# クラウド
# 重大セキュリティ脅威

## 11の悪質な脅威

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

# Table of Contents

## 目次



# Acknowledgments


## Co-Chairs

Jon-Michael C. Brook

## Contributors

Jon-Michael Brook
Alexander Getsin
Greg Jensen
Laurie Jameson
Michael Roza
Neha Thethi
Ashish Kurmi
Shachaf Levy
Shira Shamban
Vic Hargrave
Victor Chin
Zoran Lalic
Randall Brooks

## Cloud Security Alliance Global Staff

Victor Chin
Stephen Lumpe (Cover Art)
AnnMarie Ulskey (Design)

# 日本語版提供に際しての告知及び注意事項

本書「クラウドの重大セキュリティ脅威　11 の悪質な脅威」は、Cloud Security Alliance（CSA）が公開している「Top Threats to Cloud Computing The Egregious 11」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版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 |
|---|---|---|
| 2019 年 10 月 31 日 | 日本語版 1.0 | 初版発行 |



# 日本語版作成に際しての謝辞

「クラウドの重大セキュリティ脅威　11 の悪質な脅威」の日本語訳は、CSA ジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

伊賀　誠
井上　淳
小川　依真恵
塩田　英二
高瀬　一彰
谷　　徹也
成川　達也
満田　淳
諸角　昌宏
門瀬　幸恵

# エグゼクティブサマリー

重大脅威（Top Threats）レポートは、従来、クラウド内の脅威、リスク、脆弱性に対する認識を高めることを目的としていました。このような問題は、多くの場合、クラウドコンピューティングのシェアード（共有）およびオンデマンドの特性によるものです。この第4回の記事では、クラウド業界のセキュリティ問題に関係する業界の専門家241人に対して再調査を行いました。今年は、回答者が、クラウド環境における11の顕著な脅威、リスク、脆弱性を評価しました。Top Threats Working Groupは、調査結果と専門知識を用いて、2019年の最終レポートを作成しました。

最新のレポートでは、11の悪質な脅威（Egregious Eleven）が強調されています（以前のランキングで行われたように、調査結果ごとに重要な順にランク付けしています）。

1. データ侵害
2. 設定ミスと不適切な変更管理
3. クラウドセキュリティアーキテクチャと戦略の欠如
4. ID、資格情報、アクセス、鍵の不十分な管理
5. アカウントハイジャック
6. 内部者の脅威
7. 安全でないインターフェースとAPI
8. 弱い管理プレーン
9. メタストラクチャとアプリストラクチャの障害
10. クラウド利用の可視性の限界
11. クラウドサービスの悪用・乱用・不正利用

## 観察と根拠

この調査の回答を分析した結果、クラウドサービスプロバイダー（CSP）の責任下においては、従来のクラウドセキュリティ問題の優先度が低下していることがわかりました。以前の「危険な12 の落とし穴」で取り上げられていた、DoS、共有テクノロジーの脆弱性、CSPデータの損失、システムの脆弱性などの懸念は、非常に低い評価となり、このレポートでは除外されました。これらが除外されたことは、CSPの責任のもとで従来のセキュリティ問題はそれほど問題ではないと思われていることを示唆しています。代わりに、上級管理職の決断の結果として、テクノロジースタックの上位に位置するセキュリティ問題に対処する必要性が高まっています。

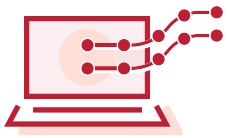
調査において新たに高く評価された項目は、より微妙であり、クラウドに対する消費者の理解の成熟度を示唆しています。これらの問題は本質的にクラウド固有のものであるため、消費者がクラウドへの移行を積極的に検討しているテクノロジーの展望を示しています。このようなトピックは、潜在的な管理プレーンの弱点、メタストラクチャやアプリケーションの障害、制限されたクラウドの可視性について言及しています。この新たな重点は、以前の重大脅威レポートでより強く取り上げられていた、一般的な脅威、リスク、脆弱性（データの損失やDoSなど）とは著しく異なります。

本書により、セキュリティ上の重要な問題とその低減策に関する組織の意識が高まり、クラウドへの移行とセキュリティの予算を立てる際に考慮されるようになることを願っています。このレポートは、コンプライアンス、リスク、テクノロジーのスタッフが使用することを意図した管理上の推奨事項と参照例を提供します。経営陣は、レポートに記載されている技術動向と概要に関する説明からも恩恵を受けることができます。

# セキュリティ問題: データ侵害



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たり、閲覧されたり、盗まれたり、権限のない人によって使用されたりするサイバーセキュリティインシデントです。データ侵害は、標的型攻撃の主な目的である場合もありますし、単に人的エラー、アプリケーションの脆弱性、不適切なセキュリティ対策の結果の場合もあります。データ侵害には、個人の健康医療情報、金融資産情報、個人を特定できる情報（PII）、営業秘密、知的財産などの、非公開のあらゆる情報が含まれますが、これらに限定されません。

| SECURITY RESPONSIBILITY |
| --- |
| ☒ Customer |
| ☒ Cloud Service Provider |
| ☑ Both |
| **ARCHITECTURE** |
| ☑ Infra |
| ☑ Meta |
| ☑ Info |
| ☑ Appli |
| **CLOUD SERVICE MODEL** |
| ☑ Software as a service (SaaS) |
| ☑ Platform as a service (PaaS) |
| ☑ Infrastructure as a service (IaaS) |

## ビジネスインパクト

データ侵害による負の影響として、次のものがあります:

1. 顧客やパートナーの評価と信頼への影響
2. 競合他社に対する知的財産（IP）の漏洩と、それによる製品リリースへの影響
3. 金銭的損失につながる規制の影響
4. （前項の結果として）市場価値の低下を引き起こすブランドへの影響
5. 法的および契約上の責任
6. インシデント対応とフォレンジックにより発生した金銭的損失

侵害から数か月後までデータ侵害が検出されない場合があります。そのようなインシデントは、その影響がすぐには明らかにならない場合があります（知的財産の流出など）。たとえば、米連邦政府人事管理局（OPM）やソニーピクチャーズのセキュリティ侵害では、どちらも検出までに約1年かかりました[1]。

## 要点

1. データがサイバー攻撃の主な標的になりつつあります。データのビジネス価値とその損失の影響を定義することは、データを所有または処理する組織にとって非常に重要です。
2. データを保護することは、誰がデータにアクセスできるかという問題に行きつきます。
3. インターネットを介してアクセスできるデータは、設定の誤りや悪用に対して最も脆弱な資産です。
4. 暗号化技術はデータの保護に役立ちますが、システムのパフォーマンスに悪影響を及ぼし、アプリケーションの使いやすさを低下させます。
5. 個々のCSPおよびデータプライバシーに関する法律を考慮した堅牢で十分にテストされたインシデント対応計画は、データ侵害の被害からの回復に役立ちます。

[1] Improving Cyber Resiliency https://cloudsecurityalliance.org/artifacts/improving-metrics-in-cyber-resiliency/

# 想定事例と実例

- Timehop社は、クラウドコンピューティング環境の侵害により、2,100万人のユーザに影響を与えるデータ侵害を起こしました。ソーシャルメディアアクセストークンも侵害されました。
- Uber社は、2016年後半にAmazon Web Services（AWS）アカウントがハッキングされ、世界中の5,700万人のユーザの個人情報が侵害されたことを明らかにしました。
- 2019年、VoIPサービスを提供する通信会社であるVoipo社は、何百万もの顧客通話ログ、SMSログ、認証情報を意図せず公開していました。データベースは2018年6月に公開され、2015年5月にさかのぼる通話ログとメッセージログが含まれていました。多くのファイルには詳細な通話記録（誰が誰に電話をかけたのか、通話時間など）が含まれていました。Voipo社は、700万件の通話記録、600万件のテキストメッセージ、および暗号化されていないパスワードを含むその他の内部ドキュメント（利用されると、攻撃者が会社のシステムの奥深くまでアクセス可能となる）を公開していました。

# CSAガイダンス

Domain 2: ガバナンスとエンタープライズリスクマネジメント
Domain 3: 法的課題 、契約および電子証拠開示
Domain 4: コンプライアンスと監査マネジメント
Domain 5: 情報ガバナンス
Domain 6: 管理画面 と事業継続
Domain 9: インシデントレスポンス
Domain 11: データセキュリティと暗号化
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理 （IAM）
Domain 14: 関連技術

# CCM Controls

## AIS アプリケーションとインターフェースセキュリティ

AIS-01: アプリケーションセキュリティ
AIS-02: 顧客アクセス要求
AIS-03: データの完全性
AIS-04: データセキュリティ/完全性

## CCC 変更管理と構成管理

CCC-05: 業務の変更

## DSI データセキュリティと情報ライフサイクル管理

DSI-01: 分類
DSI-02: データの管理表とフロー
DSI-03: E コマーストランザクション
DSI-04: 処理 / ラベル付 / セキュリティポリシー
DSI-05: 非実稼働データ
DSI-07: 安全な廃棄

## EKM 暗号化と鍵管理

EKM-01: 権限付与
EKM-02: 鍵生成
EKM-03: 機微データの保護
EKM-04: 保管とアクセス

## GRM ガバナンスとリスク管理

GRM-02: データフォーカスリスクアセスメント
GRM-06: ポリシー
GRM-10: リスクアセスメント

## IAM アイデンティティとアクセス管理

IAM-01: 監査ツールアクセス
IAM-04: ポリシーと手順

| THREAT ANALYSIS | LINKS AND REFERENCES |
| --- | --- |
| ☒ Spoofing Identity<br>☒ Tampering with Data<br>☒ Repudiation<br>☑ Information Disclosure<br>☒ Denial of Service<br>☒ Elevation of Privilege | 1. *Timehop Security Incident, July 4, 2018:* https://www.timehop.com/security/<br>2. *Uber Discloses Year-Old AWS Data Breach, Exposing Millions of Users:* https://awsinsider.net/articles/2017/11/21/uber-aws-data-breach.aspx<br>3. *Amazon hit with major data breach days before Black Friday:* https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday<br>4. *VOIPO database exposed millions of call and SMS logs, system data:* https://www.zdnet.com/article/voipo-database-exposed-millions-of-call-and-sms-logs-system-data/ |

# セキュリティ問題: 設定ミスと不適切な変更管理

| SECURITY RESPONSIBILITY |
| --- |
| ☑ Customer |
| ☒ Cloud Service Provider |
| ☒ Both |

| ARCHITECTURE |
| --- |
| ☑ Infra |
| ☑ Meta |
| ☑ Info |
| ☑ Appli |

| CLOUD SERVICE MODEL |
| --- |
| ☑ Software as a Service (SaaS) |
| ☑ Platform as a Service (PaaS) |
| ☑ Infrastructure as a Service (IaaS) |

コンピューティング資産が正しくセットアップされていない場合に設定ミスが発生し、多くの場合、悪意のある活動に対して脆弱になります。一般的な例には、セキュリティ保護されていないデータストレージ要素もしくはコンテナ、過剰な許可、デフォルトから変更されないままの資格情報や設定、標準のセキュリティ制御が無効、パッチが未適用なシステム、ロギングもしくは監視が無効でポートやサービスへの無制限のアクセスが含まれます。クラウドリソースの設定ミスは、データ侵害の主要な原因であり、リソースの削除もしくは変更やサービスの中断を引き起こす可能性があります。

適切な変更管理を欠いていることが、クラウド環境での設定ミスの一般的な原因です。クラウド環境とクラウドコンピューティングの手法は、従来のITとは異なり、変更の制御がより困難になります。
従来の変更プロセスには複数の役割と承認が関係しており、本番に達するまでに数日または数週間かかることがありました。企業のデータセンターで静的だったインフラストラクチャ要素は、クラウド内のソフトウェアに抽象化され、変更プロセスのライフサイクル全体はほんの数分または数秒で済む場合があります。クラウドコンピューティング技術は、急速な変化をサポートするための自動化、役割の拡大、アクセスに依存しています。複数のクラウドプロバイダを使用すると、各プロバイダがほぼ毎日拡張する独自の機能を備えているため、複雑さが増します。この動的な環境では、多くの企業がまだ習得していない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です。

## 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、設定ミスの内容と、それが検出、緩和される速さによっては深刻になる可能性があります。最も一般的に報告されている影響は、クラウドリポジトリに保存されているデータの漏洩です。

## 要点

1. クラウドベースのリソースは非常に複雑で動的であるため、注意深い設定が必要です。
2. 従来の制御および変更管理アプローチは、クラウドでは効果的ではありません。
3. 企業は自動化を採用し、誤って設定されたリソースを継続的に検査し、リアルタイムで問題を修正するテクノロジーを採用する必要があります。

# 想定事例と実例

設定ミスや不適切な変更管理に関連する問題の最近の事例には、次のものがあります：

1. AWS Simple Storage Service（S3）クラウドストレージバケットの設定ミスにより、1億2300万人のアメリカの世帯の詳細なプライベートデータが公開されました。データセットは、信用調査会社であるExperian社が所有し、Alteryx社と呼ばれるオンラインマーケティング／データ分析会社へデータを販売しました。ファイルを公開したのはAlteryx社でした。
2. Exactis社が所有するセキュリティ保護されていないElasticsearchデータベースは、2億3000万人の米国消費者の個人データを含む大規模な侵害をもたらしました。データベースサーバーが、パブリックにアクセスできるように設定されていました。
3. 自動化プロセスとアセンブリを専門とするエンジニアリング企業であるLevel One Robotics社は、フォルクスワーゲン、クライスラー、フォード、トヨタ、ゼネラルモーターズ、テスラ、ティッセンクルップを含む100社以上の製造会社に属する機密情報を公開しました。この場合、誤って設定されたアセットは、任意のrsyncクライアントへの認証されていないデータ転送を許可するrsync（バックアップ）サーバでした。

# CSAガイダンス

Domain 4: コンプライアンスと監査マネジメント
Domain 5: 情報ガバナンス
Domain 6: 管理画面 と事業継続
Domain 7: インフラストラクチャ・ セキュリティ
Domain 8: 仮想化とコンテナ技術
Domain 10: アプリケーションセキュリティ
Domain 11: データセキュリティと暗号化
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理（IAM）

# CCM Controls

AIS アプリケーションとインターフェースセキュリティ
AIS-01: アプリケーションセキュリティ
AIS-04: データセキュリティ/完全性

CCC 変更管理と構成管理
CCC-02: 開発の外部委託
CCC-03: 品質検査
CCC-05: 業務の変更

DSI データセキュリティと情報ライフサイクル管理
DSI-01: 分類
DSI-04: 処理 / ラベル付 / セキュリティポリシー

EKM 暗号化と鍵管理
EKM-03: 機微データの保護
EKM-04: 保管とアクセス

GRM ガバナンスとリスク管理
GRM-01: ベースライン要件
GRM-02: データフォーカスリスクアセスメント

HRS 人事
HRS-09: 訓練 / 認識向上

IAM アイデンティティとアクセス管理
IAM-02: 資格証明のライフサイクル / プロビジョニング管理
IAM-05: 職務の分離

IVS インフラと仮想化のセキュリティ

IVS-02: 変更検知

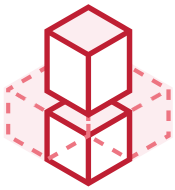
IVS-06: ネットワークセキュリティ

IVS-07: OS 堅牢性と基本管理

| THREAT ANALYSIS | LINKS AND REFERENCES |
| --- | --- |
| ☒ Spoofing Identity<br>☑ Tampering with Data<br>☑ Repudiation<br>☑ Information Disclosure<br>☑ Denial of Service<br>☒ Elevation of Privilege | 1. *120 Million American Households Exposed in 'Massive' ConsumerView Database Leak:* https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-households-exposed-in-massive-consumerview-database-leak/#37bb94d27961<br>2. *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records:* https://www.wired.com/story/exactis-database-leak-340-million-records/<br>3. *Short Circuit: How a Robotics Vendor Exposed Confidential Data for Major Manufacturing Companies:* https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-major-manufacturing-companies |

# セキュリティ問題: クラウドセキュリティアーキテクチャと戦略の欠如



世界中で、組織は組織のITインフラストラクチャの一部をパブリッククラウドへ移行することを進めています。この変化に対してもっとも大きな挑戦の一つはサイバー攻撃に対抗する適切なセキュリティアーキテクチャの実装です。不幸なことに、このプロセスは多くの組織にとって未だ謎に包まれています。組織がクラウド移行を既存のITスタックとセキュリティコントロールをクラウド環境に単純に移植する「リフト・アンド・シフト」の試みだと考えた場合、データは従来とは異なる脅威群に晒されます。共有セキュリティ責任モデルに対する理解の不足もまた一つの要因となります。

| SECURITY RESPONSIBILITY |
| --- |
| ☑ Customer |
| ☒ Cloud Service Provider |
| ☒ Both |
| **ARCHITECTURE** |
| ☑ Infra |
| ☒ Meta |
| ☒ Info |
| ☒ Appli |
| **CLOUD SERVICE MODEL** |
| ☒ Software as a Service (SaaS) |
| ☑ Platform as a Service (PaaS) |
| ☑ Infrastructure as a Service (IaaS) |

更に、機能性と移行の速さはしばしばセキュリティより優先します。これらの要因は、クラウドにおけるセキュリティアーキテクチャ並びに戦略の欠如を引き起こします — サイバー攻撃に対して組織は脆弱になります。セキュリティアーキテクチャの実装と堅牢なセキュリティ戦略の策定は、組織に対して、クラウドにおけるビジネス活動の運用と推進のための強固な基盤を提供します。クラウド環境の可視性を高めるためのクラウドネイティブなツールを活用することで、リスクとコストを最小化できます。このような予防策を採用すれば、侵害のリスクは劇的に低減されるでしょう。

## ビジネスインパクト

企業が大きいか小さいかに関係無く、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す。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ります。

## 要点

1. セキュリティアーキテクチャがビジネスのゴールと目標に整合していることを確実にします。
2. セキュリティアーキテクチャフレームワークを策定し実装します。
3. 脅威モデルが継続的に最新に維持されることを確実にします。
4. 実際のセキュリティの状態を見える状態にして継続的に提供します。

# 想定事例と実例

クラウドセキュリティアーキテクチャと戦略の欠如に関連する最近の問題の例として以下が挙げられます:

- テクノロジーとクラウドの大手であるアクセンチュア社は、最近、セキュアでない４つのクラウドサーバに大規模なプライベートデータストアを不注意に残し、機密性の高いパスワードと復号鍵が暴露され、大きな被害を同社と同社の顧客にもたらす可能性があったことを確認しました。Amazon の S3 ストレージサービスにホストされたそれらのサーバ群には、同社のエンタープライズクラウド製品のための数百ギガバイトのデータを保持していました。同社は Fortune 100 に名を連ねる大多数の企業にサポートを提供していると述べていました。それらのデータは、サーバのウェブアドレスを知っている誰もがパスワード無しでダウンロード可能でした。
- Kromtech Security Center社 のリサーチャーは Honda Connect アプリケーションに紐付く大量のデータがオンラインで晒されていることを見つけました。これらのデータはパブリックにアクセスでき、かつ保護されていない二つの危険なAmazon AWS S3 バケットに保管されていました。

# CSAガイダンス

Domain 1: クラウドコンピューティングのコンセプトとアーキテクチャ
Domain 6: 管理画面 と事業継続
Domain 7: インフラストラクチャ・ セキュリティ

# CCM Controls

AIS アプリケーションとインターフェースセキュリティ
AIS-04: データセキュリティ/完全性

GRM ガバナンスとリスク管理
GRM-01: ベースライン要件
GRM-02: データフォーカスリスクアセスメント
GRM-05: サポート / 関与
GRM-08: リスクアセスメントにおけるポリシーの影響

IAM アイデンティティとアクセス管理
IAM-02: 資格証明のライフサイクル / プロビジョニング管理

IVS インフラと仮想化のセキュリティ
IVS-06: ネットワークセキュリティ
IVS-08: 本番 / テスト環境
IVS-09: 区分
IVS-13: ネットワークアーキテクチャ

STA サプライチェーンの管理、透明性、説明責任
STA-03: ネットワーク / インフラストラクチャサービス
STA-05: サプライチェーンの合意

| THREAT ANALYSIS | LINKS AND REFERENCES |
| --- | --- |
| ☑ Spoofing Identity<br>☑ Tampering with Data<br>☑ Repudiation<br>☑ Information Disclosure<br>☑ Denial of Service<br>☑ Elevation of Privilege | 1. *Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective:* https://www.infoq.com/articles/cloud-security-architecture-intro<br>2. *The New Shared Responsibility Model For Cloud Security:* https://www.forbes.com/sites/forbestechcouncil/2018/10/15/the-new-shared- responsibility-model-for-cloud-security/#508d0f422490<br>3. *The Importance of a Defined Cloud Strategy:* https://www.expedient.com/blog/the-importance-of-a-defined-cloud-strategy/<br>4. *Accenture left a huge trove of highly sensitive data on exposed servers:* https://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers/<br>5. *The Consequences of a Cyber Security Breach:* https://www.sungardas.com/en/about/resources/articles/the-consequences-of-a-cyber-security-breach/<br>6. *Why Enterprise Architecture Deserves a Seat at the Security Table:* https://erwin.com/blog/enterprise-architecture-seat-security-table/<br>7. *Personal data of over 50,000 Honda Connect App leaked:* https://www.hackread.com/personal-data-of-over-50000-honda-connect-app-leaked/ |

# セキュリティ問題: ID、資格情報、アクセス、鍵の不十分な管理

ID、資格情報およびアクセス管理システムには、価値のある資産に対する管理・監視およびセキュアなアクセスを組織に可能とするためのツールやポリシーが含まれます。例としては、電子ファイル、コンピュータシステム、サーバルームやビルのような物理資源があります。

| SECURITY RESPONSIBILITY |
| --- |
| ☑ Customer |
| ☒ Cloud Service Provider |
| ☒ Both |
| **ARCHITECTURE** |
| ☑ Infra |
| ☒ Meta |
| ☒ Info |
| ☒ Appli |
| **CLOUD SERVICE MODEL** |
| ☒ Software as a Service (SaaS) |
| ☑ Platform as a Service (PaaS) |
| ☑ Infrastructure as a Service (IaaS) |

クラウドコンピューティングはIDとアクセス管理（IAM: Identity and access management）に関連する従来の内部システム管理手法に複数の変更をもたらします。これらは必ずしも新しい問題ではありませんが、それらはクラウドを扱う際にはより重大な問題です。なぜなら、クラウドコンピューティングはID・資格情報・アクセス管理に大きな影響を与えるからです。プライベートクラウドとパブリッククラウド両方の設定において、CSP とクラウド利用者はセキュリティを損なうこと無く IAM を管理しなければなりません。

セキュリティインシデントとデータ侵害は資格情報を適切に保護できていないことによって起こされます。例えば -暗号鍵・パスワードおよび証明書の定常的かつ自動化されたローテーションの欠如、ID・資格情報およびアクセス管理システムのスケーラビリティの欠如、多要素認証の不適切な利用、強固なパスワードを未使用、等。

資格情報と暗号鍵はソースコードに含まれてはならず、（GitHubにあるような）公開されているリポジトリに配置されてもなりません。なぜなら、発見され悪用される高いリスクがあるためです。鍵は適切に保護される必要があり、かつ鍵管理の活動を確実に実行するために、十分に保護された公開鍵認証基盤（PKI）が必須です。

ID管理システムは数百万のユーザとCSPのライフサイクルマネジメントを扱うために拡張する必要があります。ID管理システムは退職や役割の変更など、人事異動に対応するために、即時のリソースアクセス権停止をサポートできていなければなりません。そのようなID管理ライフサイクルプロセスは、クラウド環境と統合され、自動化され、タイムリーに行われるべきです。

IDシステムはより相互接続されるようになっており、ユーザメンテナンスの手間を軽減するためにクラウドプロバイダとのID連携（例: Security Assertion Markup Language（SAML）の利用）もより普及しています。クラウドプロバイダとのID連携を計画する組織は、クラウドプロバイダの ID ソリューションに関するセキュリティを理解していなければなりません。これにはプロセス、インフラストラクチャおよび顧客間の分離（IDを共有するソリューションの場合）を含みます。

クラウドサービスのユーザとオペレータ（つまり、クラウド利用者）には多要素認証システム -- 例としてはスマートカード、ワンタイムパスワード（OTP）、電話認証 -- が必要とされるべきです。

これらの形式の認証は、パスワードが盗まれた場合の解決に役立ちます。パスワードが盗まれた場合、ユーザの同意なくリソースにアクセスすることが可能になってしまいます。パスワード盗難は、"pass the hash" 攻撃のような一般的な Network lateral movement 攻撃などで発生することがあります。

レガシーなシステムがパスワードのみの使用を必要とする場合には、認証システムは強固なパスワードの確認や組織が定義したパスワード有効期限などのポリシー強制をサポートしなければなりません。

保管データを守るために使う暗号鍵の管理は、生成、配置、保管、更新および削除を含むライフサイクルを通して実施されていなければなりません。鍵に対して認可されていないアクセスを行う攻撃への対処に役立ちます。鍵のローテーションポリシーが欠落している状態で暗号鍵が盗難されると、侵害を受ける時間と範囲を劇的に増加させるかも知れません。

秘密情報（例：パスワード、秘密鍵、または秘密の顧客連絡先データベース）を保管しているあらゆる集中化したストレージメカニズムは、攻撃者にとって極めて高い価値を持つターゲットになります。鍵やパスワードの集中管理を選択することは組織が注意深く検討しなければならない妥協案です。つまり、鍵集中管理の利便性は、これらの鍵をグループ化することによるリスクを伴います。あらゆる高い価値のある資産と同様に、IDと鍵管理システムの監視と保護は高い優先度を持つべきです。

## ビジネスインパクト

悪意を企てる者は、正規のユーザ、オペレータ、開発者の振りをしてデータの読み取り・抽出、変更、削除したり；コントロールプレーンや管理機能に問題を引き起こしたり；移動中のデータをのぞき見したり；正規のサイトと見せかけて悪意のあるソフトウェアをリリースしたりします。結果として、ID、資格情報、鍵の不十分な管理は、データに対する許可されていないアクセスを可能にし、組織やエンドユーザに対して壊滅的なダメージを与える可能性があります。

## 要点

1. アカウントを安全にします。二要素認証、ルートアカウントの利用の制限が含まれます。
2. クラウドユーザとIDに対する最も厳格なIDとアクセス制御を行います。
3. ビジネスニーズと最小権限の原則に基づいて、アカウント、バーチャルプライベートクラウド（VPC）、IDグループの隔離と分離を行います。
4. 鍵のローテーション、利用していない資格情報と権限の削除、集中的かつ機械的な鍵管理を採用します。

# 想定事例と実例

ID、資格情報、アクセス、鍵の不十分な管理に関連する問題の最近の事例を以下に示します:

- 2018年12月、ドイツの学生は脆弱なパスワードを使用して保護しているデータをハックし、クラウドプラットフォームを利用してそのデータを共有しました。その二十歳の学生は、政治的なスタンスが気に入らない数百人の議員や個人のオンラインアカウントをハックするために ″ Iloveyou″ や ″1234″ のようなパスワードを使いました。ドイツのサイバーセキュリティ当局は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、照合され、 Twitter やその他のオンラインプラットフォームを通じて拡散されたことを発表しました。
- 会計ファームのデロイトは、ID、資格情報、アクセスの管理が弱いことにより大量のデータ侵害を経験しました。2017年9月25日、同社は脆弱な管理者 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ことを検知したと発表しています。この侵害は 2017年3月に発生しており、攻撃者には特権が与えられたと見られ、「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ます。管理者アカウントには一つのパスワードのみが必要とされており、二段階認証プロセスは採用されていませんでした。伝えられるところによると、攻撃者は 2016年10月～11月からサーバをコントロールしていたといいます。デロイトの24万4千人のスタッフは受信および送信メールを保管するため、 Microsoft から提供される Azure クラウドサービスを利用していました。加えてハッカー達は eメールの他に、ユーザ名、パスワード、IPアドレス、企業向けのアーキテクチャダイアグラムおよび健康情報にアクセスした可能性があります。一部の eメールには機密性の高いセキュリティと設計の詳細が添付されていました。さらに、ハッカー達は優良顧客のユーザ名、パスワードおよび個人データにもアクセスした可能性があります。
- 2017年5月31日、ある脅威アクターがOneLogin の AWS 鍵を利用し、USの他の小規模サービスプロバイダとの中間のホストから、API を経由して同社のAWSプラットフォームにアクセスしました。IDとパスワードの管理サービスを提供している OneLogin はその侵害を検知し、侵害を止めるために数分以内に影響を受けたシステム（および、侵害された鍵）をシャットダウンしました。彼らはまた、他のアクティブな脅威が存在しないことを確認しました。
- 攻撃者達は、以前 GitHub からクラウドサービスの資格情報を収集し、仮想通貨のマイニングを行うためにアカウントをハイジャックしていました。- GitHub プロジェクトに含まれていたクラウドサービスプロバイダの資格情報はプロジェクトの立ち上げ36時間以内に発見され悪用されました。
- テキサス州オースティンを拠点とする情報セキュリティソリューションプロバイダの Praetorian は、Amazon 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新たなクラウドベースのプラットフォームを立ち上げました。

# CSAガイダンス

Domain 11: 暗号化と鍵管理
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理 (IAM)

# CCM Controls

**EKM** 暗号化と鍵管理

EKM-01: 権限付与
EKM-02: 鍵生成
EKM-03: 機微データの保護
EKM-04: 保管とアクセス

**HRS** 人事

HRS-01: 資産返却
HRS-03: 雇用契約
HRS-04: 雇用の終了
HRS-08: 技術的に受け入れられる使用
HRS-09: 訓練 / 認識向上
HRS-10: ユーザ責任

**IAM** アイデンティティとアクセス管理

IAM-01: 監査ツールアクセス
IAM-02: 資格証明のライフサイクル / プロビジョニング管理
IAM-03: 診断 / 設定ポートアクセス
IAM-04: ポリシーと手順
IAM-05: 職務の分離
IAM-06: ソースコードアクセス制限
IAM-07: 第三者アクセス
IAM-08: 信頼された発行元
IAM-09: ユーザアクセス認可
IAM-10: ユーザアクセスレビュー
IAM-11: ユーザアクセス取り消し
IAM-12: ユーザ ID 資格情報
IAM-13: ユーティリティプログラムアクセス

## THREAT ANALYSIS

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

## LINKS AND REFERENCES


1. *German Man Confesses to Hacking Politicians' Data, Officials Say:* https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html
2. *German data hacker says he was 'annoyed' by politicians:* https://www.irishtimes.com/news/world/europe/german-data-hacker-says-he-was-annoyed-by-politicians-1.3751332
3. *Deloitte hit by cyber-attack revealing clients' secret emails:* https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails
4. *Deloitte breached by hackers for months:* https://blog.malwarebytes.com/security-world/2017/09/deloitte-breached-by-hackers-for-months/
5. *Major identity manager breach exposes sensitive user info:* https://www.engadget.com/2017/06/03/major-identity-manager-breach-stole-sensitive-user-info/?guccounter=1
6. *OneLogin, May 31, 2017 Security Incident:* https://www.onelogin.com/blog/may-31-2017-security-incident
7. *System Shock: How A Cloud Leak Exposed Accenture's Business:* https://www.upguard.com/breaches/cloud-leak-accenture
8. *Quora breach leaks data on over 100 million users:* https://www.engadget.com/2018/12/03/quora-breach/
9. *Attackers Scrape GitHub for Cloud Service Credentials, Hijack Account to Mine Virtual Currency:* http://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/
10. *Dell Releases Fix for Root Certificate Fail:* http://www.bankinfosecurity.com/dell-releases-fix-for-root-certificate-fail-a-8701/op-1

# セキュリティ問題: アカウントハイジャック

アカウントハイジャックは、悪意のある攻撃者が、高い権限または機密性の高いアカウントをアクセスし、悪用する脅威です。クラウド環境において、リスクが最も高いアカウントはクラウドサービスアカウントまたはサブスクリプションです。フィッシング攻撃、クラウドベース・システムへの攻撃、資格情報の盗難により、これらのアカウントが侵害される可能性があります。これらの脅威は、ユニークで潜在的に強力であり、データや資産の損失や運用への侵害等、クラウド環境の重大な混乱を引き起こす可能性があります。これらのリスクは、クラウドサービスの配備モデル、およびその組織とガバナンスのモデルに起因します。データとアプリケーションが、クラウドアカウントまたはサブスクリプションの存在するクラウドサービスに存在します。特に、サブスクリプションは、権限と資格情報を持っている人なら誰でも、オンラインでアクセスできます。

| SECURITY RESPONSIBILITY |
| --- |
| ☑ Customer |
| ☑ Cloud Service Provider |
| ☑ Both |
| **ARCHITECTURE** |
| ☒ Infra |
| ☑ Meta |
| ☒ Info |
| ☑ Appli |
| **CLOUD SERVICE MODEL** |
| ☑ Software as a Service (SaaS) |
| ☑ Platform as a Service (PaaS) |
| ☑ Infrastructure as a Service (IaaS) |

組織は、侵害被害を抑えるために、これらの脅威に対する認識と、多層防御戦略を、積極的に促進すべきです。

## ビジネスインパクト

アカウントとサービスのハイジャックは、アカウント、サービス、内部データの制御に対する完全なセキュリティ侵害を意味します。このようなシナリオでは、アカウントサービスに依存するビジネスロジック、機能、データ、アプリケーションが危険にさらされます。

そのようなセキュリティ侵害から発生する影響は、深刻になることがあります。最近の侵害事例では、例えば、組織の資産、データ、機能が完全に削除される等、重大な運用上およびビジネス上の混乱をきたしました。

アカウントハイジャックの結果には、評判の低下、ブランド価値の低下、法的責任の発生、機微な個人情報やビジネス情報の開示につながるデータ漏洩が含まれます。

## 要点

1. アカウントハイジャックは、真剣に取り組まなければならない脅威です。
2. 多層防御とIAMコントロールは、アカウントハイジャックを緩和する上で重要です。

# 想定事例と実例

アカウントハイジャックに関する問題の最新事例は次のとおりです:

- 2014年6月、Code Space 社（以前は、コードホスティングサービス会社）のAWSアカウントが、管理用コンソールを多要素認証で防御していなかったため被害に遭いました。全ての情報資産が破壊され、事業が継続不能となりました。
- 2018年、Consumer Cloud Services社はハイジャックされ、ダークネット市場で大規模にデータを販売されました。
- 2017年、特にMicrosoft Office 365において、クラウドアカウントをターゲットとした攻撃の増加が記録されました。
- 2010年4月、アマゾンでクロスサイトスクリプティング（XSS）バグが確認されました。このバグは攻撃者にサイトからの認証情報の乗っ取りを許してしまいます。2009 年には、非常に多くのアマゾン上のシステムがハイジャックされ、Zeus ボットネットのノードが走らされました。

# CSAガイダンス

Domain 2: ガバナンスとエンタープライズリスクマネジメント
Domain 6: 管理画面 と事業継続
Domain 9: インシデントレスポンス
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理 (IAM)

# CCM Controls

BCR 事業継続管理と運用レジリエンス
BCR-01: 事業継続計画

IAM アイデンティティとアクセス管理
IAM-02: 資格証明のライフサイクル / プロビジョニング管理
IAM-05: 職務の分離
IAM-08: 信頼された発行元
IAM-10: ユーザアクセスレビュー
IAM-11: ユーザアクセス取り消し

IVS インフラと仮想化のセキュリティ
IVS-01: 監査ログ / 侵入検知
IVS-08: 本番 / テスト環境

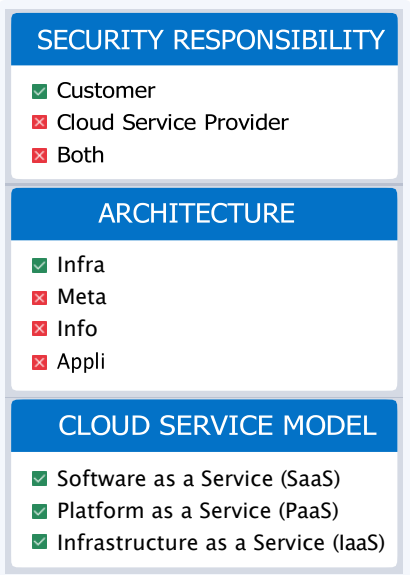
SEF セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス
SEF-01: 契約 / 機関の維持

| THREAT ANALYSIS | LINKS AND REFERENCES |
|---|---|
| ☑ Spoofing Identity<br>☑ Tampering with Data<br>☑ Repudiation<br>☑ Information Disclosure<br>☑ Denial of Service<br>☑ Elevation of Privilege | 1. *Murder in the Amazon cloud:* https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html<br>2. *Alleged hacker tried to sell details of 319 million iCloud users for bitcoin:* https://www.cultofmac.com/583836/alleged-hacker-tried-to-sell-details-of-319-million-icloud-for-bitcoin/<br>3. *PoC Exploit Compromises Microsoft Live Accounts via Subdomain Hijacking:* https://threatpost.com/poc-exploit-compromises-microsoft-live-accounts-via-subdomain-hijacking/138719/<br>4. *How can Office 365 phishing threats be addressed?:* https://www.helpnetsecurity.com/2018/05/18/office-365-phishing-threats/ |

# セキュリティ問題: 内部者の脅威

CERTは、内部者の脅威を「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」と定義しています。現在の、または元の従業者、請負業者、信頼しているビジネスパートナーが内部者となり得ます。外部の脅威主体と違い、内部者は、ファイアウォール、VPN、その他境界防御を破る必要がありません。ネットワーク、コンピュータシステム、企業の機密データに直接アクセスできるセキュリティ上信頼できる領域の内側で、内部者は行動します。




内部者の脅威は、あなたが思っている以上に広がっています。「Netwrix 2018 Cloud Security Report」によると、58%の企業がセキュリティ侵害を内部者に起因しているとしています。セキュリティインシデントの原因で最も多いのは内部者の過失なのです。

Ponemon Instituteの「2018 Cost of Insider Threats study」によると、報告された内部者のインシデントの根本的な原因は、64%が社員または請負業者の過失であったのに対し、内部犯行は23%、資格情報の盗難は13%でした。次のような一般的なシナリオも挙がっています。クラウドサーバの誤設定、企業の機密データを個人所有の安全でない機器やシステムに保存する社員、企業の資産への悪意のある攻撃であるフィッシングメールに引っかかる社員やその他の内部者、など。

## ビジネスインパクト

内部者の脅威は、機密情報や知的財産の損失をもたらします。攻撃によるシステムの停止は、企業の生産性に悪影響を及ぼします。さらに、データの損失や顧客の被害は、会社のサービスに対する信頼を低下させます。

内部者によるセキュリティインシデントへの対応には、次に挙げる対応が必要となります：封じ込め、復旧、インシデント対応、調査、事後分析、エスカレーション、モニタリング、監視。これらの対応は、企業の作業負荷とセキュリティ予算を大幅に増やすことになります。Ponemon Instituteが調査した企業においては、2017年の内部者によるインシデントの１社あたりの平均コストは870万ドルを超え、最大コストは2,650万ドルに達しました。

# 要点

1. 内部者の過失を最小限に抑える対策は、内部者の脅威による悪影響を低減する効果があります。以下に説明するアクションは、怠慢なユーザおよび管理者がもたらすセキュリティ問題の解決に役立ちます。
2. セキュリティ担当者のトレーニングと教育:コンピュータシステム、ネットワーク、モバイル機器、バックアップ機器の正しい導入、設定、監視のためのトレーニングをセキュリティチームに提供します。
3. 常勤社員の意識向上トレーニング: フィッシングや、ノートPCやモバイル機器で社外に持ち出す企業データの保護など、セキュリティリスクへの対処方法を常勤社員に周知するトレーニングを提供します。強固なパスワードの使用や適宜パスワードを変更することが必要です。社員に不正な行動が与える影響について教えます。
4. 誤設定されたクラウドサーバの修正: クラウドとオンプレミスのサーバを定期的に監査し、組織全体で設定されたセキュリティ基準（ベースライン）からのずれを修正します。
5. 重要なシステムへのアクセス制限:セキュリティシステムと重要なサーバへの特権アクセスが必要最小限の社員に制限されていて、それぞれがミッションクリティカルなサーバに対処するトレーニングを受けていることを確認しなさい。様々な権限レベルでアクセスする全てのコンピュータサーバへのアクセスをモニターしなさい。

# 想定事例と実例

内部者の脅威に関連する最新事例は次のとおりです:

- 2018年6月、テスラ社CEO、イーロンマスク氏は、自社の従業員に業務妨害行為があったと主張する電子メールをテスラ社員に送付しました。不満を持つ従業員であるこの妨害者は、偽のユーザ名を使用し、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を書き換えたと言われています。従業員はまた、「大量のテスラの機密データを未知の第三者」に提供していました。
- また、2018年には、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ました。ダイヤモンド商人が作ったそのスキームとは、サプライヤーから石ころを買い、銀行向けに値札をつけるもので、その総額は: $18 億ドルになりました。
- IBM X-Force Threat Intelligence Index 2018 によると、「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、20億件超のレコードを危険な状態に晒しました。2017年にX-Forceが追跡調査した不正アクセスされたレコードの数の７割近くです。

# CSAガイダンス

Domain 2: ガバナンスとエンタープライズリスクマネジメント
Domain 5: 情報ガバナンス
Domain 11: 暗号化と鍵管理
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理 (IAM)

# CCM Controls

DCS データセンタセキュリティ
DCS-04: オフサイトへの許可
DCS-08: 許可されていない個人エントリの入室
DCS-09: ユーザアクセス

DSI データセキュリティと情報ライフサイクル管理
DSI-04: 処理 / ラベル付 / セキュリティポリシー
DSI-06: 所有者/管理責任

EKM 暗号化と鍵管理
EKM-02: 鍵生成
EKM-03: 機微データの保護

GRM ガバナンスとリスク管理
GRM-03: 管理監督
GRM-04: 管理プログラム
GRM-06: ポリシー
GRM-07: ポリシー適用
GRM-10: リスクアセスメント

HRS 人事
HRS-02: 経歴スクリーニング
HRS-03: 雇用契約
HRS-07: ロール / 責任

IAM アイデンティティとアクセス管理
IAM-01: 監査ツールアクセス
IAM-05: 職務の分離
IAM-08: 信頼された発行元
IAM-09: ユーザアクセス認可
IAM-10: ユーザアクセスレビュー
IAM-11: ユーザアクセス取り消し

IVS インフラと仮想化のセキュリティ
IVS-09: 区分

STA サプライチェーンの管理、透明性、説明責任
STA-09: 第三者の監査

| THREAT ANALYSIS |
| --- |
| ☑ Spoofing Identity |
| ☑ Tampering with Data |
| ☒ Repudiation |
| ☑ Information Disclosure |
| ☒ Denial of Service |
| ☑ Elevation of Privilege |

## LINKS AND REFERENCES


1. *CERT Definition of an 'Insider Threat' - Updated:* https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html
2. *Cloud Security Risks and Concerns in 2018:* https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/
3. *IBM X-Force Threat Intelligence Index 2018:* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN
4. *Insider Threat – 2018 Statistics:* https://www.uscybersecurity.net/insider-threats-2018-statistics//2018_Global_Cost_of_a_Data_Breach_Report.pdf
5. *Examining the 2018 Cost of a Data Breach:* https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
6. *Tesla's Tough Lesson on Malicious Insider Threats:* https://www.infosecurity-magazine.com/news/teslas-tough-lesson-on-malicious/
7. *The 6 Worst Insider Attacks of 2018 – So Far:* https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d-id/1332183

# セキュリティ問題: 安全でないインターフェースとAPI

クラウドサービス提供者は、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インタフェースやAPIを公開します。一般的なクラウドサービスのセキュリティと可用性は、これらAPIのセキュリティに依存します。

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くぐる偶発的あるいは悪意ある攻撃を防ぐように設計されなければなりません。APIがうまく設計されていないと、使い方を誤ったり、さらに深刻な場合にはデータ漏洩を引き起こすかもしれません。中途半端な、無防備な、あるいは、不法侵入を許すようなAPIにより、いくつかの大規模なデータ漏洩が発生しました。組織は、これらのインターフェースの設計やインターネット上での提供についてのセキュリティ要件を理解しておく必要があります。

APIやユーザインタフェースは、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、おそらく、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す。「フロントドア」として、これらのインターフェースは継続的に攻撃にさらされる可能性が高いです。そのため、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です。

| SECURITY RESPONSIBILITY |
| --- |
| ☒ Customer |
| ☒ Cloud Service Provider |
| ☑ Both |
| **ARCHITECTURE** |
| ☑ Infra |
| ☑ Meta |
| ☒ Info |
| ☑ Appli |
| **CLOUD SERVICE MODEL** |
| ☑ Software as a Service (SaaS) |
| ☑ Platform as a Service (PaaS) |
| ☑ Infrastructure as a Service (IaaS) |

## ビジネスインパクト

大抵のサービス提供者がサービスモデルの中に確実にセキュリティが統合されるよう努力する一方で、これらサービスの利用者にとって、クラウドサービスの利用、管理、連携、監視に関係したセキュリティへの影響を理解することが極めて重要です。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課題に直面します。加えて法的、金銭的影響も非常に重要な場合があります。

## 要点

1. APIを安全な状態に保つ。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うことが挙げられる。
2. 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。
3. 標準的に公開されたAPIフレームワークの利用を検討する（例：Open Cloud Computing Interface (OCCI)，Cloud Infrastructure Management Interface (CIMI)）。

# 想定事例と実例

安全でないインターフェース、APIに関する課題の最近の事例として、以下のものがあります：

- Facebookは、2018年9月28日に5,000万を超えるユーザに影響を及ぼすデータ漏洩があったことを発表しました。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ました。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アカウントの情報が漏れたか、わからないことを認めました。

# CSAガイダンス

Domain 5: 情報ガバナンス
Domain 6: 相互運用性と移植容易性
Domain 9: インシデントレスポンス
Domain 10: アプリケーションセキュリティ
Domain 11: 暗号化と鍵管理
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理（IAM）

# CCM Controls

AIS アプリケーションとインターフェースセキュリティ
AIS-01: アプリケーションセキュリティ
AIS-03: データの完全性
AIS-04: データセキュリティ/完全性

IAM アイデンティティとアクセス管理
IAM-01: 監査ツールアクセス
IAM-07: 第三者アクセス
IAM-08: 信頼された発行元
IAM-09: ユーザアクセス認可
IAM-10: ユーザアクセスレビュー
IAM-11: ユーザアクセス取り消し
IAM-12: ユーザ ID 資格情報
IAM-13: ユーティリティプログラムアクセス

| THREAT ANALYSIS | LINKS AND REFERENCES |
| --- | --- |
| ☒ Spoofing Identity<br>☑ Tampering with Data<br>☑ Repudiation<br>☑ Information Disclosure<br>☒ Denial of Service<br>☑ Elevation of Privilege | 1. *The Treacherous 12: Top Threats to Cloud Computing + Industry Insights:* https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf<br>2. Cloud API security risks: How to assess cloud service provider APIs: https://searchcloudsecurity.techtarget.com/tip/Cloud-API-security-risks-How-to-assess-cloud-service-provider-APIs<br>3. *Insecure API Implementations Threaten Cloud:* https://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550<br>4. *Facebook data breach highlights API vulnerabilities:* https://www.pingidentity.com/en/company/blog/posts/2018/facebook-data-breach-highlights-api-vulnerabilities.html<br>5. *Facebook says at least 50 million users affected by security breach:* https://techcrunch.com/2018/09/28/facebook-says-50-million-accounts-affected-by-account-takeover-bug/<br>6. *Cloud Security Threats - Insecure APIs:* https://community.hpe.com/t5/Shifting-to-Software-Defined/Cloud-Security-Threats-Insecure-APIs/ba-p/6871684#.XBkCEGhKiUl |

# セキュリティ問題: 弱い管理プレーン

データセンターからクラウドへ移行する際は、十分なデータストレージおよびデータ保護計画の作成に課題があります。ユーザは、データの複製、移行、保管の新しいプロセスを開発しなければならず、マルチクラウドを利用する場合はさらに複雑な問題となります。管理プレーンは、実行時のデータとその安定性を提供するデータプレーンを補完してセキュリティと完全性の確保を可能とし、これらの問題の解決策でなければなりません。「弱い管理プレーン」とは、担当者（システムアーキテクトやDevOpsエンジニア）が、データインフラストラクチャのロジック、セキュリティ、および検証を十分に管理できないことを意味しています。このシナリオでは、管理者は、セキュリティ設定、どのようなデータフローか、どこにアーキテクチャの盲点と弱点があるかがわかりません。これらの欠点は、データの破損、使用不能、漏洩を引き起こす可能性があります。

| SECURITY RESPONSIBILITY |
| --- |
| ☑ Customer |
| ☒ Cloud Service Provider |
| ☒ Both |

| ARCHITECTURE |
| --- |
| ☑ Infra |
| ☒ Meta |
| ☒ Info |
| ☒ Appli |

| CLOUD SERVICE MODEL |
| --- |
| ☑ Software as a Service (SaaS) |
| ☑ Platform as a Service (PaaS) |
| ☑ Infrastructure as a Service (IaaS) |

## ビジネスインパクト

「弱い管理プレーン」は、窃取や破損よるデータ損失を引き起こす可能性があります。これは、特に個人データを含むデータ損失の場合に、ビジネスに大きな影響を与えるおそれがあります。さらに、データ損失に対する監督機関の処罰を受けるかもしれません。たとえば、一般データ保護規則（GDPR）では、罰金が2000万ユーロか、世界の売上高の4%に達する可能性があります。

「弱い管理プレーン」では、ユーザはクラウド上のビジネスデータやアプリケーションを保護できず、サービスや提供製品に対する不満や信頼の喪失につながる可能性があります。最終的には、収益の減少となるおそれがあります。

## 要点

1. クラウドカスタマが法的な義務を果たせるよう、CSPによって提供される適切なセキュリティ管理が必要です。
2. クラウド利用者は、デュー・デリジェンスを実施し、利用予定のクラウド サービスが適切な管理プレーンを持っているかどうかを判断する必要があります。

# 想定事例と実例

「弱い管理プレーン」に関連する最近の事例は以下になります：

- クラウドサービスの管理プレーンは非常に重要であり、IDおよびアクセスの管理により適切に保護する必要があります。2要素認証は、CSPによってクラウドユーザに提供される標準的な管理機能のひとつである必要があります。残念ながら、多くのCSPにおいて、利用者は、プレミアムサービスでしか2要素認証を利用できません。このような慣行は、特にこのプレミアムサービスを利用しない、または利用できない者にとって、クラウド利用者のセキュリティ態勢を弱めます。

# CSAガイダンス

Domain 1: クラウドコンピューティングのコンセプトとアーキテクチャ
Domain 5: 情報ガバナンス
Domain 7: インフラストラクチャ・ セキュリティ
Domain 8: 仮想化とコンテナ技術
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理（IAM）

# CCM Controls

AIS アプリケーションとインターフェースセキュリティ
AIS-03: データの完全性
AIS-04: データセキュリティ/完全性

AAC 監査保証とコンプライアンス
AAC-03: 情報システムに関する規制の把握

BCR 事業継続管理と運用レジリエンス
BCR-04: 文書

DSI データセキュリティと情報ライフサイクル管理
DSI-04: 処理 / ラベル付 / セキュリティポリシー

GRM ガバナンスとリスク管理
GRM-01: ベースライン要件
GRM-02: データフォーカスリスクアセスメント
GRM-06: ポリシー
GRM-07: ポリシー適用
GRM-08: リスクアセスメントにおけるポリシーの影響
GRM-09: ポリシーレビュー
GRM-10: リスクアセスメント
GRM-11: リスク管理フレームワーク

IVS インフラと仮想化のセキュリティ
IVS-01: 監査ログ / 侵入検知
IVS-04: 情報システム文書
IVS-06: ネットワークセキュリティ
IVS-09: 区分
IVS-13: ネットワークアーキテクチャ

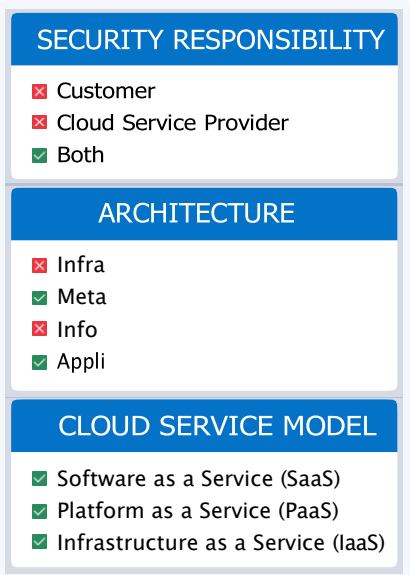
 

| THREAT ANALYSIS | LINKS AND REFERENCES |
| --- | --- |
| ☒ Spoofing Identity<br>☑ Tampering with Data<br>☒ Repudiation<br>☑ Information Disclosure<br>☒ Denial of Service<br>☑ Elevation of Privilege | 1. *Uber fined $148m for failing to notify drivers they had been hacked:* https://www.theguardian.com/technology/2018/sep/26/uber-hack-fine-driver-data-breach<br>2. *Exposed S3 bucket compromises 120 million Brazilian citizens:* https://www.scmagazine.com/home/security-news/exposed-s3-bucket-compromises-120-million-brazilian-citizens/ |

# セキュリティ問題: メタストラクチャとアプリストラクチャの障害

クラウドサービスプロバイダは、運用およびシステムを適切に実装し保護するために必要なセキュリティ保護を定期的に開示します。通常、APIコールでこの情報を開示し、このセキュリティ保護をCSPのメタストラクチャ層に組み込みます。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）と見なされます。




このモデルには複数のレベルで障害の可能性があります。例えば、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あたえます。

利用者に対してクラウドの可視性を高めるために、CSPはしばしばウォーターライン上で、APIとセキュリティプロセスとのやりとりを開示したり許可したりしています。未熟なCSPでは顧客にどうやって、またどの程度までAPIを利用可能とするかが不確かな場合が多いです。例えば、ログを取得したりシステムアクセスを監査することを顧客に許可するようなAPIには、非常にセンシティブな情報が含まれている場合があります。しかしながら、このプロセスはまたテナントが不正アクセスを検知するために必要です。

ウォーターラインより上では、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するためには、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ります。例えば、クラウド環境向けに設計されていないアプリケーションは、利用可能なクラウドのリソースや機能の十分な活用や使用ができません。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、「リフト・アンド・シフト」アプローチを取るだけでは十分ではありません。

## 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す。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ります。同時に、テナントによる設定ミスは、経済的、運用的に、ユーザに非常に大きな影響を与える可能性があります。

## 要点

1. クラウド サービス プロバイダは、テナントに対するクラウド特有の透明性の欠如を解消するため、可視性を提供し、緩和策を提示しなければなりません。
2. クラウドテナントは、クラウドネイティブに設計された適切な機能と制御を実装する必要があります。
3. すべてのCSPはペネトレーションテストを実施し、顧客へ調査結果を提供する必要があります。

## 想定事例と実例

メタストラクチャとアプリストラクチャの最近の障害事例には、次のものがあります：

- 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す。多くの組織は今でもユーザ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無視しています。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めに、Office 365メールサービスの内容を流出しました。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ました。

  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ます。攻撃者はメタストラクチャの資格情報に価値を見出します：Microsoftはクラウドの資格情報を狙った攻撃が年々増加していると警告しています。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倍になりました。2018年の「Microsoft Security Intelligence Report」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」と記載しています。
- 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ました。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ます。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ません。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ます。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と同様の問題があります。

## CSAガイダンス

Domain 1: クラウドコンピューティングのコンセプトとアーキテクチャ
Domain 2: ガバナンスとエンタープライズリスクマネジメント

Domain 4: コンプライアンスと監査マネジメント
Domain 5: 情報ガバナンス
Domain 6: 管理画面 と事業継続
Domain 7: インフラストラクチャ・ セキュリティ
Domain 8: 仮想化とコンテナ技術
Domain 9: インシデントレスポンス
Domain 10: アプリケーションセキュリティ
Domain 11: データセキュリティと暗号化
Domain 12: アイデンティティ管理、権限付与管理、アクセス管理 (IAM)

# CCM Controls

AIS アプリケーションとインターフェースセキュリティ
AIS-01: アプリケーションセキュリティ
AIS-03: データの完全性
AIS-04: データセキュリティ/完全性

AAC 監査保証とコンプライアンス
AAC-01: 監査計画

BCR 事業継続管理と運用レジリエンス
BCR-02: 事業継続テスト
BCR-04: 文書

CCC 変更管理と構成管理
CCC-01: 新規開発及び調達
CCC-05: 業務の変更

DSI データセキュリティと情報ライフサイクル管理
DSI-02: データの管理表とフロー
DSI-03: E コマーストランザクション
DSI-04: 処理 / ラベル付 / セキュリティポリシー
DSI-07: 安全な廃棄

EKM 暗号化と鍵管理
EKM-02: 鍵生成
EKM-03 : 機微データの保護

HRS 人事
HRS-08: 技術的に受け入れられる使用

IAM アイデンティティとアクセス管理
IAM-01: 監査ツールアクセス
IAM-02: 資格証明のライフサイクル / プロビジョニング管理
IAM-04: ポリシーと手順
IAM-05: 職務の分離
IAM-07: 第三者アクセス
IAM-08: 信頼された発行元
IAM-09: ユーザアクセス認可
IAM-10: ユーザアクセスレビュー
IAM-11: ユーザアクセス取り消し
IAM-12: ユーザ ID 資格情報
IAM-13: ユーティリティプログラムアクセス

IVS インフラと仮想化のセキュリティ
IVS-09: 区分

IPY 相互運用性と移植容易性
IPY-01: API

SEF セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス
SEF-04: インシデントレスポンスの法的準備

STA サプライチェーンの管理、透明性、説明責任
STA-03: ネットワーク / インフラストラクチャサービス

## THREAT ANALYSIS

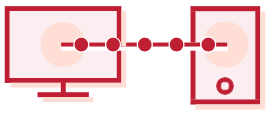
- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

## LINKS AND REFERENCES

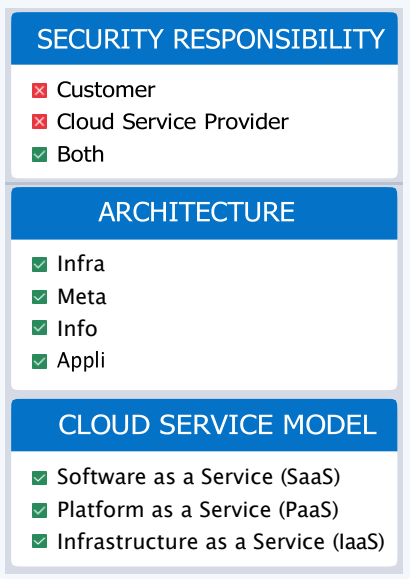

1. *Why Cloud Security Is Everyone's Business:* https://www.gartner.com/smarterwithgartner/why-cloud-security-is-everyones-business/
2. *Source: Deloitte Breach Affected All Company Email, Admin Accounts:* https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/
3. *Deloitte hack hit server containing emails from across US government:* https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government
4. *Deloitte Gets Hacked: What We Know So Far:* http://fortune.com/2017/09/25/deloitte-hack
5. *"Get Off of My Cloud": Cloud Credential Compromise and Exposure:* https://www.defcon.org/images/defcon-19/dc-19-presentations/Feinstein-Jarmoc/DEFCON-19-Feinstein-Jarmoc-Get-Off-of-My-Cloud.pdf
6. *Netflix Cloud Security: Detecting Credential Compromise in AWS:* https://medium.com/netflix-techblog/netflix-cloud-security-detecting-credential-compromise-in-aws-9493d6fd373a
7. *Microsoft Security Intelligence Report:* https://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf
8. *Microsoft warns that hackers are increasingly targeting cloud accounts:* https://www.theinquirer.net/inquirer/news/3016031/microsoft-warns-that-hackers-are-increasingly-targeting-cloud-accounts
9. *Microsoft Security Intelligence Report volume 23 is now availablePoorly secured Cloud Apps:* https://cloudblogs.microsoft.com/microsoftsecure/2018/03/15/microsoft-security-intelligence-report-volume-23-is-now-available/
10. *Understand top trends in the threat landscape:* https://www.microsoft.com/sir
11. *What Is Amazon EC2?:* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/building-shared-amis.htm
12. *Virtual machine prerequisites:* https://docs.microsoft.com/en-us/azure/marketplace/cloud-partner-portal/virtual-machine/cpp-prerequisites
13. *How to Log a Security Event Support Ticket:* https://docs.microsoft.com/en-us/azure/security/azure-security-event-support-ticket
14. *Apple tells app developers to disclose or remove screen recording code:* https://techcrunch.com/2019/02/07/apple-glassbox-apps/
15. *Announcing AWS CloudTrail:* https://aws.amazon.com/about-aws/whats-new/2013/11/13/announcing-aws-cloudtrail/
16. *AWS Discussion Forums - AWS CloudTrail Feature Additions:* https://forums.aws.amazon.com/forum.jspa?forumID=168
17. *AWS Discussion Forums - AWS CloudWatch Feature Aadditions:* https://forums.aws.amazon.com/forum.jspa?forumID=138
18. *Announcing the public preview of Azure Monitor:* https://azure.microsoft.com/en-us/blog/announcing-the-public-preview-of-azure-monitor/
19. *Azure AD Activity Logs in Azure Monitor Diagnostics now in public preview:* https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Activity-Logs-in-Azure-Monitor-Diagnostics-now-in/ba-p/245435

# セキュリティ問題：クラウド利用の可視性の限界



クラウド利用の可視性の限界は、組織内でクラウドサービスの利用が安全か悪質かを視覚化および分析する機能がない場合に生じます。この概念は、2つの主要な課題に分類されます。




許可されていないアプリの使用： これは、従業員が企業のIT部門とセキュリティ部門の明確な許可とサポートのないクラウドアプリケーションとリソースを利用している場合に起きます。このシナリオは、シャドウITと呼ばれる私的利用をもたらします。安全でないクラウドサービスの利用が企業のガイドラインを満たしていない場合、特に企業の機密データを取り扱う場合、この行為は危険です。ガートナーは、2020年までに企業に対するすべてのセキュリティ攻撃の3分の1がシャドウITシステムとリソースを介して発生すると予測しています。

許可されたアプリの悪用： 組織は、多くの場合、許可されたアプリケーションを利用する部内者が、承認されたアプリケーションをどのように活用しているかを分析できません。
多くの場合、これは会社による明示的な許可なしの利用や、資格情報の盗難、SQLインジェクション、DNS攻撃などの方法を使用したサービスを標的とした外部の脅威アクターなどによって起こります。

ほとんどの場合、行動が基準から外れているか、企業のポリシーを順守しているかによって、正当なユーザと不正なユーザを区別することになります。

## ビジネスインパクト

リスクは広範ですが、以下のポイントに要約できます：

- ガバナンスの欠如： 従業員が適切なアクセスとガバナンスの制御をよく知らないと、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置かれることがよくあります。
- 認識の欠如： 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、基本的に知的財産を制御できません。 会社ではなく、従業員がデータを保持します。
- セキュリティの欠如： 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ります。マルウェア、ボットネット、暗号通貨マイニングマルウェアなどは、クラウドコンテナを侵害する可能性があり、組織のデータ、サービス、財務を危険にさらします。

各自の環境での許可されていないクラウド使用の影響について尋ねられたとき、「Oracle and KPMG Cloud Threat Report 2019」で、回答者の50%はこの無許可での使用が 「データへの不正アクセス」につながったと述べ、回答者の48%が 「マルウェアの呼び込み」を挙げたという結果になりました。

## 要点

1. これらのリスクを軽減するには、完全なクラウド可視化の取り組みをトップダウンで開発することから始めます。　このプロセスは通常、組織のクラウドセキュリティアーキテクトに、人、プロセス、技術に結びつく包括的なソリューションの作成を任せることから始まります。　以下に記述するアクションは、このプロセスを開始するのに役立ちます。
2. 承認されたクラウド利用ポリシーと、その実施に関する全社的なトレーニングを義務付けます。
3. 承認されていないすべてのクラウドサービスは、クラウドセキュリティアーキテクトまたはサードパーティのリスク管理者によるレビューと承認が必要です。
4. CASBやSDG（software defined gateway）などのソリューションに投資して、外向けのアクティビティを分析し、リスクのあるユーザによるクラウド利用を発見し、異常を特定するために資格のある従業員の利用行動を追跡します。
5. WAFに投資して、疑わしい傾向、マルウェア、DDoS、ボットネットリスクについてクラウドサービスへのすべてのインバウンド接続を分析します。
6. 主要なエンタープライズクラウドアプリケーション（ERP、人材管理、コマースエクスペリエンス、サプライチェーン管理）をすべて監視、制御し、疑わしい動作を軽減できるように特別に設計されたソリューションを選択します。
7. 組織全体にゼロトラストモデルを実装します。

## 想定事例と実例

クラウド利用の可視性の限界に関連する問題の最近の例には、次のものがあります:

- クラウドセキュリティ企業Lacework社が実施した2018年の調査によると、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おり、クラウドでワークロードを運用する際のリスクを強調しています。
- 「Skyhigh Networks Cloud Adoption & Risk Report Q2 2015」では、企業は現在、平均1,083のクラウドサービスを利用していると報告されています。その驚異的な数字は、昨年の同時期よりもほぼ50%増え、2年前からは最大100%増加してます。
- 「Skyhigh Networks Cloud Adoption & Risk Report Q2 2015」は、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と述べています。簡単に言うと、IT部門には、これらのシャドウITサービスのサービスを選択して展開することをサポートする役割はなく、また、それらが使用されていることすら知らないかもしれません。

# CSAガイダンス

Domain 5: 情報ガバナンス
Domain 11: データセキュリティと暗号化

# CCM Controls

DSI データセキュリティと情報ライフサイクル管理
DSI-01: 分類
DSI-02: データの管理表とフロー
DSI-04: 処理 / ラベル付 / セキュリティポリシー
DSI-06: 所有者/管理責任

EKM 暗号化と鍵管理
EKM-03: 機微データの保護

GRM ガバナンスとリスク管理
GRM-02: データフォーカスリスクアセスメント

HRS 人事
HRS-03: 雇用契約
HRS-07: ロール / 責任
HRS-08: 技術的に受け入れられる使用
HRS-09: 訓練 / 認識向上
HRS-10: ユーザ責任

| THREAT ANALYSIS | LINKS AND REFERENCES |
|---|---|
| ☑ Spoofing Identity<br>☑ Tampering with Data<br>☑ Repudiation<br>☑ Information Disclosure<br>☑ Denial of Service<br>☑ Elevation of Privilege | 1. *22K Open, Vulnerable Containers Found Exposed on the Net:* https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-the-net/132898/<br>2. *Five Ways Shadow IT in the cloud hurts your enterprise:* https://www.networkworld.com/article/2997152/cloud-computing/five-ways-shadow-it-in-the-cloud-hurts-your-enterprise.html<br>3. *Cloud Adoption and Risk Report:* https://info.skyhighnetworks.com/WP-CARR-Q2-2015_Download_White.html?Source=website&LSource=website |

# セキュリティ問題: クラウドサービスの悪用・乱用・不正利用

悪意を企てる者は、クラウドコンピューティングリソースを活用して、利用者、組織、あるいは他のクラウド事業者を標的にします。悪意のある攻撃者は、クラウドサービス上にマルウェアをホストすることもできます。マルウェアをホストするクラウドサービスは、マルウェアがCSPのドメインを利用するため、より正当なものに見えます。そのうえ、クラウドにホストされたマルウェアは、クラウド上でシェアするツールを、さらに自身を増殖させるための攻撃ベクターとして使うことができます。クラウドリソースの悪用例として、他には以下のものがあります:

- 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

| SECURITY RESPONSIBILITY |
| --- |
| ☒ Customer |
| ☒ Cloud Service Provider |
| ☑ Both |
| **ARCHITECTURE** |
| ☑ Infra |
| ☑ Meta |
| ☑ Info |
| ☑ Appli |
| **CLOUD SERVICE MODEL** |
| ☑ Software as a Service (SaaS) |
| ☑ Platform as a Service (PaaS) |
| ☑ Infrastructure as a Service (IaaS) |

クラウドサービスの悪用に対する緩和策としては、CSPによる支払い手段の偽装やクラウドの悪用の検出が挙げられます。CSPは、インシデント対応の仕組みを用意してリソースの悪用に対処しなければなりませんし、クラウド事業者に起因した悪用をクラウド利用者が報告できる手段を提供しなければなりません。クラウド事業者はまた、クラウド利用者が彼らのワークロードや、ファイル共有あるいはストレージサービスの状態を監視できる適切な管理手段も備えなければなりません。

## ビジネスインパクト

もし攻撃者がある顧客のクラウド基盤の管理プレーンに侵入した場合、攻撃者は、その顧客が支払う費用でそのクラウドサービスを違法な目的で利用することができます。もし、その攻撃者が暗号通貨のマイニングのような膨大なリソースを消費した場合、その請求額は膨大になる可能性があります。

あるいは、攻撃者はマルウェアの保存や増殖のためにクラウドを使うかもしれません。企業はそれらの新しい攻撃経路に気づき、適切に対処しなければなりません。このことは、クラウド基盤あるいはクラウドサービスとの間のAPIコールを監視できるセキュリティ技術を調達することを意味するかもしれません。

## 要点

- 企業は、クラウド上の従業員を監視すべきです。従来の仕組みでは、クラウドサービス利用によりもたされるリスクを軽減できません。
- クラウドDLP技術の採用により、許可されないデータ流出の監視と防止ができます。

## 想定事例と実例

クラウドサービスの悪用・乱用・不正利用問題に関する最近の事例として以下のものがあります：

- 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潜在的な被害者の手によってシェアされることで広がります。
- CloudSquirrel攻撃はフィッシングメール攻撃によってもたらされます。この攻撃メールは（"tax invoice"のような）重要に見えるタイトルを使って、被害者をだましてメールを開かせようとします。一度開くと、CloudSquirrelは追加の悪意ある処理を持つ暗号化されたJARファイルをダウンロードさせることによって利用者を感染させます。それからそのマルウェアはDropboxにホストされたC&Cに接続します。それらのコマンドは、.mp4, .wmv, .png, .dat, .wmaなどの偽の拡張子を持つプレーンテキストファイルに偽装されます。

## CSAガイダンス

Domain 6: 管理画面 と事業継続
Domain 7: インフラストラクチャ・ セキュリティ
Domain 9: インシデントレスポンス
Domain 10: アプリケーションセキュリティ

# CCM Controls

**AIS アプリケーションとインターフェースセキュリティ**
AIS-02: 顧客アクセス要求

**BCR 事業継続管理と運用レジリエンス**
BCR-09: 影響解析

**CCC 変更管理と構成管理**
CCC-02: 開発の外部委託

**DSI データセキュリティと情報ライフサイクル管理**
DSI-01: 分類
DSI-02: データの管理表とフロー
DSI-04: 処理 / ラベル付 / セキュリティポリシー

**EKM 暗号化と鍵管理**
EKM-03: 機微データの保護

**GRM ガバナンスとリスク管理**
GRM-01: ベースライン要件

**HRS 人事**
HRS-05: モバイルデバイス管理
HRS-08: 技術的に受け入れられる使用
HRS-09: 訓練 / 認識向上

**IAM アイデンティティとアクセス管理**
IAM-02: 資格証明のライフサイクル / プロビジョニング管理
IAM-04: ポリシーと手順
IAM-05: 職務の分離
IAM-09: ユーザアクセス認可
IAM-10: ユーザアクセスレビュー
IAM-11: ユーザアクセス取り消し
IAM-12: ユーザ ID 資格情報

**IVS インフラと仮想化のセキュリティ**
IVS-01: 監査ログ / 侵入検知
IVS-02: 変更検知
IVS-06: ネットワークセキュリティ
IVS-13: ネットワークアーキテクチャ

**MOS モバイルセキュリティ**
MOS-02: アプリケーションストア
MOS-03: 承認されたアプリケーション
MOS-04: BYOD 用に承認されたソフトウェア
MOS-05: 認知と訓練
MOS-06: クラウドベースサービス
MOS-19: セキュリティパッチ

**TVM 脅威と脆弱性の管理**
TVM-02: 脆弱性 / パッチ管理

## THREAT ANALYSIS

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

## LINKS AND REFERENCES


1. *Malware Used by China APT Group Abuses Dropbox:* http://www.securityweek.com/malware-used-china-apt-group-abuses-dropbox
2. *Zepto variant of Locky ransomware delivered via popular Cloud Storage apps:* https://resources.netskope.com/h/i/273457617-zepto-variant-of-locky-ransomware- delivered-via-popular-cloud-storage-apps
3. *CloudSquirrel Malware Squirrels Away Sensitive User Data Using Popular Cloud Apps:* https://resources.netskope.com/h/i/272453388-cloudsquirrel-malware-squirrels-away- sensitive-user-data-using-popular-cloud-apps
4. *CloudFanta Pops with the Cloud using SugarSync:* https://resources.netskope.com/h/i/295875750-cloudfanta-pops-with-the-cloud-using-sugarsync
5. *Data Theft Via the Cloud: You Don't Need Flash Drives Any More:* https://blog.learningtree.com/data-theft-via-cloud-dont-need-flash-drives/
6. *What Is Cloud DLP?:* https://digitalguardian.com/blog/what-cloud-dlp
7. *Best Practices for Cloud Security:* https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html

# 結論

クラウドのビジネスモデルとセキュリティ戦術が進化するにつれて、このレポートは、データ侵害、設定ミスとアイデンティティ、アクセス管理などの重要なセキュリティ問題に対する認識を高めます。その他の脅威は、クラウド利用の可視性の限界や管理プレーンの弱い管理など、利用者がCSPに対して経験する可能性のある直接管理できないことによる問題を浮き彫りにします。これらの問題は、多くの過去の事例で見られるように、今までの状況を超えたデータ侵害や漏洩につながる可能性があります。

ユーザインタフェースとAPIが、サービスを利用するための現在の方法であることを考えると、これらの機能の安全を保つことは大きな課題であり続けます。

クラウドは、その複雑さとともに、攻撃者にとってはその存在を隠すのに最適な場所でもあります。残念ながら、これは攻撃の理想的な出発点でもあります。最後に重要なことですが、内部者の脅威は、組織をデータ損失から保護することをより困難にします。

これらの落とし穴はすべて、より多くの業界の注意と研究を必要とします。

この*Top Threats in Cloud Computing*レポートは、クラウドセキュリティに関して興味深くかつやや新しい視点を提案しています。この新しい見方は、構成と認証に焦点を当て、情報セキュリティに対する従来の焦点（脆弱性やマルウェアなど）からシフトしています。言うまでもなく、これらのセキュリティ問題は、クラウドセキュリティの認識、設定、構成、ID管理を開発および強化するための行動を促す呼びかけになります。

# Appendix: 調査方法

*Egregious 11: Cloud Computing Top Threats in 2019*レポートとして、CSA の*Top Threats Working Group*は二段階の主要な調査を行いました。どちらの調査も、手法としてアンケート調査と質問を用いました。

調査の第一段階における我々の狙いは、クラウドセキュリティに関する懸念事項について、簡単なリストを作ることにありました。最初に、昨年の12 の問題に新たに14 の問題を加えて、セキュリティの懸念事項26 件のリストを作成しました。その26 の懸念事項について、ワーキンググループのメンバーが各々の所属先でその重要性を示し、状況の聞き取りを行いました。調査のこの段階では、調査対象企業が26 件のリスト以外の追加の懸念事項を述べることもできるようにしました。調査結果と追加で得られた情報を総合的に検討して、ワーキンググループ は特筆すべき19 のクラウドセキュリティに関する懸念事項を抽出しました。

調査の第二段階では、19のリストに対して重要性の観点からランク付けすることが主な目標となりました。このグループ は、調査によって、セキュリティの専門家が何を最も関心のあるセキュリティの懸念事項と考えているかを把握しようとしました。手法として10ポイントのスライド制を用いることとしました。回答者は、クラウドセキュリティの問題に対して、1から10で評価することが指示されました。1は全く重要でない、10は非常に重要となります。それぞれのカテゴリーごとのポイントは平均化され、この平均値によってセキュリティの懸念事項がランク付けされました。ワーキンググループでは、平均が7より低いすべてのセキュリティ問題を除外して、トップ11を絞りこみました。

最後に、ワーキンググループ は、また、STRIDE脅威モデルによりセキュリティの懸念事項の分析を行いました。この方式はマイクロソフトにより開発され、セキュリティ脅威を評価するのに用いられています。本書で取り上げたセキュリティの懸念事項が、以下の脅威のカテゴリーのどれかに当てはまるかを評価するのに用いられました：

- なりすまし：Spoofing identity (S)
- データの改ざん：Tampering with data (T)
- 否認：Repudiation (R)
- 情報漏洩：Information Disclosure(I)
- サービス拒否：Denial of service (D)
- 特権の昇格：Elevation of privilege (E)