分科会活動報告
共通評価フレームワーク分科会

2023年1月24日

CSIJ

Cyber Security Initiative for Japan

CSIJ：活動概要

企業における「セキュリティレベルの向上」を目指し、クラウド、ゼロトラスト、IoT、サプライチェーン等の
新領域に対する「サイバーセキュリティ」対応を、セキュリティ業界横断で顧客企業への支援活動をおこなう

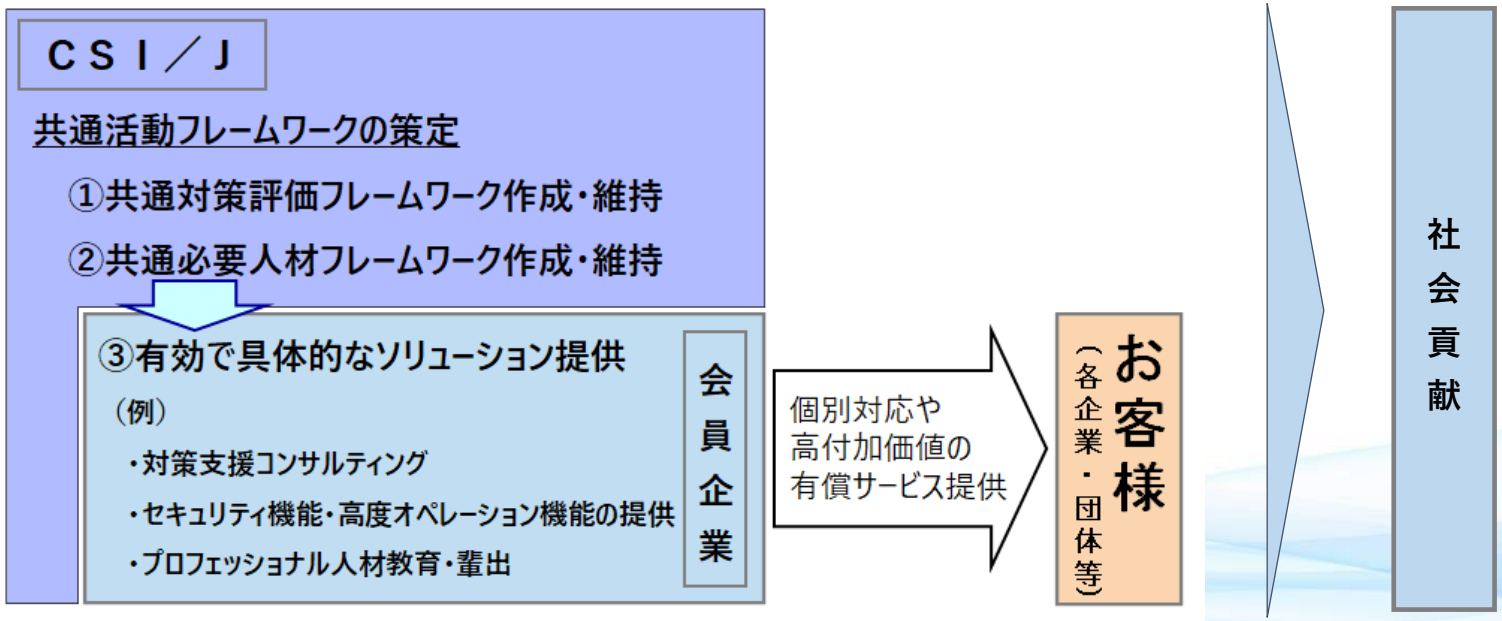
支援の切り口は以下の通り

①サイバーセキュリティ共通対策評価フレームワークの策定・維持

②共通必要人材フレームワークの策定・維持

③有効で具体的なソリューションの提供：会員企業（セキュリティベンダ）による

■活動概要



進捗状況

共通評価フレームワークについて（進捗状況）

現在公表しているWeb版と同等の内容で、属性に関する設問、対策状況を問う6領域42設問からなるExcel調査シートを用意し、Web版の提供に先立ち調査を行いました。

実施期間：**2022年7月～10月**

評価領域

Governance	クラウドの利用に関するルールの整備や教育の実施など、利用の前提となるガバナンス整備状況
Incident Responce	ログの取得やインシデント対応手順の整備等、インシデント発生時の対応準備状況
Compliance	レギュレーションに沿ったデータ保存国やその他契約等のコンプライアンス面の確認状況
Posture Management	クラウドサービスに関する設定や脆弱性の管理状況
ID Management	クラウドサービスに関する認証やアカウントの管理に関する整備状況
Data Protect	クラウドサービスに関するデータ保護や通信保護に関する対応状況

評価用アセスメント設問の構成：
・プロファイル
・本体
（Governance、 Incident Response 、Compliance、Posture Management、ID Management、Data Protect ）：42設問

先行調査にあたり22社様にご協力頂くことができました

ご協力頂いた組織の皆様、ありがとうございました

※ご回答頂いた内容は社名が判別不可能な状態でCSIJに提供し、統計データとして利用させていただくという前提でご協力をお願いしています。

共通評価フレームワークについて（進捗状況）

組織の規模が、クラウドのセキュリティ対策の遵守率に一部影響している可能性が推測できます。

売上規模別

遵守率（%）

	全体	Gov	Inc	Com	Pos	IDM	Dat
1億円未満	**63%**	0%	75%	69%	47%	71%	90%
1億～10億円未満	**62%**	53%	57%	66%	61%	70%	71%
10億～50億円未満	**71%**	55%	54%	67%	100%	90%	85%
50億～100億円未満	**65%**	36%	75%	75%	50%	64%	88%
100億～1000億円未満	**85%**	65%	90%	100%	66%	88%	94%
1000億～5000億円未満	**75%**	62%	76%	84%	58%	78%	88%
5000億～1兆円未満	-	-	-	-	-	-	-
1兆円以上	**68%**	-	75%	100%	50%	57%	70%
合計	**71%**	**52%**	**72%**	**80%**	**59%**	**77%**	**84%**

従業員規模別

遵守率（%）

	全体	Gov	Inc	Com	Pos	IDM	Dat
50人未満	**61%**	73%	44%	44%	63%	75%	65%
50～100人未満	-	-	-	-	-	-	-
100～300人未満	**66%**	42%	60%	65%	65%	84%	81%
300～1千人規模	**76%**	-	75%	100%	50%	93%	50%
1千～2千人未満	**66%**	15%	71%	88%	50%	74%	88%
2千～5千人未満	**79%**	70%	82%	83%	67%	84%	93%
5千～1万人未満	**70%**	67%	75%	75%	-	58%	80%
1万人以上	**76%**	-	84%	100%	51%	70%	89%
合計	**71%**	**52%**	**72%**	**80%**	**59%**	**77%**	**84%**

売上規模・従業員規模が大きいほど遵守率が高い

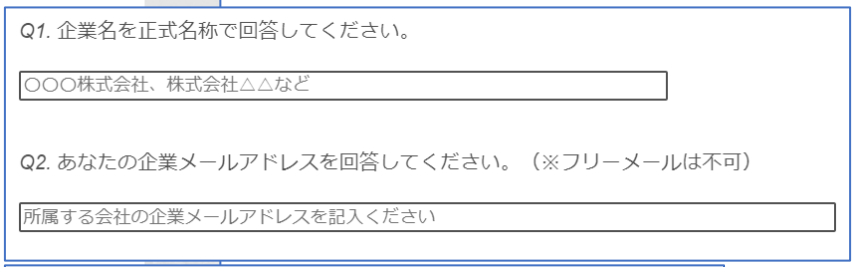
（ドメイン略称について）**Gov**:Governance　**Inc**:Incident Response　**Com**:Compliance
Pos:Posture Management　**IDM**:ID Management　**Dat**:Data Management

共通評価フレームワークについて（進捗状況：コラム）

参考：評価FW分科会 | CSIJ (csi-japan.org)

共通評価フレームワークについて（進捗状況：WEB版）

「リリース済」



次期フレーム（その①）

共通評価フレームワーク（クラウド版）を皮切りに、有用なフレームを次々と発信

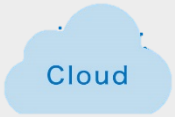
共通評価フレームワーク

【共通対策評価フレームワーク分科会】

第一弾

クラウド環境を利用しようと検討中の企業
クラウドを利用しているが、安全性に不安のある企業

- クラウドセキュリティのチェックを行う部署・担当の方
- クラウド利用を検討・推進している部署・担当の方
- クラウドサービスの企画、推進を行う方
- 情報システム部門のリーダー、担当者　など



共通必要人材フレーム

【サイバーセキュリティプロフェッショナル人材フレームワーク分科会】

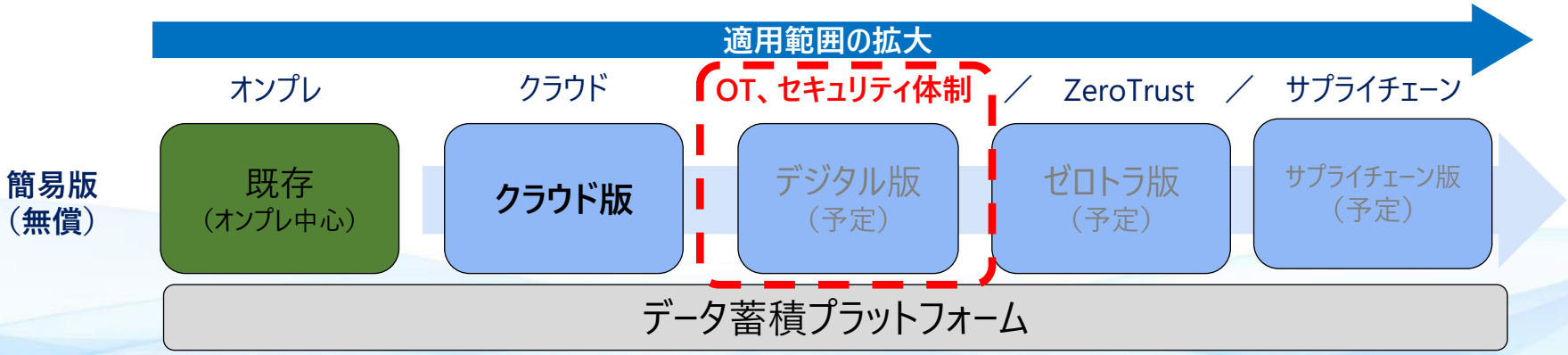
セキュリティ人材の正確な価値を見える化
優良なセキュリティ人材の健全な育成

- セキュリティ人材の正確な価値を知りたい方
- 優良な人材を所属する企業を選ぶ担当の方
- 優良人材（特にエンジニア）になりたい、育成したい方
- 人事部門長、セキュリティ人材育成担当者　など

今後も共通評価フレームワークは拡大していきます

適用範囲をクラウドから環境変化・市場ニーズに合わせ拡大

お客様の現実的な実装に向けて、会員企業が用意する各ソリューションにて推進・支援してまいります。



次期共通評価フレームワークについて

近年の情報セキュリティ情勢

「情報セキュリティ10大脅威 2022」の組織編によると、サイバー攻撃（ランサムウェアによる被害・標的型攻撃）が2021年に引き続き、2年連続1位・2位となっています。

順位	情報セキュリティ10大脅威 2022　組織	昨年順位
1位	**ランサムウェアによる被害**	1位 ➡
2位	**標的型攻撃による機密情報の盗取**	2位 ➡
3位	サプライチェーンの弱点を狙った攻撃	4位 ⬆
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位 ⬇
5位	内部不正による情報漏えい	6位 ⬆

「情報セキュリティ10大脅威」とは、前年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、 IPA（独立行政法人 情報処理推進機構）が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約150名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

出典）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 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

日本の製造業でもサイバー攻撃が増加

2022年 2月
トヨタのサプライアがサイバー攻撃受け、システム・ネットワークを全て停止したことにより、トヨタの全工場（日本国内全14工場、28ライン）が生産を停止。

2022年 1月
ドイツの石油会社がサイバー攻撃により操業停止

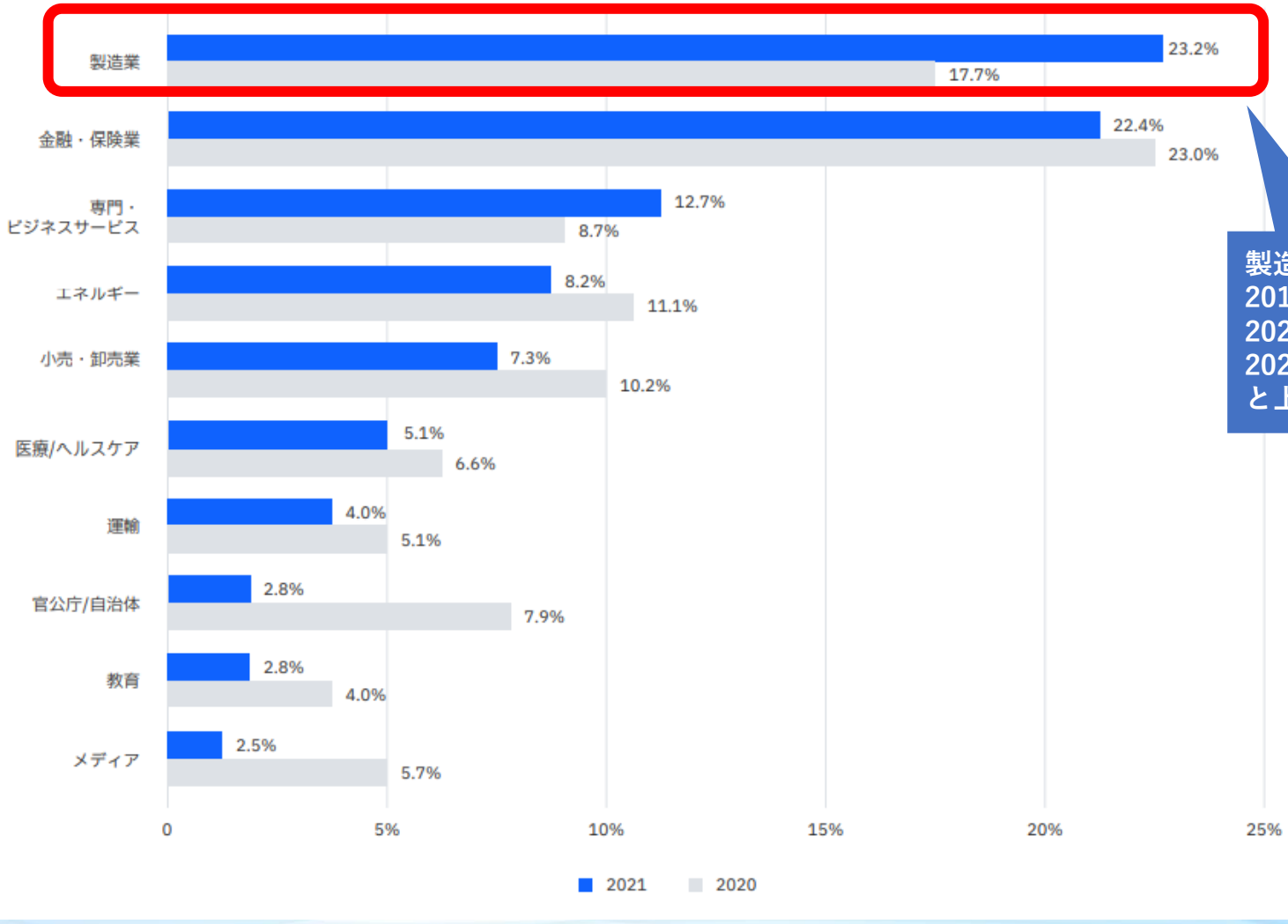
2020年6月
ホンダ社内サーバがサイバー攻撃受け、システム障害が発生。国内外の工場へ被害が広がり、世界の工場で生産停止。

2019年 2 月
HOYAタイ工場のシステムが、サイバー攻撃を受け、多数のパソコンがウイルスに感染し、レンズ生産ラインの一部が 3 日間停止。

＜X-Force（IBM社のセキュリティー研究開発機関）発表＞
2021年に最もランサムウェアの攻撃が多かったのは製造業
→　X-Forceが対処を支援した攻撃の61%にあたる

製造業が一番狙われている

攻撃対象となった上位10の業界



製造業は
2019年：8位
2020年：2位
2021年：1位
と上昇

出典：IBM

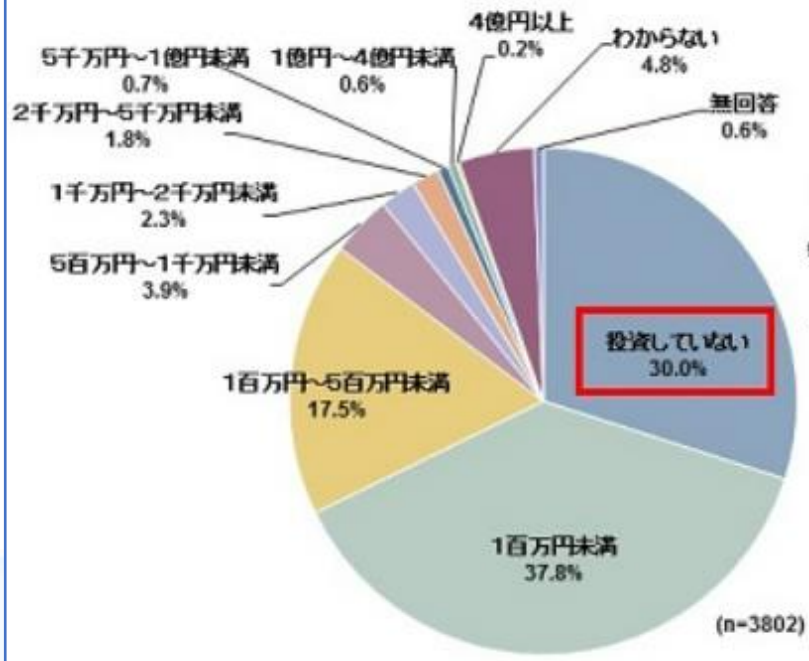
次期フレーム（その②）

中小企業のセキュリティ対策状況

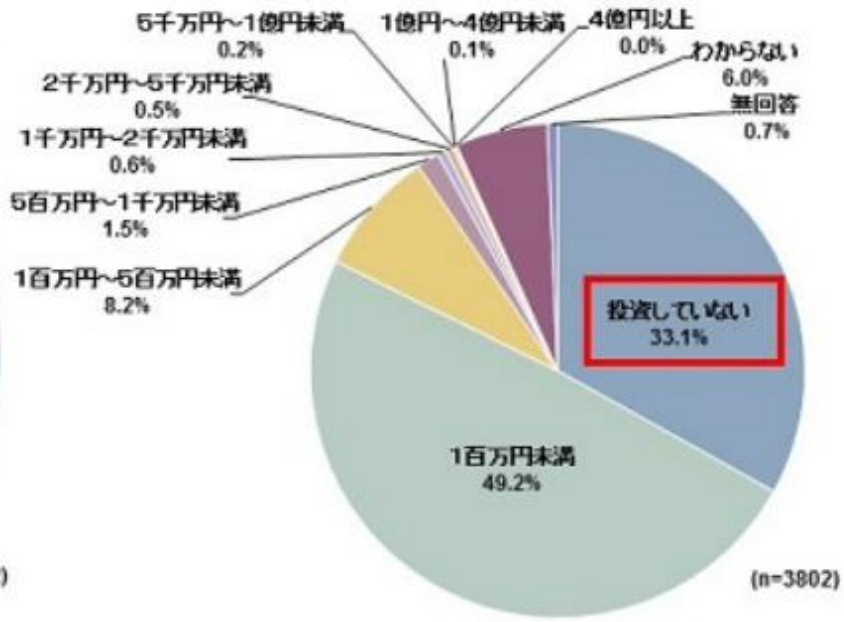
・大手（メガ）企業・・・すでに対応済み
・**中小企業・・・未開拓が多い**

過去3期

IT投資額



情報セキュリティ対策投資額

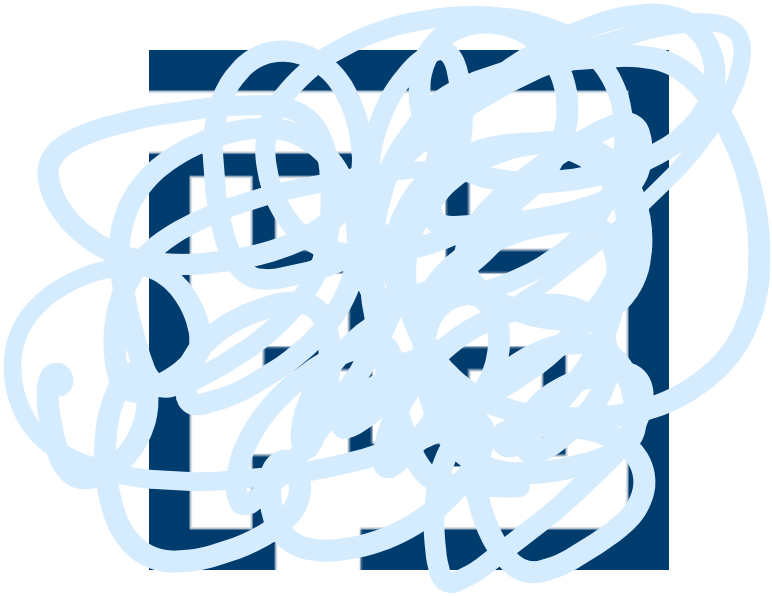


参考：「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について：IPA 独立行政法人 情報処理推進機構

次期共通評価フレームワークについて

昨今の幅広いセキュリティ対策が求められより多くの選択肢により、何から手を付けるべきか、どこまで対策を講じるべきか分からない という企業が多く存在する

Fog of More（膨大な選択肢による混沌）によって、セキュリティ対策迷子になっている可能性があります。



あれもこれもやらなければ、と
迷子になっている

根本にある問題を
発見することで…

効率的に対策をすることができる

Thank you. Any Questions ?