2025.1.29

サイバーセキュリティ対策に関する経済産業省の施策及び警察庁からの協力要請について

デジタル化の進展により、サイバー空間が広がる一方で、ランサムウェア攻撃を含めたサイバー攻撃の数は年々増加し、更に高度化・巧妙化が進んでいます。このような中、政府全体としては、「能動的サイバー防御」の実現等、日本のサイバーセキュリティ対応能力向上に向けた法制度等に関する検討を加速させてきています。
経済産業省でも、産業界のサイバーセキュリティ対策を推進するため、各種施策を推進しているところ、これら取組の活用が進むよう、会員企業等への周知のご協力をお願いいたします。併せて、警察庁からも企業の皆様への協力要請がありましたので、以下について、周知のご協力をお願いいたします。

①経済産業省におけるサイバーセキュリティに関する各種施策について
経済産業省では、産業界をサイバー攻撃から守るために内閣サイバーセキュリティセンター（NISC）等の関係省庁や所管する独立行政法人情報処理推進機構（IPA）とも連携をしつつ、産業界のサイバーセキュリティ対策の強化を促すための各種施策に取り組んでいます。

主なものとしては、以下が挙げられます（施策の内容は別添 PDF をご覧ください。）。
・サイバーセキュリティ経営ガイドライン:
　社内でサイバーセキュリティ対策を推進するための経営者を対象としたガイドライン
・セキュリティサービス審査登録制度:
　一定の基準を満たす脆弱性診断等のセキュリティサービスのリストを公開
・JC-STAR（IoT 製品に対するセキュリティ適合性評価制度）:
　IoT 製品に対するセキュリティ適合性を評価し、適合基準を満たすものにラベルを付与
・サイバーインシデント発生時の相談窓口:
　インシデント発生時の対応や平時のセキュリティ対策について専門機関によるサポート体制を構築
＜以下、特に中小企業向け＞
・中小企業の情報セキュリティガイドライン:
　中小企業の経営者・実務担当者向けにセキュリティ対策の具体的な手順等を示したガイドライン
・SECURITY ACTION：
　全ての企業に必ず実施していただきたいセキュリティ対策をまとめたもの
・サイバーセキュリティお助け隊サービス：
　中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービス
　なお、列記されていない施策もありますので、ご関心のある方は、以下の経済産業省 HP よりご確認ください。
https://www.meti.go.jp/policy/netsecurity/index.html

②警察庁からの協力要請について
１　警察への連絡体制の整備について
ランサムウェア等のサイバー事案が発生した際に迅速かつ的確な対応がなされるよう、平時から警察への連絡体制を整備するなど必要な取組を推進していただくようお願いします。
＜対策例＞
・サイバー攻撃対応マニュアル等に警察の連絡先を記載する。
・サイバー攻撃を想定した事業継続計画（BCP）を策定し、初動対応における警察との連携について記載する。

２ 被害発生時における対応について

(1) 被害発生時における速やかな通報・相談

ランサムウェア等のサイバー事案の被害が発生した際は、初動対応における被害拡大防止・復旧に向けた助言や暗号化復号ツールの案内等の支援が可能ですので、速やかに最寄りの警察署又は都道府県警察のサイバー犯罪相談窓口に通報・相談くださるようお願いいたします。

＜参考：都道府県警察のサイバー犯罪相談窓口＞

https://www.npa.go.jp/bureau/cyber/soudan.html

(2) 初動対応における警察との連携

ランサムウェア等のサイバー事案発生時における初動対応におきまして、侵入経路や侵害範囲の特定のため、外部接続機器を中心としたログの保全に努めるようお願いいたします。

なお、都道府県警察が捜査を開始するに当たっては、まずは以下の事項を聴取することになります。

・被害端末に関する情報(データの暗号化の有無、具体的な症状等)
・ネットワークの構成（ネットワーク構成図）
・インターネットに接続可能な機器に関する情報(機器名、利用状況、パッチ適用の有無等)
・業務への影響、復旧方針 等

警察は、被害情報の保秘を徹底するとともに、被害組織の復旧作業や業務継続に配慮しながら捜査を進めますので、ご協力をよろしくお願いいたします。

お問合せ先：

①について
経済産業省　商務情報政策局サイバーセキュリティ課
TEL：03-3501-1511（内線 3964）
e-mail：bzl-cyber-madoguchi@meti.go.jp

②について
警察庁　サイバー警察局サイバー企画課
サイバー事案防止対策室　サイバー対策推進第一係
TEL：03-3581-0141（内線 3961、3452）

経済産業省　製造産業局

サイバーセキュリティ経営ガイドラインVer.3.0

- 経済産業省では、経営者にリーダーシップをとってサイバーセキュリティ対策を推進していただくため、**経営者を対象としたガイドライン**を策定しています。合わせて、ガイドライン**実践のためのプラクティス集**や、**セキュリティ対策の実施状況を可視化するツール**なども整備しています。

<サイバーセキュリティ経営ガイドライン（ポイント）>

1．経営者が認識すべき３原則

（1）経営者が、**リーダーシップを取って対策**を進めることが必要
（2）自社のみならず、**サプライチェーン全体にわたる対策**への目配り
（3）平時及び緊急時のいずれにおいても、**社内外関係者との積極的なコミュニケーション**が必要

2．経営者がCISO等に指示すべき１０の重要事項

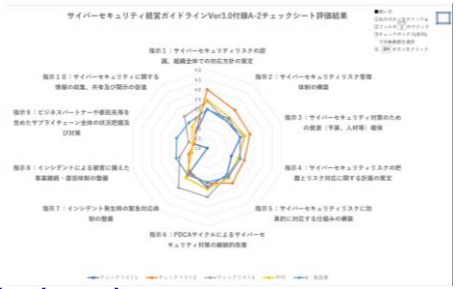
リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	**指示10** 情報収集、共有及び開示の促進

<サイバーセキュリティ経営ガイドラインVer3.0 実践のためのプラクティス集>

- **経営者**に加え、**CISO**、**セキュリティ担当者**を主な読者と想定し、実践事例に加え、セキュリティ担当者の**日常業務における悩みに対する具体的対応策を提示。**

<サイバーセキュリティ経営可視化ツール>

- 「サイバーセキュリティ経営ガイドライン」で定める重要10項目の実施状況を5段階の成熟モデルで可視化（レーダーチャート表示）

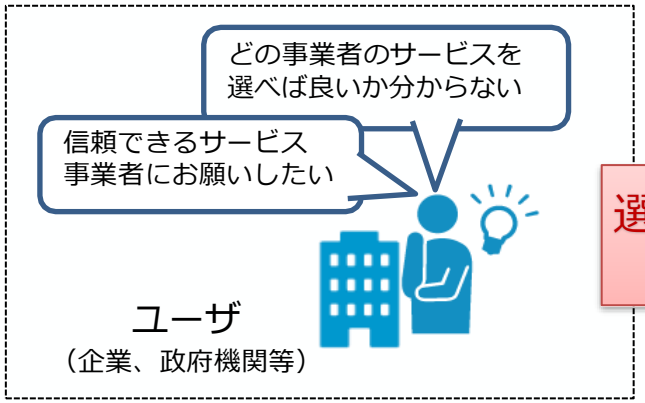


サイバーセキュリティ経営ガイドラインと支援ツール：https://www.meti.go.jp/policy/netsecurity/mng_guide.html

情報セキュリティサービス基準適合サービスリスト

- 経済産業省では、**「情報セキュリティサービス基準」を策定**し、審査登録機関による**審査をクリアしたサービスのリストを公開**※しています。※IPA（独立行政法人情報処理推進機構）が公開。
- 脆弱性診断やセキュリティ監査などのサービス（全5種、オプション1種）が対象になっており、これらのサービスを利用する際のサービス提供事業者の選定に本リストを活用いただけます。

＜情報セキュリティサービスにおける課題＞



選定時に活用

○情報セキュリティサービス基準適合サービスリスト（IPA）

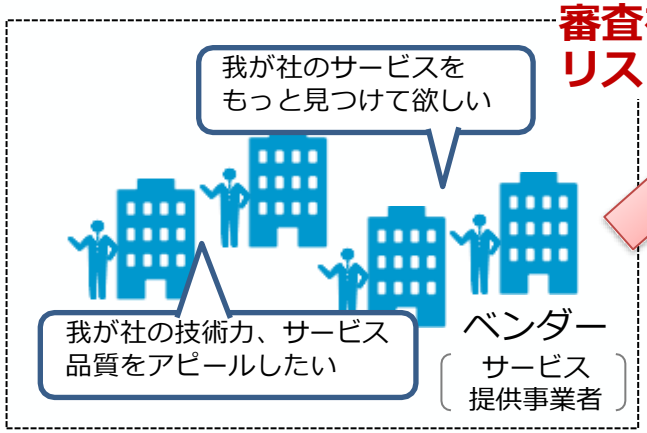
審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

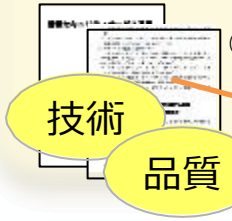
基準を満たした339サービスを掲載

- 情報セキュリティ監査（72サービス）
- 脆弱性診断（159サービス）
  うちペネトレーションテスト(侵入試験)あり(12サービス)
- デジタルフォレンジック（39サービス）
- セキュリティ監視・運用（52サービス）
- 機器検証 （17サービス）

2024年12月現在

審査を受けてリストに掲載





○情報セキュリティサービス基準（METI）

上記5サービス、1オプションに関して技術要件・品質管理要件を 定めた基準

本制度を通じて目指す社会

- **専門的知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる**
- **技術と品質を備えた情報セキュリティサービスの普及・発展**
- **制度の普及・浸透**

情報セキュリティサービス基準適合 サービスリスト：https://www.ipa.go.jp/security/service_list.html

IoT製品に対するセキュリティ適合性評価制度

- 経済産業省及びIPAでは、**IoT製品に対するセキュリティ適合性を評価**し、適合基準を満たすものについて、**ラベルを付与**する制度を、2025年3月※から**「JC-STAR（ジェーシースター）」**という制度名で開始します。　※2025年3月時点では最低限の適合基準（★１）についてのみ運用開始予定。
- 近年、IoT製品を狙ったサイバー攻撃が増加しているため、IoT製品の調達・購入・利用時には、本制度によるラベル取得の有無を確認し、セキュリティ要件を満たした安全なIoT製品を選びましょう。

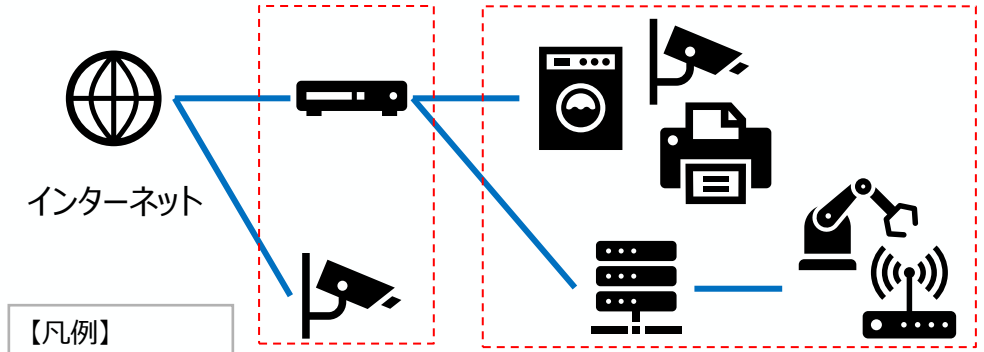
制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

JC-STAR

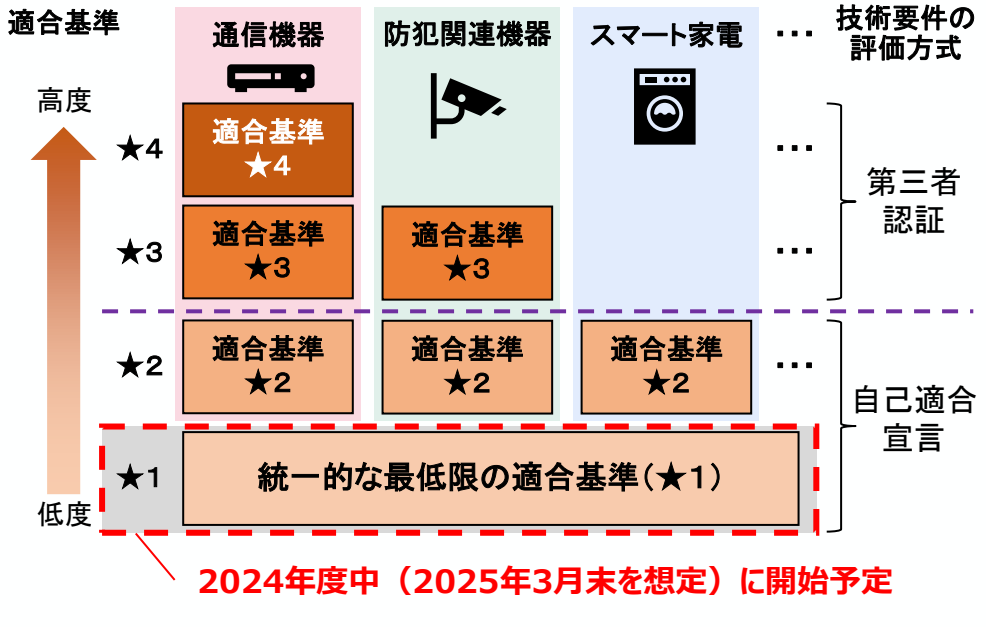
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



セキュリティ要件適合評価及びラベリング制度（JC-STAR）：https://www.ipa.go.jp/security/jc-star/index.html

サイバーセキュリティインシデント発生時の相談窓口

- サイバー攻撃又はその疑いにより、情報漏えい、ウイルス感染、システム停止などの**インシデントが発生した場合**、迅速な対応が必要です。
- 金銭被害、信用低下、事業停止等や関係者（顧客、取引先、従業員等）への**被害拡大を最小限に抑えられるよう**、警察への相談に加え、初動対応を支援する以下の**専門機関の活用**を検討ください。

独立行政法人情報処理推進機構（IPA）

- 不正アクセス等のインシデントに関する相談や届出、情報提供の受付：
  https://www.ipa.go.jp/security/todokede/incidentportal.html

（相談例）
- ランサムウェアに感染したため、対処方法について相談したい
- 普段の情報セキュリティの対策やIPAのセキュリティ施策について知りたい
- サイバー攻撃被害について、サイバー保険の適用を受けるために公的機関への届出を行いたい

一般社団法人JPCERTコーディネーションセンター

- インシデント初動対応（必要な調査、対応方針の検討、被害箇所の特定等）のサポートなどの依頼相談：

  https://www.jpcert.or.jp/form/

- インシデント対応に関する様々な相談、情報提供の受付：

  https://www.jpcert.or.jp/ir/consult.html

中小企業の情報セキュリティ対策ガイドライン第3.1版

- 経済産業省及びIPAでは、中小企業におけるセキュリティ対策を促進するため、**具体的な対策を示すガイドライン**を策定しています。**経営者編**と**実践編**から構成されており、個人事業主や小規模事業者を含む中小企業による活用を想定しています。
- ガイドラインの付録を活用した**「SECURITY ACTION」**は、**全ての企業に必ず実施していただきたいセキュリティ対策をまとめたもの**です。「SECURITY ACTION」を自己宣言することが、各種補助金の要件にもなっています。

＜中小企業の情報セキュリティガイドライン（ポイント）＞

- 中小企業の経営者や実務担当者が、情報セキュリティ**対策の必要性**を理解し、**情報を安全に管理**するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
  - 経営者が認識すべき**「3原則」**、経営者がやらなければならない**「重要7項目の取組」**を記載
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等の**ひな形**を付録
  - **「中小企業のためのセキュリティインシデント対応の手引き」**を追加

中小企業の情報セキュリティ対策ガイドライン：
https://www.ipa.go.jp/security/guide/sme/about.html

＜SECURITY ACTION＞

★一つ星

情報セキュリティ５か条に取り組む

【情報セキュリテイ５か条】

- OSやソフトウェアは常に最新の状態にしよう！
- ウイルス対策ソフトを導入しよう！
- パスワードを強化しよう！
- 共有設定を見直そう！
- 脅威や攻撃の手口を知ろう！

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

【基本方針の記載項目例】

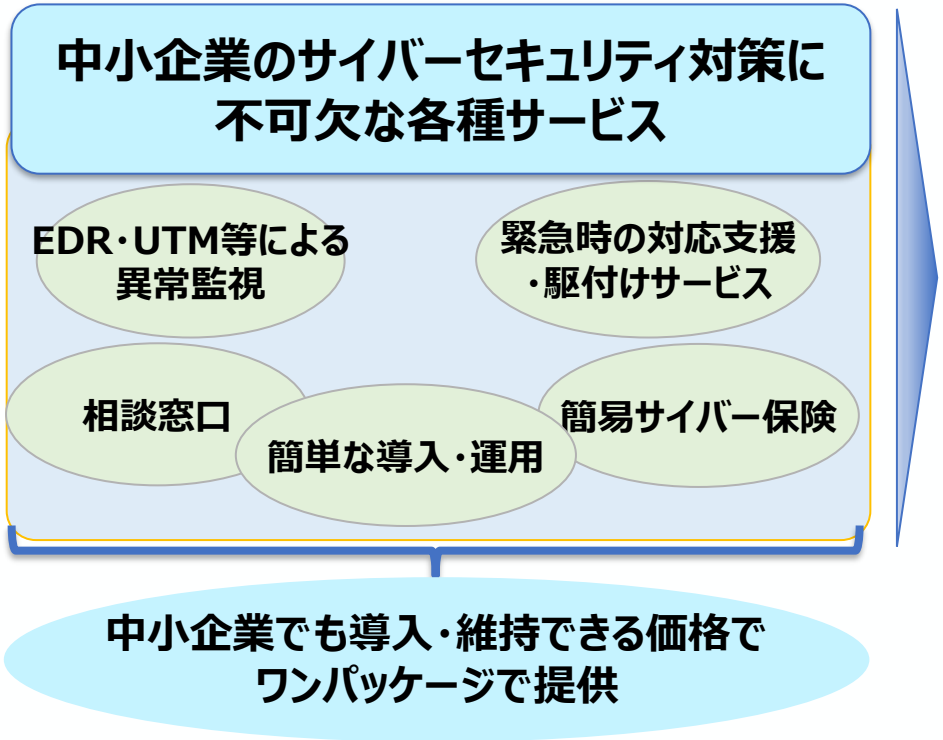
- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

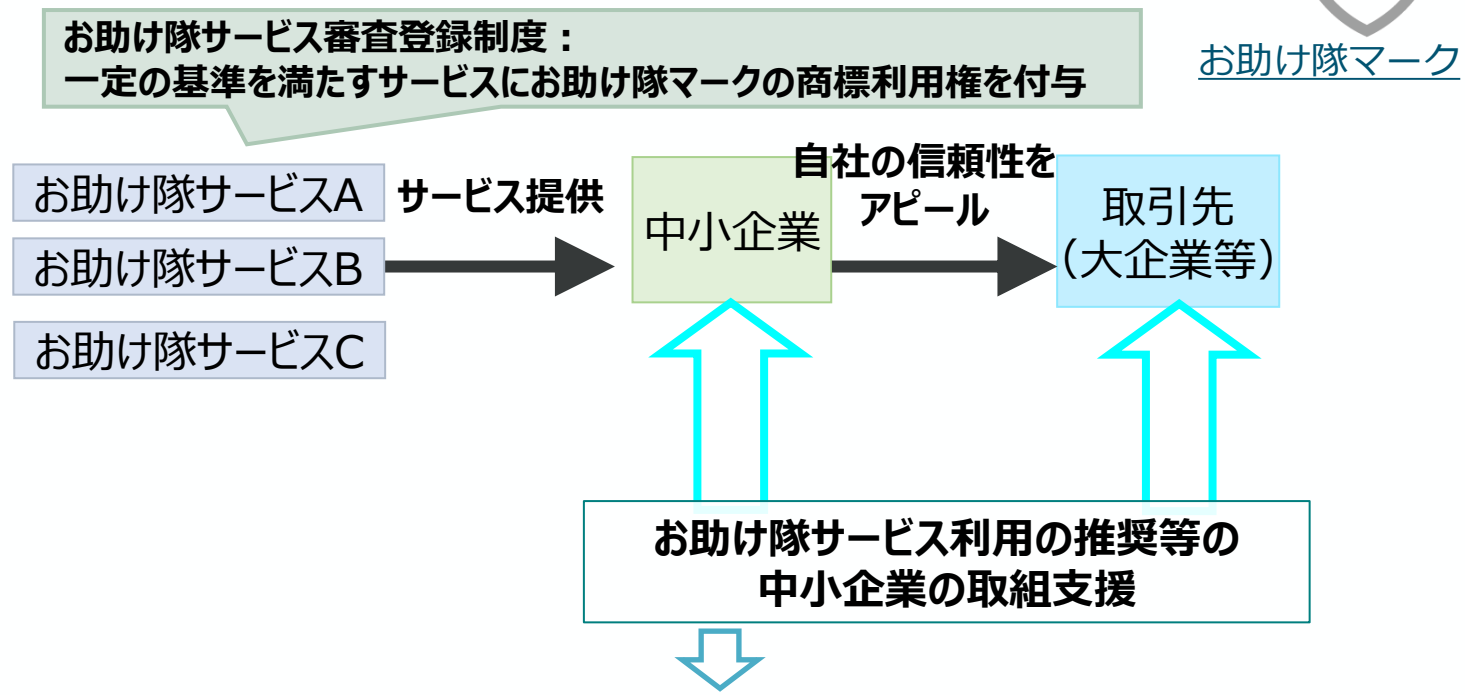
SECURITY ACTIONサイト：https://www.ipa.go.jp/security/security-action/

サイバーセキュリティお助け隊サービス

中小企業向け

- サイバーセキュリティお助け隊サービスは、**中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービスです。**IT導入補助金「セキュリティ対策推進枠」を活用することで、**費用の1/2（小規模事業者は2/3）の補助を受けられます。**





サイバーセキュリティお助け隊マーク

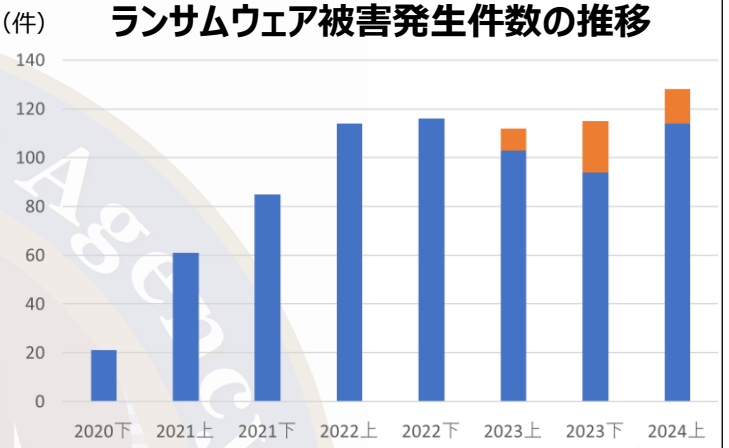
サイバーセキュリティお助け隊サービスの利用はこちらから
⇒ https://www.ipa.go.jp/security/otasuketai-pr/

サイバー事案発生に備えた警察への連絡体制の整備等について

○依然として、**サイバー空間をめぐる情勢は極めて深刻**であり、**ランサムウェア攻撃による被害件数は高水準で継続中。**
長期間のサービス停止や大規模情報流出により、**企業経営や市民生活に大きな影響を及ぼす被害が続発。**

○被害企業においては**コンプライアンス遵守の観点からも必要な関係機関への通報が求められる**ところ、レピュテーションリスク等の懸念による**「被害の潜在化」が課題**。

○**警察では、被害拡大防止・早期復旧のための初動対応支援**や**暗号化復号ツールの案内**等を行っている。



警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」より

警察庁からのお願い

①　警察への連絡体制の整備について

サイバー事案が発生した際に迅速に対応できるよう、警察への連絡体制の整備をお願いします。

＜対策例＞
・サイバー攻撃対応マニュアル等に警察の連絡先を記載する。
・サイバー攻撃を想定した事業継続計画(BCP)を策定し、初動対応における警察との連携を記載する。

よくある質問①

・関係機関との情報共有（相談）や公表の考え方は何を参考にすればよい？

⇒ **「サイバー攻撃被害に係る情報の共有・公表ガイダンス※」を参考にして下さい。**
情報共有、被害公表、外部組織との連携、機微な情報への配慮等の内容がまとめられています。

※本文 https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf
概要 https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_gaiyou.pdf

サイバー事案発生に備えた警察への連絡体制の整備等について

② 被害発生時における対応について

- **速やかな通報・相談**

  最寄りの警察署又は都道府県警察のサイバー犯罪相談窓口に通報・相談して下さい。

  ＜都道府県警察のサイバー犯罪相談窓口＞ https://www.npa.go.jp/bureau/cyber/soudan.html

- **初動対応における警察との連携**

  侵入経路や侵害範囲の特定のため、**外部接続機器を中心としたログの保全に努めてください。**
  また、必要に応じて以下の内容を伺いますので、情報提供に御協力をお願いします。

  ・被害端末に関する情報(データ暗号化の有無、具体的な症状等)
  ・ネットワークの構成（ネットワーク構成図等）
  ・インターネットに接続可能な機器に関する情報(機器名、利用状況、パッチ適用の有無等)　　等

よくある質問②

・通報したら被害を公表させられるのでは？　レピュテーションリスク（信用の毀損・風評被害）が心配！

⇒ **警察から被害の公表を求めることはありません。警察も保秘を徹底します。**
通報して必要な捜査を行うこと、つまり「社会的責任を果たすこと」が、顧客や取引先等に対する説明責任を負う上で重要な要素となります。

・少しでも早く通常業務に戻したい。通報すると、警察対応で時間をとられて復旧作業が遅れそう。
サーバや端末のデータを全て持って行かれるのでは？

⇒ **警察は、被害組織の復旧作業や業務継続に最大限配慮しながら捜査を進めます。**

・攻撃はあったが、被害が発生していない。捜査は望んでいない！

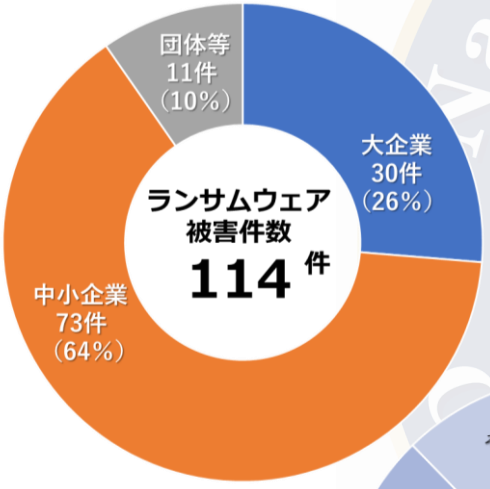
⇒ **「警察への相談 ＝ 捜査」ではありません。予兆や軽微な事案でも、ぜひ情報提供をお願いします。**

【参考１】ランサムウェアによる被害の発生状況

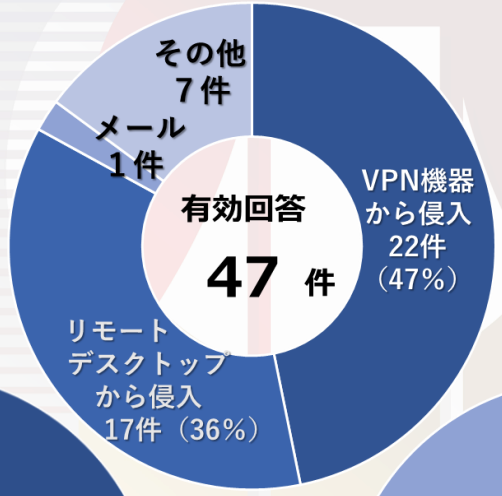
- 侵入経路は、VPN機器／リモートデスクトップからが8割強
- 被害組織の半数は、使用中のVPN機器等において最新のセキュリティパッチが未適用であった
- 約9割がウイルス対策ソフト・EDR等の対策を講じていたが、被害を受けている
  … 窃取した認証情報や機器のぜい弱性を悪用して侵入し、対策ソフト類を無効化する手法等による

VPN機器等のセキュリティパッチの速やかな適用によるぜい弱性対処、認証情報の厳正な管理を

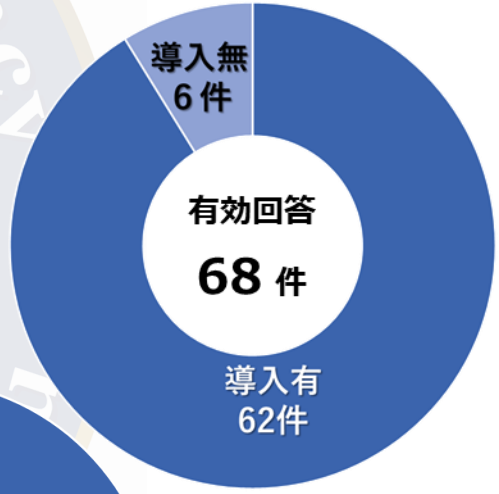
被害件数（規模別）



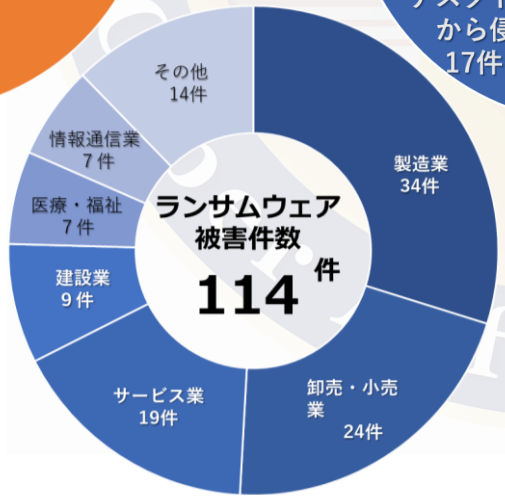
侵入経路



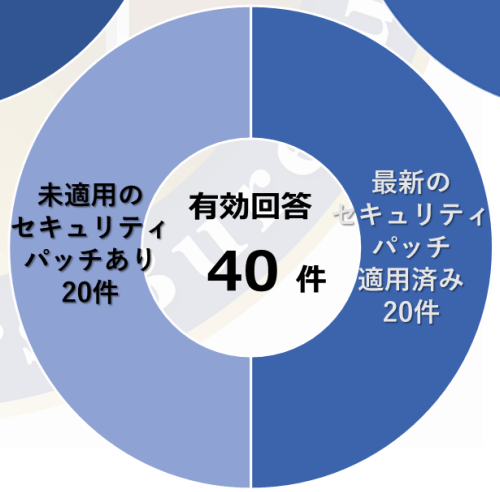
ウイルス対策ソフト等の導入状況



被害件数（業種別）



機器のパッチ適用状況



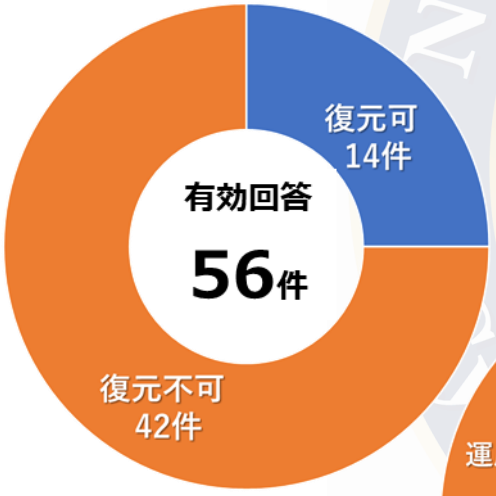
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」

【参考２】ランサムウェアによる被害の発生状況

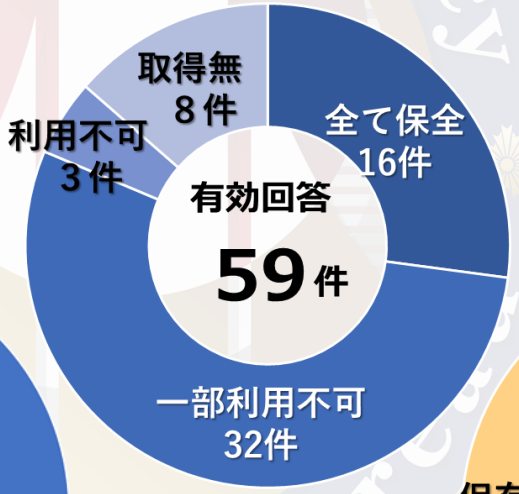
- **7割以上でバックアップからの復元に失敗**
  … オンライン接続されていることによりバックアップデータも暗号化された事例や、運用不備でバックアップを有効利用できない事例が多数。
- **侵入経路や情報窃取範囲の特定に不可欠なログも、ほとんどの場合で閲覧不可**
  … 犯人によって削除や暗号化されている事例が多数。

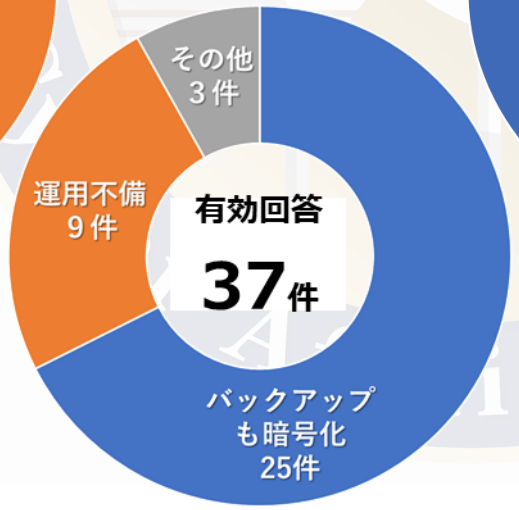
オフライン媒体を含む複数媒体への保存、運用体制の確認や訓練実施の検討を

バックアップからの復元可否

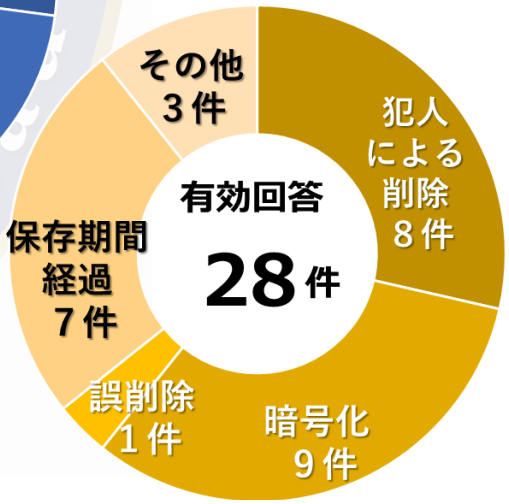


ログ保全状況





復元不可の理由



ログ閲覧不可の理由

出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」