次世代ＩＰインフラ研究会　第二次報告書（案）に係る意見招請結果及び研究会の考え方（案）　**資料6－3**

（意見提出順）

意見番号	ページ	章番号	項番号	氏名	所属団体名又は会社名	ご意見等	理由	本研究会の考え方
1	41 ～ 54 93 ～ 98	2章 5章	2.1 2.4 5.2	-	ＮＴＴコミュニケーションズ株式会社	「消費者の視点から」「誰でも、簡単かつ安全に」家電を利用するためのセキュリティの問題を議論する(P44) 「情報家電によるインターネットの利用形態は従来とは大きく異なる可能性がある(P46) 「家電業界とISP業界との情報交換・共有の必要性」(P53) という点においてＮＴＴコミュニケーションズは、賛同いたします。 情報家電のネットワーク接続のセキュリティ確保のためには、技術的仕様、事業者間取り決めの検討だけでなく、消費者への啓蒙活動を始めとした社会インフラとしての議論が必要と考えており、今後の具体的な議論へ参加し、課題解決に貢献したいと考えます。	「情報セキュリティ政策２００５」(2) ユビキタスネット社会への対応における、1) 接続検証と規格化、2) 機器認証の課題については、情報家電メーカとISPが中心となって取り組んでいるユビキタス・オープン・プラットフォーム・フォーラム(以下、UOPF)が技術仕様の策定と情報家電同士の接続実証実験を実施しており、一定の成果をあげています。UOPFでは、以下の方針の下、国内外に広く活動を展開しています。 ① 新たなマーケットの創造と育成に貢献すること ② 技術仕様やガイドラインが各社のビジネスモデルを制限しないこと ③ 消費者にとってのセキュリティがトータルで提供されること ④ サービス、機器提供者にとってセキュリティインシデントのリスクを最小限にするよう考慮していること ⑤ 情報家電全体をひとくくりにするのではなく、利用シーン・機器毎に必要十分なセキュリティを考慮すること ⑥ ワールドワイドな活動であること 本報告書が掲げる情報家電のネットワーク接続への対応の課題解決のためには、UOPFのような団体および参加企業と精力的に議論すべきと考えます。	ご意見及び本報告書を踏まえ、有効な施策が展開されることを期待している。
2	32	1章	1.4.5	（匿名希望）	個人	トレースバックを行う場合、その実施可否についての法的根拠を、今後、明確にしていって欲しい(対ボットに限らず)。	IP網におけるトレースバックは、電話網での逆探知に近い行為であると考える。逆探知には令状が必要、ということと同様に、情報の秘匿/保護についての考慮が必要であると考えるが、インターネット環境において、令状ありき、の行動では、(特に国際問題の場合)時間ロスが多く、影響が広がる可能性がある。 しかしながら、この可否判断は通信事業者毎ではなく、通信の秘密という観点からも、統一化された判断基準の制定が望まれる。	ボットネットからの攻撃については、現時点では、違法性阻却事由があるため「通信の秘密」に属する事項を追跡できる場合であっても、送信元を突き止めるための技術がそもそも存在しないのが実情である。 技術的に全くトレースバックできないままでは攻撃に対する抑止力も働かないことから、まずは技術的に、送信元を突き止めることを可能とする「トレースバック技術」の研究開発を進めるべきことを記述しているものである。 この研究開発が成就した後、開発された「トレースバック技術」を実際にどのような場合に使うことが法制上許容できるかについては、「トレースバック技術」により送信元をどの程度まで特定できるのか、また特定に当たって他にどのような情報を必要とするのかにより大きく異なる。 したがって、「トレースバック」の実施可否についての法的根拠については、「トレースバック技術」の研究開発の進捗をみつつ、より多くの法律の専門家の参加を得て、あらためて検討を行うことが適当と考えられる。
3	91	5章	5.1(1) 2)②	（匿名希望）	個人	ICT障害の広域化は経路のみならずDNSにも言及すべき。	インターネット上の大部分の通信は、DNSによるドメイン名とIPアドレスのマッピングを検索することによって行われており、DNSが機能しなければやはりICT障害の広域化となるため。	IPネットワークWGにおいても同様の意見が出たため、第三次報告書（案）の第六章でＤＮＳの信頼性確保等に係る課題について言及しているところであり、ご指摘の事項については、今後、別途検討を要する課題と考えられる。

意見番号	ページ	章番号	項番号	氏名	所属団体名又は会社名	ご意見等	理由	本研究会の考え方
4	91	5章	5.1(3)	(匿名希望)	個人	内容からして、これは「人材面の脆弱性の克服」ではなく、「人的・社会的要素に起因する脆弱性の克服」である。 また、人的・社会的要素に起因する脆弱性の克服のための意識向上の施策に加え、それを補う技術の開発にも言及することが望ましい。	人的要因にかかわる、脆弱性の克服が重要である。しかしながら、全ての利用者が知識を持ち合わせるということは現実には難しい。一般ユーザの知識がなくても安全が担保されるフレームワークを実現することによって、より安全なインフラとなりうるのではないか。 そのためにはOSなどのソフトウエア自身における技術開発、通信事業者を含めた通信の仕組みそのものにおける技術開発により、機器が自ら自動的に安全性を確保する技術を開発し、技術でそのフレームワークを実現することを考える必要がある。	人的・社会的要素に起因する脆弱性を機器等の技術開発によって克服すべきとのご意見であるので、p53を次の通り追加修正する。 「また、家電に関するユーザのセキュリティ意識は、コンピュータに関するユーザのセキュリティ意識に比べて低いという人的・社会的要素に起因する脆弱性も、情報家電におけるセキュリティ確保をコンピュータにおけるセキュリティ確保以上に難しくしている。 このため、全ての利用者がセキュリティに関する知識を十分持ち合わせていないということを前提に、情報家電を含む利用者端末が自律的に安全性を確保し得る技術を開発すること等により、家電業界と通信業界とが連携して、こうした脆弱性を補完する仕組みを構築していくことも重要である。」