

ソフトウェアに起因する通信事故の発生を踏まえた  
緊急点検の回答について

2019年2月14日

株式会社NTTドコモ

# 1. ソフトウェアの信頼性確保 回答①

質問項目	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	<ul style="list-style-type: none"> <li>● <u>ソフトウェアの導入に際しては、自社検証環境および地域限定の商用環境において十分な検証を行った後、全国の商用ネットワークに導入いたします</u></li> </ul> <p>ソフトウェアは弊社仕様で開発しており、導入においては必要機能が具備されている事やコストに加え、既知のバグ（セキュリティ脆弱性含む）が改修されていること、EoS/Lまでの期間が長い事（長く使用出来る事）、他事業者等での十分な運用実績がある事（バグが枯れている事）、等を総合的に考慮して判断します。</p> <p>試験環境としては、まず弊社R&amp;Dセンタ内の試験環境において開発部門での品質や性能チェックを実施します。その際、実際の商用環境になるべく近い環境を模擬した試験等も行います。その後、重点監視の体制の下で地域を制限した形で先行での商用導入を実施し、商用環境での動作を確認した上で、全国導入を実施しています。</p>
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	<p>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</p> <ul style="list-style-type: none"> <li>・証明書の有無の確認</li> <li>・証明書の有効期限の確認</li> <li>・未来日での動作確認</li> </ul> <p>これらの試験は、商用に近い条件の別システム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</p> <p>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</p>	<ul style="list-style-type: none"> <li>● <u>ソフトウェアの導入試験（動作確認）においては、機能の動作検証に加え、証明書の存在およびそれが有効期限内であることも同時に確認しております。</u></li> </ul> <p>証明書についての未来日での動作確認は試験として明確に行っているわけではありませんが、1-5に記載のように有効期限は管理しており、有効期限が切れる前に更改する等の運用対応も含め、有効期限切れを防ぐ方策を取っております。</p> <p>試験環境としては、まず弊社R&amp;Dセンタ内の試験環境において開発部門での品質や性能チェックを実施します。その際、実際の商用環境になるべく近い環境を模擬した試験等も行います。その後、重点監視の体制の下で地域を制限した形で先行での商用導入を実施し、商用環境での動作を確認した上で、全国導入を実施しています。</p> <p>ネットワークの通信品質等については日々最適化・高品質化に努めており、ソフトウェアの定期的なアップデートや、緊急度に応じて不定期な改修を行っています。</p>

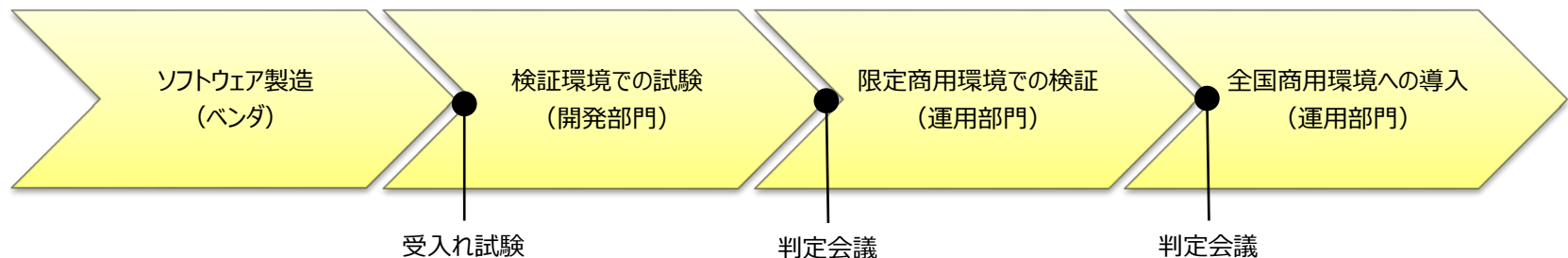


図1 ソフトウェア導入までの流れ

# 1. ソフトウェアの信頼性確保 回答②

質問項目	質問の意図・ポイント	回答
<p>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。</p>	<p>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</p> <p>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）</p>	<ul style="list-style-type: none"> <li>● <u>交換機等のバックアップデータは、システム毎にバックアップの収集ルール（バックアップ内容や実施周期等）を定め、そのルールに従いバックアップデータを収集しています。</u></li> </ul> <p>バックアップデータは、外部媒体に保存する場合、その外部媒体を該当システムが設置されているビルに施錠保管しています。また、大容量ファイルサーバーにバックアップを保存・管理する装置もあります。</p> <p>また、バックアップデータについては現用のソフトウェアバージョンだけでなく、前ソフトウェアバージョンで動作可能なバックアップデータを管理するなど、ソフトウェアの世代管理も実施しています。</p> <p>旧バージョンへの切り替えに対しては、サービス復旧を最優先として復旧に向けた措置や旧バージョンへの切り替え等を総合的に判断して実施しています。</p>
<p>1-4. ソフトウェアの監査をどのように実施しているか。</p>	<p>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</p> <p>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</p>	<ul style="list-style-type: none"> <li>● <u>交換機等のソフトウェアは弊社仕様で開発しており、ソフトウェアの導入に対する内部監査（検証）を実施しています。</u></li> </ul> <p>交換機等設備のソフトウェア導入時は、開発部門での品質や性能チェックを実施し、その後、ソフトウェアの商用導入にあたり、運用部門にて受け入れ判定を実施しています。</p> <p>更にインターネット接続を行う交換機等設備に対しては、セキュリティ審査やソフトウェアの脆弱性診断等を、導入時及び定期的に行っています。</p> <p>また、交換機等設備は、定期的に運用規定に則った対応ができることを確認しています。</p> <p>なお、ソフトウェアに関して外部機関による監査は実施していません。</p>

# 1. ソフトウェアの信頼性確保 回答③

質問項目	質問の意図・ポイント	回答
<p>1 - 5. ソフトウェアの証明書の確認をどのように行っているか。</p>	<p>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</p> <p>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</p> <p>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</p>	<ul style="list-style-type: none"> <li>● <u>交換機等のシステム開発時および商用環境への導入時、また商用環境導入後においても定期的に、ソフトウェアの中に有効期限が設定されている証明書について有効期限の確認を実施しています</u></li> </ul> <p>システム開発時において、ソフトウェアの中に有効期限が設定されている証明書について有効期限の確認を実施しています。</p> <p>また、商用への導入時においては、ソフトウェアの信頼性確保や証明書管理方法等を判定して、信頼性を担保した形で導入を実施しています。</p> <p>商用への導入後に証明書を利用している交換機等のシステムは、システム単位に証明書の有効期限の管理を実施しています。</p> <p>具体的には、自社または、ベンダーにて証明書単位の有効期限を定期的にチェックすることで、有効期限が失効する前までに更新するよう対応をルール化、運用しています。</p> <p>なお、ベンダーにて証明書の有効期限を実施している場合は、その確認結果を弊社側で確認しています。</p>
<p>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。</p>	<p>電気通信設備統括管理者が、ソフトウェアの導入、運用・管理に関しなにか管理を行っているか</p> <p>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</p>	<ul style="list-style-type: none"> <li>● <u>社内事業用電気通信設備管理規程の定めに従い、電気通信役務の確実かつ安定的な提供に関し、予算の確保、体制の構築等必要な措置を講じると共に、業務の実施及び管理の状況が適切かどうかを常に確認し、必要な改善を行っております</u></li> </ul> <p>交換機等装置の新規システム導入では、ソフトウェアを含めたシステムの導入判定を実施しており、導入するシステムの重要性に応じて判定実施者を定め全社的なルールを定めています。</p> <p>また、新バージョンのソフトウェアを導入する作業は重要工事と定め、工事期間や工事の実施方法等について確認しています。</p> <p>また、ソフトウェア起因に限らず、ネットワークやサービス障害発生時の全社的な対応マニュアルを定め、故障レベルに応じてマネジメントを実施しています。</p>
<p>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</p>	<p>多数の基地局に同時に影響を与える形でソフトウェアの利用をしているか</p> <p>該当するソフトウェアの利用がある場合、大規模な障害を起ささないように対策を行っているか</p>	<ul style="list-style-type: none"> <li>● <u>多数の基地局に同時に影響を与えるような、有効期限を有する証明書やライセンス等の利用はしていません。</u></li> </ul> <p>なお、基地局装置の型番毎に同一のソフトウェアを利用しているため、ソフトウェアの不具合に起因して型番毎に同じ障害が発生する可能性は存在します。そのため大規模な障害に繋がるソフトウェアの不具合が流出しないよう、網羅的に様々な観点で十分なソフトウェアの検証を実施しています。</p> <p>また、更新ソフトウェアを導入する際には、小規模なエリアに展開して正常性を確認した後に全面的に展開を行うことにより、更新ソフトウェアの導入に伴う大規模な障害の発生を防ぐ運用をしています。</p>

## 2. 予備機器の設置による冗長性確保 回答①

質問項目	質問の意図・ポイント	回答
2-1. パケット交換機について予備機器を設置しているか。	<p>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</p> <p>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</p> <p>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</p> <p>交換機の主機器、予備機器それぞれのメーカー（ベンダー）はどこか</p> <p>予備機器を設置していない場合はその理由</p>	<p>● 弊社のパケット交換機は装置全体あるいは部分的に予備を持ち、故障時に切り替える二重化方式を採用しています。また、さらにネットワーク全体で信頼性を向上させるため、図2に記載の通りプール化、N+1冗長、パケット交換機と無線基地局の複数帰属構成としています。（全てのパケット交換機が稼働状態）</p> <p>こうしたネットワーク構成により、以下のように信頼性を向上させることが可能です。</p> <ul style="list-style-type: none"> <li>一部のパケット交換機の故障時に別の交換機に新規呼を接続することができ、サービス中断が回避可能なため、ネットワークの信頼性が向上</li> <li>比較的広いエリアを複数のパケット交換機で制御するため、局所的もしくは急激なトラフィックの偏りがあってもパケット交換機の負荷が均等化され、ネットワークの安定運用が可能</li> </ul>

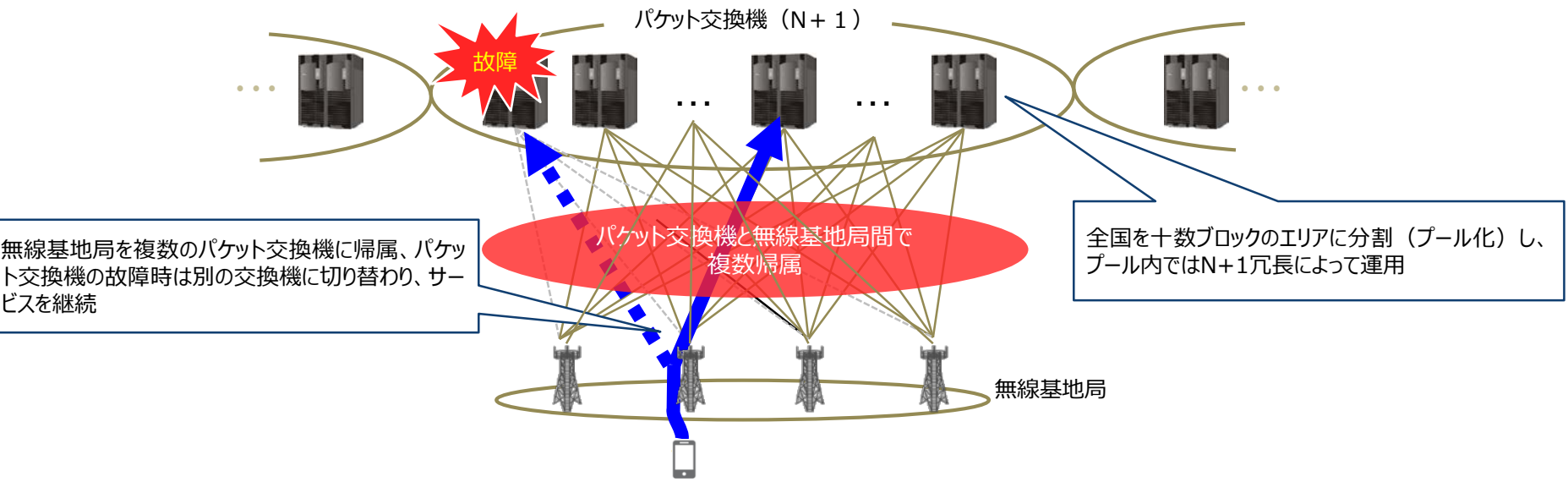
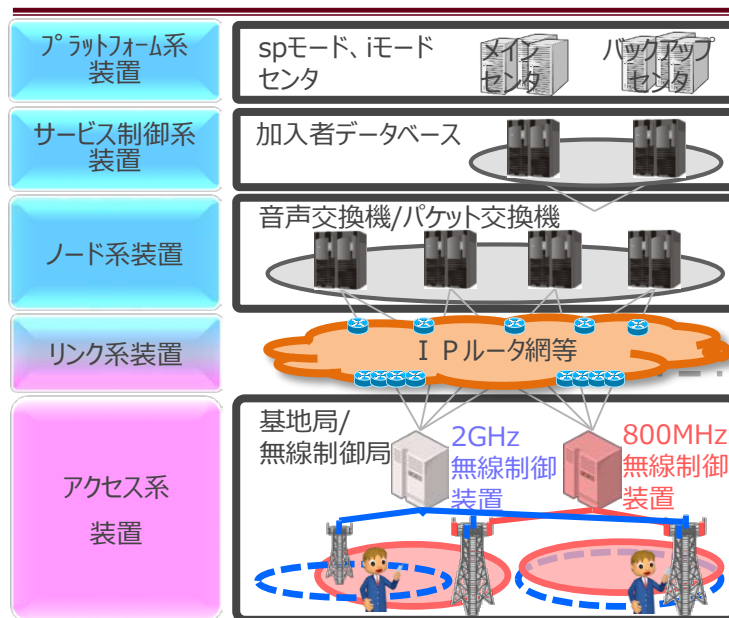


図2 パケット交換機と無線系装置間の複数帰属

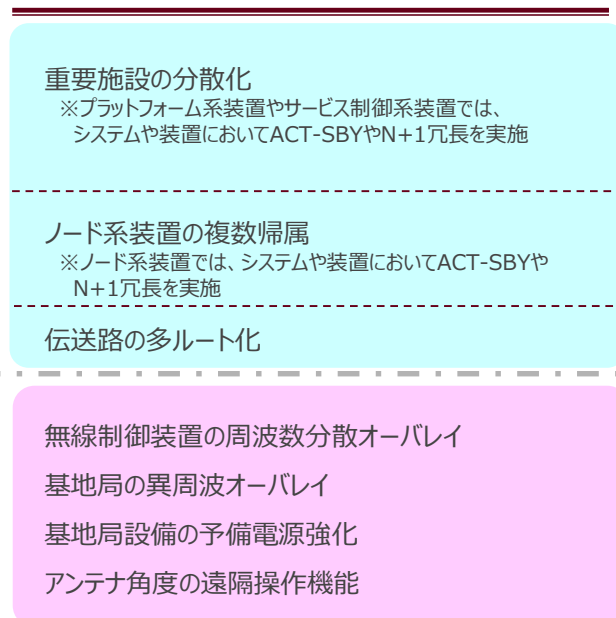
## 2. 予備機器の設置による冗長性確保 回答②

質問項目	質問の意図・ポイント	回答
<p>2-2. 予備機器の設置方針はどのようなものか。</p>	<p>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</p> <p>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</p> <p>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</p>	<ul style="list-style-type: none"> <li>● 交換機等の中核設備に対して、システムの信頼性や障害発生時の影響度等の考え方を定めており、その考え方に基づき予備機器を設置しています</li> </ul> <p>なお、ソフトウェアの不具合により現用・予備の両方の機能が喪失しないよう、新規システム導入や新規バージョンのソフトウェアを導入する際には、機能ごとに導入判定を行うとともに、商用への導入時には、地域を制限した形で商用環境での先行確認による動作を確認したうえで、全国導入を実施しています。</p> <p>特定機能（ソフトウェア）の不具合が装置全機能を喪失させることがないように、機能開始コマンドの細分化等の工夫をしています。</p> <p>各装置の主な冗長構成の取り方と信頼性向上施策を図3に示します。</p>

ドコモのネットワークの構成（概要）



主な冗長構成の取り方と信頼性向上施策



### 3. 障害発生時の対応 回答①

質問項目	質問の意図・ポイント	回答
<p>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。</p>	<p>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</p> <p>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</p> <p>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</p> <p>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）</p> <p>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）</p>	<p>● ネットワークの障害検知に関しては、社内監視部門において障害検知システムを管理しており、システムが発するアラームに応じて予め定められた手順に基づき障害要因の特定および対処を行います</p> <p>ネットワークやサービスを提供するシステムが異常を検知した場合、監視部門において初動措置内容を定め、早期復旧に向けた手順を明確に定めています。</p> <p>具体的な初動措置内容としては、保守者が装置から出力されるアラーム内容に基づき、確認ポイントや措置内容・手順等をマニュアル化しています。</p> <p>また、保守者の初動措置で復旧しない場合、社内でのエスカレーションルールを定めており、自社やベンダー等を含めた技術支援体制等に移行するルールを定め、障害原因を速やかに切り分け判断できる体制構築ルールにて運用しています。</p> <p>さらに、自社とベンダー間の連携では、平素から緊急時の連絡者や連絡先、指揮命令系統をあらかじめ情報交換するなどの連携を行うとともに、異常時においては、発生した時間や内容及び、措置内容等を共有することで迅速な復旧に向けた取り組みを実施しています。</p> <p>なお、監視システム自体も2重化されており、東京・大阪の監視拠点のうち片方の拠点が被災しても、NWの監視措置を継続させるために、2拠点オペレーションを構築しております。</p>

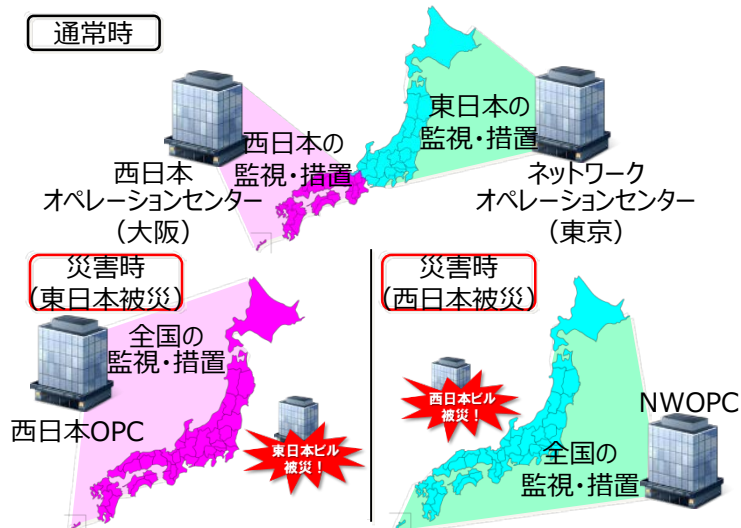
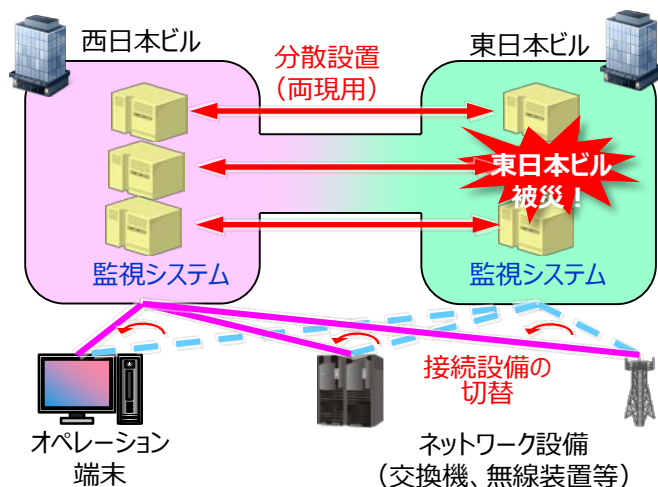


図4 監視システムの2拠点化および災害時の東西代行

### 3. 障害発生時の対応 回答②

質問項目	質問の意図・ポイント	回答
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	<ul style="list-style-type: none"> <li>● <u>障害発生時の状況共有については、対応マニュアルに沿った対応を実施しております</u></li> </ul> 社内では、ネットワークやサービス障害が発生時の全社的な対応マニュアルを定めており、そのマニュアルの中でフロントライン（コールセンターや販売代理店等）に対して情報共有ルールを定めています。フロントラインへの利用者対応は、故障状況の共有やQ&A等を準備し、速やかに共有しています。
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	<ul style="list-style-type: none"> <li>● <u>障害発生時のお客様影響を極小化するよう対策を実施しています</u></li> </ul> 障害発生時のお客様影響を極小化するよう予備機器を設置し、通信を確保する対応を実施しています。更に障害発生時に初動措置で復旧しない場合等は、お客様影響を最小限とする措置や代替手段を検討して対応しています。  なお、障害や災害時において緊急通報接続を確保するため、規制をコントロールすることで、緊急通報接続を確保する取り組みを実施しています。  また緊急通報に限った話ではありませんが、仮想化技術によるオートスケーリングやオートヒーリング等によってネットワークの信頼性を向上させる取り組みも行っています。



## 4. リスク管理 回答

質問項目	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	<ul style="list-style-type: none"> <li>● <u>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おります</u></li> </ul> <p>サービス継続のため、電気通信設備の位置づけにより信頼性の考え方を定め、各システム単位で不稼働率を定めてランク付けを実施しています。</p> <p>ランク付に応じて、現地駆け付け時間などSLAに違いを作っており、装置の種別ごとにSLAを設けて、その考えに基づき対応しています。</p> <p>SLAに基づく対応状況については、評価指標を定め、経営層も確認しています。</p>
	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	