サイバー・セキュリティーに対する ファーウェイの視点と取り組み

21世紀の通信技術とセキュリティー ——その現状と課題

ジョン・サフォーク
上級副社長｜グローバル・サイバー・セキュリティー責任者
ファーウェイ・テクノロジーズ

HUAWEI

目　次

1　はじめに 1

2　要　　旨 2

3　通信と21世紀の社会 4

3.1　深刻さを増すサイバー・セキュリティー問題 5

3.2　通信端末機器の普及とデータの増大がもたらす事態 6

3.3　サイバー犯罪の種類 7

3.4　グローバル・サプライチェーンの影響 8

3.5　デジタル世界におけるアナログな法律の限界 11

4　ファーウェイのアプローチ 12

4.1　全社のグローバル方針としてのサイバー・セキュリティー 12

4.2　内部からのセキュリティー設計
——「後付け」ではなく「ビルトイン」 14

5　成功への鍵は「協力」 18

6　共に前進する 19

7　ファーウェイについて 20

2012年9月

1　はじめに

本提言レポートは、サイバー・セキュリティーがテクノロジー、社会、私たちの日常生活に与える影響と、それに対するファーウェイの見解と取り組みをまとめたものです。

本レポートでは、サイバー犯罪の脅威となる者とステークホルダーを特定するとともに、拡大するグローバル・サプライチェーンがもたらす課題という観点に焦点を当てて、サイバー・セキュリティーの現状を概説します。

また、サイバー・セキュリティーやグローバル・サプライチェーンに関する課題にファーウェイがどのように取り組んでいるかを述べ、さらに業界全体でこうした課題にどう対処していくべきかについての提案も示します。サイバー・セキュリティーやグローバル・サプライチェーンに関わるリスクの軽減を積極的に図るためには、公共、民間を問わず、業界を挙げて透明性を確保し、公平に協調していくことが必要であると当社は考えます。

ファーウェイはグローバル企業として、世界規模で他の企業・機関と連携、協力し、イノベーションや国際標準の策定に積極的に取り組んでいます。その目的は、当社が提供するネットワーク・ソリューションやサービスにおいて、常にお客様の期待以上の完全性とセキュリティーを提供すること、さらにその先のエンド・ユーザーが求めている信頼性を確保することにあります。サイバー・スペースの将来をより安全で快適なものにするため、ファーウェイはさまざまな取り組みを進めています。本レポートは、こうした活動を広く知っていただくことを目的とし、企業や政府が世界的なサイバー・セキュリティー問題にどのように対処していくべきかについて、当社の見解を示します。

2　要　旨

つながったネットワーク社会

この20年間、商用インターネットの登場をきっかけに、世界規模のインタラクティブなデジタル・ネットワークが発展してきました。その結果、電子メールからウェブ・ブラウジング、ソーシャル・ネットワーク、オンライン・バンキング、オンライン・ショッピング、遠隔医療にいたるまで、さまざまなサービスが誕生し、一般のユーザーにも広く利用されるようになりました。

今やサイバー・スペースは新たな開拓領域となりましたが、これは私たちが慣れ親しんだ現実世界とは大きく異なっています。サイバー・スペースは、社会が機能するための「神経システム」となりつつあります。サイバー・スペース上の技術の開発はどの国でも重要視されており、デジタル・ネットワークの発展が社会の発展に直結しています。オープンなネットワークが情報の流通と共有化を促進し、より低コストで多くのイノベーションを生み出すことを可能にし、世界中の人々に身体的、精神的、経済的な恩恵をもたらしています。

ネットワーク技術というイノベーションは驚異的なものです。オープンなネットワークによって情報の入手や共有が容易になり、新たな発明を生み出す機会が格段に増えました。技術が普及するにつれてイノベーションのコストが下がり、消費者も、個人経営者や中小企業も、大企業と同じプラットフォームでイノベーションを生み出すことができるようになりました。

ネットワークの発展によって投資が促進され、新たな消費モデルが生まれたことが、グローバル規模での経済成長につながっています。オープンなネットワークが世界中をつなぎ、距離を超えた経済交流を可能にし、貿易の活性化を促しているのです。世界銀行の報告によれば、ブロードバンド普及率が10%上がるごとに、GDP（Gross Domestic Product：国内総生産）が1.38%上昇するとされています[1]。これは、情報技術が経済成長を後押しする重要な役割を果たしていることを示す一例です。

デジタル・デバイドを解消し、より多くの人たちに通信と情報システムにアクセスする手段を提供し、情報リソースを適切に分配していけば、地球上の誰もが情報技術の恩恵を受けられるようになります。ネットワークをオープンにしておくことで、人々に平等な情報アクセス手段がもたらされ、社会システムの改善や地域格差のない発展が可能になります。さらに、オープンなネットワークを通じた異文化交流により、さまざまな文化的背景を持つ人々の間で起きていた誤解や差別、対立が解消されることにもつながります。

デジタル革命とブロードバンド革命によって多大な利益が個人・企業・社会にもたらされている半面、荒らし、窃盗、スパイ、故意の破壊といった古くから存在する不正行為も、新たなデジタル環境に必然的に引き寄せられています。

ファーウェイは、世界140か国以上でビジネスを展開し、世界総人口の3分の1近くをつなぐグローバル企業として、これらの課題に積極的に取り組んでいます。世界有数のICT（Information and Communication Technology：情報通信技術）ソリューション・プロバイダーのひとつとして、当社はネットワーク技術のエキスパートであることに加え、世界中の人々の健康・安全・繁栄を支え、促進するテクノロジーの役割についても熟知しています。

残念なことに、サイバー・セキュリティーについては政治家や競合他社から否定的な発言がしばしば聞かれます。サイバー・セ

[1] http://www.broadbandcommission.org/Reports/Report_2_Executive_Summary.

キュリティー上の脅威について懸念を抱くのはもっともなことではありますが、否定的な態度を取り続けているだけでは、現実に直面している課題とそれらがもたらす真の脅威を見逃してしまうことになります。業界全体が抱える課題に対する効果的な解決策を世界規模で実現するためには、商業的・政治的な論戦ではなく、事実に基づく冷静な対話が必要です。

今や、世界人口の87%以上がモバイル・ユーザーであり、アップルのApp Storeは250億ダウンロード、グーグルのGoogle Play Storeは200億ダウンロードを突破しています[2,3,4]。このような状況において、サイバー・セキュリティーは世界中で喫緊の課題としてその重要性を増しており、合理的かつ普遍的な解決策が求められています。

テクノロジーの設計・開発・展開がひとつの国だけで完結する時代は終わりました。もはや、どの国も、どの大企業もシングル・ソーシング・モデルに固執することはできません。技術開発におけるエコシステムや設計概念は非常に複雑化しているため、あらゆる脅威を完全に阻止することは不可能です。

ICTソリューションの設計、開発、コーディング、製造には世界中の複数のサプライヤーが関わらざるをえません。こうしたソリューションが政府、企業、消費者にとって欠かせないものとなるにつれ、サイバー・セキュリティー問題の規模は急激に拡大しています。

サイバー・セキュリティーは、特定の国や企業の問題ではありません。これは世界共通の問題であり、リスク・ベースのアプローチ、ベスト・プラクティス、国際協力による対応が必要であるということを、政府・業界のあらゆるステークホルダーが認識しなければなりません。

最近のStuxnetやFlameといった非常に複雑で高度なウイルスの出現により、私たちは重大な意思決定を迫られています。サイバー犯罪を行う者が規制のない環境で自由に活動し、マルウェアを開発できる現状をこのまま放置するならば、私たちはサイバー戦争がもたらす最悪の結果を覚悟して、自分の身は自分で守るという現実を生きていかなければなりません。しかし、これに立ち向かおうとするならば、現実的な視点と強い決意を持ち、これまでも外交努力などで戦争を回避したきたように、すべてのステークホルダーの間で信頼と協力、連携体制を構築して、サイバー戦争の危機が勃発する前に国際的な法律・規範・標準・規約を制定することが必要です。

当社は、今後もテクノロジーによって全世界の経済・社会の向上を促進していくために、国際協調、オープンな姿勢、明確な相互信頼を支持します。

皆様も当社のこうした考えに賛同していただけることを願っています。

ファーウェイは、サイバー・セキュリティーに関して国際的合意を得た標準やベスト・プラクティスを支持・採用し、サイバー防衛の強化に向けた研究活動を支援することに全力を傾け、各国政府がファーウェイのセキュリティーに対する能力を評価できるように、これからもオープンで透明性の高いアプローチを採用してまいります。そして、これまで同様、お客様からのご理解とご支援のもと、当社のプロセス、テクノロジー、サイバー・セキュリティーへのアプローチの改善に努め、お客様と、さらにその先のユーザーの皆様にいっそうの価値を届けられるよう尽力してまいります。

---

[2] http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf
[3] http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html
[4] https://sites.google.com/a/pressatgoogle.com/google-i-o-press-2012/android

3　通信と21世紀の社会

信頼できるグローバルなエコシステムの構築に向けて

音声通信やデータ通信を行えることは、当たり前のように考えられがちです。ネットワークにいつでもアクセスでき、常時接続できることが期待されています。通信テクノロジーは私たちの社会生活に驚くほど深く浸透しています。日常生活の利便性は、私たちが日々使用しているシステムやアプリケーションの性能と利用可能性に左右されているのです。

政府機関、企業、消費者へのテクノロジーの普及率は急激に上昇しています。全世界のモバイル・ユーザー数は、2011年末までに59億6,000万人に達しました。これは、世界人口の86%に相当し、2010年から12.3%増加したことになります[5]。

通信の形態とインターネット・アプリケーションはますます多機能なものになり、急速に普及しています。例えば、米国におけるスマートフォンのマーケット・シェアは、2011年12月には47.8%でしたが、2012年3月には50.4%に達しました[6]。スマートフォンには多くの機能やアプリケーションが統合され、中でも連絡先、位置情報、写真、モバイル・バンキングなどの個人データを扱うアプリケーションが増えています。また、スマートフォン用アプリケーションの数自体も急増しています。アップルのApp Storeは250億ダウンロードの大台を突破しましたが、これはiPhone、iPod Touch、iPadユーザー1人あたり平均で79ダウンロードに相当します[7]。

こうした状況の中、悪質な目的での個人データの収集や、あるいは意図しない設計ミスが、ネットワークやユーザーに損害をもたらす可能性が生じています。

ソーシャル・ネットワークが世界的に発展したことで、個人情報に新たな問題が発生しています。ある調査によれば、イングランドとウェールズではFacebookに関連する犯罪件数が約1万2,300件に上っており、40分間に1件発生している計算になります[8]。これは、ソーシャル・ネットワーク自体の脆弱性によるというよりも、本来は悪意のないソーシャル・メディア・テクノロジーを不正な目的に使用することがいかに容易かを物語っています。

スマートフォンの利用が拡大するに従って、スマートフォンへの攻撃も増えています。実際、スマートフォンを標的にしたマルウェアは、2004年から2011年の間で600%増加しました[9]。

ビジネス機能の強化とユーザー・エクスペリエンスの向上に伴い、ICT関連ソフトウェアの複雑さと規模が急速に増大しています。ソフトウェアの規模と複雑さが増大すれば、それに応じてセキュリティー上の弱点も増加します[10]。

これまで、通信ネットワークのインフラストラクチャーは通信という目的に特化された閉じたものでした。しかし現在では、VoIP（Voice over IP）／IMS（IP Multimedia Subsystem）などの新たなサービスの発展に伴い、ネットワーク・インフラストラクチャーは第三者サービス・プロバイダーにインターフェースを提供しており、IPベースのオープンなシグナリング・プロトコルが使用されることが多くなっています。従来、通信機器は専用ハードウェアを使用することが一般的でした。しかし現在では、共通のイン

[5] http://www.itu.int/ITU-D/ict/statistics/
[6] http://techcrunch.com/2012/05/07/nielsen-smartphones-used-by-50-4-of-u-s-consumers-android-48-5-of-them/
[7] http://www.guardian.co.uk/technology/appsblog/2011/jul/07/apple-iphone-app-store-downloads
[8] http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html
[9] F-Secure Mobile Threat Report Q4 2011
[10] Alhazmi OH et al., Measuring, analyzing and predicting security vulnerabilities in software systems, Computers & Security (2006), doi:10.1016/

フラストラクチャー・コンポーネントとオペレーティング・システムをベースにした機器が増えており、このようなATCA（Advanced Telecommunications Computing Architecture：アドバンスト・テレコム・コンピューティング・アーキテクチャー）プラットフォームの出荷数は、2008年から2011年で10倍になりました。また、ATCAのエコシステムに参加する企業の数も100社を超えています[11]。

データ通信やオンライン・アプリケーションへのアクセスを安全に行うことができなければ、ユーザーの信頼を得ることはできません。ファーウェイは通信テクノロジーを支える役割を担う者として、信頼の維持に努め、サイバー問題に対応できるよう他企業・機関との関係性や業務プロセス、セキュリティーへのアプローチを絶えず進化させていく必要があると考えています。

3.1　深刻さを増すサイバー・セキュリティー問題

サイバー・セキュリティーへのアプローチは、当初はネットワークとデータの保護を目的としていましたが、この10年でサイバー犯罪をはじめとしたオンラインでの悪意ある行為からの防衛戦へと発展しました。テクノロジーが広く普及し、政府・企業の業務や消費者の日常生活に深く浸透するにつれて、犯罪者がサイバー犯罪から得られる潜在的利益も大きくなっており、その動機が高まっています。加えて、サイバー・スペースへの接続性が向上し、よりアクセスしやすくなったことで、サイバー犯罪の手段と機会も増加しています。インターネットが普及する以前は、コンピューターを使う人が限られていたため、攻撃によって得られる利益はそれほど大きくありませんでした。しかし、現在ではモバイル機器からインターネットに簡単にアクセスできるようになり、多くの人がネットワークを利用できる環境にあります。そのため、サイバー・スペースは個人や商用を問わずさまざまな目的で使われるようになりましたが、同時に悪意ある利用も増加してきました。

デンマークのコンピューター・セキュリティー・サービス・プロバイダーであるセキュニア社でリサーチ・アナリスト・ディレクターを務めるステファン・フレイ博士は、RSAカンファレンスのプレゼンテーションの中で、サイバー犯罪者が興味本位でハッキングを行うスクリプト・キディー（「幼稚なハッカー」の意）から、個人的利益のために他者からの依頼を受けてハッキングの実行手段を開発するエキスパートへと移行しつつあると指摘しています[12]。金銭その他の利益が得られるところには、必ず犯罪が存在します。テクノロジーも同様であり、場合によっては犯罪を助長することもあります。

グローバル・テクノロジー企業は、以下のような悪意ある利用からテクノロジーを保護しなければなりません。

- 妨害行為への利用: ネットワークやインフラストラクチャーに対する制御したり、麻痺させたり、干渉したり、停止させたりすること
- スパイ行為への利用: 第三者のテクノロジーにより個人や組織に対して違法なスパイ行為をさせること
- 特定の国家や集団の手先となること: 特定の国家や集団によってグローバル企業の他国での機能を悪用され、他の国家・地方政府、組織、個人への攻撃に利用されること
- 予防策・予防能力の欠如につけこまれること: サイバー犯罪者がベスト・プラクティスやエンド・ツー・エンドのサイバー・セキュリティー対策の欠如を狙って企業の機能やテクノロジーを違法または不適切な目的に利用すること

テクノロジーを開発・サポートするすべての企業が、潜在的な脅威や実際の脅威に対応するリスク情報活用メカニズム、対抗策、方針、手順を整備することも必要です。現在のところ、次のような脅威が存在することが知られています。

- ハードウェア・ソフトウェアの「キル・スイッチ」（固定または遠隔制御による）
- バックドア、トロイの木馬、ウイルス、ソフトウェア・ロジックボムを介した制御

---

[11] http://www.heavyreading.com/details.asp?sku_id=2228&skuitem_itemid=1111
[12] http://secunia.com/resources/reports/?action=fetch&filename=Secunia_Moving Target_presentation_RSA2012.pdf

- 企業、個人、集団に対するネットワークの停止、スパイ・妨害行為の実行、第三者による違法行為の幇助の指示
- データ（技術情報、国家機密情報、商業機密情報、秘密データなど）へのアクセス
- データや制御権を他の国家や集団に移す「コール・ホーム」／盗聴機能の組み込み
- 研究開発プロセスにおける人的脅威の送り込みやソ不正フトウェアのインストール
- サプライチェーンにおける不正コンポーネントの混入
- 個人に対する賄賂
- オンサイト・サポートに対する 人的脅威の送り込み、賄賂、または不正ソフトウェアのインストール

上記のように、テクノロジー・ベンダーのハードウェアとソフトウェアは、さまざまな方法で悪用される可能性があるため、各社は自社の技術とその脆弱性の評価を継続的に行っていく必要があります。ファーウェイは、上記の脅威をひとつずつ検証し、「脅威者がこうしたサイバー攻撃を行うには何が必要か？」「より安価で、発覚するリスクが低く、成功率の高い攻撃方法はどれか？」を考慮し、そうした攻撃の発生を回避する最適な手段を探ります。想定範囲を限定することなく、常に警戒を怠らず、あらゆる可能性を考慮したチェック体制をとっているのです。

3.2　通信端末機器の普及とデータの増大がもたらす事態

サイバー・セキュリティーが過熱報道されていることから、「データや知的財産の損失」は、従来の紙ベースの時代には見られなかった新しい現象のように思われるかもしれません。しかし、こうした事態は言うまでもなく古くから存在し、今に至るまで続いています。

わかりやすい例として、離職者が顧客リスト、将来の製品ポートフォリオ、製品価格決定モデル、次期製品の設計図などを持ち出すケースが挙げられます。テクノロジーによって膨大な量のデータの持ち出しが素早く、低コストで、さらには遠隔操作でも実行できるようになったことが、こうした不正行為を助長しています。最近の調査によると、ヨーロッパではデータ保護法で禁止されているにもかかわらず、企業に勤める回答者の32%が転職時に情報を持ち出したことがあると答えており、そのうちの51%が機密情報を含む顧客データベースを持ち出したという結果が出ています[13]。

こうしたデータ流出のコストは、悪意のない単純なものから大規模な産業スパイ行為まで含め、数十億ドル単位にのぼると言われています。もちろん、正確な損失額を算出することは不可能です。サイバー・スパイ行為によって資産価値が損なわれた企業を特定することは困難ですし、潜在的損失に対して外部監査を行う企業や、信認義務の一環として取締役会が株式市場に報告をしている上場企業も見当たりません。しかし、まずは現実として起きている事態を受け入れなければ、具体的な対策も検討できず、過剰な規制によって本来テクノロジーがもたらしてくれる恩恵を犠牲にすることにもなりかねません。

テクノロジーがもたらした変化は他にもあります。今や、データの保存、商取引の処理、事業の運営はほぼ全面的にテクノロジーに依存しており、人々の日常生活にもテクノロジーが欠かせないものとなってきました。その結果、保存されるデータの量は急速なペースで増加し続けています。

[13] http://www.businesscomputingworld.co.uk/when-employees-leave-your-company-so-does-your-data/

人々はますます多くの通信機器を所有し、それらを相互に接続するようになっています。先進国では携帯端末の普及率が国民数を上回る例も珍しくなく、そうした端末機器の1台1台がデータを保存する場所となっています。すなわち、データを消失する機会もそれだけ増えているということです。インフラストラクチャーからのデータの窃盗、データの完全な破壊や一部改ざんを狙う者にとって、これらの機器は潜在的なエントリー・ポイントになり得ます。こうした脅威が、データの保存に対するユーザーの信頼を著しく損なうことになります。

保存されている血液型データが手当たり次第に改ざんされたり、銀行取引の金額がでたらめな数字に改ざんされたりする恐怖を想像してみてください。このようなケースは目立ちにくく、追跡が難しいため、修復も困難です。こうした事態が起これば、一般市民は公共機関に対する信頼を失ってしまうでしょう。

もちろん、攻撃はランダムな改ざんだけにとどまりません。何者かが車の制御技術をハッキングし、テキスト・メッセージを介してエンジンの始動や停止を操作することも考えられます[14]（こうした脅威への対策に本格的に乗り出している企業もあります[15]）。あるいは、サイバー・テロリストが配電網をハッキングすることも実際にあり得ます。RUSI（Royal United Services Institute）ジャーナルに掲載された論文「Cyber-Weapons（サイバー兵器）」（リッド、マクバーニー著）はこのようなシナリオを詳細に検討し、重要なインフラストラクチャーに対するリモート・アクセスの仕組みと不正利用の可能性を解説しています[16]。

また、より身近なシナリオとしては、スマートフォン・アプリケーションをダウンロードし、要求されるままに「信頼状態」と保存データへのアクセスを許可した途端に、スケジュール表、連絡先、電子メール、テキストが（おそらく暗号化されていない状態で）遠く離れたサーバーにアップロードされ、その後どんな目的で使われるかもわからず、それどころかデータが抜き取られたことさえ気づかない、といった事態が考えられます。

3.3 サイバー犯罪の種類

まず、私たちが暮らすサイバー・スペースにどんな「敵」が存在するのかを知ることが重要です。主に以下のようなサイバー犯罪者が存在することが考えられます。

- 嫌がらせ、脅迫、いじめ、児童の性的搾取などを行う個人
- ハクティビスト（政治的ハッカー）と呼ばれる、独自の主張を持ち、自らの理念を広めるためにハッキングを行う個人または集団
- 不正取引、偽造行為、産業スパイなどのさまざまな犯罪行為をする犯罪組織（および無秩序な犯罪者集団）
- その定義を問わず、危害を加えることを目指すテロリスト
- 諜報手段のひとつとしてテクノロジーを利用し、諜報対象に関するデータや情報を収集する政府工作員
- 自らの利益のために、特定の国家や競合他社から最先端情報を入手しようとする産業スパイ

生活の場や労働環境におけるリスクのひとつとして、誰もが技術セキュリティーの問題について考えなくてはなりません。世界をつなぐネットワークが拡大を続け、政府、企業、消費者がテクノロジーへの依存を強める中、問題の規模は大幅に拡大しています。

---

[14] http://www.securityweek.com/car-hacking-researchers-highlight-emerging-risks-and-lack-security-automobiles
[15] http://www.reuters.com/article/2012/08/20/us-autos-hackers-idUSBRE87J03X20120820
[16] http://dx.doi.org/10.1080/03071847.2012.664354

これまでに全世界で失われた機密データの数はおそらく世界人口を上回っていると推測され、セキュリティー侵害の規模は想像を超えて拡大しています。世界のどこかで重要インフラストラクチャーがサイバー犯罪者の攻撃を受けた、あるいは攻撃の危機にさらされているという報告を聞かない日はほとんどありません。

多くのテクノロジーが出現し、それらが相互に接続されて利用・共有されるにつれて、私たちは個人データや企業データの取り扱い、使用するテクノロジーに対して注意を払わなくなってきています。こうした無関心な態度は、自分たちの生活におけるデータの重要性を軽視していることの表れであり、それがセキュリティー・リスクを高めているのです。

世界的なセキュリティー・ソフトウェア・ベンダーの主張によると、今こうしている間も1秒間に12種類のマルウェア・テクノロジーが新たに生まれていると言います[17]。また、ある業者を使えば、249米ドル（約1万9,422円※）で誰でも独自のマルウェアを入手することができ、これにはサービス水準合意に加え、購入したマルウェアが9か月以内にアンチウイルス・ソフトウェアによって検出された場合の交換保証まで付いているとされています。

各国政府が自国に対するハッキング行為を声高に非難していることを考えると、サイバー・スペースの犯罪者リストに政府を加えることは間違っているように思われるかもしれません。しかし、歴史を通じて、スパイ活動が外交関係において良くも悪くも一定の役割を担ってきたという事実を踏まえなくてはなりません。フォーブス誌は、「Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)（あなたのPCに侵入するツールをスパイに売って荒稼ぎするハッカーたち）」と「Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits（ゼロデイに備えて：ハッカーの秘密兵器の値段）」という最近の記事の中で、ゼロデイ・エクスプロイト（セキュリティー脆弱性が発見されてから、その情報や対策が公開される前に攻撃を行うプログラム）の発見・販売で活況を呈している産業があることについて、詳しく解説しています。同記事では、世界中の政府がゼロデイ・エクスプロイトを頻繁に購入していることに加え、防衛関連の大手請負業者もゼロデイ・エクスプロイトの売買を行っていることも指摘しています[18,19,20,21]。もし本当に政府がゼロデイ・エクスプロイトの取得に関与しているとすれば、あるいはFlameやStuxnetなどの攻撃ソフトウェアの開発や「兵器化」を進めているとすれば、自業自得であると言わざるをえません。

3.4 グローバル・サプライチェーンの影響

今や、スマートフォン、タブレット、パーソナル・コンピューター、テレビ、白物家電はいずれも、グローバル・サプライチェーンの存在なしには製造できません。グローバル・サプライチェーンを支える国のひとつ、台湾では、ノートブック・コンピューターは0.35秒に1台、PDAは8.54秒に1台、デスクトップ・コンピューターは0.68秒に1台の割合で生産されています[22]。

米国では、GAO（Government Accountability Office：政府監査院）が2012年3月に公開した報告書の中で、IT製品のグローバル・サプライチェーンが国家安全保障を危険にさらす恐れがあるとして、次のように警告しています。

> 「各連邦政府機関は、それぞれの職務の遂行において、コンピューター化された情報システムおよび電子データに大きく依存している。グローバル・サプライチェーンを通じたIT製品やサービスの悪用は、政府機関の機密に関わる重要なネットワークとデータの機密性、完全性、可用性を低下させる恐れのある新たな脅威である」[23]

---

[17] http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=2011_in_numbers&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17

[18] http://www.bbc.co.uk/news/technology-12633240

[19] http://www.dailytech.com/CBS+US+Israel+Opened+up+Cyberwarfare+Pandoras+Box+with+Stuxnet/article24155.htm

[20] http://www.europeaninstitute.org/EA-November-2011/main-cyber-threats-now-coming-from-governments-as-state-actors.html

[21] http://news.cnet.com/8301-1009_3-57445975-83/flame-a-glimpse-into-the-future-of-war/

[22] http://www.taiwan-technology.com/edit/p/epaper/200902180.htm

[23] http://www.gao.gov/assets/590/589568.pdf

※1米ドル78円換算

この報告書では、エネルギー省、国土安全保障省、司法省、国防総省の当局者がGAOの査察官に対し、通信ネットワークに海外開発の機器、ソフトウェア、サービスがどの程度含まれているかを把握していないと語ったとされています。同報告書によれば、エネルギー省と国土安全保障省は、サプライチェーンの保護対策を規定していません。一方、司法省は保護対策を規定しているものの、実施に移していないか、対策の遵守状況の監視手順を策定していません。

この報告書は、「海外開発」の意味を定義していないように見受けられます。また、通信ネットワークだけを取り上げていますが、本来はあらゆる技術におけるあらゆるベンダーについて考慮するのが適切なはずです。

実際には、ラップトップひとつを取ってみても、カナダ、アイルランド、ポーランド、イタリア、チェコ共和国、スロバキア共和国から、さらには中国、イスラエル、日本、マレーシア、フィリピン、シンガポール、韓国、台湾、タイ、ベトナムなど、世界中からの部品が使用されている可能性があります。

中国の成都（Chengdu）に登記している企業1万6,000社中820社は、外資系企業であり[24]、そのうちの189社はフォーチュン500企業です。いくつか例を挙げると、インテル、マイクロソフト、SAP、シスコ、オラクル、BAE、エリクソン、ノキア、ボーイング、IBM、アルカテル・ルーセントなどの著名企業が成都に拠点を構えています。これらの企業の製品は、「海外開発」とみなすべきなのでしょうか？

シスコは中国の主要6都市に研究開発センターを置いており、シスコ製品全体の25%以上が中国のパートナー企業によって生産されています。また、同社は160億米ドル（約1兆2,480億円※）規模の投資を中国国内で行う計画を発表しています。この計画には、ネットワーク技術者10万人に対するトレーニングのほか、全国300か所の専門学校内にネットワーキング技術を指導するためのセンターを開設することなどが含まれています[25]。シスコのジョン・チェンバースCEOは、「当社が行おうとしていることはすべて、中国企業化という全体的な戦略の一環です」と述べています[26,27]。

各社の報告書によれば、主要通信機器プロバイダーはいずれも中国国内に拠点を置いています。アルカテル・ルーセントの海外製造の3分の1は上海ベルによるものです[28]。エリクソンの合弁会社である南京エリクソン・パンダ・コミュニケーションズは、エリクソンにとって世界最大のサプライ・センターとなっています[29]。また、ノキア・シーメンスは2011年末の時点で10の海外製造拠点を擁していますが、そのうち5か所が中国（北京、上海、天津、杭州、蘇州）に、2か所がインドにあります[30]。

このような企業が開発した製品は、「海外開発」にあたらないのでしょうか？

インドでは、この20年間で国際的企業の進出とサポート・サービスの成熟が進んでおり、全世界の企業にテクノロジーを提供しています。数字だけを見ても、インドのIT産業の総輸出額は、2011年度実績で590億米ドル（約4兆6,020億円※）に上っています。また、世界経済の低迷にもかかわらず、2007～2011年度のCAGR（Compound Annual Growth Rate：年平均成長率）は16.4%と目覚ましく[31]、タタ、ウィプロ・テクノロジーズ、インフォシス・テクノロジーズ、HCLテクノロジーズなど、世界に名だたるIT企業を輩

---

[24] http://www.chengduhitech.co.uk/Default.asp
[25] http://www.usatoday.com/tech/products/2007-11-01-425344141_x.htm
[26] http://www.epi.org/publications/trade_policy_and_the_american_worker/
[27] http://news.xinhuanet.com/english/2005-06/17/content_3096764.htm
[28] http://www.alcatel-sbell.com.cn/Default.aspx?tabid=262&ArticleID=1173
[29] http://www.ericsson.com/cn/thecompany/ericsson-china/background-china
[30] http://i.nokia.com/blob/view/-/1015984/data/3/-/form20-f-11-pdf.pdf
[31] http://www.ibef.org/industry/IT-ITeS.aspx

出しています。そのほかにも、シーメンス、HP、フィリップス、ABB、フレクストロニクス、AT&Tといった世界的な企業がインドに拠点を構えています。シスコはインドでR&D、セールス、ビジネス・サポートにおいて8,000名を超える従業員を雇用しており、18の流通センターと、大規模なカスタマー・サポート・システムを持っているほか、バンガロールのシスコ・グローバル開発センターは米国外で最大の開発拠点となっています。また、バンガロールのウィプロ・テクノロジーズとインフォシス・テクノロジーズ、チェンナイのHCLテクノロジーズ、プネーのゼンサー・テクノロジーズとともに共同開発センターも設立しています[32]。

つまり、高度にグローバル化した今日の世界では「海外開発」という概念はすでに意味をなさず、地球上の一地域にある企業やそこで作られた製品が別の地域の企業や製品と比べて信頼性に劣るといった考えも適切ではないと言えます。こうした発想は、国家の安全保障を装った保護貿易主義と言ってもよいでしょう。グローバル化した世界では、サプライヤーがどの国の企業か、どこに本社を置いているのかだけを基準にしたサイバー・セキュリティー対策は、何の効力も持たないのです。企業の国籍のみに基づいてその企業を排除するというアプローチは、論理性を欠くばかりか、差別的であり、最恵国待遇の原則にも反することになります。

マイクロソフトが発表している「Cyber Supply Chain Risk Management: Towards a Global Vision of Transparency and Trust（サイバー・サプライチェーン・リスク管理：透明性と信頼についてのグローバルなビジョン構築に向けて）」と題した文書には次のような説明があり、ファーウェイもその考え方を全面的に支持しています。

> 「まず、ベンダーには、サプライチェーンを悪用しようとする各国政府の目論見を拒否する大きな経済的インセンティブがあります。その理由はきわめて単純です。バックドアなどの意図的な欠陥が発見され、公表されるリスクは高く、そうした事実が発覚すれば企業は社会的信頼を失い、最終的にマーケット・シェアを失うことになるからです。特に信頼の喪失が世界的規模に及ぶということを考えれば、そうした行為に意図的に加担した企業は倒産に追い込まれる恐れすらあります。たとえ敵対する外国政府に対して利用する意図で秘密のバックドアが仕込まれたとしても、そうした製品は当該ベンダーの本国の国民にさえ排斥される可能性が高いのです。多くの国では、外国による監視だけでなく、国家権力による監視も懸念する声が国民の間にあるからです」

そして、次のように結論付けています。

> 「政府の懸念は理解できるものの、政府の対応がイノベーションと競争を抑制し、全世界のICT産業の活力を脅かすことのないようにする必要があります」[33]

現実には、複数のサプライヤーの機器をテクノロジー・インフラストラクチャーに接続した場合、それらの機器とソフトウェアは、世界数十社の企業によって設計・開発・製造されたものである可能性があります。

ジョージ・H・W・ブッシュ政権下でCSG（Counter-terrorism Security Group：テロ対策安全保障グループ）議長と国家安全保障会議委員だったリチャード・クラーク氏は、クリントン政権にも参加したほか、2002年にはジョージ・W・ブッシュ大統領のサイバー・セキュリティー担当特別補佐官となり、2003年2月に発表された「サイバー・スペース安全保障のための国家戦略」の草案作成に関わった重要インフラ保護委員会の議長も務めました。クラーク氏はICTグローバル・サプライチェーンの問題について、次のように要約しています。「私の考えでは、ニューヨークで開発されたものであろうと、上海で開発されたものであろうと、ソフトウェアに潜むリスクはおそらく同じです。米国にも賄賂で買収できる人間がいるからです」[34]

---

[31] http://www.ibef.org/industry/IT-ITeS.aspx
[32] http://www.cisco.com/web/IN/about/company_overview.html
[33] http://www.microsoft.com/en-us/download/details.aspx?id=26826
[34] http://www.networkworld.com/news/2011/091911-clarke-cybersecurity-251014.html

※1米ドル78円換算

3.5 デジタル世界におけるアナログな法律の限界

サイバー・セキュリティーは地球規模の問題です。データの転送や処理は地球規模の活動であり、データは国境、政府の領有支配権、裁判所の領域的管轄権に関係なく移動します。米国内で行ったインターネット検索は、米国内のサーバーで処理されることもあれば、ヨーロッパやアジアのサーバーで処理されることもあります。しかし、法的規制・制度はそうした国境や管轄を基礎として整備されているため、多国籍企業にとって大きな問題となっています。

ICT業界に影響する代表的な法律であるデータ保護法とプライバシー法を例に取ってみましょう。ヨーロッパでは、EUデータ保護指令においてデータ保護法に対する統一的アプローチが規定されているものの、指令の施行は加盟27か国の間で大きく異なります。米国の場合、プライバシー法は連邦政府レベルと州政府レベルに分かれています。連邦法は特定業種を対象にしており、金融、医療といった特定の業界におけるプライバシーを保護する法律は存在しますが、包括的なプライバシー法はありません。州政府もプライバシー法を制定していますが、各州によってばらつきがあります。例えば、ほぼすべての州が独自のデータ・セキュリティー侵害通知法を制定しており、侵害通知の内容に関する義務や通知先（規制当局、州検事総長、または信用調査機関）は州ごとに大きく異なります。

多くの国や地域（オーストラリア、インド、中国、アルゼンチン、マレーシア、香港など）では、法律上の義務や法律の施行に格差が存在し、ひとつの国の中でも地域間で法律の施行や解釈が異なる場合があります。また、標準や規約は制定されているものの、法制化されていない国では、企業はさらなる課題に直面することになります。

つまり、ファーウェイのような機器ベンダーを含め、すべての企業とその法人顧客は、地域間だけでなく、対象分野間でも義務が異なるばらばらな法規制への対応を迫られるということです。法規制によって課される監視・傍受に関する義務は、業界標準に影響を与えます。そのため、機器メーカーが製造する機器は、数多くの業界標準と法律に適合していなければなりません。さらに、法律が変わる可能性があることも課題となります。法律が改正された場合、新しい法的要件に合わせてハードウェア・ソフトウェアを修正しなければならないからです。

ファーウェイは、データ保護およびサイバー・セキュリティーの原則に対する国際的な協調姿勢を歓迎する立場です。ベンダー、サービス・プロバイダーなどの法人が各国間で一貫性のない標準やアプローチの適用に努めるよりも、協調姿勢をとるほうが、データ保護の全体的な水準の向上が地球規模で促進されるはずだと考えます。前述のとおり、当社のような機器メーカーは複雑な法規制環境で事業を運営しています。ファーウェイは、事業を営むすべての管轄区域において、適用されるあらゆる法規制の遵守に全力で取り組んでおり、国際制裁や地域法が求めるところに従って適切な事業運営を維持してまいります。

4　ファーウェイのアプローチ

サイバー・セキュリティーは、短距離走ではなくマラソンです

ファーウェイは、自社の伝統を大切にし、起業家精神に富んだ創業者が偶然にも中国の出身者であることを誇りとしています。しかし、それがほかのどの国の出身であったとしても、同じように誇りに思うでしょう。

通信インフラストラクチャーの複雑さ、サプライヤーの多様性、急速な開発によって生じる技術的脆弱性、変化する法的義務や規制への適合の難しさのために、サイバー・サプライチェーンのリスク管理は非常に難しい課題となっていますが、当社の経験では、これは克服できない問題ではありません。ファーウェイの商業的価値のひとつは、従業員持株制度による完全な民間企業として事業の独立と政治的な独立を維持していることです。中国に本社を置く世界的規模の企業として、当社はサイバー・セキュリティー保証において常に一歩先を行く必要があると考えています。ファーウェイは、特定の国家、企業、個人に関連する機密情報を取得する意図を持つ行動を支援、容認、実行することは決してありません。また、当社の技術が違法な目的に使用されることを知りながら許容することも絶対にありません。

ファーウェイはこの問題に継続的に取り組み、お客様および政府などのステークホルダーが求める最高級の製品とサービスを提供することで、お客様のニーズを満たしていくよう最大限努力しています。ファーウェイは、実現しうる最高のセキュリティー保証によってサイバー・ワールドをすべての人々にとってより安全で安心できるものにするために、他社との協力のもと多くのリソースを投入して改善に取り組んできました。

4.1　全社のグローバル方針としてのサイバー・セキュリティー

地域の政治状況や商業環境により、現地あるいは欧米の製品の購入が推進されている市場が少数ながら存在しています。こうした市場でお客様から十分な信頼を得るためには、自社製品とプロセスの独立した評価と、徹底したローカリゼーションを通じて、供給とサポートの流れに対して高レベルでのセキュリティー保証を維持する必要があることをファーウェイは常に念頭においてきました。

ファーウェイは、エンド・ツー・エンドのグローバル・サイバー・セキュリティー保証システムを確立し、運用しています。サイバー・セキュリティーへの取り組みは、商業的利益の追求よりも常に優先されます。お客様のネットワークとビジネスの安定と安全を（とりわけ、地震や津波などの自然災害時にも）確保することがファーウェイの第一の責務であり、事業指針でもあります。ファーウェイは、サイバー・セキュリティーについての懸念が通信業界と社会全般において増大していることを深く理解しています。

前述のマイクロソフトの文書（p.10）に挙げられていたような理由から、ファーウェイはこれまで特定の国家に損害を及ぼしたり、国家機密や企業秘密を盗み出したり、個人のプライバシーを侵害したりすることは決してなく、今後もそのような行為を支持・容認することは絶対にありません。また、ある地域で違法となるような行為を行おうとするいかなる個人・組織も支持することはありません。当社が世界中から注視されており、外部からの監査や調査を積極的に実施しているという状況で、こうした悪意ある行為を行おうとする者は、もっと知名度の低い企業を選ぶことでしょう。

ファーウェイは、通信業界がこのような問題にとりわけ敏感であること、また先進的なテクノロジーには脆弱性が伴うことを理解しています。ファーウェイのエンド・ツー・エンドのグローバル・サイバー・セキュリティー保証システムは、企業の方針、組織、プロ

セス、経営、技術、仕様のすべてにわたって適用されるものです。ファーウェイは、自社の製品とソリューションの安全性を向上させるため、1999年に当社初の安全技術規則集を発行し、サイバー・セキュリティーに対する取り組みを開始しました。創業者兼CEOである任正非（Ren Zhengfei）は、2011年4月に、当社の取り組みを一層強化するために「グローバル・サイバー・セキュリティー保証システムの確立についての声明」を以下のとおり発表しています。

世界的な通信ソリューション・プロバイダーであるファーウェイは、サイバー・セキュリティーの重要性を十分に認識し、各種政府機関およびお客様のセキュリティーに関する懸念を理解しています。通信業界と情報技術の絶え間ない発展とともに、セキュリティー上の脅威と課題は増大し、サイバー・セキュリティーへの関心が強まっています。こうした状況の中、ファーウェイはサイバー・セキュリティーを優先課題とし、以前から当社の製品・サービスのセキュリティー改善に向けて実施可能で効果的な手段を採用することに注力してきました。このような取り組みを通じて、お客様のセキュリティー・リスクの低減と回避を支援するとともに、当社の事業に対する信頼を築いてきたのです。ファーウェイは、オープンかつ透明で目に見えるセキュリティー保証の枠組みを確立することが、通信業界の健全で持続可能な発展と技術革新につながると確信しています。また、これによってさらにスムーズで安全性の高い通信をユーザーに提供することも可能になります。

このような観点から、ファーウェイは、関係する国や地域の法律、規制、規格の遵守に基づき、また業界のベスト・プラクティスを参照することにより、エンド・ツー・エンドのサイバー・セキュリティー保証システムを確立し、今後もこれを継続的に最適化していくことを宣言します。このシステムは、全社方針、組織構造、ビジネス・プロセス、技術、標準的業務の側面を包括するものになります。ファーウェイは、政府、お客様、パートナーと協力し、オープンで透明な姿勢でサイバー・セキュリティーの課題に積極的に取り組んできました。サイバー・セキュリティーへの取り組みは最重要事項であり、自社の商業的利益をこれに優先させることは決してありません。

組織面では、最高レベルのサイバー・セキュリティー管理組織としてGCSC（Global Cyber Security Committee：グローバル・サイバー・セキュリティー委員会）を置き、サイバー・セキュリティー保証方針を承認する責任を負います。GCSCの重要なメンバーであるGCSO（Global Cyber Security Officer：グローバル・サイバー・セキュリティー責任者）が、方針の策定とその実施の管理・監督を担当します。この方針は、ファーウェイの世界中のすべての部門で採用され、一貫して実施されることになります。またGCSOは、ファーウェイと政府、お客様、パートナー、従業員を含むすべてのステークホルダーとの間の効果的なコミュニケーションを促進する責務も負っています。GCSOは、ファーウェイのCEOに直属します。

ビジネス・プロセスにおいては、研究開発、サプライチェーン、販売とマーケティング、デリバリー、技術サービスに関連するすべてのプロセスにセキュリティー保証を統合します。このようなセキュリティー保証の統合は、品質管理システムの基本的要求事項であり、管理規則と技術仕様書の指定に従って実施されます。さらに、サイバー・セキュリティー保証システムの実施について内部監査を行い、外部認証を取得するとともに、セキュリティー機関や独立した第三者機関にも監査を依頼し、確実な運用を目指します。ファーウェイはすでに2004年からBS7799-2／ISO27001の認定を受けています。

人材管理に関しては、当社が作成したサイバー・セキュリティー方針および要求事項を遵守することを従業員、協業者、コンサルタントに義務づけ、セキュリティーに対する考え方をファーウェイ全体に深く定着させるためのトレーニングを行います。また、サイバー・セキュリティー保証に積極的に貢献している従業員を表彰するとともに、方針に違反した従業員に対しては適切な処置を取ります。従業員が関連する法規に違反した場合には、個人的な法的責任を負う可能性もあります。

当社はオープンで透明かつ真摯な姿勢を保ち、さまざまなチャネルを通じて各種政府機関、お客様、協業者と進んで協力し、サイバー・セキュリティー上の脅威や課題にともに取り組んでいきます。また、一部の地域ではセキュリティー認証センターを設立します。認証センターは現地の政府およびお客様と透明性の高い関係を維持し、現地の政府に委任された検査員による製品検査を実施することで、ファーウェイの製品とサービスの安全性を保証します。

ファーウェイは、ITU-T（International Telecommunication Union - Telecommunication Standardization Sector）、3GPP、IETF（Internet Engineering Task Force）などが推進する通信サイバー・セキュリティー標準化の活動に積極的に関与し、FIRST（Forum of Incident Response and Security Teams）などのセキュリティー機関に参加し、主要なセキュリティー企業と提携することで、当社のお客様のサイバー・セキュリティーの保証と、業界の健全な発展を促進してきました。

このようなサイバー・セキュリティー保証システムは、ファーウェイ・ホールディング株式会社、およびその直接的または間接的管理下にあるすべての子会社と関係会社に適用されます。この宣言は、上記すべての関係者が認識するべきものとして作成されました。

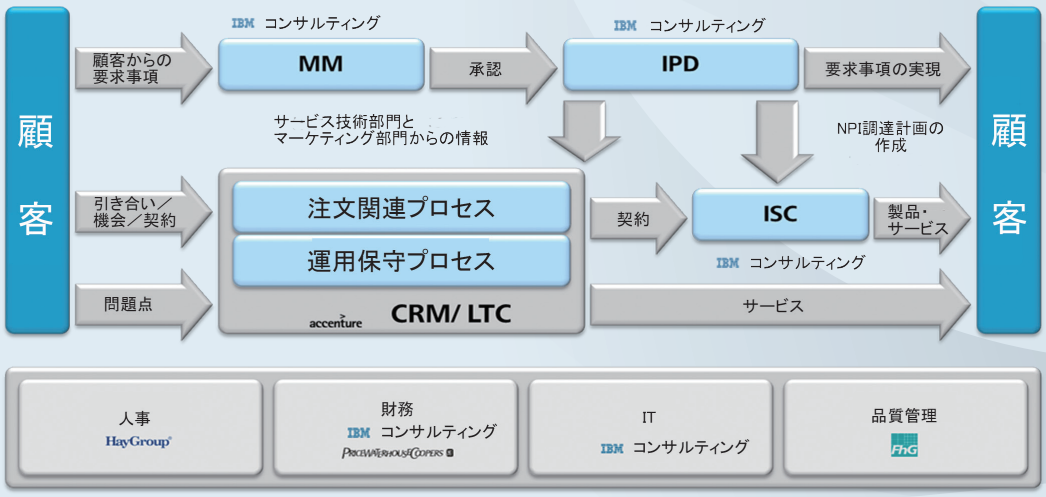
この宣言は、各地域の法律および規則に準拠すべきものであり、この宣言と各地域の法律および規則との間に何らかの不一致がある場合は、後者が優先されるものとします。ファーウェイは、この宣言を毎年見直し、法律および規則との整合性を保つものとします。

2011年4月25日　ファーウェイCEO 任正非

4.2　内部からのセキュリティー設計 ——「後付け」ではなく「ビルトイン」

多くの企業が品質や技術革新について語りますが、革新的で高品質な製品やサービスを提供しつづけるためには、世界規模で一貫して展開できる標準化されたプロセスが必要です。こうした取り組みがなければ、個々の案件、製品、顧客とのやりとりは、良い時もあれば悪い時もあるという、品質が一定しないものになってしまいます。ファーウェイは、標準化されたプロセスを基盤として、一貫した品質の製品とサービスを提供するプロセス・ベースの組織になるため、1997年以来IBMから支援を受けてきました。

当社のプロセス・マップを以下に示します。図に示すとおり、当社では世界で最も革新的かつ専門的な複数の組織に支援を依頼しています。プロセス化と情報技術についてはIBM、顧客関係管理についてはアクセンチュア、人事についてはヘイ・グループ、財務についてはプライスウォーターハウスクーパーズにコンサルティングを依頼し、外部監査機関にはKPMGを採用しています。



LTC: 引き合いから入金まで｜IPD: 統合製品開発｜MM: 市場管理｜ISC: 統合サプライチェーン｜CSR: 顧客サービス要求｜ITR: 問題から解決まで

サイバー・セキュリティー上の要求事項を満たすために、当社はすべてのプロセス、基準計画、方針、標準に、必要なベスト・プラクティスを組み込んでいます。ファーウェイではサイバー・セキュリティーを後付けの方策とするのではなく、日常業務に統合しており、これは当社のDNAの一部です。

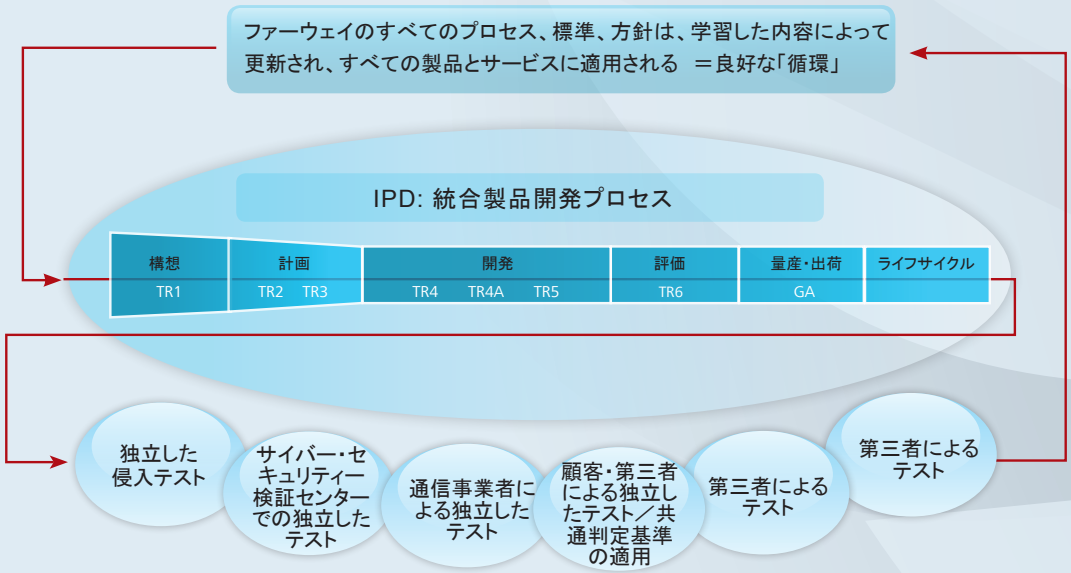
とはいえ、プロセスを備えているからといってそれが良いものであるとは限らず、また実際にすべての関係者がそのプロセスを実践しなければ意味がありません。この2つの問題に徹底して対処するために、当社は以下の対策を取ってきました。

- 標準化されたビジネス・プロセスを世界規模で確立し、各プロセスにGPO（Global Process Owner：グローバル・プロセス所有者）とKCP（Key Control Point：主要管理項目）を設定しています。さらに、各子会社および事業部門に適用されるグローバル・プロセス管理マニュアルと職務分担表も策定されます。GPOは、経営環境やリスクの影響度を考慮しながら、サイバー・セキュリティー上の要求事項がプロセス、方針、標準に適切な形で組み込まれ、有効に実施されていることを保証する責任を果たしています。

- 企業統治の点では、当社の副会長が議長を務めるGCSC（Global Cyber Security Committee：グローバル・サイバー・セキュリティー委員会）を設置しています。この委員会には取締役会の主要メンバーと、GPOが参加しており、サイバー・セキュリティーに関連した業務プロセスの不具合やリソースの問題が発生した際、、独立して変更の決定を下せる権限を有しています。

- ファーウェイの監査役は、KCPとグローバル・プロセス管理マニュアルを用いて、プロセスの実施とその有効性を判定します。さらに、外部検査や第三者評価による検証も行われます。個人レベルでの説明責任と規則・規制の遵守義務は、日常業務においてどのように行動すればよいかを記したファーウェイのビジネス・コンダクト・ガイドラインにより規定され、ビジネス・プロセスに組み込まれています。従業員はこのガイドラインについて常に最新の知識を維持するよう毎年オンライン・テストを受けています。このテストはファーウェイの内部コンプライアンス・プログラムの一環として行われています。

こうした内部統制システムの確立に加え、自社のプロセスと社内システムが、お客様、さまざまな分野の専門家、政府による監視や評価に対してオープンであることが重要です。ファーウェイが140を超える国々で事業を展開できるのは、各国のお客様からの信頼があるからです。ファーウェイは統合開発プロセスに基づいて、学習の成果や外部からの評価を次のプロセスに反映させ、良好な循環を維持しています。これを図に示すと、以下のようになります。



開発プロセスにおける具体的な改善の取り組みとしては、追跡性の確保が挙げられます。世界的な技術ベンダーの多くは、多数のサードパーティーからソフトウェア・コンポーネントのライセンスを受けて、それらを自社開発のコンピューター・コードの中に組み込んでいます。ひとつのソフトウェアが、複数の国で複数のチームによって開発されることもあります。そうした場合にも、セキュリティー問題が生じたり脆弱性が発見されたりした際に、開発プロセスを遡り、どの製品にそのコンポーネントが組み込まれているかを正確に特定できなければなりません。

ファーウェイでは、お客様にいただいた要求事項から作成されたコンピューター・コードまでの全経路を追跡できるよう、社内システムおよびプロセスを継続的に強化しています。

また、研究開発においては職務の分離を徹底しています。ソフトウェア開発者は最終的なテスト結果やリリースを承認できないようになっています。独立した厳格なレビューとサインオフのプロセスが設けられているため、ソフトウェア開発者が自分自身で設計したソフトウェアの実装を許可することはできません。サインオフされると、ソフトウェアはサポート・ウェブサイトに自動的にアップロードされて、製造現場あるいはお客様の拠点でダウンロードする準備が整います。

このような開発面でのプロセス化は当然重要ですが、しかしサイバー・セキュリティーは単に技術の問題だけではなく、人、法律、インセンティブの問題でもあります。技術の設計、開発、実装と同様、人事、法務、営業、財務、マーケティング、サプライヤー管理も同様に重視しなければなりません。例えば、サプライチェーンや人事において多様性を確保することがひとつの対策です。サプライチェーンについては、ファーウェイが使用するコンポーネントの70%は中国本土以外のサプライヤーから供給されています。最大の供給元は米国で、当社のコンポーネントの32%を供給しており、そのほとんどがハイテク・コンポーネントです。また、台湾と欧州からもあわせて32%を調達しています。人材の面では、当社が事業活動を行っている140以上の国々で平均して72%の従業員が現地採用となっています。

ファーウェイでは、サイバー・セキュリティー上の要求事項を業務プロセスに組み込んでいるため、役員、管理職、従業員それぞれに自分の職務についての説明責任と遂行義務が課せられています。こうした責任体制を維持するには、定期的にトレーニングを実施し、インセンティブと個人の義務とのバランスを適切に保つとともに、能力向上と保証レベルの検証のための継続的な循環型プロセスを整備する必要があります。

ファーウェイでは、自社事業のオープン性・透明性を高めるべく、「多くの目」「多くの手」というアプローチを採用しています。ファーウェイは、自社を含めたすべての技術ベンダーに対する公平かつ非差別的な監査・調査・検査を積極的に奨励しています。これにより、企業の理念・方針・ルールを再考し、パフォーマンス能力や、製品の品質と安全性を高めることができるからです。ファーウェイでは現在、顧客企業や政府に対し、ファーウェイ製品の検証を包括的に行う環境を提供しています。

モバイルやクラウド・コンピューティングの成長に伴い、ネットワークに対してさまざまな機能が求められるようになっています。ファーウェイはこうした需要の増大に対応すべくクラウド・コンピューティング開発に積極的に取り組んでおり、セキュリティーの面でも、仮想プラットフォーム・セキュリティー、仮想ネットワーク防衛、クラウド上のデータ保護などに関する技術や製品の開発で業界を牽引し、包括的な対策の構築を目指しています。さらに、CSA（Cloud Security Alliance）のISC（International Standard Council：国際規格評議会）の中核メンバーとして渉外係を務め、日中韓セキュリティー・ワークショップおよびCCSA（China Communications Standards Association：中国通信標準化協会）にCSAの代表として参加し、クラウド・セキュリティー標準化の推進と普及にも貢献しています。

サイバー・セキュリティーの脅威に対処するため、ファーウェイは、グローバル規模の「サイバー・セキュリティー諮問委員会」の設立に向けて、政府、通信事業者、通信業界の専門家と積極的に意見を交換し、当社のサイバー・セキュリティー環境構築についての説明に努めています。また、事業から独立した「サイバー・セキュリティー検証センター」を設立しており、製品のセキュリティーに関する独自検査を実施しているほか、製品品質やセキュリティー能力を詳細に記した検証報告書を顧客向けに公開しています。さらに、ファーウェイ製品のセキュリティーを自身で検証することができるよう、センターを当社の顧客や政府に向けて開

放しています。

ファーウェイは、脅威モデリング、マルウェア検出、攻撃行動分析などの主要なサイバー・セキュリティー分野に焦点を当てたさまざまな組織と密接な協力関係を築いており、セキュリティー能力に関する情報共有を進めています。主な組織としては、APWG（Anti-Phishing Working Group）、CNCERT／CC（Computer Emergency Response Technical Team／Coordination Center of China）、オペラ・ソフトウェア、CNNIC（China Internet Network Information Center）、APAC（Anti-Phishing Alliance of China）、ウイルス対策ソフトウェア・プロバイダーのAVG、インターポール（国際刑事警察機構）、IWF（Internet Watch Foundation：インターネット監視財団）などがあります

また当社は、サイバー・セキュリティーに関するさまざまなフォーラムや会議を後援しており、こうしたイベントに積極的に参加して情報共有と相互学習を進めています。例えば、EWI（East West Institute）主催のサイバー・セキュリティー会議では、サイバー・セキュリティーに関するグローバルなコンセンサスとサプライチェーン・セキュリティーについて検討するワークショップに参加しました。GIIC（Global Information Infrastructure Commission）ではスポンサーとなって講演を行っているほか、理事会の副議長に就任しており、Quest Forumにも参加しています。

ファーウェイは、グローバルなセキュリティー標準化策定にも大きく貢献しています。3GPPに対しては、セキュリティーに関する提案を毎年多数提出しています。また、主要な通信事業者やベンダーの協力のもと、HeNB（Home eNode B）セキュリティー標準化の策定を主導し、M2M（Machine To Machine：マシン・ツー・マシン）やPWS（Public Warning System：公衆警報システム）のセキュリティー研究を推進しています。IETFでは、IPsec（Internet Protocol Security）、Karp（Keying and Authentication for Routing Protocols）、syslog、OSPF（Open Shortest Path First）、MPLS（Multiprotocol Label Switching）、Hokey（Handover Keying）、IPv6など、セキュリティー関連の問題に対する各種作業部会に率先して参加しています。また、仮想ネットワーク・セキュリティーやアンチスパムに関する標準化にも貢献し、IEEE（Institute of Electrical and Electronics Engineers）、OMA（Open Mobile Alliance）、UPnP（Universal Plug and Play）フォーラム、WiFiアライアンスなどのセキュリティー関連標準化活動にも参加しています。

サイバー・セキュリティー問題の解決は業界共通の課題です。関係者すべてが一丸となり、オープン性と透明性をもって知識・業務プロセス・製品の向上に貢献し、国際法、標準、方針、ベスト・プラクティスの策定や実施に積極的に協力しあうことが重要です。

5　成功への鍵は「協力」

ベライゾンの2012年DBIR（Data Breach Investigations Report：データ漏えい調査レポート）によれば、4年連続でデータ漏えいの大多数（97%）は簡単な対策が施されていれば防げたはずだと報告しています[35]。サイバー・セキュリティーの問題には、対抗できる手段が必ずあるのです。

オーストラリアでは、国防省の情報機関であるDSD（Defence Signals Directorate：通信連絡局）が「対策戦略トップ35」を発表しています。これはオーストラリア政府内で発生した侵入や攻撃に対するDSDの分析に基づくもので、2010年2月に最初に発表されて以来、定期的に改訂されています。DSDによると、トップ35のうちの上位4戦略を実施していれば、2009年にDSDが対処した侵入のうち少なくとも70%が、2010年では少なくとも85%が防止できたとされています[36]。オーストラリアだけでなく、各国の政府が前もって緩和戦略を実施すれば、サイバー・セキュリティー・リスクへの懸念は大幅に軽減できます。

私たちが一丸となって決意を表明し、オープン性と透明性を標榜すれば、可能性は飛躍的に広がります。

テクノロジーを取り巻く環境はすでに複雑ですが、スマートフォンとクラウド・コンピューティングの役割が拡大し、世界中で開発された品質やセキュリティー基準の異なるソフトウェアがアプリケーション・ストアで広範囲に配布され、利用されることによって、その複雑さはさらに増しています。

サイバー・セキュリティーの問題は、社会のあらゆる領域におけるさまざまなレベルの方針、テクノロジー、行動様式、標準、ガイドライン、法律に関わるため、状況をいっそう複雑にしています。サイバー・セキュリティー問題に適切に対処するためには、官と民、さらには競合関係にあるすべての関係者が目標と責任分担について同じ認識を持ち、お互いの協力のもと、リスクに基づいた枠組みの中で、データおよび情報システムの整合性とセキュリティーを確保する必要があります。

サイバー・セキュリティーの問題に取り組むためには、すべての関係者が地理的・政治的な隔たりやビジネス上の競争関係を超えて協力しあう必要があります。こうした協力は競争上不利になるという見方もありますが、現実には、お互いに協力しなければ、グローバルなサイバー・セキュリティー対策の脆弱性に不正につけ入る隙を増やすことになります。協力体制を促進するための場はいくつか存在しますが、いずれもゆるやかな形での協力関係で、真に団結した包括的な協力体制は実現していません。

こうした状況において、サイバー・セキュリティーに対する包括的かつ協調的なアプローチを推進するためには、各国政府が率先して統合的な体制を確立する必要があります。ファーウェイはそのような取り組みを支援することが自らの使命であると考えています。

---

[35] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[36] http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

6　共に前進する

サイバー・セキュリティーの現在の状況を概観してみると、全般的にステークホルダーの間で協力と信頼関係が欠けているために、問題に対する包括的対処が進んでいないことがわかります。あらゆるテクノロジー・ユーザーとベンダーにとって、セキュリティー上の課題への対策を追求することは等しく重要な問題です。それぞれのステークホルダーがより良い前例を作っていく必要があり、産業界と各政府機関が互いに協力して適切な方針の枠組みを検討していかなければなりません。このような共同作業を進めるには、協調して行動するための枠組みを設定し、それを指針として、戦略上の優先事項と目的、時系列に沿った達成目標を互いに調整していくことが必要です。そして、初期段階では、信頼の欠如や政治的・地政学的状況、保護貿易主義や競合企業間の不十分な情報開示のために、期待するほどの貢献が得られない場合もあることも念頭におかなくてはいけません。そうだとしても、こうした事情を理由にして取り組みを先送りにすることはもはや許されないのです。

共同作業の指針として、以下の7つが挙げられます。

1. グローバルであること：ボーダーレス、相互の連携、グローバル展開といった、規制、法律、標準、認可に関する現在のサイバー環境の性質を考慮する。
2. 法規に則っていること：文化的な相違という問題を受け入れつつ、国際的な法律、標準、定義、規定の調整に努める。
3. 共同作業であること：官民の協調体制をフル活用して、攻撃を阻止する能力を最大化する。
4. 標準に基づくものであること：国際標準やICTベンダーのベンチマークの作成、合意、実施にあたっては、リスクのレベルに応じた基準を設ける。セキュリティーとリスクとのバランスをとる必要がある。
5. 検証に基づくものであること：合意された標準とベンチマークに製品が適合しているかどうかを確認するための、グローバルかつ独立した検証方法を設計、開発、実施する。
6. 証拠に基づくものであること：リスク、攻撃者、損失や被害の有無について、証拠に基づいた判断をする。憶測ではなく事実に焦点を当てる。
7. 基本を押さえること：攻撃を成功しにくくするために、基本的な要素の改善にしっかりと取り組む。

ファーウェイは、今後もテクノロジーによって全世界の経済・社会の向上を促進していけるよう、国際的な協調、オープン性、相互信頼を支持します。皆様にもこの立場に賛同していただけることを願っています。

7　ファーウェイについて

ファーウェイは、140か国以上で事業を運営するグローバルICTソリューション・プロバイダーです。14万人の従業員を擁するファーウェイは、その製品とソリューションを世界人口の3分の1以上にもおよぶ人々に提供しています。当社が業務を行っている各国において、平均72%の従業員が現地採用であり、その平均年齢は28歳です。ファーウェイは世界の上位50の通信事業者のうち45社と取引を行っています。また、2011年現在、ファーウェイのワイヤレス・ネットワーク製品とソリューションは世界500以上の通信事業者に導入されています。ファーウェイは、200万台以上の基地局無線装置を出荷し、15億人以上の携帯電話加入者にサービスを提供しています。

ファーウェイは科学とエンジニアリングを基礎とする民間企業であり、新技術の研究、開発、展開に注力しています。継続的なイノベーションを通じて通信業界を牽引し、業界屈指のIPR（Intellectual Property Rights：知的財産権）ポートフォリオを誇っています。また、他者のIPRを尊重し、その保護に努めています。ファーウェイは年間売上高の10%をR&Dに投資しており、2011年は37億6,000万米ドル（約2,932億8,000万円※）、過去10年間では総額150億米ドル（約1兆1,700億円※）をR&D費にあててきました。

当社は、エリクソン、ソニー・エリクソン、ノキア、ノキア・シーメンス、シスベル、クアルコム、アルカテル・ルーセント、ノーテル、ドルビー、ロビ、BT、KPNといった企業との間に特許ライセンス契約およびクロス・ライセンス契約を結んでいます。特許ライセンス費用として、2011年には3億米ドル（約234億円※）以上、これまでの累積では12億米ドル（約936億円※）を投資してきました。社内でのイノベーションの源泉となっているのが、世界各国の著名な教育機関から集まった1,265名の博士号取得者、4万4,690名の修士号取得者、そして6万2,000名のR&D部門の従業員です。2011年末におけるファーウェイの申請済み特許件数は中国国内で3万6,344件、PCT（Patent Cooperation Treaty：特許協力条約）に基づくものが1万650件、海外申請は1万978件です。取得済みの特許ライセンスは2万3,522件に上ります。IPRの保護はファーウェイの継続的な成功にとって不可欠であり、ファーウェイはIPR保護の第一人者となっています。

ファーウェイは全世界でR&Dセンターを23か所、一部の主要なお客様との共同イノベーション・センターを34か所、トレーニング・センターを45か所に有しています。全収益の68%は中国国外からのものであり、資材の70%は外国企業から調達しています。米国は最大の供給元で、32%の部品を185社から購入しています（2011年は米国の企業から65億米ドル（約5,070億円※）分購入しました）。また、台湾から22%、欧州から10%、中国から30%を調達しています。

ファーウェイは60か国の115のネットワークにマネージド・サービス（管理サービス）を提供し、お客様が優れた運用ができるよう支援しています。また、クラウド・ベースのITソリューションを構築し、300以上のパートナーと共同で、さまざまな業界でクラウド・コンピューティング技術の商用利用を推進してきました。2011年末までに、世界中で210のデータセンターの構築を支援しており、そのうち20か所がクラウド・コンピューティング・データセンターです。

2011年度のファーウェイのコンシューマー向け端末出荷台数は、合計で約1億5,000万台に上ります。そのうち約5,500万台が携帯電話、約6,000万台がモバイル・ブロードバンド機器、約3,000万台が固定アクセス・固定ワイヤレス端末などの家庭用装置です。

※1米ドル78円換算

ファーウェイは主要な国際標準への対応に力を入れており、それらの策定にも貢献しています。2011年末までに、3GPP、IETF、ITU、OMA、ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）、IEEE、3GPP2など130の標準化団体に参加し、これらの団体に合計2万8,000件を超える提案を提出しています。また、OMA、CCSA、ETSI、ATIS（Alliance for Telecommunications Industry Solutions：電気通信標準化連合）など、多くの権威ある組織で理事会メンバーとして活動し、180を超える役職に就いています。

「ファーウェイは他とは違う」、「ファーウェイは他と違うルールで動いている」と言われることがありますが、これはある意味では真実です。ファーウェイの株式は2011年12月31日時点で6万5,596人の従業員が保有しており、彼らが会社を所有していると言えます。こうした従業員持株制度は、長期的な視野を持ち、リスクに対する利益と戦略のバランスを取るために有効な手段です。お客様に優れたサービスを提供できなかったり、不適切な行動をとったりすれば、従業員自らの資産が損なわれることになるからです。これらに加え、ファーウェイは世界中の名だたる大学から優秀な科学者とエンジニアを採用しており、入社後短期間のうちにグローバルな経験を積ませることによって、その才能を開花させています。

最後に、ファーウェイはイノベーションを第一とした企業です。2010年のファスト・カンパニー誌では、世界で最も革新的な企業としてフェイスブック、アマゾン、アップル、グーグルに次ぐ5位にランクされています。また、エコノミスト誌からは「2010 Corporate Use of Innovation Award（2010年イノベーション活用企業賞」を受賞しています。当社は、こうした評価にふさわしい企業であり続けるために、これからもイノベーションに注力し、革新的な技術によって世界に貢献してまいります。

本レポートの作成にあたり、多大なるサポートと意見を寄せてくれたチーム・メンバーに感謝します。彼らの職業意識と協力姿勢から、ファーウェイはすばらしい人材を採用している企業であることを再認識しました。とくに、南建峰、王唯践、彭麗巍、余志林、Paul Michael Litherland、劉晨曦、Andy Purdy、Andy Hopkins、楊光磊、John Koshy、Peter Rossi、Didier Blanchardには謝意を表します。その他にも多くの人たちが直接・間接に本レポートの作成に寄与してくれました。ここに名前を挙げられない方々にはお詫び申し上げます。

Copyright © 2012 Huawei Technology Co., Ltd. All rights reserved

本レポートは参考資料としてのみ印刷・利用できます。それ以外の目的に使用することはできません。

本レポートは「現状のまま」にて提供され、明示または黙示を問わず、一切の保証を伴いません。すべての保証は明示的に放棄されます。権利非侵害、商品性、特定の目的への適合性に対する保証は一切ありません。ファーウェイは内容の正確さについて一切の責任を負いません。本レポートに記載されたすべての情報は予告なく訂正・修正・変更されることがあります。本レポートの内容を信頼し、利用するにあたってその責任はすべて利用者に帰されます。本レポートに記載された第三者に関する情報は公共の情報源または公開された報告や説明に基づいたものです。

HUAWEI、華為、はファーウェイ・テクノロジーズの商標または登録商標です。

本レポートで言及されるすべての企業名・商標は該当する各社の商標または登録商標です。