クラウドコンピューティングに対する重大な脅威2024

CSAJC cloud security alliance Japan Chapter

· PRESS START ·

CSA cloud security alliance®

The permanent and official location for Cloud Security Alliance Top Threats research:
https://cloudsecurityalliance.org/research/working-groups/top-threats/

Acknowledgments

Co-chairs

Jon-Michael Brook
Alex Getsin
Vic Hargrave
Michael
Roza

Contributors

Jon-Michael Brook
Randall Brooks
Alex Getsin
Vic Hargrave
Laura
Kenner
Michael Morgenstern
Stephen Pieraldi
Michael Roza

Reviewers

Vishnu Guttha
Yuvaraj
Madheswaran
Nishith Sinha

CSA Global Staff

Sean Heide
Claire Lehnert
Stephen Lumpe

日本語版提供に際しての告知及び注意事項

本書「クラウドコンピューティングに対する重大な脅威2024」は、Cloud Security Alliance (CSA)が公開している「Top Threats to Cloud Computing 2024」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
2024年12月09日	日本語版1.0	初版発行

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。
(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．　原典がある場合の制限事項等
本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５．　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。

日本語版作成に際しての謝辞

「クラウドコンピューティングに対する重大な脅威2024」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）

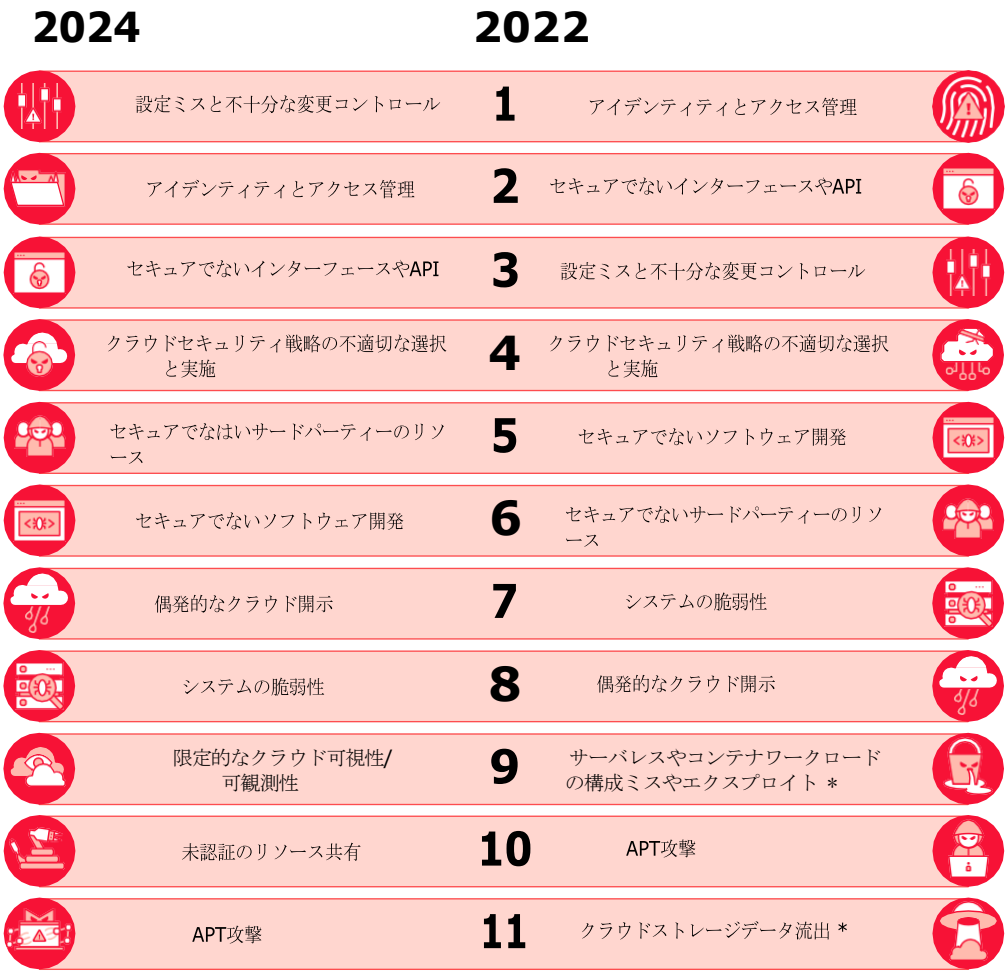
石井　英男
木村　チエ
高橋　久緒
松浦　一郎, CISSP, CISM, CDPSE
松崎　祥三
満田　淳
村田　紗矢子
諸角　昌宏
米山　努
渡邉　浩一郎 CISSP, CISA, CEH

目次

エグゼクティブサマリ

この重大脅威レポートは、クラウドの脅威、脆弱性、およびリスクに対する意識向上を目的としています。今回は、クラウド業界のセキュリティ課題について、500人以上の業界専門家を対象に調査を行いました。回答者は、今年のクラウド環境における11の重要なセキュリティ課題を特定しました。*Top Threats Working Group*は、調査結果と専門知識を活用して*「クラウドコンピューティングに対する重大脅威2024」*レポートを作成しました。

最新のレポートでは、2024年の*重大脅威*（10ページの調査による重要度の高い順にランク付け）を紹介しています。このサーベイは2024年と2022年の調査順位も示しています。



**2024年のトップ11に含まれないセキュリティ課題*

考察

調査分析では、クラウドサービスプロバイダ（CSP）の責任である従来のクラウドセキュリティの課題に関する順位が下がり続けていることを示します。前回のレポートで取り上げたサービス妨害、共有技術の脆弱性、CSP でのデータ損失などの懸念は、今回のレポートでは除外されるほど低い評価となりました。これらの除外は、クラウドへの明らかな信頼を裏付けています。

IaaS（Infrastructure as a Service）環境における昔ながらのセキュリティ課題は、それほど懸念されるものではありません。また、クラウドセキュリティの懸念事項として、データ侵害はもはや上位を占めていないことも観測しました。

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中、本レポートは次のような重要なセキュリティ課題に対する認識を深めることができます。

> - 設定ミスと不十分な変更管理
> - アイデンティティとアクセス管理（IAM）
> - セキュアでないインターフェースやAPI
> - クラウドセキュリティのアーキテクチャと戦略の欠如

設定ミスと不十分な変更管理：2024年版「*重大脅威*」調査では、2022年版レポートの3位から1位にランクアップしました。構成管理は、何十年もの間、組織能力の成熟度の礎となってきました。しかし、クラウドコンピューティングへの移行によって課題はさらに深刻化し、チームはより堅牢なクラウド固有の構成を採用することが極めて重要になっています。クラウドの永続的なネットワークアクセスと無限のキャパシティを考えると、設定ミスは組織全体に広範囲な影響を及ぼす可能性があります。

アイデンティティとアクセス管理（IAM）：これまで1位だったIAMが2位になりました。リプレイ攻撃、なりすまし、および過剰な権限などの課題は、オンプレミスのセットアップと同様にクラウド環境でも存続します。しかし、自己署名証明書の使用への移行や不十分な暗号管理は、重大なセキュリティ上の懸念を引き起こします。ゼロトラストアーキテクチャとSDP（Software-Defined Perimeters）の実装に焦点を置いているのは、調査回答者の優先事項の中でこれらの課題が際立っていることを反映しています。

セキュアでないインターフェースやAPI：2位から3位に移動したことは、マイクロサービスの採用が、インターフェースとAPIのセキュリティ確保の上で重要であることを反映しています。SaaSやPaaSを含むクラウドサービスにおいて、これらの要素は極めて重要な役割を担っているにもかかわらず、コード作成者の非効率性やクラウドの常時稼働の性質から、これらの要素のセキュリティの確保には大きな課題が残されています。

不十分なクラウドセキュリティ戦略：このエリアは4位にとどまりましたが、引き続き疑問を投げかけています：セキュリティソリューションの計画やアーキテクチャに大きな課題が残るのはなぜでしょうか？クラウドコンピューティングは、もはや目新しいものではなく、明確に定義され、実行されるアーキテクチャ戦略が必要となっています。

対象読者

クラウドとセキュリティの実務家や熱狂者は、クラウドセキュリティの脅威と課題、それらが業界に与える影響、そしてその影響を軽減するために何ができるかについて、最新の貴重な洞察を得るために本レポートを活用することができます。最終的に、このサーベイに基づく研究は、コンプライアンス、リスク、技術スタッフ、および経営陣に、現状に関する技術動向と優先度の高いクラウドセキュリティの考慮事項を提供するものです。

調査

CSA *Top Threats Working Group* は、"クラウドコンピューティングに対する重大脅威2024" 調査レポートを作成するにあたり、2 段階の調査を実施しました。それぞれの段階では、2024年の*重大脅威*を特定することを最終目標として、クラウドコンピューティングに最も関連する脅威、脆弱性、およびセキュリティ課題のリスクに関するサイバーセキュリティ専門家の考えや意見を収集するための調査を実施しました。

最初の調査段階では、ワーキンググループのメンバーを対象とした対面調査を通じて、クラウドセキュリティの課題を絞り込んだリストを作成することを目指しました。まず、前回の報告書「クラウドコンピューティングの重大脅威 - パンデミックイレブン」の*重大脅威*（セキュリティ課題）からスタートし、ディスカッションを通じて19の課題を追加しました。その後、ワーキンググループのメンバーに、それぞれの組織にとっての各問題の重要度や、自分たちの身近な組織についての知識を示してもらいながら、30項目の課題の検討を重ねました。その結果、サーベイでは28の課題が提示されました。

調査の第2段階では、500人以上のセキュリティ専門家を対象としたオンライン調査によって、28のセキュリティ課題リストの重要度をランク付けすることを主な目的としました。各課題の重要性を反映させるため、10段階のスライディングスケールを選択しました。調査参加者は、クラウドセキュリティの各課題を1から10の尺度で評価するよう指示され、1は "あまり重要でない"、10は "最も重要である "としました。各カテゴリーのポイントを合計し、平均化しました。そして、その平均値を用いて、セキュリティ課題をランク付けしました。結果、ワーキンググループが導き出したのものが、以下の「11の重大脅威」です。

サーベイ順位	サーベイスコア	課題名称
1	8.282331	設定ミスと不適切な変更管理
2	8.070780	アイデンティティとアクセス管理（IAM）
3	7.987272	セキュアでないインターフェースやAPI
4	7.620689	クラウドセキュリティ戦略の不適切な選択と実施
5	7.582061	セキュアでないサードパーティーリソース
6	7.545801	セキュアでないソフトウェア開発
7	7.506641	偶発的なクラウドデータ公開
8	7.462794	システムの脆弱性
9	7.389799	限定的なクラウド可視性/可観測性
10	7.379310	未認証のリソース共有
11	7.364326	APT攻撃

11の 重大脅威 を特定した後、ワーキンググループは各課題を分析しました。各分析では、課題、ビジネスインパクト、要点、想定事例、および実例に加え、CSA の「Security Guidance for Critical Areas of Focus in Cloud Computing v5」domain guidesの該当セクションや、CSA の「Cloud Controls Matrix（CCM）」および「CAIQ v4controls」の関連する緩和策について説明しています。最後に、全体的な手法は、CSA の「Certificate of Cloud Auditing Knowledge Study Guide v1」に示されている「Top Threats」の手法を表すものです。

セキュリティ課題１：設定ミスと不適切な変更管理

設定ミスとは、クラウドコンピューティング資産の誤った、または最適とは言えない設定のことで、意図しない損害や外部/内部の悪意ある活動に対して脆弱な状態になる可能性があります。クラウドシステムに関する知識が不足していたり、クラウドのセキュリティ設定や悪意に対する理解が不足していたりすると、誤った設定が行われる可能性があります。よくある設定ミス[1]には、次のようなものがあります：1. シークレット管理、2. 無効化された監視とロギング、3.ICMPがオープンなままになっている、4.セキュアでない自動バックアップ、5.ストレージへのアクセス、6.バリデーションの欠如、7.HTTPS/HTTPポート以外への無制限のアクセス、8.仮想マシン、コンテナ、およびホストへの過度に寛容なアクセス、9.多すぎるクラウドアクセス権限（最小特権）の有効化、10.サブドメインのハイジャック（別名ダングリングDNS）、11.AWS S3バケットのような使用中のクラウドプロバイダーに特有の設定ミス。クラウドリソースの設定ミスは、以下のビジネスインパクトのセクションで示すように、深刻な被害をもたらす可能性があります。 [2]

クラウド環境における不十分な変更管理により、不適切な設定が検出されないまま放置され、重大なセキュリティリスクをもたらす可能性があります。クラウド環境は従来のITインフラストラクチャと大きく異なるため、変更管理がより困難になります。従来の変更プロセスでは、複数の役割と承認が必要であり、本番環境に到達するまでに数日から数週間を要することがよくありました。一方、クラウドコンピューティングの方法論では、自動化、幅広いアクセス、および迅速な変更を重視し、多くの場合、静的なインフラストラクチャ要素をコードに抽象化します。さらに、複数のクラウドプロバイダーを利用すると、それぞれのプロバイダー独自の機能や頻繁な更新により、さらに複雑さが増します。このようなダイナミックな環境では、変更管理と是正に対する機敏で積極的なアプローチが必要であり、多くの企業がこれを習得しようとしています。

ビジネスインパクト

管理の影響は、その設定ミス／不適切な変更の内容や、どのくらいすぐにそれを発見し緩和できるかによって、深刻なものとなる可能性があります。クラウドの設定ミスや不十分な変更によって生じる可能性のある影響を以下に示します：

技術的な影響：

- *データの開示：*機微データへの未認可なクラウドアクセスは機密性を損ないます。
- *データの損失：*クラウドシステムから重要なデータが永久的または一時的に消去されると、可用性に影響します。
- *データの破棄：*クラウドシステムのデータに対する物理的または論理的なダメージは、完全性を危険にさらします。

運用上の影響:

- *システムパフォーマンス：*クラウドリソースのパフォーマンス低下は、ユーザエクスペリエンスと生産性に影響を与えます。
- *システム停止：*クラウドサービスの完全または部分的なシャットダウンにより、業務に支障をきたします。

財務的影響：

- *身代金の要求：*侵害されたクラウドデータまたはシステムへのアクセスを復元するために支払いが必要となる場合があります。
- *コンプライアンス違反と罰金：*規制要件を順守しなかった場合、罰金や罰則が科される可能性があります。
- *収入の損失：*クラウドサービスの障害、顧客の不満、または法的措置により、財務上の損失が発生する可能性があります。
- *株価の下落：*違反や暴露は、市場の認識や企業の評価にダメージを与える可能性があります。

風評被害：

- *会社の評判：*違反や暴露は、組織の社会的イメージやブランド価値を損なう可能性があります。

要点

1. クラウド構成のモニタリング、監査、評価- [3]:機械学習を活用することで、企業はクラウドシステムのセキュリティ設定ミスの定期的な検出を自動化し、手作業による検査/監査/評価への依存を減らして効率を高めることができます。
2. クラウドシステム、変更管理アプローチ- [4]:継続的なビジネス変革やセキュリティ課題の終わりがなく、動的な性質は、承認された変更がリアルタイムの自動検証を使用して適切に行われることを求めます。

想定事例と実例

設定ミスと不適切な変更管理による最近のインシデントには以下があります。

- **(2023年5月)** トヨタ自動車株式会社が、日本国内の約215万人のユーザーに影響を及ぼす重大な車両情報漏えいを認めたとの報道がありました。対象となるユーザーは、トヨタの主要なクラウドサービスプラットフォームである T-Connectを契約しているほぼすべての顧客層、 およびレクサス車オーナー向けの類似サービスであるG-Linkのユーザーでした。データの公開期間は2013年11月から2023年4月中旬までの10年間でした。この情報漏洩の原因は人為的ミスによるものでした。流出したデータには、車両の位置や識別番号などの詳細が含まれていましたが、悪用されたという報告はありません。トヨタ自動車は、本インシデントを受け、外部からのデータへのアクセスを遮断する措置を講じました。トヨタコネクティッド株式会社が管理するすべてのクラウド環境について調査を開始しました。さらに、クラウドの設定を監査するシステムの導入、継続的な監視手順の確立、データの取り扱いルールに関する従業員への包括的なトレーニングの実施に取り組んでいます。 [5]
- **(2023年9月)** マネージドクラウドサービスプロバイダーでありデジタルリスク保護企業であるDarkBeam社が、ElasticsearchとKibanaのインターフェースを不注意に無防備な状態にし、報告済および未報告のデータ侵害の記録を漏えいさせていたことが報告されました。流出した（ダウンロードされた）データには、ユーザーの電子メールとパスワードが含まれ、合計38億件以上にのぼります。DarkBeam社は、データ侵害が発生した場合に顧客へ警告するために、この情報を収集していました。このインシデントは、DarkBeamユーザー以外にも影響を与える可能性があります。漏洩は9月18日に発見され、報告後すぐにクローズされました。データ漏洩は、メンテナンス後にインスタンスをパスワードで保護することを忘れるなど、人為的なミスによって発生することがよくあります。流出したデータの中には、"email 0-9 "と "email A-F "と名付けられた16のコレクションがあり、それぞれに239,635,000件のレコードが含まれていました。このように広範かつ体系的にまとめられたデータの公開は、クレデンシャルが開示された個人にとって重大な脅威となります。脅威アクターは、個人情報を使用したフィッシングキャンペーンで影響を受けたユーザーを標的にする可能性があります。ユーザーは、オンラインアカウント全体のパスワードを変更し、強力なパスワードジェネレータを使用し、アカウントを保護するために二要素認証を有効にする必要があります。[6]

CSA 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

ドメイン 2: クラウドガバナンス
ドメイン 3: リスク、監査、コンプライアンス
ドメイン 5: アイデンティティとアクセスの管理
ドメイン 7: インフラストラクチャとネットワーク
ドメイン 9: データセキュリティ
ドメイン 10: アプリケーションセキュリティ
ドメイン 11: インシデントレスポンスとレジリエンス

CSA CCM Controls Version 4.0

A&A 監査・保証
A&A-02:独立した評価
A&A-03:リスクベースの計画評価

AIS アプリケーションとインターフェースのセキュリティ
AIS-02:アプリケーションセキュリティのベースライン要件
AIS-04:セキュアアプリケーションの設計と開発
AIS-05:自動化されたアプリケーションセキュリティテスト

BCR 事業継続管理とオペレーショナルレジリエンス
BCR-02:リスク評価と影響分析
BCR-08:バックアップ

CCC 変更管理と構成管理
CCC-02:品質テスト
CCC-04:承認されていない変更からの保護
CCC-09:変更の復元

CEK 暗号技術、暗号化、鍵管理
CEK-03:データ暗号化
CEK-05:暗号化の変更管理

DSP データセキュリティとプライバシーライフサイクル管理
DSP-07:デザイン段階からのデータ保護とデフォルト設定
DSP-08:データプライバシー・バイ・デザインとデフォルト構成
DSP-17:機微なデータの保護

GRC ガバナンス、リスク管理、コンプライアンス
GRC-02:リスク管理プログラム
GRC-05:情報セキュリティプログラム

HRS 人的リソース
HRS-09:人員の役割と責任
HRS-11:セキュリティ教育・啓発

IAM アイデンティティとアクセスの管理
IAM-03:アイデンティティ・インベントリ
IAM-08:ユーザー アクセスのレビュー

IVS インフラストラクチャと仮想化のセキュリティ
IVS-02:容量と資源の計画
IVS-03:ネットワークセキュリティ
IVS-04:OSのハードニングとベースコントロール

LOG ロギング&モニタリング
LOG-03:セキュリティモニタリングおよびアラート
LOG-05:監査ログのモニタリングとレスポンス
LOG-12:アクセスコントロールログ

SEF セキュリティインシデント管理、Eディスカバリ、およびクラウドフォレンジック
SEF-03:インシデントレスポンス計画
SEF-04:インシデント対応テスト
SEF-06:イベントのトリアージプロセス

TVM 脅威と脆弱性の管理
TVM-07:脆弱性の特定
TVM-08:脆弱性の優先順位付け
TVM-09:脆弱性管理レポート

参照文献

1. Common Cloud Misconfigurations and How to Avoid Them
   https://www.upguard.com/blog/cloud-misconfiguration
2. 13 Most Common Misconfigurations on the Cloud
   https://www.clouddefense.ai/common-misconfigurations-on-the-cloud/
3. Safeguarding Against Security Misconfigurations with the Power of Machine Learning
   https://securityboulevard.com/2023/11/safeguarding-against-security-misconfigurations-with-the-power-of-machine-learning/
4. Change execution monitoring
   https://www.versio.io/solution-change-request-management.html
5. More than 2 million Toyota users face the risk of vehicle data leak in Japan
   https://www.reuters.com/business/autos-transportation/toyota-flags-possible-leak-more-than-2-mln-users-vehicle-data-japan-2023-05-12/?ref=thestack.technology
   Apology & Notice Concerning Newly Discovered Potential Data Leakage of Customer Info Due to Cloud Settings
   https://global.toyota/en/newsroom/corporate/39241625.html
   Yet Another Toyota Cloud Data Breach Jeopardizes Thousands of Customers
   https://www.darkreading.com/ics-ot-security/toyota-cloud-data-breach-jeopardizes-thousands-customers
   Toyota spewed vehicle location data for millions onto unsecured cloud databases for 10 years
   https://www.thestack.technology/toyota-data-breach-2023-t-connect-cloud/
6. DarkBeam leaks billions of email and password combinations
   https://securityaffairs.com/151566/security/darkbeam-data-leak
   DarkBeam's Alarming Data Breach Exposes 3.8 Billion Records
   https://techreport.com/news/darkbeams-alarming-data-breach-exposes-3-8-billion-records/
   More than 3.8 billion records exposed in DarkBeam data leak
   https://www.cshub.com/data/news/darkbeam-data-leak

セキュリティ課題2：アイデンティティとアクセス管理(IAM)

アイデンティティとアクセス管理（IAM）は、個人が本人であることを証明した上で、許可（認可）されたリソースにのみアクセスできるようにします。このシステムは、ユーザーの役割、アクセス権限、およびこれらの権限が割当られ、取消される具体的な条件を、定義し管理する上で極めて重要です。IAMはその重要な役割にもかかわらず、その複雑さとサイバー脅威の進化する性質のために、サイバーセキュリティにおいて継続的な課題をもたらしています。ユーザー認証、認可、シングルサインオン（SSO）、多要素認証（MFA）、およびアクティビティモニタリングなどの主要コンポーネントは、IAMの有効性に不可欠です。しかし、これらの機能の複雑さとダイナミズムは、正しく実装、設定、更新、監視されていない場合には特に、脆弱性を招く可能性があります。サイバー脅威が高度化するにつれて、不正アクセスから機微情報を保護することはますます困難になっており、サイバーセキュリティ防御を強化するために不可欠なIAM戦略の堅牢な導入と継続的な改善をさせています。

クラウド環境におけるアイデンティティとアクセスの管理は、複雑でリスクが高い場合があります。クラウドプロバイダーによってシステムが異なるため、ミスやセキュリティギャップにつながる可能性があります。ユーザーがアカウントやリソースを自ら作成・管理できる場合、過剰な権限付与や誤った設定により、セキュリティリスクが高まる可能性があります。各ベンダーは、それぞれ異なるIAMフレームワークと、微妙な違いを持つ、きめ細かいパーミッションを採用しています。複数のシステムに対する深い理解と管理戦略がなければ、設定ミスやセキュリティポリシーの一貫性の欠如といったリスクは重大なものとなります。一元化されたIAMシステムの監視により、課題対応は容易になりますが、ポリシーの一貫性を欠くと、セキュリティ対策はさらに複雑になります。クラウドリソースの動的な性質、例えば短命なリソースや自動スケーリングなどは、管理を複雑にします。クラウドとオンプレミスシステムの統合は難しい場合があります。特にハイブリッド環境やシングルサインオンが必要な場合はなおさらです。さまざまな規制への対応もハードルのひとつです。

これらのリスクを軽減するには、1.シングルサインオンやフィッシングに強い多要素認証（MFA）などの強固な認証を備えた統合IAMソリューションの採用、2.最小特権の原則の徹底、3.プロビジョニングとプロビジョニング解除プロセスの自動化、4.アクティビティモニタリングの実施、5.ユーザーと管理者に対する継続的なトレーニングと意識向上プログラムの提供などが必要です。IAM戦略の適切な導入と継続的な改善により、機微情報を保護し、サイバーセキュリティ防御の有効性を維持します。

ビジネスインパクト

不十分なアイデンティティとアクセス管理（IAM）は、不正アクセス、データ漏洩、法規制の違反につながり、財務上および評判に大きなダメージを与えます。効果的なIAM戦略は、機微情報を保護し、堅牢なサイバーセキュリティ防御を維持するために不可欠です。

技術的な影響

- *システムへのアクセス：*認証が弱いと、バックエンドシステムから機密データを搾取される可能性があります。
- *データの漏洩：*通信の脆弱性、システムへのアクセス、またはクレデンシャルの再利用により、外部の第三者が業務データにアクセスする可能性があります。
- *データ損失：*MOVEitのキャンペーンは、流出したデータを身代金交渉の際にどのように活用できるかを示しています。

運用上の影響:

- *システム停止：*クラウドサービスの完全または部分的なシャットダウンは、業務に支障をきたす可能性があります。
- *機能遅延：*ソフトウェアの悪用に対処する必要があるため、機能アップデートが遅れることがあります。

財務的影響：

- *収入の損失：*サービスの中断、サービスの復旧、顧客の不満、または法的措置により、財務上の損失が発生する可能性があります。
- *コンプライアンス違反：*アイデンティティおよびアクセス制御の安全性を十分に確保できないと、GDPR、CCPA、PCI DSSのような業界固有の規制などの規制要件に準拠しなくなる可能性があります。規制違反は多額の罰金や法的措置につながる可能性があります。

風評被害：

- *会社の評判：*クラウドサービス組織の社会的イメージ、ビジネス、ブランド価値の毀損。
- *クライアントの評判：*セキュリティが脆弱なAPIクラウドサービスに依存しているクライアントは、データ漏洩やサービスの中断に見舞われ、評判に悪影響を及ぼす可能性があります。

要点

- **IAM ソリューションの統合：**強固な認証、一元管理、複数のクラウドプロバイダーにわたる可視性を提供するIAMソリューションを使用します。
- **最小特権の原則の遵守：**ユーザーが各自のタスクを実行するために必要なアクセス権のみを持つようにします。影響範囲を制御することで、潜在的な侵害を軽減することができます。
- **プロビジョニングとプロビジョニング解除の自動化：**アカウントと権限のライフサイクルを管理する自動化ツールを導入し、タイムリーな更新と不要なアクセスの削除を確実にします。
- **アクセス評価とモニタリング：**アカウントと権限のライフサイクルを管理する自動化ツールを導入し、タイムリーな更新と不要なアクセスの削除を確実にします。継続的なセキュリティモニタリングにより、不正アクセスを検知、警告、および防止するツールを導入します。

想定事例と実例

このセキュリティ課題のクラウドインシデントの最近の事例を紹介します。

- **(2023年5月）MOVEitキャンペーン：**ファイル転送ツール「MOVEit」に関連した一連の情報漏えいは、政府機関や医療機関を含む複数の組織に影響を与えました。例えば、オレゴン州運輸局では、約350万人に影響を及ぼす情報漏洩が発生しました。攻撃者は、過剰に権限が許可されたアカウントと職務分掌の不備により、機微な個人情報にアクセスしました。アカウントの侵害に起因するトラフィックを捕捉するには、堅牢なロギング、監査、およびトラフィックベースの異常検知が必要です。これらの事件は、サイバー犯罪者が被害者に対し、盗まれたデータの復号ではなく、その公開を阻止するために金銭を支払うよう圧力をかける、データ強要攻撃の新たな傾向を浮き彫りにしています。 [1]
- **(2023年6月）JumpCloudのデータ流出：**アイデンティティおよびアクセス管理企業のJumpCloudは、巧妙な国家主体の攻撃者による侵害に遭いました。この攻撃は、JumpCloudのコマンドフレームワークにデータをインジェクトする手段で、特定の顧客アカウントを標的としていました。この情報漏えいは当初、スピアフィッシング・キャンペーンと有効期限のないクレデンシャルが原因であったことが判明し、高度なサイバー攻撃に関連するリスクと、クレデンシャル強度のレビュー、強制的なタイムリセット、およびログレビューなどの強固なセキュリティ対策の重要性が強調されました。[2]
- **(2023年10月）Oktaデータ流出：**アイデンティティサービスと認証管理のプロバイダーであるOktaは、権限のない行為者が盗んだクレデンシャルを使ってサポートケース管理システムにアクセスするというデータ侵害を経験しました。このインシデントにより、カスタマーサポートのケース情報が漏洩し、サービスアカウントや機密情報をアクセス可能なシステム内に保管することのリスクが浮き彫りになりました。継続的なモニタリングとシステマティックレビューのプロセスが重要です。[3]

CSA 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

ドメイン2: クラウドガバナンス
ドメイン3: リスク、監査、コンプライアンス
ドメイン5: アイデンティティとアクセス管理
ドメイン6: セキュリティモニタリング
ドメイン 9: データセキュリティ
ドメイン10: アプリケーションセキュリティ
ドメイン12: 関連技術と戦略

AIS アプリケーションとインターフェースのセキュリティ

AIS-01:アプリケーションとインターフェースのセキュリティポリシーと手順
AIS-02:アプリケーションセキュリティのベースライン要件
AIS-03:アプリケーションセキュリティ・メトリクス

CCC 変更コントロールと構成管理

CCC-07:ベースラインからの逸脱の検出
CCC-08:例外管理

DSP データセキュリティとプライバシーライフサイクル管理

DSP-03:データインベントリ
DSP-04:データ分類
DSP-07:デザイン段階からのデータ保護とデフォルト設定
DSP-17:機微なデータの保護
DSP-19:データの所在地

GRC ガバナンス、リスク管理、コンプライアンス

GRC-02:リスク管理プログラム
GRC-05:情報セキュリティプログラム
GRC-06:ガバナンス責任モデル

IAM アイデンティティとアクセスの管理

IAM-01:アイデンティティおよびアクセス管理ポリシーと手順
IAM-03:アイデンティティ・インベントリ
IAM-05:最小権限
IAM-08:ユーザー アクセスのレビュー

LOG ロギング&モニタリング

LOG-10:暗号に関するモニタリングとレポート

IVS インフラストラクチャと仮想化のセキュリティ

IVS-03:ネットワークセキュリティ
IVS-06:分割と分離

TVM 脅威と脆弱性の管理

TVM-08:脆弱性の優先順位付け

参考文献

1. MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023 https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business
2. JumpCloud: June 20 Incident Details and Remediation https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation
3. Okta hit by third-party data breach exposing employee information https://www.bleepingcomputer.com/news/security/okta-hit-by-third-party-data-breach-exposing-employee-information/
4. The 10 Biggest Data Breaches of 2023 (so far) https://www.crn.com/news/security/the-10-biggest-data-breaches-of-2023-so-far
5. DOJ-Collected Information Exposed in Data Breach Affecting 340,000 https://www.securityweek.com/doj-collected-information-exposed-in-data-breach-affecting-340000/

セキュリティ課題3：セキュアでないインターフェースやAPI

クラウドサービスプロバイダー（CSP）、企業ベンダー、社内開発者は、通常、システム制御のために、マシン間のアプリケーションプログラミングインターフェース（API）、またはヒューマンユーザーインターフェース（UI）の包括的なスイートを提供しています。 初期の設計要件が長期的な利用時とは一致しないことはよくあります。リーダーシップの変更、企業戦略の方向性、またはサードパーティパートナーによるアクセスにより、配備に追われることになります。以前の決定、文書化されていない仮定、レガシーサポート要件、不十分なアーキテクチャ設計、またはオンプレミス/IaaS/SaaS製品が同じであるとの同等性への期待は 、企業のクラウドへの継続的な移行に影響を与えます。

APIやUIが脆弱になる理由は様々です：1.不十分な認証メカニズム、2.暗号化の欠如、3.不適切なセッション管理、4.不十分な入力検証、5.不十分なロギングとモニタリング、6.古い、またはパッチが適用されていないソフトウェア、7.クラウド移行時の保護が同等との仮定、8.過度に寛容なアクセス制御、9.レート制限の欠如。Akamai 2024 のレポートによると、「12カ月間（2023年1月から12月まで）にウェブ攻撃の 29% が API を標的としたものであり、API がサイバー犯罪者の重点分野であることを示している」とのことです。[1] ヒューマンポータルの認証方法には、脆弱なパスワードや再利用されたパスワードなど、容易に漏洩するリスクがあります。攻撃者はこれらの脆弱性を悪用し、不正アクセス、機密データの窃取、サービスの中断などの影響を与える可能性があります。2023年、OWASPはインターフェースのセキュリティの重要性を指摘し、人気のあるウェブリストに新しいAPIセキュリティトップ10を追加しました。 [2]

ビジネスインパクト

クラウドシステムにおけるセキュアでないインターフェースの影響は、システムの性質や、その他の安全対策や緩和策の有無によって、深刻な結果を招く可能性があります。セキュアでないインターフェースやAPIのリスクは、APIに関連する使用法やデータ、脆弱性の検出と緩和の速さによって異なります。最も多く報告されているビジネスへの影響は、APIによって保護されないまま放置された機微データや個人データの意図しない露出です。セキュアでないインターフェースがもたらす影響を検討する際には、以下を考慮してください：

技術的な影響：

- *システムへのアクセス：*認証が不十分な場合、バックエンドシステムが悪用される可能性があります。
- *データの漏洩：*通信の脆弱性、システムへのアクセス、またはクレデンシャルの再利用により、外部の第三者が業務データにアクセスする可能性があります。

運用上の影響:

- *システム停止：*クラウドサービスの完全または部分的なシャットダウンは、業務に支障をきたす可能性があります。
- *機能遅延：*ソフトウェアの悪用に対応する必要があるため、機能アップデートが遅れることがあります。

財務的影響：

- *収入の損失：*サービスの中断、サービスの復旧、顧客の不満、または法的措置により、財務上の損失が発生する可能性があります。
- *コンプライアンス違反と罰金：*脆弱性管理に関する規制要件を遵守しなかった場合、罰則の対象となる可能性があります。

風評被害：

- *会社の評判：*クラウドサービス組織の公共イメージとブランド価値の毀損。
- *クライアントの評判：*セキュリティが脆弱なAPIクラウドサービスに依存しているクライアントは、データ漏洩やサービスの中断に見舞われ、評判に悪影響を及ぼす可能性があります。

要点

- APIによって提供されるアタックサーフェスは、ベストプラクティスに従って監視され、保護されるべきです。
- サービス拒否（DoS）攻撃やクレデンシャル・スタッフィングから保護するために、レート制限とスロットリングを実装する必要があります。
- 従来のセキュリティ管理アプローチと変更管理ポリシーは、クラウドベースのAPIの成長と変化に対応するために更新する必要があります。ベアラートークンやユーザー名/パスワードの代わりに、自動的な時間ベースのローテーションを用いたより短い期間のクレデンシャルを検討します。MFA 要素を備え人間がアクセス可能なユーザーインターフェースは、セキュリティを向上させます。認証イベントに関連するすべてのトークンは、発行時刻を検査できる標準に従うべきです。
- ケイパビリティを移行する際、製品とサービスの同等性を確認します。ベンダーのオンプレミス・インターフェース・ソリューションは、ベンダーの SaaS 構成で、またはハイパースケーラ CSP 間で移動すると、大幅に動作が異なる場合があります。
- クレデンシャルライフサイクルの自動化と、異常な API トラフィックを継続的に監視する技術を調査します。拡張検出用のインテリジェンス・フィードを組み込みます。これらのツールは、ほぼリアルタイムで問題を修正します。

想定事例と実例

セキュアでないインターフェースやAPIに関する最近の問題は次の通りです。

- **(2024年1月)** セキュリティ研究者のトロイ・ハント氏が、Twitterの代替サービスであるSpoutibleのAPIの脆弱性を特定しました。この悪用により、ユーザーアカウント情報へのアクセスが可能になります。 これはメールアドレスやbcryptでハッシュ化されたパスワードを含むユーザーアカウント情報へのアクセスを可能にします。この情報漏えいにより、20万7000件分のデータが流出しました。 [3]
- **(2024年1月)** 既存のメールデータベースとTrelloアカウントをマッチングさせる公開APIにより、1500万以上のTrelloアカウントが流出しました。この事件はAPIのセキュリティの低さを浮き彫りにし、ユーザーデータの露出につながり、後にダークウェブで販売されました。[4]
- **(2024年1月)** 2024年、メルセデス・ベンツで重大なAPI漏えいが発生し、ハッカーが同社のGitHub Enterpriseにアクセスし、ソースコード、クラウドキー、および内部文書が流出しました。この情報漏洩は、前年に公開リポジトリで発見された、タイムスタンプのない従業員のGitHubトークンに端を発しています。[5]
- **(2024年2月)** オーストラリアのISP Tangerineが侵害され、20万件以上の記録が流出しました。この情報漏洩は、単一の請負企業のログイン情報に起因するものでした。盗まれたデータには、氏名、生年月日、電話番号、電子メールアドレスなどの個人情報が含まれていました。[6]

CSA 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

ドメイン 3: リスク、監査、コンプライアンス
ドメイン 4: 組織運営
ドメイン 5: アイデンティティとアクセス管理
ドメイン 6: セキュリティモニタリング
ドメイン 7: インフラストラクチャとネットワーク
ドメイン 8: クラウドワークロードセキュリティ
ドメイン 9: データセキュリティ
ドメイン 10: アプリケーションセキュリティ
ドメイン 11: インシデントレスポンスとレジリエンス

CSA CCM Controls Version 4.0

AIS アプリケーションとインターフェースのセキュリティ

AIS-01:アプリケーションとインターフェースのセキュリティポリシーと手順
AIS-04:セキュアアプリケーションの設計と開発
AIS-06:セキュアなアプリケーション導入の自動化

CEK 暗号技術、暗号化、鍵管理

CEK-03:データ暗号化
CEK-04:暗号化アルゴリズム

CCC 変更コントロールと構成管理

CCC-01:変更管理方針と手順
CCC-02:品質テスト
CCC-05:合意事項の変更

DSP データセキュリティとプライバシーライフサイクル管理

DSP-03:データインベントリ
DSP-04:データ分類
DSP-05:データフロー文書
DSP-17:セキュリティおよびプライバシーについてのポリシーおよび手順

IVS インフラストラクチャと仮想化のセキュリティ

IVS-03:ネットワークセキュリティ
IVS-04:OSのハードニングとベースコントロール
IVS-09:ネットワーク防御

参考文献

1. 2024 State of the Internet Report on API Security: Shining a Light on API Threats https://www.akamai.com/lp/soti/lurking-in-the-shadows
2. OWASP API Security Project https://owasp.org/www-project-api-security/
3. Twitter rival Spoutible alleges smear campaign amid security breach controversy https://techcrunch.com/2024/02/12/twitter-alternative-spoutible-clashes-with-critics-over-security-breach/
4. Massive Trello User Data Leak: Hacker Lists 15 Million Records on a Dark Web Hacking Forum https://www.cpomagazine.com/cyber-security/massive-trello-user-data-leak-hacker-lists-15-million-records-on-a-dark-web-hacking-forum/
5. Mercedes Source Code Exposed by Leaked GitHub Token https://www.securityweek.com/leaked-github-token-exposed-mercedes-source-code/
6. 230k Individuals Impacted by Data Breach at Australian Telco Tangerine https://www.securityweek.com/230k-individuals-impacted-by-data-breach-at-australian-telco-tangerine/

セキュリティ課題4：不十分なクラウドセキュリティ戦略

クラウドセキュリティ戦略には、外部要因、既存の実装、クラウド技術の選択、優先事項、およびトレンドを考慮し、ハイレベルな計画やアプローチを策定することが含まれます。これらの洞察は、企業がクラウドセキュリティの目標を達成し、ビジネス目標をサポートするのに役立ちます。戦略には、クラウドアーキテクチャやクラウドデプロイメントモデルの設計、クラウドサービスモデル、クラウドサービスプロバイダー（CSP）、サービスリージョンのアベイラビリティゾーン、特定のクラウドサービス、国や環境もしくは社会の影響に基づいたCSPの優先順位というような一般原則、また、オンデマンドサービスの利用と課金モデルの許容または回避などを含めることができます。クラウドセキュリティ戦略の策定では、既存のベンダーロックイン、ローカルでのデータ保持を要求する特定の地域での事業展開の意図、特定のCSPやモデルに対する全社的な嗜好などを考慮することがあります。さらに、戦略は、異なるクラウドアカウント、ベンダー、サービス、環境にまたがるIAM、ネットワーキング、およびセキュリティ管理の将来を見据えた設計に影響を与えたり、指示したりすることもあります。

戦略はデザインに先行し、かつ指示されるべきですが、クラウドテクノロジーは、計画、戦略、および改善に対して段階的かつアジャイルなアプローチを要求することが一般的です。健全なクラウドセキュリティ戦略は、クラウドアカウント、ネットワーク、およびサービスにおけるワークロードのセキュアな運用と生産性向上を実現します。さらに、ビジネス、技術、およびリスクの不確実性がある場合でも、セキュリティ上の課題やリスクを克服（または回避）し、意思決定を支援し、有意義なメリットを得ることで、組織に貢献します。

ビジネスインパクト

クラウドセキュリティ戦略やアーキテクチャが存在しないことが、効果的かつ効率的なインフラストラクチャセキュリティの取り組みや設計の実施を妨げています。繰り返されるセキュリティの失敗は、不適切な戦略と設計に起因し、さまざまな影響をもたらします。

技術的な影響：

- *データの漏洩：*健全なクラウドセキュリティ戦略の設計や導入に失敗すると、セキュリティインシデントや侵害が繰り返し発生し、重大な機密保持上の課題が生じる可能性があります。

運用上の影響:

- *デプロイメント*：クラウドセキュリティに対する不適切な戦略的アプローチは、労力の配分の誤り、デプロイやエンジニアリングへの阻害、作業やライセンスソリューションの重複、スコープの拡大、設計レベルの対策がより効果的であるにもかかわらず効果のないパッチや修正につながる可能性があります。

財務的影響：

- *財務コスト：*適切なクラウドセキュリティ戦略の策定や導入の失敗が原因で、セキュリティインシデントや侵害が繰り返し発生すると、多額の封じ込め費用が発生する可能性があります。
- *コンプライアンス違反と罰金：*クラウドセキュリティ戦略の不適切な設計と実装が原因で規制が遵守されない場合、罰則や罰金が科される可能性があります。

風評被害：

- *会社の評判：*クラウドセキュリティの障害が発生した場合、侵害や悪意がない場合でも、否定的な報道がなされたり、口コミで広まったりすることがよくあります。これらは、特に短期的には、顧客獲得、コラボレーション、および株価評価に悪影響を及ぼします。セキュリティベンダーやクラウドベンダーは、特にブランドの信頼に依存しており、セキュリティの失敗の影響を受けやすいです。

要点

- 目標や目的を明確にしたクラウドセキュリティ戦略、または主要な指針を策定します。
- クラウドサービスやセキュリティ対策を設計・導入する際には、ビジネス目標、リスク、効率性、セキュリティ上の脅威、法令遵守を考慮する必要があります。
- クラウドの戦略とセキュリティにおいて、人的ミス、あなたのクラウドのレジリエンシーを阻害する永続的な脅威アクター、中核的な防御策や基本的な管理策（徹底的な防御、構成に依存しないクラウドデプロイメントモデルの優先順位付けなど）の有効化が失敗する可能性を考慮してください。
- 定義されたクラウド戦略と目標に焦点を当て、適切かつベストプラクティスのクラウドネットワーク、アカウント、データ、ID管理、および境界を設計します。

想定事例と実例

クラウドセキュリティのアーキテクチャと戦略の欠如に関連する最近の課題例としては、以下のようなものがあります。

- **(2023年6月)** 何万もの企業顧客の資産とアイデンティティシステムを統合するクラウドベースのアイデンティティとアクセス管理（IAM）サービスであるJumpCloudは、エンジニアに対するスピアフィッシングによる不正アクセスを含むセキュリティ侵害を経験しました。高度で持続的な攻撃と、その結果もたらされた調査、封じ込め、および侵害に関する教訓は、APIキー、ユーザー意識、ソースコードの管理と統合、サービスデプロイメントモデルと管理、エンドポイントとアイデンティティのセキュリティ対策、インフラストラクチャとコンテナ技術の設計、顧客と当局の関与、およびコミュニケーションに及びました。複雑なクラウドベースかつセキュリティに敏感なテクノロジーサービスにおいて、高度な攻撃を阻止する効果的なレジリエンスを構築するには、コンピテンシーと気概が必要です。それでも、技術やサービスを横断的に計画し提供するには、セキュリティや関連領域に対する先見性と深い考察が必要です。 [2]
- **(2022年および2023年)** 2022年1月、LAPSUS$ハッキンググループがサードパーティーのカスタマーサポートエンジニアのアカウントを侵害し、Oktaの内部管理システムにアクセスしました。攻撃者はOktaのシステム、顧客管理、データポータル、およびいくつかの機密情報を操作することができました。2023年、OktaはBeyondTrustや1Passwordを含む複数の著名な顧客から、さらなる情報漏えいの警告を受けました。この 2 回目の侵害は、クラウドベースのアイデンティティ管理会社の IAM、検知、および全体的なレジリエンスに、依然としてギャップがあることを示しました。[3]

CSA 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

ドメイン 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
ドメイン 2: クラウドガバナンス
ドメイン 3: リスク、監査、コンプライアンス
ドメイン 12: 関連技術と戦略

CSA CCM Controls Version 4.0

A&A 監査・保証

A&A-03:リスクベースの計画評価

A&A-04:要件のコンプライアンス

BCR 事業継続管理レジリエンス

BCR-03:事業継続の戦略

BCR-08:事業継続計画

DCS データセンタセキュリティ

DCS-06:資産のカタログ化と追跡

DSP データセキュリティとプライバシーライフサイクル管理

DSP-03:データインベントリ

DSP-07:デザイン段階からのデータ保護とデフォルト設定

DSP-17:セキュリティおよびプライバシーについてのポリシーおよび手順

GRC ガバナンス、リスク管理、コンプライアンス

GRC-02:リスク管理プログラム

GRC-06:ガバナンス責任モデル

GRC-08:Special Interest Group (SIG)

HRS 人的資源

HRS-11:技術利用に関する方針と手順

IAM アイデンティティとアクセスの管理

IAM-01:アイデンティティおよびアクセス管理ポリシーと手順

IAM-08:職務の分離

IAM-09:特権的なアクセスロールの分離

IPY 相互運用性と移植容易性

IPY-01:相互運用性と移植容易性のポリシーと手順

IVS インフラストラクチャと仮想化のセキュリティ

IVS-06:分割と分離

IVS-07:クラウド環境への移行

IVS-04:ネットワーク・アーキテクチャ・ドキュメント

STA サプライチェーンの管理、透明性、説明責任

STA-04:SSRM コントロールオーナーシップ

STA-08:サプライチェーンリスクマネジメント

TVM 脅威と脆弱性の管理

TVM-01:脅威と脆弱性管理ポリシーと手順

参考文献

1. IBM Security. (2023). *IBM X-Force Cloud Threat Landscape 2023 Report - Section 3, Recommendations and best practices.* https://community.ibm.com/community/user/security/blogs/sarah-dudley/2023/09/13/x-force-cloud-threat-landscape-2023
2. [Security Update] June 20 Incident Details and Remediation https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation
3. Okta, with a bruised reputation, rethinks security from the top down https://www.cybersecuritydive.com/news/okta-security-revival/708636/

セキュリティ課題5：セキュアでないサードパーティーリソース

クラウドコンピューティングの普及は急速に進んでおり、サードパーティーのリソースは、オープンソースのライブラリを通じて外部で書かれたコードからSaaS製品まで、あるいはセキュリティ課題2（訳注：セキュアでないインターフェースやAPIは”セキュリティ課題３”）で述べたセキュアでないインターフェースやAPIまで、さまざまなものを意味します。サードパーティーのリソースに起因するリスクも、クラウドサービスやアプリケーションを顧客に提供する一部であるため、サプライチェーンの脆弱性とみなされます。これはサイバーセキュリティサプライチェーンリスク管理（C-CSRM）（訳注：C-SCRMの誤り）とも呼ばれ、自社のクラウドサービスやアプリケーションに課されるサプライチェーンのサイバーセキュリティリスクに焦点を当てています。また、コロラド州立大学の調査によると、情報漏えいの3分の2はサプライヤやサードパーティーの脆弱性に起因しています。[1]

製品あるいはサービスは、それが使用する他の製品あるいはサービスすべてのまとまりであるため、アプリケーションに統合された任意のコンポーネント(例えば1行のコード)が原因でエクスプロイトが開始される可能性があります。悪意のあるハッカーにとっては、目的を達成するために、最も弱いリンクを入り口として探すこと「だけ」が必要なのです。この最も弱いリンクは、大企業にとっての小規模なサプライヤであることがよくあります。

ビジネスインパクト

セキュアでないサードパーティーリソースの利用から生じる課題は、技術的、運用的、財務的、および風評的な影響を中心にビジネス上の影響を及ぼします。以下は、これらが組織にどのような影響を与えるかを検討するための出発点です。

技術的な影響：

- *データの漏洩：侵害された*サードパーティーからのアクセスにより、クラウド経由で重要データへの不正アクセスが発生し、機密性が損なわれる可能性があります。
- *データの破壊：*不適切なコード・リファクタリングにより、不正アクセスが引き起こされ、結果としてデータの漏洩をもたらします。

運用上の影響:

- *本番システムの停止：*サードパーティーリソースのパッチ適用の遅延やパッチ未適用の脆弱性は、本番システムを侵害するアクセスにつながる可能性があります。

財務的影響：

- *コンプライアンス違反と罰金：サードパーティー*が準拠しない場合、企業は損害賠償、罰則、および罰金の責任を負う可能性があります。

風評被害：

- *会社の信頼：セキュア*でないサードパーティーのリソースによって引き起こされた情報漏えいが公になると、企業の機密情報保護能力に対する顧客の信頼を失うことになります。

要点

- 特に自組織が作成したものではないコードや製品のソフトウェアを完全に保護することはできません。組織は、どの製品を使用するかについて、十分な情報を得た上で決定することができます。公式にサポートされているサードパーティーのリソースを活用してください。適切なコンプライアンス認証、セキュリティへの取り組みの透明性、バグ報奨金プログラム、セキュリティ課題への対応、およびタイムリーな修正プログラムの提供に対する責任あるアプローチをチェックします。
- ソフトウェア構成分析（SCA）を通じてサードパーティーのリソースを特定し、ソフトウェア部品表（SBOM）またはSaaS部品表（SaaSBOM）を作成します。
- SBOMまたはSaaSBOMと、組織が使用しているサードパーティーを追跡します。組織は、被害者リストが公表されたときになって初めて、脆弱な製品を使用していたことを知るような事態を避けたいと考えています。これには、オープンソース、SaaS製品、クラウドプロバイダー、マネージドサービス、その他アプリケーションに追加した統合機能などが含まれます。
- サードパーティーリソースを定期的に自動および手動でレビューしてください。もし自組織のプロセスで、必要のない製品が検出されたり、セキュリティ上の課題がある古いバージョンが使用されたりした場合は、適切なメカニズムによって修復されるべきです。これには、コードリポジトリ、インフラストラクチャ、または影響の大きい個々のアプリケーションなど、重要なコンポーネントに付与されるアクセス権の調査も含まれます。
- サプライヤと協力して、自動化されたアプリケーションセキュリティテストを実施するためのトレーニングやツールをサプライヤが備えていることを確認します。

最近のサードパーティー関連では、以下のような問題がありました。

- **(2024年2月)** IBMによると、データ侵害のコストは2023年の世界平均で445万ドルとのことです。さらに、2023年4月、インターネット電話会社の3CXは、サプライチェーンに狙いを定めた攻撃について顧客に通知しました。サイバー犯罪者は、3CXの1つまたは複数のソースコードリポジトリを標的とし、同社のデスクトップアプリケーションにマルウェアを埋め込みました。 [2]
- **(2024年3月)** 広く使用されているデータ圧縮ユーティリティである xz Utils に、 CVE-2024-3094 として識別されている悪意のあるバックドアが発見されました。このユーティリティは、ほとんどすべての Linux および Unix オペレーティングシステムで利用しています。xz Utilsは可逆データ圧縮を提供します。このバックドアは、プロジェクトに長年貢献してきた2人の主要なxz Utils開発者のうちの1人が、バージョン5.6.0と5.6.1に意図的に仕込んだものです。[3]
- **(2024年4月)** 2024年最新レポートによると、サプライチェーン攻撃は、クレデンシャルの窃盗、ソフトウェアやファームウェアの改ざん、データの窃盗、サービス拒否など、いくつかの形態を取る可能性があると、Cyberint社は指摘しています。また、最近、サプライヤへの侵害が急増していると指摘しています。さらに、他の組織に対するベンダーの製品やサービスを改ざんする試みも行われています。[4]

CSA 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

ドメイン 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
ドメイン 2: クラウドガバナンス
ドメイン 5: アイデンティティとアクセス管理
ドメイン 7: インフラストラクチャとネットワーク
ドメイン 10: アプリケーションセキュリティ

CSA CCM Controls Version 4.0

BCR 事業継続管理レジリエンス

BCR-01:事業継続管理方針および手順
BCR-02:リスク評価と影響分析
BCR-03:事業継続の戦略

CCC 変更コントロールと構成管理

CCC-04:承認されていない変更からの保護
CCC-05:合意事項の変更

IAM アイデンティティとアクセスの管理

IAM-05:最小権限
IAM-10:特権的なアクセスロールの管理
IAM-11:合意された特権的なアクセスロールに対するCSCの承認
IAM-14:強固な認証
IAM-16:認可メカニズム

IPY 相互運用性と移植容易性

IPY-01:相互運用性と移植容易性のポリシーと手順
IPY-02:アプリケーションインターフェースの可用性
IPY-03:セキュアな相互運用性と移植容易性の管理
IPY-04:データ移植容易性の契約遵守事項

SEF セキュリティインシデント管理、Eディス

カバリ、およびクラウドフォレンジック

SEF-01:セキュリティインシデント管理ポリシーと手順
SEF-03:インシデントレスポンス計画
SEF-07:セキュリティ侵害の通知

DCS データセンタセキュリティ

DCS-02:資産の分類
DCS-06:資産のカタログ化と追跡
DCS-07:制御されたアクセスポイント

DSP データセキュリティとプライバシーライフサイクル管理

DSP-03:データインベントリ
DSP-05:データフロー文書
DSP-06:データ所有権と管理責任
DSP-08:データプライバシー・バイ・デザインとデフォルト構成
DSP-10:機微なデータの転送
DSP-16:データの保持と削除

STA サプライチェーンの管理、透明性、説明責任

STA-01:SSRMの方針と手続き
STA-02:SSRMサプライチェーン
STA-03:SSRMガイダンス
STA-04:SSRM コントロールオーナーシップ
STA-05:SSRMドキュメントレビュー
STA-06:SSRMコントロールの実装
STA-07:サプライチェーンインベントリ
STA-08:サプライチェーンリスクマネジメント
STA-09:主要なサービスと契約上の合意
STA-10:サプライチェーン合意の確認
STA-11:内部コンプライアンステスト
STA-12:サプライチェーンにおけるサービスアグリーメント準拠
STA-13:サプライチェーンにおけるガバナンスレビュー
STA-14:サプライチェーンにおけるデータセキュリティアセスメント

参考文献

1. Hackers Putting Global Supply Chain at Risk
   https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk
2. Rising Threat: Understanding Software Supply Chain Cyberattacks And Protecting Against Them
   https://www.forbes.com/sites/forbestechcouncil/2024/02/06/rising-threat-understanding-software-supply-chain-cyberattacks-and-protecting-against-them/?sh=4e0f3fd16907
3. Backdoor found in widely used Linux utility targets encrypted SSH connections
   https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/
4. The Weak Link: Recent Supply Chain Attacks Examined
   https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/

セキュリティ課題6：セキュアでないソフトウェア開発

開発者が意図的にセキュアでないソフトウェアを作成することはありませんが、ソフトウェアとクラウド技術の複雑さによって、意図せずに脆弱性がもたらされる可能性があります。このようなセキュアでないソフトウェアがデプロイされると、脅威アクターはこれらの弱点をエクスプロイトしてクラウドアプリケーションを侵害する可能性があります。クラウドファーストのアプローチに注力することで、組織はDevOpsパイプラインの作成を促進し、CI/CD（継続的インテグレーション/継続的デプロイメント）パイプラインを実現できます。クラウドサービスプロバイダー（CSP）は、ガードレールや自動化されたアプリケーションセキュリティテストなど、セキュアな開発機能を提供することもあります。さらに、CSP は IAM 機能を提供し、開発者環境における最小特権の強制と、否認性を確保します。

開発者一人ひとりが、CSPと企業の責任共有の前提を理解するようにするには、継続的な教育が必要です。例えば、開発者のソフトウェアにゼロデイ・エクスプロイトが報告された場合、開発者はその課題を修正する責任を負います。逆に、CSP がソフトウェアの開発または運用環境を提供する場合、課題を修正するためのパッチを実装するのは CSP の責任です。

クラウド技術を採用することで、企業は自社のビジネスに特化したものに集中できる一方、コモディティ化する可能性のあるものはすべてCSPに所有・管理させることができます。クラウドコントロールマトリックス4.0で述べられているように、組織は以下のことを行う必要があります：「組織によって定義されたセキュリティ要件に従って、アプリケーションの設計、開発、デプロイメント、および運用のための（セキュア開発ライフサイクル）SDLC プロセスを定義し、実装する」。SDLCを導入することで、よりセキュアなクラウドアプリケーションを提供することに焦点を当てられます。

ビジネスインパクト

セキュアでないソフトウェア開発は、技術面、運用面、財務面、および風評面に焦点を置いたビジネス上の影響を及ぼします。これらの影響が組織にどのような影響を与えるかを検討するための出発点を以下に挙げます。

技術的な影響：

- *データの開示：セキュア*でないソフトウェアは、機微データへの不正なクラウドアクセスを引き起こし、機密性を損なう可能性があります。
- *データの破壊：セキュア*でないソフトウェア開発に起因する不正アクセスは、データを侵害する可能性があります。

運用上の影響:

- *機能遅延：セキュア*でないソフトウェア開発は、機能アップデートの遅れにつながります。
- *システム停止：セキュア*でないソフトウェアは、クラウドサービスの完全または部分的なシャットダウンを引き起こす可能性があります。

財務的影響：

- *コンプライアンス違反と罰金*規制要件を遵守しない企業は、損害賠償、罰則、および罰金の責任を問われる可能性があります。

風評被害：

- *顧客の信頼：セキュア*でないソフトウェア開発によって引き起こされた情報侵害が公になることで、企業の機密情報保護能力に対する消費者の信頼が失われる可能性があります。

要点

> - 設計、開発、および運用における弱点や脆弱性のスキャンを含む、セキュア開発ライフサイクル（SDLC）プロセスを定義し、実装します。
> - どのようなソフトウェアアプリケーションも、本当にセキュアであることはありえません。組織の開発者は、クラウド技術を活用して、よりセキュアなクラウドアプリケーションを開発し、レジリエンシーを実現するメカニズムを導入します。
> - クラウド技術を使用することで、既存のソリューションを再発明することを防ぐことができます。開発者はガードレールやその他のAPIを活用し、ビジネス特有の課題に集中できます。
> - 責任共有モデルを理解することで、CSPサービスや開発者のアプリケーションの脆弱性にパッチを当てるなど、タイムリーな修復が可能になります。
> - CSP は、セキュリティを重視し、サービスをセキュアに実装するための「Well-Architected Framework」やセキュアなデザインパターンなどのガイダンスを提供します。[1]

想定事例と実例

アカウントの乗っ取りに関する最近の問題には、以下のようなものがあります。

- **(2024年4月)** WordPressプラグインに脆弱性。CVE-2024-27956として識別され、CVSSスコアは9.9/10(Critical)です。この脆弱性により、攻撃者は管理者権限を持つユーザーアカウントを作成し、長期的なアクセスのためのバックドアを仕掛けることができます。根本的な問題は、SQLに影響する一般的な弱点です。この攻撃はSQLインジェクションの問題で、WP Automaticの3.9.2.0以前のバージョンに影響を与えます。この脆弱性は30,000のウェブサイトに影響を与えます。 [2]
- **(2024年4月)** ハッキンググループFancy Bear（APT28）は、Windows Print Spoolerの脆弱性を利用し、権限の昇格、クレデンシャルの取得、およびデータの流出を行っています。このアクターは、GooseEggというこれまで公開されていなかったハッキングツールを利用しています。GooseEggツールは、少なくとも2020年6月以降、APT28によって使用されていることが確認されています。[3]
- **(2024年4月)** サイバーセキュリティ研究者は、Cordova App Harnessと呼ばれる非推奨のApacheプロジェクトに影響を及ぼす依存関係のかく乱による脆弱性を特定しました。この攻撃は、パッケージマネージャがプライベートレジストリよりもパブリックレジストリを優先してチェックする傾向を狙ったものです。脅威アクターは同じ名前の悪意のあるパッケージを公開パッケージリポジトリに公開することができます。依存関係はソフトウェア開発の過程における潜在的な弱点であると指摘されています。[4]

CSA 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

ドメイン 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
ドメイン 5: アイデンティティとアクセス管理
ドメイン 10: アプリケーションセキュリティ
ドメイン 11: インシデントレスポンスとレジリエンス

CSA CCM Controls Version 4.0

AIS アプリケーションとインターフェースのセキュリティ

AIS-01:アプリケーションとインターフェースのセキュリティポリシーと手順
AIS-02:アプリケーションセキュリティのベースライン要件
AIS-03:アプリケーションセキュリティ・メトリクス
AIS-04:セキュアアプリケーションの設計と開発
AIS-05:自動化されたアプリケーションセキュリティテスト
AIS-06:セキュアなアプリケーション導入の自動化
AIS-07:アプリケーション脆弱性の修復

CCC 変更コントロールと構成管理

CCC-02:品質テスト

IAM アイデンティティとアクセスの管理

IAM-01:アイデンティティおよびアクセス管理ポリシーと手順
IAM-04:職務の分離
IAM-05:最小権限
IAM-14:強固な認証
IAM-16:認可メカニズム

TVM 脅威と脆弱性の管理

TVM-03:脆弱性の修復スケジュール

参考文献

1. AWS Well-Architected Framework
   https://thehackernews.com/2024/04/apache-cordova-app-harness-targeted-in.html
2. WP Automatic WordPress plugin hit by millions of SQL injection attacks
   https://www.bleepingcomputer.com/news/security/wp-automatic-wordpress-plugin-hit-by-millions-of-sql-injection-attacks/
3. Microsoft: APT28 hackers exploit Windows flaw reported by NSA
   https://www.bleepingcomputer.com/news/security/microsoft-russian-apt28-hackers-exploit-windows-flaw-reported-by-nsa-using-gooseegg-tool/
4. Apache Cordova App Harness Targeted in Dependency Confusion Attack
   https://thehackernews.com/2024/04/apache-cordova-app-harness-targeted-in.html

セキュリティ課題7：偶発的なクラウドデータ公開

予想外のデータ漏洩（多くの場合、設定ミスによる）のリスクは年々高まっています。[1]無料のパブリック検索ツールは、データの公開リポジトリを見つけるために役立ちます。 [2]これらのリスクは、Amazon（S3バケット、Elastic Container Registry、Elastic Block Storage）、Azure Blob、GCP Storage、Docker Hub、Elasticsearch、Redis、およびGitHubに存在します。 [3]過去2年間、この問題は広く知られ議論されてきましたが、ElasticsearchとS3の侵害は多くの場合、露出から24時間以内に発生しています。
クラウドセキュリティアライアンスは2024年4月、公開バケットの21.1%に機微データが含まれているという調査結果を発表しました。この1年だけでも、氏名、国籍、生年月日、および性別といった一般的な情報に加え、パスポート情報、パスワード、教育データ、運転免許証、自動車情報、医療記録、および生体情報など、さまざまな機微データが誤って開示されています。このような予想外な開示の多くは予防可能であり、見落としや不十分な管理によって発生します。

例えば、S3バケットを作成するとき、ユーザーまたは管理者は、公開読み取りアクセスを有効にするかどうかを決定し、データが追加されるとき、ユーザーは通常、同じ選択結果が提供されます。デフォルトの設定は非公開とし、手動で公開に変更するようにしなければなりません。古いバケットにはまだ過去の設定が残っていますが、このセキュリティ課題は、セキュリティよりも利便性を選択したために発生しています。

ビジネスインパクト

予想外のデータ漏洩は、脅威であると同時に結果でもあります。セキュリティの影響を考慮することなく、知らず知らずのうちに従業員が自分たちの生活を容易にしようとする内部脅威です。これは、侵入やその他の脅威による結果です。結果は明らかで、毎月のニュースになっています。

技術的な影響：

- *データ露出：*設定ミスやその他のエラーによって機密性の高い企業データや個人データが流出した場合、データの所持や使用を許可されていない人にもデータが露出されます。

運用上の影響:

- *ビジネスの途絶：*攻撃者は数分以内に、保護されていないストレージやコンテナを見つけて侵害し、システムの運用を妨げることができます。

財務的影響：

- *コンプライアンス違反：*カリフォルニア州消費者プライバシー法（CCPA）と一般データ保護規則（GDPR）は、違反に対して高額な罰金を定めています。

風評被害：

- *会社の評判：*情報漏えいが世間に知れ渡ることで、企業の誠実さや、事業を管理、統制、および運営する能力に対する消費者や企業からの認識が影響を受ける可能性があります。

要点

- すべてのクラウドプラットフォームは、設定ミスやユーザーによるエラーの影響を受けやすく、技術的な解決策も限られています。これらは、多くの場合、強固な教育プログラム、IT監査イニシアティブ、法的計画などを必要とするプロセス上の課題です。
- いくつかの基本的な設定手順を踏むことで、この課題の「予想外」な部分の可能性を劇的に減らすことができます。バケットを適切に設定し、アクセスを最小限に抑えること（プライベート設定の維持、コンテンツの暗号化、多要素認証（MFA）による強固なパスワードの使用）。各主要クラウドプロバイダー（Amazon, Google, Microsoft）は、セキュアな設定のためのステップバイステップのガイドを提供しています。[5]
- 露出を大幅に減らすには、データベースに対する最小特権のアイデンティティとアクセス管理（IAM）ポリシーを実装します。本ポリシーの割り当てが厳格に管理され、監視されていることを確実にします。アクセス制御リスト（ACL）を無効化/使用せず、より高度なセキュリティのためにIAMを使用します。ゼロトラストアーキテクチャへの進展を継続します。
- コンプライアンスを確保するために、データ所有者は定期的にデータバケットとその権限を特定し、監査する必要があります。構成されている場合、Cloud Security Posture Management（CSPM）ツールは自動修復を行うことができます。

想定事例と実例

予想外のクラウドデータの漏洩課題の様々な種類の最近の例には、以下が含まれます。

- **(2023年6月）パスワード：**公開アクセス可能なリンクから、Microsoftのパスワード、Teamsのメッセージ、ファイルが保存された38TBのAzureストレージバケットにアクセスできました。AmazonとCSAは、このようなリンクを使用しないよう強く勧告しています。 [4, 5, 6]
- **(2023年6月）パスポート情報：**世界野球ソフトボール連盟のS3バケットに設定ミスがあり、パスポート4,600件を含む48,000件の記録が露出しました。セキュリティ課題3（設定ミスと不十分な変更管理）、AmazonとCSAによる推奨を参照してください。 [4, 5, 7]
- **(2023年5月）教育データ：**CaptainU（大学リクルーティング組織）は、写真や私的なメッセージを含む約100万人の高校生の学業記録を露出させました（13歳から18歳の学生を含む）。この例は、ユーザー属性が保存され、漏洩しているだけでなく、会話や画像などがそれらの記録に添付され、同じ場所に保存されていることを示しています。[8]
- **(2023年5月）バイオメトリクス：**U.S.政府のAI請負業者であるVeritone AIは、550GBのオーディオ、ビデオ、生体画像メディア、従業員の個人情報、警察のボディカメラの映像、情報公開法（FOIA）の要求と関連文書、従業員のクレデンシャル、認可トークンを含むシステムログを公開しました。このデータの一部を組み合わせてディープフェイクを作成し、詐欺師としての価値をさらに高めました。[9]

CSA 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

ドメイン 2: クラウドガバナンス
ドメイン 5: アイデンティティとアクセス管理
ドメイン 7: インフラストラクチャとネットワーク
ドメイン 9: データセキュリティ
ドメイン 10: アプリケーションセキュリティ

CSA CCM Controls Version 4.0

AIS アプリケーションとインターフェースのセキュリティ

AIS-02:アプリケーションセキュリティのベースライン要件
AIS-04:セキュアアプリケーションの設計と開発

BCR 事業継続管理レジリエンス

BCR-05:文書化

DSP データセキュリティとプライバシーライフサイクル管理

DSP-01：セキュリティおよびプライバシーについてのポリシーおよび手順
DSP-03:データインベントリ
DSP-05:データフロー文書
DSP-06:データ所有権と管理責任
DSP-07:デザイン段階からのデータ保護とデフォルト設定
DSP-09:データ保護影響評価
DSP-10:機微なデータの転送
DSP-11:個人データへのアクセス、取り消し、修正および削除
DSP-13:個人データの再処理
DSP-14:データサブ処理者の開示
DSP-16:データの保持と削除
DSP-17:機微なデータの保護

GRC ガバナンス、リスク管理、コンプライアンス

GRC-01:ガバナンスプログラムのポリシーと手順
GRC-05:リスク管理プログラム

IAM アイデンティティとアクセスの管理

IAM-01:アイデンティティおよびアクセス管理ポリシーと手順
IAM-03:アイデンティティ・インベントリ
IAM-05:最小権限

IVS インフラストラクチャと仮想化のセキュリティ

IVS-01:インフラストラクチャと仮想化のセキュリティポリシーと手順
IVS-03:ネットワークセキュリティ
IVS-06:分割と分離

参考文献

1. Code42 Annual Data Exposure Report 2024
   https://www.code42.com/resources/reports/2024-data-exposure
2. Bucket Search Tool
   https://buckets.grayhatwarfare.com/
3. 2023 Honeypotting in the Cloud Report
   https://orca.security/resources/blog/2023-honeypotting-in-the-cloud-report/
4. Cloud Security Alliance - The Data on the Danger of Publicly Exposed S3 Buckets (and how to remediate)
   https://cloudsecurityalliance.org/blog/2023/04/06/the-data-on-the-danger-of-publicly-exposed-s3-buckets
5. Security Best Practices for Amazon S3
   https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html
6. Microsoft Azure Data Leak Exposes Dangers of File-Sharing Links
   https://www.darkreading.com/cloud-security/microsoft-azure-data-leak-exposes-dangers-of-file-sharing-links
7. Misconfigured WBSC server leaks thousands of passports
   https://cybernews.com/security/wbsc-data-leak-passports/
8. College recruitment database leaking nearly 1 million students' GPAs, SAT scores, IDs, and other personal data
   https://cybernews.com/security/college-recruitment-database-leaking-nearly-1-million-students-gpas-sat-scores-ids-and-other-personal-data/
9. AI firm with ties to U.S. government exposes billions of documents in breach
   https://www.biometricupdate.com/202405/ai-firm-with-ties-to-u-s-government-exposes-of-billions-of-documents-in-breach

セキュリティ課題8：
システムの脆弱性

システムの脆弱性とは、データの機密性、完全性、および可用性を侵害するためにエクスプロイトされる可能性のあるクラウドサービスプラットフォームの欠陥であり、サービスの運用を停止させる可能性があります。クラウドサービスは通常、カスタムソフトウェア、サードパーティーのライブラリやサービス、およびオペレーティングシステムから構築されます。これらのコンポーネントのいずれかに脆弱性があると、クラウドサービスはサイバー攻撃を受けやすくなります。システムの脆弱性は、大きく4つに分類されます。

- **構成の誤り** - 脆弱性は、クラウドサービスがデフォルトまたは誤った構成設定でデプロイされた場合に発生します。NSAによると、クラウドリソースの設定ミスは、最も一般的なクラウドの脆弱性です。 [4]前述のとおり、本書の「重大脅威」調査の回答者が特定したセキュリティ課題の第1位は、設定の誤りです。
- **ゼロデイ脆弱性** - クラウドサービスプロバイダーやソフトウェアベンダーには知られていないが、脅威アクターによって発見されエクスプロイトされている脆弱性をいいます。
- **パッチが適用されていないソフトウェア** - 既知のセキュリティ上の弱点が含まれており、その課題に対するパッチが提供されているにもかかわらず修正されていないソフトウェアです。
- **脆弱な認証情報またはデフォルトのクレデンシャル** - 強固な認証の欠如により、脅威アクターが機密データやシステムに不正アクセスする可能性が高まります。

システムの脆弱性に対処するには、システムとネットワークのアクティビティを継続的にモニタリングすることと、ハッカーに発見される前にセキュリティ課題を発見するための定期的な脆弱性スキャンが必要です。
パッチ管理システムは、アプリケーションやシステムに存在する既知のセキュリティ脆弱性を修正するためのソフトウェアアップデートやパッチを発見、取得、テスト、およびデプロイするために定期的に使用されるべきです。
ゼロトラストアーキテクチャをデプロイすることで、継続的な認証と最小特権アクセスの実施によって重要なシステムリソースへのアクセスを制限し、攻撃に対抗することができます。

ビジネスインパクト

システムの脆弱性は、クラウドサービスのパフォーマンスや運用にさまざまな形で悪影響を及ぼします。クラウドサービスへの影響は、パッチが適用されていない限り続きます。システムの脆弱性がもたらす影響の一部を紹介します。

技術的な影響

- *セキュリティの弱体化：*システムの脆弱性に対処できないクラウドサービスは、攻撃や侵害を受けやすくなります。
- *データ損失:*機密データやミッションクリティカルなデータは、パッチが適用されていない脆弱性のあるシステムから簡単に盗まれたり、露出したりする可能性があります。

運用上の影響:

- *ビジネスの途絶：*データの損失は、組織がパートナーや顧客に対するビジネス上の義務を果たすことを妨げます。
- *システムパフォーマンス：*攻撃を受けたクラウドサービスは、システムパフォーマンスの低下やシステム停止に至る可能性があります。

財務的影響：

- *収入の損失：*サービスの途絶、復旧、顧客不満足、または法的措置による金銭的損失。
- *コンプライアンス違反と罰金：*脆弱性管理に関する規制要件の不遵守とそれに伴う罰則。

風評被害：

- *会社の評判：*クラウドサービス組織の公共イメージとブランド価値の毀損。
- *顧客の評判：*危険なサードパーティーのクラウドサービスに依存しているクライアントは、データ漏洩やサービスの中断に見舞われ、評判に悪影響を及ぼす可能性があります。

要点

- システムの脆弱性とは、アタックサーフェスを拡大するクラウドサービス内の欠陥のことです。
- NSA と Top Threats の調査回答者は、最も重大なクラウドサービスの脆弱性として設定ミスを挙げています。
- システムとネットワークを継続的なモニタリングすることで、セキュリティの脆弱性やその他のシステムの完全性に関する課題を可視化します。
- 定期的なパッチ管理により、最新のセキュリティパッチが確実に取得・導入され、サイバー攻撃に対するシステムの耐性が高まります。
- ゼロトラストアーキテクチャは、重要なクラウドリソースへのアクセスを制限することで、ゼロデイ脆弱性による潜在的な被害を抑えることができます。

想定事例と実例

クラウドにおけるシステムの脆弱性に関する最近の問題例としては、以下があります。

- **(2023年1月)** Fortra は、同社の GoAnywhere Managed File Transfer (MFT) のリモートコード実行 (RCE) 脆弱性が活発にエクスプロイトされていることを公表しました。CVE-2023-0669として追跡されているこの脆弱性により、攻撃者は一部の顧客環境で不正なユーザーアカウントを作成し、MFTサービスからファイルをダウンロードすることを可能にしました。 [3]
- **(2023 年 3 月)** OpenAIは、Redisキャッシュクライアントコードに導入されたバグを修正するため、ChatGPT サービスをオフラインにしました。Redisは、ChatGPTがデータベースへの直接アクセスを最小化するためにユーザーデータをキャッシュするために使用するオープンソースシステムです。このバグは、ユーザーのチャット履歴と新しく作成された会話の最初のメッセージを公開しました。また、ChatGPT Plus加入者の1.2%に相当する決済関連情報（姓名、メールアドレス、決済先住所、カード有効期限、およびカード番号下4桁）も流出しました。[1]
- **(2023年5月)** ロシアを拠点とするClopランサムウェアグループは、MOVEit Managed File Transfer (MFT) を侵害し、MFTシステムの4つのSQLインジェクション脆弱性をエクスプロイトしました。この脆弱性は、CVE-2023-34362、CVE-2023-35036、CVE-2023-35708、およびCVE-2023-3693Xとして追跡されています。この攻撃は、米国政府機関や民間企業を含む複数のMOVEitの顧客に影響を与えました。500以上の組織と 3,400万人以上の個人が被害を受けたと推定され、Clopの被害組織の72%は米国にありましたが、その他多くの組織が欧州とアジアにありました。Clopランサムウェアグループの活動方法は、データの暗号化から、ターゲットから取得した機密データを露出する脅威へと変化しています[6]。

CSA 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

ドメイン 5: アイデンティティとアクセス管理
ドメイン 6: セキュリティモニタリング
ドメイン 7: インフラストラクチャとネットワーク
ドメイン 9: データセキュリティ
ドメイン 10: アプリケーションセキュリティ
ドメイン 11: インシデントレスポンスとレジリエンス

CSA CCM Controls Version 4.0

AIS アプリケーションとインターフェースのセキュリティ

AIS-01:アプリケーションとインターフェースのセキュリティポリシーと手順
AIS-02:アプリケーションセキュリティのベースライン要件
AIS-06:セキュアなアプリケーション導入の自動化
AIS-07:アプリケーション脆弱性の修復

CEK 暗号、暗号化、鍵管理

CEK-03:データ暗号化
CEK-04:暗号化アルゴリズム

IAM アイデンティティとアクセスの管理

IAM-02:強固なパスワードポリシーと手順
IAM-14:強固な認証
IAM-15:パスワード管理
IAM-16：認可メカニズム

IVS インフラストラクチャと仮想化のセキュリティ

IVS-04:OSのハードニングとベースコントロール

TVM 脅威と脆弱性の管理

TVM-01：脅威と脆弱性管理ポリシーと手順
TVM-02:マルウェア対策ポリシーと手順
TVM-03:脆弱性の修復スケジュール
TVM-04:検出の更新
TVM-05:外部ライブラリの脆弱性
TVM-06:ペネトレーションテスト
TVM-07:脆弱性の特定
TVM-08:脆弱性の優先順位付け
TVM-09:脆弱性管理レポート

参考文献

1. ChatGPT Data Breach Confirmed as Security Firm Warns of Vulnerable Component Exploitation
   https://www.securityweek.com/chatgpt-data-breach-confirmed-as-security-firm-warns-of-vulnerable-component-exploitation/
2. Cyber Security Vulnerabilities and Their Business Impacts
   https://www.verizon.com/business/resources/articles/s/cyber-security-vulnerabilities-and-their-business-impact/
3. Forta Sheds Light on GoAnywhere MFT Zero-Day Exploit Used in Ransomware Attacks
   https://thehackernews.com/2023/04/fortra-sheds-light-on-goanywhere-mft.html
4. Mitigating Cloud Vulnerabilities
   https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF
5. Most Common Types of CyberVulnerabilities
   https://www.crowdstrike.com/cybersecurity-101/types-of-cyber-vulnerabilities/
6. MOVEit Vulnerability Impact: Over 500 Organizations, 34M+ Individuals and Counting
   https://www.spiceworks.com/it-security/security-general/articles/moveit-vulnerability-impact-victims/
7. What is a zero-day exploit?
   https://www.ibm.com/topics/zero-day

セキュリティ課題9：限定的なクラウド可視性/可観測性

組織がクラウドサービスの利用が安全か悪意があるかを効果的に可視化・分析できない場合、制限されたクラウド可視性の課題が起こります。

この課題には2つの重要な課題が含まれます：承認されていないアプリの使用と承認されたアプリの不正使用です。承認されていないアプリの使用とは、従業員が企業のIT部門やセキュリティ部門の特別な許可やサポートを得ずにクラウドアプリケーションやリソースを利用することで、シャドーITにつながります。このシナリオは、機密性の高い企業データが関与している場合に特にリスクがあります。
承認されたアプリの不正使用は、組織が、承認されたアプリが内部関係者によってどのように使用されているか、または多くの場合、クレデンシャルの窃取、SQLインジェクション、DNS攻撃などの手法によって、外部の脅威アクターによってどのように標的化されているかを監視できない場合に発生します。[1, 2, 3]

2023年、いくつかの重大なクラウド侵害が発生し、クラウドの可視性の欠如という課題が浮き彫りになりました。注目すべき例は次のようなものです。

- **データ漏洩につながるヒューマンエラー：Thales**（2023年）によると、企業の3分の1以上（39%）がクラウド環境でのデータ侵害を経験しており、これらのインシデントの半数以上（55%）の主な原因は人為的ミスでした。これは、このようなエラーを防止するために、クラウド環境の可視性とコントロールを向上させることの重要性を浮き彫りにしています。
- **セキュリティ侵害の発見：**Gigamonによれば、セキュリティ侵害の3分の1が、ITやセキュリティの専門家によって発見されていません。このような検知の欠如は、認識されているセキュリティと実際のセキュリティのギャップを浮き彫りにし、可視性と監視ツールの改善の必要性を強調しています。
- **クラウド侵害のコスト：**Illumioの調査（2023年）によると、データ侵害の約半数がクラウドから発生しており、1件当たりの平均コストは410万ドル（約4億円）でした。これらの侵害の大きな要因は、クラウド接続やサードパーティソフトウェアの相互作用の可視化が不十分であったことです。

- 設定ミスとアクセスの課題：Expert Insights（2023年）は、クラウド侵害の多くはアクセス許可の設定ミスが原因であると報告しています。約83%の組織が、アクセス設定ミスに関連するクラウドデータ侵害を少なくとも1回経験し、 多くの企業はユーザーの権限とリソースへのアクセスを可視化していません。

組織は、堅牢なアクセス制御を包括的にモニタリングし[3]、ゼロトラストセグメンテーションのような先進的なセキュリティ手法を採用することで、これらのリスクを軽減し、クラウドセキュリティ全体のレジリエンスを高めることの重要性を認識しています。[4, 5]

ビジネスインパクト

限定的なクラウド可視性は、技術面、運用面、財務面、および風評面などさまざまな面でビジネスに深刻な影響を及ぼします。主な影響は以下の通りです。

技術的な影響：

- *セキュリティの弱体化：*可視性の課題を軽減していないクラウドサービスは、監視されていない脆弱性や設定ミスによる攻撃や侵害を受けやすくなります。
- *データ損失：*APT攻撃は、多くの場合、機微データやミッションクリティカルなデータの窃取や露出を目的としており、ビジネス情報の完全性や機密性を損ないます。

運用上の影響:

- *ビジネスの途絶：*データ損失は、企業がパートナーや顧客に対するビジネス上の義務を果たすことを妨げ、重大な業務停止につながる可能性があります。
- *システムパフォーマンス：*クラウドサービスに対する攻撃は、システムのパフォーマンスを低下させたり、システム停止を引き起こしたりする可能性があり、全体的な生産性やサービス提供に影響を及ぼします。

財務的影響：

- *収入の損失：*サービスの途絶、復旧コスト、顧客の不満足、または侵害後の法的措置などにより、金銭的損失が発生する可能性があります。
- *コンプライアンス違反と罰金：*規制上のセキュリティ要件が守られない場合、多額の罰金や罰則が課され、組織の財務的安定性に影響を及ぼす可能性があります。

風評被害：

- *会社の評判：*データ漏えいは、クラウドサービスプロバイダーの社会的イメージやブランド価値を損ない、顧客の信頼を回復することを困難にします。
- *顧客の評判：侵害されたクラウドサービスに依存している顧客も、データ侵害やサービス中断に見舞われる可能性があり、評判や顧客関係に悪影響を及ぼしかねません。

要点

- **包括的なクラウドの可視化：**クラウドセキュリティアーキテクトに、人、プロセス、およびテクノロジーを統合したソリューションの作成を任せるなど、トップダウン型のアプローチから始めます。
- **全社的な研修の義務化：**全従業員に対し、クラウド利用ポリシーとその実施方法に関するトレーニングを実施します。[6]
- **承認されていないサービスのレビューと承認：**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リスクマネジメントが、承認されていないクラウドサービスをすべてレビューし、承認するようにします。

- **クラウドアクセスセキュリティブローカー（CASB）とゼロトラストセキュリティ（ZTS）ソリューションへの投資：**これらのツールを使用して、アウトバウンド・アクティビティを分析し、クラウドの使用状況を発見し、リスクのあるユーザーや資格のある従業員の異常な行動を特定します。
- **ウェブアプリケーションファイアウォール（WAF）の導入：**不審な傾向、マルウェア、DDoS、およびボットネットのリスクについて、すべてのインバウンド接続を監視します。
- **主要なエンタープライズクラウドアプリケーションを監視：**主要なアプリケーションをコントロールし、疑わしい動作を軽減するソリューションを選択します。
- **ゼロトラストモデルの導入：**組織全体でゼロトラストアプローチを採用し、強固なセキュリティを確保します。

想定事例と実例

限定的なクラウドの可視性に関連する最近の問題例には、以下のようなものがあります。

- **（2023年9月～2023年10月）** 約22日間に及んだOktaの侵害は、クラウドの可視性の重要性を浮き彫りにするもう1つの例です。Oktaの顧客である1Passwordが最初に情報漏洩を検知し、その後BeyondTrustによって確認されました。攻撃者は、Oktaのサービスアカウント情報を保存するために使用されていたOkta従業員の個人的なGoogleアカウントを侵害することでアクセスしました。この侵害は、FedRamp HighおよびDoD IL4環境を除く、すべてのOkta Workforce Identity Cloud（WIC）およびCustomer Identity Solution（CIS）の顧客に影響を与えました。FedEx、Hewlett Packard、T-Mobileなどの大企業を含む、Oktaの数百のクライアントの機密データが露出した可能性があります。この侵害は、クラウドサービスプロバイダーの脆弱性と、このような侵害が広範囲に影響を及ぼす可能性を浮き彫りにし、Oktaのセキュリティ慣行と顧客データを保護する能力に対する懸念を高めました。 [7, 8]
- **（2023年10月～2023年12月）** 大手消費者向け遺伝子会社23 and Meが、クラウドストレージバケットの設定ミスにより大規模なデータ漏洩に見舞われました。500万人以上の顧客の個人ゲノムデータが侵害されました。この侵害は、クラウド環境、特に機密性の高い情報を扱うクラウド環境において、厳格な可視化とアクセス制御を維持することの重要性を浮き彫りにしました。このような機密データの露出は、顧客のプライバシーを損なうだけでなく、社内のデータセキュリティ慣行に対する重大な懸念を引き起こしました。このインシデントは、クラウドの可視化が不十分であった場合に起こりうる結果と、機密データを保護するための継続的なモニタリングと構成管理の必要性を痛感させるものでした。 [9, 10]

CSA 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

ドメイン 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
ドメイン 3: リスク、監査、コンプライアンス
ドメイン 5: アイデンティティとアクセス管理
ドメイン 8: クラウドワークロードセキュリティ
ドメイン 9: データセキュリティ
ドメイン 10: アプリケーションセキュリティ
ドメイン 11: インシデントレスポンスとレジリエンス

CSA CCM Controls Version 4.0

IAM アイデンティティとアクセスの管理
IAM-03:アイデンティティ・インベントリ
IAM-08:ユーザーアクセスレビュー

LOG ロギングとモニタリング
LOG-03:セキュリティモニタリングおよびアラート
LOG-05:監査ログのモニタリングとレスポンス

SEF セキュリティインシデント管理、Eディスカバリ、およびクラウドフォレンジック
SEF-03:インシデントレスポンス計画
SEF-04:インシデント対応テスト

STA サプライチェーンの管理、透明性、説明責任
STA-08:サプライチェーンリスクマネジメント

TVM 脅威と脆弱性の管理
TVM-01:脅威と脆弱性管理ポリシーと手順
TVM-09:マルウェア対策ポリシーと手順
TVM-03:脆弱性の修復スケジュール
TVM-04:検出の更新
TVM-05:外部ライブラリの脆弱性
TVM-06:ペネトレーションテスト
TVM-07:脆弱性の特定
TVM-08:脆弱性の優先順位付け
TVM-09:脆弱性管理レポート
TVM-10:脆弱性管理指標

参考文献

1. Prisma Cloud by Palo Alto Networks: Cloud Discovery and Exposure Management
   https://start.paloaltonetworks.com/prisma-cloud-request-a-trial
2. Gigamon: Five Top Concerns in Private Cloud Visibility
   https://blog.gigamon.com/2024/03/05/five-top-concerns-in-private-cloud-visibility/
3. Thales: 2023 Cloud Security Study - Global Edition
   https://cpl.thalesgroup.com/cloud-security-research
4. Illumio: Cloud Security Index: Redefine Cloud Security with Zero Trust Segmentation
   https://www.illumio.com/resource-center/cloud-security-index-2023
5. CrowdStrike: 2023 Cloud Risk Report
   https://www.crowdstrike.com/cloud-risk-report/
6. 50 Cloud Security Stats You Should Know In 2024
   https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/
7. ManageEngine: Understanding the Okta Supply Chain Attack of 2023: A Comprehensive Analysis
   https://blogs.manageengine.com/it-security/2024/01/25/understanding-the-okta-supply-chain-attack-of-2023-a-comprehensive-analysis.html
8. BeyondTrust: Okta Support Unit Breach Update
   https://www.beyondtrust.com/blog/entry/okta-support-unit-breach-update
9. 23andMe's data hack went unnoticed for months
   https://www.engadget.com/23andmes-data-hack-went-unnoticed-for-months-081332978.html
10. 23andMe confirms hackers stole ancestry data on 6.9 million users
    https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/

セキュリティ課題10：未認証のリソース共有

認証されていないクラウドリソースの共有は、クラウドサービスに重大なセキュリティリスクをもたらす可能性があります。クラウドのリソースには、仮想マシン、ストレージバケット、データベースなどがあり、これらにはすべて、業務に不可欠な機微データやアプリケーションが含まれています。適切なユーザー認証や最小特権の原則に従わなければ、クラウドリソースは、企業や個人所有の機微データを盗み出そうとする脅威にさらされる可能性があります。

クラウドリソースを保護するためのベストプラクティスの中でも、パスワード入力を伴うBASIC認証は最低でも必要不可欠です。しかし、毎年、パスワードで保護されていないクラウドストレージやデータベースシステムから大規模なデータ侵害が発生しています。今日のインターネット上の膨大なデータの海の中で、セキュリティ保護されていないクラウドリソースを見つけるのは難しいように思えるかもしれませんが、その逆です。Shodan、Binary Edge、およびGrayhat Warfareのような一般に利用可能なIoT（モノのインターネット）検索ツールは何年も前から存在しており、保護されていないデータリポジトリを比較的簡単に見つけることができます。

パスワード保護以外にも、重要なデータを保護するためのセキュリティ対策を講じることができます。

- MFA(多要素認証):MFA は、データへのアクセスを試みる際に、ワンタイムアクセスコードや生体認証などの二次的な検証を通じた本人確認をユーザーに要求します。
- **サードパーティー認証プラットフォーム：**ユーザーのアイデンティティ確認に特化したサービスを使用することで、組織はユーザー認証を確実に管理し、ワンクリックやワンタッチ認証など、ユーザーフレンドリーな認証スキームを提供することができます。
- **ユーザーアクセスの管理：**ユーザーには、必要なデータやアプリケーションへのアクセス権のみが付与されるべきです。
- **活動の継続的モニタリング：**ユーザーを継続的に監視し、不規則な活動を追跡することが重要です。不審なユーザーの行動は、データ侵害の前兆であったり、データ侵害が進行中であることを示す可能性があります。

セキュリティコントロールは、設定ミスがないか定期的に監査し、弱点を特定するためにセキュリティテストを実施すべきです。脆弱性が発見できれば、サイバー犯罪者に発見されエクスプロイトされる前に修正できます。

ビジネスインパクト

認証されていないクラウドリソースがもたらす悪影響をいくつか紹介します。

技術的な影響：

- *データ侵害：未認可*の脅威者は、機密データやミッションクリティカルなデータを盗んだり、露出したりする可能性があります。
- *データの損失：*データへの無制限のアクセスは、データの一部または全部の破壊につながる可能性があります。

運用上の影響:

- *ビジネスの途絶：*データの損失は、組織がパートナーや顧客に対するビジネス上の義務を果たすことを妨げます。

財務的影響：

- *収入の損失：*サービスの途絶、サービスの復旧、顧客不満足、または法的措置による金銭的損失。
- *コンプライアンス違反と罰金：*脆弱性管理に関する規制要件の不遵守とそれに伴う罰則。

風評被害：

- *会社の評判：*クラウドサービス組織の公共イメージとブランド価値の毀損。
- *顧客の評判：*危険なサードパーティーのクラウドサービスに依存しているクライアントは、データ侵害やサービスの中断に見舞われ、評判に悪影響を及ぼす可能性があります。

要点

> - クラウドストレージやデータベース設備はパスワードで保護されていないことがあり、誰でも簡単にエクスプロイトできます。クラウドリソースへのアクセスを制限するには、パスワードによる基本的なユーザー認証が不可欠です。
> - MFAを導入し、サードパーティーの認可サービスを利用することで、認証はさらに改善されます。
> - ユーザーを継続的にモニタリングすることで、その活動が正当なものか悪意あるものかを判断することができます。

想定事例と実例

認証されていないリソース共有に関連する最近の問題例には、以下のようなものがあります。

- **(2023年9月)** KidSecurityは、親が子供を追跡したり、子供の音を聞いたり、ゲームの制限を設定したりするために使用できる、広く使用されているペアレンタルコントロールアプリです。研究者は、同社が自社サービスのElasticsearchとLogstashのコレクションをセキュアにしていなかったことで、ユーザーの個人情報が露出されていることを発見しました。KidSecurityのログは、インターネット上の誰にでも1ヶ月以上公開されていました。21,000件の電話番号、31,000件の電子メールアドレスなど、3億件以上の個人情報が露出しました。このアプリはまた、クレジットカード番号の最初の6桁と最後の4桁、有効期限、および発行銀行を明らかにし、ユーザーの支払い情報を露出しました。 [2, 4]
- **(2023年10月)** インド国営のNational Logistics Portal-Marineウェブサイトが、Amazon S3バケットの設定ミスにより、機密データや個人情報を保管していました。このウェブサイトはまた、ログインクレデンシャルを含むJavascriptファイルをブラウザに送信していました。露出されたデータには、フルネーム、国籍、生年月日、性別、パスポート番号、パスポート発行機関、船舶の有効期限、その他渡航のために提出された船舶乗組員が含まれていました。請求書、出荷指示書、貨物請求書も機微データでした。[3]
- **(2024年1月)** Spotify、Amazon's Audible、Apple Musicなどのストリーミングシステムから音楽を変換するために使用されるTunefabコンバーターが、ユーザーの個人情報を露出していることを研究者が発見しました。このプラットフォームは、ユーザーのIPアドレス、地域、ID、電子メールアドレス、およびデバイス情報を含む1億5100万件以上のレコードを露出しました。データ漏洩の原因は、パスワードで保護されていないMongoDBデータベースに設定ミスがあり、インターネット上に公開されたことでした。このデータベースは、9月26日に一般公開されているIoT検索エンジンで発見されました。[4, 5]

CSA 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

ドメイン 3: リスク、監査、コンプライアンス
ドメイン 5: アイデンティティとアクセス管理
ドメイン 6: セキュリティモニタリング
ドメイン 9: データセキュリティ
ドメイン 10: アプリケーションセキュリティ

CSA CCM Controls Version 4.0

A&A 監査・保証

A&A-04:要件のコンプライアンス

A&A-05:監査管理プロセス

DSP データセキュリティとプライバシーライフサイクル管理

DSP-07:デザイン段階からのデータ保護とデフォルト設定

DSP-17:機微なデータの保護

DSP-19:データの所在地

IAM アイデンティティとアクセスの管理

IAM-01:アイデンティティおよびアクセス管理ポリシーと手順

IAM-02:強力なパスワードポリシーと手順

IAM-07:ユーザー アクセスの変更と取り消し

IAM-08:ユーザー アクセスのレビュー

IAM-14:強固な認証

IAM-15:パスワード管理

IAM-16:認可メカニズム

LOG ロギング&モニタリング

LOG-05:監査ログのモニタリングとレスポンス

LOG-12:アクセスコントロールログ

TVM 脅威と脆弱性の管理

TVM-06:ペネトレーションテスト

TVM-07:脆弱性の特定

参考文献

1. Cloud Basics, Best Practices & Implementation
   https://www.okta.com/blog/2020/12/cloud-security-basics-best-practices-implementation/
2. KidSecurity's user data was compromised after the app failed to set the password
   https://cybernews.com/security/kidsecurity-parental-control-data-leak/
3. India's national logistics portal exposed sensitive personal data trade records
   https://techcrunch.com/2023/10/02/india-national-logistics-portal-marine-data-expose/
4. List of Data Breaches and Cyber Attacks in 2023 - 8,216,886,660 records breached
   https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023
5. Spotify music converter puts users at risk
   https://cybernews.com/news/spotify-music-converter-puts-users-at-risk/

セキュリティ課題11：APT攻撃

APT攻撃は、クラウドセキュリティに重大なリスクをもたらし続けています。国家主体の攻撃者や組織化された犯罪組織などの洗練された攻撃者は、クラウド上の機微データやリソースを標的とした長期的な攻撃キャンペーンを実施するためのリソースと専門知識を持っています。[1]

2022年から2023年にかけて、APTの活動は、ランサムウェアや恐喝、ゼロデイ脆弱性のエクスプロイト、フィッシング、クレデンシャルの窃取、破壊的なワイパー攻撃、サプライチェーンの侵害など、さまざまな手口を通じてクラウド環境を著しく脅かしました。[3]これらの手口は、APTの永続的な性質を浮き彫りにしており、このような高度な脅威からクラウドインフラストラクチャを保護するための強固なセキュリティ対策が必要とされています。

クラウド上のAPT攻撃に対し防御するために、組織はサイバー脅威インテリジェンスを監視し、最も関連性の高いAPTグループとその戦術、技術、および手順（TTP）を理解する必要があります。レッドチームの演習は、エミュレートされたAPT攻撃に対する検知・対応能力をテストし、向上させるために役立ちます。また、クラウド環境における脅威ハンティング活動は、APTのステルス的かつ持続的な存在を特定するためにも極めて重要です。このような高度な敵に対抗するには、強力なアクセス制御、暗号化、モニタリング、インシデント対応など、多層的なクラウドセキュリティ戦略が不可欠です。

ビジネスインパクト

APT攻撃は、さまざまなチャネルを通じて企業に深刻な影響を与え、技術的、運用的、財務的、および評判的に重大な結果をもたらします。

技術的な影響：

- *セキュリティの弱体化：*APT攻撃の脆弱性に対処できないクラウドサービスは、攻撃や侵害を受けやすくなります。
- *データ損失:*APT攻撃による攻撃は多くの場合、機密データやミッションクリティカルなデータの窃取や露出を目的としており、ビジネス情報の完全性と機密性を損ないます。

運用上の影響:

- *ビジネスの途絶：*データ損失は、組織がパートナーや顧客に対するビジネス上の義務を果たす妨げとなり、業務停止につながります。
- *システムパフォーマンス：*クラウドサービスに対する攻撃は、システムのパフォーマンスを低下させたり、システム停止を引き起こしたりする可能性があり、全体的な生産性やサービス提供に影響を及ぼします。

財務的影響：

- *収入の損失：*サービスの途絶、復旧コスト、顧客不満足、および侵害後の法的措置などにより、金銭的損失が発生する可能性があります。
- *コンプライアンス違反と罰金：*規制上のセキュリティ要件が守られない場合、多額の罰金や罰則が課され、組織の財務的安定性に影響を及ぼす可能性があります。

風評被害：

- *会社の評判：*APT攻撃による侵害は、クラウドサービスプロバイダーのパブリックイメージやブランド価値を損ない、顧客の信頼を回復することを困難にします。
- *顧客の評判：侵害されたクラウドサービスに依存している顧客も、データ漏洩やサービス中断に見舞われる可能性があり、評判や顧客関係に悪影響を及ぼしかねません。*

要点

- **ビジネスインパクト分析：**ビジネスインパクトを定期的に分析し、組織の重要な情報資産と潜在的な脆弱性を特定・把握します。これにより、APT攻撃の脅威から最も貴重なデータを保護するためのセキュリティ対策とリソース配分の優先順位付けが可能になります。
- **サイバーセキュリティ情報の共有：**サイバーセキュリティ情報共有グループやフォーラムに参加し、関連するAPTグループやその戦術、技術、および手順（TTP）について常に情報を得ます。この集合的な知識は、組織の準備と対応能力を高めます。
- **攻撃的なセキュリティ演習：**レッドチームや脅威ハンティング活動を通じて、APT攻撃のTTPを定期的にシミュレートします。このような攻撃的なセキュリティ演習は、高度な脅威に対するセキュリティ対策が効果的であることを確実にし、検知および対応能力のテストと改善に役立ちます。

想定事例と実例

APT、組織犯罪、ハッカーに関する最近の問題の事例には次のようなものがあります。

- **(2023年3月)** 北朝鮮のAPTグループLABYRINTH CHOLLIMAは、暗号通貨および金融テクノロジー企業のクラウドリソースを標的としていました。このグループは、ランサムウェアと恐喝の手口を採用し、Windows、Linux、およびmacOSを含む複数のプラットフォームで活動する能力を示しました。この攻撃は、同グループの洗練された能力と、金融部門における高価値のターゲットへの集中を実証するものでした。ランサムウェアと恐喝の二重のアプローチは、目先の金銭的利益と、被害を受けた組織に対する長期的な混乱と圧力の発生を目的としています [2, 6]。
- **(2023年6月)** イランのAPTグループは、金銭的な利益のためだけでなく、スパイ活動の隠れ蓑としてランサムウェアを使用していることが確認されています。これらのグループは、侵入の証拠を隠滅するためにワイパー（データ消去プログラム）を配備し、典型的なランサムウェア攻撃のように見せかけています。この戦術によって、彼らは真の意図を隠蔽しながらスパイ活動やその他の隠密活動を行うことができました。ワイパーは、その存在と操作の痕跡を消すための戦略的アプローチを示しており、インシデント対応やフォレンジック調査を複雑にします。ランサムウェアとワイパーを組み合わせるこの手法は、APT攻撃の脅威の進化と欺瞞的な性質を浮き彫りにしています[4, 5]。
- **(2023年5月)** 中国のAPTグループAPT41が、Microsoftのソフトウェアのゼロデイ脆弱性「Follina」を悪用し、様々な政府機関のクラウド環境を侵害しました。この攻撃は、新たに発見された脆弱性を迅速かつ効果的に活用するAPT41の能力を浮き彫りにしました。Follinaの脆弱性を悪用することで、政府機関のクラウドシステムに不正アクセスし、機密情報を抜き取ることができました。この事件は、高度な脅威から身を守るために、タイムリーなパッチ管理と脆弱性評価が極めて重要であることを浮き彫りにしました。 [2, 4].

CSA 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

ドメイン 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
ドメイン 3: リスク、監査、コンプライアンス
ドメイン 5: アイデンティティとアクセス管理
ドメイン 8: クラウドワークロードセキュリティ
ドメイン 9: データセキュリティ
ドメイン 10: アプリケーションセキュリティ
ドメイン 11: インシデントレスポンスとレジリエンス

CSA CCM Controls Version 4.0

IAM アイデンティティとアクセスの管理

IAM-03:アイデンティティ・インベントリ
IAM-08:ユーザーアクセスレビュー

LOG ロギング&モニタリング

LOG-03:セキュリティモニタリングおよびアラート
LOG-05:監査ログのモニタリングとレスポンス

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

SEF-03:インシデントレスポンス計画
SEF-04:インシデント対応テスト

STA サプライチェーンの管理、透明性、説明責任

STA-08:サプライチェーンリスクマネジメント

TVM 脅威と脆弱性の管理

TVM-01:脅威と脆弱性管理ポリシーと手順
TVM-02:マルウェア対策ポリシーと手順
TVM-03:脆弱性の修復スケジュール
TVM-04:検出の更新
TVM-05:外部ライブラリの脆弱性
TVM-06:ペネトレーションテスト
TVM-07:脆弱性の特定
TVM-08:脆弱性の優先順位付け
TVM-09:脆弱性管理レポート
TVM-10:脆弱性管理指標

参考文献

1. APT definition.
   https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
2. CrowdStrike: CrowdStrike 2023 Threat Hunting Report
   https://www.crowdstrike.com/resources/reports/threat-hunting-report/
3. IBM Security: IBM X-Force Cloud Threat Landscape 2023 Report
   https://community.ibm.com/community/user/security/blogs/sarah-dudley/2023/09/13/x-force-cloud-threat-landscape-2023
4. Mandiant: M-Trends 2023 Report
   https://services.google.com/fh/files/misc/m_trends_2023_report.pdf
5. Palo Alto Networks: 2023 Unit 42 Ransomware and Extortion Report
   https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report
6. How APT groups ramped up in 2023
   https://www.techradar.com/pro/how-apt-groups-ramped-up-in-2023

結論と今後の見通し

本レポートでは、進化を続けるクラウドセキュリティの脅威の状況を分析し、設定ミス、IAMの脆弱性、セキュアでないAPI、および包括的なセキュリティ戦略の欠如などの永続的な性質に焦点を当てています。これらの脅威は2022年の報告書で指摘されたものと変わりませんが、引き続き存在することで、その重要性が浮き彫りになっています。

クラウドセキュリティの脅威の将来を形作るであろうトレンドは数多くあります。企業は、セキュアなクラウド環境を維持するために、常に情報を入手し、これらのトレンドに適応する必要があります。主なトレンドは以下の通りです。

- **攻撃の高度化：**攻撃者は、クラウド環境の脆弱性をエクスプロイトするために、AIを含むより高度な技術を開発し続けるでしょう。このような新しい技術には、継続的な監視と脅威を発見する機能を備えた積極的なセキュリティポスチャが必要になります。
- **サプライチェーンのリスク：**クラウドエコシステムの複雑化により、サプライチェーンの脆弱性に対するアタックサーフェスが拡大します。組織は、ベンダーやパートナーにもセキュリティ対策を拡大する必要があります。
- **進化する規制の状況：**規制機関は、より厳しいデータプライバシーとセキュリティの規制を実施する可能性が高く、企業は自組織のクラウドセキュリティ活動をそれに適応させる必要があります。
- **Ransomware-as-a-Service（RaaS）の台頭：**RaaSは、クラウド環境に対して高度なランサムウェア攻撃を仕掛けることを、未熟な行為者にも容易にします。企業は、強力なアクセス制御とともに、堅牢なデータバックアップおよびリカバリソリューションを必要とします。

主な軽減策は以下の通りです。

- **SDLC（ソフトウェア開発ライフサイクル）を通じたAIの統合：**開発の初期段階でコードレビューや自動脆弱性スキャンなどの作業にAIを活用することで、コードが本番環境に到達する前にセキュリティ上の課題を特定し、対処できます。
- **AIを活用した攻めのセキュリティツール：**これらのツールは攻撃者の行動をシミュレートし、クラウド設定、IAMプロトコル、およびAPIの脆弱性を発見します。この積極的なアプローチにより、企業は潜在的な脅威の一歩先を行くことができます。
- **クラウドネイティブのセキュリティツール：**クラウド環境に特化して設計されたクラウドネイティブセキュリティツールの導入が進むでしょう。これらのツールは、従来のセキュリティソリューションよりも優れた可視性とコントロールを提供します。
- **ゼロトラストセキュリティモデル：**ゼロトラストモデルは、継続的な検証と最小特権アクセスを重視し、クラウドセキュリティの標準となっています。
- **自動化とオーケストレーション：**複雑なクラウドセキュリティを大規模に管理するには、セキュリティプロ

セスとワークフローの自動化が不可欠です。

- **セキュリティスキルの格差：**サイバーセキュリティのスキル格差は今後も続くでしょう。組織は、必要な専門知識を構築するために、トレーニングと開発プログラムに投資しなければなりません。このギャップに対処するには、従業員に対する継続的な教育と意識向上プログラムが不可欠です。

企業は、これらの戦略を採用し、進化する脅威に対する警戒を怠らないことで、セキュアでレジリエントなクラウド環境を構築することができます。しかし、サイバーセキュリティの状況は常に変化しています。Cloud Security Posture Management（CSPM）やEndpoint Detection and Response（EDR）ツールなど、最先端のセキュリティソリューションへの継続的な適応と投資は、時代の最先端を走り続け、また、クラウドセキュリティ侵害に関連する財務リスクや評判リスクを軽減するために不可欠です。