中小企業向けセキュリティ対策支援制度の活用事例の紹介

２０２２年１０月１４日

独立行政法人情報処理推進機構（IPA）
セキュリティセンター 企画部 中小企業支援グループ
グループリーダー 江島 将和

目次

【政府発表】 3月1日経済産業省ニュースリリースより
同時発表：金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター（NISC）

サイバーセキュリティ対策の強化について（注意喚起）

- 昨今の情勢を踏まえると**サイバー攻撃事案の潜在的なリスクは高まっている。**
  （3月1日、国内の自動車部品メーカーから被害にあった旨の発表）
- 経営者のリーダーシップの下、中小企業、取引先等、**サプライチェーン全体で今一度、適切なセキュリティ対策を実施**するようにお願い（国外拠点も同様）。

＜行うべき対策の一例＞

1.リスク低減のための措置	➢ **パスワードが単純でないかの確認**、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、**本人認証を強化**する。 ➢ IoT 機器を含む**情報資産の保有状況を把握**する。特にVPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、**セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用**する。 ➢ メールの**添付ファイルを不用意に開かない、URL を不用意にクリックしない**、連絡・相談を迅速に行うこと等について、組織内に周知する。
2.インシデントの早期検知	➢ サーバ等における各種ログを確認する。 ➢ 通信の監視・分析やアクセスコントロールを再点検する。
3.インシデント発生時の適切な対処・回復	➢ データ消失等に備えて、**データのバックアップの実施及び復旧手順を確認**する。 ➢ インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

✓ 実際に情報流出等の被害が発生していなかったとしても、**不審な動きを検知した場合**は、早期対処のために**速やかに所管省庁、セキュリティ関係機関に対して連絡、警察にも相談を**。

3月24日の経済産業省によるニュースリリースでは、中小企業においては、自社がサイバー攻撃による被害を受けた場合、その影響が自社にとどまらず、サプライチェーン全体の事業活動に及ぶ可能性があることを踏まえ、**「サイバーセキュリティお助け隊サービス」**の活用など、積極的なサイバーセキュリティ対策に取り組むことを推奨。

中小企業を巡るサイバーセキュリティの状況

サイバーセキュリティお助け隊実証事業（2019年度）の対応事例

- 実証期間中に、重大なインシデントの懸念・可能性ありと判断し、**対処・支援を行った件数は128件**。対処を怠った場合の**被害想定額が5000万円**近くなる事案も。
- 実証参加前後の中小企業の意識変化や、お助け隊サービスに求められる機能等が明らかになった。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用

・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。

・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。

・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。

・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。

・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ホテルWi-Fiの利用

・社員が**出張先ホテルのWi-Fi環境**でなりすましメールを受信し、添付されたマルウェアを実行したことで**Emotetに感染**。

・感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

・実証参加企業でマルウェア添付メールを集中検知。

・**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。

・メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

経済産業省　昨今の産業を巡るサイバーセキュリティ
https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

中小企業を巡るサイバーセキュリティの状況

サイバーセキュリティお助け隊実証事業（2020年度）の対応事例

- **1,117社**が参加した2020年度実証事業でも、**中小企業において業種や規模を問わず例外なく　サイバー攻撃を受けている状況**を確認するとともに、**検知・防御のための対策の必要性**を確認。

＜2020年度実証事業における具体的な対応事例＞

事例１	UTMサービスを導入した企業において、同一ホストにて断続的に**要注意検知が発生していることが確認**されたため、お助け隊事業者が駆けつけ支援を実施。 対象の**マルウェアと判定されたプログラム**は、インターネットからダウンロードしたフリーソフトであったことが判明、**駆除を実施**した。
事例２	UTMサービスを導入した企業において、PCの「ウィルス対策ソフト」を導入済みであったものの、**「不正なIPアドレスへの通信」が成立していることが確認**されたため、緊急度「高」のアラートを発報、支援を実施。 接続元端末をLANから分離した上、**ウイルス対策ソフトでのフルスキャンを実施した結果、何も検知されなかった**ものの、もし被害に至っていた場合の**被害試算額**は**54,760,000円**にも。
事例３	UTMサービスを導入した企業において、**マルウェアへの感染の疑いがある通信をUTMで検知**、リモート支援により駆除を実施。 該当端末(PC)をLANから分離した上でフルスキャンを実施した結果、**Hacktool及びトロイの木馬、計6件のマルウェアを発見したため駆除を実施**した。

https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html

中小企業を巡るサイバーセキュリティの状況
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　概要

- **中小企業の情報セキュリティ対策への取り組みや被害の状況、対策実施における課題、経営層の関与や認識に関する実態を把握するため、アンケート調査を実施。**

【アンケート調査実施概要】

調査手法	ウェブによるアンケート調査
調査対象	全国の中小企業を対象とし、業種別、企業規模別、で中小企業基本法の定義に基づいて割付を行い、サンプルを回収。
調査項目	• 企業概要 • ITの導入状況 • 情報セキュリティに関する意識・状況 • 情報セキュリティ被害 • 取引先を含む情報セキュリティ対策
調査期間	2021年10月～2021年12月
有効回答数	4,074人 （内訳：経営層2,819人、ITや情報セキュリティの社内担当者561人、一般社員、役職無回答・不明：694人）

【アンケート送付数内訳】

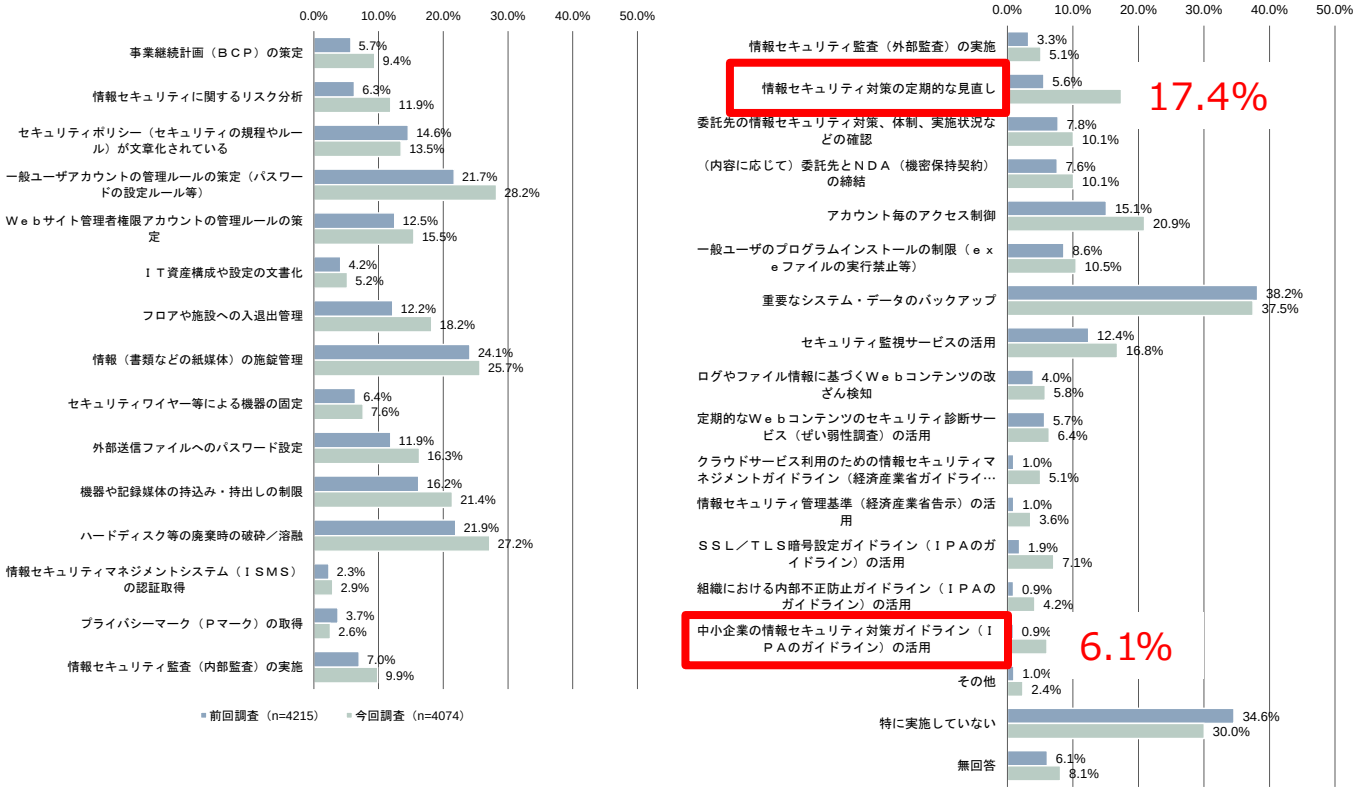
業種名	中小企業数	小規模企業数	業種別合計数
農業・林業・漁業	746	1,049	1,795
建設業	1,353	3,160	4,513
製造業、鉱業・採石業・砂利採取業、電気・ガス・熱供給・水道業	1,337	3,123	4,460
情報通信業	529	1,229	1,758
運輸業・郵便業	529	1,229	1,758
卸売業・小売業	2,530	6,074	8,604
金融業・保険業	528	1,231	1,759
不動産業・物品賃貸業	1,115	2,599	3,714
サービス業・その他	3,495	8,144	11,639
合計	12,162	27,838	40,000

中小企業を巡るサイバーセキュリティの状況

中小企業における実態調査（2021年度）の結果（１）

- **被害防止のための組織面・運用面の対策の実施状況**について、前回調査の結果と比較すると、大半の項目で対策実施の割合が増加（微増）。
- 特に、**「情報セキュリティ対策の定期的な見直し」**については**17.4%**と前回調査（5.6%）から10%以上増加するとともに、**「中小企業の情報セキュリティ対策ガイドライン（IPA）の活用」**も0.9%から**6.1%**に増加。

【被害防止のための組織面・運用面の対策（前回比較）】



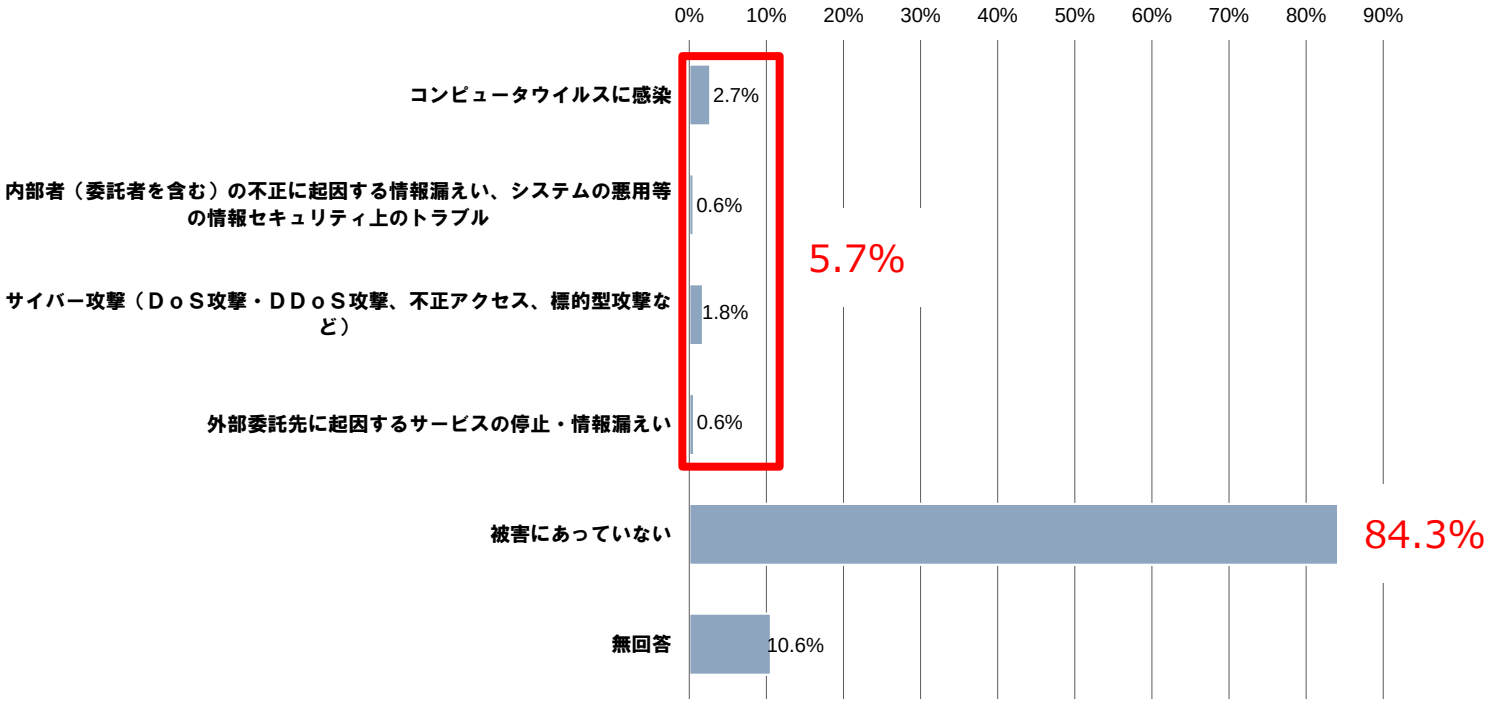
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

中小企業を巡るサイバーセキュリティの状況

中小企業における実態調査（2021年度）の結果（２）

- 2020年度の1年間に情報セキュリティ被害にあったか否かを聞いた設問では、**84.3%が「被害にあっていない」と回答**。何らかの被害にあったとする企業は5.7%で、最も多い回答は「コンピュータウイルスに感染(2.7%)」。
- ただし、前述のお助け隊実証事業等の結果も踏まえれば、**回答企業においてサイバー攻撃を認識できていない可能性も否定できない**。

【2020年度における情報セキュリティ被害の有無】



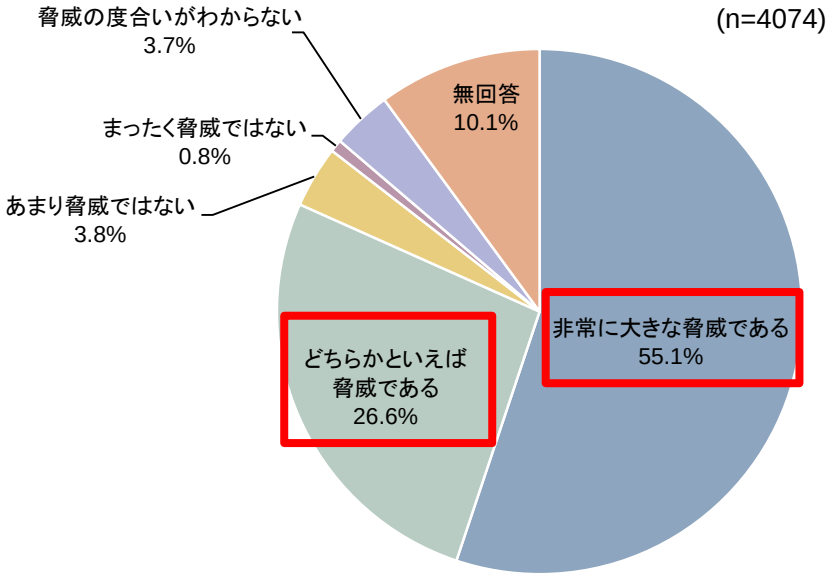
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

中小企業を巡るサイバーセキュリティの状況

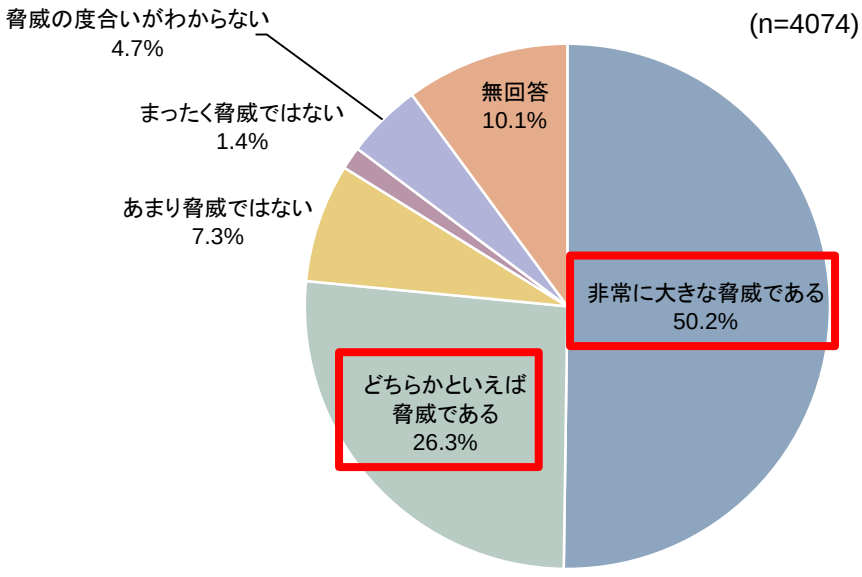
中小企業における実態調査（2021年度）の結果（３）

- **コンピュータウイルス**について、**「非常に大きな脅威である」の割合が最も高く55.1%**となっている。次いで**「どちらかといえば脅威である（26.6%）」**となっている。
  不正アクセスについても**「非常に大きな脅威である」**と**「どちらかといえば脅威である」**を合わせると**7割**を超えており、**これら情報セキュリティに関する脅威について、中小企業においても「脅威」としては広く認知されている**といえる。

【情報セキュリティに関する脅威（コンピュータウイルス）】



【情報セキュリティに関する脅威（不正アクセス）】



https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

中小企業を巡るサイバーセキュリティの状況

中小企業における実態調査（2021年度）の被害事例

事例	業種	所在地	従業員規模
ランサムウエアに感染し、サーバ上のファイルが暗号化されてしまい、その解除と引き換えに金銭の要求を受けた。この対応のために、**相当の時間と費用を費やしている**。そこで、IPAが提供する資料を参考に**社内規定を整備**し、従業員に対して**リテラシー向上のための周知を継続的**に行った。また、管理者権限を持つアカウントを限定することで、**ソフトウエアのインストールを制限**するなどの対策を行った。	建設業	石川県	101～300名
利用する外部の**ホームページ作成・管理サービスへの不正アクセス**を受けた。トップページの動作や画面表示がおかしいことで気付いて調査すると、外部サービスの**安易なパスワード設定を破られて不正ログイン**されてしまい、不明なファイルが設置されていた。そこで、**ID・パスワードを強固なものに変更**し、**IPアドレス制御**を行い社外からのアクセスを制限した。また、不明なファイルを削除した。加えて、**関連会社も同じパスワードを使い回し**ていたので別のものに変更したり、**外部サービスのアップデートのルール**も定めたりと、対策を根本的に見直した。	サービス業	兵庫県	6～20名
元従業員による機密情報の持ち出しが疑われる事案を経験した。元従業員は退職前に大量のファイルをダウンロードしていたが、端末上の証跡を消去しており、外部専門家が調査しても確定的な証拠を得ることができず、被害届を提出することができなかった。そこで、**機密情報の取り扱いに関する社内規定を整備**するとともに、**従業員向けの研修**を実施し、会社の情報資産に関する共通認識を持つように努めた。また、**情報資産管理やログ（記録）管理**、**デバイス管理**を行うシステムを導入して再発防止に取り組んだ。	卸売業	東京都	6～20名

情報セキュリティ対策はなぜ必要？

- IT活用がビジネスに利益をもたらす一方で、サイバー攻撃や従業員の不注意などによる損害が多発
- 大企業だけではなく、**中小企業もサイバー攻撃のターゲットになっている**
- 取引先攻撃への踏み台にされる懸念
- 近年増加しているサイバー攻撃は金銭窃取などを目的としていることが多く日々巧妙化、複雑化、悪質化
- 組織の損害を未然に防ぐために、今や**情報セキュリティ対策は必須**

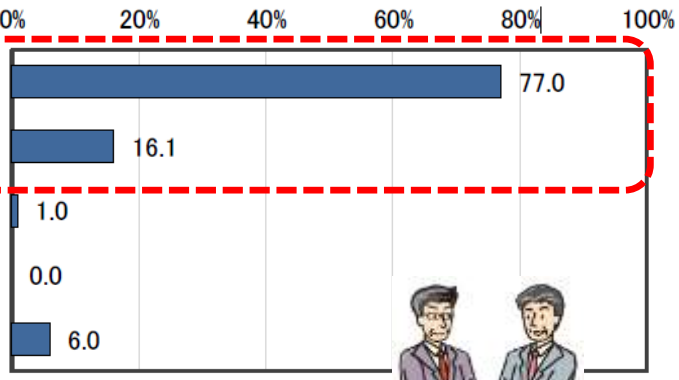
顧客や取引先はどう考えているか？

- デジタル化が進む今の社会、顧客や取引先の情報セキュリティに対する要求、期待は確実に高まっている。

IPA「ITサプライチェーン における情報セキュリティの責任範囲に関する調査」から
＜以下の情報セキュリティ要求事項に関し、業務委託契約において、**委託先の責任を明確にしたいと思う度合**について、当てはまるものをお選びください。(それぞれひとつずつ)＞

a.秘密保持

選択肢	%	N
1　強くそう思う	77.0	321
2　ややそう思う	16.1	67
3　あまりそう思わない	1.0	4
4　全くそう思わない	0.0	0
5　分からない・無回答	6.0	25
計	100	417



責任や義務はあるのか？

- 個人情報保護法では委託先の監督が求められている。
- 顧客や取引先から見て自社が委託先に該当する場合は、「監督」される立場にある。

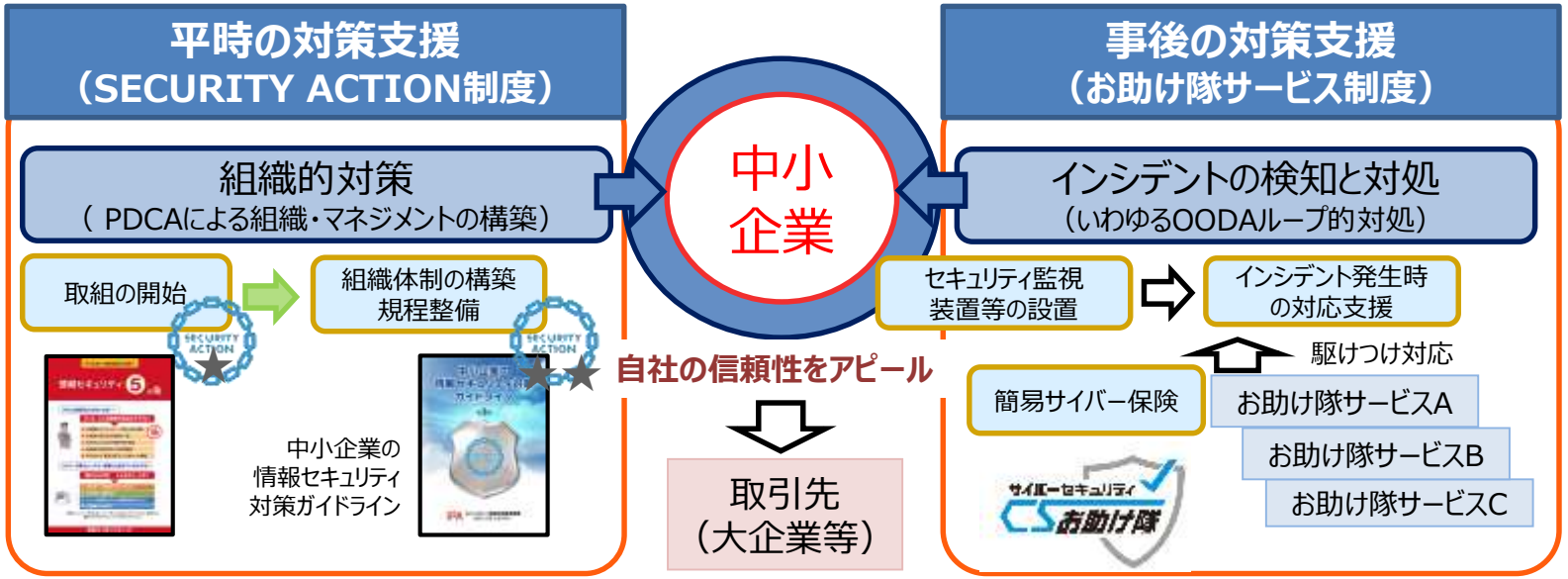
「個人情報保護法」
(委託先の監督)
第22条 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、**委託を受けた者に対する必要かつ適切な監督を行わなければならない。**

「個人情報の保護に関する法律についてのガイドライン(通則編)」
次の(1)から(3)までに掲げる必要かつ適切な措置を講じなければならない
(1)適切な委託先の選定
(2)委託契約の締結
(3)委託先における個人データ取扱状況の把握

中小企業向けサイバーセキュリティ対策支援

- **中小企業**が業種や規模を問わず例外なく**サイバー攻撃の脅威**にさらされている中、**不審なアクセスを検知・防御するための対策**が必要となっている。一方、多数のセキュリティ脅威の中「攻撃の糸口」は似通っており、**基本的な対策の重要性**は長年変わらないことから、「**情報セキュリティ対策の基本**」は常に意識し、**組織として一丸となって対策**をしていく必要がある。
- そこでIPAでは、事後の対策支援として『**サイバーセキュリティお助け隊サービス制度**』、平時の対策支援として『**SECURITY ACTION制度**』の活用を推奨している。

中小企業向けサイバーセキュリティ対策促進事業



目次

SECURITY ACTION 制度

SECURITY ACTION 制度概要

https://www.ipa.go.jp/security/security-action/

- **中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度※**
  - 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに２段階の取組み目標を用意

１段階目（一つ星）

「情報セキュリティ5か条」に取組むことを宣言

２段階目（二つ星）

「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言

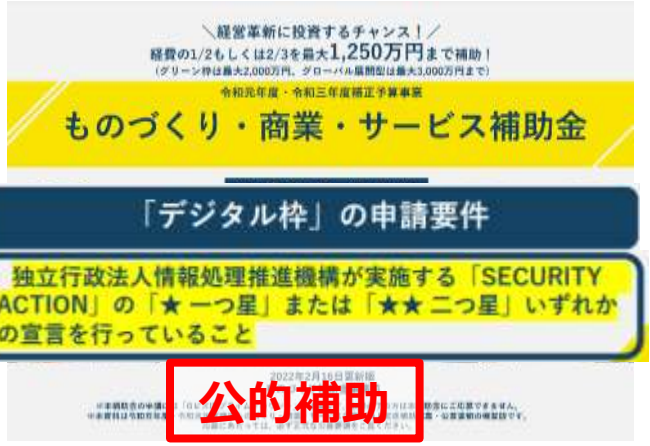
※SECURITY ACTION制度は、中小企業等自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。
各企業等の情報セキュリティ対策状況等をIPAが認定する、あるいは認証等を付与する制度ではありません。

SECURITY ACTION制度のメリット

- **情報セキュリティ対策への取組みの見える化**
  - ☞ ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに 印刷することで自らの取組み姿勢をアピール
- **顧客や取引先との信頼関係の構築**
  - ☞ 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに
- **公的補助・民間の支援を受けやすく**
  - ☞ SECURITY ACTIONを要件とする補助金の申請、普及賛同企業から提供される様々な支援策が利用可能

見える化

信頼関係

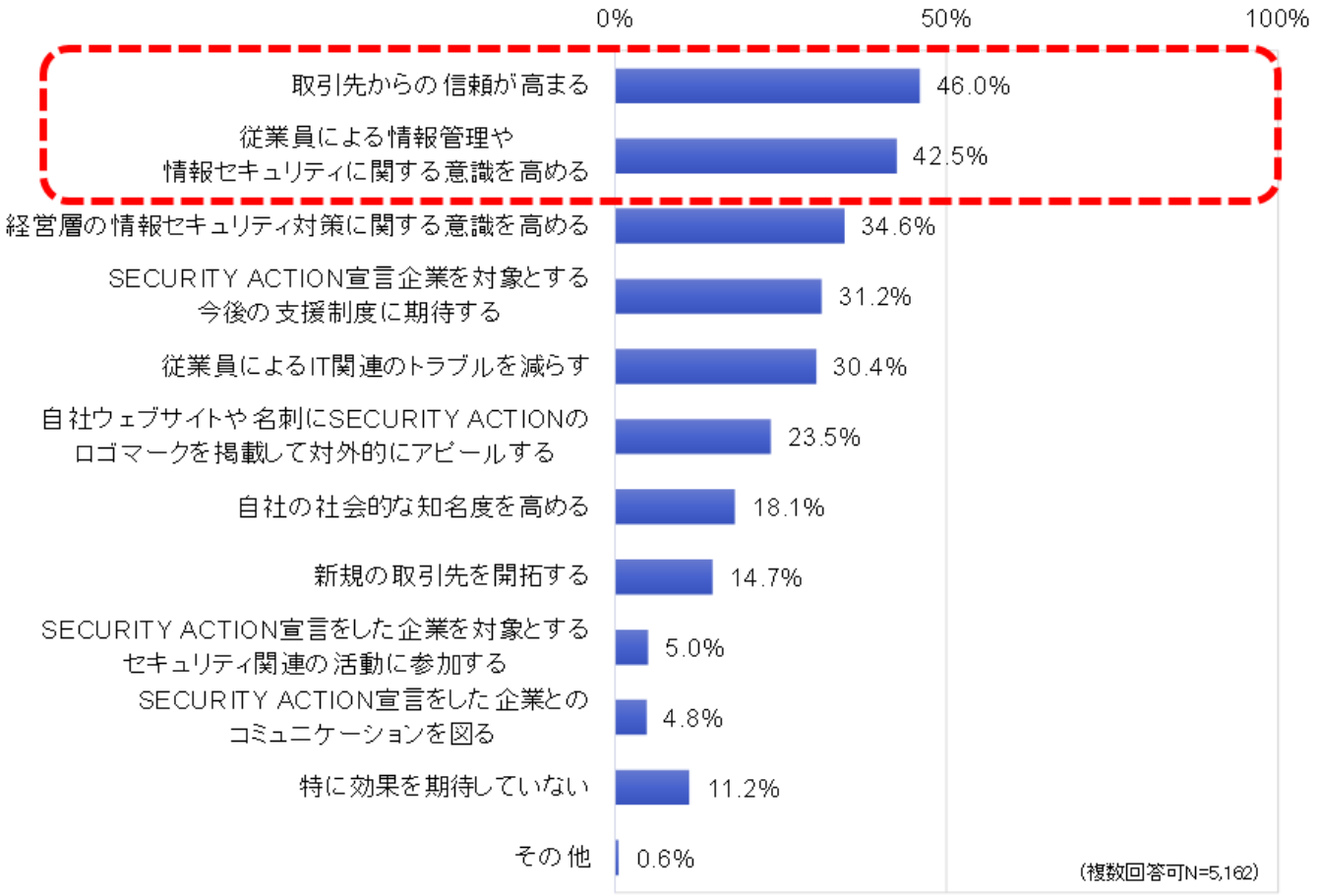


公的補助

SECURITY ACTION宣言で期待した効果

SECURITY ACTION宣言事業者における情報セキュリティ対策の実態調査

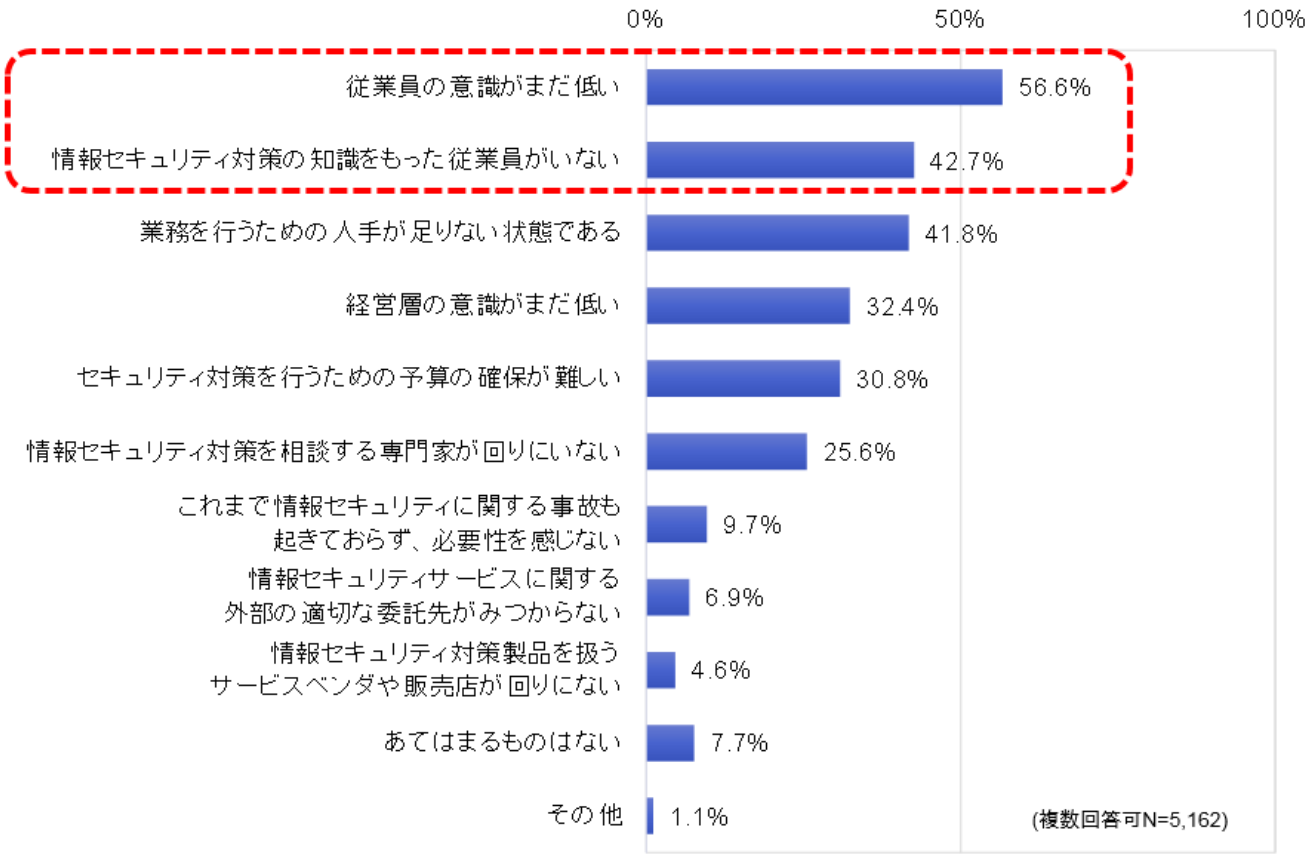
- 「**取引先からの信頼が高まる**」が46.0%と最も高く、「**従業員による情報管理や情報セキュリティに関する意識を高める**」も42.5%となってる。



情報セキュリティ対策を進める上での課題点

SECURITY ACTION宣言事業者における情報セキュリティ対策の実態調査

- **「従業員の意識がまだ低い」**が56.6%と最も高く、**「情報セキュリティ対策の知識をもった従業員がいない」**が42.7%、**「業務を行うための人手が足りない状態である」**が41.8%となっている。



SECURITY ACTION

自治体等における活用事例

- デジタル化やサイバーセキュリティ対策などを支援するIT導入の補助金申請の要件にするなど、各種補助金・助成金制度において**SECURITY ACTION制度を活用**。
- 引き続き各地方自治体や団体組織等とも連携の上、取組み拡大予定。

【本年度における自治体等におけるSA制度の活用事例】

- **IT導入補助金**【継続】（通常枠に加えてデジタル枠・セキュリティ枠が追加）
  ：中小企業庁
- **ものづくり補助金（デジタル枠）**【新規】
  ：中小企業庁
- **事業承継・引継ぎ補助金（経営革新）**【新規】
  ：中小企業庁
- **地域医療介護総合確保基金を利用したICT導入支援事業**【新規】
  ：厚生労働省（実施主体は各都道府県）

- **令和4年度 デジタル化トライアル事業費補助金**【活用継続】
  ：秋田県
- **令和4年度 サイバーセキュリティ対策促進助成金**【継続】
- **「情報セキュリティ基本方針 策定支援専門家派遣」事業**【継続】
  ：東京都中小企業振興公社
- **令和4年度 中小企業等スマートワーク促進補助金（情報セキュリティ事業）**【新規】
  ：岐阜県
- **令和4年度 堺市中小企業デジタル化促進補助金**【活用継続】
  ：大阪府堺市

目次

中小企業の情報セキュリティ対策ガイドライン

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/keihatsu/sme/guideline/

- 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（第1部経営者編）
  - 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（第2部実践編）
  - 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

ガイドラインの構成

- 中小企業の情報セキュリティ対策の考え方や実践方法について、本編２部と付録より構成

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	付録６　中小企業のためのクラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。

ガイドラインの対象

- 対象組織
  - 全ての業種の中小企業および小規模事業者
    （法人、個人事業主、各種団体も含む）
- 想定読者
  - 経営者と情報セキュリティ対策を実践する責任者・担当者

経営者

責任者・担当者

中小企業の情報セキュリティ対策ガイドライン
ガイドラインの活用事例
(中小企業の情報セキュリティマネジメント指導業務（2020年度）)

IPA

● マネジメント指導先企業アンケートから、中小企業等に参考となる取組みを抽出、当該指導先企業（8社）に対するヒアリング調査を行い、「セキュリティマネジメント指導事例集」を作成した。

指導先企業ヒアリング調査の概要（抜粋）

※詳細は「【別紙2】セキュリティマネジメント指導事例集」を参照

（新潟県）卸売・小売業	（東京都）社会保険事務	（広島県）製造業	（大分県）技術サービス業
－小売・卸売業のECとDX推進に伴うセキュリティ対策の強化－	**－業務のIT化に伴う個人情報管理の改善－**	**－サプライチェーン上の必須要件となる情報セキュリティ対策－**	**－情報セキュリティの実装には対外的宣言が重要－**
●オンラインストアの構築や受発注業務の電子化等、**経営者としてDXを強力に進めてきた**が、情報セキュリティ対策が十分かどうか不安があった。 ●指導を受けて、**問題の可視化と整理が非常に役立った**。策定したルールの遵守について、実行施策を担うIT・セキュリティ担当者を配置することにした。 ●指導専門家の方は、今後もITの活用や情報セキュリティに関して**継続した支援を依頼**した。	●個人情報を預かっているが、事務所として**IT化が進み、クラウドサービス活用やテレワーク**をする中、現状のままで本当に大丈夫なのか、第三者に確認してもらいたかった。。 ●クラウドサービスを**同じアカウントで共有利用**していたため、**運用ルールを改善**した。 ●顧客企業のテレワークに係る就業規則の改訂相談に、同じ士業として**登録セキスペ(RISS)を紹介する機会**もある。	●取引先の大手自動車メーカーから、定期的にどのようなセキュリティ対策を行っているか問合せを受けており、**信頼を得るため対策強化が必要**だった。 ●**現場目線で取組めるセキュリティ対策**の検討を進め、改善項目は**優先順位**が分かるように実行計画を作成した。 ●社内体制と現場対策の両面の課題が明らかになり、**トップとボトムの両輪で対策を本格的に推進する風土**ができた。	●セキュリティに関する会社としてのポリシーや規程が整備できておらず、**対外的にポリシーを示すことが、取引先への信用上必要**と感じていた。 ●本事業の指導カリキュラムによって、**基本ポリシー、関連規程の整備**ができ、必要だったものが全て揃えることができた。 ●外部の専門家の目で課題を見える化して経営者に示したことで、**経営者の情報セキュリティに対する理解が深まった**。

https://www.ipa.go.jp/security/fy2020/reports/sme/management.html

目次

サイバーセキュリティお助け隊サービス

サイバーセキュリティお助け隊サービス
【参考】お助け隊サービス登録サービスリスト

■ 各地域の中小企業に選択・利用可能な**「サイバーセキュリティお助け隊サービス」登録サービスリスト。**これまでに**18のサービス**が登録、今後も拡充予定。

【サイバーセキュリティお助け隊サービス　登録サービスリスト】

※2022年9月時点

	サービス名	事業者名	対象地域
1	商工会議所サイバーセキュリティお助け隊サービス	大阪商工会議所	全国（離島など一部地域を除く）
2	防検サイバー	ＭＳ＆ＡＤインターリスク総研株式会社	全国
3	PCセキュリティみまもりパック	株式会社ＰＦＵ	全国
4	EDR運用監視サービス「ミハルとマモル」	株式会社デジタルハーツ	全国
5	SOMPO SHERIFF（標準プラン）	ＳＯＭＰＯリスクマネジメント株式会社	全国
6	ランサムガード	株式会社アイティフォー	関東地方、中部地方、関西地方、九州地方、沖縄県
7	オフィスSOCおうちSOC	富士ソフト株式会社	東北地方（岩手）を中心　※全国展開を計画中
8	セキュリティ見守りサービス「＆セキュリティ＋」	株式会社BCC	全国
9	CBM ネットワーク監視サービス	中部事務機株式会社	岐阜県（飛騨地方除く）・愛知県（三河地方除く）
10	中部電力ミライズ　サイバー対策支援サービス	中部電力ミライズ株式会社	愛知県・岐阜県・三重県・長野県・静岡県（富士川以西） ※順次全国に拡大予定
11	ＣＳＰサイバーガード	セントラル警備保障株式会社	東京・神奈川・千葉・埼玉　※順次全国に拡大予定
12	PCお助けパック　PC定期侵害調査プラン	沖電グローバルシステムズ株式会社	沖縄県を中心　※全国展開を計画中
13	ネットワークセキュリティ見守り隊＆PCセキュリティ見守り隊サービス	株式会社コハマ	静岡県
14	マイセキュア　ビジネス	ＮＴＴコミュニケーションズ株式会社	全国
15	セキュアエッジＭＤＲ９９	セキュアエッジ株式会社	全国
16	Cloud Edge運用支援 EasySOC Plus　パック	株式会社大塚商会	北海道地方、東北地方、関東地方、中部地方、関西地方、中国地方、九州地方（一部地域を除く）※順次全国に拡大予定
17	アクロネットサイバーセキュリティサービス	株式会社アクロネット	全国（離島など一部地域を除く）
18	ビジネスサポートサービス	コスモテレコム株式会社	山形県

サイバーセキュリティお助け隊サービス

中小企業ユーザーの主な声

＜サイバーセキュリティお助け隊サービスについて中小企業から寄せられた声＞

●自社の対策が不十分であることにより、**取引先に迷惑をおかけするわけにはいかない**ため、サイバーセキュリティお助け隊サービスの導入を決めた。

●検知・監視してくれるだけでなく**何かあった時の事後対応まで含まれる**ところがよい。セキュリティについて全く分からないので、**まとめてお任せできるところにお願いしたい**と考えていた。

●アラート通知が来るので、**防御できていることが実感でき安心**。
本社のほか複数の拠点でも利用しているが**サービス利用料が安いので助かって**いる。

●**何も無いということがわかる**ことも良い点。**セキュリティレポートをストックしておくことで、報告資料としても使える**ので助かっている。

※サイバーセキュリティお助け隊サービス提供事業者　提供情報より

目次

（参考）東京都産業労働局
中小企業サイバーセキュリティ対策強化緊急サポート事業

- 東京都にて、中小企業を対象に**EDR環境を導入**し、**サイバー攻撃の実態把握**や**インシデントへの対応支援**を行う事業を実施中。
- IPAのお助け隊サービスに登録されている「株式会社アイティフォー」社が運営を行っております。是非ご活用ください。

【募集概要】

申込み期間	2022年8月12日 ～ 2022年10月頃
参加対象企業	東京都内に主な事業所を有する、 自社サイバーセキュリティ対策の取り組みに意欲を持つ中小企業
募集社数	100社程度（1社あたり300台まで）　※先着順
EDR導入期間	3ヵ月程度
参加費用	無料
案内サイト	https://security-kyoka.metro.tokyo.lg.jp/
主催	東京都