

我が国の安全保障を考えるディスカッション

@AIAA-JFSC総会

日時:2010年6月1日 14:30~17:00

プログラム

司会:福地 一

安田靖彦:わが国の安全保障問題についての一私見

飯田尚志:安全保障としての衛星通信の考え方

(司会)安全保障と衛星通信に関する忌憚のないディスカッションをJFSC総会の前イベントとして関係者で行うことにした。今日は安田先生、飯田さん、若菜さんをお願いします。まず安田先生からよろしくをお願いします。

(安田)それでは我が国の安全保障問題に関する知見をということで、全体のテーマは安全保障と衛星通信ということでしたが、私、特別衛星通信に関係していることでもなければ、特段の知識もないものですから、この主題に直接的なプレゼンテーションの方は飯田さんにお任せすることにして、私はもうちょっと広い立場で我が国の安全保障の問題を、根本的な問題について触れてみたいと思います。自説を開陳するというか、一風変わっていると思われるかもしれない。あるいはその通りだと思われる方も中にはおられるかもしれない。それでは始めさせていただきます。

わが国の安全保障問題 についての一私見

安田 靖彦

10年位前まで、総務省というか郵政省で、安全保障に関する研究会をやり、報告書の中に安全保障に役に立つと言おうとすると、非常に抵抗があった。最近はどうでもないが、こういうテーマを学会なんかでやろうとすると同様に、我が国は第2次大戦後にいろんなタブーだとか神話というのが流布されてきたわけでございます。私がこれからお話するようなことも本当はタブーなのかもしれない。

それはさておくとして、戦後神話の一つに、我が国が高度経済成長することが出来たのは平和憲法の下、軍備に金をかけず、すべての資源・人材を民需に投入したからであるというのがある。昭和40年代、50年代、60年代に日本だけが高度経済成長をしているように見えたときに、大抵の有識者はそういうことを言った。私は経済の専門家でもないし、そのへんがどうなのか判らないが、経済の方を犠牲にしても適切な軍事力を持つことは必要であると思っておりました。しかし、今日振り返ってみれば、この言説がいかに根拠のないいい加減なものであったかということがよく分かるわけです。繰り返して言いますように、国防費の対GDP比は中国(3~4%)、韓国(3%)、台湾(2.5%)、米国(5%)とまあこの程度なのですが、中国や韓国や台湾は高度成長しているではないか、日本が憲法のお陰で軍備費を掛けなかった(日本(1%))からというのは全然うそであった。これははっきりしていることを指摘したい。それから、1990年代の初め頃は日本のGDPはアメリカの半分以上あったわけですね。それが、今や1/3くらいに落ちている。アメリカはずっと5%くらいの軍事費を維持して

戦後神話の一例

- わが国が高度経済成長することが出来たのは平和憲法の下、軍備に金をかけず、すべての資源・人材を民需に投入したからである
- 国防費の対GDP比
日本(1%)、中国(3~4%)、韓国(3%)、台湾(2.5%)、米国(5%)

いる。それで、アメリカは経済成長しているのに、何故日本は経済成長しないかという疑問が第1に起こってくるわけです。日本がこのように長期に停滞しているのは国防費の割合が低いからではないか。誰も反論できないのではないかと思います。

日米貿易摩擦(1980年代)のために内需拡大策というか、中曽根首相は結局は米国の強硬な要求により、公共事業への過大な投資(10年で430兆円)を行うことになりました。その結果、バブル経済が発生し、経済構造が大きく歪められた。それからスーパー301条によって衛星開発には大打撃を受けたわけです。何故、こんな馬鹿なことになったかということです。安全保障への適当な投資がなく、単に経済効果ばかりを狙ったからです。

内需拡大が何故できないか。現在でも大きな需給ギャップが存在し、デフレからの脱却ができない。この理由は、軍事需要がないからである。我が国は他国には存在する需要部門が存在しない。すなわち安全保障部門が欠落している。

この安全保障需要というのは、一定の投資を行えば一定の経済効果がある。安全保障分野への投資拡大の効果として、国の安全保障の強化ができ、その波及効果として最近の軍事では高度な研究開発をしなければ相手にできませんので、高度な科学者・技術者の養成と雇用が拡大できる。しかし、実際はそういう需要がないわけです。何故、こんな馬鹿げたことになっているか。そういうメリットはある筈であるのに。少なくとも子ども手当などよりずっとましであるわけです。

それで、私は、諸悪の根源として日本国憲法エイズ論というのを前から唱えています。エイズはご承知のとおり、後天性免疫不全症候群でありまして、HIVウイルスが免疫体に感染して免疫不全症候群を引き起こす病気でございます。HIVウイルスというのは直接人体に害を与えるものではなくて、まず無防備にしてその結果人体が完全無防備に陥ってしまう。長い時間じわじわと防衛能力をなくし人体を蝕むのがエイズでございます。我が国の場合、敗戦により、強制的に日本国憲法というエイズに感染させられた。免疫力を破壊した上で、日米安全保障条約、これは無菌室なんです。これとセットになったわけです。これで無菌室に入れた

諸悪の根源

- 日本国憲法エイズ論
所謂日本国憲法はわが国の免疫システム(防衛本能)を破壊するために占領軍によって強制的に感染させられたHIVウイルス
- 日米安全保障条約という無菌室に入れられた

日米貿易摩擦(1980年代)

- 内需拡大策 公共事業への過大な投資(10年で430兆円)
- バブル経済の発生、経済構造を歪める

内需拡大は何故できないのか

- 現在でも大きな需給ギャップが存在
- デフレからの脱却ができない
- わが国は他国には存在するある需要部門が存在しない。すなわち安全保障部門が欠落

安全保障分野への投資拡大の効果

- 国の安全保障の強化
- 高度な研究開発 とその波及効果
- 高度な科学者・技術者の養成
- 雇用の拡大

れて60数余年経ってしまった。所謂日本国憲法は我が国の免疫システム(防衛本能)を破壊するために占領軍によって強制的に感染させられたHIVウイルスで、日米安全保障条約という無菌室に入れられたというわけです。社会党、今の社民党です、などの左翼はうとうしいから早く無菌室を撤去しろと叫んだわけですよ。一方、自民党を中心とする保守勢力はこの無菌室をいつまでもアメリカに提供してくれと言っているわけですね。どちらが現実的かというそりや勿論、左翼が言っているやつは出たとたんに感染症にかかって死んでしまいますから、そう言う意味では自民党の言っている方がまだいいんですけども、こういうことをやっていると無菌室から永久に出られない、一人前の人間ではないわけです。そういう状態に日本はあるということです。

エイズを撲滅しない限り、経済的には情けない状態になっていると私は思います。最近、鳩山首相が大変脳天気な発言で、沖縄普天間基地問題が政局を揺るがすというようなことになったが、要するに一国の首相にとって最大の責務であるこの国の安全保障の問題について、鳩山さんは何も考えていなかったということが露呈したわけです。これは鳩山さんに限らず、それを非難する国民自体が胸に手を当てて良く考えてみたらどうか。今まで安全保障問題をどれくらい考えたか、あるいはどんな知識があるんですかと。日本全体が世界的なビジョンを含めて結局そういうことを議論する場が全然ない。大学にはそもそも安全保障問題を取り扱う講座がない。私は早稲田大学にまだいた頃、理工学部を再編するということで学科もいろいろ検討したわけですが、半分冗談だけれど情報軍事学というのを作ったら学生が集まるぞと提案した。むしろ先鞭をつける意味で価値があると思ったのですが、やっぱり無理でしょうということになった。そういうわけで普通の日本人は何も知らないわけです。ということは無知の群衆にすぎない。自分の安全保障問題を自らの問題として考えない。これは完全な植民地地盤ですよ。そうやっている諸悪の根源は日本国憲法である。

日本の米軍基地がどうなっているかをよく見るために、日米の立場を逆転してアメリカに配置してみると、ワシントン郊外のアンドリュー基地が日本空軍の基地、東海岸のノーフォーク海軍基地が日本海軍の基地、アンドリュー基地は横田、ノーフォーク海軍基地は横須賀ですね、それからニューワークは厚木の飛行場、こういう対応をすることができる。西の方のハワイは日本陸海空軍の大基地で沖縄に相当する。サンディエゴ軍港は日本海軍基地で佐世保に相当。シアトルは三沢、ニューオリンズの辺りは岩国、まあ適当に考えてみたのですが、こんなことはアメリカ人が65年我慢するだろうかと。日本人は基地問題について不感症になってしまっている。こう考えると、日本という国がいかに異常な状況に置かれているかよく分かるわけです。

幕末頃の日本が末期症状の頃、徳川政権が日米修好通商条約を結ばされたわけです。明治政権は革命政権であって前の政権とは違うわけだが、日本人は非常にまじめで不平等条約を引き継いで、それを改定するために官民揃って涙ぐましい努力をした、結局30年くらいして日清戦争のときに不平等条約が改定されて平等な条約が結ばれた。このときは、とにかく官民が一緒に一丸となって当たった。日本国憲法は、昭和21年に発布された。東京裁判でやむなく憲法は飲まされた。その事実をなぜ知らせないのか。憲法ほど非民主主義的なものはない。どうみてもこんな非民主主義的な憲法はありえない。こういう馬鹿げた状況を打破しない限りは憲法改正はあり得ないというように考えています。

日米修好通商条約

- 安政年間、末期症状の徳川政権が結んだ不平等条約(関税自主権なし、領事裁判権をあたえる)
- 明治維新政府は数十年かけて外交努力で改正に成功(一致した国論の下、涙ぐましい努力を行った)

日本国憲法=昭和の不平等条約

東アジアの国際情勢というのは極めて外患憂慮の状態、朝鮮半島の情勢も非常に憂慮すべき状態ですけれども、もっと長期的にみるとより大きな問題は、中国の発展です。1995年に当時首相であった李鵬が、「日本なんていう国は数十年後に消えて無くなっている。」と言ったという。また1992年に領海法というのを制定して、尖閣列島、南沙諸島、西沙諸島を領土に入れちゃったわけです。実際に南沙諸島、スプラトリー諸島はフィリピンとの間にあるわけですが、それを武力で取ったわけです。西沙諸島についてはベトナムとの間で戦争を起こして、それで占領しているわけです。で、尖閣列島も、鳩山さんは脳天気のようなことを言って、抑止力は関係ないというようなことを言っているとあつという間に取られます。というのは、今アメリカは尖閣列島については手出しをしない。日中で話し合えと言っている。前にモンデール駐日大使が「尖閣諸島の帰属に関する実力行使を伴う国際紛争の場合、日米安保は発動しない」と発言し、石原慎太郎が非常に怒って、大使が交代させられた。しかし、今のアメリカはもうそういうことを平気で言っているわけで、ここは非常に危ない。尖閣列島は取られてしまう。それから、中国海軍が今非常に増強され、近代化している。米国と中国とで太平洋を分割支配しようと持ちかけたと、これも一部の新聞に出ていた。こんなことを総合すると中国がいろいろ野心を持っているという。朝日新聞の記者で軍事評論家の田岡俊次が先日も米中関係は日米関係よりずっと親密になっていると言っていた。日中が活発に軍事衝突するようになるとアメリカが困る。これは一面の理だろうけれども、私の感じでは米中が将来に亘って親密で在り続けることはあり得ない。何故かという、第1位と第2位の覇権国家である。その覇権国家が仲良くすることはあり得ない。必ず利害が衝突する局面が出てくる。特に中国の場合は、2010年中に日本のGDPを超えていくけれども、それでもまだ一人当たりで考えると1/10である。ということはまだまだ成長するわけです。そのとき何が起こるかという、アメリカの勢力圏をしっかりとしなければいけない。よく形勢を見て、しっかりとするためには日本の軍事力をもっと自分で守れるだけの軍事体制を整えておかねばと思うわけです。この辺で終わりにします。

(司会)ありがとうございました。取りあえず質問があればお願いします。

(Q) 日本にあるアメリカの基地を全部日本に返せということか。

(安田) 全部ではない。

(Q) 日本の基地はアメリカのためにあるので、日本のためにあるわけではない。だから、日米安全保障といっても日本のためにはやってくれるわけではなく、前戦基地として置いているということか。

(安田) 勿論そうだ。日本が自分で軍備をもって自立してその上で本当の意味で対等の立場でアメリカと交渉できる。核の問題は日本は唯一の核被爆国である。だから核アレルギーがある。被爆国が核武装するとなるとインパクトが強い。2度と核攻撃を受けないために核武装をする。中国が尖閣列島についていちゃもんをつける。アメリカは手をださないと言っている。中国は核を持っているから、日本が中国に対抗するには私は核武装すべきだと思う。日本も核保有国として軍縮に参加すればいい。とにかく日本人の戦後の発想はなさない。

(Q) 先ほど安全保障が内需拡大に貢献するというのは非常に大きなポイントだと思うのですが、今まで何故それが表に出てこないか考えてみると、防衛生産とかを経団連が推進していた防衛生産委員会というのは重工業とかのいわゆる正面装備の方ばかりで、情報通信産業とかでなく、しかも役所の所掌に左右されてきた。どこか体制を動かしているところがあるといいのですが。

(安田) だから憲法を変えろということです。■

我が国の安全保障を考えるディスカッション

@AIAA-JFSC 総会

日時：2010年6月1日 14:30~17:00

プログラム

司会：福地 一

安田靖彦：わが国の安全保障問題についての一私見

飯田尚志：安全保障としての衛星通信の考え方

若菜弘充：安全保障と衛星通信—通信技術の観点から

(司会) 一通り話を伺うことにして、次、飯田さんをお願いします。

(飯田) すごい話を聞いちゃったのですが、一応「安全保障としての衛星通信の考え方」というタイトルでお話します。内容は2009年に電子情報通信学会の衛星通信研究会でしゃべったことを基にして通信学会のオピニオンに書いてくれということで、今印刷中のものです。そこで書いたのは、今まで宇宙の平和利用に限定された環境に慣れてきてしまった我々にと

って、安全保障に係わる衛星通信技術の研究開発は従来行ってきたものとどう違うのか戸惑うと。それで私は、安全保障に係わる研究開発の仕方は従来とは違いますよということを主張したいわけです。オピニオンに書いたら、コメントが面白いのが来て、通信学会というのは日本人だけではない、外国人も見ているから、もう少し柔らかく書いてくれとか、の話がきました。それで、例として日本の場合だったらこうですよというように書きました。ただし、内容に機密の話はありません。

それで、「安全保障における衛星通信技術の重要性」ということですが、衛星の利用は、ランド研究所と言うところが偵察衛星のコロナ作戦というのを1958年から開始し、1960年に13回目の衛星打ち上げで漸く成功したということです。失敗しても何でもやってしまうわけですね。それで、情報収集をしたら、アイゼンハワー大統領がものすごく喜んだそうです。いままで、偵察飛行をし

衛星通信の話題「衛星通信と安全保障」@AIAA-JFSC総会
2010年6月1日(火)
首都大学東京秋葉原キャンパス

安全保障としての衛星通信の考え方

Thinking over Satellite Communication for National Security

飯田尚志
Takashi Iida

はじめに

- 宇宙基本法の成立
- 米軍における宇宙技術、とりわけ衛星通信の役割の増大
- 今まで宇宙の平和利用に限定された環境に慣れてきてしまった我々にとって、安全保障に係わる衛星通信技術の研究開発は従来行ってきたものとどう違うのか戸惑う
 - 安全保障に係わる研究開発の仕方は従来とは異なる性質を有すると主張したい*

飯田尚志: "オピニオン 安全保障としての衛星通信—その役割の増大と今後の研究の一進め方—", 電子情報通信学会誌 (印刷中)

安全保障における衛星通信技術の重要性

- 宇宙は軍事的に極めて重要
 - 核・ミサイル・宇宙戦力の一環
- 宇宙技術による冷戦時の戦争回避
 - 宇宙技術が有効に利用されるものの例
 - ・ 偵察衛星
 - ・ U2航空機による偵察から偵察衛星に移ったことにより領空侵犯の危険性の回避*
 - コロナ作戦 (RAND研究所)**
 - ・ 1958年: 衛星打ち上げ開始
 - ・ 1960年: 13回目の衛星打ち上げでようやく成功
 - ・ 冷戦での情報収集に役立つ
 - 1967年: イスラエル・アラブ諸国の間の「6日間戦争」
 - 1968年: ソ連のチェコスロバキア侵襲などの情報収集
 - 情報を得ることによる相手動向を把握することによる疑念の回避
 - 緊張の緩和をもたらし冷戦時の平和維持に貢献
- 冷戦の終結
 - ・ 1989年: ベルリンの壁の崩壊
 - ・ 衛星通信・衛星放送の果たした役割大
- 混沌の21世紀の到来
 - 2001年9月11日の米国同時多発テロ
 - テロとの対決
 - 情報通信、特に衛星通信の重要性が増大

*Dr. W.F. Balhaus Jr. "Successes and Challenges in Transforming National-Security Space", 43rd Aerospace Sciences Meeting, Reno, NV, AIAA-2005-2002, Jan. 12, 2005.
**アレックス・アベラ [訳] "ランド 世界を支配した研究所", (株)文芸春秋, Oct. 30, 2008.

てもなかなか情報がわからない、それで偵察衛星で得られた情報は何百億ドルつぎ込んでも価値があると言ったらしいです。実際に、イスラエル・アラブ諸国間の「6日間戦争」とかソ連のチェコスロバキア侵攻などの情報収集に役立ったということらしいです。冷戦は終了したけれど、その後渾沌の21世紀が来て、安全保障には情報が益々大切になってくるといふわけです。

それで、軍事的に考えれば、私は軍事の専門的なことは分からないのですが、RMA (Revolution in Military Affairs) という軍事の大変革が起こっているらしいです。要は情報化時代で、今までの戦争と違うやり方がきているということです。情報化時代というのは何でも報道しますから、戦争が勃発すると自国兵士のみならず敵兵士さえもできるだけ殺傷しないで目的を達成するように求められるということです。ですから、今のイラク戦争でも何千かの戦死者は出ていますが、昔の戦争の比ではない。昔は日本が上海事変を起こしただけでも日本軍の戦死者は約1万人だったわけですから、それに比べればまるっきり犠牲が出ていない。とにかく戦争のやり方が変わってきている。情報が大切になってきているというわけです。ここでも、ランド研究所というのはRMAの考えを昔からやっているということです。

それから、宇宙技術がこのRMAに貢献しているものとしては、諜報能力の強化と精密攻撃システムがあります。特に精密兵器はイラク戦争の当初難民発生が回避できたということです。いままで戦争が起こればもの凄い難民が出ていたけれど、精密兵器では目標だけ正確に攻撃しますので、とにかく難民が起こらなかったということです。軍の配備の効率性を追求するという最近の米軍再編で基盤となるのは通信衛星TSAT、これはキャンセルされましたけれど、情報の円滑化を図るNetwork Centric Military Communicationということで、情報をもって軍事作戦をやっていくということに重きが置かれているということです。情報を使うと何が良くなったかと言うことですが、攻撃までの時間の短縮ができたということで、今まで空軍に攻撃してくれというと何日も掛かってやっと来るらしいんですが、それが今ですと15分位で来ちゃうという話で、この辺がうまくいって

情報型軍事革命RMA (Revolution in Military Affairs)

○ 20世紀末からの軍事大変革*

- 兵器技術のみならずそれをどう使うか、どのような組織が最適かについても大変革が起き、戦争の形態、性格までも変わってきている
- 工業化時代の軍隊の撃破を目的とする消耗戦から相手国の国家機能を麻痺させることが追求される麻痺戦へと変化
- 情報化時代には戦争が勃発すると自国兵士のみならず敵兵士さえもできるだけ殺傷しないで目的を達成するように求められる
- 1991年の湾岸戦争においてはこれらの初期の利用
- 1999年のコソボ戦争では全く新しい軍隊の運用法、編成・組織が生まれ、戦いの形態までも変わり始めた

○ RMAの考え方自体はランド研究所で長い間温められていたということである**

*中村好寿:「軍事革命 (RMA) <情報>が戦争を変える」, 中公新書, Aug.15, 2001.
**アレックス・アベラ[牧野洋訳]:「ランド 世界を支配した研究所」, (株)文藝春秋, 2008.

4

宇宙技術によるRMA

○ 情報・諜報能力の強化と長距離精密攻撃システム

- 精密兵器の発達では、イラク戦争当初において難民発生が回避*

○ 軍の配備の効率性を追求する最近の米軍再編では、基盤となるのは軍用通信衛星TSAT (Transformational Satellite)**

- 米国の安全保障政策に影響を持つジョン・カイル上院議員

「人工衛星は我が米国の軍事優位を支えている。米軍の部隊は偵察、通信、航行その他のミッションに関して衛星に依存している。現在、開発を進めている新世代の軍事衛星システムもすべて衛星依存の度合いが高い。米軍のいかなる作戦も、通常、戦術、ミサイル防衛のいずれを問わず、宇宙依存の部分なしには機能できなくなっている。」***

○ Network Centric Military Communication****

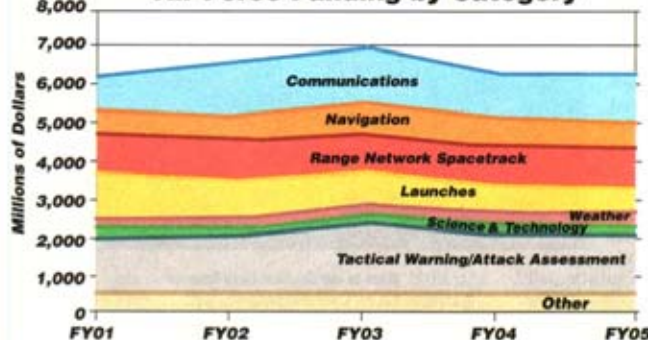
- 情報収集・伝達、作戦会議、指令伝達等をネットワークを通じて行うもの
- 情報伝送バンド幅要求
 - 湾岸戦争で100 Mbps、アフガニスタン作戦で700 Mbps、イラク戦争で3200 Mbps**
 - 無人航空機JAVのオペレーションには衛星経由のバンド幅要求が膨大: Predator: 1.5 Mbps, Global Hawk: 50 Mbps
- 攻撃までの時間の短縮: 従来では何時間から何日も掛かったものが15分**

*W.F.Balhaus, Jr.: "Successes and Challenges in Transforming National-Security Space", Aerospace Science Meeting, AIAA-2005-2002, Jan.12, 2005.
**J.W.Cannon: "Timing in battle: The T-Sat edge", Aerospace America, pp.39-43, Jan. 2006.
***野田浩徳:「宇宙基本法—宇宙開発への課題」, 宇宙誌, Vol.55, No.642, pp.2-7, July 2007
****IEEE Communications Magazine, Nov. 2008.

5

米空軍の宇宙開発予算*

Air Force Funding by Category



*L.M.DeFrance: "Military Space Market Looks Robust As NASA Goes Commercial", Aviation Week & Space Tech., Vol.153, No.18, Oct.30, 2000.

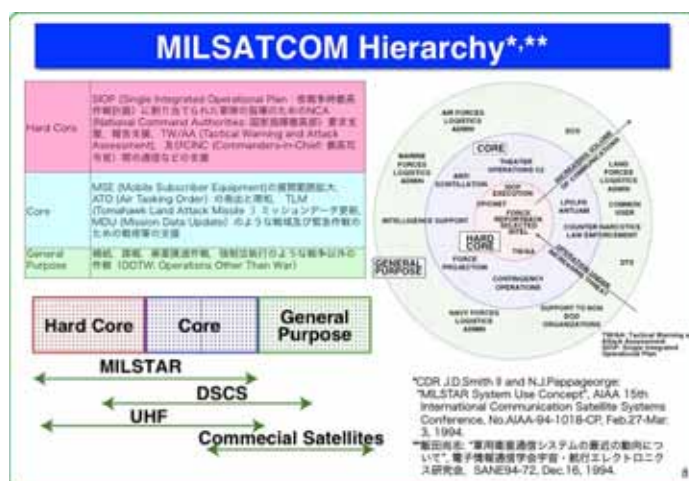
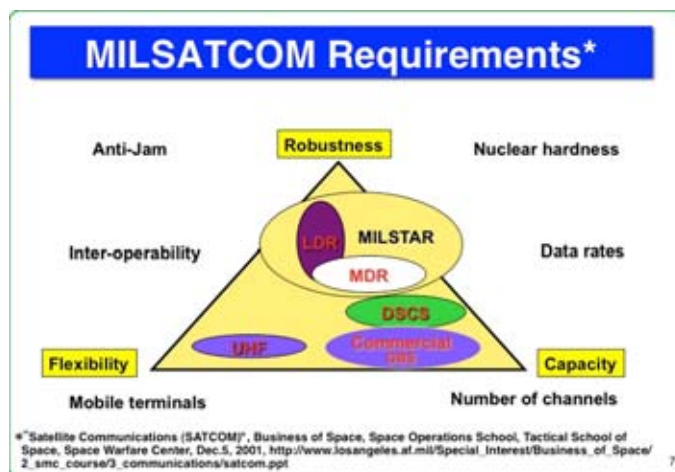
6

いるという話です。ただ、バンド幅が多く要るので、戦争ですと地上通信は使えませんので、衛星通信になるわけですが、無人飛行機のためにバンド幅要求が増大しているということです。今、イラクやアフガンを攻撃している無人飛行機のコントロールはアメリカ国内で行っているらしいので、バンド幅要求が大きいということです。

それから、ちょっと古い Aviation Week の記事ですが、米空軍の宇宙開発予算で communication 及び navigation 関係に毎年 2000 億円以上使っている。JAXA などは通信衛星をもうやらないとかと言っているが、米軍はもの凄くやっている。ですから注意していかなくてはいけないというわけです。

これは軍の通信衛星はどんなものを目指すかということですが、民間衛星ですと capacity とか flexibility とかですが、軍の衛星となると robustness というか、要するに jamming に強いとか、nuclear hardness ということで、核戦争で、空中で核爆発があると通信が止まってしまう。ところが周波数が高いほど回復が早いということで、ミリ波を盛んにやるわけです。

それからこれもちょっと文献が古いですが、MILSATCOM のヒエラルキーということで、3つに分けているそうです。Hard core, Core, General purpose と分けている。Hard core というのは本当に核を落としていいかどうか、Yes か No かを伝達する通信、これは聞かれては困るし、間違っては困るということです。真ん中が Core、それから General Purpose というのは補給とかの通信を行うわけです。どういう衛星が関与しているか決まっているが、General Purpose の方は民間商業衛星でいいが、Hard core, Core は軍の衛星で行うと言っているわけです。



それで、一昨年サンディエゴで開催されました ICSSC のコロキウムで軍の方がしゃべった内容ですが、軍の通信が伸びていくということで、どんどん容量が増えていくわけです。それで、2種類あって Protected communication と Wideband communication で、protected は先ほどの hard core とか core に相当する通信だと思いますが、Milstar から始まって、最近ですと AEHF (Advanced EHF)それから将来は TSAT ということです。Wideband communication は DSCS とか最近ですと WGS (Wideband Global Satellite)がある。WGS は成功している例で、軍の衛星ですので、暗号化は衛星の中で行いますが、例えばサッカーゲームなどを中継する、アメリカ軍は世界中に展開しているので、世界中継が実現するそうですが、暗号があってもうまく行っているそうです。Protected communication の中には耐 Jamming とか核戦争対策などがありますが、LPI/LPD (Low Probability of Intercept/Low Probability of Detection)という事で、通信していること自体が検出し難いというような技術を開発しているということです。

General Purpose では、一般の商用衛星を使うということで、軍の衛星だけですとどうしても容量が足りない。ICSSC2008 のコロキウムで XStar の Curtin 氏が講演したのですが、軍の需要の 80%位は民間の衛星を使わざるを得ないということです。日本で、これから軍の衛星を開発しても民間の衛星の需要は伸びていくということはいえると思います。

通信衛星ではありませんが、勿論、盗聴衛星も衛星通信に関係します。Sigint という盗聴衛星は、非常に大きな 300 フィート、100mクラスのアンテナを使っているらしいです。Sigint のプログラムも First generation から Second, Third, Forth と generation を追ってちゃんと開発しているということで、思いつきでいきなり出てきた物ではないということです。江畑著「最新・アメリカの軍事力」という本によるとこの分野が一番機密度が高いそ



盗聴衛星 (Sigint)*

- 最高の軍事機密***
- Trumpet
- 300 feet antenna
- 軌道: HEO
- 重量: 推定4.5トン
- 移動体通信衛星に技術転用*

SIGINT Programs	First generation 1960s	Second generation 1970s	Third generation 1980s	Fourth generation 1990s	Fifth generation 2000+
GEO - USAF COMINT		Canyon	Chariot	Mercury	Intruder
GEO - CIA ELINT		Rhyolite	Vortex	Mentor	
HEO - USAF ELINT		Aquacade	Magnum Orion	Trumpet	Prowler
LEO - USAF ELINT	Ferret	Sub-Sats			SB-WASS
LEO - Navy ELINT	GRAB	NOSS		SB-WASS	

*C.Covault: "NRO Radar, Sigint Launches Readied", Aviation Week & Space Tech., Vol.147, No.9, pp.22-24, Sep.1, 1997.
 **http://www.fas.org/spp/military/program/sigint/index.html
 ***江畑謙介:「最新・アメリカの軍事力-変化する国防戦略と兵器システム」, 講談社現代新書, No.1594, Mar.20, 2002. 11

盗聴衛星の最近の状況

- 電子偵察衛星 Advanced Orion NROL-26*
 - 米国家偵察局 (National Reconnaissance Office) の最新の大型Sigint衛星
 - 重量6トン、バスケットボールコート大 (24x15m) 以上のアンテナ
 - 2008年1月18日Delta IV Heavyでの打上げ**
- 大型盗聴衛星に関する議論***
 - 経費が大、打上げ間隔の増大、不具合の場合の損失大、ASATに対して弱い
 - 小型の衛星でしかもアンテナが小さいことから低軌道に投入するというような小型衛星
 - 静止軌道から静かに盗聴する環境が今後も必要

Delta IV Heavy

*C.Covault: "World News & Analysis: Night Fright --NRO braces for flight of eavesdropping spacecraft on agency's first Delta IV Heavy", Aviation Week & Space Technology, pp.26-28, Dec.8, 2008.
 **http://www.aviationweek.com/awgeneric/story_channel.jsp?channel=space&id=news/NRODSP12108.xml
 ***A.Butler: "World News & Analysis: Mixed Sats", Aviation Week & Space Technology, pp.28-29, Dec.8, 2008. 12

うです。ですから何をやっているのか全然わからないということです。

最近打ち上げた盗聴衛星は、重量6トン、それほど大きなアンテナではなく、バスケットボールコートサイズのものであるそうですが、3つのエンジンを持つ大きなロケットのデルタ4Heavyで打ち上げました。アメリカの中でも議論があって、こういう衛星は非常に高価であること、高価であるから打ち上げ間隔が延びてしまうこと、不具合の場合に損失が大きいこと、衛星攻撃兵器に対して弱いということで、アンテナの小さい低軌道に投入する小型の衛星でいいのではないかという議論もあるみたいです。ただ、私思うに、静止軌道から静かにじっと聞き耳を立てるような衛星が今後にも必要ではないかと思います。

それから、安全保障関連の研究の進め方ですけども、通信学会誌にも書きましたけれども、安全保障関連研究の通常研究との相違点を3つ私は挙げてみました。1つは研究には暗黙の了解が不可欠ということです。意味深長なのですが、宇宙をしていると宇宙の使われ方がよく分からない、何に使うのですかとすぐ聞かれる。そうすると宇宙の専門家がこう使うという資料を一生懸命作っているが、こういうのは本務ではないし、私はやる必要はないと思う。宇宙研でロケットを開発しようとしたとき、あれは完全にミサイル技術であったにもかかわらず、そのときこれミサイルだろうなんて議論は起こらなかった。多分暗黙の了解です。そういうわけで特に安全保障に関する研究は、暗黙の了解が必要だと思います。細かいところまで、これ何に使うんですかというように根掘り葉掘り聞く必要はないというわけです。それで、やはり得られた成果を何に使うかというのは、例えば衛星から得られた情報はこう使う、こう使わないと意味がないと言ってしまふと情報をインテリジェンスにするのは他の部署ですから非常に危険なことだと思います。暗黙の了解が必要ということです。そういう意味で、言うてはいけない「第2位じゃまずいんですか」というような、そんなことを言う必要は全然ない。みんな1位だと思っているわけですから。

それから、研究の「集中と選択」でなく「抽出と強化」というのがどうかと思います。集中と選択というのは、10年位前から言われてきたと思いますが、それをやっていくと今役立てないと思われる研究はどんどん無くなっていってしまう。研究が無くなるだけでなく人も無くなってしまふ。そうすると将来何になるか分からないものはできない。特に安全保障関係は何に使えるか分からないものもちゃんとやっておかなければいけないので、非常に問題ありということで、私は「集中と選択」でなく「抽出と強化」、つまりいろんなものがある中で抽出して強化することはどうでしょうかということ。それから、国による衛星通信研究は不可欠ということで、これは衛星通信の研究は民間でできているから、国でやる必要はないのではないかという議論

安全保障関連研究の進め方^{*,**}

- 安全保障関連研究の通常研究との相違点
 - 研究には暗黙の了解が不可欠
 - 研究の「集中と選択」でなく「抽出と強化」を
 - 国による衛星通信研究は不可欠
- 情報の取得と扱い
 - 100%秘密では研究の広がり・投資の波及効果を期待できない。
 - 安全保障には絶え間ない技術革新が必要
 - ・ 秘密情報の95~98%は公開情報の再整理より得られる
 - ・ 学会活動などを通じた幅広い活動により優れた研究ができる可能性
 - 一世代前のシステム性能でもトップレベルを保てるように
 - ・ 性能値そのものの発表というよりもその性能に達するための最適、最大、最小などの研究手法を究め、発表していくことが研究のレベルを上げるために大切

*飯田尚志:「[Space Japan Opinion] 安全保障、特にネットワーク中心防衛システムの核となる衛星通信技術の研究開発をどう進めるべきか」、Space Japan Review, No.59, 60, Dec./Jan.&Feb./Mar. 2008/2009.
**飯田尚志:「[特別講演] 安全保障としての衛星通信: その役割の増大と今後の研究の進め方」、電子情報通信学会衛星通信研究会, No.1EICE-SANE2008-119, 1EICE-SAT2008-64, Feb.26, 2009.

公的研究機関の研究課題

- ランド研究所 (RAND Corporation)^{*}
 - 1946年設立
 - 国家安全保障上の脅威に対する上で必要
 - 国家安全保障上の脅威に対する上で必要なのは外交よりむしろ科学にあるという思考方法
 - 優秀な頭脳を第2次大戦終結後に数えざない
 - 本当は、自らのイメージするところによって神のように世界を作り替えることを狙った
 - 先進的は研究
 - ・ RMAの考え、パケットスイッチング技術、フレイムワーク、ゲーム理論、システム分析、MiniMax定理
 - ・ 合理的選択理論、基礎研究、水爆戦争論
 - ・ 1946年: 人工衛星打ち上げの可能性の調査に着手
 - ・ 1958年: コロナ作戦
 - ・ 1960年: 通信衛星開発に関する政策問題の研究 (NASA委託)
 - ・ 一時的に22人
 - 設立時の注目すべき理念
 - ・ 基礎研究に由来以上の多額の資金を投じること。
 - ・ 自身の研究を進める上で必要な自由を最大限与えるべきであること。
 - ・ いるいるな制約を最小限に止れば、陸軍の衛星の今までの想像できなかったような新しい貢献をすることとされること。
 - ・ 独断的・独断的な意思決定を促すことで最も効果的な方法は研究者全員に同等の権限を与えて競争させること
- 公的研究機関の研究課題は安全保障関連に集中はどうか^{**}
- (独)情報通信研究機構
 - 従来の研究開発の理念は今後も妥当。
 - ・ 新しい電波数帯の開発、資源の有効利用技術の開発
 - ・ システムの強靱性の追求
 - ・ 妨害(ジャミング)や破壊に耐える技術
 - ・ 偽装処理やアンテナビーム形成技術
 - ・ ミリ波帯以上の衛星通信技術
 - ・ 複雑なアラスカで環境下での電波伝搬などを理解している研究者は必須
 - ・ 通信(固定、移動、ブロードバンド、衛星間通信)
 - ・ 測位(準天頂、日本版GPS)
 - ・ 監視・警告(直観、画像、ミサイル警告、赤外線探知)
 - ・ 電波伝搬(電離層伝搬、宇宙天気予報含む)
 - 研究者の散逸を防ぎつつ、研究課題の位置付けを明確にして再認識重要

*アレックス・アハラ(牧野洋訳):「ランド、世界を支配した研究所」(株)文藝春秋, Oct.30, 2008.
**飯田尚志:「Space Japan Opinion: 衛星を眺めるか」、Space Japan Review, No.35, Jun./Jul. 2004.

はあるが、実は違う。例えば、大型アンテナでも盗聴衛星に使えるかもしれませんが大いにやっておく必要がある。しかも機密度が高いですから秘密にしてやらなければいけないということで、国としては技術を持っておく必要があるということです。ただ、情報の取得と取扱については、何でも 100%秘密にすると研究の拡がりがない。投資の効果が期待できません。それに安全保障には絶え間ない技術革新が必要なわけです。日本が止めれば隣国がどんどんやってしまう。競争が激しいわけです。機密情報の 95~98%は公開情報の再整理からできてくるということが言われていますので、やはり学会活動などを通じて幅広い活動を行うといい研究ができてくる。それでは発表するにはどうするかというと、1世代前のものを発表してもいいし、1世代前のものでも学会ではトップクラスだというものを目指すべきであると思います。

安全保障の研究に関して、ランド研究所は 1946 年に設立されましたが、何故作ったかという、大戦中は優秀な人が軍の研究に関与していたけれど、戦争が終わると散ってしまうということで、それを何とか散らせないようにしようとして創ったということです。ここから我々に関係するような研究が沢山できていますし、先進的研究として、RMA の考え方、パケットスイッチング技術、フェイルセーフ、ゲーム理論、システム分析、MiniMax 定理とかみんなランドから出ている。それで、ノーベル賞を取った人が 29 人出ているそうです。ここは空軍がお金を出したが、お金を出しても干渉しないということでやったみたいで、今ちょっと衰退しているみたいですが、そういう研究所であったようです。

それで、公的研究機関の研究課題は安全保障関連に集中はどうかということです。私の提案ですけど。先ほどの「集中と選択」というのもノーベル賞を取るにはいいと思うんですが、安全保障には適さない。で、公的研究機関の研究課題は安全保障関連に集中してはどうかと思います。情報通信研究機構の研究の中にも見方を変えると安全保障に関するものが一杯ある。衛星通信以外に、電波伝搬に関する研究、宇宙天気予報などをやっているが、今その辺がネグレクトされつつある。ただ、電波伝搬の研究は非常に大切で、分かった人がいないと、先ほどの核戦争のときの問題もありますから、大切にしていかなければいけないということです。ですから、研究者の散逸を防ぎつつ、研究課題の位置付けを明確にして再認識することが重要だと思います。

次に、安全保障を語る上で必要なこととして、私が読んだ文献を挙げてみました。上の 2 つは植田さんからお聞きして最近読みました。孫崎 享: "日米同盟の正体 迷走する安全保障", 講談社現代新書, No.1985, 2009 というのは非常に面白い本で、外務省に居られた方ですが、日米の安全保障条約の目的は日本に原爆を持たせないということが一番の目的だそう

です。日独に原爆を持たせないというのが一大決意のようです。それと CIA は日本の政界を牛耳ってきたらしい。武村官房長官を辞めさせたのもアメリカらしい。あの人に言うと情報が筒に抜けになるという恐れがあったからということです。孫崎さんという方はちょっと鳩派なんですね。

清谷信一: "防衛破綻「ガラパゴス化」する自衛隊装備", 中公新書ラクレ, No.33, 2010。これも面白い本で、防衛予算は GDP の 1%使っているがほとんど役に立っていないみたいです。私、一番ショックだったのは、自衛隊の人は上着はともかくとして下に着るシャツは自分のものを着ているのだそうです。自分でお金を出して。GI は何故 GI と言うかということ、

安全保障を語る上で必要なこと

- 孫崎 享: "日米同盟の正体 迷走する安全保障", 講談社現代新書, No.1985, 2009.
- 清谷信一: "防衛破綻「ガラパゴス化」する自衛隊装備", 中公新書ラクレ, No.33, 2010.
- ジョージ・フリードマン、櫻井祐子訳: "100年予測 世界最強のインテリジェンス企業が示す未来覇権地図", 早川書房, 2009.
- 加藤陽子: "満州事変から日中戦争へ シリーズ日本近現代史⑤", 岩波新書, No.1046, 2007.
- 小谷 賢(こたにけん): "日本軍のインテリジェンス なぜ情報が活かされないのか", 講談社選書メチエ, 2007.
- マイケル・バスターソン、角敦子訳: "エニグマ・コードを解読せよ一新証言にみる天才たちのドラマ", 原書房, 2009.
- 村上龍: "半島を出よ(上)(下)", 幻冬舎文庫, 2007.
- ケント・E・カルダー、武井操一訳: "米軍再編の政治学 一駐留米軍と海外基地のゆくえ", 日本経済新聞社, 2008.
- アレックス・アベラ[牧野洋訳]: "ランド 世界を支配した研究所", (株)文藝春秋, 2008.
- 中村好寿: "軍事革命(RMA) <情報>が戦争を変える", 中公新書, 2001.
- 大森義夫: "日本のインテリジェンス機関", 文春新書, No.463, 2005.
- H.マーク・A.レヴィン、柘植監訳: "研究開発のマネージメント", 三田出版会, 1989.
- 手嶋龍一、佐藤優: "インテリジェンス 武器なき戦争", 幻冬舎新書, 2006.

15

Government issue という。全部着ているものから何まで政府で支給されてそれで軍隊であると。その考えが今無いみたいです。私、この前、ワシントンのモニュメントタワーの守衛を見るとみんな Government issue で同じものを着ていました。非常にショックでした。

ジョージ・フリードマン、櫻井祐子訳: "100 年予測 世界最強のインテリジェンス企業が示す未来覇権地図", 早川書房, 2009。これも面白い本で、地政学からきている話で、アメリカはこれから衰退するのではないかと言われているが、アメリカの世紀はこれからだという。何故かというアメリカは世界の海を海軍力で抑えている。これからの 100 年間でアメリカに対抗する国として 3 つ、日本、トルコ、ポーランドだそうです。中国は駄目らしい。西は砂漠、東は海、独裁でバブルが起こって崩壊する。2050 年に日本はアメリカと戦争するという。月を挟んで宇宙戦争をするという。

加藤陽子: "満州事変から日中戦争へ", 岩波新書, No.1046, 2007。東大の先生ですが、これはちょっと読むには堅くて辛いですが、当時日本はいろいろな手を使って満州を占領していったということです。

小谷 賢(こたにけん): "日本軍のインテリジェンス なぜ情報が活かされないのか", 講談社選書メチエ, 2007。防衛研究所の人ですが、日本軍が暗号を大事にしなかった。海軍と陸軍で暗号も違うし、私の生まれた昭和 17 年 6 月にはミッドウェー海戦が起こっている。そのとき日本海軍の暗号をアメリカは解読していたが、場所の「AF」というのが特定できなかった。そこで、米軍はミッドウェーには蒸留装置に故障で水がないよと平文で流した。そうしたら日本海軍が「AF」の蒸留装置が故障という暗号を流したんで、「AF」はミッドウェーだと断定されたということです。

マイケル・パターソン、角敦子訳: "エニグマ・コードを解読せよ—新証言にみる天才たちのドラマ", 原書房, 2009。英軍の情報機関の話。チューリングが大活躍した話。英軍の将校が情報施設が必要と予算を要求したら財務に拒否された。そうしたら、その将校が自費で貴族の館を購入して情報機関を作ったという話。チューリングは変わった人で、一般社会では通用しないような人で掛け算ができないらしい。何故かというあまり秀才なので、いきなり高等数学に進んでしまったという。

村上龍: "半島を出よ(上)(下)", 幻冬舎文庫, 2007。読まれた方もおられるかもしれませんが、恐ろしい話で、北朝鮮の特殊部隊が九州を占領する話。北朝鮮で反乱が起こって亡命したということで、福岡の球場を人質を何万もとって占領してしまう。結末はくだらないのですが、恐ろしい話です。

ケント・E・カルダー、武井揚一訳: "米軍再編の政治学 一駐留米軍と海外基地のゆくえ", 日本経済新聞社, 2008。米大使館にいた人で、奥さんは日本人ですが、基地があると経済的にもいいという話。

アレックス・アペラ[牧野洋訳]: "ランド 世界を支配した研究所", (株)文藝春秋, 2008。これは先ほどからお話した本です。

中村好寿: "軍事革命(RMA) <情報>が戦争を変える", 中公新書, 2001。RMA の話。

大森義夫: "日本のインテリジェンス機関", 文春新書, No.463, 2005。内閣情報調査室の話。ここに秘密情報の 98%は通常の情報の整理から得られると書いてある。

H.マーク、A.レヴィン、柘植監訳: "研究開発のマネージメント", 三田出版会, 1989。これはちょっと古い話であるが、原子力潜水艦の開発でのすごいマネージメントの話。

手嶋龍一、佐藤優: "インテリジェンス 武器なき戦争", 幻冬舎新書, 2006。これも面白いです。

最後に、2つ言いたい。研究者、特に若い研究者が入ってこないようなところは駄目なんで、若い研究者が不可欠。研究には暗黙の了解が不可欠。それから、衛星通信を安全保障に生かすためには防衛関係専門家と衛星通信専門家の緊密な連携が必要です。衛星通信関係者は防衛に素人なので、分からない。逆に防衛の人は今まで禁じられていましたから多分衛星が分からない。ですから密に連携しないとこれからの展開は難しいと思います。

それから、ランド研究所の言葉として「国家安全保障という目標達成には絶え間ない技術革新が必要」というのがあります。このように非常に緊張した事項ですので、日本の科学技術を駄目にするような政策をとると我々が困るだけでなく、外の国が喜ぶ。大喝采する。研究の事業仕分けなどは大喝采だと思います。どうもありがとうございました。

おわりに

○最後に2つ

- 研究者、特に若い研究者からのいろいろな提案が不可欠
 - ・ 研究指導者の研究理念とか目標の明確化、研究開発すべき技術課題に対する深い理解が重要
- 研究には暗黙の了解が不可欠
 - ・ 指導者の素質が非常に大きく影響する
 - ・ 衛星搭載機器は宇宙実証を経て始めて実用になるという特殊性
 - ・ 宇宙を知っている者が研究をマネージするか否が大きな問題

○衛星通信を安全保障に生かすために

- 防衛関係専門家と衛星通信専門家の緊密な連携必要

○最後に、ランド研究所の言葉を引用する

- 「国家安全保障という目標達成には絶え間ない技術革新が必要」
(National security is an ever-receding goal requiring incessant technological improvement.)

16

我が国の安全保障を考えるディスカッション

@AIAA-JFSC総会

日時:2010年6月1日 14:30~17:00

プログラム

司会:福地 一

安田靖彦:わが国の安全保障問題についての一私見

飯田尚志:安全保障としての衛星通信の考え方

若菜弘充:安全保障と衛星通信—通信技術の観点から

((司会)それでは、若菜さんお願いします。

(若菜)Military communication には抗堪性やLPI/LPDなどの言葉がでてくるので、それらを調べて、どのような内容かを紹介し、無線通信や衛星通信技術との関係について何人かで議論しましょうということでしたが、まずは私が報告することにします。これまでのSpace Japan Review誌編集委員会でもたびたび話題になった「抗堪性」という言葉は、辞書を引いてもなかなか出ていないのですが、軍事関係ではよく使われているようです。Anti-jamming、LPD/LPI、CIAは無線通信技術に関係があります。Military communicationの中で、我々衛星通信の研究者にとって身近な技術がどこで関係があるのか、その特徴、課題、解決手段や最近の誤り訂正符号化技術についてお話ししたいと思います。これまで衛星通信では畳み込み符号やリードソロモン符号が使われてきました。その後、ターボ符号へ移ってきました。さらに、最近ではLDPC 符号が使われ始めています。最近ではレートレスコードがMilitary Communication関係で出てきていますので、これについてもご紹介したいと思います。

まず「抗堪性」ですけれども、これは軍事用語で、航空基地やレーダサイトなどの軍事施設が敵の攻撃に耐えてその機能を維持する能力ということで、この定義はハードウェア的な内容で、無線通信ではありませんが。これに関連する無線通信の技術としては、低検出確率(LPDP: Low Probability of Detection)と低妨害確率(LPI: Low Probability of Intercept)があります。この観点で無線通信のシステムを設置しないといけないということで、信号が検出されない、妨害されないということです。無線通信技術としては身近なテーマだと思います。これ以外にはサイバーテロに出てくるCIA があります。これは、3つの単語の頭文字からなります。Confidentiality(機密性)、これは認可された人だけが情報にアクセスできること。Integrity(保全性)は、情報が改竄されないようにきちんと維持できていること。Availability(可用性)はシステムの壊れにくさ、障害の発生しにくさや障害発生時にどれだけ早く修復できるかということです。これらが抗堪性と同じ意味で、無線通信技術や情報セキュリティ技術にとっては大切になるわけです。具体的にどのような研究がされているかをご紹介します。例えば、Anti-Jamming やLPI/LPD を有する無線通信システムにはどのような技術課題があり、どのように解決されようとしているか。無線通信方式でスペクトル拡散技術は、周波数を拡散することで傍受されず妨害を受けにくい方式として開発されてきましたが、それだけでは電波のエネルギーを検出し

内容
• 抗堪性, Anti-jamming, LPD/LPI, CIA
• Military Communication: network centric
– mobile ad-hoc networks
– 特徴、課題、解決手段
• 新しい誤り訂正符号化技術
– Low-Density Parity-Check (LDPC) Codes
– Rateless Codes, etc.

抗堪性(invulnerability), LPD/LPI and CIA
• 抗堪性:航空基地やレーダサイトなどの軍事施設が、敵の攻撃に耐えてその機能を維持する能力。 – “In military circles Vulnerability is a subset of Survivability (the others being Susceptibility and Recoverability). Vulnerability is defined in various ways depending on the nation and service arm concerned, but in general it refers to the near-instantaneous effects of a weapon attack. In some definitions Recoverability (damage control, firefighting, restoration of capability) is included in Vulnerability.” in Wikipedia
• Low Probability of Detection (LPD):低検出確率
• Low Probability of Intercept (LPI):低妨害確率 – Low probability of intercept electromagnetic emitters, such as radio and radar transmitters, use a number of mechanisms to minimize the probability they will be detected by electronic intelligence sensors, and, if detected, precisely located. – Methods to do this include: Frequency agility, Spread spectrum, Directional antennas, Ultra-low Side-lobe Antennas, Encrypted and highly variable pulse trains, Multi-static systems, Passive radar.
• Confidentiality「機密性」:認可された者だけが情報にアクセスできること
• Integrity「保全性」:情報の正確性や完全性が維持されること
• Availability「可用性」:システムの壊れにくさ、障害の発生しにくさや、障害発生時の修復速度などによって計られる。

て、送信している方向が分かってしまう。ですから信号処理技術だけではうまくいなくて、アンテナの低サイドローブ化やフェーズドアレーアンテナを組み合わせる特定の方向だけに必要な時に電波のエネルギーを送る工夫が必要になる。それは通信するものがどこにいるかによって、耐妨害性を高める様々な工夫が考えられます。飛行機同士なのか、飛行機と地上との間なのかに応じて、通信方式(周波数ホッピングやUWBも含め)アンテナの方式、大きさ、使用する周波数帯(吸収バンドを考慮してミリ波を使うことも考えられる)、電波伝搬特性などが検討課題になります。空間光通信も優れた耐妨害性やLPD/LPIの観点から候補になります。

Mitigate Jamming and Increase LPI/LPD

- スペクトル拡散、周波数ホッピング、ウルトラワイドバンド (UWB)
- スマートアンテナ: 超低サイドローブ、フェーズドアレーアンテナ
- 吸収バンド使用: 55-65 GHz
- 空間光通信

▲ Protecting against silent threat

軍用通信だけがanti-jammingの問題かというそうではありません。衛星放送に対するjammingの問題もあります。例えば2003年キューバからのjamming、2010年にイランで放送しているBBC 或いはドイツの番組がたえずjamming を受けており、EU はそれに対して抗議をしているという現実的問題がある。タイのテレビ番組に首相が出演した時に非常に強い電波妨害があったと報じられている。これらは衛星放送を使っているチャンネルでそういうことがある。大規模災害時に携帯電話などの無線通信システムが使えない場合もある。自然災害ではない非常時に衛星通信も使えない場合もあるだろう。普通の人々が通常使っているような通信手段は、きわめて妨害を受けやすい状況にある。

衛星(放送)ネットワークへの現実的な脅威

Libya jamming 'exposed vulnerability'

BBC joins international protests against Iranian TV interference

次に最近のMilitary communicationの研究開発で、どのようなテーマがあるかをお話しをしたいと思います。私自身は軍用通信を技術的に深く知っているわけではありません。IEEE Communication Magazineで定期的にmilitary communication の特集をしていますので、そこで公表されている範囲内で、特に2009年10月号に掲載されている論文に基づいてお話しします。最近のテーマでは、兵士同士の無線通信にターゲットを置いた論文がいくつかあります。そこでは商用ネットワークでは通常ないような特殊条件の使用環境で使うことになる。あるいは高度なセキュリティレベルで通信を行わなければならない。例えば頻繁に移動しながら使用する、複雑な電波伝搬の環境下で使用するなど、通常の無線基地局と携帯端末間で使われているような技術をそのまま持ってきてすぐには使える状況にはならない。この場合、通信は兵士同士の通信ですから、1対1のアドホック通信です。IEEEでもアドホック通信は標準化されている技術ですが、そのまま軍用通信に適用するとかならずしもうまくいかないところがある、どのような課題があるかを論文では紹介しています。実際に実証実験を行った結果の紹介もあります。電波伝搬環境も通常とは違い絶えず電波が遮断されるなど信頼性の低いネットワークであったり、帯域制限がかかったり、通信環境が絶えず変動し、また通信負荷も変動する。最初の論文ではそのような条件下での実証実験結果を述べています。無線LAN (IEEE 802.11g) をそのまま使っても最大でも1/50程度の1Mbps くらいしか伝送ができない。都市環境では不感地域が絶えず発生し、遠隔操作型のロボットでは通信断により制御不能になる。頻繁に移動したり、飛行

Military Communications

in IEEE Communications Magazine, October 2009, Vol. 47, No. 10

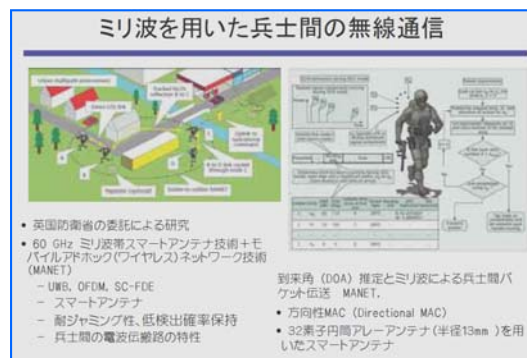
- S. Alexander (Telcordia Tech.) et al., "The dynamic community of interest and its realization in ZODIAC"
- C.R.A. Gonzalez (Virginia Tech) et al., "Open-source SCA-based core framework and rapid development tools enable software-defined radio education and research"
- N. Suri (Florida Inst) et al., "Communications middleware for tactical environments: observations, experiences, and lessons learned"
- O. Younis (Telcordia) et al., "Cognitive MANET design for mission-critical networks"
- S.L. Cotton (Univ. Belfast) et al., "Millimeter-wave soldier-to-soldier communications for covert battlefield operations"

特約な挑戦的テーマ

- ・ 商用ネットワークアプリケーションには通常ないような特殊な使用条件と環境、高度なセキュリティレベルの必要性
- ・ 頻繁に移動しながらの運用、制約条件下での通信機能の実現、複雑な電波伝搬環境の下での使用など

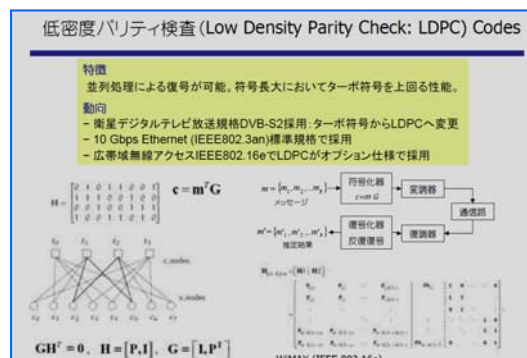
体と地上設備間の速度の違いも通信の障害になる。ロボットの遠隔操縦、センサーデータの収集、VoIPによる音声通話、メッセージと多様なデータタイプでの通信が必要になる。戦略的なネットワークにおけるデータフローは様々で、その優先度も異なる。過度の通信障害を避けるためには、送信するデータ量を注意深く制御する必要が生じます。実証実験の結果、TCP/IPではこのような使用条件下では伝送性能に限界があることが明らかになったと述べています。

次の論文では、60GHz帯ミリ波を用いた兵士間の無線通信を紹介しています。スマートアンテナ技術(半径13mmの32素子円筒アレーアンテナ)とモバイルアドホック(ワイヤレス)ネットワーク技術 MANET 及び UWB、OFDM、SC-FDE 技術等を用いています。兵士の携帯端末では到来角(DOA)を推定し兵士間のパケット伝送を実現します。これらの技術基盤の基で耐ジャミング性、低検出確率を保持しようとするシステムです。



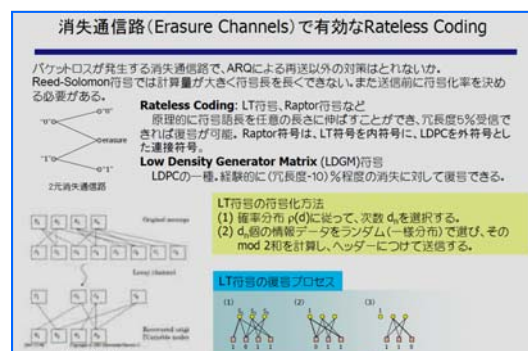
次の論文では、軍用通信で用いるZODIACシステムで、3つのセキュリティコンセプト(機密性、完全性、可用性)を有するネットワークアーキテクチャに関するものです。1つのネットワーク内に複数の動的なコミュニティが形成され、それぞれのコミュニティ内の参加メンバー、アプリケーション、リソースは強制力のあるポリシーに基づいて管理される。つまり動的なコミュニティ内は特定のアプリケーションのみが使用できるようになっている。地理的な位置情報に基づいてルーティング等を行うものです。続く論文では、Cognitive MANETを紹介しています。コグニティブ技術を用いて隣接ノードを発見し、自動的にルーティングを行う。難しい通信環境下でもいかに安定した信頼性の高い通信を確保しているかの研究です。以上がMilitary Communicationの研究概要です。

次に、誤り訂正符号化の最近の話題についてご紹介します。まずは、低密度パリティ検査符号 (Low Density Parity Check: LDPC) です。LDPC符号は、非常に疎な、行列内の非ゼロ要素の数が非常に少ない検査行列を用いる線形ブロック符号です。並列処理による復号が可能で、符号長が長くなるとターボ符号を上回りシャノン限界に近い特性が得られるのが特徴です。最近では、衛星デジタルテレビ放送規格DVB-S2の誤り訂正符号がターボ符号からLDPCへと変更になりました。10 Gbps Ethernet (IEEE 802.3an) 標準規格で採用され、広帯域無線アクセス(IEEE 802.16e)でもLDPCがオプション仕様として採用になりました。図にあるように、メッセージ m を、符号化器で生成行列 G を乗算して符号語を得ます。検査行列 H と生成行列 G の間にはここで示すような関係にあります。これは、WiMax (IEEE 802.16e)の検査行列です。LDPCの復号アルゴリズムの一つであるsum-product復号法を説明します。この図は、タナグラフといい、下側は変数ノード(v_nodes)といい検査行列の列の数に等しいノードを持ちます。上側はチェックノード(c_nodes)といって、検査行列の行数に等しいノードを持ちます。ここでは4行8列の検査行列ですので、変数ノードが8つ、チェックノードが4つあります。検査行列 H の m 行 n 列の要素が1の場合に、 n 番目の変数ノードと m 番目のチェックノードの間が連結するように図示されます。このグラフを用いて再帰的に計算を行い、復号化を行います。～当日は再帰的な計算の仕方を説明しましたが、ここでは省略いたします。～



次に消失通信路(Erasure Channels)で有効なRateless符号について説明します。衛星通信では、伝

送品質を上げるために、先ほど述べたような前方誤り訂正(FEC)と自動再送要求(Automatic Repeat Request: ARQ)を組み合わせ用いられてきました。衛星通信のように伝搬遅延が大きい通信回線では伝送速度が大きくなると再送遅延による影響が大きくなるため、ARQが有効に働きません。また移動体衛星通信や光空間通信などのように受信信号がバースト的に信号消失が起こってパケットロスが発生するような消失通信路では、再送以外に対策があるでしょうか。Reed-Solomon符号では計算量が大きくなるため符号長を長くできない。また送信前に符号化率等を決める必要があります。この消失通信路に有効な符号化技術として、LT符号やRaptor符号などのRateless符号が提案されている。Rateless符号では、原理的に符号語長を任意の長さに伸ばすことができ、冗長度5%受信できれば復号が可能である。後者のRaptor符号は、LT符号を内符号に、LDPCを外符号として接続符号です。LT符号の符号化方法は、(1)確率分布 $p(d)$ に従って、次数 d_n を選択し、(2) d_n 個の情報データをランダム(一様分布)で選択し、そのmod 2和を計算し、ヘッダーをつけて送信する。このように符号長を、符号化し順次送信している途中でも任意に伸ばすことができるため、符号化率が可変になる。～詳しい符号・復号プロセスの説明は省略します～。



まとめますと、military communicationでは通常の商用通信回線と比較して特異的な通信環境下での通信技術が必要になる。頻繁に移動しながらの運用、厳しい制約条件下での安定な通信機能の実現、複雑な電波伝搬環境下での使用が前提となる。また高度なセキュリティレベルが必要で、耐妨害性、低検出確率等が重要である。これはmilitary communicationだけの要求条件ではなく、非常時、大規模災害時における通信も同様な性質が必要になる。そのためにはロバストで、セキュアな通信、汎用ではなくその通信環境条件に適合した通信、コグニティブ無線技術を応用した柔軟な無線通信技術が必要になる。衛星通信システムでは、さらに何が技術課題になるだろうか。また何を提供できるだろうか。次のテーマとして今日の講演を終えることにしたい。ありがとうございました。■

- まとめ
- 通信環境の特異性
 - 特殊な使用条件と環境(頻繁に移動しながらの運用、制約条件下での通信機能の実現、複雑な電波伝搬環境の下での使用)
 - 高度なセキュリティレベルの必要性: LPD/LPI, CIA
 - 非常時、大規模災害時における通信も同様な性質が必要になる。
 - robust, secure, specific, cognitive, etc.
 - 衛星通信システムは何を提供するか？