2016 年 5 月 ~~17~~xx 日
（第 1 版ドラフト~~版~~）

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 ～

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、「関係者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「共助」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分かりやすくまとめることを主眼として作成いたしました。インターネットに関係するみなさんが、自分のシステムの安心度 [2]を向上させ、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、みなさん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

[1] Collaborative Security by All Stakeholders
[2] Trust

紹介していきます。

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、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。

- ü 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
- ü 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、具体的実際に役立てていただきたいと考えています。

■ 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実現する上で基本となる 10 の考えを順に示します。

3. インターネットセキュリティを考える際の基本

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、情報の機密性と可用性と整合性を守り、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。

- ü グローバルなネットワークであること
- ü 選択肢が存在し、選択・利用可能であること
- ü チャレンジ(挑戦)が継続できること
- ü 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)
- ü 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と整合性とは情報セキュリティの三大要件要素とされ[3]で、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。

- ü 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
- ü 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
- ü 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。

[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。

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。

~~また、厳しすぎる規制は、「安全過ぎる」環境を提供することになり、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分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を奪ってしまいます。したがって、私たちは生き残る種であり続けるために、「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になります。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。~~

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

コメントの追加 [y1]: 直後の 2 つの段落と重複するため、削除を提案します。元々は、2016 年 2 月 22 日 11:57 sec-doc ML 投稿にて、分かりにくいので直後 2 段落で本段落の置き換えを提案されていました。以下公開版でも同じ指摘がコメントとなっています：http://igcj.jp/meetings/2016/0414/approach-for-security-draft.pdf

[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。

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 2 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~~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場合でも、価格の安い~~セキュリティー~~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~~れ~~られます。しかし、適切な~~セキュリティー~~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時には、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

[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。

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。例えば、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。

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（有害 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。しかし、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。