投資テーマの軸は「AIをどう動かすか」から「どう守るか」へ移りつつある

So What

AIエージェントが本格的に普及するほど、
守るべき「身分証」は爆発的に増える。
セキュリティの重要性は、AIの普及で
減るどころか、むしろこれから増す。

2月：「AIに中抜きされる」と急落 → **5月：「AIを守る側」として最高値圏へ反転**

3ヶ月の往復は、この見立てを裏づける動きだった

01

過剰反応だった2月の急落

「コードを直すAI」が出ても、フィッシング・権限管理・認証の守りは消えない。コードスキャン以外まで一括で売られた。

02

新しい守備範囲の出現

自律エージェントの増加で、人間以外の「身分証（NHI）」が急増。乗っ取り・権限過多・認証残存など新たなリスク面が広がる。

03

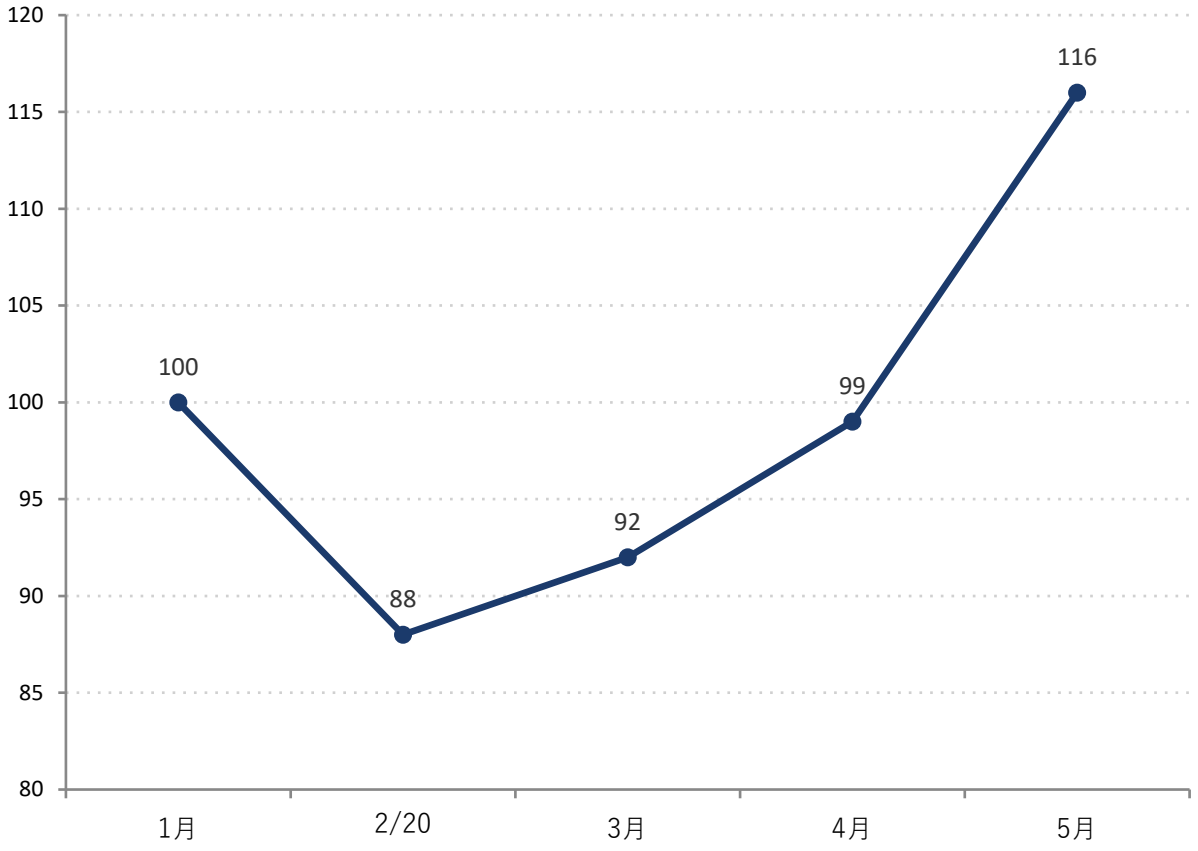
中核を担う3社

アイデンティティのOkta、エンドポイントのCrowdStrike、ランタイム＋統合のPalo Alto。守る場所が違い、補い合う関係にある。

出所：各社IR、報道各社をもとに作成

2026年2月20日、AIへの「中抜き」懸念で大手セキュリティ株が一斉に急落した

セクターETF（CIBR）の推移イメージ



※ 1月初を100として指数化（図示のためのイメージ）

約150億 ドル

1営業日で消えた大手各社の時価総額（2兆円超）

▲25%超

JFrog の下落率（コードスキャン専業が直撃）

引き金：Claude Code Security の発表

ソースコードを自律的にスキャンし、脆弱性を発見・修正案を提示する機能。社内テストで500件超の未知の重大な脆弱性を発見と説明。

前年11月にはAIを悪用した大規模攻撃も公表されており、「AIがセキュリティ業界を飲み込む」懸念が一気に表面化した。

出所：Bloomberg、CNBC、各社報道をもとに作成

急落は「ひとくくり」の過剰反応 — コードスキャン以外の守りは消えない

Claude Code Securityが脅かすのは「コードの中の脆弱性」だけ。下表のリスクはコードが綺麗になっても残り、AIが攻撃を高速化するほど重要性はむしろ増す。

コードが綺麗でも残るリスク

1. 従業員がフィッシングのリンクをクリックする
2. ヘルプデスクがだまされ、パスワードを再設定する
3. 使い回されたパスワードがどこかで漏れる
4. 退職者のアカウントが消されずに残る

「論理的でない」と見たプロの声

バークレイズ

「Claude Code Securityはエンドポイント検知・ID管理・ネットワーク防御とは競合しない。この売りは論理的でない。」

CrowdStrike CEO

「コードをスキャンするAIが、我々のプラットフォームを置き換えることはない。」

Palo Alto CEO

「なぜ市場がAIを脅威と見るのか困惑。顧客はむしろもっとAIを求めている。」

Anthropic自身が攻守両面に 脆弱性を見つけるAIを作る一方、防御側が先に塞ぐ枠組み「Project Glasswing」を主導。CrowdStrikeやPalo Altoも参加とされる。

出所：Barclays、各社IRをもとに作成

AIエージェントの普及が「身分証の爆発」を生み、4つの新しいリスク面を広げる

自律的に動くエージェントやサービスアカウント等の「人間でない身分証（NHI）」は人間を大きく上回る。守る対象が増えることで、次の攻撃面が新たに立ち上がる。

① エージェントの乗っ取り

読み込ませる文章に指示を仕込む「プロンプトインジェクション」。細工したカレンダー招待でAIアシスタントを操り、情報を引き出せた実証例も。

例：カレンダー招待／AIブラウザの買い物代行

② 権限の与えすぎ

強い権限を渡したエージェントが暴走・乗っ取られると被害が一気に拡大。最小権限の原則が守りの基本になる。

例：コーディングAIが本番DBを削除（2025年7月）

③ 身分証が消えずに残る

発行された認証トークンが役目を終えても有効なまま放置されると、攻撃者の入口に。「置き忘れた合鍵」を確実に無効化する仕組みが要る。

例：クラウド侵害で数ヶ月有効なトークンが残存

④ 共通規格MCPを狙う攻撃

AIと外部ツールをつなぐMCPが事実上の標準に急拡大。共通言語のすき間に穴があれば、無数のシステムが一気に危険にさらされる。

公開サーバー1万件超／SDK月間DL 1億回に迫る

出所：Okta、各社報道、セキュリティ研究をもとに作成

広がった守備範囲を、3つの層で中核3社が分担して押さえにいく

これらは従来のセキュリティと入れ替わるのではなく、上乗せされる新領域。守る相手は「人間とPC」から「人間＋無数のエージェント＋膨大な身分証」へ広がる。

アイデンティティ層

1

無数に増える「身分証」を、誰が・どこまでの権限で・いつまで持つのかを管理する。

Okta（OKTA）

エンドポイント層

2

エージェントが動く端末やサーバーの上で、おかしな挙動が起きていないかを検知する。

CrowdStrike（CRWD）

ランタイム層

3

エージェントの入力と出力を、その瞬間に検査して危険を弾く。買収で統合も主導。

Palo Alto Networks（PANW）

守る場所が違うため、競合というより互いを補い合う関係

出所：各社IRをもとに作成

Okta：エージェントを「新しい労働力」と捉え、中立のID基盤で攻める

戦略：エージェントにも人間と同じ「身元管理」を

- **エージェント＝新しい労働力**

  入社手続き・権限付与・退職時の停止。人間社員と同じ統治を、無数のエージェントにも適用する発想。

- **Okta for AI Agents**

  エージェントの身分証を発見・登録・権限付与・統治する製品群を投入。

- **Cross App Access**

  アプリ任せの権限をID基盤側で一元管理。MCPサーバーへの安全接続の推奨方式とされ、Salesforce・AWS・Google Cloudが支持。

- **強みは「中立性」**

  特定の巨大プラットフォームに縛られず、各社の製品を等しく扱える独立の立場。

直近四半期（2026年2〜4月）

+11%
売上高（前年同期比）
市場予想を上回る

+16%
RPO（受注残）47億ドル超
先行指標が伸長

約25%
新製品群が占める予約比率
AI案件は大型

+30%
決算翌日の株価上昇率（5/29）
終値約123ドル、年初来高値

「反撃の狼煙」

通期見通しも引き上げ。エージェント時代の新需要が、初期ながら実際の受注として表れ始めた手応え。2026年Forrester WaveでもID基盤のリーダーに位置づけ。

出所：Okta IR（FY2027 Q1、2026年5月28日発表）をもとに作成

CrowdStrike：エージェントを「守る」と「作って走らせる」の両面で攻める

戦略：端末の足元を押さえ、防御もエージェント化

- **Falcon プラットフォーム**

  端末・サーバー・仮想マシン一台ずつに軽量センサーを置き、あやしい挙動をリアルタイムに検知・遮断。エージェントもどこかの端末上で動く。

- **守る対象としての監視**

  AIエージェントの異常な挙動を検知対象に取り込む。

- **Charlotte AI / AgentWorks**

  AIアシスタントをFalconに組み込み、ノーコードでセキュリティ用エージェントを構築。人手不足の監視現場をエージェントで回す。

数字の勢いは3社で際立つ

52.5億$

ARR（年間経常収益）
前年比 +24%

最速

専業として50億ドル超え達成
AI契約が牽引

「GPUからエージェント、プロンプトに至るまで、あらゆる層でAIを守るミッションクリティカルなインフラだ」（CEO）

留意点

株価には期待が厚く乗り「織り込みすぎ」を警戒する声も。2024年7月の世界的システム障害の記憶も完全には消えていない。次回決算は2026年6月初旬。

出所：CrowdStrike IR（FY2026、2026年3月発表）をもとに作成

Palo Alto：ランタイム防御に加え、巨大買収で「全部入り」を狙う

AIの時代に向けた2つの大きな手

① Prisma AIRS ― ランタイム防御

AIアプリ／エージェントとLLMの「あいだ」に検問所を置き、入力と出力の両方を検査する「LLMガードレール」。プロンプトインジェクションを遮断し、機密情報の漏れも防ぐ。2026年4月にはAIゲートウェイ・監視のPortkey買収も発表。

② CyberArk買収 ― アイデンティティへ

2026年2月、特権アクセス管理の最大手CyberArkを約250億ドル（3.5兆円超）で買収完了。業界過去最大級。これでネットワーク防御・SOC・アイデンティティの3本柱が一つの傘に揃い、脅威検知の瞬間にアクセス権を取り上げる連携が社内で完結する。

直近四半期と統合の狙い

+33%

NGS ARR（63億ドル超）
会社見通しを上回る

250億$

CyberArk買収額（業界最大級）
3.5兆円超

一つの傘に揃う3本柱

- ネットワーク防御
- SOC（監視の司令塔）
- アイデンティティ

次回決算は2026年6月2日。CyberArk統合の初期の手応えが注目点。

出所：Palo Alto Networks IR（FY2026 Q2、2026年2月発表）をもとに作成

中核3社は守る層が異なり、競合ではなく補完関係にある

	Okta（OKTA）	CrowdStrike（CRWD）	Palo Alto（PANW）
担う層	アイデンティティ	エンドポイント	ランタイム＋統合
強み	中立のID基盤、 エージェント＝労働力	端末の足元を押さえる Falcon＋防御の自動化	LLMガードレール＋ 買収で3本柱を統合
AI向けの一手	Okta for AI Agents / Cross App Access	Charlotte AI / AgentWorks	Prisma AIRS / CyberArk・Portkey買収
直近の成長	売上 +11%、RPO +16%	ARR 52.5億$（+24%）	NGS ARR +33%
次の注目	新需要の受注化	6月初旬の決算	6/2決算・統合の進捗

守る場所が違うため、3社は奪い合うより、増え続けるエージェント需要を分担して取り込む関係にある

出所：各社IR（直近決算）をもとに作成

今後の注意点：過敏な地合い・割高感・統合・トレンド維持の4点

1 AI発表への過敏さ

フロンティアAIの新発表が出るたびに「今度こそ中抜き」の連想で急落しうる。次世代モデル登場時はとくに身構えたい。逆に、事業を冷静に見る投資家には観察に値する場面にも。

2 バリュエーション

OktaのPERは急騰後にGAAPベースで70倍前後へ。期待を大きく織り込むほど、それが揺らいだときの下げも急になりやすい。

3 CyberArk統合

Palo Altoは巨大買収を統合できるかが当面の鍵。費用で利益見通しが一時的に圧迫される面も。6/2決算が試金石。

4 セクターのトレンド維持

CIBR等のETFが2〜5月の上昇トレンドを保てるか。前年秋の高値超えを維持できるうちは地合い継続、明確に割り込めば期待が冷えたサイン。

「AIをどう動かすか」から「どう守るか」へ ― 主役交代が本物かを、決算のたびに確かめていきたい

出所：各社IR、報道各社をもとに作成