金融高度化セミナー資料

2015年3月

重要な顧客情報の管理の視点を踏まえたシステムリスク管理上の留意点

日本銀行　金融機構局

日本銀行
BANK OF JAPAN

1. 本日の説明内容

- 日本銀行では、2015年1月に、調査論文「重要な顧客情報のセキュリティ強化に向けて　－コンピュータ・システムのリスク管理上の留意点－」を公表。

- 本日は、同論文の内容等を踏まえ、重要な顧客情報の管理の視点を踏まえたシステムリスク管理上の留意点等を解説します。

1. 本日の説明内容（続き）

- 重要な顧客情報の取扱いと環境変化
- システム面のリスク管理強化に向けた留意点
  - 重要情報の保有状況の把握

    ～ログ情報にも内在し得る重要情報
  - 重要情報を取り扱う運用業務の把握

    ～ 障害対応にも留意が必要
  - リスク対策の実施状況の把握

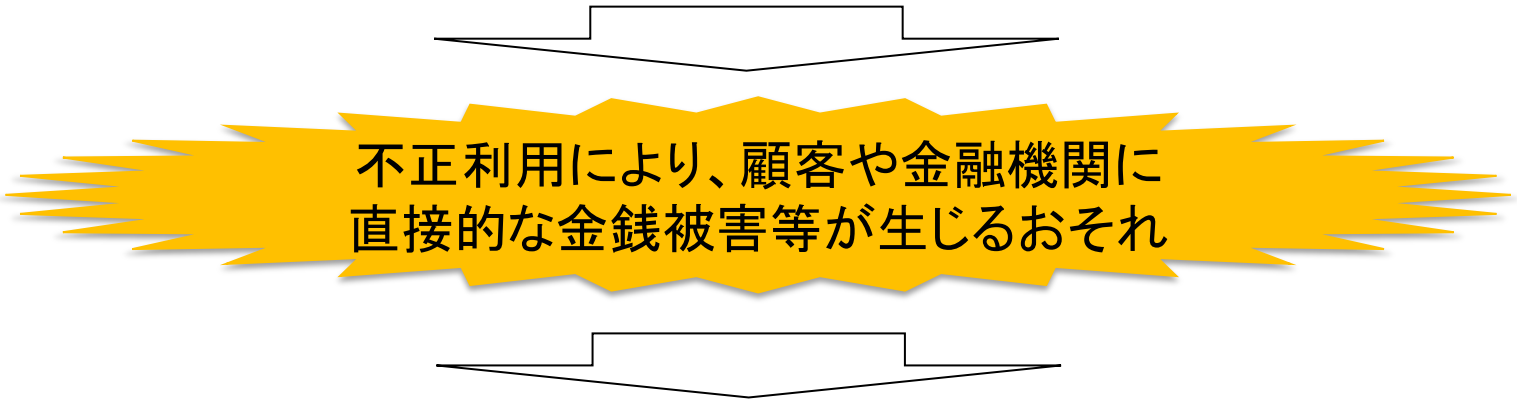
    ～重要情報に対するアクセス制御の実施状況等
  - リスク評価を踏まえた対策の強化
- 状況変化に応じた見直しの実施

2. 重要な顧客情報の取扱い

- **重要な顧客情報の取扱い**と環境変化
- システム面のリスク管理強化に向けた留意点
  - 重要情報の保有状況の把握
    ～ログ情報にも内在し得る重要情報
  - 重要情報を取り扱う運用業務の把握
    ～ 障害対応にも留意が必要
  - リスク対策の実施状況の把握
    ～重要情報に対するアクセス制御の実施状況等
  - リスク評価を踏まえた対策の強化
- 状況変化に応じた見直しの実施

2. 重要な顧客情報の取扱い（続き）

- 金融機関の取り扱う重要な顧客情報（以下、重要情報）
  - 預金口座や証券口座の**口座番号**
  - キャッシュカードの**暗証番号**
  - インターネット取引の**ログインID・パスワード**　等



重要情報には特に厳格な管理が求められる！

2. 重要な顧客情報の取扱い（続き）

- 重要情報が不正使用された事例①
  - 再々委託先の開発担当者が、不正処理を実行し、システム障害の調査等に必要となる情報から重要情報を詐取し、不正出金を行った。

- 重要情報が不正使用された事例②
  - 再々委託先のATM保守管理を担当する責任者が、各種作業の権限者であるという立場を利用し、ATMの障害解析作業の中で重要情報を詐取し、キャッシュカードを偽造のうえ、不正出金を行った。

2. システムを巡る環境変化

- 重要な顧客情報の取扱いと**環境変化**
- システム面のリスク管理強化に向けた留意点
  - 重要情報の保有状況の把握

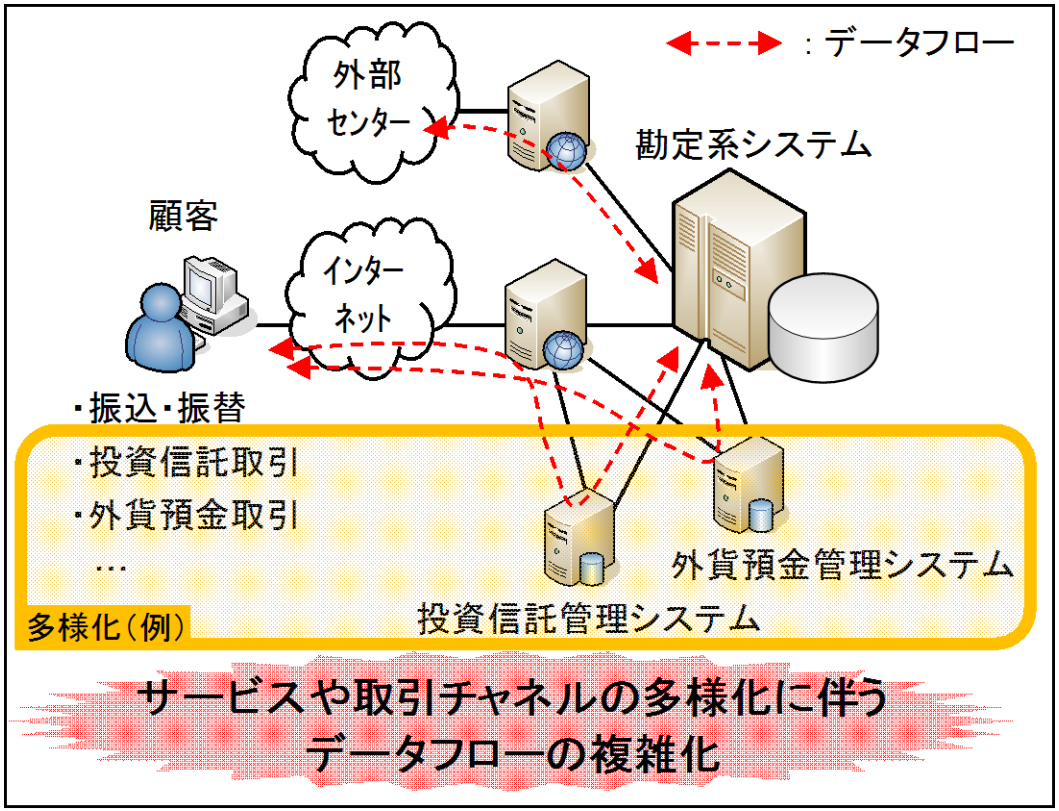
    ～ログ情報にも内在し得る重要情報
  - 重要情報を取り扱う運用業務の把握

    ～ 障害対応にも留意が必要
  - リスク対策の実施状況の把握

    ～重要情報に対するアクセス制御の実施状況等
  - リスク評価を踏まえた対策の強化
- 状況変化に応じた見直しの実施

2. システムを巡る環境変化（続き）

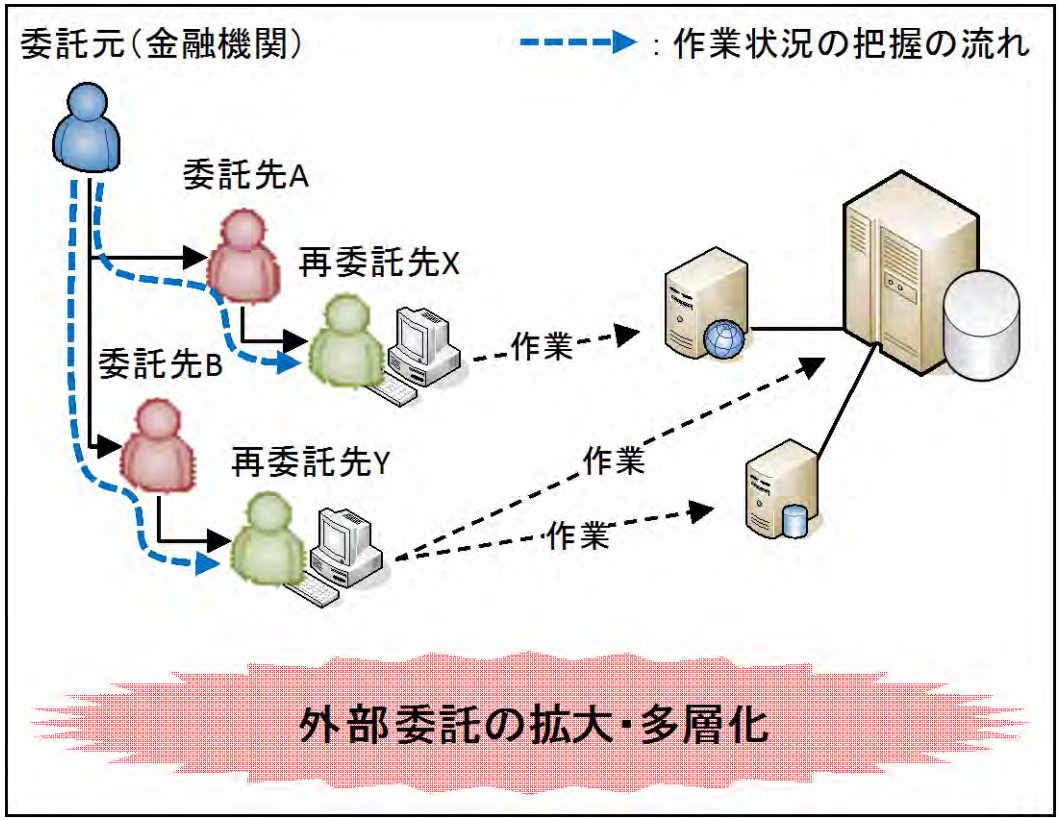
- 環境変化①： システム構成のさらなる複雑化



重要情報はどのシステム・機器で処理され、どのように保有されている？？

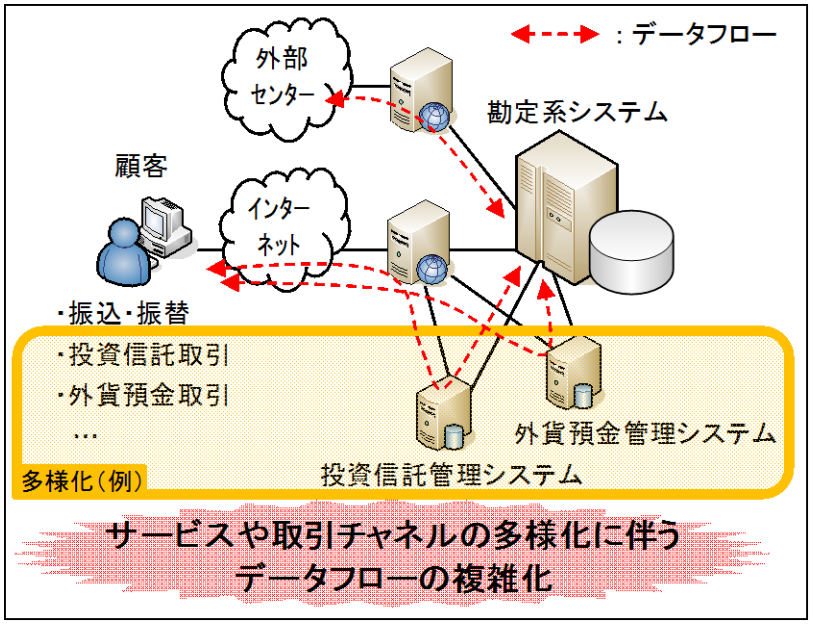
2. システムを巡る環境変化（続き）

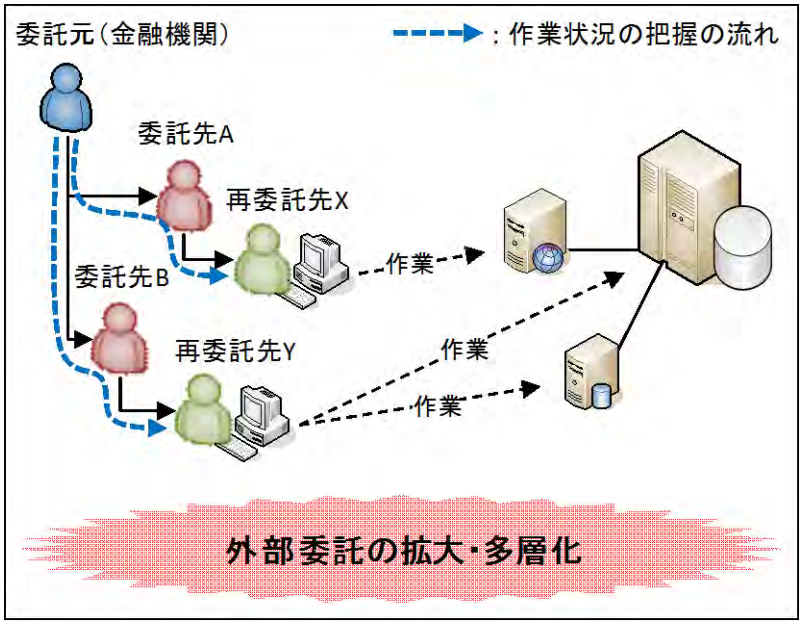
- 環境変化②： 外部委託化の一層の進展



重要情報は誰が、どのような業務で取り扱っている？？

2. システムを巡る環境変化（続き）





・システム内の重要情報の保有状況

・重要情報の取扱者や運用業務の実態

正確な把握が重要

3. 留意点①:重要情報の保有状況の把握

- 重要な顧客情報の取扱いと環境変化
- **システム面のリスク管理強化に向けた留意点**
  - **重要情報の保有状況の把握**

    ～ログ情報にも内在し得る重要情報
  - 重要情報を取り扱う運用業務の把握

    ～ 障害対応にも留意が必要
  - リスク対策の実施状況の把握

    ～重要情報に対するアクセス制御の実施状況等
  - リスク評価を踏まえた対策の強化
- 状況変化に応じた見直しの実施

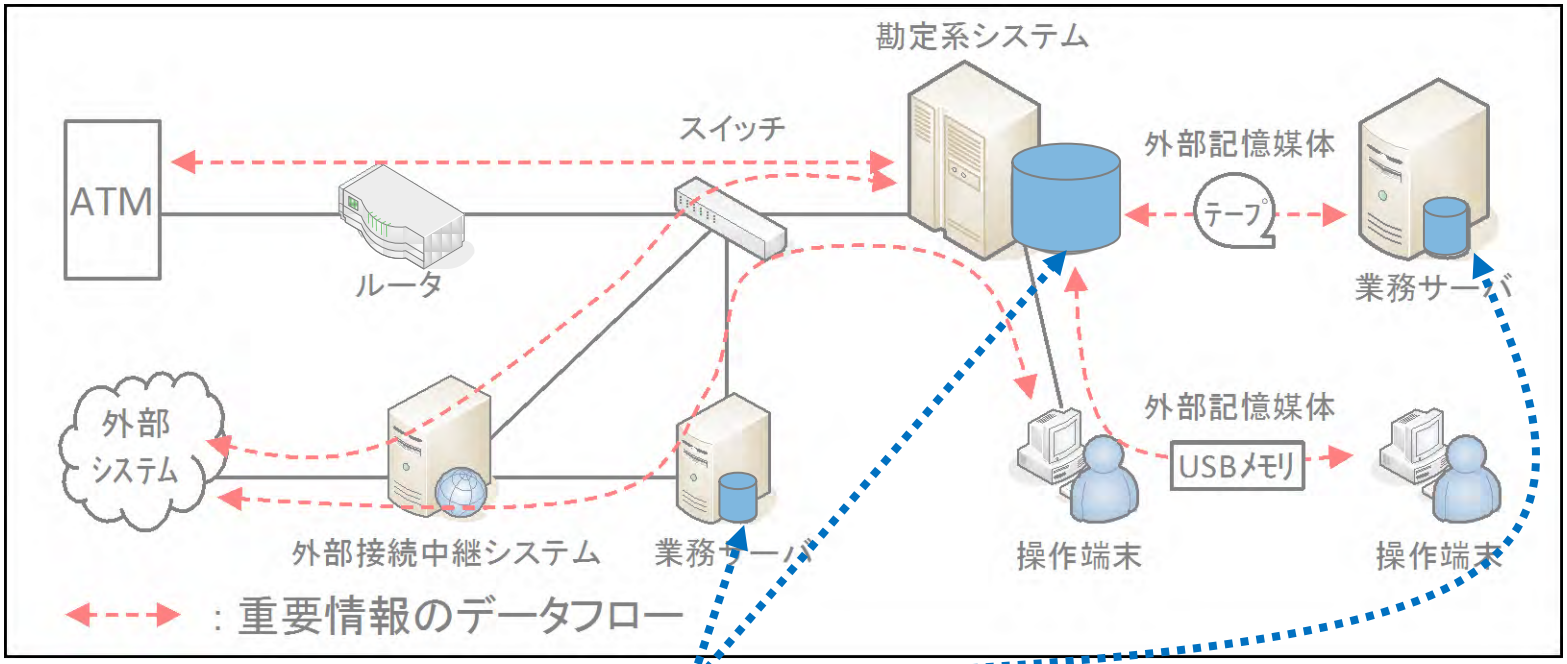
3. 留意点①:重要情報の保有状況の把握(続き)

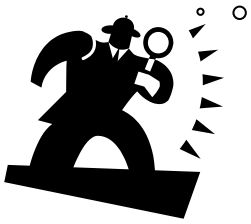
- 重要情報の保有状況の把握

- 重要情報を**取り扱う業務**を特定
- 重要情報の**データフロー**を把握
- 重要情報を**保有する可能性のあるシステム・機器**を特定

3. 留意点①:重要情報の保有状況の把握(続き)

- 従来のリスク管理手法





データベースを中心にリスク評価

⇒ ATMやネットワーク機器等でも、ログ等で重要情報を保有する可能性がある。また、エラー処理の際に詳細なログを出力する仕組みとなっているプログラムもある。

3. 留意点①：重要情報の保有状況の把握（続き）

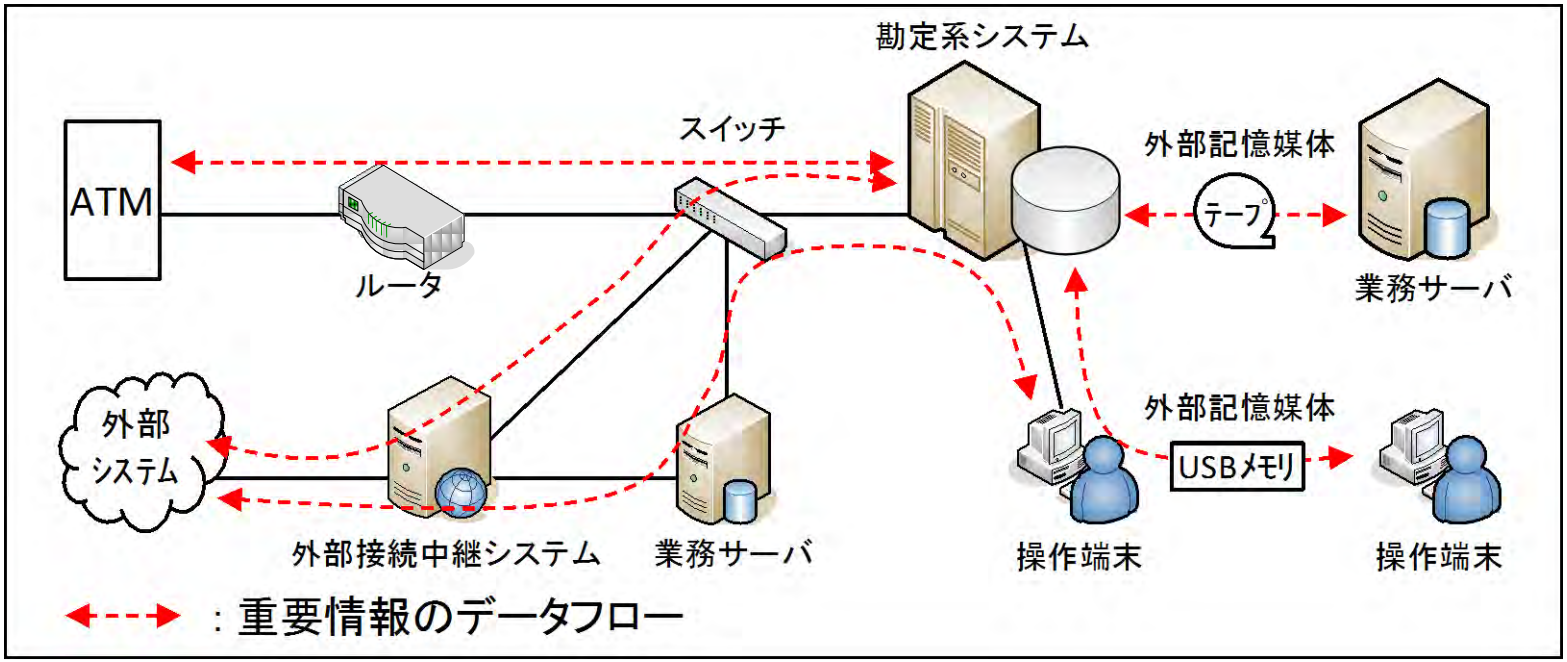
- 重要情報を取り扱う業務の特定

業務種別	業務内容
銀行取引関連業務	・入出金取引 ・振込・振替取引　等
システム関連業務	・バックアップデータ保管 ・バッチ処理　等

銀行取引業務以外にも、システム関連業務等でも
重要情報を取り扱う可能性もある点、留意が必要。

3. 留意点①:重要情報の保有状況の把握(続き)

- 重要情報のデータフローの把握



- 業務毎にデータフローを確認し、どのシステム・機器を経由しているか特定。
- ネットワーク経由のデータフローだけでなく、テープやUSB等を経由したデータフローも考慮する。

3. 留意点①:重要情報の保有状況の把握(続き)

- 重要情報を保有する可能性のあるシステム・機器の特定

確認項目	想定される保有の形態
保有場所	・データベースとして格納 ・ログ等の中だけに保有　等
保有期間	・一時的保有 ・長期的保有　等
加工状況	・平文 ・暗号化 ・マスキング　等

  - データフロー上の各システム・機器について、上記の項目を確認。

3. 留意点②:重要情報を取り扱う運用業務の把握

- 重要な顧客情報の取扱いと環境変化
- **システム面のリスク管理強化に向けた留意点**
  - 重要情報の保有状況の把握
    ～ログ情報にも内在し得る重要情報
  - **重要情報を取り扱う運用業務の把握**
    ～ 障害対応にも留意が必要
  - リスク対策の実施状況の把握
    ～重要情報に対するアクセス制御の実施状況等
  - リスク評価を踏まえた対策の強化
- 状況変化に応じた見直しの実施

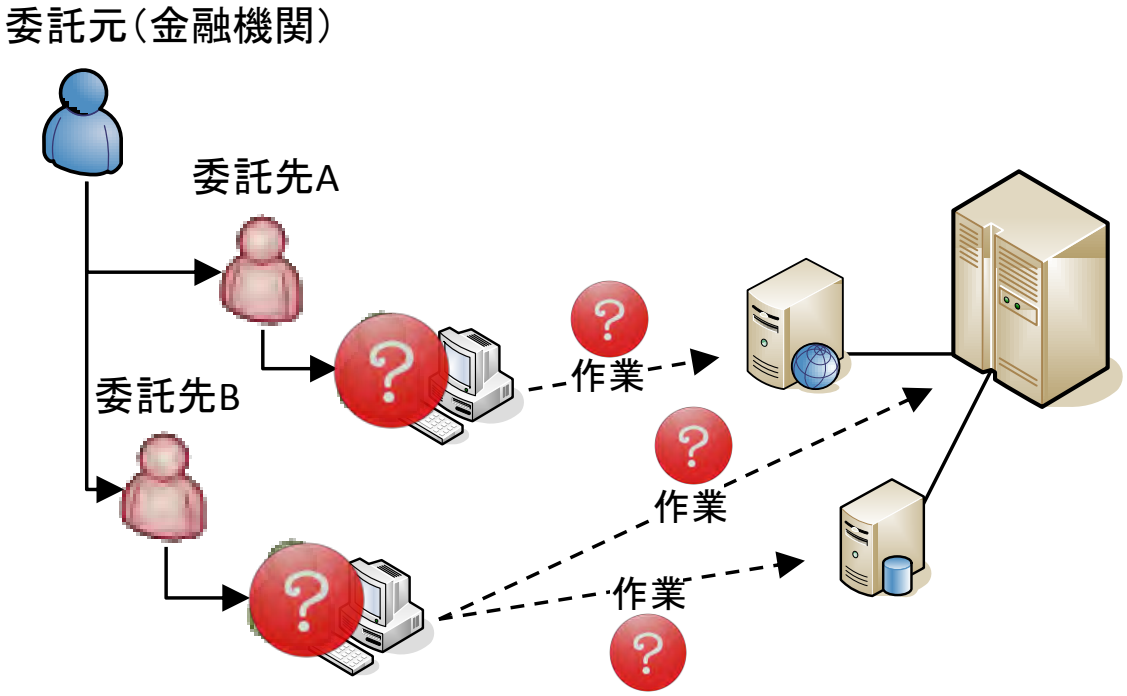
3. 留意点②：重要情報を取り扱う運用業務の把握（続き）

- 重要情報を取り扱う運用業務の把握

- 各業務に関与する**取扱者を特定**
- 各システム・機器で発生し得る**業務の内容を特定**

3. 留意点②：重要情報を取り扱う運用業務の把握（続き）

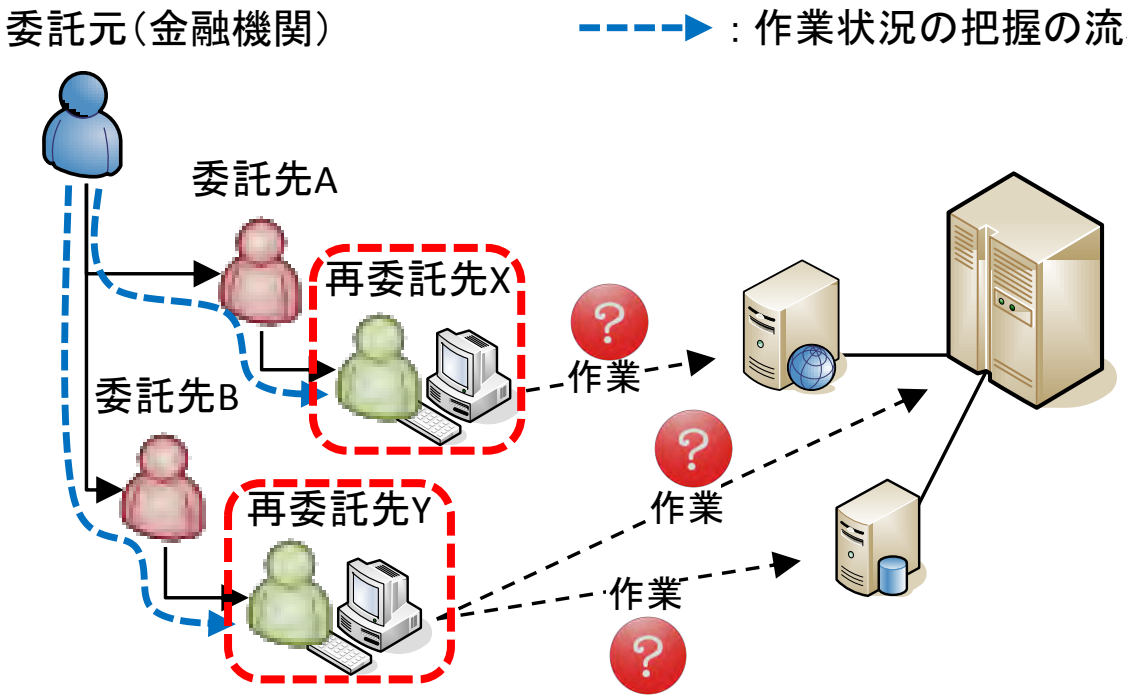
- 外部委託の拡大・多層化に伴うリスク管理の困難化

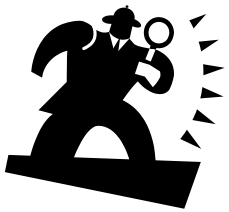


重要情報は誰が、どのような業務で取り扱っている？？

3. 留意点②:重要情報を取り扱う運用業務の把握(続き)

- 取扱者の把握





各業務に関与する取扱者の特定！

3. 留意点②：重要情報を取り扱う運用業務の把握（続き）

- 各システム・機器で発生し得る運用の内容の特定

システム運用の分類	想定される作業
通常時運用 ⇒作業内容がほぼ定型化	・システム起動・停止 ・システム監視 ・ジョブの実行 ・データバックアップ ・定期保守点検　等
臨時運用	・障害対応（ログ収集、障害分析、障害復旧） ・臨時保守　等

臨時運用は、通常時運用に比べ、予め十分な管理体制を確保しないまま、意図せず重要情報を取扱ってしまうリスクが懸念される点、留意が必要。

3. 留意点②：重要情報を取り扱う運用業務の把握（続き）

- 各システム・機器で発生し得る運用の内容の特定

臨時運用	想定される運用事例
障害対応	・ネットワーク機器での電文の取得 ・本番作業エリア外（委託先の執務エリア等）での障害分析作業　等
臨時保守	・機器交換　等

機器やソフトウェアによっては、通常運用では使用しない可能性のある管理ツールが搭載され、重要情報の取得が可能となっている状況も想定される。
⇒搭載されている機能を十分に把握することが重要！

3. 留意点③:リスク対策の実施状況の把握

- 重要な顧客情報の取扱いと環境変化
- **システム面のリスク管理強化に向けた留意点**
  - 重要情報の保有状況の把握
    ～ログ情報にも内在し得る重要情報
  - 重要情報を取り扱う運用業務の把握
    ～ 障害対応にも留意が必要
  - **リスク対策の実施状況の把握**
    ～重要情報に対するアクセス制御の実施状況等
  - リスク評価を踏まえた対策の強化
- 状況変化に応じた見直しの実施

3. 留意点③:リスク対策の実施状況の把握(続き)

- リスク対策の実施状況の把握

項目	対策内容
重要情報を保有する機器における対策	・重要情報の暗号化やマスキング ・重要情報を保有する機器でのアクセス制御、不要な機能の無効化、重要情報アクセス時のアラーム発報　等
重要情報を取り扱う運用における対策	・特権IDの管理、複数名での運用、操作ログの取得・検証、作業権限の分離、カメラ等での監視等

3. 留意点④:リスク評価を踏まえた対策の強化

- 重要な顧客情報の取扱いと環境変化
- **システム面のリスク管理強化に向けた留意点**
  - 重要情報の保有状況の把握
    ～ログ情報にも内在し得る重要情報
  - 重要情報を取り扱う運用業務の把握
    ～ 障害対応にも留意が必要
  - リスク対策の実施状況の把握
    ～重要情報に対するアクセス制御の実施状況等
  - **リスク評価を踏まえた対策の強化**
- 状況変化に応じた見直しの実施

3. 留意点④:リスク評価を踏まえた対策の強化(続き)

- 留意点①～③の整理

確認項目	確認すべき内容
重要情報を取り扱う業務	・業務のプロセスと重要情報
重要情報の保有状況	・重要情報を保有するシステム・機器 ・保有の形態 －保有場所(データベースとして格納／ログ等の中だけに保有　等) －保有期間(一時的保有／長期的保有　等) －加工状況(平文／暗号化／マスキング　等)
重要情報を取り扱う運用	・上記機器毎の取扱者(金融機関職員／委託先)、運用内容　等)
リスク対策	・アクセス制御や、データの暗号化等のリスク対策の内容

3. 留意点④:リスク評価を踏まえた対策の強化(続き)

- 確認結果の一覧化(一覧表のイメージ)

[業務名 : 自行宛送金]

機器	営業店端末	スイッチ	ルータ	外部ネットワーク	中継サーバ	スイッチ	勘定系サーバ
設置場所	営業店			外部	システムセンター(本番環境)		
重要情報の保有場所(保有期間)	システムログ(1カ月)、ジャーナル(1カ月)	電文中継	電文中継	電文中継	システムログ(3カ月)、アプリケーションログ(3カ月)、エラーログ(3カ月)	電文中継	データベース(無期限)、システムログ(3カ月)、アプリケーションログ(3カ月)、エラーログ(3カ月)
保有する重要情報(加工状況)	口座番号(暗号化)、暗証番号(マスキング)	口座番号(平文)、暗証番号(暗号化)	口座番号(平文)、暗証番号(暗号化)	口座番号(通信暗号化)、暗証番号(通信暗号化)	口座番号(平文)、暗証番号(平文)	口座番号(平文)、暗証番号(暗号化)	口座番号(暗号化)、暗証番号(暗号化)
取扱者	端末管理担当者、〇〇社保守要員	ネットワーク管理者、××社保守要員	ネットワーク管理者、××社保守要員	△△社保守要員	□□社運用要員、〇〇社保守要員	ネットワーク管理者、××社保守要員	運用担当者、□□社運用要員、〇〇社保守要員
運用内容	通常時:ログ取得 臨時:ログ・ジャーナル取得、設定変更、機器交換	通常時:なし 臨時:設定変更、パケットキャプチャ、機器交換	通常時:なし 臨時:ログ取得、設定変更、パケットキャプチャ、機器交換	通常時:ログ取得 臨時:ログ取得、パケットキャプチャ、機器交換	通常時:なし 臨時:ログ取得、設定変更、機器交換	通常時:なし 臨時:ログ取得、設定変更、パケットキャプチャ、機器交換	通常時:設定変更、プログラムリリース 等 臨時:ログ取得、設定変更、プログラムリリース、機器交換
リスク対策	・監視カメラ ・特権ID管理 ・アクセス制限 ・無線機能無効化 ・複数人作業 ・外部記憶媒体利用ログ取得・ログ監査	・特権ID管理 ・施錠管理 ・複数人作業 ・作業証跡確認 ・不要なサービス・ポートの停止	・特権ID管理 ・施錠管理 ・複数人作業 ・作業証跡確認 ・不要なサービス・ポートの停止	・監視カメラ ・入退室管理 ・特権ID管理 ・作業証跡確認 ・複数人作業	・入退室管理 ・特権ID管理 重要情報を不正取得されるリスクあり	・監視カメラ ・入退室管理 ・特権ID管理 ・作業証跡確認 ・複数人作業 ・不要なサービス・ポートの停止	・監視カメラ ・入退室管理 ・特権ID管理 ・作業証跡確認 ・複数人作業 ・外部記憶媒体利用ログ取得・ログ監査
備考				対策状況は、外部ネットワーク提供先に確認			

3. 留意点④:リスク評価を踏まえた対策の強化(続き)

- 整理に基づく、リスク対策の十分性の評価

【評価にあたってのポイント】

- 正当な作業に乗じた不正行為の防止または検知に有効か、といった視点をもつこと
- 重要情報の暗号化・マスキング等が難しい場合、運用面での対策も組み合わせることで、必要な牽制体制を確保すること
- 重要情報のデータフローの中に、外部機関が提供するサービス(ATMやインターネットバンキング等)が関与する場合には、同様の確認を行うこと

4. 状況変化に応じた見直しの実施

- 重要な顧客情報の取扱いと環境変化
- システム面のリスク管理強化に向けた留意点
  - 重要情報の保有状況の把握
    ～ログ情報にも内在し得る重要情報
  - 重要情報を取り扱う運用業務の把握
    ～ 障害対応にも留意が必要
  - リスク対策の実施状況の把握
    ～重要情報に対するアクセス制御の実施状況等
  - リスク評価を踏まえた対策の強化
- **状況変化に応じた見直しの実施**

4. 状況変化に応じた見直しの実施（続き）

- 一時的なリスク評価・対策に止まらず、システム構成やサービスの変化等に応じて、適時適切に見直すことが重要。

体制整備	具体的内容
開発標準への反映	システムの新規構築時や改修時には、リスクプロファイルの変化が想定されるため、開発時に使用する開発標準へ重要情報にかかるリスク評価項目を設定する。
既存のリスク評価プロセスへの反映	既存システムについても、環境変化や利用状況の変化によるリスクプロファイルの変化が想定されるため、既存のリスク評価プロセスへ重要情報にかかるリスク評価項目を設定する。

ご清聴ありがとうございました

本資料に関する照会先

日本銀行　金融機構局　考査企画課　システム・業務継続グループ　志村、伊藤、中井

tel: 03-3664-4333

email: csrbcm@boj.or.jp