サイバーインテリジェンスが事業継続にもたらすもの

脅威インテリジェンスを正しく理解し、活用するために

株式会社マキナレコード
代表取締役 軍司祐介

MACHINA RECORD
Cyber Threat Intelligence

禁複製・再使用・転用

自己紹介

株式会社マキナレコード　代表取締役 軍司祐介

エンジニアのキャリアを経て、セキュリティ専門家としてヤフー株式会社、株式会社ミクシィ、楽天株式会社などでセキュリティ向上に寄与する。各組織で CSIRT チームの構築や、M&A 時のデューデリを含む各種アセスメント、セキュリティ施策の設計・運用など、セキュリティ分野において20年以上の経験を持つ。

2015年にサイバーインテリジェンスに出会い強い感銘を受け、日本においても広めていく決意を持ってマキナレコードを創業。

共同著書紹介

販売ページ(Amazon)
348頁/4,180円

サイバーセキュリティ対応の企業実務

平時・有事における組織的・法的対策の進め方

企業のサイバーセキュリティ対策につき最低限押さえておくべきこと、平時・有事それぞれの組織的・法的対応(国内・海外)を詳説。多発するランサムウェアインシデントへの対応をケースで解説。

杉山　一郎(編著)・寺門　峻佑(編著)

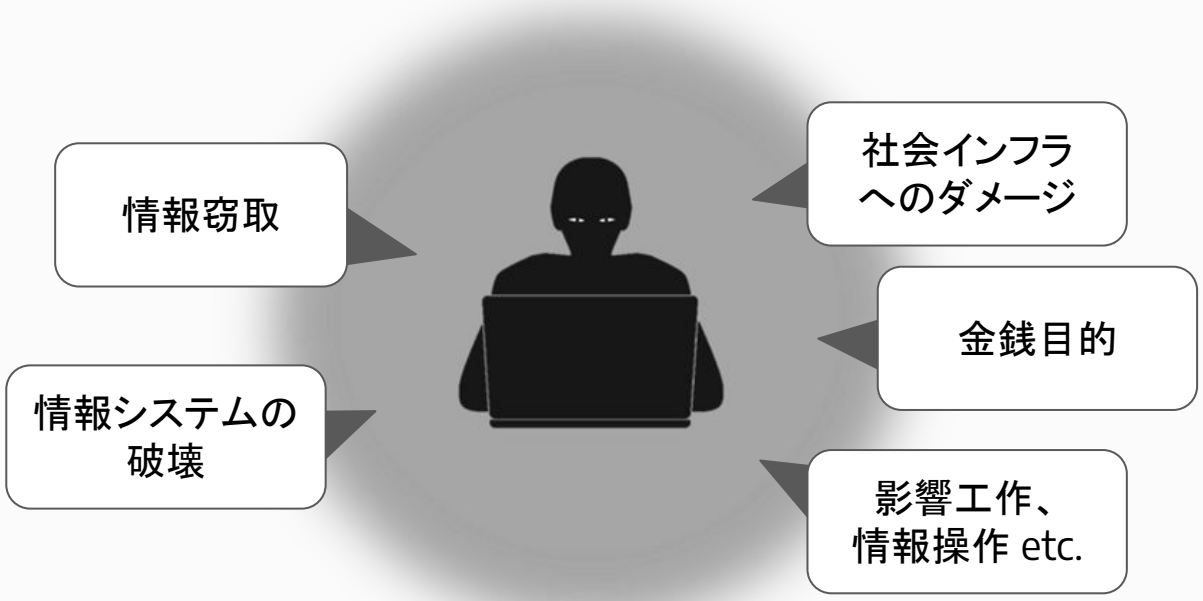
－ 著者一覧 －

前田　典彦：株式会社FFRIセキュリティ 社長室長
軍司　祐介：株式会社マキナレコード 代表取締役
茂岩　祐樹：freee株式会社 常務執行役員CISO兼エンジニアリング基盤本部長
小出　洋　：九州大学情報基盤研究開発センター 教授

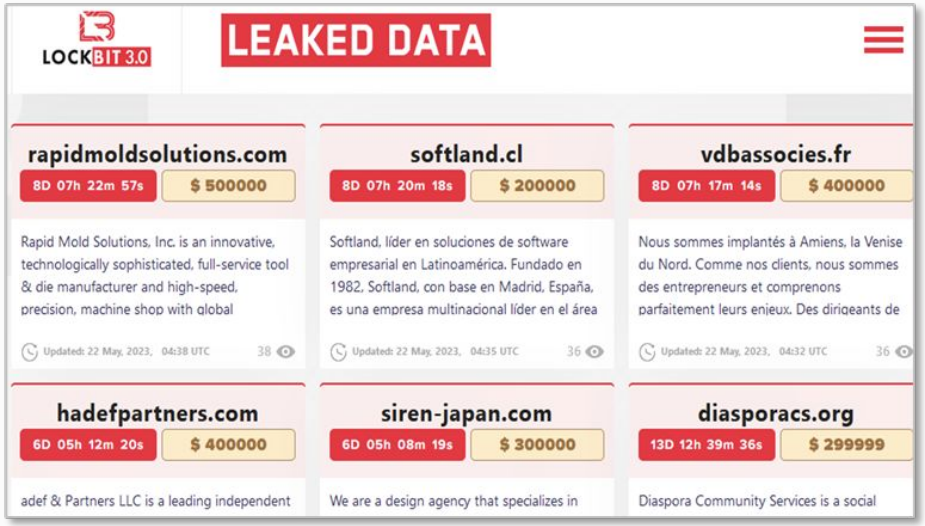
前説

攻撃は日々進化し、コモディティ化している

アクターの動機・意図



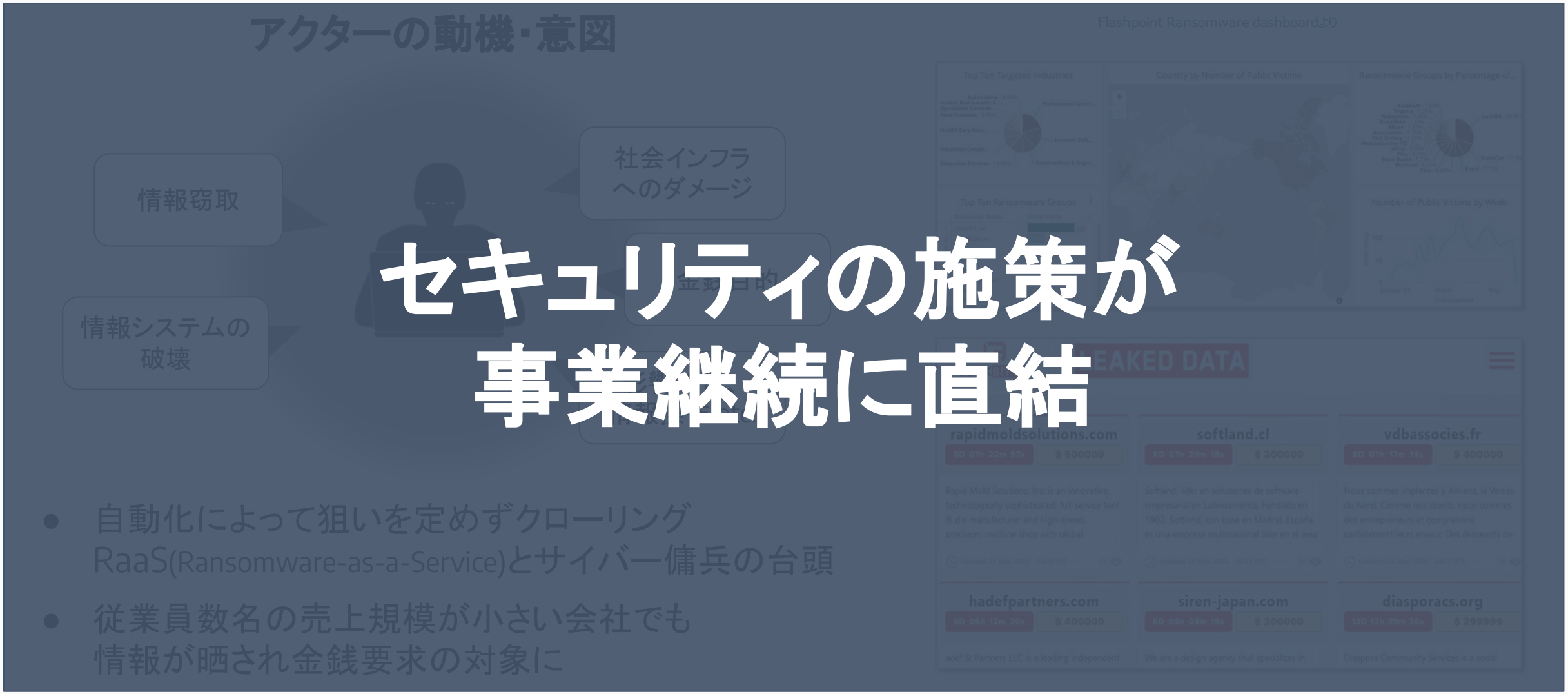
Flashpoint Ransomware dashboardより



- 自動化によって狙いを定めずクローリング
  RaaS(Ransomware-as-a-Service)とサイバー傭兵の台頭
- 従業員数名の売上規模が小さい会社でも
  情報が晒され金銭要求の対象に

攻撃は日々進化し、コモディティ化している

攻撃は日々進化し、コモディティ化している



セキュリティの施策が事業継続に直結

- 自動化によって狙いを定めずクローリング
  RaaS(Ransomware-as-a-Service)とサイバー傭兵の台頭
- 従業員数名の売上規模が小さい会社でも
  情報が晒され金銭要求の対象に

いままでのセキュリティ施策における限界と課題

既存のセキュリティの役割

チーム	役　割
セキュリティ （施策検討）	●組織全体のポリシーの策定・ セキュリティマネジメントの運用 ●脅威の洗い出し・特定 ●対策の検討と実施
セキュリティ （Red/Blue/Purple）	●技術的な脆弱性の発見・ 防御施策の検討
SOC	●攻撃の検知
CSIRT	●インシデントハンドリング

課題

- 一向に攻撃は減らない
- 適切な予算と人員に正解が見つからない
- 事業を拡大すればするほど、攻撃される可能性が高まる
- 扱う情報は増え続ける
- 法的な要件も増える
- サードパーティをどこまで管理するべきか
- 政治情勢や軍事活動がサイバーに大きな影響
- 経営層と現場の認識に大きなギャップ

経営者、現場担当者、それぞれの立場において
考えないといけないことが多すぎる・・・

サイバーインテリジェンスとは

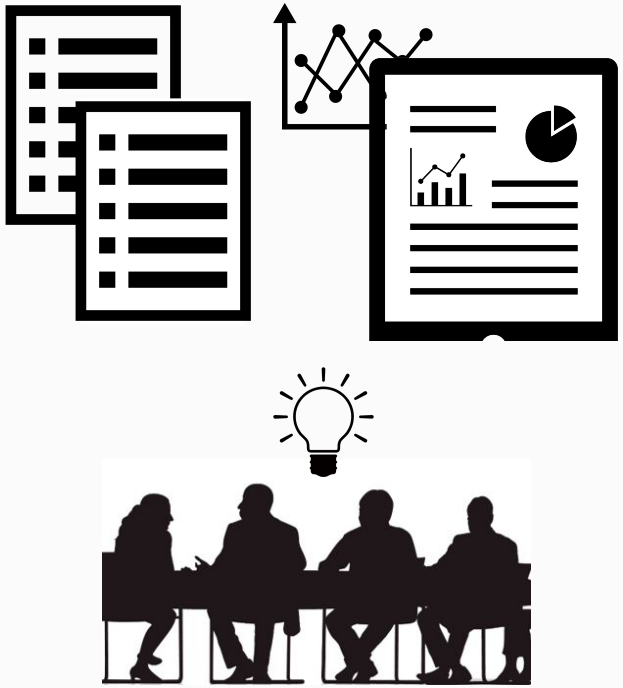
情報とインテリジェンスの違い

生データ・情報

よくわからない
意思決定の支援にならない

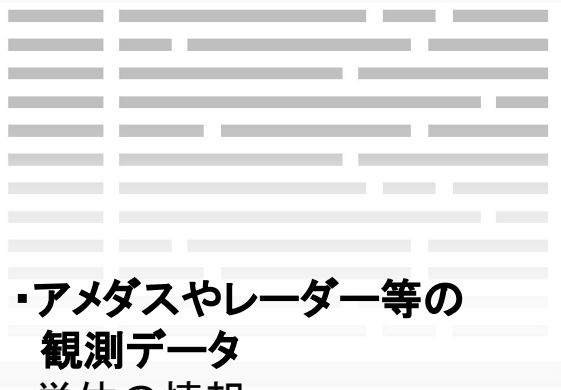
≠

完成されたインテリジェンス

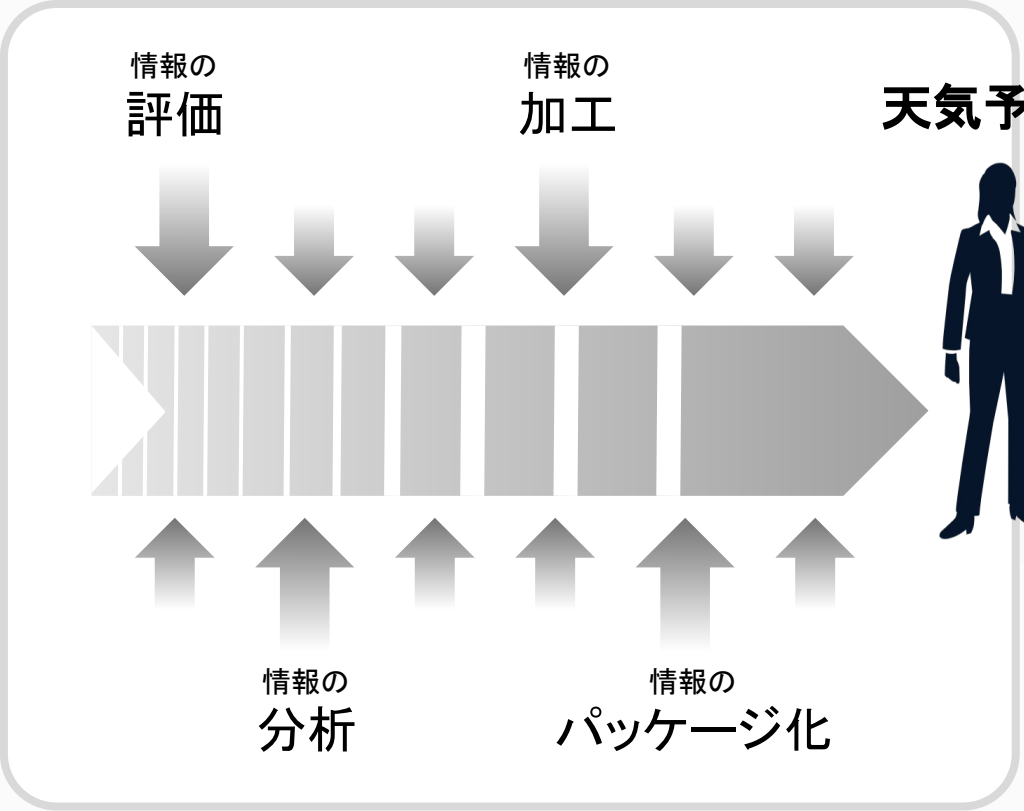


理解できる、評価済である
＝意思決定を支援できる

身近なインテリジェンスの例『天気予報』



・アメダスやレーダー等の
観測データ
・単体の情報
・収集済みだが未評価



天気予報士

降水確率予報

ピンポイント降水予報

週末天気予報

**そのままでは意思決定が
難しい生データ・情報**

**意思決定を支援できる
完成されたインテリジェンス**

インテリジェンスの定義

What - 何を？ | Why - なぜ？ | How - どうやって？

サイバー（脅威）インテリジェンスの役割

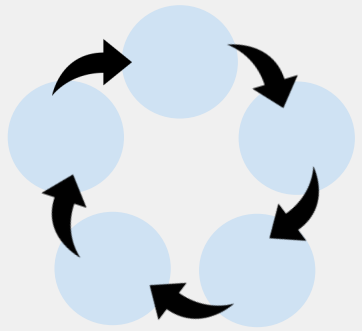
脅威の特定
↓
情報収集
↓
分析
↓
意思決定
↓
対策

インテリジェンスとは

意思決定を円滑に行うための支援的役割

- 意思決定者あるいはクライアント（オーディエンス）に提示するための、わかりやすく効果的なレポートを書く、またはアウトプットを提供すること
- インテリジェンスを強化する上で、根本的な目的が損なわれないよう、チームの役割を理解しなければならない

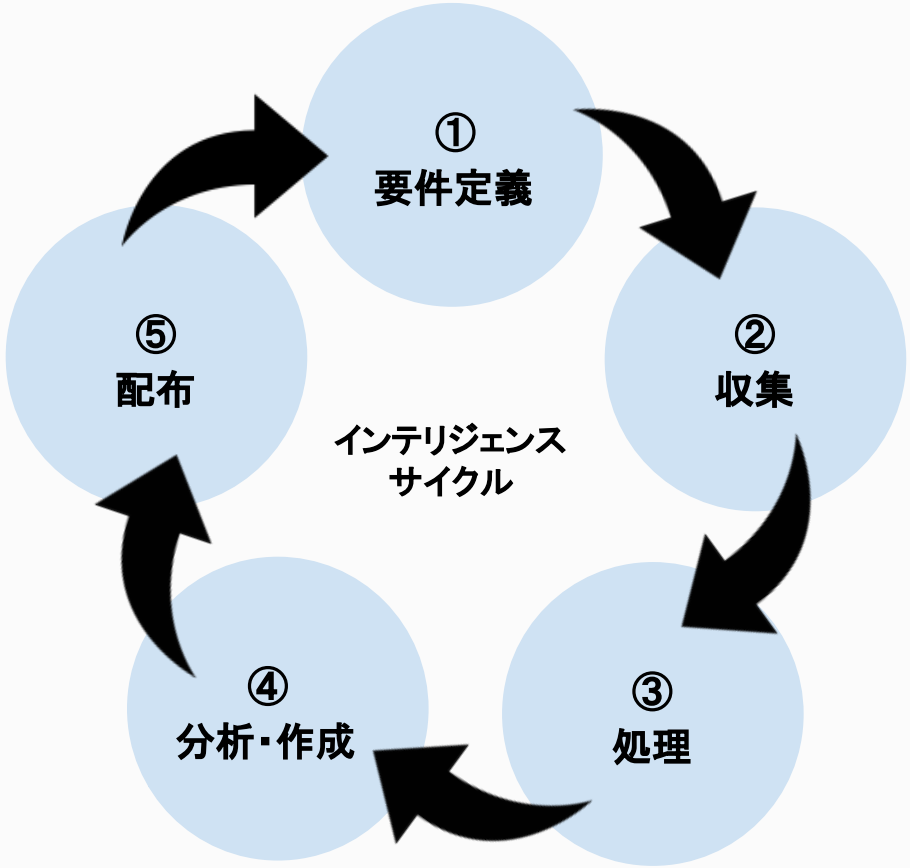
効果的なレポートを作成するためには
業界基準のプロセス
インテリジェンス・サイクル



を使用する必要がある

インテリジェンスの実行「インテリジェンスサイクル」

効果的なインテリジェンスレポート作成のための標準インテリジェンスプロセス



① 要件定義	オーディエンス（インテリジェンスの提供を受ける意思決定者）を理解
② 収集	ソース選択とデータ・情報収集
③ 処理	収集した情報を分析可能な形に処理
④ 分析・作成	インテリジェンスへの変換
⑤ 配布	オーディエンスへの提供とフィードバック

要件定義（プランニング）の意義

意思決定を円滑に行うための支援的アウトプットを行うためには

「意思決定者が何を求めているのか」
を明らかにすること

What
なにを
知りたいのか

Who
誰が
必要としているの
か

Why
どうして
必要なのか

How
どんな
フォーマットで
提供を
受けたいか

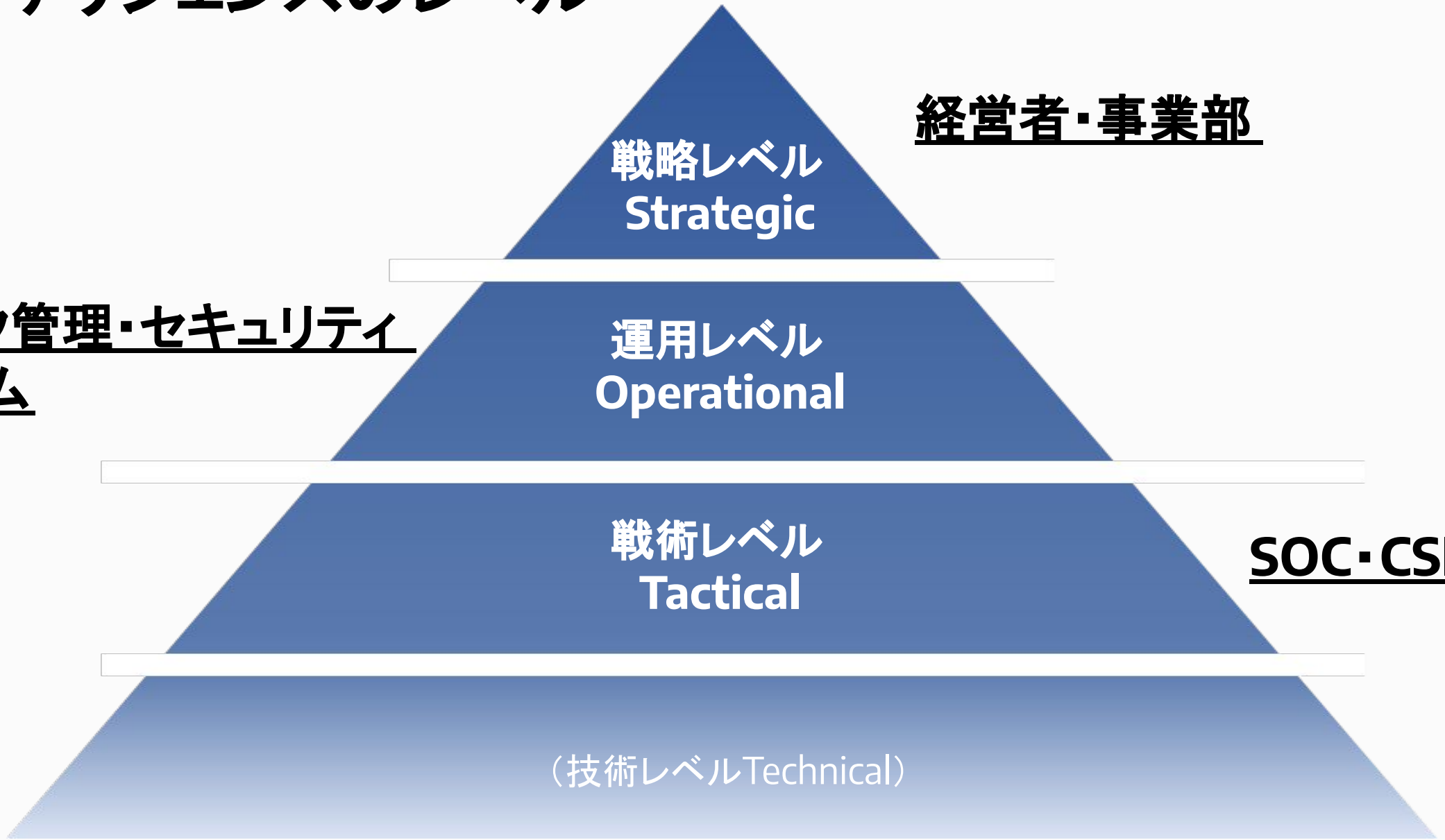
When
いつ、
どれくらいの
頻度で提供
してほしいか

**ここがインテリジェンスを
やる上で、最重要ポイントです。**

要件定義を疎かにすると、不要な仕事が
増えるだけでなく、本質の情報が
オーディエンスに届かなくなり、
意思決定がスムーズに行われなくなります。
ひいては、インテリジェンスの価値が
損なわれることになります。

⇨ 意思決定を促す、Actionableなインテリジェンスを提供する

インテリジェンスのレベル



経営者・事業部

リスク管理・セキュリティチーム

SOC・CSIRT

サイバーインテリジェンス概略

サイバーインテリジェンスが事業継続にもたらすもの

Priority Intelligence Requirement

事業継続に必要なセキュリティ要件のカテゴリ（ ※詳細）

- インサイダー脅威
- エクスプロイトキットとマルウェア
- サプライチェーンリスク
- データ侵害の影響
- なりすましとフィッシング
- 競合他社の動向
- 脅威アクターとグループ
- 脅威アクターとマルウェアの動向
- 業界の技術動向
- 経営リスク
- 攻撃手法の動向
- 詐欺とマネーロンダリング
- 自然災害と健康リスク
- 情報漏洩と露出
- 脆弱性の動向
- 大規模な侵害と攻撃
- 地政学的リスク
- 敵対者の目的とTTP
- 法規制と政策

- 経営者
- CISO
- リスク管理
- セキュリティチーム
- SOC
- 人事
- 購買管理
- マーケティング
- 事業管理
- CSIRT

それぞれの担当が適切に情報を収集し、分析し、求められた問いに答えられるように常に準備しておくことが必要。

・・・現実的にできるのか。必要なことは理解できるが、リソースや専門性からおざなりになり、**意思決定にまで繋げられない** のではないか

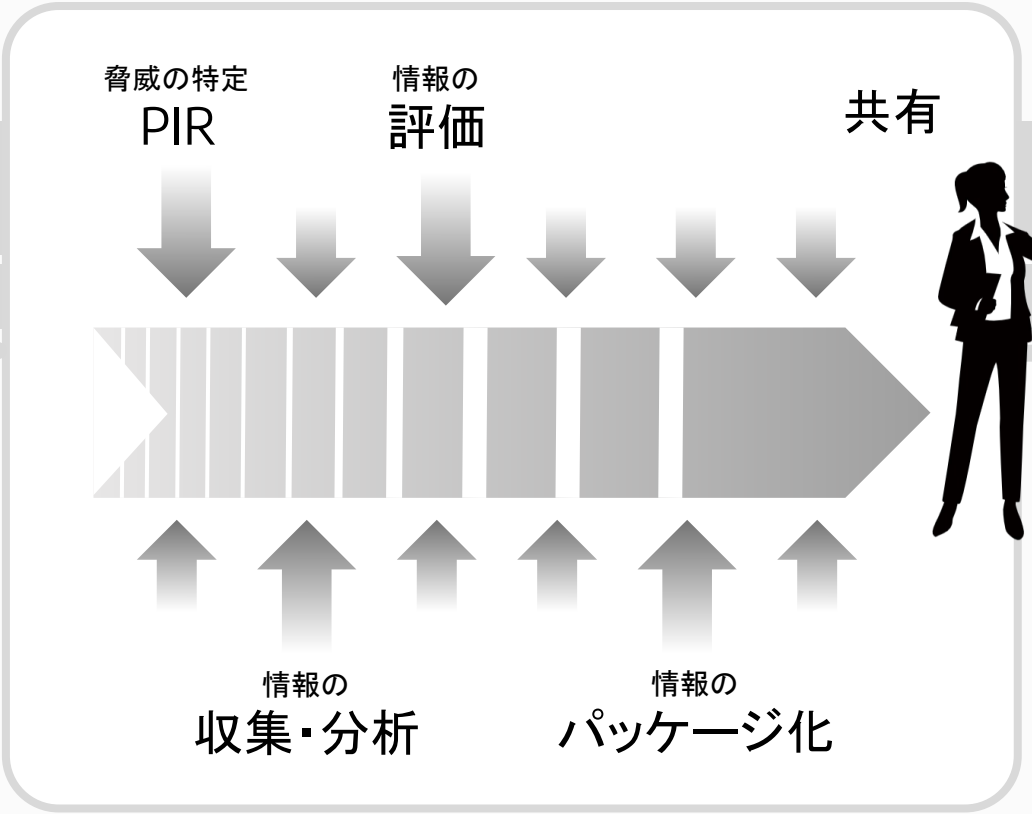
インテリジェンスはセキュリティチームの価値を増大

セキュリティチーム

セキュリティ（施策検討）	セキュリティ（Red/Blue/Purple）
SOC	CSIRT

レポート

それぞれが異なる粒度
リソースの重複・迷子



セキュリティチームの強化

セキュリティ（施策検討）	セキュリティ（Red/Blue/Purple）
SOC	CSIRT

レポート

理解できる、評価済である
＝意思決定を支援できる

インテリジェンスはセキュリティ戦略の意思決定を支援

- 脅威とリスクの洗い出し、言語化、可視化
- 経営層と現場の問題認識の乖離を埋める
  戦略決定や問題認識のためのコミュニケーションを圧倒的に増加させる
- 攻撃者の思考や手段を理解する
- 膨大な情報の中から、本当に必要な情報を見つけ出し、
  分析する能力と、適切にそれを報告する能力を身につける
- 実行するための予算・人員のリソースを **適切に** 確保する

インテリジェンスをチームで取り組むメリット

一概に情報収集や分析と言っても、専門性がそれぞれ異なる。
アウトプットも応じて異なる。

- Strategic、Operational、Tactical
- ダークウェブ等からTTPに関するもの
- 認証情報やクレジットカード番号
- 脆弱性情報やPoC、マルウェアに関する情報
- IPアドレスやHashといったIOC関連の情報
- 地政学や、物理的なセキュリティに関連する情報も（サイバーとは異なる）

- **情報収集**
- **分析**
- **レポーティング**

に特化した専門チーム

「インテリジェンス」という
カテゴリで統一見解を持ち、
分析を実施する。

- 情報の粒度の標準化
- 技術～事業戦略まで広範囲にわたるリスクの可視化
- 高度化したAI x 専門家の経験値 = ∞
- 意思決定者が活用できるActionable インテリジェンス

マキナレコードで支援できること

1. **インテリジェンスに関するコンサルティング**
   - チームビルディング
   - 適切な予算配分
2. **よりよいインテリジェンスを作成するためのトレーニング**
   - インテリジェンスの定義～ハンズオン
3. **最先端のインテリジェンスサービスの導入支援**
   - ダークウェブ監視、アクターエンゲージ
   - OSINT
   - IOC分析
4. **インテリジェンスの作成支援**
   - マネージドサービス
   - レポート作成、監視
5. **翻訳支援**

PRODUCTS
主な活用プロダクト

FLASHPOINT
ANOMALI
Silobreaker
Recorded Future
VulnDB
SILENT PUSH

MACHINA RECORD
Cyber Threat Intelligence

ご静聴、ありがとうございました

MACHINARECORD.COM

東京都港区虎ノ門1-2-15 YSビル6F
info@machinarecord.com
03-6550-9630