

クラウド重大セキュリティ脅威対策

– DevSecOps のユースケース –

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)
クラウドセキュリティワーキンググループ

目次

1. はじめに	5
2. 検討指針	6
2.1. 目的	6
2.2. 前提	6
3. ユースケース(クラウド重大セキュリティ脅威 11 の悪質な脅威)	7
3.1. ケース 1: データ侵害	7
3.2. ケース 2 設定ミスと不適切な変更管理	12
3.3. ケース 3 クラウドセキュリティアーキテクチャと戦略の欠如	16
3.4. ケース 4 ID・資格情報・アクセス・鍵の不十分な管理	21
3.5. ケース 5 アカウントハイジャック	25
3.6. ケース 6 内部者の脅威	29
3.7. ケース 7 安全でないインターフェースと API	33
3.8. ケース 8 弱い管理プレーン	37
3.9. ケース 9 メタストラクチャとアプリストラクチャの障害	39
3.10. ケース 10 クラウド利用の可視性の限界	43
3.11. ケース 11 クラウドサービスの悪用・乱用・不正利用	47
4. 参考・引用文献	51

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、以下の場合に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。
- (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。

本書執筆編集メンバー

井上 淳

釜山 公德

平鹿 一久

森田 翔

※五十音順

● 変更履歴

日付	版数	変更内容
2021 年 10 月 25 日	1.0	初版発行

1. はじめに

パブリッククラウド(以下クラウド)において、民需にて市民権を得るだけでなく、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」にてクラウド・バイ・デフォルトの原則が公開されている通り、パブリックセクターにおいてもクラウドの利用を促進していることが伺える。

なぜ、クラウドか。

クラウドには NIST SP800-146 に記載がある通り未解決の問題があるが、それを補って余る多大なメリットがあり、ビジネスアジリティの向上、バリュークリエーションの実現に欠かせない存在となっている。ただし、ただ単にクラウドを利用するだけではクラウドメリットの享受は極小的になり、デメリットが前面にでてしまう事態が散見され、例えば、移行戦略で rehost を選択する場合、オンプレミスのサーバー群をそのまま IaaS へと移行するといった手段だ。これでは、ハードウェアにおけるメンテナンスフリーは実現できるものの、責任共有モデルでいうところの OS レイヤー以上の責任部分は利用者にあたるため、運用・管理・監視がオンプレミスとクラウドとで二重苦になり、クラウドの利用で不幸を事案が発生することは少なくない。

クラウドメリットを最大限享受するためには、PaaS や SaaS といった抽象度の高いサービスモデルであらゆる負荷を軽減し、体制として開発(Dev)と運用(Ops)を最適化し、継続的な改善と価値創造を実現する DevOps に専念すべきである。

ここで留意すべき点は、セキュリティだ。

クラウドは総じてセキュアとは言えるが、責任共有モデルが示す通り、どのサービスモデルにおいても利用者側には責任が生じる。DevOps により継続的な改善と価値創造を実現しても、攻撃者によりシステムやサービスの停止、最悪の場合は顧客情報や機密情報等の漏洩に繋がり、信頼の失墜や収益の激減にいたることが懸念される。

このためには DevSecOps (SecDevOps) が有効だと考えるが、DevSecOps を実現させるための情報が乏しい。

実現の課題を解決するため、クラウドセキュリティ WG では、クラウドセキュリティアライアンスの成果物である「クラウドの重大セキュリティ脅威 11 の悪質な脅威」を用いて、脅威を起点としたユースケースを整理し、利用者がよりイメージをつきやすくする一助となるドキュメントの作成に踏み切った。

DevSecOps の実現を容易にすることに寄与できれば幸甚である。

日本クラウドセキュリティアライアンス
クラウドセキュリティワーキンググループ
リーダー 釜山 公徳

2. 検討指針

2.1. 目的

Cloud Security Alliance (CSA) において、クラウドコンピューティングのためのセキュリティガイダンス（以下、ガイダンス）において DevSecOps の重要性を説いている。現状、実環境へ DevSecOps を落とし込むにあたり、公開されている具体的な情報が少ない。ここで、ユースケース毎に DevSecOps を当て嵌め、実現性の向上に寄与する。

2.2. 前提

以下 3 事項を前提とする。

① 記載の方針

ガイドラインの要約、ならびにワーキンググループにて独自に解釈したものとする。

② DevSecOps における解釈の正確性

現状、知り得る範囲で考察して執筆しているため、正確性の保証はない。

③ 全体の記載粒度

- ・ ケース毎に担当を割り振り、執筆者のパッションを重視しているため、粒度に相違を許容している。
- ・ [DevSecOps を踏まえた対処] の記載内容は、ケース毎に完結することを前提とし、同じ項目でもケースが異なれば概要と対応例が異なる。ただし、他ケースの引用する場合はその限りでは無い。

④ 対応例の内容

- ・ 具体性を出すため、プロダクトやクラウドサービスを記載するが、全ての対応例に一律に記載するのではなく、必要に応じて記載することとする。
- ・ クラウドサービスは執筆時点での名称とし、利用可能なリージョンは意識しない。

3. ユースケース(クラウド重大セキュリティ脅威 11 の悪質な脅威)

3.1. ケース 1: データ侵害

3.1.1. 概要

データ侵害とは、機微情報、保護情報、機密情報が外部に公開されることであり、勝手に閲覧、盗用など、権限のない人によってデータが使用されてしまうものである。

データ侵害は、標的型攻撃のほか、人的エラーやアプリケーション脆弱性などが起因して発生する。

3.1.2. ビジネスインパクト

データ侵害は、企業の信頼の低下をはじめ、以下のような影響をもたらす。

- ・ 評価、信頼の影響
- ・ 競合他社に対する知的財産の漏洩
- ・ 金銭的損失につながる規制の影響
- ・ ブランド価値の低下
- ・ 法的および契約上の責任の発生
- ・ 対応に関わる金銭的損失

3.1.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- 2018 年、Timehop 社はクラウド環境の侵害により、ユーザー 2,100 万人分のデータ侵害にあった。
- 2016 年後半、Uber 社は AWS アカウントのハッキングにより、ユーザー 5,700 万人の個人情報に関するデータ侵害が発生した。
- 2019 年、Voipo 社は 700 万件の顧客通話記録、600 万件の SMS ログ、認証情報を含む内部ドキュメントを意図せず公開していた。

3.1.4. 当問題に対するポイントと対応策

「データ侵害」における対応策の第 1 のポイントは、当該システムが取り扱うデータのプロファイルを明確にしておくことである。これには、データ管理表としてアプリケーションやネットワークに常時または一時的に存在するデータを明らかにし、データフローの文書化、データタイプ、価値、機微性、重要性に基づいて機密区分を付しておくことが含まれる。これにより、データ侵害に対する対策を適切に維持するとともに、万一の侵害発生の影響の限定を図ることが可能になる。

第 2 のポイントは、データセキュリティを確保するためのポリシーと手順を確立し、それを維持することである。特に、複数のシステムや取引を構成する機能をまたがる場合に、データの機密性、完全性、可用性を確保できるように留意しなければならない。また、システムにアクセスするすべての人に関する ID 情報を保管・管理し、個人のアクセスレベルを決定できるようにしなければならない。ポリシーは影響を受ける全ての関係者がいつでもレビューできるようにし、事業責任者により承認を受けることが必要である。

第 3 のポイントは、暗号プロトコルの適切な使用と鍵管理である。

機微なデータは、ストレージ内、データ使用時、及びデータの送受信時に適切な暗号プロトコルにより暗号化されなければならない。また、鍵の生成から廃棄、更新に至るライフサイクルを管理し、安全な鍵生成に適した

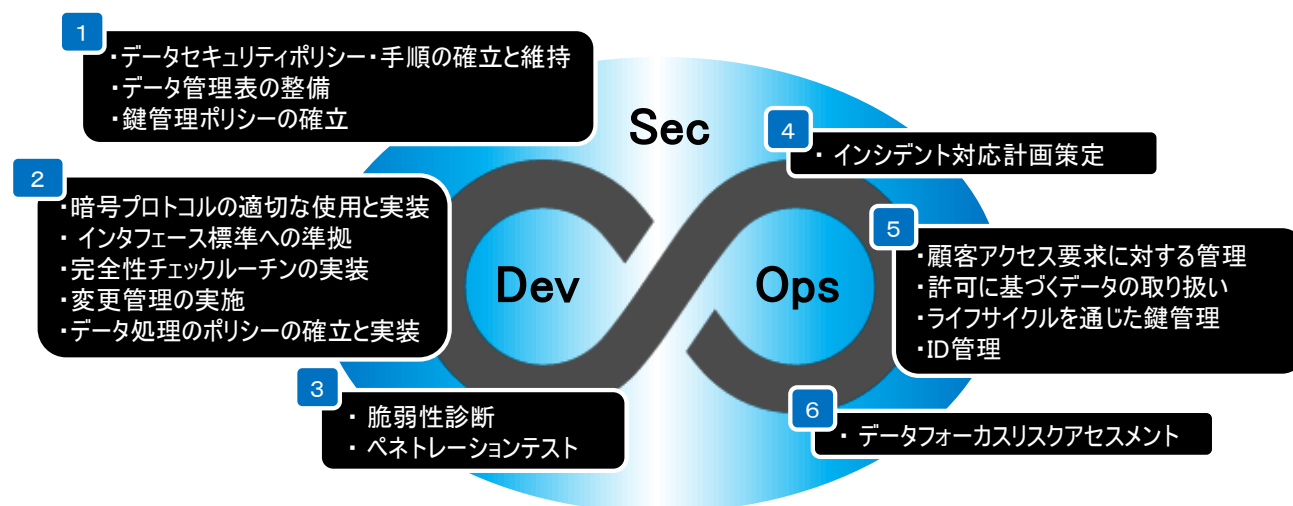
アクセス制御、鍵の交換及び保管を実現しなければならない。クラウド事業者が提供するマネージド HSM（ハードウェア暗号モジュール）サービスを活用することが有効である。鍵の管理と鍵の使用は、異なる責務として分離されなければならない。

最後のポイントは、データフォーカスリスクアセスメントの実施である。

データガバナンスの要求事項に従い、リスクアセスメントを事前に定められた間隔、及びシステムを変更した際に実施しなければならない。アセスメントには、機微なデータがどこで保管され送受信しているかの認識、定められた保存期間及び使用終了時の廃棄に関する要求事項への準拠、データの分類ならびに許可されていない使用、アクセス、紛失、破壊、改竄からの保護に関する事項が含まれる。

3.1.5. DevSecOps サイクル

アプリケーションとインターフェースセキュリティ、変更管理と構成管理、データセキュリティと情報ライフサイクル管理、暗号化と鍵管理、ガバナンスとリスク管理、アイデンティティとアクセス管理から主要なアクティビティを抽出し、DevOps サイクルに対応策をマッピングしている。



3.1.6. DevSecOps を踏まえた対処

3.1.5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	データセキュリティポリシー・手順の確立と維持	複数のシステムや取引を構成する機能をまたがる際、データの機密性、完全性、可用性を確保できるようにデータセキュリティのポリシー及び手順を確立する。 ポリシーは影響をうける全ての関係者がいつでもレビューできるようにし、事業責任者により承認を受けておく。	- 以下データセキュリティポリシーを整備する。 -基本方針 -対策基準 -管理体制 - 以下データセキュリティ手順を整備する。 -データ資産管理手順 -アクセス制御認証手順 -機器利用手順

			-鍵管理手順
	データ管理表の整備	データ管理表としてアプリケーションやネットワークに常時または一時的に存在するデータのデータフローを作成し、文書化する。 また、データ及びデータを含むオブジェクトに対して、データタイプ、価値、機微性、重要性に基づいて機密区分を付しておく。	・データ管理表を整備する。 ・データフロー図を整備する。
	鍵管理ポリシーの確立	組織として鍵管理に関するポリシーを確立する。鍵には識別可能な所有者を対応づけておく。また、鍵の管理と鍵の使用は、異なる責務として分離する。	・以下鍵管理ポリシーを整備する。 -使用アルゴリズム -ライフサイクル -アクセス方法 -保管・配布 -バックアップ
2	暗号プロトコルの適切な使用と実装	機微なデータについて、ストレージ内、データ使用時、及びデータの送受信時の暗号化を行う。暗号化には、オープン、検証済の標準アルゴリズムを利用する。 クラウド事業者が提供するマネージド HSM サービスを活用することが有効である。	・ TLS を使用する。 ・ HSM (Hardware Security Module) サービスを使用する。以下、パブリッククラウドのサービス例。 -AWS CloudHSM -Azure Dedicated HSM -Google Cloud HSM
	インターフェース標準への準拠	プログラム間のインターフェースには、業界の認める標準に基づいた設計、開発及び導入を行う。当該インターフェースは該当する法的及び規制を遵守する。	・ 以下のような標準化された API を使用する。 -(FAPI) Financial-grade API -Open Banking API
	完全性チェックルーチンの実装	データの入出力について、マッチングやエディットチェックなどデータ完全性をチェックするためのルーチンを実装する。	・ 完全性確認ツールを使用する。 -Tripwire ・ エディットチェックツールを使用する。
	変更管理の実施	システム間のインターフェース変更に関わる設計、及び設定の変更を行う場合は、確立されたポリシーと手順に基づいて実施する。	・ 変更管理ポリシーを整備する。 ・ 変更管理手順を整備する。
	データ処理のポリシーの確立と実装	データ、及びデータを含むオブジェクトのラベリングを確立されたポリシーに基づいて実施する。データをまと	・ 情報の分類体系を整備する。 ・ タグ付け機能を実装する。 ・ メタデータ付与する。

		めて格納するオブジェクトには、ラベルを継承して保持する仕組みを実装する。	
3	脆弱性診断	公開されるサービスに対してデータ侵害に対する脆弱性有無を診断する。	・対象サービスに応じて、プラットフォーム診断とアプリケーション診断の実施有無を判断し、適切に実施する。
	ペネトレーションテスト	公開されるサービスに対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。事前に定められた間隔及びシステム変更時に実施する。	・適切なエンゲージメントの上、ペネトレーションテストやレッドチーム演習を実施する。
4	インシデント対応計画策定	データ侵害に関するインシデントが発生した際の検知、復旧、事後対応までの体制、連絡フロー、各種手順を対応計画として定める。法律や関連する規制、社内規定に準拠する。	・インシデント対応計画を整備する。 -インシデント対応体制 -連絡フロー -対応プロセス -業務復旧・継続手順
5	アクセス要求に対する管理	データへのアクセス要求があった場合は、セキュリティ、契約、規制における要求事項を把握した上で許可を行う。	左記に同じ
	許可に基づくデータの取り扱い	データの利用は、影響を受けるデータのすべての顧客からの文書化された許可を必要とする。また、関連する法律及び規制に従う。本番環境のデータのテスト環境へのコピーは禁止する。	左記に同じ
	ライフサイクルを通じた鍵管理	鍵の生成から廃棄、更新に至るライフサイクルを管理し、安全な鍵生成に適したアクセス制御、鍵の交換及び保管を実現する。	左記に同じ
	ID 管理	システムにアクセスするすべての人に関する ID 情報を保管・管理し、個人のアクセスレベルを決定できるように管理する。	左記に同じ
6	データフォーカスリスクアセスメント	データガバナンスの要求事項に従い、アセスメントを実施する。アセスメントでは、機微なデータがどこで保管され送受信しているか、データ廃棄が要求事項に準拠して行われているか、データの分類に従い、許可されていない	・以下アセスメントを実施する。 -データ保管状況 -データ廃棄状況 -データ使用状況

		使用が行われていないか、紛失/破壊/改竄が発生しているか確認を行い、データ侵害に焦点をあてたリスク要因の特定と評価を行う。リスクアセスメントを事前に定められた間隔、及びシステムを変更した際に実施する。	
--	--	---	--

3.2. ケース 2 設定ミスと不適切な変更管理

3.2.1. 概要

設定ミスは多くの場合、悪意ある活動に対して脆弱な状況を生む。これには、セキュリティ保護されていないデータストレージ、過剰なアクセス権限、デフォルトから変更されないままの資格情報や設定、標準セキュリティ制御の無効化、パッチの未適用、ロギングや監視の無効化、ポートやサービスへの無制限のアクセスなどが含まれる。

適切な変更管理の欠如は、設定ミスの一般的な原因となる。

クラウド環境では、従来の変更プロセスより変更の制御が困難になる。インフラストラクチャの要素はソフトウェアに抽象化され、変更ライフサイクルはごく短時間になるなど複雑さが増しているため、このような環境下では、変更管理と修復のためのアジャイルでプロアクティブなアプローチが必要になる。

3.2.2. ビジネスインパクト

設定ミスによるビジネスインパクトは、設定ミスの内容、それが検出・緩和される速度により深刻度は変わるが、最も一般的な影響は、クラウドに保存されているデータの漏洩となる。

3.2.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- 2017 年、Amazon S3 の設定ミスにより、データ分析会社 Alteryx 社所有のデータが公開状態になっていることが発覚した。このデータには Experian 社の調査情報や米国国税調査局のデータ 1 億 2300 万人分が含まれていた。
- 2018 年、データベースサーバーの設定ミスにより、Exactis 社が所有する 2 億 3000 万人の個人データを含むデータが公開状態になっていることが発覚した。
- 2018 年、rsync サーバの設定ミスにより、Level One Robotics 社は GM、フォード、テスラ、トヨタなど 100 社以上の機密情報を誰でもアクセスできる状態にしていた。

3.2.4. 当問題に対するポイントと対応策

「設定ミスと不適切な変更管理」の対応策の第 1 のポイントは、変更管理ポリシーとベースラインの確立である。

全ての変更に対して、リリースされる前に登録された変更要求や顧客の承認を全て満たしていることを保証できるよう変更管理ポリシー、及び手順を策定することが望ましい。また、セキュリティのベースラインとなる要求事項を定め、標準的な設定から逸脱する場合は、変更管理ポリシーに従って承認を受けなければならないようにする。これらは、クラウド特有の抽象度・ライフサイクルの速度に対応できるよう考慮する。

第 2 のポイントは、品質検査の実施である。ベースライン、テスト及びリリース基準を備えた品質検査により、定義されたセキュリティ品質基準を満たせるようにする。各クラウド事業者から提供される設定の自動チェックツールも併せて利用することも有効である。また、すべての変更を記録し、仮想化されたインフラの変更実績を確認できるようにする。

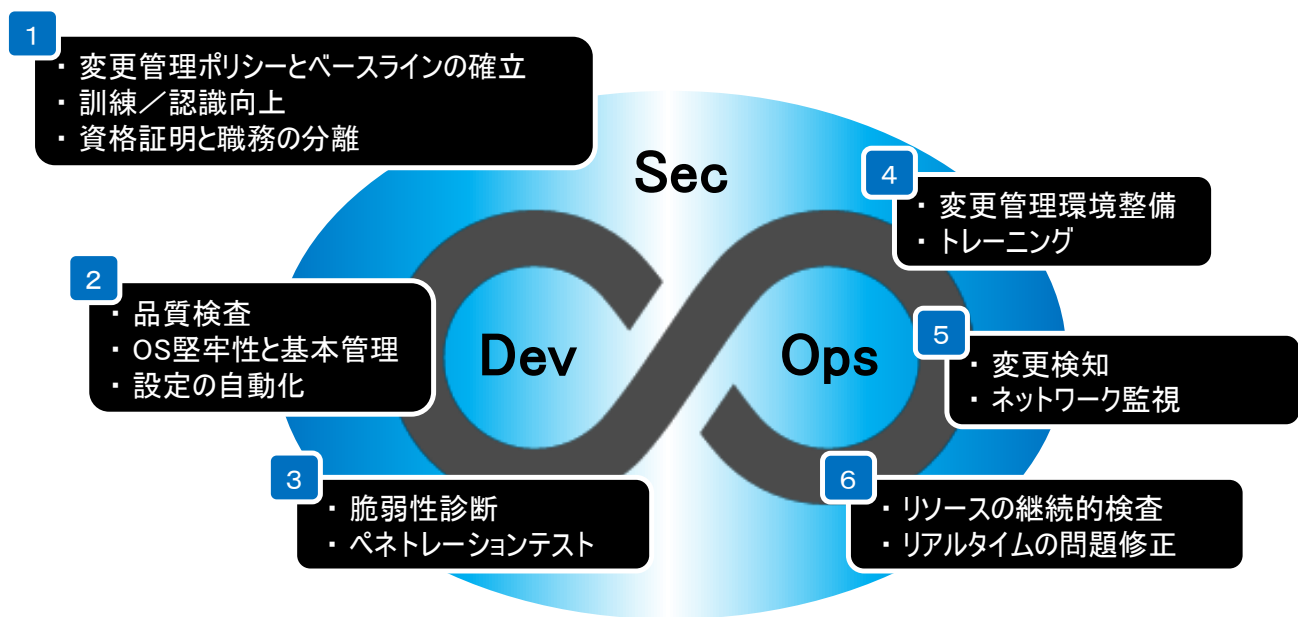
第 3 のポイントは、関係者に対する訓練および資格証明と職務の分離である。セキュリティ意識向上の訓練プログラムを策定し、ポリシー、手順、プロセスに対する意識向上を図る。また、適切な身元確認、権限付与を行

うとともに、職務分離方針に基づき、実施できる業務を制限する。

最後のポイントは、OS 堅牢性と基本管理の徹底である。各システム、コンポーネントは業務に必要十分なポート、プロトコル、サービスのみを提供するようにする。また、クラウド事業者が提供する境界防御、モニタリング、ログ収集等のサービスをベストプラクティスに基づき活用する。

3. 2. 5. DevSecOps サイクル

変更管理と構成管理、データセキュリティと情報ライフサイクル管理、暗号化と鍵管理、ガバナンスとリスク管理、人事、アイデンティティとアクセス管理、インフラと仮想化のセキュリティから主要なアクティビティを抽出し、DevOps サイクルに対応策をマッピングしている。



3. 2. 6. DevSecOps を踏まえた対処

3. 2. 5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	変更管理ポリシーとベースラインの確立	リリースされるサービスに関して、影響度や優先順位を定義する。 全ての変更に対して、リリースされる前に登録された変更要求や顧客の承認を全て満たしていることを確認する。 セキュリティのベースラインとなる要求事項を定め、標準的な設定から逸脱する場合は、変更管理ポリシーに従って承認を受けるように定める。	左記に同じ
	訓練／認識向上	関係者に対するセキュリティ意識向上の訓練プログラムを策定し、必要に応じてその受講を義務付ける。ポリシー	・セキュリティ訓練(セキュリティ基礎など)の実施 ・レッドチーム演習／TLPTの実施

		一、手順、プロセスに対する意識向上及び定期的更新を実現する。	
	資格証明と職務の分離	適切な身元確認、権限付与、アクセス管理を行うためのポリシー及び手順を確立し、これらを補強するためのプロセスと技術的対策を実装する。	・アクセス管理ポリシーの設定 ・身元確認方法の確立
2	品質検査	ベースライン、テスト及びリリース基準を備えた品質検査により、定義された品質基準を満たせるようにする。クラウド事業者毎に用意された設定の自動チェックツールも併せて利用することが有効である。	・以下（例）のサービスを利用した管理を実施 -AWS Blueprints -Azure Security Center, Azure Blueprints
	OS 堅牢性と基本管理	各システム、コンポーネントが業務に必要な十分なポート、プロトコル、サービスのみを提供するように設計・設定する。また、クラウド事業者が提供する境界防御、モニタリング、ログ収集等のサービスをベストプラクティスに基づき活用する。	・以下（例）のサービスを利用した管理を実施 -AWS Trusted Advisor -Azure Advisor -Google Security Command Center
	設定の自動化	設定をソフトウェアで定義し、その変更をパイプラインなど自動化した手続きで実施する。	左記に同じ
3	脆弱性診断	公開されるサービスに対して脆弱性診断を実施し、脆弱性の有無を確認する。	・対象サービスに応じて、プラットフォーム診断とアプリケーション診断の実施有無を判断し、適切に実施する。
	ペネトレーションテスト	公開されるサービスに対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。	・適切なエンゲージメントの上、ペネトレーションテストやレッドチーム演習を実施する。
4	変更管理環境整備	設定自動化、検査、リアルタイムの問題修正などを実施するために、その時点で最適なテクノロジーを採用し、利用環境を整備する。	左記に同じ
	トレーニング	対象者に対し、設定および環境維持に必要なトレーニングを実施する。	・IT サービスマネジメントに関するトレーニングを実施する。
5	変更管理	変更管理ポリシー及び手順に従って変更管理を実施する。すべての変更を記録し、承認された変更以外の変更が実施されないようチェックする。	・変更記録（ログ）を収集・管理し、定期的なチェックを行う。
	ネットワーク監視	信頼できるネットワークと信頼でき	・以下（例）を導入し、ネットワー

		ないネットワーク間のトラフィックを制限し、監視を行う。不正なトラフィックが検知された場合は、通信遮断などの対処を行う。	ク制御・監視を実施する。 -ファイアウォール -IDS/IPS -WAF
6	リソースの継続的検査	設定が適切に保たれているか、変更管理が適切に維持されているか検査を行う。	左記に同じ
	リアルタイムの問題修正	問題が検知された場合、リアルタイムに修正を行う。	・問題発生時に即座に検知する仕組みを導入し、適切な対応フローと体制の整備を行う。

3.3. ケース 3 クラウドセキュリティアーキテクチャと戦略の欠如

3.3.1. 概要

この問題は、利用者のサービス機能の拡張とセキュリティ施策に対して警鐘を鳴らした内容である。クラウドへ移行する企業が増えている現在、サービス機能の拡張が優先され、不適切なセキュリティアーキテクチャだった場合、攻撃に対するリスクが発生する危険性がある。

3.3.2. ビジネスインパクト

適切なセキュリティアーキテクチャと戦略は、クラウドにおける安全な移動、配置、運用に必要な要素である。不適切なクラウドアーキテクチャに対してサイバー攻撃が成功すると財務上の損失、信用ダメージ、法的な悪影響、罰金などのビジネスに対する重大なインパクトを及ぼす可能性がある。

3.3.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- クラウドストレージにホストしたセキュアでないクラウドサーバにプライベートデータを保管し、サーバの Web アドレスさえ分かれば、パスワードなしでデータをダウンロードできる状態だった。保管しているデータには機密性の高いパスワードや復号鍵が含まれていた。(アクセンチュア、2017 年)
- 自動車と連動するアプリに登録しているユーザーの個人情報 5 万人分以上がクラウドサービス上で公開されていた。データを保存するディレクトリの設定を誰でも閲覧できる「公開状態」にしていたのが原因。(本田インド法人、2018 年)

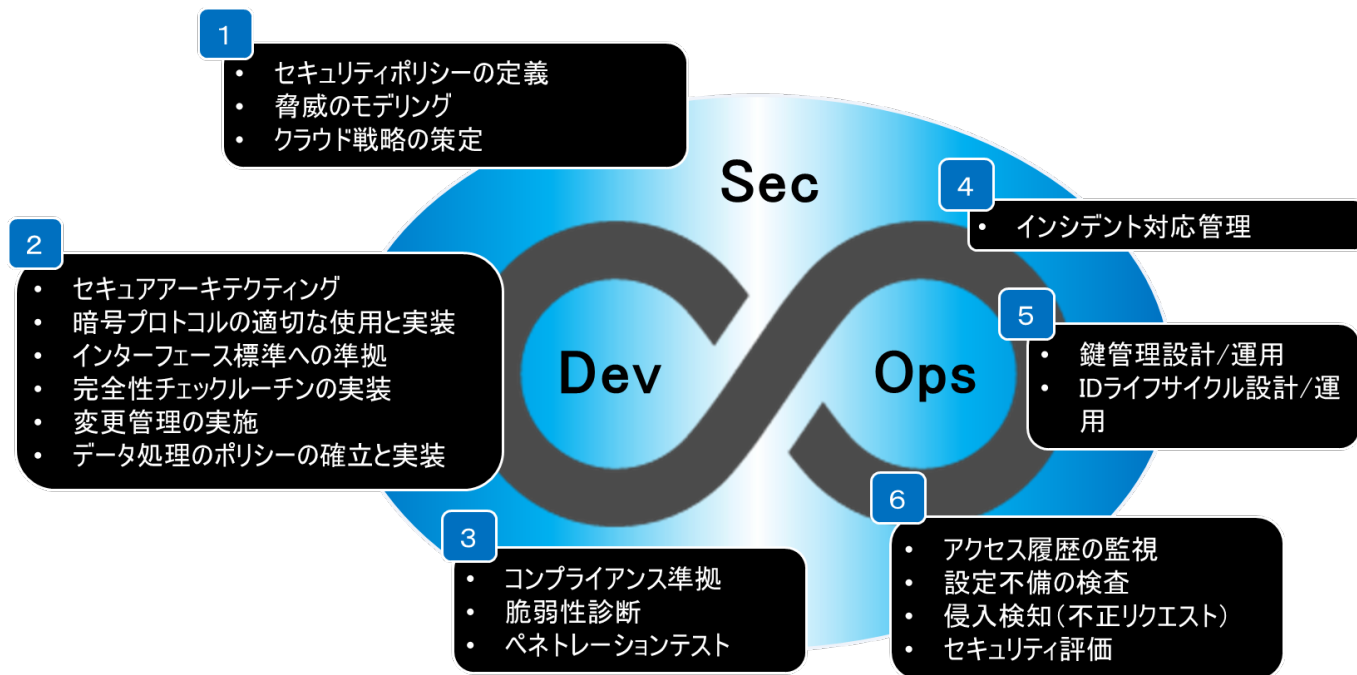
3.3.4. 当問題に対するポイントと対応策

本章では、「クラウドセキュリティアーキテクチャと戦略の欠如」の対応策として、重要なポイントについて記載している。

- ・ クラウド戦略の策定
どのような目的に対して、クラウド戦略を定義し、クラウド展開・利用するかを検討する。
- ・ セキュリティポリシーの定義
利用するクラウドサービスのアーキテクチャにあわせ、情報セキュリティ関連の法律や規定、ガイドラインを参考に、クラウドサービスの実態にあったセキュリティポリシー（監視ポリシー、運用ポリシー等）を策定する。
- ・ 定期的な脅威モデリングの実施
開発対象のソフトウェアがどのような脅威にさらされており、攻略の可能性を持ちうるか洗い出す活動を定期的に実施する。
- ・ システムの運用状況の把握
セキュリティポリシーに則って稼働状況、運用状況等を定期的に把握できるような施策を講じる

3.3.5. DevSecOps サイクル

セキュリティポリシーの策定とその管理にフォーカスし、DevOps サイクルに対応策をマッピングしている。



3.3.6. DevSecOps を踏まえた対処

3.3.5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	セキュリティポリシーの定義	利用するクラウドサービスのアーキテクチャにあわせ、情報セキュリティ関連の法律や規定、ガイドラインを参考に、クラウドサービスの実態にあったセキュリティポリシー（監視ポリシー、運用ポリシー等）を策定する。	左記に同じ
	リスク評価と脅威分析	想定されるリスクと脅威の検討	公開されているフレームワーク等を参考に、脅威・リスク分析を実施する。 ・ STRIDE (for Microsoft) ・ DREAD
	クラウド戦略の策定	目的に対して、どのようなクラウド戦略を定義し、クラウド展開・利用するかを検討する。	例としては以下のような計画が挙げられる。 ・ 導入（投資）効果の検討 ・ ワークロードの配置計画 ・ 管理ツールの検討 ・ SaaS 統合・連携の検討
2	セキュアアーキテクティング	不正なアクセスを防止するための策を講じる（IDS/IPS、WAF など）	外部からの不正侵入に対応できるソリューションの導入を検討する。

			・ IDS/IPS ・ WAF ・ DDoS protection
	暗号プロトコルの適切な使用と実装	機微なデータについて、ストレージ内、データ使用時、及びデータの送受信時の暗号化を行う。暗号化には、オープン、検証済の標準アルゴリズムを利用する。 クラウド事業者が提供するマネージド HSM サービスを活用することが有効である。	・ TLS を使用。 ・ HSM サービスを使用。以下、パブリッククラウドのサービス例。 -AWS CloudHSM -Azure Dedicated HSM -Google Cloud HSM
	インターフェース標準への準拠	プログラム間のインターフェースには、業界の認める標準に基づいた設計、開発及び導入を行う。当該インターフェースは該当する法的及び規制上の遵守義務に従う。	・ 以下のような標準化された API を使用。 -Financial-grade API -Open Banking API
	完全性チェックルーチンの実装	データの入出力について、マッチングやエディットチェックなどデータ完全性をチェックするためのルーチンを実装する。	・ 完全性確認ツールを使用。 -Tripwire ・ エディットチェックツールを使用。
	変更管理の実施	システム間インターフェースの変更に伴う設計及び設定の変更を行う場合は、確立されたポリシーと手順に基づいて実施する。	・ 変更管理ポリシーを整備。 ・ 変更管理手順を整備。
	データ処理のポリシーの確立と実装	データ及びデータを含むオブジェクトのラベリングを確立されたポリシーに基づいて実施する。データをまとめて格納するオブジェクトには、ラベルを継承して保持する仕組みを実装する。	・ 情報の分類体系を整備。 ・ タグ付け機能を実装。 ・ メタデータ付与。
3	コンプライアンス準拠	監督省庁における法的要件や、業界団体のコンプライアンスを基に、セキュリティポスチャを評価する。	・ 以下サービスで、コンプライアンス準拠状況を確認する。 -AWS Artifact -Azure Policy、Azure Blueprints -Google Compliance Reports Manager
	ペネトレーションテスト	公開されるサービスに対してペネト	・ 適切なエンゲージメントの上、ペ

		レーションテストを行い、攻撃防御・検知の確認を行う。事前に定められた間隔及びシステム変更時に実施する。	ネトレーションテストやレッドチーム演習を実施する。。
	脆弱性診断	公開されるサービスに対してデータ侵害に対する脆弱性有無を診断する。	・対象サービスに応じて、プラットフォーム診断とアプリケーション診断の実施有無を判断し、適切に実施する。
4	インシデント対応計画策定	データ侵害に関するインシデントが発生した際の検知、復旧、事後対応までの体制、連絡フロー、各種手順を対応計画として定める。法律や関連する規制、社内規定に準拠する。	・インシデント対応計画を整備。 -インシデント対応体制 -連絡フロー -対応プロセス -業務復旧・継続手順
5	鍵管理設計/運用	・認証、署名、データ暗号化などの用途に応じ、鍵のライフサイクル(生成、配布、更新、失効、再発行などのイベント)を踏まえた運用設計を行う。	・HIPAA、FedRAMPなどのコンプライアンス準拠が必要なケースでは、サービスとして用いる暗号鍵について、クラウド基盤が提供する鍵管理サービス(HSM)の採用を検討する。
	ID ライフサイクル設計/運用	ID を適切に管理するための運用管理方法を検討する。	・不要な ID や権限が残存していないか確認するため、定期的に棚卸を実行する。 ・不要な ID や権限を残さないために、利用者による申請ベースの処理だけではなく、人事イベントやワークフロー等と連動したメンテナンスも検討する。
6	アクセス履歴の監視	資産へのアクセス履歴を監視し、不正なアクセスがないか確認する。また、監視を行うことでの不正行為の抑止を行う。	・以下、監視項目例。 -アクセス試行の傾向 -許可されていないリソースへのアクセス -業務時間外のアクセス -許可外の端末・環境からのアクセス
	設定不備の検査	設定不備などにより、意図せず公開されている資産などがないか確認する。	・セキュリティ診断(設定不備の有無確認)の実施
	侵入検知(不正リクエスト)	内外部からの不正な侵入の有無をモニタリングする。	・セキュリティシステム(センサー)からのアラートチェックを行う。
	セキュリティ評価	実施している施策に対して、定期的な評価(実施状況、妥当性、過不足など)	・組織の対策状況を評価するものとして以下が挙げられる。

		を実施する。	-ISMS 適合性評価制度 -情報セキュリティ監査 -情報セキュリティ対策ベンチマーク -セキュリティ製品の評価（ IT セキュリティ評価及び認証制度、暗号モジュール試験及び認証制度など）
--	--	--------	---

3.4. ケース 4 ID・資格情報・アクセス・鍵の不十分な管理

3.4.1. 概要

資格情報を適切に保護できていないことにより、正規ユーザーへのなりすましによるデータ侵害や、管理機能の乗っ取り、移動中のデータの盗聴、正規のサイトと見せかけた悪意のあるソフトウェアのリリースなどのセキュリティインシデントが発生する。

3.4.2. ビジネスインパクト

データに対する許可されていないアクセスが可能になることで、組織やエンドユーザーに対して壊滅的なダメージを与える可能性がある。

3.4.3. 想定事例と実例

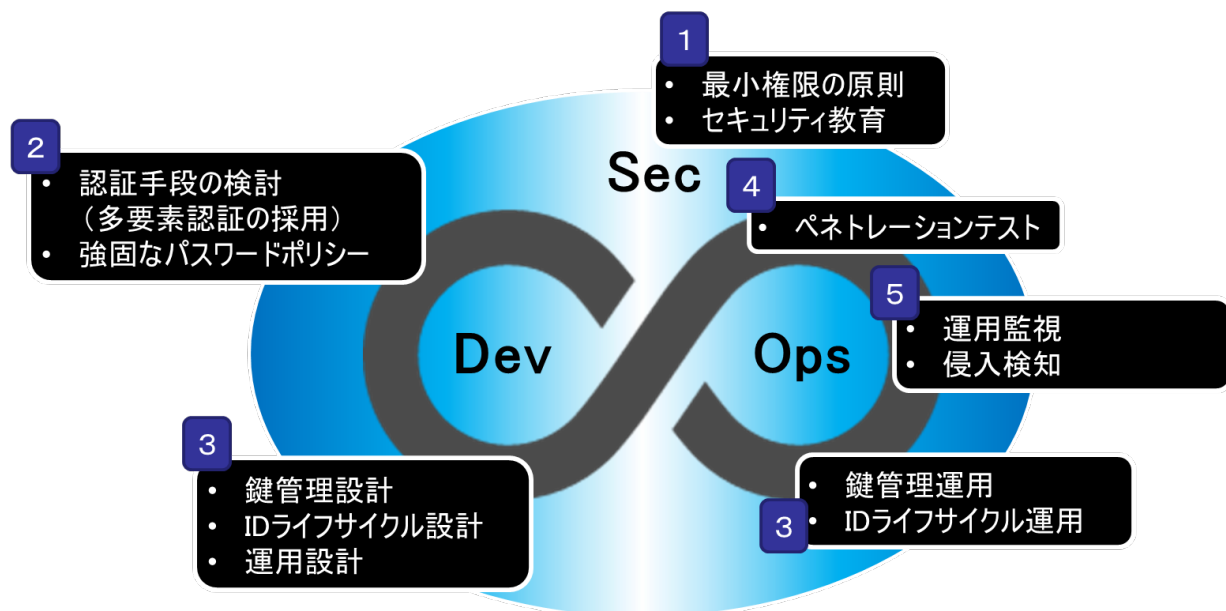
「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- 2018 年 12 月、ドイツの学生による脆弱なパスワードに対するハッキングにより、1000 人の議会メンバー、ジャーナリスト、その他の著名人に紐付けられた電話番号、テキストメッセージ、写真、クレジットカード番号、その他のデータが盗難され、Twitter などを通じて拡散された。
- 2017 年 9 月 25 日、デロイトは、脆弱な管理者 e メールアカウントが原因でグローバル e メールサーバが侵害されたと発表した。攻撃者には特権が与えられ、「全てのエリア」に対して無制限のアクセスが可能になったと推測されている。管理者アカウントに対して二段階認証プロセスは採用されていなかった。
- 2017 年 5 月 31 日、ある攻撃者が、ID・パスワードを管理するサービスを提供している OneLogin の AWS 鍵を利用し、同社の AWS プラットフォームにアクセスした。同社はその侵害を検知し、侵害を止めるために数分以内に対処を行った。
- GitHub から収集されたクラウドサービスの資格情報によって、アカウントがハイジャックされた。プロジェクトの立ち上げから 36 時間以内に発見され悪用されたケースも存在した。
- 情報セキュリティソリューションプロバイダの Praetorian は、AWS のコンピューティングパワーを活用したシンプルな方法によりパスワードハッシュをクラックするためのプラットフォームを立ち上げた。

3.4.4. 当問題に対するポイントと対応策

クラウド基盤が提供するセキュリティ機能を把握した上で、万が一の事態に被害を最小限に留めるために最小権限の原則に従うこと、ID や鍵のライフサイクルに合わせた運用ルールを設計段階から意識することが必要である。

3.4.5. DevSecOps サイクル



3. 4. 6. DevSecOps を踏まえた対処

3. 4. 5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	アクセス管理ポリシーの検討	職務分掌を適切に行い、役割にあった権限を定義する。	・ ロール(全体管理者、運用管理者、オペレータ、バックアップ&リカバリ、一般ユーザーなど)の定義 ・ 運用オペレーションにおける、不必要な高権限 ID (root など) の排除 ・ システム管理者やテナント管理者などの強い権限を持つアカウントには、利用者のデータを操作する権限を与えない。 ・ 不要な ID や権限は残さない。
	従業員に対するセキュリティ意識向上トレーニングの実施	従業員に対してセキュリティに対する意識向上を目的としたトレーニングを実施する。	左記に同じ
2	認証手段の検討 (多要素認証の採用)	特権 ID の認証については、まず多要素認証を提供しているサービス事業者を選定し、設定を有効にすることが望ましい。 また一般利用者の認証については、サービスレベルや利用者のリテラシーを考慮して認証方式を検討する。	・ 認証手段を検討する上での考慮事項(例)として、以下のようなものが挙げられる。 – 初回登録時と2回目以降の2つのユースケースについて検討が必要。 – 管理機能のアクセス元 IP アドレスを制限する。 – 追加コストがかけられない場

			合などは、SNS 認証やメールアドレス認証など、比較的低コストで実現可能な認証手段を検討する。 –モバイルアプリの場合、2 回目以降の認証については端末認証の採用を検討する。 –認証強化を他のサービス（IDaaS など）に委託し、シングルサインオン環境を構築する。
	パスワードポリシーの検討	原則、パスワードのみに依存しない認証方式を採用すべきであるが、やむを得ない場合、十分に複雑で安全なパスワードポリシーを設定すべきである。パスワード忘れに対応するための機能が、アカウントハイジャックなどの攻撃手段として利用されないよう、十分に注意が必要である。	左記に同じ
3	鍵管理設計と運用	認証、署名、データ暗号化などの用途に応じ、鍵のライフサイクル（生成、配布、更新、失効、再発行などのイベント）を踏まえた運用設計を行う。	・HIPAA、FedRAMP などのコンプライアンス準拠が必要なケースでは、サービスとして用いる暗号鍵について、クラウド基盤が提供する鍵管理サービス（HSM）の採用を検討する。
	ID ライフサイクル設計/運用	ID を適切に管理するための運用管理方法を検討する。	・不要な ID や権限が残存していないか確認するため、定期的に棚卸を実行する。 ・不要な ID や権限を残さないために、利用者による申請ベースの処理だけでなく、人事イベントやワークフロー等と連動したメンテナンスも検討する。
	運用ルール の定義	システムで対策できない（あるいはコストの問題などで対策しきれなかった）リスクについて、運用対処が可能なものは必要に応じて運用ルールや利用ルールなどの整備を行う	・実施している内容や利用システムに関係するため、システム的な対応が行えない箇所を整理して、運用ルールを検討する。
4	ペネトレーションテスト	公開されるサービスに対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。事前に定められた間隔及びシステム変更時に実施する。	・適切なエンゲージメントの上、ペネトレーションテストやレッドチーム演習を実施する。

5	アクセス履歴の監視	内外部からの不審なアクセスや、IDの利用状況を監視し、不正アクセスの有無を確認できるようにする。	・アクセスログ監視によって、ログイン失敗の増加などの異常を検知する仕組みを用意する。 ・特権ユーザーによる設定変更については、誰がいつ何を変更したのかを監査ログとして保存する。 ・root などの高い権限を持つ共有 ID については、実際に誰が利用したのかを特定できるように特権 ID 管理製品の導入も選択肢となる
	侵入検知（不正リクエスト）	外部からの不正な侵入の有無をモニタリングする。	・セキュリティシステム（センサー）からのアラートチェックを行う。

3.5. ケース 5 アカウントハイジャック

3.5.1. 概要

内部者の脅威とは「組織の資産へアクセスする権限を持っているか、またはかつて持っていた個人がその権利を使用し、悪意を持ってあるいは意図せずに、組織に悪影響を及ぼすおそれのある行動を取る可能性」と定義されており、現在のまたは元の従業員、請負業者、信頼しているビジネスパートナーなどの「内部者」が企業内の機密データに不正にアクセスし、情報を取得するような行為が該当する。

3.5.2. ビジネスインパクト

機密情報や知的財産の損失、信頼の低下をもたらす。

- ・ システムの停止が伴う場合には、「企業の生産性」に悪影響を及ぼす。
- ・ データの損失は、顧客への被害に繋がり、「会社のサービスに対する信頼」を低下させる。

3.5.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- 2018 年 6 月、テスラ社において、従業員（妨害者）は、不正なユーザー名を使用し、テスラの製造オペレーションシステムで使用されるコードの改ざんを行っていた。また、「大量のテスラの機密データを未知の第三者」に提供していた。
- 2018 年に、インドのパンジャブ国立銀行の従業員が、SWIFT（銀行間取引システム）の機密パスワードに不正アクセスし、不正取引の仕組みで資金を拠出していた。
- 誤設定のクラウドサーバ、ネットワークバックアップインシデント、およびその他の不適切に設定されたシステムが数多く存在しており、おおよそ 20 億件超のレコードが危険な状態に晒されていることが確認された。その中で不正にアクセスされたレコードは、約 7 割に当たると言われている。

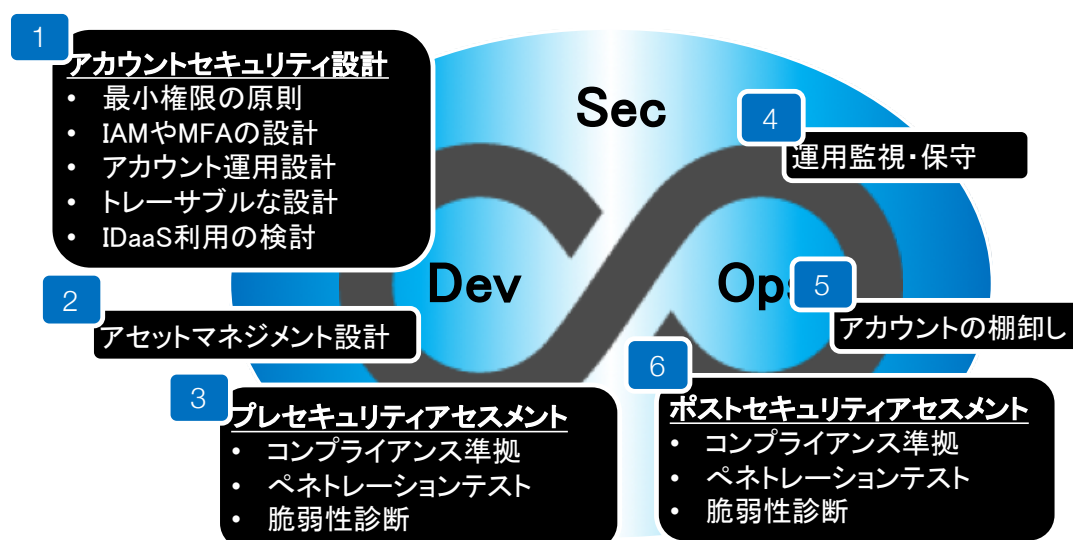
3.5.4. 当問題に対するポイントと対応策

「内部者の脅威」の対応策の重要なポイントとして、大きく以下のようなものが挙げられる。

- ・ システム構築におけるセキュリティ基準の定義・見直し
- ・ データへのアクセス権限の定義と管理方法の確立
- ・ システム担当者へのシステム活用・運用におけるトレーニングの実施
- ・ 従業員に対するセキュリティ意識向上トレーニングの実施
- ・ 情報リソースへのアクセス履歴の定期的な検査
- ・ 設定誤り等に対する定期的な検査や監査

3.5.5. DevSecOps サイクル

システムを構築する際のアカウントセキュリティとアセスメントにフォーカスし、DevOps サイクルに対応策をマッピングしている。



3.5.6. DevSecOps を踏まえた対応

5.6.5 の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	アクセス管理ポリシーの検討	職務分掌を適切に行い、役割にあった権限を定義する。	・ロール（全体管理者、運用管理者、オペレータ、バックアップ&リカバリ、一般ユーザーなど）の定義 ・運用オペレーションにおける、不必要な高権限 ID（root など）の排除 ・システム管理者やテナント管理者などの強い権限を持つアカウントには、利用者のデータを操作する権限を与えない。 ・不要な ID や権限は残さない。
	IAM や MFA の設計	・ストレージや仮想ネットワーク、IAM など、管理プレーンから設定可能な IaaS 環境のセキュリティ関連設定について、設定ミスやコンプライアンスルールへの不適合、不適切な権限昇格を継続的にチェックする仕組みを導入する。 ・リソース（資産）にアクセスするた	・IAM に関するマネージドサービスやサードパーティ製品を活用する ・公開リソースの配置環境に応じて適切な認証方法・方式（MFA、リスクベース、CAPTCHA、FID など）の定義を行う。

		めの認証方法を検討する。	
	アカウントの運用設計	アカウント不正利用防止機の方針を検討する。	・ アカウントロックを設定する。 ・ 不正な利用が発見された際にリモートロック・ワイプを行える準備を行う。
	トレーサブルな設計	インシデント発生時のトレースにあたり「誰が」、「いつ」、「何を」、「どうしたか」を早急に対応可能な設計をする。	以下サービスを利用する。 -AWS Cloud Watch、AWS Cloud Trail -Azure Activity Log、Azure Security Center -Google Cloud Monitoring、Google Security Command Center
	IDaaS 利用の検討	管理対象 ID の総数、IdP (Identity Provider) の総数などの増加に伴う管理負荷を軽減するために、一元管理する。	・ 以下 IDaaS を利用する。 -Azure AD (Azure Active Directory) -Cloud Identity -OneLogin
2	アセットマネジメント設計	IT アセット情報、並びにアカウント情報を収集し、攻撃者による不正操作の検知やインシデントレスポンスに備える。	・ 以下でサービスを利用する。 -AWS IAM、AWS Config -Azure AD、Azure Security Center -Cloud IAM、Cloud Identity、Security Command Center
3	コンプライアンス準拠	監督省庁における法的要件や、業界団体のコンプライアンスを基に、セキュリティポスチャを評価する。	・ 以下サービスで、コンプライアンス準拠状況を確認する。 -AWS Artifact -Azure Policy、Azure Blueprints -Google Compliance Reports Manager
	ペネトレーションテスト	公開されるサービスに対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。事前に定められた間隔及びシステム変更時に実施する。	・ 適切なエンゲージメントの上、ペネトレーションテストやレッドチーム演習を実施する。
	脆弱性診断	公開されるサービスに対してデータ侵害に対する脆弱性有無を診断する。	・ 対象サービスに応じて、プラットフォーム診断とアプリケーション診断の実施有無を判断し、適切に実施する。
4	インシデント対応計画	セキュリティインシデントレスポンス	左記に同じ

		スに対応できる体制、対応フロー、システムを定義、および設計する。	
5	アカウントの棚卸し	アカウントの棚卸を行い、退職者や、契約が終了した外部パートナーのふようになつたアカウントを削除する。	・ 棚卸対象アカウントの整理を実施 -退職者アカウント -外部パートナーアカウント -制限付き（特定の目的で作成したものなど）アカウント -管理者アカウント
6	コンプライアンス準拠	監督省庁における法的要件や、業界団体のコンプライアンスを基に、セキュリティポスチャを評価する。	・ 以下サービスで、コンプライアンス準拠状況を確認する。 -AWS Artifact -Azure Policy、Azure Blueprints -Google Compliance Reports Manager
	ペネトレーションテスト	公開されるサービスに対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。事前に定められた間隔及びシステム変更時に実施する。	・ 適切なエンゲージメントの上、ペネトレーションテストやレッドチーム演習を実施する。
	脆弱性診断	公開されるサービスに対してデータ侵害に対する脆弱性有無を診断する。	対象サービスに応じて、プラットフォーム診断とアプリケーション診断の実施有無を判断し、適切に実施する。

3.6. ケース 6 内部者の脅威

3.6.1. 概要

内部者の脅威とは「組織の資産へアクセスする権利を持っているか、またはかつて持っていた個人がその権利を使用し、悪意を持ってあるいは意図せずに、組織に悪影響を及ぼすおそれのある行動を取る可能性」と定義されており、現在のまたは元の従業員、請負業者、信頼しているビジネスパートナーなどの「内部者」が企業内の機密データに不正にアクセスし、情報を取得するような行為が該当する。

3.6.2. ビジネスインパクト

機密情報や知的財産の損失、信頼の低下をもたらす。

- ・ システムの停止が伴う場合には、「企業の生産性」に悪影響を及ぼす。
- ・ データの損失は、顧客への被害に繋がり、「会社のサービスに対する信頼」を低下させる。

3.6.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- 2018 年 6 月、テスラ社において、従業員（妨害者）は、不正なユーザー名を使用し、テスラの製造オペレーションシステムで使用されるコードの改ざんを行っていた。また、「大量のテスラの機密データを未知の第三者」に提供していた。
- 2018 年に、インドのパンジャブ国立銀行の従業員が、SWIFT（銀行間取引システム）の機密パスワードに不正アクセスし、不正取引の仕組みで資金を拠出していた。
- 誤設定のクラウドサーバ、ネットワークバックアップインシデント、およびその他の不適切に設定されたシステムが数多く存在しており、おおよそ 20 億件超のレコードが危険な状態に晒されていることが確認された。その中で不正にアクセスされたレコードは、約 7 割に当たると言われている。
-

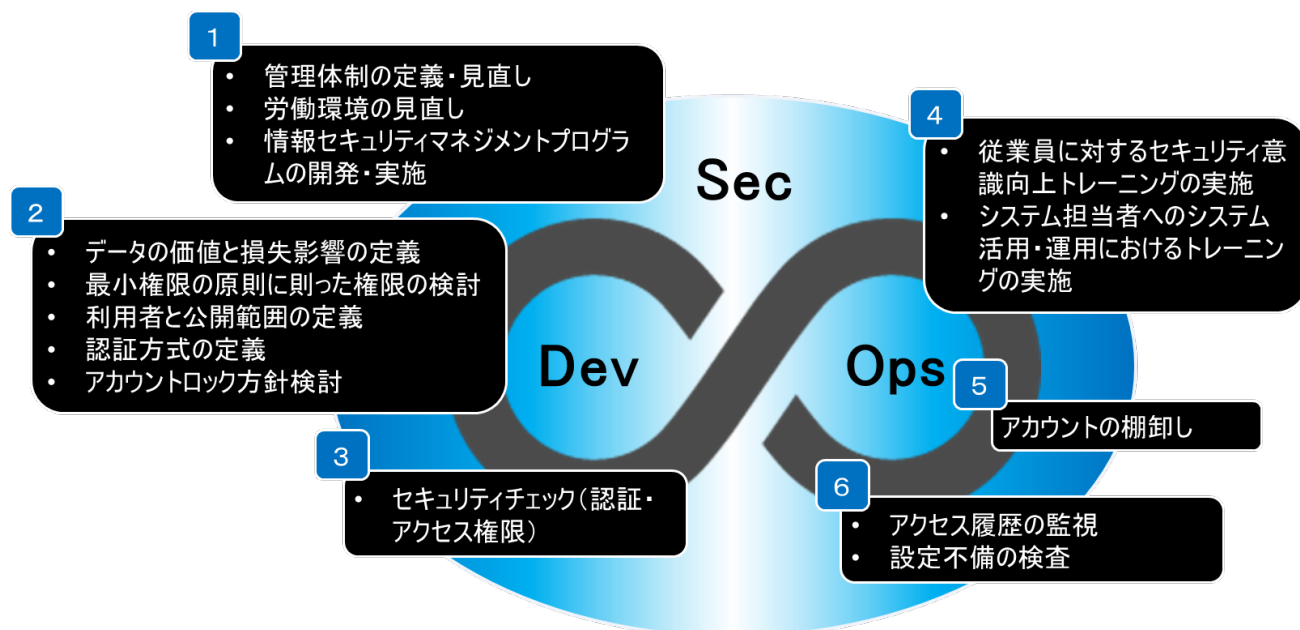
3.6.4. 当問題に対するポイントと対応策

「内部者の脅威」の対応策の重要なポイントとして、大きく以下のようなものが挙げられる。

- ・ システム構築におけるセキュリティ基準の定義・見直し
- ・ データへのアクセス権限の定義と管理方法の確立
- ・ システム担当者へのシステム活用・運用におけるトレーニングの実施
- ・ 従業員に対するセキュリティ意識向上トレーニングの実施
- ・ 情報リソースへのアクセス履歴の定期的な検査
- ・ 設定誤り等に対する定期的な検査や監査

3. 6. 5. DevSecOps サイクル

システムを構築する際のデータの管理、アクセス制限、アカウント管理にフォーカスし、DevOps サイクルに対応策をマッピングしている。



3. 6. 6. DevSecOps を踏まえた対応

3. 6. 5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	管理体制の定義・見直し	組織横断的な管理体制や関連部門の役割を具体化、明文化し、その役割を徹底させる。従業員管理体制に問題がある場合には、適宜見直しを図る また、業務委託においては、機密情報を提供する際に、提供元から提供先に対して、機密情報の指定またはその保持に必要とされる情報セキュリティ対策の具体的な実施内容を示すことが重要である。	左記に同じ
	社内制度の見直し	公正な人事評価や適正な労働環境により、従業員の不満やストレスを減らす(犯行の誘引)を減らすことを目的とした対応を実施	- 作業環境の見直し - 作業方法の見直し・効率化 - 疲労回復支援施設の検討 - 職場生活支援施設の検討
	情報セキュリティマネジメントプログラムの開発・実施	資産及びデータを紛失、誤用、許可されていないアクセス、暴露、改ざん、破壊から保護するために、管理的、技術的、物理的な保護措置を含む情報	- セキュリティのプログラムは、事業の特性に関わる範囲で以下を定義する。 -リスク管理

		セキュリティマネジメントのプログラムを開発し、実施する。	-セキュリティポリシー -資産管理 -人的セキュリティ -物理的及び環境的セキュリティ -通信及び運用管理 -アクセス制御 -情報システムの調達、開発及び保守
2	データの価値と損失影響の定義	公開する資産にどのような情報（個人情報、機微情報）があるか確認し、その情報が外部に漏えいした場合のリスクを検討する。	左記に同じ
	最小権限の原則に則った権限の検討	職務分掌を適切に行い、役割にあった権限を定義する。	・ロール（全体管理者、運用管理者、オペレータ、バックアップ&リカバリ、一般ユーザーなど）の定義 ・運用オペレーションにおける、不必要な高権限 ID（root など）の排除 ・システム管理者やテナント管理者などの強い権限を持つアカウントには、利用者のデータを操作する権限を与えない。 ・不要な ID や権限は残さない。
	利用者と公開範囲の定義	リソース（資産）にアクセスする利用者とリソースを公開する範囲を検討する。	・公開するリソースにアクセス可能な利用者の選定 ・選定された利用者に公開するリソースの決定
	認証方法の定義	リソース（資産）にアクセスするための認証方法を検討する。	・公開リソースの配置環境に応じて適切な認証方法・方式（MFA、リスクベース、CAPTCHA、FID など）の定義を行う。
	不正利用防止策の検討	アカウント不正利用防止機の方針を検討する。	・アカウントロックを設定する。 ・不正な利用が発見された際にリモートロック・ワイプを行える準備を行う。
3	セキュリティチェック（認証・アクセス権限）	公開するリソース（資産）に対する認証および、アクセスにおいて、意図したものになっているか確認する。	・セキュリティ診断（設定不備の有無確認）の実施
4	従業員に対するセキュリティ意識向上トレーニング	従業員に対してセキュリティに対する意識向上を目的としたトレーニング	左記に同じ

	グの実施	グを実施する。	
	システム担当者へのシステム活用・運用におけるトレーニングの実施	利用するシステムに関する知識を向上させるためのトレーニングを実施する。	左記に同じ
5	アカウントの棚卸し	アカウントの棚卸を行い、退職者や、契約が終了した外部パートナーのふようになったアカウントを削除する。	・ 棚卸対象アカウントの整理を実施 -退職者アカウント -外部パートナーアカウント -制限付き（特定の目的で作成したものなど）アカウント -管理者アカウント
6	アクセス履歴の監視	資産へのアクセス履歴を監視し、不正なアクセスがないか確認する。また、監視を行うことでの不正行為の抑止を行う。	・ 以下監視項目例 -アクセス試行の傾向 -許可されていないリソースへのアクセス -業務時間外のアクセス -許可外の端末・環境からのアクセス
	設定不備の検査	設定不備などにより、意図せず公開されている資産などがいないか確認する。	・ セキュリティ診断（設定不備の有無確認）の実施

3.7. ケース 7 安全でないインターフェースと API

3.7.1. 概要

サービスの利用者がクラウドサービスを管理し、情報の授受ができるよう、ソフトウェアユーザーインターフェースや API を公開するが、認証やアクセス制御から暗号化や動作の監視まで、これらのインターフェースは、セキュリティポリシーの隙間をかいぐる偶発的あるいは悪意ある攻撃を防ぐように設計がされていない場合、誤った使われ方や、さらに深刻な場合にはデータ漏洩を引き起こす可能性がある。

API やユーザーインターフェースは、一般的にシステムの中で最も外部にさらされる部位であり、信頼できる組織の外側から利用可能なパブリック IP アドレスを付与された唯一の方法であるため、これらを攻撃から防御するためにセキュリティ・バイ・デザインと適切な制御が必要となる。

3.7.2. ビジネスインパクト

セキュリティが弱いインターフェースや API に依存すると、機密性、完全性、可用性、そして説明責任に関する様々なセキュリティリスクが発生する。

3.7.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- Facebook は、2018 年 9 月 28 日に 5,000 万を超えるユーザーに影響を及ぼすデータ漏洩があったことを発表した。報道によると、1 年以上前の 2017 年 7 月に Facebook のコードに資格情報の窃取の脆弱性が埋め込まれており、同社は、どのような情報が盗まれ、他にどの程度の数のユーザーアカウントの情報が漏れたか、わからないことを認めた。

3.7.4. 当問題に対するポイントと対応策

API を安全な状態に保つことが必要である。

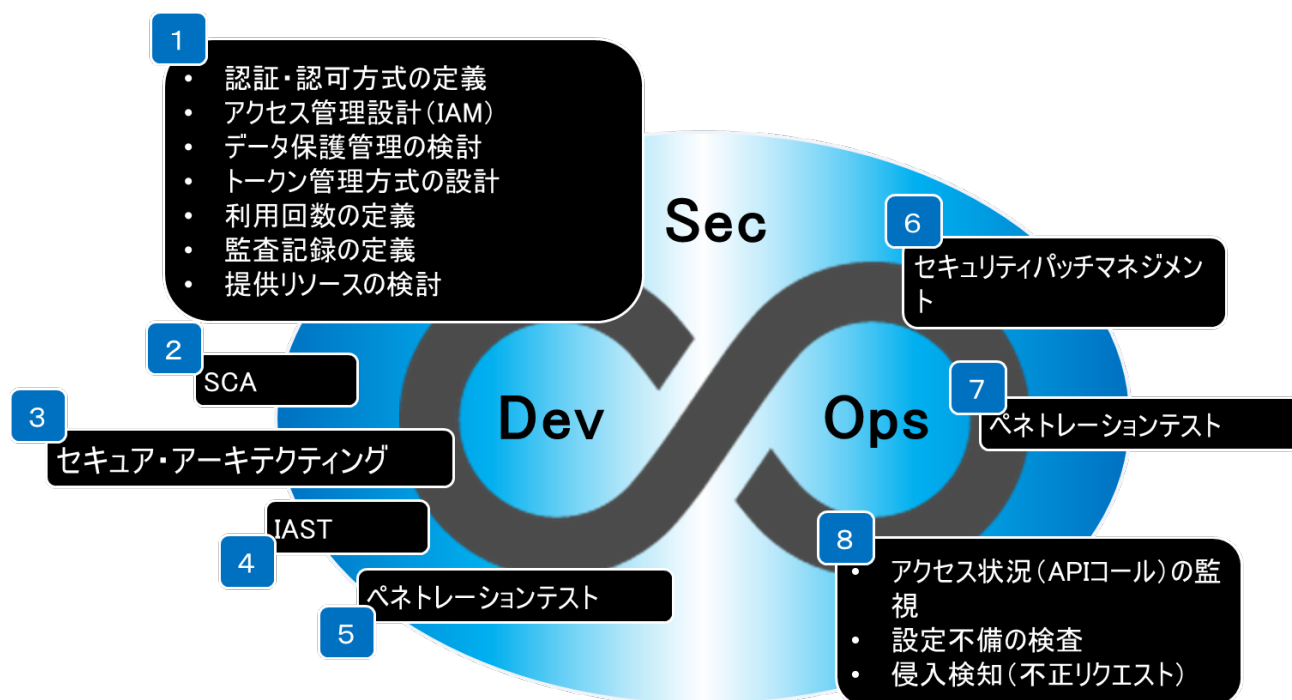
そのための取り組みとして、構成管理、テスト、監査、異常活動防止等のような入念な管理を行い、API キーを適切に保護し、再利用を避けることを確実に実施する。

また、標準的に公開された API フレームワーク※の利用を検討し、安全な API を準備することも重要である。

※Open Cloud Computing Interface (OCCI) , Cloud Infrastructure Management Interface (CIMI)

3.7.5. DevSecOps サイクル

外部に公開されるインターフェースや API にフォーカスし、DevOps サイクルに対応策をマッピングしている。



3.7.6. DevSecOps を踏まえた対処

3.7.5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	認証・認可方式の検討	アクセス認証、認可、署名、ライフサイクル管理をどのように行うか検討する。 各ユーザーが必要な情報以外を読み書きできないようにするため、各ユーザーやアプリケーションが保持する権限レベルを管理、保守する必要がある。	・ OAuth (OpenID Connect) による認証方法の検討 ・ 環境に応じた認可フロー (OAuth) の定義
	アクセス管理設計	当該 API (リソース) を誰に対して提供するのか、それが適切かを検討する。	・ 利用者の検討 ・ 利用者に対する提供リソースの精査
	データ保護方式の検討	提供するデータや、API を利用して取得したデータの暗号化を検討する。また、ネットワーク上の通信の暗号化も併せて検討する。	・ エンドツーエンドでの適切な暗号化処理 (TLS)、セッション管理の実施 ・ Mutual TLS に依存したセキュリティ強化仕様への準拠
	トークン管理の設計	API キー、トークンの保護、提供期限	・ 利用体系 (参照系・更新系) に応

		設定を適切に行うよう設計する。	じた有効期限やリフレッシュトークンの利用有無を検討する。 ・トークンの失効管理を行う。
	利用制限の定義	ユーザーの API 呼び出し回数を要件に応じて制限することを検討する。	左記に同じ
	監査記録の検討	API を利用する際にユーザーを一意に識別し、その呼び出しと戻り値のステータスを監査記録としてログに記録する方法を検討する。	左記に同じ
	提供リソースの検討	API の形態において提供するリソースの質をとらえた保護要件の検討を行う。	・ API の形態例 -パブリック API（不特定多数） -アクウェインタンス API（資格を有する法人、個人） -メンバーAPI（規範性のあるコミュニティ） -パートナーAPI（個別契約締結先） -プライベート API（内部）
2	SCA (Software Composition Analysis)	アプリケーションが利用するライブラリ、コンポーネントに対して脆弱性が報告されていないかをチェックする	ソフトウェア静的解析ツール等を利用したテストを実施
3	セキュアアーキテクティング	不正なアクセスを防止するための策を講じる（IPS、WAF など） また、API ゲートウェイを利用したエッジ処理等も検討する。	・ 外部からの不正侵入に対応できるソリューションの導入を検討する。 -IDS/IPS -WAF -DDoS protection
4	動作テスト（脆弱性診断）	リアルタイムなコードのチェックや動的なアプリケーション解析を実施する。	・ IAST・DAST ツールを利用し、機能テストを実行
5	ペネトレーションテスト	公開される API に対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。	・ 公開 API に対するペネトレーションテストの実施
6	セキュリティパッチ管理	定期的にセキュリティパッチの公開有無をチェックし、必要に応じて適用する。	左記に同じ
7	ペネトレーションテスト	公開される API に対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。	・ 公開 API に対するペネトレーションテストを定期的実施

8	アクセス状況（API コール）の監視	定常時と比較し、おかしい傾向がないかなどを確認する。	・ 以下監視項目例 - アクセス試行の傾向 - 許可されていないリソースへのアクセス
	設定不備の検査	設定不備などにより、意図せず公開されている資産などがいないか確認する。	・ セキュリティ診断（設定不備の有無確認）の実施
	侵入検知（不正リクエスト）	内外部からの不正な侵入の有無をモニタリングする。	・ セキュリティシステム（センサー）からのアラートチェックを行う。

3.8. ケース 8 弱い管理プレーン

3.8.1. 概要

クラウドにおけるマネジメントプレーンではクラウド上のあらゆるサービス、データ、デバイスの管理を求められるため、管理者は、セキュリティ設定、データフロー、またアーキテクチャの弱点を適切に把握する必要がある。管理が不十分な場合、データの破損、使用不能、漏洩を引き起こす可能性がある。

3.8.2. ビジネスインパクト

サービスや提供製品に対する不満や信頼の喪失により、最終的には、収益の減少につながる恐れがある。さらに、特に個人データを含むデータ損失の場合には、監督機関の処罰を受ける可能性がある

(例：GDPR では、2000 万ユーロまたは売上高の 4%の罰金が課される可能性がある)

3.8.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

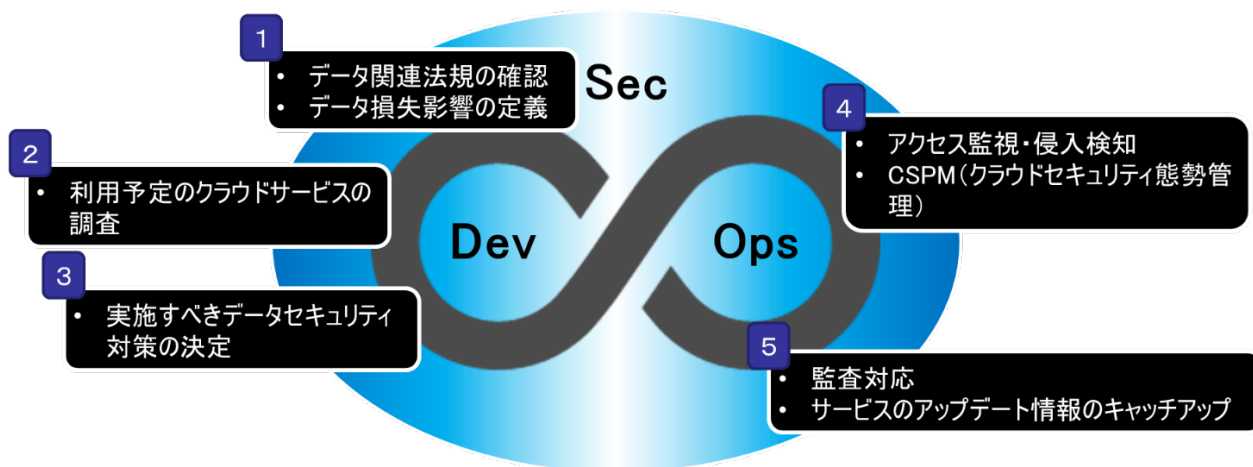
- 2 要素認証は、有効な対策のひとつであるが、多くの CSP が、2 要素認証に対して追加料金を設定している。このような慣行が、クラウド利用者のセキュリティ対策を弱めている

3.8.4. 当問題に対するポイントと対応策

他の脅威と同様、まずはリスクを評価し、重要さに応じた適切な対処を検討する必要がある。特に、仮想リソースの設定ひとつで重大なセキュリティ事故が発生しうるリスクについては、持続的（継続的）な状態監視が必要である。

3.8.5. DevSecOps サイクル

新たなクラウドサービスを利用する上での要点にフォーカスし、DevOps サイクルに対応策をマッピングしている。



3.8.6. DevSecOps を踏まえた対処

3.8.5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	データ関連法規の確認	業界や地域などによって異なる、当該ビジネス領域で従うべき法令を確認する。	・データ関連法規：J-SOX 法、個人情報保護法、GDPR、PCI DSS、HIPAA など
	データ損失影響の定義	データ損失により発生する可能性がある、金銭的被害などのリスクを定義する。	・データ復旧費用、情報漏えいに対する金銭的補償、ビジネス機会損失影響、法令違反による制裁金、株価への影響など
2	利用予定のクラウドサービスの調査	・利用予定のクラウドサービスに対するデューデリジェンスを実施する。 ・利用予定のクラウドサービスについて、多要素認証や権限レベル、取得可能な監査対応ログの内容など、管理プレーンのセキュリティ機能に対する調査を実施する。	・利用予定のサービスを評価するために認証取得有無や各種フレームワークに準拠しているか評価する -STAR 認証の有無 -ENISA/IPA：クラウドコンピューティング 情報セキュリティ確保のためのフレームワークの確認
3	実施すべきデータセキュリティ対策の決定	リスクへの対応方針や利用予定のクラウドサービスのセキュリティ機能を踏まえて、運用管理におけるセキュリティ管理策を決定する。	・2 要素認証の採用、利用者 ID 管理の徹底、データ保全計画の策定、CloudHSM の使用による強力な鍵管理などが例として挙げられる
4	アクセス監視	各種サービスへのログインやアクセスに関するログを収集し、不正アクセスを検知する仕組みを用意する。	・AWS CloudTrail やサードパーティー製品の活用したログ管理を実施する。
	侵入検知（不正リクエスト）	内外部からの不正な侵入の有無をモニタリングする。	・セキュリティシステム（センサー）からのアラートチェックを行う。
	CSPM（クラウドセキュリティポスチャ管理）	ストレージや仮想ネットワーク、IAM など、管理プレーンから設定可能な IaaS 環境のセキュリティ関連設定について、設定ミスやコンプライアンスルールへの不適合、不適切な権限昇格を継続的にチェックする仕組みを導入する。	・AWS Trusted Adviser やサードパーティー製品の活用したインフラストラクチャクラウドスタック全体のセキュリティ評価とコンプライアンスの監視を実施する。
5	データアクセス証跡の確保	対応すべきデータ関連法規に従った監査証跡の確保	・特権 ID 管理、アクセスログの収集・保全を行う。
	サービスのアップデート情報のキャッチアップ	サービスが提供するセキュリティ関連の新機能や機能改善の適用による	・定期的なアップデート情報や脆弱性情報を確認する運用業務を検

		運用改善	討する
--	--	------	-----

3.9. ケース 9 メタストラクチャとアプリストラクチャの障害

3.9.1. 概要

メタストラクチャは CSP と利用者の境界線（別名ウォーターライン）と見なされる。CSP はシステム運用に必要な機能を API によって提供するが、CSP による貧弱な API 実装は、サービスの機密性、完全性、可用性を損なわせ、クラウド利用者を混乱させる機会を攻撃者に与える。防衛策として、クラウド利用者は、安全性の高いクラウドサービスを選定するとともに、セキュリティを確保するために CSP が提供する機能を活用する必要がある。

また、クラウド利用者は、クラウドプラットフォームを十分に活用して、クラウドアプリケーションを適切に実装する方法を理解する必要がある。クラウドにビジネスオペレーションとアプリケーションを移行する場合、アプリケーションをそのままクラウドに移行する「リフト」アプローチを取るだけでは不十分である。

3.9.2. ビジネスインパクト

メタストラクチャやアプリストラクチャはクラウドサービスの重大なコンポーネントである。CSP レベルでこれらの機能に関わる障害は、すべてのサービス利用者に重大な影響を与える可能性がある。同時に、テナントによる設定ミスは、経済的、運用的に、ユーザーに非常に大きな影響を与える可能性がある。

3.9.3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

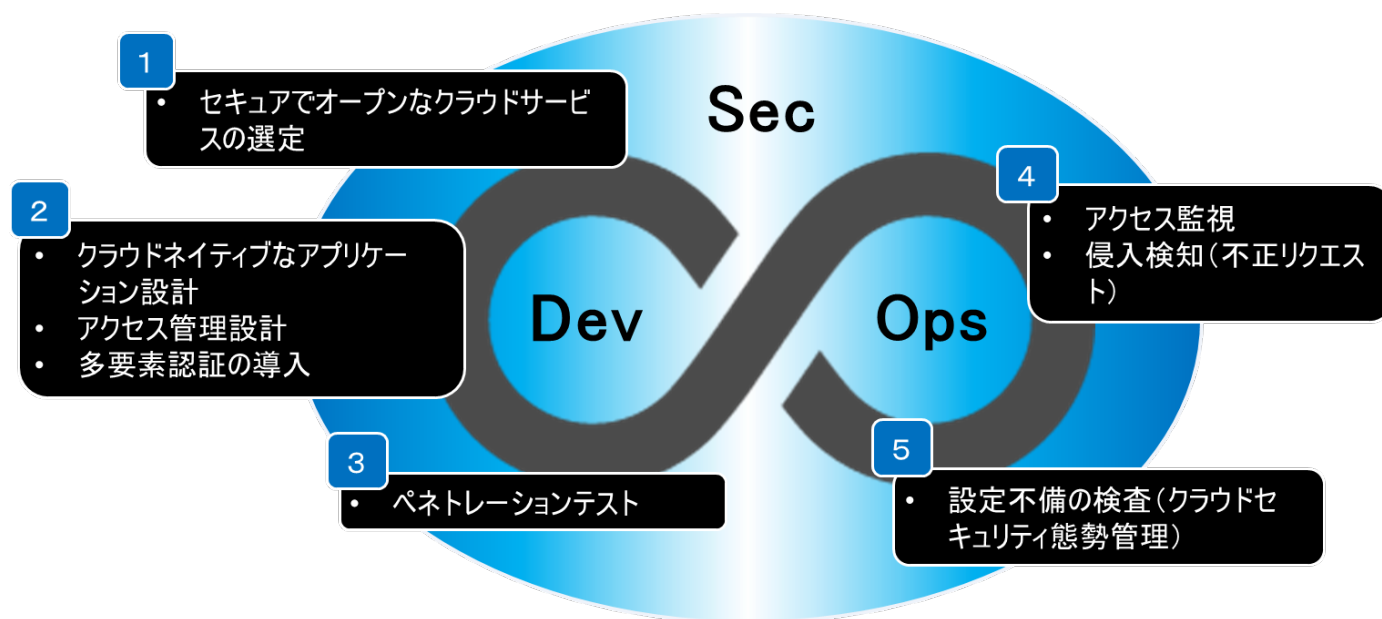
- 利用者側でのメタ/アプリストラクチャの障害の最もよくある例は、ID やアクセス管理に関することである。多くの組織は今でもユーザー名とパスワードのみに依存しており、クラウド内で提供され簡単に実装されるシングルサインオン(SSO)、ID フェデレーション、多要素認証(MFA)のような進んだセキュリティ機能を見逃している。例えば、デロイト社は、(MFA オプションを Microsoft が提供していたにも関わらず) 管理者アカウント用に単一のパスワードに頼った運用をし続けたために、Office 365 メールサービスの内容を流出した。その結果、ハッカーがアカウントを侵害し、大量のクライアント情報が漏洩した。
- AWS のヘビーユーザーの 1 つである Netflix 社は、メタストラクチャアクセスがどれほど重要であるかを理解しており、自社のセキュリティ運用プロセスで使用される資格情報の漏洩を検知する手順を提供している。攻撃者はメタストラクチャの資格情報に価値を見出す。2017 年の「Microsoft Security Intelligence Report」によると、これらの攻撃の頻度は前年から 3 倍になった。2018 年の調査結果でも、「79%の SaaS ストレージ アプリケーションと 86%の SaaS コラボレーション アプリケーションが保存中および転送中のどちらもデータを暗号化していない」と記載している。
- 初期の SecureWorks 社の AWS Community Marketplace 調査では、Amazon Machine Image (AMI)にある半分以上のイメージに何らかの欠陥があることを発見した。この欠陥にはテンポラリディレクトリ内のファイル、システムに残された埋め込みキー、スナップショットに残された追加のランレベル実行制御(rc)スクリプトが含まれる。イメージの出所が分からなければ、イメージを信頼することができない。そのため、Infrastructure as a service (IaaS)プロバイダは、様々なマーケットプレイスで共有するための説明書や要求事項を公開している。加えて、アプリストラクチャの実装には、顧客分析用の画面の操作記録が原因で 2019 年に iOS アプリプロバイダーを制限した Apple と同様の問題がある。

3.9.4. 当問題に対するポイントと対応策

必要なセキュリティ機能（多要素認証など）を有するクラウドサービスを選定し、メタストラクチャを保護するとともに、クラウドネイティブなアプリケーション設計や侵入検知・防止の仕組みによりワークロードの保護を行う。

3.9.5. DevSecOps サイクル

クラウドサービスにおけるメタストラクチャで発生する問題にフォーカスし、DevOps サイクルに対応策をマッピングしている。



3.9.6. DevSecOps を踏まえた対処

3.9.5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	セキュアでオープンなクラウドサービスの選定	・API の権限コントロールや MFA の機能が成熟し、かつドキュメントが充実している CSP を利用する	・利用予定のサービスを評価するために認証取得有無や各種フレームワークに準拠しているか評価する -STAR 認証の有無 -ENISA/IPA : クラウドコンピューティング 情報セキュリティ確保のためのフレームワークの確認
2	クラウドネイティブなアプリケーション設計	・クラウドにビジネスオペレーションとアプリケーションを移行する場合、オンプレミスのアプリケーションをそのままクラウドに移行する「リフト・アンド・シフト」のアプローチだけではなく、クラウドプラットフォーム	・CI/CD の導入やコンテナの利用によるイミュータブルなインフラ設計 -マイクロサービスの採用 -サーバーレスアーキテクチャの採用

		ムの機能を積極的に活用する。	
	アクセス管理ポリシーの検討	職務分掌を適切に行い、役割にあった権限を定義する。	・ロール(全体管理者、運用管理者、オペレータ、バックアップ&リカバリ、一般ユーザーなど)の定義 ・運用オペレーションにおける、不必要な高権限 ID (root など) の排除 ・システム管理者やテナント管理者などの強い権限を持つアカウントには、利用者のデータを操作する権限を与えない。 ・不要な ID や権限は残さない。
	認証手段の検討 (多要素認証の採用)	特権 ID の認証については、まず多要素認証を提供しているサービス事業者を選定し、設定を有効にすることが望ましい。 また一般利用者の認証については、サービスレベルや利用者のリテラシーを考慮して認証方式を検討する。	・認証手段を検討する上での考慮事項(例)として、以下のようなものが挙げられる。 -初回登録時と2回目以降の2つのユースケースについて検討が必要。 -管理機能のアクセス元 IP アドレスを制限する。 -追加コストがかかけられない場合などは、SNS 認証やメールアドレス認証など、比較的低コストで実現可能な認証手段を検討する。 -モバイルアプリの場合、2回目以降の認証については端末認証の採用を検討する。 -認証強化を他のサービス(IDaaS など)に委託し、シングルサインオン環境を構築する。
3	ペネトレーションテスト	公開されるサービスに対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。事前に定められた間隔及びシステム変更時に実施する。	・適切なエンゲージメントの上、ペネトレーションテストやレッドチーム演習を実施する。
4	アクセス監視	管理プレーンへのログインやアクセスに関するログを収集し、不正アクセスを検知する仕組みを用意する。	・AWS CloudTrail やサードパーティー製品の活用したログ管理を実施する。
	侵入検知(不正リクエスト)	・不正なアクセスを防止するための策を講じる(IPS、WAF など) ・API ゲートウェイを利用したエッジ	・IDS/IPS、WAF、DDoS protection など、外部からの不正侵入に対応できるソリューションの導入を検討

		処理等も検討する。	討する。
5	設定不備の検査（クラウドセキュリティ態勢管理）	ストレージや仮想ネットワーク、IAM など、管理プレーンから設定可能な IaaS 環境のセキュリティ関連設定について、設定ミスやコンプライアンスルールへの不適合、不適切な権限昇格を継続的にチェックする仕組みを導入する。	・ AWS Trusted Adviser やサードパーティ製品の活用したインフラストラクチャクラウドスタック全体のセキュリティ評価とコンプライアンスの監視を実施する。

3. 10. ケース 10 クラウド利用の可視性の限界

3. 10. 1. 概要

企業でクラウドを利用する場合、その状況を可視化し的確に把握することが重要になる。もし、可視性が保たれていない場合、シャドウ IT と呼ばれる私的利用の温床にもなりかねない。

3. 10. 2. ビジネスインパクト

利用しているクラウドサービスおよび、利用状況を把握できないことで以下のような影響がある。

- ・従業員に対しての適切なアクセス制限が出来ていない場合やガバナンスの不足により、プライベートの場所に置くべき企業の機密データがパブリックな場所に配置される可能性がある。
- ・データとサービスが会社の知らないところで使用されている場合、財産を制御することができなくなる。
- ・従業員がクラウドサービスを誤って設定した場合、既存のデータだけでなく、将来のデータに対しても攻撃可能になる可能性がある。

3. 10. 3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- 22,000を超えるコンテナオーケストレーションとAPI管理システムが保護されていないか、インターネット上で公開されている (Lacework社調査, 2018年)
- 今日使用されている1,000以上のクラウドサービスのうち、その多くがシャドウITのカテゴリーに分類される可能性がある (Skyhigh Networks Cloud Adoption & Risk Report 2015 Q2, 2015年)

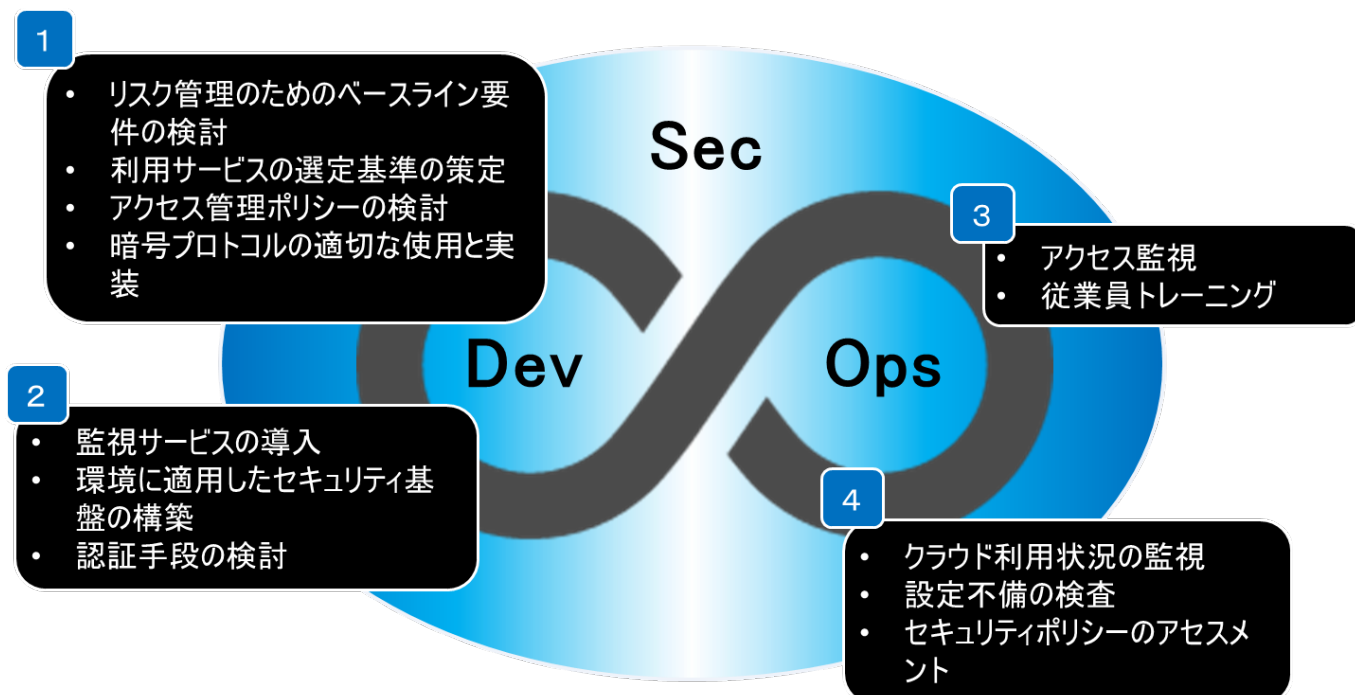
3. 10. 4. 当問題に対するポイントと対応策

クラウド可視化にかかわる対応策のポイントとして、大きく以下のようなものが挙げられる。

- ・クラウドサービス選定基準の策定
- ・適切なアクセス制限・管理
- ・クラウド利用ポリシーの策定と継続的なトレーニング
- ・シャドウ IT 対策ソリューションの導入
- ・データ保護方法の策定
- ・利用しているクラウドサービスの把握と利用状況の可視化

3. 10. 5. DevSecOps サイクル

企業内でのクラウドサービス利用および状況管理にフォーカスし、DevOps サイクルに対応策をマッピングしている。



3. 10. 6. DevSecOps を踏まえた対処

3. 10. 5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	リスク管理のためのベースライン要件の検討	適用される法律、法令と規制上の義務を順守した開発または調達を行うため、組織が所有または管理する物理的または仮想的な、アプリケーション及び基盤システムとネットワークコンポーネントのベースラインセキュリティ要件を定める。 標準的なベースライン設定から逸脱する場合は、導入、提供、使用前に、変更管理ポリシー及び手順に基づいて承認する。	・ 公開されているガイドラインや各種基準を元にベースラインアプローチを実施する。 -FISC 安全対策基準 -ISO270001 -Critical Security Control -PCI DSS
	利用サービスの選定基準の策定	従業員のアクティビティを全て管理することが難しいことを想定し、運用にあたっては厳格なポリシーを定めると共にクラウドサービスの利用制限や、利用できるサービスを限定するなどの対応を行う。	左記に同じ

	アクセス管理ポリシーの検討	職務分掌を適切に行い、役割にあった権限を定義する。	・ロール(全体管理者、運用管理者、オペレータ、バックアップ&リカバリ、一般ユーザーなど)の定義 ・運用オペレーションにおける、不必要な高権限 ID (root など) の排除 ・システム管理者やテナント管理者などの強い権限を持つアカウントには、利用者のデータを操作する権限を与えない。 ・不要な ID や権限は残さない。
	暗号プロトコルの適切な使用と実装	機微なデータについて、ストレージ内、データ使用時、及びデータの送受信時の暗号化を行う。暗号化には、オープン、検証済の標準アルゴリズムを利用する。 クラウド事業者が提供するマネージド HSM サービスを活用することが有効である。	・TLS を使用。 ・HSM サービスを使用。以下、パブリッククラウドのサービス例。 -AWS CloudHSM -Azure Dedicated HSM -Google Cloud HSM
2	監視サービスの導入	CASB などシャドーIT 対策ソリューションの活用を検討する。	左記に同じ
	環境に適応したセキュリティ基盤の構築	働き方の多様化に伴い、セキュリティの考え方も変化しているため、環境に適用したセキュリティモデルを構築する。	・例として、ゼロトラストセキュリティに即した環境の構築などが挙げられる。
	認証手段の検討 (多要素認証の採用)	特権 ID の認証については、まず多要素認証を提供しているサービス事業者を選定し、設定を有効にすることが望ましい。 また一般利用者の認証については、サービスレベルや利用者のリテラシーを考慮して認証方式を検討する。	・認証手段を検討する上での考慮事項(例)として、以下のようなものが挙げられる。 -初回登録時と2回目以降の2つのユースケースについて検討が必要。 -管理機能のアクセス元 IP アドレスを制限する。 -追加コストがかけられない場合などは、SNS 認証やメールアドレス認証など、比較的低コストで実現可能な認証手段を検討する。 -モバイルアプリの場合、2回目以降の認証については端末認証の採用を検討する。

			- 認証強化を他のサービス (IDaaS など) に委託し、シングルサインオン環境を構築する。
3	アクセス監視	従業員のクラウドサービス利用状況を常時監視し、不審な行動をチェックできるようにする。	・監視の観点としては以下が挙げられる - 普段と異なる行動 - ポリシーに反した行動 - 管理外のリソースアクセス
	従業員に対するセキュリティ意識向上トレーニングの実施	従業員に対してセキュリティに対する意識向上を目的としたトレーニングを実施する。	左記に同じ
4	クラウド利用状況の監視	内外部からのアクセス状況や操作履歴など、想定と異なる利用がないか確認する。	・監視項目例 - アクセス試行の傾向 - 許可されていないリソースへのアクセス
	設定不備の検査	設定不備などにより、意図せず公開されている資産などがいないか確認する。	・セキュリティ診断(設定不備の有無確認)の実施
	セキュリティベースラインのアセスメント	セキュリティベースライン要件の遵守状況を定期的 (少なくとも年 1 回) は再評価する。	左記に同じ

3. 11. ケース 11 クラウドサービスの悪用・乱用・不正利用

3. 11. 1. 概要

クラウドサービスの悪用・乱用・不正利用とは、悪意ある攻撃者がクラウド上のシステムを悪用し、以下に挙げるような行為が該当する。

- ・ DDoS攻撃
- ・ スパムメールとフィッシング詐欺
- ・ デジタル通貨のマイニング
- ・ 大規模な自動化されたクリック詐欺
- ・ 盗まれた認証情報データベースによるブルートフォース攻撃
- ・ 悪意のあるコンテンツや海賊版コンテンツのホスティング

3. 11. 2. ビジネスインパクト

- ・ 顧客の利用システムが侵入を許し、マイニング活動等に当該システムが利用された場合、システム利用料が膨大になる可能性がある。
- ・ マルウェアの感染による BOT 化や攻撃のための踏み台などに利用された場合、その企業のシステムが攻撃者に加担する形で利用されてしまう。

3. 11. 3. 想定事例と実例

「クラウド重大セキュリティ脅威 11 の悪質な脅威」に記載のある事例として以下が挙げられる。

- ランサムウェア Locky の亜種である Zepto は Microsoft OneDrive、GoogleDrive、Box などのクラウドサービスを通じて、悪意のあるファイルが被害者の手によってシェアされることで拡散されていた。
- CloudSquirrel（キャンペーン名）はフィッシングメールを利用して被害者をマルウェアに感染させるものであった。

フィッシングメールを開封（リンクを叩くと）すると、CloudSquirrel は、JAR ファイルによって別の暗号化されたマルウェアのペイロードをダウンロードして ユーザーを感染させる。感染後にマルウェアが Dropbox 上の C&C サーバと接続し、ユーザーの情報やパスワードが取得されてしまった。

3.11.4. 当問題に対するポイントと対応策

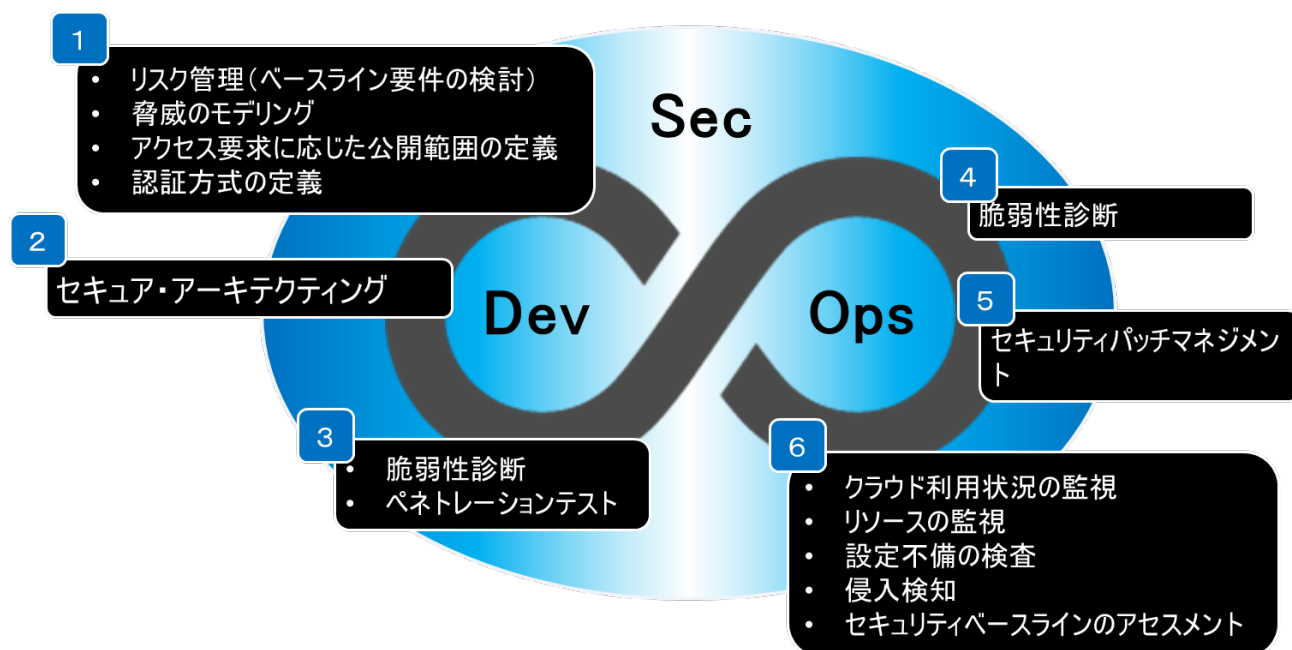
本章では、「クラウドサービスの悪用・乱用・不正利用」の対応策として、重要なポイントについて記載している。

クラウドサービスの不正利用において、利用者によるクラウドサービス利用を監視することが重要な対応策となる。監視要件として、いつ、どこから、誰が、どのリソースにアクセスしたかを把握し、正当な理由によるアクセスか否かを確認することで、不正利用を防止する。

また、DLP などを利用し、ファイルのダウンロードを制限（禁止）するなどの対策も有効となる。

3.11.5. DevSecOps サイクル

保有しているクラウド環境への攻撃（侵入）にフォーカスし、DevOps サイクルに対応策をマッピングしている。



3.11.6. DevSecOps を踏まえた対処

3.11.5. の図内の対応の詳細を以下に記載する。

項番	項目	概要	対応例
1	リスク管理のためのベースライン要件の検討	適用される法律、法令と規制上の義務を順守した開発または調達を行うため、組織が所有または管理する物理的または仮想的な、アプリケーション及び基盤システムとネットワークコンポーネントのベースラインセキュリティ要件を定める。 標準的なベースライン設定から逸脱する場合は、導入、提供、使用の前に、変更管理ポリシー及び手順に基づいて承認する。	・公開されているガイドラインや各種基準を元にベースラインアプローチを実施する。 -FISC 安全対策基準 -ISO270001 -Critical Security Control -PCI DSS
	リスク評価と脅威分析	想定されるリスクと脅威の検討	・公開されているフレームワーク等を参考に、脅威・リスク分析を実施する。 -STRIDE (for Microsoft) -DREAD
	アクセス要求に応じた公開範囲の定義	システムに対して、アクセス範囲をできる限り限定するような検討を行う。	・公開するリソースの分類（情報レベルなど） ・分類されたレベルに対するアクセス権の定義
	認証方法の定義	リソース（資産）にアクセスするための認証方法を検討する。	・公開リソースの配置環境に応じて適切な認証方法・方式（MFA、リスクベース、CAPTCHA、FID など）の定義を行う。
2	セキュアアーキテクティング	不正な侵入を防止するための策を講じる（IPS、WAF、DDOS 対策など）	・外部からの不正侵入に対応できるソリューションの導入を検討する。 -IDS/IPS -WAF -DDoS protection
3	動作テスト（脆弱性診断）	リアルタイムなコードのチェックや動的なアプリケーション解析を実施する。	・IAST・DAST ツールを利用し、機能テストを実行
	ペネトレーションテスト	公開されるサービスに対してペネトレーションテストを行い、攻撃防御・検知の確認を行う。事前に定められた間隔及びシステム変更時に実施する。	・適切なエンゲージメントの上、ペネトレーションテストやレッドチーム演習を実施する。

4	脆弱性診断	定期的な脆弱性診断を行う。	対象サービスに応じて、プラットフォーム診断とアプリケーション診断の実施有無を判断し、適切に実施する。
5	セキュリティパッチ管理	定期的にセキュリティパッチの公開有無をチェックし、必要に応じて適用する。	左記に同じ
6	クラウド利用状況の監視	内外部からのアクセス状況や操作履歴など、想定と異なる利用がないか確認する。	・以下監視項目例 -アクセス試行の傾向 -許可されていないリソースへのアクセス
	リソースの監視	リソースの過剰な負荷などを確認する。	左記に同じ
	設定不備の検査	設定不備などにより、意図せず公開されている資産などがいないか確認する。	・セキュリティ診断（設定不備の有無確認）の実施
	侵入検知（不正リクエスト）	内外部からの不正な侵入の有無をモニタリングする。	・セキュリティシステム（センサー）からのアラートチェックを行う。
	セキュリティベースラインのアセスメント	セキュリティベースライン要件の遵守状況を定期的（少なくとも年１回）は再評価する。	左記に同じ

4. 参考・引用文献

- ・ 政府情報システムにおけるクラウドサービスの利用に係る基本方針
 - https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf
- ・ クラウドの重大セキュリティ脅威 11 の悪質な脅威
 - https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/10/top-threats-to-cloud-computing-egregious-eleven_J_20191031.pdf
- ・ CCM Controls Frameworks
 - <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>