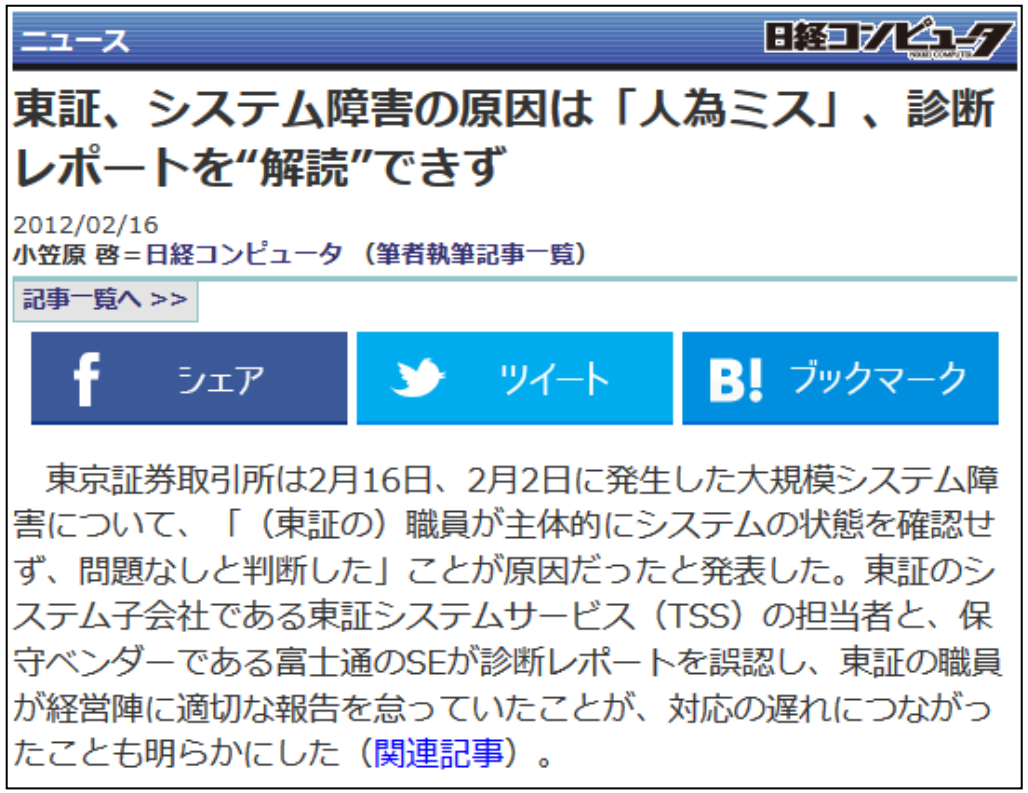
コンピュータ科学III

担当：武田敦志 <takeda@cs.tohoku-gakuin.ac.jp>

http://takeda.cs.tohoku-gakuin.ac.jp/

システム障害の例(1)

- 金融取引システムの停止



ニュース 日経コンピュータ

東証、システム障害の原因は「人為ミス」、診断レポートを“解読”できず

2012/02/16
小笠原 啓＝日経コンピュータ （筆者執筆記事一覧）

記事一覧へ >>

シェア ツイート B! ブックマーク

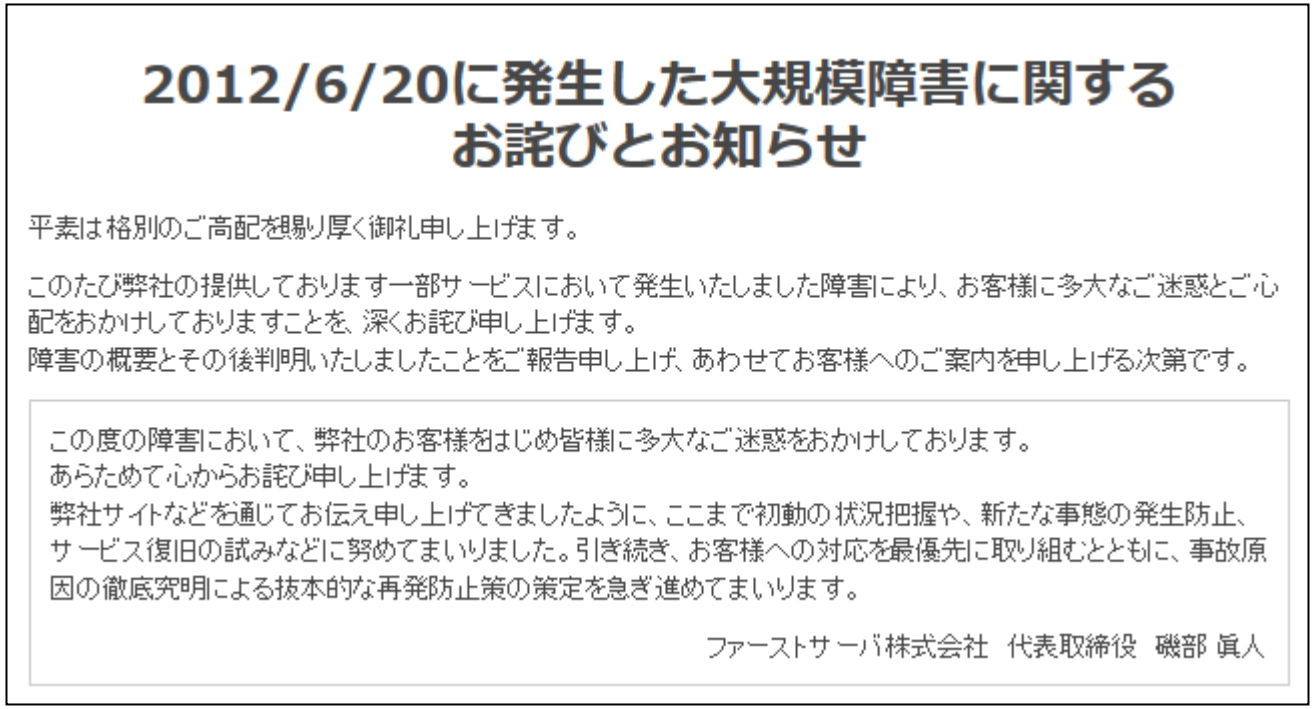
東京証券取引所は2月16日、2月2日に発生した大規模システム障害について、「（東証の）職員が主体的にシステムの状態を確認せず、問題なしと判断した」ことが原因だったと発表した。東証のシステム子会社である東証システムサービス（TSS）の担当者と、保守ベンダーである富士通のSEが診断レポートを誤認し、東証の職員が経営陣に適切な報告を怠っていたことが、対応の遅れにつながったことも明らかにした（関連記事）。

「IT Pro by 日経コンピュータ」のWebページより引用（2014/06）

http://itpro.nikkeibp.co.jp/article/NEWS/20120216/381903/

システム障害の例(2)

- クラウドシステムでのデータ消失



2012/6/20に発生した大規模障害に関する お詫びとお知らせ

平素は格別のご高配を賜り厚く御礼申し上げます。

このたび弊社の提供しております一部サービスにおいて発生いたしました障害により、お客様に多大なご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。
障害の概要とその後判明いたしましたことをご報告申し上げ、あわせてお客様へのご案内を申し上げる次第です。

この度の障害において、弊社のお客様をはじめ皆様に多大なご迷惑をおかけしております。
あらためて心からお詫び申し上げます。
弊社サイトなどを通じてお伝え申し上げてきましたように、ここまで初動の状況把握や、新たな事態の発生防止、サービス復旧の試みなどに努めてまいりました。引き続き、お客様への対応を最優先に取り組むとともに、事故原因の徹底究明による抜本的な再発防止策の策定を急ぎ進めてまいります。

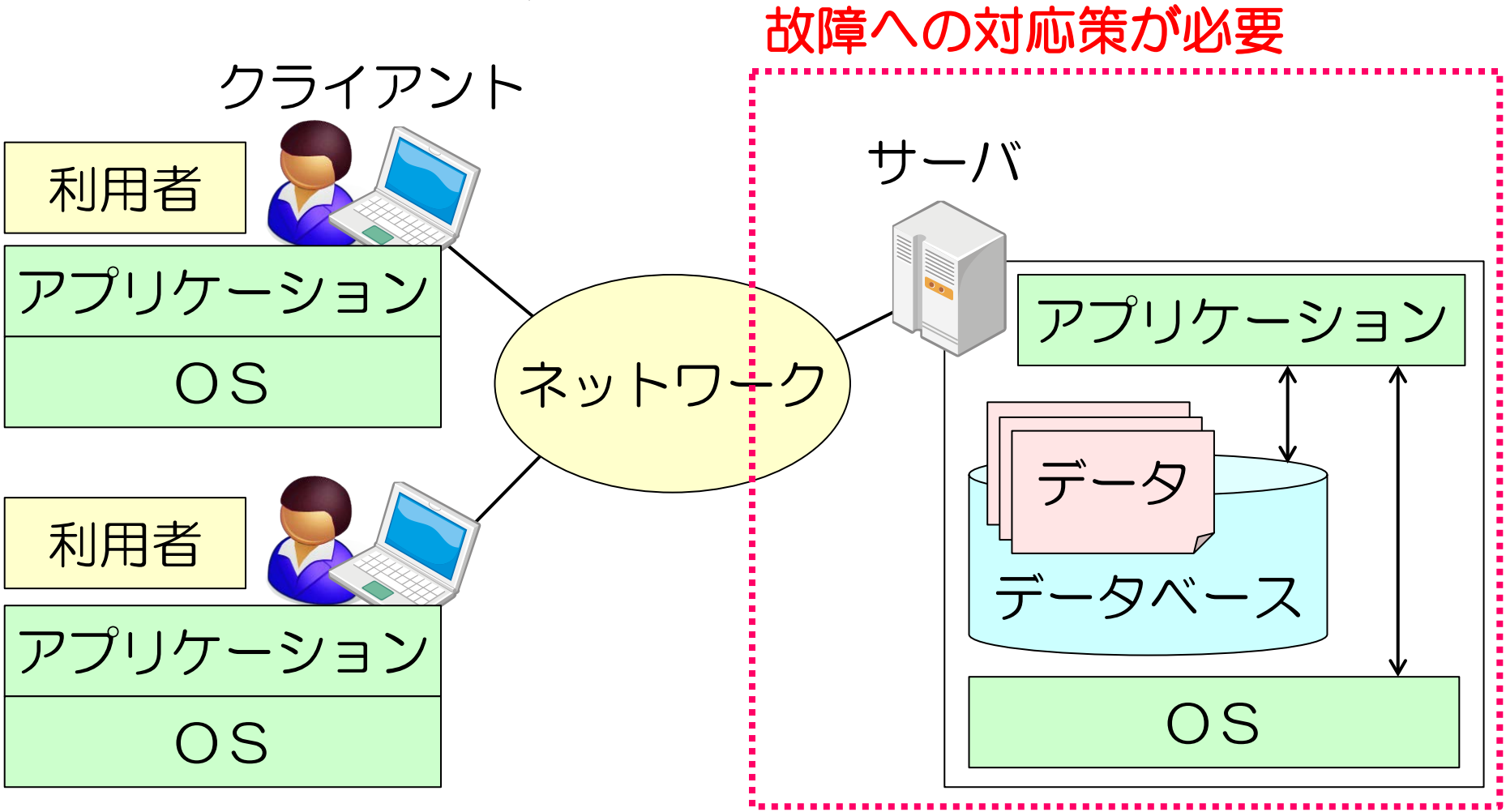
ファーストサーバ株式会社　代表取締役　磯部 眞人

「ファーストサーバ株式会社」のWebページより引用（2014/06）

http://support.fsv.jp/urgent/

サービス可用性(1)

- 情報システムと故障



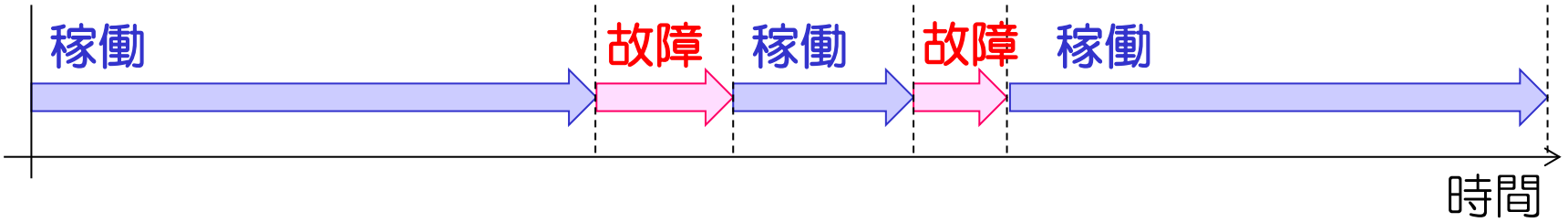
サービス可用性(2)

- サービス可用性の指標

  サービスの稼働時間と故障時間で評価する

  - 平均故障間隔（MTBF）
  - 平均復旧時間（MTTR）

情報システムは「稼働」と「故障」を繰り返す



MTBF := １回の稼働時間の平均値

MTTR := １回の故障時間の平均値

サービス可用性(3)

- 平均故障間隔（MTBF）の向上

  MTBF := 情報システムの**連続稼働時間**の平均

  MTBFを向上させるためには ⇨ 故障の確率を下げる

  - 故障原因

    ハードウェア（ディスク, メモリなど）の故障

    コンピュータネットワークの通信障害

  - MTBF向上の対策

    信頼性の高い機器を使う

    ハードウェアの構成を冗長化する（例：RAID）

サービス可用性(4)

- 平均復旧時間（MTTR）の削減

  MTTR := 情報システムの**復旧にかかる時間**の平均

  MTTRを低下させるためには ⇨ 故障時の対策を計画する

  - 復旧に必要な作業

    故障したハードウェアの交換

    システムの切り替えや再起動

  - MTTR削減の対策

    交換用のハードウェアを準備する

    システムの切り替えや再起動の手順を決めておく

サービス可用性(5)

- システムの稼働率

  稼働率 = システムが稼働している割合

  $$R = MTBF / (MTBF + MTTR)$$

  稼働率 R を向上させるには

  平均故障間隔 MTBF を向上させる

  ⇨ 故障の確率を下げる

  平均復旧時間 MTTFを低下させる

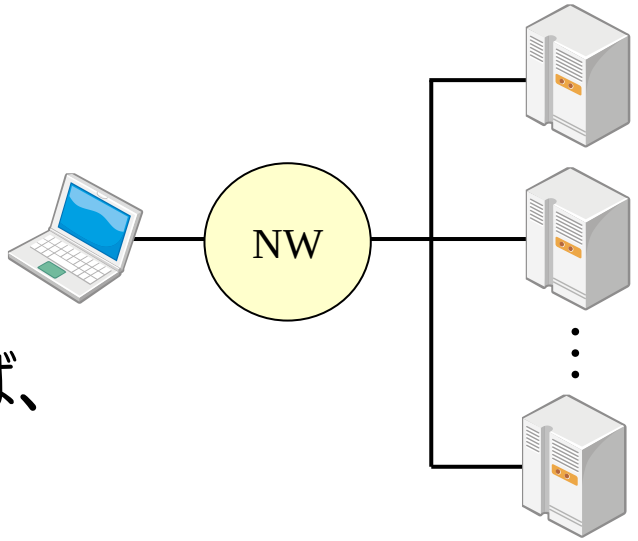
  ⇨ 故障時の対策を計画する

サービス可用性(6)

- 多重系システムの稼働率

  多重系システム

  - n個のハードウェアから構成
  - 1個以上が正常に動作していれば、情報システムとしては稼働する



稼働率

i番目のハードウェアの稼働率 r_i とすると

$$R = 1 - \Pi (1 - r_i)$$

すべてのハードウェアの稼働率が同じ r だとすると

$$R = 1 - (1 - r)^n$$

サービス継続性(1)

- 災害によるデータの消失

消えてしまった戸籍データ

象徴的な出来事として、今回の震災で大きな被害を受けた市町では、戸籍情報システムの滅失が相次いだ。戸籍の正本が失われる事態となった宮城県本吉郡南三陸町，同県牡鹿郡女川町，岩手県陸前高田市および同県上閉伊郡大槌町の4市町のケースを見ていく。

> ***事実1***
> 4市町では戸籍の正本が失われたが、副本などが管轄法務局に保存されていた。それらに基づき戸籍の再製作業を開始、4月25日にデータの復旧が終了したものの、最終的には完全な復元に至ることができなかった。

> ***事実2***
> また4市町とも、災害直前にかけ提出された届出については失われた。管轄法務局で、まだ副本が保管されていなかったのが理由だ。その該当期間は、南三陸町、女川町、陸前高田市では1月下旬から震災当日まで。大槌町では2月下旬から震災当日まで。結局、当該期間に戸籍に関する届出を行った4市町の住民は、再度申し出ることになった。

「ZDNet Japan」のWebページより引用（2014/06）

http://japan.zdnet.com/extra/ca_201105/35002559/

サービス継続性(2)

- ディザスターリカバリ

  災害によりハードウェアが故障することもある

  - 火災
  - 地震
  - 津波

  ｝システム設置場所が被災する

  ⇨ 同じ場所で記憶しているデータも消失

対策：データのバックアップは別の地域で行う

（例）ある医療法人の診療データ

情報システムの設置場所：東北地方太平洋側

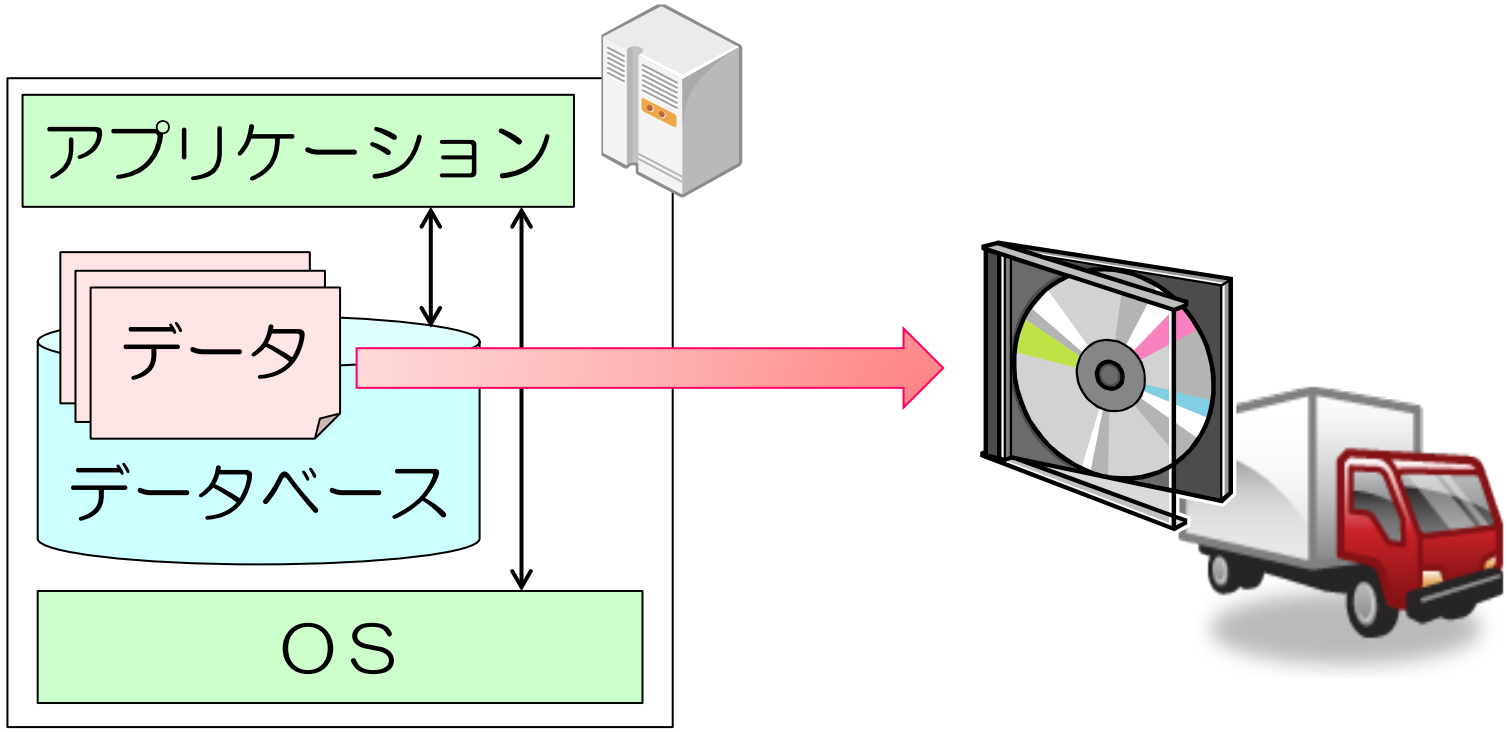
バックアップの設置場所：日本海側

サービス継続性(3)

- テープベース方式

  記録メディア（テープなど）に記録し、別の地域で保管

  ⇨ 復旧：情報システムを構築し直す必要がある

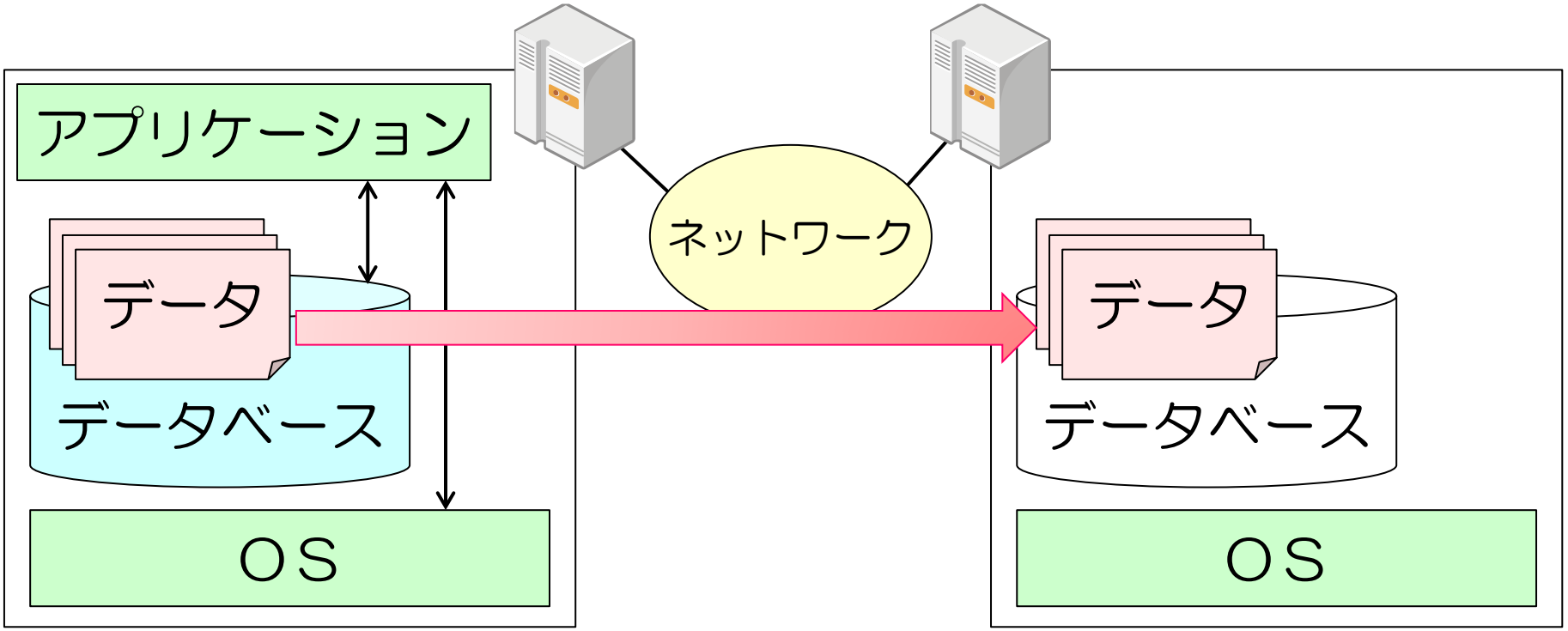


サービス継続性(4)

- レプリケーション方式

  遠隔地にあるストレージディスクに保存する

  ⇨ 復旧：アプリケーションを構築し直す必要がある

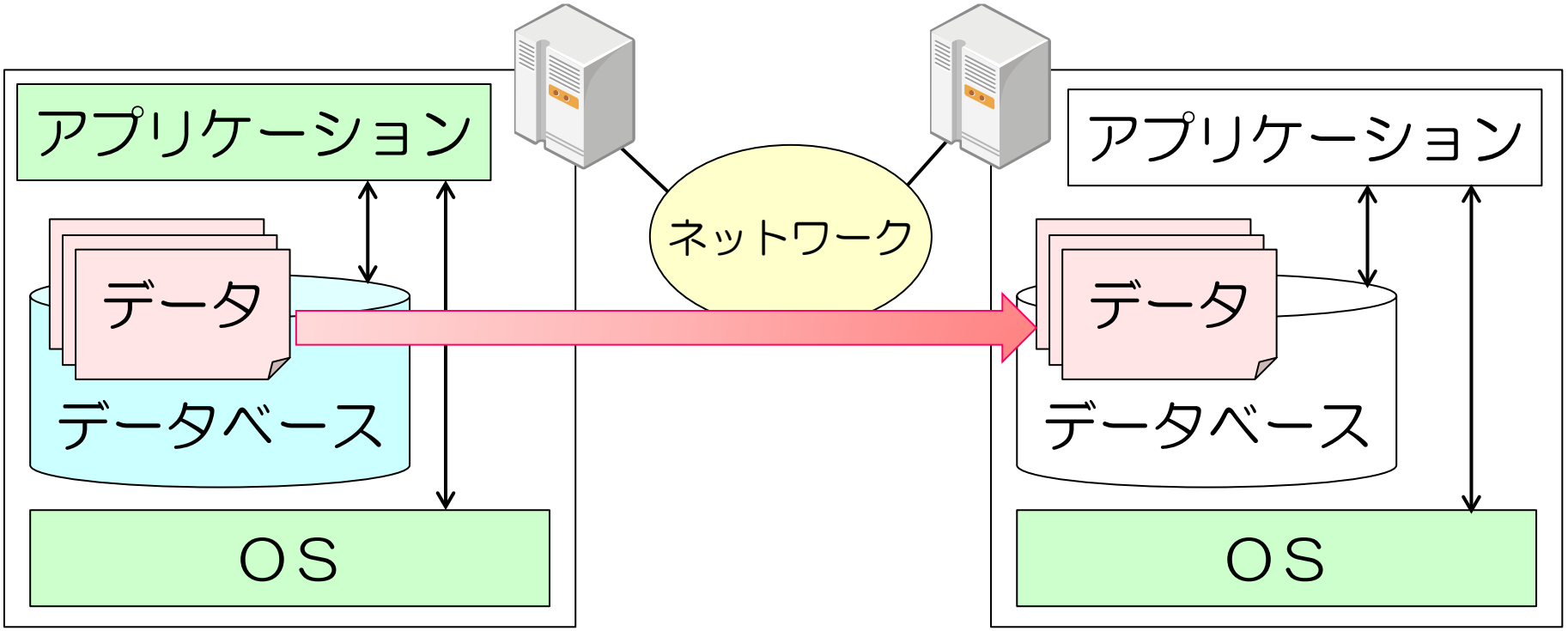


サービス継続性(5)

- サイト間フェイルオーバー方式

  遠隔地にある**同じ情報システム**に保存する

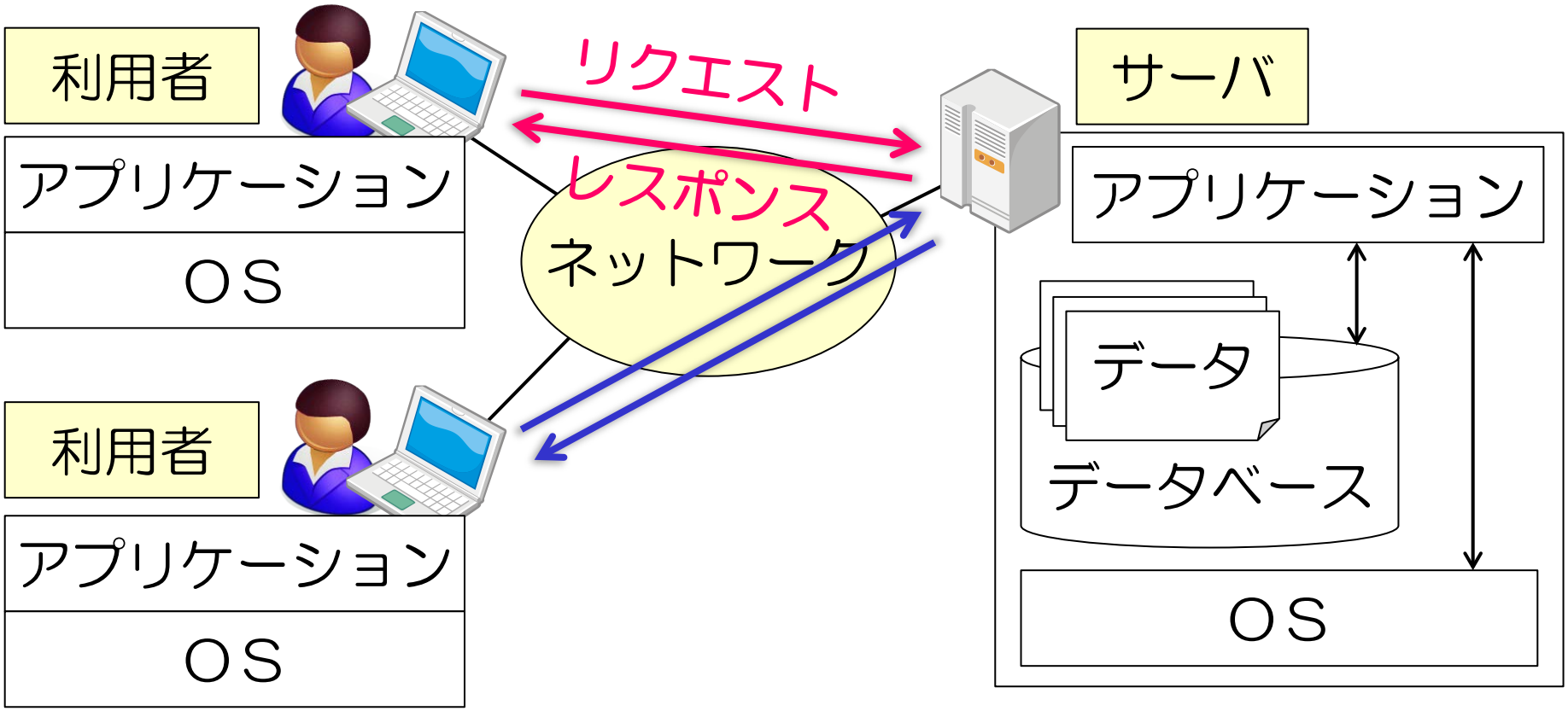
  復旧：稼働システムを切り替えるだけでよい



性能評価(1)

- サービスのレスポンスタイム

「リクエスト」送信から「レスポンス」受信までの時間



性能評価(2)

- 負荷とレスポンスタイム

  一般的に

  システムの負荷が高い ⇨ レスポンスタイムが大きい

  - 負荷率とレスポンスタイムの関係

$$T = S / (1 - \rho)$$

T: レスポンスタイム
S: 負荷が0の時のレスポンスタイム
ρ: 負荷率

ただし、負荷率（CPU）だけで
レスポンスタイムが決定するわけではない

性能評価(3)

- キャパシティ管理

利用者が増える or 利用回数が増える

⇨ リクエストが増える ⇨ レスポンスタイムが増加する

システムの「キャパシティ」を超えたリクエストがはっせい

⇨ サービス継続不能（サービス停止）

リクエストに対応できるシステム構成にする

- CPU
- メモリ
- ディスク容量
- ディスクへのアクセス速度
- ネットワークの通信帯域

リスク管理（1）

- リスク管理

  不足の事態に備える

  - 物理的リスク管理
  - 技術的リスク管理
  - 管理的リスク管理

  情報システム以外の要因によるリスクを想定

リスク管理 (2)

- 物理的リスク管理
  - 火災
  - 停電
  - 地震
- 管理的リスク管理
  - 不正なシステム利用
  - 不正なネットワーク通信
- 技術的リスク管理
  - 不正アクセス
  - 情報漏えい

システム監査(1)

- システム監査の目的

  システムが正しく利用されているかを調べる

  - 所有者の利益になるように利用されているか

    企業の場合は「企業の利益」に貢献しているか？

  - 所有者の目的に則して利用されているか

    システム導入時の目的を達成しているか？

  - 管理する情報が信頼できるものか

    システム内の情報を正確に管理しているか？

  - 法令や契約に従って利用されているか

    社会的なルールを守って利用しているか？

システム監査(2)

- システム監査体制
  - 内部監査

    内部組織による監査

    企業の場合、企業内のメンバーによって監査組織を構成

    ただし、システムに関わらないメンバーで構成

    ⇨ システム導入目的の達成度を調べる

  - 外部監査

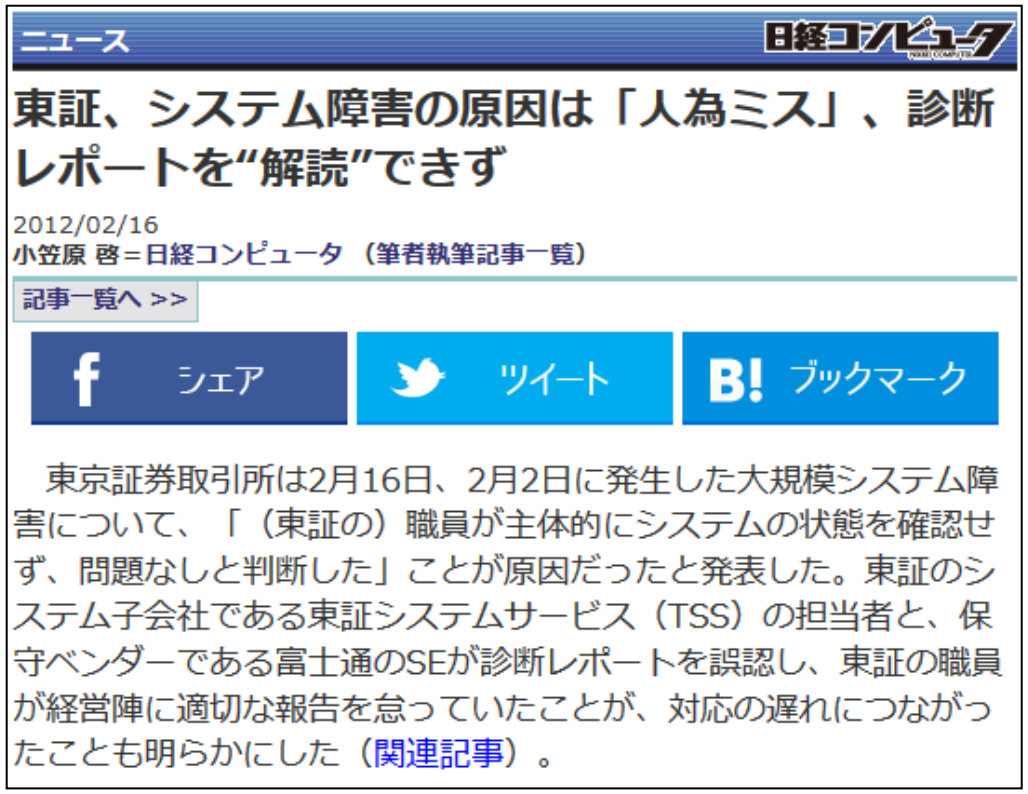
    外部組織による監査

    企業の場合、企業外のメンバーによって監査組織を構成

    ⇨ 社会的なルールを守っているかを調べる

最後に(1)

- 金融取引システムの停止



ニュース　日経コンピュータ

東証、システム障害の原因は「人為ミス」、診断レポートを“解読”できず

2012/02/16
小笠原 啓＝日経コンピュータ （筆者執筆記事一覧）

記事一覧へ >>

シェア　ツイート　B! ブックマーク

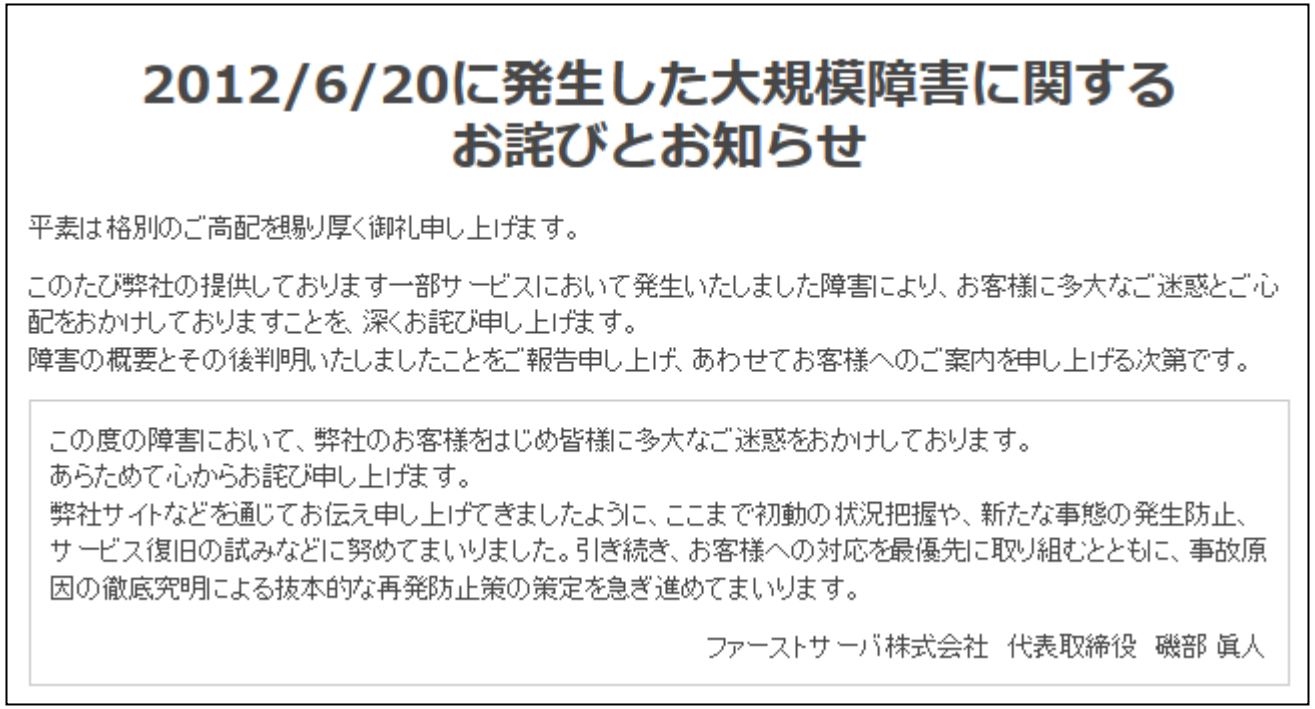
東京証券取引所は2月16日、2月2日に発生した大規模システム障害について、「（東証の）職員が主体的にシステムの状態を確認せず、問題なしと判断した」ことが原因だったと発表した。東証のシステム子会社である東証システムサービス（TSS）の担当者と、保守ベンダーである富士通のSEが診断レポートを誤認し、東証の職員が経営陣に適切な報告を怠っていたことが、対応の遅れにつながったことも明らかにした（関連記事）。

「IT Pro by 日経コンピュータ」のWebページより引用（2014/06）

http://itpro.nikkeibp.co.jp/article/NEWS/20120216/381903/

最後に(2)

- クラウドシステムでのデータ消失



2012/6/20に発生した大規模障害に関する お詫びとお知らせ

平素は格別のご高配を賜り厚く御礼申し上げます。

このたび弊社の提供しております一部サービスにおいて発生いたしました障害により、お客様に多大なご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。
障害の概要とその後判明いたしましたことをご報告申し上げ、あわせてお客様へのご案内を申し上げる次第です。

この度の障害において、弊社のお客様をはじめ皆様に多大なご迷惑をおかけしております。
あらためて心からお詫び申し上げます。
弊社サイトなどを通じてお伝え申し上げてきましたように、ここまで初動の状況把握や、新たな事態の発生防止、サービス復旧の試みなどに努めてまいりました。引き続き、お客様への対応を最優先に取り組むとともに、事故原因の徹底究明による抜本的な再発防止策の策定を急ぎ進めてまいります。

ファーストサーバ株式会社　代表取締役　磯部 眞人

「ファーストサーバ株式会社」のWebページより引用（2014/06）

http://support.fsv.jp/urgent/