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

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

Cloud Security Alliance Top Threats Working Groupの恒久的かつ公式なリンクはこちら：
https://cloudsecurityalliance.org/research/working-groups/top-threats/

© 2022 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, non- commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Co-chairs

Jon-Michael Brook
Alexander Stone Getsin
Michael Roza

Contributors

Jon-Michael C Brook
Victor Chin
Hugh Foskett
Alex Getzin
Vic Hargrave
Shachaf Levy
Andrew McCormick
Stephen Pieraldi
Michael Roza
Marcus Ryan
Alon Schindel
Shira Shamban

Reviewers

Guy Dahan
Moshe Ferber
Alex Rebo
Daniel Schwartzer
Udith Wickramasuriya

CSA Global Staff

Sean Heide
Claire Lehnert (graphic design)
Stephen Lumpe (graphic design)

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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の重大脅威 - パンデミックイレブン」は、Cloud Security Alliance (CSA)が公開している「Top Threats to Cloud Computing - Pandemic Eleven」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
2022年11月16日	日本語版1.0	初版発行

本翻訳の著作権はCSAジャパンに帰属します。引用に際しては、出典を明記してください。無断転載を禁止します。転載および商用利用に際しては、事前にCSAジャパンにご相談ください。
本翻訳の原著作物の著作権は、CSAまたは執筆者に帰属します。CSAジャパンはこれら権利者を代理しません。原著作物における著作権表示と、利用に関する許容・制限事項の日本語訳は、前ページに記したとおりです。なお、本日本語訳は参考用であり、転載等の利用に際しては、原文の記載をご確認下さい。

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。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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の重大脅威 - パンデミックイレブン」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, CISSP, CISA, CISM
井上 淳
釜山 公徳
斎藤 知明, CISM
鈴木 伸
千田 哲秀
高橋 久緒, CISSP, RISS, PMP
松浦 一郎, CISSP, CISM, CDPSE
満田 淳
諸角 昌宏
山口 弘行, CISSP, CISA
渡邉 浩一郎, CISSP, CISA, CEH

© Copyright 2022, Cloud Security Alliance. All rights reserved.

目次

エグゼクティブサマリ 9
サーベイ内容 10
セキュリティの課題1: 不十分なアイデンティティ、クレデンシャル、アクセスおよび鍵の管理、ならびに特権アカウント 12
ビジネスインパクト 12
要点 13
想定事例と実例 13
CSA CBK Security Guidance Version 4.0 13
CSA CCM Controls Version 14
セキュリティの課題2: セキュアでないインターフェースやAPI 15
ビジネスインパクト 15
要点 16
想定事例と実例 16
CSA CBK Security Guidance Version 4.0 16
CSA CCM Controls Version 17
セキュリティの課題3: 設定ミスと不適切な変更管理 18
ビジネスインパクト 18
要点 19
想定事例と実例 19
CSA CBK Security Guidance Version 4.0 20
CSA CCM Controls Version 4.0 20
セキュリティ課題4 ： クラウドセキュリティのアーキテクチャと戦略の欠如 22
ビジネスインパクト 22
要点 23
想定事例と実例 23
CSA CBK Security Guidance Version 4.0 23
CSA CCM Controls Version 4.0 24
セキュリティ課題5 ： セキュアでないソフトウェア開発 25
ビジネスインパクト 25
要点 26
想定事例と実例 26
CSA CBK Security Guidance Version 4.0 26
CSA CCM Controls Version 4.0 27
セキュリティ課題6 ： セキュアでないサードパーティーのリソース 28
ビジネスインパクト 28
要点 29
想定事例と実例 29
CSA CBK Security Guidance Version 4.0 30

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CCM Controls Version 4.0 30
セキュリティの課題7： システムの脆弱性 32
ビジネスインパクト 32
要点 33
想定事例と実例 33
CSA CBK Security Guidance Version 4.0 34
CCM Controls Version 4.0 34
セキュリティ課題8： 予想外のクラウドデータ公開 36
ビジネスインパクト 36
要点 36
想定事例と実例 37
CSA CBK Security Guidance Version 4.0 37
CSA CCM Controls Version 4.0 38
セキュリティ課題9： サーバーレスやコンテナワークロードの構成ミスやエクスプロイト 39
ビジネスインパクト 40
要点 40
想定事例と実例 40
CSA CBK Security Guidance Version 4.0 41
CSA CCM Controls Version 4.0 41
セキュリティ課題10： 組織的な犯罪、ハッカーとAPT 43
ビジネスインパクト 43
要点 44
想定事例と実例 44
CSA CBK Security Guidance Version 4.0 44
CSA CCM Controls Version 4.0 44
セキュリティ課題11： クラウドストレージデータ流出 46
ビジネスインパクト 47
要点 47
想定事例と実例 47
CSA CBK Security Guidance Version 4.0 48
CSA CCM Controls Version 4.0 48
結論 50

© Copyright 2022, Cloud Security Alliance. All rights reserved.

エグゼクティブサマリ

重大脅威レポートは従来から、クラウドの脅威、脆弱性、リスクに対する意識向上を目的としています。第6回目となる今回は、700名以上の業界専門家を対象に、クラウド業界におけるセキュリティの課題について調査を実施しました。今年の回答者は、クラウド環境における11の重要なセキュリティ課題を指摘しました。Top Threats Working Groupは、調査結果とその知見をもとに、2022年の「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」レポートを作成しました。

最新のレポートでは、「パンデミックイレブン」（11ページ記載の調査による重要度順に基づく）を取り上げています。また、カッコ（ ）内は2019年調査で既出または類似の課題のランキングを示します。

1. 不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理、ならびに特権アカウント[1] (4)
2. セキュアでないインターフェースやAPI(7)
3. 設定ミスと不適切な変更管理(2)
4. クラウドセキュリティのアーキテクチャと戦略の欠如(3)
5. セキュアでないソフトウェア開発
6. セキュアでないサードパーティーのリソース
7. システムの脆弱性 (8)
8. 予想外のクラウドデータ公開
9. サーバレスやコンテナワークロードの構成ミスやエクスプロイト
10. 組織的な犯罪、ハッカーとAPT(11)
11. クラウドストレージデータ流出

考察と根拠

COVID-19の大流行とその後のロックダウンにより、職場は再定義され、在宅勤務はもはや有ると便利な柔軟性のある利点としてではなく、企業活動を継続するために必要なものとして強調されるようになりました。パンデミックとクラウドワークロードの複雑さ、サプライチェーン、そしてEdge Compute、IoT（Internet of Things）、OT（Operational Technology）、およびブロックチェーンなどの新しいテクノロジーによって、クラウドのセキュリティ状況は一変しました。SDP（Software Defined Perimeter）やZTA（Zero Trust Architecture）といった新しいコンセプトは、それらのランドスケープへのアクセスに関する私たちの視界を変えました。

調査結果の回答を分析すると、クラウドサービスプロバイダ（CSP）の管理下に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がわかります。サービス妨害、共有技術の脆弱性、CSPのデータ損失、システムの脆弱性などの懸念 ～ 以前に発行されている「11の悪質な脅威(EE)」クラウドの重大セキュリティ 脅威 2019」で紹介された事項 ～ は、今回のレポートから除外されるほど低評価となりました。Infrastructure as a Service (IaaS)環境における年代物のクラウドのセキュリティ課題は、あまり懸念されていないようにみえます。

[1] (訳注)原文では目次と本文タイトルが相違しているが、和訳では本文のタイトルに合わせた。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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。

サーベイで新たに高順位を得た項目は、クラウド利用者が弱点であることを指摘しています。回答者は、メタストラクチャ(EE:9)、弱いコントロールプレーン(EE:8)、利用状況の可視性(EE:10)がクラウド導入における課題になるかもしれないという疑問を、もはや抱いていません。「危険な12の落とし穴」から「11の悪質な脅威」を経て今回の調査に至るまで、責任の所在をスタックの上位層に押し上げる傾向が続いています。本パンデミックイレブンは、アイデンティティやアクセス管理、暗号化、構成管理、不適切なコーディングの実践、およびクラウドの戦略的方向性無視など、ユーザが直接コントロールできる状況に焦点を当てています。

アジャイルプロジェクトマネジメントとDevOpsの盛り上がりは、これらの複合的な問題を直接に、エンドソフトウェアチームに担当させます。

最高の業績を発揮するクラウド組織であるかどうかを分けるのは、変更管理を重視し、従業員の相互トレーニングを強化し、セキュリティ・チャンピオンチームを結成し、セキュリティとコンプライアンスを文化的に確立している企業であるかどうかという点に尽きるでしょう。クラウドは、COVIDのロックダウンの即時的な要求からずいぶん経過した後も、日常化が期待され、繁栄し続けています。これらの11の脅威、リスク、および脆弱性を調査し、将来の成功のためにクラウドをセキュアにしましょう。

対象読者

クラウドとセキュリティの専門家や愛好家は、本レポートを通じて、クラウドセキュリティの脅威と課題の現状、それらが業界にどのような影響を及ぼすようになったか、個人または業界として何を改善すべきかについて、最新の知見を得ることができます。最後に、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。

サーベイ内容

本2022年版「クラウドコンピューティングのトップ脅威-パンデミックイレブン」レポートの作成にあたり、CSA*Top Threats Working Group* は 2段階に分けて調査を実施しました。両段階とも、クラウドコンピューティングに最も関連する脅威、脆弱性やリスクセキュリティ課題に関心を持つサイバーセキュリティ専門家の考えや意見を収集し、2022年の重大脅威を特定することを最終目的としました。

最初の調査段階では、ワーキンググループのメンバを対象にした対面調査から、クラウドセキュリティの課題の短いリスト作成を目標としました。本グループは、まず前回のレポート(クラウドコンピューティングの重大脅威:11の悪質な脅威2019)に掲載されている11の重大脅威(セキュリティ課題)から始まり、議論を通じて15の新しい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に、各自の組織にとっての重要度や、各自の身近な組織に関する知識を示してもらいながら、26の課題を一連の会議で検討しました。

また、この調査の初期段階では、ワーキンググループのメンバは、26のリストに含まれていない懸念事項を追加で提案することもできました。すべての情報を検討した結果、ワーキンググループは、最も顕著なクラウドのセキ

© Copyright 2022, Cloud Security Alliance. All rights reserved.

ュリティ課題の上位19項目を特定しました。

調査の第2段階では、この凝縮された19のセキュリティ課題を、主に本ワーキンググループ以外のセキュリティ専門家を対象にしたオンライン調査によって、重要度に基づいてランク付けすることを主眼としました。その重要性を反映させるために、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、各クラウドセキュリティ課題を1から10で評価するよう指示され、1は「非常に重要でない」、10は「非常に重要である」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「重大脅威11」です。

Survey Results Rank	Survey Average Score	Issue Name
1	7.729927	不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理、ならびに特権アカウント
2	7.592701	セキュアでないインターフェースやAPI
3	7.424818	設定ミスと不適切な変更管理
4	7.408759	クラウドセキュリティのアーキテクチャと戦略の欠如
5	7.275912	セキュアでないソフトウェア開発
6	7.214493	セキュアではないサードパーティーのリソース
7	7.143066	システムの脆弱性
8	7.114659	予想外のクラウドデータ公開
9	7.097810	サーバレスやコンテナワークロードの構成ミスやエクスプロイト
10	7.088534	組織的な犯罪、ハッカーとAPT
11	7.085631	クラウドストレージデータ流出

これら11の「重大脅威」を特定した上で、ワーキンググループは各課題について分析を行いました。各分析では、項目、CSPまたはクラウド利用者が共有責任を所有しているかどうかを説明し、クラウドスタックおよびクラウドサービスの種類（SaaS、PaaS、IaaSまたはSPI）モデル内のどこに存在するかを定義しています。ビジネスへの影響、要点、想定事例と実例をもとに、各リスクに関し、どこでどのような影響が予測できるかを説明します。CSAの製品を通じて説明される概念的推論と緩和策には、The Security GuidanceのCommon Body of Knowledge (CBK) v4ドメインマッピング、Cloud Controls Matrix (CCM) v4コントロール、STRIDE脅威モデリングへの関連性、想定事例の詳細に関する参照リンクが含まれています。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティの課題1:
不十分なアイデンティティ、クレデンシャル、アクセスおよび鍵の管理、ならびに特権アカウント

Security Responsibility	
✓ Customer	
✗ Cloud Service Provider	
✗ Shared	
Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra
Cloud Service Model	
✓ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

アイデンティティ、クレデンシャル、アクセス管理システムには、組織が貴重なリソースへのアクセスを管理、監視、セキュアにするためのツールやポリシーが含まれています。例えば、電子ファイル、コンピュータシステム、サーバールームやアイデンティティ、クレデンシャル、アクセス管理システムには、組織が貴重なリソースへのアクセスを管理、監視、セキュアにするためのツールやポリシーが含まれています。例えば、電子ファイル、コンピュータシステム、サーバールームや建物などの物理的なリソースが含まれる場合があります。

適切なメンテナンスと継続的な警戒が重要です。IAM（アイデンティティ・アンド・アクセス・マネジメント）においてリスクスコアリングを使用することで、セキュリティ体制を強化することができます。明確なリスク割り当てモデルを使用し、入念に監視し、その動作を適切に分離することで、IAM システムのクロスチェックが可能になります。リスクスコアリングのためのターゲットアクセスや頻度の追跡も、リスクの状況を理解するために重要です。

特権アカウントは、オフボーディングや役割変更後の担当者によるアクセスを防ぐために、正確かつ迅速な方法で無効化される必要があります。これにより、データの流出や侵害の可能性を低減することができます。特権アカウントの無効化以外では、役割と責任がNeed-to-Knowの権限のレベルと一致することが必須です。複数の過剰な権限を持つ担当者がいると、データの誤操作やアカウントの乗っ取りが発生する可能性が高くなります。

ビジネスインパクト

不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵管理、ならびに特権アカウントによる悪影響は、以下を含む場合があります。

- 後手後手の過剰なロックダウンによる業績悪化と生産性の低下
- 従業員のテスト疲れによるコンプライアンス不足とセキュリティへの無関心
- データの置き換えや破損と、不正または悪意のあるユーザによるデータの流出の比較
- 市場からの信頼と収益の損失
- インシデント対応およびフォレンジックにかかる金銭的費用
- ランサムウェアとサプライチェーンの混乱

© Copyright 2022, Cloud Security Alliance. All rights reserved.

要点

適切なIAM、クレデンシャル、鍵管理の結果には、以下のようなものがあります。

1. エンタープライズアーキテクチャの中核をなす強固な防御は、ハッキングの標的を攻撃がより容易なエンドポイントユーザのアイデンティティへ移します。
2. 堅牢なゼロ・トラストレイヤには、個別のユーザに対する単純な認証や、アプリケーションベースの隔離以上のものが必要です。
3. 運用ポリシーや構造化リスクもまた、CIEMのような先進的なツールに不可欠なモデルです。[1]
4. ユーザオブジェクトには、ビジネスの要求に応じて動的に調整されるリスクスコアを与えなければなりません。信頼は獲得されるべきもので、単に鍵やコードを提供することではありません。

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。

- (2021）国家による攻撃は増加傾向にあり、より巧妙になっています。2021年は、Twitch、Cosmology Kozmetik、PeopleGIS、Premier Diagnostics、SeniorAdvisor、Reindeer、Twilloを巻き込んだ侵入があり、これらの攻撃の大半は内部脅威からの特権乱用でした。リスクとレジリエンスを監視していない企業は、ダイナミックな脅威の状況に足元から直面しています。[2]
- (10/2021) SEGA Europeのクラウドのケースを詳しく見ると、2つの重要な構成管理クラウドの設定ミスが浮き彫りになりました - AWS S3バケットがパブリックアクセス権限に設定されていました。ハードコードされたクレデンシャルは、クラウドに保存されていました。AWSとCDNネットワークにおけるコンテンツの置き換えは、サンドボックスへの取り込みが実装され、システムによる変更の検証やアクセスコンテキストにリスクスコアを付ける時間をより多く確保することが出来ていれば、回避できたはずです。[3]
- (2019/1～2019/7) CapitalOne AWSの内部者漏洩では、借用した動的IAMロールが漏洩の鍵になりました。他の多くの侵害のようにS3バケットがインターネットに露出されたわけではありませんが、過剰なIAMロールを持つEC2インスタンスが原因であった可能性があります。[4]

CSA CBK Security Guidance Version 4.0

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 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
Domain 14:関連技術

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CCM Controls Version

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 変更管理と構成管理

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の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、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のポリシーと手順
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 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

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. CIEM Home - CIEM - HOME (ciemgroup.com)
✗	Tampering with Data	2. Worst AWS Data Breachest of 2021 https://sonraisecurity.com/blog/worst-aws-data-breaches-of-2021/
✗	Repudiation	3. SEGA Europe Thoroughly Scrutinizes its Cloud Security https://vpnoverview.com/news/sega-europe-security-report/ Securin Blog | Lessons Learned from SEGA Europe's recent security blunder SEGA Barely Avoided Huge Data Breach After It Left Database Publicly Open | Eyerys
✓	Disclosure	4. The Capital One - AWS incident highlights the roles and responsibilities of cloud customers, providers https://diginomica.com/capital-one-aws-incident-highlights-roles-and-responsibilities-cloud-customers-providers
✗	Denial of Service	
✗	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティの課題2:
セキュアでないインターフェースやAPI

Security Responsibility	
✓ Customer	
✓ Cloud Service Provider	
✗ Shared	
Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra
Cloud Service Model	
✓ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

APIの利用はますます盛んになっており、これらのインターフェースをセキュアにすることが最も重要な課題となっています。APIやマイクロサービスは、設定の誤り、不適切なコーディング手法、認証の欠如、不適切な認可による脆弱性をチェックする必要があります。このような見落としがあると、悪意のある行為に対してインターフェースが脆弱になる可能性があります。

一般的な例としては、1. 未認証のエンドポイント、2. 弱い認証、3. 過剰な権限、4. 標準的なセキュリティコントロールの無効化 5.パッチ未適用のシステム、6. 論理設計上の課題、および7. ロギングまたはモニタリングの無効化APIなどのインターフェースの設定ミスは、インシデントやデータ侵害の主な原因となっています。これらは、リソースの流出、削除または変更、データの調整、サービスの中断を引き起こす可能性があります。

企業は、接続性と俊敏性を向上させるために（プロバイダと利用者の両方で）APIを急速に採用しています。

これには、API開発者と利用者がデジタル体験を利用できるようになるという利点があります。開発者は、APIの急速な成長と普及により、これらのAPIの管理とセキュリティ確保という難題に直面しています。Akamai 2021 のレポートによると、「（前年）、Akamaiは 300 兆を超える API リクエストを配信し、前年比 53% 増となった」との記述があります。[1] 様々なタイプの API プロバイダと利用者のパターンが複雑に絡み合っていることも、API のカタログ化さえも難しくしています。API のカタログには、内部向けか外部向けか、何に使われるか、どのようなデータが公開され、どのように消費されるかなどの詳細を記載する必要があります。APIがデジタルエコシステムを効率化するように、クラウド技術はAPIを迅速かつ容易に作成または使用するための触媒となります。拡張と自動化のためには、複数のテクノロジーやクラウドサービスプロバイダ間でセキュリティパターンを標準化する必要があります。また、継続的なモニタリングやテストも、現在の指数関数的な速度では問題が生じるでしょう。

ビジネスインパクト

セキュアでないインターフェースやAPIのリスクは、APIに関連する使用状況やデータ、また脆弱性の発見と緩和の速さによって変化します。

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密データや個人データの意図しない暴露です。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

要点

以下、主な要点を列挙します。

1. API提供により提供されるアタック・サーフェスは、追跡、設定、およびセキュリティ保護される必要があります。
2. クラウドベースのAPIの成長と変化に対応するために、従来のコントロールや変更管理のポリシーやアプローチを更新する必要があります。
3. 企業は自動化を受け入れ、異常なAPIトラフィックを継続的に監視し、問題をほぼリアルタイムで修正する技術を採用する必要があります。

想定事例と実例

セキュアでないインターフェースやAPIに最近の課題は次の通りです。

1. (2021年4月28日）KrebsOnSecurityの調べによると、エクスペリアンのパートナーサイトでは、名前と住所を入力するだけで、誰でも数千万人のアメリカ人のクレジットスコアを調べることができると、セキュリティ研究者によって報告されたそうです。このデータセットは信用調査会社エクスペリアンのものですが、このサービスは第三者によって提供されていました。[2]
2. (2021年5月5日）壊れたユーザ認証と壊れたオブジェクトレベルの認可が原因となり、APIを経由の直接呼び出しによって、Pelotonの顧客のPIIを露出しました。これには、ユーザID、位置情報、体重、性別、年齢などが含まれていました。[3]
3. (2021年4月22日）農業機械、重機、芝生管理機器などのメーカーであるJohn Deere社が、認証やレート制限を行わずにユーザ名をクエリする機能を公開しました。その結果、Fortune 1000企業の20%近くがJohn Deere社のアカウントを持っていることが分かりました。さらに調査を進めると、車体番号のAPI検索により、住所やトラクター名など、機器の所有者情報が判明しました。[4]

CSA CBK Security Guidance Version 4.0

Domain 4: コンプライアンス・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: インフラセキュリティ
Domain 8: 仮想化・コンテナ
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

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CCM Controls Version

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 変更管理と構成管理

CCC-01:変更管理ポリシーと手順

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の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-04:データ分類

DSP-05:データフロー文書

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

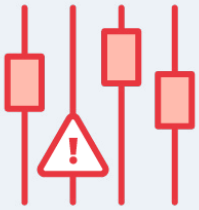
IVS-04:OS要塞化とベースライン制御

IVS-09:ネットワーク防御

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. Akamai Report: https://www.ir.akamai.com/static-files/1ef574a5-ae14-48f6-854a-47d96c4a75fe
✓	Tampering with Data	2. Experian API Exposed Credit Scores of Most Americans: https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/
✗	Repudiation	3. Peloton's Leaky API Spilled Riders' Private Data: https://threatpost.com/pelotons-spilled-riders-data/165880/
✓	Disclosure	4. Leaky John Deere API's:Serious Food Supply Chain Vulnerabilities: https://sick.codes/leaky-john-deere-apis-serious-food-supply-chain-vulnerabilities-discovered-by-sick-codes-kevin-kenney-willie-cade/
✗	Denial of Service	
✗	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティの課題3:
設定ミスと不適切な変更管理



Security Responsibility	
✓ Customer	
✓ Cloud Service Provider	
✓ Shared	
Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra
Cloud Service Model	
✓ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

設定ミスとは、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ままとなっている、コンピューティング資産の不正確または最適とは言えない設定のことです。システムに関する知識やセキュリティ設定への理解の欠如、悪意などが、設定ミスへと繋がります。よくある設定ミスには次のようなものがあります。

1.セキュリティが確保されていないデータストレージ要素やコンテナ、2.過剰な権限、3.変更されないままとなっているデフォルトのクレデンシャルおよび構成設定、4.無効化された標準的なセキュリティコントロール 5.パッチが適用されていないシステム、6.ロギングの無効化またはモニタリングの無効化、7.ポートおよびサービスへの無制限のアクセス、8.セキュアでないシークレット管理、および9.設定不良または設定検証の不足。クラウドリソースの設定ミスはデータ侵害の主な原因であり、リソースの削除や変更、サービスの中断を受け入れてしまう可能性があります。

クラウド環境における不適切な変更管理は、誤った設定をもたらし、設定ミスの修正を妨げてしまいます。クラウド環境やクラウドコンピューティングの手法は、変更をコントロールすることがより困難な点で、従来の情報技術（IT）とは異なります。従来の変更プロセスは、複数の役割と承認を必要とするため、本番環境に到達するまでに数日から数週間を要しました。クラウドコンピューティングのベストプラクティスは、急速な変更を支援する、自動化、役割の拡張、アクセスによって成り立っています。企業のデータセンターでは静的であるインフラ要素が、クラウド環境ではコードとして抽象化されることがあります。さらに、複数のクラウドプロバイダを利用すると、各プロバイダ独自の機能がほぼ毎日強化・拡張され、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

ある設定ミス／不適切な変更管理の影響は、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。Certificate of Cloud Auditing Knowledge Study Guideを使用すると、影響の分類は次のようになります。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

1. データの開示 - 技術的影響 - 機密保持
2. データの損失 - 技術的な影響 - 可用性
3. データの破壊 - 技術的影響 - 完全性
4. システムパフォーマンス - 運用への影響
5. システム障害 - 運用への影響
6. 身代金要求 - 財務的影響
7. コンプライアンス違反と罰金 - コンプライアンスと財務的影響
8. 失われた収入 - 財務的影響
9. 株価の下落 - 財務的影響
10. 企業の評判 - 信用・評判（レピュテーション）への影響

要点

要点は次の通りです。

- 企業は、設定ミスのあるリソースを継続的にスキャンし、リアルタイムで脆弱性を修正することができる、利用可能な技術を採用する必要があります。
- 変更管理のアプローチは、継続的なビジネス変革の絶え間ないダイナミックな性質とセキュリティの課題を反映し、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ようにする必要があります。

想定事例と実例

設定ミスと不適切な変更管理に起因する最近のインシデントには、次のものがあります。

1. (2022年3月9日）テストを行ったServiceNowインスタンスの約70%に、顧客管理のServiceNowのACL（アクセス制御リスト）での設定ミスや、ゲストユーザへの権限の過剰プロビジョニングなどの、セキュリティ課題があったことが報告されました。[1]
2. (2021年10月4日）Facebook傘下のアプリ「Facebook」「Instagram」「Whatsapp」「Oculus」がオフラインになりました。誤った設定変更により、データセンター間のネットワークトラフィックを調整するバックボーンルータに課題が発生し、通信が中断されました。ネットワークトラフィックの障害は、データセンターの通信に連鎖的に影響を及ぼし、サービスを停止させました。この障害は、日々の業務で使用する内部ツールやシステムの多くにも影響を及ぼし、課題の診断と解決を複雑なものにしました。[2]
3. (2021年1月7日）マイクロソフトが、サードパーティーのデータを格納する自社のMicrosoft Azure Blob（クラウドストレージ）バケットの設定を誤って構成していたことが報じられました。マイクロソフトとのパートナー提携を希望する100以上の企業のアイデアと知的財産を含む「スライドデック」とソースコードが漏えいしました。[3]

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CBK Security Guidance Version 4.0

Domain 4:コンプライアンス・監査マネジメント
Domain 5:情報ガバナンス
Domain 6:マネジメントプレーンと事業継続
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

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 事業継続マネジメントとオペレーショナルレジリエンス

BCR-02:リスクアセスメントと影響度分析
BCR-03:事業継続の戦略
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、暗号化、鍵管理

CEK-03:データ暗号化
CEK-05:暗号化変更管理

DSP データセキュリティとプライバシーの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:デザインおよびデフォルトによるデータ保護
DSP-17:機微なデータの保護

GRC ガバナンス・リスク・コンプライアンス・マネジメント

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 人的資源

HRS-09:人事部の役割と責任
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管理

IAM-03:アイデンティティ・インベントリ
IAM-08:ユーザ 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のセキュリティ強化とベースコントロール

LOG ロギング＆モニタリング

LOG-03:セキュリティ監視とアラート
LOG-05:監査ログの監視と対応
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-Discovery、クラウド・フォレンジック

SEF-03 インシデント対応計画
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

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Stride Threat Analysis	
✓	Spoofing Identity
✓	Tampering with Data
✓	Repudiation
✓	Disclosure
✓	Denial of Service
✓	Elevation of Privilege

Reference Links

1. Major Security Misconfiguration Impacting ServiceNow Instances Discovered
https://appomni.com/press_release/2022-major-security- misconfiguration-impacting-servicenow-and-other-saas- instances-discovered/
Major Security Misconfiguration Impacting ServiceNow and Other SaaS Instances Discovered
https://appomni.com/resources/aolabs/appomni-discovers- security-misconfiguration-impacting-servicenow/
ServiceNow Shared Security Model and Access Control Information
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1095978
ServiceNow releases guidance on Access Control List misconfigurations
https://www.zdnet.com/article/servicenow-releases-guidance-on-access-control-list-misconfigurations-after- report-highlights-prevalence/
2. Understanding How Facebook Disappeared from the Internet
https://blog.cloudflare.com/october-2021-facebook-outage/
Update about the October 4th outage
https://engineering.fb.com/2021/10/04/networking-traffic/ outage/
More details about the October 4 outage
https://engineering.fb.com/2021/10/05/networking-traffic/ outage-details/
Why Facebook, Instagram, and WhatsApp All Went Down Today
https://www.wired.com/story/why-facebook-instagram- whatsapp-went-down-outage/
3. Report:Software Companies Exposed to Hacking in Major Data Breach
https://www.vpnmentor.com/blog/report-microsoft-dynamics-leak/

Additional:

4. Report:Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach
https://www.websiteplanet.com/blog/prestige-soft-breach- report/
Leaky AWS S3 bucket once again at centre of data breach
https://www.computerweekly.com/news/252491842/Leaky- AWS-S3-bucket-once-again-at-centre-of-data-breach
5. Unsecured-aws-server-exposed-airport-employee-records-3tb- in-data
https://www.zdnet.com/article/unsecured-aws-server- exposed-airport-employee-records-3tb-in-data/
6. https://www.zdnet.com/article/amazon-steps-in-to-close- exposed-flexbooker-bucket-after-december-data-breach/

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティ課題4：クラウドセキュリティのアーキテクチャと戦略の欠如

クラウドセキュリティ戦略とセキュリティアーキテクチャは、クラウド導入モデル、クラウドサービスモデル、クラウドサービスプロバイダ（CSP）、サービス地域の可用性ゾーン、特定のクラウドサービス、一般原則[2]、事前決定[3]などの検討と選択を包含しています。さらに、異なるクラウドアカウント、ベンダー、サービス、および環境にまたがるIAM[4]、ネットワーク、セキュリティコントロールの将来を見据えた設計がスコープに含まれます。戦略的な考慮はデザインを優先して記述されるべきものですが、一般的には、クラウドにチャレンジするには、段階的かつ機動的なアプローチが求められます。

Security Responsibility	
✓ Customer	
✗ Cloud Service Provider	
✗ Shared	
Architecture	
✓ Application	✓ Meta
✓ Info	✓ Infra
Cloud Service Model	
✓ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

クラウドインフラ管理は、変化のスピードが速く、分散型セルフサービス方式が一般的であるため、技術やビジネスに関する考慮や意識的な設計を行うことができません。しかし、クラウドの試みを成功させ安全にするためには、セキュリティへの配慮とリスクを無視することはできません。業界の違反に関する想定事例によると、このような計画が欠けていると、クラウド環境とアプリケーションがサイバー攻撃に耐えられなくなったり、効率的に攻撃されたりする可能性があることがわかります。このような課題への挑戦は、クラウドのセキュリティ戦略や設計の容易な実装に貢献可能です。

ビジネスインパクト

クラウドのセキュリティ戦略やアーキテクチャが存在しないと、企業やインフラのセキュリティアーキテクチャを効果的かつ効率的に実装することが制限されます。これらのセキュリティ/コンプライアンス目標が達成されないと、罰金や違反が発生したり、回避策の実施、リファクタリング、移行にコストがかかります。

[2] 一般的なクラウドコンピューティングの原則には、影響（国や社会）を考慮したCSPの選択（「ローカルファースト」など）や、オンデマンドサービスの消費および課金モデルの回避に対する許容度などが含まれます。

[3] 事前決定には、既存のベンダーへのロックイン、ローカルデータ・レジデンシー要件を持つ特定の地域での事業拡大、特定のCSPやモデル（銀行でも採用されようとしている0-servers footprint など）を全社的に好む場合などが含まれます。

[4] 特定のクラウドサービスのことではなく、1 つのドメインとしてのIDとアクセス管理の意。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

要点

ここでは、その要点をご紹介します。

- 企業は、クラウドサービスやインフラの設計や決定において、ビジネス目標、リスク、セキュリティ脅威、法令遵守を考慮する必要があります。
- クラウドサービスやインフラの戦略・設計原則は、変化のスピードが速く、集中管理が限定的であることから、策定や遵守がより重要であると考えてください。
- デューデリジェンスとサードパーティーベンダーのセキュリティ評価を基礎的なプラクティスとして考慮してください。また、脅威のモデル化、ベンダーの障害による影響を見据えたセキュアな設計と統合で補完してください。

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。

- (2021年1月）ウォルマート傘下の米衣料品店ボノボスが、数百万人の顧客の個人情報を流出させる大規模なデータ侵害に遭いました。ShinyHuntersと呼ばれる脅威者は、顧客の住所、電話番号、クレジットカード番号の一部、およびサイト上での注文を含むBonobosのデータベース全体（700万人のユーザレコードを含む70GBのSQLデータベース）を投稿しました。これは、バックアップファイルをホストする外部のクラウドバックアップサービスが侵害されたために発生しました。アクセス制御、暗号化、ベンダーのセキュリティ、冗長性、その他の領域を選択することで、同様の侵害の影響や可能性を抑えることができます。[1] [2]
- (2021年7月2日） Kaseyaは、顧客から、Kaseyaが管理するエンドポイント上で異常な動作やマルウェアが実行されていることを示唆する報告を受けました。攻撃者は、仮想ストレージアプライアンス（VSA）製品のゼロデイ脆弱性をエクスプロイトし、認証を回避して任意のコマンドを実行することができます。これにより、攻撃者は、VSA製品の標準機能を利用して、MSP（Manage Service Provider）クライアント（つまり、サービス利用者の顧客）のエンドポイントにランサムウェアを展開することができました。この障害は、異なる環境に展開されたソフトウェアに対して、ゼロタッチで自動更新する戦略により、多くのお客様に影響を与えました。ベンダーと利用者は、将来的に同様の攻撃を制限するために、この戦略を再考することができます。[3]

CSA CBK Security Guidance Version 4.0

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 6:マネジメントプレーンと事業継続

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CCM Controls Version 4.0

A&A 監査・保証

A&A-03 リスクベースド・プランニング評価

A&A-04 要求事項への対応

AIS アプリケーションおよびインターフェースのセキュリティ

AIS-04 セキュアアプリケーションの設計と開発

BCR 事業継続マネジメント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-03 事業継続の戦略

BCR-04 事業継続計画

BCR-08 バックアップ

CEK 暗号、暗号化、鍵管理

CEK-08 CSC 鍵管理能力

CEK-07 暗号化リスク管理

DCS データセンター・セキュリティ

DCS-01 オフサイト機器廃棄方針と手順

DSP データセキュリティとプライバシーの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-05 データフロー文書

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-09 データ保護影響評価

GRC ガバナンス、リスク、コンプライアンスマネジメント

GRC-08 Special Interest Groups

GRC-02 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-04 職務の分離

IAM-05 最小権限

IAM-09 特権的なアクセスロールの分離

IAM-01 アイデンティティとアクセスの管理

IAM-06 ユーザアクセスプロビジョニング

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に関する方針と手順

IVS インフラストラクチャと仮想化のセキュリティ

IVS-03 ネットワークセキュリティ

IVS-05 本番環境と非本番環境

IVS-08 ネットワークアーキテクチャの文書化

IVS-06 分割と分離

STA サプライチェーンの管理、透明性、説明責任

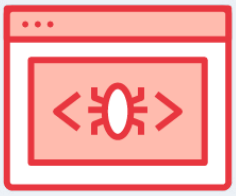
STA-01 セキュリティ責任共有モデル (SSRM) の ポリシーと手順

STA-08 サプライチェーンリスクマネジメント

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. Incident Overview & Technical Details https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961
✓	Tampering with Data	2. Independence Day:REvil uses supply chain exploit to attack hundreds of businesses https://news.sophos.com/en-us/2021/07/04/independence- day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	3. Data breach at Bonobos hits up to 7 million:What to do [updated] https://www.tomsguide.com/news/bonobos-data-breach-7- million
✓	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティ課題5：
セキュアでないソフトウェア開発



ソフトウェアは複雑であり、クラウド技術はさらに複雑さを増す傾向にあります。その複雑さの中で、意図しない機能が出現し、エクスプロイト攻撃[1]や設定ミスが発生する可能性があります。クラウドが利用しやすくなったおかげで、脅威者はこれらの「機能」を以前よりも簡単に活用できるようになりました。

Security Responsibility	
✔ Customer	
✔ Cloud Service Provider	
✔ Shared	
Architecture	
✔ Application	✘ Meta
✘ Info	✘ Infra
Cloud Service Model	
✔ Software as a Service (SaaS)	
✔ Platform as a Service (PaaS)	
✔ Infrastructure as a Service (IaaS)	

クラウドファーストの戦略的な姿勢を採用することで、企業は保守とセキュリティの問題をクラウドサービスプロバイダ（CSP）に任せることができるようになります。インフラやプラットフォーム層の管理をCSPに任せることで、開発者が車輪の再発明をすることを防ぐことができます。鍵の保管・管理、セキュアなCI/CD（Continuous Integration/Continuous Deployment）のサービスにより、開発者はビジネスロジックに集中することができます。

CSPは、IDおよびアクセス管理（IAM）のための機能を提供し、開発者に審査ツールや適切な実装に関するガイダンスを提供します。これによって、企業は、自社でサービスを作る必要がなくなり、その分、より影響力があり優先的なビジネスにリソースを投下することができます。

各開発者が、CSPと企業が責任を共有するという前提を理解できるようにするためには、教育が必要です。例えば、Kubernetesに対する0-dayエクスプロイトが報告され、企業がCSPのKubernetesソリューションを活用している場合、その課題を軽減する責任はCSPが負うことになります。クラウドネイティブテクノロジーを使用したWebアプリケーションで、ビジネスエラーが発生した場合、開発者の責任で修正する必要があります。いずれの場合も、結果として生じる情報開示は、企業に影響を与えます。

セキュアでないソフトウェアを作ろうとする開発者はいません。しかし、システムの機密性、完全性、可用性に影響を与える可能性のあるバグを修正するパッチは、毎月、主要ソフトウェアベンダーからリリースされています。すべてのソフトウェアのバグがセキュリティに影響を与えるわけではありませんが、歴史が証明しているように、想定外の動作であっても重大な脅威を引き起こす可能性があります。[2] クラウド技術を利用することで、企業は自社のビジネスに特化することができ、コモディティ化する可能性がある他のすべての分野をCSPに所有・管理させることができます。

ビジネスインパクト

セキュアでないソフトウェア開発がもたらす影響には、次のようなものがあります。

- 製品・ソリューションに対するお客様の信頼の失墜
- データ侵害によるブランドの信用失墜

© Copyright 2022, Cloud Security Alliance. All rights reserved.

- 訴訟による法的・経済的影響

要点

要点は次の通りです。

- クラウドテクノロジーを使用することで、既存のソリューションの再構築を防ぎ、開発者がビジネス固有の課題に集中できるようになります。
- 共有された責任モデルを活用することで、パッチ適用などの項目は、ビジネスではなくCSPによって所有される可能性があります。
- CSPはセキュリティを重視しており、Well Architected Frameworkやセキュアな設計パターンなど、セキュアな方法でサービスを実装する方法に関するガイダンスを提供します。

想定事例と実例

アカウントハイジャックに関連する課題の最近の事例には、次のものがあります。

- (2021年12月9日) 悪名高いLog4Shellの脆弱性では、log4jライブラリ[3]の構文解析バグにより、些細な操作でのRCEを実行可能にしました。
- (2021年1月5日) Microsoft Exchange のProxyOracleやProxyShellに属する脆弱性が公表され、リモートコード実行とクレデンシャルの盗難[4]に関するいくつかの方法が明らかになりました。
- (2021年9月13日) Apple のiOS では、NSO社の「Pegasus」ソフトウェアを用いてエクスプロイトされる可能が発見されました。これはリモートコード実行[5]できるゼロクリック脆弱性を活用しています。

CSA CBK Security Guidance Version 4.0

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 10:アプリケーションセキュリティ

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 13:Security as a Service

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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
AIS-05:アプリケーションセキュリティテストの自動化 AIS-06:セキュアなアプリケーション導入の自動化

CCC 変更管理と構成管理

CCC-02:品質テスト

TVM 脅威と脆弱性の管理

TVM-04: 検出の更新

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のポリシーと手順
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

	Stride Threat Analysis	Reference Links
✓	Spoofing Identity	1. I always call them glue bugs, I think I got that from you! https://twitter.com/taviso/status/1379447309864345602
✓	Tampering with Data	2. An Exploration of JSON Interoperability Vulnerabilities https://bishopfox.com/blog/json-interoperability-vulnerabilities
✓	Repudiation	3. Log4Shell:RCE 0-day exploit found in log4j 2, a popular Java logging package https://www.lunasec.io/docs/blog/log4j-zero-day/
✓	Disclosure	4. A New Attack Surface on MS Exchange Part 1 - ProxyLogon! https://blog.orange.tw/2021/08/proxylogon-a-new-attack- surface-on-ms-exchange-part-1.html
✓	Denial of Service	5. A deep dive into an NSO zero-click iMessage exploit:Remote Code Execution https://googleprojectzero.blogspot.com/2021/12/a-deep- dive-into-nso-zero-click.html
✓	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティ課題6：セキュアでないサードパーティーのリソース

クラウドコンピューティングの導入が急速に進む中、サードパーティーリソースは、オープンソースのコードから、SaaS製品やAPIリスク（セキュリティ課題2）、そしてクラウドベンダーが提供するマネージドサービスまで、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、製品やサービスを提供するプロセスの一部であるため、サプライチェーンの脆弱性とみなされます。これらのリスクは、消費されるすべての製品・サービスに存在します。それでも、近年はサードパーティーのサービスやソフトウェアベースの製品への依存度が高まっているため、こうした脆弱性のエクスプロイトやハッキング可能な構成がより多く発生しています。実際、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、サプライヤーやサードパーティーの脆弱性が原因となっています。

Security Responsibility
✔ Customer
✘ Cloud Service Provider
✘ Shared

Architecture	
✔ Application	✔ Meta
✔ Info	✔ Infra

Cloud Service Model
✔ Software as a Service (SaaS)
✔ Platform as a Service (PaaS)
✔ Infrastructure as a Service (IaaS)

製品やサービスとは、サプライヤーやサードパーティーで用いられている他のすべての製品やサービスの総和であるため、エクスプロイトはチェーンのどのポイントからでも始まり、そこから拡散していく可能性があるのです。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。ソフトウェアの世界では、SaaSやオープンソースを利用して規模を拡大することが一般的です。悪意のあるハッカーは、同じエクスプロイトでより多くのターゲットを傷つけ、成長する機会を得ることができるのです。

ビジネスインパクト

- 重要なビジネスプロセスの損失または停止
- 業務データが外部からアクセスされる（セキュリティ課題11）
- セキュリティ課題のパッチや修正は、プロバイダーとその対応スピードに依存します。修正プログラムを提供した後、統合のために社内のアプリケーションや製品のアップデートが必要になる場合もあります。アプリケーションにおける脆弱なコンポーネントの重要性によっては、ビジネスへの影響が極めて大きくなる可能性があります。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

要点

ここでは、その要点をご紹介します。

- 自分が作ったものではないコードや製品の脆弱性を防ぐことはできませんが、どの製品を使うかについて適切な判断をするように努めることはできます。また、公式にサポートされている製品、コンプライアンス認証を受けている製品、セキュリティへの取り組みについてオープンに話している製品、バグバウンティプログラムを持っている製品、セキュリティ課題を報告し、迅速に修正を提供することでユーザに責任を持って対応している製品を探してみてください。
- お客様が利用している第三者を特定し、追跡します。被害者リストが公開されて初めて、脆弱な製品を使っていたことに気づくということは避けたいものです。これには、オープンソース、SaaS製品、クラウドプロバイダ、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。
- サードパーティー資源の定期的な見直しを行います。不要な製品が見つかった場合は、それらを削除し、コードリポジトリ、インフラストラクチャ、またはアプリケーションに付与した可能性のあるアクセス権や権限をすべて取り消します。
- 最も弱いリンクにならないようにします。自社に最適なスコープでアプリケーションのペネトレーションテストを行い、開発者にセキュアなコーディングについて教え、静的アプリケーションセキュリティテスト（SAST）と動的アプリケーションセキュリティテスト（DAST）ソリューションを使用します。

想定事例と実例

最近のサードパーティー関連では、以下のような課題があります。

- (2020年12月13日、2021年4月6日まで） Solarwinds社は、米国に本社を置くネットワーク監視会社です。2020年、同社の政府および民間の顧客数千人が、Solarwinds社のネットワークと製品から、顧客のネットワーク、クレデンシャルおよび個人情報へとつながる、様々なベクトルを用いたサプライチェーン攻撃で被害を受けたことが公表されました。この攻撃の本当の効果はまだ不明です。流出した機密データによっては、ネットワークやサーバを丸ごと再構築しなければならない組織もありました。[1] [2]
- (2021年11月） Log4shellは、オープンソースのJavaロギングフレームワークとして人気の高いLog4jに発見されたゼロデイ脆弱性です。この脆弱性は2021年11月に公開され、その数日後にパッチが適用されました。このフレームワークの人気から、過去最大の脆弱性と言われています。攻撃者は、この脆弱性を暗号マイニング、ランサムウェア攻撃、ボットネット、およびスパムメールに利用しました。[3] [4]
- (2019年5月から2021年8月まで) フォルクスワーゲングループの北米子会社は、2019年5月から2021年8月までの約2年間、あるベンダーがストレージサービスを無防備にしたことによるデータ侵害の被害に遭いました。流出したデータには、個人を特定できる情報（PII）や、一部の顧客にとってはより機密性の高い財務データが含まれ、330万人の顧客が関与していました。[5] [6]

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CBK Security Guidance Version 4.0

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 7:インフラストラクチャ・セキュリティ
Domain 10:アプリケーションセキュリティ
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)

CSA CCM Controls Version 4.0

BCR 事業継続マネジメントとオペレーショナル・レジリエンス

BCR-01:事業継続管理ポリシーと手順
BCR-02:リスク評価と影響分析
BCR-03:事業継続の戦略

CCC 変更管理と構成管理

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

DCS データセンタセキュリティ

DCS-05: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の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

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

STA サプライチェーンの管理、透明性、説明責任

STA-01:セキュリティ責任共有モデル (SSRM)のポリシーと手順
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

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. Solarwinds the supply chain hack https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/ 2. Using Microsoft for the Solarwinds hack https://www.reuters.com/article/us-global-cyber-usa-idUSKBN28Y1BF 3. Log4J hack https://blog.cloudflare.com/inside-the-log4j2-vulnerability- cve-2021-44228/ 4. More than 1.2m attacks using log4j https://www.ft.com/content/d3c244f2-eaba-4c46-9a51-b28fc13d9551 5. Volkswagen and Audi customer's data leakage https://www.bleepingcomputer.com/news/security/audi-volkswagen-data-breach-affects-33-million-customers/ 6. Two third of breaches are supply chain attacks https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk
✗	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✓	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティの課題7：
システムの脆弱性

Security Responsibility
✔ Customer
✔ Cloud Service Provider
✔ Shared

Architecture	
✔ Application	✔ Meta
✔ Info	✔ Infra

Cloud Service Model
✔ Software as a Service (SaaS)
✔ Platform as a Service (PaaS)
✔ Infrastructure as a Service (IaaS)

システムの脆弱性とは、クラウドサービス基盤に存在する欠陥のことです。システムをエクスプロイトされ、データの機密性、完全性、可用性が損なわれ、サービスの運営に支障をきたす可能性があります。すべてのコンポーネントには、クラウドサービスを攻撃対象にする可能性のある脆弱性が含まれている可能性があります。セキュリティリスクを軽減するためには、以下の脆弱性カテゴリーに対応したセキュリティ強化を実施することが不可欠です。

システムの脆弱性は、大きく4つに分類されます。

- ゼロデイ脆弱性 - 新たに発見された、パッチが存在しない脆弱性。ハッカーは、パッチが配布されるまでは脆弱性を止める手段がないため、このような脆弱性をエクスプロイトするために素早く行動します。最近発見されたLog4Shellは、広く導入されているJavaベースのLog4jログ機能を使用するサービスに影響を与える深刻なゼロデイ脆弱性の顕著な例です。
- セキュリティパッチの欠落 - 既知の重要な脆弱性に対するパッチが利用可能になり次第、できるだけ早くそれを展開することで、システムの攻撃対象領域を減らすことができます。時間の経過とともに、新たなシステム脆弱性が発見され、パッチが提供されます。パッチを適用していない脆弱性の数が増えれば、システム全体のセキュリティリスクも高まります。
- 設定に基づく脆弱性 - この種の脆弱性は、システムがデフォルトまたは誤った設定のままデプロイされた場合に発生します。設定ベースの脆弱性の例としては、レガシーセキュリティプロトコルの使用、脆弱な暗号化方式、脆弱な権限管理、保護が不十分なシステム管理インターフェースなどが挙げられます。システム上で不要なサービスを実行することも、設定に関連する課題です。
- 弱いまたはデフォルトの認証クレデンシャル - 強固な認証クレデンシャルがないため、潜在的な攻撃者がシステムリソースや関連データに簡単にアクセスできるようになります。同様に、セキュアに保管されていないパスワードが盗まれ、システムへの侵入に使われる可能性もあります。

ビジネスインパクト

- データ侵害の成功例の多くは、システムの脆弱性をエクスプロイトした攻撃によるものです。IBMのCost of Data Breach 2021 Report [2] によると、調査したデータ侵害のうち、サードパーティー製ソフトウェアの脆弱性が14%、クラウドの設定ミスと認証クレデンシャルの漏えいがそれぞれ20%と15%であることが示されています。
- データ侵害が発生すると、企業のビジネスに支障をきたし、お客様がその企業のサービスを利用できなくなる可能性があります。情報漏えいの結果、企業のブランドやサービスが信頼されなくなると、新規顧客の獲得が難しくなる可能性があります。どちらの結果も、収益の損失につながる可能性があります。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

- IBMのレポートでは、4つのデータ侵害に関係するコストセンターと、その1件あたりの平均コスト（百万米ドル単位）を特定しています。侵害の検知と拡大が29%（124万ドル）、通知が6%（27万ドル）、侵害後の対応が27%（114万ドル）、事業の損失が38%（159万ドル）を占めた。1件あたりの総費用は424万ドルでした。これらの事例では、2千件から1万1千件のデータ侵害がありました。5,000万件から6,500万件の大規模な情報漏えいの場合、1件あたりの平均コストは4億100万ドルでした。

要点

要点は次の通りです。

- システムの脆弱性とは、システム構成要素に存在する欠陥のことで、人為的なミスによってもたらされることが多く、ハッカーが企業のクラウドサービスを攻撃することを容易にします。
- ポスト・インシデント・レスポンスにはコストがかかります。企業データの損失は、企業の収益や評判に悪影響を及ぼす可能性があります。
- システムの脆弱性に起因するセキュリティリスクは、日常的な脆弱性検出とパッチ適用、厳格なIAMの実践により、大幅に抑制することができます。

想定事例と実例

システムの脆弱性の課題に関する最近の事例としては、以下が挙げられます。

- (2021年12月9日） Log4Shell の脆弱性 CVE-2021-45046 は、Java ベースの Log4j logging facilityバージョン 2.0beta9 から 2.14.1 に影響するリモートコードの脆弱性です。Log4Shellは、クラウドシステムでJavaが広く使用されていることを考えると、深刻な脅威と言えます。攻撃者は、脆弱なシステムに悪意のあるリクエストを送信することで、Log4Shell をエクスプロイトし、システムに任意のコードを実行させ、攻撃者が情報を盗んだり、ランサムウェアを起動したり、システムの制御を奪取したりすることができます。CISA、FBI、NSAなどの政府機関は、Log4Shellのエクスプロイトが長期に渡って続くと予想しています。[1]
- (2021年8月）クラウドセキュリティ企業Wizのセキュリティ研究者が、Microsoft Azureの顧客数千人分のデータに完全にアクセスできたことを公表しました。AzureのCosmosDB（研究者はChaosDBと呼ぶ）にセキュリティ上の欠陥があり、この脆弱性により、ユーザはユーザの認証クレデンシャルなしにデータのダウンロード、削除、その他の操作を行うことができました。[2]
- (2021年9月）マイクロソフトの研究者は、ロシア政府と関係のあるサイバー諜報グループが、ActiveDirectoryフェデレーションをエクスプロイトして、構成データベースやセキュリティトークンを盗み出すバックドアを配備していることを確認しました。マイクロソフトは、このマルウェアをFoggyWebと呼び、ロシアのハッカーグループAPT29（別名Cozy Bear、NOBELIUM）によるものであると説明しています。[2]
- (2021年）Ivanti社の「Ransomware Spotlight Year-End 2021 Report」によると、ランサムウェア攻撃に関連する脆弱性の数は、2020年の233から2021年には288となり、29%増加したとのことです。[3]

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CBK Security Guidance Version 4.0

Domain 7:インフラストラクチャ・セキュリティ
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 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:パスワードの管理
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要塞化とベースライン制御

TVM 脅威と脆弱性の管理

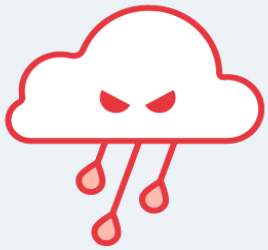
TVM-01:脅威と脆弱性管理ポリシーと手順
TVM-02:マルウェア対策ポリシーと手順
TVM-03:脆弱性の修復スケジュール
TVM-04:検出の更新
TVM-05:外部ライブラリの脆弱性
TVM-06:ペネトレーションテスト
TVM-07:脆弱性の特定
TVM-08:脆弱性の優先順位付け
TVM-09:脆弱性管理レポート

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. Log4Shell 0-day Vulnerability:All You Need to Know https://jfrog.com/blog/log4shell-0-day-vulnerability-all-you-need-to-know/ 2. Microsoft's very bad year for security:A timeline https://www.csoonline.com/article/3635849/microsofts-very-bad-year-for-security-a-timeline.html 3. Ransomware Spotlight Year End 2021 Report (Ivanti) https://www.ivanti.de/lp/security/reports/ransomware-spotlight-year-end-2021-report *Additional:* 1. 2021 marks another record year for security vulnerabilities https://www.techrepublic.com/article/2021-marks-another-record-year-for-security-vulnerabilities/ 2. Cost of Data Breach Report (IBM) https://www.ibm.com/security/data-breach 3. Cybersecurity vulnerabilities and their business impact https://www.verizon.com/business/resources/articles/s/ cyber-security-vulnerabilities-and-their-business-impact 4. Mitigating Log#Shell and Other Log4j-Related Vulnerabilities https://www.cisa.gov/uscert/ncas/alerts/aa21-356a 5. The Internet is on Fire https://www.wired.com/story/log4j-flaw-hacking-internet/ 6. Ransomware attacks are increasingly exploiting security vulnerabilties https://www.techrepublic.com/article/ransomware-attacks-are-increasingly-exploiting-security-vulnerabilities/ 7. Top Routinely Exploited Vulnerabilities https://www.cisa.gov/uscert/ncas/alerts/aa21-209a 8. What are the different types of vulnerabilities? https://www.packetlabs.net/types-of-vulnerabilities/
✓	Tampering with Data	
✗	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✓	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティ課題8：
予想外のクラウドデータ公開



Security Responsibility
✔ Customer
✔ Cloud Service Provider
✔ Shared

Architecture	
✔ Application	✔ Meta
✔ Info	✘ Infra

Cloud Service Model
✔ Software as a Service (SaaS)
✔ Platform as a Service (PaaS)
✔ IaaS（Infrastructure as a Service）

クラウドサービスは、企業がこれまでにない速度で構築、革新、およびスケールすることを可能にします。しかし、クラウドの複雑および多様なチームや事業部門によるクラウドサービスオーナーシップへの移行は、しばしばセキュリティガバナンスやコントロールの欠如を導きます。異なるCSPのクラウドリソースに対する設定数の増加により、設定ミスがより頻繁になり、クラウドインベントリに対する透明性の欠如とネットワーク露出により、意図しないデータ漏えいが発生する可能性があります。

データの流出はまだまだ蔓延しています。55%以上の企業が、現在インターネットに公開されているデータベースを少なくとも1つは持っています。[1] これらのデータベースの多くは、脆弱なパスワードを使用したり、認証を必要としなかったりするため、このような露出したデータベースはインターネットを継続的にスキャンする攻撃者による格好の標的になっています。セキュアでないElasticsearchサーバーが8時間で侵入される [2] ことを考慮すると、このような露出は可及的速やかに修正される必要があります。

ビジネスインパクト

クラウドの使い易さ、具体的には、マネージドデータベースやストレージオブジェクトのセットアップの速さが、大変人気を集めています。

- これらのデータベースには、機密性の高い顧客データ、従業員情報、製品データなどが含まれている可能性があります。このようなデータの流出は、フォレンジックチーム、カスタマーサポートプロセス、影響を受けた顧客への補償など、予想外の出費をもたらします。
- IBM Research [3] によると、2021年、データ侵害のコストは386万米ドルから424万米ドルに増加しました。IBMのレポートでは、データ侵害による社内調査やコミュニケーション、現在の顧客損失、企業への信頼の影響による将来の顧客損失など、さらなる間接的な追加コストについて言及しています。

要点

意図しない情報漏えいを防ぐために、クラウド利用者は以下の質問に簡単に答えられるようにしておくことをお勧めします。

1. PaaSデータベース、ストレージ、およびデータベースをホストするコンピュートワークロードをレビューします。VM、コンテナ、およびそれらにインストールされたDBソフトウェアを含みます。コンフィギュレーションベースのソリューションでは、必要な可視性を提供する機能が限られており、ワークロードを検査またはスキャンすることができません。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

2. クラウド環境を完全に可視化できる露出エンジンを選択し、トラフィックを外部に露出できるルーティングやネットワーク・サービスを特定します。ロードバランサ、アプリケーションロードバランサ、CDN、ネットワークピアリング、クラウドファイアウォール、Kubernetesネットワーキングなどを含みます。
3. データベースが最小権限のIAMポリシーを実装し、このポリシーの割り当てを制御・監視することで、アクセスの露出を減らすことができます。

想定事例と実例

最近の予想外のクラウドデータ侵害事故の課題例としては、以下のようなものがあります。

- VIP Games、23Mレコード、2021年1月 - クラウドの誤設定により、メールアドレス、ユーザ名、ソーシャルネットワークID、プレーヤーデータを含む60K以上のユーザの23Mレコードがウェブ上で公開されました。[4]
- Reverb、5.6Mレコード、2021年4月 - 5.6Mの顧客レコードを保存するElasticsearchがウェブ上で公開されました。[5]
- The Telegraph、10TBの記録、2021年9月 - 英紙The Telegraphは、購読者データ10TBのデータベースを公開しました。[6]
- Securitas、1Mレコード、2022年1月 - 認証されていないAWSサーバから3TBの空港従業員の記録が公開されました。[7]
- FlexBooker、19Mレコード、2022年2月 - Amazonは、12月のデータ侵害後、露出したFlexBookerバケットの閉鎖に踏み切りました。[8]

CSA CBK Security Guidance Version 4.0

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 12:アイデンティティ管理、権限付与管理、アクセス管理 (IAM)

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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

DSP データセキュリティと情報ライフサイクル

DSP-03:データインベントリ

DSP-08:デザイン段階からのデータ保護とデフォルト設定

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のポリシーと手順

IAM-03:アイデンティティ・インベントリ

GRC ガバナンス、リスク、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 I

GRC-02 ：リスク管理プログラム

BCR 事業継続マネジメントとオペレーショナルレジリエンス

BCR-05:文書化

IVS インフラ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

Stride Threat Analysis	
✗	Spoofing Identity
✓	Tampering with Data
✓	Repudiation
✓	Disclosure
✗	Denial of Service
✗	Elevation of Privilege

Reference Links

1. 2022 Cloud Security Threats report https://www.wiz.io/blog/2022-cloud-security-threats
2. Unsecured Elasticsearch server breached in eight hours flat https://www.computerweekly.com/news/252484365/Unsecured- ElasticSearch-server-breached-in-eight-hours-flat
3. How much does a data breach cost? https://www.ibm.com/security/data-breach
4. A cloud misconfiguration exposed 23M records of over 60K users containing emails, user names, social network ID, and player data on the web https://portswigger.net/daily-swig/online-gaming-platform-vip- games-exposes-23-million-data-records-on-misconfigured-server
5. Elasticsearch storing 5.6M customer records was exposed on the web https://www.bitdefender.com/blog/hotforsecurity/etsy-owned- musical-instrument-marketplace-reverb-suffers-data-breach
6. UK newspaper The Telegraph exposed 10TB database with subscriber data https://securityaffairs.co/wordpress/123020/data-breach/the- telegraph-data-leak.html
7. Unauthenticated AWS server exposed 3TB in airport employee records https://www.zdnet.com/article/unsecured-aws-server-exposed- airport-employee-records-3tb-in-data/
8. Amazon steps in to close exposed FlexBooker bucket after December data breach https://www.zdnet.com/article/amazon-steps-in-to-close-exposed- flexbooker-bucket-after-december-data-breach/

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティ課題9：サーバーレスやコンテナワークロードの構成ミスやエクスプロイト

Security Responsibility	
✔ Customer	
✔ Cloud Service Provider	
✔ Shared	
Architecture	
✘ Application	✔ Meta
✔ Info	✘ Infra
Cloud Service Model	
✘ Software as a Service (SaaS)	
✔ Platform as a Service (PaaS)	
✔ Infrastructure as a Service (IaaS)	

クラウドインフラへの移行とDevOpsプラクティスの採用により、ITチームはこれまでになく迅速にビジネスへ価値を提供することができます。アプリケーションを実行するためのインフラやセキュリティコントロールの管理・拡張は、開発チームにとって依然として大きな負担となっています。オンプレミス環境の管理に慣れているレガシーなインフラチームは、Infrastructure as Codeやクラウドセキュリティなど、新しいスキルを習得する必要があります。同じチームが、アプリケーションをサポートするネットワークとセキュリティコントロールに対して、より大きな責任を負う必要があります。サーバーレスやクラウドネイティブのコンテナ型ワークロードでは、その責任をクラウドサービスプロバイダ（CSP）に委ねることから、この問題を解決する打開策であるように見えるかもしれません。それでもなお、仮想マシンをクラウドに移行するよりも高いレベルの、クラウドとアプリケーションのセキュリティ成熟度が要求されます。

サーバーレスモデルでは、CSPが基盤となるインフラのセキュリティと管理に責任を負います。開発・運用上のメリットに加え、CSPはデフォルトで短命のコンテナ内で関数コードを実行することから、攻撃対象領域を減らすことができます。常に更新されるシステムは、エクスプロイトされた場合の永続性を大幅に制限します。ただし、CSPにより、より長いライフタイムや「ウォームスタート」構成のサーバレスコンテナを利用者に許可すると、環境のセキュリティは低下します。追加のリスクとして、一時ファイルシステムや共有メモリから機密情報が漏えいする可能性もあります。一時ストレージへのアクセスは、マルウェアをホストまたは実行するために使用される可能性があり、アプリケーションコードによってワイプされることが必要です。

サーバーレスの責任モデルは、より繊細かつ複雑な環境をもたらします。Netskopeが行った分析では、分析したIAMポリシーの4%が完全な管理者アクセスを持っており、60%がAWS AdministratorAccessの役割を持っていました。[1] 仮に、これらの権限が公開されているAWSのサーバーレスなLambda関数に割り当てられているとすると、脆弱性が多数存在している可能性があります。クラウド環境へのアクセス、機密データの流出、AWSアカウントの乗っ取りといった可能性が考えられます。

また、インフラをコントロールすることができないため、アプリケーションセキュリティの課題に対する軽減策や、従来のセキュリティツールの可視性も制限されます。このため、クラウドハイジーン、アプリケーションセキュリティ、可観測性、アクセスコントロール、シークレット管理などに関する強力な組織的プラクティスを構築し、攻撃の被害範囲を小さくすることが重要になります。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

ビジネスインパクト

このため、クラウドハイジーン、アプリケーションセキュリティ、可観測性、アクセスコントロール、シークレット管理などに関する強力な組織的プラクティスを構築し、攻撃の被害範囲を小さくすることが重要になります。必要な専門知識やデューデリジェンスなしにサーバーレス技術で実装されたアプリケーションは、重大な侵害、データの損失、及び財務的消耗につながる可能性があります。

要点

要点は次の通りです。

- 企業は、クラウドセキュリティポスチャ管理、クラウドインフラストラクチャエンタイトルメント管理、及びクラウドワークロード保護プラットフォームによる自動チェックを実装する必要があります。
- セキュアでないクラウド構成のリスクと頻度を減らすために、クラウドセキュリティトレーニング、ガバナンスプロセス、及び再利用可能なセキュアなクラウドアーキテクチャパターンに投資する必要があります。
- 開発チームは、従来のセキュリティコントロールを解除するサーバーレス技術に移行する前に、強力なアプリケーションセキュリティとエンジニアリングのベストプラクティスをさらに厳重する必要があります。

想定事例と実例

サーバーレスやコンテナエクスプロイトに関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。

- 2021年現在、DoW（Denial of Wallet）攻撃をめぐる研究が進んでいます。DoW攻撃は、機能的にはDoS（Denial of Service）攻撃と似ています。攻撃者は、サーバーレスアプリケーションに大量のリクエストを送信し、基盤となるインフラに影響を与えます。しかし、DoW攻撃では、サーバーレスプラットフォームの自動スケーリング消費モデルを利用することで、クラウド利用者に金銭的負担を負わすことが目的です。これらの攻撃は、同時実行数の制限によって軽減することができますが、その場合、攻撃ベクターがDoWからDoSに変わります。[2]
- (2021) CVE-2022-0811 (CRI-O コンテナエスケープ脆弱性) [3], CVE-2022-0185 (Linux Kernelのバッファオーバーフロー [4]), Azurescape [5] を含む、異なるコンテナランタイム環境で複数のエスケープ脆弱性が発見されました。これらの脆弱性はそれぞれ、攻撃者がコンテナ環境を抜け出し、コンテナホストへの特権アクセスを得ることができる可能性を生み出します。これらの脆弱性はそれぞれ、攻撃者がコンテナ環境を抜け出し、コンテナホストへの特権アクセスを得ることができる可能性を生み出します。
- (2022年2月) Cado Labsの研究者は、Denoniaと名付けられたAWS Lambdaを直接標的とする最初の既知のマルウェアが実際に活発に使用されている証拠を発見しました。Denoniaは、DNS over HTTPSを使用してC2サーバーと通信するMoneroマイニングのLambda関数です。このマルウェアはLambdaの脆弱性をエクスプロイトしたものではなく、配備には管理者権限が必要ですが、攻撃者が組織の費用でサーバーレス環境を利用することにより金銭的利益を得ることができる一例です。[6]

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CBK Security Guidance Version 4.0

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、エンタイトルメント、アクセス管理

CSA CCM Controls Version 4.0

AIS 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
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
A&A-06:修復

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-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

BCR 事業継続マネジメント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-03:事業継続の戦略

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

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の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

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-05:最小権限
IAM-09:特権的なアクセスロールの分離
IAM-10:特権的なアクセスロールの管理
IAM-14:強固な認証
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-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要塞化とベースライン制御
IVS-05:本番環境と非本番環境
IVS-07:クラウド環境への移行
IVS-09[i]:ネットワーク防御

[i] 英語原文ではIVS-07と表示されているが、項目の内容から和訳版ではIVS-09とした。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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

LOG-13[5]:故障と異常の報告

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 インシデントレスポンスのテスト

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

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. A-real-world-look-at-aws-best-practices-iam-policies https://www.netskope.com/blog/a-real-world-look-at-aws-best-practices-iam-policies 2. S221421262100079X https://www.sciencedirect.com/science/article/pii/S221421262100079X 3. Cri-o-vulnerability https://blog.aquasec.com/cve-2022-0811-cri-o-vulnerability 4. Linux-kernel-container-escape-in-kubernetes https://blog.aquasec.com/cve-2022-0185-linux-kernel-container-escape-in-kubernetes 5. Azure Escape https://www.paloaltonetworks.com/blog/2021/09/azurescape/ 6. First-malware-targeting-aws-lambda https://thehackernews.com/2022/04/first-malware-targeting- aws-lambda.html
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

[5] 英語原文ではLOG-12と表示されているが、項目の内容から和訳版ではLOG-13とした。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティ課題10：
組織的な犯罪、ハッカーとAPT

Security Responsibility
✔ Customer
✔ Cloud Service Provider
✔ Both

Architecture	
✔ Infra	✔ Info
✔ Meta	✔ Application

Cloud Service Model
✔ Software as a Service (SaaS)
✔ Platform as a Service (PaaS)
✔ Infrastructure as a Service (IaaS)

APT（Advanced Persistent Threats）とは、侵入者または侵入者のチームが、ネットワーク上に不正かつ長期的なプレゼンスを確立し、機密性の高いデータを探索する攻撃キャンペーンを表す広義の用語です。このようなチームには、国家や組織的な犯罪集団が含まれることがあります[1]。組織犯罪という用語は、集団の個人 [5] の努力を反映した計画的かつ合理的な行為を行う際に、その集団が持つであろう組織のレベルを表す手段として意味されています。APTは、ターゲットに侵入するための高度な戦術、技術、プロトコル（TTP）を確立しています。APTグループは、標的のネットワークで数ヶ月間発見されずに過ごすことも珍しくありません。このように時間がかかると、機密性の高いビジネスデータや資産に向かって横方向に移動することが可能になります。また、APTグループの中には、歴史的に特定の産業や組織を好んでいるものもあります。例えば、APT33は、イランに拠点を置く脅威者が関与しているとされています。彼らはこれまでエネルギーや航空分野を標的にしてきました。APTグループは、政治的、経済的など、さまざまな動機で悪意のある活動を行っています。

脅威情報コミュニティは、APTグループを綿密に調査しています。脅威情報のレポートは、APTグループとその行動について、組織や国家を啓発するものです。組織は、報告書に記載されているAPTグループの行動を模擬したレッドチーム演習を実施することで、より効果的に身を守ることができます。このようなサイバー演習により、組織はAPTグループに関連するさまざまなTTPに対するサイバー検知能力をテストし、向上させることができます。また、組織は、ネットワーク内のAPTの存在を検知するために、脅威ハンティング活動を実施する必要があります。

ビジネスインパクト

- APTグループの動機は様々で、グループごとに異なる場合があります。政治的な動機（ハクティビストなど）を持つグループもあれば、組織的な犯罪集団の一員であるグループもあります。いくつかのグループは、国家的のアクターでさえあります。例えば、APT38は、北朝鮮の国家が支援するグループであると疑われており、世界の金融機関を標的としたサイバー強盗を行うことで知られています。
- APTグループが組織に与えるビジネスインパクトを理解するためには、組織の情報資産に対するビジネスインパクト分析を行う必要があります。これにより、APTグループがどのように、そしてなぜ組織を狙うのか、潜在的なセキュリティ侵害がビジネスに及ぼす影響とはどのようなものかを理解することができます。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

要点

要点は次の通りです。

- 自社の情報資産を把握するために、組織のビジネスインパクト分析を行います。
- サイバーセキュリティ情報共有グループに参加し、関連するAPTグループとそのTTPを理解します。
- 攻撃的なセキュリティ演習を実施し、これらのAPTグループのTTPをシミュレートし、セキュリティ監視ツールが検知できるようにチューニングします。

想定事例と実例

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

- (2022年4月5日) Broadcom のシマンテック部門のマルウェアハンターは、中国の国家的ハッカーに関連する長期的なサイバースパイ活動が、よりグローバルな足場を持つマネージドサービスプロバイダ (MSP) を標的としている兆候を発見しました。[2]
- (2016年2月5日) Lazarusグループ（APT38）は、バングラデシュの国立銀行へのほぼ完全な強奪を行いました。[3]
- (2022年1月21日) LAPSUS$グループがNvidiaの内部ネットワークをハッキングし、機密データを盗み出しました。このグループは、Nvidiaにデータを身代金として渡す代わりに、Nvidiaが暗号マイニング用のグラフィックス プロセッシング ユニットの制限を解除するよう要求しました。[4]

CSA CBK Security Guidance Version 4.0

Domain 9:インシデントレスポンス
Domain 13:Security as a Service

CSA CCM Controls Version 4.0

TVM アプリケーションとインターフェースのセキュリティ

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

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

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. APT Definition https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ 2. Chinese APT Group Targeting Global MSPs: https://www.securityweek.com/symantec-chinese-apt-group- targeting-global-msps 3. How North Korea almost pulled off a billion-dollar hack: https://www.bbc.com/news/stories-57520169 4. Lapsus$ group demanding Nvidia release restrictions on crypto mining on its GPUs: https://cybersecuritynews.com/beware-lapsus-ransomware-group/ 5. Cyber Organized Crime:What is it? https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

セキュリティ課題11：
クラウドストレージデータ流出

Security Responsibility
✓ Customer
✓ Cloud Service Provider
✓ Shared

Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra

Cloud Service Model
✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)

クラウドストレージのデータ流出は、機微情報、保護された情報、または機密情報に関わる事件です。これらのデータは、組織の運用環境の外部にいる人によって公開、閲覧、盗難、または使用される可能性があります。データの流出は、標的型攻撃の主な目的であり、エクスプロイトされた脆弱性または設定ミス、アプリケーションの脆弱性、あるいは不十分なセキュリティ慣行に起因する可能性があります。流出は、例えば、個人の健康情報、金融情報、個人を特定できる情報（PII）、企業秘密、知的財産など、公開を意図していないあらゆる種類の情報に関わる可能性があります。

データ流出シナリオでは、被害者は通常、データ損失を意識することはありません。攻撃者は、直接的な金銭的利益やランサムウェアなどの目的の一部になる場合には、組織に通知することがあります。それでも、データが流出した事実が不明であったり、時間が経ってから発見されたりして、どんな緩和策も無意味になってしまうケースもあります。

データは主要資産であるため、クラウドの使いやすさ、構成、弾力性、レジリエンス、そしてあらゆる合理的なニーズに適した複数のサービスは、クラウドデータストレージを非常に魅力的なものにしています。それに伴い、流出先も複数存在します。PaaSサービスの設定ミスなど、人為的なミスや悪用が原因となる場合があります。ストレージオブジェクトもまた、個人のクラウドストレージアプリケーションを通じて外部で共有される機密データやファイルを公開する可能性があります。

その他のクラウドストレージのデータ流出は、アプリケーションやサービスを操作するフィッシング攻撃から始まる場合もあります。最初の侵害のベクトルは、クレデンシャルの盗難やクラウドデータへの不正アクセスにつながる可能性があります。その後、攻撃者は、後で使用するためにデータを抽出するなどのいくつかの潜在的なアクションを取りながら、ランサムウェアのために組織のデータの暗号化を行います。

サプライチェーン攻撃は、下層のデータへのアクセスを提供し、検出と回復をより複雑なものにする可能性があります。組織がゼロトラストモデルに向かうにつれて、従来の組織の境界線はあまり役割を果たさなくなります。最小権限のアクセスとIDベースのセキュリティコントロールにより、データの露出を制限する必要があります。また、CSPのベストプラクティスや規制のベースライン、攻撃検知やデータ災害復旧の仕組みに準拠したクラウドポスチャ管理の実施も重要です。

© Copyright 2022, Cloud Security Alliance. All rights reserved.

ビジネスインパクト

データ侵害が発生すると、以下の影響を受ける可能性があります：

- 知的財産の喪失。ユニークな知識が失われ、製品開発、戦略的計画、さらには将来の攻撃への一歩に利用されます。
- 顧客、ステークホルダー、パートナー、従業員の信頼を失うと、事業活動、投資、購買が阻害され、その組織で働きたい、働きたいという気持ちが低下する可能性があります。
- 規制当局による措置には、金銭的な罰金やプロセスおよび業務の変更要求が含まれます。
- 地政学的な影響は、企業行動に影響を与える可能性があります。
- 従業員のデータを保護する組織の能力に対する従業員の信頼の喪失。

要点

要点は次の通りです。

- クラウドストレージには、しっかりとした環境（SSPM、CSPM）が必要です。
- 攻撃やデータ流出を検知・防止するために、CSPのベストプラクティスガイド、監視、検知機能を適用します。
- データは様々な場所に散在し、様々なペルソナによって管理されているため、クラウドストレージの使用に関する従業員の意識改革が必要です。
- 必要に応じて、クライアントサイドの暗号化を実施します。
- データを分類することで、さまざまなコントロールを設定し、インシデント対応計画に必要な影響とリカバリ措置を文書化するのに役立ちます。

想定事例と実例

クラウドデータの流出に関する最近の課題例は、以下のようなものがあります：

- (2021/6/24) “2019年にさかのぼりますが、5億3300万以上のアカウントに関する情報がハッカーフォーラムに無料でダウンロードできるよう掲載されているのが見つかり、最近になって明るみに出たユーザデータの大規模流出について、Facebookが欧州で提訴されることになりました。” [1]
- (2019/3/11) “セキュリティ研究者は、スタッフがBoxエンタープライズストレージアカウント内のファイルへのパブリックリンクを簡単に発見できるように共有しているため、企業や顧客の機密データが不用意に流出している数十の企業を発見しましたと述べています。” [2]
- (4/12/2022) “Amazon Web Services (AWS) は月曜日、Amazon Relational Database Service (RDS) の脆弱性に最近対処し、内部クレデンシャルの漏洩につながる可能性があることを発表しました。” [3]

© Copyright 2022, Cloud Security Alliance. All rights reserved.

CSA CBK Security Guidance Version 4.0

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 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
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 13:Security as a Service

CSA CCM Controls Version 4.0

A&A 監査・保証

A&A-02:独立した評価
A&A-04:要件のコンプライアンス

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-07:アプリケーション脆弱性の修復

CCC 変更管理と構成管理

CCC-03:変更管理技術
CCC-04:承認されていない変更からの保護
CCC-07:ベースラインからの逸脱の検出

CEK 暗号、暗号化、鍵管理

CEK-03:データ暗号化
CEK-19:鍵の侵害

DCD データセンタセキュリティ

DCS-02:オフサイト転送承認ポリシーと手順

DSP データセキュリティとプライバシーの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-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-17:機微なデータの保護

GRC ガバナンス、リスク、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-08:Special Interest Group (SIG)

HRS 人的リソース

HRS-04:リモートおよび在宅勤務のポリシーと手順
HRS-11:セキュリティ意識向上トレーニング

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-07:ユーザ アクセスの変更と取り消し
IAM-14:強固な認証
IAM-16:認可メカニズム

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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要塞化とベースライン制御

IVS-09:ネットワーク防御

IPY 相互運用性と移植容易性

IPY-03:セキュアな相互運用性と移植容易性の管理

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-06:イベントのトリアージプロセス

STA サプライチェーンの管理、透明性、説明責任

STA-02:SSRMサプライチェーン

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-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

TVM 脅威と脆弱性の管理

TVM-02:マルウェア対策ポリシーと手順

TVM-04:検出の更新

TVM-07:脆弱性の特定

UEM ユニバーサルエンドポイント管理

UEM-09:マルウェア対策による検知及び保護

UEM-14:サードパーティーのエンドポイントに対するセキュリティポスチャ

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. Facebook faces 'mass action' lawsuit in Europe over 2019 breach https://techcrunch.com/2021/04/16/facebook-faces-mass-action-lawsuit-in-europe-over-2019-breach/ 2. Dozens of companies leaked sensitive data thanks to misconfigured Box accounts https://techcrunch.com/2019/03/11/data-leak-box-accounts/ 3. Amazon RDS Vulnerability Led to Exposure of Credentials https://www.securityweek.com/amazon-rds-vulnerability-led- exposure-credentials
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

© Copyright 2022, Cloud Security Alliance. All rights reserved.

結論

クラウドのビジネスモデルやセキュリティ戦術が進化する中で、本レポートは、（1）不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理、（2）セキュアでないインターフェースやAPI、（3）誤設定と不適切な変更管理、（4）クラウドセキュリティのアーキテクチャと戦略の欠如といった、重要なセキュリティ課題への認識を高めています。その他の脅威としては、（5）セキュアでないソフトウェア開発、（6）セキュアでないサードパーティーリソース、（7）システムの脆弱性が挙げられます。

不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理が上位を占めています。リプレイ攻撃、なりすまし、および過剰な権限付与は、クラウド環境ではより高いアクセス性が期待されるにもかかわらず、オンプレミスと同様に続いています。自己署名証明書の使用、不十分な暗号技術の管理、あるいはすべてのルート認証局を信頼することなどは、疑わしい選択のほんの一例です。ゼロ・トラスト・アーキテクチャとSDPが強調される中、本パンデミックイレブンで取り上げたセキュリティ課題1がアンケート回答者の頭に浮かぶのは不思議ではありません。

マイクロサービスの継続的な採用は、セキュアなインターフェースとAPIの重要性を強調しています。このようなセキュアなインターフェースとAPIはもっとたくさんあるべきですが、利用者側での開発においてクラウドは最小限の役割を果たすのみであり、これらの機能のセキュリティ確保に未だに大きなチャレンジがあるのが課題です。提供されるSaaSやPaaSにこれらのAPIが普及すると、プログラマの非効率性とクラウドの常時稼働性が大きなリスクを生み出します。

以前は、「設定ミスと不適切な変更管理」が「11の悪質な脅威」の第2位を占めていました。これは、クラウドの問題がセキュリティ・スタックの上に移動していることを示すもう一つの例です。構成管理は何十年もの間、組織の能力成熟の一部とされていますが、チームが進んでクラウドを採用する限り、深刻さが増す一方です。クラウドの永続的なネットワークアクセスと無限の容量に関する設定ミスは、企業内の多くの組織に対し潜在的な影響を与えます。

最後に、前回3位を占めた「戦略とアーキテクチャ」は、「なぜ、セキュリティ・ソリューションの計画と設計に未だに問題があるのか」という疑問を投げかけるものです。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、全体像のアプローチを定義し、アーキテクチャのデザインパターンに基づいて実行するものです。

クラウドコンピューティングの重大脅威：11の悪質な脅威2019では、従来の情報セキュリティ（脆弱性やマルウェアなど）に対する焦点からのシフトを報告しましたが、本「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」レポートでもその傾向を引き継いでいます。ともあれ、これらのセキュリティ課題は、クラウドセキュリティに関する意識向上、設定、およびID管理を発展・強化させるための行動を呼びかけるものです。クラウドそのものへの懸念は少なくなってきているため、現在のCSAはクラウド技術の実装により焦点を当てています。

© Copyright 2022, Cloud Security Alliance. All rights reserved.