

情報セキュリティ人材に必要な知識

(ISC)² Japan

代表 衣川 俊章 (CISSP)

1. (ISC)² Japan独自の行政に特化した知識群

前回までで、情報セキュリティ業務に関わる方々にとって必要な基礎知識について2回にわたって説明してきました。今回は、私ども (ISC)² Japanで調査、特定した日本の行政機関の情報セキュリティに関連する知識群について説明をしたいと思います。

この知識群ですが、(ISC)² Japanが提供する日本独自の情報セキュリティ要件について包括的に網羅し、行政組織のセキュリティ事業遂行に関わる人材を認証することを目的としている資格「日本行政情報セキュリティプロフェッショナル (JGISP)」取得に必要とされる知識項目から抜き出したものです。

前回までの管理・技術系の基礎知識に加えて、この行政に特化した知識を習得する事で、行政機関におけるいかなる情報セキュリティについても対応することが出来るようになります。

この知識群は、下記の4つに分類されています。

(1) 組織と政策・制度

ここでは、日本国の情報セキュリティに関わる政府や関連機関などの組織、およびそれら組織が策定した政策や制度などを理解することが必要となります。これらを理解することで、自組織の情報セキュリティ要件の背景や成り立ちについて知る事ができます。具体的には、下記の項目について知っていることが求められます。

- ①日本国の情報セキュリティ上、重要な組織である府省庁および関連機関の把握
- ②府省庁および関連機関の「役割や行動規範」の基

となる政策や制度の把握

- ③日本国の情報セキュリティ戦略において、その基盤を形成する上で重要な政策や制度の理解
- ④情報セキュリティ政策や制度に関連した「重点施策・基準・ガイドライン」の理解
- ⑤「要件定義・設計・実装・運用・管理体制等」に関わるセキュリティを実現するための日本国内における枠組みや手法の理解

(2) 法

ここでは、前述の政策や制度を基に策定された情報セキュリティに関わる日本国法令の理解（法令の目的、内容、その効果などについて）が必要となります。これらを理解することで、自組織の情報セキュリティ構築における必須条件が把握できるようになります。具体的には、以下の9分野にわたる法令についての理解が必要となります。

- ①日本国における法令の概念
- ②電子政府システムの情報セキュリティに関わる法令の理解
- ③行政手続の情報セキュリティに関わる法令の理解
- ④企業間商取引の情報セキュリティに関わる法令の理解
- ⑤企業と一般消費者との商取引の情報セキュリティに関わる法令の理解
- ⑥企業内の情報セキュリティに関わる法令の理解
- ⑦サイバー犯罪やその取り締りに関わる法令の理解
- ⑧重要インフラの保護に関わる法令の理解
- ⑨知的財産権に関わる法令の理解

(3) 技術

ここで言う技術とは、日本の行政機関で利用されている固有の情報セキュリティ技術要素を指しています。具体的には、下記の3つの項目について理解をすることが必要と考えます。

- ①政府機関・地方公共団体の情報セキュリティにおける日本特有技術インフラ（GPKIや住基ネットなど）内容を理解するための基礎知識の理解
- ②政府機関・地方公共団体で行っている情報サービスに利用されている技術の理解と、その背景となっている制度の理解
- ③政府機関・地方公共団体の情報システムのセキュリティを保証するための技術・制度の理解

(4) 倫理と慣行

情報セキュリティを考えるに当たっては、技術や制度、法令の理解だけでなく、国独自の文化に根ざしたビジネス上の倫理に関する概念、規定などを理解する事は非常に重要な要素です。いくら素晴らしい技術を導入しても、それらを利用する人たちに倫理観が伴っていないと全く予期しない結果を招く事もあり得ます。特に行政機関で扱う情報の種類を考えると、倫理にまつわる知識を正確に理解している事は必須と考えます。同時に行政機関における調達制度や契約に関連する慣行についての知識を理解することも必要と考えます。

- ①国家公務員倫理法・規程の概要と情報セキュリティとの関係の理解
- ②企業行動憲章の概要と情報セキュリティとの関係の理解
- ③契約に関連した制度・慣行の概要の理解

以上が私ども（ISC）²が提供しているJGISPを取得するのに必要な4つの分野の知識の説明となります。

2. 最後に— (ISC)² Japanについて

最後に少しだけ、(ISC)²Japanについてご紹介したいと思います。

(ISC)²は、世界135カ国以上で70,000人以上の認定情

報セキュリティプロフェッショナルの会員を擁する、非営利会員団体です。(ISC)²は、代表的な資格として世界中で認知されているCertified Information Systems Security Professional (CISSP[®]) およびその上位資格や Certified Secure Software Lifecycle Professional (CSSLP[®])、Certified Authorization Professional (CAP[®])、Systems Security Certified Practitioner (SSCP[®]) などの資格を提供しています。これらの認定資格は、IT関連資格としては初めて、個人認証制度に対するグローバル基準のベンチマークであるANSI/ISO/IEC標準17024の認証を取得しています。これらのグローバル視点での資格に加えて、唯一国に特化した資格として、今回ご紹介した日本行政情報セキュリティプロフェッショナル (JGISP) があります。(ISC)²はまた、情報セキュリティ知識を体系化したCBK[®]に基づき、教育プログラムやサービスを提供しています。

これらの資格取得は、組織にとっては、日本の行政に関わる情報セキュリティ知識を理解し、第三者認証を受けた人員を抱える事で、自組織の情報セキュリティが向上するだけでなく、外部からの信頼度向上にも寄与できると考えます。また、高度な認定資格の取得奨励は、人員の士気向上に大きく寄与します。

さて、この連載も今回が最終回となりました。行政機関における情報セキュリティの必要性から始まり、行政機関で情報セキュリティ業務に従事している方々が、各組織においてより効果的、かつ適切な情報セキュリティ対策構築、導入、運用していくに当たって知っているべき知識をまとめてみました。これらについて少しでも理解を深めていただけることができ、今後の情報セキュリティレベル向上に向けて参考にしていただけたら、本連載の目的達成と言えると思います。ご自身の知識習得、組織としての情報セキュリティ人員の育成、業務委託先の人材評価、JGISP資格の詳細などについて、更に情報を欲しいという方はぜひ一度(ISC)² Japanまでご連絡下さい。

< (ISC)² Japan連絡先 >

URL : <https://isc2.org/japan/> E-mail : infoisc2-j@isc2.org

TEL : 03-6757-0138