ホワイトペーパー

Axisデータシート用クイックガイド

認証、認定およびプロトコル

2019年2月

目次

1. はじめに

アクシスコミュニケーションズは、市場に投入するすべての製品において、適用される業界標準およびコンプライアンス基準を順守しています。本ドキュメントは、Axisデータシートに記載されている頭字語、認証、認定、およびプロトコルの定義と概要について補足します。

本ドキュメントでは、下のデータシート画像でハイライト表示および拡大表示されているデータシートの箇所に関する情報を提供します。

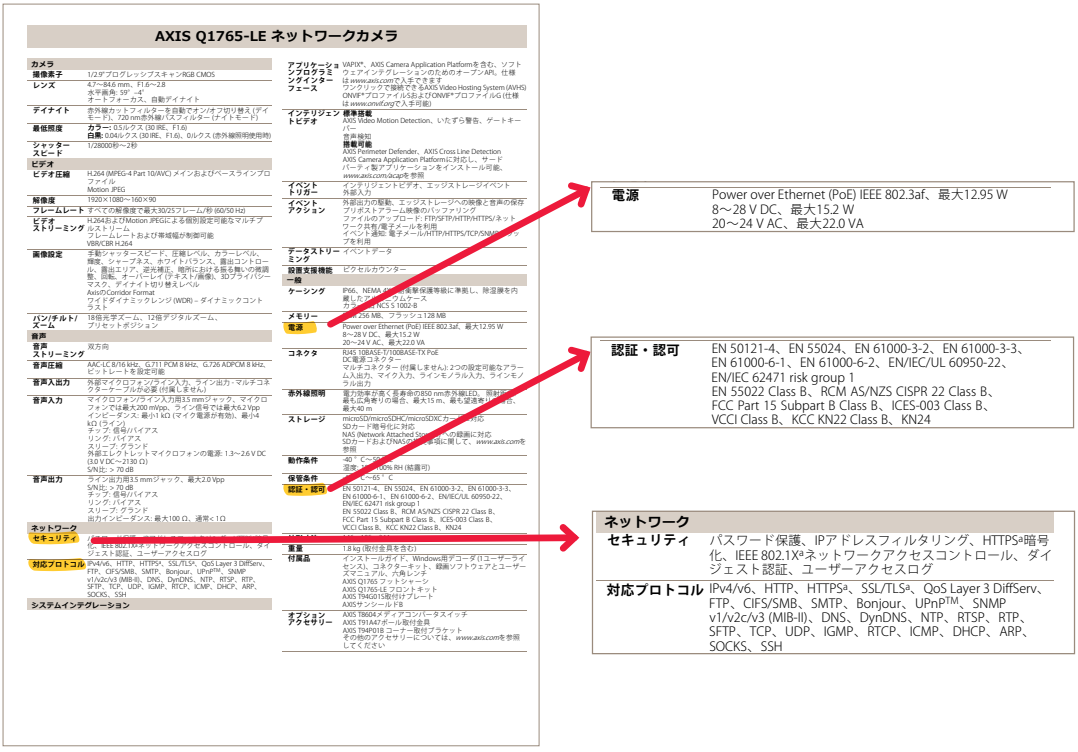

図1 本ドキュメントで焦点を当てているAxisデータシートの箇所 (ハイライト表示)。

2. 認証

Axisデータシートの認証の欄には、さまざまな規格への準拠について記載されてます。このセクションは多くの場合、EMC、安全性、環境、およびその他の項目に分けられています。「その他」には、防爆性能やアクセスコントロールにおけるセキュリティなどが含まれます。製品にミッドスパンが付属している場合は、ミッドスパンに関する認証の項目が設けられていることもあります。

2.1 EMC (電磁両立性)

すべてのネットワークビデオメーカーは、自社のネットワークビデオ製品のEMCについて宣言する必要があります。場合によってはメーカーが自己認証することも可能ですが、ほとんどのメーカーは認定試験機関を使用し、そこから提供されるレポートで適合性を確認します。EMC認証は、以下の2つの要素、エミッションとイミュニティに基づいています。

*エミッション*は、同じ環境内にある他の機器に妨害を与える可能性のある電磁エネルギーを大量に放射せず、性能を十分に発揮できる機器の能力を表します。

*イミュニティ*は、他の電子製品から放射または伝搬される電気エネルギーや電磁現象の影響に対する電子製品の耐性を表します。欧州では、EMCはEUの整合法令に含まれるCEマークに含まれています。

下記の規格は、電磁妨害放射 (エミッション) と電磁妨害耐性 (イミュニティ) に関する限度値と試験方法を定めています。適合性を包括的にカバーする試験は存在しないため、コードは各地域/用途に応じて異なる場合があります。

2.1.1 情報技術装置 (ITE) 規格

> EN 55022 クラスA: エミッション規格 (商業、工業、ビジネス)、国際規格と整合

> EN 55022 クラスB: エミッション規格 (住宅)、国際規格と整合

> EN 55024 クラスA: イミュニティ規格 (商業、工業)、国際規格と整合

> EN 55024 クラスB: イミュニティ規格 (住宅)、国際規格と整合

2.1.2 整合規格 (国/地域別)

> EN 61000-6: 適合性一般規格 (欧州)

> FCC パート15 サブパートB クラスA/B: FCCが定める電気通信機器に関する規則や規制、エミッションのみを規定 (米国)

> ICES-003 クラスA/B: (カナダ)

> VCCI (日本)

> KN22、KN24、KN32、KN35 (韓国)

> CISPR 22 クラスA/B (オーストラリア/ニュージーランド)

2.1.3 その他の規格 (用途/製品別)

> EN 50121-4、IEC 62236-4: 鉄道環境の他の装置と干渉する可能性がある信号機器および電気通信機器の性能基準を定めています。

> EN 50130-4: アクセスコントロールシステム、CCTVシステム、火災検知システム、火災警報システム、強盗警報システム、侵入者警報システム、緊急通報システムを含む警報システムのコンポーネントに適用されます。

> EN 55032 (エミッション) – EN 55035 (イミュニティ): AC電源またはDC電源の電圧が600V以下のマルチメディア機器 (MME) に適用されます。マルチメディア機器 (MME) は、情報技術装置 (ITE)、オーディオ機器、ビデオ機器、放送受信機、娯楽用照明制御装置と定義されています。

2.2 安全性

> 低電圧指令 (2014/35/EU): 電気機器の安全性に関する広範な目標を定めています。ケガや物的損害の危険性なく、製品が安全に使用できることを保証します。

> IEC/EN/UL 60950-1: 火災、感電、または装置に接触する可能性のある人のケガの危険性を低減することを目的とした要件に対する、ネットワークカメラ、エンコーダ、電源装置の適合性。

> IEC/EN/UL 60950-22: 屋外対応製品および屋外対応エンクロージャーに対する特定の安全要件。

> IEC/EN 62471: 暴露限度に関する要件、目や皮膚に対する危険性を防止します。

> EN 62368-1: EN 60950規格に置き換わる規格。ただし、2019年までは両規格とも有効です。IECおよびULでは同じ番号を使用した整合規格を設定しています。

> EN/UL/CSA 60065: 主電源、電源装置、電池または遠隔電力供給から給電し、オーディオ、ビデオおよび関連の信号を受信、発生、記録または再生することを意図して設計された電子機器に適用されます。

2.3 環境

2.3.1 IP 保護等級

IEC (国際電気標準会議) の規格、IEC 60529は、IP (侵入保護または国際保護) 保護等級を2桁のコードで表します。このコードは、固形物や埃の侵入、偶発的な接触、水に対する電化製品の保護レベルを定義しています。

表1. IP保護等級、1桁目 (IP**x**x) – 外来固形物

レベル	保護対象	詳細
0	無保護	無保護
1	50 mm以上の物体	手の甲など身体の大きな表面。身体の一部による故意の接触に対しては無保護。
2	12.5 mm以上の物体	危険な箇所に接触しない場合、指または類似物を80 mmまで挿入できる。直径12.5 mmの物体が完全には侵入できない。
3	2.5 mm以上の物体	工具や太いワイヤーなどの物体が内部に侵入しない。
4	1 mm以上の物体	ワイヤーやねじなどの物体が内部に侵入しない。
5	防塵	粉塵の侵入を完全には防がないが、装置の正常な動作を阻害するほどの粉塵は侵入しない。
6	防塵	粉塵が内部に侵入しない。

表2. IP保護等級、2桁目 (IPx**x**) – 液体

レベル	保護対象	詳細
0	無保護	特には保護されていない。
1	水滴	水滴 (鉛直に落下する水滴) によって有害な影響を受けない。
2	水滴 (傾斜角が最大15°まで)	エンクロージャーがその正常な取り付け位置より最大15°まで傾いても、鉛直に落下する水滴によって有害な影響を受けない。
3	散水	垂直から60°までの角度で落下する散水によって有害な影響を受けない。
4	飛沫	エンクロージャーに対するいかなる方向からの飛沫によっても有害な影響を受けない。
5	噴流水	エンクロージャーに対するいかなる方向からのノズルによる噴流水によっても有害な影響を受けない。
6	強い噴流水	荒波あるいは強い噴流が、有害な影響を及ぼすほどエンクロージャーに侵入しない。
7	短時間の浸漬	規程の圧力と時間でエンクロージャーを水に浸漬しても、有害な量の水は侵入しない。
8	連続的な浸漬	メーカーによって規定される条件に従って、連続的に水中に置かれる場合に適する。この条件は、IPX7の条件 (上記参照) よりも厳しい必要がある。
9	高圧・スチームジェット洗浄による水	ハウジングに対し非常に高い圧力でいかなる方向から放水しても、有害な影響を受けない。

2.3.2 その他関連IEC規格

> IEC 60068-2は、電子機器および電子製品が、極度の低温および高温低湿を含む環境条件下で性能を発揮できる能力を評価するための環境試験向けの規格です。一般的に、この規格における以下の手順は、試験の実施中に温度安定性を得ることを目的としています。

- IEC 60068-2-1: 低温
- IEC 60068-2-2: 高温低湿
- IEC 60068-2-6: 振動 (連続的)
- IEC 60068-2-14: 温度変化
- IEC 60068-2-27: (衝撃)
- IEC 60068-2-30: 高温高湿 (サイクル)
- IEC 60068-2-64: 振動 (広域帯ランダム)
- IEC 60068-2-78: 高温高湿 (定常)

> IEC 60825 クラスIは、レーザーモジュールで使用されるレーザーが、通常の使用のあらゆる条件下で安全であることを保証するための規格です。

2.3.3 NEMA等級

NEMA (アメリカ電機工業会) は米国を拠点とする協会で、電気機器のエンクロージャーに関する規格を提供しています。NEMAは、独自の規格である「NEMA 250」を世界中で展開しています。また、米国規格協会 (ANSI) を通じて、整合IP規格、ANSI/IEC 60529を採用し、公開しています。

NEMA 250は、侵入に対する保護を対象としていますが、耐食性、性能、構造などのその他の要因も考慮します。そのため、NEMAのタイプはIPに相当しますが、IPはNEMAに相当しません。

UL規格であるUL 50およびUL 50Eは、NEMA 250規格に基づいています。NEMAは自己認証を許容していますが、ULは第三者機関による試験および検査への合格を要求することで、規格への順守を徹底しています。

表3. 危険区域外にあるエンクロージャーのNEMA保護等級

NEMA	同等のIP保護等級	屋内向け	屋外対応	保護対象
Type 1	IP10	X		危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵)。液体に対する保護はなし。
Type 3	IP54	X	X	危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵および吹き付けられる粉塵)。水の侵入 (雨、みぞれ、雪)。エンクロージャー外側の氷結によって損傷しない。
Type 3R	IP14	X	X	危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵)。水の侵入 (雨、みぞれ、雪)。エンクロージャー外側の氷結によって損傷しない。
Type 3S	IP54	X	X	危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵および吹き付けられる粉塵)。水の侵入 (雨、みぞれ、雪)。氷が堆積しても外部機器が機能する。
Type 4	IP56	X	X	危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵および吹き付けられる粉塵)。水の侵入 (雨、みぞれ、雪、飛沫、噴流)。エンクロージャー外側の氷結によって損傷しない。
NEMA 4X	IP56	X	X	危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵および吹き付けられる粉塵)。水の侵入 (雨、みぞれ、雪、飛沫、噴流)。腐食に対しさらに優れた保護を提供する。エンクロージャー外側の氷結によって損傷しない。
Type 6	IP67	X	X	危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵)。水の侵入 (噴流および一時的に発生するある程度の深さの水没により侵入する水) エンクロージャー外側の氷結によって損傷しない。
Type 6P	IP67	X	X	危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵)。水の侵入 (噴流および長時間にわたる、ある程度の深さの水没により侵入する水)。腐食に対しさらに優れた保護を提供する。エンクロージャー外側の氷結によって損傷しない。
Type 12	IP52	X		ノックアウト穴なし。危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵、浮遊する粉塵、糸くず、繊維、綿埃)。水の侵入 (水滴および少量の飛沫)。
Type 12K	IP52	X		ノックアウト穴あり。危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵、浮遊する粉塵、糸くず、繊維、綿埃)。水の侵入 (水滴および少量の飛沫)。
Type 13	IP54	X		危険箇所へのアクセスおよび外来固形物の侵入 (落下する粉塵、浮遊する粉塵、糸くず、繊維、綿埃)。水の侵入 (水滴および少量の飛沫)。散水、飛沫、オイルおよび非腐食性の冷媒の侵入。

2.3.4 IK保護等級

IK保護等級は、外部からの機械的衝撃に対する保護の度合いを規定する国際規格、IEC/EN 62262に含まれています。1994年に欧州規格のEN 50102として初めて承認され、2002年に国際規格として採用されました。

多くのメーカーは、製品寿命を通して堅牢性を保証するため、製品の最も弱い部分をテストします。

表4. IK保護等級

レベル	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK10+*
衝撃エネルギー (ジュール)	0.14	0.2	0.35	0.5	0.7	1	2	5	10倍	20	50*
質量 (kg)	<0.2	<0.2	0.2	0.2	0.2	0.5	0.5	1.7	5	5	
落下高さ (mm)	56	80	140	200	280	400	400	300	200	400	

*最大50 Jの衝撃。メーカーは、打撃を与える要素のエネルギー、質量および落下高さを表記する必要があります。

2.4 その他の認証

2.4.1 防爆性能

> IEC/EN/UL/SANS/CSA 60079-0: 爆発性雰囲気中での使用を目的としたEx機器およびExコンポーネントの構造、試験および表示に関する一般的な要件。

> IEC/EN/UL/SANS/CSA 60079-1: 爆発性ガス雰囲気での使用を目的とした、耐圧防爆構造「d」を持つ電気機器の構造および試験に関する特有の要件。

2.4.2 ミッドスパン関連の認証

製品にミッドスパンが付属している場合は、そのミッドスパンに関連する認証がデータシートのこのセクションに記載されています。説明は本ドキュメントの前のセクションに記載されています。

2.4.3 アクセスコントロールにおけるセキュリティ

> UL 294: アクセスコントロールシステムの構造、性能、および動作に関する要件を定めています。

3. 認定

爆発のおそれのある環境にカメラを設置する場合は、ハウジングが特定の安全基準を満たしていなくてはなりません。カメラやその他の機器から発生し得る発火から、環境を保護できる必要があります。

欧州の製品は、ATEX指令 (対応国際規格: IECEx) に準拠している必要があります。北米では、ATEXやIECExのゾーンによる分類よりも、主にNEMAのクラス/区域による等級が使用されています。

表5. 防爆等級

クラス / 区域	雰囲気	定義	ゾーン (IECExおよびATEX)
Class I / Division 1	ガス	爆発性雰囲気が連続して、または長時間存在する区域。	Zone 0
Class 1 / Division 1	ガス	通常の運転時に爆発性雰囲気を生成するおそれのある区域。	Zone 1
Class 1 / Division 2	ガス	通常の運転時に爆発性雰囲気を生成するおそれが少ない、または生成するとしても、短時間しか存在しない区域。	Zone 2
Class II / Division 1	粉塵	爆発性雰囲気が連続して、または長時間存在する区域。	Zone 20
Class II / Division 1	粉塵	通常の運転時に爆発性雰囲気を生成するおそれのある区域。	Zone 21
Class II / Division 2	粉塵	通常の運転時に爆発性雰囲気を生成するおそれが少ない、または生成するとしても、短時間しか存在しない区域。	Zone 22

4. 電力

4.1 Power over Ethernet (PoE) クラス

PoEクラスは、受電機器 (PD) が必要とする電力量を指定することにより、効率的な配電を保証します。

表6. PoEクラス

等級	タイプ	給電機器 (PSE) の保証電力レベル	受電機器 (PD) が消費する最大電力レベル
0	Type 1、802.3af	15.4 W	0.44 W～12.95 W
1	Type 1、802.3af	40.0 W	0.44 W～3.84 W
2	Type 1、802.3af	7.0 W	3.84 W～6.49 W
3	Type 1、802.3af	15.4 W	6.49 W～12.95 W
4	Type 2、802.3at*	30 W	12.95 W～25.5 W
6	Type 3、802.3bt	60 W	51 W
8	Type 4、802.3bt	100 W	71.3 W

*このタイプはPoE+とも呼ばれます。

5. ネットワーク

5.1 保護およびセキュリティコントロール

システム資産に対する脅威への対処方法はいくつかあります。脅威には、装置にリスクをもたらすものと、ネットワークまたは転送中やストレージ内のデータにリスクをもたらすものがあります。以下は、装置とネットワークに適用可能なセキュリティ対策の一部です。

- 認証情報 (ユーザー/パスワード) は、映像や装置の設定への不正アクセスを防止します。異なるレベルのアカウント権限を設定することにより、アクセスできる人物とコンテンツを管理することができます。

- IPフィルタリング (ファイアウォール) は、装置のローカルネットワークへの露出を低減することで、不正なクライアントがアクセスできないようにします。これにより、装置のパスワードが侵害された場合だけでなく、新しい重大な脆弱性が発見された場合のリスクも軽減されます。

- 802.1Xは、不正なクライアントからネットワークを保護します。802.1Xは、マネージドスイッチとRADIUSサーバーを使用したネットワークインフラの保護です。装置の802.1Xクライアントは、ネットワーク上の装置の認証を行います。

- HTTPS (Hypertext transfer protocol secure) は、ネットワークの盗聴からデータ (映像) を保護します。HTTPSで署名付き証明書を使用することにより、ビデオクライアントが正規のカメラにアクセスしているのか、悪意のあるコンピューターがカメラになりすましているのかを検出できます。

サイバーセキュリティに関するその他のリソースについては、www.axis.com/cybersecurityをご覧ください。

5.2 対応プロトコル

データをあるネットワーク装置から別の装置に安全に転送するときは、多くのプロトコルが関与します。

5.2.1 プロトコル参照モデル

さまざまなプロトコルが相互作用するしくみについては、Open Systems Interconnection (開放型システム間相互接続/OSI) 通信モデルを見ると最も良く理解することができます。また、TCP/IP参照モデルもあります。

5.2.1.1 OSI参照モデル

オープンシステム間のデータ通信を説明するモデルです。
各層は、そのすぐ下の層のサービスを利用してサービスを提供します。
それぞれの層は、特定のルールまたはプロトコルに従ってサービスを実行する必要があります。

第7層 – アプリケーション層
ウェブ、ファイル、メールの転送などの機能をアプリケーションで使用できるようにします。

例
> File Transfer Protocol (FTP)
> Simple Mail Transfer Protocol (SMTP)
> Hypertext Transfer Protocol (HTTP)

ウェブブラウザやメールプログラムなどの実際のアプリケーションは、この層の上位に存在し、OSIモデルではカバーされていません。

第6層 – プレゼンテーション層 (データ)
システムのアプリケーション層から送信されたデータを、別のシステムのアプリケーション層が確実に読み取れるようにします。ASCIIなどのシステム依存のデータ形式を独立した形式に変換し、異なるシステム間での構文的に正しいデータ交換を可能にします。

例
> Telnet
> Apple Filing Protocol

第5層 – セッション層 (ピアホスト間の持続的接続)
アプリケーション指向のサービスを提供し、2つのシステム間のプロセス通信を行います。プロセス通信は、2つのシステム間における仮想接続の基礎を形成するセッションの確立から始まります。

例
> Remote Procedure Call
> Network File System

第4層 – トランスポート層 (エンドツーエンド・トランスポート (コネクション型プロトコル))
第5層とその上位の層に、(フロー制御とエラー制御による) 信頼性の高いデータ転送サービスを提供します。

例:
> Transmission Control Protocol (TCP)
> User Datagram Protocol (UDP)

第3層 – ネットワーク層 (パケット (アドレッシング/フラグメンテーション))
ルーティングを行い、システム間でデータパケットを転送することにより実際のデータ転送を実行します。ルーティング表の作成と管理を行い、ネットワークの境界を超えて通信するためのオプションを提供します。この層のデータには宛先アドレスと送信元アドレスが割り当てられ、経路制御時の基本情報として使用されます。

例
> IP (Internet Protocol) – インターネット対応装置が通信するために必要な、個々のパブリックアドレス
> IPv4 – IPのオリジナルバージョン、32ビットアドレスを使用
> IPv6 – 最新バージョンのIP、4桁の16進数を1つのグループとし、8つのグループに区切った128ビットのアドレスを使用
> Routing Information Protocol
> Internet Protocol Security (IPSec)

第2層 – データリンク層 (フレーム)
データをフレームと呼ばれる単位に結合することで、データ伝送を行うとともに伝送媒体へのアクセスを制御します。第2層は上位の論理リンク制御 (LLC) 副層と、下位のメディアアクセス制御 (MAC) 副層の、2つの副層に分割されます。LLCはデータ交換を簡素化し、MACは伝送媒体へのアクセスを制御します。

例
> IEEE 802.2 (LLC)
> IEEE 802.3 (イーサーネットMAC)
> 802.11 (WLAN MAC)

第1層 – 物理層 (ビット)
有線または無線の伝送リンクなど、媒体を介したビットストリームとしてのデータ伝送に対応するサービスを提供します。

5.2.1.2 トランスミッション・コントロール・プロトコル/インターネット・プロトコル参照モデル

TCP/IP参照モデルは、プロトコルと通信方法を理解するために使用される、もう1つのモデルです。TCP/IP参照モデルは、以下のようにOSI参照モデルに相当する4つの層に分類されます。

表7. 参照モデルの比較

OSIモデル	TCP/IPモデル
第7層 - アプリケーション層	第4層 - アプリケーション層
第6層 - プレゼンテーション層	
第5層 - セッション層	
第4層 - トランスポート層	第3層 - トランスポート層
第3層 - ネットワーク層	第2層 - インターネットワーク層
第2層 - データリンク層	第1層 - ネットワークインターフェース層
第1層 - 物理層	

5.2.2 IPアドレス管理用プロトコル

DHCP (Dynamic Host Configuration Protocol) – IPアドレスの自動割り当ておよび管理

DNS (Domain Name System) – ドメイン名を関連するIPアドレスに変換します (トランスポート層で動作)。

DynDNS (Dynamic Domain Name System) –IPv4アドレスの変更に対するドメイン名のリンクを追跡するために使用されます。

UPnP (Universal Plug and Play) – Microsoftのオペレーティングシステムが、ネットワーク上のリソース (Axis製品) を自動的に検出することができます。

Zeroconf – ネットワークデバイスを169.254.1.0～169.254.254.255の範囲にある未使用のIPアドレスに自動的に割り当てます。

Bonjour – Macコンピューターを使用し、ネットワークビデオ製品を検出することを目的として、または任意のネットワーク内の新しいデバイスの検出プロトコルとして使用できます。

ARP (Address Resolution Protocol) – 宛先ホストのMACアドレスを検出するために使用されます。

5.2.3 アプリケーション層プロトコル

HTTP (Hypertext Transfer Protocol) – 主にウェブサイトからウェブブラウザに、テキストや画像を読み込むために使用されます。ネットワークビデオシステムは、設定やライブ映像のダウンロードを目的として、ウェブブラウザからシステムへのアクセスを許可するHTTPサーバーサービスを提供します。

HTTPS (HTTP Secure) – コンピューターネットワーク上での安全な通信を実現するHTTPの強化版で、インターネット上で広く使用されています。HTTPSでは、通信プロトコルがTransport Layer Security (TLS) によって暗号化されます。

FTP (File Transfer Protocol) – 主にサーバーからクライアントへ (ダウンロード) またはクライアントからサーバーへ (アップロード) ファイルを転送するために使用されます。ディレクトリの作成と選択、およびディレクトリとファイルの名前変更または削除にも使用できます。

RTP (Real-Time Transport Protocol) – システムのエンドポイント間におけるリアルタイムデータの転送を許可します。

RTCP (Real-Time Control Protocol) – RTPセッションの帯域外統計データおよび制御情報を提供します。RTPと連携してマルチメディアデータの配信やパッケージ化を行いますが、RTCP自体がデータを転送することはありません。

RTSP (Real-Time Streaming Protocol) – リアルタイムメディアの転送に対する拡張制御。

SMTP (Simple Mail Transfer Protocol) – インターネットを介したメール送信のための標準プロトコル。ネットワークカメラはSMTPをサポートし、メール通知の送信を可能にしています。

SNMP (Simple Network Management Protocol) – スイッチ、ルーター、ネットワークカメラなどのネットワーク機器を、リモートで監視したり管理したりするために使用されます。SNMPのサポートにより、ネットワークカメラをオープンソースツールで管理することができます。

SIP (Session Initiation Protocol) – マルチメディア通信セッションのシグナリングおよび制御用通信プロトコル。

SSL/TLS (Secure Sockets Layer/Transport Layer Security) – クライアントとサーバー間における信頼性の高いプライベート接続をネゴシエートします。SSLは、一般的な規格であるTLSの前身です。

LLDP (Link Layer Discovery Protocol) – 装置および同じネットワーク内で接続されている他の装置の情報や機能を通知するために使用されます。

CIFS/SMB (Common Internet File System/Server Message Block) – 主にファイル、プリンター、シリアルポートへの共有アクセスやネットワーク上のノード間における、その他の通信を提供するために使用されます。

NTP (Network Time Protocol) – コンピューターのクライアントまたはサーバーの時刻を別のサーバーと同期させるために使用されます。

SFTP (Secure File Transfer Protocol) – 信頼性の高いデータストリーム上でのファイルアクセス、ファイル転送およびファイル管理を可能にします。

IGMP (Internet Group Management Protocol) – IPv4ネットワーク上のホストおよび隣接ルーターが、マルチキャストグループに参加するために使用します。こういったタイプのアプリケーションをサポートする際にリソースのさらに効率的な使用を可能にします。

5.2.4 データ転送プロトコル

TCP (Transmission control protocol) – シーケンス番号に基づいた信頼性の高いコネクション型のデータストリーム配信。最も一般的なデータ転送プロトコルです。

UDP (User Datagram Protocol) – コネクションレス型伝送サービス。信頼性よりもタイムリーなデータ配信を優先します。

ICMP (Internet Control Message Protocol) – 要求されたサービスが利用できないこと、またはホストやルーターにアクセスできないことを示すエラーメッセージおよび操作情報を送信します。

5.2.5 ユニキャスト、ブロードキャストおよびマルチキャスト

コンピューターネットワーク上でデータを送信する方法は、3つあります。

ユニキャスト - 最も一般的な方法で、送信者と受信者がポイントツーポイント方式で通信を行います。データパケットは1人の受信者にのみ送信され、他のクライアントにその情報が送信されることはありません。

マルチキャスト – ネットワーク上の送信者1人と複数の受信者間の通信。単一の情報ストリームを多数の受信者に配信することで、ネットワークトラフィックを軽減します。

ブロードキャスト- 送信者はネットワーク上の他のサーバーすべてに同じ情報を送信します。ネットワーク上のすべてのホストはそのメッセージを受信し、必要に応じて処理します。

5.2.6 QoS (Quaity of Service)

IPネットワークでは、各サービスの要件を満たすためにネットワークリソースの共有方法を制御する必要があります。

QoS (Quality of Service) – 重要なフローを優先度の低いフローよりも先に処理できるよう、ネットワークトラフィックに優先順位を付ける機能。アプリケーションが使用できる帯域幅の量を制御し、アプリケーション間における帯域幅の競合を制御する機能を提供することで、ネットワークの信頼性を高めます。

DiffServ – ネットワークは、各パケットによって指定されたQoSに基づいて、特定のサービスを配信しようとします。

73139/JA/R1/1904

Axis Communicationsについて

アクシスは、セキュリティの向上とビジネスの新しい推進方法に関する洞察を提供するネットワークソリューションを生み出すことで、よりスマートでより安全な世界の実現を目指しています。ネットワークビデオ業界をけん引するリーダーとして、アクシスは映像監視、インテリジェントアプリケーション、アクセスコントロール、音声システムなどに関連する製品とサービスを提供しています。アクシスは50ヶ国以上に3,000人を超える熱意にあふれた従業員を擁し、世界中のパートナーと連携することで、カスタマーソリューションをお届けしています。アクシスは1984年に創業し、スウェーデン・ルンドに本社を構えています。

より詳しい情報はwww.axis.comをご覧ください。

AXIS COMMUNICATIONS