連合によって設立された。EUVD の使命は、EU のデジタルインフラストラクチャに影響を与えるサイバーセキュリティの脆弱性を識別、定義、およびカタログ化することだ。各脆弱性には、一貫した追跡と国境を越えた連携を確保するために、固有の EUVD レコードが割り当てられる。レコードは、各国の CERT、信頼できる研究者、および業界パートナーによって提供される。各エントリには、深刻度、セクターへの影響、緩和策の参考情報、および MITRE CVE® プログラム[19] に基づく関連 CVE へのリンクが含まれる。

以下の注意事項を考慮してください。

- **単一の枠組みに依存することによる影響に注意してください。**CTL 全体を構築するために単一の枠組みを選択すると、コンテンツが構造化されているため、防御担当者が即座に対応できるなど、大きなメリットがある場合があります。一方、その枠組みの対象者以外には関連性がないため、適用範囲が狭くなるという欠点もあります。
- **使用する枠組みを再検討する。**選択した枠組みが、CTL の方向性および計画段階で設定した目的および目標に適合しているかどうかを再評価することは、議論の余地があり、困難ですが、必要な作業です。

2.4.5 処理済みコンテンツの統合

処理済みコンテンツの統合とは、利用可能なすべての処理済みデータをより効率的で利用しやすい形式にまとめることだ。これには、純粋なデータの形式変換、言語翻訳、データの関連性や信頼性の評価などが含まれる。データ統合は、データセットの正確性も確保する。

2.4.6 処理済みコンテンツの相関分析と充実

相関とは、可能であればデータポイントを結び付けて、データセット間の関係やパターンを識別することだ。相関により、分析の精度が向上し、脅威活動の包括的な理解が促進される。

---

[16]https://www.oasis-open.org/committees/cti

[17]https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[18]https://euvd.enisa.europa.eu/homepage

[19]https://cve.mitre.org/

エンリッチメントとは、地政学的コンテキスト、報告されたインシデントの考えられる要因、サイバー攻撃の評価された目的など、関連するコンテキスト情報を追加して、処理されたデータを強化することだ。このステップは、孤立した指標やインシデントを意味のあるインテリジェンスに変換し、関連性と有用性の両方を向上させる。

2.5 分析と作成

分析および作成段階では、CTL チームは要件セクションで提起された質問への回答を試みます。さらに、チームは、ENISA の過去の推奨事項やその他の情報源に基づいて、推奨事項の作成に利用できる可能性のあるギャップを識別します。**このステップでは、ETL 編集チームが専門家による分析を行い、収集した情報に基づいて有意義なアセスメントを提供できるようにします**。これらのアセスメントに基づいて、ETL は実行可能な推奨事項とサイバーセキュリティ対策を提供します。

図 5：CTL データ分析および制作プロセス

2.5.1 分析の準備

分析には、手動分析、自動分析、自動分析と手動分析の混合など、さまざまな手法を用いることができる。手動分析では、通常、複数のチームがデータセットを検証し、評価を行う。

CTL のドラフトを作成する際には、構造化分析手法（SAT）の適用が非常に有用であることがわかるだろう[20] 。SAT の目的は、CTL のアナリストや開発者が構造化された方法で思考を構築・拡大し、バイアスを取り除くことで評価を進め、情報分析の品質を向上させ、分析結果の信頼性を高めることである。

ENISA のアナリストは、さまざまな手法および分析手法を採用しているが、これらは、使用される分析手法の性質および利用可能なデータのタイプに基づいて、4 つの大きなカテゴリーに分類することができる。すなわち、専門家の判断のみ、構造化分析、準定量分析、および経験的分析である[21] 。入手可能なデータに応じて、CTL のドラフト作成時には、これらのカテゴリーの 2 つ以上の手法を併用することができる。現在、ETL は、構造化された分析手法と、批判的思考および専門家の推論を伴う、いわゆる「伝統的な分析」である専門家の判断のみに基づいている。

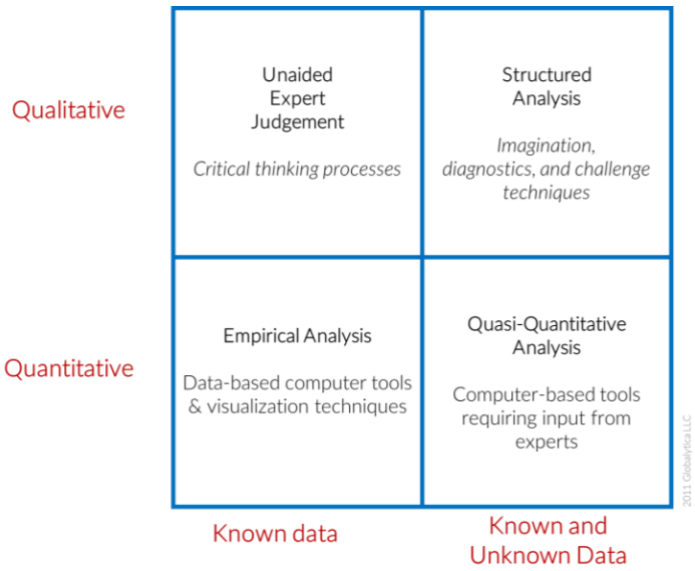

図 6：分析アプローチ

[20]Heuer and Pherson, Structured Analytic Techniques for Intelligence Analysis, 2019

[21]『マスター・シンカーの 5 つの習慣』によると、

2.5.2 分析の実施

[22]分析の準備段階で述べたように、分析の実施には、手動分析、自動分析、あるいはハイブリッドモードのような自動分析と手動分析の混合など、さまざまな方法論がある。構造化分析手法（SAT）を適用する場合、アナリストは、自分の考え方を直感的に考え、特定の技術が必要かどうか、出力をどのように視覚化するかを考える。

分析中に直面する課題としては、収集したデータや情報の信頼性の欠如、複数の作成者や専門家が関与している、信頼性の高いコンテンツや統計をドラフトする必要がある、などが挙げられる。この点に関しては、以下の点を考慮する必要がある。

- **アセスメントの確認：**重要なアセスメントを確立し、それを疑問視すべきタイミングを理解する。
- **代替案の検討：**すべての事象に対して代替説明や仮説を検討する；
- **矛盾を考慮する：**作業仮説を迅速に破棄したり、矛盾に対処したりするのに十分な根拠となる矛盾したデータを探します。
- **主要な要因を検討する：**発生した事象や発生しそうな事象を最もよく説明する主要な要因に焦点を当てる。
- **文脈に焦点を当てる：**ステークホルダーのニーズを予測し、分析が行われる包括的な文脈を理解する。

2.5.3 CTL の妥当性確認

CTL 報告書は、公開して関係者に配布する前に、妥当性を確認する必要がある。妥当性の確認とは、レビュー、フィードバック、コメント、微調整を行うことを意味する。このようにして、CTL の内容が正確かつ適切であることを確認する。

2.5.4 普及手段の妥当性確認

CTL を配布するために使用できる媒体はさまざまです。これは、初期の方向性決定段階で定義する必要があります。この段階では、配布媒体が目的に適しているかどうかを妥当性確認する必要があります。例えば、CTL は、当社のウェブサイトからのダウンロード機能、専用の対話型ウェブサイトの開設、またはソーシャルメディアへの主要調査結果の直接掲載などを通じて配信することができます。この方法論では、CTI のプレゼンテーション形式を、テキスト（散文文書）と機械可読の 2 つの大カテゴリーに識別しています。

テキスト形式

テキスト形式の CTL に関しては、参照用（半標準化された）プレゼンテーションまたは出力テンプレートの導入が不可欠だ。参照用テンプレートには、文章構成の一貫性、反復的なプロセスの半標準化など、いくつかの利点がある。さらに、出力テンプレートは、ステークホルダーの要件、および の作成者、この場合は ENISA が伝えたいメッセージ（ステークホルダーの質問に対する回答）に基づいて設計される。その結果、プレゼンテーションまたは出力テンプレートは、情報収集および分析のプロセスに影響を与え、またそのプロセスによって影響を受ける。例えば、参照テンプレートは、収集、処理、分析すべき情報、そして最終的にその表現方法を推測する。2025 年には、CTL テンプレートにいくつかの変更が加えられる予定だ。

機械可読形式

機械可読表現フォーマットは、CTI を運用し、共有するための手段を防御者に提供する。防御者は、専用のソフトウェアを使用して、機械可読フォーマットにより状況認識と CTI の配信速度を向上させ、機械指向の自動処理（収集、正規化、相関）および分析を可能にする。このようなフォーマットおよびデータや情報を収集、処理、分析するための対応するソフトウェア（脅威インテリジェンスプラットフォーム）は、多くの場合、他の技術ソリューションと統合され、追

[22]著者 Richards J. Heuer、Richards J. Heuer Jr.、Randolph H. Pherson、出版社 CQ Press、2010 年、ISBN 1608710181、9781608710188

加の脅威コンテキストを導き出し、防御コンポーネントや人間エージェントに、攻撃の検知、防止、緩和に関する情報をシームレスに提供します。さらに、CTI を機械可読フォーマットで表現するための標準化されたアプローチにより、相互運用性が実現し、防御担当者は組織や地理的な境界を越えて、よりシームレスにインテリジェンスを共有および利用することが可能になります。現在、CTL はテキスト形式（PDF）で公開されており、分析結果を視覚的に表現したインフォグラフィックで充実している。

2.5.5 成果物の作成

分析が完了すると、その結果が文書化され、最終的な成果物が作成される。これにより、収集および分析後に、結果が特定の構造[23] で保存される成果物が生成される。CTL を作成するために最終的なテキストを編集する前に

- 各脅威に関するテキストを要約し、1 つまたは複数の文書に統合する必要があります；
- 文書は、内部レビュー、専門家グループレビュー、管理承認、校正を含むレビュープロセスを経る必要がある。
- 最終編集が行われ、その後公開される。

2.6 配布

情報分析サイクルの「情報分析」の段階では、収集した情報を分析し、CTL 報告書を作成する。分析とドラフト作成が完了したら、CTL 報告書を適切な関係者に配布する。通常、関係者の要件に応じて、報告書、説明会、ブログ記事、E メール、ソーシャルメディア、デジタル転送や専用の脅威情報プラットフォームを利用した機械可読フィードの共有、説明会やプレゼンテーションなど、公開または非公開のチャネルを通じて情報を配信することができる。

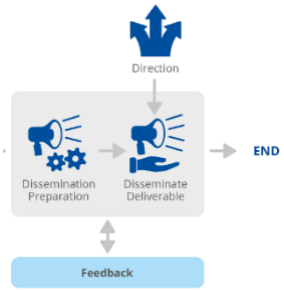

図 7：CTL の配布プロセス

2.6.1 拡散の準備

この段階では、対象とするオーディエンスとの相互作用のモデルを選択する必要があります。CTL オーディエンスとの相互作用には、プッシュ、プル、インタラクティブの 3 つのモデルがあります。すべてのモデルには異なる価値があるため、CTL の要件、オーディエンス、および目的に合わせて選択する必要があります。

2.6.2 CTL 成果物の配信

これは、議論されたパラメーターに基づき、以前のステップで決定された内容に基づいて CTL 報告書を実際に配布する段階だ。CTI コミュニティとの連携は有益であり、ENISA のウェブサイト[24] への公開に加え、ソーシャルチャネル（例：X[25] 、LinkedIn[26] ）やその他のコミュニティエンゲージメント手段を活用することが推奨される。さらに、このプロセス段階は、CTL の普及後、異なるステークホルダーからフィードバック、コメント、観察結果、考察、アイデアを収集し、CTL の改善に反映させることで、CTL の方向性や計画段階にも貢献する可能性がある。フィードバックの収集方法は、CTL の普及手段に応じて異なる可能性がある。

[23]現在の ETL レポート構造、ENISA.docx

[24]https://www.enisa.europa.eu/topics/cyber-threats

[25]https://x.com/enisa_eu

[26]https://www.linkedin.com/company/european-union-agency-for-cybersecurity-enisa

2.7 フィードバック

CTL を改善するには、受け取ったフィードバックを収集し、それに基づいて行動することが不可欠だ。フィードバックは、CTL の内容（方向性、データ収集、分析方法）や形式について言及する場合がある。受け取ったフィードバックは、その CTL の当初の目的を念頭に置いて処理し、CTL 開発チームはそれに応じて行動すべきだ。さまざまな CTL 対象者の個々のニーズを明確かつ詳細に把握することは、継続的なフィードバックループを構築することで実現できる。CTL 開発ライフサイクルのすべての段階を通じて、ステークホルダーとのフィードバックのコミュニケーションプロセスを継続的に維持することが、CTL の成功の鍵となる。

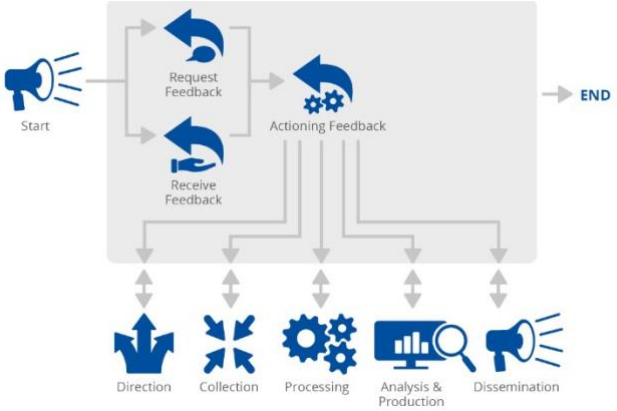

図 8：CTL フィードバックの収集プロセス

2.7.1 フィードバックの収集

フィードバックを求める方法はさまざまです。CTL に関するフィードバックは、提供されたメールアドレス、アンケート、ソーシャルメディア、または直接、継続的に受け取ることができます。フィードバックを提供している「誰」を理解することに加えて、できるだけ多くのフィードバックを収集することが常に重要です。

「誰が」フィードバックを提供しているかを把握するだけでなく、できるだけ多くのフィードバックを収集することが常に重要だ。時には、ごくわずかな提案が、長期的な改善につながることもある。

2.7.2 フィードバックの対応

フィードバックへの対応は、受け取ったコメントを採用した後に実施する措置を決定することであるため、おそらく最も重要なステップだ。定期的または臨時に受け取ったフィードバックは、CTL チームによる事前の処理が必要であるため、すぐに対応することはできない。これには時間がかかり、その時間は制作リソースの見積もりには含まれていない場合もある。

収集したフィードバックへの対応をさらに改善するには、その提供者をより深く理解することが重要だ。これには、CTL の視聴者だけでなく、利害関係者も含まれる。より詳細な理解を持つことで、対応すべきフィードバックと無視すべきフィードバックを、意識的に選択することができる。フィードバックが処理されたら、その件について決定権のある関係者に提案を行い、改善点を承認または却下するかどうかを決定することができる。

3. 今後の作業

ENISA の手法は、CTL のドラフト作成方法の概要を高いレベルで説明している。ある意味で、これは生きた文書だ。ENISA および ETL 編集チームは、この手法の改善や更新に関するフィードバックや方法を常に募集している。このプロセスは、すべてを網羅するものではなく、いくつかの重要な手順を紹介するものだ。

ENISA の方法論を公開するもう 1 つの理由は、他の事業体が独自の年次報告書を作成できるようにすることだ。そうすることで、ENISA は、コミュニティの成熟とサイバーセキュリティのさらなる向上を支援することを目指している。これは、ENISA の主な目標の 1 つでもある。

3.1 自動化された情報処理への移行

2025 年においても、この手法には依然として多くの手作業が伴う。人間の介入や分析は依然としてこのプロセスの重要な部分となるが、作業の大部分は自動化されるだろう。例えば、電子的に保存された情報 (ESI) を識別、収集、保存、処理、レビュー、分析、作成するために、1 つ以上の分野に特化したさまざまなソリューションがある。

このようなソリューションにより、OSINT、脆弱性データベース、EU 加盟国や民間パートナーから受け取った情報などの一般的な情報源から、CTL の作成に現在使用されているさまざまな ESI を効率的に処理、相互妥当性確認、分析することが可能になる。この文脈において、これらの自動化ソリューションは、構造化データおよび非構造化データ内のパターン、傾向、および関係を探索し、ステークホルダーが将来のサイバーセキュリティの課題に事前または事後に対応するための洞察や情報を発見することを可能にする。

さらに、機械可読性はサイバーセキュリティコミュニティでますます利用されている。中期的に、CTL は、ENISA の利害関係者が状況認識を容易に把握できるように、機械可読形式のフォーマットを増やすことを目指す。