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1月2日	CPAI-2017-1216	CVE-2017-5645	Apache Log4j のリモートからコードを実行される脆弱性 (CVE-2017-5645)	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 Log4j Remote Code Execution (CVE-2017-5645)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年1月4日	CPAI-2020-3444	CVE-2020-25366	D-Link のサービス拒否（DoS）の脆弱性 (CVE-2020-25366)	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 Denial Of Service (CVE-2020-25366)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2021-1049	CVE-2021-44702 APSB22-01	Adobe Acrobat および Reader の不適切なアクセス制御の脆弱性 (APSB22-01: CVE-2021-44702)	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 Access Control (APSB22-01: CVE-2021-44702)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2022-0006	CVE-2022-21887	Microsoft Win32k の特権の昇格の脆弱性 (CVE-2022-21887)	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-2022-21887)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2022-0007	CVE-2022-21882	Microsoft Windows Win32k の特権の昇格の脆弱性 (CVE-2022-21882)	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-2022-21882)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2022-0005	CVE-2022-21897	Microsoft Windows の共通ログ ファイル システム ドライバーの特権の昇格の脆弱性 (CVE-2022-21897)	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 Common Log File System Driver Elevation of Privilege (CVE-2022-21897)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2022-0003	CVE-2022-21919	Microsoft Windows User Profile Service の特権の昇格の脆弱性 (CVE-2022-21919)	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 User Profile Service Elevation of Privilege (CVE-2022-21919)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2021-1045	CVE-2021-45062 APSB22-01	Adobe Acrobat および Reader の解放済みメモリ使用の脆弱性 (APSB22-01: CVE-2021-45062)	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 (APSB22-01: CVE-2021-45062)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2022-0011	CVE-2021-44740	Adobe Acrobat および Reader の NULL ポインタデリファレンスの脆弱性 (APSB22-01: CVE-2021-44740)	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 NULL Pointer Dereference (APSB22-01: CVE-2021-44740)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2022-0002	CVE-2022-21908	Microsoft Windows インストーラの特権の昇格の脆弱性 (CVE-2022-21908)	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 Installer Elevation of Privilege (CVE-2022-21908)］保護機能を探し、保護機能の設定を編集します。
高	2022年1月11日	CPAI-2022-0006	CVE-2022-21887	Microsoft Win32k の特権の昇格の脆弱性 (CVE-2022-21887)	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-2022-21887)］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1月16日	CPAI-2020-0385	CVE-2020-4427	IBM Data Risk Manager の認証を回避される脆弱性 (CVE-2020-4427)	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 Data Risk Manager Authentication Bypass (CVE-2020-4427)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年1月23日	CPAI-2021-1056	CVE-2021-42392	H2 Database Console のリモートからコードを実行される脆弱性 (CVE-2021-42392)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［H2 Database Console Remote Code Execution (CVE-2021-42392)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年2月2日	CPAI-2021-1061	CVE-2021-32648	October CMS の認証を回避される脆弱性 (CVE-2021-32648)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［October CMS Authentication Bypass (CVE-2021-32648)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年2月6日	CPAI-2021-1065	CVE-2021-20038	SonicWall SMA100 のバッファオーバーフロー (CVE-2021-20038)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［SonicWall SMA100 Buffer Overflow (CVE-2021-20038)］保護機能を探し、保護機能の設定を編集します。
高	2022年2月6日	CPAI-2022-0023		D-Link ルータの Cookie のコマンドインジェクション	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［D-Link Routers Cookie 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2月6日	CPAI-2021-0894	CVE-2021-42237	Sitecore XP のリモートからコードを実行される脆弱性 (CVE-2021-42237)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Sitecore XP Remote Code Execution (CVE-2021-42237)］保護機能を探し、保護機能の設定を編集します。
緊急	2022年1月11日	CPAI-2022-0015	CVE-2022-21907	Microsoft HTTP プロトコル スタックでリモートからコードを実行される脆弱性 (CVE-2022-21907)	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 HTTP Protocol Stack Remote Code Execution (CVE-2022-21907)］保護機能を探し、保護機能の設定を編集します。
高	2022年2月8日	CPAI-2022-0029	CVE-2022-21989	Microsoft Windows Kernel の特権が昇格される脆弱性 (CVE-2022-21989)	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 Kernel Elevation of Privilege (CVE-2022-21989)］保護機能を探し、保護機能の設定を編集します。
高	2022年2月8日	CPAI-2022-0024	CVE-2022-22715	Microsoft の名前付きパイプファイルシステムで特権が昇格される脆弱性 (CVE-2022-22715)	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 Named Pipe File System Elevation of Privilege (CVE-2022-22715)］保護機能を探し、保護機能の設定を編集します。
高	2022年2月8日	CPAI-2022-0025	CVE-2022-22718	Microsoft Windows の印刷スプーラーで特権が昇格される脆弱性 (CVE-2022-22718)	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-2022-22718)］保護機能を探し、保護機能の設定を編集します。