Gartner

サイバーセキュリティの脅威：ディープフェイクによるなりすまし

インサイト

- 生成AIによるディープフェイクが広まり、なりすましや偽情報の攻撃にさらされる範囲は一気に拡大しました。多額の金銭的被害、企業の信用の失墜など、想定される被害は多岐にわたります。サイバーセキュリティ・リーダーに求められるのは、検知ツールを個別に導入して終わりにしないことです。多層防御の戦略と部門横断のガバナンスを組み合わせ、信頼と事業運営の健全性を守らなければなりません。
- 2027年までに、AIで生成したディープフェイクによる顔認証への攻撃が広がり、企業の40%が、こうした本人確認・認証ソリューションだけでは十分ではないと判断するようになります。
- ディープフェイクが企業に向けられる経路は、主に2つです。1つは生体認証システムを狙ったなりすまし、もう1つは採用担当者や経理部門といった従業員を狙ったソーシャル・エンジニアリングです (ページ5 図1を参照)。

Gartner®

主なインサイトとデータ

- 41%の組織が、音声通話でディープフェイクとソーシャル・エンジニアリングを組み合わせた攻撃を経験しています。
- 北朝鮮をはじめとする制裁対象国の工作員が、リモート勤務の職に応募するケースの報告が急増しています。面接の通話でディープフェイクが使用された事例も数多く確認されています。
- ディープフェイクの検知ベンダーは急速に増えています。一方で、その精度を見極めるための標準やベンチマークは整っていません。

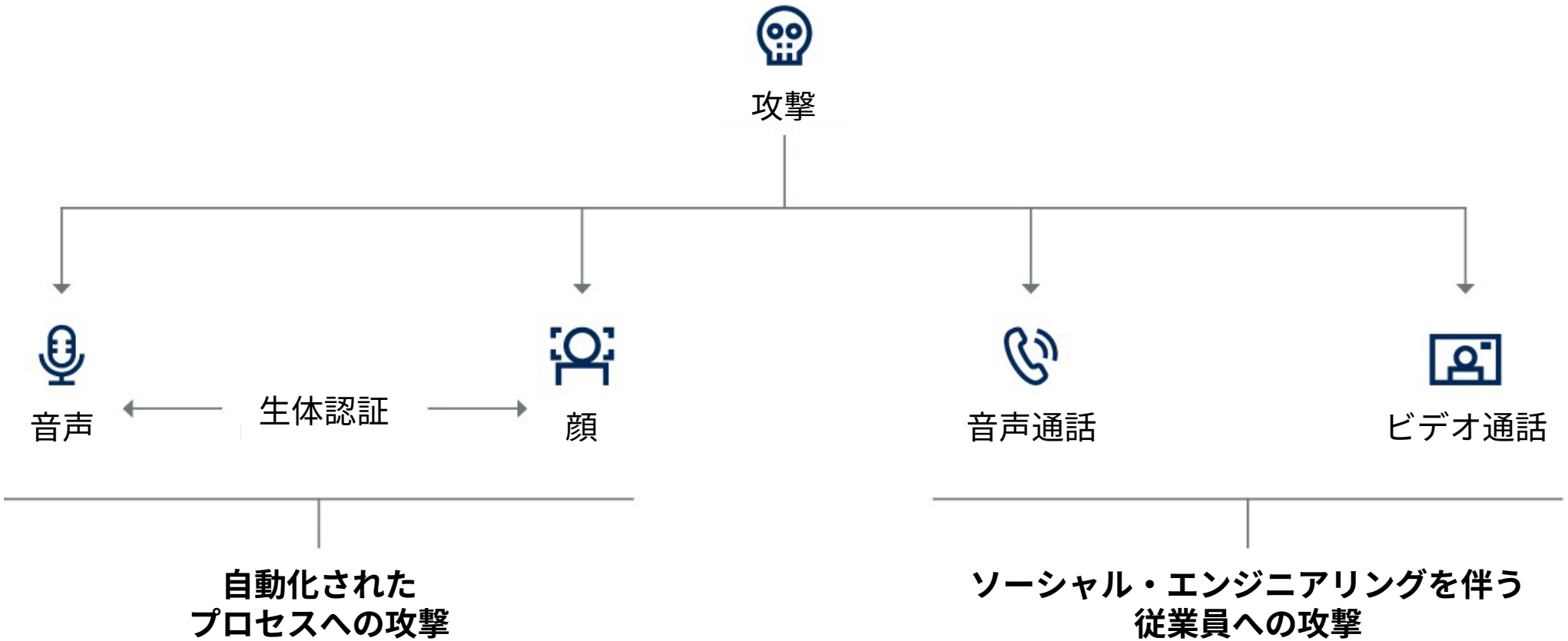
Gartner

提言

- 検知技術だけに依存した統制策は危険です。ディープフェイクの生成技術は進化が速く、検知精度を評価する方法にも限界があります。この前提を踏まえて対策を講じてください。
- ディープフェイクがリスクとなる場面ごとに、複数の統制策を組み合わせましょう。検知だけに頼らず、前後の状況から得られるコンテキスト情報、認証要素の追加、コンテンツの出所や履歴の確認を組み合わせます。
- サイバーセキュリティ、IT、広報、マーケティング、法務、リスクの各リーダーが集まる、部門横断の「トラスト評議会」を設けてください。ディープフェイクによるなりすましと偽情報に対するセキュリティ戦略を統括し、必要に応じて、危機対応の司令塔にもなります。

Gartner®

図1：ディープフェイクによるなりすましの攻撃ベクトル



Gartner

実用的で客観的なインサイト

成功に向けて、組織の態勢を整えましょう。サイバーセキュリティ・リーダー
およびそのチーム向けの無料リソースとツールも、ぜひご活用ください。

コンファレンス

ガートナー サイバーセキュリティ & リスク・マネジメント サミット

複雑化し、変化し続けるサイバー脅威に対して、組織を守るためのインサイトを入手できます。

詳細を見る

Gartnerによるご支援

Gartner for CISOs: 最高情報セキュリティ責任者 (CISO) 向けサービス

AI搭載ツール、オンデマンドのインサイト、インタラクティブな体験で、成果の創出を加速します。

詳細を見る

Webinar

ランサムウェア対策：事業停止リスクに備えるバックアップの再定義と復旧戦略

ランサムウェア被害時に重要なのは、バックアップの有無ではなく迅速な復旧能力です。事業再開を阻まれたケースから学び、事業停止期間を短縮するための復旧戦略を解説します。

今すぐ視聴

Webinar

AI時代のセキュリティ運用に求められる新しいアプローチ方法

AIを活用して自社のセキュリティをどのように強化すべきか、そしてその取り組みをどのように推進するのかについて、「AIセキュリティ戦略」の観点から解説します。

今すぐ視聴

Gartner のお客様は、クライアント・ポータルでさらに多くのリソースをご利用いただけます。 ログイン ↗

Gartner

Connect with us

Gartner は、経営幹部およびそのチームに対し、実行可能かつ客観的なビジネスおよびテクノロジのインサイトを提供します。Gartner のエキスパートによるガイダンスやツールは、組織の重要な課題について、迅速で優れた意思決定と大きな成果の創出を可能にします。

Gartnerのサービスに関するお問い合わせ

サイバーセキュリティ・リーダーを成功に導く
gartner.co.jp/ja/cybersecurity

最新のインサイトをご確認ください

Gartner のコンファレンスにご参加ください
コンファレンスの最新情報を見る

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner