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7月26日	CPAI-2020-3466	CVE-2020-11117	Qualcomm Snapdragon のリモートからコードを実行される脆弱性 (CVE-2020-11117)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Qualcomm Snapdragon Remote Code Execution (CVE-2020-11117)］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27日	CPAI-2022-0458	CVE-2022-36408	PrestaShop のコマンドインジェクション (CVE-2022-36408)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［PrestaShop Command Injection (CVE-2022-36408)］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27日	CPAI-2022-0454	CVE-2022-32417	PbootCMS のリモートからコードを実行される脆弱性 (CVE-2022-32417)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［PbootCMS Remote Code Execution (CVE-2022-32417)］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28日	CPAI-2022-0425	CVE-2022-32035	Tenda M3 ルータのバッファオーバーフロー (CVE-2022-32035)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Tenda M3 Router Buffer Overflow (CVE-2022-32035)］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28日	CPAI-2022-0373		HTTP ペイロードの CRLF インジェクション	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［HTTP Payload CRLF Injection］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28日	CPAI-2022-0433		HTTP ペイロードの Eメール ヘッダ インジェクション	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［HTTP Payload Email Header Injection］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28日	CPAI-2022-0432	CVE-2022-25237	Bonitasoft Bonita Web の認証を回避される脆弱性 (CVE-2022-25237)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Bonitasoft Bonita Web Authorization Bypass (CVE-2022-25237)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年8月2日	CPAI-2022-0403	CVE-2022-24562	IOBit IOTransfer の任意のファイル書き込みの脆弱性 (CVE-2022-24562)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［IOBit IOTransfer Arbitrary File Write (CVE-2022-24562)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月7日	CPAI-2022-0426		BitTorrent プロトコル	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［BitTorrent Protocol］保護機能を探し、保護機能の設定を編集します。
緊急	2022年8月7日	CPAI-2018-1804	CVE-2018-3991	WibuKey Network Server Management のヒープオーバーフロー (CVE-2018-3991)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［WibuKey Network Server Management Heap Overflow (CVE-2018-3991)］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8月9日	CPAI-2022-0508	CVE-2022-35667	Adobe Acrobat および Reader の領域外メモリへの書き出し (APSB22-39: CVE-2022-35667)	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 (APSB22-39: CVE-2022-35667)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0476	CVE-2022-35756	Microsoft Windows Kerberos の特権が昇格される脆弱性 (CVE-2022-35756)	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 Kerberos Elevation of Privilege (CVE-2022-35756)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0506	CVE-2022-35678	Adobe Acrobat および Reader の領域外のメモリ参照 (APSB22-39: CVE-2022-35678)	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 (APSB22-39: CVE-2022-35678)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0474		Microsoft Windows 印刷スプーラーで特権が昇格される脆弱性 (CVE-2022-35793)	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 Print Spooler Elevation of Privilege (CVE-2022-35793)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0504	CVE-2022-35665	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-39: CVE-2022-35665)	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 (APSB22-39: CVE-2022-35665)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0471	CVE-2022-34713	Microsoft Windows サポート診断ツール (MSDT) のリモートからコードを実行される脆弱性 (CVE-2022-34713)	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 Support Diagnostic Tool (MSDT) Remote Code Execution (CVE-2022-34713)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0503	CVE-2022-35671	Adobe Acrobat および Reader の領域外のメモリ参照 (APSB22-39: CVE-2022-35671)	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 (APSB22-39: CVE-2022-35671)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0470	CVE-2022-35750	Microsoft Win32k の特権が昇格される脆弱性 (CVE-2022-35750)	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 Win32k Elevation of Privilege (CVE-2022-35750)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0502	CVE-2022-35668	Adobe Acrobat および Reader の不適切な入力バリデーション (APSB22-39: CVE-2022-35668)	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 Improper Input Validation (APSB22-39: CVE-2022-35668)］保護機能を探し、保護機能の設定を編集します。
高	2022年8月9日	CPAI-2022-0501	CVE-2022-35666	Adobe Acrobat および Reader の不適切な入力バリデーション (APSB22-39: CVE-2022-35666)	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 Improper Input Validation (APSB22-39: CVE-2022-35666)］保護機能を探し、保護機能の設定を編集します。