資料２－２

フォローアップアンケートの集計結果
～平成28年度検証報告のフォローアップ～

アンケート概要

○ 「平成28年度電気通信事故に関する検証報告」（28年度年次報告）の活用状況について、平成29年度末に電気通信事業者に対しアンケートを実施

○ 28年度年次報告における提言内容（教訓）を23項目に整理した上で、各項目の実施状況及び実施効果を選択式（理由等の自由記述欄付）で質問

- 実施状況：「既に実施」、「当教訓を受け、新たに実施」、「当教訓を受け、既存の実施内容を見直し」、「当教訓を受け、今後実施予定」、「実施予定なし」、「教訓が該当しない」
- 実施効果：「十分な効果があった」、「一定の効果があった」、「効果が見られなかった」、「効果があるのか現時点では分からない」

○ 回答事業者数：220者（利用者数3万以上：42者、3万未満：178者）

（参考）電気通信事業者への依頼ルート

・各地方総合通信局（沖縄総合通信事務所含む）
・一般社団法人電気通信事業者協会
・一般社団法人テレコムサービス協会
・一般社団法人日本インターネットプロバイダー協会
・一般社団法人日本ケーブルテレビ連盟

実施状況の集計結果①

○ 実施※が70%以上の項目：8件

記載項目	教訓	実施
（7） 作業管理	工事作業中の人為ミスを防止するためには、工事担当者同士による二重のチェックや第三者の目による複線的なチェックなど、ミスを起こさない工事手順の策定とその遵守が求められる。**【複線的なチェック】**	82%
（5） 監視項目・監視方法	監視項目・監視頻度の設定に当たっては、提供する各サービスに求められるサービスレベルを考慮して行うことが重要である。**【監視項目・監視頻度の設定における考慮】**	81%
（1） 社内でのエスカレーション	事故発生後の経過時間や利用者からの問い合わせ状況も考慮しながら、例えば、一定時間経過後は、二次措置や全社体制へ移行することとするなど柔軟な対応が必要である。**【時間の経過に伴う体制移行】**	80%
（3） 利用者周知	事故の発生の際には、利用者に対する速やかな情報提供が求められる。一定時間経過後、まずは障害が発生している旨の第一報を発出し、具体的な障害内容、原因、復旧見込み等が判明した段階で、第二、第三報を発出する手順とすることが望ましい。**【段階的な情報提供】**	80%
（5） 監視項目・監視方法	障害を的確に検知するためには、日々のトラヒック分析について、平時の状態からどの程度差異が生じてもよいのかの許容値を定めておくことが重要であり、許容値については、トラヒック量等の中長期的な変化に対応させて都度調整することが必要である。**【トラヒック分析における適切な許容値の設定】**	72%
（3） 利用者周知	利用者は必ずしもリアルタイムに事故情報を確認するとは限らないことから、利用者が事後に事故の内容を正確に把握できるよう情報提供の方法を工夫する必要がある。例えば、第一報から復旧報までの履歴を保持し、復旧後も当面の間は掲載しておくことが重要である。**【第一報から復旧報までの履歴の保持】**	72%
（2） ソフトウェアのバージョン管理	修正される不具合や追加機能といったバージョンアップの規模や内容、インターネットに接続して使用する機器か否か、どういう設定状況になっているのか等の使用環境の変化を考慮し、バージョンアップの実施に伴うリスクと実施しないことに伴うリスクを比較評価の上でソフトウェア管理を行うことが重要である。**【ソフトウェアのバージョンアップにおけるリスク評価の実施】**	71%
（4） 適切な環境における試験・検証	事故の発生を未然に防止するため、新しいハードウェア・ソフトウェアの導入に当たり行う試験・検証作業は、機種、ソフトウェアのバージョン、システム構成等について、可能な限り運用環境と同一の環境で行うことが望ましい。**【試験・検証環境の同一化】**	70%

○ 実施※が50%未満の項目：5件

記載項目	教訓	実施
（1） 外部の目を入れた再発防止策の検討	再発防止策が発生原因に照らして妥当な内容であるか、追加で実施すべき対策が考えられないか等について、専門的な知見を有する第三者によるチェックを受けることは、事故の再発防止を図る上で有用である。**【再発防止策策定における第三者チェックの活用】**	30%
（7） 作業管理	データの自動入力、入力データの自動処理、誤入力時のアラームの発出等、なるべく人の手によらない仕組みを築くことも重要なポイントであり、電気通信事業者にあっては、ICTサービスの開発におけるノウハウも生かして取り組んでいくことが望ましい。**【人の手によらない仕組みの構築】**	37%
（3） 利用者周知	事故の状況によっては、情報提供については、多様な媒体により行うべきであり、事故情報を掲載するホームページのURLや他の媒体の周知に平時から努めるべきである。**【多様な媒体による情報提供】**	41%
（2） ソフトウェアのバージョン管理	過去の修正プログラムの適用に当たってのリスク評価は、将来の事故発生への対応に資するものであり、当該リスク評価の過程・結果については、社内で記録に残しておくことが望ましい。**【リスク評価の過程・結果の記録】**	48%
（2） 定期的なレビューの実施	電気通信サービスを継続的・安定的に提供していくためには、その管理の状況に問題がないかというソフト面でのチェックも含めた定期的かつ総合的なレビューが必要である。**【定期的・総合的なレビューの実施】**	49%

※「既に実施」、「既存の内容を見直し」、「当教訓を受け新たに実施」の合計。

実施状況の集計結果②

○ 「当教訓を受け、今後実施予定」が30%以上の項目：7件

記載項目	教訓	当教訓を受け、今後実施予定
（2） 定期的なレビューの実施	電気通信サービスを継続的・安定的に提供していくためには、その管理の状況に問題がないかというソフト面でのチェックも含めた定期的かつ総合的なレビューが必要である。**【定期的・総合的なレビューの実施】**	38%
（2） ソフトウェアのバージョン管理	過去の修正プログラムの適用に当たってのリスク評価は、将来の事故発生への対応に資するものであり、当該リスク評価の過程・結果については、社内で記録に残しておくことが望ましい。**【リスク評価の過程・結果の記録】**	37%
（7） 作業管理	データの自動入力、入力データの自動処理、誤入力時のアラームの発出等、なるべく人の手によらない仕組みを築くことも重要なポイントであり、電気通信事業者にあっては、ICTサービスの開発におけるノウハウも生かして取り組んでいくことが望ましい。**【人の手によらない仕組みの構築】**	35%
（5） 監視項目・監視方法	監視体制の構築に当たっては、利用者へのサービス提供の継続性を優先するのか、ネットワーク・設備の安全性を優先するのか等の運用ポリシーを運用担当者のみならず経営層も含めて明確にしておくべきであり、また、当該運用ポリシーはベンダー等の外部関係者とも共有しておく必要がある。**【運用ポリシーの明確化・外部関係者との共有】**	32%
（1） ソフトウェアの不具合への対応	電気通信事業者は、ソフトウェア等の不具合情報の提供に関し、どういった情報を共有するのか等について、ベンダーとの間で具体的な提供基準を設けておくべきである。**【電気通信事業者とベンダーのソフトウェア等の不具合情報の提供基準】**	31%
（1） 外部の目を入れた再発防止策の検討	再発防止策が発生原因に照らして妥当な内容であるか、追加で実施すべき対策が考えられないか等について、専門的な知見を有する第三者によるチェックを受けることは、事故の再発防止を図る上で有用である。**【再発防止策策定における第三者チェックの活用】**	31%
（2） フェイルソフトの考え方に基づくサービスの継続	事故の発生時の対応方針が、フェイルソフトの考え方に基づきサービスの継続を重視する方針である場合には、そのための具体的な手法・手順をあらかじめ定めておくことが重要である。例えば、各ユーザの利用量を管理し、トラヒック制御を行うこと等を目的とするポリシー制御を行う装置に故障が発生した場合には、ユーザ管理よりもサービス継続を優先し、当該機器を一時的に切り離すこととするといった手順をあらかじめ定めておくことにより、可用性の確保に寄与することが期待できる。**【可用性確保に寄与する障害発生時の具体的な手法・手順の規定】**	30%

実施状況の集計結果③

○ 「実施予定なし」が20%以上の項目：5件

記載項目	教訓	実施予定なし
（1） 外部の目を入れた再発防止策の検討	再発防止策が発生原因に照らして妥当な内容であるか、追加で実施すべき対策が考えられないか等について、専門的な知見を有する第三者によるチェックを受けることは、事故の再発防止を図る上で有用である。**【再発防止策策定における第三者チェックの活用】**	39%
（3） 利用者周知	事故の状況によっては、情報提供については、多様な媒体により行うべきであり、事故情報を掲載するホームページのURLや他の媒体の周知に平時から努めるべきである。**【多様な媒体による情報提供】**	34%
（7） 作業管理	データの自動入力、入力データの自動処理、誤入力時のアラームの発出等、なるべく人の手によらない仕組みを築くことも重要なポイントであり、電気通信事業者にあっては、ICTサービスの開発におけるノウハウも生かして取り組んでいくことが望ましい。**【人の手によらない仕組みの構築】**	28%
（6） 組織外の関係者との連携	クラウドサービス等の外部サービスを利用する場合には、加入者数の増加も見込んだ上で、自社のサービスにとって十分なスペックを備えているか、ネットワーク・設備に不具合が生じた場合のサービスへの影響、対応等の十分な説明を受けた上で、SLA（Service Level Agreement：サービス品質保証）を締結しておく必要がある。**【外部サービス利用における内容の把握】**	23%
（2） フェイルソフトの考え方に基づくサービスの継続	事故の発生時の対応方針が、フェイルソフトの考え方に基づきサービスの継続を重視する方針である場合には、そのための具体的な手法・手順をあらかじめ定めておくことが重要である。例えば、各ユーザの利用量を管理し、トラヒック制御を行うこと等を目的とするポリシー制御を行う装置に故障が発生した場合には、ユーザ管理よりもサービス継続を優先し、当該機器を一時的に切り離すこととするといった手順をあらかじめ定めておくことにより、可用性の確保に寄与することが期待できる。**【可用性確保に寄与する障害発生時の具体的な手法・手順の規定】**	20%

記載項目	理由
（1） 外部の目を入れた再発防止策の検討	①ベンダーが不具合を修正するため検証できない。専門家に依頼する費用も無いため ②チェックフローや第三者のあてがなく、予算も組んでいないため　③詳細を第三者へ情報提供する予定はないため ④専門的な知見を有する第三者がいない、依頼先が分からないため　など
（3） 利用者周知	①SNSの活用を現在行っていない。誤報や乗っ取りも考えられ、余計に混乱する可能性があるため ②SMS配信については管理が難しい（携帯電話番号の把握も必要となるため） ③地域がら高齢者が多く、SNS等の情報発信は効果が薄いため　④こちらから能動的に呼びかけることはしていない　など
（7） 作業管理	①現状の仕組みでも運用上、問題ないと考えるため　②保守事業者に委託しているため ③該当機器がバラバラで台数も少ないため、自動化にするメリットが少なく、予算も取りづらいため ④具体的にどのようなシステムが構築可能か分からないため、現時点では実施予定なし　など
（6） 組織外の関係者との連携	①外部サービスを利用していないため／利用する予定はないため ②大規模ISPからのサービス提供を受けており、加入者数増での変動はISPにとっては微増であり、品質に関しても先方が満たす基準が十分当社の品質レベルを満足するため　など
（2） フェイルソフトの考え方に基づくサービスの継続	①フェイルソフトで実施可能な装置がないため　②重要な機器は冗長化しており、可用性は確保できていると考えているため ③状況によって、停止覚悟で障害箇所を早急に発見した方がよい場合もあるため、臨機応変に対応を行う ④保守事業者に委託しているため　⑤キャッシュやトラフィック制御系システムは導入していないため ⑥サービス継続方法は故障箇所ごとに多岐にわたるため、あらかじめ手順を定めておくことは非現実的であると考えるため　など

実施効果の集計結果①

○ 「効果有り」※が80%以上の項目：6件

記載項目	教訓	効果有り
（4） 適切な環境における試験・検証	事故の発生を未然に防止するため、新しいハードウェア・ソフトウェアの導入に当たり行う試験・検証作業は、機種、ソフトウェアのバージョン、システム構成等について、可能な限り運用環境と同一の環境で行うことが望ましい。**【試験・検証環境の同一化】**	89%
（5） 監視項目・監視方法	監視項目・監視頻度の設定に当たっては、提供する各サービスに求められるサービスレベルを考慮して行うことが重要である。**【監視項目・監視頻度の設定における考慮】**	89%
（7） 作業管理	工事作業中の人為ミスを防止するためには、工事担当者同士による二重のチェックや第三者の目による複線的なチェックなど、ミスを起こさない工事手順の策定とその遵守が求められる。**【複線的なチェック】**	88%
（5） 監視項目・監視方法	早期の障害検知のためには、CPU使用率、ディスク容量等の直接のリソースを監視するだけではなく、呼処理の遅延時間や通信速度等のサービス品質に係る項目も監視することが重要である。**【サービス品質の監視】**	86%
（5） 監視項目・監視方法	障害を的確に検知するためには、日々のトラヒック分析について、平時の状態からどの程度差異が生じてもよいのかの許容値を定めておくことが重要であり、許容値については、トラヒック量等の中長期的な変化に対応させて都度調整することが必要である。**【トラヒック分析における適切な許容値の設定】**	83%
（7） 作業管理	データの自動入力、入力データの自動処理、誤入力時のアラームの発出等、なるべく人の手によらない仕組みを築くことも重要なポイントであり、電気通信事業者にあっては、ICTサービスの開発におけるノウハウも生かして取り組んでいくことが望ましい。**【人の手によらない仕組みの構築】**	83%

○ 「効果有り」※が60%未満の項目：3件

記載項目	教訓	効果有り
（3） 利用者周知	利用者は必ずしもリアルタイムに事故情報を確認するとは限らないことから、利用者が事後に事故の内容を正確に把握できるよう情報提供の方法を工夫する必要がある。例えば、第一報から復旧報までの履歴を保持し、復旧後も当面の間は掲載しておくことが重要である。**【第一報から復旧報までの履歴の保持】**	55%
（3） 利用者周知	事故の状況によっては、情報提供については、多様な媒体により行うべきであり、事故情報を掲載するホームページのURLや他の媒体の周知に平時から努めるべきである。**【多様な媒体による情報提供】**	59%
（1） 外部の目を入れた再発防止策の検討	再発防止策が発生原因に照らして妥当な内容であるか、追加で実施すべき対策が考えられないか等について、専門的な知見を有する第三者によるチェックを受けることは、事故の再発防止を図る上で有用である。**【再発防止策策定における第三者チェックの活用】**	59%

※ 「十分な効果があった」、「一定の効果があった」の合計

実施効果の集計結果②

○ 「効果がみられなかった」が5%以上の項目：なし

○ 「効果があるのか現時点では分からない」が30%以上の項目：7件

記載項目	教訓	効果があるのか現時点では分からない
（3） 利用者周知	利用者は必ずしもリアルタイムに事故情報を確認するとは限らないことから、利用者が事後に事故の内容を正確に把握できるよう情報提供の方法を工夫する必要がある。例えば、第一報から復旧報までの履歴を保持し、復旧後も当面の間は掲載しておくことが重要である。**【第一報から復旧報までの履歴の保持】**	45%
（3） 利用者周知	事故の状況によっては、情報提供については、多様な媒体により行うべきであり、事故情報を掲載するホームページのURLや他の媒体の周知に平時から努めるべきである。**【多様な媒体による情報提供】**	41%
（1） 外部の目を入れた再発防止策の検討	再発防止策が発生原因に照らして妥当な内容であるか、追加で実施すべき対策が考えられないか等について、専門的な知見を有する第三者によるチェックを受けることは、事故の再発防止を図る上で有用である。**【再発防止策策定における第三者チェックの活用】**	41%
（5） 監視項目・監視方法	監視体制の構築に当たっては、利用者へのサービス提供の継続性を優先するのか、ネットワーク・設備の安全性を優先するのか等の運用ポリシーを運用担当者のみならず経営層も含めて明確にしておくべきであり、また、当該運用ポリシーはベンダー等の外部関係者とも共有しておく必要がある。**【運用ポリシーの明確化・外部関係者との共有】**	35%
（1） ソフトウェアの不具合への対応	不具合の発生確率に関わらず両系ダウンやデータの喪失の恐れのある重要な不具合情報については、ベンダー等から確実に提供されることが必要であり、事故を起こした場合には常に当該基準の見直しを行うことが重要である。**【不具合情報の提供基準の見直し】**	34%
（2） ソフトウェアのバージョン管理	過去の修正プログラムの適用に当たってのリスク評価は、将来の事故発生への対応に資するものであり、当該リスク評価の過程・結果については、社内で記録に残しておくことが望ましい。**【リスク評価の過程・結果の記録】**	33%
（1） ソフトウェアの不具合への対応	電気通信事業者は、ソフトウェア等の不具合情報の提供に関し、どういった情報を共有するのか等について、ベンダーとの間で具体的な提供基準を設けておくべきである。**【電気通信事業者とベンダーのソフトウェア等の不具合情報の提供基準】**	30%

サービス規模による実施状況

○　利用者3万以上の事業者が、利用者3万未満の事業者と比べて、実施率が20%以上高い項目：10件

記載項目	教訓	実施率の差
（2）ソフトウェアのバージョン管理	不具合の修正を目的としたソフトウェアのバージョンアップについては、ベンダー等による重要度の情報のみならず、機器の自社のシステム構成上での役割を考慮すべきである。**【ソフトウェアのバージョンアップにおける考慮】**	32%
（4）適切な環境における試験・検証	事故の発生を未然に防止するため、新しいハードウェア・ソフトウェアの導入に当たり行う試験・検証作業は、機種、ソフトウェアのバージョン、システム構成等について、可能な限り運用環境と同一の環境で行うことが望ましい。**【試験・検証環境の同一化】**	31%
（2）フェイルソフトの考え方に基づくサービスの継続	事故の発生時の対応方針が、フェイルソフトの考え方に基づきサービスの継続を重視する方針である場合には、そのための具体的な手法・手順をあらかじめ定めておくことが重要である。例えば、各ユーザの利用量を管理し、トラヒック制御を行うこと等を目的とするポリシー制御を行う装置に故障が発生した場合には、ユーザ管理よりもサービス継続を優先し、当該機器を一時的に切り離すこととするといった手順をあらかじめ定めておくことにより、可用性の確保に寄与することが期待できる。**【可用性確保に寄与する障害発生時の具体的な手法・手順の規定】**	29%
（1）ソフトウェアの不具合への対応	電気通信事業者は、ベンダーから情報提供を受けるだけではなく、自らソフトウェアの不具合情報の積極的な収集・分析に努めることが必要である。少なくとも機器メーカーが発出するリリースノートについては、自ら収集し、不具合情報の確認を行うべきである。**【不具合情報の積極的な収集・分析】**	28%
（2）ソフトウェアのバージョン管理	修正される不具合や追加機能といったバージョンアップの規模や内容、インターネットに接続して使用する機器か否か、どういう設定状況になっているのか等の使用環境の変化を考慮し、バージョンアップの実施に伴うリスクと実施しないことに伴うリスクを比較評価の上でソフトウェア管理を行うことが重要である。**【ソフトウェアのバージョンアップにおけるリスク評価の実施】**	27%
（5）監視項目・監視方法	障害を的確に検知するためには、日々のトラヒック分析について、平時の状態からどの程度差異が生じてもよいのかの許容値を定めておくことが重要であり、許容値については、トラヒック量等の中長期的な変化に対応させて都度調整することが必要である。**【トラヒック分析における適切な許容値の設定】**	26%
（6）組織外の関係者との連携	クラウドサービス等の外部サービスを利用する場合には、加入者数の増加も見込んだ上で、自社のサービスにとって十分なスペックを備えているか、ネットワーク・設備に不具合が生じた場合のサービスへの影響、対応等の十分な説明を受けた上で、SLA（Service Level Agreement：サービス品質保証）を締結しておく必要がある。**【外部サービス利用における内容の把握】**	26%
（5）監視項目・監視方法	早期の障害検知のためには、CPU使用率、ディスク容量等の直接のリソースを監視するだけではなく、呼処理の遅延時間や通信速度等のサービス品質に係る項目も監視することが重要である。**【サービス品質の監視】**	22%
（3）冗長化	システム構成上の重要な役割を担う設備については、自社の運用ポリシーとの整合性を図りつつ、ソフトウェアの不具合も考慮に入れた冗長化の検討を行うことが望ましい。**【冗長化の検討における考慮】**	21%
（1）ソフトウェアの不具合への対応	電気通信事業者は、ソフトウェア等の不具合情報の提供に関し、どういった情報を共有するのか等について、ベンダーとの間で具体的な提供基準を設けておくべきである。**【電気通信事業者とベンダーのソフトウェア等の不具合情報の提供基準】**	20%

実施状況／実施効果

実施状況

実施状況 「高（80%以上）」かつ実施効果 「低（50%以下）」

（なし）

実施状況 「高（80%以上）」かつ実施効果 「高（80%以上）」

（7） 作業管理
工事作業中の人為ミスを防止するためには、工事担当者同士による二重のチェックや第三者の目による複線的なチェックなど、ミスを起こさない工事手順の策定とその遵守が求められる。【複線的なチェック】 [実施状況82%、実施効果88%]

（5） 監視項目・監視方法
監視項目・監視頻度の設定に当たっては、提供する各サービスに求められるサービスレベルを考慮して行うことが重要である。【監視項目・監視頻度の設定における考慮】 [実施状況81%、実施効果89%]

実施効果

実施状況 「低（50%以下）」かつ実施効果 「低（50%以下）」

（なし）

実施状況 「低（50%以下）」かつ実施効果 「高（80%以上）」

（7） 作業管理
データの自動入力、入力データの自動処理、誤入力時のアラームの発出等、なるべく人の手によらない仕組みを築くことも重要なポイントであり、電気通信事業者にあっては、ICTサービスの開発におけるノウハウも生かして取り組んでいくことが望ましい。【人の手によらない仕組みの構築】 [実施状況37%、実施効果83%]

27年度年次報告及び28年度年次報告の実施率比較

○　27年度年次報告及び28年度年次報告において提言内容が似ている主な教訓に関して、実施率を比較

27年度年次報告	実施率	28年度年次報告	実施率
ハードウェアやソフトウェアの障害情報について、ベンダー等との定期的な情報交換の場を設定したり、ベンダー等との保守契約をプロアクティブなものに見直すことが考えられる。【ベンダー等との定期的な情報交換】	62%	電気通信事業者とベンダーは、機器のシステム構成上の役割等についての共通理解を図った上で、不具合がシステム全体にどのような影響を及ぼす可能性があるのか、利用者のサービス提供にどのような影響が考えられ得るのか等のレベルまで共有できるような深い連携に努めるべきである。【電気通信事業者とベンダーの深い連携】	68%
特に、サイレント故障への対応にあたっては、ログ情報だけでなく、スループット、パケット廃棄量、CPU利用率などのネットワーク装置の性能情報も収集する等して総合的に判断することが望ましい。【サイレント故障への対応】	55%	早期の障害検知のためには、CPU使用率、ディスク容量等の直接のリソースを監視するだけではなく、呼処理の遅延時間や通信速度等のサービス品質に係る項目も監視することが重要である。【サービス品質の監視】	66%
ネットワーク・設備構成の設計に当たって十分な設備量を確保するとともに、トラヒックと設備量の推移を適切に監視することが必要。【十分な設備量の確保】	81%	障害を的確に検知するためには、日々のトラヒック分析について、平時の状態からどの程度差異が生じてもよいのかの許容値を定めておくことが重要であり、許容値については、トラヒック量等の中長期的な変化に対応させて都度調整することが必要である。【トラヒック分析における適切な許容値の設定】	72%
事業者は、事故の発生の際には速やかに一報を発出することが求められる。事故の発生時点で原因や故障設備の特定ができなければ、その旨を周知しておけばよいと思われる。【速やかな情報提供】	78%	事故の発生の際には、利用者に対する速やかな情報提供が求められる。一定時間経過後、まずは障害が発生している旨の第一報を発出し、具体的な障害内容、原因、復旧見込み等が判明した段階で、第二、第三報を発出する手順とすることが望ましい。【段階的な情報提供】	80%
インターネット接続サービスに障害が発生した場合には、利用者がすぐにホームページの情報を確認することができない場合もあることから、SNSの活用など情報提供手段の多様化を図る必要がある。すなわち、「情報提供体制の冗長化」が必要である。【情報提供手段の多様化】	40%	事故の状況によっては、情報提供については、多様な媒体により行うべきであり、事故情報を掲載するホームページのURLや他の媒体の周知に平時から努めるべきである。【多様な媒体による情報提供】	41%
事業者は重大な事故を起こした際には積極的に活用することが望ましい。【第三者検証の積極活用】	28%	再発防止策が発生原因に照らして妥当な内容であるか、追加で実施すべき対策が考えられないか等について、専門的な知見を有する第三者によるチェックを受けることは、事故の再発防止を図る上で有用である。【再発防止策策定における第三者チェックの活用】	30%
電気通信事業者には、以上の検証を踏まえ、今一度、管理規程や内規等で定めた事項が十分遵守できているかどうか等について点検することを求めたい。特に、重大な事故を発生させた事業者は、事故後の対応や再発防止策の実施状況について積極的に情報公開を行うことが望ましい。【管理規程等の点検】	37%	電気通信サービスを継続的・安定的に提供していくためには、その管理の状況に問題がないかというソフト面でのチェックも含めた定期的かつ総合的なレビューが必要である。【定期的・総合的なレビューの実施】	49%

参考　平成28年度年次報告書にてまとめられた教訓（23項目）

1．事故の事前防止の在り方

（1）ソフトウェアの不具合への対応

・電気通信事業者とベンダーの深い連携

電気通信事業者とベンダーは、単なる不具合情報の共有に留まることなく、当該機器のシステム構成上の役割等についての共通理解を図った上で、当該不具合がシステム全体にどのような影響を及ぼす可能性があるのか、利用者のサービス提供にどのような影響が考えられ得るのか等のレベルまで共有できるような深い連携に努めるべきである。

・電気通信事業者とベンダーのソフトウェア等の不具合情報の提供基準

電気通信事業者は、ソフトウェア等の不具合情報の提供に関し、どういった情報を共有するのか等について、ベンダーとの間で具体的な提供基準を設けておくべきである。

・不具合情報の提供基準の見直し

不具合の発生確率に関わらず両系ダウンやデータの喪失の恐れのある重要な不具合情報については、ベンダー等から確実に提供されることが必要であり、事故を起こした場合には常に当該基準の見直しを行うことが重要である。

・不具合情報の積極的な収集・分析

電気通信事業者は、ベンダーから情報提供を受けるだけではなく、自らソフトウェアの不具合情報の積極的な収集・分析に努めることが必要である。少なくとも機器メーカーが発出するリリースノートについては、自ら収集し、不具合情報の確認を行うべきである。

（2）ソフトウェアのバージョン管理

・ソフトウェアのバージョンアップにおける考慮

不具合の修正を目的としたソフトウェアのバージョンアップについては、ベンダー等による重要度の情報のみならず、機器の自社のシステム構成上での役割を考慮すべきである。

・ソフトウェアのバージョンアップにおけるリスク評価の実施

導入しているソフトウェアのバージョンアップが行われた場合であっても、システムの安定的な稼働の観点から、直ちに修正プログラムを適用することはしないという対応はあり得る。しかしながら、修正される不具合や追加機能といったバージョンアップの規模や内容、インターネットに接続して使用する機器か否か、どういう設定状況になっているのか等の使用環境の変化を考慮し、バージョンアップの実施に伴うリスクと実施しないことに伴うリスクを比較評価の上でソフトウェア管理を行うことが重要である。

・リスク評価の過程・結果の記録

過去の修正プログラムの適用に当たってのリスク評価は、将来の事故発生への対応に資するものであり、当該リスク評価の過程・結果については、社内で記録に残しておくことが望ましい。

（3）冗長化

・冗長化の検討における考慮

システム構成上の重要な役割を担う設備については、自社の運用ポリシーとの整合性を図りつつ、ソフトウェアの不具合も考慮に入れた冗長化の検討を行うことが望ましい。

参考 平成28年度年次報告書にてまとめられた教訓（23項目）

（４）適切な環境における試験・検証

・試験・検証環境の同一化

事故の発生を未然に防止するため、新しいハードウェア・ソフトウェアの導入に当たり行う試験・検証作業は、機種、ソフトウェアのバージョン、システム構成等について、可能な限り運用環境と同一の環境で行うことが望ましい。

（５）監視項目・監視方法

・監視項目・監視頻度の設定における考慮

監視項目・監視頻度の設定に当たっては、提供する各サービスに求められるサービスレベルを考慮して行うことが重要である。

・サービス品質の監視

早期の障害検知のためには、CPU使用率、ディスク容量等の直接のリソースを監視するだけではなく、呼処理の遅延時間や通信速度等のサービス品質に係る項目も監視することが重要である。

・運用ポリシーの明確化・外部関係者との共有

監視体制の構築に当たっては、利用者へのサービス提供の継続性を優先するのか、ネットワーク・設備の安全性を優先するのか等の運用ポリシーを運用担当者のみならず経営層も含めて明確にしておくべきであり、また、当該運用ポリシーはベンダー等の外部関係者とも共有しておく必要がある。

・トラヒック分析における適切な許容値の設定

障害を的確に検知するためには、日々のトラヒック分析について、平時の状態からどの程度差異が生じてもよいのかの許容値を定めておくことが重要であり、許容値については、トラヒック量等の中長期的な変化に対応させて都度調整することが必要である。

（６）組織外の関係者との連携

・外部サービス利用における内容の把握

電気通信サービスの提供に当たり、クラウドサービス等の外部サービスを利用する場合には、加入者数の増加も見込んだ上で、自社のサービスにとって十分なスペックを備えているか、ネットワーク・設備に不具合が生じた場合のサービスへの影響、対応等の十分な説明を受けた上で、SLA（Service Level Agreement：サービス品質保証）を締結しておく必要がある。利用している外部サービスの内容について把握しておくことは、事故発生時に自社のサービス利用者への対応を迅速・適切に行う観点からも重要である。

（７）作業管理

・複線的なチェック

工事作業中の人為ミスを防止するためには、工事担当者同士による二重のチェックや第三者の目による複線的なチェックなど、ミスを起こさない工事手順の策定とその遵守が求められる。

・人の手によらない仕組みの構築

データの自動入力、入力データの自動処理、誤入力時のアラームの発出等、なるべく人の手によらない仕組みを築くことも重要なポイントであり、電気通信事業者にあっては、ICTサービスの開発におけるノウハウも生かして取り組んでいくことが望ましい。

2. 事故発生時の対応の在り方

（1）社内でのエスカレーション

・時間の経過に伴う体制移行

事故発生後の経過時間や利用者からの問い合わせ状況も考慮しながら、例えば、一定時間経過後は、二次措置や全社体制へ移行することとするなど柔軟な対応が必要である。

（2）フェイルソフトの考え方に基づくサービスの継続

・可用性確保に寄与する障害発生時の具体的な手法・手順の規定

事故の発生時の対応方針が、フェイルソフトの考え方に基づきサービスの継続を重視する方針である場合には、そのための具体的な手法・手順をあらかじめ定めておくことが重要である。例えば、各ユーザの利用量を管理し、トラヒック制御を行うこと等を目的とするポリシー制御を行う装置に故障が発生した場合には、ユーザ管理よりもサービス継続を優先し、当該機器を一時的に切り離すこととするといった手順をあらかじめ定めておくことにより、可用性の確保に寄与することが期待できる。

（3）利用者周知

・段階的な情報提供

事故の発生の際には、利用者に対する速やかな情報提供が求められる。情報の発出を社内エスカレーションと連動させず、一定時間経過後、まずは障害が発生している旨の第一報を発出し、具体的な障害内容、原因、復旧見込み等が判明した段階で、第二、第三報を発出する手順とすることが望ましい。また、途中で利用者に影響のある事象の変化が認められた場合には速やかに利用者に情報提供を行うことが必要である。

・第一報から復旧報までの履歴の保持

利用者は必ずしもリアルタイムに事故情報を確認するとは限らないことから、利用者が事後に事故の内容を正確に把握できるよう情報提供の方法を工夫する必要がある。例えば、ホームページに掲載した事故情報については、安信基準の解説に措置例として記載しているように、第一報から復旧報までの履歴を保持し、復旧後も当面の間は掲載しておくことが重要である。

・多様な媒体による情報提供

事故の状況によっては、ホームページへの掲載のみでは利用者が事故に関する情報を把握することが困難な場合があるため、情報提供については、多様な媒体により行うべきであり、事故情報を掲載するホームページのURLや他の媒体の周知に平時から努めるべきである。事故発生時に携帯電話のSMSを通じてホームページのURLを周知することも考えられる。

3. 事故収束後のフォローアップの在り方

（1）外部の目を入れた再発防止策の検討

・再発防止策策定における第三者チェックの活用

事故の収束後は、まずは事故発生事業者が、事故の原因等を自ら検証した上で必要な再発防止策を策定することが重要であるが、当該再発防止策が発生原因に照らして妥当な内容であるか、追加で実施すべき対策が考えられないか等について、専門的な知見を有する第三者によるチェックを受けることは、事故の再発防止を図る上で有用である。

（2）定期的なレビューの実施

・定期的・総合的なレビューの実施

国民生活や企業の社会経済活動に不可欠な電気通信サービスを継続的・安定的に提供していくためには、ネットワーク・設備の故障の有無といったハード面のチェックのみならず、その管理の状況に問題がないかというソフト面でのチェックも含めた定期的かつ総合的なレビューが必要である。