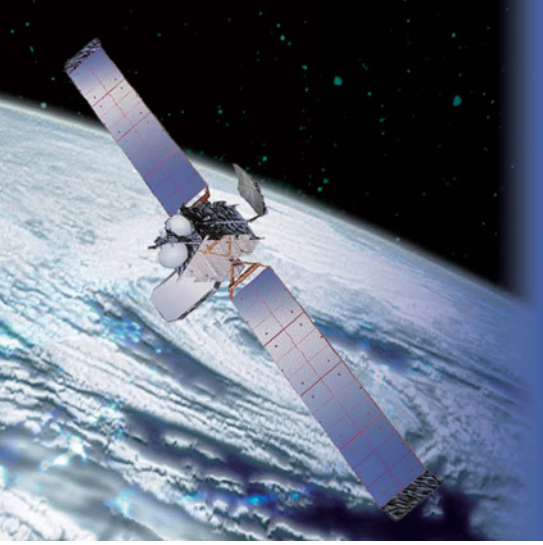


Lascom News

ラスコム・ニュース
2010-10 No.42

地域衛星通信ネットワーク

公的個人認証サービスセンター

全国知事会議in和歌山（全国知事会）

Lascom 財団法人 自治体衛星通信機構

一斉指令回線の増速

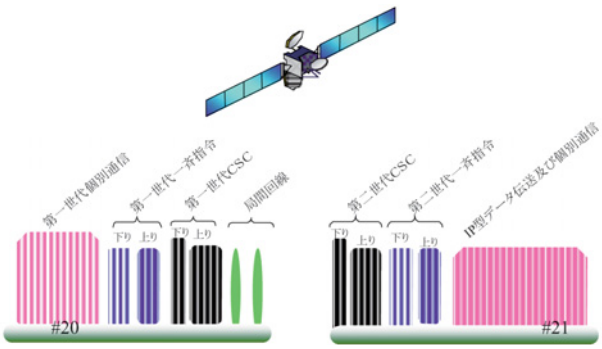
機構では一斉指令回線の増速について検討した結果を平成22年度・地域衛星通信ネットワーク担当者連絡会議において、次の４点にまとめ報告いたしました。

●割当帯域は、上下合計で400KHz以下とする
●隣接チャネル等に干渉を与えないこと
●料金は無料とする
●その他詳細については、当機構と事前に打合せること

◇一斉指令回線の現状

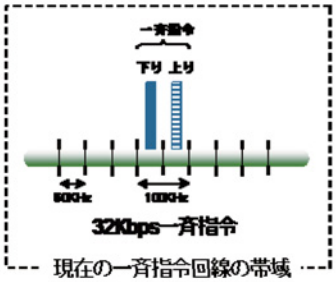
一斉指令回線は、消防庁に割当てられた一斉指令回線と各都道府県に割当てられ、親局である都道府県庁局から各市町村等へ下り回線を用いて、音声、FAX、IPデータを一斉配信する２つに分類されます。また、上り回線を利用して、小容量のデータ収集も可能となっています。

第一世代の一斉指令回線は音声とFAXが、第二世代では音声・FAXに加えてIPデータの配信が可能となっています。第一世代を利用している37県は#20トラポン上に割当され、第二世代を利用している12県は#21トラポンに配置されています。（３県が両方を利用中）



図－１　#20、#21トラポンのキャリア配置

一斉指令回線は第一世代、第二世代いずれの回線もベースバンドの伝送速度は32kbpsで、上り下り合わせて100kHzの帯域を使っています。



図－２　一斉指令回線の上下キャリア配置

第二世代ではIPデータを扱えることから、IPデータの高速配信や上り回線を利用したデータ収集（計測地震計等）の時間短縮ニーズが高まり、伝送速度の増大が求められるようになりました。機構では、伝送速度の増速のニーズに応えるため次の３点の検討を行いました。

①トラポン割当

伝送速度を増速した場合、当然それに比例して帯域が増大しますが、現状のトラポン帯域内で増速した帯域の割当が可能かどうか？

②伝送方式

現在の伝送方式は第一世代の技術を継承していますが、その後の技術進歩により誤り訂正等の性能が向上しており、それらの技術を採用することで、伝送容量の効率的な増大や降雨に対するマージンの増大など、一斉指令回線の性能向上に寄与することが考えられます。これらを採用した新しい伝送方式を如何にするか？

③運用方法

前項で、新しい伝送方式が採用された場合に山口管制局による監視をどうするか？

◇トラポン割当

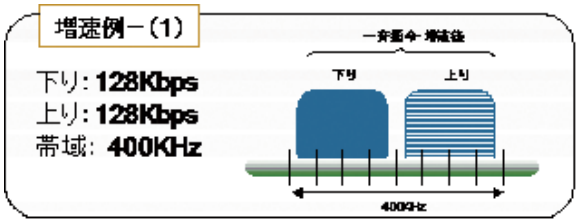
機構では現在３本のトラポンを利用しています。#19トラポンで５chのデジタル映像を、#20トラポンは主に第一世代の個別通信・一斉指令・準動画を#21トラポンでは第二世代の個別通信・一斉指令・IP伝送等に利用されています。

#19トラポンのデジタル映像は災害時に５chが

全て利用される（チリ沖地震等）ことから、#19トラポン上に新たな一斉指令回線の割当を行わず、#20、#21トラポン上から割当ることを検討しました。前提条件として大規模災害時に想定される個別通信帯域等を確保することを念頭に検討した結果、高速IPデータの帯域等を若干狭めて運用することで、現状の一斉指令回線の帯域を４倍、１県あたり400kHzとすることが適当であるとしました。

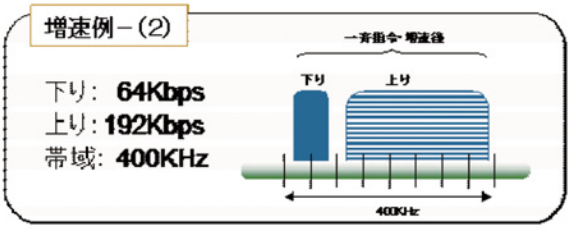
◇伝送方式

現在の都道府県一斉指令回線は変調方式や多重方式などを消防一斉指令と同じ方式を採用しています。前項にあるように増速のために帯域を４倍とした場合、現状の変調方式や多重方式をそのまま継承し、伝送速度を４倍の128kbpsへ増速することも可能です。（図－３参照）



図－３　帯域４倍　利用例（上下対称）

上下非対称として、下り回線の伝送速度を大きくする配信重視の回線構成や、地震データ等を高速に短時間で収集するため、上り回線の伝送速度を大きくする回線構成も考えられます。（図―４参照）、



図－４　帯域４倍　利用例（上下非対称）

さらに、最新の誤り訂正や変調技術等を採用することにより、現在の一斉指令回線に比べて帯域あたりより大きな情報量を伝送する、あるいは降雨に強い回線とするなど、目的に合わせた伝送方式の採用が可能となっています。

都道府県一斉指令回線は各都道府県内に閉じた回線であるため、機構として統一仕様とするメリットよりも、各都道府県が利用形態や環境に合わせた最適な伝送方式を採用するメリットが大きいと判断して、伝送方式を規定しないことにいたしました。（帯域だけを最大400kHzとして規定）

◇運用方法

前項で説明したように、一斉指令回線の伝送方式を機構の標準規格として規定しないため、現状の仕様を４倍に拡張した仕様も含めて、各都道府県が独自の方式を採用することになります。あらたな伝送方式で#20トラポン、#21トラポンの上に割当される新一斉指令回線は、既存のキャリアを始めとして他のキャリアに干渉等を与えないこと、配分されたキャリア帯域・電力等を守ることなど、適切な運用が求められます。そのため、導入する際には、事前に機構とキャリア配置や電力、隣接キャリアとのガードバンドなど運用全般について打ち合わせをお願いいたします。

また、山口管制局では、標準規格の一斉指令端末を整備して、一斉指令回線のモニターを行い各都道府県の運用をサポートしておりますが、今後、各都道府県が独自の方式を採用した場合、山口管制局において従来同様にモニターできるよう、各都道府県が導入した一斉指令端末の貸出をお願いいたします。

◇まとめ

一斉指令回線は、災害時の一斉情報配信や地震データの収集用として、有効に活用されてきましたが、今後増大するニーズに対応するため、機構として、現状の４倍の帯域（400kHz）を自由に活用できるよう規定を改定いたします。

具体的な導入にあたっては、ネットワーク推進課までご連絡をお願いします。

技術部 ネットワーク推進課

E-mail：net5@lascom.or.jp

Tel：衛星 048(300)100(第１世代)　NTT 03(3434)0253

衛星 048(302)100(第２世代)

地球局再免許後の関係書類の備付け

現在使用されている地球局（一部の地球局及びVSATを除く。）は、12月１日付けで再免許となる予定です。地球局の再免許は電波法により５年に１回行われるもので、無線局の免許が更新されます。契約者の皆様におかれましては、改めて地球局に関する従前の無線局免許状、備付書類の整理をお願いします。

１．新たな免許状等をお送りする時期

各総合通信局によりますと、11月中旬から下旬にかけて、新たな無線局免許状が機構宛に交付される予定です。機構では交付された免許状の内容を確認して必要な備付書類を添付し、各地球局の契約者様に郵送致します。

これにより、新免許状と備付書類が皆様のお手元に届くのは、11月下旬から12月中旬頃になるかと思われます。

２．従前の免許状の返納

無線局免許状が効力を失った場合、１ヶ月以内に返納する必要があります（注１）。皆様には、お手数でも本年内を目標に、機構(免許管理課)宛、ご返送をお願い致します。これまでに変更や訂正等で交付された免許状がありましたら、全て一緒にお送り下さい。

３．新たな備付書類

無線局再免許申請書の写しを併せてお送りします。これは、地球局の現状を示す「備付書類」です。いつでも閲覧できるよう、保管して下さい(注２)。免許申請を電子申請で行うので、本書類は電子媒体（CD-R）になっています。

届きましたら必ず最初に、インターネット環境のパソコンで閲覧してみて下さい。

なお、昨年の告示の改正により、時計、業務日誌、無線局検査簿の備付は省略/免除されています（注３）。

備付書類であるCD-R（選解任届の例）

４．従前の備付書類の扱い

これまでにも変更や訂正等で何度か備付書類(CD-R）が送付されているかと思います。
これらは返納の義務はありませんが、再免許により内容が更新されていますので、廃棄して下さい。

また、CD-Rでお送りしている「無線従事者選解任届」は、今回の再免許と連動はしていませんが、最新の内容のみを保管して頂ければ結構です。

新たな免許状の誤りや、CD-Rの不具合等ありましたら、免許管理課にご連絡下さい。

menkyo@lascom.or.jp

注１）電波法第24条
注２）電波法第60条
注３）電波法施行規則第38条の二

ヘリサットへの機構の対応

ヘリサット（ヘリコプター衛星通信システム）は、機構も参画した消防庁の「ヘリコプターによる被災情報収集の在り方に関する検討会」（平成18年２月～12月）で活用のための方策等が検討されました。平成18年９月26日のデモフライトでは1.5Mbps伝送が達成され、デモ画像は適当であるとの評価を多く受けました。

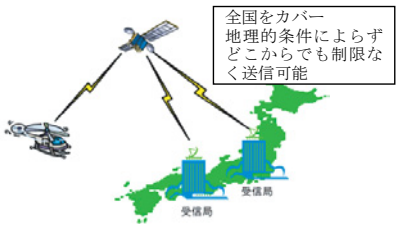


図１　ヘリサット概要

その後、機材の小型化と高出力化の開発が進み、40cmφパラボラアンテナで６Mbps伝送や高画像圧縮技術H.264と組合せたハイビジョン並みの映像伝送も可能となりました。

ヘリサットは全国をカバーする衛星で直接中継することにより、地理的条件によらずどこからでも制限なく映像伝送と双方向音声通信が可能となっています。また大規模災害等では、同時に複数のヘリコプター運用による同時多チャンネル映像送信も可能です。

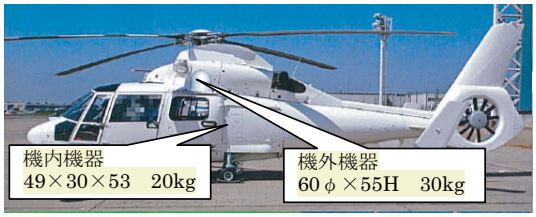


図２　ヘリサット機器概要

さらに双方向データ通信によりヘリコプターの位置＋姿勢の情報が送られて来ますので地図情報GISと連携するなど多様な活用が期待されています。また基地局からは、ヘリコプターに向けて制御信号が送られて映像伝送のコントロールやヘリコプター搭載カメラ等の制御も可能となっています。

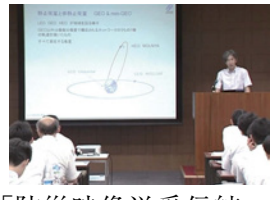
ヘリサットは消防庁を始めとして官公庁や放送局等で導入検討が進められており実運用も近いと考えられます。機構では、消防庁・各県でのヘリサット導入に備えて、LASCOMネットワークでの運用について検討を始めました。

LASCOMネットワークにヘリサットが導入されると、従来のディジタル映像やディジタル準動画、IP画像伝送用キャリアにヘリサット用キャリアを加えたトラポン上のキャリア配置・割当運用ルールおよび運用手順の確立、輻輳が予想される大規模災害時等の複数機同時運用におけるキャリア設定・割り当ての自動化にむけたヘリサット統合管理システムの検討、ヘリサットから送られてくるH.264方式で圧縮された画像を現行のMPEG方式ディジタル画像への変換、再配信等など、来るべきヘリサット時代へ準備を進めております。

地域衛星通信ネットワーク担当者連絡会議について

平成22年度の地域衛星通信ネットワーク担当者連絡会議は、平成22年７月６日（火）に全国都市会館第２会議室で開催されました。

冒頭に当機構理事長の荒木慶司よりご挨拶申し上げ、災害からの被害を最小限にするためには、初動体制が重要であり、地域衛星通信ネットワークは、正確かつ迅速な情報伝達手段として大きな役割を担っていること、地方公共団体においては、緊急時に確実に対処できるよう十分な訓練を実施していただきたいことなどをお話ししました。



続いて、技術部長の大内智晴より「衛星通信について」と題して、衛星通信の歴史、特徴や技術などの説明をしました。

更に、総務省消防庁から「防災映像送受信統一訓練について」、「Ｊ－ALERTの高度化について」など最新の施策の説明がありました。

最後に、機構職員より機構業務についての説明を行いました。なお、この会議の模様は、地域衛星通信ネットワークを通じて全国の自治体に配信されました。当日は多数のご参加をいただきまして、ありがとうございました。

簡易に構築可能なネットワーク構成と展開に関する調査研究会の中間まとめについて

第３回の「簡易に構築可能なネットワーク構成と展開に関する調査研究会」（以下、「研究会」という。）では、中間まとめを作成しましたので、その概要について紹介します。

１　更新における問題点

第二世代システムが平成15年に運用開始してから既に７年が経過しようとしています。

また第一世代システムも現存しており老朽化が進んでいます。しかしながら、更新は進んでおりません。

問題点として、地球局の各装置が独自の仕様から専用化しており高価となっていること、伝送速度が低いため、高速な光ファイバー網へ機能が移され、利用頻度が低下していること、また、伝送遅延や降雨減衰等、衛星通信特有の技術的問題があげられました。さらに、ネットワークを構築する上で、更新整備時期及び更新期間の不統一に伴う全体システムの世代交代の難しさも指摘されました。

本研究会では、設備価格と利用頻度の問題を中心に対応するため、地球局の各装置の低廉化、各種サービスのIP化及び利用を促進する効果的なアプリケーションに主眼をおき調査・検討しています。

２　低廉なシステムの構築手法

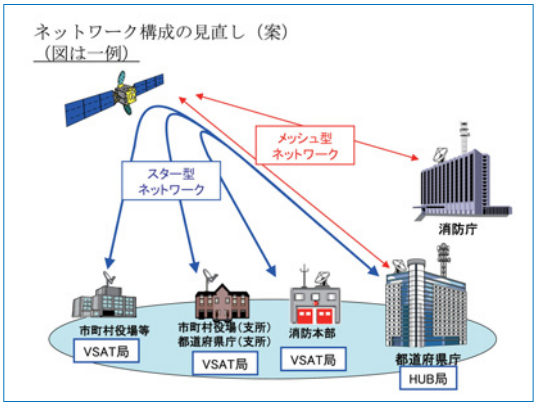
地球局の各装置を低廉化するために次の手法を検討しています。

第１に、地域衛星通信ネットワークのIP化です。地上系のネットワークはIP化が進み、それに対応した様々な周辺機器が販売され、利用されています。現行の地域衛星通信ネットワークの第２世代システムは、IP化に対応したものとなっております。そこで地域衛星通信ネットワークのIP化を推進していきます。電話、ファクシミリ、一斉指令及び映像は、既にIP化することが技術的にも可能です。これらのサービスをIP化することにより、汎用のネットワーク機器の導入が可能となりシステムとして低廉とすることが可能となります。

第２に、地球局装置の汎用化と標準化です。現在の地域衛星通信ネットワークのシステムは、独自の仕様であり、各装置が専用化しています。そこで、この独自な仕様を見直し、海外製品を含めた汎用品が活用できるように変えていき、低廉化を図ります。さらに周辺機器の標準化を図っていきます。

第３に、ネットワーク構成を見直します。地域衛星通信ネットワークは、どことでも１ホップで通信ができるよう、メッシュ型のネットワーク構成です。しかし、地域衛星通信ネットワークの通信のほとんどが、市町村と都道府県との間で行われています。そのため都道府県を中心としたスター型ネットワーク構成と見ることが可能です。

スター型ネットワークの装置は、特に海外で広く使われており廉価です。構成の一部を見直すことにより、廉価な装置の導入が期待されシステム全体として低廉化することが可能となります。



3　各種サービスのIP化

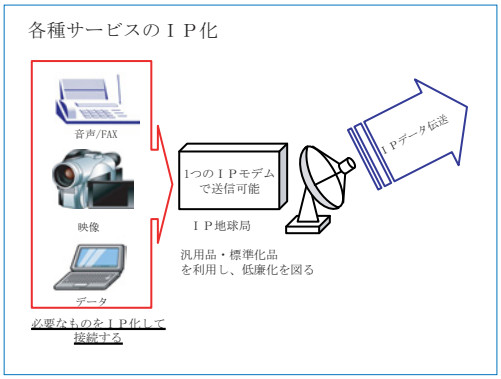
地域衛星通信ネットワークのIP化に向け、音声、ファクシミリ、映像の各種サービスをIP化する必要があります。既に地上系のネットワークにて利用されています。

音声については、VoIPという音声をIP化する技術があり、この技術を衛星系のネットワークにも応用し導入させていくものです。

ファクシミリについては、前出のVoIPに疑似音声として送出する方法と、ファクシミリの内容をPDF化させデータとして送出する方法があります。

映像についても、近年映像のディジタル圧縮技術が進み、低速回線でも高画質の映像を送信することが可能となりました。

このように、地域衛星通信ネットワークで利用されているすべての情報をIP化によりデータとして伝送することができます。IPに統一することにより､モデムの数を減らすことも可能となり、システム低廉化の有効な手段と見込まれます。



4　効果的なアプリケーション

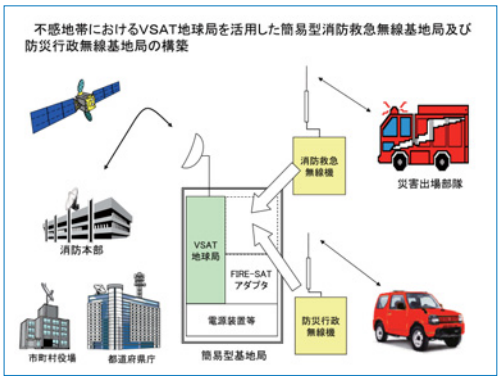
効果的なアプリケーションとして、音声、映像、データを利用したものがあげられています。

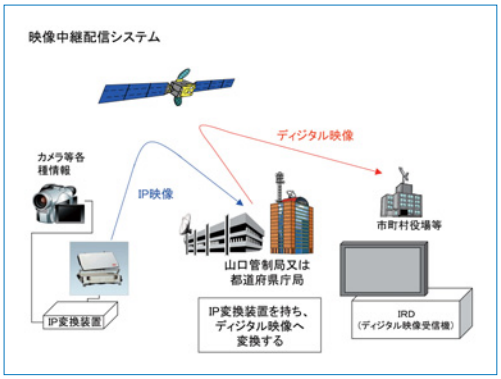
音声を利用したものでは、「地域衛星通信ネットワークの新たな展開に関する調査研究会最終報告書（平成21年３月）」の他網接続にて開発された消防救急無線との接続アダプタを可搬局からVSAT地球局に変えて接続することで簡易型消防救急無線基地局の構築の可能性がでてきます。また、消防救急無線を防災行政無線に変えることで簡易型防災行政無線基地局の構築の可能性があります。

映像を利用したものでは、IP映像をディジタル映像に変換配信する映像中継配信システム、IP映像をそのまま利用するテレビ電話又はテレビ会議システムといったものの実用化が見込まれます。

データ通信を利用したものとしては市町村等からの震度情報を都道府県庁局に収集する震度（環境）情報システム、小規模な文字情報を利用したチャットシステムなどが考えられます。

今後これらシステムの導入条件について検討、実証していきます。





5　今後の検討

今後、音声、ファクシミリ及び映像のIP化による実用性についてアプリケーションを含めて、実証検討していきます。

また、ネットワークの構成を、合理性、低廉性及び構築の容易性の面から検討していきます。

以上を踏まえ、平成23年３月までに、低廉な構築方策の策定と効果的なアプリケーションの提案を行いたいと考えております。

J-ALERTへの取組状況及び地上配信機関業務終了について

1．現状までの経緯

J-ALERTは、全国国民を災害等から保護するための緊急情報を瞬時に伝える目的で、平成19年２月から正式運用を開始しました。この時全国へ瞬時に配信可能な通信基盤として、地域衛星通信ネットワークが採用されました。

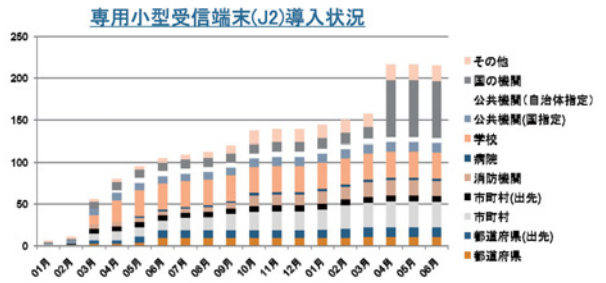
平成19年９月「地域衛星通信ネットワークの新たな展開に関する調査検討会」において、J-ALERTの改良・普及推進について議論され、当機構は、主に可用性（確実性）の向上、普及促進を目的として、地上系接続、専用小型受信端末の開発・提供を行うこととなり、平成21年１月地上配信機関として業務を開始するに至りました。

その後、現在まで、テクニカルサポート窓口開設、普及促進キャラバン、システムの安定化、地域情報変更への対処等を実施して参りました。

また、消防庁主催のJ-ALERT高度化検討会に協力し、本年12月から開始する新J-ALERTシステム構築への協力、移行支援を行っています。

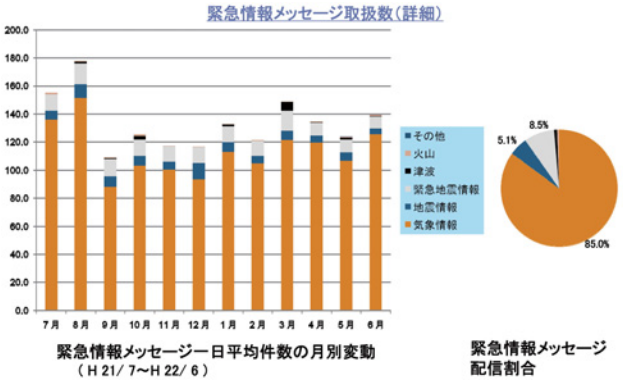
2．J-ALERT（J2）展開、運用状況

J-ALERT（J2）小型受信端末の端末登録件数は、平成21年１月から平成22年７月末時点で232件となっています。（下図参照）



この様に、当初対象の市町村のみならず、学校、病院への導入や、全国気象台への導入、水門の開閉システムへの展開等、幅広い用途で導入されています。また、この間加入団体、関連業者からの問合せは300件以上あり、初期設定、環境条件、動作・仕様の確認、訓練メッセージ等に関連した多数の問合わせに対応してきています。

最近一年間に、実際、全国各地に向けて送出された緊急情報メッセージの取扱い（配信）状況は、下図様になっており、昨今の気象状況の激化により、一日平均100件あまりの気象情報が配信されています。



3．J-ALERT（J2）業務終了および現行業務の今後について

消防庁からの連絡（平成22年６月18日消防国第53号）により新J-ALERTへの全面移行と現行地上配信機関終了が周知されました。これに伴い、当機構においても「J-ALERT高度化に伴う地上配信機関業務の終了について」（平成22年６月21日自治衛通第92号）により、現在行っている地上配信機関業務の本年12月での終了を連絡させていただきました。

新J-ALERT導入以降の各種業務については、消防庁国民保護室に於いて一元的に実施されることとなりました。当機構では今後とも移行期間の継続的な支援を続けるとともに、新J-ALERTに対しての地域衛星通信ネットワークの提供を引き続き行っていく予定となっています。

映像情報の発信事例

生中継

全国知事会議（全国知事会）

平成22年４月６日と５月27日に都道府県会館で開催された同会議の模様を生中継で放映しました。

全国都道府県財政課長・市町村担当課長合同会議（総務省）

平成22年４月23日に総務省地下講堂で開催された同会議の模様を生中継で放映しました。

第80回全国市長会議（通常総会）（全国市長会）

平成22年６月９日にグランドプリンスホテル赤坂で開催された同会議の模様を生中継で放映しました。

全国知事会議in和歌山（全国知事会）

平成22年７月15日から16日にかけて、和歌山県ダイワロイネットホテルで開催された同会議の模様を生中継で放映しました。

防災訓練・災害映像（各都道府県・市町村）

都道府県・市町村で防災訓練が開催され、その映像が訓練の一環として送信されました。左は平成22年６月５日に愛知県で行われた第４回緊急消防援助隊合同訓練の様子です。

録画による放映

平成22年度東京会場地方債事務取扱講習会（総務省）

平成22年４月16日にルポール麹町で開催された同講習会の模様を放映しました。

環境フォーラム（全国市長会）

平成22年６月８日に全国都市会館で開催された同フォーラムの模様を放映しました。

平成22年度地域衛星通信ネットワーク担当者連絡会議（自治体衛星通信機構）

平成22年７月６日に全国都市会館で開催された同会議の模様を放映しました。

暗号危殆化への対応について

「暗号技術の2010年問題」というのをご存知でしょうか。米国政府の調達するシステムでは、使用する暗号技術を米国国立標準技術研究所（以下、NIST）で決めています。

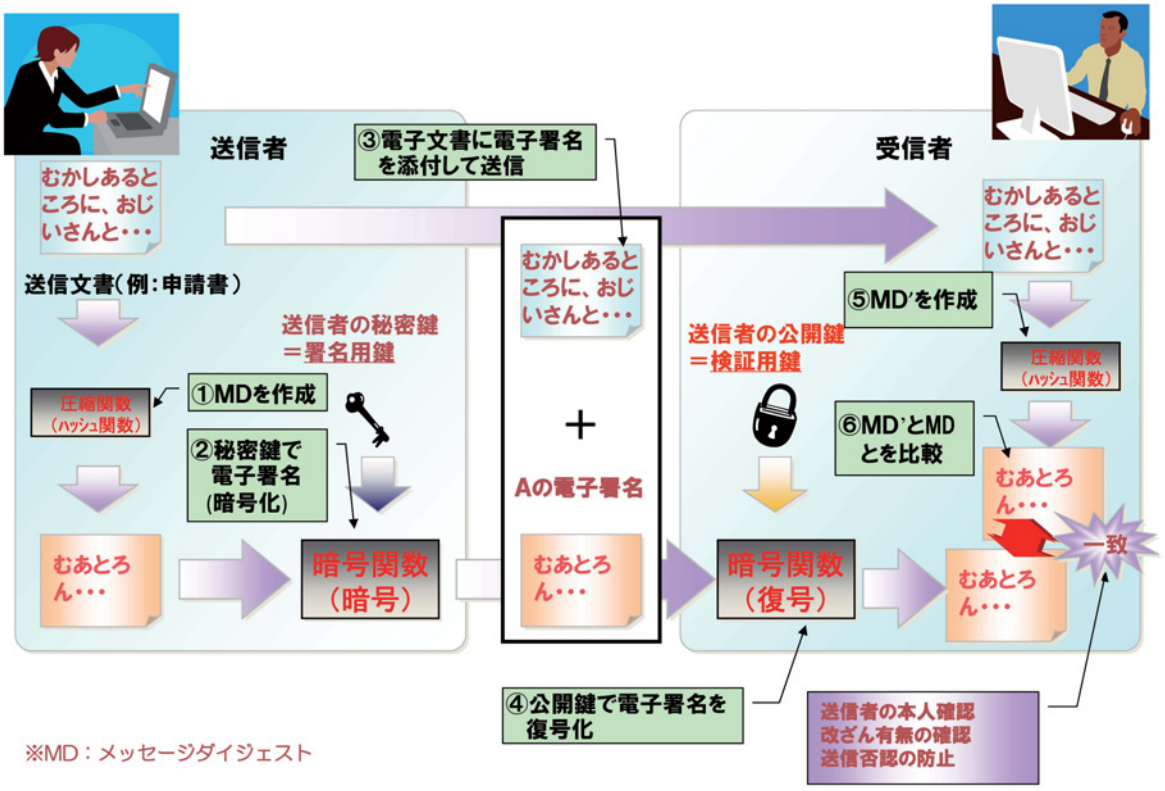
NISTでは、2010年に弱い暗号技術の規格を調達対象から除くこととしており、除外対象にSHA-1、RSA1024という現在一般に使用されている規格が含まれます。

この除外対象規格を使用しているシステムは、別の暗号技術規格への変更などが必要となることから、「暗号技術の2010年問題」と呼ばれています。

公的個人認証サービスでは鍵ペア＜秘密鍵と公開鍵のペア＞と電子証明書を安全なICカードに格納し、電子申請や電子申告（以下、電子申請等）で電子署名を行う際に使用しています。

ICカードに格納した鍵ペアと電子証明書、そしてそれを使用した電子署名を例えていうと、秘密鍵は実印に相当、電子証明書＜公開鍵の証明書＞は印鑑登録証明書に相当し、電子署名は実印を捺印する行為に相当します。

公的個人認証サービスでは「なりすまし」「改竄」「送信否認」を防止するために暗号技術を使用しています。ここでは、申請書や申告書が通信途中で書きかえられること（以下、改竄）を例に、どのように暗号技術を使用して防止しているのかを下の図に示します。



○なぜこの図の手順で確認できると、改竄されていないと言えるのでしょうか？

公的個人認証サービスではSHA-1、RSA1024という規格の暗号技術が使用されています。

RSA1024は、公開鍵暗号方式と呼ばれる暗号技術の一つで、次のような特徴があります。

・秘密鍵と公開鍵の対を使用し、公開鍵で暗号化したものは秘密鍵でないと復号化できない。また、RSA方式では秘密鍵で暗号化したものは公開鍵でないと復号できない。

・秘密鍵はICカードから無理に出そうとすると破壊される構造で、ICカードの外に出すことはできず、複製不可能なために世界でただ一つしか存在しない。

そのため、「秘密鍵による電子署名は本人しか実施できないこと」が安全の根拠となっています。

○ではどうして秘密鍵が複製不可能といえるのでしょうか？

複製するにはICカードから秘密鍵を取り出すしかないのですが、前述のように無理に取り出そうとすると破壊されて秘密鍵は消滅してしまいます。

そのため、公開鍵や電子署名を元に秘密鍵を推定するには、組み合わせを総当たりで試してみるしか方法がなく、現時点で世界最高速のスーパーコンピューターを使用しても数年かかることがわかっており、電子証明書の有効期間内に複製することは事実上できません。

しかしながら、コンピューターの性能は年々向上していますので、秘密鍵推定までの所要時間は年々短くなっており、世界最高速のスーパーコンピューターを使用して１年程度で推定できるようになると、有効期間内に秘密鍵が推定されて実害を生じることが危惧されます。

このように秘密鍵が短時間で推定できるような状態になることを「暗号危殆化」と呼び、より強度の高い＜秘密鍵の推定に時間がかかる＞規格の暗号技術へ移行することが必要となります。

NISTでは2010年中にSHA-1とRSA1024を米国政府で使用できる暗号技術から除外することとしており、日本でも2014年度早期にSHA-256とRSA2048という規格の暗号技術（以下、「新暗号技術」という）へ移行することが計画されています。

公的個人認証サービスも、関係する住民基本台帳ネットワーク、国や都道府県の電子申請・申告システムなどと足並みを揃えて新暗号技術への移行準備を進めていくことが必要です。

参考文献：

・「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年４月22日情報セキュリティ政策会議決定）

・公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書（平成21年１月）