次世代IPネットワーク推進フォーラム
技術基準検討WG報告書

別添2　安全性・信頼性SWG　検討資料

平成18年10月

重点的に検討すべき技術的条件

番号	検討項目	技術的条件（案）	必要性
1	発信者番号偽装対策	事業者は、0AB-J_IP電話端末からの発信者番号の正当性の検証を行い、正当でない発信者番号が検出された場合は、発信者番号を無効にする等の措置を講ずること。	発信者番号の正当性を担保することについての社会的な重要性の高まりから、自網のユーザが発信者番号を偽って発信ができないようにすることなどの、発信者番号を偽装されない対策を、事業用電気通信回線設備が具備することが望ましい。
2	自動再発信を行う端末の発信回数制限	0AB-J_IP電話端末は、アナログ電話端末等と同様に、自動再発信を行なう場合（自動再発信の回数が十五回以内の場合を除く）、その回数は最初の発信から三分間に二回以内とする機能を具備すること。	端末の自動再発信機能の濫用によるネットワーク輻輳の発生などの影響を低減させるため、0AB-J_IP電話端末についても、アナログ電話端末等と同様に、自動再発信の回数を制限する機能を具備することが望ましい。
3	ユーザネットワーク及び相互接続網との間の不正アクセス等の流入／流出の対策	不正アクセス等に対し、通信の緊急遮断等の対応措置が事業者により適切に行なわれるための基準等を明示するようなガイドラインの策定などが望ましい。	ユーザネットワークや相互接続網からの不正アクセスに対し、網設備の可用性確保や他ユーザに対する迷惑行為の防止の目的で、攻撃の発信源となっているユーザ等からの通信の緊急遮断等の対応措置が事業者により適切に行なわれるよう、基準等を明確化する必要がある。
4	端末のソフトウェア/ファームウェア更新機能	0AB-J_IP電話端末は、その端末のソフトウェアに脆弱性が発見された場合は、それを修復するための更新機能を具備すること。	ソフトウェアの脆弱性のある端末を悪用した攻撃等により、網設備や他ユーザに対して悪影響を及ぼすことを防ぐために、脆弱性のあるソフトウェアを早期に修復するためのソフトウェア更新等の機能が端末に具備されることが望ましい。

1. 発信者番号偽装対策

検討項目	安全性　ー　個人認証・個人情報　ー　発信者番号偽装対策

技術的条件（案）	電気通信事業者は、0AB-J_IP電話端末からの発信者番号の正当性の検証を行い、正当でない発信者番号が検出された場合は、発信者番号を無効にする等の措置を講ずること。

必要性	発信者の電気通信番号の正当性を担保することについての社会的な重要性が高まっていることから、自網のユーザが発信者番号を偽って発信ができないようにすることなどの、発信者番号を偽装されない対策を、事業用電気通信回線設備が具備することが望ましい。 （現状の対策） ・携帯電話・一般家庭の固定電話に対して、警察や自宅などの電話番号を偽って表示させ（発信者番号偽装表示）、相手を信用させた上で「振り込め詐欺」などの行為に及ぶ事件が発生し、社会問題化した。 ・このような発信者番号偽装表示の問題については、TCAが「発信者番号偽装表示ガイドライン」を制定し、電気通信事業者がガイドラインを遵守することで、対策がなされている。 （発信者番号偽装に係る課題） ・昨今、転送電話サービス等を悪用し、ヤミ金業者が、電話の発信元を匿名化して、取り締まりや摘発を困難にしている事例が発生しているとの報道がある等、発信者番号表示の信頼性を損なうような事件も再び起きている。 ・平成18年1月に改正交付（施行は平成19年4月1日）された事業用電気通信設備規則においては、緊急通報の要件として、発信者番号を緊急通報の受理機関（警察、消防等）に通知する機能を具備することとされた。

現状の規定等	・TCA発信者番号偽装表示対策ガイドライン（平成17年6月制定） ・TTC標準（JJ-90.22 発信者番号の取扱い、JJ-90.21 発アドレス偽装等の対策）

留意点等	・端末に付与されている電話番号以外に、例えば代表者番号やフリーフォン番号などが現在は発信者番号として表示されているが、これらの番号は、正当性が確認され表示されていることから認めるべき。どのような番号が発信者番号として認められるかについて一定の整理が必要

2. 自動再発信を行う端末の発信回数制限

検討項目	安全性 － サイバー攻撃対策 － 端末における発信の規制
技術的条件（案）	0AB-J_IP電話端末は、アナログ電話端末等と同等に、自動再発信を行なう場合（自動再発信の回数が十五回以内の場合を除く）、その回数は最初の発信から三分間に二回以内（最初の発信から三分を超えて行なわれる発信は別の発信とみなす）とする機能を具備すること。
必要性	自動再発信機能による発信を高頻度に繰り返し行なった場合の、ネットワーク輻輳の発生などの影響を低減させるため、0AB-J_IP電話端末についても、アナログ電話端末等と同様に、自動再発信の回数を制限する機能を具備することが望ましい。 （現状の対策） ・自動再発信機能を有する端末は、ユーザにとって相手先への接続性を高めるため便利である一方で、高頻度に発信を繰り返すと、通話中等により接続できない呼（無効呼）の発生を増大させ、網設備に対して無用な負荷がかかり、輻輳を発生させるなどのネットワークへの悪影響を及ぼす恐れがある。 ・このため、アナログ電話端末やISDN端末では、現在、端末設備等規則において、自動再発信の回数を3分間に2回以内とすると定められており、端末機器がこの規定を遵守することで、自動再発信機能によるネットワークへの影響を低減してきた。 （0AB-J_IP電話端末における自動再発信回数制限の必要性） ・0AB-J_IP電話端末においても、自動再発信機能による発信を高頻度に繰り返し行なった場合には、アナログ電話等と同様に、ネットワークへの影響を及ぼす恐れがある。
現状の規定等	[端末設備等規則]　第11条 （発信の機能） 三　自動再発信（応答のない相手に対し引き続いて繰り返し自動的に行なう発信をいう。以下同じ。）を行なう場合（自動再発信の回数が十五回以内の場合を除く。）にあつては、その回数は最初の発信から三分間に二回以内であること。この場合において、最初の発信から三分を超えて行なわれる発信は、別の発信とみなす。
留意点等	・本機能については、業界での標準化を図るなどしながら、端末への機能実装の普及促進を図ることが必要

3. ユーザネットワーク及び相互接続網との間の不正アクセス等の流入／流出の対策

検討項目	安全性　－　サイバー攻撃対策　－　緊急遮断
技術的条件（案）	ユーザネットワークや相互接続網からの不正アクセスが発生した場合において、通信の緊急遮断等の対応措置が事業者により適切に行なわれるための基準等を明示するようなガイドラインの策定などが望ましい。
必要性	ユーザネットワークや相互接続網からの不正アクセスに対し、網設備の可用性確保や他ユーザに対する迷惑行為の防止の目的で、攻撃の発信源となっているユーザ等からの通信の一時的遮断等の対応措置が事業者により適切に行なわれるよう、緊急遮断を行える基準等を明確化する必要がある。 （現状の対策） ・ユーザネットワークや相互接続網からの不正アクセスへの対策に関する技術的条件は、事業用電気通信設備規則に「事業用電気通信回線設備の防護措置」「異常輻輳対策」として定められている。 （事業者が緊急遮断を行うための課題） ・事業用電気通信設備規則に基づく対策を講じていたとしても、同時大量に不正アクセスなどが行われた場合には、ネットワーク設備に対して無用な負荷がかかり、影響を及ぼす恐れがある。 ・この様な場合には、不正アクセスの発生元となっている利用者などからの通信を緊急遮断する事が有効であるが、どの様な理由であれば「緊急遮断」を行えるかに関する基準等は現状明確になっていない。 ・不正アクセスに対する緊急遮断実施のための技術的な方法については、事業者の網設備やサービスの条件により多岐にわたると考えられるため、特に規定にするものではない。
現状の規定等	[事業用電気通信設備規則] ・第6条　事業用電気通信回線設備の防護措置 ・第8条　異常ふくそう対策
留意点等	・緊急遮断を行うための基準等としては、緊急遮断の対象となる攻撃通信の種別・形態や、事業者として許される措置の範囲、措置実施の運用条件（約款の規定等）が考えられる。

4. 端末のソフトウェア／ファームウェア更新機能

検討項目	安全性 － 端末機器 － 端末のソフトウェア／ファームウェア更新機能
技術的条件（案）	0AB-J_IP電話端末は、その端末のソフトウェアに脆弱性が発見された場合は、それを修復するための更新機能を具備すること。
必要性	ソフトウェアの脆弱性のある端末を悪用した攻撃等により、網設備や他ユーザに対して悪影響を及ぼすことを防ぐために、脆弱性のあるソフトウェアを早期に修復するためのソフトウェア更新等の機能が端末に具備されることが望ましい。 （端末の脆弱性に係る課題） ・昨今、インターネットに接続する機器等においては、ソフトウェアの脆弱性が発見され、また脆弱性に関する情報が幅広く公開されるとともに、それらの脆弱性をついた攻撃が行なわれる事態が増えている。 ・ソフトウェアの脆弱性に対する攻撃では、例えば機器等が乗っ取られ、他ユーザへの不正アクセスの踏み台として使われたり、また、機器等に保管されている個人情報等が抜き取られ暴露されたりする等があり、これらは大きな社会的問題となっている。 ・電気通信設備につながる端末機器等については、ソフトウェア等の脆弱性が存在しないよう開発・試験時のチェックが行なわれているが、それでも脆弱性が残る可能性はある。 ・これらの脆弱性を放置すると場合によっては、端末機器が攻撃者に乗っ取られ、網設備等への攻撃に使われる可能性があり、例えばネットワーク接続や発信用の機能が異常な動作をさせられた場合、ネットワークに無効な呼を発生させるなどして、網設備や他ユーザに対して甚大な悪影響を及ぼす可能性がある。
現状の規定等	[電気通信事業法] 第52条 （端末設備の接続の技術基準） 2 前項の技術基準は、これにより次の事項が確保されるものとして定められなければならない。 一 電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること。 二 電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること。 三 電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界が明確であるようにすること。
留意点等	・本機能については、業界の標準化を図るなどしながら、端末への機能実装の普及促進を図ることが必要 ・技術基準適合確認後に機能を修復することについて、現行の「端末機器の技術基準適合認定に関する規則」に照らして問題ないことを確認することが必要

具体的な検討課題（1）

大項目	中項目	課題項目	検討内容
A.安全性	A.1 重要通信等の確保	A.1-1 緊急通報機能	・IP電話における緊急通報の機能要件
		A.1-2 重要通信の優先的取り扱い	・優先的に取り扱うべき重要通信の定義
		A.1-3 広域災害時における重要通信等の確保の対策	・事業者間で重要通信を優先的に取り扱うためのルール等
		A.1-4 輻輳対策	・様々な異常輻輳から網を守るために必要な機能要件
	A.2 個人認証・個人情報	A.2-1 発信者番号偽装対策	・発信者番号偽装への対策
		A.2-2 個人情報保護	・発信者情報や位置情報、その他利用者に係わる情報の保護対策
		A-2.3 逆探知	・発信者の特定等を実現するために必要なNW設備及び端末の要件
	A.3 サイバー攻撃対策	A.3-1 端末における発信の規制	・自動再発信を行う端末の発信回数制限 ・REGISTER呼の集中を防止するための端末の機能要件 ・SPIT (Spam over Internet Telephony)やワン切りなどの攻撃を防止するための端末の機能要件
		A.3-2 緊急遮断	・ユーザネットワーク及び相互接続網との間の不正アクセス等の流入／流出の対策 ・不正アクセス等の原因および実施者の特定
		A.3-3 通信の盗聴	・通信の秘密を保護する対策
		A.3-4 SIPと連動しない音声通信流通の制限	・音声サービスにおけるP2P等を利用した電話端末への直接通信の扱い（迷惑行為への対応） ・一般的なP2P等通信の扱い
	A.4 端末機器	A.4-1 端末のソフトウェア／ファームウェア更新機能	・端末のソフトウェアの脆弱性に対する対策

具体的な検討課題（2）

大項目	中項目	課題項目	検討内容
S.信頼性	S.1 設備障害等	S.1-1 障害箇所の特定等	・IPネットワーク上での障害箇所の特定
		S.1-2 設備の損壊・故障および通信路の途絶に対する対策	・IPネットワーク上で、設備の損壊・故障があった場合の予備機器への切り替えや、伝送路の複数経路化の在り方 ・障害の波及防止のための措置
		S.1-3 端末の停電対策	・端末のバッテリー搭載等停電対策の考え方整理
	S.2 広域災害	S.2-1 緊急対応体制・事業者間の情報連絡方法	・広域災害時に各社が取るべき緊急対応体制の在り方と、会社間での情報連絡方法の取り決め
		S.2-2 音声通信の優先	・他のIP通信に対して音声通信を優先させることの是非、仕組み

A. 1−1 緊急通報機能

検討課題

A. 1 重要通信等の確保
A. 1−1 緊急通報機能

検討の方針

●ＩＰ電話における緊急通報の機能要件
ー情報通信審議会答申「ＩＰネットワークにおける緊急通報等重要通信の確保方策」をベースにＩＰ電話における緊急通報の実現を検討する。

現状の規定等

●ＩＰ電話における緊急通報の機能要件
・総務省令「事業用電気通信設備規則の一部を改正する省令」（H18.1.5公布） 緊急通報を扱う事業用電気通信回線設備
・情報通信審議会答申「ＩＰネットワークにおける緊急通報等重要通信の確保方策」（H17.3.30発表）

素案

●ＩＰ電話における緊急通報の機能要件
・IP電話における緊急通報に対する要件は、PSTNの機能を踏襲する方向で、情報通信審議会答申「ＩＰネットワークにおける緊急通報等重要通信の確保方策」がなされており、IP電話からの緊急通報の確保方策について具体的な実現方法も検討されていることから、この答申内容をベースにIP電話における緊急通報を実現するのが適当である。
・なお、同答申における緊急通報の要件については、総務省令「事業用電気通信設備規則の一部を改正する省令」（H18.1.5公布） にて事業用電気通信設備規則に盛り込まれる（H19.4.1施行）

（参考）同答申ではＩＰ電話からの緊急通報について、１）発信場所を管轄する指示台への接続、２）回線保留、３）電話番号通知・取得、４）位置番号通知・取得、５）優先的取扱い、６）なりすまし防止、の６つの機能要件を整理している。提示されている技術条件はＩＰ－ＰＳＴＮ接続が前提であり、緊急通報受理機関（指示台）はＰＳＴＮ側に接続にされる（指示台のＩＰ電話接続については将来課題の位置づけ）。

課題の方向性

Ａ：現行の技術的条件等を踏襲

A．1―2　重要通信の優先的取扱い　No.2

検討課題

A．１　重要通信等の確保
　A．１－２　重要通信の優先的取扱い

検討の方針

●優先的に取り扱うべき重要通信の定義
ー事業法及び施行規則で定められた重要通信の定義をベースに検討する。

現状の規定等

●優先的に取り扱うべき重要通信の定義
（電気通信事業法）
・第8条（重要通信の確保）事業者は、災害の予防若しくは救援、交通、通信、若しくは電力の供給確保等のため必要な通信を優先的に取り扱わなくてはならない
（電気通信事業法施行規則）
・第５５条（緊急に行うことを要する通信）事業法第８条で定める重要通信は次の通り：人命安全に関わる事項、治安維持に関わる事項、選挙執行、災害報道、気象情報の報告連絡、水道・ガスなどのライフライン用の通信

素案

●優先的に取り扱うべき重要通信の定義
・電気通信は社会のライフラインとしての役割を担っていることから、重要通信の優先的な取り扱いについては、現行、電気通信事業法で全ての電気通信事業者に対して課せられている責務であり、その優先的取扱いを要する通信は、事業法施行規則に定められているところである。
・今後IP化されたネットワークのOAB-J_IP電話においても、社会のライフラインとしての重要性は何ら変わることがないことから、引き続き、この現行の規定を踏襲することが適当である。

課題の方向性

Ａ：現行の技術的条件等を踏襲

A. 1－3　広域災害時における重要通信等の確保の対策　No.3

検討課題

A. 1　重要通信等の確保
　A. 1－3　広域災害時における重要通信等の確保の対策

検討の方針

●事業者間で重要通信を優先的に取り扱うためのルール等

－電気通信事業法施行規則で定められた重要通信を優先的に取り扱うためのルールについて検討する。

－事業者間での運用ルールの確認や、優先呼／一般呼の識別方法、優先接続手順について検討する。

現状の規定等

●事業者間で重要通信を優先的に取り扱うためのルール等

（電気通信事業法施行規則）

・第５６条の２（事業者間取り決め）次の事項を事業者間で取り決める：１）他の通信を制限・停止すること、２）重要通信の取扱いを一時的に停止する際の通知、３）重要通信に付与された信号を識別した際の優先的取扱い

・JJ-90.10　付録B「相互接続事業者間の服装制御方式」
「発ユーザ種別」に基づく「優先発ユーザ回線留保機能及び両方向回線留保機能」による制御。

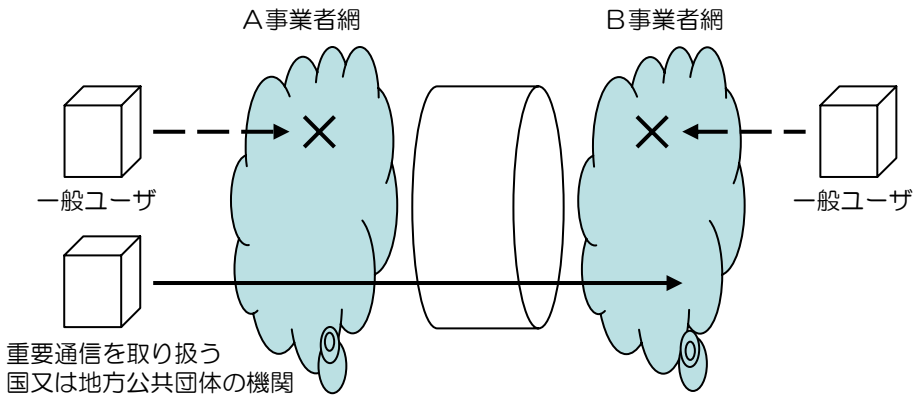
素案

●事業者間で重要通信を優先的に取り扱うためのルール等

・電気通信事業法施行規則で定められた重要通信を優先的に取り扱うための事業者間の取り決めのルールについては、今後のIPネットワークにおいても必要性等に変わりがないことから、踏襲することが望ましい。

・事業者は、JJ-90.10　付録B「相互接続事業者間の輻輳制御方式」をベースにSIP信号においても優先接続手順を検討し、更に事業者間で「保守確認事項」により運用ルールを確認するのが適当である。

・SIP信号上での優先呼／一般呼の識別方法、優先接続手順については、相互接続・運用性SWGの検討結果に従う。



課題の方向性

（事業者間のルール）Ａ：現行の技術的条件等を踏襲
（具体的な取決め）　Ｂ：ＴＴＣ標準化

検討課題

A．１　重要通信等の確保
A．１－４　輻輳対策

検討の方針

●様々な異常輻輳から網を守るために必要な機能要件

－異常輻輳から網を守るための対策について、現状の規定である設備規則第８条、第２２条をベースに検討する。

現状の規定等

●様々な異常輻輳から網を守るために必要な機能要件

（事業用電気通信設備規則）

・第８条（異常ふくそう対策）交換設備は、異常ふくそうが発生した場合に、これを検出し、通信の集中を規制する機能等を具備すること。

・第２２条（異常ふくそう対策）他の事業者の設備を接続する交換設備は、異常ふくそうの派生による他の事業者に対して重大な支障を及ぼすことのないよう、直ちに発生を検出し、通信の集中を規制する機能等を具備すること。

素案

●様々な異常輻輳から網を守るために必要な機能要件

・従来から発生しているネットワークの輻輳には、地震等の発生に伴って被災した地域内の通信または被災地と他の地域との間の通信が集中して発生するもの（いわゆる「災害時輻輳」）と、特定の催し物のチケットの電話予約等に伴って発生するもの（いわゆる「企画型輻輳」）とがある。

・これらの輻輳は通話を目的とした発信の集中であるため、必要な期間、通信規制をかけることで網を守ることが可能である。このため、事業者は設備規則第８条の規定に従い、交換設備において通信規制の機能を具備している。また、輻輳の波及防止のため、事業者間の接続においては、設備規則第２２条の規定に従い、輻輳を検知し、また通信規制する機能を具備している。

・災害時輻輳や企画型輻輳などの異常輻輳から網を守るためには、OAB-J_IP電話についても、PSTNと同様に、異常ふくそうの検知や通信規制を行なうべきであり、現行の技術的条件を踏襲することが適当である。

検討の方向性

Ａ：現行の技術的条件等を踏襲

A. 2―1　発信者番号偽装対策　No.5

検討課題

A．２　個人認証・個人情報
　A．２－１　発信者番号偽装対策

検討の方針

●発信者番号偽装への対策

―発信者番号偽装への対策について、ＴＣＡ発信者番号偽装表示対策ガイドラインをベースに、今後のIP化において事業用電気通信回線設備で求められる技術的条件について検討する。

現状の規定等

●発信者番号偽装への対策

・ＴＣＡ発信者番号偽装表示対策ガイドライン（平成１７年６月制定）
・JJ-90.22 発信者番号の取扱い
・JJ-90.21 発アドレス偽装等の対策

素案

●発信者番号偽装への対策

・携帯電話・一般家庭の固定電話に対して、警察や自宅などの電話番号を偽って表示させ（発信者番号偽装表示）、相手を信用させた上で「振り込め詐欺」などの行為に及ぶ事件が発生し、社会問題化した。
・このような発信者番号偽装表示の問題については、ＴＣＡが「発信者番号偽装表示ガイドライン」を制定し、電気通信事業者がガイドラインを遵守することで、対策がなされている。　・発信者番号偽装表示の問題については、ＴＣＡが「発信者番号偽装表示ガイドライン」を制定）し、会員事業者がガイドラインを遵守することで、対策がなされている。
・昨今、転送電話サービス等を悪用し、ヤミ金業者が、電話の発信元を匿名化して、取り締まりや摘発を困難にしている事例が発生しているとの報道がある等、発信者番号表示の信頼性を損なうような事件も再び起きている。
・平成１８年１月に改正交付（施行は平成１９年４月１日）された事業用電気通信設備規則においては、緊急通報の要件として、発信者番号を緊急通報の受理機関（警察、消防等）に通知する機能を具備することとされた。
・このように、発信者の電気通信番号の正当性を担保することについての社会的な重要性が高まっていることから、自網のユーザが発信者番号を偽って発信ができないようにすることなどの、発信者番号を偽装されない対策を、事業用電気通信回線設備が具備することが望ましい。
・なお、端末に付与されている電話番号以外に、例えば代表者番号やフリーフォン番号などが現在は発信者番号として表示されているが、これらの番号は、正当性が確認され表示されていることから認めるべき。どのような番号が発信者番号として認められるかについて一定の整理が必要である。

課題の方向性

Ａ：新たな技術的条件として提案

検討課題

A．２　個人認証・個人情報
　A．２－２　個人情報保護

検討の方針

●発信者情報や位置情報、その他利用者に係わる情報の保護対策

ー個人情報保護法や、電気通信事業における個人情報に関する保護ガイドラインをベースに、事業者における個人情報の適切な管理・取扱いの在り方について検討する。

現状の規定等

●発信者情報や位置情報、その他利用者に係わる情報の保護対策

・個人情報の保護に関する法律（個人情報保護法）
・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

素案

●発信者情報や位置情報、その他利用者に係わる情報の保護対策

・「個人情報保護法」や「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」に従い、事業者は保管する個人情報の適切な管理・取扱いを実施するのが適当である。

課題の方向性

Ａ：現行の技術的条件等を踏襲

検討課題

A．２　個人認証・個人情報
A．２－３　逆探知

検討の方針

●発信者の特定等を実現するために必要なNW設備及び端末の要件
－OAB-J IP電話における発信者位置の特定は、発信者番号より可能であり、IP化されたネットワークでも同様に発信者番号の特定は可能である。
－発信者位置特定に関する技術的条件の必要性について検討が必要である。

現状の規定等

●発信者の特定等を実現するために必要なNW設備及び端末の要件
（特になし）

素案

●発信者の特定等を実現するために必要なNW設備及び端末の要件
・OAB-J_IP電話における発信者位置の特定は、発信者番号より可能であり、IP化されたネットワークでも同様に発信者番号の特定は可能である。
・現在、発信者位置特定に関する技術的条件は定められていないが、各電気通信事業者は司法当局などからの求めに応じ対応しているところであり、今後の社会的動向をみながら検討することが望ましい。

課題の方向性

C：今後の課題

A．3－1　端末における発信の規制

検討課題

A．３　サイバー攻撃対策
　A．３－１　端末における発信の規制

検討の方針

●自動再発信を行う端末の発信回数制限
－ＩＰ電話端末における自動再発信回数制限については、アナログ電話端末と同等の機能を盛り込む等の対策について検討する。
●REGISTER呼の集中を防止するための端末の機能要件
－網が端末の登録（REGISTER）を受付できない場合に、端末が再登録要求の送信タイミング調整を行なう等の対策について検討する。
●SPITやワン切りなどの攻撃を防止するための端末の機能要件
－SPIT攻撃やワン切の発生を抑止するための対策について検討する。

現状の規定等

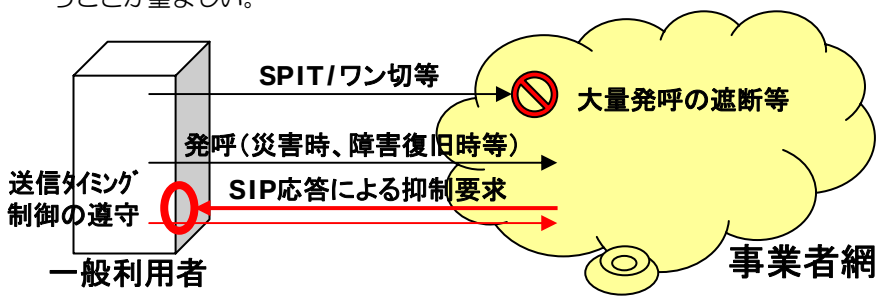
●自動再発信を行う端末の発信回数制限
・端末設備等規則第１１条第３号　自動再発信を行う場合（自動再発信の回数が十五回以内の場合を除く。）にあっては、その回数は最初の発信から三分間に二回以内であること。
●REGISTER呼の集中を防止するための端末の機能要件
・端末設備等規則第１９条～２１条　送信タイミング制御機能（移動端末の場合）
・JJ-90.24 端末の輻輳制御機能等
●SPITやワン切りなどの攻撃を防止するための端末の機能要件
・有線電気通信法第13条の２　ワン切等を行った事業者に対する罰則等
・「迷惑通信への対応のあり方に関する研究会」報告書（H14.10）
・事業用電気通信設備等委員会報告書(H15.9)　参考：電気通信における輻輳を防止するために主に端末機器が具備すべき機能要件

素案

●自動再発信を行う端末の発信回数制限
・自動再発信機能を有する端末は、ユーザにとって相手先への接続性を高めるため便利である一方で、高頻度に発信を繰り返すと、通話中等により接続できない呼（無効呼）の発生を増大させ、ネットワーク設備に対して無用な負荷がかかり、輻輳を発生させるなどのネットワークへの影響を及ぼす恐れがある。
・OAB-J_IP電話についても、アナログ電話端末と同様に自動再発信の回数を制限する機能を盛り込むことが望ましい。
・本機能については、業界での標準化を図るなどしながら、端末への機能実装の普及促進を図ることが必要である。

●REGISTER呼の集中を防止するための端末の機能要件
・網が端末の登録（REGISTER）を受付できない場合に、端末がREGISTER呼の送信タイミングを調整することにより、ネットワーク輻輳を抑止するような対策を行なうことが適当である（品質・機能ＳＷＧの検討結果による）。

●SPITやワン切りなどの攻撃を防止するための端末の機能要件
・端末のワン切によるネットワーク輻輳への対応については、現行、有線電気通信法に罰則が制度として定められているが、技術的条件としては定められていない
・今後、SPITやワン切による攻撃がさらなる脅威として顕在化した場合は、例えば罰則規定の追加、異なる番号に対する連続した発信を規制するなどの検討を行なうことが望ましい。



課題の方向性

（自動再発信回数制限）　Ａ：新たな技術的条件として提案
（REGISTER呼集中防止）Ａ：新たな技術的条件として提案（品質・機能ＳＷＧの報告を参照）
（SPIT・ワン切対策）　　Ｃ：今後の検討

A. 3―2　緊急遮断

No.9

検討課題

A．３　サイバー攻撃対策
　A．３－２　緊急遮断

検討の方針

●ユーザネットワーク及び相互接続網との間の不正アクセス等の流入／流出の対策

ーユーザネットワーク及び相互接続網からの不正アクセス等への対策について、攻撃等が発生した場合の緊急遮断を含めて検討する。

●不正アクセス等の原因および実施者の特定

ー不正アクセス等が発生した場合に、その原因および実施者の特定のため、各事業者において保存すべき情報や、事業者間での情報の共有方法について検討する。

現状の規定等

●ユーザネットワーク及び相互接続網との間の不正アクセス等の流入／流出の対策

（事業用電気通信設備規則）

・第６条：事業用電気通信回線設備の防護措置（利用者又は他事業者から受信したプログラムにより事業者の意図に反する動作を禁止）

・第８条：異常ふくそう対策（通信の集中を規制する機能等を要求）

●不正アクセス等の原因および実施者の特定

・情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る行動計画」（H17.12.13決定）

素案

●ユーザネットワーク及び相互接続網との間の不正アクセス等の流入／流出の対策

・ユーザネットワークや相互接続網からの不正アクセスへの対策に関する技術的条件は、事業用電気通信設備規則に「事業用電気通信回線設備の防護措置」「異常輻輳対策」として定められている。

・しかしながら、これらの対策を講じていたとしても、同時大量に不正アクセスなどが行われた場合には、ネットワーク設備に対して無用な負荷がかかり、影響を及ぼす恐れがある。この様な場合には、不正アクセスの発生元となっている利用者などからの通信を緊急遮断する事が有効であるが、どの様な理由であれば「緊急遮断」を行えるかに関する基準等は現状明確になっていない。

・そこで、ユーザネットワークや相互接続網からの不正アクセスに対し、ネットワーク設備の可用性確保や他ユーザに対する迷惑行為の防止の目的で、攻撃の発信源となっているユーザ等からの通信の一時的遮断等の対応措置が事業者により適切に行われるよう、緊急遮断を行える基準等を明確化する必要がある。

・不正アクセスに対する緊急遮断実施のための技術的な方法については、事業者の網設備やサービスの条件により多岐にわたると考えられるため、特に規定にするものではないが、上記の基準等を明示するようなガイドラインの策定などが望ましい。

・なお、これらの基準等としては、緊急遮断の対象となる攻撃通信の種別・形態や、事業者として許される措置の範囲、措置実施の運用条件（約款の規定等）が考えられる。

●不正アクセス等の原因および実施者の特定

・不正アクセス等が発生した場合に、その原因および実施者の特定のため、各事業者において保存すべき情報や、事業者間での情報の共有方法については、政府を中心に検討が進められている重要インフラの情報セキュリティ対策に検討結果等を踏まえ、必要に応じて検討することが適当である。

・なお、電気通信分野における情報共有・分析を行うCEPTOAR (Capability of Engineering of Protection, Technical Operation, Analysis and Response)の検討については、電気通信事業者の協議会である「電気通信分野における情報セキュリティ対策協議会」（H18.4発足）で、H１８年度末を完了目途に進められる予定である。

課題の方向性

Ａ：新たな技術的条件として提案

検討課題

A．３　サイバー攻撃対策
　A．３－３　通信の盗聴

検討の方針

●通信の秘密を保護する対策

－事業者の電気通信設備内、及び利用者との接続点(UNI)からの情報漏洩リスク：通信の秘密の保護について、現行の技術的条件等をベースに検討する。

－他事業者との接続点(NNI)からの情報漏洩リスク：事業者間のルール等による通信の秘密の保護対策について検討する。

現状の規定等

●通信の秘密を保護する対策

（事業用電気通信設備規則）

・第１７条（通信内容の秘匿）UNIにて他の通信の内容が電気通信設備の通常の使用の状態で判読できないように必要な措置が必要

・第１８条（蓄積情報保護）利用者の通信の内容等を回線設備に蓄積する場合は、当該利用者以外のものが情報を知得し、又は破壊することを防止するため、識別符号の照合確認等の防止措置を行う。

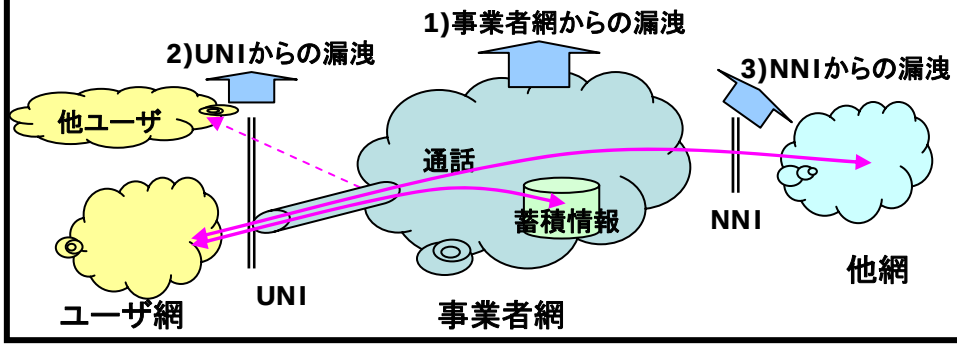
素案

●通信の秘密を保護する対策

・通信の秘密の保護対象としては、通信の内容及び蓄積された通信内容とそれに関わる情報、を考える（現状の設備規則の通り）。漏洩リスクの発生場所として、１）事業者設備内、２）利用者との接続点(UNI)、３）他事業者との接続点(NNI)、の3つを想定する。

・事業者の電気通信設備内、及び、利用者との接続点(UNI)における情報漏洩リスク
OAB-J_IP電話においても、現状の設備規則第１７条（通信内容の秘匿措置）、１８条（蓄積情報保護）に基づき、各事業者が必要な対策を実施することが適当。

・他事業者との接続点(NNI)における情報漏洩リスク
他事業者との接続点や接続回線において通信の秘密が漏洩しないよう、事業者間のルール等による通信の秘密の保護対策の在り方を検討するのが適当。



検討の方向性

（通信の秘密の対策）Ａ：現行の技術的条件等を踏襲
（他事業者との接続点における対策）　Ｃ：今後の検討

A. 3－4　SIPと連動しない音声通信流通の制限　No.11

検討課題

A. ３　サイバー攻撃対策
　A. ３－４　ＳＩＰと連動しない音声通信流通の制限

検討の方針

●音声サービスにおけるＰ２Ｐ等を利用した電話端末への直接通信の扱い（迷惑行為への対応）
－Ｐ２Ｐでユーザに直接音声通信を大量に送りつける迷惑行為についての対策について検討する。

●一般的なＰ２Ｐ等通信の扱い
－Ｐ２Ｐ通信の許可・非許可の扱いや利用制限の扱いについて検討する。

現状の規定等

●音声サービスにおけるＰ２Ｐ等を利用した電話端末への直接通信の扱い（迷惑行為への対応）
（特になし）

●一般的なＰ２Ｐ等通信の扱い
（特になし）

素案

●音声サービスにおけるＰ２Ｐ等を利用した電話端末への直接通信の扱い（迷惑行為への対応）
・今後のIP化されたネットワークでは、Ｐ２Ｐでユーザに直接音声通信を大量に送りつける迷惑行為を行なうことも考えられる。
・これら迷惑行為については、端末にＰ２Ｐによる音声通信を拒否する機能を盛り込むなどの対策が考えられるが、それらの対策は現在は、利用者の判断に委ねるべきである。
・今後、このような迷惑行為が顕在化し、その防止機能の社会的必要性が高まった場合は、検討することが望ましい。

●一般的なＰ２Ｐ等通信の扱い
・Ｐ２Ｐ通信の許可・非許可の扱いや利用制限の扱いについては、社会的動向を見ながら検討することが望ましい。

課題の方向性

（音声サービスにおけるＰ２Ｐ等による迷惑行為対策）Ｃ：今後の課題
（一般的なＰ２Ｐ等通信の扱い）　Ｃ：今後の課題

検討課題

Ａ．４　端末機器
　Ａ．４－１　端末のソフトウェア／ファームウェア更新機能

検討の方針

●端末のソフトウェアの脆弱性に対する対策
－セキュリティ問題（脆弱性）のある端末を悪用した攻撃等により、網や他ユーザに対して甚大な悪影響を及ぼすことを防ぐため、端末に対して、ソフトウェア更新を行なう機能の導入を検討する。

現状の規定等

●端末のソフトウェアの脆弱性に対する対策
（特になし）

素案

●端末のソフトウェアの脆弱性に対する対策
・昨今、インターネットに接続する機器等においては、ソフトウェアの脆弱性が発見され、また脆弱性に関する情報が幅広く公開されるとともに、それらの脆弱性をついた攻撃が行なわれる事態が増えている。
・ソフトウェアの脆弱性に対する攻撃では、例えば機器等が乗っ取られ、他ユーザへの不正アクセスの踏み台として使われたり、また、機器等に保管されている個人情報等が抜き取られ暴露されたりする等があり、これらは大きな社会的問題となっている。
・電気通信設備につながる端末機器等については、ソフトウェア等の脆弱性が存在しないよう開発・試験時のチェックが行なわれているが、それでも脆弱性が残る可能性はある。
・これらの脆弱性を放置すると場合によっては、端末機器が攻撃者に乗っ取られ、網設備等への攻撃に使われる可能性があり、例えばネットワーク接続や発信用の機能が異常な動作をさせられた場合、ネットワークに無効な呼を発生させるなどして、網設備や他ユーザに対して甚大な悪影響を及ぼす可能性がある。
・よって、ソフトウェアの脆弱性のある端末を悪用した攻撃等により、網設備や他ユーザに対して悪影響を及ぼすことを防ぐために、脆弱性のあるソフトウェアを早期に修復するためのソフトウェア更新等の機能が端末に具備されることが望ましい。
・本機能については、業界の標準化を図るなどしながら、端末への機能実装の普及促進を図ることが必要である。
・技術基準適合確認後に機能を修復することについて、現行の「端末機器の技術基準適合認定に関する規則」に照らして問題ないことを確認する必要がある。

課題の方向性

Ａ：新たな技術的条件として提案

検討課題

S．１　設備障害等
　S．１ー１　障害箇所の特定等

検討の方針

●ＩＰネットワーク上での障害箇所の特定
ー現状の技術的条件である事業用電気通信設備規則の「故障検出」をベースに、IPネットワーク上における障害箇所の特定等の在り方について検討する。

現状の規定等

●ＩＰネットワーク上での障害箇所の特定
（事業用電気通信設備規則）
・第５条（故障検出）　電気通信役務の提供に重大な支障を及ぼす故障等の発生時に、これを直ちに検知し、通知する機能の具備が必要

素案

●ＩＰネットワーク上での障害箇所の特定
・事業用電気通信設備規則の第５条故障検出に、故障を直ちに検出し、保守者に通信する機能を具備することが定められている。
・今後IP化されたネットワークの0AB-J_IP電話においても、引き続き、この現行の規定を踏襲することが適当である。

課題の方向性

Ａ：現行の技術的条件等を踏襲

S．1―2　設備の損壊･故障および通信路の途絶に対する対策　No.14

検討課題

S．１　設備障害等
　S．１－2　設備の損壊・故障および通信路の途絶に対する対策

検討の方針

●ＩＰネットワーク上で、設備の損壊・故障があった場合の予備機器への切替えや、伝送路の複数経路化の在り方

－現状の技術的条件である事業用電気通信設備規則の「予備機器等」及び「試験機器及び応急復旧機材の配備等」をベースに、予備機器への切り替えや、伝送路の複数経路化の在り方について検討する。

●障害の波及防止のための措置

－障害が発生した場合の他事業者への障害の波及防止を目的とした、故障連絡や障害の切り分け、回線の閉塞などの措置について検討する。

現状の規定等

●ＩＰネットワーク上で、設備の損壊・故障があった場合の予備機器への切替えや、伝送路の複数経路化の在り方

（事業用電気通信設備規則）

・第４条（予備機器等）故障時等の切り替えのため、機器を代替できる予備機器の設置・配備が必要。設備をつなぐ伝送路設備は複数の経路により設置されることが必要

・第７条（試験機器及び応急復旧機材の配備）故障等が発生した場合における応急復旧工事、臨時の電気通信回線の設置、電力の供給その他の応急復旧措置を行うために必要な機材の配備等が必要

●障害の波及防止のための措置

・JT-Q764等：故障発生、回線通知手順等の規定

素案

●ＩＰネットワーク上で、設備の損壊・故障があった場合の予備機器への切替えや、伝送路の複数経路化の在り方

・障害対策のための予備機器への切り替えや、伝送路の在り方については、現在、事業用電気通信設備規則に「予備機器等」「試験機器及び応急復旧機材の配備」として定められている。

・今後IP化されたネットワークのOAB-J_IP電話においても、引き続き、これらの現行の規定を踏襲することが適当である。

●障害の波及防止のための措置

・障害が発生した場合の他事業者への障害の波及防止を目的として、故障連絡や障害の切り分け、回線の閉塞などの措置は、相互接続した事業者間の合意に基づき行なわれているところである。

・今後のIP化されたネットワークのOAB-J_IP電話においても、現行の事業者間の合意に基づく取決めによることが適当である。

課題の方向性

（予備機器への切り替え・伝送路の在り方）Ａ：現行の技術的条件等を踏襲
（障害の波及防止のための措置）　Ｂ：事業者間の取決め

検討課題

S．１　設備障害等
　S．１－３　端末の停電対策

検討の方針

●端末のバッテリー搭載等停電対策の考え方整理
－OAB-J_IP電話における停電対策として、端末へのバッテリー搭載などの対策を実施することについて検討する。

現状の規定等

●端末のバッテリー搭載等停電対策の考え方整理
・設備規則第２７条　端末への電源供給（アナログ電話設備）

素案

●端末のバッテリー搭載等停電対策の考え方整理
・端末への電源供給に関しては、現行、アナログ電話のみが事業用電気通信設備規則に「端末への電源供給」として技術的条件が定められているところであり、ISDNに関してはその定めはない。
・今後のIP化されたネットワークのOAB-J_IP電話では、端末へのバッテリー搭載による停電対策が考えられるが、それらの対策は利用者の判断に委ねるべきであり、今後、停電に対する対策への社会的必要性の動向をみながら検討することが望ましい。

課題の方向性

Ｃ：今後の課題

S．2―1　緊急対応体制･事業者間の情報連絡方法　No.16

検討課題

S．２　広域災害
　S．２－１　緊急対応体制・事業者間の情報連絡方法

検討の方針

●広域災害時に各社が取るべき緊急対応体制の在り方と、会社間での情報連絡方法の取り決め

－現行の防災関連の法制度を踏まえた、防災計画や緊急時の連絡体制の在り方について検討する。

現状の規定等

●広域災害時に各社が取るべき緊急対応体制の在り方と、会社間での情報連絡方法の取り決め

・災害対策基本法
・大規模地震対策特別措置法
・武力攻撃事態等における国民の保護のための措置に関する法律

素案

●広域災害時に各社が取るべき緊急対応体制の在り方と、会社間での情報連絡方法の取り決め

・広域災害に対しては、「災害対策基本法」「大規模地震対策特別措置法」「武力攻撃事態における国民の保護のための措置に関する法律」などの関連法令を元に、防災計画や緊急時の連絡体制などの備えを図っている。
・また、広域災害発生時の連絡方法は、電話、FAXなどの様々な手段で行なっている。
・今後、これら連絡手段を統一的な方法で行なうなどの必要性が高まった場合は検討することが望ましい。

課題の方向性

Ｃ：今後の課題

検討課題

S．２　広域災害
　S．２－２　音声通信の優先

検討の方針

●他のＩＰ通信に対して音声通信を優先させることの是非、仕組み

－広域災害発生時に、重要通信以外の一般的な音声通信を他の通信に対して優先的に疎通させることの是非、仕組みについて検討する。

現状の規定等

●他のＩＰ通信に対して音声通信を優先させることの是非、仕組み

（特になし）

素案

●他のＩＰ通信に対して音声通信を優先させることの是非、仕組み

・被災地や周辺の住人の安否・状況等を確認し、連絡をとる方法として、現状、電話は最も一般的かつ効果的な手段である。そのため、災害時輻輳等に際して、電話による音声通信の疎通を出来るだけ確保することが、NWに対して期待されている。

・NWのIP統合網化にともない、音声通信を他のIP通信から優先させることは電話の疎通率を向上させる有効な手段になりうるが、どのIP通信に対して音声通信を優先させるかが課題となる。

・特に、重要インフラ分野と呼ばれる金融や航空に関わる企業・組織で使われる通信（IP通信の場合もあり）は、音声通信でなくても優先度が高く、電話の疎通確保の目的であっても何らかの支障を及ぼすことはできない

・よって、広域災害発生時に、重要通信以外の一般的な音声通信を他の通信に対して優先的に疎通させることについては、今後の社会的な動向を見ながら検討することが望ましい。

課題の方向性

Ｃ：今後の課題