情報通信技術 SoftEther VPN による社会変革戦略

登 大遊（ソフトイーサ株式会社，筑波大学大学院システム情報工学研究科）

概要 2003 年に開発した SoftEther 1.0 はフリーウェアとして公開し約 30 万人程度のユーザを得た．これを元に，2004 年にソフトイーサ株式会社を起業し，2005 年に製品版 PacketiX VPN 2.0 を販売した．本 VPN ソフトウェアの製品版は現在までに 4,180 社を超える企業等で導入していただき，日本において，個人レベルで開発を行ったソフトウェアとしては比較的良好なビジネス展開をすることができ，社会の役に立つことが些かできたと思う．現在本ソフトウェアは日本国内のみでしか普及していない．これから本格的に全世界で普及させたいと考えている．そのためには先ずこの VPN ソフトウェアを開発しようと思った動機および開発における技術的な設計上の思想について省みる．また技術的な開発が完了してからビジネス的に安定するまでの間は，単なるソフトウェア技術者としての知識だけでは解決することができない問題が多く発生した．そこでそれらについて考察することも有益であろう．そしてこれから本ソフトウェアによって世界に対してどのような影響を与えることができ得るかという想定を行う．筆者は本ソフトウェアが大きな社会変革を実現し得る重要な道具であり，そしてそれを世界に普及させることができるのではないかと考えている．この論文では，潜在的に強力な社会的価値があると思われるソフトウェアを開発または公開しようとするソフトウェア技術者にとって有益な情報を提供することを目的として，本ソフトウェアに関する技術的および非技術的な過去の思考過程および将来の戦略を述べる．

1. はじめに

SoftEther 1.0[1] 及びこれを基にして開発した製品版 PacketiX VPN （2005 年 12 月発売）並びにオープンソース版 UT-VPN（以下「SoftEther」という）は，Ethernet セグメントを仮想化し HTTPS プロトコルにカプセル化することにより，一般的なインターネットの Web サイトが閲覧可能な環境であれば必ず使用することができる VPN (Virtual Private Network) ソフトウェアである．HTTP 以外の通信（例えば TCP の任意のポート）を HTTP や HTTPS にカプセル化する試みは以前よりあったが，SoftEther は Ethernet フレームを HTTPS にカプセル化することを実現した．ユーザは HTTPS さえ通ればその上にどのような通信でも載せることができるようになった．

SoftEther は多くのオペレーティングシステム（Windows, Linux, FreeBSD, Solaris 及び Mac OS X） で動作し，使用方法が簡単であるため，ネットワークのエキスパート以外でも容易に導入および管理を行うことができるという特徴を持つ．またすべての VPN 通信は SSL によって暗号化され，VPN 接続時におけるユーザ認証にはパスワードの他 PKI を使用することができるという安全性を備えている．さらに VPN 通信におけるスループットを最大化するチューニングに努力した結果，他社のソフトウェアベースの VPN 製品と比較して大幅な高速化を実現した （図 1）．

しかし SoftEther の特筆すべき点は強力なカプセル化能力と透過性にある．カプセル化とは，ある通信プロトコル A に基づく伝送データを，別の通信プロトコル B のペイロードとして認識されるような形のヘッダ等を付加して，通信プロトコル B に内包させて通信させることを意味する．もともとある通信プロトコルの通信をすることが出来ないネットワークで，その通信を可能にするた

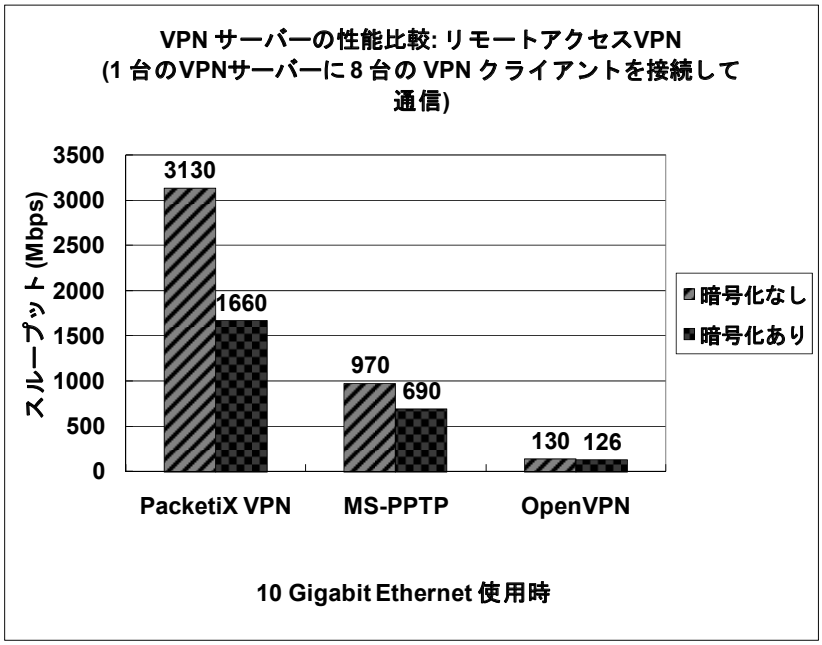

図 1 他の VPN システムとの速度比較

めに技術的に一種の「偽装」を行って，力ずくで通信することができるようにする工夫である．

SoftEther 以前の VPN システムとしては，代表的には IPsec，L2TP，PPTP があった．これらは通信途中のファイアウォール等のゲートウェイから見れば明らかに VPN プロトコルであると分かるものであり，必要な場合はゲートウェイで容易に遮断することができた．また HTTP を中継するためのプロキシサーバを経由することで通信する必要がある社内 LAN などでは，そもそも外部ネットワークとの間の VPN 通信ができなかった．社内 LAN においてネットワーク管理部門は社員が自由に外部の VPN サーバとの間で VPN 通信をすることに危機感を持つ．これを禁止するため，ファイアウォールやプロキシサーバ等を社内 LAN とインターネットとの間に設置している管理が多かった．このような状況でも問題無く使用できるのが SoftEther である．このことが話題となり，一時的に経済産業省から配布停止を要請されるに至った．

その後 SoftEther の製品版である PacketiX VPN を開発し販売する上で，SSL による暗号化やユーザ認証がいかに安全であるかというようなセキュリティ面の特徴を強調してきた．その結果，現在までに 4,180 社を超える企業等で導入いただくことができ，ビジネス的には一応の成功を収めた．だがこれは SoftEther の第一歩目である．このソフトウェアは強力な透過性，途中のゲートウェイにおける監視と遮断の困難度の高さを特徴として普及させるべきと考える．その普及先ターゲットは，全世界を対象としたい．そう考えた理由を明らかにするために，SoftEther を開発しようと思うに至った動機とこれまでの開発および販売における技術さらにマーケティングの出来事を述べる．また世界中に SoftEther を普及させるために現在検討している事項，すなわち SoftEther が社会の既存システムに対して影響を与える可能性とそれにより社会をより良い方向に変革させていくことができる可能性について述べる．

2. SoftEther の開発動機

2.1 開発の直接のきっかけ

筆者が SoftEther 1.0 を開発する直接のきっかけになったのは平成 15 年度未踏ソフトウェア創造事業未踏ユース部門で SoftEther 開発プロジェクトが採択されたことである．実際，筆者が筑波大学に入学した直後に学内 LAN の無線 LAN アクセスポイントが HTTP 通信しか許容しないことを知ったのだが，それ以外のすべての TCP/IP の通信をインターネットとの間で行いたかったからである．しかし，SoftEther を開発したいという潜在的な動機はそれよりも前から持っていた．概ね以下のような非技術的な思想に由る．

2.2. 創造の機会損失を防ぎたい

一般的に我々は，社会において何らかの形で所属している組織の管理者による管理を受けている．例えば国民としては政府による管理，学生としては大学による管理，社員としては会社の管理者・経営者による管理などである．ところで我々がこの世界に存在する合理的な理由は何らかの創造的活動（より詳しく言えば我々しか実施することができない高度な脳を用いた論理処理機能および高速感情処理機能を用いた思考および思考結果を実現しようとする活動）であると思う．我々がそれらの創造的活動を行う際には，必ず自己の所属している組織の外部の者と物質および非物質の流通を必要とする．物質とは例えば食糧とか原材料とか製品とか貨幣などのことである．非物質とは情報のことである．

現代社会における組織の管理者の役割は，このような物質および情報の外部との流通を制御する行為が重要な部分を占めている．規制があるということは特定の物質または情報の流通を許可するか禁止するかを特定の管理者が決定することを意味する．勿論，管理者の存在にはメリットもあるが，ここでは流通の制御について考える．

管理者たる者には，個々人の創造的活動を阻害せず，かつ有害なトラブルを起こさないために適切に流通を制御して，最大効率化を実現する能力が要求される．しかし，有害なトラブルにつながる可能性（または有害なトラブルが発生した際の損失の額と発生の確率から計算される期待値）が比較的低いにもかかわらず，その可能性をできるだけゼロに近づけようとして，却って人々の創造的活動を妨害する結果となってしまう管理が見られる．例えば国家が海外との当面の競争を避けようとするために高額な関税障壁等を設置して流通を規制して，自国の企業の技術革新が遅れ，海外の技術革新に追従することができなくなったとしたら，その国は悪い管理を行っていることになる．また会社において，外部への情報漏洩を防ぐためにインターネットの通信に特定の安全と思われるプロトコル以外の通信を禁止して，多くの創造的な社員が効率的な業務の源泉であったインターネットを用いた外部とのコミュニケーションができなくなり，業務効率が低下したなら，その社内 LAN の管理方針には問題があると言える．

創造的活動をできるだけ多く成し遂げたいと思う者

にとって，それを阻害するような管理下にある状態は，非合理的な状況である．有能な人々が，たとえ数年間程度であっても，このような管理下に置かれることにより，創造的な仕事がし難い状況は，世界にとって大きな機会損失である．

2.3. 有益な創造活動を促進する仕組み

ここでは流通のうち非物質的なもの（情報流通）について考える．管理の一環としての情報流通の規制は，必要悪であると考えることもできる．何故なら目的合理性なしに当面の利益のために行動するような人もいるので，情報流通の規制がなければ，その組織にとって全体的に大きな損失が生じてしまう可能性が有る．理想的な管理とは，管理対象の社員の能力に応じて情報流通の規制内容を峻別する管理であろう．全ての組織において，このような管理が行われることが望ましい．しかし多くの組織ではこれは実現されていないようだ．むしろ，すべての人々に対して無差別に規制をかけている事例が多いと思う．

筆者が SoftEther を開発し，無償で公開した動機は，情報処理や情報管理について十分な能力を有する個人に SoftEther を使って貰いたかったからである．つまりインターネットを用いて外部の人やサーバと自由に交信し，周囲の者と比較して何倍もの能率を発揮することを可能にし，それによってその組織内で良い業績を挙げ，それに見合った待遇を受けるという合理的な環境を作りたかったのである．

3.強い透過性の実現

3.1. 子供の頃に理解したカプセル化

SoftEther は VPN ソフトウェアであり，通信におけるカプセル化処理は中核機能の一つである．カプセル化の概念は技術書などで理解したのではない．子供のころ偶然聞いた次の話からカプセル化が大変素晴らしい仕組みだと感動したことに遡る．

ある会社員がいつも自宅にいる妻に夕方，会社の近くの公衆電話から電話をかけ（携帯電話が普及していなかった時代），その日の夕食が必要か否かという旨と帰宅予定時刻を伝達したいのだが電話料金がもったいない．その会社員は大変真面目で，ルールに反することはしたくないと思っていた．そこで，公衆電話から自宅に 1 回目の電話をし，「夕食が不要な場合」は呼び出し音を 1 回だけ鳴らし，「夕食が必要な場合」は呼び出し音を 2 回以上鳴らしてから電話を切る（妻は電話はとらない）．そして 2 回目の電話では「18 時に帰る予定」の場合は「1 回」，「19 時に帰る予定」の場合は「2 回」・・・ というような具合で帰宅する予定時刻から 17 を引いた回数だけ呼び出し音を鳴らして電話を切る．こうすれば課金されずに，必要な情報を毎日定時に伝えることができる．

これは，カプセル化技術の本質だと思う．技術的にみれば NTT は「無料通信の対象となるプロトコル」として「呼び出し音をどう鳴らすか（1 秒鳴らし，2 秒休む）という旨のプロトコル」を無料で提供している．だが，呼び出し音を鳴らした回数は立派な情報である．利用者はこの方法を繰り返して，どのような複雑なバイナリデータでも原理上，無料で相手方に伝えることができる．

SoftEther を開発するのに最も重要であったカプセル化という概念の大元は子供の頃に聞いたこの話である，既存のルールを守りつつ，既存のルールでは通信することができないと考えられていた通信を自由に行うというアイデアを具体的にソフトウェアの形で実現しただけなのである．

3.2. HTTPS によるカプセル化

カプセル化は従来の VPN プロトコルでも広く使われていた．しかし従来の VPN のカプセル化処理は，ハードウェアによる高速処理を目的として，出来る限り単純に規定されていた．一方 SoftEther ではこれと逆に出来る限り複雑にカプセル化を行うようにした．

SoftEther は名前の通りソフトウェアで VPN 処理を実現するので，カプセル化に係る処理はとても柔軟に実装することができる．そのため以下のことを最も重要な目標としてプロトコルを設計した．

多くの社内 LAN においてはルータ，プロキシまたはファイアウォールが設置されているが，ほとんどの場合，社内 LAN とインターネットとの間で HTTP 通信を行うことは許可されている．何故ならばインターネット上の Web サイトを閲覧することは，ネットワーク管理部門にとって他のプロトコル（Skype やメッセンジャー，ファイル共有ソフトウェア等）を使うことと比べたら比較的安全な行為であると認識されているためである．

SoftEther のプロトタイプ版を開発した 2003 年当時，既に HTTP による社外の Web サイトの閲覧ができなければ，仕事に差し支える程度にインターネットが普及していた．そこで HTTP 通信によってカプセル化すれば良いと考えた．だが，HTTP 通信は暗号化されておらず，HTTP 通信の内部を HTTP の RFC 規格[2] に合わせて POST データのペイロード部に VPN の通信対象データを投入する形でカプセル化しようとしても，途中のファイアウォ

ール等によって当該通信が異常に大きな POST データ量の HTTP 通信であると判断され遮断されてしまう可能性があった．そこで標準で SSL によって暗号化されている HTTPS をカプセル化することにした．ネットワーク管理部門が HTTPS を遮断していないという事実は，「HTTPS というプロトコルに従うすべての通信は通過しても良い」ということを意味すると解釈できる．何故ならば HTTPS はいかなるデータでも POST メソッドのペイロードとして通過させることができると RFC に規定されている．すなわち，HTTPS の通信が許可されているネットワークに於いて SoftEther で VPN 通信を行うことは，そのネットワークの利用ルールに反しない．

筆者の考えではルール，規則というものは一旦決定して公示した後は，頻繁に，または恣意的に変更してはいけないし，また特定の行為がルールに違反するか否かという判断は，管理担当がその都度自由に決定して良いものではない．特定行為がルールに抵触するかどうかの判断は，行為の事実と，予め設定されているルールの内容とを論理的かつ機械的に判断し，ルールに違反するか否かを二分的に厳密かつ客観的に決定するプロセスが保証されていて，はじめて正当化される．更にルールに違反するか否かが微妙な行為の場合は，疑わしきは罰せずの原則が適用されなければならない．このような前提がないと，ルールは抑圧的制約のための道具になってしまう．

社内で HTTPS の通信を許可しているのに，その HTTPS に準拠した通信をを行う SoftEther を使用することが規則違反だとすることは，管理体制の根拠となるルールに矛盾があることの表れである．SoftEther は分別のある人々にとって，その組織の管理レベルを認識，判断するための材料を増やすためのリトマス試験紙であると言える．その意味で第 2 章で述べた人々の創造的活動を支援するという SoftEther の役割が図らずも発揮できていると言える．

3.3. トラフィックパターン検出の防止

SoftEther を公開して間もなく，HTTPS 通信としてカプセル化された SoftEther の VPN 通信を検出または遮断することができるファイアウォールが国内および海外の会社から登場した．これらのファイアウォールにより，第 2 章で述べた目標，すなわち会社にとって有益な創造的活動までもが阻害される可能性があった．調べてみると、SoftEther を遮断することができるこれらの装置はトラフィックパターンを調べ（SSL で暗号化されている），HTTPS の通信の内容を解読することなく，通信パケットのデータ長やその送受信順序，通信パターン（例えば，長時間コネクションを張り続けている HTTPS セッションは VPN 通信であると仮定する等）によって SoftEther を検出していることが判明した．これでは，折角すべての通信を SSL で暗号化していることが無駄になってしまう．だからトラフィックパターンによって検出されないように工夫をした．

主な手法は 3 つである．先ず全ての HTTPS パケットについて，パケット長から当該通信が SoftEther によるものであることを認識されにくいようにするため，毎回異なった長さのパケット長となるように調整した．そのために無意味なパディングをランダムな長さで挿入した．

次に 1 本の HTTPS セッションにおいて，当該セッションが確立されてから切断されるまでの間の送信・受信方向の入れ替わりの回数を削減することにした．そもそも HTTPS (HTTP) では，通常クライアントとサーバとの間では，一方が何らかのリクエストを送信し，もう一方からそれを受け取ってからレスポンスを返すというような順序の通信しか発生しない．つまり 1 本のセッションでは，同時に送信方向と受信方向の通信が発生することはない． SoftEther の古いバージョンでは，1 本のセッションで送信と受信の両方を行っていた．これがトラフィックパターンによる検出を容易にさせた原因であった．新バージョンでは複数本のセッションを張り，そのうちどの特定の 1 本のセッションを監視しても，普通の HTTPS 通信と異なるデータの流れの特徴を無くすようにした．

最後に 1 本の HTTPS セッションが確立されてから切断されるまでの間の時間が長すぎたり，伝送データ量が多すぎたりすると，普通の Web ブラウザ等を用いた HTTPS サーバとの間の Web ページの閲覧やデータの POST の通信と比較して明らかに異常であると認識され，SoftEther による通信として検出されてしまう可能性があった．この問題を解決するために複数本の HTTPS セッション（合計 32 本まで）を並行して確立し，それぞれの HTTPS セッションは一定時間で自動的に切断されるようにした．最初にすべての HTTPS セッションを一度に確立すると，特異な通信であると認識されてしまうので，ある一定秒間隔で順番に接続するようにした．セッションの維持期間はユーザが自由に設定することができるようにした．これによってトラフィックパターンによる SoftEther の通信を検出することを一層困難にした（図 2）．

3.4. TCP/IP コネクション確立の逆転

SoftEther はすべての VPN 通信を TCP/IP 上で HTTPS

によってカプセル化して伝送している．TCP/IP は 2 台の端末間で 1 本のコネクションを確立するプロトコルであるため，通信しようとする 2 台のホストのうち何れか一方が待ち受け側（終点）として TCP ポートをリッスンし，もう一方を始点としてコネクションを確立する必要がある．一度コネクションが確立された後は双方の立場は対等となる．

SoftEther を含めたすべての VPN システムの使い方の 1 つにリモートアクセス接続がある．既存の社内 LAN などに 1 台の VPN サーバを設置し，その VPN サーバに対して，遠隔地の VPN クライアントが接続し，あたかも社内 LAN に直接接続しているかのように通信する方式である．従来の常識ではリモートアクセスの目的となる LAN 側が VPN による接続を待ち受ける必要がある．SoftEther は TCP/IP を使用するため，本来であれば社内 LAN の側に設置する 1 台の VPN サーバとなる PC にグローバル IP アドレスを割り当て，またインターネット側からのポートを開放してリッスンできるように設定する必要がある．しかしそのためには管理部門の協力が必要である．何故ならばグローバル IP アドレスを社内 LAN の PC に設定したり，外部からのポート開放をしたりするためには，当然社内 LAN の管理部門による明示的な設定が必要であるためである．だが，管理部門の手を煩わせずに，VPN の実現ができればさらに良い．

多くの会社の LAN では外から中の方向の TCP/IP コネクションの確立は禁止されているが，中から外の方向の TCP/IP コネクションの確立は許容されていることが多い．社内 LAN に対するリモートアクセス VPN サーバを構築する際に，VPN サーバの役割を担う PC を社外の自由なネットワークに設置して，社内にある 1 台の PC を VPN のブリッジとして設定し，その VPN ブリッジから当該 VPN サーバに対して中から外の方向の VPN コネクションを確立してしまえば，社内におけるグローバル IP アドレスの調達や外部からのポートを開放するファイアウォールの設定をせずに，その社内 LAN に外部からアクセスすることができるようになる．

分かりやすく説明すると，ドアの鍵は外側にいる人は開けることはできないが，内側にいる人であればいつでも開けることができる．そして，一度その鍵を開けた状態で外部との間のパイプ（VPN セッション）を接続し，すぐにドアの鍵を閉めてもその VPN セッションは継続的に利用可能になるのである．

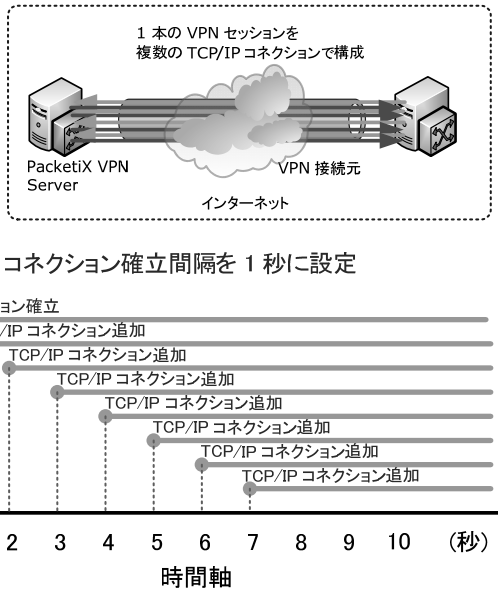

図 2 複数のコネクションを並列に確立する仕組み

4. 製品版 SoftEther PacketiX VPN

4.1. PacketiX VPN という名前の理由

これまで SoftEther の開発の動機と特徴について述べたが，このような動機が明らかとなれば，SoftEther の製品版は企業のシステム管理部門にはあまり歓迎されない可能性があると思われた．そこで SoftEther の製品版を販売する際，いくつかの工夫を行った．

名称は SoftEther ではなく PacketiX VPN とした．これには SoftEther が社内 LAN の管理部門とは無関係に VPN を構築することができるツールであるという話が広く浸透していたことによるマイナスイメージを避けるためのイメージ戦略である．ただし，製品名の変更がイメージ戦略上ほとんど意味が無かったのではないかと今では思う．しかし，実際には多くの企業に導入していただいた．これについては次節で述べる．

名前の変更にはもう 1 つ理由がある．それは某大企業と共同で SoftEther の商標出願をしたからである．SoftEther を元に認証機能を改良した SoftEther CA を共同で開発販売しようという話になったときに共同開発の契約書を締結し，また，商標の出願費用は全部先方が負担するので一緒に「SoftEther」という商標を出願したのであった．筆者は 19 歳，不勉強であり，契約について詳しくなく，相手は大企業であった．言うとおりにしておれば困ったことにはならないと信用して契約を結んだ．そして随分と後になって

SoftEther CA に関する共同開発の契約書を見て，ソフトイーサ社の得るべき対価は売上金額の数パーセントである旨が記載されていたことに気がついたのであった．この経験から学んだことについて 4.3, 4.4 節で詳しく述べる．

4.2. SoftEther の企業での活用事例

PacketiX VPN（図 3）は 2005 年 12 月に発売されてから 5 年間で 4,180 社の民間企業，官公庁および個人事業者等に採用された．身近なところではファミリーレストラン等のチェーン店の運営管理や医療サービス，物流サービス，マスメディア，航空施設の管理などの民間事業のための社内通信や，地方自治体の行政ネットワーク，さらには中央政府機関の本部と海外拠点を接続するための通信等のために 24 時間 365 日間止まらずに安定した VPN を実現している．

前述のように，SoftEther は経済産業省に配布停止を要請される程に強力な透過性を持つ VPN ソフトウェアであり，企業内の個人が勝手に使用するとセキュリティ上危険であるという批判が多くのネットワーク管理者から上がっていた．それにもかかわらず，なぜ SoftEther の製品版 PacketiX VPN は多くの企業に導入されたのであろうか．

勿論，本ソフトウェアが従来のハードウェアベースの VPN を置換し，安定性はそのまま，既存の PC サーバを活用した安価な VPN を構築する道を拓いたということは理由の 1 つである．たとえば，大規模回転寿司統合管理システムの VPN 通信に本ソフトウェアを導入したあるレストラン企業は，VPN 構築のために想定していた予算の 20%で全国に大規模な VPN を構築することができた点を評価している[3]．しかし，本ソフトウェアが企業向け製品として成功したユニークな理由として，他に 2 つあるのではないかと思う．

まず，SoftEther は強力な機能をとても簡単に試すことができる形式でインターネット上で配布され，約 30 万人がダウンロードして，自宅や会社などで使ってみた．これらの人のうち，割合は正確には分からないが，多くの部分をコンピュータのパワーユーザが占めていた可能性がある．こういったパワーユーザは企業での情報システムの管理を行っている担当者であったり，または，企業内の情報システムについて管理者に対して鋭い意見や改善要望などを主張する能力に長けている一般の社員であったりする場合がある．そういった人々が，従来は VPN は導入・設定およびメンテナンスが難解であり取っ付きにくいというイメージを持っていたのに，SoftEther を試しに使ってみて，その固定観念が大幅に変化し，簡単に VPN を構築することができることに驚き，SoftEther のサポート付き製品版が出たら是非自社の業務に導入してみたいと思ったのではないだろうか．そして，後に PacketiX VPN が発売された際に採用してくれたのではないかと思われる．最初のバージョンを無償で公開し，また情報リテラシーが高い方々によってインターネット上で話題となったことが良い結果をもたらしたと思われる．

もう 1 つの理由は，本ソフトウェアの持つ強力な透過性に因ると考えられる．社内で従来は IPsec や PPTP ベースの VPN を導入していたり，試しに使ってみたりしたことがある企業はこれまでも多くあったが，従来の VPN プロトコルはファイアウォールや NAT，プロキシサーバがある環境ではうまく繋がらない場合が多く，利用にあたって不満が生じていたのではいか．その状況で，本ソフトウェアが，その強力な透過性を理由として，当初はセキュリティ上の懸念として批判的な話題を集めたのであるが，逆にこのような透過性を有することが知れ渡った結果，従来の VPN に関する不満を持っていた情報リテラシーが高い方々の脳内にこの不満を解決してくれる良いソフトウェアとして記憶された可能性がある．そして，後にそういった方々の熱意が情報システムを利用している企業等において製品版を是非導入してみようという積極的な検討につながったのではないだろうか．

この 2 つの理由が推測されるが，共通点としては，ソフトウェアのみで動作するという特徴と，簡単で強力であ

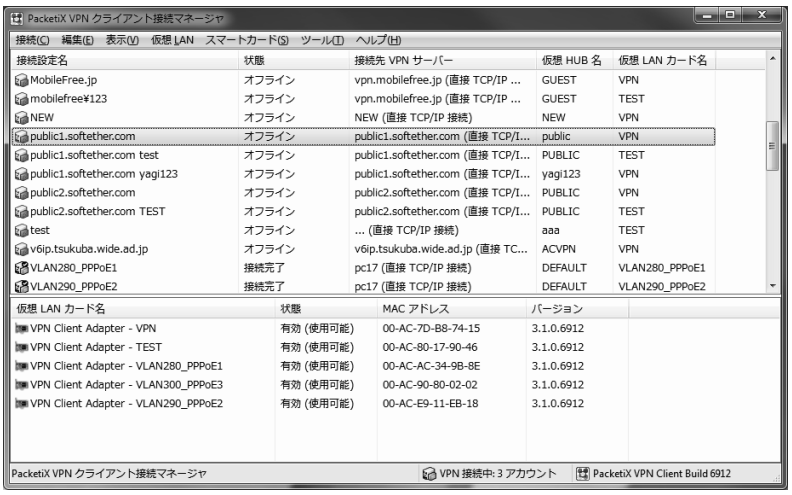

図 3 PacketiX VPN Client 製品版の画面

り使い方を誤ると危険という話が偶然口コミやニュース記事で広がり始めたことがきっかけとなって，インターネット上で SoftEther が広く知れ渡ることとなり，それが 2 年後の製品版 PacketiX VPN の製品に結びついたということが言えよう．

これからの時代は，インターネットでソフトウェアやオンラインサービス等で広めることが益々重要な手段となる可能性が高い．その効果的な方法として，あえて賛否両論の批判が巻き起こりやすいような何らかの強力な機能・特徴を持たせ，それで騒ぎのようなものが起きたら，それに乗って多くの人々に知れ渡るように開発・公開を行うという手法は大変有効であると思う．

4.3. ソフトウェア技術の収益への変換

ソフトウェアを開発したからといってすぐに収益につながるということはない．SoftEther の場合，本格的に販売を行ったのは 2006 年からである．また当初は後のことをあまり考えずにソフトウェアライセンスを販売していた．また，ソフトイーサ社では SoftEther を基にしたいくつかの通信ソフトウェアやサービスも開発し販売してきた．その過程において分かったことは，ソフトウェア技術を収益に変更するためには社会的知識の習得が必要であるということである．

社会的知識で最も重要なことは，会社の財務に関するマネジメントや，対外的な契約，取引の履行等に関する実践的知識である．これらは，習得してみると実は大変容易なのだが，これらを学習していなかった頃を振り返ると，難解でソフトウェア技術とは全く異なる取りつき難いものと決めつけていた．しかしソフトウェア技術者にとって，これらの社会的知識の習得はかなり容易なのではないだろうか．ソフトウェアの動作の仕組みを設計，実装したり脳内でイメージしたりすることが出来る能力があれば、社会システムの動作の仕組みをうまく活用するという行為を殆ど同一の脳内機能によって実施することができるのではないかと思う．

一例を挙げよう．ソフトイーサ社において数回，いわゆる訴訟沙汰のような対外的取引に関する事件が生じたことがあるが，これらを解決するための方法は殆ど既に自己が持っている情報と智慧を併せてプログラムを設計したり記述したりする行為と同じであった．

4.4.社会的知識を身に付ければ最強

ソフトウェア技術者は良いソフトウェアを開発したら起業してビジネス化するべきと考える．これはすべての創造的な人々にとって共通して言えるだろう．問題は起業した後に必要な社会的知識，つまりは法律や契約，取引に関する知識が欠けている状態で会社を経営している人が多い点にあると思う．せっかく有益な仕事に自己の能力を最大限活用して行ったにもかかわらず，その対価が他人に取得されてしまいかねない．つまり本来自分のものにすることができたはずの対価を元手に，次に新たな製品を開発する機会を失うことになってしまう．だから高い創造的能力を持つ人は，社会で本来得られるはずの対価を奪われないようにするために，技術だけではなく総合的な社会的知識をできるだけ広く深く身に付けたほうがよいと思う．技術に詳しいのに，社会的知識について専門分野以外であるからという理由で敬遠する人もいるが，社会における既成のプロセスを技術に詳しい人が体得して運用すると，非技術者（日本では一般的に文系と呼ばれる人）と比較して，相当強力に社会の既成システムを活用することができ，対価の横取りに対して強い防御能力を発揮できると思う．技術者は自分の特定分野の技術を高めることと並行して，社会システムに関する文系的技術についても同時に習得するべきである．日本の技術者は総じてこのような知識に弱いと思う．グローバル化した世界で日本に残されたほぼ唯一の重要な商業的な価値は高い技術力を持った技術者たちである．その技術者たちが社会的知識を身に付けて，技術をもとに得た所得を最適に再投資し，得られたさらに高い技術を世界のために最大限生かすことができると期待される．

5. グローバル化と SoftEther VPN

5.1. SoftEther はグローバル展開可能

日本でも，高品質なソフトウェア製品は，ある程度の数，過去に開発されている．例えばワープロソフトや業務システム等パッケージ製品は多い．しかしそれらは殆ど日本の慣習上の仕事をデジタル化して重宝されている製品なので，一歩海外に出れば，あまり活用の場はないだろう．一方 SoftEther は VPN ソフトウェアであり，Ethernet に載せることができるすべてのプロトコルを通信対象とする．世界中でコンピュータネットワークにおいて Ethernet や TCP/IP が使われていない国はない．したがって，SoftEther はすべての国において需要があるソフトウェアである．SoftEther が日本においてある程度ビジネス的に成功したが，それが海外では上手く通用しないということに合理的な理由は見当たらない．

実はこれまで SoftEther を海外で積極的に普及させることは実施していなかった．その理由は国内においてビジネス的にソフトイーサ社を安定させるために多くの時

間を要したためである．その安定化が一段落したので，2010 年から，先ず中国に SoftEther を普及させる試みを開始した．北京市に Beijing Daiyuu SoftEther Technology Co., Ltd 社を設立し，PacketiX VPN 3.0 の中国語版を開発し，また中国政府から販売登録を取得したのが 2010 年 12 月である．今後，中国を初めとして多くの国・地域で PacketiX VPN およびその他の SoftEther を基にした技術を普及させたいと考えている．

5.2. SoftEther によるグローバル化の加速

SoftEther はグローバル展開することで利益を得ることができるソフトウェア製品であるだけではなく，世界全体のグローバル化の加速に貢献することができるソフトウェア製品でもあると考える．これに関して以下の 3 つのポイントがある．

1 つ目は，多くの優秀な企業は今後ますます多くの国・地域にまたがって活動することになるという点である．これまではどの国でも自国内だけで多くの産業の経済が回っていた．競争は特定の国・地域の中だけで行われていた．しかし現在では競争は必然的に世界の他の競合者との間で行われるようになりつつある[4]．以前は大企業のみが海外進出を行っていたが，今後は中小企業であっても海外進出を行うか，或いは少なくとも提携会社と共に海外取引を活発に行うことが必要となるであろう．その時に元手資金が潤沢でない企業であっても，国際専用線を利用することができる大企業と同様に遠距離間の Ethernet による通信を行いたいという需要があるはずである．インターネット VPN をどのような国・地域間でも安定して接続することができる SoftEther の意義はここにある．

2 つ目は，いくつかの保守的な先進国は自国の労働者の雇用を守るために発展途上国などからの労働者の流入を制限しているが，それはもはや無意味な抵抗ではないかと思われる点である．最近は機械的な単純労働にはほとんど付加価値がない．もとより付加価値が高いのは知能労働である．知能労働でコンピュータ，電話，机さえあれば遂行可能な仕事で高収益，高賃金なものは数多くある．これらの高賃金労働は，例えば日本では日本企業に勤める日本人によって主として行われてきていた．しかしそれらの労働の中には実は発展途上国の労働者でも同じ能力で遂行することが出来るものが多い．それらの労働者が日本に流入すると，日本の既存の高賃金で終身雇用する建前の約束となっていたはずの労働者の賃金を競争によって下げなければならなくなる．そうすると労働機会を失うと恐れる既得権者層の人たちが中心となり，政府の力を用いて外国人労働者の流入を物理的に制限するという方向に流れるのが自然である．だがこれらの知能労働の大半はインターネット VPN を用いて発展途上国内でその国の労働者が居住しながらにして，つまり在宅勤務の形で日本企業に遠隔勤務して遂行することができる．単に生まれた場所が発展途上国であるという理由だけで先進国の企業に勤務することができなかった有能な人々が，先進国の企業から直接，条件の良い仕事を得ることが出来たなら理想であろう．そのためのツールとして SoftEther を使ってもらえれば嬉しい．国は発展途上国からの物理的な労働者の入国を防ぐことができたとしても，インターネットを経由して遠隔で働いてもらう形の仮想的な入国を防ぐことは誰にもできないのである．従ってこれからはそのような勤務形態が一般的であるという前提で国は政策を決定しなければならないであろう．

3 つ目は，国ごとのビジネス上のルールの違いはもはや意味が無くなるのではないかという点である．昨今では物理的に物質の移動が伴う製品やサービスは利益率が低く，一方非物質的な情報サービスのほうが逆に利益率が高くなっているように思える．今後も情報サービスの付加価値はますます高くなるであろう．情報サービスに関する規制は，国ごとに異なる．例えば A 国においては特定のサービス S は違法であり，B 国では合法であるとする．A 国の市民に対して A 国で提供することが違法な当該サービスを，B 国にサーバを設置してインターネット経由で行うことは合法であろうか．A 国政府は違法だと主張しても，B 国政府は合法だとして問題視しないはずだ．サーバ本体は B 国にあるので A 国の主権は及ばない．だが A 国政府は A 国の国民がサービス S を利用できないようにするために B 国の当該サーバとの間の通信を遮断するかも知れない．このような事態を避けるために SoftEther は有用かもしれない．

上記のようなインターネットおよび VPN を活用したグローバルな通信が可能になることによるビジネス環境の変化は，それを好むと好まざるにかかわらず，この世界に生きているすべての人々に影響を与えることは不可避である．不可避なのであれば，出来るだけ簡単に，素早く，安価に，安全かつ確実にそれを実現するためのツールとして SoftEther を活用していただけるように望んでいる．

5.3. VPN 技術が社会にもたらす意味

情報流通を促進する技術は，過去の人類の歴史を大きく変化させるきっかけになってきた．たとえば，グーテンベルクの活版印刷は，支配階級にある者の意見以外の

多様性に富んだ主張を誰でも行うことができる状況を生み出し，これがヨーロッパでの革命につながり，近代国家の仕組みが確立され，産業が発展し多くの人々の生活レベルが向上した．

VPN 技術は情報流通を促進する技術の 1 つであり，かつ，極めて強力なものであると考える．このように影響力の高い技術にはどうしても「諸刃の剣」の特性がある．例えば，VPN 技術のうち，インターネット等の公衆ネットワーク上に安全なトンネルを確立する暗号化技術は，盗聴されない通信を実現する．通信内容を隠蔽し，第三者に傍受されないことは，たとえば個人や団体が情報を悪意のある第三者に傍受されないようにするという正当な目的で使えばビジネスの促進に繋がる．一方，例えばテロリストが犯罪計画を国家に事前に傍受されないようにするために通信内容を隠蔽するなど，国家にとって解読することができない暗号化システムが誰にでも利用可能になることについて反対する人もいる．さらに近代の歴史を見ると，国家が国民に対して本当の情報やその通信内容を隠蔽し，早期に公表しないことによって，誰の利益にも繋がらない戦争が引き起こされたり，経済計画の誤りが長期間正されなかったりすることもある．これらに鑑み，国家が重要な情報を隠蔽することができる状況について批判する人も多い．これらから導き出される結論は，通信内容を隠蔽するということ自体には善悪はなく，それを実現するための技術は中立的立場にあるとみなされるべきであるということである．筆者は，VPN のような強力な情報流通を促進する技術はこれからもどんどん強力で使いやすく，解読されにくく，透過性が高くなるべきであると思う．

SoftEther の持つ強い透過性は，企業のファイアウォールだけではなく，国際社会における国境の存在を揺るがすものである．国境における悪い面，つまりどの国に生まれたかという事実だけでビジネス上の有利不利が決まってしまう事を軽減させることにつながる．また，国境において国民の利益とならない情報検閲をできなくする技術である．この特徴をうまく活用すると，社会における不正を正したり，独裁者が情報統制を行っている国家を民主化するなど，社会を良い方向へ変革させることにつなげることができる．すなわち，真のボーダーレス社会を生み出す原動力となり得る．その変化の過程で社会から既存の不自然な固まった体制が徐々に解消されていくことになるため，一時的には混乱するかもしれない．だが，長期的には必ず，より平和で安定した環境に収束していくのではないかと思う．

SoftEther は上記のように現在，多くの企業や政府機関などで採用され，大きなメリットを生み出しており，価値のある仕事のために正しく使われている．これからは，SoftEther またはこれを元に今後開発するソフトウェアがグローバルに普及し，世界中の色々な地域の人々に使用され，長期間持続する安定および継続的なグローバルな成長の実現に寄与できればと思う．

5.4. オープンソース化

SoftEther をグローバルに普及させるためには，日本国内においてのみ行っていたライセンスの法人向け販売という手法に加えて，世界的に通用する高速な普及方法を採用する必要があろう．そこで製品版 PacketiX VPN のオープンソース版 UT-VPN を新たに開発した．この執筆時点ではまだ英語版は完成していないが 2011 年春までには公開したいと考えている．

6. まとめ

本論文では SoftEther の開発の動機，技術的な特徴，および戦略について述べた．SoftEther は単に便利な VPN ソフトウェアであるだけではなく，インターネットによって今後大きく変化する世界全体の人々の行動様式の変革について何らかの形で寄与できるツールとなる可能性があると考えている．また SoftEther がそのようなツールとしてボトムアップ形式で多くの人々に受け入れられるようにするための施策を行っていく必要がある．

そもそも SoftEther は情報流通環境が大きく変化することを前提としてそれを加速するためのツールとして普及させるべきソフトウェアである．だから SoftEther のようなソフトウェアを今後開発して普及していく際に重要なことは，情報流通環境は常に大きく変化する可能性があるということを念頭に入れることである．こう考えて自由に SoftEther の普及を行えるのは，筆者自身の企業でそれを行っているからである．多くの日本企業においては昔から正しいことは今後も正しく，環境は変化しないという前提で意思決定が行われているようだ．だから革新的な技術を開発してそれを広めたいと考える技術者は，今自分が置かれている枠組みにとらわれずに別の方法を試すことが重要だと思う．

世界の人々が，生まれた環境，現在属している環境からの影響や制約を受けずに，自己の能力を最大限に発揮してその人でなければ創造することができないものを創造する機会，及びそのような人々の間で物理的に離れていても人脈を構築して共同で作業を行い，共同で行わなければ創造することができないものを創造する機会を得ることが理想である．インターネットが普及した現在，

SoftEther が普及すれば全ての人々にこのようなことを実現する機会を与えられると信じている．

参考文献

[1] 登 大遊, "SoftEther の内部構造", 情報処理学会誌「情報処理」, Vol.45, No.10, pp.1057-1062, 2004.
[2] Fielding, et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC2616, http://www.ietf.org/rfc/rfc2616.txt, 1999.
[3] PacketiX VPN 2.0 導入事例記事, ぷらっとホーム株式会社, http://www.plathome.co.jp/jirei/packetix_akindo-sushiro.html, 2006.
[4] Thomas Friedman, "The World Is Flat: A Brief History of the Twenty-First Century", ISBN 0-374-29288-4, 2005.

登 大遊（正会員）
E-mail: da.se@softether.co.jp
1984 年生まれ．ソフトイーサ社代表取締役．CYBERDYNE 株式会社情報通信担当顧問．筑波大学大学院システム情報工学研究科コンピュータサイエンス専攻博士前期課程（休学中）．2003 年に筑波大入学後，独立行政法人情報処理推進機構 (IPA) の未踏ソフトウェア創造事業未踏ユース部門に採択され VPN ソフトウェア「SoftEther」を開発．2004 年に筑波大学発ベンチャー「ソフトイーサ株式会社」を設立. 同社で PacketiX VPN を開発, 2005 年末に製品化. 著書「公式 SoftEther 活用ガイド」(2004 年),「XP 時代の VC++プログラミング」(2002 年),「DirectX 8.0 3D アクションゲーム・プログラミング」(2001 年)

投稿受付：2010 年 12 月 16 日
採録決定：2011 年 2 月 16 日
編集担当：竹内　郁雄（早稲田大学）
　　中田　登志之（日本電気）