



米国 インターネット犯罪の動向

～ Internet Crime Complaint Center 「2007 Internet Crime Report」 より ～

KDDI総研 制度・政策G 研究主査 藤崎 太郎

はじめに

警察庁によると、日本におけるサイバー犯罪^①相談窓口（都道府県警察本部相談窓口：<http://www.npa.go.jp/cyber/soudan.htm>）が、2007年中に受理した相談件数は73,193件にのぼる（前年比19.1%増）^②（6ページ【コラム】欄参照）。

実際、各地の相談窓口には、「自分の携帯電話に勝手にメールが送られてきたため、何かと思って開いたとたんアダルトサイトに会員登録され、入会金を請求された。」等の架空請求・不当請求に関するもの、「オークションで落札し、代金を振り込んだが商品が送られてこない。」等のオークション詐欺に関するもの、「自分がオンラインゲームで使っていたID・パスワードを盗まれて不正アクセスされ、ゲーム上で集めたアイテムが盗まれてしまった。」等の不正アクセスに関するもの等、サイバー犯罪に関する様々な苦情・相談が届けられているとのことである^③。

一方、米国におけるサイバー犯罪については、米国のInternet Crime Complaint



①（脚注1）サイバー犯罪とは、「コンピューター技術及び電気通信技術を悪用した犯罪」で、ネットワーク利用犯罪、コンピューター・電磁的記録を対象とした犯罪、不正アクセス禁止法違反が対象となる。（出典）<http://www.npa.go.jp/cyber/existing/hightech.html>

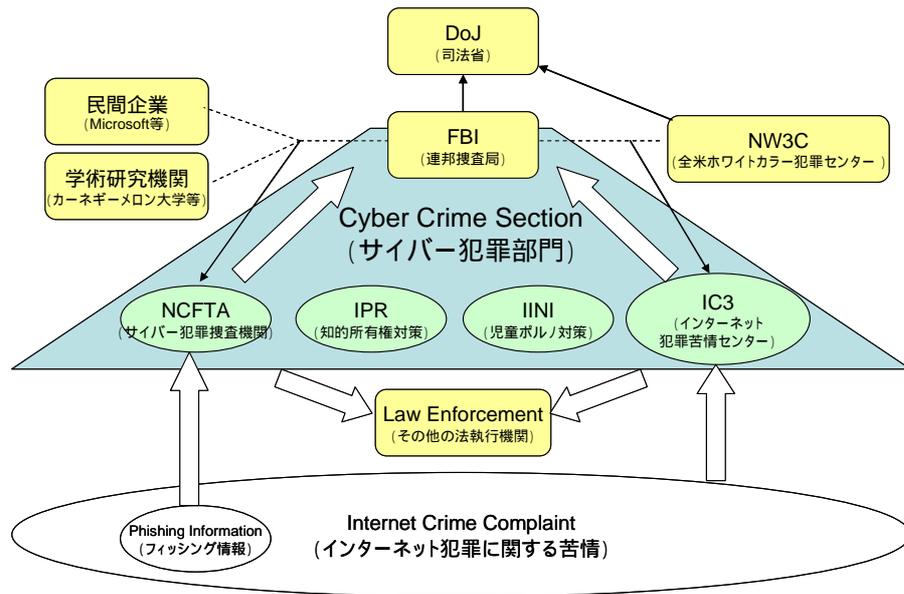
②（脚注2）（出典）警察庁「平成19年中のサイバー犯罪の検挙状況等について」（2008.2）なお、同報告書によると、2007年中にサイバー犯罪として検挙された件数は5,473件（前年比23.7%増）と、過去5年間で約3倍に増加している。

③（脚注3）（出典）同上

Center (IC3 : インターネット犯罪苦情センター) ^{④(脚注1)} が公表した「2007 Internet Crime Report」により、その動向を窺い知ることができる。

IC3は、Federal Bureau of Investigation(FBI : 連邦捜査局)や、National White Collar Crime Center (NW3C : 全米ホワイトカラー犯罪センター) ^{④(脚注2)} と連携し、急速に拡大するインターネット犯罪に関する一般からの苦情の受理、及び法執行機関・規制機関に対する受理した事案の照会等の役割を担う機関である(【図表1】参照)。

【図表1】FBIを中心とする関係機関の連携



(出典) 社会安全研究財団「フィッシングに関する調査研究報告書」(2006.3)



^{④(脚注1)} 2000年、FBIはNW3C(脚注2参照)と連携して、米国におけるインターネット詐欺に関する一般からの報告受付窓口として、Internet Fraud Complaint Center(IFCC : インターネット詐欺苦情センター)を開設した。その後、詐欺に限らず多様なインターネット犯罪の報告を受け付けることとし、2003年、組織の名称をInternet Crime Complaint Centerに変更した。(出典) 社会安全研究財団「フィッシングに関する調査研究報告書」(2006.3)

^{④(脚注2)} NW3Cは、Department of Justice (DoJ : 司法部)、FBI 及びFederal Trade Commission (FTC : 連邦取引委員会)の連携により1980年に設立された非営利組織である。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、起訴等について州や地域の法執行機関のサポートをしている。(出典) 同上

なお、「White Collar Crime」とは、ビジネスの中で、被害者との信頼関係を持った個人または企業のマネージャーによってなされ、利益を求めてなされる犯罪をいい、具体的には、反トラスト、贈賄、破産犯罪、コンピューター詐欺等が挙げられる。(出典) 白石賢「米国white collar crime・企業犯罪の動向」(2004.11)

「2007 Internet Crime Report」は、IC3が2007年中に受理したインターネット犯罪^①に関するComplaint(苦情)を編纂・分析したものである。具体的には、IC3が受理し、または法執行機関・規制機関に照会したインターネット犯罪に関する苦情(206,884件)について、件数の推移のほか、犯罪の種類、被害の内容(金銭損害)、地理的分類、性別・年代別構成等、米国のインターネット犯罪の動向を把握する上で興味深い分析を行っている。

本稿では、同報告書に基づき^②、米国のインターネット犯罪の最新動向を紹介する^③。

1 インターネット犯罪の動向

インターネット犯罪についての苦情は、主としてIC3のWeb(www.ic3.gov)または電話を利用してIC3に通知される。IC3に届けられた情報は、IC3の内部で審査、分類され、適切な法執行機関または規制機関に展開される。

1 - 1 件数の推移

2007年、IC3に対し、Webを通じて届けられた苦情は、206,884件である。2006年の207,492件と比較すると0.3%の減少であり、ここ4年間、ほぼ横ばいの状態である(【図表2】参照)。

このうち、IC3が法執行機関・規制機関に対し照会した苦情の件数は、90,008件であり、2006年の86,279件からわずかに増加している(【図表3】参照)。

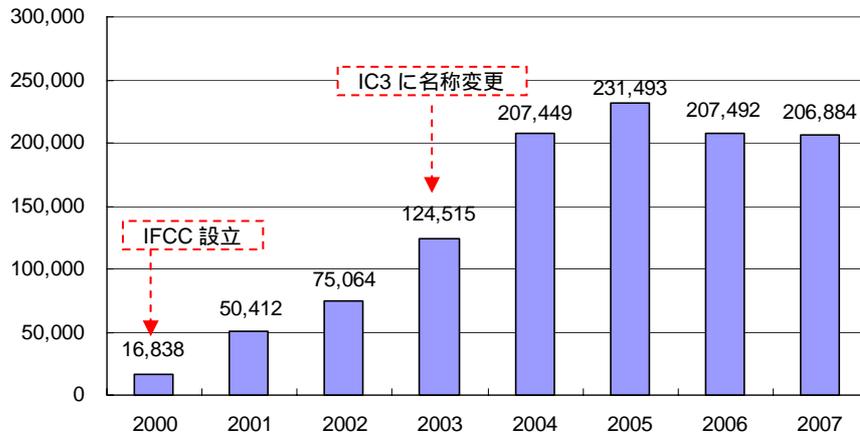


^①(脚注1) 本報告書においては、「Cyber (Internet)」と表記される等、サイバーとインターネットはほぼ同義語として取扱われている。本稿でも、同様とする。

^②(脚注2) 本報告書は、IC3が受理した苦情についての情報であり、インターネット犯罪または詐欺に関する被害者全ての実態を表すものではないことに留意する必要がある(本報告書にも明記されている)。

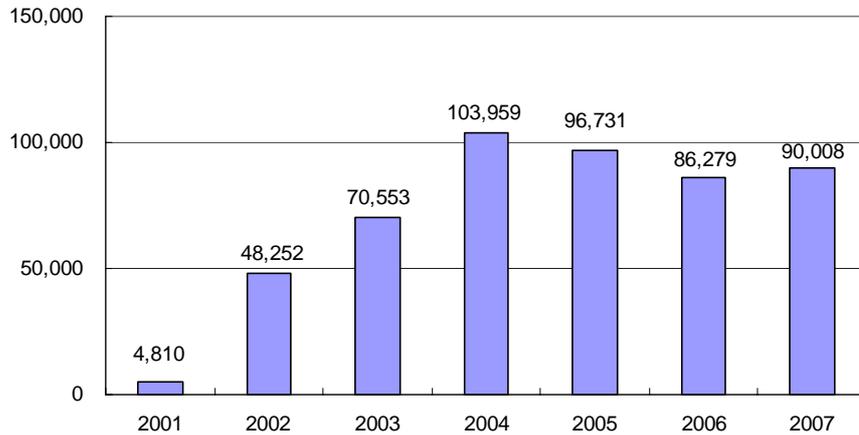
^③(脚注3) 現在、米国には全米規模のサイバー犯罪(検挙件数等)の公式統計調査は存在していない。ただしDoJ(司法省)は、Department of Homeland Security(DHS:国土安全保障省)と共同で、全米を対象とした初のサイバー犯罪の調査を実施中であり、2008年中にその報告が公表される予定である。(http://www.ncss.rand.org/index.html)

【図表2】Webサイト経由で受理した苦情件数



(出典) IC3 「2007 Internet Crime Report」

【図表3】法執行機関・規制機関に照会された苦情の件数



(出典) IC3 「2007 Internet Crime Report」

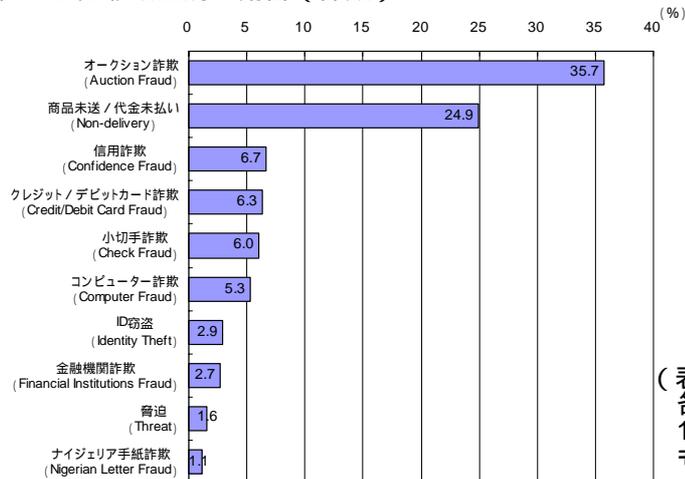
一方、IC3に通知された苦情のうち、法執行機関・規制機関に直接展開されなかったもの（116,876件）は、インターネット犯罪の傾向・類型の分析、啓蒙活動等に活用され、また、IC3のデータベースに登録される。そして、IC3と連携する法執行機関・規制機関は、当該データベースを参照できている。たとえば、2007年、IC3は13の機関と新たに連携することになっている（12件は、NW3Cの会員、1件はNW3Cの非会員）。

1 - 2 犯罪の種類

IC3が法執行機関・規制機関に照会した事案の中では、オークション詐欺の割合が35.7%と最も高く、購入商品の未送／代金未払いが24.9%、信用詐欺（マルチ商法

等)が6.7%と順につづく(【図表4】参照)^①(脚注1)。2006年と比べると、オークション詐欺、投資詐欺を除いた、他の犯罪類型の割合が上昇している。

【図表4】犯罪類型別の割合(件数)



(表注) 各犯罪類型の説明は、12ページ【図表15】も参照。

(出典) IC3「2007 Internet Crime Report」

IC3は、詐欺事件と判断すれば、その事件を管轄に属する法執行機関・規制機関に照会する。また、ID窃盗の場合は、Federal Trade Commission (FTC: 連邦取引委員会)に、ナイジェリアの手紙詐欺(ナイジェリア刑法419条詐欺)^②(脚注2)は、United States Secret Service (USSS: USシークレットサービス)に照会する等の適切な対



^①(脚注1) 被害の内容は複数のカテゴリーに属する場合があるが、被害者がその被害のどの部分を重視するかにより分類結果も影響を受ける。また、IC3が主要なEコマースの利害関係者の協力を得ているという事実を認識する必要がある。すなわち、eBayのような多くの企業がIC3のWebサイトにリンクを貼っているため、その結果として、被害者が「オークション詐欺」と表現する場合が多くなる。

^②(脚注2) ナイジェリアを舞台に世界的広がりを見せた、大規模な資金送金や商談をエサに前渡金や商品を詐取する国際詐欺事件のこと。通称「419詐欺事件(ナイジェリア刑法419条に抵触する犯罪)」。80年代に欧米諸国で顕在化し、その後日本にも上陸、さらに世界的に広がり、被害者も資産家や法人関係者から一般市民にも及んでいる。

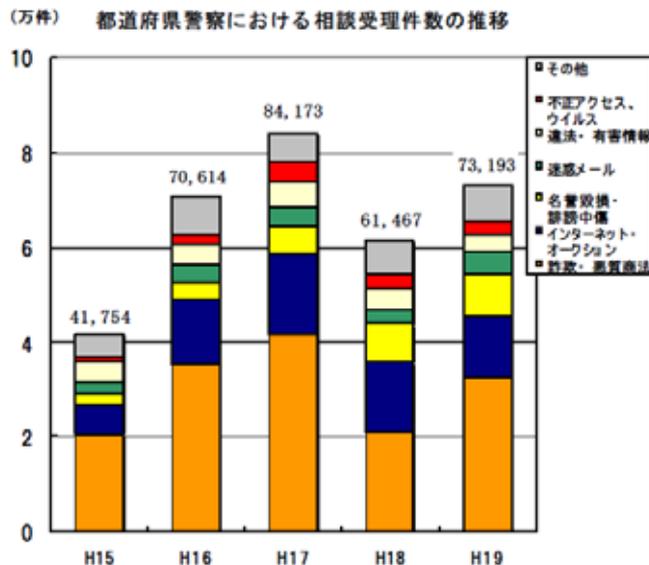
アプローチ方法は、以前の手紙やFAXから、今では電子メールの利用が主流となり、アフリカや欧州、アジア地域を中心に、世界各地から大量に勧誘メールが届く等、発信源も広域化した。「マネーロンダリング型(前渡金詐取)」、「貿易取引型(商品/前渡金詐取)」等が代表的である。突然、「全く面識のない海外の人物や法人」から、「緊急かつ極秘の取引」との名目で、「巨額の隠蔽資金や遺産の送金や商品の大量注文」を持ちかけるメールが舞い込んできた場合、それはアフリカ地域、アジア地域を発信源とする国際的な犯罪集団による詐欺勧誘の可能性がある。(出典)日本貿易振興機構(JETRO)「国際的詐欺事件について」(<http://www.jetro.go.jp/contact/faq/419/>)

応を行っている。そのほか、児童ポルノのような金銭被害を伴わない事案は、National Center for Missing and Exploited Children(失踪・虐待児童の全米ネットワーク)に、テロリストの情報は Public Access Center Unit (PACU) に、脅迫事件は州、地域の法執行機関に展開される。

【コラム】日本のサイバー犯罪の動向

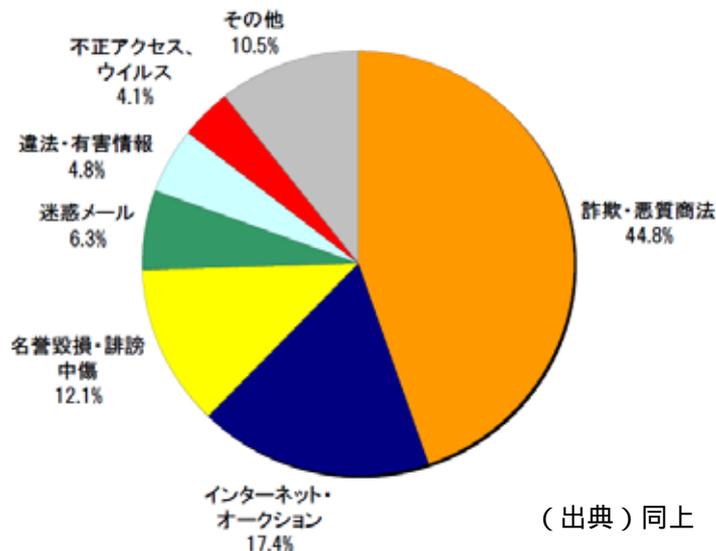
警察庁の発表によると、2007年（H19）各都道府県警察の受理したサイバー犯罪の相談件数は、合計で73,193件であり（【図表5】参照）このうち、「詐欺・悪徳商法」が44.8%、「インターネットオークション」が17.4%となっている（【図表6】参照）。

【図表5】都道府県警察における相談受理件数の推移



(出典) 警察庁「平成 19 年中のサイバー犯罪の検挙状況等について」

【図表6】相談区分別の割合



(出典) 同上

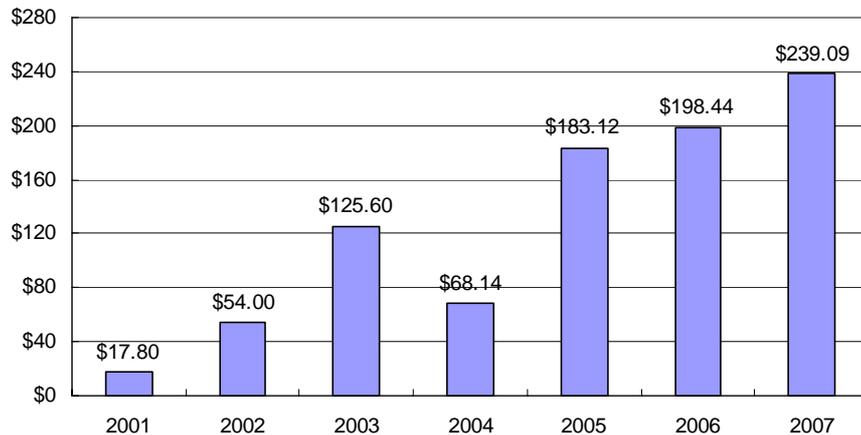
単純な比較はできないが、「詐欺・悪徳商法」、「インターネットオークション」の相談件数の割合が高い点は、日本と米国の共通の傾向であるといえる。

1 - 3 被害の内容（金銭被害）

IC3が、法執行機関・規制機関に照会した90,008件のうち、72,226件は金銭被害を伴う事案である^{☞（脚注1）}。

また、IC3が法執行機関・規制機関に照会した詐欺事案の総被害金額は、239.9百万ドル（約255億円）^{☞（脚注2）}であり、2006年の198.44百万ドル（約211億円）よりも増加している（【図表7】参照）。

【図表7】詐欺事案の総被害金額



（出典）IC3「2007 Internet Crime Report」

これら被害金額の平均値（mean or average）は、2,529.90ドル（約269千円）で、中央値（median）^{☞（脚注3）}は、680.00ドル（約72千円）となっている。

類型別でみると、最も金銭被害の大きいものは、投資詐欺（中央値は、3,547.94ドル（約377千円））である。さらに、小切手詐欺の中央値は、3,000ドル（約319千円）である。



^{☞（脚注1）} 残りは、被害に遭う前に事件を報告したか、または被害に遭う前に金銭を回復していたものと考えられる。

^{☞（脚注2）} 1ドル=106.24円（東京市場TTMレート 2008年7月1日）

^{☞（脚注3）} 中央値（median）とは、データの大きさの順に並べた時に中央にくる値で、データのばらつきが著しい場合に平均値（mean or average）では誤差が大きいため、中央値が用いられる。（出典）酒井隆「アンケート調査と統計解析がわかる本」（2003.10）

円) ナイジェリアの手紙詐欺の中央値は1,922.99ドル(約204千円)とつづく。

一方、被害の小さい類型は、クレジット/デビットカード詐欺で、被害額の中央値は298ドル(約32千円)である(【図表8】参照)。

【図表8】犯罪類型別の割合(金額)と被害額(中央値)

	割合(対被害額合計)	被害額(中央値)
投資詐欺(Investment Fraud)	6.1%	\$3,547.94
小切手詐欺(Check Fraud)	9.9%	\$3,000.00
ナイジェリアの手紙詐欺 (Nigerian Letter Fraud)	6.4%	\$1,922.99
信用詐欺(Confidence Fraud)	12.6%	\$1,200.00
オークション詐欺(Auction Fraud)	22.4%	\$483.95
商品未送/代金未払い(Non-delivery)	17.8%	\$466.00
クレジット/デビットカード詐欺 (Credit/Debit Card Fraud)	4.6%	\$298.00

(表注) 各犯罪類型については、12ページ【図表15】参照。

(出典) IC3「2007 Internet Crime Report」

1 - 4 加害者の特徴

インターネット犯罪の加害者について、その居住地域を見た場合(米国内に居住する者)、人口数の多い州に偏る傾向がある。具体的には、カリフォルニア州、ニューヨーク州、テキサス州、イリノイ州、ペンシルベニア州、ジョージア州で全体の53%を占める(【図表9】参照)。(脚注)。

【図表9】加害者の居住地域



1.カリフォルニア	15.8%	6.ペンシルベニア	3.5%
2.フロリダ	10.1%	7.ジョージア	3.1%
3.ニューヨーク	9.9%	8.オハイオ	2.8%
4.テキサス	7.0%	9.ワシントン	2.8%
5.イリノイ	3.6%	10.ニュージャージー	2.8%

(出典) IC3「2007 Internet Crime Report」



(脚注) 加害者の性別で見ると、男性が全体の約4分の3(75.2%)を占めている。

米国以外の国に居住する加害者も含めると、米国内に居住する者は全体の63.2%に過ぎず、英国、ナイジェリア、カナダ等その居住地は多様である(【図表10】参照)。

【図表10】加害者の居住国



1.米国	63.2%	6.イタリア	1.3%
2.英国	15.3%	7.スペイン	0.9%
3.ナイジェリア	5.7%	8.南アフリカ	0.9%
4.カナダ	5.6%	9.ロシア	0.8%
5.ルーマニア	1.5%	10.ガーナ	0.7%

(出典) IC3 「2007 Internet Crime Report」

1 - 5 被害者の特徴

インターネット犯罪の被害者数が多いのは、カリフォルニア州、フロリダ州、テキサス州、ニューヨーク州等の人口数の多い地域となっている(【図表11】参照)。

【図表11】被害者の居住地



1.カリフォルニア	14.4%	6.イリノイ	3.5%
2.フロリダ	7.2%	7.オハイオ	3.1%
3.テキサス	7.2%	8.ワシントン	3.1%
4.ニューヨーク	5.7%	9.ニュージャージー	3.1%
5.ペンシルベニア	3.6%	10.ヴァージニア	2.9%

(出典) IC3 「2007 Internet Crime Report」

また、被害者の大部分は米国（91.9%）に居住しているが、カナダ（2.1%）、英国（1.1%）、オーストラリア（0.6%）等、米国以外に居住する者からの苦情申立ても全体の10%弱を占めている。

さらに、被害者について、その性別[※]（脚注）、年齢と被害金額との関係を見ると、男性は女性より、年長者は年少者より被害金額が大きくなる傾向がある（【図表12】参照）。

【図表12】被害者の属性と被害金額（中央値）

属性	被害金額（中央値）
男性	\$765.00
女性	\$552.00
～19歳	\$384.99
20～29歳	\$610.00
30～39歳	\$699.99
40～49歳	\$760.00
50～59歳	\$750.00
60歳～	\$760.00

（出典）IC3「2007 Internet Crime Report」

1 - 6 加害者と被害者の関係

実際、加害者と被害者の居住地の関係について、加害者の実数が最も多いカリフォルニアでさえ、加害者と被害者が同州に居住している事案は、全体のわずか18.3%に過ぎない（【図表13】参照）。

【図表13】加害者と被害者の居住地の関係

州（ 1 ）	同州（ 2 ）	1（ 3 ）	2（ 3 ）	3（ 3 ）
1.カリフォルニア（CA）	18.3%	（NY 9.1%）	（FL 8.0%）	（TX 5.7%）
2.フロリダ（FL）	13.6%	（CA 13.4%）	（NY 8.1%）	（TX 5.7%）
3.ニューヨーク（NY）	12.6%	（CA 12.9%）	（FL 9.1%）	（TX 5.9%）
4.ネバダ	10.9%	（CA 14.4%）	（FL 9.5%）	（NY 9.5%）
5.テキサス（TX）	10.9%	（CA 11.7%）	（FL 9.5%）	（NY 8.9%）
6.アリゾナ	10.6%	（CA 12.9%）	（FL 8.8%）	（NY 8.4%）
7.イリノイ	9.2%	（CA 12.9%）	（FL 8.9%）	（NY 8.9%）
8.ニューメキシコ	8.8%	（CA 11.3%）	（FL 8.3%）	（NY 8.0%）
9.ワシントン	8.8%	（CA 13.6%）	（NY 9.3%）	（FL 8.8%）
10.テネシー	8.7%	（CA 12.2%）	（FL 10.3%）	（NY 9.5%）

（表注） 1 加害者の居住地域
2 加害者と被害者が同州の割合
3 同州以外で、被害者の割合の高い上位3州

（出典）IC3「2007 Internet Crime Report」

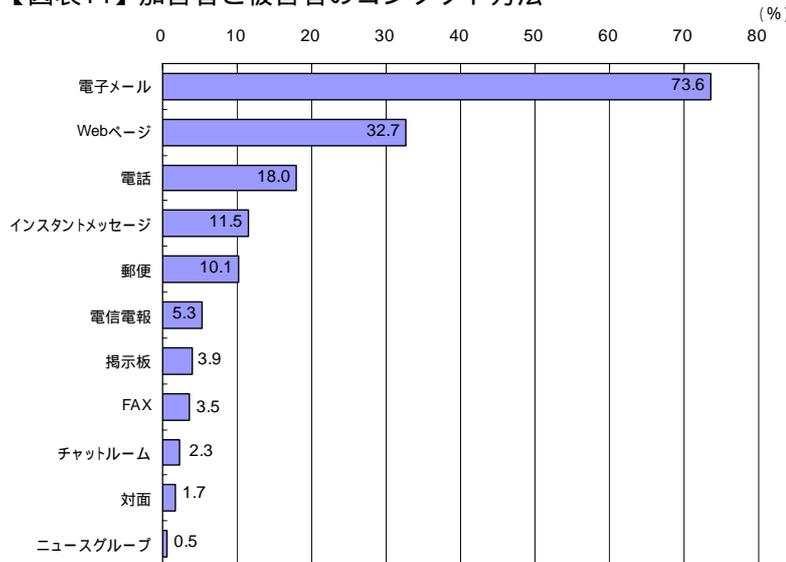


※（脚注） 被害者のうち、男性は57.6%、女性は42.4%である。

加害者と被害者の地理関係に関連性がないというのはインターネット犯罪の特徴である。しかし、加害者と被害者の地理関係は、司法管轄に影響する。すなわち、司法管轄が異なると、捜査権発動の基準（金額の多寡）の違い等、インターネット犯罪の捜査や訴追の妨げとなる事情となる場合が多い[☞]（脚注）。

また、被害者と加害者のやり取りは、電子メール（73.6%）、Webページ（32.7%）による場合が多く、電話でのコンタクト（18.0%）、インスタントメッセージ（11.5%）がそれに続く。対面によるやり取りは1.7%である（【図表14】参照）。

【図表14】加害者と被害者のコンタクト方法



（出典）IC3「2007 Internet Crime Report」

被害者が加害者と対面して取引するという事例が少ないという事情は、インターネットの匿名性という性質によるものであるが、前述の地理関係とともに、犯罪の捜査と訴追を妨害する要因となりうる。



[☞]（脚注）州をまたがる捜査は、FBIが管轄権を有する。（出典）Oxford 現代英英辞典

なお、アメリカの警察制度は非常に複雑である。基本的には、連邦に属する機関と州に関する機関に分けられ、連邦については、法律の執行という警察官の職務を遂行する機関（law enforcement agencies）は、職務内容に応じて合衆国政府の各省庁に分配・所属している。したがって、日本の警察庁のように、多様な警察業務を統括する単一の警察組織は存在しない。FBIは、DoJ（司法省）の一部局であり、そのほか、麻薬取締局がある。アル・カポネらのマフィアとの闘いで勇名をはせた「アルコール取締官」は、アルコール・タバコ・銃火器局（もと財務省であったが司法省に移管）に所属している。

また、州の警察制度は、州の歴史により様々であるが、基本的には行政単位ごとに州、郡、地方の3種類に分けられる。地方警察の中には、市や町などの警察がある。

（出典）島伸一「アメリカの刑事司法 ワシントン州キング郡を基点として」（2002.10）

2 インターネット犯罪（詐欺）の類型（代表的な詐欺類型）

インターネットを悪用した犯罪には多種多様な類型があり、また次々に新たな類型が生み出されている。このうち、代表的な詐欺類型を採り上げ、その内容を説明する（【図表15】参照）。

【図表15】多種多様な詐欺類型

用語	説明
金融機関詐欺 Financial Institution Fraud	虚偽の事実を示したり、重要事項を隠蔽したりすることで、金融機関を欺くこと。ID窃盗に関する場合で、犯罪者が被害者の真のID（社会保障カード、運転免許証、出生証明書）を保持する場合でクレジット/デビットカード詐欺に至らないものは、このカテゴリーに分類される。
クレジットカード/ デビットカード詐欺 Credit/Debit Card Fraud	カードの無権限利用により、目的物（価値ある物）を入手すること。
ID窃盗 Identity Theft	他人の個人識別情報（氏名、生年月日、社会保障カードナンバー、クレジットカードナンバー等）を違法利用すること。米国で急速に増加している犯罪の1つ。
小切手詐欺 Check Fraud	小切手の偽造、変造、口座閉鎖や残高不足を知らずながら小切手を発行すること。
信用詐欺 Confidence Fraud	信頼関係に背き財産的損害をもたらすこと。故意に虚偽事実を示し、重要事項の隠蔽を図ることで他人に損害をもたらすこと。オークション詐欺、商品未送/代金不払い詐欺、ナイジェリア手紙詐欺もこの類型に属する。
ナイジェリアの手紙詐欺 Nigerian Letter Fraud	ナイジェリア等の国から電子メール送信し、メールの受け手に対し大金を得られることを約束する詐欺のこと。メールの受け手は、その代わりに手数料の前払いや個人情報、クレジットカード、銀行口座番号等の情報の提供を要求される。被詐欺者は、一切の見返りはなく、メールの発信者に預けた金を失う結果となる。なお、5ページ【脚注2】も参照。
賭博詐欺 Gaming Fraud	賭金（bet）やイベント内容を偽り、金銭等を得ること。スポーツ買収や賭金（bet）の偽装表示等が挙げられる。
情報通信詐欺 Communications Fraud	携帯電話や固定電話等のメディアでやり取りされる情報に対する不正行為、不正処理のこと。携帯電話、衛星、固定電話のただ乗り等である。
公共サービス詐欺 Utility Fraud	個人や企業が虚偽の事実を示し、または故意に害する目的で、水道や電気等の公共サービスを提供する公益企業を騙すこと。
保険詐欺 Insurance Fraud	保険購入者、または契約者が保険金の請求に際し、虚偽の事実を示すこと。「水増し（padding）請求」、保険申込書への虚偽記載、虚偽の怪我、傷害の申告、偽装事故等が含まれる。
政府詐欺 Government Fraud	故意に虚偽事実を示し、あるいは重要事項を隠蔽し、政府あるいは公共・公益に損害をもたらすこと。脱税、生活保護の不正受給、通貨偽造等が該当する。

用語	説明
投資詐欺 Investment Fraud	収益発生型事業体 (income-producing vehicles、投資組合等) や、リスク志向のベンチャーを悪用して、うまい儲け話をうたうこと。ポンジ (Ponzi) スキーム / ピラミッドスキーム (いわゆるネズミ講、マルチ商法のこと) や、市場操作が典型である。
企業詐欺 Business Fraud	法人、企業が、故意に虚偽事実を示し、あるいは重要事項を隠蔽すること。倒産詐欺や著作権侵害がこれに該当する。
コンピューター詐欺 Computer Fraud	広義では、コンピューターによる違法行為全般を指す。米国会計検査院の定義によれば、ここでのコンピューターとは「従来型の犯罪のためのツールとして利用されるもの」との意味である。すなわち、ソフトウェアやインターネットのような機能を利用して違法行為を犯す場合である。これには、「真の (true)」コンピューター犯罪とコンピューターに関連する犯罪の2つの意味がある。前者は、コンピューターの運用システム、プログラム、ネットワークをターゲットとする犯罪である。

(出典) IC3 「2007 Internet Crime Report」

【コラム】インターネット犯罪の防止に向けた通信事業者の取り組み

インターネット犯罪の増加は各国共通の課題であり、また、犯罪の防止に向けた取り組みは、立法、行政機関による規制活動、通信事業者・ISP等の事業者による自主的規制、NGO (非政府組織) による活動等を中心とする総合的なアプローチがなされている点でも共通しているといえる。

このうち、米国の主要通信事業者であるVerizonやAT&Tは、通信事業者として、さらにCSR (Corporate Social Responsibility) の一環として、インターネット犯罪の防止に向けた活動を推進している。インターネットの安全性を確保するための青少年に対する啓蒙活動の推進や、財団を通じて地域の各種団体等に対する資金援助等がその一例である (【図表16】参照)。

【図表16】Verizon、AT&Tの取り組み一例

	青少年のインターネットの安全な利用教育を目的として設立された非営利組織に対する支援	その他
Verizon	i-SAFE i-SAFEは、Verizon、Microsoft、IBM等が支援する非営利組織。米国政府からも補助金を得ている (2002年以降合計で1,100万ドル (約11.6億円))。	Verizon Foundation (基金) を通じて、インターネットの安全な利用教育に取り組む団体等に対し資金を援助している (2007年には、合計で20万ドル (約2.1億円) の支援を行っている。)
AT&T	Project Online Safety Project Online Safetyは、AT&T、Qwest、Comcast、NCTA (全米ケーブルテレビ協会)、facebook、MySpace等が参加する非営利組織。	AT&T Foundationを通じてインターネットの安全な利用教育に取り組む団体等に対し資金を援助している。

【図表17】 Verizon i-SAFE (<http://www.isafe.org/verizon/>)【図表18】 AT&T Project Online Safety (<http://www.projectonlinesafety.com/>)

📖 執筆者コメント

インターネット犯罪、とりわけインターネット詐欺の手口はますます巧妙となり、我々インターネット利用者は、常にそれら巧妙な犯罪の被害者となりうる危険にさらされている。

各自がインターネット犯罪から身を守るためには、やはり、「自分の身は自分で守る」べく、犯罪手口の類型をあらかじめ把握しておくことが重要であると思われる。

日本では、たとえば、警察庁がサイバー犯罪対策ホームページを公開し、犯罪対策に関する最新情報を提供している（<http://www.npa.go.jp/cyber/>）。インターネットの利用者は、日常的にこれらのホームページを参照するなどして、インターネット犯罪の最新動向に目を光らせておくべきだろう。

かつて日本人の被害者も続出した「ナイジェリアの手紙詐欺」のように、インターネット犯罪には国境は無関係である。そうすると、IC3の本報告書は、米国のものとはいえ、犯罪手口の最新動向を把握する上で有益なものであると考える。

なお、現在のところ、米国には全米規模のサイバー犯罪（検挙件数等）の公式統計調査は存在していないが、2008年中にはそれが公表される予定である^④（脚注）。当該調査の結果が公表された際は、別稿にて報告したい。

📖 出典・参考文献

本文中記載の出典・参考文献のほか、以下の文献も参照。

IC3ホームページ（<http://www.ic3.gov/>）

FBIホームページ（<http://www.fbi.gov/>）

Verizonホームページ（<http://www22.verizon.com/>）

AT&Tホームページ（<http://www.att.com/>） 等

【執筆者プロフィール】

氏名：藤崎 太郎（ふじさき たろう）

専門：米州・大洋州の通信市場に関する調査研究

最近の主なレポート：

「米国 ケーブルテレビ事業者への水平的所有規制について」（KDDI総研 R&A 2008年3月号）

（http://www.kddi-ri.jp/ja/r_a/pdf/KDDI-RA-200803-01-PRT.pdf）

「オーストラリアにおける児童・青少年保護を目的とするインターネット上の違法・有害情報対策」

（KDDI総研 R&A6月号）

（http://www.kddi-ri.jp/ja/r_a/pdf/KDDI-RA-200806-02-PRT.pdf）

E-mail：ta-fujisaki@kddi.com



^④（脚注）（参照）3ページ【脚注3】