



SaaS活用企業必見！ セキュリティ強化の鍵：CASB, SWG, DLP, SSPM徹底解説

東京エレクトロン デバイス株式会社

CN BU CN営業本部

※本資料に掲載されている会社名・製品・サービス名・ロゴは各社の商標または登録商標です。
また、写真・ロゴマーク・その他の著作物に関する著作権はそれぞれの権利を有する各社に帰属します。

Agenda

- ビジネス成長の秘訣はSaaSの活用
- SaaS活用の裏に潜むセキュリティリスク
- CASB, SWG, DLPでユーザーを守る
- SSPMでデータを守る
- 東京エレクトロンデバイス 会社概要

ビジネス成長の秘訣はSaaSの活用

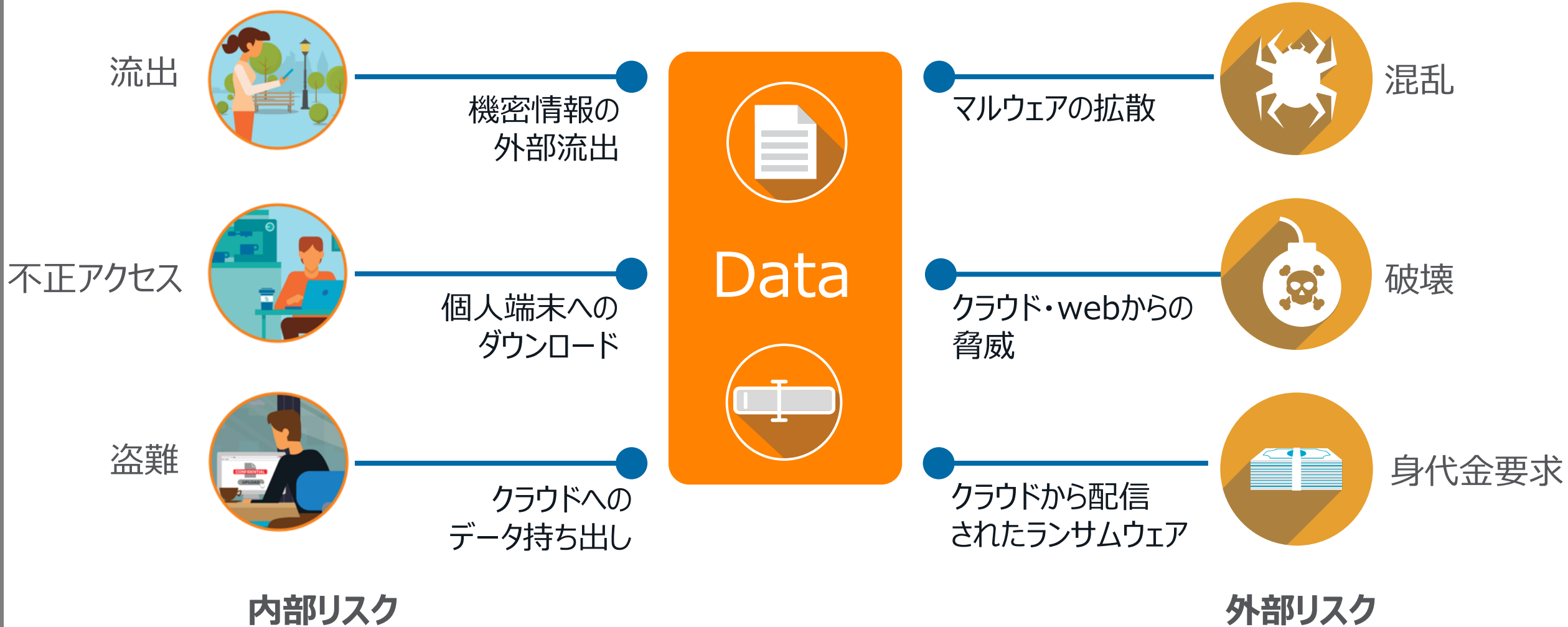


いつでも、どこでも、
あらゆるデバイスで

瞬時の共有と
コラボレーション

月額課金のため
気軽に活用

データ管理はユーザー企業



IPA情報セキュリティ10大脅威でもランクイン

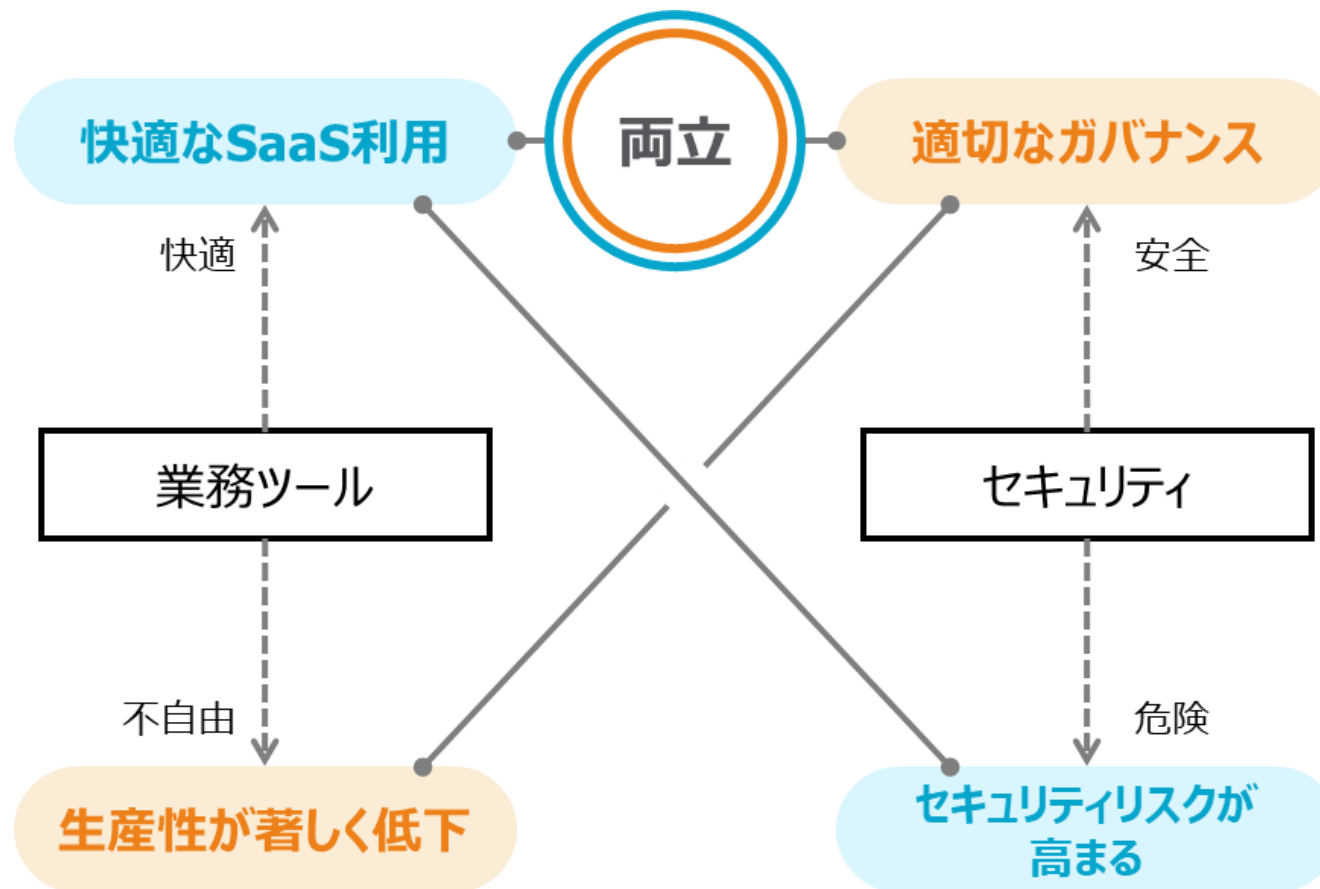
順位	「組織」向け脅威	初選出年	10大脅威での取り扱い (2016年以降)
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

主な適切なセキュリティ対策の例

- サービス利用の可視化
- サービス利用方法の制御
- アクセス制御の強化
- データ暗号化
- 従業員の教育

参照：情報セキュリティ10大脅威 2025(2025年1月30日)
<https://www.ipa.go.jp/security/10threats/10threats2025.html>

=「快適SaaS利用」と「適切なガバナンス」の両立



快適なSaaS利用 x 適切なガバナンスのために

SSPM

SaaS設定のセキュリティを管理



CASB

SaaSの可視化・制御
安全なアクセスを確保



DLP

機密データの漏えいを防止



SWG

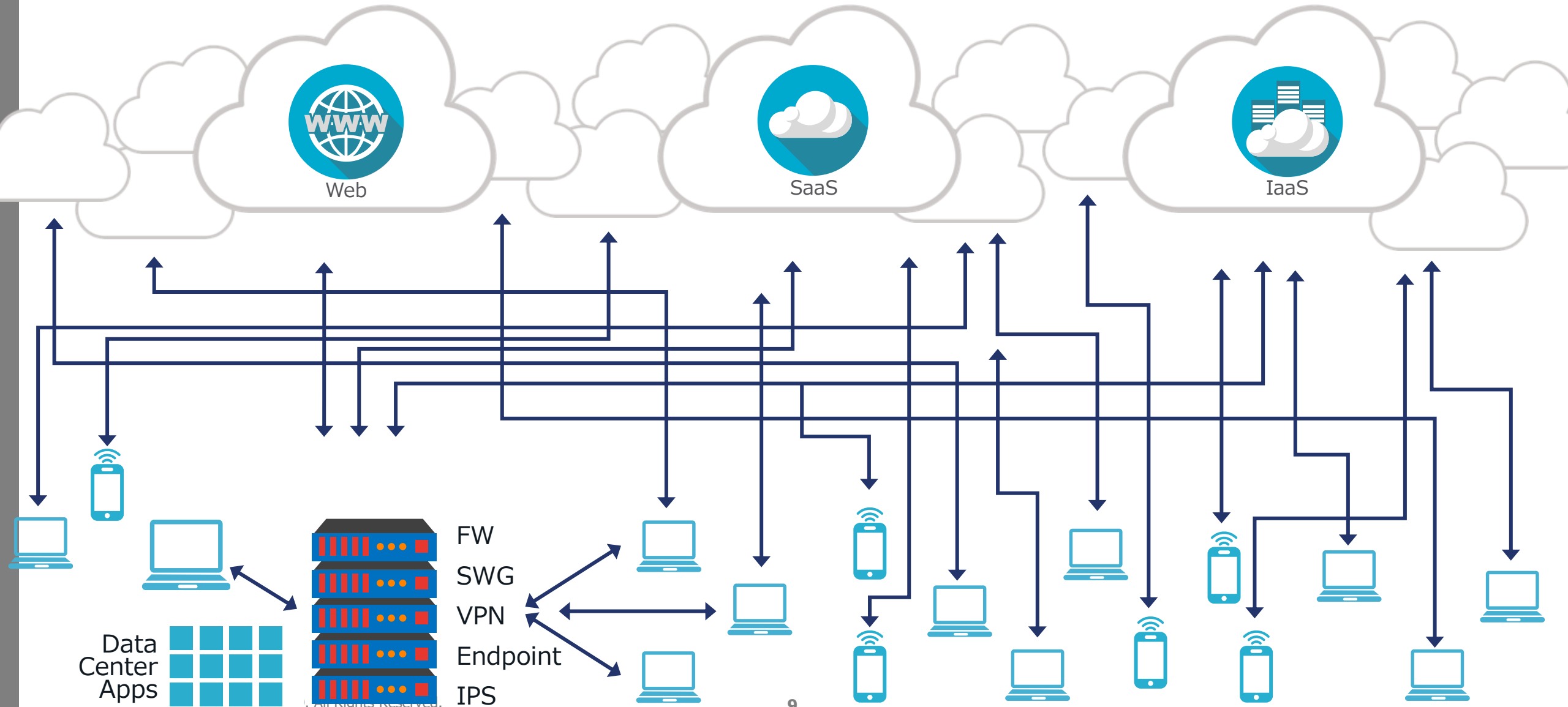
安全なインターネットアクセスを提供

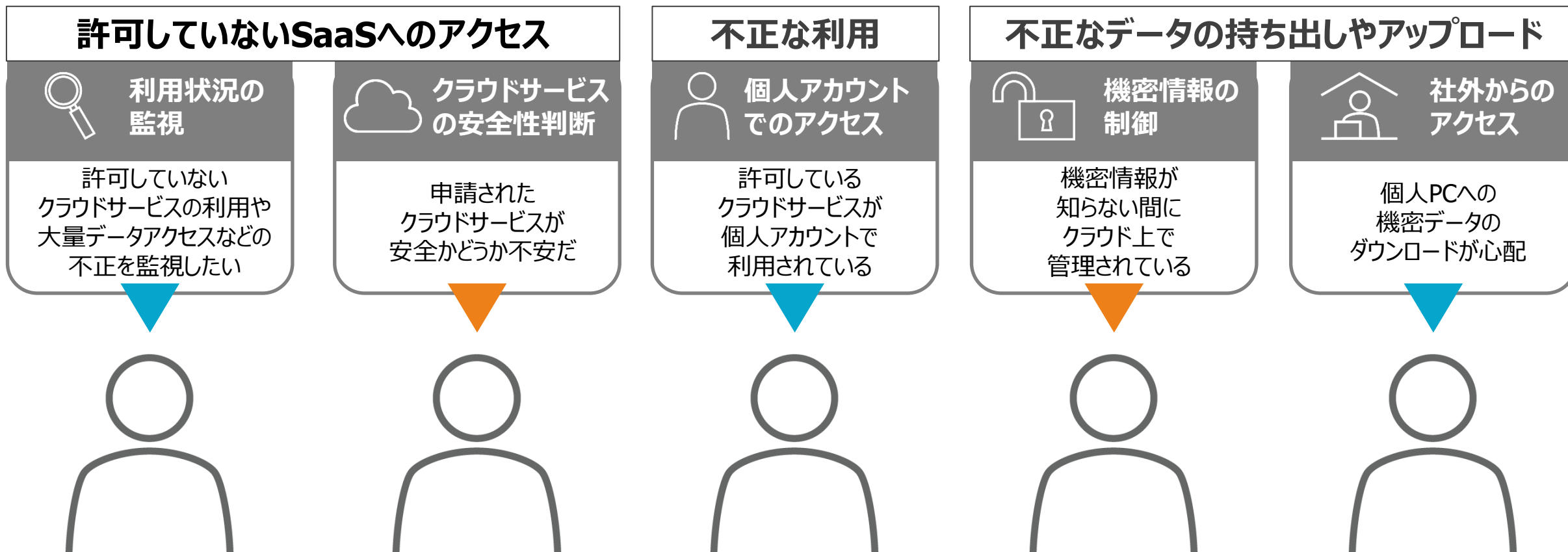




CASB, SWG, DLPでユーザーを守る

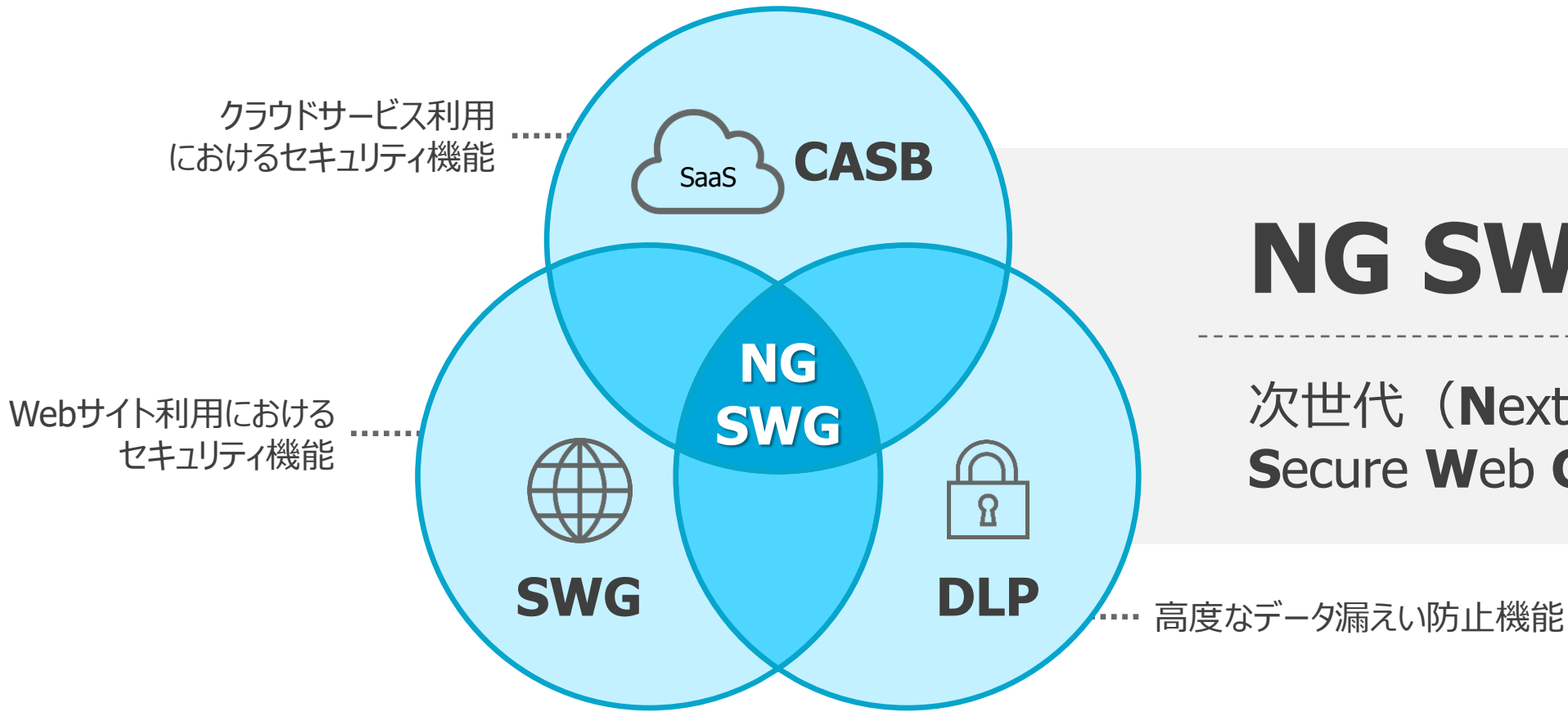
現在のクラウドセキュリティの状況





CASB・SWG・DLPが解決！

CASB+SWG+DLP = NG SWG



NG SWG

次世代 (Next Generation)
Secure Web Gateway

CASBとSWGとDLPを共通の制御ポリシーとともに統合したセキュリティを実現



利用するクラウドサービスを制限・管理

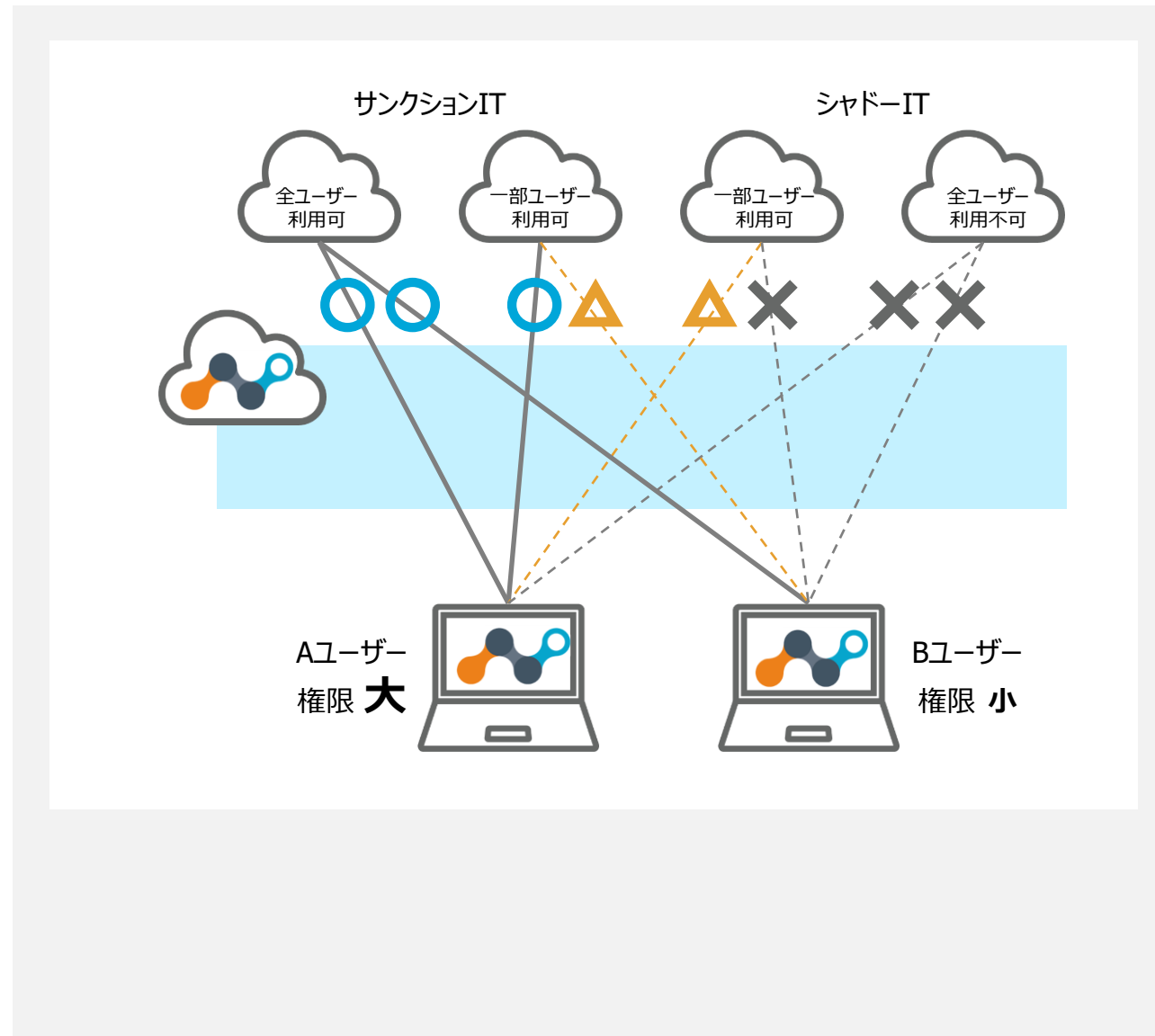
- ユーザー毎に利用可能なクラウドを制御可能
- 自社契約クラウドかどうか識別し、ファイル内容に応じた操作権限を付与可能
- 接続元制限（Netskopeからのみに制限）し、不正ログインを防止
- SaaS安全性評価データベースのスコアに応じたクラウドサービス制御が可能

ユーザーのクラウドサービス利用を管理

- ユーザーの操作（アクティビティ）を可視化・監視
- データ持ち出しなどのアノマリ操作を検出
- ポリシーに応じて禁止操作をブロック
- 機密情報のアップロードをリアルタイムに遮断可能

FW、プロキシで制御できていないシャドーIT対策

- 部門での契約、個人での登録といったシャドーITの可視化とリスク分析
- 個人アカウント利用や禁止操作をブロック
- 社外利用端末からの非許可クラウドへのアクセスも可視化・制御





Webサイトも含めた幅広いアクセス管理 (SWG)

一般的な課題

- クラウドサービスだけでなく、業務上のWebサイトへのアクセスも増加
- オンプレミスのWebフィルタリングやIPフィルタリングだけでは網羅性や利便性が低く、運用的にも限界

Netskopeの更なる活用

- 業務に関係のないサイトや、悪意のあるサイトへのアクセスを制御
- ユーザーやグループ単位で制御可能
- C&Cサーバーへのアクセス制御





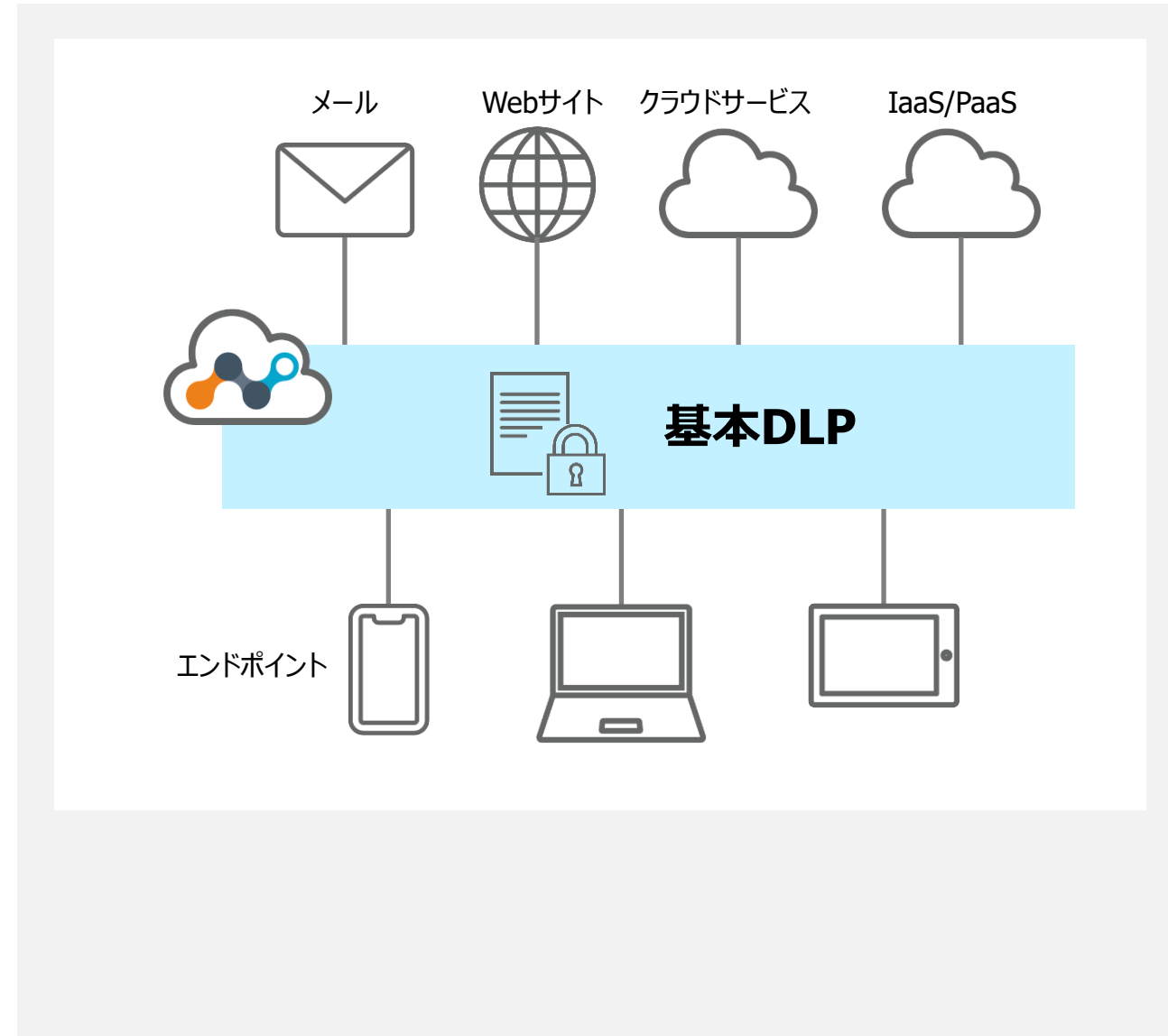
機密情報のアップロード/ダウンロードの制御（DLP）

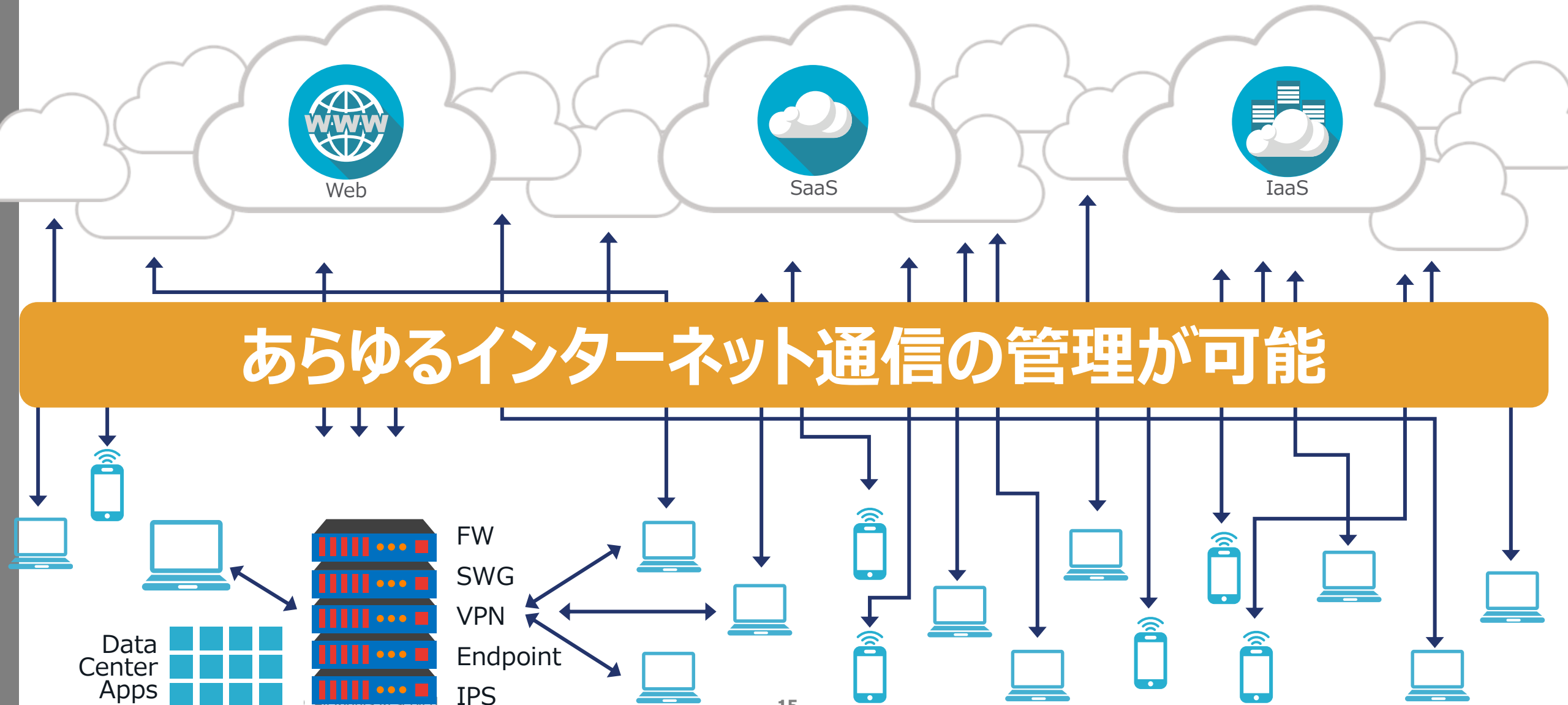
一般的な課題

- 悪意ある人間によるデータ流出や漏えいなどの内部不正は、外部からの攻撃よりも見抜くのが困難
- アクセスが許可されているため、アクセス履歴だけでは不正かどうかの判断が不可能

Netskopeの更なる活用

- 特定キーワードや個人情報を含むファイルの、メール添付やクラウドサービスへのアップロードなどを禁止
- 豊富なファイル形式に対応
- ブロック・隔離・リーガルホールド・削除・属性変更・メール通知・ユーザーアラートなどの追加アクションが可能







SSPMでデータを守る

OneDriveで
ファイル共有

GitHubで
ソース管理

Zoomで
打ち合わせ

Slackで
情報連携

誤って社外担当者に
機密ファイルを共有

リポジトリのアクセス権を
協力会社に渡してしまった

録音にアクセス可能な
API接続を有効化していた

ユーザーが3rd Party
アプリを勝手に追加した

近年に発生したセキュリティインシデント

- M社 – O365 – 約1万件の情報漏えい
- R社 – 某クラウドサービス – 約36万件の情報漏えい
- A社 – Googleドライブ – 約94万件の情報漏えい

SaaSのセキュリティについて考慮する必要はない、という認識は誤り
アクセス権をはじめ、各種設定を正しく行うことで安全に利用可能

対象

必要な取り組み

対策

PCユーザー
スマホユーザー

デバイスの監査ツールを用い、
利用状況を可視化し、
通信を保護

CASB/SWG/DLP

IaaS
(AWS/Azure/GCP/etc)

IaaSの監査ツールを用い、
クラウドの設定を管理し、
リスクを検出

CNAPP/CSPM

SaaS
(O365/Google Workspace/etc)

SaaSの監査ツールを用い、
アプリケーションの設定を管理し、
リスクを検出

SSPM



セキュリティ対策

SaaS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検出し、修正のためのアクションを提供。



一元管理

複数のSaaSアプリケーションに対する、セキュリティ設定やポリシーを可視化し、ダッシュボードから一元管理。



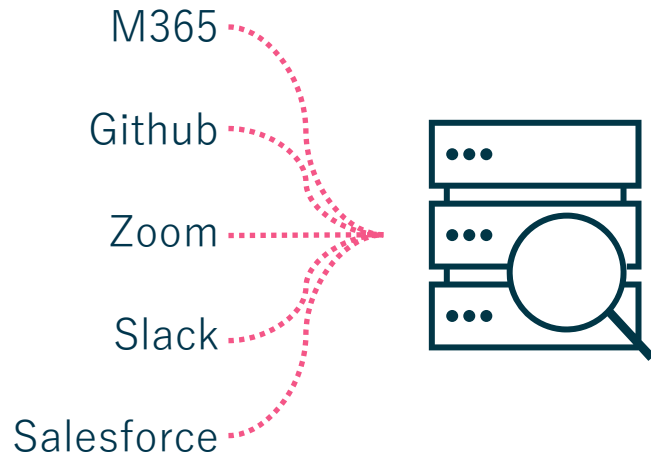
コンプライアンス遵守

企業が遵守すべきセキュリティ標準や法的要件に基づいて、SaaSアプリケーションのコンプライアンス状態を評価し、修正を支援。

SaaSに対するセキュリティ対策を一元管理し
企業のコンプライアンス遵守を支援するソリューション

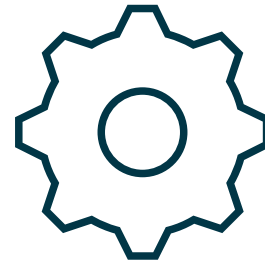
3ステップで実現するSSPMによるセキュリティ対策

STEP.1



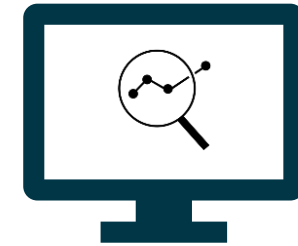
対象SaaSに
管理者権限を付与する

STEP.2



SaaS側及び
SSPM側に設定実施

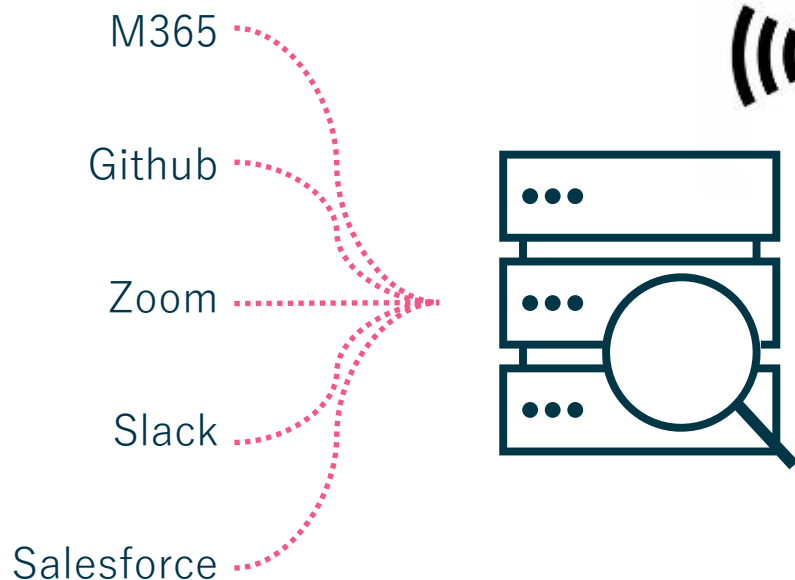
STEP.3



セキュリティリスクを
検出開始

管理者権限を与えて設定を完了したら、
セキュリティ対策は完了

検出



リスク検出時の対応

- ① ダッシュボードにてリスクを表示
- ② 修正方法のガイドラインが提示される
- ③ ガイドラインに従って該当SaaS上の設定を修正

指示に従うだけでセキュリティリスクに対する対応が完了



セキュリティ専門家の不在

SSPMを導入したとしても使いこなすことができない

Valence Security

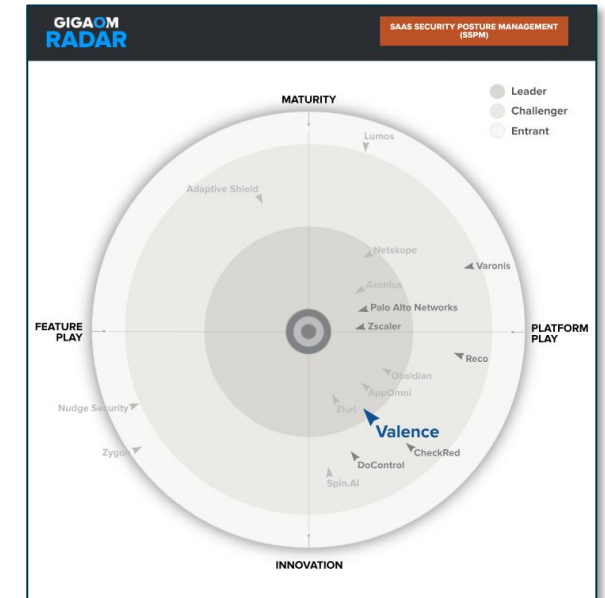
① 導入が簡単

SaaS側の設定変更は不要

SSPM側のポリシー設定も不要

② リスク対応が簡単

検知したリスクに対して自動修正



簡単な導入と、自動化対応によって
セキュリティの専門家がいなくても利用可能



東京エレクトロンデバイス会社概要

会社概要

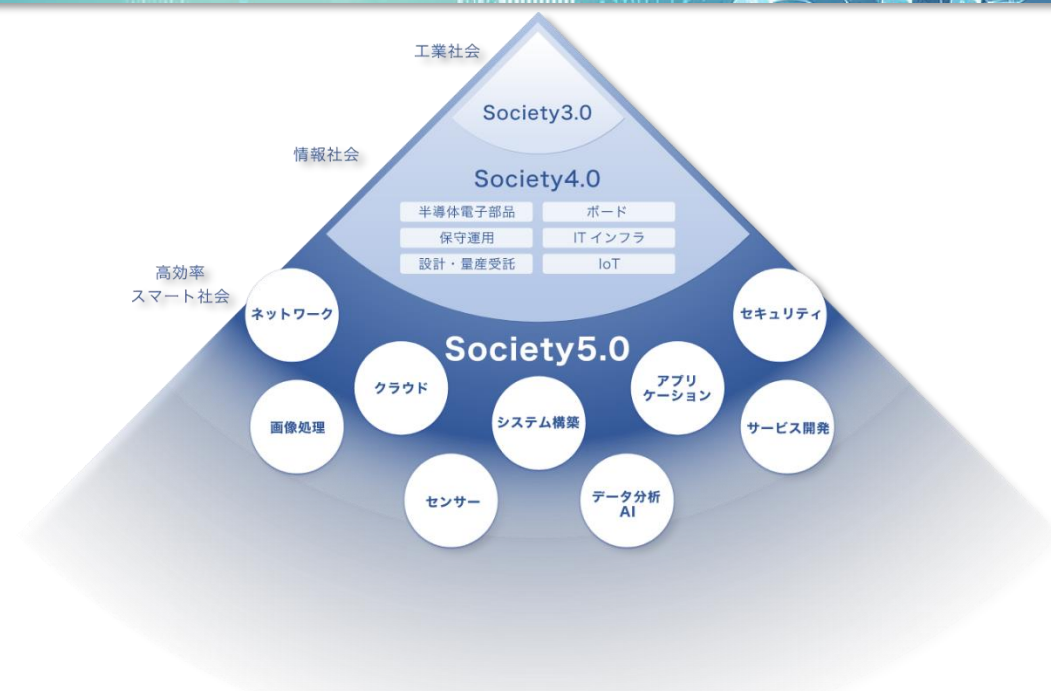
- 会社名** : 東京エレクトロ デバイス株式会社 (TED)
- 設立** : 1986年3月3日
- 代表** : 代表取締役社長・CEO 徳重 敦之
- 株式** : 東京証券取引所 プライム市場 (証券コード : 2760)
- 資本金** : 24億9千5百万円
- 売上高** : 2,428億88百万円 (2024年3月期)
- 従業員** : 連結: 1,357名 (2024年3月31日現在)
- 子会社** : 東京エレクトロ デバイス長崎株式会社
TOKYO ELECTRON DEVICE ASIA PASIFIC LTD. (TED APAC)
TOKYO ELECTRON DEVICE (SHANGHAI). LTD
TOKYO ELECTRON DEVICE SINGAPORE PTE. LTD. (TEDSG)
TOKYO ELECTRON DEVICE (THAILAND) LIMITED. (TEDTH)
TOKYO ELECTRON DEVICE AMERICA, INC. (TEDAI)

事業内容

半導体ソリューション
inrevium 自社ブランド製品
ITソリューション

EC Biz **CN Biz**

TED DRIVING DIGITAL TRANSFORMATION

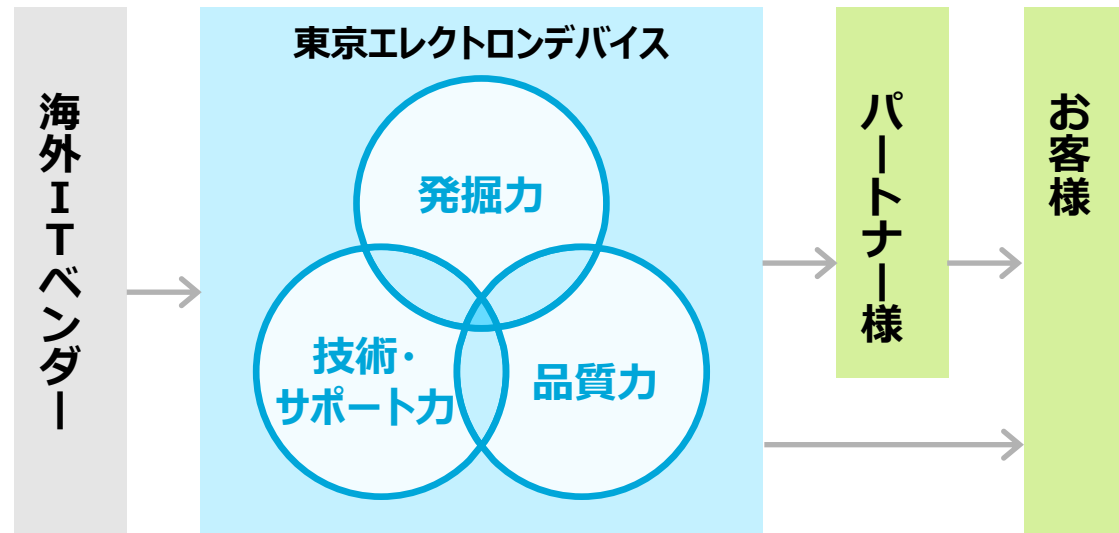


CN BU (Computer Network Business Unit) について

CN事業 (Computer Network事業)

■ 3つの力

- **発掘力**
最先端テクノロジー・ビジネスの発掘と開拓
- **技術・サポート力**
導入支援・アフターサービス
- **品質力**
受入検査・出荷検査



■ フォーカスエリア

セキュリティ



高度化するサイバー攻撃対策
やセキュリティ対策

ネットワーク



高速・高可用性ネットワーク環境を構築、
効率的な運用管理の支援

ストレージ



オンプレとクラウドをシームレスにつなぐ
データ保護・管理

AI



ビジネスを加速する
AIプラットフォーム/サービスを提案

クラウド



管理性・運用性・可用性が高く、
スケーラブルなクラウド環境の構築

テレワーク/クラウドアクセス関連ソリューション

CASB	SWG	ZTNA	IDaas
SSE/SASE			SSO/多要素認証
エンドポイント	HSM	シークレット管理	
Active EDR/XDR		Hashicorp	

社内/トラストネットワーク関連ソリューション

Firewall	VPN	WAF
 		 Distributed Cloud Services
Wi-Fi	DNS/DHCP	NDR
Cognitive Wi-Fi	DNSセキュリティ	

セキュリティ診断

ASV

PenTest, ASM

データ分析

SIEM/SOAR/UEBA

その他取扱い製品

その他の取り扱い製品については以下のWebよりご覧ください。

<https://cn.teldevice.co.jp/>

クラウド管理

CSPM/CNAPP	SSPM	IaC
		Hashicorp

クラウド

パブリッククラウド

AI/DLソリューション

GPU	Accelerator

仮想化基盤ソリューション

HCI	3Tier

ファイルストレージソリューション

Scale Out	Scale Up
Power Scale	Unity XT

ネットワークソリューション

IP Clos	L2/L3スイッチ	ADC
	DCNW 	キャンパス

バックアップソリューション

クラウドバックアップ対応



ご清聴ありがとうございました