TTC技術レポート
Technical Report

# TR-XSup.44

## X.1060 の付属文書 - 概略的な実装の考察

## Supplement on high level implementation considerations

第 1.0 版

2025 年 11 月 28 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

# 目次

## ＜参考＞

### 1. 国際勧告などとの関連

本標準は量子鍵配送ネットワークの機能要求条件について規定しており、2025 年 4 月に ITU-T SG17 において発行された ITU-T X Suppl. 44 に準拠している。

### 2. 上記勧告などに対する追加項目など

#### 2.1 オプション選択項目

なし

#### 2.2 ナショナルマター決定項目

なし

#### 2.3 その他

なし

#### 2.4 原勧告との章立て構成比較表

章立てに変更なし

### 3. 改版の履歴

| 版数 | 発行日 | 改版内容 |
|---|---|---|
| 第 1 版 | 2025 年 11 月 28 日 | 制定 |

### 4. 工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、TTC ホームページでご覧になれます。

### 5. その他

(1) 参照している勧告、標準など

| | |
|---|---|
| ITU-T 勧告 | ITU-T X.1060 |
| JT 標準 | JT-X1060 |

### 6. 標準作成部門

セキュリティ専門委員会

# X.1060 の付属文書 - 概略的な実装の考察

## 1　規定範囲

この付属文書は CDC/CSC の内容を提供することで、セキュリティの専門家の X.1060 の理解と実装の手助けになるものである。

## 2　参考文献

[ITU-T X.1060]　Recommendation ITU-T X.1060 (2021), *Framework for the creation and operation of a cyber defence centre*.

## 3　定義

### 3.1　他の標準等で定義されている用語

本付属文書は、以下のほかで定義される用語を使用する。

**3.1.1　アウトソーシング[b-ITU-T X.1053]:企業が内部のプロセ氏や機能の 1 つまたは複数を外部の企業に委託すること。アウトソーシングは、企業のリソースを外部の企業に移すとともに、アウトソースされたプロセスとの関係性を管理する能力を保有する。**

**3.1.2　サイバーディフェンスセンター(CDC) [b-ITU-T X.1060]:組織において、ビジネス活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する主体。**

**3.1.3　サイバーセキュリティセンター(CSC) [b-ITU-T X.1060]:サイバーディフェンスセンター(CDC) の同義語(3.1.2 を参照).**

### 3.2　本標準で定義する用語

なし

## 4　略語及び頭字語

本付属文書では、次の略語及び頭文語を使用する。

CDC　Cyber Defence Centre(サイバーディフェンスセンター)

CISO　Chief Information Security Officer(最高情報セキュリティ責任者)

CSC　Cyber Security Centre(サイバーセキュリティセンター)

CSIRT　Computer Security Incident Response Team(コンピューターセキュリティインシデント対応チーム)

CSO　Chief Security Officer(最高セキュリティ責任者)

CxO　C-suite Officer(経営層)

FIRST　Forum of Incident Response and Security Teams(インシデントレスポンスとセキュリティチームのフォーラム)

SOC　Security Operation Centre(セキュリティオペレーションセンター)

## 5　規則

なし

## 6　はじめに

### 6.1　なぜ今CDC/CSCが必要か？

サイバーセキュリティにおいて、世界的に対処すべき共通の課題があり、協調が必要とされるものがある。

1. 各組織やCISO（最高情報セキュリティ責任者）は、それぞれ独自のSOC（セキュリティオペレーションセンター）の定義を持っており、さまざまな見解が存在する。すべての組織は独自のものであり、それが業界における最大の課題の一つとなっている。
2. 各関係者（民間および公共の組織）が担う業務を説明するための共通の言語が存在しないため、国や地域がサイバー攻撃に対抗するために組織化、協力、連携することが困難になっている。
3. サイバー空間を保護するために何をすべきかについての共通の理解が不足しており、それを実行するためのリソースも不足している。サイバーセキュリティは依然として主に実務的な領域であるため、サービスの体系化を進めることで、能力開発の取り組みを加速したり、それに合わせることができる可能性がある。

X.1060は、最先端の多言語対応でグローバルなガバナンスアプローチを提供し、あらゆる組織が利用可能なサイバーディフェンス/セキュリティセンター（CDC/CSC）のフレームワークを確立することを目的としている。

CDC/CSCは、セキュリティポリシーをサービスとして実装する。サービスカタログを定義し、メンバーが適切なトレーニング、サービス、テクノロジーを活用できるようにする条件を提供する。このフレームワークは理論的なものにとどまらず、CDC/CSCがどのように、誰によってセキュリティサービスを実施するか（インソース、アウトソース、またはその組み合わせ）を評価するためのスコアリングシステムも提供する。

CDC/CSCのメンバーは、戦略マネジメントを含むすべてのセキュリティ活動に対してポリシーの設定やリソース計画を行う責任がある。まず9つの主要なCDC/CSCサービスカテゴリーには、以下の項目が含まれる：

A)　CDC/CSCの戦略マネジメント
B)　即時分析
C)　深堀分析
D)　インシデント対応
E)　診断と評価
F)　脅威情報の収集および分析と評価
G)　CDC/CSCプラットフォームの開発・保守
H)　内部不正対応支援
I)　外部組織との積極的連携

詳細については、X.1060の12章を参照のこと。

### 6.2　すでにあるSOCやCSIRTのようなセキュリティの活動を変える必要があるのか？

X.1060 は CDC/CSC のためのフレームワークを提供する。CDC/CSC は、エンティティとして新しい概念および用語である。この概念には、既存のセキュリティ活動である SOC、CSIRT などが含まれる。

CDC/CSC の対象は、内部の IT システムにとどまらず、顧客向けのビジネスサービスも含まれる。CDC/CSC は、SOC や CSIRT の既存の活動ではカバーしきれない顧客向けのすべてのセキュリティ活動を定義する。

ほとんどの SOC は、専門コミュニティ（例：FIRST（https://www.first.org/））の成果物に基づいて、インシデント対応を中心に構成されている。しかし、最高水準の SOC であっても、リスクを適切に管理するためには継続的な進化が求められる。すべてをできる SOC はない。多くの組織は彼らのビジネス目標に沿って潜在的な脅威に対処するための能力の構築と、サービス選択のガイドラインを提供するフレームワークを求めている。

サイバーセキュリティリスクは、既存のセキュリティ活動だけでは対処が難しくなっている。そのため、CISO やセキュリティマネージャーは、これらのリスクを管理するために CDC/CSC の概念を理解する必要がある。

X.1060 は、セキュリティサービスのリストを提供する。これにより、組織はセキュリティサービスとセキュリティ活動をマッピングすることができる。リストに記載されたセキュリティサービスの一部は、SOC や CSIRT など各セキュリティチームに割り当てることができる。

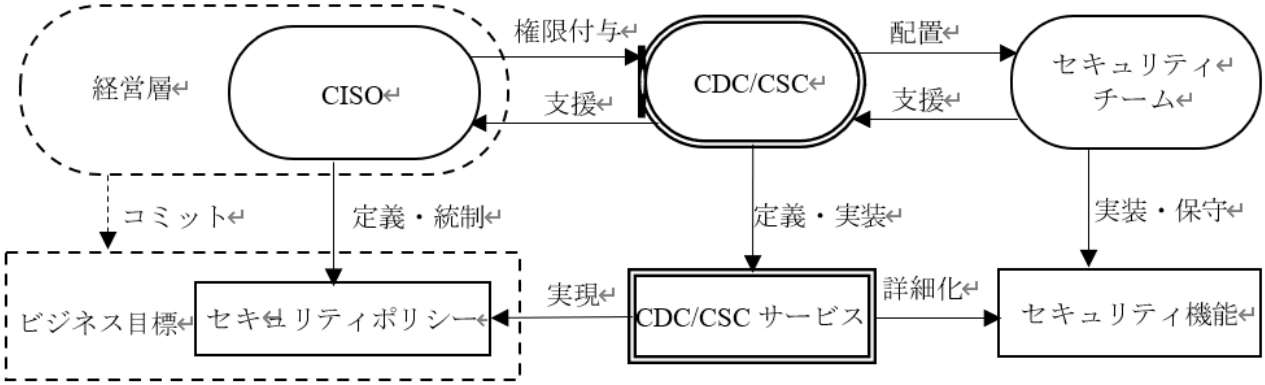
X.1060 は、CDC/CSC の構築と運用のためのフレームワークを提供しているため、組織は独自に CDC/CSC を設計してセキュリティチームを構築することができる。このフレームワークに基づき、サービスを体系化することで、ベストプラクティスに基づいた SOC を構築し、適切なリソース管理が可能になる。共通のフレームワークに基づいて、組織が独自に SOC の変革を行えるようにする。サービスを体系化することで、最先端の SOC によって適切なリソース管理を行うことができるようになる。

## 7　CDC/CSCの内容について

### 7.1　X.1060の対象外のもの

X.1060 は、サイバーディフェンスセンター/サイバーセキュリティセンター（CDC/CSC）の構築と運用に関するフレームワークを定義するため、明確な範囲で策定された。

この範囲設定は、X.1060 の焦点を CDC/CSC そのものに絞るため、いくつかの領域を意図的に対象外としている。X.1060 の図 1 に対してこれらの対象外となる領域が示されている。



X.1060 には 4 つの領域に対象外のものがある。

1. 経営層が何をするか示していない
    - サイバーセキュリティの重要性を認識する
    - CISO を選任する
    - CISO への明確な指示を行う
    - CDC/CSC の設置を決定する
2. CISO が何をするか示していない
    - 以下の 2 点からセキュリティポリシーを決定すること
        - 組織のビジネス環境やビジネスの目的を考慮する
        - 経営層からの指示
    - CDC/CSC の設立について経営層に啓発して推進する
3. それぞれの組織における CDC/CSC の詳細な設計や配置を示していない
4. 以下に示すような内容をもとに CDC/CSC のサービスポートフォリオをどう実装するかを示していない。
    - どんなシステムやプロセスが利用されているか
    - CDC/CSC のサービスをどこまでスコープとするか

1 や 2 は明白で、3 や 4 は今後取り組むことで X.1060 の進歩やその適用が進むものである。

## 7.2 CDC/CSC の実装について

X.1060 は、各サービスを組織内でどのように実装するかを具体的に定めていない。サービスを実装するには、次の 2 つのステップがある。まず、サービスリストから組織に合ったサービスを選択し、その後、サービスを実装することである。

サービスの選択は、組織によって異なる。各組織は独自のガイドラインや手続きを使用しており、CDC/CSC の実装方法も他の組織とは異なる。

X.1060 は、サービスリストからサービスを選択する際の「CDC/CSC サービス推奨レベル」を提供している。組織は最初に基本的なレベルに基づいたサービスを定義し、次にそれらの優先順位を付け、実装を行うことができる。

もう一つのポイントは、各サービスをどのように実装するかである。すでに採用されているサービスについては、実装については既存のガイドラインや手続きが多く存在する。新たに実装するサービスについても、参照できる既存の業界フォーラムや標準化組織の資料がある。

サービスが一度実装された後は、組織は継続的に評価と改善を行うべきである。

## 7.3 CDC/CSCの成熟度の測り方について

X.1060 では、組織内の各サービスに対するセルフアセスメントを提供している。しかし、これは組織における CDC/CSC の成熟度レベルを測定することを目的としたものではない。「成熟度」には 2 つの用途がある。一つは組織内でのサービス改善、もう一つは他の組織とのベンチマーク（比較）である。X.1060 のセルフアセスメントは、組織内のサービス改善を測定するのには適しているが、ベンチマークには適していない。

組織では成熟度モデルやスコアのある既存のガイドラインや手続きを参考にしてサービスを実装することがある。組織はそのようなモデルやスコアを用いてサービスを測定することは可能だが、その適用範囲

は、既存のガイドラインや手続きでカバーされているサービスに限定される点に注意が必要である。この場合、CDC/CSC 全体のサービス改善を測定するには不十分である。

組織が成熟度測定のベンチマークを必要とする場合、第三者によるアセスメントを検討することも可能である。ただし、これは X.1060 の適用範囲外となる。

## 8　今後のCDC/CSCとX.1060シリーズでの検討事項

### 8.1　CDC/CSCサービスの実装について

組織がサービスを実装するには適切なガイドラインや参照元が必要だが、既存のサービスを詳細にするのに参照できるものは多岐にわたるため、X.1060 では各サービスに対する具体的な参照元について言及していない。

ベンダーやセキュリティサービスプロバイダーが提供するベストプラクティスは、組織の各サービスにおいて何を実施すべきかを理解する上で有用である。一方で、これらのベストプラクティスを収集し、セキュリティサービスの標準化を進めることも必要である。ITU-T Study Group 17(SG17)ではこれについては今後の ITU-T 1060 シリーズでの検討課題である。

### 8.2　CDC/CSCの成熟度について

X.1060 は、本書 7.3 で述べたように、各サービスの成熟度を測定するものは提供していない。

組織の成熟度を第三者が評価するには、指標のセットが必要となる。さらに、各サービスをどのように実装するかの検討も必要である。各サービスに対するさまざまな指標をまず明らかにする必要がある。

### 8.3　複数のCDC/CSCの構造

X.1060 では、「単一の組織内に 1 つの CDC/CSC が存在する」というシンプルな構造が定義されている。しかし、実際には、1 つの組織内に複数の CDC/CSC が存在するケースや、CDC/CSC が階層的・多層的な構造を持つケースもある。

例えば、国家機関のような組織では、カテゴリーA「CDC/CSC の戦略マネジメント」に基づくポリシーがガバナンスとして機能し、組織全体に影響を及ぼす。組織のアプローチには、フラットな組織構造でサービスを割り当てる場合と、階層構造を持たせる場合など、さまざまなバリエーションが存在する。

このような複雑な構造は、X.1060 ではまだ定義されておらず、今後の発展に向けた検討課題となっている。

確実なのは、X.1060 が組織内のセキュリティ活動における共通言語として機能することである。それは、どのようなサービスを実装すべきかを定義し、それらのサービスを分類することで、包括的なセキュリティ活動を促進する。

## 9　ITU-T X.1060チュートリアル

本付属文書は X.1060 のチュートリアルのためのプレゼンテーション資料を提供する。

このプレゼンテーション資料は 3 つのセクションを含む。

1. なぜ X.1060 を使うのか
2. ITU-T 勧告 X.1060 の概要：CDC/CSC とは何か?
3. サイバーディフェンスセンター/サイバーセキュリティセンターを構築と運用のためのフレームワーク

1. なぜ X.1060 を使うのか?

このセクションでは、X.1060 の 6 章についてである。CDC/CSC は新しい概念であり、X.1060 は CDC/CSC の構築と運用のためのフレームワークを提供する。CDC/CSC とは何かを理解することはセキュリティの専門家が X.1060 を活用する際に助けになる。

2. ITU-T 勧告 X.1060 の概要：CDC/CSC とは何か?

このセクションは、X.1060 の 7 章および 8 章に関連しており、X.1060 の概要や、適用範囲外となる事項について提供する。

3. サイバーディフェンスセンター/サイバーセキュリティセンターの構築と運用のためのフレームワーク

このセクションは X.1060 に基づくものである。フレームワークの概要、フレームワークの 3 つのプロセス、すでに組織に SOC や CSIRT のようにすでにいくつかサービスを持つ場合のマッピングのケースなどのいくつかのポイントを示している。

## 10 よくある質問(FAQ)

**Table 1 FAQ**

| # | 質問 | 回答 |
|---|---|---|
| 1 | なぜ CDC/CSC が必要なのですか？ | 6 章を参照のこと (6.1 なぜ今 CDC/CSC が必要か？) |
| 2 | SOC や CSIRT のようなすでにセキュリティ活動を行っているものを変えるべきなのか? | 6 章を参照のこと (6.2 すでにある SOC や CSIRT のようなセキュリティの活動を変える必要があるのか？) |
| 3 | CDC/CSC とは何ですか? | X.1060 では、CDC/CSC を「組織において、ビジネス活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する主体」と定義している。<br>また、X.1060 では CDC/CSC について次のようにも紹介している。<br>「…実際にセキュリティ対策を実現するためには、そういった最高セキュリティ責任者（CSO）や最高情報セキュリティ責任者（CISO）の活動を、組織レベルで戦略的にマネジメントしサポートする主体が必要となる。この主体を、本勧告ではサイバーディフェンスセンター／サイバーセキュリティセンター（CDC/CSC）と表現している。」 |
| 4 | X.1060 は CDC/CSC について何を提供していますか？ | X.1060 は、サイバーディフェンスセンター／サイバーセキュリティセンター（CDC/CSC）の構築と運用のためのフレームワークを提供している。一方、CDC/CSC は一つの概念としての組織体（エンティティ）である。 |

| | | |
|---|---|---|
| | | X.1060 の規定範囲は以下の通りである。<br>「この勧告は、組織がサイバーディフェンスセンター/サイバーセキュリティセンター(CDC/CSC)を構築、マネジメントするとともに、その有効性の評価するためのフレームワークを提供するものである。このフレームワークは、組織のセキュリティを実現するために、CDC/CSC がどのようにセキュリティサービスを決定し実装すべきかを示している。」 このフレームワークは、組織がサイバーセキュリティのリスクに対処するために役に立つ。 |
| 5 | X.1060 を利用することの利点は何ですか？ | X.1060 は、サイバーセキュリティにおける内部および外部のコミュニケーションの共通言語となるよう、ベストプラクティスとしてセキュリティサービスの一覧を提供する。 |
| 6 | どのように既存の SOC や CSIRT を CDC/CSC にマッピングできますか？ | X.1060 のフレームワークは、構築プロセス（Build process）、管理プロセス（Management process）、評価プロセス（Evaluation process）の 3 つのプロセスで構成されている。<br>SOC および CSIRT については、マネジメントプロセスを説明する X.1060 の 10 章で言及されている。<br>(2) 運用フェーズ<br>“…このような業務を行うチームは、セキュリティオペレーションセンター（SOC）と呼ばれることが多い。”<br>(3) 対応フェーズ<br>“運用フェーズでの分析によってイベントが検知された場合、インシデント対応が発動される。このフェーズは有事の対応となる。インシデントに対応する組織は、コンピューターセキュリティインシデント対応チーム（CSIRT）と呼ばれることが多い。”<br>すでに SOC、CSIRT を持つ組織では、それらが提供するセキュリティサービスは X.1060 のセキュリティサービスに対応している。これらのセキュリティサービスは、一般的にカテゴリーB、C、D にマッピングされる。<br>一方で、既存の SOC や CSIRT が提供するセキュリティサービスは多岐にわたるため、一部のサービスは他のカテゴリーにもマッピングされる場合がある。 |
| 7 | CDC/CSC は国家の防衛や軍関連の組織に関係しますか？ | 基本的には関係しない。<br>CDC/CSC はある組織において業務の活動におけるサイバーセキュリティのリスクに対応するセキュリティサービスを含む主体である。それは国家の防衛や軍だけのものではない。<br>サイバーディフェンスはセキュリティの専門家によって共通的に使われる用語であり、サイバー攻撃を含むサイバーの脅威に対して資産を守るための日々の活動を示している。 |

| | | |
|---|---|---|
| | | CDC/CSC の機能を持つ主体の名前や（組織の）形は異なる組織では別のものであるなど組織に依る。ある組織ではその主体を SOC とし、ある組織では CERT,CSIRT やその他の名前にする場合もある。<br><br>CDC/CSC は SOC や CSIRT を含む広いコンセプトである。<br>CDC/CSC はサービスの一部としてそれらを含んでいる。<br><br>しかしながら、国家の防衛のセクターや軍の組織でもサイバー空間における他の組織のように CDC/CSC の機能的な主体を持つべきである |
| 8 | CDC/CSC を組織に配置するための詳細な設計は何がありますか？ | このポイントは X.1060 の範囲外である。X.1060 は CDC/CSC をそれぞれの組織にどのように配置するかの詳細な設計を提供していない。<br><br>CDC/CSC は幅広く組織のビジネス活動をカバーするセキュリティサービスを提供している。それは組織内の IT 部門やビジネス部門、バックオフィス部門を含む様々な部署に関係するものである。 |
| 9 | 組織においてサービスリストからどうやってサービスを選択しますか？ | 最初に、マネジメントプロセスを開始できるように組織において必須となるベーシックレベルのサービスを選択する(FAQ 項目 10 を参考)。<br><br>マネジメントプロセスは 3 つのフェーズを含む。戦略マネジメント、運用、対応。<br><br>• 戦略マネジメントのフェーズでは、カテゴリーA(CDC/CSC の戦略マネジメント)が対応する。<br>• 運用フェーズでは、カテゴリーB (即時分析)とカテゴリーC(深堀分析)が対応する。<br>• 対応フェーズでは、カテゴリーD(インシデントレスポンス)とカテゴリーH(内部不正対応支援)が対応する。<br><br>マネジメントプロセスにおいて、カテゴリーA,B,D のベーシックレベルのサービスが選択されるべきである。<br><br>カテゴリーA はマネジメントプロセスでは戦略マネジメントフェーズに、カテゴリーB は運用フェーズに、カテゴリーD は対応フェーズに対応する。<br><br>そのあとで、組織は推奨レベルに応じてほかのカテゴリーのサービスを選択する。 |
| 10 | サービスリストからサービスを選ぶ際の、CDC/CSC サービスの推奨レベルをどう理解しますか？ | X.1060 の 9.2 章では CDC/CSC サービスの推奨レベルは 5 つのウェイトを持つ。不要、ベーシック、スタンダード、アドバンスド、オプションである。<br><br>ベーシックは実装される最小の数のサービスとなる。 |

| | | |
|---|---|---|
| | | 組織で従うべき規定やマネジメントシステムがあるなら、関連したサービスをベーシックやスタンダードで選択することになる。<br><br>いくつかのセキュリティの活動ためのプロセスがすでに存在するなら、組織はそのプロセスに関連したサービスをベーシックかスタンダードのレベルでサービスを設定する。 |
| 11 | それぞれのサービスをどうやって実装しますか? | このポイントは X.1060 の対象外である。X.1060 は、どうやって CDC/CSC サービスを実装するか、システムやプロセスを使うか、それぞれの CDC/CSC サービスのスコープを定義するかについて明確にはしていない。 |
| 12 | 他の主要なドキュメントとの関連性について | X.1060 は組織がセキュリティ活動を実践するフレームワークを提供する。経営層が CDC/CSC を設置すると決めた際に活用できるフレームワークである。<br><br>X.1060 に加えて、X.1060 のスコープを超えて広いセキュリティのエリアをカバーできるたくさんの数の標準や参照できるドキュメントがある。それぞれのドキュメントは自身のスコープがあり、組織にどう適用するのか、利用するのかのガイダンスを提供する。<br><br>それらの様々なドキュメントは以下のようにカテゴライズされる：<br><br>- 組織の構造を形作るようなガバナンスとマネジメント<br>- プロセスや手順<br>- スキルやスキルの開発<br><br>ガバナンスとマネジメントのドキュメントは組織を効果的に管理する方法を提供し、参考にすることができる。<br><br>X.1060 はガバナンスとマネジメントの中で CDC/CSC を設立し、セキュリティサービスの選択や実装を決定するために利用できる。<br><br>X.1060 が定義されたサービスの概要を提供する一方で、実際のプロセスのなかでそれぞれのサービスを実装する詳細な説明は他の参照文書で補完される必要がある。<br><br>プロセスと手順を定義することで、個人に必要なスキルと能力を決めることができる。この目的のために、スキルと能力に焦点を当てた主要なドキュメントを参照することができる。<br><br>それぞれの主要なドキュメントのスコープを理解することは極めて重要である。<br><br>これによりそれぞれの範囲内での適切に利用することができる。 |

| | | |
|---|---|---|
| 13 | 業界独自の視点、例えば政府機関 – 規制当局や、民間のセクターをどう考えるか？ | 8 章を参照のこと (8.3 複数の CDC/CSC の構造). |

## 付属資料 A

## <X.1060チュートリアルのためのプレゼンテーション資料>

ファイル、「ITU-T.X.1060tutorial.pptx」を参照のこと。

## 付録 I

## CDC/CSCにおけるジョブの記述について

この次のステップについてはまだですが、8 章の「8.1 CDC/CSC サービスの実装について」はサービスを実装するために必要なジョブの記述を定義する方法に関する問題を示している。

これは、7 章の「7.2 CDC/CSC の実装について」の内容で示すように、なぜ CDC/CSC がスタートしたかの核心である。今日の世界では何百万人のサイバーセキュリティの専門家が不足している。サイバーセキュリティは依然として職業的に発展しているのに対して専門的には発展していないからである。

X.1060 の適用が進むにつれ、多くのパラメータが決まり、サービスが決まり、ジョブの記述が決まる可能性がある。ジョブの記述から、学術や教育の世界において適切な専門向けのカリキュラムを開発する機会を得ることができ、これからの認定プログラムを含む可能性がある。