資料46-4

ソフトウェアに起因する
通信事故の発生を踏まえた
緊急点検について

2019年2月14日

ソフトバンク株式会社

SoftBank

1　ソフトウェアの信頼性確保 1/3

項番	質問	質問の意図・ポイント	回答
1－1	ソフトウェア導入時に留意している点があるか。	○交換機等設備のソフトウェアのバージョンについて、最新型の導入は見送る、他事業者で一定期間運用実績があることを確認の上導入する、商用環境に近い環境で十分な期間の試験や検証を行った上で導入する等の運用方針、留意点があるか	【商用環境適用前】 • 机上にて旧バージョンとの機能差分を確認 • 自社検証環境（商用環境に準ずる）を用いた十分な検証試験を実施 【商用環境適用時】 • 最小規模でのソフトウェアの安定性を確認 • 段階的に展開台数を増加し、一定の期間をもって全台のソフトウェア更新を行う 各ポイントにおいて判定会議を実施
1－2	ソフトウェアに関し導入時試験においてどのような項目の確認を行っているか。	○交換機等設備の導入時試験において、ソフトウェアに関して以下の項目を実施しているか ・証明書の有無の確認 ・証明書の有効期限の確認 ・未来日での動作確認 ○交換機等設備の導入後においても、ソフトウェアに関する検証やリスク分析のための試験を定期的に実施し、改善点が見つかれば商用ネットワークにフィードバックしているか ○これらの試験は、商用に近い条件の別系統のネットワークを構築して実施するなど、商用環境に近い環境で実施しているか	【導入時試験での主な確認事項】 • 新規機能および既存機能の確認 （商用トラフィックを想定した各種サービス試験） • 負荷試験および連続運転試験による安定性の確認 【導入後の主な確認事項】 • 他マーケットで発見された問題に対するリリース情報をベンダーより適宜入手し、都度適用可否判断を実施 • 商用環境への適用は、導入時の試験および商用展開と同様 【今回の事故原因を踏まえた対応】 • 証明書が利用されているものについては、有効期限の確認徹底 • 検証環境にて未来日動作確認を行う社内ルールを整備

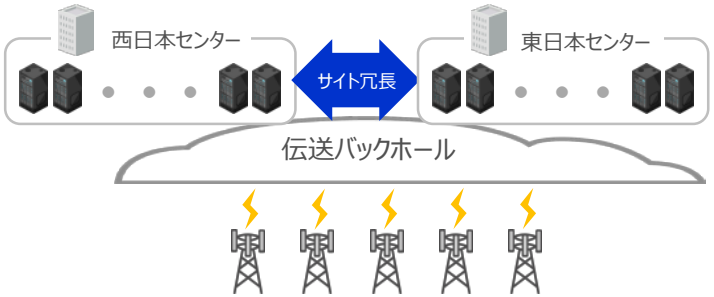
1　ソフトウェアの信頼性確保 2/3

項番	質問	質問の意図・ポイント	回答
1－3	ソフトウェアに関してバックアップデータをどのように保持しているか。	○交換機等設備のソフトウェアのバックアップとして、安定運用していた旧バージョンを自社で保持、またはベンダーにおいて保持しており、すぐに旧バージョンに切り替えられる体制を整えている等の対策を採っているか ○ソフトウェアの異常を検知した場合に、どのような検討プロセスを経て、どのような場合に旧バージョンに切り替える対策が有効と判断するのか（他の手段による対策と比較して有効度・優先度をどのように評価しているのか）	• 複数世代のソフトウェアをバックアップサーバに保存 • 旧バージョンへの切り替えができる体制を構築 • 致命的なソフトウェアの不具合により、すべての設備が機能を停止した場合、旧バージョンに切り替える運用方針 【今回の事故原因を踏まえた対応】 • 各種設備の旧バージョンへ切り替える手順の再確認
1－4	ソフトウェアの監査をどのように実施しているか。	○交換機等設備の導入時にソフトウェアに関し外部機関による監査を実施しているか ○ソフトウェアに特化した定期的なシステム監査を行っているか。行っている場合、内部監査かあるいは外部監査か	• 社内規程に基づき社内セキュリティ部門によるセキュリティ監査を実施 • 商用運用中の設備へのセキュリティ監査はお客様のサービス提供に支障の出ない範囲で定期的に実施 • 他マーケットで発見された問題もベンダーより適宜共有・分析することでソフトウェアの品質管理を実施 • 交換機のソフトウェア（アプリケーション）そのものを監査する外部機関は確認できていない
1－5	ソフトウェアの証明書の確認をどのようにおこなっているか。	○交換機に限らず、現在利用しているソフトウェアの中に、有効期限が設定されている証明書を利用しているものがあるかを確認しているか ○確認している場合において、実際に有効期限が設定されている証明書を利用している場合、その証明書（有効期限）は自社で確認可能なものか ○自社で有効期限を把握・管理しているか、もしくはベンダーで把握・管理するとともに、通信事業者の求めに応じてすぐに提示されるような体制を構築しているか	• 証明書の管理はベンダーおよび自社双方で実施 【今回の事故原因を踏まえた対応】 • 交換設備、無線設備、サーバ設備の総点検を実施 • 有効期限管理・運用が適切に実施されていることを再確認 • 今後は、設計段階において、証明書のように期限を持つ情報は、外部から確認できるような構造となるようベンダーへ改善を要求

1　ソフトウェアの信頼性確保 3/3

項番	質問	質問の意図・ポイント	回答
1－6	ソフトウェアの導入、運用・管理に関し、電気通信設備統括管理者が行っていることは何か。	○電気通信設備統括管理者が、ソフトウェアの導入、運用・管理に関しなんらかマネージメントを行っているか 例）ソフトウェアの監査を行うことを決定している、ソフトウェア開発者の雇用・配備方針を決定している、ソフトウェアに関する事故等発生時の対応マニュアルを策定している	電気通信役務の確実かつ安定的な提供を確保するために、組織全体かつ横断的に関与し、事故防止に関する方針、体制および方法等へ主体的に関与 【ソフトウェアの導入】 新規設備導入および大規模な機能追加に伴うソフトウェア導入時の承認 【ソフトウェアの運用・管理】 運用管理体制および異常時の対応マニュアルの承認
1－7	基地局において同様な障害が発生しないように留意している点があるか。	○多数の基地局に同時に影響を与えうる形でソフトウェアの利用をしているか ○該当するソフトウェアの利用がある場合、大規模な障害を起こさないように対策を行っているか	基地局は複数のベンダーにより構成されており、今回のようにソフトウェアの不具合によってすべての基地局に不具合が発生する構造ではない 基地局においても留意点は１－１，１－２と同様 【商用環境適用前】 • 机上にて旧バージョンとの機能差分を確認 • 自社検証環境（商用環境に準ずる）を用いた十分な検証試験を実施 【商用環境適用時】 • 最小規模でのソフトウェアの安定性を確認 • 段階的に展開台数を増加し、一定の期間をもって全台のソフトウェア更新を行う 【導入時試験での主な確認事項】 • 新規機能および既存機能の確認 （商用トラフィックを想定した各種サービス試験） • 負荷試験および連続運転試験による安定性の確認 【導入後の主な確認事項】 • 他マーケットで発見された問題に対するリリース情報をベンダーより適宜入手し、都度適用可否判断を実施 • 商用環境への適用は、導入時の試験および商用展開と同様

2　予備機器の設置による冗長性確保

項番	質問	質問の意図・ポイント	回答
2－1	今般の障害原因であったLTEパケット交換機について予備機器を設置しているか。	○パケット交換機は予備機器を設置しているか 予備機器の設置は、 ①同一ベンダー同一機器の設置場所を別にする措置か ②同一ベンダーの別機器を導入する措置か ③他ベンダーの機器を導入（マルチベンダー化）する措置か ○予備機器として他ベンダーの機器を導入している場合、ハードウェア、ソフトウェア双方ともに主機器とは別種のものか ○予備機器を設置している場合、予備機器はホットスタンバイかコールドスタンバイか ○交換機の主機器、予備機器それぞれのメーカ（ベンダー）はどこか ○予備機器を設置していない場合はその理由	• 全台を稼働状態で運用する冗長方式（プール化方式） • 個々の設備はAct/Sby構成（二重化方式） • 東西センターにてサイト冗長を実現するための十分な容量を確保  【今回の事故原因を踏まえた対応】 今後予備機器として異なるソフトウェアで動作する設備の導入を検討
2－2	予備機器の設置方針はどのようなものか。	○交換機に限らず、中核設備については全て予備機器を設置しているか。予備機器を設置する対象設備の範囲、方法等の考え方・方針があるか ○中核設備の現用・予備の機器が同一の仕様のソフトウェアが制御する仕組みとなっている場合は、そのソフトウェアの不具合により現用・予備の両方の機能が動作しないような事態が起こり得る。こうした事態を踏まえた、「ソフトウェアによる機能の冗長性」及び「故障等に応じた複数段階（最低限）の機能維持」の考え方・方針があるか ○なお、中核設備以外についても、予備機器を設置する対象設備の範囲、方法等の考え方・方針があるか	設備冗長については設備の重要度および冗長機能によって方針を策定 • 全台を稼働状態で運用する冗長方式（プール化方式） • 個々の設備はAct/Sby構成（二重化方式） • 予備機への切り替えによる冗長構成（N+1方式） • 上記の組み合わせ ソフトウェア機能の冗長性に関しては、ソフトウェア更新時期以外は提供サービスの差分等が発生する可能性があるため、ソフトウェアバージョンの異なるものを併存した運用は行っていない 万一ソフトウェアの不具合により同時刻に全台が機能を停止するような事態に備え、バックアップファイルを利用し復旧できる体制を構築している

3　障害発生時の対応　1/2

項番	質問	質問の意図・ポイント	回答
3－1	交換機で障害が発生した場合の障害原因の特定をどのように行っているか。	○交換機において異常を検知した場合の障害箇所特定手順や復旧手順は定めているか ○ソフトウェアの異常か、サイバー攻撃によるものか、障害原因を速やかに分別できる検知方法又は切り分け方法を有しているか ○交換機で障害が発生した際に、結果として交換機以外の設備においても異常を検知した場合に、障害原因が交換機であること（及び交換機のどの機器であること）を迅速かつ的確に把握できる仕組みになっているのか ○上記問で速やかに分別・把握できる方法を有している場合、それは自社で対応可能な措置か（もしくはベンダー等で速やかな対応が可能となっているか） ○障害発生時にベンダーとどのような方法（手段）でどのような情報のやりとりをすることとしているか（障害発生時に事業者及びベンダーそれぞれが行うことや連絡方法（手段）・連絡内容等をマニュアル等により定めているか、平素からベンダーとの連携に関し留意していることがあるかなど）	• 知得したアラーム情報より原因箇所を特定し、対応すべき手順を準備している • サイレント障害（ソフトウェア不具合によりアラームが発生しない）時はサービス監視（トラフィック監視）により異常を知得し、原因箇所を特定する運用 • サービス復旧に関わる電気通信設備の操作は全て自社で対応 • ベンダーからの必要な支援を受けられるよう連絡体制（電話会議）を構築 • ベンダーへ故障原因解析に必要な情報を提供できるような体制を構築 事故発生時は、被疑箇所を排除する等のサービス復旧を優先する 根本原因（サイバー攻撃かの判断含む）の解析は、ベンダーにより復旧作業と並行して行われるが、サービス復旧後となる場合が多い 【今回の事故の分析】 事故発生時はソフトウェア障害の手順に従い復旧作業を実施 復旧作業の過程で特定のバージョンで発生していることをベンダーより知得 原因については復旧後ベンダーによる分析により特定
3－2	コールセンターや販売代理店での利用者対応はどのように行っているか。	○事故が発生した場合の利用者対応の手順・内容をマニュアル等で整理しているか ○マニュアル等を整理している場合、利用者対応として、誰（コールセンター、販売代理店等）がどのような内容を行うように整理しているか	• 店舗、コールセンター共に発生した事柄、復旧目処、原因など応対スタンスをマニュアルとして整理 • 事故などお客さま影響の高い事案を知得した時点で「障害報」を店舗、コールセンターにそれぞれ告知し、障害発生を周知 以降内容が判明次第情報を更新 • 事故が発生した場合、お客さまに対する回答マニュアルを作成、店舗およびコールセンターに展開 • 利用者対応は主にコールセンターが担当し、店舗でもその時点で判明している事象の説明を実施

3　障害発生時の対応　2/2

SoftBank

項番	質問	質問の意図・ポイント	回答
3－3	大規模な障害が発生した際に、通信を確保するための代替手段としてどのような手段があるか。	○今般の障害のようにLTEが通信不可となった場合に、通信を確保するための代替手段として行っている、もしくは検討していることがあるか （4G→3Gへの切替、BWAの利用など） ○実施には至っていないが、技術的な手段以外も含め、代替手段として有効と考えられる方策（アイデア）としてどのようなものが考えられるか ○特に緊急通報の確保のために行っている措置があるか	大規模な事故発生時の代替手段は、事故の内容・支障サービスにより異なるため、影響を受けた利用者がその時とりうる手段についての周知を行う 【今回と同様なサービス影響に対する代替手段】 • 音声サービスは3G（※緊急通報確保の観点より通信規制を実施） • パケット通信は3GおよびWi-Fi

４　リスク管理

項番	質問	質問の意図・ポイント	回答
４－１	電気通信設備の重要度に応じて要求品質に違いを設ける等の対策を行っているか。	○リスク管理の観点での重要度に応じて電気通信設備のランク付けを行っているか ○上記電気通信設備のランク付けに応じてSLAに反映、もしくはパッケージ品の購入に際しての基準に反映させているか ○上記SLAの策定に当たっての考え方、方針があれば教示願う ○SLAへの反映等を行っていない場合にはその理由 ○リスク管理及びSLAへの反映方針について経営陣への共有がなされているか	電気通信設備の導入時（新設・増設）では、サービス内容や需要計画に基づき設備構成、容量等を考慮した設計を行っている 設計段階では、障害発生時に重大事故とならないよう設備構成は事業所内での装置冗長の他、複数拠点でのサイト冗長をとり、かつ縮退した設備で役務継続出来る容量の確保等を考慮している これら設計要件を満たすベンダー選定を行っており、また設備導入にあたっては投資に関わる事項でもあるため経営陣への説明・承認のうえで実行している 導入した設備に対しては、ベンダー毎に保守サポート契約を締結してハードウェア・ソフトウェアのサポート要件を定めている 保守サポートの要件は、対象製品について開示された情報のうち、自社で対応可能な範囲を除きサポートを受けている

今回の事故をうけたソフトウェア導入時に留意すべき事項

SoftBank

設計段階における留意事項

課題	証明書がプログラムに埋め込まれており 外部から有効期限の確認不可
留意すべき事項	証明書のように期限を持つ情報はソフトウェアの設計上 外部から確認できる構造とすべき

検証段階における留意事項

課題	検証項目に未来日での動作確認がなかった
留意すべき事項	検証試験において未来日での動作確認を行うことが有効