Cloud Data Protection

CSA ジャパン　データセキュリティワーキンググループ

バージョン 1.0

本書の提供について

本書「**Cloud Data Protection**」は、CSAジャパン クラウドデータセキュリティワーキンググループの以下のメンバーが作成し公開したものです（順不同、敬称略）。

花村 実：　マイクロソフトコーポレーション、Data Protection-WG リーダー
諸角昌宏：　日本クラウドセキュリティアライアンス
舟木 康浩：　タレスジャパン株式会社
小町 紘之：　日本マイクロソフト株式会社
大井 喜智：　マイクロソフトコーポレーション
武藤 健史：　マイクロソフトコーポレーション
平鹿 一久：　株式会社セブン銀行
塩田 英二：
安部　高城：TIS 株式会社
宮本 吉晴:　株式会社日本ジーアイエス
山澤　昌夫:

また、本書は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2021 年 8 月 2 日	1.0	新規リリース

日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能です。
https://cloudsecurityalliance.jp

2021 年 8 月 2 日

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

CSA ジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSA ジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．　責任の限定

CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３．　本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSA ジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

コンテンツ

はじめに 1
1. IT 環境の変化とクラウドの発展 2
2. 攻撃トレンドを踏まえた包括的なアプローチ 3
3. CSA ガイダンスにおけるデータセキュリティ 4
4. ゼロトラストアーキテクチャ 11
5. 暗号化・鍵管理 13
6. クラウド認証・認可を活用したデータ保護事例 - Microsoft Information Protection 25
7. モニタリング - CWPP、CSPM 31
おわりに 34

はじめに

クラウド環境に保存されるデータの保護は、クラウドセキュリティにおける重要なポイントです。また、クラウド環境（仮想化による論理境界、IaaS/PaaS/SaaS サービスモデルなど）ごとに、データの保護の仕方も様々です。CSA のクラウドセキュリティガイダンスにおいては、クラウド上のデータ保護として、アクセス管理、暗号化、鍵管理、モニタリング等の推奨事項が記載されていますが、プロバイダのデータ保護対策の内容の把握、利用者側で取るべき対策、プロバイダが提供するデータ保護の機能の利用など、具体的な対応方法をガイダンスから読み解くことが難しい状況にあります。データセキュリティ WG では、このような課題に対してよりわかりやすい技術的な解説を行い、ガイダンスのデータ保護に関する解説書的な位置づけを目指しました。

まずデータがクラウドの置かれるようになった時代背景と攻撃トレンドについて俯瞰します。その上で必要となる包括的なアプローチ、データセキュリティライフサイクルと機能・アクター・コントロールの必要性について考えていきます。コロナ禍でリモートワークが広がる中で注目されているゼロトラストアーキテクチャによるデータ保護の考え方も取り上げました。データ保護で最も大切な暗号化・鍵管理について解説し具体例として Microsoft Information Protection を紹介しています。最後に継続的なモニタリングの重要性について確認し CSPM（Cloud Security Posture Management）を推奨しています。

クラウドコンピューティングは必要なときに必要なリソースをどこからでもアクセス・共有できるとても便利なツールでデジタルトランスフォーメーションに必要不可欠なものです。一方で適切なセキュリテイ戦略を持って運用しないと社会的信用を失墜しかねないリスクも持ち合わせています。本書が、読者皆様方の安全なクラウド利用の一助になれば幸いです。

なお、末筆とはなりますが、本資料作成にあたって有志の方のご協力いただきました。この場をお借りして御礼申し上げます。

Data Security WG リーダー 花村 実

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

1. IT 環境の変化とクラウドの発展

旧来のセキュリティの考え方の基本として、下記のネットワーク境界モデルをとっていました。基本的に非信頼ゾーンからの信頼ゾーンのアクセスを禁止することによりデータを保護していました。

① 信頼ゾーン：社内ネットワーク（オンプレミス内のサーバー、ネットワーク、クライアントなどのリソース）

② 非信頼ゾーン：社外ネットワーク（クラウド、スマホ、自宅 PC、持ち出し PC など）

しかし、なりすまし攻撃など犯罪者の手法は洗練化されてきて、オンプレミス内の侵入も珍しいことではなくなってきました。またクラウドコンピューティング(以降クラウド)の普及により、私たちはどこからでもインターネット経由で会社のデータにアクセスできるようになりました。ネットワーク境界モデルは限界を迎え、私たちはデータ保護に対する新しい戦略が必要になりました。

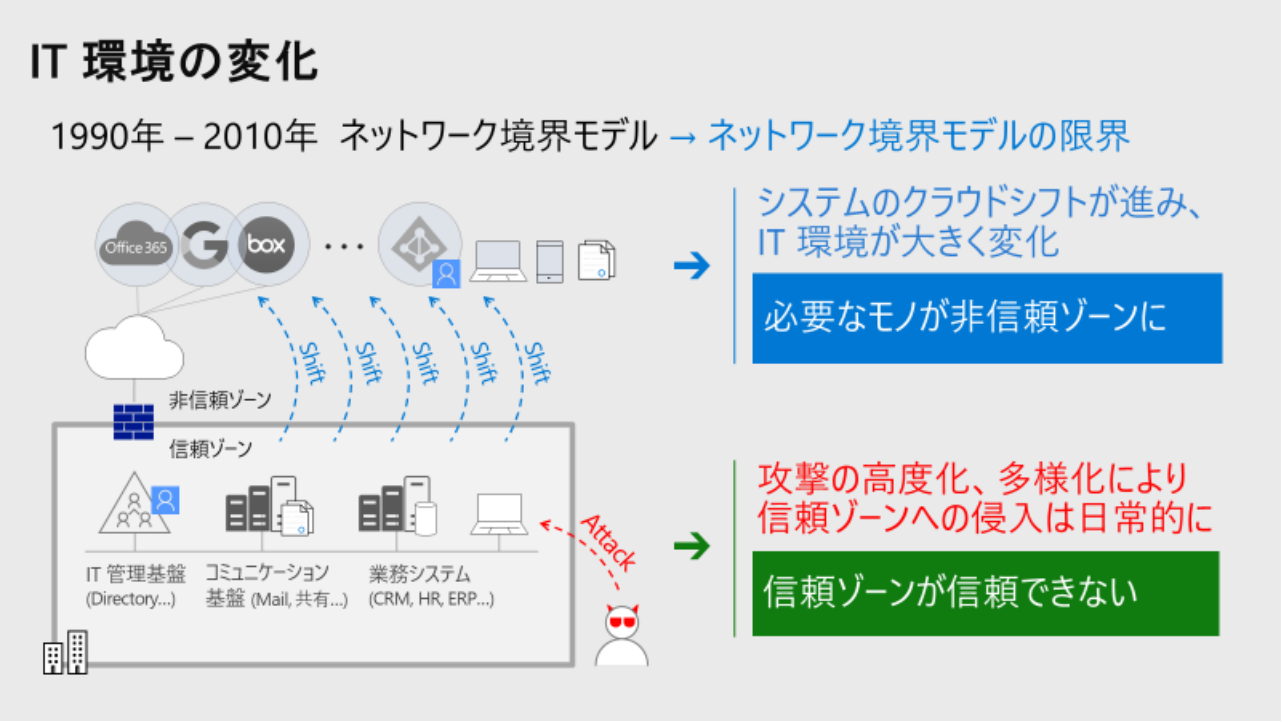


図１：IT 環境の変化

© 2021 一般社団法人 日本クラウドセキュリティアライアンス

2. 攻撃トレンドを踏まえた包括的なアプローチ

クラウド時代のセキュリテイ戦略を立てる前提としてある程度の侵入を前提（Assume Breach）に考えることが重要です。最初にできる限り自分たちのリソースに対するアクセスを防ぎます（アクセス制御、サンドボックス）。フィッシングメールの添付ファイルや悪意のある Web サイトを開いてしまいマルウェアがエンドポイントに着弾した場合も IOC（Indicator of Compromise）シグネチャーによる検知、隔離の自動化により被害の拡大を防ぎます。検知ができなかった場合でも水平展開、通常使われないスクリプトの実行などの異常な振る舞いから悪質な行為の判別が可能になります。パスワードスプレー攻撃、特権アカウントへの昇格などのアカウント情報に対する対処も重要になります。犯罪者の目的であるデータ窃取も CASB, DLP で早期の対処をします。犯行が社員・パートナなどの内部からの発生に備えたモニタリングも取り入れる企業が多くなっています。こうした多層防御のそれぞれのフェーズでの包括的なアプローチにより効率的なデータ保護を図っていくことが求められています。

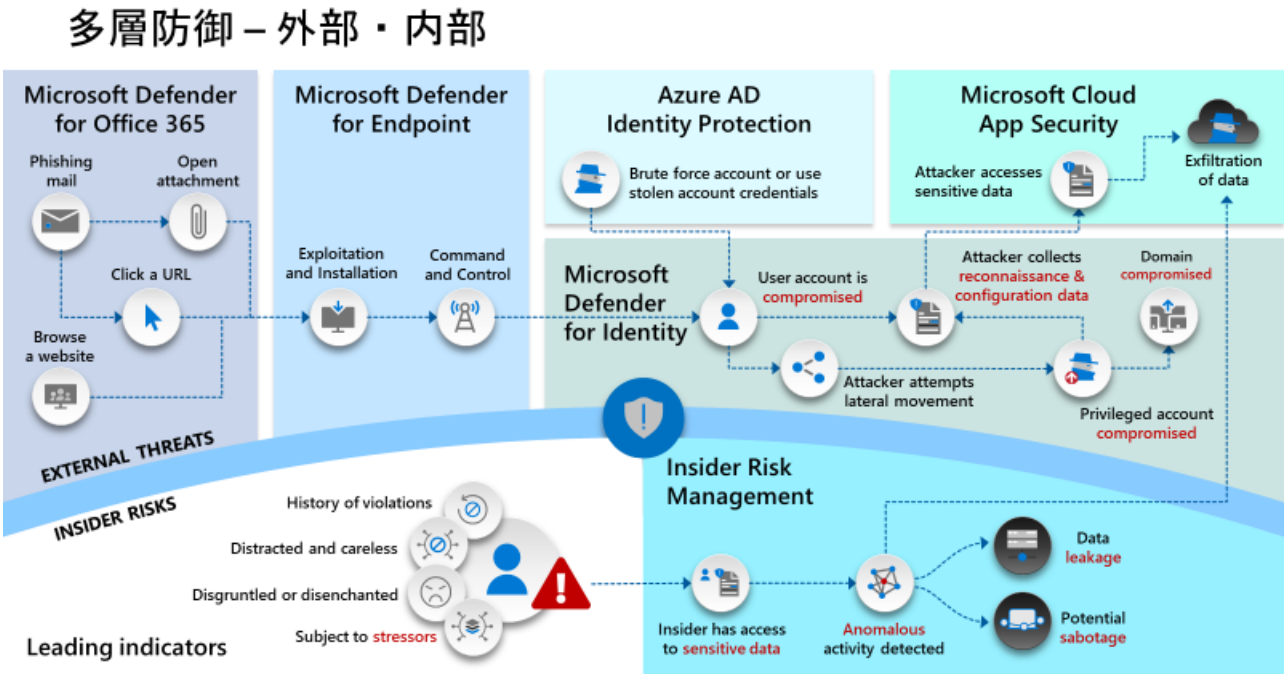


図 2：包括的なアプローチ：多層防御

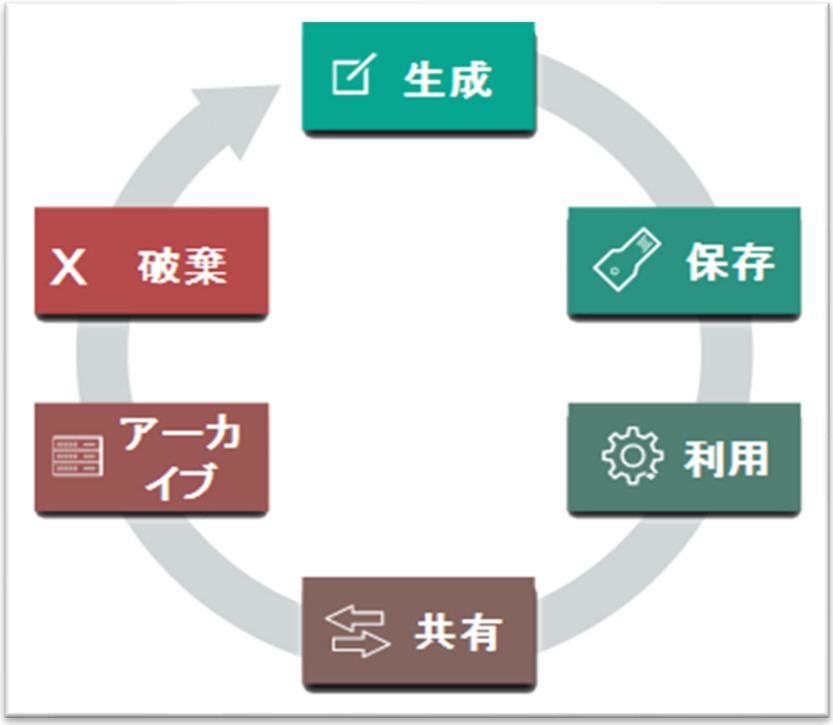
© 2021 一般社団法人　日本クラウドセキュリティアライアンス

3. CSA ガイダンスにおけるデータセキュリティ

クラウドセキュリティを考える際、データセキュリティはその中核の要素となります。本章では、クラウドにおけるデータセキュリティについて、CSA ガイダンスで説明されている考え方として、データセキュリティライフサイクルに基づいて説明します。なお、データセキュリティライフサイクルを用いた考え方はあくまでフレームワークであり、実際の実装方法と完全に一致するものではないことを注意してください。

1. データセキュリティライフサイクルとは？

   データセキュリティライフサイクルは、情報セキュリティライフサイクル（ILM）の考え方に基づいて、セキュリティの観点から作成されたものです。ILM は、情報（電子データ）の重要度や利用目的・頻度などの変化に応じて、それを格納するのに適したストレージへ適宜、移動・配置することにより、効果的な情報活用と効率的なストレージ投資を実現するという考え方です。これに対して、データセキュリティライフサイクルは、セキュリティの観点で必要となる考え方および対策をデータライフサイクルの各フェーズでどのように行っていくかを表しています。CSA ガイダンスでは、以下の図にあるように 6 つのフェーズでデータセキュリティライフサイクルを表現し、各フェーズにおいて必要となるセキュリティの考え方及び対策を可視化しています。



© 2021 一般社団法人　日本クラウドセキュリティアライアンス

以下の表では、このデータセキュリティライフサイクルの各フェーズの内容、および必要となる代表的なセキュリティ対策を示しています。データセキュリティライフサイクル自体はクラウド固有というものではなく、一般的なものですが、クラウド環境においても、このライフサイクルの各フェーズにおけるセキュリティ対策を考えていく必要があります。

フェーズ	内容	セキュリティ対策・手法
作成	新しくデジタルコンテンツを作成、あるいは既存コンテンツを変更／更新／修正	情報の分類、アクセス管理
保存	デジタルデータを何らかの保存格納場所に収納する作業	アクセス管理、データ保存時の暗号化、デジタル著作権管理（DRM）、コンテンツディスカバリ
利用	データが、閲覧、処理、その他の活動に利用される	アクセス管理、アプリケーションセキュリティ、モニタリング
共有	ユーザ相互間、顧客向け、パートナー向けなどのように、第三者からアクセスできるようにする	DLP，アプリケーションセキュリティ、データ移動時の暗号化
アーカイブ	データがアクティブには利用されなくなり、長期保存に回される	暗号化、アセット管理
破棄	データが、物理的またはデジタルな手法によって恒久的に破棄される	永久的かつ安全な削除（クリプトシュレッディング）、コンテンツディスカバリ

2. 所在場所、権限付与の考え方

上記のデータセキュリティライフサイクルでは、ライフサイクルの各フェーズにおけるセキュリティを扱うことができます。しかしながら、データの移動やデータのアクセス方法（誰がどのようにアクセスするか）については考慮されていません。したがって、データセキュリティライフサイクルは、組織が使用するデータのフレームワークとして考えることができますが、クラウドにおいては、追加で考える必要のある要素があります。これは、クラウドの基本特性である「幅広いネットワークアクセス」に起因するもので、「所在場所」と「権限付与」です。データのある場所、およびアクセスのための権限付与を明確に理解し、セキュリティ対策を行うことが必要になります。以下の図で示すように、データはオンプレ、パブリッククラウド、プライベートクラウド等のさまざまな場所に保存されます。また、データは、様々なデバイス（PC,スマートフォンなど）からオンプレあるいはクラウドに移動する可能性があります。さらに、データが移動するネットワークも、オンプレ、自宅、コーヒーショップのフリーWiFi 等、様々です。したがって、データセキュリティライフサイクルにおいて、この場所およびアクセスを考慮したセキュリティを考えていく必要があります。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

① 所在場所

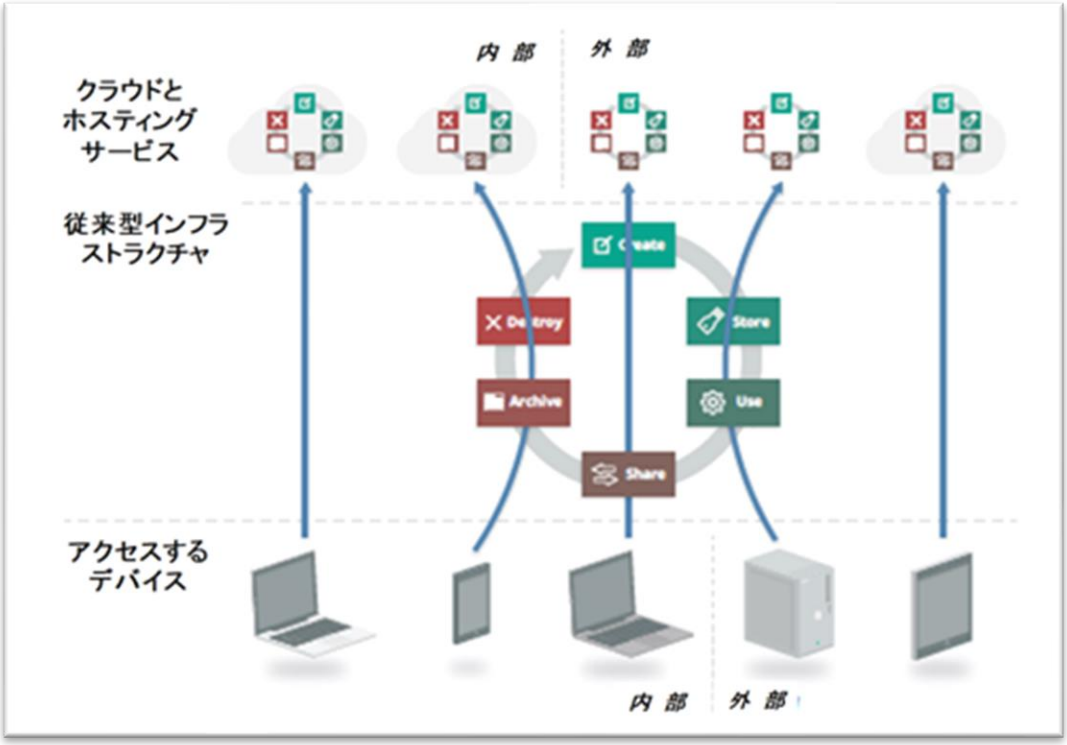
クラウド環境では、プロバイダ、オンプレ、データセンタ内の複数の場所でデータが移動する可能性があります。したがって、データの場所はどこか？それぞれの場所におけるライフサイクルのフェーズにおけるセキュリティ対策は何か？データはどの場所からどの場所に移動するか？データはどのように移動するか？などを考慮する必要があります。

今までは、データはオンプレの中に存在するということが言えましたが、現在は、データは移動可能であり、組織の内外の様々な場所に迅速かつ容易に移動できる状況となっています。クラウドについても同様であり、データがオンプレからクラウドに移動するとともに、プロバイダ間を移動することもあります。また、場所により適用される法律や規制が変わってくることがあるように、場所によるセキュリティ対策を考慮する必要があります。

② 権限付与

権限付与においては、データに対して誰がアクセスできるのか？また、どのように（デバイスやネットワーク）アクセスできるのかをを考慮し、必要なアクセス権を設定していく必要があります。

これらをまとめて表現したのが下の図になります。



© 2021 一般社団法人　日本クラウドセキュリティアライアンス

3. 機能、アクター（CSA ガイダンス 4.0 では「主体」と表現されている）、コントロール

上記のように、データセキュリティライフサイクルに所在場所、権限付与の考え方を取り込んだ上で、データに対してどのようなコントロールを適用していくかを考えていく必要があります。それを、機能、アクター（以下の図では実行者）、所在場所におけるコントロール方法で表現されます。なお、場所、アクターについては前述しているので、ここでは機能とコントロールの考え方を示します。

① 機能

機能は、データに対してどのようなことを行うことができるかということで、以下の 3 つの主な機能があります：

- 読込(read)：データを参照したりアクセスしたりする機能。コピー、ファイル転送などを含む。
- 処理(process)： データに対するトランザクションを行う。アップデート、使用などを含む。
- 保存(store)：データの保存。ファイルやデータベースなどへの保存。

実際には、さらに細かく、データに対して「Read only」,「Read-Write」、「Delete」等の機能が定義できます。

以下のテーブルは、上記の 3 つの機能が、データセキュリティライフサイクルの各フェーズとどのようにマッピングできるかを示しています。

	作成	保存	利用	共有	アーカイブ	破棄
読込	×	×	×	×	×	×
処理	×		×			
保存		×			×	

② コントロール

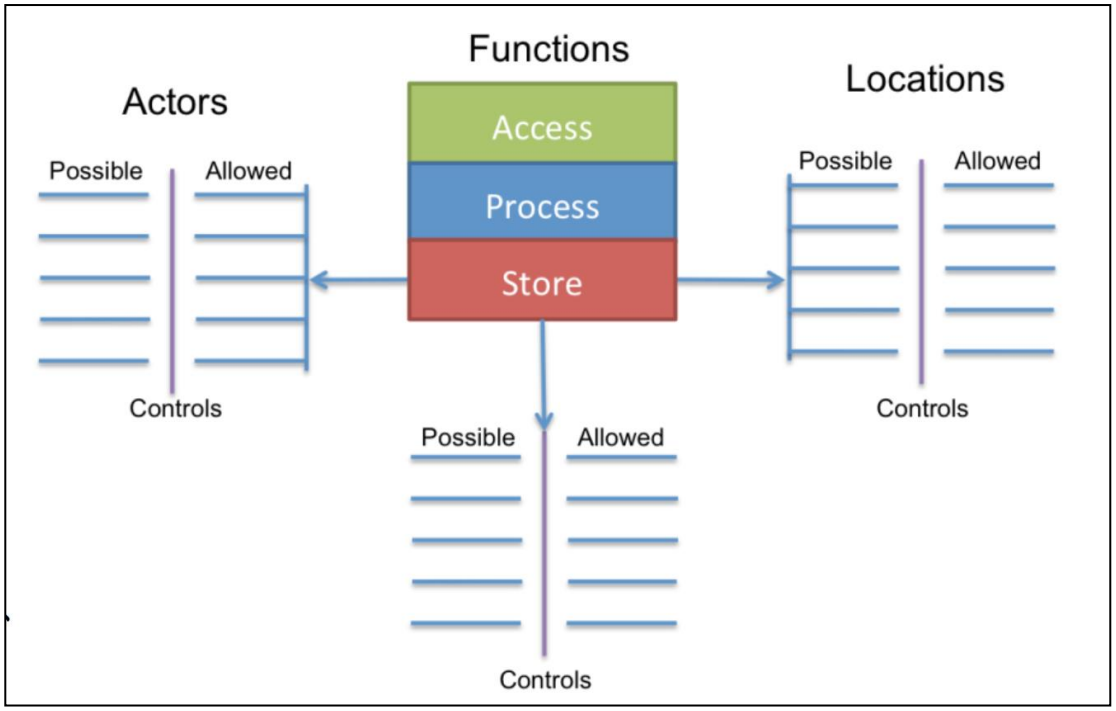
ここでいうコントロールは、アクションが「可能」であるものが実際に「許可」するかどうかを決めるのに用います。したがって、コントロールを決めるにはすべての「可能」な機能、場所、アクターをリストアップし、それらに対して「許可」するかどうかを決めていきます。そのためには、以下の 5 つの点でコントロールを考える必要があります：

1. データの機能
2. データの場所
3. データのアクター
4. データが転送されるネットワーク
5. データにアクセスするデバイス

以下はそのイメージになります。これらの要素に対して「可能」「許可」を考えていきます。それをデータセキュリティライフサイクルとマップすることで、コントロールの明確な定義を行うことができます。

（注： 以下の図は CSA ガイダンス 3.0 より引用しています。CSA ガイダンス 4.0 では、図が切れているため、こちらを引用しました）

© 2021 一般社団法人 日本クラウドセキュリティアライアンス



このモデルの考え方は、複雑すぎるように見えるが、この考え方に基づいてデータガバナンスの一般的なガイドラインをより大きな観点から検討する際に役立ちます。

以上の考え方に基づいた例として、以下の表を示します。ここでは、場所ごとのアクセス制御を例としています。

アクター	場所	機能	可能	許可
社員 01	BYOD モバイル	閲覧/読込	○	×
〃	社内 LAN	閲覧/読込	○	○
〃	自宅	処理実行	○	○
〃	〃	データ保持	○	×
・・・・	・・・・	・・・・	・・・・	・・・・

2 データセキュリティと暗号化

クラウド環境におけるデータセキュリティとして、暗号化は非常に重要なツールです。データの状況に応じて以下の点において暗号化を考慮する必要があります：

① データの保存時（Data At Rest）： クラウド内のストレージにデータを保存する場合
② データの移動時（Data In Motion）：クラウドへのデータ転送、クラウドからのデータ転送、および、クラウド内でのデータ転送の場合

© 2021 一般社団法人 日本クラウドセキュリティアライアンス

なお、データが扱われるケースとして、もう 1 つ「データの使用時（Data In Use）」がありますが、データ使用時の暗号化は現段階では求められていません。それは、暗号化されたデータをそのままアプリケーションが扱うことができないことによります。ただし、これは今後完全順同型暗号の技術が商用化されてくる段階で要求されてくる可能性がありますので、今後の動向に注目してください。

以上の考慮点の中で、ここではクラウド環境における暗号化として、データの保存時における暗号化についてその概要を示します。

① クラウドデータの暗号化のアーキテクチャ

暗号化のアーキテクチャとして、以下の 3 つのコンポーネントがあります：

- データ： 暗号化の対象となるデータ
- 暗号化エンジン： 暗号化を実行
- 暗号化鍵： 暗号化に使用する鍵

クラウド環境、特に IaaS の環境においては、これらの 3 つのコンポーネントをどのように配備するかを検討する必要があります。

② サービスモデルで用いられる暗号化

- IaaS

  IaaS においては、以下の暗号化を使用します：

  - インスタンス管理暗号化

    上記のアーキテクチャにおける「暗号化エンジン」をインスタンスの中に配備するモデルです。この際、暗号化鍵はインスタンス内部に保管します。
  - 外部（鍵）管理暗号化

    インスタンス管理暗号化ですが、鍵をインスタンスの外部に保管する方法です。セキュリティの観点から、こちらの方法が推奨されます。
  - クライアントサイド暗号化

    暗号化エンジンをアプリケーションあるいはクライアント内に配備するモデルです。暗号化鍵は、利用者が管理します。
  - サーバサイド暗号化

    プロバイダが提供する暗号化方式で、プロバイダが暗号化鍵を管理します。
  - プロキシ暗号化

    暗号化エンジンをプロキシ・インスタンスあるいはプロキシ・アプライアンス上に配備するモデルです。プロキシはインスタンスへのアクセスとストレージ上のデータのマッピングを行います。鍵は、プロキシ内あるいは外部の鍵ストレージに保存します。
- PaaS

  PaaS においては、以下の暗号化を使用することになります：

© 2021 一般社団法人 日本クラウドセキュリティアライアンス

- アプリケーションベース暗号化
  暗号化は、利用者が作りこむアプリケーションの中で行われます。
- データベース暗号化
  データベース・プラットフォームが暗号化機能を持ちます。代表的なのは透過型データベース暗号化と呼ばれる方法で、データベースプラットフォームが、データベース全体あるいは個々のフィールドのデータごとに暗号化を行います。この透過型暗号化が、データベースにおける推奨になります。
  その他
  PaaS プロバイダが暗号化を提供し、利用者のアプリケーションがそれを利用する方法です。

- SaaS
  SaaS プロバイダが暗号化機能を提供するのが一般的ですが、SaaS プロバイダが IaaS あるいは PaaS プロバイダが提供する暗号化機能を利用する場合もあります。SaaS における暗号化においては、可能な限り利用者ごとの鍵を実装することが推奨されます。

3．新しい暗号化の代替技術（エマージングテクノロジ）

ここでは、暗号化に代わる技術として広まってきている 2 つの技術（秘密分散技術と完全準同型暗号）について、その非常にハイレベルな概要を記述します。詳細は、数学的な知識が必要となるため、該当する文献等を参照してください。

① 秘密分散技術
秘密分散技術は、データをいくつかの断片に分割して管理する方式です。分割した断片は一定数集めると、元のデータに復元することが出来ますが、一定数より少ない個数の断片からではデータを復元することができません。例えば、秘密分散技術を使って、1 つのデータを 100 個の断片に分割したとします。その内の任意の 50 個を集めれば元のデータに復元できますが、49 個では復元できないというものです。秘密分散技術は、暗号化と違って鍵を持つ必要がありません。したがって、鍵管理の問題や危殆化の問題に対応できる方法となります。
また、秘密分散方式を利用した秘密計算も実用化してきています。こちらは、データを秘匿化したまま計算処理することができる技術で、アプリケーションが秘匿化されたままのデータを処理できるようになります。クラウド環境、特に SaaS 環境において、利用者のデータを秘匿化したまま処理できることになるため、安全なデータの処理を行うことができるようになります。秘密分散技術の国際標準(ISO/IEC 19592-2:2017)が 2017 年に ISO から発行されています。現在標準化されている方式では、分散数に応じてデータサイズが増加します。増加しない方式は、まだ標準化に至っていません。

② 完全準同型暗号
完全順同型暗号は、暗号化されたデータを復号化することなく処理することができる方法です。こちらは、利用者が暗号化したデータをそのままクラウドに送り、クラウドのアプリケーションで復号することなく処理することができるため、クラウドにおいては非常に有効なソリューションとなります。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

4. ゼロトラストアーキテクチャ[1]

由来と 6 エンティティ（ID, Device, Data, Apps, Infra, NW）

クラウド環境ではデータの物理的な場所を特定するのは難しいのでゼロトラストアーキテクチャを基点にします。ゼロトラストの起源は古く、2004 年の Jericho Forum（旧約聖書 ヨシュア記　エリコの要塞に由来）で提唱された“de-perimeterisation：境界型セキュリティでもう守れない” という概念から始まっています。なりすまし、洗練化された手法により攻撃は境界（つまり Firewall などでかこまれたトラストゾーン）を突破することが多くなりました。また境界の内側は“安全”という前提なので、内側に入られた場合は楽々と水平展開（Lateral Move）されてしまい重要データや権限昇格して特権アカウントを窃取されてしまいます。

ゼロトラストは境界型セキュリティ戦略を見直します。ゼロトラストの基本的な構造は 2 つの Access Entity（ID, Device）、4 つの Requested Entity（Data, App, Infra, Network）、Access Request の許可、制限、拒否を決定する Policy Enforcer から成ります。アクセスするときに“毎回”、トラストレベルを確認し,ポリシーに則ってアクセスの許可、制限、拒否を決定します。認証・認可、マイクロセグメンテーションを適切に実装することにより、安全なリモートワークをサポートします。

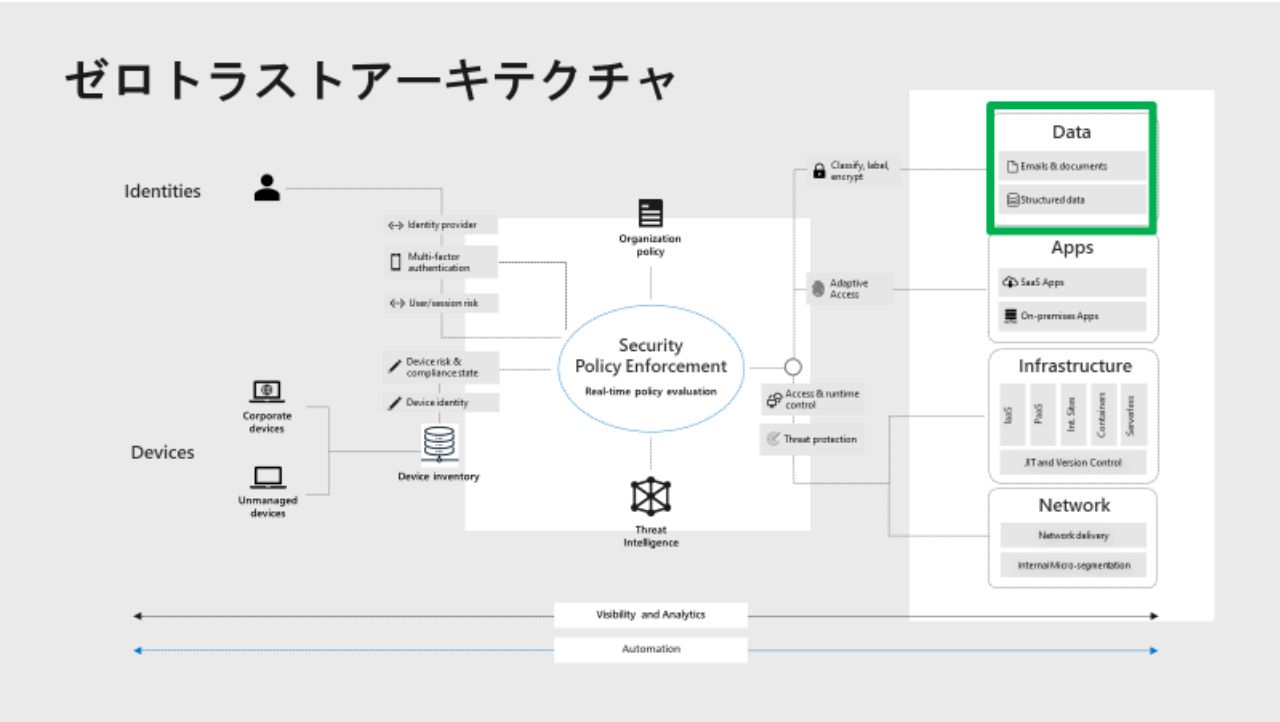


図２：ゼロトラストアーキテクチャ

[1] NIST SP 800-207: Zero Trust Architecture Zero Trust Architecture (nist.gov)

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

基本的な考え方

ゼロトラストではすべてのデータソースとコンピューティング サービスを"リソース"として考え、そのリソースに対するアクセスを１つ１つのセッションごとに許可・制限・拒否をコントロールします。社内のネットワークからのアクセスか否かといったことは関係なく、すべてのコミュニケーションで最も安全な方法を取るようにします。エンティティの状態と異常な振る舞い・環境要因（例：脅威インテリジェンス）を基に"リソース"へのアクセスは動的なポリシーにより制御されます。継続的な診断とリスク低減（ CDM: Continuous Diagnostics and Mitigation）を定常的なモニタリングにより実現し、脆弱性のあるリソースへのアクセスを制限・拒否します。

アイデンティティ・アクセス管理（IAM）

IAM でセキュリティポリシーを実現するためには最小限のアクセス権限（Least Privilege）とデータに対する的確な機密性の定義が必要です。動的なアクセス制御をするためにユーザアカウントとデバイスのアイデンティティの健全性（Hygiene）をもとにリスク度合いを測り、またリソースの機密度により許可・制限・拒否を判断します。ID 認証時になりすましでないことを証明し認可でリクエストが許可されることを決めます。この時にゼロトラストではセッションごとの動的なアクセス制御を Policy Enforcer が行います。振る舞い、データの機密度、ログ解析、脅威インテリジェンスなどからリスクを判定します。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

5. 暗号化・鍵管理

背景[2]

クラウドでは共有責任モデルとしてユーザーがデータセキュリティの責任を持ちます。そのデータを保護する技術として「暗号化」が有効な技術であることが各法規制やガイドライン等で言及されており、多くの情報システムにおいて暗号技術は活用されています。

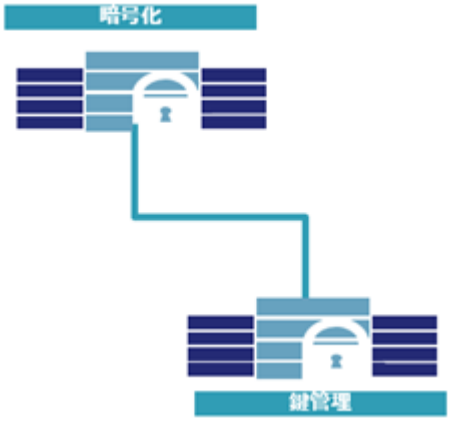
また暗号化技術を利用する場合には「暗号鍵」もユーザーの責任で保護する必要があり、ユーザー自身の責任で鍵管理技術を理解して実装方法を選択して運用する必要があります。

一例として個人情報保護法では個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」と記載があります。

高度な暗号化の例として、

- 暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること
- 遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること
- 第三者が復号鍵を行使できないように設計されていること

のいずれかの要件を満たす必要があり、保護されているデータと鍵管理は分離する設計が必要です。



[2] 参考資料：
クラウドセキュリティアライアンス:
https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf
ISMAP 管理基準: https://www.ipa.go.jp/files/000082277.pdf
金融機関におけるクラウド利用に関する有識者検討会報告書:
https://www.fisc.or.jp/document/fintech/file/190_0.pdf
個人情報の保護に関する法律についてのガイドラインに関する QA:
https://www.ppc.go.jp/files/pdf/170530_faq_rouei.pdf

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

クラウドサービス利用時においても各ガイドライン等（以下参考資料）で鍵管理の重要性について言及されています。

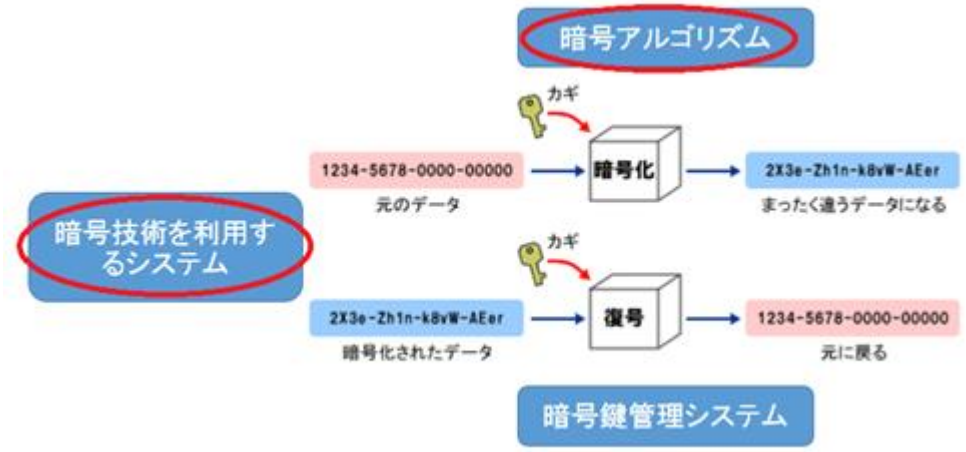
本章では暗号技術全般、暗号鍵運用管理、クラウドサービスと鍵管理システムの構成例、クラウドサービス事業者の鍵管理サービス例、鍵を管理する専用ハードウェアであるハードウェアセキュリティモジュールについて記載します。

注：本章では復号、署名、検証等各処理で利用する鍵を「暗号鍵」と記載しています。

暗号技術の活用[3]

各クラウドサービスインフラストラクチャ（IaaS）、プラットフォーム（PaaS）、またはソフトウェア（SaaS）サービスにおいてデータ暗号は標準提供されている技術となってきています。

本章では暗号アルゴリズム、利用するシステムについて記載します。



暗号アルゴリズムはクラウドサービスに限らず、電子政府推奨暗号の安全性を評価、監視している CRYPTREC の「電子政府における調達のために参照すべき暗号のリスト」が参考(以下参考図)となります。クラウドサービス事業者が暗号アルゴリズムを決定しておりユーザー側が選択不可の場合には利用しているアルゴリズムを確認することを推奨します。

---

[3] 参考資料
暗号化の仕組み(総務省より):
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/02.html
電子政府における調達のために参照すべき暗号のリスト(CRYPTREC):
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r5.pdf
トークナイゼーションの説明:
https://cpl.thalesgroup.com/ja/encryption/tokenization
https://pcireadycloud.com/token/
量子セキュアクラウド技術の確立に向けて始動: https://www.nict.go.jp/press/2020/10/19-1.html

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード(注13)	CCM
		GCM(注4)

暗号を利用するシステムがクラウドサービスの場合にはユーザー自身で暗号鍵を制御可能なレベルを把握して設計する必要があります。

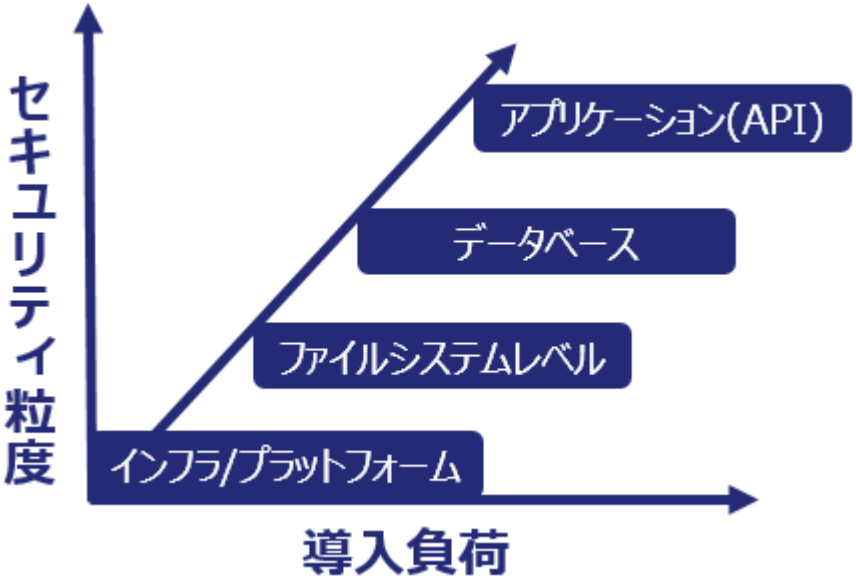
クラウドサービス事業者が提供するサービスを一般的に利用されている用語(BYOK 等)を基に示すと以下の図になります。

BYOE は自社がオンプレミスで利用している暗号化技術をクラウドサービスで利用する管理方法であり、クラウドサービス事業者は暗号鍵に一切アクセス不可のため制御レベル高くなります。

以下各手法の「鍵管理」の差異については「クラウドサービスと鍵管理システムの構成例」で説明します。

クラウドサービス、オンプレミスシステムともに暗号技術を利用するシステムは一般的に暗号技術を実装する箇所によりセキュリティ粒度と導入負荷が異なります。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス



- アプリケーション
  - API を利用して暗号技術を利用する場合はユーザー自身で設計した技術を利用することでより柔軟にシステム要件にあわせて暗号化技術を導入することが可能
  - トークナイゼーションと呼ばれる技術も利用することが可能
    - データサイズ(桁数)を変更せずにデータ保護が可能であり、ビックデータ解析のためにクラウド上にデータ移行時に活用する事例あり
    - トークナイゼーションをクラウドサービスで提供している企業もあり
- データベース
  - 多くの商用データベース製品は標準で暗号化技術が提供されており、システム開発の必要なし
  - ユーザー自身が定義した関数を利用して DB ユーザー単位で暗号復号権限を与えることで DB 管理者が復号不可という実装が可能
- ファイルシステムレベル
  - オペレーティングシステム上で動作する各アプリケーションに透過的に動作をさせることが可能
  - ユーザーやプロセスごとに鍵利用権限を管理することで、OS 特権ユーザー復号不可という実装が可能な製品もある
- インフラ/プラットフォーム
  - VMWare 等の仮想環境やストレージシステム、ディスク単位で KMIP (鍵管理用 OASIS 標準プロトコル) がサポートされており、鍵管理システムと連携して暗号化技術の実装が可能
  - 暗号化実装によるシステム処理性能に対する影響は少ない

耐量子暗号技術は RSA 等の公開鍵暗号技術に対して解読にかかる期間が大幅に短縮されるリスクがあるため研究開発がすすんでおり、NIST(アメリカ国立標準技術研究所)で今後正式に 2024 年をめどにアルゴリズムが選定される予定です。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

日本では NICT にて研究や実証実験が行われており、量子セキュアクラウド技術連携において主に認証強化のために既存の暗号技術から耐量子暗号技術への移行を視野に入れて検証がされています。

暗号鍵の運用管理[4]

暗号鍵の運用において日本国内のガイドラインでは NIST(アメリカ国立標準技術研究所)の資料が参照されることが多く、それら資料は一部翻訳されており、SP 800-57 (鍵管理における推奨事項) と SP800-130(暗号鍵管理システム設計のフレームワーク) が情報システムにおける鍵運用管理に役立てることが可能です。

以下は CSA が作成したクラウドサービスの鍵管理内の鍵管理コントロールの運用管理で記載されている内容を NIST SP800-57 の用語にマッピングした図です。

[4] 参考資料：
セキュリティ関連 NIST 文書(IPA より): https://www.ipa.go.jp/security/publications/nist/
暗号鍵管理ガイドライン(IPA より/NIST 翻訳資料含む): https://www.ipa.go.jp/security/vuln/ckms.html
クラウドサービスの鍵管理(CSAJ の翻訳資料)
https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2021/02/Key-Management-in-Cloud-Services_J.pdf
BYOK の開発手法例: https://www.cyberware.co.jp/professional-services/byok/
クラウドサービス鍵管理システム例:
https://cpl.thalesgroup.com/ja/encryption/key-management/ciphertrust-cloud-key-manager

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

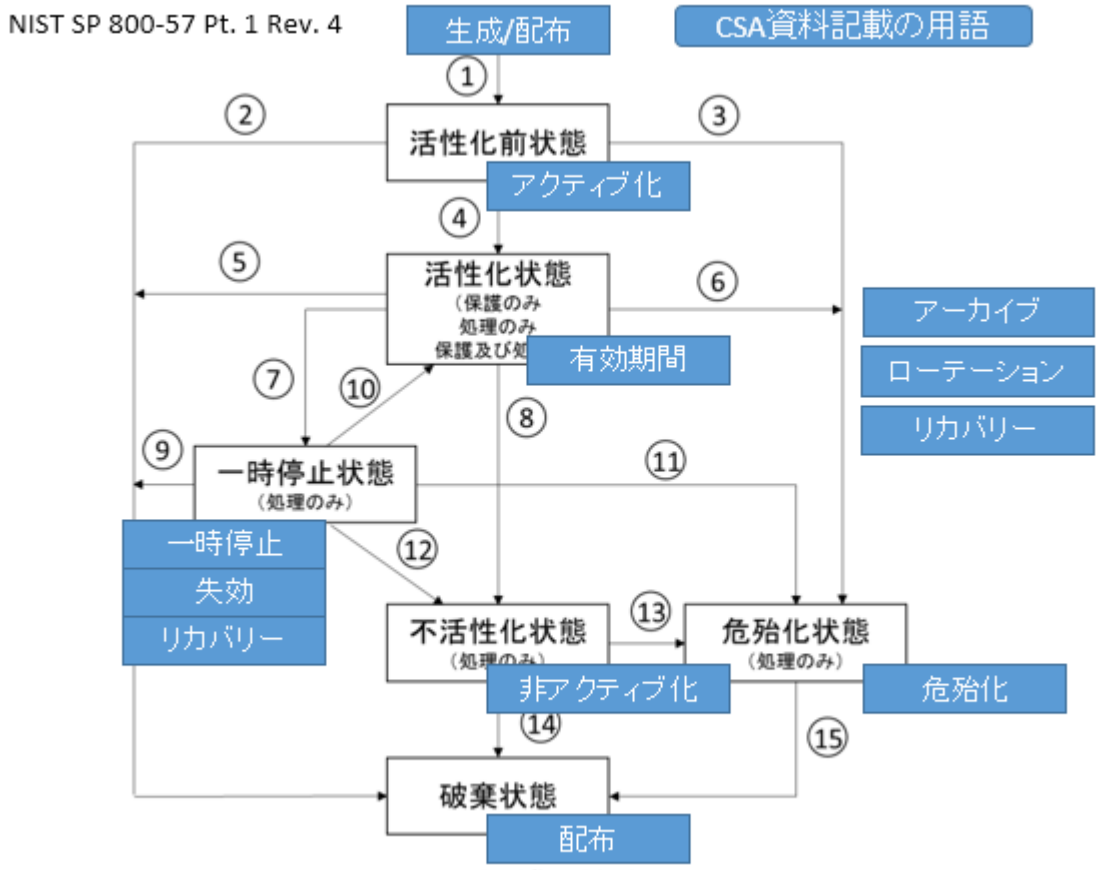


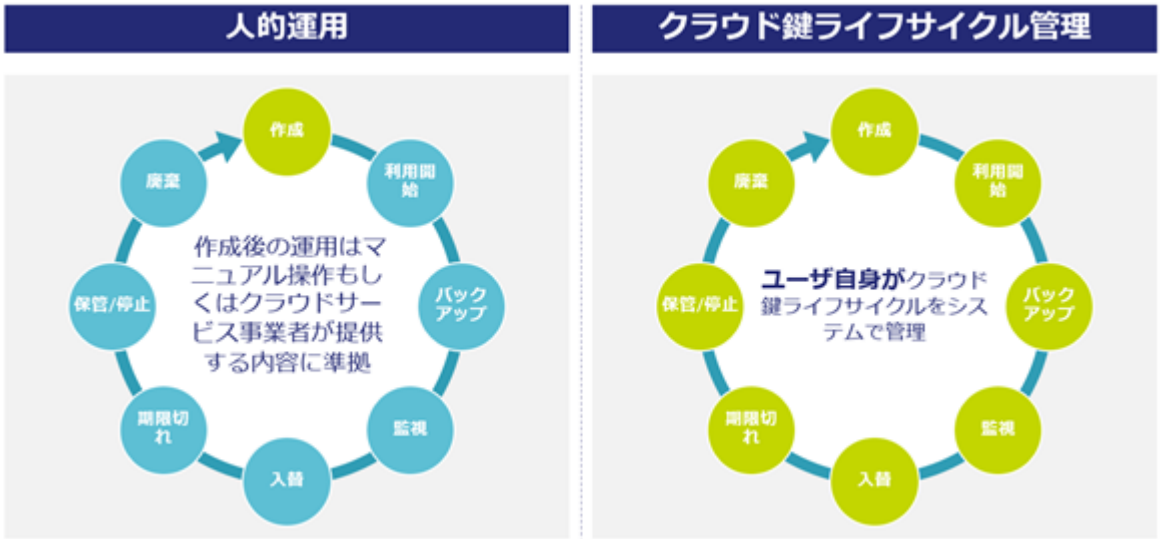
図 3 ： 鍵の状態と遷移の例

鍵自体もデータであり、保護する必要があるとともに、その重要性から作成、利用開始/終了、バックアップ、バージョン管理、ローテーションを意識して運用管理設計をする必要があります。

クラウドサービスが提供する KMS を利用することで容易に暗号鍵管理は実現可能ですが、暗号鍵の運用管理は設計が必要です。

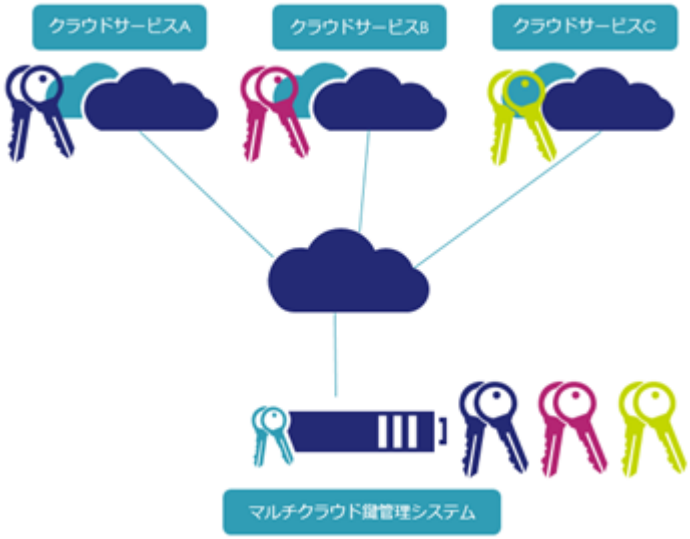
- 複数の暗号鍵を運用管理
- 複数のクラウドサービスの KMS を利用する
- 鍵を利用するシステム固有の要件
    - ユーザーが作成した鍵を利用する(BYOK)
    - ユーザーが保有する鍵を利用する(HYOK)
    - バックアップ/リストア等

© 2021 一般社団法人　日本クラウドセキュリティアライアンス



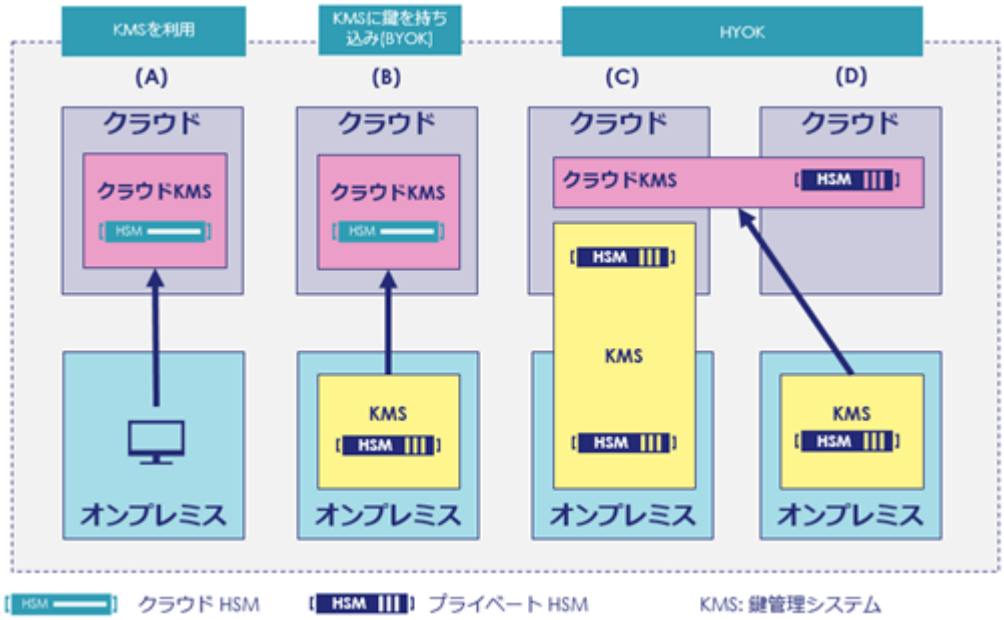
上記運用管理をクラウドサービス事業者が提供する各種ツール、API 等を利用してシステム開発を行うことも可能です。

またクラウドサービス鍵管理を支援する製品やサービスがリリースされており、そのような製品やサービスを活用することで鍵運用管理コストの削減や監査対応に役立てることが可能です。



© 2021 一般社団法人　日本クラウドセキュリティアライアンス

クラウドサービスと鍵管理システムの構成例[5]



クラウドサービス事業者の KMS はユーザーが要求するセキュリティ要件に対応するために鍵管理においていくつかの機能を提供しています。

- BYOK(Bring Your Own Key)
  - ユーザー自身が暗号鍵を作成してクラウドサービスに持ち込むシステム構成
  - 持ち込んだ後の暗号鍵はクラウドサービス事業者内で管理
  - API が公開されることが多く、オンプレミスの HSM 等で作成した鍵をアプリケーションを開発することで持ち込むことが可能

BYOK が要求される背景には「鍵」自体のセキュリティを理解する必要があります。鍵生成には乱数等が重要な技術として利用されており、暗号技術同様に仕様が決まっています。また鍵生成手順について監査を受ける必要がある場合にはユーザー自身が決まった手順、技術仕様で鍵を生成する必要があり、そのためクラウドサービス事業者にユーザーが作成した鍵を持ち込むサービスが提供されています。

---

[5] 参考資料
Microsoft Azure Double Encryption について:
https://docs.microsoft.com/ja-jp/microsoft-365/compliance/double-key-encryption-overview?view=o365-worldwide
https://techcommunity.microsoft.com/t5/microsoft-security-and/understanding-microsoft-information-protection-encryption-key/ba-p/2214589
Google Cloud EKM について: https://cloud.google.com/kms/docs/ekm
Salesforce キャッシュのみの鍵サービス(Cache-Only Key) :
https://releasenotes.docs.salesforce.com/ja-jp/spring19/release-notes/rn_security_pe_cache_only_key_ga.htm

© 2021 一般社団法人 日本クラウドセキュリティアライアンス

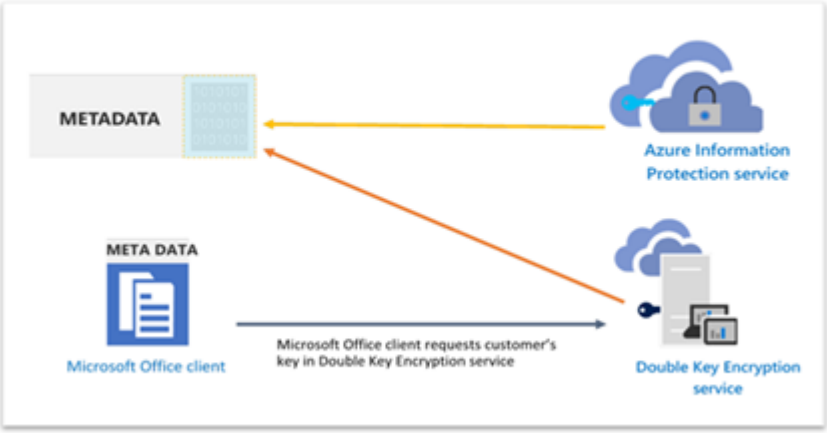
- HYOK(Hold Your Own Key)
  - クラウド事業者のサービスがユーザーの鍵管理システムを利用
  - ユーザーの暗号鍵はクラウドサービス事業者外部で管理

HYOK サービス例として Microsoft Azure の 2 重キー暗号化 (Double Key Encryption) や Google Cloud External Key Manager、Salesforce キャッシュのみの鍵サービス(Cache-Only Key) があります。

2 重キー暗号化は Azure 内のデータ保護で 2 つの鍵を利用する技術であり、マイクロソフト社が管理する鍵とユーザーが管理している鍵でデータは暗号化されているため、マイクロソフト社の管理している鍵のみではデータは復号できません。

本サービスのリリースされた背景には各種法規制への対応の記載があり、ユーザー自身の鍵管理技術は今後も拡張されることが想定されます。

High Level Architecture of Double Key Encryption:

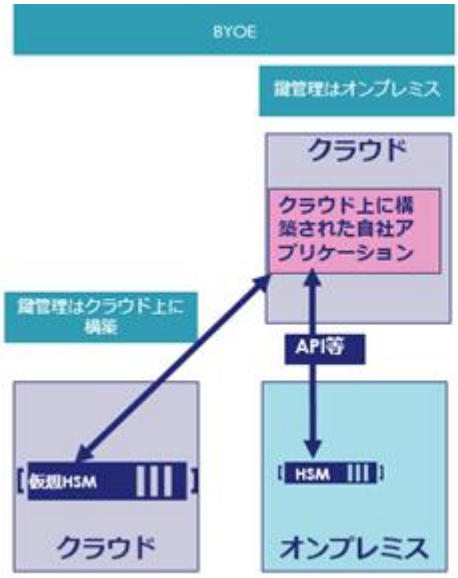


鍵管理と暗号化技術をユーザー自身でクラウドサービス上に実装することも可能です。

- BYOE(Bring Your Own Encryption)
  - オンプレミスで利用している暗号技術/鍵を利用可能
  - 自社鍵管理システムを自社が利用するアプリケーションのみがアクセス可能
  - クラウドサービス事業者内またはオンプレミスに鍵管理システム構築

HYOK と異なる点は「クラウド事業者のサービス」も暗号鍵にアクセス不可とすることが可能であり、ユーザーが設計したアプリケーションのみをアクセス可能にできること、複数のクラウドサービス事業者やオンプレミスでも同じ技術でデータ保護が可能となります。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス



まとめ

システム構成	暗号鍵管理	暗号鍵利用
BYOK	クラウド事業者	クラウド事業者
HYOK	ユーザー	クラウド事業者
BYOE	ユーザー	ユーザー

鍵管理におけるハードウェアセキュリティモジュールの役割[6]

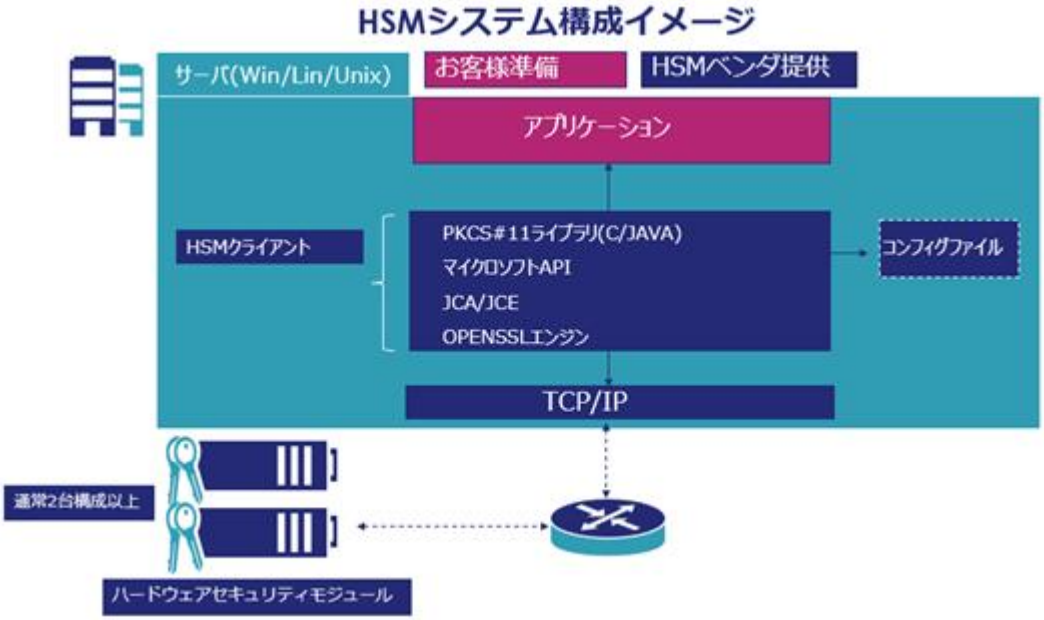
鍵管理において重要な機能であるハードウェアセキュリティモジュール(HSM)について説明します。

- HSM は鍵管理、利用のために設計された専用ハードウェアであり PCIE ボード、ネットワークアプライアンス、USB 接続等で利用可能
- アプリケーションサーバに鍵を渡すことなく、HSM 内部で暗号処理を実現することが可能
- FIPS (Federal Information Processing Standard) 140-2、ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation (コモンクライテリア)等の認定規格を取得

数十年前から PKI システムや金融決済ネットワークで多数利用実績があり、その信頼性から最近ではリモート署名システム,5G,各種製造業,ブロックチェーン等でも利用が進んでいます。

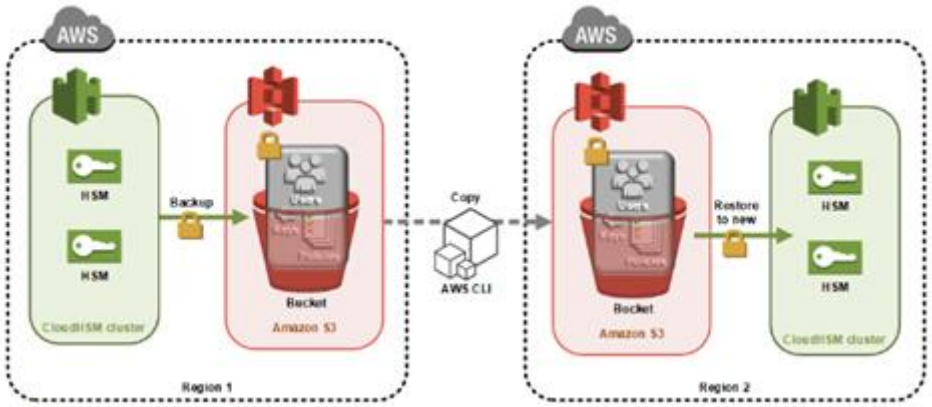
[6] 参考資料
Microsoft Azure Dedicated HSM: https://azure.microsoft.com/ja-jp/services/azure-dedicated-hsm/
AWS CloudHSM: https://aws.amazon.com/jp/cloudhsm/
https://aws.amazon.com/jp/blogs/security/how-to-clone-an-aws-cloudhsm-cluster-across-regions/
HSM を利用した鍵管理について (JNSA より): https://www.jnsa.org/seminar/seckey/201013/index.html

© 2021 一般社団法人　日本クラウドセキュリティアライアンス



多くのクラウドサービス事業者では KMS(鍵管理サービス)と HSM が提供されており以下が主要な差異になります。

- KMS
  - クラウドサービス事業者がマルチテナント式で鍵管理しているサービスであり、各種クラウドサービス (例、ストレージサービス) と連携されている暗号鍵管理サービス
- HSM
  - 顧客専用の HSM であり、SDK による開発、PKCS#11 をサポートしているアプリケーション連携可能な専用鍵管理システム
  - ユーザー自身で HA、バックアップスケジュール等の設計が必要
  - AWS CloudHSM では以下 4 台構成が推奨



各クラウドサービス事業者で HSM の提供形態は異なります。例えばマイクロソフト社や IBM 社ではオンプレミスでも提供されている Thales 社の HSM をクラウドで提供しており、オンプレミスとクラウドで同じシステムを構築することが可能です。また HSM ベンダ自身がクラウド HSM サービスを提供している例もあり、複数のクラウドサービス事業者上から Windows や Linux 上から API を利用してアクセスしたり、オンプレミスの HSM との HA 構成等が可能です。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

クラウドサービス事業者が提供している HSM サービスの多くが以下をサポートしておらず、オンプレミスの HSM の利用を検討する必要があります。

- HSM 自体に機能追加
- コモンクライテリア認定
- HSM 管理運用利用における 2 要素認証
- 鍵は常に HSM/バックアップ媒体も HSM であること
- 鍵生成の監査が必要
- 金融決済向け用途

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

6. クラウド認証・認可を活用したデータ保護事例
- Microsoft Information Protection

昨今、組織にとって情報保護が重要であるか？ という質問をした場合、ほとんど全ての組織が重要であると回答します。しかしながら、次に組織にとって保護するべき情報はどんな情報であり、またそれらはどこに保存してあり、どれだけの量が存在しているのか？という質問をした場合、即時回答する事が可能な組織は非常にまれです。

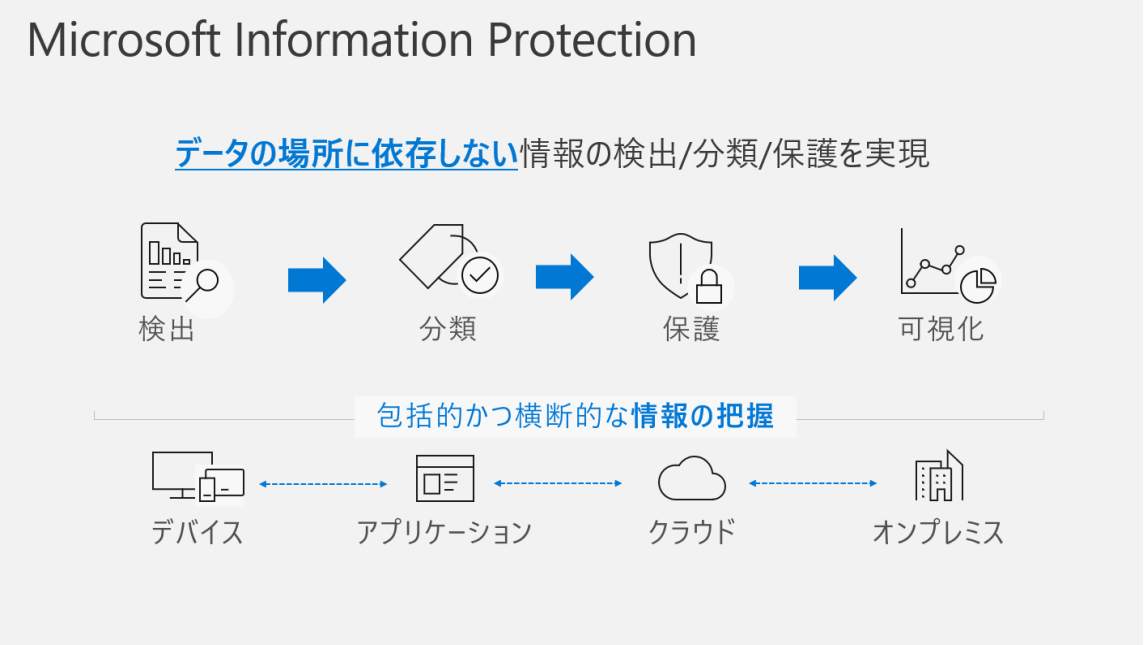
守るべき対象のデータの詳細を把握する事ができない状態で、どのようにして情報保護を実施する事ができるのでしょうか？

この一つの原因は、クラウド化に伴うデータの保管先の多様化にあります。これまで組織にとって重要なデータは境界 NW の内側である社内 NW 内に全て保管され、社内 NW 内のデバイスから、社内 NW 内のアプリケーションによってのみ利用されていました。しかしながらクラウド化が進むことにより、データは社内 NW の外に保管されるようになり、社外に持ち出されたデバイス上からクラウド上のアプリケーションによって利用されています。

その結果、これまでの方法で情報を保護する事が困難になっています。

そこで Microsoft は Microsoft Information Protection （以下 MIP）というデータ保護のためのフレームワークを提供しています。※ MIP は製品名ではなく、フレームワークの名前です。

MIP ではデータが、「デバイス」、「アプリケーション」、「クラウドサービス」、「オンプレミス」 いずれに保管/利用 されていたとしても機密情報を適切に保護する事を想定しています。そして、 MIP ではデータの場所に依存せずに機密情報を保護するために 「検出」⇒「分類」⇒「保護」⇒「可視化」 の 4 つのプロセスを自動的に処理する事でユーザーに負荷を与えることなく、情報保護を実現しています。



© 2021 一般社団法人 日本クラウドセキュリティアライアンス

検出

このプロセスはしばしば見逃しがちです。ほとんどの場合、ユーザーは「データを保護する」ことに注力しており暗号化等の保護方法ばかり検討していますが、「検出」は保護するべき対象を正確に把握するために非常に重要なプロセスとなります。

以前はこのプロセスは比較的容易に実現が可能でした。組織内の機密データは全て組織内の NW 内部に格納されており、全てが組織内で完結していました。しかしながら、クラウドが利用されるようになり、またエンドユーザーの働き方も変化する中でこの前提条件は既に過去のモノとされ、守るべき機密データは組織内のオンプレミス NW 内、クラウドストレージ内、クラウドアプリケーション内、エンドポイントのデバイス内と様々な場所に拡散しています。組織はこれらの完全にガバナンスを効かせる事ができない領域に保存された多様なデータを把握する必要があります。

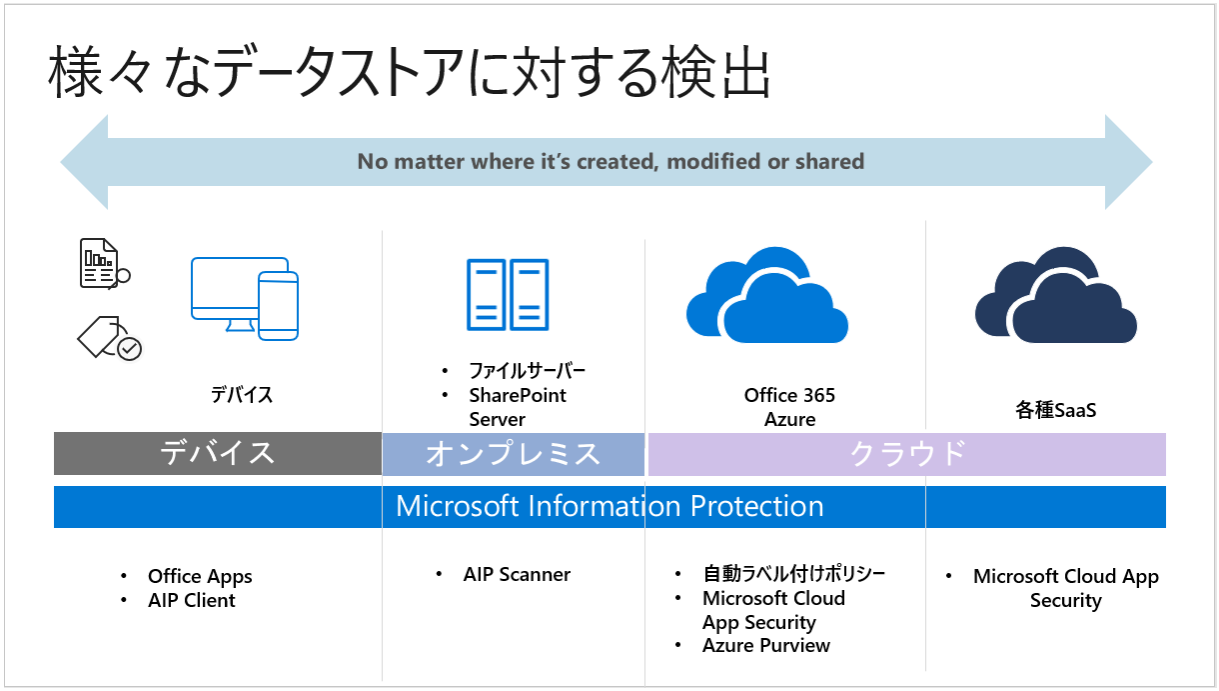
そのような環境において、どんなデータが現在どこに格納されているのか？を組織が明確に把握するためには、それぞれのデータストアに適したツールを決定する必要があります。 MIP の世界では

・オンプレミスリポジトリ（ファイル共有と SharePoint Server）の場合は Azure Information Protection スキャナー
・Office 365 クラウドアプリ（Exchange/SharePoint Online/OneDrive for Business）の場合は Office 365 自動ラベリング機能 または Microsoft Cloud App Security
・3rd パーティーのクラウドアプリケーションの場合は Microsoft Cloud App Security
・クライアント端末の場合は Azure Information Protection クライアント
・構造化データ内にある機密データの場合は Azure Purview

を用いてこれを実現しています。

これらのツールを利用し、それぞれのファイルを自動的にスキャンし、どのような種類の機密データが存在するのか？どのファイルに機密データが含まれているのか？ それらのファイルはどこに存在するのか？を検出します。

© 2021 一般社団法人 日本クラウドセキュリティアライアンス



分類

前述のプロセスで検出されたデータは、その重要度に応じたリスクレベルを設定する必要があります。そのためにはデータを分類分けし、各分類モデルの定義に対するリスク分析の結果に応じたデータ保護を実施する事で最もコスト効率の高い方法を選択する事が必要です。

※しばしば多くの組織において情報漏えいを恐れるあまり、全てのデータを暗号化する事でそのリスクを回避しようとしますが、これは非推奨となります。全てのデータを暗号化しても情報漏えいのリスクを完全に回避する事はできません。また、過剰な保護を実施する事でコスト効率が悪化するためセキュリティへの過剰な投資になるばかりでなく、利便性の悪化やリスクとなる場合があります。

しかしながら、この分類分けの作業は組織において情報保護ソリューションの導入の最初のハードルとなる事が多くあります。その多くは、分類モデルの定義の難しさとデータの分類手段です。

MIP では、この問題の内、分類分けの手段を MIP が既定で保持している世界中の様々な規制にマッピングされた 150 種類以上の機密情報タイプを利用して自動的に実施する事が可能です。また、組織固有の機密情報にも対応できるように、カスタム機密情報の種類を作成することも可能です。

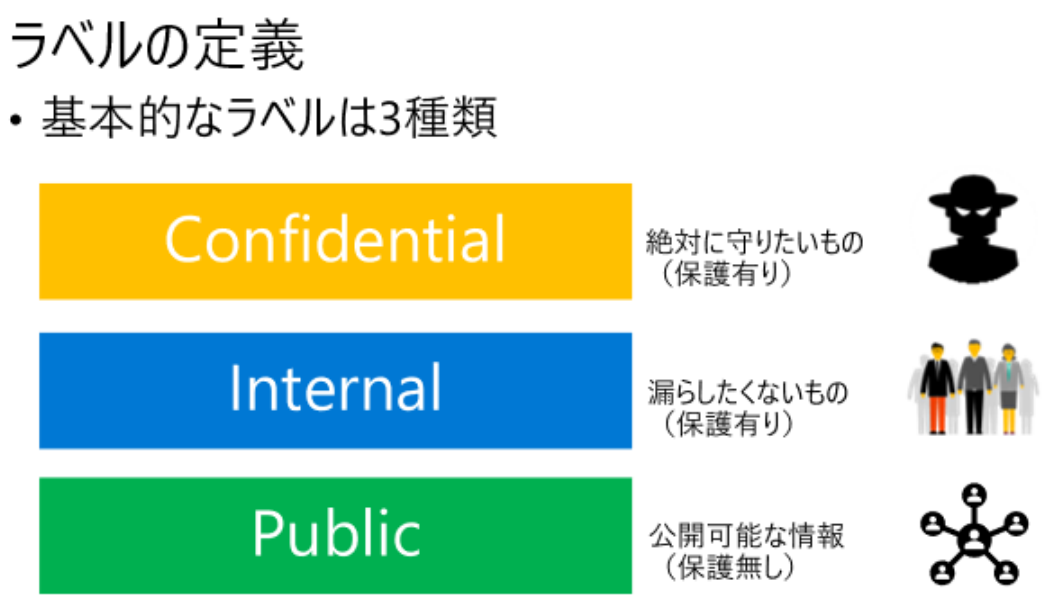
これらの自動的な分類分けポリシーを作成しそれに従って分類分けされたデータは、組織の分類モデルの定義によって作成されたラベルを付与され、ラベルによって MIP 内で管理されます。ラベルはデータに付与されたメタデータであり、それ自体は分類のための識別子でしかありません。

ラベルを付与されたデータは、今後この識別子に対して設定されたポリシーに従って保護、可視化されていきます。

MIP の世界において非常に重要なこれらのラベルやポリシーは Azure Information Protection（AIP） という製品において定義が可能となっています。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

AIP によって定義されたラベルは、その機密度に応じて保護の有無、保護内容を個別に設定する事が可能です。例えば、公開（Public）ラベルは保護設定はなし、社内限り（Internal）ラベルは暗号化保護を実施し社内のユーザーであれば誰でもアクセスが可能、機密（Confidential）ラベルは暗号化保護を実施し社内の VIP ユーザーのみアクセス可能といったラベル定義が可能です。



保護

分類時に付与されたメタデータであるラベルは、前述の通りそれ自体は識別子でしかありません。AIP ではそのラベル毎にポリシーを設定することができ、ラベルはポリシーに従い付与されたドキュメントに対して自動的に保護を実施します。保護を設定されたラベルは、ドキュメントを暗号化すると共に、そのドキュメントの承認された利用方法を定義します。

具体的には、保護を設定されたラベルによって暗号化されたデータは、どの ID によってアクセスが許可されているのか？を定義するだけでなく、編集が可能なのか？データをコピーする事は可能なのか？印刷する事は可能なのか？それらの許可の期限はいつまでなのか？等の詳細な認可情報を定義します。

これらの認可情報は全て Azure AD におけるユーザーID と紐ついており、ユーザーが暗号化されたファイルにアクセスする際には必ず Azure AD への認証および認可が必要となっています。

ユーザーが暗号化されたファイルにアクセスした場合、まず Azure AD で認証を要求されます。Azure AD で認証が成功した場合、次にそのユーザーID が認可されている情報が確認されます。対象のデータにおいて認可された情報が定義されていた場合、ユーザーはその認可情報に従ってデータへのアクセスが可能となります。

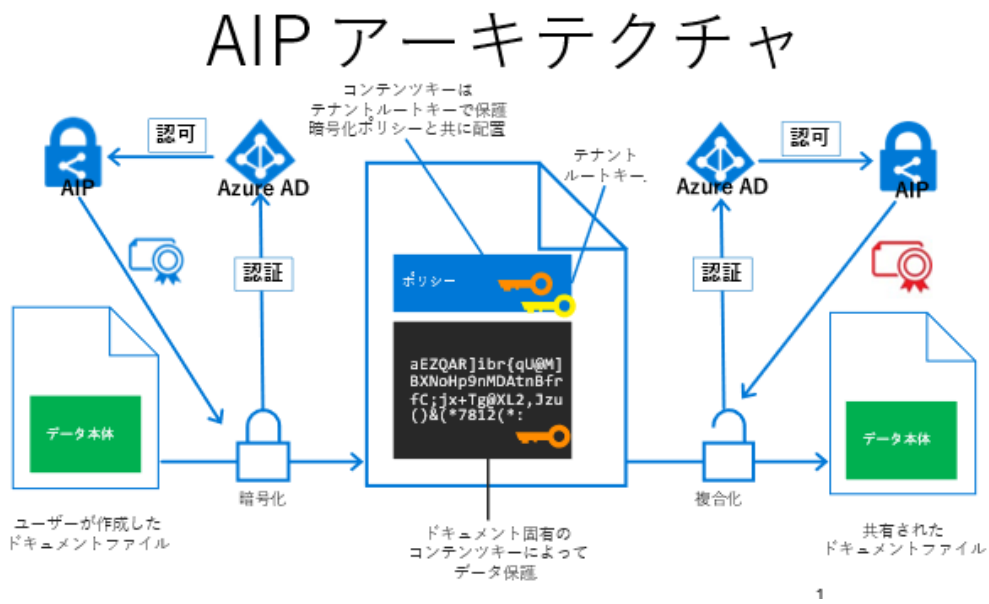
このような暗号化ソリューションは他にも多数ありますが、 AIP のデータ保護における最大のメリットはこのドキュメントのアクセスコントロールを Microsoft の IDaaS である Azure AD 上の ID 情報と紐付けた点になります。

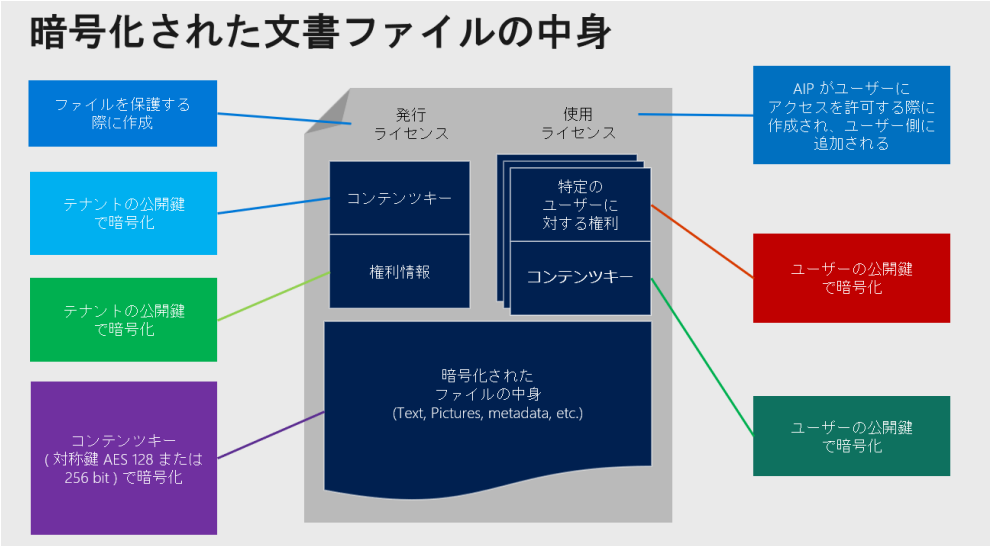
これまで ID 情報はオンプレミスの社内 NW 内にのみ存在していました。そのため、利用範囲が社内 NW にアクセスできる範囲に限られ、また社外のユーザーとの共有が難しいという課題がありました。それをクラウド上の IDaaS

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

をデータに対する認証基盤として選択する事で、社内であっても社外であっても保護が可能となり、また社外のユーザーとのセキュアな情報共有を実現しています。

また、データへのアクセス制御を IDaaS への認証・認可を必須とすることによって、全てのアクティビティログをクラウド上で確保する事ができるようになり、アクセス制御において重要な説明責任を容易に果たすことが可能となっています。この説明責任を果たすことは、この後記載している可視化に大きく影響を及ぼしています。





© 2021 一般社団法人　日本クラウドセキュリティアライアンス

可視化

前述の保護において、AIP は説明責任を IDaaS である Azure AD で果たしていると記載しました。これは AIP で保護されたファイルは、各ファイル毎にアクセスログ、アクティビティログをクラウド上で確保できることを意味しています。具体的には、いつ、どの IP アドレスから、どの ID から、どのファイルに対してアクセスのリクエストがあり、その結果アクセスが許可されたのか？それとも拒否されたのか？それらのリクエストは何回実行されたのか？等が全て Azure AD 上で可視化されます。

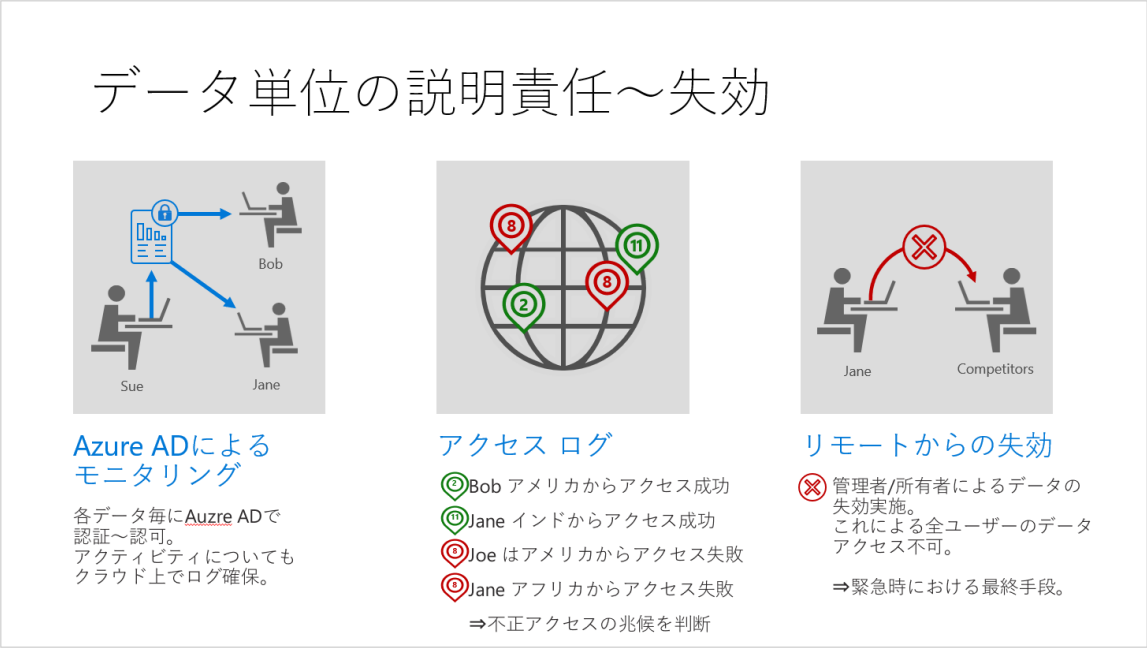
暗号化 ZIP ファイルに代表されるファイル共有方法の最大の問題点がこの説明責任の可視化です。

ファイル単位で暗号化だけを実施した場合、そのファイルが所有者の手元から離れた場合、暗号化が解除されたのか？誰がアクセスしたのか？等の把握をする事は困難です。また逆にそれらが把握ができない結果、手元を離れたデータが所有者の意図した機密性を維持できている事を証明することができなくなり、そもそもの目的である機密データの保護が実現できなくなります。

AIP ではクラウド上でこれらのログを保管し、また分析も同時に実施します。その結果、社内からしかアクセスされないはずの機密ファイルが、想定していない場所から頻繁にアクセスリクエストがある等の不審なアクセスが可視化され、情報の漏えいの前兆をとらえる事が可能となります。

そして、もしその機密ファイルはまだアクセスに成功はされていないが、不審なアクセスのリクエストが継続して実施されていると判断された場合は、クラウド上に存在するそのドキュメントを複号化するための秘密キーを失効させることで、該当ファイルは誰もアクセスできない状態に強制し、情報漏えいを防ぐ事が可能となります。

これにより機密データが所有者の手元から離れた状態にあっても、可視化によって機密性の確保状態を分析し、情報漏えいのリスクがあると判断される場合には失効によって機密性の確保を可能とします。



© 2021 一般社団法人　日本クラウドセキュリティアライアンス

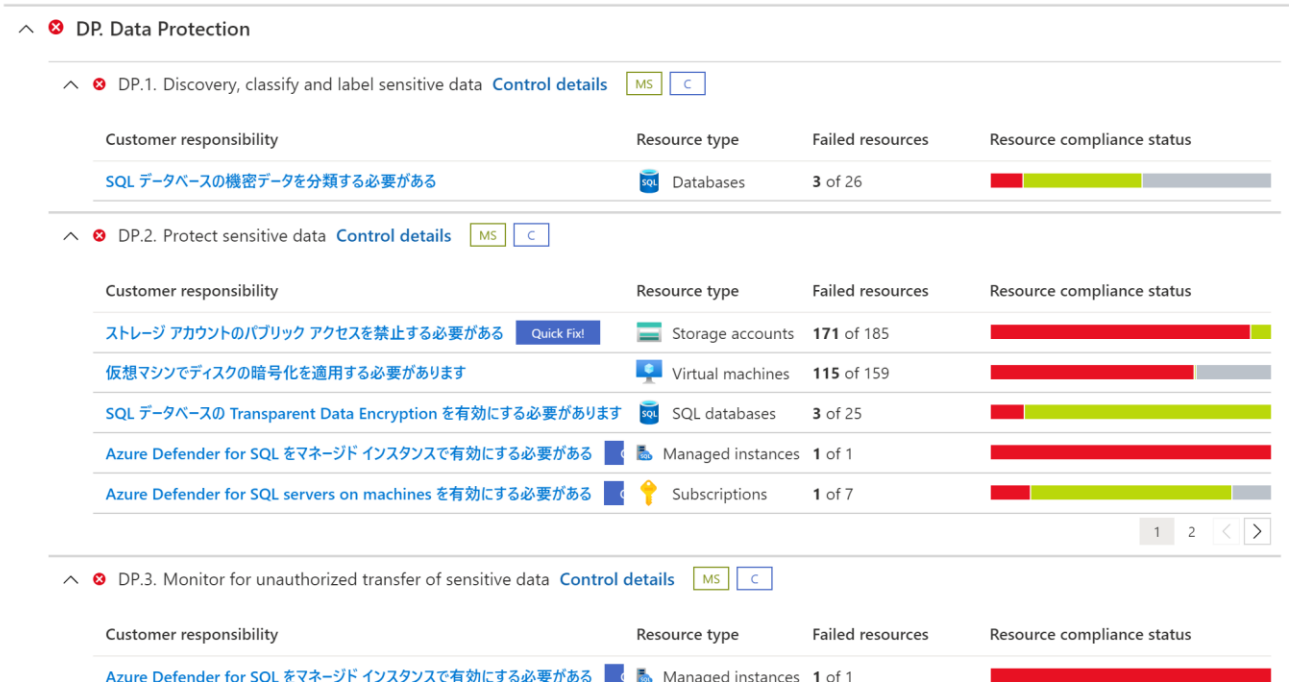
7. モニタリング

- CWPP、CSPM

パブリッククラウドにおいて、データは IaaS 上の仮想サーバーや、PaaS のデータベース、オブジェクトストレージ、データレイクなどに保存されます。パブリッククラウドにおいては、データを保存したり分析したりする環境を容易に作成できますが、その一方で各リソースのセキュリティ構成の管理が難しくなります。パブリッククラウドのデータにまつわるセキュリティインシデントの多くが、セキュリティ構成の誤りから生じており、これをいかに防ぐかが重要になります。

そのためには、パブリッククラウドのセキュリティ構成を継続的に可視化し、誤構成の検知やポリシーの適用、コンプライアンスの評価を行っていく必要があります。主要なパブリッククラウドでは、構成を評価する機能（Cloud Security Posture Management, CSPM）が提供されており、まずはそれらのツールを活用し、誤構成を検知し修正していくことが重要です。

たとえば、Microsoft Azure の場合、Azure Security Center が CSPM の役割を担います。セキュリティ管理者は、Azure 上のシステム（サブスクリプション）に対して、Security Center を通して可視性を確保し、仮想マシンやデータベース、ストレージへのアクセス設定などの不備がないことを日々確認することが推奨されています。

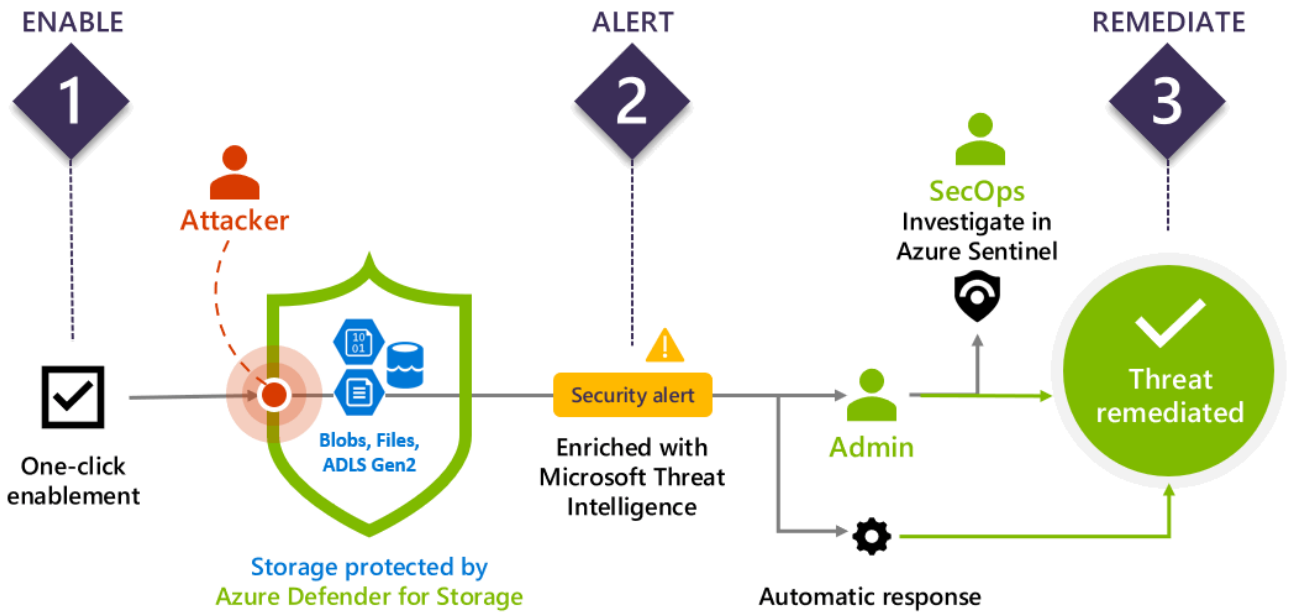


また、ゼロトラストのアプローチに基づき、パブリッククラウドの環境においてもふるまい分析をベースに侵害の検知を常に同時に行っていく必要があります。仮想サーバー上のデータを保護するには、OS 以上のレイヤーについてはユーザー側でセキュリティ管理を行っていく必要があります。サーバーの脆弱性の評価や不正アクセスの検知、不正操作の検出などを常

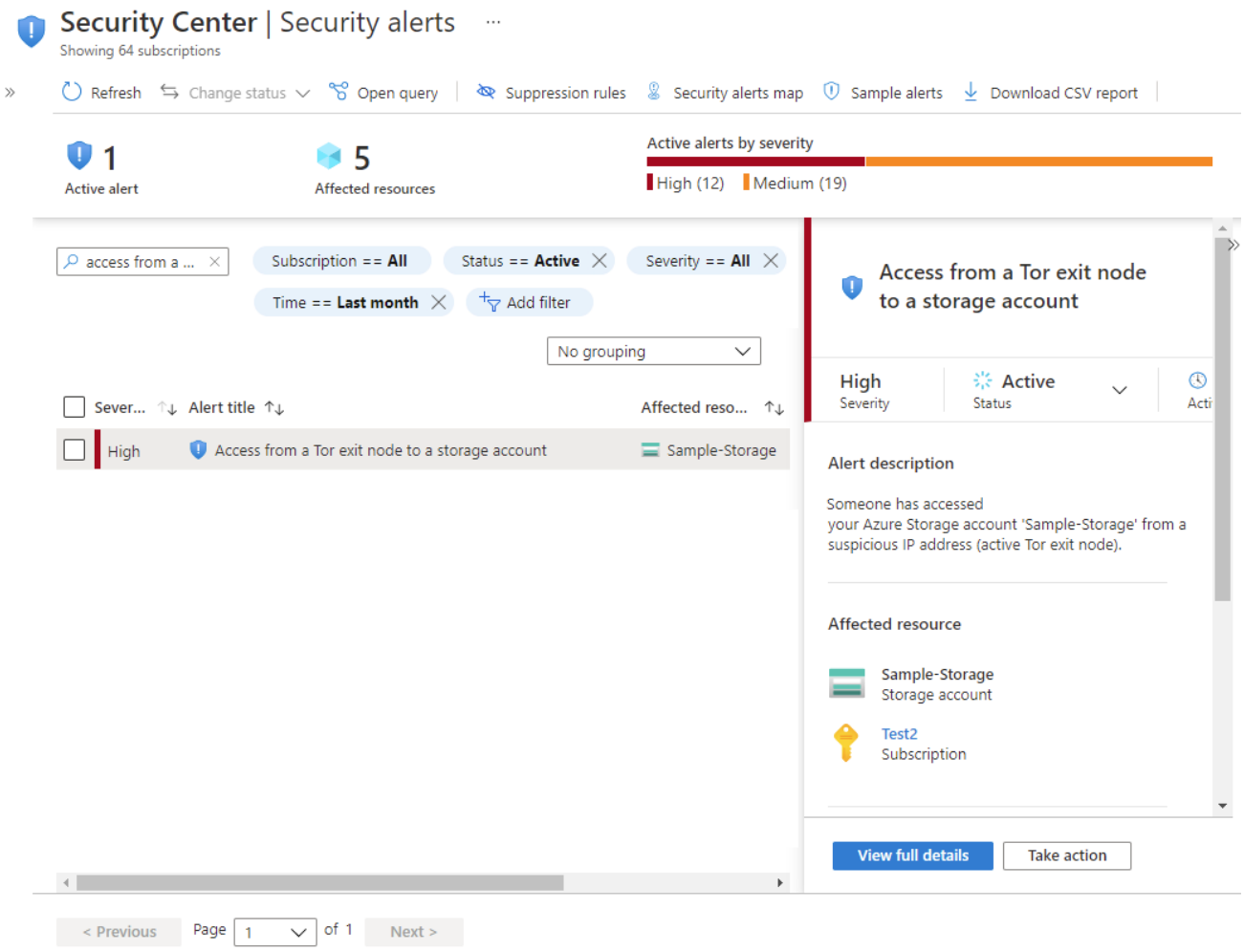
© 2021 一般社団法人　日本クラウドセキュリティアライアンス

時行うことが重要です。一方、PaaS の場合は、OS やランタイムの管理はクラウドプロバイダーの担う範囲となり、ユーザー側のセキュリティ負荷が下がり、一般的にセキュリティは向上します。ただ、アクセスの管理はユーザー側の責任であることは変わらず、データへのアクセスを監視し、個々のアクセスの正常性を確認する必要があります。

たとえば、Microsoft Azure の場合、Cloud Workload Protection Platform (CWPP) のツールである、Azure Defender を活用して IaaS や PaaS の脅威検知を行うことが、CIS Benchmark などで推奨されています。IaaS のサーバーに対してはエージェントやスキャナーを導入し、ユーザーは OS 以上のレイヤーの脆弱性や攻撃の検知を行うことが推奨されています。一方、PaaS に対しては、Azure Defender によって、ストレージやデータベースへの不正アクセスや不正操作が検知されます。



© 2021 一般社団法人　日本クラウドセキュリティアライアンス



また、CWPP によるデータへの不正アクセスや不正操作のアラートは、認証ログやアクセスログとともに、Security Information and Event Management (SIEM)ツールで SOC チームによって監視されるのが理想的です。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス

おわりに

本資料では暗号化・鍵管理といったデータ保護の基礎だけでなく IT 環境の変化、データセキュリティライフサイクル、ゼロトラスト、モニタリング（CSPM：Cloud Security Posture Management）についても触れました。実装例として MIP, Microsoft Information Protection、を取り上げ読者がクラウド環境でのデータ保護についてイメージし易いように工夫いたしました。

国家主導型も含め、サイバー攻撃は収まることがなく高度化していきます。クラウド活用による利便性を享受しつつデータ漏洩を防ぐことがセキュリティ担当者に求められています。本書がそういった困難な状況に立ち向かっている方たちへの一助となれば幸いです。

© 2021 一般社団法人　日本クラウドセキュリティアライアンス