第 II 部

制御ネットワークの IP 化

第 2 部
制御ネットワークの IP 化

第 1 章　はじめに

TACA ワーキンググループでは、PC のように豊富なリソースを持っていないデバイスがネットワークに接続される環境を想定し、それを可能とする技術の研究と開発を行っている。扱っている問題の例を挙げると、大量のデバイスをどのように運用・管理するか、計算能力の低いデバイスでいかにしてセキュリティーを確保するかなどである。具体的には PA（Process Automation）、BA（Building Automation）、FA（Factory Automation）等の制御ネットワークへの適用を想定している。

昨年度は、IETF において、IPsec 用鍵交換プロトコルである KINK の標準化を完了させた [208]。KINK は、認証に Kerberos[1] を用いるため、公開鍵暗号が必須でないため、計算能力の低いデバイスでも適応可能と考えている。

本年度は、12 月までに 7 回の定期ミーティング（議事録は WIDE Memo 化済み）を開催し、主に制御系ネットワークの運用に際して Kerberos の直面する課題に関しての研究を行った [293, 294, 295, 296, 297, 298, 314]。

具体的には、Kerberos の cross-realm に関する課題の解決である。大規模なシステムを管理する場合、それらを管理可能な領域に分割し、それらを連係させるのが、管理技術の常道である。Kerberos の場合は、管理領域をレルムと呼ぶ。現状の Kerberos では、異なる realm に属している機器間で通信を行う場合に、機器が多くの Kerberos メッセージを交換せねばならず、計算能力の制約された機器に適していない。

本年度は、IETF に以下の 2 種類の提案を行った。1) 上述した通り、現状の Kerberos の cross-realm の仕様が、計算能力の制約された機器に適していない、という問題提起を行った。2) 上記課題を解決するための Kerberos プロトコルの拡張に関する提案を行った。

第 2 章　活動内容の詳細

2.1 Kerberos の cross-realm 問題

まず、現状の Kerberos の cross-realm の仕様が、計算能力の制約された機器に適していないことを、IETF Kerberos WG へ問題提起した [209]。この結果、本課題の解決活動が、Kerberos WG の次期 charter 案に加えられた[2]。以下は、[209] の内容を元に、最新の調査を反映させたものである。

2.1.1 Kerberos の基本運用

Kerberos[171] は、鍵配布センター（Key Distribution Center）のモデルに基づく認証システムである。Kerberos の場合、そのサーバを一般的に KDC、管理領域をレルム（realm）、識別子をプリンシパル（principal）と呼ぶ。この認証サービスを受けるノードは、その識別子と秘密情報を KDC と共有する。

例えば、レルム X に属するノード A が、ノード Y と相互認証するためには、次の手順を必要とする（図 2.1

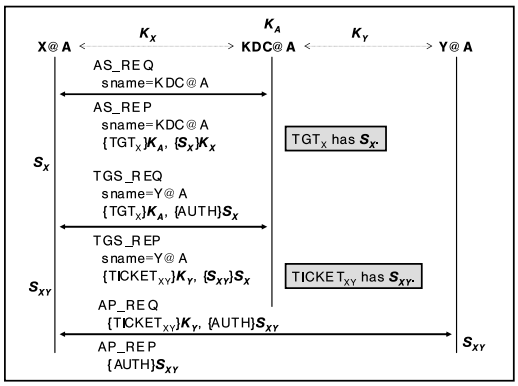

図 2.1. Kerberos の基本オペレーション

1　Kerberos is a trademark of the Massachusetts Institute of Technology (MIT).

2　http://www3.ietf.org/proceedings/06nov/slides/krb-wg-1.pdf

を参照)。まず、X は AS（Authentication Service）メッセージを用いて、TGT（Ticket Granting Ticket）を取得する。次に、X は TGS（Ticket Service）メッセージを用いて、サービスチケット $TICKET_{XY}$ を取得する。そして、X は AP（APplication）メッセージを用いて、Y との相互認証を完了し、KDC の生成したセッション鍵を共有する。

2.1.2 Kerberos の cross-realm 運用

大規模な管理領域を分割するのは、大規模システムにおける管理手法の常道である。Kerberos の場合には、KDC 間で秘密情報を共有することで、レルム間の信頼関係を構築する（図 2.2 を参照)。あるレルムに属するノードが、異なるレルムに属するノードと相互に認証するためには、cross-realm TGT と呼ばれる特殊な TGT を取得しながら、レルム間の信頼関係を辿り、最終的なサービスチケットを取得する（図 2.3 を参照)。

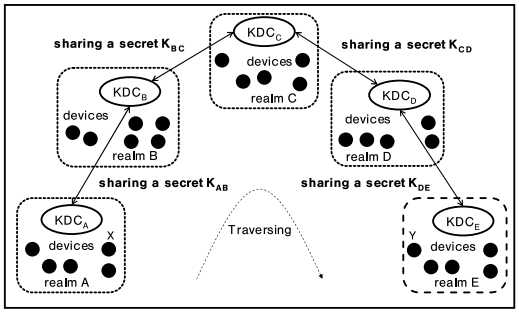

図 2.2.　Cross-realm における KDC の関係

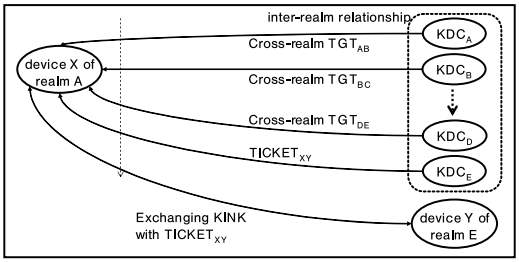

図 2.3.　Cross-realm のオペレーション

2.1.3 実プラントシステムの規模

典型的な PA（Process Automation）システムは、情報領域、制御領域、フィールド領域の 3 つから構成されている（図 2.4 参照)。情報層と制御層には Ethernet と IP が普及しているが、フィールド層では

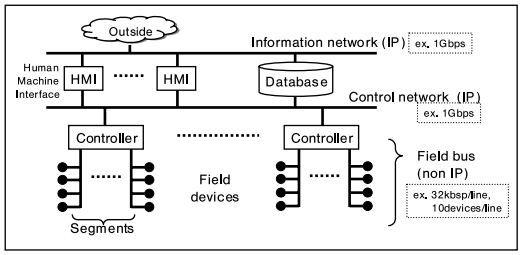

図 2.4.　PA システムの構造

FF（FOUNDATION Fieldbus）H1[3]や PROFIBUS[4] など、IEC61784[94] で定義されているネットワーク技術が使われている。このデータリンクは、32 k bps という低速性能であるが、100 m sec オーダのリアルタイム性能が要求される。以下では、実際に運用されている PA システムを例示する。

CSPC[263] は、CNOOC（China National Offshore Oil Corporation）と Shall Petrochemicals Company Limited の合弁企業であり、3.4 km^2 の規模を誇る最も巨大な石油化学プラントの一つである。本プラント（図 2.5 を参照）は、9 つのサブシステムから構成され、LAN で相互接続してる。システム全体では、120 個のコントローラ、3000 個のフィールドセグメント、16000 個のフィールドデバイスから構成され、2×10^5 個のタグと呼ばれる論理的な識別子を有する。

NAM（Nederlandse Aarodolie Maatschappij）[167] は Shell と ExxonMobile の合弁企業であり、オランダにおけるガス需要の 75%を供給する、巨大な液化ガスプラントを運用している。本プラントは（図 2.6 を参照)、863 km^2 の領域に分散した 26 のクラスターと呼ばれるサブシステムから構成される。各クラスターは、500〜1000 個のフィールドデバイスと数百のフィールドセグメントを持つ。クラスターは、プライベートな WAN で相互接続している。システム全体では、10^6 個のタグと呼ばれる論理的な識別子を有する。

本研究では、これらのシステムに Kerberos を用いることで、機器の通信にネットワークセキュリティを導入することを目指している。Kerberos を利用するにあたり、以下を仮定する。

1. フィールド領域を含めて、システム全体で IP をネットワーク層のトランスポート技術とする。
2. 従って、フィールドデバイスを含むシステム全ての機器は、IP で通信を行う。

3　FOUNDATION Fieldbus is a registered trademark of the Fieldbus Foundation.
4　PROFIBUS is a registered trademark of PROFIBUS International.

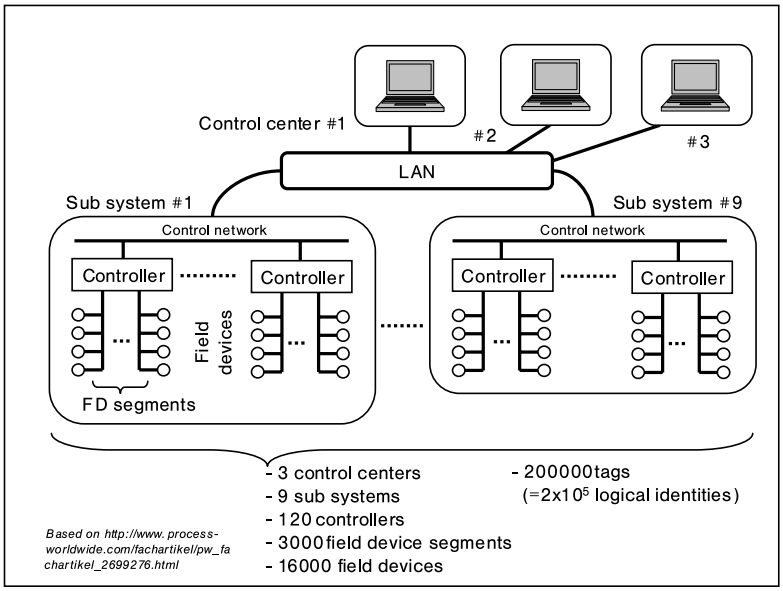

図 2.5. CSPC[263]

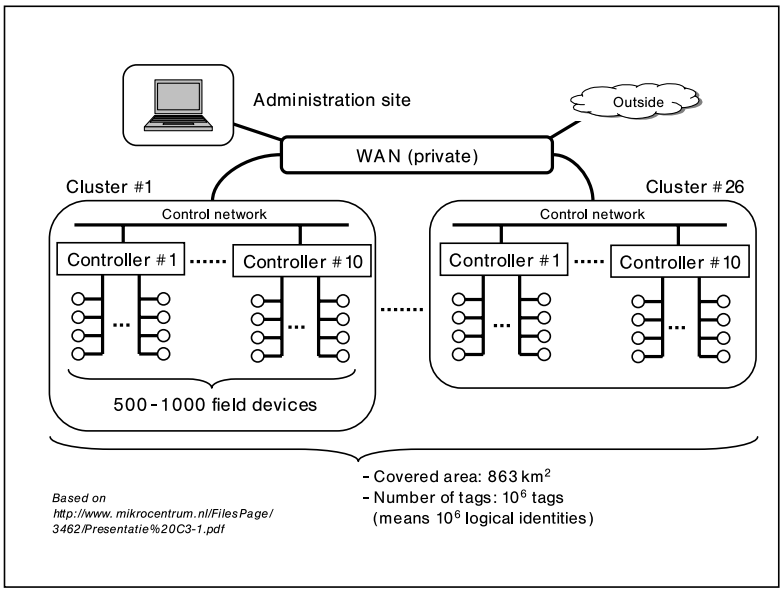

図 2.6. NAM[89]

3. 更に、フィールドデバイスを含むシステム全ての機器の通信は、Kerberos で相互認証し、Kerberos 化されたセキュリティで守る。
4. この結果、Kerberos が扱う規模は以下となる。
   (a) 数十以上の管理領域
   (b) 数万以上の機器
   (c) 数百万以上の識別子

次項では、これらのシステムに Kerberos を導入した場合に、cross-realm 運用に求められる要求と制約、および直面する課題について述べる。

2.1.4 要求と制約

本項では、前項で述べた事例に基づき、管理領域の分割に対する要求を示す。R1〜R3 は、分割管理に対する一般的な要求である。一方、R4〜R6 は、上述した大規模プラントを考慮した場合に要求される項目である。

R1 互いに独立した管理領域が同一システム上に共存できること。

R2 ある管理領域が、その管理権限を別の管理領域に委譲できること。

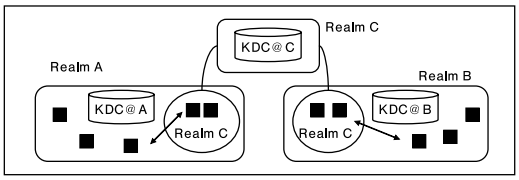

図 2.7.　運用：出島モデル

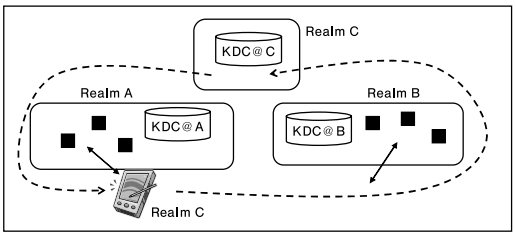

図 2.8.　運用：ローミングモデル

R3 異なる管理領域に属する機器同士が、通信できること。

R4 同じ管理領域に属する全ての機器のネットワーク的又は物理的距離が近いとは限らない。

R5 ある管理領域下にあるネットワーク上に存在する全ての機器が、その管理領域に属しているとは限らない（図 2.7 を参照）。ある機器は、異なる管理領域に属しているにも関わらず、そのネットワーク上に存在し、他の機器と通信できねばならない場合がある。例えば、プラント内の一部の機器の管理が、アウトソースされ外部組織により、遠隔で管理されている場合が考えられる。

R6 これは、R5 の派生形である。ある管理領域に属する機器が、一時的に異なる管理領域下のネットワークに出現し、他の機器と通信せねばならない場合がある（図 2.8 を参照）。例えば、プラントの管理部門に属する測定機器が、プラントを巡回する場合などである。

一方、システムに複数管理領域を導入する場合、以下の制約を考慮せねばならない。

C1 システムの管理コストを、できるだけ削減できること。

C2 一般的に採用されている防火壁によるセキュリティ対策は、IP や無線技術の普及に伴い、不十分になりつつある [212]。従って、機器間の通信は、秘匿性（confidentiality）と完全性（integrity）を保証せねばならない。更に、DoS（Denial of Service）攻撃を考慮せねばならない。

C3 システムを構成する機器の多くは、計算能力の限定された CPU を使っていることを考慮せねばならない。例えば、典型的な組込み CPU の性能は、一般的な PC と比べて 10^{-6} 程度しかない。生産システムには引火性ガス環境下で運用する場合もあり、防爆などの安全基準がある[5]。これらの基準は、機器が使える総エネルギー量を規制しているため、フィールドデバイスの計算能力の向上に対する制約となる。

C4 フィールドデバイスに要求するトラフィック量をできるだけ少なくする必要がある。なぜなら、上述した安全基準は通信帯域の向上に対しても制約となる。例えば、Ethernet は防爆基準を満たしていない。しかも、その制約下で 100 msec のリアルタイム性を保証せねばならない。

2.1.5 課題

上述したシステムに対して cross-realm を導入すると、下記の課題が生じる。

I1 Unreliability of authentication chain
レルムが図 2.2 の様に連鎖している場合、もし中間の KDC 自身の故障や KDC への到達性が失われると、最終レルムへ到達することができなくなる。

I2 No PFS (Perfect Forward Secrecy)
[30] は cross-realm の脆弱性を指摘している。レルムが図 2.2 の様に連鎖している場合、もし中間の KDC が汚染されると、cross-realm 環境下にある Kerberos で守られた通信の PFS[6]が保証できなくなる。

I3 Scalability of the direct trust model
レルム同士を階層構造などにすると信頼性やセキュリティに関して様々課題が生じる（I1 と I2 を参照）。これを解決するためには、レルム同士をフルメッシュで関連付けることが考えられる。しかし、KDC 間で共有する秘密情報の量は、レルムの数 n の二乗となり、管理コストを増大させる。

I4 Exposure to DoS Attacks
cross-realm 運用を行う場合、KDC を他レルム

5　この安全基準は国別のものである。日本では、電気設備技術基準などが、それに該当する。これらの安全基準は IEC60079[93] に基づいている。

6　PFS の定義は、RFC2409 の 3.3 節を参照のこと。

から到達可能にする必要があるため、KDC を外部に露出させることが必要になる。R4 の場合、機器間の通信が同一レルムの範囲内であったとしても、KDC はネットワーク的に露出せねばならない場合も考え得る。R5 や R6 の場合、自分と異なるレルムに visiting している機器が Kerberos 認証を使う場合には、自分の所属している KDC（ホーム KDC と呼ぶ）への到達性が必要であり、このホーム KDC を外部へ露出する必要が生じる。外部へ露出した KDC を DoS 攻撃や不正アクセスから守るためには、KDC 自身でのアクセス制御や関連する防火壁の設定が必要であり、管理コストを増大させる。

I5 Client's performance

図 2.3 が示す通り、cross-realm で必要な cross-realm TGT のためのメッセージ交換の数は、辿るレルムの数に比例する。これらのメッセージ交換には、暗号処理が必要となる。一方、プラントシステムに多数存在するフィールドデバイス等の計算資源は限定されているため（C3）、暗号処理が必要な Kerberos のメッセージ交換は大きな負担となるため、メッセージ交換の数をできるだけ少なくせねばならない。表 2.1 に、組込み機器で実装した Kerberos メッセージの処理時間を示す。これらの処理時間は、純粋な処理時間であり、パケットの待ち時間は含まれていない。

I6 Pre-authentication problem in roaming scenarios

R5 や R6 の場合、他レルムを訪れた機器がそこの機器と通信するために最初に必要なのは、自分の属する KDC（ホーム KDC）から cross-realm TGT を取得することである。しかし、両レルムが cross-realm の信頼関係を確立したとしても、訪れたレルムからホーム KDC への到達性はないかもしれない（例えば、訪れたネットワークのセキュリティポリシーなどにより）。すなわち、実際に行われている運用形態を考慮すると、単にレルム間の信頼関係を確立しただけでは、cross-realm の運用を行えない場合が存在する。

表 2.1. 組込み機器における Kerberos メッセージ処理時間（msec、H8/3029@20 MHz）[181, 182]

Source	MIT-1.2.4		Original	
Crypt H/W	w/	w/o	w/	w/o
TGT	74	106	26	47
TGS	195	294	49	178

2.2 cross-realm 問題を解決するための Kerberos 拡張提案

次に、IETF Kerberos WG で提起した cross-realm の課題 [209] を解決するために、Kerberos プロトコルの拡張に関する提案を同 WG へ行った [284, 285]。本提案は、2.1.5 節で述べた課題（I1〜I6）を解決しようとするための手法の一つである（図 2.9 を参照）。

しかし、本提案以外の手法でも、上記課題を緩和することができる。具体的に課題を解決するためには、解決手法の整理と評価を行わねばならない。

2.2.1 XAS プロトコル

XAS プロトコルは主に、ローミングユーザが訪問先のアクセスネットワークに接続する場合に、ホーム KDC にアクセスできないという問題を解決するためのプロトコルである。多くのネットワークでは認証されたクライアントのみに接続を許すという運用が行われているが、このような環境では Kerberos 認証を利用することが難しい。なぜなら、Kerberos では認証のためのチケットを取得するために、ホーム KDC にアクセスする必要があるからである。つまり、認証を受けるためにはネットワーク接続が必要である一方、ネットワーク接続を得るためには認証が必要であるという、循環依存問題が発生する。

XAS プロトコルでは、訪問先 KDC がホーム KDC へ AS メッセージ（Kerberos の初期チケットを取得するメッセージ）をプロキシし、協調して認証やチケットの発行を行うことで、これを解決する。

認証前の時点では、ローミングクライアントは外部ネットワークへの接続性をもっておらず、ホーム KDC にアクセスできないため、訪問先 KDC に対して XAS プロトコルによる認証を要求する。訪問先 KDC は XAS プロトコルを用いてホーム KDC と通信し、訪問先レルムにおけるクレデンシャルを発行する。そのクレデンシャルは、訪問先 KDC が発行したチケットと、ホーム KDC が当該クライアント向けに暗号化したセッション鍵からなり、それを用いてクライアントは訪問先レルムで直接認証を行うことができるようになる。

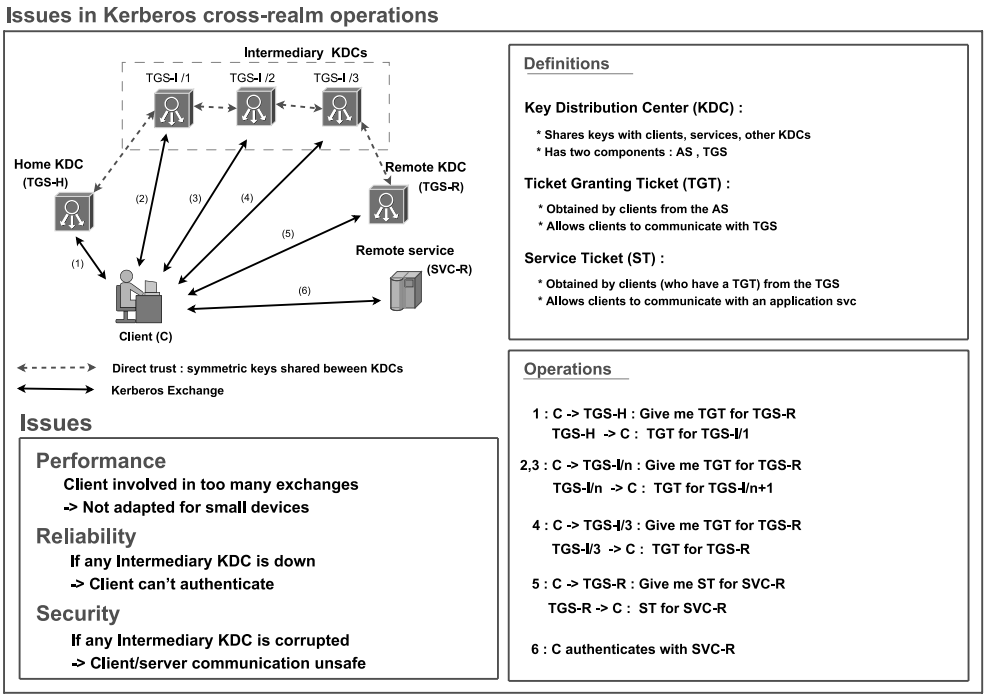

図 2.9.　Issues in Kerberos cross-realm operations

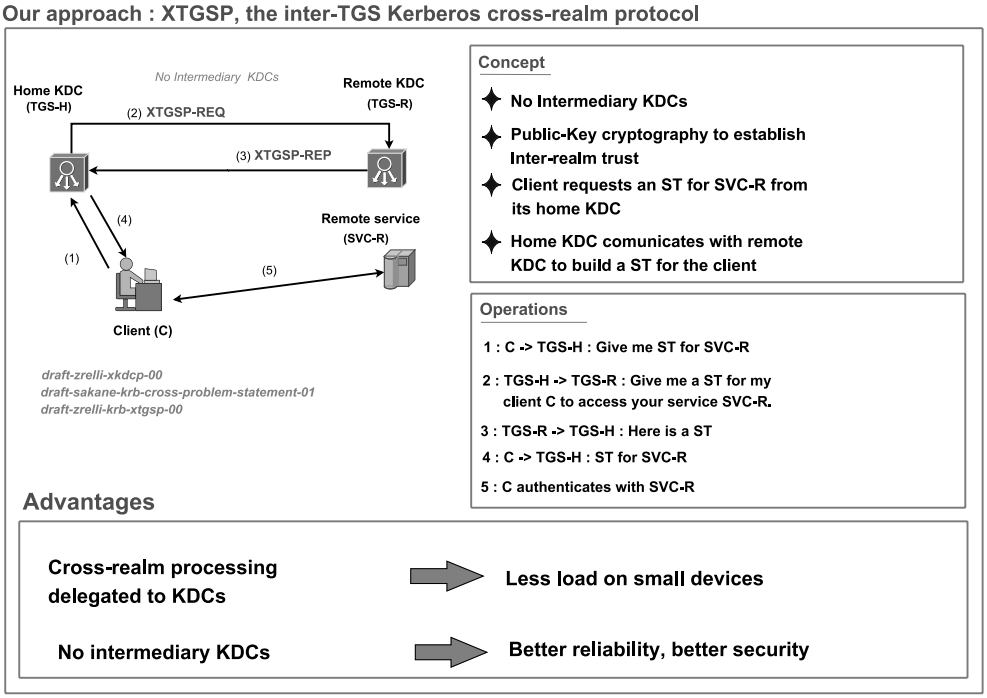

図 2.10.　XTGS プロトコル

2.2.2 XTGS プロトコル

XTGS プロトコルは、クライアントがレルム間の認証パスをたどることなく、手元の KDC から直接サービスチケットを入手するプロトコルである。ここで「手元」とは、自分がすでに TGT を持っているレルムの KDC のことを指すものとする。すなわち、通常は自レルムの KDC であり、XAS によって TGT を入手した場合は訪問先 KDC である。

XTGS プロトコルの概要を図 2.10 に示す。XTGS においては、クライアントは直接手元の KDC に、遠

隔レルムのサービス宛のチケットを要求する。要求を受けたKDCは、公開鍵認証を用いて遠隔KDCにアクセスし、必要な情報を取得した後にサービスチケットを生成する。

XTGSを用いたサービスチケットの取得は、通常のTGSと同様、クライアントが手元のKDCに遠隔レルムへのチケットを要求することから始まる。このとき通常であればcross-realm TGTを要求するが、XTGSクライアントは最初から遠隔サービスのサービスチケットを要求する。手元のKDCはクライアントを認証した後、XTGSプロトコルによって遠隔KDCと通信を行い、遠隔レルムにおけるクレデンシャルを直接生成する。クレデンシャルの生成はXASプロトコルの場合と類似しており、遠隔KDCがチケットを発行し、手元のKDCがそのセッション鍵をクライアント向けに暗号化することで、このように手元のKDCが遠隔レルムのチケットを直接発行することが可能になっている。

第3章　まとめ

TACAワーキンググループでは、産業分野（PAやBAやFAなど）のシステムにおけるIPとセキュリティの適用に関する研究と開発を行っている。具体的なセキュリティ技術としては、Kerberosに基づいたものを想定している。

今年度は、1) 実際に稼働している大規模PAシステムから導いた要求に基づき、Kerberosのcross-realm運用に関する課題を明らかにし、2) それをIETF Kerberos WGへ問題提起し、3) その解決案としてのXASプロトコルとXTGSプロトコルを同WGへ提案した。この結果、課題の解決活動が、同WGの次のcharter案に加えられた。

しかし、本提案以外の手法でも、上記課題を緩和することができる。今後は、具体的に課題を解決するためには、解決手法の整理と評価を行う予定である。