MONEYKit

Enterprise General: EG-08

ソニー銀行の考える金融機関のAWS活用方式

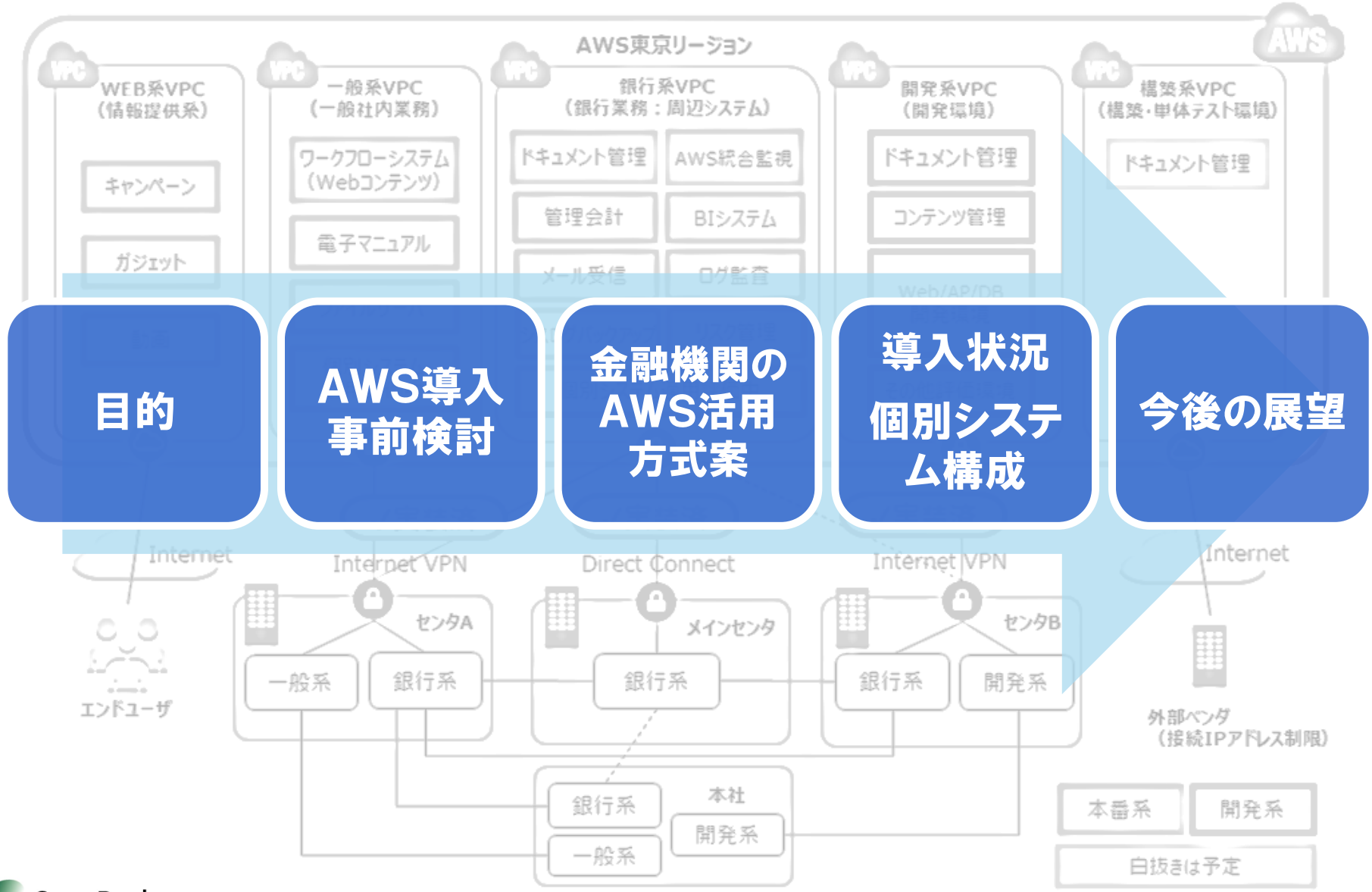
2014年7月18日

ソニー銀行株式会社
システム企画部 マネージャー 大久保光伸（基盤統括担当）

Sony Bank

MONEYKit

本セッションの構成



Sony Bank

MONEYKit

1 ソニー銀行の概要

Sony Bank

MONEYKit

企業概要

【事業概要】

個人向けインターネット専業銀行

【開　業】

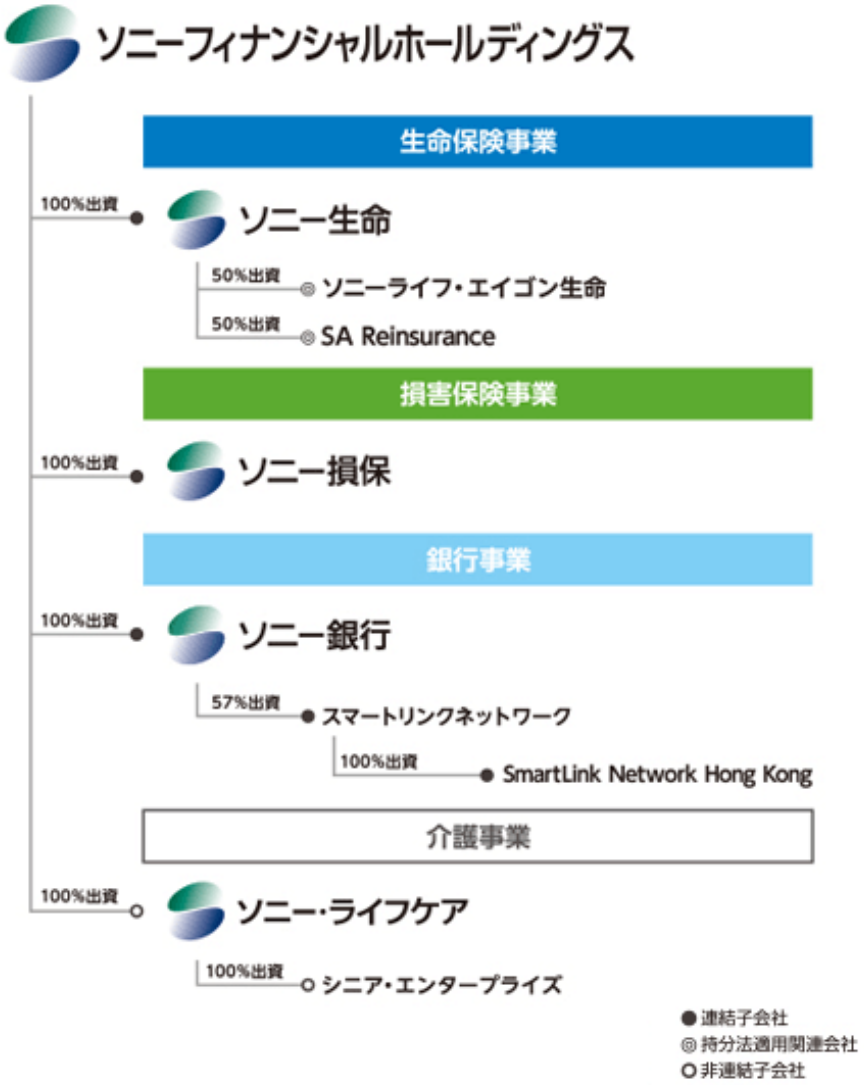
2001年6月11日

【資本金】

310億円

【主な商品】

預金（特に外貨預金に特徴）
住宅ローン
投資信託



＊ソニー・ライフケアは、ソニーフィナンシャルホールディングスの非連結子会社となる見込みです。

（2014年 4月1日現在）

MONEYKit

企業理念

Be fair. フェアであるということ。

- フェアである
- 日本経済の新たな成長に貢献する
- 資産運用ツールを提供する
- IT技術を最大限活用する
- 一人ひとりのお客さまのためのサービスを提供する
- より有利な商品、よりよいサービスを提供する
- インターネット・サービスのためのインフラを整備する
- 自由闊達で愉快な業務環境を整備する

MONEYKit

事業コンセプト・ミッション

自立した個人のための資産運用銀行

社会や企業から精神的に自立し、自分自身で投資判断を行う、
または行おうとする個人

MONEYkitは“お金のための道具箱”

個人が自分自身で選べるだけの十分な商品と情報を提供

お客さま目線の商品・サービスを追求

MONEYKit

MONEYKitの挑戦

MONEYKitは古い金融の常識を「新しい常識」に変えてきた。

	それまでの常識	Change!	MONEYKitの常識
インターネットバンキング	■ 振込み、残高照会などが中心の決済型バンキング ■ 銀行窓口営業時のみ稼動		■ 資産運用商品中心のフルバンキング ■ 24時間365日資産運用可能
為替レート	■ 為替レートは朝10時に決定し、１日１レート ■ 為替手数料１米ドルあたり片道１円		■ 市場レートと連動する取引レートを常時提示 ■ 為替手数料１米ドルあたり片道15銭（更に残高に応じた優遇制度で片道8銭）
預金金利	■ 都市銀行を中心とした横並び		■ 人件費や店舗コストを抑え、よりマーケットに近い金利を提示 ■ マーケット変動を迅速に反映
住宅ローン	■ 申し込みは銀行窓口で ■ 繰り上げ返済は店頭で、まとまった金額から。手数料も必要 ■ 変動／固定金利の組み合わせは対応できない		■ 来店不要、ネットでのやり取りでローン実行 ■ 繰り上げ返済はネットでいつでも1万円から手数料は無料 ■ お借り入れ後も金利タイプ変更可能、変動／固定金利比率も可変

MONEYKit

沿革

ソニー生命主要支社での住宅ローン対面相談受け付け開始 **2013年1月**

ワンタイムパスワード導入 **2012年7月**

変動セレクト住宅ローンの取り扱い開始 **2011年8月**

スマートフォンサイト開設 **2011年8月**

開業10周年 **2011年6月**

住宅ローンプラザ設置 **2010年6月**

2008年1月 ソニー生命が銀行代理店に

2007年4月 ソニー生命を引受保険会社とする
住宅ローン3大疾病保障特約付団
信取り扱い開始

2004年12月 ソニー生命のライフプランナーによる
住宅ローンの取り次ぎ業務開始

SFH設立 **2004年4月**

2002年3月 住宅ローンの取り扱い開始

2001年9月 外貨預金の取り扱い開始

2001年4月 設立／6月 開業（円預金・投資信託・カードローン）

Sony Bank

MONEYKit

大久保 光伸「オオクボ ミツノブ」

2009年12月入社（前職：株式会社電通国際情報サービス）

特技：基盤と英語

趣味：目黒『SUN＊MASTERS』（キッズフラッグフットボール）のコーチ

システム企画部 マネージャー 基盤統括担当

【主な担当業務】

- ITインフラ構造の全体最適化推進、クラウド基盤活用
- インフラ更改案件、個別案件の実施
- 国内外における先端技術の調査、活用検討

ミッション：ソニー銀行システムの安定稼働（24時間365日）

MONEYKit

2 ＡＷＳ導入の狙いと背景

Sony Bank

MONEYKit

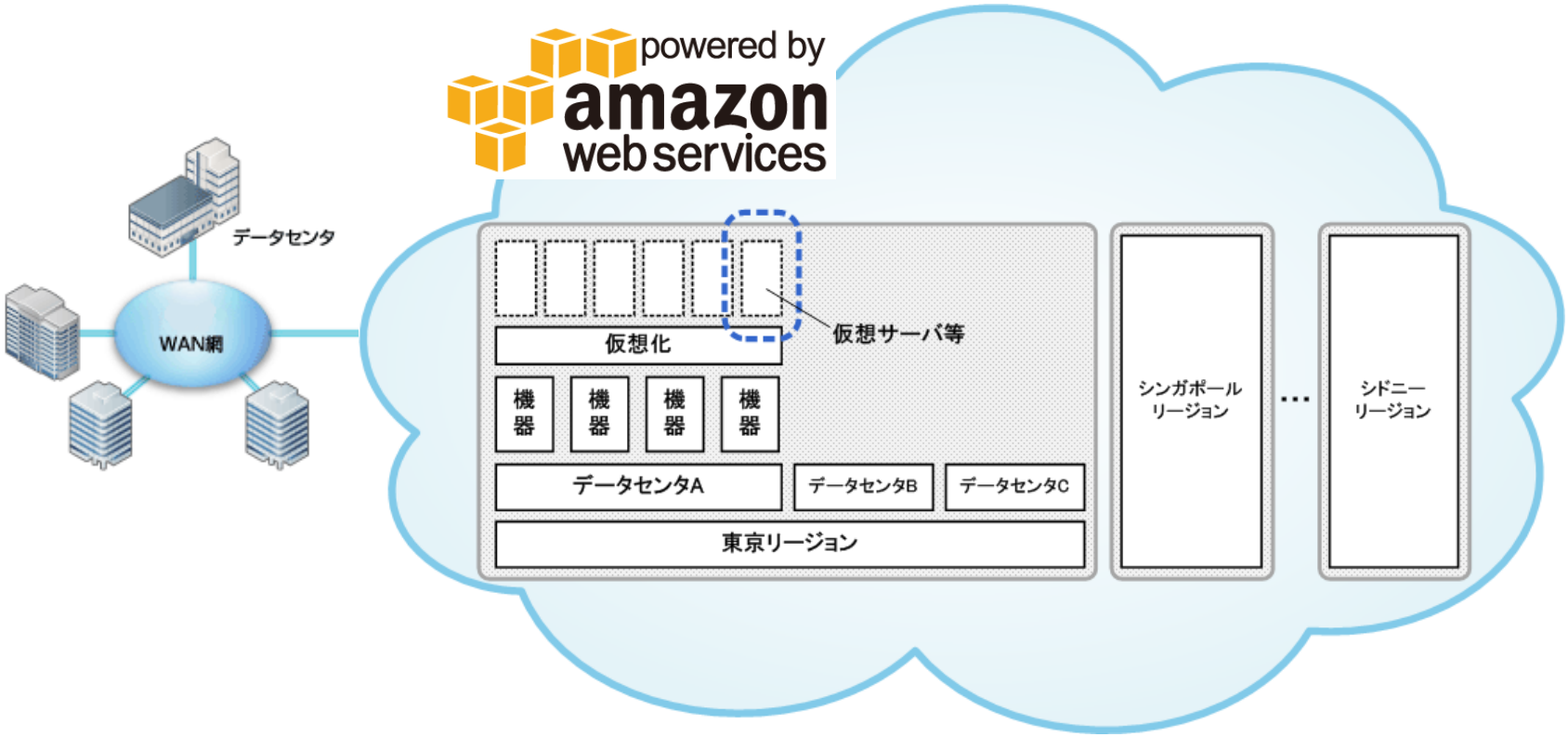
AWSの導入目的

- ITコストの最適化
  （インフラ構築・管理の効率化）
- 俊敏性の向上（ビジネスの加速）

MONEYKit

クラウドサービスの選定

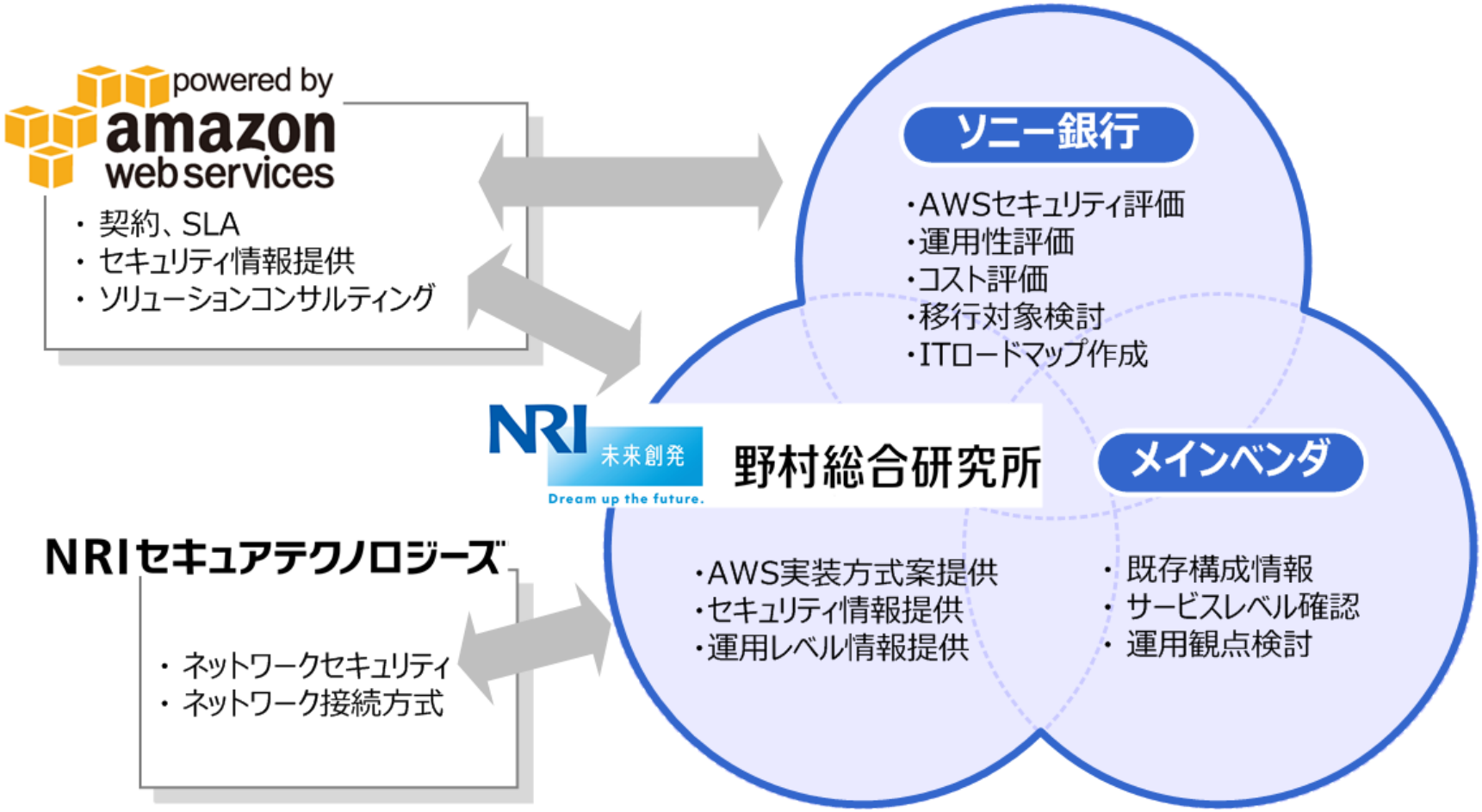
- 既存データセンタと直結可能なIaas型クラウドサービスについて2011年度から検討開始
- 国内を含め大手クラウドサービスの①実績と信頼性、②セキュリティ認証、③コスト、④テクノロジ、⑤システムメンテナンスをポイントに比較した結果、AWSを事前検討対象として選定



MONEYKit

AWS事前検討体制

AWS導入コンサルタントとしての実績からNRIを選定し、事前検討を実施



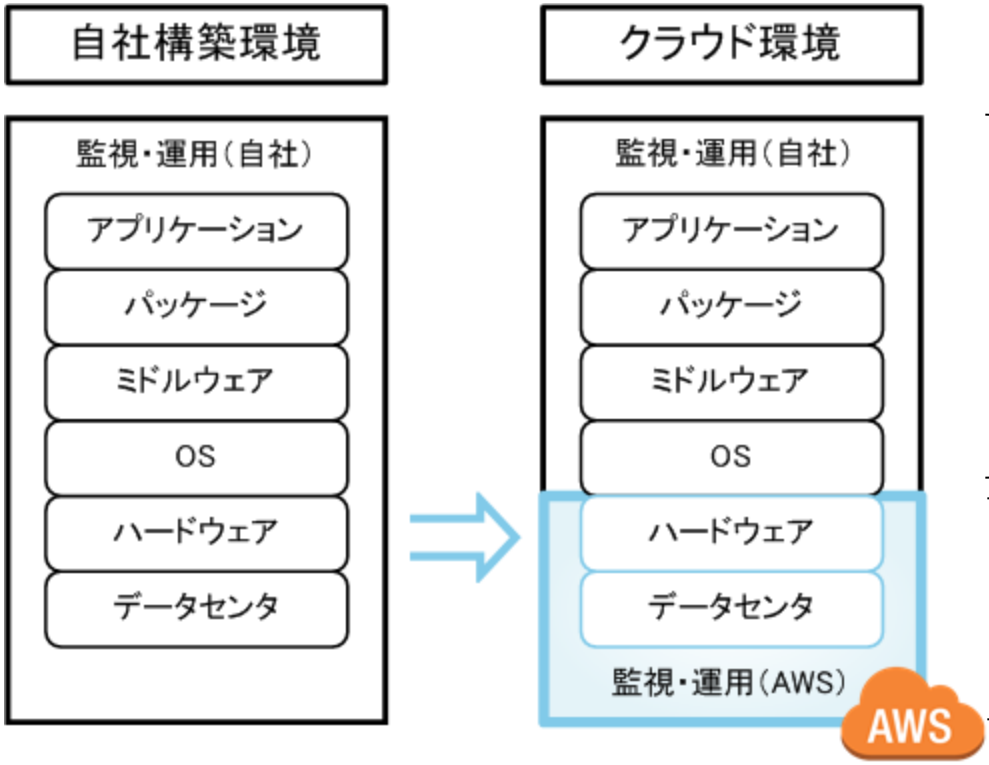
MONEYKit

AWSセキュリティ確認

- AWSクラウドセキュリティモデルの評価
- FISC安全対策基準の適合性確認
- 当社制定のリスク評価項目に基づく確認

MONEYKit

AWS責任共有モデル



自社構築の範囲

- クラウド移行後もOSより上の構築管理は、従来通り監視・運用を含めメインベンダにて実施
- 本番作業申請、承認フローのついても同様

AWSの範囲

MONEYKit

AWSセキュリティ評価

AWSではセキュリティ・内部統制の基準をクリアした信頼性の高いシステム運用を実施

- グローバルな基準である、ISO27001（セキュリティ基準）、SSAE3402（内部統制基準、旧SAS-70 Type II）、PCI DSS（クレジットカードのセキュリティ基準）などの認証を取得。
- 米国の国防総省、NASAなど各種政府機関がAWSを利用しており、それら機関の基準をクリア。
- NRI、SCSK、ISIDによりFISC安全対策基準への適合も確認済み。

- SSAE16/ISAE3402（旧SAS-70 Type II）認証
  - ✓ 外部委託作業における内部統制の監査を効率化する規定
  - ✓ 体制、従業員ライフサイクル、物理/論理セキュリティ、データ保存/可用性、変更管理、インシデント発生時対応などの項目についての認証
- ISO27001認証
  - ✓ 組織のISMS（情報セキュリティマネジメントシステム）の認証
- PCI DSS 認証（Payment Card Industry Data Security Standard）
  - ✓ カード業界のグローバルセキュリティ基準
  - ✓ VISA,MC,Amex,JCB等が策定
- FISMA Moderateレベル（Federal Information Security Management Moderate）
  - ✓ 連邦情報セキュリティマネジメント法
  - ✓ 情報システムのセキュリティ強化、安全な運用

MONEYKit

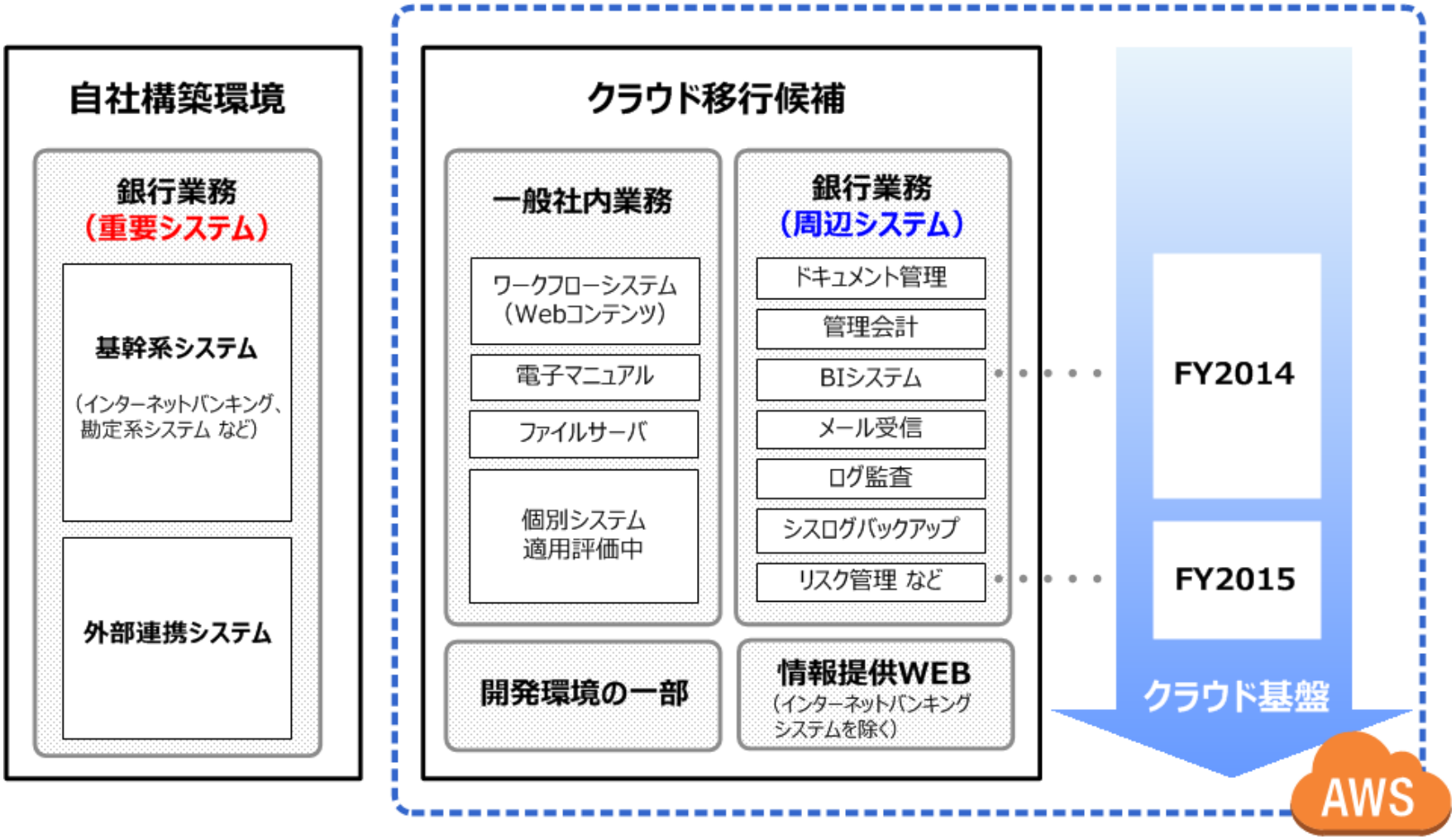
AWSサービスマッピング

- システム全体AWS構成定義
- 運用フィージビリティー確認
- コスト試算（サービス選定、サイジング）

MONEYKit

AWS移行候補システム

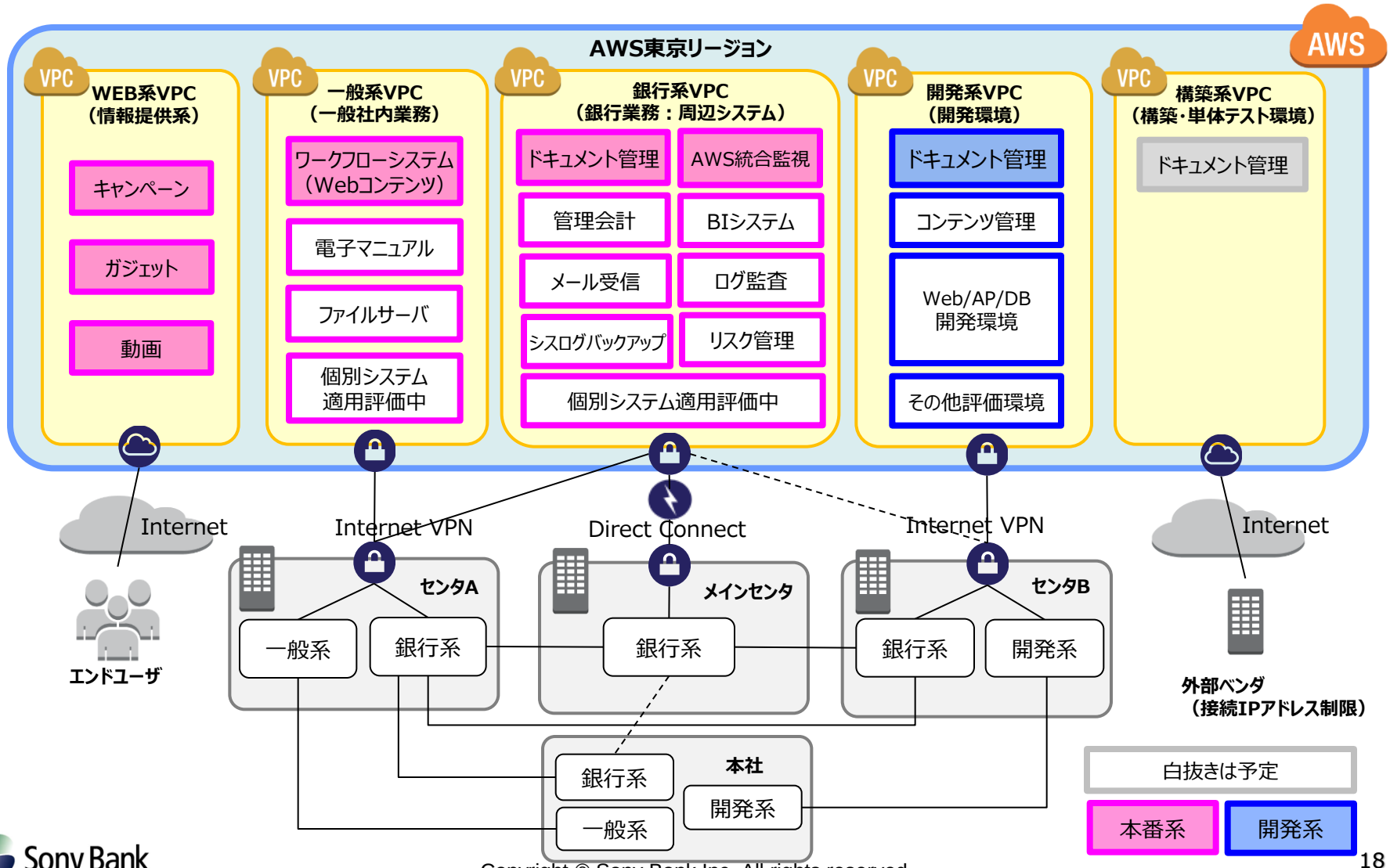
移行対象は『一般社内業務システム』および『銀行業務（周辺システム）』



MONEYKit

AWS導入のスコープ決定

評価結果を踏まえ2013/12/4にAWS導入における方針決裁を取得



Sony Bank

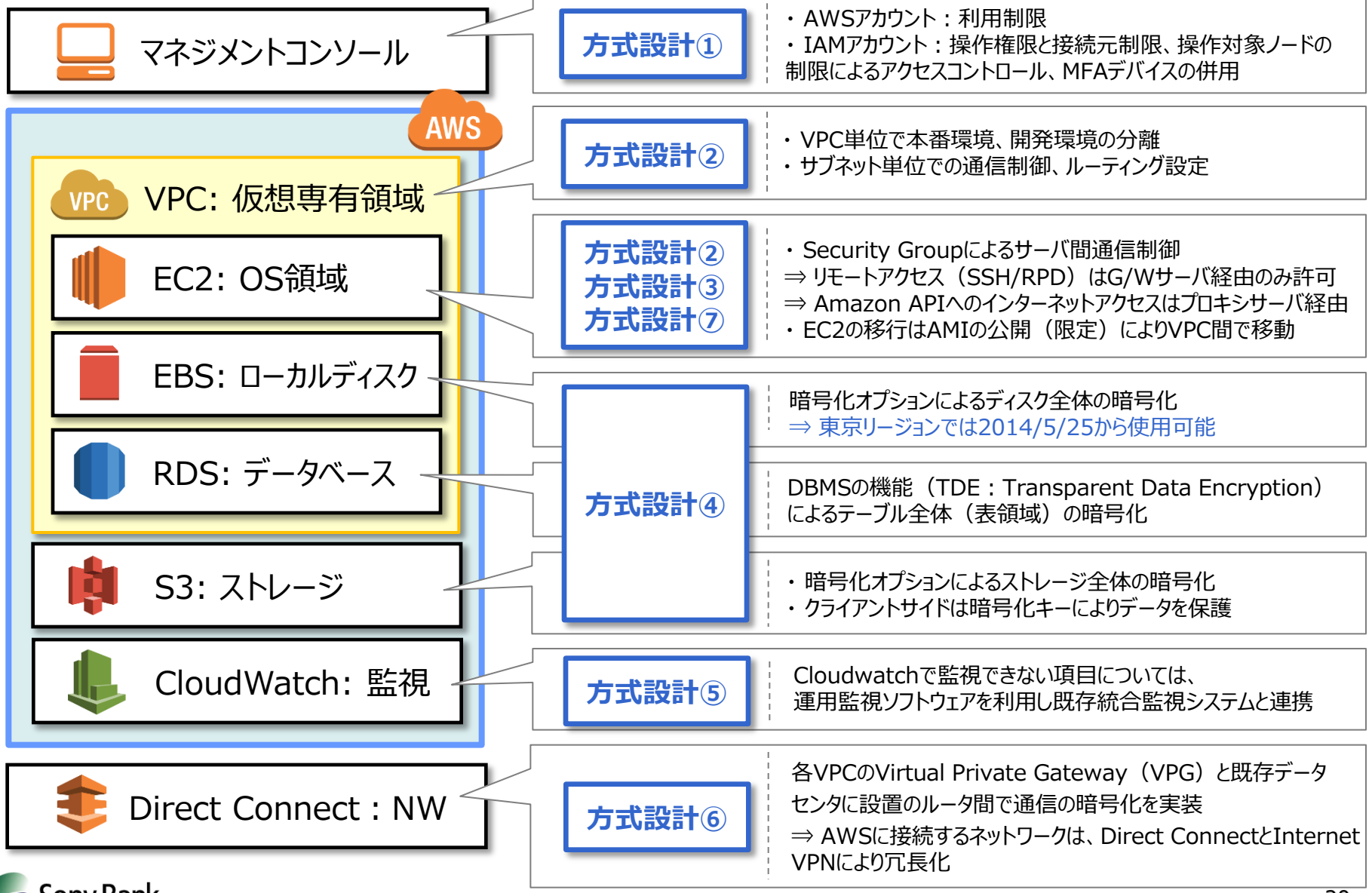
MONEYKit

3 金融機関におけるＡＷＳの活用方式案

Sony Bank

MONEYKit

基盤として活用するための7つのポイント



Sony Bank

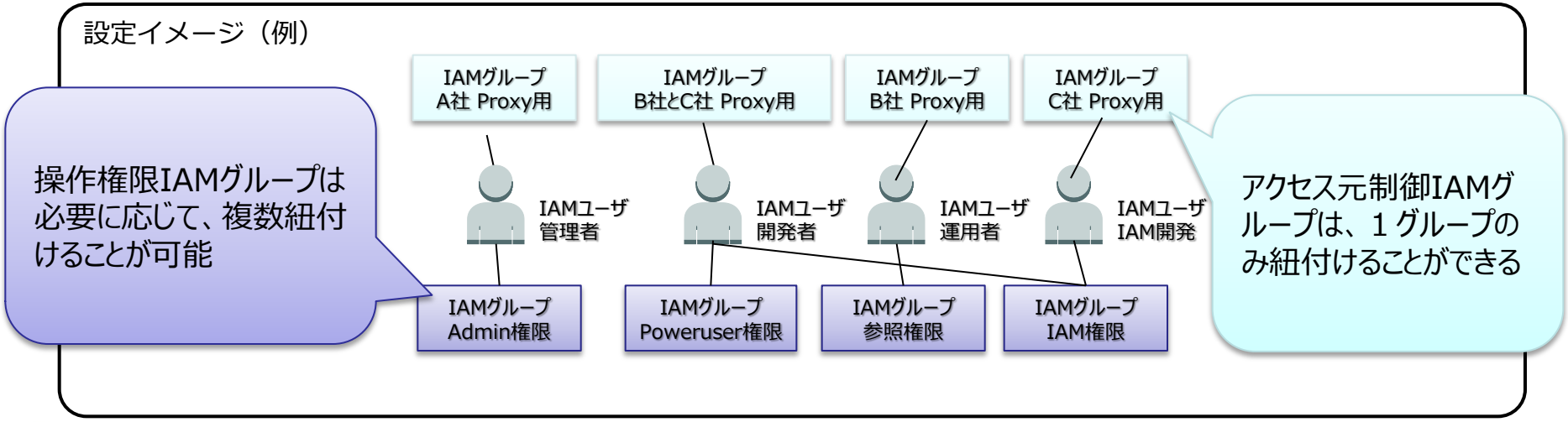
MONEYKit

方式設計①：IAMアカウント設計

- IAMユーザとIAMグループでAWSサービスに関する権限を管理
  ⇒ さらにIAMグループは『操作権限グループ』と『アクセス元制限グループ』を用意
  ⇒ アクセス元制限グループの制御により、アカウントを『無効』状態にすることも可能
- 運用や構築時に利用するIAMユーザーは、タグを利用し、関係のないEC2インスタンスに対する操作を制御
- AWSサービスの変更権限を持つアカウントはMFAデバイスを併用

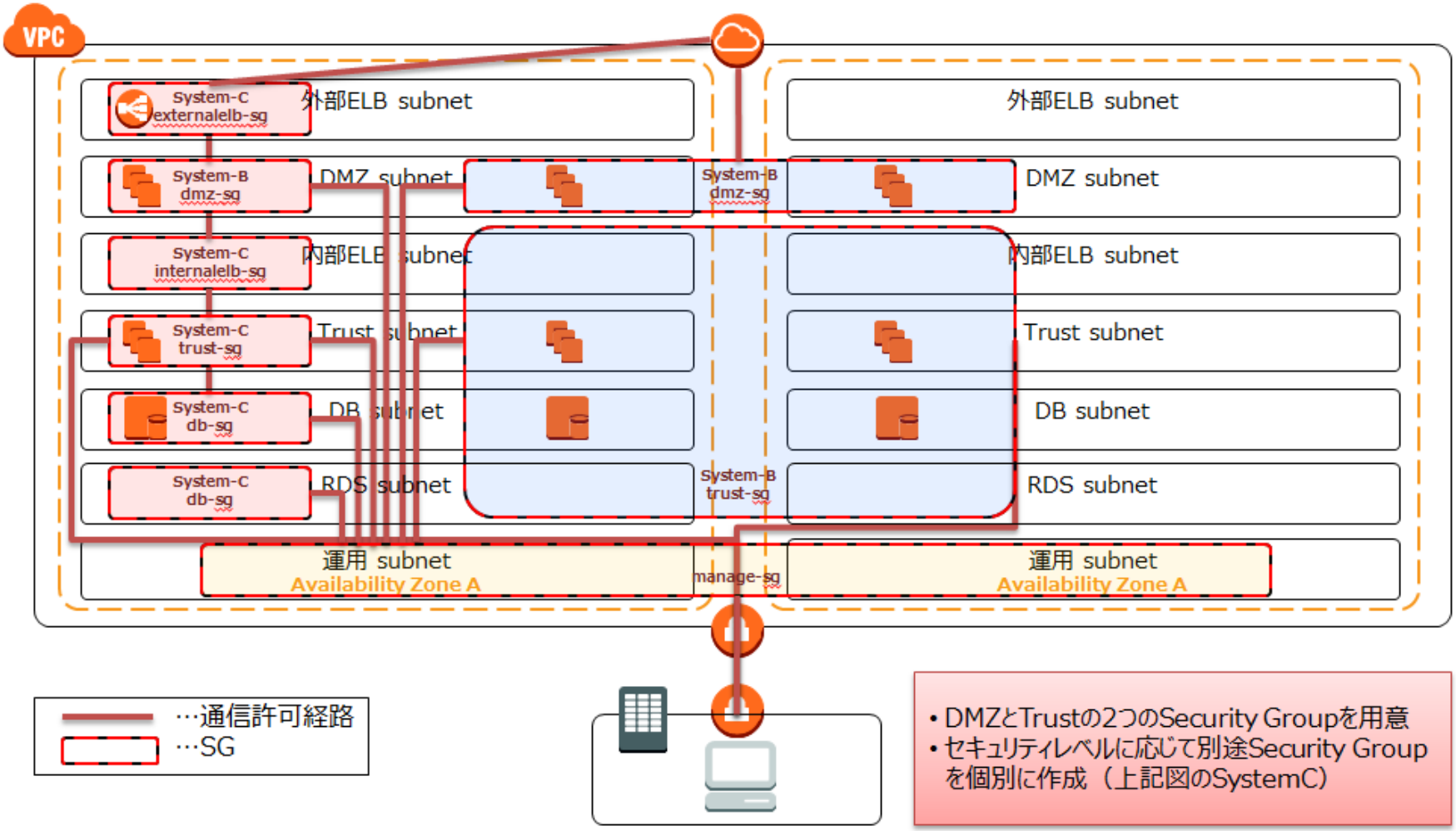
IAMユーザー（個人orチーム単位）	IAMグループ１（操作権限IAMグループ）	IAMグループ２（アクセス元制限IAMグループ）
（例）SBK_mitsunobu_okubo	ref, start-stop	from_sonybank

設定イメージ（例）



方式設計②：システム間通信制御

- 通信制御はSecurity Groupを利用（Subnet単位でのNetworkACLはデフォルト）
- Subnet用途、システム毎にSecurity Groupを作成し、必要最低限の通信を許可



方式設計③：インターネット通信制御

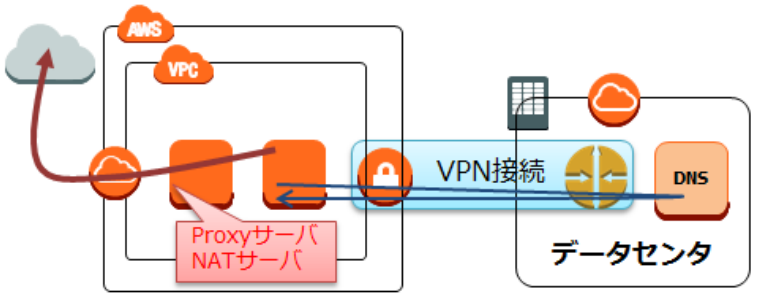
インターネット接続が必要なケース（例）

- AWS管理コンソールへの接続
- EC2の起動停止やS3へのログ格納などでAmazonAPIを利用する場合
- EC2やRDSのエンドポイント（IPアドレスの別名）の名前解決が必要な場合
  ⇒ RDSのIPアドレスはサブネットで設定した範囲内で自動的にIPアドレスが変わることがあるため、当該エンドポイントをOracleクライアント等接続元で設定
  ⇒ 本件は、AWS内部のDNSを参照することで回避が可能

【課題：FW機器による通信制御】

FW機器はそもそもの仕様として設定configが一瞬で反映されるものではないので、TTLが短く頻繁にIPが変わるドメイン名でのフィルタは難しい

【ソリューション（例）】



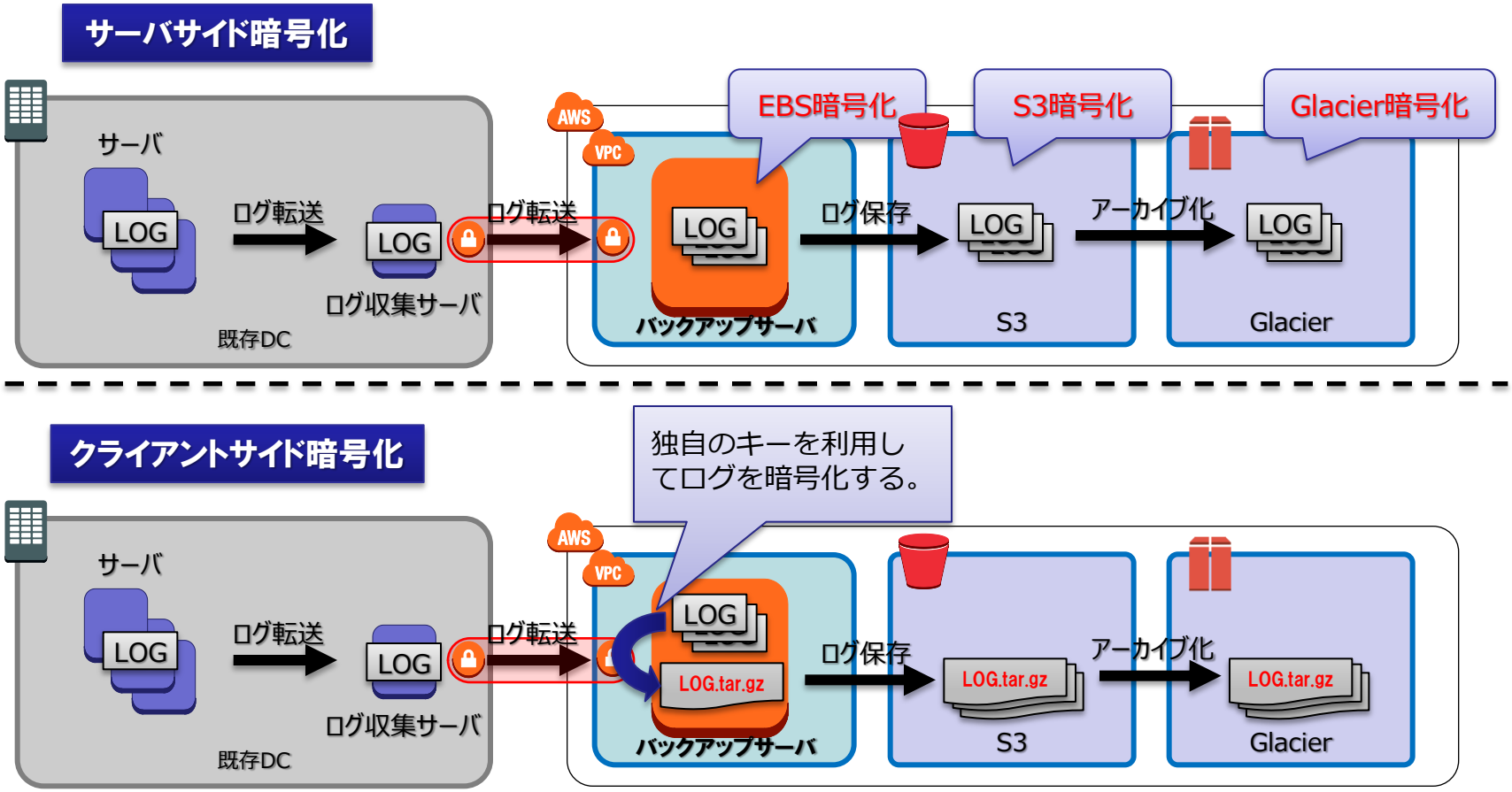
① Proxyサーバ経由でインターネットへアクセス
② Proxyサーバの設定で送信先のURLと接続ポートを制限
③ Proxyサーバへのアクセスコントロール（SG）

MONEYKit

方式設計④：暗号化方式

データの暗号化は下記の２つの方式で実装

- サーバサイド暗号化・・・EBSやS3などの**AWSの機能を利用**した暗号化
- クライアントサイド暗号化・・・**独自のキーを利用**してログそのものを暗号化



Sony Bank

MONEYKit

方式設計⑤：監視方式

Cloudwatchで監視できない項目については、運用監視ソフトウェアで補完

⇒ 当社の場合はOSSのZabbixを採用し、既存統合監視システムと連携

＜システム監視項目と監視方法＞

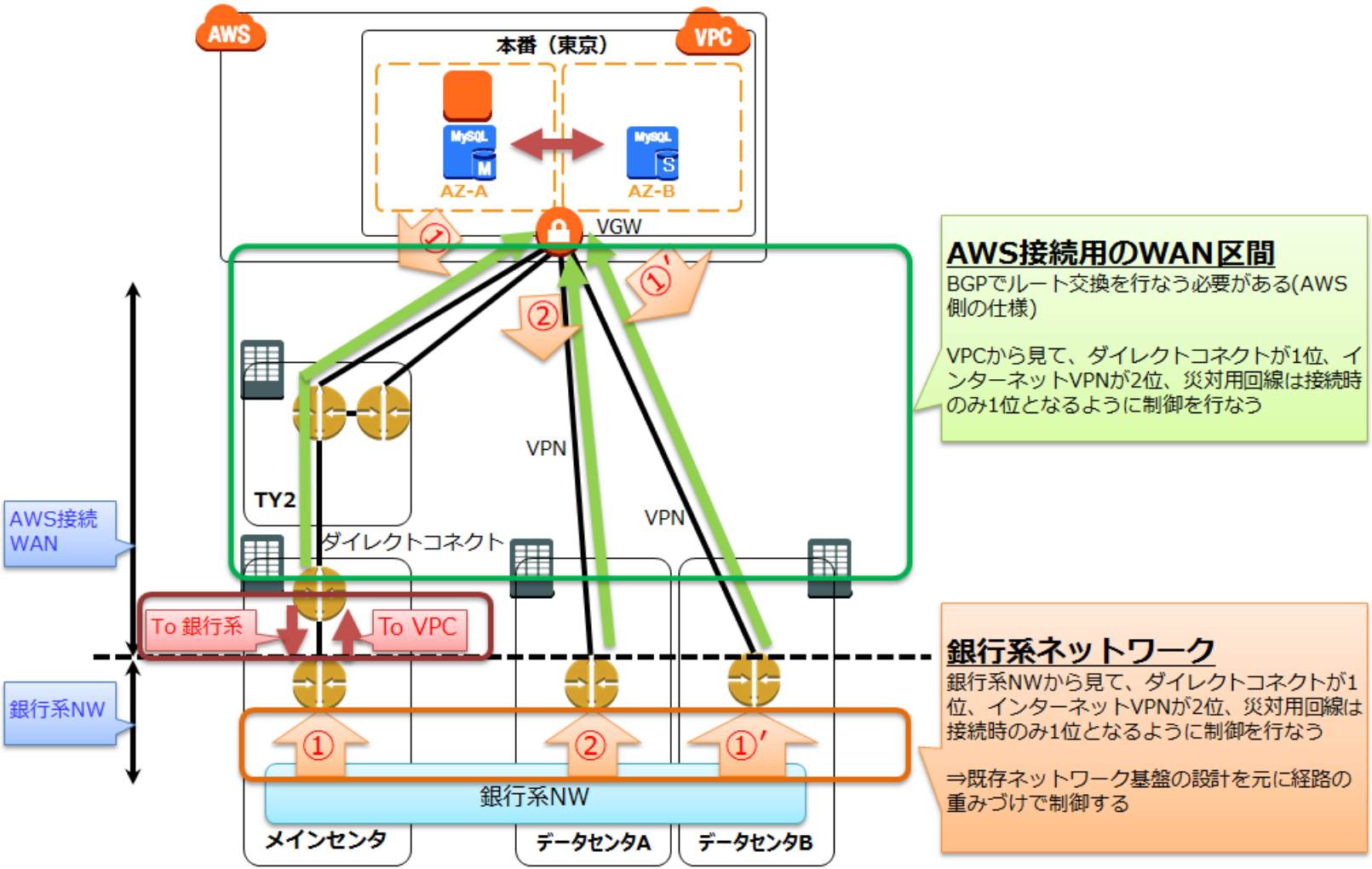
サーバー監視機能	監視項目	監視方式	備考
H/W監視	サーバ機器監視	AWS責任範囲	・HW、Hyper Visorのレイヤは AWSで管理 ・全て多重化されているため通常障害時も業務影響はないが、機器交換時にOSリブート要
	ストレージ機器監視	AWS責任範囲	
	ネットワーク機器監視	AWS責任範囲	
Hypervisor監視	Hypervisor監視	AWS責任範囲	
VM監視	VM 監視	運用監視ソフト or CloudWatch監視	・障害発生時は運用担当者にメールを送信することも可能 ・プロセス監視、ログ監視はCloudWatchで監視することができないため、Zabbixの機能で補完
プロセス監視	**プロセス監視**	**運用監視ソフト**	
リソース監視	CPU監視	運用監視ソフト or CloudWatch監視	
	メモリ監視	運用監視ソフト or CloudWatch監視	
	ディスク監視	運用監視ソフト or CloudWatch監視	
	ネットワークI/O監視	運用監視ソフト or CloudWatch監視	
	ディスクI/O監視	運用監視ソフト or CloudWatch監視	
ログ監視	**システムログ監視**	**運用監視ソフト**	
	ミドルウェアログ監視	**運用監視ソフト**	
	アプリケーションログ監視	**運用監視ソフト**	

＜Cloudwatchについて＞
- Cloudwatch標準機能で、サーバの死活、CPU利用率、Network In/Outなどの情報を見ることが可能
  （標準で5分に1回。有料オプションで1分に1回に変更可能）
- Cloudwatchの値をベースにアラーム設定可能（メール通知など）
- Cloudwatchのデータは２週間分保存

MONEYKit

方式設計⑥：ネットワーク冗長化

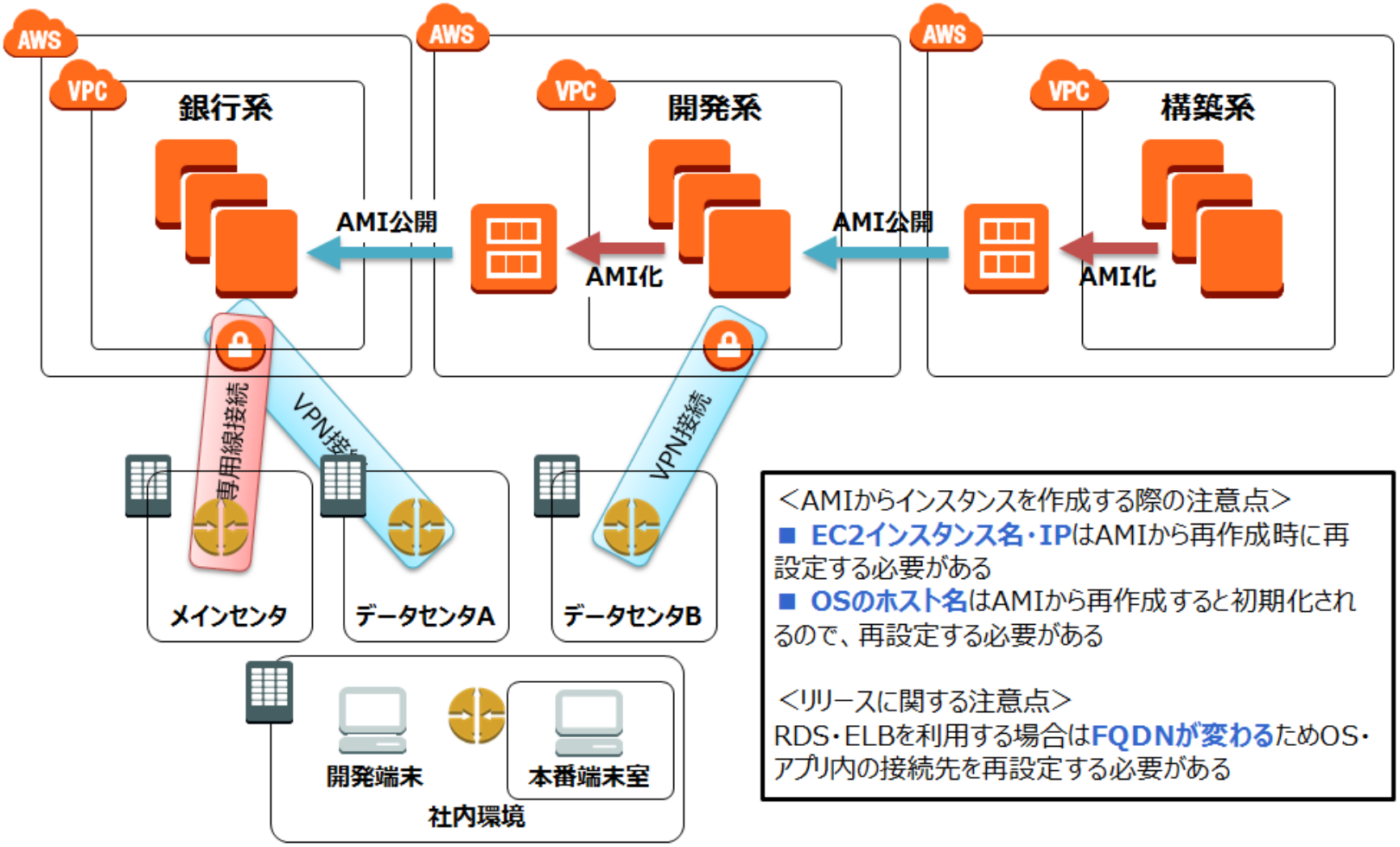
ネットワーク回線（基地局）の冗長化におけるルーティング制御方式
⇒ Direct Connectはデータ通信費で一定の効果があるため主系として利用



Sony Bank

方式設計⑦：EC2の移行方式

EC2の移行は、構築系における単体テスト・セキュリティグループ設定の完了後、
『AMIを公開』し、開発環境（移行リハーサル、結合テスト環境）へ移行



＜AMIからインスタンスを作成する際の注意点＞
■ **EC2インスタンス名・IP**はAMIから再作成時に再設定する必要がある
■ **OSのホスト名**はAMIから再作成すると初期化されるので、再設定する必要がある

＜リリースに関する注意点＞
RDS・ELBを利用する場合は**FQDNが変わる**ためOS・アプリ内の接続先を再設定する必要がある

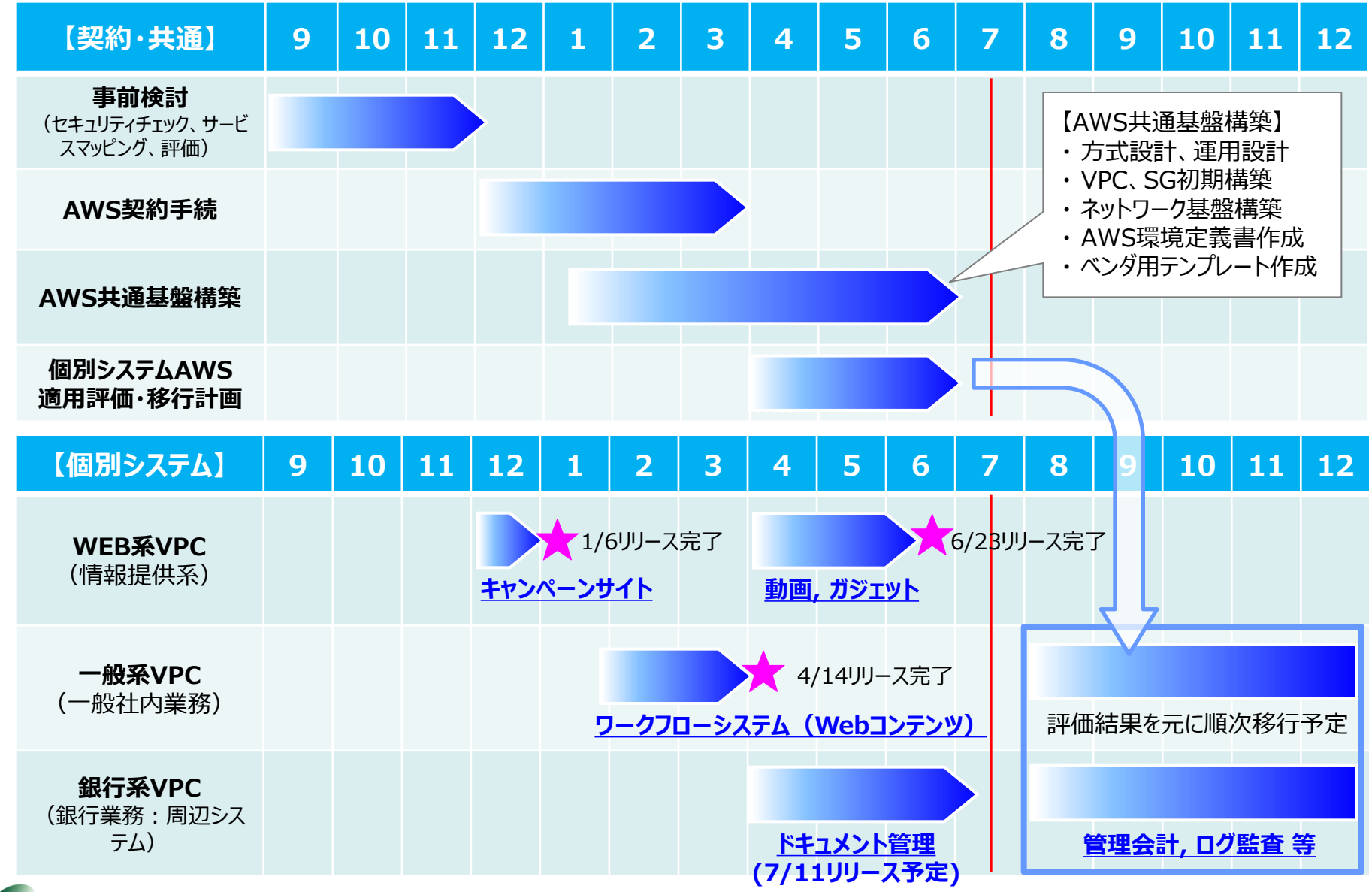
MONEYKit

4 ＡＷＳ導入進捗状況

Sony Bank

MONEYKit

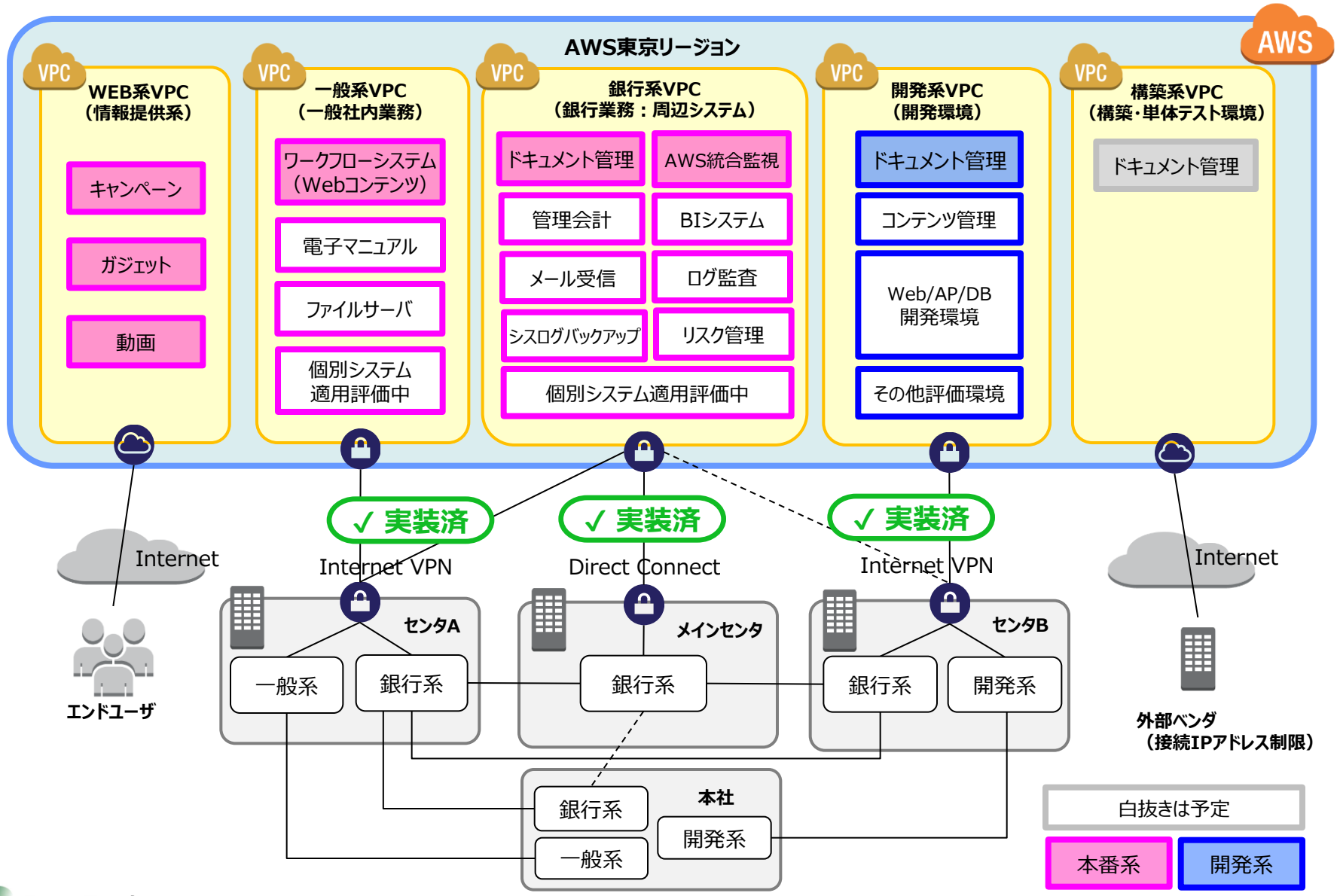
【AWS導入進捗状況】スケジュール（2013-2014）



Sony Bank

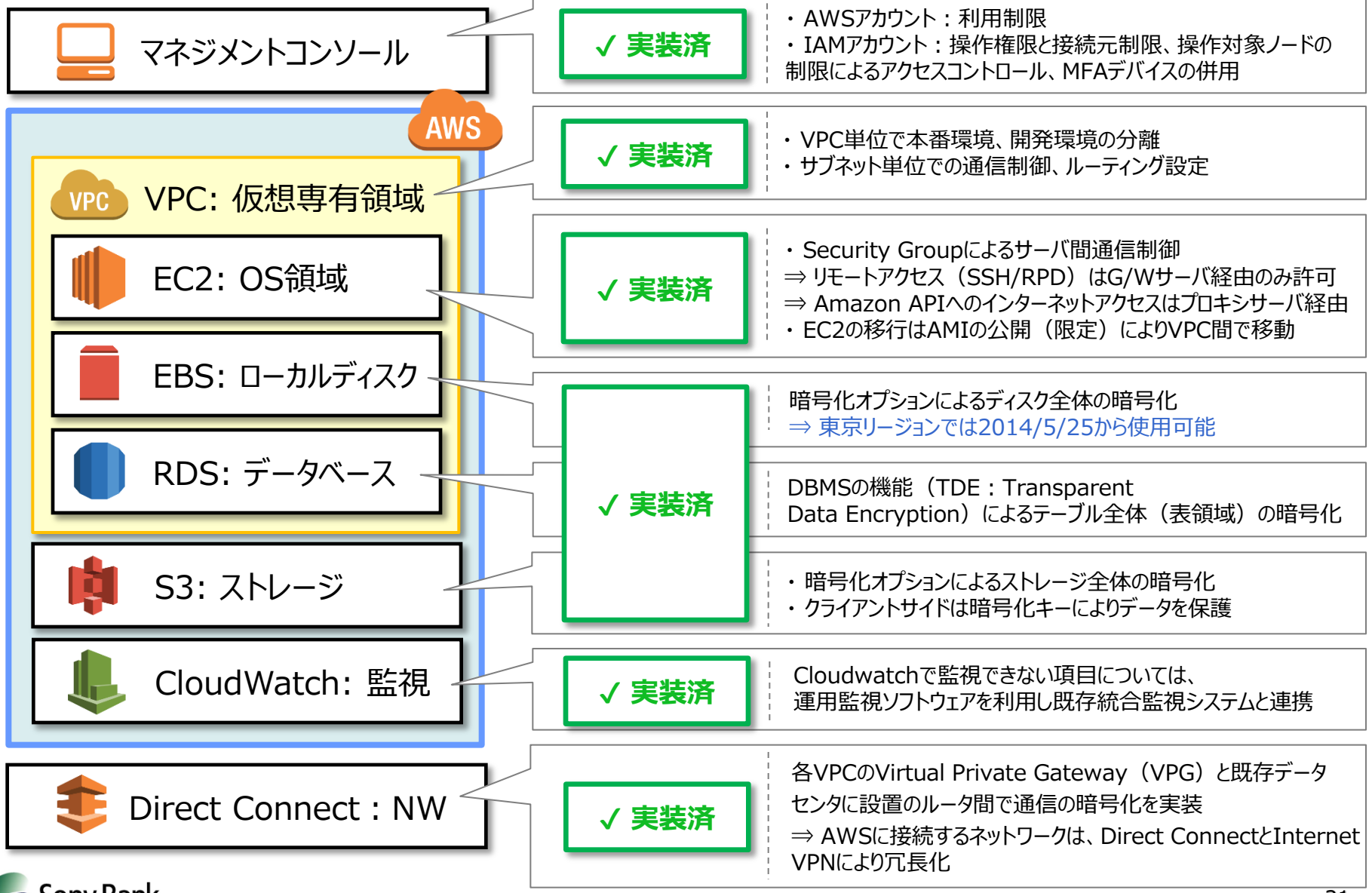
MONEYKit

AWS共通基盤および個別システムのリリース状況



MONEYKit

個別セキュリティ対応状況



Sony Bank

MONEYKit

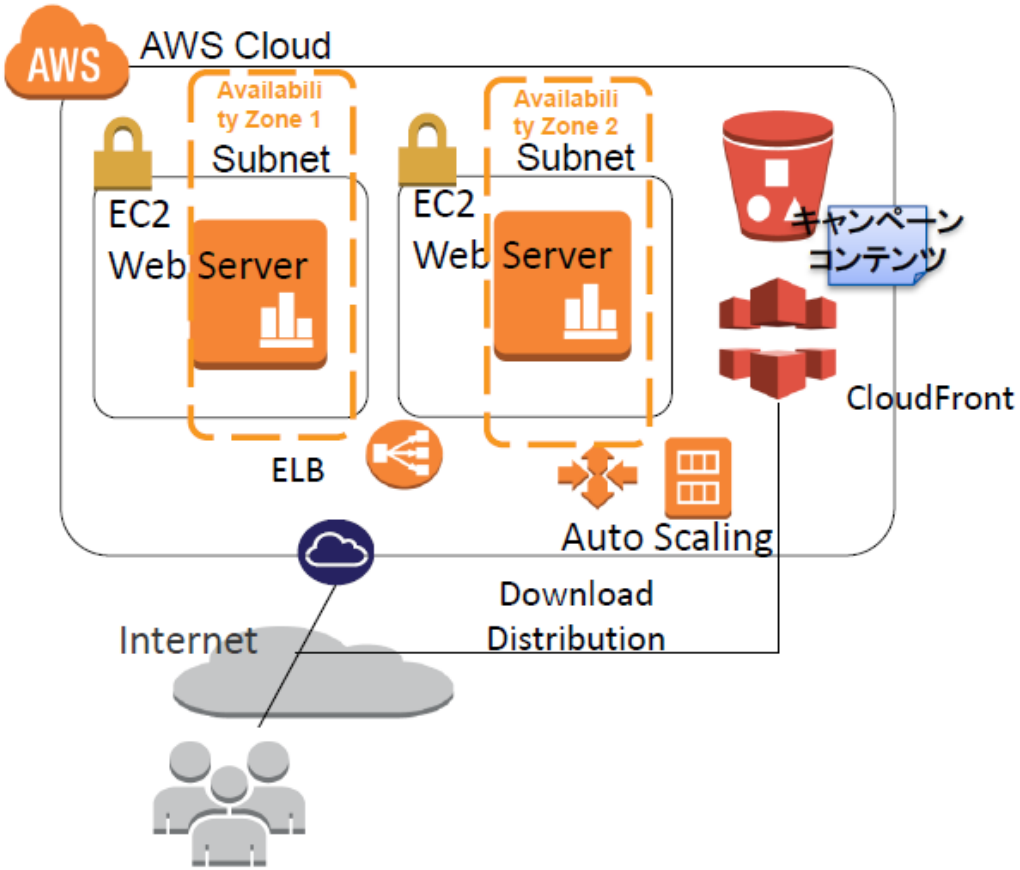
5 個別システム構成

Sony Bank

MONEYKit

【WEB系VPC】キャンペーンサイト

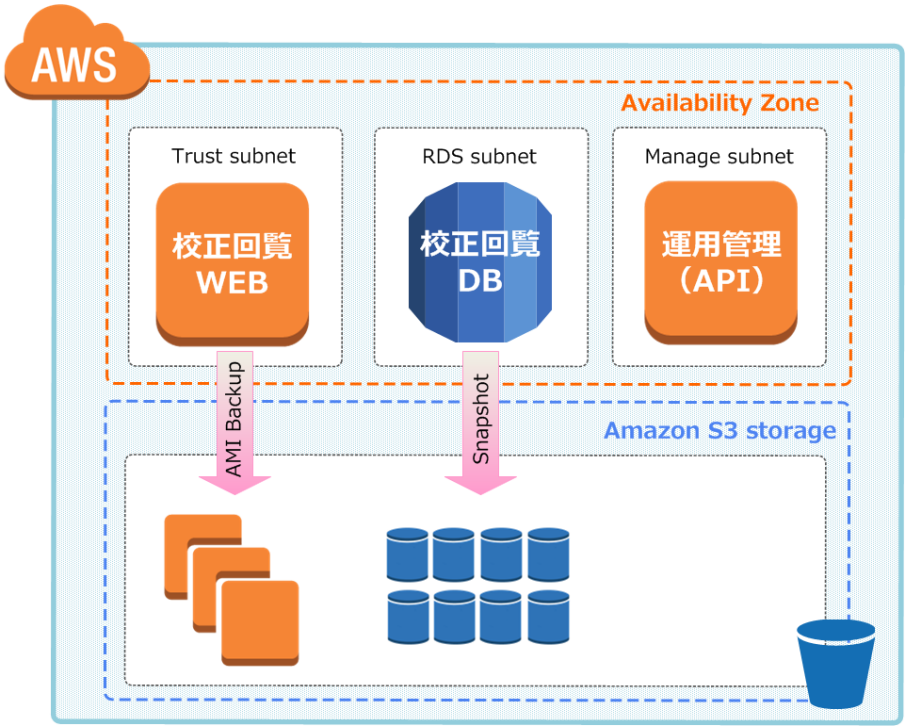
- 異なるAvailability Zoneに配置した複数台のWebサーバにAuto Scaling機能を設定
- 重いコンテンツ（壁紙）はCloudFrontに配置
- NRIにてリリース方式の設計から構築・検証まで約1週間で実施（2014年1月リリース）

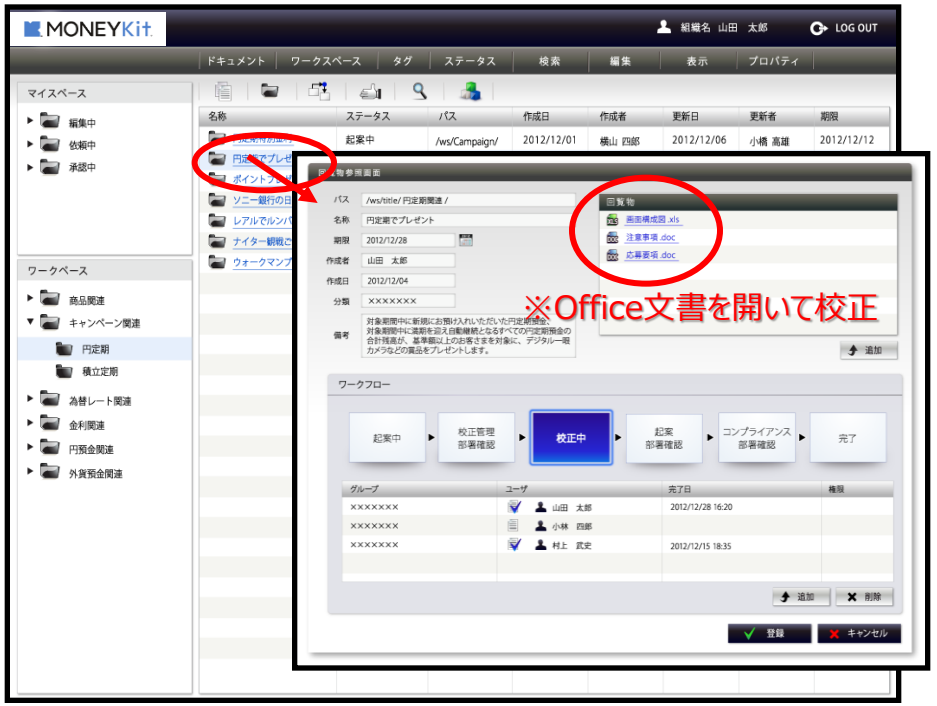


MONEYKit

【一般系VPC】文書管理ワークフロー

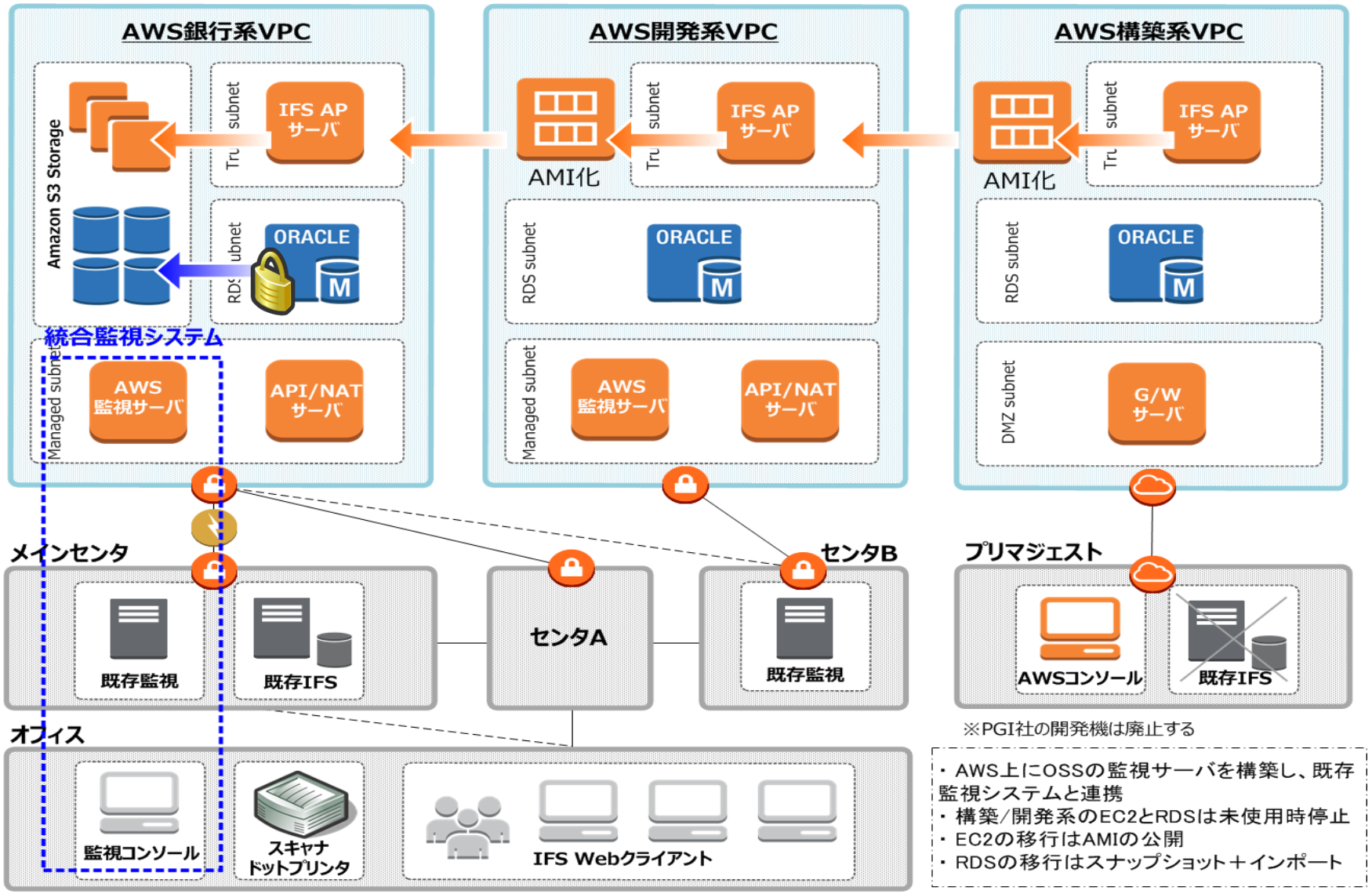
- CTC社のEIMANAGERをAWS上に構築
  ⇒ Webコンテンツのワークフローシステム（校正回覧）
- インフラの設計・実装・検証期間は約２週間（2014年4月リリース）
- 安定稼働しており、リリース後の障害発生件数は０件。性能面でも懸念なし。





MONEYKit

【銀行系VPC】ドキュメント管理システム



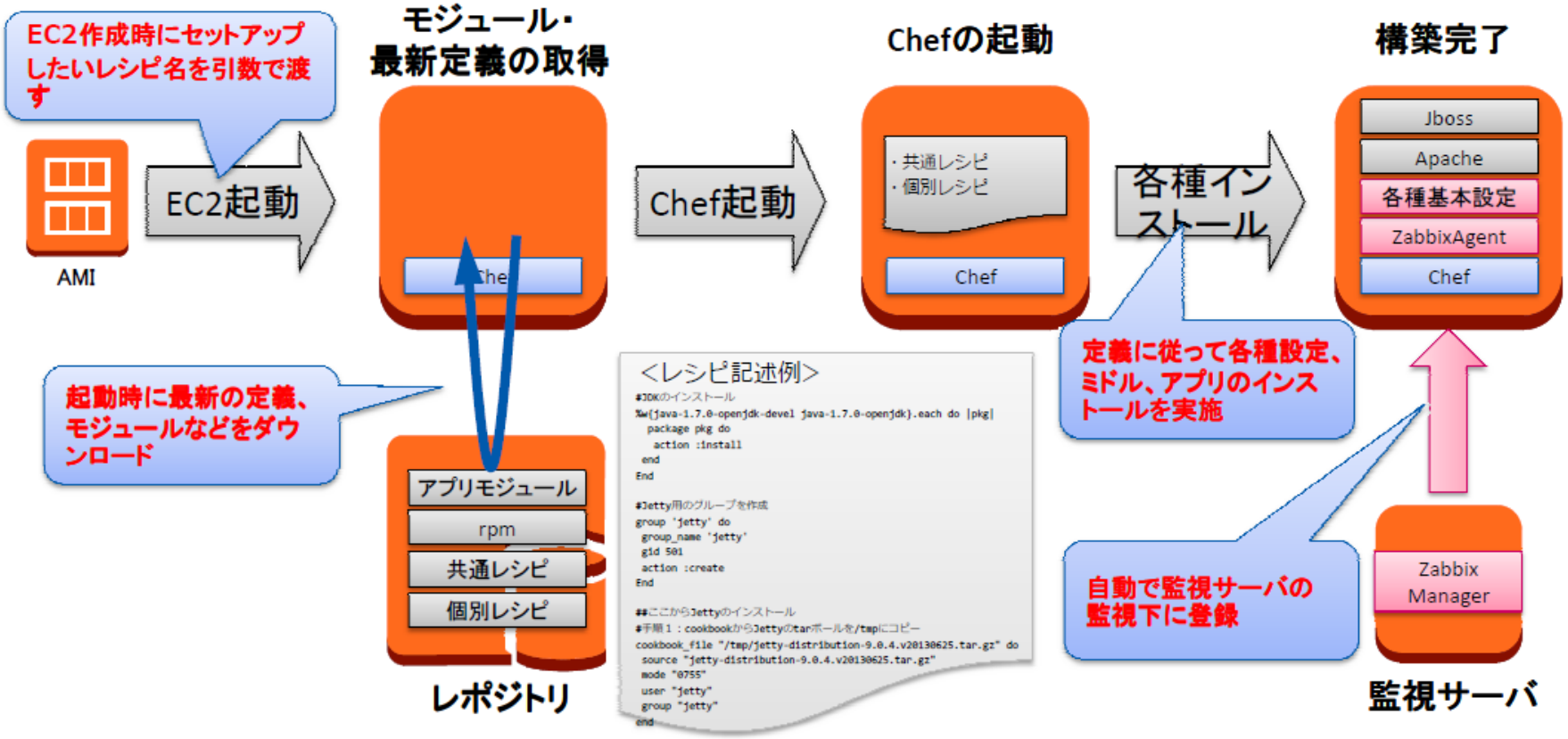
※PGI社の開発機は廃止する

- AWS上にOSSの監視サーバを構築し、既存監視システムと連携
- 構築/開発系のEC2とRDSは未使用時停止
- EC2の移行はAMIの公開
- RDSの移行はスナップショット＋インポート

MONEYKit

【評価予定】インフラ構築・管理の効率化

- ベンダや構築者に依存することなく、Zabbix監視込みの標準基盤を自動で構築
- AWS上のサーバで必要な共通設計に加え、個別設定用の定義でカスタマイズ可能
- ツール比較検討候補： Chef、Puppet、cloud-init、OpsWorks

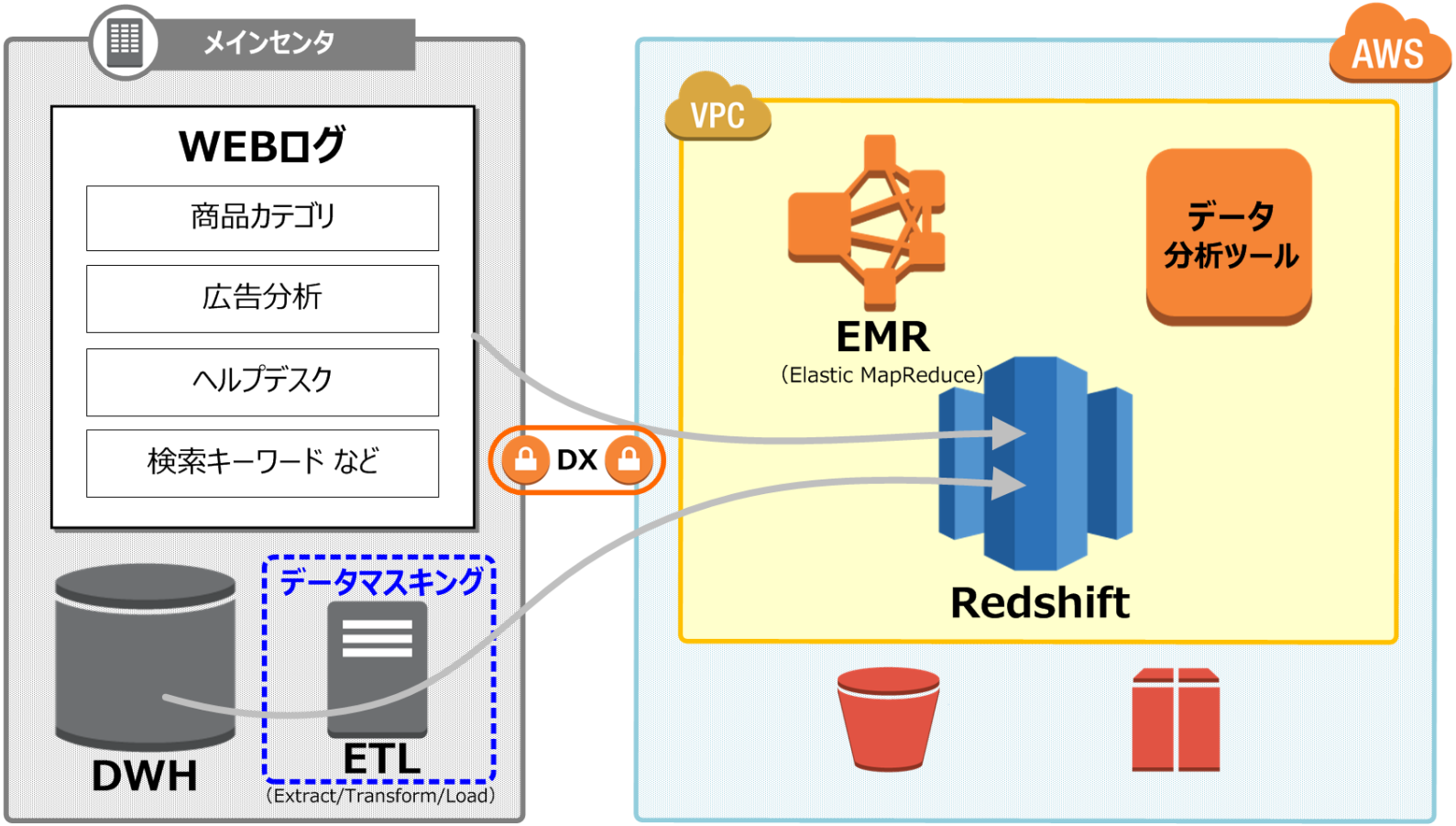


Sony Bank

MONEYKit

今後の展望

- **“お客様に最良の商品・サービスを提供”**するためのデータ分析基盤の展望
- AWSを導入することで、最先端の技術をスピーディ且つ容易に活用することが可能となる



MONEYKit

6 ＡＷＳ導入効果

Sony Bank

MONEYKit

一般社内業務システムのAWS適用評価結果

- 評価期間（NRIによる週２回の半常駐体制）： 2014/4～6（3ヶ月）
- 対象の一般社内業務システム（サーバ）

対象システム数	対象サーバ数
39システム	52台

- AWSに移行することで得られるコストメリット

自社構築総額 vs AWS総額： **約37%のコスト削減**

【前提】
・「データセンタ費用、サーバ費用、障害監視費用**（SE費用、PKG費用を除く）**」について、既存システムと同一のシステム要件に基づいてAWSに移行した場合にかかる費用の試算結果（５年総額の比較）
・ストレージは5年後想定の容量で試算しており、移行時はより小さな容量で構成することが可能であるため、さらなる費用削減の余地あり

Sony Bank

MONEYKit

AWS導入効果のまとめ

	項目	種別	AWS導入効果
1	拡張運用	運用効率化	・追加HWリソースの発注、導入の期間が不要になり、コストも極小化される。 ・EC2/RDS: HWリソース(CPU、メモリ、NIC)の拡張が必要な場合、リブート時にインスタンスタイプを変更して起動するだけで、拡張が可能。 ・EBS: 既にアタッチしてあるボリュームの拡張、追加EBSのアタッチがオンデマンドで可能。 ・S3: 最大容量は考慮する必要がなく、必要な分だけ使用できる。
2	保守期限対応・ファームウェアアップデート	運用効率化	HW保守期限や、ファームウェアのアップデートはAWS側の管理するレイヤのため考慮不要。アップデート時はリブートでインスタンスを切り替える対応のみ。
3	HW障害運用	運用効率化	EC2インスタンス、EBSの稼働に影響のないHWやハイパーバイザレイヤの障害時は、通常利用側は何もする必要がない。（事前通知の上、別サーバに載せ替えのためリブートが求められることがあるため、定期リブートをあらかじめ設定しておく）
4	テープ(メディア)運用	運用効率化	テープ(その他メディア)運用にかかるオペレータ運用の廃止
5	手作業でのアップデート運用	運用効率化	オペレータによる手作業でのアップデート運用の廃止
6	ライセンスコスト効率化	コスト効率化	筐体分離によるミドルウェアのライセンスの効率化と、時間課金によるライセンスコストの削減
7	システム非稼働時のコスト効率化	コスト効率化	システムが稼働していない、夜間・休日などの余剰リソースにかかるコストの削減
8	ピーク性のあるシステムのコスト効率化	コスト効率化	ピーク性のあるトランザクションを処理するシステムで、ピーク時に合わせたＨＷリソースの通常時の余剰リソースにかかるコストの削減
9	見込み拡張分のコスト効率化	コスト効率化	将来の需要予測を見越して購入したＨＷリソースにかかるコストの削減
10	耐障害性	業務継続性向上	AZを跨る構成をとることで、１データセンタの全面障害までに対応可能。
11	災害時業務継続性	業務継続性向上	リージョンを跨る構成をとることで、１地域をまたがる広域障害までに対応可能。
12	障害復旧時間	業務継続性向上	シングル構成サーバの復旧時間の短縮。サーバ停止に陥るHW障害が発生した場合でも、インスタンスのリブートの時間で復旧可能。

MONEYKit

7 ＡＷＳ導入予定企業様へのメッセージ

Sony Bank

MONEYKit

AWS導入予定企業様へのメッセージ

（１）AWSの特徴

■ コストメリット

・初期費用無し、完全従量制（1時間単位での課金）
・夜間などユーザが使わない時間帯はシステムを停止しておくことでコストセーブが可能
・ハードウェアの運用、管理が不要
・システム環境全体をコピー可能であるため、システム構築工数の大幅削減が可能

■ 信頼性

・ISO27001のセキュリティ基準に準拠した運用
・FISC安全対策基準の適合性を確認済み
・SLA稼働率99.95%以上（停止時間：4.5時間/年　未満）

■ 柔軟性

・キャンペーンサイトや開発環境など、必要な時に必要なだけ機器を使用することが可能
・容易にサーバリソースの追加が可能、条件設定による自動追加も可能

MONEYKit

AWS導入予定企業様へのメッセージ

（２）データセンタ

- 各リージョン内の各データセンタは一定距離隔離
- DCは自然災害を考慮した立地と構造（東日本大震災時も影響なし）
- 電源障害に対して各データセンターにはUPSおよび自家発電が設置
- **電源は供給元から２系統以上**の経路を確保
- セキュリティゲートや出入管理設備、防犯設備を備えており、**ISO 27001のセキュリティ基準に準拠したシステム運営**を実施

（３）仮想サーバ構成

- 仮想サーバは、冗長化された物理機器により構成されており、単一機器障害による影響を受けない
- **仮想サーバは冗長化が可能**であり、**複数データセンタに跨った構成**とすることも可能
- 監視サービス（Cloud Watch）と連携することにより、仮想サーバの負荷に応じて**自動でサーバを追加する機能（オートスケールアウト）**も利用可能

MONEYKit

AWS導入予定企業様へのメッセージ

（４）アクセスコントロール

- AWSを管理するアカウントはIAMを使用し、システム毎に権限を付与することが可能
- AWS管理画面へのログイン時には**トークンを用いたワンタイムパスワード**による多要素認証を行うことも可能

（５）データ管理

- 重要なデータは、**暗号化し複数のデータセンタで保管することが可能**
- リスクを考慮の上、シンガポールリージョン等のストレージにデータを配置しておく事も可能

（６）Webセキュリティ

- AWSの標準機能として、ホストベースのファイヤーウオールが実装されており、ユーザは許可するポートを個別に登録することが可能
- **IDS/IPS/WAFは、必要に応じて導入することが可能**
- 事前申請に基づき、当社で個別にセキュリティ診断を行うことも可能

MONEYKit

AWS導入予定企業様へのメッセージ

（７）先端技術の活用

- AWSに互換性のある豊富なソリューション
- 最先端の技術を取り入れたバージョンアップ、機能追加

⇒ **AWS re:Invent**

November 11 - 14, 2014 | The Venetian - Las Vegas, NV

MONEYKit

以　上

ご清聴、ありがとうございました。

Sony Bank