CASBの理想と現実とこれから

ウェブセキュリティと一体化していくCASB

株式会社シマンテック

エバンジェリスト

髙岡 隆佳

アジェンダ

1 CASBの理想

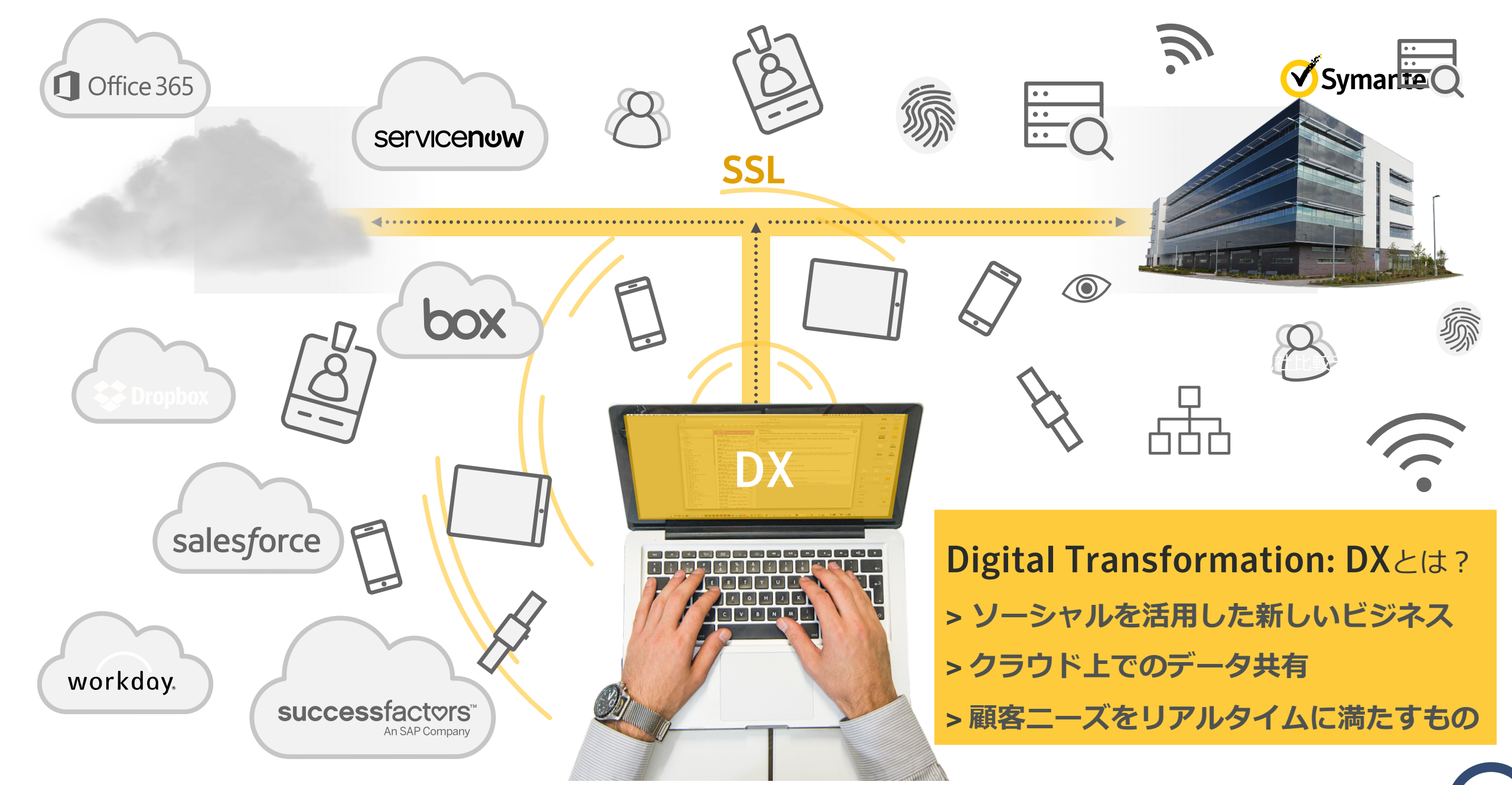
2 CASB導入後の課題と誤解

3 先を見据えた境界線を定義する

Symantec™

CASBの理想

Symantec™



Digital Transformation: DXとは？

> ソーシャルを活用した新しいビジネス

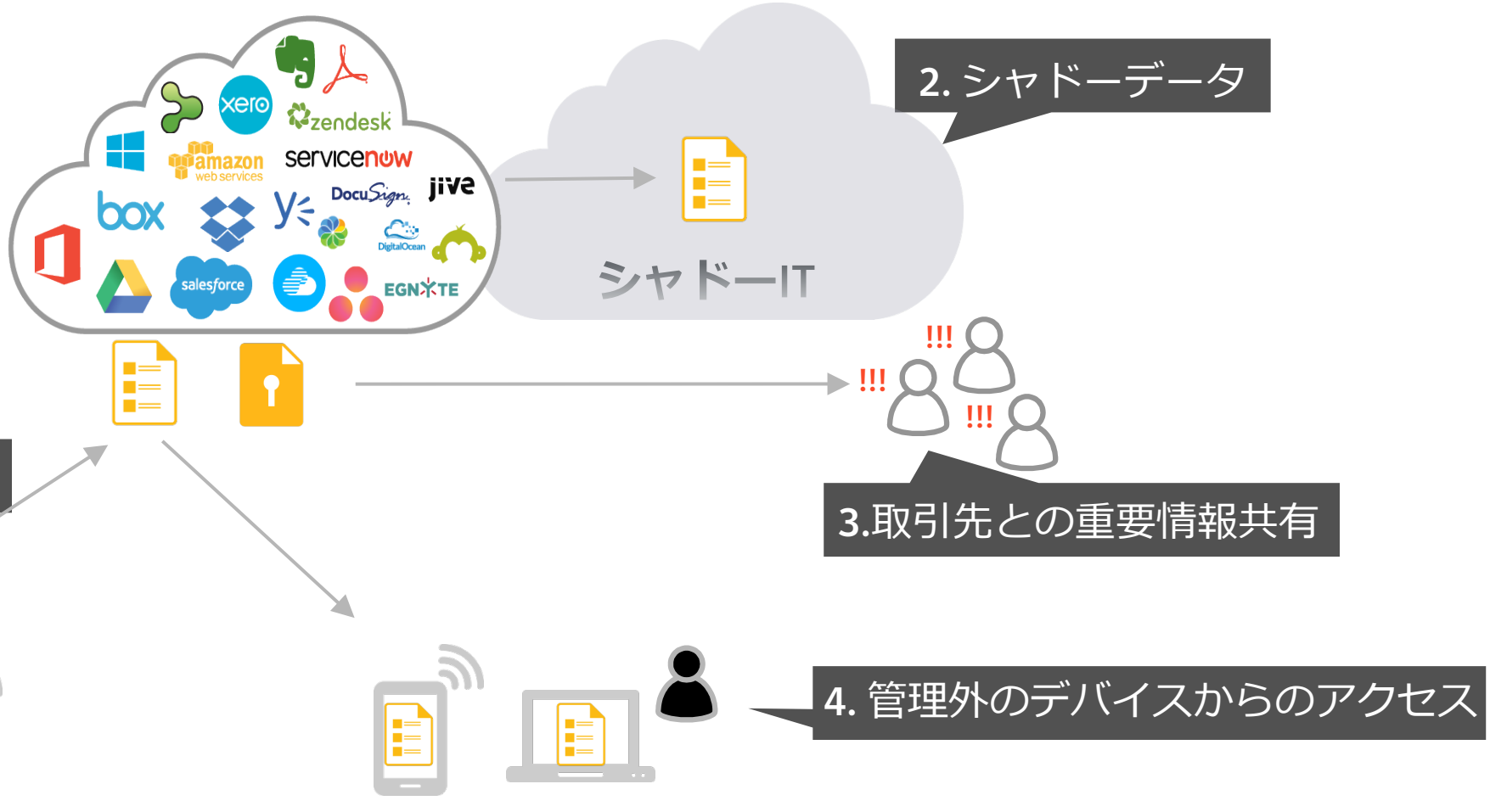
> クラウド上でのデータ共有

> 顧客ニーズをリアルタイムに満たすもの

クラウドシフトに伴うデータの流出リスク

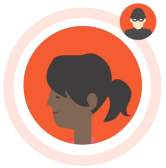
Symantec

○主要な
4つのリスク



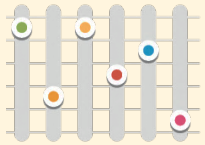
CASBがもたらすメリット

「機密情報」
の自動認識

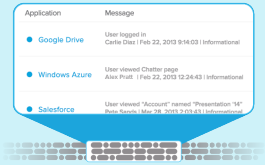


「シャドーユーザ
の特定

「社外リソース」
の制御



「データ共有先」
の把握



「クラウド活用」
の監視

クラウドシフトすればするほど投資効果＝企業のクラウドシフトを加速化

CASB実装方式について

管理者アカウント

1 クラウド上のデータ保護とアクセス制御
→ API

2 一元的なセキュリティポリシーの施行
→ ProxyまたはAgent

CASB

Proxy

Agent

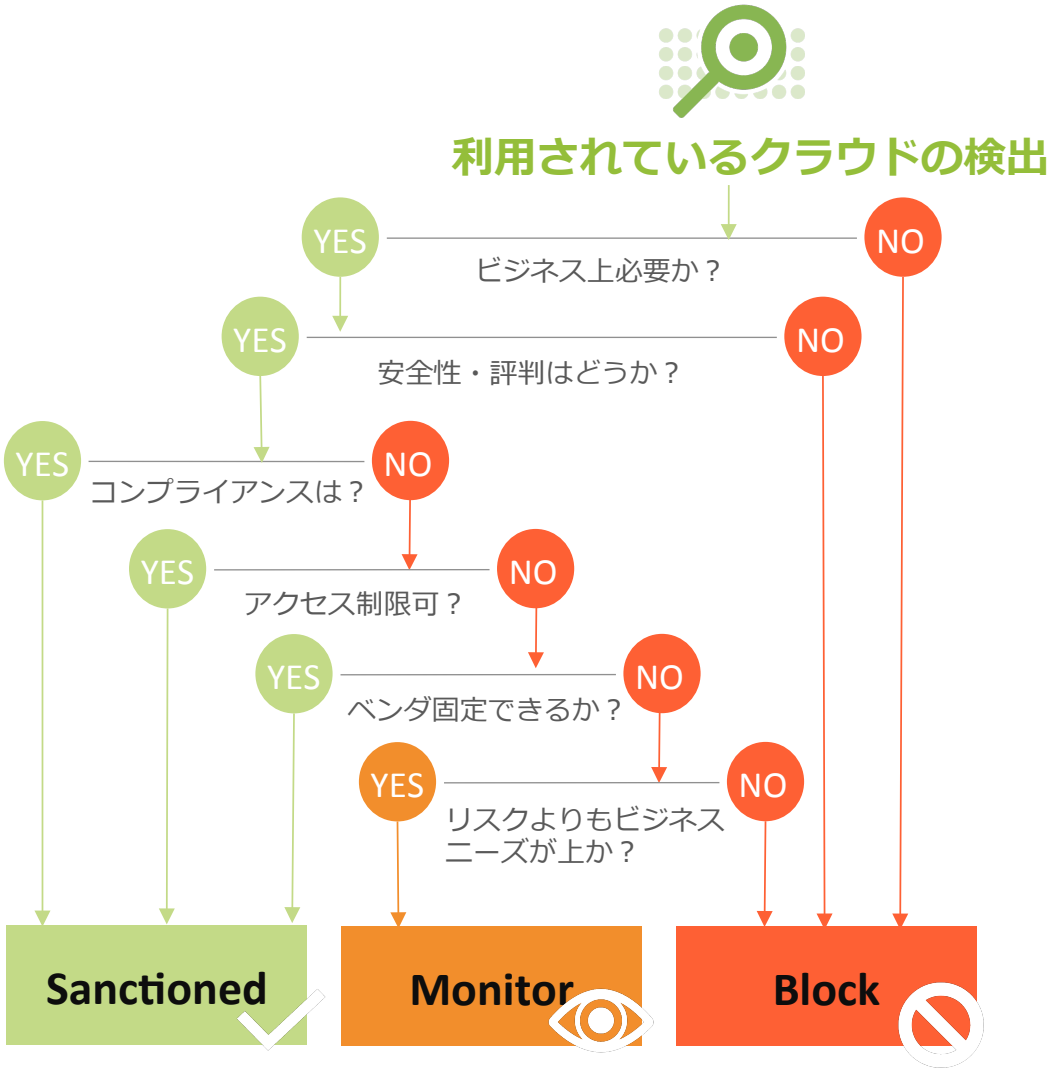
オンプレミス

在宅勤務ユーザ

3 シャドーIT可視化とユーザふるまい分析
→ Proxy/FWまたはAgentのアクセスログ

クラウドアプリケーションの整理→ 活用

- グレーゾーンを無くし、クラウドシフトを促進



- **Sanction | 認可アプリ** API
  - 企業が社員に対し投資しているアプリ
  - IT側で責任持ってデータ保護が必要（**クラウドベンダ側はユーザの利活用における漏洩においては責任を取らない**）
- **Monitor | 監視対象アプリ** Proxy/Agent
  - 業務上止めることができないアプリ
  - コンプライアンス上、害はないと判断されたアプリについては利用許可（**ただし監視対象とする**）
- **Block | ブロック対象アプリ** Proxy
  - セキュリティ上、コンプライアンス上リスクなりうるアプリは利用の禁止

CASB導入後の課題と誤解

Symantec™

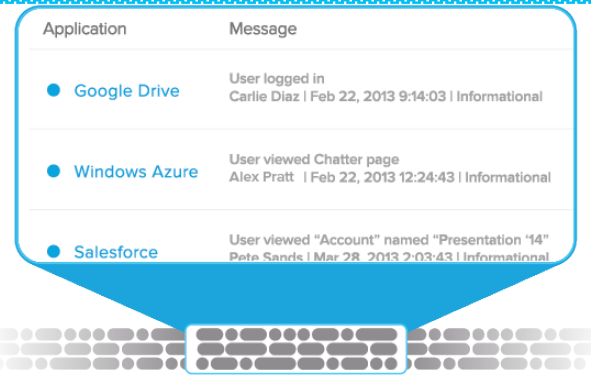
CASB実装後の課題

CASBはとどのつまりSSL可視化＋DLP

IDと付随するユーザのステータスを元にクラウド利用を制御

SSL Proxy　本人認証　アクセス監査　DLP　暗号化

CASB (Cloud Access Security Broker)

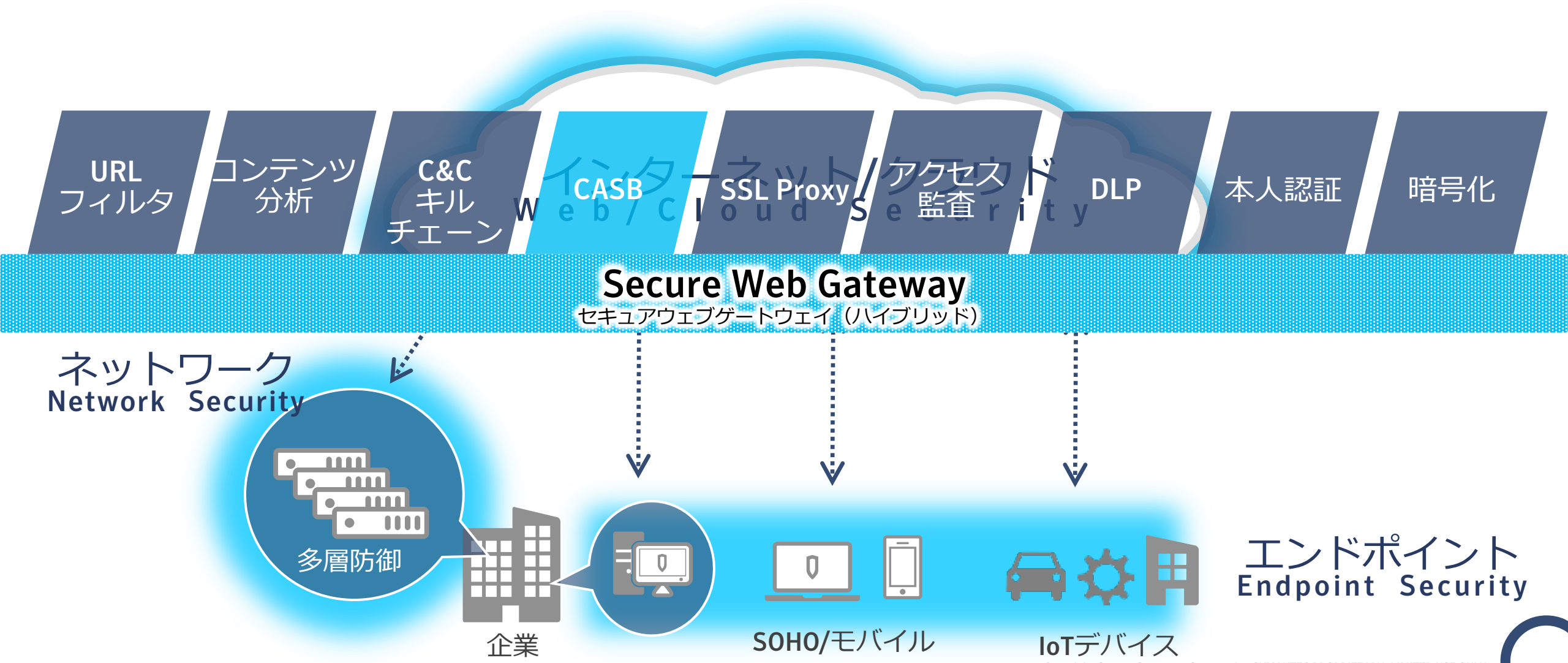


SSL（https）

クラウド

CASBだけでは足りない？

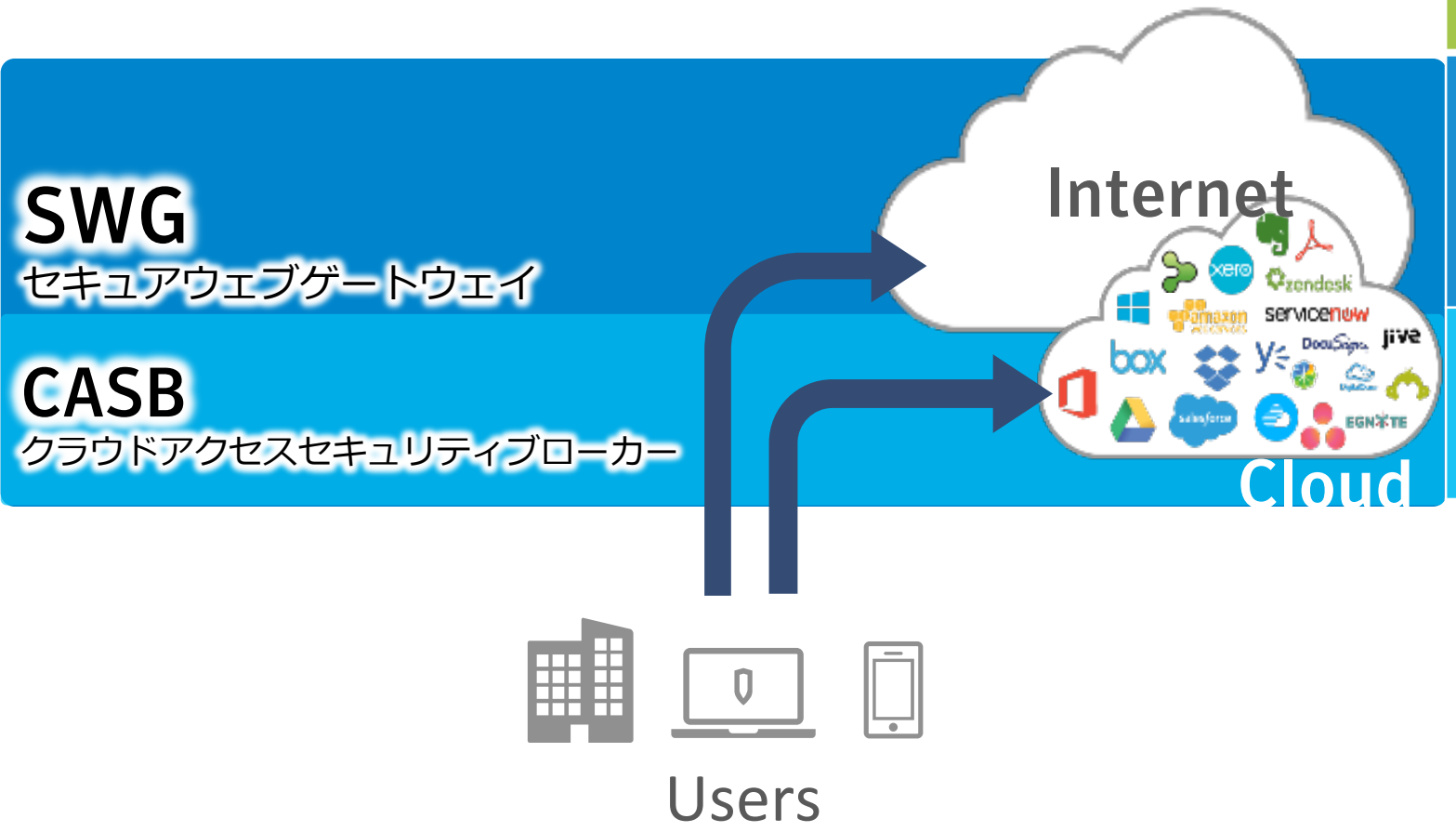
場所を問わず企業のセキュリティポリシーを一元的に適用



SWG v.s. CASB

CASBはSWGに包含されて初めて価値が出る

無害化（ウェブ分離）	C&Cキルチェーン	暗号化	DLP（API）	DLP（事前）	SSL可視化	アクセス監査	ユーザ認証	コンテンツフィルタリング	URLフィルタリング
○（クラウド含む）	○（クラウド含む）	○（クラウド含む）	×	○（クラウド含む）	○（クラウド含む）	○（クラウド含む）	○（クラウド含む）	○（クラウド含む）	○（クラウド含む）
×	×	クラウドのみ	クラウドのみ	クラウドのみ	クラウドのみ	クラウドのみ	クラウドのみ	クラウドのみ	クラウドのみ



CASBのDLPは実用的ではない？

データ形式に合わせた適切な検出ロジックが必要

フィンガープリント 適合性チェック

非構造化情報

デザイン、ソースコード等
派生的な適合性
完全に近い正確性

機械分析

非構造化テキスト

デザイン、ソースコード等
派生的な適合性
かなり高い正確性

コンテンツ表現の 適合性チェック

文章などのデータ

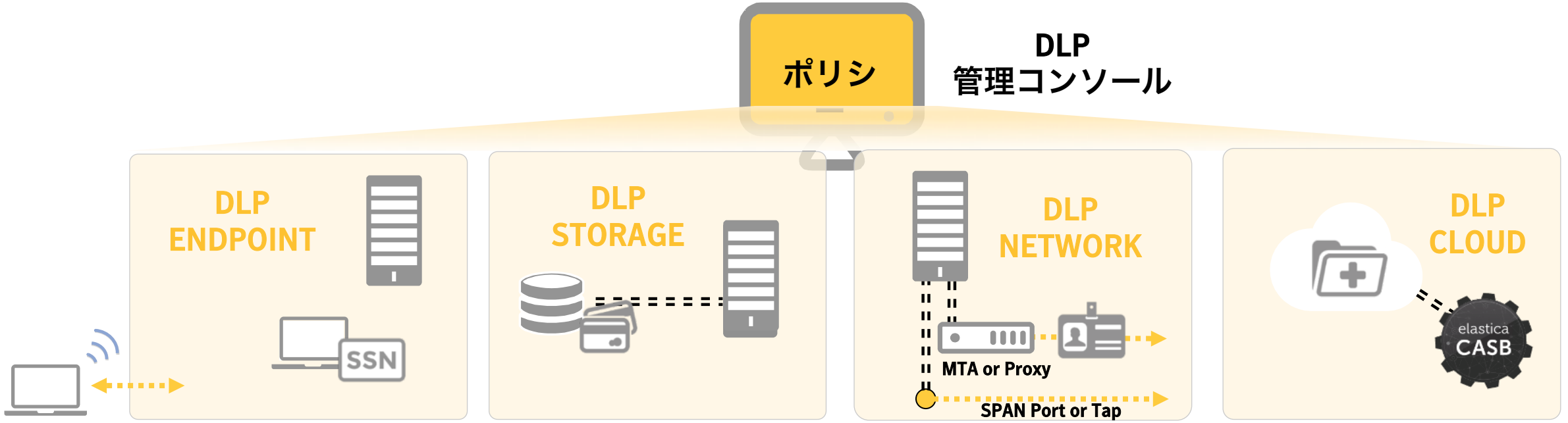
インデックス化できないデータ
専門用語
データを特定する情報

完全なデータ 適合性チェック

構造化データ

クレジットカード情報、価格、
部分マッチ、
ほぼ完全に近い正確性

データ経路の網羅性



→ Windows・Mac
→ 外部デバイス
→ アプリケーション

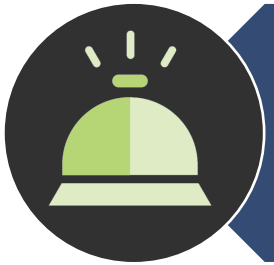
→ ファイルサーバ
→ データベース
→ NAS

→ ウェブ通信
→ メール
→ ファイル転送

→ クラウドメール
→ クラウドストレージ
→ シャドーデータ

- **現場・現物に即したデータの棚卸し**(ヒアリングや机上のレビューのみに依存しない)と**台帳化**により、見逃しなく対象データを把握
- 管理対象データに対する**適切な技術的・組織的セキュリティ対策を確認**し、**個人情報保護法/GDPR要件とのギャップを識別**、修正

後悔しないCASB選定のポイント



**CASBで分類できないクラウドを
ウェブセキュリティで補完できるか？**

→ SWG連携、多段プロキシなどのURLフィルタ機能で漏れなくポリシー施行できるか

**データの分類と制御の精度は
運用の妨げにならないか？**

→ 幅広いデータ形式の対応
→ 社内のデータ、端末上のデータにポリシーを適用できるか

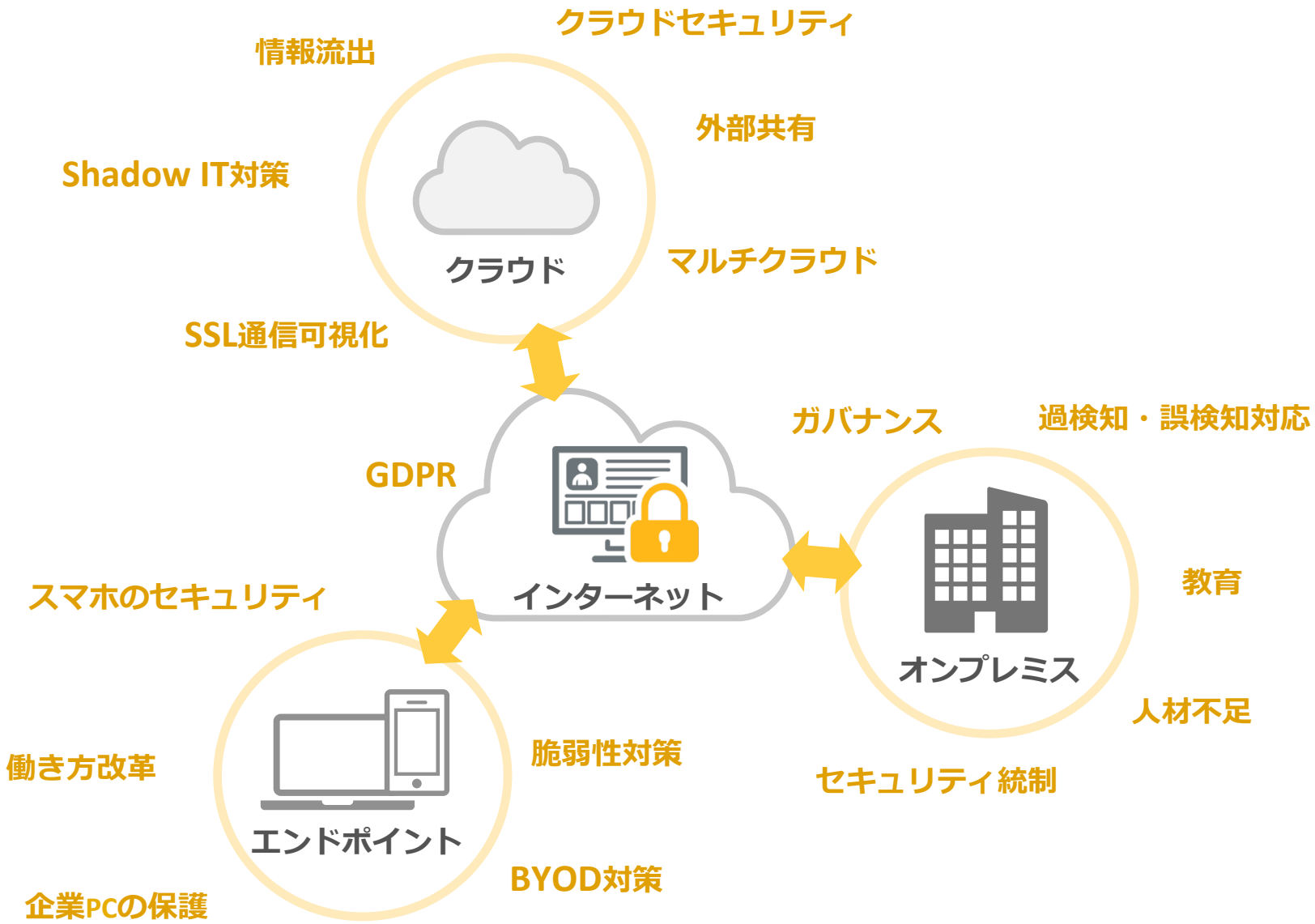
**企業としてのクラウド活用指針や
データ取扱い規定を定義しているか？**

→ 指針がなければ適切なポリシーもかけられず、十分な投資効果が得られないどころか情報流出のリスクが残る

先を見据えた境界線を定義する

Symantec™

企業のセキュリティ課題は多岐にわたる



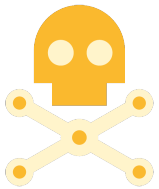
働き方改革、クラウドシフト、DX…

- ✓ 企業の守るべきデータは境界線を越えて活用
- ✓ データとユーザを取り巻く脅威は従来の枠組みを超える
- ✓ オンプレ、モバイル、クラウド全方位型のセキュリティ対策

統合化前提のセキュリティ投資の必要性

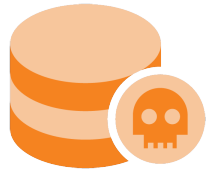
Symantec

インシデント
最新の攻撃
ビジネス継続性



サイバー攻撃対策

\?



情報流出対策

コンプライアンス
クラウドシフト
働き方改革

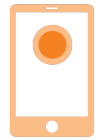
Orchestration & Automation

メール

ウェブ

クラウド

PC



モバイル

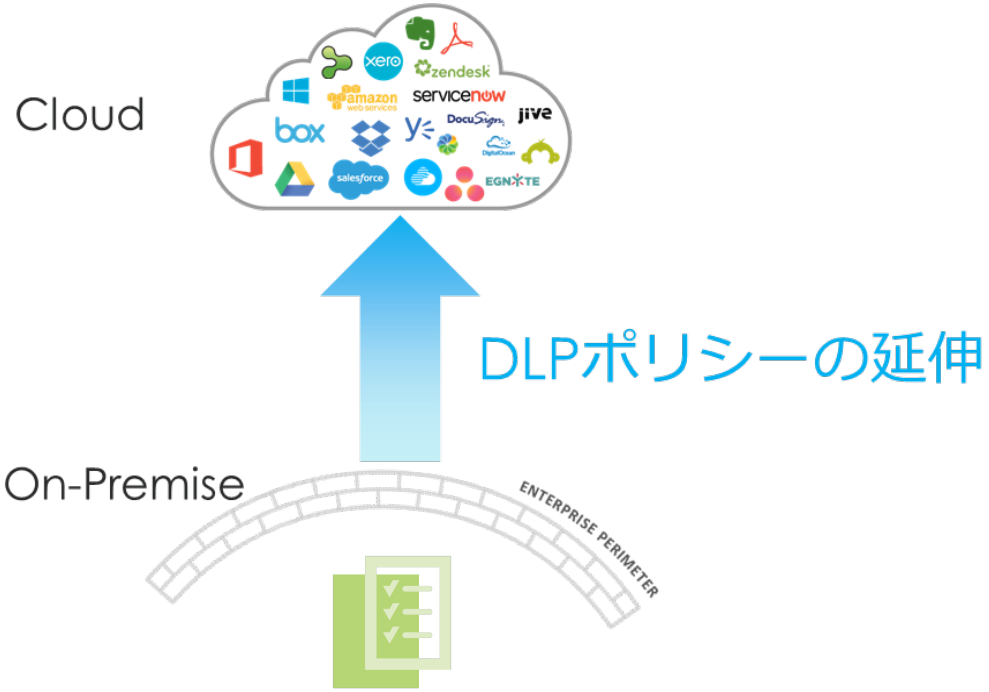
VM

統合化基盤（セキュリティプラットフォーム）で投資効果と運用負荷の最小化が必要

海外とは異なるデータガバナンス事情

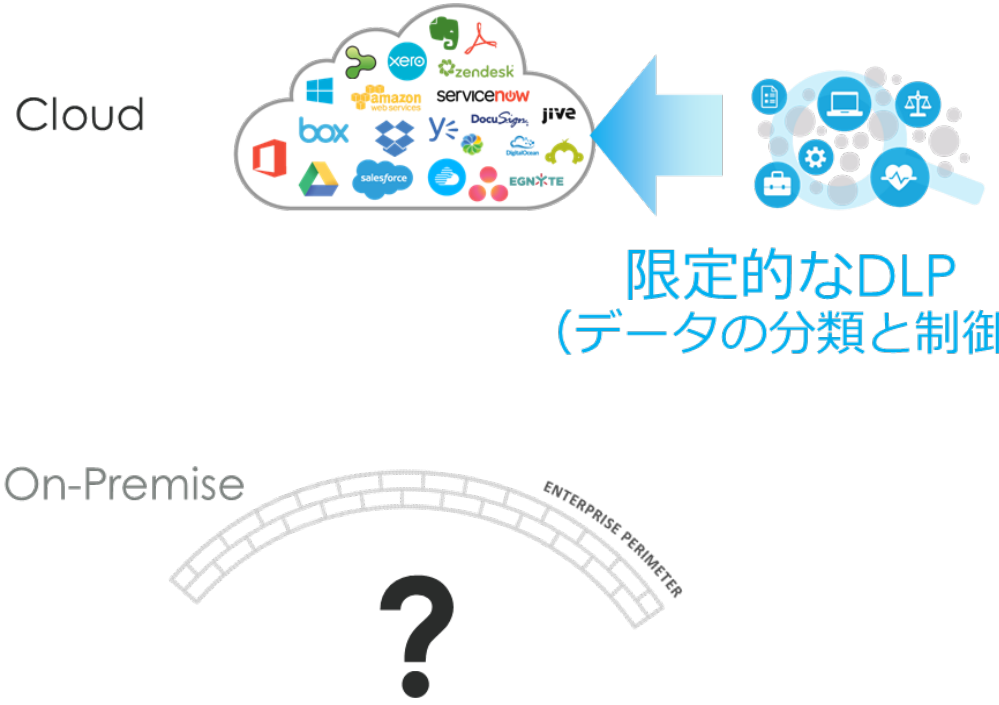
Symantec

○ 欧米欧州



データ取扱いに対するポリシー

○ 日本（ほとんどのケース）



製品ではお客様の課題を解決できません

＋統合化基盤による運用負荷最小化

＋サイバー攻撃対策とデータ保護の両立

**信頼できる
セキュリティ
統合ベンダーの
選択**

＝投資効果をもたらす
セキュリティ基盤の構築

各セキュリティ対策の評価ポイント

シマンテックのプラットフォームは確かな技術の上に成り立っています

対策	サイバー攻撃対策	情報流出対策	インシデント対応
評価ポイント	**脅威インテリジェンスの質と量** 既知の脅威情報の量はもちろんのこと、どのようなロジックで未知の脅威を検出できるのか（質）？	**多様なデータ形式に対応したDLPエンジン** 様々なデータ形式（テキスト、文章、画像、データベース、フォーム等）に対応したDLPエンジンか？	**ユーザとデータのふるまい検出の網羅性** 企業の境界線を越えたユーザやデータを漏れなく可視化し、適切なリスク分析に対応できるか？
適用先	→ ウェブ、メール、CASB → エンドポイント → サンドボックス → フォレンジック → SSL可視化など	→ ウェブ、メール、CASB → エンドポイント → 暗号化、本人認証 → フォレンジック → SSL可視化など	→ ウェブ、メール、CASB → エンドポイント → サンドボックス → 暗号化、本人認証 → SSL可視化など

3年後の未来予想図

クラウドシフトがセキュリティ境界線の延伸を加速する

CASB、DX化などの流れにより
クラウドシフトが加速

ユーザは場所関わらず
クラウド活用が必要に

流動的なデータに対して
企業は責任ある対応が急務

従来のログ分析だけでは
脅威がより見えなくなる

1 クラウドが業務基盤化

> US企業では平均10~20アプリを採用
> 企業の外向け通信はほぼSSL化へ
> 「見えない化」による事後対応増加

2 企業の境界線の延伸

> オフプレミス環境でのシームレスなセキュリティが必要に
（全方位のサイバー対策）

3 データガバナンスの強制

> 守るべきデータを正確に追跡、制御がビジネスを左右する
（コンプライアンス対応）

4 多角的なログ情報によるリスク分析

> セキュリティBI時代の到来（SOC-AI）

10 境界線の延伸

オンプレミス・クラウド・モバイルをつなぐSWG

Secure Web Gateway | SWG

リアルタイムURLフィルタリング

> **“今”のリスク**に基づくリスクを分析
> **ドメインに依存しない**正確なリスクの検知
> **誤検知・過検知の防止**とユーザ生産性の維持

多層コンテンツフィルタリング

> “二重”のアンチマルウェア分析で**誤検知低減**
> 未知のコンテンツに対して**静的分析と動的分析**
> エンドポイントへの**リスクを極小化**

マルチクラウドの可視化と制御

> 企業の定めた**信頼度に基づくクラウドの精査**
> **シャドーITの自動制御**とウェブフィルタ連携
> **デバイス・場所・ユーザに基づくアクセス制御**

境界線の延伸

オンプレミス・クラウド・モバイルをつなぐSWG

Symantec

Secure Web Gateway ｜ SWG

URLで判定

リアルタイムURL評価

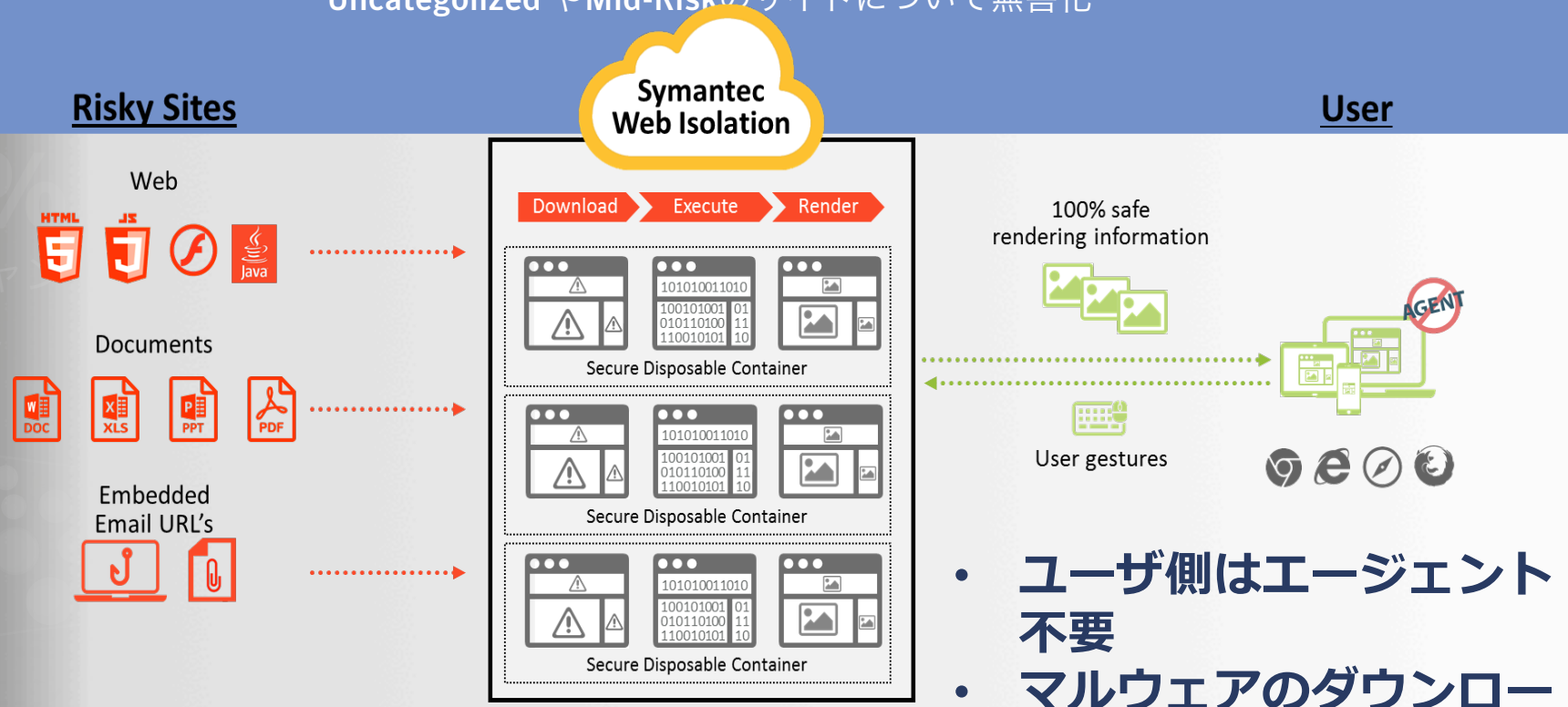
99.9%

の脅威ある

URLアクセスのブロック

コンテンツの無害化（Web分離）

Uncategolized やMid-Riskのサイトについて無害化



- ユーザ側はエージェント不要
- マルウェアのダウンロードによる感染リスク回避

2 リスクの可視化

見えないリスクを可視化し気づきを得る

Information Centric Security | ICS

データの自動認識（機械分析+タグ）

> **データの形式に応じた多角的な分析**で高精度な検出
> テキスト、文書、データベース、画像、フォーム
> 組織ごとに指定されたタグに基づいたポリシー試行

本人認証の徹底（ふるまい認証）

> ログイン時だけでなく**オンデマンドの認証実行**
> 機密データアクセス時、ふるまいリスク検知時
> **オフプレミス環境におけるデータ保護の実現**

データに紐づく暗号化

> DLPポリシーに応じたファイルの暗号化
> 暗号データと鍵の分離、**漏洩ファイルの無効化**
> **別名保存、第3者転送におけるポリシー強制**

データ可視化と検閲ポイントの連携

データの自動分類

DLP

CloudSOC™

本人認証

VIP

PGP

暗号化

ENTERPRISE PERIMETER

ファイル破棄

同僚

パートナー

顧客

ベンダー

3 対応の自動化

ユーザとデータに紐づくリスク対応の自動化

DLP
(Symantec DLP)

エンドポイント
(Symantec SEP)

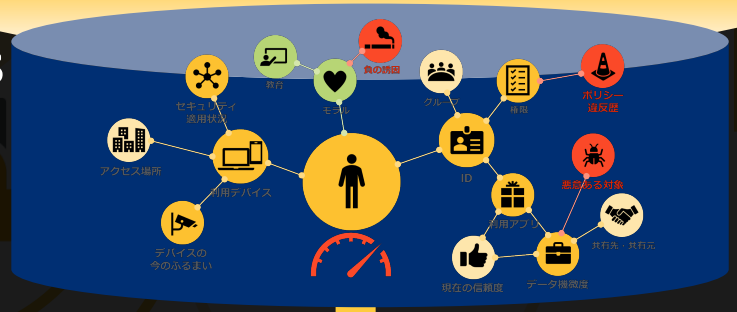
ウェブ
(Symantec CASB,ProxySG)

データ暗号化
(Symantec ICE)

ユーザ認証
(AD等)

SIEM
ネットワーク、その他セキュリティ製品ログ

Information Centric Analysis
| ICA



管理者

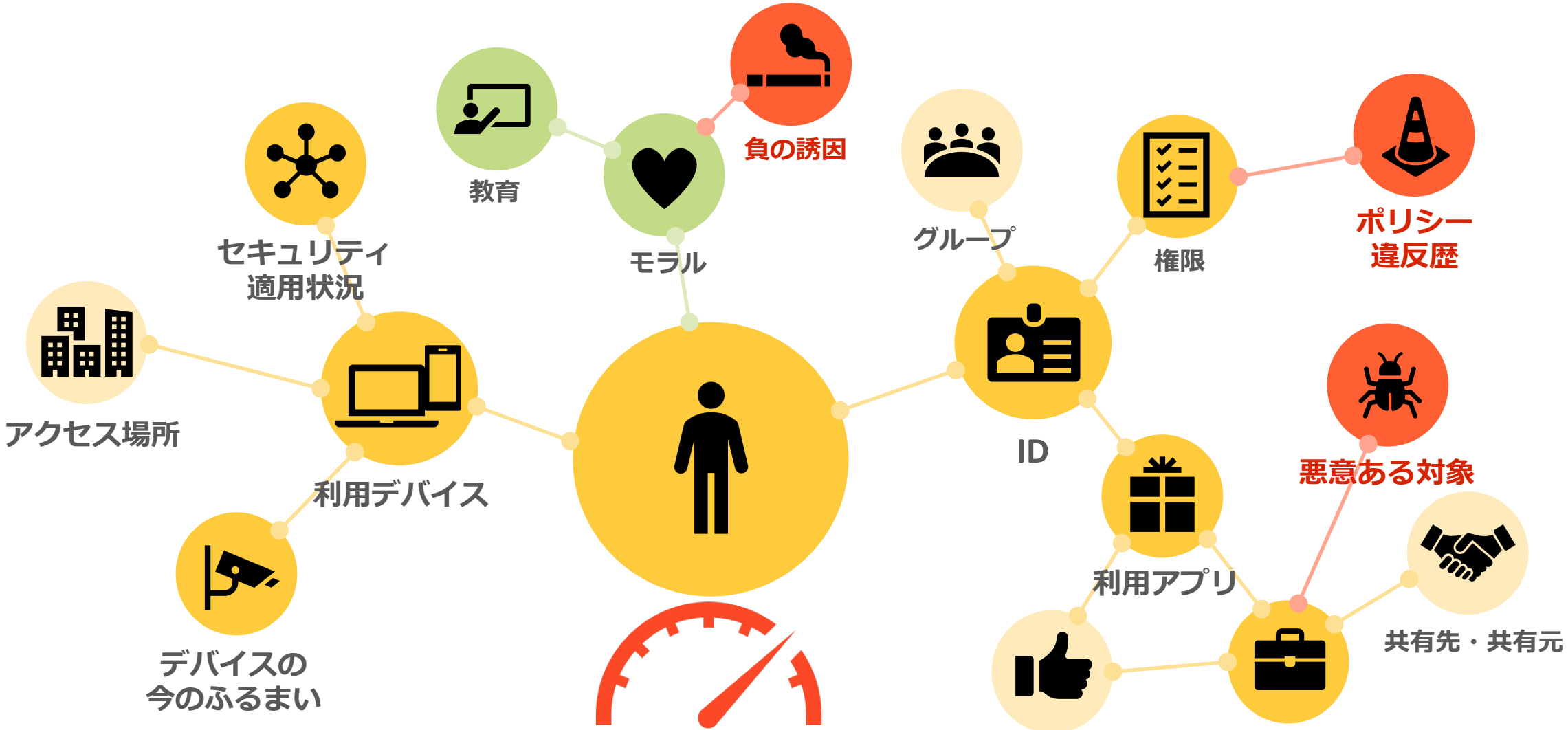
ブラックリスト追加
アップロード制御
暗号化・復号・追加認証

SWG

SEP

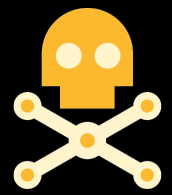
EDR連携
（ブラックリスト追加）
（隔離）

これからのセキュリティ（UEBA）



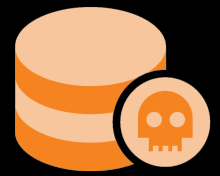
統合化基盤を目指したセキュリティ投資

インシデント
最新の攻撃
ビジネス継続性



サイバー攻撃対策

\?



情報流出対策

コンプライアンス
クラウドシフト
働き方改革

Security Platform

各センサーに対するポリシーの統合と
リスクの可視化・運用負荷最小化

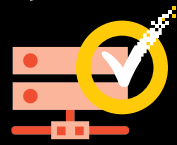
メール

ウェブ

クラウド

PC

モバイル



VM

統合化基盤（セキュリティプラットフォーム）で投資効果と運用負荷の最小化を実現

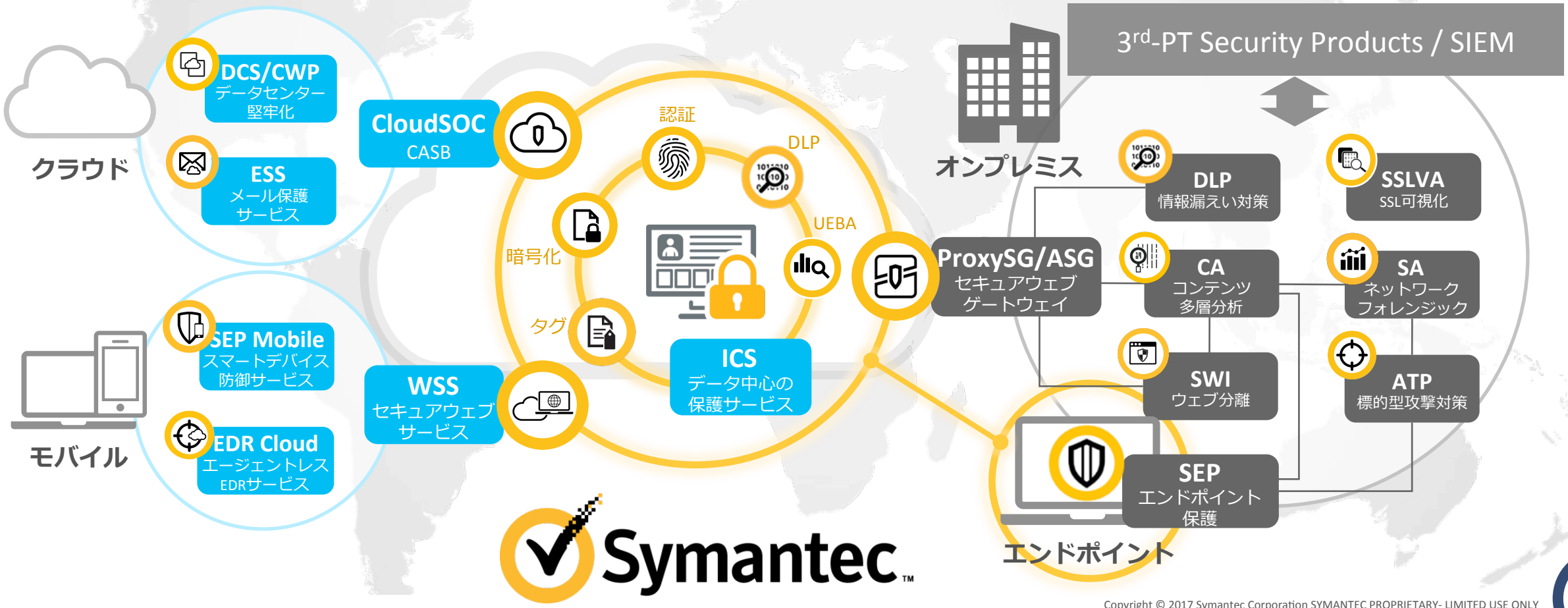
Integrated Cyber Defense | ICD Platform

ビジネス革新に沿ってセキュリティ境界線を延伸

運用支援サービス　クラウドサービス　製品

運用支援&インテリジェンス

- **GIN** 脅威インテリジェンス
- **CSS (MSS/IR)** セキュリティ監視・育成 インシデント対応
- **Premium Support** サイバーレジリエンス
- **Consulting** セキュリティコンサルティング 脆弱性診断



Symantec™

ICD Platformがもたらすメリット

複雑化するビジネス課題を解決し、ビジネスを加速化させる

サイバー攻撃対策

- ✓ SOC/CSIRTで対応が必要なアラートが最小化される
- ✓ 高いセキュリティレベルが本社・拠点・端末間で一元化される
- ✓ ゼロデイ対策がウェブ、メール、エンドポイントで可能に

情報流出対策

- ✓ あらゆる場所のデータが可視化され事前対応が可能に
- ✓ クラウドシフト加速化で利便性向上とコスト削減
- ✓ データの機微度やユーザのリスクに応じた制御が可能に

- ✓ エンドポイントはシングルエージェントでサイバー対策と情報流出対策が可能に
- ✓ 既存投資したセキュリティ投資からのフィードをリスク分析に活用し分析精度を向上させることが可能
- ✓ SOC自動運用へのシフトチェンジに対応できる統合化基盤の構築で先につながるセキュリティ投資が可能

お客様のビジネス革新をナビゲート

シマンテックは将来に繋がるセキュリティを提案します

オンプレミス・モバイル・クラウドを業界トップの技術でつなぐ。

お客様の財産である「データ」と「人」の保護とガバナンスを提供する。

シマンテックはお客様のビジネス革新をナビゲートします。

Symantec™

Thank You!