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11月22日	CPAI-2022-0886	CVE-2022-28575 CVE-2022-28577 CVE-2022-28578 CVE-2022-28579 CVE-2022-28580 CVE-2022-28581 CVE-2022-28582 CVE-2022-28583 CVE-2022-28584	TOTOLINK A7100RU ルータのコマンドインジェクション (CVE-2022-28575; CVE-2022-28577; CVE-2022-28578; CVE-2022-28579; CVE-2022-28580; CVE-2022-28581; CVE-2022-28582; CVE-2022-28583; CVE-2022-28584)	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 A7100RU Router Command 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11月21日	CPAI-2019-2526	CVE-2019-10068	Kentico CMS のリモートからコードを実行される脆弱性 (CVE-2019-10068)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Kentico CMS Remote Code Execution (CVE-2019-10068)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月22日	CPAI-2022-0891	CVE-2022-25064	TP-Link TL-WR840N のコマンドインジェクション (CVE-2022-25064)	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-2022-25064)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月22日	CPAI-2018-2134	CVE-2018-15381	Cisco Unity Express の安全でないデシアライゼーション (CVE-2018-15381)	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 Unity Express Insecure Deserialization (CVE-2018-15381)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月22日	CPAI-2020-3609	CVE-2020-27868	Qognify Ocularis の安全でないデシアライゼーション (CVE-2020-27868)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Qognify Ocularis Insecure Deserialization (CVE-2020-27868)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月22日	CPAI-2022-0903	CVE-2022-26272	IonizeCMS のリモートからコードを実行される脆弱性 (CVE-2022-26272)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［IonizeCMS Remote Code Execution (CVE-2022-26272)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月23日	CPAI-2022-0911	CVE-2022-1162	GitLab のハードコードされた認証情報 (CVE-2022-1162)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［GitLab Hardcoded Credentials (CVE-2022-1162)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月23日	CPAI-2022-0924	CVE-2022-36267	Airspan AirSpot 5410 のコマンドインジェクション (CVE-2022-36267)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Airspan AirSpot 5410 Command Injection (CVE-2022-36267)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月23日	CPAI-2022-0925	CVE-2022-37130	D-Link DIR-816 のコマンドインジェクション (CVE-2022-37130)	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-816 Command Injection (CVE-2022-37130)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月23日	CPAI-2022-0929	CVE-2022-37661	SmartRG ルータのコマンドインジェクション (CVE-2022-37661)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［SmartRG Routers Command Injection (CVE-2022-37661)］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11月23日	CPAI-2022-0906	CVE-2022-38621	Doufox で任意のファイルがアップロードされる脆弱性 (CVE-2022-38621)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Doufox Arbitrary File Upload (CVE-2022-38621)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月24日	CPAI-2021-1377	CVE-2021-21669	Jenkins Generic Webhook Trigger プラグインの外部エンティティ インジェクション (CVE-2021-21669)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Jenkins Generic Webhook Trigger Plugin External Entity Injection (CVE-2021-21669)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月24日	CPAI-2022-0881	CVE-2022-31885	Marval MSM のリモートからコードを実行される脆弱性 (CVE-2022-31885)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Marval MSM Remote Code Execution (CVE-2022-31885)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月24日	CPAI-2022-0890	CVE-2022-30450	WaimairenCMS のリモートからコードを実行される脆弱性 (CVE-2022-30450)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［WaimairenCMS Remote Code Execution (CVE-2022-30450)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月24日	CPAI-2022-0704		Open Web Analytics の情報漏洩の脆弱性 (CVE-2022-24637)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Open Web Analytics Information Disclosure (CVE-2022-24637)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月27日	CPAI-2022-0939	CVE-2022-34974	D-Link DIR810LA1 のコマンドインジェクション (CVE-2022-34974)	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 DIR810LA1 Command Injection (CVE-2022-34974)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月27日	CPAI-2022-0943	CVE-2022-37057	D-Link GO-RT-AC750 のコマンドインジェクション (CVE-2022-37057)	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 GO-RT-AC750 Command Injection (CVE-2022-37057)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月27日	CPAI-2022-0950	CVE-2022-21186	Acrontum Filesystem-Template パッケージのコマンドインジェクション (CVE-2022-21186)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Acrontum Filesystem-Template Package Command Injection (CVE-2022-21186)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月28日	CPAI-2021-1430	CVE-2021-22802	Schneider Electric IGSS のバッファオーバーフロー (CVE-2021-22802)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Schneider Electric IGSS Buffer Overflow (CVE-2021-22802)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月28日	CPAI-2022-0926	CVE-2022-26213	TOTOLINK X5000R のコマンドインジェクション (CVE-2022-26213)	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 X5000R Command Injection (CVE-2022-26213)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年11月28日	CPAI-2021-1431	CVE-2021-22823	Schneider Electric IGSS で任意のファイルが削除される脆弱性 (CVE-2021-22823)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Schneider Electric IGSS Arbitrary File Deletion (CVE-2021-22823)］保護機能を探し、保護機能の設定を編集します。