調査報告書

（最終報告書）

＜要約版＞

2012年7月31日

ファーストサーバ株式会社　第三者調査委員会

2012年7月31日

ファーストサーバ株式会社　御中

[第三者調査委員会]

委員長　葉玉　匡美

委員　　三輪　信雄

委員　　柴野　相雄

目　次

第１　調査の概要

１　委員会設置の経緯

ファーストサーバ株式会社（以下「ファーストサーバ」という。）は、2012 年 6 月 20 日から 21 日にかけて発生した、ファーストサーバが提供するレンタルサーバーサービス（以下「本サービス」という。）の一連の事故（以下「本件事故」という。）について、専門的及び客観的な見地からの原因調査や再発防止策等の策定が必要と判断し、ファーストサーバと利害関係のない外部の専門家で構成される第三者調査委員会（以下「本委員会」という。）を、2012 年 6 月 28 日付で設置した。本委員会の構成は、以下のとおりである。

委員長　葉玉　匡美　（TMI 総合法律事務所　弁護士）
委員　　三輪　信雄　（S&J コンサルティング株式会社　代表取締役）
委員　　柴野　相雄　（TMI 総合法律事務所　弁護士）

２　本件事故の概要

本件事故は、大別して 2 件の事故に分けられる。

（１）　1 件目の事故は、2012 年 6 月 20 日午後 5 時ころに、本サービスで使用されている特定のサーバー群に対して実施されたメールシステム障害解消のためのメンテナンスにより、本サービスの顧客の大量のデータが消失したという事故である（以下「第 1 事故」という。）。

（２）　2 件目の事故は、第 1 事故によって消失した大量のデータを復元するために、同月 21 日午前 9 時ころに、消失したデータを復元できるプログラムを用いて、消失データの復元を実行し、その結果をリカバードファイルとして、本サービスの顧客に提供したところ、想定した以上の量のデータが想定外の場所（データ領域）に復元された事故である（以下「第 2 事故」という。）。

３　調査の目的

本報告書は、2012 年 7 月 30 日までの調査に基づき、次項記載の諮問事項に関して、本報告書提出時における本委員会の見解を報告することを目的としたものである。

なお、本報告書は、ファーストサーバが本委員会を構成した目的に照らして、あくまで中立・公正な立場から、当該諮問事項について本委員会の見解を述べるものであり、関係者の個人的な法的責任の追及を目的とするものではない。

４　諮問事項

ファーストサーバより、本委員会が諮問を受けた事項は、第 1 事故及び第 2 事故に関する

① 原因探究のための事実調査

② 過失の内容及びその程度に関する検討

③ 再発防止策の適切性の検討

の3点である。

5 調査期間

2012年6月28日から同年7月30日まで

6 調査方法

本委員会は、本報告書を作成するに当たり、ファーストサーバから開示された資料、ファーストサーバの役員・従業員に対する事情聴取において取得した事実、及び、インターネット情報を含む一般に入手可能な公開情報に基づき、調査を実施した。

第2 第1事故について

1 調査によって判明した事実

(1) システム変更に関する社内マニュアルの存在

ファーストサーバでは、システム変更のための社内マニュアルが存在し、通常は、当該社内マニュアルに従ってシステム変更が行われていた。当該社内マニュアル等によれば、システム変更は、通常、次のような手順で行われることとなっている。

① 担当者は、更新プログラムを作成し、検証環境下において、更新の対象となるサーバー群（以下「対象サーバー群」という。）で実行する。

② 担当者は、検証環境下において不具合がなければ、上長に対し、「先行ユーザー」（対象サーバー群全体に更新プログラムを実行する前に、先行して更新プログラムを実行するサーバーを利用している少数のユーザーをいう。）に対する更新プログラムの適用の許可を申請する。上長は、検証環境下の結果をチェックして問題がなければ、「先行ユーザー」に対する適用を許可する。

③ 担当者は、更新プログラムを、「配布システム」を利用して「先行ユーザー」が利用しているサーバーに送付して実行し、不具合をチェックする。そして、担当者は、先行ユーザーが利用するサーバーに不具合が生じていなければ、更新プログラムを、「配布システム」を利用して、対象サーバー群に送付して更新プログラムを実行する（このように対象サーバー群全部について更新プログラムを適用することを「本番」という。）。

④ なお、更新プログラムは、プライマリーディスクにのみ適用され、バックアップディスクには適用されない。バックアップディスクのシステムは、更

新後のプライマリーディスクが毎日午前6時30分に自動的にバックアップディスクにコピーされることによって、更新される。

（2）　担当者による本番環境下での独自のメンテナンス方法

（1）記載のとおり、ファーストサーバでは、システム変更について社内マニュアルが存在し、第1事故の原因となったシステム変更の担当者であるA氏（以下「担当者A」という。）以外の担当者は当該社内マニュアルに沿ってシステム変更を行っていたが、担当者Aだけは、配布システムが導入される以前から、自ら作成した更新プログラムを利用する等、独自のシステム変更方法（以下「独自方式」という。）を確立し、当該社内マニュアルに規定されている配布システムを利用せず、独自方式でシステム変更を行っていた。

（3）　メンテナンスの実施及び第1事故の発生

第1事故が発生した状況は、以下のとおりである。

①　担当者Aは、2012年6月20日午後5時ころ、メールシステムの障害対策を行うため、対象サーバー群についてメンテナンス（以下「本件メンテナンス」という。）を行うこととした。

そこで、担当者Aは、過去に自分が作成した更新プログラムを改変して、本件メンテナンスで使用する更新プログラム（以下「本件更新プログラム」という。）を作成したが、その際、過去に記述していた「対象外サーバー群についてファイルの削除を行う旨のコマンド」を消し忘れるという不具合（以下「本件更新プログラムの不具合」という。）を生じさせた。

②　担当者Aは、更新プログラムを作成後、検証環境下で、対象サーバー群に更新プログラムを送付して実行した。本件更新プログラムの不具合は「対象外サーバー群についてファイルを削除する」という内容であったため、対象サーバー群については、悪影響（データの消失）は発生せず、その結果、担当者Aは、本件更新プログラムの不具合を確認することができなかった。

③　担当者Aは、検証後、上長に許可を得ようとしたが、上長が会議中であったため、すぐに許可を取ることができなかった。しかし、担当者Aは、

・　前日に、上長に対し、本件メンテナンスを行う予定であることを報告していたこと

・　本件メンテナンスがメールシステムの障害を防止するために空ファイルを対象サーバー群に作成するという簡単で、それ自体はリスクが低い作業であったこと

等から、上長の許可を得なくても、本番のシステム更新を行って良いものと判断した。

④　また、担当者 A は、本件メンテナンスが簡単かつリスクの低いものであることから、「先行ユーザー」への適用というプロセスを省き、いきなり「本番」のシステム更新を行ってよいものと判断した。

⑤　そこで、担当者 A は、本番環境下において、独自方式に基づき、更新プログラムを、対象サーバー群のみならず、対象外サーバー群を含む全てのサーバー群に送付して実行し、プライマリーディスク及びバックアップディスクを同時に更新した。

その結果、本件更新プログラムの不具合により、対象外サーバー群のデータがバックアップを含めて消失した（第1事故の発生）。

⑥　担当者Aは、同日午後5時48分ころ、監視システムによるアラートにより異常に気がつき、本件更新プログラムを緊急停止したが、その時点で、既にほとんど全ての対象外サーバー群のデータが消失していた[1]。

2　過失の内容及びその程度

（1）　注意義務の内容

ファーストサーバは、第 1 事故発生時において、本サービスの顧客に対し、安全管理上必要な作業手順等の内部規程等の作成、運用、監査等の必要な措置を講じて、本サービスにて保管されているデータを安全に維持、管理し、これを損壊又は消去してはならない義務を負っていた。

（2）　過失の内容

ファーストサーバには、第 1 事故において、以下の管理上の過失を前提として、運用上の過失が認められる。

ア　管理上の過失

①　ファーストサーバにおいて、システム変更を行う場合には、システム変更のための社内マニュアルに従わなければならないこととされていたにもかかわらず、担当者 A は、従来から、当該社内マニュアルに従わず、更新プログラムの不具合によって全サーバーのプライマリーディスク及びバックアップディスクに障害が生ずるリスクのある独自方式でメンテナンスを行っていた。

②　上長が、①を認識していながら、これを容認していた。

イ　運用上の過失

担当者 A が不具合のある更新プログラムを作成し、これを上長の許可無く、独自方式に基づいて全サーバーで実行した。

---

1 ファーストサーバによる2012年6月26日付「障害の対象および対象範囲以外のサービスに関するご報告」においては、障害の対象サービスを「5698件」としたが、その後に被害を受けなかったサーバーが存在したことが判明しており、実際には5676件であった。http://support2.fsv.jp/urgent/service.html

（3）　過失の程度

担当者Aが、約10年前から独自方式でメンテナンスを行ってきたにもかかわらず、第1事故以前は重大な事故はなかったこと、及び、第1事故に関して本委員会が認定したファーストサーバの過失のうちのいずれか一つでも存在しなければ第1事故が生じなかったことを勘案すれば、ほとんどの者が第1事故を容易に予見することができたという評価をすることは困難であり、第1事故に関する過失は、故意と同視できるほどの悪質な過失（重過失）には該当しないものと解される。

しかし、第1事故は、不備のある更新プログラムによってデータを消失させたという積極的な過失であること、担当者Aが、ファーストサーバが作成、実施をしてきたシステム変更のための社内マニュアルを故意に無視し、上長もこれを是認することで、積極的に情報セキュリティの不備を生じさせていたこと、担当者Aが、本来上長の許可が必要であることを認識しながら、無許可で本件メンテナンスを行ったことを考慮すれば、ファーストサーバの過失は、軽過失の枠内ではあるものの、比較的重度の過失であったものと解される。

3　再発防止策の適切性

本委員会は、2012年7月24日付で、ファーストサーバから、ファーストサーバ自らが認識している第1事故の原因分析及びこれに対する再発防止策について、最終案の開示を受け、その内容の適切性を検討した。

（1）　第1事故の原因分析

ファーストサーバは、第1事故の根本原因を、以下のとおり分析している。

ア　開発・運用管理体制の問題

①　更新プログラムのバグによる事故を未然に防止するための仕組みが組織的に欠落していた。

②　基準策定、標準化を進めていたが、遵守しない担当者の存在を管理責任者が黙認していた。

③　全社として業務ルールの遵守状況や業務のリスクマネジメントの有効性を客観的に判断するスキームを有していなかった。

イ　脆弱なシステム構造の問題

バックアップを同一筐体内に1次バックアップまでしか保存しておらず、バックアップとしては不十分な状態であった。

ウ　データ消失に対する希薄な危機意識

プログラムのバグにより、データが完全に消去出来てしまう運用方法を許容する危機意識の希薄さがあった。

（2）再発防止策

ア　総論

ファーストサーバは、上記（1）ア～ウの3つの根本原因毎に、以下のとおり、再発防止策を 4 つの項目に分けて検討している。なお、再発防止策の具体的内容については、次項以下で具体的に説明する。

No	再発防止策	根本原因との関連
1.	開発・運用プロセスの見直し	ア　開発・運用管理体制の問題
2.	牽制（開発・運用）を含めた体制の確立	
3.	システム変更業務の運用移管と分掌整理	
4.	2次バックアップの取得	イ　脆弱なシステム構造の問題 ウ　データ消失に対する希薄な危機意識

なお、再発防止策 No. 1～No. 3 に関しては、下表のとおり、第1事故の対象となったサービスのみならず、同一の業務体制で提供される同型のサービスをも、再発防止策の対象としている。

第1事故の対象となったサービス	ビズ・シリーズ、ビズ2・シリーズ エンタープライズ3・シリーズ、エントリー・ビズ EC-CUBE クラウドサーバー、サイボウズ専用サーバー
同一の業務体制で提供される同型のサービス	ビジネス・シリーズ（エントリ、スーパービジネス含む。） ギガント／ウルトラビジネス／オルテビズ／ライトビジネス ギガントmini／ギガント2／ウルトラビジネス2／ギガビジネス／ギガビジネスプラス エコノミー・シリーズ エンタープライズ・シリーズ、エンタープライズ2・シリーズ ビギーガ、ギャラクティカ1／ギャラクティカ2

但し、再発防止策No.4に関しては、下表のとおり、まずは第1事故の対象となったサービスより実施し、記載のないサービスに対しては、順次実現性を検討し再発防止策の対象とするか否かを検討する予定である。

第1事故の対象となったサービス	ビズ・シリーズ、ビズ2・シリーズ エンタープライズ3・シリーズ、エントリー・ビズ EC-CUBEクラウドサーバー、サイボウズ専用サーバー

イ　「開発・運用管理体制の問題」に対する再発防止策

（ア）　開発・運用プロセスの見直し

「開発・運用プロセスの見直し」として、次の再発防止策を実施する。

①　システム変更のための社内マニュアルを開発プロセス、運用プロセスの視点により検証し、安全性を確認した上で、部内ルールとして再徹底する。

②　潜在的な問題が発見された場合には、リスク分析の上で対処方法を検討する。

③　開発・運用プロセスについて、以下の改定を行う。

a.　運用組織における「リリース作業」の受け入れ厳格化と受け入れ基準の明確化

(a)　本番システムのシステム変更権限を運用部門に限定し組織牽制を明確にする。

(b)　運用部門にて受け入れ業務を定義し、システム変更作業の受け入れを可能とする。

(c)　システム変更のための社内マニュアルに則った受け入れ基準（条件）を定義する。

・　運用部門での配布試験
・　運用部門でのサンプリングによるシステム検証試験
・　各種レビューの実施状況と結果
・　CS部門等関連部門への外部仕様レビュー結果　　等

(d)　リリース作業に関するワークフロー及び条件を運用部門内においても整備する。

b.　完全に排除できないリスクへの対応

(a)　システム変更のための社内マニュアル及び配布システムを利用しても発生するリスクとして重大と判断した以下のケースにおいては、コードレビューの実施についてシステム変更のための社内マニュアルに規定する。

・　プラグインを開発し、システム変更を実施する場合

・　ホスト環境のシステム変更を実施する場合

(b)　その他関連する課題についても、下表のとおり、規定の追加や見直しを実施する。

No	課題	対策
①	検証範囲に関する課題の検討	配布範囲と検証内容の適合性を確認する規定を追加し検証内容の漏れをなくす。
②	バックアップ領域に関する運用の明確化	バックアップディスクへの変更について、明確に禁止した条項がないことから追加し、バックアップディスクの更新禁止を明確化する。
③	プライマリーディスク障害時の運用設計	プライマリーディスクに障害が発生した場合の対策について検討し、リスクの回避を実施する。

（イ）　牽制（開発・運用）を含めた体制の確立

牽制を含めた体制の確立のため、次の再発防止策を実施する。

①　開発、運用組織に関しては兼務者を極力廃止し、責任と役割の分担を明確化する。

②　開発部門と運用部門を分離し、社内ルールの徹底及びシステム変更管理業務の責任範囲を明確化する。

（ウ）　システム変更業務の運用移管と分掌整理

システム変更業務の運用移管と分掌整理に関して次の再発防止策を実施する。

①　システム変更のための社内マニュアルにて記述されているシステム変更に関する業務フローについて見直しを実施し、本番環境下のシステムへのリリース作業を運用部門へ移管することにより、開発担当者の属人的なシステム変更を抑制する。

②　業務移管にあたっては、システム変更のための社内マニュアルの改善にて実施する「①運用組織における受け入れ基準の明確化」に基づいた運用部門での受け入れ精査を実施する。

③　業務フローの見直し（曖昧な内容の排除）を実施し、開発部門と運用部門の業務を明確化する。

ウ　「脆弱なシステム構造の問題」及び「データ消失に対する希薄な危機意識」に対する再発防止策

根本原因である「脆弱なシステム構造の問題」及び「データ消失に対する希薄な危機意識」に関して、再発防止策として、次のとおり、2次バックアップの取得を実施する。

① 毎朝午前6時30分に同一筐体内で取得する現在の運用のバックアップに加え、オペレーションミスや、プログラムのバグなどの影響を受けない外部バックアップシステムを構築し、2次バックアップを追加する。

② 2次バックアップシステムは、バックアップシステム側から本番環境下のサーバーに接続してデータを取得する設計とし、サーバーのオペレーションや更新プログラムの配布システムの不具合によるデータの消失が発生しにくい仕組みとする。

なお、バックアップ周期、世代管理数に関する仕様は、現在策定中である。

（3） 再発防止策の適切性の検討

ファーストサーバの提案する上述の再発防止策は、第1事故の複数の根本原因を前提としたものであり、個々の原因を解消する目的で検討されている。

再発防止策の内容は、根本原因に対応したいずれも具体的かつ現実的な内容であり、これらの予防策が実施され、機能した場合には、今回発生した第1事故を防ぐことができる内容と評価することができる。

従って、第1事故に対する上述の再発防止策は、一般的なレンタルサーバー業者の水準に照らしても、適切なものと評価することができる。

第3 第2事故について

1 調査によって判明した事実

（1） データ消失を想定したマニュアルの不存在

ファーストサーバは、本件事故当時、バックアップディスクの存在により、同業他社と比較して、データ消失に強い仕組みを導入していると自負しており、創業以来サーバー単体でのデータ消失の経験が無かったこともあいまって、データ消失のリスクを想定していなかった。

そのため、ファーストサーバは、データの消失を想定したマニュアルや手順書を作成していなかった。

（2） 復元作業の実施及び第2事故の発生

ア 復元プログラムの検証

ファーストサーバは、第1事故発覚後、顧客に与える損害を可及的に軽減するために、顧客のデータを少しでも復元したいと考え、2012年6月20日午後8時ころ、検証環境下において、オープンソースソフトウェアである復元プログラム（以

下「本件復元プログラム」という。）を用いて、消失データのファイルの復元の検証を行った。

ファーストサーバは、本件復元プログラムがファイルの更新履歴のみを参照するだけで、その他の情報との整合性を確認しないままに強制的にファイル復元する方式の復元プログラムであったが、復元されたファイルに不整合が生じる可能性があることを認識しておらず、技術的な検討も不十分なまま、不完全なデータであっても復元させることが顧客の利益にかなうと判断し、本件復元プログラムで復元したデータを顧客にFTPで提供することを決定した。

なお、本件復元プログラムによる復元により、データの混在又は置き換わりが生じてしまう可能性があることは、技術者には一般的に認識されているが、ファーストサーバの役職員は、特定の顧客のデータに他の顧客のデータが混在するリスクを失念していた。

イ　復元プログラムの実行

ファーストサーバは、アの検証を終えた後、同月21日午前9時ころ、本番環境下で、本件復元プログラムを利用して復元作業を実施し、復元されたデータを、リカバードファイルとして顧客に提供した（第2事故の発生）。

ところが、その後、ファーストサーバは、顧客から、専用サーバー内において、アクセス権限を有していない者から情報を参照できる状態になっているとの連絡を受けて、第2事故に気付き、同月22日午後9時ころ、リカバードファイルの提供を停止した。

ウ　第2事故の発生状況

第2事故の発生後、ファーストサーバは、他の顧客のデータが含まれる可能性のあるリカバードファイルをFTPでダウンロードした可能性のある顧客に対して、ダウンロードしたリカバードファイルを全て削除するように依頼した。本報告書作成の時点では、他の顧客のデータを閲覧することができたという報告は受けておらず、ある顧客のデータが他の顧客に対して漏えいしたという事実は確認されていない。

しかし、サーバーの利用状況等を分析した結果、第2事故により、次のような情報漏えいが生じた可能性はある。

a.　共有サーバー方式

ファーストサーバによる調査の結果、共有サーバー方式では、最大60者の顧客で同じサーバー筐体を共有している。そのため、60者の内の1者でもリカバードファイルを提供したフォルダにアクセスした形跡があった場合は、最大59者の情報が混在していた可能性がある。

解約済みの顧客データに関しても復元された可能性があり、その場合は最大72者の情報が混在していた可能性がある。

b. 専用サーバー方式

ファーストサーバによる調査の結果、専用サーバーが再利用されている場合には、リカバードファイルをダウンロードしたとき、当該専用サーバーを利用していた過去の顧客の情報が復元されて、ダウンロードされた可能性があることが判明した。

他方、現在利用している顧客のデータが漏洩した可能性はない。

c. 漏えい被害の最大範囲

ファーストサーバにおいて、復元データの提供期間中にFTP/POP/IMAPでアクセス履歴があった物理サーバーに収容されたことがある全ての契約者（解約済みを含む。）から、他者にデータをダウンロードされた可能性がない契約者を除いて計算した数は、2359者である[2]。

d. 他社のデータをダウンロードした契約者の最大範囲

ファーストサーバにおいて、復元データの提供期間中にFTP/POP/IMAPでアクセス履歴があった全契約者を合計した数は、145者である。

e. 1者あたりの混在先の最大数

ファーストサーバによる調査の結果、本件復元データの提供期間中に複数の契約者からのFTPアクセス履歴が残っていた共有サーバーがあり、全サーバー中、最大アクセス数は6者であったことが判明した。

そのサーバーに収容されたことがある全ての契約者（解約済みを含む。）は、その6者がアクセスした復元データ全てに自身のデータが混入している可能性がある。

f. アクセスされた物理サーバーの台数

ファーストサーバによる調査において、復元データの提供期間中にFTP/POP/IMAPでアクセス履歴があった物理サーバーの台数は103台である（但し、過去を含めて他の契約者がそのサーバーを利用した経歴がないものは除く。）。

---

2 ファーストサーバによる2012年6月29日付プレスリリースにて「最大2308者」としたが、解約ユーザーの抽出条件漏れ等の作業ミスによる誤りであった。
http://www.firstserver.co.jp/news/2012/2012062901.html

2　過失の内容及びその程度

（1）　注意義務の内容

ファーストサーバは、第2事故発生時において、情報漏えいに関する対策を行い、安全管理措置を定める規程等の作成、運用及びその監督等の必要な措置を講じて、本サービスで取扱うデータを安全に管理し、これを漏洩してはならない義務を負っていた[3]。

（2）　過失の内容

以上の義務に照らせば、ファーストサーバには、第2事故について、次の過失（注意義務違反）が認められる。

①　本件復元プログラムの実行によって、復元したデータに他の顧客のデータが混在する可能性があったにもかかわらず、本件復元プログラムを利用してデータを復元し、FTPによるダウンロードサービスを提供したこと。

②　データが消失した場合を想定したマニュアルや手順書を事前に作成し、これを周知・教育する等の措置を講じるべきであったのに、これらを作成せず、従業員に対しデータが消失した場合を想定した教育等を行っていなかったこと。

（3）　過失の程度

ファーストサーバでは、複数の役職員で消失データの復元に関する検討を行った上で、本件復元プログラムによるデータの復元及び顧客への提供を行っていたにもかかわらず、その過程で、誰も第2事故を予見することができなかったのであるから、ファーストサーバには、故意と同視できるほどの悪質な過失（重過失）は認められないものと解される。しかし、第2事故は、本件復元プログラムによる復元及び復元データの顧客への提供というファーストサーバの積極的な過失によって生じたものであること等を考慮すれば、ファーストサーバの過失は、軽過失の枠内ではあるものの、その過失の程度は比較的重度のものであると解される。

3　再発防止策の適切性

本委員会は、2012年7月24日付で、ファーストサーバから、ファーストサーバ自らが認識している第2事故の原因分析及びこれに対する再発防止策について、最終案の開示を受け、その内容の適切性を検討した。

（1）　第2事故の原因分析

ファーストサーバは、第2事故の根本原因を、以下のとおり分析している。

---

[3] 大阪地判平成18年5月19日判例タイムズ1230号227頁は、電気通信事業者かつ個人情報取扱事業者に該当する事業者が「顧客の個人情報を保有、管理する電気通信事業者として、当該情報への不正なアクセスや当該情報の漏えいの防止その他の個人情報の適切な管理のために必要な措置を講ずべき注意義務を負っていたと認められる」と判示した。

① ファーストサーバが本サービスを開始したときから現在に至るまで、顧客データが消失するという事象は想定されておらず、ルールやマニュアルの類いのものは存在しない。

② そのため、復元プログラムによるデータ復元を検討した過去はなく、復元プログラムを使用した際に発生する技術的リスクの洗い出しが出来ていなかった。

③ このように、技術的リスクに対して熟慮されていない状況であったにも関わらず、第 1 事故によって発生した顧客データの復旧を急ぐあまり、データ復元作業を実施し、復元データを顧客に開示してしまった。

（2） 再発防止策

ファーストサーバは、第 2 事故の再発防止策として、以下の 3 点を挙げている。

① 第 2 事故の前提となった第 1 事故の再発防止策の実施。

② それでも第 1 事故のようなデータの消失事故が発生した場合に備え、データ消失時の対応マニュアルを整備して、第 2 事故のような情報の漏洩事故の発生を防止する。具体的には、データ復旧ソフトによる復旧は実施しないことを明確化する。

③ 第 2 事故と同様に、事前に想定していない事象が発生した際に、場当たり的な対応にならないよう、リスクマネジメントに関する組織を設置し、重大事故発生に備えた社員教育等を実施する。

なお、③のリスクマネジメントに関する組織の設置に関し、具体的には、以下のような対策を検討している。

a. リスクを回避、軽減する目的で「リスクマネジメント委員会」を創設する。

b. リスクマネジメント委員会は、リスクを横断的に統括管理することにより、リスクの未然防止及び危機発生時の迅速な対応の体制を強化し、企業価値の維持・発展・向上を目指すことを目的とする。

c. 様々な対策の実行にも関わらず、リスクが顕在化した場合に備え、対応プロセスを整備する。

d. 自然災害・事故、サービスの事故・不具合、システムやサービスのトラブル、コンプライアンス違反、情報セキュリティ事故、環境問題などの重要なリスクが顕在化した場合、各担当部門は直ちにリスクマネジメント委員会に報告し、対策本部を設置するなど適切な対応によって問題の早期解決や 2 次障害の発生を防止する。

また、②の対応マニュアルの整備に関し、具体的には、以下のような対策を検討している。

a.　通常のハードディスクの障害対応に関するマニュアルに以下の事項を加え、社員教育を徹底し、顧客データの取り扱いに関して、緊急時においても適正な対応がとれるようにトレーニングを実施する。

①　物理的故障、論理的故障、オペレーションミスにより、顧客データの一部又は全ての欠損が生じた場合の対応マニュアルを整備する。

②　影響範囲の規模に応じた対応マニュアルを整備する（初期化手順の整備等）。

③　専用サーバー、共有サーバー共に同基準とする。

④　対応マニュアルには、原則としてデータ復旧ソフト及び専門業者の利用を禁止する条項を盛り込む。

b.　顧客の同意を前提としてデータ復旧を実施することを想定したサービスを設計・提供する場合、運用設計において、他社データが混在しない安全性が確保されていることを条件とする。

（3）　再発防止策の適切性の検討

ファーストサーバの提案する上述の再発防止策は、第 2 事故の複数の根本原因を前提としたものであり、個々の原因を解消する目的で検討されている。

再発防止策の内容は、根本原因に対応したいずれも具体的かつ現実的な内容であり、これらの予防策が実施され、機能した場合には、今回発生した第 2 事故を防ぐことができる内容と評価できる。

従って、第 2 事故に対する上述の再発防止策は、一般的なレンタルサーバー業者の水準に照らして、適切なものと評価することができる。

以上