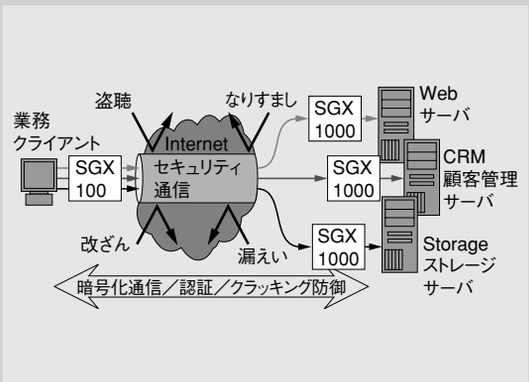
セキュリティゲートウェイ
SAFETYTUBE（セーフティチューブ） SGX1000/SGX100

セキュリティ，認証，暗号化，エンド・ツー・エンド

＊飯島　渉　Wataru Iijima

概　　要

SAFETYTUBE（セーフティチューブ） SGX1000（以下，SGX1000）及びSAFETYTUBE SGX100（以下，SGX100）は，機器相互の認証及びTCP層のペイロード部の暗号化というセキュリティ機能を装備したネットワークコンポーネントである。SGX1000及びSGX100は，暗号化機能，SGX相互認証機能，ポートフィルタリング機能などのセキュリティ機能によりネットワークのエンド・ツー・エンドにSGXシリーズを追加することで，情報漏えいや詐称・なりすましの防止が可能である。SGX1000はサーバ側への適用を意識し，19型ラックに収納可能な筐体であり，SGX100は端末側への適用を意識し，小形・軽量である。また，SGX1000/100はメンテナンス性を考慮し，ブラウザによる設定・参照が可能である。



SGXを適用した全体システム

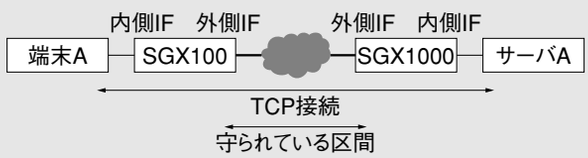
1. ま　え　が　き

Ethernet及びインターネットの普及に伴い，監視・制御分野においても各種機器の相互接続にEthernetが使われ，システムのリモート監視にインターネットを利用する傾向にある。一方，イントラネット及びインターネットを効果的に活用するために，通信路上のセキュリティ機能の実装が不可欠な状況になってきた。

本稿では，機器相互の認証及びTCPセグメントのペイロード部を暗号化するセキュリティ機能を装備したネットワークコンポーネントのSAFETYTUBE（セーフティチューブ） SGX1000（以下，SGX1000）とSAFETYTUBE SGX100（以下，SGX100）を開発したので紹介する。SGX1000とSGX100をネットワークのエンド・ツー・エンドに追加し対向させ，暗号化通信と認証機能を提供することにより，改ざんや盗聴，なりすましなどの防止が可能である。

2. 特　　長

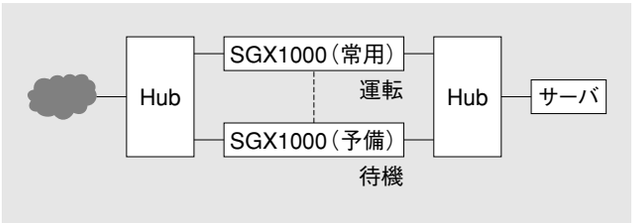
第 1 図にSGX1000とSGX100を使用したシステム構成例を示す。以下にSGX1000/100（以下，SGX）の特長を示す。



SGX：SGX100あるいはSGX1000（IPアドレスを持たない）
内側IF：端末を接続するインタフェース
外側IF：ネットワーク機器を接続するインタフェース
端末：TCP通信を行う装置（UDP，そのほかパケットも使用できるが，暗号処理はされない）

第 1 図　システム構成例
端末にSGX1000/100を実装することで，容易に安全なネットワークの構築が可能である。

＊電子機器工場



第 2 図　SGX1000を二重化した構成
SGX1000を二重化することにより，信頼性の向上が期待できる。

2.1　SGXの特長

⑴ 設置が容易　　SGXはブリッジ機能及びSGX相互での認証機能を有している。そのため，相手がSGXであれば暗号化通信，SGXでなければ通常の通信を自動的に切り替えて動作する。また，SGXはIPアドレスが不要であり，**第 1 図**に示すように，端末のすぐ近くにSGXを置いて，Ethernetケーブルで接続するだけで使用できる。従って，既存のネットワークへの導入が容易である。

⑵ 安全な通信経路　　SGX相互で認証，暗号処理，改ざん検出を実施することで，SGX間で安全な通信経路を構築できる。**第 1 図**中に「守られている区間」を示す。

⑶ 設定・参照が容易　　Webブラウザで，SGXの設定及び各種情報の参照を容易に行うことができる。

⑷ RAS（Reliability Availability Serviceability）機能　　SGX1000は，CPU温度異常・ファン回転数異常・WDT（Watch Dog Timer）監視により異常検出を行う。異常内容と二重化機能の設定により，異常時の動作として電源OFF，機能停止，再起動の動作選択が行える。SGX100はWDT監視により，異常発生時，自動再起動を行う。

⑸ 二重化対応　　**第 2 図**にSGX1000を二重化した構成を示す。SGX1000を常用と予備の2台を設置し，一方が異常又は電源OFFなどにより停止すると，他方を運転状態にすることにより通信処理の継続が可能である。

3.　機　能　概　要

第 1 表にSGXの機能概要を示す。SGXは，以下の機能を搭載している。

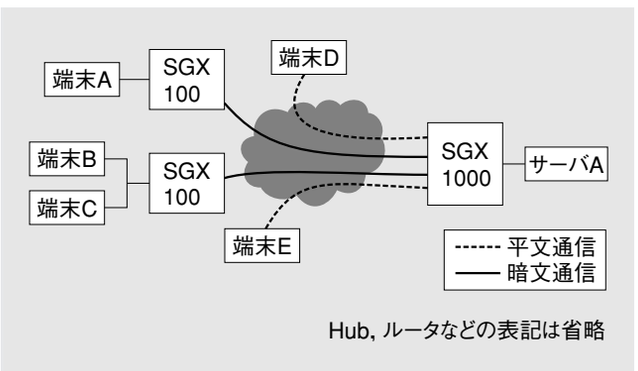
3.1　基本機能

3.1.1　暗号化通信

SGXは，IP層に依存せずにTCP層以上の層で暗号化通信や自動鍵交換を実施し，TCPセグメントのペイロード部の暗号化を実行する。暗号ロジックはAES（Advanced Encryption Standard）方式である。暗号化通信時の片方向の実効伝送速度は，SGX1000が約300Mbps，SGX100が約40Mbpsである。

第 1 表　SGX1000/100機能概要
SGX1000/100機能概要を示す。

機能	概要
アクセスコントロール	ID（Username/Password）による利用者認証及びMACアドレスによる接続機器の認証を行う。
暗号化	TCPペイロードをAESで暗号化する。
ブロッキング	SGX1000/100の有／無，IDによる利用者認証の成功／失敗により，接続のブロッキングを行う。
ポートフィルタリング	ポートの設定により，通信ポートの接続許可／拒否を行う。
ステルス化	SGX1000/100に直接接続される通信機器（サーバなど）を不可視にすることが可能。SGX1000/100はIPレスであるため，SGX1000/100も不可視となる。
通信ログ	通信ログ（成立／遮断）の収集及び通信状況の確認を行う。



第 3 図　SGX有／無が混在したシステム構成
SGX100が無しの場合でも平文通信で通信することが可能である。

3.1.2　認証

SGXは相互認証を行い，SGX間の暗号化経路を構築する。また，複数の相互認証を組み合わせることで，特定のSGX間だけ通信を許可することができる。

⑴ SGXの自動認証　　TCP接続を行う際に相手側SGXの存在を自動検出する。相手SGXが有りの場合，相手SGXの認証及び暗号処理を実施する。相手SGXが無い場合は，自分のSGX設定により切断あるいは平文通信（暗号化しないモード）を行うことができる。以上より，相手SGXが無い場合でも平文通信を行えるため，**第 3 図**で示すように混在した通信環境でも運用が可能となる。

⑵ キーワードによるグループ認証　　SGXは自

動認証とは別に，送信キーワードと受信許可キーワードによる認証を実施する。キーワードはセキュリティプロトコルに従い，ネットワークへそのまま送信されることはない。認証処理において，送信側のSGXが送信キーワードから生成したデータを送信し，相手SGXがデータを受信して，受信許可キーワードに登録されているか検証する。SGX相互で認証できた時，通信を行う。通信したいSGXは，相互に相手のキーワードを登録することでSGXのグルーピングを実現する。

⑶ HTML認証　1台の端末に1台のSGXを接続し1人で使用する時，相手側から見ると特定の人だけに許可された通信として取り扱うことができる。しかし，1台の端末を複数の人が使用したり，複数の端末をHub経由でSGXに接続した場合は，特定の人に限定した接続と見なすことができない。そのため，SGXにHTML認証機能を実装し，ユーザ／パスワードを入力するダイアログをブラウザ上に表示し，登録されたユーザのみアクセスを許可する機能を搭載した。本機能はWebアクセス限定であるが，SGXの認証とHTML認証を組み合わせることにより，特定の個人に認証を与えることが可能である。

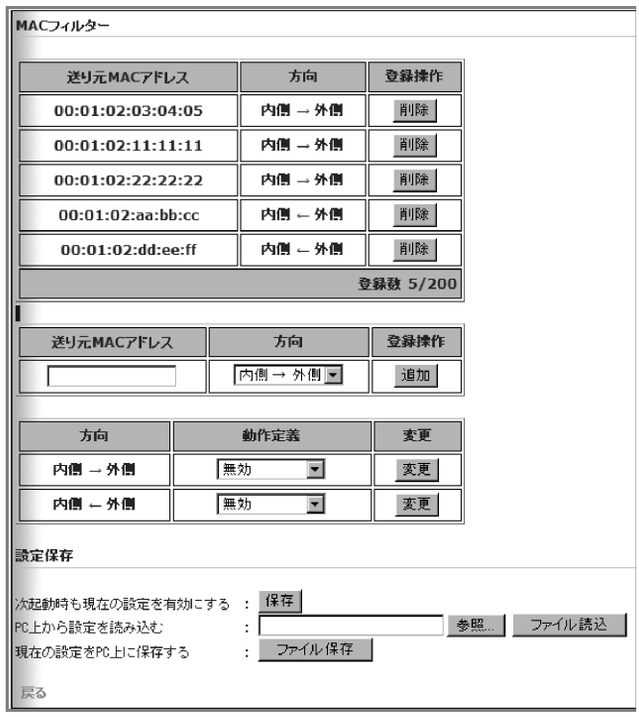
3.1.3　フィルタリング機能

⑴ MACアドレスフィルタ　　SGXは，送信元MACアドレスを監視し，設定に従ってパケットを破棄する。本機能により，SGXは接続機器を限定することが可能である。MACアドレスの設定は，内側→外側，内側←外側，各方向について指定できる。

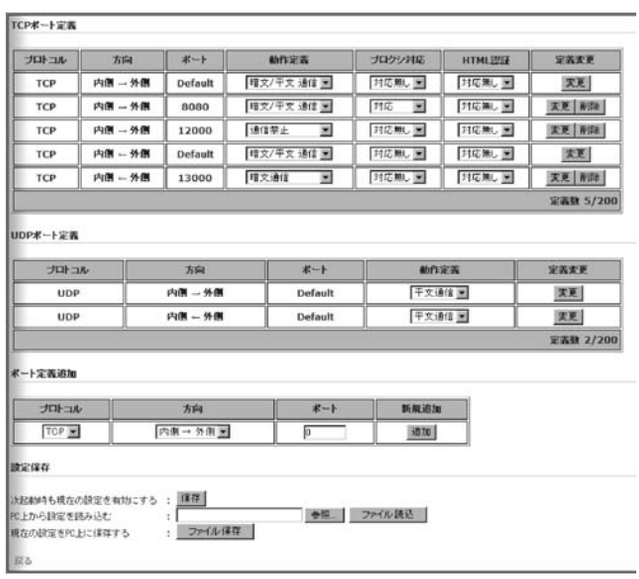
⑵ ポートフィルタリング　　SGXは，TCPとUDPの送信先ポート単位に動作を定義し，自分側のSGXと相手側のSGXの動作定義の組み合わせにより通信方法を決定する。本機能により，ポート単位でアクセスの禁止／許可，暗号化通信／平文通信の選択が可能である。

3.1.4　設定・メンテナンス機能

SGXは各種動作を指定するための設定情報及び各種ログ情報をSGX内部に格納している。この設定情報やログ情報は，ブラウザで設定や参照ができる。SGX1000はメンテナンス専用に100BASE－TXのLANポートを実装しているため，専用の保守を行うことができる。

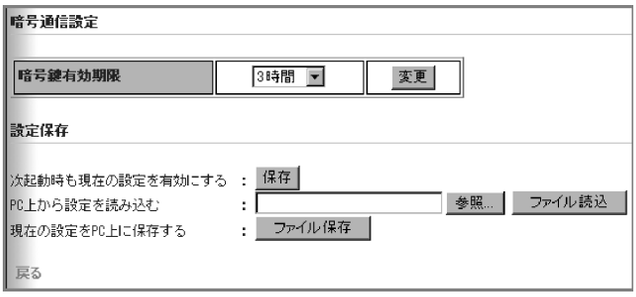


第 4 図　MACフィルタ設定用画面
「追加」「削除」「変更」ボタンを押すとその場でその設定が有効になる。

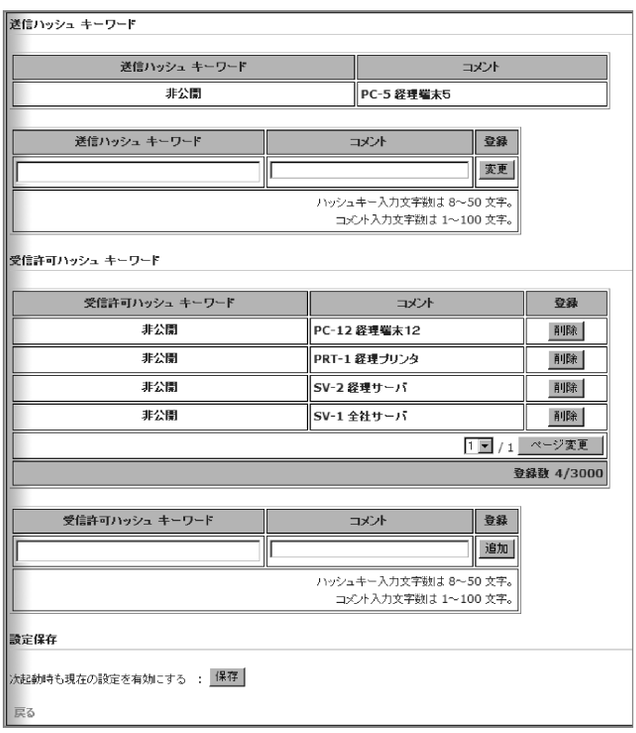


第 5 図　ポート設定用画面
TCPとUDPについて送受信方向ごとにポート単位の動作を定義する。ポート単位に定義するが，未定義のポートは上図にある4つのDefault項目に従って動作する。

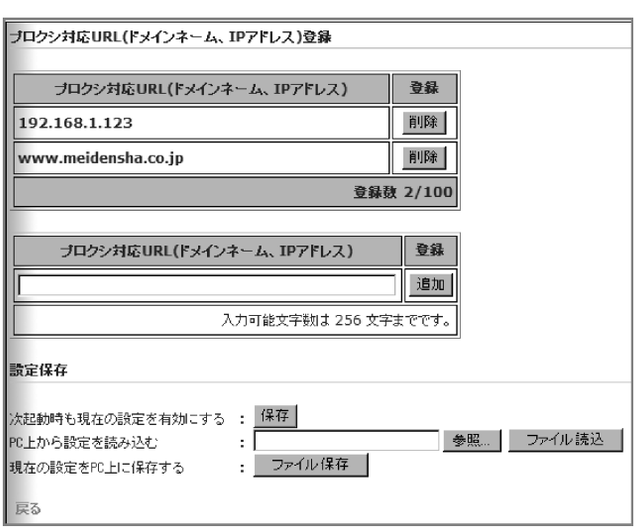
⑴ 設定　　前述の各種機能を実行するために，ブラウザから必要な情報を設定する。設定する内容は，MACアドレスフィルタ（**第 4 図**），ポート定義（**第 5 図**），暗号通信時パラメータ（**第 6 図**），認証時のキーワード（**第 7 図**），プロクシ経由時のURL（**第 8 図**）及びHTML認証用ユーザ設定（**第 9 図**）である。各設定項目の登録できる数は，



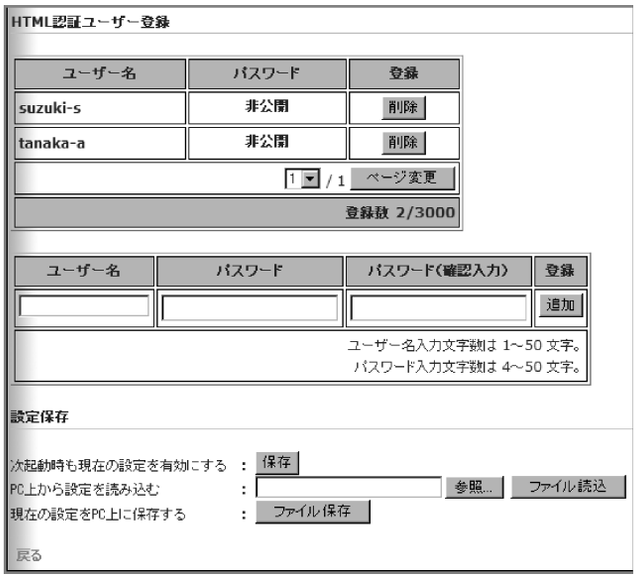
第 6 図　パラメータ設定用画面
通信相手ごとに鍵交換を行うが，同じ接続先であっても一定期間経過すると鍵交換を実施する。



第 7 図　キーワード設定用画面
認証と暗号処理は送信ハッシュキーワードと受信許可ハッシュキーワードを使用する。



第 8 図　接続先URL設定用画面
ブラウザで接続先を指定する時のURLからホスト名部分を抜き出し設定する。



第 9 図　HTML認証用設定
HTML認証時に使用する。ユーザ／パスワードをサーバ側のSGXに登録する。

第 2 表　各設定項目における最大登録数
各設定項目における最大登録数を示す。

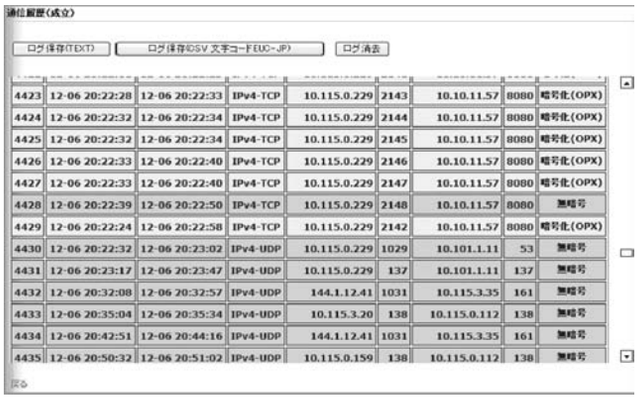
設定項目	最大登録数	
	SGX1000	SGX100
MACフィルタのMAC登録 （内側→外側, 内側←外側の合計）	200個	200個
ポート設定（TCP） （内側→外側, 内側←外側の合計）	200個	200個
ポート設定（UDP） （内側→外側, 内側←外側の合計）	200個	200個
受信許可ハッシュキーワード	3000個	100個
プロクシ越えURL	100個	100個
HTML認証のユーザ登録	3000個	100個

第10図　セキュリティ通信状況の表示
送信元の2000番ポートと送信先の3000番ポートで暗号化通信されていることが確認できる。

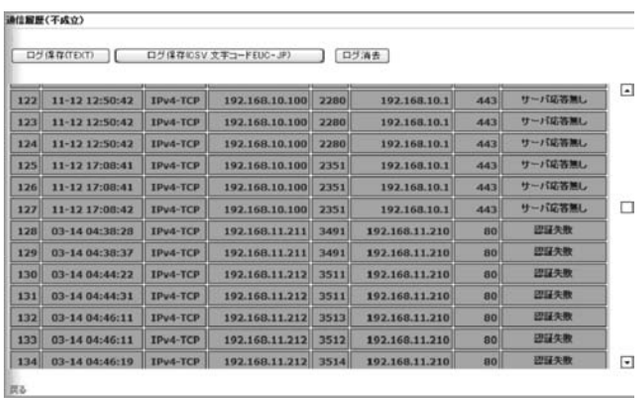
SGX1000とSGX100とでは異なる。**第 2 表**に各種設定項目における最大登録数を示す。

⑵ ログ参照　　SGXは，現在の通信状態（**第10図**），過去の接続履歴（**第11図**）や遮断履歴（**第12図**）をブラウザで確認することができる。

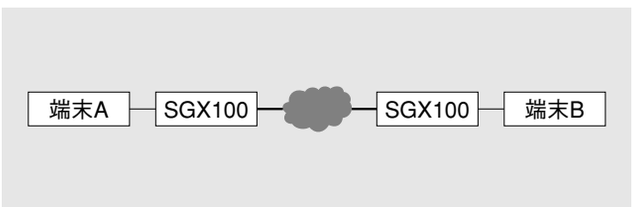
⑶ F/W更新　　SGX自身が機能強化された場合を想定し，ブラウザからF/Wの更新を実施することができる。



第11図　通信履歴（成立）の表示
過去の通信について，暗号化通信及び平文通信を行った履歴を表示する。



第12図　通信履歴（遮断）の表示
過去の通信について，通信を遮断した履歴を表示する。履歴に表示される遮断理由を確認することで安全性向上に役立つ。



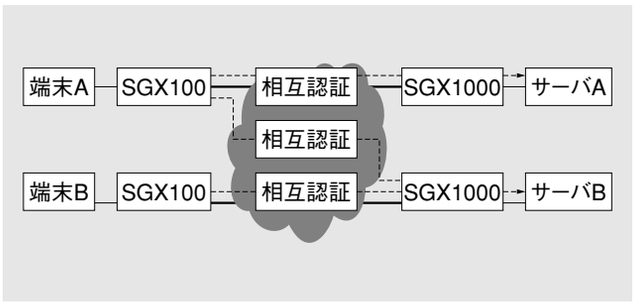
第13図　コスト削減を目的としたSGX利用例
SGXとインターネットを使用した接続により，通信コストを削減する。

3.2　SGXの利用例

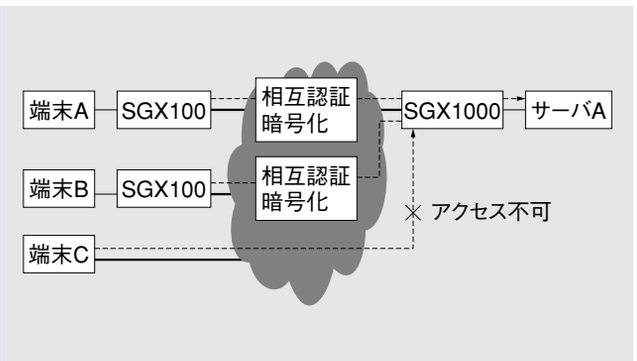
第13図から**第15図**にSGXを用いた利用例を示す。また，利用形態を以下に示す。

⑴ 通信コスト削減を目的に，端末とSGX100を介して相互接続することにより，従来専用線で実施してきたデータ通信をインターネット経由で行うことができる（**第13図**）。

⑵ サーバ側にSGX1000を，端末側にSGX100を設置し，SGXが持つグルーピング機能を使用することで，各種サーバへのアクセスに対して柔軟に対応できる（**第14図**）。



第14図　サーバへのアクセス制限を目的としたSGX利用例
サーバ側のSGXの認証機能を活用することにより，柔軟なアクセス制御を実施する。



第15図　端末ーサーバ間のセキュア通信を目的とした利用例
SGXの認証／暗号化通信機能を活用し，SGX以外からのアクセスを遮断することで，端末ーサーバ間のセキュア通信を実施する。

⑶ サーバ側にSGX1000を，端末側にSGX100を設置し，SGXの相互認証機能と暗号化機能を使用することで，各種サーバへのアクセスに対する通信の安全性及び端末の正当性を確保することができる（**第15図**）。

4.　仕　様　一　覧

第 3 表にSGX1000の基本仕様を，**第 4 表**にSGX100の基本仕様を示す。また，**第16図**にSGX1000の外観を，**第17図**にSGX100の外観を示す。

5.　ま　と　め

今回，クライント側及びサーバ側に設置して機器相互の認証及び暗号化を行うネットワークコンポーネントを開発した。

本装置を従来のネットワークにアドオンすることで，よりセキュアなネットワークとして運用することができる。今後は，安全なネットワークを更に容易に構築できるようにするため，ネット

第 3 表　SGX1000基本仕様

SGX1000の基本仕様を示す。

項目		仕様
セキュリティ機能		対象プロトコル：IP 暗号化フォワーディング機能 （AES暗号）：TCP 鍵交換機能／ポートフィルタリング機能／ グルーピング機能
コンソールポート		EIA/TIA-232-E準拠
LANインタフェース		HOST側（LAN0） 10/100/1000Base-TX（自動認識） LAN/WAN側（LAN1） 10/100/1000Base-TX（自動認識）
実行通信速度		無暗号時：700Mbps（片方向） 暗号化時：約300Mbps（片方向）
RAS機能		CPU温度異常監視，ファン回転数 異常監視，WDTエラー監視 自動再起動機能（異常検出時）
二重化機能		常用，待機によるユニットの冗長化
保存温度		−20～+60℃（電池内蔵）
動作温度		0～40℃
動作湿度		20～90%（非結露）
冷却方式		強制空冷
設置環境		腐食性ガス及びじんあいの無いこと
電源電圧	付属ACケーブル使用の場合	AC85～125V，47～63Hz※1
	装置電源入力範囲	AC85～264V，47～63Hz
消費電力		120W以下
外形		W395×H70×D235mm　突起を除く
質量		約5kg（取り付けブラケットを含む）
適合規格		VCCI　クラスA

注：※1. 国内の商用電源に接続する際は，必ず付属のACケーブルを使用

第 4 表　SGX100基本仕様

SGX100の基本仕様を示す。

項目		仕様
セキュリティ機能		対象プロトコル：IP 暗号化フォワーディング機能 （AES暗号）：TCP 鍵交換機能／ポートフィルタリング機能／ グルーピング機能
シリアル		USB（2.0）×2ch（Reserved）
LANインタフェース		HOST側（LAN0） 10/100Base-TX（自動認識） LAN/WAN側（LAN1） 10/100Base-TX（自動認識）
実行通信速度		無暗号時：100Mbps（片方向） 暗号化時：約40Mbps（片方向）
RAS機能		WDTエラー監視 自動再起動機能（異常検出時）
保存温度		−20～+60℃（二次電池内蔵）
動作温度		0～40℃（縦置き）
動作湿度		20～95%（非結露）
冷却方式		自然空冷
設置環境		腐食性ガス及びじんあいの無いこと
電源電圧	本体	DC4.75～5.25V
	付属ACアダプタ	AC90～132V
本体消費電力		約5.0W（USBへの供給電源を除く）
外形		W27×H126×D118mm（突起物含まず）
質量		約220g（本体のみ）
適合規格		VCCI クラスA

注：※1. USBポートから外部への供給電流は，2ポート合計で500mA以下
2. ネゴシエーション，固定設定に関わらずAuto MDI/MDIX 機能は有効

第16図　SAFETYTUBE SGX1000
サーバ側への適用を考慮し，19型ラックへの実装が可能である。

第17図　SAFETYTUBE SGX100
端末側に容易に設置できるよう，小形・軽量・縦置きとしている。

ワークコンポーネントの小形化並びに高機能化を進めていく所存である。

《執筆者紹介》

飯島　渉　Wataru Iijima
通信関連製品の企画・開発に従事