

○岩手県警察サイバー犯罪等対処能力検定の実施に係る細目的事項について

令和3年3月4日
岩生安第18号
岩警務第26号 警察本部長
岩警備第13号

各 部 長
首 席 監 察 官
各 所 属 長

「岩手県警察サイバー犯罪等対処能力検定実施要綱」（令和3年3月4日付け岩生安第17号ほか別添）の規定に基づき、サイバー犯罪及びサイバー攻撃への対処（以下「サイバー犯罪等対処」という。）に関する能力についての検定（以下「能力検定」という。）の初級及び中級の実施に関する細目的事項については下記のとおり定め、令和3年4月1日から施行するので、事務処理上遺漏のないようにされたい。

なお、本通達の実施に伴い、岩手県警察サイバー犯罪等対処能力検定の実施に係る細目的事項について（令和元年10月11日付け岩生安第108号ほか）は廃止する。

記

- 1 能力検定の実施日
能力検定の実施日については、能力検定の都度、定めるものとする。
- 2 能力検定の実施日等の周知
能力検定を実施するときは、その実施日、実施場所、受検資格、出題範囲、特例合格の要件、受検の申込み方法等について、十分な時間的余裕を持って周知するものとする。
- 3 能力検定の実施
 - (1) 能力検定の実施場所
能力検定は、警察の施設において行う。
 - (2) 監督員
能力検定の実施場所に、職員の中から必要な数の監督員を配置するものとする。
 - (3) 能力検定の対象
全ての警察職員としていることから、本部長は、本県警察職員以外の警察職員が初級又は中級の能力検定を受検することができるよう配慮するものとする。
 - (4) 受検手続
所属長は、検定を受けようとする者がいるときは、サイバー犯罪等対処能力検定受検申請書（様式第1号）により、生活安全部サイバー犯罪対策課長を経由して本部長に申請するものとする。
- 4 能力検定の出題範囲及び難易度
 - (1) 能力検定の出題範囲の詳細は、別表1のとおりとする。
 - (2) 能力検定におけるインターネットその他の高度情報通信ネットワークに関する知識に係る問題の難易度は、次のとおりとする。

ア 初級

独立行政法人情報処理推進機構（以下「IPA」という。）が実施するITパスポート試験と同程度の難易度

イ 中級

IPAが実施する基本情報技術者試験と同程度の難易度

5 特例合格の対象となる資格

実施要綱の第10の1(1)ア(エ)及び第10の1(2)ア(ウ)に掲げる「別途定める資格」は、別表2のとおりとする。

6 合格証書の交付等

(1) 検定の報告

生活安全部長は、能力検定の実施結果をサイバー犯罪等対処能力検定実施結果報告書（様式第2号）により、本部長に報告するものとする。

(2) 合格証書の交付

本部長は、合格証書（様式第3号）を作成し、合格者に交付するものとする。

(3) 合格者の管理

ア 本部長は、警務部警務課長及び合格者の属する所属の長に対し、サイバー犯罪等対処能力検定合格通知書（様式第4号）により、合格者を通知するものとする。

イ 警務部警務課長及び合格者の属する所属の長は、(2)の通知を受けたときは、当該合格者の勤務記録カード（岩手県警察職員の勤務記録カードに関する訓令（昭和39年岩手県警察本部訓令第23号）第2条に規定する勤務記録カードをいう。）に必要な事項を記載しなければならない。

7 合格者台帳の作成

生活安全部長は、サイバー犯罪等対処能力検定合格者台帳（様式第5号）により、合格者台帳を級位ごとに作成するものとする。

8 その他

実施要綱及び本通達に定めるもののほか、能力検定について必要な事項は、本部長が定める。

別表 1

出題範囲	出題範囲の詳細
関係法令及び捜査手続に関すること	サイバー犯罪及びサイバー攻撃の類型・概要、関係法令、違法情報及び有害情報、サイバーテロ及びサイバーインテリジェンスの概要、サイバー犯罪捜査の流れ、プロバイダ及びSNS事業者等に対する通信記録等の差押え、リモートアクセスに係る捜査手続、被疑者宅における捜索、差押え及び検証、捜査上の留意事項等
情報技術の解析の活用に関すること	情報技術の解析の概要、パソコン、携帯電話機及び電磁的記録媒体並びに各種ログ等の解析、電磁的記録の取扱等
痕跡等の追跡に関すること	痕跡等の追跡及び実態解明の必要性、匿名化通信技術の概要、証拠保全に関する留意事項、国際捜査共助、外国の機関、団体等に対する協力要請等、広域性への対応等
各種インターネットサービスに関すること	インターネット、プロバイダ（ISP）、IPアドレス、ドメイン名、電子メール、FTP、telnet、IX（Internet Exchangepoint）、ネットオークション、仮想通貨、ネットバンキング、SNS、ダークネット、Tor、クラウド、IoT、CDS、コンテンツ事業者等
各種サーバ及びネットワークに関すること	WWWサーバ、DNSサーバ、SMTPサーバ（メール）、POP及びIMAPサーバ（メール）、FTPサーバ、プロキシサーバ、NTPサーバ、データベースサーバ、認証サーバ、ブロードバンドルータ、WiFi、VPN、仮想サーバ（VPS）等
各種ログに関すること	アクセスログ、認証ログ、システムログ、messages、syslog、lastlog、sulog、cookie等
各種不正プログラムに関すること	スパイウェア、ウイルス、ワーム、トロイの木馬、ランサムウェア、ボット、キーロガー、バックドア等
情報セキュリティに関すること	脆弱性、不正のメカニズム、攻撃者の種類及び動機、サイバー攻撃（SQLインジェクション、DoS攻撃、標的型メール攻撃、水飲み場型攻撃、XSS、フィッシング等）、暗号化技術等
情報セキュリティ対策に関すること	不正プログラム対策、不正アクセス対策、アカウント管理、ログ管理、脆弱性管理、アクセス制御、無線LANセキュリティ、携帯端末のセキュリティ、セキュリティ製品・サービス等
情報セキュリティ実装技術に関すること	セキュアプロトコル（IPSec、SSL/TLS、SSH等）、認証プロトコル（SPF、DKIM等）、セキュアOS、ネットワークセキュリティ、データベースセキュリティ、アプリケーションセキュリティ等
サイバー犯罪等対処に関する基本的な要領を理解するために必要なもの	事情聴取・資料等に基づく事案概要及び被害状況の把握・報告、被害拡大の防止措置、捜査における証拠保全等の協力要請
サイバー犯罪等対処に従事するため	発信元及び経路の特定、実態解明の推進、被疑者の犯人性の立証等

に必要なもの	
サイバー犯罪等対処に関する技術的助言を行うために必要なもの	被疑者が犯行に利用した情報通信技術の解明、新たな手口や脅威となり得る技術等の把握、実態解明結果に基づく管理者対策等

別表 2

認定団体	資 格
I P A	情報セキュリティスペシャリスト
	テクニカルエンジニア（情報セキュリティ）
	ネットワークスペシャリスト（平成21年以降に取得したものに 限る。）
	テクニカルエンジニア（ネットワーク）
	システム監査技術者（平成21年以降に取得したものに限る。）
(I S C) ²	C I S S P (Certified Information Systems Security Pro fessional)
	S S C P (Systems Security Certified Practitioner)
I S A C A	C I S A (Certified Information Systems Auditor)
	C I S M (Certified Information Security Manager)
S A N S I n s t i t u t e	G S L C (GIAC Security Leadership Certification)
	G S N A (GIAC Systems and Network Auditor)
	G X P N (GIAC Exploit Researcher and Advanced Penetra tion Tester)
	G R E M (GIAC Reverse Engineering Malware)
	G C I A (GIAC Certified Intrusion Analyst)
	G C I H (GIAC Certified Incident Handler)
	G S E C (GIAC Security Essentials Certification)
E C - C o u n c i l	C E H (Certified Ethical Hacker)
その他上記資格と同等程度であるものとして別途通知する資格	

様式第3号
第 号

合格証書

(階級)	(氏名)
岩手県警察サイバー犯罪等対処能力検定(級)に合格したことを証する。	
年 月 日	
岩手県警察本部長	
警視長	印

