



要求事項・評価基準の変更箇所

SCS評価制度 制度運営事務局

2026/10/28

独立行政法人

情報処理推進機構

セキュリティセンター

© 2026 Innovation Platform Agency, Japan (IPA)

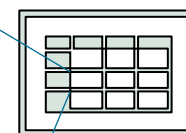
セキュリティパッチ及びアップデート（評価基準4-4-4-2）の対応について、脆弱性悪用のリスクを低減する対策を「自己評価等ガイド」及び「要求事項・評価基準 解説書」に記載することで、情報セキュリティに係る国内外の情勢変化に応じて機動的な見直しを実施することを可能にする。

- **リスクベースの考え方を踏まえた対象選定**： CVSS基本値7.0以上であり、攻撃が観測されている脆弱性については引き続き14日以内の対応を継続。（IPA「重要なセキュリティ情報」又はCISA「KEV」等、公的機関等のリストに掲載されている脆弱性）
- **対応計画及び代替策に基づくリスク低減及び対応管理の実施**： CVSS基本値7.0以上の脆弱性について、情報公開時点で攻撃が観測されていない又はその蓋然性が低いと考えられるものと、攻撃が観測されているものを区別し、それぞれ対応計画の策定及びそれに基づく管理や、代替策による脆弱性悪用のリスク低減策を行うことを前提に、脆弱性対応期限の延長に関する運用を認める旨を記載。

1. 評価基準4-4-4-2の修正 ※取消線部を削除

- ・利用している機能又は設定に関して、以下のいずれかに該当するアップデートプログラムがリリースされてから14日以内に、アップデートすること。
(略)
 - ・やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、**以下のいずれかにより**脆弱性悪用のリスクを低減する対策を実施すること。
 - 脆弱性悪用の対象となる機能を無効化すること。
 - ベンダーが推奨する回避策を実施すること。
 - 対象となる情報機器を適用範囲内のネットワークから分離すること。
 - 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入すること。
- (以下略)

★3・★4 要求事項・評価基準



★3・★4
自己評価等
ガイド

★4
第三者評価
ガイド

★4
技術検証
ガイド

★3・★4
要求事項・
評価基準 解説書

取消線部を評価ガイド及び解説書で説明

2. 上記に関連して、評価基準4-4-2-1（★4）及び4-4-4-1（★3）について整合を図るため修正

② 「要求事項・評価基準」 変更一覧



- 以下3つの評価基準について修正を実施。

★3/ 評価基準		2026/3/27公開版 (Ver.1.0)
★4 No.		
★4	4-4-2-1	・利用するOS及びソフトウェアについて、以下のいずれかを適用すること。 - 全てのOS及びソフトウェアについてサポートのあるものを利用すること。 - やむを得ずサポート切れのOS及びソフトウェアを利用する場合(例えば、代替システムを調達する必要がある、直ちに更改できない場合)は、更改計画を策定した上で、更改するまでの間、No.4-4-4-2で求める脆弱性悪用のリスクを低減する対策を実施すること。
★3	4-4-4-1	・システム、情報機器及びソフトウェアは以下の状態とすること。 - ライセンスが付与され、サポートされている。 - サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。 - 可能であれば、自動アップデートが有効化されている。
	4-4-4-2	・利用している機能又は設定に関して、以下のいずれかに該当するアップデートプログラムがリリースされてから14日以内に、アップデートすること。 - 当該アップデートが、ベンダーにより「重大」(Critical)又は「高リスク」(High Risk)と説明される脆弱性を修正するものである。 - 当該アップデートが、CVSSの基本値が7.0以上の脆弱性を修正するものである。 - 当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない。 ・やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施すること。 - 脆弱性悪用の対象となる機能を無効化すること。 - ベンダーが推奨する回避策を実施すること。 - 対象となる情報機器を適用範囲内のネットワークから分離すること。 - 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入すること。 [対象] -会社支給のパソコンの OS、ブラウザ及びOffice ソフト -サーバの OS及びミドルウェア -会社支給のスマートデバイスのOS及びアプリ -インターネットとの境界に設置されているネットワーク機器のOS及びファームウェア

★3/ ★4	評価基準 No.	2026/10/28公開版 (Ver.1.1)
★4	4-4-2-1	・利用するOS及びソフトウェアについて、サポートのあるものを利用すること。 ・やむを得ずサポート切れのOS及びソフトウェアをそのまま利用する場合(例えば、代替システムを調達する必要がある、直ちに更改できない場合)は更改計画を策定した上で、更改するまでの間、脆弱性悪用のリスクを低減する対策を実施すること。
★3	4-4-4-1	・情報機器、OS及びソフトウェアについて、以下の状態とすること。 - ライセンスが付与され、サポートされている。 - サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。 - やむを得ず、サポートが終了したものを利用する場合、脆弱性悪用のリスクを低減する対策を実施している。 - 可能であれば、自動アップデートが有効化されている
	4-4-4-2	・利用している機能又は設定に関して、以下のいずれかに該当するアップデートプログラムがリリースされてから14日以内に、アップデートすること。 - 当該アップデートが、ベンダーにより「重大」(Critical)又は「高リスク」(High Risk)と説明される脆弱性を修正するものである。 - 当該アップデートが、CVSSの基本値が7.0以上の脆弱性を修正するものである。 - 当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない。 ・やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、脆弱性悪用のリスクを低減する対策を実施すること。 (※やむを得ない場合の対策については、自己評価等ガイド及び解説書で説明) [対象] -会社支給のパソコンの OS、ブラウザ及びOffice ソフト -サーバの OS及びミドルウェア -会社支給のスマートデバイスのOS及びアプリ -インターネットとの境界に設置されているネットワーク機器のOS及びファームウェア

③ 「要求事項・評価基準」 評価基準4-4-4-2に係る関連ガイド及び解説書の記載

- ・セキュリティパッチ及びアップデート（評価基準 4-4-4-2）に係る「★3・★4 自己評価等ガイド」及び「★3・★4 要求事項・評価基準 解説書」（2026年10月28日公開版）の記載箇所を以下に示す。※詳細については、各文書を参照されたい。

	「★3・★4 自己評価等ガイド」	「★3・★4 要求事項・評価基準 解説書」
記載箇所	別紙 自己評価における適合基準等（P90） ・ 4. 攻撃等の防御 ・ 4-4 プラットフォームセキュリティ ・ 4-4-4 セキュリティパッチ・アップデートの手続 ・ (2) No.4-4-4-2	別紙 要求事項・評価基準の個別解説（P93） ・ No.4 攻撃等の防御 ・ No.4-4 プラットフォームセキュリティ ・ (4)セキュリティパッチ・アップデートの手続 [No.4-4-4] ・ 評価基準No. 4-4-4-2関連
主な内容	適合基準及び自己評価方法として主に以下を記載 ✓ ベンダーが「重大（Critical）」又は「高リスク（High Risk）」と説明する脆弱性、CVSSの基本値が7.0以上の脆弱性、又はベンダーが詳細を提供していない脆弱性を修正するアップデートプログラムを、リリースから14日以内に適用していること。 ✓ やむを得ず14日以内にアップデートできない場合は、アップデートに係る対応計画を策定した上で、以下の対応を行うこと。 ＜既に攻撃を観測している脆弱性の場合＞ 機能無効化、ベンダー提供回避策、ネットワーク分離、監視強化等を実施すること。 ＜攻撃を観測していない脆弱性の場合＞ 対応計画を、完了するまで管理、記録すること。	解説として主に以下を記載 ✓ リリースから14日以内のアップデートについて、すべての脆弱性に対応することが難しい場合、実際の脆弱性悪用状況等も考慮して緊急度の高い脆弱性を特定して優先的に期限内に対応する運用を許容することが、効率的かつ効果的なアプローチとなる。 ✓ 脆弱性情報の収集源として、国内外の公的機関等が発出する情報源を例示。 ✓ CVSSの基本値が7.0未満で攻撃が観測されているインターネットとの境界に設置されている機器の脆弱性についても早急に対応することを強く推奨。 ✓ アップデート対応計画策定にあたって機器のインターネットへの露出状況等を踏まえて対応期限を設定すると共に、攻撃が観測された場合に見直しを行う。



独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

Beyond Digital