

# インターネット経由のファイル転送： その危険性と対応策

## 目次

概要 .....	1
FTP の問題 .....	1
FTP に代わるデータ交換手段に 必要な 10 の要素 .....	1
安全なデータ交換の 5 つの事例 .....	3
事例 1: 金融サービス会社 .....	3
事例 2: IT 企業 .....	3
事例 3: 医療機関 .....	3
事例 4: 製造会社 .....	4
事例 5: 給与計算および健康保険 業務にサービスプロバイダを 使用する企業 .....	4
<b>AttachmateWRQ:</b> 転送データの保護 .....	4
SSH のファイル転送機能 .....	4
SSL/TLS のファイル転送機能 .....	5
AttachmateWRQ セキュリティ ソリューション .....	5
<b>SSH と SSL/TLS:</b> 最も安全な選択肢 .....	6
AttachmateWRQ について .....	6

## 概要

情報共有の需要が高まる中、ファイル交換をすばやく簡単に適切なコストで行うことを望む企業は、その手段としてインターネットを選択するようになってきました。多くの企業では現在、ファイル転送プロトコル (FTP) を使用して公共のインターネット経由で機密情報をやり取りしています。しかし、FTP には看過できない重大なセキュリティリスクが存在するのをご存知でしょうか？

この白書では、FTP の問題を取り上げ、FTP に代わるデータ交換手段に必要な 10 の要素について概要を説明します。また、SSH プロトコルと SSL/TLS プロトコルに準拠した製品を使用して信頼性の高いファイル転送セキュリティを適切なコストで確保している 5 つの事例を紹介します。最後に、AttachmateWRQ のファイル転送ソリューションで転送データの相互運用性、機密性、整合性を維持する方法について説明します。

## FTP の問題

情報の共有において、インターネットのスピード、使いやすさ、コストは魅力的です。会社は、使い勝手のよい設計済みの通信基盤を持っているようなものです。そこで、ファイル転送の方法として FTP がよく使用されるようになってきました。

FTP は規格に準拠したプロトコルなので、高い相互運用性があります。また、高速で使い方も簡単です。このため、大企業、中小企業、官公庁、非営利団体など、あらゆる業界で多くの組織に使用されるようになりました。

しかし、FTP はその性質上 1 つの問題を抱えています。FTP は保護されておらず、危険にさらされているのです。FTP 経由で転送される情報は通常のテキスト形式でネットワークに送信されるため、スニッファを使用すれば誰でも読み取ることができます。さらに、FTP サーバへのログオン時に使用したユーザ名とパスワードも、保護されていない通常のテキスト形式で送信され、悪意のある人間にちょっとした技術で簡単に知られてしまう可能性があります。このようなセキュリティの欠如は、機密データの保護を目的とした厳重な規制で管理されている組織にとってはきわめて危険です。

## FTP に代わるデータ交換手段に必要な 10 の要素

FTP に代わる理想的なデータ交換手段とは、このプロトコルの長所であるスピード、使いやすさ、相互運用性を維持しつつ、しかも公共のインターネット通信に必要なセキュリティを確保するものでしょう。このような特性が備わっていれば、専用回線と付加価値通信網の使用料を必要とするため費用のかかる従来の電子データ取引 (EDI) から簡単に交換することができます。また、ファイル転送方法としてやはりよく使用される安全な電子メールを増強することもできますが、添付ファイルのサイズに限度があります。

FTP に代わるデータ交換手段に必要な 10 の要素は、以下のとおりです。

### 1. 業界標準のクライアント接続

取引先やお客様のクライアント接続用ソフトウェアを管理することはできないため、業界標準のプロトコルに準拠した簡単に使用できるセキュリティソリューションを選択する必要があります。これによって、データ交換が簡単になり、コストを下げることができます。また、別の方法でのファイル転送を許可する必要もあります。場合によっては、オンデマンドシンクライアントを使用したブラウザ接続が必要になります。その他の場合には、自動化をスクリプト記述できるコマンドラインクライアントが必要になります。または、ファイル転送をユーザが簡単に実行できるグラフィカルユーザインタフェースを備えた Windows クライアントを選択することもできます。

### 2. データの機密性

インターネットは公共のネットワークであるため、機密データはスクランブル処理して転送中に読み取られないようにする必要があります。そのためには、標準的な暗号化方式 SSL (Secure Sockets Layer)、SSL の新しいバージョンである TLS (Transport Layer Security)、あるいは SSH (Secure Shell) などを使用します。これらのプロトコルにはそれぞれ、異なる暗号レベルを持つさまざまな標準暗号化方式が用意されています。

**3. データの整合性**

悪意のある人間がデータを改ざんして利益を得ることがあります。例えば、口座の残高や注文書の金額が変更される場合などです。クライアントからサーバに送信する時またはサーバからサーバに送信する時に何も変更されないようにするには、ある種のメッセージ認証コードを使用する必要があります。このコードは、メッセージの信頼性を確保する役割も果たします。さらに、接続が切断されて中断した転送がその時点から自動的に再開されるように設定する必要もあります。

**4. 認証**

安全なセッションを開始するには、ユーザが本人確認を行うことができ、指定のサーバへの接続権を確立できる必要があります。また、正しいサーバに接続していることを確認する必要もあります。この双方向認証を安全に行うために、強力な認証方式を使用するか、ユーザ名 / パスワード暗号化を使用します。確固とした認証方式がない場合は、盗聴、ソーシャルエンジニアリング、パスワード推測などによって、侵入者に個人ファイルやシステムへのアクセス権を簡単に入手されてしまいます。

**5. 自動化**

組織では、日常的なファイル転送を自動化して時間と費用を節約することがよくあります。例えば、事務処理業務をバッチ処理で広範囲に行っている大手企業の場合、事務処理システムの負荷が軽い時に複数のファイルをバッチ転送できます。こうしたジョブは、スケジュール設定され、通常はスクリプトを使用して実行されます。この時、安全な方法でデータをアップロードするスクリプトを選択することが重要です。

**6. アクセス権の制御**

多くの組織では、ユーザに内部ネットワーク上の特定ディレクトリへのアクセス権のみを付与する必要があります。この場合、ユーザとアクセス権の定義は必須です。また、ファイアウォールで開いているポートの数を制限して、悪意のあるトラフィックが通過する機会を最低限に抑える必要もあります。

**7. 監査**

クライアントまたはサーバに侵入され、データが不正に抽出された場合は、詳しく調べる必要があります。送受信通信を記録することで、疑わしい使用パターン、不注意によるアクセスまたは見落とされたアクセス、有害または意図的な攻撃を監査ツールを使用して識別できます。明らかな侵入形態の検出にも、わかりにくい侵入形態の検出にも欠かせないこれらのツールは、セキュリティソリューションの重要な一部です。

**8. 集中管理**

まったく新しい対象ユーザがますます必要とする情報の需要を満たすには、ファイル転送プロセスのクライアント側の集中管理が不可欠です。これは実際、急速に変化する最近の構成および展開要件に対応する唯一の効果的な方法です。

**9. 混在環境への対応**

お客様や取引先が異なるプラットフォームを使用していれば、異種環境になる場合があります。このため、安全なファイル転送ソリューションはクロスプラットフォームに対応しているのが理想的です。

**10. エンドツーエンドセキュリティ**

インターネットを経由してファイルを安全に転送することと、そのファイルを安全に終点（更新対象のサーバ）に届けることは別です。金融詐欺の大半は、安全なネットワークへの外部からの侵入よりも、内部でのハッキングが原因です。このため、非武装地帯 (DMZ) からバックオフィスまでの最後の区間が重要です。こうした内部犯罪を防ぐには、エンドツーエンドセキュリティが必要です。

以上の点を熟慮して、データ交換に最も安全と思われるソリューションを選択し、時間と費用を長期的に節約できます。

## 安全なデータ交換の 5 つの事例

組織によって、安全なデータ交換のニーズは異なります。以下の 5 つの事例では、規格に準拠した安全なファイル転送により、転送データを保護する低コストで信頼性の高い方法をどのように実現するのかについて説明します。

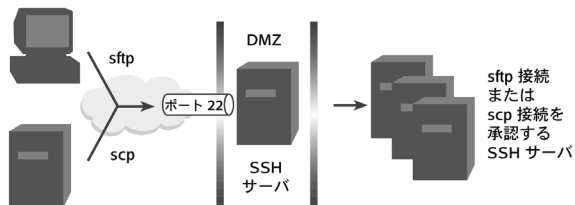
### 事例 1: 金融サービス会社

この事例では、金融サービス業で口座の振り替え、貸借取引の実施、小切手画像の送信が必要な場合を取り上げます。

この企業のセキュリティソリューションは、SSH ファイル転送プロトコル (sftp) と安全なコピー (scp) という、SSH プロトコルの一部である 2 つの安全なファイル転送方式を非武装地帯のゲートウェイホストまたは要塞ホストで実行するように構成されています。この構成では、外部ネットワークと内部ネットワークの間でアプリケーションレベルの制限付きアクセスを許可します。

sftp 転送は対話型です。scp 転送は自動化されているので、ユーザの操作は必要ありません。認証は、ホストベースで行われるか、エージェント転送付きの公開鍵を使用して行われます (ゲートウェイホストを使用する別の方法では、プロキシコマンド機能を使用して sftp セッションをゲートウェイからバックオフィスサーバまでトンネリングします)。ファイアウォールで SSH ポート 22 のみを開けば、これらの転送を通過させることができます。

金融情報を送信する取引先

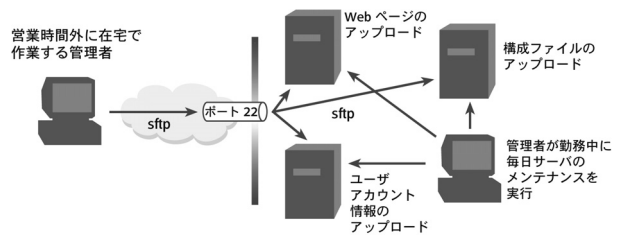


事例 1: 金融情報を送信する取引先

### 事例 2: IT 企業

この事例では、構成ファイルの転送、ユーザアカウントの変更、使用記録の監視、Web ページの新規作成を行う必要があるシステム管理者を取り上げます。

管理者は、サーバへのルートアクセス権があり、インターネット経由での作業が多いので、自分のユーザ名とパスワードを保護する必要があります。FTP を sftp に代えることにより、管理者のユーザ名とパスワードを送信時に確実に暗号化できるようになります。または、管理者はパスワードの代わりに、さらに強力な認証方式 (ユーザ公開鍵) を使用することもできます。

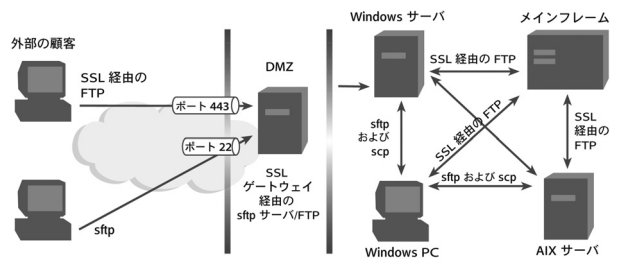


事例 2: 営業時間外に在宅で作業する管理者

### 事例 3: 医療機関

この事例では、医療機関で患者記録をサーバからサーバに内部移動させて外部機関と交換する場合を取り上げます。

パスワードと患者の機密情報が通常のテキスト形式でネットワークに送信されていることが外部監査でわかり、この医療機関は FTP を停止するように命令されました。内部と取引先の両方で使用されていた FTP の代わりに、この機関は SSH プロトコルと SSL プロトコルを採用しました。取引先はどちらかのプロトコルを非武装地帯で使用します。内部ではサーバ環境に応じて最適な方を選択します。



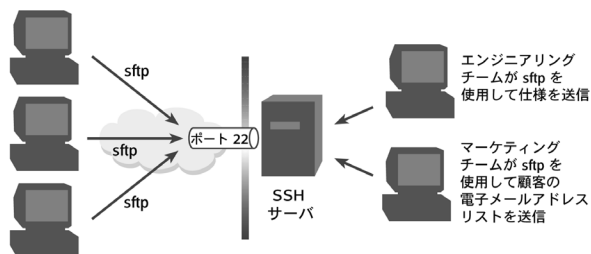
事例 3: 患者記録を内部および外部で移動させる医療機関

### 事例 4: 製造会社

この事例では、競争の激しい業界にあり、製品の製造と販売の両方で多くの取引先を持つ製造会社を取り上げます。最新の設計仕様とお客様リストは知的所有権であり、保護する必要があります。特に、このような業界には産業スパイが暗躍しているので保護は必須です。

SSH プロトコルスイートを使用し、ファイアウォールを設定した 1 台のサーバを機密性の高いすべてのファイル転送に使用することで、製造会社はすべての機密通信を監視し保護することができます。

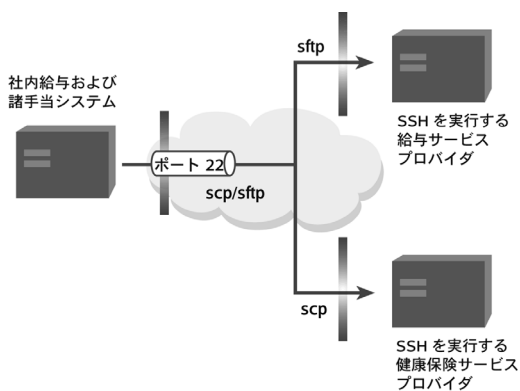
製造およびマーケティングのパートナー企業



事例 4: 取引先と知的所有権を交換する製造会社

### 事例 5: 給与計算および健康保険業務にサービスプロバイダを使用する企業

企業が従業員データ（個人の ID 番号、保険金請求、健康情報など）を第三者のプロバイダと交換する場合は、常に電子ファイルを保護する必要があります。ここでは SSH が最適です。scp を使用すれば、ファイル転送を簡単に自動化できます。



事例 5: 給与計算および健康保険業務にサービスプロバイダを使用する企業

## AttachmateWRQ: 転送データの保護

安全なファイル転送のために、AttachmateWRQ ではさまざまなクライアントおよびサーバソリューションを提供しています。これらはすべて、業界標準の SSH プロトコルと SSL/TLS プロトコルに準拠しています。ここでは、これらのプロトコルの安全なファイル転送機能について、また、これらのプロトコルが AttachmateWRQ セキュリティソリューションセットでどのように採用されているかについて説明します。

### SSH のファイル転送機能

SSH の主な目的は、強力な暗号化方式と認証方式を使用して、ネットワーク接続によるデータ転送を行うことです。SSH は、Telnet、FTP、X11、Berkeley r コマンド (rlogin、rcp、rsh) といった、データを通常のテキスト形式で送信するという、安全とはいえない方式に取って代わるソリューションです。

現在、SSH には SSH1 と SSH2 の 2 つバージョンがあります。この 2 つはまったく別のプロトコルに基づいていて、両者の間に互換性はありません。また、SSH1 は廃止される可能性があり、使用はお勧めしません。安全なファイル転送のために、AttachmateWRQ では SSH2 に対応しています。SSH2 は、インターネット技術標準化委員会 (IETF) によって標準化されています。

SSH では、rcp (リモートコピー) コマンドラインユーティリティに代わって scp コマンドラインユーティリティが使用されています (rcp は従来は UNIX 環境で指定ファイルとディレクトリのコピーに使用されていました)。また、FTP に代わって sftp が使用されています。sftp には FTP のすべての機能が備わっていますが、FTP のようなリスクはありません。SSH2 のサブシステムとして作成された sftp では、sftp クライアントとサーバの間で交換されるすべての情報 ( ユーザ名、パスワード、ディレクトリー覧、ファイル ) が暗号化されます。SSH の sftp 機能を使用することにより、組織は FTP の使用をやめて、ネットワークの弱点を取り除くことができます。

SSH では、データの機密性を保つために 3DES や AES などの強力な暗号化方式を使用しています。また、整合性の確認にハッシュメッセージ認証コード (HMAC) アルゴリズムを使用しています。

## SSL/TLS のファイル転送機能

SSL は、Web 上でのトランザクションを保護するために開発されました。

オプションで証明書に基づいた認証を提供し、強力な暗号化方式を使用した安全なデータ転送を実現します。SSL 3.0 を基盤として、SSL 機能をすべて備えた標準プロトコルの TLS (Transport Layer Security) が IETF によって開発されました。

SSL 3.0 と TLS 1.0 は若干異なります。TLS では、SSL で使用される MAC よりも破られにくい HMAC アルゴリズムを整合性の確認に使用します。ただし、この 2 つのプロトコルの違いはごくわずかなので、この白書では SSL/TLS プロトコルと表記しています。

SSL/TLS は、SSH のように FTP に代わるものではなく、FTP トラフィック用の暗号化された安全なトンネルの作成に使用します。以下の 2 つの RFC に、このプロセスの処理方法が記述されています。

- SSL 経由の FTP (RFC 2228) は、FTP プロトコルを拡張して、制御チャンネルとデータチャンネルの両方で強力な認証、整合性、機密性を実現します。
- TLS (RFC 2246) は、盗聴、改ざん、メッセージ偽造などを防ぎながらクライアント / サーバアプリケーションでインターネットを経由して通信できるように設計されたプロトコルを定義します。

FTP 転送で SSL トンネルを経由する場合は、FTP プロトコルのデュアルチャンネル特性を考慮する必要があります。FTP では、制御チャンネル用とデータチャンネル用の 2 つのトンネルを使用します。このため、ファイアウォールで 2 つのポートを開く必要があります。AttachmateWRQ ソリューションには、FTP トラフィックを SSL 経由で送信する際にファイアウォールへの影響を低減する方法が用意されており、開くポートは 1 つだけで済みます。

## AttachmateWRQ セキュリティソリューション

以下の AttachmateWRQ セキュリティソリューションには、SSH プロトコルと SSL/TLS プロトコルの両方が含まれています。

### • Reflection for Secure IT

Windows、UNIX、Linux 用の SSH サーバと、Windows、UNIX、Linux 用のサーバ / クライアントアプリケーション

### • Reflection for the Web

全プラットフォーム用の SSL/TLS シンクライアントと、全プラットフォーム用の SSL/TLS プロキシサーバ

### • Reflection エミュレーションソフトウェア

Windows 用の SSH および SSL/TLS アプリケーション

表 1 を参照して、必要なセキュリティ対策に合った AttachmateWRQ 製品を選択してください。

表 1: AttachmateWRQ セキュリティソリューション

	AttachmateWRQ SSL/TLS ソリューション	AttachmateWRQ SSH ソリューション
<b>クライアント接続</b>		
ブラウザからのオンデマンド	○ シンクライアントを任意のブラウザで使用可能	× シンクライアントでの sftp は未対応
コマンドラインインタフェース	○	○ scp と sftp の両方で使用可能
グラフィカルインタフェース	○	○ sftp で使用可能
相互運用性	○ RFC 2228 と RFC 2246 に対応	○ RFC 4251 に対応
<b>データの機密性</b>		
暗号化	○ AES や 3DES などの暗号レベルを選択可能	○ AES、3DES、Blowfish などの暗号レベルを選択可能
SSL/TLS	○ SSL 3.0 と TLS 1.0 に対応	非適用
SSH	非適用	○
<b>データの整合性</b>		
メッセージの不変	整合性の確認にハッシュメッセージ認証コードを使用	整合性の確認にハッシュメッセージ認証コードを使用
自動チェックポイント再開機能	×	○

次のページに続く

表 1: AttachmateWRQ セキュリティソリューション (続き)

	AttachmateWRQ SSL/TLS ソリューション	AttachmateWRQ SSH ソリューション
<b>認証</b>		
ユーザ名 / パスワード	○	○
公開鍵	×	○ ユーザ名とパスワードの代わりに使用可能。 複数サーバへのシングルサインオン (SSO) 用鍵エージェント。 サーバとクライアントの両方の認証
電子証明書	○ x.509 証明書に対応。管理サーバに証明書署名 および証明書生成ツールが付属	○ x.509 証明書に対応
Kerberos	○	○
<b>自動化</b>		
スクリプト記述	○	○
スケジュール設定	○ 外部プログラムを使用	○ 外部プログラムを使用
<b>アクセス権の制御</b>		
特定ディレクトリへの アクセス制限	×	○ chroot コマンドと仮想ディレクトリを使用
ユーザごとのアクセス権の設定	○ 管理サーバと安全なトークン認証機能を使用	○ ユーザアクセスを sftp のみに制限可能。各ファイル およびフォルダへの読み取り / 書き込みアクセスの セキュリティ権限をサーバで設定
ファイアウォールへの影響の低減	○ SSL プロキシサーバを使用する場合、 ファイアウォールで開くポートは 1 つのみ	○ ファイアウォールで開くポートは 1 つのみ
<b>監査</b>		
記録	○ さまざまな記録レベルの設定が可能。メータリング サーバにより、ログを集中管理し、レポートを作成	○ さまざまな記録レベルの設定が可能
<b>集中管理</b>		
接続の集中構成	○ クライアント構成に管理サーバを使用	○ クライアント構成に管理サーバを使用
ユーザアクセスの集中制御	○ 構成に管理サーバを使用	○ 構成に管理サーバを使用
<b>異種環境対応</b>		
	○ Windows 用のサーバ / クライアントアプリケーション。 任意のプラットフォーム上にあるブラウザで実行する シンクライアント。任意のプラットフォームで JVM を使用して実行する SSL プロキシサーバ。	○ Windows、UNIX、Linux 用の サーバ / クライアントアプリケーション。 Windows、UNIX、Linux で実行するサーバ
<b>エンドツーエンドセキュリティ</b>		
	○ SSL プロキシサーバを転送先のサーバで実行可能 または SSL プロキシサーバで SSL を使用してプロ キシサーバから転送先のサーバにトンネリング可能	○ 通常は SSH サーバを転送先のサーバで実行

## SSH と SSL/TLS: 最も安全な選択肢

FTP はインターネットでのファイル送信方法として有効性が実証されていますが、FTP の使用によって組織の機密情報のセキュリティが重大な危機にさらされる可能性があります。FTP を業界標準の SSH プロトコルと SSL/TLS プロトコルに変更するか、これらのプロトコルで強化することは、適切なコストで信頼性を高める現実的な選択肢です。AttachmateWRQ では、これらのプロトコルに準拠したさまざまなクライアントおよびサーバセキュリティオプションを提供しています。AttachmateWRQ 製品は既存または計画中のセキュリティポリシーに対応した設計になっており、転送データの安全性を効果的に確保することができます。

## AttachmateWRQ について

AttachmateWRQ は、ホストアクセスおよびホストインテグレーションにおける世界的なリーダーです。お客様が長期の企業戦略を推進されるにあたり、既存の IT 資産を最大限に活用するお手伝いをしています。当社の製品とサービスは、企業資産の拡張性、管理性、そして安全性を高めるために、世界 60 ヶ国で 4 万社以上のお客様企業にご愛顧いただいています。当社の詳細については、[www.attachmatewrq.jp](http://www.attachmatewrq.jp) を参照してください。



**本社**

1500 Dexter Avenue North  
Seattle, Washington 98109  
USA

TEL 206 217 7500  
800 872 2829  
FAX 206 217 7515

**日本支社**

東京  
TEL 03 5560 8970  
FAX 03 5560 8975

日本語 Web サイト [attachmatewrq.jp](http://attachmatewrq.jp)  
日本語 E-mail [j-info@attachmatewrq.com](mailto:j-info@attachmatewrq.com)

**販売代理店**

**サイバネット システム 株式会社**

本社 / 東京都文京区大塚2丁目15番6号ニッセイ音羽ビル  
TEL: 03 5978 5453 FAX: 03 5978 2201  
西日本支社 / 大阪府中央区常盤町1丁目3番8号中央大通FNビル(20階)  
TEL: 06 6940 3650 FAX: 06 6940 3601

E-mail : [rinfo@cybernet.co.jp](mailto:rinfo@cybernet.co.jp)  
URL : <http://www.cybernet.co.jp/reflection>

その他の海外支店については、[www.attachmatewrq.jp](http://www.attachmatewrq.jp) をご覧ください。

© 2006 Attachmate Corporation. All Rights Reserved. 本書の内容は、参照用としてのみ使用され、予告なしに変更されることがあり、Attachmate Corporation (事業社名 AttachmateWRQ) の責務として解釈されることがあってはなりません。AttachmateWRQ 社は、本書の内容におけるいかなる誤謬または不正確な記述に対しても、なんら責任または補償を負うものではありません。AttachmateWRQ、AttachmateWRQ ロゴ、Reflection は Attachmate Corporation の商標または登録商標です。その他のすべての商標、名称および会社名は識別の目的のみに使用されるものであり、また、それらはそれぞれの所有者に帰属します。本書に明記されている場合を除き、本書で Attachmate Corporation 以外の商標が使用されていても、そらの商標の所有者が AttachmateWRQ を支援したり、AttachmateWRQ と提携したり、AttachmateWRQ の製品を承認していることを示すものではありません。Printed in the USA.

06-0008.0106