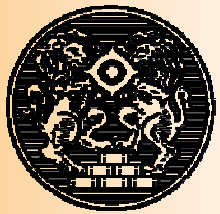
2007年3月23日

事例からみたコンピュータ・システム・リスク管理の具体策



日本銀行
BANK OF JAPAN

日本銀行金融機構局
システム関連考査担当
江見　明弘

説明資料の構成

Ⅰ. システム障害・情報セキュリティ侵害の発生状況
　⑴ システム障害
　⑵ 情報セキュリティ侵害

Ⅱ. システム障害・情報セキュリティ侵害の防止策
　⑴ ＰＤＣＡに基づくシステム障害・情報セキュリティ侵害管理
　⑵ 「他山の石」の活用

Ⅲ. 「想定される障害事例と対応策」の事例紹介

Ⅳ. 「想定される情報セキュリティ侵害に繋がる事例と対応策」の事例紹介

Ⅰ.システム障害・情報セキュリティ侵害の発生状況

(1)システム障害

▽　各金融機関から日本銀行への報告ベースで分析

- 足元増加傾向
- 但しオンライン全面ダウン等大規模障害は減少傾向
- システムの安定性を損なう障害のウエイトが、信頼性、安全性に比べ圧倒的に高い
- システム間のデータ連携が進むなかで、システム障害時の影響が広範化している事例がみられる
- 他社に影響を与える障害も少なくない
- 共同センター障害による多数社同時障害も数多く発生
- 復旧作業時のオペ・ミスによる長時間障害も目立つ

⑵情報セキュリティ侵害

- システム障害に比べ、外部からの情報セキュリティ侵害事例はまだ少ない
- ただ、セキュリティ侵害に繋がりかねない情報セキュリティ管理の不備事例は数多く見られる
- オープン系システムの利用が、勘定系システムの中心部分まで拡大するなかで、金融機関側のリスク対策が追い付いていない事例が目立っている

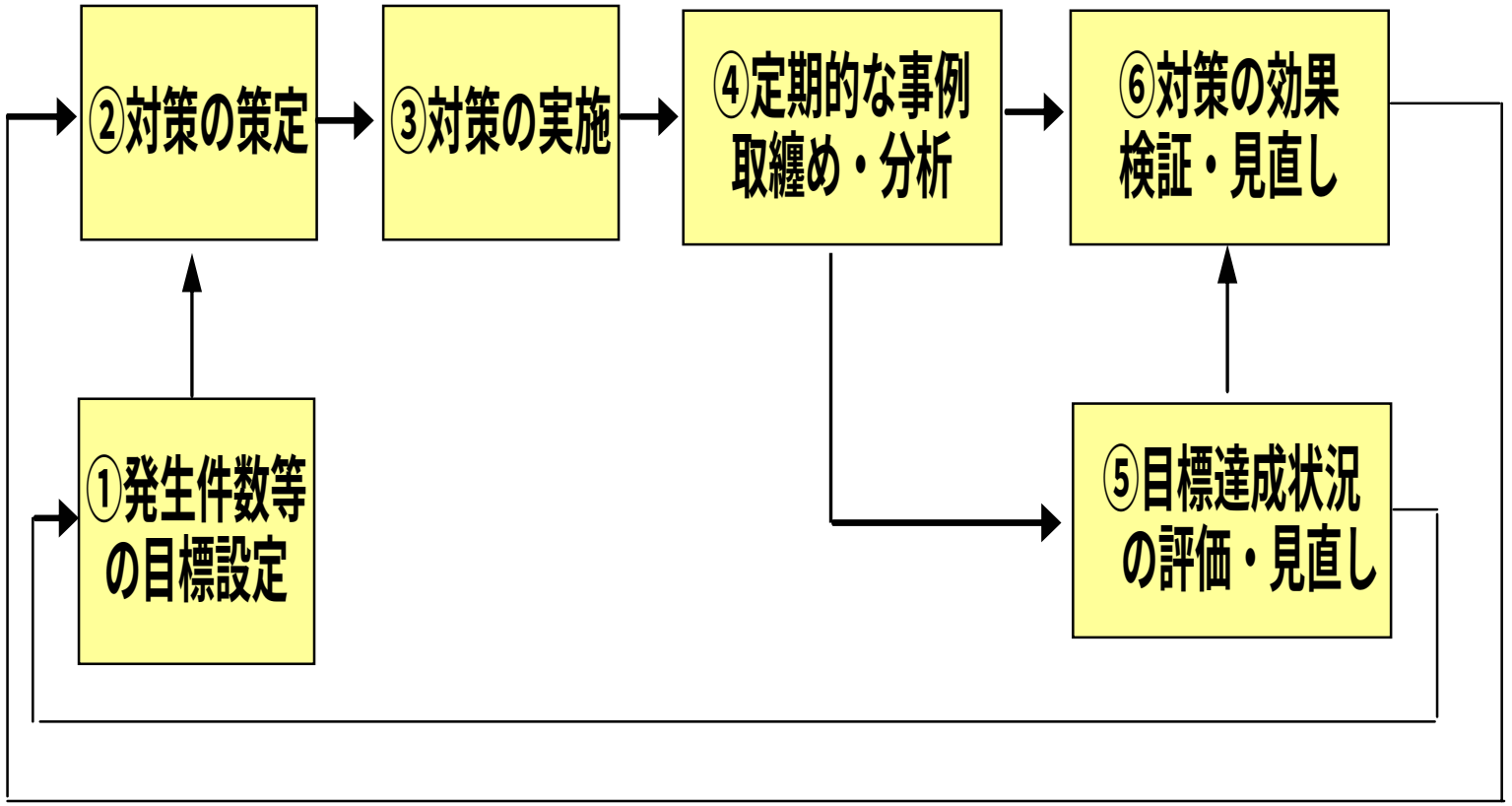
Ⅱ. システム障害・情報セキュリティ侵害の防止策

(1)ＰＤＣＡに基づくシステム障害・情報セキュリティ侵害管理

・システム障害、情報セキュリティ侵害の相当部分は金融機関側の適切なリスク管理により回避可能

障害・セキュリティ侵害	リスク管理策
ハードウェアに起因した障害	機器の二重化、定期保守、切替え訓練の実施等
ソフトウェアに起因した障害	レビュー、テストの充実等
システム性能に起因した障害	性能・負荷テストの実施、定期的な監視
運用・保守に起因した障害	運用・障害マニュアル、プログラム登録手順書等の整備、運用訓練の実施
情報セキュリティ侵害	ユーザーＩＤ管理、暗号化等の適切なセキュリティ対策の実施

▼システム障害・情報セキュリティ侵害管理のためのＰＤＣＡ



⑵「他山の石」の活用

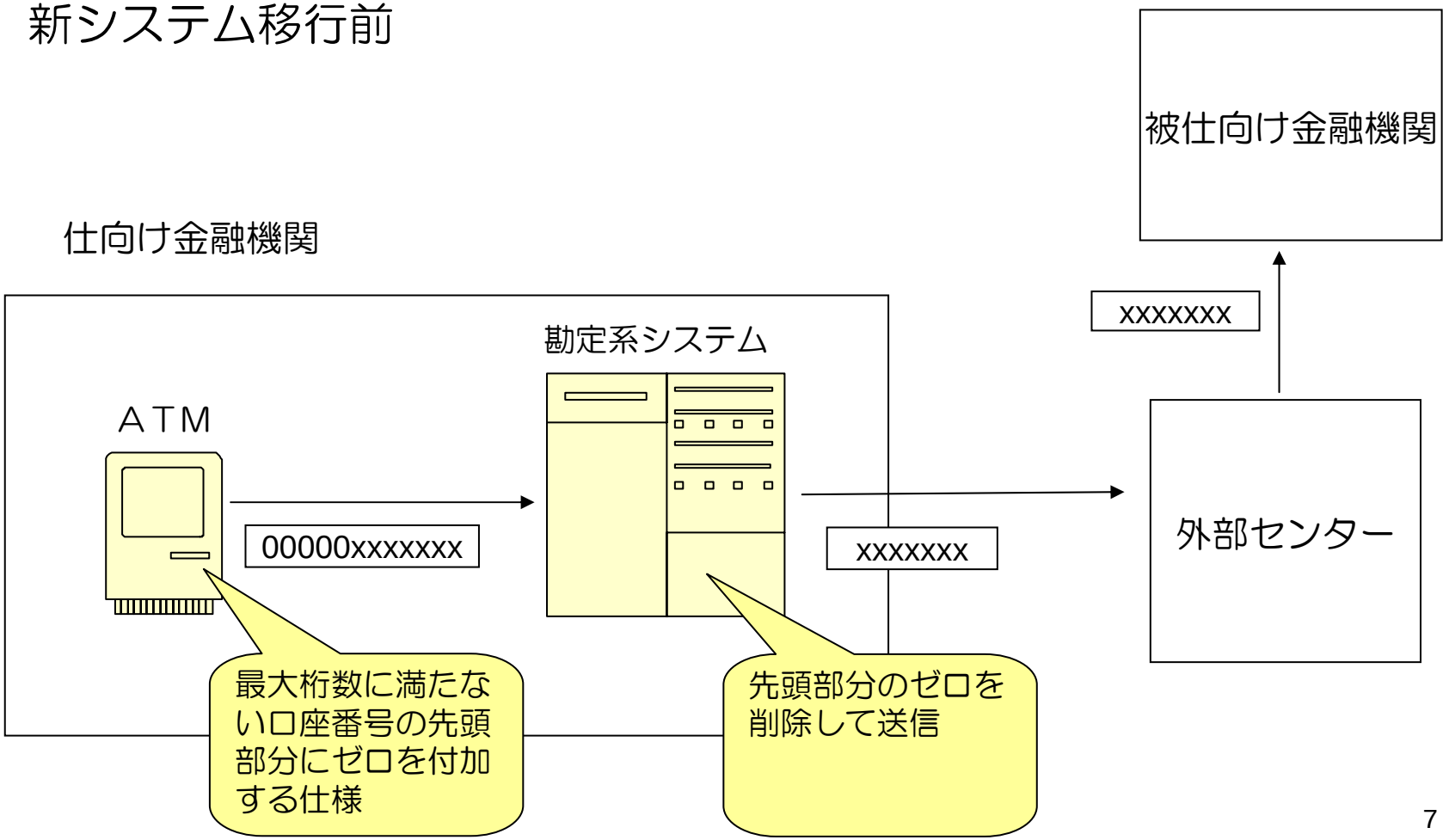
・ システム障害・情報セキュリティ侵害事例の分析にあたっては、自社事例のみならず、他社事例を参考とすることも有益

・日本銀行では、考査等の場で見られた要改善事例やシステム障害事例等を基に、「想定される障害事例と対応策」、「想定される情報セキュリティ侵害に繋がる事例と対応策」を作成

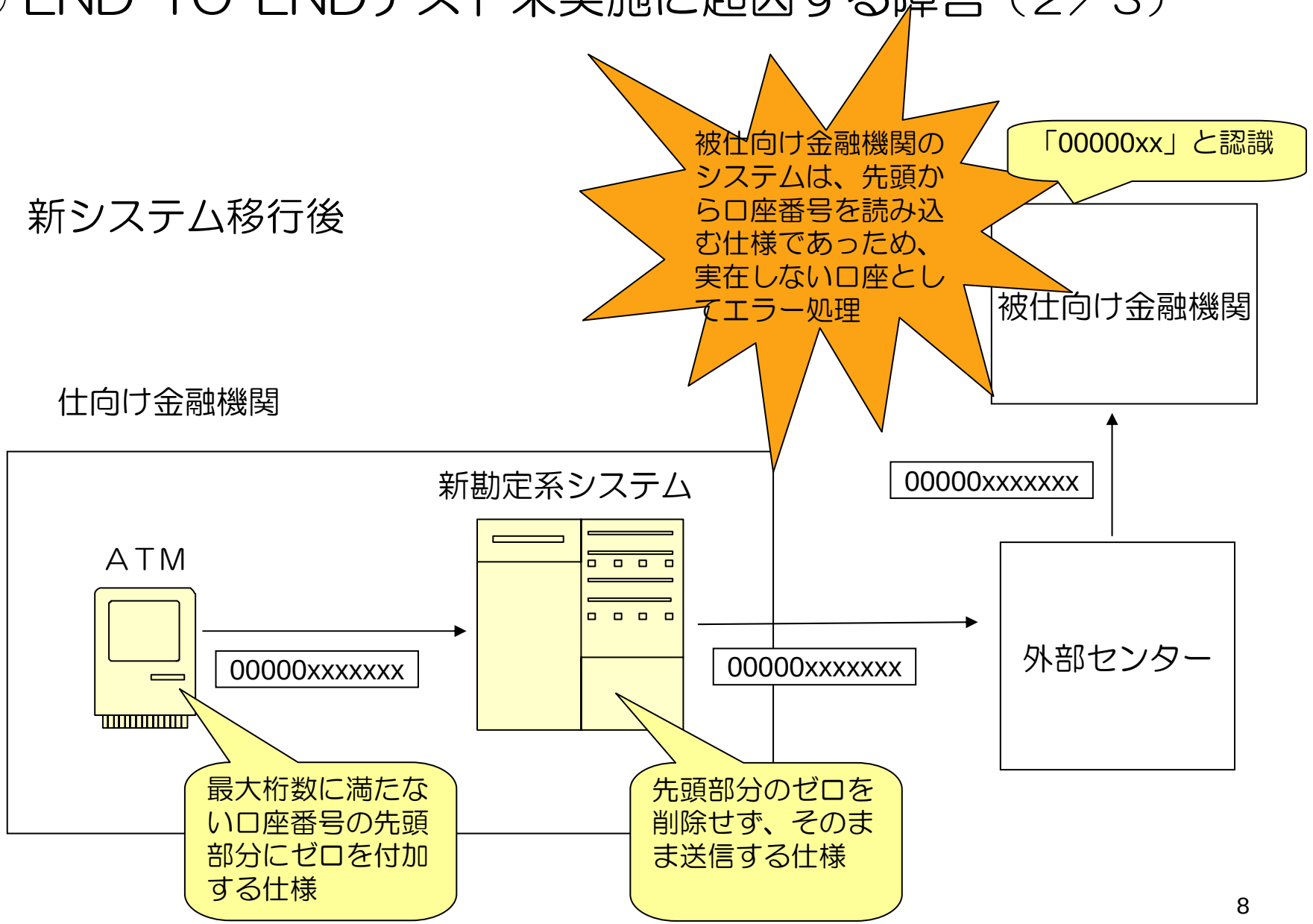
Ⅲ.「想定される障害事例と対応策」の事例紹介

① END-TO-ENDテスト未実施に起因する障害（１／３）

新システム移行前



① END-TO-ENDテスト未実施に起因する障害（２／３）



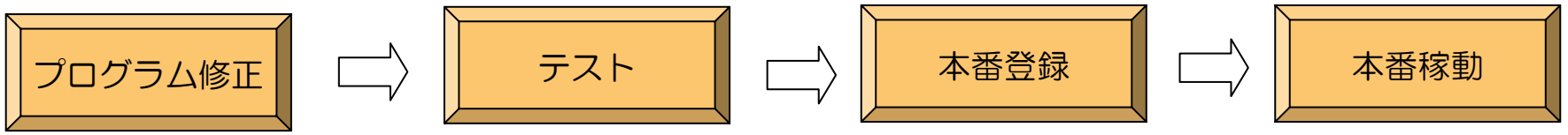
① END-TO-ENDテスト未実施に起因する障害（3／3）

障害事例からみた対応策

●対外接続系業務のテストにおいては、外部接続先を含むEND-TO-ENDのテストを実施すること

●システム間のデータ連動時にミスが生じないよう、外部接続先の仕様を踏まえたうえで、システムを構築すること

② プログラム変更時のディグレードに起因する障害（1／2）



② プログラム変更時のディグレードに起因する障害（2／2）

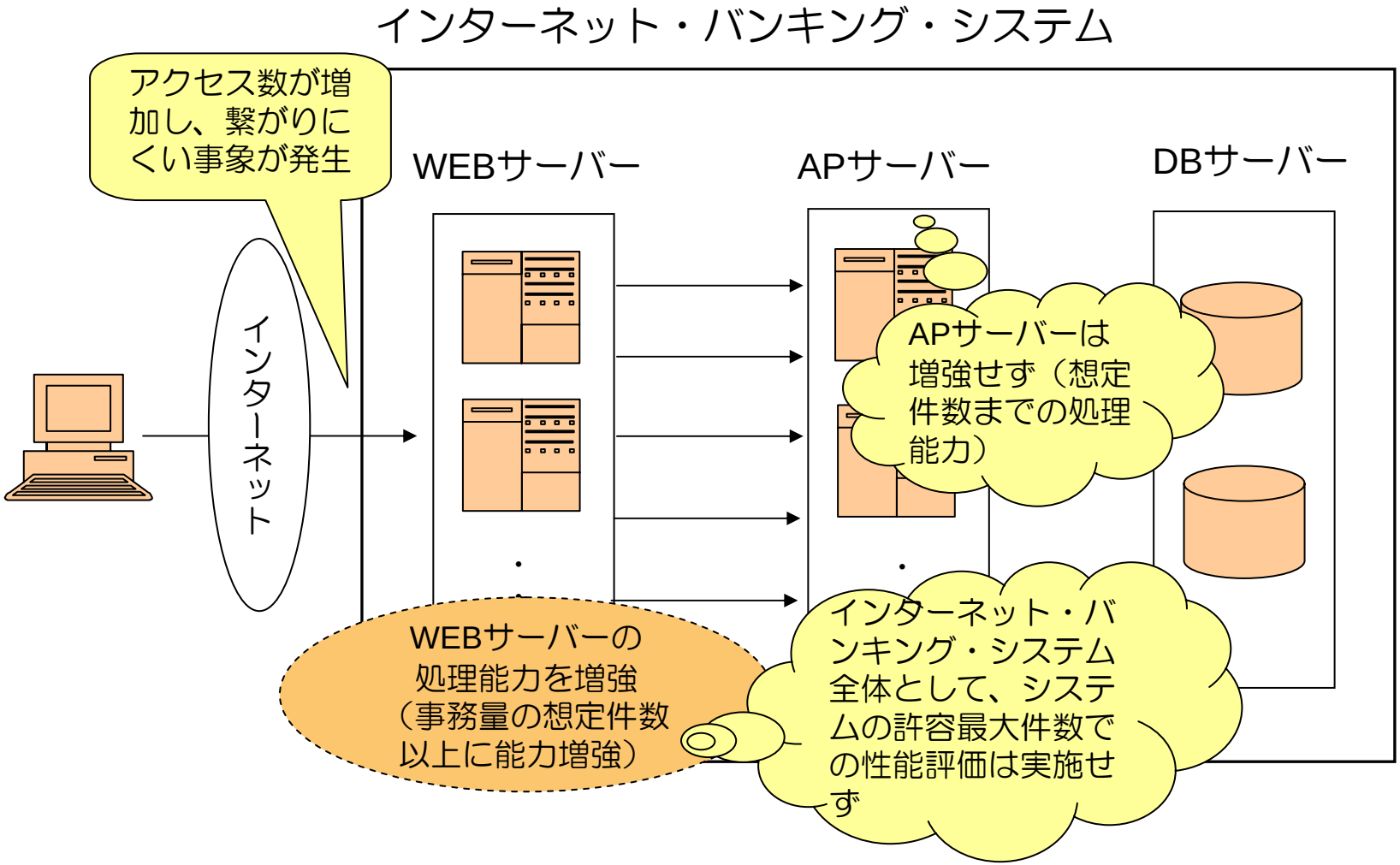
障害事例からみた対応策

●修正箇所以外も対象とした標準的なテスト項目を予め用意すること

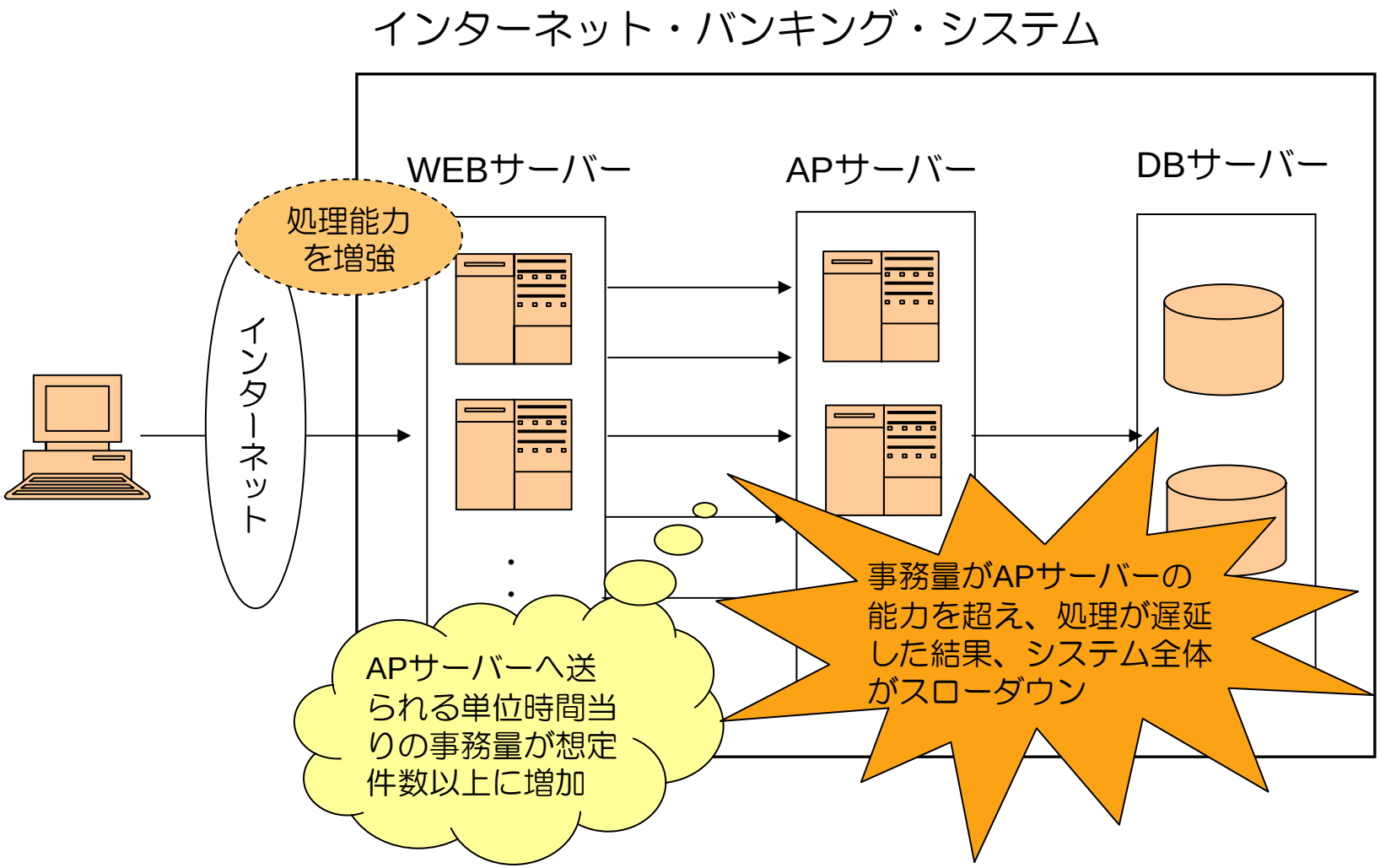
●修正プログラムを本番登録（リリース）する際、修正前プログラムと差分を比較するなど、修正箇所を確認できる仕組みを構築すること

▽　ディグレード防止テストの要否を論理的なインターフェースの有無のみで判断すると、ディグレードを検出できないことがある

③ 性能（システム全体の性能評価未実施）に起因する障害（１／３）



③ 性能（システム全体の性能評価未実施）に起因する障害（２／３）



③ 性能（システム全体の性能評価未実施）に起因する障害（３／３）

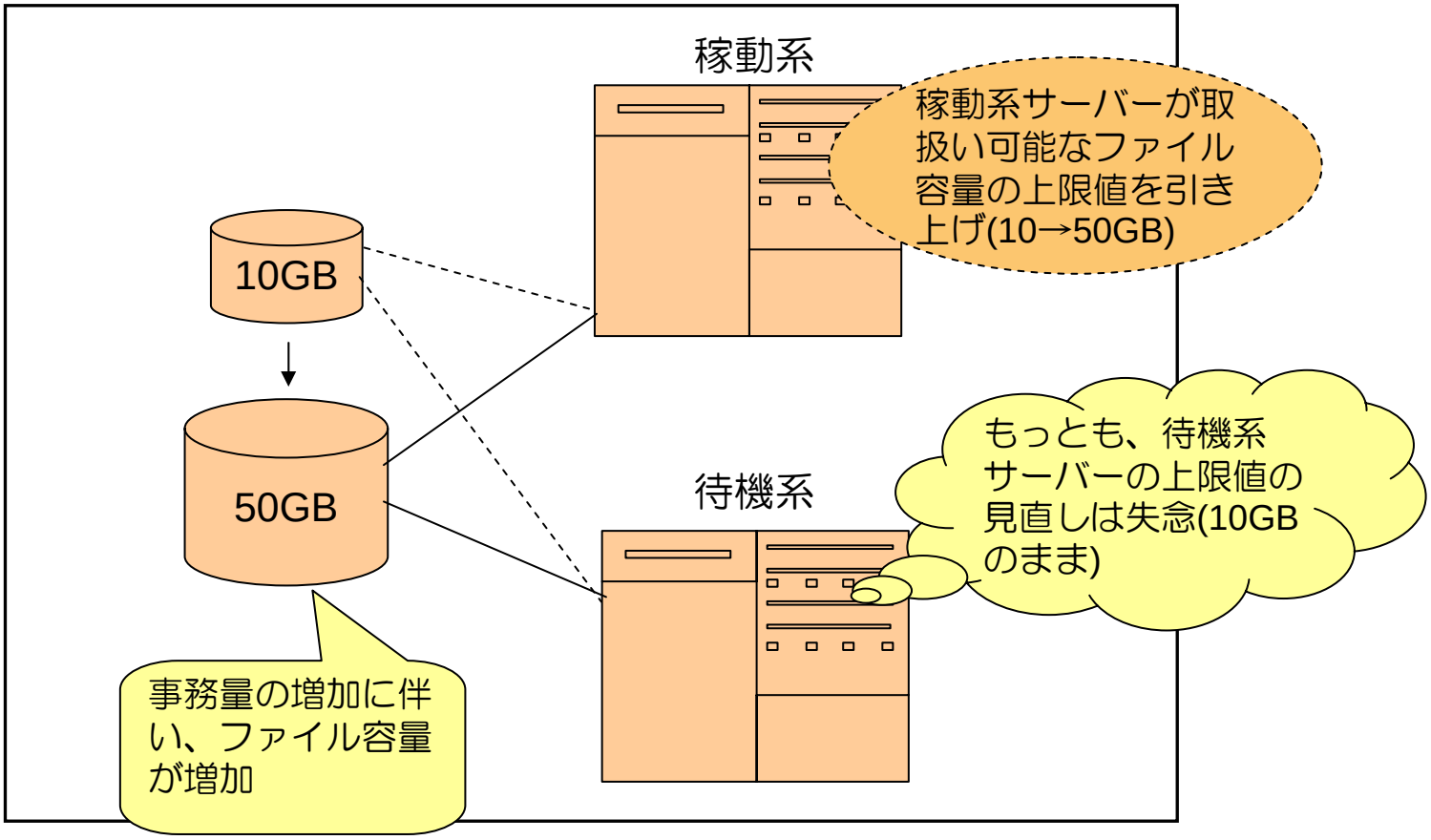
障害事例からみた対応策

●一部システムの能力増強を行う際に、システム全体のピーク時処理量の整合性を含めた性能評価を行うこと

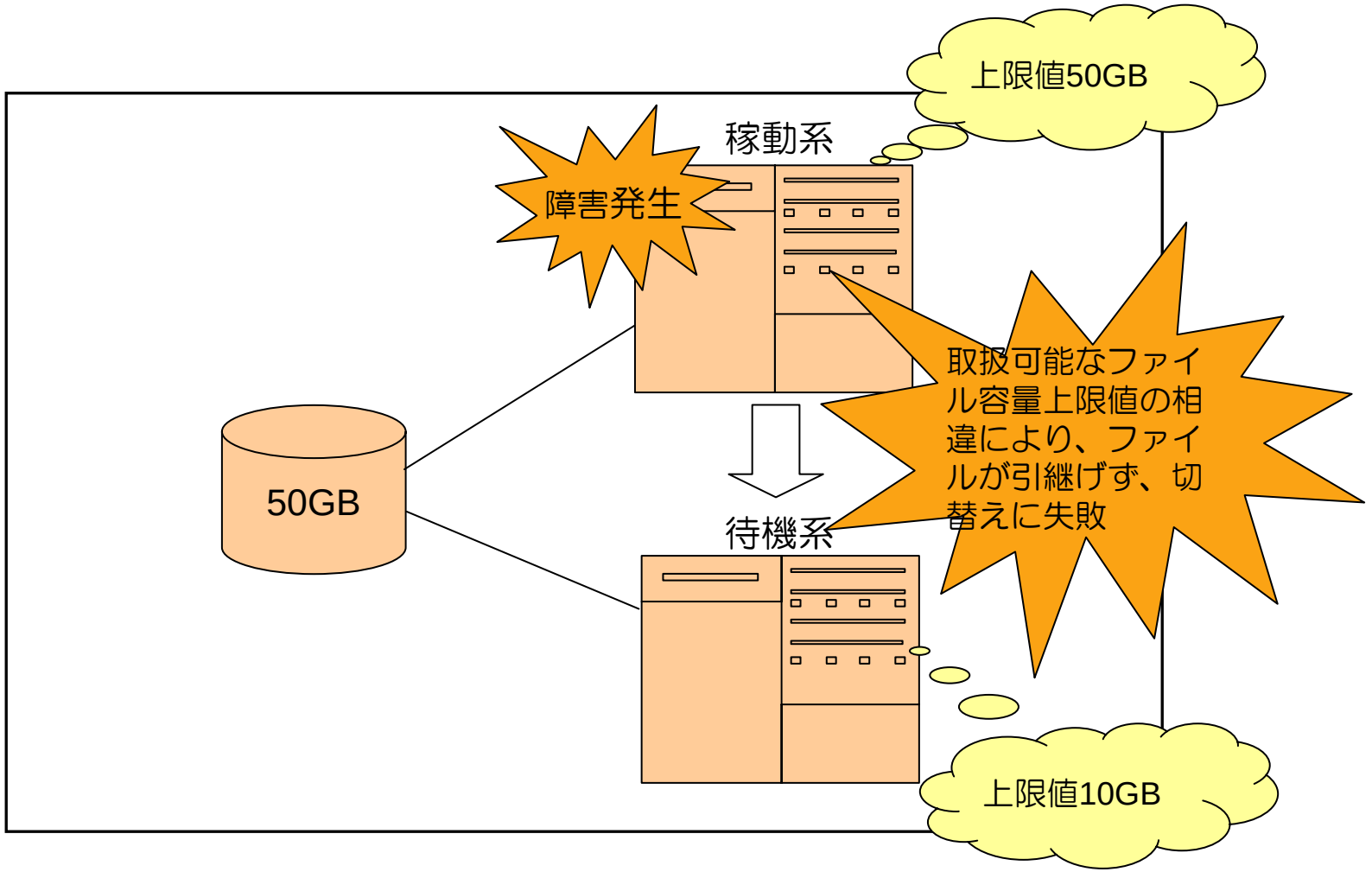
●その際、「想定件数」に加えて、「許容最大件数」の性能負荷テストを行うこと
▽　シミュレータを利用して負荷試験を行う場合、負荷のかからない箇所を明確にし、別途評価を行うこと

●WEBシステムにおいて、アクセスを制限できる仕組み（流量制限）を構築すること

④ 稼動系と待機系の設定値の差異に起因する障害（１／３）



④ 稼動系と待機系の設定値の差異に起因する障害（２／３）

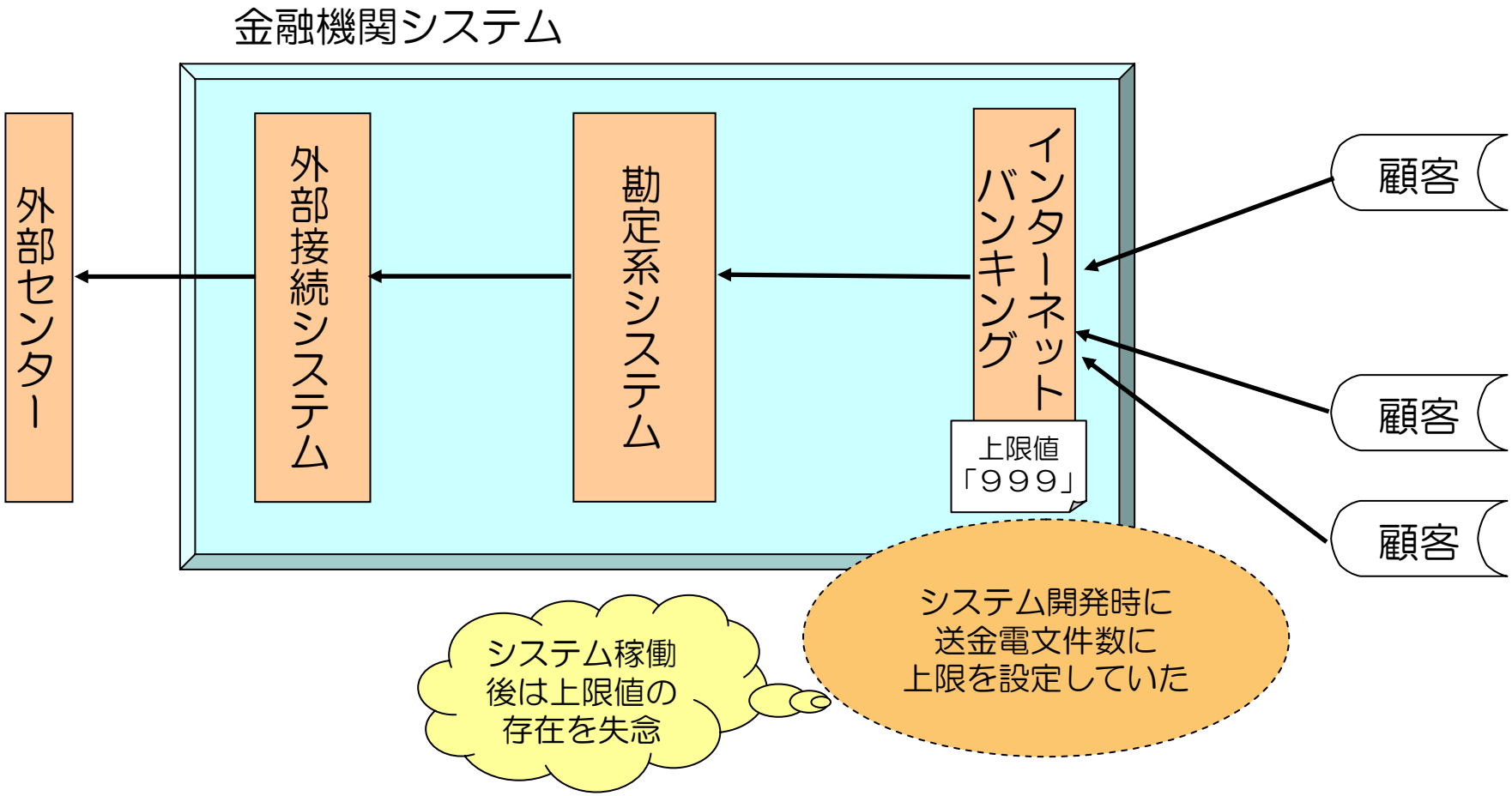


④ 稼動系と待機系の設定値の差異に起因する障害（3／3）

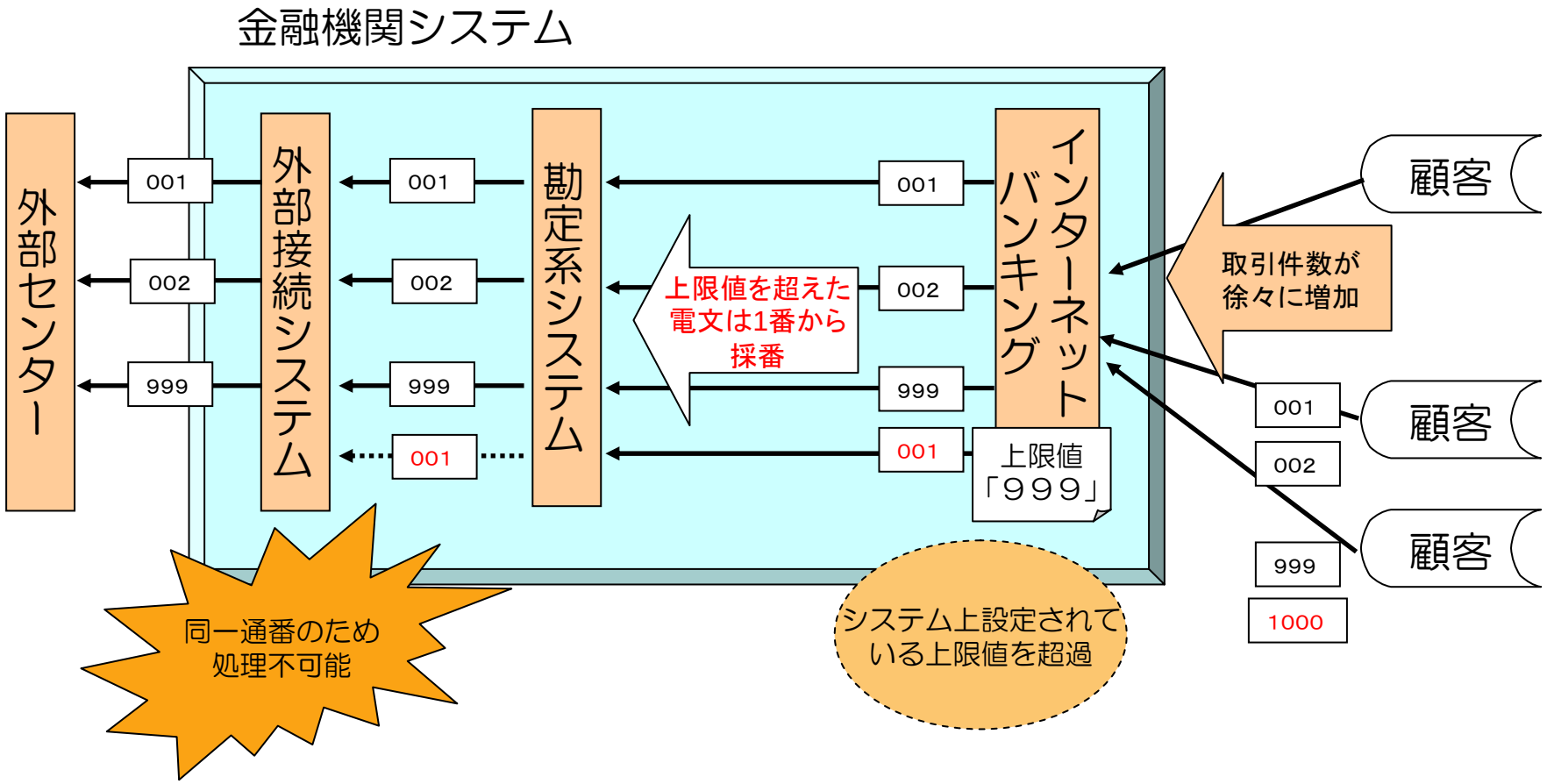
障害事例からみた対応策

●稼動系機器と待機系機器の設定値に差異のないことを、システム構築時および設定変更時に確認すること

⑤ プログラムの上限値に起因する障害（１／３）



⑤ プログラムの上限値に起因する障害（２／３）



⑤ プログラムの上限値に起因する障害（３／３）

障害事例からみた対応策

●システム内に有している各種の上限値を管理すること
▽　アプリケーション・プログラムのみならず、ミドルウェア等についても管理すること
▽　上限値の例として、数値項目の桁数、処理の繰返し回数、同時アクセス可能数、プログラムが展開する内部テーブルの大きさなどがある

●当該上限値と取引データ等の実績値を踏まえた定期的な検証を行うこと

⑥ 運用・作業ミス（コンチ・プラン未整備）に起因する障害（１／２）

●振込等で大量の未処理が発生した場合のコンチ・プラン未整備
　▽障害報告ルール、代替策、緊急避難策
●未処理明細の特定、営業店・決済日別仕分けのための仕組みなし

為替処理でプログラムの不具合により、大量の振込依頼が滞留

障害対応に問題

●関係部署への障害発生報告の遅れ
●外部センターへのMT持込、営業店での代行入力等の代替策の未実行
●為替処理の新規受付停止等の緊急避難策の未実行

当日決済の振込を当日中に送信できなかった

⑥ 運用・作業ミス（コンチ・プラン未整備）に起因する障害（２／２）

障害事例からみた対応策

●為替、口座振替等大量取引を扱い顧客影響の大きい処理において、大量の未処理データが発生した場合のコンチ・プランを策定すること

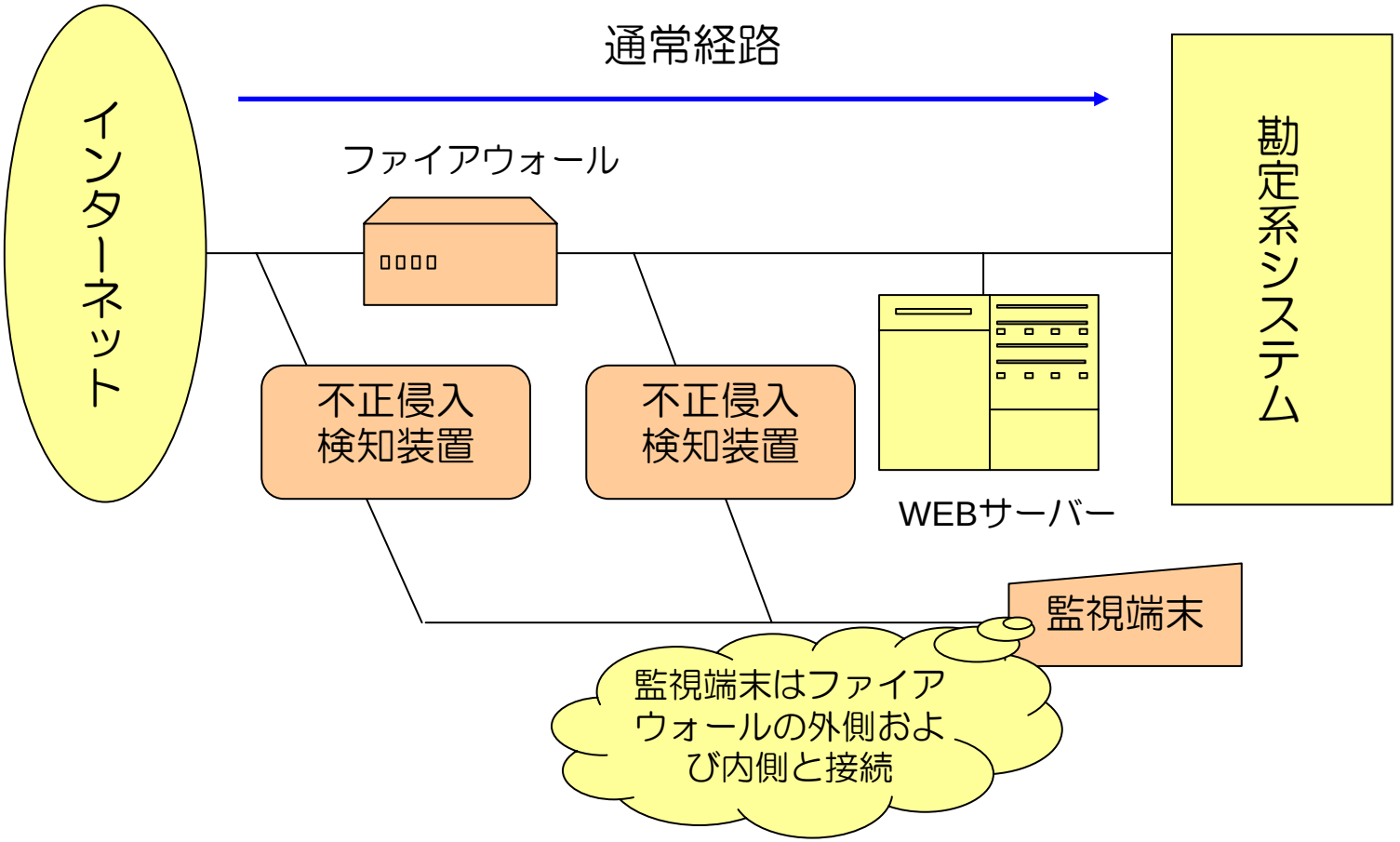
▽　コンチ・プランに基づき未処理明細の特定や再処理方法を明確にすること

▽　障害の発生箇所により対応が異なるため、想定されるケースに応じたきめ細かなプランを策定すること

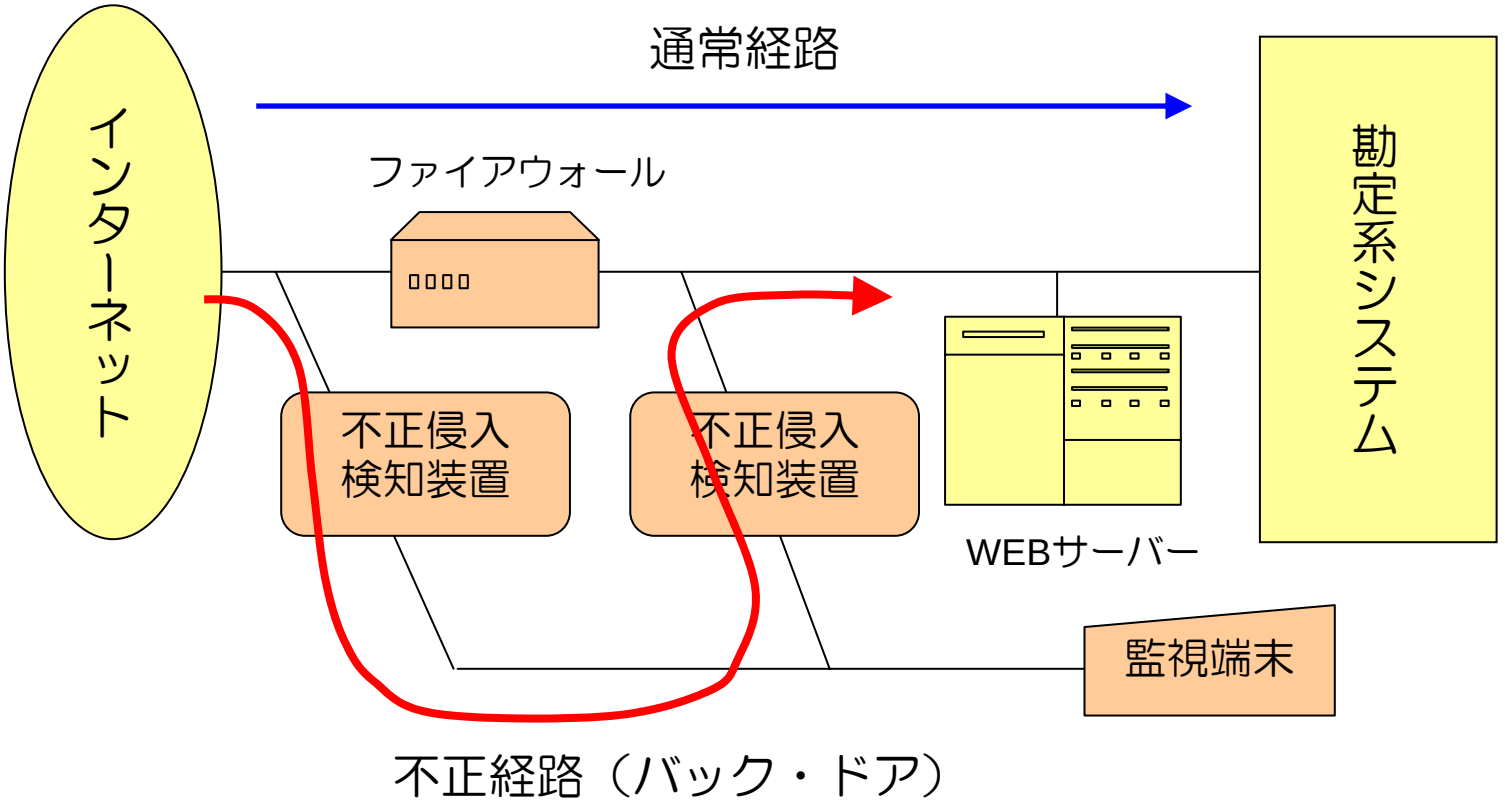
●コンチ・プランに基づく実戦的な訓練を実施し、その実効性を確認すること

Ⅳ.「想定される情報セキュリティ侵害に繋がる事例と対応策」の事例紹介

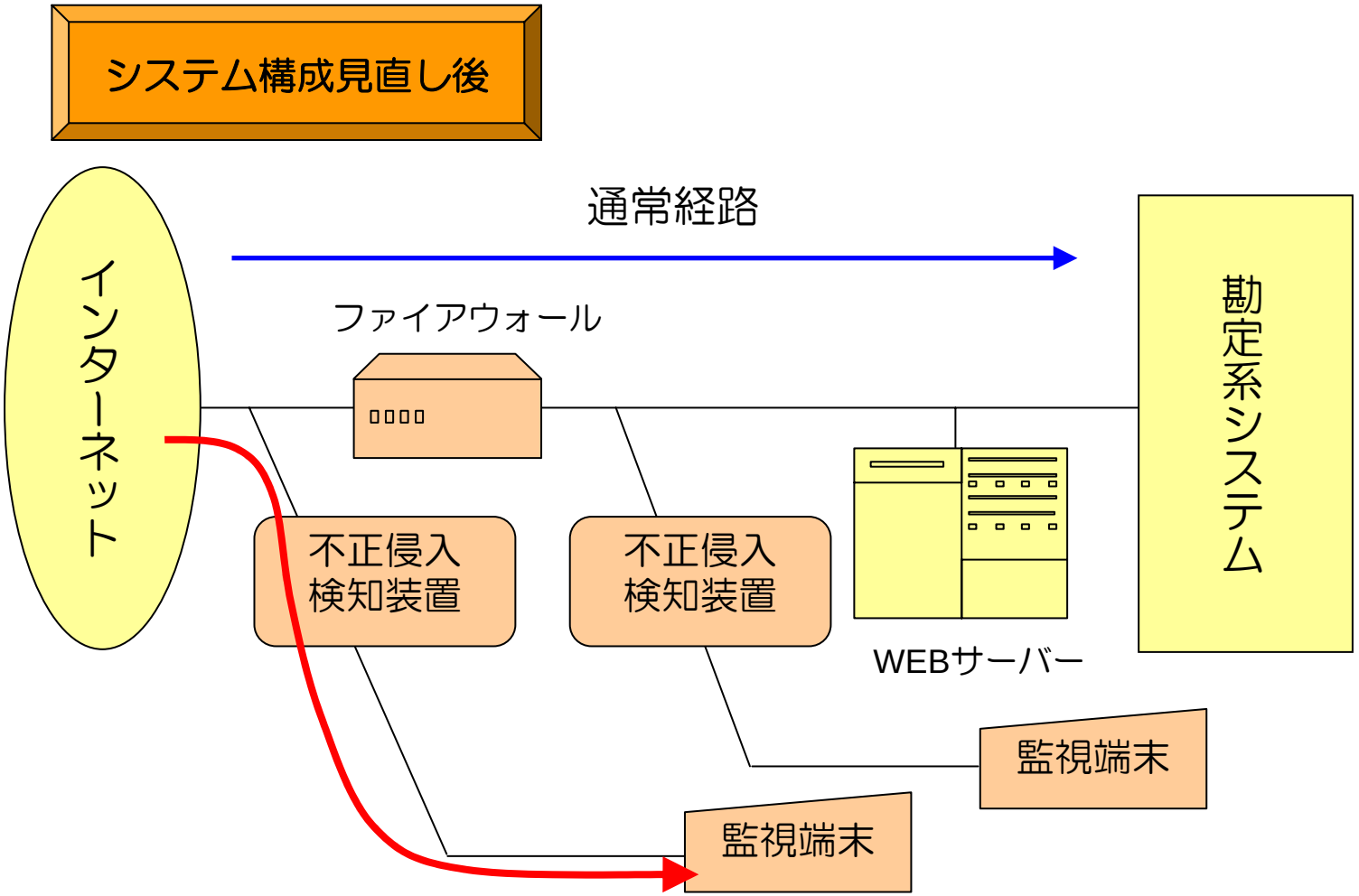
① 外部からの不正アクセスに繋がる事例（1／4）



① 外部からの不正アクセスに繋がる事例（２／４）



① 外部からの不正アクセスに繋がる事例（３／４）



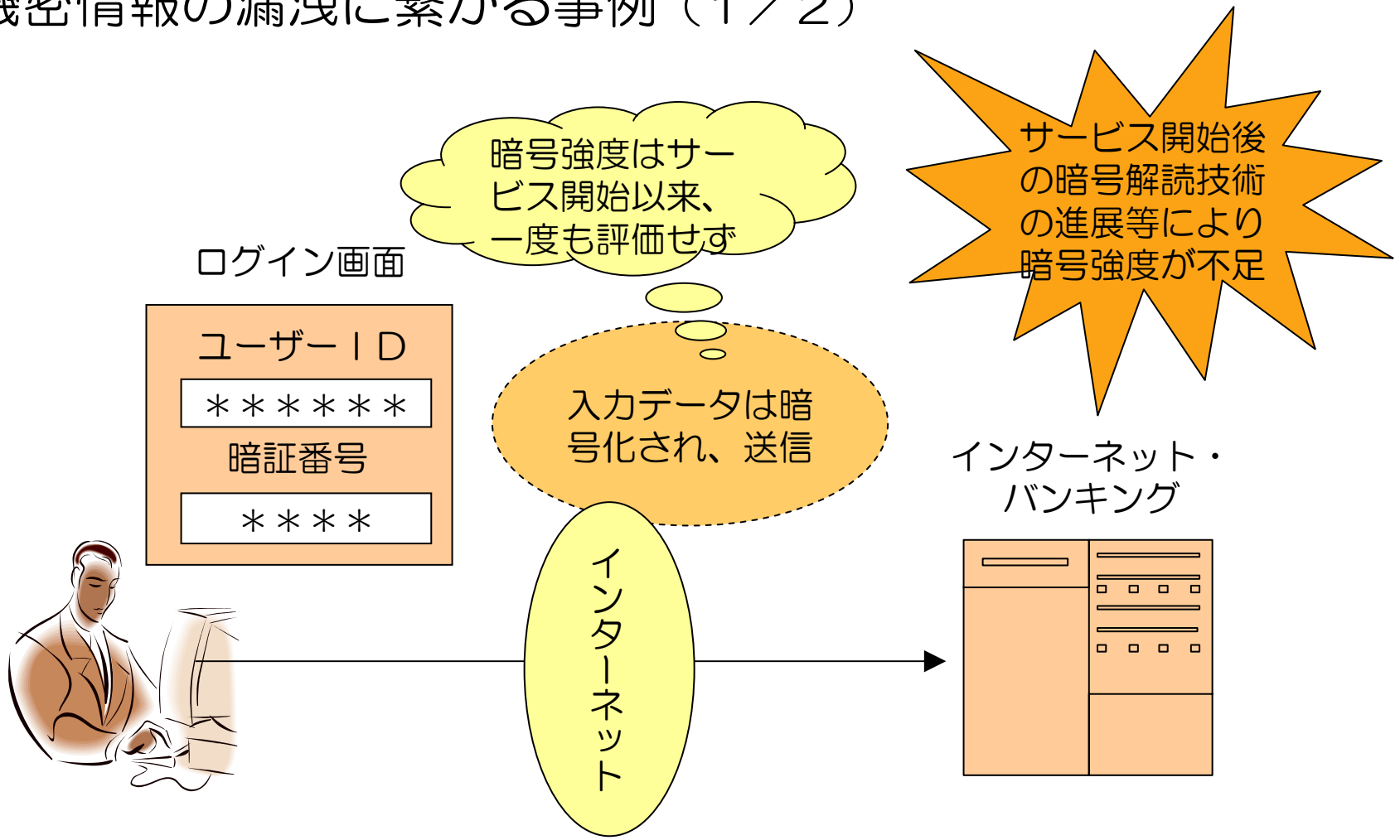
① 外部からの不正アクセスに繋がる事例（４／４）

事例からみた対応策

●システムの機器構成を十分に理解し、不正な侵入を許す経路が存在しないシステムを構築すること

● システムの機器構成を変更する際には、不正な侵入を許す経路が生じていないか検証すること

② 機密情報の漏洩に繋がる事例（１／２）



② 機密情報の漏洩に繋がる事例（2／2）

事例からみた対応策

●暗号の強度について、システムの重要性および利用環境（インターネットのように不特定多数が接続可能か等）を考慮したうえで、採用する暗号の強度を評価すること。また、定期的に強度評価を見直すこと

●暗号の採用にあたっては、総務省および経済産業省が公表している「電子政府推奨暗号リスト」等信頼度の高いガイドライン類を参照し、強度を保つこと

ご清聴有難うございました。