

JPCERT/CC、APCERT と合同で

マルウェアが埋め込まれたサイトを遮断するインシデント対応ドリルを実施

有限責任中間法人 JPCERT コーディネーションセンター(東京都千代田区、代表理事 歌代 和正、以下 JPCERT/CC)は本日、APCERT(アジア太平洋コンピュータ緊急対応チーム)と APEC 経済地域で活動する CSIRT(コンピュータセキュリティインシデント対応チーム)が合同で実施した、サイバー攻撃への即時対応能力を確認するインシデント対応ドリルが完了したと発表しました。このインシデント対応ドリルは年に1度実施されており、今回で3度目となります。

近年、コンピュータセキュリティインシデントは、愉快犯から金銭目的へと変化し、ボットやフィッシングなどの国際的なセキュリティインシデントが増加しています。そのため、国内のセキュリティインシデント対応はもとより、国際的な連携確立の必要性が高まっています。

今回のドリルは国際間インシデントハンドリング能力の向上、参加国間及び参加国内での連携体制を確認することを目的とし、DDoS 攻撃を行う悪意あるプログラム(以下、マルウェア)が埋め込まれた Web サイトへの対応を想定して実施されました。

(※1)DDoS 攻撃:インターネットを通じた攻撃手法の一種で、ターゲットのサーバに対して複数のコンピュータから大量のデータを送信し、サーバの機能を停止させる手法。

今回のドリルには APEC 経済地域内の 13 カ国(日本、オーストラリア、ブルネイ、中国、香港、インド、韓国、ニュージーランド、マレーシア、シンガポール、タイ、台湾、ベトナム)から 15 チームが参加し、マルウェアが埋め込まれた Web サイトの停止、DDoS 攻撃の阻止アクションについて共同ドリルを行いました。APCERT に所属していない APEC TEL 参加国/地域からも 2 チームが招待され、同経済地域におけるレスポンス能力の確認を行ないました。ドリルは、インドからニュージーランドまで、8 時間 30 分もの時差が発生する幅広い地域で実施されました。CSIRT の他に各国の ISP や法執行機関が参加し、日本国内においては、財団法人日本データ通信協会 Telecom-ISAC Japan(東京都港区、会長 芳山 憲治(日本電気株式会社 顧問))と、社団法人日本インターネットプロバイダー協会(東京都渋谷区、会長 渡辺 武経)の協力を得て実施しました。

APCERT の代表グラハム イングラム(Graham Ingram)氏は、「今回で3回目となる APCERT 主催のインシデント対応ドリルには、APEC 加盟国の CSIRT 組織からも参加があり、非常に嬉しく思います。今回の合同ドリルによって、APCERT と APEC との緊密な関係を、あらためて確認することがで

きました。このドリルは APCERT が国際的なサイバー攻撃に対して、協力体制を確認する重要な機会です。また、確立された連絡体制や手順を改善することは、現在も脅威を与え続けているサイバー攻撃に対応する上で不可欠です。今回のドリルを通じて、手順の見直しと改善が可能となり、効果的、かつ効率的な協力体制の準備を整えることができます」と述べています。

今回実施されたインシデント対応ドリルの提案、およびドリルのシナリオは、韓国情報保護振興院 (Korea Information Security Agency) の一部門である KrCERT/CC が作成しました。KrcERT/CC の代表を務めるキム ウーハン (Woo-Han Kim) 氏は、「このドリルでは、国際的なインシデントに対応する枠組みの構築を目的としました。実際にインシデントが発生した際の対応には、各経済地域における CSIRT と ISP の緊密な協力、円滑なコミュニケーション、効率的な意思決定が必要不可欠になるでしょう」と述べています。

APCERT はアジア太平洋地域における CSIRT 間の連携、レスポンス、情報共有のレベル向上を目的とし、同経済地域で活動する主な CSIRT 組織によって設立されました。現在は、14 カ国から 19 の CSIRT 組織が参加しています。JPCERT/CC はこの APCERT の事務局を担当しています。APCERT に関する詳細は以下の URL をご参照下さい。 <http://www.apcert.org>

有限責任中間法人 JPCERT コーディネーションセンター (JPCERT/CC) に関する詳細は以下の URL をご参照下さい。 <http://www.jpcert.or.jp/>

財団法人日本データ通信協会 (Telecom-ISAC) に関する詳細は以下の URL をご参照下さい。 <https://www.telecom-isac.jp/>

社団法人日本インターネットプロバイダー協会 (JAIPA) に関する詳細は以下の URL をご参照下さい。 <http://www.jaipa.or.jp/>