

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

TOP SECRET

INFORMATION

インフォメーション





もしかしてサイバー攻撃? ここに連絡を!



事前に情報を整理しましょう

サイバー攻撃を受けた可能性がある場合は、事前に次のような情報を整理して緊急連絡先に連絡しましょう。



- 対象となる端末の種類（パソコン、スマートフォンなど）
- 対象となる端末のOS（Windows 10、Androidなど）
- インストールしているセキュリティソフトの名称
- 利用しているクラウドサービスの名称
- 事象が発生した日とその内容、その後発生した事象
- ウィルスまたは不正アクセスによるものと判断した根拠
- 他に相談した窓口や機関



犯罪の可能性がある場合の相談窓口

警視庁 サイバー犯罪対策課

<https://www.keishicho.metro.tokyo.jp/sodan/madoguchi/sogo.html>

TEL 03-5805-1731

受付時間：平日8:30-17:15



一般的な情報セキュリティ相談

独立行政法人 情報処理推進機構（IPA） 情報セキュリティ安心相談窓口

<https://www.ipa.go.jp/security/anshin/>

TEL 03-5978-7509 FAX 03-5978-7518

受付時間：10:00-12:00 13:30-17:00（土日祝日・年末年始を除く）

E-mail anshin@ipa.go.jp



被害の報告・連絡・相談窓口

ウイルスに関する届け出（IPA）

<https://www.ipa.go.jp/security/outline/todokede-j.html>

不正アクセスに関する届け出（IPA）

<https://www.ipa.go.jp/security/ciadr/>

フィッシング詐欺（フィッシング対策協議会）

<https://www.antiphishing.jp/>

迷惑メール（日本データ通信協会 迷惑メール相談センター）

<https://www.dekyo.or.jp/soudan/>

なりすましECサイト（なりすましECサイト対策協議会）

<https://www.saferinternet.or.jp/e-commerce/narismashi/>

インシデント報告・届出（JPCERT/CC）

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

インシデント報告・届出（IPA J-CRAT 標的型サイバー攻撃特別相談窓口）

<https://www.ipa.go.jp/security/tokubetsu/>

法律相談（日本司法支援センター 法テラス）

<https://www.houterasu.or.jp/>



その他の主な報告・連絡・相談窓口等



被害が発生している可能性がある場合

違法・有害情報（セーファーインターネット協会）

<https://www.safe-line.jp/>

違法・有害情報（インターネット違法・有害情報相談センター）

<https://www.ihaho.jp/>

違法・有害情報（インターネット・ホットラインセンター）

<http://www.internethotline.jp/>

個人情報（個人情報保護委員会）

<https://www.ppc.go.jp/>

嫌がらせ・ネットストーカー（管轄の警察署の生活安全課）

Webブラウザーで「警察署一覧」で検索

人権侵害（法務省人権擁護局 みんなの人権110番）

http://www.moj.go.jp/JINKEN/index_soudan.html





恒久的対策を行うための情報源

情報セキュリティ対策支援サイト (IPA)

<https://security-shien.ipa.go.jp/>

セキュリティプレゼンター支援 (IPA)

<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 (IPA)

https://www.ipa.go.jp/security/it-service/service_list.html

サイバーアクセント緊急対応企業一覧 (JNSA)

https://www.jnsa.org/emergency_response/

経営とIT化相談窓口 (ITコーディネータ協会)

<https://www.itc.or.jp/management/diagnosis/>

東京都テレワーク推進センター (東京都)

<https://tokyo-telework.jp/>

テレワーク相談センター (厚生労働省委託事業)

<https://www.tw-sodan.jp/>

テレワークのセキュリティあんしん相談窓口 (LAC)

<https://www.lac.co.jp/telework/security.html>

ワンストップ総合相談窓口 (東京都中小企業振興公社)

<https://www.tokyo-kosha.or.jp/support/shien/soudan/>



東京都による情報源

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です。

<https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/soudan/>
TEL 03-5320-4773

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30階北側）

受付時間：都庁開庁日の9:00～12:00、13:00～17:00

東京中小企業支援 サイバーセキュリティ

<https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/>

「中小企業向けサイバーセキュリティの極意」ポータルサイト

<https://cybersecurity-tokyo.jp/>



セキュリティ お役立ちリンク

サイバーセキュリティ対策に有用な文献、Webページには下記のようなものがあります。必要に応じて情報を収集しましょう。

●サイバーセキュリティに関する基本文書、白書、解説文書

基本文書 (法律・ 基本計画・ 各種方針等)	サイバーセキュリティ基本法 サイバーセキュリティ戦略 サイバーセキュリティ2020 セキュリティ関連NIST文書	総務省 NISC NISC IPA
各種白書・ 年次報告書類	情報通信白書 AI白書 情報セキュリティ白書 IT人材白書	総務省 IPA IPA IPA

●各実施事項の参考情報

全般	企業経営のためのサイバーセキュリティの考え方 サイバーセキュリティ経営ガイドライン サイバーフィジカルセキュリティフレームワーク (CPSF) サイバーサプライチェーンリスクマネジメント ISMS適合評価制度	NISC 経済産業省 経済産業省 IPA JIPDEC
	Society5.0	内閣府
	サイバーフィジカルシステム (CPS)	JEITA
	DXレポート2 中間取りまとめ（概要）	経済産業省
	DXの推進に関するお役立ちコンテンツ一覧	IPA
テレワーク 関連	テレワークで始める働き方改革—テレワークの導入・運用ガイドブック テレワークを実施する際にセキュリティ上留意すべき点について テレワークセキュリティガイドライン第4版 テレワーク勤務のサイバーセキュリティ対策！	厚生労働省 NISC 総務省 警視庁

IoT セキュリティ 関連	IoTセキュリティガイドライン ver 1.0	総務省
	IoTセキュリティ対応マニュアル産業保安版	経済産業省
	安全なIoTシステムのためのセキュリティに関する一般的枠組	NISC
	IoTセキュリティチェックリスト	JPCERT/CC
	IoT・5Gセキュリティ総合対策プログレスレポート	総務省
人材育成関連	iコンピテンシディクショナリ（iCD）について	IPA
	ITSS+・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報	IPA
	サイバーセキュリティ体制構築・人材確保の手引き	経済産業省
	情報処理技術者試験・情報処理安全確保支援士試験	IPA

●各実施事項の参考情報

内閣サイバーセキュリティセンター（NISC）	
	みんなでしっかりサイバーセキュリティ
	みんなで使おうサイバーセキュリティ・ポータルサイト
	サイバーセキュリティ関係法令_Q&AハンドブックVer1.0
情報処理推進機構（IPA）	
	情報セキュリティ
	ここからセキュリティ
	SECURITY ACTION セキュリティ対策自己宣言
	サイバー情報共有イニシアティブ（J-CSIP）
JPCERTコーディネーションセンター（JPCERT/CC）	
	緊急情報を確認する
	脆弱性対策情報データベース（JVN iPedia）
	JPCERT/CCに依頼する
総務省	
	国民のためのサイバーセキュリティサイト
	国民のためのサイバーセキュリティサイトリンク集
日本サイバー犯罪対策センター（JC3）	
警視庁 情報セキュリティ広場	



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の進め方

情報技術の進歩・普及に伴い経営効率が向上した一方、重要情報の漏えいや消失、改ざんなど技術特有の不利益が発生する機会も増してきています。

これら不利益が対策の不備により生じた場合、経営者は取引先や従業員などへの社会的・道義的責任に加え、法的責任も追及されるおそれがあります。

近年は企業情報を狙うサイバー脅威も日々巧妙化しています。自社を守るためには、経営者が率先して対策に取り組むことが大切です。

●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/>

情報セキュリティ対策を推進する際に参考にしたいのが、「中小企業の情報セキュリティ対策ガイドライン」（情報処理推進機構〈IPA〉）です。

このガイドラインは情報の安全管理の重要性や企業の保有する機微な情報を各種の脅威から保護するための

対策の考え方や段階的に実現するための方策を紹介する目的で作成されたものです。まずはこのガイドラインを参考に、自社に適した対策を実践していくとよいでしょう。



● 「中小企業の情報セキュリティ対策ガイドライン」

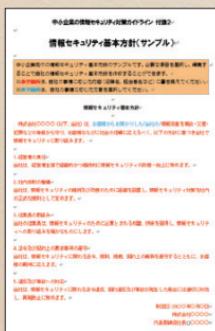


第1部 経営者編

経営者編では、情報セキュリティ対策に関して、
経営者が認識し、
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ます。

1 | 2 | 3 | 4 | 5 | 目次

信用失墜、取り扱い停止、業務低落、顧客や取引先への迷惑、刑罰、損害賠償、
... といった問題を避けるにはどうすれば良いか
分からないなら 市場に任せると?



新 5分でできる！ 情報セキュリティ自社診断

最新動向への対応、できてますか？

脅威や攻撃の変化	IT機器の変化
----------	---------

取り組むべきことにならないとならない
あなたの会社のセキュリティ状況
「5分でできる！自社診断」でチェック！

中小企業の情報セキュリティ関連規程(サンプル)

規程名: [規程名] - 第1回定期検査実施規程

規程内容: [規程内容]

項目	内容
1. 調査実施時期	1月1日～1月31日
2. 対象組織	本社・支社
3. 調査実施範囲	全社
4. フォーマット実施期間	1月1日～1月31日
5. 対象調査員	社員全員
6. 対象調査項目	IT機器の状況、セキュリティポリシー、データ漏洩対策等
7. 対象調査方法	問診調査、実証調査、監査調査等
8. 対象調査結果	調査結果報告書
9. 対象調査費用	調査費用
10. 対象調査期間	1ヶ月
11. 対象調査結果の提出期限	2月1日～2月28日

●付録2

「情報セキュリティ
基本方針（サンプル）」

●付録3

「5分でできる！ 情報
セキュリティ自社診断」

●付録5

「情報セキュリティ
関連規程（サンプル）」

**ACTION
1**

最低限のルール 「情報セキュリティ5か条」

資金や人材が限られる中小企業にとって、最初から全ての対策に取り組むことは容易ではありません。まずは、基本的な対策を取りまとめた「情報セキュリティ5か条」に取り組むことからはじめ、段階的に対策を講じていきましょう。

1 OSやソフトウェアは常に最新の状態にしよう！

Windows OS、Mac OS、Androidなどはいずれも常に最新バージョンに！Office、Adobe Readerなど利用中のソフトウェアも常に最新バージョンに！

 「自動アップデート」は必ずONに！



2 ウイルス対策ソフトを導入しよう！

ウイルス定義ファイルは自動更新に設定！

ファイアウォールや脆弱性対策なども可能な統合型セキュリティ対策ソフトを導入！

 ウイルス対策ソフトも常に最新に！



3 パスワードを強化しよう！

ID・パスワードは推測や解析、ウェブサービスからの流出することで不正ログインに悪用される恐れがある！

「長く」「複雑」「使い回さない」を徹底しよう！

パスワードは使い回さない！



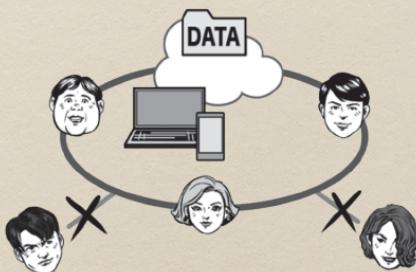
4 共有設定を見直そう！

クラウドサービスの共有を限定的に！

ネットワーク接続の複合機、カメラ、ハードディスク、NASなどの共有を限定的に！

従業員の異動や退職時に設定の変更や削除漏れがないように！

利用者は必要な人だけに！



5 脅威や攻撃の手口を知ろう！

セキュリティ専門機関から常に最新の脅威情報を収集！

利用中のネットバンクやクラウド

サービスからの注意喚起を確認！

最新情報で対策を！



**ACTION
2**

組織的な対策に取り組む

基本的対策の次は組織的な対策です。「中小企業の情報セキュリティ対策ガイドライン」とその付録を参考に自社に適した基本方針を作成し、社内関係者に周知します。また、自社のセキュリティ診断を実施して、取り得る対策を検討していきましょう。

1 情報セキュリティ基本方針の作成と周知

従業員の指針であり、関係者に対して取り組みを表明するための情報セキュリティに関する基本方針を経営者が定め、簡潔な文書にまとめて周知します。「中小企業の情報セキュリティ対策ガイドライン」と付録2の「情報セキュリティ基本方針（サンプル）」を参考に、経営者と連携して自社に適した基本方針を作成しましょう。

2 実施状況の把握

付録3の「5分でできる！情報セキュリティ自社診断」を利用して、情報セキュリティ対策がどれくらい実施できているかを把握しましょう。

3 対策の決定と周知

「5分でできる！情報セキュリティ自社診断」の結果を基に、解説編を参考にして実施すべき情報セキュリティを検討しましょう。





本格的に対策に取り組む

情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ責任者を任命して責任分担と連絡体制を整備しましょう。また、情報セキュリティ事故が発生した場合など、緊急時対応体制も整備しておきましょう。

1 管理体制の構築

情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ責任者、情報部門責任者、システム管理者、教育責任者、点検責任者を任命して責任分担と連絡体制を整備しましょう。また、情報セキュリティ事故が発生した場合など、緊急時対応体制も整備しておきましょう。

2 IT利活用方針と情報セキュリティの予算化

クラウドサービスの普及によってIT利活用の方法が多様化したこと、情報セキュリティリスクも多様化しています。自社で利用している情報システムやサービスの台帳を作成したり図式化したりして把握した上で対策を検討し、必要な予算を確保しましょう。



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

3 情報セキュリティ規程の作成

事業内容や取り扱う情報、職場環境、IT利活用の状況に応じて、「中小企業の情報セキュリティ対策ガイドライン」付録5の「情報セキュリティ関連規程（サンプル）」を参考に、情報セキュリティ規程を作成しましょう。（1）対応するリスクの特定、（2）対策の決定、（3）規程の作成の順に進めます。

4 委託時の対策

業務の一部または全部を外部に委託したり、レンタルサーバーやクラウドサービスなどの外部サービスを利用したりして、重要な情報を渡したり処理を依頼したりする場合には、委託先に実施してもらう情報セキュリティ対策も決めましょう。取引条件のひとつとして、契約書や覚書に具体的な対策を明記しましょう。

5 点検と改善

「情報セキュリティ5か条」や「5分でできる！情報セキュリティ自社診断」、自社の情報セキュリティ対策に関するルール・規程を基準に、情報セキュリティ対策が、計画通りに実行されているか、見落としている対策はないか、対策がセキュリティ事故防止の役に立っているかを確認しましょう。





対策をより強固にする

本格的な対策に取り組んでいても、必要な対策を追加して強固にしましょう。

1 情報収集と共有

情報セキュリティに関する脅威や攻撃の手口を知り、社内や取引先、同業者と共有することで対策レベルの向上につなげましょう。

2 ウェブサイトの情報セキュリティ

情報漏えいや改ざんなどの被害が発生する攻撃の対象になりやすいWebサイトの運営形態、構築、運営それぞれの段階に応じた対策を講じましょう。

3 クラウドサービスの情報セキュリティ

クラウドサービスに適した情報セキュリティ対策について、サービスの選定、運用、セキュリティ対策の3段階で検討しましょう。

4 情報セキュリティサービスの活用

コンサルテーションや教育サービス、監査サービスなど、情報セキュリティ対策を強固にする外部のサービスの利用を検討しましょう。

5 技術的対策例と活用

ネットワーク脅威対策やコンテンツセキュリティ対策など、情報セキュリティ対策の向上に資する製品やソフトウェアの導入を検討しましょう。

6 詳細リスク分析の実施

(1) 情報資産の洗い出し、(2) リスク値の算定、(3) 情報セキュリティ対策の決定の順で、リスクの洗い出しと対策の検討を行いましょう。



中小企業のためのクラウド サービス安全利用手引き



クラウドサービスとは

インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービスをクラウドサービスと呼びます。クラウドサービスの利用は、情報システムの構築や管理といった手間が省けるなど、自社での所有・運用と比較して業務の効率化やコストダウンを図れるといったメリットがあります。



利用前の確認

クラウドサービスの利用を検討する際は、情報セキュリティ対策の一部がサービス提供事業者に依存してしまうことや、クラウドサービス固有のリスクがある点についても考慮する必要があります。『クラウドサービス安全利用の手引き』(情報処理推進機構<IPA>)では、サービスを選択するときのポイントについて事例をあげて解説しています。

●中小企業のためのクラウドサービス安全利用の手引き

<https://www.ipa.go.jp/files/000072150.pdf>



パブリッククラウドとプライベートクラウド

クラウドには大きく「パブリッククラウド」と「プライベートクラウド」があり、前者は、企業・個人を問わず必要なときにサーバーやサービス活用が可能です。後者は、企業・組織が専用環境を構築して社内各部署などにサービス提供する形を指します。しかし、各々メリット・デメリットがあり、両者を統合して利用する「ハイブリッドクラウド」の活用が増えつつあります。



クラウドサービス利用時の確認事項

●選択するときのポイント

1	どの業務で利用するか明確にする	どの業務クラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？
2	クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？
3	取り扱う情報の重要度を確認する	クラウドサービスで取り扱う情報が漏えい、改ざん、消失したり、サービスが停止したりした場合の影響を確認しましたか？
4	セキュリティのルールと矛盾しないようにする	自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？
5	クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者ですか？
6	クラウドサービスの安全・信頼性を確認する	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？

●運用するときのポイント

7	管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
8	利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
9	利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
10	バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要な情報を手元に確保して必要なときに使えるようにしていますか？

●セキュリティ管理のポイント

11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取り扱い条件について確認しましたか？
14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的な契約条件の各項目について確認しましたか？
15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

No15 クラウドサービスのサーバーは日本国外に設定されている場合もありますが、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。No 6、11、12、13はスマートSMEセンター（認定情報処理支援機関）開示情報で確認できます。

出典：IPA「中小企業のためのクラウドサービス安全利用の手引き」より



IT活用に不可欠なIT人材の確保と育成



セキュリティ人材育成と考え方の変化

企業規模等によっても異なりますが、セキュリティ対策の中心となるのは、セキュリティ統括分野やセキュリティ監視・運用分野等を担うセキュリティ人材です。さらに、ITを利活用して社会を変えるSociety5.0の進展など、時代の変化を受け、本来の業務の中でITを利活用する人材にもセキュリティに関するスキルが求められるようになっています。



求められる「プラス・セキュリティ人材」

企業におけるあらゆる業務でデジタルトランスフォーメーション（DX）が進んでいますが、DXによる利便性はサイバー攻撃にも悪用されやすいため、DXを活用する企業ではセキュリティを意識して必要な対策を総合的に実施することが求められます。

一方、IPAなどによる調査では、そうしたセキュリティ人材の量的・質的不足が大きな課題となっています。セキュリティ対策がセキュリティ人材だけでは対処できなくなっているため、デジタル部門、事業部門、管理部門など、セキュリティ対策が不十分な場合にセキュリティ上の問題が生じるような業務を担っている人材にも、セキュリティに関する意識を養い、対策の実施に求められる知識・スキルを積極的に身に付けてもらう必要があります。

こうした「プラス・セキュリティ人材」の育成がこれからの企業には求められます。



「プラス・セキュリティ人材」の育成

「プラス・セキュリティ人材」を育成する際には、経済産業省が定めている、セキュリティ領域のIT人材に求められる個人のIT関連能力を明確化・体系化し、スキルやキャリア（職業）を示した指標である「ITSS+（セキュリティ領域）」を活用し、関連部門でセキュリティ関連タスクを担う人材の特定・育成・配置等を検討するとよいでしょう。

●IT人材の育成（IPA）

<https://www.ipa.go.jp/jinzai/itss/itssplus.html>

●サイバーセキュリティ体制構築・人材確保の手引き（経済産業省）

<https://www.meti.go.jp/press/2020/09/20200930004/20200930004-1.pdf>



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info



情報セキュリティ関連法令

企業の情報セキュリティに関する国内の法令は、下記のように多岐にわたります。また、海外に子会社や支店、営業所などを有し、日本から海外に商品やサービスを提供している企業や海外から個人データの処理について委託を受けている事業など、業務の内容によっては、EU域内の各国に適用される個人データ保護を規定したEU一般データ保護規則（GDPR：General Data Protection Regulation）などの海外法令への対応も必要になります。

- ・サイバーセキュリティ基本法
- ・不正アクセス禁止法
- ・個人情報保護法
- ・民法、刑法
- ・その他のセキュリティ関連法規（電子署名及び認証業務等に関する法律、プロバイダ責任制限法、特定電子メール法）
- ・知財関連法規（著作権法、産業財産権法、不正競争防止法）
- ・労働関連・取引関連法規（労働基準法、労働者派遣法、男女雇用機会均等法、公益通報者保護法、労働安全衛生法、下請法、特定商取引法、電子消費者契約法）
- ・海外法令（GDPR等）
- ・その他の法律・ガイドライン・技術者倫理
- ・「非連邦政府組織およびシステムにおける管理対象非機密情報CUIの保護（SP800-171）」

内閣官房内閣サイバーセキュリティセンター（NISC）は、関連法令をQ&A形式で解説する「サイバーセキュリティ関係法令Q&Aハンドブック」を公開しています。自社の業務と照らし合わせながら、効率的・効果的なサイバーセキュリティ対策・法令遵守を実践するとよいでしょう。

●内閣官房内閣サイバーセキュリティセンター（NISC）関係法令等
<https://www.nisc.go.jp/law/>



情報管理が不適切な場合の 処罰など

個人情報などの法的な管理義務がある情報を適切に管理していなかった場合には、企業の経営者や役員、担当者は下記の表に示すような責任を問われ、処罰されることになります。

法令	条項	処罰など
個人情報保護法 個人情報の保護に関する法律	40条 報告及び立入検査	委員会による立入検査、帳簿書類等の物件検査及び質問
	83条 個人情報データベース等不正提供罪	1年以下の懲役又は50万円以下の罰金
	84条 委員会からの命令に違反	6月以下の懲役又は30万円以下の罰金
	85条 委員会への虚偽の報告など	30万円以下の罰金
	87条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
マイナンバー法 (番号法) 行政手続における特定の個人を識別するための番号の利用等に関する法律	48条 正当な理由なく特定個人情報ファイルを提供	4年以下の懲役若しくは200万円以下の罰金又は併科
	49条 不正な利益を図る目的で、個人番号を提供又は盗用	3年以下の懲役若しくは150万円以下の罰金又は併科
	50条 情報提供ネットワークシステムに関する秘密を漏えい又は盗用	同上
	51条 人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入、不正アクセス等により個人番号を取得	3年以下の懲役又は150万円以下の罰金
	53条 委員会からの命令に違反	2年以下の懲役又は50万円以下の罰金
	54条 委員会への虚偽の報告など	1年以下の懲役又は50万円以下の罰金
	55条 偽りその他不正の手段により個人番号カード等を取得	6月以下の懲役又は50万円以下の罰金
	57条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑

法令	条項	処罰など
不正競争防止法 営業秘密・限定提供データに係る不正行為の防止など	3条 差止請求	利益を侵害された者からの侵害の停止又は予防の請求
	4条 損害賠償請求	利益を侵害した者は損害を賠償する責任
	14条 信頼回復措置請求	信用を害された者からの信用回復措置請求
金融商品取引法 インサイダー取引の規制など	197条の2 刑事罰	5年以下の懲役若しくは500万円以下の罰金又はこれらの併科
	207条1項2号 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
	198条の2 没収・追徴	犯罪行為により得た財産の必要的没収・追徴
	175条 課徴金	違反者の経済的利得相当額
民法	709条 不法行為による損害賠償	故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う

出典：IPA「中小企業の情報セキュリティ対策ガイドライン」より

主な参考文献

ジャンル	タイトル	発行元
サイバーセキュリティ対策全般	中小企業の情報セキュリティ対策ガイドライン 第3版	IPA
	サイバーセキュリティ経営ガイドライン	経済産業省 ・ IPA
	サイバーセキュリティ経営ガイドライン解説書	IPA
	企業経営のためのサイバーセキュリティの考え方の策定について 情報セキュリティ5カ条	NISC
	インシデント対応マニュアルの作成について	IPA
	中小企業における組織的な情報セキュリティ対策ガイドライン 事例集	JPCERT/CC IPA
	企業(組織)における最低限の情報セキュリティ対策のしおり	IPA
	中小企業における情報セキュリティ対策の実態調査 事例集	IPA
	ISO27002:2014情報セキュリティ管理策の実践（11物理的 及び環境的セキュリティ）	JIS
	地方公共団体における情報セキュリティポリシーに関するガイ ドライン（平成27年3月）	総務省
サイバー攻撃について	情報管理はマネーです	JIPDEC
	サイバーセキュリティ関係法令Q&Aハンドブック	NISC
	情報セキュリティ10大脅威 2021	IPA
個別のサイバー攻撃対策	サイバー攻撃ってなに？	NISC
	サイバーセキュリティ 2020	NISC
	ランサムウェアの脅威と対策	IPA
	IPA テクニカルウォッチ 「標的型攻撃メールの例と見分け方」	IPA
	組織における内部不正防止ガイドライン	IPA
	情報漏えい発生時の対応ポイント集	IPA
	IPA 対策のしおり(1) ウイルス対策のしおり	IPA
	IPA 対策のしおり(2) スパイウェア対策のしおり	IPA
個別のサイバー攻撃対策	IPA 対策のしおり(3) ポット対策のしおり	IPA
	IPA 対策のしおり(4) 不正アクセス対策のしおり	IPA
	IPA 対策のしおり(5) 情報漏えい対策のしおり	IPA
	IPA 対策のしおり(6) インターネット利用時の危険対策のしおり	IPA
	IPA 対策のしおり(7) 電子メール利用時の危険対策のしおり	IPA
	IPA 対策のしおり(8) スマートフォンのセキュリティ<危険回 避>対策のしおり	IPA

ジャンル	タイトル	発行元
個別のサイバー攻撃対策	IPA 対策のしおり(9) 初めての情報セキュリティ 対策のしおり IPA 対策のしおり(10) 標的型攻撃メール＜危険回避＞対策のしおり コンピュータセキュリティインシデントへの対応 高度サイバー攻撃対処のためのリスク評価等のガイドライン付属書 「標的型メール攻撃」対策に向けたシステム設計ガイド スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書	IPA IPA JPCERT/CC NISC IPA NISC
役に立つツール	情報セキュリティハンドブックひな形 情報セキュリティポリシーサンプル 情報セキュリティ自己診断チェックリスト 5分でできる！情報セキュリティ自社診断シート・パンフレット 情報セキュリティ対策自己診断テスト ～情報セキュリティ対策ベンチマークVer.5～ 中小企業のためのクラウドサービス安全利用の手引き	IPA IPA NISC IPA IPA IPA
IoT対策	IoT セキュリティガイドライン IoT、AI、ロボットに関する経済産業省の施策について 2017 攻めのIT経営中小企業百選 中小ものづくり企業IoT等活用事例集	経済産業省 経済産業省 経済産業省 経済産業省
個人情報	ホームページ「マイナンバー制度とマイナンバーカード」 個人情報取扱事業者のみなさん、新たに個人情報取扱事業者となるみなさんへ 「個人情報」の「取扱いのルール」が改正されます！	総務省 経済産業省
その他	2020年版中小企業白書 令和2年版情報通信白書 IT人材白書2020 自治体CIO育成研修 集合研修 SLAの考え方 情報システムに係る政府調達へのSLA導入ガイドライン ICTの進化が雇用と働き方に及ぼす影響に関する調査研究 平成28年	中小企業庁 総務省 IPA 総務省 IPA 総務省

IPA：独立行政法人情報処理推進機構

NISC：内閣サイバーセキュリティセンター

JPCERT/CC：一般社団法人JPCERT コーディネーションセンター

JIPDEC：日本情報経済社会推進機構

用語解説インデックス

[A]	AI	120,124	変革)
	Android	38	
	スマートフォン用のOSの1つ		
[B]	BEC	11,52	
	Business Email Compromise (ビジネスメール詐欺)		
[C]	CISO	106	
	Chief Information Security Officer (最高情報セキュリティ責任者)		
	CPS	119	
	Cyber-Physical System		
	CSIRT	113,116	
	Computer Security Incident Response Team		
	CSR	112	
	corporate social responsibility (企業の社会的責任)		
[D]	DDoS攻撃	21	
	複数のネットワークに分散する大量のコンピューターが一斉に特定の対象に送信し、通信容量をあふれさせて機能を停止させてしまう攻撃		
	DKIM	71	
	DMARC	71	
	DoS攻撃	21	
	Denial of Servicesの略。企業や組織のWebシステムに大量の通信パケットを送りつけて利用できなくなる攻撃		
	DX	96,119	
	Digital Transformation (デジタル		
[E]	ECサイト	34	
	Electronic Commerceの略でインターネット上で商品やサービスの売買を行うサイト		
[G]	GDPR	182	
	General Data Protection Regulation : EU一般データ保護規則		
[I]	ICカード	66	
	ID	29	
	Identification の略。コンピューターシステムで利用者を識別するための符号		
	IoT	31,46,120,122,126,128	
	IPアドレス	71,74	
	Internet Protocol Addressの略で、ネットワーク上にあるコンピューターや通信機器を判別するための番号		
	IT	21	
	Information Technologyの略で情報技術の総称		
	IT-BCP	119,146	
	IT-Business Continuity Plan (ITにおける事業継続計画)		
	ITSS+	181	
	IT skill standard + (ITスキル標準プラス)		
	ITガバナンス	99	
	IT governance : 企業がITへの投資や効果、リスクを継続的に最適化するために構築する組織的な仕組み		

[N] NAS	173	Webサーバー	28
Network Attached Storageの略で ネットワークに接続された記憶装置		ホームページや情報・機能を提供す るコンピューター	
NIST	93	Webサービス	28
National Institute of Standards and Technology（米国国立標準技 術研究所）		Webアプリケーションを使い、ネッ トワークを通じてソフトウェアの機 能を利用できるようにしたもの	
NOTICE	47,131	【あ】 アカウント	35
		ユーザーがネットワークやコンピュー ターにログインするための権利	
[O] OS	27	アクセス権	33
Operating Systemの略。パソコン を動かすための基本ソフトウェア		コンピューターやネットワーク、データベースなどを利用する権利	
[P] PDCA	106	アップデート	39
Plan（計画）、Do（実行）、Check（評 価）、Act（改善）の繰り返しで管理 業務を円滑に進める手法の一つ		ソフトウェアやアプリケーションを 最新の状態にすること	
[S] SECURITY ACTION	115	アプリ	38
		スマートフォンなどで、さまざまな 機能を提供するプログラム	
SNS	31,63	暗号化	27
		データの内容を他人には分からなく するための方法	
Society5.0	119,131	暗号化技術（SSL）	71
狩猟社会（Society 1.0）、農耕社会 (Society 2.0)、工業社会（Society 3.0）、情報社会（Society 4.0）に 続く、新たな社会を指すもの			
SPF	71	【い】 インシデント	21
		コンピューターやネットワークのセキ ュリティを脅かす事象。セキュリティ インシデントとも呼ぶ	
[U] URL	27	インターネットバンキング	5
URLとは、インターネット上に存在 する情報の位置を記述するためのデ ータ形式		コンピューターを使ってインターネッ ト経由で銀行などの金融機関のサー ビスを利用すること	
USBメモリー	32	【う】 ウィルス	6
Universal Serial Bus。パソコンな どに周辺機器を簡単に接続するため の記憶媒体			
UTM	59	【か】 可用性	64,80
		完全性	64,80
[W] Webアプリケーション	29		

【き】 機密性	64,80	スリープモード	83
共有サーバー	27	パソコン操作をしない間、省電力のため画面が暗くなる機能。第三者による操作やのぞき見防止にもなる	
情報や機能を共有で使用するサーバー			
共有設定	173		
プリンターやデータなどを複数人で共有できるよう設定すること			
【く】 クラウドサービス	178		
クリアスクリーン	82,83	【せ】 脆弱性	28
クリアデスク	82,83	セキュリティコード	151
【こ】 個人情報保護法	182,183	クレジットカード裏面に印字されている3桁の番号	
コンテンツ	35	セキュリティ・バイ・デザイン	108
WebサイトやDVD、CD-ROMに含まれる情報の内容		Security by Design：企画・設計段階から必要なセキュリティ対策を施しておくという考え方	
コンテンツフィルター	94	セキュリティホール	29
業務上不要または有害な内容を含むWebサイトへの接続を制限する機能		ソフトウェアの設計ミスなどによって生じたセキュリティ上の弱点	
【さ】 サイバー空間(仮想空間)	119	セキュリティポリシー	94,107
サイバーセキュリティ	21	センサー	120
残留リスク	99	音や光、温度、振動などを検出して信号に変える装置	
【し】 指紋認証	66		
指紋を利用する生体認証		【そ】 ソーシャルエンジニアリング	43
情報資産	64,81	social engineering：人間の心理的な隙や、行動のミスにつけ込んで、IT技術を使用せずに秘密情報を入手する方法	
情報セキュリティ	21	外付けハードディスク	27
【す】 スクリーンセーバー	83	パソコン本体にケーブルで接続するタイプのハードディスク装置	
パソコン操作をしない間、画面を図形や模様などで隠す機能		ソフトウェア	27
スタンダロン	85	コンピューターを動作させる命令や処理手順のまとめ	
スパムメール	72		
不特定多数に対して送信される広告や詐欺的な内容を主としたメール		【た】 第4次産業革命	119
		蒸気機関（第1次）、電気機器（第2次）、コンピュータ（第3次）に続くAI等の技術、デジタル情報を活用した産業構造の変革を示す	

多要素認証	43	バックアップ	27
サービス利用時の利用者の認証を、複数の要素を用いて行うもの		データの破損や損失に備えて複製を作成して保管すること	
【て】 定義ファイル	21	【ひ】 ビッグデータ	120,122
コンピューターウイルスの特徴を記録したファイル		標的型攻撃	24,73
テザリング	69	【ふ】 ファイアウォール	94
スマートフォンなどを経由してパソコンをインターネットに接続する方法		外部から送られてくる通信を制御・監視し安全を保持するための仕組み	
テレワーク	68,79	5G	119,122
ICT機器等を活用して、時間や場所の制約を受けずに、柔軟に働くことができる形態		5th Generation (第5世代移動通信システム)	
電子証明書	77	フィジカル空間（現実空間）	119,131
信頼できる第三者（認証局）が本人であることを証明するもの		フィッシング詐欺	36
【と】 回報メール	70	フィルタリング	51,78
同じ内容のメールを複数の人へ同時に送付すること		特定のWebサイトや迷惑メールなどを選別・閲覧制限する仕組み	
トロイの木馬	21	踏み台	7
正体を偽ってコンピューターへ侵入し、破壊活動を行うプログラム		外部の第三者に乗っ取られ、不正アクセスの中継地点や迷惑メールの発信源などに利用されてしまうこと	
【な】 なりすまし	42	プラス・セキュリティ人材	180
他人のIDとパスワードを使用し、その人のふりをして活動すること		本来の業務を担いながらITを利活用する中でセキュリティスキルも必要となる人材	
【ね】 ネットワークカメラ	46	【へ】 ベンチマーク	101
主にネットワーク上に設置されたカメラ。監視カメラなどに用いられる		比較のために用いる指標	
【は】 パターンファイル	21	【ほ】 ボットネットウイルス	21
定義ファイルと同じ		ボットはロボットの略。攻撃者が遠隔から操作して、別のコンピューターへの攻撃の踏み台にする。ボットネットは、外部からの指令で一斉に攻撃を行わせるネットワークのこと	
ハッキング	2	ポップアップ画面	37
他人のコンピューターや通信システムを不正な手段で勝手に操作したり、不正に機密情報を入手したりすること		Webページ上に、自動的に新しいウ	

【ま】 インドウが開いて表示される画面	40
【ま】 マイナンバー	145
住民票を有する個人に割り当てられた12桁の番号	
【ま】 マルウェア	21
Malicious software (悪意のあるソフトウェア) の略語。コンピューターの正常な利用を妨げたり、利用者やコンピューターに害を成す不正な動作を行うソフトウェアの総称	
【め】 メーリングリスト	117
あらかじめ登録した複数の人に同じメールを同時配信できる仕組み	
【め】 メールサーバー	74
メールの送受信を行うためのサーバーのこと	
【も】 モバイル端末	88
インターネットに接続できる携帯電話やタブレット端末などの通信機器	
【よ】 溶解処分	85
紙の重要な情報を主に水と機械で溶かして処分する方法。専門業者に依頼	
【ら】 ランサムウェア	27
【り】 リモート管理	29
離れた場所にあるコンピューターを通信回線などを通じて管理すること	
【ろ】 ログ	29
コンピューターなどの内部で起こった出来事についての情報を時系列に記録・蓄積したデータ	
【わ】 ワーム	21
自立的に動作する不正プログラムで、コンピューターに侵入し、破壊活動や別のコンピューターへの侵入などをを行う	
【わ】 ワンクリック詐欺	5
認証方法の1つで、ワンタイム (=1回) 限りで短時間のみ有効な“使い捨て” パスワードのこと	
【わ】 ワンタイムパスワード	5

中小企業向け サイバーセキュリティ対策の極意 Ver 2.0

令和3年3月発行

編集・発行 東京都産業労働局商工部経営支援課

新宿区西新宿二丁目8番1号

電話番号 03 (5320) 4770

印刷

印刷物規格表 第1類

印刷番号

協力

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)

※掲載の情報は令和3年2月現在のものです

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info