ゼロトラストのためのコンテキストベースアクセス制御

CSA JC cloud security alliance Japan Chapter

CSA cloud security alliance®

The permanent and official location for the CSA Zero Trust Working Group is https://cloudsecurityalliance.org/research/working-groups/zero-trust/

Acknowledgments

Co-Chair

Shruti Kulkarni

Lead Authors

Paul Simmonds
Clement Betacorne

Contributors

Irshad Javid
Hani Raouda
Kevin Dillaway
Heinrich Smit
Michael Roza

Reviewers

Daniele Catteddu
Jason Garbis
Michaline Todd
Jay Leslie
Antony Martin
Joseph Ohaeche
Kelly Onu
Joseph Emerick
Fernando Martins
Roberto Gomez-Vazquez
Rob Doyon

CSA Global Staff

Erik Johnson
Ryan Gifford
Stephen Smith

日本語版提供に際しての告知及び注意事項

本書「ゼロトラストのためのコンテキストベースアクセス制御」は、Cloud Security Alliance（CSA）が公開している「Context-Based Access Control for Zero Trust」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
2025年03月07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

「ゼロトラストのためのコンテキストベースアクセス制御」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
井上　尚人
笠松　隆幸
土肥　千明
諸角　昌宏
山﨑　英人
山下　亮一

目次

要旨

従来のアクセス決定は、ゼロトラストとコンテキストの両方に依存していませんでした。歴史的に、資産やリソースへのアクセスは信頼に基づいていました。デジタルアイデンティティは特定のエンティティに委託され、そのアイデンティティまたはアイデンティティを含むグループに権限が割り当てられ、リソースへのすべてのアクセス要求はそれらの権限にのみ照合されます。その後、ロールベースアクセスコントロール（RBAC）は、ロールに権限を割り当てることで、このモデルを強化しました。これは、エンティティが職務などのプロファイルを変更する際に、複数のきめ細かな役割の間を動的に移動することができたためです。複数のペルソナ（アイデンティティ）を保持することができ、それぞれが目的に応じて適切に許可されていますが、それ以上は保持できません。RBACは文脈にとらわれず、その大部分が暗黙の信頼に基づいています。権限は、特定の取引に関係なく、固定されたままでした。これは環境に対する暗黙の信頼につながります。

ゼロトラストは、暗黙の信頼や仮定を含む信頼をアクセス決定から排除し、リソースへの各アクセス要求をリスクに基づいて評価し、エビデンスに基づいて承認することを目的としています。リソースへのリクエストが受信されるたびに、アクセス管理プロバイダによって、単に権限に照らし合わせるだけでなく、リクエスト自体の属性、リソースのリスク分類、リクエスト元のアイデンティティの属性、一般的な属性、ソースデバイスのリスクプロファイル、ソースネットワーク、場所、IPアドレス、エンドポイントエージェントの存在（多くの場合）、時間帯などを組み合わせたコンテキストで評価されます。言い換えれば、コンテキストベースアクセス制御（CBAC）は、かつての信頼への依存を、アクセスルール、アクセスポリシー、属性のリクエストごとの評価に置き換えることで、ゼロトラストをサポートします。

対象読者

主な対象者：アイデンティティアクセス管理アーキテクト、ゼロトラスト・アーキテクト、セキュリティ・オペレーション・チーム

第二の対象者：アイデンティティとアクセス管理者、アイデンティティとアクセス管理エンジニア、法執行機関、チーフ・エクスペリエンス・オフィサー（CXO）

はじめに

国家安全保障電気通信諮問委員会（NSTAC）の「Report to the President on Zero Trust and Trusted Identity Management」では、ゼロトラスト（ZT）を「*いかなるユーザーや資産も暗黙のうちに信頼されることはないという考えを前提としたサイバーセキュリティ戦略です。これは、情報漏洩がすでに発生しているか、または今後発生することを前提としているため、組織の境界で行われる単一の検証によって、機密情報へのアクセスが許可されるべきではありません。その代わり、各ユーザー、デバイス、アプリケーション、およびトランザクションを継続的に検証する必要があります*」と定義しています。

従来の中央集権的な信頼ベースの「城と堀」の物理ネットワーク境界セキュリティアーキテクチャは、分散型クラウドコンピューティングとリモートワークフォースの時代には効果がありません。

インターネット接続を多用する、高度に分散した現代の企業ネットワークにおいて、技術的または人的な脆弱性を悪用することに、洗練された脅威行為者はますます習熟しています。サイバー攻撃は一般的に、何らかの形で誤った信頼を悪用します。このため、「信頼の前提」は危険な脆弱性であり、不利益を回避するために緩和・管理されるべきです。ゼロトラストでは、すべてのネットワーク接続とパケットは信頼されず、システムを流れる他のすべてのパケットと同じように扱われます。信頼レベルはゼロと定義されるため、ゼロトラストという言葉になります。

ゼロトラストは、クラウド/マルチクラウド（あらゆるサービスモデル）、オンプレミス/ハイブリッドシステム、社内外のパートナー/利害関係者のユーザー（組織管理およびBYOD（Bring Your Own Device））エンドポイントを包括する、総合的な企業セキュリティ戦略です。これには運用技術（OT）、産業制御システム（ICS）、モノのインターネット（IoT）が含まれます。その結果、ゼロトラストは、一歩ずつ登っていかなければならない（つまり、段階的に、できればリスクベースで実施されなければならない）山に例えられてきました。これらの原則は、CSAのZTガイダンスに共通するテーマです。

ゼロトラストの企業導入は広範に広がり、拡大しています。Venture Beatによると、クラウドに移行する企業の90%がゼロトラスト戦略を採用しており[1]、Gartnerは、2026年までに大企業の10%が成熟した測定可能なゼロトラストプログラムを導入すると予測しています[2]。

文書の範囲

本文書は、ゼロトラストアーキテクチャにおいてシグナルを消費し、リソースへのアクセスを許可する前にリスクベースの判断を提供し、コンテキストベースアクセス制御（CBAC）に関するガイダンスを提供します。本文書では、従来のセキュリティ管理策と、コンテキストやゼロトラストを用いて構築されたセキュリティ管理策を比較しています。この研究では、CBACがアクセス要求の受信速度とアクセス判断の速度とを対応させるように、消費されたシグナルを分析するためにAIモデルを利用しています。CBACの制約が文書化され、それに対処するためのソリューションが提供されます。成熟度モデルが開発され、ゼロトラストの段階的アプローチと成熟度に合わせた追加が行われました。現在、様々なベンダーが提供しているCBACソ

[1] Venture Beat, "Why 90% of Enterprises Migrating to the Cloud are Adopting Zero Trust
[2] Gartner, "Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero Trust Program in Place by 2026

リューションのバリエーションのリストを、 この文書の最後の方に追加しています 。本文書では、ゼロトラストの実装/アーキテクチャの詳細については触れません。また、AIとその構成要素にも焦点を当てていません。この文書は、CBACである特定の状況に対処するためにAIを使用したものであり、AIのみに焦点を当てた論文と解釈されるべきではありません。

背景

従来は、本人確認（認証）の後、エンタイトルメント（権限）に基づいてアクセス決定が行われています。本来、これらは静的な要素です。RBACは、潜在的に動的な要素を追加することによってこのモデルを拡張し、職務上の役割、機能、およびその他の静的な役割ベースのパラメータに対して変化する役割をもたらします。ゼロトラストは、属性などのダイナミックなリスクベースの概念によって、これらの判断をさらに強化することを提案しています。なぜなら、定義上、ZTの中核的な信条の1つは、すべてのアクセス要求は異なるものであり、個別に検討され、判断されなければならないということだからです。

属性は、a)送信され、b)消費されるまでは、必ずしもシグナルではありません。画面の背景や室温など、すべての属性が必ずしもアクセス決定に関連するとは限りません。しかし、シグナルの提供者（送信者）がそれを範囲内とみなし、意思決定者がそれを期待して消費するのであれば、関連している可能性があります。

意思決定者（ポリシー定義ポイント (PDP)、エンドポイント、サービス、 データベースなど）は、入ってきたアクセス要求を評価します。意思決定者は、アイデンティティのためのアイデンティティプロバイダ、ネットワーク属性のためのネットワークデバイス、クライアント属性の収集のためのクライアントエンドポイントサービスまたはデーモンなどのシグナルプロバイダ、およびリクエストが到着した時刻と日付のためのネットワークタイムプロトコル(NTP)に依存します。意思決定者は、リソースへのアクセスに対するその着信リクエストに対して、 コンテキストに基づくアクセス決定を行い、その後のリクエストを評価します。

CBACアプローチは、認証と認可の間のユーザー行動の変化に対処します。人間と人間以外のアイデンティティのコンテキストに基づいたアクセスを可能にします。適応認証は、組織がネットワーク境界ベースの防御から境界のない環境へと移行する中で、ゼロトラストに不可欠です。組織内の複数のリソースにアクセスする必要性は日々高まっています。BYODや組織支給デバイスの増加に伴い、アクセスメカニズムはより適応的で堅牢であるべきです。エンティティを表す適切なサブジェクト属性、使用するデバイス、ジオロケーション、または組織が合意できるその他の属性を利用できなければなりません。アクセスは、コンテキストの属性を考慮して評価されます。リアルタイムでコンテキストが確立されると、ポリシー実施エンジンにそれを供給して、適切なリソースへのアクセス許可に関するインテリジェントな決定を下すことができます。期待されたシグナルからの逸脱（あるいは文脈から外れたシグナル）は、侵害を意味します。ルールは、すべての利害関係者が合意した属性を考慮して作られるべきです。ルールを作成する際には、静的属性（ユーザー名、役割、アプリケーションID、デバイスIDなど）と動的属性（ジオロケーション、時間など）を分けて考える必要があります。しかし、ユーザーエクスペリエンスは、全プロセスにおいて考慮されるべき不可欠な要素です。

従来の信頼ベースのアクセスコントロール

アイデンティティやペルソナの数の増加に伴い、アイデンティティベースの攻撃や漏洩したクレデンシャルベースの攻撃が急激に増加しています。ここ数年のアイデンティティの増加の要因としては、クラウドの採用を含むデジタル導入の増加、かつての紙ベースのシステムのデジタル化の増加、モバイルデバイスの使用の増加、ダイナミックに変化する場所でのリモートワークなどが挙げられます。各エンティティは複数のアイデンティティ/ペルソナと関連付けられます。その結果、これらのアイデンティティの管理は複雑さを増しています。アイデンティティベースの攻撃は、侵害の主要なベクトルの1つです。Crowdstrike Global Threat Report 2024によると、脅威行為者はますます、侵害された認証情報を使用して、インタラクティブな侵入キャンペーンを実行するようになっています。最初に侵害されたホストは、必ずしも望ましい標的とは限りません。ラテラルムーブメントは、危殆化したクレデンシャルで可能になります。アクセスブローカーは、ランサムウェアの運営者など、他の行為者にアクセス権を売るためにアクセス権を獲得する役割を担っています。認証情報が侵害された結果、敵対者は機密データや知的財産の流出、アカウントのシャットダウン、国家攻撃の開始など、アカウントの乗っ取りに関連するあらゆる活動を実行できます。

アイデンティティベースの攻撃を行う理由の1つは、認証および認可を危険にさらすのにはわずかなミスのみで利用できることがあります。盗まれた、弱い、またはデフォルトのクレデンシャルを侵害に使用することは新しいことではなく、難しいことでも派手なことでもありませんが、広まっています。

かなりの数の違反は、間違って付与されたアクセスや悪意を持って取得されたアクセスから始まります。このようなミスや攻撃に直面した場合、これらの脆弱性を軽減するためには、侵害を早期に検出することが重要であり、CBACは効果的なソリューションを提供します。

従来のアイデンティティベースアクセス制御の失敗

今日使われているシステムのほとんどは、"バイナリー・アクセス "という概念に依存しています。システムはエンティティを認証し、認証が通ると仮定して、"これはエンティティである "というバイナリ・アサーションをアクセス制御システムに渡します。認証メカニズムとしてパスワードだけでは信頼性がますます低くなっているため、組織はMFA、SMS、トークン、その他の方法を用いてこのシステムを補強し、それが想定されるエンティティである確率を高めています。しかし、基本的で根本的欠陥は依然として残っています。システムは、中心点で二値（イエスかノーか）の決定を下し、これをパスします。アクセスされるシステムは、確実性のレベル、設定された「パスのしきい値」、またはそのパスを得るために使用された方法/仮定を知りません。

このため、組織が所有するアイデンティティエコシステムに全面的に依存することになり、組織はそのエコシステムに登録されたすべてのエンティティを（できればアイデンティティ防御のレベルで）維持および管理する必要があります。これは、組織が第三者からのアサーション、属性、識別子を受け入れることができないか、あるいは、受け入れられそうにないことを意味し、多くの場合、単にデータおよび/またはシステムにアクセスできるようにするために、雇用していない人や管理していない人を「不明なユーザー」として登録する必要があります。

CBAC は、エンティティがその主張する人物であることの確実性を向上させる可能性があり、システムが第三者からのクレデンシャル、アサーション、および属性を受け入れられるようにします。しかし、これが機能するのは、これらの認証情報をチェックするシステムが 、リスクを負ってアクセスを許可するシステムに必要な情報をすべて伝える場合だけです。

したがって、大規模にゼロトラストアーキテクチャを実装する場合、現代の組織が機能するために必要な膨大な数のスタッフ、非スタッフ、ユーザーデバイス、IoTデバイスなどに対応し、機能し、拡張するためには、適切にアーキテクチャ化されたCBAC実装が必要になる可能性があります。

コンテキストの定義

なぜコンテキストベースアクセス制御が重要なのかを理解するためには、まずコンテキストとは何かを定義する必要があります。

コンテキスト： 何かが存在したり起こったりする状況であり、それを説明するのに役立つもの
参照： ケンブリッジ辞典

人は実生活の中で「コンテキスト」を把握することができます。しかし、両者が正式な関係を持たず、何千マイルも離れているかもしれないデジタル領域では、コンテキストは次の2つのソースからシグナルを消費することによって提供されます。

- システム内の アイデンティティ/オブジェクトからの静的シグナル：
  - エンティティの認証情報
  - スマートフォンの識別情報
  - 権威によって署名されたソフトウェア
- システム内の他の関連するエンティティ/オブジェクトから消費される動的シグナル：
  - スマートフォンとGPS位置情報
  - IPアドレスとそのジオロケーション
  - アプリケーションの状態
  - 機器のセキュリティの健全性
  - システムで行われているアクション
  - アクセス頻度（アクセス要求の頻度の急増）および要求の同時実行性
  - 時間帯

動的シグナルは、さらなる理解やコンテキストを提供します。このように、静的なシグナルで異常が発生した場合、動的シグナルがより高いレベルの信頼性を提供します。これにより、取引を進めるかどうかについて、より適切なリスクベースの判断が可能となります。

より良い情報に基づいたコンテキストによる判断を下す能力の向上は、セキュリティのあらゆる面で有益です。しかし、ゼロトラストへの移行においてコンテキストのデジタル表現を活用することは、アサーション、アイデンティティクレデンシャル、および関連するシグナルをリアルタイムで評価するために不可欠です。

図1:CBACの簡単な例では、「職員が割り当てられた企業用デバイスを使用しているか」という権限ルールを使用

コンテキストベースアクセス制御

CBACは、企業のアクセス要求にまつわる状況を評価します。その実体は人間であったり、人間でなかったりします。前のセクションで説明したように、境界ベースのセキュリティには欠陥があります。

ゼロトラストの観点からは、コンテキストはさまざまなパラメータによって定義されます。位置情報、デバイスの健康状態、デバイスの挙動、ネットワークの場所といったこれらのパラメータは、ゼロトラストアーキテクチャの様々な柱からのシグナルです。例えば、IT管理者がオフィスのLAN上にあるデバイスからDNSサーバーに定期的にアクセスすることがあります。DNSサーバーにアクセスする管理者のコンテキストは、IPアドレス、デバイスID、および管理者の認証情報によって確立されます。ポリシーエンジンがこれらのサービスを消費するたびに、管理者はDNSサーバーへのアクセスが許可されます。しかし、ポリシーエンジンが管理者の自宅のIPアドレスからのシグナルを受信した場合、コンテキストは満たされず、逸脱しているのは別のIPアドレスという形になります。

その逸脱が認められたシナリオである場合、アクセスは許可されますが、多要素認証のような追加的な検証が必要となる場合があります。その逸脱が受け入れ可能なシナリオでない場合、アクセスは拒否されるか、あるいはリクエストを承認するために追加の検証が実行されます。例えば、CBACは、自宅からのアクセス要求の理由がアプリケーションを立ち上げるためである場合、アプリケーションのステータスを確認することができます。アプリケーションからのシグナルが、アプリケーションが健全であることを示す場合、アク

セ スリクエストに疑わしいフラグを立てることができます。

重要なことは、組織は自社のビジネスリスクに対応するシグナルのみを消費するということです。ビジネスリスクが低い場合、組織は認証とネットワークからのシグナルを消費することを決定するかもしれません。機器からのシグナルを無視することもあります。
コンテキストは、静的シグナルと動的シグナルの両方から構築されます。アクセス制御の決定は、同じセッションですべてを消費することによって、静的シグナルと動的シグナルの両方で行うことができます。しかし、この文書の後半で説明されているように、運営上のオーバーヘッドが発生する可能性があります。異常がない場合のアクセス判定には静的シグナルを使用し、異常がある場合は動的シグナルを使用することが望まれます。

CBACのアプローチは、従来のネットワーク境界防御やIAMコントロールを超越し、ゼロトラスト原則を採用する権限を組織に与えます。アイデンティティとともにコンテキストを組み込むことで、CBAC は、各アクセスリクエストの特定の状況に合わせた、動的に適応するリスクベースの認証および認可ワークフローを可能にします。この汎用性は、人間と人間以外のアイデンティティをサポートし、最新のAI/ML機能とのより良い相乗効果と相互運用性を促進し、強固な認可の意思決定プロセスをもたらします。CBACの2つの重要な利点は、適応性と知性です。

適応性

CBACメカニズムは、進化するユーザー行動、デバイスのヘルススコア、リスクプロファイル、ジオロケーション、ネットワーク、データ、アプリケーション、アセット、サービス（DAAS）、その他のリアルタイムで起こりうるコンテキスト要因に適応します。これは、現代の職場環境の流動性の増加、アクセスパターン、BYODや管理対象デバイスの普及と一致しています。

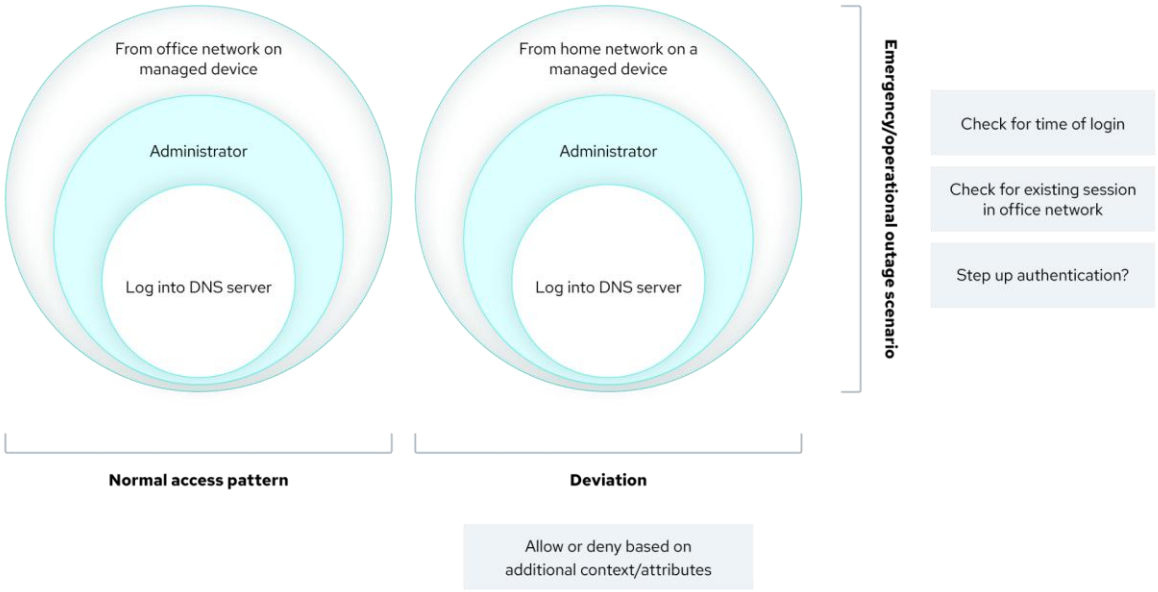
AI/MLは、デバイス管理システムやユーザー・アクティビティ・ログなど、さまざまなコンテキスト・シグナル・ソースからのデータを使用して、アイデンティティの行動やアクセスパターン、DAAS要素、プロテクトサーフェス、適応性をプロファイリングおよびベースライン化することができます。

ベースラインが確立されると、AI/MLモデルがリアルタイムでパターンや異常を検出し、CBACがポリシーエンジンのアクセス決定を動的に調整できるようになります。

インテリジェンス

アイデンティティをコンテキスト（ユーザーの役割、要求されたデータカテゴリ、時間帯、デバイスの健全性スコア、IP地域など）にリンクし、さまざまなリアルタイムのリスクスコアを評価することで、CBACはポリシーエンジンの検証アルゴリズムが微妙なアクセス決定を行うことを可能にし、アタックサーフェスを縮小します。

アイデンティティシステム、デバイス、ブラウザ、ネットワーク、および外部データ（SIEM、グローバルな脅威、脆弱性、ゼロデイなど）からのコンテキストデータを組み合わせることで、機械学習モデルがパターンを特定し、予測を行い、自己改善することができます。



以下は静的シグナルと動的シグナルの例です：

静的属性：

- デバイスID/アセットID
- アプリケーションID
- 認証されたユーザーID

動的シグナル：

- ジオロケーションからのシグナル
- ネットワークからのシグナル
- デバイスの健康状態
- アクセスされているアプリケーション/リソースの動作状況

CBACとゼロトラスト

CBACとゼロトラストは密接な関係にあります。両者とも、リソースへのアクセスは、リスクと状況を徹底的かつリアルタイムに評価した後にのみ許可されるようにしています。つまり、一度認証されれば信用されるという古いモデルから脱却しました。その代わりに、それらはすべてのアクセス試行を常に検証することに重点を置いています。ゼロトラストは、"決して信用せず、常に検証する "という考え方に基づいており、CBACは、あなたが誰であるか、どこにいるか、使用しているデバイス、ネットワークの状態などに基づいてアクセス決定を行うことで、これをサポートしています。この2つを組み合わせることで、誰かが何かにアクセスしようとするたびに、そのアクセスが慎重に評価され、不正アクセスのリスクが低減されます。

CBACは、アクセスを許可する前に、IPアドレス、場所、時間帯、デバイスの状態など、さまざまなリアルタイムの信号を調べます。例えば、普段オフィスから会社のリソースにアクセスしている人が、突然新しいデバイスで見知らぬ場所からログインしようとした場合、CBACはこれを潜在的なリスクとして警告します。ゼロトラスト・アプローチでは、多要素認証のような特別な検証ステップが必要になるかもしれませんし、アクセスを完全にブロックするかもしれません。このアダプティブ・アプローチは、最新の情報に基づいて意味のある場合にのみアクセスが許可されることを意味し、暗黙の信頼を排除するというゼロトラストの目標に完全に合致しています。

しかし、CBACとゼロトラストを組み合わせるには、リアルタイム評価の規模を管理することと、追加された複雑性を処理することという2つの主要な課題があります。

スケールへの挑戦：

- 規模が大きい：利用可能で必要なすべてのシグナルをリアルタイムで使用してアクセス要求を継続的に評価するには、特に何千ものユーザーとデバイスを抱える大組織では、多くのコンピューティングパワーを必要とします。
- 待ち時間：このようなデータ処理はすべて、人々が仕事をこなそうとしているときに遅れが生じないように、十分に速く行われなければなりません。

複雑性への挑戦：

- 複雑さ：CBACは多くのシグナルを分析するため、従来のモデルよりも判断プロセスが複雑になります。
- レガシーシステム：古いシステムは、このダイナミックなアクセス制御のために作られたものではないので、 CBACを統合するのは難しいかもしれません。
- コミュニケーション：CBACシステムを既存のシステムとスムーズに通信させるのは、複雑な場合があります。

これらの課題に対処するために、組織は以下のような行動をとることができます。

スケール・ソリューション

- ロードバランシングとクラウドソリューション：処理負荷を複数のサーバーに分散させるか、クラウドプラットフォームを利用することで、システムが減速することなく多くのトラフィックを処理できるようにします。

- データをキャッシュ：よく使われるデータを一時的に保存して意思決定を迅速化し、すべてをゼロから処理する必要性を減らします 。

複雑性の解決：

- 段階的配備：まず、重要なシステムにCBACを導入することから小さく始め、その後、システムを微調整しながら拡大していきます。
- アクセスポリシーの簡素化：段階的なアプローチを用います。リスクの高いリクエストは詳細に審査され、 リスクの低いリクエストはよりシンプルに評価されます。
- ハイブリッドモデル：組織がより動的なアクセス制御モデルに移行する間、CBACとレガシーシステムを共存させます。

CBACとRBACおよびABACとの比較

役割ベースアクセス制御（RBAC）：役割ベースアクセス制御は、事前に定義された権限とパーミッションが割り当てられたグループにユーザーを追加することに基づいています。アクセスは、ユーザーのグループメンバーに基づいて許可/拒否されます。組織要件やリスクレベルの変化に対応する柔軟性に欠けます。RBACは複雑さと指数関数的な関係にあります。役割の数が増えれば、それを維持するのも複雑になります。ロールの入れ子（これはグループメンバーシップの入れ子につながる）は、RBACに伴うもう一つのセキュリティ上の課題です。RBACは、アクセス要求を許可または拒否するためにチェックされる唯一の要素がグループメンバーシップであるため、ゼロトラストの原則に沿ったものではありません。

属性ベースアクセス制御（ABAC）：ABACは、RBACのグループメンバーシップから、アクセス要求を許可または拒否するための属性グループに焦点を移します。ABACは静的な属性に基づきますが、組織の要件やリスクレベルの変更に柔軟に対応できます。ABACは、アクセスを許可または拒否する前にアクセス要求の条件がチェックされるため、ゼロトラストの原則に合致しています。

コンテキストベースアクセス制御（CBAC）：CBACは、アクセス要求を許可または拒否する前に、静的属性と動的属性を消費します。CBACはABACを含むことができますが、静的シグナルのリスクを確認することによってABACを拡張し、リスクレベルが決定された閾値を下回る場合に認証要素をステップアップさせます。組織の変化する要件やリスクレベルに柔軟に対応できます。これは、アクセス要求がなされる条件とその背景を検討するという点で、ゼロトラストの原則と密接に連携しています。

戦略

特徴	RBAC (役割ベースアクセス制御)	ABAC （属性ベースアクセス制御）	CBAC (コンテキストベースアクセス制御)
IAMの判断基準	一連の権限を持つ定義済みの役割に基づく	ユーザーとリソースの属性に基づく	関連資産の属性、ダイナミックシグナル、アクセス要求のリスクレベルに基づく
ゼロトラスト・インテグレーション	ゼロトラストとは本質的に一致しない	ゼロトラストとの整合性	アクセス要求が行われるコンテキストを決定することにより、ゼロトラストに整合させる。
暗黙の信頼の排除	暗黙の信頼の排除を支持しない	クレデンシャルのみに依存せず、属性を使用することでサポート	各アクセスリクエストをコンテキストの観点から評価することでサポート
AIインテグレーション	AIは関係ない	AIをある程度組み込むことができる	AIを組み込むことで、文脈を判断しながらスピードと敏捷性をもたらすことができる

ガバナンス、リスク、コンプライアンス（GRC）

ガバナンスと方針の一致	シンプルな構造だが柔軟性に欠ける	特定の組織ポリシーに沿ったきめ細かなポリシー	組織のポリシーに沿ったきめ細かなポリシーの枠組み
リスク管理	リスク管理は初歩的	属性を用いることで、リスクに対するより微妙なアプローチが可能になる	コンテキストの一部である静的・動的シグナルを用いたリスクベースの評価
コンプライアンスと監査	ロギングと監査を簡素化するが、必ずしもコンプライアンスに準拠する必要はない	より詳細なロギングと監査機能を提供	ロギングと監査のための豊富なイベントセットを提供する。

オペレーション

実装 複雑さ	複雑性が低い	複数の属性を管理するため、より複雑になる	高い複雑性、システム内の複数のコンテキスト
政策管理	役割の数が増えると複雑になる	複雑なポリシーは、より正確なコントロールを可能にする	コンテキストルール、関連するダイナミズム、ユーザーの行動を考慮することによる複雑さ
相互運用性	事前に定義された役割と互換性のあるシステムで動作	属性を慎重に調整することで、さまざまなシステムに適応	コンテキストルールによる高い相互運用性
スケーラビリティ：	役割が爆発する可能性があるため、規模拡大が難しい	複数のユーザーとシナリオにまたがって拡張される属性	属性とコンテキストは組織全体に拡大縮小できる
適応性	ユーザーの役割や動的な脅威の変化に容易に対応できない	より幅広い条件や属性に適応できる	適応性はフィードバックループで達成できる

セキュリティ

インサイダーの脅威	内部脅威の影響を受けやすい	属性を介した内部脅威の軽減において、RBACよりも優れている	静的・動的シグナルとユーザー行動分析を適切に組み合わせることで、内部脅威を効果的に評価。
脅威の検知と対応	統合された脅威の検知と対応が欠けている	脅威検知の監視属性を組み込む	これは、コンテキストのシグナルの1つとして脅威の検出を組み込んでいる。
脅威インテリジェンスとの統合	脅威インテリジェンスとの統合に欠ける	静的シグナルとして脅威インテリジェンスを活用できる	CBACは、Policy Engineによって消費される脅威インテリジェンスと統合する機能を持っており、脅威インテリジェンスのシグナルには、拒否リストのIPアドレス、ジオロケーションなどが含まれる。
アクセスコントロールの粒度	広範で役割ベースだが、十分な粒度を提供できない可能性がある	複数の属性を使用することで、より細かいアクセス制御が可能になる	アクセス要求のコンテキストに基づく高い粒度レベル
最小特権の実施	ロールを介した最小権限だが、ロールは過剰アクセスにつながる可能性がある	属性を使用するが、事前に定義された条件を使用する	定義されたコンテキストセットによる最小特権のきめ細かな実施
ユーザー行動分析（UBA）：	UBAには追加のツールが必要	属性の変更を監視するが、外部ツールが必要	シグナルを使ってユーザーの行動を評する

CBAC成熟度モデル

CBACの成熟度レベルは、「初期（Initial）」、「反復可能（Repeatable）」、「定義済み（Defined）」、「管理可能/対応可能（Managed/Capable）」、「効率的（Efficient）」と定義されています[3]。

レベル1 - 初期

CBACを始めたばかりか、非常に限られた機能しか持たないCBACを使用しています。静的シグナルを消費し、ビジネスリスクとの整合性を高める必要があります。

- アイデンティティのエコシステムは、制御の軌跡としても知られる一連の静的シグナルの中で作動しています。
- コンテキストは、当該静的シグナル内に保持されるエンティティに限定されます。
- 各事業者のアクセスがバラバラになり、データセキュリティが損なわれます。
- 一元化されたコンテキストデータがありません
- リスク管理は非公式で、アクセス制御との統合はほとんどありません。

レベル2 - 反復可能

この組織では、静的および動的シグナルによるCBACを使用していますが、ステップアップ認証のためには、より多くの統合が必要です。

- コンテキストは、ロギングと監視を強化し、より良い脅威アラートを出すために使用されます。
- 外部エンティティからの属性やシグナルは、文脈上の決定を強化するために使用されます。
- 生体認証および/または多要素認証により、人体認証が強化されます。
- アイデンティティクレデンシャルは、SAAS サービスなどの外部エンティティ（限定的なフェデレーション）に渡すことができます。
- 静的および動的シグナルに基づくモニタリングとアラートによるリスク管理が行われています。

レベル3 - 定義済み

同組織では、静的および動的シグナルによるCBACを使用し、ステップアップ認証を統合的に使用しています。

- 許可されたユーザーであれば、摩擦は軽減されます
- ステップアップ認証/多要素認証が導入されています
- パスワードレス認証が導入されています
- 人間の実体検証は、タイピング速度、マウスの動き、閲覧行動などの要因によって強化されます。
- リスク管理がより構造化され、セキュリティを損なうことなく摩擦が減少します。

[3] CISA Zero Trust Maturity Model では「Traditional」、「Initial」、「Advanced」、「Optimal」を使用していますが、これはCMU標準の5段階成熟度モデルとは矛盾しています。

レベル4 - 管理可能 /対応可能

この組織はCBACを使用しており、シグナルを消費してアクセス決定のためのコンテキストを導出/開発します。

- CBACは、アサーション、クレデンシャル、その他のコンテキストを、組織内部のアクセス制御システムにエンティティを登録することなく、直接利用することができます。
- 消費されるシグナルには、ユーザーの行動パターンや習慣の分析が含まれます。
- CBACは、エンティティとアサーションの間の不変性のレベルを理解することができます。
- AI/MLは、有害な行動パターンや異常を発見するために使用されます。
- リスク管理は、動的シグナルとユーザー行動を利用したアクセス制御と統合されています。

レベル5 - 効率的

同組織は、静的および動的シグナルを消費し、組織のリスク管理プロセスと統合されたCBACを使用しています。

- リスク管理はアクセス決定と完全に統合され、ビジネスリスクはリアルタイムで体系的に対処されます。
- AI/MLは、利用可能なすべてのシグナルを使用して異常な行動を検出するために使用されます。

CBACにおける運用オーバーヘッドとユーザーエクスペリエンスへの対応

セキュリティ管理には、運用上のオーバーヘッド、管理上のオーバーヘッド、財務上のオーバーヘッド、ユーザーエクスペリエンスの低下など、さまざまなオーバーヘッドが伴います。

この点で、CBACではシグナルを消費する間に遅延が発生する可能性があることを覚えておくことが重要です。このような実施による遅れに対処する方法はたくさんあります。そのような方法の一つは、コンテキストに定義された最小限の静的シグナルを消費し、異常が検出されたときに動的シグナルを消費することです。この例を以下に示します。左側の図は、すべてのシグナルを一度に消費するため、待ち時間が発生する可能性があります。2つ目の図は、通常のパターンとしての静的シグナルの消費と、検出された異常のリスクに応じた動的シグナルの消費を分割したものです。

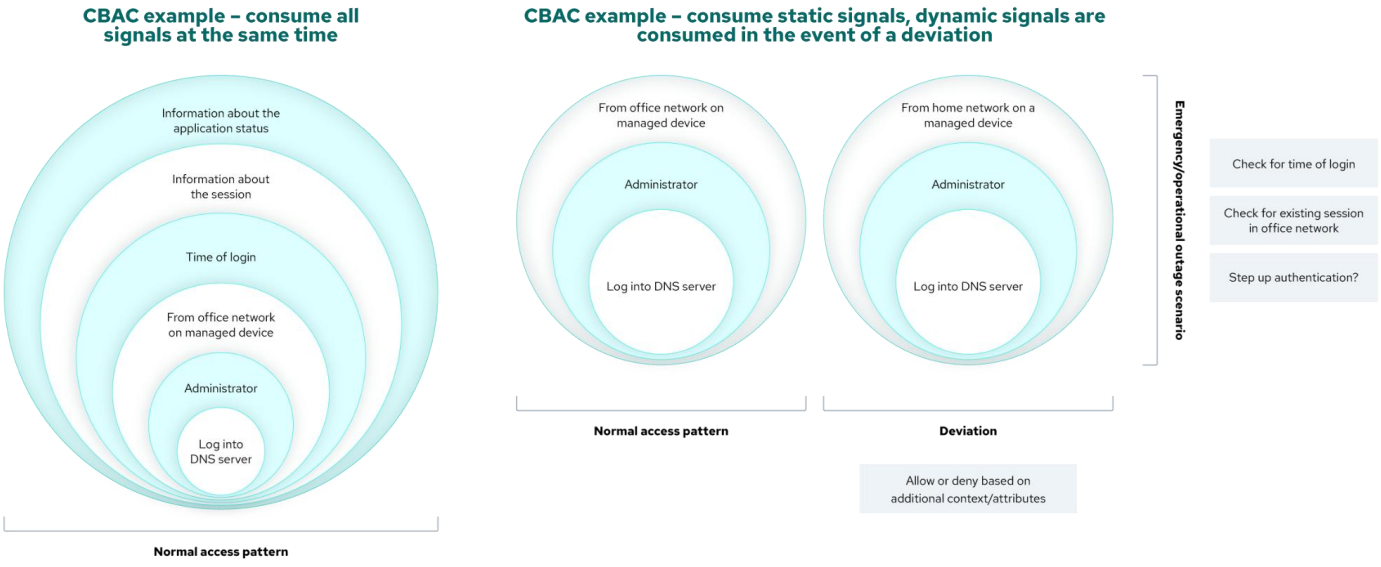


図2:CBACのオーバーヘッドへの対応

すべてのシグナルを同時に消費しないことで、遅延に対処し、管理可能なシステムを確保することができます。以下は静的シグナルと動的シグナルの例です。

静的属性：

- デバイスID/アセットID
- デバイスの健康状態
- アプリケーションID
- 認証されたユーザーID

動的シグナル：

- ネットワークからのシグナル
- ジオロケーションからのシグナル
- タイムスタンプからのシグナル
- アクセス中のアプリケーション/リソースの動作状況

フィードバックによるCBACの改善ループ

フィードバックはシステムを改善する強力なメカニズムであり、CBACにも適用されます。ポリシーの作成、シグナルの消費、コンテキストの特定、アクセスの許可/拒否は、CBAC実装のいくつかの側面ですが、システムが要件を満たしているかどうかの検証も必要です。これを行う強力な方法は、CBACからのすべてのログを中央データベースに送り込み、ログを分析し、欠点や改善点を特定することです。この働き方は、「すべてを記録する」というゼロトラストの原則に沿い、可視性と分析に合致しています。

これは、特定された欠点/改善点を自動化/オーケストレーション・エンジンに送り込み、自動化された形でフィードバックを適用することで、さらに一歩進めることができます。これには高い成熟度が必要であり、適用には注意が必要です。

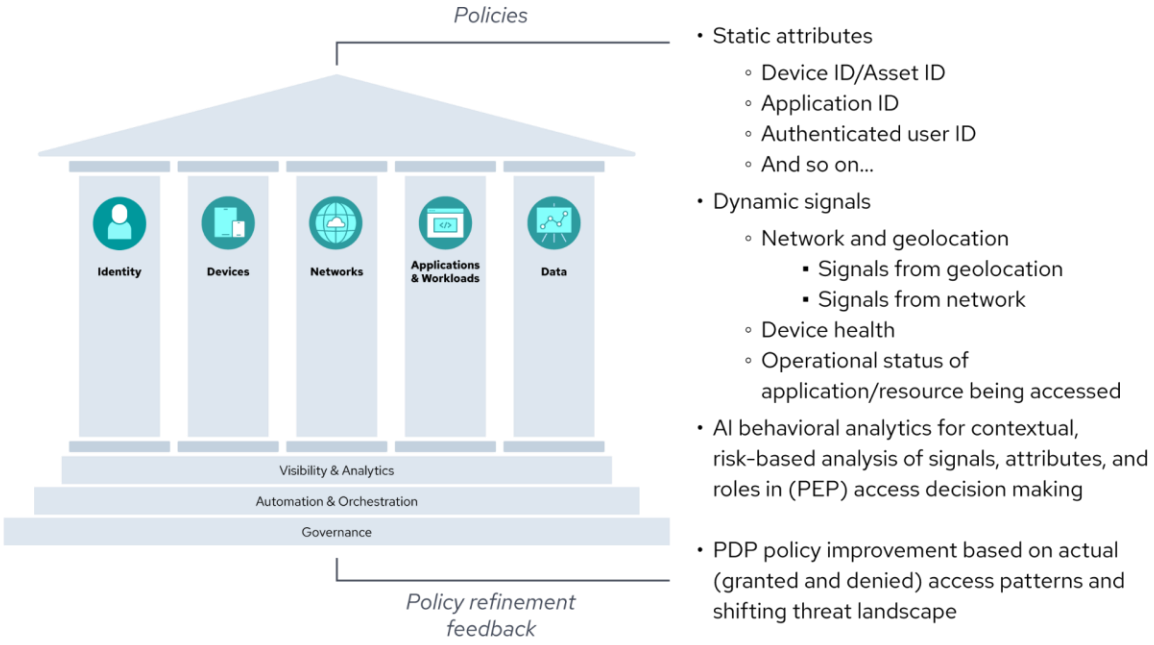


図3:CBACフィードバック

データセットのシグナルと品質

CBACエンジンによる効果的な意思決定を確実にするため、シグナルはデータセットに集約されます。したがって、高品質のシグナルと改ざんされていないデータセットに頼ることが不可欠です。信頼性の高いシグナルは、ユーザーの行動、デバイスの属性、ネットワークの状態など、さまざまなコンテキスト要因に関する正確で最新の情報を提供します。また、改ざんされていないデータセットは、意思決定に使用される情報が本物であり、改ざんされていないことを保証し、システムの分析の信頼性と正確性を維持します。シグナルとデータセットの完全性と正確性を優先することで、組織はCBACメカニズムの有効性と信頼性を高めることができ、それによってゼロトラストの原則に沿ったセキュリティポスチャを強化することができます。

シグナルの信頼性とデータセットの完全性を確保することに加え、データセットの継続的なモニタリングが不可欠です。組織は、アクセス制御の仕組みの性能と、利用されているデータの品質を定期的に評価することによって、潜在的な問題や矛盾を速やかに特定し、対処することができます。このプロアクティブなアプローチにより、タイムリーな調整と最適化が可能になり、進化する脅威や状況要因にシステムが対応し続けることができます。さらに、継続的な監視により、異常や疑わしい活動の検出が容易になり、潜在的なセキュリティリスクを軽減するための迅速な是正措置が可能になります。強固なモニタリング手法をアクセス制御のフレームワークに組み込むことで、組織は重要な資産をプロアクティブに保護し、ゼロトラストの原則を守ることができます。

AIはどのようにCBACを強化できるか

AIは、アクセス制御の文脈におけるゼロトラストに関して、相反する2つの力を発揮します。第一に、AIはサイバーセキュリティやデータ保護の管理を回避するために、脅威行為者によってますます利用されるようになっています。第二に、可視化と分析、インシデント対応、自動化とオーケストレーションなどに使用されるAIは、ゼロトラストにおいて有用です。組織が受け取るアクセス要求の量を考えると、AIを使用することは、アクセス要求を分析し、意図した要求者のみにアクセスを許可する上で現実的です。

適応的意思決定とリアルタイムの脅威検知：

- **CBAC：**アクセスの判断は、位置、時間、デバイスのシグナルを用いて行われます。
- **AI：**様々なシグナルをリアルタイムで分析し、アクセス判定を調整します。脅威からのシグナルを消費してパターンを発見し、逸脱を特定し、アクセスを許可または拒否することができます。

パーソナライゼーション：

- **CBAC：**すべてのユーザーに一般的なルールを適用し、個人の行動や嗜好に基づくものではありません。
- **AI：**各ユーザーの習慣や行動を長期にわたって学習し、ユーザーの行動に基づいてアクセス決定をカスタマイズできるようにします。これにより、正規のユーザーには、通常とは異なる状況においても、より安全で柔軟なエクスペリエンスを提供することができます。

自動化

- **CBAC：**手作業で更新し、定期的に見直さなければならないルールやポリシーに依存します。
- **AI：**行動とコンテキストの分析により、リアルタイムでのアクセスポリシーの更新を支援します。これにより、ITスタッフの作業負荷が軽減され、システムが進化するセキュリティ脅威に常に対応できるようになります。

リスクベースのアクセス制御：

- **CBAC：**文脈的要因を用いてアクセス要求を評価するルールを使用しますが、変化するリスクに迅速に適応できません。
- **AI：**各リクエストのリスクスコアをリアルタイムで自動計算します。脅威インテリジェンス、サードパーティシグナル、行動分析などから）現在の脅威に基づいてアクセス許可を調整 し、進化するリスクに対してより迅速なアプローチを提供します。

スピード：

- **CBAC：**膨大なデータの処理には時間がかかり、手作業で管理するのは困難です。
- **AI：**膨大な量のデータをほぼ瞬時に処理し、意思決定を迅速化します。ほぼリアルタイムのアクセス制御により、ユーザーエクスペリエンスは向上します。

ユーザーエクスペリエンス：

- **CBAC：**位置情報、デバイスの種類、行動に基づいてアクセスを許可することで、スムーズなエクスペリエンスを実現します。
- **AI：**リアルタイムでアクセス決定を行い、ユーザーごとにプロセスをカスタマイズします。これにより、正当なユーザーの中断を減らし、よりシームレスで安全なエクスペリエンスを提供します。
- **AI**：ユーザーにMFAプロンプトを表示させ、生産性を低下させる誤検知を減らします。

フォレンジック：

- **CBAC：**セキュリティインシデント後のフォレンジック分析に役立つ、コンテキストに応じたアクセス決定のログを提供します。
- **AI**：アクセスパターンに関する詳細なレポートを作成することで、フォレンジックを改善します。異常のフラグを立て、 予測的な洞察を提供することで、脆弱性の発見やミスの迅速な修正が容易になります。

CBACのビジネスメリット

CBACにより、組織はユーザーアイデンティティ、デバイスポスチャ、環境条件、その他のシグナルなど、さまざまなコンテキスト要因に基づいてアクセス制御ポリシーを実装できます。このようにきめ細かくコントロールすることで、いくつかのビジネス上のメリットを得ることができます。

- **セキュリティの向上：**CBACは、アクセスを許可する前に幅広い文脈上の要因を評価することで、機密データやリソースへの不正アクセスを防止するのに役立ちます。これにより、データ漏洩やその他のセキュリティ事故のリスクを軽減することができます。

- **業務効率の向上：**CBACは、事前に定義されたポリシーに基づいてアクセス決定を自動化し、手作業による介入の必要性を減らし、アクセス要求を合理化することができます。これにより、業務効率を向上させ、ITスタッフの負担を軽減することができます。

- **コンプライアンスの強化：**CBACは、アクセス試行と決定の詳細なログとレポートを提供することにより、組織が規制および業界のコンプライアンス要件を満たすのを支援することができます。これは、データプライバシーおよびセキュリティ規制の遵守を証明するのに役立ちます。

- **より良いユーザーエクスペリエンス：**CBACは、デバイスの種類、場所、ユーザーの行動などのコンテキスト要因に基づいたアクセスを可能にすることで、よりシームレスでパーソナライズされたユーザーエクスペリエンスを提供することができます。これにより、ユーザーの満足度と生産性を向上させることができます。

- **スケーラビリティ：**CBACは、大規模で複雑な環境をサポートするために簡単に拡張できるため、あらゆる規模の組織に適しています。

- **統合：**ビジネスが独立したエンティティであることは稀であり、CBAC は、それらのエンティティを組織内部のアクセス制御システムに登録する必要なく、アサーション、クレデンシャル、その他のコンテキスト情報を直接消費し、活用できる可能性があります。

- **ロギングとフォレンジック：**アクセス要求を文脈の中で理解することで、それらの要求を検討し、よりよく理解し、アクセスを許可するかどうかを決定することができます。これにより、セキュリティチームは、不正にアクセス権が付与された事例をより適切に分析できるようになり、ITチームは、あるエンティティが誤ってアクセス禁止にされた場合に、そのエンタイトルメント・ルールを修正できるようになります。

結論

ハッカーは、盗んだパスワード、弱いパスワード、デフォルトのパスワードを使ってシステムに侵入します。この古い手口は今でも最も効果的なもののひとつで、事故であれ意図的な攻撃であれ、不正アクセスにつながることがよくあります。
この脅威は部外者だけからもたらされるものではありません — 内部関係者もリスクになります。だからこそ、強力なアクセス制御が重要なのです。

これに取り組むために、企業は一度認証されれば永遠に信頼されるという時代遅れのセキュリティモデルから脱却する必要があります。その代わりに、アクセス要求は、リアルタイムまたはほぼリアルタイムで不審な行動を検出するために、様々な要因を見てリアルタイムで継続的に評価されるべきです。
コンテキストベースアクセス制御（CBAC）は、アクセスが要求される条件を評価することによって、より高度なアクセス制御を提供する上で重要な役割を果たします。CBACは、アクセス要求がどこに置かれてい

るのか、誰が要求を出しているのか、なぜ要求が出されているのか、どのようにアクセスが要求されているのかを理解するのに役立つシグナルを消費することによってこれを行います。CBACはまた、リスクに対処するために必要なシグナルのみを消費することで、組織のリスク選好度に合わせることもできます。これは、CBACを組織の要求に合わせてスケーラブルにする上で重要です。CBACはすべてのログを記録する機能を持ち、ゼロトラストの原則に沿い、可視性を提供し、アクセスポリシーを改善するフィードバックループをサポートし、必要なものだけにアクセスを制限し、定期的にリスクを評価します。

役立つリソース

- Phil Venables on LinkedIn: How AI can strengthen digital security
- How AI can strengthen digital security
- Zero Trust in the Cloud: Total Context Matters | CSA
- Exploring the Intersection of IAM and Generative AI in the Cloud
- Mistaken identity: the mistakes we make and a lack of understanding about what identity is-part 3
- Personas as a Basis for Context and Trust
- Dynamic Defense: Context-Based Access Control and Zero Trust

用語集

- CSA Glossary (main/primary)

その他の定義

- **コンテキスト：**何かが存在する、あるいは起こる状況、そしてそれを説明するのに役立つ状況。(参照）：ケンブリッジ辞典)
- **アイデンティティ：**そのエンティティに関連するすべてのペルソナおよび属性の集まり。
- **ローカス・オブ・コントロール（Locus-of-control）：**すべてのエンティティ、属性、および信頼されたシグナルを、単一のエコシステム（またはアクセス制御システム）で維持して機能させる必要性。
- **エンティティ:**明確で独立した存在を持つ唯一無二の「もの」。どのようなエンティティも、 他のどのようなエンティティとも相互作用することができ （その意味で、両者は機能的に同一である）、ペルソナを作成するための相互作用はコンテキストを付与。
- **属性：**ある実体の特性、特徴、要素、性質、または固有の部分。
- **署名された属性：**その属性の権威エンティティによってデジタル署名された属性。
- **ペルソナ：**エンティティを特定する文脈上の設定（全体的なアイデンティティの特定の「facet」）に記述または配置する属性の集まり。例えば、Fredは状況/用途/ニーズ/プライバシー要件に応じて、さまざまなアイデンティティ/ペルソナを身につける。
- **事業リスク：**その暴露が利益の低下、あるいは倒産につながる前に、組織が許容できる暴露。

付録1 関連ソリューションプロバイダー

ベンダーは、様々な形でコンテキストベースアクセス制御（CBAC）を提供しています。CBACの最も初期の例の1つは、与えられた時間に1つのセッションしか許可しないようにアプリケーションをセットアップすることでした（通常、セッションにsingletonクラスを使用します）。別のブラウザで作成された追加セッションは終了します。このシナリオは金融部門で顕著でした。

マイクロソフトは、PEP（ポリシー実施ポイント）と呼ばれるもので、意思決定に使用される消費シグナル（IPロケーション情報、ユーザー/グループ、アプリケーションなど）に基づく条件付きアクセスを行ってきました。

Thales Groupは、SafeNet Trusted AccessによるCBACソリューションを持っています。

以下は、市販されているCBACの例です。

- Microsoft (conditional access with M365)
- Thales’s SafeNet Trusted Access
- Google’s Context-Aware Access
- Cisco IOS® Firewall Feature Set’s Context-Based Access Control
- Beyond Identity's passwordless platform
- OKTA’s Contextual Access Management
- CrowdStrike Falcon and Zscaler Zero Trust Exchange’s inputs to context with users, endpoints, networks, the apps users are trying to access, and where those apps live
- NetSkope’s Context-Aware Information Rights Management
- Pomerium
- StrongDM Zero Trust PAM with Contextual Security Awareness