

オープンソース & 内製化 & クラウド移行で
情報系システムを進化させた、積水化学グループ
～AWS(アマゾンウェブサービス)を使ってみて～



積水化学工業株式会社 経営管理部 情報システムグループ 原和哉

会社概要

積水化学グループについて

SEKISUI

社名	積水化学工業株式会社 (SEKISUI CHEMICAL CO.,LTD.)
設立	1947年3月3日
資本金	1,000億円
代表者	代表取締役社長 根岸 修史
従業員数	23,017名 (2014年3月期連結ベース)
売上高	11,109億円 (2014年3月期連結ベース)
経常利益	833億円 (2014年3月期連結ベース)
本社	<u>大阪本社</u> 〒530-8565 大阪市北区西天満2丁目4番4号 06-6365-4122 <u>東京本社</u> 〒105-8450 東京都港区虎ノ門2丁目3番17号 03-5521-0521
URL	http://www.sekisui.co.jp/



大阪本社



東京本社

【 事業展開:売上構成 】



【社名の由来】

SEKISUI

【積水】の
いわれ

勝者の民を戦わしむるや
積水を千仞の谿に
決するがごときは形なり

(孫子「軍形篇第四」)



孫武

AWS移行対象システム

❖ iSmile の狙い

- 間接業務の削減・効率化 (標準化)
- ナレッジマネジメント (理念伝達・風土改革・知識開拓)
- グローバル情報共有 (単一ドメイン・Know-Who管理)

WEBメール機能強化とBCP対応 2013



AWS移行による機能強化とBCP(DR)対応
IaaS移行で生産性の無いハード更新から脱却

グローバル対応と単一ドメイン化 2008,2012



社員証システムグローバル対応や
iSmileによるインターネットダイレクトアクセス

Smile(イントラネット) 2004



グループ全体への情報発信源とし、
グループ経営の礎となる基幹システムへの入り口

Smile(メール) 2004



ビジネスに欠かせないセキュアなメールシステム
※容量拡大(ギガメール対応)で更に活用促進

Smile(グループウェア) 2005



会議室・文書管理・スケジュール等全ての
間接業務の効率化とコミュニケーションを支援

SmileNET 2005



高速・2重化・低価格なネットワークとして
国内積水グループ全社へ展開

セキュリティ(監査含む) 2005



個人情報・機密情報保護を推進
ウイルスゼロへ!

(電子)社員証情報 (約23,000人)

❖ 積水化学グループ全員が使うイントラ基盤

カンパニー別にページを用意

個人別情報は MyInfoへ集約

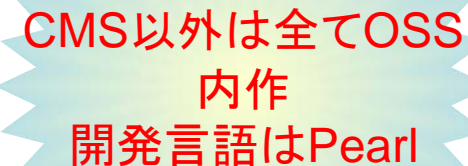
全社情報はメインに配置

リンクと検索は集中配置



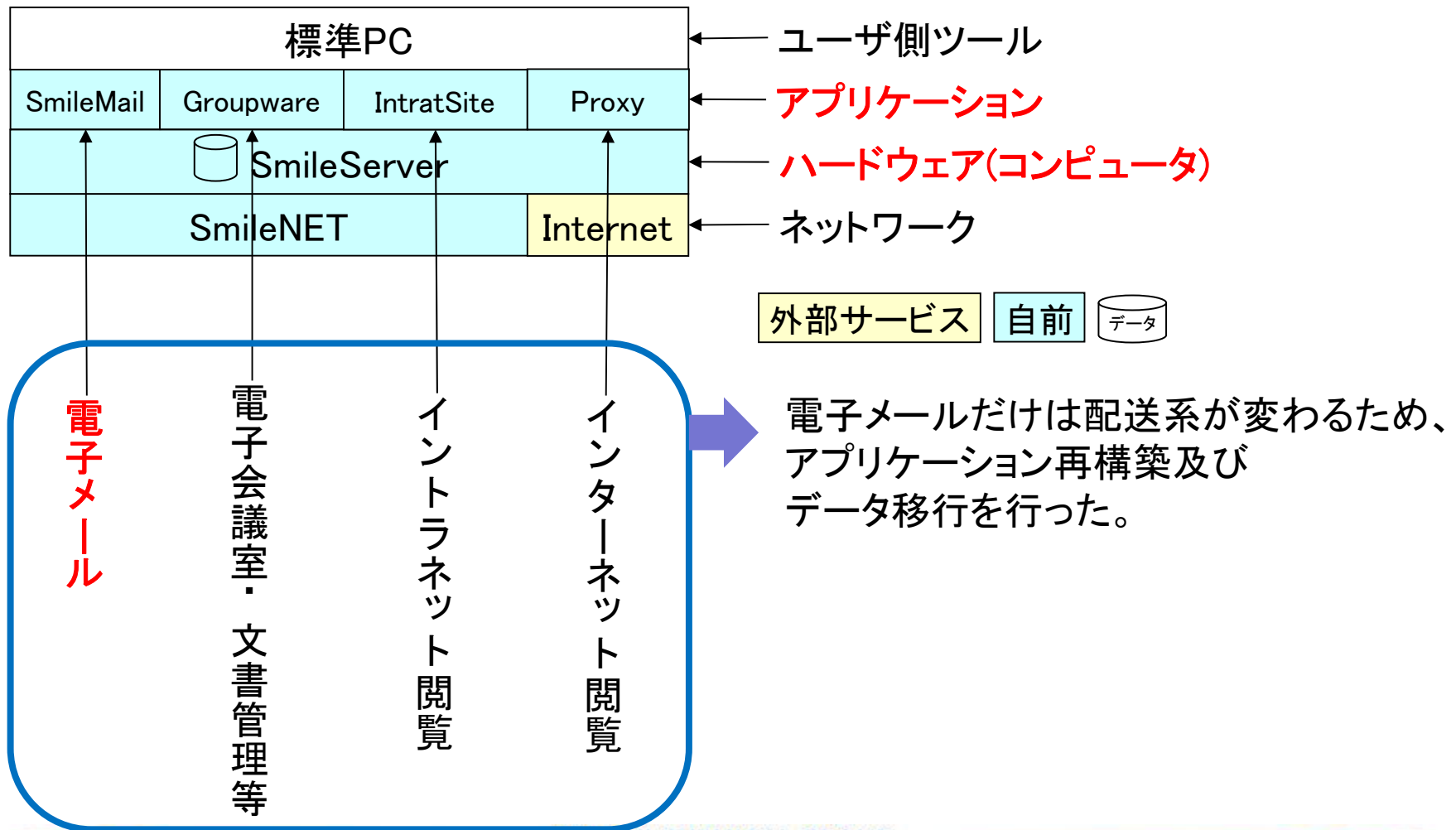
対象システム(Smile)の主な機能

- ❖ **ポータルサイト**
- ❖ **電子メール**
- ❖ スケジュール(自分・他のSmileユーザのスケジュール)
- ❖ コンテンツブラウズ・購読リスト(コンテンツを探す・購読する)
- ❖ **掲示板・会議室**(連絡・案内・ディスカッション)
- ❖ 施設予約(会議室・設備 利用予約)
- ❖ 行事予定(会社・部所・グループ単位のスケジュール)
- ❖ **文書管理**(ファイル管理・共有)
- ❖ マイフォルダ(個人用ファイルスペース)
- ❖ ブックマーク(Smileオンラインブックマーク)
- ❖ TODOリスト(作業管理)
- ❖ 来客対応(来客スケジュール)
- ❖ SmileWEB会議(オンラインWEB会議)
- ❖ 確認依頼(記事・文書の確認依頼)
- ❖ 権限グループ(利用ユーザグループ設定)
- ❖ 携帯版Smile(スケジュール・施設予約・メール転送設定ON/OFF)
- ❖ 回覧



CMS以外は全てOSS
内作
開発言語はPerl

❖ 下記Smileの構成のハードウェア及びアプリケーションが対象



外部サービス 自前 データ

電子メールだけは配送系が変わるため、アプリケーション再構築及びデータ移行を行った。

利用中のグループウェア **iSmile** はLinuxServerで動作するOSS自社開発品

iSmile の課題

- ✖ メールストレージの保守期限が来て、ハード更新する必要がある
- ✖ メールボックスの容量が乏しく(100MB)容量増加への要望が強い
- ✖ 約100台のグループウェアサーバ群を毎年数十台ずつ更新するのが大変

追加要求

- ✖ コンプライアンス経営の一環として、電子メール保存機能を追加したい
- ✖ BCP対応(遠隔2重化相当)が必要
- ✖ 社業のグローバル化に伴い、情報共有基盤はグローバルで統一したい

オンプレミス・SaaS・IaaSの3案を検討

比較対象と選定基準

	現状	全面更新	SaaS	IaaS【AWS】
コスト	◎	×	×	○
BCP対応	×	○	○	○
アーカイブ	×	○	○	○
ユーザ操作	○	○	×	○
メール容量	×	△	◎	○
総合評価	×	×	×	○

評価項目解説

❖ コスト

- 5年間のTCOで計算
- システム運用費用(人件費)も算入
- 更新案は5年後のハード更新費用も算入

❖ BCP対応

- システムを異なる場所で2重化する前提

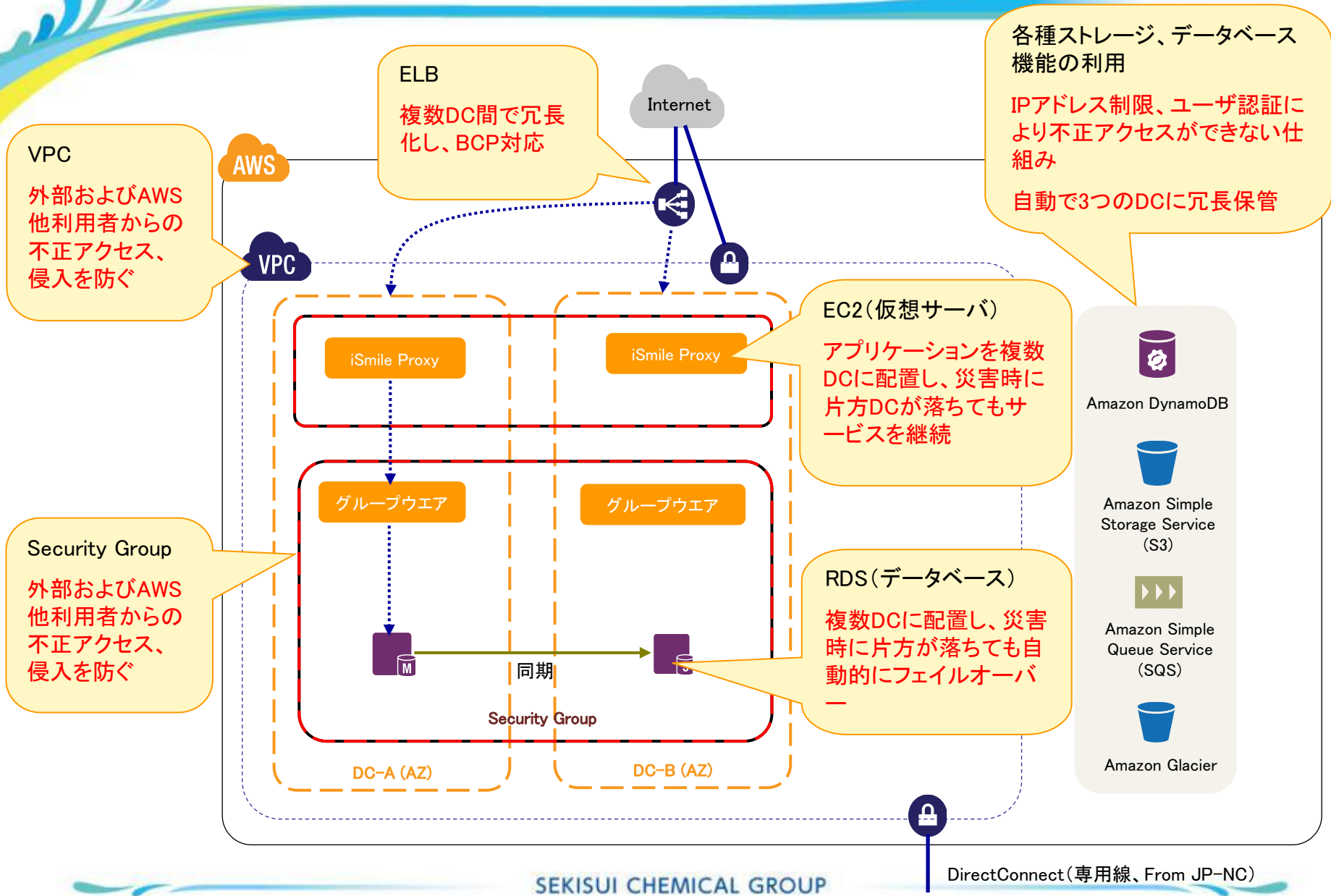
❖ アーカイブ

- 社外送信メールのみを長期保存する

❖ ユーザ操作

- 現状の操作からの変化度合いで、混乱を招かないことを重要視する

セキュリティ対策の説明(社内解説用)



- ❖ セキュリティを支えるのは仕組みではなく、最後は人です。
- ❖ 最も大きなセキュリティリスクは内部犯行です。



普段は評価されず、
何かあると責任を問われる
過重労働のIT運用部門



どっちが良いですか？



契約に従って定時退社する
利害関係のない
クラウドベンダーの運用部門

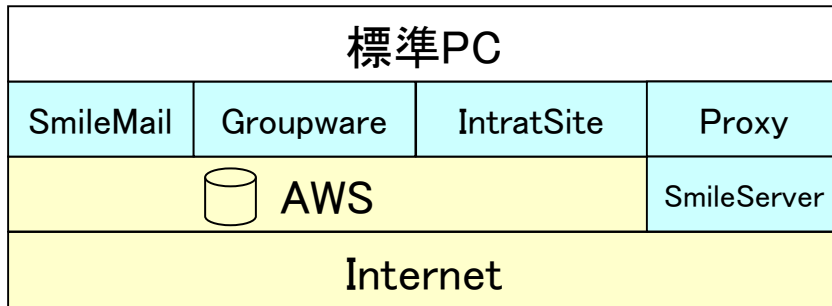
しっかりと契約交渉を行えば、
クラウドの方がセキュリティリスクが少ないと言えるのでは？

- ❖ AWSサービス条件
 - AWSのサービス内容を規定している
- ❖ AWS 適正利用規約 アマゾン ウェブ サービス(AWS)
 - 違法、有害、コンテンツの禁止など利用者が不正利用することを禁止して
- ❖ AWSカスタマーアグリーメント アマゾン ウェブ サービス(AWS)
 - 2.1 提供される本サービス内容の変更 アマゾンは、随時、(提供される本サービス内容全体を含めて)提供される本サービス内容のいずれの部分についても変更、中止、廃止し、あるいは提供される本サービス内容の属性もしくは機能を変更または削除することができるものとする。提供される本サービス内容の重要な変更または中止を行う場合には、アマゾンは、サービス利用者に対して通知する。
 - 2.2 API の変更 アマゾンは、随時、本サービスのAPIを変更、中止または廃止することができるものとするが、**変更、中止または廃止から12ヶ月間は、変更、中止または廃止されたAPIの以前のバージョンのサポートを継続するため商業上合理的な努力をする。**ただし、それにより、(a)セキュリティもしくは知的財産の問題が生じる場合、(b)経済的もしくは技術的に負担が大きい場合、または(c)法律もしくは政府機関の要請を遵守する必要がある場合を除く。

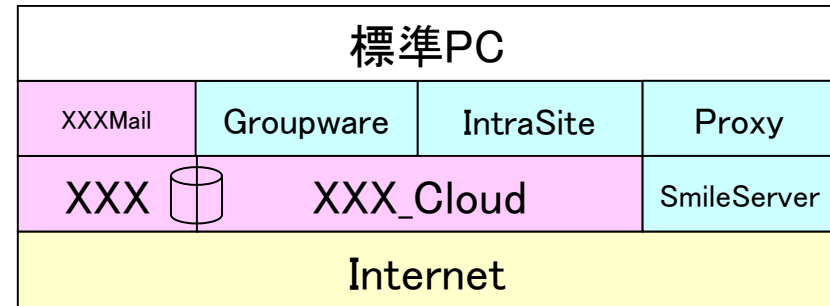
この部分で、最悪の事態に備え代替えサービス(次ページ)を設計しておく

❖ Amazon社が無くなったり、AWSのサービスが中止された場合の代替え案を検討した

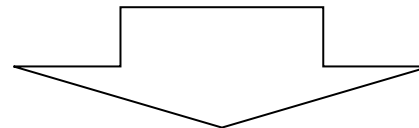
❖ AmazonWebService



❖ 代替え案の構成(赤色)



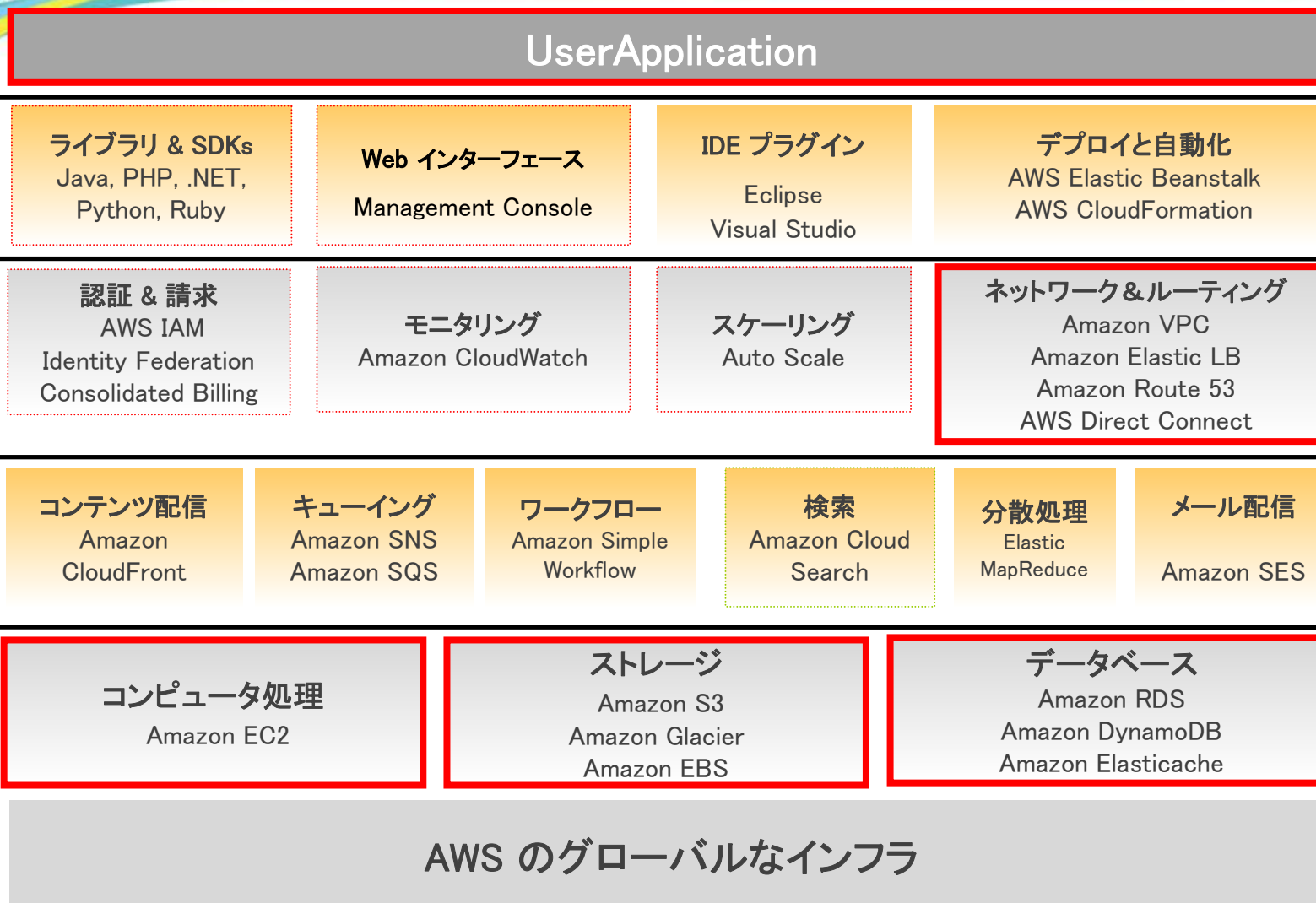
❖ 本来は、AWSと類似のXXX_Cloudのみの構成としたいが、メールシステムが技術的にNGのため(後述)、メール部分のみ別のサービスを適用




メールシステムは、海外でよく利用されているXXX社のXXXを検討する

AWS上の構成

利用しているAWSのサービス



構成一覽

システム、サービス名	AWSサービス	利用開始日	利用パッケージ OSS	システム規模 備考
グループウェア 	EC2 x111 EBS 11TB S3 4TB DynamoDB RW各 5000unit RDS×6 SQS ElasticCache×6 Glacier ?TB Route53 ELB DirectConnect PVC	2013/9~	OSS(Pearl) MySQL PostgreSQL Spamassassin Postfix Apache OpenLDAP Hobbit MRTG :	利用ユーザ数 20,000名 Mailbox 2GB
AWS管理 Sheltie	EC2 x12 RDS 40GB ELB	2013/10~	MySQL :	AWSコンソール代 替

Smile(電子メール)の機能改善例

- ❖ メールボックスサイズの**20倍化** 100MB→2GB
- ❖ **アーカイブ機能**誘導の「整理」ボタンの追加

The screenshot displays the Smile Webmail interface. At the top, there are navigation links for 'グループ電話帳', 'ホーム', and 'ヘルプ', along with a status bar showing '0.1MB / 100.0MB (0.1%) 使用中'. Below this, the 'Webmail' section includes options for '受信箱', 'メール作成', 'アドレス帳', and 'オプション設定'. The main area shows a list of folders on the left and a list of emails in the inbox. A red box highlights the '整理する' button in the email list toolbar. Another red box highlights the 'アーカイブフォルダ' section in the left sidebar, which contains a folder for '2013' with 1871 items. The email list shows various messages with details like sender, date, and size.

件名	差出人	日時	サイズ
■iOS 7にKindleFire...「脱獄」社員も逃	キーマンズネット編集部 <new	今日 11:00	19.3KB
シャープ メビスタタブレットご紹介お	nakamura-takeshi@sharpc	今日 10:50	2.6MB
[MPMC] アラート: 経営管理部 C 情	smile-norophy@sekisui.jp	今日 10:33	3.2KB
これまでの限界を超え、不可能を可能に	富士通 BizNews事務局 <cont	今日 08:05	28.1KB
「原発のごみ」封印実験 来夏にも北海	日経ニューズメール <nikkei-r	今日 07:45	9.3KB
【公認会計士が語る】消費税改正時の備	新着セミナー キーマンズネット	今日 07:33	12.7KB
【仮想ネットワークで進化】クラウドサ	キーマンズネット <news-key	今日 07:21	17.4KB
すり合わせ能力は弱みに変わる/環境指標	Tech-On! 通信 <techon-m	今日 07:03	23.4KB
[NEC] いよいよ明日(11/14)より開	NEC Business Solution New	今日 06:58	22.4KB
[PCO] 楽天が二重価格問題で対策/ト	PC Online <npc@nikkeibp	今日 06:16	19.4KB

經驗

❖ オンプレミスからの移行で、AWSのサービス起因かアプリケーション起因か分からない不具合が発生

➤ AWS側はサポートで解決

- ・ トラブルシューティング時の即時性を求めるなら BusinessLevelが必須
DeveloperLevelでは埒が明かない
 - BusinessLevelは従量課金なので、ReservedInstanceを利用する場合は、初月に大量課金が発生→逃れる術はない

➤ アプリケーション側は・・・

- ・ オンプレで発覚しなかった設計レベルのバグが多発
 - AWSの Performanceは実際に使ってみないとわからない
 - エンジニアの瞬発力が必須
 - » AWSで実装して、Performanceを計測し、勘で修正

❖ 請求は



- コーポレートカードが使えるれば問題ないが、毎月Invoice+海外送金は面倒

❖ 為替差で予算が狂う

- AWS移行企画時→1\$=80円
 - ・ 為替変動を予測して、1\$=100円で稟議提出
- AWS移行完了時→1\$=105円
 - ・ 想定以上に円安だが、AWS値下げにより企画時の数値はクリア
- 今後→1\$=???円
 - ・ 固定資産が経費化したが、経費予算の組み方が難しい

Amazonさんの値下げビジネスモデルに期待しつつ、¥での取り扱いもお願いします。

❖ ReservedInstance購入は要注意

1. ReservedInstance購入時のサポート料

- ・ BusinessLevelにするなら、途中でサポートレベル変更しても年契約と同じ料金が発生

2. InstanceTypeはReservedの中でのみ変更可能

- ・ 性能の違うサービスは別途Reservedの契約が必要(オンデマンド利用なら問題ないが、価格が違う)
- ・ AWSの性能はスペック通りとは限らない
 - 以外とリソースを使用しないアプリや想定以上にリソースを食うアプリが存在するので、Reservedにするタイミングが重要

3. Reservedの契約をバラバラに行うと、前払い費用発生タイミングもバラバラになり、経費管理が大変

- ・ 可能であれば、1回/年にまとめる
→AmazonでEnterprise向けに期間調整してくれる可能性もある「打診中」

❖ メールシステムならではのポイント

- DynamoDB(I/Oギャランティ型高速DB)をメールシステムで採用
- ・ MailboxのPerformance維持のため
- ・ DynamoDBのスループットが性能限界となる



DynamoDBの限界をシステムの性能限界に設定すると、過負荷状態でメールシステムダウン+関連システムも全滅する



DynamoDBの処理状況を監視し、不急の処理はサブルーチンに任せるような工夫を実施し対応

実はこのDynamoDBが他のIaaSにないサービスだったので代替案が...

❖ その他もろもろ

- AWS移行後のシステムはIE8とFirefoxを環境指定
 - ・ IE6撲滅運動での戯言(現在はWindows7移行が完了している)
「俺は既にIE8なのになぜ警告される？」
「IEって何？バージョンって何？」
「クロムは駄目なの？」
：
- メールサーバをIP指定している埋め込みシステム対策
 - ・ 旧型複合機のメール機能
 - ・ 子会社個別システム(めっちゃ古い)のメール連動
 - ・ 社内にある外部システム(郵便・印刷・・・)
- 組織ID(メーリングリスト)管理不足
 - ・ 転送ループや宛先不明など

クラウドデータセンタ

オンプレミスDC(西日本DC、東日本DC)とクラウドDCにおいて、IS基盤プラットフォームをそれぞれ提供する。

1

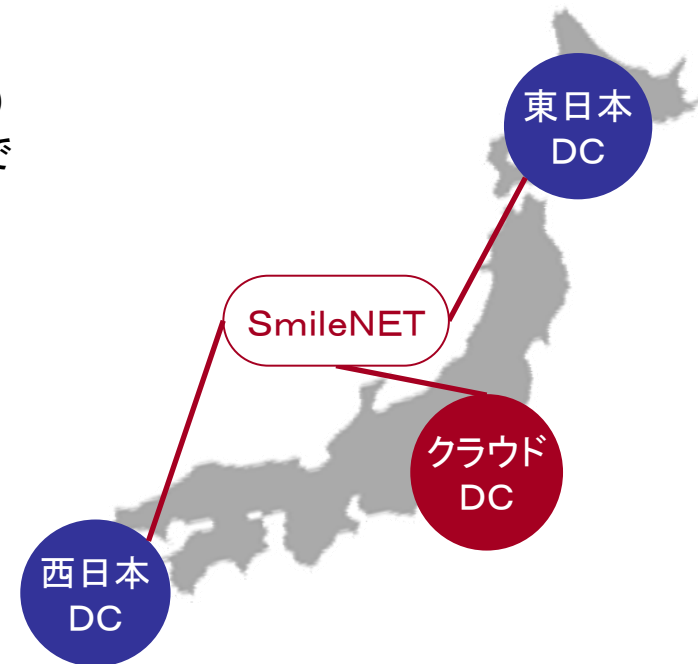
オンプレミスDC

- ・AS/400、AIXは統合基幹サーバ(Powerプロセッサ)でLPARにより、Windowsは統合WindowsサーバでHyper-Vにより仮想サーバを提供する。
- ・統合ストレージの指定の領域に保存されたデータは、災対DC(東日本DC)に自動的に遠隔地保管される。

2

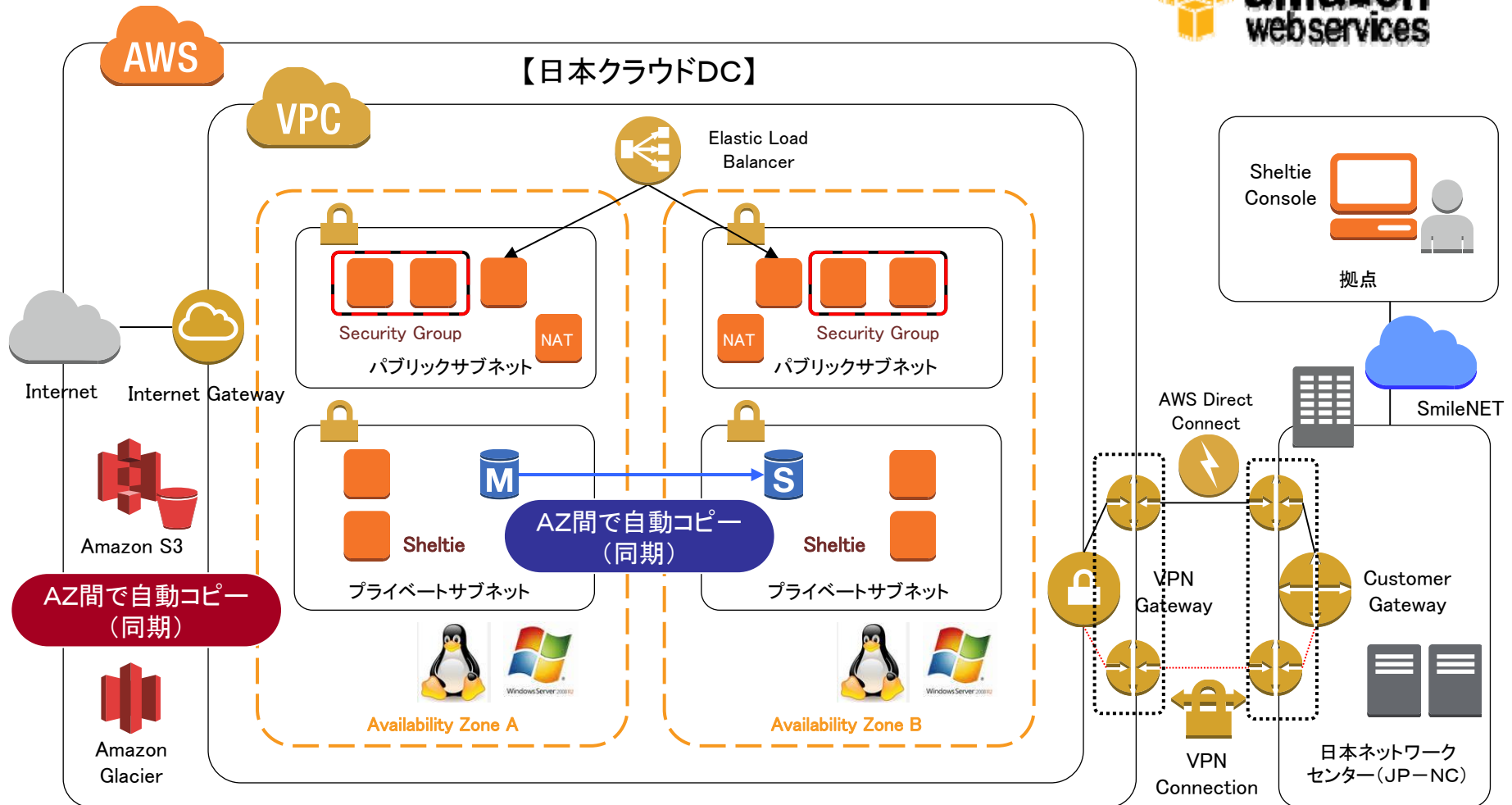
クラウドDC

- ・クラウドDC(AWS VPC)において、AMIを用いてEC2インスタンスを構築する。
- ・システムオーナーはインスタンス及び各種サービスの管理を標準管理システム(Sheltie)経由で行う。



クラウドデータセンタとしてみたAWS

クラウドDC



Sheltieの意味

- 概要

Amazon Web Serviceの管理者機能を担当者ごとに制限

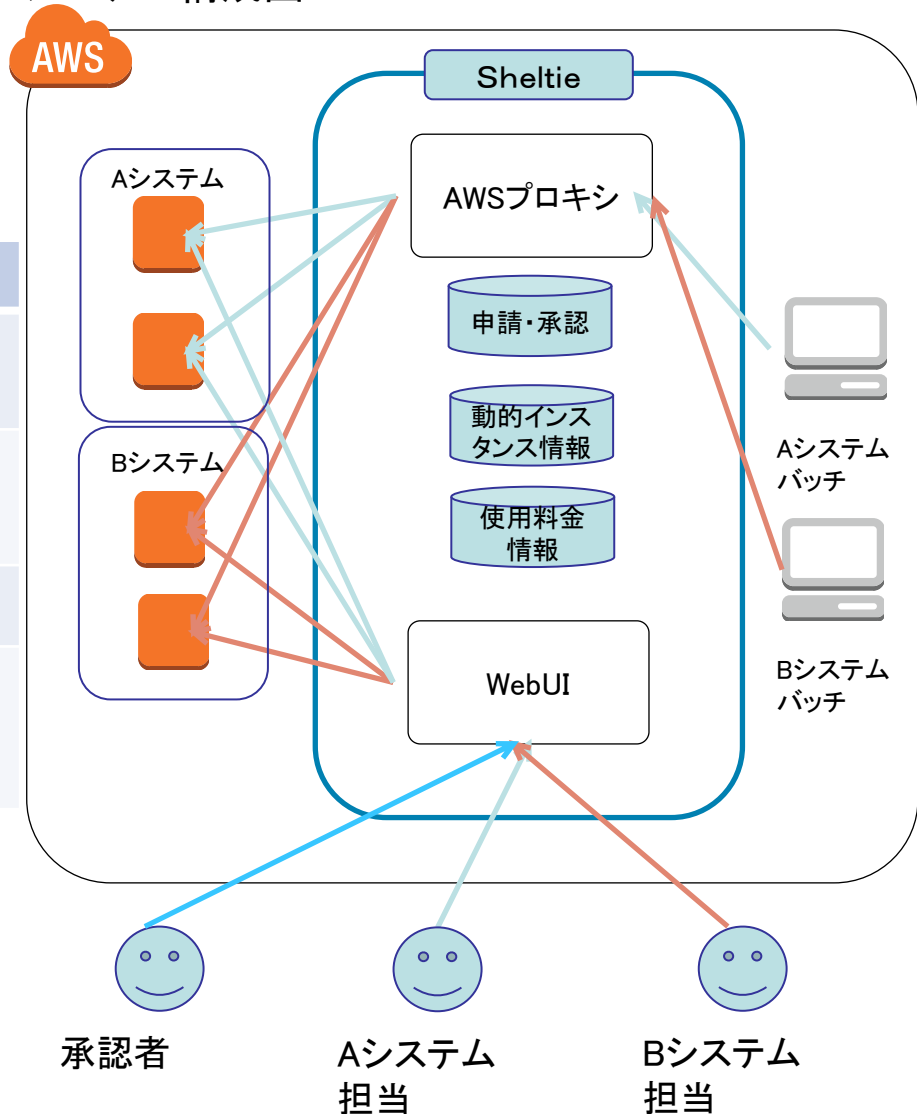
- AWS問題点

オブジェクト作成・削除が自由にできる

問題点	解決方法
想定外の使用料	申請・承認した範囲に制限 使用料金情報の収集
操作ミスが重大事故	操作できる範囲を担当者ごとに制限
動的情報が不明	インスタンス情報の提供
不正使用リスク	AWSサービスの利用権限チェック 不正インスタンスの起動チェック 操作ログ

AWS操作を制限するフィルター機能が必要
Sheltie でフィルター機能を実現

● システム構成図



SLAで24/365稼働サービスについては冗長構成とする。冗長構成とする場合、以下の方針とする

1. AWSサービスを利用できるものはサービスを利用する
2. HTTP/HTTPSサービスについてはELBを利用する
3. ミドルウェア・ツールに可用性確保のための仕組みがある場合はその仕組みを利用する
4. DNSラウンドロビンが利用可能なサービスはDNSラウンドロビンを利用する
5. DNSラウンドロビンに対応していないクライアントの場合は、DNSレコードの変更やEIPのマッピング変更で対応する
6. 上記で対応できない場合はheartbeatを利用する

実際の対応は以下の通り

可用性方針対象	Smile on AWSで使用する機能を対象
1.AWSサービス利用	ストレージ(S3)、RDS、DynamoDB、SQS→AWSのSLAに依存 (AWSのSLAや提供仕様から、オンプレSmile以上の可用性を有していると判断)
2.ELB利用	グループウェア、Webメール、iSmileプロキシなどのHTTPサーバ
3.ミドルウェア・ツールの可用性確保の仕組み	ログ管理(Fluentd)
4.DNSラウンドロビン	LDAP、POP/POPS、SMTP/SMTPS
6.heartbeat利用	無し

バックアップ対象と保存期間

バックアップ対象、方法、保存期間は以下を標準とした

対象	バックアップ方法	取得間隔	保存期間	リカバリポイント
RDS(DB)	自動バックアップ	-(※)	2日	5分前の状態まで戻る
	テキストダンプ	日次	long-period	ダンプ取得時の状態まで戻る
アプリデータ (EBSに持つもの)	EBSスナップショット	日次	2日	EBSスナップショット取得時の状態まで戻る
ログ	S3(FluentdによりS3へ保管)	日次	mid-period	S3保管時の状態まで戻る
個別ファイル	S3	個別	long/mid/short個別判断	S3保管時の状態まで戻る

※RDSの自動バックアップにより1日1回RDSスナップショットが実行され、スナップショット実行時からのトランザクションログが自動的にバックアップされる。

スナップショットとトランザクションログを組み合わせることにより5分前の状態までリカバリすることができる。

まとめ

1. ハードウェア台数が多いなら、更新作業が超効率化

- 生産性ゼロの更新Projectを無くすことができる
- 貴重なエンジニアは、アプリケーションの開発・保守・運用に特化する

2. CRは期待しない

- 資産が経費化するため予算管理には注意
 - ・ 元々リースなら同じようなもの
- サイジングを工夫(チューニング)すれば多少のCRは期待できる
 - ・ ReservedInstance利用はCRの必須条件
 - ・ サイズ変動の大きいシステムならかなりのCRは期待が期待できる

3. お試しシステムは超便利

- 期間限定システムや、開発のお試しなどオンデマンドでリソースが必要な場合は、一切のハードウェア投資がないので便利

- ❖ エンジニア(関係会社)のモチベーションが上がった
 - 最先端のサービスを提供するAmazonの技術を直接利用できる
Wakuwaku感と、難解なパズルを解くように作り上げたアプリケーションに対するSatisfaction

OSSを活用してアプリケーションを内製化し、AWS上で動かす時の最大**勝因**

- ❖ IaaS(AWS)の利用による次の戦略が見えてきた
 - IaaSはオンプレデータセンターと同じ
 - ・ Server(Instance)運用、監視システム構築など、通常のデータセンターと同じことをやる必要があるが、ここを乗り越れば、BCP対応やScaleOutが簡単にできるクラウドデータセンターとなる

Enterpriseに於ける**次世代**のインフラ戦略に、AWSは絶好のサービス



Enterprise
JAWS-UG
AWS User Group - Japan

- ❖ Enterprise-Japan AWS User Group
 - コミッティーメンバー 原 和哉
 - ・ aws-jp-entug@amazon.com