

情報漏えいインシデント対応方策に関する 調査報告書

平成 19 年 5 月

独立行政法人 情報処理推進機構

調査委託先 財団法人ひょうご情報教育機構
(カーネギーメロン大学日本校)

情報漏えいインシデント対応方策に関する調査委員会名簿

(五十音順・敬称略)

調査委員（報告書執筆者）

(座長)	高橋 郁夫	IT 法律事務所
	新井 悠	株式会社ラック
	小山 覚	Telecom-ISAC Japan
	武田 圭史	カーネギーメロン大学日本校
	寺田 真敏	株式会社日立製作所
	平林 実	NTT コミュニケーションズ株式会社

謝辞

本報告書各章の執筆にあたり専門領域の経験に基づく知見等を得るために下記の組織・個人の方々にヒアリングのご協力を得た。本報告書の重要な個所において彼らの貢献は多大なものとなった。ここに感謝の意を表する。

ヒアリングに御協力いただいた組織・人物（五十音順）

- ・石川 慶子 氏
- ・株式会社インターリスク総研
- ・ウエバー・シャントウイック・ワルト・ワイド株式会社
- ・警察庁
- ・総務省
- ・株式会社ネットエージェント
- ・株式会社ぷららネットワークス

本調査委員会において活発な議論に参加していただいた有志のオブザーバの諸氏にも感謝する。

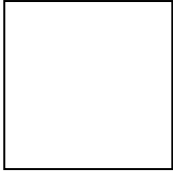
- 目 次 -

	Page
本編.....	1
序.....	2
第1 情報漏えい対応の定義・態様.....	4
1 情報漏えいの概念.....	4
1.1 情報漏えい事件とインシデント・レスポンス.....	4
1.2 情報の種別.....	5
1.3 漏えいの概念.....	5
1.4 対応の概念と各ステップ.....	5
2 本報告の基本的な立場について.....	7
2.1 中小企業と情報漏えい事件対応チームの責任者.....	7
2.2 基本的な視点について.....	8
3 情報漏えいの態様について.....	11
3.1 紛失・盗難.....	11
3.2 誤送信・Web での誤公開等.....	11
3.3 内部犯行.....	11
3.4 Winny/Share ネットワークへの漏えい.....	11
3.5 不正プログラム.....	12
3.6 不正アクセス.....	12
3.7 ブログ掲載・風評等.....	12
4 情報の分類.....	12
4.1 企業（組織）の情報とその種別.....	12
4.2 個人情報とその種別.....	12
第2 事件事例の調査分析.....	14
1 調査分析の概要.....	14
2 調査分析手法.....	14
2.1 情報漏えい事例の収集.....	14
2.2 情報漏えい態様、事後対応及び事故後経過の分類.....	15
3 調査結果.....	22
3.1 調査データの概要.....	22
4 分析結果.....	33
4.1 分析結果の概要.....	33

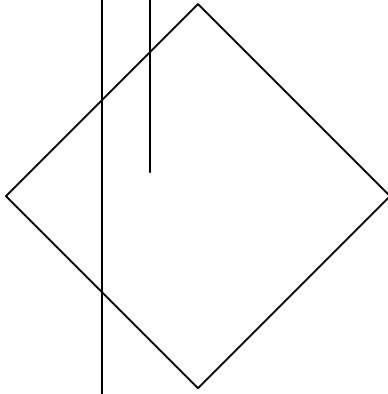
4.2	対応ステップに関する傾向	33
4.3	漏えい態様毎の分析	41
4.4	漏えい情報のタイプの留意事項	43
第3	情報漏えい対応策	44
1	情報漏えい対応の枠組みと基礎	44
1.1	情報漏えい対応ポリシーの必要性	44
1.2	情報漏えい対応の目標	47
1.3	情報漏えい対応の諸原則	48
2	情報漏えい対応の具体的な段階	51
2.1	準備段階	51
2.2	発見および報告	57
2.3	初動対応	60
2.4	調査	65
2.5	通知・報告・公表等	75
2.6	抑止措置と復旧	87
2.7	事後対応	90
第4	情報漏えい対応のまとめ	97
1	情報漏えいパターン別対応フロー ～紛失・盗難～	97
2	情報漏えいパターン別対応フロー ～誤送信・Web 誤公開等～	98
3	情報漏えいパターン別対応フロー ～内部犯行～	99
4	情報漏えいパターン別対応フロー ～Winny/Share 等への漏えい～	100
5	情報漏えいパターン別対応フロー ～不正プログラム～	101
6	情報漏えいパターン別対応フロー ～不正アクセス～	102
7	情報漏えいパターン別対応フロー ～その他（風評・ブログ掲載）～	103
8	全般的な留意事項	104
9	事後告知、謝罪などの構成例	104

付録編	105
付録1 Winny (P2Pネットワーク) とインターネットの関係	106
はじめに	106
1 P2Pファイル交換ソフトが形成するネットワークについて	106
1.1 プライベートネットワークとP2Pネットワークの比較	106
1.2 オーバーレイネットワークとしてのP2Pネットワーク	107
2 P2Pファイル交換ネットワークの問題点	109
2.1 権利侵害(著作権)	110
2.2 情報漏えい	110
2.3 ウイルスの流通	111
3 P2Pネットワークがインターネットに及ぼす影響	115
3.1 大量の通信	115
4 今後に期待すること	118
付録2 Winnyネットワークの特性および情報漏えい対応に影響を与える特殊性について	120
1 Winnyの概念	120
1.1 Winnyプログラムとは	120
1.2 Winnyの匿名性について	120
1.3 Winnyの効率性について	121
2 Winnyネットワークの実態および特性	121
2.1 Winnyネットワークとは	121
2.2 Winnyネットワークにおける通信内容	121
2.3 Winnyネットワークの変容性	121
2.4 漏えい情報収集家(コレクター)の存在	121
3 Winnyネットワークの特性が情報漏えい対応に与える影響	122
3.1 Winnyネットワークにおける流出情報	122
3.2 Winnyネットワークにおける流出情報対応について	122
3.3 漏えい対応における特殊事情	123
4 Winny漏えい対策について	123
4.1 Winny漏えい対策の傾向	123
4.2 現時点における対応策の限界	124
付録3 Winnyトラフィックの制限と通信の秘密	125
序	125
1 3月16日のプレスリリースに至る経緯	125
2 「通信の秘密」との関係	127
3 その後のぶららの対応	129
4 示唆するもの	129

付録4 Winnycをめぐり法律問題の概観	131
1 Winnycをめぐり法律問題とは	131
1.1 概念	131
1.2 Winnycネットワークの利用に関する問題	131
1.3 暴露ウイルスによる情報漏えいの責任問題	131
1.4 Winnycネットワークによる情報漏えい対応および防止のための法律問題	131
1.5 Winnycネットワークの抑制に関する法律問題	132
2 Winnycネットワークの利用に関する問題点	132
2.1 Winnyc利用の法的問題の所在	132
2.2 著作権との関係	132
2.3 その他の観念	135
3 Winnycネットワークによる情報漏えい対応および防止のための法律問題	136
3.1 問題の概説	136
3.2 使用者の不正行為に対する調査権の根拠・範囲・限界	136
3.3 使用者が私的領域での行為に対する懲戒の可否および合意等を求めることの根拠	139
付録5 警察に助力を求めり際の留意事項	143
序	143
1 都道府県警察本部サイバー犯罪相談窓口の活用	143
2 情報漏えいにおける捜査への協力	144
3 漏えい情報に関して不正な金銭等の要求を受けた場合の対応	146
4 遺失物届及び盗難被害届について	146
参考文献一覧	147



本編



序

個人情報保護法が本格施行され個人情報保護の重要性が広く認知されるようになり久しいが、その後も、企業（組織）等から個人情報の漏えい事故・事件が続いており、社会的な注目を浴びたものも多い。自宅や出張先で使用するために持ち運んでいたノートPCやUSBメモリなどを、紛失してしまうという事故や、ウイルスに感染したPCからWinnyやShareといったファイル交換ソフトを介して企業（組織）の重要情報が漏えいするという事故などが頻発し、損害賠償を求める裁判も提起されており、きわめて大きな社会問題となっている。

そのような状況にあるにもかかわらず、情報漏えいに直面した組織・企業が、どのような対応をするのが望ましいのかという点についてマネジメント的、法規制的、技術的など総合的な観点から調査した研究は、これまであまり例がみられない¹。特に匿名性のあるフ

¹ 事前の情報漏えい防止策については、情報処理推進機構「情報セキュリティ読本」(実教出版、2006)、同「情報セキュリティ教本 -組織の情報セキュリティ対策実践の手引き」(実教出版、2007)など多数の啓発・研究の文書がある。

ただし、漏えい対応についての技術的な側面からの分析としては、Kevin Mandia・Chris Prosis 著 酒井順行・新井 悠監修 エクストランス訳「インシデント レスポンス 不正アクセスの発見と対策」(翔泳社、2006)、

NIST “Computer Security Incident Handling Guide-Recommendations of the National Institute of Standards and Technology” NIST special Publication 800-61 (翻訳：独立行政法人 情報処理推進機構 及び NRI セキュアテクノロジーズ株式会社「コンピュータセキュリティインシデント対応ガイド」米国立標準技術研究所による勧告)(以下、NIST, SP800-61 という)(<http://www.ipa.go.jp/security/publications/nist/documents/SP800-61-J.pdf>)

JPCER/CC「技術メモ-コンピュータセキュリティインシデントへの対応」

(<http://www.jpCERT.or.jp/ed/2002/ed020002.txt>)、

JPCERT/CC「万が一の事態(インシデント)が起こった後の対応手順」

(<http://www soi.wide.ad.jp/class/20030011/slides/20/10.html>)、

RFC「サイトセキュリティハンドブック」

(日本語)(<http://www.ipa.go.jp/security/rfc/RFC2196-00JA.html>)

などがある。

また、法的なものとしては、中島信一郎・青木耕一「企業自治体のための個人情報流出 事故対応マニュアル」(ぎょうせい、2007)、大塚和成・竹内朗・田中克幸・鶴巻暁「個人情報流出対応にみる実践的リスクマネジメント」NBL 808、809、810、811、812号以下所収(商事法務、2005)などをあげることができる。

ファイル交換ソフトウェアやそれらを狙ったコンピュータウイルスによる情報漏えい事件については、漏えいした情報のコントロールが効かないなどの特殊性があるにもかかわらず、このような特殊性を踏まえての対応という点までふれた調査研究について広く認知されたものは存在しない。

このような現状認識を前提として、本研究では情報漏えいに直面した組織・企業が、どのような対応をするのが望ましいのかという点を総合的な観点から整理することを目的としている。

本報告書においては、このような目的を達成するために、(1)特に漏えいした情報の内容と流出経路に応じて具体的対応を深く検討した上で、その要旨を、参考事例を示した形で公表する(2)経営者が漏えい事案に直面した際に、参考になるマネジメント的、法規制的、技術的な留意点をまとめる(3)情報漏えい時の望ましい対応策についての提言を行う。

このような観点からの研究の成果をまとめた報告書は、法律や技術などを専任で担当する従業員などを十分に確保することが困難と考えられる中小企業をはじめとして、現在のわが国の多くの組織・企業にとって役立つものと考えられる。

その他の文献については、報告書巻末「参考文献一覧」を参照いただきたい。

第1 情報漏えい対応の定義・態様

1 情報漏えいの概念

1.1 情報漏えい事件とインシデント・レスポンス

本報告書においては、情報漏えいに直面した組織・企業が、どのような対応をするのが望ましいのかという点について検討する。情報セキュリティの分野においては、一般に「(セキュリティ) インシデント・レスポンス」(以下、インシデント・レスポンスという)という用語のもとに、組織・企業の対応について語られることが多い。ここで、「インシデント」というのは、「コンピュータもしくはネットワークのセキュリティの何らかの観点を犯す、あらゆる有害なイベント。」と定義されている²。具体的には、例えば、不正アクセス、データの破壊、意図しない情報の開示、リソースの不正使用、サービス妨害行為や、さらにそれらに至るための行為(事象)などがある。これに対して、「情報漏えい」³については、企業(組織)等の管理する秘密情報について、第三者が知りうる状態に陥ったことをいう。インシデント・レスポンスも情報漏えい対応も、情報セキュリティに対する問題が起きた際の対応という点で共通点がある。(なお、理論的には、情報システムが関与しない情報漏えいがありうるが、本報告書においては、除外して論じるものとする)。しかしながら、本報告書における「情報漏えい」と「インシデント」についての概念は、以下の各点において、その守備範囲を異にする。

² RFC2350「コンピュータセキュリティインシデント対応への期待(Expectations for Computer Security Incident Response)」による

(<http://www.ipa.go.jp/security/rfc/RFC2350JA.html#AB>)

なお、インシデントの定義については、そのほかに「セキュリティポリシーに対する明瞭な、もしくは、暗黙の違反行為」であるとか「コンピュータセキュリティに係る人為的事象で、意図的および偶発的なもの(その疑いがある場合)を含む。」との定義もある。

³情報についての漏えいについての代表的な法律としては、以下のような法律をあげることができる。

(1) 個人情報の保護に関する法律 (安全管理措置) 第二十条 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

(2) 行政機関の保有する個人情報の保護に関する法律 (安全確保の措置) 第六条 行政機関の長は、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならない。

また、その他「住民基本台帳法」、「ヒトに関するクローン技術等の規制に関する法律」、「電子署名に係る地方公共団体の認証業務に関する法律」などにも情報の漏えいに関する規定がある。

- (1) いわゆる情報セキュリティの3要素との関係でいえば、情報漏えいが、情報の機密性の侵害に関する概念であるのに対して、インシデントは、完全性・可用性についての侵害をも含む概念である。
- (2) 情報漏えいは、企業（組織）等が、社会通念上、あるいは企業（組織）自体の要求により機密にすべき情報について、それが、第三者が知りうる状態になっているという場合の概念であり、企業（組織）等が、過失によって、安全管理手段を施すのを怠った場合を含む。これに対して、インシデント・レスポンスは、情報セキュリティの要素が「侵害」される場合の概念である。
- (3) セキュリティの侵害について考えると、情報漏えいが、実際に秘密情報が第三者が知りうるに至った場合の概念であるのに対して、インシデントは、その侵害の危険性が存在する場合にも用いられる。
- (4) 情報漏えいという観点からみる場合には、その漏えいした情報が、そもそもどのような性質を有するものが（個人情報か、企業秘密やその他の企業活動に必要な機密情報か）などの機密性の程度などに注目して、議論されることが多いが、インシデントという観点から見た場合には、情報セキュリティに対する侵害から、どのように防衛するかという見地から判断されることが多い。

1.2 情報の種別

本報告書においては、いわゆる個人情報漏えい事件にかぎらず、広く情報漏えい一般を取り扱う。

対象とする情報については、種々の観点から分類することができる。情報の性質によって、個人情報・企業情報・その他の情報などに分類することができる。さらに個人情報については、顧客情報、従業員情報、その他の情報に分類されることになる。また、企業情報、その他の情報についても、企業秘密に該当する情報や通信の秘密などその情報の特性によって特別に法的な保護が与えられている情報などがある。

1.3 漏えいの概念

「漏えい」とは、企業（組織）等が管理し、かつ、社会通念上、企業（組織）等の要求から第三者が知るべきではない情報について、具体的に、第三者が知りうる状態になることをいう。

この場合において、その情報を第三者が現実に知り得たことは必要とされない。

この点で、情報が「暗号」化されていた場合においても、本報告書においては、漏えいという概念として把握することとする。もっとも、情報が「暗号」化されていた場合においては、種々の対応において、第三者の知覚の可能性が著しく減少することから、別個の配慮が必要ということになる。詳細は、個別の検討においてふれることとする。

1.4 対応の概念と各ステップ

対応とは、上記のような漏えいに対して、「情報漏えいによる直接的・間接的被害を最小限に抑える」ことを目的として、行う一連の行動をいう。このような「対応」という概念

が必要なのは、そもそも、情報セキュリティに関する事象についてあらかじめ、すべて事前に想定をしておくということが困難なことによることが大きい。そして、事前にこの対応について考えておくことは、考えていない場合に比較して、事件の際の企業の損害の減少という見地からはきわめて重要なものということができる。情報漏えいに対して早急にかつ効率的に対応することができない場合には、企業等にとってきわめて費用がかかってしまいかねないということになる。この対応は、準備段階における日頃の活動がきわめて成否を握っているということができるが、実際に情報漏えい事件が発覚したあとは、具体的には、以下の各段階を経ることになる。

(1) 発見および報告

情報漏えいをしているのではないかという発覚の契機や具体的な対応のための準備を行う。

(2) 初動対応

情報漏えい事件対等チームが、漏えい事件発覚の経緯を契機として、事件が起きていたかを確認し、その事件の重要性を位置づけ対応戦略を決定する。また、被害の拡大を防止するために必要な緊急処置を行う。

(3) 調査

情報漏えいの状況について事実関係を調べる。調査すべき事項としては、漏えいした情報の内容、規模、範囲、期間、漏えいに至った経緯、漏えいの原因、漏えいによる被害の有無、漏えい先、事前の漏えい防止策などがある。調査の手法としては、聞き取りや、流出原因と目される個所からの(特に技術的な)分析等が用いられる。

(4) 通知・報告・公表等

情報漏えいについて、利害関係者等に対して、事故・事件の発生および組織の対応状況に関して、事実を開示する手続きである。これは、二次被害回避・類似事件の予防・謝罪の意図の表明などの観点から社会的に必要なものと考えられている。また、そのような観点から法やガイドライン等によって求められることがある。また、そのような観点から法やガイドライン等によって求められることがある。また、説明責任を果たすことは、ビジネスとしても、その対応に関する信頼性を確保することになり、事業の継続性に対して良い影響をおよぼすことになる。通知・報告・公表等の範囲・手段の相当性の問題については、後述「第3の2.5 通知・報告・公表等」する。

(5) 抑制措置と復旧

事件対応の最大の目標は、情報漏えいによって発生した被害の拡大を防止し、その被害を回復することにある。そして、情報システムにおける情報セキュリティ上脆弱な点などがあれば、これを消滅させて、システムを回復する。そして、事業継続のために計画された活動とともに事業を通常に復帰させることとなる。

(6) 事後対応

事業を回復させるとともに、情報漏えい事件によって発生した諸問題についての被害の拡大阻止・回復を始め関係各位に対する法的責任・説明責任を果たしていくことが企業等

において必要とされる。

これらの各段階における留意点については、具体的に第3の各論において詳細に論じる。

2 本報告の基本的な立場について

2.1 中小企業と情報漏えい事件対応チームの責任者

本報告書は、情報漏えい事件に直面した企業等の経営等をになう責任者（企業等の代表者、もしくは、経営陣のメンバーであって実質的な責任を有する者をいう）に対して、その情報漏えい事件に対して対応する際の手順や実施の際のポイントをまとめたものである。また、その対象として、対応のための人的資源を十分に準備できないおそれがある組織等⁴、特にいわゆる中小企業を念頭において論じることとする。

情報セキュリティにおいては、インシデント・レスポンスが、情報システムの管理責任者の対応すべきプロセスとして議論されているのが多い。例えば、「本文書⁵を事前に通読され、システム運用の一環としてその発生に備えることを推奨します」という表現は、そのような位置づけを物語っているということがいえるであろう。しかしながら、次で検討するように情報漏えい事件対応については、マネジメント的な視点がきわめて重要であり、また、そのために、経営等について一定の責任と権限を有する者が対応の責任者になることが多いものと思われる。詳細については、「第3の1.3 情報漏えい対応の諸原則」で論述されるが、通常時にIT技術にかかわる従業員のみ（ボランティアベースで行っていることも多い）によって、対応をさせようとするのは、検討違いの無駄な作業が行われたり、対応の進行について混乱をきたしたりすることがありがちである。そのような事態を避けるために、経営等の責任者が、対応において重要な地位を占めるようにすべきである。

そのような対応の責任者に対する手順やポイントをまとめておくことは、きわめて重要な作業であり、本報告書は、このような問題意識にもとづくものである。なお、誰が実質的な対応の実務を主導するかは、事件対応の各局面において、経営の責任者か、現場の責任者かなど具体的な担当者が変わる場合もある。しかしながら、本書においては、経営判断を伴う責任者と具体的な事実に基づいて判断するものを異にすることのできるほどの組織体を念頭におかないために、以下においては、対応責任者として、一括して論じることとする。各組織体において、適宜検討の上、利用されることが望ましい。

また、特に中小企業においては、情報漏えい等の緊急対応の要素を含む事件が発生した場合の対応に弱点が存在するといわれている⁶。中小企業においては、緊急時の

⁴ 近時は、地方公共団体およびその関係団体、学校、病院等の企業以外からの情報漏えい事件も非常に多く、また、その情報の性質上、社会的に問題となることが多い。そのような組織における問題点をも射程にする。

⁵ (JPCERT/CC, 2002)をいう。

⁶ (東京商工会議所、2005) 85頁以下

対応のノウハウが少ないこと、マスメディア対応の基本的知識がないこと、緊急対応のためのスタッフが少ないこと、トップの指示がないと組織が動かない傾向にあることが、その弱点となりうると指摘されている。これに対応するためには、緊急対応の必要が発生した段階において外部の専門家を含む緊急対応チームを構成して、これらの弱点を克服する必要があるものと考えられる。

2.2 基本的な視点について

2.2.1 マネジメント的視点

情報漏えい事件対応は、きわめてマネジメント的な活動になる。これは、まず、情報漏えい事件対応が、企業等の危機管理の一環として、事業の継続的運用の観点から対応しなければならないということを意味している。そして、その対応にあたっては、ビジネス上の問題、法的な問題、企業方針の問題、技術能力の問題などの種々の問題についての考慮をした上で大きな決断がなされなければならない。また、一定の限られた時間、資源のもとで、対応の目標を目指して、複数の構成員からなる対応チームをまとめる活動となるため、人的・時間的・資金的資源を費やすことについての支援も必要になってくるし、また、それらを効率的に運用する必要があるために、マネジメント的な性格を有してくるのである⁷。

従来のがわが国における議論においては、技術的な視点が強調されていたり、また、理想的なインシデント対応チームの構成が議論されていたりする。その一方で、上述のようなマネジメント的な性格について論述はあまり多くはないように思える。しかしながら、上述のように情報漏えい事件対応については、マネジメント的な視点は、きわめて重要なものであり、このような視点を強調してもしすぎることはないであろう。また、理想的な情報漏えい対応においては、十全の準備が望ましいことになる。そのためには、当然資金面での問題なども起きてくることになり、その意味でもマネジメントとしての視点が必要になってくるのである。

また、近時、きわめて強調されているのが、緊急対応時におけるマスメディア等にたいする対応をめぐる問題であり、クライシス・コミュニケーションといわれている。これらのコミュニケーションを円滑に図るため、専門家の助力を得て、実際の対応の実行を行うことは、マネジメント層の職務ということになる。

⁷ (Hall, 2003) においては、「マネジメント・サポートが重要な役割を果たす」と記載されているし、また、BSI の「IT-Grundschutz Manual 2004」における、S 6 Safeguard Catalogue Contingency Planning のなかで、S 6.58 Establishment of a management system for handling security incidents が議論されており、そこでは、「セキュリティインシデントの取り扱いは、究極には、ITセキュリティ・マネジメントの責任である」と記載されている (<http://www.bsi.bund.de/english/gshb/manual/s/s06058.htm>)。

2.2.2 法規制的視点

法規制的視点については、情報漏えいに関係する企業は、情報主体たる本人（以下、本人という）に対して法的責任を負うこともあれば、関係者に対する説明責任を果たすことも必要になってくる。それらの過程で、法的・行政的規制対応の見地から考慮すべき事項も多い。これらの観点からの考慮事項に対して十分に配慮した対応が求められることはいうまでもない。具体的には、前述した対応の各段階において、法規制的視点から検討の必要な項目としては、以下のような点があげられる。

（１）発見および報告

漏えい事件発覚の経緯としては、種々の経緯がある。法規制的に要請される事項としては、たとえば、反社会的勢力が、情報漏えい事件を契機に不正な利益を要求してきた場合に、毅然として対応することなどがあげられる。

（２）初動対応

初動対応においては、漏えいについての事実確認および調査について法的観点や、その後の企業等の対応方針をも踏まえた対応方向（警察等法執行機関への助力を求めるべき事案かどうか、不正調査の手法など）の検討が、必要とされる

（３）調査

前述の調査事項について、法規制的には、証拠の保全の問題、調査の手法に対する限界、調査の根拠の問題などについての確認も重要である。

（４）通知・報告・公表等

情報漏えい事件について、企業等は、警察等への被害届の必要性についての判断および書類・証拠収集と申立書類作成・提出等、個人情報漏えいにおける漏えい情報の本人に対する法的・社会的責任についての判断、監督官庁への報告、マスメディアを通じての公表・マスメディア対応、投資家広報などの問題への対応について、法律や各種ガイドラインに求められる事項を明らかにし、適切な開示をおこなう必要がある。

（５）抑制措置と復旧

事業継続のために計画された活動とともに事業を通常に戻させる復旧の段階において、再発防止について十分な対応が望まれる。この対応において従業員に対して通常時・企業秩序侵害時において、一定の記録・調査が必要な場合について、法的な立場から根拠の検討が必要である。

（６）事後対応

復旧を果たした場合において、関係者に対する損害賠償請求の可否や被害を被ったものに対しての示談交渉などの問題が発生することになる。また、東京商工会議所の調査⁸に

⁸（東京商工会議所、2005）83 頁以下によると外部専門家として弁護士を相談相手としてあげたのが、80.6%、公認会計士が 37.1%、業界団体が 30.0%なのに対して P R 会社・広告代理店

よれば、利用される緊急時の外部専門家としては、弁護士が圧倒的に多いという調査結果がでている。その一方で、PR会社・広告代理店やリスクマネージメントのコンサルタントなどの利用は、きわめて少ないとされている。このような見地からするとき、弁護士においても後述するような特にクライシス・コミュニケーション的な問題について、一応の感覚をそなえておくことが(必要に応じて、そういった専門家を対応チームに迎えることをすすめることなども含め)求められる。

2.2.3 技術的視点

情報漏えい事件が、情報システムの脆弱な点などに起因して発生することが多いが、そのような場合、情報システムについての技術的な調査・分析・復旧・再発防止策などが重要な意味を有することになる。技術的な視点からの具体的な対応の要素を段階ごとにまとめると以下のようなになる。

(1) 発見および報告

技術的な手法により情報漏えいを発見できる場合がある。種々のログによって異常な攻撃などが認識される場合などが具体的な例としてあげられる。そのような場合に、具体的な状況や態様・日時などを正確に把握し記録する必要がある。また、事件に関連するハードウェア、ソフトウェア、ユーザ、データなどの要素を特定し、管理者に連絡することが必要である。また、ネットワークの構成などについても、技術的な知識などがまとめられていなければならない。

(2) 初動対応

事故・事件の発生を確認し、その事件の重要性を位置づけ、対応戦略を決定する過程において、情報システムに関する技術的な知識が欠かせないものであることはいうまでもない。まず、情報漏えいが認知された段階で、情報システムの基本的な構成・基本ソフトの種類・攻撃者の対応の状況などについてのチェックを行うことになる。また、基本ソフトの種類などによって必要とされる事項が異なる。

(3) 調査

具体的な漏えい事件の調査においては、情報システムに対する技術的分析が中心的な役割を果たすことになる。調査の対象としての種々のログを分析することや、また、いわゆるフォレンジック技術⁹を用いて、正確に、証拠の保管の正確性を期す点にまで留意する

が11.3%、リスクマネージメントのコンサルタントが、5.1%との結果がでている(複数回答)。

⁹ 「インシデント・レスポンス(コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為(事象)等への対応等を言う。)や法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調

ことが望ましい。また、システム管理者に対して事情聴取を行うこともある。

(4) 通知・報告・公表等

利害関係者に対しての開示の局面に対して技術者がはたすべき役割というのは、それほど大きなものではないが、技術的な事項を適切に把握し、それを漏えい事件対応責任者に対して、的確に伝えることが重要である。

(5) 抑制措置と復旧

情報セキュリティ上の脆弱性を消滅させ、システムを回復するための技術的な手法を決定し、実行する。また、抑制措置のために、サーバなどの機器をネットワークから遮断すべきかどうか、また、復旧段階において部分的な修復にするか、根本的な修復かなどの決断について技術者の提供する情報の果たすべき役割は大きい。

(6) 事後対応

利害関係者に対する技術的説明等で、事後対応においても技術的な側面が重視される場合が存在する。

3 情報漏えいの態様について

「漏えい」を考えた場合、その漏えいの態様などの観点から、種々の分類方法が存在する。漏えいを発生させるに至った脅威の性質ごとに分類した場合は、以下のとおりとなる。

3.1 紛失・盗難

これは、物理的に、企業等の管理のもとにある情報が、そのような管理から過失に因って離れる場合をいう。情報の従業員らによって外部に持ち出された記録媒体や情報を記録したPCなどを遺失したり・盗難にあたりする場合が代表的な事案である。また、委託業者などが管理している情報が、同様な経路で、その管理を離れる場合をも含む。

3.2 誤送信・Webでの誤公開等

これは、物理的には、企業等が管理しうる場所に情報が存在しているが、管理の手法を間違え、情報が第三者に公開するような設定状態になっている場合や、電子メール送信の際に送信先を誤り第三者に見える形で送信したような場合を指す。

3.3 内部犯行

これは、組織における従業員等が、当該情報が機密として管理されていることを認識しつつ、これを第三者に提供するような場合である。

3.4 Winny/Shareネットワークへの漏えい

近年きわめて問題となっているのが、Winny/Share ネットワークにおける暴露ウイルスへの感染による漏えい問題である。企業もしくは、その構成員が、管理している情報が、上記ネットワークに接続している場合で、Winny/Share ネットワークに接続していた場合に、暴露ウイルスに感染し、それによって、上記ネットワークに情報が漏えいしてしまう場合

査手法・技術」をいう(デジタル・フォレンジック研究会, 2006)(守本, 2004)など

である。

3.5 不正プログラム

不正プログラム(もしくは、悪意あるプログラム)とは、作成者等がダメージを及ぼす意図をもって利用者の予期しない、もしくは、望まない影響を及ぼすプログラムをいい、コンピュータウイルス、ワーム、トロイの木馬、悪意あるスクリプトなどの総称をいう。これらのなかで、情報漏えいを引き起こすものがあり、電子メール添付型のウイルスにおいては過去に Klez や Sircam など、感染したコンピュータの内部からファイルを取り出しこれを添付して、外部に送信するという特徴を持つものが存在する。

3.6 不正アクセス

企業が管理していた情報で、アクセス制御によって保護されている情報が、外部からの無権限アクセス行為によって、攻撃者にアクセスされてしまう場合をいう。このような無権限アクセス行為には、他人の ID/パスワードを悪用する場合と、脆弱性をついた攻撃の場合がある(不正アクセス禁止法参照)。

3.7 ブログ掲載・風評等

組織の従業員等が、組織等において機密性あるものとして取り扱うべき情報を、機密性があるとの認識をもたないで、ブログに掲載したり他人にそのまま伝えたりする場合である。後述の内部犯行に比較して、機密性についての認識を有しない特徴を有している。

4 情報の分類

本報告書においては、機密として社会通念上あるいは組織の要請として取り扱うべき情報の漏えいについて考える。機密情報および機密とすべき情報は、大きく分けると以下のような観点から分類することができる。

4.1 企業(組織)の情報とその種別

まず、情報は、その情報の関連する主体によって企業(組織)の情報か個人情報かに分けることができる。ここで、企業(組織)が主体となる情報は、企業(組織)の情報(以下企業情報)ということになる。この企業情報のなかでも、その主体が、自社の場合と他社の場合とがある。他社の場合については、その性質上、善良な管理者の注意を払って、情報を管理すべき場合が多い。その一方で、自社情報であれば、その情報については、自己のものにするのと同じの注意義務ということがいえるであろう。

もっとも、自社情報であったとしても、その重要性が他社情報に比較して劣るというわけではない。特に、自社において、漏えいによる社会的な影響が大きいと考えられる情報を管理している場合、そのような公共性の高い情報については、そのような影響度に応じた対応が必要であるということになる。

4.2 個人情報とその種別

特定の情報が関連する主体が個人である場合、個人情報として認識される。そして、情

報セキュリティの見地からは、機密情報とされる。個人情報とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により「特定の個人を識別することができるもの」（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの）をいうとされている（個人情報保護法 2 条 1 項）。

もっとも、その個人情報においても、特に個人の機微にわたる情報があり、機微情報として特に機密にすべき情報であると考えられる¹⁰。また、クレジットカード情報などの経済的な損害に直接結びつく情報についても、特に機密にすべき情報であると認識することができる。

¹⁰ 「個人情報保護マネジメントシステム 要求事項」の「4.4.2.3 特定の機微な個人情報の取得の制限」は、「次に示す内容を含む個人情報の取得，利用又は提供は，行ってはならない。」として「a) 思想，信条及び宗教に関する事項。b) 人種，民族，門地，本籍地，身体・精神障害，犯罪歴，その他社会的差別の原因となる事項。c) 勤労者の団結権，団体交涉及びその他団体行動の行為に関する事項。d) 集団示威行為への参加，請願権の行使，及びその他の政治的権利の行使に関する事項。e) 保健医療及び性生活。」をあげている。

第2 事故事例の調査分析

1 調査分析の概要

情報漏えい事故発生時における組織がとるべき対応を検討するにあたっての参考とするため、まず現状において企業等組織が実際の情報漏えいに際しどのような対応を行っているかについて調査を行った。調査は様々な事故の態様別に組織が実施した対応項目についてその有無や内容を公開情報をもとに確認した。調査対象は過去5年以内に日本国内で発生した情報漏えい事故・事件とし、当該組織がインターネット上に公開しているプレスリリース等公開資料、新聞社等オンラインニュースサイトへの掲載内容を情報源とした。これらにより明示的に記述されている事項について対応「有り」としてカウントしている。過去に実施された同様の調査としては「個人情報」に関する漏えいを対象に調査されているものが多い¹¹が、本調査分析では「個人情報」に限定せずに企業活動等で使用される経営情報等組織が保有する情報全般について発生した漏えい事故を対象としている。

2 調査分析手法

2.1 情報漏えい事例の収集

国内において過去5年間に発生した情報漏えい事例について漏えい情報の種別、漏えい経路、事故後の対応、事故後の経過（二次被害等）などの実態を把握することを目的とし事例を収集した。事故事例を収集するための情報源としては、原則として当該組織がインターネット上に公開しているプレスリリース及び新聞社等広く一般に認知されているオンラインニュースサイトに掲載されている公開情報を使用した。

本調査研究における事例の収集目的は、漏えい態様の別や状況別にとられている事故後の対応の実態を把握し、漏えい態様毎の特性を抽出することである。そのため、本調査の結果は広く様々な情報漏えい事例を網羅的に収集しどういった事故がどの程度の割合で発生しているかといったような統計情報を示すものではないことに注意が必要である。本調査では次項に示す分類体系に基づき主要な漏えい態様毎に事故後の対応の傾向を明らかにしたものである。個人情報漏えいに関する事故の発生傾向や対策全般については NPO 日本ネットワークセキュリティ協会が毎年実施している調査¹が、各種組織における情報セキュリティインシデント及び対策についての調査としては、中央大学の内田教授¹²および野村総合研究所セキュアテクノロジーズ株式会社によるもの¹³などが存在する。

¹¹ NPO 日本ネットワークセキュリティ協会，2006 年度 個人情報漏えいインシデント調査結果 <速報> ver.1.0, 2007

¹² 内田勝也，情報セキュリティ調査からみた日米情報セキュリティ比較，2007

¹³ NRI セキュアテクノロジーズ株式会社，企業における情報セキュリティ実態調査 2006，2006

2.2 情報漏えい態様、事後対応及び事故後経過の分類

調査を実施するにあたり収集した各事例について情報漏えい態様を示す各種要素について分類し、調査結果を表形式で整理した。態様については、「漏えい元組織種別」、「漏えい情報種別」、「漏えい原因」、「漏えい経路」、「発覚方法」といった要素についてそれぞれ類型化を行った。また、事故後の対応について、「情報開示方法」「情報開示内容」「被害者救済に関する取り組み」「報告・連絡先」について調査結果をまとめるとともに、事件後の経過について「二次被害」「訴訟・法的措置等」の状況について調査時に公開されている内容について記載した。以下に情報漏えい態様等に関する本調査における分類方法について示す。

(1) 情報漏えい態様の分類

ア 漏えい元組織種別

調査対象となった事故事例において漏えい元となった組織の種別について、下記の種別に分類した。「学校」には小中高等学校、大学等が含まれこれらについては業務の性質上公共性が高いことから、公共団体や私企業とは別に独立した組織種別とした。

(ア) 民間企業

(イ) 公共団体

(ウ) 学校

イ 漏えい情報種別

調査対象となった事故事例において漏えいした情報の種別について、下記に分類した。なお、他の章において、一般情報を「他社情報」「自社情報」、個人情報について「センシティブ情報」と「一般情報」に区別しているが、本調査においてはこれらの間に顕著な差異が見られないため特に区別せず集計した。ただし個人情報に関しては流出した件数により対応が異なることが考えられるため、件数による区分を設けた。

(ア) 一般情報

組織が保有する業務情報のうち個人情報及び下記重要インフラ情報以外で、公開を前提としていないもの。

例) 事業計画、経理情報、製品設計書

(イ) 公共性の高い情報

民間企業、公共団体に関わらず、当該情報の漏えいにより公共インフラ、住民の生活、安全等に影響を及ぼし得るものまたは及ぼし得ると認識かねない情報

例) 原子力発電所に関する情報、空港保安設備に関する情報等

(ウ) 個人情報

生存する個人に関する情報（個人情報保護法に定められる個人情報）

例）顧客名簿、電子メールアドレス、人事記録

なお個人情報については情報が含む個人情報の件数により以下に区分している。

- a 個人情報（100件未満）
- b 個人情報（100件以上1000件未満）
- c 個人情報（1000件以上）

ウ 漏えい態様分類

調査対象となった事故事例のタイプについて下記に分類した。なお「その他（含む風評・ブログ掲載）」については通常組織内で処理され該当する事例が確認できなかったために本調査の対象とはしていない。

（ア）紛失・盗難

情報そのものあるいは格納した記憶媒体、PC等の紛失または盗難

（イ）誤送信・Webでの誤公開等

社員・職員等が本来行ってはならない操作、設定等を行ったことにより情報が流出したケース

（ウ）内部犯行

社員・職員等が悪用する目的で内部の情報を持ち出したケース

（エ）Winny/Share等への漏えい

組織の情報がWinnyまたはShareに代表される匿名ファイル交換ネットワーク上に漏えいしたケース。これは実際には「情報の持ち出し」「Winny/Shareの利用」「ウイルス感染」の複合的な要因に起因するものであるが、昨今の事故多発の現状を鑑み「Winny/Share等への漏えい」対策の不備として独立した分類として取り扱っている。

（オ）不正プログラム

コンピュータウイルス、スパイウェア等不正なプログラムにより情報が漏えいしたケース。ただしWinny/Share等への漏えいを目的とした不正プログラムの場合を除く。

（カ）不正アクセス

攻撃者の不正アクセス行為に起因して発生した情報漏えい。

（キ）不明

情報漏えいの原因が不明であるケース

エ 発覚方法

情報漏えい事故が発覚した際の方法すなわちどのようにして組織が情報漏えいの事実を認知するに至ったかについて以下のとおり分類している。

(ア) 自組織内

組織自らが情報漏えいの事実を知ったケース

(イ) 監督官庁

「監督官庁」とは監督官庁からの通知により事故の発生を知ったケース

(ウ) 掲示板

匿名掲示板等への書き込みによって事故発生を知ったケース

(エ) 顧客等

企業の顧客、公共サービスの利用者、市民等から通報が寄せられたケース

(オ) 警察

警察から組織に対して情報漏えいの可能性について通報があったケース

(カ) マスコミ

マスメディアから情報漏えいの事実について確認を求められ発覚したケース

(キ) 第三者からの指摘（推定を含む）

上記に示された関係者以外の外部からの指摘

(ク) 不明

情報漏えいの事実をどのように認知したか不明なケース

(2) 事故後の対応の類型化

ア 情報開示方法

情報漏えいの発生に関する情報の開示手段について利用の有無について以下の項目を定義した。複数の手段が使用されることもあり得る。

(ア) Web サイト

Web サイト上に情報漏えいを知らせるページ、文書等を設置することにより情報を開示

(イ) 記者会見

記者会見を実施し情報を開示

(ウ) 直接通知

個人情報漏えいにおいて該当する個人に電話、電子メール、郵送等により直接通知

(エ) 個別訪問

個人情報漏えいにおいて該当する個人を直接に訪問し通知

(オ) 開示なし

情報漏えいの事実について組織からの情報開示が行われなかった場合

(カ) その他

上記以外の開示方法

イ 情報開示内容

漏えいに関する情報開示の際どういった内容を公開しているかについて、下記の項目に関する開示の有無を確認した。本項目はあくまでも開示情報、報道内容での記載の有無を示すものであり、実際に当該項目に関する行為等の有無を示すものではない。

(ア) 被害範囲

漏えいした情報の範囲など被害内容が確認される記述

(イ) 経過

漏えいまでの経緯、発見後の対応、被害状況等一連の経過に関する記述

(ウ) 漏えい原因

漏えいに至った原因に関する記述

(エ) 補償方法

漏えいに起因する損害に関する補償の方法に関する記述

(オ) 謝罪

情報漏えいによる被害者、被害組織等に関する謝罪または遺憾の意の表明

(カ) 再発防止

再発防止策に関する記述

(キ) 問合せ窓口

当該漏えい事故に関する問い合わせ窓口に関する記述

(ク) その他

上記以外の開示

ウ 被害者救済策

漏えい事故による被害者、被害組織に対し発生した被害についてどのような救済のための対応がとられたかについて開示情報をもとに以下の項目の有無を調査した。

(ア) 問合せ窓口設置

被害者向け問い合わせ窓口の設置及び対応

(イ) 個別説明・相談

個々の被害者に対する状況説明、相談への対応等

(ウ) 金券等配布

被害者に対する金券の配布

(エ) 損害の補償

発生した損害に対して補償することの意思表示

(オ) その他

上記以外の被害者救済策

エ 再発防止策

事故後にとられた再発防止策について開示情報をもとに以下の項目の有無を調査した。

(ア) サービス停止

被害拡大防止のための一定期間のサービスの停止、または永続的なサービスの停止

(イ) 技術対策強化

新規情報セキュリティ技術の導入等情報システムに関する技術的な対応

(ウ) 従業員教育・徹底

社員に対する情報セキュリティ教育の実施、セキュリティ意識の啓蒙等

(エ) 内部管理強化

情報セキュリティポリシーの徹底、情報セキュリティ監査等組織内部における管理体制の強化

(オ) その他

上記以外の再発防止策

オ 報告・連絡

漏えい後に行われた以下に示す情報セキュリティに関する各種機関への報告・連絡の有無について調査した。

(ア) 監督官庁

監督官庁への報告・連絡

(イ) 警察

- 都道府県警等、警察組織への通報・連絡
 - (ウ) IPA (独立行政法人 情報処理推進機構)
 - IPA に対する報告・連絡
 - (エ) JPCERT/CC (有限責任中間法人 JPCERT コーディネーションセンター)
 - JPCERT/CC に対する報告・連絡
 - (オ) 個人情報保護団体
 - 監督官庁の認定する個人情報保護団体に対する報告・連絡
 - (カ) その他
 - 上記以外の情報セキュリティ関連機関に対する報告・連絡
- (3) 漏えい後の経過
- ア 二次被害
 - 開示情報及び一般報道等において確認された事故後の二次被害について以下の事項の有無を調査した。
 - (ア) いやがらせ
 - 漏えい情報に起因して発生したいやがらせ行為
 - (イ) スпам・勧誘
 - 漏えい情報に起因するスパムメール、勧誘行為
 - (ウ) 詐欺・恐喝
 - 漏えい情報を利用した詐欺、恐喝行為
 - (エ) 詐称・不正利用
 - 漏えい個人情報を使用し本人になりすます行為、その他漏えい情報の不正な利用
 - (オ) 株価低下
 - 漏えいに起因する株価の低下
 - (カ) 風評
 - 漏えいに起因する風評による被害
 - (キ) 顧客減少
 - 漏えいに起因する顧客の減少
 - (ク) 売上低下
 - 漏えいに起因する売上の低下
 - (ケ) その他
 - 上記以外の二次被害の発生

イ 訴訟・法的措置等

漏えい後訴訟・法的措置等に発展したケースについて以下の事項の有無について調査した。

(ア) 訴訟

情報漏えいに関して被害者からの訴訟に発展したケース

(イ) 損害賠償

情報漏えいに関して被害者への損害賠償が発生したケース

(ウ) 刑事責任

情報漏えいに関して刑事責任が問われたケース

(エ) 行政指導（注意）

監督官庁による「注意」が行われたケース

(オ) 行政指導（嚴重注意）

監督官庁による「嚴重注意」が行われたケース

(カ) 行政指導（勸告）

監督官庁による「勸告」が行われたケース

3 調査結果

本調査結果の詳細を、別添「情報漏えい一覧」に示す。以下調査に基づく集計結果について記す。

3.1 調査データの概要

調査事例総数 153件

(1) 漏えい態様の内訳

ア 漏えい元組織種別 (N = 153)

民間企業	106件 (69.3%)
公共団体	27件 (17.6%)
学校	20件 (13.1%)

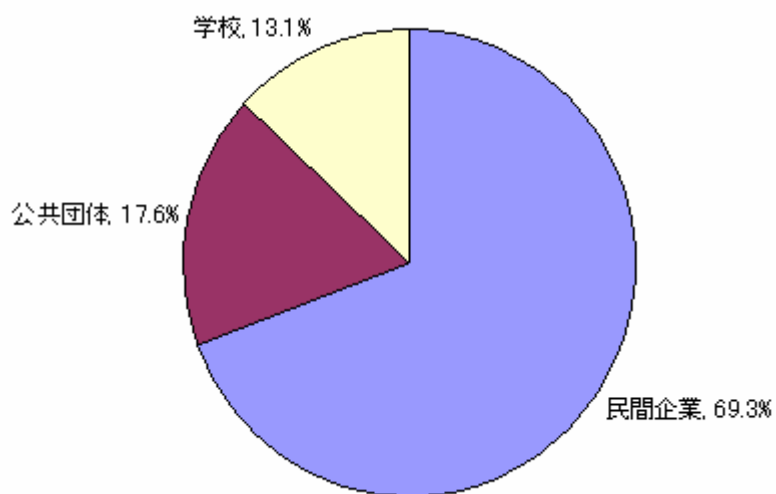


図 2.1 漏えい元組織種別

イ 漏えい情報種別 (N = 1 5 3)

個人情報	1 3 1 件 (8 5 . 6 %)
公共性の高い情報	1 1 件 (7 . 2 %)
一般情報	1 1 件 (7 . 2 %)

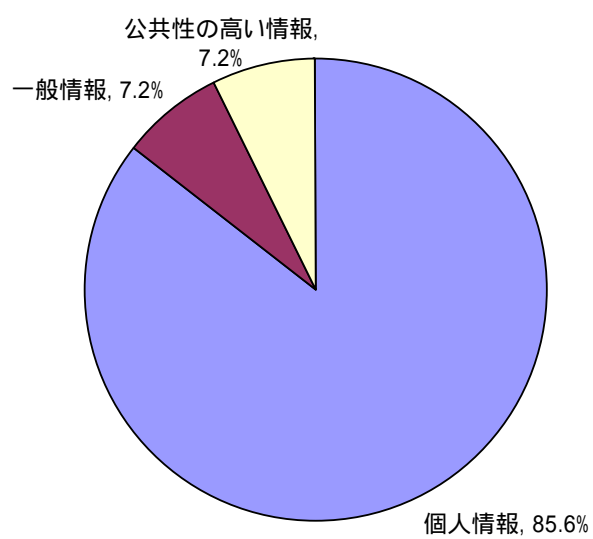


図 2.2 漏えい情報種別

ウ 漏えい態様分類 (N = 1 5 3)

紛失・盗難	49件 (32.0%)
Winny/Share 等への漏えい	40件 (26.1%)
誤送信・Web での誤公開等	22件 (14.4%)
内部犯行	21件 (13.7%)
不正アクセス	18件 (11.8%)
不正プログラム	2件 (1.3%)
不明	1件 (0.7%)

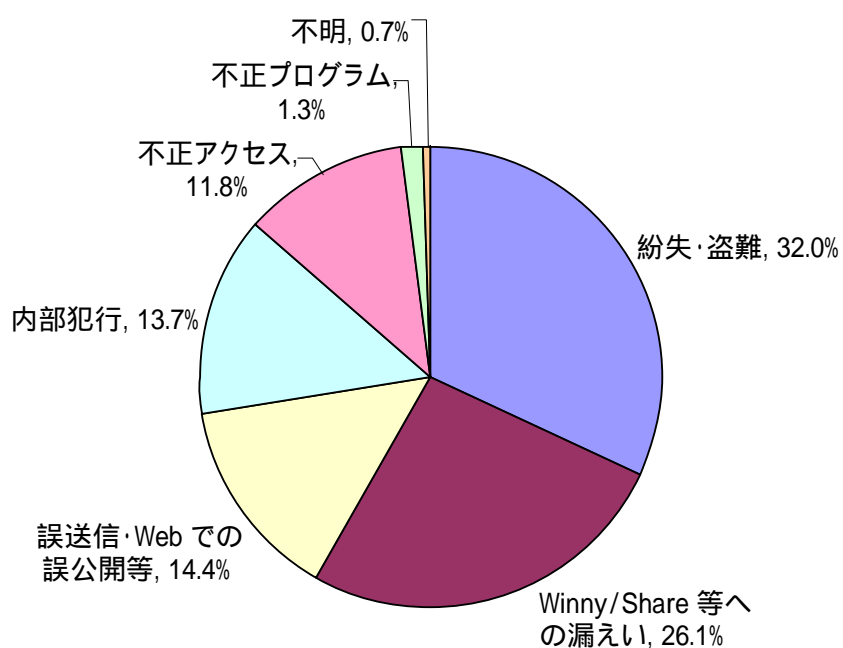


図 2.3 漏えい態様分類

(注) 上記の% (パーセント) で示す比率は本調査の対象となった事例中の割合を示すものであり、実際の情報漏えいにおける原因別の発生割合を示すものではない。

エ 発覚方法 (N = 153)

自組織内	81件 (52.9%)
第三者からの指摘 (推定を含む)	24件 (15.7%)
顧客等	21件 (13.7%)
監督官庁	10件 (6.5%)
警察	7件 (4.6%)
マスコミ	6件 (3.9%)
掲示板	1件 (0.7%)
不明	3件 (2.0%)

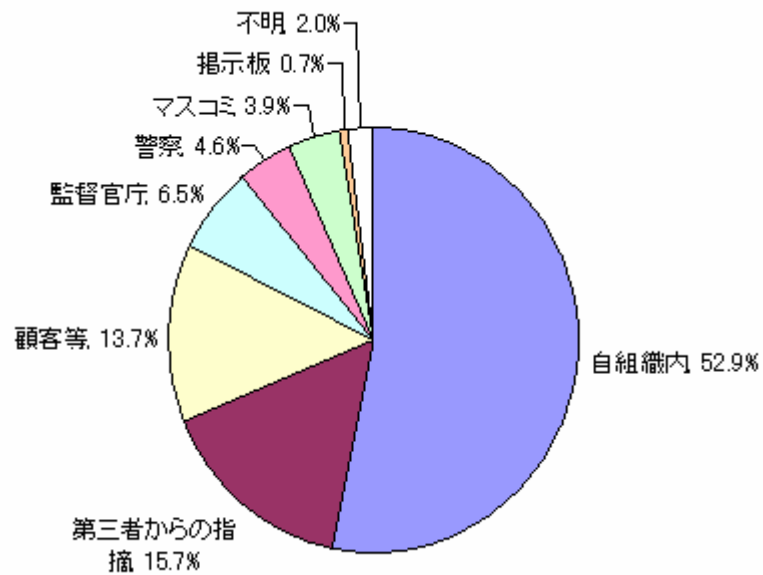


図 2.4 発覚方法

(2) 事故後の対応

ア 情報開示方法 (N = 153、個人情報を含む場合N = 131)

Web サイト	147件 (96.1%)
直接通知	89件 (67.9%)
記者会見	22件 (14.4%)
個別訪問	6件 (4.6%)
公開なし	1件 (0.7%)

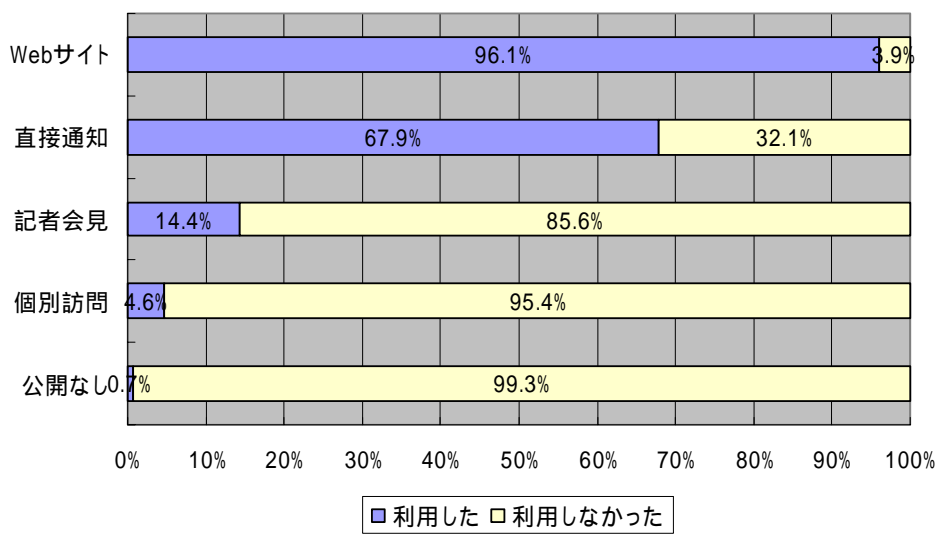


図 2.5 情報開示方法

イ 情報開示内容 (N = 153)

漏えい原因	143件 (93.5%)
謝罪	138件 (90.2%)
被害範囲	137件 (89.5%)
経過	128件 (83.7%)
再発防止	128件 (83.7%)
問合せ窓口	93件 (60.8%)
補償方法	8件 (5.2%)
その他	4件 (2.6%)

(その他項目例)

- ・情報の不正利用の有無、不正利用の状況
- ・盗難 PC のセキュリティ対策状況
- ・個人情報漏えい後の第三者からの接触の有無
- ・ウイルス関係情報、ウイルスへの対処法、スパムメールへの対処法
- ・紛失物の発見状況

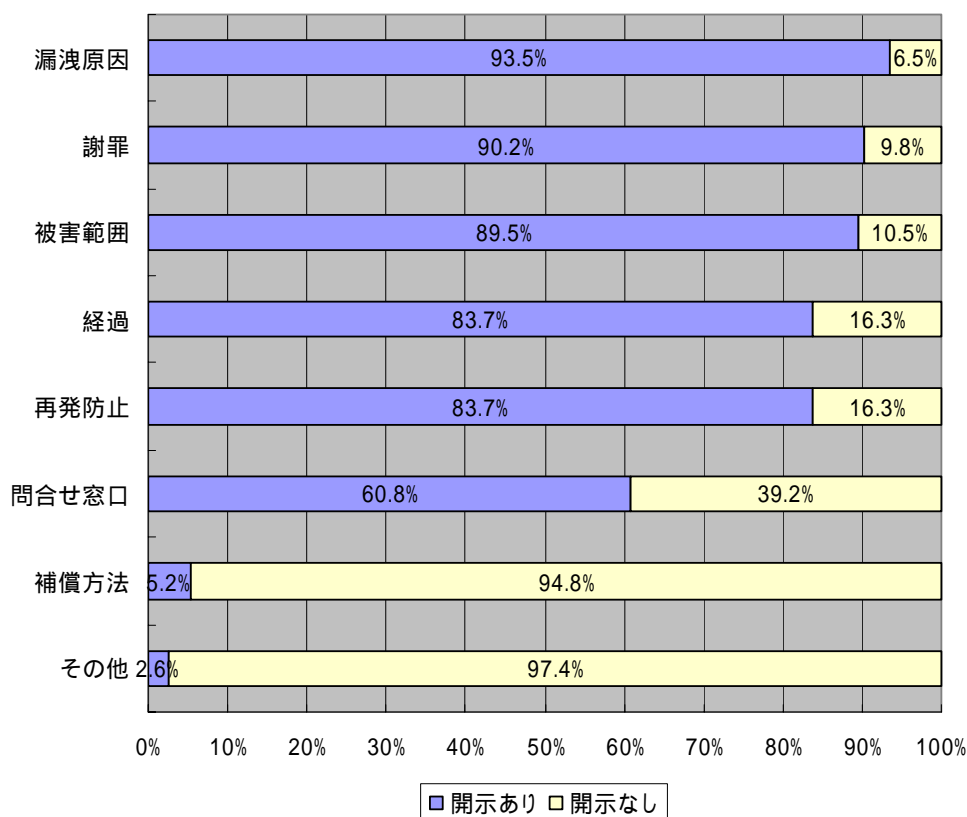


図 2.6 情報開示内容

ウ 被害者救済策（個人情報を含む場合 N = 131）

問合せ窓口設置	66件（50.4%）
個別説明・相談	58件（44.3%）
金券等配布	8件（6.1%）
損害の補償	6件（4.6%）
その他	4件（3.1%）

（その他項目例）

- ・流出パスワードの無効化
- ・会員番号、会員カード等の再発行

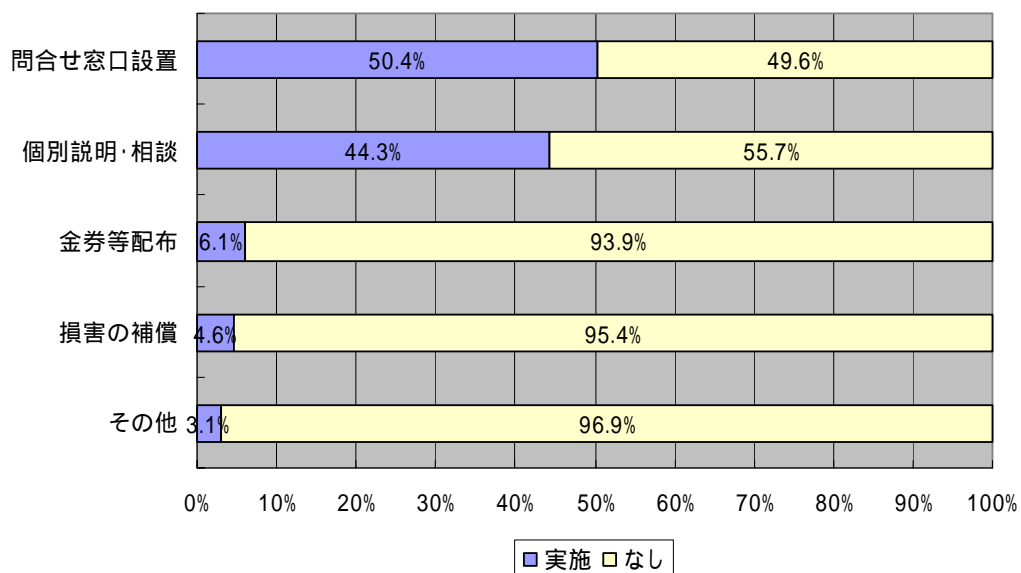


図 2.7 被害者救済策

エ 再発防止策 (N = 153)

内部管理強化	106件 (69.3%)
従業員教育・徹底	93件 (60.8%)
技術対策強化	56件 (36.6%)
サービス停止	18件 (11.8%)
その他	4件 (2.6%)

(その他項目例)

- ・細部にわたる見直し
- ・物理的防犯対策の強化

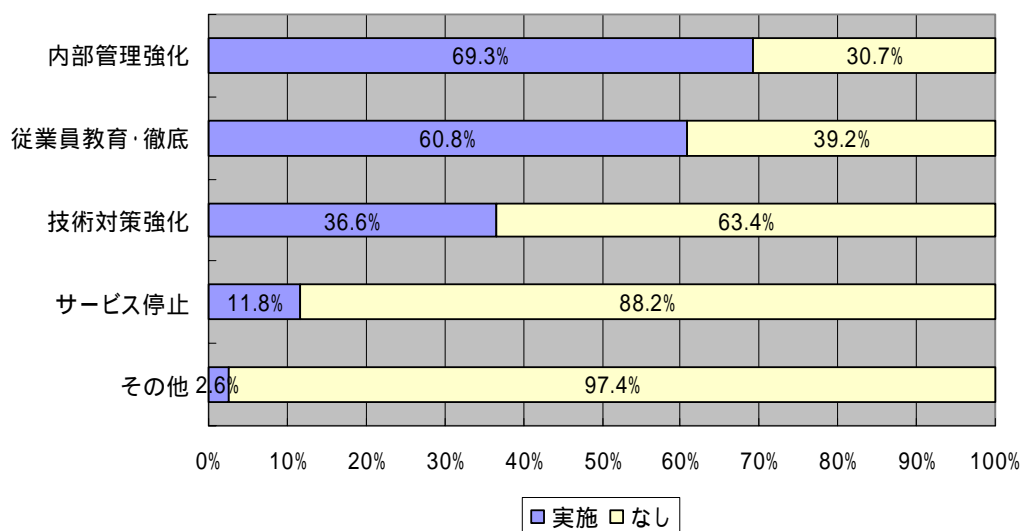


図 2.8 再発防止策

才 報告・連絡 (N = 153)

警察	67件 (43.8%)
監督官庁	37件 (24.2%)
IPA	1件 (0.7%)
個人情報保護団体	1件 (0.7%)
JPCERT/CC	0件 (0.0%)
その他	3件 (2.0%)

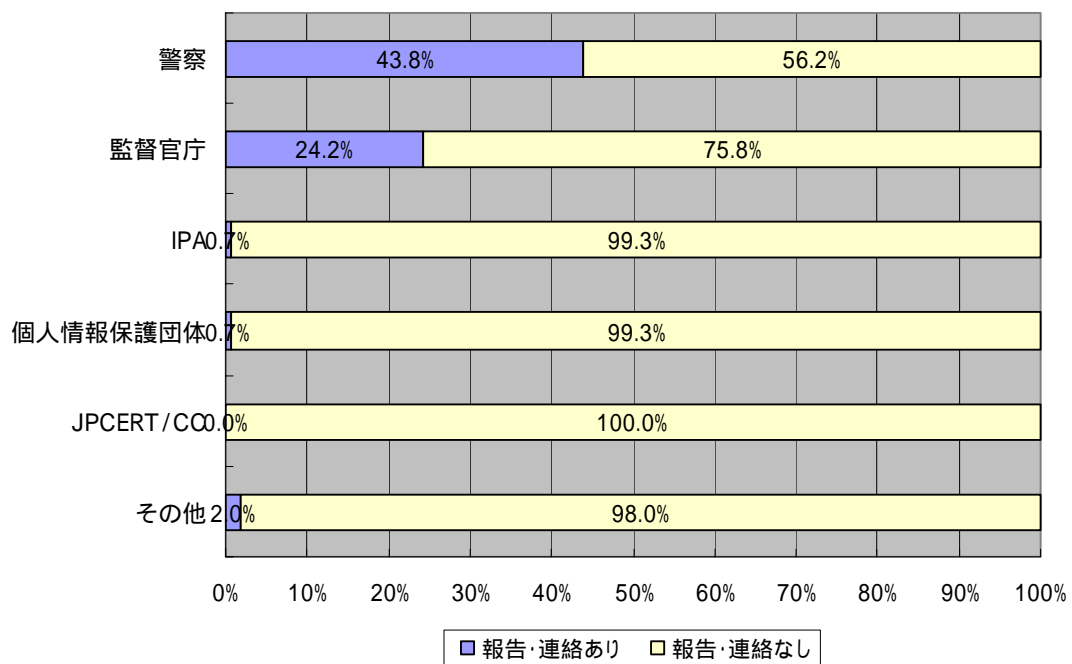


図 2.9 報告・連絡

(3) 事故後の経過

ア 二次被害（個人情報を含む場合 N = 131）

詐欺・恐喝	8件（6.1%）
詐称・不正利用	8件（6.1%）
いやがらせ	4件（3.1%）
スパム・勧誘	3件（2.3%）
株価低下	0件（0.0%）
風評	0件（0.0%）
顧客減少	0件（0.0%）
売上低下	0件（0.0%）
その他	4件（3.1%）

（その他項目例）

- ・ 営業停止
- ・ 株式上場の延期
- ・ なりすましメールによるウイルス感染

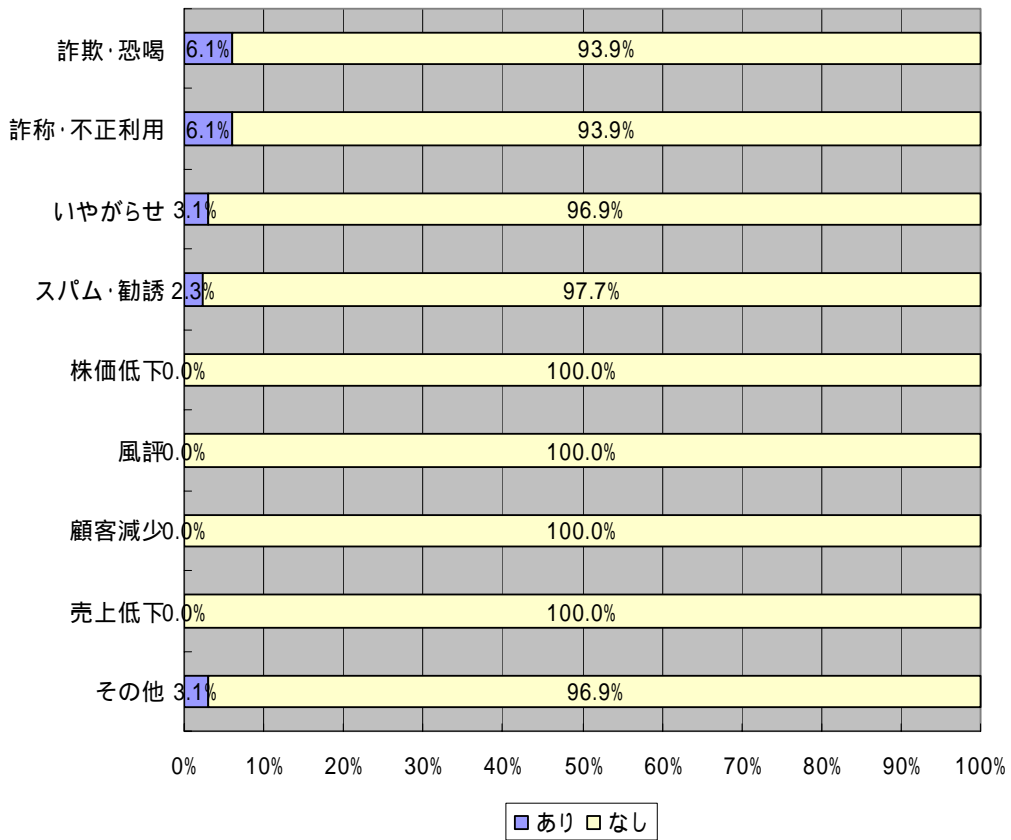


図 2.10 二次被害

イ 訴訟・法的措置等 (N = 153)

行政指導 (嚴重注意)	12 件 (7.8 %)
損害賠償	8 件 (5.3 %)
行政指導 (勸告)	6 件 (3.9 %)
訴訟	5 件 (3.3 %)
行政指導 (注意)	2 件 (1.3 %)
刑事責任	0 件 (0.0 %)

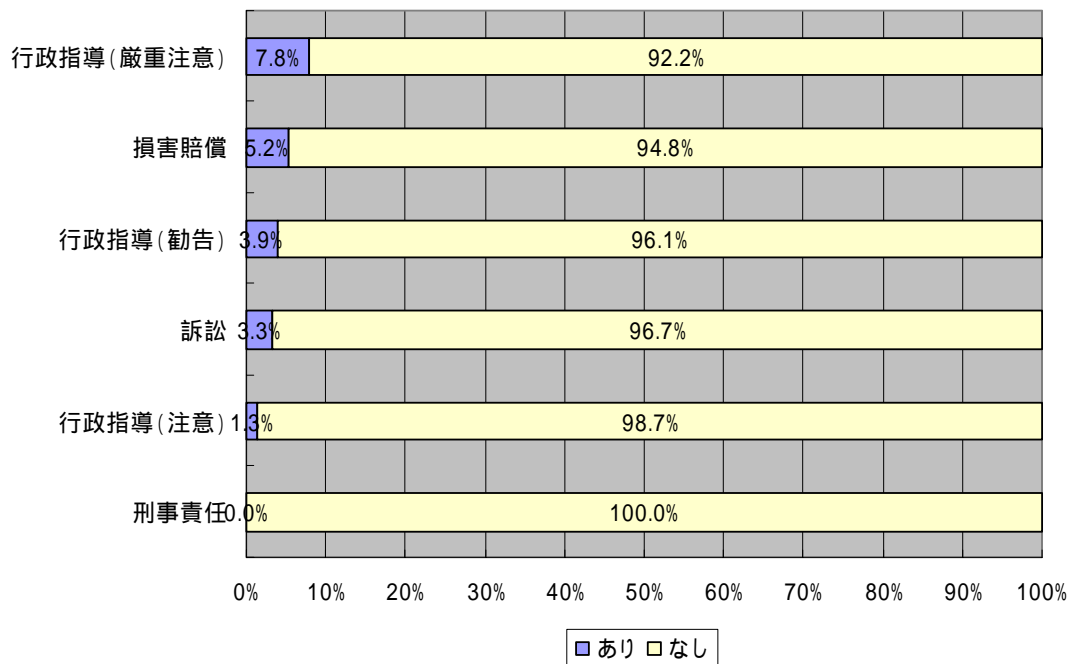


図 2.11 訴訟・法的措置等

4 分析結果

4.1 分析結果の概要

調査の結果をもとに、事故の態様毎に事故後の対応やその後の経過、特に二次被害等の状況等についてみられる傾向について分析した。全般的に以降の章で述べるべき対応に適合する傾向はみられるものの、一律にすべての組織が同じ状況において一定の対応がとれているわけではないことが確認された。

4.2 対応ステップに関する傾向

(1) 記者会見開催の有無

情報漏えい事故が発生した場合に記者会見が開催されるケースとされないケースがある。どういった場合に記者会見が行われるのかについて漏えい態様要素との関連を分析した。記者会見の開催要否については組織の立場や位置づけなど複合的な要素が関連するが、漏えい態様分類の点から見れば「内部犯行」など犯罪性の高いものについて、記者会見が開催されているケースが多いように考えられる。また、1000件以上の個人情報の漏えいなど流出情報の規模が大きい場合に記者会見を開催していることが多い。

ア 組織属性毎の記者会見開催有無

公共団体	5 / 27件 (18.5%)
学校	3 / 20件 (15.0%)
民間企業	14 / 106件 (13.2%)

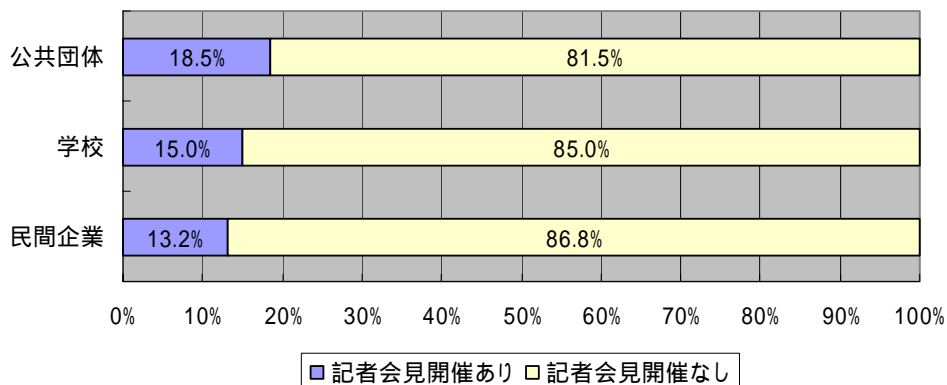


図 2.12 組織属性毎の記者会見開催有無

イ 漏えい情報種別毎の記者会見の開催数

公共性の高い情報	4 / 11件 (36.4%)
個人情報(1000件以上)	15 / 62件 (24.2%)
個人情報(100~999件)	2 / 39件 (5.1%)
個人情報(1~99件)	1 / 30件 (3.3%)
一般情報	0 / 11件 (0.0%)

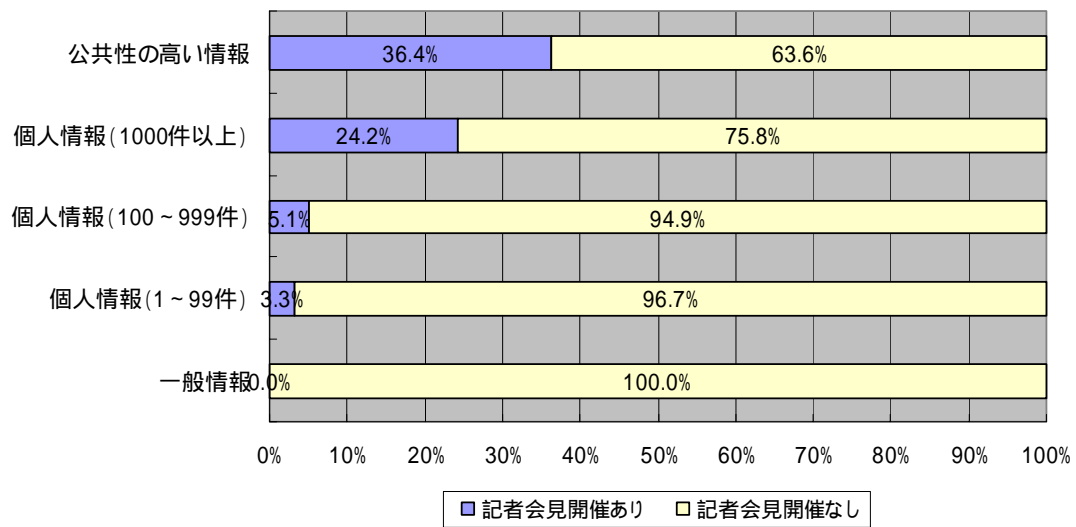


図 2.13 漏えい情報種別毎の記者会見の開催数

ウ 漏えい態様分類毎の記者会見の開催数

不正プログラム	1 / 2件 (50.0%)
内部犯行	8 / 21件 (38.1%)
Winny/Share 等への漏えい	5 / 40件 (12.5%)
不正アクセス	2 / 18件 (11.1%)
紛失・盗難	5 / 49件 (10.2%)
誤送信・Web での誤公開等	0 / 22件 (0.0%)
不明	1 / 1件 (100.0%)

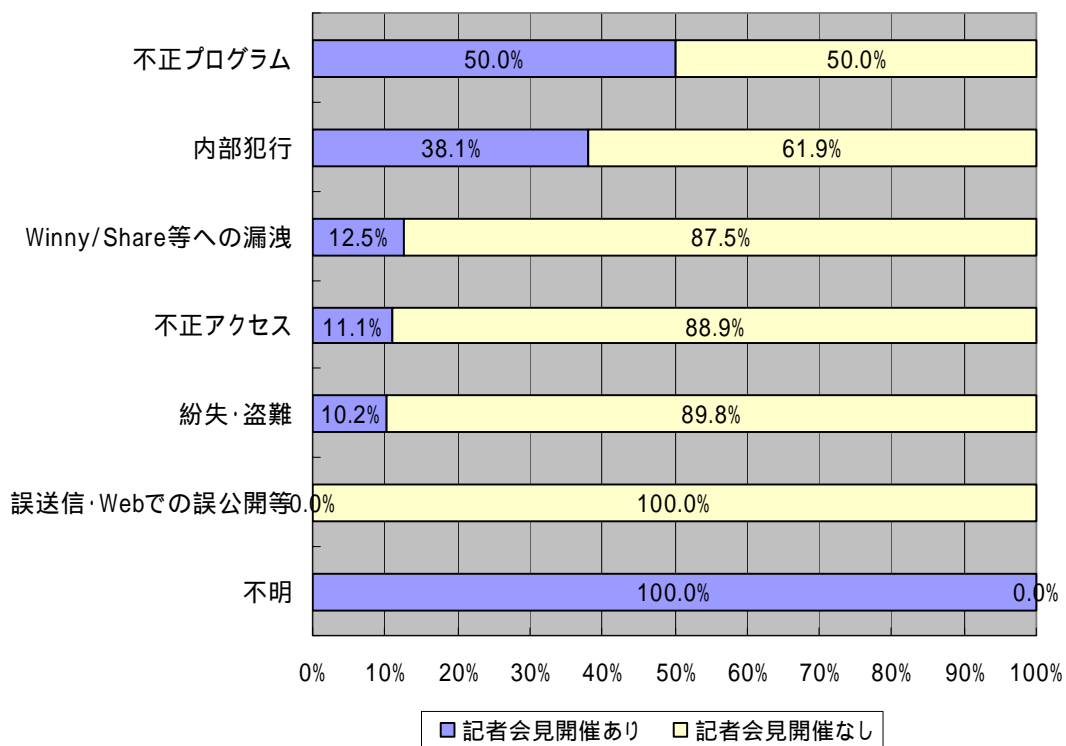


図 2.14 漏えい態様分類毎の記者会見の開催数

(2) 金券等の配布

個人情報漏えいした企業が被害者すなわち漏えいされた個人情報の本人に対して金券等が配布されるケースがある。金券の配布がどの程度実施されているかについて組織種別毎に比較した。本調査の範囲においては、金券配布は公共団体や学校ではなく、民間企業において実施されていることが確認されたが、実施される例はそれほど多くないことが確認された。これら金券等を配布したケースにおいては1件を除き500円相当の金券、カード、ポイントなどが配布されており、1000円分の金券(Quoカード)が配布されているケースもあった。

民間企業	8 / 106件 (7.5%)
学校	0 / 27件 (0.0%)
公共団体	0 / 20件 (0.0%)

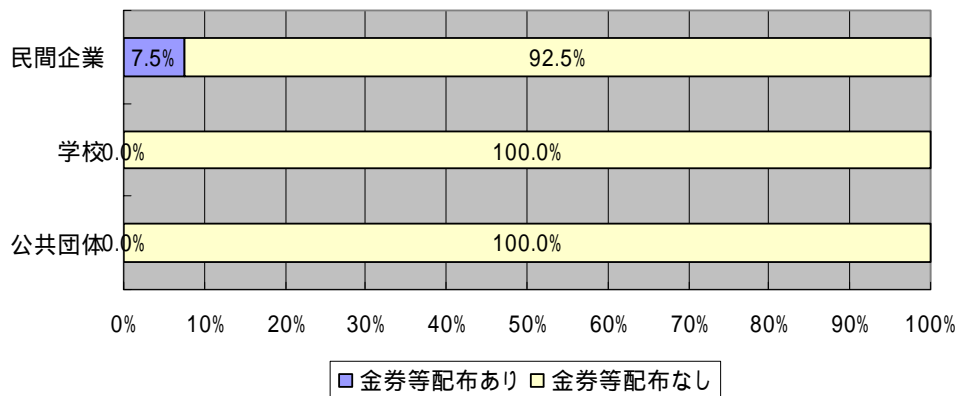


図 2.15 金券等の配布

(3) 届出・報告

情報漏えいの事実を確認した組織がどのような状況において警察へ事故の届出を行っているか、また個人情報漏えい時においてどの程度の組織が監督官庁に届け出を行ったと公表しているかについて確認した。「紛失・盗難」「内部犯行」「不正アクセス」の事例では犯罪に関連する可能性が高いこともあり警察へ通報したと公表される割合が高い。一方過失、Winny/Share 等への漏えいなどのケースでは漏えい事故自体について警察への通報はないものの、漏えいした情報が詐欺や不正送金等に利用されるケースにおいて警察への通報がおこなわれている。

ア 漏えい態様分類毎の警察への届出数

内部犯行	17 / 21件 (81.0%)
紛失・盗難	34 / 49件 (69.4%)
不正アクセス	11 / 18件 (61.1%)
不正プログラム	1 / 2件 (50.0%)
誤送信・Webでの誤公開等	2 / 22件 (9.1%)
Winny/Share 等への漏えい	2 / 40件 (5.0%)
不明	0 / 1件 (0.0%)

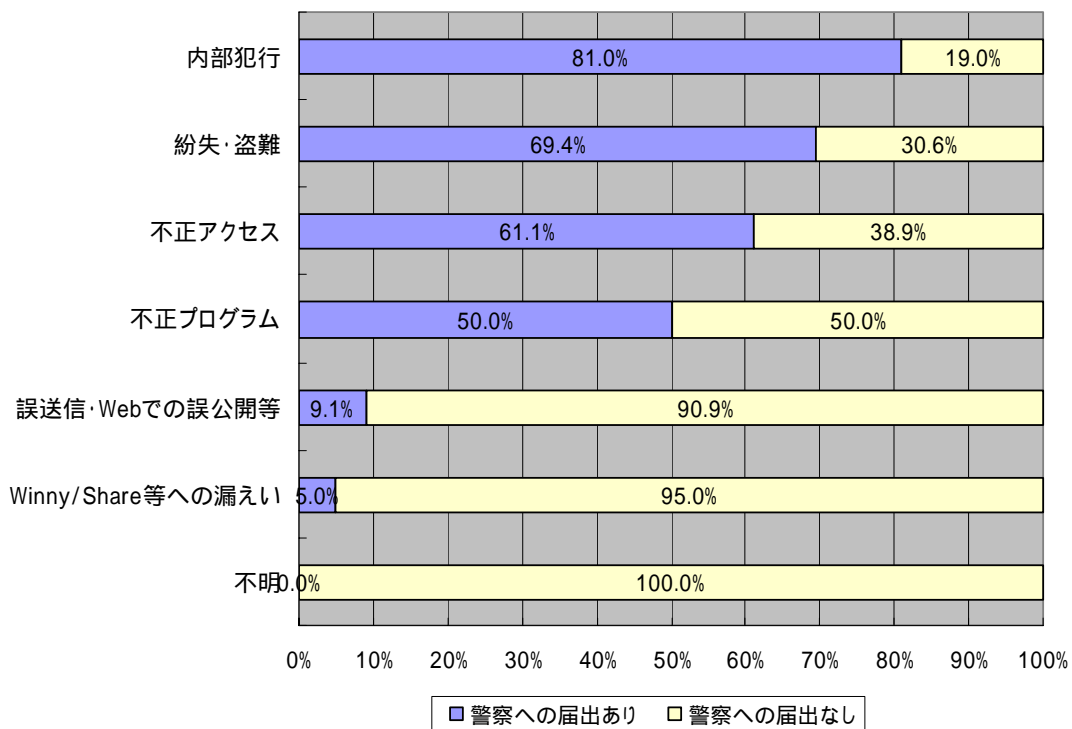


図 2.16 漏えい態様分類毎の警察への届出数

イ 個人情報漏えい事故のうち監督官庁への届け出が確認された数

個人情報漏えい事故のうち監督官庁への届け出が確認された数 (N = 131)

30件 / 131件 (22.9%)

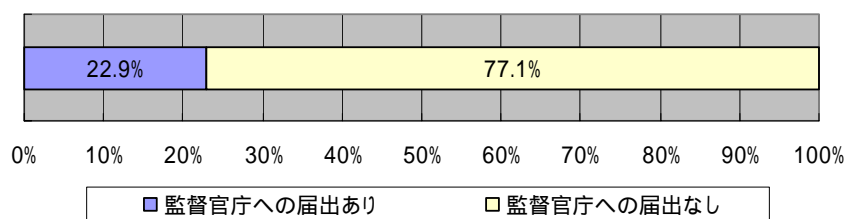


図 2.17 個人情報漏えい事故のうち監督官庁への届け出が確認された数

(4) 抑制措置と復旧

漏えい態様分類の場合に抑制措置としてサービスの停止が行われるかについて分析を行った。「不正アクセス」による情報漏えい事件において情報サービスの停止が行われるケースが多いことが確認された。

抑制措置として情報サービスを停止した事故事例の漏えい態様分類の内訳 (N = 18)

不正アクセス	11 / 18 件 (61.1%)
過失	5 / 18 件 (27.8%)
Winny/Share 等への漏えい	1 / 18 件 (5.6%)
不正プログラム	1 / 18 件 (5.6%)

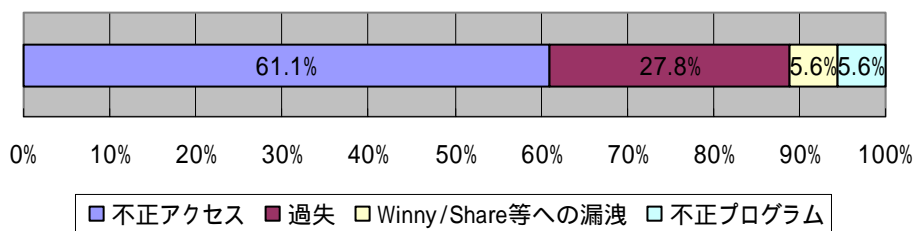


図 2.18 抑制措置として情報サービスを停止した事故事例の漏えい態様分類の内訳

漏えい態様分類が不正アクセスである事例のうちサービスを停止したもの (N = 18)

11 / 18 件 (61.1%)

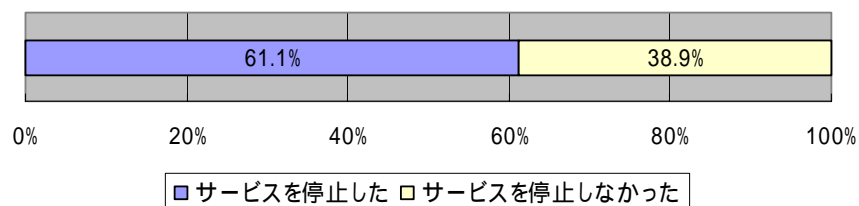


図 2.19 漏えい態様分類が不正アクセスである事例のうちサービスを停止したもの

(5) 事後対応

情報漏えい事故において損害賠償を支払うに至ったケースにおいてはこういった態様の漏えいであったかについて分析を行った。損害賠償を支払うようになったケースにおいては詐欺、いやがらせなど二次被害が発生している場合であることが確認された。

損害賠償を支払うケースのうち2次被害が発生している件数

8 / 8件 (100.0%)

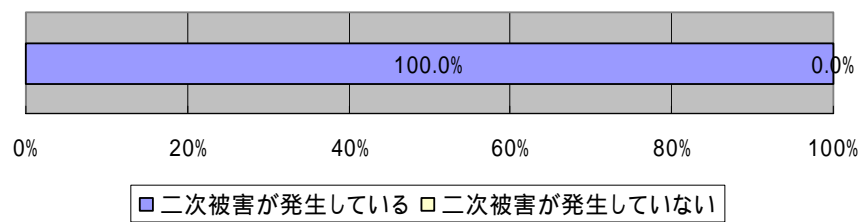


図 2.20 損害賠償を支払うケースのうち2次被害が発生している件数

4.3 漏えい態様毎の分析

(1) 二次被害につながりやすい漏えい態様分類

どういった漏えい態様分類に該当する事例について二次被害の発生が確認されることが多いかについて分析を行った。この結果「内部犯行」による事故において二次被害が確認されている割合が高いことが確認された。これは内部犯行が漏えいした個人情報を用いた詐欺など二次被害の発生から内部犯行が明らかになるケースなども含んでいる。また、「Winny/Share 等への漏えい」ケースにおいても実際に二次被害の確認に至るケースが相当数あることが明らかになった。

内部犯行	11 / 21件 (52.4%)
不正プログラム	1 / 2件 (50.0%)
不正アクセス	4 / 18件 (22.2%)
誤送信・Web 等での誤公開	4 / 22件 (18.2%)
Winny/Share 等への漏えい	2 / 40件 (5.0%)
紛失・盗難	2 / 49件 (4.1%)
不明	0 / 1件 (0.0%)

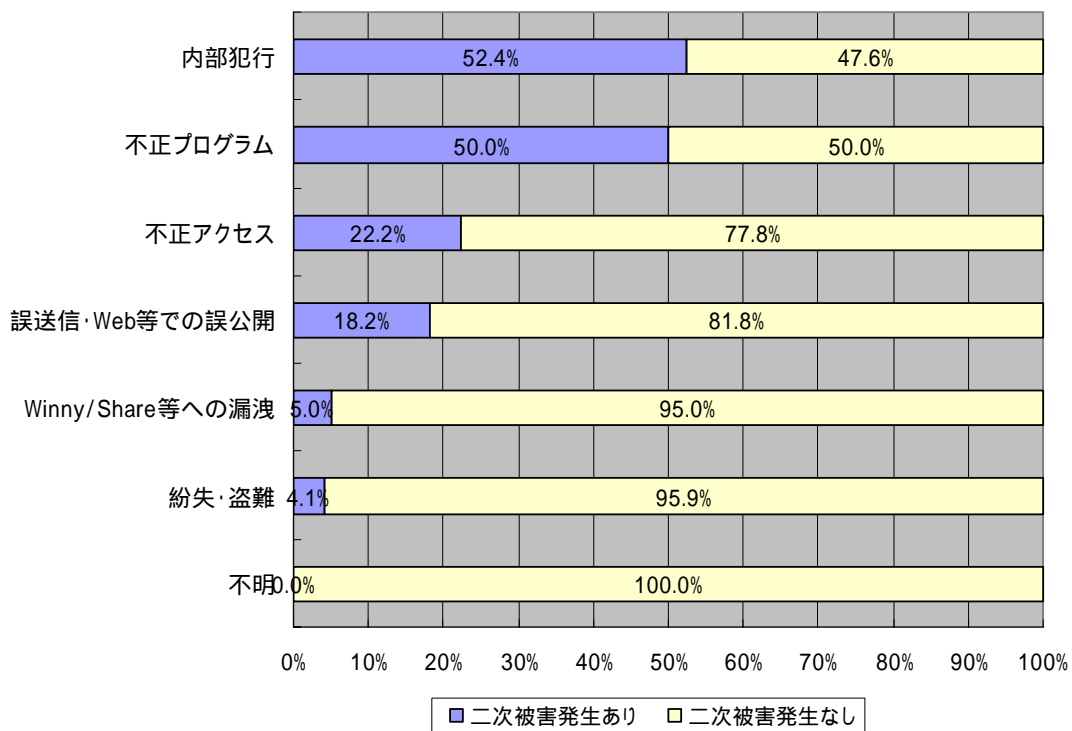


図 2.21 二次被害につながりやすい漏えい態様分類

(2) 不正アクセスを受けた場合の対応

不正アクセスにより情報漏えいが発生した場合には、被害拡大防止のためサービスを停止することが多く、再発防止として技術的対策の強化を掲げるケースが多い。

不正アクセスである事故のうちサービスを停止したものの

11 / 18件 (61.1%)

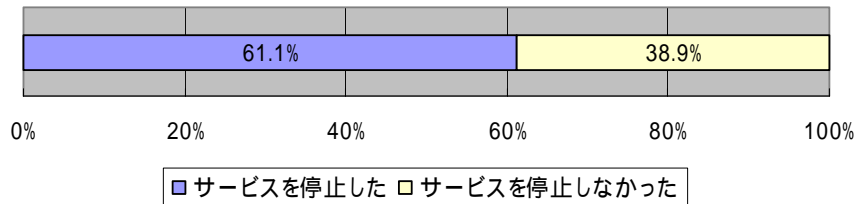


図 2.22 不正アクセスである事故のうちサービスを停止したものの

原因が不正アクセスである事故における再発防止策

技術対策強化	15 / 18件 (83.3%)
サービス停止 (一定の間)	11 / 18件 (61.1%)
内部管理強化	9 / 18件 (50.0%)
従業員教育・徹底	2 / 18件 (11.1%)
その他	0 / 18件 (0.0%)

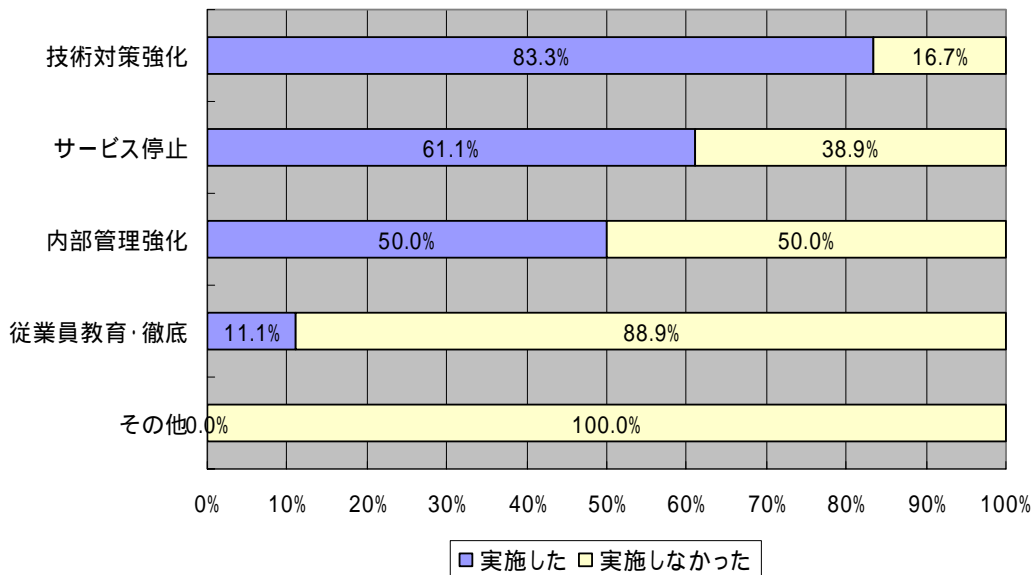


図 2.23 原因が不正アクセスである事故における再発防止策

4.4 漏えい情報のタイプの留意事項

(1) 漏えい情報種別による問い合わせ窓口の設置状況

情報漏えい事故全体に対してどの程度の割合で漏えい情報の種別により窓口設置漏えい情報の種別毎の被害者救済のための専用窓口設置の件数を確認した。また個人情報にクレジットカード情報が含まれる場合に、クレジットカードの不正利用等による二次被害に発展するケースが多く確認されている。

問い合わせ窓口を設置した事故件数 69件 / 153件 (45.1%)

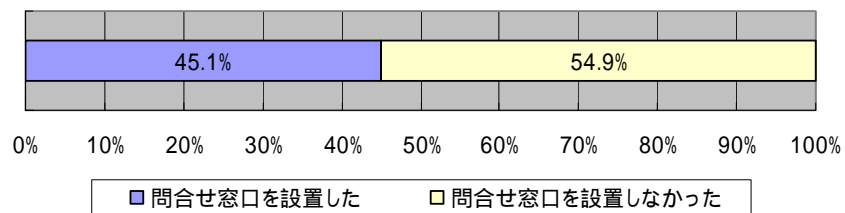


図 2.24 問い合わせ窓口の設置状況

漏えい情報種別の内訳

個人情報 66 / 131件 (50.4%)

一般情報 2 / 11件 (18.2%)

公共性の高い情報 1 / 11件 (9.1%)

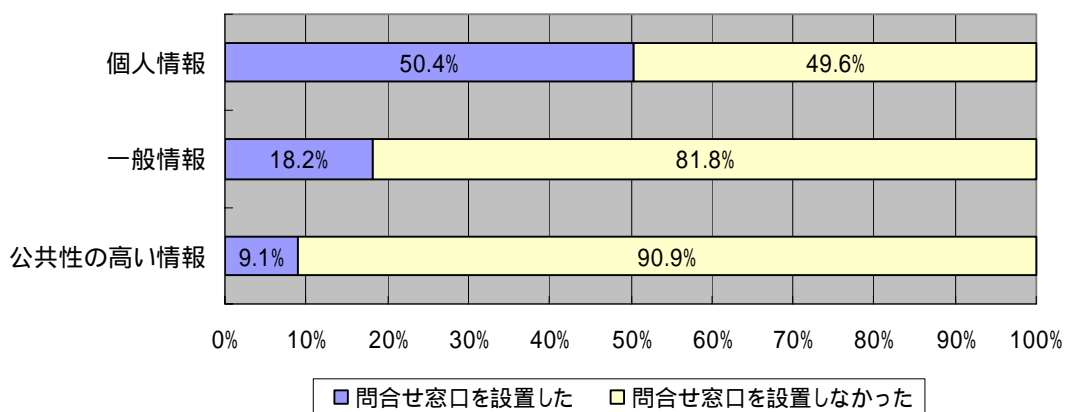


図 2.25 漏えい情報種別による問い合わせ窓口の設置状況

第3 情報漏えい対応策

1 情報漏えい対応の枠組みと基礎

1.1 情報漏えい対応ポリシーの必要性

万が一、情報漏えいが発生した場合においては、企業等は、各自、危機管理の観点をもふまえて情報漏えい対応ポリシー（対応方針と手順をいう。）を準備しておくことが有益である。ここで、情報漏えい対応ポリシーというのは、情報漏えいの際の組織等の対応に関する組織文化、原則、対応手順などについての構成員の行動をコントロールするための総体をいう。

「情報セキュリティ総合戦略-世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上」¹⁴によれば、「企業においては、情報セキュリティに係る事故が頻発しているにもかかわらず、我が身に置き換えて想定することができず、実際に被害が発生しない限り対策が進展し難い。また、対策の方向性、実施規模、実施方法などについて経営トップだけでなく現場エンジニアにとっても迷いがある。特に中小企業では、ファイアウォールやアンチウイルスなどの定番製品を導入した段階で停滞している感がある。」とされており、このような報告書においては、現在の日本における対応は、「対症療法しかとられていない」ものであるとされている¹⁵。

このような前提にたつときに、情報漏えいを想定して、情報漏えい事件が具体的に発生する以前に、十分な準備をしておくことはきわめて役に立つこととすることができる。上記報告書によれば、「『情報セキュリティに絶対はなく、事故は起こりうるもの』との前提で、事故・事件からの迅速な回復力の確保を図った『しなやかな社会システム』を構築する。すなわち、全体として事故の回避（予防）、被害の最小化・局限化及び回復力の確保が達成されるよう、官民が連携して総合的な視点から対応を強化する。」ことが大切なのである¹⁶。情報漏えい事件の発生は、緊急事態ということができる。このような場合には、通常の判断能力を期待することは困難になってしまうのである。そのような場合に、被害の拡大防止・損害の回復、企業に発生するダメージの低減、企業活動の継続などの種々の要請を果たすことは、きわめて重要かつ困難な業務になるのである。また、特に情報漏えい対応の実際は、なかなか事実関係が把握できない中で始まる対応作業であり、しかも迅速な対応が求められるのである。やり直しもできない。このような事情のもとで、よりよい判断をなそうとする場合には、事前の準備が大きな意義をもってくる。

¹⁴ 以下、「情報セキュリティ総合戦略」という。

<http://www.meti.go.jp/policy/netsecurity/strategy.htm>

¹⁵ 「情報セキュリティ総合戦略」9頁

¹⁶ 「情報セキュリティ総合戦略」14頁

また、事業継続という観点からするときには、経済産業省の「企業における情報セキュリティガバナンスのあり方に関する研究会」の報告書¹⁷（以下、「情報セキュリティガバナンスのあり方」報告書という）において、IT事故を想定した事業継続計画（BCP）の策定が推奨されている。緊急時の対応自体は、ある意味でマニュアル化に適合しない要素があるとしても、事前に緊急時を想定しておいて、これに対応することは必須であり、その意味で、情報漏えい事件対応について事前に準備することの重要性は、いくら強調しても、強調しすぎることはないということがいえよう。

情報漏えい事件などを起こしてしまった場合、普段の組織の素顔が見えてしまうのであり、そのために、企業が外部の消費者等に対して普段どのように位置づけているのか、また、対応チームが、消費者の方を向いて活動しているのかなどの企業文化が、その対応の成否の基盤となっているのである。これらを念頭において、対応の方策を考えていくことが重要である。緊急時においては、「普段できていることしかできない」「普段できることもできなくなる」「普段していないことはできない」という特徴がある¹⁸。そのような緊急時に適切に対応するためには、事前の準備が必要になってくることになる。このような観点から、経営陣が情報漏えい対応について、危機管理の観点をも踏まえて位置づけることが根本的な要請¹⁹であろう。

¹⁷ <http://www.meti.go.jp/report/downloadfiles/g50331d00j.pdf>。また、その 24 ページにおいて、情報漏えいが、事業継続計画（BCP）の発動の契機となることが記載されている。

¹⁸ 山口英「ITの専門家には任せない情報セキュリティの必要性」（RSA Conference Japan 2007 における講演）。この内容については、<http://journal.mycom.co.jp/articles/2007/04/27/rsa1/index.html> などで報道されている。

¹⁹ 上記「情報セキュリティガバナンスのあり方」報告書においては、事業継続計画（BCP）に関し、基本的考え方、総論、策定に当たったの検討項目、個別計画の4つの章と、参考資料から説明がなされている。そして、その付録の の A - 1 5 ページにおいては、「計画発動段階」「業務再開段階」「業務回復段階」「全面復旧段階」に分けられたあと、それぞれ、

「計画発動段階」

- ・情報の収集方法
- ・判定のための組織と情報の伝達
- ・対応方針の判断

「業務再開段階」

- ・復旧の方法およびダウンタイム
- ・バックアップへの移行方法
- ・顧客に対する連絡・開示・説明に関する事項

「業務回復段階」

- ・障害の原因特定や復旧作業の進捗状況の正確な把握

これらの手順を意識して、通常の業務が構築されていることが重要であり、まさに、「危機対応時に実施することを常日ごろから実施していく必要がある。通常のビジネスプロセスに危機管理の作業を組み込むことが重要なのだ」ということになる（上記・山口講演）。

その際に、情報漏えい事件対応ポリシーについて、どのように考えるかという点については、一般にリスクマネジメントで議論されていることと同様である。具体的な枠組みとしては、（１）基礎的部分（２）リスク評価部分（３）プロセスにおける業務手順の各構成要素をもとに、各組織において、それぞれ到達目標を定め、評価し、改善していくことが求められることになる（図3.1）。

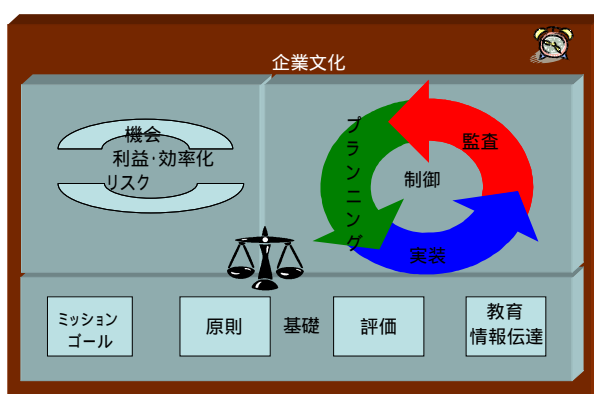


図 3.1 情報漏えい対策・基本から考える

- ・ 全面復旧に至る手順やスケジュール
- 「 全面復旧段階 」
- ・ バックアップサイトからメインシステムへの切り替え
 - ・ 平常運用に移行するためのテストや検証
 - ・ 各種データの受け渡しや保全に係るチェックリストの策定
 - ・ 全面復旧完了の対外的通知
- などの事項が、このような計画の内容として設けられている。

- (1) 基礎的部分としては、各組織のミッションおよびゴール、対応の基本原則、評価基準、教育・伝達の要素があげられる。これらは、情報漏えい対応ポリシーという形態で、具体化されることになる。これらのポリシーの全体像は、

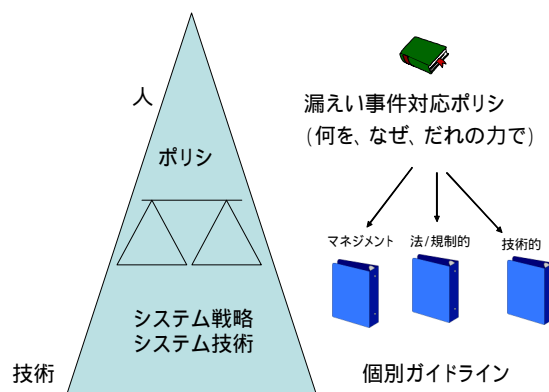


図 3.2 漏えい事件対応ポリシーと個別プログラム

とう形で図解される。この三角形の一番高いところにまさに図 3.2 で基盤となっている企業のミッション、ゴール、基本原則などであり、それらが情報漏えい対応の際の各対応チームメンバーの具体的な行動に具体的に反映されたものとなる。

- (2) リスク評価部分については、その保有している情報が漏えいした場合の組織等における損失、また、漏えい対応にかかるコストなどの評価がなされることになる。
- (3) プロセスにおける業務手順については、情報漏えい対応チームの各構成員の行うべき業務手順を作成することになる。本書の「第3の2 情報漏えい対応の具体的な段階」以下は、そのような業務手順をまとめる際の留意点として参考になろう。

1.2 情報漏えい対応の目標

本章の最初でふれたように、情報漏えい事件のような緊急時の対応において、まさに各企業の素顔が現れてしまうということに経営者は留意すべきである。そして、そこで、現れてくる企業の素顔は、経営者等の普段の姿であることが多いのである。これらを肝に命じて、最終的に情報漏えいによって被害を蒙る被害者のことをよく考えて行動することがきわめて重要である。他の組織が、情報漏えいを発見して公表しているからといって、こういった情報が漏えいしたのか、最終的な被害者は誰なのかなど具体的な事情を考慮せずに紋切り型で、あたかも自分たちのメンツのためだけで動くようなことは厳に慎まなければならない。このような観点から、情報漏えいに関する対応チームの構成員の行動の導きとなるような対応の目標をあげておくことは、きわめて有意義であろうと思われる。

一般に、情報漏えい対応の目標とは、情報漏えい発生前、後のいずれの場合においても

「情報漏えいによる直接的・間接的被害を最小限に抑えること」

になるものと思われる。

もっとも、この場合の具体的な被害のなかには、組織等の保有していた情報自体の損害という意味もあり、また、本人に発生した損害という場合もある。実際に、どのような被害をどのような重要性をもって位置づけるかということは、組織等において、社会の利害関係者との関係をどう考えるかということに影響されることになるであろう。

1.3 情報漏えい対応の諸原則

組織等において、情報漏えい発生時に対処する際に、守るべき諸原則を下記に述べる。

(1) 「被害拡大防止・二次被害防止・再発防止の原則」

情報漏えいの事実が確認された場合、漏えい情報から二次被害が発生するか否かを見極め、二次被害が発生する可能性がある場合は、直ちに二次被害を防止する策を実施する必要がある。例えば、電子商取引サービスを提供していて、顧客のIDとパスワード情報が流出した場合、直ちに顧客への了解を得た上でアカウントの停止や変更等の措置を取る必要がある。これによって、成りすましによる発注などの二次被害を防止する。

情報漏えいが発生した場合、必ず原因がある。直接・間接的な原因を特定し、再発を防止する措置を実施する必要がある。

(2) 「事実確認と情報の一元管理の原則」

情報漏えいがあった可能性があるという、いわば「おそれ情報」情報に接してから、組織内においては、正確な情報、あいまいな情報や噂などが、社内又は社外いずれかのルートから入ってくることになる。このような交錯する情報のもとで、情報漏えい対応チームとしては、情報漏えい自体の事実確認を実施し、漏えい情報の性格・範囲、漏えいの態様、漏えいの原因・経路などを見きわめながら、短期間の間に迅速な意思決定を行うことを要求される。関係者の努力によって、できるだけ正確な事実を見きわめて、それにもとづいて行動することが必要であり、まさに事実確認が原則となる。

そして、そのためには、「正確な情報の記録・集中・管理」が重要である。そもそも、対応チームを構成する最大の利点は、「情報の一元管理」にある。緊急時に錯綜する情報は、混乱をもたらすだけで、有意義な意味を有しない。正確な情報を対応チーム内で共有し、しかも、その対応チームのもとに対外の窓口を一本化するということが望ましい。このために、対応チームの部屋の場所や配置などへの配慮²⁰、さまざまな知識の集積、関係情報についての厳格なアクセス管理が必要になる。そして、これらの情報に基づく一元的な業務に関する指揮命令が必要かつ重要になってくる。

また、そのような目的のために正確な情報を、逐次記録することが必要になる。センシティブな情報が不適切な形で流出した場合、より大きな問題と経済的な損失をもたらしか

²⁰ (NIST SP800-61)J 3-2 では、「作戦本部室(war room)」が必要であるとしている。また、(中島, 2007)99頁は、大型スクラップブックを活用した「情報マスター」の作成を推奨している。

ねないのである。この正確な記録は、後に個別の対応の是非等についての分析などについても大きな役割をはたしてくれるであろう。

その上に、情報システムが関係するデジタルデータは、うつろいやすく、容易に変更・改ざんがなされるので、後々に事件に発展する場合や原因を特定するために、機器類のデータやログ等を保全する必要がある。しかも、事件後の詳細な調査の際に、そのデータ等の信用性に疑問をいだかせないような確立した実務的な手順を遵守する必要がでてくる。事実確認や調査の際には、既存のデータやログなどに影響がないよう操作・調査する必要がある。

(3) 「透明性・開示の原則」

情報漏えいが発生した場合、利害関係者に対して、当該事実を開示・報告する必要がある。利害関係者とは、顧客（個人情報、企業等情報）、業務取引先（企業等）等の漏えいした当該情報の当事者は当然含まれるが、当事者以外にも、監督官庁、報道機関、当事者以外の業務取引先などを含むものである。これらは、二次被害防止・類似被害防止・説明義務の履行の観点から必要とされるものである。詳しくは、「第3の2.5 通知・報告・公表等」を参照のこと。特に現代社会において、一般消費者との接点を有する組織等において、説明責任を果たすべきことは、義務の一つであると認識すべきであるといえる²¹。また、適切な対応がなされれば、ブランドの評判を維持することができるばかりか、場合によっては、その評価をあげることができる²²とされている。

なお、報道機関への広報やインターネットによる自社発表等の手法により開示をするか

²¹ 食品衛生法上販売が許されていない添加物がダスキンの販売する食品に使用されていたという事実に関するいわゆるダスキン事件の一連の判決のうち、事実隠蔽行為について、大阪高裁判決(平成18年6月9日)は、「事実を隠ぺいしたなどということになると、その点について更に厳しい非難を受けることになるのは目に見えている。」現に行われてしまった重大な違法行為によってダスキンが受ける企業としての信頼喪失の損害を最小限度に止める方策を積極的に検討することこそが、このとき経営者に求められていたことは明らか」と述べている。なお、この事件を含む説明責任の概念については、高橋郁夫「2006年情報セキュリティと法的問題の概観」(<http://www.ipa.go.jp/security/event/2006/ipa-forum/061024h.pdf>)参照。

²² 国民生活センター特別調査事務局の「[特別調査]:「製品回収」をめぐる現状と問題(概要)」(http://www.kokusen.go.jp/pdf/n-20030806_1.pdf)における「製品回収のあり方に関するアンケート調査・1.消費者へのアンケート調査」の「(3)告知して回収を行う企業に対するイメージ」によれば、企業が製品の回収を実施するに当たり、新聞社などで告知して回収をおこなった場合、一般消費者が、その事業者に対して「その企業やブランドに対する信頼はかえって高まる」と回答した人が、47.3%に達するという。このことから、企業活動に関する事件については誠実に説明義務をはたすことが、好結果を産むことが明らかになるであろう。

否かは、二次被害の防止の観点（公開することによる被害の拡大）、漏えい情報の内容と量から想定される社会的影響から判断の余地がある。この点については、「第3の2.5.1（4）」において詳細に検討される。

いうまでもないが、情報漏えい対応としては、その対応が、法律・基準・社会常識等の見地から見て適正なものであることが必要である。事実究明のためとはいえ、法律に違反した形での究明手段が認められるわけではないし、また、反社会的な活動勢力に対して、援助する等の効果を有するような行為が許されるわけではない。そのような対応が社会に対して開示しえるかというのが、その適正性の判断の一つの基準となるのであろう。社外からの情報漏えいの事実の通報や内部犯罪の発覚に名を借りた反社会的勢力等からの要求の例を見受けることができる「第3の2.2.3」。このような場合には、毅然とした対応が必要となる。特に、社外からの情報漏えいの事実通報の場合、善意の第三者を装う場合があるため、その見極めと警察や弁護士等との連携が必要となる。

（4）「チームワークの原則」

本報告書が対象とする中小企業においては、経営に属する問題の決定権を有する対応責任者というチームリーダーによってリードされる少数のメンバによって構成されるチームが必要であり、しかも、そのチームワークで情報漏えい事件に対応することが何にもまして必要になってくる。

緊急時には、きわめて多数の困難な判断を迅速になさなければならず、また、それぞれの判断にもとづいてなされる行動もきわめて精神的に負担が重いものである。そのような状況のもとで適切な対応をするためには、チームのチームワークによって解決されなければならない。中小企業でいえば、一つの会議室で集まって、リーダーのもとで、みんなで議論をしながら、対応していくという対応方法が望ましいということがいえる。その一方で、組織のトップが、部下に対して「具体的な対応は、あとは任せたから、よろしくな」という対応姿勢が一番問題になる。これは、組織のトップが、重要性を認識していないということの意味しているし、また、具体的な対応途中で起きる種々の経営判断の問題を責任をもって処理し得ないことにつながることになる。なお、大規模な企業においては、分散型対応チームとでもいうべき構成²³が念頭におかれるが、本報告書においては、割愛することにする。

中心的なメンバとしては、リーダー以外には、会社において、広報を担当するもの、情報

²³ NIST SP800-61 は、2-8 で、特定の担当分野（広報、法務、渉外、営業など）もしくは物理的な要素ごとに対応責任を有する対応チームの分散型対応チームを紹介している。もっとも、この場合でも、対応チーム本部がすべての本部となり、組織にわたって統一的な対応ができ、情報が共有されるようになっていることが重要なことはいうまでもない。

技術を担当するもの、法律面を担当するもの、顧客への対応を担当するものなどが含まれることになる²⁴。

(5) 「備えあれば憂いなしの原則」

情報漏えいは、発生させないように事前に予防措置を取ることが肝要であるが、それにもかかわらず、情報漏えい事件に関与した場合のための準備をしておくことが、最大の防御になる。前述したように緊急時においては、「普段できていることしかできない」「普段できることもできなくなる」「普段していないことはできない」のであるから、緊急時に適切に対応するためには、事前の準備が必要になってくることになる。情報漏えい発生時の準備として、情報漏えい対応ポリシーの整備が必要なのである。

2 情報漏えい対応の具体的な段階

2.1 準備段階

2.1.1 総論

経営陣としては、情報漏えい時の対応が、いわば、危機管理対応の一環としても位置づけられ、しかも、その対応時の計画が、通常システム運用におけるポリシーの一環として構築・実装されることと連携し、しかも、そのような認識にもとづいて、通常運用においても、日頃から意識され、実行し、かつ実行されていることを確認・問題があれば改善していくことがもとめられることになる。

²⁴ (NIST SP800-61)J2-9 においては、対応チームについて、「24時間365日対応の必要性」「職員のモラル」「予算の問題」「専門技術の問題」などがあり、それらが重要になることを論じている。

これらの観点から準備段階において考慮すべき事項としては、以下のようにまとめることができるものと思われる。

表 3.1 情報漏えい対応の準備段階で考慮すべき事項

必要な機能	平常時の主な業務内容	情報漏えい発生時の主な業務内容
マネジメント	<ul style="list-style-type: none"> ・セキュリティポリシーの制定 ・セキュリティポリシーの遵守状況のモニタリングと是正策の企画・実施 ・セキュリティインシデントの把握（報告が上がる文化を醸成すること）と対策の企画・実施 ・組織内へのセキュリティ教育の企画・実施 	<ul style="list-style-type: none"> ・情報漏えい事実の確認 ・必要な情報を一元的に集約、整理する ・情報漏えい発生時に必要に応じて情報を集約し、対応チームを構成し、組織としての情報共有、意思決定、各機能を担う部署・メンバへ指示を行なう。また、経営トップへの報告を実施する。 ・再発防止策の立案
情報システム	<ul style="list-style-type: none"> ・組織内の情報システムの企画・設計・運用 	<ul style="list-style-type: none"> ・情報資産の重要性の分析・格付け、攻撃の影響力想定 ・証拠保全 ・情報システムのログ調査、分析 ・情報漏えいの発生原因の取り除き ・再発防止策の実施
広報	<ul style="list-style-type: none"> ・社内広報 ・社外広報 	<ul style="list-style-type: none"> ・対外広報が必要な場合 <ul style="list-style-type: none"> ・文案の策定 ・経営陣へのレクチャ ・対外広報の一元的対応（記者会見、Webによる発表、取材申し込みによる対応）
法務	<ul style="list-style-type: none"> ・法的規制の把握 ・弁護士との窓口 	<ul style="list-style-type: none"> ・広報内容のリーガルチェック、場合によっては、弁護士への確認 ・個人情報保護法等法的に報告義務がある監督官庁への報告 ・プライバシーマーク等民間の認証登録機関への報告
総務・人事	<ul style="list-style-type: none"> ・組織内でのリスクマネジメント全般（恐喝等犯罪等） ・就業規則等の規定類の制定 	<ul style="list-style-type: none"> ・リスク管理、捜査機関への相談・届出 ・必要に応じて、懲戒処分等の検討、決定

そして、これらの観点について、一定の対応ポリシーを準備して、従業員教育、漏えい対応訓練などを行うことが有意義になってくるのである。

そして、個人情報保護ガイドラインにおいて、このような漏えい対応策を事前に検討しておくことが個人情報保護法の第20条の「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」において求められている措置の一つに含まれているものと解されている。具体的には、その安全管理措置のうちの「組織的安全管理措置」に「事故又は違反への対処」が含まれるものと解されている。詳しくは、法律的観点の記述

を参照。

特に、このようなマネジメントの体制において、重要なのが、「広報」に関するマネジメントである。現代社会においては、説明責任の観点がかきわめて強く要請されていることを念頭におかなければならない。この観点から、「不測の事態が発生した場合、その影響やダメージを最小限にとどめるため、内外の必要と考えられる対象に対する『情報開示』を基本にした、迅速、かつ適切なコミュニケーション活動」としてのいわゆる「クライシス・コミュニケーション」²⁵対応は、きわめて重要な意味をもつものといえる。「人はおこしたことでなく、おこしたことにどう対応したかによって非難される」といわれることも多い。準備段階において、情報漏えいが発生した場合の対応の目的をきちんと押さえておくことが重要である。一般的には、組織外における被害者がいる場合（本人など）には、そのような被害の低減・最小化・回復を主としつつ、自社と個々の利害関係者の損失を最小限に押さえることが目的となろう。その具体的な広報の活動においては、種々の利害関係者の利害を判断する必要性が生じる。その様な場合に、一定の判断をしたときに、どういう合理的な判断をしたかをきちんと残しておくことが重要になってくる。

以下、具体的に本報告書の前提とする3つの観点から、基本的な点について解説をする。

2.1.2 具体的な観点

(1) マネジメント的観点

情報漏えい事故を起こさないように、セキュリティを十分に考慮したシステム・アプリケーションの運用を考えることが一番大切であり、そのような運用によって、事故までにいたらない事象の数を減少させることは、トータルで見た場合に万が一の対応の余裕を生むものということもできるであろう。そして、日頃の運用において定期的にセキュリティのリスクの評価を見直し、ポリシーを見直し・改善していくということが重要になる。特に外部からの攻撃を考えたときに、日々新たな攻撃手法が生まれ、脆弱性が発見されており、定期的なリスクの見直しというのは、欠かせないものなのである。

しかし、それでも万が一のことはありうるのであり、上記のような準備的な事項について、あらかじめ準備し、普段から、予行演習等を行うことが望ましい。予算の準備、時間の確保なども経営者の責任となる。また、通常の業務において、営業担当者は、取引先の一覧などをまとめておいて、事故が発生した場合に謝罪に訪問できるようにしておくことも意義がある。

(2) 法規制的観点

このような情報漏えい事件を想定して、事前に準備しておくということは、法/規制という観点からも、本来要請されているものであると考えることも可能である。

各省庁における個人情報保護のガイドラインにおいて、このような情報漏えいの事件を想定して対応すべき組織・権限・留意すべき事項を事前にまとめておくことが、個人情報

²⁵ (東京商工会議所, 2005) 26 ページ

保護法の第20条の「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならぬ」に関して求められている。経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成19年3月版）（以下、「経済産業分野ガイドライン」という）²⁶は、法20条の措置の一つの「組織的安全管理措置」に「事故又は違反への対処」が含まれるとしており、また、「金融分野における個人情報保護に関するガイドライン」（以下、金融分野ガイドラインという）の「第20条関連」の「(2)各管理段階における安全管理に係る取扱規程」において「漏えい事案等への対応の段階における取扱規程」を定めるべきとの記載がある²⁷。

「電気通信事業における個人情報保護に関するガイドライン」は、第11条（安全管理措置）において、「電気通信事業者は、安全管理措置を講ずるに当たっては、情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）等の基準を活用するものとする」とし、そこで引用されている「情報通信ネットワーク安全・信頼性基準」（昭和62年郵政省告示第73号）の別表第2管理基準の「5 情報セキュリティ管理」（2）は、「危機管理計画の策定」「不正アクセス等への対処を定めた危機管理計画を策定し、適宜見直しを行うこと。」と記載している²⁸。「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」²⁹（以下、金融分野実務指針という）においては、「(2)個人データの安全管理措置に係る実施体制の整備」における「1)実施体制の整備に関する組織的安全管理措置」において「漏えい事案等に対応する体制の整備」が必要としている。そして、具体的に2-6以下において「金融分野における個人情報取扱事業者は、『漏えい事案等に対応する体制の整備』として、次に掲げる体制を整備しなければならない。

対応部署

漏えい事案等の影響・原因等に関する調査体制

再発防止策・事後対策の検討体制

自社内外への報告体制」と定められている。

法的な観点からの事前準備という立場からは、情報漏えい事件が発生した場合に検討が必要となる法的な問題点およびその際に具体的に連絡すべき担当者などを一目でわかるように準備しておくことが必要である。刑事的な対応が必要になる場合に備えて、管轄の警察署等におけるサイバー犯罪担当者の氏名・連絡先などについて、事前に準備しておく

²⁶ http://www.meti.go.jp/policy/it_policy/privacy/070330guideline.pdf

²⁷ <http://www.fsa.go.jp/common/law/kj-hogo/01.pdf>

²⁸ http://www.soumu.go.jp/joho_tsusin/whatsnew/kokuji/network_0203_2.html

²⁹ <http://www.fsa.go.jp/common/law/kj-hogo/04.pdf>

ことは有意義であろう。また、上場企業においては、投資家関係窓口の氏名・連絡先が必要になってくることもある。

(3) 技術的観点

NIST SP800-61の「3.1 準備」によれば、一般的な準備として(ア)組織において漏えい前兆・兆候の探知および分析の重要性の強調(イ)事前における情報漏えい事件の影響分析が必要であるとしており、具体的な準備として(ウ)事件処理担当者への連絡と設備(エ)事件分析ハードウェアとソフトウェア(オ)事件分析リソースが必要であるとしている。

これらの事項の内容は、以下のとおりである。

ア 漏えい前兆・兆候の探知および分析の重要性の強調

組織等においては、通常において、ログインやセキュリティに関する記録を取得しており、実際の事件が発生した場合、それらの記録が重要な分析のためのツールになる。したがって、これらを自動的に分析するのに容易なように事前に準備しておくことが望ましく、また、技術的な観点からもそのような分析が可能になるようにしておくことが重要であることを組織等において常に強調しておくことが望ましい。

セキュリティイベント相関分析手法や集中監査システムは、この分析を自動化するのに効率的な手法であるといわれており、通常から、そのようなシステムの導入を経営層に強調しておくだけの意義はあるものとされている。

イ 事前における情報漏えい事件の影響分析

上記のような事業継続計画において、その計画のもとをなすのは、情報漏えい事件が組織等に対して、どのような影響をおよぼすかという点についてのリスク評価ということになる。この影響は、攻撃等を受けたネットワーク資源(サーバやワークステーション、その他の通信機器)の重要性の観点と、事件の技術的影響(管理者権限の奪取、データの損壊)の影響の二つの観点から、分析されることになる。

これらの分析に基づいて、経営陣は、下請けなどに際して、どれだけの脅威があった時に、どれだけの営業停止時間が必要であるかというのを把握することができる。また、組織において優先順位を定めることができ、また、回復のために行うべきことがきまってくるのである。そして、このような考察に基づいたときに、サービス・レベル・アグリーメントを締結することも可能になってくるのである。

ウ 技術者の通信手段および設備

具体的には、連絡先情報、報告手段、携帯電話、暗号ソフトウェア、作戦本部室、安全な管理手段などがあげられる。ここで、報告手段というのは、システム関係において問題となる契機が見つかった場合に、一般のユーザなどが連絡すべき電話番号、電子メールアドレスなどのことをいう。

エ 分析のためのハードウェアおよびソフトウェア

具体的には、フォレンジック・ワークステーションとバックアップ機器、ノート PC、

PC・サーバ・ネットワーク機器のスペア、記録メディア、持ち運び用プリンタ、パケット・スニッファなどがあげられる。

オ 分析のための参考資料

実際の現場で、種々の情報が事前に準備できていないと対応が困難になる。事前に準備できていると望ましい情報資料としては、ポートのリスト、説明書、ネットワーク構成図などがある。

2.1.3 準備を怠っていた場合には

危機管理においては、平常時、緊急時、収束時の3つの局面があるといわれる。そして、平常時において、組織体の構成員における意識と行動についてのコントロールがなされていれば、緊急時においても、その被害の低減や利害関係者への説明責任の遂行などがスムーズになされるものと考えられる。まさに「Be prepared and you'll be all right (備えあれば、憂いなし)」となるのである。しかしながら、実際には、そのようなうまくいかないのも現実である。そのような場合には、本報告書などをはじめとして早急に対応方針を決め、関係者での対応チームを構築し、情報漏えい事件に対応していくことになる。そのような場合に、まず大切なことは、情報漏えいなどの事件対応において、常日頃、各組織体の構成員が、なにを大切に考えているのかということが明らかになるということである。その意味で、通常各組織体の行動を司っている行動規範を改めて認識することになるものと思われる。

そのような認識を前提にして、「行うべきこと」と「してはいけないこと」を認識することは重要なことであろうと思われる。

このような観点から、「行うべきこと」としては以下があげられる。

- ✓ 「情報漏えい対応には、その組織が、社会において果たしている普通の姿がもっとも凝縮して表れることを認識すること」
- ✓ 「関連する関係者の意識とちからをあわせて、協力しあって漏えい事件を乗り越えること」
- ✓ 「事実関係の正確な把握・確認が対応の基本を決定する」
- ✓ 「現代社会では、説明責任にもとづいて開示の姿勢が根本的なものとなる」

その一方で、してはいけないこととしては以下があげられる。

- ✓ 「普段やっていないことをやろうとしない」
- ✓ 「現場の人間だけに対応を任せきりにしたりしない」
- ✓ 「上司等への連絡において事実を隠蔽しない」
- ✓ 「消費者・マスメディアなどに対して現場の個人等で対応したりしない」
- ✓ 「ごまかしても世間にばれるはずがないと思わない」

また、そのような場合、情報漏えい対応サービスを提供している会社のなかで、緊急時の相談サービスを提供しているところもあり、そこに電話連絡をするというのも一つの対応のヒントやきっかけとなるであろう。ここでは、無料で、技術的な視点から、最低限や

っていけないことを伝えることもある。このようなサービスを証拠となるコンピュータに対して、触ってはいけないということを聞くことも有意義なものとなるであろう。

2.2 発見および報告

2.2.1 「発見および報告」のステップ

情報が漏えいしている可能性があることを、その情報の管理者たる企業等が発見する経緯には、種々のものがある。その契機としては、「自主的な申告（PCの紛失の場合など）」、「内部告発」、「内部監査」、「外部のものからの通報」、「マスメディアによる取材」などがある。そして、これらの発見の契機をはじめとして、このような情報は、情報漏えい対応チームリーダーである対応責任者に集約されることとなる。対応責任者は、これをもとに、次のステップである初動対応の段階に移行することになるのである。初動対応に移行すべきかどうか、情報を取得して、決断する過程が「発見および報告」のステップということになる。

2.2.2 「発見および報告」のステップにおける情報収集

「発見および報告」の段階で、発見の経緯に関連する情報は、その後の対応に有意義であるように網羅的で、かつ、効率的な利用できるような体制で取得される必要がある。また、このような情報は、最初に危機が発生したのかどうかという点について、その発見に関する契機につながる情報については、報告のルールをさだめて安全側に倒しておくことが重要である。通報基準と通報ルールの準備が必要ということになる。通報基準には、危機管理対応上、早期に把握することが必要な情報を例示して、判断しやすくすることが必要である。また、通報ルールに定められるべき通報ルートであるが、通常の職制が基本となるが、飛び越え、複数ルートの確保等により、連絡が途中で中断しないようにしておくことが必要である。

それらの目的なのために、「ヒアリングシート」の利用は、有効であろう。このようなヒアリングの際になされる項目および各項目ごとの注意事項は、以下のとおりとなる。

ア) 報告書の氏名および連絡先

イ) 漏えい情報の内容

ウ) 報告の根拠

エ) 根拠の詳細

オ) 協力依頼等

これらをチェックシートの形でまとめたものは、以下のようになる。

参考			
情報漏えい情報共有シート(例)			
件名	の情報漏えいについて		
報告者所属	事業部 担当	発災当事者所属	事業部 担当
報告者氏名	情報 太郎	発災当事者氏名	漏洩 次郎
報告者 Tel	03-XXXX-XXXX	発災当事者 Tel	03-XXXX-XXXX
報告者 Mail	XXX@XX.XX	発災当事者 Mail	XXX@XX.XX
下記の事項で、判明していることを記述する。 初報なので、不明な項目は不明として迅速に報告する事。			
情報漏えいの情報のソース(誰が発見したのか、どこから漏えい情報を入手したのか)			
情報漏えい判明日時			
情報漏えい発生日時			
情報漏えい内容			
情報漏えい内容の件数			
想定される原因			
対応状況(行なっていれば記述) ・特に組織外からの通報の場合、相手が何を要求しているのかを記述			

図 3.3 情報漏えい情報共有シート(例)

発見者は、情報漏えいの報告を予め組織内で定められた対応責任者に報告するという基本的な行動を社内教育等で浸透させておく必要がある。必要に応じて、発見者が情報漏えいの事実を隠蔽したり報告を怠ったりすることに対して、社員就業規則等で罰則を規定し、発見者の報告義務という行動責任を明文化することも考慮するべきである。

2.2.3 マネジメント的観点

上記のような情報をもとに、対応責任者は、次からのべる初動調査以降のステップに移行するかどうかという判断をしていくことになる。対応責任者に対して、この発見の段階において、事実関係が正確につたわるようにするのが最大の問題ということになる。そし

て、対応責任者は、これらの伝わった事実関係をもとに初動調査の段階に移行する判断をすることになる。そしてこれに関連して、組織内で情報をどの程度まで明らかにするか、刑事的な対応を依頼するかなどの付随的な判断をすることになる。

また、企業等に対して接触を図ってくる者のなかには、このような情報漏えいをきっかけとして不法な利益をえようとするものもいる³⁰。具体的には、金銭を支払えば、このような情報を消すといってくるものである。このような場合においては、このような不当な要求に対しては、法律専門家のアドバイス等をも活用しながら断固とした姿勢をもって対応することが推奨される。

2.2.4 法規制的観点

なお、この段階において、法律専門家が情報漏えい対応として関与することは一般的ではない。もっとも、内部告発（公益通報制度やそれに関連する広範囲な組織等の不正行為に関する情報受領）制度の担当窓口として、もしくは、組織等に対する不正行為者に対する対応過程において、情報漏えい発見の契機となることは、十分にありうることである。

内部告発において、このような情報漏えいの契機を把握した場合には、あらかじめ定められている手順にしたがって対応責任者に対して伝達することになる。

2.2.5 技術的観点

技術的専門家が、直接に、このような情報漏えいの契機として、情報漏えいの可能性を認識することは十分にありうることである。

具体的には、不正侵入の痕跡があるとか（具体的には、侵入探知システムがアラートを発したりすることがあるであろう）、ネットワークにおいて、不審な挙動があるとか、通信のスピードが遅くなるとかコンピュータの動作が遅くなるなどの場合である。また、技術的なもの以外にも、ヘルプデスクに問い合わせが多くなるとかもそのようなきっかけとなりうる。このような契機を示唆する情報が意味するところを正確に理解できようにするために、技術的な観点から、以下の情報が、きわめて重要な意味をもってくる。

ア アラート

侵入検知装置（IDS）、ファイル・インテグリティ・チェック・ソフトウェア、第三者による監視サービスなど

イ ログ

基本ソフトのシステム、サービス、アプリケーションのログ
ネットワーク・デバイスのログ、ハニーポットのログ

³⁰ NBL808号41ページ以下に若干の例があげられている。

そのあとの例として、DIONの個人情報、約400万件が流出、恐喝未遂で容疑者を逮捕という事件（平成18年6月13日）（<http://journal.mycom.co.jp/news/2006/06/13/381.html>）業務委託先の社長が、委託元の顧客情報約85万件が含まれている可能性のあるPCを隠匿し、金銭を脅し取ろうとした事件で、恐喝を受けた企業が、直ちに警察に被害を申告したという事件がある（平成17年9月16日）。

ウ その他

脆弱性や攻撃手法についての公になっている情報、他の組織における事件情報

これらの情報から、情報漏えいの可能性の存在の蓋然性を示す情報であると判断した場合は、証拠の確保の観点を中心に置きながら、収集した情報を事前に定められた対応責任者に対して伝達することになる。

2.3 初動対応

2.3.1 初動対応の概念

初動対応は、上記の発見および報告のステップで取得した情報をもとに、具体的な対応方法を発動すべきかどうかを決定するための情報収集・検討および決断するためのプロセスとして認識されることになる。対応責任者に対して情報漏えいの事実が伝達された段階までが、「発見および報告」の段階であるのに対して、その後、対応方法の決断に至るまでが初動対応の段階ということになる。

この初動対応において、どのような情報が、どのような経緯において、どの程度・範囲に流出したかというのを、迅速に究明し、明らかになった事実は、その後の具体的な調査に引き継がれていくことになる。具体的に収集されるべき情報としては、以下のものがあるものと思われる。

- (1) いつ漏えいしたか
- (2) 何が漏えいしたか
- (3) 何件漏えいしたか
- (4) どうやって漏えいしたか
- (5) どこから漏えいしたか
- (6) 何故漏えいしたか

これらの事実確認をもとに、開示の有無・手法・時期等の決定、証拠の確保、被害拡大の防止などに対して、正確な判断をなし、対応チームによる対処に移行することになる。

2.3.2 マネジメント的観点

(1) マネジメントの責務と基盤

対応責任者に対して、情報漏えいの発見および報告の情報が伝達されると、対応責任者は、情報漏えい事件として対応方針を検討することになる。このような対応方針という場合、「漏えいなしとして対応打ち切り」という場合以外には、漏えい事件として漏えい事件対応チームの構成に移ることになる。対応チームが構成された段階で、原因究明・(漏えい被害)本人対応・業務運営の継続・中断の判断、広報対応などに関して、専門的な対応のための準備事項を決定していくことになる。

(2) 正確な情報の記録・集中・管理³¹

構成チームの行うべき職務のうち、後述の法規制的観点、技術的観点とは、異なる要素としては、広報、渉外、消費者担当などがあり、また、それらを支える基本的な要素としては、「正確な情報の記録・集中・管理」がある。

(3) 正確な調査のための準備

情報漏えいの発見の契機から、復旧・事後対応にいたるまで、正確な調査は、きわめて重要な意味を有することになる。

(4) 対応方針と優先性の判断について

情報システム、広報、法務、総務・人事、営業に関する事項について、それぞれ対応方針として決定し、実際に遂行しなければならないのは、本章2.1.1でふれた通りである。

このうち、広報、法務、総務・人事に関する事項については、後述の法・規制的観点からの記載を参考のこと。また、情報システムで検討すべき事項については、後述の技術的側面からの記載を参照のこと。

(5) 業務の遂行の継続性についての判断

具体的には、抑制措置の項で議論されるが、外部からの攻撃によって継続して情報が漏えいしているような場合においては、組織等のシステムをインターネットから遮断することが必要になる場合がある。これは、組織等のシステムが、消費者との関係で重要な位置を占めるといういわゆるネット企業においては、業務の遂行を停止するのと同様な意味を有する。緊急時対応において考慮するのと同様に、何を優先するべきかというきわめて困難な判断になる。これについては、普段から、緊急時に停止しうる時間がどの程度ならば許容できるかというのを想定して、代替手段などについて準備をしておくことが望ましいことになる。

攻撃者のモニターの継続や証拠の収集の必要性の見地から、ネットワークからの切断を遅らせるという戦略をとる可能性が存在したとしても、その遮断が遅れたことによって、

³¹ 危機対応において、重要なのは、3つのC、すなわち、Command, Control, Communicationであるといわれる。

さらなる被害を惹起することがあって、そのような場合における組織等の責任の重さは、否定しうるものではない。経営者は、ネットワークからの切断を遅らせる戦略は、きわめて危険であるという評価があることを念頭におくべきである。

(6) 広報担当としての責務として、

「正確な情報の記録・集中・管理」にもとづいて、広報対応方針を定めることになる。ここで、必要になるのは、情報開示基準と開示方法の選択基準ということになる。ここで問題になるのは、開示の是非・方法・時期を検討することになる。具体的な内容については、2.5 通知・報告・公表等で論じる。

(7) 消費者対応のための準備

情報開示基準と開示方法の選択基準などの基準にもとづいて開示情報マスタープランを作成するのが、最初の準備ということになる。

(8) 判断の迅速性について

責任者における迅速な判断の必要性というのは、強調しすぎることはないものといえる。判断を遅らせるとどんどん被害が大きくなっていくことになる。特に、Winny ネットワークにおける情報漏えいにおいては、土日をはさまないように対応すべきということがある。Winny ネットワークにおいては、土日に活動するコレクター（「付録2の2.4 漏えい情報収集家（コレクター）の存在」参照）の数が1.5倍になるといわれている。漏えい事件が発生した場合、金曜日の夜までに全部決定して判断をすることが強く求められるといえよう。広まっていく確率も、土日をはさむと多くなる。

2.3.3 法規制的観点

(1) 留意点について

初動段階において、法規制等の観点からの留意点としては、対処方法の判断、証拠の保全のための法的対応の問題、緊急記者会見における法的チェックなどがある。

(2) 対処方法の見通し

ここで対処方法の見通しというのは、警察等の助力を得て証拠の保全、確保を行い、原因究明を行う手法を優先するかどうかということである。刑事手続きの利用の有無の判断である。情報漏えい事件において、刑事罰に該当する行為が存在している場合においては、組織等において告訴・告発などを行うことによって、原因究明等において、このような刑事手続きをある意味で、利用することができる。具体的には、情報漏えいに関して不正アクセス禁止法3条違反、不正競争防止法2条1項10号違反、窃盗（刑法235条）、背任（刑法247条）などの法規に違反した行為が存在することが多いものといえよう。

刑事手続きを利用することができれば、証拠収集について強力な手法でもって証拠を収集し、保全することができることになる。また、企業等において、当該不正行為が組織や上司ぐるみではなかったという態度をしめすことにもつながることになる。

もっとも、告訴・告発を警察等におこない受理してもらい警察等に動いてもらうということがなかなか容易ではないことは、法律実務家のよく経験するところである。また、刑

事事件化することによって、企業等のイメージ等が傷つくのではないか、企業等における懲戒制度等によって十分な場合があるのではないかという点などについても考慮が必要になる。警察等において、任意にせよ強制にせよ捜査がなされ、搜索・押収がなされることになった場合には、事前に証拠のありかなどについて検討の上、このような捜査活動によって企業の正当な業務活動への支障をきたさないように配慮することも必要となるであろう。

以上の観点から刑事手続きの利用の是非を検討し、対応チームにおいて、情報の集中管理および開示の手法・時機などについて判断がなされるものと思われる。犯人がわからず、刑事的手法を採用する場合においては、情報を特定のものだけにおいて限定して、本人に対する開示等が、刑事的手法の進展をみながら対応するということもありえよう。なお、警察に対する相談および捜査協力については、「付録5 警察に助力を求める際の留意事項」を参照のこと

(3) 証拠の保全

初動対応の段階において、特定の従業員のコンピュータから情報漏えいがなされたと信じるについて合理的な根拠が発生した場合には、証拠を保全することになる。このような保全について適切な対応をとることが一つの重要な要素ということになる。

このような保全とそれに基づく究明行為は、漏えい情報の範囲を特定することに役立つこととなる。また、原因の究明に役立つことになり、利害関係者への正確な状況説明に資することとなる。場合によっては、関係のない従業員を漏えいの原因としてしまうという過ちを避けるという意味からもこのような証拠保全の重要性はいくら強調してもしすぎることはないものと思われる。

また、特に証拠が従業員の私物である場合が多く、そのような場合には、証拠として変更等がなされて実態の究明に差し支えが生じる可能性がある。また、適切な保全手法をとらなかった場合には、組織等が証拠について改ざん・隠滅等を図ったのではないかという疑いをひき起こすことになり、これらは、保全を実施しない場合のデメリットとすることができる。

この保全は、一般的に、このような特定の従業員の上司もしくは、会社の調査担当の部署のものが対応することになる。詳細な法的な問題点や具体的な法的な問題を避ける手法については「付録4 Winnyをめぐる法律問題の概観」の「3 Winny ネットワークによる情報漏えい対応および防止のための法律問題」を参照のこと。

(4) 緊急記者会見等における法務的チェック

記者会見において、会見者が、不適切な説明をした場合、その内容や表現そのものが訴訟の対象になる可能性が存在するし、また、株主代表訴訟等において、経営者等に不利な証拠となる可能性が存在する。したがって、緊急記者会見を開催する場合に、その会見内容について、弁護士が法的な側面からチェックすることが望ましいものといえよう。

しかしながら、訴訟において不利な表現をさけるという観点からの法的な意見を述べる

だけでは、かえって、誤解や疑惑を招いてしまう、場合によっては、不都合なことを隠蔽しているのではないかと受け取られかねない。また、「法的には、責任はない」などと主張することは、『開き直り』と認識されかねないことに留意すべきである。

これらの観点から、社会的・道義的責任についてどう考えているのかといった点について企業等はどのように認識しているのかというのが、マスメディアの主たる関心であることに留意しなければならない³²。場合によっては、違法性はないにせよ社会的な責任を感じているというような表現を採用することも考慮にいれていいことになる。

2.3.4 技術的観点

(1) 事件の脅威の見極めおよび優先度の位置づけ

情報漏えい事件の契機を発見した場合には、技術的な見地から、その事件の性質を見極め、影響力を分析して、技術的な対応方針を決定する必要がある。どの範囲(ネットワーク、システム、アプリケーション)に対して攻撃等がなされたのか、誰が、その事件を引き起こしたのか、どのようにして(ツールの利用の有無、用いられた脆弱性の内容・性質など)事件が惹起されたのかという点について分析がなされることになる。また、初動調査において、重要情報・極秘情報があるのを早めに察知することが重要である。これらの情報が存在しているかどうかによって、その後の対応においての対応手段の選択に影響を及ぼすのである。

また、原因および漏えい経緯の見極めも重要な意義をもつ。たとえば、廃棄した PC がそのまま利用されて、そこから Winny ネットワークで漏えいしたというケースが存在している。この場合、どの廃棄 PC から漏えいしたのか、また、その廃棄 PC に記録されていた情報には、どのようなものがあつたのかということ特定することが重要になってくる。なお、ネットワークにつながっていた場合には、ウイルススキャンをすべきかどうかについては、見解の相違がある。

これらの初動調査によって、具体的な事件の評価を行うことになるが、疑いがある場合には、最悪を想定して対応すべきだとされている。

(2) 初動調査および評価のために

初動調査および評価は、かぎられた時間と情報から、対応方針を定めるための必要な情報の収集という性格から、きわめて困難な作業ということが出来る。このような作業をすすめるために、以下により有益な情報・準備等が提供されるといわれている³³。

ア ネットワークおよびシステムの状況の把握(プロファイリング)

イ ネットワークの通常の動作についての理解

ウ 集中ログインシステムの採用とログの保存

³² Public Acceptance 法務という表現をもって主張される立場である(東京商工会議所、2005) 67 頁。

³³ (NIST SP800-61) 3-10 による。

エ イベント対照

オ ホストの時刻設定の同期

カ 情報の集積および利用

キ インターネット・サーチエンジンの利用

(3) ネットワークからの切断等についての意見

ネットワークからの遮断が、事業継続可能性に関わる場合もあることについては、前述した。情報漏えい対応において、上記情報をもとに、攻撃の手法および影響力についての確かな分析をなして、その情報資産の保護を図るためにどのような対応が最善かという判断が必要になる。

(4) 個人の私物等に対する証拠の保全

技術的側面として、証拠の保全の要請がある。証拠の保全の必要性については、上記法・規制等からの留意点で説明した通りである。

この場合、本来であれば、このような調査の専門的な技術をもった者に対して、このような調査の手法などについてアドバイスを求めるということが望ましいであろう。もっとも、種々の要請から、そのようなことが困難であれば、情報漏えい対応チームの技術者としては、具体的なデジタル情報が書き換えられやすく・消去されやすいという性質に留意すべきことを実際の保全を対応する上司等に対して十分に説明することになる。なお、調査技術者が、従業員の自宅等を訪問することなどは一般ではなく、これは、具体的な取得の際の手続きの問題に巻き込まれることを避ける観点からである。

実際の取得に際して重要なことは、調査対象者がPCを操作する余裕をあたえずに取得することである。携帯電話を使わせないということもポイントになる。上司が、調査対象者からの「アダルト画像を消去していいか」という問い合わせに、その間待ってやるということで、その間に消去されたりするという可能性も存在するし、また、にせものとか、実際の問題にはならなかった端末を提出してくる者も存在するのである。さらに調査対象者の管理する情報機器について、すべて提出させることが重要になる。

個人所有のPC内のデータの調査にあたっては、専用の書き込み禁止の機能がついた複製装置をもちいてデータの複製をして、その複製したデータに対して調査をする。これは、調査の過程でのデータの改変等を防ぐため必要であり、例えば、調査が当該調査対象者の処分などにつながる場合には、証拠の信用性の確保という観点から重要なことである。電源を入れてしまうとタイムスタンプが変更されてしまい、漏えい行為の時間の確定や漏えい情報の範囲の確定に支障をきたすことになる。

このような手法で取得したコンピュータ内のデータを分析して、例えば、Winny ネットワークに情報が流出している場合には、その一致を見ていくことになる。

2.4 調査

2.4.1 調査の対象

初動対応の際にも、一定の調査がなされることは前述したが、このような初動対応をへ

て、情報漏えい対応チームとして活動して、以下のような事項を究明することになる。この段階での究明された事実が、開示等に関する諸問題、被害の拡大防止・回復等の諸問題、再発防止等に関する諸問題、事故対応後の諸問題の際の対応の基礎となる。

(1) いつ漏えいしたのか

「いつ(から)漏えいしたのか、いつ漏えいの事実を確認できたのか」

いつ漏えいしたのかという事実は、被害の範囲を特定するための重要な要素になる。それとともに、その漏えいの事実を確認したのがいつかということは、その後、組織等の対応が迅速にできたのか、逆に、組織等において放置・隠蔽がなかったのかという社会的な評価に関連することになる。

(2) 何が

「どのような情報が漏えいしたのか、それは、どのような措置をほどこされていたのか」

表 3.2 情報区分

情報区分(大)	情報区分(中)	情報区分(小)
個人情報 (お客様の個人情報、取引先企業社員の個人情報、自社の個人情報の区別が必要)	一般的な個人情報	氏名、性別、生年月日、住所、メールアドレス(自宅 or 会社)・電話番号(自宅 or 会社) 職業、社員番号、会員番号等
	センシティブな個人情報	学歴、職歴、成績(学業、会社内評定) 結婚/離婚、賞罰、身体特徴(身長、体重、血液型等) 年収、趣味、クレジットカード情報(カード番号と有効期限) 銀行口座番号等
	特にセンシティブな個人情報	本籍、国籍、犯罪歴、健康状態、病歴、手術歴、DNA 情報、宗教、思想、与信ブラックリスト等
法人情報 (お客様の企業情報、取引先の企業情報、自社の企業情報の区別が必要)	一般的な法人情報	企業名、企業内組織名、企業内電話番号、企業内組織構成図、企業内業務内容(一般的)等
	センシティブな法人情報	<ul style="list-style-type: none"> ・企業システム情報(グローバル IP アドレス、ネットワーク構成図、システム構成図、使用機器の仕様等) ・会計情報(取引内容、発表前決算情報等) ・知的財産情報(製品仕様、価格等) ・公共性の高い情報

漏えいした情報がなにかという点は、まさに本人や組織に生じた損害の根本的なものを基礎づけることになる。不正使用により経済的被害に直結するような情報(クレジットカード番号等)であったとすれば、二次被害の危険性はきわめて高いということがいえるであろう。また、情報が流通する範囲・程度などにも影響することになる。

漏えいした情報には、どのような保護策がなされていたのかを確認する
これを確認することにより、各利害関係者に対してどの程度リスクがあるのかを示すことができるし、どのような対策を採っていたのか説明することができる。

ア 紛失・盗難の場合

(ア) PC やサーバの盗難や紛失の場合

- ・ PC/サーバの OS へのログインパスワードは設定されていたのか
- ・ ハードディスク全体の暗号化は実施していたのか、その暗号化のアルゴリズムは何か、パスワードの強度は
- ・ BIOS のパスワードは掛けていたのか
- ・ ファイル毎の暗号化はかけていたのか、その暗号化のアルゴリズムは何か、パスワードの強度は

(イ) 外部媒体 (USB メモリ) の紛失、盗難の場合

- ・ USB 使用者の認証機能付きか (生体認証または ID/パスワード)
- ・ USB のメモリに暗号化は実施していたのかその暗号化のアルゴリズムは何か、パスワードの強度は
- ・ メモリ内の各ファイル毎の暗号化はかけていたのか、その暗号化のアルゴリズムは何か、パスワードの強度は

イ 誤送信・Web での誤公開等の場合

(ア) メール誤送信、Web での誤公開の場合

- ・ ファイルに、暗号化を実施していたのか、その暗号化のアルゴリズムは何か、パスワードの強度は

ウ 内部犯行の場合

機密性が高いファイルの管理は、どのように行なっていたのか、

(ア) 入退室管理

- ・ 個人認証を行なっていたか、ID 管理 (登録と削除) は適切だったか、映像記録は取っていたか、入退室記録のログを取得しチェックを行なっていたか

(イ) ファイルへのアクセス権管理

- ・ 個人認証を行なっていたか、業務に応じたアクセスコントロール (ファイルの更新、閲覧、印刷、書出し別) を行なっていたか、ファイルの操作ログの取得を行なっていたか
- ・ ファイルが格納されているサーバの特権 ID (root、admin) 権限の共用を禁止していたか

(ウ) ファイルの持ち出し管理

- ・ インターネットを介したメールや HTTP、FTP などでの外部へのファイル送信を規制していたか、これらの操作ログを取得していたか
- ・ 私物 PC の持込や組織内 LAN への接続規制を行なっていたか、組織貸与の PC の持ち出し管理を規制していたか、いずれもルールだけではなく技術的な規制を行なっていたか

- ・ PC やサーバから、USB や CD/DVD 等の外部記憶媒体への書き出し制限や外部記憶媒体の持ち込み、持ち出し制限を行っていたか、いずれもルールだけではなく技術的な規制を行っていたか

エ Winny や Share 等の P2P ファイル交換ソフトを介した情報漏えいの場合

- (ア) PC やサーバへのウイルス検知ソフトウェアは導入していたのか、ウイルスパターンファイルの更新は常に最新版に保つ仕組みを導入していたのか
- (イ) Winny や Share 等の P2P ファイル交換ソフトの導入の扱いについて、組織内にてルール上禁止していたのか、技術的に当該ソフトウェアを PC へ組み入れられない、起動できない等の措置を実施していたのか
- (ウ) 漏えいしたファイルに、暗号化を実施していたのか、その暗号化のアルゴリズムは何か、パスワードの強度は

オ 不正プログラムの場合

- (ア) PC やサーバへのウイルス検知ソフトウェアは導入していたのか、ウイルスパターンファイルの更新は常に最新版に保つ仕組みを導入していたのか
- (イ) 危険な Web へのアクセスコントロール(フィルタリング)を実施していたのか
- (ウ) 電子メールの扱いにおいて、exe ファイルや怪しい受信メールの扱いについて、組織内にて規定・規制していたのか

カ 不正アクセスの場合

外部からの無権限者によるアクセスによる情報搾取であるが、情報システムの運用をどのように行っていたのか

- (ア) ネットワーク機器による外部からの不正アクセス防止対策
 - ・ ファイアウォールやIDS、IPS等の設置によって、外部からの不正なアクセスを遮断、防御、検知する仕組みを導入していたか
 - ・ これらの機器のソフトウェアバージョンアップや運用状況のチェック、監視を定期的に行っていたか
- (イ) PC やサーバの不正アクセス防止策
 - ・ サーバの要塞化を行っていたか不要サービスの停止、OS やアプリケーションへのセキュリティパッチ適用等
 - ・ サーバへの不正アクセスが検知できる仕組みを導入していたか
 - ・ ID / パスワードの定期的な強制変更、パスワードの強度(桁数や利用文字の複雑化) 特権ID (root や admin) 権限のIDの変更を行っていたか(デフォルトのroot や admin を使っていないか)

漏えいした情報による被害の重要度の特定

2. 3の初動対応にて把握した情報を元に、被害の重要度の特定を行なう。
以下の表のように、漏えい情報項目毎に整理し、想定されるリスクをまとめる。

表 3.3 漏えい情報一覧とりまとめ例

		顧客情報の場合の例	想定されるリスク	重大度
個人情報	機微な個人情報	クレジットカード番号、 有効期限：50件	電子商取引上でなりすまし により不正利用され、顧客に 実害発生	重大
	一般的な個人情報	氏名：150件 メールアドレス：150件 住所：150件	迷惑メール、ダル外郵便等を 送付される	大
法人情報	センシティブな 法人情報	企業名：1件 ネットワーク構成図：1件 IPアドレス(グローバル): 30件	該当 IP アドレスへ不正アク セスや DoS 攻撃をされる	大

注) 網掛け部分は、個人情報保護法対象

法人情報の項目でも、漏えい元の業種によっては法的な対象となる情報項目がある(例：電気通信事業法、郵便法：通信の秘密等)

(3) どれだけ漏えいしたのか

「(2)の各々の項目毎の件数がどれだけであるのか」

これによって、漏えいした情報が個人情報であれば、被害を受けた本人がどれだけの範囲になるのか、が特定されることになる。被害者の数は、被害者への連絡のとり方の問題やマスメディアでの広報の要否などにつながる要素となる。

(4) どこから漏えいしたのか

「漏えいした情報は、どこから漏えいしたのか」

具体的な漏えいに関与した場所が、組織内であるのか組織外であるのかという問題である。また、それに関与した人間がいるとして、その人は、組織の誰であるのか、組織外の誰(委託先、第三者等)であるのかという問題である。

(5) どこに・どのように(漏えい状況)漏えいしたのか

これは、漏えいした情報が、どこに漏えいしているのか、今も漏えいし続けているのか、漏えいを止めることができるのかという問題である。

漏えい情報が、特定の犯罪者の中で情報として保持されているのか、物理的な媒体として出回っているのか、掲示板などに書き込まれていないか、Winny などの匿名 P 2 P ネットワークに流出していないかどうか、また、さらに振り込め詐欺などに悪用されていないかどうかなどの観点から検討されることになる。これらの要素は、そもそも具体的な調査の対象・手法などに関連することになる。また、被害者への連絡のとり方の問題やマスメディアでの広報の要否、また、対策方法の準備などにつながる要素となる。

発見された情報が、紙、媒体（PC、可搬型記憶媒体等）などの媒体のままであるのか、インターネット（Winny 等の P2P ファイル交換ソフト）、インターネット（不正アクセス）、Web 掲示板、ブログ（風評）、メール、FTP 等）、マスメディア（雑誌、TV、ラジオ等）などのネットワークに流出しているのかという点において、上記要素に強い影響を与えることになる。

ア 発見媒体が PC や外部媒体、紙の場合

（ア）組織内で気付いた場合

行方がわからなくなった PC や外部媒体は、それらの所持者及び管理責任者に対して「紛失したのか、盗難にあったのか」「何故、紛失・盗難といえるのか」といった事項を確認することが必要である。いずれも内部犯罪か外部犯罪の可能性がないか見極めが必要となる。

（イ）外部の第三者からの申告の場合

行方がわからなくなった PC や外部媒体における情報が漏えいしているという連絡が、マスメディアから提供された場合や、見ず知らずの第三者から提供される場合がある。マスメディアからの場合、どこから情報を手に入れたのか、返還可能かという点について確認することになる。一方、見ず知らずの第三者から提供された場合、どこから情報を手に入れたのか、情報が返還可能かを確認することになる。なお、PC 等の返還を求める際に、拾得物に返還に対する謝礼として一般常識（菓子折り程度）を超える金品を要求される場合は、善意の第三者を装っている可能性があるため、弁護士や警察に相談することを検討する。

（ウ）犯罪の可能性について

いずれの場合においても内部犯罪か外部犯罪の可能性がないか見極めが必要となる。

イ Winny 等ファイル交換ソフト上に情報漏えいしている場合

漏えいしている情報から、情報を漏えいさせた人物と会社 PC か自宅 PC かの絞込みを行い、当該人物及び当該人物の上長（又はシステム管理者）に、下記の事項を確認し、過失なのか第三者による故意なのか判別する。

（ア）会社 PC の場合

会社 PC への Winny 等のソフトウェアのインストールの有無の確認、Winny 等のソフトウェアの起動履歴の確認、ウイルス感染履歴の有無の確認、ウイルス対策ソフ

トウェアのインストール有無とパターンファイルのバージョンの確認などをおこなう必要がある。そのために、当該 PC を隔離し、PC 内のデータを保全し、漏えいした情報と PC 内データの比較を行なうことになる。

(イ) 自宅 PC の場合

自宅 PC での Winny 等のソフトウェアのインストールの有無の確認、Winny 等のソフトウェアの起動履歴の確認、ウイルス感染履歴の有無の確認、ウイルス対策ソフトウェアのインストール有無とパターンファイルのバージョンの確認をおこなうことになる。そのために、当該 PC を隔離し、PC 内のデータを保全し、漏えいした情報と PC 内データの比較を行なうことになる。なお、その際の法的な問題については、付録を参照のこと。

ウ ネットワーク経由で被害にあった場合

不正アクセス行為などにより、ネットワーク経由で情報が流出してしまった場合である。この場合、経路の確認、流出原因の特定、外部からの不正アクセスの痕跡がないか、不正アクセスされる脆弱性がないか調査することになる。

(6) 何故漏えいしたのか

組織等において過失が存在するのか、それともないのか、もしくは、犯罪による被害の場合、組織等の内部犯行なのかどうかという見極めが必要である。これは、いうまでもなく企業等において法的責任や社会的な非難の程度に関連することになる。

2.4.2 マネジメント的観点

復旧後の調査と異なり、この段階における調査は、情報漏えい対応の活動を行う基礎となる事実を明らかにすることとなる。上述のように証拠の獲得とその調査をはじめとして、種々の方法によって事実の究明がはかられることになる。情報漏えい対応本部において、収集される事実をもとに、人間関係をも含めて判明した事実をもとに、上記の個々の事実について判断していくことになる。

なお、事実究明の方向性としては、発見の経緯となった情報から、情報リストの所在地までたどり着く「川下からの調査」と流出原因の早期発見から、究明を図ろうとする「川上からの調査」の方向性があるとされる³⁴。

2.4.3 法規制的観点

(1) 証拠の収集と取扱の権限

具体的な調査の根拠をおこなう場合には、企業秩序維持からする調査権があることが前提となる。使用者は、企業の存立・運営に不可欠な企業秩序を鼎立し維持する当然の権限を有し、労働者は労働契約の締結によって当然にこの企業秩序の遵守義務を負うものと考えられ、その関係で、このような調査権に対して調査を受任すべき法的な義務があるもの

³⁴ (大塚、2005) NBL808 号、45 頁以下。

といえよう。もっとも、このような調査権と受任義務といったとしても、具体的な場合には、従業員のプライバシーと企業秩序維持の必要性との衝突が発生することになる。このような問題点に配慮して、事前に企業秩序維持からする調査権についての一般的な承諾をえているような形で就業規則等で定めておくことが望ましいものといえるが、実際に問題がおきたあとは、微妙な価値判断を必要とされることになる。具体的な問題点および対応方法については、「付録4 Winnyをめぐる法律問題の概観」で詳細に論じているとおりである。

(2) 証拠の収集の作戦の立案

また、後述のように技術的調査を行う場合に、どの範囲において事実調査をして、どのようにして真実を究明していくべきかが問題になる。たとえば、真実の究明を妨げる場合として、経営層の一部と情報システム部門の担当者が協同して不正行為を企んでいる場合を例にとってみる場合、通常の調査のみでは、真実の究明が困難になる可能性がある。このような可能性をも念頭に置いて、漏えい調査を行わなければならないことになるのである。

(3) 証拠の取扱いについての法的な立場

企業が証拠を収集したあと、それを裁判所等に提出するまでにどのように取り扱うかという点についてのノウハウについて指導をなしておくことは有意義であろう。バッグに証拠の名称・取得日時・担当者を記載したタグをつけて、紛失等のないように保管すること、また、特に企業内において保管する際には、セキュリティ的な安全措置を講じることなどが推奨されるべきことになる。

2.4.4 技術的観点

(1) 証拠の収集と取り扱い

ア 調査の目的と調査の記録

事件についての原因・影響範囲を明らかにして対応するために証拠を収集するのが第一の目的ということになる。そして、そのためには、漏えいに関する事実についての記録(ログブック等作成)をするのが重要である。システムイベント、電話の会議、ファイルにおける変化などが記録され、漏えいの事実の発見から、解決に向かうまでに採用された技術的なステップが、時刻とともに文書化されるのが望ましい。

イ 証拠の取扱いの記録

また、上記のような対応のための基礎的事実の収集という目的の一方で、後々の法的等な対応の根拠にするためという目的も存在する。したがって、取得・保管・分析・提出の一連の過程において、証拠の信用性に影響をあたえるような事柄をできるだけ避けるような手順で取り扱うのが望ましいことになる。

このような見地から、証拠に関する取扱は、すべて記録されるのが望ましいことになる。そして、記録されるべき情報としては、

特定のための情報(取得場所、シリアルナンバー、モデルナンバー、ホストネーム、

MACアドレス、コンピュータのIPアドレス)

調査に関与した者の氏名、連絡先

証拠の取扱をした時間

証拠の保管場所

などがある³⁵。

ウ 記録媒体の複製の取得

漏えいの原因を探る調査において、事故が発生したと思われるPCを差し押さえることに成功したとする。このとき、当該PCに付属のハードディスク等の記録媒体の完全性は保持したまま、記録されたデータを調べる必要性が出てくる。仮に、当該PCを起動した場合には、記録媒体への書き込み等が生じることで、事故発生当時の記録を毀損してしまう恐れがある。

以上のことから、当該PCに付属のハードディスク等を取り外した上で、複製をとることが望ましい。複製を調査対象とすることで、原本の完全性を崩すことなく、データやアプリケーションを操作することが可能となる。ただし、複製をとるための作業は、改ざん等の事実のないことを証明するために立会人の下で行われることが理想であり、原本と複製とのハッシュ値の一致を確認したことの証明として署名を記入してもらおうとよい。加えて、それらの様子を撮影し、記録することはより作業の信憑性を高めると考えられる。

一方、複製の手段として「ソフトコピー」と「物理コピー」が存在する。これら手段は前者がファイルのみをバックアップするものであり、後者は原本の完全な複写となる。後者を使用した場合、当該複製は完全な複写であるため、ファイルのみならず消去されたデータ、メモリのスワップ先といったものを含むことになる。ファイルのみならずこれらを調査することは、当該PCにおいてどのような操作が事故発生時に行われたのかを知るための、重要な手がかりとなる可能性があるため、複製をとることが可能な場合は、物理コピーを行うことが望ましい。

エ 複製の調査

複製の調査を行うためには、専用のソフトウェアが必要となる場合がある。これらソフトウェアは「ユーティリティ」や「ツール」といった呼称である場合もあり、特定の処理を自動化してくれる。一方、これらソフトウェアは多数存在しており、特定の処理に限られるため、包括的に調査を実施するには複数のツールを場合に応じて使い分けていかななくてはならない。

このような煩雑さを解消できる複製の調査に特化した商用ソフトウェアが存在しており、情報セキュリティ事業者への聴取によると、そうした商用のソフトウェアを使用することで調査時間の短縮を図っているという。

³⁵ (NIST SP800-61) J3-19 頁。

オ 調査における問題等

調査において問題となるのは、暗号化によって複製からはデータが読み取れない場合である。この場合、完全性が損なわれることを了解のうえで調査対象 PC にソフトウェアを新たにインストールし、それを使用して調査を実施することが選択肢のひとつにあげられる。

さらに、近年特定の技術手段を駆使することで、不正アクセスの痕跡を隠蔽する手口が考案されている³⁶。このような手段が、悪意を持った者によって意図的な情報漏えいが行われた際に使用された場合、その特定をより困難にさせることが想定される。また、ここ数年での技術革新とそれに伴う記録媒体の変化は、著しいものがある。90年代中盤において、それなりに利用されたが、現在では、一般に使用されていないZIPドライブのなかから復元することなどもあり、そのような記録媒体からの回復なども必要性として存在しているのである。

(2) 攻撃者の特定

情報漏えい事故が、外部からの攻撃者によるものであって、それに対応している最中であっても、攻撃が継続する場合には、システム管理者は、攻撃者がいかなるものか特定をしたいと考えるものである。しかしながら、攻撃者を起訴したいと考えていたとしても、まずは、被害の抑制・拡大防止・復旧に集中すべきである。攻撃者の特定というのは、時間もかかるし、結果も不確かなものであり、利害関係者の被害の最小化というもっとも重要な目標に集中すべきということになる。

技術的には、攻撃者の特定に資するものとしては、攻撃者のIPアドレスの評価、攻撃者システムのスキャン、サーチエンジンによる分析、インシデント・データベースによる分析、攻撃者の通信チャンネルのモニタリングなどの手法がある³⁷。

2.5 通知・報告・公表等

2.5.1 通知・報告・公表等の意義

情報漏えいの可能性を基礎づける事実が認識された場合、原則として下記に示す内容を本人に通知し、各利害関係者に開示し、また、監督官庁へ報告を行うことになる（以下、通知・報告・公表等を合わせて開示と呼ぶことがある）。

これは、特に漏えい情報の主体である本人については、情報漏えいの可能性がある事実を伝達して、事実関係や謝意をつたえるとともに、本人に対して注意喚起をすることによって二次被害などにあわないようにするというを理由とするものである。また、類似事案の発生を回避するというのも目的の一つといえるであろう。

³⁶ 塩月誠人「アンチ・フォレンジック」http://www.st.rim.or.jp/~shio/sa/sa2005_shio.pdf

³⁷ (NIST SP800-61) J3-22 による。

(1) 通知・報告・公表等する相手方について

組織において、情報漏えいが発生した際の主な利害関係者は下記が想定される。

ア 顧客（個人）・顧客（企業）

組織等が顧客の個人情報を預かっていたり、また、取引先の企業情報を預かっていたりした場合に、そのような情報が漏えいした場合に、個人情報の主体や企業情報の主体に対しての通知をすることが必要である。これは、そのような情報の主体に関して、主として二次的被害防止の観点および謝罪の意思を伝えるという観点から通知をすることになる。

イ マスメディア

これは、大多数の被害を被った本人が存在する場合に、潜在的被害者に対する個別の通知に替えるという性格を有するとともに、情報漏えい事件という社会的に注目をあびる事件に関与したことに關して、組織等としての社会への謝罪・認識・対応策を公表することにより、社会的責任を果たすという性格を有することになる。

ウ 監督官庁

後述するような個人情報保護法にもとづく監督官庁の指導の基盤を形成するものとして、また、その他の法的な根拠に基づいて監督官庁に対する報告等をなさなければならない場合がある。

エ 株主および証券取引所関係

株式会社において情報漏えいが発生した場合において会社の所有者である株主に対しては、適時にそのような事実関係が開示されなくてはならないことはいままでもない。また、証券取引所は、そのような開示のルールを定めており、そのようなルールにしたがって、開示することが必要になる。

オ 従業員

情報漏えい事件対応において、当該漏えいが発生したという事実およびどのような事実が漏えいしたのかというのは、初動対応の期間中は、当該組織の従業員等に対しても、秘密にされるのが一般である。その場合、時機をみて、従業員に対して、漏えい的事实を明らかにすることにより、従業員のセキュリティ意識や社会的責任の醸成を図るものである。

カ 取引先

具体的に、取引先等から預かっている情報を漏えいさせてしまった場合は、もちろんのこと、取引先としては、具体的な仕事を依頼する会社において、情報漏えい対応に十分な努力を図っているかというのを見極めるのは、当然の責務である。取引先が、十分な調査もしないで、その会社と取引を継続して、再発をしてしまったという場合には、その取引先のみずからの問題となってしまうのである。

したがって、漏えい事故に関与した会社としては、原因を究明し、漏えい事故についての説明責任を果たすとともに、その漏えいについて過失があったような場合には、

特に再発防止策を十分に実行して、取引の継続等を依頼することになる。

キ IPA (情報処理推進機構)・JPCERT コーディネーションセンター・ISAC

情報漏えいが、特定の攻撃方法等によって発生した場合、そのようなセキュリティインシデント対応調整機関などの機能をもつ上記機構に対して、連絡することが考慮されるべきである。

(ア) 独立行政法人情報処理推進機構 (略称 IPA、以下 IPA という)

IPA は、(1) オープンソースソフトウェアの普及促進・基盤整備・情報の集約と発信、(2) 高品質なソフトウェア開発の効率化支援をするソフトウェアエンジニアリング手法の確立、(3) 安心できる情報化社会の実現を目指した情報セキュリティ対策などの目的のために設立された独立行政法人である。

情報漏えい事件に関連した制度として、情報漏えい事件が、コンピュータウイルスによって発生した場合、不正アクセスによって発生した場合、脆弱性を利用された攻撃によって発生した場合には、IPA セキュリティセンターに対して届出をすることが推奨される。

(イ) JPCERT/CC

JPCERT コーディネーションセンターは、国内外からの報告に基づくコンピュータセキュリティインシデント対応の支援活動を行っているほか、ソフトウェアやハードウェアに関する脆弱性情報を国内及び海外ベンダーに展開、対策情報の作成や公開日の調整を行う脆弱性ハンドリング活動を行っており、こうした活動から得られる情報を分析し、国内外において適切な情報発信を行うことで、社会全体のセキュリティ上のリスクを低減させることを目的とする非営利かつ中立的な組織である。

また、コンピュータセキュリティインシデントへの対応体制である CSIRT (Computer Security Incident Response Team) の構築と運用の支援に関する活動も行っている。国内に存在する CSIRT 間での情報共有や、緊密な連携体制の構築を目的とした「日本シーサート 協議会」の事務局をはじめ、世界各国に存在する海外の CSIRT との連携活動も行っており、アジア太平洋地域における CSIRT 連携の枠組みである APCERT (Asia Pacific Computer Emergency Response Team) の事務局も務めている。

情報漏えいインシデントについては、インシデント発生の原因となった技術的な事象 (システムへの侵入やウイルスの感染など) に関する観点から、報告の受付、対応の支援活動を行っている。

(ウ) ISAC

一般的に、情報システムに対する各種インシデントは、業界毎に一定の特徴を持ちやすい傾向にあることから、実際に発生したインシデントに関する情報を業界内で分析・共有することが有意義である。

ISAC (Information Sharing and Analysis Center) とは、そのような認識のもと

づいて構成された業界における情報交換および分析センターである。このような考え方から、設立されているものとして Telecom - ISAC Japan³⁸があるし、内閣官房情報セキュリティセンター(NISC)による第1次情報セキュリティ基本計画においては、具体的なものとして自治体 ISAC や各重要インフラ分野内に「情報共有・分析機能」(CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response)を構築することが述べられている³⁹。

このような情報共有のルートに対して情報を連絡することも同一の業界に共通する情報共有の観点から必要になってくる。

ク その他

また、事件の態様などによって異なるが、ISP(インターネット・サービス・プロバイダ)、攻撃者のアドレス、ソフトウェアベンダ、攻撃の影響を受けている他のサイトの管理者などに対する連絡が必要となることもありうる。

(2) 通知・報告・公表等される内容について

開示される内容については、下記の項目が基本となる。

ただし、顧客向けやマスメディア向けリリース(配布資料)、監督官庁への報告など提出・開示する内容の深さについては取捨選択することはあるが、基本的なデータや組織としての方針はぶれがなく同じであることが肝要である。

ア 情報漏えいを発生させたことに対する謝罪

これは、個人情報漏えい事件などにおいて被害が発生した場合、重要インフラに関する情報漏えいの場合などにおいて、そのことに対する社会的責任についての認識と組織等としての謝罪の意向を伝えるというものである。普段から、情報漏えい対応について基本と原則をどのように考えているかということを考えていれば、おのずから謝罪の対象は明らかになるものといえよう。謝罪の対象を明らかにすることは、基本であるということとができるが、その一方で、不明確になりがちなことでもある。よく、被害者がいるのに、元請けに対して謝罪しているかのような表現がなされることがあり、その点については、留意が必要であろう。

イ 情報漏えいの事実説明

事実の概要から始まって詳細な内容についての記述がされる。いわゆる5W1Hの要素が網羅されることになる。

何の情報か、いつ、どこで、どうやって、どれだけ流出したのかを事実に基づいて説明することが重要である。この時点で、判明していない事実は、「調査中」とし、事実だけを伝えるようにすべきである。誤解を生む想定事項をださないようにすることが重要である。また、組織が知りえた経緯についても、時系列で示すことになる。

³⁸ <https://www.telecom-isac.jp/>

³⁹ http://www.nisc.go.jp/active/kihon/ts/bpc01_f.html

ウ 危険性の有無に関する情報

当該情報漏えいによって、想定される危険性があるのかないのかを判断するために必要な事実に関する情報を提供する。例えば、「PCを盗難、紛失したが、政府推奨方式の暗号化を行っているため、復号は困難で危険性は低い」とか、「電子モールの顧客のIDとパスワードが流出したため、成りすましによる発注が発生する可能性がある」等である。根拠なく都合のよい主観的な判断結果を提示することは危険であり避けるべきである。被害者や報道機関が危険性の有無を判断するために必要な事実に関する情報を提供すべきである。

エ 情報漏えい発生の原因

何故、情報が流出したのかという原因に対する事実である。この時点で原因が判明していない場合は、調査中とするべきである。

オ 現状での対策状況

初動対応として、何をしたのかを示すことが重要である。例えば、流出原因となったネットワークサービスを停止させ、流出を停止させた上で詳細調査中、並行して顧客へ情報漏えいの事実を通知し、二次被害発生の防止に努めている等の内容となる。

カ 組織としての対応

主に次の観点について盛り込んだ内容を示すことになる。

組織としては、被害の拡大を抑えること、原因究明を迅速に進めること、原因が究明された段階で、再発防止策を策定・実施すること、迷惑を掛けた方への謝罪と事実説明を行うこと、法（個人情報保護法等）に従って適正に対処することについて対応することになるのであり、これらの内容を具体的に開示することになる。

キ 本件に関する問合せ先

被害者に対する対応指針を明確にしておくことが必要である。外部からの問合せ先は、利害関係者の利便性と組織としての対応の一元化を図るため明示しておくことが必要になる。

(3) 開示をスムーズにおこなうために

開示をスムーズにおこなうためには、「情報開示用のひな形 開示情報マスタープラン」を準備することが有効である。この開示情報マスタープランというのは、上記イに記載された内容をまとめたものである。

これをもとにプレスリリースが作成され、広報担当者は、個別取材、記者会見などに応じているまた、社告・テレビCMなどにも利用・応用され、その結果、新聞記事、テレビ報道などにもこの内容が反映されることになる。

また、その一方で、このマスタープランをもとに、自社ホームページ説明文書、被害者向けお詫び文書、記者会見資料、ポジションペーパー、社内説明文書・得意先・取引先説明文書、証券取引所適時開示の書類、監督官庁宛の説明文書などに利用される。特に、ポジションペーパーは、ある問題について、対立や意見相違が生じた場合に、この経緯や

事実関係、双方の主張などを時系列的かつ客観的に整理した文書をいい、客観的な事実を説明し、第三者に公平な判断を仰ぐことを可能にするものとしてきわめて重要なものである⁴⁰。

このような作業をすることによって、開示情報のぶれを防止し、作業の効率化をはかることができる。また、関係者が個人の憶測などを差し込む余地がなくなってくるのである。

(4) 情報漏えいに関する開示の判断ポイントについて

組織外の利害関係者及び監督官庁への開示については、組織内にて判断を要する事項である。そこで、検討委員会において、開示の要否等に影響を与えるであろう事項について基本的な考え方について以下に整理する。

もっとも、下記の判断基準については、各組織における状況に応じて変化するものであり、参考情報として扱い、各々の組織内にて判断基準を制定することが望ましいものといえる。

ア 本人に対する通知について

個人情報であれ、法人情報であれ、関連する情報が漏えいした場合、後述の例外状況がないかぎり、その本人に対して、通知をすることが要求される。被害者に対する開示・説明については、その態様・順番などについても考慮しなければならない。これらを考える際には、被害者の数およびその連絡先についてどれだけ把握しているかということも影響を及ぼすものである。

大雑把な観点から整理するとき、本人への通知は、二次被害のおそれなくなった段階で、必須なものと認識されることが多いものと思われる。

イ 監督官庁に対する報告

個人情報であれば、個人情報保護法との関連で監督官庁に対して報告を行うことになる。詳細については、後述する。また、それ以外にも、各組織等においてそれぞれ規制があり、規制によって報告等が求められている場合があるので、それにも留意することが必要である。

ウ マスメディアを通じての開示

一般にマスメディアへの開示といっても具体的な手法として、ホームページでの資料発表、プレスリリース（記者クラブへの資料投げ込み）、電話取材等に対する対応、記者会見がある。

通常マスメディアへの開示は、漏えいした情報項目は必要だが、二次被害のおそれがあるため情報の内容そのものまでは公表する必要はない。

それ以外へのマスメディアを通じての開示については、Webでの発表、プレスリリースによる公表ということにしておいて、そのあと、これらの手段による公表にたいする社会の反応などをみながら、記者会見が合理的かどうかという判断をしていくもの

⁴⁰（東京商工会議所，2005）53頁。（石川，2004）84頁

と思われる。

(5) 対応の実践について

開示に対する具体的な対応の実際上のものとしては、具体的な開示のスケジュールの立案、説明文書およびQ & Aの準備、本人への通知の実行、プレスリリース準備、記者会見準備、社内会見準備などがある。

ア 具体的なスケジュール

具体的な開示のスケジュールに関して検討すべきこととしては、基本的には、被害者全員に対して、原則として、情報漏えいの可能性が存在したことについて早急に連絡をとるべきことになる。ただし、その際情報を開示することがさらなる二次被害を発生させないことを確認したうえ開示しなければならない。原則的な順番としては、たとえば、マスコミリリース前に被害者に説明・謝罪を済ませることを考慮するというものを検討すべきである。被害者への連絡より、マスメディアへの公表が先な場合において被害者の心情に複雑なものがあることは想像に難くない。一方、マスメディアに対しての公表は、被害者が、多数にわたり、すべての被害者に対して連絡をとることに困難性を感じる場合であるとか、時間的にロスが発生しては損害の回復や回避が困難になる場合などに行われることになる。現実の事件においては、名簿屋に売られる、いやがらせや振り込み詐欺の電話がかかってくる、流出した裸の写真が第三者により販売されるなどの2次被害が発生しているものもあり、できるかぎり、それらの損害を発生させないような対応をすべきということになる。

また、この段階で、利害関係者の意向・利害にもとづいて具体的な開示のスケジュール等が決定されることになる。

イ 説明文書およびQ & Aの準備

上記マスタープランをもとに具体的な対応のために組織等の基本的な立場を明らかにするポジションペーパーを作成することがある。

そして、マスメディアからの取材などに対応するためにQ & Aを準備する。

このQ & Aにおいては、聞かれると困るようなことからきちんと準備する必要がある。準備しなくても答えられるようなのは、そもそも、前記のマスタープランにおいて準備されている事項である。むしろ、記者などが事件のいわゆる「筋」からみたときに質問したくなるような質問事項を予測して、作成し、回答を検討しておくことが必要である。また、作成された質疑応答は、事実経緯に関する質問、原因に関する質問、これまでに実施した対応、今後の対応、被害者対応、責任の所在、再発防止策、会社経営への営業などの個々のカテゴリーごとにわけて整理しておくことにより後にも効率的に利用することができよう。

ウ 本人に対する通知の実務

個人情報であれ、法人情報であれ、関連する情報が漏えいした場合、後述2.5.3の例外状況がないかぎり、その本人に対して、通知をすることが要求される。

この通知は、二次被害防止・類似事案防止および漏えいに関与した組織等の謝罪の意図の表明のためのものになる。実際には、自宅宛の電話、自宅住所宛の文書による通知、電子メールによる連絡などの手法がある。緊急性を要する場合などは、自宅への電話により連絡するということが優先されることもあるであろう。一方、本人に対する通知のタイミングのズレの問題が発生する場合には、文書による連絡が望ましいことになる。電子メールによる連絡も可能（もっとも、情報の登録が古いものであれば電子メールアドレスも変更されている可能性が高いことなどもある）であろう。

なお、電話連絡の際の準備等については、後述 2.5.2. 参照。

エ マスメディア対応の実務

(ア) メディアによる開示の必要性についての検討

被害者たる本人の数が多数ではないときに個別の連絡をもって、通知することができ、漏えいの形態において、類似事案の防止という要請がないような場合においては、マスメディアへの開示という形態をとる必要はないであろうと考えることができる。また、Winny ネットワークにおける情報流出においては、そのような事実の報道がかえって、情報の流通を促進するという事実が指摘されている。このような事実も、上記開示等の原則に対する例外として認識しうるものと考えられる。

(イ) 取材対応

取材対応については、特に中小企業の場合、元請けである大企業が記者会見などを行って、それに関係している中小企業に対して裏付けの観点から取材が行われるということが比較的多いものと思われる。この場合、広報担当者が原則として対応すること（できれば、対応する人数は複数望ましい）、電話の取材は避け面談対応とすること、取材の申し入れがあったときに趣旨・質問事項を可能な限り確認すること、開示可能な情報はどこまでか、範囲を明確にしておくことなどの留意事項がある。

この場合において、開示マスタープランに従って説明できるようにしておくべきである。そのような準備をしていれば、時系列できちんと説明できるようになり、また、原因はどうか、という質問にきちんと誘因・素因という観点も踏まえて、説明できるようにあらかじめ準備しておくことが必要である。

(ウ) 記者会見準備

記者会見対応としては、1) 入場時においては、会場への入場や退場の場所などに留意し、記者が、個別に代表者等に対して取材を行う、いわゆる「ぶらさがり」をふせぐ必要がある。また、会見開始直前に資料を配付するようすべきであるといわれている。2) 冒頭会見においては、被害者・取引先等の利害関係者への謝罪が必要であり、また、最後の一礼を忘れないこと 3) 説明においては、説明文書にもとづき説明を実施し、組織等における基本的な立場を離れた説明をなさないこととされる。

また、記者会見における記者とのQ&Aについては、記者会見については、Q&Aから開始されるわけではなく、事前の説明において、上述の開示マスタープランにおいてきちんと記載されている内容を説明することが必要であり、そのことによって、記者が必要とする情報を十分伝えることができるので、質問自体の必要性が低くなるものと思われる。

2.5.2 マネジメント的観点

開示そのものについて検討した上述の事項は、まさにマネジメント的観点から留意すべき事項といえることができる。

まず本人に対して、電話による漏えいの事実の通知をおこなう場合⁴¹には、その通知について連絡のひな型および想定の間答を作成する。そして、作成した作成者がオペレーター（電話をかける担当者）に対して教育をおこなうことが効果的である。

また、このような開示をきっかけにして、本人からの問い合わせが殺到する場合も多い。このような場合にそなえて、問い合わせ窓口の準備・専用電話回線の確保・問い合わせに対する回答のひな型・窓口の人員の確保という問題についても考えなければならない。

2.5.3 法規制的観点

(1) 開示等の根拠とその法的な性格

本項で検討した開示に含まれる通知・報告・公表等は、いずれも直接に明文で法律で求められているというものではない。しかしながら、上記謝罪の意の表明や本人における二次被害の回避のためにという観点から求められており、個人情報については、個人情報保護法に関する各省庁のガイドラインに記載が存在する。わが国では、平成16年4月2日閣議決定においてふれられており、そのあと、各省庁のガイドラインにおいてもふれられている。もっとも、そのそれぞれの要否等については、個別に検討した方が妥当であろう。これらの開示等の体制の整備までにふれている記載として、金融分野実務指針における「2-6-1 金融分野における個人情報取扱事業者は、1-2 又は6-6-1に基づき、自社内外への報告体制を整備するとともに、漏えい事案等が発生した場合には、次に掲げる事項を実施しなければならない。

監督官庁等への報告

本人への通知等

二次被害の防止・類似事案の発生回避等の観点からの漏えい事案等の事実関係及び再発防止策等の早急な公表」をあげることができる。

また、一般論としては、元請けからの委託作業を実施中に漏えい等に直面したという場合、契約書において、元請けとの守秘義務などを定めていることが多いものと思われ、そのような観点からのチェックも必要となる。

ア 本人への通知

⁴¹ (白井、2006) 26頁以下が詳しい。

各分野のガイドラインにおいて、情報漏えい時において、本人への通知を定めて⁴²いる。このような通知について法的な義務であると解する立場も存在する⁴³。また、個人情報保護法20条の「安全管理措置」の一つとして、事故時の対応が含まれ、そのなかの内容として、本人への通知が求められていると考えることもある。経済産業分野ガイドライン26頁は、『「事故又は違反への対処」を実践するために講じることが望まれる手法の例示』のなかで「(工)影響を受ける可能性のある本人への連絡 事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。」としているところである。

まず、このような通知は、「情報漏えいのおそれが存在する場合」に「原則として」求められるものになる。「情報漏えいのおそれが存在する場合」であるから、例えば、組織内において保管されていた情報データがそのまま流出したのかどうか確認しがたいという場合においても、上記開示等が求められることになる。

しかしながら、その一方で、漏えいと認識される事実が存在したから、すべて、このような通知等をなさなければならないというものではない。例外として、法執行の必要から、秘密裏に捜査を行う必要がある場合においては、このような法執行の必要

⁴² 金融分野ガイドライン 22条3項は「金融分野における個人情報取扱事業者は、個人情報の漏えい事案等の事故が発生した場合には、漏えい事案等の対象となった本人に速やかに漏えい事案等の事実関係等の通知を行うこととする。」とする

(<http://www.fsa.go.jp/common/law/kj-hogo/01.pdf>)

「個人情報の適正な取扱いを確保するために農林水産分野における事業者が講ずべき措置に関するガイドライン」(以下、農林水産分野ガイドラインという)25条(漏えい等が発生した場合の対応)は、1項は「事業者は、自己の取り扱う個人情報(委託を受けた者が取り扱うものを含む。以下この条において同じ。)の漏えい等の事実を把握した場合は、当該漏えい等に係る個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くものとする。」としている(<http://www.maff.go.jp/densiseifu/kojin/1.pdf>)

「国土交通省所管分野における個人情報保護に関するガイドライン」(以下、国土交通分野ガイドラインという)21条は、(漏えい等が発生した場合の対応)として「個人情報取扱事業者は、個人データの漏えい等が発生した場合は、事実関係を本人に速やかに通知するものとする。」としている。

2 個人情報取扱事業者は、個人データの漏えい等が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表するものとする。

など

⁴³ 「事業者と本人が契約関係にある場合には、その契約関係に由来する安全配慮義務の一種と解することもできるし、契約関係にないばあいであれば、不作為による不法行為の前提となる作為義務とも解される」という(大塚等、2005)32頁。

から、開示等がなされるべきではない場合というのを認識することができる。そのような場合には、犯人において証拠の隠滅・逃亡などを行うおそれが存在するのである。

それ以外にも、二次被害の防止および類似事案の回避という観点からするとき、そのような考慮がいない事案については、当事者への通知がいない場合も考えられる。経済産業分野ガイドラインにおいては、「ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。」とされ、そのような例外に当てはまる場合として「・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合、・高度な暗号化等の秘匿化が施されている場合、・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）」が例としてあげられているのである。

イ 監督官庁等への報告

個人情報保護法 32 条が、「主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し報告をさせることができる。」と一般的な報告の徴収を定めることに関連して、漏えいした情報が、個人情報である場合、監督官庁は、当該事件について必要があれば、報告を求める一般的な権限があることになる。また、そもそも、ガイドラインにおいて、個人情報の漏えい事件について監督官庁に対しての報告を定めていることがある。具体的には、経済産業省ガイドラインでは、監督官庁に対する報告について、認定個人情報保護団体に報告をおこなうことができるとする一方で機微的な情報の漏えいがあった場合には「経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。」としている（27 頁）。また、農林水産分野ガイドライン⁴⁴では、「3 事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、事実関係、発生原因及び対応策を農林水産省に直ちに報告するものとする。」としている。

ウ マスメディアへの公表

まず、二次被害防止と類似案件の防止という観点から公表が求められている。例えば⁴⁵、経済産業分野ガイドライン 27 頁において「二次被害の防止、類似事案の発生回

⁴⁴ 国土交通分野ガイドライン 2 1 条 3 項において「個人情報取扱事業者は、個人データの漏えい等が発生した場合は事実関係を国土交通省に直ちに報告するものとする。」としている。

⁴⁵ 医療・介護分野ガイドライン 4.(5) は、「(5) 個人情報の漏えい等の問題が発生した場合における二次被害の防止等 個人情報の漏えい等の問題が発生した場合には、二次被害の防止、類似事案の発生回避等の観点から、個人情報の保護に配慮しつつ、可能な限り事実関係を公表するとともに、都道府県の所管課等に速やかに報告する。」と定めている。

避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。」とされている。逆にそのような要請が強くない場合には、公表が必要ないものと考えられる。上記経済産業分野ガイドランにおいて「例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合⁴⁶には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。」とされているのは、このような趣旨であると思われる。

法律的な観点からは、公表等の文言が法的な責任問題等に関連しないように検討するということはもちろんのことである。特に不正行為による情報漏えいの場合、マスメディアは、その不正行為の広がり（特定の従業員のみ不正行為であるのか、一定のひろがりをもって不正行為なのか）という点について、興味をもつことがあるという点については、留意する必要がある。この場合、どのような手法で、この点についての調査したのかというのを明らかにしておくことが望ましい。また、メディアトレーニングやQ&A作成の際に、法的な問題を起こしそうな表現に注意すること、また、逆に、事件の性質によって新聞記者からの質問について予測することにも貢献すべきであろう。

しかしながら、その一方で、法律的な観点からの発言等にならないようにこころがける必要がある。マスメディアの問いたいのは、社会に対する責任であって、法律的な責任の問題に限らないのである。詳細については、初動調査の際の記述を参考されたい。

2.5.4 技術的観点

開示等においては、流出の経路・範囲等について一定の情報を開示する必要がある。その場合に、システムの構成等その他システムの脆弱性に関する情報を開示しないようにする必要がある。

農林水産分野ガイドランでは、25条2項において「2 事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、二次被害の防止、類似事案の発生回避の観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表するものとする。」と定めている（国土交通分野ガイドラン21条2項も同じ）。

⁴⁶ 具体的には、以下の場合をいう

- ・ 影響を受ける可能性のある本人すべてに連絡がついた場合
 - ・ 紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
 - ・ 高度な暗号化等の秘匿化が施されている場合
 - ・ 漏えい等をした事業者以外では、特定の個人を識別することができない場合
- （事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）

2.6 抑制措置と復旧

2.6.1 意義

(1) 概念

情報漏えい事件が発生したあと、被害については、拡大を防止し、漏えいした情報を消去することなどをこころみたりすることが必要である。そして、通常の業務に復帰していくことになる。被害拡大防止および被害回復が抑制措置ということになる。通常の業務に復帰していくことが復旧ということになる。

(2) 抑制措置

情報漏えい事件において、漏えいした情報について、被害拡大を防止し、その上で原状回復を図ることである。

被害拡大の防止としては、外部から自組織内のネットワークに侵入されて、組織内の情報が漏えいした疑いがある場合については、自組織のネットワークを調査し、侵入されている口をふさぐ。または攻撃されている先からの通信を遮断する、或いは、自組織のシステムに脆弱性があった場合は、パッチを適用するなどの措置を実施することが必要になる。また、Winny上に自組織内のファイルが流出している場合については、ウイルスに感染しているPCを抽出して、ネットワークから遮断することが必要である。

被害情報の回収については、漏えいした情報を可能な限り回収することが目標となる。この場合、漏えいした情報が紙や外部記憶媒体、PCなど物理的に存在する媒体に格納されている場合、これらの媒体を回収することにより、情報漏えいの被害は最小化できる。

従って、これらの媒体の紛失や盗難などが発覚した場合、盗難届けの提出や紛失した箇所の搜索など、可能な限りの搜索活動を実施することが必要である。

一方、デジタルデータとしてインターネット等に漏えいしてしまった場合は、情報の回収がより困難となるが、可能な限りの回収措置をとるべきである。

具体例については、Web等への掲示板系に掲載された場合においては、サイト管理者へ情報削除依頼をする。メールの誤送信で第三者へ送付してしまった場合においては、誤送信先へデータの削除依頼をする。もっとも、Winny上にファイルが流通している場合については、実効的な削除の方法というのは、困難である。

(3) 復旧措置

復旧措置とは、通常の業務に復帰していく過程をいうことになる。前述のようにバックアップからシステムを再構築したり、一からくみ上げるなどしたりして通常の運用にもどすことをいう。また、当座、もしできるのであれば、システムが同様の問題を引き起こさないようにすることをも含むであろう。その上、正常なファイルを回復すること、パッチをあてること、パスワードを変更することなどがある。

2.6.2 マネジメント的観点

被害の回復措置という観点から、500円から1000円程度の金品等(商品券やポイント等)を被害にあった本人に対して提供することがあり、それについてどのような認識をもって

対応するかという問題がある。本人に対する誠意の表明・企業イメージの早期回復、クレームや訴訟の回避の手段として有効であるという認識もある⁴⁷。その一方で、具体的な損害がない場合に、そのような対応が望ましいといえないのではないかという見解も存在している。被害対応の方法としては、組織等において、自主的に謝意をあらわす。そして、具体的な損害があれば、本人からの申入れに応じて、個別に聴取して、誠意を持って対応するという方法も十分になりたちうる対応方策である。

2.6.3 法規制的観点

被害拡散防止措置については、金融分野実務指針において「二次被害防止」が盛り込まれているのは前述したとおりである。また、情報漏えいに関する損害賠償事件において、流出した情報の回収に務めたことが事実認定され、それが、具体的な損害賠償の金銭的評価の際に斟酌された⁴⁸ことが伺える。これらの観点からいって、被害拡大防止措置を採用するのは、法律的な義務であると評価してもよいものと思われる。なお、ACCS に関する不正アクセス事件⁴⁹に関連して、「個人情報の掲載が確認された場合は、ACCS に報告するととも

⁴⁷ このような企業における対応の代表例であるヤフーBB 情報漏えい事件においては、その本人からの損害賠償をめぐる判決（大阪地判・平成 18 年 5 月 19 日）のなかで「原告らの個人情報は秘匿されるべき必要性が必ずしも高いものではなかったこと、被告BBテクノロジーが、本件恐喝未遂事件後、顧客情報の社外流出について発表を行い、不正取得されたことが確認できた顧客に対してその旨連絡するとともに、本件サービスの全会員に 500 円の金券を交付するなどして謝罪を行う一方、顧客情報についてのセキュリティ強化等の対策をとっていること（略）といった」一切の事情から、ひとりあたり 5000 円の損害、1000 円の弁護士費用が認定されている。

⁴⁸ 宇治市住民基本台帳情報漏えい事件（大阪高判・平成 13 年 12 月 25 日）では、「被控訴人らのプライバシーの権利が侵害された程度・結果は、それほど大きいものとは認められないこと、控訴人が本件データの回収等に努め、また市民に対する説明を行い、今後の防止策を講じたことを含め、本件に現れた一切の事情を考慮すると、被控訴人らの慰謝料としては、1 人あたり 1 万円と認めるのが相当である。」とされている。

TBC 情報漏えい事件判決（東京地判・平成 19 年 2 月 8 日）では、「本件情報の性質、本件情報流出事故の態様、実際に 2 次流出あるいは 2 次被害があること、原告らの本件訴訟の提起の目的が被告の行為の違法性を確認するためにいわゆる名目的な損害賠償を求めるものではなく、精神的な苦痛を慰藉するために損害賠償を求めるものと認められること、本件情報流出事故の発生後、被告は、謝罪のメールを送信し、全国紙に謝罪の社告を掲載するとともに、データ流出被害対策室及び TBC 顧客情報事故対策室を設置して、2 次被害あるいは 2 次流出の防止のための対策を検討し、発信者情報開示請求訴訟の提起や保全処分事件の申立てをするといった措置をとったことなど」といった事情の総合考慮の結果、1 人あたり各 3 万円の慰藉料の支払を命ずるのが相当であるとしている。

⁴⁹ 東京地裁判決・平成 17 年 3 月 25 日

に、掲示板の管理者などに対して個人情報の削除を求め、当該個人情報を掲載した者を特定するための情報収集を行うこと。」という条件で和解が成立している事実もある⁵⁰。

なお、流出した情報がいわゆる名簿屋等に並んでいる場合に、買い取るべきかどうかという法的な問題がある。不当要求の場面でもないかぎり、適切な値段で買い取ることであり被害拡散防止・原状回復に努めることができるという見解がある。

2.6.4 技術的観点

(1) 被害拡大防止戦略について

被害拡大防止のために重要なものは、システムの遮断、ネットワークからの切断、特定の機能の無効化などの決断作業そのものになる。この決断の作業は、困難な経営判断を本質とするが、技術者としては、攻撃の性質と損なわれたシステムの資源の性質から、経営者に対してアドバイスを与えることになる。

また、このような決断は事前に十分な評価をなしておいて、予め決めておくようにしておくことが望ましいことは前述した(2.3 初動対応)。

また、この避害拡大防止策については、その対応策を採用する段階で二次的な不具合を引き起こすことがありうるということに注意する必要がある。このような具体例として、攻撃されたシステムが、定期的に他のホストに対して定期的に通信を行うプロセスを実行することがあり、そのような場合に、ネットワークから切断すると、そのプロセスが、ハードドライブのすべてのデータを上書きしてしまうことがある⁵¹。技術者としては、具体的におきている事象について、そのような二次的な不都合を十分に予測して対応をしなければならないことになる。

上記の判断を問題に対しての当面の回避策とするのか、根本的な防止策とするのかという点についても判断が必要となる。

(2) 損害発生防止策の具体例について

技術的な攻撃により情報漏えいが発生した場合、代表的な攻撃に対して考慮すべき事項は、以下のとおりである。

ア 不正アクセスによる攻撃の場合の損害発生予防策について

不正アクセス時においては、早急な対応が必要である。攻撃者がパスワードファイルを取得してしまったような場合、攻撃されたコンピュータのみならず、そのパスワードを悪用されて他のコンピュータに対しての侵入の可能性も発生してくる。これらの状況のもとで、「影響を受けたシステムの隔離」「影響を受けたサービスの無効化」「環境への攻撃者の侵入ルートの排除」「攻撃に用いられたユーザの無

この事件と脆弱性の位置づけについては、高橋郁夫「脆弱性にかかわる法的側面について」(情報処理 484 巻・659 頁参照。

⁵⁰ <http://www2.accsjp.or.jp/news/news.html>

⁵¹ (NIST SP800-61) J3-19 参照

効化」「物理的セキュリティの強化」などの手段を採用することになる。

イ 内部犯行の場合

企業において営業秘密が漏えいしている場合においては、実際に当人の家において、該当データを消してくることになる。具体的には、個人宅において、上記のような手段でもって、個人の利用している利用している PC を確保して、その HDD 等の記録媒体の情報を完全消去して、再インストールすることになる。また、この場合においては、調査の項目で説明した証拠の収集の要素が重要なことになる。

2.7 事後対応

2.7.1 事後対応の概念

情報漏えい事件対応のなかで、もっとも重要なことは、再発防止のためにこのような対応によって何を学び、何を改善していくかということになる。復旧によって、通常に復帰したあとに、事件から発生した種々の関係に対する対応を行うのと同時に事件対応から学び日常の業務を改善するのが事後対応である。事後対応としては、ア 再発防止策の立案と実行、イ 調査委員会による原因・経過等に対する調査、ウ 不正行為が存在している場合の行為者への懲戒・責任追及、エ 管理態勢構築を怠ったことに対する責任追及、オ 被害者に対する損害賠償の問題、カ 日常業務の改善などの問題がある。

(1) 再発防止策の立案と実行

発生した情報漏えいに関して、前述の調査によって明らかになった原因に対して、根本的に再発を防止する策を立案し、実行することが必要になる。

主に再発防止策は、技術面、業務プロセス面、人的側面の3つの観点を組み合わせて立案することが一般的である。

ア 技術面

技術的にツール類を導入し、原因となった事象を「検知する」、「操作ログなどを取得することにより抑止させる」、「強制的にできなくさせる」の3つのレベルを業務状況に合わせて導入する。

イ 業務プロセス面

ツール導入により、或いはツール導入をしない場合でも、原因となった事象について業務プロセス上、可視化し一定のチェックが入るようにすること、業務プロセスを変更して、事象が発生しないように工夫する等の施策を導入する。

ウ 人的側面

原因となった事象について、従業員研修のメニューに追加し、全従業員の意識向上を図る。また、必要に応じて従業員就業規則を見直し、罰則規定を明確化し抑止効果を図る。

(2) 調査委員会による原因・経過等に対する調査

情報漏えい事故がきわめて深刻な被害を引き起こしたとか、社会の注目をひいたという場合に、調査委員会を構成し、委員会が事故の原因を追及し、情報漏えい事故の原因に関

連する事実を明らかにすることは、原因者に対する懲戒、責任請求、管理者に対する責任追及、再発防止措置の基礎となるのとともに、対外的に、事故をおこした会社が、自浄機能を有することを社会に対してアピールする効果を有することも含めて、きわめて有意義である。

この委員会は、取締役会決議等に基づいて設置され、また、中立性・独立性維持の観点から社外からの専門家もメンバとして、参加する形になる。

また、この段階で、調査委員会もしくは、会社の経営層は、技術専門家からの技術専門調査報告書の提出を受けることになる。

この調査委員会の報告書⁵²については、社会に対して公表されることも多い。

(3) 事後的な責任についての諸問題の検討および対応

この問題に該当する事項として「不正行為が存在している場合の行為者への懲戒・責任追及」「管理態勢構築を怠ったことに対する責任追及」「被害者に対する損害賠償の問題」などがあげられる。具体的な検討については、後述の法的な見解からの分析を参照のこと。

(4) 広報との関係での事後対応

広報面において(ア)進捗管理(イ)事後検証(ウ)ブランドイメージ回復措置が必要になることは留意すべきである。

ア 進捗管理というのは、危機が完全に収束したと判断できるまで、組織内外の状況を継続的に把握し、追加の広報対応が必要だと思われる場合には、情報漏えい対応本部に提言することになる。

イ 事後検証というのは、情報漏えい事故に対する対応について、広報の観点から振り返り改善策を検討することになる。

ウ ブランドイメージ回復措置

漏えい事故対応が収束したと判断された段階で、ブランドイメージ回復のための取り組みについて提案する作業である。

(5) 日常業務の改善

情報漏えい対応について復旧手続が終わった段階などで、情報漏えい事件から復旧して、遅滞なく、当該事件から学ぶことはなにかという点についての関係者の会合が開かれることが望ましい。

2.7.2 マネジメント的観点

(1) 企業文化と事後対応

再発防止策については、まさに経営そのものであり、企業の文化・風土というものについての根本的な見直しの可能性をも含むものである可能性がある。例えば、自宅で週末に仕

⁵² (大塚, 2005) は、調査委員会およびその作成すべき報告書について、調査の委員の構成、委員会の根拠、組織の必要性、調査の目的と項目、報告の提出、公開の必要性などの各点について詳細に検討する (NBL811・91 頁以下)。

事を作業して、翌週の仕事に間に合わせようとして仕事用のデータをいれていた PC を帰宅途上で紛失したという事件をとってみても、この事件が再発されないようにするには、自宅で仕事をするを「よい」とする文化について、どのように認識するかということまで検討しないと抜本的な解決にならないのである。また、PC の紛失について、それが報告としてきちんと報告のルートに載っているかということもある。

その一方で、事件に対して、情報の活用を忘れ去ったかのように情報システム構築をすること、従業員に対する不信からする監視強化も経営者の陥りやすい罠ということができよう。本書の性格上、詳細に論じる余裕はないが、再発防止策を考慮し、実装していくに際しては、組織等における情報の利用とセキュリティのバランスというリスク管理の基本に配慮した対応が必要とされるものということができるであろう。

(2) 情報セキュリティポリシー・漏えい対応ポリシーの見直し・改善

後述するような技術的な報告書などに表れる数値の意味することなどを前提にしながら、情報漏えい対応ポリシーおよび手順の見直しをしていくことになる。また、それによって通常のセキュリティポリシーに対する見直しなどもおこなわれるであろう。

(3) 情報漏えい保険の適用

また、事後的な対応のなかには、上記のような種々の対応以外にも、いわゆる情報漏えい損害保険の適用を検討することもありうるであろう。この個人情報漏えい損害保険というのは、業務遂行の過程にともなって発生した個人情報の漏えいに起因して損害賠償がなされた場合において、法律上の損害賠償を負う場合に、その被る損害をカバーするものである。一般には、法律相談費用、コンサルティング費用、事故対応費用、広告宣伝活動費用、見舞金費用が担保されることになる。したがって、具体的な項目としては、詫言状発送費用、謝罪広告費用なども担保されることになる。

2.7.3 法規制的観点

(1) 問題の所在等

事後対応と法的観点の問題としては、(ア) 調査委員会に対する関与、(イ) 不正行為が存在している場合の行為者への懲戒・責任追及(ウ) 管理態勢構築を怠ったことに対する責任追及、(エ) 被害者に対する損害賠償の問題などの問題がある。また、再発防止体制を構築するのにあたっての法的な観点についても検討する必要がある。その上で、証拠の保存方針についても検討しておく必要がある。

本報告書は、法律の専門的な解釈等を議論するものではないが、上記各問題について法的な問題点については、おおよそ以下のような内容になる。

(2) 具体的な法的問題点等

ア 調査委員会に対する関与

復旧が終了し、通常時に復帰したとしても、組織等としては、情報漏えい事件について事実関係を究明して、今後の再発防止に役立て、また、責任追及等を行わなければならないことは上述したとおりである。このような調査に際しては、弁護士が、事

実調査についての専門家としての役割を期待されること、そして、調査対象となる組織等の利害から独立した第三者としての役割を担い得るという独立性の見地から、調査委員会において、重要な地位につくことが多い。弁護士等としては、不正調査の手法については、かなりの専門性があることや証拠としてのデジタル情報の重要性やこのような情報から詳細な事項を明らかにするデジタル・フォレンジックの活用の可能性などについて日頃から理解できるように研鑽を積んでおく必要があるものといえよう。

イ 不正行為が存在している場合の行為者への懲戒・責任追及

内部者が情報漏えいに関与している場合などについては、そのような事実を確認した上で、そのものに対して企業秩序維持の観点から、懲戒処分をなさなければならぬし、また、組織等において発生した損害について、損害賠償を請求すべきかどうかという問題がある。

従業員に対する懲戒の問題については、発生した情報漏えいに関して、組織内における責任の所在を明らかにしておく必要がある。役員の就業規則及び従業員の就業規則と照らし合わせて、処分をする必要があるか否かを判断した上で、結論を出すことになる。これは、対外的に責任の所在を明確化し、再発防止策の実施と合わせて組織として自浄能力があることを示すことになること、組織内において、過失や故意の事象について厳格な処分対象となることを示すことにより抑止効果を図るという2つの目的がある。但し、各就業規則と照らし合わせて、処分の有無は普遍性かつ公平性が問われるため、他の罰則を鑑み慎重に決定する必要がある。

一般的には、就業規則等の違反として、解雇される例が多いようである。もっとも、Winny や Share ネットワーク利用による情報漏えい事件においては、Winny/Share というソフトウェアは、通常の利用者が適法に利用しうる余地がきわめて少ないものであることを根拠として、組織において、Winny ネットワーク利用が厳格に禁止されていること、それらが事前に周知されていること、また、規則が実際に遵守されていることなども重要であろう。また、組織が、自宅での仕事を許容しており、むしろそれを推奨していたような場合、漏えいという結果に対して懲戒するということがないような配慮は必要とされるであろう。

ウ 管理態勢構築を怠ったことに対する責任追及

情報漏えいによって、直接の損害を被った（例、企業秘密の流出など）り、個人情報漏えいに関して信用低下により顧客離れをきたしたりした場合、その原因となった行為自体ではなく、その行為者が、そのような行為をなさないような管理・監督体制を取締役が事前に構築しておくべきであったのではないかという問題がある。

この点について、取締役においては、リスク管理態勢を事前に構築すべきであり、そのような管理態勢の構築を怠る場合には、その管理態勢構築義務を怠ったことを理由に損害賠償が認められることがあるものと解される。なお、株主代表訴訟の場合に

限らず、被害者が、商法 266 条の 3（改正前）にもとづいて取締役等に対して直接にみずからの損害賠償を求めて請求が認容されている例⁵³がある。

エ 被害者に対して負う損害賠償債務の問題

これは、情報漏えいによって、その個人情報漏えいした本人に生じた損害を賠償するかどうかという問題である。近時の判決例として、宇治市住民基本台帳情報漏えい事件、ヤフーBB 情報漏えい事件判決、TBC 情報漏えい事件判決は、すでに紹介している（本章 2.6.2 および 2.6.3）。

また、Winny ネットワークにおけるいわゆる暴露ウイルスによって、平成 16 年 3 月に、北海道警察江別署交番勤務の巡査が所有するノート PC から、個人情報 8 人分を含む捜査関係書類 5 種類 6 件（現行犯人逮捕手続書、捜査報告書、参考報告書、交通事故発生報告書、実況見分調書）が流出し、ネット上で閲覧できる状態になったのに対して、その本人が、北海道に対して損害賠償を求めたという事件は、興味深いものである。第 1 審判決（札幌地裁判決（平成 17 年 4 月 28 日）は、北海道に 40 万円の賠償を命じ、札幌高等裁判所（平成 17 年 11 月 11 日判決）は、損害賠償を認めなかった（最高裁判所が平成 18 年 10 月 19 日に、上告を棄却）もっともこの事件については、Winny ネットワークおよび暴露ウイルスの危険性が明らかになっている現時点においては、自宅での私的利用の際に業務上の情報が漏えいした場合でも、組織等における責任問題になるものと思われ、事件として特殊性が存在しているものと認識しておく方が妥当であろう。

なお、個人情報漏えいした場合に個人情報保護に関する各省庁のガイドラインについては、その不遵守が、直接に法的な意味で過失を意味するものではないということが出来るが、その一方で、何故に、ガイドラインに定めている事項について、これを守っていなかったのかという点について明らかにすることはもとめられるのであろう。

オ 再発防止策における法的留意点

再発防止策において、具体的な手法において、法的な問題が発生しないのか、また、法的に問題が発生しないとしても、経営上、望ましいのかについて判断が必要となる。

現在、情報漏えい事件に対応するために、従業員のネットワーク活動に対する記録を行うサービス等の提供が盛んになってきている。このような場合、そのような記録を取得することを従業員あてに明示しておくことが必要になるものと考えられよう。経済産業分野ガイドライン 36 頁は「従業者を対象とするビデオ及びオンラインによるモニタリング（以下「モニタリング」という。）を実施する場合は、次の点に留意する。その際、雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あら

⁵³ なお、現在の会社法 429 条（役員等の第三者に対する損害賠償責任）の規定に対応する。判決例としては、東京地判・平成 15 年 2 月 27 日（判例時報 1832 号 155 頁） などがある。

かじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましい。また、その重要事項を定めたときは、労働者等に周知することが望ましい。」としている。

また、その運用によって従業員に対する監視的なものになってしまうことが考えられ、そのような運用は、かえって不正行為を産む企業文化をつくってしまうことになるものと考えられるのである。

カ 証拠の保存方針について⁵⁴

情報漏えい対応の際に収集された証拠について、どの程度の期間、保存しておくべきかというのを決めて運用することになる。具体的には、刑事手続きの可能性、民事手続きの可能性、通常の文書保存方針、コストの問題などから総合的に考察することになる。

2.7.4 技術的観点

(1) 技術的分析による事実究明の意義

確保した PC を詳細に技術的に検討することによって、種々の事実を判明させることになる。種々の法的な対応ができるかどうかにかかわらずこのような事実の判明のためにそのような事実が必要になってくる。

たとえば、従業員に対して、懲戒等の処分を行う際に、その従業員が、P2P ファイル交換ソフトを利用しませんという誓約書を書いたのちに、その誓約に違反していたかどうか、また、その漏えいが、ウイルスでもれたのか、それとも、意図的だったのかかなどを調査する必要がある。聴取によると、一般の事案において、これを調べなければならないケースが増えているとのことである。

(2) インシデント対応記録分析と対応ポリシーの改善

再発防止策および日常のセキュリティポリシーの改善、情報漏えい対応ポリシーの改善のために、技術者が、情報漏えい対応した際に経験し、学んだ事項を経営層にフィードバックすることはきわめて重要なことである。

情報漏えい事件から復旧して、遅滞なく、当該事件から学ぶことはなにかという点についての関係者の会合が開かれることが望ましい。そして、その際に技術者としては、「厳密にいつ何が発生したのか」「経営層・スタッフの対応は適切であったか、従前の手順は、遵守されたのか」「より早く入手されるべき情報は何か」「復旧を妨げたかもしれない行動等が存在したのか」「再発を防止するための適切な措置は何か」「分析・調査・対応などに際して将来必要となるツールや資産などがあるか」という点について、一定の見解を明らかにしておくことは有意義である。

(3) 技術的報告書作成の際の留意事項

また、技術的見地からの報告書も将来に向けてきわめて有意義な意味をもつ。まず、そのような報告書は、同様な事件に際しての有意義な参考文献となる。事件および対応の時

⁵⁴ 米国に於ける議論については、(NIST SP800-61) J3 - 26 頁参照

系列的な記録を参照できるようにまとめておくことは、法的な対応にも役立つし、また、事件によって組織等に発生した損害の額（データ、ソフトウェア、ハードウェア、対応の人件費）を認識するのに役に立つことになる。

（４）技術的手段による監視

情報漏えい事故の形態によっては、技術的手段を使用した監視を行うことが重要となる場合がある。

たとえば、ノートPCの盗難によって情報漏えいが発生したならば、盗難品が出品されていないかについてネットオークションサイトを一定期間監視する、といった手段が有効に作用することもありうる。

第4 情報漏えい対応のまとめ

1. 情報漏えいパターン別対応フロー～紛失・盗難～



ステップ1 【事故分類と主なきっかけ】

No	事故事例の例	主なきっかけ
1	パソコンやUSBメモリなどを電車の中、飲み屋などに置き忘れてしまった。	・自己申告 ・警察からの連絡 ・取得者からの連絡
2	パソコンやUSBメモリが入った鞆をひったくりにあい、盗まれてしまった。	
3	海外での置き引きや車上荒らしにあい、パソコンやUSBメモリなどを盗まれてしまった。	
4	事務所荒らしにあい、事務所のパソコンを盗まれてしまった。	

ステップ2 【紛失・盗難による漏えいの事実確認を5W1Hで実施する。】

(1) 紛失、盗難の当事者は誰なのか?
 (2) 何(物)が紛失、盗難したのか?
 (3) 紛失、盗難の対象物に格納されていた情報はなに?
 (4) いつ紛失、盗難が発生したのか?
 (5) どこで紛失、盗難が発生したのか?
 (6) なぜ紛失、盗難が発生したのか?
 (7) 紛失、盗難が発覚した理由は何なのか?

a) 誰の情報なのか?
 b) 何の情報なのか?
 c) いつ頃の情報なのか?
 d) どの(ら)い量の量なのか? (1件なのか100万件なのか)
 e) どのような形で保護されていたのか?
 (暗号化、平文、HDD保護、パスワード保護)

ステップ2 【応急措置の例】

No	応急処置	留意事項
1	紛失物の捜索・回収	-
2	警察への届出	

ステップ5 【二次被害防止の例】

No	二次被害防止策	留意事項
1	クレジットカード、銀行口座番号、IDパスワードが含まれていた場合: 本人に通知し、カード停止、口座停止、ID停止を促す。	-

2. 情報漏えいパターン別対応フロー～誤送信・Web誤公開等～



ステップ1 【事故分類と主なきっかけ】

No	事故事例	主なきっかけ
1	メールで、メールアドレスを打ち間違え誤送信した。	・自己申告(内部発見) ・受信者からの指摘 (風評も含む)
2	メールで本来BCCとすべき送信先をCCにして送信してしまった。	
3	FAXで電話番号を間違え送信した。郵便で、住所を間違えて送付した。	
4	Webの脆弱性で非公開情報が公開されていることがわかった。	
5	Webプログラムのミスで誤った個人情報を掲示してしまった。	
6	Webサイトから他の会員へ誤ってIDパスワードを送信してしまった。	
7	Webで誤って非公開情報を公開情報としてしまった。(サーバ移行時の非公開情報の削除漏れ、IDパスワードにより保護されるべき情報がサーバ設定ミスで公開エリアに保管、公開サーバへデータを転送する際に非公開の情報データを誤って転送など)	
8	譲渡が禁止されている情報を第三者へ売却してしまった。	

ステップ2 【遺失(誤送信・Web誤公開)による漏えいの事実確認の手段】

(1) 誤送信・Web誤公開の当事者は誰なのか？	a) 誰の情報なのか？
(2) 何(物)を誤送信・Web誤公開したのか？	b) 何の情報なのか？
(3) 誤送信・Web誤公開の対象物に格納されていた情報はなに？	c) いつ頃の情報なのか？
(4) いつ誤送信・Web誤公開が発生したのか？	d) どの(らしい)量なのか？ (1件なのか100万件なのか)
(5) どこで誤送信・Web誤公開が発生したのか？	e) どのような形で保護されていたのか？
(6) なぜ誤送信・Web誤公開が発生したのか？	(暗号化、平文、パスワード保護)
(7) 誤送信・Web誤公開が発生した理由は何なのか？	

ステップ2 【応急措置の例と留意事項】

No	応急処置	留意事項
1	【メール・FAX・郵便の誤送信/誤譲渡の場合】 (1) 受信者への連絡と情報の廃棄	受信者に連絡が取れない場合の対応 (例えばフリーメールアドレスへの誤送信など)
2	【Webサイトへの誤公開】 (1) 誤って公開してしまった情報の削除	情報の削除 該当情報を保持又は掲載する第三者が情報削除に応じてくれない場合の対応

ステップ5 【二次被害防止の例】

No	二次被害防止策	留意事項
1	【Webサイトへの誤公開】 (1) 検索サイトからのキャッシュ削除 (2) サイトの停止/脆弱性の除去	クレジットカード、銀行口座番号、IDパスワードが含まれていた場合: 本人に通知し、カード停止、口座停止、ID停止を促す。

3. 情報漏えいパターン別対応フロー～内部犯行～



ステップ1 【事故分類と主なきっかけ】

No	事故事例	主なきっかけ
1	社内データベースから顧客情報を不正に持ち出し転売した。	・外部からの指摘 (風評も含む)
2	社外Webシステムへ過去業務で利用していたIDを利用してアクセスし、不正にデータを持ち出した。	
3	社内から設計機密情報を不正に持ち出し、他社へ渡した。	

ステップ2 【内部犯行による漏えいの実事確認を5W1Hで実施する、】

- (1) 内部犯行の当事者は誰なのか？
 (2) 何(物)を持ち出されたのか？
 (3) 内部犯行の対象物に格納されていた情報はなにか？
 (4) いつ内部犯行が発生したのか？
 (5) どこで内部犯行が発生したのか？
 (6) なぜ内部犯行が発生したのか？
 (7) 内部犯行が発覚した理由は何なのか？
- a) 誰の情報なのか？
 b) 何の情報なのか？
 c) いつ頃の情報なのか？
 d) どの(らしい)量なのか？ (1件なのか100万件なのか)
 e) どのような形で保護されていたのか？
 (暗号化、平文、HDD保護、パスワード保護)

ステップ2 【応急措置の例】

No	応急処置	留意事項
1	社内対象サイト(イントラサーバ、共有ファイルサーバなど)のID停止やアクセス制御の実施	証拠保存を実施する際には、コンピュータフォレンジックを考慮した確保が必要のため、慎重な対応を行うこと。(専門家への依頼なども考慮する)
2	内部犯行当事者の関連装置の確保(証拠保存)	

ステップ5 【二次被害防止の例】

No	二次被害防止策	留意事項
1	警察への届出	・第三者から情報回収 該当情報を保持又は掲載する第三者が情報回収に応じてくれない場合の対応
2	漏えいの可能性のある情報の回収	
3	ID/パスワード、アクセス権限の見直し	
4	脆弱性の除去	
5	クレジットカード、銀行口座番号、ID/パスワードが含まれていた場合:本人に通知し、カード停止、口座停止、ID停止を促す。	

4. 情報漏えいパターン別対応フロー～Winny/Share等への漏えい～



ステップ1 【事故分類と主なきっかけ】

No	事故事例	主なきっかけ
1	社員が会社機密情報や個人情報を持ち帰り(USBメモリでの持ち出しや社内メールを自宅メールへ転送したもの)、自宅の個人PCへ格納しており、本人や家族がWinnyを利用していたところアンチウィルスに感染し、Winny/Shareネットワークへ情報が漏えいした。	・外部からの指摘(風評も含む)

ステップ2 【Winny/Shareによる漏えいの事実確認を5W1Hで実施する。】

(1) Winny / Share ネットへ流出させた当事者は誰なのか？	a) 誰の情報なのか？
(2) 何(物)をWinny / Share ネットへ流出されたのか？	b) 何の情報なのか？
(3) Winny / Share ネットへ流出した情報は、	c) いくつの情報なのか？
(4) いつWinny / Share ネットへの流出が発生したのか？	d) どの(くらい)の量なのか？ (1件なのか100万件なのか)
(5) どこでWinny / Share ネットへ流出が発生したのか？	e) どのような形で保護されていたのか？ (暗号化、平文、HDD保護、パスワード保護)
(6) なぜWinny / Share ネットへの流出が発生したのか？	
(7) Winny / Share ネットへの流出が発覚した理由は何なのか？	

ステップ2 【応急措置の例】

No	応急処置	留意事項
1	インターネットからのPCの切り離し(Winny/Shareの利用停止)	-
2	漏えいしたファイル(情報)の確保	

ステップ5 【二次被害防止策の例】

No	二次被害防止策	留意事項
1	ウィルス駆除	・Winnyなどネットワーク上の情報削除 WinnyなどのP2P環境から情報削除に応じてくれなかった時の対応
2	個人情報や会社情報の削除	
3	クレジットカード、銀行口座番号、IDパスワードが含まれていた場合:本人に通知し、カード停止、口座停止、ID停止を促す。	

5. 情報漏えいパターン別対応フロー～不正プログラム～



ステップ1 【事故分類と主なきっかけ】

No	事故事例	主なきっかけ
1	ウイルスに感染し、PCを不正操作され、PC内の会社機密情報が悪意のある第三者に搾取された。	・自己申告 / 内部発見
2	ウイルスに感染し、会社機密情報がWebサイトへ掲載され、誰でも閲覧可能な状態になっていた。	・外部からの指摘

ステップ2 【不正プログラムによる漏えいの事実確認を5W1Hで実施する。】

- (1) ウイルス感染した当事者は誰なのか？
 (2) 何(物)がウイルス感染したのか？
 (3) ウイルス感染により漏えいした情報は、
 (4) いつウイルス感染が発生したのか？
 (5) どこでウイルス感染が発生したのか？
 (6) なぜウイルス感染が発生したのか？
 (7) ウイルス感染が発覚した理由は何なのか？
- a) 誰の情報なのか？
 b) 何の情報なのか？
 c) いつ頃の情報なのか？
 d) どの(ら)い量の量なのか？ (1件なのか100万件なのか)
 e) どのような形で保護されていたのか？
 (暗号化、平文、HDD保護、パスワード保護)

ステップ2 【応急措置の例】

No	応急処置	留意事項
1	ウイルス感染したPCの特定	-
2	ウイルス感染したPCのネットワークからの切り離し	

ステップ5 【二次被害防止策の例】

No	二次被害防止策	留意事項
1	ウイルス名の特定と駆除	・第三者から情報回収 該当情報を保持又は掲載する第三者が情報回収に応じられない場合の対応
2	脆弱性の除去	
3	漏えいした情報の回収	
4	クレジットカード、銀行口座番号、ID/パスワードが含まれていた場合：本人に通知し、カード停止、口座停止、ID停止を促す。	

6. 情報漏えいパターン別対応フロー～不正アクセス～



ステップ1 【事故分類と主なきっかけ】

No	事故事例	主なきっかけ
1	WebでのIDパスワードを不正利用され、情報を他のサイトに掲示された。	・自己申告(内部発見)
2	Webでの脆弱性を悪用し、不正アクセスされ、非公開情報を搾取された。	・外部からの指摘
3	Webアプリケーションの脆弱性を悪用されDBサーバの非公開情報を搾取された。	(風評も含む)
4	Webアプリケーションの脆弱性を悪用されWebサイトへウィルスを埋め込まれた。	

ステップ2 【不正アクセスによる情報漏えいの事実確認を5W1Hで実施する。】

- (1)不正アクセスした当事者は誰なのか？
- (2)何(物)を不正アクセスされたのか？
- (3)不正アクセスされた情報は、
- (4)いつ不正アクセスが発生したのか？
- (5)どこで不正アクセスが発生したのか？
- (6)なぜ不正アクセスが発生したのか？
- (7)不正アクセスが発覚した理由は何なのか？
- a) 誰の情報なのか？
b) 何の情報なのか？
c) いくつ頃の情報のか？
d) どのくらいの量なのか？ (1件なのか100万件なのか)
e) どのような形で保護されていたのか？
(暗号化、平文、HDD保護、パスワード保護)

ステップ2 【応急措置の例】

No	応急処置	留意事項
1	不正アクセスを受けた機器(サイト)のネットワークからの切り離し	
2	不正アクセスを受けた機器(サイト)の停止	
3	暫定サイトの立ち上げ	

ステップ5 【二次被害防止の例】

No	二次被害防止策	留意事項
1	漏えいした情報の回収	・第三者から情報回収
2	Webサーバ設定の見直し/IDパスワードの変更	該当情報を保持又は掲載する第三者が情報回収に応じてくれない場合の対応
3	サーバ、Webアプリケーションの脆弱性の除去	
4	クレジットカード、銀行口座番号、IDパスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID停止を促す。	

7. 情報漏えいパターン別対応フロー～その他(風評・ブログ掲載)編～



ステップ1 【事故分類と主なきっかけ】

No	事故事例	主なきっかけ
1	社内の機密情報が匿名掲示板へ書き込まれた。	・外部からの指摘 (風評も含む)
2	自分の公開しているブログであまり意識せずに、会社機密情報を公開情報としてしまった。	

ステップ2 【その他(風評・ブログ掲載)の事実確認を5W1Hで実施する。】

- | | |
|--|---|
| (1) 掲示板・ブログへ書き込んだ当事者は誰なのか？
(2) 何(物)を掲示板・ブログへ書き込まれたのか？
(3) 掲示板・ブログへ書き込まれた情報はなにか？
(4) いつ掲示板・ブログへ書き込まれたのか？
(5) どこで掲示板・ブログへ書き込まれたのか？
(6) なぜ掲示板・ブログへの書き込みが起こったのか？
(7) 掲示板・ブログへ書き込みが発覚した理由は何なのか？ | a) 誰の情報なのか？
b) 何の情報なのか？
c) いつ頃の情報なのか？
d) どの(ら)い量の量なのか？ (1件なのか100万件なのか)
e) どのような形で保護されていたのか？
(暗号化、平文、HDD保護、パスワード保護) |
|--|---|

ステップ2 【応急措置の例】

No	応急処置	留意事項
1	掲示板・ブログへ書き込まれた情報の削除	・第三者から情報回収 該当情報を保持又は掲載する第三者が情報回収に応じてくれない場合の対応

ステップ3 【二次被害防止の例】

No	二次被害防止策	留意事項
1	検索サイトからのキャッシュ削除	-

8. 全般的な留意事項

警察への被害届

下記のような可能性のある場合は、警察へ被害届を行うことを考慮する。

- (1) 従業員の内部犯行によって情報が漏えいしてしまった場合
(背任、不正競争防止法違反等被疑事件)
- (2) 外部からの侵入等によって情報が漏えいしてしまった場合
(不正アクセス禁止法違反被疑事件)
- (3) 漏えい情報に関して不正な金銭等の要求を受けた場合
(恐喝・脅迫・強要等非議事件)

マスコミへの公表

マスコミへ公表をする際には、個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン、「改訂に伴う「事実関係、再発防止策等の公表」の考え方を考慮し、対応方法を検討する。

～以下抜粋～

(カ)事実関係、再発防止策等の公表

二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。

ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。

- ・影響を受ける可能性のある本人すべてに連絡がついた場合
- ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
- ・高度な暗号化等の秘匿化が施されている場合
- ・漏えい等をした事業者以外では、特定の個人を識別することができない場合
(事業者が所有する個人データと照合することによって、はじめて個人データとなる場合)

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
(平成16年10月22日厚生労働省経済産業省告示第4号、平成19年3月30日改正) (PDF:411KB)
http://www.meti.go.jp/policy/it_policy/privacy/070330guideline.pdf

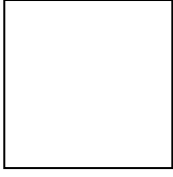
9. 事故告知、謝罪などの構成例

外部向け(プレス、個人宛など)の告知、謝罪に含まれるべき項目

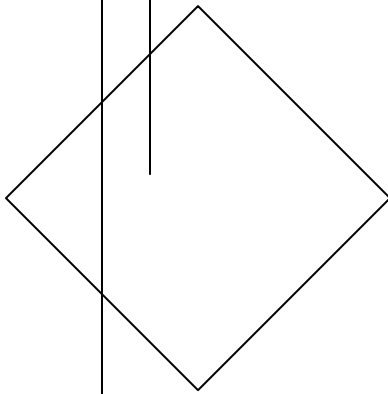
- ↓序文(発生した情報漏えい事故に関する謝罪、今後の会社としての取り組みなど)
- ↓事故発生に関する状況報告
 - ↓事実経緯
 - ↓調査方法及び状況
 - ↓漏えいした情報の内容
 - ↓事故の被害内容(二次被害の影響含む)
 - ↓事故原因
 - ↓当面の対応策
 - ↓再発防止策
- ↓問い合わせ窓口(事故に関する連絡先)

官庁向け事故報告書に含まれるべき項目

- ↓事業者名
- ↓発覚日
- ↓事故原因
- ↓漏えいした情報の内容
- ↓事故の被害内容(二次被害の影響含む)
- ↓警察届出有無
- ↓個人への連絡
- ↓再発防止策



付録編



付録1 Winnny (P2Pネットワーク)とインターネットの関係

はじめに

Winnnyに代表されるP2Pファイル交換ソフトは、我が国におけるブロードバンドインターネットと歩調を合わせるように普及した。2001年頃からADSL等のブロードバンドインターネットが全国で利用可能となり、インターネットの成長期に入るとともに、WinMX等のP2Pファイル交換ソフトの利用が加速し、インターネットへのトラフィックの影響が出始めたのもこの時期であると思われる。また、2001年11月28日にはファイル交換ソフトによる著作権侵害で容疑者が逮捕されるなど、P2Pファイル交換ソフトを取り巻く様々な問題が顕在化しだしたのもこの頃である。2002年にはWinnnyが開発され、さらに2003年8月にはWinnny利用者の情報漏えいを引き起こすウイルス「Antinny.A」の感染活動が確認され、現在の混沌としたP2Pファイル交換ソフトを取り巻く情勢が出揃ったのがこの時期である。

本稿ではWinnnyなどのP2Pファイル交換ソフトがインターネットとユーザに与えた影響について述べることにしたい。

1 P2Pファイル交換ソフトが形成するネットワークについて

1.1 プライベートネットワークとP2Pネットワークの比較

P2Pファイル交換ソフトが形成するネットワーク(以下、P2Pネットワークと称す)は、特定のP2Pファイル交換ソフト利用者で構成するネットワークであり、インターネット全体からみると、インターネットVPN等で構成されるプライベートネットワークと同様に無数に存在するインターネットネットワークの一つである。企業などが構築するプライベートネットワークとP2Pネットワークを比較すると以下の特徴がある。

表.1 プライベートネットワークとP2Pネットワークの比較

	プライベートネットワーク	P2Pネットワーク
管理者	存在し通信を管理	不在
通信の秘匿性	有している	同左
利用者	固定的	不特定多数
取り扱う情報	企業等の内部情報	音楽・動画等が多い?
セキュリティ対策	実施可能	実施困難
通信品質	管理可能	管理困難

P2P ネットワークには明確な管理者が存在しないため、ネットワークに参加するユーザのセキュリティ対策や通信品質など品質の担保が難しい。特にセキュリティ対策に関する問題は深刻で、P2P ネットワークのメンバのなかでセキュリティレベルの低い人の影響を全員が受けることになる。更にメンバの中に Antinny 等の情報漏えいを行うウイルスを故意に流布する人がいた場合は更に深刻である。P2P ネットワークでは電子ファイルの柔軟で効率的な交換が可能となる反面、Antinny などのウイルスの除去、つまり一度流通しだした電子ファイルの回収作業が極めて難しい特徴があることに留意しなければならない。

1.2 オーバーレイネットワークとしての P2P ネットワーク

インターネットは多数の ISP が相互接続し一つのネットワークを形成している言わば「相互接続型ネットワーク」である。ある定点からインターネットを見上げると、前述の企業のプライベートネットワークや P2P ネットワークは複数の ISP を跨って構成された「オーバーレイネットワーク」であることに気づく。TCP/IP よりも上位のアプリケーションで構成されたオーバーレイネットワークは、ISP などのネットワーク構成に依存せず、アプリケーション単位に独立した柔軟なネットワーキングが可能となり、今後の多彩なサービス展開が期待されているものの、管理者が存在しない現状の P2P ネットワークには「不正・違法行為等の防止、効率的な通信、通信品質の確保」など、公衆ネットワークとしての基本的な要件を実現するうえでの課題がある。

(1) 不正・違法行為等の防止

インターネットにおける不正・違法行為等の防止には、SPAM メールやウイルス流布、掲示板等での誹謗中傷や違法コンテンツの流通など様々なものがあり、それぞれの不正・違法行為に対して、法制度による規制と ISP やユーザによる対策が行われてきた。

最も積極的な取組みが行われた SPAM メール対策の事例では、まず、SPAM メール等に関するユーザからの苦情に対応する形で、多くの ISP の契約約款に SPAM メール送信者に対する契約解除条項が設けられた。これは一部の ISP の自主規制として始まったものであるが、現在では大半の ISP の契約約款に盛り込まれるようになった。

迷惑メールを規制する法律としては、総務省の「特定電子メールの送信の適正化等に関する法律」(以下特電法)⁵⁵と経済産業省の「特定商取引に関する法律」(特商法)⁵⁶の2つが制定され、「特電法」では平成 17 年に改正され SPAM メールを送信者情報を偽った送信に対して「直罰規定」を導入するなど法制度面でも踏み込んだ取組みを行っている。

更に SPAM メールの技術的対策としては従来の受信メールサーバや受信 PC 端末でのフィ

⁵⁵ 特定電子メールの送信の適正化等に関する法律

http://www.soumu.go.jp/joho_tsusin/top/meiwaku.html

⁵⁶ 特定商取引に関する法律

<http://www.meti.go.jp/policy/consumer/contents1.html>

ルタリング処理だけではなく、ISP のネットワークの相互接続部分で、SPAM メールがよく送られる手法である 25/tcp を使った SMTP 通信を制限する OP25B (Outbound Port 25 Blocking) や IP25B (Inbound Port 25 Blocking) などの対策が採られ、「法・制度・技術的対策・運用」のバランスの良い対策の実装が実現できた好例である。

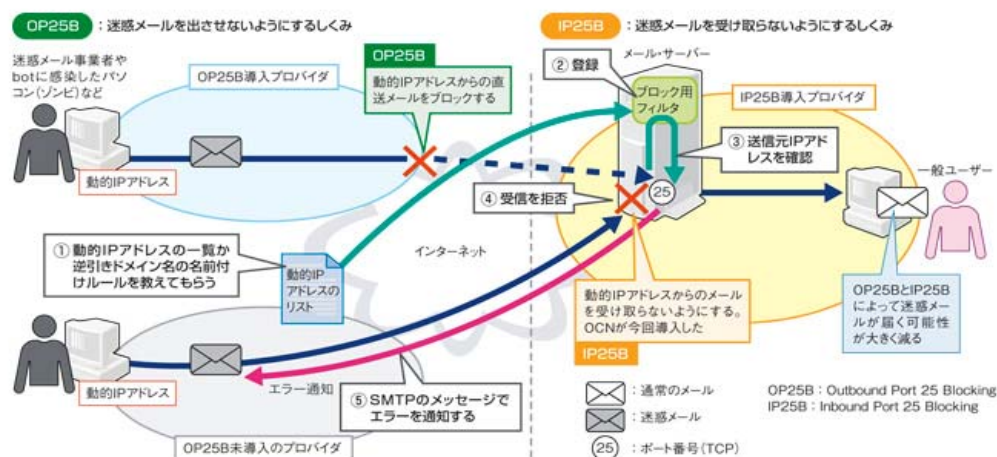


図 付 1.1 OP25B と IP25B の概要 (出展：日経 ITPro)⁵⁷

P2P ネットワークなどの管理者不在のオーバーレイネットワークにおいては、不正・違法行為が横行した場合でも、インターネットで実現できた SPAM メール対策のようなベストプラクティスの再演はかなり難しい状況にある。例えば、P2P ネットワークに対しては電気通信事業法等の法制度が所掌する範囲が明確ではなく、さらに Winny などの P2P ファイル交換ソフトには通信当事者を秘匿する仕掛けが実装されているため、P2P ネットワークのメンバーに対する心理的な抑止力が働きにくくモラルの醸成も困難な状況にある。

また、ISP としても従来の「OP25B/IP25B」などの SPAM メール対策のように ISP 同士の相互接続点で SPAM メールを互いに流通させないような効果的な仕組みを導入するようなことが物理的にも論理的にも困難であり、結果的に P2P アプリケーションを含む全ての通信総量を抑制するような消極的な対策に限られているのが実態である。

(2) 効率的な通信 (通信経路の最適化)

インターネットでは、ISP が自社ネットワーク内部の通信経路を最適化し無駄のない通信を実現しつつ、相互接続先の ISP や他の ISP との通信の最適化を図るため、互いの IP アドレス分布と最適な通信経路を示した経路情報を交換し、インターネット全体の通信の最適

⁵⁷ OP25B と IP25B の概要

<http://itpro.nikkeibp.co.jp/article/COLUMN/20060523/238776/?SS=imgview&FD=-1369990986>

化を図っている。これらは通信先の住所である IP アドレスを教える「DNS」と、早く安くたどり着く道順を教える「BGP-4」などの「ルーティングプロトコル」によって実現している。現在普及しているメールや Web 等の汎用アプリケーションは、DNS の指示した通信先に BGP が教える経路をたどる行儀の良い通信を行うため、ISP もネットワークの構築運用が比較的容易であった。

オーバーレイネットワークは、通信経路の最適化が行われている TCP/IP 通信とはまったく独立したネットワークである。例えば Winny ネットワークにおいて、図らずしもマンションの隣の人と通信している場合でも、実際には地理的にも通信経路的にも遠方にある中継ノードを介してコンテンツのダウンロードを行う場合がある。これは、Winny ネットワーク内部の最適な通信経路が、(当然のことではあるが) ISP 単位に最適化されたトポロジーとはまったく関係なしに決定されるからである。つまり、高性能な PC と早い回線に接続されたノードが近隣のノードのハブ機能を有し通信が集中する。このように、P2P ネットワークとしての効率的な通信とインターネットとしての効率的な通信の経路が一致しないことを想定したネットワーク構築など、ISP が抱える課題は多い。

(3) エンドエンドでの通信品質の確保

通信経路の最適化が難しいと同様の理由で、エンドエンドで通信品質を求めるアプリケーションや利用形態には P2P ネットワークは適さない。

現状多くの ISP は法人向け接続サービスで SLA (Service Level Agreement)「サービス品質保証制度」設けており、回線の最低通信帯域や ISP ネットワーク内の平均遅延時間、故障等による利用不能時間の上限などを定めている。これら SLA はインターネットが通信インフラとして定着した昨今では、最低限の通信品質管理項目とし、更なる厳しい通信品質や運用基準が求められているのが実態である。

しかし、オーバーレイネットワークである P2P ネットワークでは複数の常に ISP に跨って通信が行われているため、上記の「最低通信帯域・平均遅延時間・利用不能時間」などの基本的な通信品質の担保すら難しいのが実態である。また逆説的に言えば現状の品質管理項目をそのまま P2P ネットワーク当てはめることが出来ないため、P2P ネットワークに通信品質を求める場合は、このような実態を踏まえた新たな QoS 技術の開発や実装が求められる。

2 P2P ファイル交換ネットワークの問題点

P2P ネットワークには構造的に「不正・違法行為等の防止、効率的な通信、通信品質の確保」の面で課題があることは前章で述べた。現在の P2P ネットワークではこれらが複雑に絡み合って多くの問題が発生している。

2.1 権利侵害（著作権）

P2P ネットワークでは多くの音楽や映像コンテンツが流通しその大半は著作権侵害に当たるといわれているが全容の解明はできていなかった。平成 18 年 11 月 28 日 ACCS（社団法人コンピュータソフトウェア著作権協会）及び JASRAC（社団法人日本音楽著作権協会）の発表⁵⁸によれば、「ファイル交換ソフト「Winny」ネットワーク上で権利者に無許諾で送信可能な状態に置かれ、流通している音楽ファイル、コンピュータソフトウェア等についての実態調査を実施し、その金額を試算した場合、音楽ファイル 4.4 億円、コンピュータソフトウェア等 95 億円、合計で約 100 億円相当に達する」という。

この実態調査は、「2006 年 10 月 10 日の 18 時から 24 時までの 6 時間について実施し、その結果、少なくとも 21 万ユーザのコンピュータなどでファイル交換ソフト「Winny」が利用されていること、また音楽では 61 万ファイル（1 ファイル当たりの JASRAC 管理楽曲を 7 曲とすれば、月額使用料換算で約 4.4 億円相当）、ビジネスソフトウェア約 61 万タイトル（平均価格換算で約 19.5 億円相当）、ゲームソフトウェア約 117 万タイトル（同約 51.3 億円相当）、アニメーション約 18 万タイトル（同約 17.2 億円相当）コミック約 159 万タイトル（同約 7.0 億円相当）が流通している」ことが確認された。

インターネットが音楽や映像などのデジタルコンテンツの流通基盤として定着している現在において、著作権問題は権利保護の視点だけではなく、インターネットビジネス発展や若年層をはじめとするユーザのモラル醸成の面でも重要な課題である。また、他人の著作物を再配布する行為は犯罪であることを認識しなければならない。

2.2 情報漏えい

Winny ネットワークでは Antinny 等のウイルスが感染した PC の情報を流出させている。多くの個人情報や企業秘密から国家機密に相当するような情報までありとあらゆる情報が流出している。Antinny が猛威を振るいだした 2003 年から 2004 年頃は、不幸にして Antinny に感染したユーザ PC から情報が漏えいしたとして同情する風潮もあったが、その実態が明るみになるにつれ、情報漏えいをした当事者の社会的責任が問われるようになり、多くの企業や中央省庁及び地方公共団体で Winny の利用禁止などの規制措置が取られた。しかし、多くは仕事に使う PC で Winny の利用を禁止するレベルにとどまるなど、対症療法的な対応策が中心となったため、情報漏えい事件は止むことなく継続している。

情報が漏えいした場合の対応策として、漏えいされた当該情報を送信可能な状態にしている PC を突き止め、その IP アドレスとタイムスタンプの情報を元に、ISP に対してプロバ

⁵⁸ ACCS 及び JASRAC の発表

<http://www2.accsjp.or.jp/news/news.html>

イダ責任制限法⁵⁹に基づく、情報の削除依頼や発信者情報開示を行うような動きも一時期活発化した。しかし、一度インターネットに漏えいした情報を 100%回収することは不可能である。

P2P ファイル交換ソフトの利用者は自分自身でリクエストした「情報」に対応し、P2P ネットワークからかき集められた「ファイル」が求めているものかどうかを確認するための選別作業を行う段階で、Antinny 等の情報漏えいを意図して開発されたウイルスに感染する。言い換えれば、音楽や映像ファイルと勘違いし、自ら「情報漏えいソフト」をクリックし実行しているため、自分自身の PC の情報が流出したとしても自業自得ともいえる。しかし、第三者の PC から漏えいした情報に自分や自社の情報が含まれている場合など、第三者に情報漏えいされた被害者の立場や心情は察して余りあるものがあるが、漏えいした情報の回収に関して特効薬は見つかっていないのが実態だ。

2.3 ウイルスの流通

P2P ネットワークは Antinny などの情報漏えいウイルスだけでなくワームやボットなどのウイルスにとっても自分自身を流通させ感染拡大する上で好都合なインフラになりつつある。大別すると、Antinny など Winny ネットワークを感染媒体として利用する P2P ネットワーク特有のウイルスと、P2P ネットワークの利用者が共通して持つ脆弱性を狙うようにして感染拡大するワームやボットなどのウイルスに分けられる。前者はユーザ心理を巧みに突いて PC に侵入する「ソーシャルエンジニアリング」の手法を用いていることに対して、後者は OS の脆弱性や甘いパスワード設定などを突いて侵入する手法を用いていると思われる。

(1) P2P ネットワーク特有のウイルスについて

P2P ネットワークの情報流通は一般的に「情報の検索」と「ファイル転送」の二段階に分けて行われる。情報の検索は情報の所在を管理するインデックスサーバを経由する方法や、ピアツーピアで検索する方法、その両方の特徴を持つ方法などがある。

ファイル転送に関しては、中継するノードが存在する場合もあるが、ファイルの転送そのものはピアツーピアで行われる場合が多い。つまり、取得した電子ファイルが自ら求めたものかどうかなど、情報の中身の確認に関しては信頼のおける第三者が保障するような仕組みはなく、利用者の自己責任となっている。

第三者が情報の中身を確認できる仕組みだけを評価するのであれば、You Tube (ユーチューブ) 等の仕組みが有効である。

P2P ネットワークにウイルスがどれだけ流通しているか調査した結果では、ある条件で絞り込んだファイル群の約 63% が Antinny 等のウイルスだったという報告もある。小山らの

⁵⁹ プロバイダー責任制限法

http://www.soumu.go.jp/joho_tsusin/top/denki_h.html

調査⁶⁰によれば、Winny ネットワークの調査ツールである「Winnybot」を利用して拡張子が「*.exe」のファイルをファイルサイズの小さいものから順に「352」収集し、最新のアンチウイルスソフトでスキャンしたところ、約 63%に相当する「221」がウイルスとして検知されたという。



図 付 1.2 Winny で流通しているウイルス (出展 : 日経 ITPro 小山らの調査)

しかも、拡張子が「*.exe」でありながら多くのファイルのアイコンは音楽ファイルや動画ファイルと同じアイコンに偽装されており、ファイル名も同様に音楽ファイルや動画ファイルを思わせるファイル名が使われていた。おそらく当該ファイルをダウンロードしたユーザは自分がリクエストしたファイルであるか確認するためクリックし、ウイルスを実行している可能性が高い。

P2P ネットワークでは、利用者の性癖とも思える行動特性を巧みに利用したソーシャルエンジニアリングを用いて、効率的にウイルスを配布する行為が行われている可能性が高い。小山らの調査では Winny 利用者の 1 台の PC から最大で、ファイル名もファイルアイコンも音楽ファイルや動画ファイル等に偽装された 128 種類のファイルが発見され、その大半は Antinny 等の情報漏えいウイルスだったことが報告されている。このようにウイルスを音楽ファイルや動画ファイルに偽装し、第三者に対してアップロード可能な状態にしている利用者が存在することを正しく認識した上で適切なセキュリティ対策を行わない限り、情報漏えいは止まることはないと思われる。

⁶⁰ 小山らの調査「Winny ネットワークはやっぱり真っ黒 , NTT コミュニケーションズの小山氏に聞く」

<http://itpro.nikkeibp.co.jp/article/Interview/20070413/268234/>

(2) P2Pネットワークの利用者が共通して持つ脆弱性を狙うウイルス

P2P ネットワークの利用者は、効率的にファイル交換を行うため、PC やネットワーク環境の設定変更を行っている。その結果、ボットやワームなどのウイルスに感染しやすくなることから、非常に危険な状態に置かれている。

ア ブロードバンドルータの設定

昨今のブロードバンド環境では、ADSL モデムや光終端装置とブロードバンドルータがセットになって、ISP から提供されている。通常ブロードバンドルータには WAN 側と LAN 側で異なる IP アドレスを割り当てて、アドレス変換を行う IP マスカレード機能により、外側から内側の IP アドレスを直接見せずに通信を行う仕組みが実装されている。WAN 側インターフェイスには ISP から割り当てられたグローバルアドレスが、LAN 側インターフェイスには 192.168.0.1 などのプライベートアドレスが割り当てられる。

この機能により、ブロードバンドルータの内側にある PC には、インターネットからの攻撃があった場合でも直撃を免れることが可能となる。つまり、インターネットからの攻撃は WAN 側インターフェイスに割り当てられたグローバルアドレスまでは到着し、ブロードバンドルータは攻撃を受けることになるが、プライベートアドレスが割り当てられた PC には外からの攻撃は届かない。まさに簡易なファイアウォールとして機能している。

このような簡易ファイアウォール機能は、Web サーバなどをインターネットに公開するような利用形態では不十分であるが、外からの通信を単純に防止するだけの目的であれば必要十分な機能を発揮する。

例えばインターネットに直接接続して OS のアップデートを行う場合、アップデートに必要な数分間という短い時間であっても、以前の OS のバージョンに含まれていた脆弱性等を突く攻撃に遭遇しボット等のウイルスに感染してしまう。しかし、PC をインターネットに直接接続せず、ブロードバンドルータの内側に接続するだけで、インターネットから攻撃を避けて安全に OS のアップデートを行うことが出来る。

P2P ネットワークのメンバはメンバ間でフルメッシュの通信を行うことから、非常に多くの TCP ポートを開放している場合が多い。また第三者からのリクエストに応じて、ファイルをアップロードするためには、外部から接続要求してきた通信に対する通信路を確保する必要があるため、PC をインターネットに直接接続するか、ブロードバンドルータ等を導入している場合でも、インターネットからの通信がブロードバンドルータの内側の PC に直接届くような設定にしていることが多いと思われる。また近年のネットワーク機器の多くは UPnP (ユニバーサルプラグアンドプレイ) を採用しているため、ユーザが意識しない状態で、アプリケーションが使用するポートをインターネ

ットに向けて開放されている場合も考えられ、一般的なインターネットユーザと比較して非常に危険な状態でインターネットに接続している。

イ ウイルス対策ソフトの設定

P2P ファイル交換ソフトでリクエストしたファイルをダウンロード中に、ウイルス対策ソフトのパターンファイルに合致するファイルがあると、自動的に通信が遮断され、その後のファイルがダウンロードされない場合がある。このため P2P ファイル交換ソフトのユーザは、ウイルス対策ソフトの動作を止めているかインストールしていない場合があると言われている。

前述のとおり、P2P ネットワークには大量のウイルスが故意にばら撒かれている可能性があり、且つ、P2P ネットワークで流通しているウイルスは、相対的にウイルス対策ソフトのパターンファイルに反映されていないため、最新のパターンファイルを反映したウイルス対策ソフトを利用していても安心できるとは言いがたい状況にある。

また、P2P ファイル交換ソフトを利用していない場合でも、ブロードバンドルータ等の甘い設定で、インターネットからの攻撃の直撃を受ける可能性が高いことは既に述べたとおりである。このような場合でもウイルス対策ソフトを最新の状態にしていれば、既知の攻撃や感染手法の場合は感染や被害を免れることが出来るが、ウイルス対策ソフトの導入や更新を怠った場合はボットやワーム等に感染してしまう可能性が高い。

ウ OSのアップデート（セキュリティパッチの適用）

P2P ファイル交換ソフトのユーザは先にも述べたとおり、ファイル交換の効率性を高めるための設定を PC やブロードバンドルータに施している。Windows 等の OS はセキュリティパッチ等を更新すると自動的に再起動を行う場合がある。この場合、ダウンロード作業は中断されるため、OS のセキュリティ更新すら止めているユーザが存在する。

このように P2P ファイル交換ソフトの効率化を高めるためには、基本的なセキュリティ設定を全て無視し、自らの PC を危険にさらす実態がある。近年、ボットネットの脅威が叫ばれているが、P2P ネットワークが共通して持つ脆弱性はボットネットなどのウイルス感染の温床と考えられており、既にインターネットの大きなリスクになっている。

P2P ファイル交換ソフトのヘビーユーザの中にはこのようなリスクを承知した上で、P2P ファイル交換ソフト専用 PC を用意してファイル交換を行うような事例もあるという。P2P ファイル交換ソフト専用端末であれば、ウイルスに感染しようが、情報漏えいしようが、本人は痛くも痒くもないかもしれないが、同じブロードバンドルータに接続した別の PC や、インターネットの他の PC などに対する影響を考慮する必要がある。

3 P2Pネットワークがインターネットに及ぼす影響

P2P ネットワークは、TCP/IP 層での通信経路の最適化を行うインターネットとは独立したアプリケーション単位に構成されたネットワークの最適化ポリシーによって、その通信経路が決定されるオーバーレイネットワークである。情報転送効率だけを見ればメールや Web アクセスと比較してインターネットに対して高い負荷を与える利用形態である。

このようなインターネットに優しくない P2P ネットワークが発展をなしえた背景には、多少の非効率な通信が気にならないほど大容量化したブロードバンドインターネットが、定額制常時接続サービスとして普及したことが挙げられる。まさに、P2P 技術はブロードバンド大国と呼ばれるまでに成長した我が国のインターネットの将来に大きな影響を与えうるアプリケーションを支えうる技術なのである。本章では P2P ネットワークがインターネットに与えた影響などを紹介する。

3.1 大量の通信

1965 年に Intel の共同創業者 Gordon Moore は、チップ上のトランジスタの数は 2 年で倍増すると予測した。俗に言う「ムーアの法則」である。IT 産業は「ムーアの法則」を裏付けるように、高性能・高機能化路線を走り続けた。インターネット業界も同様にバックボーン回線を高速広帯域化し、爆発的に加速するブロードバンド化を支えた。

我が国に商用プロバイダサービスが登場した 1990 年代の前半から、一般家庭にもインターネットの普及が始まった 90 年代の後半にかけての期間を「黎明期」とし、ADSL 等のブロードバンドインターネットが普及した 2001 年から 2005 年が「成長期」そして Web2.0 や SNS など 2005 年以降を「発展期」と仮に名づけ、インターネットのトラフィック変動を見てみたい。ただし、インターネットのトラフィック変動のデータは全て同じ測定点で得たものではないので、相対的な変化を理解する参考としてご覧いただきたい。

(1) トラフィックの成長

多くの ISP がトラフィックの相互流通基盤として活用している JPIX の公開データから、インターネットの過去と現在を調べてみた。インターネットの「黎明期」である 1998 年のデータ(図.3)では、一日の最大トラフィックは 23 時~24 時頃で約 100Mbps、最低トラフィックは早朝 6 時頃で約 30Mbps となっている。いまでは家庭のインターネットでも同等のスループットが出せることを考えると隔世の感がある。1998 年から 8 年後の 2006 年のデータ(図.3)では、一日のトラフィック変動のパターンはほとんど同じで、深夜帯に最大トラフィックが発生し、早朝にトラフィックが最低値を記録している。また、特徴的なのは昼休みの時間帯にトラフィックの盛り上がりが見られることまで含めて傾向は似ている。

大きく異なることはトラフィックの総量である。最大トラフィックは約 65Gbps、最低トラフィックは 30Gbps であり、最低トラフィックの伸びは 8 年間で約 1000 倍となっている。早朝の時間帯のトラフィックはユーザ自身がインターネットアクセスしているのではなく、

自動的なファイル転送やクロージングなどの機械検索処理などの通信、企業のデータ転送などが多いといわれている。この底溜まりとも言えるトラフィックの大半は P2P ネットワークによるものといわれている。

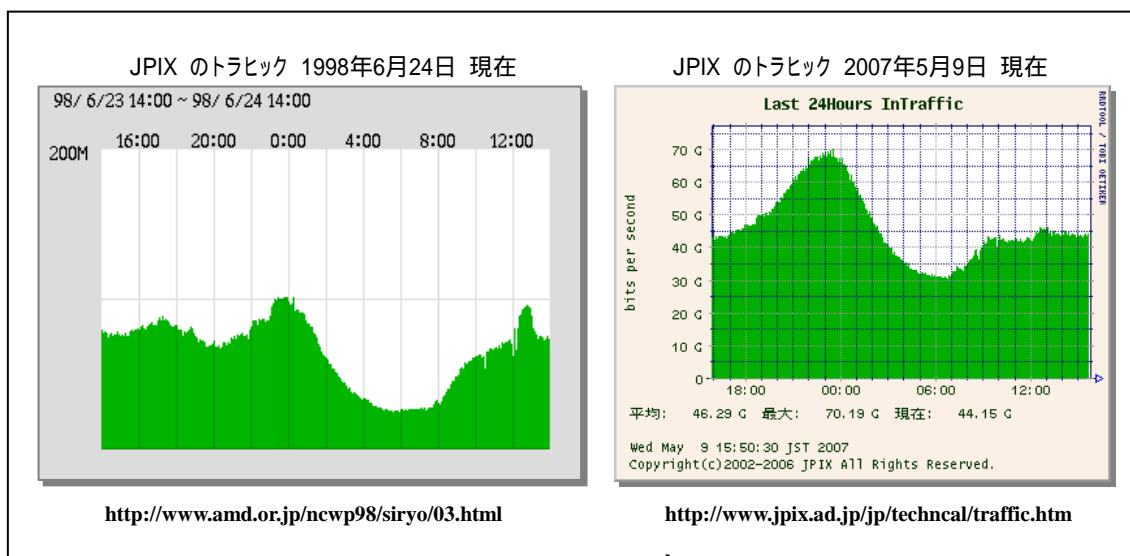


図 付 1.3 JPIX のトラフィックの変化

(2) トラフィックパターンの変化

総務省「次世代 IP インフラ研究会 第一次報告書 2004 年 6 月 7 日」⁶¹によれば、「約 1 割の利用者が全体の 8 割の回線容量を占有」し、「P2P ファイル交換によるトラフィックが大宗を占める」とある。また、福田ら⁶²によれば「約 4%の特定のユーザが全体の 99%のトラフィックを発生させる」と同様の報告もあるとおり、インターネットが一部のヘビーユーザのトラフィックに占有されていることが伺える。そもそもインターネットは「ベストエフォート」であり、繋がらない又は遅いこともあることが前提で設計されている。言い換えれば ISP の契約者が全員同時に契約回線容量一杯の通信を行うことは物理的に出来ないのが実態である。インターネットの定額制は「使いたい放題」ではなく「使ったもの勝ち」の状態を作り出した。しかもそのトラフィックの大半は P2P ネットワークである。

次世代 IP インフラ研究会の報告書によれば、インターネットの「成長期」において、ユ

⁶¹ 次世代 IP インフラ研究会 第一次報告書

http://www.soumu.go.jp/s-news/2005/050707_2.html

⁶² 福田らの調査 The Impact of Residential Broadband Trafficon Japanese ISP Backbones

<http://portal.acm.org/citation.cfm?id=1052812.1052820>

ーザのトラフィックパターンに大きな変化が起きている。

あるISPにおけるトラフィック・パターンの変化

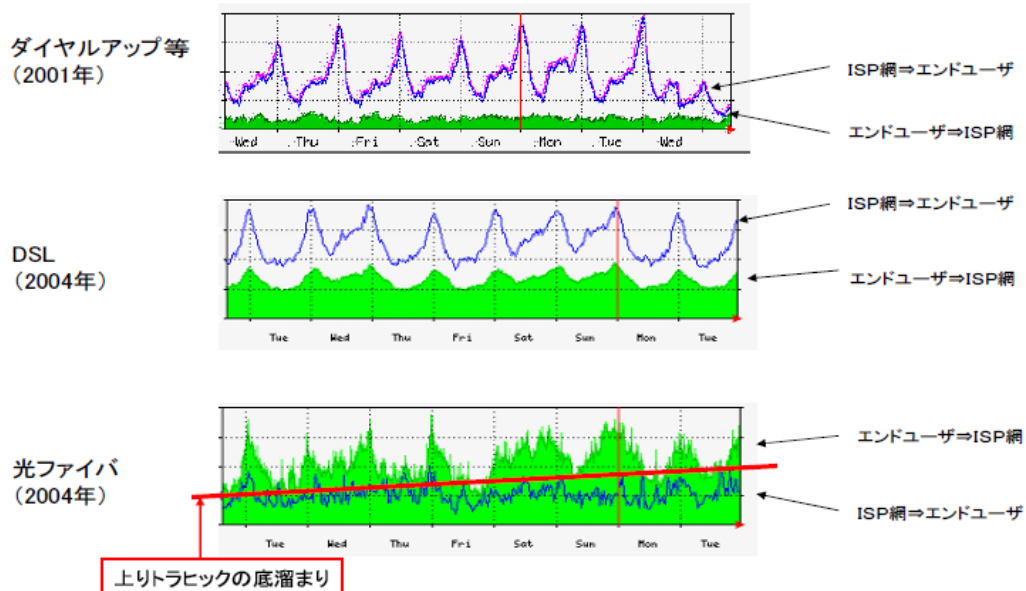


図 付 1.4 ある ISP におけるトラフィック・パターンの変化

2001 年の時点で主流であったダイヤルアップユーザのトラフィックパターンは、ユーザがインターネットにアクセスしてメールや Web コンテンツを PC にダウンロードする「下りトラフィック」が、ユーザがメール送信や Web の情報発信を行うような、インターネットに情報をアップロードする「上りトラフィック」を大きく上回っている。ダイヤルアップ等の narrow-band インターネットでは当然のトラフィックパターンであるが、2004 年の DSL 利用者のトラフィックでは大きな傾向に変化はないものの「上りトラフィック」が相対的に増加していることが見て取れる。

DSL の多くは「ADSL (Asymmetric Digital Subscriber Line)」に代表されるように、下りが速く上りが遅い非対称の通信速度をもつ回線サービスを ISP へのアクセスラインに利用している。したがって、もともと下りの帯域を上りが上回ることがない設計にも係わらず、2001 年のダイヤルアップ等のトラフィックと比較して、上りが相対的に増加している。この要因は P2P ネットワークにおいて、音楽や動画などのリッチコンテンツのファイル交換が加速化したのではないかと考えられている。

また同時期の「光ファイバ」のトラフィックは更に特徴的な傾向が出ている。上りトラフィックが下りを上回っているのである。Winny ネットワークなどでは Winny がインストールされたノードが接続された PC 環境や回線環境の性能によって「スーパーノード」と呼ばれるコンテンツの集積拠点が作り出され、そのスーパーノードに対してトラフィックが集

中することもあるという。また猥褻な動画配信サイトなども同様に上りのトラフィックが伸張する要因だと思われる。

(3) ユーザ通信の中身

総務省「2007年4月24日 ネットワークの中立性に関する懇談会/P2P /P2P-WG」⁶³によれば、NTT が提供するアクセス回線サービス「フレッツサービス」の大半は P2P トラフィックであると推測したデータが提出されている。

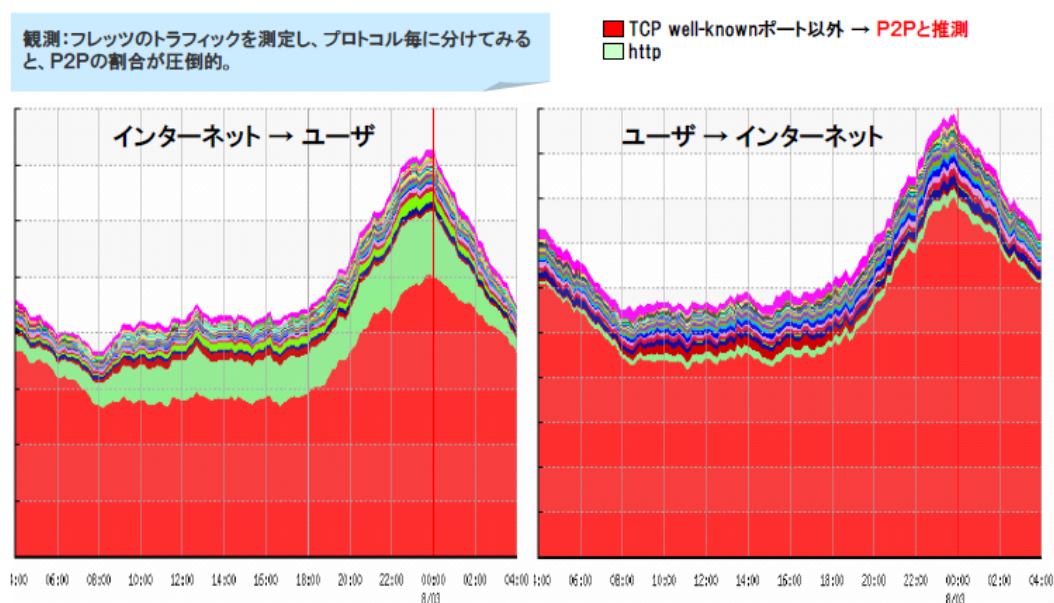


図 付 1.5 プロトコル別の終日トラフィックトラフィック変化（フレッツの例）

P2P ネットワークと無関係なユーザにとっては理解しがたいデータだが、ごく一部の P2P ユーザがインターネットを独り占めしている状況がうかがえる。

4 今後期待すること

P2P 技術はブロードバンドインターネットに相応しい新しい可能性を秘めている。P2P ネットワークと、インターネットのアーキテクチャやトポロジーとの親和性に関する課題は、インターネットの成長期には盛んに議論されたが、現在ではインターネットの伝送能力に関する技術革新や、各 ISP の努力もあって大きな山は越えた感がある。インターネットは今後も多種多様なアプリケーションが登場し、多種多様なオーバーレイネットワークが縦横無尽に張り巡らされていけよう。インターネットは、P2P ネットワークなどの個別の

⁶³ ネットワークの中立性に関する懇談会/P2P /P2P-WG

http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/network_churitsu/index.html

アプリケーションに最適化するのではなく、今まで以上に「高速大容量な土管」として「ユーザ通信を速く安く確実に伝達する役割」の重要性がますます高まっている。

快適で便利になったインターネットに「陰の部分」があるとすれば、その代表格は P2P ネットワークではないだろうか。現実社会では犯罪とされる「著作権侵害コンテンツの流通」行為や、現行法では取り締まることが難しい「ウイルス作成や配布」が、なかば公然と行われている。このような状況を打開し、安全で安心なインターネットを実現していくことが、インターネットに係わる全ての関係者に与えられた課題である。インターネットが生活に欠かせないインフラとなった現在では、インターネットに深く係わる ISP や IT 業界や PC メーカー等の専門的な立場の人々だけでなく、一般家庭の利用者も自分や家族の問題として認識し取り組んでいただきたい。

付録2 Winnny ネットワークの特性および情報漏えい

対応に影響を与える特殊性について

本報告書において、Winnny 等における情報漏えい対応については、その特殊性に応じて、考察すべき事情があるということがたびたび報告されている。そのような特殊性として論じられている点については、以下のような Winnny ネットワークの技術的・実的な事実関係が影響を与えている。そのような影響を与えている事情について、委員会において、Winnny ネットワークにおける情報漏えい事件対応をその業務の一つとして行っているネットエージェント株式会社に対するヒアリングの結果等をもとにしてまとめると以下のとおりである。

1 Winnny の概念

1.1 Winnny プログラムとは

ソフトウェアとしての Winnny は、「匿名性」「共有効率の高さ」を目的として Windows ネイティブプログラムとして開発された P2P ファイル交換ソフトである。中央サーバの存在を必要としない、いわゆるピア P2P 型のソフトウェアであり「プロクシー技術」を「匿名機構」「キャッシュ機構」として活用することにより、匿名性・効率的なファイル交換を図ろうとしたものである。

1.2 Winnny の匿名性について

一般に Winnny ネットワークにおいては、匿名性があり、情報の第一発信者がわからないとされている。Winnny においては、あるファイルがアップロードされるとそのファイルの位置情報等が要約されたキーが作成され、これがインターネット上の一定の範囲内にある他の PC に拡散し、そのファイルをダウンロードしたい他の Winnny 利用者は、ファイル検索によってそのキーから当該ファイルの位置情報を取得し、この情報に基づいてファイルの送受信がなされる。また、このキーは一定の割合で書き換えがなされ、書き換えられたキーをもとにダウンロードが実行されると、もともと当該ファイルのあった PC とは別の PC にファイルが複製され、この複製されたファイルがさらにダウンロードされる。このような中継機能によって当該ファイル情報の一次的発信者が誰であるのかが判別できなくすることを目的としている。

もっとも、聴取によれば、Winnny クライアントの処理を追いかけていき、パケットを解析しつつ、試行錯誤してデータを逆アセンブルしていくことにより、Winnny の暗号化解読することができ、その結果、1年分の接続者情報（Winnny ネットワークに接続している者の IP アドレス、ポート番号、キー等）を解明して、保有することができたとしている。その意

味で、「匿名性は、ないといいきってもいいだろう。」という認識をしているとのことであった。

1.3 Winnyの効率性について

Winny においてはファイル検索等の効率性を図るために、同じ嗜好性のある PC 同士をネットワーク上の概念的に近い場所に置くクラスタリングという方法が採用され、またファイルの送受信の効率性を図るために、一つのファイルがアップロードされると、当該ファイルは一定の大きさに分割されたキャッシュファイルに断片化されて、ファイルの転送はこのキャッシュファイルがブロックごとに転送される仕組みとなっている。また、それら以外にも、同じファイルを有する複数の PC からファイルが同時にダウンロードされる多重ダウンロード機能や、ダウンロードの再開が自動化できる自動ダウンロード機構等が備わっている。

2 Winny ネットワークの実態および特性

2.1 Winny ネットワークとは

Winny プログラムを利用しているコンピュータをノードと呼ぶが、各ノードは、近隣のいくつかのノードを認識し、通信している。しかしながら、実際にインターネットを使って多数接続して、他のノードの情報やファイルの所在を交換しながらファイルの検索や転送を可能にしている。各ノードがインターネットを介して接続し、形成しているネットワークを Winny ネットワークと呼ぶ。

Winny ネットワークを流れる通信内容・変容性およびその利用者における特定の利用方法については、留意しておくべき事実であるといえる。

2.2 Winny ネットワークにおける通信内容

一般的なファイル交換ソフトの利用状況についての調査については、「付録 1 Winny(P2P ネットワーク)とインターネットの関係」の「2.2」を参照のこと。

2.3 Winny ネットワークの変容性

Winny の各ノードは、キャッシュという形で記録されているキーやファイルが記録領域がいっぱいになった段階で、消去される。一般の状況において、こういった消去が行われるには、1 週間もかからないものと思慮される。このような要素があるために、Winny ネットワークで通信されるファイルの特定の内容については、1 週間程度できわめて変容してしまうといえる。多数の人間に興味をもたれてダウンロードされないかぎり、自然消滅してしまうことも良くあるのである。その意味で、Winny ネットワークにおいて通信される内容は、変容するものであるということが出来る。

2.4 漏えい情報収集家(コレクター)の存在

聴取によれば、Winny ネットワークにおいては、情報漏えい事件などで流出したファイルを特に目的としてダウンロードするのを指向するユーザが存在するとのことである。そのようなユーザを、便宜上、コレクターと表現する。コレクターについては、およそ人数と

して1000人であると考えられ、ほとんどが趣味でそういったファイルをダウンロードしているものと思われる。もっとも特定のユーザにおいては、大量のデータをかかえこんで(1万件)アップロード状態になっているものもいる。また、まれな例としては、かかるデータを抱え込んでいて、情報主体・被害企業等から情報について消去等の要求があった際に、金銭の要求をするユーザも存在するとのことであった。

3 Winnyネットワークの特性が情報漏えい対応に与える影響

3.1 Winnyネットワークにおける流出情報

Winnyネットワークにおいて特定の情報については、上記の理由により、変容性があるため、場合によっては、何らの措置をなさないでも、自然に消滅してしまうという特性がある。もっとも、これは、比較的少数のコンピュータに保存されていたにすぎない場合ということがいえる。これに対して、匿名掲示板等で話題になった場合には、数十人にダウンロードされてしまうことになる。そのような場合には、Winnyネットワークにおいて、上記コレクター等にもダウンロードされてしまいそのまま消滅することを期待するのは困難な状況になる。

3.2 Winnyネットワークにおける流出情報対応について

聴取によれば、いわゆる暴露ウイルスにより、機密性のある情報が、Winnyネットワークに流出してしまった場合における標準的な対処法のポイントとしては、以下のようなものがあるとされる。

(1) 現状把握

上記Winnyネットワークの性質からいって、まず、現状において、当該流出情報が、Winnyネットワークにおいて、どのくらいの程度保有されているかといことを把握することが、初動のステップの目標ということになる。

もっとも、事件においては、漏えいした情報じたいについて、その内容を確認する必要がでてくる。しかしながら、この場合、流出に関与した企業等が、その流出の可能性を認知したことをもって、みずからWinnyネットワークで、そのファイルの存在を確認しようとすることは逆効果となり、Winnyネットワークに当該ファイルの基本要素が記載されたキーを拡散することになることに留意すべきである。したがって、新たな検索・ダウンロード行為をなさずに、その漏えい情報を確認するような形で事実確認を図るような手法が望ましい。

(2) 流出規模ごとの対応

ア ごく少数のWinnyノードにダウンロードされている場合

この場合は、上述のようなWinnyネットワークの性質から、自然消滅という蓋然性がかなりの程度ある。

なお、聴取によれば、Winnyノードがいわゆるコレクターのブラックリストにのっているような場合、そういった保有者の行動が予測することができ、それに応じた対応

が可能であるとのことである。内容証明郵便等により削除を依頼することで消去されることもありうるだろうとのことであった。

イ ある程度のWinnyノードにダウンロードされている場合

これらのWinnyノードの発信者を特定する必要がでてくる。発信者を特定することができれば、状況によっては、消去依頼や内容証明郵便などでの通知を行うことができる。

聴取によれば、発信者の特定にあたっては、発信者情報開示の手段を用いることがあるが、ただし、手続きが大変であるということである。また、場合によっては、プロバイダ経由でファイル所有者に対する消去願いを行うこともあるが、実効性については、種々の問題があるとされている。その上に、内容証明郵便などで、保有者に連絡した場合に、逆に匿名掲示板などに、当該ファイルの存在などを記載されることがあり、その場合は、逆効果になるとのことであった。

(3) 関連事項

聴取によれば、現在では、拡散防止サービスという形のサービスを提供しており、当該サービスの効果がでてきており、また、リスクも少ないとのことであった。

3.3 漏えい対応における特殊事情

Winny漏えい事件においては、従業員がその家庭で利用している私物のPCでWinnyを利用し、そのPCが暴露ウイルスに感染して、仕事で利用していたデータがWinnyネットワークに流出するという事案が多い。そのような場合においては、特に、如何にデータに変更をくわえずに、また、後に証拠としての信用性をできるだけ確保したままで、従業員の私物を証拠として確保するかということが問題になる。この点については、「付録4 Winnyをめぐる法律問題の概観」の「3 Winnyネットワークによる情報漏えい対応および防止のための法律問題」参照のこと。

4 Winny漏えい対策について

4.1 Winny漏えい対策の傾向

Winny漏えい対策については、種々の対策がとられている。現時点においては、Antinnyによる情報漏えいが一般的な問題となっているので、所属機関が責任をもって、漏えいを防止する責任があるということの認識にいたっているものと思われる。

そのような対応の具体例の一例として自衛隊における対応を参照するとき、まず、緊急の対応として、(1)職務上使用する私用PCについてファイル交換ソフトの削除を確認、(2)私有PCに保存されている業務用データについて秘密の情報および必要のないデータの削除などが行われた。その後、抜本的な対策として、1)私有PCの一掃、2)可搬記憶媒体のデータの暗号化等、3)ネットワークを通じた情報流出防止、4)シンクライアントシステム等の導入、5)新たなOSの検討、6)サイバー攻撃を含む各種情報流出要因等への対策など

が実施に移されている。

また、自宅での仕事はしないという形で根本的に組織の従業員等の仕事に対する認識・姿勢等から根本的に見直して対策する方向に向かっている組織も存在している。

4.2 現時点における対応策の限界

もっとも、現時点における対応策についても限界が存在している。聴取によれば、特に過去対策が十分ではないということがいえる。誓約書を記載して情報の持ち出しを禁止するという対応がなされているが、いままでに持ち出した PC に保存されている業務情報についての洗い出しが十分ではないのではないかということである。過去の業務に関連する情報をすべて消すように強調しているとのことである。

また、企業が、従業員から誓約書をとって Winny の使用を禁止したとして、子供が興味半分から Winny を使用していることが多く、企業としては子供から誓約書をとるわけにはいかない所以对策が十分に行き届かないところがあるとのことであった。

付録3 Winnnyトラフィックの制限と通信の秘密

序

Winnny 被害報道が相次いでいた平成 18 年 3 月 16 日に大手インターネット接続事業者である株式会社ぷららネットワークス（以下、ぷららという）が、通信の外形からファイル交換ソフト「Winnny」の通信を遮断する措置を同年 5 月をめどに開始する予定であるとのニュースリリースを発表した。しかしながら、ぷららネットワークスのこの決定に対して、総務省は、この措置は、「通信の秘密に抵触する可能性が高い」との見解をしめしたために、ぷららは、ユーザの希望により、Winnny 通信を遮断するサービスの提供をするか否かを選択しうる形にして、Winnny 遮断のサービスを提供することとなった。これらの問題の経緯を、ぷららネットワークスおよび総務省・消費者行政課へのヒアリングなどの結果をも踏まえて整理すると以下ようになる。

1 3 月 16 日のプレスリリースに至る経緯

ぷららは、上記のように平成 18 年 3 月 16 日、通信の外形からファイル交換ソフト「Winnny」の通信を遮断する措置を採用することを発表した⁶⁴。これは、従来からの既存の仕組みを流用すれば、Winnny の通信を遮断できるのではないかという考え方にもとづくものであった。従来からの仕組みというのは、もともと、平成 14 年 12 月の会員規約改定により、平均トラフィックを大幅に超えるユーザについては、事後的に個別対処する試みをおこなっており、さらに平成 15 年 10 月には、Win-MX や Winnny などのアプリケーションを用いている場合に、他の会員の迷惑にならないレベルまでトラフィックの制御を行っていくことにしていた⁶⁵。これは、その当時においても、著作権を侵害する形で送信されている音楽データ・映像データが、大量に送信・受信されており、ネットワーク自体のかなりの帯域を占有されてしまうという状況が発生していたのである。特定のユーザが、6 割ないし 8 割の帯域

⁶⁴ 「ぷららバックボーンにおける「Winnny」の通信規制について」

この内容は、「昨今、ウイルスに感染した PC から「Winnny」を介した、意図せぬ個人情報または機密情報の流出が相次いでおります。こうした社会問題を憂慮すべき事態と捉え、皆様に安心してご利用いただけるネットワーク環境を提供することが通信事業者としての責務であるとの考えから検討を行ってまいりましたが、「Winnny」による通信を完全に規制する決定をいたしました」というものである。

(http://www.plala.or.jp/access/living/releases/nr06_mar/0060316_2.html)

⁶⁵ 「B フレッツ値下げ、ぷららフォン for フレッツ特割の開始、及トラフィック制御の開始について」(http://www.plala.or.jp/access/topics/03_oct/20031020.html)

を占有していたのである。この点についての詳細は、「付録1」の「3 P2Pネットワークがインターネットにおよぼす影響」を参照のこと。

このような状況を解決する方法としては、帯域を増強するか、P2Pの帯域を制限するか方法はなかったのであり、そのような状況のもとで、もともと、一定のトラフィックの制限がなされていたわけである。

このような帯域の圧迫状況は、平成18年にいたるまで改善するばかりか、さらに顕著になってきた。その上、情報漏えいがかかり問題になってきて、ぶららとしても、そのような状況を看過するわけにはいかなくなっていたのである。

ぶららとしても、いうまでもなく、ユーザが、違法な公衆送信等をおこなわないことで、健全なネットワークが構築されるのであれば、それが望ましいことであることは認識していたのであるが、アプリケーションに対応して、通信を制限するシステムを導入することによって、Winnyの通信の遮断をはたすのが、望ましいもの⁶⁶と決断した。

この通信を制限することのできるシステムというのは、シスコ社のサービスコントロールエンジンであり、これの基本的な機能として、加入者ごとの識別をしながら、アプリケーションレベルでパケットを制御することが可能な点に特徴⁶⁷がある。ぶららとしても、従来からアプリケーションも考慮した形で通信を制限しているわけであり、この制限に関する設定のレベルをあげたとしても、問題はおきないものと認識していたのである。また、いうまでもなく、通常の通信を誤認識して、遮断してしまうことがないように、技術的な実証実験を繰り返しており、実用性として問題がないと認識していた。

ぶららとしても、会社の方針として、著作物について違法な公衆送信されているデータ

⁶⁶ さらに、アプリケーションを考慮して、制御する方式には、フロー・ステート・コントロール方式、ディープ・パケット・インスペクション方式の二つの種類があるという。詳しくは、「ぶららのWinny遮断は是か非か（前編）」

(<http://itpro.nikkeibp.co.jp/article/OPINION/20060424/236095/>) 参照のこと。

なお、厳密には、このシステムが、通信の内容まで踏み込んでアプリケーションを識別しているのかという問題があるが、その点については、今後の検討課題ということになる。

⁶⁷シスコ社の説明によれば、「Cisco SCE 2000 シリーズは、パケットを個別のイベントとして処理するのではなく、アプリケーション フローごとに個別のトラフィック フローおよびレイヤ 7 ステートを完全に再構築します。」とのことである

(http://www.cisco.com/japanese/warp/public/3/jp/product/hs/sce/sce2000/prodlit/sce2000_ds.shtml)

<http://www.cisco.com/japanese/warp/public/3/jp/news/pr/2005/038.shtml>

http://www.cisco.com/japanese/warp/public/3/jp/solution/casestudy/pdf/2005/plala_050801.pdf

についてこれを運ぶべきものではないと認識していたこともあり、上記プレスリリースにいたることとなった。そして、ニュースリリースに対する反応も、ぷららの認識では、ぷららに好意的なものであった。

2 「通信の秘密」との関係

総務省としては、ニュースの報道等などから、「通信の秘密」等との問題があるのではないかと認識して、具体的な説明を聞くことになった。総務省としても、ぷららの通信規制について具体的な手法についての確認をしないと「通信の秘密」等との関係で、問題が発生するのかどうかという認識ができなかったのである。そのために数度、説明を求めたことがあった。説明を受け、総務省としては、内部的にも検討し、通信の秘密との関係で、問題がある可能性があるという結論に達した。そして、通信の秘密にふれざるをえず、正当業務行為として許容されるものでなければ、そのような手法による通信規制は、許容されないということとなった。

ここで、「通信の秘密」が問題となってくる。「電気通信事業法」は、その第4条で、(秘密の保護)として、第1項では、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」と定め、また、第2項では、「電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」と定めている。また、第179条においては、「電気通信事業者の取扱中に係る通信(第一六四条第二項に規定する通信を含む。)の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。」として刑事罰が定められている。そして「電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する」とされているところである。そして、「通信の秘密」の保護する範囲については、通信の内容にとどまらず、発信人・受信人それぞれの氏名・住所はもとより、通信の日時や、電信・電話の差し出し個数など通信にかかわるすべての事実及ぶことになる。これらの規定は、電気通信法制研究会「逐条解説 電気通信事業法」(以下、「逐条解説電気通信事業法」という)⁶⁸によると、電気通信事業者の取扱中にかかる通信については、いったん通信当事者の手から離れ、事業者に託されたものであるから、通信当事者が秘密を保護するための自衛措置を講ずる余地がなく、また、秘密が侵害される危険にさらされやすいことにかんがみ、電気通信事業に対する利用者の信頼を保護するため、その秘密を侵すことを禁止しているのとされている。

そして、ぷららが行った通信の遮断行為については、通信のパターン、パケットの制御情報などの通信の内容に関わらない情報⁶⁹を判断の基本的な根拠にして、通信の遮断の是非

⁶⁸ 電気通信法制研究会「逐条解説 電気通信事業法」(第一法規、1987)

⁶⁹ 通信の内容以外の「発信人・受信人それぞれの氏名・住所はもとより、通信の日時や、電信・電話の差し出し個数など通信にかかわるすべての事実」である。通信パターン、パケットの制御

を判断している点が問題になってくるのである。仮に、通信の内容によらない情報から、Winny 通信であると判断して、通信を規制するとしたとしても、電気通信事業法に定める「通信の秘密」との関係では、通信の内容にかかわらない事実も「通信の構成要素であり、電気通信事業法第 4 条第 1 項の通信の秘密として保護される。」ことになる⁷⁰。したがって、これを記録し、それをもとに通信規制をすることも通信の秘密の侵害に該当し得る。ある意味でインターネット・サービス・プロバイダ自体は、違法性阻却事由のなかでしか日常の活動ができない状況に陥っているのである。また、何が、この正当業務行為として違法性が阻却される場合ということができるかどうかという点については、必ずしも明確ではない部分もあった。違法性阻却事由については、「電気通信事業における個人情報保護に関するガイドライン」は、「課金、料金請求、苦情対応、自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合には正当業務行為として少なくとも違法性が阻却されると考えられる。」としており（同ガイドライン 2 3 条解説）、また、DoS 攻撃、DDoS 等のサイバー攻撃、ワームの伝染、迷惑メールの大量送信及び壊れたパケット等が送信されている場合には、一定の行為は、やはり違法性阻却事由があり許容されるものと考えられる⁷²。が、その一方で、その伝送するコンテンツが、違法に複製されたものが一般であるとか、それを発信もしくは受信することが法に触れるということから、それを通信規制できるかという問題は別である。このような枠組みで考える限り、そのコンテンツに注目して、通信規制をなすということについて、なんらかの違法性阻却事由があるといえるかは、困難なものがある。

情報などをも含む。サイバー犯罪条約（第 1 条）によるとトラフィック・データという用語が用いられる（<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>）。但し、トラフィック・データという用語は、個別の通信の要素を捨象したトラフィック全体の傾向などに関するデータをさすという場合に使われることもある。

⁷⁰ 「電気通信事業における個人情報保護に関するガイドライン」（平成 16 年 8 月 31 日総務省告示第 695 号）http://www.soumu.go.jp/joho_tsusin/d_syohi/d_guide_05.html

⁷¹ 電気通信事業における個人情報保護に関するガイドライン（平成 16 年総務省告示第 695 号。最終改正平成 17 年総務省告示 1176 号）の解説

http://www.soumu.go.jp/joho_tsusin/d_syohi/pdf/051018_2.pdf

特にその 23 条の解説部分。

⁷² この点については「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（第 1 版）」（社団法人日本インターネットプロバイダー協会 社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本ケーブルテレビ連盟）（http://www.jaipa.or.jp/info/2007/info_070530.html）が一つの回答を示すにいたり、きわめて注目に値する

総務省としては、ぷららの通信規制が、具体的なアプリケーションの通信の状況を判断し、そして、その判断について通信の内容によらない情報といえども通信を構成する要素の情報を利用して Winny に特徴的な要素をそなえたと判断し、それについてその通信を規制するものである以上、「通信の秘密」を侵害するものと解さざるを得ず、そして、その行為の違法性を阻却する事由に該当するような具体的な事実も認識されなかったということになる。

3 その後のぷららの対応

結局、上記のような総務省の見解を受けて⁷³、ぷららとしては、顧客からの具体的な同意をとりながら、Winny 通信を遮断することにした⁷⁴。具体的な手法としては、新規加入者については、Winny 遮断機能を原則有効とした設定で提供し、加入後に自己の設定（設定の変更）により遮断機能を解除することができるようにした。また、既存のサービス提供者に対しては、遮断機能を利用するか否かを自己の判断で設定することができるようにした。

通信の秘密に関する事項であり、加入者に対して、その具体的な同意を問わずに、一方的にプロバイダが変更することによって、特定のアプリケーションを利用しての通信を遮断するという選択をすることができなかったということになる。また、同じ理由から、従来からの加入者について、具体的な同意をとる必要があると解されたのが、このような形での合意をとるにいたった背景ということになるのである。

4 示唆するもの

現在では、ネットワークの混雑により、通信の円滑な実施に影響がありうる場合について、通信量によって、制限する仕組みを導入することが検討されている⁷⁵。この制限モデルも結局、通信の構成要素に踏み込んで制限をなすということが解釈上、できないために通信量による制限という手法が考察されているものと思われる。しかしながら、このような考え方は、適法な利用をしているブロードバンド利用者と違法なコンテンツの配信・受信利用者ともに制限されてしまうという矛盾を招きかねない。

郵便法においては、具体的に禁制品を運ぶのを拒絶できる形での手法が整備⁷⁶されている。

⁷³ 「本日の「Winny」通信規制に関する一部報道について」

http://www.plala.or.jp/corporate/news_releases/2006/may/20060518.html

⁷⁴ 「ぷららバックボーンにおける「Winny」通信遮断サービスの提供開始について
～個人向け「ネットバリアベシク」サービスにおける「Winny フィルタ」機能を追加」

http://www.plala.or.jp/corporate/news_releases/2006/jun/20060613.html

⁷⁵ 「ネット混雑時、通信制限へ指針、総務省検討 年明けにも適用。」（平成19年5月21日、日本経済新聞）

⁷⁶ 14条（郵便禁制品）、15条（郵便約款による差出しの禁止）、23条の3（調査）、40条（引受けの際の申告および開示）、41条（取扱中に係る郵便物の開示）、42条（危険物の処

これらを参考にして、立法的対策等によって、違法利用の通信を合理的に峻別できる方法であれば、それをプロバイダ等が約款の変更によって制限できるという方策などを考えることは合理的であるように思われる。そもそも、通信の秘密のうち、トラフィック・データ部分については、そもそも他人の秘密として取り扱われていたにすぎないということもあり⁷⁷、これらをも踏まえて、ネットワーク管理のための合理的な手法を検討すべき時期にきているのではないのかということができるかもしれない。

置) 52条(還付)などの規定がある。

⁷⁷ 高橋郁夫・吉田一雄「『通信の秘密』の数奇な運命(憲法)」情報ネットワーク・ローレビュー(第5巻)(情報ネットワーク法学会、商事法務、平成18年)

付録4 Winnyをめぐる法律問題の概観

1 Winnyをめぐる法律問題とは

1.1 概念

Winnyの動作やそのWinnyネットワークの実態などは、本報告書の「付録1」および「付録2」において、明らかになっているとおりである⁷⁸。Winnyネットワークをめぐる問題については、Winnyネットワークの利用に関する問題点・暴露ウイルスによる情報漏えいの責任問題・Winnyネットワークによる情報漏えい対応および防止のための法律問題・Winnyネットワークの抑制に関する法律問題がある。

これらの法律問題を具体的に論じると以下ようになる。

1.2 Winnyネットワークの利用に関する問題

これの代表的な問題は、Winnyネットワークを流れている情報の大部分が、著作物違法複製情報もしくはわいせつ図画情報であることに関連して、Winnyネットワークの利用行為（具体的には、ダウンロード行為やアップロード行為）が、著作権侵害行為などに該当しないかという問題である。また、実際の利用状況を知っていてプログラムをアップロードしたというWinnyプログラム作者に対する刑事裁判もそのような観点の問題として位置づけられる。

1.3 暴露ウイルスによる情報漏えいの責任問題

これは、昨今の情報漏えいに関して、特定の組織等において管理していた情報が、暴露ウイルスによって、漏えいした場合にその組織等が法的な責任を負うのではないかという問題である。この点については、報告書の本編の「第3の2.7 事後対応」において述べているところであり、本付録では省略する。

1.4 Winnyネットワークによる情報漏えい対応および防止のための法律問題

本報告書の本編において、情報漏えい対応の際の重要な原則として「事実確認の原則」があることが述べられている。その際に、適切な方策で、証拠を保全することが、情報漏えい対応の際のその後の調査、開示等、被害の抑制・復帰、再発防止などの手順においてきわめて重要な意義を有することも述べられている。ところで、Winnyによる情報漏えいは、一般的に、会社の仕事のデータをUSBメモリ等に複写し、それを自宅でのPC等において処理している際に、同一のコンピュータ上でWinnyネットワークを利用しており、そこで、暴露ウイルスに感染することから漏えいすることが多い。このような場合、自宅のPCに漏えいの証拠が保存されている状態であり、組織等としては、その従業員の自宅等において

⁷⁸ なお、2006年段階において、情報漏えい事件との関係から、Winnyをめぐる法律問題を論じたものとして高橋郁夫「2006年情報セキュリティと法的問題の概観」(<http://www.ipa.go.jp/security/event/2006/ipa-forum/061024h.pdf>)がある。

証拠保全をおこなわなければならない。その際に、当然、そのような組織等の行動は、その従業員のプライバシーの合理的な期待と衝突することがあり、その場合、企業等は、どの範囲まで合理的に行動できるかという問題がある。また、その衝突を回避するために法的に合理的な方法はないのかということになる。

また、再発防止策の為に Winny の利用をしないという誓約書を従業員等にも書いてもらうということがあるとして、それに関連する法律問題も存在することになる。

1.5 Winny ネットワークの抑制に関する法律問題

平成 18 年 3 月に大手インターネット接続事業者が、「Winny」の通信を遮断する措置を予定していたが、総務省は、この措置は、電気通信事業法で定めた通信の秘密を侵すと考えられると判断した。これらの一連の動きは、「付録 3 Winny トラフィックの制限と通信の秘密」で詳細に紹介したところである。

2 Winny ネットワークの利用に関する問題点

2.1 Winny 利用の法的問題の所在

わが国においては、Winny の利用を推奨し、あたかも著作権侵害を推奨するような入門書が書店などで多数販売されており、また、法的問題についてなんら認識もしないで、著作物が簡単に手に入るという観点からの報道もなされている。

しかしながら、そもそも、Winny ネットワークの現状を前提とするかぎり、利用行為自体についても以下のような法的な問題が存在することは指摘されなければならない。

2.2 著作権との関係⁷⁹

(1) Winny におけるアップロード行為

Winny ネットワークにおいて、他人の著作物を複製したファイルを作成し、それを Winny ネットワークにおいて共有することは、その過程で以下のように著作権法に違反する行為であり、刑事罰の対象となる。すなわち、その複製自体が、複製権（同法第 21 条、第 91 条第 1 項、第 96 条、第 98 条、第 100 条の 2）を侵害する行為となる。そして、Winny ネットワークにおいて共有することは、公衆送信権若しくは送信可能化権（同法第 23 条、第 92 条の 2、第 96 条の 2、第 99 条の 2、第 100 条の 4）を侵害していることになる。これらの行為をなしたものは、損害賠償責任を負うと解される（民法第 709 条）。また、故意過失の有無に関わらず権利侵害があった場合又は侵害のおそれがある場合には権利者から差止請求を受けることもある（著作権法第 112 条）。さらに、故意かつ告訴があった場合には、刑事責任として 5 年以下の懲役又は 500 万円以下の罰金を課されることがある（同法第 119 条）。

これらの行為は、私的使用目的ではないため、私的使用目的の複製（著作権法第 30 条

⁷⁹ 「電子商取引及び情報財取引等に関する準則」平成 19 年 3 月 経済産業省
<http://www.meti.go.jp/press/20070330011/denshishoutori3.pdf>

第1項)に該当しない⁸⁰。

著作権法違反被告事件(京都地方裁判所・平成16年11月30日・判例時報1879号153頁)は、Winnyユーザである群馬県高崎市の自営業男性と愛媛県松山市の無職男性が平成15年9月、著作権者に無断でゲームソフトや映画を不特定のインターネットユーザに送信できる状態にしていたという事件であるが、裁判所は、「ハードディスクと接続したパーソナルコンピュータを用いて、インターネットに接続された状態の下、そのアップフォルダに上記各情報(筆者注-映画の著作物をさす)が入った送受信プログラムを有するファイル交換ソフト「Winny 2.0 6.6」を起動させ、同パーソナルコンピュータにアクセスしてきた不特定多数のインターネット利用者に上記各情報を自動公衆送信し得るようにし、もって上記各著作権者が有する著作物の公衆送信権を侵害した」という事実を認定して、Winny ネットワーク利用者におけるアップロード行為が公衆送信権を侵害していることを明らかにしている。

(2) Winnyにおけるダウンロード行為

Winnyを利用して、著作権侵害データをダウンロードすることは、それ自体、違法な複製権侵害にならないのかという問題がある。現実のWinny ネットワークの動作および流れているファイルの実態のもとでは、利用者は、他者提供を前提として自己のコンピュータに複製をしており、しかも、Winnyの動作およびファイルの性質についての認識も有しているのであるから、「私的複製とはいえず」違法な複製権の侵害行為をおこなっていると解される。

ダウンロードのみの行為だとしても、著作権法30条1項の「私的複製」の規定は、家庭のよう閉鎖的な私的領域における零細な複製に限って許容されているにすぎないので、Winny ネットワークのようないわば多数の参加者のいるネットワークにおけるダウンロード者自身のコンピュータに対する複製自体が、違法な著作物の複製になると解することができる(反対説もありうる)。

もっとも、上記反対説であるWinnyにおけるキャッシュ(という名の複製)自体は、私的複製だと解する立場をとったとしても、それが、同時に他のノードのために公開されていることになるので、著作権法49条1項の解釈として、私的複製に該当するものではないと解される。注2の「電子商取引及び情報財取引等に関する準則」(平成19年3月)も、直接、私的複製に該当するのか、著作権49条1項に該当するのかについては、明確にしないものの、Winnyプログラムのような作用をするプログラムでの行為(ユーザがダウンロードしたファイルをそのまま自己のPCの公衆送信用記録領域に記録し、インター

⁸⁰ 当初は、自分のみで再生して楽しもうと、購入したCDから、私的使用目的で複製した場合であったとしても、途中で気が変わってファイルをアップロードしたようなときには、著作権法第49条第1項第1号又は第102条第4項第1号の規定により、私的使用目的以外の複製を行ったとみなされる。

ネット上で送信可能な状態にした(ダウンロード行為が同時にアップロード行為に相当する)場合)については、「当該ダウンロード行為は私的使用目的の複製には該当しないため複製権侵害となる」と明言している⁸¹。

もっとも、理論的にはWinnyにおいてキャッシュが断片化して、複数のコンピュータに保存されている場合、はたして複製とどういうのか、共犯となるのか、という問題が存在するであろう。

(3) Winny 作成者の刑事裁判について

ア また、Winny 作者に対する著作権違反幫助被告事件について京都地裁判決(京都地判・平成18年12月13日、以下、本件判決という)がある。これは上記(1)の正犯者を幫助したということで起訴された事実に対する判決である。この判決は、きわめて注目を浴びたものであるので、判決の内容について紹介することにする。

イ 罪となるべき事実について

判決では、「罪となるべき事実」において正犯者が、著作権違反行為を行った際に、これに先立ち、Winny が広く利用されている状況のもとで、Winny の最新版である「Winny2.0 6.47」を被告人方から前記「Winny2 Web Site」と称するホームページ上に公開して不特定多数者が入手できる状態にした上、同日ころ、上記正犯において、「同人にこれをダウンロードさせて提供した」ことが客観的な構成要件事実として認定されている。そして、これに対応して、「6 被告人に対する著作権法違反幫助の成否」において「(1)被告人が開発、公開した Winny2 が、各実行行為における手段を提供して有形的に容易ならしめたほか、Winny の機能として匿名性があることで精神的にも容易ならしめたという客観的側面は明らかに認められる。」としている。

一般に、幫助犯の構成要件については、幫助の行為自体は、正犯の違法な行為について物理的もしくは心理的に、これを容易にすれば、犯罪が成立することとなっていることに対応するものである⁸²。

ウ 主観面について

判決では、上記幫助犯の構成要件に該当する行為について「価値中立的な技術を提供すること一般が犯罪行為となりかねないような、無限定な幫助犯の成立範囲の拡大も妥当でないことは弁護人らの主張するとおりである。」として、「6 被告人に対する

⁸¹ ファイルログ事件仮処分決定(東京地方裁判所決定・平成14年4月11日)も、いわゆるハイブリッド型P2Pネットワークであるが、その利用者は、受信者であっても、他人のために公衆に音を提示する行為は、法49条1項の解釈として、私的複製に該当するものではないとしている。

⁸² FLMASK リンク事件(大阪地判平成12年3月30日)においては、「幫助犯は、正犯者の犯罪行為を表象しつつ、その犯罪を容易にし、あるいは促進助長する行為をするものでなければならぬと解される」と判示されている。

著作権法違反幫助の成否」において、「(3)結局、そのような技術を実際に外部へ提供する場合、外部への提供行為自体が幫助行為として違法性を有するかどうかは、その技術の社会における現実の利用状況やそれに対する認識、さらに提供する際の主観的態様如何によると解すべきである。」としている。そして、判決によると、その(5)において、「『現実の利用状況(ファイル交換ソフトを利用していなされるファイルのうち、かなりの部分が著作権の対象となる、著作権を侵害する態様で広く利用、著作権侵害をしても安全なソフトとしてとりざたされていた、効率・便利で広く利用)』について認識したうえで、そのような利用状況として利用されることを認容しながら、自己の開設したホームページ上に公開し、多数の者が入手できるようにしたことが認められる」としているものである。そして、各実行犯が実行に及んだので、「被告人がそれらのソフトを公開して不特定多数の者が入手できるように提供した行為は、幫助犯を構成するとする」と判断しているのである。

エ 位置づけ

この判断については、現在、検察側、弁護側ともに控訴をしており、控訴審での判断がまたれるところである。この判決自体においては、幫助犯の故意と判決のいう「提供する際の主観的態様如何」というのが違うのかどうかという点や行為者の意図の認定に技術的な分析手法(ソースコードからの鑑定等)の応用はできないのかということからもさらなる深い議論を期待したいところである。

また、上記判決文からも明らかなように違法な利用状態が蔓延していることを承知しているという特定の心理状態のもとで、ソフトウェアをアップロードしたという事案であって、その事案の特殊性からくる判決の射程距離の狭さは了解しておく必要がある。

オ 将来の問題

もっとも、わが国において、例えば、セキュリティ侵害や著作権侵害を主たる目的としたプログラムが作成された場合に、刑事法的に違法とすべきではないかという論点が存在する。そのようなプログラムは、機能自体としては、両用に用いることができる場合も多く、そのような場合にどのように社会は対応すべきなのかという問題がある⁸³。

2.3 その他の観点

⁸³ サイバー犯罪条約においては、第6条「機器の不正使用(Misuse of devices)」として「第二条から前条までの規定に従って定められる犯罪を主として行うため設計され又は調整された装置(コンピュータ・プログラムを含む。)」を製造等する行為を刑事的に違法とするとされている。この議論の過程においては、犯罪遂行のためのプログラム(いわゆる両用のプログラムである)に対して、どのような対応をすべきかどうかという点についての問題が、正面から議論され、このときの議論においては、「主として」という用語で、刑事罰を成立させるものとしたのである

Winny ネットワークの現状において、わいせつな図画たる電子ファイルが多数流通しているとの報告がある。わいせつな画像データを記憶、蔵置させたハードディスクは、刑法 175 条が定めるわいせつ物に当たるということになる（最判平成 13 年 7 月 16 日・判例タイムズ 1071 号 157 頁）。そして、ハードディスクに記憶、蔵置された画像データを、Winny ネットワークを介して不特定多数の者が認識できる状態に置いたということになれば、わいせつ物を「公然と陳列した」ことに当たると解される（上記判例）。

また、ネットワークを流れている情報については、その相当数が、悪意あるプログラムとしての性質を有しているとされている。詳しくは、本報告書「付録 1 Winny(P2P ネットワーク)とインターネットの関係」の「2.3」参照。そのようなネットワークであるということについてなんら注意をせずに利用して、他人の権利を侵害した場合（情報を漏えいする等）には、損害賠償などの法的責任を追及されることになる。

3 Winny ネットワークによる情報漏えい対応および防止のための法律問題

3.1 問題の概説

証拠保全の重要性と従業員の自宅等における証拠保全の一般性については、本報告書「第 3 の 2.3 初動対応」で詳述している。この際の従業員のプライバシーの合理的な期待との衝突という問題があり、この点については、そもそも、企業が何らかの不正行為が発生した場合におけるその調査の権限と限界という論点から検討すべきものである。また、再発防止の為に Winny 不使用の誓約書の問題というのも実際の問題である。

具体的に、企業の不正行為に対する調査権の根拠、その範囲、限界、私的領域に対する合意等を求めることの可能性などの観点から検討することとする。

3.2 使用者の不正行為に対する調査権の根拠・範囲・限界

(1) 不正調査の権能

組織等に関して情報漏えいが発生した場合、その組織等は、情報漏えいの種類、範囲・原因を見きわめるために、関係者に対して事実関係を調査し、場合によっては、証拠を保全することなども必要になってくる。このような行為が法的にどのように位置づけられるかということが問題になる。

まず、不正調査のための使用者の権能についていえば、使用者は、「企業秩序は、企業の存立と事業の円滑な運営の維持のために必要不可欠なものであり、企業は、この企業秩序を維持確保するため、これに必要な諸事項を規則をもつて一般的に定め、あるいは具体的に労働者に指示、命令することができ、また、企業秩序に違反する行為があつた場合には、その違反行為の内容、態様、程度等を明らかにして、乱された企業秩序の回復に必要な業務上の指示、命令を発し、又は違反者に対し制裁として懲戒処分を行うため、事実関係の調査をすることができることは、当然のことといわなければならない。」というのが

一般的な認識ということになる(富士重工業事件最高裁判決、最三小判昭52年12月13日労判287号7頁)。

(2) 不正調査の範囲

そうはいつでも、上述の判決は、続けて「労働者は、労働契約を締結して企業に雇用されることによって、企業に対し、労務提供義務を負うとともに、これに付随して、企業秩序遵守義務その他の義務を負うが、企業の一般的な支配に服するものということとはできないからである。そして、右の観点に立つて考えれば、当該労働者が他の労働者に対する指導、監督ないし企業秩序の維持などを職責とする者であって、右調査に協力することがその職務の内容となっている場合には、右調査に協力することは労働契約上の基本的義務である労務提供義務の履行そのものであるから、右調査に協力すべき義務を負うものといわなければならないが、右以外の場合には、調査対象である違反行為の性質、内容、当該労働者の右違反行為見聞の機会と職務執行との関連性、より適切な調査方法の有無等諸般の事情から総合的に判断して、右調査に協力することが労務提供義務を履行する上で必要かつ合理的であると認められない限り、右調査協力義務を負うことはないものと解する」とも述べている。そして、具体的な判断としては、そのような調査義務の範囲にはないとする判決例も相当数存在する。

では、具体的に、そのような業務に関連する証拠として意味のあるデジタル情報が、個人で使用している会社のサーバ内に保存されていた場合はどうかということになる。この点について興味深い判断を提供するのが日経クイック事件(東京地裁・平成14年2月26日判決・労働判例825号50頁)ということになる。この事件は、誹謗中傷メールが会社内に送付された事実があり、原告が、その行為をなした嫌疑があるとして原告に対しておこなわれた事情聴取が名誉毀損にあたるとして会社および被告社員に対して慰謝料の支払いと調査の際入手した原告の個人データなどの返還を求めたものである。

裁判所は、本件誹謗中傷メールの送信は、「企業秩序を乱す行為であり、就業規則(略)に照らして懲戒処分の対象となる可能性があるから、その観点からいつでも速やかに調査の必要がある」とし、「原告が誹謗中傷メールの送信者であると疑う合理的理由があったから、原告に対し事情聴取その他の調査を行う業務上の必要があったということが出来る」との一般論を述べ、その後、「社内における誹謗中傷メールの送信という企業秩序違反事件の調査を目的とするもので、かつ、原告にはその送信者であると合理的に疑われる事情が存するのであるから、原告から事情聴取をする必要性と合理性は強く認められる。」として、事情聴取を認めている。そして、ファイルサーバ上のデータの調査の調査方法の相当性については、「業務に何らかの関連を有する情報が保存されていると判断されるから、上記のとおりファイルの内容を含めて調査の必要が存する以上、その調査が社会的に許容しうる限界を超えて原告の精神的自由を侵害した違法な行為であるとはいえない。原告に調査することを事前に告知しなかったことは、事前の継続的な監視とは異なり、既に送受信されたメールを特定の目的で事後に調査するものであること、原告が誹謗中傷メー

ルと私用メールという秩序違反行為を行ったと疑われる状況があり、事前の告知による調査への影響を考慮せざるを得ないことからすると、不当なこととはいえない。」そして、プライベートな情報の取得についても「結果としては誹謗中傷メール事件にも、私用メール事件にも関係を有しない私的なファイルまで調査される結果となったとしても、真にやむを得ないことで、そのような情報を入手してしまったからといって調査自体が違法となるとはいえない。」としている。

(3) 所持品検査の根拠と限界

では、従業員の私物に対して企業が調査をなすう場合は、どのような場合で、どこまで可能になるのかという問題になる。

一般に所持品検査の適法性については、西日本鉄道事件（最判昭和43年8月2日・民集22巻8号1603頁）がリーディングケースであるとされている。これは、所持品検査の手法について、靴を脱いで検査するという手法にした場合に、それが許容されるのかという点が争いになった。最高裁判所は、「おもうに、使用者がその企業の従業員に対して金品の不正隠匿の摘発・防止のために行なう、いわゆる所持品検査は、被検査者の基本的人権に関する問題であつて、その性質上つねに人権侵害のおそれを伴うものであるから、たとえ、それが企業の経営・維持にとつて必要かつ効果的な措置であり、他の同種の企業において多く行なわれるところであるとしても、また、それが労働基準法所定の手続を経て作成・変更された就業規則の条項に基づいて行なわれ、これについて従業員組合または当該職場従業員の過半数の同意があるとしても、そのことの故をもつて、当然に適法視されうるものではない。問題は、その検査の方法ないし程度であつて、所持品検査は、これを必要とする合理的理由に基づいて、一般的に妥当な方法と程度で、しかも制度として、職場従業員に対して画一的に実施されるものでなければならない。そして、このようなものとしての所持品検査が、就業規則その他、明示の根拠に基づいて行なわれるときは、他にそれに代わるべき措置をとりうる余地が絶無でないとしても、従業員は、個別的な場合にその方法や程度が妥当を欠く等、特段の事情がないかぎり、検査を受忍すべき義務がある」としている。具体的に特定の従業員において、企業秩序の侵害をなした疑いが現実に存在する場合における判断ではないことに注目がされる。

もっとも、企業秩序の侵害が現実になされた場合に、その原因究明のための検査が議論になった例は、あまり多くはない。その点で、JR東海大阪第一車両所事件・大阪地方裁判所・平成16年9月29日（労働判例884号38頁）が、企業秩序侵害があった場合の不正調査という意味できわめて示唆を含む事件といえるだろう。この事件は、従業員が、車両基地でノートを落とし、その落とししたノートを持った従業員が、会社の助役兼総務課長に届け、その総務課長は、誰が遺失したのかを確認するために遺失したノートを読んだところ、企業秩序違反に関連する事実を発見したので、ノートのすべての複写を行い、その複写したページを関西支社に届けたという事実関係のもとで、その従業員が、プライバシー権・人格権侵害等を理由として慰謝料の請求をなしたという事件である。裁判所は、

「ノートの遺失者等を特定するため、一定の限度で、ノートの記載内容を確認し、遺失者等を特定できる記載がないか調査することも、遺失物を保管している占有者として許されるというべきである。」と述べ、その上で、「ノートの遺失者等を特定するためにその記載内容を確認している際に、本件総業行為の存在や原告組合らの関与の各可能性が看取できる記載を発見した場合には、それを証拠化するとともに事後の事実調査に用いるために、当該記載部分につき写しを作成して被告会社において保管することは許されるというべきである。」とされている。もっとも、このような場合でもプライバシーに対する配慮は必要になってくる。この事件でも、「原告組合組合員らとした話の内容のほか、冠婚葬祭や交友関係等の原告甲野の私事や思想信条に関することなど所有者のプライバシーに関する記載がされているのであるから、前記目的が正当であるからといって、被告乙山において、本件ノートの前記プライバシーに関する記載部分までを含めてすべてのページについて写しを作成し、関西支社に届けることが正当化されるものではない。」としている。

この判決例は、上司が適法に調べうる権限を有している場合に、その過程で、企業秩序違反があると信じる相当な根拠を有した場合に調査・証拠保全をすることを許容しているものと考えることができよう。

(4) 同意と調査の方法

調査協力義務の限界が明確ではないので、実際上は、調査権を行使するのにあたり、具体的な同意をとることになる。同意がとれない場合、私物を提供する形で調査に協力する義務があるかどうかということは、上記富士重工原水禁事情聴取事件の一般論によって判断されることになる。

もっとも、新聞報道によると、中国人技術者による約13万件の製品データ持ち出し事件(横領で平成19年3月16日逮捕)で、担当の社員が自宅訪問をしたときに、私物のPCに内蔵されたハードディスクを千枚通しのようなもので破壊したという事件があったとされている。物に対する調査であり調査協力義務があると解したとしても、その協力義務を実効あらしめる形で、調査するためのノウハウの問題や調査方法の適法性の問題⁸⁴は、まだ、未解決の問題であると思われる。

3.3 使用者が私的領域での行為に対する懲戒の可否および合意等を求めることの根拠 私生活上の行為について、どのような規制ができるかという問題がある。

従業員の私生活上の行為については、「従業員の職場外でされた職務遂行に関係のない所為であっても、企業秩序に直接の関連を有するものもあり、それが規制の対象となりうることは明らかであるし、また、企業は社会において活動するものであるから、その社会的評価の低下毀損は、企業の円滑な運営に支障をきたすおそれなしとしないのであつて、その

⁸⁴ 例えば、具体的事情から調査協力義務があるといえるような場合において、証拠の滅失を防ぐために、その私物の管理者たる従業員に虚偽の事実を伝えて、その私物の占有を確保することはどうかという問題が考えられる。

評価の低下毀損につながるおそれがあると客観的に認められるがごとき所為については、職場外でされた職務遂行に関係のないものであつても、なお広く企業秩序の維持確保のために、これを規制の対象とすることが許される場合もありうるといわなければならない」（国鉄中国支社事件・最一小判昭49年2月28日民集28巻1号66頁）⁸⁵というのが一般的な認識である。

インターネットでの言論などについてもそのような理論は、適用される。具体的には、学生時代からインターネット上に自らのホームページを開設し、書評・映画評、紀行文といった個人的な文章を公開していた者が新聞社入社後に、新聞記者として行動しながら感じた報道現場における疑問点（記者クラブ制度、業界慣習、労働実態等）や他の記事等に対する批判等を論じた文章を「新人記者の現場から」と題する項目の中で公開するようになっていた。彼は、上司からの指摘でいったんは、そのホームページを閉鎖したものの再度、記事を掲載するようになった。これに対して、新聞社は、発表原稿の処理（執筆）を中心とした職務を担当させ、事情聴取等を行うとともに、公開した文章が新聞社の信用を害するものであることを指摘した上、控訴人に対して依願退職を勧めたが、記者が拒否したため、出勤停止処分（本件懲戒処分）に処したという事件がある。この事件で、東京高判平14年9月24日（労判844号87頁）は、その記者が自らの判断でホームページを再開するに当たり、「少なくとも問題点を指摘された文章を削除するなどの措置を講ずることは容易に可能であったにもかかわらず、控訴人（筆者注 - 新聞記者をいう）は、被控訴人（筆者注 - 新聞社をいう）の了解を得ないままホームページの公開を再開し、問題点を指摘された文章を削除したり、修正を加えたりすることもなくそのまま再掲したばかりか、その後も、取材の過程や取材源を公表する記述を含んだ新たな文章を公開したのであるから、被控訴人の就業規則33条1号によって従業員が遵守すべきこととされている「会社の経営方針あるいは編集方針を害するような行為をしないこと」に故意に反したものである」という認定がされている。組織の業務執行そのものでない私的な行為としても、就業規則の規制が及ぶことは当然のことなのである。

では、プライバシーとの関係で、Winny を利用しない旨の誓約書の作成を求めるような行為に法的な問題は、ないのかということになる。例えば、3.2. でふれたような所持品検査にかかわる確認書について、業務命令としての性格を有する署名義務のようなものを考慮しうるかという点は、どうか。この点についての判決の考え方は、明確ではない⁸⁶。

⁸⁵ 同旨のものとして関西電力事件・最一小判昭58年9月8日労判415号29頁がある。

⁸⁶ 福岡高判昭和59年2月15日（判例タイムズ538号154頁）は、確認書への押捺について、「会社の意のあるところを善解して任意これに応ずるか、その内容に危険を感じてこれを拒否するかは、その自由に委ねられるものといわざるを得ない。」として「拒否の自由のない命令としてあくまで本件確認書への押印を求めることは、正当な職務上の指示等にあたるということができず、従つてその拒否は前記懲戒事由に該当しないものというべきである。」とする（最判

その一方で、私生活において事前に組織等への報告を求める行為などについてどのように考えるかという点で、外資系証券会社を舞台にした興味深い事件がある。原告は、フラット為替⁸⁷という金融商品の販売に従事していた外資系証券会社のエグゼクティブ・ダイレクターであった。この為替取引については、ある監査法人が、ヘッジ会計が認められる範囲を厳しく判断する立場をとるようになり、平成15年2月18日には、フラット為替を利用した取引に関して、予約期間が3年を超える取引については、原則として、ヘッジ会計を認めることはできないとした。原告は、この監査法人の示した見解について自己の営業の妨げになると思い、この監査法人に対して圧力となる方策をとることとした。そして、法務部および広報部の許可を得ることなく、他の金融アナリストとの共著の形で、「金融アナリスト」の肩書で週間東洋経済に上記監査法人の見解について、挑発的な内容の文書を記した。そして、この記事を観客、ACCJ（在日アメリカ商工会議所）および5大監査法人に送付した。これらの行為の間にも原告は、独自行動を止めるように上司等からいわれていたが、それにかかわらず、結局、自分の思ったように結果がえられなかったため、自己の名義で、原告が昇進・昇給で不利益を受けることを理由として公認会計士協会に対して訴訟を提起した。証券会社は、原告に対して譴責をなすとともに、訴訟を取り下げるように指示をしたが、原告は、これに応じることはなかった。その結果、証券会社は、原告に対して「書面による取下命令にもかかわらず、訴訟を取り下げないことを明確にしたもので、この件に関する原告の態度が、被告との信頼関係を著しく損ない、被告の秩序規律を乱した」「別件訴訟を提起したことについて被告設備を使用して顧客に喧伝し、その結果、被告の世評とフランチャイズを毀損した」ことを理由にして懲戒解雇をして、予備的に普通解雇をしたという事件である。

東京地方裁判所（平成17年4月15日・労働判例895号42頁）は、決論的には、懲戒解雇は認めず、普通解雇を認めたにすぎなかった⁸⁸が、その結論に至る判断はきわめて興味深いものといえる。具体的には、裁判所は、「従業員の私生活上の行為であるとしても、使用者の利益に影響を及ぼす場合があり得るところ、従業員は、労働契約上の誠実義務として、業務の内外を問わず、使用者の利益に配慮し、誠実に行動することが要請されるのであり、個人訴訟が使用者の利益を害することとなれば、使用者から誠実義務違反を問わ

昭62・9・4、労働判例505号10頁は、この判断を支持）。

⁸⁷ 「一定期間内に一定のレートで外貨を売買することを予約する先物商品」でヘッジ会計が認められる場合には、ヘッジ対象の損益が計上される時点まで、時価評価による損益を計上する必要がないものとされる。

⁸⁸ 「これらの非違行為によって、被告が損害を被ったり、その具体的な危険が生じたとまでいうことはできない」とか「懲戒処分として、退職金が支給されない懲戒解雇を選択することは、処分として重きに失するというべきであり、本件懲戒解雇は、懲戒権を濫用したものである」という点が認定されている。

れることとなる。」とした上で、「使用者は、従業員の私生活上の行為が被告の利益を害すると判断した場合、従業員個人に対して、かかる行為を任意に修正することを要請し、また、その前提として、従業員に対して、事前に予定された行為の内容の報告を求めることは、公序良俗に反しないと解される。さらに、従業員の私生活上の行為によって、使用者の利益が害された場合、使用者は、従業員に対して、事後的に労働契約上の誠実義務違反を問うことができると解される。」と述べている。そして、「被告の事業活動としての実質的側面を有するといわざるを得ない」場合においては、「被告の利益が害されることが明白である場合、被告は、原告に対して、かかる結果を招来する行動を回避することを事前に業務として命令できると解するのが相当である。」としている。

この判決がいうように「従業員は、労働契約上の誠実義務として、業務の内外を問わず、使用者の利益に配慮し、誠実に行動することが要請される」のであり、Winny ネットワークの利用行為が情報セキュリティ上の重大な懸念をもたらしかねないというのが現時点での認識である⁸⁹ものと考えられる。そのような現状を前提とする限り、「従業員に対して、事前に予定された行為の内容の報告を求めることは、公序良俗に反しないと解される」ので、Winny の利用をしないということを誓約⁹⁰させたとしても、公序良俗に反することはないものと考えられる。もっとも、この誓約書の締結を拒絶した場合に、職務上の命令として、懲戒をなしうるのかということについての判断は微妙⁹¹であろう。

⁸⁹ いうまでもなく、従業員の私生活に対して使用者が、一定の行為を求めうるのは、そのような行為を求めるのが、企業の業務遂行にとって必要なものと思慮されることによるものである。現代社会における情報セキュリティおよびそのための管理体制の重要性は、企業の業務遂行にとってきわめて重要なものとなっていると認識されるであろう。

⁹⁰ 判決例によれば、利用についての事前報告が許容されることになる。が、使用者としては、Winny の利用は、その利益に反するという見解を表明しており、その見解に反する行為は、誠実義務違反になる。誓約書は、その誠実義務違反をしないということを事前に誓うことと位置づけられるのであり、公序良俗に反するものではないと位置づけられることになるろう。

⁹¹ 東京地裁の判断が、具体的な問題が惹起された場合の判断であり、その一方で福岡高裁の判断が抽象的な事前の段階の判断であるということになるのであろうか。

付録5 警察に助力を求める際の留意事項

序

情報漏えいに関して、犯罪行為が関連する可能性がある場合については、早い段階から警察に相談し、対応を求めることも一つの対処方法である。具体的には、従業員の内部犯行によって情報が漏えいしてしまった場合（背任、不正競争防止法違反等被疑事件等）、外部からの侵入等によって情報が漏えいしてしまった場合（不正アクセス禁止法違反被疑事件）、漏えい情報に関して不正な金銭等の要求を受けた場合（恐喝・脅迫・強要等被疑事件）などの場合が挙げられる。以下に、情報漏えいにおいて警察の助力を得るにあたり企業等において意識しておくべきと考えられる留意事項について整理した。本付録の内容については、警察庁の協力を得たことを記しておく。

1 都道府県警察本部サイバー犯罪相談窓口の活用

全国の都道府県警察本部においてサイバー犯罪相談窓口が設置されており、情報技術を悪用した犯罪等に関する相談を受け付けている。情報漏えい事件において、犯罪の関連性があると予想される場合は、「まず相談」をすることでその後の対応を円滑に運ぶことにつながることもある。

（1）犯罪性

犯罪の嫌疑と関係ない事案について処罰を求めようとしても、警察がこれに対処する根拠が存在しない。刑事事件の疑いがある場合、その犯罪行為に対して犯人を特定し、証拠を収集し、法の適用を求める手続きを行うことになるので、警察の対応を求めるにあたっては情報漏えいの事態に関して犯罪性の疎明を行うことが前提となる。電話等での相談の過程において、企業自身が気づいていない事実関係について警察からの指摘で気づくようなこともありうるだろう。その意味では少しでも犯罪への関連性の疑いがある場合には、早期に相談することが推奨される。

具体的に法的対応を求めるにあたっては、漏えいした情報が法的な保護の対象になっているのかについて、注意する必要がある。例えば、不正競争防止法2条1項10号に定める不正競争行為該当行為の可能性があると、違法な手法により情報が漏えいしたと相談しても、普段の状況においてその情報が営業秘密としてきちんと管理されていなければ法律で対応し得ない。本編でも「備えあれば憂いなし」の原則として述べたように、事前の準備・普段からの準備状況が、情報漏えい時において効果を発揮するのである。

また、不正アクセスに関しては、対象となる機器がスタンドアロンで運用されている場合やアクセス制御機能が存在しない場合には、法の適用対象外となっている。アクセス制御機能のないところに情報を置き、それに外部からアクセスされたということでは、犯罪は成立せず、警察としても対応しえないのである。

(2) 迅速な判断

警察に相談、届出をするにあたっては、「まずは」迅速に相談をすることが望ましい。特に、外部からの不正アクセス事案などにおいて迅速な判断が必要となる。不正アクセスの場合は、適切な措置を早急にとらなければ被害が拡大してしまうおそれがある。警察に相談をしたとしても、被害届の提出という段階になり結果的にこれを取り下げるということもありうるが、いずれにせよ被害届は被疑者を特定し処罰することを求める意思の発現であることから、経営トップの判断と責任に基づき提出すべきであるとともに、提出した以上は、関係資料の提供、参考人の供述など全面的に捜査に協力することも求められていることも認識しておく必要があるだろう。

(3) 社会的な説明責任

警察への相談・届出に関しては対応の面からの必要性が判断の要素となるが、現代社会においては犯罪による情報漏えいが発生した場合には、経営上利害関係者への説明責任をはたすという見地から、警察への相談を利用すべきという考え方もある。事件を内部で処理した場合に、外部の顧客に影響がでるような場合に、企業として説明責任を果たしているのかという点についても検討が必要である。

(4) 相談先

警察への相談が必要と判断された場合には、地域を管轄する警察署または各都道府県警に設置されたサイバー犯罪相談窓口に連絡することになる。また被害届等を提出する場合は管轄の警察署に提出することになる。

各都道府県警のサイバー犯罪対策に関する取組及びサイバー犯罪相談窓口については以下を参照されたい。

各県警の取り組み

<http://www.npa.go.jp/cyber/localpolice/index.html>

都道府県警察本部のサイバー犯罪相談窓口等一覧

<http://www.npa.go.jp/cyber/soudan.htm>

2 情報漏えいにおける捜査への協力

情報漏えいにおいて犯罪との関連から警察による捜査が行われる場合、企業（組織）の協力が必要不可欠となる。企業（組織）が警察と連携をはかりながら情報漏えい事件に対応していく際の留意事項を以下に示す。

(1) 連絡先の確定

企業（組織）での情報漏えいについて捜査活動が展開される際、重要となるのが、連絡担当窓口となる人物の指定である。窓口は必ずしも一人でなくてもかまわないが、窓口を担当する人物については、技術的なことについての理解があり、一方で経営的な事項についても対応できることが望ましい。組織内で一貫した方針に基づく判断と正しい情報を提

供するためにも、企業（組織）においては緊急対応のチームが確立され対応することが望ましい。

（２）資料の提供等

捜査においては、技術的な事項について以下のような資料が必要となることが多い。これらの資料については通常の企業（組織）においては当然備えておくべきものであるが、適切に維持管理されていないケースも少なくないと考えられる。いざという時の備え、これらの情報を適切に把握し管理するようにしておきたい。また、日頃からこれらの情報を適切に管理していなければいざ情報を提供するにあたり時間がかかってしまい捜査の妨げになることもある。こういった状況をふせぐ意味でも日頃より情報の適切な管理をこころがけるべきだろう。

また、いったん企業として処罰を求めたからには、警察から資料の提供等を求められたときは、きちんと提供すべきである。事情はあるかもしれないが、必要な協力を怠ることによって問題の解決に支障が及ぶ可能性もあることを認識すべきである。

ア ネットワーク構成図

捜査担当者が情報システムの概要および全体像を把握するために必須となる。

イ アカウントリスト

情報及び機器にアクセスすることができたアカウントのリストである。こういった範囲の従業員がアクセスが可能であったか、リモートアクセスが許容されてたかなどがポイントとなる。

ウ アクセス制御リスト

アカウントリスト同様関連する情報及び機器に対してどのようなアクセス制御がなされ、誰が何にどのような形でアクセスが可能であったかを示す根拠となる。また、実際のアクセス記録についても適切に維持管理されている必要がある。

エ 外部委託の場合の管理要領等資料

ネットワークの運用を外部に委託している場合などにおいて、どのような情報がどこに存在するのか、アラートはどのような形で発せられるかなど情報を事前に把握しておく必要がある。これがない場合、担当業者がいない限り何も対応できないということになってしまう。

オ ログ及び流出データ

ログや流出したデータがあれば、証拠保全上の留意点として、手をふれず、そのままの形で保存しておくことが必要である。会社（企業）に都合の悪いデータを排除して提供される場合があるが、分析の観点からもまた証拠としての観点からも不都合となる。

カ サーバ機器等

必須ではないが被害コンピュータを停止し任意提出することが望ましいとされることがある。この場合、業務に支障がでないように、代替サーバ等が必要となる。被害コンピュータを停止し任意提出するのか等については経営陣・技術者・警察との間で協議の上決定

される

3 漏えい情報に関して不正な金銭等の要求を受けた場合の対応

(恐喝・脅迫・強要等被疑事件)

漏えい情報をもとに、脅迫などの行為が行われた場合には、担当者のその場の判断などで、要求に応じるようなことがあってはならない。多くの場合こういった要求に応じたとしても、さらなる要求が提示されるなど、問題の解決につながらない場合が多い。また、こういった問題を隠蔽しようとした場合には、経営責任等のさらに大きな問題に発展することもある。不法な要求に対して、毅然とした対応をとることが重要である。このような要求においては、警察への相談や民事介入暴力担当の弁護士などに相談することが望ましいだろう。毅然とした対応を進めるにあたっては、詳細な記録をとることが勧められる。会話の録音や電子メールのやりとりについて確実に保管しておくべきである。

4 遺失物届及び盗難被害届について

PC や記憶媒体の紛失、盗難により情報が漏えいする場合も考えられる。これらの場合、警察に遺失届、盗難の被害届を提出するにあたってはメーカー・製造番号・型式などがわかった場合に発見される可能性が比較的高くなる。これらの情報を普段から記録しておくことが必要である。また保証書があればこれら情報を提示する際の参考となる。

参考文献一覧

1 日本語文献

(1) 単行本

Kevin Mandia・Chris Prosis 著 酒井順行・新井 悠監修 エクストラリス訳「インシデント レスポンス 不正アクセスの発見と対策」(翔泳社、2006)・(酒井ら，2006)

中島信一郎・青木耕一「企業自治体のための個人情報流出事故対応マニュアル」(ぎょうせい、2007)・(中島ら，2007)

大塚和成・滝川宣信・藤田和久「決定版 企業コンプライアンス体制のすべて」(きんざい，2004)

国廣正・五味祐子「なぜ企業不祥事はなくなるのか-危機に立ち向かうコンプライアンス」(日本経済新聞社，2005)

東京商工会議所 「危機管理対応マニュアル 「情報開示力」が企業の危機を救う!」(サンマーク出版，2005)・(東京商工会議所，2005)

白井 邦芳「ケーススタディ 企業の危機管理コンサルティング」(中央経済社、2006)

田中 辰巳「企業危機管理 実戦論」(文藝春秋、1999)

石川慶子「マスコミ対応緊急マニュアル」(ダイヤモンド社、2004)・(石川，2004)

中島茂「その『記者会見』間違っています!」(日本経済新聞出版社、2007)・(中島，2007)

(2) 個別論文

独立行政法人 情報処理推進機構 及び NRI セキュアテクノロジーズ株式会社翻訳「コンピュータセキュリティインシデント対応ガイド」 米国立標準技術研究所による勧告
<http://www.ipa.go.jp/security/publications/nist/documents/SP800-61-J.pdf>
(NIST， SP800-61) J

原文は、Tim Grance・Karen Kent・Brian Kim “Computer Security Incident Handling

Guide-Recommendations of the National Institute of Standards and Technology” NIST special Publication 800-61 (以下、(NIST, SP800-61))

<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

独立行政法人 情報処理推進機構 及び NRI セキユアテクノロジーズ株式会社翻訳「IT システムにおける緊急時対応計画ガイド 米国国立標準技術研究所による推奨」

<http://www.ipa.go.jp/security/publications/nist/documents/SP800-34-J.pdf>

原文は、

Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas, “Contingency Planning Guide for Information Technology Systems”(NIST, 800-34)

<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

JPCER/CC「技術メモ - コンピュータセキュリティインシデントへの対応」

<http://www.jpCERT.or.jp/ed/2002/ed020002.txt>・(JPCER/CC, 2002)

JPCERT/CC「万が一の事態(インシデント)が起こった後の対応手順」

<http://www soi.wide.ad.jp/class/20030011/slides/20/10.html>・(JPCER/CC, 2003)

IETF「サイトセキュリティハンドブック」(RFC2196 日本語)

<http://www.ipa.go.jp/security/rfc/RFC2196-00JA.html>・(RFC, 1997)

大塚和成・竹内朗・田中克幸・鶴巻暁「個人情報流出対応にみる実践的リスクマネジメント」NBL 808、809、810、811、812号以下所収(商事法務、2005)・(大塚等, 2005)

(3) 報告書脱稿後に公開された資料

JPCERT/CC「組織内 CSIRT 構築支援マテリアル」

http://www.jpCERT.or.jp/csirt_material/

「コンピュータセキュリティインシデント対応チーム (CSIRT) のためのハンドブック」
(翻訳)

http://www.jpCERT.or.jp/research/2007/handbook_gaiyou.html

2 英語文献

(1) オンライン参考文献 (代表的なもの)

Georgia Killcrece , Klaus-Peter Kossakowsk , Robin Ruefle , Mark Zajicek
“ Organizational Models for Computer Security Incident Response Teams (CSIRTs) ”
<http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb001.pdf>

Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)
http://www.cert.org/csirts/csirt_faq.html

Electronic Crime Scene Investigation: A Guide for First Responders
<http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>

RFC 3227: Guidelines for Evidence Collection and Archiving
<http://www.ietf.org/rfc/rfc3227.txt>

(2) その他

その他の参考文献については、独立行政法人 情報処理推進機構 及び NRI セキュアテクノロジー株式会社翻訳「コンピュータセキュリティインシデント対応ガイド」 米国立標準技術研究所による勧告の「付録 G オンラインのツールとリソース」所収の各資料等を参照のこと。