○経済産業省告示第百十号

ソフトウエア等脆弱性関連情報取扱基準（平成十六年経済産業省告示第二百三十五号）の全部を次のように改正する。

平成二十六年五月十四日

経済産業大臣　茂木　敏充

ソフトウエア等脆弱性関連情報取扱基準

Ⅰ．主旨

本基準は、ソフトウエア等に係る脆弱性関連情報等の取扱いにおいて関係者に推奨する行為を定めることにより、脆弱性関連情報の適切な流通及び対策の促進を図り、コンピュータウイルス、コンピュータ不正アクセス等によって不特定多数の者に対して引き起こされる被害を予防し、もって高度情報通信ネットワークの安全性の確保に資することを目的とする。

Ⅱ．用語の定義

本基準で用いられる用語の定義は、以下のとおりとする。

１．脆弱性

ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

２．脆弱性関連情報

脆弱性に関する情報であって、以下に掲げる類型のいずれかに該当するもの。

（１）脆弱性情報

脆弱性の性質及び特徴を示す情報。

（２）検証方法

脆弱性が存在することを調べる方法。

（３）攻撃方法

脆弱性を悪用するプログラム、コマンド又はデータ及びそれらの使用方法。

３．対策方法

脆弱性によって生じる問題を解決又は回避するための方法であって、以下に掲げる類型のいずれかに該当するもの。

（１）回避方法

脆弱性を修正することなく、それが原因となって生じる被害を回避するための方法。

（２）修正方法

脆弱性を修正する方法。

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。

（１）ソフトウエア製品を開発した者。

（２）（１）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。

（ｉ）発見者は、脆弱性関連情報を受付機関に届け出る。

（ii）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。

（iii）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。

（iv）調整機関は、当該脆弱性情報の公表日を定める。

（ｖ）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。

（vi）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

（１）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。

（２）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

（３）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。

（４）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

（１）受付機関は、１．（１）による届出が１．（２）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。

（２）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、２－２（４）②～④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

（３）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。

（４）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。

（５）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。

（６）受付機関は、調整機関から政府機関や事業者等に当該脆弱性関連情報及び対策方法をあらかじめ通知する旨の連絡を受けた場合、当該発見者に対して、その旨を事前に通知すること。

（７）受付機関は、調整機関が当該脆弱性情報を公表した場合には、その公表時期に合わせて当該脆弱性情報及び調整機関から当該脆弱性情報の通知を受けた製品開発者から報告された当該製品開発者の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（以下「対応状況」という。）を公表するとともに、当該発見者に対しその旨を通知すること。

（８）受付機関は、脆弱性に起因する被害の予防に資するため、脆弱性関連情報の届出状況等を公表すること。

２－２．公表等に係る調整が不可能な脆弱性関連情報に関して、公表するかどうかの判定を行う機関としての基準

（１）受付機関は、調整機関から３．（10）により、脆弱性関連情報について、公表等に係る調整が不可能である旨の通知があった場合は、公表判定委員会で審議し、公表するかどうか判定することができる。なお、製品開発者から新たな報告があった場合等事情の変化があった場合は、当該脆弱性関連情報について、調整機関と製品開発者との公表等に係る調整を再度行うように調整機関に通知することができる。

（２）受付機関は、法律又は情報セキュリティに関する専門的な知識経験を有する者から構成される公表判定委員会を組織すること。なお、公表判定委員会の委員は、中立性を考慮し、当該製品開発者等の当該脆弱性関連情報に係る特別の利害関係を有しない者とすること。

（３）受付機関は、調整機関から関係する情報を聴取し、公表判定委員会の審議に必要な資料を整理すること。

（４）受付機関は、当該脆弱性関連情報について公表判定委員会で審議し、次に示す条件を全て満たす場合は公表することと判定することができる。なお、公表判定委員会は審議に当たって、当該製品開発者が意見を表明する機会を確保すること。ただし、３．（２）後段の規定により通知をおこなったものとみなされた製品開発者については、この限りではない。

①調整機関と製品開発者との公表等に係る調整が不可能であること。

②脆弱性が存在すると判断できること。

③公表しない限り、当該脆弱性情報を知り得ない製品利用者がいるおそれがあること。

④公表が適当でないと判断する理由・事情が無いこと。

（５）受付機関は、公表するかどうかの判定結果とその理由を製品開発者に通知すること、及び脆弱性情報を公表することとなった場合は、公表する内容に関して、製品開発者から見解を聴取すること。ただし、３．（２）後段の規定により通知をおこなったものとみなされた製品開発者については、この限りではない。

（６）受付機関は、公表するかどうかの判定結果とその理由、及び製品開発者から聴取した当該脆弱性情報に関する見解を調整機関に通知すること。また、公表することとならなかった理由が（４）①に該当しないことであった場合は、調整機関と製品開発者との公表等に係る調整を再度行うように調整機関に通知すること。

３．調整機関基準

（１）調整機関は、脆弱性関連情報を製品開発者に適切に通知するために必要な製品開発者の名簿（以下「名簿」という。）を作成すること。その際、製品開発者と調整の上、当該製品開発者が調整機関との連絡をとるために設置した窓口を名簿に記載すること。

（２）調整機関は、受付機関から脆弱性関連情報の通知を受けた場合、又は受付機関から脆弱性関連情報について製品開発者との調整を再度行うべきと通知を受けた場合には、その内容に照らして当該脆弱性関連情報を通知すべき製品開発者を名簿から特定し、速やかに通知するとともに、当該製品開発者に対し、当該製品開発者の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を検証（以下「脆弱性検証」という。）しその結果を報告するよう求めること。また、名簿に記載のない製品開発者の中から新たに通知すべき者を特定した場合には、それを名簿に加えた上で、同様に通知を行い、脆弱性検証の結果を報告するよう求めること。ただし、製品開発者と連絡が一定期間とれない場合は、当該製品開発者の名称及び製品に関する情報等とともに、連絡先に係る情報の提供を求める旨をインターネット等を通じて公表することとし、一定期間公表することで、調整機関が当該製品開発者に通知を行ったものとみなすこととする。

（３）調整機関は、製品開発者から脆弱性検証の結果報告を聴取し、その結果を踏まえつつ、対策方法の作成及び海外の調整機関との調整に要する期間、当該脆弱性情報の流出するリスク等の要素を考慮した上で、当該脆弱性情報を公表すべき日（以下「脆弱性情報公表日」という。）を定めるとともに、当該脆弱性情報公表日を受付機関及び当該製品開発者に通知すること。また、当該脆弱性関連情報について脆弱性検証の結果を報告するよう求めた

製品開発者が複数いる場合、脆弱性検証の結果報告が一部の製品開発者からしか得られなかった場合は、得られた結果報告を踏まえつつ、国内外における脆弱性情報の取扱事例、海外の調整機関との調整に要する期間、当該脆弱性情報の流出するリスク等の要素を考慮した上で、脆弱性情報公表日を独自に定め、同様に、受付機関及び当該製品開発者に通知すること。

（４）調整機関は、製品開発者から脆弱性情報公表日を変更したい旨の申し出を受けた場合、当該製品開発者から意見を聴取した上で、当該脆弱性情報公表日を変更することができる。脆弱性情報公表日を変更した場合、新たに定めた脆弱性情報公表日を受付機関及び当該脆弱性情報に関して通知を行った製品開発者に対し通知すること。

（５）調整機関は、通知を行った製品開発者に対して、脆弱性情報公表日までに当該製品開発者の対応状況を報告するよう求めること。

（６）調整機関は、脆弱性情報公表日に、当該脆弱性情報並びにその日までに得られた製品開発者による脆弱性検証の結果及び対応状況について、インターネット等を通じて公表すること。

（７）調整機関は、脆弱性情報公表日までに通知を行った製品開発者から既知の脆弱性情報である旨の通知を受けた場合、その公表を取りやめることができる。公表を取りやめた場合、

受付機関にその旨を通知すること。

（８）調整機関は、脆弱性情報公表日までに通知を行った製品開発者から脆弱性による影響がない旨の脆弱性検証の結果報告を受けた場合、受付機関から通知された情報は脆弱性関連情報には該当しないものと判断し、その公表を取りやめることができる。公表を取りやめた場合、受付機関にその旨を通知すること。

（９）調整機関は、脆弱性情報公表日までの間、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し又は通知することができる。

（10）調整機関は、製品開発者と公表等に係る調整を行ったが連絡がとれないことなどにより進展が見込めなくなった場合は、調整機関と製品開発者との調整が不可能であるとして、受付機関に公表するかどうかの判定を求めること。

（11）調整機関は、受付機関の判定に基づき、脆弱性情報を公表することとなった場合は、当該脆弱性情報並びに脆弱性検証の結果、対応状況及び製品開発者の当該脆弱性情報に関する見解について、インターネット等を通じて公表すること。

（12）調整機関は、対策方法が作成されてからそれが公表されるまでの間であって、当該脆弱性関連情報が、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に

重大な影響を与えるおそれがあると認められる場合、受付機関及び当該製品開発者と協議をした上で、政府機関や当該脆弱性関連情報によって重大な影響を受ける設備を用いている事業者等に当該脆弱性関連情報及び対策方法をあらかじめ通知することができる。

４．製品開発者基準

（１）製品開発者は、調整機関と調整の上、調整機関と連絡をとるための窓口を設置し、調整機関に通知すること。

（２）製品開発者は、調整機関から通知された脆弱性関連情報に関して、遅滞なく脆弱性検証を行い、その結果を調整機関に報告すること。

（３）製品開発者は、当該脆弱性が他社のソフトウエア製品に含まれることが推定される場合には、その旨及びその理由を調整機関に通知すること。

（４）製品開発者は、脆弱性情報公表日までの間、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。

（５）製品開発者は、脆弱性情報公表日までに、対応状況を受付機関及び調整機関に報告するとともに、対策方法を作成するよう努めること。

（６）製品開発者は、対策方法を作成した場合、受付機関及び調整機関に報告し、脆弱性情報公表日以降、自らもそれを利用者に周知すること。

二．発見者が製品開発者であり、発見又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れる場合

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あり、発見又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れる場合における関係者の行動基準を以下に定める。

（１）製品開発者は、自ら開発等を行ったソフトウエア製品に影響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場合、対策方法を作成し、当該脆弱性関連情報及び対策方法を受付機関及び調整機関に通知すること。

（２）受付機関及び調整機関は、（１）による通知を受けたときは、当該脆弱性情報及び対策方法をインターネット等を通じて公表すること。ただし、調整機関はそれらを公表すべき日について、当該製品開発者から意見を聴取した上で定めること。

Ⅵ．対象がウェブアプリケーションである場合の脆弱性関連情報取扱基準

対象がウェブアプリケーションである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。

（ⅰ）発見者は、脆弱性関連情報を受付機関に届け出る。

（ⅱ）受付機関は、届出を受理した場合、一定の場合を除き、当該ウェブサイト運営者に当該脆弱性関連情報を通知する。

（ⅲ）当該ウェブサイト運営者は、受付機関から通知された脆弱性関連情報を検証し、必要に応じて当該脆弱性を修正する。

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

（１）発見者（自ら運営するウェブサイトのウェブアプリケーションについての脆弱性関連情報を発見又は取得したウェブサイト運営者を除く。）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、当該ウェブサイト運営者に対し同じ内容を届け出ることを妨げない。

（２）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脆弱性を有するウェブアプリケーションを稼働しているウェブサイトの名称等

③当該脆弱性関連情報

（３）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。

（４）発見者は、当該脆弱性が修正されるまでの間、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

（１）受付機関は、１．（１）による届出が１．（２）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。

（２）受付機関は、届出を受理したときは、速やかに、当該ウェブサイト運営者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受付機関がウェブサイト運営者から既知の脆弱性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受付機関がウェブサイト運営者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

（３）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、当該ウェブサイト運営者と協議し、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。

（４）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（ウェブサイト運営者を含む。）に開示しないこと。

（５）受付機関は、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、第三者にその分析を依頼することができる。

（６）受付機関は、当該ウェブサイト運営者から当該脆弱性を修正した旨の通知があったときは、それを速やかに発見者に通知すること。

（７）受付機関は、脆弱性に起因する被害の予防に資するため、脆弱性関連情報の届出状況等を公表すること。

３．ウェブサイト運営者基準

（１）ウェブサイト運営者は、受付機関から通知された脆弱性関連情報に関して、その内容を検証し、必要に応じて当該脆弱性を修正すること。

（２）ウェブサイト運営者は、当該脆弱性関連情報に関して検証した結果又は当該脆弱性を修正した旨を速やかに受付機関に通知すること。

（３）ウェブサイト運営者は、当該脆弱性が修正されるまでの間、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。

（４）ウェブサイト運営者は、当該脆弱性に起因する個人情報の漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表するなど必要な対策をとること。

附　則

この告示は、公布の日から施行する。