国際協力　ベトナム　サイバーセキュリティ

世界の潮流 ～国際貢献～

ベトナムにおけるサイバー攻撃対策向上プロジェクト

NTT東日本
渡邉（わたなべ） 紗知（さち） /野口（のぐち） 麻央里（まおり）
勘場（かんば） 宣男（のぶお）

NTT東日本国際室では国際協力活動の一環として，開発途上国が応募した国際機関の公募案件に対する実施支援を行っています．ここではベトナム国情報通信省の要請により，2016年５月から2019年３月にかけて実施した，サイバーセキュリティ対策向上プロジェクトについて紹介します．

NTT東日本国際室の活動

NTT東日本の国際協力の歴史は古く，開発途上国の情報通信分野の発展に寄与することを目的として，技術協力専門家派遣，青年海外協力隊員派遣支援をNTT１社時代から行ってきました．NTT東日本からの派遣実績は累計81名に及びます．一方で，グループ再編に合わせ国単位で分担されたプロジェクトがあり，NTT東日本はベトナムとインドネシアのプロジェクトを継承し，共同事業プロジェクトの実施によるリレーションを築いてきました．現在では，ベトナム・インドネシアでのビジネス形成に加えて，社内外からの要請に基づく国際活動もまた国際室の大きなミッションです．国内外政府等からの要請に基づく政府機関などの補助金を活用した国際協力事業や，研修生や視察受け入れなどを通じて，アジアを中心とした開発途上国の情報通信分野の発展に貢献しています．

APTが主催する国際協力プロジェクト

国際協力分野における活動においては，さまざまな政府組織や国際機関との連携の下実施しています．中でも，APT（Asia-Pacific Telecommunity：アジア太平洋電気通信共同体）は，NTT東日本国際室の活動と深いかかわりを持っています．APTは1979年にアジア・太平洋地域における電気通信専門の国際機関として設立されました．本部はタイ・バンコクにあり，当該地域における電気通信の均衡した発展を目的として，研修やセミナーを通じた人材育成，標準化および無線通信等の地域的政策調整を行っています．加盟国は38カ国にのぼり，多くの電気通信事業者やメーカもこれに協賛しています．このAPTが主催する２つの国際協力プログラムがあります．１つは，ICT利活用モデルの普及・展開を目的とする，日本とAPT加盟国の技術者・研修者による国際共同研究です．もう１つは，デジタルデバイド解消や人材育成を目的とするパイロットプロジェクトです．

これらの案件に優先される分野として，６つのテーマが挙げられ（**表**），本案件では「③ICTにおける信用と信頼」の中での重要なポイントであるサイバーセキュリティに着目し，2016年５月から11月の期間においてAPT国際共同研究のプログラムを，その発展形として2018年４月から2019年３月にわたって実施したAPTパイロットプログラムを実施しています．

ベトナムにおけるサイバーセキュリティ

ベトナムの経済は急速に成長してお

表　優先分野

①　デジタルエコノミーの持続的成長に資する政策 ブロードバンド環境の整備，無線周波数の調和，標準化活動の推進
②　ICTを通じた安心・安全な社会 災害管理・通信分野における情報共有・人材育成，ブロードバンドネットワークの利用
③　ICTにおける信用と信頼 サイバーセキュリティ分野における政府・民間部門の協力推進，CERT/CSIRTの活動支援
④　イノベーションのための持続可能なICTエコシステム アプリケーション・サービスの開発奨励，ICTの革新的利用の促進
⑤　キャパシティビルディングおよび制度開発 研修の強化・拡充，各国課題解決のための専門家調査の実施，専門家間の協力強化
⑥　ICT開発のための地域協力の強化 ベストプラクティス・技術の共有，官民協力パートナーシップの強化，APTのプレゼンス向上

り，海外直接投資の順調な増加も受けて2010年に中所得国の仲間入りをしています．人口１人当りのGDP，実質GDP成長率も安定して伸び続けており，海外企業のASEAN地域進出拠点の１つとなっています．そのような急激な経済発展やインターネットの利用者拡大が進む一方で，サイバー攻撃の標的としての危険性も増大しています．１つの転機となったのは，ナショナルフラッグキャリアであるベトナム航空に対する標的型サイバー攻撃でした．その攻撃により，航空制御システムおよびWebサイトがハッキングされ，ハノイ・ノイバイ空港，ホーチミン・タンソンニャット空港の表示システムやマイレージプログラムに甚大な被害をもたらしました．加えて，41万人以上の個人情報も窃取されたともいわれており，多くのベトナム人に衝撃を与えました．ベトナムでは，情報通信省がサイバーセキュリティ関連の所轄官庁となっており，その配下に政府機関や企業のコーディネーションセンターとしてセキュリティインシデント対応を実施するナショナルCSIRT（Computer Security Incident Response Team）であるVNCERT（Viet Nam Computer Emergency Response Team）があります．VNCERTは2005年に設立されており，ネットワークのモニタリング等を通じて政府機関，企業等と連携しながらサイバーセキュリティにかかわるインシデントに対応してきました．本案件は，このVNCERTからの要請により形成されました．

民間企業におけるCSIRT構築促進

VNCERTの課題の１つとして，サイバーセキュリティインシデントを統括する組織CSIRTの普及がベトナム民間企業において伸び悩んでいるというものがありました．セキュリティ分野において先行するNTTグループの知見を活かし，2015年９月にVNCERTによるAPT国際共同研究プログラムへの応募を支援，2016年１月に採択されました．NTT東日本国際室として，セキュリティ分野での国際案件形成は初となります．活動内容としては，NTTグループ内CSIRT組織におけるOJT，CSIRT構築マニュアルの作成，ベトナム企業へのヒアリング調査が主なものとなります．まず，VNCERT若手技術者４名に対し，１カ月にわたるOJTを開催し，CSIRTのあり方を学んでもらいました．それを受けて，NCA（Nippon CSIRT Association：日本シーサート協議会）が作成したCSIRT構築マニュアルをベースに，ベトナムの現状に沿ったベトナム語版マニュアルを研修生に作成してもらいました（**図１**）．その後，民間企業への現状ヒアリングを受けて内容をブラッシュアップし，政府機関VNCERTの名の下にベトナム全土の企業へ配布されました．本案件は，2016年10月に日本で行われた，アジア太平洋地域におけるCSIRT共同体であるAPCERT（Asia Pacific Computer Emergency Response Team）の年次総会において，日越協同プロジェクトとして報告されています．

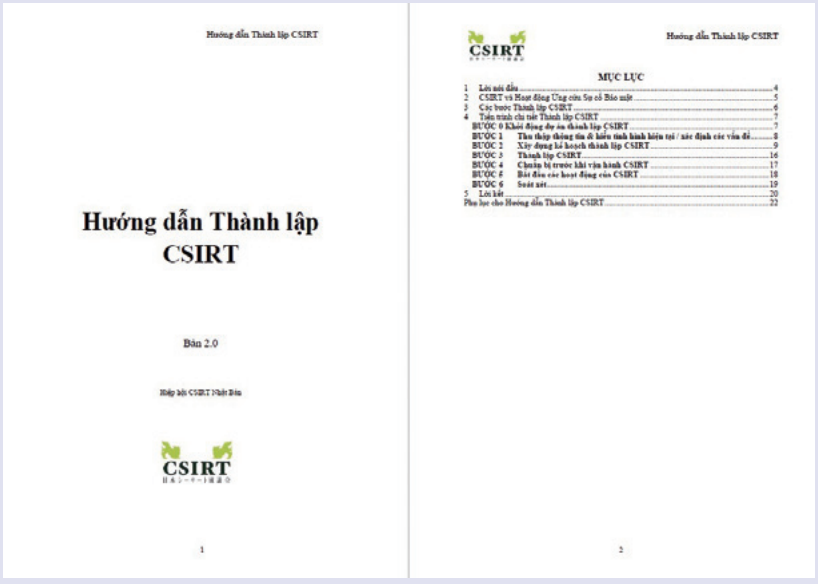

図１　マニュアルイメージ

共同研究を通して発見されたさらなる課題

サイバー攻撃事例やセキュリティ対策の現状についてベトナム企業へヒアリングする中で，前述のベトナム航空への大規模サイバー攻撃を受けて，多くの企業が標的型サイバー攻撃に対する危機感を持っていることが判明しました．標的型サイバー攻撃とは，特定の個人や組織，情報をねらったサイバー攻撃であり，無差別に行われる攻撃とは異なり対象の個人や組織特有の情報を利用するため被害が甚大となる傾向にあり，日本においても日本年金機構をはじめとして被害が多発しています．より深く分析を進めると，危機感を持っていながらもどのように対処して良いのか分からない，有効なソリューションや対処法が見つからないといった具体的な課題が見えてきました．それを受けて国際共同研究プログラムの

次のステップとして，標的型サイバー攻撃対策をテーマとしたAPTパイロットプロジェクトへの応募支援要請を受けました．共同研究プログラムの完遂後，海を挟んでの電話会議を重ね，日本でのプロジェクト参画メンバを募り，応募内容を決定しました．2017年９月の応募を経て，加盟国38カ国からの提案，さらにベトナム内から３案件が集う中，狭き門を潜り抜けて2018年１月にプロジェクトが採択されました．

標的型サイバー攻撃対策プロジェクト

ベトナムでの標的型サイバー攻撃対策向上に向けて，ハード面，ソフト面両観点からのプログラムを実施しています．

⑴　標的型サイバー攻撃対策ソリューションのトライアル検証

ハード面からのアプローチとしては，日本製標的型サイバー攻撃対策ソリューションのVNCERTへのトライアル導入・協同検証を半年間にわたり実施しています．有効なソリューションがベトナムにないことが課題とされていたこともあり，今後VNCERTが国内企業へ標的型攻撃対策向上支援をするうえでの知見を得るため，日本国内で評価の高いソリューションをまずはVNCERT各拠点に導入し，効果検証を始めることとしました．振る舞い検知により未知のマルウェアを検知するソリューション，マルウェアの侵入経路と拡散状況を分析可能なソリューションに加え，VNCERTがナショナルCSIRTとしてベトナム国内ネットワークのモニタリングをミッションとしていること，ベトナムにおいてもSOC（Security Operation Center）サービスが着目されつつあることを受けて，エンドポイントソリューションと連携してサイバー攻撃の可視化が可能となるシステムも併せて導入しました．首都ハノイ，ダナン，ホーチミンの３拠点にあるVNCERTのオフィス内のおよそ120台の端末に対しエンドポイントソリューションを，メイン拠点であるハノイに可視化システムを導入し，ソリューションの有効性を検証しました（**図２**）．日本とは環境が異なることもあり，拠点間ネットワークの未整備，端末コンソールの利用不可，度重なる停電によりネットワーク設定が初期化されてしまう等の課題もありましたが，日越技術者チームでのディスカッションを重ね，ベトナムの国情に合わせた解決方法を検討していきました（**写真１**）．検証期間を通し，マルウェア検知によるソリューション有効性を確認し，今後のベトナム国内企業支援におけるベースとなる知見が得られたことはもちろん，日本の技術者との交流を通じてVNCERT若手技術者のスキル向上にもつながりました．

⑵　日本での研修プログラム

ソフト面における活動内容としては，日本での研修プログラム，ベトナム企業向け意識啓発セミナーが挙げられます．日本での研修は，２回に分けて実施しています．2018年４月には，VNCERT若

図２　ソリューション導入イメージ

写真１　ソリューション導入の様子

写真２　ディスカッションの様子

写真３　ベトナム企業向け意識啓発セミナー

手技術者向けにテクニカルな技術交流やディスカッションが可能なプログラムを設定しました．セキュリティベンダ訪問を通じたセキュリティソリューション理解，セキュリティ関連機関との技術交流を実施し，技術交流の場ではNTTグループのサイバーセキュリティ関連部門にも参加いただき，ベトナムと日本でのサイバー攻撃対策事例の共有を通じ，積極的なディスカッションを実施しました（**写真２**）．2018年12月にはVNCERT局長が来日し，日本のセキュリティ関連機関を訪問し，CSIRTネットワーク構築やその運営方法，セキュリティ技術者育成・資格試験体系について活発な議論が交わされました．併せてサイバーセキュリティ関連の政府機関も訪問し，ナショナルCSIRTのあり方，組織体系，政策に関する知見共有を実施しています．

⑶　ベトナム企業向け意識啓発セミナー

2019年12月，パイロットプロジェクトの集大成として，ハノイにおいてプロジェクトの成果発表を兼ねた官公庁・企業向けのサイバーセキュリティセミナーを開催しました．外務省，運輸省，科学技術省等のベトナム政府機関のIT部門の責任者，VNPT（Vietnam Posts and Telecommunications Group），Viettel等の通信事業者やセキュリティベンダを中心に計70名が参加し，標的型サイバー対策のリスクやその対策方法を学びました（**写真３**）．また，サイバーセキュリティ分野における日本ASEAN諸国との国際的な連携・取り組みを強化することを目的として，年次で開催されている「第11回 日・ASEANサイバーセキュリティ政策会議」の場においても，本取り組みを発表し，ASEAN加盟国の経済・投資関係省庁および情報通信関係省庁の局長・審議官クラスに対するプロモーションを実施しています．

今後に向けて

パイロットプロジェクトを完了し，VNCERTから感謝のコメントをいただくとともに，今後も本プロジェクトを通じて得られた知見を活用し，ベトナムにおけるサイバーセキュリティ対策の向上に継続して取り組みたいとの力強い声をいただいています．サイバー攻撃手法は日々高度化・巧妙化してきており，現状の対策では十分でなく，常にアップデートが必要です．VNCERTの継続的な啓発活動の実施を信じてやみません．本案件に限らず，日本のASEAN諸国への協力の一端として国策に貢献すべく，さまざまな分野で国際協力の取り組みを続けていきます．

（左から）勘場　宣男/ 野口　麻央里/
渡邉　紗知

今後とも国際協力活動を通じて，NTTグループならびに日本の技術の海外展開に取り組みたいと思います．

◆問い合わせ先
NTT東日本
デジタル革新本部 国際室
TEL　03-5359-8691
FAX　03-5359-1208
E-mail　kikaku_all@east.ntt.co.jp