動的リスク管理の時代へ：最新脅威に対応する経営とセキュリティの新戦略

SIGHNT

アジェンダ

1. 近年の脅威背景の変化
2. サイバー攻撃の課題例
3. 従来型のリスク管理の限界
4. 動的なリスク管理の勘所
5. 不確実な脅威への対応
6. まとめ

動的リスク管理の要点

01 脅威情報の活用（情報源の多様化と品質評価）

02 脅威ハンティングとライブフォレンジックの強化

03 脅威検出ルールの動的更新

04 AI/MLの活用と自動化

05 ゼロトラストアーキテクチャの導入

近年の脅威背景の変化

中国の求人情報
攻撃ツール開発経験は就職に有利

- サイバー実戦演習の多い中国ではレッドチームの強化を図る企業が増加
- セキュリティ攻撃ツールの開発経験
  - オープンソースの攻撃ツールが好まれる傾向
  - 改良が容易
  - 追跡回避の観点でメリット

投影のみ

（中国）若年層の失業率上昇の影響？

就職・起業

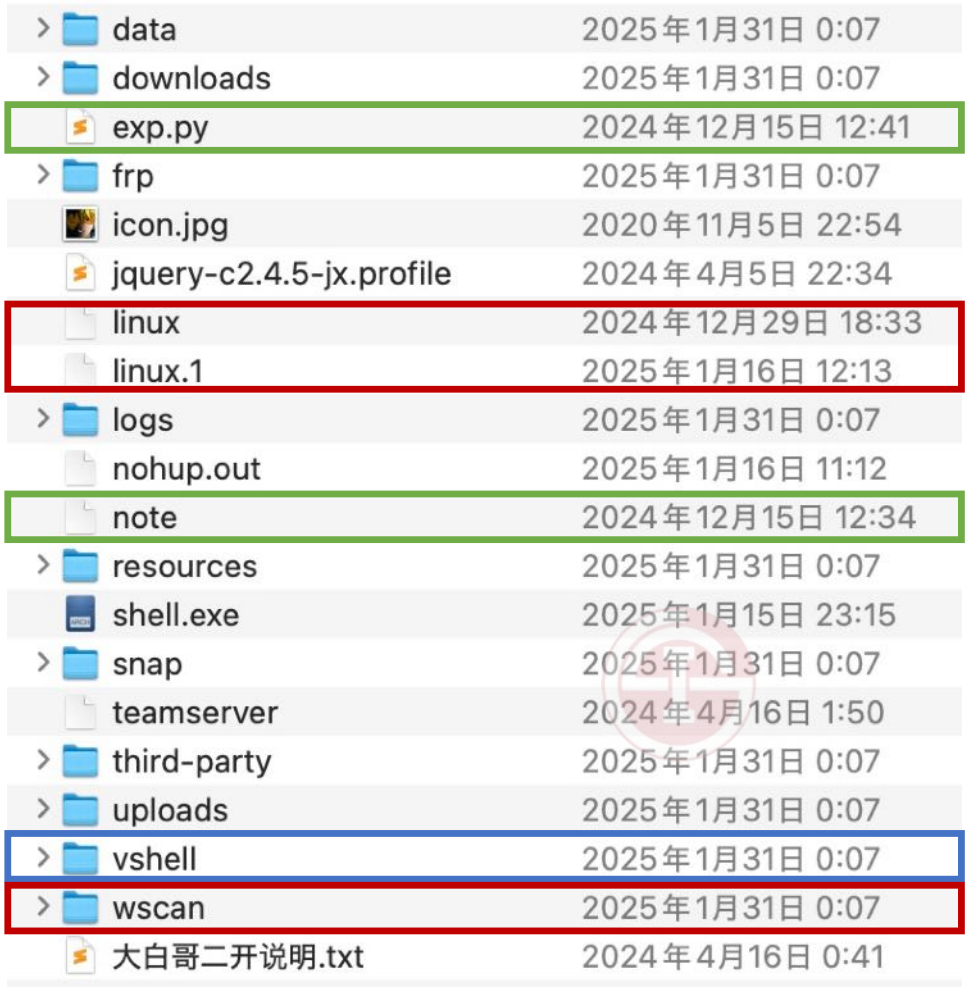
OR

裏社会ギャング

（中国）裏社会ギャングが社会的課題

脅威アクター	標的分野	目的	主な活動
SilverFox （银狐）	銀行・証券 政府・教育 エネルギー	個人情報	フィッシングのほか、WeChatやTelegramを通じて偽のMSIインストーラーを配布し、Gh0st RAT亜種（winos）やAsyncRAT、PC監視ツールのWorkWinを展開。
Leopard （花斑豹）	物流センター 宅配便サイト	速達情報 個人情報	正規の印刷モジュール（MonPrinter）の印刷コンテンツの抽出および送信機能やRustDeskなどのRMMを利用して印刷コンテンツを違法に収集する。Telegramで45億件の漏洩速達情報を根拠とする人物検索ボット「星链」の登場でで注目を集める。
Yellowbird （黄雀）	犯罪グループ	不明	CobaltStrikeを武器として、他の裏社会ギャング系グループに対する攻撃を実施するギャンググループ。
Bobcat （山猫）	・企業の財務部門 ・エネルギー分野の事務部門	情報窃取	税金、請求書を囮として易语言（Easy Programming Language）ベースのローダーとFatalRATを展開。2023 年 10 月 28 日から 11 月 1 日までの 5 日間で、エネルギー、教育、その他の業界に対する爆発的な攻撃を実施し、約 10,000 件のアラートを検知（微步在线）。
Bigpanzi	Smart TV IoT機器	DaaS	ボット化したスマートテレビなどで構成されるP2P型CDN（Pandora-CDN）やAndroid RATのPandoraspearの利用を通じたDDoSやC2などのサービス提供
Dark Mosquito （暗蚊）	IT 運用・ 保守担当者	情報窃取	PHP/JAVA 環境展開ツール （OneinStack）や Linux サーバー環境展開ツール（LNMP）に対するサプライチェーンポイズニング攻撃やSecureCRT、FinalShell、Navicatを装ったマルウェアの展開。
Golden Fox （金相狐）	金融	金融詐欺	バンキングアプリを通じて、顔の生体認証データを含む個人情報や金融情報の窃取。

（中国）とあるC2サーバの構成



「note」のヒープオーバーフローのExploitコード

C2フレームワーク（Cobalt Strike）

教材とみられるアプリケーション

中国製のC2フレームワーク「vshell」

ウェブセキュリティスキャナー / Exploitツール

攻撃の高度化と人材不足の課題

世界全体で約480万人のサイバーセキュリティ専門家が緊急に必要

- アジア太平洋地域：世界的なサイバーセキュリティ人材不足の56%以上を占める
- インド：2023年5月時点で、40,000件のサイバーセキュリティ関連の求人に対して30%が未充足
- アフリカ：14億人の人口に対して、認定セキュリティ専門家はわずか約20,000人
- 米国：サイバーセキュリティ専門家の求人数は50万件以上
- 英国：中小企業の43%がサイバーセキュリティサポートを雇用できない

現在のセキュリティ・スキルギャップ

- 1. AI（34%）
- 2. クラウドコンピューティングのセキュリティ（30%）
- 3. ゼロトラストの実装（27%）
- 4. デジタルフォレンジックとインシデント対応（25%）
- 5. アプリケーションセキュリティ（24%）

参考情報：
https://www.prnewswire.com/news-releases/growth-of-cybersecurity-workforce-slows-in-2024-as-economic-uncertainty-persists-302244585.html

- セキュリティ企業の増加
- 実戦演習の増加
- サイバー協定による攻撃力強化

未認知の脅威の増加

（各国）サイバー人材育成とAI利用を推進

サイバー攻撃の課題例

近年のサイバー攻撃の主な課題

01 未認知の脆弱性（0day）の悪用の増加

02 セキュリティ製品の回避技術の普及

03 正規ツールの利用による横展開

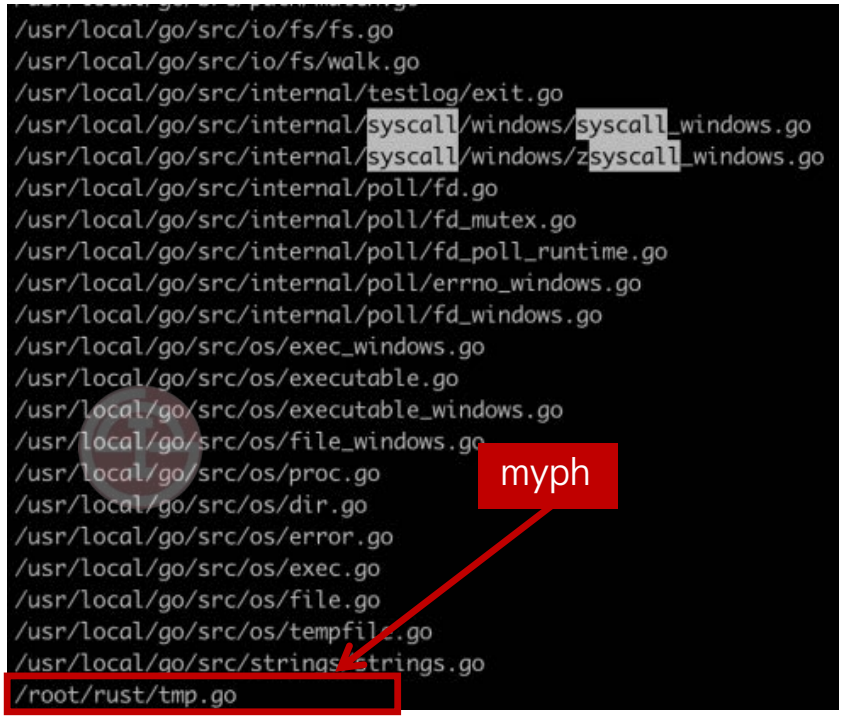
04 資格情報の流出の常態化

05 サプライチェーンを介した攻撃の増加

投影のみ

0dayの積極的な利用

セキュリティ製品の回避ツールの普及

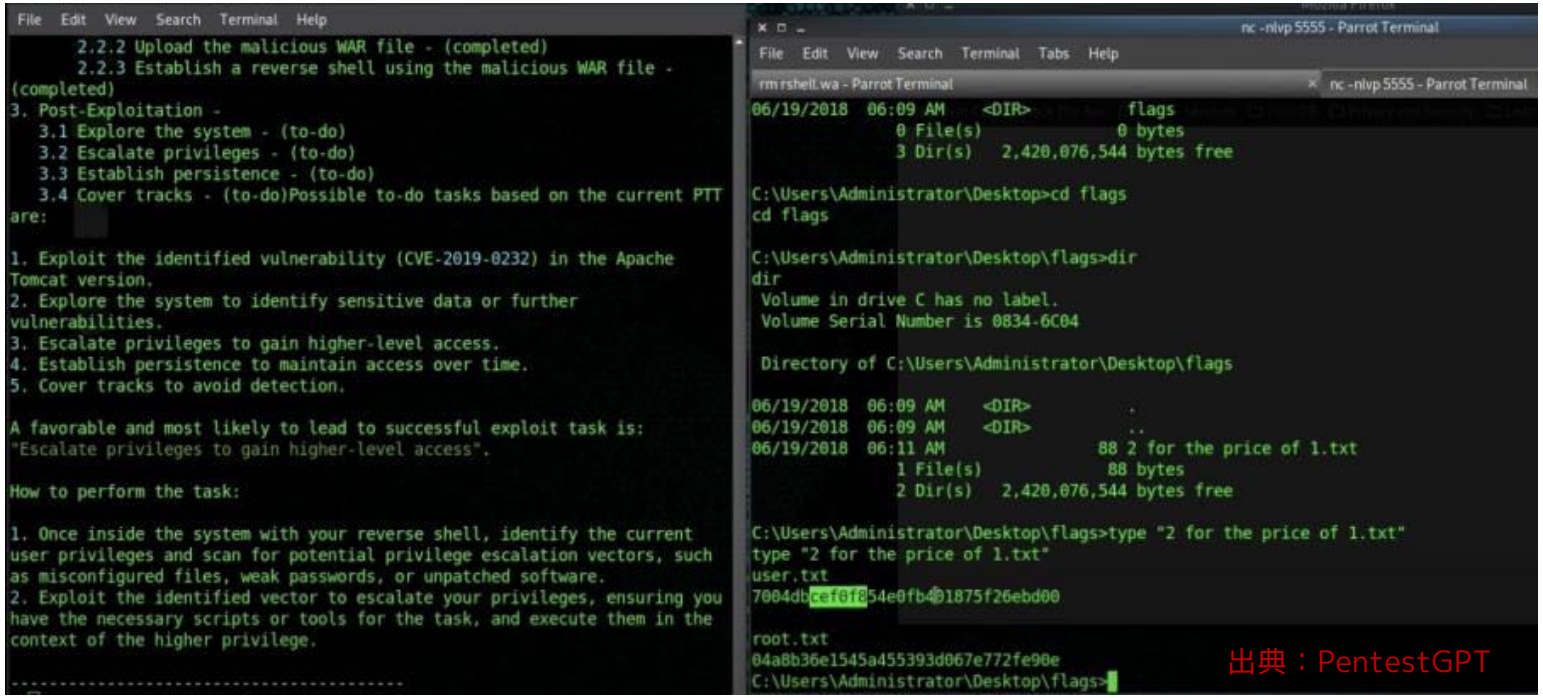


Cobalt Strikeに利用されたmyph例

ツール名	メモ
EDRSandBlast	脆弱な署名済みドライバを悪用してEDRの検出を回避
Killer Tool	イベントトレースの無効化やプロセスハロウィング技術などによりEDRを回避
Mortar Loader	Portable Executable（PE）シェルコードローダー
BypassAV	サイニングやパターンマッチング、挙動検知、サンドボックス分析などの機能を回避・無効化
EDRSilencer	Windows Filtering Platform（WFP）APIを利用
myph	chacha20、Blowfish、XORなどの暗号化方式を使用して、ペイロードを保護、APIハッシュ化
sn0wldrPublic	多様なローディング技術を利用
ZheTian	UAC回避、ユーザー作成、インテリジェントなサンドボックス回避など

AI/MLの利用

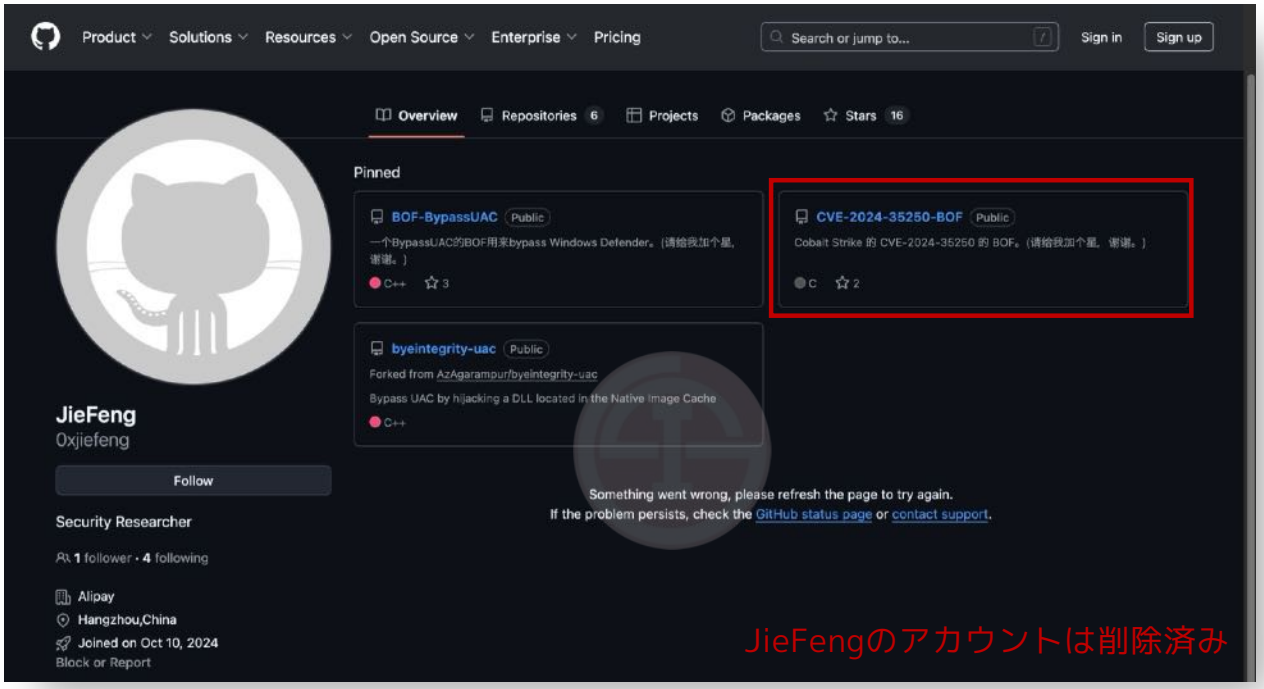
- 機械学習を行う単純な自動化するタイプは2018年頃から登場
- 近年はGPT-4など高度な大規模言語モデル（LLM）による推論能力を活用し、複雑なセキュリティシナリオでも次に取るべき最善策を提案



出典：PentestGPT

GitHubポイズニング

レッドチームが利用するツールをforkし悪性コードを混入



中国の研究者が報告した攻撃手法を利用

- ベトナムの脅威アクターと言われている。
- Cobalt StrikeのBeacon Object Fileに悪性コードを混入
- セキュリティ専門家や担当者などがVisual StudioでProjectを読み込むと、悪性コードが実行される。（EvilSln）

AIの出力へも影響

投影のみ

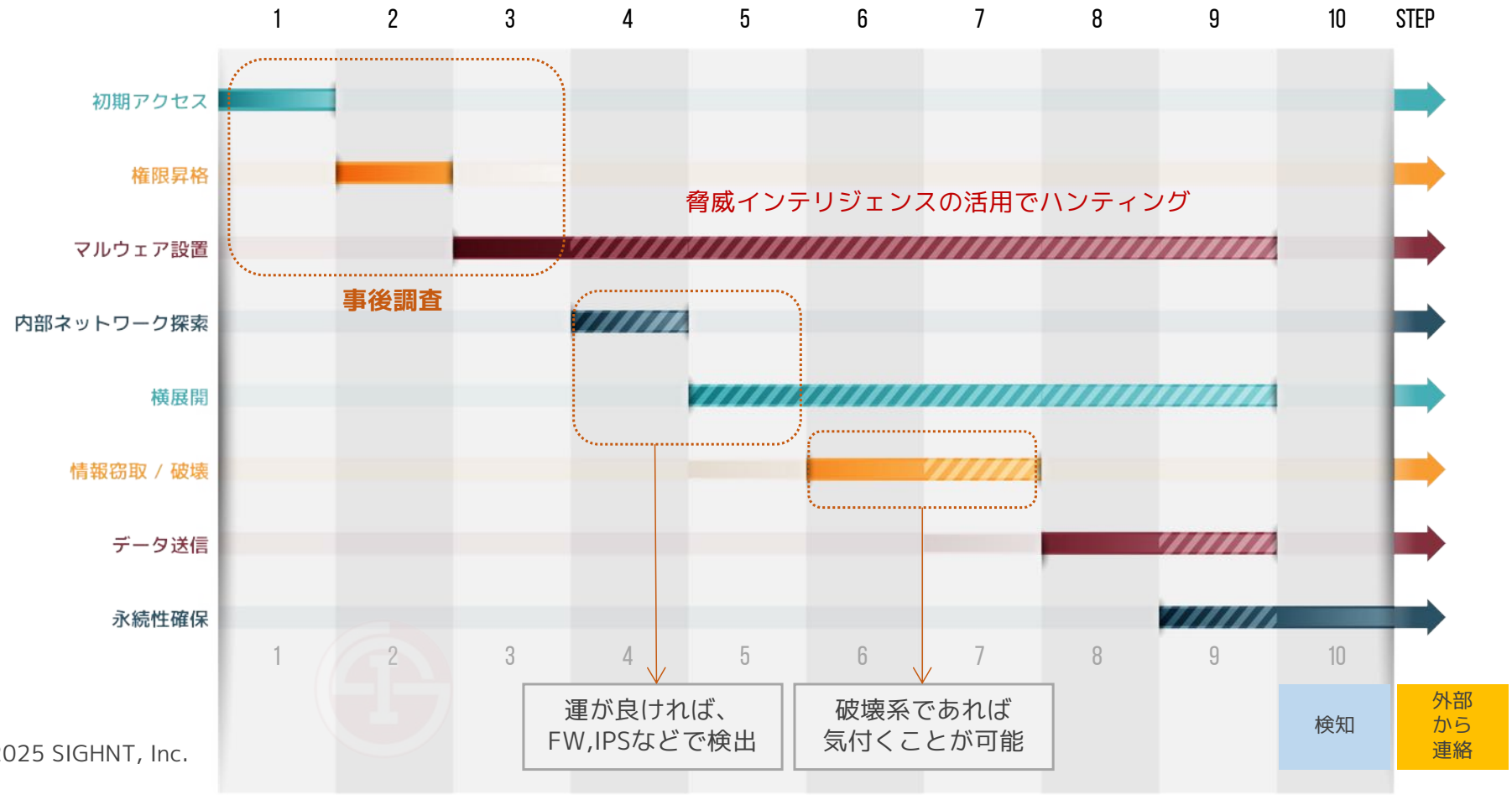
従来型のリスク管理の限界

予防的対応の困難な脅威への対応

一般的なセキュリティ運用の流れ

情報収集と監視	脆弱性管理	インシデント対応	セキュリティ運用の継続的改善	コンプライアンスと報告
● 継続的モニタリング ➢ ネットワークトラフィック ➢ ログファイル ➢ 脅威情報フィード ➢ エンドポイント、アプリケーション	● 未認知の脆弱性管理 ➢ 公開情報 ➢ アンダーグラウンド ➢ 0-day情報フィード ➢ 各国独自情報	● 管理プロセス ① 検知 ② 分析 ③ 封じ込め ④ 排除 ⑤ 復旧 ⑥ 報告 ⑦ 教訓化	● 運用品質の向上 ➢ 手順書の整備と更新 ➢ チームの教育とスキル向上 ➢ KPIによる運用評価と改善 ● 自動化の推進 ➢ ツールの統合 ➢ ワークフロー自動化 ➢ レポーティングの効率化	● 影響範囲の報告 ➢ 情報流出の状況 ➢ 侵害範囲 ➢ 初期侵入の原因
● 脅威情報の活用 ➢ 公開情報の収集 ➢ 外部脅威フィード ➢ 攻撃動向分析 ➢ 手口の把握 ➢ 攻撃準備段階の把握	● 脆弱性ライフサイクル管理 ① 資産の把握と優先順位付け ② 脆弱性評価とリスク分析 ③ 対応優先順位付け ④ 修正計画の策定と実施 ⑤ 対策の有効性確認	● フォレンジック ➢ HDD/SSD/Flash ➢ メモリ ➢ ファイル解析 ➢ OS ➢ ネットワーク ➢ クラウドストレージ	● 検出ルールの生成 ➢ IDS/IPS ➢ Yara ➢ ClamAV ➢ Sigma	● コンプライアンスと報告 ➢ セキュリティポリシーの遵守状況確認 ➢ 規制要件への対応 ➢ 経営層への報告

未認知の脅威増加による影響

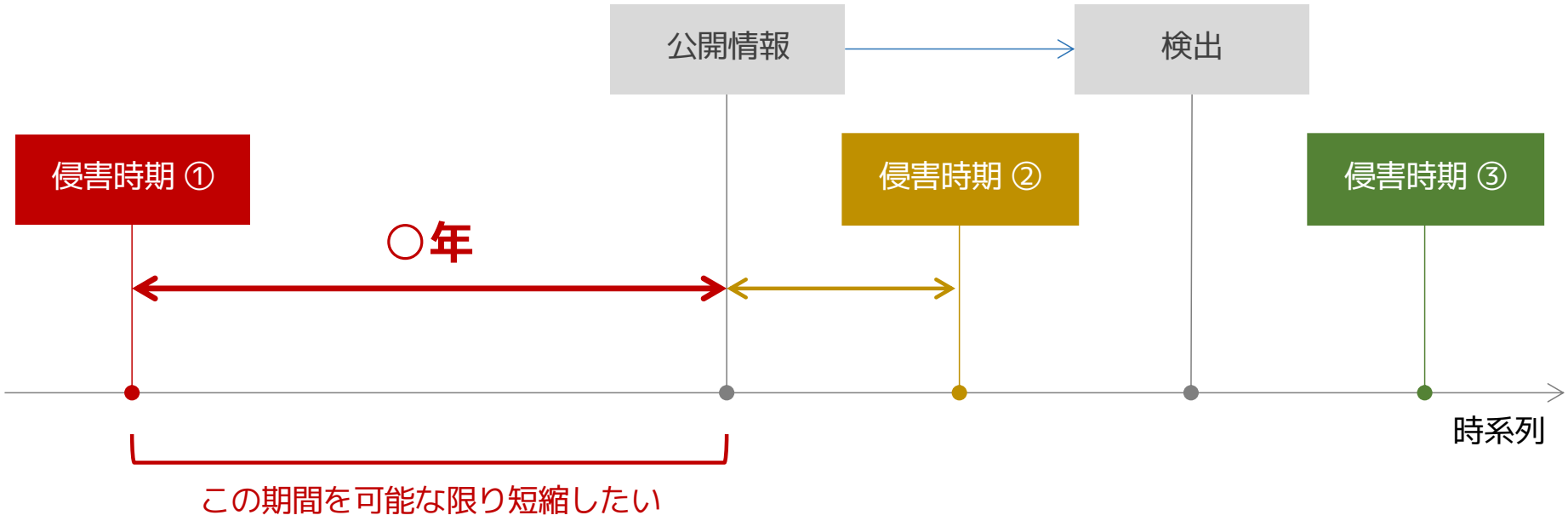


公開情報に対する初期対応例

情報の対象時期	脅威の種類	初期対応例	その他の評価例
現在	脆弱性	修正プログラムの適用	設定による回避の有無
	マルウェア	IoC、ログの確認	標的地域、開発地域
	攻撃ツール	ログの確認	自組織内での実行可否
	新規攻撃手法	実現性の評価	自組織内での実行可否
過去	脆弱性	悪用の調査	対象製品の有無
	マルウェア	通信ログの確認	EDR/XDRの確認
	攻撃ツール	悪用の調査	ログの確認
	新規攻撃手法	悪用の調査	ログの確認

動的なリスク管理の勘所

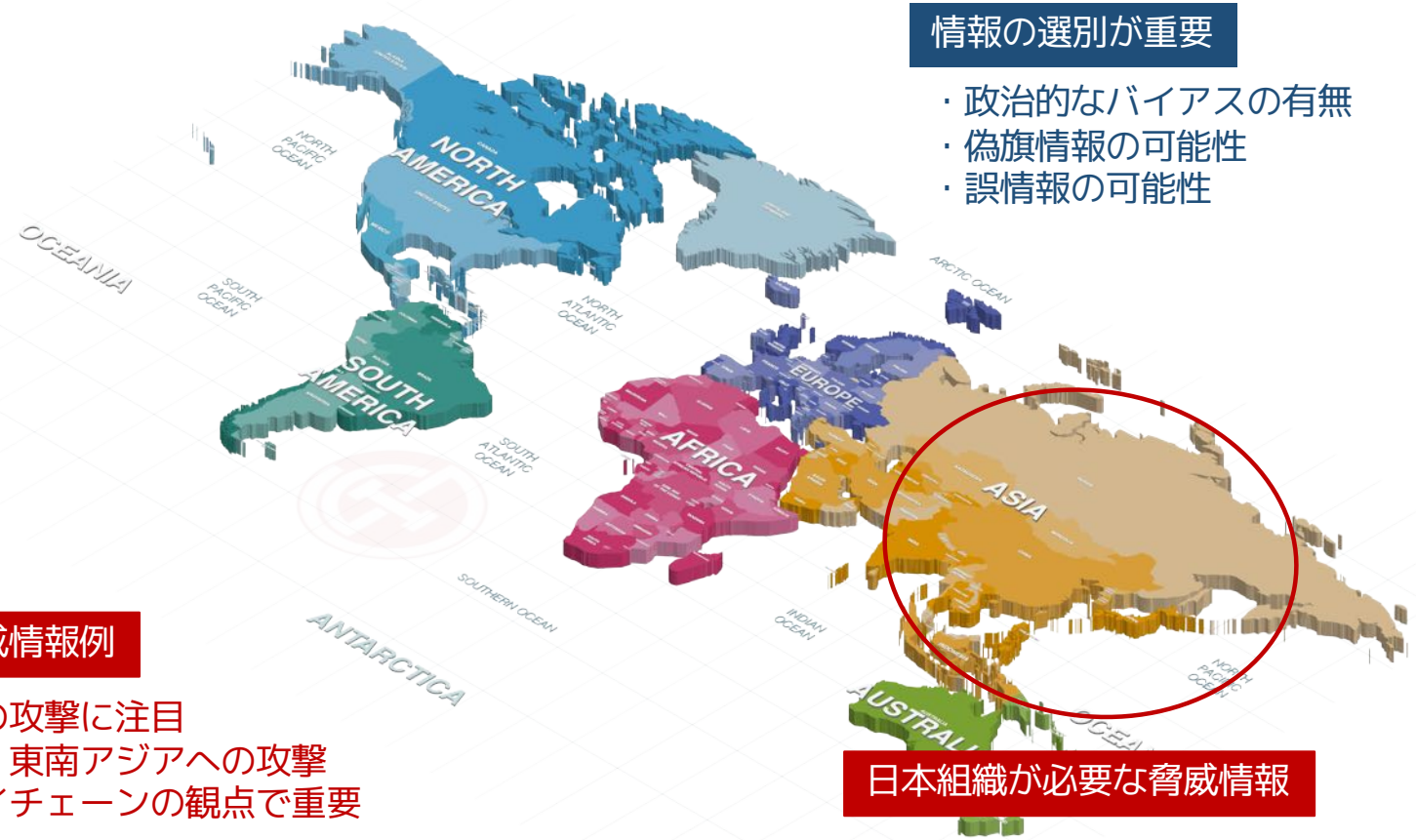
（要検討）脅威情報の一般的な課題



日本組織に必要な脅威情報の選別

情報の選別が重要

・政治的なバイアスの有無
・偽旗情報の可能性
・誤情報の可能性

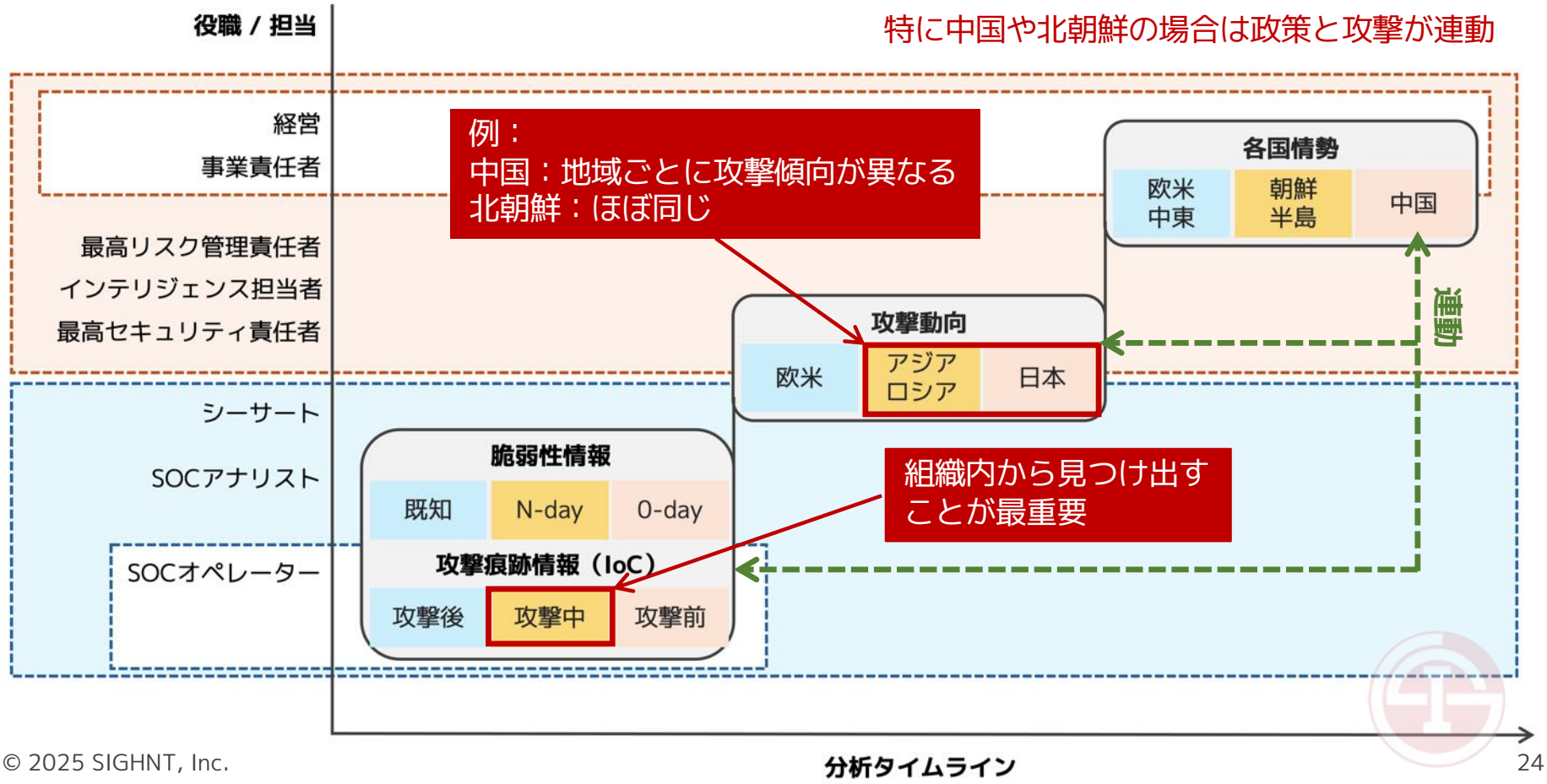


注目すべき脅威情報例

・日本企業への攻撃に注目
・台湾、韓国、東南アジアへの攻撃
情報はサプライチェーンの観点で重要

日本組織が必要な脅威情報

安保の観点で把握すべき脅威情報



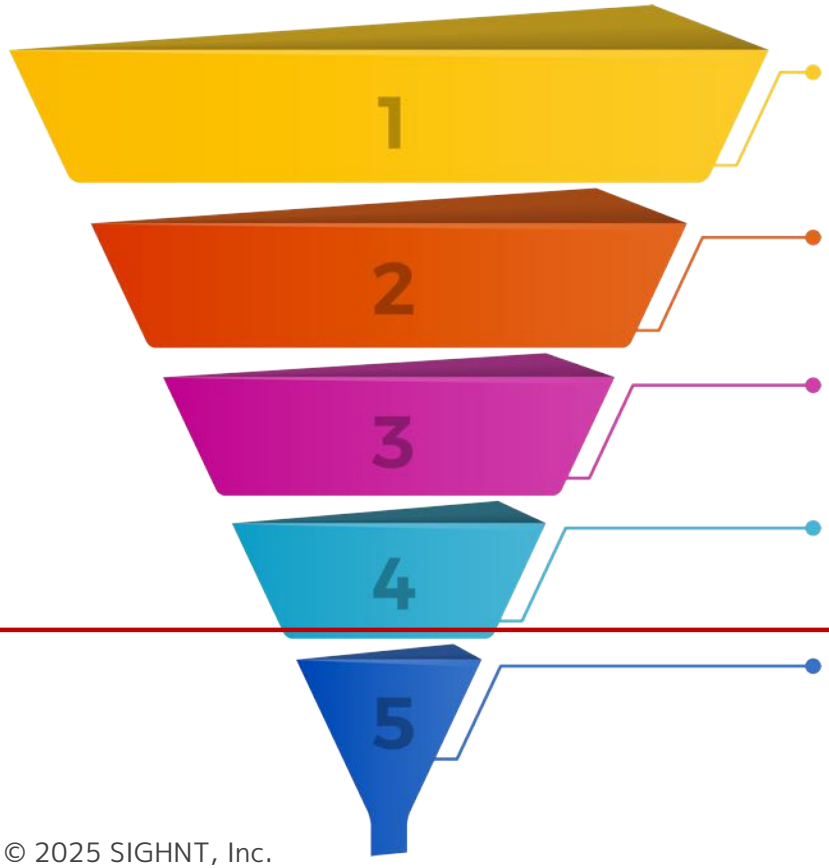
（経営層）グローバルリスクから把握

例：中国の卡脖子35項目

コアパーツ	キー・基礎材料	先進基礎技術	産業技術基礎
マイクロチップ	ITOターゲット材	フォトリソグラフィ	オペレーティングシステム
航空機エンジンナセル	航空機用受鋼材	真空蒸着機	iCLIP技術
触覚センサー	高級軸受鋼	産業用コア・ソフトウェア	大型燃焼ガスタービン
携帯電話用RF装置	フォトレジスト	航空機設計用ソフトウェア	耐空規格
LIDAR	マイクロスフェアー		コアアルゴリズム
ハイエンドコンデンサ・抵抗器	燃料電池のキー材料		高圧コモンレールシステム
フライスカッター	リチウム電池用ダイアグラム		透過型電子顕微鏡
高圧ピストンポンプ	超精密研磨加工		データベース管理システム
掘削機（ロードヘッダー）主軸受	エポキシ樹脂		走査型電子顕微鏡
水中コネクタ	高強度ステンレス鋼		
ハイエンド溶接電源			
医療用画像機器部品			

（運用）事業リスク観点での管理が前提

多くの大規模事案の要因



“不要”なネットワークトラフィックの制御
ネットワーク範囲,IPアドレス,プロトコル,特定地域,通信量,etc

“不要”なデータの制御
コンテンツ（メール,ウェブ）,プロキシ,機密情報,etc

“不要”なアプリケーションの制御
SNS,ストリーミング,ゲーム,クラウドストレージ,
不要なプロトコル,リモートアクセスツール,etc

“不要”なアクセスの制御
ロールベースアクセス制御,管理者権限,外部記憶媒体,etc

“悪意”ある活動の検出と遮断
異常ログイン,過剰トラフィック,Exploit,C2通信,
ファイル改竄,フィッシング,データ漏洩,etc

不確実な脅威への対応

不確実な脅威情報への対応

投影のみ

非公開の脅威情報の入手

投影のみ

システムの根本課題への対応

```
function Invoke-DrycberETW {
    param (
        [int]$ProcessId
    )

    # Define required Win32 API functions
    $kernel32 = Add-Type -Name 'Win32ETW' -Namespace 'Drycber' -MemberDefinition @"
        [DllImport("kernel32.dll", SetLastError = true)]
        public static extern IntPtr OpenProcess(int dwDesiredAccess, bool bInheritHandle, int dwProcessId);

        [DllImport("kernel32.dll", SetLastError = true)]
        public static extern bool WriteProcessMemory(IntPtr hProcess, IntPtr lpBaseAddress, byte[]
        lpBuffer, uint nSize, out int lpNumberOfBytesWritten);

        [DllImport("kernel32.dll", SetLastError = true)]
        public static extern bool CloseHandle(IntPtr hObject);
```

ETW (Event Tracing for Windows) の無効化
※EDRソリューションなどのセキュリティ製品の検知基盤が無効化されることになる。
加えて、**AMSI (Anti-Malware Scan Interface) も無効化**することにより、スクリプト言語で作成されたマルウェアの検出が無効化される。

まとめ

01 **未認知の脅威の増加**
0day脆弱性、新型マルウェア、セキュリティ製品の回避技術などの増加

02 **不確実な脅威の抽出と先行対応**
リアルタイムの脅威情報から対応すべき脅威を不確実なものを含めて選定

03 **動的リスク管理が必要な時代**
脅威ハンティングを含めた攻めのセキュリティ運用により未認知の脅威の炙り出し

THANK YOU