ソフトウェアベースのセグメンテーション

インサイドアウトのアプローチでセキュリティの信頼性を獲得

目次

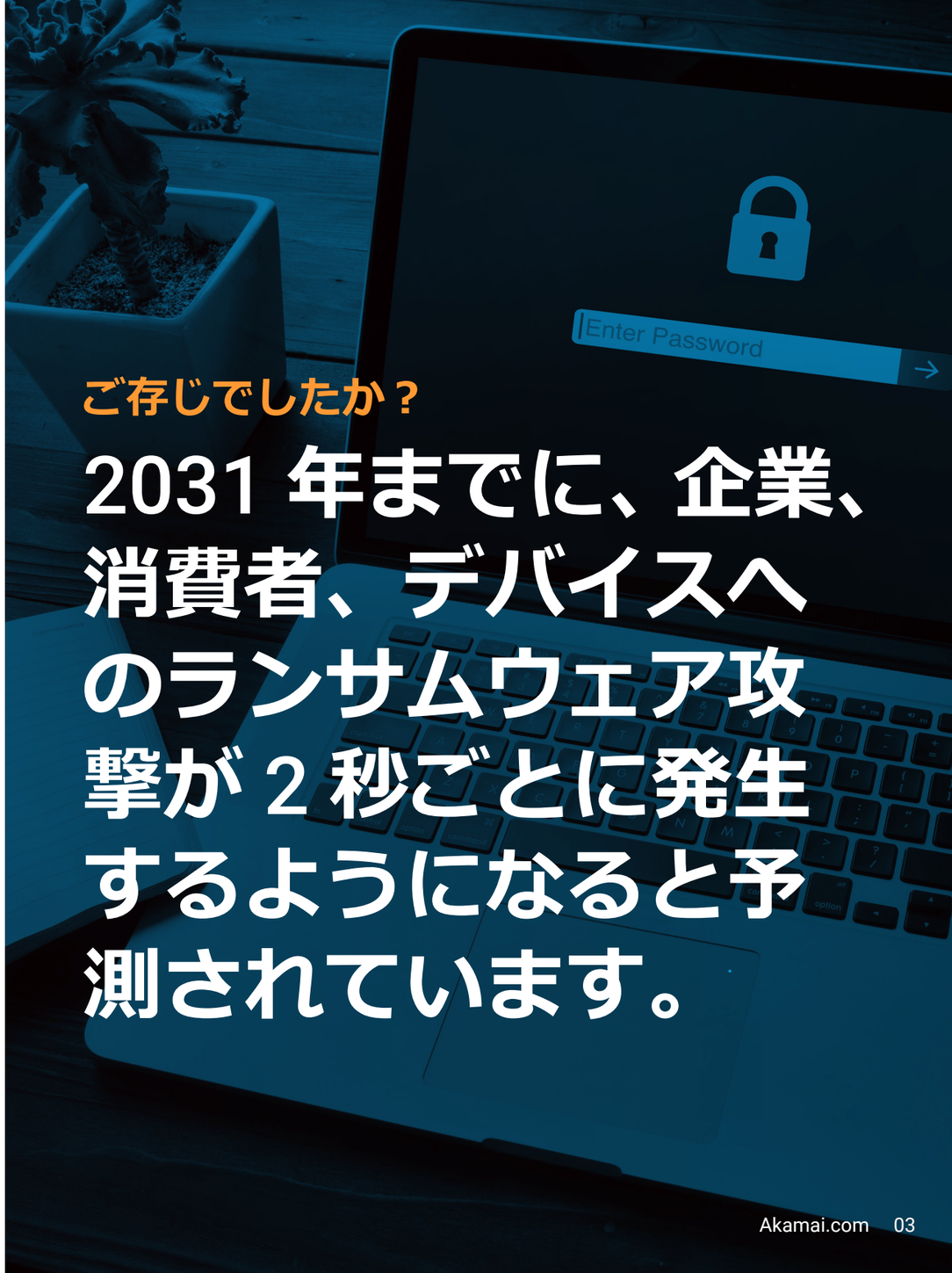
これまでのレガシーファイアウォールからの脱却

古くなったオンプレミスのファイアウォールと決別しましょう。現在の IT 環境とセキュリティ要件は、当初の目的よりもはるか先を行っています。サイバーセキュリティの状況も進化しています。攻撃手法は洗練され、サイバー犯罪者の数はこれまで以上に増えています。数十年前のアプライアンスアーキテクチャでは、最新のマルウェア、ボットネット攻撃、フィッシング行為、ソーシャルエンジニアリング、データ脅迫に太刀打ちできません。

コストの高さ、モバイルへの非対応、可視性の欠如など、レガシーファイアウォールは無数の問題を抱えていますが、現実的には、近い将来に姿を消すことはありません。ファイアウォールは、ネットワークツリーを縦方向に流れるトラフィックの境界防御で効果を発揮し、組織の周囲に強固な防御網を築きます。

しかし、オンプレミスのデータセンターやクラウド内を横方向に流れるトラフィックの管理となると、ファイアウォールの手に負えません。

そこで、ソフトウェアベースのセグメンテーションの出番です。



ご存じでしたか？

2031 年までに、企業、消費者、デバイスへのランサムウェア攻撃が 2 秒ごとに発生するようになると予測されています。

解決された

レガシーファイアウォールの3つの問題

1. 問題点：**可視性の欠如**

   データの流れを可視化できないと、ルールの導入と維持が困難になります。そのため、ファイアウォールのルールセットが非常に長くなり、緩すぎるルールや不要なルールがあふれることになります。

ソリューション

ビジュアルマップ、資産分類、アプリケーション依存度マッピングとともに、ポリシー作成と管理を統合したソリューションをご検討ください。

解決された

レガシーファイアウォールの3 つの問題

2. 問題点：ファイアウォールは維持が困難

アプリケーションオーナーとファイアウォール管理者が通信に必要な IP ポートやプロトコルを知っていることはまれです。そのため、ファイアウォールの管理は反復的なトラブルシューティングに終始します。

ソリューション

IP やポートなどの固定されたネットワーク「配管」に合わせてポリシーを構築するのではなく、アプリケーションが使用するプロセスなどの有意義な属性や、完全修飾ドメイン名（FQDN）、ユーザー ID に基づいてポリシーを構築します。こうすることで、データセンターに変更を加えたり、ワークロードをクラウドに移行しても、同じ属性を保ったまま、ポリシーをそのまま適用できます。

解決された

レガシーファイアウォールの 3 つの問題

3. 問題点：ファイアウォールはアジリティに欠けている

通常、ファイアウォールに変更を加えると、計画的なダウンタイムが必要になります。アプリケーションオーナーが変更を適用する場合、メンテナンス期間にしか作業できないため、その変更を確認して導入するまで 1 週間以上待つことになります。

ソリューション

最新の IT 組織は、変更期間を設けるという考え方から、アプリケーションを停止することなく継続的に更新できる DevOps モデルへと移行しています。アプリケーション自体で使用している同じ DevOps ツールを使用して自動化できるテクノロジーソリューションをご検討ください。このように、進化し続けるアプリケーションに合わせて、セキュリティアプローチも進化させます。

そのままの状態で移行できる

従来のやり方について考えてみましょう。複雑で適応力の低い旧式のレガシーファイアウォールの管理アプローチは、場所に基づくセグメンテーションでした。場所は容易に変更できません。通常は、ハードコードされた IP アドレスをベースとするか、データセンターにルーティングされます。つまり、ファイアウォールでセキュリティを確保するためには、あらゆるものを物理的に移動する必要があるため、当然ながら、リソースを大量に消費し、リスク回避が重要になり、時間がかかります。クラウドへの移行？可視性？十分なセキュリティ？すべて忘れましょう。

レガシーファイアウォールはそのままで大丈夫です。深呼吸して、新しいやり方を導入してみませんか。ソフトウェアベースのセグメンテーションは、既存のファイアウォールと並べて簡単に導入することができ、適応性に優れています。ソフトウェアベースのセグメンテーションでは、環境、データセンター、ネットワークを実際に見ながら変更し、ポリシーを設定できます。さらに、ワークロードやポリシーを、クラウドやデータセンターなど、どこにでも割り当てることができます。ネットワークを変更せず、システムのダウンタイムなしで、セキュリティポリシーを適用して調整することも可能です。

内部のセグメントを明らかにする

実際に目で見て確認できないものを信頼できるでしょうか。できないと思います。ファイアウォールの内側でセキュリティポリシーを確立する場合も同じです。実際に内部を見ることはできません。これは、建物の中にいる人を見ることができないまま、建物を外から眺めているようなものです。

ソフトウェアベースのセグメンテーションは、偶然には成立しません。細かいピースに分けることで、ワークロードが実際に関与するあらゆるアクティビティを総合的に把握します。環境の内部にある要素を把握できたら、特定のユースケースに合わせて計画を策定し、セグメントを有意義で効果的なパーツに分割します。

境界を越えたセキュリティ

レガシーファイアウォールは、変化に対応するように構築されていません。境界では、DDoS 防御やトラフィックのフィルタリング／検査などの重要な目的を果たしますが、ネットワーク内のセキュリティはファイアウォールでは手に負えません。その理由は、必然的な渋滞ポイントとして展開されているからです。つまり、あらゆるセグメンテーション作業には、ネットワークやアプリケーションの変更や削除など、運用上のボトルネックが伴います。手間がかかり、多くのリソースを必要とします。

ソフトウェアベースのセグメンテーションでは、こうした運用上の課題を克服し、エンドポイントや境界を越えてセキュリティ対策を継続できます。第一に、渋滞ポイントではなく、分散したファイアウォールアプローチを取ります。第二に、ワークロードを中心に考えます。つまり、ホストシステムからデータを収集してアセット分類に適用し、プロセスレベルのコンテンツやポリシーなど、ルールをさらに細かく指定します。全体として、ソフトウェアベースのセグメンテーションでは、ファイアウォールより少ない労力とリソースで、ネットワーク内の重要なアセットを柔軟かつ緻密に保護できます。

セグメンテーションの 4 つの基本

セグメンテーションはこれまで以上に重要となっています。アタックサーフェスは拡大しています。ランサムウェアなどの高度化した攻撃は、侵害後に横方向に移動するので、境界を越えたアプリケーションの依存関係についても考慮が必要です。しかし、セグメンテーションは一度限りのアプローチではありません。

セグメンテーションには一般に 4 つのタイプがあります。それぞれの違いと必要とされる理由をまとめます。

1. 環境のセグメンテーション

開発、QA、ステージング、実稼働など、異なる開発環境に分割します。環境セグメンテーションは大まかなセグメンテーションです。最終的な目的は、システムを異なる環境に分割し、必要なユーザーやアプリケーションのみにアクセスを制限することです。非実稼働システムから実稼働システムへのアクセスは、多くのコンプライアンスイニシアチブで禁止されています。

2. ネットワークセグメンテーション

アーキテクチャ型のアプローチです。ネットワークを複数のサブネットワークに分割し、それぞれが小規模なネットワークセグメントになります。ネットワークセグメンテーションにより、IT オペレーターは、ネットワークトラフィックを効果的に管理し、パフォーマンスを高めて、セキュリティを改善できます。

3. マイクロセグメンテーション

より緻密なセグメンテーションです。各ワークロードを分離し、個別にセキュリティを確保するために使用します。プロセス、コンテナ、ユーザー、ドメイン名、デバイスなどの要素に対してセグメンテーションルールを指定することもできます。このアプローチは、横方向のトラフィックコントロールに適しており、ラテラルムーブメント（横方向の移動）に対して防御力を発揮します。

4. ID ベースのセグメンテーション

マイクロセグメンテーションによる単一エンドポイント、デバイス、ワークロード、コンテナの保護機能を拡張し、通信を許可するかどうかの判断の一環として、ユーザー、デバイス、コンテキストなどの ID を評価する動的なルールを適用します。ID ベースのセグメンテーションポリシーでは、より緻密な設定が可能です。IP やポートだけでなく、タグ、OS タイプ、アプリケーション特性なども指定できます。

神話と現実：セグメンテーションの 5 つの神話の真実

神話 1

セグメンテーションプロジェクトは難易度が高く、完了までに時間がかかりすぎる。

現実：まず可視性を確保し、自社環境内で何が起こっているのか明確に把握することで、セグメンテーションプロジェクトの完了までの所要期間を数か月から数週間に、場合によっては数日に短縮できます。最新のセグメンテーションテクノロジーでは、AI を活用することでプロセスをさらに加速できます。

神話 2

セグメンテーションプロジェクトでは、ネットワークインフラの変更とダウンタイムが必須となる。

現実：ソフトウェアベースのセグメンテーションは、インフラからセキュリティを分離します。つまり、セグメンテーションは独立して実行できるため、基盤となるインフラの変更やダウンタイムは不要です。

神話 3

セグメンテーションにより、ネットワークの正当なトラフィックが遮断される。

現実：環境を視覚化し、ソフトウェアベースのセグメンテーションポリシーを適用することで、リアルタイムの適用前に、こうしたポリシーのビジネスアクティビティに対する影響を確認できます。

神話 4

セグメンテーションはユーザーのアクセスを阻害し、不要な遅延を発生させる。

現実：すべてのトラフィックを強制的に特定のファイアウォールの渋滞ポイントを通過させる代わりに、分散したソフトウェアベースのセグメンテーションポリシーを適用することで、ネットワークのボトルネックを解消できます。さらに、アプリケーションと ID をより正確に認識するポリシーにより、ユーザーアクセスを誤って阻害するリスクを削減できます。

神話 5

クラウドでは、オンプレミスと同じセグメンテーションツールを使用できない。

現実：セグメンテーションポリシーをインフラから分離する場合、データセンターで使用していた同じポリシーをクラウドでも使用できます。

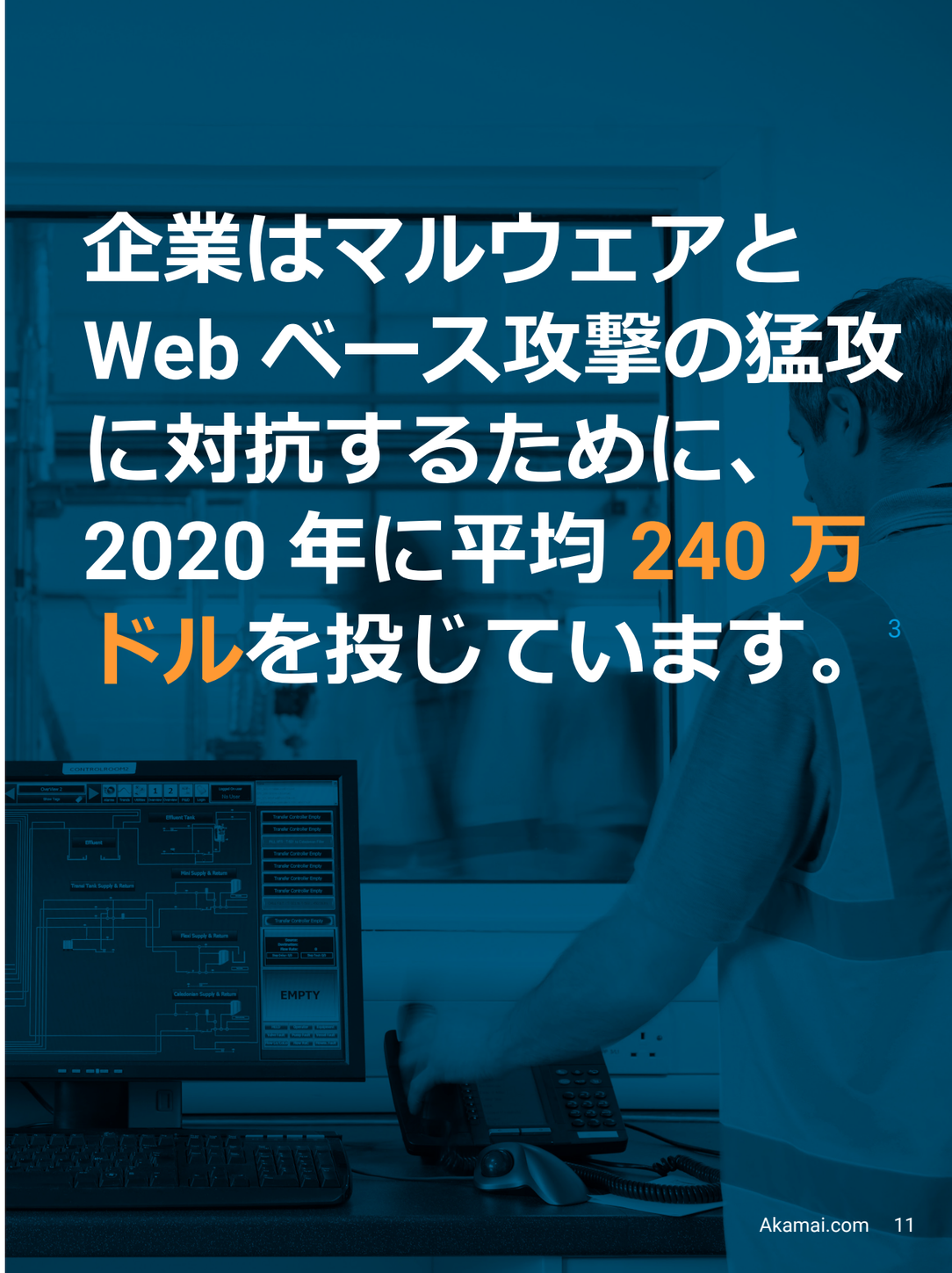
内側のリスクを軽減

侵害が発生すると、ビジネスが阻害され、データ漏えいが生じて、ブランドが損なわれ、多額の代償を負うことになります。

ファイアウォールですべてを防ぐことができると信じていますか？もう一度考えてみてください。攻撃者がネットワーク、環境、データセンターを侵害すると、ラテラルムーブメントを駆使してデータを盗み取り、アプリケーションサーバーのコントロールを奪い、データベースサーバーにアクセスするなど、大きな混乱を引き起こします。

実際、攻撃の 70% でラテラルムーブメントが試行されています。[2]

ファイアウォールはラテラルムーブメントをネットワークで発生する正当なトラフィックとみなしますが、ソフトウェアベースのセグメンテーションはこれを完全に阻止します。セキュリティプログラムの重要なコンポーネントとして、ソフトウェアベースのセグメンテーションはラテラルムーブメントを制限します。仮に侵害が発生しても、攻撃者が環境を容易に操作できないようにします。対抗する機会を得て、データや重要なアプリケーションを保護し、侵害時間を短縮し、攻撃者の検知も可能になります。このセグメンテーションアプローチは拡張性に優れ、使いやすく、ネットワークやシステムを変更することなく短時間で導入できます。



ゼロトラストを複雑に考える必要はない

ゼロトラストとは、誰が、何を、誰に、どのように行うのかを管理する手法です。つまり、ネットワーク内で誰が何をするのか明示的に制御するという考え方です。

ネットワーク内のあらゆるものにユーザーアクセスを許可すると、過大な信頼を与えることになり、その結果、組織全体がリスクにさらされます。第一に、従業員はミスをするものであり、そのミスがセキュリティに深刻な影響を与える可能性があります。悪意があるケースも考えられます。

さらに、VPN ネットワークとデバイスの外部には、対処すべきデータセンターへのエントリーポイントが数多くあります。たとえば、攻撃者は、実稼働サーバー（SolarWinds の侵害ケースなど）、インターネットに面した脆弱なアプリケーション、脆弱な VPN などを通じてネットワークに侵入します。この場合、ネットワーク内にあるというだけでサーバーを信頼しています。しかし実際には、攻撃者はあらゆるものにアクセスし、制約がない状態でラテラルムーブメントを仕掛けています。

実稼働ネットワークでゼロトラストを実現するためには、明示的に許可されていないすべてのアクティビティをブロックする必要があります。

これは、レガシーファイアウォールでは制御できないレベルの防御策です。IP アドレスやポートより深いレベルで属性を特定する必要があるからです。

また、ソフトウェアベースのセグメンテーションでは、何が実際に起きているのか細かく把握することができ、ID も含めて、人間が理解できる正確なポリシーを作成できます。

ゼロトラスト・チェックリスト：明示的な制御を得るための 6 つの方法

シンプルに考えましょう。信頼はセグメントの大きさで判断すべきです。セグメントが小さいほど、重要なデータ、資産、アプリケーションを効果的に保護できます。ここでは、運用を複雑にすることなくゼロトラストを実現するための 6 つのステップをまとめます。

1 機微な情報を特定する視覚化ラベルを使用します。

2 機微な情報の流れをマッピングする、自動化されたフローと依存度マッピングを使用します。

3 ゼロトラストのマイクロ境界を構築する、セグメンテーションやマイクロセグメンテーションポリシーをすばやく定義できる適切なツールを使用します。

4 ゼロトラスト・エコシステムを継続的に監視するリアルタイムの監視および分析機能を使用します。

5 セキュリティの自動化とオーケストレーション、API とテクノロジーの統合を導入します。

6 攻撃を受けた場合、ユーザーやセグメントにかかわらず、あらかじめ設定した属性を持つあらゆるマシンの信頼を簡単に解除できる、ユーザーやマシンの信頼を解除する機能を搭載します。

結論

現時点で、古いソリューションと決別し、ネットワーク内部のセキュリティ対策を強化することについて不安を感じているかもしれません。

ご安心ください。

レガシーファイアウォールはそのままで大丈夫です。ネットワークの境界防御には依然として効果的です。しかし、メリットはそこまでです。

最も重視すべき防御対象は組織のコアにあります。つまり、境界の内側にあるデジタル資産、データ、アプリケーションであり、企業インフラの内臓とも言うべき部分です。アウトサイドイン（外側から内側）の発想から転換して、ソフトウェアベースのセグメンテーションとゼロトラスト・フレームワークを導入することで、必要な可視性と制御が得られます。ラテラルムーブメント（横方向の移動）を検知して阻止し、緻密で柔軟なポリシーを適用し、サイバー攻撃を防いでランサムウェアなどがネットワーク全体に広まらないように対策を講じることができます。

ランサムウェア、ゼロトラスト、クラウドセキュリティなどに対して、セグメンテーションがどのように役立つのか、詳細についてはデモをお申込みになるか、こちらをご覧ください。

1 Cybersecurity Ventures、2022 Who's Who In Ransomware Report（ランサムウェアを操る者たち：2022 年レポート）Conceal、2022 年。

2 Tom Kellermann、Greg Foss、Global Incident Response Threat Report（グローバルインシデント対応の脅威レポート）、VMware Carbon Black、2020 年 10 月。

3 「2023 Cyber Security Statistics Trends & Data（2023 年サイバーセキュリティ統計の傾向とデータ）」、PurpleSec、2023 年 2 月 22 日。