

5分でかんたん完結！

情報セキュリティセルフチェックシート



目次

1. 各設問に対し、当てはまるものに丸を記入してください
2. 集計結果をレーダーチャートに反映
3. 診断結果

1. 各設問に対し、当てはまるものに を記入してください

- ・「はい」の場合◎、「取り組んでいる途中」の場合○、「取り組んでいない」場合×で回答してください。
- ・◎=2点、○=1点、×=0点とし、各設問の合計点数を算出してください。

設問		◎	○	×
A 組織的 安全管理 措置	A-1. 社内で情報セキュリティ統括体制を整え、責任者を決めていますか？	2	1	0
	A-2. 安全管理措置の評価・見直しを年1回以上行っていますか？	2	1	0
	A-3. お客様や取引先の個人情報の取引状況を把握していますか？	2	1	0
	A-4. 万が一の情報漏えいや違反への対処ルートを決めていますか？	2	1	0
	A-5. 情報セキュリティに関する社内ルールの見直しを年1回以上行っていますか？	2	1	0
	A-6. ISMSやPマークなどの第三者認証を取得していますか？	2	1	0
B 物理的 安全管理 措置	B-1. 警備会社のセキュリティサービスや監視カメラを導入し、防犯対策を行っていますか？	2	1	0
	B-2. IDカードを使った入退室管理システムで、誰がいつオフィスに出入りしたか管理していますか？	2	1	0
	B-3. 重要な書類は鍵のついたキャビネットに保管していますか？	2	1	0
	B-4. 重要な書類を破棄するときは、シュレッダーにかけたり、データの場合は消去ツールを使って確実に処分していますか？	2	1	0
	B-5. 個人情報を取扱うパソコンはセキュリティワイヤー等で固定していますか？	2	1	0
	B-6. 来客者が社内を歩き回る必要のないレイアウトになっていますか？	2	1	0

設問		◎	○	×
C 人的安全管理措置	C-1. 情報セキュリティ対策ルールを取り決め、社員がいつでも閲覧できるようにしていますか？	2	1	0
	C-2. 定期的にセキュリティに関する研修を社内で行っていますか？	2	1	0
	C-3. 業務委託先の情報セキュリティ対策を監督できていますか？	2	1	0
	C-4. 社員が個人で所有するパソコンやスマートフォンなどを業務で使用するについてのルールを決めていますか？	2	1	0
	C-5. 利用中のクラウドサービスやウェブサービスの安全、信頼性を把握して利用できていますか？	2	1	0
	C-6. 社員の役割に応じて、セキュリティに関する意識啓発ができていますか？	2	1	0
D 技術的安全管理措置	D-1. 常にパソコンのOSやソフトウェアを最新にアップデートしていますか？	2	1	0
	D-2. PCにはウイルスソフトを入れ、常に最新にアップデートしていますか？	2	1	0
	D-3. 重要なデータはアクセス権の設定を行い、適切に管理していますか？	2	1	0
	D-4. ネットワークの入口に外部からの脅威の侵入を防ぐためのファイアウォールを設置し、また導入後運用管理を行っていますか？	2	1	0
	D-5. 社内の端末からどこにアクセスしたか、どこにメールを送ったか、外部へ意図しない通信がないか、管理できていますか？	2	1	0
	D-6. 重要なデータは常にバックアップをとり、機器の故障やサイバー攻撃に備えてデータが消失しないようにしていますか？	2	1	0

点数結果

◎ =

点

○ =

点

◎ =

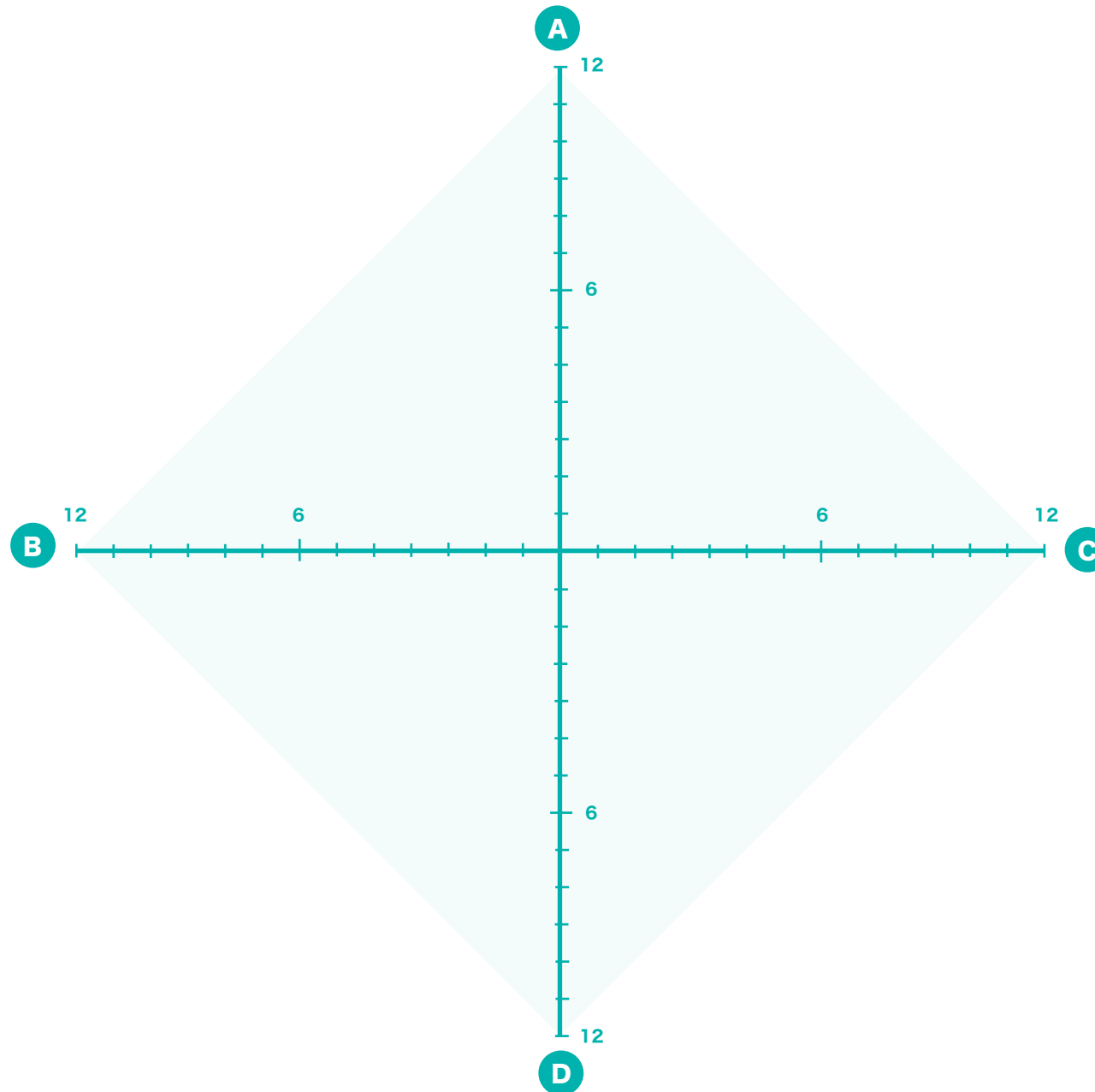
点

◎ =

点

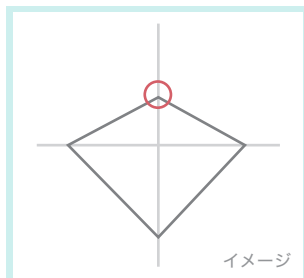
2. 結果をレーダーチャートに反映

- ・集計結果をもとに A~B の軸に点を記入。各点を線で結びます。



3. 診断結果

・レーダーチャートの結果を参照し、診断結果をご覧ください。

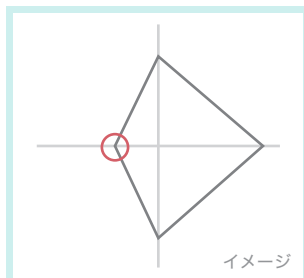


A 軸（組織的安全管理措置）が短かった方

▶ 会社としての方針を定めましょう

事故の発生を 100%防ぐことはできません。

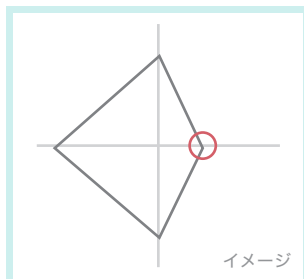
しかし、事故が起きた時どう動くのか、起こさないために何を事前で考えておくことで、被害を最小限に抑えることができます。



B 軸（物理的安全管理措置）が短かった方

▶ ハード面の見直しを！

デスクの周りを見回してみてください。「オフィスの中だから大丈夫」と安心せず、「もし何かあったら…」とあらかじめ危険を予知しておくことも重要。生産性の工業、業務効率化にもつながる糸口が見つかるかもしれません。

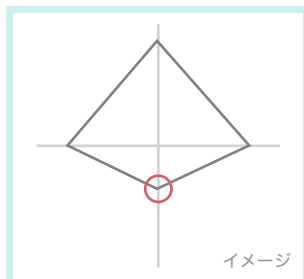


C 軸（人的安全管理措置）が短かった方

▶ 社内での教育が重要！

セキュリティに関する知識量は人それぞれ。専門家並みに詳しい方もいれば、何も知らない方もいるでしょう。

定期的にセキュリティに関して社内アナウンスをしたり、研修の機会を持つなど、長期的に取り組んでいきましょう。



D 軸（技術的安全管理措置）が短かった方

▶ できることから始めましょう

セキュリティに関する投資は、確実に効果を得ようと思うと予算があがる一方。

まずは何を守りたいのか、優先事項をつけることから始めます。それによって必要になる機器やソフトウェアが決まります。導入後は必ず評価を行い、今後の方針を決めていきましょう。

さらに具体的なセキュリティ対策をご希望の方は
こちらまでお気軽にお問い合わせください！



電話：0120-989-948（電話受付：9:00～18:00）
メールフォーム：<https://www.marugoto-navi.jp/contact>

運用元会社概要

社名 株式会社メガ
URL <https://www.mega.co.jp>
本社 〒150-0043
東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 14 階