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7月12日	CPAI-2022-0361	CVE-2022-30202	Microsoft Windows ALPC (高度なローカル プロシージャ呼び出し) の特権が昇格される脆弱性 (CVE-2022-30202)	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 Advanced Local Procedure Call Elevation of Privilege (CVE-2022-30202)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0399	CVE-2022-34219	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34219)	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 (APSB22-32: CVE-2022-34219)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0383	CVE-2022-34236	Adobe Acrobat および Reader の領域外のメモリ参照 (APSB22-32: CVE-2022-34236)	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 (APSB22-32: CVE-2022-34236)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0360	CVE-2022-30220	Microsoft Windows ストレージの特権が昇格される脆弱性 (CVE-2022-30220)	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 Storage Elevation of Privilege (CVE-2022-30220)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0398	CVE-2022-34222	Adobe Acrobat および Reader の領域外のメモリ参照 (APSB22-32: CVE-2022-34222)	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 (APSB22-32: CVE-2022-34222)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0382	CVE-2022-34220	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34220)	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 (APSB22-32: CVE-2022-34220)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0397	CVE-2022-34221	Adobe Acrobat および Reader の型の取り違えの脆弱性 (APSB22-32: CVE-2022-34221)	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 Access of Resource Using Incompatible Type (APSB22-32: CVE-2022-34221)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0381	CVE-2022-34223	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34223)	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 (APSB22-32: CVE-2022-34223)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0396	CVE-2022-34234	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34234)	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 (APSB22-32: CVE-2022-34234)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0380	CVE-2022-34217	Adobe Acrobat および Reader の領域外メモリへの書き出し (APSB22-32: CVE-2022-34217)	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 (APSB22-32: CVE-2022-34217)］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7月12日	CPAI-2022-0395	CVE-2022-34230	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34230)	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 (APSB22-32: CVE-2022-34230)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0379	CVE-2022-34237	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34237)	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 (APSB22-32: CVE-2022-34237)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0394	CVE-2022-34233	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34233)	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 (APSB22-32: CVE-2022-34233)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月12日	CPAI-2022-0378	CVE-2022-34216	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34216)	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 (APSB22-32: CVE-2022-34216)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月20日	CPAI-2022-0324	CVE-2022-31460	Owl Labs Meeting Owl の認証が回避される脆弱性 (CVE-2022-31460)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Owl Labs Meeting Owl Authentication Bypass (CVE-2022-31460)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月20日	CPAI-2017-1304	CVE-2017-5030	Google Chrome ブラウザ V8 のメモリ破損の脆弱性 (CVE-2017-5030)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Google Chrome Browser V8 Memory Corruption (CVE-2017-5030)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月20日	CPAI-2022-0357	CVE-2022-27924	Zimbra Collaboration の CRLF インジェクション (CVE-2022-27924)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Zimbra Collaboration CRLF Injection (CVE-2022-27924)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月20日	CPAI-2022-0339	CVE-2022-23642	Sourcegraph のコマンドインジェクション (CVE-2022-23642)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Sourcegraph Command Injection (CVE-2022-23642)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年7月25日	CPAI-2021-1223	CVE-2021-41403	FlatCore CMS のサーバサイドのリクエストフォージェリ (CVE-2021-41403)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［FlatCore CMS Server-Side Request Forgery (CVE-2021-41403)］保護機能を探し、保護機能の設定を編集します。
高	2022年7月26日	CPAI-2020-3543	CVE-2020-4280	IBM QRadar SIEM の安全でないデシリアライゼーション (CVE-2020-4280)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［IBM QRadar SIEM Insecure Deserialization (CVE-2020-4280)］保護機能を探し、保護機能の設定を編集します。