MOTEX

# ガイドライン対応サポートアカデミー

# サイバーセキュリティ対策パッケージ　ご紹介資料

2025年5月

エムオーテックス株式会社

# 1．会社概要

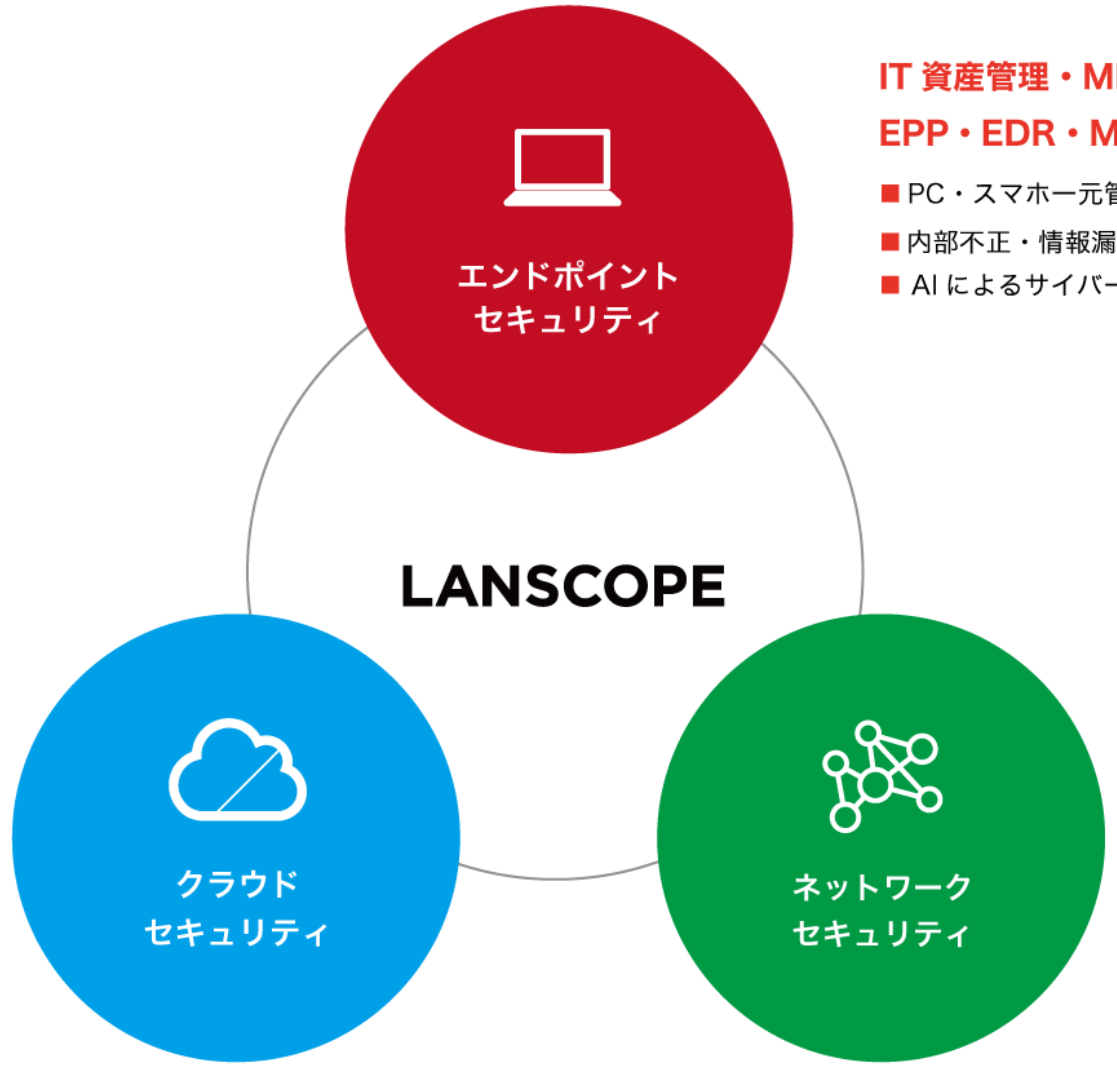
## 会社概要

| | |
|---|---|
| 会社名 | エムオーテックス株式会社 |
| 代表取締役社長 | 徳毛　博幸 |
| 設立 | 1990年7月 |
| 従業員数 | 472名（2025年4月現在） |
| 株主 | 京セラコミュニケーションシステム株式会社<br>（2012年から資本参加） |
| 事業内容 | サイバーセキュリティに関する<br>プロダクト開発・サービス事業 |

## 拠点

| | |
|---|---|
| 本社 | 大阪市淀川区西中島5-12-12<br>エムオーテックス新大阪ビル |
| 東京本部 | 東京都港区三田3-5-19<br>住友不動産東京三田ガーデンタワー 22階 |
| 名古屋支店 | 名古屋市中区錦1-11-11<br>名古屋インターシティ 3階 |
| 九州営業所 | 福岡市博多区博多駅前1-15-20<br>NMF博多駅前ビル2階 |
| 長崎Innovation Lab | 長崎県長崎市出島町1-41<br>クレインハーバー長崎ビル 3階 |

# MOTEX が提供する 3つの セキュリティソリューション




**IT 資産管理・MDM**
**EPP・EDR・MDR**

- PC・スマホ一元管理
- 内部不正・情報漏洩対策
- AI によるサイバー攻撃対策

**SaaS・IaaS の設定診断**
**Microsoft 365 監査ログ管理**

- 国家資格取得者による設定診断
- 業界トップクラスの診断項目数
- 監査ログの取得・アラート管理

**脆弱性診断・AI ネットワーク脅威検知**
**サプライチェーンリスク評価**

- AI によるネットワーク監視・遮断
- Web・ネットワークの脆弱性診断
- 外部公開資産の洗い出し・リスク評価

# “LANSCOPE” を通して、お客様の “Secure Productivity”（安全と生産性向上の両立）を支援

## エンドポイントセキュリティ

### 統合エンドポイント管理

Endpoint Manager

組織の IT 資産管理・内部不正対策・外部脅威対策をオールインワンで対応

- IT 資産管理・MDM
- 内部情報漏洩対策
- 外部脅威対策

### AI アンチウイルス

Cyber Protection

AI を活用したアンチウイルスで未知・亜種の脅威を検知・対処・復旧が可能

- EPP
- EDR
- MDR

### リモートコントロール

Remote Desktop

遠隔地のサーバーやPC、スマホへのリモート操作、画面共有などヘルプデスク業務を効率化

- リモートアクセス
- ヘルプデスク効率化

## クラウドセキュリティ

### Microsoft 365 セキュリティ

Security Auditor

Microsoft 365の監査ログを取得。利用状況の見える化やアラート管理が可能

- 監査ログ管理
- アラート管理

### セキュリティ診断

Professional Service

高い技術力を誇るセキュリティエンジニアがWeb・ネットワーク・クラウドの脆弱性を診断

- Web 診断
- ネットワーク診断
- クラウド診断

## ネットワークセキュリティ

### AI ネットワーク脅威検知

DARKTRACE

AI を活用しネットワークを監視、サイバー攻撃や内部不正の兆候を検知・遮断

- NDR
- ネットワーク遮断
- Email 監視

### サプライチェーンリスクマネジメント

Panorays

ドメイン情報やオンライン調査票からサプライチェーンリスクを可視化

- セキュリティスコアリング
- ASM

# 2．ガイドライン対応サポートアカデミーとは

## 企業を取り巻くサイバーセキュリティの情勢が変化する中で
## このようなお困りごとはありませんか？

取引先や親会社から
ガイドライン準拠の
要請が増えてきた

経産省が推進する
5段階の格付け制度が
気になる

セキュリティ規程を
整備したいが知識や
リソースが足りない

情報セキュリティに
関する各種規格への
準拠を進めたい

**ガイドライン対応サポートアカデミー** が解決します

# ガイドライン対応サポートアカデミー

**好きな時に、ずっと使える。学びとコンサルで築く確かなセキュリティ。**

お客様のセキュリティレベルの向上を「アカデミー形式」で実現するコンサルティングパッケージです。
個別支援に加え、ポータルを活用した集合学習を通じて、体系的かつ効果的にセキュリティガイドラインの遵守を
支援します。全てのお客様対応のプランと、業界特化したプランをご用意しています。

# コンサルタントによる充実した支援内容を低価格でご提供します

ガイドライン対応
サポートアカデミー

## ポイント1 月額1万円でコンサルタントが支援※1

国家資格を持つセキュリティコンサルタントへメールWeb会議で直接お悩み相談ができます※2。実施すべきセキュリティ対策の内容から、効率の良い進め方まで幅広くアドバイスします。

## ポイント2 お役立ちコンテンツ満載のポータル

コンサルタントの講座動画や、ガイドラインの基準を網羅した各種規程・管理フォーマットのひな型など、ガイドライン対応を支援するコンテンツを多数掲載しています。

## ポイント3 すき間時間に自由なペースで

専用のポータルサイトで、ガイドラインの学習から達成に必要なノウハウの習得まで、好きなペースで進められます。

※1：9カ月45万円の基本のパッケージをご購入いただき、期間を終了した後に継続される場合の価格（税別）です。
1年分を一括でのお支払いになります。
※2： Web会議での個別相談は回数制限があります

# 一般的なコンサルティングサービスとの違い

| | 一般的なコンサルティング<br>サービス | ガイドライン対応<br>サポートアカデミー |
|---|---|---|
| 目的 | 定めた目的（成果物）の完遂 | セキュリティ運用を根付かせる<br>（セキュリティ人材の育成・支援） |
| 主体性 | コンサルタント | お客様ご自身 |
| 支援内容 | 定めた目的の完遂のため<br>コンサルタントが主体のなり対応 | 人材育成・対策の実践に必要な<br>知識取得・必要なツール・サポート提供 |
| 価格 | 高額<br>数百万～数千万※3 | 低価格<br>標準的なプランで45万円※2 |
| 支援期間 | スポット<br>数百万～数千万※3 | 継続支援が可能<br>年間12万円 |

※1：9か月間の初回契約を満了後、1年ごとの契約更新が可能です。
※2：サポートアカデミーのすべての支援内容を9か月間利用できるプランの価格です。購入プランにより異なります。プランごとの価格はサービス詳細をご確認ください。
※3：総合的なセキュリティ対策をエムオーテックスへご依頼いただいた場合の参考価格となります。

# PDCAを回し続けることが大切なんです

# 継続が何よりも重要です

セキュリティ対策は1度実施すれば終わりではありません。日々変化する環境・脅威に合わせて対応を継続して実施していかなければなりません。

理想的な状態を、私は「セキュリティ対策が根付いた状態」と呼んでいます。
情報セキュリティ対策の強化を、社内の情報セキュリティ対策にかかわるすべてのメンバーが自分事ととらえ、継続して取り組んでいる状態です。

初めは、次々と現れる脅威・課題の対応に苦労するかもしれませんが、
PDCAサイクルを回すことが習慣化し、自然にセキュリティレベルを維持できるように私たちが継続して支援いたします。

「コンサルタントに任せたいが費用の問題がある」「自分たちでやるにしてもやり方が分からない」とお悩みの皆さん、私と一緒に理想の状態を実現しましょう。

# ガイドライン対応サポートアカデミー

## サイバーセキュリティ対策パッケージ

学習コース　実践コース

### すべての企業が共通で実施するべき基本的なサイバーセキュリティ対策の実施を支援

「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」 や「IPA 中小企業の情報セキュリティ対策ガイドライン」、「IPA 情報セキュリティ対策ベンチマーク」などをもとにした、企業が実施するべきセキュリティ対策の実施状況の点検ができるオリジナルのチェックシートを提供。自社の現状把握から対策強化までサポートします。（実践コースもリリースを予定しています）

## 自工会／部工会・サイバーセキュリティガイドライン対策パッケージ

学習コース　実践コース

### 自動車産業に特化したセキュリティレベルの維持・向上を支援

自動車産業にかかわるすべての企業・団体を対象としたセキュリティガイドライン「自工会／部工会・サイバーセキュリティガイドライン」に特化した支援をご提供します。年に1回自工会が求めている自己評価チェックシートの提出もサポートします。

# ３．企業のサイバーセキュリティ対策を取り巻く現状

①サプライチェーンリスクと取引先からのセキュリティ要求
②経済産業省が進めるサイバーセキュリティ対策の“格付け”制度

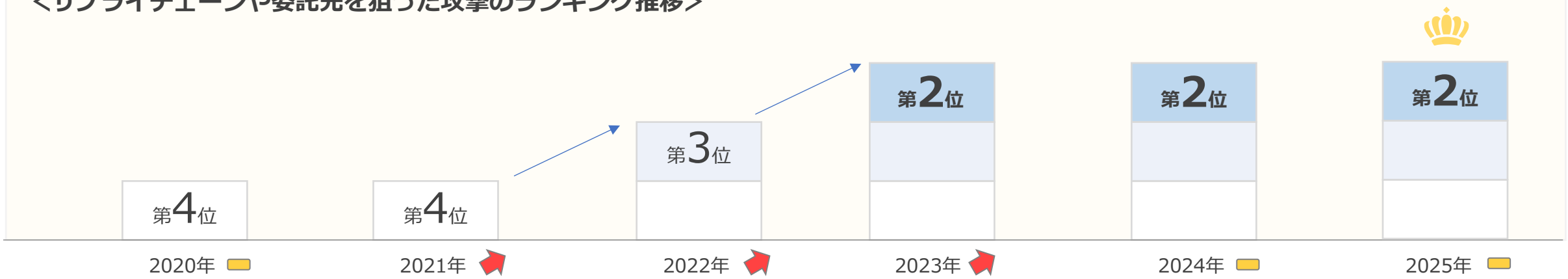
# ３．企業のサイバーセキュリティ対策を取り巻く現状

**①サプライチェーンリスクと取引先からのセキュリティ要求**

②経済産業省が進めるサイバーセキュリティ対策の“格付け”制度

# 高まる脅威！IPA「情報セキュリティ10大脅威2025」でも年々上位傾向に

**<サプライチェーンや委託先を狙った攻撃のランキング推移>**




情報セキュリティ10大脅威2025

| 順位 | 組織 | 順位 | 組織 |
|---|---|---|---|
| 1位 | ランサムウェアによる被害 | 6位 | リモートワーク等の環境や仕組みを狙った攻撃 |
| 2位 | サプライチェーンや委託先を狙った攻撃 | 7位 | 地政学的リスクに起因するサイバー攻撃 |
| 3位 | システムの脆弱性を突いた攻撃 | 8位 | 分散型サービス妨害攻撃（DDoS攻撃） |
| 4位 | 内部不正による情報漏えい等 | 9位 | ビジネスメール詐欺 |
| 5位 | 機密情報等を狙った標的型攻撃 | 10位 | 不注意による情報漏えい等 |

※IPA_情報セキュリティ10大脅威 2025を元に作成

# 某情報処理サービス企業がハッカー集団のサイバー攻撃の標的に業務を委託していた全国の自治体や企業などに**被害が拡大**

## 某情報処理サービス企業

情報処理サービスなどを展開する某企業で、2024年5月に社内の一部のサーバーやPCがランサムウェアに感染。ハッカー集団が犯行声明を出し、盗み取ったとするデータを公開した。

### 複数の地方自治体

新型コロナ予防接種券や
納税者などの個人情報など

**15万件～103万件**

### 大手機器メーカー

顧客の利用・請求明細など

**6万件**

### 商工会議所

会員企業の個人情報

**4万件**

# 某情報処理サービス企業がハッカー集団のサイバー攻撃の標的に業務を委託していた全国の自治体や企業などに**被害が拡大**

## 某情報処理サービス企業

情報処理サービスなどを展開する某企業で、2024年5月に社内の一部のサーバーやPCがランサムウェアに感染。ハッカー集団が犯行声明を出し、盗み取ったとするデータを公開した。

複数の地方自

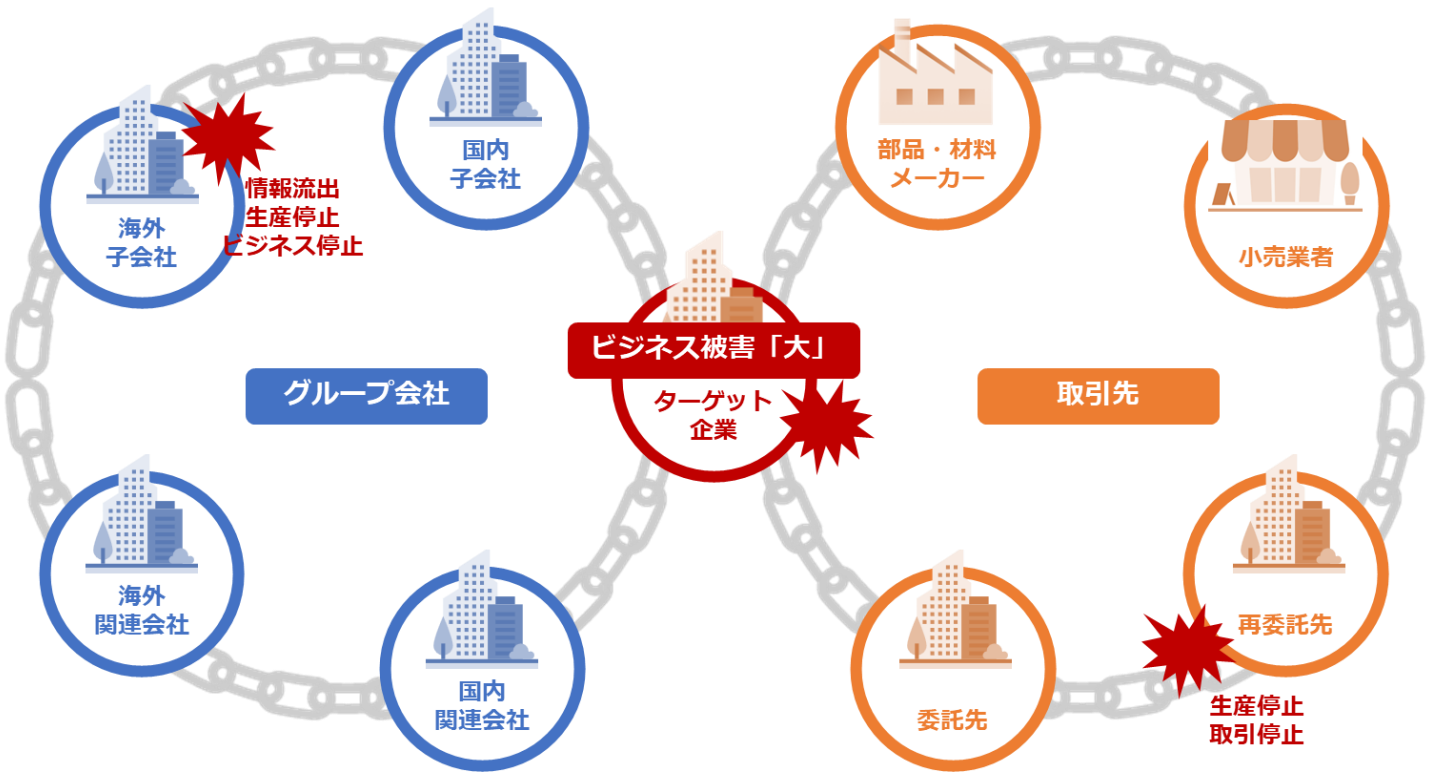
新型コロナ予防
納税者などの個人

15万件～10

**ただの不幸な事故では片づけられない、企業側のセキュリティ対策の甘さ**

- **本来であれば個人情報はネット環境から分離された別サーバーで保存されているはずだったが、それが徹底されていなかった**
- **委託元との契約終了後にデータ消去することを取り決めており、削除したとの報告も行っていたにも関わらず、実際には削除されていなかった**

# サプライチェーン攻撃（サプライチェーンの脆弱性を突いた攻撃）




**取引先・グループ会社の**
**セキュリティインシデントにより…**

- **ビジネスに影響が及ぶ（工場停止など）**
- **自社にセキュリティインシデントが飛び火し、被害を受ける**

対策として**「セキュリティチェックシート」**を送付し対応を求めるケースが増加

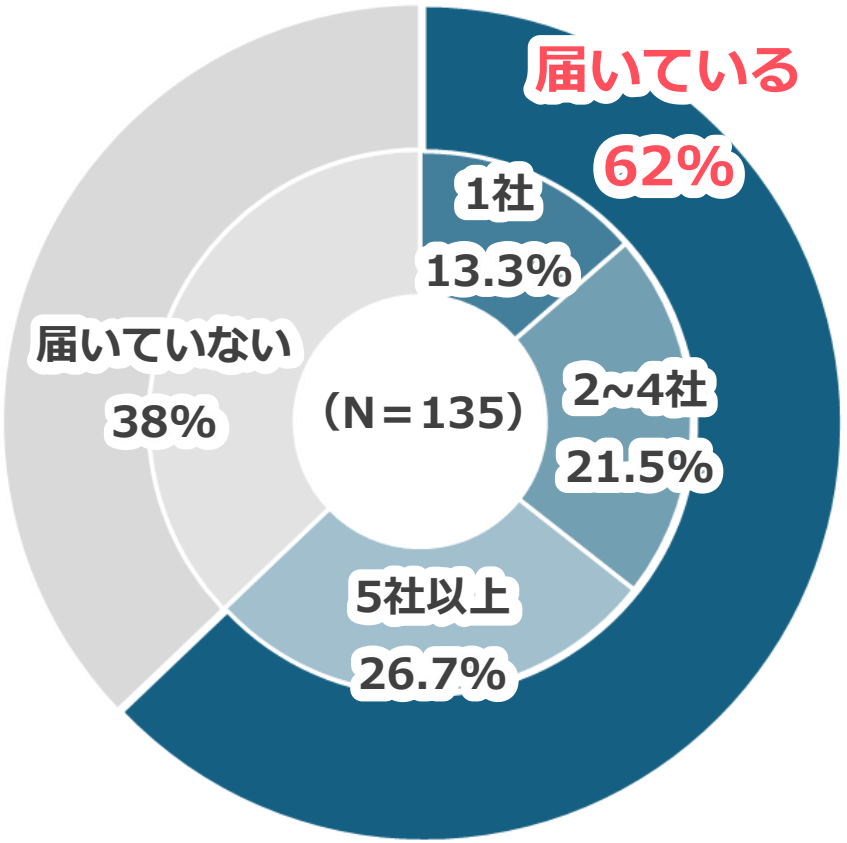
**「自社の期待するセキュリティ水準に達することができるのか？」**が問われます

**課題の8割以上**
**ガバナンス強化**

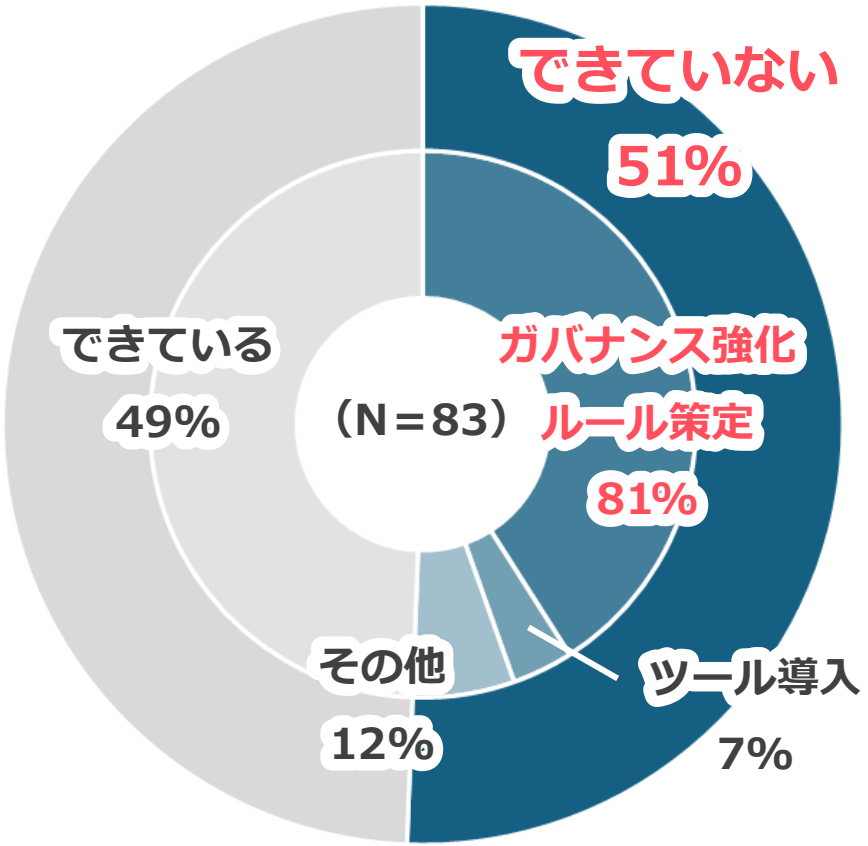
# セキュリティ監査が届いている企業は**6割以上**

# **約半数が自信をもって回答できていない**という実態

Q. 取引先からセキュリティチェックシートもしくは
セキュリティ監査が届いていますか？




Q. セキュリティチェックシートもしくはセキュリティ
監査に自信をもって答えられていますか？




※2025年1月にエムオーテックスにて開催したセミナーの参加者アンケート結果
※アンケート回答者のうち、お立場が「自社システム導入を決定する立場」「自社システムの導入を検討する立場」を選ばれた方のみを母数としています

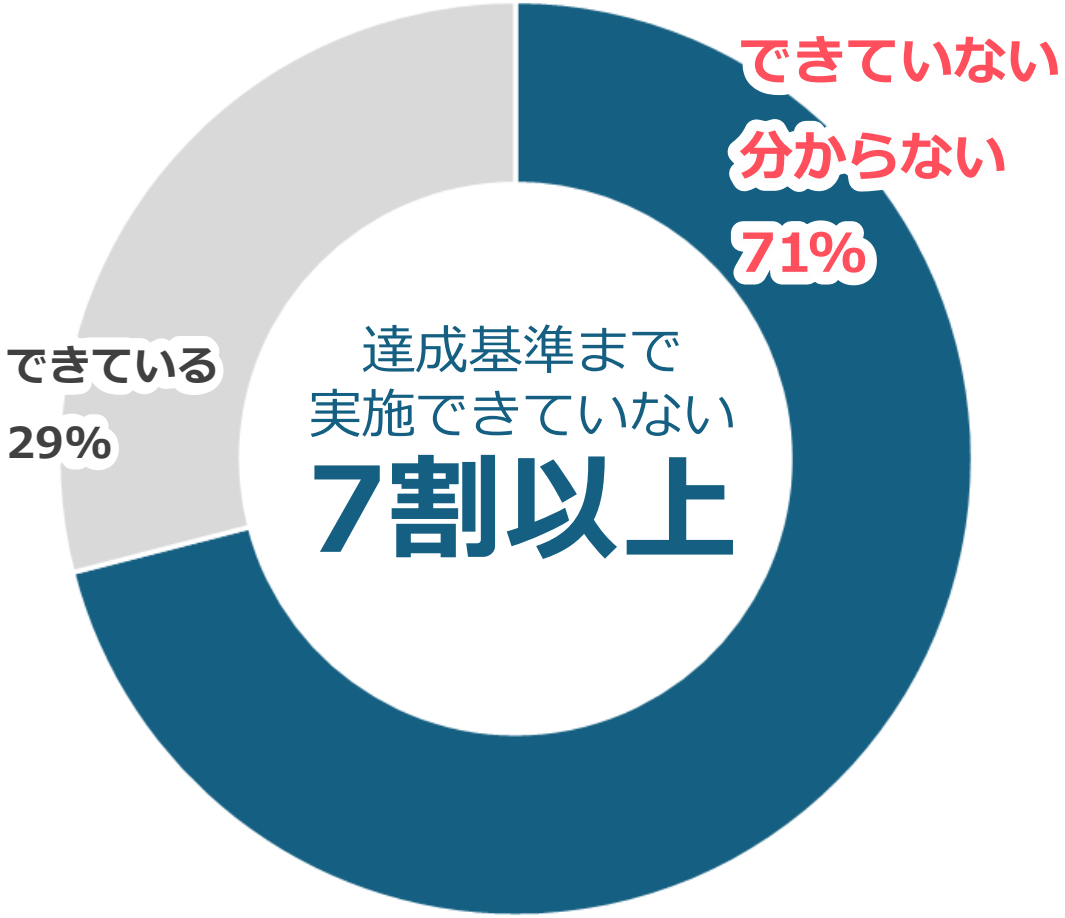
# 自信があるという方もちょっと待って！

## **約7割が達成基準まで実施できていない**という実態が明らかに

Q. 自社の情報資産の把握ができていますか？（n=233）


Q. **「できている」と回答した方へ追加で質問**です。
以下の達成基準をすべて実施ができていますか？

| 達成基準 | |
|---|---|
| □ | 情報資産(情報)について高い機密区分の一覧表を作成し、**管理項目に対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先を含めている** |
| □ | 情報資産(機器)について情報機器、OS、ソフトウェアの情報を確認できる一覧表を作成し、**管理項目にバージョン情報、管理者、管理部門、設置場所を含めている** |




※2025年1月にエムオーテックスにて開催したセミナー中にZoom投稿機能を用いて行ったアンケート結果

※達成基準は「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」 や「IPA 中小企業の情報セキュリティ対策ガイドライン」、「IPA 情報セキュリティ対策ベンチマーク」などをもとにエムオーテックス作成

# 達成基準まで実施できていなかったから起こったインシデント・・・

サプライチェーンを巻き込んだインシデント事例

## 某情報処理サービス企業がハッカー集団のサイバー攻撃の標的に業務を委託していた全国の自治体や企業などに被害が拡大

### 某情報処理サービス企業

情報処理サービスなどを展開する某企業で、2024年5月に社内の一部のサーバーやPCがランサムウェアに感染。ハッカー集団が犯行声明を出し、盗み取ったとするデータを公開した。

複数の地方

新型コロナ予防
納税者などの個人

15万件～10

**ただの不幸な事故では片づけられない、企業側**

- **本来であれば個人情報はネット環境から分離さ**
  **されているはずだったが、それが徹底されていなかった**
- **委託元との契約終了後にデータ消去することを取り決めており、削除した**
  **との報告も行っていたにも関わらず、実際には削除されていなかった**

**情報資産に「保管期限」を定め、期限になったら削除する対策ができていなかった**

## まとめ

- セキュリティ監査が届いている企業は**6割以上！**
- **その約半数が自信をもって回答できていない**という実態
- その回答理由の**約8割がガバナンス強化・ルール策定**が課題
- 自信のある企業も、**約7割が達成基準まで実施できていない**という実態
- **達成基準まで理解して実施**することが大事

今、セキュリティ対策の実施で求められている（支援）のは

# 「正しい知識」＋「ガバナンス強化」

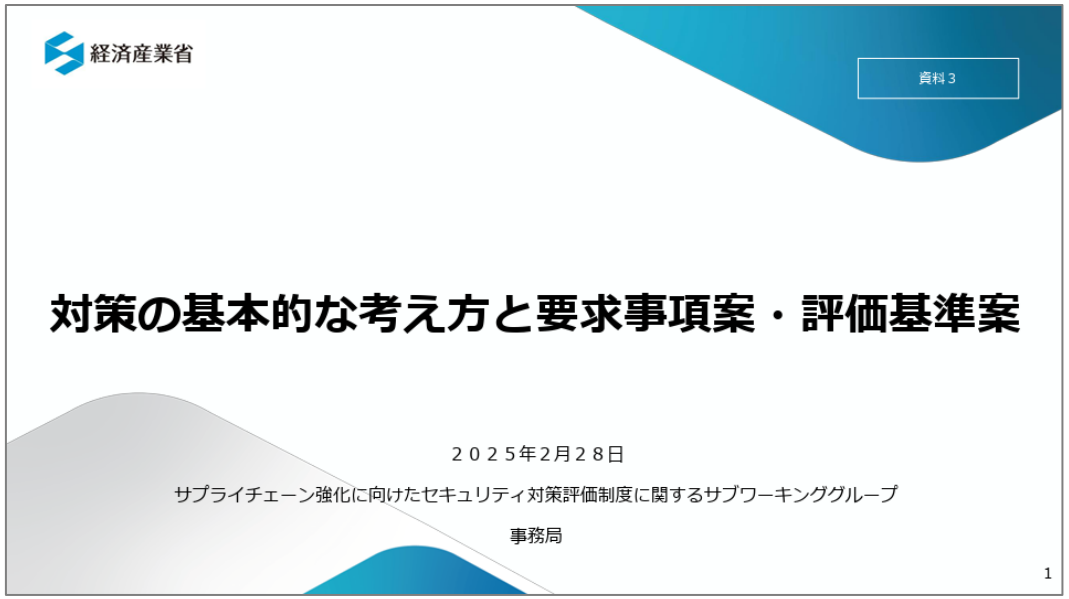
# ３．企業のサイバーセキュリティ対策を取り巻く現状

①サプライチェーンリスクと取引先からのセキュリティ要求

**②経済産業省が進めるサイバーセキュリティ対策の“格付け”制度**

# 経済産業省がサイバーセキュリティ対策状況を“格付け”する新制度を発表

- 2024年4月：経産省が方針発表
- 2024年7月：第1回の検討会が開催
- 2024年9月：第2回の検討会が開催
- 2024年12月：第3回の検討会が開催
- 2025年2月：第4回の検討会が開催





出典：経済産業省ウェブサイト（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/004.html）

# “自己宣言” からもう一歩先へ進んだ制度

## 実際にセキュリティ対策が**実施できているかどうか**が評価されます

**セキュリティ対策に取り組むことを自ら宣言** ← → **基準に適合する対策が実施できていることをチェック・認定※** ← →



1つ星　2つ星　3つ星　4つ星　5つ星

**SECURITY ACTION**
セキュリティ対策自己宣言

サプライチェーン対策評価制度
（サイバーセキュリティの格付け）

※星３については自社もしくは他社の情報処理安全確保支援士（登録セキスペ）資格の保有者、星４～５は認定された認証機関による第三者評価で適合状況を確認することが検討されています。

# 発注者側の企業が取引先に対して必要な格付けの区分を設定し要請する

- ✓ 発注を行う事業者が、取引先に対してビジネス観点で**重要度を評価し、星3/4/5に区分して対策を要請**。
- ✓ ビジネス観点での重要度だけでなく、システム観点で内部ネットワークへのアクセス手段の有無も評価の基準となる。

**➡自社ネットワークへのアクセスが可能な場合は星４の取得が推奨**

| 判断主体 | 判断の観点 | | ★3 | ★4 | ★5 |
|---|---|---|---|---|---|
| 発注者 | **ビジネス観点** | **a) データ保護**<br>（取引先がアクセス可能な情報の重要度） | 原則として、全ての取引先（ビジネスサプライチェーン及びサービスサプライチェーン企業） | 中<br>(右記以外の個人情報、営業秘密等) | 高<br>(多数または重大損害を及ぼす個人情報(例：口座番号、暗証番号)、営業秘密等) |
| | | **b) 事業継続**<br>（取引先による供給製品・サービスの重要度（代替可能性を含む）） | | 中<br>(発注者による製品・サービス供給停止につながるリスク中) | 高<br>(発注者による製品・サービス供給停止につながるリスク高) |
| | **システム観点** | 発注者内部ネットワークへの取引先環境からのアクセス手段(例：ネットワーク共有)の有無 | • 無し | • 有り<br>※ ビジネス観点で★3相当とされている場合であっても★4以上に変更推奨 | |



出典：経済産業省ウェブサイト（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/002.html）

- NISTサイバーセキュリティフレームワーク2.0の６分類に、サプライチェーン対策である「取引先管理」を加えた７分類で検討。
- 本仕組みが「サプライチェーン全体のレジリエンス」を目的としていることから、取引先管理をより強調するため独立した分類としたもの。
- ★３は基礎的なシステム防御策を中心に構成。★４は包括的な対策とし、★５はシステムに対するより高度な対策を想定。

| 分類 | ★3 | ★4 | ★5 |
|---|---|---|---|
| **対策の基本的な考え方** | **全てのサプライチェーン企業が最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に構成 | 該当する企業等が**標準的に目指すべきセキュリティ対策**として、**ガバナンスからシステム防御・検知、インシデント対応等包括的な対策**にて構成 | 該当する企業等が**高度なサイバー攻撃への対処を念頭に目指すべきセキュリティ対策**として、早期の侵入検知、被害の極小化など**防護対象システムに対するより高度な対策**にて構成 |
| ガバナンスの整備 | • **社内の役割とポリシーを明確化**している。<br>• 自社の対策状況について正しく認識している。 | • **組織的なガバナンス**が適切に構築・運用されている。(★4/5で共通) | |
| 取引先管理 | • **外部ICTサービスが把握**されている。 | • **サードパーティのリスク評価**が行われ、リスクに応じた対応が講じられている。(★4/5で共通) | |
| リスクの特定 | • IT資産管理台帳、重要な情報資産の一覧作成(取引先から受領したデータ等)を通じて、**資産が把握されている**。 | • IT環境を対象に、**資産管理台帳が作成、管理**されている。<br>• 重要システムにおいて、**定期的な脆弱性検査等**によりリスク認識が更新されている。 | • **OTも含めて網羅的に**資産とそのリスクが管理されている。<br>• 資産とそのリスクの管理が**リアルタイム**に行われている。 |
| システムの防御 | • **初期侵入及び内部拡大の防止に係る対策**のうち、効果が大きいものが実装されている。 | • ★3で網羅されていないものも含めて**包括的に要求事項が規定**されている。 | • **高度なサイバー攻撃への対処を念頭**に、★４より高い強度の対策がなされている。 |
| 攻撃等の検知 | • **外部ネットワークとの境界部分**にて通信が監視されている。 | • 外部ネットワークとの境界に加え、**内部ネットワーク上の適切な場所及び端末等**で通信やその他の挙動が監視されている。 | • 組織内の**複数箇所のログ等を相関**させ、異常が検知されている。<br>• 収集した**脅威インテリジェンス情報が検知活動に活用**されている。 |
| インシデントへの対応 | • **インシデント対応計画**が整備されている。 | • **対応計画**が定められており、内容が定期的にレビューされている。 | • 迅速な対応のため、対応の**一部が自動化**されている。 |
| インシデントからの復旧 | - | • **事業継続計画**(BCP)が定められており、内容が定期的にレビューされている。 | • 対応の**一部が自動化**されている。<br>• サイバー攻撃BCPが策定・実施されている。 |

出典：経済産業省ウェブサイト（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/002.html）

- NISTサイバーセキュリティフレームワーク2.0の６分類に、サプライチェーン対策である「取引先管理」を加えた７分類で検討。
- 本仕組みが「サプライチェーン全体のレジリエンス」を目的としていることから、取引先管理をより強調するため独立した分類としたもの。
- ★３は基礎的なシステム防御策を中心に構成。★４は包括的な対策とし、★５はシステムに対するより高度な対策を想定。

| 分類 | | ★3 |
|---|---|---|
| 対策の基本的な考え方 | | **全てのサプライチェーン企業が最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に構成 |
| ガバナンスの整備 | ① | • **社内の役割とポリシーを明確化**している。<br>• 自社の対策状況について正しく認識している。 |
| 取引先管理 | ② | • **外部ICTサービスが把握**されている。 |
| リスクの特定 | | • IT資産管理台帳、重要な情報資産の一覧作成(取引先から受領したデータ等)を通じて、**資産が把握されている**。 |
| システムの防御 | ③ | • **初期侵入及び内部拡大の防止に係る対策**のうち、効果が大きいものが実装されている。 |
| 攻撃等の検知 | ④ | • **外部ネットワークとの境界部分**にて通信が監視されている。 |
| インシデントへの対応 | ⑤ | • **インシデント対応計画**が整備されている。 |
| インシデントからの復旧 | | - |

**自信をもって「実施できている」と言えますか？**

① **自社の情報セキュリティポリシーを策定し、社内に周知していますか？**

② **社内の情報資産の一覧を作成し、正しく把握していますか？**

③ **ウイルス感染拡大防止の基本的な対策をしていますか？**

④ **ネットワーク境界の防御・監視をしていますか？**

⑤ **インシデント対応計画を立てていますか？**

出典：経済産業省ウェブサイト（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/002.html）

| | | |
|---|---|---|
| 1 | **取引先へのセキュリティ要求** | すでに自社の取引先に対してセキュリティ要求をしている企業が増加しています。“格付け“という共通の基準ができることで、独自基準を作成する必要がなくなり要求をしやすくなるため、この動きが加速することが想定されます。 |
| 2 | **投資家の投資判断・株価** | 日本の投資家に対するサイバーセキュリティ関連情報の意識調査※によると、投資先企業のセキュリティ対策を評価する投資家の割合は90%にも上ります。“格付け“制度の普及により、より他社との比較がしやすくなります。 |
| 3 | **税制優遇などのインセンティブ** | 2024年7月12日に開催された検討会の議事要旨によると、制度の普及のために具体的なインセンティブの必要性が議論されています。「セキュリティ対策にはお金がかかるからできない」という言い訳は通用しなくなる可能性があります。 |
| 4 | **いち早く獲得することで<br>ビジネスチャンス** | セキュリティ対策の評価で他社より優位に立てることでビジネスチャンスが増加する可能性があります。 |

※PwC Japan「サイバーセキュリティおよびプライバシー情報開示」に関する日米投資家の意識調査2024
（ https://www.pwc.com/jp/ja/knowledge/thoughtleadership/digital-trust-investor-survey2024.html ）

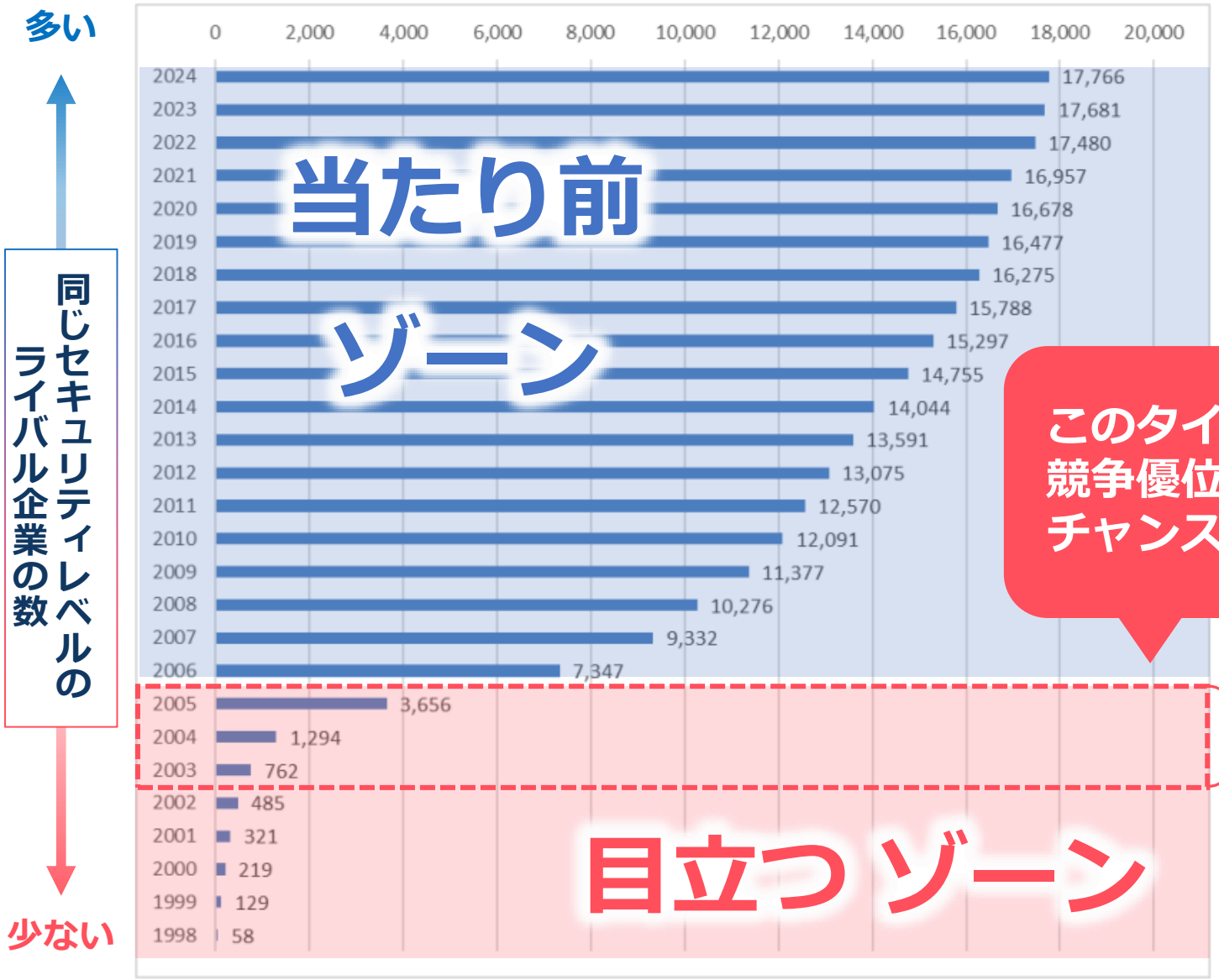
# 格付けの獲得はビジネスチャンスの拡大につながります
# 「制度が始まってから」ではなく**”先行して”**準備を進めましょう！

## 過去の事例：Pマーク（プライバシーマーク）

- 1998年に制度が開始し、2003年の**個人情報保護法の制定**～2005年の全面施行をきっかけに大きく取得企業数を伸ばした。
- Pマークは広く企業のHPや社員の名刺などに掲載されており、**顧客の信頼獲得**に活用されている。
- 官公庁等の入札では**Pマークの取得が参加条件**となっており、未取得の場合はその時点で**商談機会を失う**。

# いち早く獲得することでビジネスチャンス　～過去の事例：Pマーク～

▼Pマーク取得企業数の推移




**このタイミングで獲得していることで競争優位性を確保し、信頼性とビジネスチャンスが広がります。**

個人情報保護法が2003年5月に制定、2005年4月全面施行される

※1998年度～2024年3月31日時点の事業者数

出典：日本情報経済社会推進協会（JIPDEC） プライバシーマーク付与事業者情報（2024年9月30日版）
https://privacymark.jp/certification_info/data/g7ccig0000000gll-att/pmark_data_20240930.pdf.pdf

# 「競争優位性の確保」「信頼性の向上」「ブランド強化」などが向上
# ビジネスチャンスが増加

新制度がスタート

現在

セキュリティ対策の実施 → 認定獲得

セキュリティ対策の評価で
他社より優位に立てることで
ビジネスチャンスが増加！

何も対策を実施しない

セキュリティ対策の実施

審査待ちの行列

獲得した時には“当たり前”になっており、ビジネス
チャンスにも活かせず・・・
認定獲得までに時間がかかりビジネスに影響も！

## まとめ

- 経済産業省の“新制度で企業のサイバーセキュリティ対策を5段階で格付け
- 過去の事例としてPマーク制度を振り返ると、制度開始の数年後から
  取得企業数が急上昇、現在では取得が当たり前の状態になっている
- 詳細の発表を待っていると、**ライバル企業に差をつけられてしまう恐れが…!!**

**格付けの獲得はビジネスチャンスの拡大につながります**

**「制度が始まってから」ではなく”先行して”準備を進めましょう！**

# ４．ガイドライン対応サポートアカデミー 「サイバーセキュリティ対策パッケージ」とは

# 「サイバーセキュリティ対策」に特化した支援をご提供
# サイバーセキュリティ対策に取り組む**すべての方へ**おすすめです

## これから取り組む方

サイバーセキュリティ対策に取り組むのが
初めてで、まずはサイバーセキュリティ対策の内容
に対して理解を深めるところから始めたい

### おすすめの支援内容

- お客様の現状把握が可能なサイバーセキュリティに特化した「**チェックシート**」
- サイバーセキュリティ対策の内容や対策のポイントをコンサルタントが分かりやすく解説する「**解説講座**」
- ガバナンス強化に重要な「**各種セキュリティ　関連規程ひな型**」

## すでに取り組んでる方

サイバーセキュリティ対策の基準に対して
不足している項目をどんどん対策して、
セキュリティ対策の強化に取り組みたい

### おすすめの支援内容

- お客様の対策状況に対して、対策プログラムをご提供する「**カウンセリング**」
- 従業員のサイバーセキュリティ教育に役立つ「**教育コンテンツ**」
- ガバナンス強化の運用に役立つ「**各種運用支援ツール**」

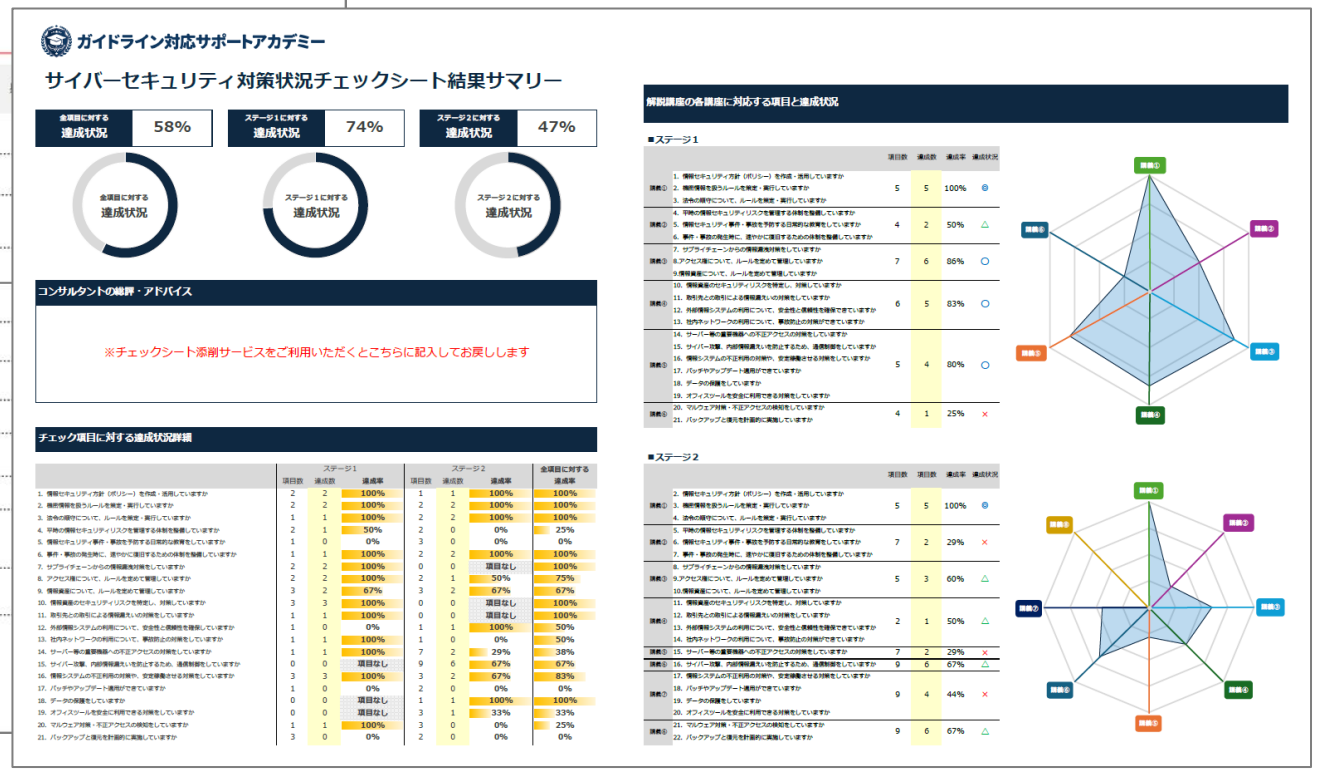
# 複数のサイバーセキュリティ対策の規格・ガイドラインをベンチマーク※した対策状況チェックシートで、自社の対策状況を把握できます

ガイドライン対応サポートアカデミー達成状況チェックシート V1.1

「お客様入力欄」の入力方法については「初めにお読みください」の内容をご参照ください

－ 達成状況チェック項目と達成状況 －　－ お客様入力欄 －

| カテゴリ | No | ステージ | チェック項目 | 判定 | 達成基準 | 達成状況をご入力ください |
|---|---|---|---|---|---|---|
| 1. 情報セキュリティ方針（ポリシー）を作成・活用していますか | 1 | 1st | 会社としてセキュリティに対する基本的な方針を作成していますか | - | 情報セキュリティに対する企業姿勢を言葉する文書を策定している | ▽プルダウンで選択ください |
| | | | | | 文書内に「経営者の責任」「法令順守」の内容が含まれている | ▽プルダウンで選択ください |
| | 2 | 1st | 作成した方針を社内に周知し、セキュリティ意識を高めていますか | - | 【作成したポリシーがA/B/どいずれかの状態にある】<br>A：ポリシーが社内に周知されている<br>B：従業員が誰でも容易に確認できる | ▽プルダウンで選択ください |
| | 3 | 2st | 社内外の環境変化を踏まえて、基本方針の内容を定期的に見直していますか | - | 年に1回以上の頻度で見直ししている | ▽プルダウンで選択ください |
| 2.機密情報を扱うルールを策定・実行していますか | 4 | 1st | 自社の守秘義務のルールを規定し、守らせていますか | - | 自社の守秘義務を文書化している | ▽プルダウンで選択ください |
| | | | | | 守秘義務には「退職・期間満了時に会社の機密情報を持ち出さない」という内容を含めている | ▽プルダウンで選択ください |
| | | | | | 社員の入社時、派遣社員等の受け入れ時に、守秘義務について説明している | ▽プルダウンで選択ください |
| | 5 | 1st | BYOD含む情報機器について、取り扱いのルールを決めて情報漏洩を防止していますか | - | 情報機器の利用ルールを策定している | ▽プルダウンで選択ください |
| | | | | | 利用ルールには「利用開始時・終了時の手続き」「利用中の遵守・禁止事項」「紛失時の手続き」を含んでいる | ▽プルダウンで選択ください |
| | | | | | 利用ルールを容易に確認できる状態にしている | ▽プルダウンで選択ください |
| | | | | | 【利用中の遵守事項に①～③をすべて含めている】<br>①周囲時にパソコン画面の覗き見や操作などができないように設定する<br>②退社時にノートパソコンや備品の盗難防止対策を実施する | ▽プルダウンで選択ください |
| | 6 | 2st | 定めたルールが守られるよう、誓約書・契約書を提出・締結させていますか | - | 従業員に対して守秘義務の誓約書を提出させている<br>（派遣社員など社外等舞を除く） | ▽プルダウンで選択ください |
| | | | | | 【派遣社員・受入出向社員について、①～②をすべて実施している】<br>①派遣元、出向元企業と守秘義務に関する契約（NDAなど）を締結している<br>②契約書に「業務で知り得た情報を外部に漏えいさせない」旨の記載がある | ▽プルダウンで選択ください |



ガイドライン対応サポートアカデミー

サイバーセキュリティ対策状況チェックシート結果サマリー

| 全項目に対する達成状況 | ステージ1に対する達成状況 | ステージ2に対する達成状況 |
|---|---|---|
| 58% | 74% | 47% |

コンサルタントの総評・アドバイス

※チェックシート添削サービスをご利用いただくとこちらに記入してお渡しします

チェック項目に対する達成状況詳細

| | ステージ1 | | | ステージ2 | | | 全項目に対する達成率 |
|---|---|---|---|---|---|---|---|
| | 項目数 | 達成数 | 達成率 | 項目数 | 達成数 | 達成率 | |
| 1. 情報セキュリティ方針（ポリシー）を作成・活用していますか | 2 | 2 | 100% | 1 | 1 | 100% | 100% |
| 2. 機密情報を扱うルールを策定・実行していますか | 2 | 2 | 100% | 2 | 2 | 100% | 100% |
| 3. 法令の順守について、ルールを策定・実行していますか | 1 | 1 | 100% | 2 | 2 | 100% | 100% |
| 4. 平時の情報セキュリティリスクを管理する体制を整備していますか | 2 | 1 | 50% | 2 | 0 | 0% | 25% |
| 5. 情報セキュリティ事件・事故を予防する日常的な教育をしていますか | 1 | 0 | 0% | 3 | 0 | 0% | 0% |
| 6. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか | 1 | 1 | 100% | 2 | 2 | 100% | 100% |
| 7. サプライチェーンからの情報漏洩対策をしていますか | 2 | 2 | 100% | 0 | 0 | 項目なし | 100% |
| 8. アクセス権について、ルールを定めて管理していますか | 2 | 2 | 100% | 2 | 1 | 50% | 75% |
| 9. 情報資産について、ルールを定めて管理していますか | 3 | 2 | 67% | 3 | 2 | 67% | 67% |
| 10. 情報資産のセキュリティリスクを特定し、対策していますか | 3 | 3 | 100% | 0 | 0 | 項目なし | 100% |
| 11. 取引先との取引による情報漏えいの対策をしていますか | 1 | 1 | 100% | 0 | 0 | 項目なし | 100% |
| 12. 外部情報システムの利用について、安全性と信頼性を確保していますか | 1 | 0 | 0% | 1 | 1 | 100% | 50% |
| 13. 社内ネットワークの利用について、事故防止の対策をしていますか | 1 | 1 | 100% | 1 | 0 | 0% | 50% |
| 14. サーバー等の重要機器への不正アクセスの対策をしていますか | 1 | 1 | 100% | 7 | 2 | 29% | 38% |
| 15. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか | 0 | 0 | 項目なし | 9 | 6 | 67% | 67% |
| 16. 情報システムの不正利用の対策や、安全稼働させる対策をしていますか | 3 | 3 | 100% | 3 | 2 | 67% | 83% |
| 17. パッチやアップデート適用ができていますか | 1 | 0 | 0% | 2 | 0 | 0% | 0% |
| 18. データの保護をしていますか | 0 | 0 | 項目なし | 1 | 1 | 100% | 100% |
| 19. オフィスツールを安全に利用できる対策をしていますか | 0 | 0 | 項目なし | 3 | 1 | 33% | 33% |
| 20. マルウェア対策・不正アクセスの検知をしていますか | 1 | 1 | 100% | 3 | 0 | 0% | 25% |
| 21. バックアップと復元を計画的に実施していますか | 3 | 0 | 0% | 2 | 0 | 0% | 0% |

解説講座の各講座に対応する項目と達成状況

■ステージ1

| | | 項目数 | 達成数 | 達成率 | 達成状況 |
|---|---|---|---|---|---|
| 講義① | 1. 情報セキュリティ方針（ポリシー）を作成・活用していますか<br>2. 機密情報を扱うルールを策定・実行していますか<br>3. 法令の順守について、ルールを策定・実行していますか | 5 | 5 | 100% | ◎ |
| 講義② | 4. 平時の情報セキュリティリスクを管理する体制を整備していますか<br>5. 情報セキュリティ事件・事故を予防する日常的な教育をしていますか<br>6. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか | 4 | 2 | 50% | △ |
| 講義③ | 7. サプライチェーンからの情報漏洩対策をしていますか<br>8. アクセス権について、ルールを定めて管理していますか<br>9. 情報資産について、ルールを定めて管理していますか | 7 | 6 | 86% | ○ |
| 講義④ | 10. 情報資産のセキュリティリスクを特定し、対策していますか<br>11. 取引先との取引による情報漏えいの対策をしていますか<br>12. 外部情報システムの利用について、安全性と信頼性を確保できていますか<br>13. 社内ネットワークの利用について、事故防止の対策ができていますか | 6 | 5 | 83% | ○ |
| 講義⑤ | 14. サーバー等の重要機器への不正アクセスの対策をしていますか<br>15. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか<br>16. 情報システムの不正利用の対策や、安全稼働させる対策をしていますか<br>17. パッチやアップデート適用ができていますか<br>18. データの保護をしていますか<br>19. オフィスツールを安全に利用できる対策をしていますか | 5 | 4 | 80% | ○ |
| 講義⑥ | 20. マルウェア対策・不正アクセスの検知をしていますか<br>21. バックアップと復元を計画的に実施していますか | 4 | 1 | 25% | × |




■ステージ2

| | | 項目数 | 達成数 | 達成率 | 達成状況 |
|---|---|---|---|---|---|
| 講義① | 2. 情報セキュリティ方針（ポリシー）を作成・活用していますか<br>3. 機密情報を扱うルールを策定・実行していますか<br>4. 法令の順守について、ルールを策定・実行していますか | 5 | 5 | 100% | ◎ |
| 講義② | 5. 平時の情報セキュリティリスクを管理する体制を整備していますか<br>6. 情報セキュリティ事件・事故を予防する日常的な教育をしていますか<br>7. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか | 7 | 2 | 29% | × |
| 講義③ | 8. サプライチェーンからの情報漏洩対策をしていますか<br>9. アクセス権について、ルールを定めて管理していますか<br>10. 情報資産について、ルールを定めて管理していますか | 5 | 3 | 60% | △ |
| 講義④ | 11. 情報資産のセキュリティリスクを特定し、対策していますか<br>12. 取引先との取引による情報漏えいの対策をしていますか<br>13. 外部情報システムの利用について、安全性と信頼性を確保できていますか<br>14. 社内ネットワークの利用について、事故防止の対策ができていますか | 2 | 1 | 50% | △ |
| 講義⑤ | 15. サーバー等の重要機器への不正アクセスの対策をしていますか | 7 | 2 | 29% | × |
| 講義⑥ | 16. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか | 9 | 6 | 67% | △ |
| 講義⑤ | 17. 情報システムの不正利用の対策や、安全稼働させる対策をしていますか<br>18. パッチやアップデート適用ができていますか<br>19. データの保護をしていますか<br>20. オフィスツールを安全に利用できる対策をしていますか | 9 | 4 | 44% | × |
| 講義⑥ | 21. マルウェア対策・不正アクセスの検知をしていますか<br>22. バックアップと復元を計画的に実施していますか | 9 | 6 | 67% | △ |




※「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」 や「IPA 中小企業の情報セキュリティ対策ガイドライン」、「IPA 情報セキュリティ対策ベンチマーク」など

# コンサルタントの解説動画でチェックシートの各項目への理解を深めましょう

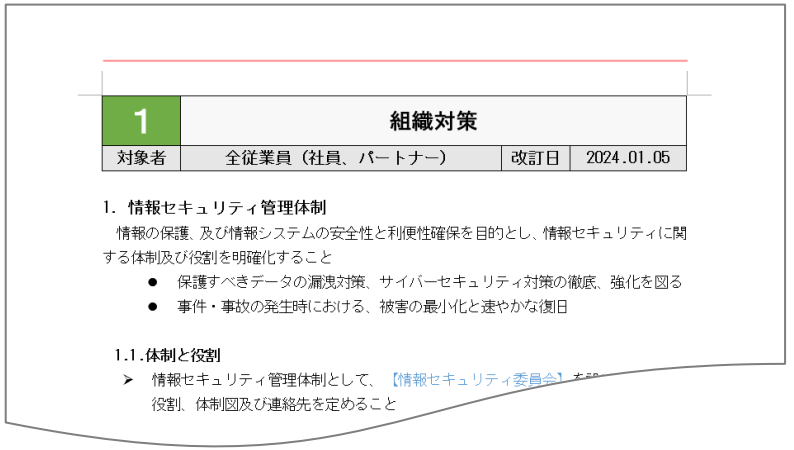
# 整備が必須となる各種セキュリティ関連規程のひな型もご提供します

## サイバーセキュリティ対策の基礎知識を身につけられる「解説講座」

セキュリティ対策の強化を実施する際に必ず知っておきたい基礎知識や対策のポイントをコンサルタントが解説。
1講義は約20分程度のため、すき間時間に自由なペースで、「いつでも・何度でも・何人でも」学ぶことができます。


## 「各種セキュリティ関連規程ひな形」を編集可能な形式でご提供

組織のセキュリティ体制を構築するために必ず必要となる各種規程類のひな型をご提供。
Word・Excelなどの編集可能な形式でダウンロードできるため、自社にあわせて必要な箇所を編集するだけで完成します。



| 1 | 組織対策 | | |
|---|---|---|---|
| 対象者 | 全従業員（社員、パートナー） | 改訂日 | 2024.01.05 |

1. 情報セキュリティ管理体制

情報の保護、及び情報システムの安全性と利便性確保を目的とし、情報セキュリティに関する体制及び役割を明確化すること

- 保護すべきデータの漏洩対策、サイバーセキュリティ対策の徹底、強化を図る
- 事件・事故の発生時における、被害の最小化と速やかな復日

1.1.体制と役割

➢ 情報セキュリティ管理体制として、【情報セキュリティ委員会】を
役割、体制図及び連絡先を定めること

困ったときには経験豊富なコンサルタントが、Web会議・メールでサポートします

# ご契約者様専用ポータルサイトですき間時間に自由なペースで進められる


エムオーテックスのYoutubeチャンネルに、ご契約者様専用ポータルサイトのご紹介動画を掲載しております。ご参考ください。
（動画時間：1分38秒）

>>https://www.youtube.com/watch?v=BKaK_zu_8yk

※You Tubeのエムオーテックス営業部チャンネルに遷移し、動画が再生されます

# ５．提供内容・価格と活用のモデルケース

# 2つのコースと提供価格

＼ まずは自社の現状や課題を把握したい ／

## 学習コース

定価：¥225,000

利用期間：3ヵ月

**こんな方におすすめ**

- セキュリティ対策・ガイドラインの内容が理解できていない
- 自社で取り組んだセキュリティ対策の内容の妥当性に不安がある
- 各種セキュリティ関連規程のひな型が欲しい

＼ 改善を進めたい・セキュリティレベルを維持したい ／

## 実践コース

【新規購入時】

定価：¥450,000

利用期間：9ヵ月

【継続更新】

定価：¥120,000

利用期間：12ヵ月

**こんな方におすすめ**

- 対策を進めるノウハウを知りたい
- 対策見直しへアドバイスが欲しい
- 従業員へセキュリティ教育をしたい
- 困ったときに専門家に相談したい
- 申請書などのフォーマットが欲しい

（価格は税別表示です）

# 活用のモデルケース

サイバーセキュリティ対策に取り組むのが初めてで、まずはサイバーセキュリティ対策の内容に対して理解を深めるところから始めたい

2024/8 新規購入
**学習コース**
**定価：¥225,000**
**利用期間：3ヵ月**

2024/11 アップグレード
**実践コース アップグレード**
**定価：¥225,000※**
**利用期間：6ヵ月**

2025/4　継続更新
**実践コース 年間継続プログラム**
**定価：¥120,000**
**利用期間：12ヵ月**

※アップグレードの場合は「学習コース」との差額のみで「実践コース」を利用できます

サイバーセキュリティ対策の基準に対して不足している項目をどんどん対策して、セキュリティ対策の強化に取り組みたい

2024/8 新規購入
**実践コース**
**定価：¥450,000**
**利用期間：9ヵ月**

2025/4　継続更新
**実践コース 年間継続プログラム**
**定価：¥120,000**
**利用期間：12ヵ月**



（価格は税別表示です）

# 提供内容（詳細）

| | | | 学習コース | 実践コース |
|---|---|---|---|---|
| 学習・現状把握 | チェックシート | お客様の現状把握が可能なサイバーセキュリティに特化したチェックシートをご提供します。 | ● | ● |
| | 解説講座 | サイバーセキュリティ対策に必要な知識の習得を目的とした講座動画をご提供します。<br>専用ポータルからいつでも何度でも視聴できます。 | ● | ● |
| | チェックシート添削 | お客様にてチェックシートに記入した内容を、セキュリティコンサルタントが確認し、記載内容の妥当性をアドバイスします。 | ●※ | ●※ |
| 計画 | カウンセリング | お客様にてチェックシートに記入した内容を、セキュリティコンサルタントが確認し、視聴すべき対策講座と対策プログラムをご提供します。 | - | ●※ |
| 改善 | 各種規程ひな型 | 各種セキュリティ関連規程のひな型をご提供します。 | ● | ● |
| | 対策講座 | サイバーセキュリティ対策に必要な実際に対策を行うためのポイントを解説した講座動画をご提供します。<br>専用ポータルからいつでも何度でも視聴できます。 | - | ● |
| | 教育コンテンツ | サイバーセキュリティ対策に必要となる従業員教育について、集合研修等で活用できる説明資料と理解度確認テストをご提供します。 | - | ● |
| | 各種運用支援ツール | 管理台帳や申請書などの各種フォーマットをご提供します。 | - | ● |
| サポート | 個別相談（メール） | メールによる個別相談をご提供します。 | ● | ● |
| | 個別相談（Web会議） | オンラインによる個別相談をご提供します。 | ●※ | ●※ |
| | よろづ相談会 | テーマに沿った相談会を開催します。 | - | ● |
| | お役立ち情報配信 | ガイドラインの改定や、セキュリティ対策に関連する法令の変更、最新のサイバー攻撃情報など、サイバーセキュリティ対策の見直しに役立つ情報を配信します。 | - | ● |

※実施回数の制限があります。

# 価格

| 種別 | 名称 | 価格（税別） | 利用期間 | 提供内容に含まれる実施回数 | | |
|---|---|---|---|---|---|---|
| | | | | 個別相談（Web会議） | チェックシート添削 | カウンセリング |
| 基本 | ガイドライン対応サポートアカデミー サイバーセキュリティ対策パッケージ 学習コース | ¥225,000 | 3か月 | 3回 | 1回 | - |
| 基本 | ガイドライン対応サポートアカデミー サイバーセキュリティ対策パッケージ 実践コース | ¥450,000 | 9か月 | 9回 | 2回 | 1回 |
| オプション | ガイドライン対応サポートアカデミー サイバーセキュリティ対策パッケージ 実践コース アップグレード | ¥225,000 | 6か月 | 9回※ | 2回※ | 1回※ |
| オプション | ガイドライン対応サポートアカデミー 個別相談 追加オプション | ¥50,000 | - | 1回 | - | - |
| 更新 | ガイドライン対応サポートアカデミー サイバーセキュリティ対策パッケージ 実践コース 年間継続プログラム | ¥120,000 | 12か月 | 12回 | 2回 | 1回 |

・初回購入時は「基本」のうち「学習コース」「実践コース」のいずれかの購入が必須となります。
・「学習コース」の購入企業が「実践コース」を利用したい場合、「実践コース アップグレード」を購入することで、差額のみで利用できます。
・「学習コース」の購入企業が「実践コース 年間継続プログラム」を利用したい場合は、先に「実践コース アップグレード」を購入してください。
・「実践コース 年間継続プログラム」は、「実践コース」または「実践コース アップグレード」の提供期間満了日の翌月1日が提供開始日となります。
「継続プログラム」 を「実践コース」または「実践コース アップグレード」の提供期間満了日を過ぎてから購入する場合、その満了日の翌月1日を「継続プロブラム」提供開始日とし、遡りでの購入となります。

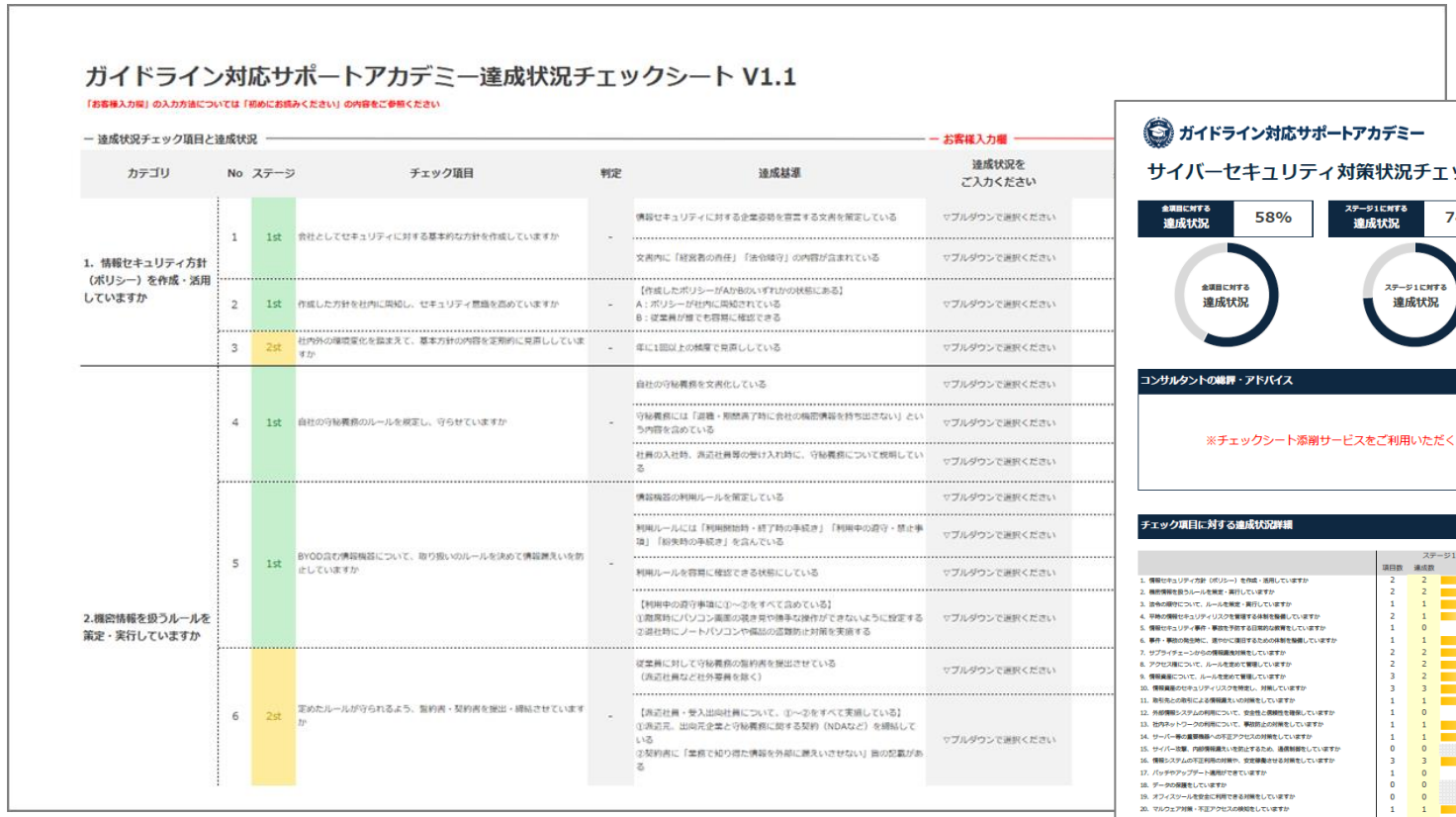
※「学習コース」の実施回数に、「実践コース　アップグレード」で追加された回数分の合計回数です

# ５．提供内容の詳細

# チェックシート

サイバーセキュリティ対策として実施が必要な事項を定義したチェックシートをご提供します。
現在の対策状況を入力することで、自社の弱点が一目でわかる結果サマリーを作成できます。

本チェックシートは、主に以下の内容をベンチマークして作成しています。
・経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク
・IPA 中小企業の情報セキュリティ対策ガイドライン
・情報セキュリティ対策ベンチマーク（IPA 独立行政法人情報処理推進機構）

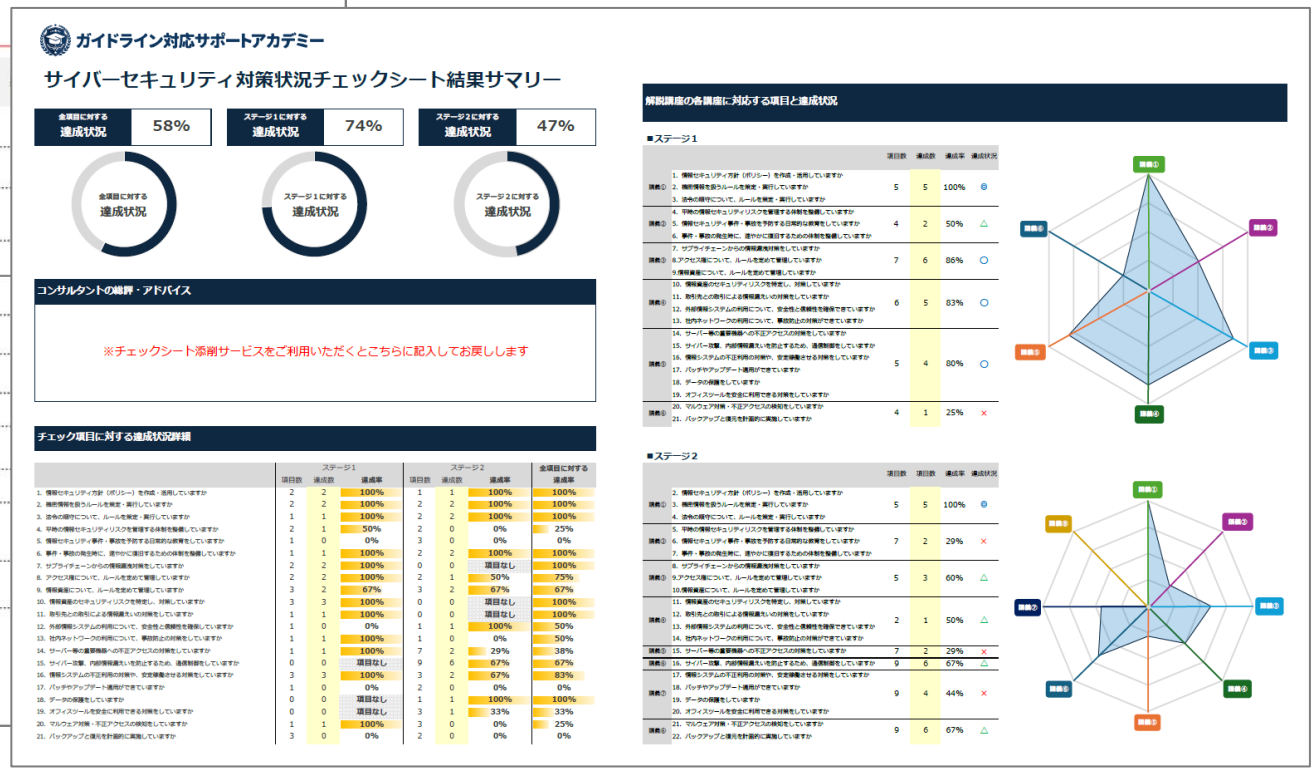


ガイドライン対応サポートアカデミー達成状況チェックシート V1.1

「お客様入力欄」の入力方法については「初めにお読みください」の内容をご参照ください

達成状況チェック項目と達成状況 — お客様入力欄

| カテゴリ | No | ステージ | チェック項目 | 判定 | 達成基準 | 達成状況をご入力ください |
|---|---|---|---|---|---|---|
| 1. 情報セキュリティ方針（ポリシー）を作成・活用していますか | 1 | 1st | 会社としてセキュリティに対する基本的な方針を作成していますか | - | 情報セキュリティに対する企業姿勢を宣言する文書を策定している | ▽プルダウンで選択ください |
| | | | | | 文書内に「経営者の責任」「法令順守」の内容が含まれている | ▽プルダウンで選択ください |
| | 2 | 1st | 作成した方針を社内に周知し、セキュリティ意識を高めていますか | - | 【作成したポリシーがA/Bのいずれかの状態にある】<br>A：ポリシーが社内に周知されている<br>B：従業員が誰でも容易に確認できる | ▽プルダウンで選択ください |
| | 3 | 2st | 社内外の環境変化を踏まえて、基本方針の内容を定期的に見直していますか | - | 年に1回以上の頻度で見直ししている | ▽プルダウンで選択ください |
| 2.機密情報を扱うルールを策定・実行していますか | 4 | 1st | 自社の守秘義務のルールを規定し、守らせていますか | - | 自社の守秘義務を文書化している | ▽プルダウンで選択ください |
| | | | | | 守秘義務には「退職・刑懲責了時に会社の機密情報を持ち出さない」という内容を含めている | ▽プルダウンで選択ください |
| | | | | | 社員の入社時、派遣社員等の受け入れ時に、守秘義務について規則している | ▽プルダウンで選択ください |
| | 5 | 1st | BYOD含む情報機器について、取り扱いのルールを決めて情報漏洩を防止していますか | - | 情報機器の利用ルールを策定している | ▽プルダウンで選択ください |
| | | | | | 利用ルールには「利用開始時・終了時の手続き」「利用中の遵守・禁止事項」「紛失時の手続き」を含んでいる | ▽プルダウンで選択ください |
| | | | | | 利用ルールを容易に確認できる状態にしている | ▽プルダウンで選択ください |
| | | | | | 【利用中の遵守事項に①～②をすべて含めている】<br>①職務時にパソコン画面の覗き見や勝手な操作ができないように設定する<br>②退社時にノートパソコンや個品の盗難防止対策を実施する | ▽プルダウンで選択ください |
| | 6 | 2st | 定めたルールが守られるよう、誓約書・契約書を提出・締結させていますか | - | 従業員に対して守秘義務の誓約書を提出させている<br>（派遣社員など社外等員を除く） | ▽プルダウンで選択ください |
| | | | | | 【派遣社員・受入出向社員について、①～②をすべて実施している】<br>①派遣元、出向元企業と守秘義務に関する契約（NDAなど）を締結している<br>②契約書に「業務で知り得た情報を外部に漏洩いさせない」旨の記載がある | ▽プルダウンで選択ください |



ガイドライン対応サポートアカデミー

サイバーセキュリティ対策状況チェックシート結果サマリー

| 全項目に対する達成状況 | 58% | ステージ1に対する達成状況 | 74% | ステージ2に対する達成状況 | 47% |
|---|---|---|---|---|---|

コンサルタントの講評・アドバイス

※チェックシート添削サービスをご利用いただくとこちらに記入してお戻しします

チェック項目に対する達成状況詳細

| | ステージ1 項目数 | ステージ1 達成数 | ステージ1 達成率 | ステージ2 項目数 | ステージ2 達成数 | ステージ2 達成率 | 全項目に対する達成率 |
|---|---|---|---|---|---|---|---|
| 1. 情報セキュリティ方針（ポリシー）を作成・活用していますか | 2 | 2 | 100% | 1 | 1 | 100% | 100% |
| 2. 機密情報を扱うルールを策定・実行していますか | 2 | 2 | 100% | 2 | 2 | 100% | 100% |
| 3. 法令の順守について、ルールを策定・実行していますか | 1 | 1 | 100% | 2 | 2 | 100% | 100% |
| 4. 平時の情報セキュリティリスクを管理する体制を整備していますか | 2 | 1 | 50% | 2 | 0 | 0% | 25% |
| 5. 情報セキュリティ事件・事故を予防する目的の教育をしていますか | 1 | 0 | 0% | 3 | 0 | 0% | 0% |
| 6. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか | 1 | 1 | 100% | 2 | 2 | 100% | 100% |
| 7. サプライチェーンからの情報漏洩対策をしていますか | 2 | 2 | 100% | 0 | 0 | 項目なし | 100% |
| 8. アクセス権について、ルールを定めて管理していますか | 2 | 2 | 100% | 2 | 1 | 50% | 75% |
| 9. 情報資産について、ルールを定めて管理していますか | 3 | 2 | 67% | 3 | 2 | 67% | 67% |
| 10. 情報資産のセキュリティリスクを特定し、対策していますか | 3 | 3 | 100% | 0 | 0 | 項目なし | 100% |
| 11. 取引先との取引による情報漏えいの対策をしていますか | 1 | 1 | 100% | 0 | 0 | 項目なし | 100% |
| 12. 外部情報システムの利用について、安全性と信頼性を確保していますか | 1 | 0 | 0% | 1 | 1 | 100% | 50% |
| 13. 社内ネットワークの利用について、事故防止の対策をしていますか | 1 | 1 | 100% | 1 | 0 | 0% | 50% |
| 14. サーバー等の重要機器への不正アクセスの対策をしていますか | 1 | 1 | 100% | 7 | 2 | 29% | 38% |
| 15. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか | 0 | 0 | 項目なし | 9 | 6 | 67% | 67% |
| 16. 情報システムの不正利用の対策や、安定稼働させる対策をしていますか | 3 | 3 | 100% | 3 | 2 | 67% | 83% |
| 17. バッチやアップデート適用ができていますか | 1 | 0 | 0% | 2 | 0 | 0% | 0% |
| 18. データの保護をしていますか | 0 | 0 | 項目なし | 1 | 1 | 100% | 100% |
| 19. オフィスツールを安全に利用できる対策をしていますか | 0 | 0 | 項目なし | 3 | 1 | 33% | 33% |
| 20. マルウェア対策・不正アクセスの検知をしていますか | 1 | 1 | 100% | 3 | 0 | 0% | 25% |
| 21. バックアップと復元を計画的に実施していますか | 3 | 0 | 0% | 2 | 0 | 0% | 0% |

解説講座の各講座に対応する項目と達成状況

■ステージ1

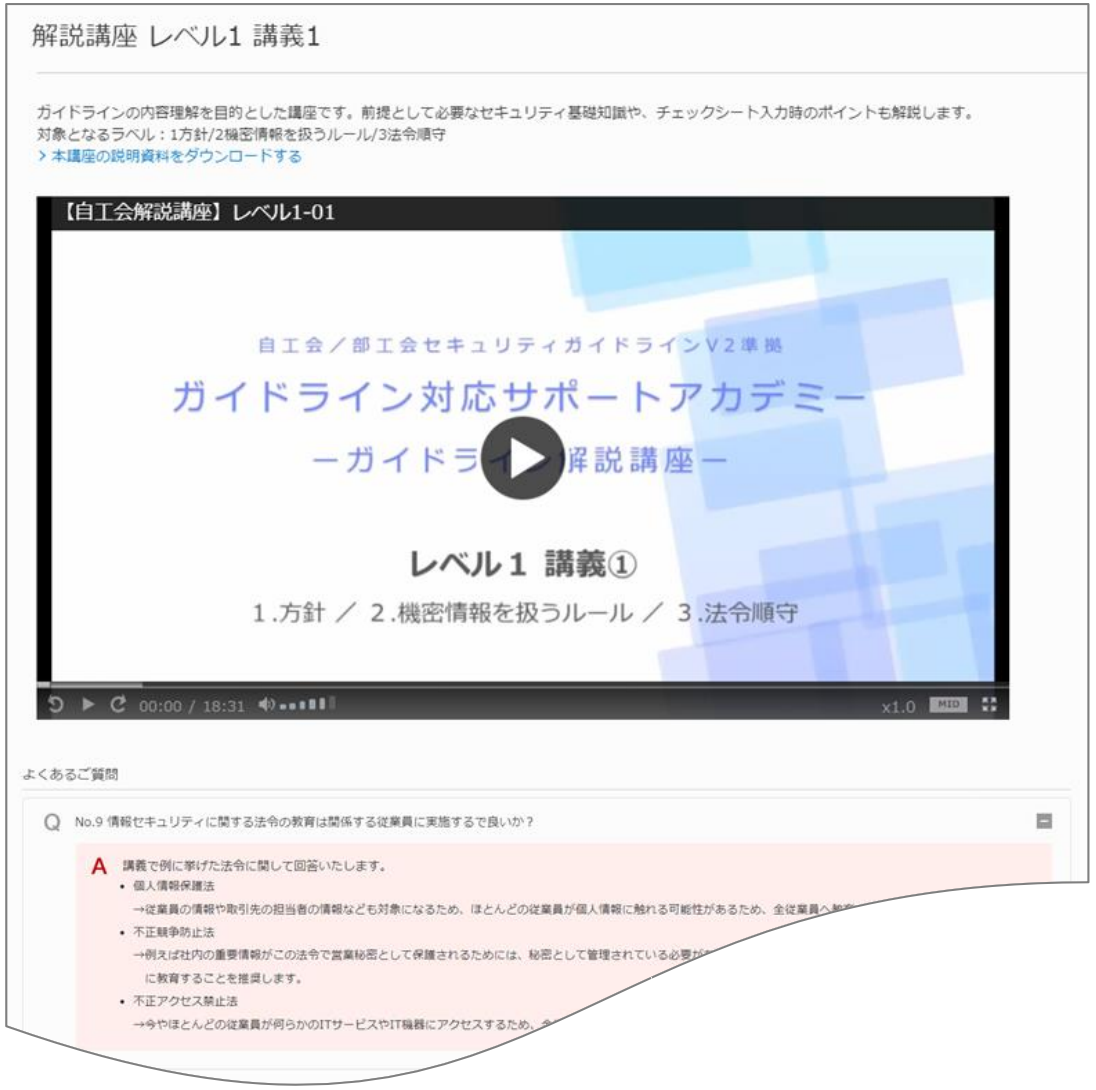
| | | 項目数 | 達成数 | 達成率 | 達成状況 |
|---|---|---|---|---|---|
| 講義① | 1. 情報セキュリティ方針（ポリシー）を作成・活用していますか<br>2. 機密情報を扱うルールを策定・実行していますか<br>3. 法令の順守について、ルールを策定・実行していますか | 5 | 5 | 100% | ◎ |
| 講義② | 4. 平時の情報セキュリティリスクを管理する体制を整備していますか<br>5. 情報セキュリティ事件・事故を予防する目的の教育をしていますか<br>6. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか | 4 | 2 | 50% | △ |
| 講義③ | 7. サプライチェーンからの情報漏洩対策をしていますか<br>8. アクセス権について、ルールを定めて管理していますか<br>9. 情報資産について、ルールを定めて管理していますか | 7 | 6 | 86% | ○ |
| 講義④ | 10. 情報資産のセキュリティリスクを特定し、対策していますか<br>11. 取引先との取引による情報漏えいの対策をしていますか<br>12. 外部情報システムの利用について、安全性と信頼性を確保できていますか<br>13. 社内ネットワークの利用について、事故防止の対策ができていますか | 6 | 5 | 83% | ○ |
| 講義⑤ | 14. サーバー等の重要機器への不正アクセスの対策をしていますか<br>15. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか<br>16. 情報システムの不正利用の対策や、安定稼働させる対策をしていますか<br>17. バッチやアップデート適用ができていますか<br>18. データの保護をしていますか<br>19. オフィスツールを安全に利用できる対策をしていますか | 5 | 4 | 80% | ○ |
| 講義⑥ | 20. マルウェア対策・不正アクセスの検知をしていますか<br>21. バックアップと復元を計画的に実施していますか | 4 | 1 | 25% | × |



■ステージ2

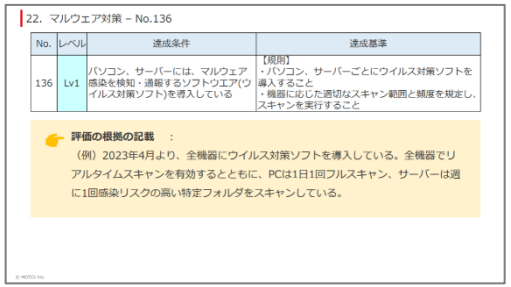
| | | 項目数 | 項目数 | 達成率 | 達成状況 |
|---|---|---|---|---|---|
| 講義① | 2. 機密情報を扱うルールを策定・実行していますか<br>3. 法令の順守について、ルールを策定・実行していますか | 5 | 5 | 100% | ◎ |
| 講義② | 5. 平時の情報セキュリティリスクを管理する体制を整備していますか<br>6. 情報セキュリティ事件・事故を予防する目的の教育をしていますか<br>7. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか | 7 | 2 | 29% | × |
| 講義③ | 8. サプライチェーンからの情報漏洩対策をしていますか<br>9. アクセス権について、ルールを定めて管理していますか<br>10. 情報資産について、ルールを定めて管理していますか | 5 | 3 | 60% | △ |
| 講義④ | 11. 情報資産のセキュリティリスクを特定し、対策していますか<br>12. 取引先との取引による情報漏えいの対策をしていますか<br>13. 外部情報システムの利用について、安全性と信頼性を確保できていますか<br>14. 社内ネットワークの利用について、事故防止の対策ができていますか | 2 | 1 | 50% | △ |
| 講義⑤ | 15. サーバー等の重要機器への不正アクセスの対策をしていますか | 7 | 2 | 29% | × |
| 講義⑥ | 16. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか | 9 | 6 | 67% | △ |
| 講義⑦ | 17. 情報システムの不正利用の対策や、安定稼働させる対策をしていますか<br>18. バッチやアップデート適用ができていますか<br>19. データの保護をしていますか<br>20. オフィスツールを安全に利用できる対策をしていますか | 9 | 4 | 44% | × |
| 講義⑧ | 21. マルウェア対策・不正アクセスの検知をしていますか<br>22. バックアップと復元を計画的に実施していますか | 9 | 6 | 67% | △ |

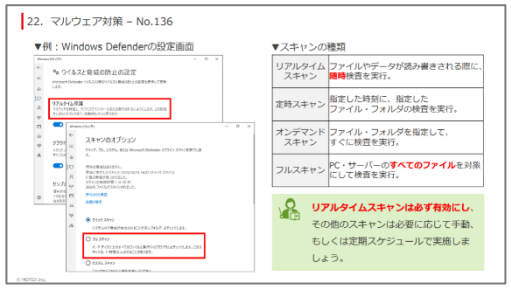
サイバーセキュリティ対策への理解を深め、対応を進めるためのノウハウをコンサルタントが分かりやすく解説した動画講座です。
視聴回数に制限はなく、利用期間中はいつでも何度でも視聴できます。




## 資料ダウンロード

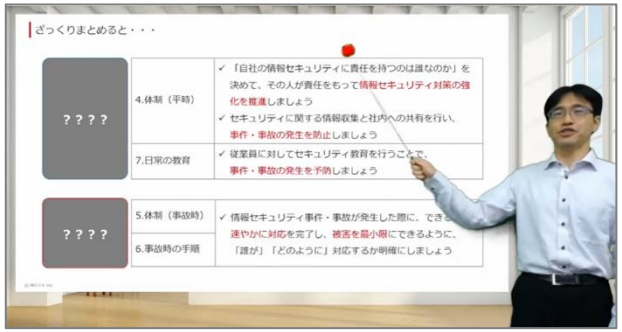
青文字のリンクから、講座内の投影資料をダウンロードできます。



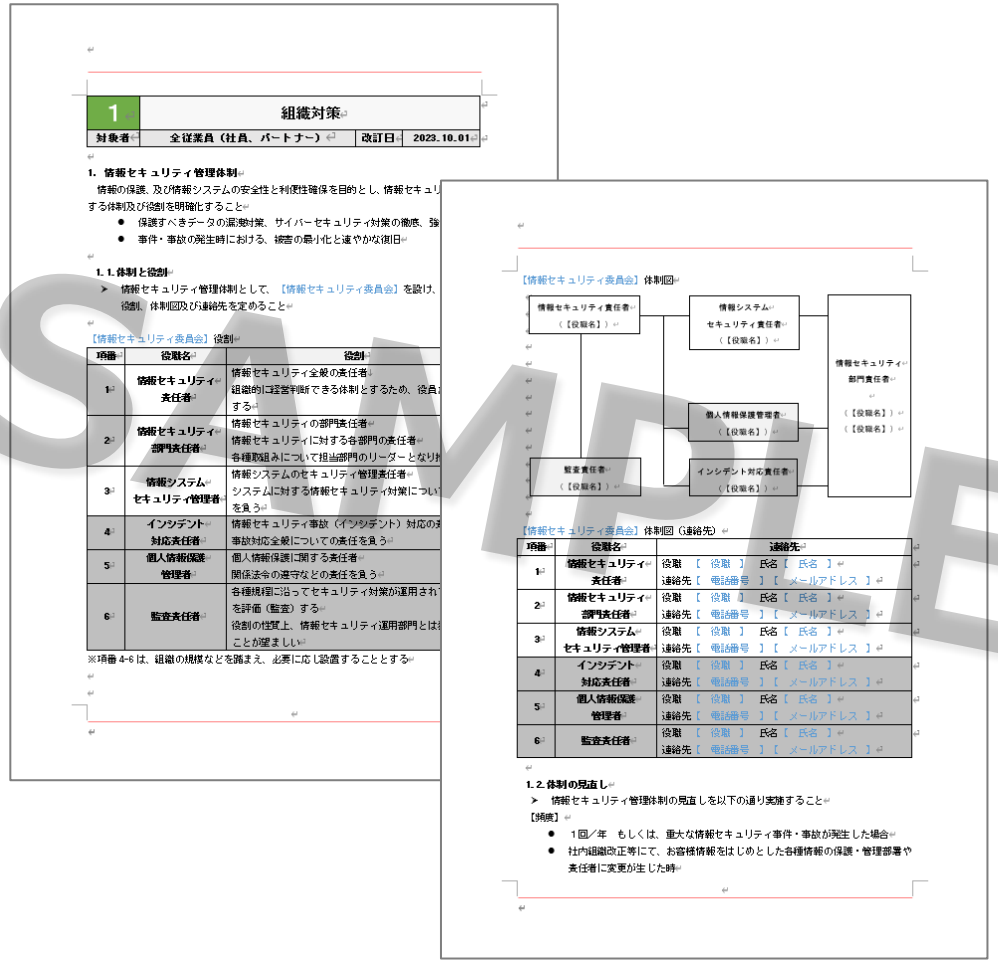

## 動画視聴・よくあるご質問

講座動画を視聴できます。
講座内容の疑問について、
よくあるご質問で解決し
ない場合には個別相談より
お問い合わせください。



# 各種規程ひな型

各種セキュリティ関連規程のひな型をご提供します。チェックシートの全項目に対応するために必要となる規程類をすべてご用意しています。



| ご提供する規程一覧 |
| --- |
| 情報セキュリティ方針案 |
| 組織対策 |
| 人的対策 |
| 情報資産保護 |
| 物理環境保護 |
| 端末管理 |
| システム管理 |
| システム管理（アクセス制御及び認証） |
| 外部委託先管理 |
| セキュリティ事故対応 |
| インシデント対応手順 |

# 教育コンテンツ

サイバーセキュリティ対策として必要となる従業員への教育について、集合研修等で活用できる説明資料と理解度確認テストをご提供します。
一般従業員向けの教育コンテンツは、情報システムやセキュリティに対する知識が少ない従業員の方にも理解していただけるよう、各テーマの『きほんの「き」』をわかりやすく解説します。


| 分類 | 名称 |
|---|---|
| 従業員向け | 【基礎1】情報セキュリティ対策方針 |
| | 【基礎2】業務で利用する情報機器の利用ルール |
| | 【基礎3】情報セキュリティ事件・事故の予防と発生時の対応 |
| | 【基礎4】重要情報の漏えいを防止するためのルール |
| | 【基礎5】その他の情報セキュリティ関連ルール |
| | 理解度チェックテスト |
| 管理者向け | 【管理者向け教育資料】部門管理者の役割と責任 |
| 経営層向け | 【経営者向け教育資料】経営者の役割と責任 |

# 各種運用支援ツール

サイバーセキュリティ対策に必要となる管理台帳や申請書などの各種フォーマットをご提供します。
全て編集可能な形式でダウンロードできますので、必要な個所をカスタマイズして活用できます。

## ▼情報資産管理台帳の例

| No | 社外提供 | 分類 | 機密区分 | 資産名 | 管理責任者 | 資産価値 | | | 脅威 | ぜい弱 | リスク値／リスク評価 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 機密性 | 完全性 | 可用性 | | | 機密性 | | 完全性 | | 可用性 | |
| 1 | 提供する | 顧客情報 | 社外秘 | 各お客様向けの提案資料 | MO一郎 | 2 | 2 | 2 | 3 | 2 | 12 | 小 | 12 | 小 | 12 | 小 |
| 2 | 提供しない | 顧客情報 | 社外秘 | 展示会来場者名簿 | MO一郎 | 4 | 3 | 2 | 2 | 2 | 16 | 中 | 12 | 小 | 8 | 小 |
| 3 | 提供しない | 社員情報 | 社外秘 | 携帯電話番号一覧 | MO一郎 | 2 | 1 | 2 | 2 | 2 | 8 | 小 | 4 | 小 | 8 | 小 |
| 4 | 提供する | 営業資料 | 公開 | チラシ、汎用的な提案資料 | MO一郎 | 1 | 1 | 3 | 2 | 2 | 4 | 小 | 4 | 小 | 12 | 小 |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |



## ▼入退出管理台帳の例

入室先：

| No | 日付 | 所属（会社名） | 入室者名（氏名） | 連絡先 | 入室目的 | 入室時刻 | 退出時刻 | 確認者 | 承認者 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | ／ | | | | | : | : | | |
| 2 | ／ | | | | | : | : | | |
| 3 | ／ | | | | | : | : | | |
| 4 | ／ | | | | | : | : | | |
| 5 | ／ | | | | | : | : | | |
| 6 | ／ | | | | | : | : | | |
| 7 | ／ | | | | | : | : | | |
| 8 | ／ | | | | | : | : | | |
| 9 | ／ | | | | | : | : | | |
| 10 | ／ | | | | | : | : | | |



| 名称 |
|---|
| 誓約書（守秘事項）の文章案） |
| 機密保持契約書の文章案 |
| 退職/期間満了時の回収物一覧チェックシート |
| インシデント管理台帳 |
| ID/アクセス権管理台帳 |
| 共有ID利用台帳 |
| アクセス権管理ルール遵守状況チェックリスト |
| 情報資産管理台帳 |
| 機密区分運用ルール遵守状況チェックリスト |
| 取り交わし情報一覧表 |
| 外部情報システム管理台帳 |
| ヒヤリハットテンプレート |
| 入退室管理台帳 |
| 持ち込み物管理台帳 |
| FWフィルタリング設定台帳 |
| 管理者権限管理台帳 |
| サーバ・NW機器設定変更作業申請書 |

# チェックシート添削／カウンセリング

「チェックシート添削」と「カウンセリング」は、お客様にて入力された、チェックシートをMOTEXへ提出いただき実施します。

### ❶お申込み

契約者ポータルの「お問い合わせ」より「チェックシート添削」もしくは「カウンセリング」の利用を申し込む。

### ❷チェックシート提出

担当者よりオンラインストレージのURLをご連絡。お客様にて入力済みチェックシートをアップロードしてご提出。

### ❸ご提供

MOTEXのコンサルタントがチェックシートの記載内容を確認し、添削、もしくは達成プログラムを作成してご提供。

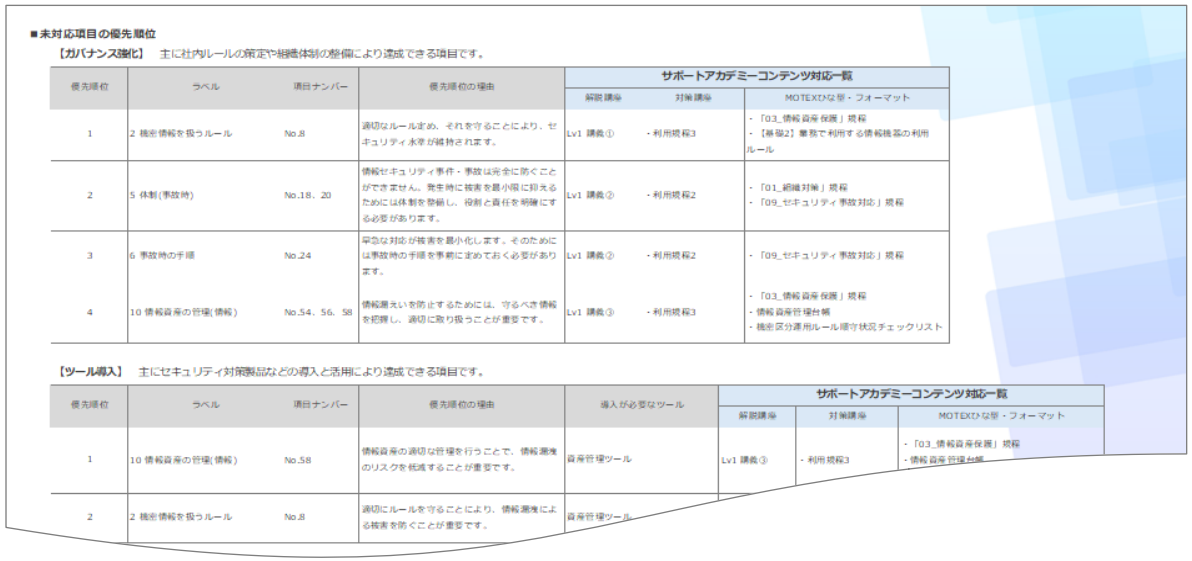
## チェックシート添削

見落としがちな達成基準を満たしているかなど、記載内容の妥当性を確認し、アドバイスします。

| 達成条件 | | 評価結果 | | MOTEX回答 |
|---|---|---|---|---|
| | | 達成条件 | 評価の根拠記入欄 | |
| 情報セキュリティ対応方針(ポリシー)を社内に周知している | ～～ | 2 | ●●●規程 | 周知方法は決められていますか |
| スマートデバイスへのアプリケーションの無断インストールを制限し、定期的にインストール状況を確認している | | 0 | ●●年度中に検討 | MDMにてインストール制限を実施されているのであれば、2（対策完了）と判断いただけるかと存じます |
| 情報資産において「機密性」「完全性」「可用性」の3要素が確保できなくなった場合のリスクを特定できている | | 2 | ●●●規程 | 「達成基準」に記載の点検（リスクアセスメント）を実施する必要があります |

## カウンセリング

お客様ごとに「対策プログラム」を作成し、対応優先度や導入が必要なセキュリティ対策ツールなどをアドバイスします。



■未対応項目の優先順位

【ガバナンス強化】　主に社内ルールの策定や組織体制の整備により達成できる項目です。

| 優先順位 | ラベル | 項目ナンバー | 優先順位の理由 | サポートアカデミーコンテンツ対応一覧 | | |
|---|---|---|---|---|---|---|
| | | | | 解説講座 | 対策講座 | MOTEXひな型・フォーマット |
| 1 | 2 機密情報を扱うルール | No.8 | 適切なルール定め、それを守ることにより、セキュリティ水準が維持されます。 | Lv1 講義① | ・利用規程3 | ・「03_情報資産保護」規程<br>・【事例2】業務で利用する情報機器の利用ルール |
| 2 | 5 体制(事故時) | No.18、20 | 情報セキュリティ事件・事故は完全に防ぐことができません。発生時に被害を最小限に抑えるためには体制を整備し、役割と責任を明確にする必要があります。 | Lv1 講義② | ・利用規程2 | ・「01_組織対策」規程<br>・「09_セキュリティ事故対応」規程 |
| 3 | 6 事故時の手順 | No.24 | 早急な対応が被害を最小化します。そのためには事故時の手順を事前に定めておく必要があります。 | Lv1 講義② | ・利用規程2 | ・「09_セキュリティ事故対応」規程 |
| 4 | 10 情報資産の管理(情報) | No.54、56、58 | 情報漏えいを防止するためには、守るべき情報を把握し、適切に取り扱うことが重要です。 | Lv1 講義③ | ・利用規程3 | ・「03_情報資産保護」規程<br>・情報資産管理台帳<br>・機密区分運用ルール順守状況チェックリスト |

【ツール導入】　主にセキュリティ対策製品などの導入と活用により達成できる項目です。

| 優先順位 | ラベル | 項目ナンバー | 優先順位の理由 | 導入が必要なツール | サポートアカデミーコンテンツ対応一覧 | | |
|---|---|---|---|---|---|---|---|
| | | | | | 解説講座 | 対策講座 | MOTEXひな型・フォーマット |
| 1 | 10 情報資産の管理(情報) | No.58 | 情報資産の適切な管理を行うことで、情報漏洩のリスクを低減することが重要です。 | 資産管理ツール | Lv1 講義③ | ・利用規程3 | ・「03_情報資産保護」規程<br>・情報資産管理台帳 |
| 2 | 2 機密情報を扱うルール | No.8 | 適切にルールを守ることにより、情報漏洩による被害を防ぐことが重要です。 | 資産管理ツール | | | |


**製品に関するお問い合わせ**

■ 営業本部

| | |
|---|---|
| 大阪本社 | 06-6308-8980 |
| 東京本部 | 03-3455-1811 |
| 名古屋支店 | 052-253-7346 |
| 九州営業所 | 092-419-2390 |
| E-mail | sales@motex.co.jp |

**ご導入後の製品利用に関するお問い合わせ**

| | |
|---|---|
| サポートセンター | 0120-968995 （携帯・PHSからは06-6308-8981） |
| お電話受付時間 | 9:30～12:00/13:00～17:30（平日、祝祭日除く） |
| Email お問い合わせ | support@motex.co.jp |