資料安作３－８

安全・信頼性検討作業班アンケート実施要領

目　　的

近年、ネットワークのＩＰ化等の進展に伴い、通信障害の影響の大規模化、広域化、長時間化等、これまでの電話サービスの障害等とは異なる傾向が見受けられるようになってきている。

このような状況を踏まえ、電気通信サービスの安全・信頼性を向上させていくために、法令、ガイドライン等で一層取り組みが必要な事項や新たに取り組みが必要と考えられる事項をはじめとして、検討課題を幅広く提案いただき、本作業班における検討課題を抽出・整理することを目的として本アンケートを実施するものである。

対　　象

安全・信頼性検討作業班構成員を対象に実施

回答期間

平成１８年１１月１７日（金）

回 答 先

anzen@ml.soumu.go.jp

実施要領

昨今の急速な技術革新やネットワークのＩＰ化に対応して、電気通信サービスの安全・信頼性向上のために、新たに検討が必要と考えられる事項等（※）を、別添アンケート回答欄にご記入願います。

・同表の左側の欄に掲載されていない課題について、積極的に追加していただき、前広にご提案をお願いいたします。
・特に重点的又は早急に取り組むことが必要な事項については、項目に「(重要)」とご記入願います。
・回答欄には、プレゼンテーションでご発言いただいた事項等をもとに、例として記入しています。

なお、本アンケート表の中の、「取り組むべき課題」として挙げている７項目（大分類）は、「電気通信分野における情報セキュリティ確保に係る安全基準（第１版)」(電気通信分野における情報セキュリティ協議会　平成１８年９月２９日策定）の規定項目に基づき、「情報通信ネットワーク安全・信頼性基準」（昭和６２年郵政省告示第７３号）の観点を追加し作成しております。（参考資料１、２）

※　①法令やガイドライン等において策定することが必要と考えられる事項
　　②既に法令やガイドライン等で策定されているが改善が必要と考えられる事項
　　③その他、新たに取り組むことが必要と考えられる事項　　等

そ の 他

実施結果の公表：アンケート結果については、個別の事業者名、セキュリティ上問題が発生するおそれがあるもの、その他作業班主任が必要と認めるものについては公表しないこととする。

なお、必要により属性（固定電話事業者、携帯電話事業者の別等）等の情報は公表する場合がある。

別添

回答者：*総務省　電気通信技術システム課*

アンケート回答表（回答例）

取り組むべき課題（４本柱）			（回答欄）
（大項目）	（中項目）	（小項目）	ネットワークのＩＰ化等に伴い検討が必要と考える事項等
１．組織・体制の整備及び資源の確保 （万全なチェック体制） （迅速な連絡・対応体制）	•基本指針・情報セキュリティのための内部組織	• 基本指針の承認・公表・通知、レビュー、経営陣の責任の明確化等	•
	•人的資源のセキュリティ	• 教育・訓練の実施、違反者に対する懲戒手続きの整備等	• 主任技術者の位置付けが実態にそぐわない状況であり、抜本的な見直しが必要。 • 新たな技術やリスク管理等の対応を含めて、ネットワーク設備管理責任者などの育成が必要。 • スキルアップ支援、意識向上プログラムの実施。 • ネットワーク管理・運用者と設計者の連携が必要。 • 設定ミス、操作ミス等人為的なミスをなくすためのチェック体制の確立
	•サイバー攻撃対策	• セキュリティ事象等の報告に対する責任体制・手順の整備、監視・評価・管理の継続的改善の実施	•
	•ネットワーク輻輳対策	• ＮＷ輻輳対応責任者の設定、対応方針の策定	•
	•故障・災害等ＩＴ障害対策	• ＩＴ障害に対する緊急対応体制・計画書の整備	•
	•情報漏えい対策	• 重要情報管理体制及び方針	•

取り組むべき課題（４本柱）			（回答欄）
（大項目）	（中項目）	（小項目）	ネットワークのＩＰ化等に伴い検討が必要と考える事項等
２．情報セキュリティについての対策	• 情報システム、取扱情報に対する責任と情報の分類	• 資産目録作成、維持、利用の明確化、管理責任者の指定、情報の分類	•
	• サイバー攻撃対策	• サーバ等に格納された情報の管理	•
	• 情報漏えい対策	• 重要情報管理責任者の設定、重要情報の一覧整備、重要情報の格付け／取扱いルール	•

取り組むべき課題（４本柱）			（回答欄）
（大項目）	（中項目）	（小項目）	ネットワークのＩＰ化等に伴い検討が必要と考える事項等
３．情報セキュリティ要件の明確化に基づく対策	• ネットワークセキュリティ管理	• サービスの適切な維持管理、スパムメール対応	•
	• 利用者アクセスの管理	• 特権管理、利用者登録、パスワード管理等	•
	• ネットワークアクセス制御	• サービス利用方針、外部利用者認証	•
	• サーバ攻撃対策	• ネットワーク防護策、発信者身元偽装対策、利用者への注意喚起	•
	• ネットワーク輻輳対策	• ネットワーク輻輳検出・規制機能、企画等の事前情報収集、事前の通信規制措置、一時的な処理量向上のための措置、障害等誘発現象に対する事前情報収集	•
	• 重要通信の確保	• 重要通信取扱いの措置・識別・優先	•
	• 情報漏えい対策	• ユーザ認証、アクセス管理等、データアクセスに関わるログ取得・保管、データ不正アクセスの検知、ネットワーク上での不正行為の検知	•

取り組むべき課題（４本柱）			（回答欄）
（大項目）	（中項目）	（小項目）	ネットワークのＩＰ化等に伴い検討が必要と考える事項等
４．情報システムについての対策	・セキュリティを保つべき領域	・情報処理施設の物理的境界の確保、入退室管理	・
	・自社の管理外の場所に設置する設備のセキュリティ	・保護された場所への設置、自社設備の保護	・
	・システムの計画作成及び受け入れ （柔軟なネットワーク設計等）	・システム利用の監視・調整、容量・能力の予測	・ルータ等設備に対する品質基準指標（最低限の技術仕様）の策定が必要。 ・全事業者における共通品質指標の設定及び定期的情報交換の実施が必要。 ・各機器の十分な呼処理のマージン設計が必要。 ・ネットワークの最適配置の検討。 ・各機器（サーバ）等の事前機能確認等。
	・情報システムのセキュリティ要求事項／システムファイルのセキュリティ／開発及びサポートプロセスにおけるセキュリティ	・セキュリティ要求事項の特定・合意、ソフトウェア導入管理手順の整備、ソフトウェア変更管理手順の整備	・
	・監視	・故障検出、ルータ・サーバ等の監視機能の導入、動作ログ等の取得・保管	・ＩＰ化に伴い従来の設備と異なり、故障の認識ができない場合や予備設備への切り替えができない状況が発生していることから、ネットワークの早期異常検知機能等の設備監視技術の研究開発を早急に行うことが必要。

	• サイバー攻撃対策	• セキュリティパッチの適用、設備等に関する脆弱性情報の迅速入手	•
	• ネットワーク輻輳対策	• 通信トラヒック量等の定期的観測・分析、計画的な設備等の増強	•
	• 障害対策	• 予備機器の設置等、メーカ等での予備機器等の配備、応急復旧機材の配備、データ等の定常的バックアップ、ネットワーク経路の二重化、オペレーションセンタの分散化等、通信経路の迂回措置等、予備電源の設置等、風害・振動・雷害・火災等対策	• 広域停電、災害時におけるシステムの機能を確保するため、電力供給の確保や空調設備の機能維持の検討が必要。

特に重点的に取り組むべき事項			（回答欄）
（大項目）	（中項目）	（小項目）	ネットワークのＩＰ化等に伴い検討が必要と考える事項等
１．ＩＴ障害の観点から見た事業継続性確保のための対策	●事業継続管理における情報セキュリティの側面	●事業継続管理手続の策定・維持、事業継続リスクアセスメント、事業継続計画の策定・実施等	●
	●情報等の管理・障害検知・切り分け	●設備（ソフト・ハード）管理、再発防止管理、障害情報の管理、ＩＴ障害の検知・可視化、ＩＴ障害の切り分け手順等の整備	●ＩＰネットワークにおいて現在は、障害原因がハードとソフトかさえ明確にならない等、故障箇所の特定に長時間を要していることから、これらの問題を解決するための研究開発を促進することが必要。 ●システムの冗長機能の確実な確保が必要。
	●緊急時の情報連絡／ＩＴ障害対応の訓練・演習の計画・実施 （迅速な連絡・対応体制）	●ユーザ等からの通報窓口の設定等、社内エスカレーション手順等の整備、監督官庁への連絡等、ユーザ・関係者等への周知、ＩＴ障害に対応する訓練の実施、演習におけるメーカ等との協調	●事業者自ら行っている事故情報の公表について迅速性、掲示期間等が各社まちまちでありガイドラインが必要。 ●事業者間の連携促進のための情報交換の拡大や訓練実施が必要。 ●障害・事故の周知広報の徹底。現在は、利用者自らが電話の問い合わせや、HP で確認しない限り通常わからないといった苦情が多い。利用者が予め必要とした情報は様々な手段を使って確実かつ迅速に伝達する仕組みが必要。 ●重大な事故の報告基準、特に総務省告示第２４８号中伝送速度により事故の規模を判断している箇所の数値が実態とあっていないため改善が必要。
	●サイバー攻撃対策	●攻撃危険度レベル設定・対応フロー、サイバー攻撃への対応手順等	●

		の整備、通信トラヒックの緊急的制御、攻撃利用回線の一時停止、攻撃設備の縮退運転／一時停止、攻撃元異業者等への攻撃停止要請等、攻撃元ユーザの特定／恒久的措置等、攻撃元情報の管理、サイバー攻撃等に対する演習	
	• ネットワーク輻輳対策 （迅速な連絡・対応体制）	• 輻輳発生時対応手順等の整備、輻輳状態の通知／発生箇所特定、緊急時の通信規制措置・解除、ユーザ端末／回線に対する規制・通知、相互接続網に対する制御・通知	•
	• 故障・災害等ＩＴ障害対策 （迅速な連絡・対応体制）	• 故障等への対応手順書等の整備、装置故障時のメーカ等との連携、災害対応・復旧の手順書等の整備、災害対応時のメーカ等との連携、重要な設備の冗長構成等	• 事業遂行の観点から電気、道路、水道他分野を越えた情報が復旧対策が必要。
	• 情報漏えい対策	• 情報漏えい対応手順書の整備、漏えいの継続可能性に対する措置	•

特に重点的に取り組むべき事項			（回答欄） ネットワークのＩＰ化等に伴い検討が必要と考える事項等
（大項目）	（中項目）	（小項目）	
２．情報漏えい防止のための対策	• 媒体の取扱い	• 取り外し可能な媒体の管理手順策定	•
	• 情報の交換	• 通信設備を利用した情報交換保護指針・手順・管理策の策定	•
	• 情報漏えい対策	• 紙資料等の保管ルール、端末への資料持出し等のルール・制限、紙・可搬媒体の持出し管理	•

特に重点的に取り組むべき事項			（回答欄）
（大項目）	（中項目）	（小項目）	ネットワークのＩＰ化等に伴い検討が必要と考える事項等
３．外部委託における情報セキュリティ確保のための対策	• 秘密保持	• 守秘保持契約・守秘義務契約の要求事項の特定・レビュー	•
	• 外部組織	• 第三者との契約の際の管理策実施	•
	• 第三者が提供するサービスの管理	• 報告・記録の常時監視・レビュー・定期的監査の実施	•
	• 情報漏えい対策	• 外部委託時の重要情報取扱いルール	•

特に重点的に取り組むべき事項			（回答欄）
（大項目）	（中項目）	（小項目）	ネットワークのＩＰ化等に伴い検討が必要と考える事項等
その他	•		• 運用支援システムへの設備投資支援が必要。 • データ設定ミス等をなくすために警察、消防等への緊急通報接続システムのデータ共有化が必要。