ルは記憶に新しい。これは、SNMP の仕様を悪用し、ネットワーク機器の設定情報を書き換えることで、機器を使用不能に出来るという点が脅威となった。今後、ルータの機能が拡張され、さまざまな機能が搭載されるようになると、新たなセキュリティ・ホールが発生してもおかしくない状況である。

上で述べた不具合やセキュリティ・ホールの悪用が起こると、最悪の場合、広範囲でネットワークが停止することもありうる。

ネットワーク機器の故障に対しては冗長構成で対応することが可能であるが、ファームウェア不具合や、セキュリティ・ホールに対しては、冗長構成は無力である。対策としては、適切な設定でファームウェアの不具合を回避したり、パッチを当てていく方法しかない。

3.3.4 運用面の脆弱性

3.3.1 で述べたとおり、インターネットはさまざまな脆弱性を持つ中で運用されている。また、3.3.3 で述べたとおり、ネットワーク機器自体にもさまざまな脆弱性がある。

このような脆弱性に対しては、それぞれの組織の運用技術者が個々に対応している。例えば、ルーティングプロトコルの欠点については、欠点が表に出ないような細かな設定を行うことで対応し、経路のフラップに対しては、不安定な経路を排除するため、ルータにフィルタを設定することで対応している。また、ルータのファームウェアの不具合や、セキュリティ・ホール等の脆弱性についても、ファームウェア情報の確認及びアップグレードの実行等の細かな対応を行っている。

このような対応は、豊富な経験と高いスキルを持つ運用技術者の存在無しには不可能である。

そもそもインターネットは、組織に閉じたネットワークを有志らが相互接続して作られたものであることから、伝統的に運用技術者のスキルに依存する度合いが強い。

現代社会が今後インターネットに密接に結びつくことが予想されるにも関わらず、運用が未だ個人のスキルに強く依存する点は問題であると言わざるを得ない。

3.3.5 無線LANのセキュリティ問題

(1) 無線 LAN の現状

無線 LAN は、容易に導入できる点・利便性・低コストなどの要因により、ここ 2,3 年で急速に発展している。また、一般的なオフィスや家庭での使用だけではなく、ホットスポットサービスとして、コンビニエンスストア・レストラン・ホテル・駅・空港など公共な場所にも無線 LAN 基地局が導入され、24 時間いつでもどこでもインターネットへの接続口となるインフラとしての地位を確立している。

一方、急速な発展と引き換えにさまざまなセキュリティ問題も起きている。米国では、医療機関の無線 LAN から患者の医療データが誰でも見られる状態だったという事例・金融機関の無線 LAN から投資家のポートフォリオデータが誰でも見られる状態だったという事例・無線 LAN 基地局探知ツールを使用して調査した結果多数の有名企業の社内 LAN に接続可能だったという事例が報告されている。また日本でも、気象庁や都庁などの無線 LAN で情報漏えいの可能性ありと指摘され使用を停止したなどの事例がある。こういった事例を踏まえて、総務省のホームページ「国民のための情報セキュリティサイト」において無線ＬＡＮのセキュリティ対策の基本となる情報を提供し、利用者への周知･啓発を実施している。また、警視庁ではホームページ上で無線 LAN 利用者への注意を呼びかけている。

これら無線 LAN のセキュリティ問題は「盗聴」と「不正侵入」の 2 つに分類できる。無線 LAN は電波による通信という特性上、電波の届く範囲であれば誰でも通信データを受信できてしまうため、常に盗聴による情報漏えいの危険性がある。また無線 LAN のセキュリティ問題は、運用方法が問題となっている場合が多い。安易な運用管理により重要なネットワークに不正侵入されてしまう。また、無線 LAN の規格・仕様脆弱性の不備も指摘されているところであり、総務省においても 2004 年度までに無線 LAN をはじめとする情報通信ネットワークのセキュリティに関する利用動向、技術動向等について更に検討を行うこととしている。

(2) 現状の無線 LAN のセキュリティ問題への対策

a) 盗聴

無線 LAN 上での通信データの盗聴を防ぐ対策としては、物理的に電波を遮断し電波漏れを防ぐ、通信路を暗号化するといった手法がある。

物理的に電波漏れを防ぐ方法は無線 LAN を使用するビルや会議室などに電波を遮断する仕組み(部屋全体を金属で覆う、電磁波を遮断するガラスの使用など)を導入する方法だが、対策のためのコストが高いなどの問題点もある。

一方、通信路の暗号化は、無線 LAN の規格としての暗号化を用いる方法と、IPsec 等の有線ネットワークと同じ（上位通信層での）暗号化方式を用いる方法が考えられる。無線 LAN の規格としての暗号化には WEP があるが、すでに多くの脆弱性が指摘されており、利用端末全てでひとつの固定鍵を共有するなどのスケーラビリティにも問題がある。こうした設定の煩雑さもあり、十分な対策を取らずに無線 LAN を導入した結果が(1)で紹介したような事例を引き起こす原因の一つになっている。

上位通信層での暗号化は無線 LAN だけではなく様々なインフラ・アクセス方法・アプリケーションにおいて有効な手段である。上位通信層での暗号化は IPSec や SSL(Secure Sockets Layer) などの方式を用いて通信路の暗号化を行うのが一般的だが、利用者側に多くの事前設定や使用する際に特別な操作が必要になるケースがあること、アクセス方法・アプリケーション毎にそれらの設定や操作が異なることなど、ユーザに対する負担が大きく、便宜性が損なわれる。

b) 不正侵入

無線 LAN への不正侵入を防ぐには、無線 LAN 接続時に接続端末の認証を行う必要がある。無線 LAN の規格としてある認証機能には、SSID・MAC アドレス認証・WEP 鍵・802.1X による認証などがある。ネットワーク管理者はユーザの利用規模・形態などから、上記の１つまたは複数の認証機能を使用して無線 LAN を構築した上で、さらに上位層での認証も併用することにより不正侵入を防ぐことが重要である。特に不特定多数のユーザが利用するホットスポットサービスにおいてはこうした上位層での認証・本人確認が重要である。

表 3.3-1 無線 LAN 規格の認証機能のメリット・デメリット

方式	メリット	デメリット	備考
SSID (※1)	● SSID のアナウンスを止めることにより基地局を特定しにくくなる	● SSID をつけない、SSID のアナウンスを止めない場合、基地局が簡単に探知されてしまう	● 本来セキュリティのためのものでない ● SSID のアナウンスを止めた場合でも、SSID が簡単に類推できるようなものにしない
MAC アドレス (※2)	● 接続端末をあらかじめ制限できる	● 接続端末を事前登録するのが面倒、スケーラビリティにかける ● 現在接続している端末の MAC アドレスを盗聴することは可能	● MAC アドレスを変更できるような製品も存在する
WEP 鍵 (※3)	● 暗号用の鍵を設定することにより、結果的に認証を行うことになる	● 各接続端末に事前に鍵を周知するのが面倒 ● ひとつの固定鍵を共有するため、スケーラビリティにかける	● WEP の脆弱性を悪用する解読ツールが出回っている
802.1X (※4)	● RADIUS サーバと連携した本格的な認証機能 ● 認証の枠組みを提供しているため、デジタル証明書を使うなどさまざまな認証方法に対応できる ● 端末接続後に異なる暗号鍵を配布する仕組みもある	● 互換性の問題がある ● 対応製品が少ない、高価である ● 対応クライアント OS が少ない ● 導入への敷居が高い	● ベンダーの独自実装なども多く、互換性の確認が必要 ● 標準化中の無線 LAN 時期セキュリティ標準（IEEE802.11i）で利用されている。

※1 SSID (Service Set-ID): 無線 LAN を識別するためのグループ名。

※2 MAC アドレス: 無線 LAN アダプタ等 LAN アダプタの固有アドレス。

※3 WEP 鍵 (Wired Equivalent Privacy Key): 無線通信における暗号化技術に用いる鍵。

※4 802.1x: LAN 内のユーザ認証の方式を定めた規格。無線 LAN には限定しない。

(3) 今後の対策と課題

無線 LAN の規格自体の対策としては、IEEE でもセキュリティの拡張を議論しており、802.11i という新しい規格がドラフト段階になっている。

そもそも不正侵入されては困るネットワークと無線 LAN を切り離すようなネットワークを構築するというアプローチを検討することも必要である。米国では、国防に関する研究を行っている国立研究所は施設内での無線 LAN の使用を禁止しているなどの例もある。ネットワーク管理者はどこに無線 LAN が必要なのか？どこを切り離すべきなのか？を慎重に検討した上で、ネットワークを構築する必要がある。

(2)で述べたような盗聴と不正侵入への対策をネットワーク管理者や利用ユーザが怠れば、それはそのまま無線 LAN と接続しているネットワーク全体のセキュリティ問題に直結してしまう。ネットワーク管理者や利用ユーザのセキュリティ対策の負担を軽減するためには、様々なネットワークへの接続方法・アプリケーションにおいて使用可能な暗号化・認証・本人確認の機能を一つのネットワーク基盤として提供していくことが必要である。

3.3.6 利用者の属性に基づくアクセス制御の必要性

(1) 現状

現在のインターネット上で提供されているアプリケーションやサービスでは利用者を利用者本人自身としてではなく、利用者が使用している端末に割り当てられた IP アドレス・DNS による所属ドメイン・メールアドレスなどによって識別しているにすぎない。そのため、アクセス制御の手法の多くは IP アドレスによる制御や IP アドレスに紐付けられた DNS の名前・逆引き名をベースにした制御しかできない。

インターネット上で電子商取引などのサービスを提供するサービス事業者では、サービス利用者に事前にどんな属性を持っているかを利用者情報としてオンライン登録させ、利用者 ID とパスワードを発行し、サービス利用時にその ID・パスワードで認証することにより、サービス提供の可否を判断するのが一般的である。しかし、実際には利用者が自分の情報を偽りなく登録しているかどうかを判断することは難しく、入力情報に対して形式的なチェックを行う程度である。

ネットオークションのような個人間の商取引の場合にも、相手から提供されている情報の正確さが保障されないため、「取引相手が本当に存在しているのか？」「取引相手の登録情報は正しいのか？」などの不安を常に抱えており、取引活発化の弊害になっている。

(2) 利用者の属性に基づくアクセス制御の必要性

2003 年 5 月 16 日に衆議院本会議で可決した出会い系サイト規制法案では、「18 歳に満たない者によるインターネット異性紹介事業の利用を防止するための措置」が求められている。(1)で指摘したように現在のインターネットを利用したサービス形態ではこのような利用者の年齢によるアクセス制限を完全に実現するのは困難である。

今後インターネット利用者が爆発的に増え続け、様々なサービス事業者が様々なサービスを提供していくようになると、サービス利用者が自分の属性を偽りなく登録し、サービス利用に必要な属性だけを公開する仕組みと、サービス事業者がサービス利用者の必要な

属性を参照し、接続・サービス提供の可否を判断するアクセス制御を実現することが必要である。ただし、サービス利用者が自分の属性を登録・公開することに関しては、プライバシーの問題に注意し、慎重に検討していかなければならない。

3.3.7 その他インターネット自体に内在する脆弱性

(1) 発信元アドレスの詐称

インターネット上の通信はパケットという単位で行われるが、パケットには必ずそのパケットの宛先アドレスと発信元アドレスが記録されている。宛先アドレスがあるおかげでパケットは正しく受信者に届けられ、発信元アドレスがあるおかげでパケットの受信者は発信元に応答を返すことが可能なのである。

実は、この発信元アドレスは、電話の発信番号通知のように電話局が設定するのではなくホスト側で設定する仕組みになっているため、原理的にはパケットの送信者が任意に設定することができる。通常、発信元アドレスを「自分」と異なるアドレスにすると通信ができなくなってしまうため、わざわざ偽るようなことは無いというのがインターネットの前提なのである。

しかし、インターネット上の犯罪者はこの「自由に設定できる発信元アドレス」を利用して自分ではない他のホストに攻撃を行ってきた。その例として smurf 攻撃と呼ばれる手法を説明する。

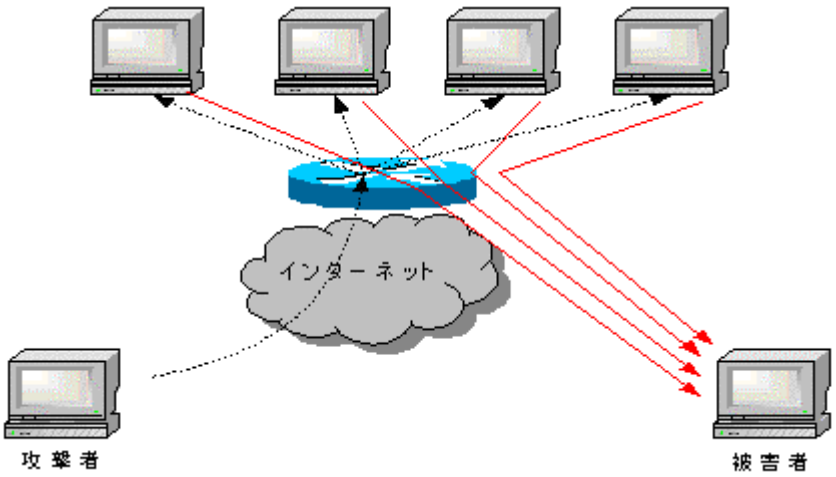

図 3.3-4　smurf **攻撃**

通信相手の生死を確認することができる ICMP というプロトコルがあるが、これは ICMP エコー要求パケットを相手ホストに送信すると、相手ホストは送信元アドレスに対して ICMP エコー応答パケットを返すというものである。攻撃者は、このとき、送信先アドレスを相手ホストの属するネットワーク（ブロードキャスト）に設定し、発信元アドレスを図中の「被害者」のアドレスと偽って設定した ICMP エコー要求を送信する。その結果、このパケットを受け取った多数のホストが一斉に被害者のホストに ICMP エコー応答パケットを「返し」被害者側ネットワーク帯域を消費させるなどの被害をもたらすのである。

ただし、smurf 攻撃に限って言えば、現在では途中経路のルータや端末にその原因となる「ブロードキャストに対する ICMP エコー要求」に応答しないように設定されていることが多く、また、発信元アドレスを詐称したパケットは ISP のルータでブロックするよう設定されていることが多いため、実際に脅威となるケースはそれほど多くない。

(2) 途中経路が指定できない

インターネット上ではパケットは途中経路のルータを順次バケツリレーされ、最終目的地に到達する。このとき、パケットの送信者が指定できるのは最終目的地と送信者のすぐ隣のルータだけであり、途中経路を選択することはできない。このため、具体的には、下記のような不安定さを内包している。

- 帯域が細く十分な通信速度が得られない可能性がある
- 通信事業者のモラルが低くパケットを盗聴されている可能性がある
- 通信したい相手の「偽者」が経路上に作成されている可能性がある
- 途中経路の経路制御が不安定で通信が途切れる可能性がある
- 特定のワームを防止するためなどの理由で、経路上の ISP が意図的にある種の通信をブロックすることがある。

以前はこれらの理由で「インターネットは信頼性が悪く使えない」との印象が広くもたれていたが、インターネットが普及し企業活動や生活に取り入れられるにしたがい、アプリケーション側がそれを補うように作られるようになってきた。そのため、今ではエンドユーザが実際に不安定さを意識することはかなり少なくなっている。例えば下記のような対応がなされている。

- 帯域が細い→可変レートの動画通信技術によるサポート
- パケットの盗聴→SSL などによる通信の暗号化
- 通信相手の成りすまし→SSL などによる通信相手の正当性証明
- 通信の途切れ→通信品質自体の向上により

通信自体の信頼性が向上した結果、現在では、操作している人が「本当にその人であるか」ということの確保の必要性がより高まってきていると言える。

3.4　利用者サイドの意識啓発

ネットワーク事業者やシステム管理者がセキュリティ対策を行うだけでは、強固なセキュリティを確保することはできない。そのネットワークを利用するユーザ自身もセキュリティに対する意識と知識を持っていなければ、用意されたセキュリティ策も意味の無いものになってしまう。つまり、一番大きなセキュリティ・ホールは人間自身であると言えるかもしれない。

2001 年 1 月に首都圏の会社員（男女 1140 名）を対象としてインターネット上でおこなわれたアンケート（「コンピュータセキュリティに関する会社員の意識調査」：RSA セキュリティ株式会社）によると、「ほぼ毎日電子メールを利用する」「ほぼ毎日ホームページを見る」と回答した人がそれぞれ 9 割にのぼるものの、利用方法の習得については 8 割以上が「独習」と回答しており、「勤務先などで講習を受けた」という回答は 1 割未満という結果になっている。具体的な操作方法は使ううちに身に着いていくと思われるが、セキュリティ面に関しては特に本人が意識して学習しなければなかなか習得できない。
インターネット利用の際の不安要因として最も多くあげられた回答は、自宅での利用、勤務先での利用ともに「ウィルスの侵入」であり、ついで「個人情報を盗まれる」「全く知らない人からメールが来る」「個人情報を見られる」など個人情報の流出に対する不安も大きい。「自分の PC の中に無断で侵入される」「会社のネットワークに無断で侵入される」といった外部からの不正侵入に対する不安感も目立っている。
これに対し、実際に行っているセキュリティ対策については、「ウィルス対策ソフトの導入」については約 7 割が実施しているのに対し、「SSL に対応しているサイトでしか個人情報を入力しない」が 27.5%、「ホームページで個人情報を入力しない」が 12.4%にとどまっている。さらに、「特に対策は講じていない」という回答が約 2 割にのぼっており、インターネット利用の安全性に対して不安は持っているものの、危機意識はまだまだ低いということがうかがえる。

一方、総務省が中小企業（従業員 300 人以下の非上場企業）の基幹システム管理者に対して行った「情報セキュリティ対策の状況調査」（2002 年 5 月、有効回答 951 社）によると、過去 1 年間にセキュリティ侵害が発生した企業は 49.2%と 2 社に 1 社の割合で被害を受けていることがわかった。内容としては「ウィルス・ワーム感染」が最も多く、次いで、「スパム・メールの中継利用・踏み台」、「DoS 攻撃」となっている。セキュリティ確保のために実施している具体的な施策については、クライアント用のアンチウィルスソフトの導入率

は 77.2%と比較的高水準となっているものの、外部からのセキュリティ上の脅威を防御するファイアウォールの導入率については 46.4%にとどまっている。また企業のセキュリティ理念やファイアウォールの運用方法などを明文化するセキュリティポリシーについても、その策定率は 12.5%と低水準である。ファイアウォールを設置していない、セキュリティポリシーを策定していない理由については「知識・ノウハウがない」ことが主な理由となっており、加えて「情報セキュリティの重要性に対する認識がない」との回答が約 3 割に上るなど、セキュリティに対する認識の低さが明らかになっている。

ADSL や CATV などインターネットに対して高速かつ常時接続できる環境が普及するに伴って、個人ユーザレベルであっても「インターネットからの脅威」への対策の必要性は高まっている。すでに述べた意識調査にもあるように、利用者として不安は持っているもののセキュリティ対策を講じるにはそれ相応のノウハウと手間が必要であり、全ての利用者が独自に行うのは困難である。個人ユーザだけでなく、専任のセキュリティ担当者を設けることが難しい中小企業などに関しても、同様の懸念がある。
このような背景のもと、インターネット接続サービスを提供する ISP 事業者各社において、ネットワークユーザに対して様々なセキュリティサービスを提供するようになった。サービスの内容としては、受信メールのウィルスチェックといった個人ユーザ向けのものから、自社システムのセキュリティ対策をトータルにサポートする企業向けセキュリティサービスまで、様々なタイプのものが用意されており、利用者サイドのセキュリティ対策をバックアップできるものとなっている（表 3.4-1）。

表 3.4-1 セキュリティサービスの例

サービス名	概要
セキュリティ診断	ポートスキャンや擬似的クラッキングなどを行い、ユーザネットワークのセキュリティ診断を実施する。
ウィルスチェック	利用者が受信する電子メールに対しサーバ上でウィルスを検知・駆除するだけのものから、ウィルス対策を付加したホスティング又は自営サーバの構築まで、ウィルス対策の様々なアウトソーシングニーズに対応したサービスがある。
FireWall マネージメント	FireWall 機器のレンタルから、24 時間 365 日の稼動監視・保守サポートまで一元的に行う。
インターネット VPN	FireWall や VPN 装置をセットで提供し、インターネットを活用した WAN 環境下においてセキュアな通信を提供する。

サービス提供者側のこのような取り組みにより、利用者は高い知識がなくともセキュリ

ティ保護に対して比較的容易に自衛を図ることが可能となる。このような利用者サイドに立ったセキュリティサービスが浸透し、利用者が簡単・安全にインターネットを利用できるようにすることによって、更なるインターネット普及の呼び水になるとも考えられる。
しかしながら、インターネット利用の普及度と比較して、セキュリティシステム及びサービスの導入状況は個人、法人とも普及率が低いのが現状である。「セキュリティ対策はお金と労力がかかる」「やるのが面倒だ」「よく分からない」といった意見がまだまだ多く聞かれることは否めない。我が国特有とも言える「安全はタダ」という認識が、ネットワーク社会においても見え隠れしているようにも思われる。
自宅のドアに高性能のカギを取り付けたとしても、カギをかけるのを忘れてしまっては意味が無い。利用者自身、さらには企業の経営者自身にとって、情報セキュリティに対する意識向上と危機感の醸成といった根本的な意識改革が必要と考えられる。

一方、企業がネットワークを利用したサービスを提供する場合を考えてみる。システムのセキュリティ対策を十分行っていたとしても、自社ではコントロールできないリスクによりサービスが停止し、顧客に損害を出してしまう可能性がある。例えば、アライアンス先の企業のシステム停止、契約している ISP のネットワークのダウン、あるいは電力が停止するなどのリスクを完全に回避することは難しい。このため、情報リスクに対する保険（リスクファイナンシング）という概念が必要になっている。
しかしながら、現状では企業やユーザのセキュリティに対する意識が低い上に、特にネットワーク社会においてはベンダーや事業者の責任が重過ぎる傾向がある。（例えば自動車事故の場合、自動車メーカーと運転者双方がそれぞれに事故の責任を分担できている）そのため、情報リスクに対する保険を提供することが難しい。実際に常に最先端の情報リスクに対する保険を開発・提供出来るのは世界でも 10 数社と言われており、また再保険の制度も十分に確立されていないので大きな問題が発生した場合には現行保険制度の安定的運用を脅かす可能性もある。
このような状況から、情報リスクに対する保険の適用を一般化し、情報通信ネットワークや情報システムに対するリスクコストの適正化（社会コストの低減化）を行うためにも、企業やユーザ側のセキュリティ意識及び自己責任の意識の啓発が必要である。

このように、インターネットに接続する個々の利用者において、情報セキュリティに対する意識向上と危機管理、適切な対策の実施は大変重要な問題である。意識啓発のための具体的な施策のひとつとしては、総務省が同省ホームページ内に開設した「国民のための情報セキュリティサイト」があげられる。このサイトでは、インターネットと情報セキュリティに関する基礎的な知識の習得を促すとともに、正しい情報セキュリティ対策を行っていない場合に起こりうる事故や被害の例を紹介することにより、セキュリティに対する危機感の醸成を促している。加えて、エンドユーザやホームページ開設者、企業・組織と

いうようにネットワークの利用方法に応じた情報セキュリティ対策の基本となる情報をわかりやすく提供している。

警察庁においてもウィルス情報などのセキュリティ関連情報を提供する専門サイト「@police」を開設しており、子供から管理者レベルまでの幅広い層に向けて情報提供してセキュリティ啓発活動を行っている。子供向けに提供されている「キッズ」コーナーにおいては、通常の文字によるものではなく Flash アニメによる情報提供を行っており、ゲーム感覚で分かりやすく解説するといった工夫がなされている。また「一般 PC ユーザー」向けのコーナーでは、セキュリティを学ぶことができるカリキュラム「セキュリティ講座」や、現在利用している OS やブラウザ、メールソフトを入力することにより、その環境にあわせたセキュリティパッチ情報などを提供する「セキュリティ簡易診断」が利用できる。さらに「サーバ管理者」向けのコーナーでは、警察庁が保有しているセキュリティ関連情報の中から、利用 OS やアプリケーション毎に検索し、それぞれの既知の脆弱性などを調べることができるなど、一般ユーザーコーナーよりも一歩踏み込んだ情報の入手が可能となっている。この他、米 Dartmouth 大学セキュリティ技術研究科プロジェクトの協力により海外セキュリティニュースサイトの記事を掲載する「世界のセキュリティ事情」や、ユーザ参加型のイベント企画など趣向を凝らしたセキュリティ意識啓発サイトとなっている。

公共及び民間の様々なインターネットサービスの利用普及のためにも、利用者サイドにおけるセキュリティ意識の向上は非常に重要である。現在、ホームページにおける情報発信やセキュリティベンダーによるセミナー実施、企業内での勉強会など、様々な形で情報セキュリティ意識の啓発が取り組まれてはいるが、断片的に行われている感が否めない。インターネット利用者ひとりひとりについて今後さらにセキュリティ意識向上を図るため、適切で体系だったセキュリティ教育の実現をめざして課題と対策の検討が必要と思われる。また、利用者サイドの意識啓発とあわせて、ネットワーク事業者及びサービス提供者サイドにおいても、利用者に使いやすいセキュリティの仕組みを検討し、提供して行く必要があると考えられる。

4　今後推進すべき取り組み

2.2 で述べたように、ネットワーク接続のブロードバンド化、ネットワーク接続の低価格化により、インターネットに接続している利用者は爆発的に増加した。また、インターネットへの接続方法もダイヤルアップ方式から CATV、ADSL、FTTH といった常時接続方式が主流となり、さらには、有線接続方式のみならず、携帯電話・無線 LAN といった無線接続方式も登場し、インターネットへの多様なアクセス手段が提供されるようになってきて

いる。このような傾向は、今後、ますます強くなり、更に多くの利用者・機器が様々な接続方式でインターネットに接続していくことが予想される。
この結果、日本国全体がインターネットに依存し、インターネットが新たなライフラインとなることが予想される。

しかしながら、現状のインターネットは、日本国民誰もが安心・安全に参加できるネットワーク社会を実現するライフラインとしてはあまりに脆弱であると言わざるを得ない。例えば、上述のような利用者層の拡大は、インターネットの仕組みや安全に無知なまま、無防備にネットワークに接続する利用者の増加を生み、2.3 で述べたように、サイバーインシデントが爆発的に発生する原因の一つとなった。また、3.2 で述べたように、サイバー攻撃の手法は、日々、新たな手法が生み出され、高度化・多様化を続けている。このような状況のもと、現在、国民は漠然とした不安を抱きながらインターネットを利用しているのが現状であり、このまま、サイバーインシデントが増加の一途を辿れば、国民のインターネット利用が停滞することになりかねない。

このような状況に鑑み、政府としては、インターネットを日本国国民誰もが安心・安全に参加できるネットワーク社会を実現するライフラインとなすため、必要に応じて法制度をも視野に入れた調査研究など、様々なアプローチからの取り組みを推進していくことが求められる。また、今後推進すべき具体的な取り組みとしては、

(1) Telecom-ISAC Japan の活動強化
(2) セキュリティ技術に関する研究開発の推進
(3) セキュリティ技術の研究開発体制の充実・強化
(4) その他の重点的に検討すべき取り組み（利用者の啓発・教育、ネットワークセキュリティの充実に向けた環境整備）

があり、それぞれについて適切な取り組みを行っていくことが必要である。

4.1 Telecom-ISAC Japanの活動強化

4.1.1 Telecom-ISAC Japan の概要

(1) 設立の背景及び趣旨

近年、不正アクセス、ウィルス/ワーム、ＤｏＳ攻撃などによる被害が世界中で多発しており、サイバー空間における脅威は今後ともますます増加する傾向にある。特に、インターネットを代表するネットワーク通信基盤の安全性確保が大きな課題である情報通信業界では、ネットワーク通信基盤を揺らがすセキュリティに関わる事故・事件（インシデント

と呼ぶ）に対する早期のセキュリティ対策・対応が強く望まれている。しかしながら、情報通信業界における実態を見ると、個々の事業者における個別の取り組みに委ねられているのが現状であり、情報セキュリティ対策の重要性が今後ますます高まっていくことを考えれば、情報通信業界として一丸となった一層の取り組みが求められる。一般的に、情報システムに対する各種インシデントは、業界毎に一定の特徴を持ちやすい傾向にあることから、実際に発生したインシデントに関する情報を業界内で分析・共有することが情報セキュリティ対策の確保に有効であることは言うまでもない。

このような考え方に基づき、米国及び韓国においては、通信、金融などの重要インフラ業界において既に ISAC（Incident Sharing and Analysis Center）が設立されており、我が国の情報通信業界においても、同様の仕組みを早急に構築することが強く求められいるところである。

(2) 設立の目的

我が国の重要インフラである情報通信基盤の安全を確保することは、各種通信サービスを提供する情報通信事業者にとって、最重要課題であると言っても過言ではない。

「Telecom-ISAC Japan」は、情報通信事業者（以下「会員」）のビジネス基盤となる情報通信基盤（インフラ）の安全性確保を広義の目的として、通信サービスの提供を妨げる各種インシデントを収集・分析し、その分析結果を会員間で共有することにより、当該インシデントに対する強固な情報通信基盤の提供を目指す。

具体的に「Telecom-ISAC Japan 」は、参加資格要件を満たした会員間で対象とするインシデントに対する防護連携を図るもので、会員間でのインシデントに関する適切な情報共有をはかるための場の提供及び、会員間の連絡・連携をはかる中立且つ信頼された機関としてその責務を負う。従って、「Telecom-ISAC Japan」は、対象とするインシデントの情報収集、情報共有、インシデント分析、分析情報提供を行う「信頼された中立的組織」として運営されなければならない。これらの分析結果に基づき、情報通信業界におけるインシデントに対する防御連携を円滑に図り、重要インフラの安全性確保に資することを目指している。

さらに、他のインシデント対応組織（NIRT、JPCERT/CC 等）との間での情報共有、連携を柔軟に提供することも Telecom-ISAC Japan の大きな使命のひとつである。以下、図 4-1-1 に Telecom-ISAC Japan の構想イメージを示す。

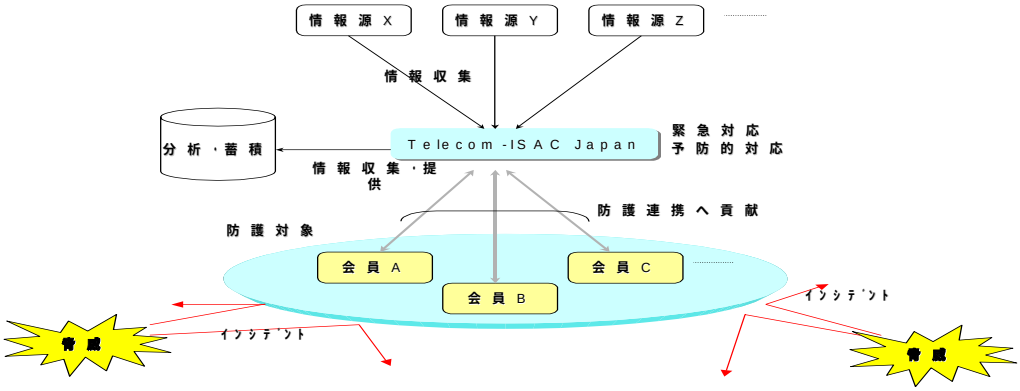

図 4-1-1　Telecom-ISAC Japan の構想概念

(2)　Telecom-ISAC Japan による提供サービスと現状

2002 年 7 月の発足以降、Telecom-ISAC Japan では、提供すべきサービス内容の選定の検討を進め、図 4-1-2 で示すとおり、６つのサービスコンセプトに基づく構想を固めた。これらのサービス内容の概要は以下のとおりである。

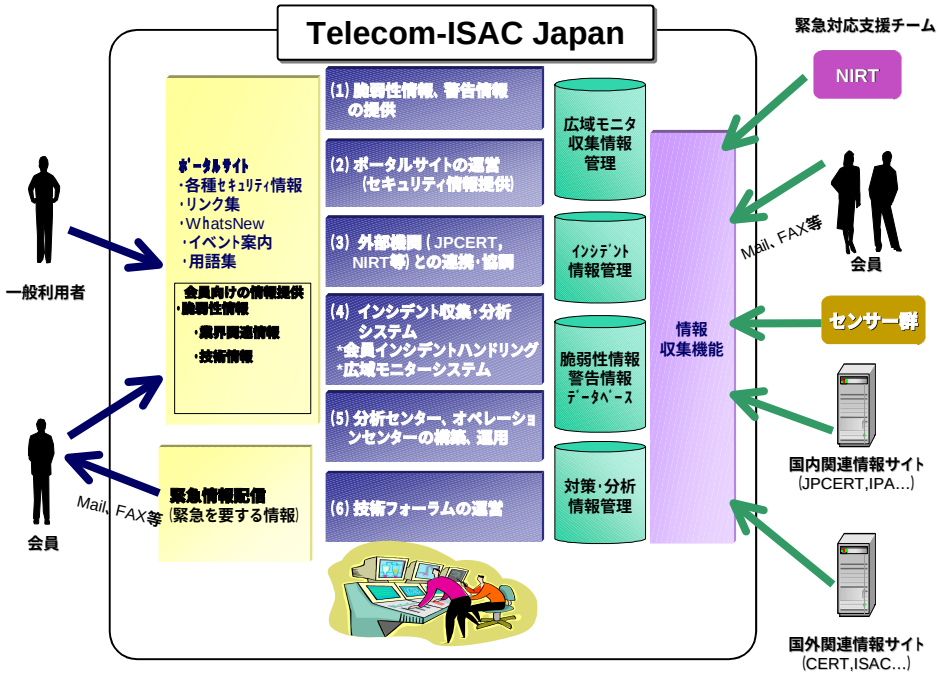

図 4.1-2　Telecom-ISAC Japan 提供サービス内容構想

＜サービス構想＞

a) **脆弱性情報、警告（アラート）情報の提供（運用中）**

テレコム業界の情報通信システム基盤に大きな影響を与える脆弱性情報、有益な警告（アラート）情報を調査・収集しISACサイトのポータルから会員間で共有する。また、会員の要望に沿ったフィルタリング機能を搭載する。

b) ポータルサイトの運営（セキュリティ情報の提供など）　（上記 a）と連動運用中）

上記a)の情報、その他のセキュリティ情報（製品情報、各種セミナー情報等）、Telecom-ISAC Japan紹介情報などの提供を目的としたポータルサイトの立ち上げ、 運用を実施する。

c) 外部機関との連携、協調（H15年度検討開始）

JPCERT/CC、NIRT、他国Telecom-ISACとの連携を図り、情報交換・共有などの連携共同作業を実施する。

d) インシデント収集・分析システムの構築（H14年度検討開始）

会員で起きたインシデント情報の申請・分析依頼を実現するインシデントハンドリングシステム及び日本に広域的に存在するISPのセキュリティ情報を自動モニタすることにより、インシデント分析に資するための広域モニターシステムの構築を実施。

e) 分析センター、オペレーションセンターの構築・運用（H15年度から検討開始）

上記 d)で収集したインシデント情報の傾向分析、頻度分析、影響度分析を実施する分析センター及びそれらの真偽度確認のための試験環境（テストベット）を構築する。さらに、上記 d)と連動したオペレーションセンターの構築・運用を実施する。

f) 技術フォーラム（H15年度から段階的に開始）

技術フォーラムを立ち上げることにより、テレコム企業間の技術・情報共有を行い、ISACへの要求条件の整理、検討を実施し、これらの要件の吸い上げ、ISACセンタ機能向上に反映させる。

＜現状の提供サービス＞

2003 年 3 月 31 日から上記（１）と（２）を組み合わせた、脆弱性情報及びアラート（警告）情報を提供するポータルサイトを開設した。本サービスは、Telecom-ISAC Japan における初期サービスであり、基本的なセキュリティ情報を会員に提供するサービス内容である。脆弱性情報の提供においては、海外から調査・収集した脆弱性情報を翻訳してデータベース化し、迅速な脆弱性情報を提供している。また、アラート情報提供については、調査・収集した脆弱性ならびに悪質なソフトウェアに関する警告情報を会員にメールなどで通知するサービスを実施している。

これらの情報提供サービスは、一般ユーザ用の情報提供と理事会員メンバ（7 社）用の情報提供とに分かれており、一般ユーザには、「 Telecom-ISAC Japan 」の概要説明等の紹介情報を提供し、会員には具体的な脆弱性情報、アラート情報の提供を実施している。各アクセス URL は以下のとおりである。本基本サービスイメージを図 4-1-3 で示す。

一般ユーザアクセス用 URL: https://www.telecom-isac.jp/

会員メンバ用 URL：https://www.telecom-isac.jp/member/

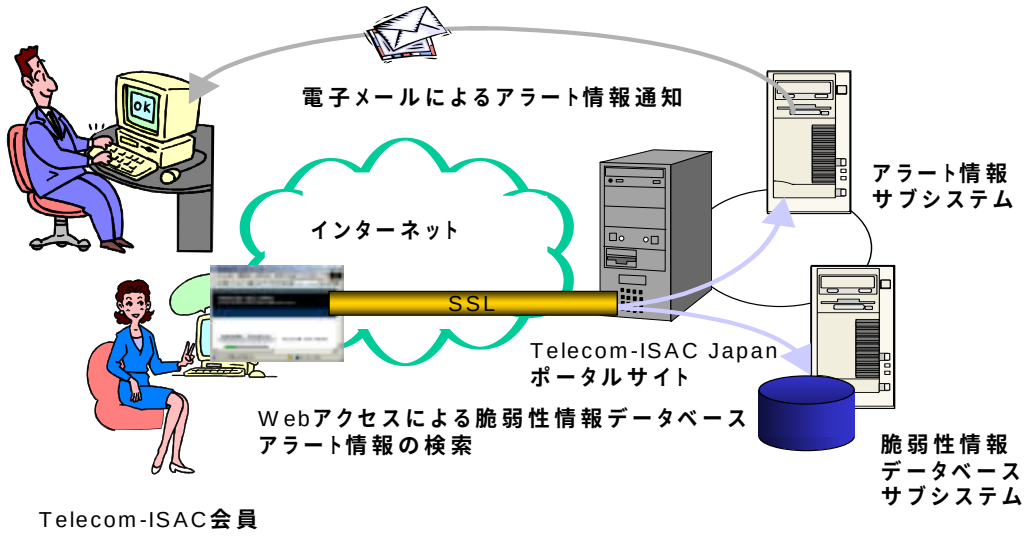

図 4-1-3　提供サービスのシステムイメージ

4.1.2　Telecom-ISAC Japan の今後の取り組み

現状の 4.1.2 で述べた情報提供サービスに加えて、インシデント収集システム、インシデント分析センター、総合的な Telecom-ISAC Japan のオペレーションセンターの構築が重要となる。さらに、他情報提供サービス（JPCERT、NIRT 等）とのサービス連携も重要な課題となる。以下に各サービス内容の構想を述べる。

(1)　インシデントハンドリングシステムの構築（構築中）

インシデント収集・分析システムの一環として、メンバサイトにおいて発覚したインシデント情報に関わる分析を目的として、メンバから該インシデントの申請を ISAC に対して実施できる仕組み（インシデントハンドリングシステム）の構築を進める。具体的には、Telecom-ISAC Japan は、会員からのインシデント分析依頼を受付けて、それに関連する情報と分析結果を返す。また、処理されたインシデント分析結果を全会員に公開し、会員間で情報共有する。（図 4-1-4 参照）

本サービスの提供を受けることにより、会員の所属企業だけでは解決できないインシデントに対して、高度なインシデント分析の支援を得ることができる。本技術支援により、インシデントの影響の拡大抑止、インシデントに対する効果的な対策、インシデントからの迅速な復旧が可能となる。また、インシデントが広範囲に及ぶ場合は会員間の調整も依

頼できる。さらに、分析された様々なインシデント情報を会員間で共有することにより、インシデント発生の未然防止を行うことも可能となる。

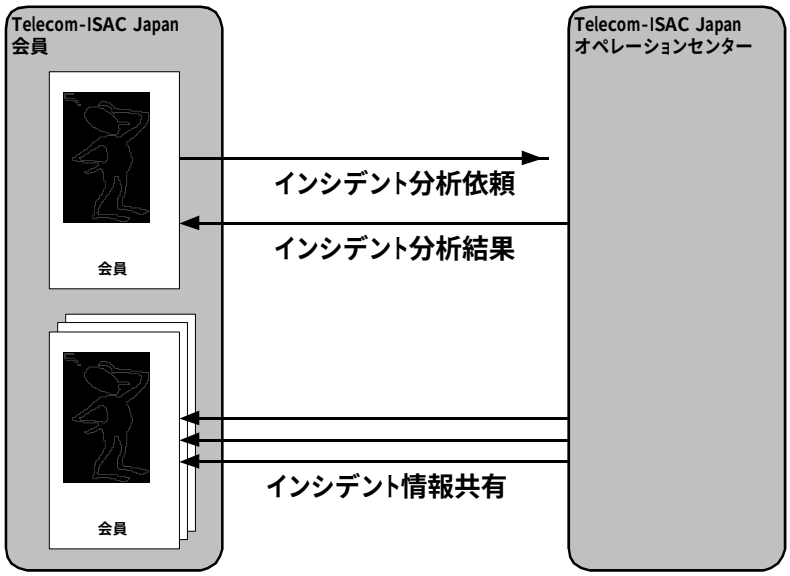

図 4-1-4　インシデントハンドリングシステム

(2)　広域モニターシステムの構築（設計中）

インシデント収集・分析システムの一環として、ISP(インターネットサービスプロバイダ)を中心とする国内ネットワークの各拠点にセキュリティ情報を収集するための機器を配備することにより、１局集中型のセンタにてセキュリティ情報を迅速に収集・分析し、各拠点におけるサイバーテロによる汚染状況・被害状況を実時間で把握し、互いの情報共有を行うことができる研究開発基盤の整備を実施する。このことにより、ハッカーの具体的な挙動・攻撃傾向を把握し、早期の警戒情報の策定を容易とすることを目指す。

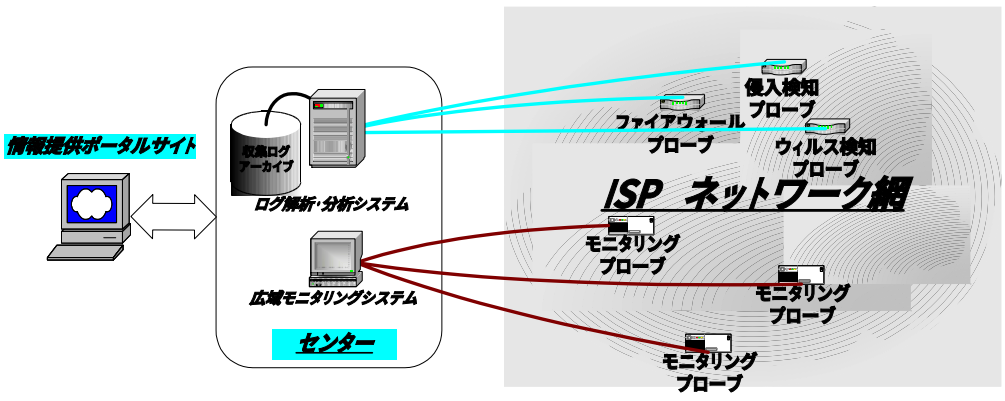

図 4-1-5　**広域モニターシステム**

(3)　**インシデント分析センタ構築**

上記のインシデントハンドリングシステム及び広域モニターシステムの構築において、さらなる高度なインシデント分析を実施するため、これらの ISAC **システムと強く連携を行うインシデント分析センタの構築が必要となる。本分析センタにおいては、通常の傾向分析や頻度分析だけではなく、インシデント相関分析、閾値学習分析、プロファイル分析などの高度分析手法によるインシデントの解析を実施する。本解析・分析結果は、会員メンバ間で共有され、メンバ内/間における高度なインシデント対策に資することが可能となる。本分析センタは、独立行政法人通信総合研究所（**CRL**）及び通信・放送機構（**TAO**）の中に数十名の分析専担チームを結成し、分析専門の研究開発を実施する予定である。**CRL、TAO **及び** Telecom-ISAC Japan **の間では、共同研究を実施し、密な連携をもった分析作業を行う。（**CRL **及び** TAO **は、平成** 16 **年** 4 **月より独立行政法人情報通信研究開発機構に統合される予定である。）**

(4)　Telecom-ISAC **オペレーションセンタ構築**

インシデントハンドリングシステム、広域モニターシステムの構築において、ISAC **運用を円滑化させ、実効的なシステムとして機能させるためには、**ISAC **のためのオペレーションセンタの構築が必須となり、今後構築に向けた検討を行う必要がある。**

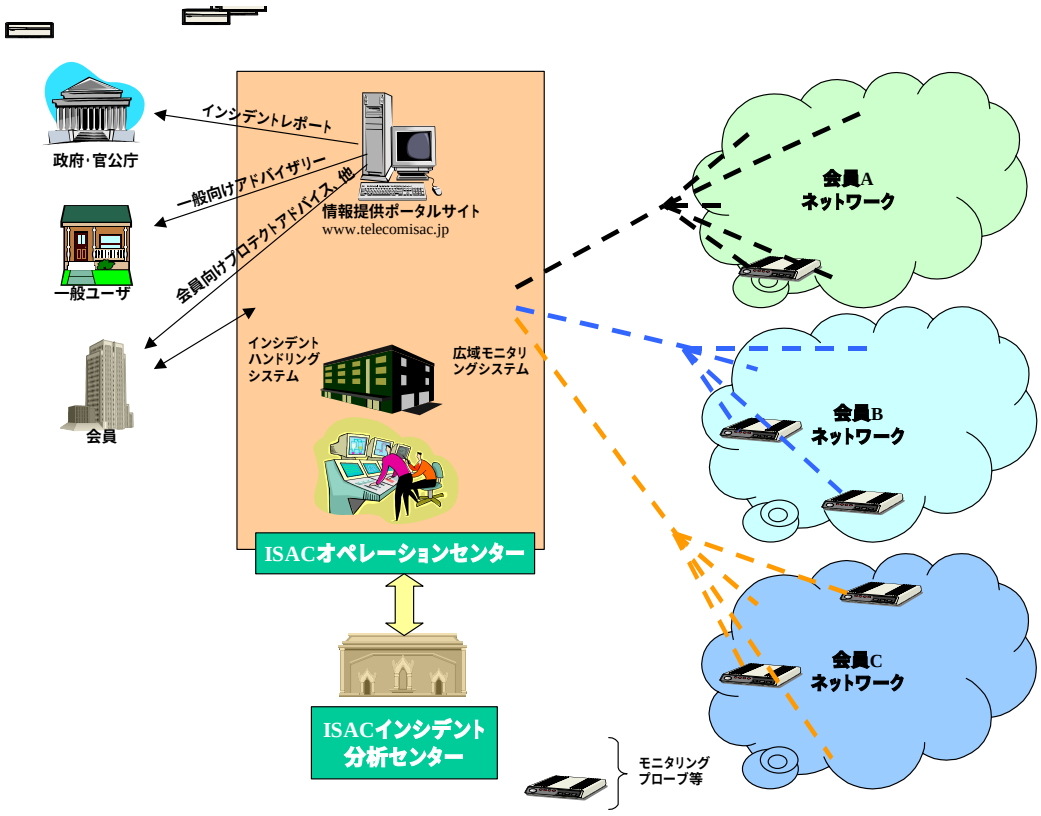

図 4．1-6　ISAC オペレーションセンタ

4.1.3　外部機関との連携

外部団体との情報交換、情報共有は、ISAC 機能を活性化させるために重要となる。Telecom-ISAC Japan としては、当面、連携の対象となる外部団体としては、以下を検討中である。

(1) 緊急対応支援チーム（NIRT）との連携

NITR は、内閣官房情報セキュリティ対策室が主管となり、各省庁の緊急対応支援を提供する専門チームである。本チームでは、チーム内で検討した被害防止対策を省庁以外の関連部門へ配布する形態を想定している。今後は、Telecom-ISAC Japan としては、NIRT との情報共有を行うことにより、多方面からの情報に基づく分析に資することとしたい。

(2) JPCERT コーディネーションセンター（JPCERT/CC）との連携

インシデント収集分析システムの構築にあたり、JPCERT/CC の検討中の定点観測システムとの連携が必要となる。Telecom-ISAC Japan では、ISP を主眼としたモニター点を想定す

るインシデント収集・分析を実施するが、JPCERT/CC では、企業一般をモニター対象としたインシデント収集を実施する。収集情報、分析結果の共有及び分析手法などの共同開発などの連携を進めていく予定である。

4.1.4 海外機関との連携

米国 Telecom-ISAC（NCC　ISAC）は、米国商務省の主管で 2000 年 3 月に運用を開始し、情報通信事業者、通信機器ベンダー、ソフトウェアベンダーが多数参加している ISAC である。現段階では、詳細な分析手法やサービス内容が開示されていないが、今後直接的なコンタクトをもち、情報共有などの連携を強化する予定である。

また、韓国 Telecom-ISAC も同様に運用を開始しているが、現段階ではセキュリティ情報の提供にとどまっており、インシデントハンドリングや広域モニターシステムなどの提供には至っていない。本 ISAC とも連携をとって進めていく予定である。

4.2 研究開発の推進

3.3 で述べたように、現在のインターネットを構成している基本的なコンポーネントの中には、セキュアでないコンポーネントも利用されているため、インターネットを構成している基本的なコンポーネントをよりセキュアにしていくための要素技術の研究開発も重要である。

しかしながら、インターネットをライフライン化するために研究開発が必要となるセキュリティ技術は、非常に多岐で広範な分野にわたるため、研究開発が達成すべき技術目標を設定し、当該目標に関連する要素技術について集中的に研究開発を行うことが、研究開発の効率化と研究成果の明確化といった観点から有効である。

この広範な研究分野において中心的な役割を果たすセキュリティ技術の中で、前述の Telecom-ISAC Japan の活動のために緊急に研究開発を行うことが期待される、サイバーテロ対策に係る技術及び今後の電子商取引の更なる発展の基盤となる技術の研究開発を特に実施していくことが必要である。

4.2.1 サイバーテロ対策に係る技術の研究開発

サイバーテロ対策に係る技術は、大きく、サイバーテロを防止するための技術、サイバ

ーテロを早期に検知するための技術、サイバーテロに対抗するための技術、の 3 つが考えられるが、サイバーテロ対策が十分な効果をあげるためには、その 3 つのいずれについても研究開発を継続的に進めていくことが必要である。

(1) 取り組みの目的

サイバーテロを計画するものは国家の重要インフラを第一のターゲットとするであろうから、3.1 で述べた重要インフラの防護は重要な課題である。しかしながら、サイバーテロは重要インフラを直接のターゲットとするとは限らない。インターネットの基本コンポーネントを攻撃し、インターネット自体を麻痺させることができれば、警戒厳重な重要インフラを攻撃するのと同じ効果を簡単に得ることができる。

3.2 で述べたように、サイバー攻撃の手口はますます多様化・複雑化してきている。例えば、SQL Slammer 事件のように、セキュリティ意識の低い一般ユーザが使用している端末を踏み台として DDoS 攻撃が行われた場合、本当の犯人を特定することは現状では極めて困難である。

さらには、3.3 で述べたように、インターネット自体がその基本コンポーネントに脆弱性を持ったものが含まれている。

我が国が強くインターネットに依存してきている現状を考えると、一旦、サイバーテロが発生した場合の影響・被害の大きさは計り知れないものであり、サイバーテロ対策に係る技術の研究開発は緊急の課題であり、Telecom ISAC Japan が活動するために必要不可欠の取り組みであるといえる。

(2) 具体的な取り組み内容

サイバーテロ対策に係る技術の具体的な研究開発項目としては以下が技術が挙げられる。

(a) 広域モニタシステム構築技術
(b) 広域モニタ及び各種ファイアウォール、IDS 等のアラートログ分析技術
(c) 高精度トレースバック技術
(d) 未知のサイバー攻撃検知技術
(e) インターネットの基本コンポーネントのセキュア化

(a) 広域モニターシステム構築技術

サイバーテロの被害を最小限に抑えるためには、サイバーテロを初期の段階で察知し、すばやく対抗措置を講じることが重要である。サイバーテロを初期の段階で察知するためには、広域にモニタを設置して、情報を収集することにより、サイバーテロの具体的な挙動・攻撃傾向を把握することが有効である。特に、セキュリティの低い利用者端末を踏み台とする DDoS 攻撃のようなサイバー攻撃には通信事業者や ISP が提供するネットワークからの情報収集が有効であるため、通信事業者や ISP を中心とする国内ネットワー

クの各拠点にセキュリティ情報を収集するための機器を設置し、セキュリティ情報を収集・共有する仕組みを整備する必要がある。

そこで、通信事業者や ISP を中心とする国内ネットワークの各拠点にセキュリティ情報を収集するための機器を設置し、１局集中型のセンターにおいてセキュリティ情報を迅速に収集するための技術を開発する必要がある。

(b) 広域モニター及び各種ファイアウォール、IDS 等のアラートログ分析技術

国内ネットワークの各拠点にモニタを設置して情報を収集することにより、サイバーテロの具体的な挙動・攻撃傾向を把握することができるようになる。また、重要インフラなどに設置されたファイアウォールや IDS 等から情報も加味することによって、その精度は更に高くなると期待できる。

しかしながら、モニタから収集される情報の中から実際のサイバーテロに関する情報のみをいち早く取り出すことができなければ、早期に警戒情報を策定することはできない。

そこで、上記取り組みによって広域に設置されたモニタや各種ファイアウォール、IDS 等から収集された情報を分析し、リアルタイムにサイバーテロの汚染状況・被害状況を把握し、Telecom-ISAC Japan やその他のインシデント対応組織がすばやく情報共有を行うことができる技術を開発する必要がある。

(c) 高精度トレースバック技術

現在のインターネットでは、不正の発覚が分かっても真の犯人が識別できず、抑止力が働かないので、不正が増加する、という問題がある。例えば、セキュリティ意識の低い一般ユーザが使用している端末を踏み台として DDoS 攻撃が行われた場合、本当の犯人を特定することは現状では極めて困難である。

そこで、通常用いられている、トラフィックの流量による経路探索技術ではなく、インターネットを流れている不正パケットの特徴を記録し、その痕跡に基づいて不正パケットごとに対して不正侵入を追跡（トレースバック）できる技術の研究開発が必要である。

(d) 未知のサイバー攻撃検知技術

現在のサイバー攻撃の検知手法は、既に知られている攻撃手法の特徴をパターンとしてデータベース化しておき、そのデータベースと照合を行うことによって、サイバー攻撃が行われているか否かを判定する。ウィルスへの対策はこの典型例である。

しかしながら、3.2 で述べたように、ウィルスが流行してからそのウィルスのパターンが配布されるまでには時間差が生じるため、短時間で感染するウィルスの場合にはその被害が甚大になってしまう。

さらには、今後は、感染するごとにコードが変化する新世代のウィルス（メタモルフィックウィルス）が登場するとの予測もあり、既存の対策手法では対応が困難となると考えられる。

ウィルスに対しては閉じた環境や仮想的な環境でウィルスの可能性のあるコードを実行し、動作を確認した上で、実際の環境での実行を許可する、といった手法が有効であると考えられるが、この手法では検出に時間がかかるという問題がある。また、ウィルス以外のサイバー攻撃に対しては有効な手法はあまり提案されていない。

そこで、このような未知のサイバー攻撃でも迅速に検知することができる技術の研究開発が必要である。

e) モバイルセキュリティの強化

2.2 で述べたように、我が国では携帯電話によるインターネット接続が広く普及している。最近の携帯電話は高機能化も進んでおり、重要システムにアクセスするに十分な機能を備えてきている。また、無線 LAN も普及してきており、各所に公衆アクセスポイントが設置されるようになってきている。

このような状況を鑑みると、近い将来には、モバイルアクセスもまた重要インフラとなることが予想される。

しかしながら、3.3 で述べたように、現在の無線 LAN はセキュリティ上の脆弱性を抱えているなど、モバイルアクセス自体はサイバーテロの対象となりやすいと言える。

また、モバイルアクセスを突破口としたサイバーテロの可能性も考えられる。さらには、移動しながらサイバーテロを実行することによって攻撃者の追跡を困難にする、などモバイルの特性を利用することも考えられる。

そこで、PKI のような高度なセキュリティ機能をモバイル端末に負荷をかけずに利用できるモバイルアクセス技術を開発するなどモバイルセキュリティの強化が必要である。

(f) インターネットの基本コンポーネントのセキュア化

3.3 で述べたように、インターネットを構成する基本コンポーネントの中には脆弱性を含んだコンポーネントが存在している。我が国がインターネットに強く依存するようになった現在、その基本コンポーネントの脆弱性は、サイバーテロの格好の対象となりうる。

そこで、こうしたインターネットの基本コンポーネントをセキュア化する技術の研究開発が必要である。

なお、基本コンポーネントをセキュア化するについては、開発した技術への移行をスムーズにするためにも、従来の基本コンポーネントとの相互接続性を確保する必要がある。

さらには、取り組みを進めるにあたっては、欧米諸国、アジア諸国、IETF、ISO、ITU-T

などの国際標準化団体と密接な連携を取ることが望まれる。

4.2.2 インターネット自体の安全性・信頼性を向上し、電子商取引の発展の基盤となる技術の研究開発

インターネット自体の安全性・信頼性を向上し、電子商取引の更なる発展を促すためには、アクセスしてきた利用者が確かに本人であるかどうかを確認し、その利用者のセキュリティレベルに見合ったサービスを提供できるようなネットワーク基盤を実現する技術、すなわち、本人確認機能を持ったネットワーク基盤を実現するための技術の研究開発が必要である。

(1) 取り組みの目的

現在のインターネットで電子商取引などのサービスを提供するためには、サービス提供者が、セキュリティを確保するためのハードウェア・ソフトウェアの全てを用意する必要がある。

特に、近年のサイバーインシデントの増加はサービスを提供する際のセキュリティ対策を必然のものとしており、サービス提供者は、サービスのための各種アプリケーションにセキュリティ機能を組み込み、セキュリティを確保する必要に迫られている。

これは、アプリケーション開発の複雑化、アプリケーション開発コストの増大に結びついている。

このため、現状では、高度なセキュリティ要素技術が開発されたとしても、サービス提供者がそうしたセキュリティ要素技術を採用しないため、インターネットの安全性・信頼性がなかなか向上しない、という結果になっている。

例えば、相手を確認したり、自身の正当性を証明したりする手段として、PKI のような暗号技術を活用した高度な認証技術も研究開発されている。しかしながら、サービス提供者側のセキュリティに関する関心や意識の低さ、あるいは景気の低迷による設備投資の凍結のため、セキュリティが低い、ID とパスワードによる認証方式が未だに各所で使われつづけている、という現状などはその証左であるといえる。

また、アプリケーション毎にセキュリティ対策が行われている現状は、サービスを利用するための設定の複雑化・ユーザ利便性の低下をも生みだしており、ひいては、セキュリティに関する設定の不備や複数のアプリケーション間でのセキュリティ機能の連携の不備によるセキュリティの低下が生じる原因ともなっている。

例えば、現在はパソコンという汎用的な端末を利用者が操作し、利用者自らが基本パラ

メータを入力したり、ソフトウェアパッチを適用したりしている。この結果、利用者がパラメータを誤ったり、ソフトウェアパッチを適用しなかった結果、セキュリティの低い端末がインターネットに接続されてしまう。2.3 で述べた、SQL Slammer 事件では、このようなセキュリティの低い端末が乗っ取られ、インターネット全体のセキュリティを脅かすことになってしまった。

3.2 で述べたように、攻撃手法はますます高度化・多様化してきており、現状のままでは、サービス提供者が提供しなければならないセキュリティ機能や、利用者が設定しなければならないセキュリティ設定は今後ますます複雑になっていくと考えられる。

現在、高度なセキュリティ要素技術が簡単・手軽に利用できない原因の一つは、現状のインターネットがネットワーク基盤としては何らのセキュリティ機能も提供しないことにある。現在のインターネット上にセキュリティ機能を提供するネットワーク基盤を構築することにより、サービス提供者のアプリケーション開発コストの低減と、利用者のセキュリティ設定の簡略化を実現することができる。この結果、様々なサービスの提供や利用者の増加などが見込まれ、電子商取引の更なる発展が促されると期待できる。

様々なセキュリティを実現する上での基礎となるのが、行為を行っているのが誰であるのかを特定する「認証」である。したがって、セキュリティ機能を提供するネットワーク基盤を構築するための基礎となる技術は、アクセスしてきた利用者が確かに本人であるかどうかを確認し、その利用者のセキュリティレベルに見合ったサービスを提供できるようなネットワーク基盤を実現する技術、すなわち、本人確認機能を持ったネットワーク基盤を実現するための技術であると考えられる。

(2) 具体的な取り組み内容

本人確認機能を持ったネットワーク基盤を実現する技術の研究開発の具体的な研究開発項目としては以下のものが挙げられる。

a) ネットワークに本人確認機能を持たせるための技術の研究開発
b) 本人確認機能を持ったネットワーク基盤において、安全な通信環境を確立するための技術の研究開発
c) 安全な通信のための IC チップ利用技術の研究開発
d) 利用者の端末を安全に保つための技術の研究開発
e) 本人確認機能を持ったネットワーク基盤の運用監査体制の確立
f) 本人確認機能を持ったネットワーク基盤の実証実験の展開
g) 本人確認機能を持ったネットワーク基盤の国内標準化・国際間連携の推進

a) ネットワークに本人確認機能を持たせるための技術の研究開発

現状では、通信を行う者同士がお互いに通信相手が誰であるのかを直接に認証し、サービス提供や通信を許可してよいかどうかの権限の確認（アクセス制御）を行っている。ネットワークが本人確認機能を持つ場合、通信相手の認証や、アクセス制御をネットワークが行うことになる。そこで、ネットワークに本人確認機能を持たせるためには、ネットワーク基盤が信頼できる仲介者（メディエータ）として通信相手を相互に認証し、通信相手の身元を保証し、アクセス制御を行う技術を開発する必要がある。

また、ネットワーク側で本人確認やアクセス制御を行うためには、本人であることや、アクセス権限を確認するための基礎となる情報をネットワークで持つ必要がある。これらの情報のネットワーク側での管理方法やその技術についても研究が必要である。

b) 本人確認機能を持ったネットワーク基盤において、安全な通信環境を確立するための技術の研究開発

現在のインターネットでの通信のセットアップ手順では、通信する者同士が自己責任で、通信相手の探索、相手の認証、通信設定の調停、等を当事者間で直接行っている。

そこで、ネットワークが本人確認機能を持っていることを前提とし、通信の開始から終了・切断まで、あるいは通信設定の決定や、通信品質の制限など、通信全体のコーディネートをネットワークが行い、安全な通信環境を確立するような、新たな通信技術の開発が必要である。

c) 安全な通信のためのICチップ利用技術の研究開発

本人確認機能を持ったネットワークがコーディネートした通信環境を使って、通信相手とのP2P通信を安全に行うためには、さらに、P2P通信の盗聴や改ざんを防止するための鍵を交換する必要がある。

今後は、様々な情報通信機器からネットワークにアクセスすることが予想されるが、こうした情報機器ごとに上述の機能が異なって実装された場合、利用者の使い勝手が非常に悪くなると予想される。これに対しては、セキュリティ機能を集約したICチップを様々な情報機器に搭載することが有効であると考えられる。

そこで、セキュリティ機能を集約したICチップを情報通信機器に搭載し、そのICチップを利用することで、ダイナミックにVPNを確立することを可能とする技術を開発する。

d) 利用者の端末を安全に保つための技術の研究開発

ネットワークにセキュリティの低い端末が接続された場合、SQL Slammer事件のよう

にネットワークの機能を完全に麻痺させるようなサイバーインシデントが発生する可能性がある。このような問題を回避するため、利用者を教育・啓発すると同時に、利用者端末のセキュリティレベルに見合ったサービスをネットワークが提供することも有効であり（例えば、新しいセキュリティパッチやワクチンが発行されていれば、利用者に通知するなど）、通信を試みている利用者の端末や通信を受ける利用者の端末が適切なセキュリティ状態にない場合には、ネットワークがそのセキュリティ状態を高める技術を開発する。

e) 本人確認機能を持ったネットワーク基盤の運用監査体制の確立

本人確認機能を持ったネットワーク基盤が実際のサービスに供された場合には、そのネットワーク基盤が適切に運営されていることを利用者やサービス提供者に保証する必要がある。そのため、ネットワーク基盤の運営管理基準（ガイドライン）を作成し、広く公開する必要がある。（一例としては、ICチップ発行主体の運営管理基準などが考えられる。）

さらには、ネットワーク基盤が上述の運営管理基準に従って適切に運営されていることを監査する体制を整備する必要がある。

ｆ) 本人確認機能を持ったネットワーク基盤の実証実験の展開

本人確認機能を持ったネットワーク基盤を利用した新たなサービスが実際に実用展開されていくためには、技術の研究開発から実ビジネスへ展開していくための支援措置を講じていくことが必要である。この支援措置により、利用者の潜在的需要が喚起され、さらにそのニーズに支えられて、独創的なアイデアを持ったサービスが続々と生み出されていく、という好循環が期待される。

具体的には、本人確認機能を持ったネットワーク基盤を利用したアプリケーションの実証実験を展開し、より多くの利用者が自由に実験に参加したり、様々なサービス提供者が実験基盤の上で自由にサービスを提供することによって、より多くの参加者が実験基盤の評価を繰り返すことが重要である。

一方では、新たに構築した本人確認機能を持ったネットワーク基盤でも、電子商取引やIP電話など、現在のインターネットで実際に幅広く利用されているアプリケーションが問題なく動作し、さらには、これらの既存アプリケーションが本人確認機能を持つネットワーク基盤を利用することによりセキュリティが高くなることを実証することが望ましい。

さらには、様々な信頼度のネットワーク基盤が存在する場合でも、利用者やサービス提供者の利便性が低下することなく、できる限り高いセキュリティを保った通信が行え

ることを検証する必要がある。

g) 本人確認機能を持ったネットワーク基盤の国内標準化・国際間連携の推進

本人確認機能を持ったネットワーク基盤は、通信事業者やISPなど複数の運営主体によって少しずつ提供される機能が異なることが考えられる（例えば、特定の業者に向けた特別な機能を提供するなど）。

一方では、複数のネットワーク基盤が存在する場合には、あるネットワーク基盤の利用者が別のネットワーク基盤の上で提供されているサービスを利用する場合も考えられる。

このとき、似たような機能を提供してはいるが、相互接続性がないネットワーク基盤が乱立する状況が発生した場合、利用者やサービス提供者の囲い込みが発生し、市場が断片化してしまうことになる。これは、個々のネットワーク基盤で提供されるサービスが限定されたものとなる結果を生み、利用者がネットワーク基盤の利用を控え、市場が更に縮小していく、という悪循環に陥る危険性が高い。このような悪循環を発生させないためにも、上述の取り組みによって開発・実証した、本人確認機能を持ったネットワーク基盤に関する技術を広く公開し、国内標準化を推進する必要がある。

また、複数のネットワーク基盤の間で、できる限り高いセキュリティを保った通信を行うための技術や、その際に相互にやり取りされる情報の保護技術を開発する必要がある。

さらには、本人確認機能を持ったネットワーク基盤に関する技術を、次世代のネットワーク技術の一つと位置付け、日本発の標準確立を目指し、国際電気通信連合（ITU）等の国際標準化団体への提案や、欧米・アジア各国との共同研究などの連携の強化を推進する。

なお、前述の取り組みと、インターネットを構成する各コンポーネントをセキュアにしていく取り組み、特にサイバーテロ対策に係る技術の研究開発とは、互いに補完関係にあり、両取り組みを併行かつ継続的に実施していくことがインターネット自体の安全性・信頼性を向上するためには必要不可欠である。

4.3　セキュリティ技術の研究開発体制の充実・強化

前述の米国における実験「Eligible Receiver」によって明らかになったように、サイバーテロにより、重要インフラをはじめとする国家の中枢機能を麻痺させることも可能であり、情報セキュリティにかかる技術の研究開発は、極めて重要な課題である。他方で、情報セキュリティに係る技術は、非常に多岐にわたる上に、情報セキュリティに脅威を与える側の技術・手法は、常に高度化・多様化していることから、これらに適切に対応するためには、情報セキュリティに関する研究開発の拠点構築による体制の強化・充実は、焦眉の急であると言える。また、我が国における情報セキュリティ人材の不足がしばしば指摘されるが、研究開発体制の強化・充実により、多数の優秀な情報セキュリティ技術者の輩出も同時に期待できる。

さらには、「4.1　Telecom-ISAC Japan の活動強化」の項でも触れたが、Telecom-ISAC Japan のような情報セキュリティ対策・インシデント対応の実践を行う組織と研究開発機関との連携の強化が極めて重要である。Telecom-ISAC Japan がインシデントハンドリングや広域モニターなどの活動を実施するに当たっては、収集した各種情報の分析・解析が不可欠であるが、研究開発機関との連携により、分析・解析機能の高度化を図ることが可能となり、実際の情報セキュリティ対策・インシデント対応の充実に寄与するところは非常に大きい。

他方で、研究開発機関の側から見た場合、Telecom-ISAC Japan との連携を図ることにより、Telecom-ISAC Japan がインシデントハンドリングや広域モニターなどの活動を通して収集した各種情報を研究材料として活用できるというメリットがある。特に我が国においては、各企業はインシデント情報などを外部に明らかにすることを躊躇する傾向にあり、純粋にアカデミックな研究活動においては、研究材料として、豊富なインシデント情報を収集することは困難である。

したがって、情報セキュリティ技術に係る研究開発体制の充実・強化として、ヒト・モノ・カネなどのリソースの充実により研究開発・人材育成の拠点構築を図ることに加えて、Telecom-ISAC Japan をはじめとする情報セキュリティ対策・インシデント対応を実践する組織との連携強化を併せて実施することによって、大きな相乗効果を期待することができるものと考えられる。

4.4　利用者の教育・啓発等

3.4 で述べたように、インターネットの利用者サイドの意識啓発が、インターネットを日

本国国民誰もが安心・安全に参加できるネットワーク社会を実現するためには必要不可欠である。
したがって、その他の重点的に検討すべき取り組みとして以下のようなものが考えられる。

① インターネット利用者の教育・啓発
② ネットワークセキュリティの充実に向けた環境整備

① インターネット利用者の教育・啓発

ネットワークにセキュリティの低い端末が接続された場合、SQL スラマー事件のようにネットワークの機能を完全に麻痺させるようなサイバーインシデントが発生する可能性がある。すなわち、現状は、ネットワーク利用者のセキュリティ意識の低さがインターネット全体のセキュリティを脅かす可能性があるという状況であり、利用者のセキュリティ意識の向上なくしてはセキュリティ水準の底上げはなしえない。

一方、利用者といっても、情報セキュリティとの関係でいえばその幅は広く、例えば、企業の内部を考えても、システム管理部門の職員（相当程度のセキュリティ知識が必要)、一般社員（企業内 LAN の利用者として、主に利用上の知識が重要)、経営者（セキュリティポリシー上の最高責任者として大枠の意識・知識が必要）等、利用者のセグメントにより、持つべき意識や知識のレベルにも相当広がりがある。

したがって、ネットワーク利用者を様々なセグメントに分類し、そのセグメントごとに適切な教育・啓発のあり方について検討していく等の取り組みが今後必要であると考えられる。

ブロードバンド・常時接続の普及に伴い、家庭の個人ユーザのセキュリティ意識の向上もますます重要となっているが、一般ユーザのセキュリティ意識の向上を図るには、多様な取り組みを着実に推進していくことが必要である。ホームページを利用した意識啓発の取り組みとして、総務省の「国民のための情報セキュリティサイト」等においては、一般ユーザ向けのセキュリティ意識の普及啓発に努めている。今後も、こうした取り組みの一層の充実が必要である。

また、国や公的機関による情報提供とともに、個人ユーザにとって身近な存在である ISP の取り組みも重要である。

ISP は、安全安心マーク制度等を通じて、ユーザに対するセキュリティ情報の提供を推進しており、今後も同制度の普及等を通じて、ユーザへの情報提供を充実していくことが効果的であり、一層の推進が必要である。

また､ウィルスチェックサービス等 ISP によるセキュリティ支援機能の普及を通じてセキュリティ対策に係る負担の軽減を図り、専門知識の乏しい個人ユーザでも、必要最小限の対策を執ることで、安心してブロードバンド・インターネットを利用できる環境を整備していくことが期待される。

② ネットワークセキュリティの充実に向けた環境整備

国民誰もが安心・安全に参加できるネットワーク社会は、安全を提供する側のベンダーや通信事業者・ISP の努力だけでは達成不可能であり、安心を得る側のネットワーク利用者にも応分の努力が求められる。

このため、インターネットにおいても、ネットワーク利用者が負うべき責任を明確化するとともに、ネットワーク利用者が負うべき責任コストを適正化するための、ネットワークセキュリティに関する保険の充実に向け、利用者の意識啓発、ソフトベンダー・事業者の責任の在り方の見直し等による責任コストの適正化を推進する必要があると考えられる。

また、2.2 **で述べたように、我が国では携帯電話によるインターネット接続が広く普及し、無線** LAN **も各所に公衆アクセスポイントが設置されるなど普及が進んできている。このような状況を鑑みると、近い将来には、モバイルアクセスもまた重要インフラとなることが予想される。そこで、**PKI **のような高度なセキュリティ機能をモバイル端末に負荷をかけずに利用できるモバイルアクセス技術を開発するなどモバイルセキュリティの強化が必要であると考えられる。**

したがって、ネットワークセキュリティの充実に向けた環境整備のため、以下のような取り組みについて、今後の更なる議論・検討が必要であると考えられる。

- **利用者・ソフトベンダー・事業者の責任を明確化するための、情報システムの評価・監査・認定の基準について**
- **ネットワーク利用者が積極的にセキュリティ知識を身に付けようとする環境を整備する施策について（法整備等を含む）**
- **ネットワーク利用者のセキュリティ知識の評価・認定の在り方について**
- **モバイルセキュリティの強化について**