サイバーセキュリティ 2019.9.3

サイバーセキュリティ基本法で押さえておくべきポイント

この記事をシェア

日本のサイバーセキュリティに関する施策に関し、基本理念を定めるサイバーセキュリティ基本法。本法律は、2014年に制定され、国際情勢やICTの進化に応じて改正が続いている。我が国のサイバーセキュリティ対策の根幹をなす法律であり、世界規模化しているサイバーセキュリティ対策を推進していくために重要な役割を果たすと期待されている。2020年には東京オリンピックを控え、AIやIoTといった次世代を担うIT技術が急速に進化するなど、サイバーセキュリティ基本法の重要度は今後一層高まっていく。本記事では、企業がセキュリティ対策を推進する上で、押さえておきたいサイバーセキュリティ基本法のポイントについて解説する。

サイバーセキュリティ基本法制定の経緯

新着記事 NEW

2019.9.3 特集
サイバーセキュリティ基本法で押さえておくべきポイント

2019.9.2 ニュース
東京メトロをかたるフィッシングについての注意喚起

2019.8.29 特集
サイバー犯罪者がスマートビルを狙う理由

アクセスランキング

1 スマートフォンのデータを完全に削除するにはどうしたらいいですか

2 スマートフォンがマルウェア感染した場合の5つの兆候

3 ブラウザーに潜伏して悪さをするアドウェアとは？

4 無線LANルーターのSSIDはステルスにした方が良いのでしょうか？

5 スマホへの買い替えでデータ移行と旧端末の処分はどうすべき？

6 ブラウザーが乗っ取られ、変な検索エンジンが表示されます。削除しても表示されます。どうしたらいい？

7 Androidスマートフォンの顔認証、写真でも突破できる！？

8 スマートテレビはどこが危険なのか

9 Wi-Fiのセキュリティはなぜ WEPでは駄目なのか

2014年11月、サイバーセキュリティ基本法が可決・成立し、翌年1月に施行された。本法では、日本の情報セキュリティ対策として中心的な役割を担う、「サイバーセキュリティ戦略本部」を内閣に設置することを定めた。もともと、日本では、官公庁を横串で跨ぐような組織や戦略は存在しなかった。各省庁間の縦割りによるセキュリティ対策では限界があることは、2000年1月に発生した中央省庁のウェブサイト連続改ざんで露呈。さらに翌年の米国における同時多発テロやインターネットの急速な進化といった社会情勢の変化もあり、2005年には「内閣官房情報セキュリティ対策推進室」を前身に、「内閣官房情報セキュリティセンター（以降、旧NISC）」が政府部内に創設され、内閣官房長官を議長にした「情報セキュリティ対策会議」も設置された。

旧NISCは、情報セキュリティ政策に関する基本戦略の策定や、重要インフラに関する情報セキュリティ対策の官民連携を推進するなど、国の情報セキュリティ対策を実行に移す中で重要な役割を担ってきた。しかし、官公庁のウェブサイト改ざんが起こるなど政府機関などへの攻撃も激化。サイバーセキュリティ攻撃の手法は多様化するとともに、その規模も世界規模に拡大してきた。2013年には東京オリンピック開催が決定し、サイバーセキュリティにかかる国家戦略を策定・推進するための、司令塔機能の強化や体制整備が急務となってきたのだ。こうした中、「情報セキュリティ対策会議」で立案された情報セキュリティ基本計画やサイバーセキュリティ戦略という前段階を経て、サイバーセキュリティ基本法が設立されるに至った。

サイバーセキュリティ基本法の概要

サイバーセキュリティ基本法を理解する上で、まずは「基本法」が担う役割を把握しておく必要がある。法制局によれば、基本法とは「国政に重要なウェイトを占める分野について国の制度、政策、対策に関する基本方針・原則・準則・大綱を明示したもの」と定義されている。憲法と個別法をつなぐ役割として、憲法の理念を具体化する役割を果たすのが基本法だ。基本法の名がつく、サイバーセキュリティ基本法は、我が国がサイバーセキュリティ対策を講じる上で、上位に立つ重要な法案なのだ。サイバーセキュリティに携わるのであれば、まずここの理解を深めておきたい。

サイバーセキュリティ基本法の目的は、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」と定められている。世界規模で高まっているサイバーセキュリティの脅威に対し、国をあげてサイバーセキュリティ対策を総合的かつ効果的に推進することが求められているのだ。サイバーセキュリティ基本法の基本的施策の対象には、行政機関だけではなく、電力やガスなどの重要インフラ、民間事業者、教育研究機関も挙げられている。サイバーセキュリティに関する研究の促進や人材教育、一般事業者の果たすべき責務にも言及しており、国による情報セキュリティ戦略の基盤となる。

サイバーセキュリティ基本法では、組織的な体制も強化された。本法律では、内閣官房長官を本部長とする「サイバーセキュリティ戦略本部」を創設している。従来は「会議」として位置づけられていた「情報セキュリティ対策会議」が、法的な裏付けのもと、大きな権限を掌握することになったということだ。国家レベルでサイバーセキュリティを推進する体制が整ったといえる。同時に、前進である旧NISCを発展・強化し、名称と組織形態を改組する形で「内閣サイバーセキュリティセンター（NISC）」が設置された。英語略称はNISCと

10 Windows OSのメインストリームサポートと延長サポートの違いや、サポート終了について企業が注意すべきポイントを教えてください。

して変わらないが、より強い権限を得てサイバーセキュリティ戦略本部とも深く関わっていくことになる。

サイバーセキュリティ戦略本部

サイバーセキュリティに関する施策を総合的かつ効果的に推進するために内閣に設置される。内閣官房長官をサイバーセキュリティ戦略本部長とし、国務大臣をサイバーセキュリティ戦略副本部長とする。サイバーセキュリティ戦略本部員は、国家公安委員会委員長や防衛大臣に加え、民間の有識者などが担当することになる。サイバーセキュリティ戦略本部の役割は、以下の4点である。

①サイバーセキュリティ戦略案の作成
②政府機関など防御施策評価（監査を含む）
③重大事象の施策評価（原因究明調査を含む）
④各府省の施策の総合調整

各府省に対しては、セキュリティ対策について勧告できる権限を持つほか、IT戦略本部や国家安全保障会議（NSC）とも密接に連携する。

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基本法の施行にともない、旧NISCを改組して、内閣官房に設置された。センター長は、内閣官房副長官補。NISCの役割は以下の通りである。

①「政府機関情報セキュリティ横断監視・即応調整チーム」（GSOC）に関する事務
②原因究明調査に関する事務
③監査などに関する事務
④サイバーセキュリティに関する企画・立案、総合調整

NISCは、サイバーセキュリティ戦略本部の事務局としても機能する。

サイバーセキュリティ基本法改正の経緯

2015年1月に施行されたサイバーセキュリティ基本法は、権限が強化されたサイバーセキュリティ戦略本部やNISCのもと、国をあげたサイバーセキュリティ対策に乗り出した。さらに同法は、サイバーセキュリティ脅威や社会情勢を加味して2019年6月時点ですでに、二回改正されている。

1）2016年改正の概要

2016年の改正は、日本年金機構における個人情報漏えい事件が背景にあるとされる。すでにサイバーセキュリティ基本法が施行されていたものの、NISCの原因究明調査対象が、中央省庁に限られていたため、十分な調査をおこなうことができなかった。その結果、調査が後手に回り、事態を悪化させることになったのだ。

これを踏まえ、NISCの権限をさらに強化するためにサイバーセキュリティ基本法が改正された。それまでは中央省庁に限られていた、原因究明調査対象を独立行政法人や特殊法人にまで拡大する規定を盛り込んだのだ。その結果、業務量が大幅に増大したことを受け、NISCの負担軽減を目的に、一部事務を情報処理推進機構（IPA）へ委託できるようにした。

さらに2016年の改正では、情報セキュリティ対策の実践的な能力を持つ国家資格「情報処理安全確保支援士」の新設も盛り込まれた。高まるサイバーセキュ

リティの脅威に対し、制度面から国のセキュリティ強度を高める狙いがあるとみられる。

2）2018年改正の概要

平昌オリンピックをはじめ、リオやロンドンオリンピックでも、多くのサイバー攻撃が発生したとされる。こうした経緯を踏まえ、2020年に開催される東京オリンピックに向け、官民が連携してサイバーセキュリティ対策を講じることが求められている。このような動きに対応しやすくするために、「サイバーセキュリティ協議会」を新たに設置することを軸としたサイバーセキュリティ基本法の改正案が、2018年12月に可決、成立した。改正案は、2019年4月に施行されている。

サイバーセキュリティ協議会は、NISCをはじめとする国の関係行政機関に加え、ガスや電力などの重要インフラ事業者、参加の希望がある組織などにより構成される。このような官民が有機的に連携してサイバーセキュリティ対策を実行に移す取り組みは、世界的にも前例がないとされる。

3ヵ年のサイバーセキュリティ戦略とは

2018年7月、サイバーセキュリティ戦略本部にて、サイバーセキュリティ戦略が閣議決定された。サイバーセキュリティ戦略とは、サイバーセキュリティ基本法に基づき制定される3ヵ年の行動計画だ。2015年から実施されていた計画が終了を迎えるにあたり、社会情勢やサイバーセキュリティの脅威を加味して新たな戦略「2018年戦略」が制定されるに至った。2018年戦略では、2015年戦略で掲げた「①情報の自由な流通の確保」、「②法の支配」、「③開放性」、「④自律性」、「⑤多様な主体の連携」の5つの原則を堅持することが確認された。そのうえで、サイバーセキュリティ基本法で掲げる目的、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」を達成するための具体的な施策が明示された。

本戦略では、企業が新たな価値を創出し、持続的な成長を促すために、IoT、AI、VR、ブロックチェーン、次世代通信技術の利活用についても言及している。最新技術の活用を促しながら、経営層の意識改革やサイバーセキュリティ投資の促進策を打ち出し、サイバーセキュリティ対策の徹底を宣言している。中小企業のサイバーセキュリティ対策の推進も支援するとしており、AIやIoTを安全に活用できる社会の実現を目指していく。

重要インフラに障害が発生した場合、国民生活に与える影響を5段階で評価する取り組みもおこなわれるなど、東京オリンピック・パラリンピック競技大会の開催に向けた体制の整備や、大会以降のサイバーセキュリティ強化にも触れている。これらの動きに対し、政府がリーダーシップを発揮し推進していくことで、点ではなく面としての対策が充実していくことが期待される。

関連トピックス

> 2018.12.20 従業員のサイバーセキュリティに対する意識が低下する実情

特集のトップへ >

マルウェア情報局の
最新情報をチェック！

メールマガジン登録　@MalwareInfo_JP　RSSを購読

マルウェア情報局

ESET社について

法人向け製品に関する
お問い合わせ

当サイトの情報は、「ESETセキュリティ ソフトウェア シリーズ」の日本国内総販売代理店である、キヤノンマーケティングジャパン株式会社が提供しています。

@MalwareInfo_JPさんのツイート

マルウェア情報局
@MalwareInfo_JP

【特集】サイバーセキュリティ基本法で押さえておくべきポイント eset-info.canon-its.jp/malware_info/s… 企業がセキュリティ対策を推進する上で、押さえておきたいサイバーセキュリティ基本法のポイントについて解説します#ESET#キヤノンマーケティングジャパン

埋め込む　Twitterで表示