# 米国情報セキュリティ関連オフィス訪問
# 報告書

平成 15 年 9 月

日本ネットワークセキュリティ協会

# 米国情報セキュリティ関連オフィス訪問報告書

## 目次

## 1. はじめに

土居範久（視察団団長）

パソコンの世帯普及率が２００２年末で７１．７％、インターネットの人口普及率が５４．５％、ＤＳＬ・ＦＴＴＨ・ＣＡＴＶの常時接続サービス利用者数が９００万人を越えた現在、まさに高度情報社会を実現するためのインフラが整ってきたと言えるでしょう。また、ネットバンキング・ネットオークション・ネット証券など、従来の単なる情報伝達だけでなく、現実の経済活動・社会生活と直接に関係したサービスが続々と誕生しています。特に住基ネットに代表される国家的 IT プロジェクトが進む中、ネットワークを中心とした新たな社会が構築されようとしていることを認識すべきでしょう。

インターネットでつながれた社会は言うまでもなく、国境なき世界であり、この世界でどのようにして我が国と我が国民の生命および財産を保全するのかが問題です。もはや我が国の島国という地理的特長はこのインターネット社会においては優位に作用するものではなく、我が国以外の思想・信条・価値観ならびにその行動に直接さらされています。

また、翻って国内のことに目を向けますと、急速なインターネットの普及が利用する人々の IT に対する理解、特に情報セキュリティに対する認識が限りなく拡大しつつあります。これは、まるで昭和４０年代の自動車社会の高度発展時期と同じように思われ、交通事故の多発が社会問題化した時期と似ているように思われます。

このような認識のもと、９．１１の同時多発テロから急速に国土安全保障に力点を移すとともに、その安全保障の一環として情報セキュリティを国家戦略の要諦として位置づけた米国の情報セキュリティに対する取り組みを調査したく、JNSA 米国情報セキュリティ視察団を結成し、実施しました。これは、米国が感じている危機感が我が国においても共有できるという考えから発想したものです。したがって、今回の視察は特に米国政府関連の組織を対象とし、彼らが持っている問題認識ならびにその対処をどのように考えているのかを中心に意見交換を行ってきました。視察団は、巻末に示しましたように、情報セキュリティに関して問題意識ならびに知見を有する我が国を代表する方々で構成し、７月２８日より８月１日の５日間、以下の米国政府機関ならびに民間企業を訪問し、意見交換を行いました。

今回の米国視察においては、米国の情報セキュリティに対する長い歴史を感じるとともに、国家安全保障という視点からの情報セキュリティと米国型自由主義経済のポリシーに基づく民間セクターの意識とをどのように折り合わせるのかに問題があるように感じました。つまり、ネットワークならびにインターネットが発達したことにより、情報インフラが国家安全保障と民間セクターの活動の両方に共用せざるを得ないことから、民間セクターの脆弱性が、ひいては国防の脆弱性になり得るところに問題があるように感じられます。ただ、我が国とまったく異なりますが、きわめて重要な点は、国防というキーワードが民間セクターも含む米国全体の情報セキュリティシステムならびに産業を牽引していることです。重要インフラの９５％以上は民間セクターのものであり、民間セクターの協力なくしては重要インフラの情報セキュリティならびに物理的防衛について実行できないことを認識し、この協力関係を如何に樹立するかがテーマとなっているように思います。このよう

に米国は情報セキュリティ施策を推進する上で、民間セクターの協力が重要と考え、そのために施策のひとつとして積極的にISACの設立に関与し、脆弱性情報の提供などを推し進めています。ISACは業界等をベースとして、すでに13のISACが設立されていますが、その運営は順調とは言いがたいようです。また、ISACを運営した結果として、彼らが経験したことは、個々のISACが共有できる情報が８０％以上占めているという事実も興味深い点です。これらの経験から、ISAC間の連携を強めるべくISACカウンシルを設立していることも注目に値します。

上述してきたことは、脆弱性の発見とその防御についてですが、そもそも脆弱性を発生させないシステムや製品の開発も重要です。この場合、民間セクターの製品ならびにシステムについては、ある一定のセキュリティレベルを単に要求することだけでは、それに到達しようとする動機が民間セクターには発生しないでしょう。そこで、民間セクターは基本的に利益を追求しており、これを刺激しないと民間セクターは積極的にセキュリティレベルの高い製品を出してこないであろうことを認識したようです。また、セキュリティレベルを高度にする場合にかかるコストならびにその評価認定にかかるコストが大きく、これをどのように吸収するかについても問題があると認識しています。特に、成功した大企業はいいとしても、ベンチャー企業に代表されるスタートアップ段階の小企業についてはコスト問題が大きいと考えているようです。これらの解決については、今後の課題として、セキュリティ標準の見直しも含めて考えているというところが興味深いところです。

今回の米国視察を終えて我が国のことを考えますと、我が国の国益と国家安全保障を確保するために，どこが、なにを、誰に対して責任を持つのかについてのグランドデザインを早急につくり、高度情報社会のあり方に対する国民的コンセンサスを形成することが喫緊の課題となっているように思います。

今回、有志が集まり、自発的に実行したJNSA米国情報セキュリティ視察団の本報告書が、我が国の安全で安心な高度情報社会を実現してゆくためになすべきことを検討される際の一助となれば幸いです。

最後になりましたが、今回の米国視察を実行するに当たって、訪問先の選出・手配などに多大なるご支援とご協力を賜った内閣官房、経済産業省、総務省、米国大使館、株式会社シマンテック、三菱商事株式会社、米国三菱商事会社、日本電気株式会社に感謝致します。

以上

## 2. Department of Commerce

日時:　2003年7月28日　　9:00 ～ 12:00
場所：　Hoover Building/Department of Commerce
出席者: Ms. Patricia M. Sefcik
Director, Office of Information Technologies and Electronic Commerce
International Trade Administration
U.S. Department of Commerce

Ms. Helen Anderson Shaw
Senior Telecommunications Policy Advisor
National Telecommunications and Information Administration
U.S. Department of Commerce

訪問先概要：
商務省の役割は、日本の経済産業省というより、中小企業庁に近いと考える必要がある。主に大企業は独自に政府・議会に働きかけを行っているが、中小企業にはそれができない面があり、商務省が中小企業に重点を置いて対応していると考えるとわかりやすい。

内容：
（１）電子商取引のあり方とＯＥＣＤ準拠ならびに情報セキュリティの国際協力の必要性
(Ms. Patricia M. Sefcik)

■商務省のミッション（３つの目的を持っている）
米国の輸出を推進し、工業力を高める。
米国の通商政策の策定、各国の条約遵守の監視
海外企業が米国企業のビジネス展開を行う場合の対応
■自分の局は、名前の通り、２つのグループ、ITチームと電子商取引チームがある
■以下はプレゼン資料に従って説明を行う。
－ ITチーム： IT産業の専門家集団で、通商政策、IT産業発展、海外IT政策・IT産業の分析を行うことにより、米国IT産業に寄与する。
ハードウェア業界、ソフトウェア業界、ITサービス業界等があり、IBMやマイクロソフトなどの大企業から、従業員が１、２名の企業まで範囲としている。
情報技術産業の標準化、カウンセリング、海外諸国の関税制度、海外市場の拡大等の情報提供を行っている。
－ 電子商取引（EC）チーム： 従来取引では通商障壁があり、それを除去することが仕事であったが、ECでは、通商障壁を各国が持ち込めるかの分析から始めなければならない。
大企業だけでなく、中小企業の国際的なECへの対応があり、グローバルなフレームワークへの対応が大切である。
重要事項としては、消費者保護、ADR（Alternative Dispute Resolution: 裁判外紛争処理制度)、プライバシー、電子政府、SPAM、電子認証、重要基盤保護がある。
日本のようなIT先進国は問題ないが、発展途上国では、基本的な問題、通信基盤、デジタルディバイドなどを考える必要がある。
文化的セキュリティについては、OECDの９原則を重視している。
日本とは、OECD、APECに加盟しており、APECでの対応も行ってきた。
また、去年はEUとの二国間協議を行ったし、今年10月には日本との協議があ

る。
日本との二国間での検討事項
IT ワーキンググループがあり、以下の検討を行っている。
- EC の規制や障壁の除去。民間企業同士の自主的ルールやガイドラインの作成
- 知的所有権の保護、ISP の責任、商標権や著作権の保護
- EC 政策の強化、日本のプライバシーの保護の内容のヒアリング、
- 電子署名については、技術的に中立であるべきと考えている。
- ネットワークセキュリティガイドライン。９月に日本と会合がある。
- IT 製品調達。日本政府の調達の考え方
- ３月に東京・京都で、EC 教育に関して会合を持った。

■コメント及び質問

① Japan Security Market の説明
スキルマップに興味を持っていたが、プレゼンのスキルマップ図は、ある人が持っているスキルを示したものであることが最初は理解できていなかった。（スキルとして持つべきレベルを示したものであると誤解していた。）

② 日本の Common Criteria の対応について
ISO15408 を JIS 化しており、政府は省庁の利用製品では、ISO15408 の認証取得の製品を調達することが望ましいとしている。
認証スキームは 2002 年末から始まっており、２評価組織ができているが、製品としては２つしか認定を取得していない。
CCRA については、今年中に取得を目指している。

③ 政府への申請が非常に煩雑であるが、電子政府でも同様な問題はないのか？
電子政府では可能な限り、一元的な申請を目指している。

④ 日本の個人情報保護が障壁にならないか
米国・EU でも EU 指令の対応のため、Safe Harbour での対応を米国がやっているが、同じような方法が日米間であっても良いのではないか？

⑤ リスク管理について
日本の情報セキュリティに関連したリスク管理は遅れている。CSI/FBI 調査等の内容を参考にしたいと考えている。
脆弱性データベースについては、団長の土居先生が行っている。

⑥ 日本での PKI の利用は？
政府で一部使っている。またインターネットショッピングの支払いを銀行から直接行うデビット決済に電子証明書を使っている。

⑦電子署名法が貿易障壁にならないことを願っている。PKI は中小企業ではまだ高くつく。パスワード、カード等安価な認証方式も使えるようにすべきである。

（２）Economic Security Component of CIP(Critical Infrastructure Protection) Role of Industry and Government(Ms. Helen A. Shaw)

■ CIP（重要基盤保護）について
初期には国防と法執行機関の分野であったが、911 テロ以降はセキュリティが経済問題としても取り上げられるようになった。
経済問題としては、商務省、財務省、国家安全保障省が役割を担っている。
CIP については、商務省は 100 年間たずさわってきた。
商務省と産業界との連携及び信頼性
CIP の解決要因としては、以下の３つの要素が大切
- 技術：標準化
- プロセス： ガイドライン／ポリシー
- 人： 最善策、教育・啓発

■ コンピュータ犯罪について

CSI/FBI 調査についての説明

■ CIP プログラムについて

BIS： 輸出行政を担っており、商用・軍用とも対応。

TA/NIST： IT 関連の標準化を行っている。連邦政府における緊急なものでないものに対応している。

EDA： 中小企業へのサイバー攻撃への対応

■ セキュリティ標準

NIST が担っており、緊密な関係を構築している。

■ 重要基盤保護

重要基盤の 95%以上は民間が保有している。

毎月１回、50～70 名を集めて会合を行っているが、これは、経済安全保障の問題であるため。

民間のビジネス活動を高めるために、セキュリティ、リスク管理などに関連した内容をこの会合で話をしている。

政府と民間のパートナーシップが重要であるとの認識の下に行っている。

■コメント及び質問

① 民間との会合の具体的な方法

中小企業以下を対象に行っている。DC 以外の地区での開催も行っている。

サイバーテロなどの説明はかえって逆効果になってしまった。

② 民間との会合の内容は

情報技術やプロセスについての情報提供を行っている。

会合の目的が効率的になっているとは言えない状況である。

商務省と産業界は一心同体で動くことを考えている。

③ 事業継続計画（BCP）を持っている企業割合

ダートマス大学と意見交換が行われたが、担当でないので詳細はあまり知らない。 DHS がどの様に関係してくるかもまだ明確になっていないため、もう少し時間が掛かるかも知れない。

BCP については、金融機関以外の業界では規制があるのかについては、良く知らない（もう少し勉強しなければならない)。

④ BS7799 について

NIST の役割になっている。米国としては BS7799 では不十分であると考えており、ISO に対して何らかの提案をしたいと考えている。但し、詳細は NIST に任せている。

## 3．NIST (National Institute of Standards and Technology)

日時:　2003年7月28日　　14:00 ～ 17:00
場所：　NIST, Gaithersburg
出席者: Dr. Stuart W. Katzke Ph.D.
Senior Research Scientist
Computer Security Division

Ms. Annabelle Lee
Computer Specialist
Computer Security Division

Dr. Susan F.Heller Zeisler,Ph.D.
International Academic Affairs
Office of International and Academic Affairs

訪問先概要：

米国商務省の所管の国立研究所であり、各種の先進的な技術研究開発を行うほか、技術や計量の標準化を所掌している機関である。通商の促進と生活品質の向上のために先進的な技術開発と計量や技術の標準化を行っている。
職員数：約3000人の職員と1600人の臨時職員（アソシエイト）がいる
予算：2003年度の年間予算は＄864M（1000億円超）である。

内容：

（１）主な予算の内訳は以下の通り。

①ＮＩＳＴラボラトリー(計量の技術の標準を所掌している)　　＄352.9 Ｍ
インフォメーションテクノロジー、製造技術、国土安全保障やヘルスケアなどの分野の計量と技術標準について、標準化や研究開発を行い、その結果を公表している。

②アドバンスド　テクノロジー　プログラム（ＡＴＰ）　　$178.8 Ｍ
先進的な技術開発を促進している。1990 年から＄11.7Ｂの予算を費やしている。特にベンチャーキャピタルも出資しないハイリスクな研究開発にも＄3.9Ｂを費やしている。これは民間企業と折半で出資しており、＄2.0ＢをＡＴＰ、＄1.9Ｂを民間で出資している。

③マニュファクチャリング エクステンション プログラム(ＭＥＰ)　＄105.9 Ｍ
中小の製造業者が世界的な競争力をもつために支援を行っている。経営上の支援と技術的な支援を行っている。3年前の調査によると、このＭＥＰの結果として、25,000 の仕事が創出され、＄2.2Ｂの売上げ増、＄442Mのコスト削減、＄681Mの投資がうまれた。

④ボルドリッジ　ナショナル　クオリティアウォード　　＄5.2 Ｍ
元長官ボルドリッジの名を拝した表彰制度。製品・サービスではなく、総合的で高いクオリティマネジメントに対して表彰を行っている。

（2）暗号とＦＩＰＳについて

ＣＭＶＰ（暗号モジュール認証プログラム）で、ＮＩＳＴの発行する認証の種類は 330、モジュール数は約 500。近年、特に 911 以降、認証の発行数が急激に増加している。ＦＩＰＳ140-02 は、デファクト標準化しているが、そのＩＳＯ化（ISO19790）に向けて以下のスケジュールで、現在作業中。

2002 年 11 月　　ワーキングドラフト作成
2003 年 4 月　　コミッティドラフト作成
2004 年 11 月　　国際標準最終ドラフト作成
2005 年 5 月　　国際標準化

- Ms.アナベルは３人いる Editor のうちのひとりになっている。他の Editor はカナダとフランス。１週間毎に会合を行っている。
- FIPS140-2 の ISO 化の具体的な作業は、用語のＩＳＯ参照用語化、米国独自の基準であるところの EMI/EMC の削除などである。

（3）コメント及び質問

1) ＣＣ化を行った方が、結局相互認証がしやすくなるのではとの問いに対して

a. 140-2 をＣＣ化しないのは、各国の意見として、まずは早急に国際標準化するべきとの意見があったからである（ＣＣ化するのはフォーマット化など手間がかかる作業であり、ＣＣ化を当初から目指すと国際標準化が遅れるおそれがある。）
b. 各国の合意ができているのも、ＩＳＯ化するところまでである。
c. ＣＣ化は各国の戦略の問題もあり、ＣＣＲＡの参加各国の意見もまちまちである。ＣＣ化は新規検討課題であり、現在の ISO の検討課題の枠外である。ＣＣで記述したとしても、ＣＣＲＡでそう簡単には相互認証できないだろう。そもそも、140-2 のＩＳＯ化後の相互認証についても、相互認証は現在まだ議題になっていない。(CC 化を目指しているわけではないので)、ＣＣ化に必要なマンパワーについても、特に検討しているわけはない。

2) ＡＥＳの利用状況の質問に対しては

a. ＡＥＳの利用状況は把握していない。ウェブサイトにＡＥＳのバリデイションのリストがあるのでそれをチェックし、ベンダーに確認して頂きたい。

## 4．Good Harbor Consulting, LLC

日時:　2003年7月29日　　09:30 ～ 10:30
場所：　Hotel Mayflower
出席者: Mr. John Tritak　Ex CIAO(Critical Information Assurance Office)Director

訪問先概要

Mr. Tritakは、クリントン大統領により発令されたPDD63(大統領令６３)により創設されたCIAO（Critical Information Assurance office）のDirectorに就任され、現在は、大統領のCritical Infrastructure Protection Boardの最高責任者を務めたMr. Richard ClarkeとともにGood Harbor Consulting LLCを設立し、Homeland Security に関するコンサルテーションを行っている。米国政府の重要インフラ保護政策に最も精通した方である。官職を離れた立場で、CIAO およびDHS(Department of Homeland Security)の実態についてお話を伺った。

内容

１．911による国家重要インフラ保護における変化

CIAOは、PDD63によりNIPC（National Infrastructure Protection Center）とともに設立された重要インフラ保護を目的とした組織である。CIAOは、商務省に設置され、商務省所管の情報通信インフラを含む8つの重要インフラ保護を統括していた。CIAOが設立された背景には、国家重要インフラの約９０％が民営であり、官民の協力体制が需要インフラ保護に不可欠であるという事情からである。

911以前のCIAOは、サイバーセキュリティを中心とした重要インフラ保護であった。物理的重要インフラ保護対策についてはすでに十分実施されているという理由からであった。

また、情報共有も脆弱性が中心であり、「真の脅威」についての情報共有はされなかった。WTC（World Trade Center）の脅威を事前に伝えたとしても、それは、誇張された脅威としか受け止められなかったからである。

911は重要インフラ保護政策に、２つの大きな変化をもたらした。（１）サイバーセキュリティのみでなく、物理的セキュリティについても国家重要インフラ保護イニシアティブに組み込まなければならなくなった。（２）脆弱性のみならず「真の脅威」に関する情報共有が求められるようになった。

２．Homeland Securityの抱える課題

（１）官民の国家安全保障に関する認識のギャップ

最も大きな課題として、Mr. Tritakは、国家と民間セクターとの認識、言語のギャップを指摘した。

第一のギャップは、サイバーセキュリティおよび物理的セキュリティの区別についてである。911 以後、サイバーおよび物理的セキュリティが重要インフラ保護の枠に組み込まれた。911 が物理的攻撃であったため、サイバーテロの脅威を軽視し、物理的セキュリティへの関心が集中する社会的傾向もある。しかし、テロは、米国の脆弱性を付いて来るのであり、サイバーと物理的手法を混合すること

によりさらに大きな打撃を講じられる可能性もある。サイバーと物理を区別する国家の考え方に限界があり、この点では、むしろビジネスリスクとしてサイバーおよび物理的脅威を統合する考え方をもっている民間企業に政府は学ぶべきかもしれない。

第二のギャップは、経営者の認識の低さである。CEO にとって最大の関心事は戦略リスクであり、サイバーセキュリティ、物理的セキュリティを雑務としてしか捕らえていない。CEO にサイバーおよび物理的セキュリティについて聞くと、IT セキュリティは CIO、物理的セキュリティはセキュリティオフィサーに任せているという返事が返ってくる。IT サービスプロバイダーは別として、いわゆる IT エンドユーザーの企業においては、このような返答が最も典型的なものである。情報共有においても重要インフラ別に ISAC（Information Sharing and Analysis Center）が存在するが、Fortune 500 級の企業ですら年会費 7000 ドルの支払いを躊躇する向きがある。

DHS は、今後、民間企業との連携を実現するために以下の３つを実行する必要がある。

（１） 政府において、サイバーおよび物理的セキュリティについての考え方を見直し、明確な説明を行う。

（２） 民間企業に対して Homeland Security がどこまでのセキュリティ対策を要求していくのかを明確にする。

（３） 民営企業に対して Homeland Security に関する国家政策がどこまでの強制力をもつのかを明確にする。

## ３．DHS 組織

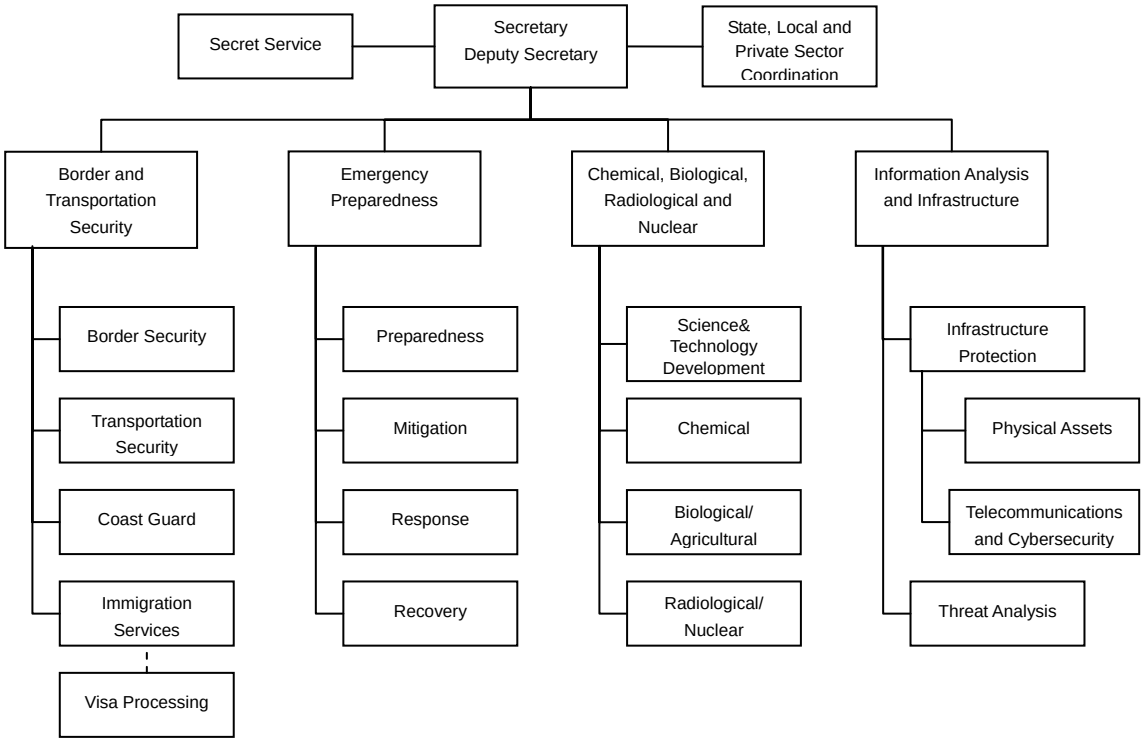
2002 年 6 月、ブッシュ大統領は、DHS(Department of Homeland Security)を創設する考えを発表した。1940 年以来最も大掛かりな省庁再編である。その目的は３つである。（１）米国におけるテロ攻撃を防ぐ。（２）テロに対する米国の脆弱性を軽減する。（３）テロ攻撃が発生した場合に、その復旧を支援する。

DHS は、４つの部門により構成される。（１）Border and Transportation Security ( 国境および運輸におけるセキュリティ)（２）Emergency Preparedness（危機管理） （３）Chemical, Biological, Radiological and Nuclear（化学、バイオ、放射能、原子兵器対策）（４）Information Analysis and Infrastructure（重要インフラ保護に関する情報収集および分析）また、Secret Service （シークレットサービス)、Coast Guard (沿岸警備隊)も DHS に統合された。

100 を超える政府機関に影響を与え、22 の政府機関を統合する DHS は、2002 年１月に Tom Ridge を長官に向かえ動き始めた。3 月に、180,000 人のスタッフを抱えた DHS はスタートしたが、全組織の具体的な活動については、既存の省庁とのコーディネーションも含めて、現在も詳細のつめが進められている。このような現状を説明する上で、Mr.Tritak は２つの事例を挙げた。NIPC は、DHS に移行したが、人材は FBI に残ったため、NIPC は、新たに有能な人材を採用しなければならいのが現状である。National Security Agency（国家安全保障委員会）は、国内についても関与していくのかを明確にするために、これまでの組織のミッション

の修正も必要となるであろう。

DHS の組織図




４．DHS における IAIP 【(Information Analysis and Infrastructure Protection) 重要インフラ保護に関する情報収集および分析】

DHS の創設に伴い、５つの省庁におかれていた重要インフラ保護に関する情報収集および分析機能が統合された。(１) CIAO (Critical Infrastructures Assurance Office) 商務省、(２) FedCIRC (Federal Computer Incident Response Center) 連邦調達庁、(３) National Communications Systems 国防省、(４) NIPC (National Infrastructure Protection Center) FBI、(５) Energy Security and Assurance Program エネルギー省。

IAIP の活動は、The National Strategy for Homeland Security, The National Strategy for the Physical Protection of Critical Infrastructures and Key assets, The National Strategy to Secure Cyberspace の 3 つの国家戦略に基づき進められる。

サイバー脅威に関しては、IAIP に NCSD(National Cyber Security Division)が 6 月設立された。２４ｘ７体制（３６５日 24 時間体制）で、脆弱性、脅威の情報収集および分析、警告、情報共有、インシデント対応、国家レベルでの復旧対応を行うことになった。NCSD により、政府の民間企業および他の組織との連携が強化されることになる。

## 5．Homeland Security Council, White House

日時:　2003年7月29日　　15:00 ～ 16:00
場所：　Old Exec Building
出席者: Mr. Paul Kurtz
Special Assistant to the President and Senior Director for Critical Infrastructure Protection
Homeland Security Council
The White House

Ms. Cheryl D. Peace
Director for Cyberspace Security
Homeland Security Council
The White House

会談要旨：

（1）Kurts氏自身及びOffice of Critical Infrastructure Protectionの役割について

９１１という重要な事件を経験した過去二年間において、私のホワイトハウスでの役割も進化してきました。私は現在、Homeland Security Council の下部組織であるOffice of Critical Infrastructure ProtectionのSenior Directorであり、又、Special assistant to Presidentを兼任しています。ホワイトハウスのHomeland Security Council は、数ヶ月前に、下院が Department of Homeland Securityを設立したのと同時に設立されました。

Homeland Security Council における我々の役割は国土安全関連の問題に関して大統領に助言することです。我々は、Dr. Rice が統括する National Security Councilと緊密に協力しています。Homeland Security Councilを統括するのは、二ヶ月前に就任した退役将軍 John Gordonです。Homeland Security Councilには五つの理事会があり、その内の一つである Critical Infrastructure Protectionは、物理的セキュリティとサイバーセキュリティの双方を一元的に取り扱う組織で、これを私が担当しています。

ここでの我々の担当範囲は、原子力発電所、水利システム、ダム、電力網、銀行と金融、都市の大量輸送等の交通システム、エネルギー関連問題、我々が911システムと呼ぶエマージェンシー対応システム､からサイバーの全領域に渉ります。ホワイトハウスにあって我々は運用を事とする組織ではありません；我々は政策担当者の集まりであり、大統領に対して政策上の助言を行うものです。合衆国の膨大なセキュリティインフラストラクチャのセキュリティの運用面は、原則とし

て Department of Homeland Security 及び他の適切な機関の責任です。さらに言えば、Department of Homeland Security は地方政府や民間を協力し我が国の基幹インフラストラクチャの重要課題を特定し優先度を定めることを責務としています。これは以下のような複数の理由で非常に困難な責務であることはお解りでしょう。第一に、多くの基幹インフラストラクチャは民間に帰属すること。第二に、物理的、仮想的を問わず、これらの基幹インフラストラクチャ間の相互依存関係を理解することが困難であること。第三に、ご承知のように、我々のリソースに限りがあるということ。従って、インフラストラクチャのセキュリティに関する現実の意志決定は、ビジネスが最も重要な資産に関する決定を下すのと同様なやり方で下されるのです。我々は民間及、州、地方自治体と協力し、何が最も重要な資産であるかについて、決定を行います。これは必ずしも恣意的な決定ではありません。(しかし) 多くの場合、この決定が恣意的であるように感じられてしまい、この問題を取り扱う際にある種の緊張を生じるということがあります。リスク管理というのは政府、民間、州、自治体等全てが関与してこれを行うものである、というのが基本的な考え方です。

(2) National Cyber Security Division について

我々が現在緊急に立ち上げようとしている合衆国のサイバーセキュリティに注力する組織について説明しましょう。この組織は二ヶ月前に公表された National Cyber Security Division, NCSD で、Department of Homeland Security 内に設置されます。

NCSD は米国政府内でサイバーセキュリティ関連の問題を取り扱う中心的な組織になります。この組織の活動範囲は主要なサイバーシステムの特定、これらのサイバーシステムの問題の軽減ないしは解消、教育と啓蒙、我々のシステムをよりセキュアにするための様々なテクノロジの発見と開発にまで渉ります。NCSD は米国政府内に既に存在するサイバーセキュリティ担当の多くの組織体を置換するものではありません。その目的は、カーネギーメロンの CERT のような、他の組織の能力の活用を計る拠点となることです。

(3) 政府の責任範囲について

何時の時代も変わらぬ政府の責任範囲というものがこの分野にも存在しています。例をあげればソフトメーカーがソフトウェアの問題に対処するパッチをあてることを推奨する、という場合があります。政府はセキュリティ問題に関する助言をすることはできますが、究極的にはシステムの所有者、管理者自身が、自らのシ

ステムにパッチをあてる責任を持っているのです。この事実は、改めて民間、州、自治体との緊密な協力の重要性を強調するものと思います。

---

（４）質疑応答

４－１．組織間の障壁について

米国政府は、民間、地方政府と協力していますが、これらの組織間に障壁というものが存在することは事実です。その原因は、双方にあるというのが正しいと思います。１９９７年以来、この課題に取り組んでいますが、当初、「国家安全のためにサーバーセキュリティに民間も取り組むべきだ」といったアプローチを試み、これは上手く行きませんでした。そこで、手法を変更し、政府も、民間も、各々のシステムを、自らのためにセキュアにするよう努めるべきである。という語り口に変えました。過去数年において、民間のセキュリティへの取り組みが進展したことは興味深い事実です。サイバーセキュリティが自社の売上、事業、消費者の信頼、投資家の評価に大きな影響があることが理解され、重視されるようになったのです。同様のことがハードウェア、ソフトウェアの供給者にも起きており、製品がセキュアであることが販売に直結すると認識されるようになっています。

４－２．情報共有について

情報共有については、業界毎に固有の情報共有組織を創ることを推奨しています。しかし、障壁がなくなったということではなく、協力して対処せねばならない問題が存在しています。

Department of Homeland Security と Homeland Security Council の設立に関わった Homeland Security 議案の中に情報共有を支援する条項が存在しています。これは同議案の中にある Critical Infrastructure Information 議案というものです。多少、複雑な嫌いはありますが、説明しますと：この議案は、「民間が自主的に脆弱性およびその他の問題について、この情報が安全な方法で扱われる（ただし、秘密扱いされる、という事ではなく）という保証の元に自主的に情報提供することを可能にする」のです。ですから、Department of Homeland Security が、特定のシステムの脆弱性を認識した場合、必要な無害化を行った上で、１）問題の明示、２）パッチ等の解決方法を得られる場所の指示に関する助言を公表できることになっています。我々は米国政府がこの種の情報をどう扱うか、また、Department of Homeland Security が、これに関して何を行うかを明確にする条例の提案を終えており、これらの機能はこの秋には発効すると予期しています。

４－３．CERT CC 及び FIRST との関係

米国政府はカーネギーメロンの CERT に脆弱性の高度に技術的な分析において依存しています。National Cyber Security Division が設立されたために、我々は CERT と NCSD に緊密な協力関係を築く過程にあります。NCSD 内部に全てのリソースがあるのではありません。ワシントンの CERT 等のリソース或いは NIST を活用し、また、民間とも緊密な協力関係を創りその中心となるのが NCSD の役割です。ＦＩＲＳＴは米国の CERT、JPCERT、他の世界の CERT が協力関係を築く基盤として重要です。国際間でサイバー問題を協力的に解決するための枠組みがどう在るべきか、日本がこの問題についてどのような考えをもっているかに関心があります。

４－４．National Security Council 対 Homeland Security Council

National Security Council と Homeland Security Council はどちらも政策調整機関であり、大統領のスタッフとして政策を米国政府全体を通じて調整しているという点が共通しています。Homeland Security Council が国内のセキュリティ、National Security Council がより国際的、対外関係的な問題に重点を置いているという相違はあります。

両者の活動範囲が重なっているのは事実です。結論から言えば、ＩＴシステムを純粋に国内のものと国際的なものにわけることは困難です。国際的なシステムの問題が国内経済に影響することも、その逆のケースも存在します。したがって、National と Homeland の間に人工的な境界線を引くことは不可能です。

４－５．日本について

サイバーセキュリティに関する日本と米国の対話の過去の積み重ねの結果､既に、具体的な協力の領域を検討できる段階に至っていると思います。ひとつは、サイバーセキュリティに関する両国間の協力を担当する中心的な存在を特定すること、これによって、両国政府内で、誰が何をやっているのかがお互いに明確にわかることが狙いです。関連する政府組織、民間での中心的な存在も明確にしたい。サイバー問題に関する情報共有のための国際的な枠組みを開発することを考えねばならないでしょう。情報を交換する経路と手順についても日本との協力が必要ですし期待されます。日本を含む世界のパートナーと米国が共有すべきは何でしょう？又、日本と米国の二国間においても、両国が共に依存しているシステムを特定することは必要です。例えば銀行と金融が挙げられるでしょう。私見では、最も重要なのは両国において「誰が何をしているのか」を理解していること､即ち、

お互いが「誰に話しをすればいいのか」を判っていることです。

４－６　米独　対　米日

多くのイニシアチブが存在することは認識しています。政府も民間も、一度、これらのイニシアチブを、それぞれの目的も含めて一枚の紙に書いてみることが必要と思います。これらを止めようというのではなく、認識するために。例えば商務省は欧州との活発な関係を持っていますし、国務省にも Department of Homeland Security にも個々にイニシアチブがある。これらの活動に調和をもたらすことが必要です。

４－７．日本との共同研究の可能性について。

ドイツ政府と二ヶ月前に最初の試みを始めたところです。日本政府とのこの件に関する対話は、他の国々とのものより遙かに進んでおり、答えはイエスであると申し上げます

## 6．FBI　InfraGuard

日時:　2003年7月30日　　09:30 ～ 11:30
場所：　FBI本部
出席者: Mr. James Burrell
Chief, Cyber Division, International Investigative Support Unit

Mr. Brett Hovington
Supervisory Special Agent, Cyber Division

Ms. Gail Seavey
Section Chief, Cyber Division

Ms. Joy Faith
Liaison Analyst, Protocol Affairs Office,
International Operation Section

訪問先概要：

■　日米両国において、重要インフラの大半が民営であることから、経済社会の基盤となる重要インフラをサイバーテロ等の破壊活動から防護するためには、官民が連携して対処していくことが重要である。InfraGuardは、FBIの現場サイドの要請に基づき、民間セクター、学界、公共部門の広範な関与を求めて、地方から発展してきたところが特異であり、今回の訪問ではその運営実態についてお話を伺った。

■　InfraGuard は、1996年にFBIクリーブランド支局において試験運用プロジェクトとして発足した。現在、FBIの56支局に80支部が設置されており、民間セクター、学界、FBI や関係省庁、州及び地方の法執行機関等の代表者が参加している。

■　InfraGuard プログラムは、NIPC（National Infrastructure Protection Center：国家インフラ防護センター、）の活動を補完するために不可欠なものとなっており、重要インフラに対する脅威や脆弱性に関する官民の情報交換、情報共有のための組織として機能している。また、脅威等に関する分析結果を民間部門に伝達するための場でもあり、アラート・ネットワークの提供及びメンバーに対する教育・訓練なども行われている。NIPCはDHS(Department of Homeland Security：国土安全保障省)に統合されたが、InfraGuard は依然としてFBIが所管している。

内容：

(1) Cyber Division について　(Mr. James Burrell)

FBIのCyber Divisionは、分散していた関係部署を統合して昨年創設された。その役割は、サイバー犯罪捜査に当たって、装備と人員を有効に活用し、サイバー犯罪及び犯罪者に対処することである。FBIは、サイバー犯罪捜査における国際的な

取り組みの重要性やInfraGuardプログラムの重要性を認識している。また、FBIは、国際捜査の実施に当たって、外国警察への捜査共助要請及び法執行に当たっての産業界との連携に関して、政府と協調して仕事を行っている。

東京には渉外担当のMoynihan氏が駐在しており、警察庁や関係省庁と協力を行っている。本年５月には、NIPCの機構やサイバー犯罪についての新しい取り組みを調査するため、日本から訪問者を迎えた。

NIPCは、司法省とFBIにより創設され、FBIの管轄下にあったが、この度、DHSに統合された。NIPCは次の３つの使命を果たしてきたが、警告についてはDHSに移管された。

- サイバー犯罪捜査（FBIの捜査指揮による。）
- InfraGuard（政府と民間メンバー間での情報交換の推進等）
- 脅威や脆弱性についての警告

サイバー犯罪捜査官を確保するために、技術者やコンピュータ・サイエンス学科の卒業生をリクルートし、ハイテク犯罪捜査官として訓練している。これには相当な経費を費やしているが、この人員でも十分ではないため、ハイテク犯罪捜査の経験者を捜査官として確保している。この捜査官の場合は、4～5年の技術的経験を有する者に匹敵する能力がある。

ハイテク犯罪捜査官には、最新の技術知識を修得させるための訓練プログラムやOJTにより、継続的に訓練を実施している。育てた人材の中には民間企業に引き抜かれる者もいるが、大局的には、民間において、このような分野で貢献するのであれば問題はない。FBIは、ハッカーを職員として採用していないが、捜査や裁判において、協力を依頼することはある。ハッカーを採用している国も見受けられるが、本当に重要な情報を見せるかどうかなど微妙な問題も多い。

(2) InfraGuardについて　(Mr. Brett Hovington)

InfraGuardは、FBIの56の支局に80の支部が設置されている。民間のメンバーは、9,000人で、電子産業、ガス及び石油、金融など様々な産業界から個人として参加している。

InfraGuardは、重要インフラを運営している民間部門から情報を入手できるため、大変有益である。重要インフラ対策では民間の協力が極めて重要であり、FBIは企業トップとの対話を進めている。企業トップは、重要インフラ対策を経済面から考えがちであるが、国家安全保障の観点から捉えることが重要である。

InfraGuardの目的の一つに、メンバー、FBI支局及びNIPCとの間において、脅威や脆弱性に関する情報の共有及び双方向の情報交換が挙げられているが、この目的を達成するためには、相互の信頼関係の構築が課題である。信頼関係に関して言えば、1998年、1999年及び2000年にハードルを超え、現在、相互の信頼関係はできてきている。民間からの情報提供は、年々増加してはいるが、依然として少ないのが実情である。

InfraGuardプログラムを民間主導で進めるため、FBI捜査官の民間セミナー等への出席、民間部門とのフェイス・ツー・フェイスの対話及びシステム上の問題に関して民間部門がFBIに容易に連絡が取れるように、コンタクト・ポイントを設定

するなどの対策をとっている。
重要インフラを防護するためには、車の両輪のように物的防護及びサイバー上の防護の両面が重要である。
NIPC は、DHS に移管され、重要インフラ防護の使命は、DHS に移ったが、FBI 長官は、InfraGuard の重要性を考慮して、FBI の下に残した。
DHS は、22 の省庁から国土安全保障に係わる機関を統合して創設されたが、元の省庁にも、これまで関与していた職員が残っており、各省庁との連携が重要である。このような意味で、FBI は DHS 及び他省庁とも連携している。FBI は、昨年から金融業界とも連携しており、捜査中のものを除いて、金融 ISAC（Information Sharing and Analysis Center：情報共有分析センター）から情報を得ている。
InfraGuard と ISAC の違いであるが、InfraGuard は、官民のパートナーシップに基づく民間主導の草根的な活動であり、参加は無料である。ISAC は産業界の分野別の会員制組織であり、有料で運営されている。
InfraGuard のメンバーシップには、セキュア・メンバーバーシップとノンセキュア・メンバーバーシップがある。企業の情報セキュリティ責任者又は CEO の署名が必要となるセキュア・メンバーには、機密性の高い情報が提供される。

## 7．ISA　(Internet Security Alliance)

日時:　2003 年 7 月 30 日　　12:30 ～ 14:30
場所：　ISA 本部
出席者: Mr. Larry Clinton
Deputy Executive Director Chief of Operation
INTERNET SECURITY ALLIANCE

Ms. Barbara L. Wortmann　Senior Vice President
Policy & Planning Industry Relations
Electronic Industries Alliance

Mr. Brain Kelly
Senior Director, Federal Government Affairs
Comcast Corporation

Ms. Barbara S. Laswell Ph.D.
Technical Manager Practices
Development and Training
Networked Systems Survivability Program
Carnegie Mellon Software Engineering Institute

訪問先概要：

ISA は EIA（エレクトロニック　インダストリーズ　アライアンス）と CERT/CC と連携をもち、会員企業は 2500 社以上である

内容：

（１）ISA 事業内容

Economic Security と National Security は別である。すなわち国は企業を守ってくれない。民間会社同士の関係は健全であるが、民間会社と民間会社の間に国家が介入することは不自然である。情報セキュリティの分野においても、政府指導ではなく民間主導であるべきであり、B to B のビジネス環境を保障するベストプラクティスの必要性を確保することが重要である。ビジネスは民主導であり、政府はそれを保護する役目を果たすのが望ましい。ISA は EIA と CERT/CC が参画することにより、会員企業に対する様々な情報セキュリティ情報ならびにサービスを提供しており、さらにそれをバックアップすべき政府機関との連携を取っている

- CERT/CC からは定期的な情報提供、ナレッジベースへのアクセス、最新の脅威の動向の報告がある。
- Slammer を始めとした最近の脅威に対しても迅速に対応している。Exploit コードが発表される前に対策を公表している場合がある。
- Configuration 管理とパッチ管理は難しい。サービスの一環として、ISA の

メンバーの使用に耐えられる自動パッチ管理ツールの開発を行っている。

- ＩＳＡメンバー企業向けにＡＩＧ（ＩＳＡのスポンサーにもなっている）が、サイバーインシュランス「ネットアドバンテイジ」を提供している。メンバーは無料でＡＩＧのリスク診断（オンライン版とオンサイト版がある）を受けられ、サイバーインシュランスに加入する際には１０％割引（ＮＳＡ会員割引）、更にＮＳＡのベストプラクティスに適合している場合には５％割引（合計１５％割引）が適用される。保険料は１企業あたり、１００千ドル～２５０千ドル（約1,200万円～3,000万円）程度であり、１５％割引の効果は、15千ドル～38千ドル程度となり、メンバー年会費の25千ドルを賄ってしまう。スタート間もない制度であるが、現在、既に６社の加入がある。なお、ＡＩＧ社はサイバーインシュランス分野で７０％のシェアを持ち、世界で5,000社の加入があると聞いている。

（２）ＣＥＲＴ／ＣＣ概要（Barbara S. Laswell）

Software Engineering Instituteは米国合衆国の基金により設立されたＲ＆Ｄセンターであり、国防省が資金提供をし、カーネギーメロン大学が運営している組織である。目的はソフトウェアエンジニアリング分野における、評価された改善手法の導入を支援することである。CERT/CC はその機能の一部である。以下、インシデント、リスク管理等について一般論の説明。

・インシデント報告は1999年以降指数的に増加している
・脆弱性情報も同様
・アタック手法は高度化しているが侵入者の必要知識は低下している
・インシデント対応組織は２００２年現在全世界で合計約１２０組織、米国が約６０組織、ヨーロッパが約５０組織である。
・組織の戦略として、防御・検知・対応・維持／改善を考える必要がある
・CERT/CCのホームページには各種の有効情報があるので参照してほしい
・CERT/CCのミッションは以下：
　－教育
　－トレーニング
　－知識ベース
　－啓発
・教育コースの受講者としてＵＳ産業界３６％、国防省２１％、合衆国官庁１２％、地方公共団体６％、教育機関４％、海外２１％である
・各種出版も行っている
・ガートナー、ＣＩＯ協議会、米空軍等多くの機関と協力関係にある
・ＥＣｏｍ（日本）、ＩＳＳ台湾等へライセンスしている

## 8．CSIS（Center for Strategic & International Studies）

日時:　2003年7月30日　　15:00 ～ 16:00
場所：　CSIS
出席者：Dr. John J. Hamre
　　President & CEO

　　Mr. James A. Lewis
　　Senior Fellow and Director Technology Policy

訪問先概要：

CSIS（国際戦略研究所）は国際政治、内政、軍事などで米国を代表するシンクタンクの一つである。今回は元国防副長官であるHamre氏と会談する機会を得た。

内容：

■　Hamre 氏より「3 年前に情報セキュリティに関する日本からの訪米団を迎えた際は、サイバーセキュリティ自体についてあまり理解をしていないとの印象がありましたが、今回このように政府の委員、学会、民間と多様な立場の方々が訪問されたことはこの3年間で日本の情報セキュリティに対する認識、取り組みが大きく進歩したと驚いております。」とのコメントが出されました。

■　米国では安全保障、サイバーテロを強調する政府とサイバー犯罪に具体的な対応をする民間企業とで認識に齟齬が生まれています。サイバーセキュリティの中でサイバーテロとサイバー犯罪との位置づけを明確にすることにより、各々すべきことがはっきりします。また、サイバーその物がテロの道具にならない場合でも、テロを手助けする手段にはなります。IT依存度が高まる中、重要インフラ企業はもう少しサイバーテロに対する認識を高め、コスト負担を含めた措置を取るべきで、必要であれば政府が予算措置を伴わない規制、指導もするべきです。また、DHS（Department of Homeland Security）の設立は米政府にとって大規模な組織変更であるため､未だサイバーセキュリティの扱いがはっきりしておらず、今後どのような形になるかが一つのポイントとなります。

■　このような中、米国では情報セキュリティについてポジティブな新たな動きが出始めております。企業が収益性のあるセキュリティ商品を開発したり、ソフトウェアについてはセキュリティが確保されていないと商売にならなくなってきました。また、景気が悪い状況から抜け出す情報セキュリティに関わる企業として、分散型の安いルーター産業、オープンソースの分野に期待が持てます。

■　国際間のサイバーセキュリティについては二国間と多国間協議を並行的に進めることが重要です。グローバルな枠組を視野に入れながら、他国との協議に矛盾しないように効果的に進められる二国間協議を行い、最終的にはグローバルな枠組みに入れるべきです。

## 9．SAIC (Science Application International Corporation)

日時:　2003年7月31日　　9:00 ～ 12:00
場所：　SAIC社、
出席者: (SAIC社)
Mr. John .P. Cassiano
Group Senior Vice President,
Enterprise Security Solutions Group

Mr. Thomas J. Lyden
Group Director,
Managed Security Service
E.S.S. Group

Mr. James H. Jones
Assistant Vice President,
Technology
E.S.S. Group

Mr. Nicholas M. Nahas
Director,
Japanese Business Initiatives

(ConocoPhilips社)
Mr. Bobby R.Gillham
Manager,

Global Security

訪問先概要：

SAIC社は１９６９年設立、従業員は約40,000人、年間売上$6.1Bの企業である。（子会社のベルコア分を含む）　本社はサンディエゴである。

主な事業内容は、SI、MSSP、コンサルおよび通信事業（ベルコアが実施）である。その中でも、国土安全保障省（DHS: Department of Home Land Security ）関連のサービスをはじめとした政府関連セキュリティサービスの比重が高く、全社売上の４３％を占める。SI会社としては全米４位だが、政府関連の受注では１位である。

CC（Common Criteria）の評価機関でもあり、１０~１２名程度の評価者を有し、EAL1からEAL4までの評価を行っている。これまでに、全米で７０例の評価件数の内、約半数をSAICが評価した。

MSS（Managed Security Service)としてSOCを３サイト保有しており、それ以外にも顧客サイトでのSOC運用を行っている。DRP(BCP)やIRTなどのサービスも行っており、分析ではCMUと連携して政府向けのサービスを行っている。

ISACについては、FS（金融)、Energy 等へサービスを提供している。以前は子会社のGlobal Integrity社がサービスを提供していたが、最近SAICがサービスを引き取り、自らサービスを提供している。なお、SAICではFS-ISACとEnergy-ISACを4名のスタッフが常駐し運用している。

米国政府がセキュリティに関するセクションを DHS に統合したのに対応し、SAICもセキュリティに関するセクションを統合し、One Stop Shopping を目指している。

内容：

（１）ISAC、FS-ISAC

米国重要インフラ保護に関する 1998 年の大統領令 PDP63 を基に、国家インフラ防護センター（NIPC: National Infrastructure Protection Center)、重要インフラ保証局（CIAO: Critical Infrastructure Assurance Office）と共に、ISAC(:Information Sharing and Analysis Center)、が設立された。

ISAC は業界の会員組織であり、会費で運営され、会員相互の情報交換を目的としている。ISAC の主な機能は、情報収集、セキュア DB、情報分析、情報の匿名化、配布等である。これら機能を用いて、ISAC は、脅威、脆弱性、インシデント、解決法などの情報を提供している。

ISAC の情報チャネルとしては、会員、パブリックソース、商用ソース、政府等があり、これらのチャネルからの情報を、分析・判断し、会員に提供する。提供するサービスの種類としては、アラート、サポート、会員やベンダーとの共有・協力、質問への応答、報告等がある。

現在の課題は、業界の参加者が予想より少なく運営資金が少ないこと、ならびに会員からの情報提供が少なく提供される情報は ISAC からの一方通行となっていることである。

特に９．１１以降は、政府から業界への情報の提供手段としても利用されつつある。政府はサーバーテロ対策として、特定の業界向けに非公開情報を提供することを考えており、このために ISAC を利用したいようである。またこれに対応し、業界側も政府のサポートや費用支援を期待しており、実施について検討中である（Energy ISAC の費用はすでに補助を受けている)。しかし、政府の補助を受けた場合、法律で情報を開示する義務が生じることから、整理が必要である。また、ISAC のあり方について、会員のなかにも様々な考えがあることから、これについても調整が必要になると考える。

（２）Energy ISAC

Energy ISAC は Banking & Financial ISAC を参考に 2001 年 11 月に設立された。石油・ガスを含む多くの会員を集めることを目的として、サイバーセキュリティと物理的セキュリティの両方をスコープにしている。

Energy ISAC の活動は、基本的にスピード重視の push 型を目指している。会員企業 11 社から構成される理事会で戦略を議論し、実際の運用は SAIC 社が行っている。Energy ISAC では、会員からの情報提供を当初から期待せずに、一方的に ISAC 側から情報を流している。

当初の会員は大手 35 社で、一社あたり$7,500 の年会費で運営費用を賄っていた。会費＄7,500 の内、$5.000 が運用費用として SAIC 社、残りの$2,500 が ISAC のその他の活動費用であった（FS-ISAC も同じ料金体系である)。しかし、有償のため中小規模の企業の参加がなかった。そこで会員を出来るだけ増やしたいという政府方針により、エネルギー省が年間$600,000 を負担して、中小規模の企業の会費を無料とした。これら無料会員向けに Energy ISAC は基本サービスを提供している。現在は企業だけでなく、業界団体も参加している。

サービス内容は、サイバーセキュリティや物理セキュリティの脅威・脆弱性に関する情報提供で、短時間に分析して提供している。基本サービスでは、2 名／会員企業まで情報にアクセスでき、利用者を追加する場合は、$150／利用者の追加料金が必要である。情報受信のメディアとしては、WEB の他、電子メール、ページャ、FAX、携帯電話等が利用できる。

今後は物理セキュリティに関するインシデント情報の扱いや、ISAC 間での共有、政府との共有、さらに機密性の高い情報へのアクセス等を考えている。

（３）ISAC Council

ISAC Council は ISAC 相互のシナジー効果、効率化、コストセーブを目的として 2003 年に設立された。当初の参加は、８業種分野の 8 会員だったが、現在は 13 会員である。各 ISAC やサポートベンダが参加しているが、投票権は各 ISAC が一

票ずつ持つ。民間主体であるが、DHS の参加も検討している。
主な活動は、ISAC 全体のポリシーフレームワーク策定で、2003 年 6 月 24 日には、DHS および White House も参加した会議を開催した。
各 ISAC が提供している情報の 70%~80%は、ISAC 間で共有可能であり、残りが各 ISAC に固有な情報と考えられている。そこで、ポータルサイトを共有化する等で効率化して、各 ISAC はその固有な分野での活動に専念すべきと考えて推進している。

## 10．DISA (Defense Information Systems Agency)

日時:　2003年7月31日　　13:30 ～ 16:00
場所：　Maiflower Hotel
出席者：Mr. Stephen T. Goya
General Manager
Foreign Military Sales

Mr. Bill Keeky
IA Program Manager
Office of the Chief Information Assurance Executive

Mr. Timothy D. Bloechl
Director
International Information Assurance Program
Department of Defense, Directorate of Information Assurance

Mr. Ron Ritchey
Senior Technical Analyst
Information Assurance Technology Analysis Center

Mr. Ajay N. Gupta
Senior Associates
Booz Allen Hamilton

訪問先概要ならびに内容
（1）JNSA視察団向けDISAご紹介(Steve Goya)

■　国防情報システム庁（DISA）は平時・有事にかかわらず、指揮・統制・コミュニケーション・情報システム（C3I システム）の計画・開発・展開・運用・支援を任務とする、戦闘を支援する庁である。これらの業務は大統領、副大統領、国防長官(the Secretary of Defense)、統合参謀本部(the Joint Chiefs of Staff)、戦闘司令官（the Combat Commanders)、及びその他の国防総省の組織のニーズを満たすものである。

■　DISAにはGIG（Global Information Grid）という軍事・安全保障のために米国国防総省が運用しているネットワークがある。GIG は基盤、通信、コンピューティング、アプリケーション、戦闘武器の５つの要素から成り立っている。GIGへの脅威には従来型の物理的な脅威とそうでないウイルスのような脅威とがある。

■　統合ネットワークセキュリティチームはグローバルネットワーク運用安全センター（GNOSC)、コンピュータ緊急対応センター（CERT)、コンピュータ・ネットワーク防衛統合任務部隊（JTF-CNO)、全米調整センター（NCC）から成る。GNOSCではDODのネットワーク管理（GIG管理）を行っている。CERTではネットワーク

問題の分析や対応を行っている。JTF-CNO では実際の作戦を行っている。JTF-CNO にはコンピュータ・ネットワーク防衛（CND: Computer Network Defense）という任務がある。NCC では通信業界における官民情報共有等の連携を行っている。

■ DISA の職員は約 8000 人である。

（2）ISA 情報保証 概要（Bill Keely）

■ DISA における情報保証の概要は以下の４点である。

- 国防総省横断的なセキュリティ及び関連する相互運用性
- 戦闘員の指揮、構成、部隊配備の支援
- 防衛、攻撃検知／分析システムの構築及び運用、セキュリティ基盤の支援
- 情報保証業務

■ DISA におけるグローバルネットワーク運用安全センター（GNOSC）の業務は、グローバルな状況の掌握、GIG ネットワーク運用管理、侵入検知である。

■ DOD CERT はグローバルな状況掌握にフォーカスを当てており、情報検知、調査、対応を行っている。世界的な規模で４箇所に分かれてウイルス攻撃やその他の悪性の攻撃をコンピュータでモニタしている。また、国防省関係で 500 万程度のコンピュータがあり、それらに対してウイルス対策支援を行なっている。

■ DISA には次の業務がある。アプリケーションセキュリティ、CERT の運用、侵入検知、オフサイトセキュリティ、脆弱性管理、プログラム管理支援、COCOM 支援、教育・訓練、識別管理。例えば脆弱性管理については、脆弱性の特定・対応・Gold Disk（パッチ等の入った CD-ROM）の配布・ペネトレーションテストによる確認の４つのステップがある。これら各ステップの状況はデータベースで管理しており、月次報告の他、随時参照可能となっている。現時点における DOD の公開鍵基盤として、アクセスカードを 250 万枚程度発行している。これはユーザの身分証明書にもなり、将来的にはより多くのアプリケーションをのせたいと考えている。

（3）米国国防総省 情報保証 サイバーセキュリティのポリシーと実践（Tim Bloechl）

■ 情報保証とは、可用性、完全性、認証、機密性、否認防止により情報及び情報システムを守る活動のことである。「情報保証」は「情報セキュリティ」よりも大きな概念である。情報保証戦略の目標は以下の５点である。

✧ 情報保護
✧ システム及びネットワークの保護
✧ 情報保証状況の把握と指揮命令系統の確立
✧ 情報保証の変化への対応
✧ 人材育成

■ 国防総省の情報保証戦略は人材、運用、技術の全ての面からのアプ

ローチが必要である

- CERT/CC に報告された主要な事故件数だけでも 10 万件程度の攻撃が発生している。また、悪意をもったコードは増加の一途をたどっている。2002 年に検出されたのは 46,000 件程度である。国防省で発生する事故の 97%は職員が適切なパッチを当てなかったことから生じている。
- 演習は様々なタイプをミックスして行なっている。机上の演習やシニアリーダーが率いる演習等がある。サイバー戦争のコミュニケーション演習、ネットワーク侵入や攻守チームに分けて実際に攻撃シミュレーションを行う。いろいろなチームに分けてどこが一番優れているかをテストする。状況を設定し、２～３日の間にどのような反応をするかを演習している。国際演習も行なっている。日本も１～２年のうちに同様の演習が行なえることを期待している。

（４）悪意のあるコードの最新技術（Ron Ritchey）

悪意のこもったソフトウェアにはメリッサ、コードレッド、ニムダ、ハイブリス等がある。ハイブリスはメールの送受信によって増殖活動を行うのみであり、単独では破壊活動は行わない。しかし、プラグインによって様々な被害を発生させることが可能である。プラグインは何者かがニュースグループを通じて流通させており、これを自動的にダウンロードするようにできている。世界中のサーバーがバケツリレー式に記事を運搬するニュースグループの特性のため、特定の Web サイトからプラグインを取得する他のワームに比べ､拡散を防ぐのが困難である。このハイブリスワームはマスコミではあまり取り上げられていないが、他のものより脅威があると捉えている。これはシステムの中での活動が見えず、一見ダメージがないように見える。ハードディスクをチェックする等、時々いろいろな動作をするが、何が起こるかはわからない。

マイクロソフトは「SQL サーバー2000 デスクトップ・エンジン」(MSDE2000）を無料で提供している｡プログラマーが MSDE2000 を使用するときセキュリティ面への影響を正しく認識しないとマシンにパッチを当てる必要があることがわからない。このため、攻撃に対して無防備な状態に置かれてしまう。スラマーは SQL Server の脆弱性を狙ったワームである。これは、セキュリティのメーリングリストに出てきたワームであり、MSDE2000 の脆弱性が証明されたので、ウイルスを作ろうという意欲が高まる可能性がある。

わずか数人でも高度な知識を持っている人間がいると、悪性コードを増殖させるツールを作る。そうすると、その他大勢のさほど高度な知識を持たない人間がツールを使って悪性コードを作ることができる。

検知・防止方式としては依然として署名方式が多い。署名方式は既知のウイルスについては、ほぼ 100%検出できるが、ウイルスの発見と署名の開発タイミングには時間的なギャップがあることと、未知のウイルスは検出できないという脆弱性がある。Sandboxing は怪しいコードを発見すると一時的に隔離し、バーチャル環境の中でそのコードがどのような行動をとるか観察するという技術である。

## 11．Symantec SOC（Security Operation Center）

日時:　2003年8月1日　　9:30 ～ 12:00
場所：　Symantec, Alexandria
出席者：Mr. Grant Geyer
　　Senior Director
　　Operations
　　Managed Security Services

訪問先概要：

Symantec SOCは1998年に国防総省のセキュリティの専門家により設立された旧Riptech社のSOCをSymantec社が買収に伴い継承したものであり、政府機関を始め多くの顧客を有する世界で有数のセキュリティオペレーションセンターである

内容：

（１） MSS（Managed Operation Center）の必要性

- 2001年の統計によれば、その年に何らかのセキュリティの被害を受けた組織のうち、61%の顧客が侵入検知装置を、95%の顧客がファイアウォールを導入していた。ウイルス、ワームが多様な攻撃手法を取り始めたのと同時に、管理者が十分な設定・管理を行っていないこと、さらに様々なセキュリティ機器からはきだされる膨大なログの意味を読み取れないこと、さらにアナリストの不足などが原因と考えられる
- SOCにおいては、その膨大なログを相関をとりながら解析し、限定した対処可能な数のインシデントに絞り込む。実例をあげれば、ある会社で発生したログの総数が950万件あった時、SOCではそれを一桁の単位まで絞り込んでいる

（２） SOCにおいては、顧客データの秘匿性を守るため、物理的なセキュリティを十分確保すると同時に、人的な面においても、軍関係者など信頼のおけるアナリストを採用し、採用時には十分な背景調査を行っている。

## 12．Telecom ISAC

日時:　2003年8月1日　　13:30 ～ 16:30
場所：　Mayflower Hotel
出席者：
政府関連出席者：

Mr. Don Smith,
Acting Manager, NCC, NCS

Lt Col Frances Wentworth (USAF)
Telecommunication ISAC Operations

Mr. Henry Daniel
Information Technology Specialist(INFOSEC)

CDR Ray Emmerson (USN), NCC Staff Member

業界関連出席者:

Mr. Shawn Cochran
Director
National Security and Strategic Policy
Bellsouth Corporation

Mr. Thomas F. Snee,
Director
Government Services
Qwest

Ms. Rosemary Leffler
Director
NSEP
SBC Communications Inc.

訪問先概要

今回の打合せの出席者は、空軍中佐および海軍中佐を含む政府系４名と民間３名であった。Telecom ISACは政府が運営しているため、会費は不要だが参加企業および参加団体は代表をTelecom ISACに参画（出向）させる必要がある。民間からは現在３０企業、3協会が参画している。オペレーションセンタが24時間のサービスを行っている。政府系のセキュリティ組織や参加会員のIRTやSOC連携およびメールや電話等の問合せに対する回答が主な活動内容である。

内容

（1）ミッションおよびゴールについて

Telecom ISACのミッションは、脆弱性、脅威、侵入、異常状態に関する情報を複数のソースから得て、分析して、その結果により警告あるいは通信インフラに与える影響を軽減することである。
ゴールは次の項目を達成することである。

・公正公平な情報ブローカであること。
・会員である政府・民間の協力を推進する。

・リエゾンパートナーあるいは外部ソースとの連携協力を育てること
・全てのソースを見張り、情報を纏め、分析し、フィルターして、他では出来ない情報を供給：価値を付加すること。
・情報の持ち主の権利、情報そのものを確実に保護すること。

（2）組織

NCS(National Communication System)は 1962 年以来、通信業界と関連政府局との協力を推進してきた。2003 年 3 月に DHS(Department of Homeland Security)の一部となり、現在２３の連邦の省や局を束ねる組織である。NCS の管理下に置かれた NCC(National Coordinating Center for Telecommunications)は、1984 年に設立され官民協力のための組織として活動している。本 telecom ISAC の運営も NCC において行われている。正式には、NCC Telecom ISAC は 2000 年に設立され、活動を開始した。

（3）メンバーシップ

NCC に参加している産業界会員として、通信業者、ネットワークサービス、それらを対象としてベンダーが参加している。また関連協会も参加。その他に政府系として NCC 参加の省、局およびセキュリティ関連組織が参加。
産業界からの参加は当初 17 社、現在は 30 社、3 協会
（Americom, AT&T, AT&T Wireless, Avici, Bell South, Boeing, Cable & Wireless, Cincinnati Bell, Cingular Wireless, Cisco Systems, Computer Sciences Corporation, Cellular Telecommunications & Internet Association*, EDS, Intrado, Level 3 communications, Lockheed Martin, Lucent Technologies, MCI, McLeodUSA, Motorola, Nextel, Nortel Networks, Northrop Grumman, PhotonEX, Qwest Communications, Raytheon, Science Applications International Corporation, SBC Communications, Sprint, Telecommunications Industry Association*, United States Telecom Association*, VeriSign, Verizon.: アルファベット順、*印は協会）

Telecom ISAC では、参加企業は代表を手弁当で出向させて活動するが、施設他の運用に関する費用はすべて政府から支出されて、会員会費は存在しない。他の ISAC では Energy ISAC を除き産業界を主体として、会員の会費で活動に関する費用を賄っている。

（4）活動内容

Telecom ISAC の施設は DoD の IT サポートを行っている DISA(Defense Information Systems Agency)に位置する。そこに会員企業、会員組織からの代表者が集まり活動している。各代表の給与は会員企業が支払っているが、それ以外の運用費用・活動費用はすべて政府が支出している。予算額は、質疑応答からは回答が得られず、不明である。週一回の定例会議が開催される。
2000 年 11 月に 24 時間の運用センターのサービスが開始された。21 名のエンジニアで構成され、最低 2 名以上が常駐している。政府や会員企業の SOC（セキュリティオペレーションセンター）、IRT 等と連携して活動している。細かい脆弱性情報の提供や警告情報の提供を行っているのではなく、会員企業の IRT や CMU（カーネギーメロン大）/CERT 等の関連組織との連携や会員からの問合せ応答等を行っている。サービスに関する会員との特別な契約は存在しない。
各会員からの情報の取り扱いは信頼関係（Trust）に基づき、非常に慎重に行っている。逆に、会員からの情報を Telecom ISAC から他会員に出すときには匿名化処理(sanitization)を施す。活動内容について、独占禁止法の観点からの配慮をしている。

本活動においては、CMU/CERT や他の ISAC との連携を行っており、World Wide ISAC や英国の Telecom ISAC との連携も進めている。

（5）まとめ他

基本的に政府はサイバーテロ、サイバーウォーを想定して活動を進めている。民間は基本的に利益確保のためにセキュリティが必要という認識に立っている。重要インフラ防護では、民間が自分の利益追求では活動できない活動には政府主体の活動あるいは政府支援がある。

ISAC 全体では既に 13 の ISAC が立ち上がっており、民間主体が原則だが、Telecom ISAC はその国としての重要性から、政府が運営している（国土安全省管轄）。エネルギーISAC も国としての重要性から、費用負担をエネルギー省が行っている（運用は SAIC 社)。すべての ISAC を横串にさした ISAC カウンシルが 2003 年に設立されて、政府に支援要請の動きもあるようである

## 13. 視察団訪問日程

---

- **July28** 09:30-12:00 @Hoover Bldg
  - Department of Commerce
- **July 28** 14:00-17:00 @NIST in Gaithersburg
  - NIST

---

- **July 29** 09:00-10:30 @Hotel Mayflower
  - Good Harbour Consulting, LLC
- **July 29** 15:00-16:00 @Old Exec Bldg.
  - Homeland Security Council, White House

---

- **July 30** 09:30-11:30@FBI Head Quarters
  - InfraGuard (FBI)
- **July 30** 13:00-14:30 @ISA
  - ISA (FBI)
- **July 30** 15:00-16:00 @CSIS
  - CSIS(Center for Strategic and Internatonal Studies)

---

- **July 31** 09:30-12:00@SAIC
  - Finance-ISAC
  - Energy-ISAC
- **July 31** 13:30-15:30 @Hotel Mayflower
  - DISA
- **July 31** 16:00-20:00 @Hotel Mayflower
  - Wrap Up

---

- **August 01** 09:30-12:00 @Symantec
  - SOC office tour and meeting on Incident response
- **August 01** 14:00-17:00 @Hotel Mayflower
  - Telecom-ISAC

---

## 14. 視察団参加者

50 音順、敬称略

| | | |
|---|---|---|
| 団長 | 土居 範久 | 中央大学教授 慶應義塾大学名誉教授 |
| 団員(*) | 秋元 諭宏 | 米国三菱商事会社 |
| | 池田 泰造 | ㈱ シマンテック |
| | 内田 勝也 | 中央大学 |
| | 大野 浩之 | 独立行政法人 通信総合研究所 |
| | 岸田 明 | 富士通(株) |
| | 清松 哲郎 | (株)日立製作所 情報･通信グループ |
| | 熊平 肇 | (財)クマヒラセキュリティ財団 |
| | 熊平 美香 | (財)クマヒラセキュリティ財団 |
| | 河野 雅彦 | 米国三菱商事会社 |
| | 郡山 信 | (財)金融情報システムセンター |
| | 小橋 哲郎 | NTT Data AgileNet LLC |
| | 小林 一雅 | 日本電気(株) |
| | 佐々木 良一 | 東京電機大学 |
| | 下村 正洋 | ㈱ ディアイティ |
| | 武智 洋 | 横河電機(株) |
| | 田代 勤 | (株)日立製作所 情報･通信グループ |
| | 陳 宇耀 | ㈱ ディアイティ |
| | 中尾 康司 | ＫＤＤＩ㈱ |
| | 中上 昇一 | (株)日立製作所 情報･通信グループ |
| | 長嶋 潔 | 東京海上火災保険(株) |
| | 長瀬 正人 | 三菱商事(株) |
| | 林 誠一郎 | 日本インターネット決済推進協議会 |
| | 林 工 | (株)日立製作所 情報･通信グループ |
| | 林 簡 | (株)インフォセック |
| | 早貸 淳子 | IPA㈱情報処理振興事業協会) |
| | 日岡 幹也 | 米国三菱商事会社 |
| | 藤森 慶太 | 富士通エフ･アイ･ピー㈱ |
| | 舟橋 信 | 未来工学研究所 |
| | 森本 正弘 | シマンテック コーポレーション |
| | 守山 栄松 | 独立行政法人 通信総合研究所 |
| | 山口 美紀夫 | ㈱ フォーバルクリエーティブ |
| | 渡部 茂信 | 日本電気(株) |
| | Eugene J. Yu | 米国三菱商事会社 |
| | Ira Winkler | Hewlett-Packard |

㈱ 一部のみ参加された方を含みます

| | | |
|---|---|---|
| 事務局 | 下村 正洋 | JNSA 事務局長 |
| | 池田 泰造 | JNSA 事務局 |
| | 陳 宇耀 | JNSA 事務局 |

通訳　　中村 忠彦

協力旅行会社　JTB 海外旅行虎ノ門支店

平成 15 年 9 月発行
発行：日本ネットワークセキュリティ協会
東京都江東区新砂 1-6-35
T.T.ランディック東陽町ビル 1F
Tel:03-5633-6061
E-mail:sec@jnsa.org