SIAM™のガバナンスってなんでしょう？　：　リテインド能力

20230204(3.1)　MIJ LLC　三浦
本文は、SIAM™ Foundation & Professional BOK
及び事例の研究やMIJの経験に基づきまとめています

はじめに

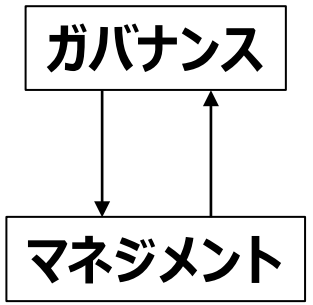
SIAM™では、**リテインド能力**と言う**聞きなれない言葉**が紹介されています。
また、**ガバナンス**と言う**聞きなれてはいますが、意味が今一つ理解できない言葉**も出てきます。
これらをなるほどと理解して頂き、**リテインド能力の**役割をアサインしたり、組織化や人材育成を検討していただく一助として作成しています。

実はSIAM™　ＢOK（知識体系の本）のFoundation本でもProfessional本でも、リテインド能力は、「このような項目をガバナンスしなければいけない」として、8項目をリストしていますが、それぞれにどういう狙いか、どうそれを実現すればいいか、等のリテインド能力の具体的な内容は触れてはいません（よく考えれば、リテインド能力は顧客側で備えるべきものであり、SIAM™エコステムの外とも解釈できます）。
顧客側でセキュリティ事故がありマルチソーシングのガバナンスを強化したいとお考えの場合、或いは、サービスインテグレータを引き受けるが顧客側のリテインド能力の強化も支援したいような場合に、何をどのようにガバナンスすればいいのか、その為の人材に求められるものは何かを説明するものです。

I. ガバナンスとは

- **SIAM™においては、ガバナンス（統治）**とは、**顧客・ビジネスの求める期待やニーズが、複数の内外のサービスプロバイダにより満たされているようにする**仕組みです。

- **ガバナンス**は方向性を与えますが、それを受けて**マネジメント**が、実現します。



（顧客のビジネスの成功を目指し）ポリシーやルール、ガイドラインを示します。
それに従っているかをマネジメントからの**報告で確認**し、必要なら**是正**します。
例　顧の信頼できるサービス提供を目指し、セキュリティポリシーを定め展開します。

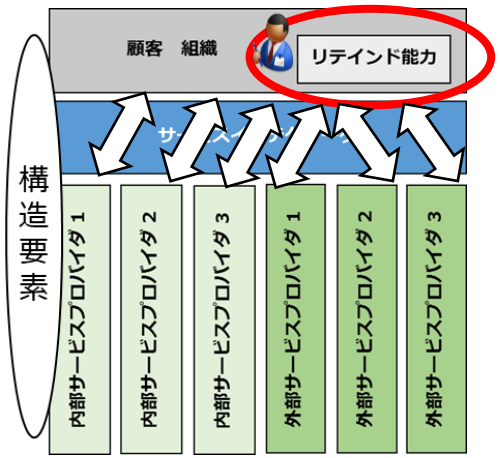
自らの活動をマネジメントする際に、**ポリシーやルール、ガイドライン**に基づきます。
途中経過や結果を**報告**し、ガバナンスに沿っていることを確認します。
例　ポリシーを受け、セキュリティ管理を設計・計画し、実施します。

ちょっと再確認

「**こういう事は当然やってる筈だ！何故やってなかったのか？！**」と言っても後の祭りです。

何を実現していてほしいのかを、きちんと明示しておく必要があります。
明示しないまま、マスコミの前で、頭を下げても説明責任を果たしたことにはなりません。

II.　SIAM™でガバナンスの責任を持つリテインド能力



- **多数のプロバイダに広がるサービス提供が確実に適切にガバナンス**されるように**リテインド能力**と言う機能を（アウトソーシングしないで）自前で保持します。
- **リテインド能力は、**マルチプロバイダ環境で守るべき**方向性やポリシー、ルールやガイド**を定めます。

- **リテインド能力は、サービスインテグレータに権限委譲します。**
- **サービスインテグレータ(SI)は、多数のプロバイダのマネジメントと共に、各ガバナンス項目を展開**します。

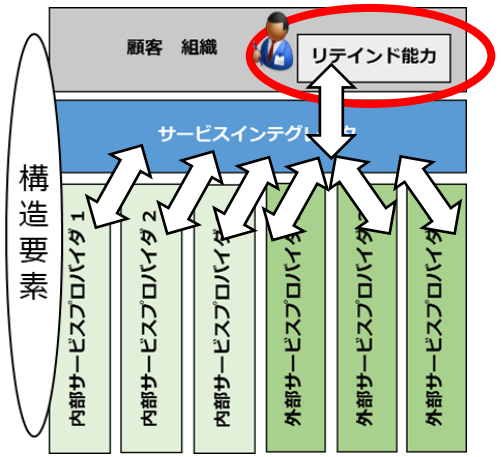
SIと各プロバイダはサービス提供に当たり、**ガバナンス要請を守るべくマネジメント**します。
適宜、その実現状況を**確認・監査**し、是正することで、ガバナンスを実現します。

III.　SIAM™では、マルチソーシング環境では少なくとも以下の８項目をガバナンスするべき項目だとしています

① **エンタープライズアーキテクチャ**
② **ITリスク**
③ **ソーシング**
④ **セキュリティやコンプライアンスのポリシーや標準**
⑤ **サービスポートフォリオ**
⑥ **購買・契約・取引・予算とコスト**
⑦ **サービスインテグレータのガバナンス**
⑧ **需要管理（デマンドマネジメント）**

次ページから検討しましょう

■ ガバナンスするべき８つの項目の概要



ガバナンス項目を展開し確認する

①　エンタープライズアーキテクチャ

サービスやITのアーキテクチャをエンタープライズ・レベルで定め、各サービス選定や統合において、それに従うようにすることで、ITシステムやITサービスの整合を図り、無駄なコストの発生を抑えます。
このようなアーキテクチャが無いと、各サービスの選定や統合、開発、導入などにおいて、個別最適により実現され、全体として、無駄や不足が発生する可能性があります。
一般にサービスインテグレータ(SI)や各プロバイダのアーキテクトが集まるEA委員会を持ちます。

②　ソーシング

サービスの提供において、内部プロバイダ（顧客・ビジネスと同じプロバイダ組織）か外部プロバイダからソーシングするのかの基準と判断を行います。アウトソーシング判断は、その対象がコアコンピテンシであるか、重要なIP（知的資産）か、セキュリティの重要性、目標とするコストでサービス提供できるかなどの戦略的見地からなされます。或いは、現在アウトソーシングしているものを内部に戻すなどの判断もあります。サービス品質の向上を見込めない問題プロバイダについては契約をやめ他と入れ替えるリコメンドをする場合もあります。
一般にリテインド能力のソーシングマネージャはIT（情報技術）やクラウドサービスなどITサービスとプロバイダの動向についてSIの支援を得て理解し、これらの判断を行います。

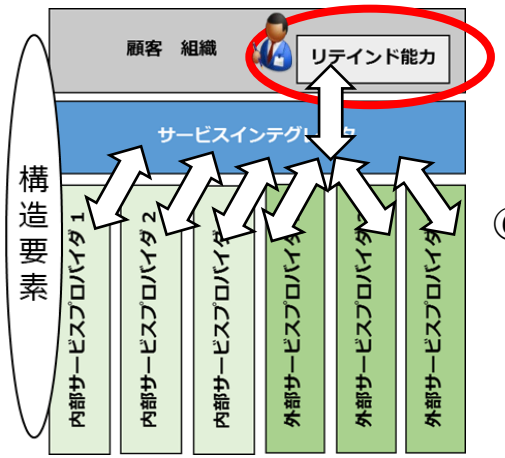
③　ITリスク

マルチソーシング環境全体にまたがるリスク（例　プロバイダの廃業によるサービス提供の中断、セキュリティ等）を分析し、リスク対策案を立案し、対策を実施し、レビュし、改善します。
一般に、SIや各プロバイダのリスクマネージャとのリスクガバナンス委員会を持ちます。

④　セキュリティやコンプライアンスのポリシーや標準　（詳細は6ページ）

セキュリティやコンプライアンス（法令準拠）のポリシーやガイドラインを定め、サービスインテグレータ(SI)や各プロバイダ群が業務遂行にあたりそれらに従っていることを確認することで、顧客・ビジネスや顧客データの安全を守ります。
このガバナンスが無いと、個々のサービスプロバイダが良かれと考える独自なやり方になり、セキュリティ事故につながります。
一般にSIやプロバイダのセキュリティマネージャなどとのセキュリティガバナンス委員会やセキュリティプロセスフォーラムを持ちます。

■ ガバナンスするべき８つの項目の概要（続き）



ガバナンス項目を展開し確認する

⑤　サービスポートフォリオ

サービスポートフォリオはサービスプロバイダから提供される個々のサービスやエンドツエンドサービスのカタログ一式です。ここには、新規の設計開発や、新たなサービスの契約など、リテインド能力が各プロバイダと契約或いは合意したサービスが載っています。ここに載るという事は顧客・ビジネス側が費用を払う事を承認していることになります。サービスポートフォリオマネージャがこのカタログリストの責任者となります。
顧客・ビジネス側は、このポートフォリオのリストを見て、求めるサービスを見付け、使いたいと要求していきます（ユーザ登録依頼）。

⑥　購買・契約・取引・予算とコスト

このSIAM™環境の予算管理を行います。⑧需要管理で定義したビジネス要求に基づき、サービスインテグレータの支援で候補プロバイダにRFPを出し、提案を求め、IT予算に基づく費用を交渉し、選定し、契約します。サービスを活用し、支払います。
使用時に請求されるコストに相応しいサービス価値であることを(SLAなどを見て）確認します。
プロバイダとの契約の中で、他のプロバイダと協調・協働することを求めます。SIに権限委譲していること、即ち、SIがそれをリテインド能力に成り代わってリードすることを明確にします。
なお、近年のDXな環境では、成果物を定義できないサービス開発が多々発生します。そのようなアジャイルな場合、いわゆる請負契約は結べないことがあり、工数ベースの契約になることもあり得ます。

⑦　サービスインテグレータのガバナンス

顧客・リテインド能力は個々のプロバイダと直に契約しますが同時に、SIとも契約します。リテインド能力は、SIが、サービスの設計開発、提供、運営改善においてプロバイダの協調や協働をリードしていることを確認します。或いは、リテインド能力が進める（①～⑧の）ガバナンスをリテインド能力に成り代わって進めることなどを確認し、SI契約価格を支払い、契約更新します。

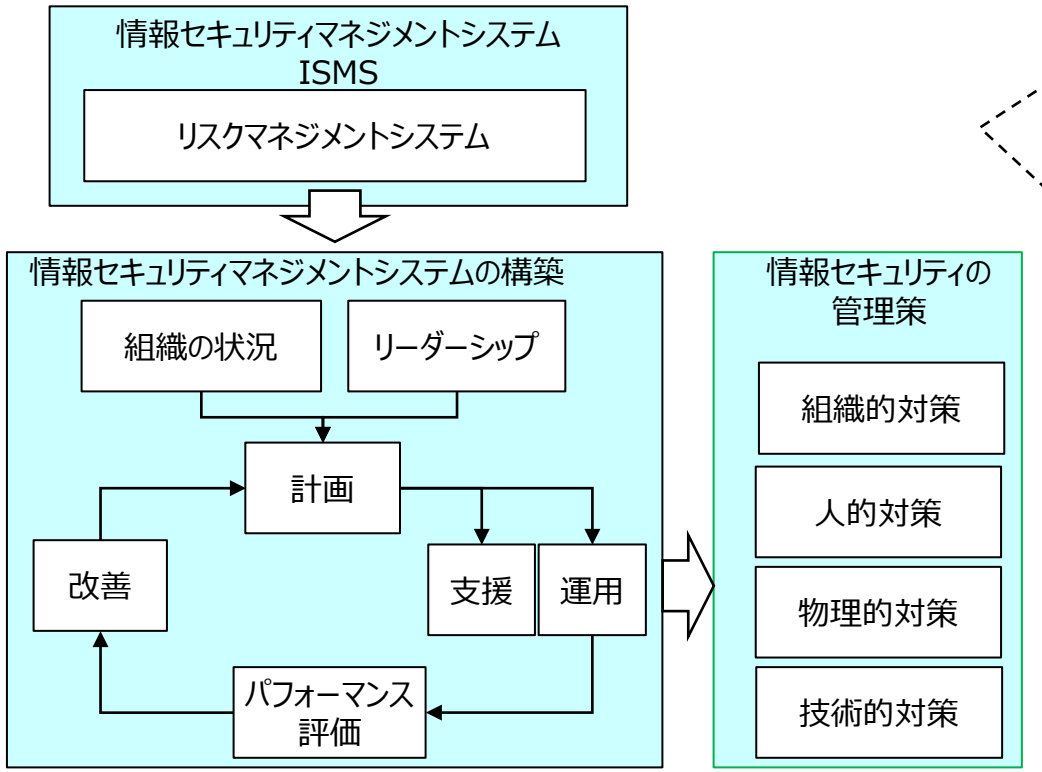
⑧　需要管理（デマンドマネジメント）

顧客・ビジネスの要求は、サービス供給によって満たされる必要があります。
顧客・ビジネス側の要求は関係者の集まりで検討され合意されたものがサービスに対する要求となってきます（お客様は神様であるとして、管理されない要求に全て対応しますと際限なくITコストがかかります）。またそれら合意されたサービスへの要求に対して適切なマルチソーシングによりサービス供給されなければなりません。このようなサービス供給には、新たなサービスの設計開発や既存サービスの入れ替えを含めたプロジェクト的な要求や、ユーザー登録削除のような標準的なサービス要求対応があります。

補足説明

④セキュリティのガバナンス　概要説明　(1/2)

セキュリティ事故の再発を防止し、信頼されるサービスを提供する為には、情報セキュリティマネジメントシステムをマルチソーシング環境に融合し、展開する必要があります。
現実のITの世界は複数の企業が絡んでいます。
ITの**セキュリティリスク**は、人的、物理的、技術的など様々な側面を持ちます。
そのような環境でのセキュリティ事故の再発防止は、一つだけの対策を一社に打つだけではすみません。
ISMSとSIAM™の融合が、効果的です。



セキュリティリスクの例

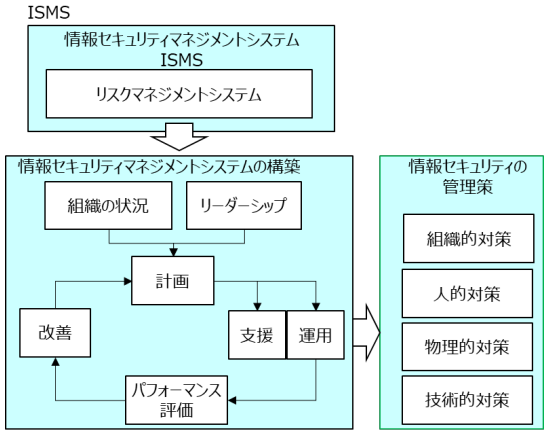
- ✓ 故意の破損、盗難
- ✓ 記憶媒体の不正使用
- ✓ ユーザIDの誤り
- ✓ 不正な方法でのシステム侵入
- ✓ 悪意のあるソフトウエアのアップロード
- ✓ フィッシング
- ✓ 停電、ハードウエア故障
- ✓ ネットワークの障害
- ✓ データ誤入力、誤削除、
- ✓ 供給者との合意におけるセキュリティ、など

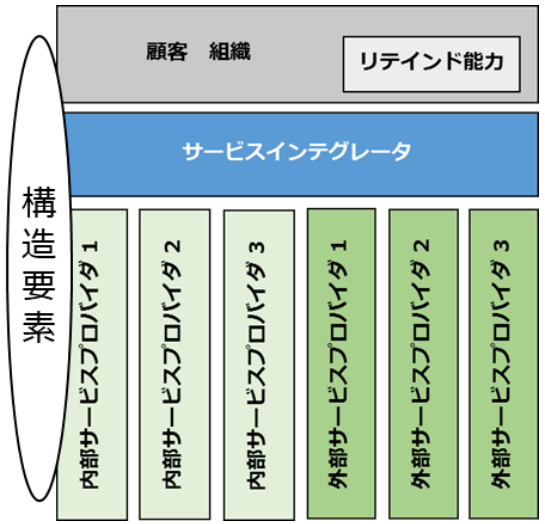
ISMS　ISO27001 情報セキュリティマネジメントシステム

補足説明

④ セキュリティのガバナンス　概要説明　(2/2)

情報セキュリティマネジメントシステムをマルチソーシング環境に展開





ISMSとSIAM™の融合

顧客・リテインド能力は求めるセキュリティポリシーやルール、ガイドラインを示します。
サービスインテグレータと複数のプロバイダはセキュリティ管理プロセスの中で、セキュリティリスクを洗い出し、対応し、セキュリティインシデントの解決と再発防止を実現します。

- **リテインド能力のセキュリティ責任者**が、**セキュリティポリシーやガイド**を定め表明します。
- **サービスインテグレータのセキュリティマネージャ**は、**各プロバイダのセキュリティマネージャ**と共に、全体の**リスク**を洗い出します。
- リスクに対する対策（**管理策**）を計画します（組織的、人的、物理的、技術的対策）。
- 各プロバイダは、プロバイダ内で展開します。
- 全メンバーに**教育**します。
- **セキュリティインシデント**が発生したらプロバイダはサービスインテグレータに報告し対処します。サービスインテグレータは必要に応じて他のプロバイダに展開します。
- 定期的（例　3か月毎）に、**リスク分析と対処策の更新**を行います。
- リテインド能力は、（SIに命じて）定期的（例　6か月毎）に環境全体を監査し、不適合があれば是正します。

ちょっと再確認

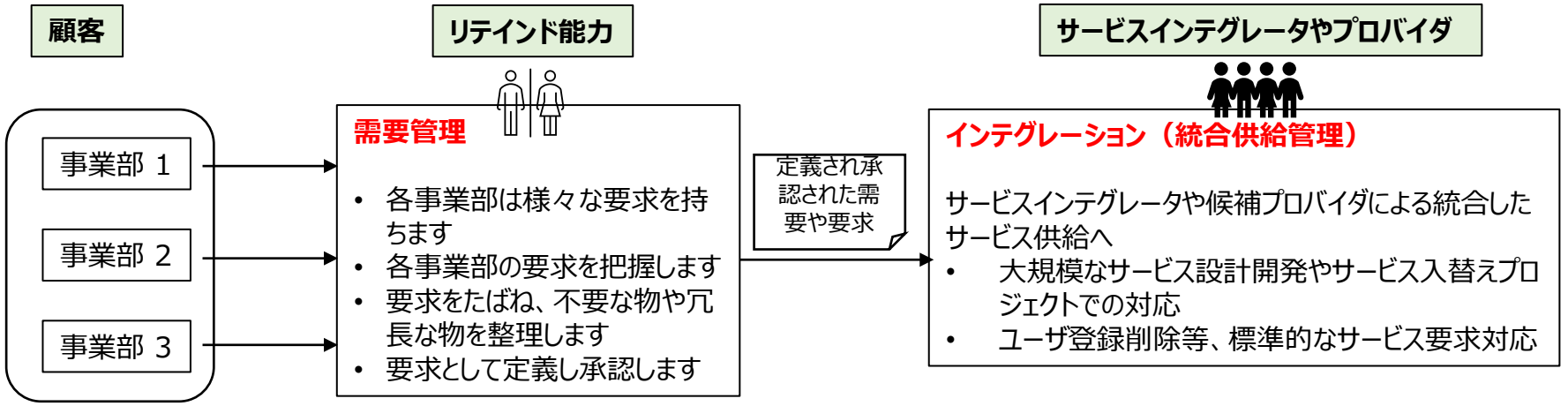
外部サービスプロバイダの場合、多くの顧客にサービスを提供しいている場合があります。
そのような場合、**全社がISMSの認証を受けていいたとして**も、**この顧客にサービスを提供する際**にどのようなセキュリティ管理を行うかは顧客向けに個別に計画し教育しないと、その範囲内の人たちは具体的にどうすればいいのか分かりません。全社の仕組みを**テーラリング**し、**この顧客向けのISMSを明確**にして、**教育する**必要があります。

補足説明
⑧ 需要管理（デマンドマネジメント）　概要説明

- ✓ SIAM™では、**顧客のビジネス要求を満たすべく、複数の適切なITサービスを、統合して提供**します　（**需要と供給**）。

- ✓ 需要管理とは、複数のビジネスから出るビジネス要求・ユーザ要求をきちんと把握し、評価し、承認し、予算を付けまることです。
  要求に無条件で対応しますとITコストがかかり続けます。声の大きいユーザの要求だけを聞いていると、他のユーザ要求に割く予算が無くなり、不公平になりかねません。
  需要は評価され管理されなくてはなりません。

- ✓ **需要管理**は、サービスインテグレータやサービスプロバイダのインテグレーション（**統合した供給管理**）と対になります。
  供給では、**大規模なサービス設計開発やサービス入替を含むプロジェクト対応**や、ユーザ登録削除等のような**標準的なサービス要求対応**があります。



IV.　リテインド能力の組織化

- **リテインド能力って組織なんですか？**
  リテインド能力はガバナンスと言う役割を果たす能力であり、SIAM™では前述の8項目を統治できる能力としています。

  これらを、**どのように組織化するか**は、その状況によります。

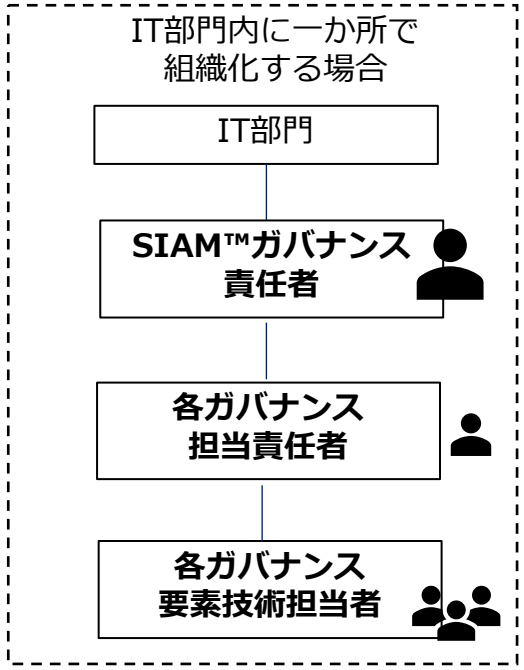
  状況例　ビジネス規模、複雑さ、プロバイダ数、ITサービス数と複雑さ、契約金額等

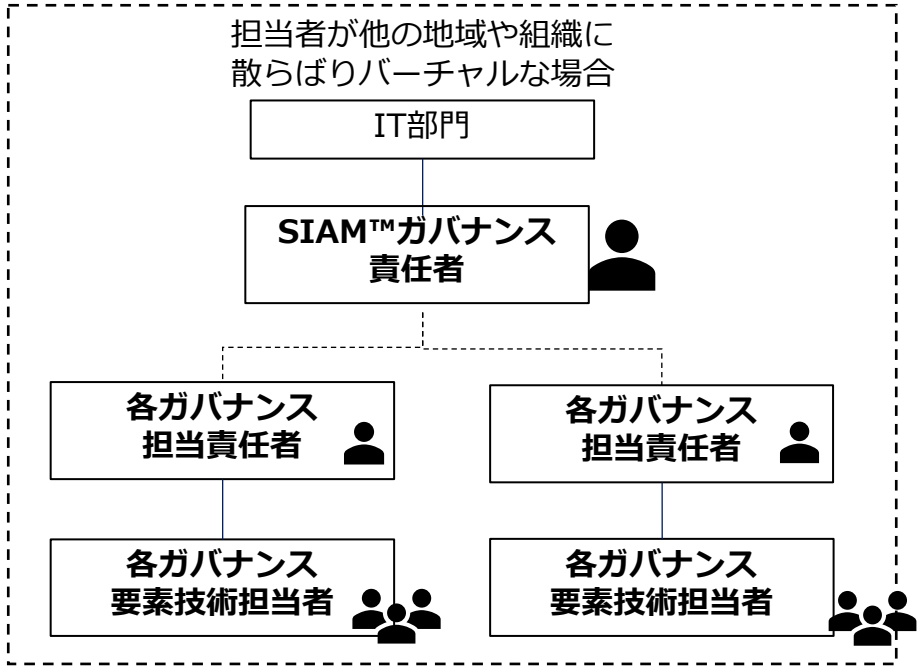
- 全体のガバナンス責任者（リテインド能力の長）を設けます。また各ガバナンス項目ごとに担当責任者を設けます。各担当責任者は、複数、又は一人です。他のガバナンス担当と兼任することも可能です。

- **リテインド能力は、アウトソースしないで自前で保持する**ものですが、要素技術担当は**外部の支援を得て**も良いものです。

  例　セキュリティのガバナンス責任者　：自前でリテインド能力内に用意。
  　　セキュリティの要素技術者　　：サービスインテグレータから支援を受ける、又は外部要員を契約する。

- **リテインド能力の組織化の例**





例

- ✓ A社では主に日本のIT部門にガバナンス責任者がいる
- ✓ セキュリティは、アメリカのITから担当責任者が全世界を見ている
- ✓ 需要管理は、それぞれヨーロッパ・アメリカ・アジア・日本のビジネスに対応して計4名の担当責任者がいる。4人は毎週需要管理ミーティングを開催し当月の要求を並べ、分析し、ビジネスに対する重要度や優先度、予算などを検討し、定義され承認された要求をまとめサービスインテグレータに提示している。

V.　リテインド能力の人材育成

- **リテインド能力の担当者の育成は、何を目指して、どのようにやればいいのでしょうか？**
  - ✓ 担当責任者の責任や目的・目標を明確にします。
  - ✓ 知識と経験を定義します。
  - ✓ 必要な**教育やOJT**を行います。
  - ✓ 各担当者同士のやり方を**シェアし、良いものは見習います**。

SIAM™ガバナンス
責任者

各ガバナンス
担当責任者

  - ✓ リテインド能力に必要なコンピテンシの例（コンピテンシ：知識・経験と実務能力）

顧客･ビジネスに関する知識 • ビジネスの狙いや競合や強化策を理解する • ビジネスプロセスを理解する • ビジネスに対するITの貢献を把握する • ビジネスのITに対する期待や要望を理解する	**IT（情報通信技術）に関する知識** • 最新の情報技術をウォッチする • 担当ガバナンスの為に役立つ技術を理解する 例　セキュリティ管理システムISMS クラウドコンピューティングサービス
外部プロバイダとの協調に関する知識 • 外部プロバイダとの契約方法と評価法を理解する • プロバイダのサービスを評価する • パフォーマンスが悪い時の改善策や、ペナルティ、契約終了を決断する • プロバイダとのwin winの関係を作る 例　SIAM™の知恵	**リーダシップ** • 担当ガバナンス項目の目的や目標を明らかにする 例　セキュリティポリシやルール、ガイド • サービスインテグレータやプロバイダからなる仮想的なチームをリードし担当するガバナンスを実現し維持する

ちょっと再確認

- ✓ このコンピテンシを全てのガバナンス担当者が備えることは困難です。
- ✓ これらのコンピテンシを、リテインド能力全体で備えるようにします（従って、チーム内でシェアし高め合う事が大事）
- ✓ これらをの表を参考に、各ガバナンス担当者ごとに必要なコンピテンシを定義し、職務記述化し、育成を計画します。

終わりに

複数のプロバイダ、特に外部プロバイダ環境では、「こうであってもらいたい」と言う方向性やルール、ガイドラインを明確にしておくことは、非常に重要です。

SIAM™では、リテインド能力をきちんとアサインし、ガバナンスの要件を明確にしましょう。

但し、全てを自分がやるのではなく、かなりの部分でサービスインテグレータに権限移譲し、自らは軽くします。

少しややこしい概念でもありますので、**同じリテインド能力の方々ともシェアし合い**、理解を深め、**ガバナンスプロセスを設計構築展開し、常に改善**しましょう。