重要度	発行日	アドバイザリ ID	関連セキュリティ勧告	タイトル	保護機能設定方法
緊急	2022年4月10日	CPAI-2021-1153	CVE-2021-35587	Oracle Access Manager の認証が回避される脆弱性 (CVE-2021-35587)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Oracle Access Manager Authentication Bypass (CVE-2021-35587)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0135	CVE-2022-28237	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-16: CVE-2022-28237)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Use After Free (APSB22-16: CVE-2022-28237)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0169	CVE-2022-28249	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28249)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28249)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0186	CVE-2022-27793	Adobe Acrobat および Reader の領域外メモリへの書き出しの脆弱性 (APSB22-16: CVE-2022-27793)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Write (APSB22-16: CVE-2022-27793)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0160	CVE-2022-28246	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28246)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28246)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0142	CVE-2022-28257	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28257)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28257)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0102	CVE-2022-24542	Microsoft Windows Win32k で権限が昇格される脆弱性 (CVE-2022-24542)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Microsoft Windows Win32k Elevation of Privilege (CVE-2022-24542)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0159	CVE-2022-28251	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28251)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28251)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0187	CVE-2022-27785	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-16: CVE-2022-27785)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Use After Free (APSB22-16: CVE-2022-27785)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0134	CVE-2022-28243	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28243)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28243)］保護機能を探し、保護機能の設定を編集します。

重要度	発行日	アドバイザリ ID	関連セキュリティ勧告	タイトル	保護機能設定方法
高	2022年4月12日	CPAI-2022-0158	CVE-2022-28236	Adobe Acrobat および Reader の領域外メモリへの書き出しの脆弱性 (APSB22-16: CVE-2022-28236)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Write (APSB22-16: CVE-2022-28236)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0181	CVE-2022-27790	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-16: CVE-2022-27790)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Use After Free (APSB22-16: CVE-2022-27790)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0100	CVE-2022-24547	Microsoft Windows Digital Media Receiver で権限が昇格される脆弱性 (CVE-2022-24547)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Microsoft Windows Digital Media Receiver Elevation of Privilege (CVE-2022-24547)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0180	CVE-2022-28245	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28245)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28245)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0103	CVE-2022-24546	Microsoft Windows DWM Core ライブラリの権限が昇格される脆弱性 (CVE-2022-24546)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Microsoft Windows DWM Core Library Elevation of Privilege (CVE-2022-24546)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0154	CVE-2022-28265	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28265)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28265)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0175	CVE-2022-28252	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28252)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28252)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0169	CVE-2022-28249	Adobe Acrobat および Reader の領域外のメモリ参照の脆弱性 (APSB22-16: CVE-2022-28249)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Read (APSB22-16: CVE-2022-28249)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0187	CVE-2022-27785	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-16: CVE-2022-27785)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Use After Free (APSB22-16: CVE-2022-27785)］保護機能を探し、保護機能の設定を編集します。
高	2022年4月12日	CPAI-2022-0158	CVE-2022-28236	Adobe Acrobat および Reader の領域外メモリへの書き出しの脆弱性 (APSB22-16: CVE-2022-28236)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Adobe Acrobat and Reader Out-of-bounds Write (APSB22-16: CVE-2022-28236)］保護機能を探し、保護機能の設定を編集します。