金融業界のための SaaSセキュリティ対策：

- SSPMによる可視化とガバナンス強化 -

東京エレクトロン デバイス株式会社

CNビジネス開発室

小野瀬　翼

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

自己紹介

TOKYO ELECTRON DEVICE LIMITED

小野瀬　翼

Tsubasa Onose

入社	2021年入社
経歴	NW系SE → 新規商材立ち上げ等
趣味	旅行、自然散策
特技	ブラインドテイスティング（と言いたい）
業務内容	SaaSセキュリティ製品の啓蒙・拡販
メッセージ	話し掛けやすい雰囲気と言われます。 雑談や相談がとても好きなので お気軽にお声掛けください。 本日はよろしくお願いします！

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

はじめに：目次

1 金融機関におけるクラウドサービスの利用状況と利用上の課題

2 金融分野におけるサイバーセキュリティに関するガイドライン

3 SaaS利用における課題と対処

4 SSPMの基本概念と選定ポイント

5 Valence Security社について

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融機関におけるクラウドサービスの利用状況と利用上の課題

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融機関におけるクラウドサービスの利用状況と利用上の課題について

■ **日本銀行が実施した「クラウドサービスの利用状況等に関するアンケート」の調査結果**

- 2023年4月から5月にかけて実施
- 取引先金融機関のうち155先を対象
- “金融システムレポート”を補完するもの

■ **金融機関が今後のクラウドの利活用を検討していくうえで、金融業界におけるクラウド利用の現状と課題、リスク管理上の論点などを整理したもの**

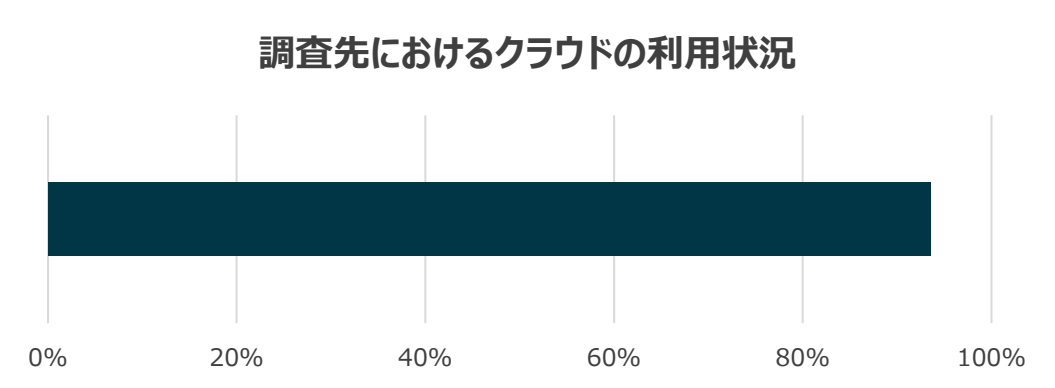
2025年8月時点での
現状把握と整理・振り返り

※日本銀行金融機構局 -「金融機関におけるクラウドサービスの利用状況と利用上の課題について - アンケート調査結果から -」（令和6年1月30日）- https://www.boj.or.jp/research/brp/fsr/data/fsrb240130a.pdf

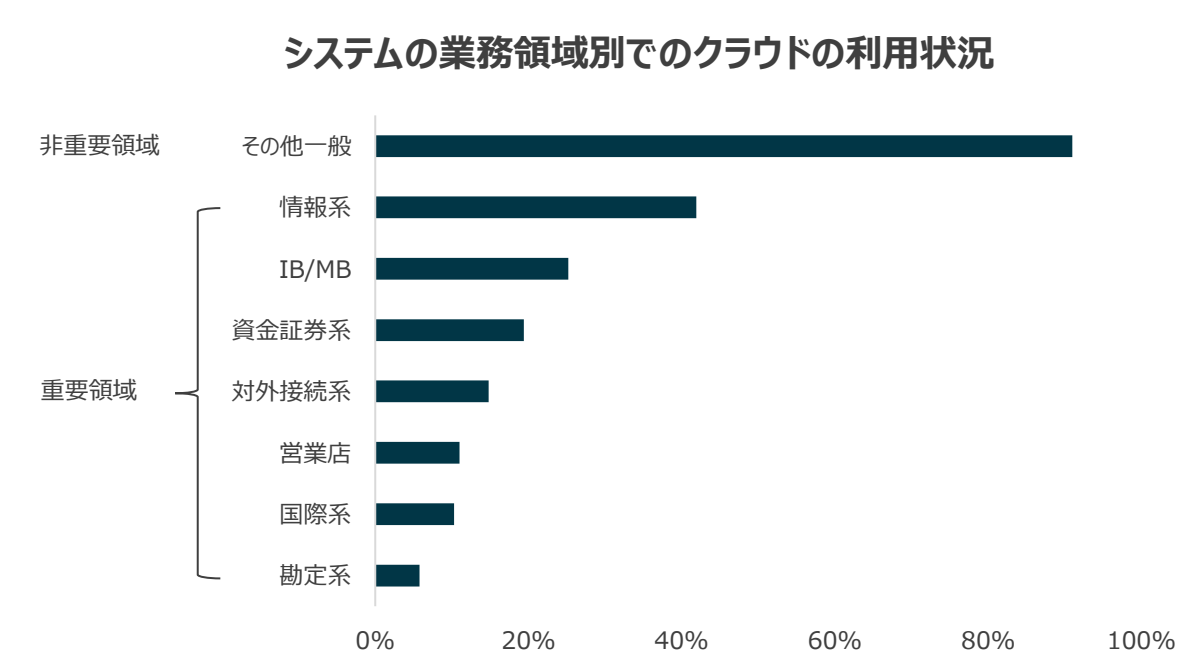
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融機関におけるクラウドサービスの利用状況と利用上の課題について

- ９割超の調査先が既にクラウドを利用
- システムの業務領域別にみると、顧客情報や決済業務に直接関連しない”その他一般システム（非重要領域）”では、**<u>９割以上が利用</u>**



93.5%が既に利用中

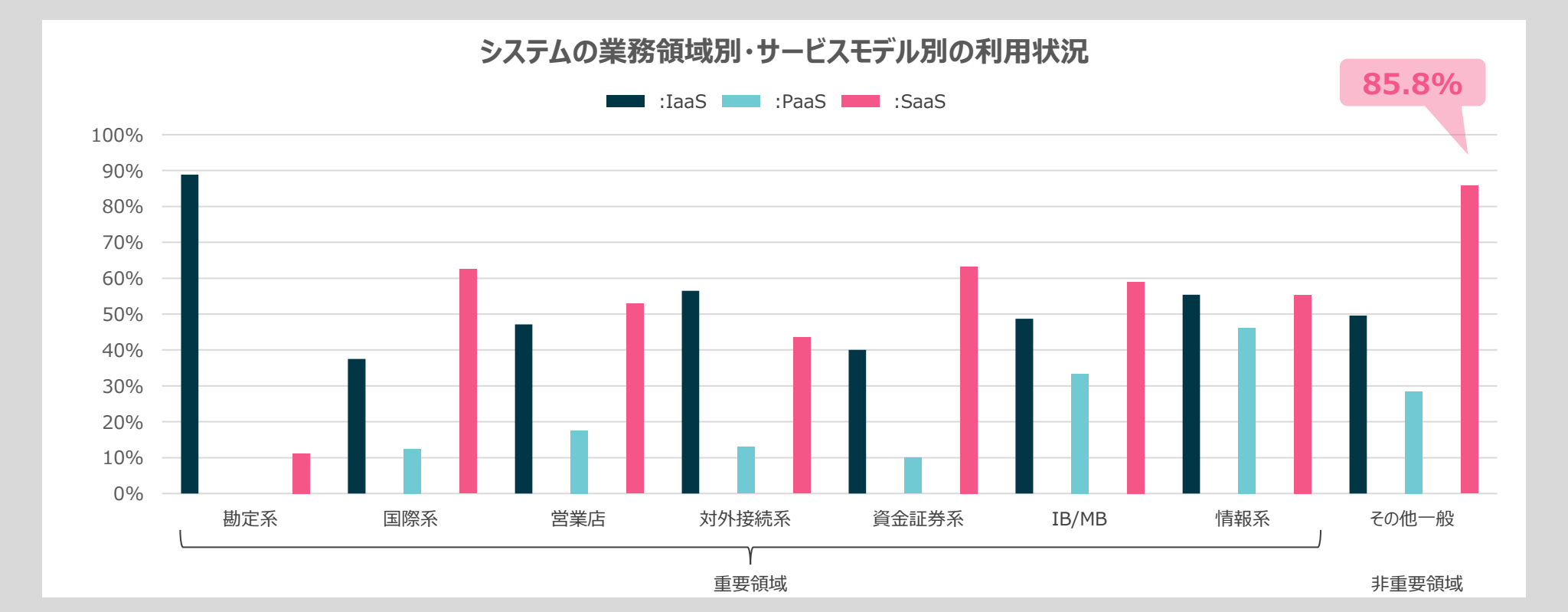


※日本銀行金融機構局 -「金融機関におけるクラウドサービスの利用状況と利用上の課題について - アンケート調査結果から -」（令和6年1月30日）- https://www.boj.or.jp/research/brp/fsr/data/fsrb240130a.pdf

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融機関におけるクラウドサービスの利用状況と利用上の課題について

- 勘定系システムではIaaSの利用が大半を占めている
- 一方で、資金証券系や国際系（重要領域）と、その他一般（非重要領域）では**SaaSが過半**を占めている

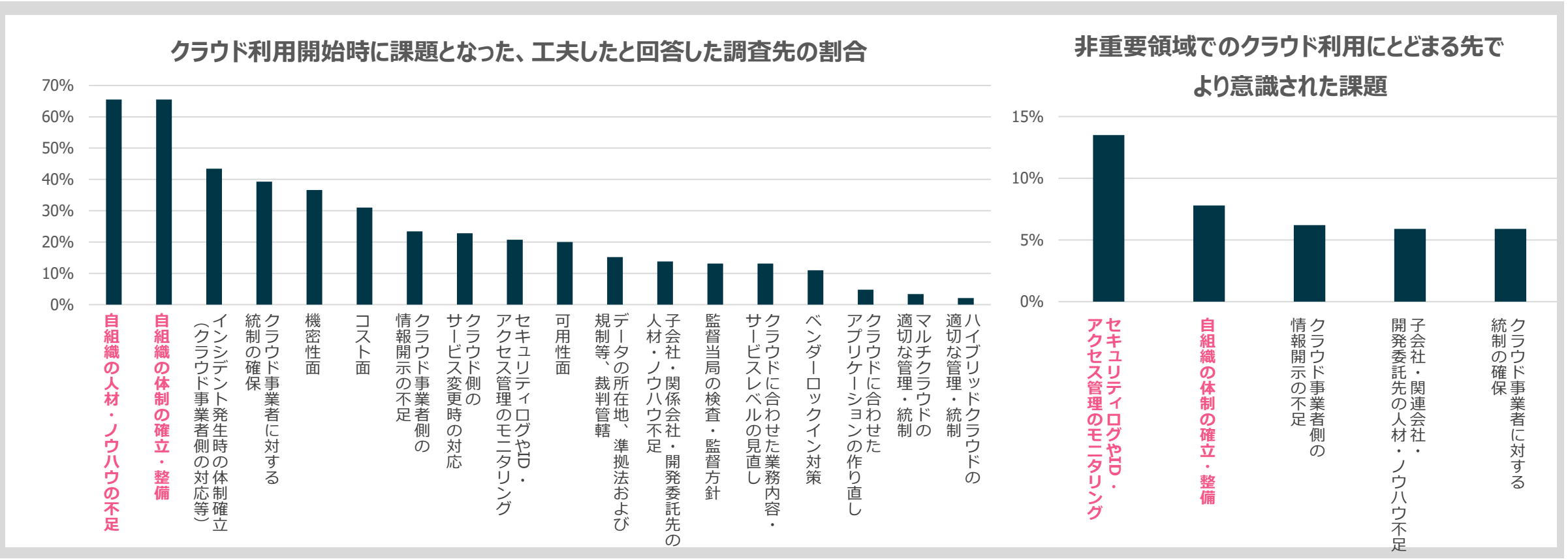


※日本銀行金融機構局 -「金融機関におけるクラウドサービスの利用状況と利用上の課題について - アンケート調査結果から -」（令和6年1月30日）- https://www.boj.or.jp/research/brp/fsr/data/fsrb240130a.pdf

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融機関におけるクラウドサービスの利用状況と利用上の課題について

- 自組織の人材・ノウハウ不足、自組織の体制確立・整備を挙げた先が**6割強**と最も多い
- 非重要領域での利用にとどまる先では**セキュリティログや ID・アクセス管理のモニタリング、自組織の体制確立・整備**といった基本的な事項が意識されている



※日本銀行金融機構局 -「金融機関におけるクラウドサービスの利用状況と利用上の課題について - アンケート調査結果から -」（令和6年1月30日）- https://www.boj.or.jp/research/brp/fsr/data/fsrb240130a.pdf

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

サマリ：アンケート結果より

- 多くの金融機関で、既にクラウドは使われている（9割以上）
- 勘定系含む重要領域ではクラウド利用は限定的ではあるが、一部の重要領域及び非重要領域では半数以上がクラウドを利用
- 金融機関のクラウド利用の中でも、資金証券系、国際系、その他一般システムではSaaSが積極的に利用されている
- クラウド利用が積極的に進められる中で、人材・ノウハウに加え体制確立といった組織面の課題や、ログ・ID・アクセス管理に課題意識あり

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融分野における
サイバーセキュリティに関するガイドライン

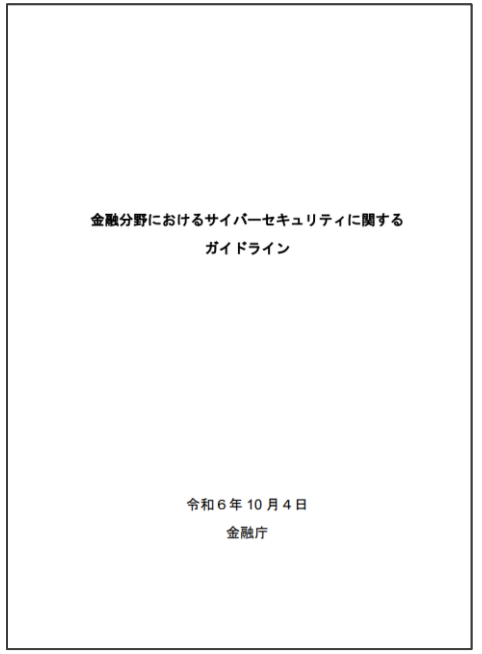
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融分野におけるサイバーセキュリティに関するガイドライン

- **“金融分野におけるサイバーセキュリティに関するガイドライン”**とは：
  - **金融機関が確保すべき**サイバーセキュリティの水準と管理態勢を示したガイドライン
  - 対象は銀行、証券、保険など**すべての金融業態**
  - **経営層の関与**や、**リスクベースアプローチの導入**を強調
  - サイバー攻撃の**予防・検知・対応・復旧**について記載
  - **"基本的な対応事項”**と**"対応が望ましい事項”**に分けて記載

基本的な対応事項

対応が望ましい事項



※金融庁 -「金融分野におけるサイバーセキュリティに関するガイドライン」（令和6年10月4日）- https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf より

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

“基本的な対応事項”と“対応が望ましい事項”

基本的な対応事項

【定義】

サイバーハイジーン（Cyber Hygiene）と呼ばれる、最低限守るべき基本的なサイバーセキュリティ対策

【事例】

- セキュリティパッチの適用
- アクセス権限や状態の管理
- 情報資産の棚卸し、分類
- 定期的なインシデント訓練、教育

対応が望ましい事項

【定義】

金融機関の規模や社会的影響の大きさに応じて、先進的に取り組む、実践することが望ましい対策

【事例】

- 主要な清算・振替機関等が参照すべき事例
- 海外当局や他社との対話で得られた事例
- 地域社会・経済等に大きな影響を及ぼす可能性がある場合、実践することが望ましいと考えられる取組み

リスクベース・アプローチ

金融機関はそれぞれのリスク許容度・戦略・事業環境に応じて、必要な対策を見極めることが求められる

※金融庁 -「金融分野におけるサイバーセキュリティに関するガイドライン」（令和6年10月4日）- https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf より

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融分野におけるサイバーセキュリティに関するガイドライン：詳細

金融分野におけるサイバーセキュリティに関するガイドライン					基本的な対応事項数	対応が望ましい事項数
1	基本的考え方				-	-
2	サイバーセキュリティ管理態勢				-	-
	2.1	サイバーセキュリティ管理態勢の構築	2.1.1	基本方針、規程類の策定等	9	5
			2.1.2	規程整備及び業務プロセスの整備	2	0
			2.1.3	経営資源の確保、人材の育成	4	0
			2.1.4	リスク管理部門による牽制	2	1
			2.1.5	内部監査	2	1
	2.2	サイバーセキュリティリスクの特定	2.2.1	情報資産管理	6	5
			2.2.2	リスク管理プロセス	12	7
			2.2.3	ハードウェア・ソフトウェア等の脆弱性管理	6	1
			2.2.4	脆弱性診断及びペネトレーションテスト	1	4
			2.2.5	演習・訓練	5	4
	2.3	サイバー攻撃の防御			1	0
			2.3.1	認証・アクセス管理	8	0
			2.3.2	教育・研修	5	2
			2.3.3	データ保護	5	2
			2.3.4	システムのセキュリティ対策	19	8
	2.4	サイバー攻撃の検知			2	0
			2.4.1	監視	7	3
	2.5	サイバーインシデント対応及び復旧	2.5.1	インシデント対応計画及びコンティンジェンシープランの策定	1	1
			2.5.2	インシデントへの対応及び復旧	19	1
	2.6	サードパーティリスク管理			10	5
3	金融庁と関係機関の連携強化				-	-
	合計				126	50

基本的な対応事項数：126、対応が望ましい事項数：50、管理態勢にも多数言及

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融分野におけるサイバーセキュリティに関するガイドライン：抜粋①

2. サイバーセキュリティ管理態勢				
2.2	サイバーセキュリティリスクの特定			
	2.2.1	情報資産管理		
		2.2.1.2	ハードウェア・ソフトウェア等	
			【対応が望ましい事項】b	必要に応じて、**サードパーティの資産についても管理対象とする**こと。
			【対応が望ましい事項】d	管理対象外となっている個人所有端末等の情報資産や**未承認のクラウドサービスの利用（シャドーIT 等）を特定**し、管理対象とするか使用を中止するなど、適切に対応すること。
2.3	サイバー攻撃の防御			
	2.3.1	認証・アクセス管理		
			【基本的な対応事項】①	**認証及びアクセス権の付与に係る方針及び規程等を策定**し、定期的に見直すこと。その際、以下の観点を踏まえること。
				ユーザ（システムを含む）の**アクセス権限を必要最小限に制限**し、職務の分離を考慮すること。
				アカウントのライフサイクル（作成、使用、終了）を管理すること及び**アカウントの定期的な棚卸しや操作履歴のレビュー**を実施すること並びに無権限者によるアカウントの不正使用を防止すること。
				特権アカウントの利用を厳格に制限し、管理すること（多要素認証、操作のダブルチェック、アカウントの時間制限の設定等）。
				外部委託先による**アクセス権の利用を適切に管理**すること。
			【基本的な対応事項】③	機器（API に認証情報を組み込むことを含む）及び**ユーザの ID 及び認証情報を適切に管理**すること（初期設定されたパスワードの変更、パスワード強度の要件、ID の自動失効、システム責任者による定期的なアクセスレビュー等）。

技術領域課題（SaaS）

サードパーティ管理 | シャドーIT特定 | アクセス権管理 | アカウント棚卸し

※金融庁 -「金融分野におけるサイバーセキュリティに関するガイドライン」（令和6年10月4日）- https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf より抜粋

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融分野におけるサイバーセキュリティに関するガイドライン：抜粋②

2. サイバーセキュリティ管理態勢				
2.3	サイバー攻撃の防御			
	2.3.3	データ保護		
		【基本的な対応事項】④		ライフサイクル全体（媒体の廃棄、**データの安全な消去**、外部委託先によるデータの取得・返却・破棄に至るまでの過程を含む）を通じて、データを適切に管理すること。
	2.3.4	システムのセキュリティ対策		
		2.3.4.5	クラウドサービス利用時の対策	
			【基本的な対応事項】③	**情報公開等の設定にミスがないか確認**すること。設定の妥当性の確認においては、必要に応じて、専門家によるシステム監査や誤設定の自動検知等の診断サービス等を利用すること。
			【基本的な対応事項】④	責任分界に応じて、**サービス仕様が変わる際には影響を確認**すること。
2.6	サードパーティリスク管理			
	【基本的な対応事項】④			**サードパーティを特定**し、サードパーティやサードパーティが提供する商品・サービスの自組織業務における位置づけ・役割・重要度、重要な情報（個人情報や営業機密等）の取扱いの有無、組織内システムへの接続状況（インターネット接続等の外部からのアクセスの容易さ）などをふまえ、サードパーティのリスク評価を行い、そのリスクに応じた対応をすること。
	【基本的な対応事項】⑤			**サードパーティを管理するための台帳等を整備し、維持する**こと（管理項目の例：サードパーティの名称、提供する商品・サービス及び機能、サードパーティが自組織のシステムに対し有するアクセスレベル、サードパーティが保持又は処理する自組織のデータの種類や機密性及び場所）。

技術領域課題（SaaS）

データ保護と安全な消去	情報公開範囲設定	サービス仕様確認	サードパーティ管理

※金融庁 -「金融分野におけるサイバーセキュリティに関するガイドライン」（令和6年10月4日）- https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf より抜粋

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

サマリ：ガイドラインから見えてきたSaaS利用における課題

：本講演で対策を模索していく課題

金融庁ガイドラインにて言及	SaaS	非技術領域課題（SaaS）	アクセス権管理	アカウント棚卸し
			情報公開範囲設定	データ保護と安全な消去
			サービス仕様確認	シャドーIT特定
			サードパーティ管理	
			技術領域課題（SaaS）	
	PaaS	非技術領域課題（PaaS）	技術領域課題（PaaS）	
	IaaS	非技術領域課題（IaaS）	技術領域課題（IaaS）	
	オンプレ	非技術領域課題（オンプレミス）	技術領域課題（オンプレミス）	
アンケート結果から判明した課題意識		人材・ノウハウ	組織体制	ID・アクセス管理	セキュリティログ
		非技術領域		技術領域	

【参考】クラウドサービスにおける責任共有モデル

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SaaS利用における課題と対処

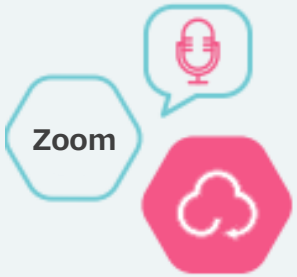
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

見過ごされがちなSaaSセキュリティの盲点

機密性の高いファイルが「リンクを知っていれば
誰でもアクセス可」の状態となっている

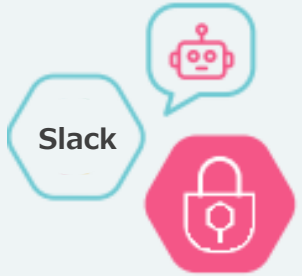
一時的に社外共有向けに格納した
ファイルが公開されたまま放置されている

多要素認証（MFA）を有効化
しない状態でユーザーを追加している



退職者がZoomの通話録音データに
アクセスできる状態のままになっている

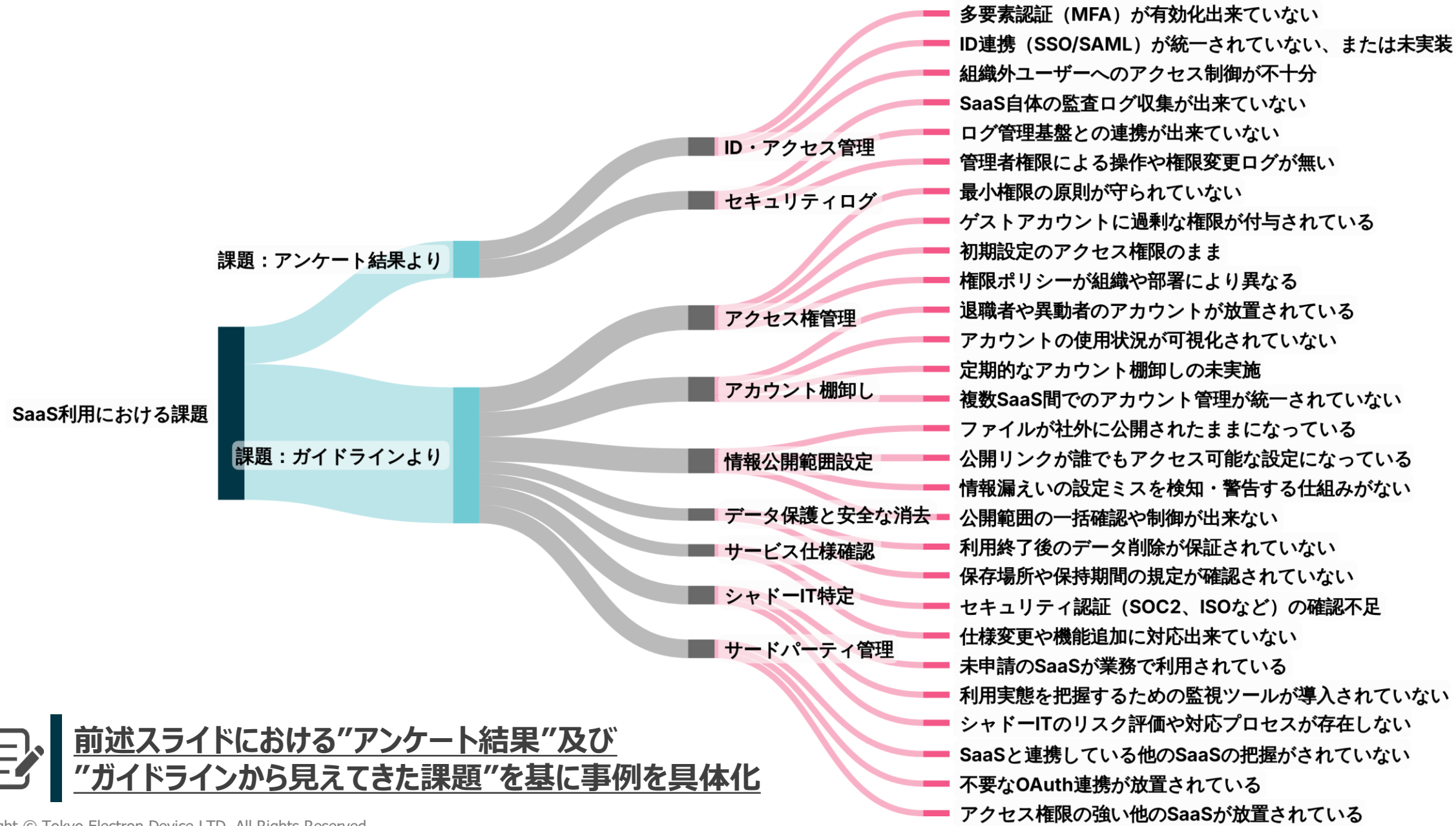
本来であれば不要なはずの管理者権限を
付与しているアカウントが存在する



SaaSに対しAIやロボットアカウントが
管理者の許可無くアクセス出来るようになっている

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SaaS利用における課題の分類と具体例



前述スライドにおける”アンケート結果”及び
”ガイドラインから見えてきた課題”を基に事例を具体化

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SaaSセキュリティの誤解と発生し得る脅威

- SaaSのセキュリティについて考慮せずとも問題無い
- SaaSのセキュリティはSaaSプロバイダーが管理する仕事である
- 情報システム部門がSaaSに関する全ての設定を管理している
- SaaSを安全に利用するには利用者にMFA/SSOを徹底させれば良い
- CASB/SMPにより、自社で利用しているSaaSは保護されている

SaaSセキュリティに対する誤解が、企業単体だけでなく社会影響を与える脅威と成り得る

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

直近の事例と対応状況

Microsoft SharePoint	**Fortinet Data Breach - 2024年9月12日** Fortinetは、社内のMicrosoft SharePointサーバーへ侵入にされ、機密データを含む440GBの内部情報が流出したと発表しました。 攻撃者はクラウドでホストされているMicrosoft SharePointサーバーにアクセスしたと報告されています。 この事例は、ビジネスに不可欠な情報を保存し続けるSaaSアプリケーション内の機密データを保護することの重要性を浮き彫りにしています。
Dropbox	**Dropbox - 2024年4月24日** Dropbox Signで全ユーザーのメールやアカウント設定が流出する侵害が発生。 NHI（=Non-Human Identity、人間以外のID情報）のセキュリティ不足が狙われたもので、 NHIには多要素認証などの強力なセキュリティ対策が欠けていることが多く、SaaS環境におけるNHI保護の重要性を示しています。
Salesforce	**Salesforce Misconfiguration - 2024年3月13日** SalesforceのHealth Cloudプラットフォーム上に構築されたアイルランド保健サービス局（HSE）の ワクチン接種ポータルの設定ミスにより100万人以上の個人情報が閲覧可能な状態に。 個人情報悪用は現在のところ確認されていませんが、SaaS設定管理やアクセス制御の重要性を示す事例です。
Microsoft 365	**Microsoft Midnight Blizzard - 2024年1月25日** Microsoftの検証環境やOAuthアプリを悪用し、重大なSaaS侵害が行われました。 経営陣や上級管理職・法務チームを標的とした攻撃で、包括的なSaaSセキュリティの必要性が浮き彫りになりました。 本事例の詳細に関しては**後述のスライド**でご説明させて頂きます。

IPA 総務省

●国内の対応状況

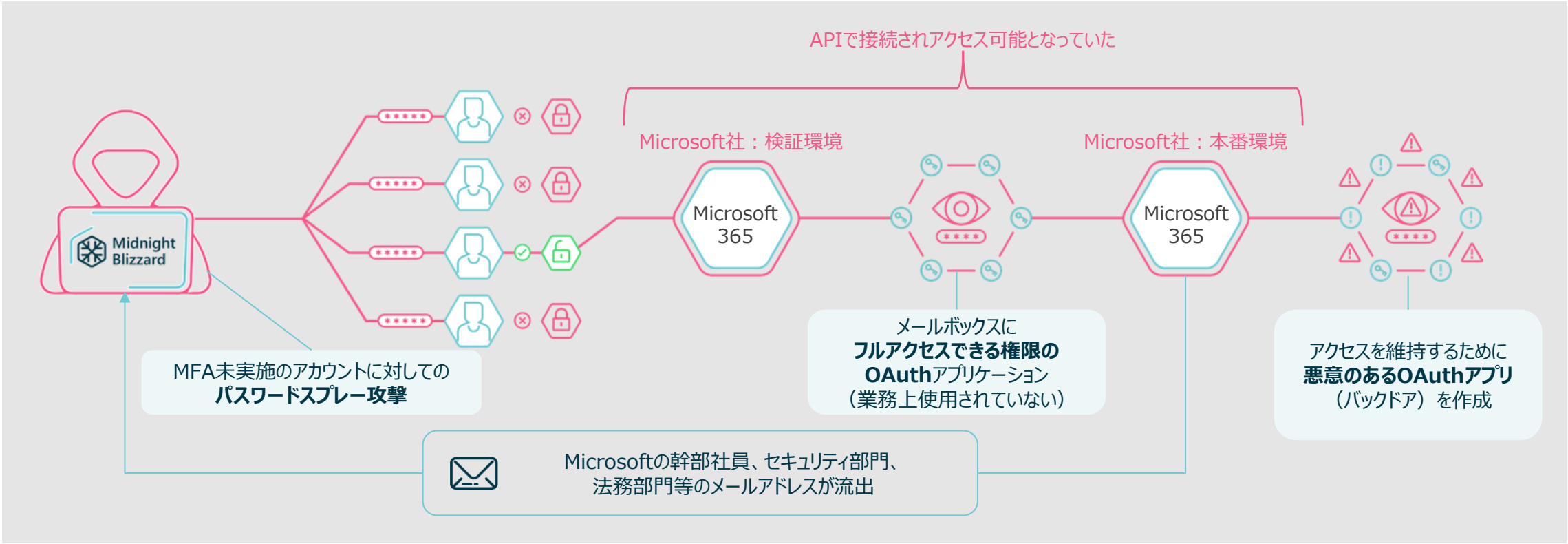
- **情報処理推進機構：情報セキュリティ10大脅威として“不注意による情報漏えい等の被害”が第6位に**
- **総務省　　：“クラウドの設定ミス対策ガイドブック”を公表、対策を呼び掛け**

独立行政法人情報処理推進機構 - 情報セキュリティ10大脅威 2024：https://www.ipa.go.jp/security/10threats/10threats2024.html

総務省 -「クラウドの設定ミス対策ガイドブック」の公表：https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00209.html

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

事例：Microsoft Midnight Blizzard Breach



MFAを始めとした
アカウント設定状況の把握

SaaS内で保持している
機密データの把握・保護

SaaSがAPIを介して接続している
3rd-Party-SaaSの把握・管理

1. クラウド利用加速により攻撃対象はオンプレからデータが集中している**SaaSへ移行**
2. Microsoft 365は日本国内で**最も利用されている**グループウェア
3. 高いシェアを誇るSaaSであるMicrosoft 365は**"攻撃のメインターゲット"**と成り得る

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

課題への対処：国内で普及している製品群

CSPM	CASB	SMP
Cloud Security Posture Management	**Cloud Access Security Broker**	**SaaS Management Platform**
クラウドセキュリティ態勢管理 IaaS/PaaSに対するセキュリティ態勢管理を提供	**セキュアなクラウドアクセスのための制御・中継機能** ユーザーとSaaSの間に介在しセキュリティや可視化機能を提供	**SaaS管理プラットフォーム** 複数SaaSの一元的な可視化と管理機能を提供
【提供する機能】 • クラウド環境内のリソースとリスクの可視化 • セキュリティ向上のための対処法の提示 • 効率的なセキュリティ運用のためのトリアージ **【補足事項】** • IaaS/PaaSが対象となる • SaaS環境の可視化や態勢管理は不可	**【提供する機能】** • SaaSの可視化（シャドーIT検知） • アクセス制御・ポリシー強制 • データ損失防止（DLP） **【補足事項】** • SaaSの可視化や制御は有効 • SaaS自体の設定不備は検出出来ない • 通信に介在するためリモートアクセスの際に例外設定を行う必要が出てくるケースがある	**【提供する機能】** • アカウント状態確認・棚卸し • SaaSアクセス権限の管理 • コスト管理（未使用ライセンス洗い出し等） **【補足事項】** • SaaSのアカウント管理に特化 • SaaSのアカウント状態や権限管理に有効 • セキュリティ設定不備検出やコンプライアンス遵守状態は確認することが出来ない

SaaSのセキュリティは既存のセキュリティ製品群を用いて防御し切ることは難しい

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SSPMの基本概念と選定ポイント

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SSPMとは

- SaaS Security Posture Management（=**SSPM**）
- 日本語に直訳すると”**SaaSセキュリティ態勢管理**”

【SSPMの代表的な機能】

セキュリティ設定の監視

SaaSアプリケーションのセキュリティ設定を継続的に監視し、不適切な設定や潜在的なリスクを検出

コンプライアンスの評価

企業が遵守すべきセキュリティ標準や法規制に基づき、SaaSのコンプライアンス状態を評価

リスクの評価と修正

検出された問題に対してリスクの評価を行い、自動的に修正するためのアクションを提供

可視性の向上

SaaS全体のセキュリティ態勢を可視化し、セキュリティの強化に役立つ視点を提供

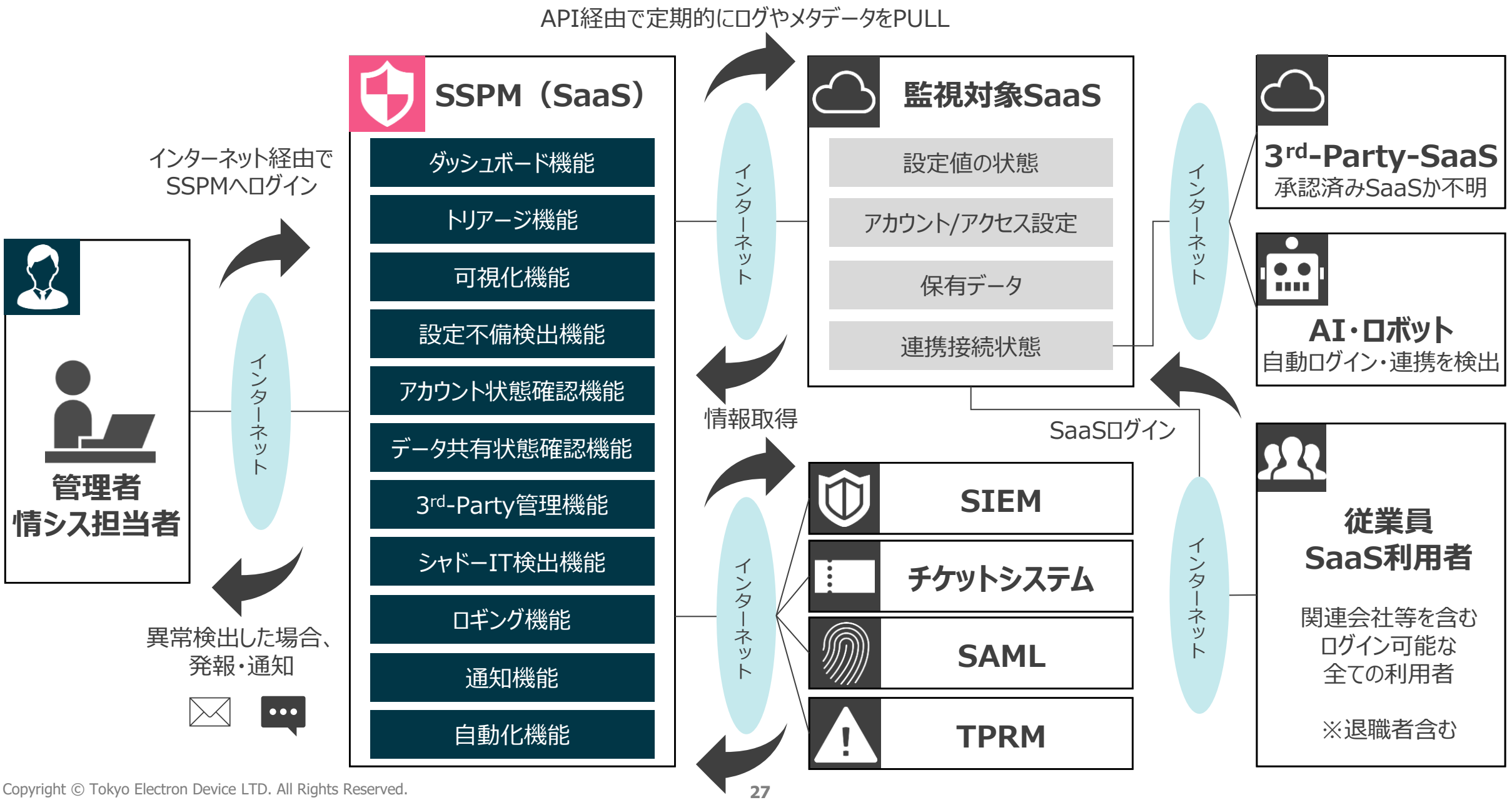
SSPMの利点

- セキュリティ設定の定期的な監視による**潜在的なリスク・脆弱性の特定**
- SaaSに特化した**効果的なセキュリティ対策の実施**が出来る
- 複数SaaSのセキュリティ設定の**問題点を一元管理**出来るようになる
- 可視化による**迅速な確認と対処**を行うことが出来る
- 自動化を併用する事による**運用管理の効率化・工数削減**
- コンプライアンス違反検出やレポート機能搭載、**監査・報告が容易に**
- 企業が**自律的にコンプライアンス遵守を徹底出来る**ようになる

組織が利用している様々なSaaSの設定内容や利用状態を随時確認し、
セキュリティリスクを特定・継続監視する**SaaS型セキュリティソリューション**

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SSPM：動作仕様概要図



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SSPM：選定のポイント

■ サポートしているSaaSのカバレッジ

- 監視や可視化対象と出来るSaaSがどれくらいあるか
- 将来的に監視・可視化対象とする予定のSaaSもサポートしているか

■ 監視・可視化対象とするSaaSのセキュリティ状態のチェック項目数や監査内容

- クリティカルなSaaSを特定し、該当SaaSのセキュリティチェック項目がどれくらいあるか
- 期待した監査項目をチェックする項目が存在するか

■ 初期設定・プロビジョニングの容易さ

- 導入負荷が無い or 少ない負荷で導入が可能か

■ セキュリティ標準や規格のカバレッジ

- 自社で遵守すべきセキュリティ標準や規格をカバーしているか

■ 運用管理面や自動化機能の有無

- 運用管理工数はどの程度か、削減できる仕組みはあるか
- 自動化機能や外部連携機能はあるか

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Valence Security社について

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Valence Security社について

valence

Find and Fix SaaS Risks.

Connect Beyond

企業概要

社名	Valence Security, Inc.
設立	2021年
本社	米国カリフォルニア州サンフランシスコ
最高経営責任者	Yoni Shohet
顧客	米国を中心に多数
受賞歴	• RSA 2023 Innovation Sandbox Finalist • CRN® The 10 Hottest Cybersecurity Startups • Hot Company SaaS/Cloud Security • SaaS Security Posture Management (SSPM) • 2023 Global InfoSec Awards • 2023 SC Media – Finalist: Most Promising Early-Stage Startup

視認性の高いユーザーインターフェース

Valence Security ログイン後の画面（Dashboard画面）

4つの領域（Security Checks , Identities , Integrations , Data Shares）から詳細を確認し、安全なセキュリティ状態を維持

Dashboard画面で各SaaSの状況やアラートの一元監視が可能

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Valence Security - サポートしているセキュリティ標準規格

Valenceが監査しているセキュリティ標準規格	セキュリティ標準規格の詳細
CIS Microsoft 365 Foundations Benchmark	Microsoft 365環境のセキュリティ強化のためのベストプラクティスを提供する基準
CIS Critical Security Controls	サイバー攻撃から防御するための20の主要なセキュリティ対策ガイドライン
NIST Cybersecurity Framework	リスク管理とセキュリティ強化のための5つの基本機能（識別、防御、検知、対応、復旧）を提供する枠組み
ISO 27001 Information Security Management Systems	情報セキュリティ管理システム（ISMS）の設計、導入、運用、監査のための国際規格
CIS Google Workspace Foundations Benchmark	Google Workspaceの安全な設定と運用のための推奨ベストプラクティス
CISA Cybersecurity Performance Goals	中小企業を含む多様な組織のサイバーセキュリティパフォーマンスを向上させるための指針
NCSC Cyber Assessment Framework	サイバーリスクを評価し管理するためのイギリス国家サイバーセキュリティセンターによるガイドライン
DOD Cybersecurity Maturity Model Certification	米国国防総省が求めるサプライチェーンにおけるサイバーセキュリティ成熟度の認証モデル
ISACA COBIT 19	ITガバナンスと管理のフレームワークで、情報と技術の管理を体系的に行うためのベストプラクティスを提供
HIPAA	米国の医療情報保護に関する法律で、電子化された医療情報のセキュリティとプライバシーを規定
PCI Data Security Standard（PCI-DSS）	クレジットカード情報のセキュリティ基準で、カード決済環境におけるデータ保護を目的とする
NIST Special Publication 800-53	連邦政府機関向けに情報システムのセキュリティとプライバシー管理を規定した標準
SOC2	クラウドやサービスプロバイダーのセキュリティ、可用性、機密性、プライバシーに関する監査基準
CSA Cloud Controls Matrix (CCM)	クラウドセキュリティのためのフレームワークで、セキュリティコントロールと規制要件のマッピングを提供
Federal Risk and Authorization Management Program	米国政府向けクラウドサービスのセキュリティ認証プログラム

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

導入事例：Goosehead Insurance Inc.の紹介

- 企業名：Goosehead Insurance Inc.（GSHD）
- 設立：2003年
- URL：https://www.goosehead.com/
- 株式公開：Post IPO（NYSE）
- 事業内容：米国内顧客に向けた主に個人向け保険・サービスの販売及び提供

Customer Impact：

“データの露出低減・情報漏洩防止のために”

valence

Valence SaaS Risk Assessment

リスクアセスメントサービス

ステップはたったの3つ。簡単、スピーディ、もう迷わない。

1. まずは1時間、SaaSセキュリティの専門家とご相談。
2. 数日以内に、詳細なセキュリティ診断レポートをお届け。
3. すぐに活かせる“気づき”を、最低でも3つ、ご提供。

■ **対象となるSaaSアプリケーション：**

- 主にご利用にされているグループウェア　（例：Microsoft 365, Google Workspaceなど）
- アイデンティティ管理/IDaaS　（例：Okta, Azure ADなど）
- ビジネス上で重要な位置付けとされているSaaS　（例：Salesforce, GitHub, Zoom, Atlassianなど）

■ **実施条件：**

- ご利用になられているSaaSに対する読み取り専用アクセス権(*)のみ　（*：構成メタデータと監査ログに限定）

リスクアセスメントサービス、先着3社様限定で無料実施中！残り僅か！

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

共に創る　新たな価値を