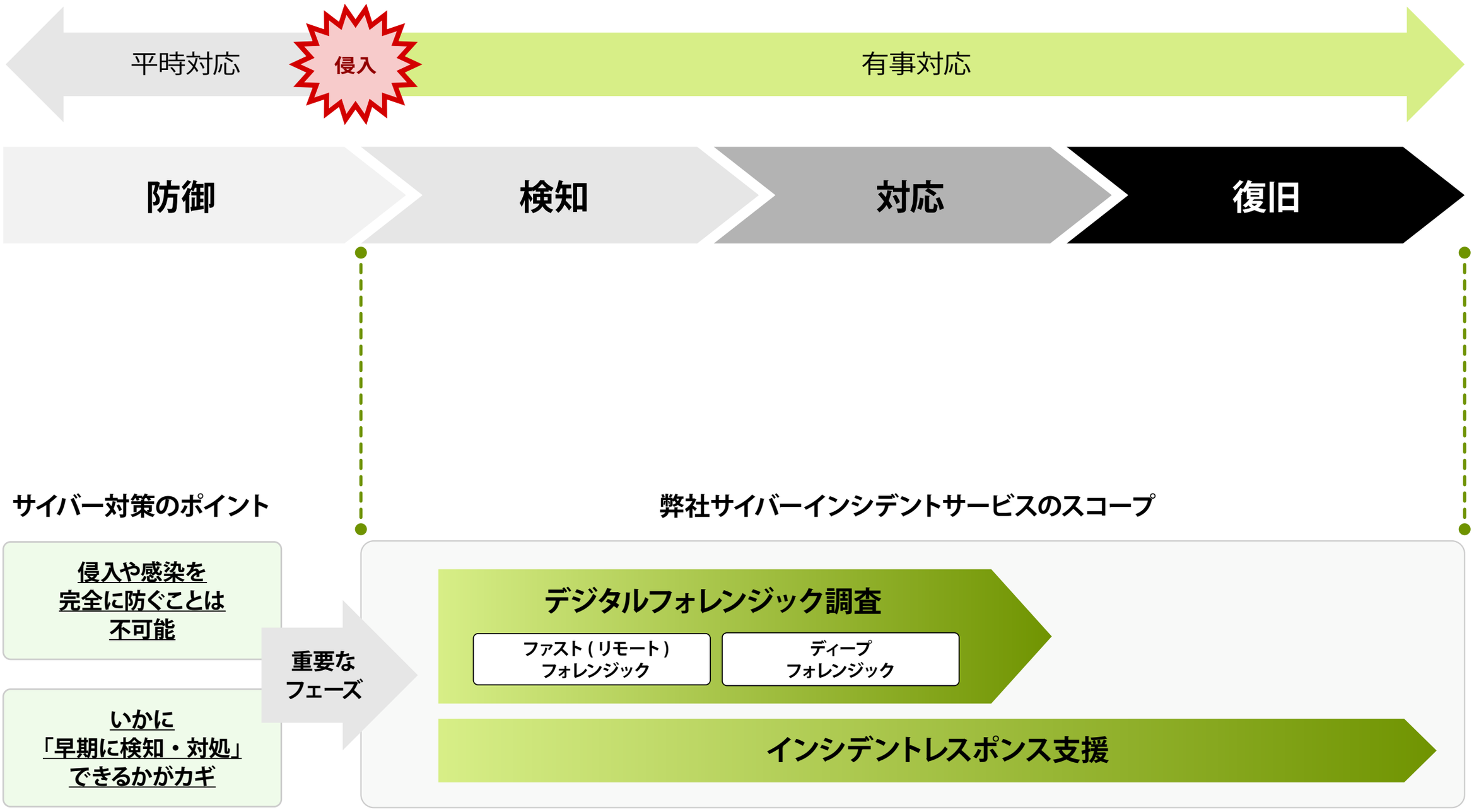
sprout

デジタルフォレンジック / インシデントレスポンス

サイバーインシデント対応サービスのご紹介

サイバーインシデント対応サービスについて

- サイバー攻撃が発生した際の原因究明、影響範囲の特定を目的とした**デジタルフォレンジック調査**を提供します
- また攻撃発生からの初動対応、封じ込め、復旧等、貴社の一連の**インシデントレスポンス対応**をご支援します



ファストフォレンジックの必要性

従来のデジタルフォレンジック調査の主な課題

- **大量のエンドポイントをどう調査**するか？
  - 数百、数千台のエンドポイントを短期間で調査することは非現実的
- **攻撃の兆候をどのように発見**するか？
  - 従来のフォレンジック調査では、アナリストの経験頼みが大きい
- フォレンジック**調査の速さが被害発生防止**に追いつけるか？
  - 調査中でも、攻撃は継続されている可能性があり、被害につながることも

これらの解決策とは？

「網羅性」と「迅速性」を重視した AI を利用したファストフォレンジックの実施

まず攻撃が起きているのか、範囲はどこまでかを**トリアージ**する	攻撃の原因を把握し、即時対応に利用することで**実害を発生させない**	エビデンスの解析に**AIを利用**することで、多数のエンドポイントに対応	最終的な判断は人間がすることにより、**それぞれの利点を活用**	攻撃の兆候は、**AIが不審な挙動をスコアリング**

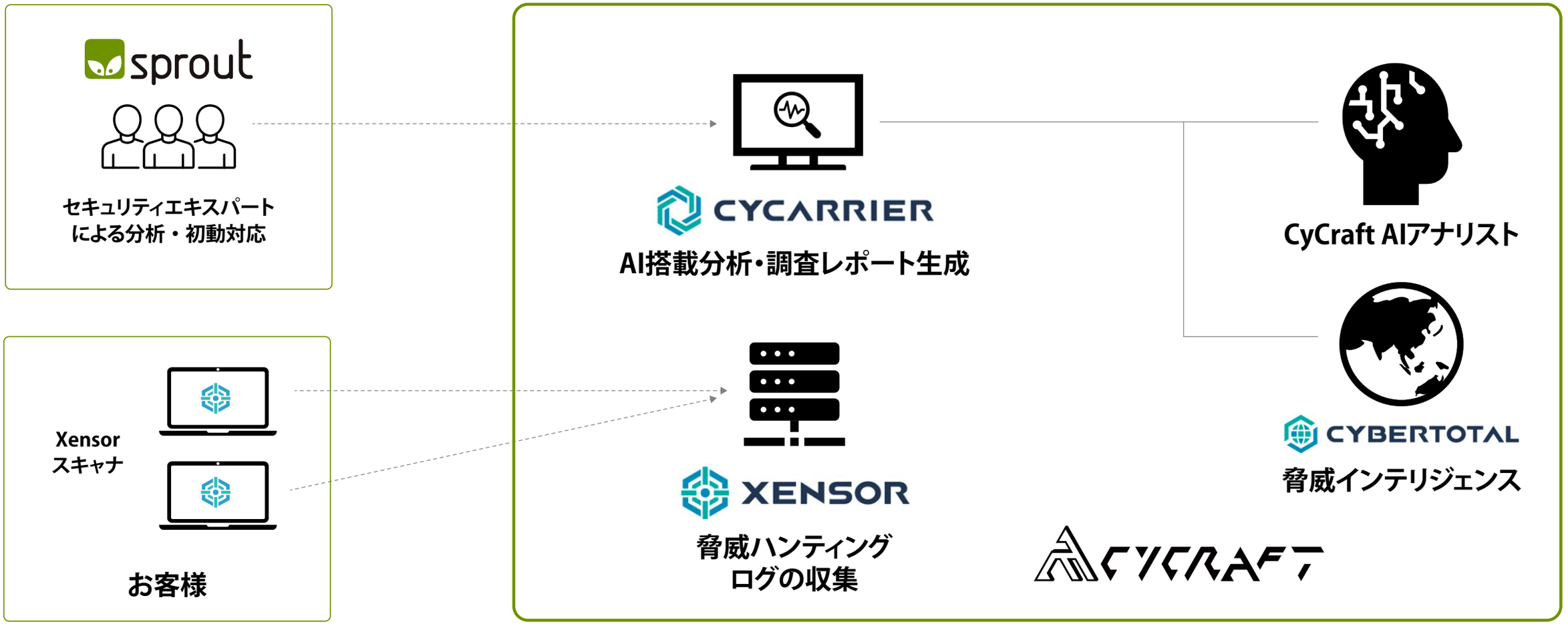
CyCraft AIR ソリューションの特徴

- ファストフォレンジックソリューションとして、台湾に本社を置き世界をリードする AI 情報セキュリティ企業である**CyCraft 社の「CyCraft AIR ソリューション」を採用、迅速性且つ網羅性を確保したファストフォレンジックを提供**します

CyCraft AIR ソリューションの優位性

「迅速性」と「網羅性」を重視したファストフォレンジックソリューション	エンドポイントから収集した情報を元に、**AIを用いたプラットフォームで解析**	エンドポイント間の**水平移動（Lateral Movement）を可視化**	AIが判定した脅威を手掛かりとし、**アナリストによる調査時間の短縮化が可能**	期間・Severityレベルを指定した**調査結果レポートの自動生成が可能**

CyCraft AIR のシステム構成



サービスご提供内容

ヒアリングにて事象の詳細をお伺いした上で、適切な調査・ご支援方法をご提案します

	デジタルフォレンジック		インシデントレスポンス支援
	ファストフォレンジック	ディープフォレンジック	
目的・ゴール	・多数のエンドポイント環境（数百台～数千台）における迅速性を重視した攻撃概要・侵害状況把握 ・ディープフォレンジック実施対象の特定　等	・原因の究明 ・侵入経路の特定 ・不正プログラムの実行痕跡の特定 ・情報漏えいの痕跡把握　等	・被害の最小化、迅速な事象把握を目的とした、有事対応の円滑化
手法	・台湾 CyCraft 社が提供する CyCraft AIR® プラットフォームを使用した調査	・従来のデジタルフォレンジック手法に基づく調査（証拠保全、解析分析、報告）	・ご希望に応じてオンサイト・オフサイトでのご支援を想定
具体的な対応事項	・対象クライアントにインストールする CyCraft 社ツールの提供、インストール成功状況の確認 ・クライアントインストール作業（顧客側での対応） ・全対象クライアントへのインストール完了後、調査・分析作業を実施 ・ファストフォレンジック調査報告書作成、ご提出 ・オンライン報告会の実施（オプション）	・データお預かり・現地データ保全作業（オプション） ・調査・分析作業の実施 ・ディープフォレンジック調査報告書作成、ご提出 ・マルウェア解析の実施（オプション） ・マルウェア解析報告書作成、提出（オプション） ・オンライン報告会の実施（オプション）	・下記対応フェーズ（封じ込め＞根絶＞回復）におけるクライアント先協議機会への参加及び各フェーズ対応策の検討、トリアージ・優先順位付け等の支援 ・具体的にはお客様担当者の補佐となり、経営リスクの観点（二次被害・情報漏洩等の発生有無）も踏まえた優先順位付け、具体策のアドバイザリー提供　等
対象 OS・端末	・Windows、Mac、Linux のパソコン・サーバー	・Windows、Mac、Linux のパソコン・サーバー、外部記憶媒体等	―
提出物	・ファストフォレンジック調査報告書 ・ファストフォレンジックツールにてスキャンが完了したクライアント一覧リスト	・ディープフォレンジック調査報告書 ・マルウェア解析報告書（マルウェア解析オプションご用命時）	・案件ごとご相談に応じて、資料作成のご支援をいたします（経営層向け進捗報告資料、社外向け事象説明資料等）

ご提供価格・サービス開始までの流れ

- 価格につきましては、対応内容・期間などにより変動いたします。詳細なお見積もりについてはお気軽にお問い合わせください
- 各種サービスごと、ご注文からご報告までは、約 4 週間程度での提供が可能です

※ディープフォレンジックの場合

https://sproutgroup.co.jp/

株式会社スプラウト
〒104-0031 東京都中央区京橋3-12-7 GINZA EAST SQUARE 2F