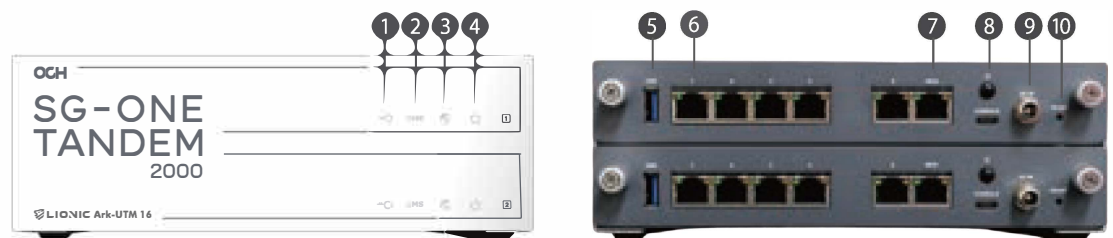


[製品仕様]



- 1 License
- 2 CMS
- 3 Internet
- 4 Power
- 5 USB
- 6 LAN (1-5)
- 7 WAN
- 8 Power
- 9 DC IN
- 10 Reset

シリーズ名	SG-ONE TANDEM			
モデル名	2000			
型番	SG-O2000	SG-O2000S	SG-O2000H	SG-O2000SH
リモート駆除	—	あり	—	あり
サイバー保険	—	—	あり	あり
ハードウェア	CPU : Marvell 7040 ARM Cortex A72, Dual-core CPU 1.4 Ghz			
	Memory : 4GB			
	Flash : 2GB			
	LAN : 10x RJ45(2x5LAN)			
	WAN : 2x RJ45(1 WAN)			
インジケータランプ	Power Status, Internet Active, CMS Status, License Active			
電源	2x DC 12V/40W Power adapter with 2x Japanese Power codes			
温度範囲 耐久性	0~40℃			
寸法	208W×69H×150D(mm)			
認証	VCCI/Telec T			
保守	5年 / 6年 / 7年			

セキュリティ性能 (UTM) 約900Mbps (脅威保護スループット)※
 ※ファイアウォール、アンチウイルス および IPSがON。当社の試験環境にて測定した結果です。

提供サービス

- ・本体(ライセンス 5年/6年/7年) ・先出しセンドバック保守
- ・フォームからの問い合わせ (保守問い合わせ対応、操作 / 設定方法)
- ・本体マニュアルの提供 ・ウイルス駆除サービス ・サイバー保険 ・CMSサーバー

導入のご相談、お問い合わせはこちらから



お見積はこちらからご依頼ください



SG-ONE TANDEM

秒刻みの脅威から
 2つのUTMで守り抜く
 大企業レベルのセキュリティをあなたのものに



〒900-0029
 沖縄県那覇市旭町1番地9 カフーナ旭橋B街区ビル3階

WEBサイト <https://www.och.co.jp/>

お問合せ先 sales@och.co.jp

筐体1台で高可用性

故障時の通信やセキュリティも安心!

(HA機能)を実装!

これまでにない新時代のUTM

POINT.01

高可用性

UTMの2重化により、
ネットワークの通信断が発生した場合、
スタンバイ用の機器に
自動的に切り替わり
ネットワークの接続を確保します。
ネットワークが突然止まる
心配がありません。

POINT.02

端末無制限

デスクトップパソコン、ノートパソコン、
タブレットやスマートフォンはもちろんのこと、
ネットワークカメラやサーバーなど
社内の機器を無制限に接続できます。

※快適な動作は光回線1Gbps100台
前後を推奨します。

POINT.03

圧倒的な スループット

セキュリティ性能を
有効にした状態でも
高速スキャン約900Mbpsで
業界最速クラスの
処理速度で
業務の遅延無く利用できます。

難しい操作

は一切不要!

届いたらお手軽

に設置が可能!

POINT.04

安心の セキュリティ保護

セキュリティ業界が認定した
ウイルスデータベースで、
ネットワークを最新の脅威や
ウイルスから保護します。
企業に求めるサイバー攻撃対策を
この1台でカバー
することができます。

直観的なユーザーインターフェースにより、機器の設

定や脅威ログをいつでもご覧いただくことが可能です。

[高可用性 (HA機能) とは?]

TANDEM は筐体の中に2つのUTM が格納されています。
これにより、冗長構成を保ち、社内のインターネット環境を止めずに、且つセキュリティも継続的に担保したままご利用いただけます。

1 ネットワーク通信の障害が発生した場合

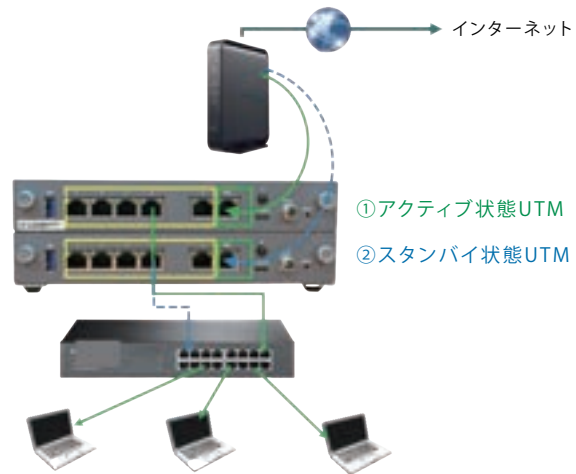
スタンバイ用の機器に自動的に切り替わり、ネットワーク接続を確保します。

2 機器故障時

万が一、故障した場合もスタンバイ用の機器に切り替わるため、交換機が到着するまでの間にセキュリティ通信がなくなってしまう心配がありません。



[設置例]



HA構成を設定した状態で出荷します。
機器到着後は3ステップで高可用性の機能をご利用いただけます。

STEP.1

ルーターとTANDEMのWANポートを接続

STEP.2

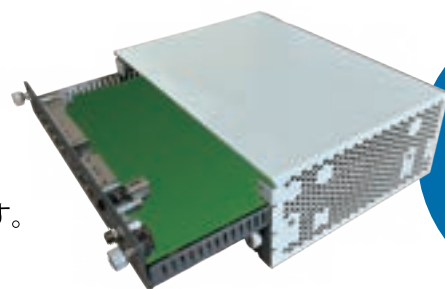
TANDEM のLANポートへ
スイッチングハブを接続

STEP.3

スイッチングハブから社内の機器を接続

[故障時の交換]

標準オプションにて、
先出しセンドバック保守サービス
が付いています。
交換時も故障しているUTM 基盤の
入れ替えにより簡単に交換が完了します。



check! /
UTMボードは
簡単に
取り替えが
できます。

[ウィルス駆除サービス]

万が一、PC がウィルス感染した場合、リモートもしくは現地訪問（離島は除く）にて、
ウィルス駆除のサポートを無料で実施します。

1 ウィルス感染



2 ウィルス駆除受付



3 リモートによるウィルス駆除



POINT!

リモート駆除が
できない場合は、
現地訪問により
ウィルス駆除



4 ウィルス 駆除完了



- ・確実にウィルスが駆除できる事を保証するサービスではありません。
- ・ウィルス感染に起因するデータ損傷・消失等の復旧は保証対象外となる可能性があります。

[サイバー保険サービス]

ウィルス駆除サービス（訪問サポート）で駆除できなかった場合、ウィルス感染による
情報漏えいの損害賠償や、システムの復旧費用として最大100万円/年を補償します。

項目	内容
補償条件	SG-ONE TANDEMを設置したネットワーク配下でマルウェアに感染してしまった場合において、SG-ONE TANDEMに対して別途定める「PC ウィルス駆除サービス」により、マルウェアの駆除が出来なかった場合のマルウェア感染による情報漏えいの損害賠償や、システムの復旧費用を補償
補償対象者(被保険者)	SG-ONE TANDEMを購入されたお客様
対象端末	Windows パソコン、Windows サーバー ※Microsoft社がサポートしているWindows OSのみ。その他のパソコンやネットワーク周辺機器は対象外
対象期間	SG-ONE TANDEMのライセンス有効期間終了まで ※SG-ONE TANDEMが正常に稼働していることが条件
補償内容	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> 保険金をお受け取り いただける主なケース </div> 賠償損害: 他人の情報の漏えいまたはそのおそれなど 費用損害: 事故原因・被害範囲調査費用や情報システム復旧費用など
補償金額	損害賠償: 最大100万円/年・費用損害: 最大100万円/年 ※賠償損害と費用損害を合わせて、100万円/年を限度とする
免責金額	賠償損害: 無し・費用損害: 無し
縮小支払割合	賠償損害: 100%・費用損害: 100%
引受保険会社	あいおいニッセイ同和損害保険株式会社
取扱保険代理店	丸紅セーフネット株式会社

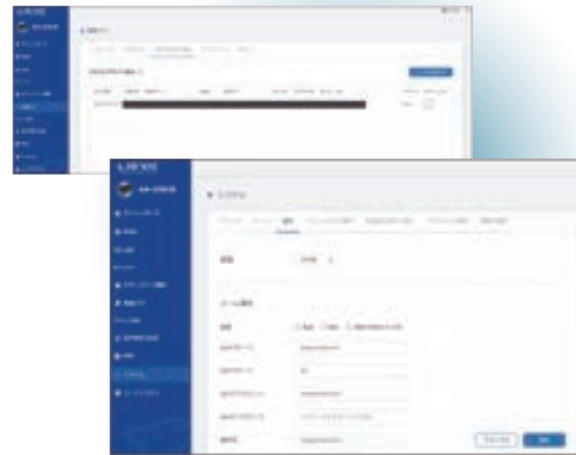


01 | ダッシュボード

現在のセキュリティ設定やウイルス検知状況、システムのリアルタイムな稼働状況など必要な情報を分かりやすくまとめています。また、PCだけでなくスマートフォンやタブレットからもお手軽に管理画面にアクセスすることができます。

02 | ウイルス検知 ログ・レポート通知

各種セキュリティスキャンで検知したログを一覧で確認することができます。確認後、ブロックしたくない通信がある場合は、そのままホワイトリストへワンクリックで追加することができます。お客様のメールサーバを設定することで、ウイルス検知状況のレポートをメール通知することができます。



03 | システム画面

機器の再起動やネットワーク設定など洗練されたデザインにより直感的な操作でご利用頂けます。定期リポート機能を備えており、指定した時刻に再起動を行います。これによりリソースがリフレッシュされて、システムの安定性がより向上します。



分類	機能
ネットワークプロテクション	セキュアファイアウォール
	侵入防御 (IPS)
	侵入検知 (IDS)
Web脅威対策	URLフィルタリング
	アンチフィッシング
	webアンチウイルス
アンチウイルス、アンチマルウェア	Windowsファイル共有 (CIFS)
	ファイル共有 (FTP)
	暗号化されていない圧縮ファイル (ZIP/GZIP/RAR)
ログ	各サービスのログ取得
自動アップデート	アンチウイルスパターンファイル
	Webフィルタリング

セキュリティ機能

- 一般的なプロトコルでのウイルス検出 (FTP, HTTP, SAMBA)
- ハイブリッドウイルススキャン
- ウイルスファイル破壊
- 実行ファイルのスキャン
- オフィスドキュメントのスキャン
- 圧縮ファイルのスキャン
- メールと添付ファイルのスキャン
- ランサムウェア検知機能の強化
- トロイの木馬検知機能の強化
- 1対多のウイルスシグネチャ
- クラウドウイルスデータベース
- サイバー攻撃ブロック
- 総当たり攻撃の検知
- ポートスキャンの検知
- DoS攻撃の検知
- プロトコル異常動作の検出
- SAMBAの不正侵入防止
- ボットネット攻撃検出
- 仮想パッチを即時更新
- 安全でない web サイトへのアクセスをブロック
- ドメイン名チェック
- URLチェック
- IPv4およびIPv6チェック
- 悪質・フィッシングサイトのクラウドデータベース
- セキュリティポリシーに応じたホワイトリスト設定
- TCPとUDP プロトコルの両方に対応したユーザー定義のファイアウォール
- 許可/拒否するwebサイトリスト
- 検出した脅威の詳細情報リスト
- 脅威ログをエクスポート (CSV形式)
- 脅威源分析、ジオブロック

ネットワーク機能

- ブリッジモードで提供
- 高可用性 (HA機能) に対応

