

情報通信審議会 情報通信技術分科会
I Pネットワーク設備委員会（第 45 回）
議事概要

1 日時

平成 31 年 1 月 18 日（金）10 時 00 分～11 時 20 分

2 場所

総務省 8 階 第 1 特別会議室

3 出席者（敬称略）

（1）委員会構成員

相田 仁（主査）、岡野 直樹（主査代理）、有木 節二、内田 真人、江崎 浩、尾形 わかは、片山 泰祥、前田 洋一、松野 敏行、向山 友也、村山 優子

（2）オブザーバ

高嶋 幹夫（（一財）日本データ通信協会）、藤田 周（（一社）情報通信エンジニアリング協会）、山内 明（（一社）情報通信設備協会）、桂 一詞（日本電信電話株式会社）、小畑 和則（株式会社 NTT ドコモ）、甘楽 雅和（KDDI 株式会社）、喜安 明彦（ソフトバンク株式会社）、渡部 康雄（ソフトバンク株式会社）、カーン アシック（楽天モバイルネットワーク株式会社）

（3）事務局（総合通信基盤局 電気通信事業部）

秋本 芳徳（電気通信事業部長）、藤田 和重（電気通信技術システム課長）、井手 信二（電気通信技術システム課認証分析官）、佐伯 宜昭（安全・信頼性対策室企画官）、影井 敬義（電気通信技術システム課課長補佐）、佐々木 信行（電気通信技術システム課課長補佐）、岡 元紀（安全・信頼性対策室課長補佐）、大内 康次（事業政策課調査官）

4 議事

（1）開会

- ・相田主査より、今回合合では本委員会におけるこれまでの 2 回のヒアリング及び前回の主査ヒアリングの内容や議論を踏まえた検討を行う旨、及び、ソフトウェアの信頼性に関する議論の参考とするため、平成 30 年 12 月 6 日に発生した携帯電話の通信障害の内容や対応について、ソフトバンク株式会社より説明してもらう旨の説明があった。

（2）議事

① IoT の普及やネットワーク仮想化等に対応した技術基準及び資格制度等について

- ・事務局（影井課長補佐）より、資料 45-1 及び参考資料 45-1 に基づき、IoT の普及やネットワーク仮想化等に対応した技術基準及び資格制度等、電気通信設備の安全・信頼性の確保に関する現行制度等について説明があった。
- ・ソフトバンク株式会社 喜安部長より、資料 45-2 に基づき、平成 30 年 12 月 6 日に発生した携帯電話サービスの重大事故について説明があった。
- ・主な質疑は以下のとおり。

【相田主査】

ソフトバンクの説明について、交換機のソフトウェア切替時には旧バージョンと現バージョンの並行運用を行うとのことだが、東日本ネットワークセンターと西日本ネットワークセンターに冗長化されているが、何台かが旧バージョン、何台かが新バージョンで並行運用されたという理解でよいか。また、1台の上でVMで両方動いたということではなく、機器ごとに動いたという理解でよいか。

【喜安オブザーバ】

ソフトウェアの更新期間においては、順次更新作業を行い、全体で約1.5ヶ月かけて行った。その期間において、ご理解のとおり、新旧のバージョンが並行して運用された形となっている。また、1台の上でVMで動いたのではなく機器ごとに動いたかという点については、ご理解のとおり。

【内田構成員】

資料45-1の17ページの②ソフトウェアの信頼性の確保について、①ハードウェアの汎用化に伴う機能維持・冗長性の考え方とも関係するが、今回のソフトバンクの事故も関係していると思う。

ソフトバンクから、マルチベンダーで今後対処していくとのことであったが、確かにマルチベンダー化は今回のケースに関しては、効果的な対策の1つではあると思う。しかし、運用の複雑化のような側面など、良し悪しがあり、一概に良いとは言い切れない。ソフトウェアの信頼性の確保や冗長性を議論する際には、リスク評価や管理などを踏まえ、トータルで考え、何が良いか考えるべきであり、今回はあくまで1つの事例であり、一般化してしまうのは危険だと思う。

【村山構成員】

事故の原因が証明書の有効期限切れとわかるまで、どのくらいかかったのか。また、これは世界各国で同時に起こった事故であるため、同じソフトを使用しているところが危機管理の意味で情報共有すると、より発見が早かったのか。あるいは原因を突き止める際に、JPCERTやSIRTなどのような、ベンダーオリエンテッドでなく、ユーザー同士で行う情報交換はあったのか。

【渡部オブザーバ】

障害発生時点では、短期間で復旧させることを優先し、原因追究している訳ではないが、ベンダーと会議しながらの復旧作業の中、原因はわからないが、海外でも同じような現象が同時に起きているという情報がまず入ってきた。しばらく時間が経つと、同じソフトウェアの同じバージョンを使用する事業者にのみ障害が起きていることがわかったため、原因は不明だが、異なるバージョンに直せば復旧することが分かったため、復旧させたということが実態。

原因そのものについては、復旧作業と同時にベンダーにおいて解析していたため、ある程度、今回の証明書のところが原因であると分かってきていたが、最終的に確定したのは、復旧した後になる。

【村山構成員】

原因を突き止めるまでに、どのくらいの時間がかかったのか。

【渡部オブザーバ】

少なくとも今回の証明書が原因であるということについては、ベンダーからの公開情報も色々出ており、発生した当日には分かっていた。ただ、復旧作業自体においては、どうしても復旧を優先するために、何が原因だということまで追究されなかった。

【相田主査】

確認になるが、基本的にソフトバンクが言われた情報は、機器ベンダーのエリクソンとのやりとりで把握したものであり、海外の事業者と直接やりとりしたということではない、ということでしょうか。

【渡部オブザーバ】

ご理解のとおり。

【江崎構成員】

今回の事故に関して、旧バージョンをバックアップにしていたので戻れたということは、非常に褒めていただいてもいいような内容かと思う。他のところではなかったということも伺っており、もちろん事故を褒めるわけではないが、そのような対策をきちんとできていたということは1つ申しておいたほうがいだろうと思う。

資料 45-1 の 17 ページ、17 ページについて幾つか。

最初の①について、「ハードの汎用化に伴う」というよりも、内容としては仮想化の話。したがって、「ハードの仮想化に伴う」というのが正確な気がする。ハードが汎用化すると、ハードウェア的な多様性というか、チェックするポイントは逆に減ってくるので、ハードウェアに対しては多分楽になる。一方で仮想化しているということなので、チェックするところが少し変わってきているという意味においては、汎用化という言葉よりも仮想化のほうが正確な気がした。

さらに、②のところのポイントかとは思いますが、ある意味、高度のブラックボックス化という話を考えていくと、対策にも入ってくるが、多分ソースコードのチェックを可能にするという、契約関係の部分も入ってくる。インタラクティブプロパティ管理に関しての契約条項をどうするかということにも関係するかと思うが、それが単独でソースコードチェックが全部できるほどリソースを各社持っているわけではないと思うため、そうすると、このあたりのソースコードチェックをどうしていくか、あるいは導入するときのアップデートのソースコードに関してのチェックをどうするのかということが問題としては入ってくるだろう。

また、⑤について、2番目のポツ「ソフトウェアがAPIを通して連携すると、E to Eで機能が実現される形態になり」というのは、多分読んでもわからないと思う。1つ言えることは、エンド・ツー・エンドに新しい機能がダウンロードされながらエンド側にインストールされているというような話を書いてあると思うので、もう少し、丁寧に書かないとまずいと思う。というのは、エンド・ツー・エンドの次に、⑥にも関係するが、スライシングの定義も、いわゆるデータプレーンのスライシングのような話は昔からある話。ネットワークとしてのバーチャライゼーションが行われている。ただ、今起こっていることは、ファンクション部分のSDNとしてのスライシングということをしっかり言わないと、問題点を正確に把握できないのではないかと。

それから、⑥の前のフル仮想化を見据えたということについて、フルである必要は全くなく、やはり

仮想化を見据えた上での課題と捉えたほうがいいのではないかと。これは多分5Gコアが最初のところになってくるかもしれないが、同じような問題は既にデータセンターの中では起こっているわけで、そういう意味で、「仮想化を見据えた将来の課題」が正確であり、少しこの書き方の用語の使い方とかを正確にしたほうがいいのではないかと思った。

もう一つは、対策としてのブラックボックス化に対してどのようにしていくかというところを考える必要があると思う。

【相田主査】

事業者に話を伺った範囲内では、現時点では極めてコンサーバティブというか、汎用ハードだが、既に規格化された全く同じハードのラックを幾つか並べ、容量が足りなくなったときにということは考えているが、このハードの上でこのソフトが動いているというようなことでスタートされている。今後いわゆるエッジコンピューティングというか、いろいろな機能がネットワークの中のセンターで動いていたものが、ある時点でエッジのほうに動くようなことになってくると、メモリ容量や、アクセラレータがついている・ついていないなど、違う環境にソフトが移ったりすることがあり得るということになる。それこそ仮想化がどこまで完全かということにも関係するかもしれないが、実際に本当のハードが微妙に違う上でソフトが動く可能性があるということになるとまた一段難しくなってくると思う。

【松野構成員】

資料45-1の2ページ目のスケジュールでイメージを確認させてもらいたい。12月からの欄の一番下に、ネットワーク仮想化に対応した技術基準（追加）というものがあって、短期的な課題を整理し、例えば技術基準適合自己確認の方法などについて追加する、と記載があり、第二次報告案が3月に出る、と解釈した。

参考資料45-1の4ページ目に一覧の表があるが、先ほどのスケジュール、線表で書いてある技術基準適合自己確認の方法の見直しというのは、例えばこの4ページの右側の届出書類のどこがどう変わるか、を示す、という解釈でよいか。

【事務局（影井課長補佐）】

ご理解のとおり。本委員会や主査ヒアリングで議論があったとおり、参考資料45-1の4ページのような届出書類の規定は物理ベースが前提となっており、今のままでよいのか、事業者がこれを参照して書類に記載するときに事業者によって解釈が紛れたり、共通認識を図れないと問題であるため、これを明確化するために、例えばガイドラインやマニュアルを整備する必要があるのではないかと、といった御意見、御議論がありましたので、これらの点はこの短期的な課題の中で整理していくものの1つと考えている。

【松野構成員】

資料45-1の11ページ目に主査ヒアリングの概要があり、その下半分に、当面は大きく見直す必要はないが、仮想化技術の特性に応じた自己確認の説明方法については一部議論が必要、とある。これだけを見ると、今年の3月に自己確認の届出書類をこう直すとかいうものが出てこなさそうなイメージを持った。なので、どこがターゲットになっているかということをもう少し具体的に言っていたら

と見やすいと思う。

【事務局（藤田課長）】

今ご指摘の点は、例えば資料 45-1 の論点を書いてある 17、18 ページ目の③番の物理構成と論理構成の把握のあり方というところと、参考資料 45-1 の 4 ページ目の右側の届出書類が深くリンクしており、こちらに関しては、可能であれば 3 月までに一定の方向性を出していただきたいと考えている。

併せて、17 ページ目、18 ページ目全てではないが、例えば②番のソフトウェアの信頼性の対策についても、完璧な対策というところまで行かないにせよ、当面これぐらいは必要なのではないかとこのものがあれば、こういった点もやはり 3 月までにご議論いただければと考えている。

【相田主査】

私のほうからも補足させていただく。先ほどの資料 45-1 の 15 ページ目に、実際の例ではないが、現在事業者から出している図の例がある。全部、設備の箱になっており、今後これでいいのか、という点について、事業者の話をお伺いすると、直近では大体これでそれほど外してないということだと思う。

先ほどのように、当然これは本来設備というよりは機能であるべきであり、それが将来的にこちらで動いているソフトがこっちに移動したりするということがあるのだとしたら、それをこの絵の上にどのように描きあらわしたらよいかなど、そのようなことはおいおい必ず見直さなければいけないということになるのだろうと思いつつ、3 月までに大急ぎで修正すべき点というのはそれほど多くなさそうであるということが、先日行った主査ヒアリング等の印象。

【内田構成員】

先ほどの発言にまた関連してもう少し付け加えさせてほしい。資料 45-1 の 17 ページ目の②の点線の四角で囲われた 2 つ目のポツのところ、「緊急点検を実施し」という表現が使われている。点検というと、チェック項目があって、これはできているかどうかみたいな形でチェックをしていくということとを連想するわけだが、今回のようなソフトウェアの信頼性にかかわるような事案の場合に、技術的にも何をチェックしたらいいのかがそもそもわからないような状況であると思っている。もちろん、先ほどの例えば旧バージョンをきちんと持っているかどうかというような、できることもあるかとは思いますが、危機感は理解するのだが、そもそも点検できる項目がわかっていないという状況でもあるということとを認識した上で緊急ヒアリングことをするというような方向でやっていただけたらと思った。

【相田主査】

このページのタイトルは「これまでのヒアリングを踏まえた主な論点」となっていて、この点線の枠の中は、この委員会として何かしたというより、総務省が独自に行われる施策であり、それをこの委員会で活かしていただきたい、と考えてよろしいでしょうか。

【事務局（藤田課長）】

ご理解のとおり。資料 45-1 の 17 ページ目の②を御議論いただくに当たり、本日ソフトバンクからも御説明いただいたが、さらに他事業者の状況も含め参考になる情報が必要かと思っており、それを総

務省として、この会議の終了後、点検、調査をし、その結果を次回の会合までに取りまとめて何らかの形で提供したいと思っている。

詳細は今後決定するが、調査項目としては、ソフトウェアの管理の仕方や冗長化の方策をどのように捉えているのかといった点を中心にしたと思っている。

ご指摘のとおり、あらかじめ質問を確定するのは確かに難しいと思っており、その点に関しては、事業者には手間にはなるが、必要に応じて議論、調整もさせていただきながら進めていきたいと考えている。

【向山構成員】

今日のソフトバンクの障害等もお伺いすると、資料 45-1 の 18 ページ、これまでのヒアリングを踏まえた主な論点の④の専門性、知識、能力について、今回のソフトバンクのようなソフトウェアに絡む故障を切り分けて立ち直らせる専門性、技術と、レガシーと言うと怒られてしまうかもしれないが、ハード的なものを切り分けていく技術は専門性は結構違うと思う。ここにある④のポチの 4 番目に資格者区分の見直しがあるが、今は伝送交換と線路になっている。これを例えば物理的な部分と論理的な部分に分けるということも 1 つの考え方と思った。

【相田主査】

昨日の事故検証会議でもいろいろ議論が交換されたところ、先ほどの点検という言葉にも関係するが、このようなソフトウェアの故障にどう対処していったら良いかというのは、今正解があり、それがなされているかどうかチェックするという段階ではまだない。本委員会では、11 月 20 日までの時点で、やはりこういうことが大事だよねと言っていたところ、タイミングよくというか、12 月 6 日に実例が 1 つ起きてしまった。これを踏まえながら、どのようにしていったら良いかと、これから知恵を集めなければいけない段階であると考えている。

したがって、先ほどの線表の中でも、3 月までに何か結論を出すということではなく、もちろんこの委員会でもご意見を頂戴することになるかと思うが、やはり現場で実際にネットワークを運用しているキャリア方に、こういうことが効果あるのではないかというような、ベストプラクティスというような形で、これからどういうことをやっていったらいいかというのをみんなで考えていかなければならない段階かなと思います。どのような体制でやっていくことが良いのかということも含めて、今日この場でなかなかすぐにご意見というわけにもいかないと思うので、思いつかれたこと等あれば、ぜひ事務局のほうまでご連絡していただきたい。

【村山構成員】

現在、災害情報や災害コミュニケーションに興味があるのだが、この分野は、このような緊急事態管理といって、緊急事態というのは、リスクコミュニケーションのように、初めからわかっているわけではないこと、想定外のことが起こったときにどうするかということがとても大事とされている。先ほど私から原因がどれぐらいの時間でわかったのか、という質問をして、ソフトバンクの方の回答は的確で、原因究明よりもオペレーションが早く復旧するということが先だった。多分緊急管理ではきっとそうなのだろうと思う。先ほどのこれまでのヒアリングを踏まえた主な論点の 17 ページについて、②番のソフトウェアの信頼性確保というのは、初めからわかっていることではないので、想定外のことが起

きたときどうするのか、という手順、原因がわからなくても、動くようになれば初期対応としては良いので、原因究明はその後という感じがした。そういったプライオリティーをはっきりさせるほうが良いのでは感じた。

【江崎構成員】

3月に向けてということからすると、仮想化に伴う、あるいはソフトウェア化によるブラックボックスの問題については、後ろ側のブラックボックスの問題が今回は出てきたという整理をしっかりとしようと思う。それから、仮想化が本格的に進むところに対する検討に着手をし、議論をスタートした。今回ヒアリングしたところ、幸い、いわゆるフルの仮想化というレベルにはなっていないので、今の基準の中で対応できるようなシステム構成になっているということが明らかになったということがポイントだと思う。つまり、1つのハードウェアで1つのファンクションが動いている、かつ、マイグレーションはまだ実際には行われていないので、そうすると、今の枠組は緊急に変える必要はないということが正確なポイントだろうと思う。

もう一つは、先ほど村山先生がおっしゃったように、緊急対策に対して、想定できなかったものがあったということは課題ではあるが、それに対するアクションはしっかりしていただいていると考える。さらに次のステップとして、村山先生がおっしゃったように、会社としてのリスクレスポンスガバナンスが必要になってきますという話が出てくる。それはこの会合の中でも、リスクマネジメントに対するコーポレートガバナンスを、いわゆるルールとしての手順ということにプラスをして、会社経営的なガバナンスとしての構造をきちんとつくらなければいけないという話が出ている。そのあたりが大枠として今回の事故が起こる前にこの委員会としては着手していて、現状では、問題に対しての対応としての枠組みとしては不適切なものにはなっていないし、今の状況であれば大体合致した形で動いていると思う。

【事務局（秋本部長）】

ソフトバンクに確認させていただきたいことがある。資料45-2の3ページに、12月6日の13時39分にLTE交換機向け通信に故障が発生して、LTE交換機被疑を特定するまで2時間15分かかったと記載がある。まず、伝送装置から疑ったということは、どういう理由によるものか。

【喜安オブザーバ】

伝送装置のほうを疑ったのは、今回事象として、LTE当該交換機が全台故障した。交換機の構成として、東西のサイト冗長を含めてサイトも分けて設置しており、その共通部に当たるところ、いわゆる伝送区間でどこか共通部がないかというところで伝送路の切り離し等を行う切り分け作業を行っていた。

【事務局（秋本部長）】

13時39分に故障が発生した後、アラームは、伝送装置からも、LTE交換機からも出ていたと理解してよろしいか。

【渡部オブザーバ】

記載の時系列については、全ての作業が終わった後の判明した後で書いている。13時39分に今回の原因になったLTE交換機向けの通信に故障が発生したということは、あくまで結果がわかってから書いた形になっており、実際の当時の作業については、当然ながらアラームが一斉に上がっているため、LTE交換機向けに通信が行ってないのかどうかというところまでは実際には判断はできていない。これはあくまで時系列を最終的にまとめたものであり、LTE交換機が故障したことが39分ではなかったかという、そうではない。

また、伝送路のところの話は、まず復旧作業において、実際に当日作業していたことがあり、その作業のところをまず一旦は疑い、何もしていない状態のところから1回復旧作業をし、戻したためにこのような書き方になっている。

【事務局（秋本部長）】

そうすると、13時39分の時点では、全国的に故障が発生したということだけわかっていて、個々のユーザーの携帯端末からLTE基地局までは無線が発せられており、その先の疎通ができていないということで、基地局から交換機までの伝送路に係る被疑の特定をまず作業として行ったという理解でよいか。

【渡部オブザーバ】

全国一斉のアラームの中には、当然ながら基地局で全部のアラームが出ており、基地局からその上位の設備にアクセスができていないというところまではわかったため、下から順番に確認をしていったというところ。

【事務局（秋本部長）】

資料45-2の11ページ、デジタル証明書の有効期限の誤処理という記述があり、※印で、「デジタル証明書が誤った形で利用されていました」と記載いただいている。どのように誤っていて、本来どうであればよかったのかという点を教えていただけないか。

【喜安オブザーバ】

資料45-2の10ページ目、左側が一般的な証明書の運用形態で、右側が今回の不具合があったソフトウェアに埋め込まれた証明書の形態を記載したものとなっている。先ほどご指摘いただいた11ページ目のデジタル証明書の有効期限の誤処理というところについては、意図するところとしては、今回ソフトウェアに証明書が埋め込まれていたというところ。本来は証明書を使うのであれば、10ページ目の左側のような形で利用者のほうでも更新時期の確認が可能な形であるべきで、それを誤処理という形で記載している。

【事務局（秋本部長）】

資料45-2の14ページで、今後、新規設備、新規ソフトウェアにおいて、未来日の動作確認を実行するとされている。これまではソフトウェアを導入する際にどのような項目をチェックしていたか、可能な限りで教えていただきたい。

【喜安オブザーバ】

通常ソフトウェアの検証においては、一般的な項目として、機能を追加するものであり、その新しい機能の検証及び元々の既存機能の検証を中心に行うとあわせて、内容に応じて負荷試験等運用を意識した試験は行っている。

【相田主査】

今の質問に関して、私のほうからも補足させていただく。大量のアラームが出てきたときに何が一番本の原因であるのかということは、研究課題にもなっている。昨今の流れでいうと、これはA I の出番というような気がする。ソフトウェア、ハードウェアがどのようなモジュール構成になっているかということ把握できて、このモジュールで障害が起きるとそれこそどのようなエラーメッセージが出てくるかを事前にシミュレーションし、そういうようなものをベースに、現実に出ている大量のアラームの中から、元となる原因がどこであるのか、を即座に突きとめるというのは、現状全部人が経験に基づいてやっているわけであるが、本当にこれはこれから研究課題、A I などが活躍し得る分野なのではないかと思う。

【村山構成委員】

先ほどの未来日動作の確認実行について、昔、2000 年問題があった。あのときどうしてあのよう問題なく過ぎたかというのを検証し、どういう対応をとったのかを調査してもよいのではないか。今は状況が違うと思うので、同様なことをするにはどうしたら良いのかを考えれば、対策となる可能性もある。

【江崎構成員】

未来日動作の確認というのは、今回の問題に対してのことではなく、あまり強調するのではなく、ラボ試験の検証項目を根本的にもう一回しっかりチェックしなければいけない。それで、秋本部長は何をやっていたのかということをお聞きになったと思うが、そうすると、どこをプラスしなければいけないかというところが多分出て、それはもちろん検討中だということになるが、その中で最優先というか、今すぐにはできることとしては、今回の問題に対してはこのチェックを増やすという構造にしておく方が結構かと思う。

【相田主査】

今回はベンダーのほうのソフトウェア作成上のミスということだったかと思うが、いわゆるマルウェアのようなものを仕込まれたときに、同じようなことが起こるわけであり、爆弾をどのようなタイミングに仕掛けられるかがわからないため、時刻を進めればチェックできるかということとそんなものではない。

うるう秒をやめようという議論のときに、うるう秒で動作するソフトがあり得る、というような話があるが、そのようなものを事前に検証しようとする、どのような手順でやったらいいのか、ということとはなかなか難しい。未来日はもちろんやらないに越したことはないが、今、江崎先生がおっしゃるように、これをやったらそれでいいかということ、そうではないというのは明らかと思う。

【尾形構成員】

今回の起こった事故において、ここをこうすれば避けられるかもしれないという今後のこともあるが、業界全体の課題ということだとすると、今後ここを直していったらということはあるが、例えばマルチベンダー化をすれば、今回のことは防げるが、別の観点でやはり複雑になって別のリスクが生じるかもしれないものであり、新しく何か対策をとるといのはなかなか難しい。難しいとってやらないわけにもいかないが、逆に今回これをやっておいてよかったというようなことがもしあれば、それを教えていただきたい。

先ほど江崎先生から、古いバージョンのバックアップをとっておいたことは1つ、不幸中の幸いというか、よかっただろうとのご発言があったが、他にも、こういうことをやっておいたから少し軽く済んだ、復旧が早く済んだというようなことがあれば、他の会社や他のベンダーはやってなかったことに対して、うちもそれはやったほうがいいねという、何か効果的だったものがあれば教えていただきたい。

【渡部オブザーバ】

今この段階ではないが、ヒアリングをされるという話があったので、そのようなところでいろいろとフィードバックさせていただければと思っている。

【相田主査】

私どもで見たところ、バックアップがとってあったということ、さらに大きなことでいうと、3Gが横にあったことで、少なくとも緊急通報についてはそちら経由で、少し時間はかかったが、確保できたというところで、これも冗長化ということは今後考えるに当たっての1つの参考にはなると思う。

(3) その他

事務局より、次回のIPネットワーク設備委員会は、2月14日（木）15時から開催予定である旨の説明があった。

以上