なぜ今、DLPが再注目されるのか ～クラウド時代のデータ保護戦略とNetskopeの最新アプローチ～

東京エレクトロン デバイス株式会社

CN BU　CN技術本部
カスタマーサクセスデザイン部

講演者紹介

講演者紹介

大橋 賢

所属

東京エレクトロン デバイス株式会社
CNBU CN技術本部カスタマーサクセスデザイン部

主な役務

- Netskope導入時の設計/構築等の技術支援
- 導入後の製品満足度向上の為のカスタマーサクセス活動

経歴

- Network運用/設計/構築及びSOC等の経験を経て
  2022年よりNetskopeの製品担当として従事
- 30社以上のNetskope導入支援の担当経験あり
- Netskope上位資格 NSK-300を取得

なぜ今DLPが必要なのか

DLP(データ損失防止)市場の拡大
注目される情報対策

- DLPはセキュリティカテゴリーとして**2010年頃**から広く認知
- ここ数年市場として**年間平均約20%以上**の成長率
- 2029年までに**年間平均27.5%**の成長予測
- DLP未導入企業が多い**アジア地域で急速に成長**する見込み
- **データ侵害件数やデータ量の増加傾向**に起因して需要増加
- **リモートワーク、クラウドサービス利用拡大**も需要増加の一因

  オンプレミス中心→クラウド／エンドポイント中心へのシフト

出典：データ損失防止の世界市場レポート 2025
https://www.thebusinessresearchcompany.com/report/data-loss-prevention-global-market-report?

DLPはクラウド時代に再注目されるセキュリティトレンド

機密データに対して取り組むべき課題

データ侵害対策

データ流出

外部からの攻撃

規制への対応

国際規制：GDPR、CCPAなど

日本：個人情報保護法

金融：PCI-DSS、金融庁ガイドライン

その他：各業界のガイドライン

内部関係者の行動監視

悪意のある内部関係者

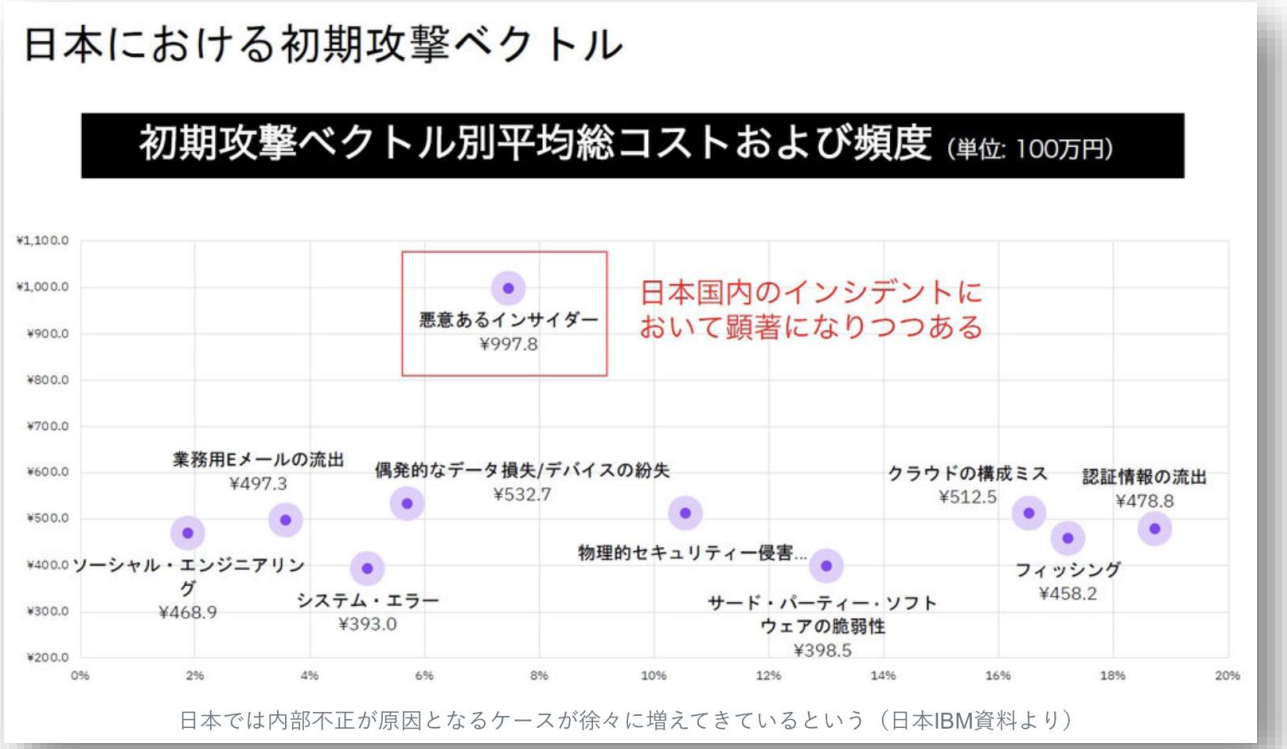
内部関係者による過失

日本のセキュリティリスク動向
内部からの情報漏えい対策の重要性

IPA 情報セキュリティ10大脅威2025

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

出典：IPA 情報セキュリティ10大脅威2025
https://www.ipa.go.jp/security/10threats/10threats2025.html



出典：2021/08　日本は内部不正によるセキュリティ被害が増えている--IBM報告書
https://japan.zdnet.com/article/35175707/

悪意あるインサイダーの他、
ユーザーに悪意がない漏えいもある

クラウド時代のDLP要件と Netskopeのアプローチ

従来のDLP課題

保護範囲が狭く情報漏えい経路を網羅できない

- 従来の境界型DLPではネットワークからアクセスする昨今の多様化した漏えい経路を制御しきれない

→境界型ではなくデータそのものを守る DLP が求められる

マルチポイントでバラバラ運用

- Email・Network・Endpointなどプロダクトごとにポリシー管理や設定画面が存在し、運用負荷が高い

→シンプルな設定構成でポリシーを一括管理できる運用が求められる

誤検知・過検知が多い

- 文字列ベース検知が中心で調整できる要素が少ない
- 正規表現による調整が必要となり、ルールが複雑化しやすい
- 正常な通信をブロックしてしまう等の業務影響

→ユーザー体験を損なわない運用が求められる

Netskope DLP の特徴・強み

包括的なカバレッジ

移動データおよび保存データについて、あらゆる重要なユースケースをカバー

最高水準のデータ保護機能

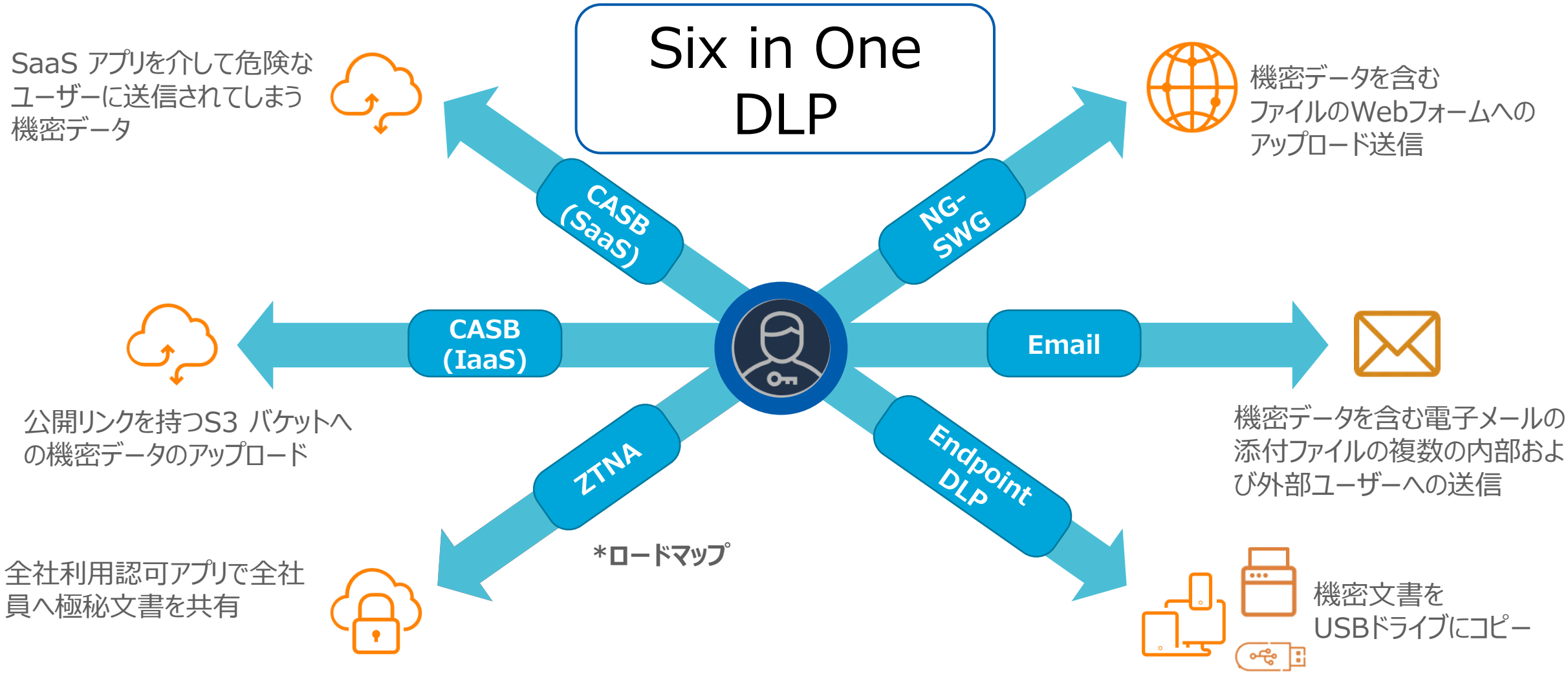
古くから日本語検知にも対応

誤検知を最小化し、手作業を削減。コーチングによるエンドユーザーとの摩擦を軽減

高い運用効率

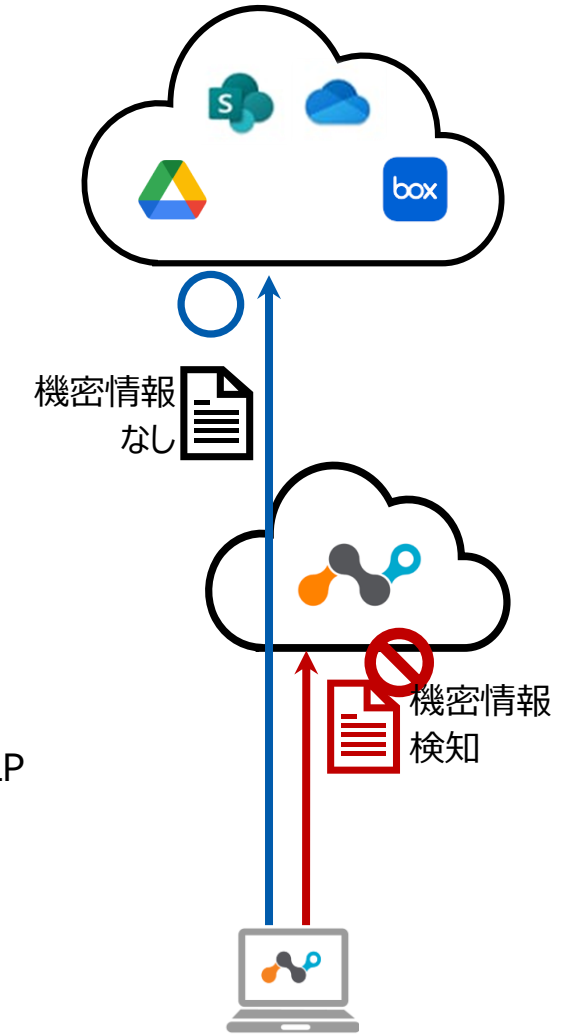
同じ検出ポリシーを複数のチャネルへ適応することで、異なるテクノロジーを導入することなく、生産性を向上

Netskope DLP – 包括的なユースケースをカバー



SaaS/Webに対するインラインDLP

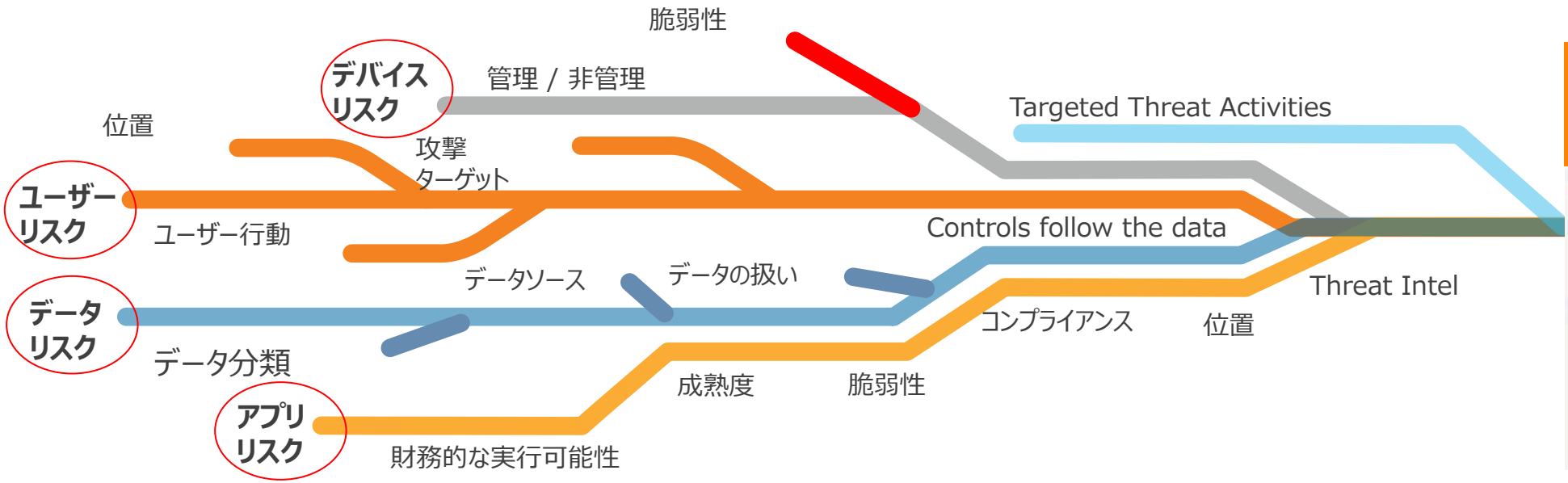
- **移動データ**に対するコンテンツのスキャンと制御を提供
- **主な機能/利用例**
  - クラウドストレージ利用時の機密データのアップロードを制御
  - 生成AIに機密情報を含む内容の投稿もしくはアップロードを制御
  - チャットツールに機密情報を含む内容の投稿もしくはアップロードを制御
  - Webメールにファイル添付する際に、機密データの添付を制御
  - Webフォームに機密情報を含む内容を入力して送信することを制御
- **Netskope 次世代SWGにネイティブに統合**
  - SWG/CASB機能と合わせてSaaS/Webに対する柔軟なDLPポリシーを設定可能
  - シングルエージェント、シングルコンソール、シングルプラットフォームで提供
  - Netskope CASBの強みである、アプリインスタンス識別とアクティビティ制御を組み合わせることでより精度の高いDLPポリシーの運用が可能
    - 他社インスタンスへのアップロードのみDLPポリシーを適用するなど
  - アラート、ブロックだけなくコーチングによるユーザー利便性を損なわないアラートの仕組みを提供



柔軟なデータ保護ポリシー

アプリインスタンスやアクティビティなどリスクに応じたきめ細やかなポリシー制御が可能

ID	デバイスリスク	SaaSアプリ	アプリインスタンス	アプリリスク	URLカテゴリ	アクティビティ制御	ユーザーリスク	脅威	データリスク(DLP)	ポリシーアクション
Pat Smith	管理 私有/BYOD	Google Drive 認可 非認可	企業 個人	93 高レート(低リスク) 8万以上のアプリ	クラウドストレージ 130以上のカテゴリ	Upload Share Create Delete Move Download (120+)	↓863 行動分析(中リスク) (UEBA)	脅威防御 AV Sandbox IPS ML CTE	GDPR AU Privacy Act 3500以上の識別子	コンテキスト: Allow Coach Block Encrypt Legal Hold Quarantine



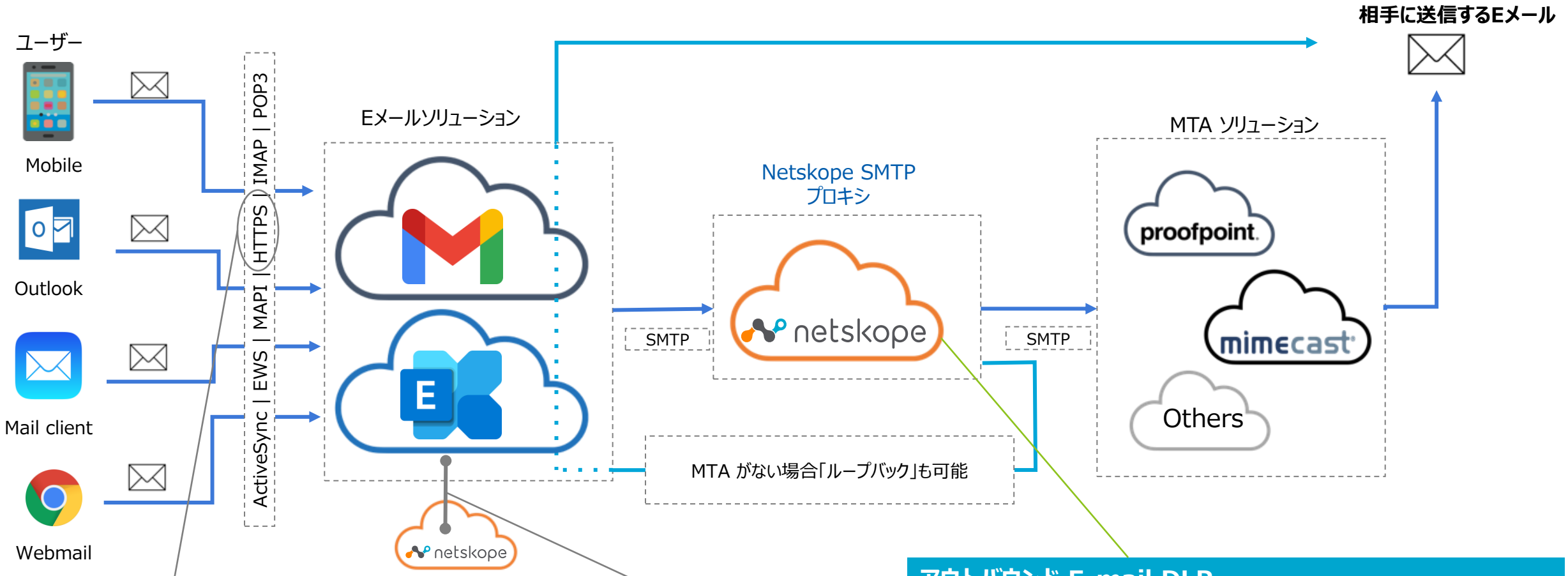
リアルタイムでのカスタマイズ可能なユーザーコーチング(ユーザー通知)

東京エレクトロン デバイス

API による保存データの分析・制御

- SaaSの**保存データ**に対するコンテンツのスキャンと制御を提供
- **主な機能/利用例**
  - 保存データの分類
  - 機密データが含まれるコンテンツに対して、アクセスできるユーザーを制限、公開リンクを削除、ファイル隔離、BoxラベルやMPIPラベルを付与などのアクション
- **SaaSの保存データに対して詳細な可視化と制御が可能に**
  - アップロードや編集されたファイルにDLPスキャンを実行し、アラートや所有者の変更、アクセス制限などのアクションが可能
  - SaaS アプリで行われた変更 (アップロード、ダウンロード、削除など) などの監査が可能
  - すでに保存済みのファイルに対して遡及スキャンを実施することで、保存データの分類が可能
  - インベントリとダッシュボードによりファイル種別やDLP違反ファイル、外部ユーザーなどのさまざまなエンティティに関する深い洞察を提供

Email に対するDLP

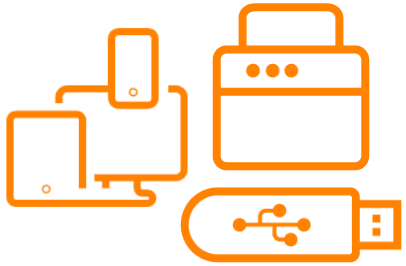


インラインDLP
- HTTPSで送信されるWebメールへのコンテンツチェックと制御
- リアルタイムでのブロック可能

API Protection
- 送信フォルダにあるメールに対してコンテンツチェックとアラート

アウトバウンド E-mail DLP
- Netskope SMTPプロキシによるリアルタイムDLP
- 管理、非管理端末でのアウトバウンドメールを保護
- ブロックだけでなく、Eメールソリューションと連携した上長承認なども可能
- Microsoft Exchange、Gmailに対応

エンドポイント DLP



- デバイス制御ポリシーにより、USBストレージやローカル/ネットワークプリンタがエンドポイント上で動作する方法を管理
- 高度なコンテンツ制御ポリシーと既存のNetskope DLPルールが活用可能

主な機能

- 軽量な単一Netskopeクライアントとクラウドベースの検査機能
- 統一ポリシーエンジン、アラート、レポート、インシデント管理を活用可能
- エンドユーザーデバイスのUSBデバイス保護を実現し、許可されていないUSBストレージデバイスの使用を防止
- ローカルおよびネットワークプリンタのデバイス制御ポリシーにより、エンドポイントでの動作許可方法を管理
- MPIPラベルの読み取りが可能
- デバイス分類を伴うポスチャーチェックルールにより、デバイスの管理対象/非管理対象ステータスを判定
- Windows および Mac デバイスをサポート

主要ユースケースご紹介

Netskope DLP の主な技術機能

- 3500種類以上の事前定義データ識別子
- 1800種類以上のファイルタイプに対応（データ構造による真のファイルタイプ検知）
- 日本語検知（日本語文字コードUTF-8、Shift-JIS対応）
- 暗号化やパスワード保護されたファイルの判別、MPIPラベルの識別
- 埋込みコンテンツの検出 (Word ファイル内の Excel)
- テキストおよびメタデータの抽出 (分類タグ、ウォーターマーク、など)
- 正規表現、辞書ファイルに基づいたカスタムのデータ識別子（事前、カスタム辞書対応）
- 標準MLによるレジュメ、ソースコードの検知
- フォレンジック: クラウドストレージへの検体(メタデータもしくは実データ)の保存
- アラート、コーチング、ブロック、隔離などのアクションに対応

さらに高度なDLP検知オプション

- OCR検知: 日本語未対応（ロードマップ）
- 完全データ一致(Exact Data Match)
- フィンガープリント検知: フォーマットの学習
- 高度なMLによるドキュメント/イメージ分類

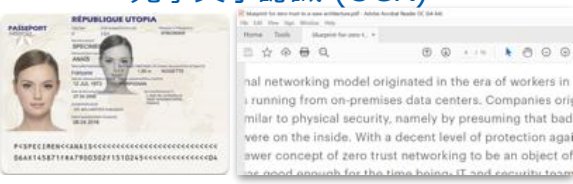
データ識別子 + 近似

11 22 33 0 440

SSN 1771-88-3003

099011 5555

光学文字認識 (OCR)



ML ドキュメント&イメージ分類

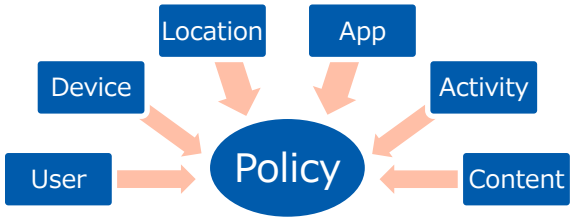
Exact Data Matching (EDM)

First Name	Last Name	Address	Zip Co	Phone	SSN	Account
John	White	12 First St	90100	101-11-1010	xxx-xx-1010	12345
Mark	Brown	5 Second Ave	95200	202-22-2020	xxx-xx-2020	12346
Olivia	Red	18 Large Circl	98500	303-33-3030	xxx-xx-3030	12347
Jake	Green	22 Main St	93202	505-55-5050	xxx-xx-4040	12348

source content → generate hash → perform match

フィンガープリント

コンテキストに基づくポリシー

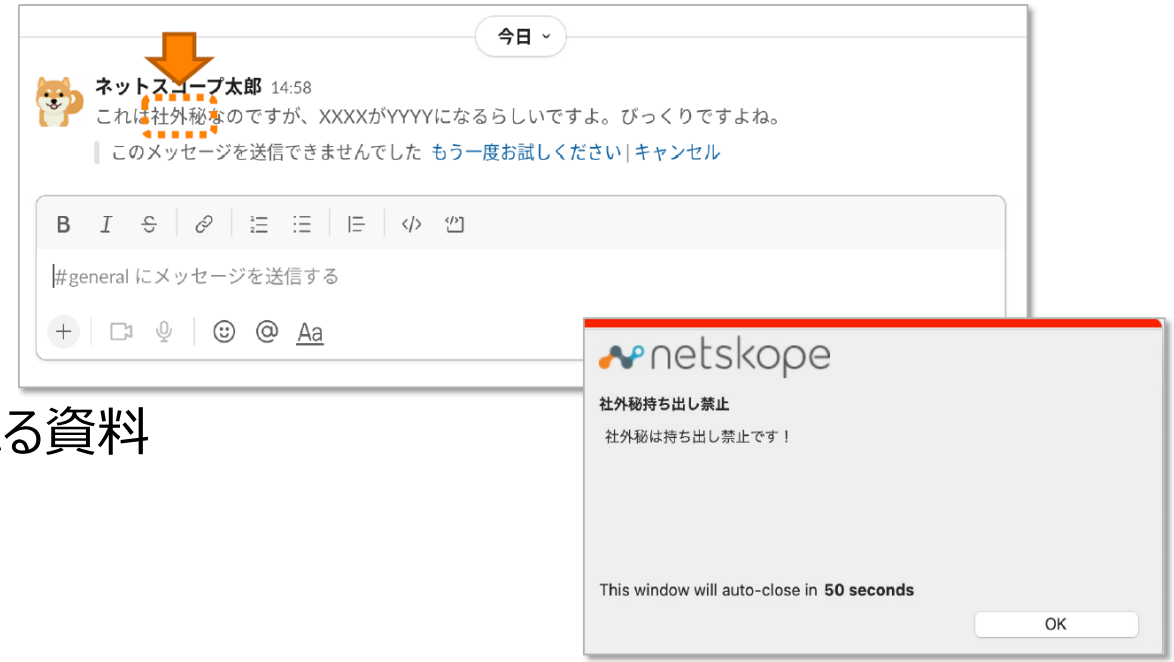


東京エレクトロン デバイス

DLPの検知方法
識別子によるデータ検知

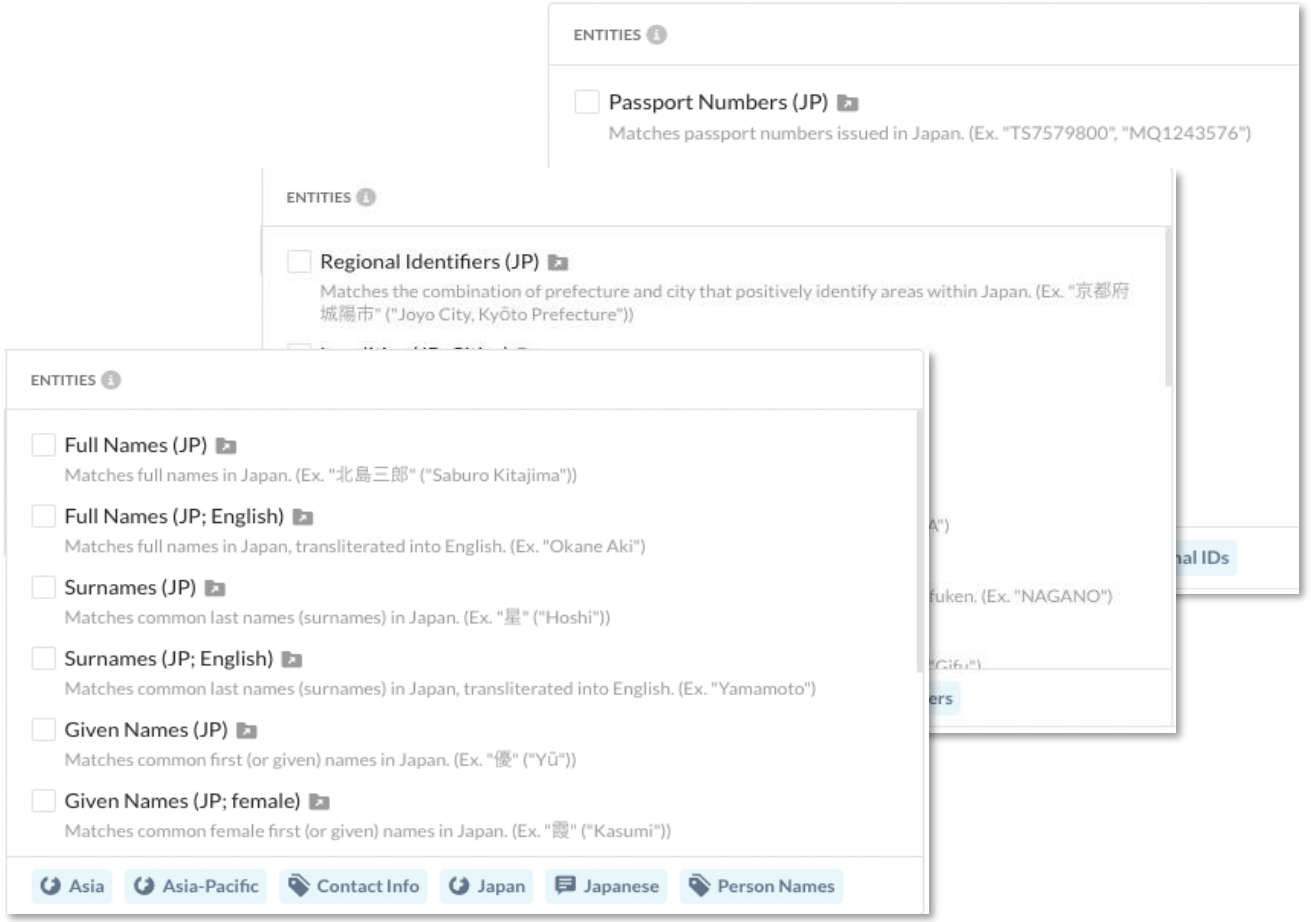
- **事前定義されている識別子**による検知
  - マイナンバー：775494886040
  - 住所：福岡県福岡市
  - 姓名：山田　太郎
  - クレジットカード番号：378282246310005

- **カスタムで定義する識別子**による検知
  - 「社外秘」「Confidential」といったキーワードが含まれる資料
  - 顧客番号：182983 (数字6桁)
  - 口座番号：2721838 (数字7桁)
  - キーワード、正規表現での定義が可能



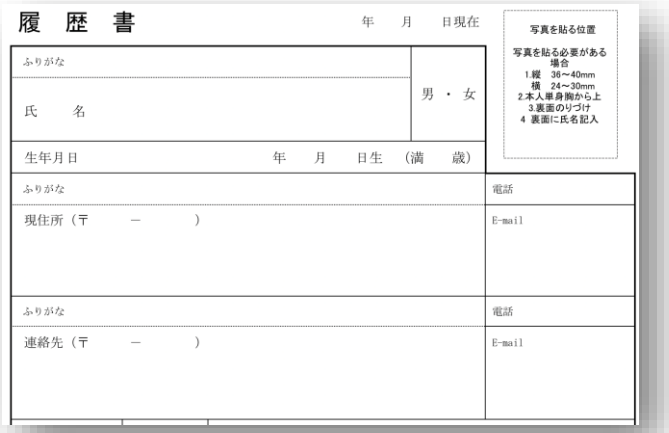
DLPの検知方法
豊富な事前定義識別子

- 3,500種類以上
- **日本に特化した事前定義識別子** の例
  - マイナンバー
  - クレジットカード番号(JCB含む)
  - 姓名（日本語含む）
  - 郵便番号
  - 住所（日本語含む）
  - 日付（令和など）
  - 運転免許証番号
  - パスポート番号
  - 法人番号



DLPの検知方法
さらに高度なデータ検知

- **フィンガープリント**
  - フォーマットを読み込ませて機械学習。内容が入力されたデータに対して類似性を見て検知


履　歴　書

年　月　日現在

写真を貼る位置

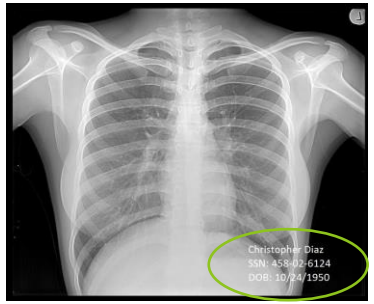
写真を貼る必要がある場合
1.縦　36～40mm
横　24～30mm
2.本人単身胸から上
3.裏面のりづけ
4 裏面に氏名記入

ふりがな
氏　名
男・女
生年月日　年　月　日生（満　歳）
ふりがな
現住所（〒　－　）
電話
E-mail
ふりがな
連絡先（〒　－　）
電話
E-mail

- **Exact Data Match (EDM)**
  - 顧客データ（顧客番号、氏名、メールアドレスなど）をハッシュ化し登録。その内容に一致するデータを検知

顧客番号	氏名	メールアドレス
185244	山田 太郎	ytaro@email.com
194064	鈴木 花子	shanako@email.com
256890	佐藤 一郎	sichiro@email.com
266789	山本 二郎	yjiro@email.com

- **OCR**
  - 画像の中にある文字を読んで検知



- **マシンラーニングによるイメージ分類**
  - パスポート、クレジットカードなどのイメージを検知

東京エレクトロン デバイス

まとめ

本セッションのまとめ

なぜ今 DLP が必要なのか

- 内部不正/過失による情報漏えい件数は増加傾向でありセキュリティ対策として検討すべきテーマ
- クラウド/エンドポイント中心のネットワーク構成でも対応可能な情報漏えい対策が必要
  →データは境界の外側で動くのが当たり前になった

クラウド時代のDLP要件

- 境界型ではなくデータそのものを守る DLP
- シンプルな設定構成でポリシーを一括管理可能
- ユーザー体験を損なわない運用

Netskopeのアプローチ

- エージェント型でネットワーク構成に関わらずデータ移動を検知(API連携による保存データの保護も対応可能)
- 統一されたプラットフォームでSaaS/IaaS/Web/Endpoint/Emailを包括的にデータ保護
- コーチングによる実運用しやすいデータ保護機能

東京エレクトロン デバイス株式会社