netskope

ホワイトペーパー

クラウドにおける データ保護戦略の立て方

継続的なリスク管理を実現する データ保護の進化

過去10年の間に、データは企業にとって最も強力なツールの1つになった

データは、イノベーション、目的の達成、そして最終的なビジネスの成功の原動力となっています。データの収集、分析、解釈を行える企業は、社内外の戦略的意思決定に役立つインサイトを入手、活用することができます。

Netskopeはデータを単なるツールではなく、企業にとっての付加価値を創出する資産と考えています。企業は顧客にサービスを提供し、その過程のビジネスプロセスや顧客とのやりとりの中で、業務に必要なデータが発生します。データがなければ実行可能なビジネスプロセスも生まれません。その結果、顧客にサービスを提供することができなくなります。競争力維持、顧客や社員の個人情報保護、安定した精度の高い業務の継続にはデータ保護が不可欠です。

その一方でデータの量は爆発的に増加しており、管理や保護がさらに困難になっています。そのため、データセキュリティに新たな方法で取り組む必要があります。

データ保護とは、データの作成から処理、修正、送信、消去に至るまで、データのライフサイクル全体でデータを保護するプロセスです。しかし従来の方法は、デジタルトランスフォーメーションの時代には適していません。

DCによると、2025年までに世界中のデータ量が61%増加

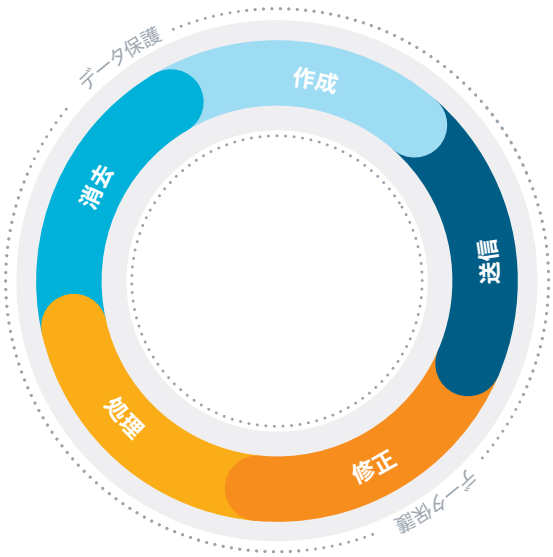

図1：データのライフサイクル

データ保護の推進要因

現在のデータ保護には5つの主要な推進要因があり、企業はそれらをすべて理解しておく必要があります。
クラウドでもクラウド以外のデータにおいてもこれは共通で、より良いデータ保護戦略には不可欠となっています。

5つの推進要因：

01

データの保存場所を把握する

ローカル、クラウド、サードパーティなど、情報をどこに保存しているかを確認し、管轄のデータプライバシー要件を理解してデジタルリスクを正確に見極める。

02

データの機密性を把握する

データの機密性、ビジネス上の重要性、許可されていない誰か（一般公開を含む）がデータを取得、もしくはデータが修正、破損した場合のビジネスへの影響を理解する。

03

エコシステム全体で**データフロー**を把握する

データの流れを理解し、権限を持つユーザーによるアクセスだけを許可することで、管理下にない場所や保護されていない環境へのデータの送信を防ぐ。

04

データにアクセスできる対象を把握する

サードパーティサプライヤー、パートナー企業など、データにアクセスできるユーザーを把握する。アクセス元（マシンおよび人）のIDを特定し、不正アクセスが行われていないかを確認する。

05

データの保護が適切かを把握する

どのような制御でデータを保護しているかを把握する。設計通り機能しているか、効果的に運用されているか。

環境と状態

現在、データは大きく分けてオンプレミスとクラウドという2つの環境に置かれています。データトランスフォーメーションによって大きな変化が生まれ、オンプレミスデータからクラウド（特にパブリッククラウド）への移行が急増しています。企業はクラウド環境による運用コストの削減、ユーザーエクスペリエンス（そしてパフォーマンス）の向上、パートナー企業やサードパーティとのコラボレーションの促進効果を期待しています。Netskopeの調査によると、多くの企業でWebゲートウェイトラフィックの50%以上がクラウドサービスやアプリケーションに関連していることが判明しています。データセンターやオンプレミスでデータを管理していた頃と比較すると驚くほどの変化と言えます。またユーザーの83%が個人用のアプリインスタンスを企業貸与の管理デバイスで使用しており、会社の機密ファイルを毎月平均20も個人インスタンスにアップロードしていることが明らかになりました。

この傾向は今後も増え、企業が自社内でデータセンターを管理する必要性はますます減少します。したがって、企業は**今すぐにクラウドデータ保護戦略を立てる必要があります。**

多くの企業でWebゲートウェイを通過するトラフィックの50%以上がクラウドサービスやアプリケーション関連

オンプレミスとクラウドという2つの環境内で、移動中のデータ、保管中のデータ、メモリー内のデータという3つの状態で使用されています。環境や状況に合わせてアプローチも変わり、データ資産に対する企業のリスク許容ルールの範囲内でリスクを適切に管理しなければなりません。

オンプレミスとクラウドでのデータ保護の違いとは

クラウドとオンプレミスでは異なるアプローチでデータを保護する必要があります。クラウドにデータがあると、アクセスするたびにパブリックネットワークでアクセスすることになるためデータ流出のリスクが高まります。一方オンプレミスデータは多くの社内業務において、イントラネット経由でアクセスできます。

このようなデータのユニバーサルな可用性とアクセシビリティが高い環境によって、BYOD（Bring Your Own Device）の使用やWFH（Work-From-Home：在宅勤務）が増加しました。その結果、攻撃対象領域が拡大し、制御において目に見える状態で最前線に立って保護してくれていた「境界線」もなくなります。

物理的なセキュリティ、バックアップ、災害復旧などの対策はデータ保護において重要であることに変わりありませんが、クラウドに保存されたデータについては（一般的に）CSP（Cloud Service Providers：クラウドサービスプロバイダー）が保護責任を負っているためCSPとの間でセキュリティ共有モデルが必要になります。このモデルを十分理解した上で、ニーズに合った適切なサービス実装についてCSPと合意しておかなければなりません。

企業の**95%**が個人のデバイスを職場で使用することを許可している。
（出典：Cisco）

オンプレミスデータとは異なり、クラウドデータはAPIリクエストやJSON（クラウドでの言語ともいえます）でアクセス、操作します。そのため使用するセキュリティツールは、このクラウド言語を理解できることが必須条件になります。これにより適切なアプリケーションの制御が可能となり可視性も向上します。従来のオンプレミスソリューションではクラウドトラフィックを把握できないためこういったことは不可能でした。これは制御スタックによるJSONの復号化、APIリクエストの読み取りが必要なことを意味します。このように高度な検証機能がなければコンテキストを適切に理解することができません。ここで言うコンテキストとはデータ分類、ユーザーアクション、アプリケーション間のトランザクション、ユーザーの不審な振る舞いやデバイスの種類といった情報を指します。コンテキストを理解できなければ、ポリシーの適用や制御が適切に行えなくなり、企業はクラウドサービスを十分に活用できなくなります。結果、デジタルトランスフォーメーション戦略に支障をきたしてしまいます。

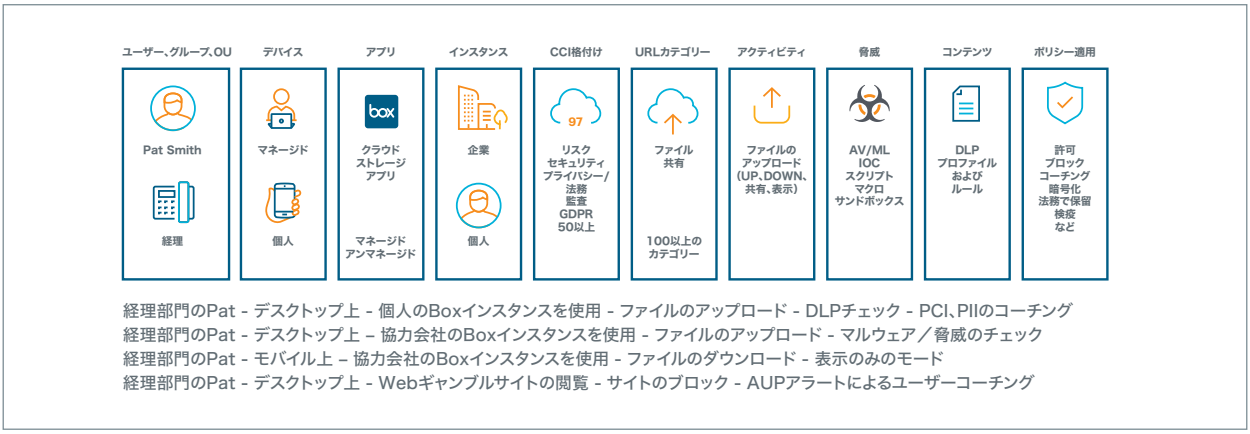

図2：Cloud XD

クラウドベースのシステムには特有のセキュリティリスクがあります。静的IPアドレスや一定数のリソースを持つオンプレミスシステムとは異なり、クラウドでは新しいリソースが常に起動、停止されます。したがってリソースは本質的には動的であり、簡単な設定ミスが非常に大きなリスクにつながることがあります。実際にNetskopeの脅威研究でも、IaaSとPaaS環境での設定ミスがデータ侵害を増加させる主な要因になっていることが明らかになりました。

クラウド内にデータがあるとCSPにデータを預けることになり、サードパーティリスクが高まります。しかしデータ保護に対するセキュリティ対策だけでなく、規制コンプライアンス要件を満たすためにもCSPに任せることになりますが、CSPのほうが環境を安全に管理するためのスキルや能力が高いので、企業の全体的な技術的リスクが軽減します。特にパッチ適用や最新テクノロジーの活用など、基本的な対策についてはCSPのほうが優れています。CSPに移行することで、多くの企業が苦戦していた基本的な対策を大幅に強化することができます。

2020年に発生したデータ侵害のうちの22%がエラー（間違い）による侵害で、設定ミスが最も急増したエラーだと判明した。[1]

[1] 出典：Verizon 2020 Data Breach Investigations Report

マルチクラウド環境

「卵を一つのカゴに盛るな」ということわざはデータセキュリティにも当てはまります。複数のCSPにデータやシステムを分散させる判断を下す際にはある種のトレードオフが必要になります。データやシステムを複数のネットワークに分散することで攻撃対象領域が拡大しますが、データ侵害や特定のCSPによるサービスデリバリー障害の影響を軽減することができます。

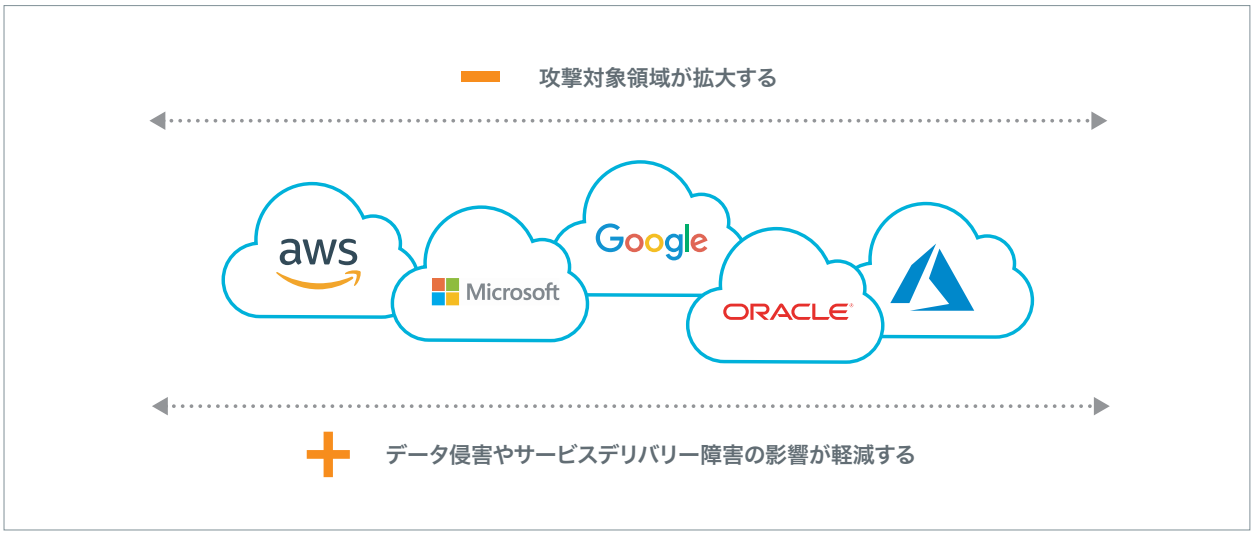

図3：複数のCSPにデータを分散する際のトレードオフ

システムを複数のCSPに分散することでいくつかのメリットがあります。たとえば多種多様なツールのアクセス、コスト最適化、冗長性の向上、データ侵害時の影響軽減などです。しかしマルチクラウド環境では攻撃対象領域が拡大してしまうため、セキュリティ対策を講じる必要があります。社内で使用されるクラウドベースのSaaSはさらに攻撃対象領域を拡大する可能性があるため、セキュリティ対策の一部として検討しなければなりません。

セキュリティ共有モデルでは使用するクラウドサービスが増えるたびに複雑性が増します。各サービスに固有の脆弱性があり、企業のセキュリティチームによる検討が必要です。そしてデューデリジェンスと呼ばれる精査を行い、サービスプロバイダーのセキュリティ体制が企業のリスク許容度と規制コンプライアンス要件の両方を満たしていることを確認しなければなりません。

マルチクラウド環境では以下が求められます。

1. **社内で使用しているすべてのクラウドサービスを確認する：**サービスプロバイダーとの間でやり取りされるデータのセキュリティを考慮しないまま、SaaSソリューションを導入して様々な部署がビジネス目標を達成しようとしています。こうしたサービスをできるだけ迅速に特定して、適切な制御を実施する必要があります。
2. **様々なクラウド導入環境におけるセキュリティ設定とポリシーの一貫性を確認する：**社員に対してシンプルかつ一貫したセキュリティを提供することができます。

3. **SaaSソリューションの迅速な導入、入れ替えによって、セキュリティチームは必要なセキュリティを確保することが困難になることを認識する：**頻繁な変更は、手作業での処理による設定ミスも多くなります。この問題を解決するためには、以下のようなメリットを提供する自動セキュリティプロセスを実装する必要があります。
    a. エラー／設定ミスの可能性が低くなり、一貫性が高まる
    b. ポリシーと監視用ツールの導入スピードが格段に上がる - 効率改善
    c. 手動では煩わしかった反復作業をプロセスが行い、セキュリティチームが本来の業務に専念できるようにする
4. **使用中のクラウドサービス全体で可視性を向上する効果的なツールを活用する**

情報セキュリティ領域と情報セキュリティ規定について

以下の図は従来の情報セキュリティ規定で包括的なデータ保護アプローチに必要な側面や領域を示しています（すべてを網羅しているわけではありません）。

各領域が１つの規定になっています。企業はこのような様々な領域の機能を開発し、環境、状況に基づき、前述にある５つのデータ保護推進要因に沿って自社に適したデータ保護機能を実装する必要があります。

実践的かつ段階的なクラウドデータ保護

ステップ1: データの保存場所を把握する — データディスカバリー

企業が処理するあらゆる構造化／非構造化データのディスカバリー／検出／場所特定というプロセスです。データは企業のハードウェア（エンドポイントデバイス、データベース）、社員のBYODまたはクラウドに保存されています。

データ（移動中と保管中のデータ）ディスカバリーに役立つツールが多数ありますが、オンプレミスかクラウド、どちらにのデータかによって使い分けが必要になる場合もあります。このプロセスはすべてのデータを把握、保護するためのものです。**データセントリックな保護アプローチの核**を成し、自社データをすべて網羅したインベントリを作成する必要があります。このインベントリは総合的なデータガバナンス戦略とプラクティスに不可欠な情報です。

情報資産は常に変化しています。常に新しい資産が追加されているため、静的なリストはすぐに古くなり、不要となります。データディスカバリーのプロセスを確立は自動で行う必要があります。自動化は情報資産を常に表示し、リスクを効果的に管理できる唯一の方法です。

ステップ2: データの機密性を把握する — データの分類

発見したデータは分類する必要があります。データ分類とはデータの内容を分析し、PII、PHIなどの機密データを検索して、適切に分類するプロセスです。一般的には3〜4のレベルで分類されます。

3レベルのポリシー：

公開
社外秘
機密

4レベルのポリシー：

公開
社外秘
機密
極秘

ポリシーを作成後、データ自体にもメタデータ内にタグを付けます（これがデータ分類ポリシーの実装です）。以下は従来のアプローチ例ですが、この作業は複雑で、精度が低くなることがよくありました。

- ルールベース
- 正規表現、キーワード照合、ディクショナリー
- フィンガープリンティングとIP保護
- 正確なデータ照合
- OCR（イメージデータからの文字識別）
- コンプライアンス遵守
- 例外管理

データ分類アプローチは日々進化しています。自社で作成、所有する膨大なデータを正確に分類したい場合は、新たな機能が必要です。たとえば以下の方法があります。

- マシンラーニング（ML）による文書分類と分析：事前に定義しておいたML分類子を使って自社のデータセットでモデルと分類子をトレーニングします（これによって企業は複雑なデータサイエンススキルがなくても分類子を作成することができます）。（Netskopeによる分析を参照）
- 自然言語処理（NLP）
- コンテキスト解析
- 画像解析と分類
- リダクションとプライバシー

いずれのアプローチも自動分類とプロセス統合のための、APIベースのクラウドネイティブなサービスに対応しています。これによって企業はプロセスとテクノロジー（モデルを含む）の使用やデータ分類のための機能を構築できます。こうして分類されたデータはその後、追加の検査が必要になった場合にデータポイントとして使用します。その結果、リアルタイムの自動分類機能が提供されます。

分類のエスカレーションと逆エスカレーションは検出したすべてのデータを分類するための一般的な方法です。未分類のデータオブジェクトに対して、デフォルトの分類を適用し、メタデータに挿入します（たとえば未分類の場合、デフォルトを「機密」または「極秘」に設定します）。数回のテストまたは一定の基準に従って、オブジェクトの分類を適切なレベルまで徐々にエスカレーション／逆エスカレーションさせます。これはゼロトラストの原則とも一致しています。ゼロトラストはデータ保護戦略の基本的な機能として急速に拡大しています。

（ゼロトラストに関する詳細は、こちらをご覧ください。Netskopeによる文書「What is Zero Trust Security?（ゼロトラストセキュリティとは）」でもご確認いただけます。）

「クラウンジュエル」探しと優先順位付けについて

データ分類は企業のクラウンジュエルを見つけるサポートするようなものです。ここでは企業にとって最も重要なデータへのアクセス、保存、転送、削除を行う資産を「クラウンジュエル」と呼びます。データセントリックアプローチでは機密性と重要性の両方を評価しながら、最も重要なデータを見極めることが不可欠です。このような作業にはデータ分類だけでは不十分です。

データの重要性を見極める実際のモデルでは、機密性を示す分類、完全性、可用性というセキュリティの3つの観点から、関連するポリシーや基準にそれぞれ1～4までのウエイト（加重）スコアを付けます。合計スコアが「12」（4+4+4）のデータオブジェクトは、機密性が高く、完全性に対する要件も高く、かつ高可用性が求められるものと判定されます。

ある企業が使用している一般的なシステムとウエイト判定の例を紹介します。

分類：
極秘 = 4
機密 = 3
社外秘 = 2
公開 = 1

完全性：
完全性が高い = 4
完全性は普通 = 3
完全性が低い = 2
完全性要件なし = 1

可用性（BCPと IT DRプロセスを基に判定）：
高可用性 = 4
RTO 0～4時間 = 3
RTO 4～12時間 = 2
RTO > 12時間 = 1

	分類	完全性	可用性	ウエイト（加重）スコア
銀行取引 	3	4	3	10
調達 	3	2	2	7
レポート処理データベース 	3	3	1	7
人事システム 	3	2	2	7
マーケティングデータベース 	2	2	1	5
総勘定元帳 	3	3	2	8

企業はリスク許容度に応じてデータオブジェクトに最高を「12」として合計スコアを設定できます。合計スコアが「12」であれば、データの機密性が非常に高く、完全性に対する要件が高く、かつ高可用性が求められることを示します。リスク許容度に従ってクラウンジュエルを示すスコア評価を設定できます。これによって非常に論理的できめ細かい方法で、制御や、必要に応じて修正作業の優先順位付けを行えます。設定されたスコアはそのデータを使用しているアプリケーション、システム、サードパーティに適用できます。こうすることで資産（アプリケーション、システム、サードパーティ）のグループ化ができ、「クラウンジュエル」となるかを判定できます。

ステップ3: エコシステム全体でデータフローを把握する — ユーザーとデータの間の検査ポイントになる

データは水のように自由に流れるものです。すべてのトラフィックを検査して以下を確認できるような可視性が求められます。

1. 重要性と機密性（データの分類）に基づき、移動中のデータを把握する
2. どこからどこに移動しているのか、移動元と移動先の環境はディスカバリープロセスと合っているのか、調査の必要な未知のデータレポジトリを検出しているか、最後のポイントは特に重要な点です。ビジネスプロセスの変化に伴い、データフローも変化します。企業はデータフローを常に監視し、新しいフローを特定したら適切なアクションを実施する必要があります。一般に以下のようなアクションがあります。
    a. 新たに検出した送信元／送信先（新しいSaaSアプリケーションやそのインスタンスの場合もあります）のセキュリティ制御または体制が、求めるセキュリティ基準に準拠していることを確認する
    b. データにアクセスできるようになった新たなサードパーティのセキュリティ制御または体制（そして結果的にはサードパーティ環境のセキュリティとなります）がセキュリティや個人情報保護規程に準拠していることを確認する
    c. 不正な、もしくはビジネスプロセスではない、修正が必要なユーザーアクションではないなど、データフローが適切であることを確認する
3. プライバシーや規制要件に反する可能性がある地理的または管理しているデータの移動だと特定できるかどうかを確認する

ユーザーとデータの間に、クラウド言語(API、JSON)を読み取れるクラウドネイティブな検査ポイントを作成することで、クラウド関連のあらゆるデータを識別できるデータディスカバリー機能が実現しました。さらにステップ2で説明した機能を活用して膨大な量のデータを非常に高い精度で自動的に、そしてリアルタイムに分類することができます。また、保存中のデータについてもこのような自動分類機能が必要です。データディスカバリーとデータ分類を自動化する方法は2つあります。一般的には保存中と移動中という両方のデータセットに対し自動分類エンジンを継続的に適用する必要があります。

これによってリアルタイムの分析と可視化が強化されます。これらはいずれもデータ保護に不可欠な要素で、セキュリティ運用チームの新たな武器になってきています。このような分析はSIEMの代わりにはなりませんが、効果的なセキュリティ分析、インシデント対応、サードパーティによるリスク管理に必要な作業を再定義するうえで役立ちます。この機能はクラウドデータの影響と依存性の理解に必要なあらゆる情報とインテリジェンスへのリアルタイムアクセスが可能であることを確認し、情報に基づくタイムリーな意思決定とアクションを実現するための軸となる要素です。

ステップ4: データにアクセスできる対象を把握する — 可視性の向上

ユーザーとデータ間のチェックポイントになることで、企業はデータがどこからどこに流れているかを把握できるだけでなく、データにアクセスできるID（マシンまたはユーザー）を把握することもできます。

これにより企業のIAM（Identity and Access Management：ID管理とアクセス管理）機能が強化されます。この情報を使用して、たとえばロールベースのアクセス制御の定義など、既存のIAMを検証することができます。また、異常を検知した場合は調査や是正作業の実施も可能です。これはエンドユーザーと特権アクセスの両方に適用されます。

このような可視性により、企業はデータとアプリケーションへのアクセスを最小限に抑え、リスクも最小化できます。詳細なアクセス制御はサイバー攻撃の被害を最小限に抑えるうえで不可欠です。

ステップ5: データの保護が適切かを把握する — ユーザーとデータ間のポリシー適用ポイントになる

保存中のデータ：クラウド関連のデータにおいて、AWS、Azure、GCPなどのクラウド環境のセキュリティ体制をスキャンおよび評価することが重要です、環境内の設定を検証することでデータ侵害を防ぐことができます。クラウド環境の設定ミスはデータ侵害の代表的な原因の1つです。セキュリティ設定のコンプライアンス監視はオンプレミスインフラストラクチャ向けに長年使用されてきた機能です。したがってこれをクラウドベースのIaaSとPaaSサービスに拡張する必要があります。

移動中のデータ：クラウド関連のデータにおいて、ユーザーとデータ間のPEP（Policy Enforcement Point：ポリシー適用ポイント）を設定する機能を確立する必要があります。（これはステップ3で説明した検査ポイントを論理的に拡張したものです。）

企業には現在いくつかのデータポイントがあり、コンテキストに基づいてポリシーを決定します。目的やリスクに合わせたアプローチによってアプリケーション制御が実現します。たとえば（推奨する方法です）データの重要性や機密性（分類を基に）を理解することで、最も高いレベルに分類されたデータ保護を最優先し、下から2番目のレベルに分類されたデータまで保護することができます。なお、一番下のレベルは一般に「Public」として分類されているため、対策はほとんど不要です。

リスクベースのデータポリシーアプローチ

データ保護ポリシーはコンテンツベースと目的ベースという2つの方法で作成できます。

コンテンツベースのプロセスでは機密性の高いコンテンツ（PHI、PIIなど）を識別し、適切なポリシーを適用することで社内ポリシーや規制コンプライアンスをサポートします。分類レベルに基づいて一括で適用できるため、高速で広範囲なプロセスとして活用できます。

正しく計画しておけばコンテンツベースのポリシーは適度に厳密であるため、データを分類したら、適切な状況下でのみアクセス／転送／編集／削除が可能になります。しかしポリシーが広範囲であるため、正当なアクションもブロックしてしまう可能性があります。それでも機密データの保護は不十分であるよりも、十分すぎるほどであるほうがよいでしょう。

適度に厳密なコンテンツベースポリシーにするため、企業はデータ監査を実施することができます。データ監査はきめ細かいプロセスなので時間がかかります。特定のデータオブジェクトの目的を識別して追加データの保護要件（必要な場合）を割り出し、適切な人が正当な方法でデータのアクセスや操作を行えるようにします。

条件付き承認

条件付き承認は安全性の高いアクセス制御につながります。特定のリソースにアクセスしようとしているデジタルIDだけでなく、環境（IPアドレス、時間帯、場所、デバイスなど）も考慮して許可を制限します。これにより悪意のあるユーザーが認証プロセスを突破できたとしても、不正アクションを阻止することができます。

条件付きの承認は通常ABAC（Attribute-Based Access Control：属性ベースのアクセス制御）で行われます。ABACではポリシーとルールが属性、サブジェクト（デジタルID）、リソース（アクセス先のデータ）、アクション（編集、読み込み、実行、削除など）、環境（IPアドレス、クラウドサービス、デバイスなど）という4つの属性に基づきます。

クラウド関連データに対するポリシーの定義と実装方法を検討する場合、データの使用方法に関するコンテキストを明らかにする**検査／ポリシー適用ポイント（PEP）をユーザーとデータの間に設けられる**機能（前述のような機能）を作成することが重要です。このような検査／PEPによってデバイス、SaaSアプリインスタンス、アプリケーションや環境内でのデータとのやり取り（特に削除、編集、共有など、具体的なコマンドの内容）を詳細に把握し、これを基に挙動が正常か異常かを判定します。

制御

定義されたポリシーに従って適用が不可欠で軸となる制御があります。この種の制御は定義済みの環境や状態にも適用されます。具体的には以下が挙げられます。

1. データの暗号化
2. データのマスキング
3. データのトークン化
4. デジタル権限管理を含むユーザーアクセス権の管理

これらはいずれも確立された制御で、市販のソリューションがあります。しかしこれらの制御を少なくともエンドポイント、Webトラフィック、メール、IaaS、PaaS、SaaS、クラウド以外のアプリケーション、メッセージアプリに適用できなければ意味がありません。そしてもちろん新しいデータフローチャネル（ステップ3に記載）にも適用しなければなりません。

エンドポイントにおける情報漏洩対策（Data Leakage Protection：DLP）について

エンドポイント（ラップトップ、デスクトップ、サーバー）には3つの不正侵入シナリオがあります。本書に記載しているような方法でデータを保護するには、自社の管理や制御機能の範囲内でこの3つのシナリオに対処する必要があります。3つのシナリオとはリムーバブルメディア（USBなど）、印刷物、コピー&ペースト／クリップボードです。

リムーバブルメディア

リムーバブルメディア（USBメモリ、外付けハードドライブなど）へデータを転送する際、は必ずログに記録し、転送をブロックするか、暗号化を実施します。暗号化を行う場合は、エンドポイント（またはエンタープライズ）データ保護機能と統合すれば、キーの管理、共有、復旧をスムーズに行えます。

印刷物

企業は一般にローカルプリンタの利用状況を把握したいと考えています。オフプレミスでは特にそうで、少なくとも監査証跡やログによって印刷内容、印刷者、データ分類を記録しておこうとします。エンドポイントセキュリティによってローカルプリンタを使用できる人を限定し、不正ユーザーによる印刷を阻止する必要があります。

コピー&ペースト

ユーザーがクリップボード機能でアプリケーションのコピー&ペーストを行ってデータが流出することもあります。こうしたシナリオに対しても同様なデータ保護ポリシーを適用し、デバイスの種類、データ分類、ユーザーに基づき、コピー&ペーストを禁止する機能など、必要な対策を講じる必要があります。

ゼロトラストとデータ保護

データは企業が価値を生み出すための資産のため、資産の保護は最重要事項です。データセントリックアプローチの必要性についてこれまでお伝えしてきましたが、そのためにはセキュリティ領域全体に多くのサービスや機能を実装する必要があります。このアプローチはデータが軸となって初めて活用できます（以下の図４を参照）。

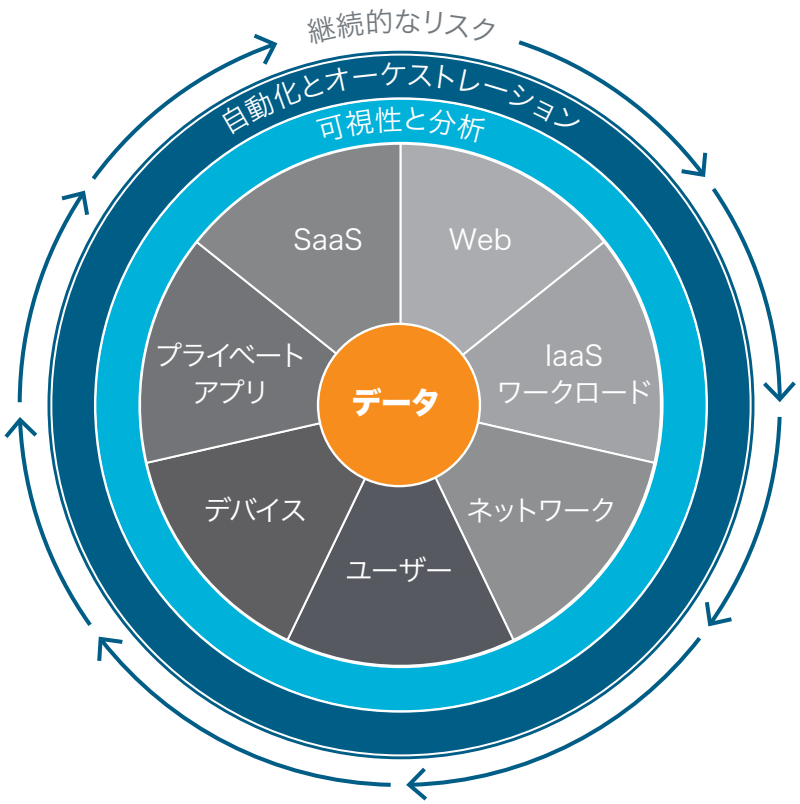

図4：継続的なリスク管理

ゼロトラストのコンセプトは業界全体で支持されています。ゼロトラストの最大のメリットは、正しく適用すれば機能や制御におけるエコシステムを確立できるという点です。このエコシステムを継続的に管理することで、潜在的なリスクを考慮しながら、ある時点で必要なアクセスを提供できる、すなわちリアルタイムの意思決定が可能となります。従来のアプローチとの違いは、ユーザーやサードパーティの運用環境をかつてないほど詳細に把握できるようになったことです。ユーザーの振る舞い、データの機密性と重要性、エンドデバイス、環境に潜む脅威、使用しているアプリケーションのリスクについて詳細かつ継続的に（最も重要です）把握できるようになりました。

ゼロトラストは「デフォルトでブロックする」というスキームを採用しており、明示的に許可された場合に限りアクセスとアクションが認められます。現在提供されている多くのデータポイントで得た情報に基づき、リスク計算を行いアクションやアクセスを許可するかの判断を下します。データポイントを継続的に評価し、リスク計算に基づいてポリシーも常に更新します。このようなアプローチによってデータ資産の攻撃対象領域を常に最小に抑えることができます。ユーザー、デバイス、アプリ、データ間の相互作用を把握できるため、データの機密性、アプリやユーザーの振る舞いによるリスク、その他の要因に基づいてアクセス制御を条件付きで定義、実施することができます。その結果、継続的なリスク管理による全体的なセキュリティ強化につながります。

データ保護の未来

爆発的なデータの急増、今後さらに広がる相互接続した社会とそれを支えるサービスの高速化、これまでにない速さで増加しているデバイスという状況下で、データ保護の課題は引き続き存在し、深刻になっていきます。しかし希望が見えないわけではありません。

データをほぼリアルタイムに自動分類する方法として、AI/MLとNLP（Natural Language Processing：自然言語処理）の分野が今後も大きく進化することとなります。AI/MLの観点からPIIデータ分類について考えてみましょう。PII検出で難しいことは機密情報（生年月日など）の属性を正確に設定する作業です。英語で一般的な用語の多くが、人の氏名としても使われているためです。

その結果、文書を処理する場合に主語（サブジェクト）を簡単に特定できないことがあります。NLPを応用したNER（Named Entity Recognition：固有表現認識）は氏名、住所、場所、組織、生年月日などの固有表現を特定、分類するための効果的な方法です。将来的にはPII情報の正確な識別のために、NERのような手法が増加することになります。これは個人情報保護規制が強化されるなかで規制の遵守には欠かせないことです。このアプローチはPIIだけなく、あらゆる種類のデータ分類に使用されます。

個人情報保護責任は今後も進化し続けるため、同意管理はますます複雑で重要な課題となります。データ収集者への責任が重くなり、これまでと異なり、消費者の同意を技術的な方法で取得しなければなりません。さらに、データ収集者はあらゆる時点で同意取得を立証する必要もでてきます。

これはAPIの保護につながります。APIがますます充実し、サードパーティからさらにその先のパーティにデータを渡すようになると、APIのセキュリティ保護技術が向上し、システム間の情報の流れ特定してサービス間の依存性のマッピングが可能になります。

最後に、ゼロトラストの導入が今後も普及するほどデータ保護の重要性も高まります。高度なゼロトラスト（前述）をアーキテクチャの中心に位置付け、データとデバイスを保護するための新たなテクノロジーとプロセスを模索します。あらゆるリーダーは自社データの日々のやり取りをリアルタイムに把握する高度なテクノロジーに常に精通していなければなりません。データの機密性、ID、アプリケーション、デバイス、送信元と送信先の場所、デバイス、ユーザーの振る舞いといったテレメトリーをリアルタイムに収集、分析することが成功のカギとなります。そして高度なリスクエンジンを使って適切なアクション（許可、拒否、制限、リダイレクトなど）を実行することで、真のゼロトラストアーキテクチャが導入できます。

分析できるテレメトリーが増えるほど、リスクに関する意思決定の精度が上がります。その結果、ビジネス推進、リスクポートフォリオの管理、データ保護の適切なバランスをとることができます。データは最も大切な資産です。どこに保存されているか、どこからアクセスされるかに関係なく、データを保護することが重要になっています。

netskope

SASEのリーダーであるネットスコープは、ネットワークの内外を問わず、あらゆるデバイスからインターネット、アプリケーション、およびインフラストラクチャに、ユーザーを安全、迅速かつダイレクトに接続します。1つのプラットフォーム上にネイティブに構築されたCASB、SWG、およびZTNAにより、ネットスコープは、あらゆる場所で高速、データ中心、クラウドスマートなソリューションで、優れたデジタル化を実現し、トータルコストの削減に貢献しています。

詳しくは https://www.netskope.com/jp/ をご覧ください。