

WatchGuard® Firebox® S6 ユーザーガイド

S6 - firmware version 6.3



認定および通知

FCC 認定

本アプライアンスについて行われたテストにより、FCC 規則 Part 15 によるクラス A デジタル装置に関する制限に準拠しているものと認められました。使用する際は次の 2 つの条件を満たしている必要があります。

- このアプライアンスが有害な障害を引き起こすおそれがないこと。
- このアプライアンスが、あらゆる障害を受け入れる必要があること（好ましくない動作を引き起こすおそれのある障害を含む）。

CE に関する通知

WatchGuard Technologies 製機器の CE マークは、その機器が欧州連合 (EU) の Electromagnetic Compatibility (EMC) 指令および Low Voltage Directive (LVD) に準拠していることを示しています。



Industry Canada

この Class A デジタル機器は、Canadian Interference-Causing Equipment Regulations の全条件を満たしています。

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI Notice Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

適合宣言

DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product (s):

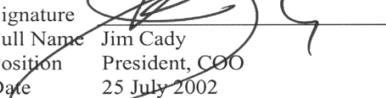
Internet Firewall, Model B0F4S16E6

EU Directive(s):

Low Voltage (73/23/EEC)
Electromagnetic Compatibility (89/336/EEC)

Standard(s):

This product has no safety requirements per the LVD
EN50022 (1998), Class A Emissions for ITE
EN50024 (1998) Immunity for ITE

Signature 
Full Name Jim Cady
Position President, COO
Date 25 July 2002

WATCHGUARD SOHO ソフトウェア エンド・ユーザー使用許諾契約書

WATCHGUARD SOHO ソフトウェア エンドユーザー使用許諾契約書

重要－ウォッチガード社のソフトウェアにアクセスする前によくお読みください。
このウォッチガード社 SOHO ソフトウェアエンドユーザー使用許諾契約書（以下使用許諾契約書）は、WATCHGUARD SOHO ソフトウェア製品に関する、お客様（個人と一企業体の両方を含む）とウォッチガード・テクノロジーズ社（以下ウォッチガード社）との間の法的な契約です。この製品には（コンピューターワークステーションあるいは WatchGuard 製ハードウェア製品にかかわらず独立してインストールした）コンピューターソフトウェア製品、また一部の関連するメディア、印刷物、オンライン文書あるいは電子文書、さらにそれらの更新版あるいは改訂版が含まれます。これらには WatchGuard LiveSecurity サービス（あるいはそれと同等のサービス）（以下ソフトウェア製品）を介して受取るものを含みます。

ウォッチガード社は、本使用許諾契約書に含まれる条項を承諾する限り、お客様のソフトウェア製品の使用を進んで許可致します。

本使用許諾契約書をよくお読みください。

ソフトウェア製品をインストールし、使用することにより、お客様は本使用許諾契約書の条項による制約に同意したものとみなされます。

もしお客様が本使用許諾契約書の条項に同意しない場合は、ウォッチガード社はソフトウェア製品の使用許可をお客様に与えず、お客様はソフトウェア製品におけるいかなる権利も持たないものとします。

その場合は、このソフトウェア製品に支払証明を添えて速やかに購入元の正規販売店に返却し、代金の全額払い戻しを受けてください。

1. 所有権と使用許可

ソフトウェア製品は、著作権法と国際著作権条約、およびその他の知的財産権や条約によって保護されています。

本契約書はライセンス契約に関するものであり、販売に供する契約書ではありません。ソフトウェア製品（ソフトウェア製品に組み込まれたいかなる画像、写真、動画、映像、音声、音楽、文章、アプレットをも含みますが、これらに限定されるものではありません）とそれに付随した印刷物、またいかなるソフトウェア製品の複製の所有権および著作権は、ウォッチガード社あるいはそのライセンサーに属しています。

お客様のソフトウェア製品の利用権については本使用許諾契約書に明記されており、全ての権限はウォッチガード社が留保し、本使用許諾契約書でお客様に特別に与えられているものではありません。

本使用許諾契約書において、米国著作権法あるいはその他全ての法および条約のもと、弊社の権利を放棄する条項は含まれていません。

2. 認められる使用

ソフトウェア製品の使用に関し、お客様には以下の権利が与えられています。

(A) SOHOあるいはユーザーの付属書類に従った SOHO ハードウェア製品の使用を目的とした時のみ、ソフトウェア製品を利用することができる。
ウェブベースのインストールプログラムを介してソフトウェア製品にアクセスする場合は、ソフトウェア製品の使用に関し、さらに以下の権利が与えられます。

(A) SOHO ユーザーの付属書類に従った SOHO ハードウェア製品への関連した接続を用いて、いかなるコンピュータにもソフトウェア製品をインストールし、使用することができる。
(B) 一つ以上のコンピュータでソフトウェア製品を使用する場合、ソフトウェア製品をインストールするそれぞれのコンピュータが同じ SOHO ハードウェア製品に接続しているという条件で、使用許可なしにソフトウェア製品の複製をそれぞれのコンピュータに同時にインストールし使用することができる。

;そして

(C) バックアップあるいは永久保存用記録を目的とした場合に限り、一つだけソフトウェア製品の複製を作成することができる。

3. 禁止される使用

ウォッチガード社からの明確な書面による許諾を得ずに以下を行うことは禁止されています:

- (A) ソフトウェア製品のリバース・エンジニアリング、逆アセンブル、逆コンパイル;
- (B) ソフトウェア製品あるいは本使用許諾契約書に記述された例外を除く印刷物の使用、複製、変更、マージ、譲渡;
- (C) オリジナル製品が破壊されたあるいは欠陥が生じた場合の使用を除く、いかなる目的に基いたソフトウェア製品のバックアップあるいは永久保存用記録の使用 (または他人への使用許可);
- (D) ソフトウェア製品のサブライセンス、貸与、リースまたは賃貸 ;あるいは
- (E) 以下の場合を除きこのライセンスを他者に譲渡すること
 - (i) 譲渡が恒久的である場合
 - (ii) 第三者の受領者が本使用許諾契約書の条項に同意する場合
 - (iii) お客様がいかなるソフトウェア製品も保有しない場合

4. 限定保証

ウォッチガード社は、お客様がウォッチガード社あるいはその正規販売店からソフトウェア製品を購入した日より 90 日間、次の限定保証を致します;

(A) メディア。ディスクと付属文書は通常の使用条件の下で製品および製造上の欠陥がない。もしディスクあるいは付属文書がこの保証に適合しない場合、お客様の唯一かつ排他的な救済として、欠陥のあるディスクあるいは付属文書を日付入りの購入証明書を添付して返却すれば、無料で交換することができます; また

(B) ソフトウェア製品。ソフトウェア製品は、製品上それに付属した文書に適合します。もしソフトウェア製品がこの保証に合致して作動しない場合は、お客様の唯一かつ排他的な救済として、そのソフトウェア製品および付属文書を日付入りの購入証明書を添付して購入先の正規販売店に返却し、問題を明示すれば、彼らの選択により、新バージョンのソフトウェア製品あるいは代金の全額払い戻しを受けることができます。

責任範囲の限定と免責

上記第 4 条 4 (A) および 4 (B) に記載されたウォッチガード社の保証、義務および責任、お客様の救済方法は排他的なものであり、ウォッチガード社およびそのライセンサーのそ

の他一切の保証、義務および責任、ソフトウェア製品におけるいかなる不適合あるいは欠陥に関して、明示であると黙示であると問わず、また法律その他により生ずるものであると問わず、お客様がウォッチガード社およびそのライセンサーに対して有しうるその他一切の権利、請求権、および救済方法（これらに限定されませんが、商品性または特定目的への適合性についての一切の黙示の保証、履行の経過、取引の経過或いは取引慣行に起因する一切の黙示の保証、非侵害についての一切の保証、あるいはこのソフトウェア製品がお客様の要望に適合することの一切の保証、障害あるいは誤作動がないことの一切の保証、当社の過失（能動過失、受動過失、転嫁過失を問いません）またはウォッチガード社の過誤に起因すると否にかかわらず、不法行為法上の一切の義務、責任、権利、請求権または救済方法、ソフトウェア製品に起因する或いはこれが寄与する損失または損害の賠償義務、責任、権利、請求権または救済方法を含む）に代わるものであり、また、お客様は、ここに、お客様ウォッチガード社に対して有しうるその他一切の権利、請求権および救済方法等を放棄し、免除するものとします。

責任の制限

ソフトウェア製品に関し、ウォッチガード社がお客様に対して負う責任（契約法、不法行為法その他いづれに生じるかを問いませんし、過誤、過失責任、無過失責任もしくは製造物責任にかかわらず）は、お客様がその製品を購入した価格を超えないものとします。この原則は、合意された救済方法の履行を怠った場合であっても、適用されるものとします。いかなる場合も、ウォッチガード社は、契約法（保証を含む）、不法行為法（能動過失、受動過失または転嫁過失、無過失責任、過誤を含む）の何れに起因すると問わず、本保証またはソフトウェア製品の使用または使用不可能に起因し、またはこれに関連する一切の間接損害、特別損害、付随的損害または派生的損害（これらに限定されませんが、事業利益の逸失、事業の中断または事業情報の喪失を含みます）につき、お客様またはいかなる第三者に対しても責任を負いません。このことは、たとえウォッチガード社が、かかる損害の可能性について告知されていた場合であっても同様とします。この原則は、合意された救済方法の履行を怠った場合であっても、適用されるものとします。

5. 米国政府の制限つき権利 (United States Government Restricted Rights)

同封のソフトウェア製品および付属文書は、制限つき権利 (Restricted Rights) とともに提供されます。

米国政府あるいは一切の代理店またその手段による使用、複製、あるいは開示は、DFARS 第 252. 227-7013 節の「技術データおよびコンピュータソフトウェアにおける権利条項」の (c) (1) (ii) 項、もしくは CFR48 号第 52. 227-19 節の「商業用コンピュータ・ソフトウェア制限付権利」の (c) (1) および (2) のいずれか該当する方に規定された制限に従います。製造者はウォッチガードテクノロジーズ株式会社 (505 5th Ave. South, Suite 500, Seattle, WA 98104) です。

6. エクスポート管理

お客様はソフトウェア製品あるいはその付属文書を、米国輸出管理法および以下に述べる規定によって輸出が禁止されている一切の国々に、直接的あるいは間接的に関わらず輸出しないことに同意するものとします。

7. 契約終了

本ライセンスとお客様のソフトウェア製品の著作権は、本使用許諾契約書の如何なる規定にも準拠しなかった場合、またお客様の所有下であらゆるソフトウェア製品が破壊された場合、あるいはお客様の自由意志によりウォッチガード社にソフトウェア製品を返却した場合、自動的に終了するものとします。契約終了に当たり、お客様は使用中あるいは所有している全てのソフトウェア製品およびその付属文書を破棄するものとします。

8. その他

本保証書に対しては、修正された 1980 United National Convention on Contracts for the International Sale of Goods の条項を除き、ワシントン州法に準拠し、同法に基づき解釈されるものとします。本保証書は、お客様とウォッチガード社との間の本製品の内容に関する使用許諾契約書であり、ソフトウェア製品に関するあらゆる受注書、通信文書、広告、表示に代わるものです。また、ソフトウェア製品を使用することで、お客様はこれらの条項に同意したものとします。ソフトウェア製品が事業体によって使用される場合、これらの条項に対し同意を示す個人は、(A) 事業体のために本契約書を承諾することを正式に授權されており、かつ、本契約の諸条件に従い事業体を拘束する権限を有していること、(B) 事業体が、本契約を締結し、本契約書に基づく義務を履行する、法人または個人としての完全な権限を有していること、並びに (C) 本契約書および本契約書に基づく義務を事業体が履行することは、事業体が当事者である何れかの第三者との契約に違反するものではないことを表明かつ保証するものです。

ウォッチガード社によって署名された書面による合意がない限り、本使用許諾契約書の変更は無効です。

注意

このガイドに記載されている事項は、予告なく変更されることがありますので、予めご了承ください。このガイドの例で使われている企業、名称、およびデータは、特に記述がない限り架空のもです。本書の一部または全部を、WatchGuard Technologies, Inc の書面による明示的な許可なく、いかなる目的においても、電子的または機械的などいかなる手段によっても、またいかなる形式によっても、複製または伝送することを禁じます。

著作権、商標、特許に関する情報

Copyright© 1998 - 2003 WatchGuard Technologies, Inc. All rights reserved.
AppLock®, AppLock®/Web, Designing peace of mind®, Firebox®, Firebox® 1000, Firebox® 2500, Firebox® 4500, Firebox® II, Firebox® II Plus, Firebox® II FastVPN, Firebox® III, Firebox® SOHO, Firebox® SOHO 6, Firebox® SOHO 6tc, Firebox® SOHO|tc, Firebox® V100, Firebox® V80, Firebox® V60, Firebox® V10, LiveSecurity®, LockSolid®, RapidStream®, RapidCore®, ServerLock®, WatchGuard®, WatchGuard® Technologies, Inc., DVCP™ technology, Enforcer/MUVPN™, FireChip™, HackAdmin™, HostWatch™, Make Security Your Strength™, RapidCare™, SchoolMate™, ServiceWatch™, Smart Security. Simply Done.™, Vcontroller™ および VPNforce™ は、米国およびその他の国における WatchGuard Technologies, Inc の登録商標または商標です。

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT®, および Windows® 2000 は、米国およびその他の国における Microsoft Corporation の登録商標または商標です。

Netscape および Netscape Navigator は、米国およびその他の国における Netscape Communications Corporation の登録商標です。

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TTPM, RSA Public Key Cryptosystem, MD, MD2, MD4, および MD5 は、RSA Data Security, Inc. の登録商標または商標です。Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, および RealVideo は、米国およびその他の国における RealNetworks, Inc. の登録商標または商標です。

Java および Java に関するマークは、米国およびその他の国における Sun Microsystems, Inc. の商標または登録商標です。All rights reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-2000 The OpenSSL Project. All rights reserved. 次の条件が満たされるなら、ソースやバイナリ形式の再配布と使用が、変更の有無にかかわらず認められます：

1. ソースコードの再配布には、上記コピーライト、この条文のリストとそれに続く断り書きを維持しなくてはなりません。
2. バイナリ形式での再配布には、上記コピーライト、この条文のリストとそれに続く断り書きを、文書化して／あるいは他の方法で、配布物といっしょに複製しなくてはなりません。
3. このソフトウェアの特徴あるいは使用について述べているすべての広告物は次の一文を表示しなくてはなりません：「このプロダクトは OpenSSL プロジェクトによって開発された OpenSSL ツールキットで使用するためのソフトウェアを含みます。
(<http://www.openssl.org/>)」
4. 事前の書面による許可なしで、このソフトウェアから得られたプロダクトを保証するために、あるいは宣伝するために「OpenSSL ツールキット」と「OpenSSL プロジェクト」という名称を使ってはなりません。書面による許可は openssl-core@openssl.org と連絡を取ってください。
5. OpenSSL プロジェクトの事前の書面による許可なしで、このソフトウェアから得られたプロダクトは「OpenSSL」と呼んではいけません。また、それらの名前に「OpenSSL」が現れてもいけません。
6. どんな形の再配布でも、それらには次の一文を維持しなくてはなりません：「このプロダクトは OpenSSL プロジェクトによって開発された OpenSSL ツールキットで使用するためのソフトウェアを含みます。
(<http://www.openssl.org/>)」

このソフトウェアは「現状のままで」OpenSSL プロジェクトによって提供されます、そして、特定の目的のために MERCHANTABILITY とフィットネスの暗黙の保証を含め、明示的あるいは暗黙のどんな保証も致しません。OpenSSL プロジェクトあるいはその貢献者は、どんな責任問題も、契約書に書かれているか否かにかかわらず、厳密な責任、あるいは不法行為（怠慢であるか否かを含めて）で、たとえ不幸にも起きてしまったこのような損害の可能性を見越しての故意であるとしても、このソフトウェアの使用から生ずるどんな面にしても（代用となる商品あるいはサービスの調達；使用権、データ、あるいは利益の損失；あるいは営業の中断を含めて）直接的な、間接的な、付随的な、特別な、みせしめ的な、あるいは重大な損害賠償になんら責任はありません。

このプロダクトは Eric Young (eay@cryptsoft.com) によって書かれた暗号のソフトウェアを含みます。

このプロダクトは Tim Hudson (tjh@cryptsoft.com) によって書かれたソフトウェアを含みます。

© 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

このパッケージは Eric Young (eay@cryptsoft.com) によって書かれた SSL インプリメンテーションです。

インプリメンテーションはネットスケープ SSL に則するように書かれました。

このライブラリは、次の条件が守られている間は、営利、非営利いずれでの使用もフリーです。次の条件は、C4、RSA、lhash、DES などの SSL コードでないものを除き、この配布物に含まれているすべてのコードに当てはまります。保有者が Tim Hudson (tjh@cryptsoft.com) であること以外、このディストリビューションに含まれている SSL ドキュメンテーションは同じコピーライト条件でカバーされます。

著作権は Eric Young にあり、そしてコード中の著作権揭示は取り去られません。もしこのパッケージがプロダクトで使われるなら、Eric Young は使われたライブラリの部分の著者として帰属を与えられるべきです。プログラムのセットアップで、あるいはこのパッケージで提供された（オンラインか、あるいは原文の）ドキュメンテーションに、原文ままのかたちで存在します。次の条件が満たされるなら、ソースやバイナリ形式の再分配と使用が、変更の有無にかかわらず認められます：

1. ソースコードの再配布には、コピーライトの揭示、この条文のリストとそれに続く断り書きを維持しなくてはなりません。
2. バイナリ形式での再配布には、上記コピーライト、この条文のリストとそれに続く断り書きを、文書化して／あるいは他の方法で、配布物といっしょに複製しなくてはなりません。
3. このソフトウェアの特徴あるいは使用について述べているすべての広告物は次の一文を表示しなくてはなりません：「このプロダクトは Eric Young (eay@cryptsoft.com) によって書かれた暗号のソフトウェアを含んでいます」。もし使われているライブラリのルーチンが暗号と関係ないなら、「cryptographic (暗号)」という単語は取り去ることができません :-)。
4. もしあなたがアプリケーションディレクトリ（アプリケーションコード）から Windows のどんな特定のコード（あるいはその派生物）を含むなら、次の一文を含まなくてはなりません：「このプロダクトは Tim Hudson (tjh@cryptsoft.com) によって書かれたソフトウェアを含みます」

このソフトウェアは「現状のまま」Eric Young によって提供されます、そして、特定の目的のために MERCHANTABILITY とフィットネスの暗黙の保証を含め、明示的あるいは暗黙のどんな保証も致しません。Eric Young あるいは貢献者は、どんな責任問題も、契約書に書かれているか否かにかかわらず、厳密な責任、あるいは不法行為（怠慢であるかないかを含めて）で、たとえ不幸にも起きてしまったこのような損害の可能性を見越しての故意であるとしても、このソフトウェアの使用から生ずるどんな面にも（代用となる商品あるいはサービスの調達；使用権、データ、あるいは利益の損失；あるいは営業の中断を含めて）直接的な、間接的な、付随的な、特別な、みせしめ的な、あるいは重大な損害賠償になんら責任はありません。

公開された利用可能などんなバージョンも、このコードからの派生物もライセンスや配布条件を変更できません。つまり、このコードは、簡単にコピーし、別の分配ライセンスの下に置くことは出来ません。[GNU Public Licence を含めて]

mod_ssl package パッケージは、BSD 型ライセンスのもとで配布されるので、Open-Source Software ラベルの管理下にあります。ライセンス情報の詳細は次のとおりです。Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

次の条件が満たされた場合に限り、そのままの状態または一部を修正した状態における、ソース形式およびバイナリ形式での再配布および使用を許可します。

1. ソース・コードを再配布する場合、前述の著作権表示、この条件リスト、および後述の免責事項を順守する必要があります。
2. バイナリ形式で再配布する場合、前述の著作権表示、この条件リスト、および後述の免責事項を、再配布時に添付される文書に記載する必要があります。
3. このソフトウェアの機能または使用について記載するすべての広告文書に、「この製品には、Ralf S. Engelschall 氏 (<rse@engelschall.com>) によって開発された、mod_ssl プロジェクト (<http://www.modssl.org/>) の中で使われるソフトウェアが含まれています。」という謝辞を記載する必要があります。
4. このソフトウェアから派生する製品を推奨または宣伝する際、書面による事前の許可なく、「mod_ssl」という名前を使用することを禁じます。書面による許可が必要な場合は、rse@engelschall.com に問い合わせてください。
5. Ralf S. Engelschall 氏の書面による事前の許可なく、このソフトウェアから派生する製品に「mod_ssl」という名称をつけること、および製品名称の中に「mod_ssl」という単語を含めることはできません。
6. いかなる形式で再配布する場合でも、「この製品には、Ralf S. Engelschall 氏 (<rse@engelschall.com>) によって開発された、mod_ssl プロジェクト (<http://www.modssl.org/>) の中で使われるソフトウェアが含まれています。」という謝辞を記載する必要があります。

このソフトウェアは、Ralf S. Engelschall 氏によって現状有姿のまま提供されます。商品性および特定目的への適合性などに対する明示的または暗黙的な保証を一切いたしません。Ralf S. Engelschall 氏および作成協力者は、直接的または間接的を問わず、偶発的な損害、特殊な損害、典型的な損害、派生的な損害（代替品や代替サービスの調達、使用不可状態の発生、データや利益の消失、業務の中断など）に対して、契約内の記述、厳格な責任、このソフトウェアの使用によって発生する不法行為（過失など）を含めいかなる

責任論においても、またそのような損害が発生する可能性について事前に勧告していた場合においても、一切責任を負いません。

Apache ソフトウェアライセンス バージョン 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

変更の有無に関わらず、下記条件が満たされれば、ソースやバイナリ形式での再配布および使用が許可されます：

1. ソースコードの再配布には、上記の著作権表示、この条件リスト、および下記の免責事項を残さなければならない。

2. バイナリ形式での再配布には、上記の著作権表示、この条件リスト、および下記の免責事項を、配布物と共に提供される文書および（または）他の資料に複製しなければならない。

3. 再配布物に含まれるエンドユーザー向け文書（ほんの少量であっても）は以下の謝辞を引用しなければならない：

“本製品は Apache Software Foundation <<http://www.apache.org/>> により開発されたソフトウェアを含みます。” 本謝辞はソフトウェア自身に現れるかもしれませんが、もし現れるのであれば、サードパーティの謝辞が通常現れるところにはどこでも現れるでしょう。

4. “Apache”、および “Apache Software Foundation” の名称は、事前掲載許可なしに、本ソフトウェアから派生した製作物の推薦または宣伝に使用してはいけません。掲載許可を得るには <apache@apache.org> に連絡してください。

5. 本ソフトウェアから派生する製作物は、“Apache” と呼ばれなくてもかまいません、Apache Software Foundation の事前掲載許可なしに “Apache” の名前がそれらの名前に現れなくともかまいません。

本ソフトはそのまま提供され、いかなる表現されたもの、または暗黙の保証を含んでいません。しかし、制限はされません。市場向けの暗黙的な保証や特別な目的への適用は放棄されます。Apache Software Foundation、もしくはその貢献者たちは、直接的、間接的、付随的、特別の、懲戒的、または（代替商品又は代替サービスの為の費用、利用できなかったことによる損失、データの損失、失利益、ビジネス割込み、これらに限定されないものを含む）派生的損害について何ら責任を負わないものとします。本ソフトウェアの利用範囲外で起きた責任の理由、契約の中、厳しい責任、または不正行為（過失やその他の場合も含む）に関しても同様とします。このことは、当該損害の可能性について知らされた場合でも同様とします。

本ソフトウェアは、Apache Software Foundation を代表する多くの個人のボランティアによる貢献から成りたっています。Apache Software Foundation に関する詳しい情報は <<http://www.apache.org/>> を参照してください。

このソフトウェアの一部は、イリノイ大学（所在地：アーバナ市およびシャンペーン市）の National Center for Supercomputing Applications によって開発されたパブリック・ドメイン・ソフトウェアをベースにしています。

この文書に記載されているその他の商標および称号は、各社に帰属します。
品番：0814-000

このガイドで使用されている略称

3DES	Triple Data Encryption Standard
DES	Data Encryption Standard
DNS	Domain Name Service
DHCP	Dynamic Host Control Protocol
DSL	Digital Subscriber Line
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
MAC	Media Access Control
MUVPN	Mobile User Virtual Private Network
NAT	Network Address Translation
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WSEP	WatchGuard Security Event Processor

目次

第 1 章	はじめに	1
	パッケージ内容	3
	ファイアウォールの動作	3
	インターネット上での情報の流れ	4
	IP アドレス	5
	プロトコル	5
	ポート番号	5
	S6 の情報処理方法	6
	サービス	6
	ネットワーク・アドレス交換 (NAT)	6
	S6 ハードウェア概要	6
	S6 の正面および裏面外観	7

第 2 章	インストール	11
	事前作業	12
	現在の TCP/IP 設定情報を確認しメモしておきます。	12
	ウェブ・ブラウザ HTTP プロキシ設定の無効化	15
	コンピューターの DHCP 設定の有効化	16
	S6 の物理的な接続	19
	S6 を 1 ～ 4 台の機器と接続する場合の配線	19
	S6 を 5 台以上の機器と接続する場合の配線	21
第 3 章	S6 の基本事項	25
	S6 の [システム・ステータス] ページ	25
	デフォルト出荷設定	27
	S6 のデフォルト出荷設定へのリセット	29
	ベース・モデルの S6	30
	S6 および LiveSecurity サービスの登録	30
	S6 のリブート	31
第 4 章	ネットワーク・インターフェイスの設定	33
	外部ネットワークの設定	33
	ネットワーク・アドレスの割り当て	33
	動的アドレス割り当てを使う場合の S6 外部ネットワークの設定	34
	アドレス割り当てを使う場合の S6 外部ネットワークの設定	35
	PPPoE を使う場合の S6 外部ネットワークの設定	36
	トラステッド・ネットワークの設定	38
	DHCP サーバーと DHCP リレイの設定	38

	トラステッド・ネットワーク上に追加されたコンピューターの設定	40
	静的アドレスを使用する場合のトラステッド・ネットワークの設定	41
	静的ルートの設定	41
	ネットワーク統計情報の表示	43
	ダイナミック DNS サービスの設定	44
	OPT ポート・アップグレード版の設定	46
	Dual ISP Port の設定	46
	VPNforce™ Port の設定	49
第 5 章	管理オプション	53
	[システム・セキュリティ] ページ	53
	システム・セキュリティ	54
	S6 リモート管理	55
	VPN Manager アクセスの設定	57
	ファームウェアの更新	59
	S6 アップグレード版・オプションの有効化	61
	コンフィギュレーション・ファイルの表示	64
第 6 章	ファイアウォールの設定	65
	ファイアウォール設定	65
	受信サービスと送信サービスの設定	66
	標準サービス	66
	カスタム・サービスの作成	68
	外部サイトの遮断	70
	ファイアウォール・オプション	71

外部ネットワークからの ping 要求への応答	72
トラステッド・ネットワーク・インターフェイスに対する FTP アクセスの拒否	72
Firebox S6 の SOCKS のインプリメンテーション	73
許可されたすべての送信トラフィックのログ出力	75
外部ネットワークの MAC アドレスのオーバーライドを有効にする	75
無制限パス・スルーの作成	76
第 7 章 ロギングの設定	79
S6 Wireless のログ・メッセージの表示	80
WatchGuard Security Event Processor ログホストへのロギングの設定	81
シスログ (Syslog) ホストへのロギングの設定	83
システム時間の設定	84
第 8 章 S6 WebBlocker	87
WebBlocker の動作	87
S6 WebBlocker の回避	88
S6WebBlocker の購入と有効化	89
S6WebBlocker の設定	89
WebBlocker が使用するサイト・カテゴリー	93
第 9 章 VPN-Virtual Private Networking(仮想プライベート・ネットワーク)	97
Virtual Private Network を構築する理由	97
VPN の構築に必要なもの	97
VPN アップグレード版の有効化	100

複数の S6 間の VPN トンネルの設定	101
IPSec 準拠アプライアンスと S6 への VPN トンネルの作 成	105
要注意点	105
分割トンネリングの設定	106
MUVPN クライアント s の使用	107
VPN 統計の表示	108
FAQ(よく寄せられる質問とその回答)	108
なぜ静的外部アドレスが必要なのですか。	108
静的外部アドレスを取得する方法を教えてください。 108	
VPN 接続でのトラブルシューティングの方法を教えてください。 109	
Ping を発行できません。	109
VPN アップグレード版のライセンス・キーを取得する方 法を教えてください。	109
VPN トンネルを有効化する方法を教えてください。	110
第 10 章 MUVPN クライアント	111
MUVPN クライアントを用いるための S6 の設定 ..	112
MUVPN クライアント使用のためのリモート・コン ピューターの準備	114
システム要件	114
Windows 98/ME オペレーティング・システムのセット アップ	115
Windows NT オペレーティング・システムのセットアッ プ	120

Windows 2000 オペレーティング・システムのセットアップ	122
Windows XP オペレーティング・システムのセットアップ	126
MUVPN クライアントのインストールと設定	129
MUVPN クライアントのインストール	130
MUVPN クライアントの設定	131
フェーズ 1 およびフェーズ 2 の設定の定義	137
MUVPN クライアントのアンインストール	139
MUVPN クライアントの接続と切断	141
MUVPN クライアントの接続	141
MUVPN クライアント・アイコン	142
パーソナル・ファイアウォールを介した MUVPN クライアントの作動許可	144
MUVPN クライアントの切断	145
MUVPN クライアント接続の監視	146
Log Viewer の使用	146
Connection Monitor の使用	146
ZoneAlarm パーソナル・ファイアウォール	147
ZoneAlarm を介したトラフィックの許可	149
ZoneAlarm の終了	150
ZoneAlarm のアンインストール	150
トラブルシューティングのヒント	151
MUVPN クライアントをインストールした直後にコンピューターが停止してしまいます。	152
ネットワークに接続していないときでもネットワークのログイン情報を入力しなくてはならないのですが...	152

コンピューターの電源を入れたときに、ユーザー名とパスワードの入力を要求されません。 153

MUVPN トンネルが作動しているか分かりません。 153
マップされたドライブに赤い×印が付けられています。
153

どうやってネットワーク・ドライブをマップすればいいのでしょうか。 154

会社のネットワークをブラウザで閲覧している最中にパスワードの入力を要求されることがあります。
154

MUVPN クライアントを使用した後、コンピューターを終了するのに極めて長い時間を要します。 155

自分の ISP への接続が絶たれてしまい、会社のネットワークを使用することができません。 155

第 11 章	VPNforce の使用	157
	VPNforce を用いた企業ネットワークへの接続	157
	オプション・ネットワークの設定	158
	VPNforce と MUVPN クライアントアップグレード版を用いた企業ポリシーの強化	161
	S6 の設定	162
	MUVPN クライアントの設定	164
	セキュリティ・ポリシー設定の定義	166
	My Identity 設定の定義	167
	フェーズ 1 およびフェーズ 2 の設定の定義	170
	MUVPN クライアントを用いたワイヤレス・ネットワークの保護	172
第 12 章	サポート情報	175
	トラブルシューティングのヒント	175

全般	175
設定	179
VPN 管理	182
テクニカル・サポート窓口	184
オンライン・ドキュメントと FAQ	184
特別の注意	184
索引	185

はじめに

本ガイドでは、WatchGuard®Firebox®S6 および Firebox®S6-VPN をご利用のお客様のために、設定および構成を行い、インターネットにセキュアにアクセスする方法について説明します。



本ガイドでは、S6 および S6-VPN をどちらも S6 と表記します。S6 および S6-VPN の唯一の違いは、VPN（仮想プライベート・ネットワーク）機能です。S6 の場合、VPN はアップグレード・オプションとして入手できますが、S6-VPN には VPN アップグレード・オプションが含まれています。

S6 は、高速ケーブル・モデム、DSL モデム、専用回線、または ISDN を使ってユーザーのコンピューターをインターネットに接続する際のセキュリティを提供します。

最新のインストラクションおよびユーザー情報については、ウォッチガード社ウェブサイトをご覧ください。

<http://support.watchguard.com/sohoresources/>

本ガイドでは、下記の表記法を使用します。

- ・ 設定手順では、ボタン、メニュー・アイテム、ダイアログ・ボックス、フィールド、タブなど、ユーザー・インターフェイスの表示項目はボールド体で表記します。
- ・ 矢印 (⇒) で区切られたメニュー・アイテムは、各メニューを順番に選択していくことを意味します。例えば、**[ファイル]** ⇒ **[開く]** ⇒ **[設定ファイル]** と記載されている場合、**[ファイル]** メニューから **[開く]** を選択し、次に **[開く]** メニューから **[設定ファイル]** を選択します。
- ・ URL および電子メール・アドレスは、サンセリフ体で表記します。例えば、`wg-users@watchguard.com` となります。
- ・ コード、メッセージ、ファイル名は、等幅フォントで表記します。例えば、`.wgl` および `.idx` ファイルとなります。
- ・ コマンド構文の変数は、イタリック体で表記します。例えば、`fbidsmate import_passphrase` となります。
- ・ オプションのコマンド・パラメーターは、角括弧で表記します。

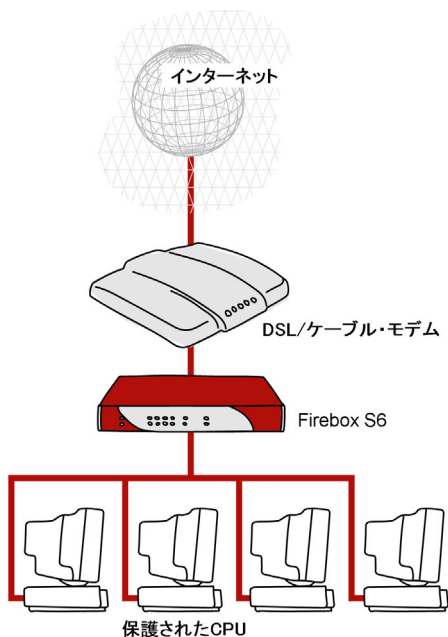
パッケージ内容

パッケージ内に次のものが揃っているか確認してください。

- ・ S6 クイックスタート・ガイド
- ・ ユーザー・ガイド
- ・ LiveSecurity サービス^A アクティベーション・カード
- ・ ハードウェア保証書
- ・ AC アダプター (12 V、1.0-1.2 A)
- ・ ストレート・スルー・イーサネット・ケーブル
- ・ S6 セキュリティ・アプライアンス

ファイアウォールの動作

インターネットは、ネットワークをワールド・ワイド・ウェブ (WWW)、電子メール、ビデオ/オーディオ会議などのリソースに繋がります。けれども、インターネットへの接続には、ネットワークのプライバシーやセキュリティを侵害する危険性があります。ファイアウォールは、ユーザーの内部ネットワークとインターネットを分離し、その危険性を軽減させます。トラステッド側のアプライアンスは S6 ファイアウォールに保護されます。以下の図では、S6 がいかにトラステッド・ネットワークをインターネットから分離させるかを示しています。



S6 は、外部ネットワーク（インターネット）とトラステッド・ネットワーク（ユーザーのコンピューター）間のすべてのトラフィックを制御します。不審なトラフィックを認定するルールおよびポリシーは、66 ページの「受信サービスと送信サービスの設定」に示されています。

インターネット上での情報の流れ

インターネットを介して送られるデータは、パケットに分割されます。そして、パケットが送信先に届いたことを確認するための情報がパケットに追加されます。これらのパケットを送受信するプロトコルを TCP または IP と呼びます。TCP はデータの分解および組み立て直しを行います。例えば、データは電子メール・

メッセージやプログラム・ファイルで構成されています。IP は、送信先や処理要件を含む情報をパケットに追加します。

IP アドレス

IP アドレスは、インターネット上でパケットの送受信を行うコンピューターを識別します。インターネット上の各コンピューターは、それぞれひとつのアドレスを持ちます。S6 もまた 1 台のコンピューターであるため、IP アドレスを 1 つ持っています。ファイアウォールの内側でサービスの構成を行う場合、サービスを提供するコンピューターのトラステッド・ネットワーク IP アドレスを含んでいる必要があります。

URL (Uniform Resource Locator) は、インターネット上の各 IP アドレスを識別します。URL とは、例えば、次のようなものです。

<http://www.watchguard.com/>

プロトコル

プロトコルは、パケットがどのように組み立てられてネットワーク上を転送するかを規定します。最も一般的に使用されるプロトコルは TCP および UDP (User Datagram Protocol) です。IP プロトコルには他にも種類がありますが、あまり使用されていません。

ポート番号

コンピューター間で通信を行う際、ポート番号はどのプログラムまたはアプリケーションが接続されるかを識別します。

S6 の情報処理方法

サービス

サービスは、特定のプログラムやアプリケーション・タイプが使用するプロトコルおよびポート番号のグループです。S6 の標準構成には、多くの標準的なサービスで 사용할 ことができる適切な設定値が含まれています。

ネットワーク・アドレス交換 (NAT)

トラステッド・ネットワークから S6 を介した外部ネットワークへのすべての接続は、動的 NAT を使用します。動的 NAT は、プライベート IP アドレスがユーザーのトラステッド・ネットワークからインターネット上へ送信されることを防止します。

S6 は、プライベート IP アドレスをパブリック IP アドレスに置き換えることで、トラステッド・ネットワークを保護します。インターネット上に伝送される各パケットには、IP アドレス情報が含まれています。動的 NAT により S6 を介して送信されるパケットには、S6 のパブリック IP アドレスのみが含まれており、トラステッド・ネットワーク上のコンピューターのプライベート IP アドレスは含まれません。S6 の IP アドレスのみが外部ネットワークに伝送されるため、アクセス権限をもたない公衆ネットワーク上のコンピューターがトラステッド・ネットワーク上のコンピューターにアクセスすることはできません。

S6 ハードウェア概要

S6 のハードウェアには、旧バージョンの S モデルよりも新しい技術が採用されています。

高速化したプロセッサ

S6 には新しいネットワーク・プロセッサが実装されており、150MHz で動作します。また、イーサネットおよび暗号化技術が搭載されています。

イーサネット・ポート

S6 には、6 個の 10/100 Base TX ポートが実装されています。イーサネット・ポートには、0～3、OPT、WAN というラベルが付いています。

S6 の正面および裏面外観

S6 の正面パネルには、14 個のインジケータ・ライトが付いています。以下の写真は、正面パネルの外観です。



PWR

PWR ライトは、S6 が電源装置に接続されているときに点灯します。

ステータス

ステータス・ライトは、管理用接続が使用されているときに点灯します。

リンク

リンク・インジケータは、アクティブな物理的接続が該当するイーサネット・ポートに接続されているときに点滅します。

100

100 インジケータは、ポートが 100Mb で動作しているときに点灯します。100 インジケータは、ポートが 10Mb で動作しているときには点灯しません。

WAN

WAN インジケータは、アクティブな物理的接続が WAN ポートに接続されているときに点滅します。

モード

モード・インジケータは、インターネットに接続されているときに点灯します。

S6 の裏面パネルには、6 個のイーサネット・ポート、リセット・ボタン、電源コネクタが実装されています。以下の写真は、裏面パネルの外観です。



OPT ポート

OPT ポートは、オプションのネットワーク・インターフェイスです。このインターフェイスは、Dual ISP Port アップグレードおよび VPNforce®Port アップグレードを購入した場合に有効になります。Dual ISP Port アップグレードおよび VPNforce Port アップグレードについては詳細、46 ページの「OPT ポート・アップグレード版の設定」を参照してください。

注意

OPT ポートは、Dual ISP Port アップグレードおよび VPNforce Port アップグレードのみに使用されます。OPT ポートは、トラステッド・ネットワーク上のイーサネット・ポートとして使用することはできません。

リセット・ボタン

リセット・ボタンを押すと、S6 をリセットして、工場出荷状態のデフォルト設定に戻すことができます。操作手順については、詳細、29 ページの「S6 のデフォルト出荷設定へのリセット」を参照してください。

WAN ポート

WAN ポートは、外部ネットワーク・インターフェイスとして使用されます。

4 つの番号付きポート (0 ~ 3)

これらのイーサネット・ポートは、トラステッド・ネットワーク・インターフェイスとして使用されます。

電源コネクタ

S6 に付属の 12 ボルト AC アダプターを使って、電源コネクタと電源装置を接続します。

S6 は、イーサネット・ケーブルを使って接続しているコンピュータを保護します。本章の手順に従い、ユーザーのネットワークに S6 をインストールして下さい。

S6 をインストールするには、下記の手順に従って下さい。

- ・ 現在の TCP/IP 設定情報を確認し、メモしておきます。
- ・ ウェブ・ブラウザの HTTP プロキシ設定を無効にします。
- ・ ユーザーのコンピュータの DHCP 設定を使用可能にします。
- ・ S6 をネットワークに物理的に接続します。

S6 に同梱されている『S6 クイックスタート・ガイド』では、この章で説明する内容が簡単にまとめられています。

事前作業

S6 をインストールする前に、次のものが揃っているか確認して下さい。

- 10/100 BASE-T イーサネット・I/O・カードが実装され、Netscape または Internet Explorer などのウェブ・ブラウザがインストールされたコンピューター。
- 正常に動作しているインターネット接続。10/100 BASE-T ポートを備えたケーブル・モデムまたは DSL モデム、ISDN ルーター、あるいは直接 LAN 接続を使って、インターネットに接続します。接続が正常でない場合は、インターネット・サービス・プロバイダー (ISP) にお問い合わせ下さい。
- RJ45 コネクタが付いたストレート・スルー・イーサネット・ネットワーク・ケーブル 2 本。クロスオーバー・ケーブル (通常、赤またはオレンジ色) は使用できません。S6 には、ケーブルが 1 本付属しています。もう 1 本は、モデムに付属されているケーブルをご使用いただけますが、モデムにケーブルが付属していない場合は、別途、購入して下さい。モデム (またはルーター) から S6 まで、そして、S6 からコンピューターまでを接続するケーブルの長さが充分であるかどうかを確認して下さい。
- ユーザーの ISP がネットワーク・アドレスを割り当てる際に使っている方式 (静的アドレス、DHCP、または PPPoE) を確認します。分からない場合は、ISP にお問い合わせ下さい。
- S6 のシリアル番号。アプライアンスの底面に記載されています。

現在の TCP/IP 設定情報を確認しメモしておきます。

現在の TCP/IP 設定情報を確認し、あとで参照できるようにテーブルに記入しておきます 14 ページの「TCP/IP 設定」。ご使用のオペレーティング・システムの種類に従って、該当するインストール手順を実行して下さい。

Microsoft Windows 2000 および Windows XP の場合

- 1 [スタート]⇒[プログラム]⇒[アクセサリ]⇒[MS-DOS プロンプト] を選択します。
- 2 デフォルトのプロンプトで ipconfig/all と入力し、[Enter] キーを押します。
- 3 提供された TCP/IP 設定情報をテーブルに記入します。
- 4 [キャンセル] をクリックします。

Microsoft Windows NT の場合

- 1 [スタート]⇒[プログラム]⇒[MS-DOS プロンプト] を選択します。
- 2 デフォルトのプロンプトで ipconfig/all と入力し、[Enter] キーを押します。
- 3 提供された TCP/IP 設定情報を表に記入します。
- 4 [キャンセル] をクリックします。

Microsoft Windows 95、Windows 98 および Windows Me の場合

- 1 [スタート] ⇒ [ファイル名を指定して実行] を選択します。
- 2 winipcfg と入力します。
- 3 [OK] をクリックします。
- 4 [Ethernet Adapter] を選択します。
- 5 提供された TCP/IP 設定情報をテーブルに記入します。
- 6 [キャンセル] をクリックします。

Macintosh の場合

- 1 [Apple] ⇒ [コントロールパネル] ⇒ [TCP/IP] を選択します。

- 2 提供された TCP/IP 設定情報をテーブルに記入します。
- 3 ウィンドウを閉じます。

その他のオペレーティング・システムの場合
(UNIX、Linux など)

- 1 ユーザーのオペレーティング・システムのマニュアルを参照し、TCP/IP 設定情報画面を表示します。
- 2 提供された TCP/IP 設定情報をテーブルに記入します。
- 3 TCP/IP 設定情報画面を閉じます。

TCP/IP 設定		値
IP アドレス		. . .
サブネット・マスク		. . .
デフォルト・ゲートウェイ		. . .
DHCP 有効		はい いいえ
DNS サーバー	プライマリー	. . .
	セカンダリー	. . .

注意

S6 内側のトラステッド・ネットワークに複数のコンピューターを接続している場合は、それぞれのコンピューターの TCP/IP 設定情報を確認して下さい。

ウェブ・ブラウザ HTTP プロキシ設定の無効化

S6 を設定するには、ブラウザから S6 の中にある設定ページにアクセスします。ブラウザの HTTP プロキシ設定が有効になっている場合、このページを開くことができないので、S6 の設定を完了することができません。

HTTP プロキシ設定が有効になっている場合、インターネット上のウェブ・ページは表示できますが、他の場所にあるページは表示できません。HTTP プロキシ設定を無効にすると、S6 の中にある設定ページおよびインターネット上のウェブ・ページを表示することができます。

下記は、代表的な 3 種類のブラウザにおける HTTP プロキシ設定を無効にする手順です。ご使用のブラウザがこの 3 種類に該当しない場合は、必要な情報を調べるためにブラウザのヘルプを参照して下さい。

Netscape 4.7 の場合

- 1 Netscape を起動します。
- 2 **[編集]** ⇒ **[設定]** を選択します。
[設定] ウィンドウが表示されます。
- 3 オプションの一覧がウィンドウの左部に表示されます。**[詳細]** の左側にある + 記号をクリックし、一覧を展開表示します。
- 4 **[プロキシ]** をクリックします。
- 5 **[インターネットに直接接続する]** オプションが有効になっていることを確認します。
- 6 **[OK]** をクリックします。

Netscape 6.x の場合

- 1 Netscape を起動します。

- 2 [編集] ⇒ [設定] を選択します。
[設定] ウィンドウが表示されます。
- 3 オプションの一覧がウィンドウの左部に表示されます。[詳細] の左側にある記号をクリックし、一覧を展開表示します。
- 4 [プロキシ] をクリックします。
- 5 [インターネットに直接接続する] オプションが有効になっていることを確認します。
- 6 [OK] をクリックします。

Internet Explorer 5.0、5.5、6.0 の場合

- 1 Internet Explorer を起動します。
- 2 [ツール] ⇒ [インターネット オプション] を選択します。
[インターネット オプション] ウィンドウが表示されます。
- 3 [詳細設定] タブをクリックします。
- 4 ページをスクロールして [HTTP1.1 設定] を表示します。
- 5 チェックボックスをすべてオフにします。
- 6 [OK] をクリックします。

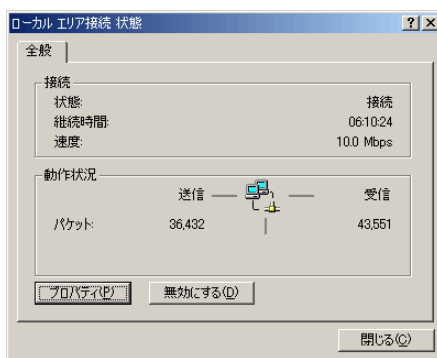
コンピューターの DHCP 設定の有効化

S6 の設定ページを開くには、DHCP を使ってネットワーク IP アドレスを受け取るようにコンピューターを構成する必要があります。ネットワーク・アドレス割り当ておよび DHCP については詳細、33 ページの「ネットワーク・アドレスの割り当て」を参照して下さい。

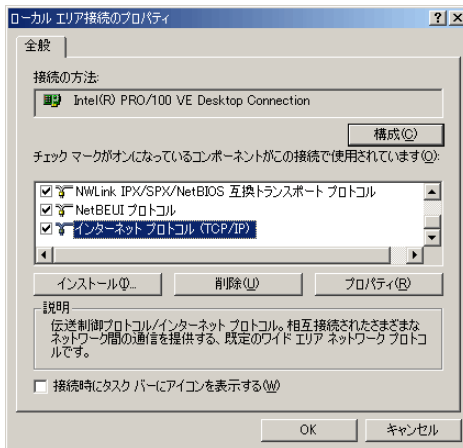
注意

このセクションで説明する設定手順は、Windows 2000 オペレーティング・システムの場合です。

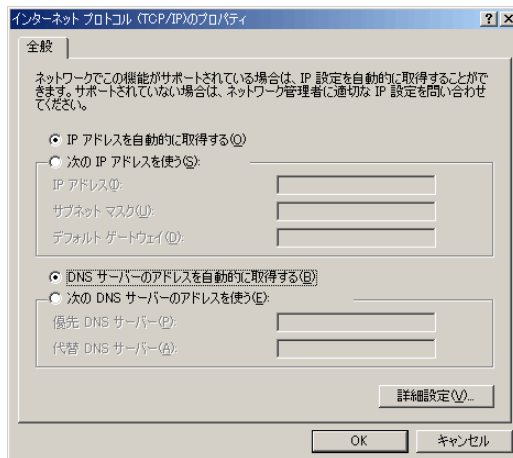
- 1 [スタート] ⇒ [設定] ⇒ [コントロール パネル] を選択します。
[コントロール パネル] ウィンドウが表示されます。
- 2 [ネットワーク] アイコンをダブルクリックします。
- 3 インターネットにアクセスする際に使う接続をダブルクリックします。
ネットワーク接続ダイアログ・ボックスが表示されます。



- 4 [プロパティ] をクリックします。
ネットワーク接続の [プロパティ] ダイアログ・ボックスが表示されます。



- 5 [インターネット プロトコル (TCP/IP)] コンポーネントをダブルクリックします。
[インターネット プロトコル (TCP/IP) のプロパティ] ダイアログ・ボックスが表示されます。



- 6 [IP アドレスを自動的に取得する] および [DNS サーバーのアドレスを自動的に取得する] を選択します。
- 7 [OK] をクリックし、[インターネット プロトコル (TCP/IP) のプロパティ] ダイアログ・ボックスを閉じます。
- 8 [OK] をクリックし、ネットワーク接続の [プロパティ] ダイアログ・ボックスを閉じます。[閉じる] をクリックし、ネットワーク接続ダイアログ・ボックスを閉じます。[コントロール パネル] ウィンドウを閉じます。

S6 の物理的な接続

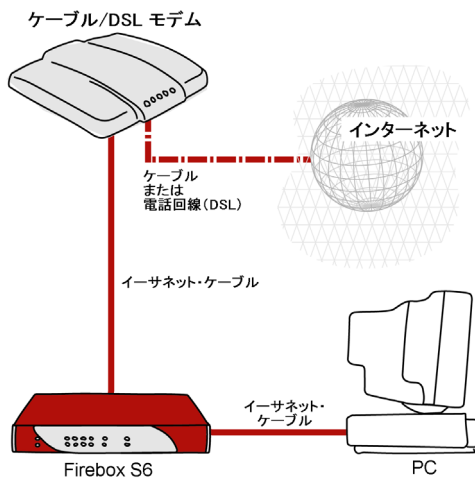
S6 は、1 台または複数のコンピューターで構成されたネットワークを保護します。また、各種アプライアンスを接続するハブとしても機能します。

S6 を 1 ～ 4 台の機器と接続する場合の配線

S6 には、コンピューター、プリンター、スキャナー、その他のネットワーク周辺アプライアンスなどを 4 台まで接続することができます。これらのアプライアンスは番号の付いた 4 個のイーサネット・ポート (0 ～ 3) に接続します。最大 4 台のアプライアンスを接続する場合は、S6 をネットワーク・ハブとして使用します。

- 1 コンピューターをシャットダウンします。
- 2 DSL/ ケーブル・モデムを使ってインターネットに接続している場合は、そのモデムの電源をオフにします。

- DSL/ ケーブル・モデムなどのインターネット接続アプライアンスとコンピューターを接続しているイーサネット・ケーブルを取り外し、S6 の WAN ポートに接続します。
これで、S6 はモデムなどのインターネット接続機器と直接接続されました。
- S6 に付属しているストレート・スルー・イーサネット・ケーブルの端を S6 のイーサネット・ポート (0 ~ 3) のいずれかに接続します。もう一方の端はコンピューターのイーサネット・ポートに接続します。
これで、S6 はインターネットとコンピューターの両方に接続されました。



- DSL/ ケーブル・モデムを使ってインターネットに接続している場合は、そのモデムの電源を再びオンにします。モデムのインジケータ・ライトの点滅が止まったら、モデムは使用可能な状態になります。
- AC アダプターを S6 に接続します。次に AC アダプターを電源に接続します。

7 コンピューターを再起動します。

デフォルト出荷設定については 27 ページの「デフォルト出荷設定」を、特別な設定内容については 33 ページの「外部ネットワークの設定」および 38 ページの「トラステッド・ネットワークの設定」を参照して下さい。

S6 を 5 台以上の機器と接続する場合の配線

S6 の裏面パネルにはイーサーネット・ポートが 4 個 (0 ~ 3) しか実装されていませんが、ネットワーク・ハブを使うことで 5 台以上のアプライアンスを S6 に接続することができます。

S6 には 10 シート分のライセンスが付属しています。つまり、トラステッド・ネットワーク上にあるコンピューターを最大 10 台までインターネットに接続することができます。トラステッド・ネットワーク上に 11 台以上のコンピューターを接続することはできませんが、S6 経由でインターネットに接続できるのは 10 台だけです。シートはコンピューターがインターネットに接続したときに取得され、接続が切れると自由に使用できる状態になります。ライセンスのアップグレード版については、ウォッチガード社ウェブサイトをご覧ください。

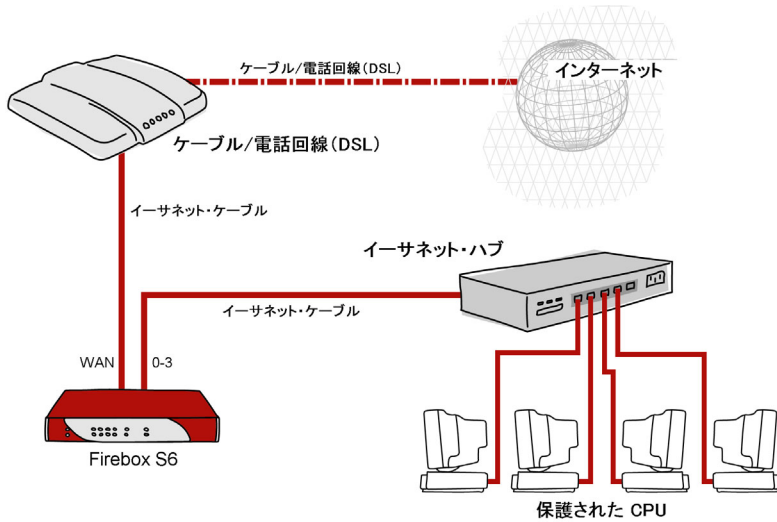
<http://www.watchguard.com/sales/buyonline.asp>

5 台以上のアプライアンスを S6 に接続するには、次のものが必要になります。

- ・ イーサーネット・ハブ
- ・ RJ-45 コネクタ付きのストレート・スルー・イーサーネット・ケーブル (接続するコンピューターの台数分)
- ・ 各ハブと S6 を接続するためのストレート・スルー・イーサーネット・ケーブル

5 台以上のアプライアンスを S6 に接続するには、下記の手順に従って下さい。

- 1 コンピューターをシャットダウンします。DSL/ ケーブル・モデムを使ってインターネットに接続している場合は、そのモデムの電源を取り外します。
- 2 DSL/ ケーブル・モデムなどのインターネット接続機器とコンピューターを接続しているイーサネット・ケーブルのコンピューター側を取り外し、S6 の WAN ポートに接続します。
これで、S6 はモデムなどのインターネット接続機器と直接接続されました。
- 3 S6 に付属しているストレート・スルー・イーサネット・ケーブルの一方の端を、S6 の 4 つのイーサネット・ポート (0 ~ 3) のいずれかに接続します。もう一方の端をハブのアップリンク・ポートに接続します。
これで、S6 はインターネットとイーサネット・ハブの両方に接続されました。
- 4 イーサネット・ケーブルを使って、各コンピューターのイーサネット・ポートとイーサネット・ハブのアップリンク・ポートを接続します。



- 5 DSL/ ケーブル・モデムを使ってインターネットに接続している場合は、モデムの電源を再びオンにします。モデムのインジケータ・ライトの点滅が止まったら、モデムは使用可能な状態になります。
- 6 AC アダプターを S6 に接続します。次に AC アダプターを電源に接続します。
- 7 コンピューターを再起動します。

デフォルト出荷設定については 27 ページの「デフォルト出荷設定」を、特別な設定内容については 33 ページの「外部ネットワークの設定」および 38 ページの「トラステッド・ネットワークの設定」を参照して下さい。

S6 の基本事項

S6 の設定は、S6 のソフトウェアに含まれているウェブ・ページから行います。これらの設定ページは、ウェブ・ブラウザからアクセスすることができます。

S6 の [システム・ステータス] ページ

ウェブ・ブラウザのウィンドウで、トラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページを表示します。

デフォルト IP アドレスは `http://192.168.111.1` です。

[システム・ステータス] ページが表示されます。



Firebox 設定画面

LiveSecurity | ヘルプ | サポート | 会社概要 | 販売代理店

システム・ステータス
ネットワーク
外部
トラステッド
オブシヨナル
ルート
Dual ISP
ネットワーク統計
ダイナミックDNS
管理
システム・セキュリティ
VPN Manager 有効
更新
アップグレード
設定ファイルの表示
ファイアウォール
受信
送信
カスタム・サービス
利用できないサイト
ブロックリスト
パス・スルー
ロギング
WSEP に対する時間
Syslog ロギング
システム時間
WebBlocker
設定
グループ
利用できるサイト
拒否サイト
VPN
管理 VPN
手動 VPN
MUVPN クライアント
VPN 統計
VPN Keep Alive

システム・ステータス

Firebox 設定画面 構成サイトへようこそ。標準構成では、ネットワーク・セキュリティ侵害に対する基本的な保護機能を利用できます。このサイトでは、各ユーザーのセキュリティ・ニーズに応じた Firebox 設定画面をカスタマイズできます。

不明な点は、本リリースについて解説したヘルプ・ページまたはオンライン・ドキュメントを参照して下さい。

コンポーネント	バージョン	機能	ステータス	
ファイアウォール	6.3 (S6-02) Oct15 2003 ビルド 004	WSEP に対する時間	無効	設定
ブート ROM	4.8	VPN Manager 有効	無効	設定
プラットフォーム	WatchGuard Firebox S6	Syslog	無効	設定
シリアル番号	6061048780008	パス・スルー	無効	設定
オプション				
		ユーザー使用許諾権	20	アップグレード
		管理 VPN	無効	設定
		手動 VPN	設定済み 最大 6	設定
		MUVPN クライアント	設定済み 最大 5	設定
		WebBlocker	無効	設定
		Dual ISP	無効	設定
		VPNforce	未インストール	アップグレード



再起動 更新

トラステッド・ネットワーク	ファイアウォール	外部ネットワーク
IP アドレス 192.168.111.1	送信 サービス 受信	モード 手動
サブネットマスク 255.255.255.0	➡ Outgoing	IP アドレス 10.168.5.210
DHCP 有効	FTP ←	サブネットマスク 255.255.255.248
ゲートウェイ IP 192.168.111.2	HTTP ←	ゲートウェイ 10.168.5.209
MAC 00907F-130759		MAC 00907F-130758

オブシヨナル・ネットワーク	
使用	Dual ISP
モード	DHCP クライアント
IP アドレス	無効
サブネットマスク	無効
ゲートウェイ	無効
MAC	無効

[システム・ステータス] ページは、S6 の設定を行うメイン・ページです。このページには、S6 についての設定情報が表示されます。表示される情報は、次のとおりです。

- ・ ファームウェアのバージョン
- ・ アプライアンスのシリアル番号

- S6 の以下の機能のステータス
 - WSEP に対するロギング
 - VPN Manager アクセス
 - シスログ (Syslog)
 - パス・スルー
- アップグレード版・オプションのステータス
- トラストド・ネットワークおよび外部ネットワークに関する設定情報
- ファイアウォール設定に関する設定情報 (受信サービスと送信サービス)
- S6 を再起動するリブート・ボタン

注意

外部ネットワークが PPPoE クライアントを使うように設定されている場合、[システム・ステータス] ページには接続ボタンまたは切断ボタンが表示されます。これらのボタンを使って、PPPoE 接続を開始または終了することができます。

デフォルト出荷設定

S6 のデフォルトネットワークおよびコンフィギュレーション設定は、次のとおりです。

外部ネットワーク

外部ネットワーク設定は DHCP を使用します。

トラステッド・ネットワーク

トラステッド・ネットワークのデフォルト IP アドレスは 192.168.111.0 です。

トラステッド・ネットワーク上のコンピューターは、DHCP を使って IP アドレスが与えられます。

ファイアウォール設定

受信サービスはすべて遮断されます。

ファイアウォールの外側に出ていくトラフィックがすべて許可される送信サービスです。

ファイアウォール・オプションはすべて無効です。

DMZ パススルーは無効です。

システム・セキュリティ

システム・セキュリティは無効であり、システム管理者およびパスフレーズは設定されていません。つまり、トラステッド・ネットワーク上のすべてのコンピューターが設定ページを表示することができます。

S6 リモート管理は無効です。

VPN Manager アクセスは無効です。

リモート・ロギングは設定されていません。

WebBlocker

WebBlocker は無効であり、設定情報が設定されていません。

アップグレード版・オプション

アップグレード版・オプションは無効です。設定ページでライセンス・キーを入力すると、アップグレード版・オプションが有効になります。

S6 のデフォルト出荷設定へのリセット

設定上の問題が解決できない場合は、S6 をデフォルト出荷設定にリセットします。停電により S6 のファームウェアが破損したり、システム・セキュリティ・パスフレーズを知らない場合、S6 をデフォルト出荷設定にリセットする必要があります。S6 をデフォルト出荷設定にリセットするには、下記の手順に従って下さい。

- 1 電源ケーブルを抜きます。
- 2 リセット・ボタンを押し続けます。
- 3 電源ケーブルを接続します。
- 4 S6 の正面パネルの赤い LED が点灯し、さらに消灯するまでリセット・ボタンを押し続けます。
- 5 電源ケーブルを抜きます。
- 6 電源ケーブルを接続します。
PWR インジケーターが点灯したら、リセットは完了です。

ベース・モデルの S6

ベース・モデルの S6 には 10 台分のライセンスが付属しています。つまり、トラステッド・ネットワーク上にある最大 10 台のコンピューターが同時にインターネットに接続することができます。トラステッド・ネットワーク上に 11 台以上のコンピューターを接続することはできますが、S6 を介してインターネットに接続できるのは 10 台までです。詳しくは 21 ページの「S6 を 5 台以上の機器と接続する場合の配線」を参照して下さい。

S6 および LiveSecurity サービスの登録

S6 の導入と構成が完了したら、S6 の登録および LiveSecurity サービスへのサブスクリプション登録を行います。LiveSecurity サービスを登録すると、危険警告通知、ウィルスからの保護（無料）、ソフトウェア・アップグレード版、ウェブまたは電話による技術サポート、豊富なオンライン・ヘルプ・リソースへのアクセス、ウォッチガード社のユーザー・フォーラムなどを利用できます。また、購入したアップグレード版のライセンス・キーを取得するために、LiveSecurity サービスへのサブスクリプション登録が必須となります。

登録には S6 のシリアル番号が必要になります。S6 のシリアル番号は、アプライアンスの底面に記載されています。シリアル番号は、以下の表に記入しておいて下さい。

シリアル番号	
--------	--

LiveSecurity サービスを受けるためには、ユーザーが S6 の登録をウォッチガード社ウェブサイトで行います。

<http://www.watchguard.co.jp/activate/index.html>

注意

LiveSecurity サービスを開始するには、ブラウザーの JavaScript 設定を有効にしておく必要があります。

登録済みの方は、ユーザー名とパスワードを入力します。まだ、ウォッチガード社ウェブサイトでユーザー・プロフィールを作成していない方は、新しいアカウントを作成します。まず、ご使用の製品を選択し、次に画面の指示に従って製品登録を行います。

LiveSecurity サービスのユーザー・プロフィール情報を以下の表に記入しておいて下さい。

ユーザー名	
パスワード	

この情報は他人に漏らさないようにして下さい。

S6 のリポート

ローカル・ネットワーク上にある S6 をリポートするには、次のいずれかの手順を実行します。

注意

S6 のリブートには 30 秒ほどかかります。S6 の正面パネルにあるモード・インジケーターが消灯し、その後点灯します。

- 1 ウェブ・ブラウザのウィンドウで、トラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。

- 2 [リブート] をクリックします。

または

- 1 電源ケーブルをいったん取り外し、再度接続します。

リモート・システム上にある S6 をリブートするには、次のいずれかの手順を実行します。

注意

リモート S6 は、インターネットからの HTTP (ウェブ) トラフィックまたは FTP トラフィックの受信を許可するように設定する必要があります。S6 が受信トラフィックを受け取るように設定する手順については、66 ページの「受信サービスと送信サービスの設定」を参照して下さい。

- 1 ウェブ・ブラウザのウィンドウで、リモート S6 の外部ネットワーク IP アドレスを入力し、リモート S6 の [システム・ステータス] ページを表示します。

- 2 [リブート] をクリックします。

または

- 1 リモート S6 に FTP コマンドを送信します。FTP アプリケーションを使ってリモート S6 に接続し、`quote rebt` というコマンドを入力します。

ネットワーク・インターフェイスの設定

外部ネットワークの設定

外部ネットワークを設定するには、S6 が ISP と通信する方法を選択します。選択する通信方法は、ISP がネットワーク・アドレスを割り当てる方法によって決まります。一般的な方法としては、静的アドレス、DHCP、PPPoE などがあります。

ネットワーク・アドレスの割り当て

TCP/IP ネットワークを接続するには、各コンピューターに IP アドレスを割り当てる必要があります。IP アドレスの割り当てには、動的割り当てと静的割り当てがあります。

- 動的 IP アドレスを使う場合、ISP は各コンピューターがネットワークに接続するたびに、各コンピューターに別々のアドレスを割り当てます。コンピューターが接続を切断すると、その IP アドレスは解放され、他のコンピューターに割り当てられるようになります。

- ・ 静的 IP アドレスを使う場合、ネットワーク上のすべてのコンピューターにはそれぞれ固有の IP アドレスが割り当てられます。複数のコンピューターが同一の IP アドレスを持つことはありません。

ほとんどの ISP は、DHCP（動的ホスト・コンフィギュレーション・プロトコル）を使って動的に IP アドレスを割り当てる方式を採用しています。コンピューターがネットワークに接続すると、ISP にある DHCP サーバーがそのコンピューターに IP アドレスを自動的に割り当てます。つまり、ISP は IP アドレスの割り当てを手作業で行う必要がありません。

ISP によっては、PPPoE（イーサネット上でのポイント・ツー・ポイント・プロトコル）を使って IP アドレスを割り当てる方式を採用しているところがあります。PPPoE は、標準的なダイヤルアップ接続をエミュレートすることによって、イーサネットと PPP の長所を組み合わせたものです。この方式では、ダイヤルアップ/DSL モデム/ケーブル・モデム接続向けに設計されたセキュリティ、課金、認証を利用することができます。PPPoE を使うように S6 を設定した場合、[システム・ステータス] ページに表示されるボタンで外部ネットワークとの接続を制御することができます。

ISP が使用している割り当て方式がわからない場合は、ISP にお問い合わせ下さい。

動的アドレス割り当てを使う場合の S6 外部ネットワークの設定

S6 は、DHCP を使って外部アドレス情報を自動的に取得するようにデフォルトで設定されています。ISP がこの方式をサポートしている場合、S6 をリブートしてインターネットに接続すると、S6 は ISP から IP アドレス情報を取得します。特に、S6 において設定を行う必要はありません。

アドレス割り当てを使う場合の S6 外部ネットワークの設定

ISP が静的アドレス割り当て方式を採用している場合、IP アドレス情報をコンピューターから S6 に渡す必要があります。この場合、ISP はコンピューターと直接通信するのではなく、S6 経由で通信するようになります。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、**[ネットワーク]** ⇒ **[外部ネットワーク構成]** を選択します。
[外部ネットワーク構成] ページが表示されます。
- 3 **[設定モード]** ドロップダウン・リストから **[手動設定]** を選択します。
ページが更新されます。

システム・ステータス	ネットワーク
外部	外部ネットワーク構成
トラステッド	
オプション	
ルート	
Dual ISP	
Network Statistics	
DynamicDNS	
管理	
システム・セキュリティ	
VPN Manager アクセス	
更新	
アップグレード	
設定ファイルの表示	
ファイアウォール	
受信	
送信	

設定モード	手動設定
IP アドレス	<input type="text" value="0.0.0.0"/>
サブネット・マスク	<input type="text" value="255.255.255.0"/>
デフォルト・ゲートウェイ	<input type="text" value="0.0.0.0"/>
プライマリ DNS	<input type="text" value="66.235.63.2"/>
セカンダリ DNS	<input type="text" value="66.235.63.4"/>
DNS ドメイン接尾辞	<input type="text"/>
<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

- 4 導入作業時にメモしておいたコンピューターの TCP/IP 設定情報を入力します。14 ページの表、「TCP/IP 設定」を参照してください。
- 5 **[サブミット]** をクリックします。
設定に対する変更結果が S6 に保存されます。

PPPoE を使う場合の S6 外部ネットワークの設定

ISP が PPPoE による IP アドレス割り当て方式を採用している場合、S6 を設定するために PPPoE のログイン名とパスワードが必要になります。

PPPoE を使うように S6 を設定するには、次の手順に従って下さい。

- 1 ウェブ・ブラウザを起動して **[停止]** をクリックします。
この時点では、インターネット接続がまだ設定されていないため、インターネットからホーム・ページをロードすることはできません。ただし、ブラウザは S6 の中にある設定ページを開くことができます。
- 2 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して S6 の **[システム・ステータス]** ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 3 左部のナビゲーション・バーで、
[ネットワーク] ⇒ **[外部ネットワーク構成]** を選択します。
[外部ネットワーク構成] ページが表示されます。
- 4 **[設定モード]** ドロップダウン・リストから **[PPPoE クライアント]** を選択します。
ページが更新されます。

システム・ステータス	ネットワーク
ネットワーク	外部ネットワーク構成
外部	
トラステッド	
オプション	
ルート	
Dual ISP	
Network Statistics	
DynamicDNS	
管理	
システム・セキュリティ	
VPN Manager アクセス	
更新	
アップグレード	
設定ファイルの表示	
ファイアウォール	
受信	
送信	

設定モード **PPPoE クライアント**

名前

ドメイン

パスワード

無操作タイムアウト (単位分)

切断された接続を自動的に復元

PPPoE デバッグ・トレースを有効化

- 5 該当フィールドの中に ISP から発行された PPPoE ログイン名、ドメイン、PPPoE パスワードを入力します。
- 6 使用されていない TCP 接続が切断される前に、タイムアウト時間を入力します。
- 7 **[切断された接続を自動的に復元]** チェックボックスをオンにします。

このオプションにより、S6 と PPPoE サーバーの間において常にトラフィック・フローが維持されるようになります。パケット損失が頻繁に発生する場合でも、このオプションを使用すれば S6 は PPPoE 接続を維持できます。トラフィック・フローが停止した場合、S6 はリブートします。リブートすると、通常、接続が復旧します。ISP は、この一定したトラフィック・フローにより、接続が維持されていると見なします。ISP 側の規定および課金ポリシーにより、このオプションの使用可否が決定します。ウォッチガード社テクニカル・サポートでは、このオプションを問題解決策として使用しています。
- 8 PPPoE のデバッグ・トレースをアクティブにするには、**[PPPoE デバッグ・トレースを有効化]** チェックボックスをオンにします。
- 9 **[サブミット]** をクリックします。

設定に対する変更結果が S6 に保存されます。

トラステッド・ネットワークの設定

DHCP サーバー・オプションにより、S6 はトラステッド・ネットワーク上のコンピューターにアドレスを割り当てるように設定されています。S6 は、アドレス割り当てに DHCP を使用します。S6 がトラステッド・ネットワークに新たに接続されたコンピューターからリクエストを受け取ると、S6 はこのコンピューターに IP アドレスを割り当てます。DHCP サーバーを使って IP アドレスを割り当てる場合は、DHCP リレイ・オプションを使用可能にします。このオプションを使用すると、S6 は DHCP リクエストを指定された DHCP サーバーに転送します。

DHCP サーバーと DHCP リレイの設定

DHCP サーバーを設定するには、次の手順に従って下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、
[ネットワーク] ⇒ [トラステッド] を選択します。
[トラステッド・ネットワーク構成] ページが表示されます。

システム・ステータス	ネットワーク
ネットワーク	トラステッド・ネットワーク構成
外部	
トラステッド	
オプション	
ルート	IP アドレス <input type="text" value="192.168.111.1"/>
Dual ISP	サブネット・マスク <input type="text" value="255.255.255.0"/>
Network Statistics	<input checked="" type="checkbox"/> トラステッド・ネットワークで DHCP サーバーを有効化
DynamicDNS	DHCP サーバーの最初のアドレス <input type="text" value="192.168.111.2"/>
管理	WINS サーバー・アドレス <input type="text"/>
システム・セキュリティ	DNS サーバー・アドレス <input type="text"/>
VPN Manager アクセス	セカンダリ DNS サーバー・アドレス <input type="text"/>
更新	DNS ドメイン接尾辞 <input type="text"/>
アップグレード	<input type="checkbox"/> DHCP リレーを有効化
設定ファイルの表示	DHCP リレー・サーバー <input type="text"/>
ファイアウォール	
受信	
送信	
カスタム・サービス	
利用できないサイト	

- IP アドレスとサブネット・マスクを該当するフィールドに入力します。
- [トラステッド・ネットワークで DHCP サーバーを有効化]** チェックボックスをオンにします。
- トラステッド・ネットワーク上のコンピューターに割り当てることができる最初の IP アドレスを該当するフィールドに入力します。
- WINS サーバー・アドレス、DNS プライマリ・サーバー・アドレス、DNS セカンダリー・サーバー・アドレス、DNS ドメイン・サーバー・サフィックスを該当するフィールドに入力します。
- DHCP リレー・サーバーを設定するには、**[DHCP リレーを有効化]** チェックボックスをオンにします。
- DHCP リレー・サーバーの IP アドレスを該当するフィールドに入力します。
- [サブミット]** をクリックします。

10 S6 をリブートします。

S6 は、すべての DHCP 要求を指定したリモート DHCP サーバーに転送し、DHCP サーバーから返された IP アドレスをトラステッド・ネットワーク上のコンピューターに中継します。S6 が指定したリモート DHCP サーバーに 30 秒以内に接続できない場合、内蔵の DHCP サーバー機能を使う方式に復帰し、トラステッド・ネットワーク上のコンピューターに応答します。

トラステッド・ネットワーク上に追加されたコンピューターの設定

S6 には、コンピューター、プリンター、スキャナー、その他のネットワーク機器などを最大 4 台まで直接接続することができます。アプライアンスを追加するときは、RJ-45 コネクターの付いた 10 Base T イーサーネット・ケーブルを使って接続します。

トラステッド・ネットワークにコンピューターを追加するには、次の手順に従って下さい。

- 1 追加するコンピューターにイーサーネット・カードが装着されていることを確認します。
- 2 コンピューターをシャットダウンします。
- 3 21 ページの「S6 を 5 台以上の機器と接続する場合の配線」に示されたように、コンピューターをネットワークに接続します。
- 4 コンピューターを再起動します。
- 5 16 ページの「コンピューターの DHCP 設定の有効化」に示されたように、DHCP を使ってアドレスを取得するようにコンピューターを設定します。
- 6 コンピューターをシャットダウンし、その後再起動します。

静的アドレスを使用する場合のトラステッド・ネットワークの設定

S6 の DHCP サーバーを使用不可にしてアドレスを静的に割り当てるには、次の手順に従って下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、**[ネットワーク] ⇒ [トラステッド]** を選択します。
[トラステッド・ネットワーク構成] ページが表示されます。
- 3 IP アドレスとサブネット・マスクを該当フィールドに入力します。
- 4 **[トラステッド・ネットワークで DHCP サーバーを有効化]** チェックボックスをオフにします。
- 5 **[サブミット]** をクリックします。
- 6 必要に応じて、S6 をリブートします。
- 7 静的アドレスを使用するようにトラステッド・ネットワーク上のアプライアンスを設定します。

静的ルートの設定

ルーターまたはスイッチを介して接続されているトラステッド・ネットワークの別のセグメントに指定したパケットを送信するには、静的ルートを設定します。

静的ルートを設定するには、次の手順に従って下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、
[ネットワーク] ⇒ [ルート] を選択します。
[ルート] ページが表示されます。



- 3 [追加] をクリックします。
[ルートの追加] ページが表示されます。

The screenshot shows a web-based configuration interface. On the left is a sidebar menu with categories: システム・ステータス, ネットワーク, and 管理. Under 'ネットワーク', the 'ルート' (Route) option is selected. The main content area is titled 'ネットワーク > ルート' and 'ルートの追加'. It contains a form with three input fields: 'タイプ' (Type) is a dropdown menu with 'ホスト' (Host) selected; 'アドレス' (Address) is a text input field; 'ゲートウェイ' (Gateway) is a text input field. At the bottom of the form are three buttons: 'Submit', 'Reset', and 'Cancel'.

- 4 [タイプ] ドロップダウン・リストから [ホスト] または [ネットワーク] を選択します。
 - 5 ルートの IP アドレスとゲートウェイを該当フィールドに入力します。
ルートのゲートウェイは、ルーターのローカル・インターフェイスです。
 - 6 [サブミット] をクリックします。
- ルートを削除するには、削除するルートを選択して [削除] をクリックします。

ネットワーク統計情報の表示

ネットワーク統計ページには、ネットワーク・パフォーマンスに関する情報が表示されます。このページはトラブルシューティングに役立ちます。

ネットワーク統計ページを表示するには、次の手順に従って下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、
[ネットワーク] ⇒ [ネットワーク統計] を選択します。
[ネットワーク統計] ページが表示されます。

システム・ステータス	ネットワーク
ネットワーク	統計
外部	
トラステッド	
オプション	
ルート	
Dual ISP	
Network Statistics	IP
Dynamic DNS	IP: Up for 2 days 1 hour 34 minutes 30 seconds
管理	Network Buffers Allocated/Total (4/40) Memory Total/Lar
システム・セキュリティ	Sockets Allocated/Total (12/80) NAT Ports Avail (1000)R
VPN Manager アクセス	Tx: packets (2388)
更新	Rx: packets (89006) hdr Err(39) delivered (68867)
アップグレード	
設定ファイルの表示	外部ネットワーク
ファイアウォール	eth0: Link encap:Ethernet HWaddr 00:90:7f:12:9b:07 inet addr
受信	RX packets:2539 errors:0 bcast:815671 disc:0 unk:0
送信	TX packets:2382 errors:0 bcast:2
カスタム・サービス	
利用できないサイト	トラステッド・ネットワーク
ファイアウォール・オプション	

ダイナミック DNS サービスの設定

この機能を使用すると、S6 の外部 IP アドレスをダイナミック DNS (Domain Name Server) サービス (DynDNS.org) に登録できます。ダイナミック DNS サービス機能を利用すると、ISP が新しい

IP アドレスを割り当てた場合に、ユーザーのドメイン名に接続された IP アドレスが正しく変更されるようになります。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。

注意

ウォッチガード社は `dyndns.org` に加入していません。

- 2 左部のナビゲーション・バーで、
[ネットワーク] ⇒ [ダイナミック DNS クライアント] を選択
します。
[ダイナミック DNS クライアント] ページが表示されます。

The screenshot shows the 'DynamicDNS' configuration page. On the left is a navigation menu with items: システム・ステータス, ネットワーク, 外部, トラステッド, オプション, ルート, Dual ISP, Network Statistics, DynamicDNS (highlighted), 管理, システム・セキュリティ, VPN Manager アクセス, 更新. The main content area is titled 'ネットワーク 動的 DNS クライアント'. It contains a checkbox for '動的 DNS クライアントの有効化' (unchecked), three input fields for 'ドメイン', '名前', and 'パスワード', and 'Submit' and 'Reset' buttons at the bottom.

- 3 [ダイナミック DNS クライアントの有効化] チェックボックスをオンにします。
- 4 ドメイン、名前、およびパスワードを該当フィールドに入力します。

注意

S6 は、タイム・サーバーに接続したときに `members.dyndns.org` の IP アドレスを受信します。

5 [サブミット] をクリックします。

OPT ポート・アップグレード版の設定

S6 のオプション・ポート (OPT ポート) は、次の 2 つのアップグレード版をサポートしています。

- Dual ISP Port アップグレード版
- VPNforce Port アップグレード版

S6 をアップグレード版にするには、新たにライセンスを購入し、新しいアップグレード版・オプションをアクティブにします。S6 のアップグレード版にする方法についての詳細は、61 ページの「S6 アップグレード版・オプションの有効化」を参照して下さい。

注意

OPT ポートは、Dual ISP Port アップグレード版または VPNforce Port アップグレード版を購入した場合にのみ使用できます。OPT ポートをトラステッド・ネットワーク上のイーサネット・ポートとして使うことはできません。

Dual ISP Port の設定

Dual ISP Port アップグレード版は、外部インターフェイスの冗長化機能を提供します。このアップグレード版を導入すると、プライマリ外部ポートの接続に障害が発生した場合、S6 はオプション・ポートを使って新しい接続を開始します。

ポリシーを新規に定義する必要はありません。オプション・インターフェイスは、外部インターフェイスで使われるものと同じポリシーを使用します。

S6 では次の 2 つの方法を使って、外部ポート接続に障害が発生しているかどうかを判断します。

- ・ 最も近くにあるルーターへのリンクのステータス
- ・ 指定された場所に対する ping コマンドの発行

S6 は、デフォルト・ゲートウェイまたは管理者によって指定された別の場所に対して ping コマンドを発行します。応答がない場合、S6 はセカンダリー外部ネットワーク接続を使用するように切り替えを行います。

このアップグレード版・オプションがアクティブになっている場合、これらは自動的に実行されます。

- ・ 外部ポート (EXT) 接続に障害が発生した場合、オプション・ポート (OPT) 接続が開始されます。
- ・ オプション・ポート (OPT) 接続に障害が発生した場合、外部ポート (EXT) 接続が開始されます。
- ・ 外部ポート (EXT) およびオプション・ポート (OPT) の両方の接続に障害が発生した場合、S6 は、いずれかの接続が確立するまで両ポートの接続を繰り返し試行します。

オプション・ポート (OPT) を使用している場合で、IP アドレスの割り当てに PPPoE を使っていないときは、外部ポート (EXT) 接続が復旧しても、外部ポート (EXT) 接続に自動的に戻ることはありません。つまり、オプション・ポート (OPT) に切り替わった場合、外部ポート (EXT) が復旧したら、管理者が手作業で設定を変更して外部ポート (EXT) 接続に戻す必要があります。

PPPoE を使っている場合、無効タイムアウトを設定し、トラフィックが再開されるまでの間、障害状態の TCP 接続は無効になります。PPPoE の設定については 36 ページの「PPPoE を使う場合の S6 外部ネットワークの設定」を参照して下さい。外部ポート (EXT) 接続に障害が発生した場合、オプション・ポート (OPT)

接続が開始されます。TCP 接続がタイムアウトになるまでの間、オプション・ポート (OPT) は接続されたままになります。トラフィックが再開されると、S6 はまず外部ポート (EXT) を使った接続を試みます。接続が確立できた場合、外部ポート (EXT) 接続が再び使われます。外部ポート (EXT) 接続がまだ使用可能な状態になっていない場合、S6 はオプション・ポート (OPT) を使った接続を試みます。

S6 をアップグレードし、アップグレード・オプションをアクティブにしたら、次の手順に従って設定を完了して下さい。

- 1 ストレート・スルー・イーサネット・ケーブルの一方の端を OPT ポートに接続し、もう一方の端をセカンダリー外部ネットワーク接続機器に接続します。セカンダリー外部ネットワーク接続機器としては、DSL モデム、ケーブル・モデム、ハブが使用できます。
- 2 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 3 左部のナビゲーション・バーで、
[Network] ⇒ **[Dual ISP オプション]** を選択します。
[Dual ISP オプション] ページが表示されます。

システム・ステータス	ネットワーク
ネットワーク	Dual ISP オプション
外部	
トラステッド	
オプション	
ルート	
Dual ISP	<input type="checkbox"/> Dual ISP の有効化
ネットワーク統計	外部で ping するホスト <input type="text"/>
ダイナミックDNS	オプションで ping するホスト <input type="text"/>
管理	Ping 間隔 (秒単位) <input type="text" value="60"/>
システム・セキュリティ	応答タイムアウト (秒単位) <input type="text" value="5"/>
VPN Manager 対応	応答制限なし <input type="text" value="5"/>
更新	
アップグレード	<input type="button" value="サブミット"/> <input type="button" value="リセット"/>
設定ファイルの表示	

- 4 [Dual ISP の有効化] チェックボックスをオンにします。
- 5 インターフェイスとオプション・インターフェイスの IP アドレスを該当するフィールドに入力します。
- 6 ping コマンドの発行間隔 (秒単位) と応答を待つ時間 (秒単位) を該当するフィールドに入力します。
- 7 ping コマンドを発行する回数の上限值を該当するフィールドに入力します。
- 8 [サブミット] をクリックします。

VPNforce™ Port の設定

VPNforce Port アップグレード版を利用すると、S6 のオプション・ポート (OPT) を使って、トラステッド側の 2 つ目のネットワークに接続することができます。このオプションを使用すると、ファイアウォールの保護を在宅勤務者やリモート・オフィスのネットワークにまで拡張することができます。新規ユーザーは、社内ネットワークへのセキュア・アクセスと、インターネットへの保護されたアクセスを得ることができます。

オプション・ポート (OPT) を VPNforce Port アップグレード版に使用すると、トラステッド・ネットワークによって使われるネットワークとは異なる新しいネットワークが定義されます。オプション・ポートに接続されたネットワークのデフォルト IP アドレスは 192.168.112.0 です。

S6 をアップグレードし、このアップグレード・オプションをアクティブにしたら、次の手順に従って設定を完了して下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、
[ネットワーク] ⇒ [オプション・ネットワーク構成] を選択します。
[オプション・ネットワーク構成] ページが表示されます。

システム・ステータス	ネットワーク
ネットワーク	外部
外部	トラステッド
トラステッド	オプション
オプション	ルート
ルート	Network Statistics
Network Statistics	DynamicDNS
DynamicDNS	管理
管理	システム・セキュリティ
システム・セキュリティ	VPN Manager アクセス
VPN Manager アクセス	更新
更新	アップグレード
アップグレード	設定ファイルの表示
設定ファイルの表示	ファイアウォール
ファイアウォール	受信
受信	送信
送信	カスタム・サービス
カスタム・サービス	利用できないサイト
利用できないサイト	ファイアウォール・オプション
ファイアウォール・オプション	パス・スルー
パス・スルー	ロギング
ロギング	WSEPP に対するロギング
WSEPP に対するロギング	Syslog ロギング
Syslog ロギング	システム時間
システム時間	WebBlocker
WebBlocker	

ネットワーク
オプション・ネットワーク構成

オプション・ネットワークの有効化

IP アドレス

サブネット・マスク

オプション・ネットワークで DHCP サーバーを有効化

DHCP サーバーの最初のアドレス

WINS サーバー・アドレス

DNS サーバー・アドレス

セカンダリ DNS サーバー・アドレス

DNS ドメイン接尾辞

オプション・ネットワークで DHCP リレーを有効化

DHCP リレー・サーバー

オプション・ネットワークとトラステッド・ネットワーク間のトラフィックを有効化

現在のインターフェイス上で暗号化 MUVPN 接続を要求

- VPNforce Port を使用可能にするには、[オプション。ネットワークの有効化] チェックボックスをオンにします。
- オプション・インターフェイスに対する IP アドレス、DHCP サーバー、DHCP リレーを該当するフィールドに入力します。これは、トラステッド・ネットワークの設定と同じです。これらのフィールドについての詳細は 38 ページの「トラステッド・ネットワークの設定」を参照して下さい。
- オプション・ネットワークとトラステッド・ネットワークの間でトラフィックを受け渡しできるようにするには、[Allow traffic between Optional Network and Trusted Network] チェックボックスをオンにします。

- 6 このインターフェイスにおいて暗号化された MUVPN 接続を要求するには、**[現在のインターフェイス上で暗号化 MUVPN 接続を要求]** チェックボックスをオンにします。
- 7 **[サブミット]** をクリックします。

管理オプション

S6 の [管理] ページでは、S6 へのアクセス方法を設定できます。例えば、システム・セキュリティ、S6 リモート管理機能、VPN Manager アクセスの設定などを行うことができます。また、ファームウェアの更新、アップグレード版・オプションの有効化、S6 コンフィギュレーション・ファイルのテキスト形式での表示を実行することができます。

[システム・セキュリティ] ページ

[システム・セキュリティ] ページでは、S6 の設定をするためのアクセス権を制御することができます。システム管理者名とシステム・パスワードを設定すると、設定ページへのアクセスを制限できます。リモート管理を使用可能にし、外部ネットワークから S6 を設定できるように設定することができます。

システム・セキュリティ

パスワードは、トラステッド・ネットワーク上の権限のないユーザーが S6 の設定を不正に変更することを防止します。パスワードの使用は、ネットワーク・セキュリティにとって重要です。

注意

システム管理者名とパスワードを安全な場所に記入しておいて下さい。システム・セキュリティを使用可能にすると、設定ページを表示する際に、システム管理者名とパスワードの入力が必要になります。システム管理者名とパスワードを知らない場合、S6 をデフォルト出荷設定にリセットする必要があります。詳しくは 27 ページの「デフォルト出荷設定」を参照して下さい。

システム管理者パスワードは毎月変更して下さい。パスワードは 8 文字で、文字、数字、記号を組み合わせで作成します。一般的な英語や外国語の単語は使用しないで下さい。セキュリティを強化するため、パスワードには特殊文字や数字 1 つ以上含め、大文字と小文字を混在させることをお勧めします。

次の手順に従って、システム・セキュリティを使用可能にして下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは <http://192.168.111.1> です。
- 2 左部のナビゲーション・バーで、
[管理] ⇒ [システム・セキュリティ] を選択します。
[システム・セキュリティ] ページが表示されます。

システム・ステータス	管理
ネットワーク	システム・セキュリティ
外部	
トラステッド	
オプション	
ルート	
Network Statistics	
DynamicDNS	
管理	
システム・セキュリティ	
VPN Manager アクセス	
更新	
アップグレード	
設定ファイルの表示	
ファイアウォール	
受信	
送信	
カスタム・サービス	
利用できないサイト	
ファイアウォール・オプション	
パス・スルー	

HTTP サーバー・ポート

システム・セキュリティの有効化

システム管理者名

システム・パスフレーズ

システム・パスフレーズの確認

Firebox S6 リモート管理の有効化

仮想 IP アドレス

認証アルゴリズム

暗号化アルゴリズム

VPN クライアント・タイプ

- 3 [HTTP サーバー・ポート] ボックスに「80」と入力されていることを確認します。
- 4 [システム・セキュリティの有効化] チェックボックスをオンにします。
- 5 システム管理者パスフレーズを該当するフィールドに入力します。確認のため、再度入力します。
- 6 [サブミット] をクリックします。

S6 リモート管理

S6 および S6-VPN にはどちらも、S6 リモート管理機能が搭載されています。この機能により、セキュアでないネットワーク上のリモート・コンピューターからセキュアな接続を介して S6 を管理することができます。セキュアな接続は、リモート・コンピューター上の MUVPN クライアントまたは Pocket PC クライアント・ソ

フトウェア・アプリケーションを使って確立します。これらのクライアント・ソフトウェア・アプリケーションはどちらも Internet Protocol Security (IPSec) 規格を使用します。

下記は、リモート管理機能の使用例です。まず、標準インターネット接続を使って、リモート・コンピュータを S6 に接続します。次に MUVPN クライアント・ソフトウェアをアクティブにします。最後に、MUVPN クライアントが S6 への暗号化トンネルを確立します。これでリモート・コンピュータは、セキュリティを侵害することなく、S6 の設定ページにアクセスできるようになります。

次は、リモート管理機能の別の使用例です。Pocket PC を使って、S6 をインターネットに接続します。Pocket PC クライアントが S6 への暗号化トンネルを確立します。これでリモート・コンピュータは、セキュリティを侵害することなく S6 の設定ページにアクセスできるようになります。

- 1 最初に 54 ページの「システム・セキュリティ」の手順に従って下さい。
- 2 **[S6 リモート管理の有効化]** チェックボックスをオンにします。
- 3 仮想 IP アドレスを該当するフィールドに入力します。
このアドレスは、リモート管理コンピュータが S6 に接続するとき
に使用されます。
- 4 **[認証アルゴリズム]** ドロップダウン・リストから、認証アル
ゴリズムを選択します。
MD5-HMAC (128 ビット認証) または SHA1-HMCA (160 ビット認証) の
いずれかを選択します。
- 5 **[暗号化アルゴリズム]** ドロップダウン・リストから、暗号化
アルゴリズムを選択します。
DES-CBC または 3DES-CBC のいずれかを選択します。
- 6 **[VPN クライアント・タイプ]** ドロップダウン・リストから、
VPN クライアント・タイプを選択します。
Mobile User (MUVPN) または Pocket PC のいずれかを選択します。
- 7 **[サブミット]** をクリックします。

- 8 リモート・コンピューターに MUVPN クライアントを導入し、設定します。
詳しくは、第 10 章 111 ページの「MUVPN クライアント」を参照して下さい。
- 9 MUVPN クライアントの導入および設定の完了後、ダイアルアップ・ネットワーク、LAN または WAN 接続を使用し、インターネットに接続します。

Windows デスクトップのシステム・トレイで、次の手順に従って下さい。

- 10 MUVPN クライアントがアクティブになっていることを確認します。MUVPN クライアントがアクティブになっていない場合、アイコンをダブルクリックして、[**アクティブ・セキュリティ・ポリシー**] を選択します。
MUVPN アイコンのステータスを決定する方法については、142 ページの「MUVPN クライアント・アイコン」を参照して下さい。
- 11 アイコンを右クリックして、[**接続**] を選択します。
[ウォッチガード社モバイル・ユーザー接続] ウィンドウが表示されます。
- 12 [**Yes**] をクリックします。
- 13 ブラウザーのウィンドウで、S6 外部ネットワークの IP アドレスを入力して [**システム・ステータス**] ページを表示します。

VPN Manager アクセスの設定

[VPN Manager アクセス] ページでは、WatchGuard VPN Manager ソフトウェアを使って S6 をリモートで管理できるように S6 を設定することができます。WatchGuard VPN Manager ソフトウェアは VPN トンネルを設定および管理します。

VPN Manager ソフトウェアは別売りです。また、WatchGuard Firebox II/III 上で実行する必要があります。VPN Manager 製品

の詳細については、ウォッチガード社ウェブサイトをご覧ください。

<https://www.watchguard.com/products/vpnmanager.asp>

次の手順に従って、VPN Manager アクセスを設定して下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、
[管理] =>[VPN Manager アクセス] を選択します。
[VPN Manager アクセス] ページが表示されます。

システム・ステータス
ネットワーク
外部
トラステッド
オプション
ルート
Dual ISP
Network Statistics
DynamicDNS
管理
システム・セキュリティ
VPN Manager アクセス
更新
アップグレード
設定ファイルの表示
ファイアウォール

管理
VPN Manager アクセス

VPN Manager アクセスの有効化

ステータス・パズフレーズ

ステータス・パズフレーズの確認

構成パズフレーズ

構成パズフレーズの確認

Submit Reset

- 3 [VPN Manager の有効化] チェックボックスをオンにします。
- 4 ステータス・パズフレーズを該当するフィールドに入力します。確認のため、再度入力します。
- 5 設定パズフレーズを該当するフィールドに入力します。確認のため、再度入力します。

注意

これらのパスワードは、VPN Manager ソフトウェアで使われているパスワードと同一でなければなりません。同一でない場合、接続は失敗します。

6 [サブミット] をクリックします。

ファームウェアの更新

S6 ファームウェアが更新されていないかどうか、定期的にウォッチガード社ウェブサイトをチェックして下さい。

<http://support.watchguard.com/sohoresources/>

ファームウェア・アップデート版の含まれたファイルをダウンロードします。ファイルをコンピューター上に保存します。

次の手順に従って、S6 上に新しいファームウェアを転送して下さい。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは <http://192.168.111.1> です。
- 2 左部のナビゲーション・バーで、**[管理]** ⇒ **[更新]** を選択します。
[更新] ページが表示されます。

注意

Macintosh、Linux などの Windows オペレーティング・システムを使用していないコンピューターから S6 を設定している場合、ユーザーは、この設定手順に従ってファームウェアを更新する必要があります。CD-ROM に含まれているウォッチガード社インストール・プログラムは、Windows プラットフォーム版のみとなっています。

- 3 エンドユーザー使用許諾契約書を読み、ページの下部にある [上記の使用許諾条件を受諾します。] チェックボックスをオンにします。

上記の使用許諾契約条件を受諾します。

ファイルの選択

- 4 ユーザーのコンピューター上でファームウェア・ファイルが配置されているディレクトリを入力します。あるいは、[Browse] をクリックして ファームウェア・ファイルを検索し、そのディレクトリを選択します。
- 5 [更新] をクリックします。
更新ウィザードの指示に従って処理を進めます。

注意

更新ウィザードの途中で、ユーザー名とパスワードを入力するよう求められます。その際、[システム・セキュリティ] ページで指定したシステム管理者名とパスワードを入力します。デフォルト値はそれぞれ「User」と「Pass」です。

S6 アップグレード版・オプションの有効化

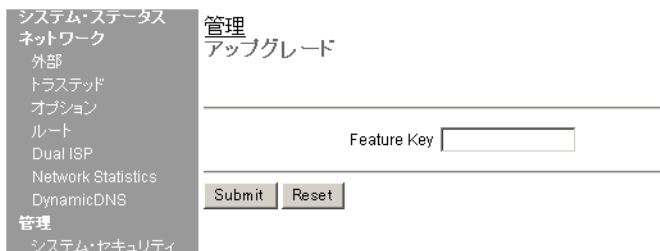
すべての S6 には、アップグレード版・オプション用ソフトウェアが付属しています。アップグレード版・オプションを有効にするには、S6 の設定ページでライセンス・キーを入力します。ライセンス・キーは、アップグレード版・オプションを購入して LiveSecurity サービスのウェブサイト登録すると発行されます。詳しくは 30 ページの「S6 および LiveSecurity サービスの登録」を参照して下さい。

次の手順に従って、アップグレード版・オプションを有効にします。

- 1 ウォッチガード社ウェブサイトのアップグレード版ページにアクセスします。

<http://www.watchguard.com/upgrade>

- 2 ユーザー名とパスワードを該当するフィールドに入力します。
- 3 [ログイン] をクリックします。
- 4 ウェブサイトに表示される指示に従って、アップグレード版ライセンス・キーを有効にします。
- 5 LiveSecurity サービスのウェブサイトに表示される Feature Key をコピーします。
- 6 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは <http://192.168.111.1> です。
- 7 左部のナビゲーション・バーで、
[管理] ⇒ [アップグレード] をクリックします。
[アップグレード] ページが表示されます。



- 8 [Feature Key] を該当ボックスに貼り付けます。
- 9 [サブミット] をクリックします。

アップグレード版オプション

シート・ライセンス

シート・ライセンス・アップグレード版は、トラステッド・ネットワークと外部ネットワーク間での接続を増やすものです。例えば、25 シート・ライセンスは、標準装備されているシート数は 10 接続に代わり、25 の接続が可能になります。

Dual ISP Port

Dual ISP Port アップグレード版は、外部インターフェースの冗長化機能を提供します。

VPNforce Port

VPNforce Port アップグレード版は、S6 のオプション・ポート (OPT) を有効にし、トラステッド側に 2 つ目のネットワークに接続することができるようにします。このオプションにより、リモート・オフィスのネットワークや在宅勤務者にファイアウォールの保護を拡張させることができます。

IPSec 仮想プライベート・ネットワーク (VPN)

VPN アップグレード版は、仮想プライベート・ネットワークを設定するために必要になります。S6-VPN には、VPN アップグレード版・ライセンス・キーが含まれています。S6 には、VPN アップグレード版ライセンス・キーは付属していません。

WebBlocker

WebBlocker アップグレード版は、ウェブ・フィルタリング・オプションを使用可能にします。

MUVPN クライアント

MUVPN クライアント・アップグレード版を有効にした場合、リモート・ユーザーはセキュアな IPSec VPN トンネルを使って S6 に接続することができます。これらのユーザーは、トラステッド・ネットワーク上のネットワーク・リソースを利用することができます。

LiveSecurity サービス加入契約の更新

LiveSecurity サブスクリプションは 1 年間または 2 年間更新でき、販売店またはウォッチガード社オンライン・ストアで購入できます。ウォッチガード社ウェブサイトの更新ページにアクセスし、サブスクリプション更新を購入または有効にしてください。

<http://www.watchguard.com/renew/>

ウェブサイトの指示に従ってください。

コンフィギュレーション・ファイルの表示

コンフィギュレーション・ファイルページでは、S6 のコンフィギュレーション・ファイルの内容をテキスト形式で表示できます。

- 1 ブラウザーのウィンドウで、トラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページを表示します。
デフォルト IP アドレスは `http://192.168.111.1` です。
- 2 左部のナビゲーション・バーで、
[管理] ⇒ [コンフィギュレーション・ファイルの表示] を選択します。
[コンフィギュレーション・ファイルの表示] ページが表示されます。

ファイアウォールの 設定

ファイアウォール設定

トラステッド・ネットワークと外部ネットワークとの間のトラフィックの流れは、S6 の設定により制御します。選択する設定は、トラステッド・ネットワークに対し許容可能なリスクのタイプに依存します。

設定ページには、S6 の標準サービスが数多く一覧表示されています。サービスとは、アプリケーションまたは通信のタイプに対応したプロトコルとポート番号の組み合わせのことです。

受信サービスと送信サービスの設定

S6 のデフォルトの設定は、外部ネットワークからトラステッド・ネットワークへのすべてのパケットの送信を遮断します。許容されるトラフィックのタイプを選択するには設定を変更します。例えば、トラステッド・ネットワーク上のウェブサーバーを操作するには、受信ウェブサービスを追加します。

追加するサービスの数とタイプに注意し選択します。サービスを追加するとネットワークのセキュリティが低下します。各サービスへアクセスする利点と、そのサービスに起因するセキュリティ・リスクとを比較します。

標準サービス

標準サービスに対応するために受信フィルターの設定を変更するには、以下の手順に従ってください。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、`http://192.168.111.1` です。
- 2 左側のナビゲーション・バーで、**[Firewall]** ⇒ **[Incoming]** または **[Outgoing]** を選択します。
[トラフィックのフィルタリング] ページが表示されます。

システム・ステータス
ネットワーク
外部
トラステッド
オプション
ルート
Dual ISP
Network Statistics
DynamicDNS

ファイアウォール
受信トラフィックのフィルタリング

警告:

共通サービス

フィルタ	サービス	サービス・ホスト
ルールなし	CU-SeeMe	0.0.0.0
ルールなし	DNS	0.0.0.0
ルールなし	FTP	0.0.0.0
ルールなし	HTTP	0.0.0.0
ルールなし	HTTPS	0.0.0.0
ルールなし	iLS	0.0.0.0
ルールなし	IPSec	0.0.0.0
ルールなし	NetMeeting	0.0.0.0
ルールなし	NNTP	0.0.0.0

管理
システム・セキュリティ
VPN Manager アクセス
更新
アップグレード
設定ファイルの表示
ファイアウォール
送信
カスタム・サービス
利用できないサイト
ファイアウォール・オプション

- FTP、Web、Telnet のような設定済みのサービスを選択し、そのドロップダウン・リストから **[Allow]** または **[Deny]** のどちらかを選択します。
上記の画面では、HTTP サービスは、受信トラフィックを許可するように設定されています。
- このルールが適用されるコンピューターのトラステッド・ネットワークの IP アドレスを、該当するフィールドに入力します。
画面では、HTTP サービスは、受信トラフィックを IP アドレス 192.168.111.2 を有するコンピューターに許可するように設定されています。
- [Submit]** をクリックします。

カスタム・サービスの作成

標準サービスの一覧にないサービスを許可する必要がある場合、TCP ポート、UDP ポート、あるいはプロトコルに基づき、カスタムサービスを設定します。

カスタム・サービスを作成するには、次の手順に従います。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーで、**[ファイアウォール] ⇒ [カスタム・サービス]** を選択します。
[カスタム・サービス] ページが表示されます。

The screenshot displays the 'Custom Services' configuration page in the WatchGuard Firebox S6 web interface. On the left, a navigation sidebar lists various system settings, with 'Custom Services' highlighted. The main content area is titled 'ファイアウォール' (Firewall) and 'カスタム・サービス' (Custom Services). It features a table for defining services with columns for 'サービス名' (Service Name), 'プロトコル' (Protocol), and 'ポート' (Port). Below the table, there are input fields for 'TCP ポート' (TCP Port), '送信先' (Destination), and '送信元' (Source), along with 'Add' and 'Remove' buttons. The '送信元' field is currently set to '0.0.0.0'. At the bottom, there are additional fields for '受信フィルタ' (Receive Filter) and '送信フィルタ' (Send Filter), both set to 'ルールなし' (No Rules).

- 3 [サービス・ネーム] のフィールドに、サービスの名前を入力します。
- 4 [プロトコル・セッティング] の下にあるドロップダウン・リストから [TCP ポート]、[UDP ポート]、または [プロトコル] を選択します。
[カスタム・サービス] ページが更新されます。
- 5 [To] で区切られたフィールドにポート番号またはポート番号の範囲を入力するか、もしくは、プロトコル番号を入力します。

注意

TCP ポートあるいは UDP ポートには、ポート番号を指定します。プロトコルには、プロトコル番号を指定します。プロトコルには、ポート番号を指定できません。

- 6 [Add] をクリックします。
以下の手順は、サービスをフィルターする方法を決定するものです。
- 7 [Incoming Filter] および [Outgoing Filter] ドロップダウン・リストから、[Allow] または [Deny] のどちらかを選択します。
- 8 ページ下部のドロップダウン・リストから [Host IP Address]、[Network IP Address]、[Host Range] のいずれかを選択します。
[カスタム・サービス] ページが更新されます。
- 9 単一のホスト IP アドレス、ネットワーク IP アドレス、またはホスト IP アドレスの範囲（開始アドレスと終了アドレス）のいずれかを該当フィールドに入力します。
- 10 [Add] をクリックします。
このカスタム・サービスのすべてのアドレス情報が設定されるまで、上記の3つの手順を繰り返します。
- 11 [Submit] をクリックします。

外部サイトの遮断

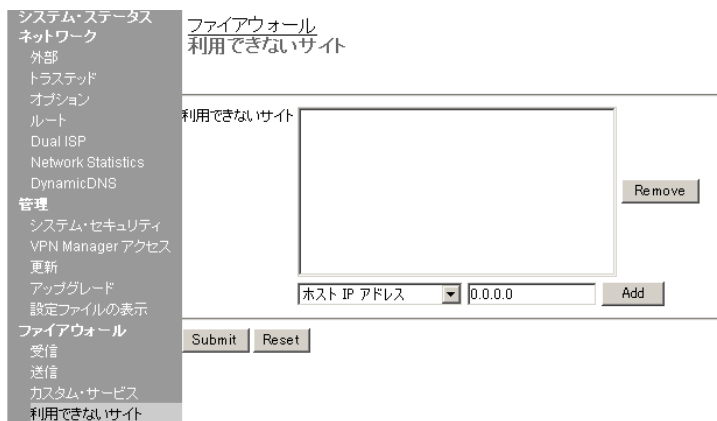
S6 のデフォルトの設定は以下の通りです：

- ・ トラストッド・ネットワークから外部ネットワークへのパケットの送信をすべて許可する
- ・ 外部ネットワークからトラस्टッド・ネットワークへのパケットの送信をすべて防止する。

特定のインターネット・サイトへのアクセスを防ぐように設定を変更することができます。以下の手順に従って遮断されたサイトの設定を行います。

- 1 左側のナビゲーション・バーで、**[ファイアウォール]** ⇒ **[遮断されたサイト]** をクリックします。

[遮断されたサイト] ページが表示されます。



- 2 ドロップダウン・リストから **[ホスト IP アドレス]**、**[ネットワーク IP アドレス]**、**[ホスト IP アドレスの範囲]** のいずれかを選択します。
[遮断されたサイト] ページが更新されます。

- 3 単一のホスト IP アドレス、ネットワーク IP アドレス、またはホスト IP アドレスの範囲（開始アドレスおよび終了アドレス）のいずれかを該当フィールドに入力します。
画面では、[ホスト IP アドレス] を選択し、IP アドレスが 207.68.172.246 となっています。
- 4 [Add] をクリックします。
[遮断されたサイト] フィールドにアドレス情報が表示されます。
- 5 [Submit] をクリックします。

ファイアウォール・オプション

上記セクションでは、サービスのクラスを全体的に許可あるいは拒否する方法について説明しました。[ファイアウォール・オプション] ページでは、一般的なセキュリティ・ポリシーを設定できます。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーで、
[ファイアウォール] ⇒ [ファイアウォール・オプション] を選択します。
[ファイアウォール・オプション] ページが開きます。

ファイアウォール ファイアウォール・オプション

- 外部ネットワークより受けた Ping 要求に応答しない
- トラステッド・ネットワーク・インターフェイスに対する FTP アクセスを許可しない
- SOCKS プロキシを無効にする
- 許可されたすべての送信アクセスのログ
- 外部ネットワークのオーバーライド MAC アドレスを有効にする

外部ネットワークのオーバーライド MAC アドレス

サブミット

リセット

外部ネットワークからの ping 要求への応答

外部インターフェイスで受信するすべての ping パケットを拒否するように S6 を設定できます。

- 1 [Do not respond to PING requests received on External Network] チェックボックスをオンにします。
- 2 [Submit] をクリックします。

トラステッド・ネットワーク・インターフェイスに対する FTP アクセスの拒否

外部ネットワーク上のコンピューターによるトラステッド・ネットワーク上のコンピューターへの FTP アクセスを遮断するように S6 を設定できます。

- 1 [Do not allow FTP access to Trusted Network] チェックボックスをオンにします。
- 2 [Submit] をクリックします。

Firebox S6 の SOCKS のインプリメンテーション

S6 は SOCKS ネットワーク・プロキシ・サーバーとして機能します。二つ以上のソケット接続を使用し、SOCKS Version 5 プロトコルを実行するアプリケーションは、S6 を通して通信ができます。SOCKS により、外部ネットワーク上のコンピューターとトラステッド・ネットワーク上のコンピューターとのセキュアな相互通信チャンネルが使用可能となります。SOCKS 対応型アプリケーションを使用するには、そのアプリケーションの S6 に関する必要な情報を設定します。

S6 は、SOCKS Version 5 のみサポートしています。S6 は認証あるいは DNS (Domain Name System) 変換をサポートしていません。

注意

SOCKS 対応型アプリケーションを、ドメイン名ではなく IP アドレスと接続するように設定します。ドメイン名の参照しか行えないアプリケーションは、S6 に適合しません。

S6 経由で使用したとき正確に機能する SOCKS 対応型アプリケーションには、ICQ、IRC、AOL Messenger 等があります。

注意

トラステッド・ネットワーク中のコンピューターで SOCKS 対応型アプリケーションを使用すると、トラステッド・ネットワーク上の他のユーザーはそのコンピューターに自由にアクセス可能になります。このセキュリティ上のリスクを防止するには、S6 上では SOCKS を無効にします。詳細は、74 ページの「S6 の SOCKS の無効化」を参照してください。

SOCKS アプリケーションの設定

トラステッド・ネットワーク内のコンピューターの SOCKS 対応型アプリケーションに、外部ネットワーク上のコンピューターと通信させるには、下記に従ってアプリケーションを設定します。

注意

SOCKS 対応型アプリケーションが使用されているコンピューターとの通信に使用する S6 のポートはポート 1080 です。ポート 1080 が他のアプリケーションによって使用されていないことを確認してください。

- SOCKS のプロトコルあるいはバージョンが選択可能な場合は、SOCKS Version 5 を選択します。
- ポート 1080 を選択します。
- URL に対する SOCKS のプロキシあるいは S6 の IP アドレスを設定します。デフォルトの IP アドレスは、`http://192.168.111.1` です。

S6 の SOCKS の無効化

S6 経由で SOCKS 対応アプリケーションを接続させた後、SOCKS ポートは開いたままになります。アプリケーションを終了すると、SOCKS ポートはトラステッド・ネットワーク上の誰もが使用可能となります。このセキュリティ上の問題を防ぐには、以下の手順に従います。

SOCKS 対応アプリケーションが使用されていないとき：

- 1 **[Disable SOCKS proxy]** チェックボックスをオンにします。
これによって S6 は SOCKS プロキシとして機能しなくなります。
- 2 **[Submit]** をクリックします。

SOCKS 対応アプリケーションを使用するには：

- 1 **[Disable SOCKS proxy]** チェックボックスをオフにします。
これによって、S6 は SOCKS プロキシサーバーとして機能するようになります。
- 2 **[Submit]** をクリックします。
これによって、S6 は SOCKS プロキシサーバーとして機能しなくなります。

許可されたすべての送信トラフィックのログ出力

デフォルト設定では、S6 は例外的なイベントを記録するだけになっています。例えば、拒否されたトラフィックはすべてログ・ファイルに記録されます。この S6 の設定を変更して、すべての送信トラフィック・イベントを記録させることができます。

注意

このオプションでは、膨大な数のログ入力記録されます。ウォッチガード社は、このオプションを問題解決の目的にのみ使用するよう推奨しています。

このオプションを使用するには、次の手順に従います。

- 1 **[Log All Allowed Outbound Access]** チェックボックスをオンにします。
- 2 **[Submit]** をクリックします。

外部ネットワークの MAC アドレスのオーバーライドを有効にする

ISP に MAC アドレスが必要な場合、このオプションを使用可にします。S6 はトラステッド・ネットワークに独自の MAC アドレスを使用します。外部ネットワーク上で使用するために新しい MAC アドレスを入力できます。

このオプションを使用するには、次の手順に従います。

- 1 **[Enable override MAC address for the External Network]** チェックボックスをオンにします。
- 2 S6 外部ネットワークへの新しい MAC アドレスを該当するフィールドに入力します。
- 3 **[Submit]** をクリックします。

注意

[**MAC address for the external network**] フィールドを空欄にして S6 を再起動すると、外部ネットワークの MAC アドレスは、デフォルト出荷時のデフォルト設定に戻ります。

MAC アドレスの衝突を避けるため、S6 は外部ネットワークを定期的に検索してオーバーライド MAC アドレスをチェックします。同じ MAC アドレスを使用しているデバイスが見つかったら、S6 の外部 MAC アドレスはデフォルト出荷時のデフォルト値にリセットされ、リブートします。

無制限パス・スルーの作成

S6 では、外部ネットワークから公認 IP アドレスを有するトラステッド・ネットワーク上のコンピューターへのトラフィックを流し出すことができます。

パス・スルーを設定するには、次の手順に従います。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、<http://192.168.111.1> です。
- 2 左側のナビゲーション・バーで、**[ファイアウォール]** ⇒ **[パス・スルー]** をクリックします。
[無制限パス・スルー IP アドレス] ページが表示されます。

システム・ステータス	ファイアウォール
ネットワーク	無制限パス・スルー IP アドレス
外部	
トラステッド	
オプション	
ルート	
ネットワーク統計	<input type="checkbox"/> パス・スルー・アドレスの有効化
ダイナミックDNS	パス・スルーするアドレス <input type="text"/>
管理	
システム・セキュリティ	<input type="button" value="サブミット"/> <input type="button" value="リセット"/>
VPN Manager アクセス	

- 3 [Enable pass through address] チェックボックスをオンにします。
- 4 該当するフィールドにコンピューターの IP アドレスを入力し、パス・スルーへ接続します。
これは公認 IP アドレスでなければなりません。
- 5 [Submit] をクリックします。

注意

パス・スルー接続を行うと、トラステッド・ネットワークのセキュリティが低下します。これは、パス・スルー接続を行っているコンピューターは、トラステッド・ネットワークと同じイーサネット・セグメントに存在するからです。パス・スルー接続がトラステッド・ネットワークのセキュリティに与える影響が分かっていない限りは、このパス・スルー接続機能を使用しないでください。

ロギングの設定

S6 のロギング機能は、トラステッド・ネットワークのセキュリティに関連したイベントを記録します。記録されたイベントの例として、WatchGuard WebBlocker データベースとの通信および流入トラフィックがあります。ログは、起こり得るセキュリティ問題を表すイベントを記録します。ロギングされるイベントの最も重要な種類は、パケットの拒否です。一連のパケットの拒否により、不正アクセスが試みられていることを知ることができます。

注意

電源が切られると、S6 のログの記録が消去されてしまいます。

S6 Wireless のログ・メッセージの表示

S6 のイベント・ログの最大ログ記録数は 150 件です。イベント・ログが最大記録数に達したときに新たに入力が行われると、最も古いログメッセージが消去されます。

ログ・メッセージには、S6 と WatchGuard Time Server の時刻の同期、パケット処理違反のため破棄されたパケット、重複メッセージ、リターン・エラー・メッセージ、IPSec メッセージなどがあります。

以下の設定手順は、イベント・ログの表示方法を示したものです。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーで [ロギング] をクリックします。
[ロギング] ページが表示されます。このページの下部にイベント・ログが表示されます。

The screenshot shows the 'ロギング' (Logging) configuration page. The left sidebar has 'ロギング' selected. The main content area is divided into three sections:

- ロギング・オプション** (Logging Options):
 - WSEP に対するロギング: Disabled, WSEP ログ・ホスト 0.0.0.0, 設定
 - Syslog ロギング: Disabled, Syslog ホスト 0.0.0.0, 設定
- システム時間** (System Time):
 - タイム・ゾーン: DST Disabled
 - タイム・ソース: WatchGuard Time Server
 - 現在の時刻: 2003-01-30-09:06:14
 - Sync Time With Browser Now
- イベント・ログ** (Event Log):

時間	カテゴリ	メッセージ
2003-01-30-09:06:14	IP	allowed from 202.224.237.6 port 62497 to 68.5.30.207 port 8000 TCP SYN (allhttp)
2003-01-30-09:06:14	MONITOR	Administrator access allowed from 202.224.237.6

注意

最新のエントリーは、イベント・ログの先頭に表示されます。

このオプションを用いることにより、S6 の時刻をコンピューターと同期させることができます。

- **[Sync Time with Browser now]** をクリックします。

時刻の同期は S6 の起動時に実行されます。

WatchGuard Security Event Processor ログホストへのロギングの設定

WSEP (WatchGuard Security Event Processor) は、Firebox II/III の *WatchGuard Firebox System* パッケージに付属しているアプリケーションです。WSEP アプリケーションはログ・ホストとして機能するコンピューター上で動作します。WSEP アプリケーションは Firebox II/III により送信されたログ・メッセージを記録します。Firebox II/III をお持ちの場合は、S6 からのログ・メッセージを受け取るように WSEP を設定します。その後以下の指示に従い、イベント・ログを WSEP に送信します。

- 1 トラストド・ネットワークの IP アドレスをブラウザーのウィンドウに入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、<http://192.168.111.1> です。
- 2 左側のナビゲーション・バーで、
[ロギング] ⇒ [WSEP に対するロギング] をクリックします。
[WatchGuard Security Event Processor] ページが表示されます。

システム・ステータス ネットワーク 外部 トラステッド オプション ルート Dual ISP Network Statistics DynamicDNS 管理 システム・セキュリティ VPN Manager アクセス 更新 アップグレード	ロギング WatchGuard Security Event Processor のロギング
	<input type="checkbox"/> WatchGuard Security Event Processor ロギングの有効化
	ホスト IP アドレスのログ <input type="text" value="0.0.0.0"/>
	暗号化キーのログ <input type="text"/>
	キーの確認 <input type="text"/>
	<input type="button" value="Submit"/> <input type="button" value="Reset"/>

- 3 [WatchGuard Security Event Processor ロギングの有効化] チェックボックスをオンにします。
- 4 ログ・ホストである WSEP サーバーの IP アドレスを該当ボックスに入力します。
- 5 パスフレーズを [暗号化キーのログ] ボックスに入力し、確認のため同じ内容を [キーの確認] ボックスに入力します。
- 6 [Submit] をクリックします。

注意

WSEP アプリケーションに記録されているものと同じ暗号化キーを使用してください。

シスログ (Syslog) ホストへのロギングの設定

このオプションにより、S6 のログ・エントリーはシスログ (Syslog) ホストに送信されます。

シスログ (Syslog) ホストを設定するには、次の手順に従います。

- 1 トラストッド・ネットワークの IP アドレスをブラウザのウィンドウに入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、`http://192.168.111.1` です。
- 2 左側のナビゲーション・バーで、
[ロギング] ⇒ [Syslog ロギング] をクリックします。
[Syslog ロギング] ページが表示されます。

ロギング
Syslog ロギング

syslog 出力の有効化

syslog ホストのアドレス

syslog メッセージにローカル時間を表示する

サブミット リセット

- 3 [Syslog 出力の有効化] チェックボックスをオンにします。
- 4 シスログ (Syslog) サーバーの IP アドレスを該当ボックスに入力します。
- 5 [Submit] をクリックします。

このオプションによって、ブラウザからシスログ・メッセージにローカル時刻を表示させることができます。

- [Syslog メッセージにローカル時間を表示する] チェックボックスをオンにします。

注意

シスログのトラフィックは暗号化されません。インターネットを通してシスログ・メッセージを送信することにより、トラステッド・ネットワークのセキュリティが低下します。シスログ・メッセージのトラフィックのセキュリティを強化するには、VPN(仮想プライベート・ネットワーク)トンネルを使用します。シスログ・メッセージがVPNトンネルを通して送信された場合には、データはIPSec 技術によって暗号化されます。

システム時間の設定

S6 により、各ログ・エントリの時刻が記録されます。

時間	カテゴリ	メッセージ
2003-01-31-19:25:15	IP	allowed from 202.224.237.6 port 62998 to 68.5.30.207 port 8000 TCP SYN (althttp)
2003-01-31-19:25:15	MONITOR	Administrator access allowed from 202.224.237.6
2003-01-31-19:25:14	IP	allowed from 202.224.237.6 port 62997 to 68.5.30.207 port 8000 TCP SYN (althttp)

ログ・エントリに記録される時刻は、S6 のシステム時間によるものです。

システム時間を設定するには、次の手順に従います。

- 1 トラステッド・ネットワークの IP アドレスをブラウザのウィンドウに入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーで、
[ログイン] ⇒ [システム時間] をクリックします。
[システム時間] ページが表示されます。

システム・ステータス	ロギング
ネットワーク	システム時間
外部	
トラステッド	
オプション	
ルート	
Dual ISP	
Network Statistics	
DynamicDNS	
管理	タイム・ソース
システム・セキュリティ	<input type="radio"/> TCP Port 37 タイム・サーバーの時間を採用 <input type="text"/>
VPN Manager アクセス	<input checked="" type="radio"/> WatchGuard タイム・サーバーの時間を採用
更新	タイム・ゾーン
アップグレード	タイム・ゾーン調節は、WatchGuard タイム・サーバーの使用時にのみ可能です。
設定ファイルの表示	<input type="text" value="(グリニッジ標準時-12:00) エニエトク、クアジャリン"/>
ファイアウォール	<input type="checkbox"/> サマータイムの調整
受信	<input type="button" value="Submit"/> <input type="button" value="Reset"/>

- ドロップダウン・リスト・ボックスの一覧で時間帯を選択します。
- [サマータイムの調整] チェックボックスをオンにします。
- [Submit] をクリックします。

WebBlocker は S6 のオプションで、システム管理者はユーザーがアクセスできるウェブサイト进行管理することができます。

WebBlocker の動作

WebBlocker では、SurfControl で所有・管理されるウェブサイト・アドレスのデータベースを利用します。データベースには、何千件ものウェブサイトの内容のタイプが示されています。ウォッチガード社は、SurfControl データベースの最新バージョンを WebBlocker サーバーに定期的に配置しています。

WebBlocker はトラステッド・ネットワークのユーザーによるウェブサイトへの要求を逐一チェックします。S6 はデータベースに要求を送信してウェブサイト上の内容のタイプを照会します。S6 は以下に示す規則を利用してウェブサイトへのアクセスを管理します。

ウェブ 사이트가 WebBlocker に登録されていない場合

アクセスしようとする 사이트가 WebBlocker データベースに注册されていない場合、Web ブラウザーにそのページが開いて表示されます。

ウェブ 사이트가 WebBlocker に登録されている場合

サイトが WatchGuard WebBlocker データベースに注册されている場合、S6 は設定を調べてそのタイプの 사이트가許可されているかどうか判断します。その 사이트のタイプが許可されていない場合は、ユーザーにはその 사이트が利用不可能であることが知られます。 사이트のタイプが許可されている場合は、ウェブ・ブラウザーはそのページを開きます。

WatchGuard WebBlocker データベースが利用できない場合

WatchGuard WebBlocker データベースが利用できない場合、ユーザーにはそのウェブ・ 사이트が利用できないことが知られます。S6 が WatchGuard サーバーに接続できない場合はデータベースは利用できません。

WebBlocker のユーザーとグループ

- **グループ**

グループとは、システムを利用する個人、すなわちユーザーの集合です。

- **ユーザー**

ユーザーとは特定のグループに属する個々のメンバーです。

S6 WebBlocker の回避

S6 WebBlocker の設定ページには、フルアクセス用パスワードのフィールドがあります。WebBlocker の回避が許可されたトラステッド・ネットワーク上のユーザーに、このパスワードを教えてください。 사이트가ブロックされている場合は、このフルアクセ

ス用パスワードを入力してウェブサイトにはアクセスすることができません。パスワードを入力すると、パスワードの有効期限が切れるかブラウザを終了するまで、インターネット上のあらゆるサイトにアクセスできません。

S6WebBlocker の購入と有効化

WatchGuard S6 WebBlocker を使用するには、まず WebBlocker アップグレードのライセンス・キーを購入して有効化する必要があります。アップグレードのライセンス・キーの購入方法については、61 ページの「S6 アップグレード版・オプションの有効化」を参照してください。

S6WebBlocker の設定

WebBlocker を設定するには、S6 の設定ページを使用します。

WebBlocker の設定

WebBlocker の設定ページを使用する

- WebBlocker の有効化
 - フルアクセス用パスワードを設定する
 - 無効化タイムアウトを設定する
 - ウェブ・ユーザーは認証を必須とする
- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、`http://192.168.111.1` です。

- 2 左側のナビゲーション・バーから、
[WebBlocker] ⇒ [Settings] をクリックします。
[WebBlocker の設定] ページが表示されます。

WebBlocker
設定

WebBlocker の有効化

フル・アクセス・パスワード

パスワードの確認

無操作タイムアウト (単位分)

Web ユーザーに認証を要求

サブミット

- 3 [WebBlocker の有効化] チェック・ボックスをオンにします。
- 4 [フルアクセス用パスワード] のフィールドに、パスフレーズを入力します。
フルアクセス用パスワードによって、ユーザーはパスワードの有効期限が切れるかブラウザーを終了するまですべてのウェブサイト
にアクセスできるようになります。
- 5 [無効化タイムアウト] のフィールドに、分単位の値を入力
します。
無効化タイムアウトによって、無効な状態が設定した時間続くと、
インターネットへの接続が切断されます。
- 6 グループとユーザーを使用するように WebBlocker を設定する
には、[Web ユーザーに認証を要求] チェックボックスをオン
にします。
- 7 [Submit] をクリックします。

WebBlocker ユーザーとグループの作成

WebBlocker のグループを作成するには、次の手順に従います。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページに接続します。

デフォルトの IP アドレスは、<http://192.168.111.1> です。

- 2 左側のナビゲーション・バーで、**[WebBlocker]** ⇒ **[グループ]** をクリックします。
[WebBlocker グループ] ページが表示されます。

WebBlocker
グループ

グループ [デフォルト・グループ](#) **新規**

ユーザー [すべてのユーザー](#)

利用できないカテゴリー

<input type="checkbox"/> お酒とタバコ	<input type="checkbox"/> 暴力/冒涇
<input type="checkbox"/> 違法ギャンブル	<input type="checkbox"/> 検索エンジン
<input type="checkbox"/> 活動家/過激派	<input type="checkbox"/> スポーツとレジャー
<input type="checkbox"/> ドラッグ文化	<input type="checkbox"/> 性教育
<input type="checkbox"/> 悪魔/カルト	<input type="checkbox"/> 性行為
<input type="checkbox"/> 不耐性	<input type="checkbox"/> ノード
<input type="checkbox"/> 卑劣な描写	<input type="checkbox"/> 部分/芸術的 ノード

サブミット **リセット**

- 3 **[新規]** をクリックして、グループ名とプロフィールを作成します。

WebBlocker > グループ
新規グループ

グループ名

利用できないカテゴリ

- | | |
|----------------------------------|------------------------------------|
| <input type="checkbox"/> お酒とタバコ | <input type="checkbox"/> 暴力/冒険 |
| <input type="checkbox"/> 違法ギャンブル | <input type="checkbox"/> 検索エンジン |
| <input type="checkbox"/> 活動家/過激派 | <input type="checkbox"/> スポーツとレジャー |
| <input type="checkbox"/> ドラッグ文化 | <input type="checkbox"/> 性教育 |
| <input type="checkbox"/> 悪魔/カルト | <input type="checkbox"/> 性行為 |
| <input type="checkbox"/> 不潔性 | <input type="checkbox"/> ノード |
| <input type="checkbox"/> 卑劣な描写 | <input type="checkbox"/> 部分芸術的ノード |

サブミット

リセット

キャンセル

- 4 [グループ名] を定義して、このグループに対するフィルターをかけたいコンテンツのタイプを選択します。
- 5 [Submit] をクリックします。
設定の変更を示す新規の [グループ] ページが表示されます。

WebBlocker
グループ

設定内容が変更されました。

グループ
test1

削除 新規

ユーザ
-

削除 新規

- 6 **【ユーザー】** フィールドの右側にある **【新規】** をクリックします。
【新規ユーザー】 ページが表示されます。

WebBlocker > グループ
新規ユーザー

ユーザー名	<input type="text"/>
パスワード	<input type="password"/>
パスワードの確認	<input type="password"/>
グループ	test1 ▾

サブミット	リセット	キャンセル
-------	------	-------

- 7 該当するフィールドに新しいユーザー名とパスワードを入力し、確認のためにもう一度パスワードを入力します。
- 8 **【グループ】** ドロップダウン・リストを用いて、与えられたグループに新規ユーザーを割り当てます。
- 9 **【Submit】** をクリックします。

注意

ユーザーあるいはグループを削除するには、選択してから **【Delete】** をクリックします。

WebBlocker が使用するサイト・カテゴリー

WebBlocker データベースには以下の 14 のカテゴリーがあります：

注意

ウェブサイトがカテゴリーに加えられるのは、その内容がカテゴリーの題目を支持する場合だけです。そのカテゴリーの題目についての意見や教育的内容を提供するウェブサイトは含まれません。例えば、麻薬 / 麻薬文化のカテゴリに関しては、マリファナの栽培方法や使用方法を記載したサイトはブロックされますが、マリファナの使用の歴史について記載したサイトはブロックされません。

お酒 / たばこ

アルコール飲料やたばこの販売、購入、生産を支持するような画像やテキスト。

違法ギャンブル

すべてまたは一部の法律に照らして違法となる可能性のある物や行為、たとえば違法な事業形態、チェーンレーター（幸運の手紙）、著作権侵害、コンピューターによるハッキング、フリーキング（他人の電話回線を許可なしに使用する行為）、ソフトウェアの不正コピーなどを支持するような画像やテキスト。さらに、宝くじ、カジノ、賭博、ナンバーズ賭博、オンライン賭博、金融賭博（金銭を伴わない賭け事も含む）などのギャンブル行為を支持するようなテキスト。

活動家 / 過激派

極端に攻撃的または戦闘的な行為、あるいは違法な政治的手段を支持するような画像やテキスト。目的を達成するための手段として暴力を支持するグループに関するトピックなど。また、武器、弾薬、火工品を製造するノウハウを提供するページ（合法か違法かは問わない）も含む。

ドラッグ文化

娯楽のための違法ドラッグの使用を支持するような画像やテキスト。このカテゴリーには、たとえばシンナー遊びなど、本来の目的から外れて個人の精神状態に変化をもたら

す物質もしくは物質を使用した行為が含まれる。現在は違法だが医療目的で合法的に処方されている薬（緑内障薬や抗がん剤など）を紹介するサイトは対象外となる。つまり、このようなサイトは WebBlocker でブロックされないためアクセスが可能となる。

悪魔 / カルト

悪魔崇拝、悪魔に対する共感、邪悪性などを擁護したり、カルトへの入信を薦めるような画像やテキスト。カルトの定義は次のとおり。1 人の教祖によって率いられ、教祖への忠誠を強制し、離脱する者を罰する閉鎖的な集団。

不耐性

人種、肌の色、国籍、宗教、身体上 / 精神上的の障害、性別、性的嗜好などによる偏見や差別を支持するような画像やテキスト。特定の人種や団体を特に擁護する画像やテキスト。また、そうした不寛容なジョークや中傷。

卑劣な描写

ひどく低俗で、礼儀や行為が著しく品性を欠いている、またスカトロジ的な嗜好を示す人や物を描写する画像やテキスト。手足の切断、血まみれの人などの描写、排泄行為のみだらな描写などのトピックを含む。

暴力 / 冒瀆

極端に残酷または不敬な画像やテキスト。残酷の定義は次のとおり。動物や人に対して危害や苦痛を加えることを意図した身体的または感情的な行為。音声、テキスト、画像などに含まれる、わいせつな言葉やフレーズ、冒瀆する表現などを含む。

検索エンジン

AltaVista、InfoSeek、Yahoo!、WebCrawler などの検索エンジン・サイト。

スポーツとレジャー

スポーツ・イベント、スポーツ選手、その他の娯楽を描写した画像やテキスト。

性教育

避妊器具の正しい使用を提唱する画像やテキスト。コンドーム、経口ピル、子宮内避妊器具などを説明および描写したサイトを含む。性感染症、妊娠、性的境界についてパートナーと話し合うためのサイトも含む。性行為に使用する道具を販売する商用サイトはこのカテゴリーに分類されず、「性行為」のカテゴリーに分類される。

性行為

明らかな性行為、わいせつで挑発的な行為にかかわる人や物を描写した画像やテキスト。自慰行為、性交、小児（性）愛なども含まれる。また、異性愛、両性愛、同性愛グループにおけるヌードや部分ヌードの人物による性行為など。テレフォン・セックスの広告、デート斡旋サービス、個人アダルト・サイト、ポルノ関係の CD/ ビデオの販売サイトなども含む。

ヌード

生殖器の全部または一部を見せた画像。健全な部分ヌードなど、部分 / 芸術的ヌードに分類されるサイトはこのカテゴリーに含まれない。たとえば、National Geographic や Smithsonian といった雑誌のサイト、グッゲンハイム美術館（New York 市の現代美術館）、ルーブル美術館、近代美術館などのサイトは対象外となる。

部分 / 芸術的ヌード

女性の胸、男性または女性の尻部を見せた画像。生殖器を見せた画像は「ヌード」のカテゴリーに入るののでここでは対象外。水着（ハイレグなどのビキニを含む）をつけている場合は対象外。

VPN-Virtual Private Networking (仮想プラ イベート・ネットワー ク)

この章では、S6 用ブランチ・オフィス VPN アップグレード・オプションの使用方法について説明します。

Virtual Private Network を構築する理由

離れた二つの場所のコンピューター間で低費用でセキュアな接続を行うには、VPN トンネルを使用します。VPN 接続には、高価な専用ポイント・ツー・ポイント接続が必要ありません。VPN トンネルを用いれば、公衆インターネットを用いるために仮想プライベート接続に必要なセキュリティが得られます。

VPN の構築に必要なもの

- VPN アップグレード・オプションがインストールされた S6 と IPSec 準拠アプライアンス。

注意

Firebox S6、FireboxII/III、Firebox Vclass を含む IPSec 準拠アプライアンス。

- 二つの IPSec 準拠アプライアンスのそれぞれに対するインターネット接続に関する ISP からのデータ。
 - 静的 IP アドレス
 - プライマリ DNS(ドメイン・ネーム・サービス)の IP アドレス(オプション)
 - セカンダリー DNS アドレス(オプション)
 - ドメイン名(オプション)
- 二つのトラステッド・ネットワークのためのネットワーク・アドレスおよびサブネット・マスク。

注意

VPN トンネルの両端にあるトラステッド・ネットワークには、それぞれ別のネットワーク・アドレスがなければなりません。

VPN トンネルを経由して接続したアプライアンスが正確に設定されていない場合、VPN トンネルは機能しません。ウォッチガード社は、以下の形式で設定情報を記録することを推奨します。

IP アドレス表の例

項目	説明	割り当て を行う人
外部 IP アドレス	インターネットへの IPSec 準拠アプライアンスを認識する IP アドレス サイト A: 207.168.55.2 サイト B: 68.130.44.15	ISP
外部サブネット・マスク	IP アドレスのどの部分がローカル・ネットワークを認識するのかわかるビットマスク。例えば、Class C のアドレスには 256 のアドレスが含まれ、ネットマスク 255.255.255.0 となります。 サイト A: 255.255.255.0 サイト B: 255.255.255.0	ISP
ローカル・ネットワーク・アドレス	ローカル・ネットワークを認識するのに使用されるアドレス。外部 IP アドレスとしてローカル・ネットワーク・アドレスを用いることはできません。ウォッチガード社は、予約された範囲のうちの一つからアドレスを用いることを推奨します。 10.0.0.0/8 172.16.0.0/12 ・ 55.240.0.0 192.168.0.0/16 ・ 55.255.0.0 サイト A: 192.168.111.0/24 サイト B: 192.168.222.0/24	ユーザー

共有シークレット	<p>共有シークレットは、VPN トンネルを経由して送られるデータの暗号化と復号化のために、二つの IPSec 準拠アプライアンスによって使用されるパスフレーズです。二つのアプライアンスが同じパスフレーズを持っていない場合は、データの暗号化および復号化が正確に行われません。</p> <p>セキュリティを向上させるには、数字、シンボル、小文字、大文字を含むパスフレーズを使用してください。例えば、「guacamole」より「Gu4c4mo!3」としたほうが良いでしょう。</p> <p>サイト A: OurLittleSecret サイト B: OurLittleSecret</p>	ユーザー
暗号化方式	<p>暗号化方式は、通信パケットを暗号化および復号化するために使用するキーのビット数を決定します。DES では 56 ビットのキーを使用します。3DES では 168 ビットのキーを使用するので、セキュリティは向上しますが、その分動作が遅くなります。3DES または DES のどちらかを選択してください。トンネルの両端では必ず同じ暗号化方式を使用してください。</p> <p>サイト A: 3DES サイト B: 3DES</p>	ユーザー
認証	<p>二つの IPSec 準拠アプライアンスには、同じ認証方法を用いなければなりません。</p> <p>サイト A: MD5(または SHA1) サイト B: MD5(または SHA1)</p>	ユーザー

VPN アップグレード版の有効化

アップグレード・オプションを有効化するには、S6 の設定についてライセンス・キーを入力する必要があります。ライセンス・

キーを得るには、LiveSecurity Service ウェブサイトでアップグレード・オプションを購入し、有効化してください。

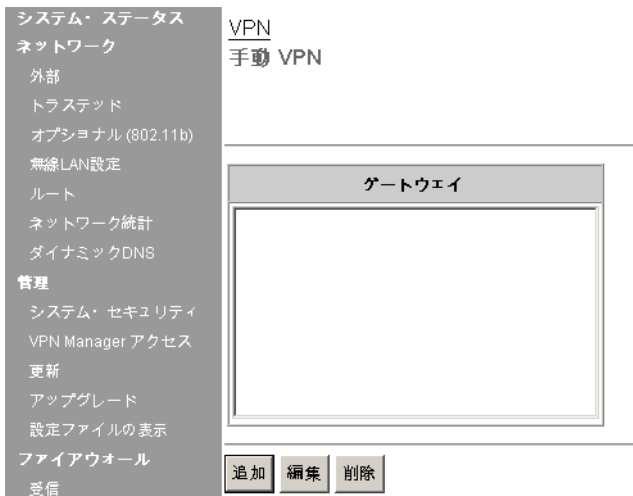
VPN アップグレード版を有効化するために必要なものは次のとおりです：

- ・ インストールおよび設定済みの S6
- ・ インターネット接続
- ・ VPN アップグレードのライセンス・キー

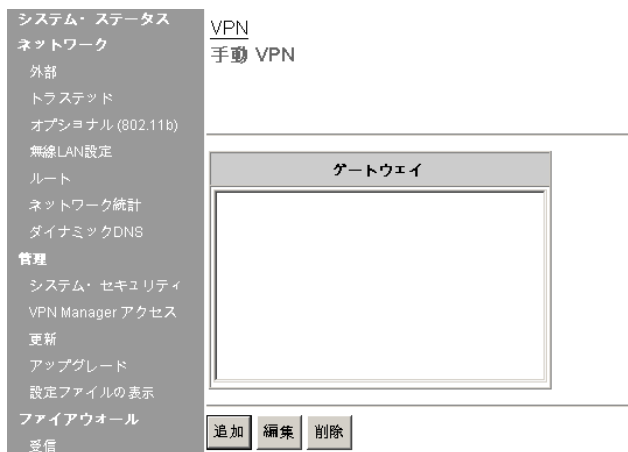
複数の S6 間の VPN トンネルの設定

S6 の管理者は別の S6 デバイスに対して、最大 6 つの VPN トンネルを設定することができます。VPN Manager ソフトウェアを用いれば、それ以上の S6 間のトンネルを設定することができます。他の S6 アプライアンスに対し複数の VPN トンネルを定義するには、次の手順に従います。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、<http://192.168.111.1> です。
- 2 左側のナビゲーション・バーから、
[VPN] ⇒ [手動 VPN] を選択します。
[手動 VPN] ページが開きます。



- 3 [Add] をクリックします。
[ゲートウェイの追加] ページが表示されます。



- 4 VPN トンネルへの [名前] と [共有シークレット] を入力します。

共有シークレットは、VPN トンネルを経由して送られるデータの暗号化と復号化のために、二つの IPSec 準拠アプライアンスによって使用されるパスフレーズです。アプライアンスが同じパスフレーズを持っていない場合は、データの暗号化および復号化が正確に行われません。

- 5 デフォルトの [フェーズ 1] の設定を利用するか、必要に応じて設定を変更します。

フェーズ 1 の設定を変更するには、以下の手順を完了します。

注意

フェーズ 1 の設定は、両方のアプライアンスで同じでなければなりません。

- 6 ドロップダウン・リストから、[フェーズ 1] に対するネゴシエーションの [モード] を選択します。選択できるモードには、[Main] と [アグレッシブ] があります。外部 IP アドレスが動的 IP アドレスである場合は、[アグレッシブ・モード] を選択します。静的 IP アドレスである場合は、どちらのモードも使用できます。
- 7 ドロップダウン・リストから、[ローカル ID] タイプおよび [リモート ID] タイプを選択します。これらの ID タイプは、リモート・ゲートウェイでの設定と一致していなければなりません。
- [メイン・モード] を使用する場合は、[ローカル ID] および [リモート ID] のタイプは IP アドレスを含む必要があります。
 - [アグレッシブ・モード] を使用する場合は、[リモート ID] のタイプとして IP アドレスあるいはドメイン名のどちらかを指定してもかまいません。外部 IP アドレスが固定の場合は、[ローカル ID] のタイプとして IP アドレスを指定する必要があります。そうでない場合は、[ローカル

ID] のタイプとしてドメイン名と IP アドレスのどちらを指定してもかまいません。

- 8 [認証アルゴリズム] ドロップダウン・リストから、認証方法を指定します。
オプションとして、MD5-HMAC(128- 認証) と SHA1-HMAC(160-bit 認証) があります。
 - 9 [暗号化アルゴリズム] ドロップダウン・リストから、暗号化方式を指定します。
オプションとして DES-CBC と 3DES-CBC があります。
 - 10 該当するフィールドに、ネゴシエーション有効期限までのキロバイト数と時間数を入力します。
 - 11 [Diffie-Hellman グループ] ドロップダウン・リストから、グループ番号を選択します。グループ 1 とグループ 2 がウォッチガード社によりサポートされています。
Diffie-Hellman は、公衆ネットワーク経路でシークレット・キーをセキュアに交渉するための数学的手法です。Diffie-Hellman グループとは、この手法を実現するために使用するパラメータの集合です。グループ 2 のほうがグループ 1 よりもセキュアですが、その分、シークレット・キーの計算に時間がかかります。
 - 12 通信がない時に VPN トンネルを開いたままにするには、[IKE Keep Alive メッセージの生成] チェックボックスをオンにします。このオプションを選択すると、VPN トンネルの接続を維持するために、トンネルに定期的に短いパケットが流されます。トンネルの接続が閉鎖されると、S6 はキーを再生し、再びトンネルを開きます。
[IKE Keep Alive メッセージの生成] チェックボックスは、デフォルトの設定に選択されています。
- デフォルトのフェーズ 2 の設定を利用するか、フェーズ 2 の設定を以下の様に変更します。

注意

フェーズ 2 の設定が両方のアプライアンスで同じであることを確認してください。

- 13 [認証アルゴリズム] ドロップダウン・リストから、認証のタイプを選択します。
- 14 [暗号化アルゴリズム] ドロップダウン・リストから、暗号化のタイプを選択します。
- 15 必要に応じて、[Perfect Forward Secrecy の有効化] チェックボックスをオンにします。
このオプションを選択すると、新規のキーが交渉されるたびに、新しく Diffie-Hellman キー交換が行われます。このオプションはセキュリティを向上させますが、毎回キー交換を行う分だけ通信に必要な時間が増加します。
- 16 該当するフィールドに、ネゴシエーション有効期限までのキロバイト数と時間数を入力します。
- 17 フェーズ 2 ネゴシエーションを使用するローカル・ネットワークとリモート・ネットワークの IP アドレスを入力します。
- 18 [Submit] をクリックします。

IPSec 準拠アプライアンスと S6 への VPN トンネルの作成

ウォッチガード社ウェブサイトにて、S6 と他の IPSec 準拠アプライアンス間の VPN トンネル設定の仕方について参照できます。

https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

要注意点

WatchGuard S6 VPN ネットワークを設定するにあたっては、以下の点に注意してください。

- ・ スター型コンフィギュレーションでは、最大 6 つの S6 アプライアンスを接続することができます。VPN トンネルを一つ以上

設定するには、WatchGuard VPN Manager が設定された WatchGuard Firebox II/III が必要です。

- VPN トンネルを形成する二つのアプライアンスには、それぞれ静的 IP アドレスがなければなりません。片方のアプライアンスが動的 IP アドレスを割り当てられていると、トンネルのもう一方のアプライアンスから送信されたパケットは送信先に届きません。動的 IP アドレスについての詳細は、33 ページの「ネットワーク・アドレスの割り当て」を参照してください。
- 両方のアプライアンスには、同じ暗号化方式を用いなければなりません。DES あるいは 3DES があります。
- 2つの Microsoft Windows NT ネットワークを接続する場合は、その2つのネットワークが同じ Microsoft Windows ドメイン内あるいはトラステッド・ドメイン内に存在する必要があります。これはマイクロソフト・ネットワークの設計上の制限であって、S6 の制限ではありません。

分割トンネリングの設定

分割トンネリングを使用すると、システム管理者は、VPN トンネルを経由したトラステッド・ネットワークからのインターネット・トラフィックの方向をすべて指定することができます。分割トンネリングを用いない場合、VPN トンネルの他端に向けられたトラフィックだけがトンネルを経由して送信され、他のインターネットアドレスへのトラフィックは直接インターネットに送信されます。分割トンネリングを使用すると、1 地点からのインターネット・ウェブサイトへのアクセスを管理することができます。

分割トンネリングを設定するには、次の手順に従います：

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、<http://192.168.111.1> です。

- 2 左側のナビゲーション・バーから、
[VPN] => [手動 VPN] を選択します。
[手動 VPN] ページが開きます。
- 3 [追加] をクリックします。
[ゲートウェイの追加] ページが表示されます。
- 4 ゲートウェイの設定
[ゲートウェイの追加] ページについての詳細は、101 ページの「複数の S6 間の VPN トンネルの設定」を参照してください。
- 5 該当するフィールドに、ローカル・ネットワークおよびリモート・ネットワークの IP アドレスを入力します。
- 6 [Submit] をクリックします。

MUVPN クライアント s の使用

MUVPN クライアントのアップグレード版により、リモート・ユーザーはセキュアな (IPSec) VPN トンネルを経由して S6 に接続することができます。このオプションにより、リモート・ユーザーは IPSec VPN トンネル経由の S6 への接続が可能となります。リモート・ユーザーは、ローカルのトラステッド・ネットワークや、VPN トンネルによってローカルの S6 に接続されたネットワークにアクセスすることができます。さらに、S6 によって、トラステッド・ネットワーク上のユーザーが VPN トンネルによってローカルの S6 に接続されたネットワークにアクセスすることもできます。もし VPNforce Port アップグレード版を購入すれば、オプションのネットワークへの MUVPN 接続が一つ得られます。VPNforce Port のユーザー・ライセンスは追加購入できます。

VPN 統計の表示

Firebox S6 には、さまざまな VPN 統計情報を提供する構成ページがあります。このページを見れば、VPN トラフィックの監視や潜在的な問題のトラブルシューティングに役立ちます。

VPN 統計ページを表示するには、次の手順を実行します。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力して、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、<http://192.168.111.1> です。
- 2 左側のナビゲーション・バーで、[VPN] => [VPN 統計] をクリックします。
[VPN 統計] ページが開きます。

FAQ(よく寄せられる質問とその回答)

なぜ静的外部アドレスが必要なのですか。

VPN 接続を形成するには、二つのアプライアンスはそれぞれ他方のアプライアンスの IP アドレスを認識していなければなりません。IP アドレスが動的であると、そのアドレスが変わる可能性があります。アドレスが変わると二つのアプライアンス間の接続が妨げられます。

静的外部アドレスを取得する方法を教えてください。

お客様のコンピューターあるいはネットワークの外部 IP アドレスはお客様の ISP によって割り当てられています。ISP は動的 IP アドレスを用いる事が多く、ネットワークの設定は比較的容易ですがウェブサーバーとネットワークの接続はより難しくなります。殆どの ISP は、オプションのサービスとして静的 IP アドレスを提供しています。

VPN 接続でのトラブルシューティングの方法を教えてください。

リモートの S6 およびリモート・ネットワーク上のコンピューターに ping することができれば、VPN トンネルは正しく機能します。その他の問題に関しては、ネットワークのソフトウェアあるいはアプリケーションの設定に原因があると考えられます。

Ping を発行できません。

リモートの S6 のローカル・ネットワーク・アドレスに Ping を発行できない場合は、次の手順に従ってください。

- 1 リモートの S6 の外部アドレスに ping を発行します。
たとえば、サイト A からサイト B(68.130.44.15) に ping を発行するには、「68.130.44.15」と入力します。もし ping が返ってこない場合は、サイト B の外部ネットワークの設定を確認してください。その設定が正しい場合は、サイト B のコンピューターがインターネットに接続されているかどうかを確認します。それでも問題が解決しない場合は、ISP へお問い合わせください。
- 2 S6 の外部アドレスに ping が発行できる場合は、リモート・ネットワーク上のローカル・アドレスに ping してみます。
サイト A で、「192.168.111.1」と入力します。VPN トンネルが正しく機能していれば、リモートの S6 が ping を送り返してきます。Ping が返ってこない場合は、ローカルの設定が正しいか確認します。VPN トンネルによって接続された二つのネットワークのローカル DHCP アドレスの範囲がどの IP アドレスとも重複していないか確認してください。トンネルによって接続された二つのネットワークの IP アドレスが重複してはいけません。

VPN アップグレード版のライセンス・キーを取得する方法を教えてください。

VPN アップグレードのライセンス・キーは、以下のウォッチガード社ウェブサイトから購入可能です。

<http://www.watchguard.com/sales/buyonline.asp>

VPN トンネルを有効化する方法を教えてください。
VPN トンネルを使用できるようにするための詳細な手順については、以下のウォッチガード社ウェブサイトを参照してください。
https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

MUVPN クライアントはリモート・コンピューターにインストールするソフトウェア・アプリケーションです。このアプリケーションにより、セキュアでないネットワークを介し、リモート・コンピューターからの保護されたネットワークへのセキュアな接続が可能となります。MUVPN クライアントは Internet Protocol Security (IPSec) を使用し、接続のセキュリティを保証しています。

MUVPN クライアントの使用方法の一例を以下に示します。まず、MUVPN クライアントをリモート・コンピューターにインストールします。すると、リモート・コンピューター上でのインターネットへの接続が確立されます。次にリモートコンピューターでインターネットへの接続が確立されます。ユーザーは MUVPN クライアントを実行し、S6 への暗号化されたトンネルを作成します。S6 により、ユーザーはトラステッド・ネットワークに接続します。S6 により、ユーザーはトラステッド・ネットワークに接続されます。こうして社員は内部ネットワークへのリモート・アクセスを

有し、ネットワークのセキュリティを危険にさらすことはありません。

MUVPN クライアントには、パーソナル・ファイアウォール・ソフトウェア・アプリケーションである ZoneAlarm がオプション機能として含まれています。ZoneAlarm は、ネットワークのリモート・ユーザーに、さらに高度なセキュリティを提供します。

この章では、リモート・コンピューターへの MUVPN クライアントのインストールおよび設定方法が記されています。また、この章には、ZoneAlarm パーソナル・ファイアウォールの機能についての情報も含まれています。

MUVPN クライアントを用いるための S6 の設定

MUVPN クライアントを用いるためには、以下の手順に従い S6 を設定します。

- 1 トラストッド・ネットワークの IP アドレスをブラウザ・ウィンドウに入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトのトラस्टッド IP アドレスは、192.168.111.1 です。
- 2 左側のナビゲーション・バーで、[VPN] ⇒ [MUVPN クライアント] をクリックします。
[MUVPN クライアント] ページが表示されます。

システム・ステータス ネットワーク 外部 トラステッド オプション (802.11b) 無線LAN設定 ルート ネットワーク統計 ダイナミックDNS 管理 システム・セキュリティ VPN Manager アクセス 更新 アップグレード 設定ファイルの表示 ファイアウォール 受信 送信 カスタム・サービス	VPN MUVPN クライアント				
	<table border="1"> <thead> <tr> <th>ユーザー</th> <th>割り当てるIP</th> </tr> </thead> <tbody> <tr> <td style="height: 100px;"></td> <td></td> </tr> </tbody> </table>	ユーザー	割り当てるIP		
	ユーザー	割り当てるIP			
	<input type="button" value="追加"/> <input type="button" value="編集"/> <input type="button" value="削除"/>				

- 3 [追加] をクリックします。
 [MUVPN クライアントの追加] ページが表示されます。

システム・ステータス ネットワーク 外部 トラステッド オプション (802.11b) 無線LAN設定 ルート ネットワーク統計 ダイナミックDNS 管理 システム・セキュリティ VPN Manager アクセス 更新 アップグレード 設定ファイルの表示 ファイアウォール 受信 送信 カスタム・サービス 利用できないサイト ファイアウォール・オプション	VPN > MUVPN クライアント MUVPN クライアントの追加
	ユーザー名 <input type="text"/>
	共有キー <input type="text"/>
	仮想IPアドレス <input type="text" value="0.0.0.0"/>
	認証アルゴリズム <input type="text" value="MD5-HMAC"/>
	暗号化アルゴリズム <input type="text" value="DES-CBC"/>
	VPN クライアント・タイプ <input type="text" value="モバイル・ユーザー"/>
	WINS サーバー <input type="text"/>
	DNS サーバー <input type="text"/>
	<input type="checkbox"/> すべてのトラフィックがトンネルを使用 (0.0.0.0/0 IP サブネット) 注: DNSとWINS設定はすべてのMUVPNユーザに共通です。
<input type="button" value="サブミット"/> <input type="button" value="リセット"/> <input type="button" value="キャンセル"/>	

- 4 該当するフィールドに、ユーザー名およびパスフレーズを入力します。
ユーザー名は電子メールアドレスとして、またパスフレーズは MUVPN クライアント使用のための事前共有キーとして使用されます。
- 5 該当するフィールドに仮想 IP アドレスを入力します。
このアドレスは、S6 へ接続するためにリモート・コンピューターにより使用されます。
- 6 **[認証アルゴリズム]** ドロップダウン・リストから、認証のタイプを選択します。
[MD5-HMAC] と [SHA1-HMAC] が選択できます。
- 7 **[暗号化アルゴリズム]** ドロップダウン・リストから、暗号化のタイプを選択します。
[DES-CBC] と [3DECS-CBC] が選択できます。
- 8 **[VPN クライアント・タイプ]** ドロップダウン・リストから、**[Mobile User]** を選択します。
- 9 **[All traffic uses tunnel (0.0.0.0/0 IP Subnet)]** チェックボックスをオンにします。
- 10 **[Submit]** をクリックします。

MUVPN クライアント使用のためのリモート・コンピューターの準備

MUVPN クライアントは、Windows オペレーティング・システムのみ互換性があります。MUVPN クライアントをインストールできるのは、これらのシステム要件を満たすコンピューターだけです。

システム要件

- Pentium プロセッサ（あるいはそれと同等のプロセッサ）を搭載したコンピューター
- 互換性のあるオペレーティング・システムおよび最小 RAM

- Microsoft Windows 98 : 32 MB
 - Microsoft Windows ME : 64 MB
 - Microsoft Windows NT 4.0 ワークステーション : 32 MB
 - Microsoft Windows 2000 プロフェッショナル : 64 MB
 - Microsoft Windows XP : 64 MB
- ・ 各オペレーティング・システムに対して最新サービス・パックが推奨されますが、必須ではありません。
 - ・ 10MB ハードディスク容量
 - ・ Native Microsoft TCP/IP コミュニケーションズ・プロトコル
 - ・ Microsoft Internet Explorer 5.0 以降
 - ・ インターネット・サービス・プロバイダー (ISP) アカウント
 - ・ ダイアルアップあるいはブロードバンド (DSL または ケーブル・モデム) 接続

MUVPN トンネルを通して共有しているウィンドウズファイルや印刷物を使用するためには、リモート・コンピューターは WINS サーバーや DNS サーバーと通信できなければなりません。これらのサーバーは、S6 によって保護されているトラステッド・ネットワークに位置しています。これらのサーバーと通信を行うには、リモート・コンピューター内に適正な Windows コンポーネントがインストール、および設定されていなければなりません。

注意

MUVPN 仮想アダプターは使用できません。使用不可であることを必ず確認してください。

Windows 98/ME オペレーティング・システムのセットアップ

このセクションでは、Windows 98/ME オペレーティング・システムに必要なネットワーク・コンポーネントをインストールし、設

定する方法を説明します。MUVPN を Windows 98/ME コンピューターで正確に機能する前に、これらのコンポーネントをインストールされなければなりません。

注意

Mobile UserVPN Adapter は、L2TP をサポートしています。

ネットワーク名の設定

Windows のデスクトップから：

- 1 [スタート] ⇒ [設定] ⇒ [コントロール・パネル] を選択します。
- 2 [ネットワーク] アイコンをダブルクリックします。
[ネットワーク] ウィンドウが表示されます。
- 3 Client for Microsoft Networks がインストールされていることを確認してください。
この設定手順を続ける前に、Client for Microsoft Networks をインストールしなければなりません。詳細については、117 ページの「Client for Microsoft Networks のインストール」を参照してください。
- 4 [Identification] タブをクリックします。
- 5 該当するフィールドに、リモート・コンピューターの名前を入力します。
この名前は、リモート・ネットワーク上で一意でなければなりません。
- 6 該当するフィールドに、この接続のドメイン・ネームを入力します。
- 7 該当するフィールドに、リモート・コンピューターの説明を入力します。
この手順はオプションです。

- 8 **[OK]** をクリックして **[ネットワーク]** ウィンドウを閉じます。
変更を保存したくない場合は、**[Cancel]** をクリックします。
- 9 コンピューターをリブートします。

Client for Microsoft Networks のインストール

ネットワークの名称を設定する前に、Client for Microsoft Network をインストールしてください。Client for Microsoft Networks がインストールされていない場合は、次の手順に従ってください。

[ネットワーク] ウィンドウから：

- 1 **[設定]** タブをクリックし、次に **[追加]** をクリックします。
[ネットワーク・コンポーネント・タイプの選択] ウィンドウが表示されます。
- 2 **[クライアント]** を選択し、次に **[Add]** をクリックします。
[ネットワーク・クライアントの選択] ウィンドウが表示されます。
- 3 左側の一覧から **[Microsoft]** を選択します。右側の一覧から **[Microsoft Networks のクライアント]** を選択し、次に **[OK]** をクリックします。
- 4 **[Microsoft Networks のクライアント]** を選択し、次に **[プロパティ]** をクリックします。
- 5 **[Windows NT ドメインにログオン]** チェックボックスをオンにします。
- 6 **[Windows NT ドメイン]** のテキスト・フィールドにドメイン・ネームを入力します。
ドメイン名の典型的な例としては、「営業」、「オフィス」、「倉庫」などがあります。
- 7 **[Restore Network Connections にログオン]** チェックボックスをオンにします。

ダイアルアップ・ネットワークのインストール

Mobile UserVPN アダプターをインストールする前に、ダイアルアップ・ネットワークをインストールしなければなりません。ダイアルアップ・ネットワークがインストールされていない場合は、次の手順に従ってください。

Windows のデスクトップから：

- 1 [スタート] ⇒ [設定] ⇒ [コントロール・パネル] を選択します。
- 2 [プログラムの追加・削除] アイコンをダブルクリックします。
[プロパティの追加・削除] ウィンドウが表示されます。
- 3 [ウィンドウズの設定] タブをクリックします。
[ウィンドウズの設定] ダイアログ・ボックスが表示されます。オペレーティング・システムはインストール済みのコンポーネントを検索します。
- 4 [Communications] チェックボックスをオンにし、次に [OK] をクリックします。
[ファイルをコピー] ダイアログ・ボックスが表示されます。オペレーティングシステムが必要なファイルをコピーします。
- 5 [ダイアルアップ・ネットワークの設定] ウィンドウが表示されます。[OK] をクリックして、コンピューターをリブートさせます。
コンピューターがリブートします。

Windows 98 のダイアルアップ・ネットワークのコンポーネントは、1.4 修正プログラムで更新しなければなりません。このアップデート版は、Microsoft のウェブサイトからダウンロードできます。

WINS および DNS の設定

リモート・コンピューターは、WINS サーバーおよび DNS サーバーと通信可能でなければなりません。これらのサーバーは、S6 によって保護されたトラステッド・ネットワーク上にあります。

Windows のデスクトップから：

- 1 [スタート] ⇒ [設定] ⇒ [コントロール・パネル] を選択します。
- 2 [ネットワーク] アイコンをダブルクリックします。
[ネットワーク] ウィンドウが表示されます。
- 3 ネットワークコンポーネントの [TCP/IP] ⇒ [Dial-Up Adapter] を選択します。次に [プロパティ] をクリックします。
[TCP/IP プロパティの情報] ウィンドウが表示されます。
- 4 [OK] をクリックします。
- 5 [DNS 設定] タブをクリックし、次に [DNS の有効化] チェックボックスをオンにします。
- 6 [DNS サーバーの検索要求] のテキスト・フィールドに、DNS サーバーの IP アドレスを入力します。[追加] をクリックします。
リモート DNS サーバーが複数ある場合は、手順 5 と 6 を繰り返します。

注意

S6 の背後の社内ネットワーク上の DNS サーバーが、一覧の最初に示されていないかもしれません。

- 7 [WINS 設定] タブをクリックし、次に [WINS Resolution の有効化] チェックボックスをオンにします。
- 8 [WINS サーバーの検索要求] のテキスト・フィールドに、WINS サーバーの IP アドレスを入力し、[追加] をクリックします。
リモート WINS サーバーを複数台有する場合、手順 7 と 8 を繰り返します。

- 9 [TCP/IP プロパティ・ウィンドウ] を閉じるために **OK** をクリックします。[ネットワーク・ウィンドウ] を閉じるために **OK** をクリックします。
[システム設定の変更] ダイアログ・ボックスが表示されます。
- 10 **[Yes]** をクリックし、コンピューターをリブートさせます。
コンピューターがリブートします。

Windows NT オペレーティング・システムのセットアップ

このセクションでは、Windows NT オペレーティング・システムに必要なネットワーク・コンポーネントをインストールし、設定する方法を説明します。MUVPN が Windows NT コンピューター上で正確に機能する前に、これらのコンポーネントがインストールされなければなりません。

注意

Mobile UserVPN Adapter は、L2TP をサポートしています。

Windows NT への Remote Access Services のインストール

Mobile UserVPN Adapter をインストールする前に、Remote Access Services (RAS) をインストールしなければなりません。RAS がインストールされていない場合は、次の手順に従ってください。

Windows のデスクトップから：

- 1 **[スタート]** ⇒ **[設定]** ⇒ **[コントロール・パネル]** を選択します。
- 2 **[ネットワーク]** アイコンをダブルクリックします。
[ネットワーク] ウィンドウが表示されます。
- 3 **[サービス]** タブをクリックし、次に **[追加]** をクリックします。

- 4 一覧から [リモート・アクセス・サービス] を選択し、次に [OK] をクリックします。
- 5 Windows NT のインストール・ファイルへのパスを入力するか、あるいはシステム・インストール CD を挿入し、次に [OK] をクリックします。
[リモート・アクセスの設定] ウィンドウが表示されます。
- 6 モデムのような RAS デバイスを追加するためには、[Yes] をクリックした後、[追加] をクリックします。
- 7 [新しいモデムのインストール] ウィザードを完了します。

注意

モデムが全くインストールされていない場合は、[Don't detect my modem; I will select it from a list] チェックボックスをオンにします。そして標準 28800 モデムを選択します。RAS をインストールするには、モデムのような少なくとも RAS デバイスをひとつ必要とします。モデムがない場合、[a serial cable between two computers] を選択できます。

- 8 [RAS Device の追加] ウィンドウから前手順で追加されたモデムを選択します。
- 9 [OK] をクリックし、[Continue] をクリックした後、[Close] をクリックします。
- 10 コンピューターをリブートします。

WINS および DNS の設定

リモート・コンピューターは、WINS サーバーおよび DNS サーバーと通信可能でなければなりません。これらのサーバーは、S6 によって保護されたトラステッド・ネットワーク上にあります。

Windows のデスクトップから：

- 1 [スタート] ⇒ [設定] ⇒ [コントロール・パネル] を選択します。

- 2 [ネットワーク] アイコンをダブルクリックします。
[ネットワーク] ウィンドウが表示されます。
- 3 [プロトコル] タブをクリックして、次に [TCP/IP] プロトコルを選択します。
- 4 [プロパティ] をクリックします。
[Microsoft TCP/IP のプロパティ] ウィンドウが表示されます。
- 5 [DNS] タブをクリックし、次に [追加] をクリックします。
- 6 該当するフィールドに DNS サーバーの IP アドレスを入力します。
更に追加の DNS サーバーを追加するには、手順 5 と 6 を繰り返します。

注意

S6 の裏側の社内ネットワーク上の DNS サーバーが、一覧の最初に示されていないければなりません。

- 7 [WINS アドレス] タブをクリックし、該当するフィールドに WINS サーバーの IP アドレスを入力し、[OK] をクリックします。
更に追加の WINS サーバーを追加するには、この手順を繰り返します。
- 8 [Close] をクリックし、[ネットワーク] ウィンドウを閉じます。
[ネットワーク設定の変更] ダイアログ・ボックスが表示されます。
- 9 コンピューターをリブートするために [Yes] をクリックします。
コンピューターがリブートします。

Windows 2000 オペレーティング・システムのセットアップ

このセクションでは、Windows 2000 オペレーティング・システムに必要なネットワーク・コンポーネントをインストールし、設定

する方法を説明します。MUVPN クライアントが Windows 2000 コンピューター上で正確に機能する前に、これらのコンポーネントがインストールされなければなりません。

Windows のデスクトップから：

- 1 [スタート] ⇒ [設定] ⇒ [ネットワークおよびダイアルアップ・コネクション] を選択します。
- 2 インターネットへのアクセスに使用するダイアルアップの接続を選択します。
接続ウィンドウが表示されます。
- 3 [プロパティ] をクリックし、[ネットワーク] タブをクリックします。
- 4 以下のコンポーネントがインストールされ、使用可能であることを確認してください。
 - Internet Protocol (TCP/IP)
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

Internet Protocol (TCP/IP) ネットワーク・コンポーネントのインストール

接続ウィンドウから、[ネットワーク] タブの：

- 1 [インストール] をクリックします。
[ネットワーク・コンポーネント・タイプの選択] ウィンドウが表示されます。
- 2 [プロトコル] ネットワーク・コンポーネントをダブルクリックします。
[ネットワーク・プロトコルの選択] ウィンドウが表示されます。
- 3 [インターネット・プロトコル (TCP/IP)] ネットワーク・プロトコルを選択し、[OK] をクリックします。

File and Printer Sharing for Microsoft Networks のインストール

接続ウィンドウから、[ネットワーク] タブの：

- 1 [インストール] をクリックします。
[ネットワーク・コンポーネント・タイプの選択] ウィンドウが表示されます。
- 2 [サービス] ネットワーク・コンポーネントをダブルクリックします。
[ネットワーク・サービスの選択] ウィンドウが表示されます。
- 3 [File and Printer Sharing for Microsoft Networks] ネットワーク・サービスを選択し、[OK] をクリックします。

Client for Microsoft Networks のインストール

接続ウィンドウから、[ネットワーク] タブの：

- 1 [インストール] をクリックします。
[ネットワーク・コンポーネント・タイプの選択] ウィンドウが表示されます。
- 2 [クライアント] ネットワーク・コンポーネントをダブルクリックします。
[ネットワーク・プロトコルの選択] ウィンドウが表示されます。
- 3 [Microsoft ネットワークのクライアント] ネットワーク・クライアントを選択し、[OK] をクリックします。

WINS および DNS の設定

リモート・コンピューターは、WINS サーバーおよび DNS サーバーと通信可能でなければなりません。これらのサーバーは、S6 によって保護されたトラステッド・ネットワーク上にあります。

接続ウィンドウから、[ネットワーク] タブの：

- 1 [インターネット・プロトコル (TCP/IP)]) コンポーネントを選択し、次に [プロパティ] をクリックします。
[インターネット・プロトコル (TCP/IP) プロパティ] ウィンドウが表示されます。
- 2 [詳細設定] をクリックします。
[TCP/IP 設定の詳細] ウィンドウが表示されます。
- 3 [DNS] タブをクリックし、次に [DNS server addresses, in order of use] と表記されたセクションから、[追加] をクリックします。
[TCP/IP DNS サーバー] ウィンドウが表示されます。
- 4 該当するフィールドに DNS サーバーの IP アドレスを入力し、[追加] をクリックします。
更に DNS サーバーを追加するには、手順 3 と 4 を繰り返します。

注意

S6 の背後の社内ネットワーク上の DNS サーバーが、一覧の最初に示されていないければなりません。

- 5 [Append these DNS suffixes (in order)] チェックボックスをオンにし、[追加] をクリックします。
[TCP/IP ドメイン・サフィックス] ウィンドウが表示されます。
- 6 該当するフィールドにドメイン・サフィックスを入力します。
更に追加の DNS サフィックスを追加するには、手順 5 に戻ってください。
- 7 [WINS] タブをクリックした後、[WINS addresses, in order of use] と表記されたセクションから、[追加] をクリックします。
[TCP/IP WINS サーバー] ウィンドウが表示されます。
- 8 該当するフィールドに WINS サーバーの IP アドレスを入力し、[Add] をクリックします。
更に追加の WINS サーバーを追加するには、手順 7 と 8 を繰り返します。

- 9 [OK] をクリックして [TCP/IP の詳細設定] ウィンドウを閉じ、[インターネット・プロトコル (TCP/IP) プロパティ] ウィンドウを閉じるために [OK] をクリックし、次に [OK] をクリックします。
- 10 接続ウィンドウを閉じるために [Cancel] をクリックします。

Windows XP オペレーティング・システムのセットアップ

このセクションでは、Windows XP オペレーティング・システムに必要なネットワーク・コンポーネントをインストールし、設定する方法を説明します。MUVPN を Windows XP コンピューターで正確に機能させるには、その前にこれらのコンポーネントをインストールしなければなりません。

Windows のデスクトップから：

- 1 [スタート] ⇒ [コントロール・パネル] を選択します。
[コントロール・パネル] ウィンドウが表示されます。
- 2 [ネットワーク接続] アイコンをダブルクリックします。
- 3 インターネットへのアクセスに使用する接続をダブルクリックします。
接続ウィンドウが表示されます。
- 4 [プロパティ] をクリックした後、[ネットワーク] タブをクリックします。
- 5 以下のコンポーネントがインストールされ、使用可能であることを確認してください。
 - Internet Protocol (TCP/IP)
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

Internet Protocol (TCP/IP) ネットワーク・コンポーネントのインストール

接続ウィンドウから、[ネットワーク] タブの：

- 1 **[インストール]** をクリックします。
[ネットワーク・コンポーネント・タイプの選択] ウィンドウが表示されます。
- 2 **[プロトコル]** ネットワーク・コンポーネントをダブルクリックします。
[ネットワーク・プロトコルの選択] ウィンドウが表示されます。
- 3 **[インターネット・プロトコル (TCP/IP)]** ネットワーク・プロトコルを選択し、**[OK]** をクリックします。

File and Printer Sharing for Microsoft Networks のインストール

接続ウィンドウから、[ネットワーク] タブの：

- 1 **[インストール]** をクリックします。
[ネットワーク・コンポーネント・タイプの選択] ウィンドウが表示されます。
- 2 **[サービス]** ネットワーク・コンポーネントをダブルクリックします。
[ネットワーク・サービスの選択] ウィンドウが表示されます。
- 3 **[File and Printer Sharing for Microsoft Networks]** ネットワーク・サービスを選択し、**[OK]** をクリックします。

Client for Microsoft Networks のインストール

接続ウィンドウから、[ネットワーク] タブの：

- 1 **[インストール]** をクリックします。
[ネットワーク・コンポーネント・タイプの選択] ウィンドウが表示されます。

- 2 **[クライアント]** ネットワーク・コンポーネントをダブルクリックします。
[ネットワーク・プロトコルの選択] ウィンドウが表示されます。
- 3 **[Microsoft ネットワークのクライアント]** ネットワーク・クライアントを選択し、**[OK]** をクリックします。

WINS および DNS の設定

リモート・コンピューターは、WINS サーバーおよび DNS サーバーと通信可能でなければなりません。これらのサーバーは、S6 によって保護されたトラステッド・ネットワーク上にあります。

接続ウィンドウから、**[ネットワーク]** タブの：

- 1 **[インターネット・プロトコル (TCP/IP)]** コンポーネントを選択します。
- 2 **[プロパティ]** をクリックします。
[インターネット・プロトコル (TCP/IP) ・プロパティ] ウィンドウが表示されます。
- 3 **[詳細設定]** をクリックします。
[TCP/IP 詳細設定] ウィンドウが表示されます。
- 4 **[DNS]** タブをクリックし、次に **[DNS サーバー・アドレス、in order of use]** と表記されたセクションから、**[追加]** をクリックします。
[TCP/IP DNS Server] ウィンドウが表示されます。
- 5 該当するフィールドに DNS サーバーの IP アドレスを入力し、**[Add]** をクリックします。
更に DNS サーバーを追加するには、手順 4 と 5 を繰り返します。

注意

S6 の背後の社内ネットワーク上の DNS サーバーが、一覧の最初に示されていないなければなりません。

- 6 [Append these DNS suffixes (in order)] チェックボックスをオンにし、[追加] をクリックします。
[TCP/IP ドメイン・サフィックス] ウィンドウが表示されます。
- 7 該当するフィールドにドメイン・サフィックスを入力します。
更に DNS サフィックスを追加するには、手順 6 に戻ってください。
- 8 [WINS] タブをクリックした後、[WINS addresses, in order of use] と表記されたセクションから、[追加] をクリックします。
[TCP/IP WINS Server] ウィンドウが表示されます。
- 9 該当するフィールドに WINS サーバーの IP アドレスを入力し、[追加] をクリックします。
更に WINS サーバーを追加するには、手順 8 と 9 を繰り返します。
- 10 [OK] をクリックして [TCP/IP の詳細設定] ウィンドウを閉じ、[OK] をクリックして [Internet Protocol (TCP/IP) Properties] ウィンドウを閉じ、次に [OK] をクリックします。
- 11 接続ウィンドウを閉じるために、[Cancel] をクリックします。

MUVPN クライアントのインストールと設定

MUVPN のインストール・ファイルは、ウォッチガード社ウェブサイトをご覧ください：

<http://www.watchguard.com/support>

注意

MUVPN クライアントのインストールと設定を行うには、リモート・コンピューターに対するローカル管理者の権利をもっていないとはいけません。

MUVPN クライアントのインストール

MUVPN クライアントをインストールするには、以下の手順に従ってください。

- 1 リモート・コンピューターに MUVPN のインストール・ファイルをコピーする。
- 2 MUVPN インストール・ファイルをダブルクリックして、InstallShield ウィザードを開始します。
もし手順をスキップしてしまった場合、キャンセルをクリックして、初めからインストールをやり直してください。
- 3 **[Next]** をクリックします。
読取専用のファイルが検出されたために InstallShield が停止した場合は、インストールを続けるために **[Yes]** をクリックします。
- 4 ウェルカム・メッセージが表示されます。 **[Next]** をクリックします。
ソフトウェア使用許諾契約書が表示されます。
- 5 使用許諾契約書に同意するには、 **[Yes]** をクリックします。
[Setup Type] ウィンドウが表示されます。
- 6 インストールのタイプを選択します。ウォッチガード社は、標準のインストールを推奨しています。 **[Next]** をクリックします。
- 7 Windows 2000 コンピューターでは、InstallShield が Windows 2000 L2TP コンポーネントを検出します。このコンポーネントがインストールされている場合、InstallShield が再びそれをインストールすることはありません。続けるためには **[OK]** をクリックします。
[Select Components] ウィンドウが表示されます。
- 8 デフォルトの選択を変更しないでください。 **[Next]** をクリックします。
[Start Copying Files] ウィンドウが表示されます。

- 9 [Next] をクリックしてファイルをインストールします。
Audni vapmpAv ファイルがインストールされる際、コマンド・プロンプト・ウィンドウが表示されます。これが正常です。ファイルがインストールされるとコマンド・プロンプト・ウィンドウは閉じ、処理が続きます。
- 10 InstallShield ウィザードが完了したら、[Finish] をクリックします。
- 11 InstallShield ウィザードは、ユーザーのプロファイル・ファイルを検索します。この手順をスキップするために、[Next] をクリックします。ユーザーのプロファイル・ファイルは、インストールされる必要がありません。
情報ダイアログ・ボックスが表示されます。
- 12 インストールを続けるために、[OK] をクリックします。
- 13 MUVPN クライアントのインストールが完了します。[Yes, I want to restart my computer now] が選択されていることを確認します。[Finish] をクリックします。
コンピューターがリブートします。

注意

コンピューターのリブートの後、ZoneAlarm パーソナル・ファイアウォールにより、ネットワークへの接続が妨げられることがあります。これが生じた場合は、インストール後まず初めに、コンピューターにはローカルでログオンしてください。ZoneAlarm に関する詳細については、147 ページの「ZoneAlarm パーソナル・ファイアウォール」をご覧ください。

MUVPN クライアントの設定

コンピューターがリブートすると、[WatchGuard Policy Import] ウィンドウが開きます。[Cancel] をクリックします。この時点でポリシーをインポートする必要はありません。

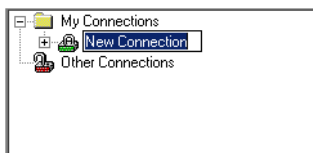
Windows のデスクトップのシステム・トレイから：

- 1 MUVPN クライアントのアイコンを右クリックして、**[Activate Security Policy]** を選択します。
- 2 MUVPN クライアントのアイコンをダブルクリックします。
[Security Policy Editor] ウィンドウが表示されます。

注意

ZoneAlarm パーソナル・ファイアウォールが警告メッセージを表示する場合があります。ZoneAlarm に関する詳細情報は、147 ページの「ZoneAlarm パーソナル・ファイアウォール」をご覧ください。

- 3 **[Edit]** ⇒ **[Add]** ⇒ **[Connection]** . を選択します。
左側の **[Network Security Policy]** のフィールドに **[New Connection]** が表示されます。**[Connection Security]**、**[Remote Party Identity]**、**[Addressing]** の設定が右側に表示されます。



- 4 新しい接続のための一意の名前を入力します。
これが特定のユーザーに対し一意のポリシーである場合は、ポリシーにおいて一意の名前を入力します。例えば、ユーザーの名前を含んだ名前にすることもできます。
- 5 **[Secure]** オプションを選択します。
これはデフォルトの設定です。
- 6 **[Only Connect Manually]** チェックボックスをオンにします。
- 7 **[ID Type]** のドロップダウン・メニューから **[IP Subnet]** オプションを選択します。
[Remote Party Identity] と **[Addressing]** のフィールドが更新されます。

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 0.0.0.0

Mask: 0.0.0.0

Protocol: All Port: All

Connect using: Secure Gateway Tunnel

ID Type: IP Address

10.168.2.137

- サブネットおよびマスク・アドレスを設定する際、MUVPN ユーザーがトンネルを介してインターネットにアクセスすることが可能にするかどうかを決定します。トラステッド・ネットワークのみアクセスできるようにするには、サブネットとマスクの各欄にトラステッド・ネットワーク・アドレスを入力してください。また、トラステッド・ネットワークおよびインターネットにアクセスできるようにする場合は、サブネットおよびマスクそれぞれの欄に「0.0.0.0」と入力してください。

注意

サブネットおよびマスクの欄に入力するアドレスは、「MUVPN Client を追加」ページに入力した仮想 IP アドレスと同様のものではないと見なされません。詳細については「MUVPN Client 用に S6 を設定する」を参照してください。

- [Protocol] ドロップダウン・リストから [All] を選択します。これはデフォルトの設定です。
- [Connect using] チェックボックスをオンにし、[Connect using] ドロップダウン・リストから [Secure Gateway Tunnel] を選択します。

- 11 **[ID Type]** ドロップダウン・リストから **[IP Address]** を選択し、該当するフィールドに外部インターフェイスの IP アドレスを入力します。

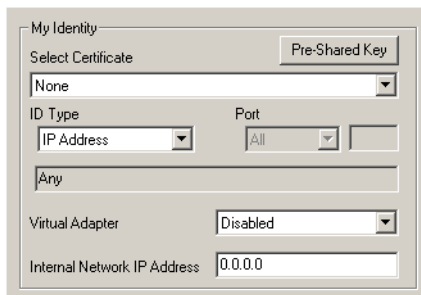
My Identity 設定の定義

My Identity の設定を定義するには、以下の手順に従います。

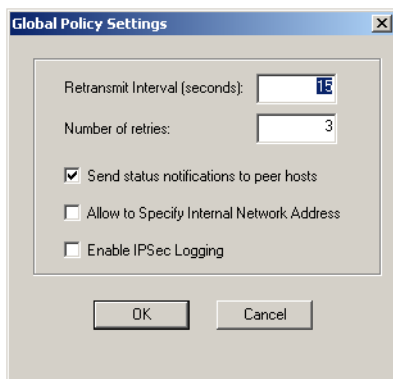
- 1 **[Network Security Policy]** を開いて、新しいエントリーを表示します。
[My Identity] と [Security Policy] のエントリーが表示されます。



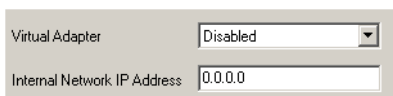
- 2 **[My Identity]** を選択します。
[My Identity] と [Internet Interface] の設定が右側に表示されます。



- 3 **[Options]** ⇒ **[Global Policy Settings]** を選択します。
[Global Policy Settings] ウィンドウが表示されます。

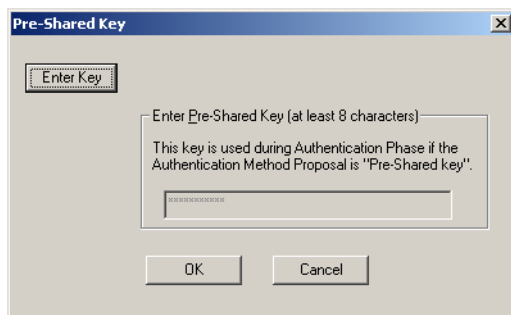


- 4 [Allow to Specify Internal Network Address] チェックボックスをオンにし、[OK] をクリックします。
[My Identity] のセクションに [Internal Network IP Address] のフィールドが表示されます。

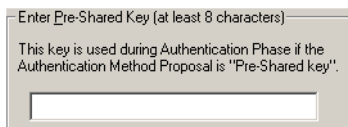


- 5 [Select Certificate] ドロップダウン・リストから、[None] を選択します。
- 6 [ID Type] ドロップダウン・リストから [E-mail Address] を選択し、該当するフィールドに S6 に定義されたユーザー名を入力します。
- 7 [Virtual Adapter] ドロップダウン・リストから [Disabled] を選択します。
- 8 [Internal Network IP Address] のテキスト・フィールドに [0.0.0.0] と入力します。
デフォルト値としてこの値が表示されます。

- 9 [Name] ドロップダウン・リストから、[Any] を選択します。
これはデフォルトの設定です。
- 10 [Pre-Shared Key] をクリックします。
[Pre-Shared Key] ダイアログ・ボックスが表示されます。



- 11 [EnterKey] をクリックします。
テキスト・フィールドが使用可能になります。



- 12 S6 に入力した MUVPN クライアント・パスフレーズと全く同じテキストを入力し、[OK] をクリックします。

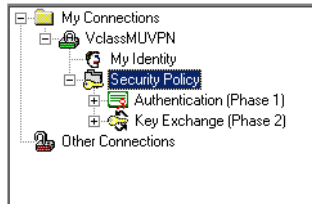
注意

事前共有キーと電子メールアドレスは両方とも、S6 に設定したシステム・パスフレーズおよびシステム管理者の名前に完全に一致しなければなりません。一致しない場合は接続できません。

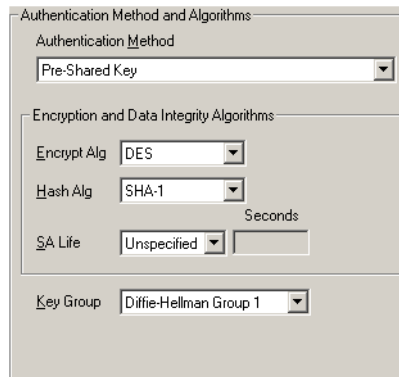
フェーズ 1 およびフェーズ 2 の設定の定義

以下の手順に従ってフェーズ 1 およびフェーズ 2 の設定を定義します。値は S6 の設定値と一致していなければなりません。

- 1 **[Network Security Policy]** のフィールドから、**[Security Policy]** を開きます。
フェーズ 1 およびフェーズ 2 両方のネゴシエーションが表示され
ます。



- 2 **[Authentication (Phase 1)]** を開きます。
[Proposal] エントリーが表示されます。
- 3 **[Proposal 1]** を選択します。
[Authentication Method and Algorithms] の設定が右側に表示され
ます。



- 4 **[Authentication Method]** ドロップダウン・リストから、**[Pre-Shared]** キーを選択します。

注意

これらの値は、Firebox S6 の設定値と一致していなければなりません。

- 5 **[Encrypt Alg]** ドロップダウン・リストから、**[DES]** を選択し、**[Hash Alg]** ドロップダウン・リストから、**[SHA-1]** を選択します。
- 6 **[SA Life]** ドロップダウン・リストから、**[Unspecified]** を選択します。
これはデフォルトの設定値です。
- 7 **[Key Group]** ドロップダウン・リストから、**[Diffie-Hellman Group 1]** を選択します。
- 8 **[Key Exchange (Phase 2)]** を開きます。
[Proposal] エントリーが表示されます。
- 9 **[Proposal 1]** を選択します。
[IPSec Protocols] の設定が右側に表示されます。


IPSec Protocols

	Seconds	KBytes
SA Life	Unspecified	
Compression	None	
<input checked="" type="checkbox"/> Encapsulation Protocol (ESP)		
Encrypt Alg	DES	
Hash Alg	SHA-1	
Encapsulation	Tunnel	
<input type="checkbox"/> Authentication Protocol (AH)		
Hash Alg	SHA-1	
Encapsulation	Tunnel	

- 10 **[SA Life]** ドロップダウン・リストから、**[Both]** を選択します。
- 11 **[Seconds]** フィールドに **[86400]**、**[Kbytes]** フィールドに **Åm8192Ån** と入力します。
- 12 **[Compression]** ドロップダウン・リストから、**[None]** を選択します。
これはデフォルトの設定値です。S6 は圧縮をサポートしていません。
- 13 **[Encapsulation Protocol (ESP)]** チェックボックスをオンにします。
- 14 **[Encrypt Alg]** および **[Hash Alg]** ドロップダウン・リストから値を選択します。

注意

これらの値は、S6 の設定値と一致していなければなりません。設定値が一致していない場合は接続できません。

- 15 **[カプセル化]** ドロップダウン・リストから、**[Tunnel]** を選択します。
これはデフォルトの設定値です。
- 16 **[Authentication Protocol (AH)]** チェックボックスがオフになっていることを確認します。
- 17 **[File]** ⇒ **[Save]** を選択するか、あるいは右側に表示されたボタンをクリックします。 

MUVPN クライアントのアンインストール

MUVPN クライアントをアンインストールするには、次の手順に従います。ウォッチガード社は Windows の [プログラムの追加と削除] ツールの使用を推奨しています。

現在のトンネルおよびダイアルアップ接続を全て切断します。リモート・コンピューターをリブートします。これらの手順は、Windows のデスクトップから行います。

- 1 **[スタート]** ⇒ **[設定]** ⇒ **[コントロール・パネル]** を選択します。
[コントロール・パネル] ウィンドウが表示されます。
- 2 **[Add/Remove Programs]** アイコンをダブルクリックします。
[プログラムの追加と削除] ウィンドウが表示されます。
- 3 **[Mobile User VPN]** を選択し、**[Change/Remove]** をクリックします。
InstallShield ウィザードが表示されます。
- 4 **[削除]** を選択し、**[Next]** をクリックします。
[Confirm File Deletion] ダイアログ・ボックスが表示されます。
- 5 **[OK]** をクリックして全てのコンポーネントを削除します。
「dni_vapmp」ファイルを削除する際、コマンド・プロンプト・ウィンドウが表示されます。これが正常です。ファイルが削除されるとコマンド・プロンプト・ウィンドウは閉じ、処理が続きます。
[Uninstall Security Policy] ダイアログ・ボックスが表示されます。
- 6 **[Yes]** をクリックして Security Policy Personal Certificates と Private/Public Keys を削除します。
[InstallShield Wizard] ウィンドウが表示されます。
- 7 **[Yes, I want to restart my computer now]** を選択します。
[Finish] オプションをクリックします。
コンピューターがリブートします。

注意

ZoneAlarm パーソナル・ファイアウォールの設定は、デフォルトで次のディレクトリに格納されます。

Windows 98: c:\windows\internet logs\

Windows NT and 2000: c:\winnt\internet logs\

Windows XP: c:\windows\internet logs

これらの設定を削除するには、適切なディレクトリの中身を削除してください。

- 8 コンピューターがリブートしたら、[スタート] ⇒ [プログラム] を選択します。
- 9 [Mobile User VPN] を右クリックし、[Delete] を選択して、[スタート] メニューからこの選択を削除します。

MUVPN クライアントの接続と切断

MUVPN クライアント・ソフトウェアにより、インターネットを介したリモート・コンピューターから保護されたネットワークへのセキュアな接続が可能になります。この接続を確立するためには、インターネットに接続し、また MUVPN クライアントを用いて保護されたネットワークへ接続しなければなりません。

MUVPN クライアントの接続

- 1 ダイアルアップ・ネットワーク、LAN、あるいは WAN を通してインターネットに接続します。

Windows のデスクトップのシステム・トレイから：

- 2 MUVPN クライアントが有効でない場合は、アイコンを右クリックして [Activate Security Policy] を選択します。
MUVPN クライアント・アイコンのステータスを判定する方法についての詳細は、142 ページの「MUVPN クライアント・アイコン」をご覧ください。

Windows のデスクトップから：

- 3 [スタート] ⇒ [プログラム] ⇒ [Mobile User VPN] ⇒ [接続] を選択します。
[WatchGuard Mobile User Connect] ウィンドウが表示されます。

4 [Yes] をクリックします。

MUVPN クライアント・アイコン

MUVPN アイコンが Windows のデスクトップのシステム・トレイに表示されます。このアイコン画像は接続状態の情報を示しています。

無効状態



MUVPN セキュリティ・ポリシーは無効になります。このアイコンは Windows のオペレーティング・システムが必要な MUVPN サービスを開始しない場合に表示されます。もしこれが生じた場合は、リモート・コンピューターをリブートしなければなりません。問題が続く場合は、MUVPN クライアントを再インストールします。

有効状態



MUVPN クライアントはセキュアな MUVPN トンネル接続を確立できる状態です。

有効状態で、セキュアでないデータの送信中



MUVPN クライアントはセキュアな MUVPN トンネル接続を確立できる状態です。アイコンの右側の赤いバーはクライアントがセキュアでないデータを送信中であることを示しています。

有効状態で、接続中



MVPN クライアントは最低一つのセキュアな MVPN トンネル接続を確立しました。データは送信していません。

有効状態で、接続中、セキュアでないデータの送信中



MVPN クライアントは最低一つのセキュアな MVPN トンネル接続を確立しました。アイコンの右側の赤いバーは、クライアントがセキュアでないデータのみを送信していることを示しています。

有効状態で、接続中、セキュアなデータの送信中



MVPN クライアントは最低一つのセキュアな MVPN トンネル接続を確立しました。アイコンの右側の緑のバーは、クライアントがセキュアなデータのみを送信していることを示しています。

有効状態で、接続中、セキュアなデータとセキュアでないデータ両方の送信中



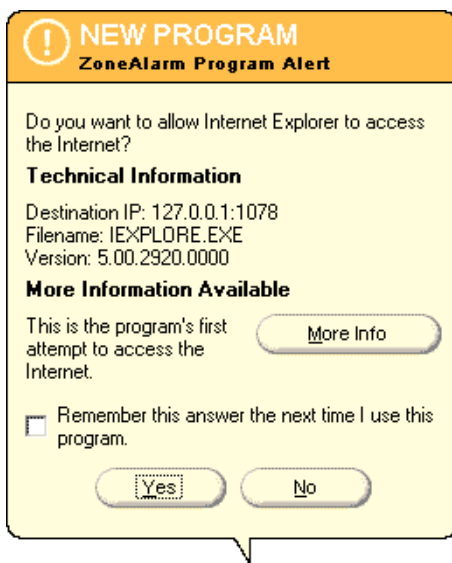
MVPN クライアントは最低一つのセキュアな MVPN トンネル接続を確立しました。アイコンの右側の赤と緑のバーは、クライアントがセキュアなデータとセキュアでないデータの両方を送信中であることを示しています。

パーソナル・ファイアウォールを介した MUVPN クライアントの作動許可

以下のプログラムは MUVPN クライアントに関連しています。MUVPN トンネルを確立するには、これらのプログラムがパーソナル・ファイアウォールを介して作動できるようにする必要があります：

- MuvpnConnect.exe
- IreIKE.exe

これらのプログラムがインターネットにアクセスしようとする
と、パーソナルファイアウォールがその動作を検出します。[New Program] 警告ウィンドウが表示され、MuvpnConnect.exe プログラムへのアクセスを要求します。



[New Program] 警告ウィンドウから：

- 1 **[Remember this answer the next time I use this program]**
 チェックボックスをオンにし、**[Yes]** をクリックします。
 オプションを選択することにより、MUVPN 接続を試みるたびに、
 ゾーンアラーム・パーソナル・ファイアウォールはこのプログラムが
 インターネットにアクセスすることを許可します。

[New Program] 警告ウィンドウが表示され、IreIKE.exe プログラムへのアクセスを要求します。

- 2 **[Remember this answer the next time I use this program]**
 チェックボックスをオンにし、**[Yes]** をクリックします。
 オプションを選択することにより、MUVPN 接続を試みるたびに、
 ZoneAlarm パーソナル・ファイアウォールはこのプログラムがイン
 ターネットにアクセスすることを許可します。

MUVPN クライアントの切断

Windows のデスクトップのシステム・トレイから：

- 1 MUVPN クライアントの**アイコン**を右クリックして、
[Deactivate Security Policy] を選択します。
 赤いバーが付いた MUVPN クライアントのアイコンが表示され、送信
 中のデータがセキュアでないことを示します。
 ZoneAlarm パーソナル・ファイアウォールが有効である場合は、
 このときに無効にします。

Windows のデスクトップのシステム・トレイから：

- 1 右側に示す ZoneAlarm アイコンを右クリックします。 **ZA**
- 2 **Shutdown [Shutdown ZoneAlarm]** を選択します。
 [Shutdown ZoneAlarm] ウィンドウが表示されます。
- 3 **[Yes]** をクリックします。

MUVPN クライアント接続の監視

MUVPN クライアントには、Log Viewer と Connection Monitor がインストールされています。これらのツールを用いることによって、MUVPN 接続の監視や、生じる可能性のある問題の診断を行うことができます。

Log Viewer の使用

Log Viewer は、通信ログを表示します。このログは MUVPN トンネルの接続中に起こるイベントを示しています。

Windows のデスクトップのシステム・トレイから：

- 1 **[Mobile User VPN]** クライアント・アイコンを右クリックします。
- 2 **[Log Viewer]** を選択します。
[Log Viewer] ウィンドウが表示されます。

Connection Monitor の使用

Connection Monitor は、セキュリティ・ポリシーにおける個々の有効な接続の統計情報や診断情報を表示します。この表示はセキュリティ・ポリシー設定やセキュリティー・アソシエーション (SA) の情報を示しています。表示された情報は、フェーズ 1 の IKE (インターネット鍵交換) ネゴシエーションおよびフェーズ 2 の IPSec ネゴシエーションの間に決定されます。

Windows のデスクトップのシステム・トレイから：

- 1 **[Mobile User VPN]** クライアント・アイコンを右クリックします。
- 2 **[Connection Monitor]** を選択します。
[Connection Monitor] ウィンドウが表示されます。
接続名の左側にアイコンが現れます。

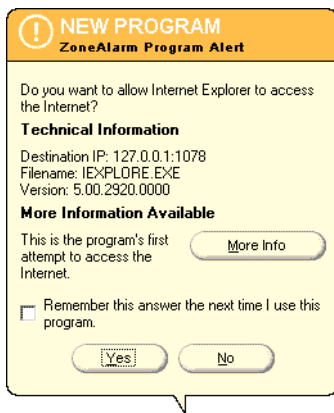
- SA は接続がフェーズ 1 の SA のみを持つことを示します。フェーズ 1 の SA は以下の状況において割り当てられます：
 - セキュアなゲートウェイ・トンネルへの接続の場合
 - フェーズ 2 の SA がまだ接続されていない場合
 - フェーズ 2 の SA 接続が不可能な場合
- キーは、接続がフェーズ 2 の SA であることを示します。この接続は、フェーズ 1 の SA を持つこともあります。
- キーの下に描かれた黒い線は、接続においてクライアントがセキュアな IP トラフィックを処理中であることを示します。
- いくつかのキーのアイコンが一つの SA アイコンの上にある場合は、複数のフェーズ 2 の SA を保護するゲートウェイへの単一のフェーズ 1 の SA であることを示しています。

ZoneAlarm パーソナル・ファイアウォール

パーソナル・ファイアウォールは、自分のコンピューターと外界との間の防壁です。コンピューターが最も被害を受けやすいのは、接続選択です。これらの接続選択をポートと言います。ポートがないと、コンピューターはインターネットに接続できません。

ZoneAlarm は、単純なルールに従うことでこれらのポートを保護しています：信頼されたプログラムへのトラフィックを明確に許可した場合を除き、全ての受信・送信トラフィックを遮断することです。

ZoneAlarm を使用した場合、以下の画像のような [New Program] 警告ウィンドウを頻繁に目にするようになります。



この警告は、プログラムの一つがインターネットあるいはローカル・ネットワークにアクセスを試みたときに表示されます。この警告は、お客様の許可がないとお客様のコンピューターから情報が流出しないことを保証するものです。

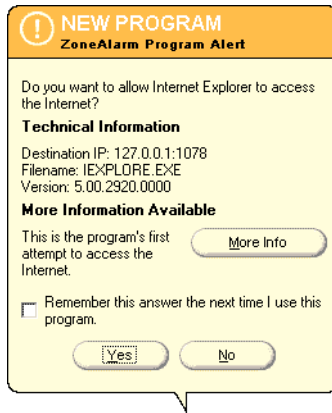
[Remember the answer each time I use this program] チェックボックスをオンにすると、それぞれのプログラムに対して一回質問に答えるだけで済みます。

ZoneAlarm パーソナル・ファイアウォールは、MUVPN クライアントをインストールした後に簡単なチュートリアルを提供します。チュートリアルに従ってこのプログラムの使い方を覚えてください。

ZoneAlarm の性能と設定の詳細情報については、ZoneAlarm のヘルプ・システムを参照してください。ヘルプ・システムにアクセスするには、**[スタート] ⇒ [Programs] ⇒ [Zone Labs] ⇒ [ZoneAlarm Help]** を選択します。

ZoneAlarm を介したトラフィックの許可

アプリケーションが ZoneAlarm パーソナル・ファイアウォールを介したアクセスを必要とする場合は、[New Program] 警告が Windows のデスクトップに表示されます。この警告は、どのプログラムがアクセスを必要としているのかをユーザーに通知するものです。プログラム名はどのアプリケーションがアクセスを必要としているかを明確に示していません。



上記の例では、Internet Explorer ウェブ・ブラウザ・アプリケーションが実行されています。アプリケーションはユーザーのホームページにアクセスしようとします。実際にファイアウォールを通過する必要があるプログラムは、「IEXPLORE.EXE」です。アプリケーションが実行するたびに、このプログラムをインターネットにアクセスさせるには、**[Remember the answer each time I use this program]** チェックボックスをオンにします。アプリケーションを使用したときに ZoneAlarm パーソナル・ファイアウォールを通過する必要があるプログラムの例の一覧を示します。

「必ず許可が必要な」プログラム


MUVPN クライアント	IreIKE.exe MuvpnConnect.exe
MUVPN Connection Monitor	CmonApp.exe
MUVPN Log Viewer	ViewLog.exe

「許可が必要な場合がある」プログラム

MS Outlook	OUTLOOK.exe
MS Internet Explorer	IEXPLORE.exe
Netscape 6.1	netscp6.exe
Opera ウェブ・ブラウザ	Opera.exe
標準 Windows ネットワーク・アプリケーション	lsass.exe services.exe svchost.exe winlogon.exe

ZoneAlarm の終了

Windows のデスクトップのシステム・トレイから：

- 1 右側の ZoneAlarm アイコンを右クリックします。 
- 2 **[Shutdown ZoneAlarm]** を選択します。
[ZoneAlarm] ウィンドウが表示されます。
- 3 **[Yes]** をクリックします。

ZoneAlarm のアンインストール

Windows のデスクトップから：

- 1 **[スタート] ⇒ [Programs] ⇒ [Zone Labs] ⇒ [Uninstall ZoneAlarm]** を選択します。
[Confirm Uninstall] ダイアログ・ボックスが表示されます。

- 2 [Yes] をクリックします。
[ZoneLabs TrueVector service] ダイアログ・ボックスが表示されます。
- 3 [Yes] をクリックします。
[Select Uninstall Method] ウィンドウが表示されます。
- 4 [Automatic] が選択されていることを確認し、[Next] をクリックします。
- 5 [Finish] をクリックします。

注意

[Remove Shared Component] ウィンドウが表示されることがあります。ZoneAlarm の最初のインストールの間、システム上の他のプログラムに共有される可能性のあるファイルがインストールされることがあります。これらのファイルをすべて完全に削除するには、[Yes to All] をクリックします。

- 6 [Install] ウィンドウが表示され、コンピューターをリブートするよう指示されますので、[OK] をクリックしてシステムをリブートします。

トラブルシューティングのヒント

MUVPN クライアントの設定方法についての詳細情報については、以下のウォッチガード社ウェブサイトをご覧ください：

www.watchguard.com/support

以下は MUVPN クライアントに関してよく寄せられる質問に対する回答です。


MUVPN クライアントをインストールした直後にコンピューターが停止してしまいます。

この原因としては以下の問題が挙げられます。

- ZoneAlarm パーソナル・ファイアウォール・アプリケーションがローカル・ネットワーク上の通常のトラフィックを妨げている。
- MUVPN クライアントは有効だが、VPN トンネルが作成できない。

MUVPN クライアントを使用していないときに、ZoneAlarm と MUVPN クライアントの両方を無効にします。

Windows のデスクトップのシステム・トレイから：

- 1 コンピューターをリブートします。
- 2 MUVPN クライアント・アイコンを右クリックし、**[Deactivate Security Policy]** を選択します。
セキュリティ・ポリシーが無効になっていることを示す、赤いバーが付いた MUVPN クライアント・アイコンが表示されます。
- 3 右側に示す ZoneAlarm アイコンを右クリックします。 
- 4 **[Shutdown ZoneAlarm]** を選択します。
[ZoneAlarm] ダイアログ・ボックスが表示されます。
- 5 **[Yes]** をクリックします。

ネットワークに接続していないときでもネットワークのログイン情報を入力しなくてはならないのですが・・・。

コンピューターを起動する際、Windows ネットワークのユーザー名、パスワード、ドメインを入力するよう指示が与えられます。オフィスにいるようなときには、この情報を正確に入力することが非常に重要です。Windows はネットワーク・アダプターやネットワーク・アプリケーションによって情報を記憶します。その後 ISP

に接続したり MUVPN クライアントを実行するときに、コンピューターは記憶された情報を用いて会社のネットワークに接続します。

コンピューターの電源を入れたときに、ユーザー名とパスワードの入力を要求されません。

これはおそらく ZoneAlarm パーソナル・ファイアウォール・アプリケーションに原因があると思われます。このプログラムは非常に高性能なのです。ZoneAlarm は、許可されていない受信・送信トラフィックからお客様のコンピューターを常に保護しています。残念ながら、ネットワーク情報のブロードキャストからコンピューターを阻止してしまうこともあります。これはログイン情報の送信を防ぐ結果となります。MUVPN 接続を切断したときに ZoneAlarm を無効にしているかを確認してください。

MUVPN トンネルが作動しているか分かりません。

アプリケーションが立ち上がると、MUVPN クライアントのアイコンが Windows のデスクトップに表示されます。MUVPN クライアントは、接続されるとキーを表示します。

接続のテストを行うためには、会社のネットワーク上コンピューターに Ping を送信します。

- ・ [スタート] => [Run] を選択し、「ping」と入力して、次にお客様の会社のネットワーク上のコンピューターの IP アドレスを入力します。

マップされたドライブに赤い×印が付けられています。

Windows 98/ME、NT、および 2000 はコンピューターが起動したとき自動的にネットワーク・ドライブを確認し、ドライブのマップを行います。コンピューターを起動しないうちは会社のネットワークとのリモート・セッションを確立することができないため、

このプロセスは失敗します。このためドライブのアイコンに赤い×印が表示されることとなります。この問題を解決するには、MUVPN トンネルを確立してネットワーク・ドライブを開きます。そのドライブの赤い×印は消えるはずですが、

どうやってネットワーク・ドライブをマップすればいいのでしょうか。

Windows の限られたオペレーティング・システムのため、リモートで作業する場合には、マップしたネットワーク・ドライブを再マップする必要があります。ネットワーク・ドライブを再マップするには、Windows のデスクトップから：

- 1 [Network Neighborhood] を右クリックします。
- 2 [Map Network Drive] を選択します。
[Map Network Drive] ウィンドウが表示されます。
- 3 ドロップダウン・リストを使ってドライブ名を選択します。
ドロップダウン・リストからドライブを選択するか、ネットワーク・ドライブ・パスを入力します。
- 4 [OK] をクリックします。

[マイコンピュータ] ウィンドウにマップしたドライブが表示されます。[Reconnect at Logon] チェックボックスをオンにしたとしても、コンピューターがネットワークに直接接続している場合は、マップされたドライブは、次回コンピューターが起動したときにしか表示されません。

会社のネットワークをブラウザーで閲覧している最中にパスワードの入力を要求されることがあります。

Windows のネットワーキング・システムの制限のために、リモート・ユーザー仮想プライベート・ネットワーク製品がアクセス許可することができるネットワーク・ドメインは一つだけです。もし会社のネットワークが、複数のネットワークに接続している場合、ユーザーは自分自身のドメインしか閲覧することができません。

ん。もし他のドメインに接続しようとしても、パスワード入力の指示が表示されるでしょう。残念ながら、正確な情報を入力したとしても、これらの付加的なネットワークにはアクセスすることはできないでしょう。

MUVPN クライアントを使用した後、コンピューターを終了するのに極めて長い時間を要します。

もし MUVPN のセッション中にマップしたドライブにアクセスする場合は、Windows オペレーション・システムは、終了作業が完了する前にネットワークからの応答を待たなければなりません。

自分の ISP への接続が絶たれてしまい、会社のネットワークを使用することができません。

インターネット接続に障害がある場合は、MUVPN トンネルへの接続も絶たれてしまうことがあります。トンネルを閉じるには、関連する設定手順に従ってください。インターネットに再接続します。そして MUVPN クライアントをリブートします。

VPNforce™ アップグレード版により、S6 のオプション・インターフェイスが使用可能になります。オプション・インターフェイスは、S6 アプライアンスには OPT と表示されています。オプション・インターフェイスによって、リモート・ユーザーは、S6 の裏側でオプション・ネットワークと呼ばれる別個のネットワークを使用することができます。オプション・ネットワークにより、企業ネットワークへのセキュアなアクセスが可能となります。トラステッド・ネットワークは中心業務以外の利用に対してのみ用います。

オプション・ネットワークは MUVPN クライアントと併用して企業セキュリティ・ポリシーを実施することができます。

VPNforce を用いた企業ネットワークへの接続

このアップグレード・オプションにより、リモート・ユーザーは、S6 の裏側でオプション・ネットワークと呼ばれる別個のネット

ワークを使用することができます。オプション・ネットワークにより、企業ネットワークへのセキュア・アクセスが可能となります。トラステッド・ネットワークは中心業務以外の利用に対してのみ用います。

注意

このアップグレード版オプションを使用するには、S6 から WatchGuard Firebox アプライアンスあるいは他の IPSec 準拠アプライアンスへの VPN トンネルを経由した企業ネットワークにアクセスする必要があります。VPN アップグレード版オプションに関する詳細は、97 ページの「VPN-Virtual Private Networking (仮想プライベート・ネットワーク)」を参照してください。

オプション・ネットワークの設定

VPNforce アップグレード版により、S6 のオプション・インターフェイスが使用可能になります。このアップグレード版オプションによって、リモート・ユーザーは、S6 の裏側でオプション・ネットワークと呼ばれる別個のネットワークを使用することができます。オプション・ネットワークにより、企業ネットワークへのセキュア・アクセスが可能となります。トラステッド・ネットワークは中心業務以外の利用に対してのみ用います。

S6 にオプション・ネットワークを設定する前に、アップグレード版オプションを有効にしなければなりません。詳細情報については、61 ページの「S6 アップグレード版・オプションの有効化」を参照してください。

このアップグレード版でオプション・インターフェイスを有効にすると、新規のサブネットが定義されます。オプション・インターフェイスに対するサブネットは、トラステッド・ネットワークに対するサブネットとは別個のものです。デフォルトで

は、オプション・インターフェイスに対するサブネットは 192.168.112.0/24 と設定されています。

- 1 ウェブ・ブラウザから、トラステッド・インターフェイスの IP アドレスを使用して [システム・ステータス] ページに進んでください。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーから、[ネットワーク] ⇒ [オプション] を選択します。
[オプション・ネットワークの設定] ページが表示されます。

システム・ステータス	ネットワーク
ネットワーク	オプション・ネットワーク構成
外部	
トラステッド	
オプション (802.11b)	
無線LAN設定	<input checked="" type="checkbox"/> オプション・ネットワークの有効化
ルート	IP アドレス <input type="text"/>
ネットワーク統計	サブネット・マスク <input type="text"/>
ダイナミックDNS	
管理	<input checked="" type="checkbox"/> オプション・ネットワークでDHCPサーバーを有効化
システム・セキュリティ	DHCP サーバーの最初のアドレス <input type="text"/>
VPN Manager アクセス	DHCPサーバーの最後のアドレス <input type="text"/>
更新	WINS サーバー・アドレス <input type="text"/>
アップグレード	DNS サーバー・アドレス <input type="text"/>
設定ファイルの表示	セカンダリDNSサーバー・アドレス <input type="text"/>
ファイアウォール	DNS ドメイン・サフィックス <input type="text"/>
受信	
送信	<input type="checkbox"/> オプション・ネットワークでDHCPリレーを有効化
カスタム・サービス	DHCP リレー・サーバー <input type="text"/>
利用できないサイト	
ファイアウォール・オプション	<input type="checkbox"/> オプション・ネットワークとトラステッド・ネットワーク間のトラフィックを有効化
ログ	<input type="checkbox"/> 現在のインターフェイス上で暗号化 MUVPN 接続を要求
WSEF に対するロギング	
Syslog ロギング	
システム時間	<input type="button" value="サブミット"/> <input type="button" value="リセット"/>

- 3 [オプション・ネットワークの有効化] チェックボックスをオンにします。

- 4 該当するフィールドに、オプション・インターフェイスの IP アドレスおよびサブネット・マスクを入力します。
この値がトラステッド・ネットワークの値と異なっていることを確認してください。
 - 5 DHCP サーバーを設定するには、**[オプション・ネットワーク上での DHCP Server の有効化]** チェックボックスをオンにします。
 - 6 該当するフィールドに、オプション・ネットワークに接続されたコンピューターに DHCP サーバーが割り当てる最初の IP アドレスを入力します。
 - 7 該当するフィールドに、**[WINS サーバー・アドレス]**、**[DNS サーバー・アドレス]**（場合により **[Secondary DNS サーバー・アドレス]** を含む）、そして **[DNS ドメイン・サフィックス]** を入力します。
これらのフィールドは任意です。
 - 8 DHCP 中継サーバーを設定するには、**Enable [DHCP リレイの有効化]** チェックボックスをオンにします。
 - 9 該当するフィールドに DHCP リレイサーバーの IP アドレスを入力します。
 - 10 **[Submit]** をクリックします。
- S6 はすべての DHCP 要求を指定されたリモート DHCP サーバーに送信し、そこで得られた IP アドレスは、オプション・ネットワークに接続されたコンピューターに中継されます。S6 が指定されたリモート DHCP サーバーに 30 秒以内に連絡が取れない場合は、独自の DHCP サーバーに戻り、それを利用してオプション・ネットワーク上のコンピューターに応答します。
- 11 オプション・ネットワークとトラステッド・ネットワークとの間のトラフィックを許可するには、**[オプション・ネット**

ワークとトラステッド・ネットワークとの間のトラフィックを許可する] チェックボックスをオンにします。

このオプションを有効にすると、二つのネットワーク間のセキュリティは解除されます。

12 [現在のインターフェイス上での暗号化 MUVPN 接続の要求]

チェックボックスをオンにします。

13 [Submit] をクリックします。

ページが更新し、S6 をリポートして変更を有効にするよう指示が表示されます。

14 [リポート] をクリックします。

15 ストレート・スルー・イーサネット・ケーブルの一端を S6 上の OPT と表示されたイーサネット・ポートに接続します。もう一端をハブのアップリンク・ポートに接続します。

16 イーサネット・ケーブルをハブのアップリンク・ポートとコンピューターのイーサネット・ポートに接続します。

VPNforce と MUVPN クライアントアップグレード版を用いた企業ポリシーの強化

リモート・ユーザーに MUVPN クライアントを使用して保護されたネットワークに接続するよう要求したい場合は、このセクションの設定手順を実行する必要があります。またこれらの設定手順により、リモート・ユーザーに対し企業セキュリティ・ポリシーを強化することもできます。最初の設定手順では、S6 の設定方法について述べています。二番目は MUVPN の設定方法についてです。

S6 に MUVPN を設定する前に、アップグレード版オプションを有効にしなければなりません。詳細情報については、61 ページの「S6 アップグレード版・オプションの有効化」を参照してください。

S6 の設定

S6 を設定するには以下の手順に従ってください。

- 1 ウェブ・ブラウザから、トラステッド IP アドレスを使用して [システム・ステータス] ページに進んでください。
デフォルトの IP アドレスは `http://192.168.111.1` です。
- 2 左側のナビゲーション・バーから、[VPN] ⇒ [MUVPN クライアント] を選択します。
[MUVPN クライアント] ページが表示されます。



The screenshot shows the MUVPN Client configuration page. The left sidebar contains the following menu items:

- システム・ステータス
- ネットワーク
 - 外部
 - トラステッド
 - オプションル (802.11b)
 - 無線LAN設定
 - ルート
 - ネットワーク統計
 - ダイナミックDNS
- 管理
 - システム・セキュリティ
 - VPN Manager アクセス
 - 更新
 - アップグレード
 - 設定ファイルの表示
 - ファイアウォール
 - 受信
 - 送信
 - カスタム・サービス

The main content area is titled 'VPN' and 'MUVPN クライアント'. It features a table with the following structure:

ユーザー	割り当てるIP

Below the table, there are three buttons: '追加' (Add), '編集' (Edit), and '削除' (Delete).

- 3 [追加] ボタンをクリックします。
[MUVPN クライアントの編集] ページが表示されます。

システム・ステータス
ネットワーク
外部
トラステッド
オプションナル (802.11b)
無線LAN設定
ルート
ネットワーク統計
ダイナミックDNS
管理
システム・セキュリティ
VPN Manager アクセス
更新
アップグレード
設定ファイルの表示
ファイアウォール
送信
送信
カスタム・サービス
利用できないサイト
ファイアウォール・オプション

VPN > MUVPN クライアント
MUVPN クライアントの追加

ユーザー名

共有キー

仮想 IP アドレス

認証アルゴリズム

暗号化アルゴリズム

VPN クライアント・タイプ

WINS サーバー

DNS サーバー

すべてのトラフィックがトンネルを使用 (0.0.0.0/0 IP サブネット)

注: DNS と WINS 設定はすべての MUVPN ユーザに共通です。

サブミット リセット キャンセル

- 4 該当するフィールドに、ユーザー名およびパスフレーズを入力します。
ユーザー名は電子メール・アドレスとして、パスフレーズは MUVPN クライアントの事前共有キーとして使用されます。
- 5 [バーチャル IP アドレス] フィールドに、トラステッド・ネットワークで用いられていない IP アドレスを入力します。これは S6 に接続する際 MUVPN クライアント・コンピューターによって使用されます。
- 6 [認証アルゴリズム] ドロップ・リストから、[MD5-HMAC] を選択します。
- 7 [暗号化アルゴリズム] ドロップ・リストから、[DES-CBC] を選択します。
- 8 [VPN クライアント・タイプ] ドロップ・リストから、[Mobile User] を選択します。
- 9 [All traffic uses tunnel (0.0.0.0/0 Subnet)] チェックボックスをオンにします。

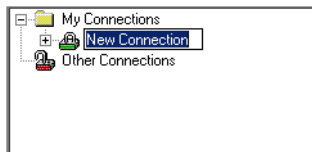
- 10 **[Submit]** をクリックします。
ページが更新し、S6 をリブートして変更を有効にするよう指示が表示されます。
- 11 **[リブート]** をクリックします。
- 12 ストレート・スルー・イーサネット・ケーブルの一端を S6 上の OPT と表示されたイーサネット・ポートに接続します。もう一端をハブのアップリンク・ポートに接続します。
- 13 イーサネット・ケーブルをハブのアップリンク・ポートとコンピューターのイーサネット・ポートに接続します。

MUVPN クライアントの設定

MUVPN クライアントを設定する前に、まずそれをコンピューターにインストールする必要があります。クライアントのインストールについての詳細情報は、129 ページの「MUVPN クライアントのインストールと設定」を参照してください。

MUVPN セキュリティ・ポリシーを構築するには、以下の設定手順に従います：

- 1 MUVPN クライアントのアイコンを右クリックし、**[セキュリティ・ポリシーの編集]** を選択します。
[セキュリティ・ポリシーの編集] ダイアログ・ボックスが表示されます。
- 2 **[編集]** ⇒ **[追加]** ⇒ **[コネクション]** を選択します。
[新規接続] が左側の [ネットワーク・セキュリティ・ポリシー] フィールドに表示され、[コネクション・セキュリティ] と [Remote Party Identity and Addressing] の設定が右側に表示されます。



- 3 新しい接続に対して一意の名前を入力します。
これが特定のユーザーに対する一意のポリシーである場合は、それが認識できるように一意の名前を入力します。例えば、希望に応じてエンド・ユーザーの実際の名前を含めることもできます。
- 4 **[Secure]** オプションを選択します。
これはデフォルト設定です。
- 5 **[手動接続のみ]** を選択します。
- 6 **[ID タイプ]** ドロップ・リストから、**[IP サブネット]** オプションを選択します。
[Remote Party Identity and Addressing] 設定が更新され、適正なフィールドに表示されます。

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 0.0.0.0

Mask: 0.0.0.0

Protocol: All Port: All

Connect using: Secure Gateway Tunnel

ID Type: IP Address

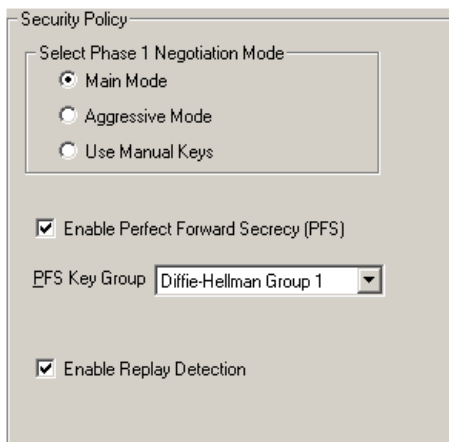
10.168.2.137

- 7 **[サブネット]** および **[マスク]** フィールドの両方に [0.0.0.0] と入力します。
これらはデフォルト値です。
- 8 **[プロトコル]** ドロップ・リストから、**[All]** を選択します。
これはデフォルト設定です。
- 9 **[Connect using]** チェックボックスをオンにし、ドロップ・リストから **[Secure Gateway Tunnel]** を選択します。
- 10 **[ID タイプ]** ドロップ・リストから、**[IP アドレス]** を選択し、該当するフィールドにオプション・インターフェイスの IP アドレスを入力します。

セキュリティ・ポリシー設定の定義

以下の指示に従ってセキュリティ・ポリシー設定を定義してください。

- 1 **[Network Security Policy]** フィールドから、**[Security Policy]** を選択します。
[Security Policy] 設定が右側に表示されます。



- 2 **[Aggressive Mode]** オプションを選択します。
- 3 **[Enable Perfect Forward Secrecy (PFS)]** チェックボックスが選択されていないことを確認します。
- 4 **[Enable Replay Detection]** チェックボックスをオンにします。

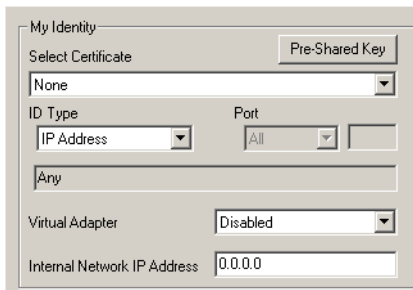
My Identity 設定の定義

以下の指示に従って My Identity の設定を定義してください。

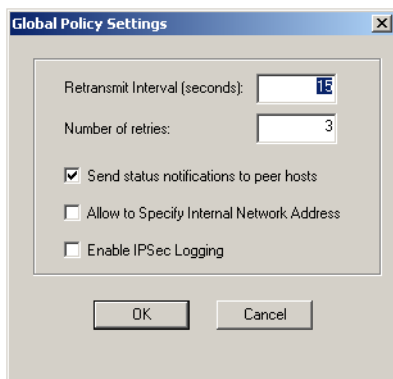
- 1 **[Network Security Policy]** フィールドから、新しいエントリーを展開します。
[My Identity] と [Security Policy] のエントリーが表示されます。



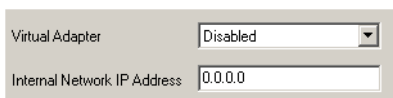
- 2 **[My Identity]** を選択します。
[My Identity] と [Internet Interface] の設定が右側に表示されます。



- 3 **[Options]** ⇒ **[Global Policy Settings]** を選択します。
[Global Policy Settings] ダイアログ・ボックスが表示されます。

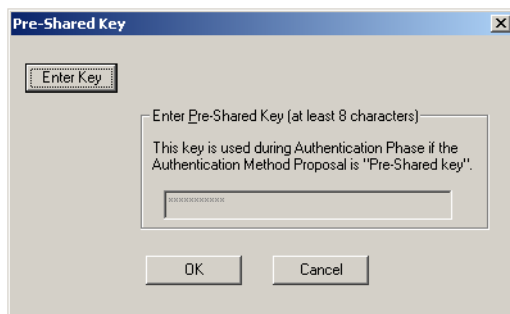


- 4 [Allow to Specify Internal Network Address] チェックボックスをオンにし、[OK] をクリックします。
[My Identity] 設定の中に [Internal Network IP Address] フィールドが表示されます。

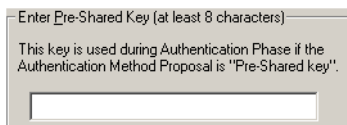


- 5 [Select Certificate] ドロップ・リストから [None] を選択します。
- 6 [ID Type] ドロップ・リストから [E-mail Address] を選択し、該当するフィールドに S6 で定義されたユーザー名を入力します。
- 7 [Virtual Adapter] ドロップ・リストから、[Disabled] を選択します。
- 8 [Internal Network IP Address] フィールドに [0.0.0.0] と入力します。
この値はデフォルトとして表示されます。

- 9 **[Name]** ドロップ・リストから、**[Any]** を選択します。
これはデフォルト設定です。
- 10 **[Pre-Shared Key]** をクリックします。
[Pre-Shared Key] ダイアログ・ボックスが表示されます。



- 11 **[Enter Key]** をクリックします。
テキスト入力フィールドが現れます。



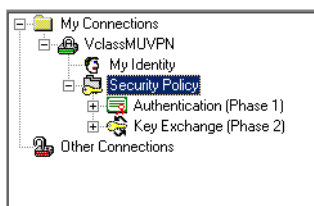
- 12 Firebox S6 アプライアンスに入力した MUVPN クライアントのパスフレーズと全く同じフレーズを入力し、**[OK]** をクリックします。

フェーズ 1 およびフェーズ 2 の設定の定義

フェーズ 1 およびフェーズ 2 の設定を定義するには、以下の指示に従います。その設定が Firebox S6 アプライアンスの設定と全く同じであることを確認してください。

- 1 [Network Security Policy] フィールドから、[Security Policy] を展開します。

フェーズ 1 およびフェーズ 2 両方のネゴシエーションが表示されま
す。

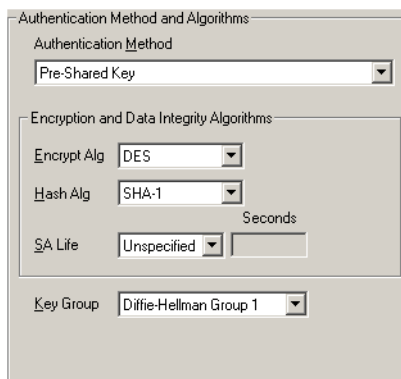


- 2 [Authentication(Phase 1)] を展開します。

[Proposal] エントリーが表示されます。

- 3 [Proposal1] を選択します。

[Authentication Method and Algorithms] の設定が右側に表示され
ます。



- 4 [Authentication Method] ドロップ・リストから [Pre-Shared Key] を選択します。


注意

これらの値は Firebox S6 アプライアンスに入力した値と全く同じでなければなりません。

- 5 [Encrypt Alg] ドロップ・リストから [DES] を、[Hash Alg] ドロップ・リストから [SHA-1] を選択します。
- 6 [SA Life] ドロップ・リストから、[Unspecified] を選択します。
これはデフォルト設定です。
- 7 [Key Group] ドロップ・リストから、[Diffie-Hellman Group 1] を選択します。
- 8 [Key Exchange (Phase 2)] を展開します。
[Proposal] エントリーが表示されます。
- 9 [Proposal1] を選択します。
[IPSec Protocols] 設定が右側に表示されます。

IPSec Protocols

	Seconds	KBytes
SA Life	Unspecified	
Compression	None	
<input checked="" type="checkbox"/> Encapsulation Protocol (ESP)		
Encrypt Alg	DES	
Hash Alg	SHA-1	
Encapsulation	Tunnel	
<input type="checkbox"/> Authentication Protocol (AH)		
Hash Alg	SHA-1	
Encapsulation	Tunnel	

- 10 [SA Life] ドロップ・リストから [Both] を選択し、
[Seconds] のフィールドに [86400]、[Kbytes] のフィールド
に [8192] と入力します。
- 11 [Compression] ドロップ・リストから [None] を選択します。
これはデフォルト設定です。S6 Firebox アプライアンスは圧縮を
サポートしていません。
- 12 [Encapsulation(ESP)] チェックボックスをオンにし、
[Encrypt Alg] および [Hash Alg] ドロップ・リストの値を選
択します。
- 13 [Encrypt Alg] ドロップ・リストから [DES] を、[Hash Alg]
ドロップ・リストから [MD5] を選択します。
- 14 [Encapsulation] ドロップ・リストから [Tunnel] を選択しま
す。
これはデフォルトの設定です。
- 15 [Authentication Protocol(AH)] チェックボックスがオンに
なっていないことを確認してください。
- 16 完了したら、[File] ⇒ [Save] を選択するか、右側のボタ
ンをクリックします。 

MUVPN クライアントを用いたワイヤレス・ネット ワークの保護

VPNForce アップグレード版と MUVPN クライアントは、ワイヤレスの「ドライブ・バイ」ハッキングを防止するためにも使用することができます。この設定には、ワイヤレス・アクセス・ポイント (WAP) から S6 の OPT ポートへのイーサネット接続が必要になります。

以下の指示に従って設定を完了してください。

- 1 DSL/ ケーブル・モデムを WAP の WAN ポートへ接続するイーサネット・ケーブルを確認します。
- 2 このケーブルを WAP の WAN ポートから外します。
- 3 このケーブルを S6 の WAN ポートに接続します。
- 4 ストレート・スルー・イーサネット・ケーブルの一端を S6 の OPT ポートに接続します。
- 5 ストレート・スルー・イーサネット・ケーブルのもう一端を WAP の LAN ポートの一つに接続します。
- 6 WAP をブリッジとして設定します。そのためには、アプライアンスの LAN ポート上の DHCP サーバーを無効化します。詳細については WAP のユーザー・マニュアルを参照してください。
- 7 コンピューターから S6 へイーサネット・ケーブルを接続し、設定ページにアクセスします。
- 8 S6 上で MUVPN クライアントのアップグレードを設定してからコンピューター上に MUVPN クライアントをインストールし、設定します。詳細については、161 ページの「VPNforce と MUVPN クライアントアップグレード版を用いた企業ポリシーの強化」を参照してください。

トラブルシューティングのヒント

S6 のインストールおよび設定の際に問題が生じた場合は、この情報を参照してください。

全般

S6 の PWR、ステータス、モードの各インジケータは何を表しているのですか。

PWR インジケータが点灯していれば、S6 は電源に接続されています。ステータス・インジケータが点灯していれば、S6 の管理用接続が存在する状態です。モード・インジケータが点灯していれば、S6 が稼動している状態です。

PWR インジケータが点滅している場合は、次の状態を意味します。

S6 がバックアップ用フラッシュ・メモリーから起動しています。4 つのイーサネット・ポート (0 ~ 3 のいずれか) のひ

とつに接続されたコンピューターから S6 に接続し、S6 の設定ができます。

モード・インジケーターが点滅している場合は、次の状態を意味します。

S6 を外部ネットワークに接続することができません。この問題の原因としては、以下のことが考えられます。

- S6 が DHCP サーバーから外部インターフェイスへの IP アドレスを受信していなかった。
- WAN ポートが他のアプライアンスに接続されていない。
- 外部インターフェイスへの接続が不良である。
- S6 の外部インターフェイスが接続されているアプライアンスが正常に作動していない。

S6 を LiveSecurity サービスに登録する方法を教えてください。

30 ページの「S6 および LiveSecurity サービスの登録」を参照してください。

S6 のリブートの手順を教えてください。

31 ページの「S6 のリブート」を参照してください。

システム・セキュリティ・パスワードを忘れてしまった場合、それを再設定するにはどうすればよいのでしょうか。

29 ページの「S6 のデフォルト出荷設定へのリセット」を参照してください。

S6 の接続数制限はどのようになっているのでしょうか

21 ページの「S6 を 5 台以上の機器と接続する場合の配線」を参照してください。

S6 の Feature Key とは何ですか。

61 ページの「S6 アップグレード版・オプションの有効化」を参照してください。

DSL モデムを扱うために必要な S6 の機能が使えません。

一部の DSL ルーターは、ネットワーク・アドレス変換 (NAT) ファイアウォールを実行しています。NAT を供給するアプライアンスを通した外部ネットワーク接続を行うと、WebBlocker の動作に問題が生じるだけでなく、IPSec のパフォーマンスも低下します。S6 が DSL ルーターを通して外部ネットワークに接続する場合は、DSL ルーターの機能をブリッジ専用に設定してください。

Macintosh(およびその他の) オペレーティング・システム上で S6 をインストールおよび設定するにはどうすればよいでしょうか。

Macintosh およびその他のオペレーティング・システム向けのインストール手順については、ウォッチガード社のウェブサイトを参照してください。

<https://support.watchguard.com/sohoresources/>

ケーブルが S6 に正しく接続されているかどうかを確認するにはどうすればよいでしょうか。

S6 の前面には、14 個のインジケータがあります。WAN というラベルのついたインジケータは、S6 がモデムに接続されているかどうかを通知します。このインジケータが消灯している場合、S6 はモデムに接続されていません。

- ケーブルが S6 からモデムに接続されていることを確認してください。
- インターネット接続が利用可能になっていることを確認してください。

0～3のラベルのついたリンク・インジケータは、トラステッド・ネットワークの4つのイーサーネット・ポートに対応しています。これらのインジケータにより、S6がコンピューターあるいはハブに接続されているかどうかわかります。これらのインジケータが消灯している場合、S6はコンピューターまたはハブに接続されていません。ケーブルが接続されているかどうか、またはコンピューターあるいはハブが電源に接続されているかどうか確認してください。

設定画面には接続できるのに、インターネットをブラウズできないのはなぜですか。

設定ページには接続できるのにインターネットには接続できない場合は、S6からインターネットへの接続に問題があります。

- ・ ケーブル・モデムあるいはDLSモデムがS6および電源に接続されていることを確認してください。
- ・ モデムのリンクライトおよびS6のWANインジケータが点灯していることを確認してください。

それでも問題が解決できない場合は、ご利用のISPに問い合わせてください。

S6のMACアドレスを確認したいのですが。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークのIPアドレスを入力し、S6の[システム・ステータス]ページに接続します。
デフォルトのIPアドレスは、<http://192.168.111.1>です。
- 2 [システム・ステータス] ページの下部右側に、外部ネットワークの欄があります。一つ以上のMACアドレスが表示されています。
これらのアドレスを記録してから、テクニカル・サポートにお問い合わせください。

設定

S6 の設定はどこに格納されるのですか。

設定パラメータは S6 のメモリーに格納されます。

S6 のトラステッド・ネットワーク上で DHCP を設定するにはどうすればよいですか。

- 1 コンピューターが DHCP を使用できる設定になっていることを確認してください。詳細情報については、16 ページの「コンピューターの DHCP 設定の有効化」を参照してください。
- 2 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 3 左側のナビゲーション・バーで、
[ネットワーク] ⇒ [トラステッド] をクリックします。
- 4 [DHCP サーバーの有効化] チェックボックスをオフにします。
- 5 [Submit] をクリックします。

トラステッド IP アドレスを静的アドレスに変更する方法を教えてください。

静的 IP アドレスを使用するには、トラステッド・ネットワークのネットワーク IP 範囲とサブネットマスクを選択します。

RFC 1918 により、次の IP 範囲とサブネット・マスクがプライベート・ネットワーク用に予約されています。ネットワーク IP アドレスの X の部分には、1 ~ 254 の数字が入ります。サブネット・アドレスを変更する必要はありません。

ネットワーク IP アドレスの範囲	サブネット・マスク
10.x.x.x	255.0.0.0

172.16.x.x	255.240.0.0
192.168.x.x	255.255.0.0

トラステッド IP アドレスを静的アドレスに変更するには、次の手順に従います。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーで、
[ネットワーク] ⇒ [トラステッド] をクリックします。
- 3 [DHCP サーバーの有効化] チェックボックスをオンにします。
- 4 [Submit] をクリックします。
- 5 該当するフィールドに情報を入力します。
- 6 [Submit] をクリックします。

WebBlocker の設定方法および無効にする方法を教えてください。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーで、
[WebBlocker] ⇒ [設定] をクリックします。
[WebBlocker の設定] ページが表示されます。
- 3 [WebBlocker 有効化] チェックボックスをオンにします。
- 4 [フルアクセス・パスワード] フィールドに、パスワードを入力します。

- 5 該当するフィールドに無効化タイムアウトの時間(分単位)を入力します。

WebBlocker を無効化するには、[WebBlocker 有効化] チェックボックスをオフにします。

POP3、Telnet、Web (HTTP) のような受信サービスを許可する方法を教えてください。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルト IP アドレスは、http://192.168.111.1 です。
- 2 左側のナビゲーション・バーで、
[ファイアウォール] ⇒ [受信] をクリックします。
[受信トラフィックのフィルタリング] ページが表示されます。
- 3 許可する設定済みサービスを指定します。
- 4 ドロップダウン・リストから、[許可] を選択します。
- 5 許可するサービスを稼動するコンピューターのトラステッド・ネットワーク IP アドレスを入力します。
- 6 [Submit] をクリックします。

受信 IP トラフィックや、あまり一般的ではない TCP および UDP プロトコルを許可するにはどうすればよいですか。

データを受信するコンピューターの IP アドレス、および新規の IP プロトコル番号を記録します。次の手順に従ってください。

- 1 ブラウザー・ウィンドウにトラステッド・ネットワークの IP アドレスを入力し、S6 の [システム・ステータス] ページに接続します。
デフォルトの IP アドレスは、http://192.168.111.1 です。

- 2 左側のナビゲーション・バーで、
[ファイアウォール] ⇒ [カスタム・サービス] をクリックします。
[カスタム・サービス] ページが開きます。
- 3 [プロトコル設定] フィールドの下にあるドロップダウン・リストから [TCP ポート]、[UDP ポート]、または [プロトコル] を選択します。
[カスタム・サービス] ページが更新されます。
- 4 [サービス] フィールドにサービス名を入力します。
- 5 [プロトコル] フィールドに新規のプロトコル番号を入力します。
- 6 [Submit] をクリックします。
- 7 左側のナビゲーション・バーで、
[ファイアウォール] ⇒ [受信] をクリックします。
[ファイアウォール受信トラフィック] ページが表示されます。
- 8 ページ下部にある [カスタム・サービス] の一覧から新規のサービスを選択し、ドロップダウン・リストから [許可] を選択します。
- 9 [サービス・ホスト] フィールドに、流入データを受信するコンピューターの IP アドレスを入力します。
- 10 [Submit] をクリックします。

VPN 管理

- 97 ページの「VPN の構築に必要なもの」を参照してください。
二つのアプライアンスが同じ暗号化と認証の方法を使用していることを確認してください。

VPN Manager Access のための S6 の設定方法を教えてください。

これにはアドオン製品である WatchGuard VPN Manager が必要です。VPN Manager を別途購入し、WatchGuard Firebox System ソフトウェアと連動させて使用してください。以下のウォッチガード社ウェブサイト参照して、VPN Manager を購入してください。

<https://www.watchguard.com/products/vpnmanager.asp>

VPN Manager を使用して S6 を管理する方法の詳細については、*VPN Guide* を参照してください。

S6 間で VPN を設定する方法を教えてください。

S6 と別の IPSec 対応アプライアンスとの間に VPN トンネルを構成する方法の詳細については、以下のウォッチガード社ウェブサイト参照してください。

https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

- 1 上記サイトにログインします。
- 2 必要なファイルをダウンロードします。
- 3 指示に従って、VPN トンネルを設定します。

テクニカル・サポート窓口

(877) 232-3531	米国エンドユーザー向けサポート窓口
(206) 521-8375	米国正規代理店サポート窓口
(360) 482-1083	米国外向けサポート窓口

オンライン・ドキュメントと FAQ

PDF 形式の文書、チュートリアル、FAQ については以下のウォッチガード社ウェブサイトを参照してください。

<https://support.watchguard.com/AdvancedFaqs/>

特別の注意

ウォッチガード社ウェブサイトでは、オンラインのヘルプ・システムはまだ利用できません。[システム・ステータス] ページのトップの **[Help]** リンクをクリックしてウォッチガード社製品の資料ページに接続すると、より多くの情報源にリンクすることができます。

索引

数字

100 インジケーター 8

D

DHCP
トラステッド・ネットワーク上
でのセットアップ 179
DHCP (動的ホスト・コンフィギュ
レーション・プロトコル)
説明 34
DNS サービス、動的 44
DSL モデム、および S6 177
Dual ISP Port 46

F

File and Printer Sharing for
Microsoft Networks
および Windows XP 127
FTP アクセス、トラステッド・ネッ
トワークへの拒否 72

H

HTTP プロキシ設定の無効化 15

I

Internet Protocol (TCP/IP) ネット
ワーク・コンポーネント
および Windows XP 127
IP アドレス
偽装 6
説明 5

動的 33
ネットワーク上 33
保守テーブル 99

L

LiveSecurity サービス
サブスクリプションの更新 63
登録 30

M

MUVPN クライアント・オプション 107
MUVPN、ライセンス・キー 63

N

NAT 6

O

OPT ポート 8

P

ping パケット、すべて拒否 72
PPPoE
設定 36
説明 34
PWR インジケーター 175
PWR ライト 7

S

- S6 31, 32
 - MAC アドレス 178
 - MUVPN クライアント・オプション 107
 - PPPoE の設定 36
 - S6 のデフォルト出荷設定へのリセット 29
 - VPN トンネルの設定 105
 - アクセスの設定 53
 - インストールする 11-23
 - および DSL モデム 177
 - および Macintosh オペレーティング・システム 177
 - および SOCKS 73
 - 間の VPN の設定 183
 - 正面外観 7
 - 静的アドレスを使う場合の設定 35
 - 接続する 25
 - 説明 2
 - デフォルト出荷設定 27
 - 登録 30
 - 動的アドレスを使う場合の設定 34
 - ハードウェア 6
 - パッケージ内容 3
 - ポート 7, 8
 - 裏面外観 8
 - ログ・メッセージの表示 80
- S6 の MAC アドレス 178
- S6 の管理ページ 53
- S6 のデフォルト出荷設定へのリセット 29
- S6 リモート管理 55
- SOCKS
 - S6 のための設定 73
 - アプリケーションの設定 73
 - 説明 73
 - 無効化 74
- Syslog ログイン・ページ 83

T

- TCP/IP 設定情報の決定 12-14

V

- VPN
 - S6 を用いた設定 105
 - 暗号化 106
 - および S6、S6-VPN 2
 - 接続のトラブルシューティング 109
 - 説明 97
 - 統計の表示 108
 - と静的 IP アドレス 108
 - トンネルの有効化 110
 - 必要なもの 97
 - 二つの S6 間 183
 - 要注意点 105
 - ライセンス・キー 63
- VPNforce Port 49
- VPN Manager
 - S6 の設定 183
 - アクセスの設定 57-59
 - 購入 183
 - 説明 57
- VPN Manager アクセスページ 58
- VPN アップグレード版
 - 取得 109
 - ページ 108
- VPN アップグレード版
 - 使用可能 [VPN あつぷぐれえどばんしょうかのう] 100
- 108

W

- WAN インジケーター 8
- WAN ポート 9
- WatchGuard Security Event Processor 81

WatchGuard Security Event Processor ページ 81
 WebBlocker
 カテゴリ 93-96
 購入と有効化 89
 設定 89
 説明 87
 データベース 87
 有効化 89
 有効化と無効化 180
 ユーザーとグループ 88
 ユーザーとグループの作成 91
 WebBlocker アップグレード版、購入 89
 WebBlocker グループ・ページ 91
 WebBlocker の設定ページ 90
 WebBlocker、ライセンス・キー 63
 Windows XP
 File and Printer Sharing for Microsoft Networks のインストール 127
 WSEP 81

あ

アップグレード版
 VPN 63
 シート・ライセンス 21
 アップグレード版・ライセンス・キー
 タイプ 62
 アップグレード・ページ 61
 アプライアンス
 定飲された 19
 イーサネット上でのポイント・ツー・ポイント・プロトコル。
 PPPoE を参照のこと。
 イベント
 説明 79
 インジケーター
 100 8
 PWR 175
 WAN 8
 ステータス 175, 176
 モード 8, 175

リンク 7
 インストール
 TCP/IP 設定情報の決定 12
 TCP/IP プロキシ設定の無効化 15
 配線 19
 インターネット
 情報の流れ 4
 ブラウザの問題 178
 Windows XP
 Internet Protocol (TCP/IP) ネットワーク・コンポーネントのインストール 127
 Macintosh オペレーティング・システム 177

か

カスタム・サービス・ページ 68, 182
 カスタム受信サービス、作成 68
 外部ネットワーク
 受信した ping パケットの拒否 72
 グループ・ページ 92
 ケーブル
 正しいセットアップ 177
 パッケージ内容 3
 更新ウィザード 60
 更新ページ 59
 コンフィギュレーション・ファイルの表示 64
 コンフィギュレーション・ファイル、表示 26

さ

サービス
 カスタム受信を作成 68
 カスタムの作成 68-69
 受信許可 181
 説明 6, 65
 サービス、標準サービスを追加 66

サイト
遮断 70
シート制限 21
シート・ライセンス、アップグレード版 62
システム時間、設定 84
システム時間ページ 84
システム・ステータス 81
システム・ステータス・ページ 80, 101, 108, 112
システム・ステータス・ページ 25, 32, 35, 36, 38, 41, 42, 44, 45, 48, 50, 54, 57, 58, 59, 61, 64, 66, 68, 71, 76, 83, 84, 89, 91, 106, 178, 179, 180, 181
システム・セキュリティ・ページ 53, 54
システム要件 114
遮断されたサイト設定 70
遮断されたサイトページ 70
シリアル番号、表示 26
新規ユーザー・ページ 93
時間、設定 84
受信サービス、カスタムの作成 68
ステータス・インジケータ 176
ステータス・インジケータ 175
ステータス・ライト 7
静的 IP アドレス
取得 108
と VPN 108
静的 IP アドレス割り当て、設定 35
静的ルート
設定 41

た

ダイナミック DNS クライアントページ 45
ダイナミック DNS サービス、設定 44-46
デフォルト出荷設定 27-28
電源コネクタ 9
登録 30

トラステッド・ネットワーク
FTP アクセスの拒否 72
トラステッド・ネットワーク
追加されたコンピューターの設定 40
トラステッド・ネットワーク構成ページ 41, 38
トラフィック
すべての送信のログ出力 75
無制限パス・スルーの作成 76
トラフィックのフィルタリングページ 66
動的 IP アドレス
設定 34
説明 33
動的ホスト・コンフィギュレーション・プロトコル。DHCP を参照のこと。34

な

ネットワーク・アドレス交換 (NAT) 6
ネットワーク統計、表示 43
ネットワーク統計ページ 44

は

ハードウェア概要 6
番号付きポート 9
パスフレーズ 54
説明 54
ファームウェア
更新 59
バージョンの表示 26
ファイアウォール・オプション・ページ 71
ファイアウォール受信トラフィック・ページ 182
分割トンネリング 106
プロトコル
受信許可 181
説明 5

ページ

S6 の管理 53
 Syslog ログイン 83
 VPN Manager アクセス 58
 VPN 統計 108
 WatchGuard Security Event Processor 81
 WebBlocker グループ 91
 WebBlocker の設定 90
 アップグレード 61
 カスタム・サービス 68, 182
 グループ 92
 更新 59
 コンフィギュレーション・ファイルの表示 64
 システム・ステータス 38
 システム時間 84
 システム・ステータス 112
 システム・ステータス 25, 32, 35, 36, 41, 42, 44, 45, 48, 50, 54, 57, 58, 59, 61, 64, 66, 68, 71, 76, 80, 81, 83, 84, 89, 91, 101, 106, 108, 178, 179, 180, 181
 システム・セキュリティ 53, 54
 遮断されたサイト 70
 新規ユーザー 93
 ダイナミック DNS クライアント 45
 トラフィックのフィルタリング 66
 ネットワーク統計 44
 ファイアウォール・オプション 71
 ファイアウォール受信トラフィック 182
 無制限パス・スルー IP アドレス 76
 ルート 42, 48, 50
 ルートの追加 42
 ログイン 80
 ボタン、リセット 8
 ポート
 OPT 8
 WAN 9
 トラステッド・ネットワーク 9
 番号 5
 番号付き 9

ま

無制限パス・スルー IP アドレス・ページ 76
 モード・インジケータ 8, 175

ら

ライセンス・キー 28, 30
 ライト
 100 8
 WAN 8
 ステータス 7
 電源 7
 モード 8
 リンク 7
 リセット・ボタン 8
 リポート 31
 リモート管理 55
 リモート・システム上のリポート 32
 リンク・インジケータ 7
 ルート、静的ルートの設定 41
 ルートの追加ページ 42
 ルート・ページ 42, 48, 50
 ログイン
 WSEP ホストへ 81
 シスログ (Syslog) ホストへ 83
 ログイン・ページ 80
 ログ・ホスト、WSEP の設定 81
 ログ・メッセージ
 内容 80
 表示 80

わ

テクニカル・サポート 184
 トラブルシューティング 175-184
 パス・スルー機能 77