株取引におけるセキュリティとサイバー犯罪

九州産業大学
商学部
商学科
学籍番号：13CC002

青木　智哉

担当教員：平川幹和子

目次

第１章

はじめに

現在の株取引はインターネットとコンピュータを駆使して取引し処理される。その中でサイバー犯罪は見逃すことのできない重要なファクターである。私自身、以前研究中にフィッシングサイトを見かけたこともあった。近年巧妙化しつつある手口とイタチごっこをするように改正される法律はサイバー犯罪への対策を難しくする。これをできる限り明解に示し現状と対策を示すことが本論文の目的である。

人々がコンピュータを用いインターネットを活用し始めて久しい。通信はより高速化し大量の情報を時間も場所も選ばず送受することが可能となった。そこで、台頭し始めたのがサイバー犯罪である。情報の窃取や改竄を目的としたこの犯罪は多くのユーザーを混乱に陥れた。一方、証券取引の市場では元来正確で高速な情報が求められる分野であったこともありインターネットの活用は進んだ。特に個人投資家に対してはオペレーターや証券マンを通さずに取引できる手軽さもあり大きく門戸を開くことになった。そこで、襲い掛かったのがサイバー犯罪である。投資家たちのアカウントを操作し情報を改竄し、自らに有利になるように捏造した事実をネット上にばらまいた。しかし、コンピュータに不慣れな投資家の中には適当な防衛手段を知らない者もいたし、法に無知な者が意識しないままに罪を犯すことさえあった。

インターネットで結ばれるということは自宅に居ながらの取引を可能とする。しかし、同じように自宅に居ながらもサイバー犯罪の被害に遭うという意味でもある。不可視の犯罪者がいつどこから襲ってくるか分からないという事実は確かに恐ろしいものである。また、証券取引とインターネットに関する法律は難解で馴染みの薄いものも少なくない。何も考えずに Web 上に投稿したコメントが法に触れる可能性もある。私はこの現状を見てサイバー犯罪が投資家に対する参入障壁の一つとなっているのではないかと考えた。

本論文では、サイバー犯罪の事例を取り上げその巧妙な手口や手法、関連する法律について分析しその実態を明らかにする目的とする。また、サイバー犯罪を投資家の参入障壁として認識することでこの解決により個人投資家のさらなる市場参入への一助となることを期待する。

第２章

サイバー犯罪とは

警察庁の広報資料「平成 28 年上半期のインターネットバンキングに係る 不正送金事犯の発生状況等について」 [1]によるとサイバー犯罪は、不正アクセス禁止法（不正アクセスの禁止等に関する法律）違反、コンピュータ・電磁的記録対象犯罪および不正指令電磁的記録に関する罪、ネットワーク利用犯罪の 3 つに分類される。株取引を行う際、このうちの不正アクセス禁止法違反は証券会社 web サイトへの不正ログイン、コンピュータ・電磁的記録対象犯罪および不正指令電磁的記録に関する罪は口座残高等の不正書き換え、ネットワーク利用犯罪は風説の流布等にあたる。よって、株取引を行う場合は、これら 3 つ全てのサイバー犯罪への理解を深め、それぞれの対処法を学ばなければならない。

図 1 は警察庁が発表したインターネットバンキングに係る不正送金事犯の発生状況の月別被害の推移（平成 27 年から 28 年上半期）を示したグラフである。の不正送金事件の発生件数を示している。現在は減少傾向にあることが分かるが、対策と新たな犯罪手口がどんどんと増えていることが分かる。

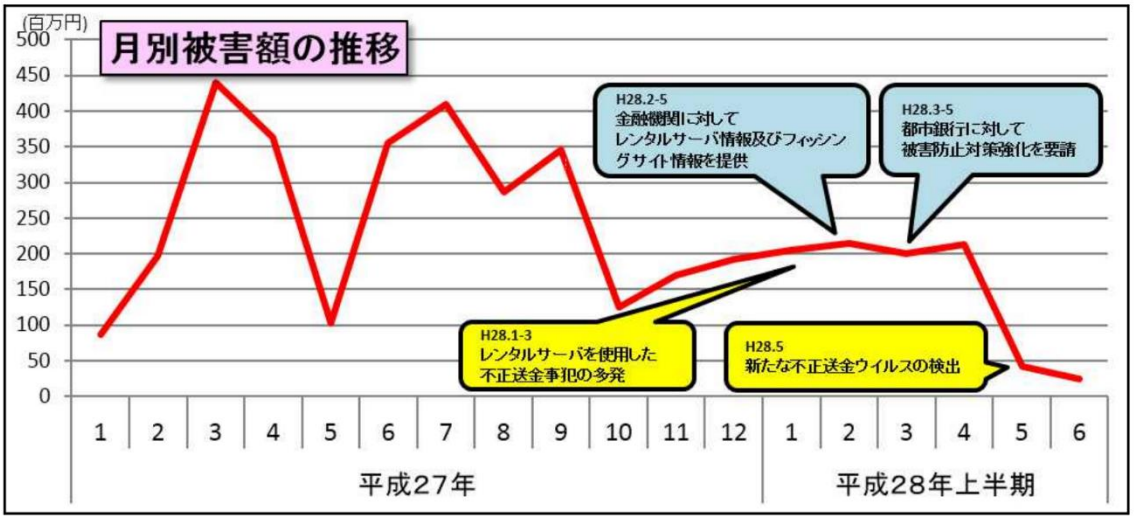

図 1　インターネットバンキングに係る不正送金事犯の発生状況−月別被害の推移

表 1 は警察庁が発表した平成 23 年から平成 26 年におけるサイバー犯罪の検挙数 [2]である。年々増加している傾向がある中で、いずれの年もネットワーク利用犯罪の割合が突出し、続いて不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪の順で割合が高い。

表 1 「検挙数の内訳」

罪名＼年	H23	H24	H25	H26	H27
不正アクセス禁止法違反	248	543	980	364	373
コンピュータ・電磁的記録対象犯罪 不正指令電磁的記録に関する罪	105	178	478	192	240
電子計算機使用詐欺	79	95	388	108	157
電磁的記録不正作出・毀棄等	17	35	56	48	32
電子計算機損壊等業務妨害	6	7	7	8	6
不正指令電磁的記録作成・提供		4	8	9	8
不正指令電磁的記録供用	1	34	14	16	21
不正指令電磁的記録取得・保管	2	3	5	3	16
ネットワーク利用犯罪	5, 388	6, 613	6, 655	7, 349	7, 483
児童買春・児童ポルノ法違反(児童ポルノ)	883	1, 085	1, 124	1, 248	1, 295
詐欺	899	1, 357	956	1, 133	951
うちオークション利用詐欺	389	235	158	381	511
わいせつ物頒布等	699	929	781	840	835
青少年保護育成条例違反	434	520	690	657	693
著作権法違反	409	472	731	824	593
児童買春・児童ポルノ法違反(児童買春)	444	435	492	493	586
脅迫	81	162	189	313	398
商標法違反	212	184	197	308	304
出会い系サイト規制法違反	464	363	339	279	235
その他	863	1, 106	1, 156	1, 254	1, 593
合　　計	5, 741	7, 334	8, 113	7, 905	8, 096

2.1 不正アクセスの禁止等に関する法律（不正アクセス禁止法）の違反

不正アクセス禁止法の違反は、富山県警 HP の Q&A [3]を参考にすると以下の

4 つに分類される。

1. 他人の ID やパスワードを無断入力し、他人になりすます。
2. アクセス制御を回避して、コンピュータのセキュリティホールを攻撃する。
3. 他人の ID やパスワードを無断で第三者に提供し、不正アクセスを助長する。
4. 他人の識別符号を不正に取得・保管・入力要求する。
   いわゆるフィッシング詐欺。

これらの違反は、ゲームや SNS、インターネットバンキングの口座を管理するサーバへの不正なアクセスを行うものであるが、表 1 にあったように平成 27 年の検挙件数では全体の約 4.6%と大きいとは言えない。また、平成 27 年版 犯罪白書 [4]によると表 2 のように、不正アクセスのアクセス元のほとんどが国内からのものであるが、近年ではアクセス元不明も増加している。これは、犯罪手口が巧妙になってきたことを示しており、今後はよりいっそうの警戒が必要であるといえる。

表 2　コンピュータ・電磁的記録対象犯罪等 検挙件数の推移

年次	総数	国内からのアクセス	海外からのアクセス	アクセス元不明
12	106	73	25	8
13	1, 253	258	448	547
14	329	286	13	30
15	212	158	35	19
16	356	303	37	16
17	592	487	53	52
18	946	855	37	54
19	1, 818	1, 684	79	55
20	2, 289	1, 993	214	82
21	2, 795	2, 673	40	82
22	1, 885	1, 755	57	73
23	889	678	110	101
24	1, 251	987	122	142
25	2, 951	2, 474	289	188
26	3, 545	2, 469	298	778

株取引における不正アクセスについては、調査する当初、インターネットバンキングにおける不正アクセスで多いフィッシングサイトを利用した不正送金事件が最も多いと予想した。しかしながら、株取引に特化した事案はほとんどなかった。表 3 は総務省の過去 5 年の不正アクセス行為に係る動機別検挙件数を示したものである [5]。表 3 においてわかることは、不正アクセスの動機の多くが、金銭や資産の操作によって利益を得ることを目的としていないことである。どちらかというと、好奇心や仕返しなど感情的な理由が多くなっている。しかしながら、総務省の証券取引監視委員会の活動状況 [6]にある不正アクセス後の行為の内訳を示した表 4 を見てみると、不正アクセス後の行為においては不正送金が最も多い。これは、好奇心などで不正アクセスをしてみた後、成功したことで次の欲求が出てきたと考えられる。

表 3 「過去 5 年の不正アクセス行為に係る動機別検挙件数」

区分 ＼ 年次	平成 23 年	平成 24 年	平成 25 年	平成 26 年	平成 27 年
好奇心を満たすため	32	85	46	15	76
顧客データの収集等情報を不正に入手するため	15	38	53	139	72
料金の請求を免れるため	0	10	25	2	58
不正に経済的利益を得るため	97	79	706	86	52
嫌がらせや仕返しのため	58	100	56	54	44
オンラインゲームやコミュニティサイトで不正操作を行うため	39	219	77	41	28
その他	1	2	5	1	2
計(件)	242	533	968	338	332

表 4 不正アクセス行為後の行為の内訳

区分 ＼ 年次	平成 25 年	平成 26 年
インターネットバンキングの不正送金	1,325	1,944
他人へのなりすまし	26	1,009
インターネットショッピングの不正購入	911	209
情報の不正入手	92	177
オンラインゲーム、コミュニティサイトの不正操作	379	130
ホームページの改ざん・消去	107	40
インターネット・オークションの不正操作	36	13
不正ファイルの蔵置	20	1
その他	55	22

フィッシング対策協会の緊急情報を 2008 年 6 月 2 日から 2016 年 11 月 27 日まで調べたが、証券会社を対象にしたフィッシングサイトは見られなかった。しかし、住信 SBI ネット銀行や三菱東京 UFJ 証券などグループ企業を対象としたフィッシングサイトは複数見られる [7]など、インターネットバンキングの不正送金事例は表 3 の通り極めて高いことがわかる。つまり株取引においてその資産が最も狙われやすい場所は、証券会社ではなく送金先の銀行であるといえる。

このように、インターネットを使った株式そのものを狙った犯罪行為は極めて低いことが分かった。これは、証券会社が対象とされない理由としては利用者が銀行に比べて少ないこと、資産が有価証券の形で保有されており現金化して引き出すまでの手順が複雑であることが関係していると考察する。

表 5 は、総務省の平成 27 年不正アクセス行為の発生状況 [5]にある過去 5 年の不正アクセス行為に係る手口別検挙件数である。フィッシングサイトやスパイウェア、セキリュティ・ホール型攻撃などの高度な技術を利用した不正アクセスの検挙数は少ない。一方で最も多いものは、利用者のパスワードの設定・管理の甘さにつけ込んだものとなっており、簡単な防御策を講じるだけで大きく被害を防ぐことができる可能性を示している。

表 5　過去 5 年の不正アクセス行為に係る手口別検挙件数

区分＼年次	平成 23 年	平成 24 年	平成 25 年	平成 26 年	平成 27 年
識別符号窃用型(件)	241	532	965	336	331
利用者のパスワードの設定・管理の甘さにつけ込んだもの	59	122	767	84	117
インターネット上に流出・公開されていた識別符号を入手したもの	1	6	9	34	57
識別符号を知りえる立場にあった元従業員や知人等によるもの	52	101	56	47	51
言葉巧みに利用者から聞き出した又はのぞき見たもの	29	229	64	53	46
フィッシングサイトにより入手したもの	59	18	9	71	24
スパイウェア*等のプログラムを使用して識別符を入手したもの	1	29	25	6	15
他人から入手したもの	37	16	33	25	13
その他	3	11	2	16	8
セキュリティホール型攻撃(件)	1	1	3	2	1

これまでに述べたように、不正アクセスの大半は、管理の甘さにつけ込んで行われる。フィッシング対策協議会の 2016 年度版「利用者向けフィッシング詐欺対策 ガイドライン」 [8]を見ても「怪しいメールに注意しましょう」「正しい URL にアクセスする」「パソコンを安全に保ちましょう」の 3 つがフィッシング対策の心得として挙げられている。

表 6 は全国銀行協会によるアンケートの結果 [9]である。全国銀行協会の申し合わせ [10]では、預金者が無過失の場合インターネットバンキングであっても全額補償するよう定められている。この補償率は表 6 を見てもわかるように、預金者の過失割合によって保証額が無過失で 100%、重過失で 0%までの増減があるが、おおよそ 90%を超えている。普段から注意して不正アクセスへの対策を講じることが、不正送金された際の過失割合を低減し、補償額の増減においても有用である。

表 6 インターネットバンキングによる預金等の不正払戻しにかかる補償件数等について

【個人顧客】(対象:正会員・準会員 189 行、単位:件、百万円)

時期		対応方針決定済案件(①)	うち補償件数(②)	補償率(①÷②)
平成 26 年度		1,51	991	94.3%
	平成 26 年 4 月~ 6 月	423	390	92.2%
	平成 26 年 7 月~ 9 月	256	248	96.9%
	平成 26 年 10 月~12 月	201	193	96.0%
	平成 27 年 1 月~ 3 月	171	160	93.6%
平成 27 年度		1,04	1,85	98.3%
	平成 27 年 4 月~ 6 月	276	266	96.4%
	平成 27 年 7 月~ 9 月	253	249	98.4%
	平成 27 年 10 月~12 月	160	160	100.0%
	平成 28 年 1 月~ 3 月	414	410	99.0%
平成 28 年度		249	232	93.2%
	平成 28 年 4 月~ 6 月	211	196	92.9%
	平成 28 年 7 月~ 9 月	38	36	94.7%

警察庁の H28 年の広報資料「平成 28 年上半期におけるインターネットバンキングに係る 不正送金事犯の発生状況等について」によると表 7 のように不正送金の被害にあった口座名義人のセキュリティ対策の実施状況では、ワンタイムパスワードの利用および非利用の割合は約 1:3 となっている。これを見ると、

確かにワンタイムパスワードの利用は不正送金の被害を防ぐ上で有用であるといえるが、約 30%の利用者がワンタイムパスワードを利用しながら不正送金の被害にあっているため、それだけを頼りにしてはいけないこともわかる。

表 7　不正送金被害に係る口座名義人のセキュリティ対策実施状況

	利用していた		利用していない		不明		合計
ワンタイムパスワード(個人口座)	255	31.4%	490	60.4%	66	8.1%	811
電子証明書(法人口座)	0	0%	42	91.3%	4	8.7%	46

このように、利用者の対策を強化するだけでは、不正送金への万全の体制を敷くことは難しい。未だインターネットとそのセキュリティは不完全で発展途上の技術であることを認識し、常に最新で正確な情報をもとにリスクを判断し、適宜対策をとることが求められる。

2.2 コンピュータ・電磁的記録対象犯罪および不正指令電磁的記録に関する罪

コンピュータ・電磁的記録対象犯罪および不正指令電磁的記録に関する罪を分類すると、以下の 6 つになる。これらは、不正な記録やデータの作成、削除、変更、使用や不正な指令をコンピュータに与える犯罪である。具体的には偽造クレジットカードでのネットショッピングやコンピュータウイルスの作成等を指す。表 1 を見ると、平成 26 年、平成 27 年ともに検挙件数は全体の 2~3%の状況である。

1. 電子計算機使用詐欺
2. 電磁的記録不正作出・毀棄等
3. 電子計算機損壊等業務妨害
4. 不正指令電磁的記録作成・提供
5. 不正指令電磁的記録共用
6. 不正指令電磁的記録取得・保管

表 8 は平成 27 年版犯罪白書 [4]にあるコンピュータ・電磁記録対象犯罪等の検挙件数の推移を示した表である。コンピュータ・電磁的記録対象犯罪が年々増加傾向にあり、支払用カード電磁的記録に関する罪では近年若干の減少傾向が見られる。また不正アクセス禁止法と比べると検挙数自体が少なく年ごとの増減も少ないことが分かる。

表 8　コンピュータ・電磁記録対象犯罪等　検挙件数の推移

年　次	コンピュータ・電磁的記録対象犯罪	支払用カード電磁的記録に関する罪	不正アクセス禁止法
12 年	44	…	67
13	63	…	67
14	30	277	105
15	55	459	145
16	55	555	142
17	73	502	277
18	129	319	703
19	113	298	1, 442
20	247	277	1, 740
21	195	259	2, 534
22	133	192	1, 601
23	105	286	248
24	178	169	543
25	478	95	980
26	192	125	364

この犯罪の特徴は、高い技術が求められるか、内部犯である可能性が高いかである。これは不正アクセスと類似する。またその性質から、不正アクセス後にコンピュータ・電磁的記録対象犯罪等に及ぶこともある。この犯罪は、個人が被害を受けるとき有効な対策を立てることは困難であるが、同様に犯行自体も困難なためリスクとしてはさほど高いとは考察する。

２.３ ネットワーク利用犯罪

サイバー犯罪の中でも割合が高いものがネットワーク利用犯罪である。インターネットを利用した犯罪であるため対象範囲が極めて広く、ブログや SNS、インターネット掲示板、オークションサイトの利用など身近な情報発信手段を用いた犯行である。必ずしも高度な技術が必要では無いということがこの犯罪の特徴である。

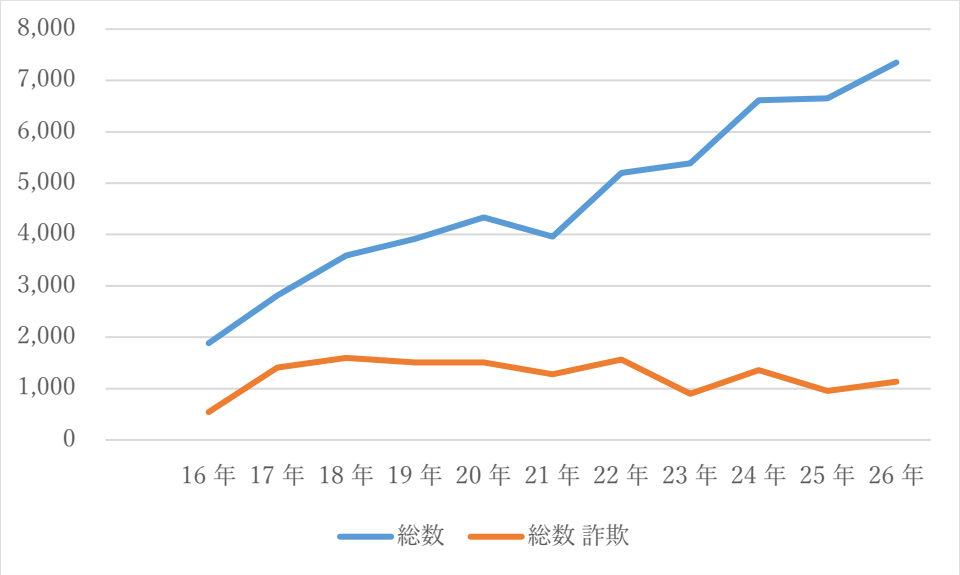

図 2　ネットワーク利用犯罪　検挙件数の推移

図 2 は平成 23 年版警察白書にあるネットワーク利用犯罪の検挙数の推移を元に作成したグラフである。ネットワーク利用犯罪自体は増加しているものの、その中に占める詐欺行為の検挙数は下降傾向にあり、ネットワーク利用犯罪の傾向が大きく変化していることがわかる。

第３章

有価証券の取引等の規制

証券取引における犯罪等を取り締まる法令には、金融商品取引法や有価証券の取引等の規制に関する内閣府令などがある。これらの法令では、相場操縦行為およびインサイダー取引、風説の流布について禁止をしている。

表 9 は証券取引等監視委員会事務局が平成 28 年 7 月に公表した「金融商品取引法における課徴金事例集~不公正取引編~」 [11]にある課徴金勧告件数と課徴金額の推移である。内部者取引では年度によってそれほど変化はないが、相場操縦行為に関して言えば、近年は増加傾向にあるといえる。

表 9　課徴金勧告件数と課徴金額の推移

年度	勧告件数(件)・課徴金額(円)					
			内部者取引		相場操縦行為	
	件数	課徴金額	件数	課徴金額	件数	課徴金額
17	4	1, 660, 000	4	1, 660, 000	0	0
18	11	49, 150, 000	11	49, 150, 000	0	0
19	16	39, 600, 000	16	39, 600, 000	0	0
20	18	66, 610, 000	17	59, 160, 000	1	7, 450, 000
21	43	55, 480, 000	38	49, 220, 000	5	6, 260, 000
22	26	63, 940, 000	20	42, 680, 000	6	21, 260, 000
23	18	31, 690, 000	15	26, 300, 000	3	5, 390, 000
24	32	135, 720, 000	19	35, 150, 000	13	100, 570, 000
25	42	4, 608, 060, 000	32	50, 960, 000	10	4, 557, 100, 000
26	42	563, 342, 935	31	38, 820, 000	11	524, 522, 935
27	35	191, 835, 000	22	75, 500, 000	13	116, 335, 000
28	3	25, 400, 000	2	5, 750, 000	1	19, 650, 000
合計	290	5, 832, 487, 935	227	473, 950, 000	63	5, 358, 537, 935

３.１ 相場操縦行為

相場操縦行為には、見せ玉、仮装売買、馴合売買、終値関与、買い上がり、作為的相場形成などがある。JPX 日本取引所グループ HP [12]によれば相場操作は「市場において相場を意識的、人為的に変動させ、その相場をあたかも自然の需給によって形成されたものであるかのように装い、他人を誤認させ、その相場の変動を利用して自己の利益を図ろうとするもの」と定義されている。この行為は、金融商品取引法により刑罰や課徴金等の罰則が科されることがある。

証券監視委の「証券取引等監視委員会の活動状況」 [13]では、以下 2 点が相場操作を行う要因・背景として挙げられている。

- インターネット取引の普及及び発注システムの進歩等により、個人投資家であっても、迅速かつ大量の発注・取消が可能となっているため、見せ玉等の手法を用いて人為的に相場を変動させれば、容易に売買差益を稼げる、又は損失回避を図ることができるとの誘惑 。
- 仮装・馴合売買等を用いて人為的に相場を変動させる行為が法令違反になるとの 認識が不足 、市場では膨大な取引が行われているため、個人が行う小規模の相場操縦行為まで は市場監視の目も届かないだろうとの誤解。

この主張によれば、インターネットの発展が相場操縦行為の助長の要因といえ、それは表 9 の件数推移から裏付けられる。また、同資料には「見せ玉と同時にインターネット掲示板に当該銘柄の買い付けを推奨する多数の書き込みがあった」との記述も見られる。このことから、相場操縦行為がインターネットを利用して行われていることがわかる。

３.２ インサイダー取引

JPX 日本取引所グループ HP によれば、インサイダー取引を「上場会社の関係者等が、その職務や地位により知り得た、投資者の投資判断に重大な影響を与える未公表の会社情報を利用して、自社の株券等を売買する行為」と定義している。未公開の情報を知り得る立場の者は、一般の投資家に比べて著しく有利であるため、インサイダー取引は投資の不公平を招く。表 9 の勧告件数を見ても、どの年度も一定数発生しており、特に法則性といったものを見つけるのは難しい。しかしながら、「証券取引等監視委員会の活動状況」によると、「金融商品取引等の国際化、高度化、複雑 化等を背景として、不公正取引も一段と複雑化、悪質・巧妙化してきている」とあるため、実際は増えてきている可能性もある。なお、インサイダー取引の要因・背景として、表 10 に示すように違反行為者側の問題と上場会社等の問題が考えられる。

表 10　インサイダー取引の要因・背景

違反行為者側の心理要因	上場会社等の問題
● 重要事実に基づいて株式を売買すれば確実に儲けられる ● 膨大な取引が行われており自分の取引は見つからないだろう ● 自己名義口座では取引できなくても、他人名義口座を利用すれば大丈夫だろう ● 自分は取引できなくても、親しい友人には儲けさせてあげたい	● 内部管理態勢や情報管理体制等の不備 ● 役職員のインサイダー取引を誘引 ● 経営陣の認識不足により、取引先等に重要事実を伝達することが付き合いだという誤解

３.３ 風説の流布・偽計

JPX 日本取引所グループ HP によれば、風説の流布とは「株券等の相場の変動を図る目的をもって、虚偽の情報等(風説)を流布すること」、偽計は「また、有価証券の募集、売買等のため、もしくは相場の変動を図る目的をもって、他人に錯誤を生じさせる詐欺的ないし不公正な策略、手段を用いること」とある。

表 11 は証券取引監視委員会の「犯則調査告発の実施状況(平成 28 年 10 月末現在)」 [14]にある告発状況である。どれも毎年一定数の告発がされており、特徴を見ることは難しい。しかしながら、平成 4 年～21 年では風説の流布が最も少ないのに対し、平成 22 年～平成 28 年を見ると 10 件であり、相場操縦・相場固定よりも高い。このことから、近年の風説の流布は増加傾向にあるといえる。

表 11　告発の実施状況(平成 28 年 10 月末現在)（単位:件）

年度	4～21	22	23	24	25	26	27	28
合計	134	8	15	7	3	6	8	4
有価証券報告書等の虚偽記載等	30	2	4	0	0	2	3	0
風説の流布・偽計	16	1	4	1	1	1	2	0
相場操縦・相場固定	20	1	1	0	1	2	1	3
インサイダー取引	61	4	6	2	1	1	2	1
その他	7	0	0	4	0	0	0	0

また近年では電子掲示板や SNS を利用した個人による犯行も発生している。証券取引監視委員会 HP [15]より証券取引等監視委員会が 3 月 19 日に金融商品取引法違反(風説の流布)の嫌疑で名古屋地方検察庁に告発した事例を以下に紹介する。

1. 告発の対象となった犯則事実

犯則嫌疑者は、別紙一覧表 1 ないし 3 記載のとおり、大阪証券取引所市場第二部に上場されていたカネヨウ株式会社ほか 2 社の株券の売買のため、及び相場の変動を図る目的をもって、平成 25 年 1 月 23 日頃から同年 2 月 18 日頃までの間、犯則嫌疑者が代表を務める会社の所在地において、パーソナルコンピューターを操作し、インターネットを介し、サーバーコンピューターの記憶装置に文字データを記録させる方法により、「株式研究掲示板」又は「Y 氏と愉快な仲間の株式掲示板」と題する電子掲示板に、合理的な根拠もないのに、「明日の暴騰仕掛け銘柄　3209 カネヨウが暴騰するという情報が入ってきました」、「倍増へ向けての暴騰仕掛け株　6775　TB グループに暴騰仕掛けが入るとの情報です」、「爆発二桁銘柄　今日の暴騰仕掛け入るとの情報株は 6862 ミナトエレクトロンです。決算黒字転換、為替レート 80 円換算ということから次は大幅黒字上方修正期待高まり株価大幅水準訂正へ始動開始。」などと書き込んで不特定かつ多数の者が閲覧できる状態に置き、もって、それぞれ有価証券の売買のため、及び有価証券の相場の変動を図る目的をもって、風説を流布したものである。

この事例は電子掲示板を利用した犯則事例である。本件で着目すべきは「嘘の情報を断定的に書き込んだこと」である。株取引において他の投資家とコミュニケーションをとり情報交換することは情報を入手する手段として有効であるが、インターネット上の情報は不確実なものが溢れていると認識し、信頼できるソースで確認する必要がある。

また、自らがインターネットへ情報発信をする際には、それが瞬時に世界中へ発信されるものと自覚して、送信の前にしっかりと内容を確認すべきである。風説の流布については相場の変動を目的としたものであるが、たとえ相場の変動を目的にしない書き込みであったとしても偽計業務妨害に抵触する恐れもある。他にも自己の書き込みで変動操作につながらないかなど注意深く確認すべきである。このようにインターネット上での発言においては、いわゆるネットリテラシーの順守が求められているのである。

第４章

問題と対策

インターネットバンキングの不正アクセス事案など、株取引に関するサイバー犯罪は、インターネットの発展とユーザー数の増加とともに件数が増加している。株取引をする上で、インターネットは直接的な取引手段としてだけでなく、情報収集の手段としても必須である。

このように、インターネットによる情報発信と情報収集は今や一般の人々が日常的に行う行為となった。しかしながら、それに伴うネットリテラシーが完全に定着したとは言い難い。すべての人が誤解の無いよう悪意を持たずに文章を書いている保障はない。むしろインターネットにあふれる情報の大半は不確かなもので信頼性の低い情報である。よって情報の取捨選択が重要な問題となる。

特にフィッシングサイトやフィッシングメールなど、株取引に関わる詐欺については、これらを警告してくれるシステムを活用するなど、ある程度の対策を利用可能ではあるものの、結局のところ個人がそれぞれ気を付けてインターネットを使うことが重要である。

４.１ フィッシングサイト

フィッシングサイトとは、ID やパスワードの窃取を目的とした偽の web サイトを用いたシステムのことである。フィッシング対策協議会では「フィッシング（Phishing）とは、金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為です。電子メールのリンクから偽サイト （フィッシングサイト） に誘導し、そこで個人情報を入力させる手口が一般的に使われています。」と書かれている。

図 3 は TechTarget ジャパン [16]が紹介しているフィッシングサイトの例である。このように、一見すると違いがわからないものであるため、無意識のうちに ID やパスワードなどの重要な情報を入力してしまうことがある。

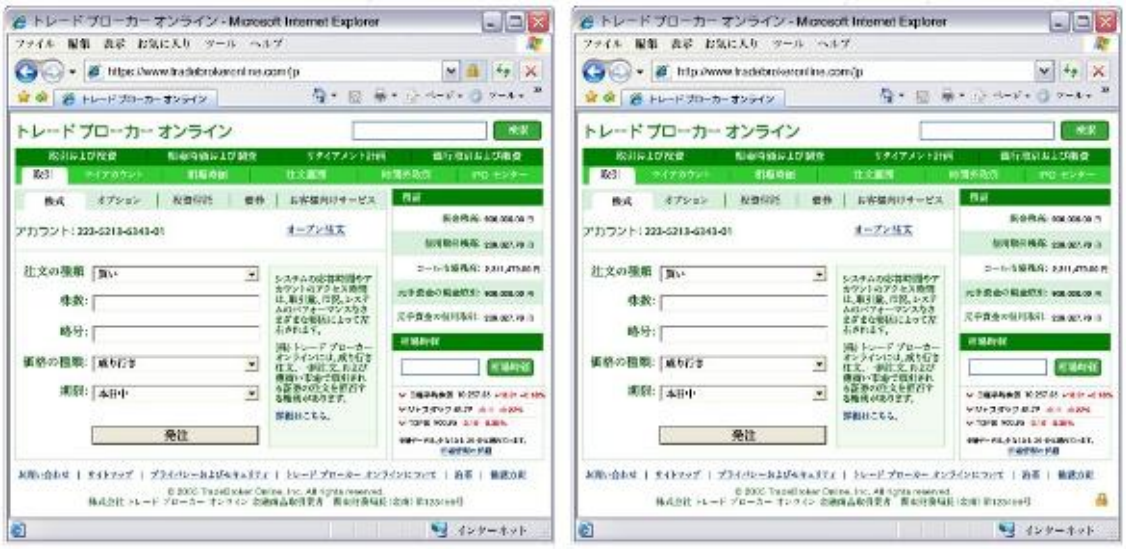

図 3　フィッシングサイトの例

図 4 は、フィッシング対策協議会が公表しているフィッシングサイトの報告件数を示したグラフ [17]であり、図 5 はフィッシング対策協議会のフィッシングサイトに悪用されたブランド件数である。毎月数百件のフィッシングサイトの URL 件数が存在しており、その数は増減を繰り返しているが、現在は減少傾向に転じていることがわかる。フィッシングサイトの対象は銀行だけでなくメールやラインなどの通信系、ショッピングサイト、ゲームなど多岐に渡っている。

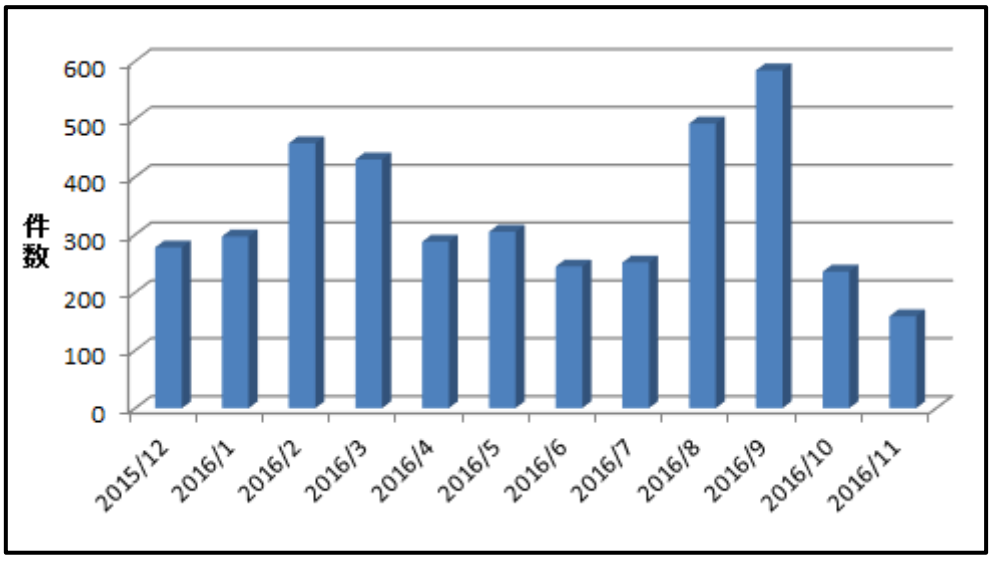

図 4　フィッシングサイトの URL 件数

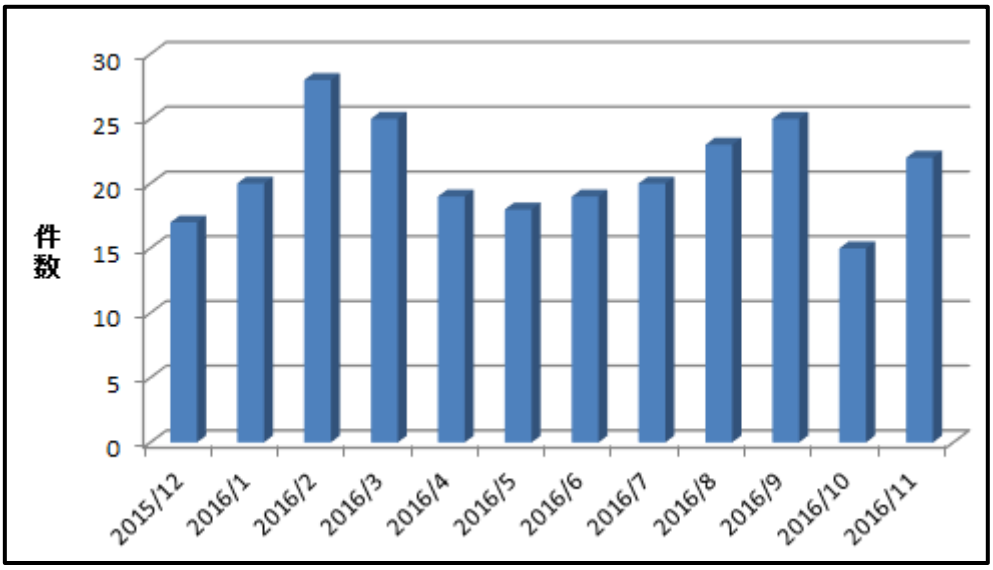

図 5　フィッシングに悪用されたブランド件数

フィッシングサイトを用いた犯罪の手口は、フィッシングサイトの URL を含むフィッシングメールを送信するか、コンピュータウイルスを用いて利用者に正規のサイトと誤認させることから始まる。犯罪に遭わない対策方法としては次のようなことが有効である。

1. 正規のサイトをアクセスした際にブックマークに追加し、以降はブックマークからしかサイトにアクセスしない。
2. 送られてきたメールやメッセージにあるリンクを安易にクリックしない。
3. ブラウザに正規の URL を直接入力し、アクセスする。
4. 表示されたページの電子証明書の確認をする。

しかしながら、DNS キャッシュポイズニングを行ったり、フィッシングサイトが SSL 証明書を取得していたりと、これらの対策方法を回避してくるフィッシングサイトの存在も確認されている。DNS キャッシュポイズニングでは、利用者が正確な URL を入力してもキャッシュを上書きされ別の有害 web サイトに接続されてしまう。この攻撃を受けるとフィッシングサイトへのアクセスを防ぐことは難しくなる。また SSL 証明書も承認局がチェックを行っているものの稀にフィッシングサイトに SSL 証明書が発行されている事案もあり、URL の隣の鍵のマークだけ見て安心してはいけない。そのほかにも新しい手法でフィッシングサイトへと誘導される可能性はあり、誰であってもゼロデイ攻撃に対処することは難しい。このように、様々な種類と手口および偽装手段が存在するフィッシングサイトへの対処は、常にイタチごっこの様相を呈しており、対策は常に不十分な状態である。その中で、常に最新の情報を集め、それをもとに最善の対策をとることが、株取引を行う上では必要である。

４.２ フィッシングメール

前項で述べたように、フィッシングサイト自体はただの web ページである。正規のサイトと間違ってアクセスされない限りは、犯罪行為は行われない。つまりフィッシングサイトは、獲物を狙った疑似餌であり、それに食いつく獲物を待っている状態である。そのため、フィッシングサイトには利用者がアクセスしたくなるような仕掛けがあり、何らかの誘導の手段と併用して運用されるのが一般的である。


こんにちは！

（2015年11月28日更新）「住信SBIネット銀行」のシステムが安全性の更新がされたため、
お客様はアカウントが凍結?休眠されないように、直ちにアカウントをご認証ください。

以下のページより登録を続けてください。

https://www.netbk.co.jp/wpl/NBGate/iO1O1O1CT/DIO1O10215
<http://www.netbk.co.jp.●●●●.date/wpl/NBGate/iO1O1O1CT/DIO1O10215/>

――Copyright (C) 2015 SBI Sumishin Net Bank――

図 6　偽メールの内容

図 6 は、住信 SBI ネット銀行のサイト [18]の注意喚起を促す文章にあるフィッシングメールの画像である。文章中に「?」が使われていたり違和感を覚える文章であるが、他にはあまり疑問を抱かせる箇所はない。フィッシングメールの文章として見られる特徴は、パスワードの変更、不正ログインの通知といったセキュリティの不安を煽る傾向が見られることである。不安を煽ることで正常な判断を失わせ、緊急の事態であると思わせて、考える間もなくアクセスをさせることを目的としている。メールの差出人の偽装は簡単にできるため、差出人のみを見て判断することはできない。

フィッシングメールを看破できれば、フィッシングサイトの被害に遭う可能性を格段に低減することが可能である。メールの文章構成や署名などから違和感を感じとること、他の詐欺行為と同じように焦らず冷静に考え他人に相談することなどが有効な対策であるといえる。

４.３ インターネットセキュリティ

この節ではインターネットセキュリティ面における証券取引の安全性の確保の方法について論じる。

日本銀行の資料 [19]によると、ネットバンキングを使った不正払出の手口は、フィッシングサイトの利用、コンピュータウイルスの利用またはそれらの複合とある。コンピュータウイルスの対策については、ワクチンソフトの利用、定期

的なアップデート、パスフレーズの活用など多種多様な対策が存在するが、いずれにおいても一つも完全なものがないことはこれまでに述べた通りである。一般の個人投資家にとって取れる対策は、ワクチンソフトを入れた後は、定期的なアップデートおよび銀行の HP に紹介されたセキュリティを設定するほかない。ここでは銀行側の対策について住信 SBI ネット銀行を例にとり解説する。

- パスワードの設定
  設定すべきパスワードとして、ログインパスワード、取引パスワード、認証番号表またはスマート認証の三種、さらに ATM からの引き出し時にキャッシュカードの暗証番号が用意されている。これらのパスワードによって口座が保護されているということである。スマート認証はワンタイムパスワードである。
- その他の対策
  セキュリティ対策の紹介として、SSL/TLS123bit 暗号化による通信、EV SSL 証明書の利用、電子署名付き電子メール(S/MIME)、フィッシング対策ソフト、ファイアウォール、サーバシステム管理が挙げられている。フィッシング対策ソフトは利用者に無償で配布している。

上記の通り、住信 SBI ネット銀行では、一般的な対策を一通り揃えてある。他のネットバンクでも、多少の差異はあるものの、おおむね同様の対策をとっている。

第５章

まとめ

本研究では、株取引におけるサイバー犯罪の実態を解明してきた。不正アクセスにおいてはその多くが国内からの接続であり、コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪では、犯罪をおこすにはそれほど高い技術力が必要とされていないことがわかった。サイバー犯罪の中では、株取引そのものが犯行の対象とされる事案では、ネットバンクなどを狙ったネットワーク利用犯罪が圧倒的な割合の高さであった。有価証券の取引等の規制では、インサイダー取引を除くと、相場操縦や風説の流布などにおいてインターネットとコンピュータの発展に併せて告発事例数の増加が見られる。SNS や電子掲示板といった情報発信手段がより身近になったことが原因として挙げられる。株取引とサイバー犯罪双方の視点から合わせて見るとインターネットを利用した犯罪者がどのように投資家を狙っているか顕著にわかる。投資家が自らを優位に立たせるための犯罪は数的に少数である。さらに不正送金事件は投資家を狙った犯罪というよりもインターネットバンキングの利用者を狙った犯罪に巻き込まれた結果といえる。

対策としては、不正アクセスにおいてはパスワードの複雑化やワンタイムパスワードの利用など多々対策はあるものの、完全に防ぐための防御手段は現在存在していない。もし被害にあったとしても、全国銀行協会の「預金等の不正な払戻しへの対応」があり、利用者に過失がなければ全額の補償が約束されているが、過失割合の低減の為かつ不正送金等の被害に遭わないためにも最新の情報を基にした各種対策を講じる必要がある。フィッシングサイトではその手口はイタチごっこの状況となっており完全な対策を確立することは極めて困難なことであると分かった。各種の証明書やアクセス方法による対処方法も述べたが、既にこれらの偽造事件もあり対処は最新の情報に基づいて実行する必要がある。つまりは自己防衛的手段に頼らざるを得ないというのが実情である。

株取引においてサイバー犯罪に遭わないために最も重要なことは、常に最新の正確な情報を入手し、それに合わせて自らができることを最大限行い、注意深くシステムを利用することである。

引用・参考文献

[1] 警察庁, “平成 28 年上半期のインターネットバンキングに係る 不正送金事犯の発生状況等について,” [オンライン].
Available: https://www.npa.go.jp/cyber/pdf/H280908_banking.pdf. [アクセス日: 10 1 2017].

[2] 警察庁, “平成 27 年におけるサイバー空間をめぐる脅威の情勢について,” [オンライン].Available: http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf. [アクセス日: 22 11 2016].

[3] 富山県警, “不正アクセス禁止法 Q&A,” [オンライン].
Available: http://police.pref.toyama.jp/sections/6110/high-tech/fusei.html#2. [アクセス日: 22 11 2016].

[4] 法務省, “平成 27 年版 犯罪白書 第 1 編/第 3 章/第 3 節/1,” [オンライン].
Available: http://hakusyo1.moj.go.jp/jp/62/nfm/n62_2_1_3_3_1.html#h1-3-3-02. [アクセス日: 22 11 2016].

[5] 総務省, “不正アクセス行為の発生状況 平成 27 年,” [オンライン]. Available: http://www.soumu.go.jp/main_content/000404563.pdf. [アクセス日: 22 11 2016].

[6] 総務省, “不正アクセス行為の発生状況 平成 26 年,” [オンライン]. Available: http://www.soumu.go.jp/main_content/000347975.pdf. [アクセス日: 22 11 2016].

[7] フィッシング対策協議会, “緊急情報一覧,” [オンライン]. Available: https://www.antiphishing.jp/news/alert/. [アクセス日: 22 11 2016].

[8] フィッシング対策協議会, “利用者向けフィッシング詐欺対策,” [オンライン].
Available:
https://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf. [アクセス日: 22 11 2016].

[9] 全国銀行協会, “インターネット･バンキングによる預金等の不正払戻し」等に関するアンケート結果,” [オンライン].
Available: http://www.zenginkyo.or.jp/fileadmin/res/news/news281129_2.pdf. [アクセス日: 22 11 2016].

[10] 全国銀行協会, “インターネットバンキングに係る補償の対象・要件・基準等について,” [オンライン].
Available: http://www.zenginkyo.or.jp/fileadmin/res/news/news200219_4.pdf. [アクセス日: 22 11 2016].

[11] 証券取引等監視委員会事務局, “金融商品取引法における課徴金事例集~不公正取引編~,” [オンライン].
Available: http://www.fsa.go.jp/sesc/jirei/torichou/20160728/01.pdf. [アクセス日: 22 11 2016].

[12] 日本取引所グループ, “日本取引所グループ,” [オンライン].
Available: http://www.jpx.co.jp. [アクセス日: 22 11 2016].

[13] 証券取引監視委員会, “証券取引等監視委員会の活動状況,” [オンライン]. Available: http://www.fsa.go.jp/sesc/reports/n_27/n_27a.pdf. [アクセス日: 22 11 2016].

[14] 証券取引監視委員会, “犯則調査告発の実施状況(平成 28 年 10 月末現在),” [オンライン]. Available: http://www.fsa.go.jp/sesc/actions/koku_joukyou.htm. [アクセス日: 22 11 2016].

[15] 証券取引等監視委員会, “電子掲示板を悪用した風説の流布事件の告発について,” [オンライン]. Available: http://www.fsa.go.jp/sesc/news/c_2014/2014/20140319-1.htm. [アクセス日: 22 11 2016].

[16] TechTarget 編集部, “TechTargetJapan,” [オンライン].
Available: http://techtarget.itmedia.co.jp/tt/news/1108/01/news02.html. [アクセス日: 17 1 2017].

[17] フィッシング対策協議会, “2016/11　フィッシング報告状況,” [オンライン].
Available: https://www.antiphishing.jp/report/monthly/201611.html. [アクセス日: 22 11 2016].

[18] 住信 SBI ネット銀行, “【重要】住信 SBI ネット銀行を装ったフィッシングメールにご注意ください,” [オンライン].
Available:
https://www.netbk.co.jp/wpl/NBGate/i900500CT/PD/mg_notice_151130_info. [アクセス日: 22 11 2016].

[19] 日本銀行金融研究所情報技術センター, “ネットバンキングのセキュリティ,” [オンライン].
Available:
https://www.boj.or.jp/announcements/release_2014/data/rel141226a3.pdf. [アクセス日: 22 11 2016].