資料－１

自律移動支援プロジェクト　第３回セキュリティポリシー検討専門委員会
議事概要（案）

１．日　時：2006 年 8 月 25 日(金)　10:00～12:00

２．場　所：東海大学校友会館　朝日の間・東海の間

３．議事次第

（１）開会

（２）委員長あいさつ

（３）議事

①第 2 回委員会の議事概要

②第 3 回委員会のポイント

③自律移動支援システムのリスク分析の考え方

④自律移動支援システムのセキュリティガイドラインの構成の考え方

（４）その他

（５）閉会

４．議　事

（１）リスク分析の考え方について

・ リスク対策はフェーズ毎に実施するものであり、リスク評価もフェーズ毎で良い。（合成して考える方法もあるが、今回の場合はフェーズ毎でも良いのではないか。）

→ 今回は、フェーズ毎に分析を実施した。

・ リスク対策には、事象発生前にできることと、発生後にできることがある。発生可能性に関わらず、影響度が大きいリスクには、普通、事後的で影響度を下げる対策が取られる。

・ 「稀」な事象でも、そのときに動くことが非常に重要となるサービスもあることを留意すべき。（例：聴覚障害者にとっての公共交通機関の事故・遅れ情報など）

→ ニーズが高い情報については、影響が大きいと評価し、最適化することとしている。

・ リスクの影響度を、定量化して評価できないか。例えば、判例によれば、損害賠償の額については、死者の発生＝3,000～4,000 万円、利用者の困惑＝10 万円などとされているといった例もあるので、それらを参考に数値化すれば分かり易い。厳密な定量化は無理でも、例えば、「重」は「軽」の何十倍なのか何百倍なのか、といった数字は必要ではないか。保険会社や弁護士に相談してみてはどうか。

→ まずは、定性的にとりまとめることを予定している。数値化については、実現可能性を含め、改めて議論させていただきたい。

・ 誰に対するリスクかを整理すべき。

例１　リスクを他者に移転しても、システム全体のリスクは減らない。当事者にとってのリスクだけを考えれば良いのか、システム全体のリスクを考えるのか？

例２　端末製造者のリスクに、「製品仕様を満たさない情報端末を出荷することにより、利用者の誘導が行われない」とあるが、これ自体は利用者に対するリスクである。適切な誘導が行われなかったことを理由として製造物責任を問われた場合は、端末製造者のリスクとなる。

→　ご指摘のとおりであり、再度整理する。
・　リスク処理４策は、単純な４つの選択肢なのか、「保有・移転」組、「最適・回避」組の組み合わせの４象限なのか、といった視点でも考えて欲しい。
・　リスク分析においては、感想など定性的判断に基づくリスクも抽出・評価すべき。
・　観念的には移転／共有できても、法的には移転／共有することができないリスクもある。例えば、個人情報の取り扱いに関するリスクは、委託先に対する監督責任という形で残り続ける。
・　リスクの移転の扱いは、主体により異なる。（民間の事業者は、安全管理措置に関し観念的にリスクの移転ができても、委託先の監督責任まで移転することは法的にはできない。行政機関・独立行政法人等は、リスクの移転の仕方・許容範囲について、委託先への措置要求という形で法的に認められる場合がある。）なお、自治体によっては条例によって異なる。
・　リスクの回避が、結果的に萎縮効果として働く可能性がある。また、リスク回避の結果責任として、違法行為や脱法行為に問われたり、事故が発生した場合は不法行為や債務不履行責任を問われたりする。回避に伴う新たなリスクが無いかを確認した上で、リスクを回避する必要がある。
→　ご指摘の通り。個別にご相談させていただきたい。
・　現状では、詳細なリスク分析結果をこの委員会の中できちんと評価できるか疑問。現実的に困るであろうリスクを念頭に置き、シンプルな評価をすべき。
→ 本日のご意見をふまえ、分析の見直しを行い、シンプルかつ大事な部分で抜けが無いような資料を作成し、次回委員会でご確認いただきたい。
・　非常時としてどんな事態を想定したかを分かる表現にすること。
→　越塚先生にも同様のご意見をいただいており、何を想定したかを明確化する。
・　自動車交通は道路空間を「案内」と「規制」で成立させているが、「規制」には「案内」より厳しい罰則を課している。自律移動支援システムのサービスは当面は案内であるが、案内の中にも「案内的なもの」と「規制的なもの」に分けられ、それによって生ずるリスクも違うことを考慮すべき。
・　ここでは、ありとあらゆる事態を想定することを目的としており、隙間の無い議論が出来ているかどうか、再度確認していただきたい。
→　まず重大なリスクから対応策を整理した後、隙間についてご議論いただきたい。

（２）セキュリティガイドラインの構成の考え方について

・　ガイドラインの目的で、「利用者の保護等、関係者の利益の尊重」とあるが、利用者の保護を中心に考えるべきではないか。
→　「利用者の保護」という目的を明確にするための文章であり、表現を見直す。
・　ガイドラインの基本方針には、「基本方針の作成の考え方」を入れた方が良い。
→　ご指摘の通り。
・　管理策の検討においては、参考資料－１の一覧表をリスク毎、主体毎に並び替えた上で、「誰がこのリスクに対してどの程度の対策を取るのか」をわかるようにすべき。ガイドラインは主体別で良い。
→　ご指摘の通り。
・　ガイドラインをシンプルにするため、参照規程を活用し、必要な部分のみ明確に記述するという方法もある。

例　電気通信役務提供者の安全管理措置は、「電気通信事業における個人情報保護に関するガイドライン（総務省）」に基づくこととする

・ 法的拘束力は持たず、自発的に守っていただく、ということで良いのか？このガイドラインを守らないと、システムに入れないようにすべきではないのか？拘束力を持たせるのであれば、その担保の仕方を考えるべき。

例　行政措置として参加を止める、罰則をかける

→ ガイドライン自体をそのまま法律にすることは考えていないが、何らかの担保をとりたいと考えている。担保の取り方は個別に違うと思われるので、個別具体に検討の上、ご相談させていただきたい。

・ 契約条件や調達条件を守らないことから、一方的に過度のセキュリティ対策を求めることは、独禁法上の「優越的地位の濫用」となる可能性があり、そのことを念頭にガイドラインの性格（範囲、趣旨、拘束力）を決定すべき。

（3）その他

・ リスク評価件数は「大」が少なく、「小」が多いが、資料－3　3ページ図の横軸（発生確率）は逆ではないか？（右側が「稀」で左側が「頻」ではないか？）

→ 発生確率「頻」の件数が少なく、「稀」の件数が多いため、リスク評価結果は「大」が少なく、「小」が多くなっている。

・ 本委員会では、非常時にサービスレベルを維持するためにはどういう対策が必要か、という整理を行い、非常時にサービスを提供するかどうかの判断は親委員会に仰げば良いのでは。

・ サービスを止めるのは、リスク回避ではなく、リスク最適化だと思われる。

→ 現状、リスク回避としたものについても、サービスをどのように止めるか、どういうアナウンスを行うかについて、ガイドラインに落とし込むことを考えている。

・ より具体的に議論をするため、サービスの提供者を明示していただきたい。

→ 現時点ではビジネスモデルがはっきりしていないが、「こういう前提では、こういう主体だ」ということを整理したい。なお、実証実験では、実験主体で全て行っている。

・ 将来、億単位のタグが入った場合には、瞬間的に故障・支障が無い状態で運用することは不可能なため、100%保証型ではなくベストエフォート型にせざるを得ない。利用者にこのことを理解してもらうためのリスクコミュニケーションを図っていくということをガイドラインの項目に入れる必要があると思われるので、今後議論頂きたい。

・ 新しい技術の導入に際しては、特に社会性が大きな場合は、規制と育成のバランスが重要。また、利用者や広い意味での関係者も含め、新しいシステムを社会的に育てていくという視点も大事。社会全体の観点から、このシステムをどう育て、利用していくか、考えていきたい。

（4）今後の進め方について

・ 将来の実用化に向けて、ガイドラインは実証実験フィールドにも反映させていきたいと考えており、今後ともご協力よろしくお願いしたい。

・ 次回、第3回委員会は11月くらいに開催予定である。日程については後日連絡する。

以　上