第１部

特集1 インターネット的なセキュリティーに対する考え方

江崎 浩

第１章　はじめに

2016年7月22日
(第1.1版)

以下の文章は、日本インターネット・ガバナンス会議(IGCJ, Internet Governance Conference Japan, www.igcj.jp) において、議論したセキュリティーに関する議論を契機に結成された執筆チームにより作成された文書である。

本文書は、インターネットの本質を理解して、これから我々が取り組むべき セキュリティー対策、特に、これからの IoT(Internet of Things)やビッグデータなど、これまで、インターネットのコミュニティーとの交流がそれほど多くなかったコミュニティーとの連携・交流を効率的・効果的に進めるために、必要となる共通言語(Common Language)ともいえる、レフェレンス・ドキュメントとして参照されることを期待して作成された。この文書を参考にしながら、各コミュニティーにおけるより具体的で詳細なセキュリティー対策が作成・実践されることを期待しているものである。

第２章　セキュリティに対する考え方 ～ 基本となる10の考え ― インターネットのセキュリティを考える際に必要なこと ～

2.1　はじめに

インターネットは、今や情報流通や商取引などに欠かせないものとなりました。さまざまなコミュニケーションや企業におけるビジネスにおいて、インターネットをいかに上手に利用するかを考えることは、いまや必須とも言えます。

しかしその一方で、管理している顧客情報の漏えいや、悪意のある第三者による詐欺なども社会的関心を集めつつあります。そのため、「セキュリティ」という概念がこれまで以上に重要になり、特に企業などの組織においては「十分なセキュリティ対策を取ることが当然」としてその対策が強く求められるようになりました。

セキュリティというと「難しいもの」というイメージを持ちがちですが、重要なのは「インターネットをいかに安心して使えるようにするか」ということを考え続けることです。この、「いかに良くしていくか」を考え続けることこそが、セキュリティの本質に近づく第一歩だということをまず念頭に置いてください。

また、セキュリティは「誰かが解決してくれるもの」ではなく、「関係するすべてのステークホルダー間による協調・協働」[*1]によって実現されるものであるということも念頭に置く必要があります。「まずは自助、次に共助、最後に公助」の考え方で、「共助」においては、機器・ソフトウェア提供者、サービス提供者、サービス利用者にまたがる垂直方向の関係者と、提供者間および利用者間での水平方向の関係者の両軸での協調・協働を実現することが重要です。

本ドキュメントは、インターネットを安心して使えるようにするための指針を皆さまが議論し策定するきっかけになることを目的として作成しました。インターネットに関係する皆さまが、自分のシステムの安心度(Trust)を

＊1　このような方向性は、ISOC(Internet Society)では「Collaborative Security」と呼ばれています。参考:「Internet Society のセキュリティに関する取り組み」(第8回IGCJ資料)http://igcj.jp/meetings/2015/0728/igcj8-4-fujisaki.pdf

向上させ、さらに自分のシステムに関係するシステムを運営する方々と協調・協働することで、皆さまが提供するサービスの品質が向上し、市場での競争力向上につながることになります。以降、順を追って「セキュリティを考える上で基本となる考え方」を紹介していきます。

2.2 本文書作成の背景と目的

インターネットがあまねく普及し重要性が増したことにより、インターネットセキュリティの確保は私たちの日々の生活を守るための大きな課題となっています。しかしながら、インターネットセキュリティの確保について以下のような状況が散見されるのも現実です。

- 多くの企業や組織において、セキュリティポリシーが厳しすぎイノベイティブな活動が阻害されている
- 多くの企業や組織において、単に「閉じていれば安全」だと考え、対策を怠っている場合が少なくない

これらは、インターネットへの接続性の提供を前提とした社会、そして内部者による情報窃取のリスクがある今日、とても危険な考え方となります。この傾向は、IoT(Internet of Things)のような、これからインターネットに新しく接続されることになる産業において顕著です。このような「引きこもり型の社会・組織」を脱却し、インターネットが引続き社会の持続的イノベーションに寄与することを願い、本文書ではセキュリティに対する基本的な考え方を示しています。たとえば、組織(例:企業内)での本文書の利用は、

- 基本的な考え方の共有のため、そのまま組織内に展開する
- 各組織に合わせて、肉付け、具体化し、ガイドラインとする

などを想定していますが、各組織の実情に合わせ、具体的に役立てていただきたいと考えています。

インターネットは、すでに我々の社会・産業活動の中に広く・深く浸透し、グローバルなデジタルエコノミー(Digital Economy)を形成しています。インターネットにおけるサイバーセキュリティに関する議論が盛んに行われある程度成熟してきたと考えられますが、インターネットが関与する領域は、人々の社会・産業活動のデジタル化とグローバル化の進展によって急拡大し、その結果、新しい課題も数多く顕在化してきています。そこで、本ドキュメントの目的は、「これまでのセキュリティの常識」を再点検し、今後のデジタルエコノミーにとって共通でグローバルな社会基盤における適切なセキュリティ対策に関する取り組みを検討・実装・運用するための参考・参照[*2]としていただくことにあります。

本ドキュメントの中の議論や整理のすべてが、すべての企業・組織・コミュニティに当てはまることは考えておらず、それぞれの 企業・組織・コミュニティにおいて当てはまる論点や方法論を見出すこと、あるいは、それぞれの企業・組織・コミュニティにおける論点や方法論の具体的な検討や議論、さらには新しい論点や方法論の発掘に参照・利用されることを期待しています。また、検討や議論の結果、それぞれの企業・組織・コミュニティに対して有用で有効なさまざまなドキュメントが生み出されることを期待しています。

■ 本文書の想定読者

全てのインターネットユーザー

■ 本文書の構成

まず、インターネットにおけるセキュリティについて説明し、以降でセキュリティを実現する上で基本となる10の考えを順に示します。

2.3 インターネットセキュリティーを考える際の基本

インターネットセキュリティを考える上では、インタ ーネットが持つ性質や特徴を維持し、情報の機密性と完全性と可用性を守り、社会の持続的なイノベーションと発展の継続に寄与することが重要です。

インターネットが持つ性質・特徴には、以下に示すも のが挙げられます。

＊2　IETF(Internet Engineering Task Force, http://www.ietf.org/)における、Informational RFC(Request For Comments) あるいは Internet-Draftのような位置付け。詳しくは次を参照してください。「IETFの構造とインターネット標準の標準化プロセス」https://www.ietf.org/proceedings/94/slides/slides-94-edu-localnew-3.pdf

・グローバルなネットワークであること
・選択肢が存 在し 、選択・利用可能であること
・チャレンジ（挑戦）が継続できること
・運用の継続に重点を置いた実践主義であること（動かし続けること）
・オープンでトランスペアレントなこと

また、情報の機密性と完全性と可用性は情報セキュリティの三要素とされ[*3]、企業や組織などの情報資産をさまざまな脅威から保護することを目的としています。

・機密性： 許可された者だけが情報にアクセスできるようにすること
・完全性：保有する情報が正確であり、完全である状態を保持すること
・可用性：許可された者が必要なときにいつでも情報にアクセスできるようにすること

そうしたことを満たしたセキュリティがあればこそ、誰もが自由に安心してインターネットにつなげる・つながることができるようになります。

2.4　基本となる10の考え

本文書では、以下で示す10の考えを基本として示します。

1. グローバルに考え、ローカルな施策を行う
2. 「原理主義」ではなく「実践主義」で進める
3. 強制する・制限するのではなく、活動の活力向上を応援する
4. 「過保護」は、かえってリスクを増大させる
5. 「やらされる」ではなく、「やりたくなる」を目指す
6. セキュリティ対策を、品質向上のための投資と捉える
7. 経験と知見の「共有」を行う
8. インシデントの経験者は、「被害者」として「保護・支援」する
9. 「匿名性」の堅持 と プライバシーの保護
10. まずは自助、次に共助、最後に公助

（1）グローバルに考え、ローカルな施策を行う

セキュリティ対策の中には、企業や個人に対して、法律や制度等により義務化されるものも存在します。それら制度は国ごとに異なり、国境を越えグローバルにデジタル情報の交換を行うコンピューターネットワーク（特にインターネット）では、異なる規則を持つ国にまたがったセキュリティ対策とシステムの最適化が行われなければなりません。セキュリティ対策もまた、グローバルな視点を持ちながら、各地域の制約を考慮してローカルな最適解を見いだす必要があります。

（2）「原理主義」ではなく「実践主義」で進める

インターネットは、常に稼働しながら、時々刻々変化するユーザーからの要求に応え、進化する技術から形成されるオープンシステムです。最初から（存在する前から）、詳細な技術仕様を決めることは不可能かつ非合理的であるため、おおまかな合意に基づいた実働可能なシステムからスタートすべきとの考え方で、インターネットにおける経験則（これをBCP：Best Current Practiceと呼ぶことがある）とされているものです。インターネットにおいては、意図的に最適化を行わず、ラフ・アーキテクチャだけを決めて動くものを尊重し、その動くものを状況に応じて適宜修正・変更していくようにしているのです。

この原則をセキュリティに置き換えると、インターネットセキュリティをプロセスとらえ、最初から100%の安全性を目指すのでなく、個人・組織・社会全体が常にセキュリティ対策を見直し続け、変わり続けることが重要と言えます。

（3）強制する・制限するのではなく、活動の活力向上を応援する

良くないセキュリティは、「我慢・忍耐・生産性減少」という方向に向かいます。それに対し、正しいセキュリティは、「のびのび、効率化、生産性向上」と「イノベーションの可能性」を提供することを目指します。

同じセキュリティ対策でも、ポジティブ思考で上手

＊3　詳細は、総務省の「情報セキュリティの概念」http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/02.htmlなどをご覧ください。

に利用すれば、成長戦略に変身することができます。具体的な手段(武器)は同じでも、「戦略」が違えば、異なる効果を産み出すことになります。

インターネットセキュリティは、イノベーションに必要な、非定型の活動を受け入れることができる環境を提供するようにデザイン・実装されなければいけません。その実現に際して、なにかを「強制(enforce)」したり、「制限(restrict)」したりすることは、可能な限り避けるべきです。活動の活力向上を応援(encourage)することが、何より重要です。

(4)「過保護」は、かえってリスクを増大させる

厳しすぎる規制は、その実現コストが高いばかりでなく、裏口やブラックマーケットの形成を助長し、環境の変化に対するリスクを高めてしまいます。したがって、インターネットセキュリティを実現するための規制は、適当な厳しさにして、システムに「あそび・ゆとり」を意図的に持たせるべきです。

すなわち、厳しすぎる規制は「安全である」という錯覚を生むだけ[*4]で、実際には、その環境で生活・活動する人を、環境の変化に対して弱体化させてしまうことになります。たとえば外部から完全に切り離された環境を提供されたオフィスではセキュリティの対策は不要という誤解を生み、従業員が自らを守る術を身につける機会さえも奪ってしまうでしょう。

怖いのは、危険が迫っていても自らを守る術を持つことなく無防備な状態が続くことです。そのようになることを避け、生き残る種であり続けるためには、「安全過ぎない」環境を意図的に作る必要があるという結論が導き出されることが大切です。これは、インターネットの一つの重要な特長である、「選択性の確保による多様性の確保」にも通じるものです。

(5)「やらされる」ではなく、「やりたくなる」を目指す

同じ技術でも、同じセキュリティ対策でも、ポジティブ思考で上手に利用すれば、成長戦略に変身することができます(項目3でも述べています)。

私たち人間は、「やらされる」状況では創意工夫の意欲が小さくなってしまいます。しかし、具体的な活動が「自身・自組織・社会」の価値や活動の質の向上に貢献する場合には、進んで知恵を絞ります。

単独では、あるいは正常な状況において利益を生み出すことは難しいけれども、非常時においても、あるいは新しい環境においても、私たちの活動を持続可能にするために必要なセキュリティ対策を実装する必要があります。

(6)セキュリティ対策を、品質向上のための投資と捉える

セキュリティ対策を、安心安全を確保するための品質の向上であると定義し、インターネットのインフラ、インターネット上で提供される様々なサービス、インターネットに接続されるすべての機器などの製品において、その品質を向上すべく、これらにかかわるすべての人たちが、それぞれの立場において「セキュリティQC活動」を実施することにより、安心安全なインターネット社会の構築ができます。

また、セキュリティを品質と捉えることができれば、製品が品質を超える障害によって損害が生じた場合の保険や保証制度を構築できます。また、品質が粗悪な物に対する何らかの法的な処置も可能になります。このような社会を構築するためには、すべての人々のセキュリティに対する考え方をしっかりと実践することが前提となります。

すなわち、企業・組織におけるセキュリティ対策の推進は、道徳や社会責任ではなく、それは、サービスの質を向上し、顧客やユーザーの情報を守り、自らのビジネスの拡大のための投資であると捉えるべきでしょう。

一方で、一般的に多くのユーザーは、そのサービス・システムが「たまたま」事故を起こしていないという

＊4　インターネットから切り離された工場で、ソフトウェアのメンテナンスの際に紛れ込んだコンピューターウィルスによって工場全体の操業が停止したといった事例もあります。

場合でも、価格の安い、セキュリティ対策が十分に実施されていなかもしれないサービス・システムを利用することが考えられます。しかし、適切なセキュリティ対策は、サービスのコストアップではなく、システムの効率化に貢献する場合が少なくないことを共有すべきでしょう。インシデント発生の要因を取り除くことで、システムの無駄が排除され、効率が向上する事例は数多く報告されています。また、「たまたま起こるかもしれない事故」のコストと、それに対処するコストを比較して、対処するコストが小さくなるように工夫することが企業競争力となり、市場での競争力向上につながることになるでしょう。どの程度の工夫を行うか、どのような工夫を行うのかは、各事業者の自律的な判断となりますが、対策を行わなかったときには、その社会的責任とユーザーに対する責任が発生することになります。

（7）経験と知見の「共有」を行う

インシデントの経験や知見は、外部の人や組織と共有すべきです。共有することにより、そのインシデントについてインターネットセキュリティ専門家を含む、より多くの人や組織に検討の機会が与えられるからです。同様の手口による被害を防ぐチャンスが与えられることは、非常に重要です。

「勇気を出して声をあげる」ことが、社会全体のセキュリティ対策に貢献すると考え、そのような勇気ある経験と知見の共有を評価すべきです。

（8）インシデントの経験者は、「被害者」として「保護・支援」する

前項に関連して、インシデント被害者が経験と知識の共有をためらう理由の一つは、当事者に対して責任の所在や対策の不備を厳しく追及する世論にあります。

攻撃者の手口は日々変化しており、十分と思われる対策をとっていても被害に遭う可能性はゼロではありません。私たちは、インシデント被害者が意図的に対策を怠っていたというようなケースを除いて[*5]、彼らを「保護・支援」するべきであり、また彼らが第三者と経験を共有する行為を賞賛すべきです。

被害者を責めることには意味がありません。責めることで被害者のセキュリティ対策をするインセンティブが失われ、経験と知見が隠されてしまうことのほうが問題です。航空機の事故調査（次の事故を防ぐための調査や情報公開が重視され、そのために真実を明らかにする。悪者を探し、追求するためのものではない）に倣い、被害者を「保護・支援」し、再発を防ぐための調査にこそ力を注ぐべきですし、より多くの情報が調査のために利用可能にする状況を作り出すべきです。

（9）「匿名性」の堅持 と プライバシーの保護

日本国憲法に定められる「通信の秘密」は、インターネットにたずさわる全ての人によって最大限尊重されるべきです。保護されるべき秘密には、通信の内容と通信者の特定の2つがあります。これらの情報を保護するための暗号化技術等については積極的に取り入れていくべきです。

「セキュリティ」の実現には、ユーザーの認証が必要と考えるのが一般的です。しかし、広義のセキュリティの観点からは、ユーザーを認識しない「匿名性」が必要かつ重要な役割を持つことになります。たとえば、通信事業者では、仮に、ユーザー通信の中身が見えても、その内容を利用することが厳密に禁止されています。その内容がテロや犯罪などの内容であっても、秘匿性を守ることが義務であるとされているのです。匿名性は、組織運営においても、不適切な行為等に対する告発が不可能にならないようにするために必須なものだと考えられます。「目安箱」などは、その一つの実装方法です。告発によって、告発者が、組織や組織を構成する人から報復や復讐を受けないことが保証されなければ、告発者は告発することを取りやめるのが普通ですから、そのようなことが起こらないように「匿名性」が必要となります。

＊5　インシデント被害者が意図的に対策を怠っていた場合には、相応の罰則がなんらかの形で発生することになるでしょう。

このような通信者と通信内容に関する秘匿性の実現は、個人情報の保護を含むプライバシーの保護という観点からも必要となります。プライバシーの保護のためにインターネット全体の利便性が損なわれるなどの事態も想定される今日では、その時代に即したプライバシーの保護のありかたについて議論を継続していくことがなによりも大切です。

（１０）まずは自助、次に共助、最後に公助

自然災害対応のような非常時の対応と同様に、インターネットセキュリティ対策にも「自助・共助・公助」の考え方が根付くべきです。自助とは、インターネットユーザー一人一人が自らの安全を守ること、備えること。共助とは、地域や業種業態ごとに助け合って安全を守ること、備えること。最後の公助とは、政府や公的機関がそれらを支援し、公共サービスの一環として安全を守ること、備えることです。

当然のことながら、ユーザー一人一人の知識や時間には限りがあり、自助だけではセキュリティ対策は立ちゆきません。そのような際に、自助でまかなえない部分を共助で補完することが求められます。そして、共助をもってしてもなお、足りない部分を埋めるのが公助なのです。

フィルタリング（危険なWebサイトへのアクセス制限）を例にとれば、これを実施する責任はユーザーにあるべきです（自助）。しかし、どのサイトが危険（たとえば、ウイルスなどをまき散らす）かを個人が把握することは困難ですから、ユーザーがこのフィルタリングを信頼可能な第三者に委任・委託すること、つまり共助や公助を頼むことは、ユーザーの責任の範囲で不可能ではありません。

2.5　結び

インターネットは、急激にその適用領域と利用法が拡大し、地球上のすべての情報流通や商取引などに必要不可欠なものとなったとともに、さらに、それらが持続的に発展するために必須なものとなりました。インターネットを前提にしたグローバルなデジタルエコノミーの進展とともに、安心・安全を実現する「セキュリティ」に関する考え方も大きく変化してきています。 たとえば、セキュリティレベルを高め、それを維持することが目的化する傾向にある組織・企業も少なくなく、組織・企業の効率化や新しい取り組みを阻害してしまうような場合も少なからず存在しています。一度、「何のためのセキュリティなのか？」を問い直し、セキュリティを「組織・企業における品質向上の投資」として捉え、安心して、組織・企業の持続的成長に貢献する新しい技術や仕組みの導入に挑戦することを可能にしなければならないと考えています。

インターネットでは、常に、グローバルに考えた、実践的でトランスペアレントな施策がローカル（それぞれの組織・企業・コミュニティ）に自律的に、しかし、グローバルと連携・協調・協働しながら展開する必要があります。セキュリティ対策は、「まずは自助、次に共助、最後に公助」の原則のもと、結果的にリスクを増大させることになる「過保護」な施策を「勇気をもって」避け、「経験や知見の共有」を実現するに資する「匿名性の堅持」と「プライバシーの保護」が実現されながら、すべての関係者（ステークホルダ）の間で連携・協調・協働しながら、すべての関係者の活動の活力を応援・支援し、向上するに資する挑戦を安心して実行することに貢献するセキュリティ施策が確立・実践されなければならないと考えます。このような、インターネットを前提にしたグローバルなデジタルエコノミー社会に貢献するセキュリティ施策の確立と実践するための検討・議論に対して、本ドキュメントが貢献できることを期待しています。

2.6　著者について Authors

本文書は、日本インターネットガバナンス会議(IGCJ)の3回の物理的な会合とオンラインでの議論内容を有志がまとめたものです。

本文書取りまとめに関わった有志（あいうえお順）

赤嶋 映子 Eiko Akashima
浅岡 浩人 Hiroto Asaoka
荒浪 一城 Kazuki Aranami
伊賀野 康生 Yasuo Igano
江崎 浩 Hiroshi Esaki

大崎 竜也 Tatsuya Osaki
川崎 基夫 Moto Kawasaki
小宮山 功一朗 Koichiro Komiyama
高松 百合 Yuri Takamatsu
中村 修 Osamu Nakamura
根津 智子 Tomoko Nezu
藤崎 智宏 Tomohiro Fujisaki
堀田 博文 Hirofumi Hotta
本間 誠治 Seiji Homma
前村 昌紀 Akinori Maemura
南 弘征 Hiroyuki Minami
山崎 信 Shin Yamasaki
横澤 誠 Makoto Yokozawa
渡辺 俊雄 Toshio Watanabe

2.7 権利および許可Rights and Permissions

上記ライセンスの元で、以下の条件に従う限り、商用目的を含み自由に複製、配布、送信、および改変が可能です。

第３章 Concept for security

~ What is needed when considering the security of the Internet ~

August 1, 2016

1st Edition

3.1 Introduction

The Internet is now critical, indispensable and basic global platform to distribute and share any digital information for all social and private activities. In business operation and in a variety of communication in business, the consideration and implementation of the best use of the Internet is critical and fatal for any single company to continue and to growth in their business.

On the other hand, leakage of customer information, management of company's business information, management of privacy information or fraud by malicious third party attacks is getting of large social interest. Therefore, the recognition of the importance of appropriate design and its implementation of security measures in every single organization has been increased. This is especially important and critical for the organization such as a private company and the sufficient security implementation is their mandatory corporate governance and management.

Security is likely to have the image of "a difficult one", but the most important point and action for the security implementation is to keep thinking "how effectively we use the Internet infrastructure, safely". Keep thinking in our/your mind about "how to implement safer environment" is the important action in order to approach to the essence of "Internet" security and to implement it.

We must remember and realize that security problem is not resolved by someone, security problem is resolved by the cooperation and collaboration among all the related stakeholders[*6]. Also, "self-help is the first, mutual assistance is the second, and public assistance is the last" is most important concept and practice for us. As for "mutual assistance", the practical implementation of the vertical collaboration and cooperation among equipment and software vendors, service providers and users and the horizontal collaboration and cooperation among vendors, providers and users is important.

The purpose of this document is stimulating and encouraging the discussion about the guideline to use the Internet safely by anyone. We believe that when all the stakeholders related to the Internet improve the quality of security and trust of their own system and collaborate/cooperate with all the operators related

＊6 This is called as "Collaborative Security" defined by ISOC (Internet Society): http://www.internetsociety.org/collaborativesecurity

with their system, the quality of service and trust provided by “you” is improved and it leads to the improvement of “your” market competitiveness. In the following sections, we discuss “idea of the underlying concepts in considering the Internet security”, step-by-step.

3.2 Background and object of this document

Since the Internet is universally popular and deployed, ensuring the Internet security has become a major and critical issue in order to protect the day-to-day of our lives. However, the followings are the reality of and frequent implementation of practical situation in many companies and organizations.

- Too rigid and strict security policy is applied to and implemented, then the activities of people is sadly inhibited
- Simply think that "disconnecting from the Internet provides safety", and neglecting mandatory measures of security

These approaches are very dangerous idea in today and in future, for the society which is premising on the provision of connectivity to the Internet and for the organizations which has a risk of information theft by insiders. This trend seems to be frequent and be typical in the industries, which start to use and start to be connected to the Internet significantly, such as the IoT (Internet of Things).

We have to improve “withdrawal type of society and organizations”, and hope that the Internet will continue to contribute to the sustainable innovation of society. In this document, we show the basic idea for the Internet security, and we would like to support your practical implementation. We may think the followings would be examples how to use this document by some organization.

- Distribute the document to organization members, so as to share the basic idea and direction for the improvement of security
- Deliver a guideline, which is adequate to your organization, with detailed and concrete description focusing in your organization, after the consideration and modification on this document

The Internet has been widely adopted and used in our social and industrial activities, and has created “global digital economy”. There has been a lot of cyber security discussion and has been delivered some guidelines. However, since the region and area where the Internet technology is adopted and used is significantly expanded by the accelerated digitization and globalization of our social and industrial infrastructure, a lot of new security issues come out in front of us.

The object of this document is stimulating and encouraging the discussion about the adequate common security guideline to preserve the design, the implementation and the operation of our future global social platform, as a referenced and discussion document. We do not think all the discussion or contexts described in this document are fit with your organization or with your community. Using this document, we hope you may find the contexts, which fit with your organization/community, or you may initiate concrete and detailed discussion and contexts for your organization/community, or may deliver new discussion item(s) and idea(s). Also, we hope, after the discussion triggered by this document, some documents, which is useful and valuable for each organization or each community, would be delivered.

■ Assumed reader of this document

All of Internet user

■ Structure of following sections

In this document, at first, we describe the essence of security in the Internet. Then, we show it by the 10 of key points to be referred to, when you design and implement appropriate security measures in your organization.

3.3 Basic when you consider the Internet security

In considering the Internet security, the followings are important; to maintain the nature and characteristics of the Internet, to protect the confidentiality, integrity and availability of information, and to contribute to the sustainable and

continuous innovations and development of the society.

The nature and characteristics of the Internet is listed, below:

- It is global and unique network on the earth
- There is alternatives and there are possible to be selected and be used
- Opportunity of challenges is preserved and encouraged
- Sustainable operation is mandatory and respected
- Everything, such as technology or operation, is transparent and open

The confidentiality, the integrity and the availability of the information are of the three major requirements for information security [*7], and is intended to protect the information assets, such as companies and organizations from a variety of threats.

- Confidentiality: to be able to access to the information by only authorized persons
- Integrity: information held is accurate, keeping the state is complete
- Availability: to be able to access the information at any time when the authorized person is required

When there is a security implementation that meets the above requirements, everyone will be able to connect any device to the Internet with confidence.

3.4 The 10 basic key idea

In this document, we show the following 10 basic key ideas for the Internet security:

1. Thinking globally, implementing local measures
2. Respecting "practice principle", than "fundamentalism"
3. Instead of restriction or enforcement , supporting the improvement activities
4. "Overprotection" causes rather the increase of risk
5. Instead of "to be enforced by someone" , aiming "want to do"
6. Security measures is the investment to quality improvement {and future}
7. Sharing of experience and knowledge of everyone
8. Protecting and supporting the person, who experiences cyber security incident, as a "victim" rather than "bad guy"
9. Preservation of "anonymity" and protection of "privacy"
10. Firstly self-help, next mutual assistance, finally public assistance

(1) Thinking globally, implementing local measures

Some of the security measures, to companies and individuals, are mandated by law, regulation or institutions defined by governments. The rules defined by government or delivered from culture are not the same, but can be different for each country. The computer networks of many organizations exchange the digital information across the national border over the globe by using the Internet or their private networks, and they must implement optimized security measures and systems across the country, where different rules are carried out. This means that the security measures must be designed and implemented, while having a global perspective and taking into account the constraints of each local region, with locally optimized solution.

(2)Respecting "practice principle", than "fundamentalism"

The Internet, while always running, in response to a request from a user that changes from moment to moment, is an open system that is formed by the continuously evolving/innovating technology. From the beginning (even before the present), it is realized that the determination or the definition of the detailed and whole of technical specifications is impossible and irrational. This is the idea of the Internet, i.e., we should start from the implementable system based on rough consensus; rule of thumb in the Internet (This is called as BCP, Best Current Practice). In the Internet, with the intentional non-optimization, respecting the actually running system in the field with rough consensus architecture, we must continue the modifications, changes and innovations.

---

*7 For more information, refer to as "the concept of information security" by the Ministry of Internal Affairs and Communications (In Japanese): http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/02.html

So as to understand this principle in the field of cyber security, we may suggest to capture this (Internet Security) as a process. It is not good idea aiming 100% of safety from the beginning. Individuals, organizations and society should constantly reviewing their security measures, and it can be said that it is important to realize the continuous change of the IT system and of the Internet.

(3) Instead of restriction or enforcement, supporting the improvement activities

Not good security will head in the direction of "patience, perseverance and productivity decrease". In contrast, the correct or good security head in the direction of "carefree, efficiency, productivity improvement" and provided "the possibility of innovation."

Even in the same security measures, if well utilized in positive thinking, it can be transformed into a growth strategy. Specific means (weapons) is also the same, different "strategy", it will spawn a different effect.

Internet security is required "for innovation", it must be designed and implemented to provide an environment that can accept atypical activity. In its implementation, "enforcing" or "restricting" something should be avoided as much as possible. It is the most important thing to cheer and to encourage the vitality improvement of activity.

(4) "Overprotection" causes rather the increase of risk

Too strict regulations lead to not only its high implementation cost, but also may conduct the formation of the back door(s) and the black market, and also will increase the risk against the change of environment. Thus, the regulation of appropriate security should be appropriate severity and should intentionally have a kind of "play-room" in the system.

In other words, too strict regulations will provide a "too safe" environment to the people who live and the activities in this inappropriate environment [*8]. Then, it leads to end up of undermining respect to a change of the environment. For example, in an office which is of completely isolated environment from the outside, people may have misconception that security measures is unnecessary, and it will take away the opportunity to learn how to protect themselves from the employees. Therefore, in order that we are surviving species, the following conclusion is derived, i.e., there is a need to create a "not too safe" environment, intentionally. This is one of the important features of the Internet, i.e., "ensuring and preservation of diversity by ensuring the alternatives and selectivity".

The real risk is that, even the vulnerable status continues, the status without having a way to defend them even with the imminent danger continues.

(5) Instead of "to be enforced by someone", aiming "want to do"

Even with the same technology or even with the same security measures, it can be transformed into a growth strategy (as we mentioned in item 2), if well utilized it with the positive thinking.

The achievement by us (i.e., human-beings) with enforced activities will be in general small. However, in the case where their specific activities will contribute to the improvement of the value and activities of the quality of their organization, community or society, their activities goes to of autonomous and enthusiastic.

Even though it is difficult to generate profits in normal circumstances, we need to implement the necessary security measures in order to make sustainable our activities even in an emergency or even in a new environment.

---

*8 In a factory, which is isolated from the Internet, the whole of the operation in the factory had been halt / suspended, due to a computer virus during the scheduled software maintenance procedure in the factory.

(6) Security measures is the investment to quality improvement {and future}

Security measures should be defined as the collaborative improvement of the quality to ensure safety and security, by all the stakeholder of the Internet. By carrying out any kind of “security QC activities” in their respective positions, such as the Internet infrastructure, various services offered on the Internet, or the products and devices connected to the Internet and by the collaborative involvement of all people involved in the Internet business/operation, the improvement of quality of the Internet is achieved and can build a safe and secure Internet.

In addition, if it is possible to consider the security and quality by us, you and we can build the insurance and compensation system even in the case of damage caused by the failure of the product, which is beyond its capability. Some legal treatment could be applied to against the services or products with poor quality. In order to build such a society, the establishment of practice and concept for the security with the collaborative security concept for all the people must be premised.

In other words, the promotion of security measures in the companies and organizations is not by moral and by social responsibility, but it should be achieved by the incentive of the improvement of the quality of services. And, it should be regarded as the important investment for the expansion and of their current and future business.

(7) Sharing of experience and knowledge of everyone

Experience and knowledge of the incidents should be shared with the outside of people and in its organization. By sharing those information, we can generate the opportunities among all stakeholders, including the Internet security experts, to share the latest security incidents. It is very important to provide and to share a chance, so as to prevent and mitigate the damage caused by the similar or the same security incident.

In other words, we want encourage to all of you “to raise your voice to share your experiences”, since it shall contribute to the society so as to improve our security measures against the security risk. Yes, we must respect and encourage the braveness of people who put their unhappy experience to be shared in the public domain.

(8) Protecting and supporting the person, who experiences cyber security incident, as a “victim” rather than “bad guy”

One of the reasons, why the incident victims may want to hesitate to share their experience and knowledge, would be because that the public opinion tends to chase or criticize their responsibility or their potentially inappropriate counter measure against the incident(s).

Arts and behavior of the attackers in cyber space are changing every day. Therefore, it is almost impossible to achieve a zero possibility, in general, even when the victim may take the possible security measures that are likely to be sufficient. We are, with the exception of the cases, such as that incident of the victim had intentionally failed to sufficient security measures, should them to “protect and support”, also respects them is the act of sharing a third party and experience you should.

There is no sense to blame them, since they are the victim. Rather, the degradation of their incentive to share and to implement their security measure is a loss and a risk of our society. As we widely shared, in case of the accident investigation of aircraft, it is well recognized and is well performed the disclosure and the sharing of any information to prevent next/future accidents. We should pour our force and power so as to prevent a recurrence by them, rather than punish them.

(9) Preservation of "anonymity” and protection of “privacy”

In many basic disciplines such as constitution, in many countries, the protection of “privacy/secrecy of communication/correspondence” and “freedom of expression” is defined as basic right and thing we must preserve. The information, that we must protect, is contents of communication and identification of communicator. In order to protect these information, we should aggressively

adopt available new technologies, such as encryption technologies, and rules.

It is commonly recognized that we need user authentication for cyber security. However, from the point of view of a broad sense of security, “anonymity”, which does not recognize a user, is necessary and play an important role. Then, as an example, for telecom operators, even if the contents of the user communication are visible, making use of its contents is strictly prohibited. Even the contents are related with terrorism and crime, the protection of the confidentiality for these communications must be mandatory.

Even in an organizational management, anonymity is considered as something essential so as to ensure that the accused does not become impossible for inappropriate conduct and for other incidents. How to implement and operate "suggestion box" or “opinion box” is one of examples. We must avoid the case where the accused person is subject to retaliation and revenge by accusation. In other words, we must guarantee the accused person is not subject to retaliation and revenge from the people that make up the organization or from the organization the accused person belongs. In order to guarantee the above operation, we need “anonymity”.

The protection of contents in communication and identification of communicator is mandatory from the view point of the protection of privacy, including the protection of individual information. Since the protection of privacy may lead to the inconvenience to use the Internet by every single individual or by organization, we have to have sustainable and continuous discussion and rule adaption, which appropriate to corresponding circumstance.

(10) Firstly self-help, next mutual assistance, finally public assistance

As well as natural disaster response, the idea of “self-help, mutual assistance, and public assistance” should be well recognized in the Internet security measures. The self-help is that each person, using the Internet, protects their own safety by himself/herself. Mutual assistance and is that protecting the safety by mutual help by every person in each region and in each business segments. Lastly, the public assistance is that the government or public institutions protect the safety of every citizen as a part of the public service.

As a matter of course, there is a limit to the user each person’s knowledge and time, only by the self-help security measures does not work well. The mutual assistance is necessary and needed to supplement the part of security that cannot be covered by self-help. And, even with the mutual assistance, we need a public assistant to fill the missing parts.

Taking the filtering (to restrict the access to harmful Web site) as an example, the responsibility to implement this should belong to the end user. However, a user can delegate the operation of content filtering to the trusted third party, that can be a kind of mutual assistance (and public assistance), by the user's responsibility.

This is exactly one of the basic principles of the Internet. This is the concept of “end-to-end”, leading to the transparent infrastructure, that end node can deliver advanced features without some inappropriate enforcement or restriction by organization or by government.

3.5 Summary

The Internet is now critical, indispensable and basic global platform for global digital economy and distribution and share of digital information for all social and private activities on the Earth. And, the Internet is recognized as the critical and mandatory resource to achieve our sustainable growth. According to the aggressive development of global digital economy premising the existence of the Internet, the framework and guideline of cyber security to achieve the safe use and operation of the Internet seems to be changing, significantly. For example, in some organizations, since they blindly adopt higher restricted rules to reach to higher security level and maintain this direction, the efficiency of organization

is going to be degraded or new challenges are discouraged or inhibited. We may think we should re-consider “what is the purpose of security?”, so that security acts should enable the introduction of new challenges, on technologies or on organization structures and operation, which contribute to the sustainable growth of organization, while considering “Security measures is the investment to quality improvement {and future}”.

In the Internet, the practical and transparent measures for local operation, while considering the global perspective and collaborating/cooperating with global system, shall be autonomously adopted in each organization or in each community. As for security measures, while premising “Firstly self-help, next mutual assistance, finally public assistance”, we think that the security measures, that aims the support and encouragement of the challenges for the growth and improvement of their activities, should be established and applied with the coordination/collaboration/cooperation by all the related stakeholders, while avoiding “overprotection” result to the increase of security risk and the “preservation of anonymity” and “protection of privacy” to achieve sharing of experience and knowledge.

We hope that this document contributes to the stimulation or encouragement of the discussion, which leads to the establishment of appropriate guideline and the implementation of security measures for the future global digital economy and society premising the existence of the Internet.

3.6 Authors

This document was developed by volunteer participants of Internet Governance Conference Japan (IGCJ) in the three face-to-face meetings and in the online discussions.

Participants (in alphabetical order):

Eiko Akashima
Kazuki Aranami
Hiroto Asaoka
Hiroshi Esaki
Tomohiro Fujisaki
Seiji Homma
Hirofumi Hotta
Yasuo Igano
Moto Kawasaki
Koichiro Komiyama
Akinori Maemura
Hiroyuki Minami
Osamu Nakamura
Tomoko Nezu
Tatsuya Osaki
Yuri Takamatsu
Toshio Watanabe
Shin Yamasaki
Makoto Yokozawa

3.7 Disclaimer

This document is a translation from the Japanese version of the document: セキュリティに対する考え方 (http://igcj.jp/meetings/concept-for-security.pdf). The translation is for informational purposes only, and is not a substitute for the original document. If a discrepancy is found between original and this translated document, the original document always supersedes.

3.8 Rights and Permissions