中小企業・小規模事業者の皆様へ

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

情報漏えい？ ウイルス感染？ システム停止？ どうしたらいいの！？

【イラスト挿入予定】

セキュリティインシデント対応の必要性

セキュリティインシデントとは、情報セキュリティの事故・事件のことです。単に「インシデント」とも呼ばれます。
重要な情報の漏えい、改ざんや破壊・消失、情報システムの機能停止または極端な性能の低下などがインシデントに該当します。
インシデント対応では、被害を想定し、あらかじめ準備することで被害や影響範囲を最小限に抑えます。また、自社だけではなく、顧客、取引先、株主、従業員などの関係者へ被害が拡大しないようにします。

インシデント発生時の想定被害

直接的な被害として、攻撃者による不正送金や金銭要求、対応人件費、原因調査や復旧のための外部委託費、復旧までの代替品費、取引先・顧客等への謝罪対応費、法的対応のための弁護士費用等の金銭的被害があります。
間接的な被害として、関係者への被害波及、会社の信用低下、事業停止による機会損失等があります。

インシデント対応の目的

被害とその影響範囲を最小限に抑え、再発を防止することです。

インシデント対応時に整理しておくべき事項

1	インシデントの分類	情報漏えい、ウィルス感染、システム停止など
2	事業者	事業者の名称 ※自社の受託案件に関連したインシデントの場合は委託元含む関係事業者の名称
3	責任者・担当者	本件に関する責任者および担当者の所属、氏名
4	発覚日時	インシデントを認知した日時
5	発生日時	インシデントの発生日時　※調査等で判明した場合
6	発生事象	表面化している事柄、被害、影響など
7	対応経過	発覚から現時点までの対応時系列経過
8	想定される原因	現時点で想定される直接的な原因
9	対象機器・ソフウェア・サービス	発覚時に利用していたり、直接の原因となった ・パソコン、サーバー、スマートフォンなどの機器 ・OS、アプリケーションなどのソフトウェア ・クラウドサービス、レンタルサーバーなどの他者が提供するサービス
10	セキュリティ対策ツール	導入しているウイルス対策ソフト、UTMなどのツール

インシデント対応の基本ステップ

ステップ 1　検知・対応判断

- **検知と連絡受付**

インシデントが疑われる兆候や実際の発生を発見した場合は、責任者に報告します。外部から通報を受け付けた場合は、通報者の連絡先等を控えます。社外での紛失または盗難の場合は警察へ届け出ます。

- **対応体制の立ち上げ**

インシデントが事業や顧客に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げます。責任者と担当者を定め、役割分担を明確にします。経営者は対応方針を策定します。

ステップ 2 対応・復旧

- **応急処置**

対応方針を基に、被害の拡大、二次被害の防止のために必要な応急処置を行います。被害を受けたシステムやサービス、アカウントを停止します。情報が外部からネットワークでアクセスできる状態にあったり、被害が広がる可能性があったりする場合には、ネットワークを遮断し、対象機器を隔離したうえでシステムを停止します。自社で対応が難しい場合は、IT製品のメーカー、保守ベンダー等の外部専門組織や公的機関の相談窓口等に支援、助言を依頼します（Ｐ８「インシデント発生時の相談窓口・報告先・問合せ先」を参照）。顧客や消費者に関係する場合は受付専用の問い合わせ窓口を開設し、被害が発生・拡大した場合にはその動向を速やかに把握し対応します。

- **証拠保全**

不用意な操作でシステム上に残された記録を消さないようにします★1。適切な対応判断を行うために、被害の実態を把握し、5W1H（いつ、どこで、誰が、何を、なぜ、どうしたのか）の観点で状況を整理します。また、発生に至る痕跡や証拠を確保します。

- **復旧**

復旧のための対応を行います。直接原因を究明し、修正プログラムの適用、設定変更、ソフトウェアやファームウェアの更新、機器の入替、データの復元等を行います。停止したシステムやサービス、アカウント等を復旧します。対応中は、復旧状況や事業への影響等について適時に経営者に状況を報告します。

★1 感染した機器を特定してフォレンジック調査（電磁的記録の調査・分析）を実施すると判断した場合、端末の再起動や電源を切ることによって証拠となるキャッシュやメモリなど揮発性情報は消失します。自社で証拠保全できる場合は、あらかじめ調査用の揮発性情報をUSBメモリなどに保存します。それが難しい場合は感染拡大を防ぐために電源を切ります。

ステップ 3　関係者への報告・公表

- **関係者への報告**

被害者や影響を及ぼした取引先があればインシデントに関して報告します。個人情報漏えいの場合は個人情報保護委員会、業法等で求められる場合は所管の省庁等、行政機関へ報告します。ウイルス感染や不正アクセスについては、IPAへ届け出ます。被害者に対する損害の補償等について必要に応じて対応します。

- **公表**

すべての関係者への個別連絡が困難であったり、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトやメディアを通じて公表します。公表が被害の拡大を招かないよう、時期、内容、対象などを考慮します。

- **再発防止策**

インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善等、抜本的な再発防止策を検討し、実施します。

ウイルス感染の場合

1．検知・対応判断

- **検知と連絡受付**
  - パソコン等を利用中に動作異常やウイルス対策ソフトの警告が表示された場合や、外部から公開しているシステムに異常があると通報を受けた場合、責任者に連絡します。
- **対応体制の立ち上げ**
  - 責任者と担当者を定め、役割分担を明確にします。経営者は対応方針を策定します。

2．対応・復旧

- **応急処置**
  - 被害拡大防止のため、感染したパソコンやサーバーの利用を停止します。
  - 感染したパソコンやサーバーは、接続するネットワークからケーブルを抜く、あるいは無線LANをオフにして遮断し、機器をネットワークから隔離します。
  - 他のパソコン等やサーバーがウイルスに感染していないかウイルス対策ソフトの定義ファイルを最新にしてからチェックします★2。
  - 自社で対応が難しい場合は、IT製品のメーカー、保守ベンダー等の外部専門組織や公的相談窓口に支援、助言を依頼します。
- **証拠保全**
  - 可能な限り、ウイルス感染の証拠保全★3を行います。
- **復旧**
  - ウイルス対策ソフトに従ってウイルスを駆除します。
  - ウイルス駆除ができない場合、OSからクリーンインストール（ソフトウェアをコンピュータに導入する際に、すでに導入済みのソフトウェアに含まれるデータやプログラムの影響を受けない形で新規にインストールすること。）等を実施します。

★2 パソコン等端末のウイルス感染を監視・検知し、担当者が集中管理できるツール（EDR：Endpoint Detection and Response）を導入すれば迅速な対応が可能です。

★3 証拠となるデータには、パソコンのハードディスク、メモリ内のデータ、サーバーやネットワーク機器のログ等があります。より具体的な内容を知りたい場合は、以下を参照ください。
IPA　インシデント対応へのフォレンジック技法の統合に関するガイド
https://www.ipa.go.jp/files/000025351.pdf

3．関係者への報告・公表

- **関係者への報告**
  - ウイルス感染による被害や経過をまとめた報告書を作成します。
  - 被害者や影響を及ぼした取引先があれば報告します。ウイルス感染については、IPAへ届け出ます。標的型攻撃など意図的な犯行とみられる場合には、警察へ届け出ます。ウイルス感染による影響によって、業法等で報告が求められる場合は所管の省庁へ報告します。
- **再発防止**
  - 抜本的な再発防止策を検討し、実施します。

IPA情報セキュリティ安心相談窓口（主にウイルスや不正アクセス）の技術的相談窓口：https://www.ipa.go.jp/security/anshin/index.html

ランサムウェア感染の場合

1．検知・対応判断

- **検知**
  - パソコンでウイルス感染等の兆候を発見したり、ウイルス対策ソフトのアラートが表示されたりした場合は、責任者に連絡します。
  - パソコンの画面に、身代金を要求するようなメッセージが表示された場合、ランサムウェア※5によるものか確認します。ランサムウェアの場合は、警察へ届け出ます。

- **対応体制の立ち上げ**
  - システム部門に加え、広報、法務とも連携した体制を立ち上げ、責任者と担当者を定め、役割を明確にします。経営者は対応方針を策定します。

★5　ランサムウェアとは、パソコン等の端末やサーバー上のデータを暗号化する等して使用不可にし、それらを復旧することと引き換えに身代金を支払うように促す脅迫メッセージを表示するウイルスの総称です。「人手によるランサムウェア攻撃」と「二重の脅迫」の2つの代表的手口があります。詳細は、IPAランサムウェア対策ページで確認ください。

2．対応・復旧

- **応急処置**
  - 影響範囲の特定、計画、封じ込め、根絶と復旧という手順を着実に進めます★6。被害が甚大な場合は、経営判断が求められる場面が多いため、意思決定のための情報を整理します。
  - 必要に応じて経過を公表し、二次被害等を抑制します。

- **証拠保全**
  - ランサムウェア感染を発見した時点から、経過報告を記録します。被害者となった場合、最終的に自社をとりまくステークホルダ（顧客、取引先、株主、所管の省庁等）に対し、どのような状況下で、どのような考え方で対応方針を定めたのかを説明可能な状態にします。

- **復旧**
  - 自社で対応が難しい場合は、保守ベンダーや、セキュリティサービス事業者等の外部専門組織や公的機関の相談窓口等に支援、助言を依頼します。

★6　ランサムウェア対策では、事前に基本的なセキュリティ対策を確実かつ多層的に適用することが重要であり、特に、企業・組織のネットワークへの侵入対策、データ・システムのバックアップを実施していることが有効です。

3．関係者への報告・公表

- **関係者への報告**
  - 原因について調査を行い、経緯や対応について整理し、経営者に報告します。
  - 必要に応じて、顧客や影響が及ぶ可能性がある組織等に公表します。

- **再発防止**
  - 抜本的な再発防止策を検討し、実施します。

IPAランサムウェア対策特設ページ：https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
侵入型ランサムウェア攻撃を受けたら読むFAQ： https://www.jpcert.or.jp/magazine/security/ransom-faq

システム停止の場合

1．検知・対応判断

- **検知と連絡受付**
  - システムに動作不良、障害、停止もしくはその兆候があれば、責任者に連絡します。

- **対応体制の立ち上げ**
  - 責任者と担当者を定め、役割分担を明確にします。
  - システム上の異常が事業に重大な影響を与える場合は、経営者が対応方針を策定します。
  - 重要なシステムの異常が事業や企業経営に影響する場合、事業継続計画（BCP）★4の発動を検討します。
  - 外部に公開しているシステムの場合、被害や影響を考慮し、関係者に連絡します。

★4　システムの事業継続計画のことを「IT-BCP」と呼びます。平時からシステムが事業に与える影響を踏まえてシステムの重要度を評価し、システムの稼働継続や復旧に関する計画を定めておくことが有効です。

2．対応・復旧

- **応急処置**
  - 原因調査を行い、サイバー攻撃によるものか、それ以外の設備や機器等の故障によるものか精査します。
  - 自社で調査や対応が難しい場合には、保守ベンダー等に協力を依頼します。

- **証拠保全**
  - 可能な限り、システム停止に関する証拠保全を行います。

- **復旧**
  - 復旧のための対応を行います。直接原因を究明し、修正プログラムの適用、設定変更、ソフトウェアやファームウェアの更新、機器の入替、データの復元等を行います。停止したシステムやサービスを復旧します。

3．関係者への報告・公表

- **関係者への報告**
  - 責任者は、インシデントの経過をまとめて報告書を作成し、経営者に報告します。
  - 業法等で報告が求められる場合は所管の省庁に報告します。取引先への影響がある場合や、取引先との取り決めがある場合には、取引先に報告します。
  - 必要に応じて、顧客や影響が及ぶ可能性がある組織等に公表します。

- **再発防止**
  - 抜本的な再発防止策を検討し、実施します。必要に応じて、事業継続計画（BCP）やIT-BCPについても見直します。

情報漏えいの場合

1．検知・対応判断

- **検知と連絡受付**
  - 情報漏えいが疑われる兆候や実際の発生を発見した場合は、責任者に報告します。責任者は、情報漏えいが事実かどうかを確認します。
  - メール誤送信、Webでの誤公開、紛失・置忘れなど過失によるものか、盗難のほか不正アクセス、内部犯行、脅迫等不正な金銭の要求など、第三者の故意あるいは犯罪性があるものかでケースを分けます。
  - 原因が社内にある場合、状況を確認し、関係者への連絡を検討します。第三者による場合、状況の確認、自社で調査が難しい場合には外部の専門家等に協力を依頼します。

- **対応体制の立ち上げ**
  - 責任者と担当者を定め、役割分担を明確にします。経営者は対応方針を策定します。

2．対応・復旧

- **応急処置**
  - 情報漏えいによる被害の拡大、二次被害の防止のために必要な応急処置を行います。
  - 情報が外部からアクセスできる状態にあったり、被害が広がる可能性があったりする場合には、接続するネットワークからケーブルを抜く、あるいは無線LANをオフにして遮断し、重要な情報を保存した機器をネットワークから分離します。また、システムやサービスを停止します。
  - 漏えいした情報の種類や件数、暗号化やアクセス制限等のセキュリティ対策状況を確認します。
  - 情報漏えいした本人や取引先等へ通知します。必要に応じてウェブサイト、メディア等による公表を検討します。個人情報が含まれる場合には、個人情報保護委員会に報告します。

- **証拠保全**
  - 事実関係を裏付ける情報や証拠を確保します。

- **復旧**
  - 復旧のための対応を行います。直接原因を究明し、修正プログラムの適用、設定変更、ソフトウェアやファームウェアの更新等を行います。停止したシステムやサービス、アカウント等を復旧します。
  - 対応中は、復旧状況や事業への影響等について適時に経営者に状況を報告します。

3．関係者への報告・公表

- **関係者への報告**
  - 被害にあった個人や取引先に対しては、連絡先がわからない等、特別な理由がない限り通知します。個人情報漏えいの場合は個人情報保護委員会へ報告します。情報漏えいの原因がウイルス感染や不正アクセスの場合は、IPAへ届け出ます。犯罪の可能性のある場合、警察へ届け出ます。

- **公表**
  - すべての関係者への個別通知が困難であったり、漏えいの影響が広く一般に及ぶ場合は、被害情報をウェブサイトやメディアを通じて公表します。公表が被害の拡大を招かないよう、時期、内容、対象などを考慮します。

- **再発防止**
  - 抜本的な再発防止策を検討し、実施します。

インシデント発生時の相談窓口・報告先・問合せ先

緊急対応についての相談窓口	
組織名称	**特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）**
連絡先	**サイバーインシデント緊急対応企業一覧** URL：https://www.jnsa.org/emergency_response/
概要	緊急対応について請負の相談が可能な企業一覧
技術的な相談窓口	
組織名称	**独立行政法人情報処理推進機構（IPA）**
連絡先	**情報セキュリティ安心相談窓口** URL：https://www.ipa.go.jp/security/anshin/ 問合せ先 Tel： 03-5978-7509 受付時間10:00～12:00、13:30～17:00 土日祝日・年末年始は除く Mail： anshin.@ipa.go.jp
概要	主にウイルスや不正アクセスに関する技術的な相談に対してアドバイスを提供
組織名称	**一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）**
連絡先	**インシデント対応 「JPCERT/CCに依頼する」** URL：https://www.jpcert.or.jp/menu_reporttojpcert.html 問合せ先 Mail：info@jpcert.or.jp
概要	インシデント対応の基礎資料、相談窓口を掲載
個人情報が漏えいした際の報告先	
組織名称	**個人情報保護委員会**
連絡先	**漏えい等の報告について** URL：https://www.ppc.go.jp/personalinfo/legal/leakAction/ **特定個人情報の漏えい等事案が発生した場合の対応について** URL：https://www.ppc.go.jp/legal/rouei/#anc_chusyo
概要	個人情報、特定個人漏えいの際の個人情報保護委員会への報告方法を掲載

被害が発生している場合の問合せ先・通報先・相談窓口・参照先①

ランサムウェア攻撃を受けた場合の問合せ先・参照先	
組織名称	**独立行政法人情報処理推進機構（IPA）**
連絡先	**ランサムウェア対策特設ページ** URL：https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html 問合せ先 情報セキュリティ安心相談窓口 Mail：anshin.@ipa.go.jp URL:https://www.ipa.go.jp/security/anshin/
概要	ランサムウェアの感染防止や被害低減のために役立つ情報を掲載
組織名称	**一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）**
連絡先	**ランサムウエア対策特設サイト** URL：https://www.jpcert.or.jp/magazine/security/nomore-ransom.htm 問合せ先 Mail：ew-info@jpcert.or.jpl
概要	ランサムウェア対策、JPCERT/CCにおける対応等を紹介
組織名称	**警察庁**
連絡先	**ランサムウェア被害防止対策** URL：https://www.npa.go.jp/cyber/ransom/
概要	ランサムウェア手口、相談窓口、ランサムウェア対策等を提供
組織名称	**No More Ransom**
連絡先	**No More Ransom** URL：https://www.nomoreransom.org/ja/about-the-project.html
概要	ランサムウェアの被害低減を目指す国際的な「No More Ransom」プロジェクトサイト

被害が発生している場合の問合せ先・通報先・相談窓口・参照先②

被害が発生あるいはその可能性がある場合の参照先・相談先・通報先	
組織名称	**一般社団法人セーファーインターネット協会**
連絡先	**セーフライン** URL：https://www.safe-line.jp/
概要	違法・有害情報に関する通報先
組織名称	**インターネット違法・有害情報相談センター**
連絡先	**インターネット違法・有害情報相談センター** URL：https://ihaho.jp/
概要	インターネット上での違法・有害情報に関する相談窓口
組織名称	**インターネット・ホットラインセンター**
連絡先	インターネットホットラインセンター URL：https://www.internethotline.jp/
概要	インターネット上の違法情報に関する通報先
組織名称	**都道府県警察本部のサイバー犯罪相談窓口**
連絡先	**都道府県警察本部のサイバー犯罪相談窓口一覧** URL：https://www.npa.go.jp/cyber/soudan.html
概要	サイバー犯罪の相談窓口
組織名称	**一般社団法人セーファーインターネット協会**
連絡先	なりすましECサイト対策協議会 URL：https://www.saferinternet.or.jp/e-commerce/narisumashi/
概要	なりすましECサイトに関する情報を提供
組織名称	**日本司法支援センター （法テラス）**
連絡先	法律相談 URL：https://www.houterasu.or.jp/ サポートダイヤル Tel：0570-078374 平日9:00～21:00、土曜9:00～17:00
概要	国が設立した法的トラブル解決の総合案内所、被害にあった際の法律相談窓口
フィッシング詐欺、ビジネスeメール詐欺が疑われる際の連絡先・相談先	
組織名称	**独立行政法人情報処理推進機構（IPA）**
連絡先	**ビジネスメール詐欺（BEC）対策特設ページ** URL：https://www.ipa.go.jp/security/bec/ 問合せ先 Tel: 03-5978-7535 Mail: isec-info@ipa.go.jp 受付時間10:00～12:00 13:30～17:00 土日祝日・年末年始は除く
概要	ビジネスメール詐欺の対策に必要となる情報を集約
組織名称	**フィッシング対策協議会**
連絡先	**フィッシング対策協議会サイト** URL：https://www.antiphishing.jp/ **フィッシングの報告** URL：https://www.antiphishing.jp/registration.html
概要	フィッシング対策に関する情報を集約、フィッシング詐欺の報告先
組織名称	**一般社団法人日本データ通信協会**
連絡先	**迷惑メール相談センター** URL：https://www.dekyo.or.jp/soudan/
概要	迷惑メールに関する情報を集約、迷惑メールの相談先

被害の届出・相談先、セキュリティ関連情報の参照先

ウイルス・脆弱性情報の届出先	
組織名称	独立行政法人情報処理推進機構（IPA）
連絡先	**コンピュータウイルス・不正アクセスに関する届出** URL：https://www.ipa.go.jp/security/outline/todokede-j.html
概要	ウイルス感染被害の拡大や再発の防止、不正アクセス被害の実態把握や同様の被害発生の防止に役立てるための、届出先
連絡先	**脆弱性関連情報の届出受付** URL：https://www.ipa.go.jp/security/vuln/report/
概要	脆弱性関連情報の適切な流通および対策の促進を図るための、経済産業省の告示に基づき策定された情報セキュリティ早期警戒パートナーシップガイドラインに則り運用されるサイト

サイバー犯罪が疑われる際の相談先	
組織名称	警察庁
連絡先	**都道府県警察本部のサイバー犯罪相談窓口等一覧** URL：https://www.npa.go.jp/cyber/soudan.html
概要	サイバー犯罪にあった際に相談する各都道府県の窓口、連絡先一覧を掲載

脅威情報、注意喚起情報を確認したい場合の参照先	
組織名称	一般財団法人日本サイバー犯罪対策センター
連絡先	**脅威情報　脅威具体例**　URL：https://www.jc3.or.jp/threats/examples/ **脅威情報**　URL：https://www.jc3.or.jp/threats/topics/
概要	脅威情報等の具体例を含めて掲載

脆弱性対策、早期警戒情報を確認したい場合の参照先	
組織名称	独立行政法人情報処理推進機構（IPA）
連絡先	**脆弱性対策** URL：https://www.ipa.go.jp/security/vuln/index.html
概要	脆弱性情報の確認、対策等を掲載
組織名称	一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
連絡先	**脆弱性対策情報** URL：https://www.jpcert.or.jp/vh/top.html **早期警戒情報** URL：https://www.jpcert.or.jp/menu_receiveinformation.html
概要	脆弱性情報を提供。早期警戒情報の提供、レポートの提供

脆弱性対策、早期警戒情報を確認したい場合の参照先	
組織名称	独立行政法人情報処理推進機構（IPA）
連絡先	**脆弱性対策** URL：https://www.ipa.go.jp/security/vuln/index.html
概要	脆弱性情報及び対策等を掲載
組織名称	一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
連絡先	**脆弱性対策情報**　URL：https://www.jpcert.or.jp/vh/top.html **早期警戒情報**　URL：https://www.jpcert.or.jp/menu_receiveinformation.html
概要	脆弱性情報を提供、早期警戒情報及びレポートを提供

セキュリティ対策のための情報入手先・相談先

セキュリティ対策を行うための情報入手先		
組織名称		**独立行政法人情報処理推進機構（IPA）**
	連絡先	**情報セキュリティ対策支援サイト** URL：https://security-shien.ipa.go.jp/ **セキュリティプレゼンター支援** URL：https://security-shien.ipa.go.jp/presenter/ **情報セキュリティサービス基準適合サービスリスト** URL：https://www.ipa.go.jp/security/it-service/service_list.html
	概要	恒常的にセキュリティ対策を進める上で役立つ情報を掲載
	連絡先	**ここからセキュリティ！情報セキュリティ・ポータルサイト** URL：https://www.ipa.go.jp/security/kokokara/
	概要	サイバー攻撃の被害にあった可能性がある場合の確認内容等を集約
組織名称		**東京都産業労働局**
	連絡先	**東京中小企業サイバーセキュリティ支援ネットワーク（Ｔｃｙｓｓ）** URL：https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/soudan/ Tel：03-5320-4773 相談窓口：東京都産業労働局商工部内 Tcyss事務局（都庁第一本庁舎20階北側） 受付時間：都庁開庁日の9:00～12:00、13:00～17:00
	概要	東京都と警視庁、中小企業支援機関、サイバーセキュリティ対策機関などが連携して開設した、中小企業のための相談窓口
	連絡先	**東京中小企業支援 サイバーセキュリティ** URL：https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/
	概要	サイバーセキュリティに関する意識啓発、情報共有、相談対応などの中小企業支援
テレワークに関連したセキュリティ対策を検討する場合の相談先		
組織名称		**厚生労働省・総務省**
	連絡先	**テレワーク総合ポータル** URL：https://telework.mhlw.go.jp/ 問合せ先 URL：https://telework.mhlw.go.jp/contact/ Tel：0120-861009　土・日・祝日を除く
	概要	厚生労働省・総務省のテレワーク導入相談窓口
組織名称		**東京都**
	連絡先	**東京都テレワーク推進センター** URL：https://tokyo-telework.jp/ **問合せ先** URL：https://tokyo-telework.metro.tokyo.lg.jp/contact
	概要	東京都のテレワーク相談窓口

【参考】中小企業のセキュリティ対策支援制度

独立行政法人情報処理推進機構（IPA）
サイバーセキュリティお助け隊サービス制度
https://www.ipa.go.jp/security/otasuketai-pr/index.html

サイバー攻撃への対処として最低限必要なサービスを
効果的かつ安価、確実に提供する中小企業向けのサイバーセキュリティサービス

IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス
TEL 03-5978-7508 FAX 03-5978-7546
E-mail isec-pr-nw@ipa.go.jp URL https://www.ipa.go.jp/security/