TIS
TIS INTEC Group
Go Beyond

金融業界でも使える！
AWS利用におけるガバナンスの効かせ方

TIS株式会社
プラットフォームサービス本部
プラットフォームサービス事業部
プラットフォームサービス第2部

Copyright © 2017 TIS Inc. All rights reserved.

登壇者プロフィール

- 久保智成
  - TIS株式会社所属
  - AWSを用いた設計全般
  - AWSパートナーアワード受賞エンジニア(2012/ビッグデータ部門)
  - AWSアライアンス関連
- エンタープライズ/金融担当
  - エンジニアとしてシステムの開発
  - 運用設計も実施
- 執筆等
  - 雑誌、Web媒体

AWS・Azure導入の先端技術情報
日経クラウドファースト
Nikkei Cloud First

Copyright © 2017 TIS Inc. All rights reserved.

お話すること

- 金融業界動向と背景
- クラウド利用プラクティス(CAFとCCoE)
- 問題と対応
- さらに行っていくこと

Copyright © 2017 TIS Inc. All rights reserved.

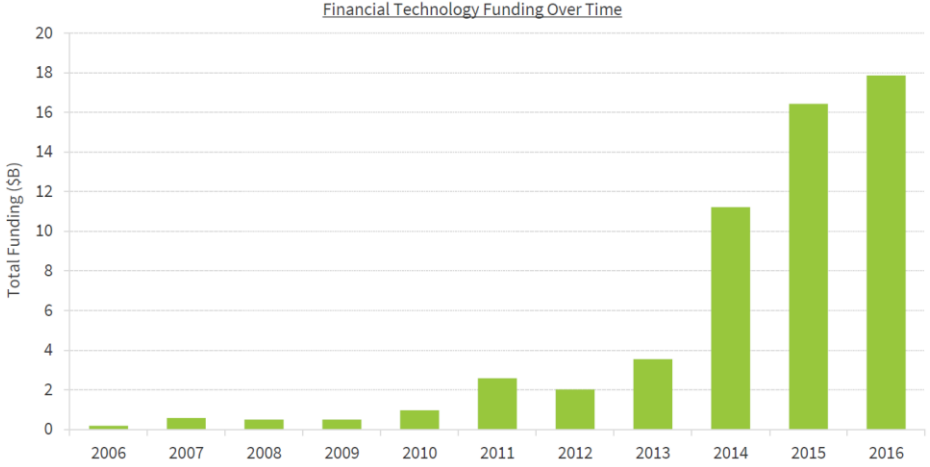
TIS
TIS INTEC Group | Go Beyond

Fintech

Fintech startups are creating new businesses and disrupting old ones

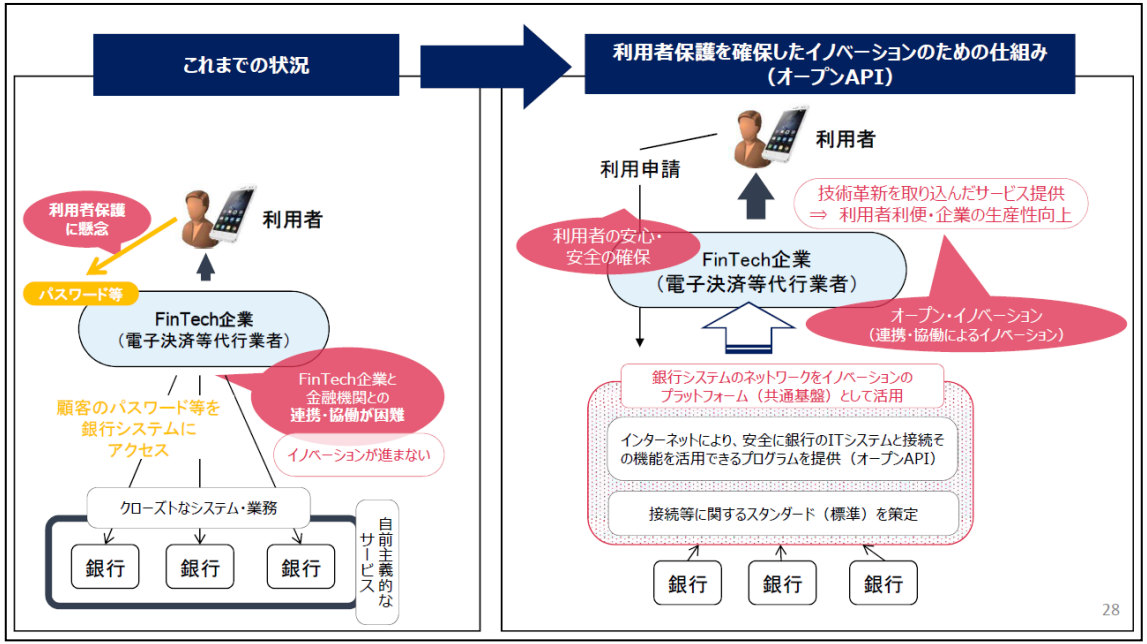
VC funding into fintech has grown substantially in recent years

Overall ***fintech VC funding grew at a CAGR of 47%*** from 2011-2016



出典：Venture Scanner Fintech Report Q1 2017
https://www.slideshare.net/NathanPacer/venture-scanner-fintech-report-q1-2017

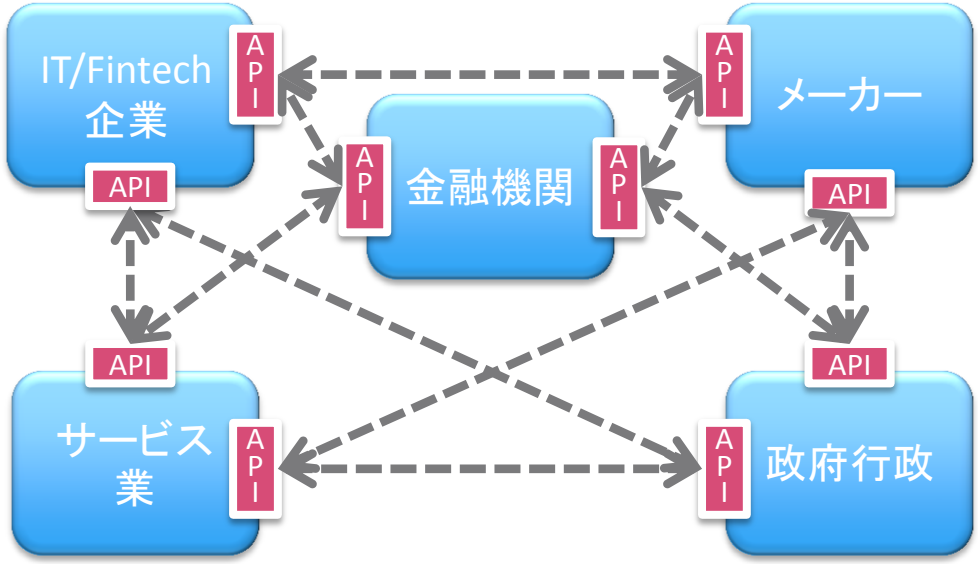
金融庁の動き



- 頻繁な検討会
- 法整備に向けた動き
- 金融機関に対しAPI公開の提言
- セキュリティ検討

出典：フィンテックに関する現状と 金融庁における取組み（金融庁）
http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai4/siryou1.pdf

金融API



- メガバンク様も昨年～本年にかけてAPI公開
- 現在は契約のある法人間での公開範囲
- 一般公開に向けて検討・課題の整理

Copyright © 2017 TIS Inc. All rights reserved.

経済産業省
Ministry of Economy, Trade and Industry

› 本文へ › よくあるご質問 › サイトマップ

文字サイズ変更 小 中 大 アクセシビリティ閲覧支援ツール

サイト内検索 検索 › 拡張検索

ホーム | 経済産業省について | お知らせ | 政策について | 統計 | 申請・お問合せ | English

TIS
TIS INTEC Group
Go Beyond

▸ お知らせ ▸ ニュースリリース ▸ 2017年度一覧 ▸ FinTech（フィンテック）に関する初めての総合的な報告・提言「FinTechビジョン」を取りまとめました

› English 印刷

お知らせ

FinTech（フィンテック）に関する初めての総合的な報告・提言「FinTechビジョン」を取りまとめました

本件の概要

経済産業省は、2016
トや課題、今後の政策
意見等も踏まえ、今

1. 背景

近年「FinTech」と呼
スを提供する動きが世

2. 「FinTechビジョン」の概要

「FinTechビジョン」は3つの章で構成されています。
第1章では、FinTechは何を変えるのか、何がその変化の原動力になっているのかなど、世界中が「FinTech」という言葉で捉えようとしている動きを概観しています。
第2章では、FinTechが我が国の経済・社会にもたらす効果を金融サービスのユーザーたる個人（家計）や企業の目線から考察し、「目指すべきFinTech社会の姿」を示しています。
第3章では、第2章で示した「目指すべきFinTech社会の姿」を実現するための課題と政策対応を提言しています。
併せて、FinTechによって日々の生活がどう変わるのかのイメージを示した、「フィンテックがある1日～お金が変わる。社会が変わる。～」ムービーを公開しました。

FinTechな生活　～お金が変わる。社会が変わる。～

- 経産省も頻繁な検討会
- クラウド関連のガイドラインも公開
(以前から)

Copyright

出典：経産省 FinTechビジョン http://www.meti.go.jp/press/2017/05/20170508001/20170508001.html

- TISも銀行口座のアプリケーションと基盤の構築
- 金融業界だけの話ではない
- ベンダー側が金融領域へ

TIS
TIS INTEC Group

サイトマップ　採用情報　お問い合わせ

ニュース　セミナー　サービス／ソリューション　導入事例　特集・レポート　会社情報

HOME ＞ ニュース ＞ TIS、三菱東京ＵＦＪ銀行のスマートフォンアプリ『My Money』の構築を支援

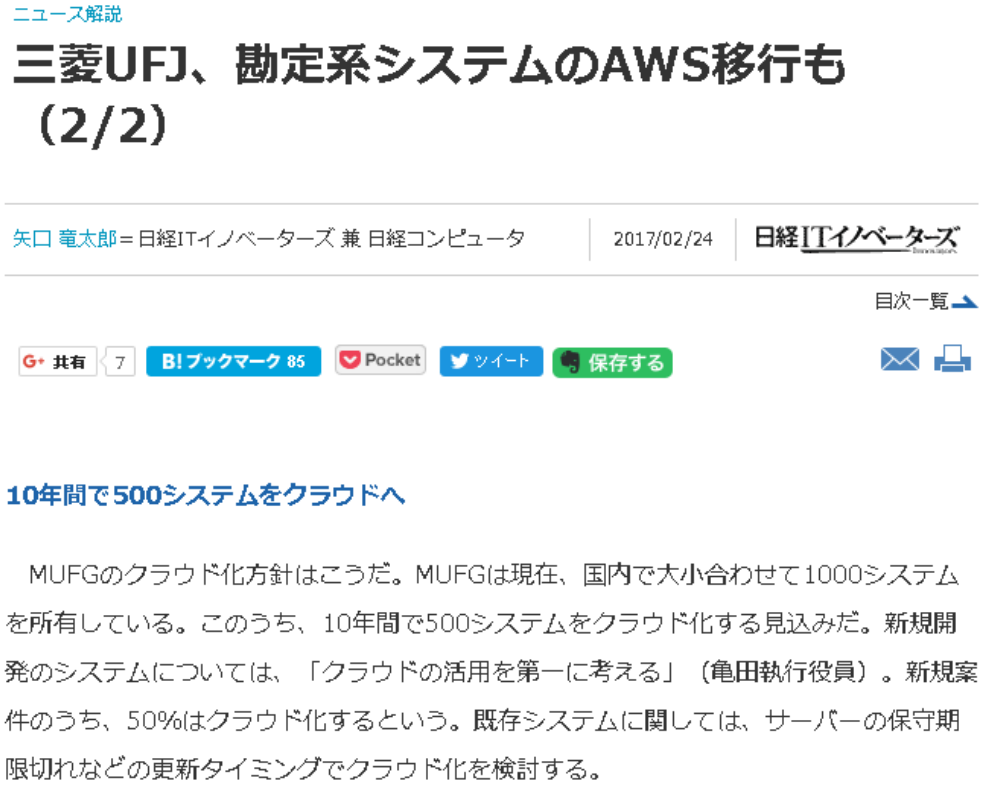
TIS、三菱東京ＵＦＪ銀行のスマートフォンアプリ『My Money』の構築を支援 ～ フェンリル社との協業により、UI/UXに優れたモバイルアプリを実現 ～

2016年12月1日
TIS株式会社

『My Money』のアプリイメージ

Copyright © 2017 TIS Inc. All rights reserved.

クラウドの利用



ニュース解説

三菱UFJ、勘定系システムのAWS移行も（2/2）

矢口 竜太郎＝日経ITイノベーターズ 兼 日経コンピュータ　2017/02/24　日経ITイノベーターズ

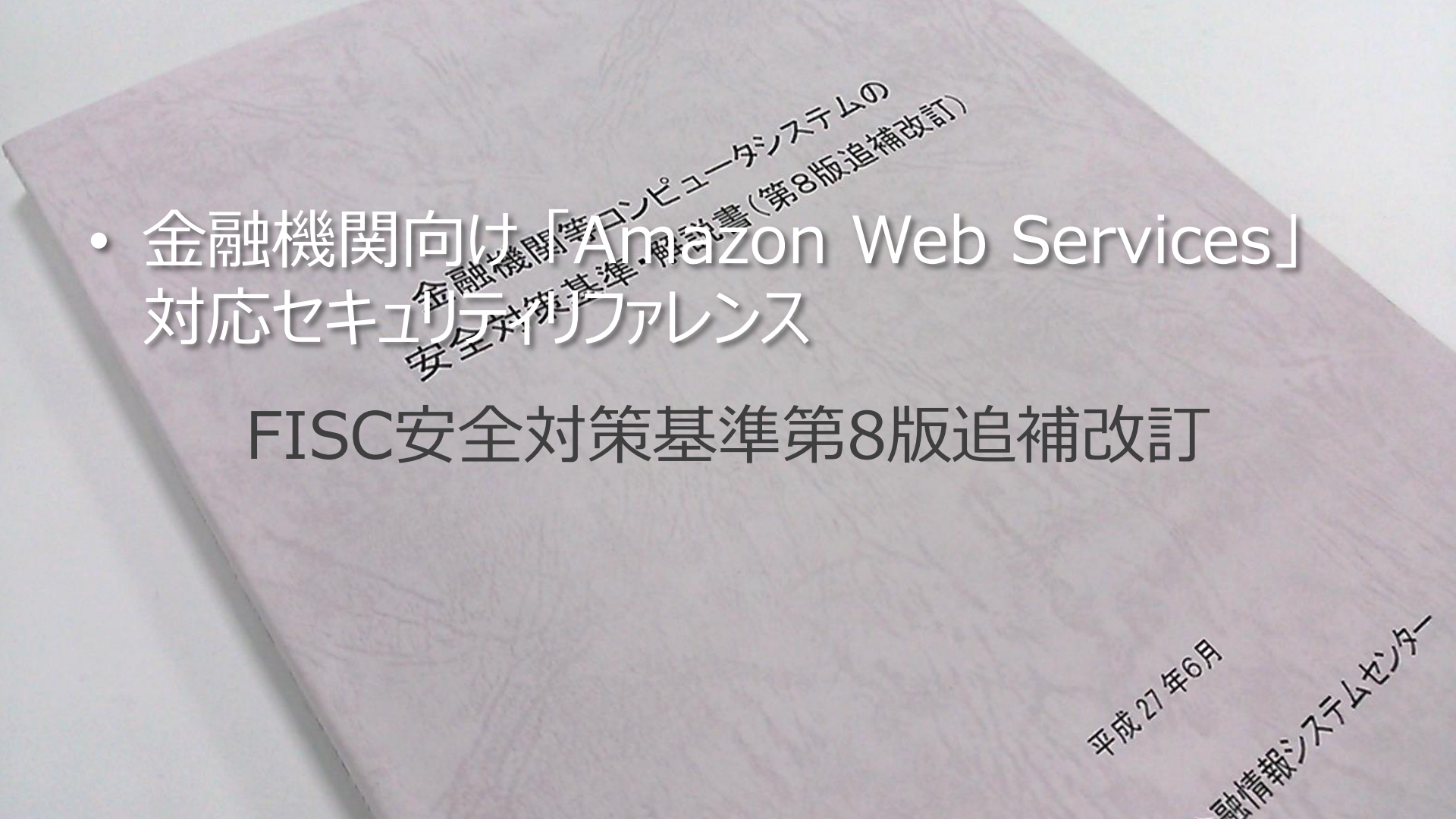
目次一覧

G+ 共有 7　B!ブックマーク 85　Pocket　ツイート　保存する

10年間で500システムをクラウドへ

MUFGのクラウド化方針はこうだ。MUFGは現在、国内で大小合わせて1000システムを所有している。このうち、10年間で500システムをクラウド化する見込みだ。新規開発のシステムについては、「クラウドの活用を第一に考える」（亀田執行役員）。新規案件のうち、50%はクラウド化するという。既存システムに関しては、サーバーの保守期限切れなどの更新タイミングでクラウド化を検討する。

- メガバンク様も利用
- 金融業界側がクラウド領域へ
- 今後の拡大を示唆する記事内容



- 金融機関向け「Amazon Web Services」対応セキュリティリファレンス

FISC安全対策基準第8版追補改訂

FISC安対基準対応

1. はじめに

近年、AWSをはじめとするクラウドサービスは、ビジネスを変革させる手段として、多数の企業で活用されはじめています。

しかし、企業の重要な情報システムにおいては、省庁や業界団体などのセキュリティガイドラインと、クラウド事業者が開示しているシステム仕様との対応、解釈が難しいという課題がありました。

AWSのソリューションプロバイダである SCSK、ISID、NRI、TIS、TrendMicro、MKI、CAC 、ワークスアプリケーションズ、JBCCの9社は、セキュリティ基準の厳しい金融機関等においてクラウドの活用を促進することを目的に、AWSのセキュリティ対応内容が、FISC「金融機関等コンピュータシステムの安全対策基準・解説書」第8版追補改訂に対し、どのように適合し得るか共同で調査／検討を行いました。その成果を「セキュリティリファレンス」第1.3版として整理し、無償で公開いたします。

Copyright © 2017 TIS Inc. All rights reserved.

FISC安対基準運108～113への対応

廃止

運108	クラウドサービスの利用にあたっては、適切なリスク管理を行うこと

新規

運108	クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること。
運109	クラウド事業者と安全対策に関する項目を盛り込んだ契約を締結すること。
運110	クラウドサービス利用にあたって、データ漏洩防止策を講ずること。
運111	クラウド契約終了時のデータ漏洩防止策を講ずること。
運112	クラウド事業者に対する立入監査・モニタリング態勢を整備すること。
運113	サイバー攻撃対応態勢を整備すること。

Copyright © 2017 TIS Inc. All rights reserved.

運108-109

- 運108　クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること。

- 運109　クラウド事業者と安全対策に関する項目を盛り込んだ契約を締結すること。

➢ 対応ドキュメントはAWS側で公開
➢ 利用者側内部の手続きで対応可能

Copyright © 2017 TIS Inc. All rights reserved.

運112

- 運112　クラウド事業者に対する立入監査・モニタリング態勢を整備すること。

- 運112.4　金融機関等において、業務の特性を十分に検討したうえで、委託する業務の重要度が高くないと判断し得る場合には、費用対効果を踏まえた管理策を講じることで、立入監査等に代替することも可能である。

Copyright © 2017 TIS Inc. All rights reserved.

運112

1. その業務の必要とする立入監査等の項目をカバーし、内容が十分と判断できる第三者認証のレポートの活用
2. クラウド事業者が準備するセキュリティに係るホワイトペーパーの確認またはレビュー
3. リスク管理に必要なデータ抽出のツールをクラウド事業者側から準備・提供する

Copyright © 2017 TIS Inc. All rights reserved.

PCI DSS対応

対象範囲内の AWS のサービスはサードパーティの監査機関により全面的に評価され、その結果として認定、Attestation of Compliance、または ATO を取得しました。

• = このサービスは現時点で対象範囲に含まれ、現在のレポートに反映されています。

進行中 = このサービスに対して、サードパーティ評価機関による全面的な評価が実施されています。

準備完了 = このサービスに対するサードパーティ評価機関による全面評価が実施され、認証当局 (AO) によって FedRAMP Security Package が入手できます。

SOC | PCI | ISO | FedRAMP | DoD CC SRG | HIPAA BAA | IRAP | MTCS | C5

サービス/プログラム	PCI
Amazon CloudFront	•
Amazon DynamoDB	•
Amazon EC2 Container Service (ECS)	•
Amazon Elastic Block Store (EBS)	•
Amazon Elastic Compute Cloud (EC2)	•
Amazon Elastic MapReduce	•
Amazon Glacier	•
Amazon Redshift	•

https://aws.amazon.com/jp/compliance/services-in-scope/

Copyright © 2017 TIS Inc. All rights reserved.

PCI DSS対応

- AWS PCI DSS Attestation of Compliance (AOC)
  - 対応サービスのRequirementへの評価
- インフラレイヤーは基本的にAWS側で対応
- ログ関連項目に対応しやすい(AWS CloudTrail、AWS Config、VPC Flow Logs等)
- 標準機能と適切な権限管理で対応できる項目多数

Copyright © 2017 TIS Inc. All rights reserved.

お話すること

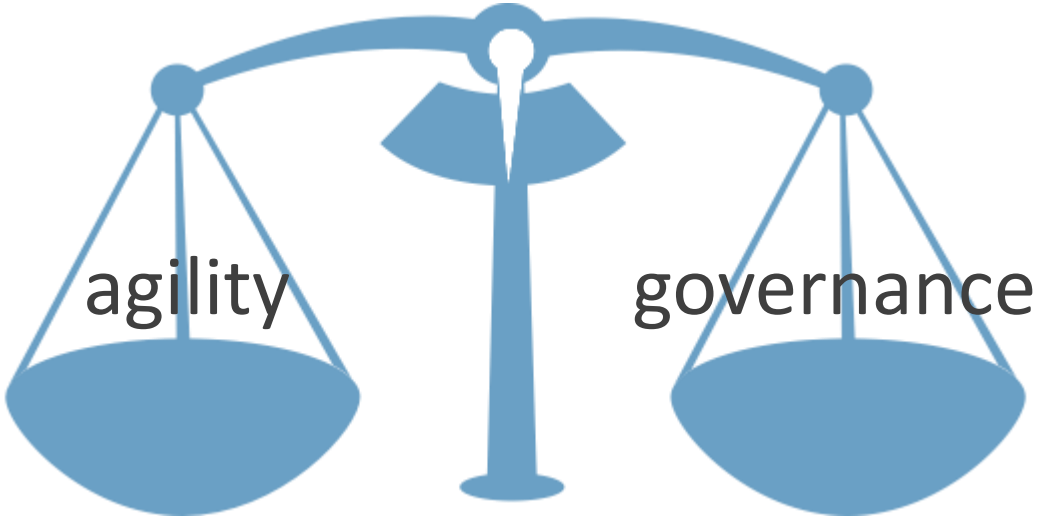
- 金融業界動向と背景
- クラウド利用プラクティス(CAFとCCoE)
- 問題と対応
- さらに行っていくこと

Copyright © 2017 TIS Inc. All rights reserved.

クラウドを使う理由

agility

Copyright © 2017 TIS Inc. All rights reserved.



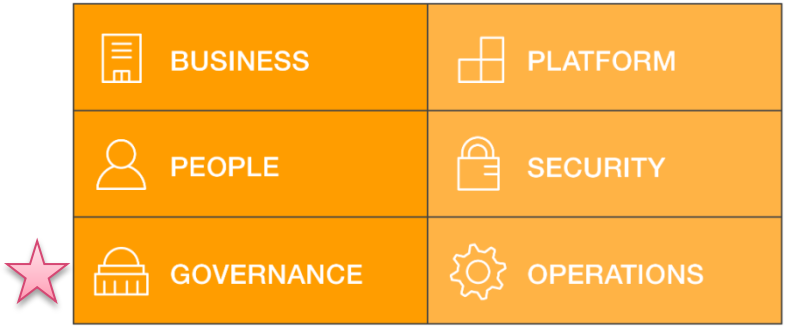
Copyright © 2017 TIS Inc. All rights reserved.

ITガバナンス

- ビジネス戦略との整合
- 価値の実現
- リスクの管理
- 資源の管理
- 成果の測定

Copyright © 2017 TIS Inc. All rights reserved.

AWS Cloud Adoption Framework



教科書となるフレームワーク
Cloud Adoption Framework(CAF)

6つの軸

AWSが行った多数のクラウド導入プロジェクトの経験に基づく知見

https://aws.amazon.com/professional-services/CAF/perspectives/

Copyright © 2017 TIS Inc. All rights reserved.

AWS Cloud Adoption Framework

- 各々に複数のコンポーネント
- 必要なコンポーネントを組み合わせて利用

AWS Cloud Adoption Framework

CAFで重要なこと

Cloud Center of Excellence(CCoE)
設立

Copyright © 2017 TIS Inc. All rights reserved.

Centers of Excellence

- Center of Excellence (CoE)
  - 特定の領域をリード
  - ベストプラクティスを提供
  - 利用者サポート・トレーニング
  - チーム、共通の機関、集団

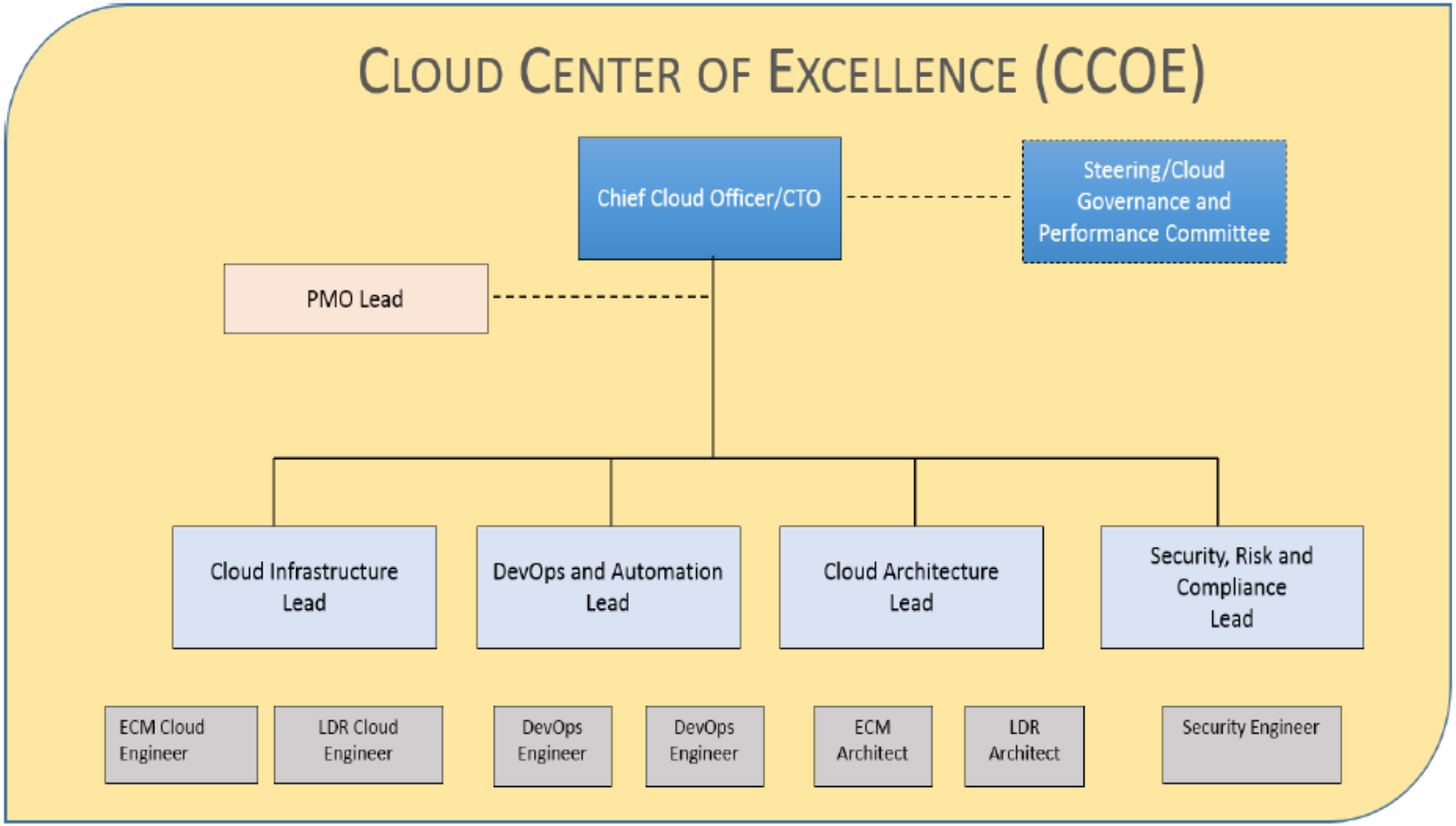
- Cloud + CoE → CCoE

Copyright © 2017 TIS Inc. All rights reserved.

Cloud Center of Excellence(CCoE)

- CCoEは分野を超えた専門性を持つチーム
  - 運用
  - 開発
  - 戦略
  - セキュリティ
  - テスト
- 標準化の推進
  - PoC
  - リファレンスアーキテクチャ
  - セキュリティパターン
  - テストパターン
  - 監視パターン
- 標準化の継続的管理
  - 頻繁なフィードバックと変更
- 知見定着後に解散することもある
- フェーズにより柔軟にメンバーの追加
- 利用部門サポート・トレーニング

Copyright © 2017 TIS Inc. All rights reserved.



出典：AWS re:Invent 2016: Governance Strategies for Cloud Transformation (WWPS302)

3 Phases of Cloud Governance

Beginning	Adopting	Mature
• Minimal integration • Reactive environment • Cost overruns • Manual deployments • No Cloud Structure	• CCoE is in place and policies are maturing • Policies matched to process • Designing for Cost • Rapid Deployment	• Full automation and self-service • Benefits of cloud services realized • Agility and control • Optimized for Cost • Secure and Compliant environment

出典：AWS re:Invent 2016: Governance Strategies for Cloud Transformation (WWPS302)

ガバナンス関連の実施事項

- 利用ガイドラインの策定
- リファレンスアーキテクチャ(構成の標準化)の作成
- ガイドライン/アーキテクチャパターンの更新
- コスト最適化
- 監視・管理の最適化
- オペレーション標準化・自動化

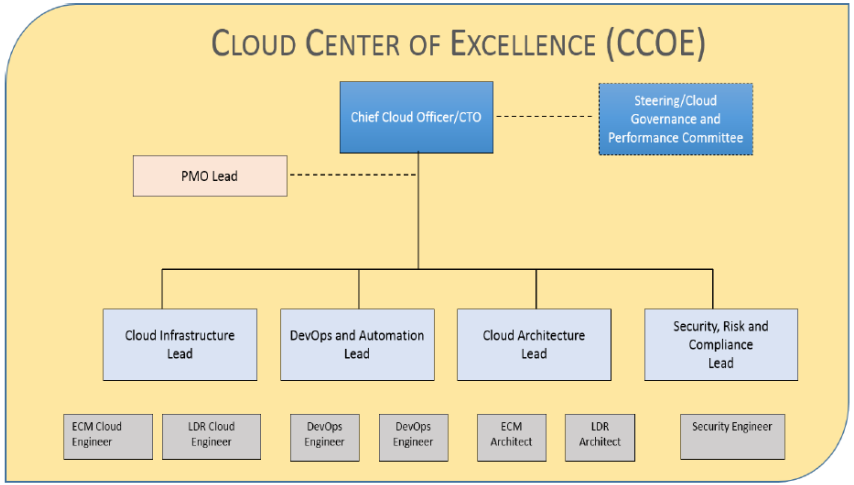
Copyright © 2017 TIS Inc. All rights reserved.

CAFと組織

- CAFは合理的なプラクティス
- 日本の組織への適合
- 既存のガバナンスフレームワークとの整合

Copyright © 2017 TIS Inc. All rights reserved.

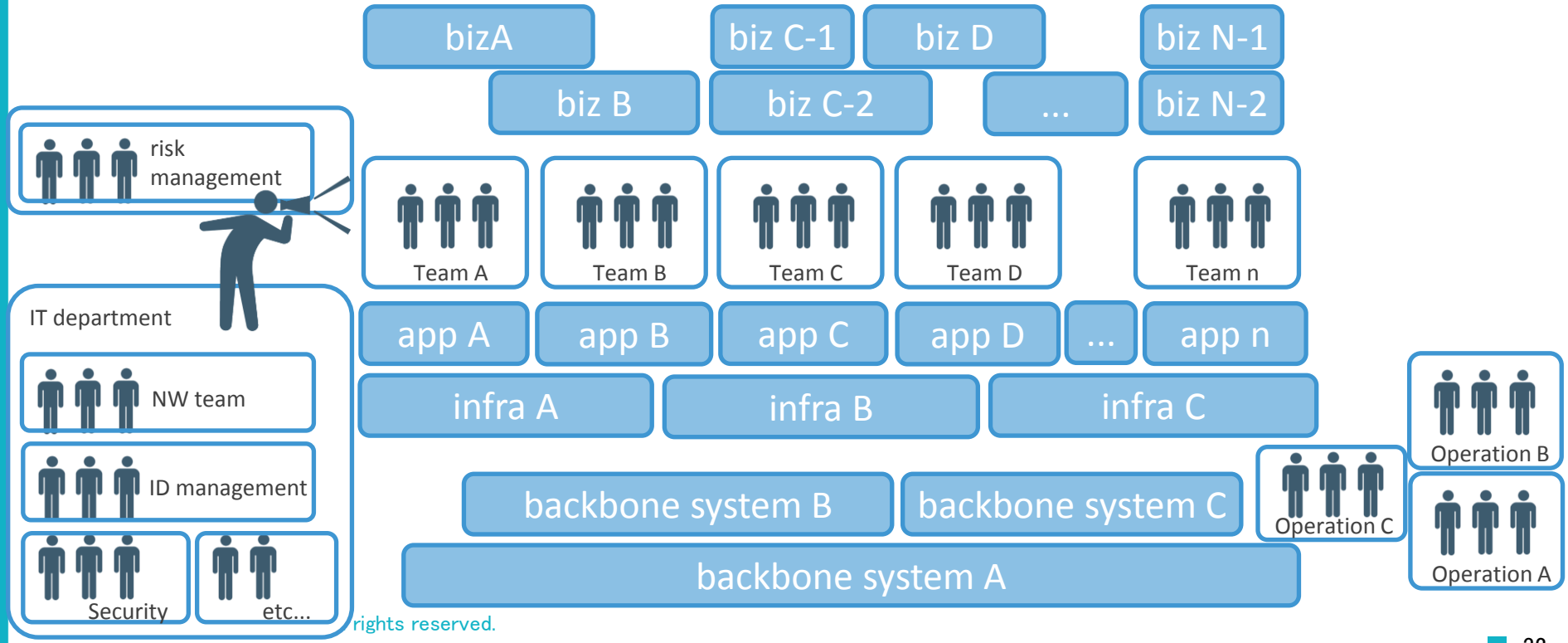
CAFと組織



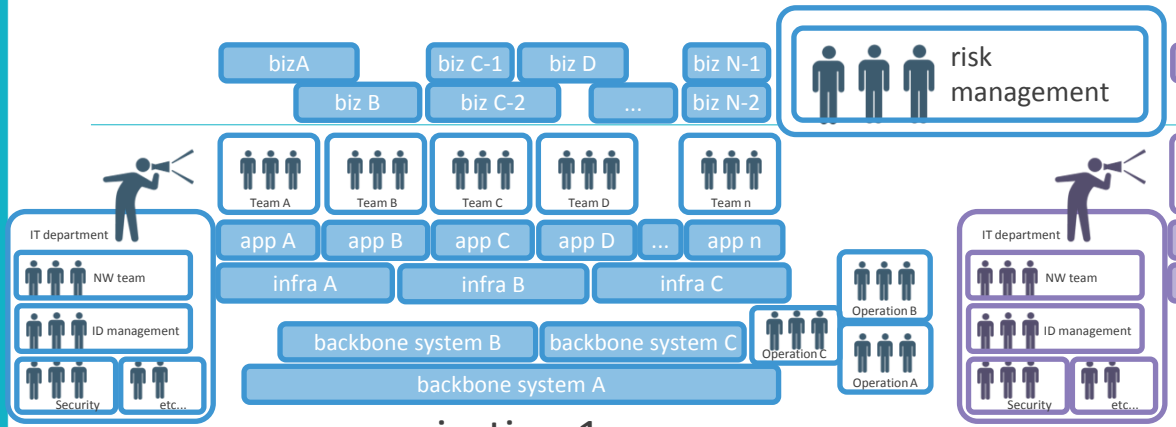
- business
- application
- infrastructure
- backbone system

Copyright © 2017 TIS Inc. All rights reserved.

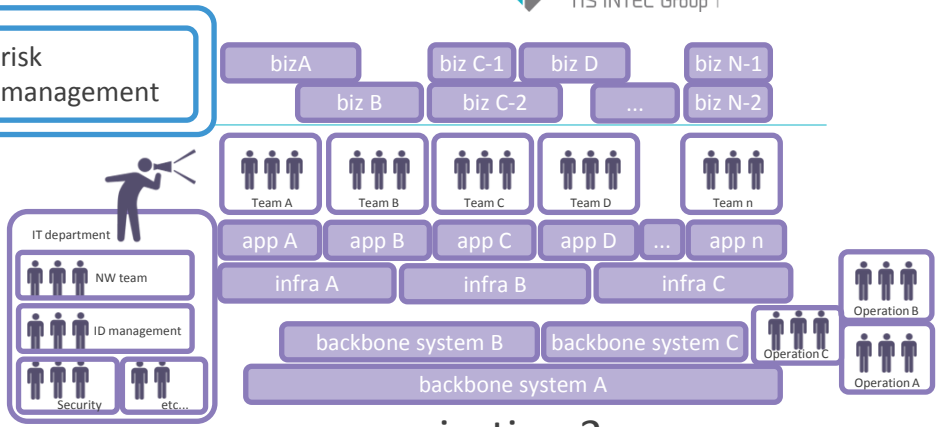
CAFと組織



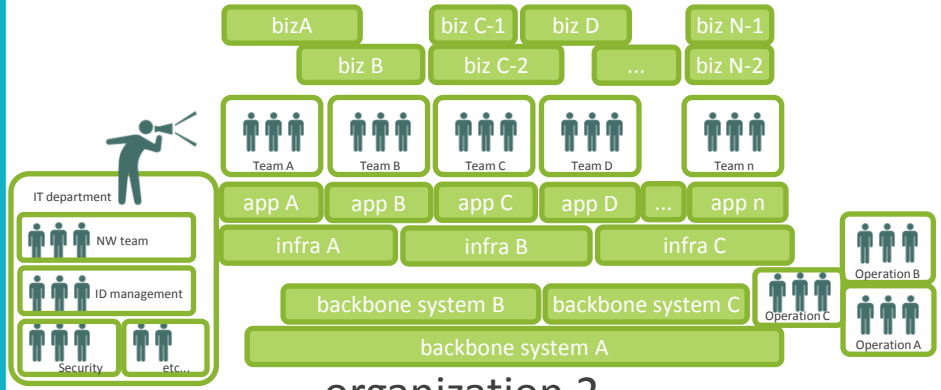
rights reserved.



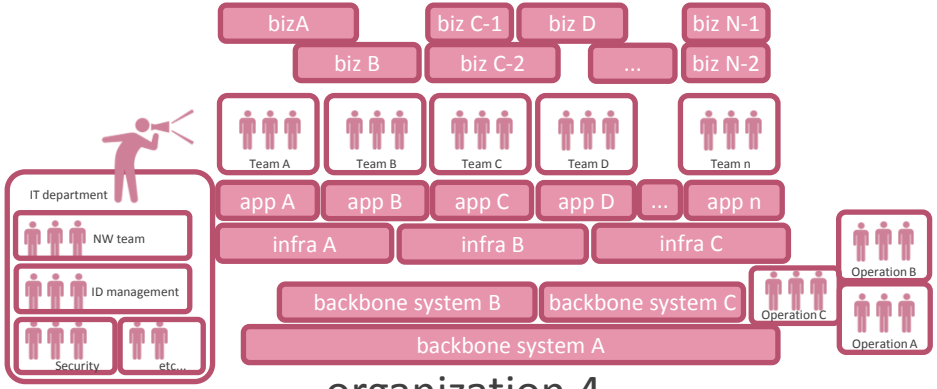
organization 1



organization 3



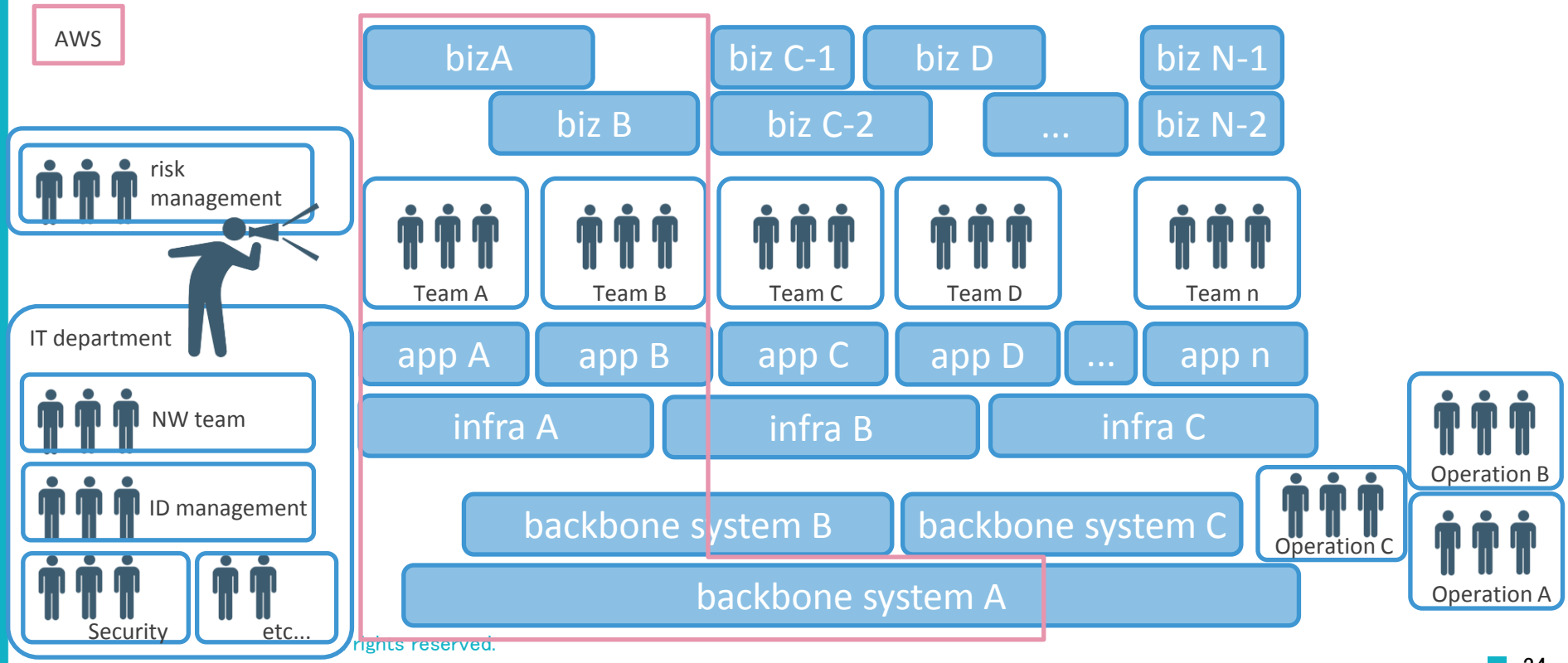
organization 2



organization 4

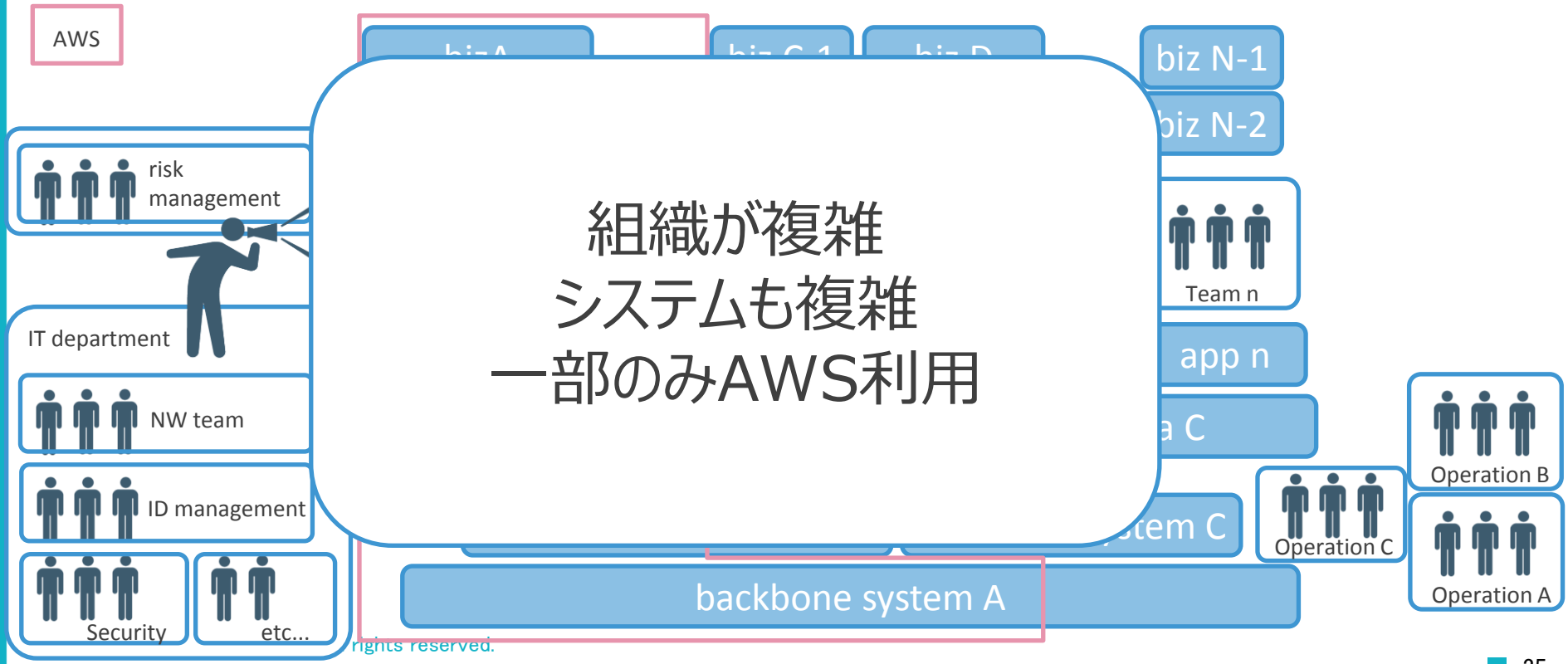
Copyright © 2017 TIS Inc. All rights reserved.

CAFと組織



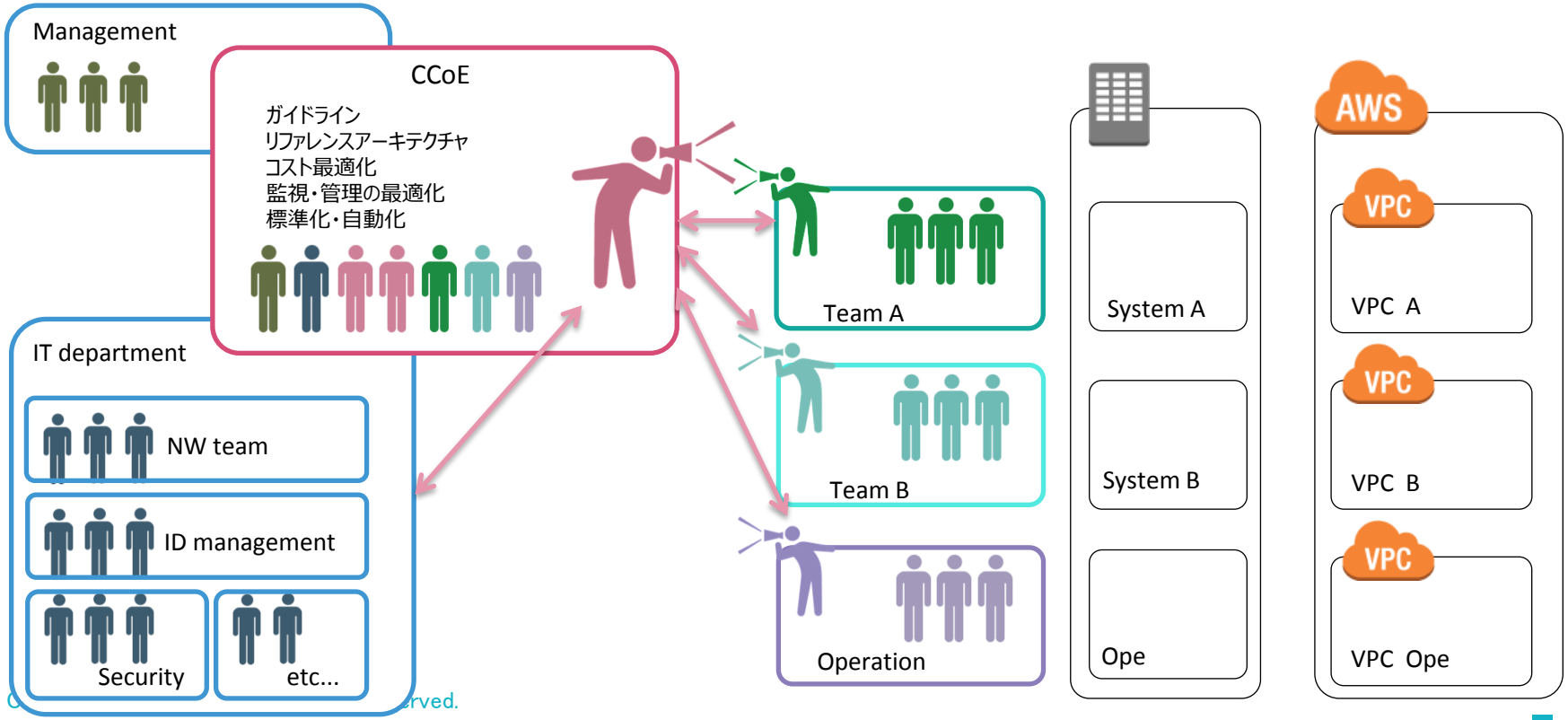
rights reserved.

CAFと組織



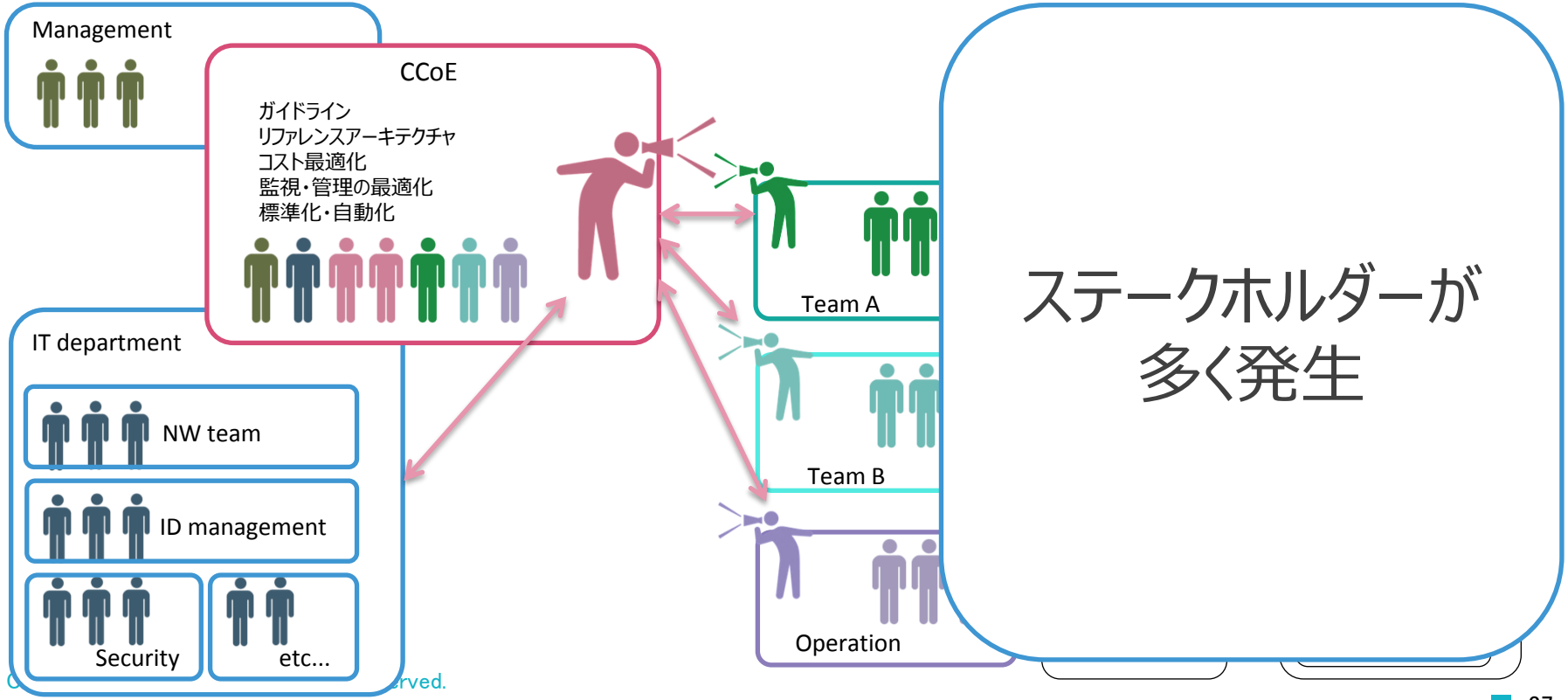
rights reserved.

CCoEと組織



served.

CCoEと組織



served.

お話すること

- 金融業界動向と背景
- クラウド利用プラクティス(CAFとCCoE)
- 問題と対応
- さらに行っていくこと

Copyright © 2017 TIS Inc. All rights reserved.

問題

Copyright © 2017 TIS Inc. All rights reserved.

よくある問題

- 組織
  - 既存文化、既存ガバナンスルール
  - 関連組織の責任・権限競合
- 手段
  - セキュリティ手段
  - システム移行/並行稼動
- コスト
  - 予算どりと料金

Copyright © 2017 TIS Inc. All rights reserved.

問題例(1)

- ガバナンス対応の主管？
  - AWS上のNW要素(ロードバランサ、NAT、Security Group他)
  - AWS上のID要素(各種ユーザー、IAM権限、MFA他)
  - AWS上のOS要素(OSユーザー、設定他)
  - AWSにおけるオペレーション要素(ログ、イベント、監視他)
- 既存管理ルールで個別に管理する？
  - EC2だけでも複数チームに管理要素が分散
  - フローの複雑化、アジリティの低下
  - 「必要なとき、必要なだけ」が困難

Copyright © 2017 TIS Inc. All rights reserved.

問題例(1)

- ガバナンス対応の主管？
  - ー
  - ー
  - ー
  - ー
- 既
  - ー
  - ー
  - ー

- ガバナンス関連主管をCCoEへ
- CCoEが権限と責任を持つ
  - ー既存環境と完全分離することも手
- CCoEは既存管理者を含むバーチャルチーム化

Copyright © 2017 TIS Inc. All rights reserved.

問題例(2)

- 既存の運用ルール適用？
  - 管理エージェント必須、EC2しか使えない
  - AutoScalingが必須ソフトウェアのライセンス体系に合わない
  - IPアドレスが構成管理アイテム
  - DBの運用ルールと、RDSの機能が合わない

Copyright © 2017 TIS Inc. All rights reserved.

問題例(2)

- 既存の運用ルール適用？
  - ー
  - ー
  - ー
  - ー

- 目的はビジネス、AWSは手段
  - ー目的から外れたルールは見直す
  - ー目的に適合する標準化の実施
  - ー管理のための仕組みも含めた標準化
  - ークラウド利用の成熟段階を踏まえた施策

合わない

Copyright © 2017 TIS Inc. All rights reserved.

~~個別対応~~

課題管理

Copyright © 2017 TIS Inc. All rights reserved.

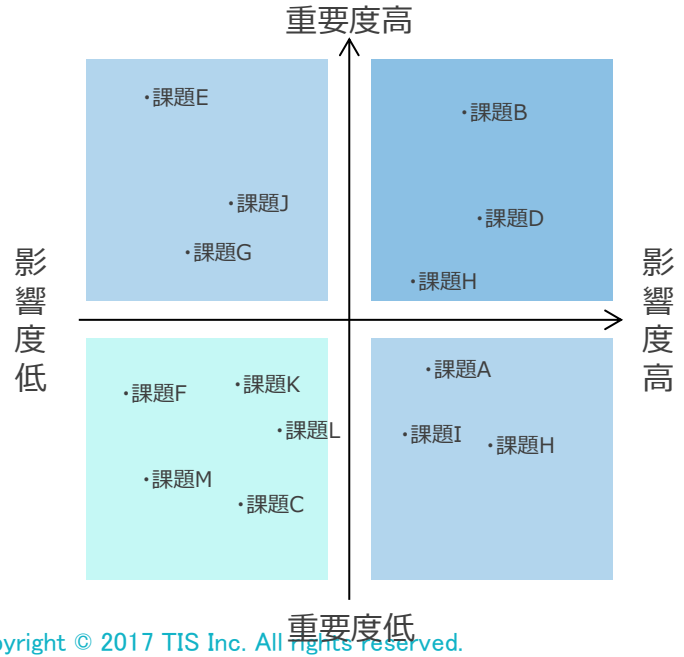
Do not over plan before experimenting with migration waves.

Learn by doing.

Copyright © 2017 TIS Inc. All rights reserved.

課題と対応

- 課題管理へと一般化



影響度

- 対象ビジネス範囲
- 対象システム範囲
- 時間的制約(緊急度)
- etc…

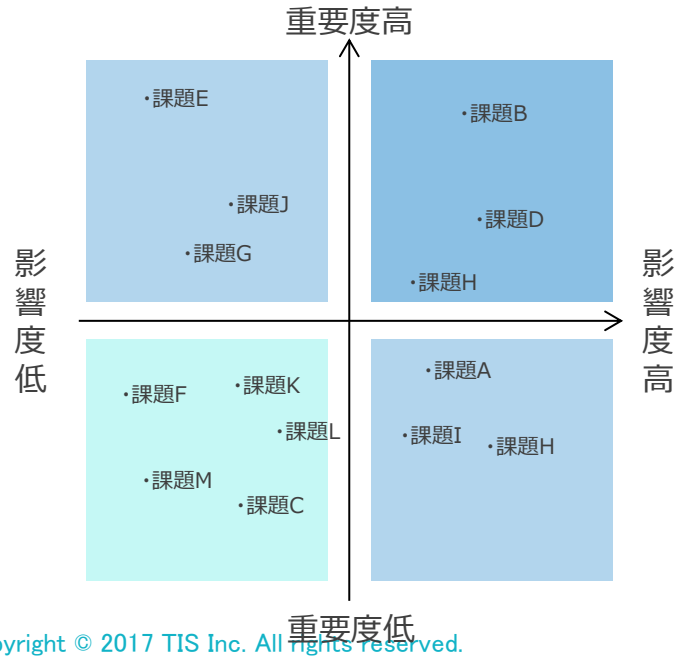
重要度 項目例：

- ビジネスインパクト
- セキュリティインパクト
- etc…

Copyright © 2017 TIS Inc. All rights reserved.

課題と対応

- 課題管理へと一般化



影響度

- 対象ビジネス範囲
- 対象システム範囲
- 時間的制約(**緊急度**)
- etc…

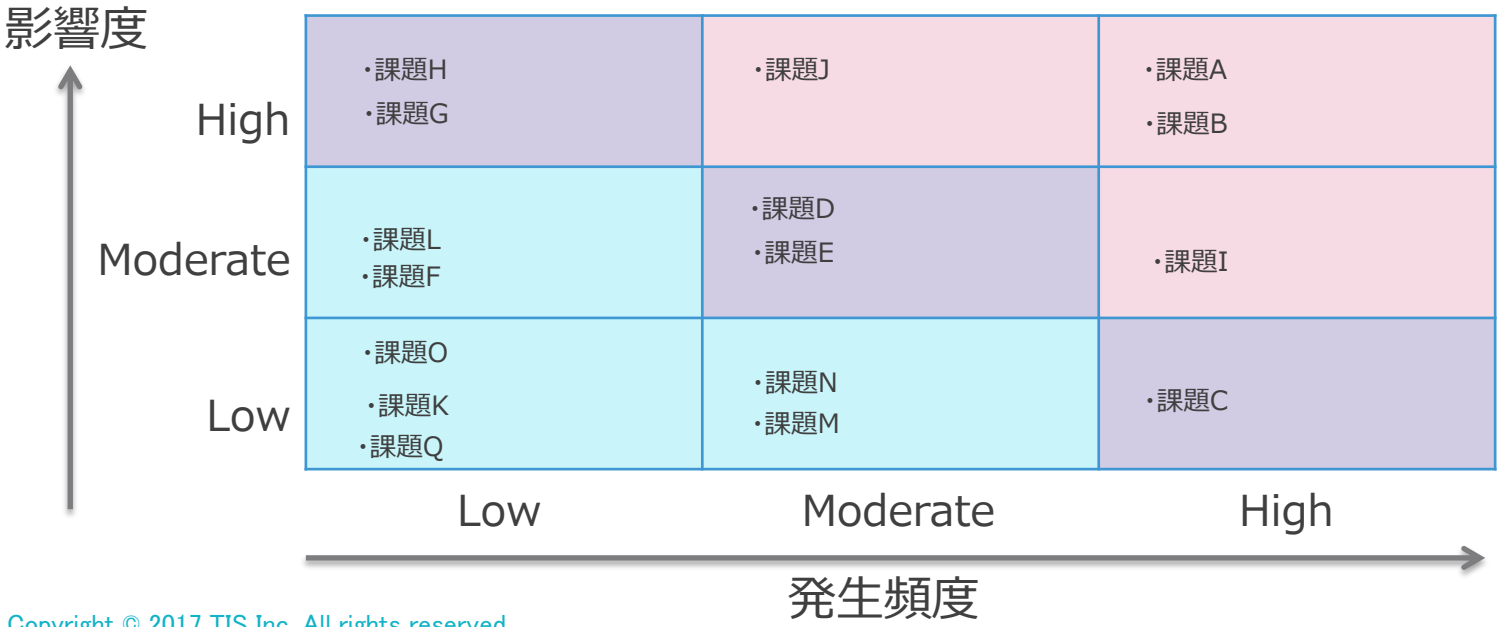
重要度 項目例：

- ビジネスインパクト
- **セキュリティインパクト**
- etc…

Copyright © 2017 TIS Inc. All rights reserved.

課題と対応

リスク分析アプローチでの対応



Copyright © 2017 TIS Inc. All rights reserved.

課題の種類

組織(体制・権限・責任範囲)
手段(技術・手法・ツール)
コスト(時間・料金関連)

Copyright © 2017 TIS Inc. All rights reserved.

課題の種類

組織(体制・権限・責任範囲)

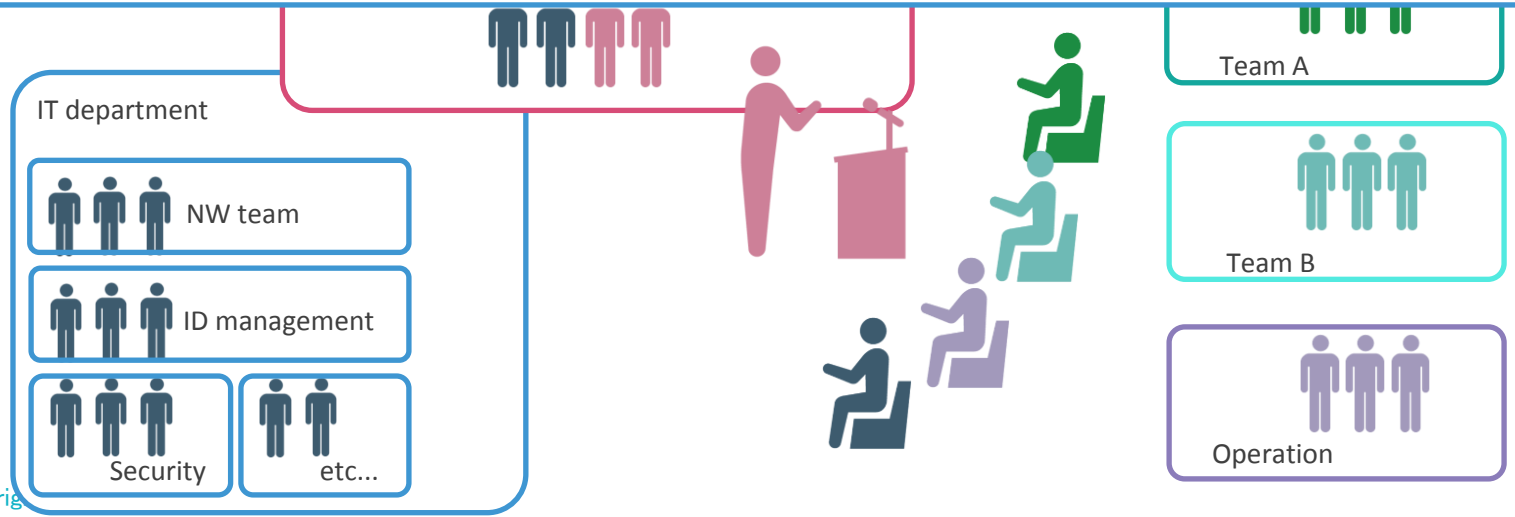
手段(技術・手法・ツール)

コスト(時間・料金関連)

Copyright © 2017 TIS Inc. All rights reserved.

対応例

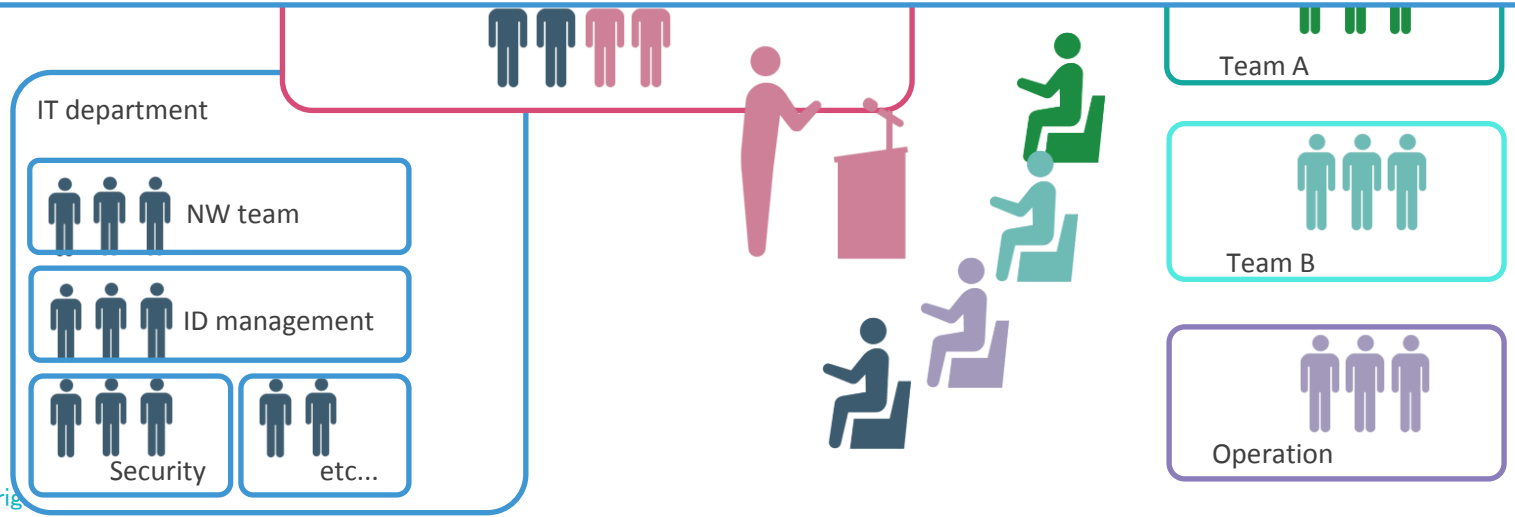
仲間を作る



Copyrig

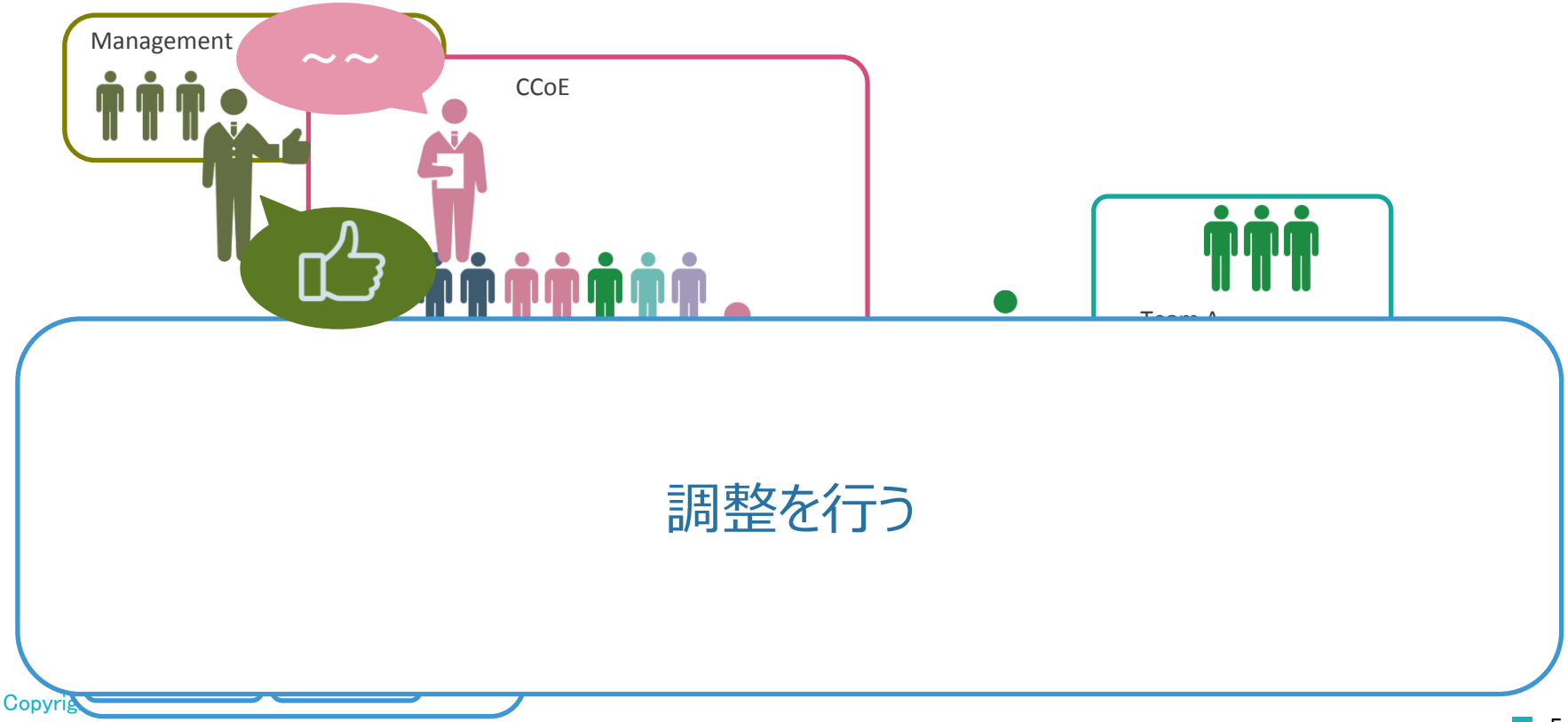
対応例

CCoE設立当初はIT部門が中心になる場合が多い
利用部門への理解と協力の獲得
社内でのコミュニティ活動、検討会



Copyrig

対応例



Copyrig

対応例

課題の中には、組織を超える決め事、組織を跨ぐ権限が
必要な場合もある
マネジメント層へのスムーズな働きかけも重要

Copyrig

対応例

- AWS利用の有効性を組織内に示す
  - 実績は効果
  - Fintech等の新規領域はひとつのきっかけ
- 仲間を作る
  - 社内コミュニティ
  - 関係部門との勉強会、サポート
- 社内でのコンセンサス、組織問題、権限問題解消の働きかけ

Copyright © 2017 TIS Inc. All rights reserved.

地道で人間くさい対応

Copyright © 2017 TIS Inc. All rights reserved.

お話すること

- 金融業界動向と背景
- クラウド利用プラクティス(CAFとCCoE)
- 問題と対応
- さらに行っていくこと

Copyright © 2017 TIS Inc. All rights reserved.

技術的につまずくポイント(一例)

- AWS-内部間のNWファンクションの挙動
  - NATやUTMを挟むと認証がうまく行かない等
- グローバルなNW経路の設計が複雑
  - 拠点-Tokyoリージョン間に全リージョンのトラフィック集中
- フェデレーション設計はどうしてもパワーが必要
- 権限管理職人の発生

Copyright © 2017 TIS Inc. All rights reserved.

つまずきへの対応

- Proof of Concept (PoC/概念実証)
- 先人の経験
- コミュニティやベンダーの知見

Copyright © 2017 TIS Inc. All rights reserved.

外部コミュニティ

JAWS-UG

Fin-JAWS
OpsJAWS
E-JAWS
…etc

API Meetup

https://api-meetup.doorkeeper.jp/

Copyright © 2017 TIS Inc. All rights reserved.

やってみる文化

- Fintechハッカソンのお手伝い
- 新規領域へのチャレンジ

TIS
TIS INTEC Group

サイトマップ　採用情報　お問い合わせ

ニュース　セミナー　サービス／ソリューション　導入事例　特集・レポート　会社情

HOME > ニュース > 三菱東京UFJ銀行主催『Fintech Challenge 2016ハッカソン』を支援

三菱東京UFJ銀行主催『Fintech Challenge 2016ハッカソン』を支援

2015年12月16日
TIS株式会社

ITホールディングスグループのTIS株式会社（本社：東京都新宿区、代表取締役会長兼社長：桑野　徹、以下　TIS）は、株式会社三菱東京UFJ銀行（本社：東京都千代田区、頭取：平野　信行、以下　三菱東京UFJ銀行）が主催する開発者イベント『Fintech Challenge 2016 “Bring Your Own Bank！”ハッカソン※1』を支援することを発表します。

本イベントは、三菱東京UFJ銀行が、「より身近で便利なIT×金融のサービスづくり」をテーマに、銀行API※2の可能性と様々な活用アイデアを探ることを目的としております。
本イベントを通じ、三菱東京UFJ銀行は、オープンイノベーション※3によるさらなる革新的な金融サービスの創造に取り組んでいきます。

Copyright © 2017 TIS Inc. All rights reserved.

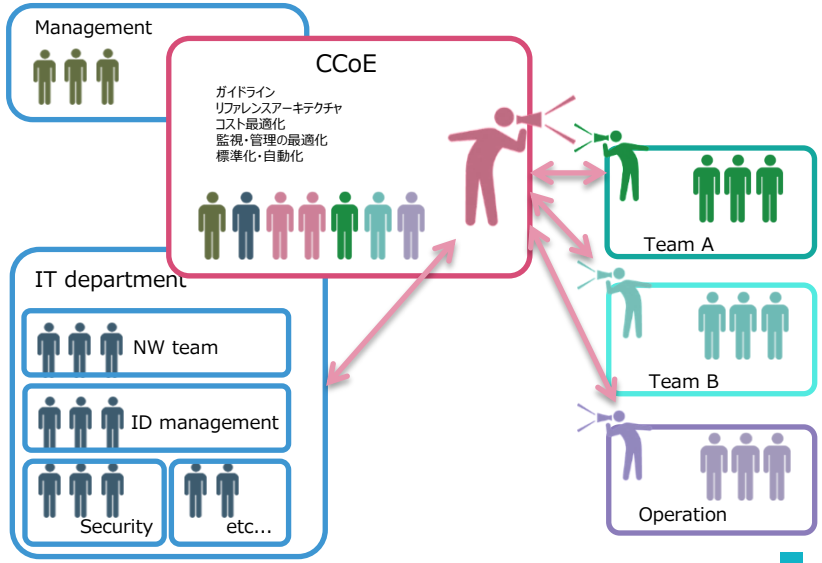
力の掛かること

- 多数の標準化、リファレンスアーキテクチャ制定
- 繰り返し行われるProof of Concept (PoC/概念実証)
- AWSのサービスアップデート → 標準化内容の更新と展開
- セキュリティ基準の更新対応
- ガイドライン最新化と展開
- 権限の設計とユーザー向けインターフェース

Copyright © 2017 TIS Inc. All rights reserved.

変更への対応

- デプロイは変更
  - 当初はCCoEによる承認、変更管理プロセス
- リリース管理
- レビュー
  - チーム間の基準差異対策
- チケット管理



Copyright © 2017 TIS Inc. All rights reserved.

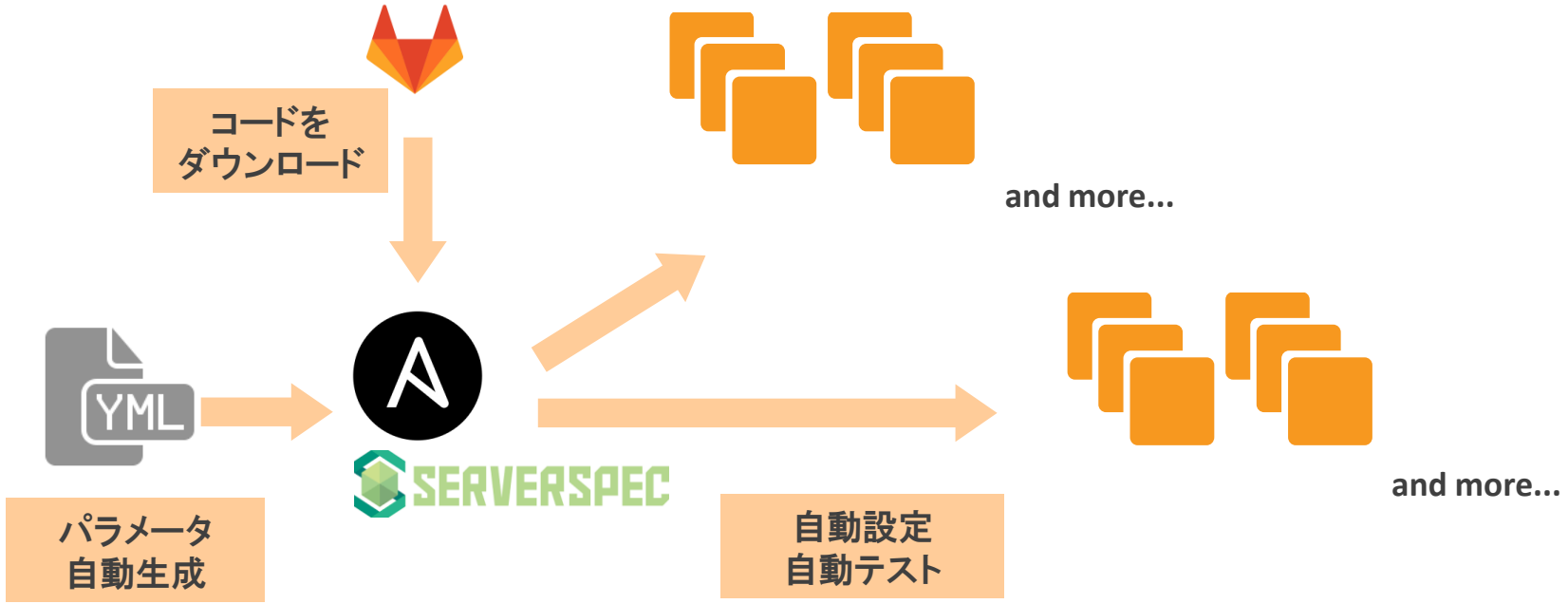
標準化と自動化

- カバナンスのための標準化
  - 品質(同一結果)

- アジリティのための自動化
  - 運用のスケール、スピードアップ

Copyright © 2017 TIS Inc. All rights reserved.

標準化と自動化



Copyright © 2017 TIS Inc. All rights reserved.

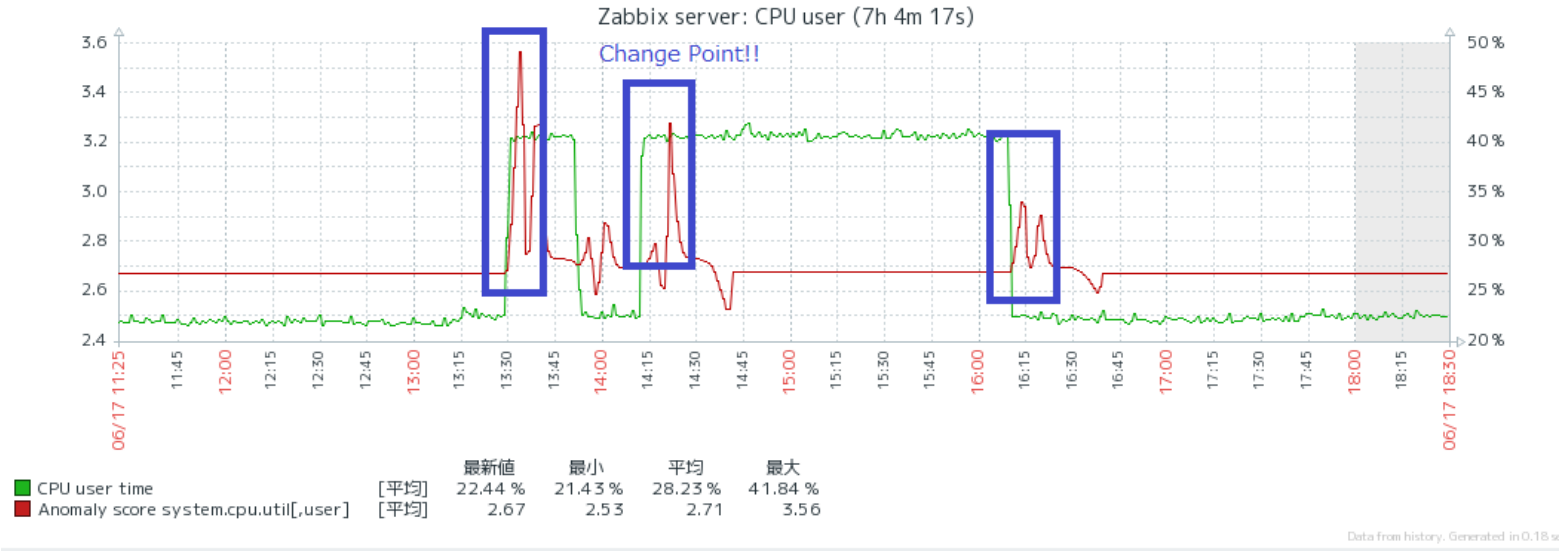
イベント駆動と自動化

- イベント駆動型による自動化
  - 人はスケールしきれない。自動化が必須。
  - 自動化は標準化の先にある。ガバナンスの一部。
- 自動化に向けたAWSの各種サービス
  - CloudWatch Events
  - AWS Config / AWS Config Rules
  - Amazon EC2 Systems Manager
- 業務レイヤーへのフィードバック(変則検知、イベント統計)

Copyright © 2017 TIS Inc. All rights reserved.

イベント駆動と自動化

例えば、変則検知もトリガーにできる



https://github.com/ike-dai/zabbix_anomaly

Copyright © 2017 TIS Inc. All rights reserved.

標準化・自動化の整理

分類	運用
メニュー/カタログ	リファレンスアーキテクチャ、標準化テンプレート管理
監視	AWSイベント、ログ・アプリケーション・OS・キャパシティ監視
ログ管理・監査	AWSログ、OS・ミドル・アプリケーションログ
イベント管理	AWS CloudWatch、監視ツール
インシデント/課題管理	チケット管理、ナレッジ、監視との統合、変更管理との統合
変更・構成管理	変更計画、ワークフロー、変更追跡, パッチ管理
リリース管理	リリース管理、構成管理
セキュリティ管理	アクセス制御、NW制御
権限管理	AWS上の権限、OS権限、フェデレーションユーザー
ジョブ自動化	ジョブ管理ツール、イベント駆動
バックアップ管理	イメージ取得、データバックアップ、リストア
タグ管理	タグ設定
コスト管理	コスト管理、RI管理

Copyright © 2017 TIS Inc. All rights reserved.

ITILフレームワークの利用

- 既存の枠組みの利用
- イベント/インシデント管理
  - AWS CloudWatch、監視ツールの利用
  - マネージドサービスプロバイダーの利用
- 問題管理
  - AWS Enterprise Support, Amazon Technical Account Manager(TAM)の利用
  - マネージドサービスプロバイダーの利用

Copyright © 2017 TIS Inc. All rights reserved.

AWSとパートナー

- CAFの利用、CCoEの進展にはコンサルティングサービスやベンダーの利用も有効
  - AWSプロフェッショナルサービスの利用
  - マネージドサービスプロバイダーの利用

Copyright © 2017 TIS Inc. All rights reserved.

まとめ

- 金融業界レベルでもAWS利用の背景が整ってきている
- ガバナンス適用にはCAFの利用が有効
- CCoEはガバナンスの要
- CCoEの柔軟なチームづくりは人間くさい動きも重要
- 問題は課題管理へと一般化、「クラウドだから」をなくす
- 問題解決やチーム作り、標準化には泥臭い対応も発生
- ガバナンスに向けた標準化と自動化
- AWSプロフェッショナルサービスやパートナーの利用も効果的

Copyright © 2017 TIS Inc. All rights reserved.

TIS
TIS INTEC Group
Go Beyond