４．米国におけるフィッシングに係る連携体制

本章では、FBI、US Secret Service、FS/ISAC、APWG、ITAC を中心とした関係機関、民間部門との連携の枠組みについて、構築の経緯、機能、フィッシングへの取組みについて解説する。

４．１．FBI における連携体制

FBI では、NW3C (National White Collar Crime Center)、IC3（Internet Crime Complaint Center)、NTFCA（National Cyber-Forensics & Training Alliance）等を構築し、関係機関・団体等との連携を推進している。

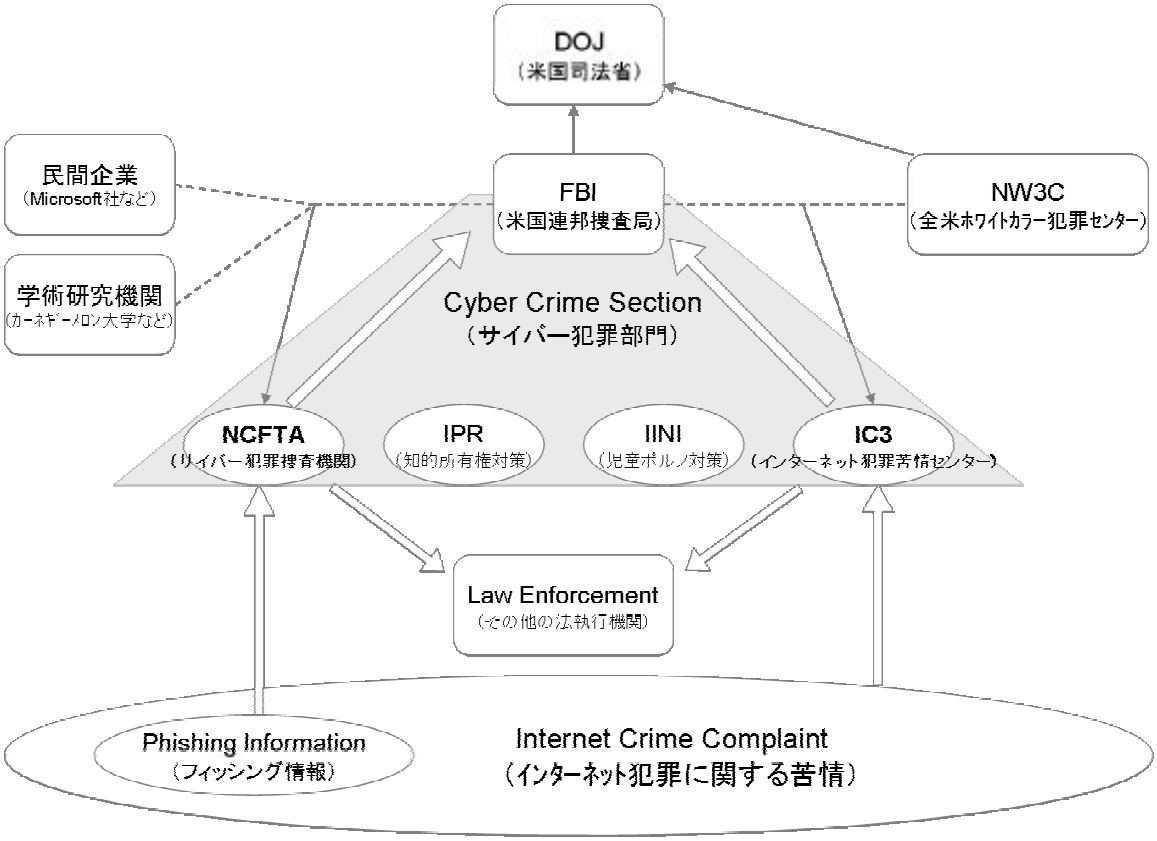

図 7　ＦＢＩと関係機関との連携

４.１.１　National White Collar Crime Center (NW3C)

①　構築の経緯

NW3C (National White Collar Crime Center ）は、DoJ、FBI 及び FTC の連携により 1980 年に設立された非営利組織である。

参加費用は無料であり、現在、1,500 以上の組織が参加している。

②　特徴

NW3C は、法執行機関のサイバー犯罪捜査の支援、ハイテク犯罪や経済犯罪の発生防止、調査、起訴などについて各州や地域法執行機関のサポートをしている。具体的には、サイバー犯罪捜査のサポートの他、サイバー犯罪や金融犯罪の調査に関する最新技術のトレーニングの実施、経済的インパクトのあるハイテク犯罪に関する論文の公開等を実施している。

また、DoJ がスポンサーとなり法執行機関や犯罪に関連する調査やトレーニングに特化した組織である IIR (Institute for Intergovernmental Research) と協力関係にある。

このほか、以下の組織が NW3C のサポーターとなっている

- Fraternal Order of Police (FOP)
- National Organization of Black Law Enforcement Executives (NOBLE)
- National Sheriffs' Association (NSA)
- International Association of Chiefs of Police (IACP)

４.１.２　Internet Crime Complaint Center (IC3)

①　構築の経緯

情報技術の高度化及びインターネット利用の拡大に伴い、法執行機関に対して、オンライン詐欺の報告が多くされるようになってきた。FBI では、これらに適切に対応するため、2000 年、NW3C と連携して、米国におけるインターネットに関する詐欺に関する一般からの報告受付窓口として、IFCC（インターネッ

ト詐欺苦情センター）を開設した。

その後、寄せられる報告が詐欺のみならず、その他の犯罪と直結するものが多く含まれるようになったことから、当該組織において詐欺に限らず多様なインターネット犯罪に関する報告を受け付けることとし、2003 年、組織の名称を IC3 (Internet Crime Complaint Center：インターネット犯罪苦情センター) と変更した。

② 体制及び活動

IC3 は、FBI の Cyber Division 内に所在している。また、IC3 には 6 人の FBI 捜査官が常駐しているほか、30 人から 40 人のインターネット犯罪捜査のスペシャリストがいる。全体の人数は、2003 年の時点では 62 人であった。また、IC3 の職員は、前述のとおり DoJ から法的な側面でのトレーニングを受けている。

また、IC3 においては、次の活動を実施している。

- すべてのインターネットに係る犯罪に関して、広く一般からの受付窓口となり、情報を蓄積し、犯罪の立証に必要な分析を実施する。
- FBI のトップページからインターネットに係る被害の報告のリンクが直接張られているなど、被害者に対して被害報告がしやすい環境を積極的に提供する。
- 法執行機関に対し、インターネットに係る犯罪に関する情報を提供する。

③ フィッシング対策への取組み

IC3 では、フィッシングに限らずインターネットに係るすべての犯罪について、被害者が直接報告する形で受け付けている。このため、フィッシングに関する報告は、インターネットに係る被害報告のひとつとして、受け付けられる。IC3 を介して法執行機関に報告ができる仕組みは、フィッシング被害への迅速な対応と被害拡大の抑制に貢献している。また、法執行機関にとっても、犯罪に結びつかない多くの紛らわしい情報が IC3 でフィルターされることにより、

捜査の効率化が図られている。

４.１.３ National Cyber-Forensics & Training Alliance (NCFTA)

① 構築の経緯

米国において、地方、州、及び連邦の法執行機関が連携したハイテク犯罪対応のための組織 HTCTF (Pittsburgh High Tech Crimes Task Force ）が設立され、2002 年に、FBI、NW3C、カーネギーメロン大学、ウェストバージニア大学などが参加して、当該連携体制を発展させたものが現在の NCFTA (National Cyber-Forensics & Training Alliance ）となっている。

※ ３．５節も参照。

② 活動

NCFTA では、次の活動を行っている。

- 法執行機関、民間部門、学術研究機関の参加により、サイバー犯罪対策の連携体制がとられている。
- NCFTA の活動のための人的リソースについては大学や IT 企業から、資材関連では、IT 企業から支援を受けている。
- インターネットに係る捜査のための解析、対応体制の構築、技術的なシミュレーションによるサイバー犯罪のモデリング解析、及び高いレベルの教育訓練を提供する。
- さまざまな分野の法執行機関に対する支援を行う。
- ウイルス検体を、契約している企業から入手する。
- Digital PhishNet のホームページ･サイト（http://www.digitalphishnet.org/）の運営により、一般の方からの情報提供を受け付けるとともに、取りまとめた情報を関係機関へ提供する。

③　フィッシング対策への取組み

NCFTA は、Digital PhishNet のサイト運営を通して、フィッシングに関するさまざまな情報を、あらかじめ契約をした特定の組織や個人から入手し、サイバー犯罪の捜査（forensic）に活用される。最近では、毎日 100 件程のフィッシングサイトの情報が報告されている。

このほか、スパマー（悪質なメール送信者）のデータベースも構築されている。ここで分析されたさまざまな情報は、法執行機関に提供され、捜査への支援を行っている。また、フィッシングのみならず、サイバー犯罪に関するさまざまな情報を入手しており、民間会社や学術機関からの支援によるところも大きい。

４.１.４　Digital PhishNet

①　設立の経緯

フィッシングの件数増加が著しく、フィッシングに関する情報共有の仕組みの必要性が高まったため、2004 年 12 月に民間企業、銀行等の金融事業者、電子商取引企業及び法執行機関が連携してフィッシングに対応するために Digital PhishNet が設立された。

運営は NCFTA が主体となって行っており、ウェブサイト上で参加メンバーからのフィッシングに関する報告の受付け、サイトの運用やデータの管理などを行っている。

Digital PhishNet には、マイクロソフトやベリサインなどの電子商取引サイトや IT 企業、AOL や EarthLink などの大手 ISP、米国の上位 10 銀行のうちの 9 行、法執行機関からは Secret Service と FTC、U.S. Postal Inspection Service、FBI がメンバーとして参加している。

②　フィッシング対策の取組み

NCFTA では、メンバーから Digital PhishNet に報告されたフィッシング情報の分析や、情報のフィードバック、データベースの運営を行っている。Digital

PhishNet に報告されるフィッシングサイト件数は 1 日 100 件以上に上り、これらの蓄積されているデータについては、メンバーが Digital PhishNet のウェブサイトにログインして検索などを行える。

※　NCFTA については、４．１．３参照

４.２. Electronic Crimes Task Force (ECTF)

① 構築の経緯

USSS では、金融システムおける偽造通貨対策のための金融関連の犯罪捜査を担当しているが、通信技術の高度化と、金融システムにおけるＩＴ技術の利用が進むに従って、新しい電子的な金融犯罪が現れ、USSS のみでの対応から官民連携した体制を構築する必要性が生まれた。このため、2000 年、ニューヨークにおいて、USSS は、民間企業、学術機関等と連携して ECTF (Electronic Crimes Task Force) を構築することによりサイバー犯罪に関する取組みを強化している。現在、50 の法執行機関、200 の民間企業、12 の学術機関が参加している。この取組みは成果をあげており、ニューヨークモデル（NYECTF）と呼ばれるに至っている。

その後、2001 年に制定された PATRIOT 法（米国愛国者法）の施行などにより、USSS のコンピュータ関連の犯罪捜査に対する期待が高まり、全米にこのニューヨークモデル（NYECTF）の展開が始まった。

現在、ECTF が１３カ所に設置されている。

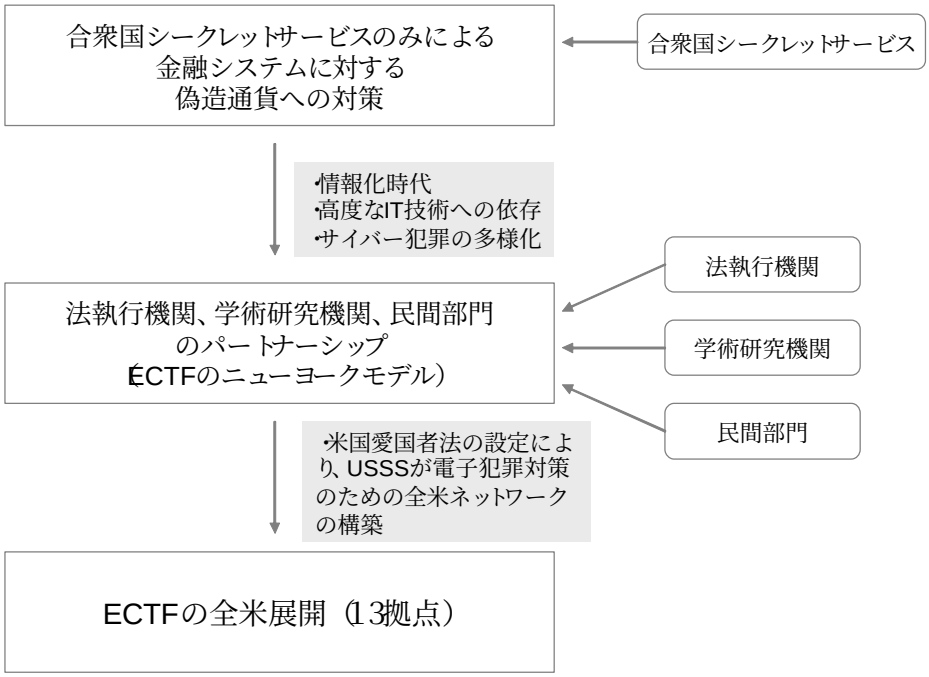

図 8　ECTF の取組みの経緯

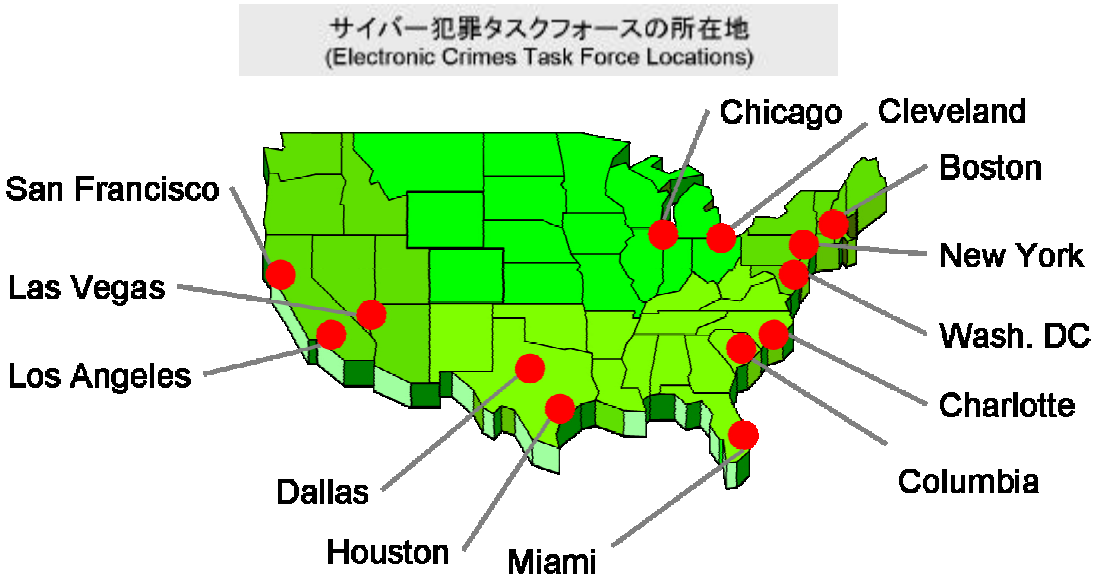

図 9　サイバー犯罪タスクフォースの所在地

② フィッシング対策の取組み

ETCF におけるフィッシング情報の取扱いの流れは次のとおりとなっている。

- 情報提供者は、最寄りの ETCF に対して、電子メール、電話、及び FAX にて、フィッシング情報を提供する。
- 法執行機関、学術研究機関、民間部門が共同で、報告された情報を分析する。
- 分析された情報等を法執行機関に対し情報提供する。

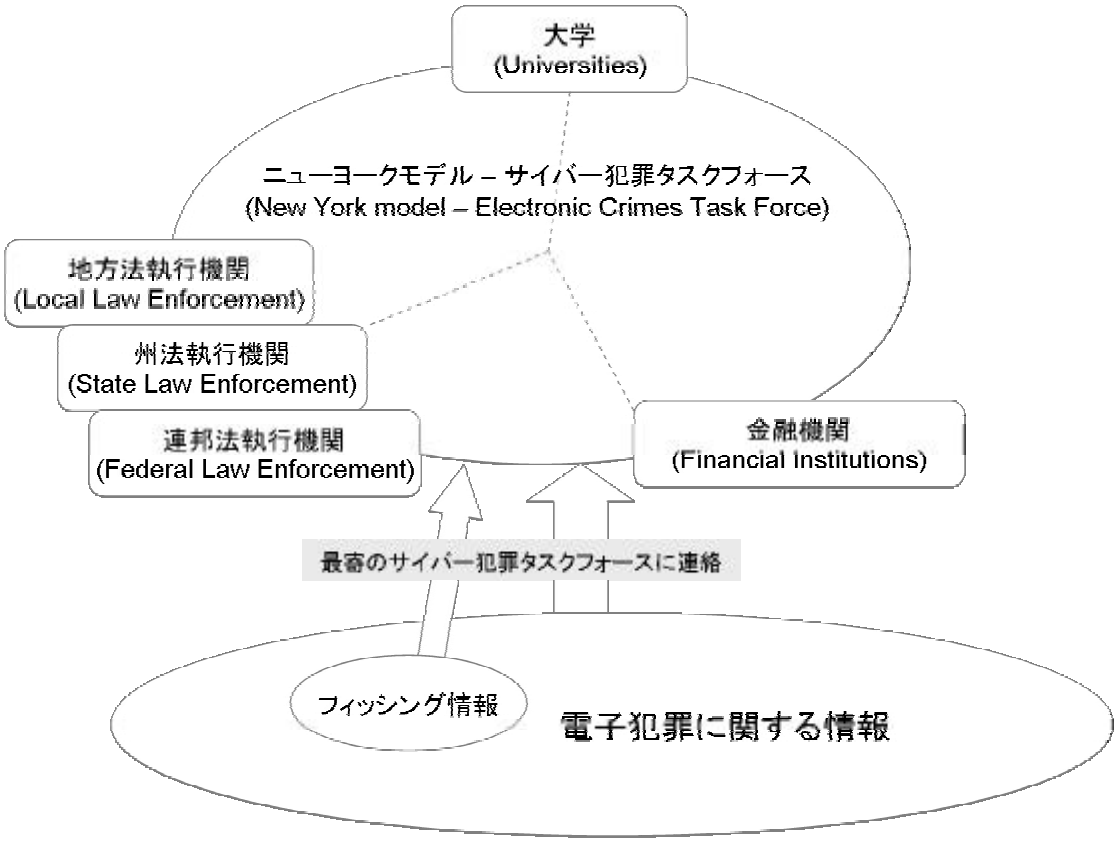

図 10　ECTF における関係機関との連携

４．３．FS/ISAC

①　設立経緯

1998 年に、米国の重要インフラを保護するために物理的及びサイバー上の脅威や脆弱性に関する情報を官民セクターが共有するように指示した大統領決定指令（Presidential Decision Directive）の発令により、金融業界において FS/ISAC (Financial Service / Information sharing and analysis Center ）が発足した。2003 年 12 月、政府は FS/ISAC に対して、米国内の金融サービス機関における物理的及びサイバー上のセキュリティ意識を強化させるため、200 万ドルの資金を提供した。これを受けて、FS/ISAC は、重要な警告情報を関係者にほぼ同時に発信し、かつ、ユーザ認証及び受信確認機能を備えた情報伝達システムを構築した。

②　連携体制

FS/ISAC において、次の連携活動を推進している。

- 金融サービス機関やセキュリティ団体、連邦法執機関などから、信頼性がありタイムリーなセキュリティ情報を常時収集し、配信している。
- 金融サービス機関から（に）法執行機関に対して（から）、インシデント情報や脆弱性の情報に関する情報が送られてきた場合は、専門家が検証、分析するとともに、推奨ソリューションを特定し、データベースに登録したのち、配信している。

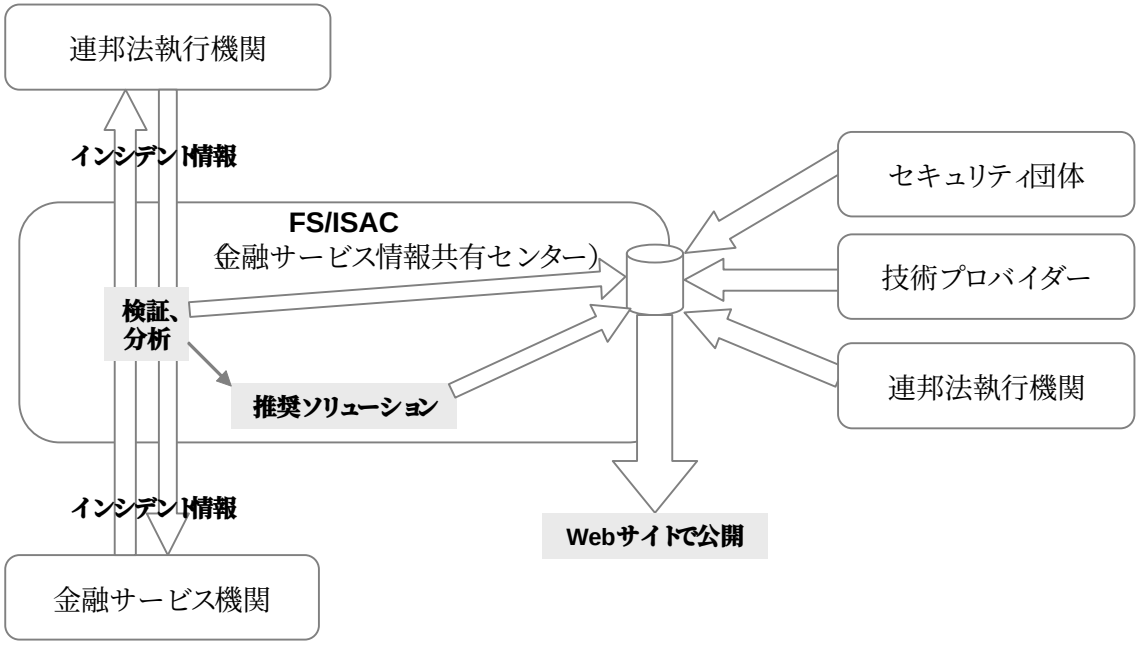

図 11　FS/ISAC における関係機関との連携

③　フィッシング対策への取組み

FS/ISAC **における、フィッシング情報の取扱いについては、個人情報流出のひとつのインシデントとして取扱っており、脅威情報の迅速な公開に努めている。**FS/ISAC **には、セキュリティ団体、技術プロバイダー、連邦法執行機関からインシデント情報が提供される仕組みが存在している。金融サービス業界と連邦法執行機関とは** FS/ISAC **を通じてインシデント情報を共有しており、その中で、情報の検証及び分析が実施され、推奨される対策が提示される。**

４.４. Anti-Phishing Working Group (APWG)

① 設立の経緯

APWG (Anti-Phishing Working Group) は、2003 年 11 月、内外の関係企業や法執行機関をメンバーとして、フィッシング対策を目的して結成された。設立の目的は、フィッシング、ファーミング、詐称電子メールなどが原因となって発生するオンライン詐欺や個人情報窃盗の被害を無くすための活動を行うとともに、法執行機関向けの情報提供を行うことである。現在は、2000 人以上の個人、1300 以上の企業及び国際機関、米国の大手銀行８社、米国の大手 ISP４社、100 以上のテクノロジーベンダー、そして、国際的な法執行機関がメンバーとなっている。

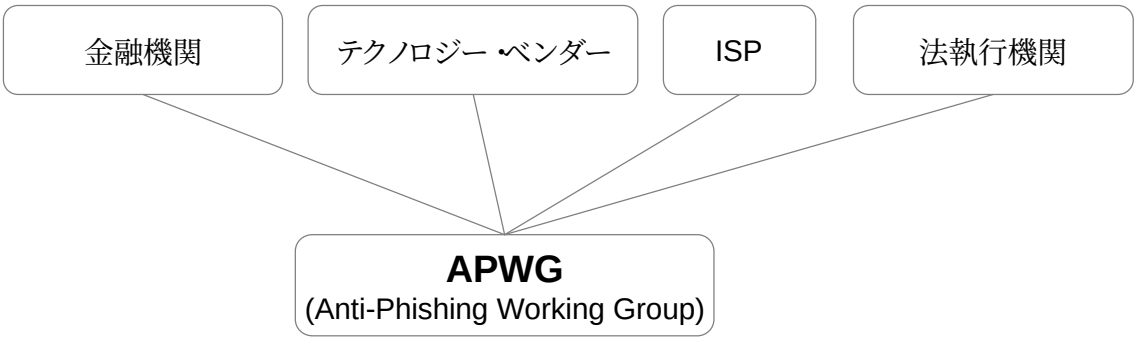

図 12　ＡＰＷＧの参加メンバー

② 活動

APWG では、次の活動を行っている。

- フィッシング対策のベストプラクティスの共有、教育、脅威予測、フィッシング関連情報の一元管理、情報配信及び警告、被害の定量化、解決策など。
- 法執行機関との連携。

③ フィッシング対策への取組み

APWG のメンバー及び一般の APWG サイト閲覧者などから、APWG に対してフィッシングに関する情報が報告され、APWG において提供された情報の分析及び評価を行った後、これらのフィッシングに関する情報や有効な対策をメンバーに積極的に公開し、被害の拡大を防止している。

また、7 つの Working Group を設置し、データの蓄積や教育、法執行機関との連携活動などを行っているほか、参加者同士が議論するためのフォーラムの提供、フィッシングの報告を受け付ける窓口の設置等を行っている。

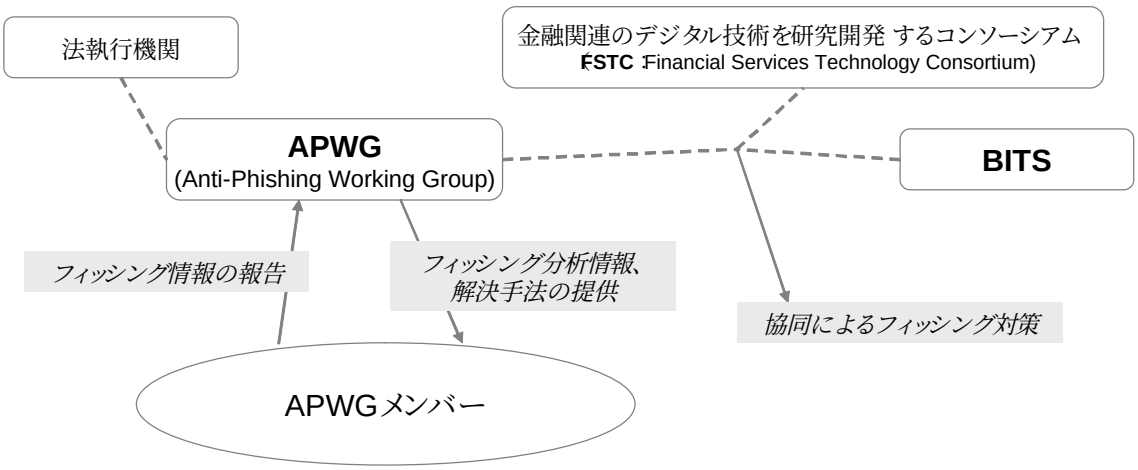

図 13　ＡＰＷＧにおける関係機関の連携

４.５. Identity Theft Assistance Center (ITAC)

① 設立経緯

2003 年、大手金融機関が参加する非営利団体 Financial Service Roundtable と BITS が連携して、ITAC (Identity Theft Assistance Center : 個人情報窃盗対策支援センター) が設立された。ITAC には、現在、50 近くの銀行等の金融機関が参加している。

ITAC の目的は、①被害にあった顧客へのサポート、②政府の法執行機関との情報共有と告訴などの支援、③金融サービス機関における個人情報窃盗の発見と対策の支援である。

※BITS については、３．６節参照。

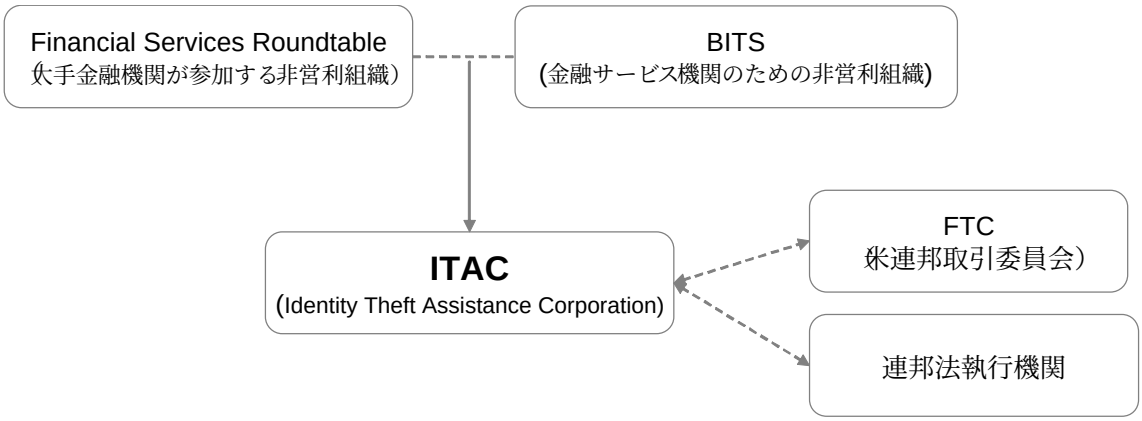

図 14　ITAC の設立経緯と関係機関との連携

② 活動

ITAC では、次の活動を行っている。

- 金融に関する個人情報窃盗の事件において、被害となった顧客に対して、円滑かつ速やかな解決ができるよう支援をしている。
- 法執行機関に対しては、FTC が管理する一般消費者からの苦情等のデータ

ベース（Consumer Sentinel）への情報提供を通じて、活動を支援している。

- 金融機関に対し、顧客が個人情報窃盗の被害にあった際の問い合わせに対応し、フィッシングサイトを閉鎖させるために必要な連絡先情報の蓄積、提供などの支援を行う。
- ITAC の支援サービスを利用する際の料金は、ITAC のメンバーであれば無料である。ITAC メンバー以外の利用はできないが、この場合、適切な相談窓口の情報が提供される。
- ITAC に報告される被害には、フィッシング被害のみではなく、個人情報窃盗に関する被害すべてが含まれる。

③ フィッシング対策への取組み

ITAC のメンバーとなっている金融機関に対し、フィッシングの被害にあった人又はそのおそれがある人から被害の報告や相談がされると、その情報はすぐに ITAC に提供され、速やかに分析及び対策に必要な支援が、当該金融機関に対してなされる。これと同時に ITAC メンバーである他の金融機関にも、必要な情報が提供されるとともに、FTC のデータベースに登録され、法執行機関と情報が共有される。

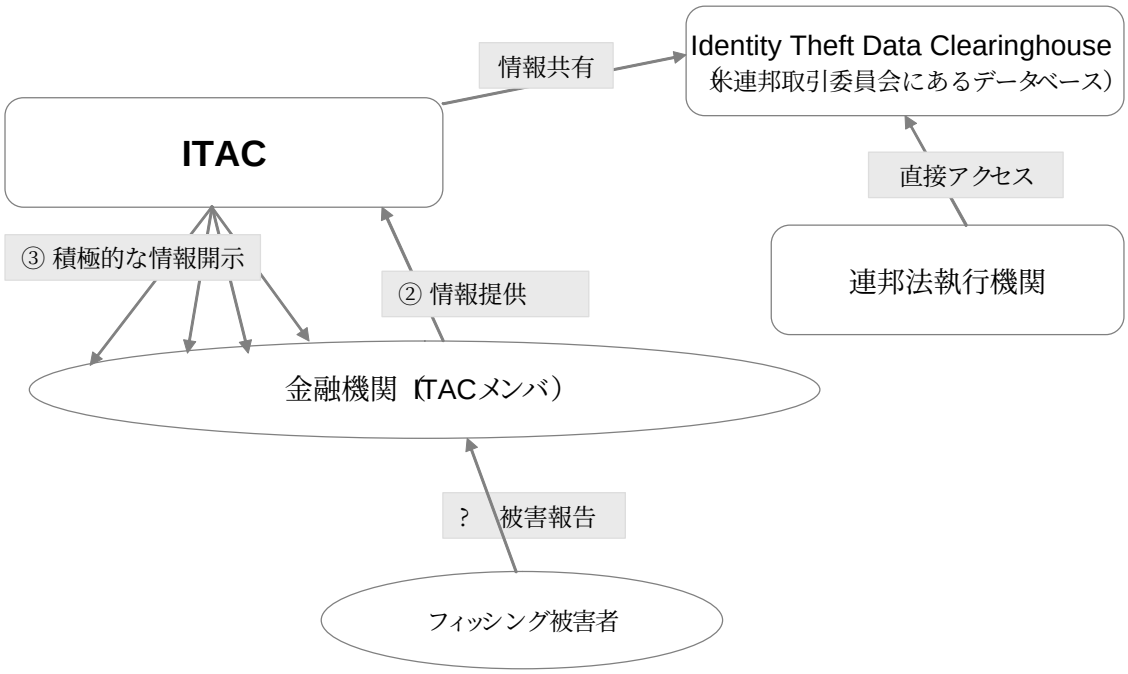

図 15　ITAC における関係機関との連携

５．フィッシングに係る連携体制の在り方

今回の調査により、米国では、法執行機関、民間団体、学術研究機関等がさまざまな形で連携体制を構築し、フィッシングに関する情報共有等の取組みが進められている状況が分かった。

こうした米国の取組み状況を踏まえ、フィッシング対策に係る連携体制の在り方としては、次の３つの視点が考えられる。

① リアルタイムな情報共有環境

サイバー犯罪においては、被害が急速に拡大する、手口が容易に模倣されるなどの特徴を有しており、特に昨今問題となっているフィッシングにおいてはこれが顕著となっている。したがって、こうした犯罪の対策には、法執行機関、関係業界、関係団体等において情報を迅速に共有し、連携して対応することが有効である。

米国では、フィッシング等に関する情報共有を推進するため、FBI や USSS から CERT/CC へのリエゾンの配置、FTC による法執行機関がリアルタイムに情報共有するためのデータベースの構築等が進められている。

② 法執行機関、民間部門、学術研究機関との協力体制

サイバー犯罪の手口が技術的に高度化しており、法執行機関、民間部門、学術研究機関が連携してこのような高度な技術を利用した犯罪に対応できる体制を構築することが有効である。また、効果的な連携体制の構築、運用が行われるよう、適切な共同トレーニングを行うことも有用である。

米国では、法執行機関において、NCFTA、ECTF などの民間部門、学術研究機関との協力体制を構築し、サイバー犯罪への的確な対応を推進している。また、FS/ISAC、APWG、ITAC などの民間部門を中心とした取組みにおいても、法執行機関との連携・情報共有が進められている。

③ 窓口機能の強化

サイバー犯罪は、その犯罪行為の容易性やインターネット利用者の増大により、被害が拡大しやすく、APWG がとりまとめているフィッシング件数にも見られるように、関係機関への被害報告が増加傾向にある。このため、被害の報告や相談、情報提供などを受け付ける窓口業務の負担増大により、各機関のリソースの飽和、他の業務への支障等が懸念される。また、フィッシング等に関する情報入手に際しては、一般のインターネット利用者からの情報提供が必要不可欠な状況であり、このための窓口の有効活用が必要である。

このような状況下において、米国では、IC3、APWG、ITAC の取組みに見られるように、中間的な組織における窓口業務が、重要な役割を担っている。また、FTC の取組みに見られるようなデータベース等による受け付けた情報の関係機関等における共有も進んでおり、窓口機能について関係機関が連携した強化が進められている。

６．おわりに

近年、インターネットを使用したサイバー犯罪が増加している背景としては、IT 技術の高度化や、IT 技術を利用した様々なサービスが実社会へ浸透していっていることがある。このような状況において、多様かつ高度なサイバー犯罪に対しては、単独組織で対応するのではなく、さまざまな組織が連携して対応することが効果的である。

米国では、法執行機関をはじめ、各組織が連携したサイバー犯罪への対応が進められている。例えば FBI では、地方、州、連邦の法執行機関及び学術研究機関が連携した NCFTA を構築し、USSS ではニューヨークモデルと言われる ECTF の構築が始まり、いずれも有用な成果を挙げている。これらの成功事例に共通している事項は、複数の組織から人的資源を出し合い、リソースを共有することで強固な体制を構築し、情報共有や連携体制を強めていることである。具体的には、被害者が直接報告を行えるような報告受付窓口をウェブサイトの公開、情報共有・連携を目的としたデータベースの構築、IT 技術のスペシャリストとして位置付けられる外部組織との密な関係を築くことなどがある。

米国においてこのような体制が構築されている背景としては、インターネットを取り巻く状況の急激な変化に伴うサイバー犯罪の多様化、高度化に柔軟に対応するために、必然的に進展してきたものであると考えられる。

こうした米国の取組みを踏まえ、我が国においてもフィッシングへの対応体制を各組織の既存機能を活かしつつ、フィッシング対策に係る組織間での情報連絡・連携体制の構築、人的資源の共有等を進めていく必要がある。