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6月28日	CPAI-2016-1186	CVE-2016-5198	Google Chrome のリモートからコードを実行される脆弱性 (CVE-2016-5198)	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 Remote Code Execution (CVE-2016-5198)］保護機能を探し、保護機能の設定を編集します。
高	2022年6月29日	CPAI-2016-1187	CVE-2016-1646	Google Chrome の領域外のメモリ参照 (CVE-2016-1646)	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 Out-of-Bounds Read (CVE-2016-1646)］保護機能を探し、保護機能の設定を編集します。
高	2022年6月30日	CPAI-2022-0325	CVE-2022-22620	Apple OS 解放済みのメモリ使用 (CVE-2022-22620)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Apple OS Use After Free (CVE-2022-22620)］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3日	CPAI-2022-0334	CVE-2022-29535	Zoho ManageEngine OPManager の SQL インジェクション (CVE-2022-29535)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Zoho ManageEngine OPManager SQL Injection (CVE-2022-29535)］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4日	CPAI-2022-0359	CVE-2022-28219	Zoho ManageEngine ADAudit Plus のリモートからコードを実行される脆弱性 (CVE-2022-28219)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Zoho ManageEngine ADAudit Plus Remote Code Execution (CVE-2022-28219)］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6日	CPAI-2017-1310	CVE-2017-20029 CVE-2017-20032	PHPList の SQL インジェクション (CVE-2017-20029; CVE-2017-20032)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［PHPList SQL Injection (CVE-2017-20029; CVE-2017-20032)］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7日	CPAI-2022-0336	CVE-2022-21993	Microsoft Windows NFS ONCRPC XDR Driver の情報漏えい (CVE-2022-21993)	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 NFS ONCRPC XDR Driver Information Disclosure (CVE-2022-21993)］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10日	CPAI-2022-0370	CVE-2022-31362	Docebo Community Edition の任意のファイルがアップロードされる脆弱性 (CVE-2022-31362)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Docebo Community Edition Arbitrary File Upload (CVE-2022-31362)］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11日	CPAI-2022-0338	CVE-2022-31279	Laravel のリモートからコードを実行される脆弱性 (CVE-2022-31279)	SmartDashboard の［IPS］タブを選択し、［Protections］を選択します。検索機能を使って［Laravel Remote Code Execution (CVE-2022-31279)］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-2022-0393	CVE-2022-34232	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34232)	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-2022-34232)］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-2022-0377	CVE-2022-34215	Adobe Acrobat および Reader の領域外のメモリ参照 (APSB22-32: CVE-2022-34215)	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-2022-34215)］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-2022-0392	CVE-2022-34215	Adobe Acrobat および Reader の領域外のメモリ参照 (APSB22-32: CVE-2022-34215)	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-2022-34215)］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-2022-0376	CVE-2022-34227	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34227)	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-2022-34227)］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-2022-0386	CVE-2022-34228	Adobe Acrobat および Reader の初期化されていないポインタ アクセス (APSB22-32: CVE-2022-34228)	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 Uninitialized Pointer (APSB22-32: CVE-2022-34228)］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-2022-0363	CVE-2022-22034	Microsoft Windows Graphics コンポーネントの 特権が昇格される脆弱性 (CVE-2022-22034)	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 Graphics Component Elevation of Privilege (CVE-2022-22034)］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-2022-0401	CVE-2022-34229	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34229)	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-2022-34229)］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-2022-0385	CVE-2022-34224	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34224)	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-2022-34224)］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-2022-0362	CVE-2022-22047	Microsoft Windows クライアント/サーバーのランタイム サブシステムで特権が昇格される脆弱性 (CVE-2022-22047)	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 Client/Server Runtime Subsystem Elevation of Privilege (CVE-2022-22047)］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-2022-0400	CVE-2022-34239	Adobe Acrobat および Reader の領域外のメモリ参照 (APSB22-32: CVE-2022-34239)	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-2022-34239)］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-2022-0384	CVE-2022-34225	Adobe Acrobat および Reader の解放後メモリ利用の脆弱性 (APSB22-32: CVE-2022-34225)	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-2022-34225)］保護機能を探し、保護機能の設定を編集します。