増え続けるSaaSに対する セキュリティの備え

CASB WG　根塚 昭憲

登壇者 & 協力者 from CSA CASB WG

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

羽田 昌弘
セキュリティコンサルタント
CCSP, CCSK

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。

Agenda

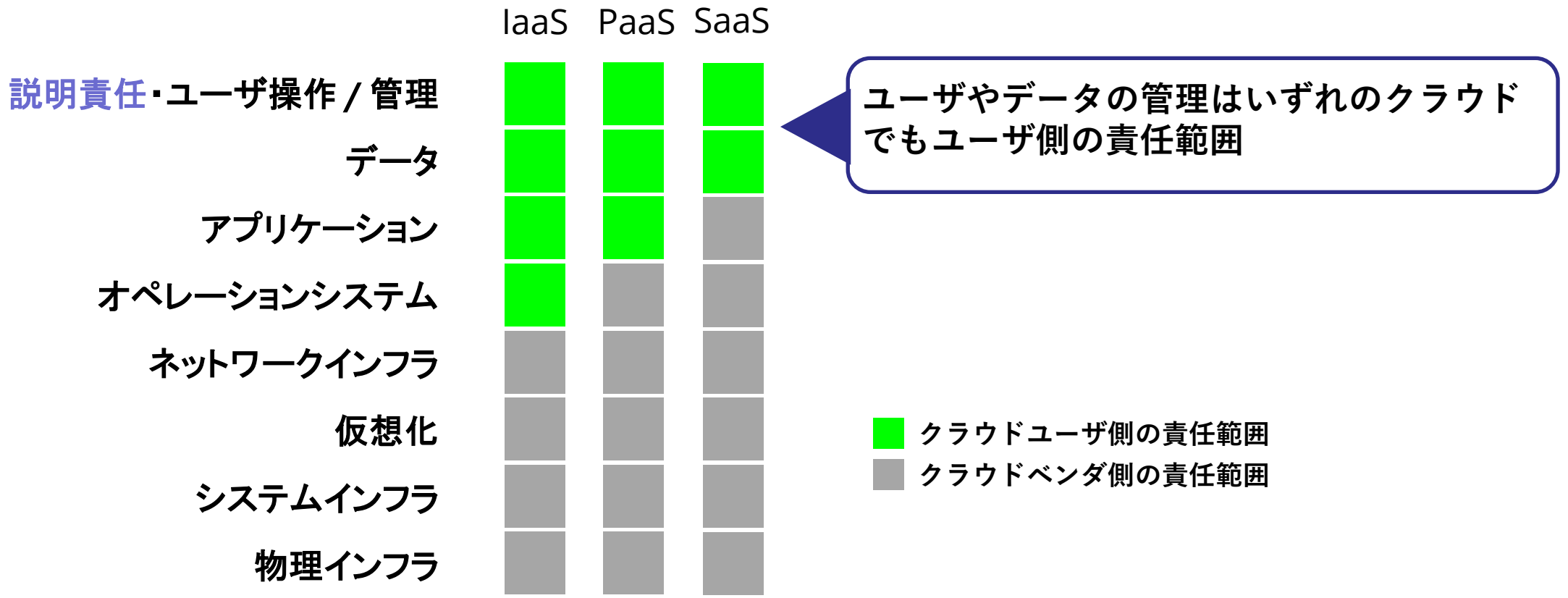
① SaaS セキュリティを取り巻く環境と参考資料のご紹介
② SaaSガバナンスのベストプラクティスの概説
③ CASBとSSPMについて
④ さいごに

① SaaS セキュリティを取り巻く環境と参考資料のご紹介

増え続けるSaaSに対するセキュリティの備え
CSA Japan CASB WG

SaaS 責任共有モデル

クラウド上の設定、ユーザの管理、データの管理、説明責任に関しては利用者側に責任（※）がある

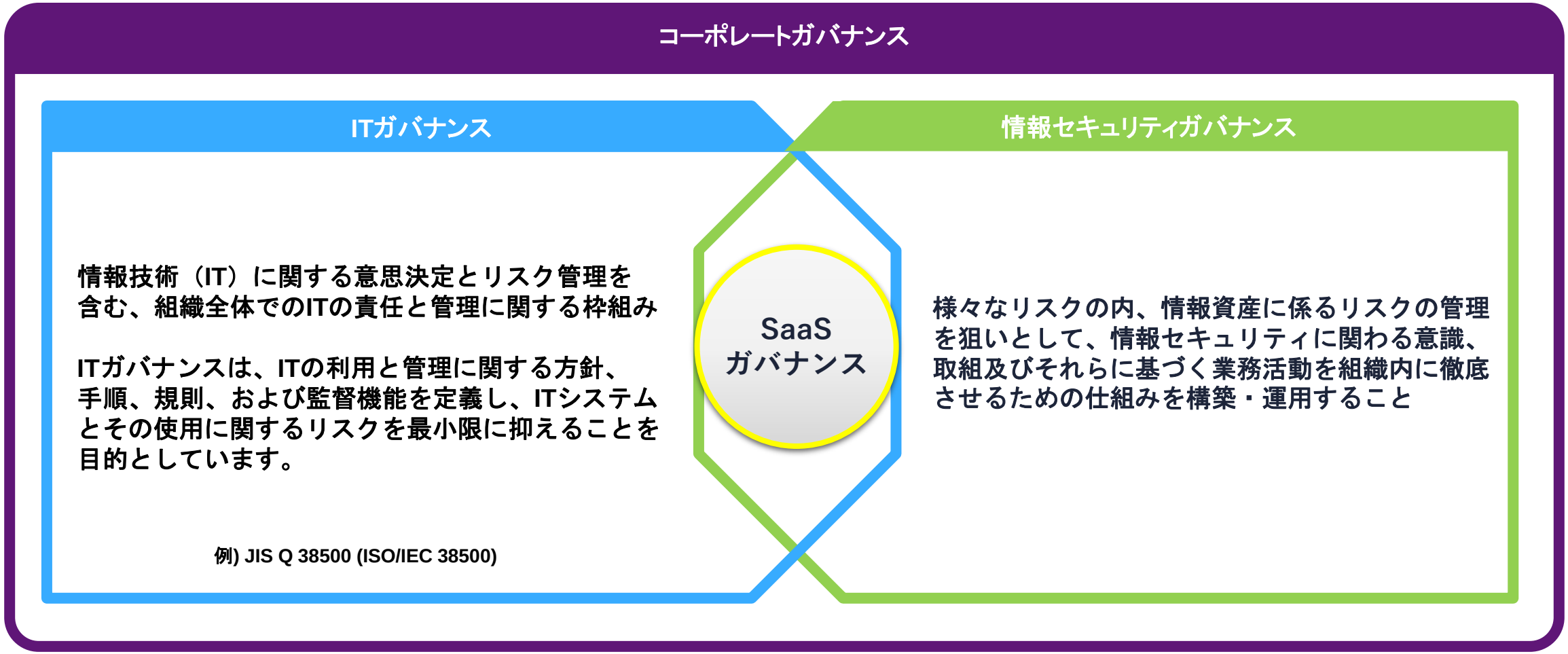


一般的な責任共有モデル

※事業者やサービスにより異なる可能性がありますので、各クラウドのご利用前に必ずご確認ください。

ガバナンスに関して

企業が健全な経営を行うための管理体制の構築、内部統制のこと



ガバナンスの欠如が引き起こすもの

ITガバナンスの欠如	情報セキュリティガバナンスの欠如
セキュリティリスクの増大	情報漏洩リスクの増大
リソースの浪費	セキュリティポリシーの不備
コンプライアンス違反	コンプライアンス違反
各プロジェクトへの影響	業務プロセスへの影響

企業価値の低下

セキュリティリスク増加　コスト増加　信頼性の低下

- 増え続けるSaaS利用数（1社平均：100以上※1）
- 広がり続けるSaaSエコシステム（次ページ）
- それぞれ異なるGUI・管理方法

SaaS利用における運用背景

- 各国の個人データ保護規制への対応
- ベンチマークに沿った設定管理の必要性
- 各SaaSの更新頻度に追い付けない

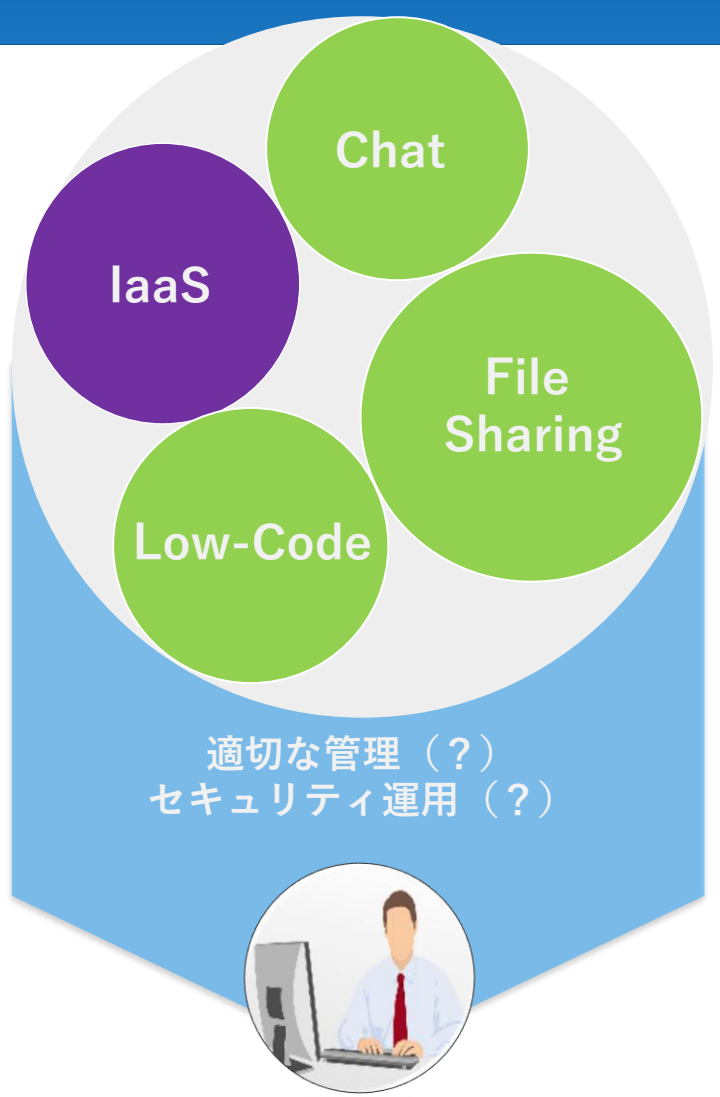
現在のSaaS運用・管理イメージ①

SaaS　IaaS/PaaS

企業・団体のIT管理者

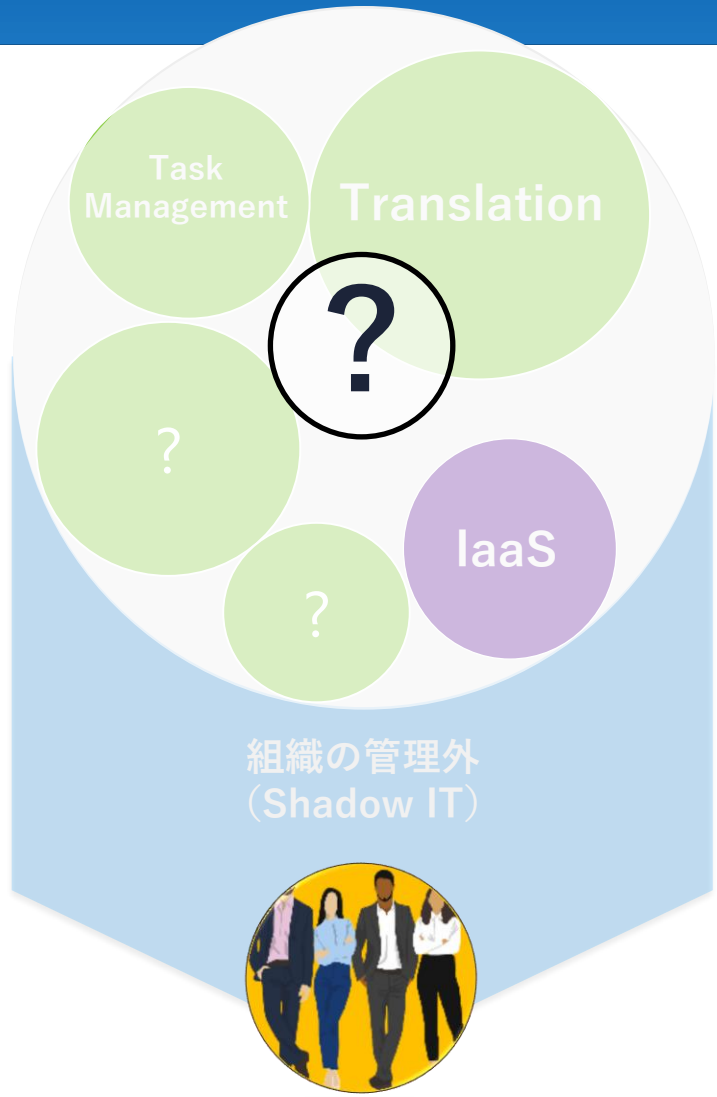
現在のSaaS運用・管理イメージ②

SaaS　IaaS/PaaS



事業部門

企業・団体のIT管理者



社員・職員

現在のSaaS運用・管理イメージ③

SaaS　IaaS/PaaS

データ連携
APIなど

Chat
IaaS
File Sharing
Low-Code

適切な管理（？）
セキュリティ運用（？）

事業部門

File Sharing
IDaaS
Chat
Web Meeting
IaaS
Mail
HR

適切な管理・セキュリティ運用
（サンクションIT）

企業・団体のIT管理者

？

Task Management
Translation
？
？
？
IaaS

組織の管理外
（Shadow IT）

社員・職員

数少ないIaaS/PaaSだけでなく、数の多いSaaSの統制が重要！

・**資料名**：SaaS Governance Best Practices for Cloud Customers（原文）
　　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（和訳）

・**発行日**：2022年6月8日（原文）

・**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：https://cloudsecurityalliance.org/
　　HOME > Research > Working Groups > SaaS Governance > Publications

　和訳：https://www.cloudsecurityalliance.jp/site/
　　TOP > 日本語資料集 > 4. CASB関連資料

② SaaSガバナンスのベストプラクティスの概説

増え続けるSaaSに対するセキュリティの備え
CSA Japan CASB WG

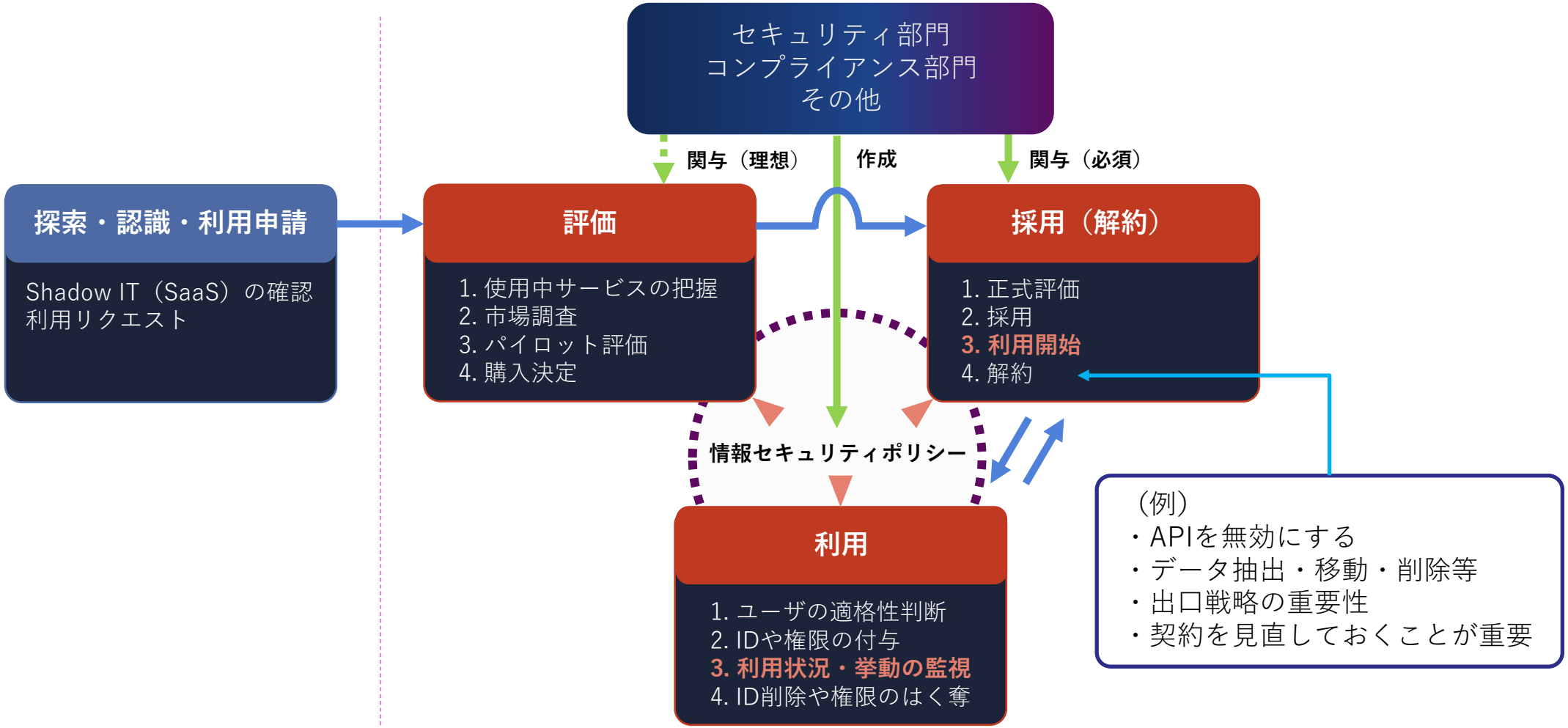
SaaSのセキュリティ運用管理がまとまっている数少ない参考資料

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 章立て

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

SaaS ライフサイクル

2章のまとめ



▶ ※Best Practiceの内容はここから

3章 1-1. 評価（利用開始に向けた準備のステップ）｜ポリシー

３章～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

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章 1-2, 1-3. 利用と契約解除（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

◆ 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

◆ 契約解除時のステップ↓

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。

4章 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。

5章　資産管理

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

◆　資産のインベントリ
- 利用しているSaaSを提示する。
- SaaSに転送されるデータの種類を提示する。
- 資産の所有権、許容できる資産の利用について提示する。
- 不要なSaaSやデータを判別可能な情報を提示する。

◆　資産のディスカバリ
- **利用されているSaaSを発見できるようにする。**

◆　資産の所有権
- SaaS上のデータの所有者を明確にする。
- SaaSの管理者を明確にする。

◆許容できる資産の利用
- CSPが許可されているデータに対する行為
- CSCが許可されているデータに対する行為

6章　アクセス制御

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

◆　アクセス制御のビジネス要件（アクセス制御ポリシー）
- ・利用者がリソースへアクセスする必要性を評価する
  - ・その必要性はビジネス要件と利用者の役割から妥当か
  - ・利用者はアクセスするデータの分類に対する適格性があるのか
- ・評価結果をデータの所有者が承認する

◆　**ユーザアクセス管理**
- **・ユーザ登録・解除**
- **・特権の管理**
- **・秘密認証情報の管理**
- **・ユーザアクセス権の見直し**
- **・アクセス権の削除または調整**
- **・ユーザアクセスの監視**

◆　**システムおよびアプリケーションのアクセス管理**
- ・情報アクセス制御
- ・安全なログオン手順
- ・パスワード管理システム
- ・特権的なユーティリティプログラム/サードパーティプラグインの使用に関する考慮事項
- ・プログラムのソースコードへのアクセス制御

7章　暗号化および鍵管理

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

◆ 転送データの暗号化
- TLS 1.2以上のプロトコルが提供されるか
- End-to-end暗号が提供されるか

◆ 保存データの暗号化
- まずはデータ流出に関するBIA（ビジネスインパクト解析）
- ディスク全体/ファイルベースの暗号化の必要性
- バックアップデータの暗号化
- 提供される暗号化のアルゴリズムと鍵長は十分な強度か

◆ CSC管理鍵暗号かぎとCSP管理暗号鍵
- 保存データの機密性はいかに
- CSPの鍵作成と管理方法への不安
- 自組織の鍵管理能力は十分か

◆ 今後検討すべき分野
- HSMaaS
- プライバシー拡張暗号（PEC）方式
- 準同型暗号
- コンフィデンシャル・コンピューティング
- ポスト量子暗号（PQC）方式

8章　運用セキュリティ

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. 運用手順に関するCSCの責任
   - 各SaaSを組織内でどう使うか把握し、運用手順を文書化することが重要

<主な項目>
- アクセス制御 (6章参照)
- SaaSを含めた変更管理プロセス
  - SaaSの機能変更による影響を評価
  - 将来、組織内で利用が広がる可能性
- ユーザー数などのキャパシティ管理
  - 利用拡大前に費用などの影響を考慮
- 本番データと本番環境の保護
  - CSPの開発に本番データを使わない
  - **本番環境の設定が安全か継続評価**
- SaaSの解約 (3.1.3章参照)

2. マルウェアからの保護
- アップロードを中心に脅威分析
- CSPが提供する機能の理解と活用

3. バックアップと高可用性
- 標準機能やAPIによるデータ削除は、CSC責任のため、対策が必要
- 過信せず、SaaS停止時の対策を用意

4. ログ出力と監視
- **CSP提供のログに利用が制限（内容、形式、ログ出力までの時差）**
- **監査ログで、SaaSの環境変更を監視**

5. 技術的脆弱性の管理
- 各SaaSの管理者と役割分担の明確化
- **設定のベストプラクティスに準拠**

6. CSPの情報システムの監査
- 業界標準への準拠をCSPと事前合意

9章　ネットワークセキュリティマネジメント

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

◆ SaaSプロバイダのネットワーク制御
・利用者は有効な証明書を使われていることを確認すること
・サービスコンポーネント間でどの程度まで暗号化が利用されているか確認すること

◆ 利用者ネットワークの管理策
・TLS 1.2以上の暗号通信の利用
・CASBを利用したテナント制御
・データ漏洩対策（DLP）
・SaaSまでのインターネット回線の冗長、キャパシティプランニングによる可用性の考慮
・Protective DNSの利用
↑
利用者が直接アクセスする場合も考慮に入れる
（ローカルブレイクアウト、自宅からのアクセス）
↑
SASEモデルを導入することでこれらを促進

10章　サプライヤーとの関係

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

◆ サプライヤーとの関係における情報セキュリティ
- 実際にはサプライヤーが提供するものは、別のIaaSやPaaSなどの上で動作している
- CSPと契約条件を交渉することも検討
- 外部認証制度は、リスクマネジメントの分析・判断に役立つが、それだけに依存するべきではない。

◆ 第三者リスク管理方針
- 事業運営の一部を他社に依存している企業はサードパーティーリスクマネジメントポリシーを導入する必要がある

◆ 契約によるセキュリティ対応
- 個々の契約書の作成が櫃世になるケースもある
  - 可用性以外のSLAの合意 / 侵入テスト結果の要求 / データセンタの新規立地に関する諸要件など

◆ 外部認証
- SaaS利用者がCSPのセキュリティを評価する際に利用できる報告書・証明書

包括的：米国公認会計士協会（AICPA） →　SOC 2
　　国際標準化機構（ISO）／国際電気標準会議（IEC） → ISO/IEC-27001
政府系：米国 → FedRAMP、EU　→　GDPR
クラウド：Cloud Security Alliance → STAR認証

11章　インシデント管理

- 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

◆ クラウドインシデント対応の詳細と各フェーズについて
・CSA Cloud Incident Response Frameworkの参照を推奨

◆ SaaSインシデントレスポンスの責任と手順
・責任共有モデルの理解
・契約上の合意も必要（議論の促進にはCAIQを活用することが可能）
・セキュリティ及び非セキュリティインシデントに関するサービスレベル合意書は契約書を通じて合意が必要

準備	・リスク分析 ・サプライチェーンリスクと事業目的の継続性（機密性、完全性、可用性）の観点から理解すること ・ステークホルダーのリストを文書化 ・SaaSに特化したプレイブックの準備
検出と解析	・IDプロバイダのシグナルやSaaSのアクセスログを活用、監視 ・データの流出、偵察活動の検知 ・SIEMなどを利用した自動化 ・サポートを受ける
封じ込め/根絶/回復	・発信元IPに基づくテナントへのアクセス制限 ・ユーザやアカウントのアクセス権の取り消し ・CSPに必要なサポートを依頼、CSCのデータバックアップと復旧計画を発動させることが重要
事後分析	・イベントの検出は間に合ったのか、それとも改善できるのか？(メトリクスとログ) ・ベンダーから必要なサポートが得られたか？(契約/SLA) ・ステークホルダーに適切なタイミングで情報を提供したか？（コンプライアンスとコミュニケーション） ・情報共有や連携の指針として、CSA Cloud Incident Response Frameworkの第6章が参考になる

12章　コンプライアンス

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

◆　セキュリティポリシーと標準へのコンプライアンス
- 機微なデータを扱うSaaSは、オンプレと同じ厳しさで評価すること
  - 社内外の関連するセキュリティポリシーや標準に対して評価
  - 扱うデータの種類や秘密度、リスク要因で、SaaSをカテゴリー分類
  - 重要なデータを扱い、かつ、外部公開しているSaaSは要注意
- 都度評価より、自動化された継続的なモニタリングシステムを導入
- 契約段階でデータ保持期間を交渉し、SaaS起因のリスクを低減
  - 処理済のデータが、いつSaaSから完全に削除されるか

◆　法律や契約上の要求事項へのコンプライアンス
- サプライヤー契約を通した対応 (10.1.2章参照)
- CSPの諸条件を理解し、第三者が自組織のデータにアクセスする可能性を把握

◆　**情報セキュリティのレビュー**
- **レビューの中で、SaaSのインベントリーや、未認可SaaSの利用状況も確認**

13章と各セキュリティツールの整理

- 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

背景

複雑性の増加

・増え続けるSaaS利用数
・広がり続けるSaaSエコシステム
・それぞれ異なるGUI・管理方法
・ついていけない更新頻度

基準/コンプライアンス

・個人データ保護規制への対応
・業界基準に則った設定/運用

SaaS経由インシデント

・Shadow ITの利用
・セキュリティの低いSaaS利用
・設定ミス
・サプライチェーン

課題

ガバナンス

・方針、基準、監督機能の強化
・情報資産に係るリスク管理
・サプライチェーンリスク管理
・費用対効果

セキュリティ運用

・脅威からの保護
・情報漏洩
・ID管理
・内部不正対策

可視性の欠如

・SaaS利用状況
・SaaSの設定
・SaaS間の連携
・利用者の権限

対策

利用SaaSの可視化/監視

・ログなどから利用SaaSを可視化
・SaaSセキュリティレベルの調査
・不正なユーザ操作を監視
・重要データの漏洩防止対策

操作制御や脅威防御

・ユーザ操作の制御
・ファイル解析(マルウェア)
・ファイル解析(DLP)

SaaS設定の可視化/監査

・業界基準に沿った設定にする
・定期的に監査する

ID/アクセス管理の強化

・MFA
・SSO
・権限管理

ソリューション

CASB
SSPM
UEBA
DLP
SSE (Secure Service Edge)
IAM(IDaaS)/IGA※1
TPRM※2

※1 Identity Governance & Administration
※2 Third Party Risk Management

実際に起こりうるSaaSのセキュリティリスク・インシデント

SaaSからの情報漏洩インシデント事例、以下はごく一部

発生年/ 影響を受けた企業	対象クラウド	クラウド 分類	認可・非認可	インシデント 原因	詳細
2018年/ 地方市役所	フリーメール	SaaS	非認可	不正アクセス	業務ルール上禁止されていた、個人アカウントのフリーメールを業務で利用していたところ、アカウントが不正アクセスを受け、約2,400件の個人情報が漏洩
2019年/ SaaS利用者	ファイル送信サービス	SaaS	認可・非認可	不正アクセス	このファイル送信サービスでは、サーバの脆弱性をついた不正アクセスにより利用者約480万人分のメールアドレスとパスワード、生年月日、氏名、性別などが流出していたことが報告される。この件では流出したパスワードが暗号化もハッシュ化もしていない平文のままだったこともあり、被害が拡大する恐れがありました。
2020年/ 対象SaaS利用企業	某CRMサービス	SaaS	認可	設定ミス	システムアップデートに伴い変更されたアクセス権限が影響し、個人情報に第三者がアクセスできていたことから、不正アクセスが相次ぎ発生。アクセスできていた期間も5年以上と長く、大きな問題となった
2022年/ 製造大手企業	コード管理サービス	SaaS	N/A	委託先	Webサイト開発を委託された企業が、運用規則に違反して、誤ってソースコードの一部を公開設定のままアップロードしたことが原因で、メールアドレスと顧客番号が漏洩するリスクが存在していた

【考えられる原因】

Shadow ITの利用

セキュリティの低いSaaSの利用

設定ミス

サプライチェーンリスク

③ CASBとSSPMについて

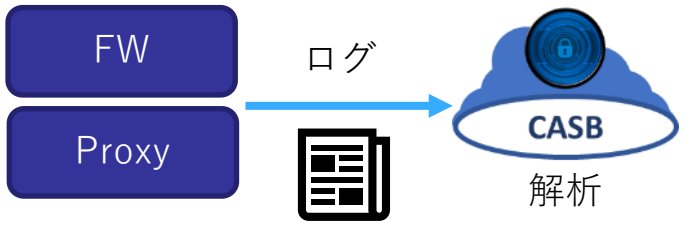
増え続けるSaaSに対するセキュリティの備え
CSA Japan CASB WG

Cloud Access Security Broker 概要

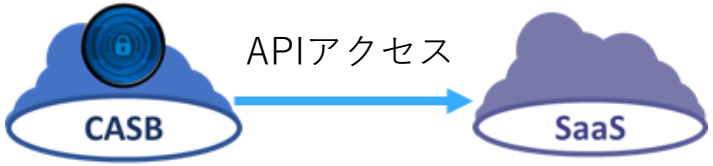
主な構成は以下の３つ。SaaSセキュリティを強化する様々な機能を提供する。

導入構成

1.ログアップロード



2.API利用



3.インライン構成(+SWG)

提供機能※

- 各SaaSのセキュリティスコアチェック
- SaaS利用状況の可視化（誰が？どこに？どのくらい？）
- 特定データの検知（DLP）

APIの場合、制御（ブロックなど）は
後追いとなり、ニアリアルタイムでの動作

- 脅威からの保護(ファイル解析)
- 特定データの制御(DLP)
- 細かいアクセス・操作制御

※ベンダーにより提供できる機能に差異あり

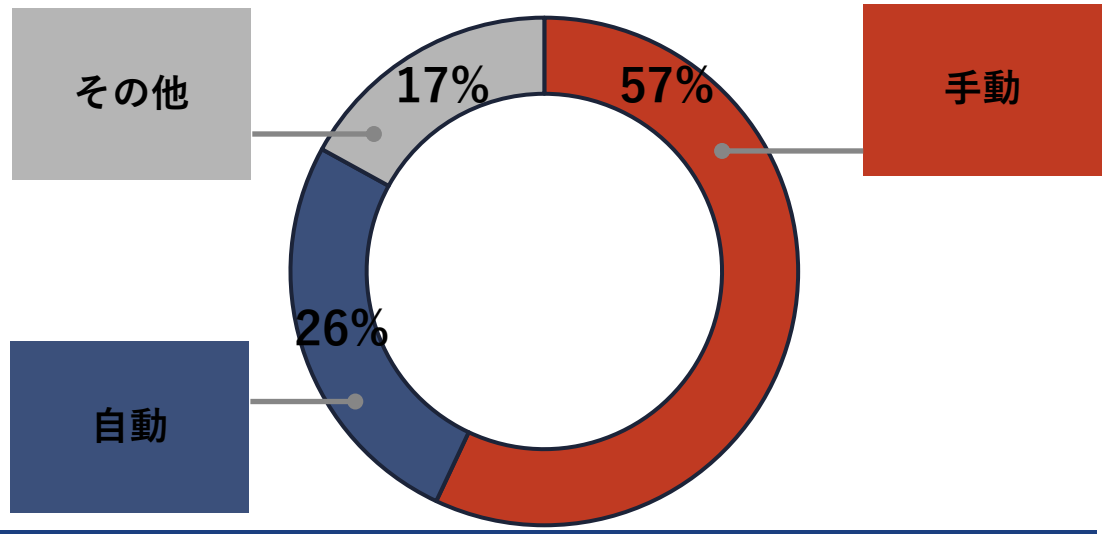
SaaS Security Posture Management 概要①

SaaS設定チェックの周期※
（340人のIT/セキュリティ担当者からの回答）

無	年	四半期	月	週	日	継続
5%	13%	15%	18%	24%	14%	10%

約半分の企業が月一回以下の設定チェック頻度

SaaS設定チェックの手法※
（340人のIT/セキュリティ担当者からの回答）

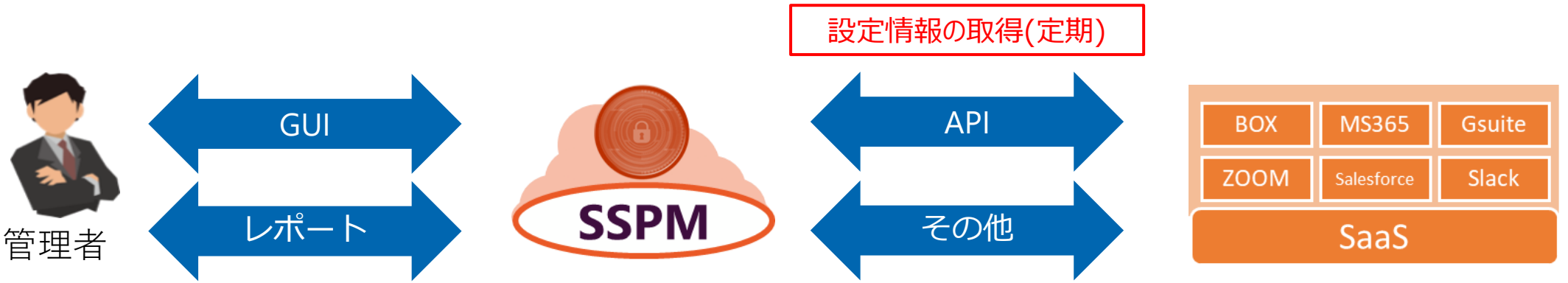


企業が利用するクラウドサービス数が急増し、それに伴い多数のクラウドアカウントや設定が必要になっている。
このような膨大な数の設定を定期的に、人手で管理することは困難であり、設定不備によるセキュリティリスクも増大している。
このような背景から、クラウドサービスのセキュリティ設定やポリシーに則り、自動化された監視・分析を行うことで、適切な設定に準拠しているかどうかを確認するためのツールとして**SSPM**が開発された。

※ クラウドセキュリティアライアンス、「2022 SaaS Security Report」、2022年

SaaS Security Posture Management 概要②

SSPM(SaaS Security Posture Management)の仕組みと機能(※1)



提供する機能(※2)

監査

各種のセキュリティスタンダード(※3)を元にした設定診断項目を提供、設定の定期監視

検出した設定ミスの影響、脅威レベル、改善方法を提示

対応

利用SaaSの現在のセキュリティリスク、コンプライアンス違反を可視化、スコア化

SaaS to SaaS連携（SaaSエコシステム）の可視化

可視化

※1 CASBの一部の機能として同等の機能を提供するベンダも存在
※2 ベンダーにより提供できる機能に差異あり
※3 SOC2, CIS, ISO/IEC 27001等

④ さいごに

増え続けるSaaSに対するセキュリティの備え
CSA Japan CASB WG

まとめ：SaaSに対するセキュリティの備え

戦略・ポリシー

・ITガバナンス
・情報セキュリティガバナンス
・各種ベンチマーク
←SaaS Governance Best Practice の参照

組織・人材

・責任共有モデルの理解
・SaaSセキュリティ体制の構築
・職務分掌（SoD）
・当局や専門家とのコンタクト

SaaS セキュリティ 強化促進

・ネットワーク
・エンドポイント
・ログ管理
・IAM / IDaaS / IGA
・SASE / SSE / CASB / SSPM / DLP / TPRM / ZTNA
・IaaS / PaaS / SaaS

インフラ・ツール

・資産管理
・アクセス制御
・暗号化と鍵管理
・各種運用・監視・監査
・ネットワーク
・インシデント対応
・コンプライアンス

プロセス・評価

CSAJC cloud security alliance Japan Chapter

是非、ご参考ください

・**資料名**：SaaS Governance Best Practices for Cloud Customers（原文）
　　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（和訳）

・**発行日**：2022年6月8日（原文）

・**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：https://cloudsecurityalliance.org/
　　HOME > Research > Working Groups > SaaS Governance > Publications

　和訳：https://www.cloudsecurityalliance.jp/site/
　　TOP > 日本語資料集 > 4. CASB関連資料

ご清聴ありがとうございました。

増え続けるSaaSに対するセキュリティの備え
CSA Japan CASB WG