HITACHI
Inspire the Next

ファイアウォールログ解析ソフトウェア

FIREWALLstaff

取扱説明書（インストール編）

株式会社 日立ソリューションズ

■ 対象製品

FIREWALLstaff 02-08

■ 輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。

なお，ご不明な場合は，弊社または弊社販売店の担当窓口へお問い合わせください。

■ 商標類

- Word，Windows，Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Microsoft は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。
- NETSCREEN，JUNIPER NETWORKS はそれぞれジュニパーネットワークス社の登録商標です。
- FORTIGATE はフォーティネット社の登録商標です。
- PALO ALTO NETWORKS はパロアルトネットワークス社の商標です。
- チェック・ポイント，VPN-1 UTM は，Check Point Software Technologies Ltd.およびその関連会社の商標，又は登録商標です。
- IPCOM は，富士通株式会社の登録商標です。
- Cisco，Cisco Systems，および Cisco Systems ロゴは，米国 Cisco Systems，Inc. の米国および他の国々における登録商標です。
- FIREWALLstaff は，株式会社日立ソリューションズの登録商標です。
- その他，本マニュアル記載の会社名，製品名は，それぞれの会社の商号，登録商標または商品名称です。

■ 発行

2021 年 12 月

はじめに

このマニュアルは，FIREWALLstaff のインストール手順について説明したものです。

■ 対象読者

FIREWALLstaff を運用，管理するシステム管理者を対象としています。

このマニュアルの記述は，次の事項を前提にしています。

- Windows の基本操作を習得している。
- コンピュータの管理者として必要な知識がある。
- ネットワークに関する基本的な知識がある。

■ 画面操作説明で使う表記

画面操作説明で使う表記を次に示します。

記号	意味
［ ］	ボタンやテキストボックスなど，画面に表示されている要素を示します。
［ ］－［ ］	画面に表示されるメニューやアイコンなどを選択する操作を示します。

■ 常用漢字以外の漢字の使用について

このマニュアルでは常用漢字を使用することを基本としていますが，次に示す用語については常用漢字以外の漢字を使用しています。

鍵（かぎ）　個所（かしょ）　必須（ひっす）

■ MB（メガバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイトです。

目次

1 FIREWALLstaff の動作環境

1.1 FIREWALLstaff の動作要件

FIREWALLstaff が動作する上で以下の要件を満たす必要があります。

1.1.1 ハードウェア要件

項番	カテゴリ	内容
1	導入機種	「1.1.2 ソフトウェア要件」に示す OS が動作する PC/AT 互換機であること。x64 Edition では，x64 プロセッサであること。
2	CPU	以下のスペックを満たしていること。 インテル(R) Core(TM) i5 2.6GHz 以上
3	メモリ容量	2GB 以上の容量を持つこと。
4	HDD 容量	NTFS 形式で，100GB 以上の空き容量を持つこと。

1.1.2 ソフトウェア要件

項番	カテゴリ	内容
1	OS	以下のいずれかの日本語版 OS が正しく稼動すること。 Windows Server 2012 Windows Server 2012 R2 Windows 8.1 Windows 10 Windows Server 2016 Windows Server 2019
2	ソフトウェア	以下のソフトウェアのいずれかが正しく稼動すること。 Microsoft .NET Framework 4.5.1～4.8

1.1.3 Windows 環境の要件

項番	カテゴリ	内容
1	Windows 環境	Windows の設定において，下記の設定で運用すること。 • 固定 IP アドレス（IPv4）を設定していること • [ハードディスクの電源を切る]設定としないこと • [システムスタンバイ]状態となる設定としないこと • [休止状態]となる設定としないこと • [カスタムテキストサイズの設定（DPI）]は 100%（「小」）であること • 画面解像度が 1024×768 以上のディスプレイであること

1.1.4 ネットワーク環境の要件

項番	カテゴリ	内容
1	ネットワーク	以下のネットワーク環境で運用すること。 • ファイアウォールを導入した，セキュアな内部ネットワークであること • ファイアウォールの外部も内部も，IPv4 ネットワークであること • メール送信する場合は，FIREWALLstaff をインストールしたコンピュータからメールサーバに TCP/IP でアクセスできること
2	メールサーバ	メールサーバの認証方式は，以下のいずれかであること。 • SMTP 認証（但し，認証方式は PLAIN，LOGIN，CRAM-MD5 のいずれかであること） • 認証なし

1.2 レポート閲覧の要件

FIREWALLstaff が生成した Word レポートを閲覧するためには，閲覧するコンピュータに以下のいずれかのソフトウェアがインストールされている必要があります。

項番	ソフトウェア
1	Microsoft Office Word 2013 Microsoft Office Word 2016 Microsoft Office Word 2019 Microsoft 365(デスクトップ版)

1.3 サポートファイアウォール

FIREWALLstaff でサポートしているファイアウォールは，下記のとおりです。

項番	ファイアウォール	OS/ファームウェア
1	Juniper NetScreen/SSG シリーズ	Juniper NetScreen シリーズ，Juniper SSG シリーズのファイアウォールで，OS が ScreenOS5.4～ScreenOS6.3 のいずれかであるファイアウォール
2	Fortinet FortiGate シリーズ	FortiGate シリーズのファイアウォールで，OS が FortiOS4.0MR3～FortiOS 6.4.6 のいずれかであるファイアウォール
3	Palo Alto PA シリーズ	Palo Alto PA シリーズのファイアウォールで，OS が PANOS3.1.x～PANOS9.1.x のいずれかであるファイアウォール
4	Juniper SRX シリーズ	Juniper SRX シリーズのファイアウォールで，OS が JUNOS10.0～JUNOS 20.4R3 のいずれかであるファイアウォール
5	CheckPoint シリーズ	CheckPoint Software Blade のファイアウォール。対応範囲は R70～R81
6	IPCOM EX IN/SC シリーズ	IPCOM EX IN/SC シリーズのファイアウォールで，OS が E10L50～E20L31 のいずれかであるファイアウォール
7	Cisco ASA シリーズ	OS のバージョンが 7.2～9.1 のいずれかであるファイアウォール

注 意

Fortinet FortiGate シリーズにて，FortiOS 5.6.0 のログを解析する場合は，以下の変更を行ってください。

1. FIREWALLstaff のデータフォルダ（詳細は「2.1.1 フォルダの決定」を参照）内に作成される「logjudgewords.xml」をメモ帳などのテキストエディタで開きます。

   ※ デフォルトのパスは以下になります。

   C:¥HitachiSolutions¥FIREWALLstaff¥Data¥system¥logjudgewords.xml

   ※ 「logjudgewords.xml」はレポートを生成すると自動的に作成されます。存在しない場合は，FIREWALLstaff AE Server メイン画面を起動し，[手動生成レポート]グループボックス内の[レポート生成]ボタンを押して，レポートを生成してください。

2. 以下のように，「FORTIGATE56_IS_APP_DENY」タグ内の値を「false」から「true」へ変更し，保存してください。

   【変更前】

   <FORTIGATE56_IS_APP_DENY>false</FORTIGATE56_IS_APP_DENY>

   【変更後】

   <FORTIGATE56_IS_APP_DENY>true</FORTIGATE56_IS_APP_DENY>

2 FIREWALLstaff のインストール

2.1 新規インストール

FIREWALLstaff を，新規にインストールする手順を説明します。

2.1.1 フォルダの決定

FIREWALLstaff をインストールするインストールフォルダと，FIREWALLstaff がデータを保存するデータフォルダを，決定してください。

表 2.1-1 FIREWALLstaff のフォルダ

項番	フォルダ種類	用途
1	インストールフォルダ	・FIREWALLstaff プログラムをインストールするフォルダ ・1GB 以上の空き容量が必要です ・デフォルトは， C:¥Program Files¥HitachiSolutions¥FIREWALLstaff です
2	データフォルダ	・FIREWALLstaff がデータを保存するフォルダ ・保存するログの容量＋30GB 以上，の空き容量が必要です ・デフォルトは， C:¥HitachiSolutions¥FIREWALLstaff¥Data です

注 意

データフォルダのパスには，半角英数字のみを使用してください。

2.1.2 新規インストール

注 意

コンピュータに **Administrator 権限を持つユーザでログオン**してください。

注 意

コンピュータに以下のいずれか**がインストールされていること**を確認してください。

Microsoft .Net Framework 4.5.1～4.8

(1) インストーラの実行

インストール CD-ROM を CD-ROM ドライブに挿入します。表 2.1-2 に従って，適切なインストーラを実行します。ユーザーアカウント制御のダイアログが出た場合は[はい]を選択してください。

表 2.1-2 実行するインストーラ

OS のビット	実行するインストーラ
32 ビット OS	CD-ROM ドライブ¥Installer¥x86¥setup_x86.exe
64 ビット OS	CD-ROM ドライブ¥Installer¥x64¥setup_x64.exe

(2) セットアップの開始

このウィンドウはセットアップ（インストール）手順を紹介し，いくつかの情報を提供します。

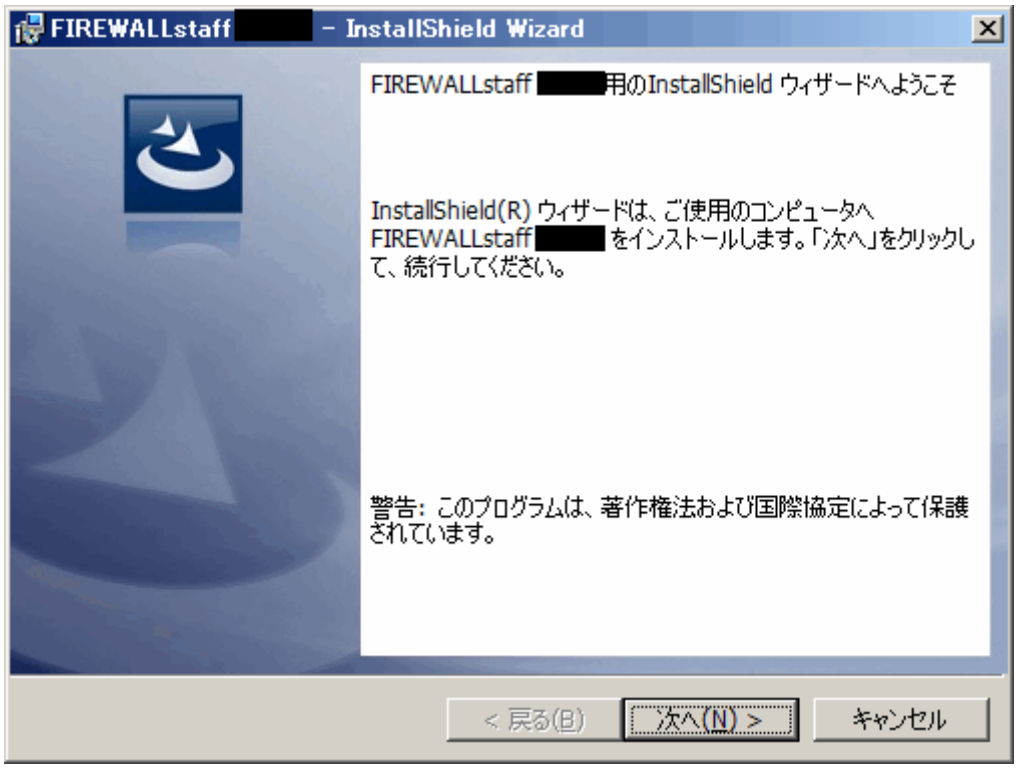


図 1 セットアップの開始

ボタンのいずれかを選択してください。

［次へ］　［使用許諾契約］ウィンドウに進み，インストールを継続します

［キャンセル］　［セットアップの中止］ウィンドウに進み，インストールを取り消します

(3) 使用許諾契約

使用許諾契約書を注意深くお読みください。

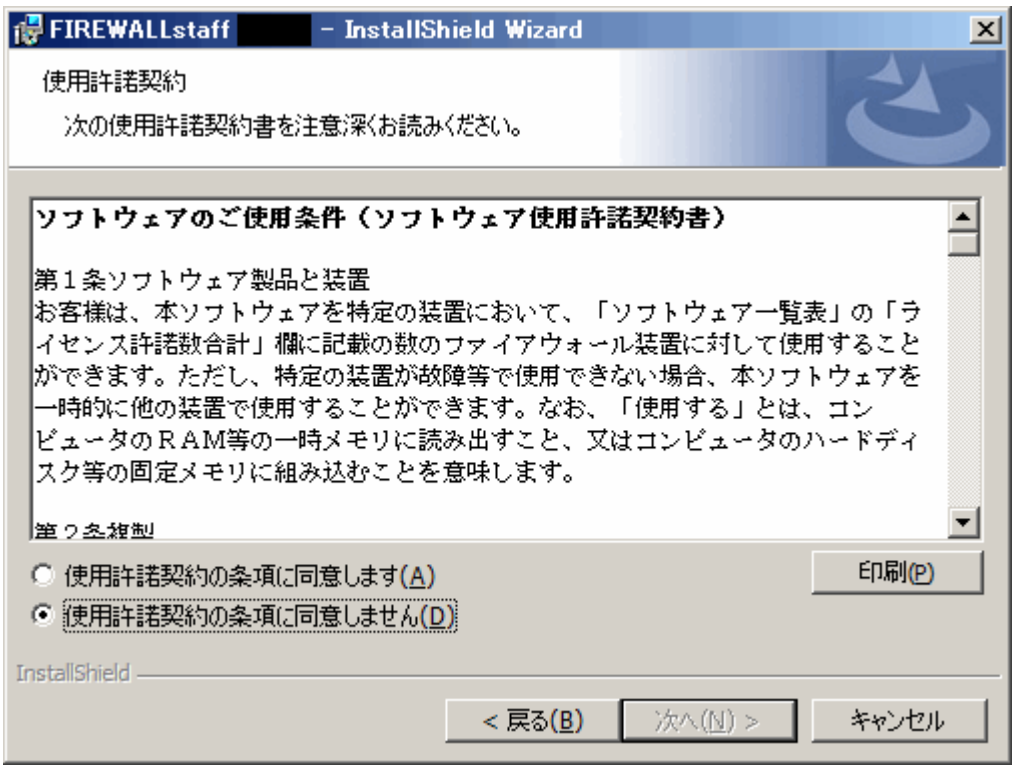


図 2 使用許諾契約

使用許諾契約の条項に同意する場合は[使用許諾契約の条項に同意します]ラジオボタンを選択してください。

[次へ]　　[インストール先のフォルダ]ウィンドウに進み，インストールを継続します

[キャンセル]　　[セットアップの中止]ウィンドウに進み，インストールを取り消します

(4) インストール先のフォルダ

このウィンドウでは，FIREWALLstaff をインストールするフォルダを選択します。

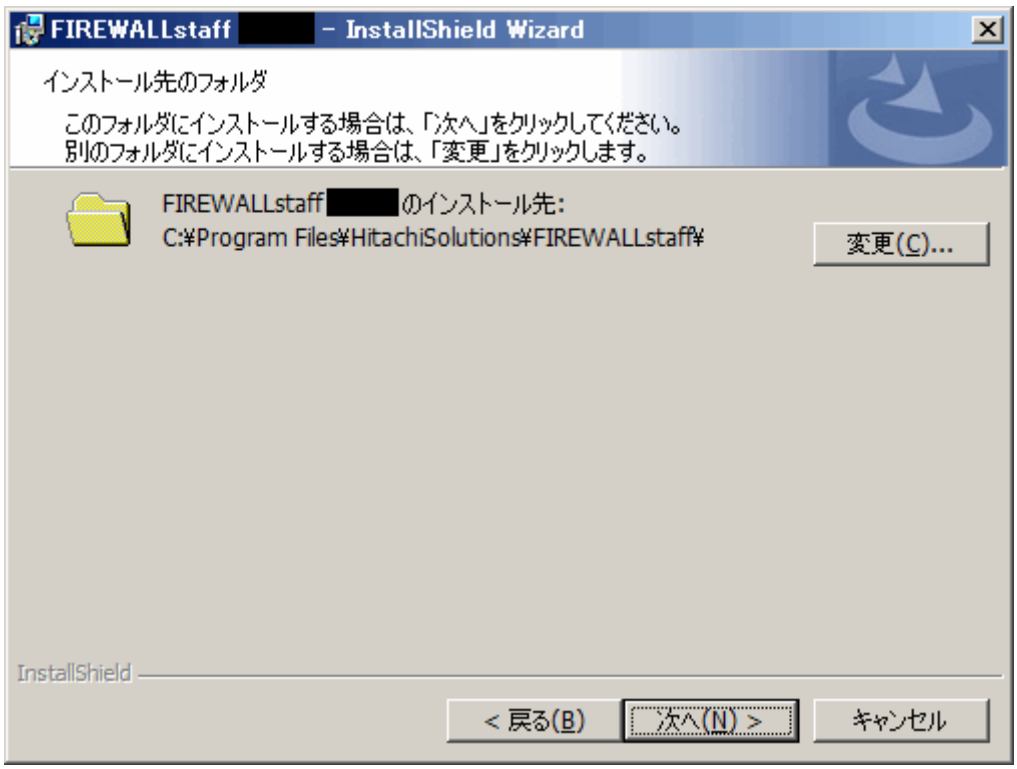


図 3 インストール先のフォルダ

ボタンのいずれかを選択してください。

［変更］	［ディレクトリの選択］ウィンドウに進み，インストール・プログラムが選択するフォルダ以外のフォルダを選択することができます
［戻る］	直前のウィンドウに戻ります
［次へ］	［データフォルダの指定］のウィンドウに進みます
［キャンセル］	［セットアップの中止］ウィンドウに進み，インストールを取り消します

(5) データフォルダの指定

このウィンドウでは，FIREWALLstaff が使用するデータフォルダを選択します。データフォルダには空のフォルダを指定してください。

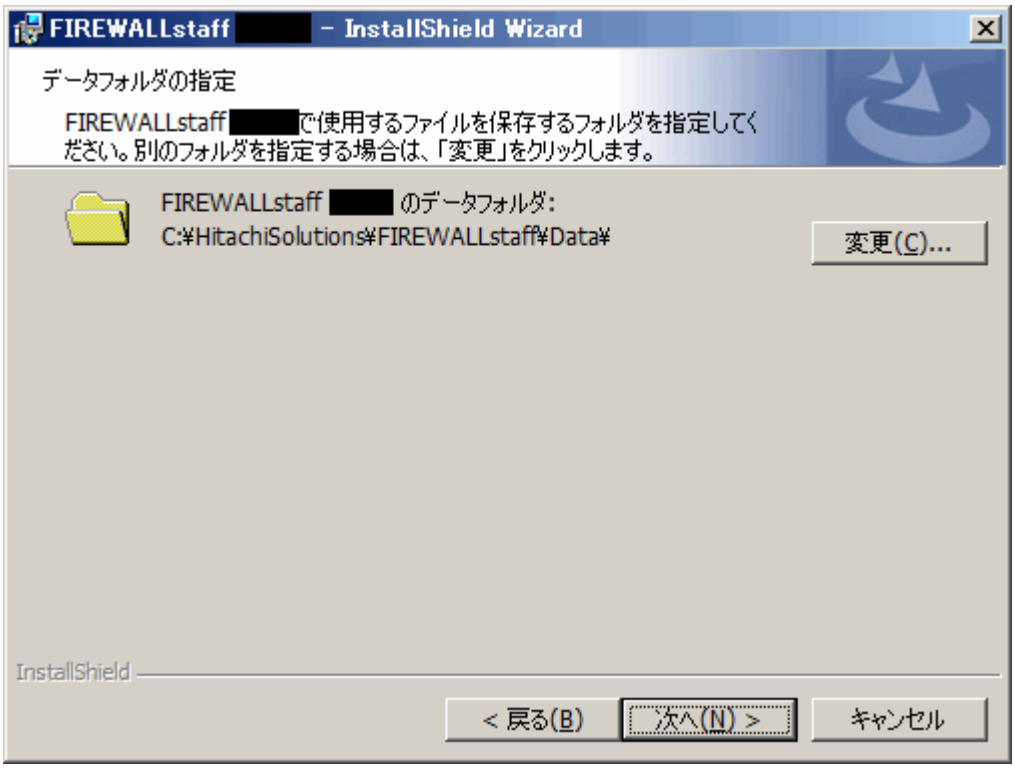


図 4 データフォルダの指定

ボタンのいずれかを選択してください。

[変更]	[ディレクトリの選択]ウィンドウに進み，インストール・プログラムが選択するフォルダ以外のフォルダを選択することができます
[戻る]	直前のウィンドウに戻ります
[次へ]	[プログラムをインストールする準備ができました]のウィンドウに進みます
[キャンセル]	[セットアップの中止]ウィンドウに進み，インストールを取り消します

注 意

データフォルダのパスには，半角英数字のみを使用してください。

(6) プログラムをインストールする準備ができました

FIREWALLstaff をインストールする準備ができました。

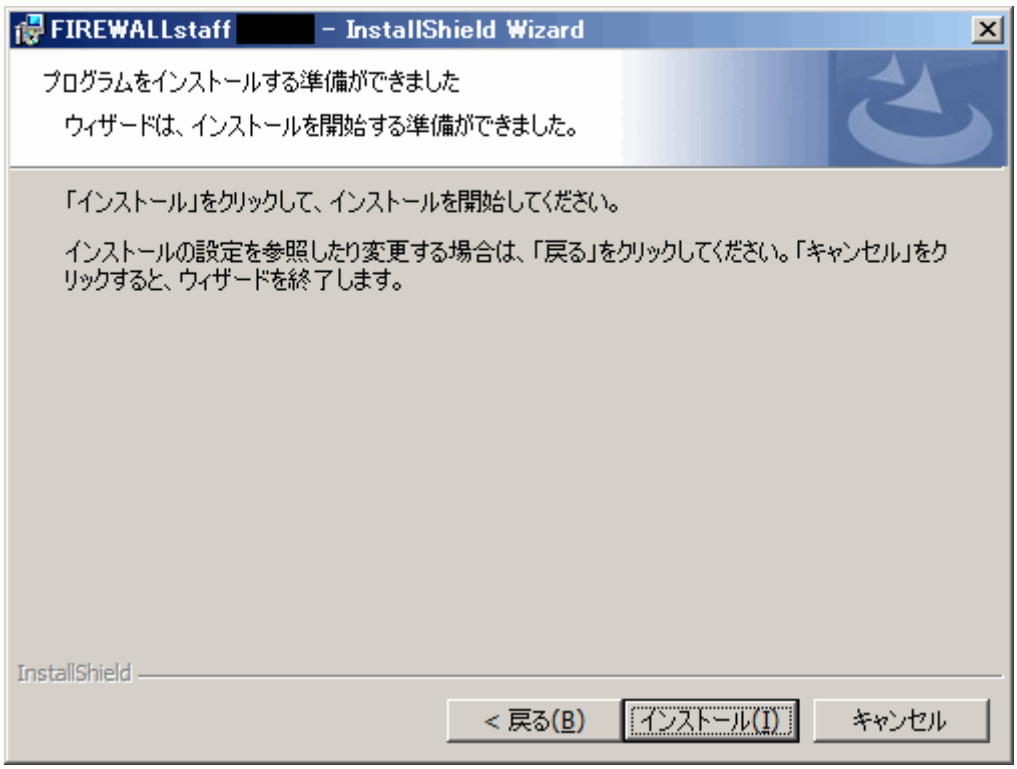


図 5 プログラムをインストールする準備ができました

ボタンのいずれかを選択してください。

[戻る]	直前のウィンドウに戻ります
[インストール]	インストールを開始します
[キャンセル]	[セットアップの中止]ウィンドウに進み，インストールを取り消します

(7) インストールステータス

インストールを開始すると，以下のようなウィンドウが表示されます。

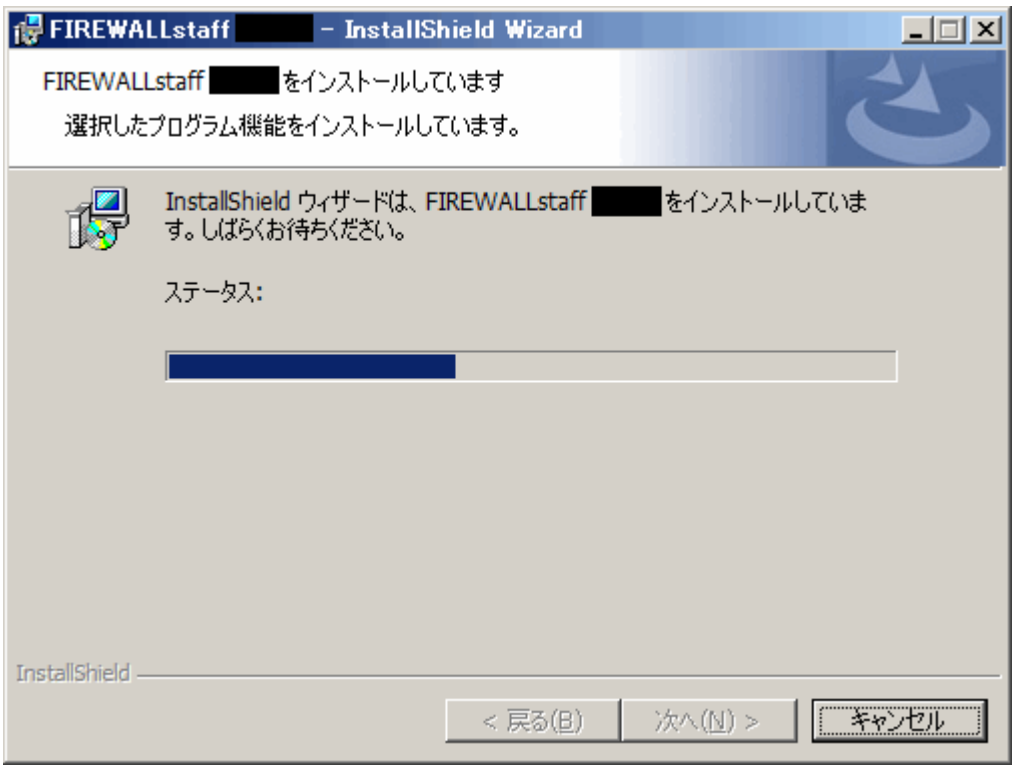


図 6 インストールステータス

(8) セットアップの終了

セットアップが終了すると，以下のようなウィンドウが表示されます。[完了]をクリックして，セットアップ（インストール）を終了してください。

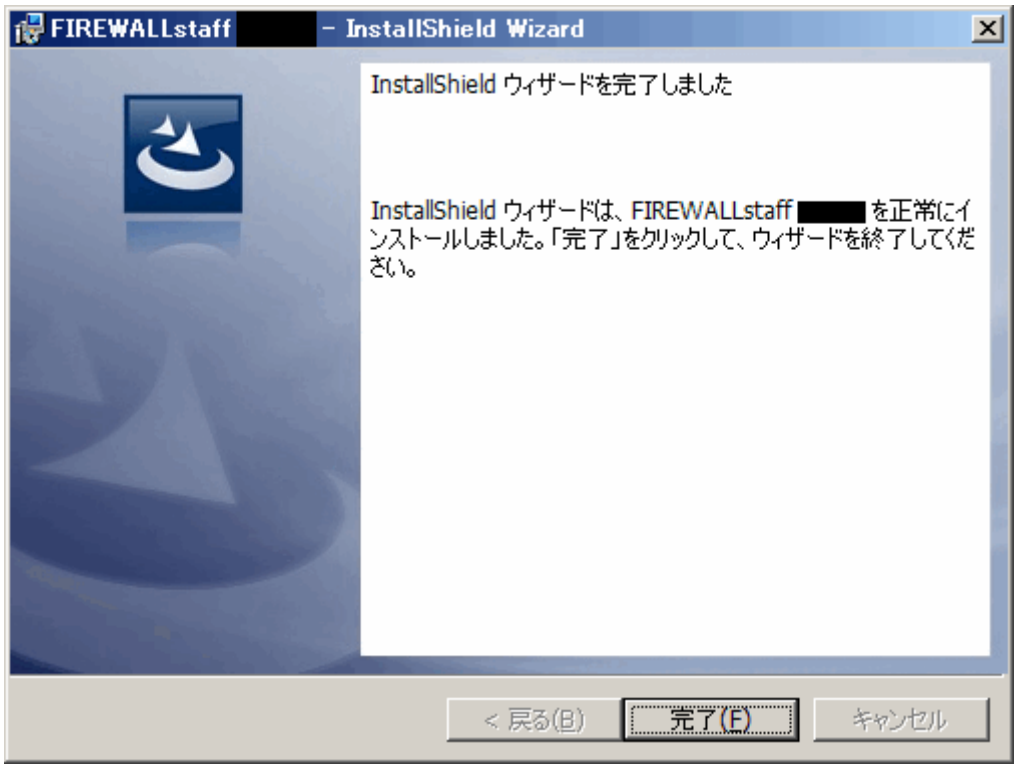


図 7 セットアップの終了

(9) Windows ファイアウォールの設定

FIREWALLstaff の Log サービスで Syslog を受信する場合，Windows ファイアウォールが有効になっていると Syslog を受信できません。その際は以下のように例外設定を行ってください。

1. ［コントロールパネル]－[システムとセキュリティ]－[Windows ファイアウォール]から Windows ファイアウォールウィンドウを開きます。
2. 左ペイン内の「詳細設定」を選択します。
3. [セキュリティが強化された Windows ファイアウォール]ウィンドウの左ペイン内の「受信の規則」を選択します。
4. 同ウィンドウ右ペイン内の「新しい規則...」を選択します。
5. [新規の受信の規則ウイザード]が表示されるので，以下を指定してください。

   規則の種類：プログラム

   プログラム：

   　このプログラムのパス：

   　　<FIREWALLstaff インストールフォルダ>¥fstaff_syslog.exe

   操作：

   　接続を許可する

   プロファイル：

   　ドメイン，プライベート，パブリックをチェック（デフォルト）

   名前：

   　名前：FIREWALLstaff Log

2.1.3 ライセンスキーのインストール

(1) FIREWALLstaff ライセンスキーのインストール

[ヘルプ]－[ライセンス]で，[ライセンス]ダイアログを起動します。

[ライセンス設定]－[ライセンスキー]に「FIREWALLstaff 対象 FW 単一構成ライセンス」または「FIREWALLstaff 対象 FW 冗長構成ライセンス」を入力して，[インストール]ボタンをクリックしてください。最後に，[OK]ボタンでダイアログを閉じてください。

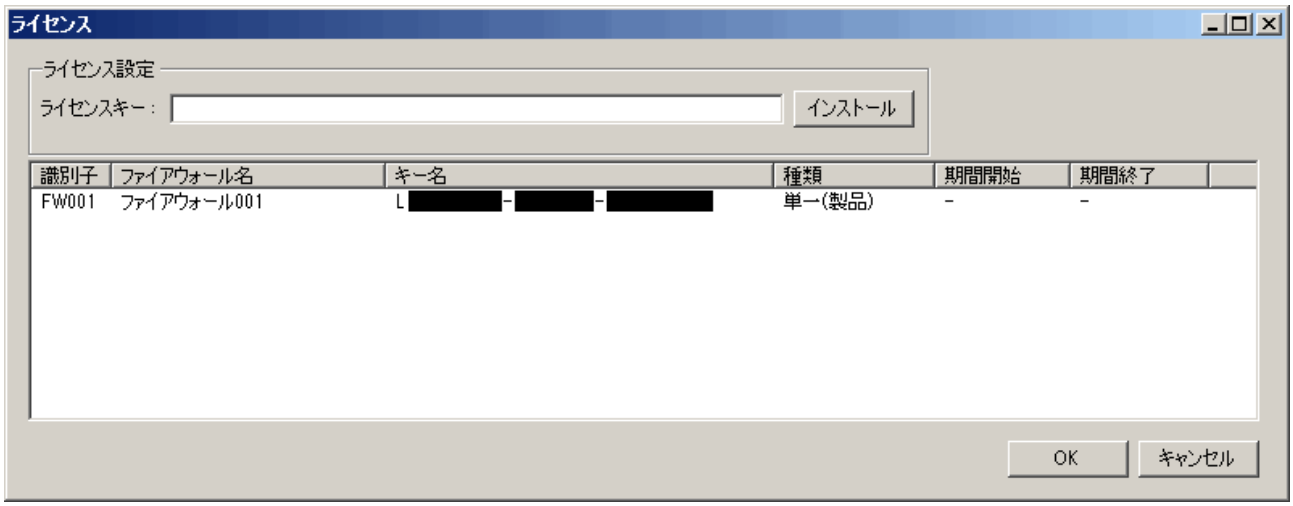


図 8 ライセンスインストール画面

インストールした順番に，[識別子]に FW001，FW002，FW003，・・・の順で上から自動採番されます。インストール後に順番を変更することはできませんので，特に，異なるファイアウォール種類のキー，異なる構成のキーをインストールする場合は注意してください。

2.2 バージョンアップインストール

FIREWALLstaff をバージョンアップインストールする手順を説明します。

注 意

コンピュータに **Administrator 権限を持つユーザでログオン**してください。

注 意

コンピュータに以下のいずれかがインストールされていることを確認してください。

Microsoft .Net Framework 4.5.1～4.8

(1) FIREWALLstaff 関連サービスの全停止

Windows の[コントロールパネル]から，[管理ツール]－[サービス]を開きます。次のサービスを停止してください。

- FIREWALLstaff Monitor
- FIREWALLstaff Scheduler
- FIREWALLstaff Log (01-02 以前は，FIREWALLstaff Syslog)

(2) FIREWALLstaff 画面を閉じる

開いている FIREWALLstaff の画面を閉じてください。

(3) インストーラの実行

インストール CD-ROM を CD-ROM ドライブに挿入します。表 2.2-1 に従って，適切なインストーラを実行します。ユーザーアカウント制御のダイアログが出た場合は[はい]を選択してください。

表 2.2-1 実行するインストーラ

OS のビット	実行するインストーラ
32 ビット OS	CD-ROM ドライブ¥Installer¥x86¥setup_x86.exe
64 ビット OS	CD-ROM ドライブ¥Installer¥x64¥setup_x64.exe

(4) セットアップの確認

バージョンアップを行うかどうか確認します（ダイアログに表示されるバージョンは，バージョンアップ前のバージョンです）。

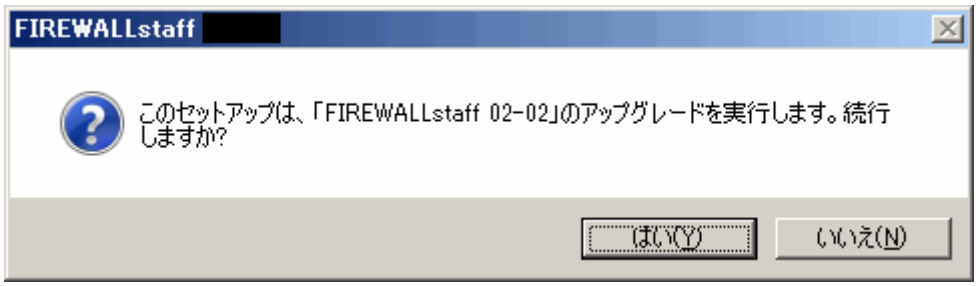


図 9 セットアップの確認

ボタンのいずれかを選択してください。

［はい］　　［セットアップの開始］ウィンドウに進み，バージョンアップを継続します

［いいえ］　　バージョンアップを取り消します

(5) セットアップの開始

このウィンドウはセットアップ（バージョンアップ）手順を紹介し，いくつかの情報を提供します。

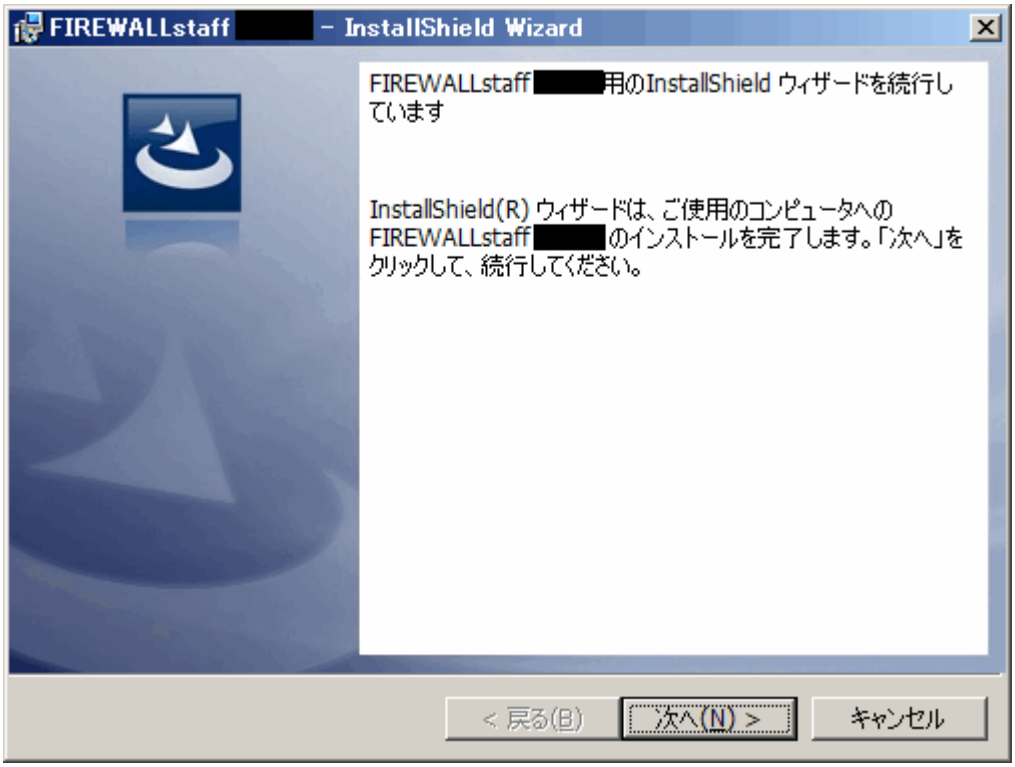


図 10 セットアップの開始

ボタンのいずれかを選択してください。

［次へ］　　バージョンアップを継続します

［キャンセル］　　［セットアップの中止］ウィンドウに進み，バージョンアップを取り消します

(6) インストールステータス

バージョンアップを開始すると，以下のようなウィンドウが表示されます。

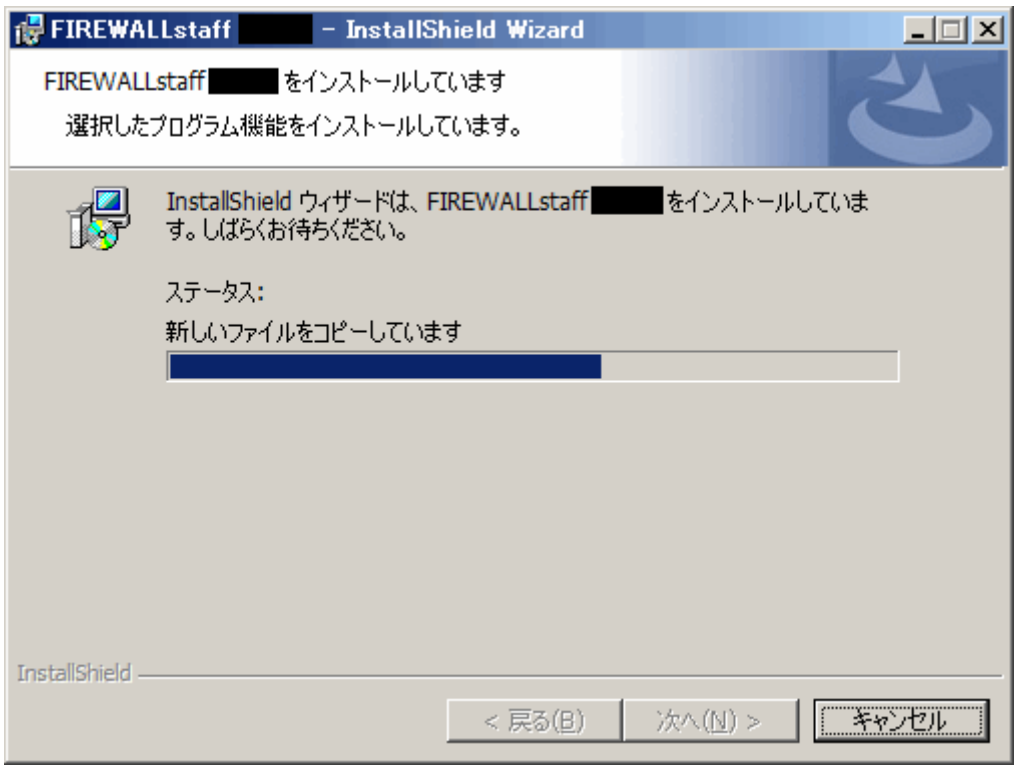


図 11 インストールステータス

(7) セットアップの終了

セットアップが終了すると，以下のようなウィンドウが表示されます。[完了]をクリックして，セットアップ（バージョンアップ）を終了してください。

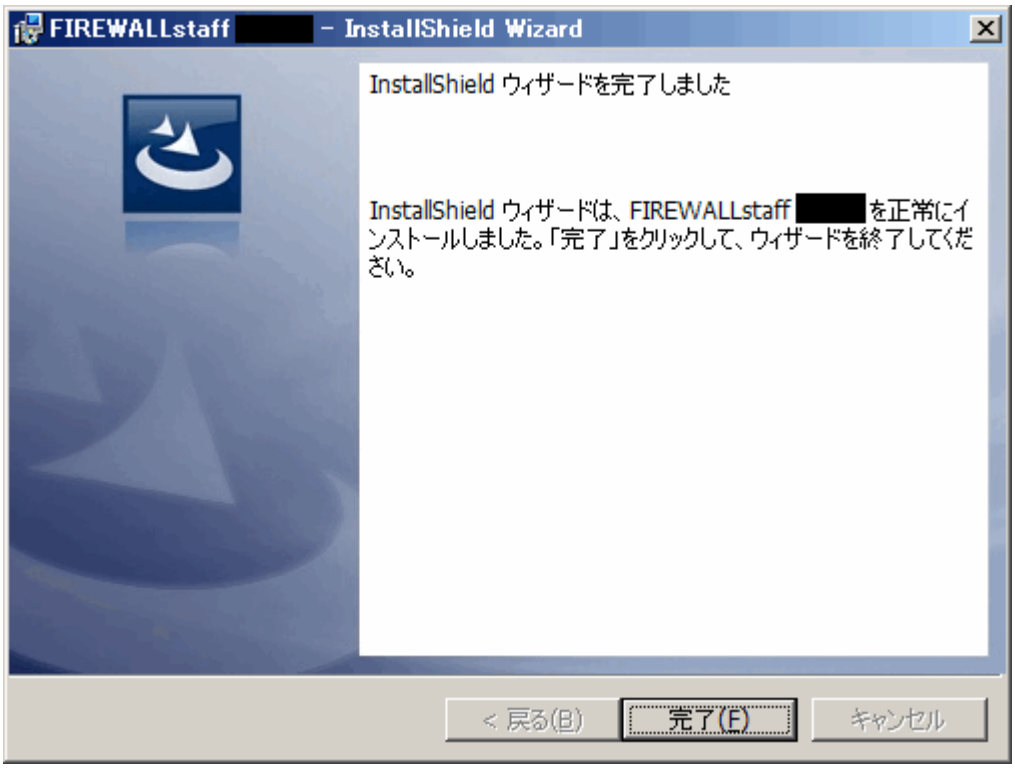
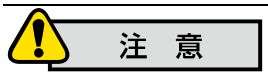


図 12 セットアップの終了

2.3 アンインストール

FIREWALLstaff をアンインストールする手順を説明します。



コンピュータに **Administrator 権限を持つユーザでログオン**してください。

(1) FIREWALLstaff 関連サービスの全停止

Windows の[コントロールパネル]から，[管理ツール]－[サービス]を開きます。次のサービスを停止してください。

- FIREWALLstaff Log
- FIREWALLstaff Monitor
- FIREWALLstaff Scheduler

(2) FIREWALLstaff 画面を閉じる

開いている FIREWALLstaff の画面を閉じてください。

(3) アンインストールの実施

Windows の[コントロールパネル]から[プログラムの追加と削除]（または[プログラムと機能]）を開きます。「FIREWALLstaff 02-08」を選択し，[削除]（または[アンインストール]）ボタンをクリックしてプログラムを削除します。

- 不明な発行元の確認ダイアログが出た場合は，「はい」を選択してください。
- アンインストール実行中に「データフォルダ以下のすべてのファイルを削除しますか？」ダイアログが表示された場合は，適切な選択を行ってください。

プログラムの削除後も，FIREWALLstaff フォルダが残る場合があります。この場合，手動で FIREWALLstaff フォルダを削除してください。

日立ソリューションズ
http://www.hitachi-solutions.co.jp/