

2015年10月7日

(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。

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。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. 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。

- ✓ 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

コメントの追加 [t1]: 全体的に内容が固いので、読者に対する導入をするための文章を追加しました。

コメントの追加 [t2]: オリジナルでは先に「インターネットセキュリティとは何か」来ていますが、話の流れを考慮してこちらを先に持ってきました。

コメントの追加 [t3]: 箇条書きは、こちらで整理してみました。

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、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。

- ✓ 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
- ✓ 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、情報の機密性と可用性と整合性とは情報セキュリティの三大要件¹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。

- ✓ 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

¹ 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。

コメントの追加 [t4]: オリジナルにはありませんが、基本となる 10 の考えの最初に「グローバルに考え、ローカルな施策を行う」があるので追加しました。

コメントの追加 [t5]: これはオペレーションなので性質とも特徴とも言い難く、違う言葉で置き換えたいです。

コメントの追加 [t6]: 説明が必要だと思いますので、加筆しました。

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。

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	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
3	「過保護」は、かえってリスクを増大させる
4	「やらされる」ではなく、「やりたくなる」を目指す
5	経験と知見の「共有」を行う
6	インシデントの経験者は、「被害者」として「保護・支援」する
7	「原理主義」ではなく「実践主義」で進める
8	「匿名性」の堅持
9	まずは自助、次に共助、最後に公助
10	セキュリティ対策を、品質向上のための投資と捉える

コメントの追加 [t7]: 「匿名性」については、反対意見があります。

(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) 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、異なる効果を生み出すこととなります。

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。

(3) 「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となります。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となります。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²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となります。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。

(4) 「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

² 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イ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。

コメントの追加 [t8]: この段落は分かりにくいと感じますので、続く 2 段落で書き直しの案を出してみました。

コメントの追加 [t9]: この書き方は、誤解を招きそうです。

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。

(5) 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。

(6) 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、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。

(7) 「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はなく、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。

(8) 「匿名性」の堅持

「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となります。日本国憲法では、「通信の秘匿性」が定義されており、通信事業者は、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は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。

対案 8. 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。具体的には、通信内容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。

一方で、通信の秘密を守る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。

(9) まずは自助、次に共助、最後に公助

自然災害対応と同様に、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

コメントの追加 [t10]: 「匿名性」については、江崎さんが残すという意見を述べています。

江崎の意見としては、「匿名性」は、残した方がよいと思います。「プライバシーの保護」では、弱い気がしますが、

「匿名性の堅持」は、「プライバシーの保護」の一部分であるという立場で書くのはどうかと思います。

コメントの追加 [t11]: 小宮山さんから出ている「匿名性」に関する代替案です。

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。

これはまさに、インターネットの基本原理の一つである「エンド・ツー・エンド」の考え方であり、トランスペアレントなインフラを提供し、高度な機能、エンドノードが実現する。

コメントの追加 [t12]: 江崎さん自身が「冗長かも」と述べていますが、編集者の立場から見ても蛇足だと思います...

(10) 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。

企業・組織におけるセキュリティ対策推進は、道徳や社会責任ではありません。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、自らのビジネスを拡大するための先行投資となります。