表1. ガイドラインの変更点

#	変更箇所(旧番号)	変更前	変更後(下線が変更部分)
1	表紙他	有限責任中間法人 JPCERT コーディネーションセンター	一般社団法人 JPCERT コーディネーションセンター
2	Ⅲ. 本ガイドラインの適用の範囲 〇ソフトウエア製品の場合: ・国内で利用されているソフトウエア製品	国内で、多くの人々に利用されている等のソフトウエア製品が該当します。プロトコルを実装しているものも含みます。	国内で、多くの人々に利用されている等のソフトウエア製品が該当します。「暗号アルゴリズム」や「プロトコル」を実装しているものも含みますが、一般的な「暗号アルゴリズム」や「プロトコル」等の仕様そのものの脆弱性は含みません。
3	Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱 3. IPA および JPCERT/CC の対応 (1)IPA 12)一般への公表日の決定	なお、脆弱性検証の結果の報告および対応状況の報告がない場合、IPA および JPCERT/CC は、その旨を、製品開発者名とともに JVN で公表することがあります。	なお、製品開発者と連絡が取れない場合、または、脆弱性検証の結果の報告および対応状況の報告がない場合、IPA および JPCERT/CC は、その旨を、製品開発者名とともに JVN で公表することがあります。
4	(2)JPCERT/CC 2)製品開発者への連絡	さらに、製品開発者との連絡が取れない場合、JPCERT/CC は、その脆弱性の影響範囲や連絡のとれない期間を考慮して取扱いを終了することがあります。	さらに、製品に添えられた宛先情報をもとに電子メールや郵便、電話、FAX 等いずれの手段で製品開発者に連絡を試みても一定期間にわたりまったく応答がない場合には、「連絡が取れない」と判断します。その場合、JPCERT/CC は、その脆弱性の影響範囲や連絡の取れない期間を考慮して取扱いを終了することがあります。
5	3)一般への公表日の決定	なお、製品開発者から脆弱性検証の結果の報告がない場合、過去の類似事例を参考にし、JPCERT/CC が公表日を決定することがあります。	なお、製品開発者と連絡が取れない場合、または、製品開発者から脆弱性検証の結果の報告がない場合、過去の類似事例を参考にし、JPCERT/CC が公表日を決定することがあります。
6	9)一般への情報の公表	なお、脆弱性検証の結果の報告および対応状況の報告がない場合、JPCERT/CC および IPA は、その旨を、製品開発者名とともに JVN で公表することがあります。	なお、製品開発者と連絡が取れない場合、または、脆弱性検証の結果の報告および対応状況の報告がない場合、JPCERT/CC および IPA は、その旨を、製品開発者名とともに JVN で公表することがあります。
7	5. その他 1) 製品開発者自身による脆弱性関連情報の発見・取得	製品開発者は、自社のソフトウエア製品についての脆弱性関連情報であって、他社のソフトウエア製品に影響を及ぼさないと認められるものを発見・取得し、調整機関からの通知によることなく、対策方法を作成した場合であっても、ユーザへの周知を徹底するために JPCERT/CC 連絡することが望まれます。この連絡をもって、IPA および JPCERT/CC に連絡したこととみなされます。	製品開発者は、自社のソフトウエア製品についての脆弱性関連情報であって、他社のソフトウエア製品に影響を及ぼさないと認められるものを発見・取得し、調整機関からの通知によることなく、対策方法を作成した場合であっても、ユーザへの周知を徹底するために JPCERT/CC または IPA に連絡することが望まれます。この連絡をもって、IPA および JPCERT/CC に連絡したこととみなされます。

#	変更箇所(旧番号)	変更前	変更後(下線が変更部分)
8	Ⅴ. ウェブアプリケーションに係る脆弱性関連情報取扱 3. IPA の対応 4)脆弱性関連情報への対応続行の判断	―	(オ)ウェブサイトの不適切な運用(付録4)のうち、脆弱性の原因が下記と判明したもので、IPA が注意喚起などの方法で広く対策を促した後、処理を取りやめる判断をした場合 ・ウェブサイトが利用しているソフトウエア製品の設定情報が、誤っていたり初期状態のままとなっている。 ・ウェブサイトが利用しているソフトウエア製品の修正プログラムが適用されていない。 なお、上記(オ)の注意喚起後は、該当する製品の開発者も対策方法の再度の周知をウェブサイト運営者へ行うことを推奨します。
9	5)ウェブサイト運営者への連絡	―	なお、ウェブサイトに掲載された宛先情報をもとに電子メールや郵便、電話、FAX 等いずれの手段でウェブサイト運営者に脆弱性関連情報に係わる問い合わせを試みても、一定期間にわたり的確な答えがない場合、IPA は、その脆弱性の影響範囲や取扱い期間を考慮して取扱いを終了することがあります。
10	付録1　発見者が心得ておくべき法的な論点 1. 脆弱性関連情報の発見に際しての法的な問 (1)関係する行為と法令の関係 a)ネットワークを用いた不正	例えば、脆弱性関連情報を利用して、アクセス制御機能を回避し、インターネットなどを介してシステムにアクセスした場合には、不正アクセス禁止法に抵触します。	例えば、脆弱性関連情報を利用して、アクセス制御機能を回避し、インターネットなどを介してシステムにアクセスした場合には、不正アクセス禁止法(不正アクセス行為の禁止等に関する法律)に抵触します。
11	付録4　具体的な説明 1. ウェブサイトの不適切な運用	ウェブサイトの不適切な運用の例を以下に挙げます。 ・URL の一部にパスワードが判別可能な形式で明示されている ・本来閉じられているべき telnet 等のポートが空いており、administrator のパスワードが付与されていない ・ウェブサイト運営者が公開を意図していないファイル(個人情報ファイル等)が、ウェブサーバに、誰にでも閲覧できる状態で(アクセス制限なしに)置かれている等	ウェブサイトの不適切な運用の例を以下に挙げます。 ・ウェブサイトにおいて、本来提供するべき対象外の機能(ウェブ管理画面等)やファイル(個人情報ファイル等)が、アクセス制限なしに公開されており、セキュリティが維持できなくなっている。 ・ウェブサイトで使用されているソフトウエア製品に脆弱性が存在している。 ・サービスを行っていないウェブサイトの脆弱性が放置されている。
12	付録6の後ろに追記	―	付録7　ウェブサイト構築事業者のための脆弱性対応マニュアル(P.42 から P.49 を追加)