初期のJNSA技術部会の活動とChallenge PKIプロジェクト

JNSAフェロー　松本　泰

1．はじめに

日本ネットワークセキュリティ協会（JNSA）は、25年前に情報セキュリティ分野における社会的責務と発展を目的として設立された非営利団体です。その設立初期において、技術部会（現在の標準化部会）はJNSAの活動を牽引する存在として、多様な取り組みを展開していました。

本稿では、初期の技術部会の活動を振り返るとともに、私自身がリーダーを務めたChallenge PKIプロジェクトなどの経験を通じて、これからのJNSA活動に何らかの示唆を与える視点を提示できればと考え執筆しました。

2．JNSA立ち上げ当初のIPsec相互接続実験

2000年代初頭、セキュリティ製品やソリューションはまだ限られており、市場は未成熟でした。そのため当時の技術部会の活動は、試行錯誤の連続でもあり、同時に「なぜ（Why）行うのか」「何を（What）解決するのか」を深く考える時期でもあったように感じます。

そうした中で最初期の活動のひとつが「IPsec相互接続実験」です。異なるベンダーの機器によるVPN運用の実現可能性を検証するものでしたが、これは単なる技術的な試みではなく、企業や業界（当時のターゲットの一つは自動車業界の受発注ネットワーク）における実利用を見据えた社会的実証の意味を持っていました。

この実験を支えたのが、工学院大学新宿校舎内に設置された物理的な「場」である共同実験室（教室）でした。大学の協力を得て、各ベンダーの機材を持ち込み、現場で設定を突き合わせ、対面で議論を重ねながら接続を試みるというのは、それまでの日本ではあまり行われていなかった活動だったのではないでしょうか。

こうした活動を通じて、製品ベンダー、SI企業、ユーザー企業、研究者など立場を超えた交流が生まれ、新たな人的ネットワークが形成されました。このようなネットワークこそが、その後の技術部会のみならず、JNSA全体の活動を支える基盤の一つとなったと感じています。

この成果はIPAの「IPSec相互接続に関する調査報告書」[(*1)]としてまとめられ、現在においても参照可能です。25年前の活動ですが、読めば当時すでに高度な課題に挑んでいたことが理解できるでしょう。

3．2002年頃のワーキンググループの多様な活動

2001年から2002年頃にかけて、技術部会傘下では様々なワーキンググループ（WG）が次々と立ち上がり、活発に活動していました。その様子は「第二期部会活動報告（2001年活動内容）」[(*2)]などで確認できます。

当時のWGリーダーには、現在もなおサイバーセキュリティ業界を牽引する方々が名を連ねています。例えば

- セキュリティポリシWG
  三輪 信雄氏（株式会社ラック）
- 技術用語WG
  佐藤 慶浩氏（日本ヒューレット・パッカード株式会社）
- IDS研究WG
  髙橋 正和氏（インターネットセキュリティシステムズ株式会社）
- 不正アクセス研究WG
  園田 道夫氏（株式会社アイ・ティ・フロンティア）
- ST（セキュリティターゲット）作成
  西本 逸郎氏（株式会社ラック）

（所属は2001年当時のものになります）

ここに紹介した方以外にも多くの方が活躍され成果を出し、今なお業界をリードしている方も多数おられます。また、非常に残念なことながら故人となられた方もおられます。

これらのWGは「IPsec相互接続実験」に見られるような技術検証だけでなく、セキュリティポリシー策定や技術用語の整理、リスク分析、インシデント対応の指針づくりなど様々な成果物を生み出しました。振り返れ

ば、これらの活動は日本におけるサイバーセキュリティの基礎を築いた重要な一歩であり、単なるワーキンググループを超えた社会的な役割を果たしていたと言えるのではないでしょうか。

私自身も、こうしたWG活動を通じて多くの人と出会い、大きな刺激を受けました。当時の議論と交流は、その後の私自身の活動にも大きな影響を与えました。

4. Challenge PKIプロジェクト

こうした多様な活動の中で、私自身がリーダーを務めたのが「Challenge PKIプロジェクト」です。2001年の報告書では「CA相互接続WG」として紹介されていますが、その後「Challenge PKI」として長期にわたり活動し、現在の標準化部会のPKI・PQC運用技術WGに受け継がれています (*3) (*4)。

Challenge PKIプロジェクトは、「IPsec相互接続実験」などに触発されて始まったもので、当時の電子政府認証基盤GPKI(その後のJPKI) などを発展させることを念頭に置き、マルチベンダーPKI、マルチドメインPKI環境下での技術的相互運用性確保を目標としていました。

このマルチベンダーPKIの相互運用という技術的課題はその後収束しましたが、マルチドメインPKIについては非技術的課題が大きく、25年を経た今も解決されているとは言えず、デジタル社会における課題として残り続けています。

私自身にとって、このプロジェクトでの大きな出会いが、2019年に逝去された稲田龍さん（当時富士ゼロックス株式会社）です。稲田さんの提案によりChallenge PKIプロジェクトの成果をIETFで発表することになり、その後、RFC 5217 Memorandum for Multi-Domain Public Key Infrastructure Interoperability (*5) として国際標準文書にまとめられたことは、国内の試みを世界に広める大きな成果でした。

5. 現在への示唆：Why/Whatを再度考える

今日のサイバーセキュリティ分野では、25年前の未成熟な市場とは大きく異なり、クラウド、ゼロトラスト、AIなど多様なソリューションが次々と登場しています。その結果、これらを使って「どのように実現するか（How）」に焦点が当たりやすくなっています。

もちろんHowの検証は必要ですが、Howだけに偏れば「なぜその取り組みを行うのか（Why）」「何を解決するのか（What）」が曖昧になり、活動が形骸化する危険があります。例えば、ゼロトラストの導入が目的化してしまい、「誰の、何を守るための施策なのか」が議論されないまま進んでしまうような事例も見受けられます。

また、現在注目される生成AIの進展は、サイバーセキュリティにも大きな影響を与えることが考えられます。

こうした社会の変化に対応するためには、初期の技術部会の活動にあったようにWhyとWhatを問い続け、また時には試行錯誤を繰り返し、その上でHowを選ぶ姿勢が今こそ重要になるのかもしれません。

6. 結びに

25周年を迎えた今、JNSAにとって大きな課題は、新しい課題に挑むこと、そしてそのための新陳代謝を続けることです。新しい人材や新しい視点が組織に入ってこそ、活動は進化し続けます。

その際に参考になるのが、JNSA初期の活動です。限られた環境の中でWhyとWhatを問い直し、仲間と共に試行錯誤しながら社会に価値を届けようとした姿勢は、これからの活動にも大きな示唆を与えます。

過去を振り返ることは、未来を築くための礎です。初期の活動に込められた理念と連携の精神を大切にしながら、新しい課題に挑戦し続けることで、JNSAは次の25年も日本のセキュリティを支える存在であり続けるはずです。初期の精神を受け継ぎ、新しい挑戦を続けることこそが、これからの25年を切り拓く原動力になると信じています。

【参考URL】

*1 IPA：「電子政府情報セキュリティ技術開発事業 / IPSec相互接続に関する調査」報告書
https://www.jnsa.org/active/2000/active00_3b.html

*2 第二期部会活動報告（2001年活動内容）
https://www.jnsa.org/active/2001/active01_2f.html

*3 Challenge PKI プロジェクト
https://www.jnsa.org/mpki/cpki/index_j.html

*4 JNSA／PKI・PQC運用技術ワーキンググループ
https://www.jnsa.org/result/pki/index.html

*5 RFC 5217
https://datatracker.ietf.org/doc/html/rfc5217