

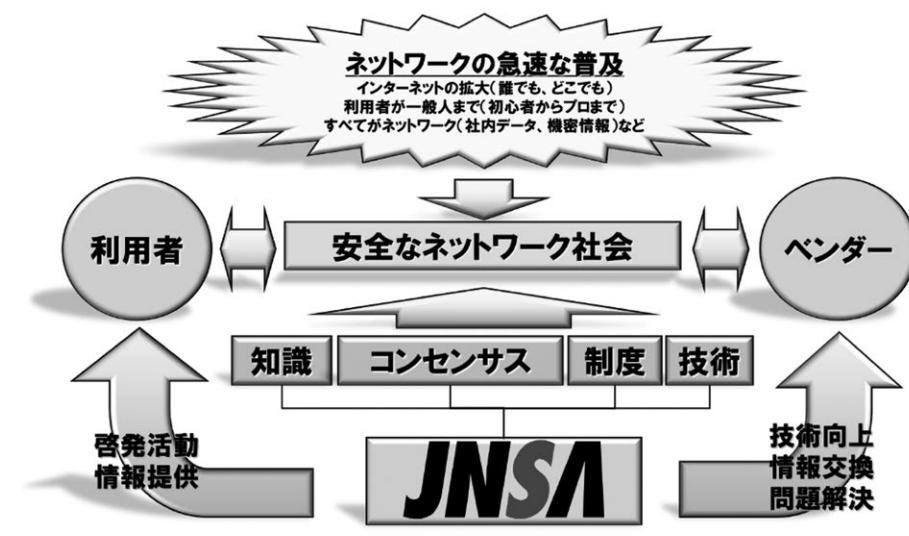
JNSAの22年を振り返って

NPO 日本ネットワークセキュリティ協会
事務局長 下村 正洋



JNSAは2000年4月13日に任意団体（翌年NPO法人化）として発足し、22年が過ぎようとしています。そこで、設立時の情報セキュリティを取り巻く社会状況と設立後数年の活動を振り返り、現在の状況を比較し、これからのサイバーセキュリティ（設立当時はネットワーク・セキュリティと言っていました）とJNSAの今後の方向性について考えてみたいと思います。

JNSA設立の検討を開始した前年1999年には、3月にMelissaウイルスが猛威を振るい、5月に京都府宇治市で21万人の住民基本台帳の漏洩事件、2000年1月には中央省庁Web改ざんが発生しました。インシデント事案以外には、1996年にJPCERT/CC創立、1998年にはPマーク制度開始、関係省庁にも情報セキュリティに関する部署が設立され、2000年2月にはNISCの前身である情報セキュリティ対策推進室が内閣官房に設置されました。以後、2002年にはISMS認証制度が始まるなど、情報セキュリティ対策関連の制度・製品・サービスも次々登場し、情報セキュリティ対策の重要性を認識した人たちにより、それを推進するための仕組みづくりが始まった時期でした。そのような中で、JNSAはセキュリティベンダーが相互に情報セキュリティ問題を共有し、かつ、連携し、社会全体の情報セキュリティ対策が進むことを目的として設立しました。設立当初の会員数は54社（2021年末は260社）でした。



設立時の活動概念図

設立当初(2000年)の主な活動は、外部接続に関するセキュリティポリシーサンプルの作成、セキュリティ評価基準の実態調査、IPsec製品の相互接続実験、PKIの研究、製品・サービスの一覧表の作成、技術用語の考察、不正アクセス調査、ダイナミックディフェンス(動的防御)フレームワーク開発でした。翌年(2001年)にはセキュリティ被害調査、コンテンツセキュリティの活動が開始し、セキュリティ技術者育成のための教育部会も発足しました。以後トピックとして一般向けインターネット安全教室開始(2003年)、セキュリティ技術者知識体系SecBoKの前身となるSkipmapの開発、情報セキュリティ教育事業者連絡会-ISEPA-(2007年)、日本セキュリティオペレーション事業者協議会-ISOG-J-(2008年)設立と続きます。その後、2009年に大幅な部会組織の改定を行って、現在の部会構成になっています。詳しくはこの冊子の後半に掲載している「事務局お知らせ：JNSA部会・WG活動内容」をご覧ください。

さて、振り返りが長くなりましたが、設立当初(約20年前)と現在の活動の分類を見ると、基本的には情報セキュリティが抱える課題の分野は大きな変化が起こっていないと見えます。これは、つまるところ、セキュリティ問題は人の活動にかかわるものであり、人が構築したもの、それを利用する人、その人達で構成する社会システムなどの脆弱性とその脆弱性を利用した不正や過失をいかに抑制するかが課題だからと考えます。ただし、すべてのものがインターネットに接続される状況(IoT)の進化とともに、情報セキュリティという語り口がサイバーセキュリティに変化し、企業活動はもとより、一般人の社会生活にも深く関係し、加えて国家安全保障問題になってきたのは、いまさら指摘することではないと思います。

とくに、近年ゼロトラストの概念が提唱されてきていますが、それまでは境界防御をいかにするかが重要なテーマでした。これは、今猛威を振っているCOVID-19の水際作戦やバブル方式とまったく同じ発想であり、それが破綻するのとも人の動きを制限することが実質的に、つまり、経済活動や人の社会活動に対抗する方式であるためだと考えます。したがって、接種証明書、検査証明書、対策済みマークなどそれぞれの主体の健全性を証明しつつ接することが必要であり、そのような対策が迅速に進めることができる社会システム(社会的コンセンサスも含む)の構築が急がれているのではと考えます。同様にサイバーセキュリティを推進するにおいて、流通する情報(データ)そのものとその情報にアクセスする主体(システムだけでなく人も)の信頼性の確保が重要になっているのではないのでしょうか。加えて、DXを推進し、その安全を確保するためのセキュリティ対策が進展してゆく中で、システムが現在よりも密接に関連することにより、社会システムとして脆弱点が絞られてくる懸念があり、これが社会全体の脆弱性に発展すると考えます。したがって、サイバーセキュリティ対策を推進する上において、単に攻撃や不正、過失を防止するというITシステム的対応だけでなく、セキュリティ対策を推進した結果として創出される社会において、民主主義を堅持し、人権を守るという視点からの社会全体のシステム設計が必要ではないかと考えます。つまり、セキュリティ対策を進めるためには、統制力を強めるこ

とシステムとのスマートな連携が必要であるが、統制が専制を誘発しないように、かつ、連携したシステムが社会のメルトダウンを惹起しないように工夫しなければならないのではないのでしょうか。2002年に発表された「OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security(情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて)」を今一度読むのもいいのではと思います。

JNSAは、単にセキュリティ対策を推進するのではなく、調和のとれた、すべての人々にとって安寧な社会を実現するために活動しなければならないと考えます。今まで述べてきたようにサイバーセキュリティは様々な要素があることから、一つの企業や組織、個人では解決できないことです。JNSAは前述した設立の理念を堅持して、これから、ますます情報セキュリティ(サイバーセキュリティ)に関係する企業や組織や人々が増えてくる、否、すでに全てがサイバーセキュリティに関係している現在において、これらの参加者(OECD9原則参照)の方々が集まり、問題を共有し、解決策を検討し、会員各位の皆様へ、ならびに社会に対してフィードバックできるような場を提供し続けることが必要ではないかと考えます。