ATN のセキュリティ

航空システム部　　※板野 賢、　　＊塩見格一
＊管制システム部

1.まえがき

ATN（航空通信網）は、従来個別に行われていた航空におけるデータ通信をビット指向型のデータ通信に統一し、航空通信用のインターネットを構築して行くものである。

ATN の SARPｓ（標準化及び勧告方式）は、コアパート（第 10 付属書の改定部分）と Doc.9705 と呼ばれる技術書で構成されている。Doc.9705 は 2000 年に改訂され、従来は５分冊であったが現在は９分冊になった。追加された内容は「ATN セキュリティ」「システム管理」「ディレクトリー・サービス」「ATN 登録」である。

当所では 1996 年版の Doc.9705 に沿って実験システムを構築し、海外の試験機関との接続実験などによって、ATN 用のアプリケーション、プロトコルおよび IS（中間システム）等の開発ならびに評価・検証を行ってきた[1,2]。本講演では、2000 年の改訂に対応することおよび近年増加傾向にあるテロへの対策のため現在開発中の「ATN セキュリティ」について報告する。

2.ATNセキュリティの概要

ATN では下記の脅威に対してセキュリティ対応が必要となる。

①通信媒体のモニタリング
②ネットワークや特定の伝送媒体の妨害や殺到
③メッセージのアドレス情報や内容の変更（改竄）
④なりすまし
⑤メッセージの再生
⑥ネットワークのルーティング情報の変更

ATN セキュリティサービスでは、③、④、⑤、⑥をセキュリティ対象とする。

項番①に関しては、単に通信媒体のモニタリングするだけなら問題はないのでセキュリティ対象外とする。また、項番②のような物理的なセキュリティは、各国のポリシーによって実装されるべきことなのでセキュリティ対象外とする。

このため、ATN セキュリティサービスには次の要求事項が必要とされる。

(1) アクセス制御

アクセス制御は、ATN リソースの無許可な使用を防止する。

(2) 認証

認証は、要求者として参加しているエンティティの身元を保証する。

(3)データ完全性

データ完全性は、ATN データが無許可な方法で、変更あるいは破壊されていないことを保証する。

図 1 は空対地の通信の概念を示す。ATC の空対地の通信は、ATS（航空管制業務）ドメインの ATS-ES（エンドシステム）と航空機ドメインの機上 ES 間で行われる。これら異なるドメイン間の通信は必ず BIS（境界型中間システム）と呼ばれる特殊な IS を介して行われる。また、図 1 で航空機ドメインと ATS ドメイン間で相互に通信可能な状態になると言うことは、航空機 BIS と A/G-BIS 間でリンクが確立して相互通信可能にな

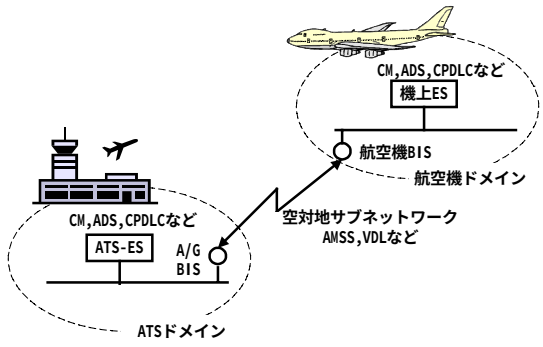


図１　空対地の通信の概念図

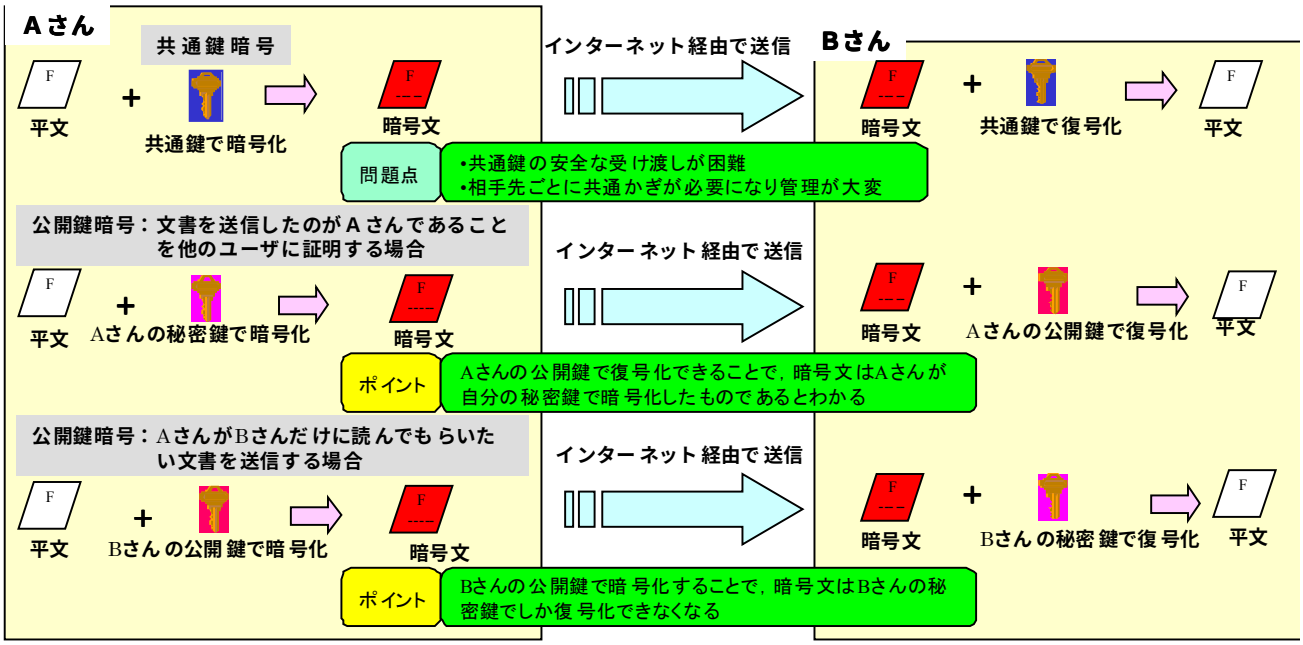


図２　暗号化と複合の手順

ることである。

偽の管制官や偽のパイロットを排除すると言うことは、偽の航空機ドメインや偽の ATS ドメインを排除することに他ならない。BIS 間のリンクを確立する際、BIS は相互に経路情報などの交換を行う。従って、これらの情報交換の際に電子署名技術を用いて互いに相手の正当性を確認することで、偽のドメインを排除することが可能になると考えられる。

また、ATN ではドメイン間のリンクが確立すると、通常は最初に CM（コンテキスト・マネジメント）アプリケーションが用いられる。CM によりお互いにどのようなアプリケーションが使用可能であり、アプリケーション毎にコンタクトすべき相手のアドレスを知ることができる。CM 間でやり取りする情報にも電子署名を用いることでセキュリティ・レベルを上げることが可能である。以上の方法が ATN でのセキュリティ対策の基本的な考え方である。

ATN では空対地アプリケーションには他にも CPDLC（管制官・パイロット間データリンク通信）や ADS（自動従属監視）などがある。これら個別のアプリケーション毎に電子署名や暗号化技術を用いてセキュリティ・レベルを上げることはもちろん可能である。しかし、空対地サブネットワークのデータ伝送速度は現時点では限られるので、現在のところこれら個別のアプリケーション毎に暗号化や電子署名を用いることは考えられていない。

3.BISのセキュリティ対策

暗号方式には表１示す共通鍵暗号と公開鍵暗号の２種類の方式がある。共通鍵暗号は通信者毎に個別の共通鍵が必要で、このため共通鍵の管理が困難である。しかし、一般に共通鍵暗号は公開鍵暗号に比べて高速に暗号化・複合化が可能とされる。

表１　暗号方式

分類	概要	暗号方式
共通鍵暗号方式	暗号化と復号に同一の鍵を利用し，暗号化鍵を公開しない。「対称暗号方式」，「秘密鍵暗号方式」，「慣用暗号方式」とも呼ばれる	DES，Triple-DES，AES，IDEA
公開鍵暗号式	暗号化鍵と復号鍵が異なり，暗号化鍵を公開し，復号鍵を秘密にしておく暗号方式である。「非対称暗号方式」とも呼ばれる	RSA，ElGamal 暗号，楕円曲線暗号

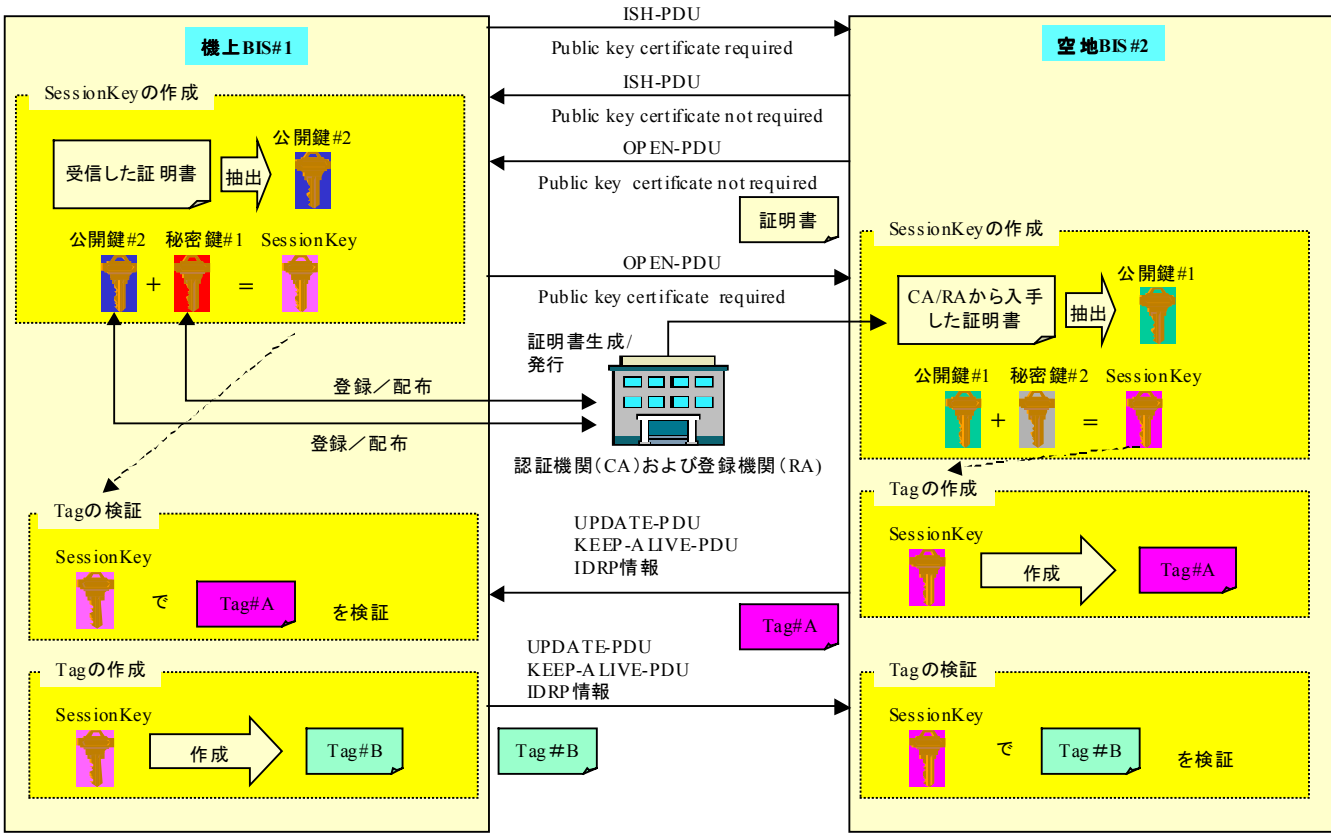


図３　ＢＩＳにおけるセキュリティ・アイテムの使用例

このため、データ部分の暗号化には共通鍵方式を用い、その鍵を安全に配送する手段として公開鍵暗号方式を組み合わせる場合が多く、ATN もこの方式を用いている。

図 2 に暗号化と複合化の手順を示す。暗号と署名は表裏一体の技術である。公開鍵方式では、送信者 A が身元を保証したい場合（署名）は、A の秘密鍵で通信文を暗号化する。受信者 B は予め配布された A の公開鍵で通信文を複合化することで、通信文は A のものだと言うことが分かる。送信者 A が受信者 B 以外には文章を秘密にしたい場合（暗号）は、予め配布された B の公開鍵で通信文を暗号化する。この暗号文は B の秘密鍵でしか複合化できないので、B 以外には解読できない。

不特定多数の通信では、通信者以外に身元を保証するための第三者機関が必要になる。公開鍵基盤では認証機関（CA）/登録機関（RA)がこれにあたり、証明書（公開鍵と人が関連付けられていることを証明するもの）の発行の可否を審査し、証明書および鍵を配布する。

図３は BIS におけるセキュリティ・アイテムの使用例を示し、相互に認証し、地上側は航空機の証明書を CA/RA から受け取り、航空機側は地上側から直接証明書を入手する（身元の確かな相手との通信では必ずしも CA/RA を通す必要は無い）場合の手順を示す。ここで、公開鍵および秘密鍵は予め CA/RA に登録されているものとする。

各 BIS は入手した証明書から相手の公開鍵を抽出し、自分の秘密鍵とで共通鍵となる SessionKey(MacKey とも呼ばれる)を作成する。この作業が OPEN-PDU（インター・ドメイン・ルーティング・プロトコル {IDRP} が使用するメッセージの一つ）の交換までに行われる。以後の通信では送信側が SessionKey で作成した Tag を IDRP 情報に付加し、受信側は同じ SessionKey で Tag を検証することで署名の役割をはたす。

CA/RA は証明書や CRL（証明書失効リスト）の生成・配布に必要な機関であるが、現在は証明

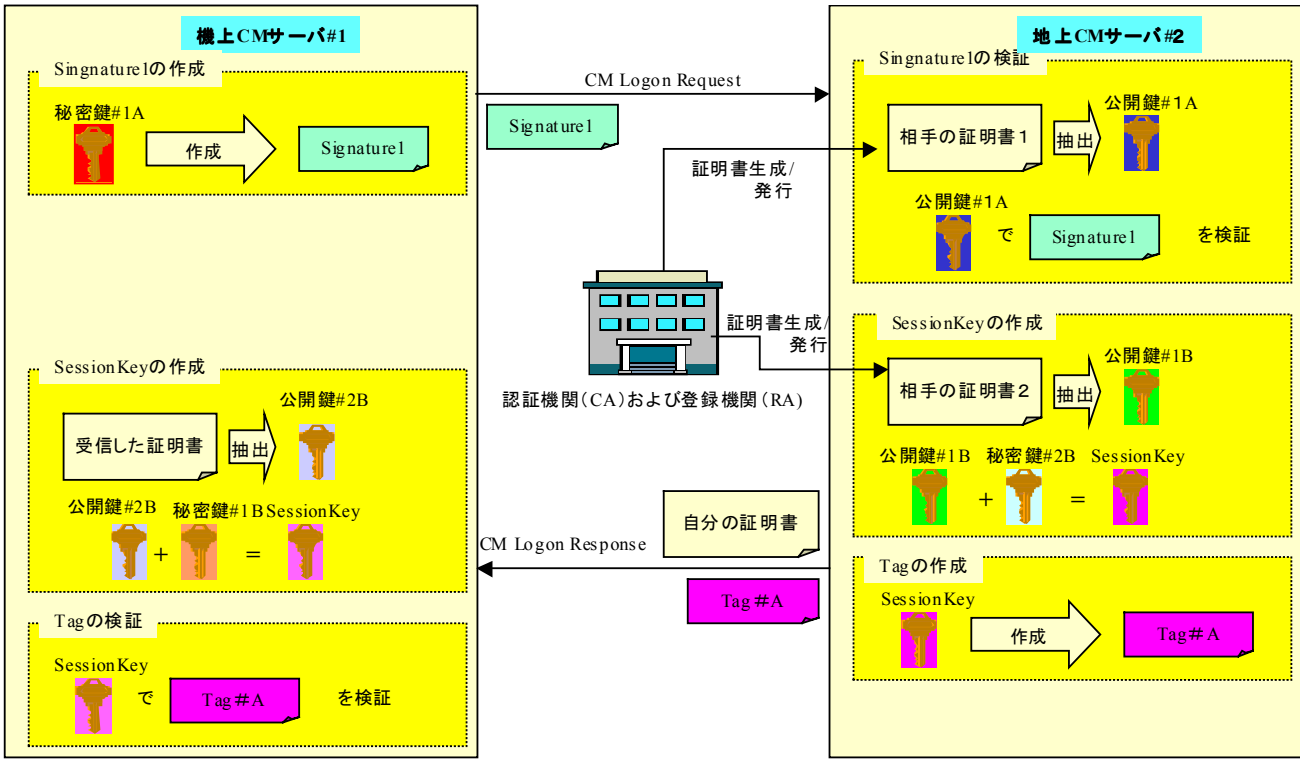


図４　ＣＭのセキュリティ・アイテムの使用例

書がどのような形で配布される未定である。また、CA/RA が BIS 間の通信にどのように介在するかも未定である（例えば、航空機側も CA/RA から証明書を入手するべきかなど）ので、試作した BIS は CA/RA との delivery service には対応していない。

4.CMのセキュリティ対策

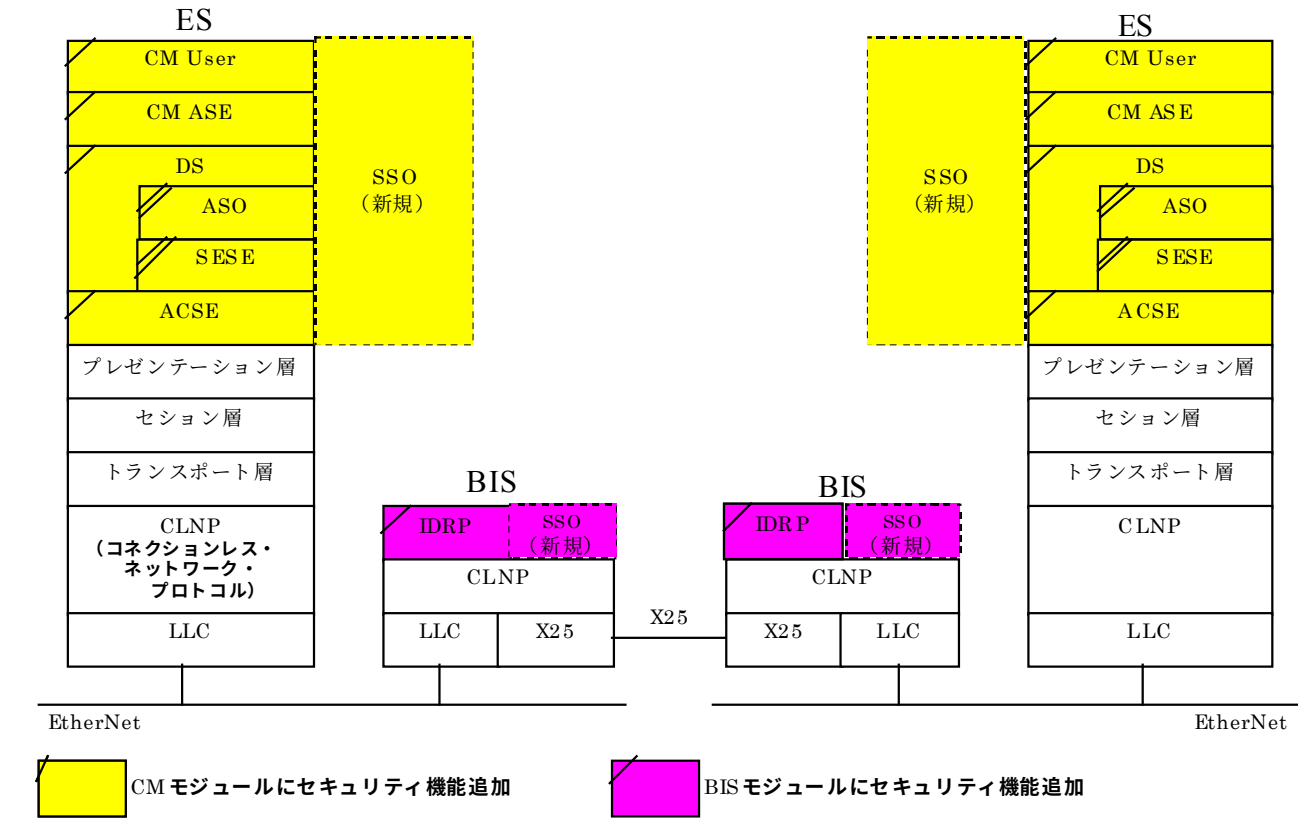
図 4 に CM のセキュリティ・アイテムの使用例を示す。機上 CM サーバはログオン要求に秘密鍵#1A（秘密署名鍵）を用いて署名（Signature 1）を付加する。地上 CM サーバは CA/RA を通じて航空機の証明書を手に入れる。この証明書は 2 通有り、証明書 1 から相手の公開鍵#1A（public signature key:公開署名鍵）を抽出して相手の署名（Signature 1）を検証する。また、証明書 2 から公開鍵#1B(public key agreement key:公開鍵合意鍵）を抽出して自分の秘密鍵#2B（秘密鍵合意鍵）とで SessionKey を作成する。

地上 CM サーバは SessionKey を用いて Tag#A を作成し、航空機にログオン応答を返すときに自分の証明書と Tag#A を付加する。機上 CM サーバは受け取った証明書から公開鍵#2B を抽出して自分の秘密鍵#1B（秘密鍵合意鍵）とで SessionKey を作成する。SessionKey で Tag#A を検証することで署名の役割をはたす。

なお、図 4 に示す手順で SessionKey を求めると毎回同じものになる。これは前節の BIS の場合も同様でセキュリティ上望ましくない。これを回避するため、実際にはお互いにランダムな数を相手に送る。この 2 つのランダムな数から共有秘密数(shared secret value)が得られる。SessionKey の作成を、相手の公開鍵、自分の秘密鍵、共有秘密数から行うことで毎回異なる SessionKey が得られる。同じ形の方程式から解を求めるとき、定数項が毎回変わっていれば得られる解も毎回異なるのと同様である。また、暗号化の関数（Hash 関数）には楕円曲線関数を用いる。

5.セキュリティ機能の実装

図 5 に新たに製作した実験システムのプロトコル・スタックを示す。セキュリティ機能を実装す



・ACSE：アソシエーション制御サービス要素。
・DS：ダイアログ・サービス。セキュリティ機能使用時/未使用時の切替機能やASOとのインタフェース機能を追加。
・ASO：応用サービス・オブジェクト。SSOやSESEとのインタフェース機能などを実現するため新規製作。
・SSO：システム・セキュリティ・オブジェクト。セキュリティ・アイテムの生成と検証を行うサービスで新規製作。
・SESE：セキュリティ交換サービス要素。認証情報や鍵を通信相手のアプリケーションと交換する機能で新規製作。
・CM：セキュアな通信を実現するために、既存サービスプリミティブのセキュリティに関する機能拡張。
・IDRP：BIS確立及びルーティング情報交換時のセキュリティ機能に関して機能拡張。

図５　セキュリティ機能を充実したＡＴＮのプロトコル・スタック・

ることにより、従来のプロトコル・スタックから変更があった部分は、ES 側では応用層の部分である。応用層以外の上位層、トランスポート層以下の部分には機能的な変更はない。応用層で機能的な変更がある部分は、ACSE（アソシエーション制御サービス要素）と DS（ダイアログ・サービス）で、これらは全ての空対地アプリケーションで用いられる。

DS は、セキュリティ機能の使用時と未使用時の切り替え機能や、新規の機能である ASO（応用サービス・オブジェクト）とのインタフェースが必要になる。ASO は同じく新規の機能である SESE（セキュリティ交換サービス要素）や SSO（システム・セキュリティ・オブジェクト）と DS のインターフェース機能などを実現するためのものである。SESE は SSO で生成・検証される認証情報や署名などのセキュリティ・アイテムを相手のアプリケーションやエンティティと交換する機能である。SSO はセキュリティ・アイテムの生成と検証を行うサービスで、ATN-OSI プロトコル・スタックの外にある。我々は暗号化や電子署名のモジュールを試作した経験は無いので、SSO の実現には ATN セキュリティに適合した市販のモジュールを用いた。

BIS での変更箇所は 3 層のルーティング・プロトコル IDRP の機能拡張が主になり、リンク確立およびルーティング情報の交換時にセキュリティ機能を使用できるように機能拡張した。ここでも、

セキュリティ・アイテムの生成や検証はSSOが行う。また、BISがATNセキュリティに対応しているかどうか、証明書が必要かどうか等の情報の交換は、ISH（中間システム・ハロー）の交換で行われる(図3参照)。ISHはIDRPではなくES-ISプロトコルが使用するメッセージであるのでES-ISプロトコルの改修も必要である。

ATNセキュリティ機能は、平成13年度から設計を行い、平成14年度に試作した。図5に示す構成で所内で行った実験では、セキュリティ・アイテムの交換や署名やTagの検証も正常に行える。

5.まとめ

以上、ATNのセキュリティ対策について述べた。平成14年度はBISおよびCMのセキュリティ機能の製作を行い、現在動作確認中である。所内の実験では、セキュリティ・アイテムの交換や署名やTagの検証も正常に行える。しかし、諸外国で製作されたものとの互換性・相互接続性を確認するためには、今後、国際間での接続実験が必要である。

平成15年度は、当所で試作中のVDLモード3実験システムと ATN 実験システムとの接続を行う。平成16年度にはVDLモード3実験システムを用いた評価実験を行いたい。評価実験では、本研究で試作開発中である DFIS（デジタル・フライト情報業務）やCMなどのアプリケーションの性能評価をセキュリティの有無に応じて行いたい。

参考文献

(1) 板野賢、塩見格一:“航空通信網(ATN)の研究”,電子航法研究所報告No.100,2003.2.

(2)板野賢、塩見格一：“ATNの国際接続実験について”,第31回電子航法研究所発表会概要,平成11年6月.