⑽　公表判定委員会
　法律又はサイバーセキュリティに関する専門的な知識経験を有する者（判定を行う脆弱性情報に関し利害関係を有しない者に限る。）により構成される機関として、受付機関が設置するものをいう。
⑾　調整機関
　ソフトウエア製品の脆弱性関連情報について、製品開発者への連絡及び公表に係る調整を行う機関として、経済産業大臣の定めるものをいう。
⑿　製品開発者
　次のいずれかに該当する者をいう。
①　ソフトウエア製品を開発した者
②　ソフトウエア製品の加工、輸入、販売又は頒布する者であって、当該者の性質及び態様その他の事情に照らして、当該ソフトウエア製品を実質的に開発した者と認められる者
⒀　ウェブサイト運営者
　ウェブサイトを運営する者をいう。
⒁　届出
　発見者が行うソフトウエア製品又はウェブアプリケーションの脆弱性関連情報に係る届出をいう。
⒂　対策方法
　脆弱性に起因して生じる影響を回避し、又は脆弱性を修正する方法をいう。
⒃　脆弱性検証
　脆弱性の有無及び新規性を検証することをいう。

4　本規程の適用範囲
　本規程は、日本国内で利用されているソフトウエア製品又は主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーションに係る脆弱性であって、その脆弱性に起因する影響が不特定又は多数の者に及ぶおそれのあるものに適用する。

第２　ソフトウエア製品に係る脆弱性関連情報に関する取扱い

1　手続の概要
　ソフトウエア製品に係る脆弱性関連情報の取扱いについての手続の概要は次のとおりとする。
①　発見者（自ら開発等を行ったソフトウエア製品に係る脆弱性関連情報（脆弱性に起因する影響が自ら開発等を行ったソフトウエア製品にとどまるものに限る。）を発見又は取得した製品開発者を除く。以下本章において同じ。）は、受付機関に脆弱性関連情報を届け出る。
②　受付機関は、届出を受理したときは、調整機関に脆弱性関連情報を速やかに通知する。
③　調整機関は、製品開発者に受付機関から通知された脆弱性関連情報を速やかに通知するとともに、当該製品開発者に脆弱性検証の結果の報告を求める。
④　調整機関は、脆弱性情報を公表する日（以下「脆弱性情報公表日」という。）を定める。
⑤　製品開発者は、脆弱性情報公表日までに、対策方法を作成する。
⑥　受付機関及び調整機関は、脆弱性情報公表日に、脆弱性情報、脆弱性検証の結果、対策方法及び対応状況（以下「脆弱性情報等」という。）について、インターネット等を通じて公表する。
⑦　前号の規定にかかわらず、受付機関又は調整機関は、製品開発者から自ら開発等を行ったソフトウエア製品に係る脆弱性関連情報（脆弱性に起因する影響が自ら開発等を行ったソフトウエア製品にとどまるものに限る。）及び対策方法の通知を受けたときは、脆弱性情報公表日を定め、脆弱性情報及び当該対策方法について、インターネット等を通じて公表する。公表に先立って、調整機関は、製品開発者から脆弱性情報公表日に係る意見を聴取する。

2　具体的な手続及び行動指針
　発見者、受付機関、調整機関及び製品開発者における具体的手続及び行動指針は次のとおりとする。
⑴　発見者
ア　発見者は、受付機関に発見又は取得した脆弱性関連情報を届け出ること。その際、製品開発者に同じ内容を通知することを妨げない。
イ　届出書には、次に掲げる事項（以下本章において「届出事項」という。）を記載すること。
①　氏名等の発見者を識別するための情報
②　電子メールアドレス等の発見者の連絡先
③　①及び②の製品開発者への通知の許否
④　製品開発者から直接連絡を受けることの許否
⑤　①の公表の許否
⑥　脆弱性関連情報に係るソフトウエア製品の名称
⑦　脆弱性関連情報の内容
ウ　発見者は、違法な方法により脆弱性関連情報を発見又は取得しないこと。
エ　発見者は、脆弱性情報公表日まで、脆弱性関連情報が第三者に漏えいしないよう適切に管理すること。
オ　発見者は、正当な理由がない限り、第三者に脆弱性関連情報を開示しないこと。正当な理由により開示するときは、あらかじめ受付機関に問い合わせること。
⑵　受付機関
ア　届出の取扱い及び脆弱性情報の公表に係る手続及び行動指針
㋐　受付機関は、発見者による届出が次に掲げる事項のいずれにも該当するときは、これを受理し、発見者に届出を受理した旨を通知すること。また、届出を不受理としたときは、発見者にその旨及びその理由を通知すること。
①　届出事項を全て記載していること。
②　本規程の適用範囲内であること。
③　既に公表されている脆弱性情報に関する脆弱性関連情報でないこと。
㋑　受付機関は、届出を受理したときは、調整機関に脆弱性関連情報を速やかに通知すること。
㋒　受付機関は、届出に係る脆弱性関連情報が次のいずれかに該当することが明らかになったときは、当該届出に係る処理を取りやめることができる。処理を取りやめるときは、発見者にその旨及びその理由を通知すること。
①　脆弱性関連情報に該当しないこと。
②　本規程の適用範囲外であること。
③　脆弱性に起因する影響が生じるおそれが著しく低いこと。
④　脆弱性関連情報が既知であり、かつ、脆弱性情報等が既に公表されていること。
⑤　違法な方法により発見又は取得されたおそれがあること。
㋓　受付機関は、発見者から問合せを受けたときは、調整機関と協議した上で、適切な情報を提供すること。その際、発見者の本人確認に留意すること。
㋔　受付機関は、発見者に係る情報を適切に管理し、当該発見者の同意がない限り、第三者（調整機関及び公表判定委員会を含む。）に開示しないこと。
㋕　受付機関は、脆弱性情報公表日まで、脆弱性関連情報が第三者に漏えいしないよう適切に管理すること。
㋖　受付機関は、正当な理由がない限り、第三者に脆弱性関連情報を開示しないこと。ただし、脆弱性検証又は脆弱性に起因する影響その他の脆弱性に関する情報の確認のために専門的な能力が必要であるときは、当該能力を有する第三者（脆弱性関連情報を適切に管理できる者に限る。）に対し当該脆弱性関連情報を提供し、又はその分析を依頼することができる。
㋗　受付機関は、調整機関から政府機関や事業者等に脆弱性情報等をあらかじめ通知する旨の連絡を受けたときは、発見者にその旨を通知すること。