クラウド脅威モデリング

cloud security alliance Japan Chapter

cloud security alliance®

The permanent and official location for Top Threats Working Group is
https://cloudsecurityalliance.org/research/working-groups/top-threats/

Acknowledgments

Lead Authors:

James Bore
Jon-Michael C. Brook
Alexander Stone Getsin
Vic Hargrave
Vani Murthy
Michael Roza
Vladi Sandler

Contributors:

Randall Brooks
Ken Dunham
Nirenj George
Ebudo Osime
Fadi Sodah
Adalberto Valle

CSA Staff:

Sean Heide
Stephen Lumpe (Cover design)
AnnMarie Ulskey (Layout and card designs)
John Yeoh

日本語版提供に際しての告知及び注意事項

本書「クラウド脅威モデリング」は、Cloud Security Alliance (CSA)が公開している「Cloud Thread Modeling」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
2021年10月31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

「クラウド脅威モデリング」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）

太田　吏城
塩田　英二
鈴木　伸
高橋久緒
福井　将樹
満田　淳
山口　弘行
渡邉　浩一郎　CISA,CISSP

目次

はじめに

企業は、新しいビジネスモデルや事業の拡大を可能にするため、クラウド技術に注目し、経済的な機会を生み出すことを目指しています。その際に問題となるのが、スキルギャップやセキュリティ、そして異なるクラウドサービスプロバイダやモデル、テクノロジをサポートするために必要な技術的な専門知識です。

攻撃者が攻撃を仕掛ける前に、攻撃や悪用される可能性のある弱点を特定することは、セキュアな開発・設計において非常に重要な作業であり、含める機能を決定したり、セキュリティの取り組みに優先順位をつけたりすることができます。脅威モデリングは、OWASP、NIST、および業界の安全なソフトウェア設計思想のリーダー（マイクロソフト）など、業界をリードするベストプラクティスで規定されているため、安全なソフトウェア開発ライフサイクル（セキュリティテストを含む）の基礎となるプロセスとして、組織に推奨されるプラクティスです。脅威モデリングは、システムやアプリケーションのセキュリティに関する考慮事項、主に脅威、および予防策のイメージを描き、特定するものです。

クラウドの急速な普及は、過去40年間の情報技術の発展によって培われてきたいくつかのセキュリティ方法論を凌駕しました。脅威モデリングは、クラウドの導入速度に追いついていない、あるいは同等でない、あるいはマッチしていないセキュリティ方法論の1つです。脅威モデリングという重要なプラクティスを、クラウドサービス、テクノロジ、モデルに合わせることには大きなメリットがあります。

クラウド特有の脅威の要因として、抽象化モデル、責任共有の境界、信頼性のメカニズム、同じ技術を提供するクラウドサービスプロバイダ（CSP）の多様性などが挙げられます。クラウドシステムにおける脅威モデリングが軽視されている主な要因は、ガイダンス、専門知識、プラクティスの適用性にギャップがあることです。本書は、このギャップを埋めることを目的としています。

クラウドのシステム、サービス、アプリケーションのための脅威モデリング（クラウド脅威モデリング）は、今日のクラウドが主流のビジネスや業界において、組織がセキュリティに関する議論を始めることや進めること、セキュリティ管理策やギャップを評価して、システム設計や緩和策の決定を行うことを可能にします。

目的

本書の目的は、クラウドのアプリケーション、サービス、およびセキュリティに関する意思決定において、脅威モデリングを可能にし、推奨することです。この目的のために、本書は、脅威モデリングのセキュリティ目的の特定、評価範囲の設定、システム／アプリケーションの分解、脅威の特定及び評価、システム設計における脆弱性の特定、緩和策及び管理策の策定及び優先順位付け、行動喚起の伝達／報告に役立つ重要な指針を提供します。

想定読者

この文書の想定読者は、脅威を分析し、システムの準備状況を評価する、もしくはクラウドシステムやサービスを設計するクラウドおよびセキュリティの実務者です。しかし、CIO、CISO、上級管理者にとっても、クラウド脅威モデリングとは何か、その独自の役割、標準的な脅威モデリングとの違い、その目的、サイバーセキュリティ戦略の中での位置づけなど、論点や洞察があります。開発者やアーキテクトが、セキュアなクラウドシステムを設計する際にこの文書が役立つと思われますし、監査人や規制当局にとっても企業の脅威モデリング活動を評価する際にも役立つものと期待しています。

主な論点

- 脅威モデリングは、クラウドのサービス、アプリケーション、システムにとって有益です。クラウドの導入、最もセキュアな利用やサービス、マルチテナンシーモデルの選択、および重要なクラウド脅威の緩和策が可能になります。

- クラウド脅威モデリングは、標準的な（オンプレミスの）脅威モデリングと比べて、実施方法が異なるわけではありませんが、クラウド特有の考慮事項（本書で説明）に加えて、独自の知識、業界の参考文献やリソースをフルに活用する必要があります。

- 組織は、クラウド脅威モデリングを今すぐ開始することを推奨されています。「クラウド脅威モデリングの作成」の章をご覧ください。

脅威モデリング

クラウド脅威モデリングについて説明する前に、さまざまな標準規格やベストプラクティスを参考にした基本的な脅威モデルとプロセスについて説明しますが、これらはクラウド脅威モデリングの基礎として最適であると考えています。

脅威モデリングは、計画中または既存のシステムやアプリケーションに対する主要な脅威、攻撃ベクター、予防策を特定し、説明する技術で構成されています。したがって、関連する管理策を早期に特定し、上記の項目の指針とすることができます。

脅威モデリングの目的：

- セキュリティ上の脅威の特定、分析、評価
- 優先順位をつけた緩和策の作成
- 攻撃対象領域の分析とリスク軽減の支援と情報提供

STRIDE[1]、MITRE ATT&CK、OWASP脅威モデリング、PASTA[2]を分析し、脅威モデリングのコアとなるプロセスステップを次のように検討しました（より包括的なリストは、参考資料を参照してください）。

[1] STRIDE - Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege, a widely used threat model.
[2] PASTA - Process for Attack Simulation and Threat Analysis (PASTA)

コアとなる脅威モデリングの取り組み：

1. 機密性、完全性、可用性、プライバシーなどの重要な側面に焦点を当てて、以下のような脅威モデリング演習のために**脅威モデリングのセキュリティ目標を特定**します。
   a. 顧客情報や規制対象の情報を含む会社のデータベースを外部の攻撃者から保護します。
   b. 電子商取引のウェブアプリケーションの高可用性を確保します。
   c. 攻撃対象領域または顧客のセキュリティ責任が最も少ないクラウドアプリケーションモデルを選択します。
2. システムまたはクラウドアプリケーションの概要を提供することで、検討中のシステムやクラウドインフラストラクチャに関する**アセスメントの範囲を設定**します。これは通常、使用されている技術スタックを含む様々な組織の資産、既存のセキュリティ対策、展開シナリオ、ユーザの種類、脅威モデリングで対処する必要のある特定のセキュリティ要件または規制要件などの分野をカバーします。
3. **システム／アプリケーションの詳細**では、システムをサブシステムに分解し、さまざまなコンポーネント間の相互作用を検証します。このフェーズで行われる主なアクティビティは次のとおりです。
   a. **信頼の境界の理解**（外部と内部の境界、特権、未認証など）
   b. **システムへの入力と出力**（インプットとアウトプット）、**データフォーマットの識別**
   c. **システム内のデータフローのマッピング**
4. **潜在的な脅威を特定し評価します**。つまり、脅威、攻撃の種類、特定のシステムまたはその機能が悪意のあるユーザによってどのように悪用される可能性があるかを特定します。一般的な脅威には、不正アクセス、サービス拒否、情報開示などに関連しています。脅威の深刻度は、DREAD[3]などのフレームワークを用いて評価することができます。
5. **システム設計とコンポーネントの弱点とギャップを特定**して、セキュリティに関する意思決定を支援し、セキュリティテストの範囲と性質を定義します。
6. 所定の脅威に適用可能な**緩和策と管理策を計画して優先順位を付け**、それらの管理策がどのように脅威またはリスクレベルを低減するかを反映します。
7. **コミュニケーションと対応の呼びかけ**： 特定された脅威と、それらの潜在的な影響と重大度、および適用可能であり提案された管理策を伝えます。モデリングデータと洞察を利用できるようにし、設計または効果による脅威の軽減の行動を呼びかけます。

さらに、以下の手順は、必ずしも脅威モデリングの一部ではありませんが、実施可能なものであり、多くの場合推奨されます：

- 既存の管理策の評価を実施し、考慮に入れることができます（システムが設計・開発中ではなく現存している場合）。
- 対象となるシステムへのセキュリティテスト（ペネトレーションテスト、セキュリティ要件テストなど）。
- 指標の測定とコントロールの主要パフォーマンス指標の評価。
- 識別された脅威は、マイクロソフト社のSTRIDEモデルなどのよく知られたモデルに基づいて分類できます。
- 攻撃のモデル化：脅威または攻撃対象領域の視覚的表現を作成します。
  脅威モデルおよび／またはセキュリティコンセプトレポートを作成し、範囲、脅威モデルの考慮事項、緩和策と脅威に関する詳細なガイダンスを提供します。詳細は「付録」の章を参照してください。
- 緩和計画またはより包括的なリスク分析および対応計画の考案。
- 脅威アクターの分析（動機、手段、方法、技術、洗練度、業界の脅威アクターとのマッチ

[3] DREAD (D = damage, R = reliability, E = exploitability, A = affected users, D = discoverability)

ングなど）

検討のために、「付録1：脅威モデリングレポート作成に関する詳細なガイダンス」を提供します。

セキュアソフトウェア開発ライフサイクル（SSDLC）[4]のベストプラクティスフレームワークでは、セキュアなソフトウェア設計の重要な初期段階として、ソフトウェアの脅威モデリングが義務付けられています。さらに脅威モデリングはアクティブセキュリティテストの実施に役立ちます。

脅威モデリングは、セキュリティ（ペネトレーション）テストのためのベストプラクティスとしてよく知られています； 脅威モデルを用いることで、テストの主要な目的に集中することができ、テストの投資対効果を高めることができます。また、その有効性を評価し、保証と信頼を確立するために、脅威モデリングで考案されたコントロールの実装後にもテストを実施する必要があります。

最後に、脅威モデリングはシステムのライフサイクルのどの段階においても、常に実施すべきものです。

さらに、クラウドの脅威モデリングがオンプレミスの脅威モデリングとどのように異なるかについての洞察と、それをどのように実施すべきかについての我々の提案について説明します。

クラウド脅威モデリング

さらに、クラウド脅威モデリングは、クラウドのサービスやアプリケーション固有の品質や考慮事項を説明するため、標準的な脅威モデリング手法を拡張します。以下の考察は、クラウド脅威モデリングが、非クラウド脅威モデリングとどのように異なるかを説明するものです。セキュリティ及びクラウドの専門家は、脅威モデリングをより効果的かつ頻繁に活用するために、これらの洞察と提案を検討することをお勧めします。

クラウド脅威モデリングは、アタックサーフェスの特定及び削減を補い、さまざまなクラウドサービスプロバイダのセキュリティ要件の抽象化を支援し、リスク管理に役立てられます。

クラウド脅威モデリングの目的は、非クラウド脅威モデリングとは異なりますか？

クラウド脅威モデリングは（非クラウド脅威モデリングと）同様の目的で役に立ちますが、追加の利点を提供します。

クラウド脅威モデリング（クラウドのシステムやサービスの脅威モデリング）の目的は、非クラウド脅威モデリングの目的と似ています。どちらの場合でも、優先順位が付いた緩和策が導き出され、セキュリティ上の考慮事項が評価され、脅威が特定されます。

まず初めに、クラウド脅威モデリングは、セキュアなクラウドの採用を可能にし、推進します。クラウドテクノロジの登場以来、セキュリティが、他のテクノロジやテクノロジの変化よりもクラウドの採用を妨げると考えられていました。テクノロジ、規制、リスクなどのセキュリティ関連の障壁のほとんどは削除または克服されたにもかかわらず、意思決定者は依然として次のような問いかけをします。

[4] CSA Six Pillars of DevSecOps: Automation page 10 Figure 1 Secure Development Lifecycle

- マルチテナント方式で、X 社とそのクラウドサービスやインフラストラクチャを信頼できますか？
- 主要なビジネスや財務プロセスを、自社施設から SaaS に移しても安全ですか？
- クラウドは機密データや規制対象データに対して、十分なプライバシーおよび機密性のコントロールを提供できますか？

クラウド脅威モデリングは、上記のような問いに答えるのに役立つ有効なステップです。脅威、資産、セキュリティコントロールに関する理解をもたらし、その結果、利害関係者に情報を提供し、意思決定を支援することにより、信頼を醸成します。

次に、クラウド脅威モデリングは、最も確実な、サービス、配備、およびマルチテナンシーモデル構成を選択するのに役立ちます。サービスモデル（SaaS、PaaS、IaaS）、配備モデル（プライベート、パブリック、ハイブリッド、コミュニティ）、およびマルチテナンシー環境を選択する時の主な考慮事項は、ビジネス目標、セキュリティ、および規制です。クラウド脅威モデリングは、特定のモデルまたはデザイン固有の脅威としてどのようなものがあるか、どのようなコントロールが利用可能か、またそれに応じてどのようなセキュリティ対策が講じられるべきかを判断するのに役立ちます。

クラウド脅威モデリングのモデルコンポーネントは、非クラウド脅威モデリングとは異なりますか？

モデルの構成要素は同じですが、クラウド固有の機能に関する説明や要素を含んでいます。

クラウド脅威モデリングの実施においては、脅威、資産、実施されているコントロール、脆弱性、適切なコントロール、評価などを引き続き考慮します。

- **範囲**　クラウドのシステムやサービスの脅威モデリングの範囲に関する考慮事項として、アイデンティティ管理、クラウドサービス構成、さらには基盤となるクラウドアカウントについて考慮します。
- **資産**　クラウド脅威モデリングの主な関心事であり続けます – データ、主要なシステムコンポーネント、金銭的な価値のある機器、及びアイデンティティ。ただし、クラウドアカウント、SaaS サブスクリプション、サービスなどといった新しい資産も導入されています。
- **脅威**　クラウドシステム、アプリケーション、および環境に対する脅威は独特です。インスタンスメタデータサービスやクロスアカウント IAM アクセスフェデレーションなどのさまざまなテクノロジが登場しています。さまざまなテクノロジや消費モデルがクラウドシステムを描写しています。そのため、さまざまな攻撃がそれらに対して実行可能であり、他の場合とは異なる影響や影響の重大性になります。
- **実施されるコントロール**　CSP に組み込まれている場合もあれば、CSP の責任範囲から外れている場合もあります。一般的に、クラウドのシステムやサービスは、非クラウドのシステムやサービスよりも多くの組み込まれたコントロールの恩恵を受けます。
- **格付け**　クラウドを範囲内にするかどうかに関係なく、重大度による脅威の格付けは必要であり、同じ考慮事項が適用されます – システムが特定の脅威に対してどれほど脆弱であるか、どの資産が影響を受けるか、そしてどの程度か。クラウドアカウント、システム、およびサービス品質によって、クラウドにおいて本質的に深刻な脅威もあれば（管理

アカウントの侵害など）、そうでないものもあります（インフラストラクチャ／プロトコルのサービス拒否など）。重大度＝発生可能性 x 影響。

- **提案される緩和策**　これは、異なる脅威にさらされていることから、クラウドのシステムやアプリケーションによって大きく異なります。さらに、AWS アカウントのサービスコントロールポリシーのように、独自に開発・設計されており、特定のクラウドシステムやアカウントでしか利用できない、または適用できない対策もあります。さらに、新しい独自のクラウドのコントロールやテクノロジ（メタデータサービス保護、CSPM[5]など）は、クラウドのサービスやアプリケーションに適用可能であり、考慮に入れる必要があります。

クラウド脅威モデリングで考慮される脅威は、非クラウド脅威モデリングとは異なりますか？

クラウドのシステム、アプリケーション、及び環境に対する脅威は独特です。インスタンスメタデータサービスやクロスアカウントIAMアクセスフェデレーションなどのさまざまなテクノロジが登場しています。さまざまなテクノロジと利用モデルがクラウドシステムを描写しています。そのため、さまざまな攻撃がそれらに対して実行可能であり、他の場合とは異なる影響や影響の大きさになります。

この研究グループの研究の多くは、クラウドの脅威について学ぶことを狙いとしています。リスクまたは影響が非クラウドと同様と判断した場合であっても（例えば 11の悪質な脅威#1：データ侵害）、脅威は独特のものです（AWS EC2 instance metadata account hijacking, Imperva breach, 2018 等）。

クラウド脅威モデリングの成果物は、非クラウド脅威モデリングとは異なりますか？

クラウド脅威モデリングの成果物やアウトプットは、標準の脅威モデリングのものと似ています。

ただし、クラウドのアプリケーションやサービスの脅威モデリングは、クラウドに関連した独自の決定に大きな影響を与えます。

脅威モデリングの成果物またはアウトプットは次のとおりです。

1. 脅威モデル。通常、Excel シートまたはツリー型マッピングなどのビジュアルモデルを介して提示されます。
2. 優先順位がランク付けされた緩和コントロール
3. セキュリティとデザイン上の決定、またはより明確かつ詳細な実施項目

アセスメントデータ及びその視覚化のモデルは、クラウドであるかどうかに関わらず、すべてのアプリケーションに固有のものです。そのため、これらの用語にはクラウド固有の区別はありません。優先度の高い緩和コントロールも、クラウドであるかどうかに関わらず、すべての範囲に対して固有のものです。

最後に、デザイン上の決定（またはより明確かつ詳細な実施項目）ではアウトプットが異なりま

[5] CSPM - Cloud Security Posture Management (CSPM), monitor for, find and remediate cloudmisconfigurations.

す。脅威モデリングの目的で述べたように、クラウドセキュリティに関するユニークかつ影響力の高い洞察は、クラウドの採用が実行可能な選択肢であるかどうか、また、どのクラウドモデルが最適であるかを判断するのに役立ちます。他のセキュリティ活動やアーキテクチャ評価では、技術的な構成要素に関する設計上の決定をもたらしますが、クラウドのアプリケーションやサービスの脅威モデリングは、クラウド関連の決定に大きな影響を与えます。

クラウド脅威モデルの構築は誰が責任を持つべきでしょうか？

クラウド脅威モデリングは、脅威モデリングチームにクラウドに関する専門知識を必要とします。

理想的には、クラウド脅威モデルは、セキュリティとクラウドの専門知識を持つ個人及びチームによって作られるべきです。正確な脅威モデルには、システムの全体的なアーキテクチャ、コンポーネント/サービス、インフラストラクチャ、ビジネス状況の理解と、対象システムまたは設計に関連する敵対的な視点が必要です。

アプリケーションアーキテクト/アナリスト、クラウドアーキテクト/アナリスト、セキュリティアーキテクト/アナリスト、及びその他の技術的な立場にある個人や役割に相談する必要があり、彼らは通常、クラウド脅威モデリングを主導するために十分な情報と専門知識を備えています。

クラウド脅威モデリングプロセス

クラウド脅威モデリングのプロセスは、クラウド以外の脅威モデリングとは異なりますか？

プロセスに違いはありませんが、他のいくつかの手順、方法論、およびニーズを組み合わせたものになります。ニーズには、例えばリスク等を処理するためのアプローチとして攻撃/障害キルチェーンにおける根本原因の検出や構成段階に焦点を当てたクラウドインフラストラクチャ（クラウドスタック）の全体的なレビューなどがあります。このプロセスは、プロファイルされた各システム/アプリケーションに対して繰り返すことが可能である点に留意することが重要です。

また、採用されているクラウドサービスモデル（つまり、IaaS / PaaS / SaaS）と、CSPとそのユーザー（CSC）の責任（セキュリティを含む）を定義する責任共有モデルを明確に理解する必要があります。 説明責任を有する組織は、潜在的な脅威を特定して軽減するために必要なアクションに対して責任を負います。たとえば、ほとんどのクラウドプロバイダには、基本的なDDoS保護がサービスに含まれますが、高度な保護はオプションかもしれません。

コア脅威モデリングアクティビティ

1. **脅威モデリングのセキュリティ目標の特定**：セキュリティ目標と要件を特定します。組織のポリシーとビジネスニーズは何ですか？ また、コンポーネント、役割、サービス、依存関係などを含むターゲットシステムのアーキテクチャを特定します。脅威モデリング実施の標準的な目標設定（最も影響力のあるコントロールまたは最も差し迫った脅威の特定、機密性の保護等）を補完するものとして、「クラウド」またはクラウドアーキテクチャ（PaaS、マルチテナンシーなど）が許容可能かどうかを判断し、最もリスクを回避できるクラウドサービスと配備モデル（IaaS、PaaS、SaaS）の特定を行う等、クラウド脅威モデリングのセキュリティ目標を設定することが重要です。
2. **アセスメントの評価範囲の設定**：資産を特定してスコアリングすることにより、レビュー中のシステムまたはアプリケーション（データ、アプリケーション、システム、ユーザ、コントロールなど）の概要を提供します。

   次のようなクラウドスタック関連の質問を検討してください。
   a. PaaSコントロールプレーンは範囲内にありますか？
   b. クラウドアカウントは対象範囲ですか？
   c. 包括的スコーピングを行うことをお勧めしますか？
3. **システムとアプリケーションの詳細**：これは、通常、システムをサブシステムに分解し、さまざまな小さなコンポーネント間の相互作用を調べます。システムをさらに分解して、システムがどのように機能し、それらの機能がどのように脆弱なのかを特定します。例えば、アプリケーションは転送中のデータの機密性をどのように保証しますか？
   a. **信頼の境界の理解**（外部境界、内部境界、特権、認証されていない等）。CSPへの信頼とCSPの隔離の管理、複数にわたるサービスとアカウントの信頼、マルチテナンシーとしての隔離の管理などのクラウドの信頼境界を理解します。
   b. **システムへの入口と出口のポイント**（入力と出力）とフォーマットの特定。 クラウド管理API、マネージドAPIゲートウェイ、インバウンドとアウトバウンドの接続、統合な

ど、クラウド固有のエントリポイントを考慮します。さらに、複数にわたるクラウドサービスの関係をマッピングします。

c. **システム内のデータフローをマッピング**。クラウドEMR、ETLサービス、BLOBストレージ、アカウントログトレイルなどのクラウド固有のデータフローと格納を考慮します。

4. **脅威の特定と評価**：脅威、攻撃の種類、および与えられたシステムまたはその機能が外部の攻撃者または悪意のあるユーザによって悪用される可能性のある様々な方法を特定します。CSA 重大脅威（Top Threats）等の業界リソースを使用して、クラウド固有の脅威を特定します。「可用性」確保のための多くの制御がCSAプラットフォームとインフラストラクチャに組み込まれていますが、「可用性」に対する脅威の評価を怠らないでください。ヒューマンエラー、内部不正に対する脅威、設定ミス、および設計の不備に特に注意してください。
5. セキュリティ判断を支援し、セキュリティテストの範囲と性質を定義するために、**システム設計とコンポーネントの弱点とギャップを特定**。一般的で影響力のあるクラウド設計や実装の弱点を検討し、多層防御の設計/制御を考慮します。
   a. 11の悪質な脅威[6]#2 – 設定ミスと不十分な変更管理
   b. EE#3 – クラウドセキュリティアーキテクチャと戦略の欠如 *（訳注： EEは「11の悪質な脅威（Egregious Eleven）」を意味します）*
   c. EE#4 – 不十分なID、資格情報、アクセス、キー管理
   d. EE#7 – 安全でないインターフェースとAPI
6. **事前に特定した脅威に適用可能な緩和策と制御を設計**して優先順位を付け、それらの制御が脅威またはリスクレベルをどのように低減するかを反映します。クラウドのセキュリティコントロール（マトリックス）[7]を活用し、いくつかのクラウドとアプリケーションの設定ミスや弱点が存在する場合でも、「攻撃キルチェーン」を含むクラウドの脅威をなくす制御に焦点を当てます。
7. **コミュニケーションと対応の呼びかけ**：適用可能で提案された制御と共に、特定された脅威、それらの潜在的な影響と重大度を伝達します。 モデリングデータと洞察を利用できるようにします。 クラウド設計の判断とコアを可能にするクラウド制御について伝達します。
8. **定期的な再評価**：クラウドプラットフォームは急速に進化しており、静的ではありません。脅威モデルも同様です。脅威モデルの定期的なレビューと更新により、脅威モデルがチームにとって適切で、非常に有用であることが保証されます。これは、アーキテクチャ全体に重要な変更がある場合（例えばコンポーネント/サービスの追加または削除など）に、特に当てはまります。時代遅れの脅威モデルは、新しい脅威ベクトルが考慮されず、したがって評価もされないという誤ったセキュリティ認識にチームを落ち着かせる可能性があります。

[6] Egregious Eleven cloud security concern, more in the CSA Top Cloud Threats Research work grouppublication *Top Threats to Cloud Computing: Egregious Eleven*

[7] The CSA Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing that maps and categorizes applicable cloud controls.

クラウド脅威モデルの作成

より多くの脅威モデリングが、設計または評価の一部としてクラウドシステムおよびサービスに適用されることが私達にとって期待される成果です。読者には、クラウド脅威モデルを今すぐ作成し、このリソースを活用することをお勧めします。

どのようにしてゼロから始めるか

クラウドの脅威モデリングを開始するために、セキュリティの専門家である必要も、脅威モデリングに熟練している必要もありません。専門家は、脅威のモデル化手法を補完するものとして、この文書を使用することができます。

ゼロから始める人のためには、まず小さなものから、慣れ親しんだものから始めます。

1. 付録2: クラウド脅威モデリングカード の脅威、脆弱性、コントロールのいずれか、または最も懸念される、あるいは最もよく知られている別の脅威モデルカードを選択します。
2. 他のカードのいずれかがあなたのカードに関連しているかどうかを判断し、{脅威、脆弱性、コントロール、資産の推奨順序に従ってそれらを整列させるか、視覚的に配置します。
3. 開発中のモデルに関連する脅威、脆弱性、コントロール、資産をさらに識別し、それらを視覚化または分析のために「混ぜ合わせた状態」にします。最新のCSA「クラウド重大セキュリティ脅威 11の悪質な脅威」を参照してください。
   - 各カードタイプのうち少なくとも1つが存在するまで繰り返します。
4. すべての脅威及び脆弱性が少なくとも1つ又は2つの適切な特定の管理によって対処されることを確保します。
5. プロセスが完了しました、おめでとうございます!

あるいは、より詳細で包括的なアプローチが必要な場合は、「クラウド脅威モデリングプロセス」で説明されている手順に従うことを検討してください。

モデリングが終了したら、セキュリティ評価を完了し、実行可能な手順、あるいはすでに実行された手順であるかを決定します。識別されたコントロールに基づいて行動し、脆弱性を緩和します（または、脆弱性がないことの保証を確立します）。

結果は基本的な脅威モデルのように見えますが、次のセクション「クラウド脅威モデル リファレンス」では、クラウド固有の考慮事項について説明します。

クラウド脅威モデル リファレンス

前のセクションで説明した手順を使用して作成した、基本的なクラウド脅威モデルのリファレンスを次に示します。

CSA 「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 ディープダイブ」を参照し、2019

年に起きたダウ・ジョーンズのデータ漏洩を思い出してください。

- **アクター**:　ダウ・ジョーンズに帰属する、AWSがホストするElasticsearchデータベースのパスワードによる保護に失敗したダウ・ジョーンズ認定サードパーティベンダー。
- **攻撃**:　データベースはパスワードで保護されておらず、誰にでも利用される状態でした。また、この不具合は誰でも利用が可能なIoT検索エンジンで見つけることができるものでした。この誤って設定されたデータベースは、著名なセキュリティ研究者によって2019年に発見され、ダウ・ジョーンズへ報告されました。
- **脆弱性**:　おそらく信頼された認定セキュリティベンダー中の１社がダウ・ジョーンズデータベースをパスワードで保護しなかった。

次に、付録2: クラウド脅威モデリングカード に記載されているクラウド脅威モデルカードだけで構成される基本的な脅威モデルを示します。

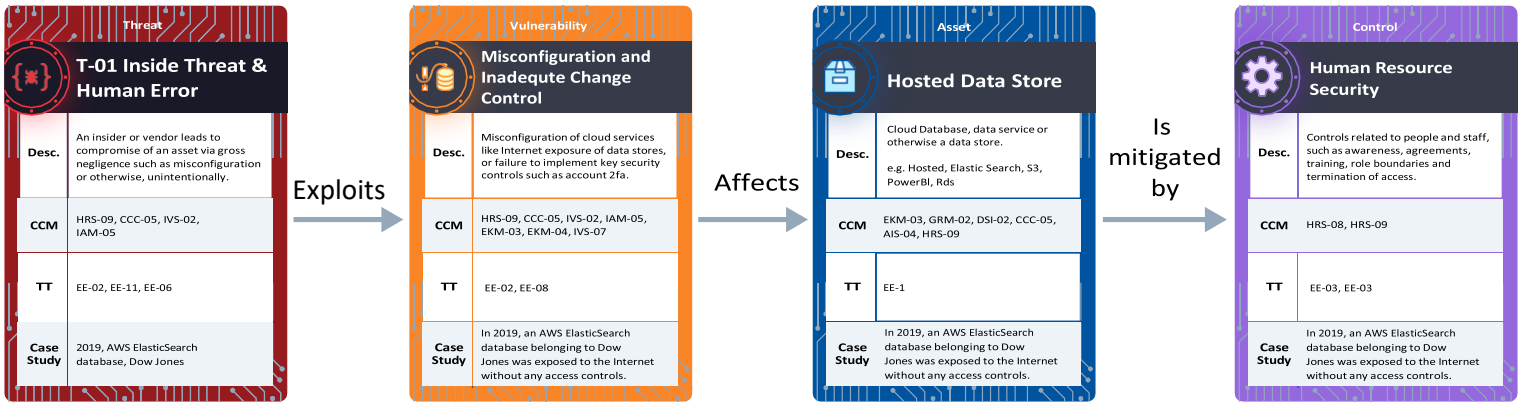


図1

しかしながら、このモデルは完全ではありません。私たちのクラウド脅威モデリングカードは、モデルを完成させるのに良いスタート地点になります。カードが組み込まれた後、適用可能な脆弱性と制御を拡張することができます。

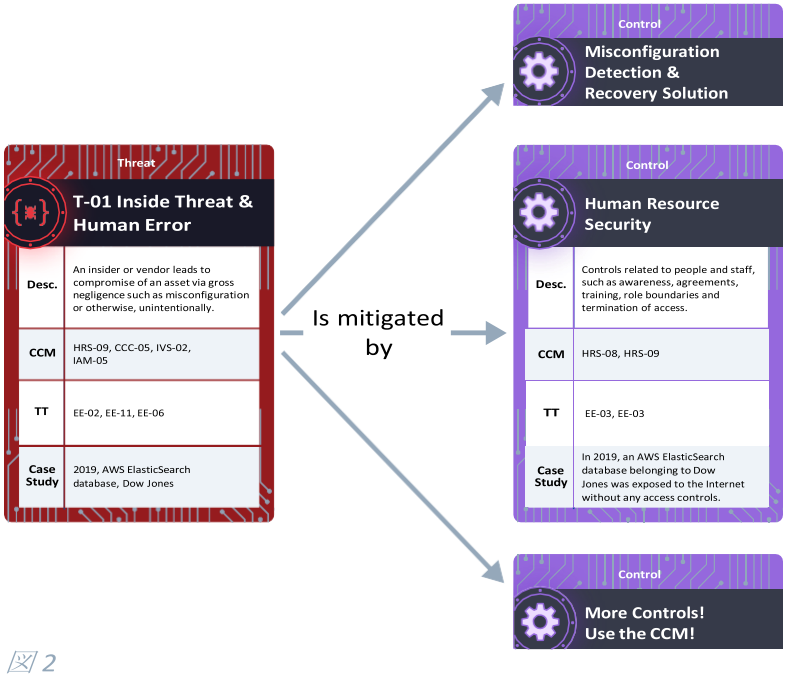


図 2

おわりに

要約すると、脅威のモデル化は、ソフトウェアおよびシステムのセキュリティにとって不可欠な実践方法であり、クラウドのソフトウェア、システム、およびサービスにとっては特に重要です。組織は、これらの脅威をモデル化するために、構造的で反復可能なアプローチを開発する必要があります。脅威モデリングを行うことで、チームはサイバー攻撃のプロセスを予測し、攻撃が起こる前に脅威の影響と可能な対策を事前に準備することができます。

これは抽象度が高く、偏在性があり、信頼境界線が共有されているクラウドが対象となる脅威モデルの実践において特にあてはまります。脅威のモデル化はセキュリティに関する議論を容易に開始でき、懸念事項と適用可能なコントロールの確立や理解するためのコミュニケーションを助けます。
これにより、組織はクラウドの設計と脅威の軽減策に関する意思決定を行うことができます。

サイバーセキュリティのリスク管理には、組織の中核的なリスク目標、目的、および高価値な資産の保護に関連する人、プロセス、および技術の優先順位付けが必然的に含まれます。これは、部分的には脅威、ツール、戦術、および手順（TTP）を特定することによって達成されます。このような脅威とTTPが特定されると、組織はリスクを管理するためにそれらを予防的、検知的、および是正的コントロールにマッピングすることができます。脅威モデルカードを使用することで、リスク管理プロセスに脅威の考慮を導入し、時間をかけてサイバーセキュリティプログラムを成熟させることができます。

この資料とガイダンスが、企業が脅威モデリングを始める際、または改善する際に役立つことを願っています。

今後の出版物では、クラウド脅威のスコアリング、ATTACK IDやその他の業界の参考資料、そしてより完全なクラウド脅威モデリング・カードデッキなど、クラウド脅威モデリングに関するさらなる洞察を提供していきたいと考えています。

乞うご期待!

参考資料

- https://en.wikipedia.org/wiki/Threat_model
- https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- https://www.microsoft.com/en-us/securityengineering/sdl/practices
- Microsoft Threat Modeling Tool: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
- Model vs methodology: https://drive.google.com/file/d/1n_uMBckp8UMBA1oq1kcKTjvXX6Ea_tLF/view?usp=sharing
- CSA Cloud Top Threats Egregious Eleven: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/
- CSA Cloud Top Threats Deep Dives Egregious Eleven: https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/
- CSA CCMv4 Matrix: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/
- Security Guidance for Critical Areas of Focus in Cloud Computing v4.0: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/
- CSA The Six Pillars of DevSecOps: Automation (Pillar 5): https://cloudsecurityalliance.org/artifacts/devsecops-automation/
- Chapter 4 - A Threat Analysis Methodology for Cloud Using CCM" in the CSA's Certificate of Cloud Audit Knowledge Common Body of Knowledge
- PASTA (Process for Attack Simulation and Threat Analysis)
- VAST (Visual, Agile, and Simple Threat Modeling)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
- DREAD risk assessment model
- NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
- MITRE ATT&CK - attack.mitre.org

付録1：脅威モデリングレポート作成に関する詳細なガイダンス

脅威モデリングレポートにマッピングされたセキュリティ設計報告書について検討します。この報告書には、提案されているセキュリティ管理の技術レベルの説明と、詳細な要件及び関連するリスクへのリファレンスが含まれます。

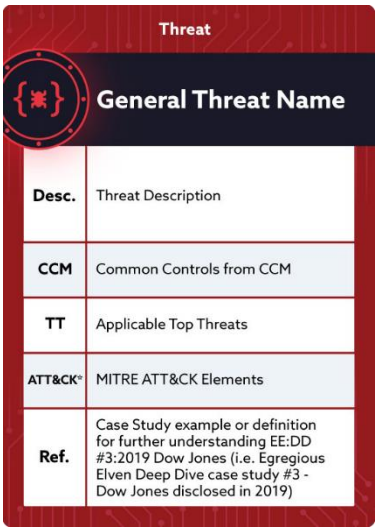
この文書は、以下の章から構成されます:

- **エグゼクティブサマリー**: プロジェクトの一般的な説明、主な目標、クラウドアーキテクチャのスナップショット。
- **システム／アプリケーションの詳解**: 一般的には、システムをサブシステムに分解し、様々な小さなコンポーネント間の相互作用を検証する内容となります。
- 攻撃ベクトルのマッピング:アーキテクチャで検出されたリスクの上位5つを説明する。説明文、検出されたリスクのアイコンが表示されたクラウドアーキテクチャのスナップショット、セキュリティ・リスクの総合スコア、まとめの章を含みます。
- **脅威モデル**: 視覚的、関係的、テキスト的など、様々な脅威モデルの構成要素やインサイトを表現し、それらの関係をマッピングしたもの。
- **緩和策**:この章では、優先順位の高い順に、必要なセキュリティ対策の実施内容を記載します。各セキュリティ対策は、以下のフィールドで構成されます。
  - セキュリティコントロール名（例：SC1-認証SSOメカニズムの実装
  - 優先度 - このフィールドは実装の優先度を定義するために必要であり、重要/高/中/低のように設定されます。
  - リスク - 脅威モデルレポートに記載されている関連リスクへの参照（例：R1、R2、R5）。
  - 要件 - このセキュリティ対策に関連する技術レベルの要件のリスト コントロール。各要件は、しなければならない(must)、してはならない(must not)、すべきである(should)、すべきではない(should not)という言葉で始まります。例えば以下のような記述となる "システムは、JSON Web Token（JWT） フォーマットを使用した OAuth 2.0 規格を実装しなければなりません。”

付録2: クラウド脅威モデリングカード

以下に参考までに脅威モデリングカードと各要素の詳細の例を示します：

一般的な脅威の名称と説明 一般的な脅威の名称」の分類法は今後の研究課題となりますが、説明文と脅威の名称の両方がユーザの状況を補強するものである必要があります。



一般的な脅威の名称と説明: 一般的な脅威の名称の分類法は今後の研究課題ではありますが、説明文と脅威の名称の両方がユーザの状況を補強するものである必要があります。

「共通コントロール」と「重大脅威」: これらは、CSA が調査したコントロール（CCM）とクラウドの脅威（重大脅威:Top Threat）へのリファレンスです。脅威の中には、招かれざる訪問者を防ぐゲートの警備員のように、特定の緩和策とうまく調和するものがあります。これらのCloud Controls Matrixのドメインを共通コントロールのセクションにリストアップします。同様に、脅威がEgregious Elevenなどの最新のTop Threats ワーキンググループの出版物に該当する場合はここの記載に含めます。

ATT&CK: MITRE ATT&CK フレームワークへの外部参照により、研究者やカードユーザーが、一連の命名法や定義などの理解を深めることができます。

リファレンス:関連するケーススタディまたはTop Threats Deep Dive出版物への参照。

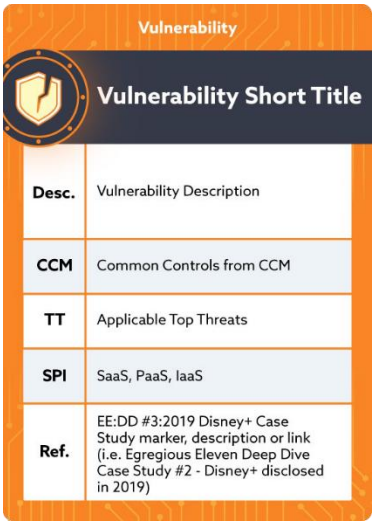
SPI資産の説明[8]: この欄には、SaaS、PaaS、または IaaS のいずれかのシステムのクラウド形態を記入します。Asset TitleとDescriptionには、他の人がカードを使用するのに必要となる情報を記入してください。

クラウドサービスプロバイダ: AWSとElasticSearchのように、一般的な用語で当該資産のCSPとサービスの例を明確にします。

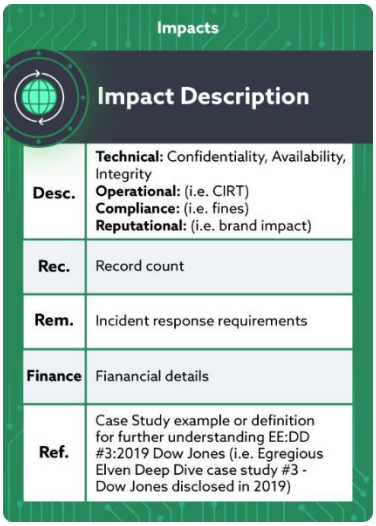
共通CCMコントロールとケーススタディ: 適用可能な標準的なCSA Cloud Control Matrix、該当の資産のタイプに一般的に適用されるコントロールを記載。ケーススタディは「脅威」セクションの説明に従います。

[8] SPI - SaaS/PaaS/IaaS cloud service models

脆弱性カードのために追加されたセクションの説明



SPIの適用性：　脆弱性は、責任共有モデル(Shared Responsibilities Model)に基づく様々なSPI（SaaS/PaaS/IaaS）のインスタンスや脆弱性そのものには適用されません。この場所では、アセットカードに対する脆弱性についてGOまたはNO-GOを素早く判断することができます。



インパクトの名称と説明：　技術的影響」または「ビジネス的影響」のいずれかを選択し、その状況について簡単に説明します。
影響の詳細については、CSA Certificate of Cloud Audit Knowledge Common Body of Knowledge の「第4章 – CCMを用いたクラウドの脅威分析手法」に記載されています。

テクニカルインパクトは、以下のカテゴリーに分けられます:

機密性：　情報の不正な開示により、組織の運営、資産、人材に限定的、深刻、または深刻な損害が生じること。

可用性：　情報の不正な変更または破壊により、組織の運用、資産、および人的資源に軽度の損害を与えること。

完全性：　情報または情報システムへのアクセスまたは使用が制限され、その結果、組織の運営、資産、または人的資源に限定的、重大、または深刻な損害が生じること。

ビジネスインパクトは、以下のカテゴリーに分けることができます:

「財務的な影響」の例としては、報酬や収益の損失、技術的な調査、ランサムウェアのシステムアップグレード、保険料の増加、訴訟費用、資金調達コストの増加、投資の減少、退職金、その他スタッフの解雇や採用にかかる費用などがあります。

「運用面での影響」の例としては、製品・サービスの売上減少、生産・サービスの遅延、BOM（部品表）の破損、生産・サービス計画ファイルの破損、製品・サービスの品質、製品・サービスの配送、新製品・サービス導入の遅延、生産・サービス報告システムなどが挙げられます。

「コンプライアンスへの影響」の例としては、規制当局による調査や罰金、影響を受けた個人に対する訴訟、その他の第三者に対する訴訟、規制当局による調査や訴訟を防御するための弁護士や専門家の雇用の必要性、法務・コンプライアンス機能の向上のためのコストなどが挙げられます。

「風評被害」の例としては、社会的認知度の低下、顧客との関係の悪化、サプライヤーとの関係の悪化、ビジネスチャンスの減少、採用難、主要スタッフの喪失、メディアによる批判などが挙げられます。

対応策:　インシデント対応の要件

コントロールカードへの追加項目

ドメインとコントロールタイトル: クラウドコントロールマトリックスからファミリーまたはドメインの短縮名とタイトルの記述を追加します。

プロセス:　このコントロールに関連する手順書の名前を入力します。

重大脅威:これらは、CSA のコントロールに関する研究（CCM）とクラウドの重大脅威へのリファレンスです。

ケーススタディの緩和策:　緩和策が判明している場合、特に、外部に公表されたものや、インシデント対応の経験から内部で導き出されたものやインシデント対応の経験から得られたものを記載。

関連するセキュリティツール(AST:Associated Security Tools):　セキュリティツールは発見的統制、予防的統制、 発見的統制のコントロールを行う際に役に立つ場合があります。