IDF第16回デジタル・フォレンジック・コミュニティ2019 in Tokyo

サイバー犯罪リスクの本質を捉えた体制構築

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）
代表理事　清水　智

2019/12/09

Cybercrime Investigation Body of Knowledge (CIBOK)

この数字は何の数字でしょうか？

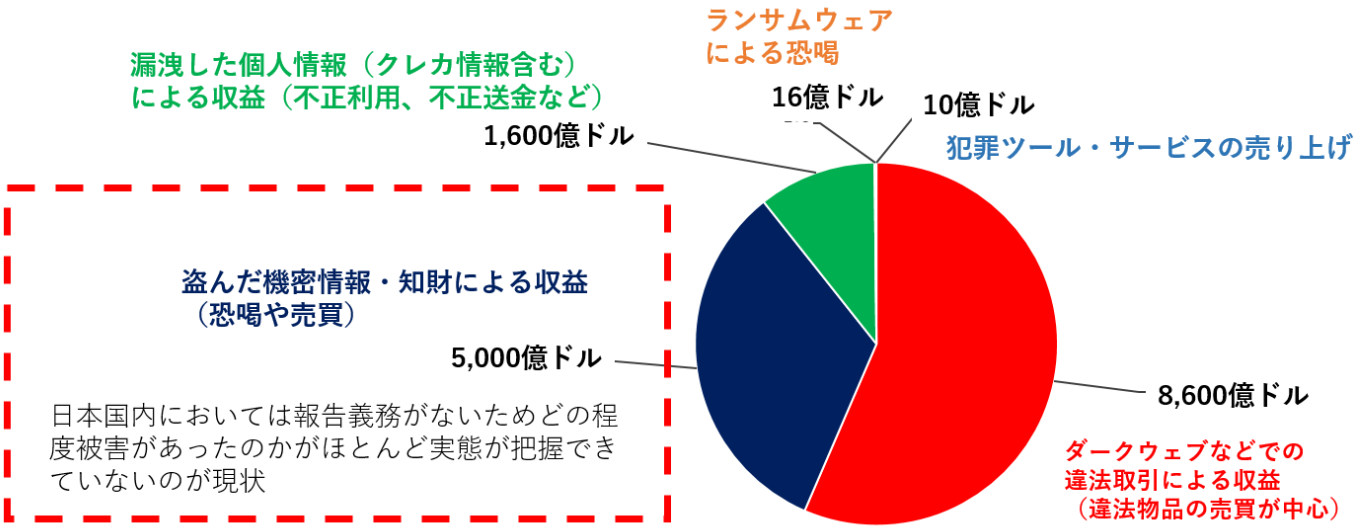
約170兆円
（1.6Trillion US$）

この数字は何の数字でしょうか？

1米国	20,580,250
2中国	13,368,073
3日本	4,971,767
4ドイツ	3,951,340
5イギリス	2,828,833
6フランス	2,780,152
7インド	2,718,732
8イタリア	2,075,856
9ブラジル	1,867,818
10韓国	1,720,489

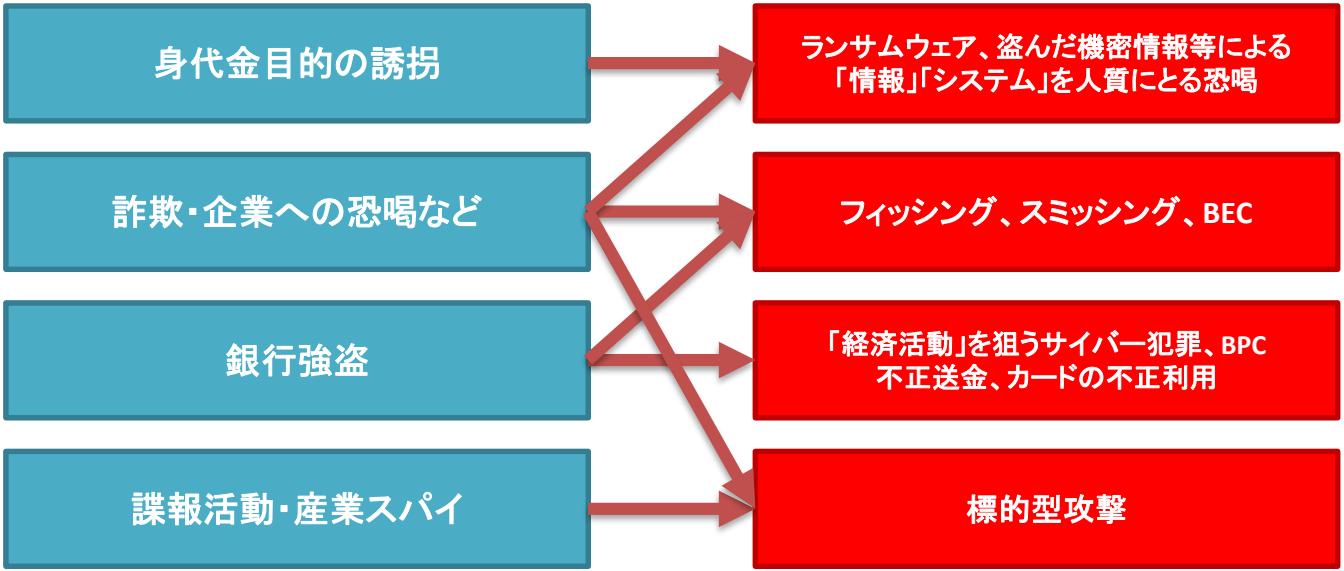
“サイバー犯罪者国”のGDP

サイバー犯罪者の収益構造



出典：Re-Hashed: 2018 Cybercrime Statistics: A closer look at the “Web of Profit”
https://www.thesslstore.com/blog/2018-cybercrime-statistics/

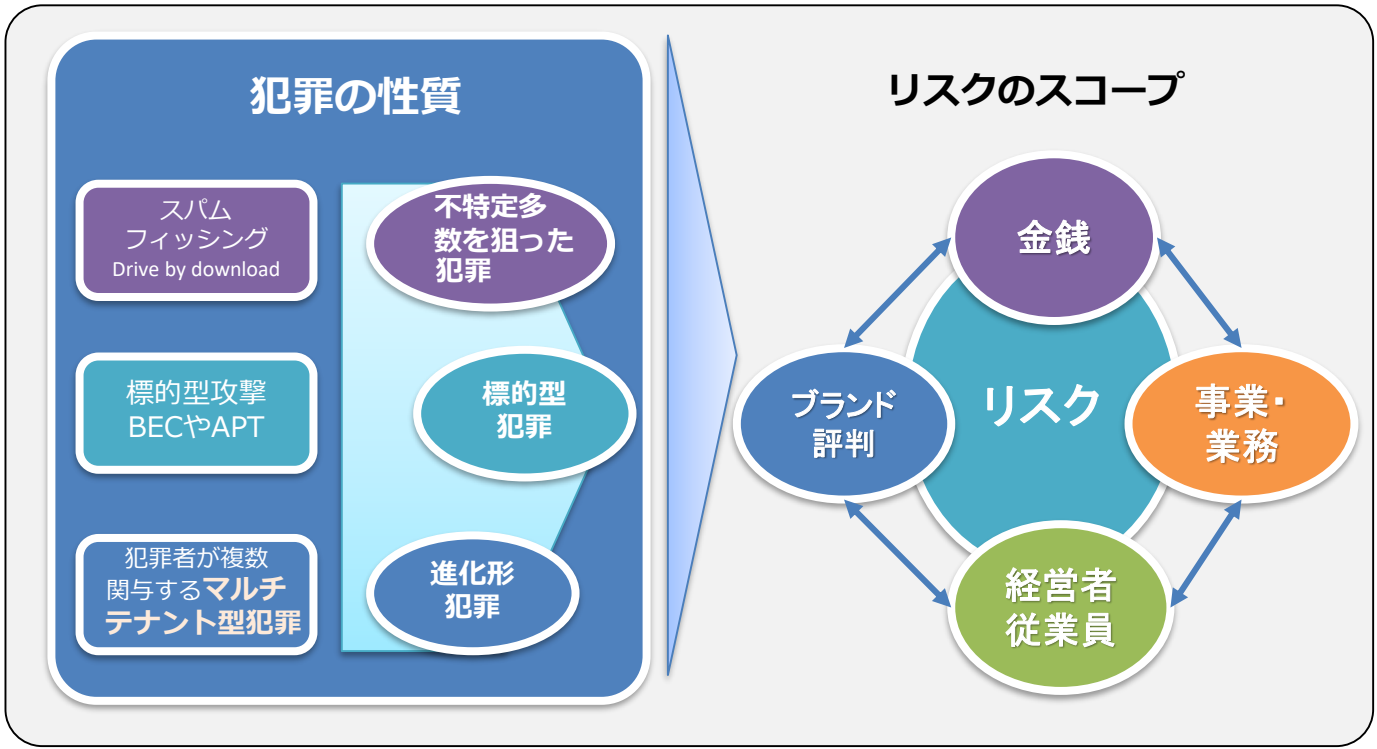
サイバー犯罪は、レガシー犯罪を置き換えつつある



サイバー犯罪の分類

犯行動機	主な加害者	主な手口	主な被害者	主な事例
金銭詐取	国家 民間の犯罪組織 個人の犯罪者	フィッシング・詐欺サイト クレデンシャル情報詐取 ランサムウェア等による脅迫 仮想通貨交換所からの詐取 不正コインマイニング	個人（消費者） 金融機関 法人・公的組織	クレカ不正利用事件 WannaCry事件 コインチェック事件 バングラディシュ銀行事件 バンキングトロジャン事件
スパイ行為	国家 民間の犯罪組織	スピア・フィッシング・SNS アカウントなりすまし リモートアクセス・情報詐取	政府・行政機関 重要インフラ組織 法人	年金機構事件 企業への標的型攻撃 平昌五輪事件
主義・主張・破壊	国家 ハッカー集団 アクティビスト集団	DDoS攻撃 WEBサイト改竄 ランサムウェアによる破壊	政府・行政機関 政党・政治家 選挙団体 イベント主催者	ソニーEP事件 政治家サイト改竄事件 太子町事件 選挙への影響行使事件
復讐・名誉棄損	内部者 民間の犯罪組織	サイバー恐喝 暴露行為 サイバーストーキング	個人・著名人 政府・行政機関 法人・公的組織	復讐サイト リベンジポルノ 暴露サイト（有名人）
性的目的・名誉欲、愉快犯その他	児童ポルノ 著作権違反サイト	不法サイト運営 コンテンツ配信 偽情報の流布	著作権者、肖像権保有者、地位のある個人など	児童ポルノ摘発事件 漫画村事件

サイバー犯罪の特性と被害者のリスク



より大事な観点

過去 → 次世代の思考

WHAT

何を
攻撃しようと
しているのか

HOW

どのように
攻撃しようと
しているのか

WHY

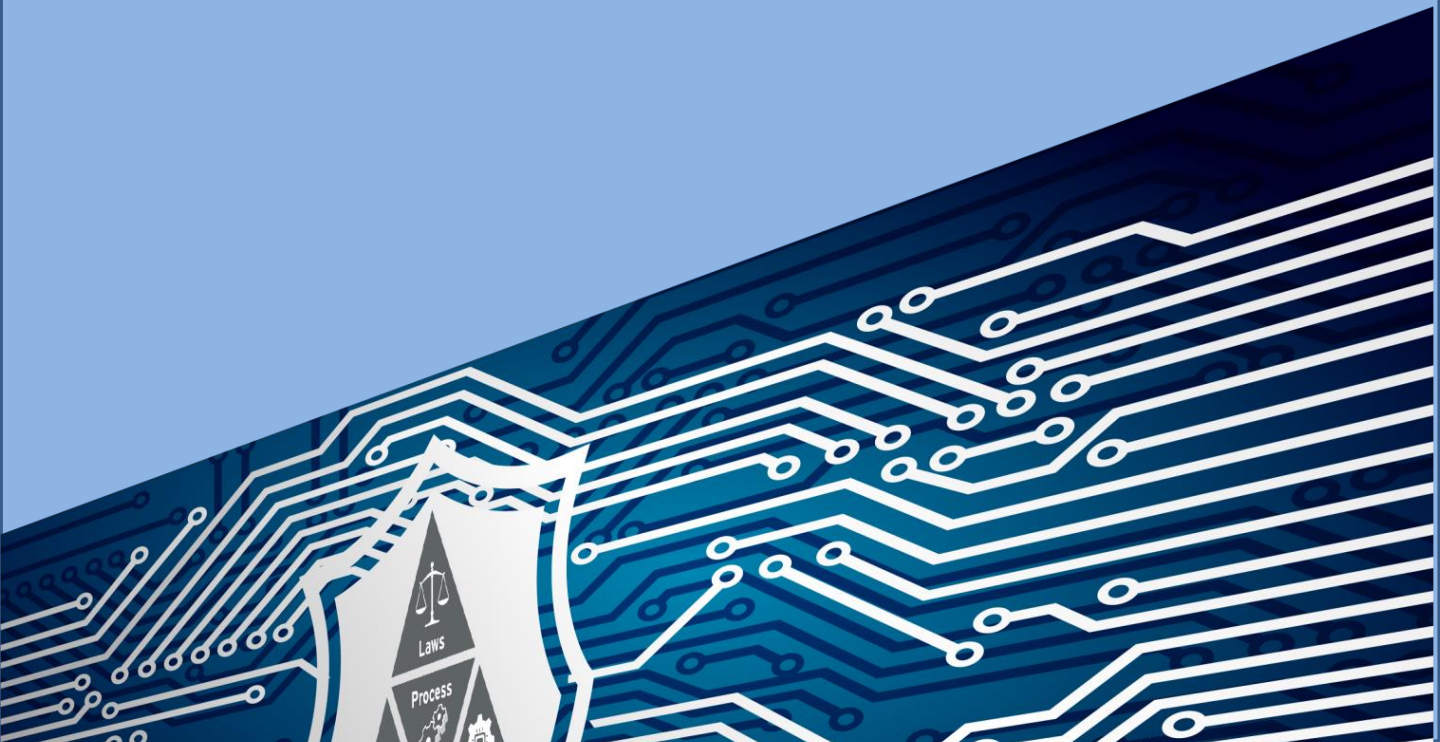
なぜ
攻撃の動機は何か

WHO

誰が誰を
狙っているのか

IDF第16回デジタル・フォレンジック・コミュニティ2019 in Tokyo

サイバー犯罪リスクに対抗する組織の課題



サイバーセキュリティを巡る課題

サイロ化した組織と連携の薄さ

リスクに対する認識

・単なるITマターなのか
・意図を持った犯罪被害なのか

“投資”とならない経営認識

・セキュリティはコスト
・費用対効果が全くわからない

横並び指向

・どこまでやるかを決められない
・同業他社と同じレベルで良い

IDF第16回デジタル・フォレンジック・コミュニティ2019 in Tokyo

必要となる「３つの力」とは？

必要な「３つの力」

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

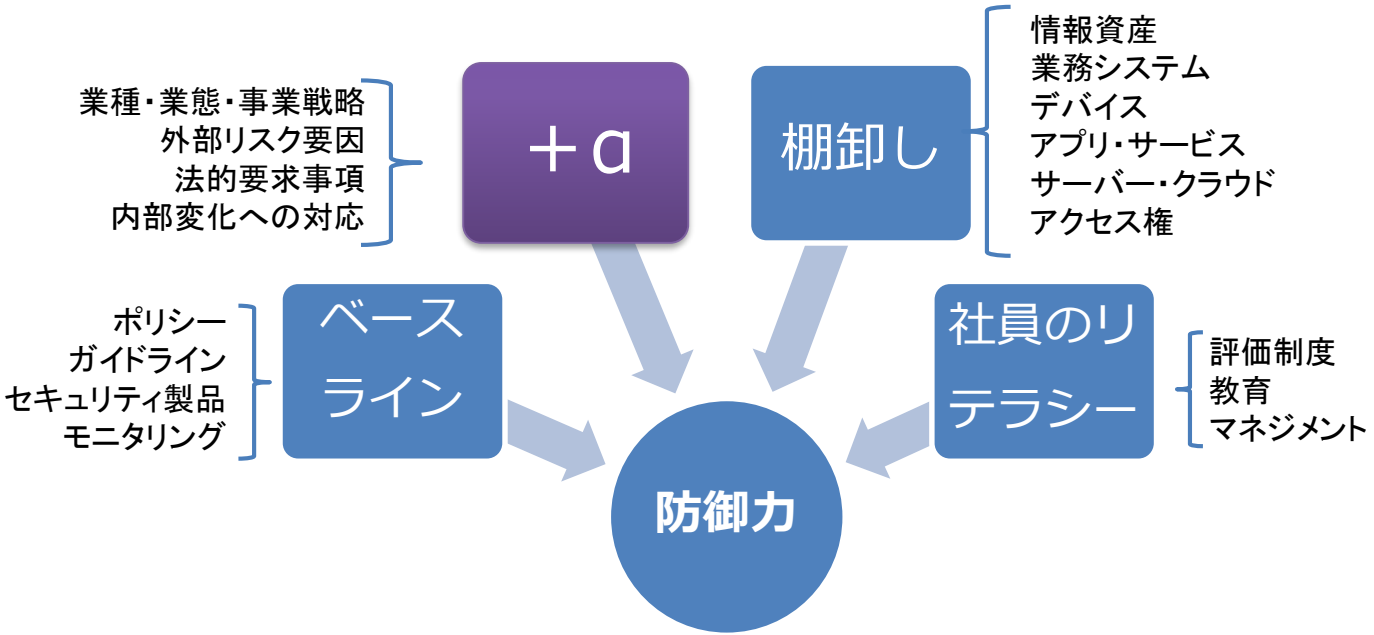
NIST CS Framework

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identify Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

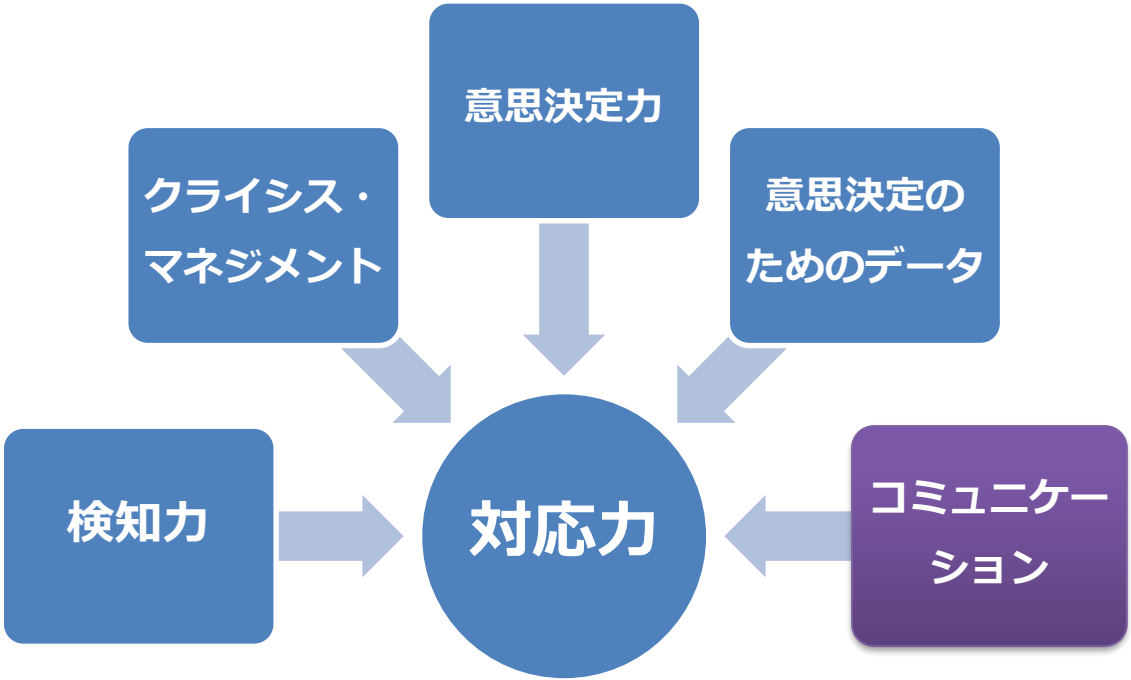
防御力

対応力

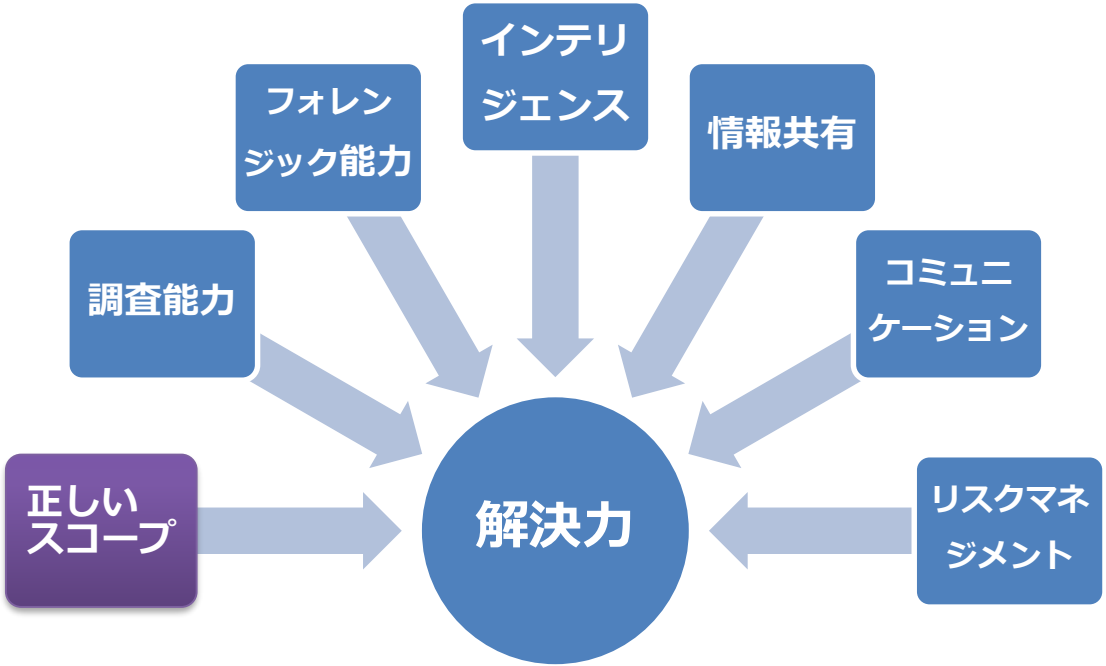
防御力に必要な要素



対応力に必要な要素

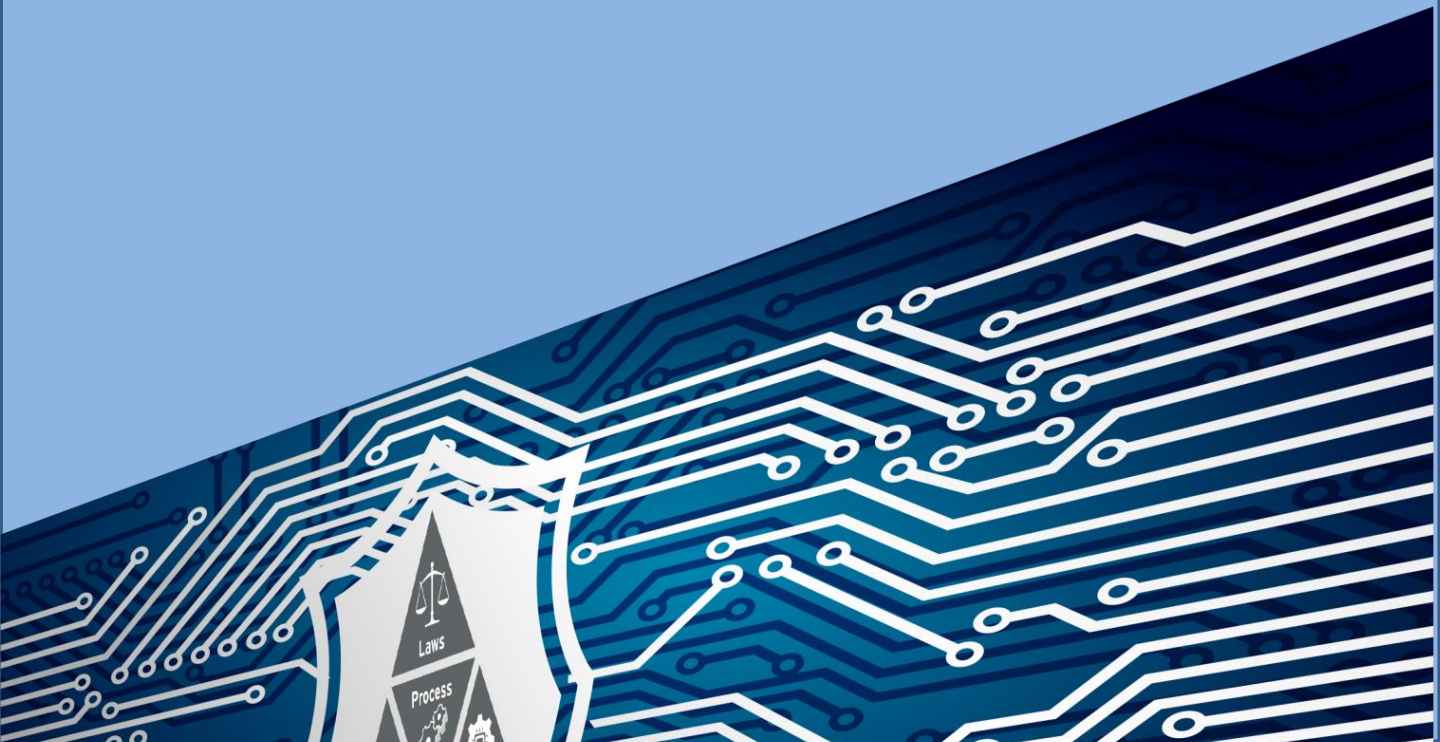


解決力に必要な要素



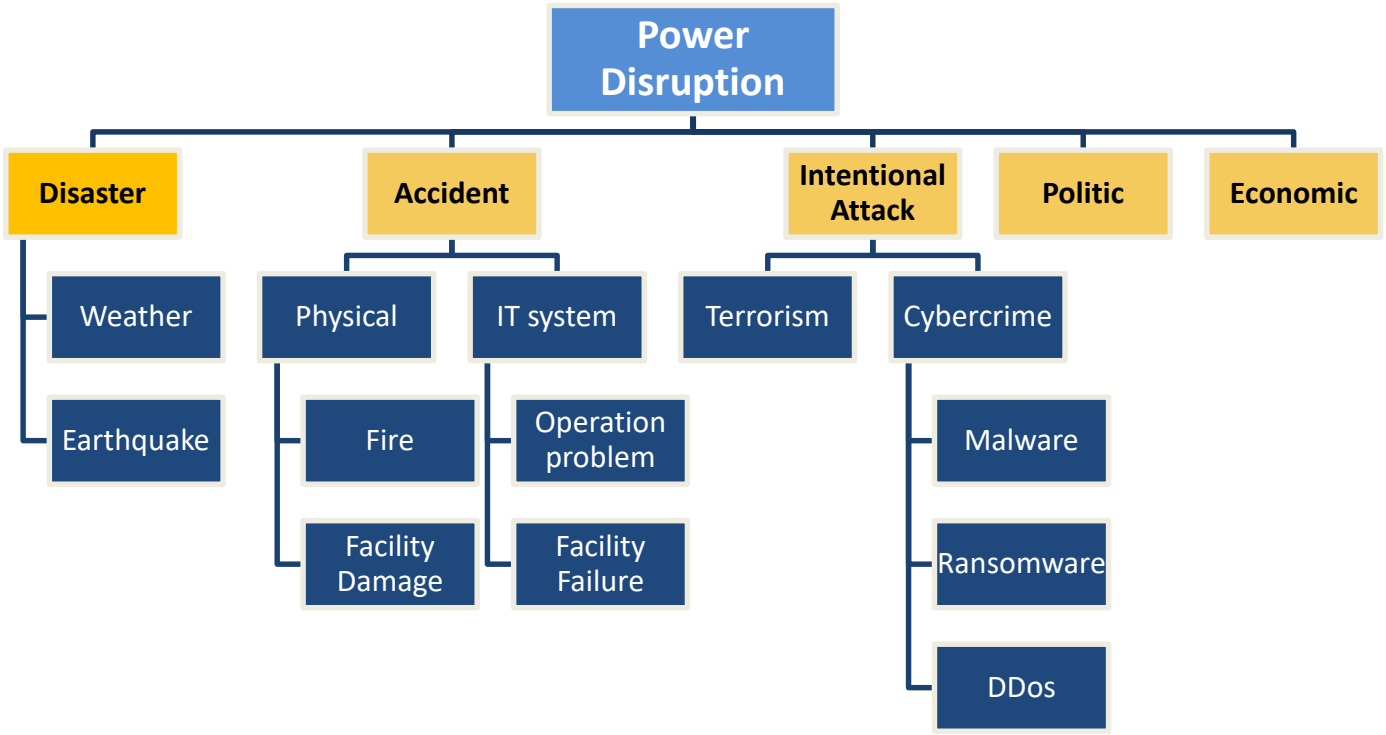
IDF第16回デジタル・フォレンジック・コミュニティ2019 in Tokyo

次世代型のセキュリティ・マネジメントのありかた



統合型モデル

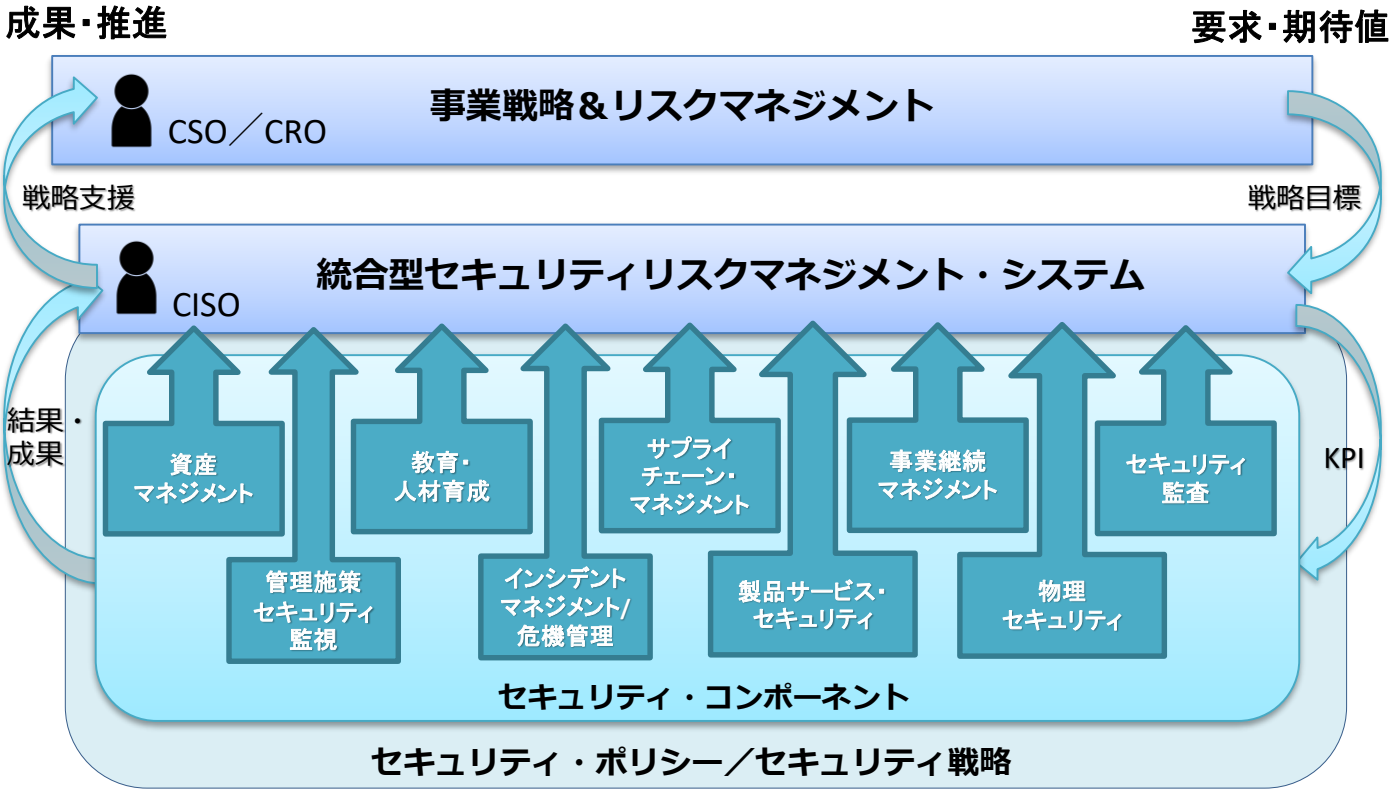
リスク構造



何と何を統合（一体化）させるべきか？

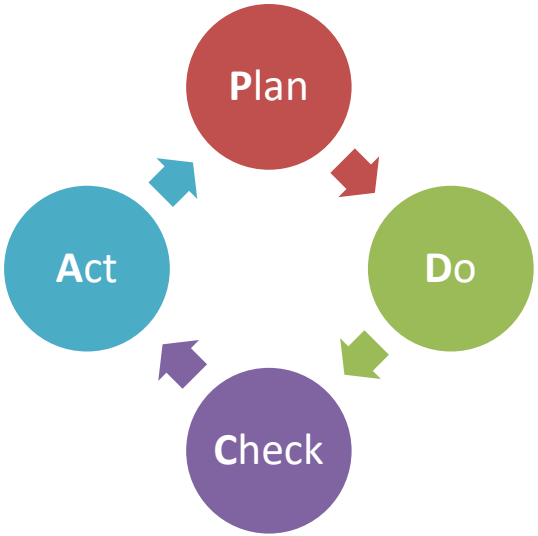
- ✓ 戦略・事業マネジメントとリスクマネジメント
- ✓ サイバーセキュリティ・リスクとその他のコーポレート・リスク
- ✓ 企業（組織）全体戦略とサイバーセキュリティ・リスク
- ✓ セキュリティに関わる各種「機能（コンポーネント）」

統合型セキュリティマネジメント



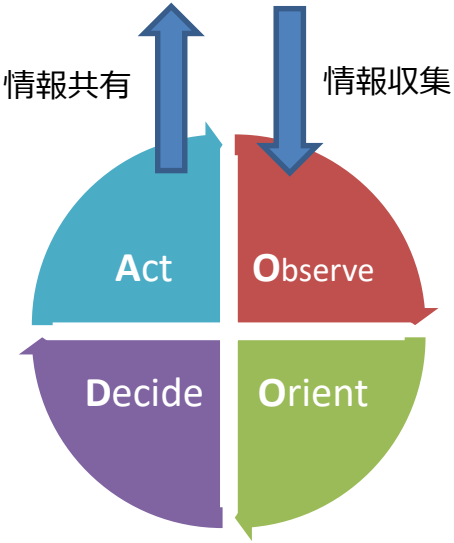
セキュリティマネジメントはPDCA+OODAで回す

ベースラインのセキュリティマネジメント



+

サイバーセキュリティ協議会
業界別ISAC
法執行機関／JC3
各種団体・協議会
OSINT／DarkWeb



動的リスクに対応するセキュリティマネジメント

真の「解決力」を得るために必要なこと

事件調査能力

1. 正しい**スコープ**
2. **インテリジェンス**の活用
3. 的確な**情報収集**
4. **情報共有**
5. **推理**力

法執行機関連携
国際連携

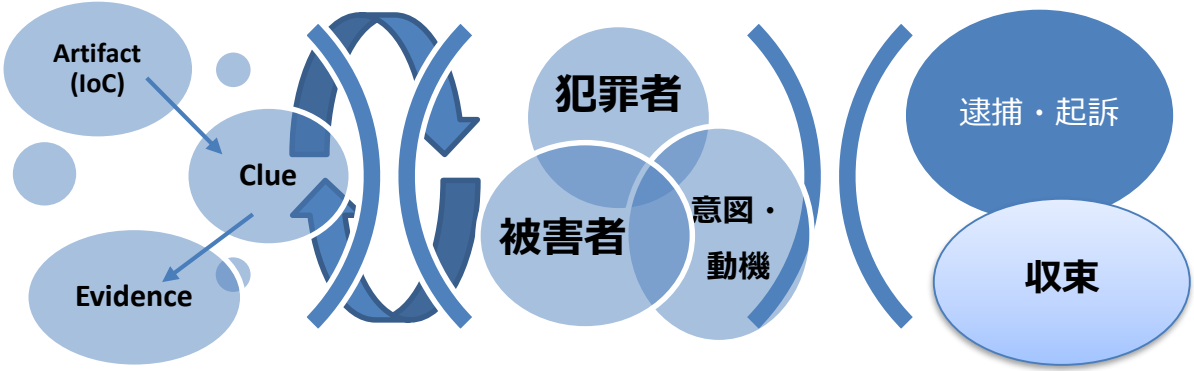
1. 共通**フレームワーク**の活用
2. **信頼関係**を構築
3. 解決**スコープ**の協議

トレーニングと訓練

1. ケーススタディ
2. **RACI**に紐づいた訓練
3. 社員**全体のリテラシー**

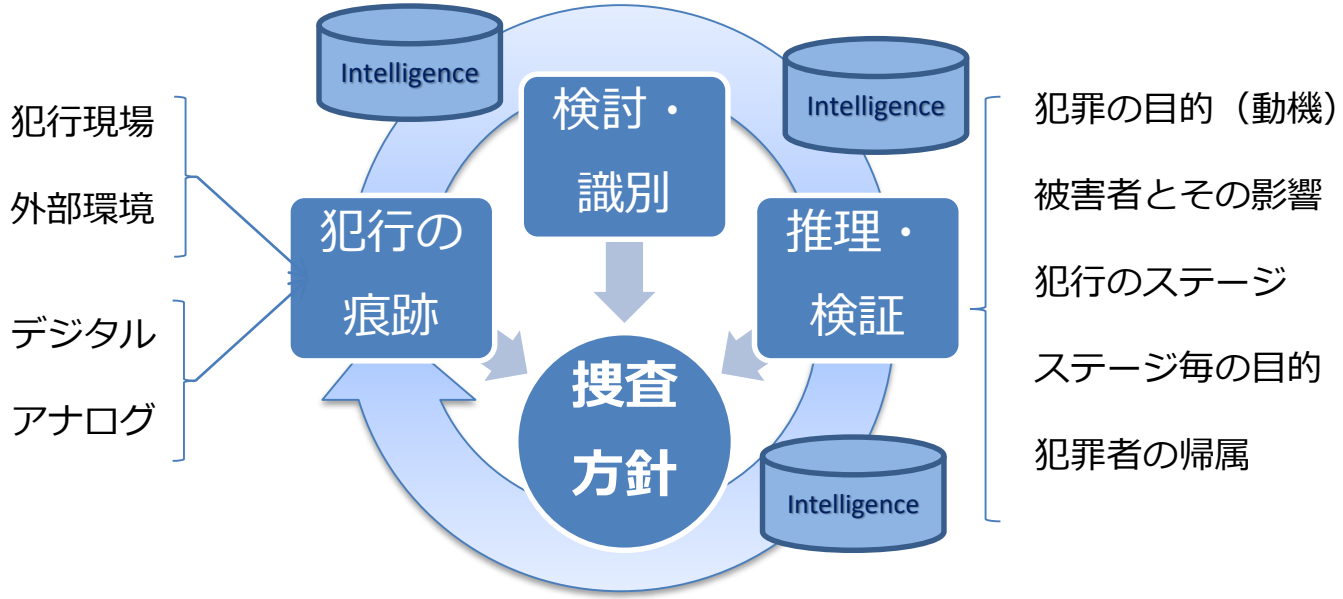
サイバー犯罪捜査とは？

何が起きた（ている）のか？　誰が何のために？　最終解決



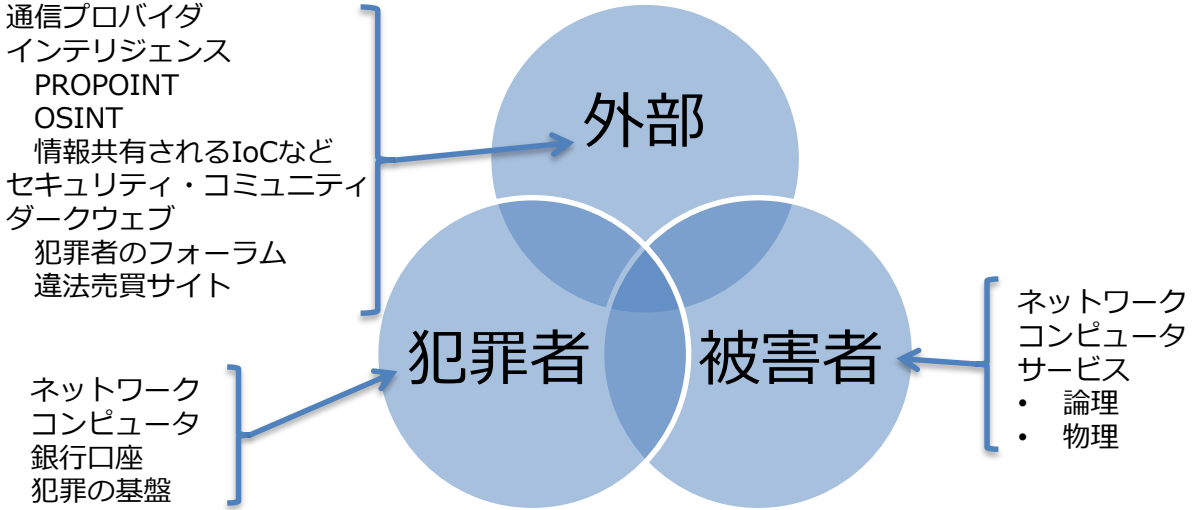
捜査（調査）　犯罪の属性　法執行・被害修復

調査スコープの検討モデル

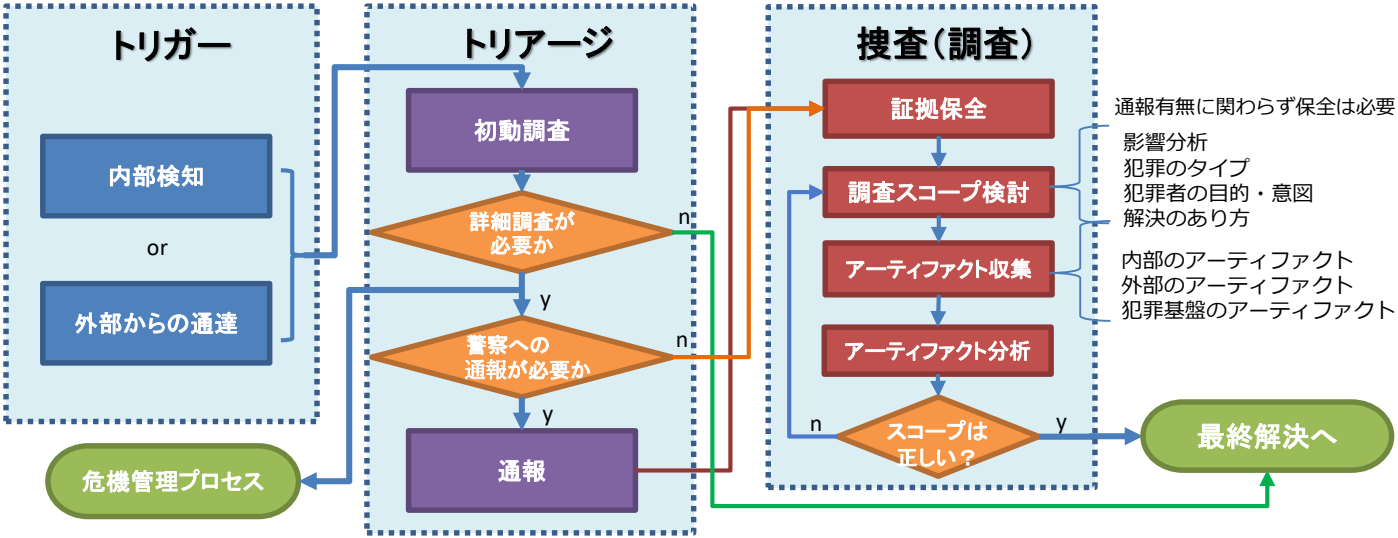


証拠に繋がる３つの情報源

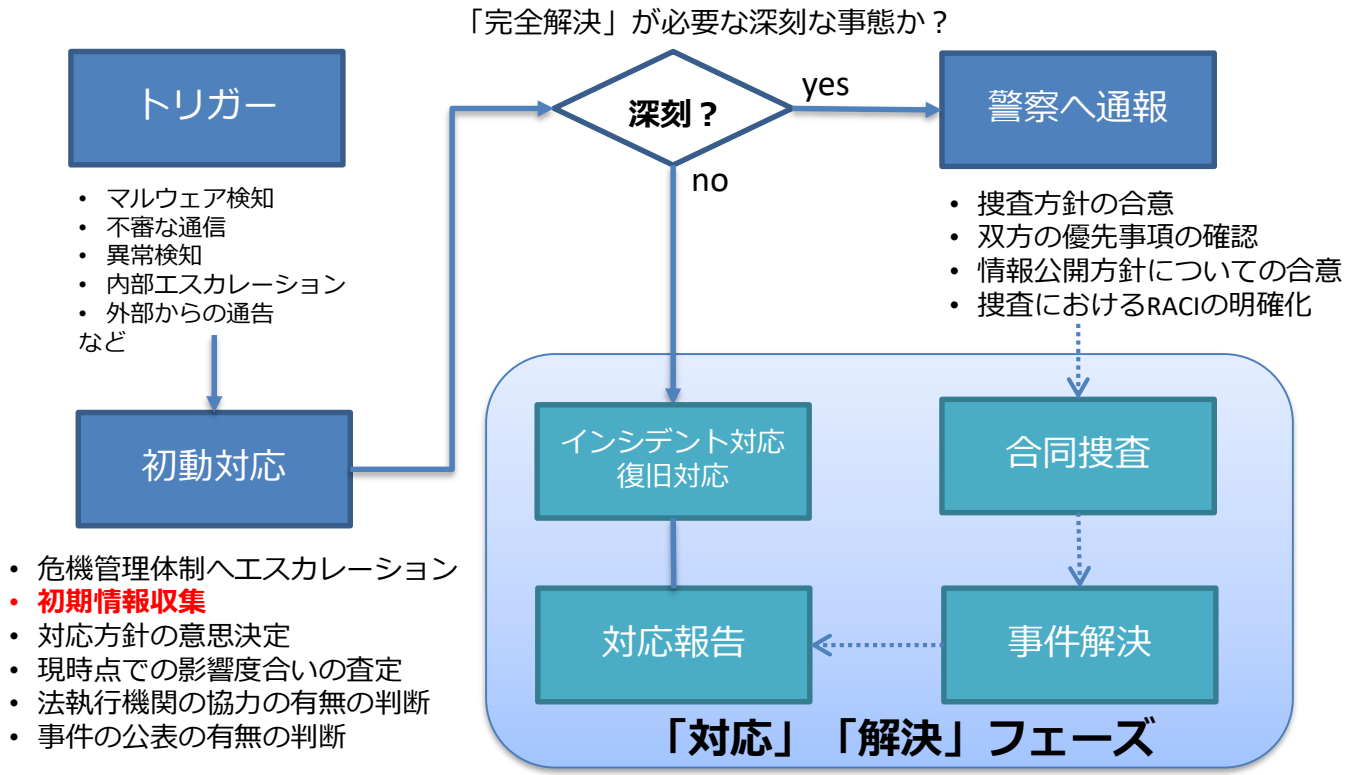
犯罪の証拠を構成する情報を得るためには、被害者（**内部**）及び**外部**の情報源から効果的に情報を収集し、相関分析を行うことで、前後関係(コンテキスト)を把握することができる。



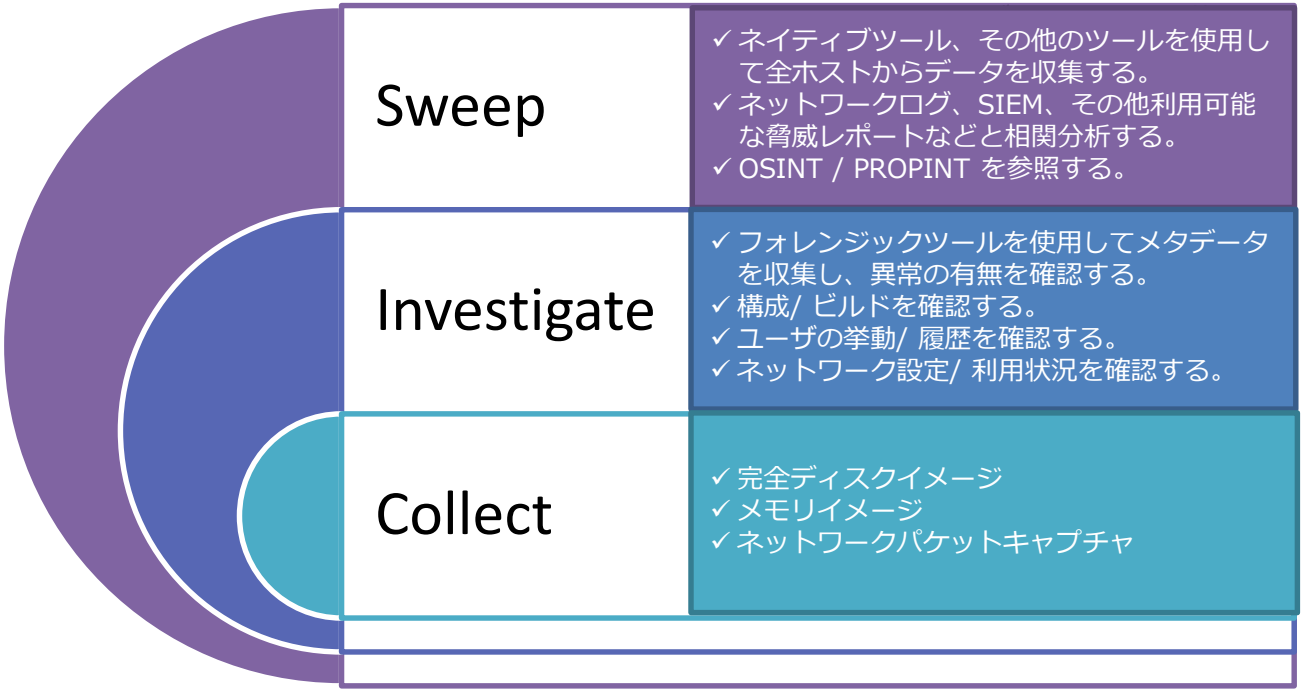
事件対応・全体の流れ



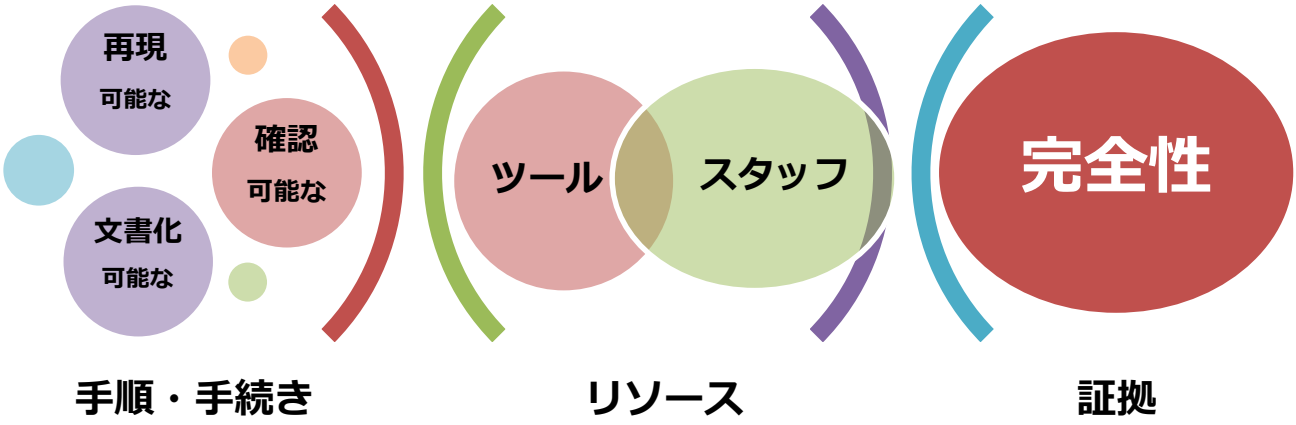
トリアージ



トリアージ型収集方法

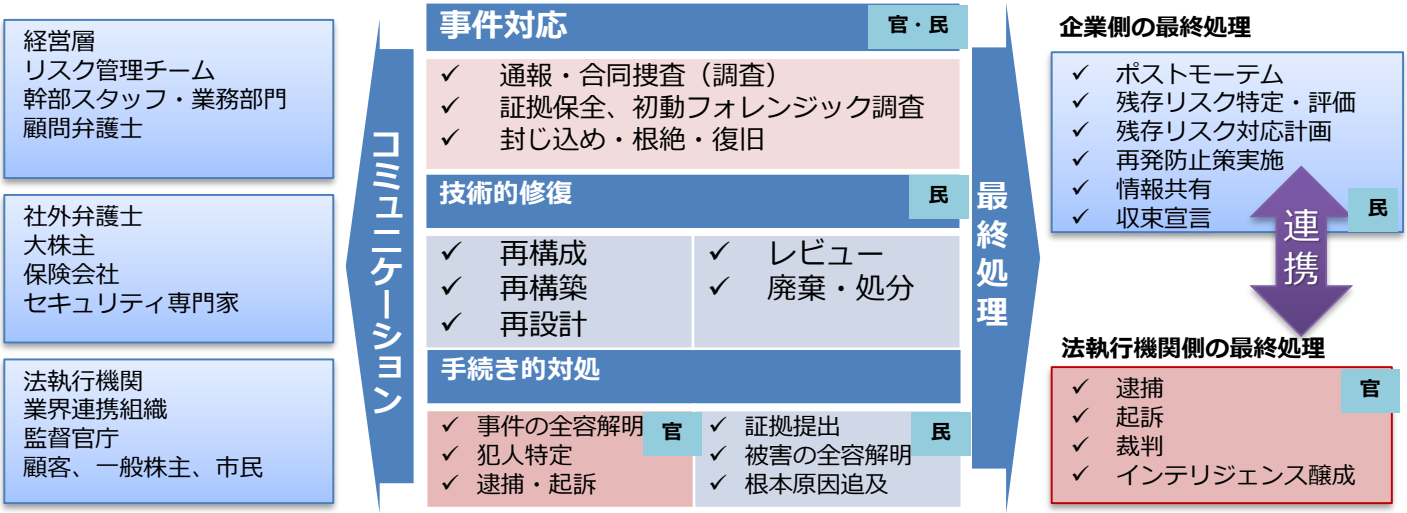


証拠の完全性の確保



- 民間企業であっても「証拠保全ガイドライン」を理解しておきたい

サイバー犯罪の最終処理モデル



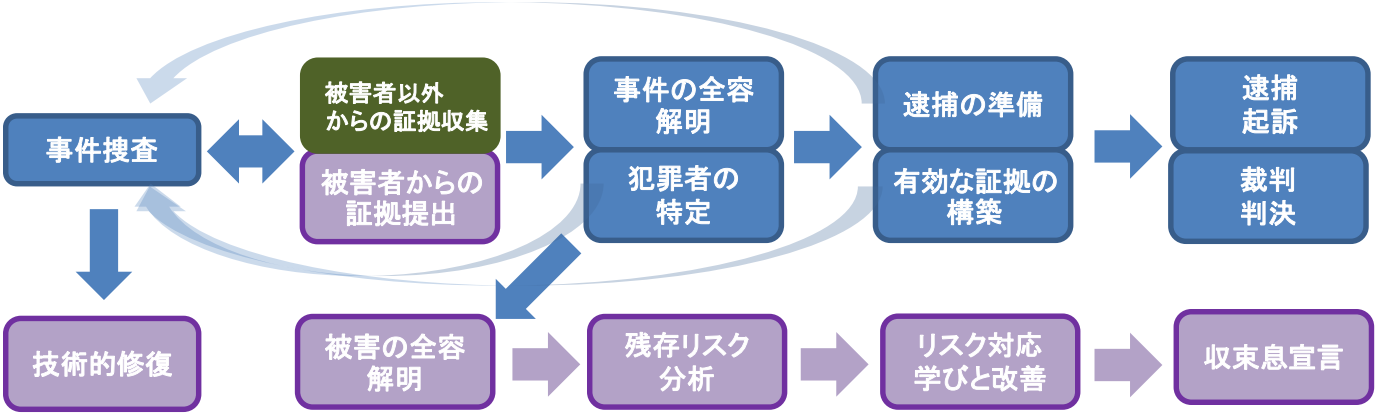
- サイバー犯罪事件の解決＝技術的修復ではない
- コアな関係者が正しい「解決」イメージを持つことが大切
- いざという時のための事前の準備を入念に行うこと

コミュニケーション上のポイント

考慮すべきポイント	留意しておくと良い点
法執行機関との関係性	あらかじめ**信頼関係を構築**しておく 米国（NCFTA）、英国（CDA)、日本（JC3）などが**参照すべき連携モデル**
情報開示の姿勢	**積極的な開示**を行った方が「信用」を傷つけないケースが増えている点 共有・開示**すること／しないことのリスク**を正しく評価・認識する
連携によるメリット	従前からの関係性構築に基づく初動を捜査の専門家を交えて実施することで**事件の実態を解明しやすくなり正しい最終処理に結びつく**
情報開示のタイミング	タイミングを間違えることで外部ステークホルダーや社会からの反感を買うことがある。**「いつ開示すべきか」をレッドブックで規定**する
情報開示の内容と当事者	「何時」だけではなく**「何を」**報告すべきか**「誰が」「誰に」**報告すべきかを事前に**レッドブックで規定**しておく
管轄官庁への報告	業種や罪体によっては**法的要件としての報告義務**を負っていることを認識しておく
秘匿すべき情報の扱い	外部に情報開示を行う場合に**秘匿すべき事項は何かを規定する**

最終解決へのプロセス

凡例：法執行機関　被害者組織



- 被害企業にとっての最大の課題は「残存リスク」
- 残存リスクに正しく対応するためにも全容解明が重要

被害企業にとっての事件の「収束」とは？

被害企業が事件の収束を判断するためには：

- ✓ 被害を受けた情報資産が何かの**特定**と、その**原因**が究明できている
- ✓ 利用された**脆弱性への対応**が完了している
- ✓ 被害を受けたITシステム・サービスが**復旧**している
- ✓ 被害を受けた**外部ステークホルダーへの対応**（計画）が完了している
- ✓ セキュリティやガバナンス強化計画が策定された（または完了した）

注意すべきこと：

- ✓ 特に情報漏洩が疑われる場合は上記のみでは不十分
- ✓ 漏洩した可能性のある情報に起因する**新たなリスクの想定**が不可欠
- ✓ 漏洩前提であらゆるリスク・シナリオを想定する必要がある
- ✓ WhoとWhyが解明していれば、シナリオ特定は比較的容易になる

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/

ご清聴ありがとうございました