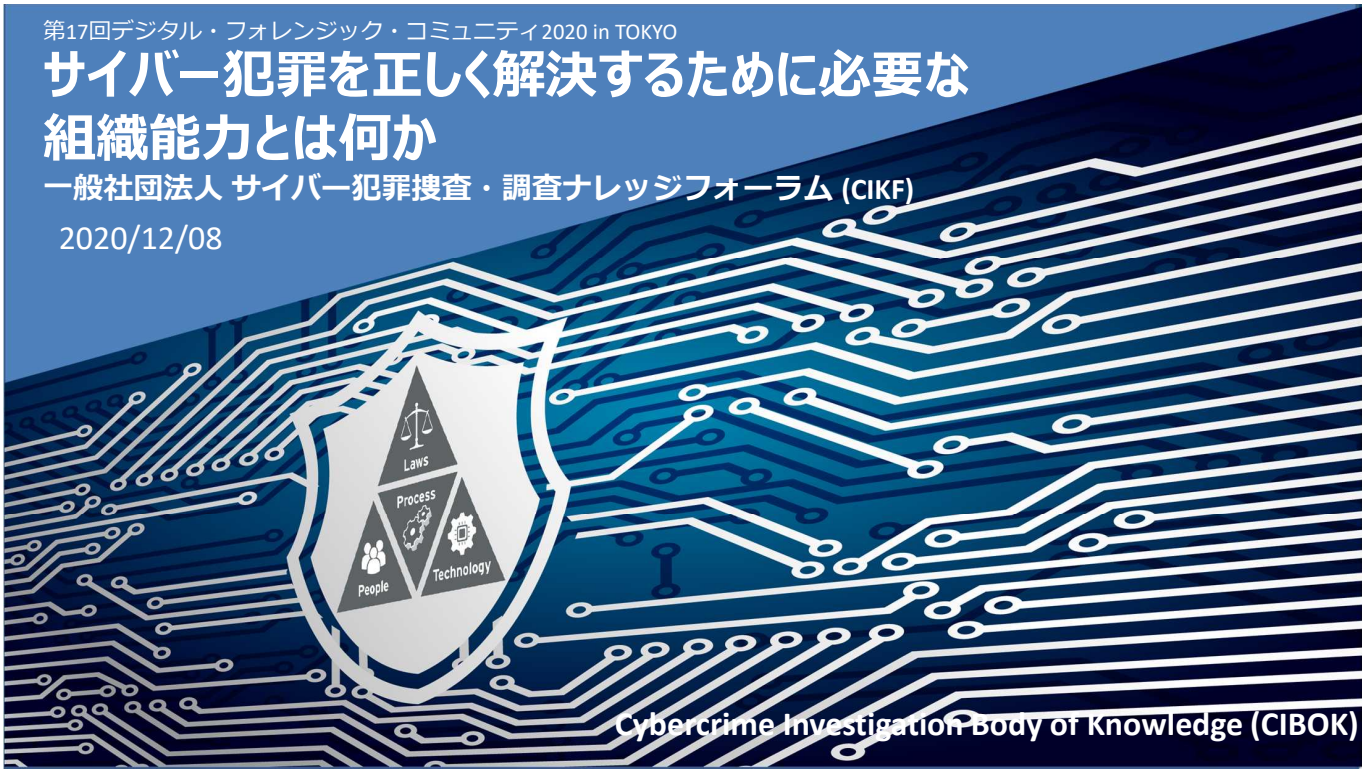
第17回デジタル・フォレンジック・コミュニティ2020 in TOKYO

サイバー犯罪を正しく解決するために必要な組織能力とは何か

一般社団法人 サイバー犯罪捜査・調査ナレッジフォーラム (CIKF)

2020/12/08



第17回デジタル・フォレンジック・コミュニティ2020 in TOKYO

サイバーセキュリティを取り巻く環境

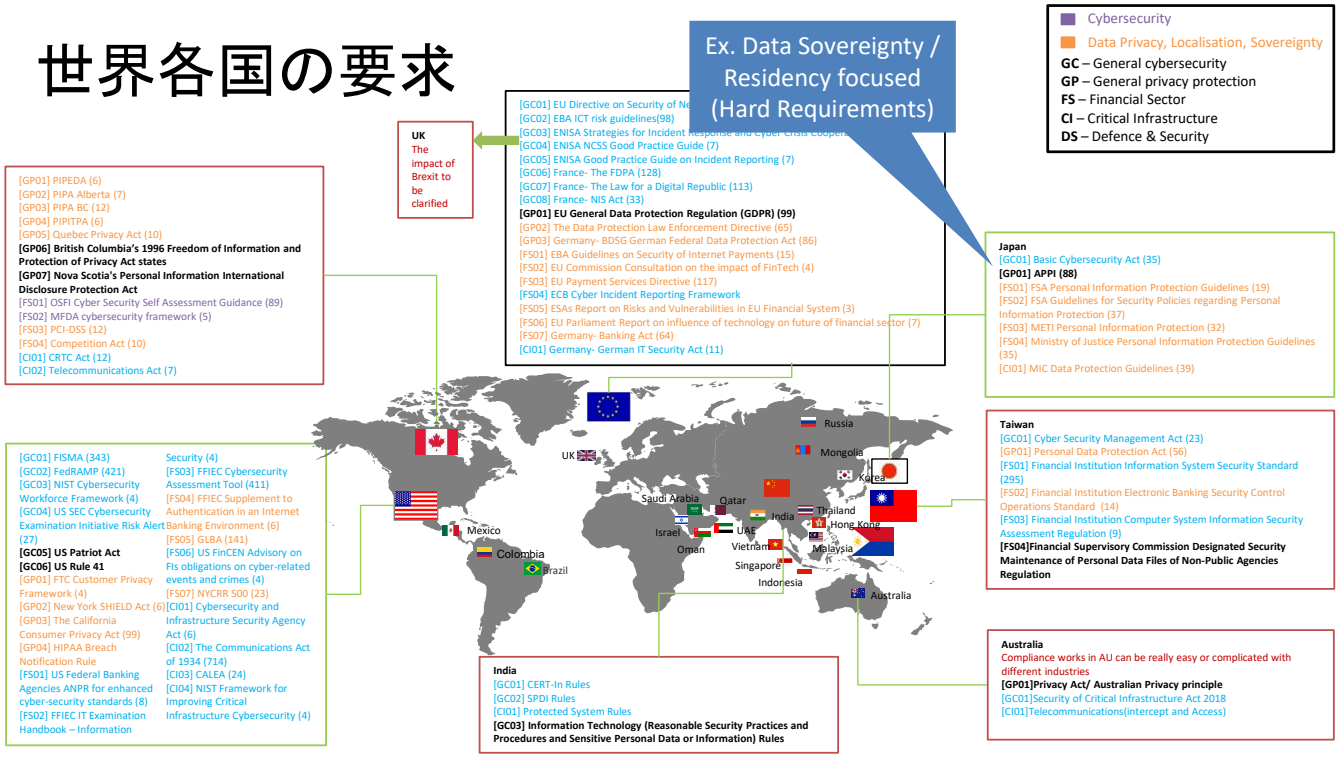
サプライチェーン・リスクへの懸念増大

1. 地政学リスクの高まり
- ① De Coupling と多極化
- ② 経済安全保障上の要求
- ③ データ保護主義の高まりと各国で異なるセキュリティ要求

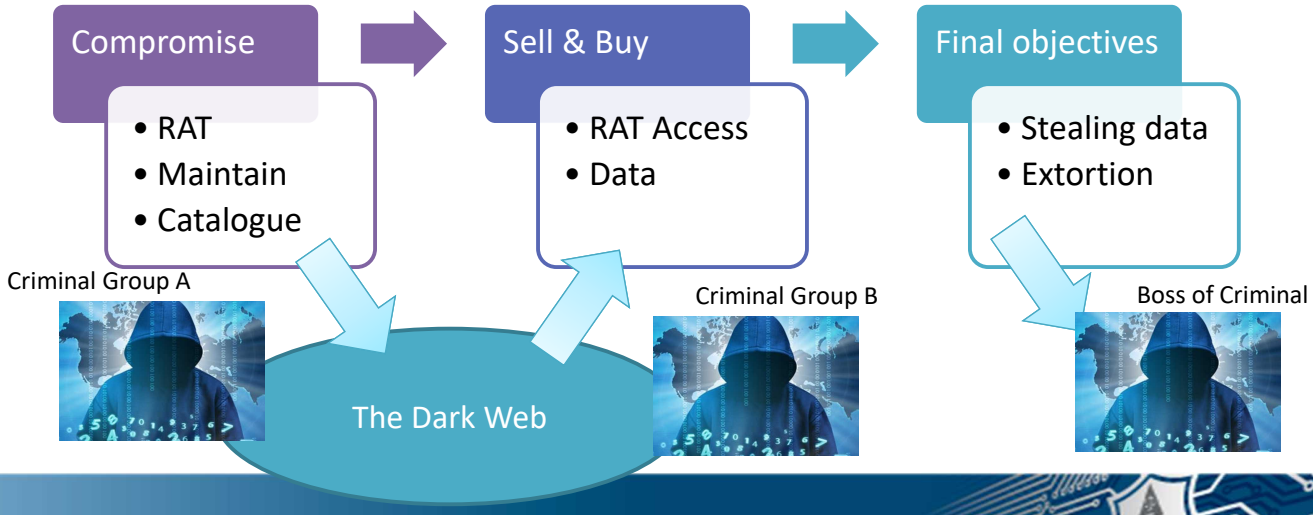
2. サイバー犯罪の高度化
- ① 進む分業化とダークウェブの役割
- ② ウィーケストリンクを狙った犯罪の増加

3. リスク・サーフェスの増加
- ① テレワークの常態化
- ② クラウド移行の加速化

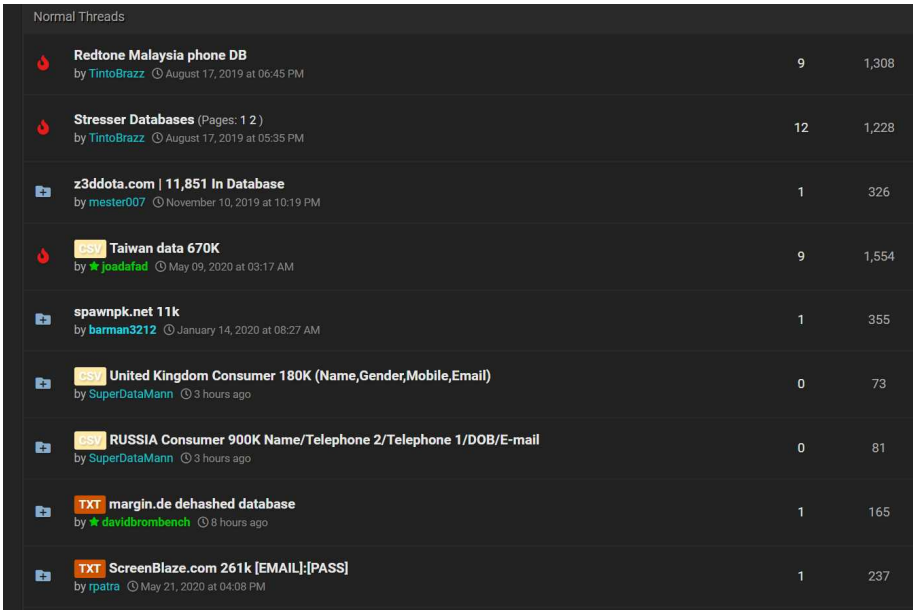
世界各国の要求



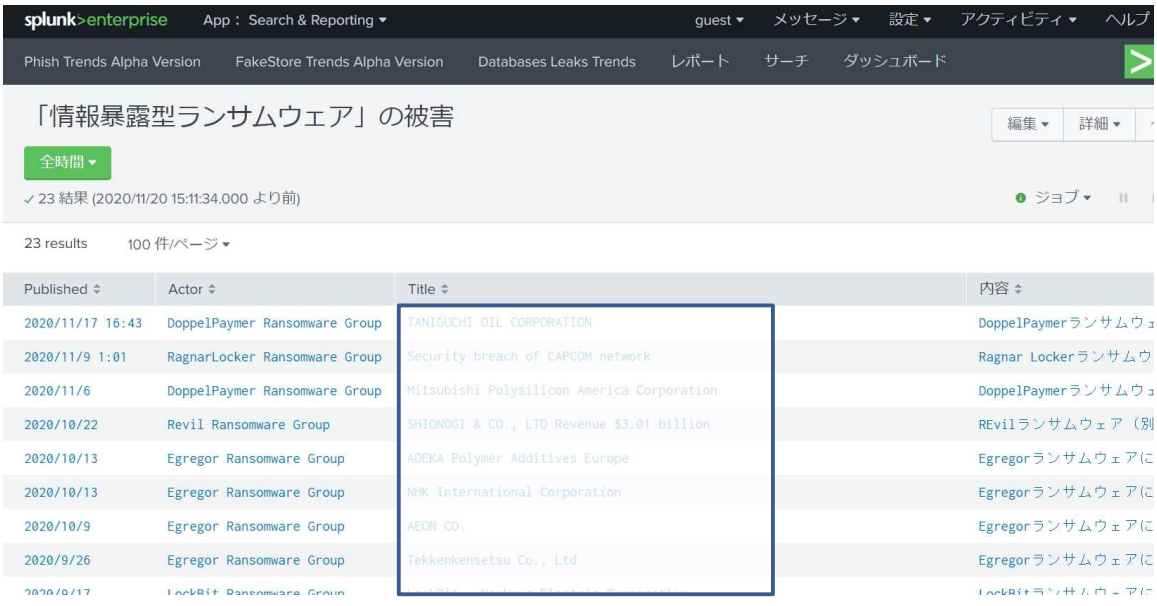
サイバー犯罪の分業化



【参考】リークサイト (surface web)



【参考】日本企業を狙う暴露型ランサムウェア被害状況



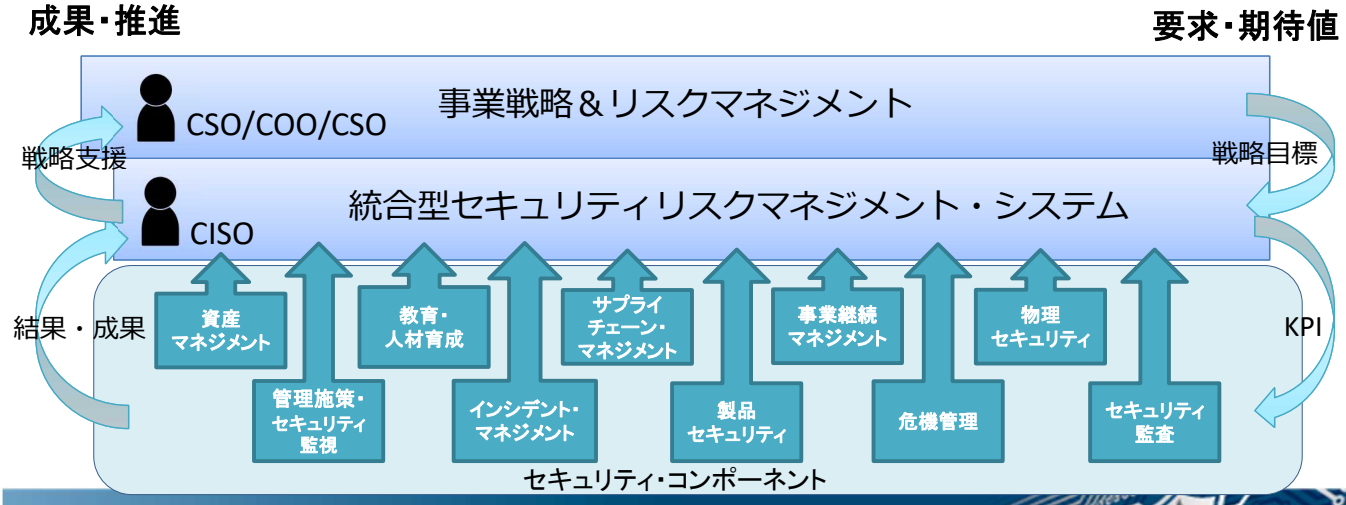
統合型モデル

統合型モデル

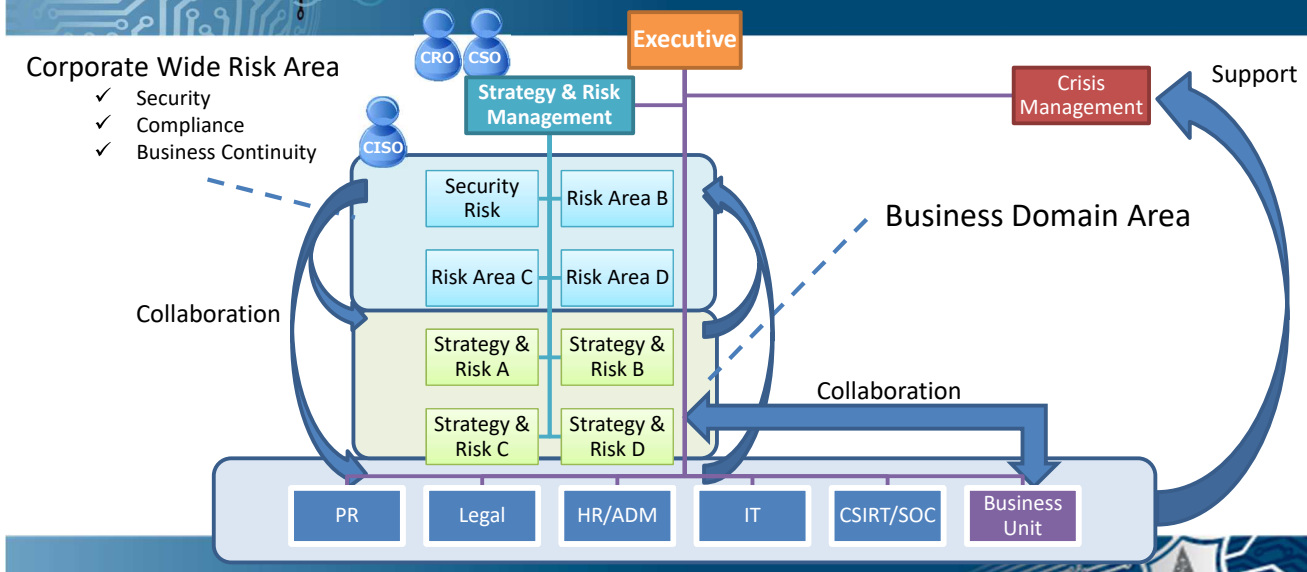
何と何を統合（一体化）させるべきか？

- ✓ **組織戦略／事業戦略**と**リスクマネジメント**
- ✓ 各種**リスク領域**（統合型リスクマネジメント）
- ✓ 各種**セキュリティ機能**（統合型セキュリティマネジメント）

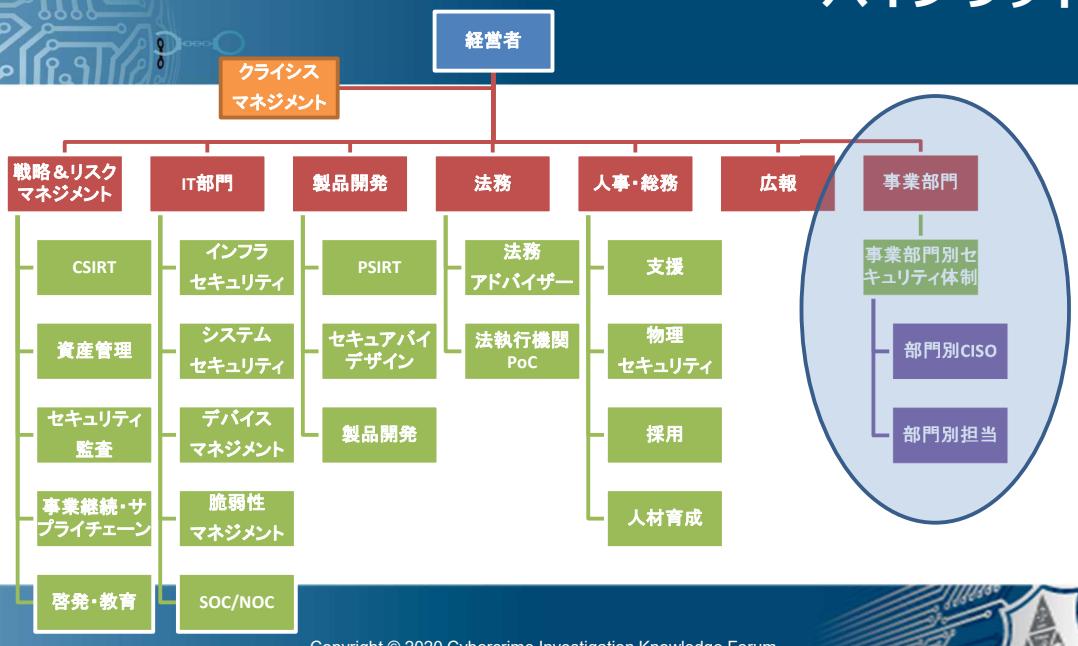
統合型セキュリティマネジメント



ハイブリッド・モデル

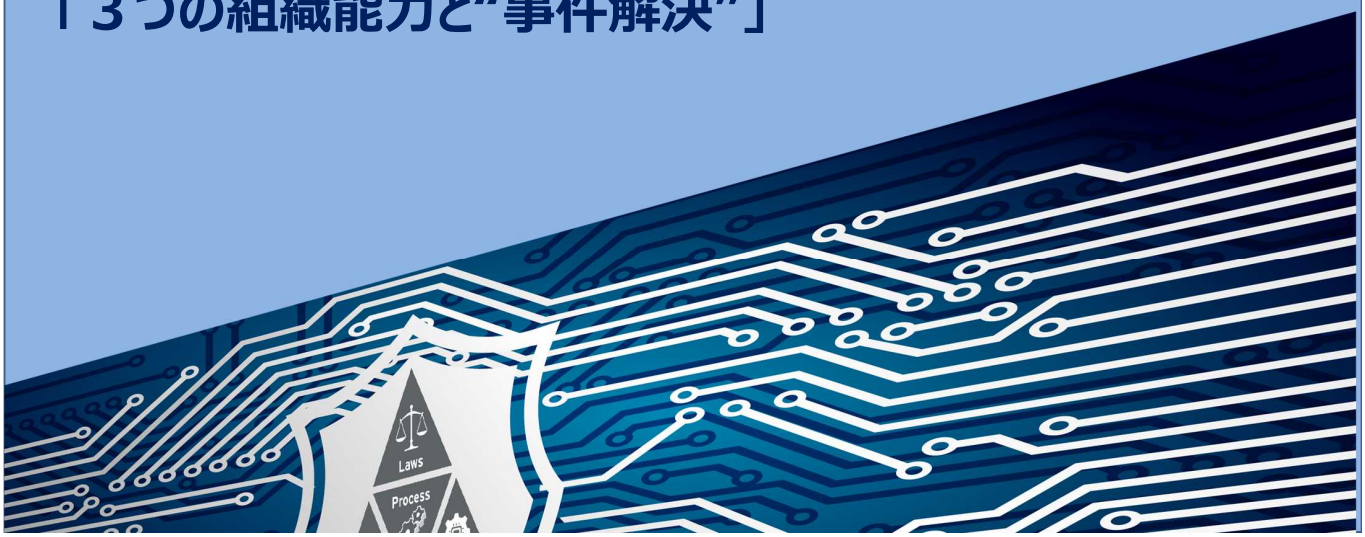


ハイブリッドの例



第17回デジタル・フォレンジック・コミュニティ2020 in TOKYO

次世代型サイバーセキュリティ・マネジメントを支える「３つの組織能力と“事件解決”」



次世代型サイバーセキュリティに必要な「３つの組織能力」

防御力

- 自社組織の成長や戦略を阻害しないようにリスクを低減する組織能力

対応力

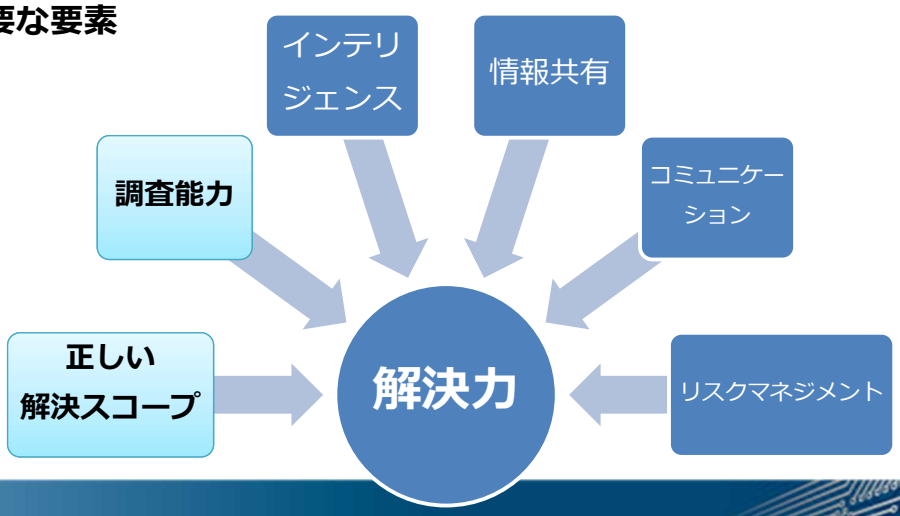
- 事件に正しく対処し影響を許容範囲内に抑え込むための組織能力

解決力

- 事件を最適な形で解決し残存リスクを許容範囲内に収めるための組織能力

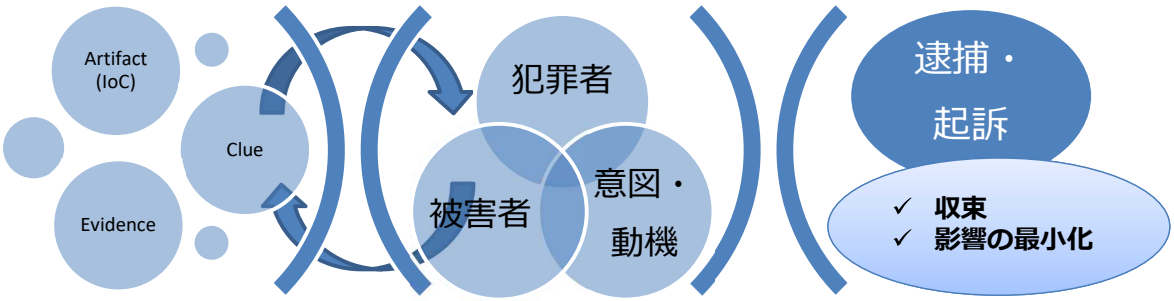
解決力

解決力に必要な要素



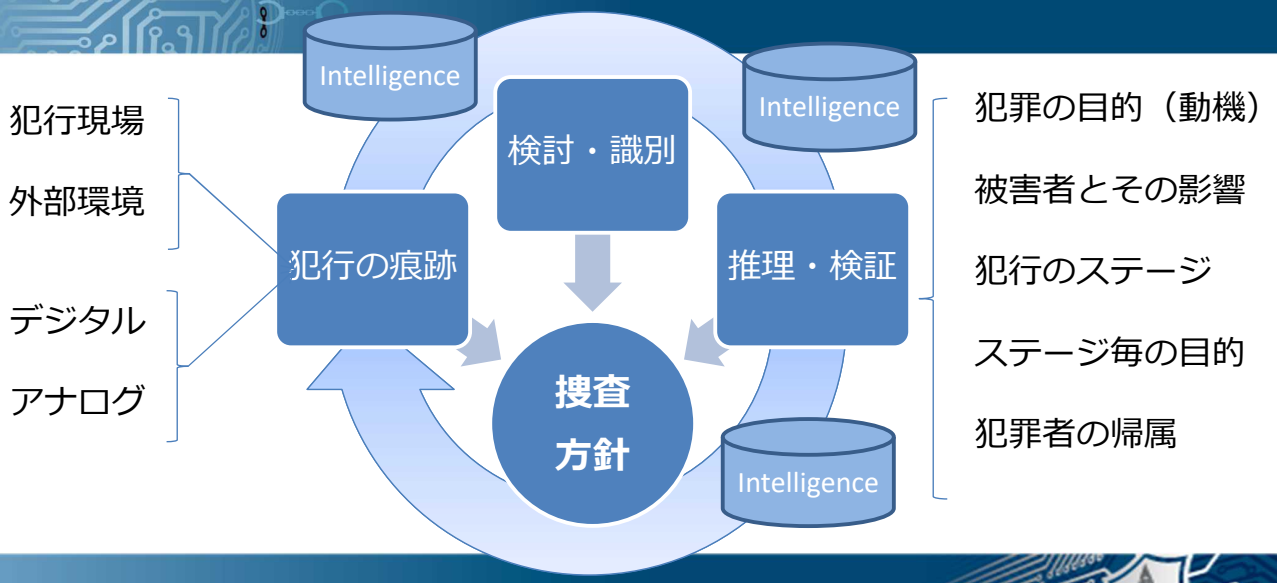
サイバー犯罪捜査（調査）とは？

何が起きた（ている）のか？　　誰が何のために？　　最終解決



捜査（調査）　　犯罪の属性　　法執行・事態の収束

調査スコープの検討



スコープ検討のフレームワーク

ロ 犯罪のスコープ（アーティファクト分析後、再確認が必要）

- 犯罪タイプ（偶発的 / 標的型 / 進化型<マルチテナント型>）
- 目的（動機） / 加害者
- 犯行ステージ（キルチェーン / MITRE (PRE) ATT&CK など）
- 影響（リスク）のスコープ (ブランド / 金銭 / 業務 / 従業員)

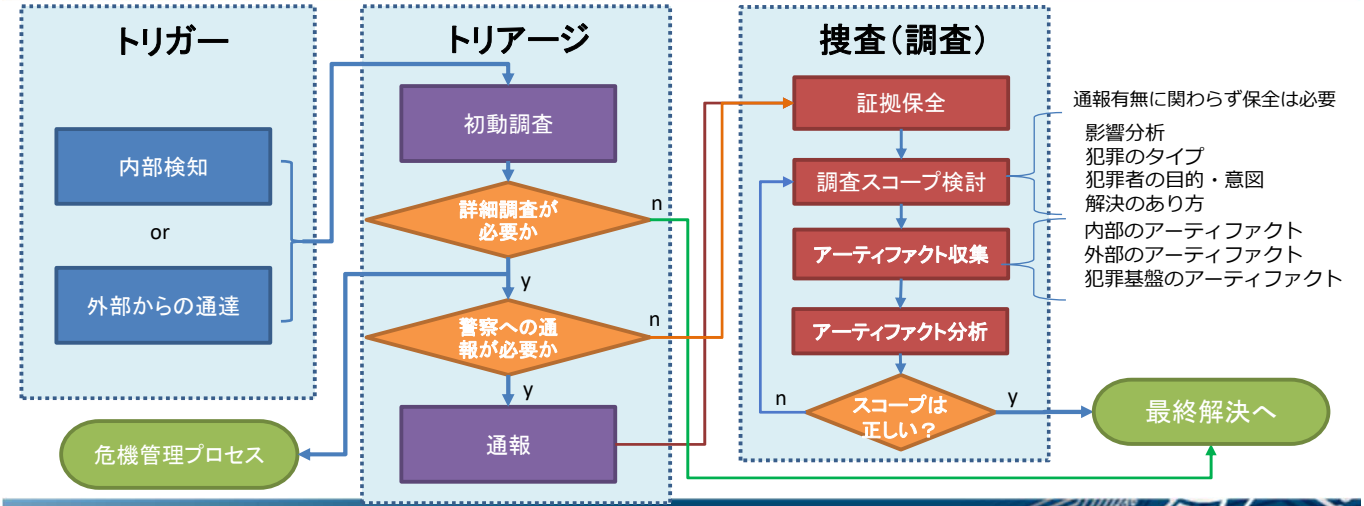
ロ 捜査（調査）のスコープ

- ゴール
  - ✓ 被害者の望むゴール
  - ✓ 法執行機関の望むゴール
- セカンド・ベスト
  - ✓ ゴール達成が困難と判明した場合の選択肢を用意しておく

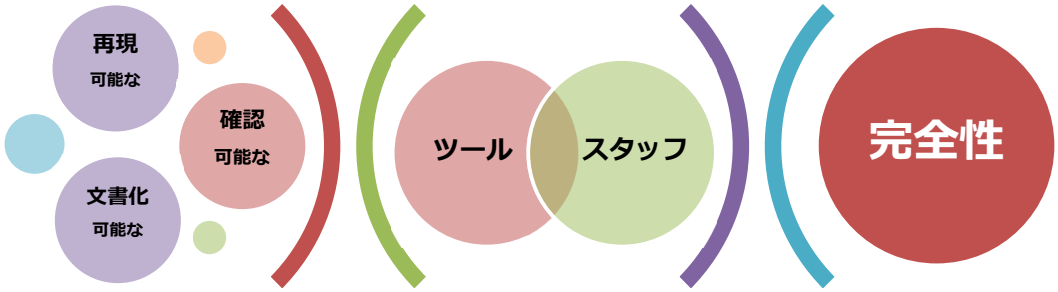
スコープ検討時の留意点

- ✓ 犯罪の「**特性**」を把握すること
- ✓ 使用されたツールや**技術的特性にのみ注目しない**こと
- ✓ **被害者が誰なのか**を十分に考慮すること
- ✓ **サイバー犯罪が分業化(CaaS)している**事実をふまえて検討すること
- ✓ **専門領域の知識が高い犯罪者の関与**の可能性を検討すること
- ✓ 金銭目的の場合、**最も儲かる機会を狙う**傾向が強いことを意識すること
- ✓ 発見される痕跡**全てが特定の犯行に帰属するとは限らない**こと
- ✓ 「めくらまし」「偽旗作戦」の痕跡に**だまされない**こと

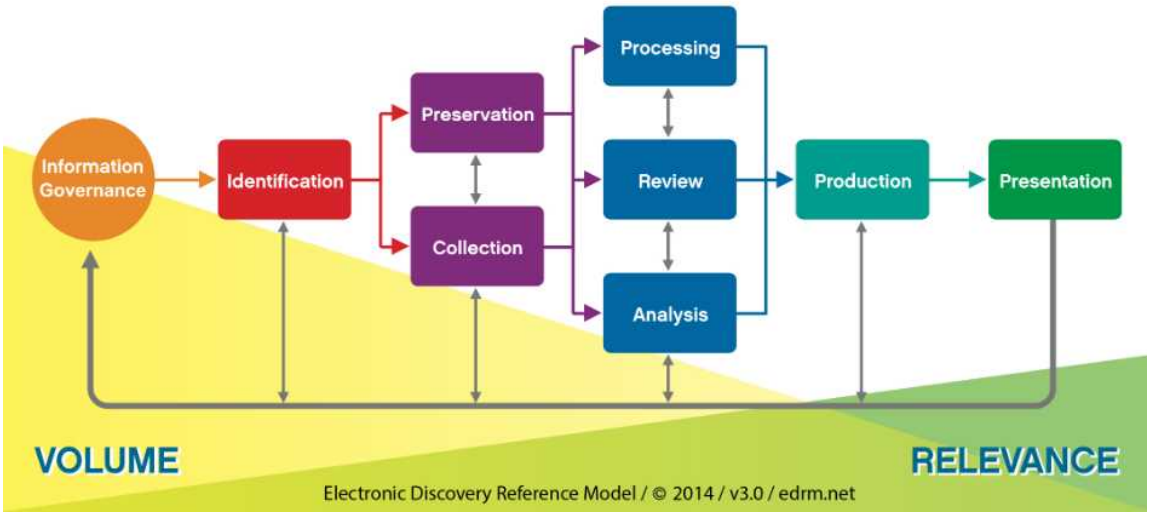
事件対応・全体の流れ



フォレンジックにおける証拠の完全性

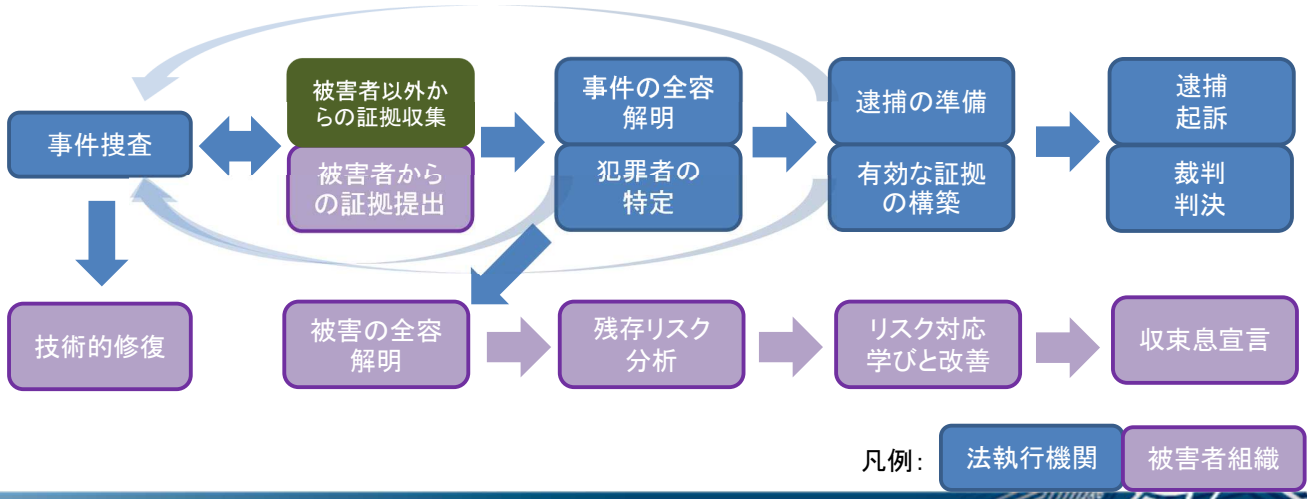


Electronic Discovery Reference Model（EDRM）



Source : Electronic Discovery Reference Model / EDRM.NET
https://www.edrm.net/frameworks-and-standards/edrm-model/

最終解決へのプロセス



CIKF
Cybercrime Investigation Knowledge Forum

Cybercrime **I**nvestigation **K**nowledge **F**orum

Any inquiries, please contact : secretariat@cibok.org

https://www.cibok.org/ja/cikf/