トレンドマイクロ ホワイトペーパー

サイバーセキュリティリスク意識調査レポート（日本）

「Cyber Risk Index」2021 年下半期版

»

Cyber Risk Index とは

トレンドマイクロは企業・組織のサイバーセキュリティリスクの状況を可視化するために、調査会社 Ponemon Institute と共同で国際的な意識調査を行いました。本調査ではさまざまなサイバー攻撃に対する組織の準備体制とサイバー脅威の環境を評価することで、サイバー攻撃への対応力を示す指数を導き出します。

本調査は幅広い業種における IT セキュリティ関与者を対象としており、2018 年に調査を開始してから 5 年目となります。調査の対象地域は北米、欧州、アジア太平洋、中南米と年々拡大し、最新の 2021 年下半期（7 月～12 月）の調査より日本が調査対象地域として含まれています。

本調査では、Cyber Risk Index（以下、CRI」）という指数をもとに、組織のサイバーリスクを算出します。CRI は、サイバー攻撃への組織の準備体制を評価する Cyber Preparedness Index（以下、CPI）と組織を取り巻くサイバー脅威の環境を評価する Cyber Threat Index（以下、CTI）で構成されます。調査対象の組織は CPI 全 31 問、CTI 全 10 問の設問に対して回答を行います。各回答にはポイント(10p、7.5p、5p、2.5p、0p)が付与され、CPI、CTI それぞれの回答の合計の平均値から指数が算出されます。CRI は CPI から CTI を引いて算出することで、組織におけるサイバー攻撃への準備体制とサイバー脅威の環境のギャップを指数として示します。CRI が高いほど、組織を取り巻くサイバー脅威に対して準備体制が整っていることを示します。一方で、CRI が低いほど、サイバー脅威に対する準備体制が整っておらず、組織のサイバーリスクが高いことを示します。

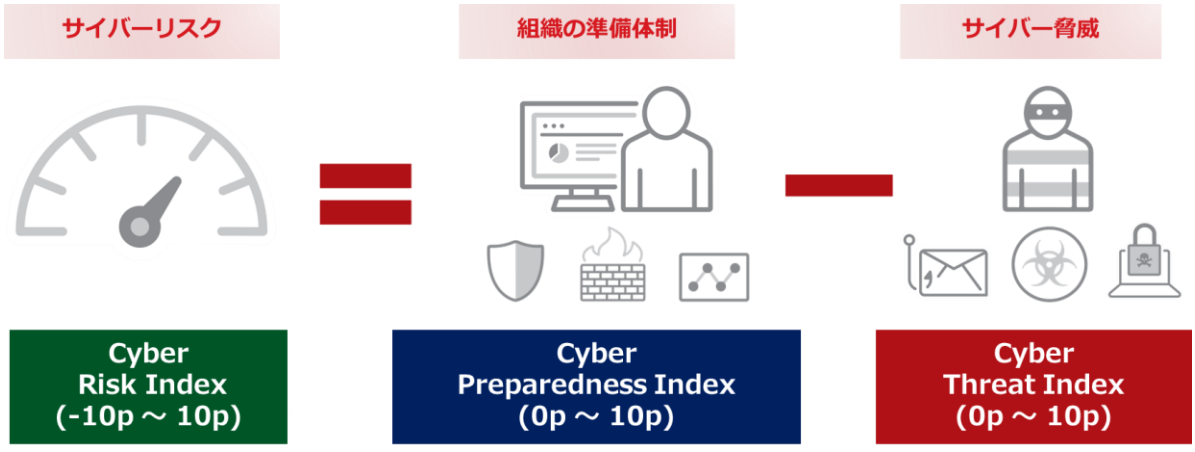

図 1：Cyber Risk Index の算出イメージ

2021 年下半期 Cyber Risk Index 調査において、日本は全 29 ヵ国中 9 位

2021 年下半期における調査では、全 29 の国と地域における 3,441 組織の IT セキュリティ関与者からサイバーセキュリティリスクに関わる設問の回答を得ています。日本では 88 組織から回答を得ています。日本における回答者のうち、約半数（48%）がマネージャ以上の役職であり、セキュリティに関する対策や投資を行う権限を持っています。

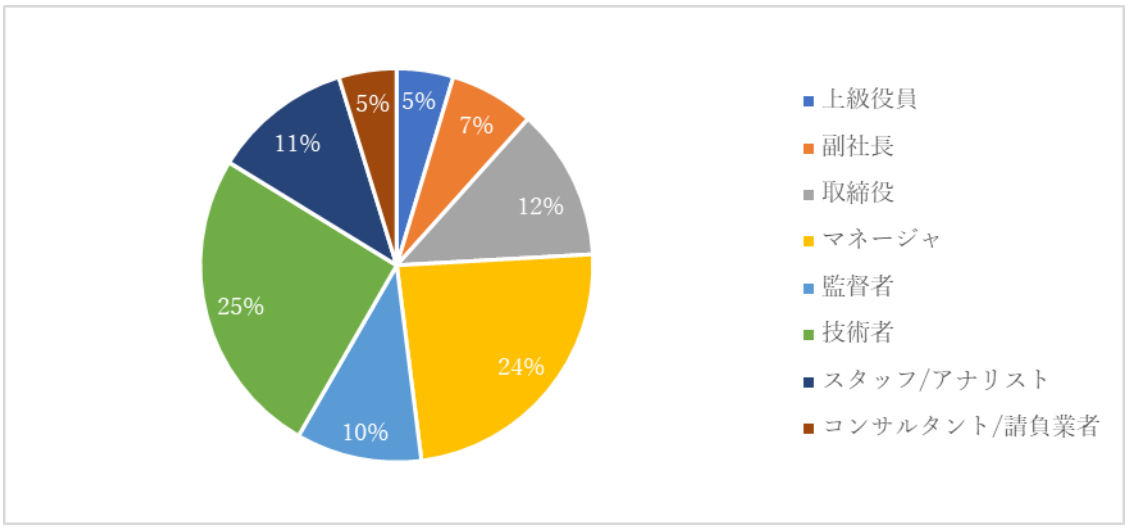

図 2：回答者の役職（日本）

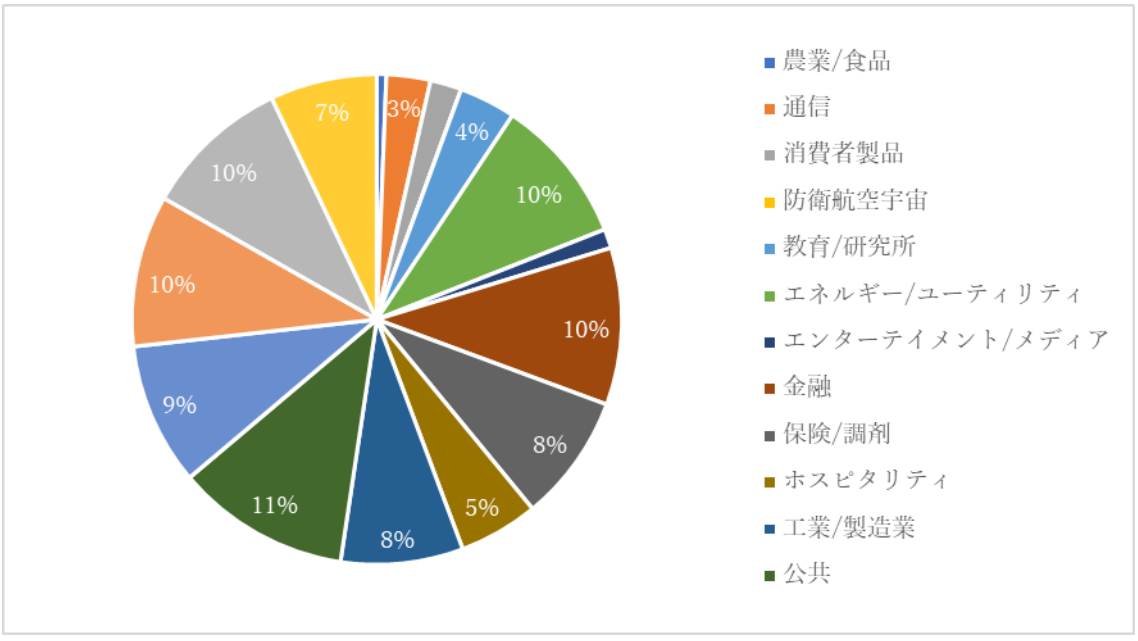

図 3：回答者の業種（日本）

組織のサイバーリスクを示す CRI の結果を、各国・地域単位で集計したところ、日本は 29 ヵ国のうち、9 番目に高い結果となりました。つまり、組織を取り巻くサイバー脅威に対して準備体制が整っている国ということになります。また、サイバー脅威に対する準備体制を示す CPI でも 9 位、組織を取り巻くサイバー脅威の状況を示す CTI では 17 位となりました。

No.	国	Cyber Risk Index	Cyber Preparedness Index	Cyber Threat index
1	台湾	0.53	5.46	4.93
2	マレーシア	0.37	5.45	5.08
3	インド	0.35	5.39	5.04
4	台湾	0.23	5.31	5.08
5	インドネシア	0.22	5.42	5.20
5	ベトナム	0.22	5.27	5.05
7	フィリピン	0.18	5.49	5.32
8	カナダ	0.16	5.41	5.25
9	**日本**	**0.15**	**5.29**	**5.14**
10	オーストラリア	0.06	5.28	5.22
23	米国	-0.18	5.29	5.47
	全体	-0.04	5.18	5.22

図 4：Cyber Risk Index(CRI)における上位 10 ヵ国、米国、全体

本調査の結果から、他国と比較して、日本はサイバー脅威に対する準備体制に関する意識は高いものの、IT セキュリティ投資分野や実際のサイバー脅威に関するリスクの把握などに関していくつかの点で改善が必要と考えられる点が見られました。

日本は IT セキュリティ予算を、実際のサイバー攻撃の防御策に割けていない

日本とその他の地域における組織の IT セキュリティ予算や経営層の関与に関する設問の結果を比較すると、日本の組織における「IT セキュリティに関する予算の十分さ」は 4.71 となっており、他の地域と比べて低い結果となっています。この結果は、日本の「CEO や取締役会の積極的な IT セキュリティへの関与度」が 4.57 であり、北米 6.53 や欧州 6.48 など他の地域と比べて低いことと無関係ではないと言えるでしょう。

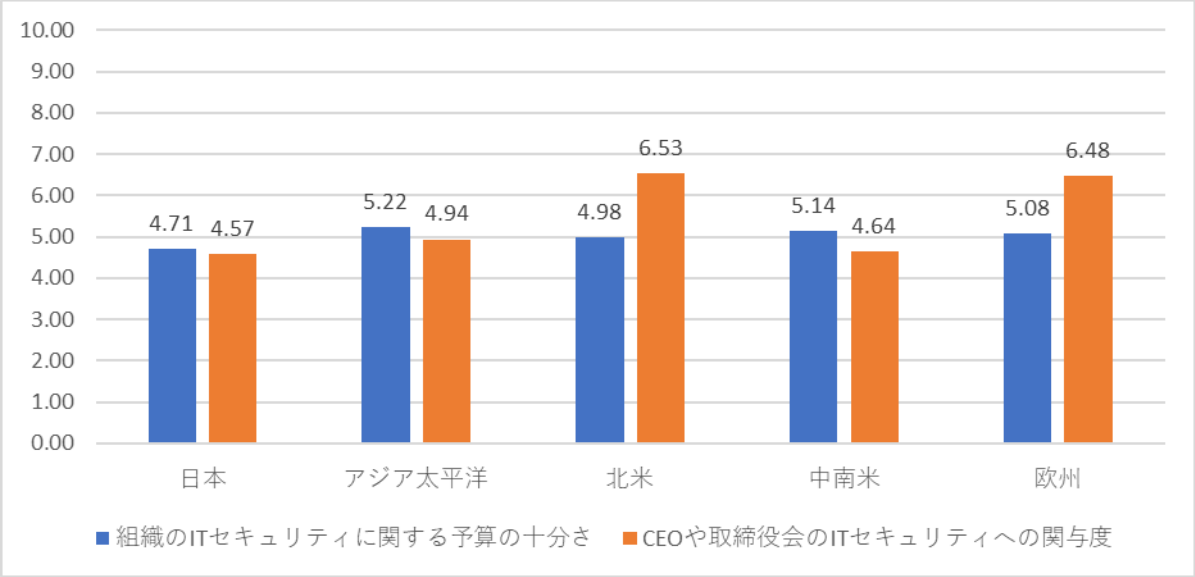

図 5：IT セキュリティの予算の十分さと CEO/取締役会の IT セキュリティへの関与度

組織のセキュリティ対策に関する設問の結果では、日本の DR/BCM(Disaster Recovery/Business Continuity Management)環境といった災害復旧や事業継続に関わる対策が 8.82、データ/プライバシー保護やコンプライアンス遵守といったレギュレーション対応が 6.57 であり、それぞれ他の地域よりも重点的に対策が行われている傾向にあることがわかります。災害復旧に関わる対策の意識が高い傾向については、日本は災害が発生する頻度が高い国であり、過去の経験から DR や BCM 環境は事業継続に重要な環境であると認識していることから、限られた IT セキュリティ予算の多くを割り当てていると考えられます。

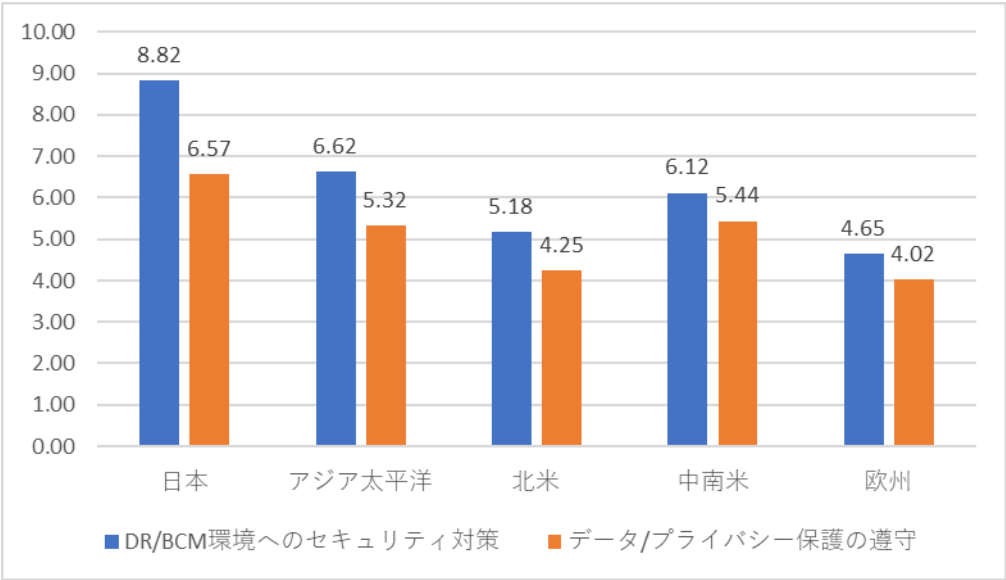

図 6：DR/BCM 環境、データ/プライバシー保護へのセキュリティ対策

一方で、機械学習や AI(Artificial Intelligence、人工知能)など最先端のセキュリティ技術への投資は 3.78、脅威や脆弱性を特定するための監査や評価が 3.45 となっており、災害復旧やレギュレーション対応に比べて対策への意識が低いことが示されています。

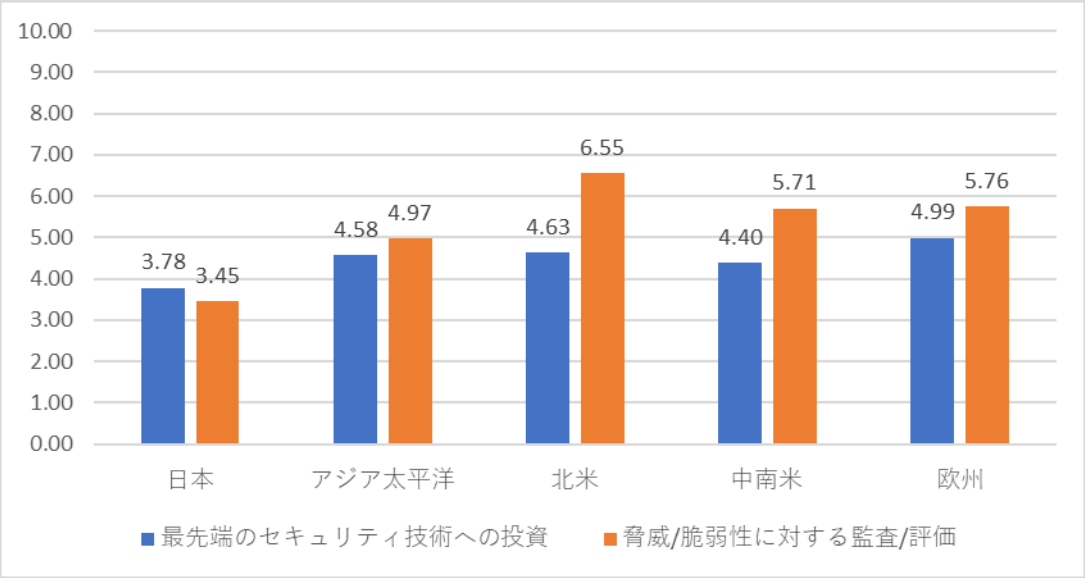

図 7：最先端のセキュリティ技術への投資、脅威/脆弱性に対する監査/評価

各組織における IT セキュリティ予算には限度があるため、現在行われているセキュリティ対策への投資が適切な分野に割り当てられているか再度検討してみる必要があるかもしれません。

日本は他の地域に比べて、ランサムウェアへの懸念が低い

組織を取り巻くサイバー脅威の環境についても、日本と他の地域を比較すると、脅威に対する懸念に違いがあることがわかります。今後 12 か月以内に組織で発生する可能性のあるサイバー脅威について、北米や欧州においては「ランサムウェア」が最も懸念される脅威であるという結果に対して、日本では「フィッシング詐欺/ソーシャルエンジニアリング」が最も懸念される脅威であるという結果になりました。

順位	日本	アジア太平洋	欧州	中南米	北米
1位	フィッシング詐欺/ソーシャルエンジニアリング (7.41)	フィッシング詐欺/ソーシャルエンジニアリング (6.91)	ランサムウェア (6.89)	クロスサイトスクリプティング (6.30)	ランサムウェア (8.30)
2位	ファイルレス攻撃 (6.83)	ボットネット (6.71)	フィッシング詐欺/ソーシャルエンジニアリング (6.74)	ファイルレス攻撃 (6.26)	DoS攻撃 (7.38)
3位	ボットネット (6.67)	ファイルレス攻撃 (6.34)	ボットネット (6.60)	DoS攻撃 (6.00)	フィッシング詐欺/ソーシャルエンジニアリング (7.28)
4位	ランサムウェア (6.34)	ランサムウェア (6.13)	標的型攻撃/APT (6.55)	ボットネット (5.71)	中間者攻撃 (6.28)
5位	中間者攻撃 (6.29)	DoS攻撃 (6.03)	DoS攻撃 (6.42)	DNSベースの攻撃 (5.71)	標的型攻撃/APT (6.13)

図 8：今後 12 か月以内に組織で発生する可能性のあるサイバー脅威 TOP5

日本におけるランサムウェアに対する懸念が 6.34 であるのに対し、北米では 8.30 と差がある結果となっています。この結果から、組織を取り巻くサイバー脅威における懸念の対象が、前章で述べた最先端のセキュリティ技術への投資や、脅威・脆弱性を特定するための監査や評価への意識の低さに繋がっていることが考えられます。

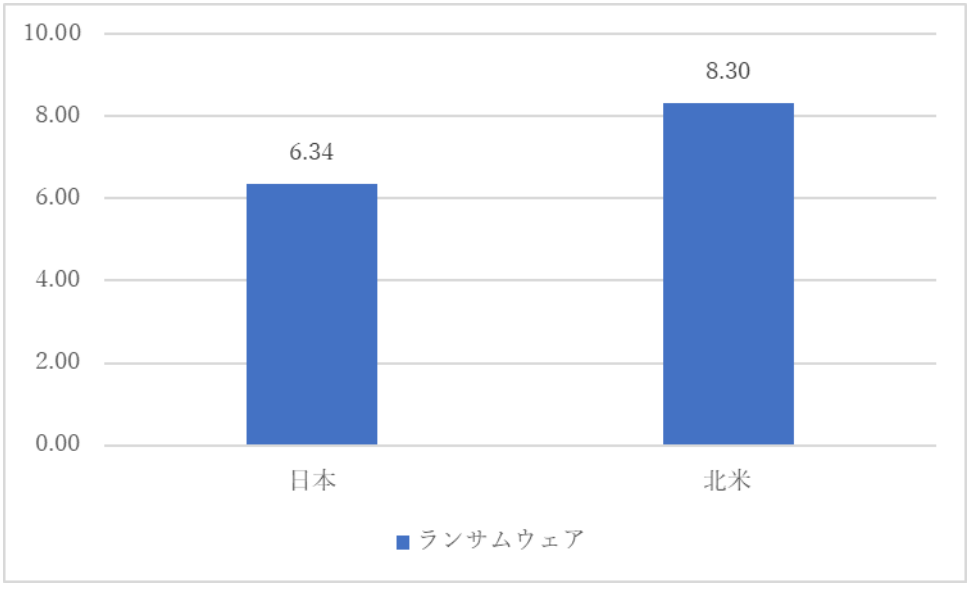

図 9：今後 12 か月以内に組織で発生する可能性のあるサイバー脅威(ランサムウェア)

日本はサイバー攻撃の実害を「物的損害」とみなしている傾向がある

サイバー攻撃に起因する実害について、日本の組織は設備に対する盗難やダメージが引き起こされることに大きな懸念がある傾向があることがわかります。これは日本が世界的にも自然災害に遭いやすいことなどから、サイバー攻撃による実害も自然災害と同様に「物損を伴う災害」と捉えられているものと思われます。

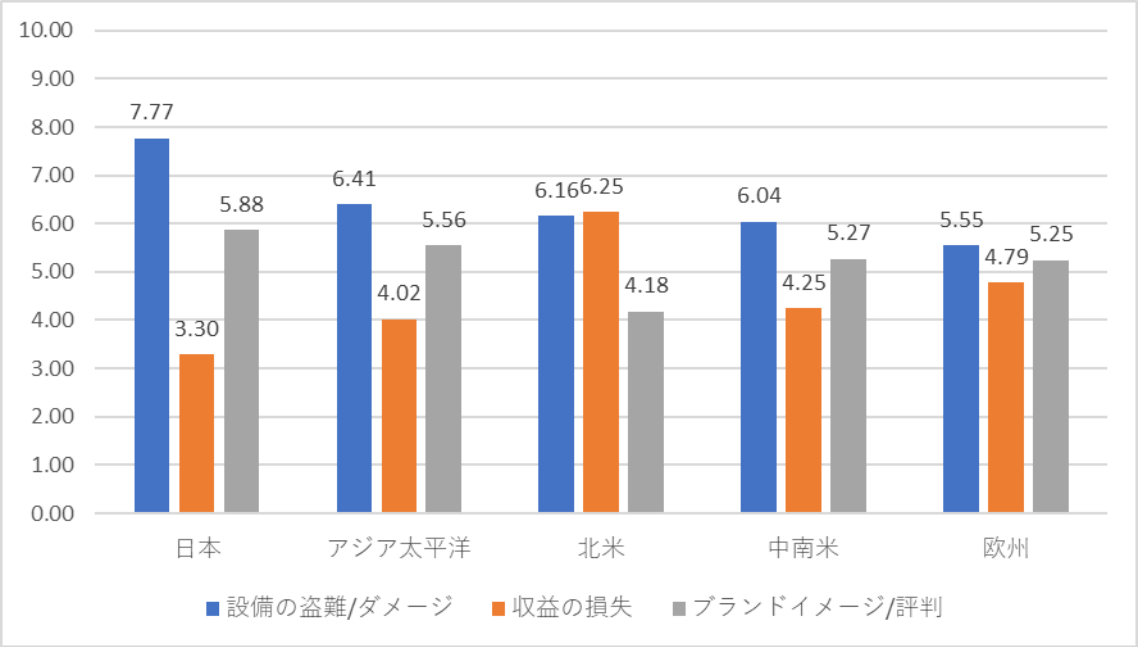

図 10：サイバー攻撃によって想定される実害

一方で、「ブランドイメージの低下」は他の地域よりも高いものの、「収益の損失」といった事業の継続性に関わる被害に対しては懸念が低いという結果になっています。実際のサイバー攻撃においては、企業のシステムが侵害されることによる生産システムの停止など、事業継続に影響が出るケースも確認されているため、収益という重要な要素も考慮に入れたうえで、想定されるさまざまな被害について配慮したセキュリティ体制を検討する必要があります。

セキュリティリスクを最も懸念する環境はクラウドインフラストラクチャ

日本において、組織の IT インフラストラクチャのなかで最もセキュリティリスクが存在する可能性のある環境は、クラウドインフラストラクチャ及びクラウドプロバイダとなっており、2 番目がモバイル/リモート従業員となっています。

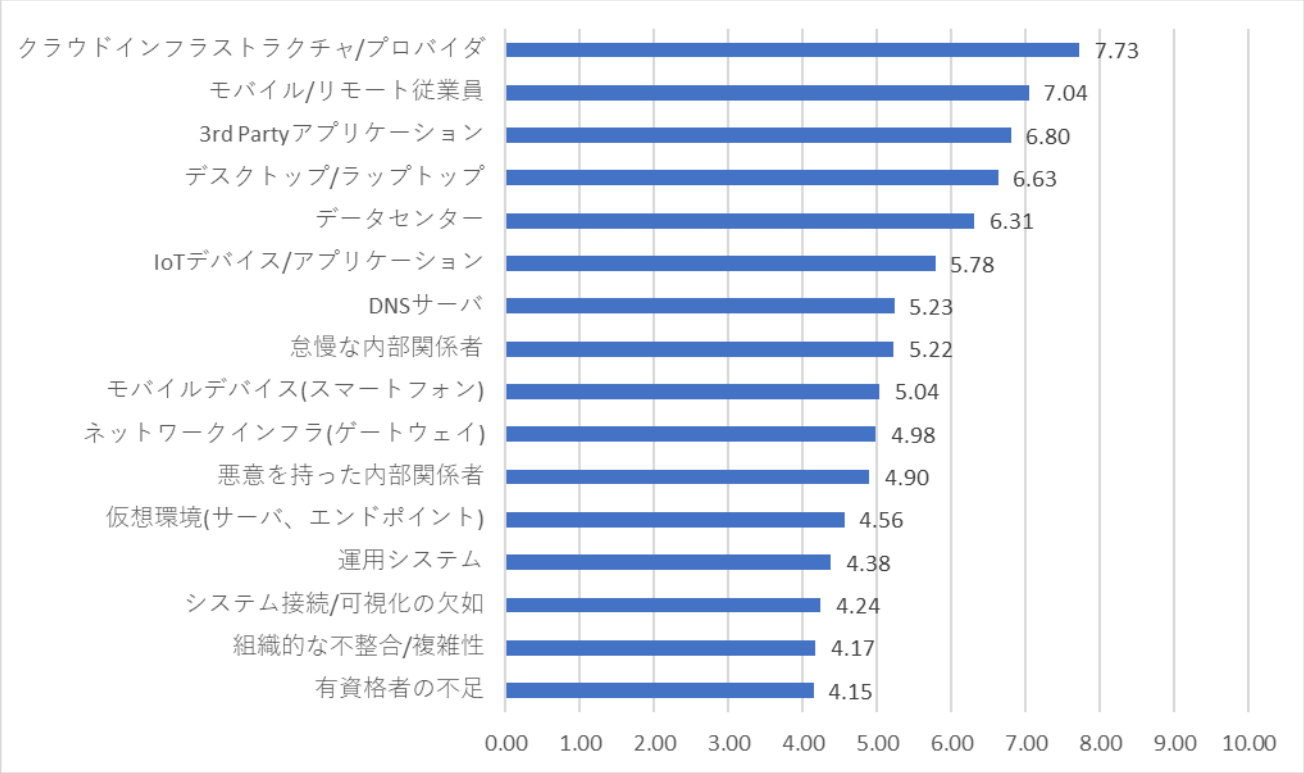

図 11：IT インフラのなかでセキュリティリスクの懸念がある環境(日本)

近年の組織におけるシステムやワークスタイルの急速なデジタルシフトに対して、講じているセキュリティ対策が十分でないという懸念を持っていることが伺えます。

サイバー脅威への防御力向上には、脅威インテリジェンスの活用が重要になる

Cyber Risk Index（CRI）によって、組織におけるサイバー攻撃への準備体制やサイバー脅威の環境を俯瞰的に捉えることができます。自組織におけるサイバーリスクの現在の状況を把握して、他の地域と相対的に比較することで、新たな発見を得られるかもしれません。

日本における Cyber Risk Index（CRI）調査の結果からは、セキュリティ体制においてデータ/プライバシー保護やコンプライアンス遵守に対する意識が高いことが伺えました。一方で、ランサムウェアのような組織を取り巻く高度なサイバー脅威に対しての懸念が他の地域に比べて低いこともわかりました。

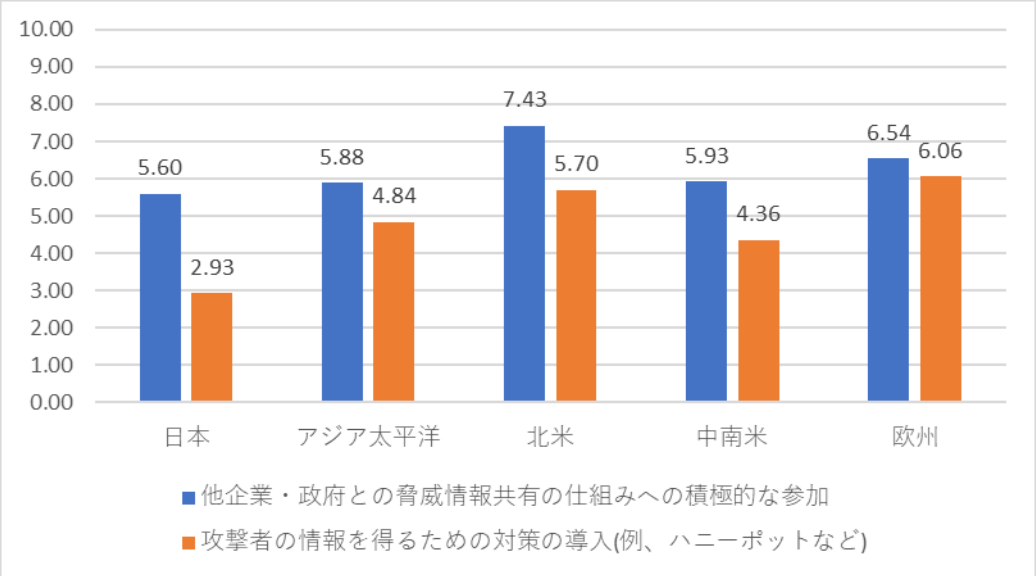

図 12：脅威・攻撃者情報取得のための取り組みや対策

日本の組織は、他の企業や政府と連携した脅威情報共有の仕組みへの積極的な参加が 5.60 であり、他の地域に比べて参加意識が低くなっています。さらに自組織における攻撃者の情報を得るための対策の導入については 2.93 と、脅威情報を収集するための対策に関する投資意欲も低い傾向であることがわかります。

これまで行っていたレギュレーション対応中心の対策に加えて、日々進化する攻撃者グループの意図や攻撃手法などの情報を脅威インテリジェンスとして収集して、彼らの目的達成を阻止するための脅威駆動型アプローチによる対策を検討することも、サイバー脅威に対する日本の組織の防御力向上に繋がることが考えられます。

TREND MICRO

トレンドマイクロ株式会社

www.trendmicro.com

東京本社
〒151-0053 東京都渋谷区代々木2-1-1
新宿マインズタワー
TEL.03-5334-3601（法人お問い合わせ窓口）
FAX.03-5334-3639

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原3-4-30
ニッセイ新大阪ビル13F
TEL.06-6350-0330　FAX.06-6350-0591

名古屋営業所
〒460-0002 愛知県名古屋市中区丸の内3-22-24
名古屋桜通ビル7F
TEL.052-955-1221　FAX.052-963-6332

福岡営業所
〒812-0011 福岡県福岡市博多区博多駅前2-3-7
シティ21ビル7F
TEL.092-471-0562　FAX.092-471-0563