

TOP SECRET

INFORMATION

インフォメーション



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info




# 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のでは？と思ったら、次ページの緊急連絡先に連絡するに当たって、事前に次のような情報を整理しておきましょう。

- 
- ☐ 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
  - ☐ ウイ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



## 緊急連絡先

**警視庁 サイバー犯罪対策課 03-3431-8109**

受付時間：平日8:30-17:15

専門の警察官が、サイバー犯罪に関わる相談や情報提供を電話で受け付けています。

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

**独立行政法人 情報処理推進機構セキュリティセンター (IPA/ISEC)  
情報セキュリティ安心相談窓口**

**03-5978-7509 E-mail [anshin@ipa.go.jp](mailto:anshin@ipa.go.jp)**

受付時間：10:00-12:00 13:30-17:00 土日祝日・年末年始を除く  
ウイルスおよび不正アクセスの技術的な相談に対してアドバイスが受けられる、IPAの窓口です。

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



## ウイルスおよび不正アクセス被害の届け出

ウイルスを発見または感染した場合、あるいは不正アクセス被害に遭った場合、被害の拡大と再発防止に役立てるため、情報処理推進機構（IPA）では情報提供を受け付けています。それぞれ以下のサイトから届け出をしましょう。

### ウイルスに関する届け出

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

### 不正アクセスに関する届け出

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



やられる前に、  
しっかり予防を！



## サイバー攻撃から会社を守るための情報源

- ☑ ソフトウェアの脆弱性と対策情報を知りたい
- ☑ 情報流出、フィッシングサイト、不正侵入など被害を最小限に抑えたい
- ☑ 脅威発生状況の把握、手口の分析、再発防止のための助言が欲しい

**一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC)**

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

- ☑ インターネットを利用した金融犯罪や情報流出の情報が欲しい
- ☑ eコマースに対する脅威、ウイルスの脅威への対策を考えたい
- ☑ サイバー犯罪の被害が懸念される警戒情報を知りたい

**一般財団法人 日本サイバー犯罪対策センター (JC3)**

<https://www.jc3.or.jp/>

- ☑ さまざまなサイバー脅威情報、脆弱性情報、攻撃予兆情報を収集し共有したい
- ☑ 信頼できる企業同士で、お互いに問題解決したい

**日本シーサート協議会**

<http://www.nca.gr.jp/>

- ☑ フィッシングサイト、ワンクリック詐欺、クレジットカード不正使用などインターネット取引におけるトラブルの相談に乗ってほしい

**消費者庁 消費者ホットライン**

**188 (全国共通)**

[http://www.caa.go.jp/region/shohisha\\_hotline.html](http://www.caa.go.jp/region/shohisha_hotline.html)

☒ 迷惑メールに関して相談に乗ってほしい

☒ 迷惑メールの情報や特定電子メール法に基づく対策を知りたい

**一般財団法人 日本データ通信協会 (JADAC) 迷惑メール相談センター**  
**03-5974-0068**

<http://www.dekyo.or.jp/soudan/index.html>

☒ フィッシング詐欺情報と注意事項を知りたい

☒ フィッシングの動向分析・技術的対策・法的対策を知りたい

**フィッシング対策協議会**

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

☒ 「中小企業の情報セキュリティ対策ガイドライン」対応製品やサービスを知りたい

☒ マイナンバー対応について、あらゆる情報が欲しい

☒ 情報セキュリティに関する調査・研究情報が知りたい

☒ 情報セキュリティに関するセミナーやイベントに参加したい

**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**

<http://www.jnsa.org/>

☒ なりすましECサイト（電子商取引）の被害状況や対処法を知りたい

**一般社団法人 セーフアーインターネット協会 なりすましECサイト対策協議会**

<https://www.saferinternet.or.jp/narisumashi/>

☒ どうしたら脆弱性対策ができるのか知りたい

☒ ソフトウェア製品の脆弱性や対策情報を知りたい

☒ 必要な脆弱性対策情報を効率よく入手したい

**警察庁 サイバー犯罪対策プロジェクト 脆弱性の対策には**

[http://www.npa.go.jp/cyber/kanminboard/siryou/sec\\_hole/vuln\\_solution.html](http://www.npa.go.jp/cyber/kanminboard/siryou/sec_hole/vuln_solution.html)



CHECK

## 主な情報セキュリティベンダー

**株式会社アンラボ**（主な製品）AhnLab MDS<http://jp.ahnlab.com/site/main.do>**株式会社カスペルスキー**（主な製品）Kaspersky Endpoint Security for Business<http://www.kaspersky.co.jp/>**株式会社シマンテック**（主な製品）Symantec Endpoint Encryption<https://www.symantec.com/ja/jp/>**ソフォス株式会社**（主な製品）Endpoint Protection<https://www.sophos.com/ja-jp.aspx>**ソースネクスト株式会社**（主な製品）ZERO スーパーセキュリティ<http://www.sourcenext.com/>**トレンドマイクロ株式会社**（主な製品）ウイルスバスター ビジネスセキュリティサービス<http://jp.trendmicro.com/>**エフセキュア株式会社**（主な製品）プロテクション サービス ビジネス<https://www.f-secure.com/>**マカフィー株式会社**（主な製品）McAfee Endpoint Protection for SMB<http://www.mcafee.com/japan/>

情報処理推進機構（IPA）「主なワクチンベンダーのWebサイト等一覧」より

CHECK

## Tcyss相談窓口

(東京中小企業サイバーセキュリティ支援ネットワーク)

サイバー攻撃に遭った！

会社の情報が流出してしまった…

セキュリティ対策って、どうすればいい？

そんなときのために、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。

困ったら、まずはお電話を **03-5320-4773**※窓口での受付は **東京都産業労働局商工部内（都庁第一本庁舎30階北側）**※

※電話、窓口とも受付時間は都庁開庁日の9:00～12:00、13:00～17:00

Webサイトからは **東京都電子申請 中小企業サイバーセキュリティ対策相談**<http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/>

The image shows two screenshots from the Tokyo Metropolitan Government website. The top screenshot displays the 'Tcyss' (Tokyo Cyber Security Support Network) consultation window, which is a hub for small and medium-sized enterprises to receive support for cyber security. It includes a diagram of the support network and a list of services. The bottom screenshot shows the '東京都電子申請 中小企業サイバーセキュリティ対策相談' (Tokyo Metropolitan Government Online Application Small and Medium Enterprise Cyber Security Support Consultation) portal. This portal provides information on how to apply for support, including a list of services and a section for '電子申請と申請済み申請の概要' (Overview of Online Application and Application Status).



# 情報セキュリティ 5カ条



## 最低限のルール「情報セキュリティ5カ条」

情報セキュリティ対策に詳しくなくても、まずはここから！

### 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！

パスワードは英数字記号含めて10文字以上に！

名前、電話番号、誕生日、簡単な英単語などは使わない！

同じID・パスワードをいろいろなWebサービスで使い回さない！



### 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！





# 情報セキュリティ 用語解説

CHECK

## 個人情報

特定の個人を識別できる場合は全て「個人情報」という扱いを受けることになります。

たとえ姓（名字）だけでは誰かを特定できないとしても、その姓（名字）に「〇〇△会社に勤務」「東京都〇△区〇△町△番地在住」などのプロフィール情報が加われば、その人が誰であるかを特定できますので、個人情報となります。つまり、ほとんどの情報が個人情報だといっても過言ではありません。

CHECK

## 改正個人情報保護法

2015年9月に改正され、2017年5月30日に全面施行された「個人情報保護法」で、保有する個人情報が5,000人以下の中小企業も新たに「個人情報取扱事業者」と定められました。つまり、個人情報をベースに活動する者全てが同法の義務を負うことになったのです。

そのポイントをまとめると、次のようになります。

- ①身体的特徴も個人情報です。
- ②人種、信条、病歴など差別や偏見を生む可能性のある個人情報を取得するときは、必ず本人の同意を得なければなりません。
- ③個人情報を本人以外の第三者に渡すときは、あらかじめ本人の同意を得なければなりません（ただし、生命、身体、財産の保護が必要なときには不要）。
- ④個人情報データベースに含まれる個人情報を第三者に提供する場合も本人の同意を得なければなりません。さらに、個人情報保護委員会への届け出も必

要です。また、提供者は提供年月日や情報の受領者氏名などを記録し保存することも義務付けられています。

- ⑤特定の個人を識別できないように個人情報を加工し、そこから個人情報を復元できないようにしてビッグデータなどに利用することができるようになりました。



## プライバシーマーク



こんなマークを見たことはありませんか。

これはプライバシーマークといいます。

「個人情報」をルールや手続きに従って安全に取り扱い、管理することのできる会社だけが使うことができるマークです。

プライバシーマークを取得するためには、審査に合格する必要があります。審査では、その会社が「個人情報」をどのように取り扱い、管理しているかを審査されます※。

通信販売など大量の個人情報を取り扱う会社は、このマークを取得しましょう。

※ 基準はJIS Q 15001をベースとして、「個人情報保護法」「個人情報保護法に関するガイドライン」「地方自治体による個人情報関連の条例」「業界団体の個人情報関連のガイドライン」などを審査に取り入れています



## 不正競争防止法改正と営業秘密の保護強化

不正競争防止法は、公正な競争を妨げる行為を禁止し、適正な競争を活性化させて、公正な市場を守るための法律です。

同法は2015年に改正されましたが、ここで「営業秘密の保護強化」が図られました。

ポイントは次の通りです。

### ①処罰の対象が拡大

- ・営業秘密を不正に開示した者からその秘密を取得して開示した者、さらにそれを取得して開示した者というように、2次3次と不正に関わった者は、全て処罰されます。
- ・不正取得や不正開示が未遂だったとしても、処罰されます。
- ・他人の営業秘密を不正に使用して生産したり輸出入したりすると、処罰されます。
- ・海外のサーバーに保管された営業秘密を海外で不正使用しても、処罰されます。

### ②罰則の強化

- ・罰金刑の上限が引き上げられました。
- ・営業秘密侵害で得た犯罪収益は、裁判所の判断で没収されることもあります。

### ③民事救済の実効性を向上

- ・損害賠償請求の際、民事訴訟法上は原則原告が「侵害した者（被告）が違法に取得した技術を使った」ことを立証しなければなりませんが、この改正により被告がそれを実証することとし、原告の立証負担を軽減しました（立証責任の転換）。
- ・営業秘密の不正使用に対する差し止め請求の期間制限が10年から20年に延長されました。

## CHECK

## 外部委託契約とSLA (Service Level Agreement)

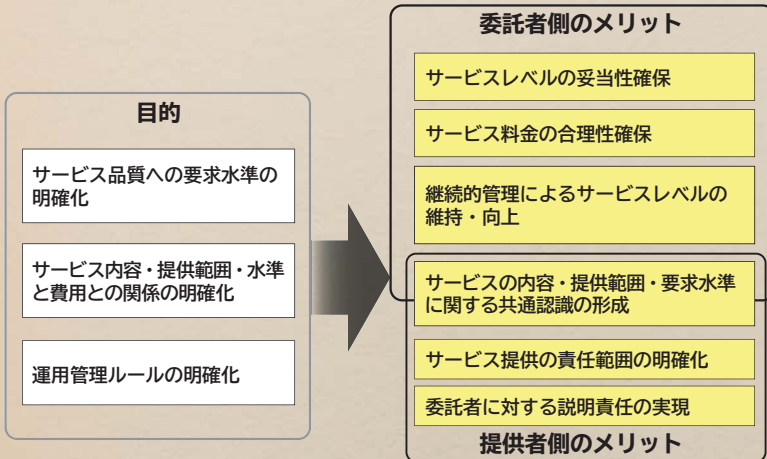
こんな経験や疑問はありませんか？

- ・サービスを委託したが、お互いに食い違いが生じてトラブルになった。
- ・委託されたサービスの品質と費用が見合っているのか不明瞭。
- ・人材コストが上がり、サービスの提供が続けられるか不安。

サービスの委託者と提供者との間で役割分担や責任の所在があいまいなままだったり、委託業務の量的変化や人材コストの変化などが影響するサービス提供の継続性について、あらかじめ契約に明示されていなかったりすると、双方にトラブルが生じます。

このような問題を解消するために、①サービス品質への要求水準の明確化②サービス内容・提供範囲・水準と費用との関係の明確化③運用管理ルールの明確化を図り、文書化します。それがSLAです。

これにより、以下のように委託者・提供者双方にメリットが生じます。



「情報システムに係る政府調達への SLA導入ガイドライン」(経済産業省) より





## マイナンバーのセキュリティ考慮事項

事業者は従業員の源泉徴収票作成時にマイナンバーを取り扱いますが、マイナンバーを含む個人情報（「特定個人情報」といいます）は、個人情報保護法とは取り扱いが異なり、さらに厳格に保護されなければならないので、要注意です。

マイナンバーはマイナンバー法でルールが定められています。次のポイントを守ってください。

### 1 社員番号への使用は禁止

マイナンバーはマイナンバー法で規定された社会保障、税、災害対策に関する事務以外に使用できません。たとえ本人の同意があったとしても、社員番号に使うというようなことはできません。

### 2 漏えい防止対策を確実に

漏えいを防止するためマイナンバーの保管は厳重に行ってください。

もし、税理士や社会保険労務士などに外部委託する場合には、①委託先との契約には秘密保持義務や情報の持ち出し禁止などを盛り込み、適切に監督すること②再委託をする場合は委託元の許諾を得ること③不正アクセスを防止する対策を取ることが求められます。

### 3 不要になったら即廃棄

マイナンバー法で規定された場合を除き、特定個人情報を収集または保管してはいけません。

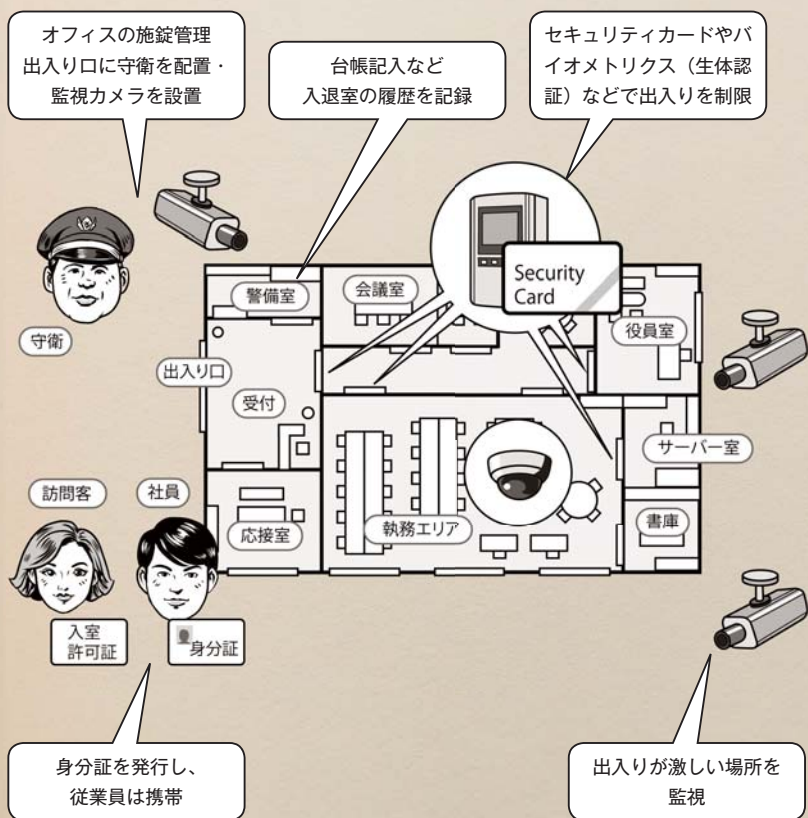
不要になったら、マイナンバーをできるだけ速やかに廃棄するか削除しなければなりません。

ただし、マイナンバーを復元できない程度にマスキングしたり削除したりした上で、他の個人情報の保管を継続することはできます。

CHECK

## 物理（環境）的セキュリティ

企業には正社員のほか派遣社員、アルバイト、パートなどの従業員、さらにはさまざまな訪問客がオフィスを出入りします。そのため、オフィスへの入退管理を強化し、容易に情報や情報機器に触れられることのないような対策が必要です。以下の図のような、オフィスの施錠管理や入退室管理、監視カメラの設置といった対策が物理（環境）的セキュリティです。





# セキュリティ お役立ちリンク

情報処理推進機構 (IPA) 情報セキュリティ	<a href="http://www.ipa.go.jp/security/index.html">http://www.ipa.go.jp/security/index.html</a>
脆弱性対策	<a href="http://www.ipa.go.jp/security/vuln/index.html">http://www.ipa.go.jp/security/vuln/index.html</a>
情報セキュリティ対策	<a href="http://www.ipa.go.jp/security/measures/index.html">http://www.ipa.go.jp/security/measures/index.html</a>
情報セキュリティ啓発	<a href="http://www.ipa.go.jp/security/keihatsu/features.html">http://www.ipa.go.jp/security/keihatsu/features.html</a>
届け出・相談・情報提供	<a href="http://www.ipa.go.jp/security/outline/todoke-top-j.html">http://www.ipa.go.jp/security/outline/todoke-top-j.html</a>
JPCERT コーディネーション センター (JPCERT/CC)	<a href="https://www.jpcert.or.jp/">https://www.jpcert.or.jp/</a>
緊急情報を確認する	<a href="https://www.jpcert.or.jp/menu_alertsandadvisories.html">https://www.jpcert.or.jp/menu_alertsandadvisories.html</a>
JPCERT/CCに依頼する	<a href="https://www.jpcert.or.jp/menu_reporttojpcert.html">https://www.jpcert.or.jp/menu_reporttojpcert.html</a>
公開資料を見る	<a href="http://www.jpcert.or.jp/menu_documents.html">http://www.jpcert.or.jp/menu_documents.html</a>
JVN脆弱性対策情報データベース MyJVNバージョンチェッカ	<a href="http://jvndb.jvn.jp/apis/myjvn/#VCCHECK">http://jvndb.jvn.jp/apis/myjvn/#VCCHECK</a>
警視庁 情報セキュリティ広場	<a href="http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html">http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html</a>
注目情報	<a href="http://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/index.html">http://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/index.html</a>
セキュリティ対策	<a href="http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/index.html">http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/index.html</a>
インターネット上における 犯罪に関する情報提供	<a href="http://www.keishicho.metro.tokyo.jp/kurashi/cyber/Internet_crime.html">http://www.keishicho.metro.tokyo.jp/kurashi/cyber/Internet_crime.html</a>
サイバー犯罪に関する情報提供	<a href="https://www.keishicho.metro.tokyo.jp/anket/jiken_cyber.html">https://www.keishicho.metro.tokyo.jp/anket/jiken_cyber.html</a>

警察庁 サイバー犯罪 対策プロジェクト 官民ボード	<a href="http://www.npa.go.jp/cyber/kanminboard/seikabutsu.html">http://www.npa.go.jp/cyber/kanminboard/seikabutsu.html</a>
内閣サイバーセキュリティセンター	<a href="https://www.nisc.go.jp/security-site/office/index.html">https://www.nisc.go.jp/security-site/office/index.html</a>
総務省 国民のための 情報セキュリティサイト	<a href="http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/">http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/</a>
国民生活センター インターネットトラブル	<a href="http://www.kokusen.go.jp/topics/internet.html">http://www.kokusen.go.jp/topics/internet.html</a>
東京くらしWEB 架空請求対策 (STOP! 架空請求!)	<a href="http://www.shouhiseikatu.metro.tokyo.jp/torihiki/taisaku/">http://www.shouhiseikatu.metro.tokyo.jp/torihiki/taisaku/</a>
日本サイバー犯罪対策センター (JC3) 情報提供	<a href="https://www.jc3.or.jp/info/index.html">https://www.jc3.or.jp/info/index.html</a>
日本産業協会 迷惑メール情報提供	<a href="http://www.nissankyo.or.jp/spam/index.html">http://www.nissankyo.or.jp/spam/index.html</a>
日本データ通信協会 迷惑メール相談センター	<a href="http://www.dekyo.or.jp/soudan/index.html">http://www.dekyo.or.jp/soudan/index.html</a>
インターネットホットライン 連絡協議会	<a href="http://www.iajapan.org/hotline/">http://www.iajapan.org/hotline/</a>
JNSAソリューションガイド	<a href="http://www.jnsa.org/JNSASolutionGuide/IndexAction.do">http://www.jnsa.org/JNSASolutionGuide/IndexAction.do</a>
ここからセキュリティ!	<a href="http://www.ipa.go.jp/security/kokokara/">http://www.ipa.go.jp/security/kokokara/</a>
インターネットを楽しむために	<a href="https://www.jaipa.or.jp/elt/">https://www.jaipa.or.jp/elt/</a>
個人情報保護委員会 中小企業サポートページ (個人情報保護法)	<a href="https://www.ppc.go.jp/personal/chusho_support/">https://www.ppc.go.jp/personal/chusho_support/</a>
日本ネットワークセキュリティ協会 マイナンバー対応のための 情報ポータル (企業向け)	<a href="http://www.jnsa.org/mynumber/index.html">http://www.jnsa.org/mynumber/index.html</a>



# 情報セキュリティポリシー サンプル



## わが社の情報セキュリティポリシーを策定する

情報処理推進機構（IPA）のWebサイト（<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>）から「中小企業の情報セキュリティ対策ガイドライン」付録3のツールをダウンロードし、以下の手順に沿って自社に合った情報セキュリティポリシーを策定してみましょう。

### 1 情報資産管理台帳を作成します

- (1) <ツールA> リスク分析シート内の「情報資産管理台帳」シートに、社員名簿や給与データなど自社で保有している情報を記入例に従って入力します。
- (2) それぞれの情報について機密性や完全性などの評価値を決めると、重要度が判定されます。

### 2 リスク値を算定します

- (1) <ツールA> 内の「脅威の状況」シートで、書類やパソコンなど保存先ごとに想定される脅威を指定すると、「情報資産管理台帳」に反映されます。
- (2) 「対策状況チェック」シートで、組織的セキュリティ対策やマイナンバー対応などの対策状況を指定します。情報資産ごとのリスク値が自動計算され、脆弱性と被害発生の可能性が「情報資産管理台帳」に反映されます。

### 3 情報セキュリティ対策を決定します

これまでの判定結果が<ツールA>内の「診断結果」シートに反映されます。そこに自社で策定すべく情報セキュリティポリシーが表示されます。



## 4 情報セキュリティポリシーを策定します

- (1) <ツールA>内の「診断結果」シートに表示された情報セキュリティポリシーを<ツールB>情報セキュリティポリシーサンプル（下表）の中から選択します。
- (2) 自社の状況に合わせて項目を追加するなど、自社専用の情報セキュリティポリシーを編集します。

### <ツールB>「情報セキュリティポリシーサンプル」表紙より

本ツールは、中小企業向けの情報セキュリティポリシーのサンプルです。ツールAの結果をもとに自社に必要なサンプルを選択し、自社で実施する対策に編集することで自社の情報セキュリティポリシーを作成することができます。

※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えて下さい。

※青字箇所は、自社の事情に応じた文言を選択して下さい。

### 目 次

1	組織的対策（基本方針）	2ページ
	組織的対策	5ページ
2	人的対策	7ページ
3	情報資産管理	9ページ
4	マイナンバー対応	12ページ
5	アクセス制御及び認証	21ページ
6	物理的対策	24ページ
7	IT機器利用	26ページ
8	IT基盤運用管理	34ページ
9	システム開発及び保守	38ページ
10	外部委託管理	40ページ
11	情報セキュリティインシデント対応ならびに事業継続管理	42ページ
12	社内体制図	47ページ
13	委託契約書機密保持条項サンプル	48ページ

以下はサンプル項目のうちの1つです。

必要に応じて項目を追加したり文言を追加したりすれば、自社に合ったオリジナルの情報セキュリティポリシーが完成します。

5	アクセス制御及び認証	改訂日	20yy.mm.dd
適用範囲	情報資産の利用者及び情報処理施設		
1. アクセス制御方針			
社外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。対象となるシステム等は「9.1 アクセス制御対象情報システム及びアクセス制御方法」に記載する。			
●「情報資産管理台帳」の利用者範囲に基づき、利用者の業務・職務に応じた必要最低限のアクセス権を付与する。			
●特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、複数名に分散してアクセス権を付与する。			
2. 利用者の認証			
社外秘又は極秘の情報資産を扱う社内情報システムは、以下の方針に基づいて利用者の認証を行う。認証方法等は「9.2 利用者認証方法」を参照のこと。			
●利用者の認証に用いるアカウントは、利用者1名につき1つを発行する。			
●複数の利用者が共有するアカウントの発行を禁止する。			
3. 利用者アカウントの登録			
利用者の認証に用いるアカウントは、代表取締役又は情報セキュリティ責任者の承認に基づき登録する。アカウント名の設定条件は「9.3 利用者アカウント・パスワードの条件」を参照のこと。			
4. 利用者アカウントの管理			
利用者の認証に用いるアカウントが不要になった場合、システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌日までに実施する。			
5. パスワードの設定			
利用者の認証に用いるパスワードは、以下に注意して設定する。パスワードの設定条件は、「9.3 利用者アカウント・パスワードの条件」を参照のこと。			
●十分な強度のあるパスワードを用いる。			
●他者に知られないようにする。			
6. 従業員以外の者に対する利用者アカウントの発行			
当社の取締役又は従業員以外の者にアカウントを発行する場合は、代表取締役又は情報セキ			

文中の赤字の部分  
を自社の事情  
に応じた内容に  
書き換えます。

6	物理的対策	改訂日	20yy.mm.dd
---	-------	-----	------------

適用範囲	情報処理設備が設置される領域
------	----------------

## 1. セキュリティ領域の設定

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。

レベル1 領域	本社受付・応接スペース・商談室・倉庫
利用者	従業員、社外関係者、部外者が立ち入り可
施錠	最終退室者による施錠
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード
制限事項	未使用時に社外秘又は極秘の情報資産の放置禁止
部外者管理	従業員の許可を受けて入室可能
管理記録	—
侵入検知	—
来客用名札	着用不要
火災対策	火災検知器、消火器設置

レベル2 領域	本社執務室・社長室・書庫・工場・営業所
利用者	従業員以外の入室は従業員の許可又はエスコートが必要
施錠	最終退室者による施錠及び警備会社への通報装置作動
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード、パソコン、複合機、電話機
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止
部外者管理	従業員/受付守衛/総務部受付の許可を受けて入室可能
管理記録	入退室を紙や様式に記録
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	スプリンクラー、消火器設置

文中の青字の部分は自社の事情に応じた文言を選択します。

レベル3 領域	サーバールーム
利用者	予め登録された者
施錠	常時施錠及び警備会社への通報装置作動、鍵の管理責任者

# 情報管理が不適切な場合の処罰など

情報の種類	根拠法による規定		処罰など
個人情報 (マイナンバーを含む)	個人情報保護法	1) 虚偽申告・命令違反	6カ月以下の懲役または30万円以下の罰金、業務停止命令
		2) データベース提供罪	1年以下の懲役または50万円以下の罰金
	民法（不法行為による損害賠償、709条）		損害賠償
	建設業法		役員または使用人が懲役刑に処せられた場合は営業停止処分
	マイナンバー法（個人および法人に対して）		秘密を漏らし、または盗用した者は、3年以下の懲役もしくは150万円以下の罰金 行為者を雇用する法人に対しても罰金
他社から預かった秘密情報 (外部非公開のデータなど)	不正競争防止法の営業秘密不正取得・利用行為など		損害賠償、信頼回復措置
自社の秘密情報 (非公開のノウハウなど)	不正競争防止法の営業秘密不正取得・利用行為など		善管注意義務違反に対する関係者からの損害賠償請求（経営者に対する民事訴訟）
上場会社の株価に影響を与える可能性のある重要な未公開の内部情報	金融商品取引法		内部情報をもとに取引が行われた場合、罰金または課徴金の可能性

「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2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	NISC
	情報セキュリティ5カ条	IPA
	インシデント対応マニュアルの作成について	JPCERT/CC
	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	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
サイバー攻撃について	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
	情報管理はマネーです	JIPDEC
	情報セキュリティ10大脅威 2017	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 2017	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
	IPA 対策のしおり(3) ボット対策のしおり	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
	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	IPA
	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	JPCERT/CC NISC
	「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 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	IPA
	情報セキュリティポリシーサンプル	IPA
	情報セキュリティ自己診断チェックリスト	NISC
	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	IPA
IoT対策	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.3～	IPA
	IoT セキュリティガイドライン	経済産業省
	IoT、AI、ロボットに関する経済産業省の施策について	経済産業省
	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
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	2016年版中小企業白書 平成28年版情報通信白書 IT人材白書2017 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 112,116  
 Android 32  
 スマートフォン用のOSの1つ
- [D]** DDoS攻撃 15  
 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
- DoS攻撃 15  
 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する攻撃
- [E]** ECサイト/eコマース 166  
 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
- [I]** ICカード 58  
 集積回路 (IC) が付いた本人認証用のカード
- ID 23  
 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 40,112,114,118,120
- IPアドレス 66  
 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 80  
 Information Technologyの略で情報技術の総称
- [N]** NAS 171  
 Network Attached Storageの略でネットワークに接続された記憶装置
- [O]** OS 21  
 Operating Systemの略。パソコンを動かすための基本ソフトウェア
- [P]** PDCA 98  
 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1つ
- [U]** URL 21  
 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
- USBメモリー 26  
 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 51
- [W]** Webアプリケーション 23
- Webサーバー 22  
 ホームページや情報・機能を提供するコンピューター
- Webサービス 23  
 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
- [あ]** アカウント 29  
 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
- アクセス権 27

INDEX  
Mission 1  
Mission 2  
Mission 3  
Mission 4  
info

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

アップデート 33  
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

アプリ 32  
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

暗号化 20  
データの内容を他人には分からなくするための方法

暗号化技術 (SSL) 69

**【い】** インシデント 15  
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

インターネットバンキング 5  
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

**【う】** ウイルス 6  
コンピューターの正常な利用を妨げることを目的として作成されたプログラム。厳密には他のプログラムに寄生し、そのプログラムに便乗して悪質な処理を実行に移すもの

**【か】** 株主代表訴訟 9  
株主が会社を代表して取締役・監査役などの役員に対して法的責任を追及するために提起する訴訟

可用性 56,72

完全性 56,72

**【き】** 機密性 56,72  
共有サーバー 21

情報や機能を共有で使用するサーバー

共有設定 171

プリンターやデータなどを複数人で共有できるように設定すること

**【く】** クラウドサービス 122

クリアスクリーン 74,75

クリアデスク 74,75

**【け】** 掲示板サイト 25  
記事を書き込んだり、閲覧したり、コメント（レス）を付けられる電子掲示板の機能を提供しているサイト

**【こ】** 個人情報保護法 85,172  
コンテンツ 29  
WebサイトやDVD、CD-ROMに含まれる情報の内容

コンテンツフィルター 86  
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

**【さ】** サイバー 表紙  
コンピューターやネットワークの中に広がる仮想空間のこと

サイバーセキュリティ 15

残留リスク 91

**【し】** 指紋認証 58  
指紋を利用する生体認証

情報資産 56

情報セキュリティ 15

**【す】** スクリーンセーバー 75  
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

スタンドアロン 77

- スパムメール** 64  
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
- スリープモード** 75  
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
- 【せ】脆弱性** 23  
ぜいじやくせい
- セキュリティコード** 153  
クレジットカード裏面に印字されている3桁の番号
- セキュリティホール** 23  
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
- セキュリティポリシー** 86,99
- センサー** 113  
音や光、温度、振動などを検出して信号に変える装置
- 【そ】外付けハードディスク** 21  
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
- ソフトウェア** 21  
コンピューターを動作させる命令や処理手順のまとめ
- 【た】多要素認証** 37  
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
- 【て】定義ファイル** 15  
コンピューターウイルスの特徴を記録したファイル
- テザリング** 61  
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
- 電子証明書** 69
- 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
- 【と】同報メール** 63  
同じ内容のメールを複数の人へ同時に送付すること
- トロイの木馬** 15  
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
- 【な】なりすまし** 36  
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
- 【に】2段階認証** 55  
2つの方法を使って、本人であることを認証する
- 【ね】ネットワークカメラ** 40  
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
- 【は】バイオメトリクス** 177  
指紋や網膜など個人の身体的特徴を用いて行う生体認証
- パターンファイル** 15  
定義ファイルと同じ
- ハッキング** 2  
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
- バックアップ** 21  
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
- 【ひ】ビッグデータ** 112,114
- ビットコイン** 25  
サイバー空間で日常生活に使えることを目指して作られた仮想通貨

## 標的型攻撃 18,64

### 【ふ】 ファイアウォール 86

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

### フィッシング詐欺 30

### フィルタリング 70

特定のWebサイトや迷惑メールなどを選別・閲覧制限したりする仕組み

### 踏み台 7

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

### 【へ】 ベンチマーク 93

比較のために用いる指標

### 【ほ】 ボットネットウイルス 15

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

### ポップアップ画面 31

Webページ上に、自動的に新しいウインドウが開いて表示される画面

### 【ま】 マイナンバー 176

住民票を有する個人に割り当てられた12桁の番号

### マルウェア 15

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 109

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

## メールサーバー 66

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 80

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 77

紙の重要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 20

### 【り】 リモート管理 23

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 23

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 15

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行う

### ワンクリック詐欺 34

### ワンタイムパスワード 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



# MEMO

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

## 中小企業向け サイバーセキュリティ対策の極意

平成29年11月発行

編集・発行 東京都産業労働局商工部調整課

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 (29) 17
--------------

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)

※掲載の情報は平成29年8月現在のものです。

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

Info