

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



Cybercrime Investigation Body of Knowledge (CIBOK)

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

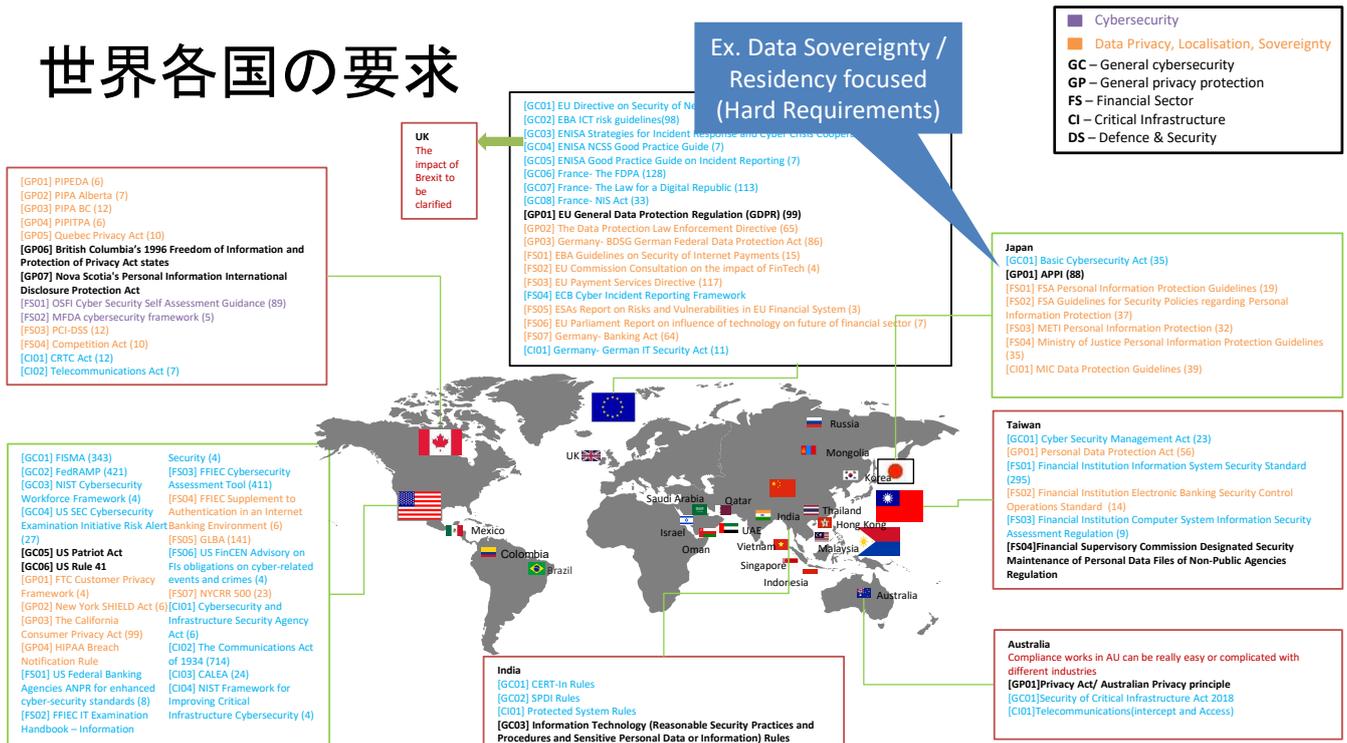
2. サイバー犯罪の高度化

- ① 進む分業化とダークウェブの役割
- ② ウィークストリンクを狙った犯罪の増加

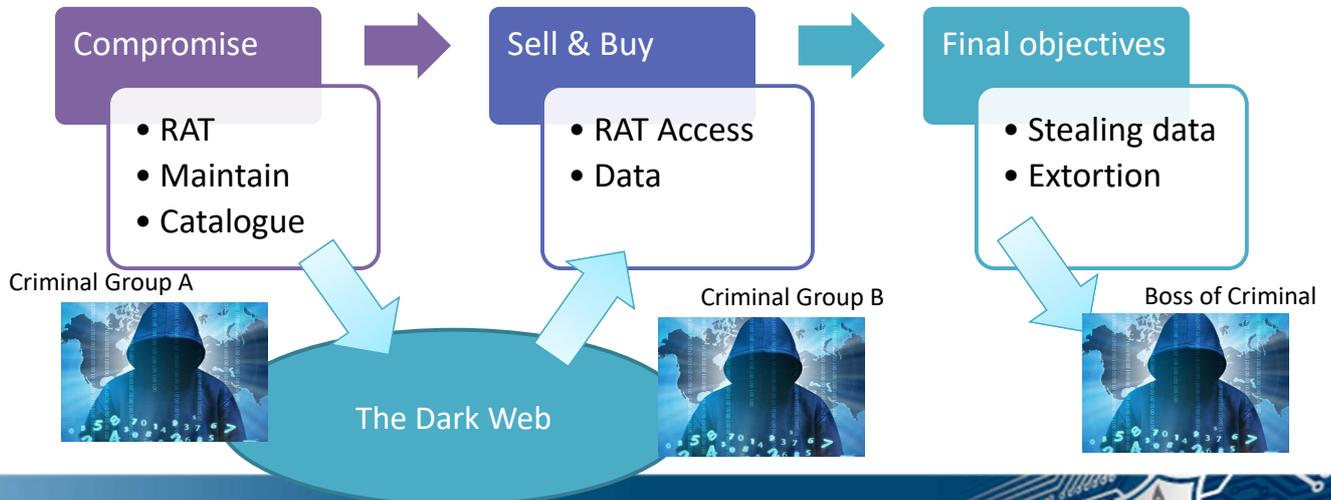
3. リスク・サーフェスの増加

- 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)

Normal Threads

	Redtone Malaysia phone DB	9	1,308
	by TintoBrazz ⌚ August 17, 2019 at 06:45 PM		
	Stresser Databases (Pages: 1 2)	12	1,228
	by TintoBrazz ⌚ August 17, 2019 at 05:35 PM		
	z3ddota.com 11,851 In Database	1	326
	by mester007 ⌚ November 10, 2019 at 10:19 PM		
	Taiwan data 670K	9	1,554
	by joadafad ⌚ May 09, 2020 at 03:17 AM		
	spawnpk.net 11k	1	355
	by barman3212 ⌚ January 14, 2020 at 08:27 AM		
	United Kingdom Consumer 180K (Name,Gender,Mobile,Email)	0	73
	by SuperDataMann ⌚ 3 hours ago		
	RUSSIA Consumer 900K Name/Telephone 2/Telephone 1/DOB/E-mail	0	81
	by SuperDataMann ⌚ 3 hours ago		
	TX1 margin.de dehashed database	1	165
	by davidbrombench ⌚ 8 hours ago		
	TX1 ScreenBlaze.com 261k [EMAIL]-[PASS]	1	237
	by rpatra ⌚ May 21, 2020 at 04:08 PM		

【参考】日本企業を狙う暴露型ランサムウェア被害状況

splunk>enterprise App: Search & Reporting

Phish Trends Alpha Version FakeStore Trends Alpha Version Databases Leaks Trends レポート サーチ ダッシュボード

「情報暴露型ランサムウェア」の被害

全時間

✓ 23 結果 (2020/11/20 15:11:34.000 より前)

23 results 100 件/ページ

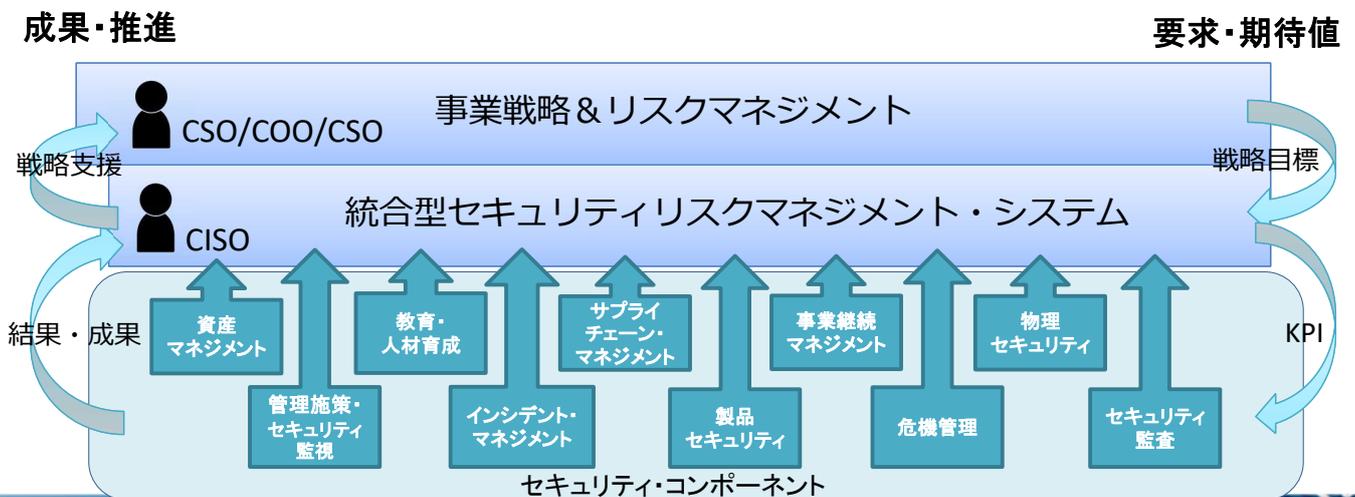
Published	Actor	Title	内容
2020/11/17 16:43	DoppelPaymer Ransomware Group	TANIGUCHI OIL CORPORATION	DoppelPaymerランサムウェア
2020/11/9 1:01	RagnarLocker Ransomware Group	Security breach of CAPCOM network	Ragnar Lockerランサムウェア
2020/11/6	DoppelPaymer Ransomware Group	Mitsubishi Polysilicon America Corporation	DoppelPaymerランサムウェア
2020/10/22	Revil Ransomware Group	SHIONOGI & CO., LTD Revenue \$3.01 billion	REvilランサムウェア (別)
2020/10/13	Egregor Ransomware Group	ADEKA Polymer Additives Europe	Egregorランサムウェアに
2020/10/13	Egregor Ransomware Group	NHK International Corporation	Egregorランサムウェアに
2020/10/9	Egregor Ransomware Group	AEON CO.	Egregorランサムウェアに
2020/9/26	Egregor Ransomware Group	Tekkenkensetsu Co., Ltd	Egregorランサムウェアに
2020/9/17	LockBit Ransomware Group		LockBitランサムウェアに

統合型モデル

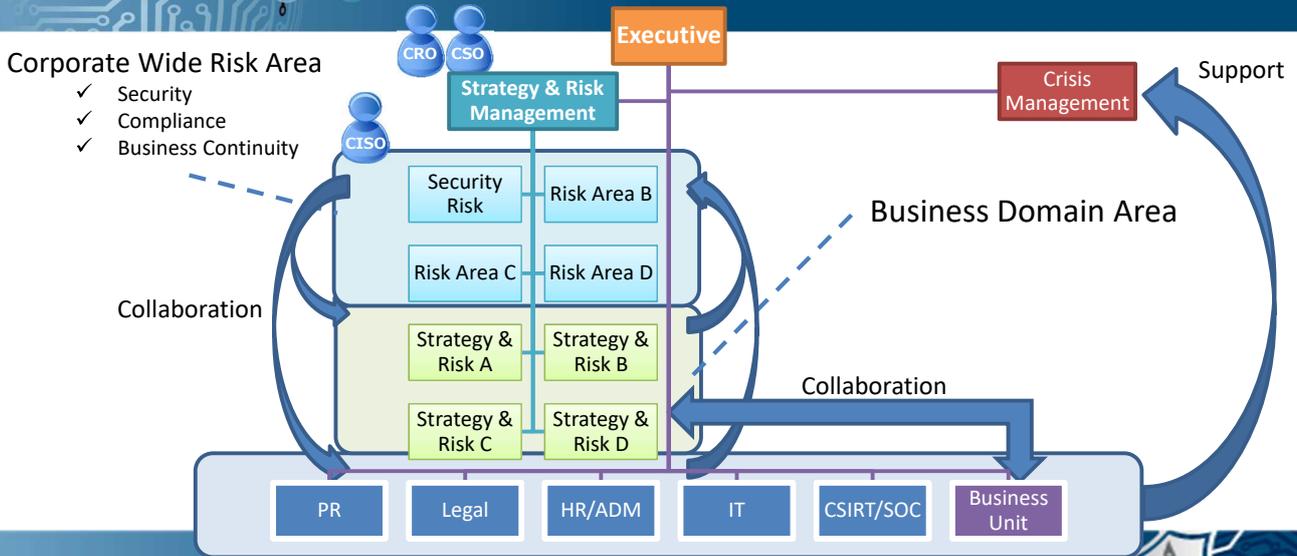
何と何を統合（一体化）させるべきか？

- ✓ 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）

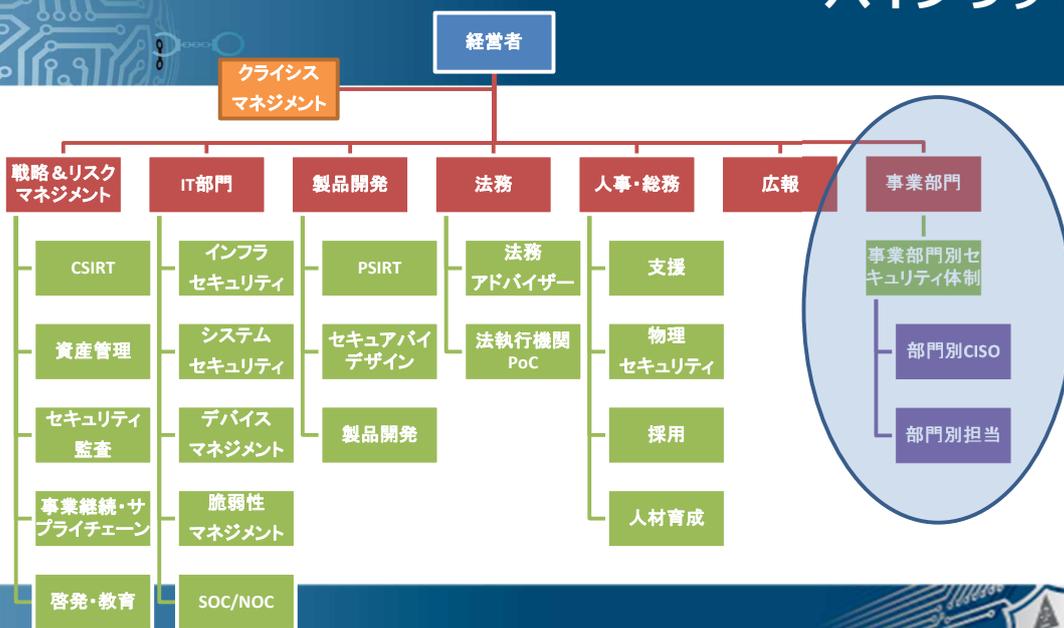
統合型セキュリティマネジメント



ハイブリッド・モデル



ハイブリッドの例



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

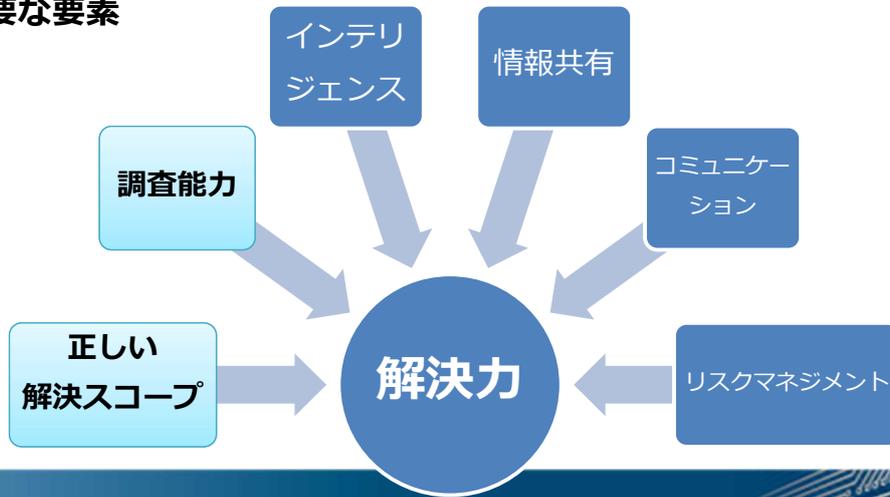
- 事件に正しく対処し影響を許容範囲内に抑え込むための組織能力

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

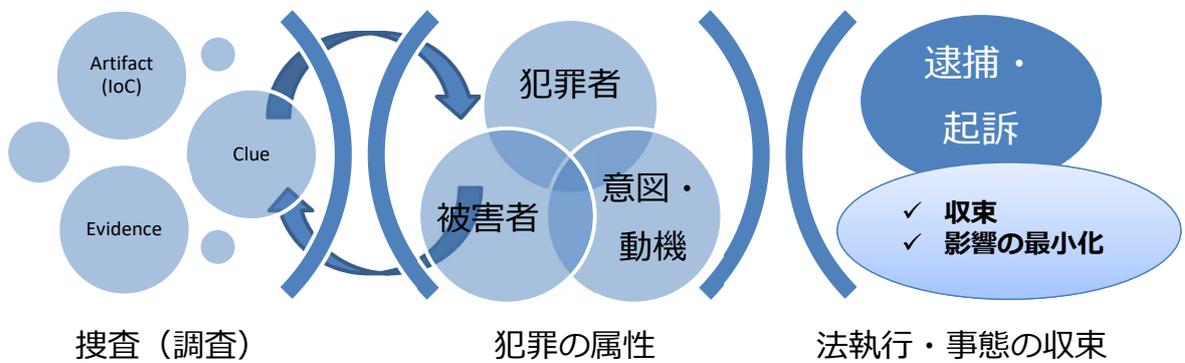


サイバー犯罪捜査（調査）とは？

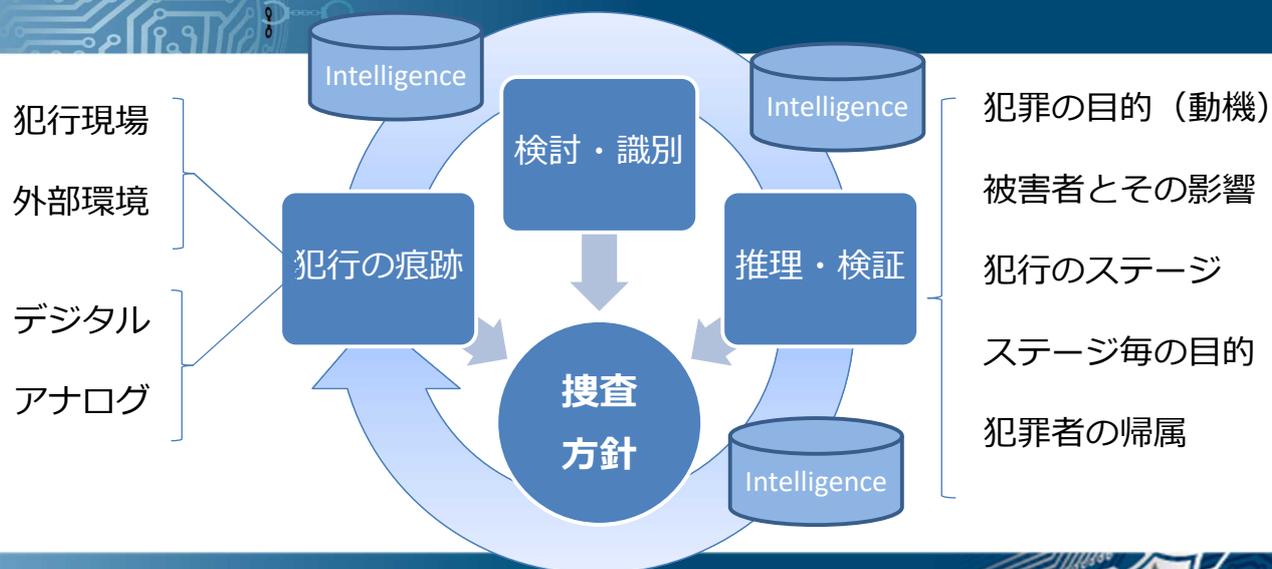
何が起きた(ている)のか？

誰が何のために？

最終解決



調査スコープの検討



17

Copyright © 2020 Cybercrime Investigation Knowledge Forum

スコープ検討のフレームワーク

□ 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）

□ 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

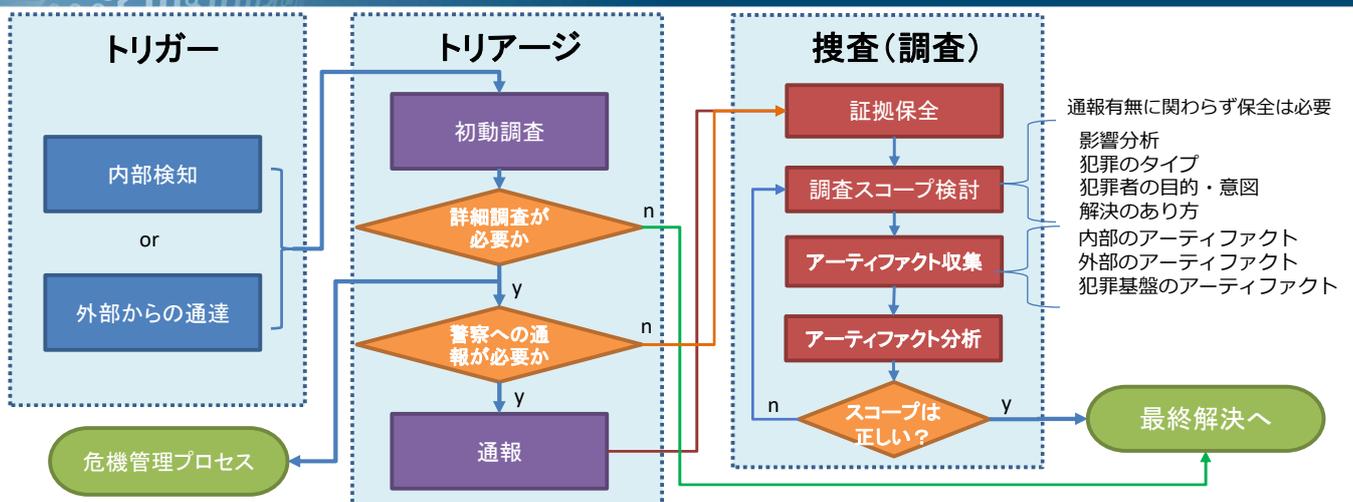
18

Copyright © 2020 Cybercrime Investigation Knowledge Forum

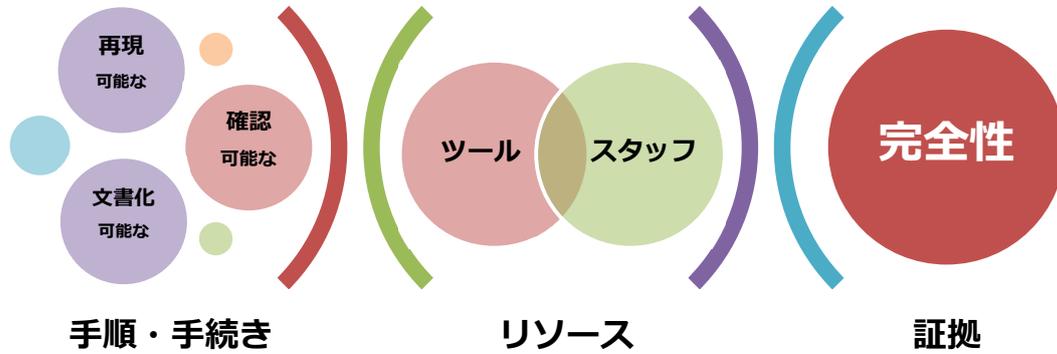
スコープ検討時の留意点

- ✓ 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

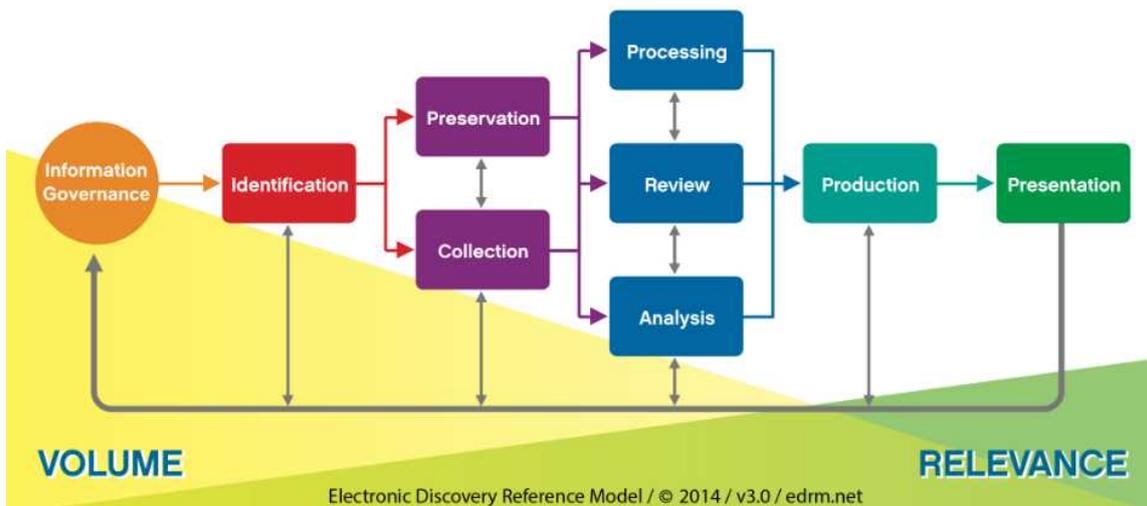
事件対応・全体の流れ



フォレンジックにおける証拠の完全性

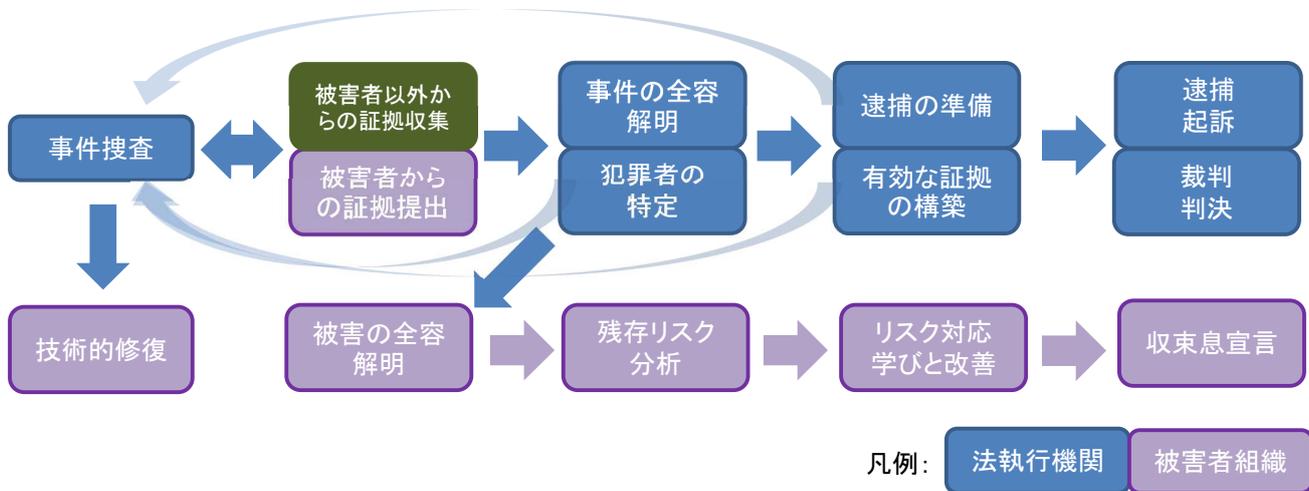


Electronic Discovery Reference Model (EDRM)



Source : Electronic Discovery Reference Model / EDM.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 Investigation Knowledge Forum

Any inquiries, please contact : secretariat@cibok.org

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