

O2next 義肢装具業務支援クラウドシステム

医療現場の業務を、
安全に、未来へつなぐ。

患者情報を守る、 O2nextのセキュリティ。

O2nextは、患者情報や病院情報を扱う義肢装具業務支援クラウドシステムです。
ログイン認証や通信の暗号化、定例バックアップ、Web攻撃対策を組み合わせ、
システムとデータを守っています。



O2nextで実施している主なセキュリティ対策



ログイン認証

ID・パスワード／
Google・Microsoft連携



アクセス制御

役割・権限に応じて
利用機能を制御



通信の暗号化

HTTPS/TLSで
通信を保護



国内クラウド

国内のクラウド環境で
保管・運用

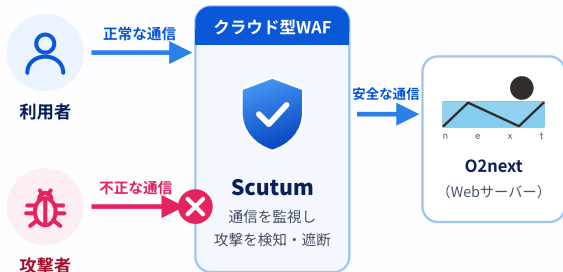


定例バックアップ

定期的にバックアップ
手順に沿って復旧

Web攻撃対策 クラウド型WAF「Scutum（スキュータム）」

O2nextは、Web攻撃を防ぐ仕組みであるクラウド型WAF「Scutum」を、Webサーバーの前面に導入しています。
すべての通信を監視し、システムの弱点（脆弱性）を突いて情報を盗み出す攻撃などから、O2nextを守ります。



24時間365日

Scutumの専門チームが
監視・保守

99.999%以上

Scutumの稼働率
(2024年までの5年間の実績)

24時間以内

重大な脆弱性が公表されてから
防御を更新するまで

AI型WAF

正常な通信を誤って止める
「誤検知」を大幅に軽減

Scutumが防御できる主な攻撃

パスワードへの攻撃

総当たり・パスワードリスト攻撃
(パスワードの不正な試行)

不正な命令

SQLインジェクション ほか
(データベースなどへの不正な命令)

利用者側への攻撃

クロスサイトスクリプティング ほか
(不正なプログラムの埋め込み)

情報の不正な閲覧

パストラバーサル ほか
(公開していないファイルの閲覧)

ソフトウェアの弱点

Apache Log4j等の脆弱性を狙った攻撃
(広く使われる部品の弱点を突く)

サービス妨害

DoS攻撃 ほか
(大量の通信でサービスを止める)

クラウド型WAF市場 12年連続シェアNo.1 2009年のサービス開始以来、金融機関や公的機関を含む多数のWebサイトで稼働

※Scutumに関する記載は、株式会社セキュアスカイ・テクノロジーの資料（2026年5月）に基づきます。シェアは同資料に記載の調査会社の調査によるものです。防御できる攻撃は代表例であり、すべての攻撃を防御するものではありません。

※本資料の内容は2026年10月時点のものです。記載の製品名・サービス名は、各社の商標または登録商標です。

