クラウド利用者のための SaaSガバナンスの ベストプラクティス ～概説～

CASB WG　羽田 昌弘

登壇者 & 協力者 from CSA CASB WG

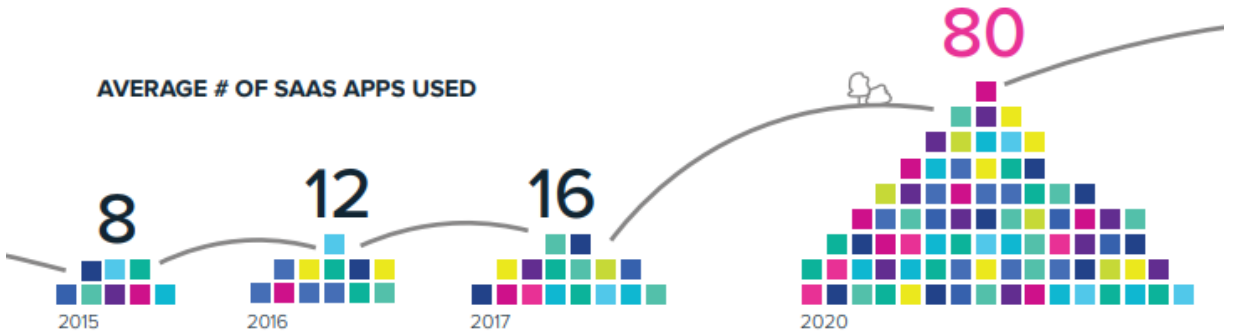
羽田 昌弘
セキュリティコンサルタント
CCSP, CCSK

根塚 昭憲
セキュリティソリューション技術者
CASB WG リーダー

小野 貴博
ユーザー企業IT技術者
CCSP, CCSK, CCAK

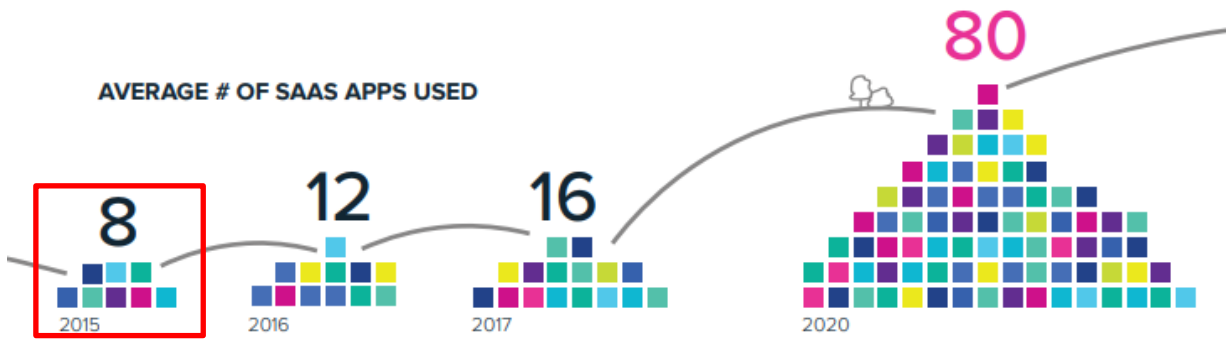
本講演内容は登壇者、協力者が所属する会社を代表する意見ではありません。

米国では1企業が利用するSaaSの数が5年間で10倍に増加した。



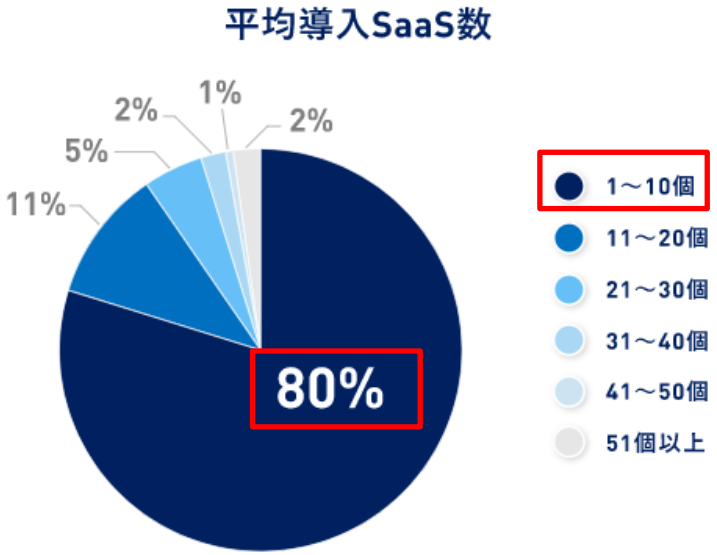
BetterCloud, 2020 State of SaaSOps (2020), p.12.

日本でも3年後くらいに2020年の米国と同等になるのではないか。



BetterCloud, 2020 State of SaaSOps (2020), p.12.

（全業界）利用SaaS数調査



株式会社メタップス,「コロナ期のSaaS導入変化でふり返る2020年」SaaS利用実態調査レポート (2020/12/29)

組織は様々なSaaSに合わせデータを保護しなければならない。
SaaSセキュリティはCSPに強く依存、そのレベルは様々である。

	IaaS/PaaS	SaaS
1企業が利用するCSP数	数社	数十～数百社
CSPのセキュリティ責任	狭い	広い
CSPのセキュリティ予算	潤沢	様々
CSPのセキュリティ人材	潤沢	様々

数少ないIaaS/PaaSだけでなく、数の多いSaaSも統制しましょう！

- 発行日：2022/6/8
- スコープ
  - **SaaS環境内のデータを保護**するための**SaaSガバナンスのベストプラクティス**の基準セット
  - SaaSの採用・利用**ライフサイクルに応じたリスク**を列挙・考察
  - SaaSの**利用者視点**での潜在的な**緩和策**
- 公開場所
  - 原文（cloudsecurityalliance.org/...）
  - 和訳（www.cloudsecurityalliance.jp/...）

本講演の背景と目的

- 背景
  - CASB WBで「クラウド利用者のためのSaaSガバナンスのベストプラクティス」を**読んでみた。**
  - 読み解くことが**難しい！**
  - Congressで**解説してはどうか？**
- 目的
  - 肝となる**序盤の理解**を助けること
  - SaaSガバナンスの改善のために、原文または日本語版を読む**きっかけ**となること

ここからは2～4章、13章を解説する。

解説済み	以降の解説範囲			
1. はじめに	2. 概要	3. 情報セキュリティポリシー	4. 情報セキュリティ組織	5. 資産管理
6. アクセス制御	7. 暗号化と鍵管理	8. 運用セキュリティ	9. ネットワークセキュリティ管理	10. サプライヤとの関係
11. インシデント管理	12. コンプライアンス	13. CASBの機能と展望	14. 結論	参考文献、定義、略語

概要

クラウド利用者のためのSaaSガバナンスのベストプラクティス

SaaSのセキュリティとガバナンスのためのアプローチ

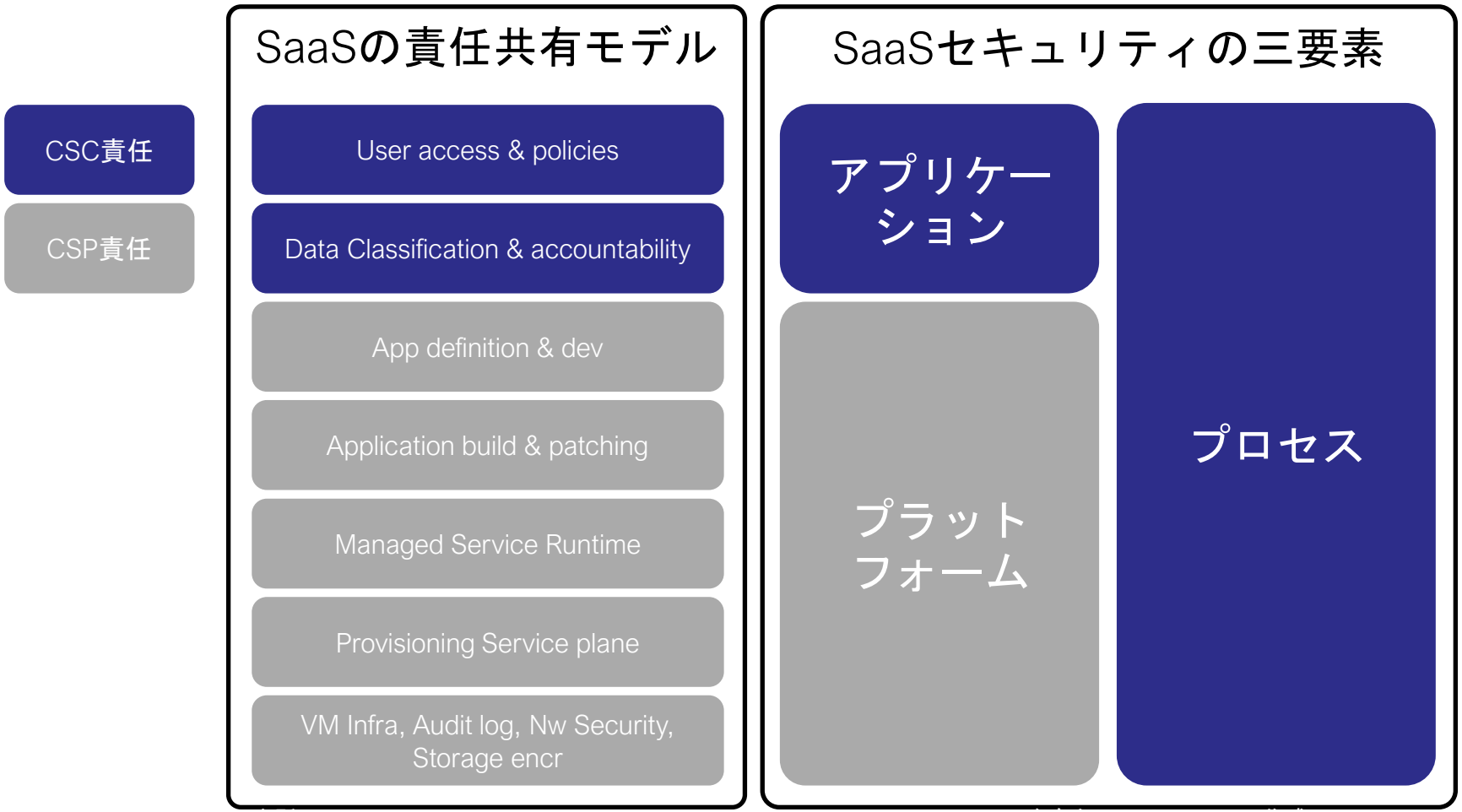
デューデリジェンスのステップ

1. SaaSの**用途と機能**を理解する。
2. どのような**データ**が保存されるか把握する。
3. **ユースケース**を把握する。

セキュリティアーキテクチャ構築ステップ

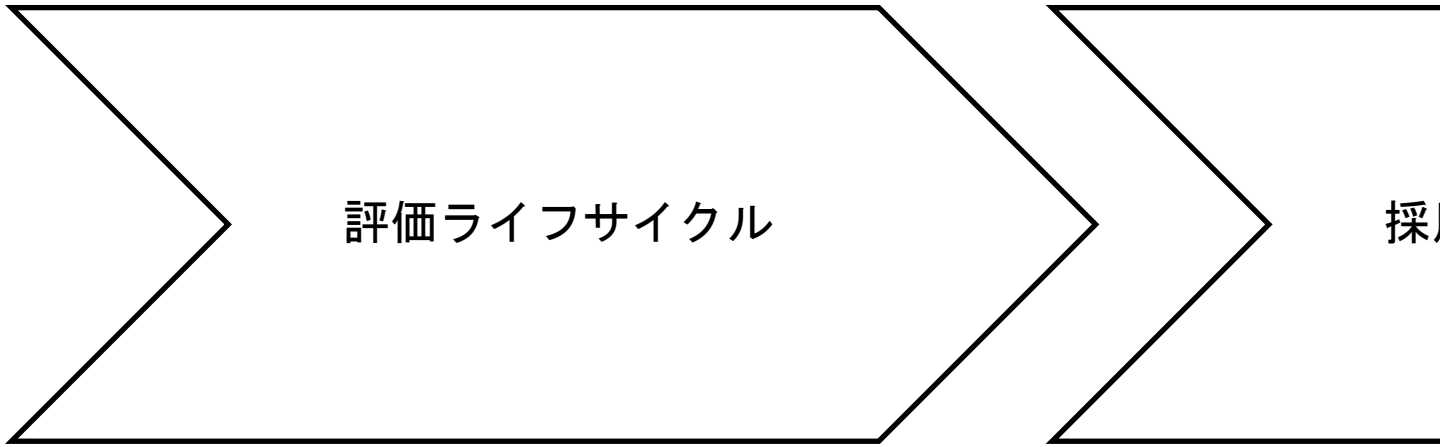
1. 情報セキュリティ**ポリシー**を策定する。
   - NIST CSFなどフレームワークを選定する。
   - 本書のベストプラクティスと組み合わせる。
2. 情報セキュリティ**組織**を組成する。
3. ガバナンスとセキュリティの**プロセス**を構築する。
4. プロセスを実現するための**技術**を導入する。

SaaSセキュリティの三要素



https://cloudsecurityalliance.org/blog/2021/02/04/the-evolution-of-cloud-computing-and-the-updated-shared-responsibility/

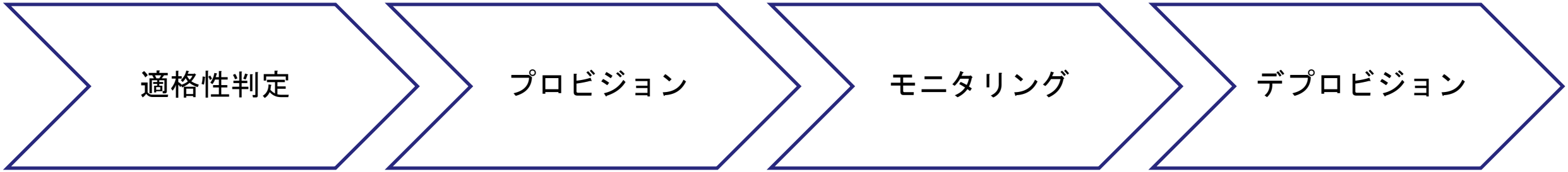
利用者は、SaaSを評価、採用、利用、利用終了する。



1.使用中サービスの把握
2.市場調査
3.パイロット評価
4.購買決定

1.正式評価
2.採用
3.利用（次頁で解説）
4.利用終了

利用サブライフサイクル



- このSaaSを利用する適格なユーザやエンティティか
- ユーザやエンティティへのIDや権限の付与
- ユーザやエンティティの挙動を監視
- ユーザやエンティティのID削除や権限はく奪

ベストプラクティスでは、利用のライフサイクルは評価と採用のライフサイクルと並列ですが、CASB WGでは採用ライフサイクルのサブライフサイクルと解釈しました。

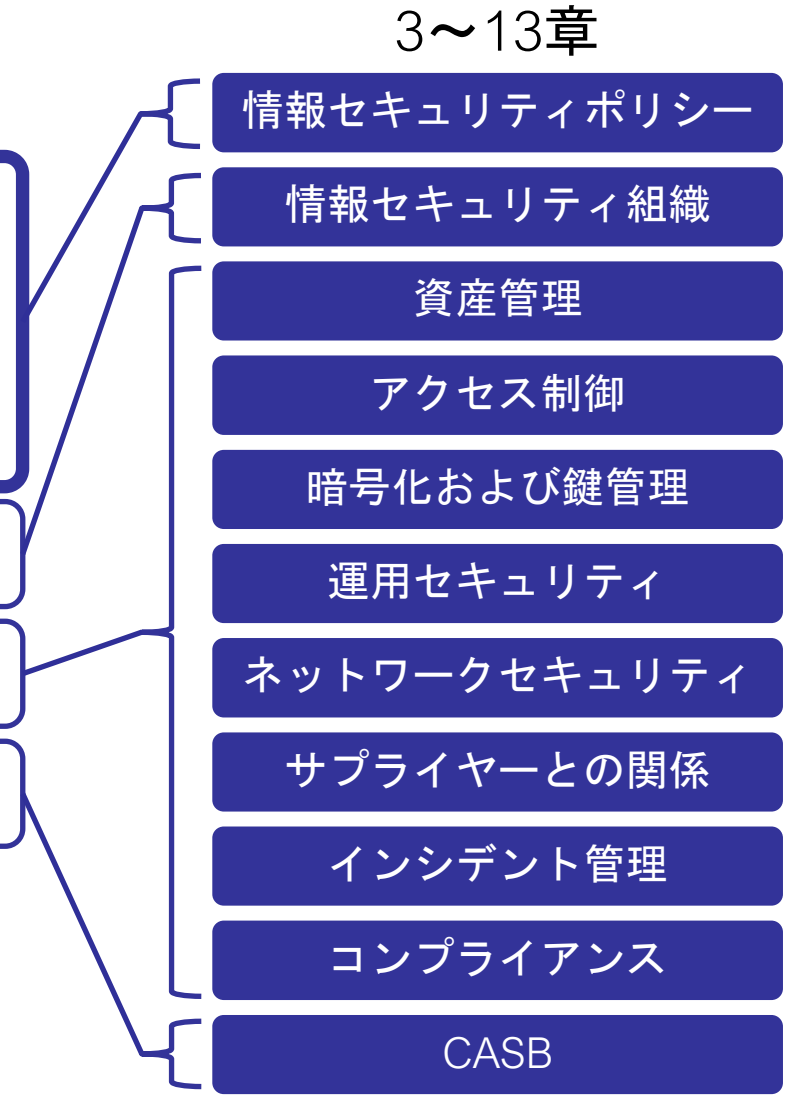
情報セキュリティポリシーの策定

クラウド利用者のためのSaaSガバナンスのベストプラクティス

セキュリティアーキテクチャ構築ステップと3〜13章

セキュリティアーキテクチャ構築ステップ

1. 情報セキュリティ**ポリシー**を策定する。
   - NIST CSFなどフレームワークを選定する。
   - 本書のベストプラクティスと組み合わせる。
2. 情報セキュリティ**組織**を組成する。
3. ガバナンスとセキュリティの**プロセス**を構築する。
4. プロセスを実現するための**技術**を導入する。



3章はポリシー策定ステップと定期的なポリシーの見直しを解説

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

- ポリシー
  - 評価
  - 利用
  - 契約解除
- ポリシーの見直し

3.1.1 評価（利用開始に向けた準備のステップ）｜ポリシー

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

1. 許容リスクの決定	SaaSを利用するにあたり組織が許容できるリスクを決定する。
2. セキュリティとプライバシーの要件	**組織のセキュリティとプライバシーの要件への適合をCSPに確認する。**
3. 要件の伝達	**組織のセキュリティとプライバシーの要件をCSPとの契約に反映する。**
4. 内部統制	セキュリティ戦略を策定し、セキュリティアーキテクチャを構築する。
5. サービス条件	**SLA、法規制対応など、サービスの前提条件をCSPと合意する。**
6. 影響を受けるデータ	法規制の影響を受けるデータ、影響、管理策を明確化する。
7. プライバシー	データ保存することによるプライバシーへの影響、管理策を明確化する。
8. 詳細なリスク評価のためのステップ	**リスクを特定し評価する前の準備を行う。**
9. リスクの特定	**ビジネス目標に支障をきたす可能性のあるリスクを特定する。**
10. リスクの評価	**特定されたリスクを定性的・定量的に評価する。**
11. リスクの管理	**リスク許容度に応じたリスク軽減策の実装、リスク移転、リスク受容を行う。**
12. レビュー・コントロール	内部/外部監査によりリスク分析を行う。
13. クラウドプロバイダー審査のベスプラ	組織がCSPを審査する体制や手順を準備する（ベストプラクティス）。
14. ポリシーとプロシージャの策定	SaaSの利用状況を継続的に評価・監視するためのポリシーと手順を策定する。
15. 構成とセキュリティ設定の管理	ベースライン構成の維持と設定変更を監視する。
16. データセキュリティ	機密データへのアクセスを監視する。
17. ユーザへの啓発とトレーニング	SaaS利用者に対し関係する対応を啓発したりトレーニングしたりする。
18. 内部脅威	内部者による脅威を分析し監視に活かす。
19. 外部脅威	外部者による脅威を分析し監視に活かす。

3.1.2 利用（利用中のリスクコントロール）｜ポリシー

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

- CSPの定期的なレビュー
- 監視
  - ユーザ視点の監視
  - 設定視点の監視
  - データ視点の監視
- 継続的な内部統制の評価と攻撃対象領域の低減

「クラウド利用者のためのSaaSガバナンスのベストプラクティス」の小見出しと一致しません。CASB WGにより整理し直しました。

3.1.3 契約解除（利用終了時のステップ）｜ポリシー

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

1.サービス終了のユーザ通知	サービス終了を全利用者に通知する（かつアクセスを停止する）。
2.外部サービス連携の解除	外部サービスとのAPIなどによる連携を解除する。
3.データの抽出と保管	データ、メタデータ、ログ、使用状況などのレポート、財務情報などを使用可能なフォーマットで抽出し、ロケーション要件に準拠し保管する。
4.データの破棄	バックアップ、残存データ/メタデータ/ログ/検索インデックスなどを確実に破棄されるようにする。
5.監視の解除	サービスのパフォーマンスやセキュリティなどの監視を解除する。
6.契約終了	CSPとの契約を終了させる。

「クラウド利用者のためのSaaSガバナンスのベストプラクティス」の小見出しと一致しません。CASB WGにより整理し直しました。

3.2 ポリシーの見直し | 情報セキュリティポリシー

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

- ポリシー
  - 評価
  - 利用
  - 契約解除
- ポリシーの見直し
  - ポリシーの定期的な見直しをする。
    - 追加のコントロールがないか
    - 組織の最低基準を満たしているか
  - CASBによるCSPの継続的なスコアリングに基づくアラートと動的アクセス制御

この節の本質はこちら

これはポリシーではなく技術の話

情報セキュリティ組織の組成

クラウド利用者のためのSaaSガバナンスのベストプラクティス

情報セキュリティ組織を組成するには何を考慮すればよいか

セキュリティアーキテクチャ構築ステップ

1. 情報セキュリティ**ポリシー**を策定する。
   - NIST CSFなどフレームワークを選定する。
   - 本書のベストプラクティスと組み合わせる。
2. 情報セキュリティ**組織**を組成する。
3. ガバナンスとセキュリティの**プロセス**を構築する。
4. プロセスを実現するための**技術**を導入する。

3～13章

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

4. 情報セキュリティ組織

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

- 内部組織
  - 情報セキュリティの役割と責任
  - 職務の分離
  - 当局との連絡
  - 専門研究グループとのコンタクト
- モバイル端末とテレワーク
  - モバイル端末のポリシー

- **本講演では4章の肝であるこの節を解説する。**

- 4章にあることに違和感
- COVID-19によりテレワークが組織に影響を与えたということでここにあると、1章から推察する。
- デバイス管理として別章にした方がよかったのではないか。

4.1 内部組織 | 情報セキュリティ組織

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

- **情報セキュリティの役割と責任**
  - CSCとCSPの**責任共有モデル**を理解する。
  - 大部分がCSPの責任だが、**CSCも一部の責任**を持つ。
  - **管理的また技術的な対策**により**CSPに依存するリスク**から資産を守る。
    (例　脆弱なTLSの使用禁止、AD認証の要求)
- **職務の分離（SoD）**
  - SoDとは重要な業務を**単独で実行不能**にすることである。
  - **最小権限の原則**によりクラウドリソースを保護する。
  - **容易に使い始めることができるクラウドの特徴**がSoDを複雑化し、制御不能にさせやすい。
- **当局との連絡**
  - SaaSを利用することに関する全ての**説明責任はCSCに残る。**
  - **インシデントや大きな変更**を主要な**関係者に通知するプロセスを文書化しCSPと共有**する。
- **専門研究グループとのコンタクト**
  - クラウドセキュリティリスクは日に日に急速に変化する。
  - 専門研究グループと関係を構築し**継続的に最新情報を追跡**する。

プロセスの構築

クラウド利用者のためのSaaSガバナンスのベストプラクティス

どんなプロセスをどう構築するとよいのか

セキュリティアーキテクチャ構築ステップ

1. 情報セキュリティ**ポリシー**を策定する。
   - NIST CSFなどフレームワークを選定する。
   - 本書のベストプラクティスと組み合わせる。
2. 情報セキュリティ**組織**を組成する。
3. ガバナンスとセキュリティの**プロセス**を構築する。
4. プロセスを実現するための**技術**を導入する。

3～13章

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

プロセスについて今後のCASB WGの活動にて解釈して参ります

プロセス

1. はじめに	2. 概要	3. 情報セキュリティポリシー	4. 情報セキュリティ組織	5. 資産管理
6. アクセス制御	7. 暗号化と鍵管理	8. 運用セキュリティ	9. ネットワークセキュリティ管理	10. サプライヤとの関係
11. インシデント管理	12. コンプライアンス	13. CASBの機能と展望	14. 結論	参考文献、定義、略語

技術の導入

クラウド利用者のためのSaaSガバナンスのベストプラクティス

情報セキュリティ組織を組成するには何を考慮すればよいか

セキュリティアーキテクチャ構築ステップ

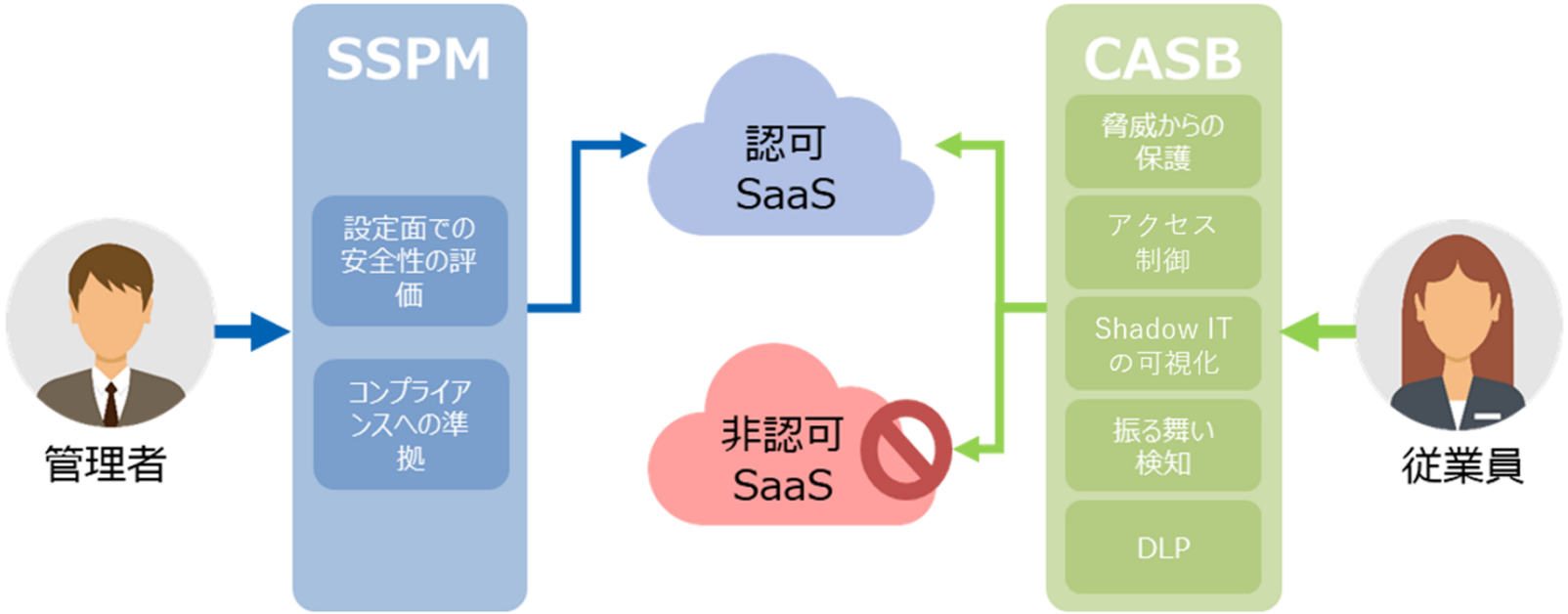
1. 情報セキュリティ**ポリシー**を策定する。
   - NIST CSFなどフレームワークを選定する。
   - 本書のベストプラクティスと組み合わせる。
2. 情報セキュリティ**組織**を組成する。
3. ガバナンスとセキュリティの**プロセス**を構築する。
4. プロセスを実現するための**技術**を導入する。

3～13章

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB

13. CASBの機能と展望

- 情報セキュリティポリシー
- 情報セキュリティ組織
- 資産管理
- アクセス制御
- 暗号化および鍵管理
- 運用セキュリティ
- ネットワークセキュリティ
- サプライヤーとの関係
- インシデント管理
- コンプライアンス
- CASB



※SSPM…SaaS Security Posture Management

Secure Service Edge (SSE)が含有する機能

SWG　ZTNA　RBI　FWaaS

HTTPSデコード　CASB　SSPM

本講演では1～4章、13章を解説しました。

1. はじめに	2. 概要	3. 情報セキュリティポリシー	4. 情報セキュリティ組織	5. 資産管理
6. アクセス制御	7. 暗号化と鍵管理	8. 運用セキュリティ	9. ネットワークセキュリティ管理	10. サプライヤとの関係
11. インシデント管理	12. コンプライアンス	13. CASBの機能と展望	14. 結論	参考文献、定義、略語

ご清聴ありがとうございました。

CSA「クラウド利用者のためのSaaSガバナンスのベストプラクティス」概説