サイバー攻撃解析協議会平成24年度活動成果のとりまとめ及び活動方針

平成25年4月19日
サイバー攻撃解析協議会

１．これまでの活動実績

（１）設立

独立行政法人情報通信研究機構（ＮＩＣＴ）、独立行政法人情報処理推進機構（ＩＰＡ）、一般財団法人日本データ通信協会テレコム・アイザック推進会議（ＩＳＡＣ）、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）の４団体は、サイバー攻撃の実態を把握し、その結果を関係省庁や重要インフラ事業者等に提供していくことを目的として、平成24年7月にサイバー攻撃解析協議会（以下、「協議会」という。）を設立した。

（２）ワーキンググループ（ＷＧ）における検討

第１回ＷＧ（平成24年7月31日）
各団体の保有するサイバー攻撃関連情報の詳細及び相互に情報共有することで解析の高度化に資する情報等について議論を行った。

第２回ＷＧ（平成24年9月6日）
情報提供にあたっての制約条件、各組織の役割分担、共同解析トライアルの実施方法及び解析結果の活用方策等について議論を行った。

第３回ＷＧ（平成24年10月18日）
共同解析トライアルの実施結果及び協議会における情報共有ルールについて議論を行った。

第４回ＷＧ（平成25年4月15日）
これまでの協議会の活動の総括及び平成25年度における協議会の活動方針について議論を行い、平成24年度活動成果のとりまとめ及び活動方針のＷＧ案を作成した。

※この他、各団体の通常の活動に関する相互理解や、最新のサイバー攻撃情報に関する意見交換を目的として、担当者レベルの非公式の勉強会を随時開催した。

（３）共同解析トライアルの実施

第１回（平成24年9月～10月）
〇情報提供元からの了解を得た標的型攻撃メール検体を各団体で共有し、各団体で解析した結果を第３回ＷＧで報告した。
〇トライアル実施の過程で、検体受け渡しの方法の改善、情報共有範囲などのルール整備の必要性が認識された。情報共有ルールは第３回ＷＧを経て、第１版を平成24年10月31日に策定した。検体受け渡しの方法については、平成25年度からの実施事項として、情報共有のためのシステム整備を検討することとなった。

第２回（平成24年10月～11月）
〇情報提供元からの了解を得た標的型攻撃メール検体を各団体で共有し、各団体で解析した結果を担当者レベルの勉強会で報告した。

○情報共有が定常化した際の各組織内の業務フロー等が今後の検討課題として認識された。

（４）とりまとめ

上記の活動実績及び検討結果を踏まえ、協議会の今後の活動方針を次の通り策定する。

２．サイバー攻撃解析協議会の活動方針

（１）目標

近年のサイバー攻撃の複雑化・巧妙化の中では、従来の個々の攻撃やマルウェア検体の解析のみでは、攻撃の全体像の把握と有効な対策が困難となっていることを踏まえ、攻撃に係る様々な情報を集約し、横断的な解析を実施することにより、解析の精度や適時性の向上を図る。その成果については、まずは、協議会に参加する各団体の活動の中で活かしていくとともに、内閣官房情報セキュリティセンター（ＮＩＳＣ）や重要インフラ事業者等への情報提供も順次図っていくこととする。

上記を達成するため、具体的には、次の目標を設定する。

ア　特定の標的に対し、様々な攻撃手法を組合せ、長期間に渡り執拗に攻撃を行う「標的型攻撃」に対しては、個々の攻撃で使用される攻撃手段や攻撃対象、攻撃の特徴等の情報を継続的に集約・解析していくことにより、個別の攻撃間の相関関係や、攻撃の意図・背景、関連性のある一連の攻撃（「攻撃キャンペーン」）の実態を解明していくことを目標とする。攻撃キャンペーンの把握により、各団体及び情報提供先機関の攻撃に対する予見能力、対処能力を高めることを目指す。

またこの活動を通じ、攻撃キャンペーンそのものの定義についても、協議会における議論の対象とする。

イ　情報窃取等を目的として、短期間のうち広範に行われる攻撃については、攻撃対象や攻撃手段の迅速な抽出の実現等を図り、個別の攻撃への対策能力の向上に活かしていくことを目標とする。

ウ　その他、各団体等の保有する広範な情報を相互に共有することにより、上記ア、イのサイバー攻撃との関係性や、現在表面化していないサイバー攻撃の予兆についても把握していくことを目標とする。

（２）実施事項

（１）の目標を達成するため、具体的に以下に取り組む。

ア　検体情報、統計情報、解析環境等の共有及び横断的な解析の実施

各団体は、以下の情報を可能な範囲で協議会に提供し、横断的な解析を行う。

○ＮＩＣＴ

・インシデント分析システム「nicter[1]」で検知したネットワーク上の攻撃活動等

[1] NICT ネットワークセキュリティ研究所で研究開発を進めている、インターネット上の脅威を迅速に把握し、有効な対策を導出するための複合的なシステム。

のログデータについて、後述する「協議会ポータルシステム（仮称）」（以下、「協議会ポータル」という。）に登録し、共有する。

〇ＩＰＡ

・ＩＰＡに届出のあった攻撃情報や、Ｊ－ＣＳＩＰ[2]で共有された情報について、情報提供元の許可を前提として、協議会ポータルに登録し、共有する。具体的には、年間数十件程度の検体情報の提供や、解析結果のインディケータ情報の登録を目指す。

〇JPCERT

・日本の窓口ＣＳＩＲＴとしての活動を通じて入手した攻撃関連情報及び解析結果のうち、協議会への共有が可能なものをシステムに登録し、共有する。さらに、攻撃キャンペーンの実態把握に資する攻撃の関連性情報や、解析時に作成したツール（デコードスクリプト等）の共有も図る。関連する検体としては、年間で数十検体を共有する。また、協議会ポータルの調整・運用を行う。

〇ＩＳＡＣ

・PRACTICEシステム[3] で検知したマルウェアの活動状況等の統計情報について、協議会ポータルに登録し、共有する。また、PRACTICEシステムに含まれるマルウェア検体の解析環境を、協議会ポータルを通じて各団体に公開するとともに、解析結果を登録し共有する。

イ　「協議会ポータル」の整備、活用推進

「協議会ポータル」を構築する。協議会ポータルでは、「マルウェア検体等の解析対象データの受け渡し」、「解析結果等の情報の保管」、「各団体が提供する情報や解析環境へのアクセス窓口」機能を提供する。

ウ　活動成果の各団体における活用

〇ＮＩＣＴでは、高度解析の結果をnicterシステムにおける分析に活用するとともに、「サイバー攻撃対策総合研究センター」（ＣＹＲＥＣ）における標的型攻撃等の新たなサイバー攻撃への実践的かつ革新的な対策技術の研究開発を加速する。

〇ＩＰＡでは、国民・企業への注意喚起や、Ｊ－ＣＳＩＰにおける共有情報の改善に活用していく。具体的には、Ｊ－ＣＳＩＰにおいては、メンバーへの解析結果の情報共有を高速化し、メンバーが類似攻撃を検知できるようにしていく。さらに、攻撃の経緯や連鎖の推測から、過去に遡って既に攻撃が行われたかどうかの検証や、今後の攻撃に対する対策等の実施までを行えるようにしていく。

〇ＪＰＣＥＲＴでは、高度解析を通じ、攻撃を広範囲かつ適時に把握することで、攻撃対象や攻撃キャンペーンの特定に努めるとともに、海外ＣＳＩＲＴとも、より精度の高い情報交換を行えるようになることで、被害拡大防止のための調整活

---

http://www.nict.go.jp/glossary/nicter.html

[2]サイバー情報共有イニシアティブ http://www.ipa.go.jp/security/J-CSIP/index.html

[3] 総務省「国際連携によるサイバー攻撃予知・即応技術の研究開発」（平成 23 年度～平成 27 年度）による実証実験を行うシステム。

動や早期警戒活動を的確に行えるようにしていく。また、高度解析の結果からインディケータを抽出し、早期警戒情報での活用を目指す。

〇ＩＳＡＣでは、他の協議会参加団体から提供を受けた情報を、サイバー攻撃の分析の高度化に役立てるとともに、必要に応じ、会員企業等に対して展開し、注意喚起等を行う。

エ　活動成果の外部連携

〇ＮＩＳＣ等に対して、協議会としての定期レポートを半年に１回及び注目すべき結果が得られた際に提供する。

〇総務省の「サイバー攻撃解析・防御モデル実践演習」事業（平成25年度予算施策）等との連携を図る。

オ　活動の見直し・改善

協議会では、高度解析の結果及び情報の活用状況を、定期的にフォローアップし、解析手法やシステム運用、情報提供・活用方法等の改善を図っていく。特に、協議会ポータルの試行期間とあわせて、同ポータルを用いた情報提供・共有、共有情報の活用範囲、活用成果の公表等のルール見直し及び策定に速やかに着手し、同ポータル本運用までに整備する。

３．今後の予定

〇会合の開催

・ＷＧは四半期に１回、親会は半年に１回を目途に開催する。担当者レベルの意見交換は月に１回程度継続して開催する。

〇協議会ポータル

・協議会ポータルの試行運用を５月頭までに開始する。

・協議会ポータルを通じた各団体からの情報提供を第１四半期中に開始する。

・第３四半期から協議会ポータルの本運用を開始する。併せて、同ポータルの本運用までに、情報の共有・活用等に関するルールの改訂を行う。

〇活動成果の外部連携

・平成25年9月を目標に、ＮＩＳＣ等に対する協議会としての第１回定期レポートをとりまとめる(別途、逐次、不定期レポートもとりまとめる)。

・協議会の成果の対外的な公表のルールを策定し、ルールに基づく公表を随時行う。

以　上