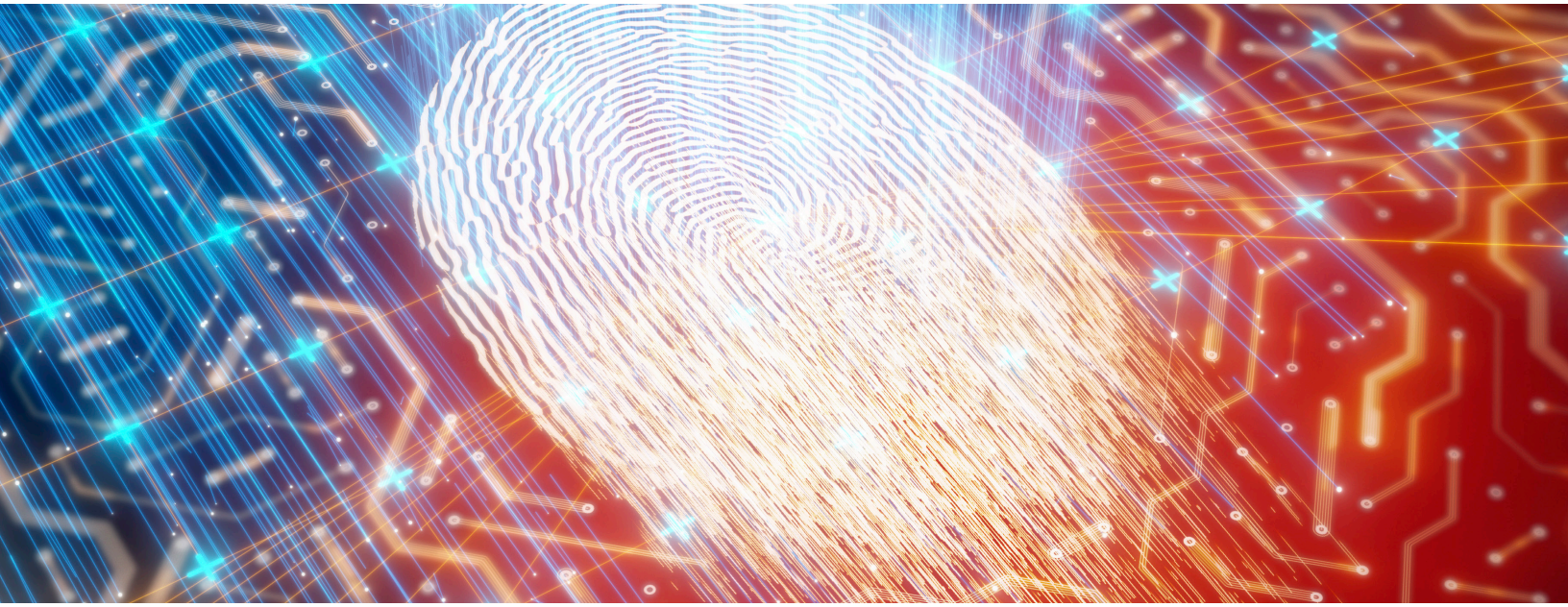
VECTRA AI, INC.
Security that thinks®

2020 Spotlight Report

特権アクセスは信頼に値する アクセスと言えるのか？



私はAI（人工知能）。
サイバー攻撃者の追跡を陰から支える原動力
となることが、私の使命です。
そう、私がCognitoです。

VECTRA AI, INC.
Security that thinks®

目次

Vectra AI社の調査によれば、様々な業界において、未知のホストからの特権アクセスが発生し、重要なシステムが予期せぬ危険に晒されていることが明らかになっています。これらの特権アカウントがどのように使用されているのかという点については、仮に特権アクセスの管理ツールを備えている場合でも、直接監視したり、技術的に制御することが、ほとんど不可能です。特権アカウントの使用状況を適切に監視、把握できないということは、企業における業務や財務上の大きなリスクにつながります。特権アカウントが不正に使用された場合、企業はデータの盗難やスパイ行為、破壊行為、さらに身代金の要求などによって、大きなダメージを受けることになるからです。

特権アクセスが不正に使用されていないかを監視することの重要性

サイバー攻撃が侵入拡大を図る過程では、特権アクセスが大きな鍵となります。多くの重要な情報にアクセスできる特権アカウントによって、重要な機能や情報を手に入れることができるからです。攻撃者は特権アカウントを使って、認証情報を盗み出したり、プロトコルの不正使用やマルウェア、フィッシング、あるいは単純に憶測やデフォルトのアカウント名とパスワードを使用するなど、様々なテクニックを駆使して、不正にアクセス権を入手しようと試みます。

また、内部の社員が、会社に故意に損害を与えたり、データを盗み出すために特権アカウントを悪用する場合もあります。この他にも、権限を持つ社員がアカウントやシステムを誤って設定することによって、問題が発生するという単純なケースもあります。

攻撃者だけでなく、セキュリティの専門家も、このような問題が露呈していることや、特権アクセスが持つリスクについて既に認識しています。実際に、ガートナーが行った最近の調査結果では、セキュリティの専門家にとっての最優先課題として、特権アクセスの管理が挙げられています。また、Forresterは、セキュリティ侵害の80%において、特権アカウントが不正に使用されている可能性があるという考えを明らかにしています。

いずれにせよ、全ての侵害行為に、何らかの形で特権アクセスの不正使用が関係していることは間違いありません。

特権アクセスによる実際の不正行為

未承認システムからの特権アクセスの犠牲となった企業の一例として、米国金融サービスのCapital Oneを挙げることができます。

同社では、未承認のアクセスを阻止するために設計されたWebアプリケーションファイアウォール（WAF）の単純な設定ミスによって、承認されていない人物がアクセストークンを入手し、侵害行為のために悪用するという事態が発生しました。

AWSでは、信頼できるユーザーに対して、AWSリソースへのアクセスを制御することが可能な、テンポラリーのセキュリティ認証情報を提供するトークンを発行することができます。テンポラリーなセキュリティ認証情報は、特定の管理アクションと同じ権限を提供する形で、恒久的なアクセスキー認証情報とほぼ同等に機能します。

テンポラリトークンは、ユーザーに特定のタスクだけを実行する権限を与え、対象となるアカウントに対するアクセス管理の手間を削減することができる優れた手段です。しかしその一方で、これが悪用された場合、情報が漏洩するというリスクもはらんでいます。

Capital Oneのケースでは、WAFの設定ミスによって、未承認の人物がテンポラリーのAWSトークンを作成できるようになり、これがAWS Simple Storage Service（S3）のバケットからデータを取り出すために悪用されました。

アクセストークンは、SSRF（Server Side Request Forgery）を使ったWebアプリケーションのAWSメタデータAPI経由で取得されました。つまり、未知のホストから一連の簡単なコマンドを使って、外部と接しているWebアプリケーションファイアウォール（WAF）を操作し、仮想プライベートクラウドの外からはアクセスできない内部のサーバーに対して、コマンドを発行させるように仕向けたということです。

Webサーバーに対する完全なアクセス権を手に入れた未承認ユーザーは、システム管理に使用されるAWSコマンドの簡単なスクリプトを実行します。最初は、S3 list-bucketsコマンドで、AWS S3バケットの全ての名称を取得します。

次に、syncコマンドを使って700のフォルダーと顧客情報を含むデータのバケットを外部にコピーしました。これらのAWSコマンドは、クラウド管理者がAWSの仮想プライベートクラウド（VPC）に保存されたデータの管理に向け日々使用するものです。

このようなタイプの攻撃を検知する上での課題は、脅威の振る舞いではなく、データソース側にあります。攻撃にマルウェアを使用することもなく、ホストにも常駐せず、特異なネットワークトラフィックが露見するわけでもありません。そして攻撃者は、通常のクラウドの管理オペレーションにも介入してきます。このような行為が発生した場合の主要なサインとなるのは、特異なホストからの特権アカウントを使ったコマンドの実行です。

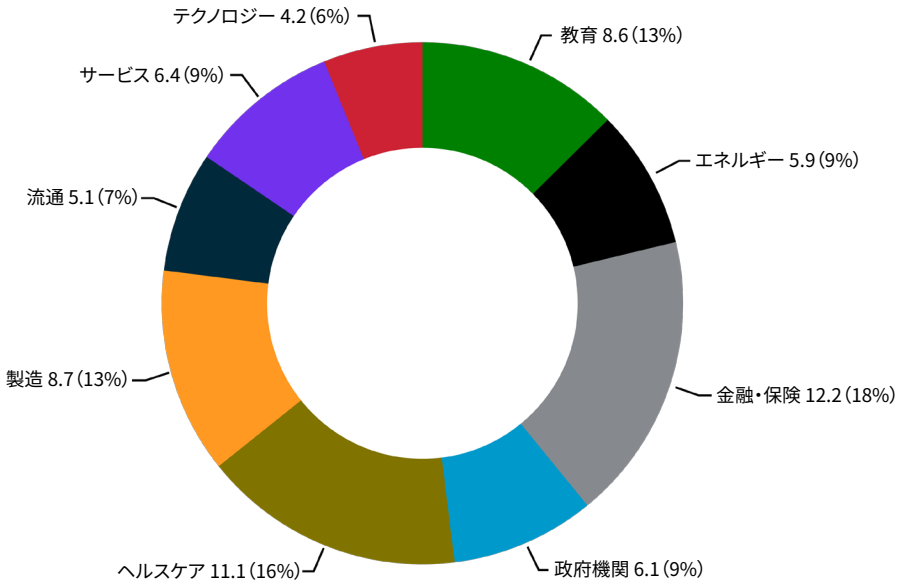
Capital Oneがこのようなミスを犯すべきではなかったと言うことは簡単ですが、企業がクラウド移行を進める際には、残念ながらこのような誤りや設定ミスを避けては通れません。このケースの原因の1つとして挙げられるのが、「責任共有モデル」です。スキルセットや運用に関する知識が異なる組織、あるいは単純にインセンティブ（業務上、金銭上その他）の異なる組織が、アクティビティやエンティティに対して同時に責任を持つことによって、ギャップが発生するというものです。

特異なホストからの特権アクセスは、日常的な問題か？

Vectra AI社の2020 RSA Edition of the Attacker Behavior Industry Report（攻撃者の振る舞いに関する業界レポート2020年RSA版）では、匿名化したお客様のセキュリティメタデータの分析結果から、2019年7月～12月の特権アクセスに関連した振る舞いの傾向が、明らかになっています。このデータを使用することで、悪意ある意図的な振る舞いの発生頻度を定量化することができます。

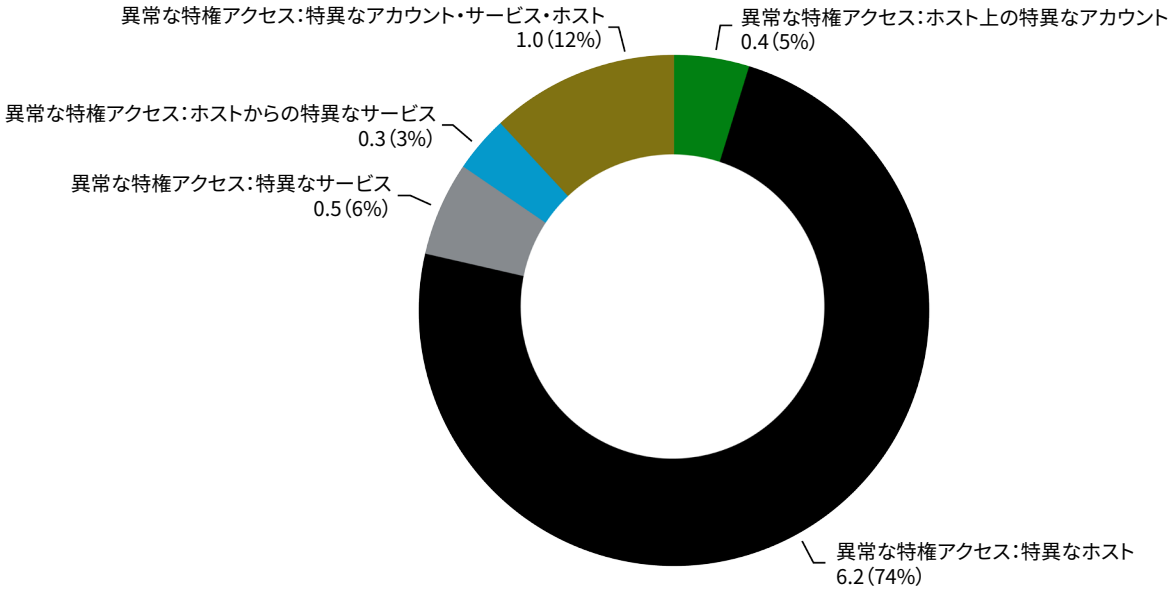
2019年7月～12月の6ヶ月間において、Cognitoネットワーク検知および対応プラットフォームでは、2万6,800件の特権アクセスによる異常な振る舞い行動を検出しました。企業別の発生頻度を把握する際には、データを正規化することで最新の傾向を明らかにすることができます。また、レポート全体を通じて、検出数を1万件のワークロードまたはデバイスあたりの値に正規化したことで、異なる業界や規模が異なる企業間でも比較ができるようになっています。

全体として分かったのは、9つの異なる業界の中でも、金融・保険、ヘルスケア、そして教育機関において、特権アクセスを使用した異常な振る舞いが多く見られるという点です。今回検知された、特権アクセスを利用した異常な振る舞いの約半数（47%）が、この3つの業界で占められています。



1万件あたりの業界別の異常な特権アクセス

さらに分析を進めて、特定のタイプ別に振る舞いを分類した結果、最も頻繁に観察されたのが、特異なホストからの特権アクセスであり、特権アクセスを使った異常な振る舞い全体の74%を占めていることが分かりました。このような振る舞いは、正にCapital Oneが侵害を受けた状況と一致しています。

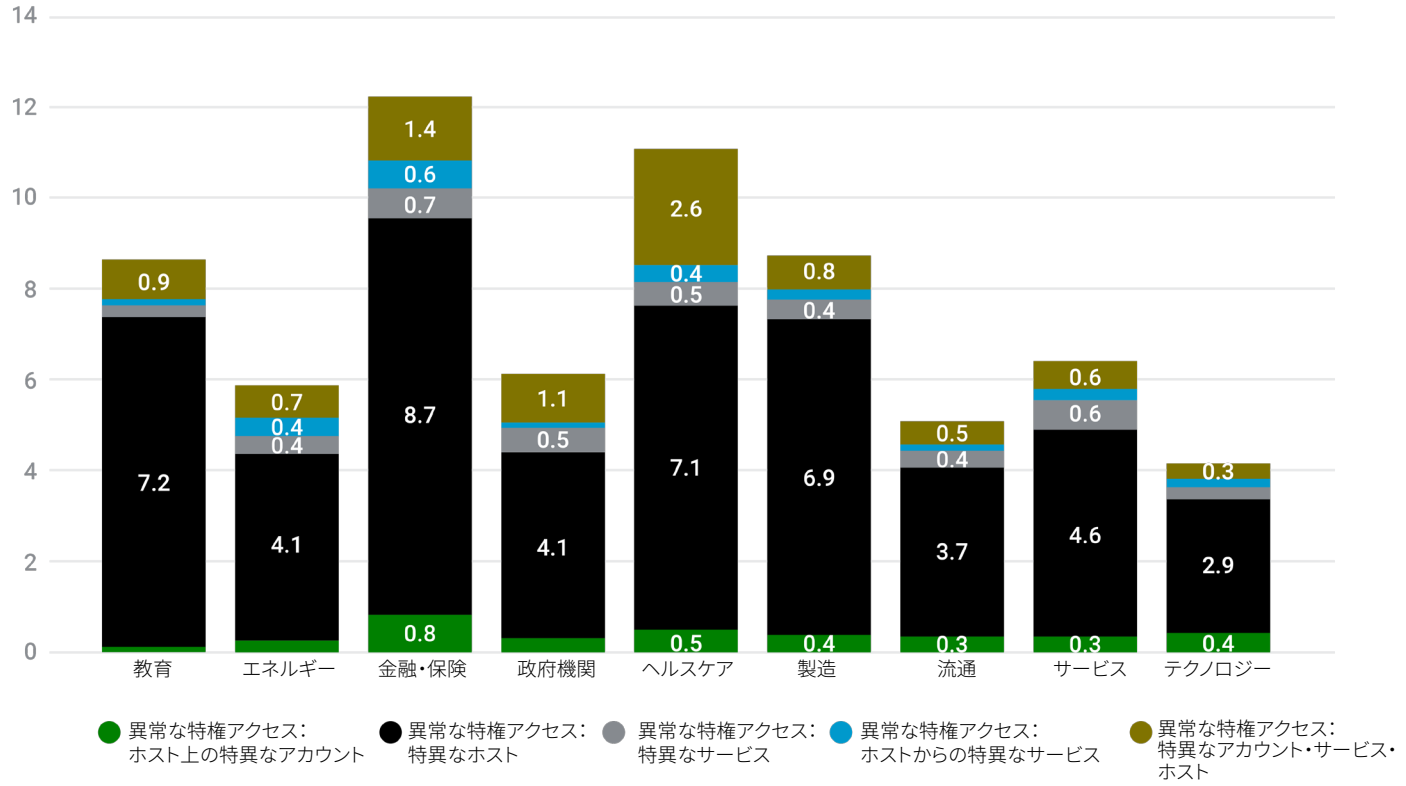


1万件あたりのタイプ別の異常な特権アクセス

特異なホストからの特権アクセス

特異なホストからの特権アクセスは、サービスに対して、通常は使用されることのないホストのアカウントを使ってアクセスを試みる行為です。

このような行動では、2つのシナリオが想定されます。1つは、該当アカウントが攻撃者のコントロール下にあり、アカウントそのものには問題がないものの、複数のサービスに接続するために、特異なホストからそのアカウントが使用されている場合です。そしてもう1つは、定常的には特定のホストから業務を行っているが、ネットワークへのアクセスが許可された社員、または契約社員に対して新しいホストが割り当てられたり、また別のホストから業務を行えるように、臨時にホストが割り当てられたような場合です。



1万件あたりの業界別の特異な特権アクセス

2019年の6ヶ月間における特異なホストからの特権アクセスのデータを、その発生数や業界を基に分析してみると、他のどのような業界と比較しても、金融・保険業界における特権アクセスが際立って多くなっていることが分かります。通常、特異なアクセスのほとんどは、特権アクセスを使って未知のシステムから正当な業務を実施しようとする社員によるもので、これらには何の問題もありません。しかし、このようなアクセスが許可され、特権アクセスがどこでどのように発生するかという件が管理されていない状況は、金融機関に限らず、全ての組織にとって大きなリスクとなります。これは、特権アクセス管理のポリシーや、その運用に大きな改善の余地があることを示しています。

攻撃者の立場で侵害を阻止

特権アクセスの不正利用に関する検知については、その大部分が静的な問題として取り扱われ、また、予防的なアプローチのため、もしくは脅威が発生した後の手作業による対応に依存してきており、本来の適切な対応を図るための努力は、ほとんど行われてきませんでした。また、全てのエンティティを同じ価値を持つものとして扱う、パターンベースの手法を採用した対応では、実際に運用することが不可能なほど大量のアラートが発生してしまいます。

セキュリティの運用では、エンティティに付与された特権に依存したり、また特権に捉われることなく、実際にエンティティがネットワーク内で特権をどのように行使しているか、例えば特権の振る舞いなどに焦点を当てる必要があります。

このような見方は、エンティティ間のやり取りを解析したり、推測する手法に類似しています。防御する側も攻撃側と同じ手法で考えることが重要だということです。そして、これは以下の2つの対応を行う際に発生します：

- エンティティ間のやり取りを分析。エンティティ間の実際のやり取りと、最終的にアクセスしたアセットの機密度に応じて、各エンティティの特権レベルを動的に決定します。同様のアクセスパターンを持つエンティティは、同類なものとしてグループ化します。この対応は、人工知能と機械学習を使って実現することができます。
- 特権エンティティ間のやり取りの異常度を決定。実際のアクセスリクエストとアクセス履歴を比較し、正常なグループからの乖離の度合いを決定します。セキュリティ上で影響を及ぼす異常そのものに焦点を当てます。

特権を分析すると、アカウントを使用する際の振る舞いには、特定の5つのパターンがあることが分かります。

1. 特定のアカウントを使ってホストからサービスにアクセスしているものの、そのホストでは、通常そのアカウントが有効になっていないか、または通常そのホストからサービスにアクセスすることがない。
2. 通常であれば特定のホストから使用されるアカウントが、どのホストからのアクセスも確認されていないサービスに対してアクセスを行っている。
3. これまでの振る舞いの観察結果と一致しない組み合わせ（アカウント・ホスト、アカウント・サービスおよびホスト・サービス）で、ホストからサービスへのアクセスリクエストにアカウントが使用されている。
4. 特定のホストによる（別のアカウントを使った）サービスへのアクセスは確認されているものの、該当する特権アカウントを使った特権サービスへのアクセスは観察されたことがない。
5. アカウントの存在を観察できたホストから、特権アカウントを使って特権サービスにアクセしているものの、そのホスト自体によるサービスへのアクセスを確認できていない場合。

まとめ

クラウドネイティブな環境とハイブリッドクラウド環境の両方を監視することが極めて重要であり、また、そこで得られた内容をセキュリティ分析に適した実践的な情報に変換するために、どのように双方のデータとコンテキストの関連付けを行うかといった点を決定する必要があります。つまり、ホストやネットワークを監視するだけでなく、ローカルネットワークやプライベートのデータセンター、さらにクラウドインスタンス間など、企業全体で、どのように特権アクセスが発生しているかを理解する必要があるということです。

さらに、ネットワークやクラウド固有のデータを活用できる適切なツールを導入することで、特権アクセスや他の攻撃者の振る舞いを可視化することができます。クラウド上のデータソースとネットワークのデータを組み合わせることで、重大なセキュリティ事故が発生する前に、不正を検出できる可能性を高め、精度の高い情報を提供することができます。

エクスプロイトを監視するだけでは、最新の侵入拡大の事例を見逃す可能性があり、また、ホスト中心のビューを取得するだけでは、攻撃者が隠れる場所を増やすことになるため、このようなアクセスの監視の取り組みは不可欠なものとなります。つまり、検知率を向上させるためには、サービスやアカウントのビューを使って様々な方向から解析する必要があるのです。

このタイプのアクティビティを監視することの重要性については、現実的に攻撃が蔓延している状況を考えれば、もはや議論の余地はありません。特異なホストによる特権アクセスの不正使用は、異常な振る舞いの多くで共通に発生しているため、ホストベースの対策に固執しているだけでは、攻撃者に対して内部での活動を隠ぺいできる多くの余地を与えることになります。このため、アカウントとサービスに対して、これまで以上に焦点を当てることが重要となります。

プロダクションシステムへの変更は、検知が困難かもしれません。しかし、企業のインフラストラクチャー全体を全方位で可視化することにより、侵害を受けたシステムやサービスにおいて、通常観察される範囲を超えた攻撃者の行動を、はるかに容易に検知できるようになります。

また、セキュリティ運用チームが、インフラストラクチャーの正常な状態に関する確かな情報を把握することで、悪意のある行動や特権の乱用を容易に識別し、緩和することも可能となります。

現実のクラウドやデータセンター、企業の環境におけるサイバー攻撃の行動に関する詳細については、Vectraの2020 RSA Edition of the Attacker Behavior Industry Report（攻撃者の振る舞いに関する業界レポート 2020年RSA版）でご確認ください。

VECTRA AI, INC.

Security that thinks®

お問合せ：

SR_PrivilegedTrustedAccess_021920

製品、ソリューションなどに関するお問い合わせは、info-japan@vectra.ai までお願いします。

© 2020 Vectra AI, Inc. All rights reserved. Vectra、Vectra AI社のロゴ、CognitoおよびSecurity that thinksは、Vectra AI社の登録商標です。Cognito Detect、Cognito Recall、Cognito Stream、Vectra Threat LabsおよびThreat Certainty Indexは、Vectra AI社の商標です。その他の会社名、製品名およびサービス名は、一般に各社の登録商標またはサービスマークです。