4．ソフトウエア製品
ソフトウエア又はそれを組み込んだハードウエアであって、汎用性を有する製品。
5．ウェブアプリケーション
インターネット上のウェブサイトで稼働する固有のシステム。
6．コンピュータウイルス
コンピュータウイルス対策基準（平成７年通商産業省告示第429号）における「コンピュータウイルス」をいう。
7．コンピュータ不正アクセス
不正アクセス行為の禁止等に関する法律（平成11年法律第128号）における「不正アクセス行為」をいう。

Ⅲ．本基準における関係者の定義
本基準における関係者の定義は、以下のとおりとする。
1．発見者
脆弱性関連情報を発見又は取得した者。
2．受付機関
発見者が脆弱性関連情報を届け出るための機関であって、かつ、調整機関と製品開発者との公表等に係る調整が不可能な脆弱性関連情報について、公表するかどうかの判定を行う機関。
3．調整機関
脆弱性関連情報に関して、製品開発者への連絡及び公表等に係る調整を行う機関。
4．製品開発者
ソフトウエア製品の開発等を行う者であって、以下のいずれかに該当する者。
⑴　ソフトウエア製品を開発した者。
⑵　⑴に掲げる者のほか、ソフトウエア製品の開発、加工、輸入又は販売に関する形態その他の事情からみて、当該ソフトウエア製品の実質的な開発者と認められる者。
5．ウェブサイト運営者
ウェブサイトを運営する者。

Ⅳ．本基準の適用範囲
本基準は、以下に掲げるものの脆弱性であって、その脆弱性に起因する被害が不特定多数の者に影響を及ぼし得るものに適用する。
1．日本国内で利用されているソフトウエア製品
（ソフトウエア製品において通信プロトコル等の仕様を実装した部分を含む。）
2．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

Ⅴ．対象がソフトウエア製品である場合の脆弱性関連情報取扱基準
一．発見者が製品開発者ではない、又は、発見者が製品開発者であり発見若しくは取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限らない場合
対象がソフトウエア製品であり、かつ、発見者が製品開発者ではない、又は、発見者が製品開発者であり発見若しくは取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限らない場合における脆弱性関連情報の取扱いの流れを以下に示す。
⑴　発見者は、脆弱性関連情報を受付機関に届け出る。
⑵　受付機関は、届出を受理した場合、一定の場合を除き、調整機関に当該脆弱性関連情報を通知する。
⑶　調整機関は、受付機関から通知された脆弱性関連情報を、製品開発者に速やかに通知するとともに、当該製品開発者が開発等を行ったソフトウエア製品における当該脆弱性の有無及びその新規性の検証結果について、当該製品開発者に報告を求める。
⑷　調整機関は、当該脆弱性情報の公表日を定める。
⑸　当該製品開発者は、当該脆弱性情報の公表日までに、対策方法を作成するよう努める。
⑹　受付機関及び調整機関は、当該脆弱性情報の公表日に、当該脆弱性情報、その日までに得られた製品開発者による当該脆弱性の有無及びその新規性の検証結果並びに当該脆弱性に関する対策方法、取組みの状況等を含む対応状況について、インターネット等を通じて公表する。

関係者における詳細な行動基準を以下に定める。
1．発見者基準
⑴　発見者（自ら開発等を行ったソフトウエア製品に影響範囲が限られると認められる脆弱性関連情報を発見又は取得した製品開発者を除く。）は、発見又は取得した脆弱性関連情報を経済産業大臣が別に指定する受付機関に届け出ること。ただし、当該製品開発者に対し同じ内容を届け出ることを妨げない。
⑵　発見者は、以下の点を明示した上で脆弱性関連情報を届け出ること。
①　発見者の氏名、連絡先等の情報及びその取扱い
②　脆弱性を有する製品の名称等
③　当該脆弱性関連情報
⑶　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。
⑷　発見者は、当該脆弱性情報が受付機関及び調整機関から公表されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、当該脆弱性関連情報を正当な理由により第三者に開示する場合、あらかじめ受付機関に問い合わせをすること。
2．受付機関基準
２－１．発見者が脆弱性関連情報を届け出るための機関としての基準
⑴　受付機関は、１．⑴による届出が１．⑵で定めた届出事項を満たしているか否かを判断し、満たすと判断した場合、これを受理したものとし、当該発見者に対しその旨を速やかに通知すること。また、届出を不受理とした場合、当該発見者に対しその旨及びその理由を速やかに通知すること。
⑵　受付機関は、届出を受理したときは、速やかに、経済産業大臣が別に指定する調整機関に対し当該脆弱性関連情報を通知すること。ただし、当該脆弱性関連情報が以下に該当すると認められる場合、当該届出に係る処理を取りやめることができる。この場合においては、当該発見者にその旨及びその理由を通知すること。
①　受付機関が既知の脆弱性関連情報であると確認した場合
②　受付機関が調整機関から既知の脆弱性関連情報である旨の通知を受けた場合
③　受付機関が脆弱性関連情報に該当しないと確認した場合
④　受付機関が調整機関から脆弱性関連情報に該当しない旨の通知を受けた場合
⑤　受付機関が違法な方法により発見又は取得されたおそれがあると認めた場合
⑥　受付機関が公表判定委員会で審議し判定した結果が、２－２⑷②～④のいずれかに該当しないことにより公表することとならなかった場合
⑶　受付機関は、届出を受理した後においても、対策上必要と認められる場合、当該脆弱性関連情報について、当該発見者に問い合わせをすること。また、発見者からの問い合わせに対しては、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。
⑷　受付機関は、氏名、連絡先等の発見者を特定し得る情報を適切に管理し、当該発見者の同意がない場合は他者（調整機関及び製品開発者を含む。）に開示しないこと。
⑸　受付機関は、当該脆弱性情報が公表されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、対策上必要と認められる場合、当該脆弱性関連情報の適切な管理を前提として、第三者に分析を依頼することができる。