

中間報告書に関する意見募集の結果 及び研究会における考え方(案)

次世代の情報セキュリティ政策に関する研究会

事務局

2008年5月23日

1 実施期間

2008年4月5日(土)から2008年5月4日(日)まで

2 意見件数

計3件

3 意見提出者一覧

(受付順、敬称略)

番号	意見提出日※	意見提出者
1	2008年5月2日	エヌ・ティ・ティ・コミュニケーションズ株式会社
2	2008年5月2日	ヤフー株式会社
3	2008年5月3日	個人

※意見提出日は、総務省に提出された日(受付日)を記載しております。

4 意見に対する考え方

別表参照

章	項	頂いたご意見	研究会における考え方
Eヌ・ティ・ティ・コミュニケー ションズ株式会社			
5. 現状及び近い 将来のICT環境に おける情報セキュ リティ対策の重要 性	5-2 今後の情報セ キュリティ対策につ いて重点的に検討・実 施すべき事項等	<p>【中間報告書の記載】 P. 41 サービス提供事業者や機器製造事業者、電気通信事業者等のICTサービス提供者側が事前に想定し得る対策を講じた上で製品・サービス等を提供しなければならない責任を有していることはそもそもの前提であるが、（略）</p> <p>【弊社意見】 想定し得る対策という表現は非常に広範囲であるため、上記引用文を以下のとおり修正することが適当であると考えます。</p> <p>【修正案】 サービス提供事業者や機器製造事業者、電気通信事業者等のICT サービス提供者側が事前に<u>必要不可欠かつ現実的に</u>想定し得る対策を講じた上で製品・サービス等を提供しなければならない責任を有していることはそもそもの前提であるが、（略）</p>	<p>中間報告書の内容は、ご指摘のと通りの趣旨を述べようとしたものであり、内容の明確化のため、貴見の通り、修正いたします。</p>

章	項	頂いたご意見	研究会における考え方
		<p>【中間報告書の記載】 P. 43</p> <p>イ)上記ア)の検討に資するため、正規のWebサイトを閲覧しただけでマルウェアに感染してしまう状況を踏まえ、利用者が誤ってフィッシングサイトやマルウェア配布サイト等の危険なWebサイトと通信することを防止するため、信頼性の高いレピュテーション・データベース(危険なWebサイト等に関するリスト)の構築とその運営方法等についての実証を促進し、その効果を検証することが必要である。</p> <p>【弊社意見】</p> <p>レピュテーション・データベースは電気通信事業者だけでなく関係機関等と共同で構築、運営される必要があることから、レピュテーション・データベースの構築とその運営方法及び実証実験の実施主体等について明確にする必要があると考えます。</p>	<p>レピュテーション・データベースを活用することにより、インターネット利用者がマルウェアサイト等へアクセスすることを制限する情報セキュリティ対策は、電気通信事業者が行う対策であることから、主体はその対策を実施する電気通信事業者であると考えております。</p> <p>なお、貴見の通り、当該データベースを構築し、運用するに当たっては、業界団体を含む関係機関との連携を整理し、情報セキュリティ対策として適切な手法とすることが必須であり、この点については、実証等を進める中で、具体化・詳細化を進めていくことが必要であると認識しております。</p>
		<p>【中間報告書の記載】 P. 44</p> <p>・ユーザーサポート体制に所属する人材としては、電気通信事業者や情報通信機器関連のベンダー等の技術者等を活用することが有効であり、高齢者の雇用機会確保にも貢献するものと期待される。</p> <p>【弊社意見】</p> <p>活用する人材を明確にするために、上記引用文を以下のとおり修正することが適当であると考えます。</p>	<p>中間報告書の内容は、ご指摘のとおり趣旨を述べようとしたものであり、貴見の通り、修正いたします。</p>

章	項	頂いたご意見	研究会における考え方
		<p>【修正案】 ・ユーザーサポート体制に所属する人材としては、電気通信事業者や情報通信機器関連のベンダー等の技術経験者等を活用することが有効であり、高齢者の雇用機会確保にも貢献するものと期待される。</p> <p>【中間報告書の記載】 P. 44 なお、このユーザーサポート体制の実現に当たっては、（中略）一定程度のスキルを身につけている者が当該業務にあたるよう、その知識やスキルを認定する仕組みを検討すべきである。</p> <p>【弊社意見】 情報セキュリティ対策において、ユーザーサポート体制の充実の必要性と、そのための認定制度を民間主体にした取組として検討することについて賛同いたします。なお、認定制度については、既存資格を最大限活用する仕組みを検討することが有効であると考えます。</p>	<p>ユーザーサポート体制について、既存資格がユーザーサポート体制に従事する者に対して要求される技能・知識等をすべて包含するものである場合には、新しい資格制度を創設せずに、該当する既存資格を活用することが、類似資格等の乱立を防ぎ、利用者等の混乱を防ぐ点からも重要であると考えております。</p> <p>こうした点を踏まえ、ユーザーサポート体制に求められる技能・知識等と既存資格との関係を整理し、資格所得希望者にとって過度な負担にならないように考慮しつつ検討を進めることが必要であるとと考えております。</p>

章	項	頂いたご意見	研究会における考え方
ヤフー株式会社			
5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性	5-2 今後の情報セキュリティ対策について重点的に検討・実施すべき事項等(関係機関における連携強化)	<p>報告書(案)47頁において、「ユビキタスネットワーク社会において、利用者が安心・安全に様々な情報通信機器・端末を駆使し、多様なサービスを利用できるようになるには、電気通信事業者、OS/アプリケーション/サービス提供者…(中略)…それぞれ独自に情報セキュリティ対策を実施するだけでなく、お互いに協調・連携することが重要である。このため、上記のような全ての関係者が参加し、継続的に情報セキュリティに関連する課題やその対策等について検討する業界横断的な検討体制を整備することが必要である。」とされていますが、そもそも、各業界間はもとより、業界内においても各社において情報セキュリティに対するポリシーはそれぞれ異なっているところであり、そのような者が集まって検討を行ったところで、意義のある議論を行うことは困難であると考えます。また、業界横断的な対策をとることが必要であるのか、有効であるか、(国際競争力の観点から)効率的であるか否かについても、求められる情報セキュリティの程度を明確にしなければ、本来は判断できないものと考えます。</p> <p>そこで、弊社と致しましては、上記「業界横断的な検討体制の整備」の前提として、ユビキタスネットワーク社会におけるそれぞれのプレイヤーが業界横断的に共通認識としてもつべき「求められる情報セキュリティの程度」について、整理する必要があるものと考えます。</p>	<p>貴見の通り、インターネット利用者である個人を含め、各主体がそれぞれの責任において、どういった情報セキュリティ対策をどの程度実施すれば良いのかについての検討、及び共通認識の醸成が必要であると考えており、こうした検討を進めるに当たっては、個別に関係者が集まり其々の立場のみから検討を進めるよりも、業界横断的な検討体制を構築して関係者間の調整を図りながら検討することが望ましいと考えております。</p> <p>また、情報セキュリティ脅威は、今後より一層速い速度で変化していくものと考えられ、こうした変化に迅速に対応していただくためにも、民間主体による継続的な検討体制の構築が重要であると考えております。</p>

章	項	頂いたご意見	研究会における考え方
個人		※「頂いたご意見」は提出者ご自身がまとめられた要旨のみを記載しております。詳細はご意見本文をご覧ください。	
4. 近い将来の ICT 環境と情報セキュリティ脅威・課題	4-1 近い将来における ICT 環境の変化（通信環境の変化の状況）	1. NTT 東西には、ADSL からの NGN へのアクセスをサポートする義務があると考えます。このサービスに関する設備投資には、NTT 東西の消費者向け光ファイバサービスの独占的状況を見る限り、ユニバーサル・サービス基金からは1円たりとも支払いをするべきではありません	ご意見の内容につきましては、本意見募集の対象外です。
2. 情報通信環境の現状	2-5 ICT による生産性の向上と ICT 産業の国際競争力強化	<p>2. IT インフラの活用による国際競争力の強化という政策に賛成しますが、実印、社印などの制度に踏み込んだ議論を期待いたします</p> <p>【事務局補足】 本意見に関しては、以下の2点について、述べられております。 ○前段のご意見： 日本が IT インフラを用いたビジネスの高速化を目指す中で、企業の業務や意思決定の迅速化は避けて通れないものであり、場合によっては実印や会社印の制度にまで踏み込んで、抜本的な解決を行う必要がある。 ○後段のご意見： 総務省の子供向けや企業向けの啓蒙的なウェブサイト（「国民のための情報セキュリティサイト」のことと思われる。）は、必ずしもその認知度が高くない。当該サイトの知名度アップを図るべき。中小企業における事業の効率化と、リスク・マネジメントのバランスの取れた現実的問題解決策とはどのようにあるべきかという議論を先導したり、広く国民的なデジタル・リテラシーの</p>	<p>貴見の前段につきましては、本意見募集の対象外ですが、今後の参考とさせていただきます。</p> <p>貴見の後段にある総務省における情報セキュリティ対策に関する普及啓発活動につきましては、ご指摘を踏まえ、総務省において「国民のための情報セキュリティサイト」の周知活動や中小企業等を対象にした情報セキュリティ対策の向上に向けた普及啓発活動の充実を図ることが適当であると考えております。</p>

章	項	頂いたご意見	研究会における考え方
		水準を上げていく政策運営を期待する。	
5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性	5-2 今後の情報セキュリティ対策について重点的に検討・実施すべき事項等(利用者を取り巻く環境における情報セキュリティ対策の徹底)	3. 安易なフィルタの設定には、通信の秘密、閲覧の禁止という観点から、賛成いたしかねます	<p>レピュテーション・データベースに関する意見だと思われませんが、本研究会では、例えば誤ってマルウェアサイトにアクセスした利用者がウイルス等に感染することによって自らが被害者となるだけではなく、本人が気付かないうちに他人に被害を及ぼす加害者になってしまう状況があること、また、今後 ICT サービスや機能等が高度化することにより、適切な情報セキュリティ対策を実施することができない利用者層の増加も懸念されることから、利用者個人の対策の重要性が第一であると認識しつつも、ネットワーク全体の安全性・信頼性を確保する観点から、電気通信事業者等による情報セキュリティ対策が必要であると考えております。</p> <p>なお、ご指摘の通信の秘密等については、きわめて重要な検討事項であると認識しており、レピュテーション・データベースを活用した電気通信事業者による情報セキュリティ対策の実施に当たっては、事前に予定している実証実験においてデータベースの構築・運用方法の確立とともに、その目的、必要性、手段の妥当性等についても、併せて検討したいと考えております。その際、諸外国の制度について、状況把握等を進めて参りたいと考えております。</p>

章	項	頂いたご意見	研究会における考え方
3. 情報セキュリティ対策の現状と課題	3-4 情報セキュリティ対策の取組み状況と課題	4. デスクトップ検索の危険性を広く国民にむけに啓蒙し、SSL だから安全なのではなく、SSL だから危険なのだという意識を浸透させる必要があります	安全と思われていた対策が、技術の進歩や別のソフトウェアとの組み合わせ等により、その安全性が低下してしまう可能性や新たな脅威が発生する可能性があることを示唆したものと考えております。 ご指摘を踏まえ、常に最新かつ適切な情報セキュリティ対策を実施する必要があることについて、利用者の理解が浸透するよう、現状認識及び普及啓発に関連する事項として、その趣旨を反映することといたします。
5. 現状及び近い将来の ICT 環境における情報セキュリティ対策の重要性	5-2 今後の情報セキュリティ対策について重点的に検討・実施すべき項目等(利用者を取り巻く環境における情報セキュリティ対策の徹底)	5. APEC や OECD でのハイレベルの議論も必要ですが、JPNIC のリソース不足を解消しなくては、現場レベルでの対応は不可能と考えます	個別の企業・団体等に限らず、中間報告書 5-2 項(産学官連携による先進的な研究開発の実施)(P.45)において、情報セキュリティ対策に係る人材育成に積極的に取り組むことが必要であるとしております。
5. 現状及び近い将来の ICT 環境における情報セキュリティ対策の重要性	5-2 今後の情報セキュリティ対策について重点的に検討・実施すべき事項等(関係機関における連携強化)	6. PC 以外の機器へのマルウェア感染が増えるとの見解に賛成するとともに、近い将来における最悪のシナリオを回避するため、自動車がボットと化す可能性のリスク査定を、行政当局や自動車業界に期待いたします	ご指摘の通り、工業製品の ICT 化に伴う脅威は、場合によっては直接人命に影響を及ぼすことが想定されることから、こうした脅威への対策は、これまで以上に重要になるものと考えられます。こうした問題認識についての追加をいたします。
4. 近い将来の ICT 環境と情報セキュリティ脅威・課題	4-2 近い将来の ICT 環境における情報セキュリティの脅威・課題		

章	項	頂いたご意見	研究会における考え方
4. 近い将来の ICT 環境と情報セキュリティ脅威・課題	4-1 近い将来における ICT 環境の変化 (社会状況の変化)	7. 将来の日本の国際競争力を考察するにあたり、人口減少社会を前提とするのではなく、ヨーロッパ先進国のように、外国からの移民や出稼ぎ労働者を受容することを真剣に考慮すべきだと考えます。また、国際競争力の維持のため、特許制度に対する国際的なアプローチを期待するとともに、NHK の事実誤認の報道について総務省の果たすべき役割とは何か、私見を述べさせていただきます	ご意見の内容につきましては、本意見募集の対象外です。
4. 近い将来の ICT 環境と情報セキュリティ脅威・課題	4-1 近い将来における ICT 環境の変化 (通信環境の変化の状況)	8. NTT 東西の NGN サービスが、中国・韓国だけではなく、米国・ヨーロッパ各国の動向を視野に入れながら、従来の NNI や UNI の概念を越えたアプリケーション・インタフェースにおいて、世界的な仕様統一を満たすものであるよう、NTT 東西に対する総務省の指導力に期待します	ご意見の内容につきましては、本意見募集の対象外です。
4. 近い将来の ICT 環境と情報セキュリティ脅威・課題	4-2 近い将来の ICT 環境における情報セキュリティの脅威・課題	9. テレワーカーを増やすという政府目標の達成のためには、ブロードバンド・モデムの機能拡大が必要であるとともに、IPv6 対応にあたってネットワーク設計に慎重な対応が求められることを重視、また、昨今の NGN より 10 年ほど前に、既に IP と X.25 を統合するメインフレーム的な発想のプロトコルが存在していたことを指摘させていただきます	IPv4 ネットワーク上で UDP パケットにより IPv6 を通過させるトンネル技術等によるセキュリティ上の問題等、IPv6 化に伴うセキュリティ環境の変化とその影響について、第 4 回目の研究会において議論しており、IPv4 との併存環境において情報セキュリティ対策が煩雑化する可能性も踏まえ、技術的な課題への対策の必要性を取りまとめているところです。

章	項	頂いたご意見	研究会における考え方
5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性	5-1 今後の情報セキュリティに関する主な課題等	10. 永遠のビギナーは、マイクロソフトとNTT DoCoMoが、「他社がやっていることに対しては、どんなつまらない機能であっても、必ず対抗策をうつ」という企業体質を変えることが無い限り大きな問題とはならず、市場に任せれば自然と解消される問題だと考えます	今後、情報通信機器の高機能化やICTサービスの多様化により、情報セキュリティ対策に対する意識やスキルが必ずしも高くないと考えられる、いわゆる「永遠のビギナー」層が増加するとともに、ウイルスに感染して意識せずに他人に被害を及ぼす加害者となってしまうことがあることを前提として、実施すべき必要な対策を検討することが必要であると考えております。
-	-	11. 成人向けコンテンツをコントロールしようとする試みは、日本の法体系の前提である「罪刑法定主義」と「刑法における拡大解釈禁止」の原理を、侵犯することがあってはなりません。既に「教えて！goo (OKWave)」のように、自主規制が言論の自由を奪い始めている危険な例が存在しますが、表現の自由と知る権利について、時計の針を逆回りさせるような政策には、賛同いたしかねます	ご意見の内容につきましては、本意見募集の対象外です。
4. 近い将来のICT環境と情報セキュリティ脅威・課題	4-1 近い将来におけるICT環境の変化(通信環境の変化の状況)	12. 電子マネーはビジネスモデルによっては運営会社破綻の可能性があります。プリペイド型の電子マネーサービスについては、本来であれば株式投資なみのリスク査定が必要であることを、広く国民に注意勧告すべきだと考えます。ただし、行政が安易に政策的介入を行うことは、本末転倒であると思えます	ご意見の内容につきましては、本意見募集の対象外です。

章	項	頂いたご意見	研究会における考え方
5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性	5-2 今後の情報セキュリティ対策について重点的に検討・実施すべき事項等(利用者、情報通信環境、情報セキュリティが共生するICT社会モデルの検討)	13. 将来の社会のあり方については、既に外国に Extended Enterprise という概念が存在することを指摘させていただくとともに、技術的にはインターネットVPNで対応可能なネットワーク構成であるものの、インターネットVPNの弱点としてDDoS攻撃による機能停止がありうることを述べさせていただきます	将来の情報通信環境においては、ネットワークに接続される端末や利用者の数、情報量が爆発的に増加するとともに、複数の関係者が関連してサービスが提供されることとなることから、現時点では、こうした状況下における情報セキュリティ対策を検討する参照モデルが確立されていないというのが研究会としての認識であり、利用者の利便性、多様なサービスを提供する情報通信環境と情報セキュリティ対策が両立するICT社会モデルを検討することは、ご指摘の企業間企業(extended enterprise)の概念における情報セキュリティ対策にも有効な参照モデルになるものと考えております。
4. 近い将来のICT環境と情報セキュリティ脅威・課題	4-2 近い将来のICT環境における情報セキュリティの脅威・課題	14. 無線局とNTT東西の関係について、NTT東西とNTT DoCoMoやウィルコムとの関係を見据えながら、施設設置負担金制度の抜本的改革の案を呈示させていただきます 【事務局補足】 本意見に関しては、以下の2点について、述べられております。 ○前段のご意見： 無線局数や破壊行為の増加という現象が本当に発生するのか、大いに疑問である。 ○後段のご意見： 施設設置負担金制度の抜本的改革の案の呈示について。	貴見の前段につきまして、フェムトセル方式の設備等が多数設置される状況が見込まれること等による物理的な脅威が増加する可能性、或いは公衆の無線アクセスポイントへのなりすまし等による脅威が増加する可能性等があることを述べているものであり、表現の適正化を検討いたします。 貴見の後段の内容につきましては、本意見募集の対象外です。

章	項	頂いたご意見	研究会における考え方
2. 情報通信環境の現状	2-3 社会経済活動のICT依存の増加	15. セカンドライフの過大評価は避けるべきものであり、匿名性の高い世界ではあっても完全な匿名であることはありえず、2ちゃんねるのように、犯行予告や風説の流布での逮捕例があることを考慮すべきだと考えます。また、セカンドライフの顧客情報保護能力は、SaaSを提供している大手の会社と同等のものであると考えてよいのか、中長期的な経過観察が必要だと考えます	セカンドライフについては、その利用者の急激な増加、民間企業の参入によるマーケティング・プロモーション活動の展開等が進展していると言われており、セカンドライフに限らず、仮想空間での活動が現実の世界に及ぼす影響が見込まれると考えられることから、今後の発展を肯定的にとらえ、現状の記述としております。
4. 近い将来のICT環境と情報セキュリティ脅威・課題 5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性	4-2 近い将来のICT環境における情報セキュリティの脅威・課題 5-2 今後の情報セキュリティ対策について重点的に検討・実施すべき項目等(利用者を取り巻く環境における情報セキュリティ対策の徹底)	16. 携帯・自動車電話事業者のネットワークモデルによっては、音声通話定額サービスの対象となる番号を間違えることによる課金ミスが否定しきれないこと、また、誤った相手につながってしまうという現象も否定しきれないことを指摘させていただきます	ご指摘の点については、個別に例示をしておりますが、中間報告書4-2項「近い将来のICT環境における情報セキュリティの脅威・課題 ①情報通信技術の高度化」に含まれる事項と考えております。 また、本件については、中間報告書の5-2項(利用者を取り巻く環境における情報セキュリティ対策の徹底)(P.41)において、「サービス提供事業者や機器製造事業者、電気通信事業者等のICTサービス提供者側が事前に想定し得る対策を講じた上で製品・サービス等を提供しなければならない責任を有していることはそもそもの前提」としており、係る事項については、電気通信事業者等の責任として必要な対策を講じるべきこととしております。

章	項	頂いたご意見	研究会における考え方
3. 情報セキュリティ対策の現状と課題	3-4 情報セキュリティ対策の取り組み状況と課題	17. デスクトップ仮想化技術やシンクライアントの利用にあたり、ハードディスクによるブレードサーバからフラッシュ・メモリへの切り替えを後押しすることで、地球温暖化対策にもなり、中国、インドでの日本企業のプレゼンス拡大にも役立つと考えます	<p>本研究会は、次世代の情報セキュリティ政策について検討しており、その目的に絞って取りまとめております。</p> <p>なお、総務省が昨年公表した「ICTを環境にやさしく活用するために」(http://www.soumu.go.jp/s-news/2007/pdf/070406_1_1.pdf)において、シンクライアントシステムはセキュリティ対策とともに環境負荷を小さくすることもできるとされているところです。また、総務省で開催した「地球温暖化問題への対応に向けたICT政策に関する研究会」の報告書が本年4月に公表されていますが(http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/ict_globalwarming/pdf/0804_h1.pdf)、本報告書において、データセンタやASP・SaaS事業者の環境配慮対策などが示されているところです。</p>
5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性	5-2 今後の情報セキュリティ対策について重点的に検討・実施すべき項目等(利用者を取り巻く環境における情報セキュリティ対策の徹底)	18. 一般消費者にもセキュリティの向上や著作権保護を義務づけるのであれば、昨今のWeb2.0やWikiの概念に抵触しない範囲でとどめるべきと判断します	<p>インターネットを利用する個人についても、意識せずに他人に被害を及ぼす可能性がある現状を踏まえると、一定程度の情報セキュリティ対策を実施することが社会的責任として必要であると考えておりますが、こうした対策の内容・レベルについてはその実施方法も含め、継続的な検討が必要であると認識しております。</p> <p>インターネットの持つ機能等を勘案しながら、社会インフラとして安心・安全に使える環境を整備することについて、検討を深めることが必要であると認識しております。</p>