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20日	CPAI-2022-0203	CVE-2022-21279	Oracle MySQL クラスタのバッファオーバーフロー (CVE-2022-21279)	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 MySQL Cluster Buffer Overflow (CVE-2022-21279)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年4月25日	CPAI-2021-1162	CVE-2021-45427	Emerson XWEB 300D のディレクトリトラバーサル (CVE-2021-45427)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Emerson XWEB 300D Directory Traversal (CVE-2021-45427)］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27日	CPAI-2021-1165	CVE-2021-42278 CVE-2021-42287	Microsoft Windows Active Directory で権限が昇格される複数の脆弱性 (CVE-2021-42278; CVE-2021-42287)	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 Active Directory Privilege Escalation Multiple Vulnerabilities］保護機能を探し、保護機能の設定を編集します。
緊急	2022年4月27日	CPAI-2022-0189	CVE-2022-25060	TP-LINK TL-WR840N のコマンドインジェクション (CVE-2022-25060)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［TP-LINK TL-WR840N Command Injection (CVE-2022-25060)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年4月27日	CPAI-2022-0206	CVE-2022-22954	VMware Workspace のリモートからコードを実行される脆弱性 (CVE-2022-22954)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［VMware Workspace Remote Code Execution (CVE-2022-22954)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2021-1163	CVE-2021-31805	Apache Struts のリモートからコードを実行される脆弱性 (CVE-2021-31805)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Apache Struts Remote Code Execution (CVE-2021-31805)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2022-0207	CVE-2022-25075	TOTOLink A3000R のコマンドインジェクション (CVE-2022-25075)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［TOTOLink A3000R Command Injection (CVE-2022-25075)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2022-0213	CVE-2022-26258	D-Link DIR-820L のコマンドインジェクション (CVE-2022-26258)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［D-Link DIR-820L Command Injection (CVE-2022-26258)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2022-0200	CVE-2022-25077	TOTOLink A3100R コマンドインジェクション (CVE-2022-25077)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［TOTOLink A3100R Command Injection (CVE-2022-25077)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2021-1166	CVE-2021-46367	RiteCMS リモートからコードを実行される脆弱性 (CVE-2021-46367)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［RiteCMS Remote Code Execution (CVE-2021-46367)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2022-0108	CVE-2022-20699	Cisco Small Business RV シリーズのルータのサービス拒否 (DoS) 攻撃 (CVE-2022-20699)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Cisco Small Business RV Series Routers Denial Of Service (CVE-2022-20699)］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
緊急	2022年5月2日	CPAI-2021-1147	CVE-2021-44622 CVE-2021-44623 CVE-2021-44625 CVE-2021-44626 CVE-2021-44627 CVE-2021-44628 CVE-2021-44629 CVE-2021-44630 CVE-2021-44631 CVE-2021-44632	TP-LINK WR-886N の複数のバッファオーバーフローの脆弱性 (CVE-2021-44622; CVE-2021-44623; CVE-2021-44625; CVE-2021-44626; CVE-2021-44627; CVE-2021-44628; CVE-2021-44629; CVE-2021-44630; CVE-2021-44631; CVE-2021-44632)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［TP-LINK WR-886N Multiple Buffer Overflow Vulnerabilities］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2021-1167	CVE-2021-43118	Draytek Vigor のコマンドインジェクションの脆弱性 (CVE-2021-43118)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Draytek Vigor Command Injection (CVE-2021-43118)］保護機能を探し、保護機能の設定を編集します。
高	2022年5月2日	CPAI-2010-0670	CVE-2010-4345	Exim のリモートからコードを実行される脆弱性 (CVE-2010-4345)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Exim Remote Code Execution (CVE-2010-4345)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2022-0213	CVE-2022-26258	D-Link DIR-820L のコマンドインジェクションの脆弱性 (CVE-2022-26258)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［D-Link DIR-820L Command Injection (CVE-2022-26258)］保護機能を探し、保護機能の設定を編集します。
高	2022年5月2日	CPAI-2021-1166	CVE-2021-46367	RiteCMS のリモートからコードを実行される脆弱性 (CVE-2021-46367)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［RiteCMS Remote Code Execution (CVE-2021-46367)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月2日	CPAI-2022-0208	CVE-2022-27115	Studio-42 elFinder のリモートからコードを実行される脆弱性 (CVE-2022-27115)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Studio-42 elFinder Remote Code Execution (CVE-2022-27115)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年5月3日	CPAI-2022-0219	CVE-2022-29464	WSO2 の複数製品に発見されたリモートからコードを実行される脆弱性 (CVE-2022-29464)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［WSO2 Multiple Products Remote Code Execution (CVE-2022-29464)］保護機能を探し、保護機能の設定を編集します。
高	2022年5月3日	CPAI-2022-0209	CVE-2022-21371	Oracle WebLogic Server のリモートからコードを実行される脆弱性 (CVE-2022-21371)	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 WebLogic Server Remote Code Execution (CVE-2022-21371)］保護機能を探し、保護機能の設定を編集します。
高	2022年5月8日	CPAI-2020-3464	CVE-2020-26950	Mozilla Firefox の解放後メモリ利用の脆弱性 (CVE-2020-26950)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Mozilla Firefox Use After Free (CVE-2020-26950)］保護機能を探し、保護機能の設定を編集します。