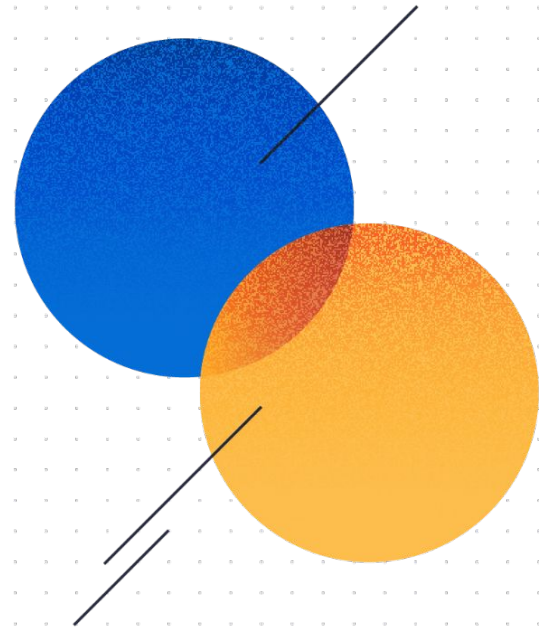


# 手元に置いておけば安心！ セキュリティに関連する法律まとめ



01: サイバーセキュリティにおける法律の近年の動き

02: サイバーセキュリティ全般の法律概要

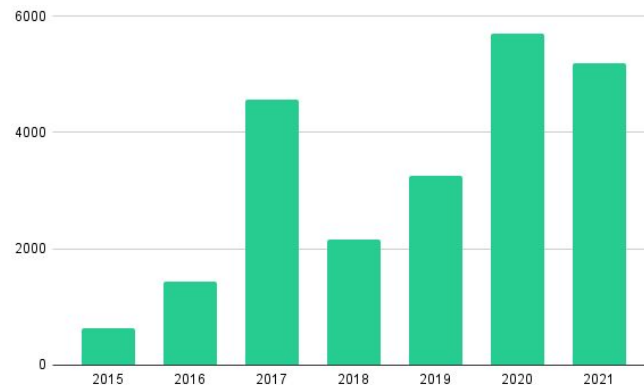


01

# サイバーセキュリティにおける法律 の近年の動き

日本におけるサイバー攻撃関連の通信数は、2015年の632億パケットから、2021年には5180億パケットと、この6年間で8.2倍に増加しています。

\*出典: NICT「[NICTER観測レポート2021](#)」を基に作成



- サイバー攻撃の脅威の高まりに対応して、日本政府はサイバー犯罪に対応する新しい法律を随時施行しています
- 法律には、明確な悪意がある場合にのみ適用される法律以外に、顧客向けメール配信など、意図せずに違反するリスクがある法律もあります。以下では、特に理解しておくべきサイバーセキュリティ関連の法律を紹介します

02

# サイバーセキュリティ全般の 法律概要

情報セキュリティに関する問題や犯罪増加に対応し、下記の法律が施行されています。

法律名	施行年	概要	罰則
サイバーセキュリティ基本法	2015年	サイバーセキュリティ基本法は、幅広い情報やデータを保護対象とし、機密性/完全性/可用性を脅かす攻撃への規制を定めます。	<ul style="list-style-type: none"><li>1年以下の懲役又は50万円以下の罰金</li></ul>
刑法	1908年	刑法は、犯罪に該当する行為と罰則について規定した法律です。時代に合わせ、サイバー犯罪に対応した罰則が追加されました。	<ul style="list-style-type: none"><li>適用される罪状により異なる 最長で10年以下の懲役</li></ul>
不正アクセス禁止法 (不正アクセス行為の禁止等に関する法律)	2000年	不正アクセス禁止法は、不正アクセス行為そのものに加えて、セキュリティ情報自体の不正取得、保管を規制しています。	<ul style="list-style-type: none"><li>3年以下の懲役又は100万円の罰金</li></ul>
特定電子メール法 (特定電子メールの送信の適正化等に関する法律)	2002年	特定電子メール法は、「営業/広告/宣伝目的の電子メール＝特定電子メール」から、メール利用者の保護を目的とする法律です。	<ul style="list-style-type: none"><li>1年以下の懲役又は100万円以下の罰金</li><li>法人の場合、法人にも3000万円以下の罰金</li></ul>
個人情報保護法 (個人情報の保護に関する法律)	2005年	個人情報保護法は、特定個人を識別できる情報保護が目的の法律です。2022年の改正では、個人情報漏えい時の個人情報保護委員会への報告、漏えいした本人への通知が義務化されました。	<ul style="list-style-type: none"><li>(法人) 1億円以下の罰金</li><li>(法人以外) 1年以下の懲役又は50万円以下の罰金</li></ul>
マイナンバー法 (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)	2015年	マイナンバー法は、行政サービス効率化のため、国民・法人に12桁の番号割り当て、ならびに特定個人情報(マイナンバーをその内容に含む個人情報)の保護管理に関して規定しています。	<ul style="list-style-type: none"><li>4年以下の懲役又は200万円以下の罰金、あるいは両方</li></ul>



## 法律の概要

サイバーセキュリティ基本法は、**サイバーセキュリティに関する施策推進を目的**として、施行された法律で、幅広い情報やデータを保護の対象となる

## 法律を理解するポイント

- サイバーセキュリティ向上のために国、地方自治体、事業者などに、サイバーセキュリティ体制整備を求めている
- 特に、重要インフラ事業者の該当業種は、具体的な行動計画が公表されている
- 罰則は、特定機関で働く公務員または事務委託者に対してのみ規定

## 罰則規定

- 国の「サイバーセキュリティ協議会」に所属する / していた人、または「サイバーセキュリティ戦略本部」から事務委託を受けた人が正当な理由なく秘密漏えい、盗用した場合、1年以下の懲役又は50万円以下の罰金

## 対策

- [「サイバーセキュリティ関連法令 Q&Aハンドブック」](#)をダウンロードし、自社が対応必要な項目について、対応が完了しているかどうかを確認する
- 特定インフラ事業者に該当する事業者は、[「重要インフラのサイバーセキュリティに係る行動計画」](#)を確認する



### 法律の概要

刑法とは、犯罪に該当する行為と罰則について規定した法律で、**サイバー犯罪の増加に伴い、新たな罰則が随時追加**されている。

### 法律を理解するポイント

- 「データの改ざん」「コンピュータウイルス」「ハッキング」「詐欺」など、多くのサイバー犯罪に関する罰則が規定されている
- 「名誉毀損」は、悪意なく該当する可能性があるため、特に対外的にコミュニケーションをとる担当者は注意が必要。

### 罰則規定

- 「電磁的記録不正作出及び供用罪」「不正指令電磁的記録作成等」「不正指令電磁的記録取得等」「電子計算機損壊等業務妨害」「電子計算機使用詐欺罪」「名誉毀損」が該当する
- 犯した罪により異なり、最長で10年以下の懲役

### 対策

- 「データの改ざん」「コンピュータウイルス」「ハッキング」「詐欺」といったサイバー攻撃を防御するための対策を講じる
- 従業員が悪意なく「名誉毀損」することがないように、対外的にメッセージを伝える立場の従業員に対して、コミュニケーショントレーニングを実施する





法律の概要	不正アクセス禁止法は、不正アクセス行為そのものに加えて、セキュリティ情報自体の不正取得、保管を規制される。
法律を理解するポイント	<ul style="list-style-type: none"><li>「電子計算機への不正アクセス」「セキュリティ情報自体を不正に取得すること」「不正アクセスを助長する行為」「不正アクセスするための情報を保管する行為」が処罰対象</li><li>故意犯のみが処罰対象であり、過失犯、未遂犯は罰則対象ではない</li></ul>
罰則規定	<ul style="list-style-type: none"><li>最高で、3年以下の懲役又は100万円以下の罰金</li></ul>
対策	<ul style="list-style-type: none"><li>自社が運用/利用するシステム、サービス、Webサイト、コミュニケーションツールを守るため、<a href="#">「国民のためのサイバーセキュリティサイト(不正アクセスによる被害と対策)」</a>を参考に、セキュリティ診断、対策を講じる</li></ul>



法律の概要	「営業・広告・宣伝目的の電子メール＝特定電子メール」から、メール利用者を保護するための法律であり、 <b>組織のマーケティング活動において注意が必要</b> となる。
法律を理解するポイント	<ul style="list-style-type: none"><li>● 送信前のオプトイン(送信同意)の取得が必要。またオプトアウト(送信禁止)の場合は、直ちにメール送信を停止せねばならない</li><li>● 違反行為として「受信者の事前同意ないメール送信」「表示義務事項の遵守」「送信者情報の偽装禁止」「送信拒否者への送信禁止」など定められている</li></ul>
罰則規定	<ul style="list-style-type: none"><li>● 最高で、1年以下の懲役又は100万円以下の罰金</li><li>● 法人の場合、上記に加えて3000万円以下の罰金</li></ul>
対策	<ul style="list-style-type: none"><li>● <a href="#">「特定電子メールの送信等に関するガイドライン」</a>を確認し、法律の趣旨を正しく理解したうえでメール配信を行うように務める</li><li>● 現場の従業員が勝手にメール送信を行った結果、法律に違反することのないように指導、注意喚起を行う</li></ul>



法律の概要	個人情報保護法は、 <b>特定個人を識別できる情報の保護を目的</b> とした法律。2022年の改正で、個人情報漏えい時の個人情報保護委員会への報告・本人通知が義務化
法律を理解するポイント	<ul style="list-style-type: none"><li>● 保護対象は、[1]個人情報(生存する個人の識別情報)、[2]個人データ(検索可能となった個人データ)、[3]保有個人データ(6ヶ月超保有の個人データで、開示/訂正/消去権限を持つもの)に分類される</li><li>● 個人情報漏えい事故を知ってから3-5日以内に速報、30日以内に個人情報保護委員会に行く義務がある(不正アクセス等調査が必要なものは60日以内報告)</li><li>● これ以外に「個人情報開示請求への対応義務」「個人情報の安全管理措置の公表義務」など、組織として多くの対応が必要となる</li></ul>
罰則規定	<ul style="list-style-type: none"><li>● (法人) 最高で1億円以下の罰金</li><li>● (法人以外) 最高で1年以下の懲役又は50万円以下の罰金</li></ul>
対策	<ul style="list-style-type: none"><li>● <a href="#">「個人情報取扱事業者等に係るガイドライン・Q&amp;A等」</a>を参照に、漏えいを防ぐための対策、個人情報利用時に問題が生じないための対策を行う</li></ul>



法律の概要	マイナンバー法は、日本国民に 12桁の番号を割り当て、 <b>特定個人情報(マイナンバーを含む個人情報)の保護管理に関して規定</b> する
法律を理解するポイント	<ul style="list-style-type: none"><li>● マイナンバーを保持する組織は、4つの安全管理措置が定められている<ul style="list-style-type: none"><li>○ 組織的安全管理措置(組織体制の整備)</li><li>○ 人的安全管理措置(取扱者の教育、監督)</li><li>○ 物理的安全管理措置(取扱担当者のみ操作できる体制整備)</li><li>○ 技術的安全管理措置(アクセス制限、サイバー攻撃対策)</li></ul></li><li>● 「<b>正当な理由なく特定個人情報ファイルを提供</b>」「<b>不正な利益を得る目的でマイナンバーを提供、盗用</b>」などの場合に罰則規定がある</li></ul>
罰則規定	<ul style="list-style-type: none"><li>● 最高で4年以下の懲役又は200万円以下の罰金、あるいは両方</li></ul>
対策	<ul style="list-style-type: none"><li>● <u><a href="#">「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」</a></u>を参照に、具体的な対策を検討・導入する</li></ul>

- ▶ サイバーセキュリティについては、政府としても重要項目として認識して、法整備を進められています。
- ▶ 法律の整備は進められている状況ですが、あくまで守る主体は各企業に一任されています。
- ▶ 攻撃者に対して罰則があるのは当然ですが、間接的な加害者になってしまうケースもあります。

次ページで紹介する、スリーシェイクが提供している「SecurifyScan」を利用することで、ツールによる脆弱性診断で可視化し、脆弱性の対策を行うことで攻撃者から情報資産を守り、ユーザを間接的な加害者にせず守ることができますので、ぜひお試しください。

## Webアプリケーションの 継続的セキュリティを簡単に実現



Securify Scan(セキュリファイ スキャン)は自社のプロダクトに対して、**手軽に、何度でも脆弱性診断の実施を可能にし、セキュリティレベルを可視化DevSecOps**への取り組みをサポートします。

▶ **まずは2週間の無料トライアルでお試しいただけます！**



Thank you.

