シャドーアクセスの定義：
新たなIAMセキュリティの課題

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

The permanent and official location for Identity and Access Management Working Group is
https://cloudsecurityalliance.org/research/working-groups/identity-and-access-management/

Acknowledgments

Lead Authors

Sasi Murthy
Venkat Raghavan
Steven Schoenfeld

Contributors

Philip Griffiths
Shruti Kulkarni
Michael Roza
Dhaval Shah
Heinrich Smit

Reviewers

Senthilkumar Chandrasekaran
Ivan Djordjevic
Rajat Dubey
Ahmed Harris
Shraddha Patil
Alberto Radice
Osama Salah

CSA Analysts

Ryan Gifford

Editor

Larry Hughes

CSA Global Staff

Claire Lehnert

日本語版提供に際しての告知及び注意事項

本書「シャドーアクセスの定義：新たなIAMセキュリティの課題」は、Cloud Security Alliance（CSA）が公開している「Defining Shadow Access: The Emerging IAM Security Challenge」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4月28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

「シャドーアクセスの定義： 新たなIAMセキュリティの課題」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
高橋 久緒, CISSP, RISS, PMP
松浦 一郎, CISSP, CISM, CDPSE
諸角 昌宏

目次

シャドーアクセス

シャドーアクセスとは、アプリケーション、ネットワーク、およびデータなどのリソースへの意図しない、あるいは望ましくないアクセスのことです。この新しい問題は、クラウドコンピューティング、DevOpsにおけるベロシティ、クラウドネイティブアーキテクチャ、およびデータ共有の発展とともに生じている新たな問題です。

シャドーアクセスは、クラウドの課題としてますます深刻になっています。これは、クラウドサービスを相互に接続するアクセスと権限付与の増加から始まり、自動化されたインフラストラクチャーとソフトウェア開発とが相まって、アカウントやリソースに対する誤ったあるいは予期しない権限の付与に起因しています。
組織規模の大小にかかわらず、かつてはセキュアな出発点であったものが、気づかぬうちにセキュアでないものへと変わってしまっているという困難な状況にしばしば遭遇します。これらの問題は、アカウントと権限のクローンを作成する一般的な慣行（一般的にはオンボーディングやアカウント作成時）と組み合わされ、真に必要とはされないアクセスを提供することによって、シャドーアクセスの問題をさらに大きなものとしています。

シャドーアクセスは壊滅的な結果をもたらす可能性があり、進化するクラウドを利用するどのような組織にも影響を及ぼす恐れがあります。この短いドキュメントでは、その背景、原因、影響、および動的でセキュアなクラウド環境のメリットを取り戻すための今後の道筋を概説することを目的としています。

背景

エンタープライズIAM 対
クラウドIAM

・LDAP, AD, エンタープライズIAMの中に存在

・エンドユーザーや管理者

・エンタープライズ、ホストされたクラウド、SaaS

アプリへのアクセス

・クラウド内で構築担当者や運用担当者によって使用される。

・AWS IAM、Google Workspace、Azure AD、Snowflake、Mongo DB、Infrastructure-As-Code の中に存在

・DevOps、クラウドインフラ、管理者、クラウドエコシステムと共に使用されるSaaSアプリケーション； エンドユーザーのアイデンティティではない

図1: エンタープライズIAM対クラウドIAM

従来のエンタープライズ IAMシステムは何十年も前から導入されており、多くの場合 LDAP や Active Directory のような一般的なサービスやプロトコルをベースに構築されています。エンタープライズ IAM システムは、アイデンティティにエンタイトルメントとクレデンシャルをプロビジョニングし、通常は権威を有し信頼できる情報源としての企業のHRシステムに依存します。確立されたポリシーとプロセスはアクションの呼び出しと、その結果としてのエンドユーザーによるリソースとアプリケーションへのアクセスを取り巻き、それらは通常、企業のファイアウォールの「内側」でホストされ、セキュアなVPN接続を介してファイアウォールの「外側」の従業員と請負業者によってアクセスされます。

クラウドアプリケーションが注目されるようになるにつれて、クラウドIDP（Identity Provider）システムが登場し始めました。定義上、クラウドアプリケーションは企業内でホストされていません。そのため、今日、多くの企業は、Okta、Azure AD、または Ping Identity のような一般的なクラウド IDP と連携して、（オンプレミスでホストされているアプリケーション用の）エンタープライズ IAMを運用しています。

クラウドコンピューティングの登場により、クラウドIAMという新しい概念が導入されました。クラウドIAMは、AWS、Google Cloud、Azure Cloudのようなパブリッククラウドエコシステムや、Kubernetesを搭載したプライベートクラウドに内在するリソース、アプリケーション、およびデータへのアクセスやエンタイトルメントをプロビジョニングし、制御するために使用されます。

一見似ていますが、実際にはそのコンセプトが大きく異なるため、別途これらのクラウドアイデンティティを分類し検討する必要があります。

では、なぜクラウドアイデンティティという新しいコンセプトが生まれ、どう違うのでしょうか？

- クラウドで起動するものはすべて、重要なクラウドサービス、サプライチェーン要素、またはデータへアクセスするアイデンティティを持っています。クラウドサービスプロバイダー（例えば、AWS、GCP、Azure）のシステムは、Cloud IAMのような基軸となるサービスを介して、すべてのアイデンティティのプロビジョニングとそのアクセスを制御します。
- クラウドの内部では、アクセスが許可される前に、要求されたすべてのアクセスが認証・認可されます。
- クラウドアイデンティティには、人間または人間以外のアイデンティティがあります。人間のアイデンティティは、主にエンドユーザー、開発者、DevOps、およびクラウド管理者です。人間以外のアイデンティティは残りの大半であり、クラウドサービス、API、マイクロサービス、ソフトウェアサプライチェーン、クラウドデータプラットフォームなどに接続されたアイデンティティで構成されます。
- クラウドの力のひとつは、「プログラム可能であること」です。この力は開発者を通じて、クラウドサービス、API、およびデータをプログラミング的に組み合わせてアプリケーションを作成することで、解き放たれます。この違いは軽視できません。最新のクラウドアプリケーションは実際のところ、プロバイダーとそのエコシステム全体に渡って、APIから駆動される多くの分散サービスの集合体です。クラウドサービスを組み合わせる開発者は、データへのアクセス経路を持つ自動化されたアイデンティティを作成します。
- クラウドのもう一つの力は自動化です。クラウドチームは、Infrastructure-as-Codeを使った自動化の力を使って、クラウドリソース、クラウドアイデンティティ、およびそれらのアクセスを容易に定義し起動できます。この場では、自動化が第一で、ガバナンスはそのつぎです。

クラウドコンピューティングはアイデンティティ中心の世界を作りあげ、それらを取り巻く上記の一連の違いはシャドーアクセスの根本原因につながります。

原因

シャドーアクセスの根本原因は、クラウドアイデンティティを持つことだけでなく、クラウドによって引き起こされる根本的な複雑さとプロセスにもあります。

複雑さ

上記で言及した「クラウドの力」は、主に開発者と自動化によって解き放たれ、以前の環境よりもかなり複雑になっています。特筆すべき違いは以下の通りです。

- データはもはや単一のデータストアに保存されているわけではありません。クラウドやSaaS環境にまたがるクラウドデータストアやデータ共有アプリケーションが急増しています。
- データストアは常に進化、拡大または縮小しており、アプリケーションによる新たな使用や更新に伴って新しいタイプが出現します。
- アプリケーションは一枚岩ではなく、相互接続されたアイデンティティシステム、クラウドサービスおよびデータの、めまぐるしい組み合わせになります。
- クラウドエコシステムに接続するSaaSアプリケーションの利用が激増しています。
- 各クラウドサービスには、機密データや操作に対する認可を提供する、関連した権限とエンタイトルメントがあります。
- 権限とエンタイトルメントの規模は、従来のオンプレミス環境と比較して、はるかに広大で桁違いに複雑です。
- 企業はマルチクラウドやパブリック／プライベートクラウド環境の組み合わせを利用しています。

複雑さの説明の例として、AWS単体だけでも12,800のクラウドサービスがあり、13,800のパーミッションが付加され、クラウドアクセスに関する膨大な順列組合せの集合になります。

図2: https://aws.permissions.cloud/ から引用

プロセスの変更

以前の環境では、アイデンティティが作成されアクセス権が付与される前に、厳格なポリシーとプロセスが実施されているのが普通でした。コントロールを確立していた組織では、このガバナンスプロセスは、作成だけでなく、一貫したレビューと承認のプロセスも考慮することが一般的でした。ここでもまた、クラウドは以下のように大きく異なります。

- 新しいアイデンティやアクセスは、多くの場合、開発者がinfrastructure-as-codeを使って一元的に作成します。
- 新しいアイデンティのプロファイルは通常、組織標準の一元的なレビュー手順があるであろうテンプレートからコピーされます。
- 新しいアイデンティティやアクセスは、ほとんどガバナンスがないまま自動的に作成されます。
- アイデンティがアクセスするアプリケーションは完全なアクセスレビューが行わないまま常に変化しています。
- アプリケーションコンポーネントはスピードを上げるために、しばしば再利用、コピー、または複数のアプリケーションに使用されます。
- 増加するSaaSやサードパーティアプリケーションの利用は、正式なセキュリティレビューが行われていません。
- アプリケーションがアクセスするデータストアは常に変化しています。

作成から欠如しているものは、アイデンティティとアクセスの作成と同様に自動化される必要がある、継続的な監視、レビュー、および権限設定です。クラウドアプリケーションは分散され、常に進化しているため、1つの要素の変更が全体のエクスポージャーにつながるような意図しない結果をもたらす可能性があります。

このような非常に複雑で進化するアプリケーションの性質と、クラウドアイデンティの作成と継続的な見直しを取り巻くプロセスの途絶こそが、シャドーアクセスと組織にとって潜在的に甚大なエクスポージャーの連続を導きます。

インパクト

先に述べたように、シャドーアクセスとは、アプリケーション、ネットワーク、およびデータ等のリソースへの意図しないあるいは望ましくないアクセスを指します。

その影響を示すために、Verizon Data Breach Investigations Report（DBIR）レポートは、侵害の80%がアイデンティティとアクセスに関連していることを強調しています。ゼタバイト級のデータがクラウドプラットフォームに保存され続け、アクセスに対する膨大な需要を高めています。

シャドーアクセスの影響は以下の通りです。

- 既存のツールは、数多くのクラウドアイデンティティとアクセス経路に気が付きません。
- ガバナンスと可視性のギャップが、IAMガードレールの実装を非常に困難にしています。
- 認識されていないアクセス経路は、脆弱性をエクスプロイトしクラウドデータを侵害できます。
- 脅威アクターはプログラマブルアクセスを兵器化し、データ侵害をはるかに超える被害を引き起こせます。
- クラウドエコシステムに接続するサードパーティやSaaSアプリケーションは、ラテラルムーブメントのリスクをもたらします。
- シャドーアクセスの存在は、データセキュリティ、監査、およびコンプライアンス上のリスクを作り出し、ポリシーとガバナンスのギャップを作ります。

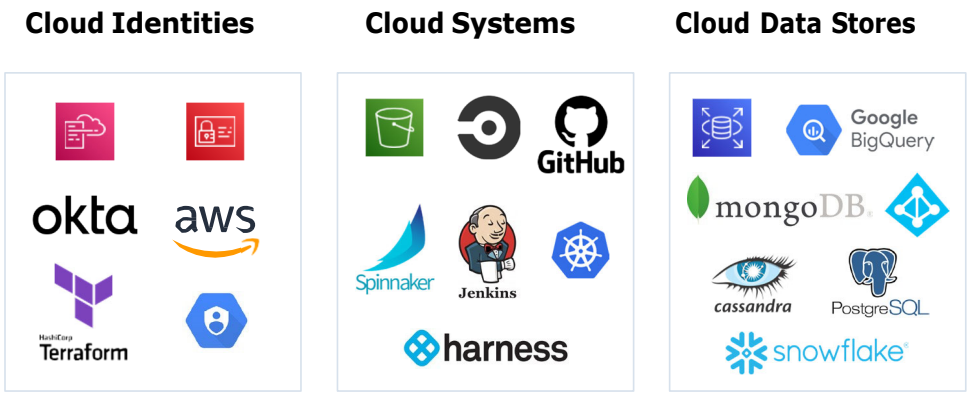

図3: シャドーアクセスは、複数のパブリッククラウドのエコシステムに渡って存在 します(例 AWS)

要するに、環境の真のセキュリティ状態は知られることはなく、その情報を導出するための仕組みやプロセスは、分析が完了する前に時代遅れになっているのが普通です。その結果として、環境は脆弱になり、環境の所有者はリスクを真に評価する方法を持ちません。

「CI/CDエコシステム全体にわたって、人間およびプログラミング的なものの両者で、数百(または時には数千)のアイデンティティが存在し、強力なアイデンティティとアクセス管理のプラクティスの欠如と過度に寛容なアカウントの一般的な用法とが組み合わさって、どのシステム上のどのユーザーアカウントを侵害することで環境に対して強力な機能を付与することができ、本番環境へのセグエ(訳注:滑らかな移行手段)として機能する可能性を持つ状態につながります」

Verbatim from OWASP Top 10 CI CD SEC-2 https://owasp.org/www-project-top-10-ci-cd-security-risks/

結論

シャドーアクセスは、新しい現象として、クラウドコンピューティングの多くの分野に影響を与えています。この課題に対処し、意図されたアクセスとデータセキュリティの状態を再確立し、クラウドの利点をフルに達成するためには、新世代のツールとプロセスを確立し搭載する必要があります。

シャドーアクセスを理解する作業はまだ始まったばかりです。自動化、AI、およびデータといった広範なトレンドは、シャドーアクセスが増えていく多くの環境を作り出しています。シャドーアクセスはアクセスだけでなく、ゼロトラスト等に広範囲に影響を与えます。シャドーアクセスとゼロトラスト、その他多くの分野との関係については、今後の文書で詳しく説明する予定です。