フィッシングに関する調査研究

報告書

平成１８年３月

財団法人　社会安全研究財団

目　次

1. 報告書の概要 3

1.1. はじめに 3

1.2. 調査方法と報告書の構成 4

2. フィッシングの現状 6

2.1. フィッシングとは 6

2.2. 海外の被害状況 6

2.3. 国内の被害状況 7

2.4. 警察における検挙状況等 7

2.5. JPCERT/CC における対応状況 9

2.6. 今後の動向 11

3. 米国の各組織の概要 13

3.1. Department of Justice (DoJ) 13

3.2. Federal Bureau of Investigation (FBI) 14

3.3. U.S. Department of Homeland Security (DHS) 16

3.4. U.S. Secret Service (USSS) 16

3.5. National Cyber-Forensics and Training Alliance (NCFTA) 18

3.6. BITS 19

3.7. Federal Trade Commissions (FTC) 20

4. 米国におけるフィッシングに係る連携体制 22

4.1. FBI における連携体制 22

4.1.1 National White Collar Crime Center (NW3C) 23

4.1.2 Internet Crime Complaint Center (IC3) 23

4.1.3 National Cyber-Forensics & Training Alliance (NCFTA) 25

4.1.4 Digital PhishNet 26
4.2. Electronic Crimes Task Force (ECTF) 27
4.3. FS/ISAC 30
4.4. Anti-Phishing Working Group (APWG) 32
4.5. Identity Theft Assistance Center (ITAC) 34
5. フィッシングに係る連携体制の在り方 37
6. おわりに 39
○ 参考資料

１．報告書の概要

１.１．はじめに

フィッシング（Phishing）とは、銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするように仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ID・パスワード等）を入力させるなどして個人の金融情報を不正に入手する行為である。

米国におけるサイバー犯罪の現状を見てみると、米 FTC に報告されたインターネットに関係する詐欺の被害件数は、2005 年の一年間に 196,503 件であり、その被害額は約 3 億 4 千万ドルとなっている。（出展：米 FTC 報告書「Consumer Fraud and Identity Theft Complaint Data January - December 2005」）

こうした状況の中、米国では、サイバー犯罪に関する法制度の整備が進められており、フィッシングについては、個人情報窃盗（ID Theft）という犯罪として処罰することができるようになっている。

また、米国では政府、法執行機関、民間企業等が協力し、サイバー犯罪への対応を行う体制整備も進められている。特に、法執行機関が民間企業と積極的に連携して問題の解決のために動いている。例えば、FBI が主体となって立ち上げた NCFTA という組織では、法執行機関や民間企業だけでなく学術研究機関の協力も得て三位一体となって情報収集・分析・事案対処を行い、その結果を法執行機関と共有している。また、金融業界においては、業界内での情報交換のための組織として FS/ISAC や BITS を構築しており、金融業界での情報交換ばかりでなく、他業界の事業者や法執行機関との連携の役割も担っている。さらに、サイバー犯罪の被害にあった顧客を支援するための組織として ITAC を立ち上げ、50 近くの金融機関が参加し、法執行機関との連携も行っている。

本報告書は、このような米国の各組織間の連携体制を中心とした取組み状況を調査したものであり、我が国の法執行機関、関係機関・団体、民間企業、研究機関等において、フィッシング対策のための体制整備等を進める上での参考

資料として活用されることを期待している。

本報告書が、我が国におけるフィッシング対策のための体制整備、関係者相互の連携強化の一助となれば幸いである。

１.２. 調査方法と報告書の構成

本報告書の作成にあたり、米国の現状の把握には、米国の各関連組織を訪問し、担当者からのヒアリングによって得られた内容を中心としてまとめている。

また、本報告書の構成は、第２章において国内外のフィッシングの現状についてまとめ、第３章では米国の各組織の概要とフィッシングに対する取組み状況等についてまとめている。また、第４章ではフィッシングに関する各組織間の連携体制についてまとめ、第６章では米国の取組み状況をふまえ、フィッシングに対する連携体制の在り方について考察している。

なお、本調査でヒアリングを行ったのは、以下の組織・担当者である。

組織名	United States Department of Justice (DoJ)
部署	Cyber Crime Division
担当者名	Andrew Levchuck John T. Lynch Jr. Anthony V. Teelucksingh

組織名	Federal Bureau of Investigation (FBI)
部署	Cyber Division
担当者名	Thomas Grasso

組織名	U.S. Department of Homeland Security (DHS)
部署	US-CERT
担当者名	Reggie McKinney

組織名	United States Secret Service (USSS)
部署	―
担当者名	Thomas

組織名	National Cyber-Forensics and Training Alliance (NCFTA)
部署	―
担当者名	Daniel J. Larkin David Bonasso Doug Brozick

組織名	Financial Services Roundtable
部署	BITS
担当者名	John W. Carlson Heather Wyson

２．フィッシングの現状

２.１．フィッシングとは

フィッシング（Phishing）とは、銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするように仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ID・パスワード等）を入力させるなどして個人の金融情報を不正に入手する行為である。

フィッシングの目的は、入手した個人の金融情報等をインターネット・バンキング、インターネット・ショッピング、偽造カード等に悪用し、不正アクセスや詐欺等の犯罪を行うことである。

フィッシングは、海外を中心に大きな被害が発生しており、法執行機関、金融機関等における対策が急務となっている。

２.２．海外の被害状況

フィッシングは平成 15 年頃より欧米を中心として被害が拡大し、米国の民間調査会社（Gartner 社[1]）では、同年中に約 170 万人がフィッシングサイトに情報を入力し、約 12 億ドルの損害が生じたと推計している。

米国では、同年、関係業界や法執行機関が参加する APWG(Anti-Phishing Working Group、30 頁参照)を設立し、フィッシングに関する情報共有やホームページ上での情報提供等の各種対策が進められているが、フィッシングは依然として数多く発生しており、17 年中に APWG に寄せられたフィッシングに関する情報提供は約 17 万 3 千件に上っている。

---

[1] Gartner 社ホームページ：http://www.gartner.com/

２.３．国内の被害状況

我が国においては、平成 15 年 12 月に国内の電気通信事業者を騙ったフィッシングが発生したほか、16 年後半にも国内の通信事業者、クレジットカード会社等を騙ったフィッシングが散発的に見られた。

また、17 年 2 月に国内クレジットカード会社がフィッシングにより個人情報を窃取される被害が発生し、これをもとに偽造クレジットカードが作成され、キャッシングにより約 150 万円が不正に引き出される被害が発生したと発表した。そして、同年 3 月には、大手銀行のフィッシングサイトが立ち上げられ、これに誘導するフィッシングメールが大量に送付される事案が発生している。

このほか、APWG の資料によれば、17 年 12 月中に発見されたフィッシングサイトのうち 3.33%が日本国内のサーバ上にあったと報告されており、我が国においてもフィッシングの脅威が継続している。

２.４．警察における検挙状況等

我が国では、平成 16 年 12 月、各都道府県警察において「フィッシング 110 番」を設置して情報収集・相談対応を強化し、捜査及び防犯の両面における対策を強化している。（参考資料２，３参照）

具体的には、フィッシング事案が発生したときの被害防止のための注意喚起、国際的な法執行機関間の連絡網（24 時間コンタクトポイント）を通じてフィッシングサイトへの個別の対応依頼を行うほか、フィッシング実行犯の捜査・検挙を行っている。

また、警察庁では、平成 17 年６月、インターネット上で相談を受け付け、基本的な対応策等を自動的に回答する「インターネット安全・安心相談システム」を開設し、フィッシング等に関する被害防止策の周知や情報提供の受付を行っている。

【検挙事例】

○　会社員の男(42)は、平成 17 年２月、インターネットサービス会社が会員に付与した識別符号を不正に入手する目的で、同社が著作権を有するホームページに酷似した「ログイン画面」をインターネット上に公開し、これを本物の「ログイン画面」であると誤信した者が入力した識別符号を不正に入手するとともに、これらの識別符号を使用して不正アクセス行為を行った。平成 17 年６月、著作権法違反及び不正アクセス禁止法違反で検挙した（警視庁）。

○　無職の男(25)は、平成 17 年 3 月から平成 18 年 1 月にかけて、インターネット・オークション運営会社を装ったメールを約 5,500 件送信して、受信者を偽のサイトであるフィッシングサイトに誘導し、同サイトを通じて約 500 件の ID・パスワードを入手した。このＩＤ・パスワードを用い、インターネット・オークションにおいて他人になりすまし、代金を支払う意思なく商品を落札し、当該商品を搾取した。平成 18 年１月、詐欺及び不正アクセス禁止法違反で検挙した（警視庁）。

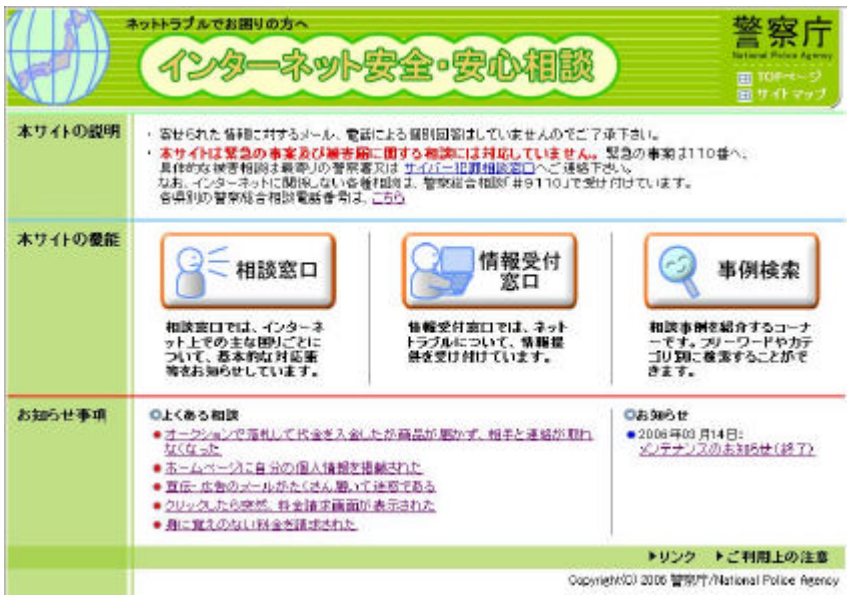

図 1　インターネット安全・安心相談システム（http://www.cybersafety.go.jp/）

２．５．JPCERT/CC における対応状況

有限責任中間法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）は、国内外の組織や個人からフィッシングサイトに関する報告を受け付けている。JPCERT/CC では、報告されたフィッシングサイトについて、サイトの管理者への連絡を行いサイトの停止を依頼する調整を行っている。その際、JPCERT/CC は、協力関係にある海外のインシデント対応組織等に連絡を行い、世界各国のサイト管理者へ情報を連絡している。2005 年 1 月から、2006 年 3 月までに JPCERT/CC が受け付けたフィッシングの総件数は 359 件であり、全てのフィッシングサイトについて停止を確認している。

表　JPCERT/CC への Phishing 関連の報告件数及び内訳

	2005 年 1 月～12 月	2006 年 1 月～2 月
総数	301 件	58 件
報告者別内訳		
CSIRT	33 件	5 件
Security Service 関連会社	84 件	13 件
銀行・カード会社	70 件	18 件
E コマース	101 件	17 件
その他	13 件	5 件
被害サイト別内訳		
国内 ISP/xSP	101 件	20 件
国内企業	144 件	22 件
国内教育機関	16 件	8 件
海外サイト	30 件	6 件
その他	10 件	2 件

２．６．今後の動向

フィッシング等の深刻な状況を踏まえ、銀行等の金融機関では新たにトークン認証を導入するなどのインターネット上での金融手続きの安全対策への取組みが急速に進められているほか、法執行機関における被疑者の検挙、民間団体による広報啓発等の様々な対策が推進されている。

しかしながら、APWG が公表しているフィッシングサイト数の推移に関する資料によると、平成 17 年 12 月中には前年同期の４倍以上の 7,197 サイトが把握されており、フィッシングの猛威は未だ収束していない様子が伺える。

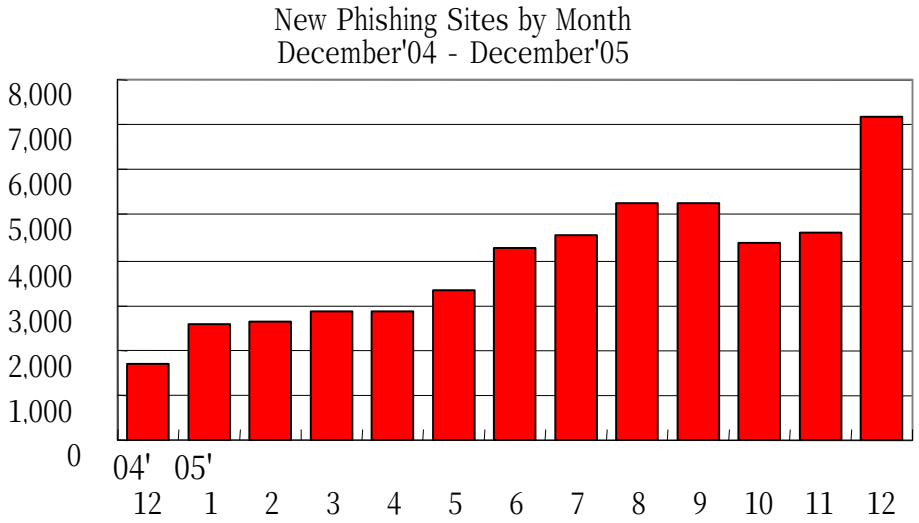

図 2　フィッシングサイト報告受理件数[2]

また、平成１７年中のサイバー犯罪検挙状況をみると、ネットワークを利用した詐欺の検挙件数が前年の約 2.6 倍に急増し、また、不正アクセス行為の発生状況等をみると、不正アクセス行為の動機として「不正に金を得るため」が増えている。（参考資料４、５参照）

[2] 出典：APWG ホームページ（http://www.antiphishing.org/）

このように、インターネット上における金銭の不正取得目的の活動が顕著となっており、フィッシングの脅威は今後も厳しい状況が予想される。

３．米国の各組織の概要

本章ではフィッシングに関する活動を行っている米国内組織･プロジェクト等の役割について、訪問によるヒアリングにより得られた内容を中心として説明する。

３.１． Department of Justice (DoJ)

DoJ (Department of Justice : 米司法省) の任務は、米国における法の執行、および国内・海外問わず潜在する脅威に対して公共の安全を確保すること、犯罪の防止と統制をすること、犯罪者を罰すること、全米国民のために正義と公平さを保つことである。フィッシングへの対応については、Criminal Division が担当している。

フィッシングの法的適用については、従前、金銭的被害の部分を捉えて「詐欺」として扱っていたが、フィッシング関連の法律が整備されてきた現在では、フィッシング行為自体を「個人情報窃盗」という犯罪として扱っている。

DoJ では、直接犯罪捜査を行わないが、フィッシングに関する各捜査機関における円滑で適正な捜査を推進するため、FBI、U.S. Secret Service、IC3 の捜査員に対する法律等に関するトレーニングを行っている。具体的には、フィッシングが犯罪に該当するケースや、そうでないケースの紹介、適用される法律、捜査が可能なケースとはどのような場合かといった内容である。そのほか、FBI、US Secret Service と週に一度の定期ミーティングを実施している。

また、米国外に関わる事件を扱う場合には、基本的には、FBI や US Secret Service のコンタクトポイントを利用しているが、海外との連携においては非公式な形での関係構築も重視している。フィッシングへの対応については、このほかに FTC（Federal Trade Commission：米連邦取引委員会）とも連携している。

DoJ は、民間企業との協力関係の構築に積極的である。その理由としては、

政府部門のみではリソース不足であるため、民間部門と協力して効率的な情報収集を行うためである。

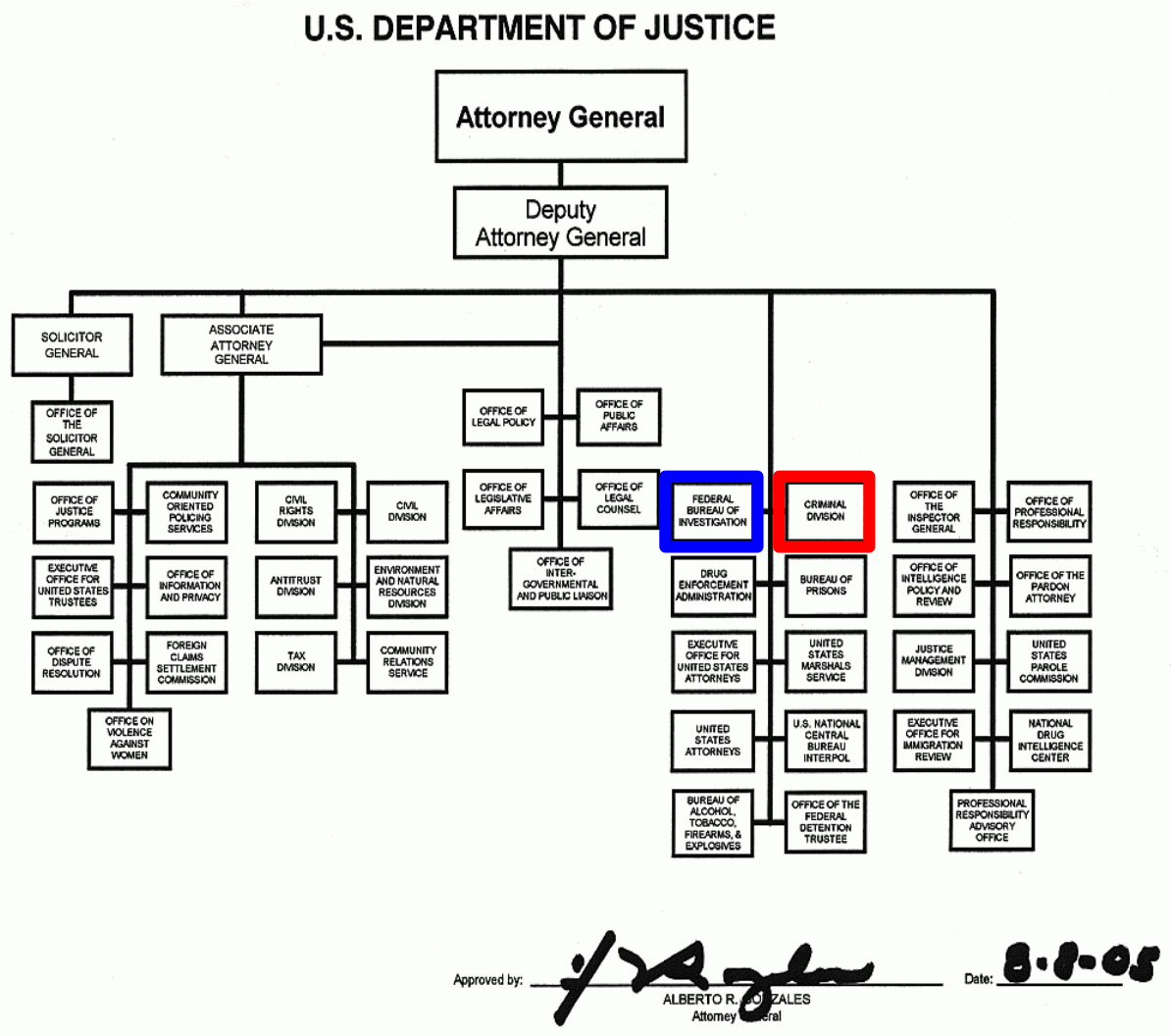

図 3　DoJ の組織図[3]

3.2. Federal Bureau of Investigation (FBI)

FBI (Federal Bureau of Investigation : 米連邦捜査局) では、Cyber Division 内にある Cyber Crime Section がフィッシングへの対応を行っている。

[3] 出典：DoJ ホームページ (http://www.usdoj.gov/)

FBI では、サイバー犯罪捜査には民間企業との協力が必要であるとの見地から、情報収集のための相談窓口 IC3 の開設や、民間企業との強固な協力体制を確保するための NCFTA の設置などに取り組んでいる。

また、FBI では、CERT/CC (CERT / Coordination Center) に専任の連絡係を設置し、関係機関との連携を強化している。CERT/CC としては、フィッシングに関する様々な情報が入って来るが、法執行機関ではないためフィッシングサイトの捜査やサイトの停止要請などはできない。そこで、FBI と連携することでこれらが可能となり、適切な役割分担により効果的な対応を実現している。

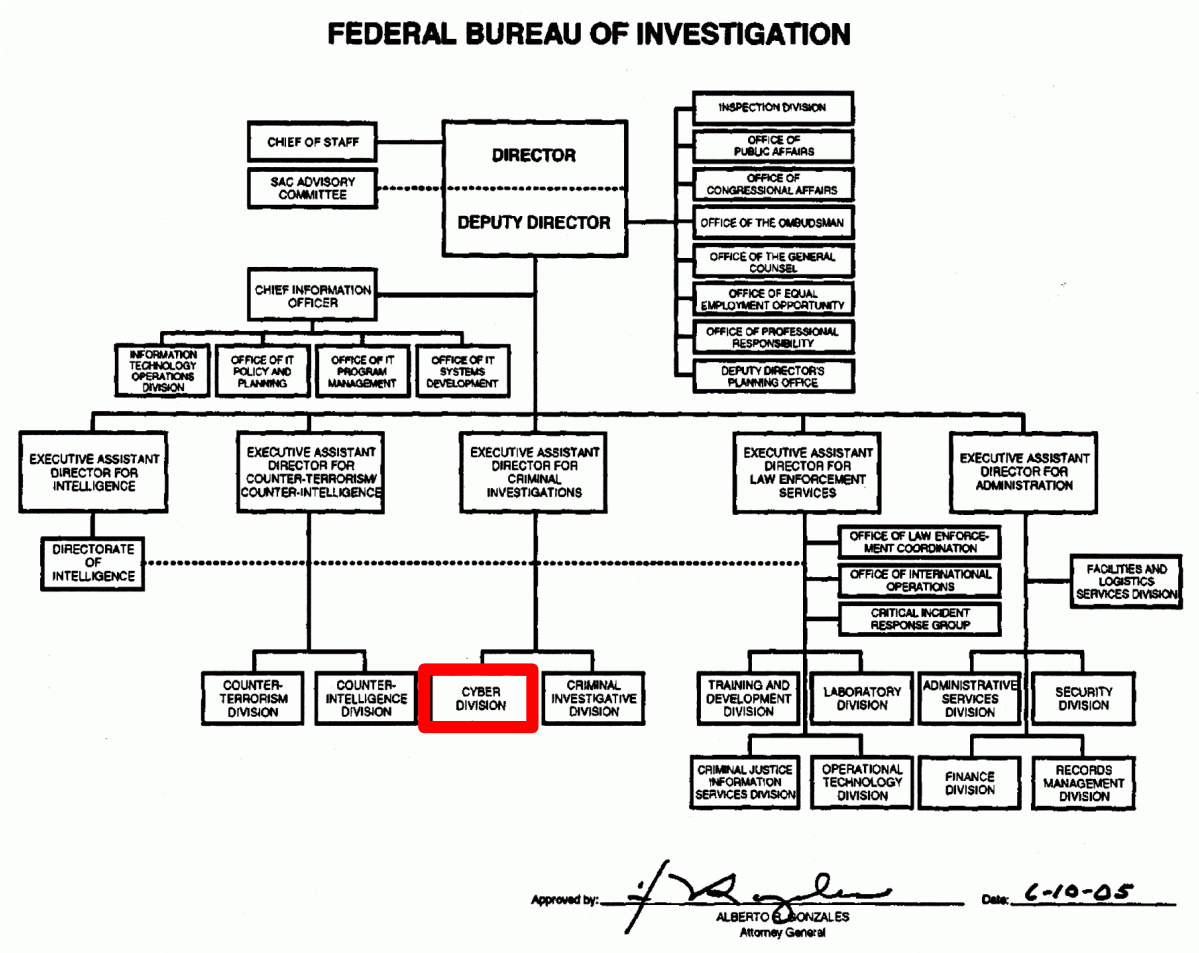

図 4　FBI の組織図[4]

[4] 出典：FBI ホームページ（http://www.fbi.gov/）

３.３. U.S. Department of Homeland Security (DHS)

DHS (U.S. Department of Homeland Security：米国土安全保障省) に設置された US-CERT (US-Computer Emergency Readiness Team) では、重要インフラ防護を任務としている。(図中の Under Secretary for Preparedness の一部門。)

US-CERT は 2003 年に設置され、米国のインターネットインフラの保護するために、DHS と公的機関、民間事業者との間のパートナーシップの構築、米国のサイバー攻撃に関する関係機関の調整を行っている。具体的な活動としては、脅威や脆弱性の分析・軽減、サイバー警戒情報の発信、インシデント対応活動の調整を行っている。

また、フィッシングに関しては、ホームページ上において報告窓口を開設し、被害防止対策のための情報収集を行っている。

３.４. U.S. Secret Service (USSS)

U.S. Secret Service （以下、「USSS」という。）は、2002 年、DHS 下の組織に移管された。USSS の任務は要人の保護と、保護するべき要人に影響する可能性のある脅威について調査することの二つである。また、脅威の調査の一環として、金銭に関わるサイバー犯罪に関し、Financial Crimes Division が情報収集、分析、各支部への情報発信などの活動を行っている。USSS は法執行機関であり、犯罪の捜査や犯罪者の逮捕、起訴なども行う。

USSS では、CERT/CC に連絡係を常時配置し、インターネットに関する最新の状況の把握、技術的な相談がすぐにできる体制を構築している。そして、CERT/CC が日々収集している情報の中から重要なものをワシントン D.C.の本部へ送り、本部にて情報を分析し、必要に応じて USSS の全米各地の支部へ情報提供を行っている。

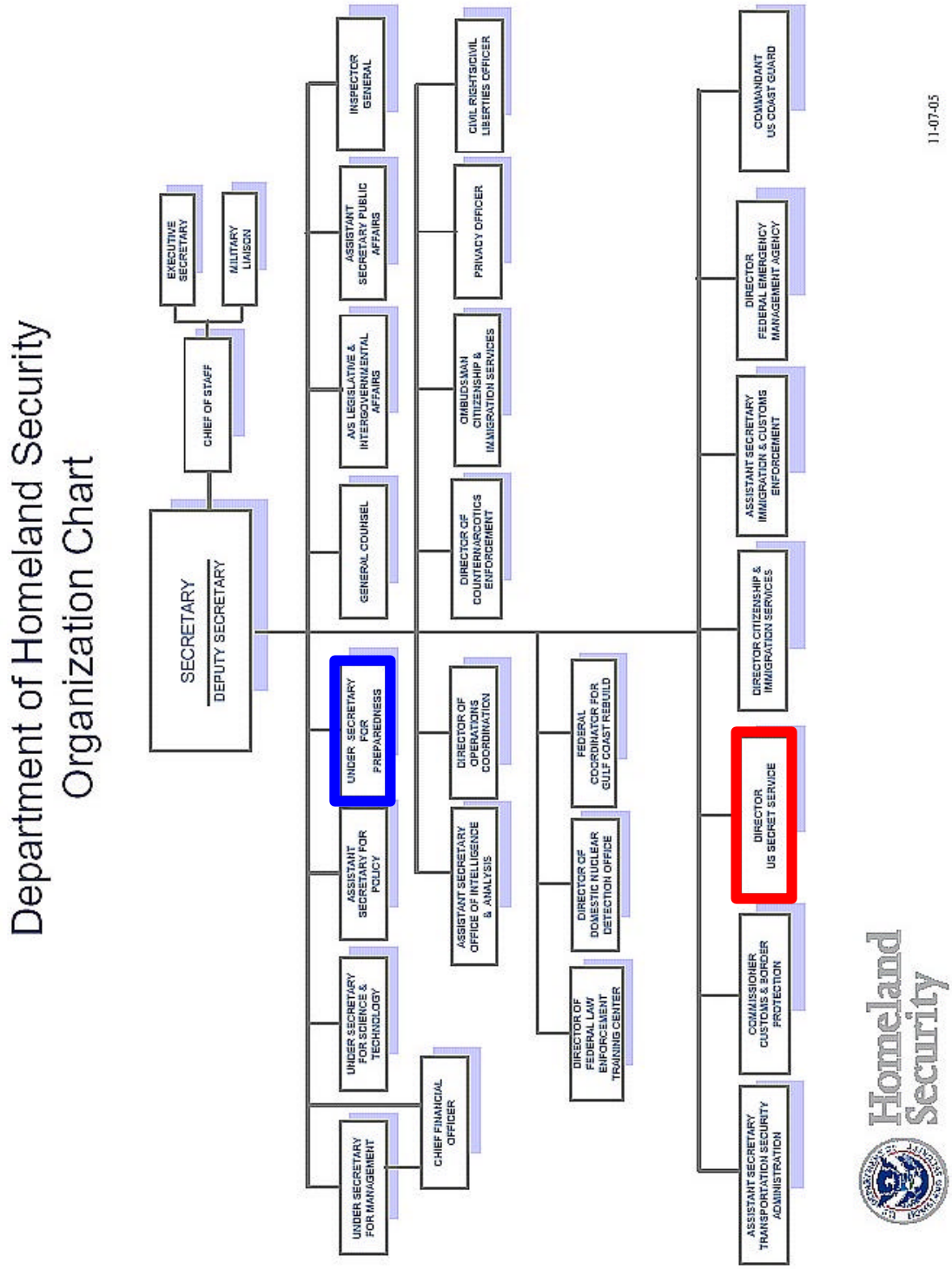

図 5　DHSの組織図[5]

[5] **出典：**DHS **ホームページ**（http://www.dhs.gov/）

３．５． National Cyber-Forensics and Training Alliance (NCFTA)

NCFTA (National Cyber-Forensics and Training Alliance) は、FBI、NW3C、カーネギーメロン大学、ウェストバージニア大学が連携して設立した非営利組織である。サイバー犯罪が増加し、フォレンジック分析や情報収集の専門家の必要性が増してきている中で、FBI 内のリソースだけではなく、民間企業、学術研究機関、政府のそれぞれから人員を出し合い、サイバー犯罪に関する取組みを推進するために組織された。

NCFTA は民間のビルに入居し、FBI の Cyber Crime Section のスタッフ５～６名に加え、研究員及び学生１０～１２名が常駐している。また、マイクロソフト社から情報分析担当者が派遣されている。

NCFTA は、非営利団体の立場で、中立的に民間企業、研究機関、法執行機関の三者の橋渡し役を担っている。具他的には、NCFTA は、Digital PhishNet の運営や、フィッシングに関する報告の受付、情報の収集、分析、検証・再現、法執行機関への捜査情報の提供、情報提供者へのフィードバックなどを行っている。

NCFTA 内の作業環境としては、ウイルスやワーム、マルウェアなどを検証するクローズドネットワーク環境、フォレンジックのためのスペース等を用意している。活動実績としては、法執行機関への 100 件以上の情報提供、125 件以上の犯罪捜査への貢献、電子的な証拠を取り扱うためのトレーニングの実施などがある。

NCFTA の立ち上げ時の担当者であった、IC3 の元センター長であり、FBI の捜査員でもある Daniel Larkin 氏によると、民間企業、学術研究機関、法執行機関のそれぞれの組織から人を集め、同じ場所で情報を共有しながら仕事ができるような環境を構想し、実現したものである。

３．６．BITS

BITS は 1996 年に設立された非営利組織であり、100 以上の大手金融機関が参加し、CEO レベルの情報交換の場として活動している。BITS という名前は、元来、“Banking Industry Technology Secretariat”を意味していたが、現在は銀行のみでなく金融業界全体が関わることになったため、単純に BITS という名称を用いている。

BITS では、電子金融サービス業界の振興や消費者保護のためのセキュリティ等について幅広く議論している。また、他の業界、政府機関、法執行機関等との連携を推進している。

BITS では、現在、次のテーマについてワーキンググループを立ち上げるなどして取り組んでいる。

- Security and Risk Assessment（セキュリティ及びリスク分析）
- Crisis Management Coordination（緊急事態対応の連携）
- Fraud Reduction（詐欺の抑止）
- Identity Theft Assistance Center（個人情報窃盗対策支援センター）
- IT Service Providers （IT サービス提供事業者）
- Operational Risk Management （リスク管理）
- Payments Strategies（決済システムの戦略）

BITS の取組みの中で、フィッシングへの対応は ITAC (Identity Theft Assistance Center) が行っている。

※ITAC については、４．５節参照。

３．７．Federal Trade Commissions (FTC)

FTC（Federal Trade Commission：米連邦取引委員会）は、連邦の独占禁止法と消費者保護法を管轄する組織であり、一般消費者を詐欺行為等から保護することを任務の一つとしている。現在、サイバー犯罪が増加していることから、関係機関との連携や、一般消費者が詐欺や個人情報窃盗などの被害から自分自身を守ることができるように様々な情報発信を行っている。

フィッシングについては、The Division of Planning and Information において、以下の二つの活動を行っている。

① Identity Theft Data Clearinghouse

ホームページ上で一般消費者向けに、個人情報窃盗から身を守るための広報啓発活動を行うとともに、一般消費者が被害に遭った場合の電話相談窓口を開設している。

○ URL：http://www.consumer.gov/idtheft/

② Consumer Sentinel

1997 年より、一般消費者からのインターネット、電話勧誘、個人情報窃盗などの詐欺行為に関する苦情内容を関係機関から集約してデータベース化する取組みを推進している。データベースの管理は FTC が行い、現在、米国内外の法執行機関等の 150 以上の組織がこの取組みに参加している。このデータベースには累計約 300 万の情報が蓄積されている。

このほか、DoJ 及び FBI と連携して NW3C の設立等にも取り組んでいる。

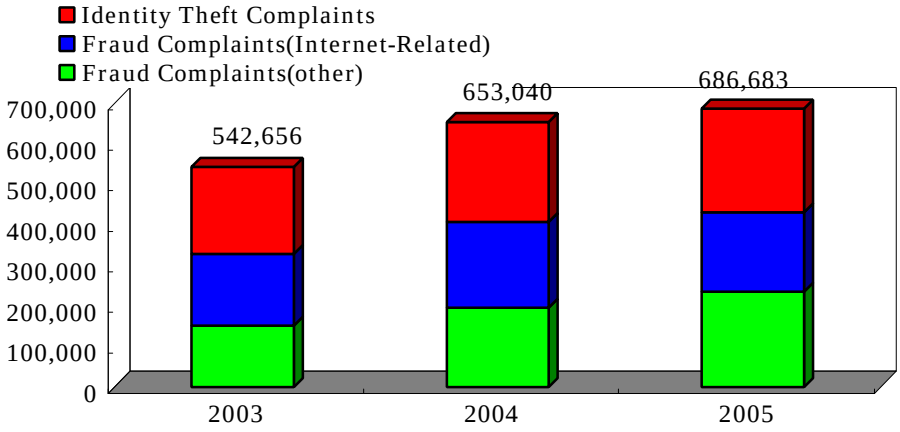

図 6　Sentinel データベースの年間件数[6]

[6] **出典：**Consumer Fraud and Identity Theft Complaint Data January - December 2005 (Federal Trade Commission, January 2006)