

ITU-T

(国際電気通信連合 電気通信標準化部門)

会合概要

○活動・組織:

- (1) ITUは、国際連合の専門機関の一つであり、電気通信の改善と合理的利用のための国際協力の推進、電気通信の利用と普及のための技術的手段の開発と能率的運用の促進などを目的として、規制、標準化及び各国の政策の調和等に係る活動を実施している。
- (2) ITU-Tでは、電気通信分野における技術、運用及び料金を世界的規模で標準化するための研究を行っており、分野ごとに分かれた研究委員会(SG: Study Group)により、4年間を1単位の会期として、具体的な研究課題に基づく標準化活動を行っている。
- (3) 情報セキュリティに関する研究課題は、主にSG17(セキュリティ、言語及び電気通信ソフトウェア)において検討されているほか、NGNやRFIDなど特定の技術・システムに係るもの、IDマネジメントなどJCA: Joint Coordination ActivityやGSI: Global Standard Initiativeが組織されているものは、関連するSGの連携により検討されている。

○参加メンバー:

ITUの活動には、191の加盟国のほか、民間企業を中心とする608の部門会員・143のアソシエイト(日本は46の部門会員・9のアソシエイト)が参加(2008年4月現在)。SG17会合には、毎回130名程度(日本から約12名)が参加。

○特色:

ITU-Tの各SGにおける研究結果は、ITU-T勧告として採択された上で、電気通信分野における国際的な共通規格(国際標準)となる。一般的に、ICT製品・サービスを世界市場に展開するためには、国際標準に準拠することが不可欠であり、また、国内で優れた技術等が開発されたとしても、国際標準として採用されなければ国際的に通用しない事態となる。このような状況は、国際標準を国内標準の基礎とすることや国際標準に基づく仕様による政府調達を義務付けるWTO/TBT協定が1995年に発効して以降、ますます顕著になっており、国際競争力強化の観点から、我が国としてITU-Tの国際標準化活動に参加することは非常に重要であるといえる。

情報セキュリティに関する動向

○SG17における主な課題:

- (1) 課題4 通信システムセキュリティプロジェクト: セキュリティ関連課題の進捗管理・課題間調整、関連SG等との調整、セキュリティ・ロードマップの作成
- (2) 課題5 セキュリティ体系及びフレームワーク: 新世代の通信環境(NGN等)におけるセキュリティ体系の検討
- (3) 課題6 サイバーセキュリティ: ネットワーク上の脅威(不正アクセスやDoS攻撃等)に対する具体的な対策技術やガイドラインの検討、IDマネジメントに関する検討
- (4) 課題7 セキュリティマネジメント: 電気通信事業者のための情報セキュリティマネジメント基準(ISMS-T)の検討
- (5) 課題8 テレバイオメトリクス: 通信にかかわる生体認証技術の検討
- (6) 課題9 セキュア通信サービス: モバイルやホームネットワーク等にかかわるセキュリティ技術の検討
- (7) 課題17 スпам対策: スпам対策技術の検討

○我が国の対処・寄与:

- (1) 情報通信審議会 情報通信技術分科会 ITU-T部会に「セキュリティ・言語委員会」を設置し、SG17会合に向けた対処方針や寄与文書に関する国内検討を実施。
- (2) SG17副議長、セキュリティ関連課題を扱うWP2の議長、課題6・7・8のラポータを担当するとともに、2006年1月～2007年2月の間に寄与文書15件(全体数の11%)を提出するなど、SG17会合の活動に積極的な貢献。
- (3) 特に、電気通信事業者のための情報セキュリティマネジメント基準の規格化(課題7におけるITU-T勧告X.1051の改訂作業)、遠隔通信における生体認証を利用した本人認証システムのプロトコル及びプロファイルに関する規格化(課題8における新規ITU-T勧告X.tsm-1の作成作業)等において、中心的な役割を果たしている。

APEC TEL

(アジア・太平洋経済協力 電気通信・情報作業部会)

会合概要

○活動・組織：

- (1)APECとは、アジア太平洋地域の持続可能な発展を目的とし、域内の主要国・地域が参加するフォーラムで、域内の貿易投資の自由化・円滑化、経済技術協力を主要な活動とする。
- (2)APECでは、13の分野別担当大臣会合が設けられており、情報通信に関する議論は電気通信・情報産業担当大臣会合(TELMIN)にて行われている。
- (3)TELMINにより示された指針に従い、電気通信情報作業部会(TEL WG)の下に設置された自由化分科会(LSG)、ICT開発分科会(DSG)、セキュリティ繁栄分科会(SPSG)及びMRAタスクフォースにおいて、電気通信の自由化、WTOへの貢献、電子商取引、電子政府、技術協力の推進、デジタル・ディバイドの解消、能力開発等幅広い内容について議論、検討が行われている。

○参加メンバー：

オーストラリア、ブルネイ、カナダ、チリ、中国、香港、インドネシア、日本、韓国、マレーシア、メキシコ、ニュージーランド、パプアニューギニア、ペルー、フィリピン、ロシア、シンガポール、台湾、タイ、ベトナム、アメリカ合衆国

○特色：

「開かれた地域協力」(APECによって得られる自由化の成果は、APEC域外国にもWTO協定に従って均てんされる。)及び「協調的自主的な行動」(APECは、法的にメンバーを拘束しない、緩やかな政府間の協力の枠組みという性格を維持。各メンバーの自発的な行動により貿易・投資の自由化・円滑化及び経済技術協力を推進することを基本原則とする。)に基づき取組みを推進。

情報セキュリティに関する動向

○SPSGにおける主なプロジェクト(TEL 37) :

- (1) セキュリティ文化の構築 - 政策運営課題(NZ)
- (2) APECエコノミー間での効果的な対応力の強化(韓国)
- (3) サイバー犯罪への執行専門家育成プロジェクト(米国)
- (4) VoIPセキュリティガイドライン(豪州)
- (5) 情報セキュリティ評価証明ガイド(豪州)
- (6) 国際PKI及び電子認証トレーニングプログラム(台湾)
- (7) ボットネットへの政策的、技術的アプローチガイド(中国)
- (8) サイバーセキュリティ演習(米国・韓国)

○我が国の対処・寄与:

- (1) TEL 35において開催された「マルウェアに関するAPEC-OECD共同ワークショップ」において、Cyber Clean Centerの取組を紹介。
- (2) TEL 37を東京で開催。「利用者にとって安全なICT製品・サービス」ワークショップを主催し、ASP・SaaSにおける情報セキュリティ対策に関する取組等を紹介するとともに、「ボットネットに対する政策と技術的アプローチに関するワークショップ」において、Cyber Clean Centerの取組を紹介。
- (3) サイバーセキュリティ演習等、各プロジェクトの推進に積極的に協力。

OECD/ICCP

(経済協力開発機構 情報・コンピュータ通信政策委員会)

会合概要

○活動・組織：

- (1)OECDは、先進国間の自由な意見交換・情報交換を通じて、1)経済成長、2)貿易自由化、3)途上国支援に貢献することを目的とする国際機関である。
- (2)OECDには、29の委員会が設置されており、情報通信に関する議論は情報コンピュータ通信政策委員会(ICCP)において行われている。ICCPの役割は、「情報・コンピュータ・通信に関するシステム・サービス(情報インフラ、電子ビジネス等)の分野における技術の発展とその応用から生じる政策課題と、これらが経済・社会に与える影響の検討に責任を負う」とされている。
- (3)ICCPの下には、4つの作業部会が設置され、情報セキュリティ・プライバシー作業部会(ISP)において、情報システムの脆弱性に対するセキュリティ対策、電子認証や暗号使用の促進、個人情報の保護等の問題に関する議論を行っている。

○参加メンバー：

イギリス、ドイツ、フランス、イタリア、オランダ、ベルギー、ルクセンブルク、フィンランド、スウェーデン、オーストリア、デンマーク、スペイン、ポルトガル、ギリシャ、アイルランド、チェコ、ハンガリー、ポーランド、スロヴァキア、日本、アメリカ合衆国、カナダ、メキシコ、オーストラリア、ニュー・ジーランド、スイス、ノルウェー、アイスランド、トルコ、韓国

○特色：

OECDは、約1000名からなる専門家を抱える「世界最大のシンクタンク」であり、相互審査をはじめとする活動を通じて「先進国標準」が醸成されていく。加盟国は、OECDの活動への参加を通じて、自国の経済・社会政策や制度を調整・改善する機会を得ている。

情報セキュリティに関する動向

○ISPにおける主なプロジェクト(2007-2008):

- (1) 情報セキュリティとプライバシーの共通フレームワークについての分析レポート
- (2) プライバシーの越境執行協力の方策
- (3) 生体認証等のデジタルID管理の分析レポート
- (4) 2002年情報セキュリティガイドラインの見直し
- (5) 1997年暗号政策ガイドラインの見直し
- (6) 国際旅行に関するセキュリティとプライバシーについての政策提言
- (7) RFID、センサーとそれらが情報セキュリティとプライバシー政策に与える影響の分析レポート
- (8) 次世代ネットワークに向けた情報セキュリティとプライバシーについての政策提言

○我が国の対処・寄与:

- (1) 各種分析レポートの作成、ガイドラインの見直し等、各プロジェクトの推進に積極的に協力。
- (2) ISPには、1995年以降、堀部 政男 一橋大学名誉教授が副議長として参加している。

IGF

(インターネット・ガバナンス・フォーラム)

会合概要

○設置経緯・目的:

- (1) 国連主催の世界情報社会サミット(2003年及び2005年)において、現状のインターネット管理の在り方に関して、特定の国の影響力が大きいこと及び途上国の参加が十分でないことが課題とされたことを受け、国連事務総長主導の下、インターネット管理に関する課題をオープンかつ包括的に議論するため設置されたフォーラム。
- (2) 2006年から5年間、毎年開催することが決定されており、2006年はアテネ、2007年はリオデジャネイロにて開催。

○参加メンバー:

国連事務次長、ITU事務総局長、各国政府・国際機関、民間企業・NGO等、毎会合1000名以上のステークホルダが参加(日本からは、総務省、経済産業省、日本経団連ミッション等が参加)

○会合組織:

事務局及びホスト国が主催する 이슈ごとのメイン・セッションのほか、参加ステークホルダ主体で運営される個別テーマごとのワークショップ及びベストプラクティス・フォーラム等を多数開催

○活動内容:

- (1) 「重要インターネット資源」、「アクセス」、「開放性」、「多様性」及び「セキュリティ」という5つの 이슈に関して、参加ステークホルダによる自由闊達な意見交換を行うことにより、インターネット管理における諸課題について共通理解を深め、国際世論を形成するための場としての役割を担う
- (2) 会合の結果は、議長報告としてとりまとめられWeb上に公表

情報セキュリティに関する動向

○「セキュリティ」イシューにおける議論：

- (1) 「セキュリティ」の定義
 - ・ 一義的な定義に関する明確な合意はなし
 - ・ 国家安全保障、ビジネスセキュリティ、ネットワークセキュリティ等の多様な概念
- (2) サイバー犯罪対処を含む法的問題
 - ・ 法執行機関の協力レベル、過剰規制等の問題
 - ・ 法的基盤として欧州サイバー犯罪条約の重要性を支持
- (3) ISPの責任
 - ・ 「セキュリティ」対「開放性」の議論
 - ・ コントロールできる可能性＝責任ととらえるべきか（プロバイダ規制には消極的）
- (4) ソフトウェアの役割
 - ・ オープンソフトウェアであるべきかどうかは賛否両論
- (5) 人権・プライバシー
 - ・ 個人情報保護法の整備がセキュリティに貢献

○我が国の対処・寄与：

- (1) 日本のプレゼンス向上に資するため、日本経団連より、日本産業界の意見を集約した提言を入力するとともに、官民連携のボット対策等、国内の先進的な取組事例を紹介
- (2) 第2回会合において、「国際協力としてのキャパシティ・ビルディング」に関するワークショップを開催（日本経団連、GIPI、ISOC及びJPCERT/CC共催）

ASEAN + J

(東南アジア諸国連合+日本)

会合概要

○活動・組織：

- (1)ASEANとは、1)域内における経済成長、社会・文化的発展の促進、2)地域における政治・経済的安定の確保、3)域内諸問題の解決を目的とした東南アジア諸国連合である。
- (2)首脳会議の下、分野別閣僚会議が毎年定期的に行われており、情報通信に関する議論は電気通信大臣会合(TELMIN)、電気通信高級事務レベル会合(TELSOM)において行われている。
- (3)近年では、ASEAN会合の開催に併せ、日本・中国・韓国を加えた担当大臣会合(ASEAN + 3)や、個別対話国との担当大臣会合(ASEAN + 1)も同時に開催されている。
※ASEANと日本との会合を「ASEAN + J」と呼んでいる。

○参加メンバー：

インドネシア、マレーシア、フィリピン、シンガポール、タイ、ブルネイ、ベトナム、ラオス、ミャンマー、カンボジア

○特色：

東南アジア諸国のICT関係の首脳が一同に会するのは本会合のみ。総務省が参加することで、日本はASEANのパートナーという意識の醸成に貢献するとともに、継続的なマルチ対談の場として、我が国の取組みの幅広い周知とASEAN諸国のニーズ把握が可能となり、今後のICT分野での協力拡大に非常に有効。

情報セキュリティに関する動向

○ASEAN-Japan ICTワークプラン 2007-2009:

平成19年8月にカンボジアで開催されたASAN+J TELMIN、ASEAN+J TELSOMにおいて、日本・ASEAN間のICT分野における協力に関する3ヶ年の作業計画が策定された。

Action 2

情報セキュリティに関するインシデント情報の収集、共有、分析に関する国際協力の推進

- ・日本のTelecom-ISACとASEAN各国のネットワークオペレーター間の連携を強化するとともに、情報通信分野におけるセキュリティ・インシデント関連情報の交換のための地域連絡窓口を設置する。
- ・ICTセキュリティ問題に関するハイレベル会合を開催する。

○我が国の対処・寄与:

- (1) 平成20年度内を目途に、ICTセキュリティ問題に関するハイレベル会合である「アジア情報セキュリティ会議」(仮称)の開催を予定。

CJK Network Information Security WG

(日中韓ネットワーク情報セキュリティワーキンググループ)

会合概要

○設置経緯・目的:

- (1)2002年9月、日本の提唱により、モロッコ・マケラシュにおいて、第1回日中韓情報通信大臣会合が開催された。第2回情報通信大臣会合(2003年9月、韓国・済州)において、協力文書が合意され、大臣会合の下に「ネットワーク情報セキュリティワーキンググループ」が設置されることとなった。
- (2)当該WGでは、(a)ネットワーク・情報セキュリティに関する政策及び制度、(b)ハッキング及びウイルスを含むサイバー攻撃への共同対処並びに情報交換、(c)オンライン上のプラバシー保護に関する情報に関して、交流の充実に努めるものとされている。

○参加メンバー:

- 日本 総務省、Telecom-ISAC Japan
中国 情報産業部(MII) 等
韓国 情報通信部(MIC) 等 ※2007年5月現在

○会合運営

・約1年に1回、各国で持ち回り開催。

・開催状況

- | | | | |
|-----|-----------|---------|---------------|
| 第1回 | 2004年3月 | @韓国・ソウル | コンタクトポイントを交換 |
| 第2回 | 2005年6月 | @日本・東京 | 協力に向けた共通認識を形成 |
| 第3回 | 2007年5月 | @中国・北京 | 具体的実施項目に合意 |
| 第4回 | 2008年開催予定 | @韓国 | |

情報セキュリティに関する動向

○第3回WGにおける合意事項:

- (1)当WGのメカニズムにより、インターネットセキュリティを強化し、また3か国間及び世界におけるインターネット保護の実践を改良しうる協力モデルを活発に探求すること。
- (2)政府機関及びネットワークオペレータの組織を含むCERT/CSIRT等による、マルチレベルの情報交換や協力体制の更なる強化方法の採用を志向すること。
- (3)電気通信政策の発展及びインターネットのネットワーク及び情報セキュリティの法規制の交換の促進に関する国際協力のための基盤を引き続き固めること。
- (4)以下の対策を通し、インシデント報告、異常なトラフィック及びセキュリティトレンドの情報共有を強化するとともに、ネットワーク運営者の組織を含むCERT/CSIRT等の協力を促進すること。
 - ・不審なネットワーク上の動向について相互に注意喚起すること
 - ・BGPプリフィックスハイジャックに関する専門家グループを設置すること
 - ・ボットネット等に係る3か国間の現在の主要な脅威について、可能な情報共有を開始すること
 - ・迷惑メール送信者に関する情報共有に向けて努力すること
 - ・2008年北京オリンピックを標的とした潜在的なサイバー攻撃への対策を支援するよう努力すること

等

○我が国の対処・寄与

- (1)日本提案であるBGPプリフィックスハイジャックに関するプロジェクトの実施に向け、各国のPoCを交換。日本から各国に向け質問票を送付予定。