IGCJ 8
2015年7月28日

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

IGCJをプラットフォームとした セキュリティドキュメントについて

セキュリティドキュメント
ドラフティングチーム
江崎浩

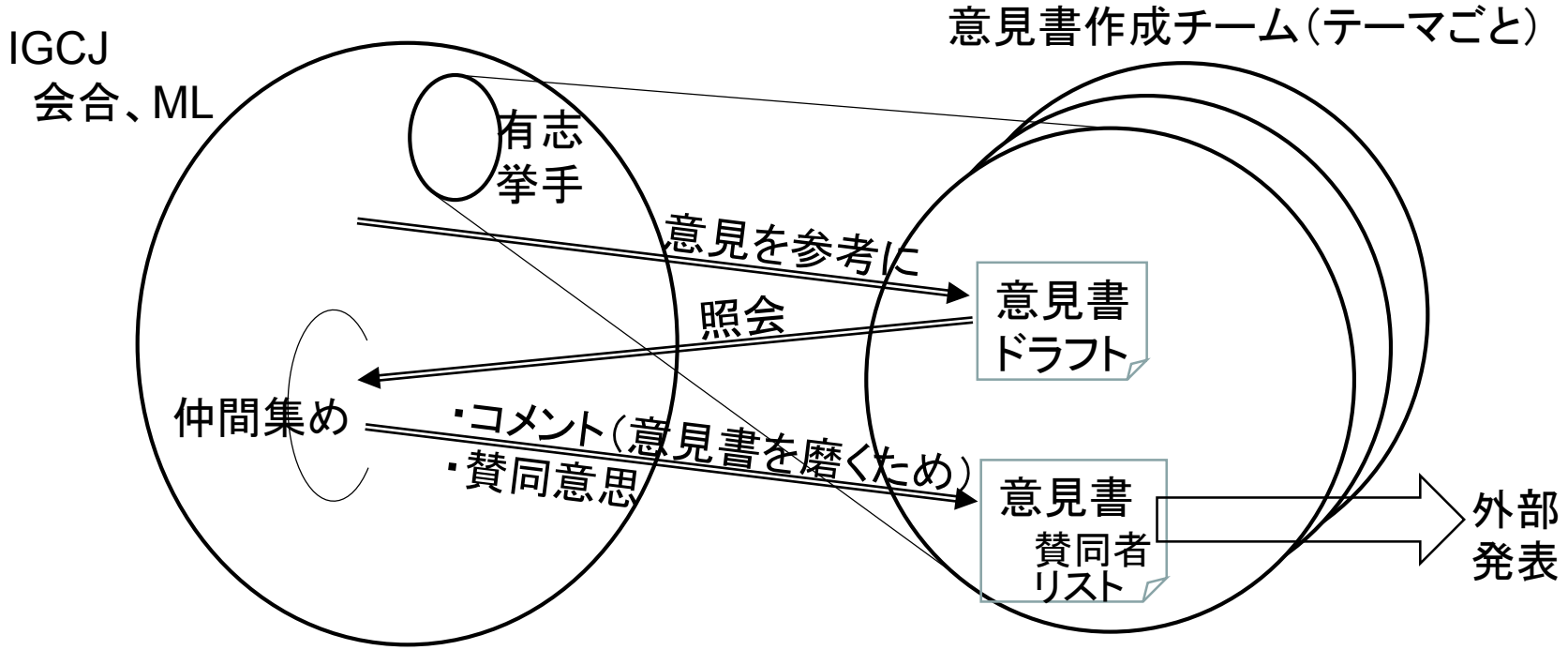
おさらい(前回のIGCJ7 の資料から):

IGCJを場として使った意見集約案

- IGCJとしての意見集約は困難という背景

⇩

- 日本からの意見発信を行うとき、IGCJをプラットフォームとして使う方法の案「賛同者募集モデル」



セキュリティドキュメントチーム/ 文書の目的とターゲット

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

- 目的とターゲット
  - (主に技術コミュニティが)思い描いてはいたが形として表現できていなかった、インターネットの特性・性質や考え方・心に基づいた「インターネットに関するセキュリティとその考え方」を端的な文書にまとめた上でそれを広めることで、『今後のインターネット』におけるセキュリティを考える上での共通理解を形成したい。
  - この文書は「基本の考え方」として、マルチステークホルダー間の議論におけるコア(Root Document)として機能させたい。「基本の考え方」であるため、「誰向け」ということはない
  - この考え方を基に、ここから先、これをもとした派生文書(対象者別、事例集等)ができていくことを目指している。

この文書に含まれるべき内容(案)

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

①インターネットセキュリティとは何か
②この「考え方」文書作成の理由／背景
③セキュリティに対する考え方(基本となる10の考え)

①インターネット・セキュリティとは何か

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

- インターネットが持つ性質や特徴を維持することで、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もの
- インターネットが持つ性質・特徴とは、
  - 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
- こうした前提があればこそ、皆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

②この文書作成の背景・理由

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

- 現在、以下のような件が散見される、「引きこもり型の社会・組織」である。こうした状況を良い方向に導きたい
  - 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。こうした状況の放置は、インターネットへの接続性の提供を前提としたインターネット社会では、とても危ない状況である
    * これからインターネットに接続されることになる産業において、特にこの傾向は顕著。
  - 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て、イノベイティブな活動が阻害されている

③セキュリティに対する考え方 (基本となる10の考え方)(案)

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

1. インターネットはグローバルなインフラである
2. 強制する(enforce)・制限する (restrict)のではなく、活動の活力向上を応援(encourage)する
3. 「過保護」は、かえって危険度を増大させる
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を、「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. 「実施権」は個人にある、ただし第三者への委任は可能
10. セキュリティ(投資)を、品質(向上)と 捉える

1.「インターネットはグローバルなインフラである」とは

- セキュリティ対策の中には、企業や個人に対し、法律等により義務化されるものも存在するが、法律は、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らない
- たとえば、情報通信システムにおけるデータの暗号化に必要な暗号ソフトウェアの輸出入は、国家安全保障に関わるものとして、国ごとに異なる管理基準を持っていることが多い。すなわち、各国ごとに、仮定可能なセキュリティレベルや施策は、必ずしも同一とすることが不可能な機能・システムが存在する場合がある

2.「強制する(enforce)・制限する (restrict)のではなく、活動の活力向上を応援(encourage)する」とは

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

- 好ましくないセキュリティは、「我慢・忍耐・生産性減少」という方向に向かうが、しかし、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すもの
- 具体的なツール(武器)は同じでも、「戦略」が違えば、異なる効果を産み出すように、「同じ技術」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る
- 「セキュリティは利益を生まない」という意見があるが、経済性だけでとらえられない
- 「セキュアな環境」が、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・実装されなければならず、この「セキュアな環境」の実現に際して、何かを「強制(enforce)」したり、「制限(restrict)」することは、可能な限り避けるべき
- 厳しすぎる規制は、その実現コストが高いばかりではなく、ブラックマーケットを形成するとともに、環境の変化に対する脆弱性の増加を発生させる可能性を持つ。したがって、安心・安全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

3.「『過保護』は、かえって危険度を増大させる」とは

- 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。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なり、人々をスポイルする。その結果、彼らが外界に出ると、彼らはインシデントに適切に対応することができず、生き残ることができなくなる
- (誤解を恐れずに言えば)生き残る種であり続けるためには、「厳しすぎない規制」による「安全過ぎない」環境を、我々は、意図的に作る必要がある。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」に通じるもの

4.「『やらされる』ではなく、『やりたくなる』を目指す」とは

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

- 「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る
- 「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う。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、進んで創意工夫の知恵を絞り、その実装・実行に貢献する。それによって、さらに、「具体的な行動」を行う インセンティブが増加することになる
- 単独では、あるいは正常な状況においては利益を生み出すことが難しいけれども、非常時においても、あるいは新しい環境においても、我々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る

5.「経験と知見の『共有』を行う」とは

- インシデントが発生したこととその対応策や結果を外部の人や組織と共有することは、インシデントに対する対応策を迅速化・可能化するとともに、その対処方法を多数の人・組織で、そして、解決すべき課題がセキュリティ分野の専門家によって検討されることを可能にする
- 「失敗の経験」や「対処法」の共有は、インシデント自体の削減とインシデント発生時の被害の低減に貢献する
- インシデントの発生とその対処、そしてその結果の共有(＝「透明化」)、すなわち、「勇気を出して引き籠らないこと」が、結果的に、セキュリティ対策の質向上に貢献する

6.「インシデントの経験者を、『被害者』として『保護・支援』する」とは

- 現在、セキュリティ関連の被害（攻撃者にもなり得る）状況は、どのようにして被害に遭ったのかなどの情報が、何となく隠蔽されている感がある
- しかし、本当に何があったのかを知り、その経験から学ぶべきことが多くある。そのため、知ることができる環境が常にあることが重要であり、被害者を責めることには意味がない。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、隠されてしまい、知ることができないことによる損失が大きい
  - 例：航空機事故調査は、真実を明らかにすることにより、次の事故を防ぐための調査や情報公開であり、悪者を探し、追求するための物ではない
- 被害に遭うのは、もちろん恥ずかしい側面もあるが、これを事実として受け入れ、各自が対応していくという意識が常識となることが望ましい

7.「『原理主義』ではなく『実践主義』で進める」とは

- 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
- 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り、大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
- 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

8.「『匿名性』の堅持」とは

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議

- 「セキュリティ」の実現には、ユーザの認証が必要と考えるのが普通であるが、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
- 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、ユーザーの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る。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る
- 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。「目安箱」などは、その一つの実装方法。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通常であり、このようなことが起こらないように、「匿名性」が必要である

9.「『実施権』は個人にある、ただし、第3者への委任は可能」とは

- 「フィルタリングは、プラットフォームが行うことは適切とは言えない。フィルタリングは、ユーザの責任であるべきである。ユーザは、このフィルタリングを信頼可能な第3者に委任・委託することは、ユーザの責任の範囲で不可能ではない」となるのではないか
- 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」の考え方です。トランスペアレントなインフラを提供し、高度な機能な、エンドノードが実現する

10.「セキュリティ(投資)を品質(向上)ととらえる」とは

- 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、その品質を向上するべく、これらに関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る
- 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る。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である。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確りと実践することが前提となる

本日、共有・議論したいこと

- 目的とターゲットについての意識合わせ
- 10の基本の考え方についての過不足、意見の相違の確認
- 今後の進め方についての相談
  - 本日いただいたコメントをドキュメントに反映する
  - MLなどですべての議論を追うことが難しいため、チームでオンサイトで意見を集める場を設ける