国家によるサイバー攻撃に対応する次世代信頼醸成措置の在り方

～日中韓 CSIRT 間連携のケーススタディから～

一般社団法人 JPCERT コーディネーションセンター
小宮山 功一朗
希望プログラム GR

1. 概要

本研究は、国家による物理的な損害を与えるためのサイバー攻撃のリスクの高まりを前提に、サイバー空間での衝突のリスクを減らす手段としての信頼醸成措置(Confidence Building Measures)について、その位置づけと必要性と限界を明らかにし、加えて実現に向けた道筋を示すことを目的とする。
サイバー空間での信頼醸成については政府、国際機関、民間事業者による検討においてその必要性が認知されつつあるが、実現にむけたロードマップが示されていない。本研究では「サイバー空間での信頼醸成は、技術者を中心とするグループによる緩やかな合意と実績あるメカニズムを政府ないし国際機関が追認するという段階を経て成立する。」、「信頼醸成措置は既存の二国間、地域間での取り組みの成功例を拡張していくという形をとる。」という 2 つの作業仮説を検証していく。そして日本･中国･韓国の 3 カ国間で 2011 年から行われている信頼醸成などを目的とする技術者レベルでの連携事例を分析する作業などを通じて、伝統的な安全保障の分野で受け入れられている信頼醸成の考え方を、サイバー空間に応用する具体的手法を提案することを目指す。

2. これまでの**研究テーマ・研究実績**

学部での研究実績

1998 年から 2002 年まで青山学院大学経営学部に在籍した。田中正郎ゼミでは経営情報学を学び、情報システムによる経営の効率化について学習した。

社会人としての研究実績

その後 2002 年からは一貫して情報セキュリティに係る問題について技術的な解決策を示す業務に携わってきた。電通大学や情報セキュリティ大学院大学の研究者との共同研究に参画し、成果を情報処理学会コンピューターセキュリティ研究会などに投稿した。

3. 研究テーマ

″国家によるサイバー攻撃のリスクに対応する次世代信頼醸成措置の在り方 ～日中韓CSIRT 間連携のケーススタディから～″

4. 研究の背景

背景 1: サイバー空間は多様な利害関係者の共通の財産であった

サイバー空間(インターネットを含む情報通信ネットワーク)は経済活動の基盤であり、数多くの技術革新を生み出してきた、現代社会のライフラインであることは論を待たない。インターネット黎明期から、これを用いたシステムへの侵入、改ざん、詐欺行為、迷惑メール送信などの問題(以後、サイバー攻撃と総称する)は絶えず起こっていたが、通信事業者や CSIRT とよばれるセキュリティ問題への即応を目的とする非営利組織などが中心となり、不正行為をまずは停止するという対応が行われてきた。不正利用をする犯罪者に対して通信事業者、CSIRT はじめとするセキュリティ専門家、政府が相互に連携するという枠組みがあった。サイバー攻撃は国境をまたがって発生するが、関係各国当局にとっても不正利用を減らし、自国のサイバー空間を健全に保つことは共通の利益であり、サイバー攻撃対応に関しては国際協力を阻む大きな制約は存在しなかった。

背景 2: 国家がサイバー攻撃を行う時代、サイバー空間は戦場となった

しかし 2007 年に発生したエストニア政府、銀行 Web サイトなどに対する大量に通信を発生させサイト閲覧を不能にする事案にロシア政府の関与が疑われたこと、2010 年に発生したイランの核処理施設へのサイバー攻撃により施設が破壊された事案でアメリカ政府の関与が米紙で報道されるなど、近年のサイバー攻撃は手口が巧妙化するばかりでなく、その背後に国家による直接的ないし間接的支援があるとの認識が広まりつつある。

このような流れの中、米国はサイバー空間を陸･海･空･宇宙に次ぐ第 5 の空間と表現し、サイバー空間での影響力を保つことは安全保障上の重要な課題であると宣言した。呼応するように日本を含めサイバーセキュリティは安全保障問題との認識は広く定着した。

ここにサイバー攻撃に関して犯罪者とそれを取り締まる者という単純な構図は崩壊し、国家間の緊張が高まりつつある。国家間の緊張は民間事業者の連携の阻害要因となり、サイバー空間を守るための新しい秩序たる国際規範あるいは国際条約を求める声が高まりつつある。

背景 3: 進展のみえない新しい秩序作り

サイバー空間の新しい秩序を求める営みの代表的なものとして国連の政府専門家会合と「サイバー空間に関するロンドン会議(通称ロンドン会議)」があげられる。

国連はこれまでに 3 回の政府専門家会合を第一委員会の下に招集した。2010 年に終了した同会合では、取られるべき 3 つの施策を示した。1. 国家の ICT 利用によるサイバースペー

スリスク軽減のための国際規範について議論を継続すること 2. サイバー空間での信頼醸成を続けること 3. ICT 格差を解消するための能力開発(以後、キャパシティビルディング)を強化することである。
ロンドン会議は政府、民間、国際機関、市民団体が一同に会するマルチレベル議論の場として、2011 年にイギリスのヘーグ外相の呼びかけで始まった。その後毎年フォローアップ会議が行われており、各会議後には上記の 3 点の重要性を踏襲する議長声明を発信している。
2014 年は国連の政府専門家会合、ロンドン会議のどちらも開催される予定がなく、多国間交渉の機会は少ない。

5. 研究の目的

国家による物理的な損害を与えるためのサイバー攻撃(Offensive Cyber Operation)のリスクの高まりを背景に、そのリスクを減らす手段を追求したいと考えたのが本分野に興味を持ったきっかけである。研究の目的は政府、民間、国際機関、NGO などのコンセンサスを重視するサイバー空間で信頼醸成の必要性とその限界を明らかにし、加えて実現に向けた諸問題を明らかにすることである。
本来、信頼醸成措置は国家間の対話を通じて、透明性を相互に確保し、戦争や危機発生時の過激化(エスカレーション)を防ぐための手段である。頼醸成措置の代表例にはキューバミサイル危機の後に米ソ首脳間に設けられたホットラインがあげられる。
信頼醸成だけでリスクが軽減されるわけではないことは言うまでもない。伝統的な国家安全保障に目をむけると、規範形成、軍備縮小などの取組みが平行しているところである。しかし軍備縮小や規範形成に向けた対話のテーブルに着くにはあたっては、まず当事者間の対話が必要であるのと同様に、サイバー攻撃のリスク低減の道筋を描く上でも、まず非友好国間での信頼醸成が必要となると考える。それが、本研究においてとりわけ信頼醸成に焦点を合わせる理由である。

6. 研究手法

サイバー空間における信頼醸成措置に関する先行研究として Baseley-walker(2012)が CSIRT や多国籍企業による民間主導の信頼醸成の可能性を提示している。また Kavanagh, C(2013)らは現在のサイバー空間のセキュリティ議論においては信頼醸成措置をもつ目的についての共通認識が存在しないという問題を指摘したうえで、更に信頼醸成措置を 4 つの側面に分類し、それぞれの項目について取り組みの具体例を提示している。

Kavanagh, C(2013)らの研究は例えば国連などの国際機関による議決を経て、信頼醸成がト

ップダウン型で行われることを前提としているのに対して本研究では「サイバー空間での信頼醸成は、通信事業者や CSIRT を中心とするグループによる緩やかな合意と実績あるメカニズムを政府ないし国際機関が追認するという段階を経て成立する。」、「信頼醸成措置は既存の二国間、地域間での取り組みの成功例を拡張していくという形をとる。」という 2 つの作業仮説を検証することを通じて信頼醸成措置の在り方を見定めていく。

具体的には新時代の信頼醸成措置に要求される機能を明らかにし、その実現可能性および実現した場合の効果の及ぶ範囲を研究する。加えて既存の軍事衝突回避や軍備縮小の枠組みとの対比によって、サイバー空間に応用可能な取り組みを抽出する。そして信頼醸成措置の議論において度々好例として言及される、日本・中国・韓国の間で実施されている CSIRT レベルでの連携強化を含めた、地域単位の取組みの実態と成立経緯をまとめ、関係が必ずしも良好な関係でない国や非同盟国との信頼醸成の成立条件、及びその限界を明らかにする。

文献調査とヒアリングを通じて以下の点を明らかにすると必要があると考える。

・既存の安全保障研究における信頼醸成措置の調査

・日中韓 CSIRT 連携、アジア地域における ISP と CSIRT の国際連携事例などに関するケーススタディ

・米国とロシア、日本と米国、米国と中国の間で行われている二国間サイバー協議のサーベイ

・既存の地域安全保障の枠組みに含まれるサイバー攻撃に関する取組の動向調査(アセアン地域フォーラム(ARF)、NATO、欧州安全保障協力機構(OSCE)、米州機構(OAS)、アフリカ連合(AU)を想定)

・主要国(20 カ国程度を想定)の CSIRT と主要通信事業者の戦略、沿革、資金提供源、役割の調査

本研究の目指す方向性を確認し、多様な有識者からの意見を集約するため、研究初期の段階から口頭発表の機会を持つこととする。Cyber Norms Workshop(www.citizenlab.org/cybernorms/)、国際安全保障学会、Cycon(ccdcoe.org/cycon/)などを発表の機会として想定している。

7. 研究の意義・期待される成果

研究の成果として、国内事業者に対するサイバー攻撃対応の前面にたち民間レベルでの国際連携に携わる立場から、より実現可能性が高く、機能する信頼醸成の取り組みを広く国際社会に提案したい。信頼醸成措置の必要性は関係者内に認識されだした段階であり、本研究によって CSIRT や民間企業による信頼醸成措置の可能性を提示することは、既存の安全保障の枠組みを強化とサイバー空間の健全な発展の両面に資すると考える。

また日本・中国・韓国の 3 カ国は緊密な経済的結びつきをもちつつ、政治的対立要素を抱えているインターネットのホットスポットである。3 カ国の間での信頼醸成の試みを明らかにすることは、同様の緊張を抱える地域(例えばベトナムとフィリピン)に一つのロールモデルを提示できると考える。

最後にサイバー攻撃は多様性、匿名性、隠密性、攻撃側の優位性が高く、ゆえに抑止が困難といわれている。日本は憲法第 9 条に戦争放棄、戦力不保持及び交戦権の否認がうたわれ、特にサイバー攻撃について自衛権が発動されうるかは未だ議論の途上にある。攻撃側の優位性が明確なサイバー空間で衝突が起きれば、専守防衛を旨とする日本の影響力は相対的に弱まりかねない。それゆえにサイバー空間の責任ある利用を対外的にも求め、サイバー空間での衝突や紛争を避けるために働きかけることは特に日本において極めて重要であり、信頼醸成の強化はその働きかけの入り口として有効であると考える。

以上をふまえ、本研究の成果としてまとめる論文では、国際社会、地域社会、そして日本(政府および民間事業者)のそれぞれへの提言を行うものとする。

8. 必要な研究施設

とくになし。

9. 関連文献

[1] Kavanagh, C., & Stauffacher, D. (2013). CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY. Geneva.

[2] Tikk-ringas, E. (2012). Developments in the Field of Information and Telecommunication in the Context of International Security : Work of the UN First Committee 1998-2012.

[3] Baseley-walker, B. (2012). Transparency and confidence-building measures in cyberspace, 10.

[4] 土屋大洋. (2013). サイバーセキュリティのグローバル・ガバナンス -国際的な規範の模索-. NEXTCOM, 14, 4-11.

[5] 第一回　日中韓　サイバーセキュリティインシデント対応年次会合に係る JPCERT/CC、CNCERT/CC、KrCERT/CC の共同声明 (2013) https://www.jpcert.or.jp/pr/2013/PR20130904-CJKJointStatement.pdf