コラム6

セキュリティ評価を経営のリスクマネジメントに組み込む

共通対策評価フレームワーク分科会

2023年3月7日

CSIJ

Cyber Security Initiative for Japan

© 2023 CSIJ.

セキュリティリスクは経営リスク

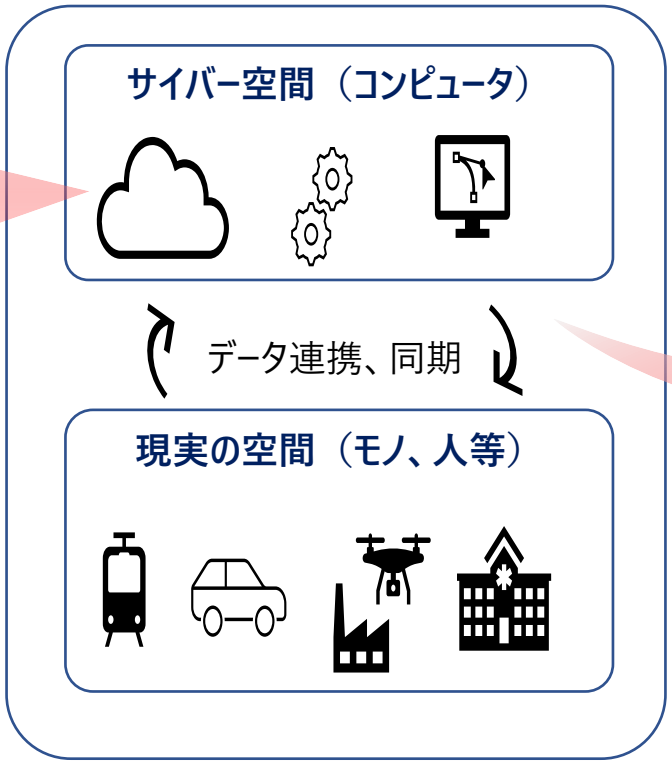
- サイバー攻撃対象はサイバー空間（コンピュータ等）のみならず現実の空間（モノ、人等）を含む広範囲におよんでいます。
- 被害が発生した場合の影響は深刻なものとなる恐れがあります。

攻撃脅威

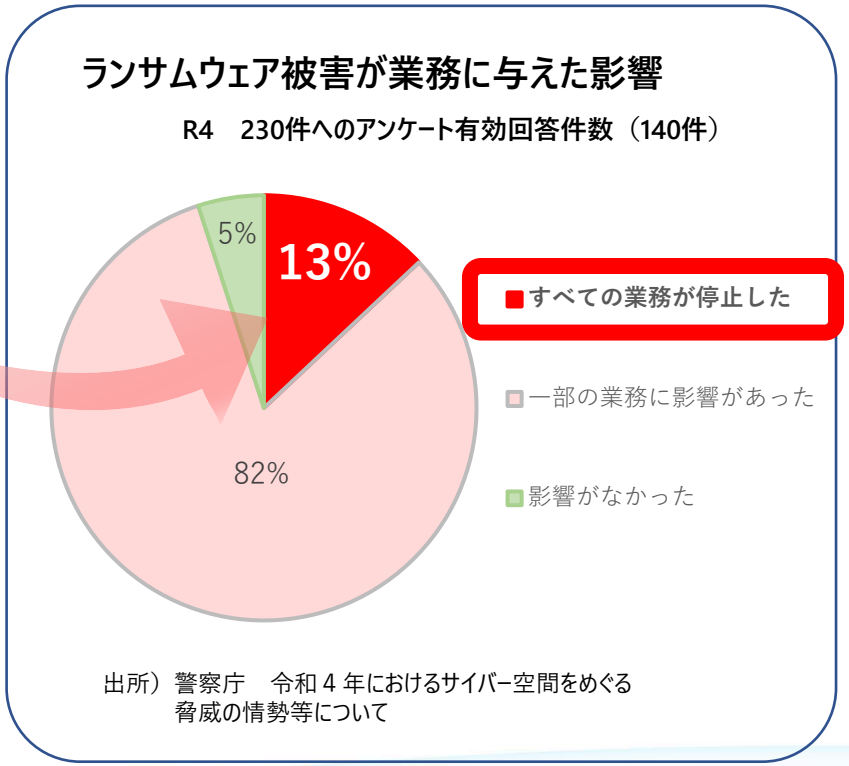
順位	組織
1	ランサムウェアによる被害
2	サプライチェーンの接点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏洩
5	テレワーク等のニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	ビジネスメール詐欺による会話被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏洩等の被害
10	犯罪のビジネス化（アンダーグラウンドサービス）

出所）IPA 独立行政法人 情報処理推進機構
情報セキュリティ10大脅威 2023

攻撃対象



影響



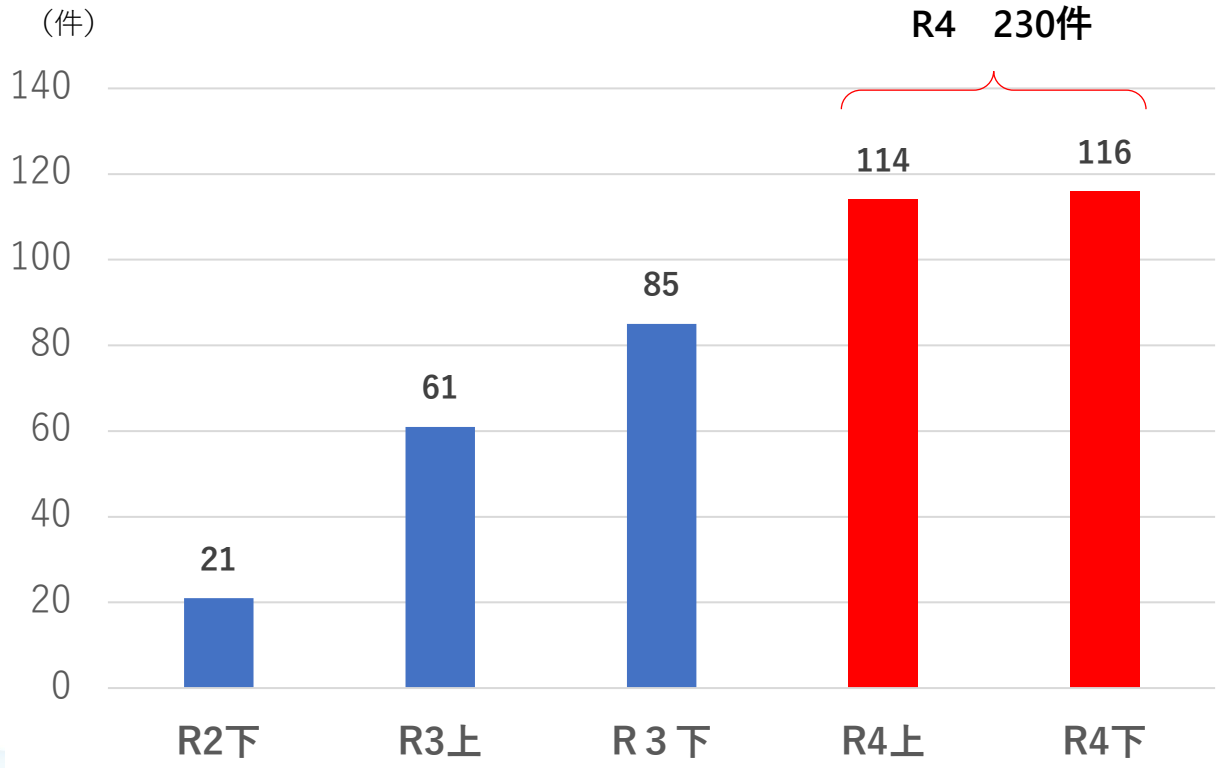
出所）警察庁　令和４年におけるサイバー空間をめぐる
脅威の情勢等について

ランサムウェア：「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼ぶ。（IPAの解説サイトhttps://www.ipa.go.jp/security/anshin/ransom_tokusetsu.htmlより）

狙われる中小企業

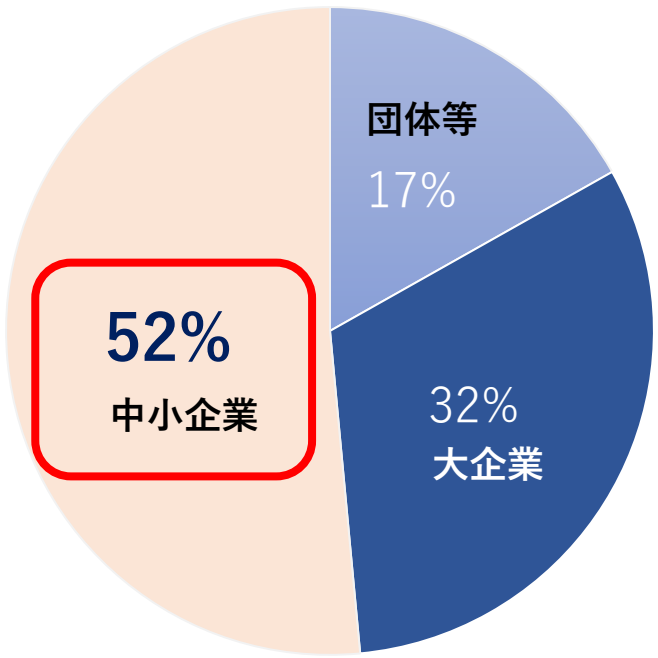
- サイバー被害（ランサムウェア被害）は右肩上がりに増加しています 。
- 令和4年の被害件数(230件)に占める中小企業の割合は121件（53%）と５割を占めます。

企業・団体等におけるランサムウェア被害の報告件数の推移



ランサムウェア被害企業等の規模別件数

R4　230件へのアンケート有効回答件数（140件）

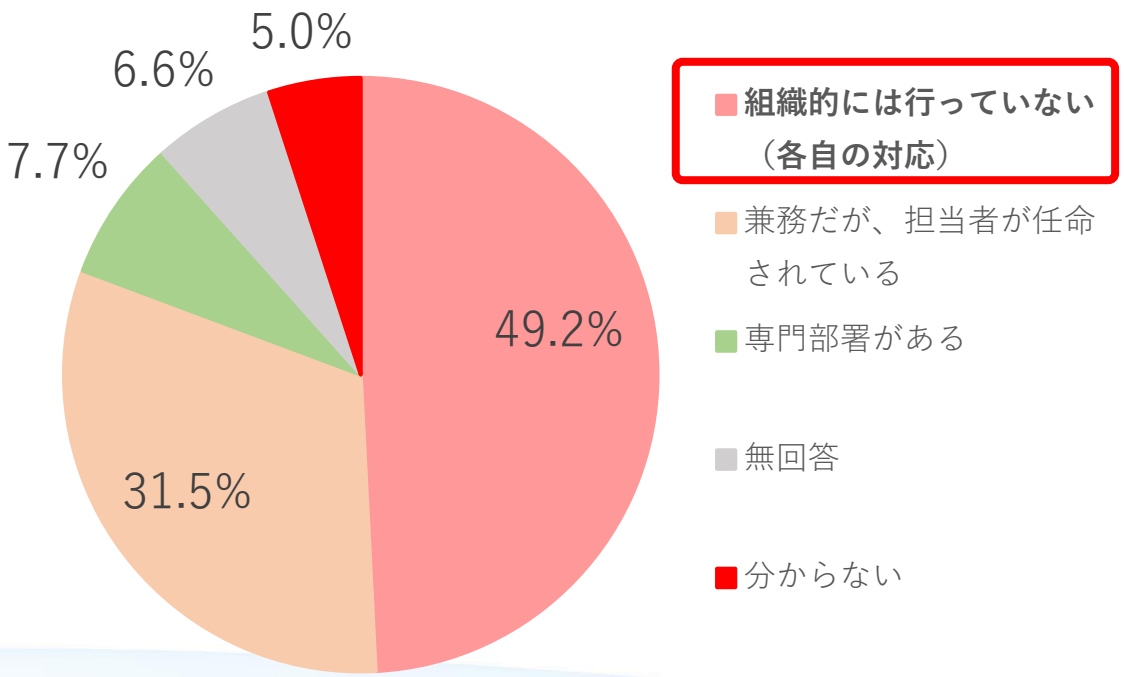


出所）警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について（令和4年9月15日）」

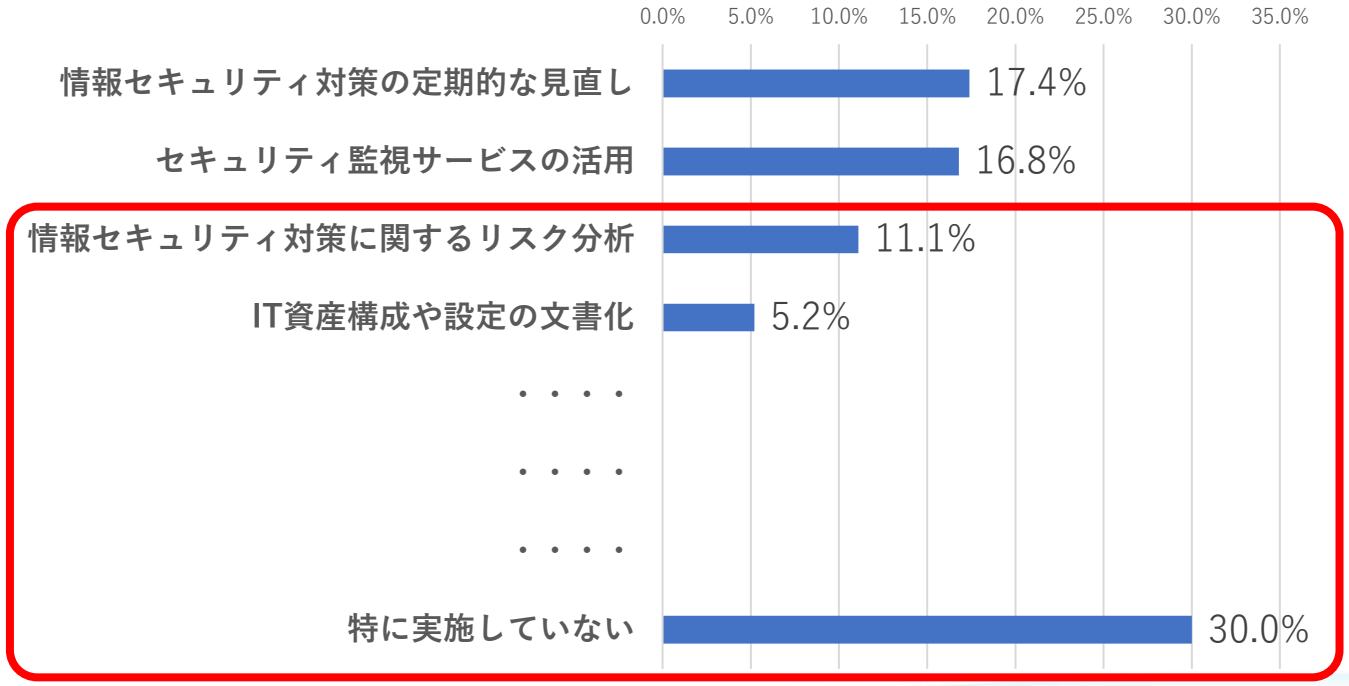
多くの中小企業はセキュリティのPDCAサイクル未確立

- IPA の調査によると、5 割弱の中小企業が情報セキュリティの対策を組織的に行っていません。
- 「情報セキュリティに関するリスク分析」が11.1%と自社でのリスク分析は低水準に留まっています。
- IT資産構成や設定の文書化もされておらずリスク分析を行う手前の現状把握ができていない中小企業が多く存在するものと想定されます。

情報セキュリティの組織体制



中小企業における被害防止のための組織面・運用面での対策（複数回答）



出所）内閣府「サイバー・フィジカル・セキュリティ 対策検討ガイドブック」（2023年2月）
IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」（2022 年 3 月）

評価フレームワークを活用してスモールスタートでPDCAを立ち上げる

- 評価フレームワークの評価レポートを活用することで、PDCAをスタートさせるためのPlanに必要な情報を得ることができます。
- 評価フレームワークはPDCA構築・運用の土台となる対策を厳選しているため、スモールスタートでPDCAを回し始めることができます。

■ 評価フレームワーク

- 状況を把握し対応方針と対策案を決める

➢ *Observe(観察)*

- 自社の現在のセキュリティレベルを確認する

➢ *Orientt(方向付け)*

- 対策強化方針を決める
例１：弱いカテゴリの対策強化を目指す
例２：他社平均レベルへの到達を目指す

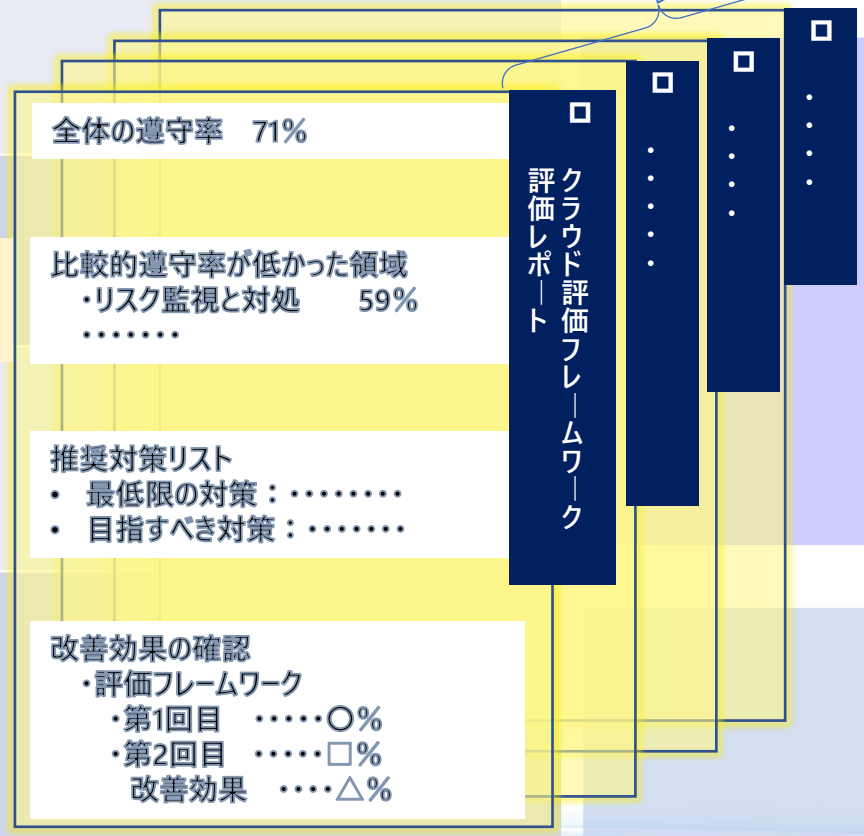
➢ *Decide(意思決定)*

- 対策を決める
—最低限の対策案を決める
—努力目標としての対策案を決める

➢ *ACT(行動)*

- 対策を実施して再評価してみる
—実施前後で、評価フレームワークの評価結果に改善がみられるかを確認する

評価フレームワークテーマ＊別の評価レポート
（＊今後、作成・発行予定）



■ PDCA

- 計画、目標に基づいて活動し継続改善を行う

➢ *Plan*

戦略	• 方針、目標、計画等
組織	• セキュリティ会議体設置・運営 セキュリティ教育、監査体制 • ルール・手順整備　等
技術	• 物理的、システム的対策
有事対応	• 異常／事故発生時対応体制 • BCP

➢ *Do*

➢ *Check*

➢ *ACT*

CSIJ会員企業のサービスを活用してPDCAの実効性を無理なく高める

- 評価フレームワークの評価レポートを活用して会員企業にご相談いただくことで、ゼロベースで会員企業にご相談いただく場合と比べ、PDCA確立のための実効的なサポートの提案をより短いリードタイムで受けることができます。

評価フレームワークの評価レポートをご活用いただくことで、**ゼロベースで相談する場合と比べて、より短いリードタイムで、より的確なサポートをCSIJ会員から受けることができます。**

情報発信、成果物公開等

各会員企業の事業としてサポート提案と提供

会員企業

- 対策評価アセスメント実施　・評価フレームワークを利用し対策評価
- ①セキュリティ機能実装　・新領域対象としたセキュリティ実装
- ②セキュリティオペレーション　・新領域対象としたセキュリティオペレーション
- ③プロフェッショナル人材教育・教育トレーニング

顧客企業

評価フレームワークによる
セキュリティ評価をご体験ください

評価フレームワーク（クラウド版）
を見てみる
⇒利用案内ページへ

CSIJ

Cyber Security Initiative for Japan

© 2022 CSI/J.