# フィッシング対策に関する事業者調査
# 報告書

2008年6月

フィッシング対策協議会

# 目　次

# 調査概要

**■調査目的**　フィッシング詐欺に対する事業者側の対策の現状と動向を踏まえた、フィッシング対策協議会及び事業者における効果的施策検討に資することを目的とした、フィッシング対策状況に関するアンケート調査を実施した。

**■調査内容**　調査項目は、フィッシング被害の有無及び被害認知経路・被害状況、フィッシング対策の有無及びその種類など。
詳細は巻末の調査票を参照。

**■調査対象者**　フィッシング被害の対象となる事業者
（金融機関、インターネットバンキング事業者、クレジットカード事業者、電子商取引・オークション事業者等）

**■調査方法**　郵送調査（一部メール調査）

**■調査期間**　2007年11月7日(水)～2007年12月17日(月)
調査協力依頼電話架電期間⇒2007年11月7日(水)～2007年11月16日(金)
調査票発送及び回収期間⇒2007年11月28日(水)～2007年12月17日(月)

**■発送数・サンプル数・回収率**

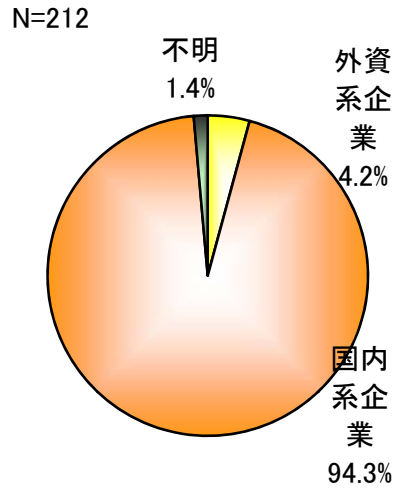
| | 全体 | メール | | 郵送 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 銀行 | 計 | 証券会社 | クレジットカード | その他金融機関（消費者金融・信用金庫等） | 通信販売 | その他 | 無回答 |
| 発送数 | 665件 | 187件 | 187件 | 478件 | 57件 | 41件 | 239件 | 120件 | 21件 | − |
| サンプル数 | 212件 | 89件 | 89件 | 123件 | 11件 | 8件 | 81件 | 13件 | 7件 | 3件 |
| 回収率 | 31.9% | 47.6% | 47.6% | 25.7% | 19.3% | 19.5% | 33.9% | 10.8% | 33.3% | − |

**■調査実施機関**　株式会社ベルシステム24

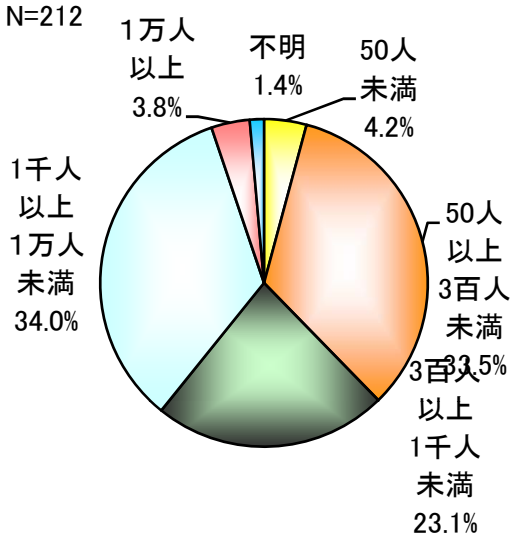
# 対象者属性

# 対象者属性

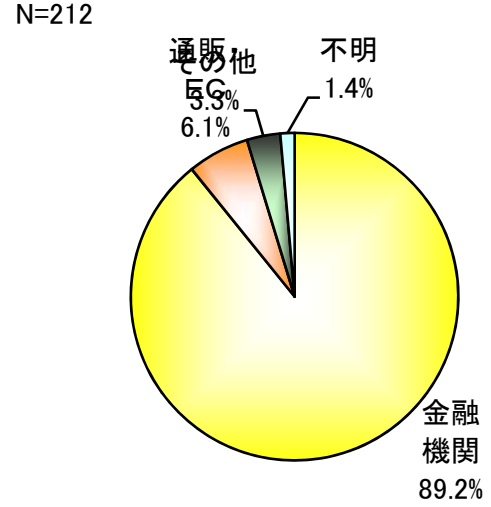
【会社形態】



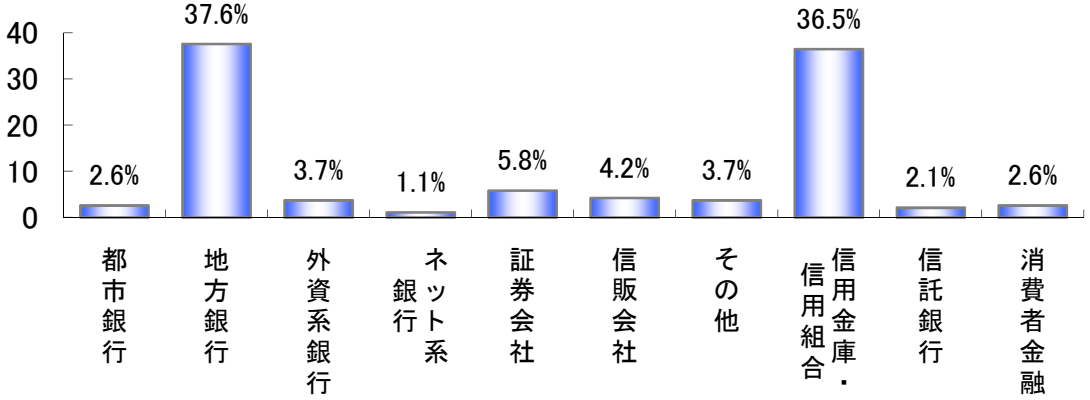

【事業規模】




【業種形態】



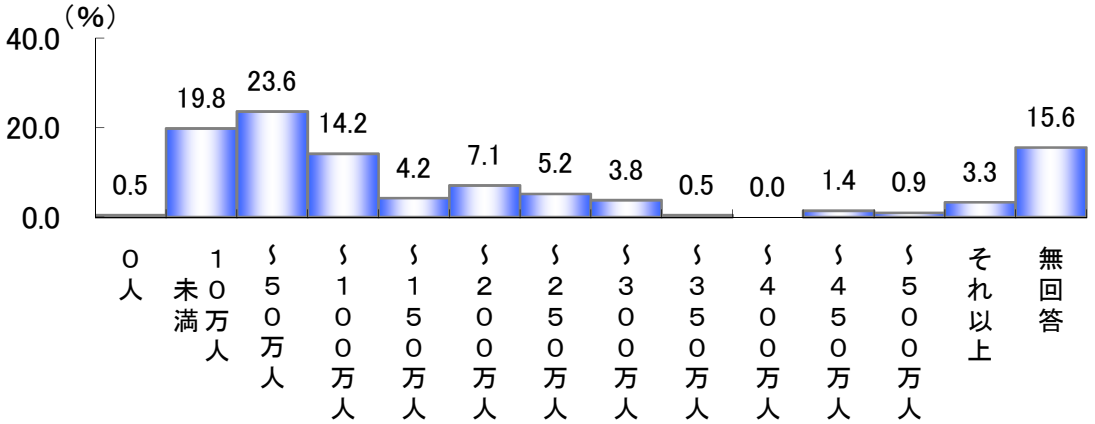

【金融機関の会社区分】 N=189



# 対象者属性

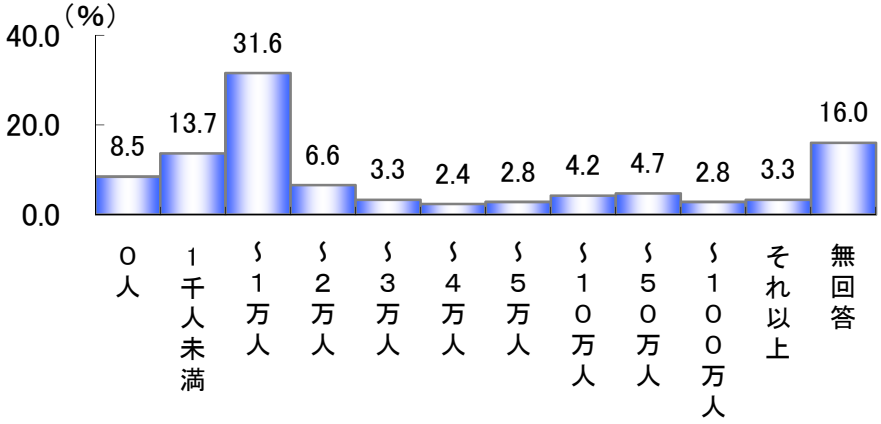
**【顧客規模】** N=212

平均「227．2万人」※




**【ネット利用顧客規模】** N=212

平均「36．8万人」※



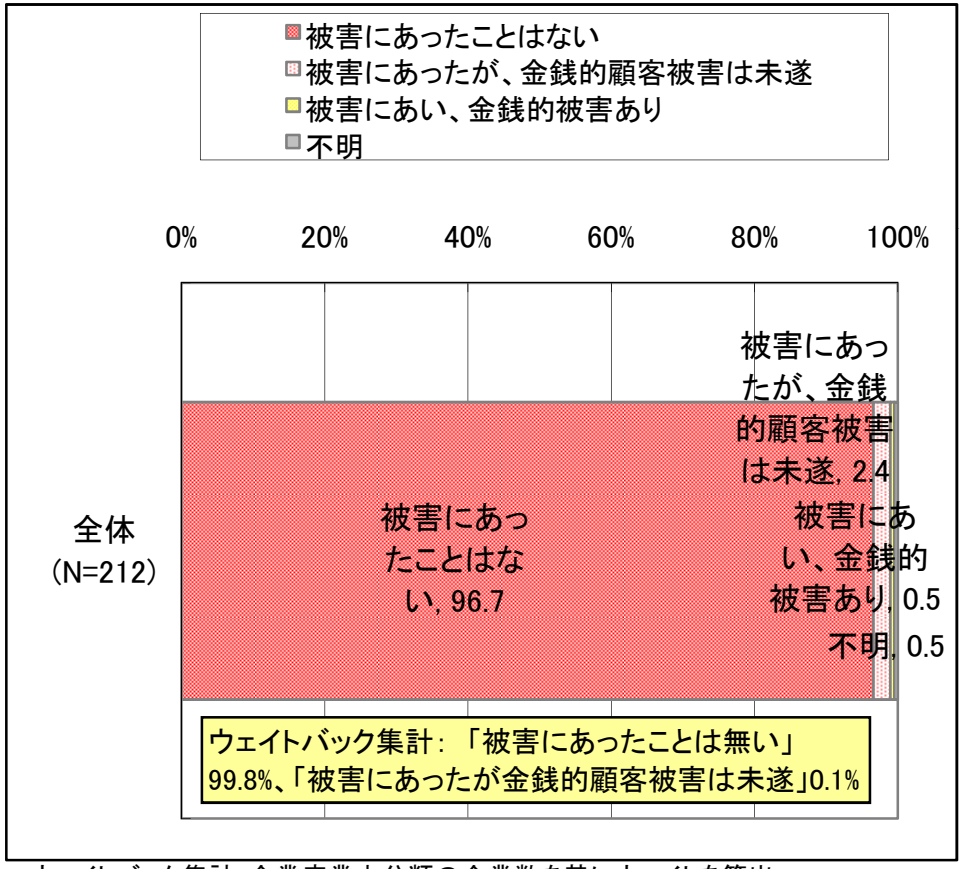

※0を含む（無回答は含まない）。

# 各論

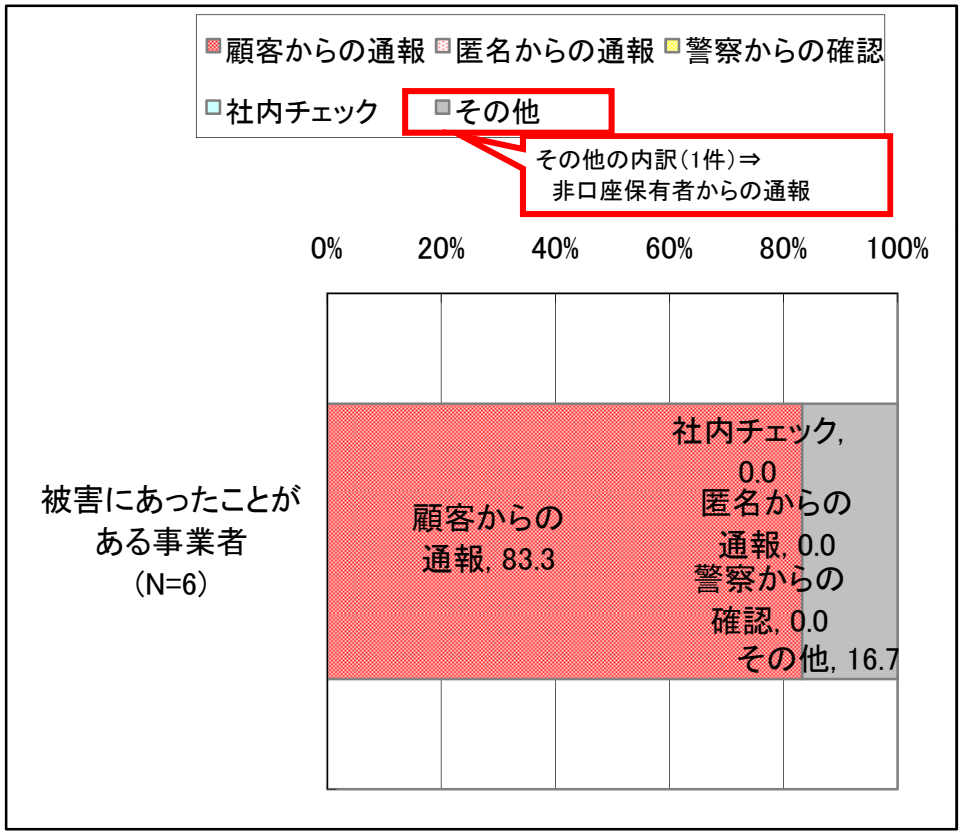
# 1.被害状況（Q1）及び被害認知経路（Q1-1）

被害状況
◆ほとんどの事業者が「被害にあったことはない」（96.7%）としているが、「被害にあったが、金銭的顧客被害は未遂」（2.4%（5件））、「被害にあい、金銭的被害あり」（0.5%（1件））という事業者も存在する。
被害認知経路
◆サンプル数が少数のため注意する必要があるが、「顧客からの通報」（83.3%（5件））が認知経路のおよそ8割を占めている。「匿名からの通報」「警察からの確認」「社内チェック」による被害認知はなかった。

■被害状況(Q1)




■被害認知経路(Q1-1)



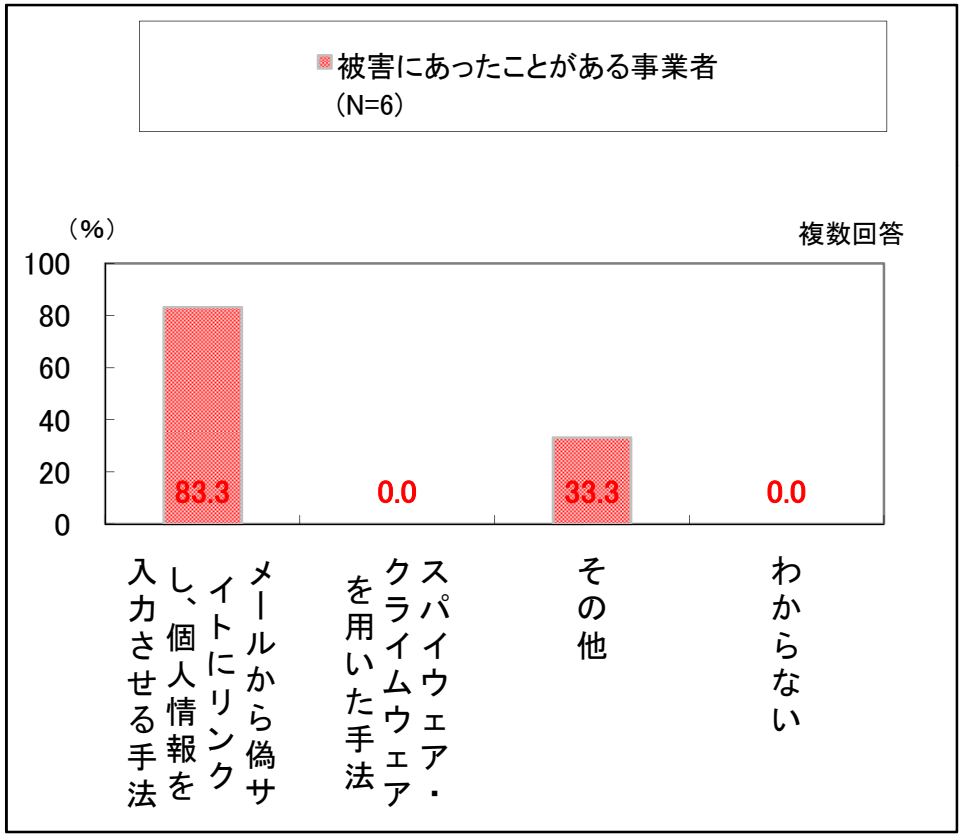

ウェイトバック集計：企業産業中分類の企業数を基にウェイトを算出。
（銀行業を0.1、EC・通販サイトを0.5、その他を99.4）回答にウェイトを乗じて、修正値を算出した。

※サンプル数が少数のため注意する必要がある。

# 2.被害にあったフィッシング手法(Q1-2)及び被害の搾取対象(Q1-3)

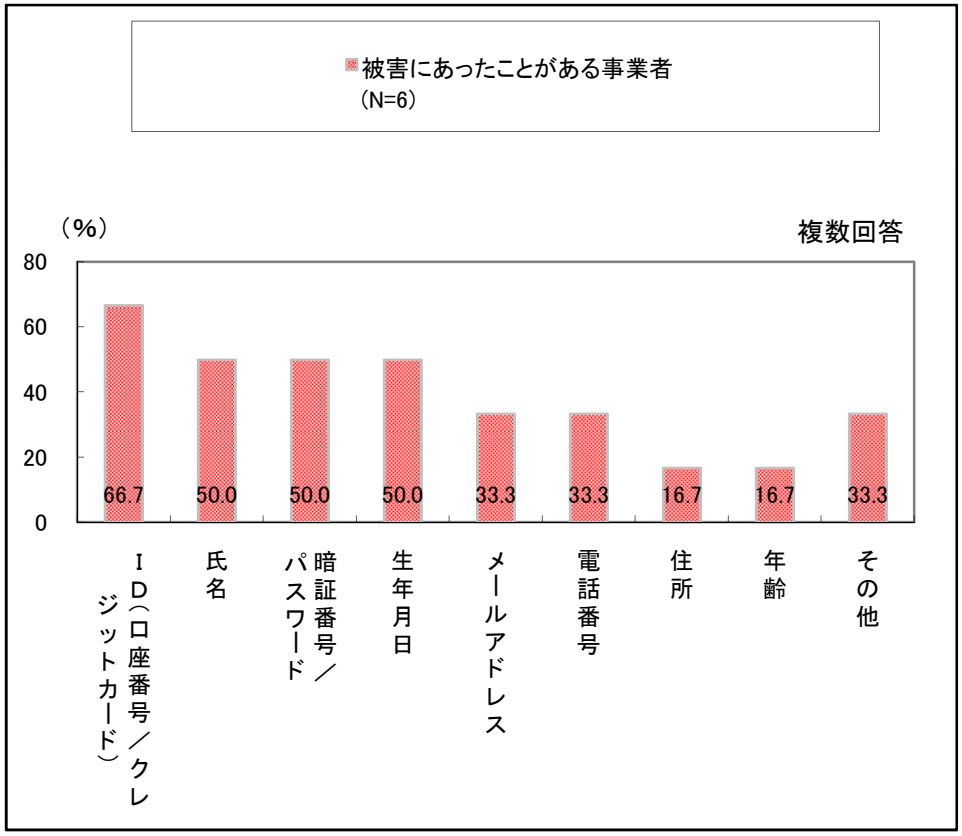
◆被害にあったフィッシング手法
「メールから偽サイトにリンクし、個人情報を入力させる手法」(83.3%(5件))が8割を占める。
◆被害の搾取対象
「ID」(66.7%(4件))が最も高く6割半ば。「氏名」「暗証番号/パスワード」「生年月日」が半数で続く。

■被害にあったフィッシング手法(Q1-2)




※サンプル数が少数のため注意する必要がある。

■被害の搾取対象(Q1-3)

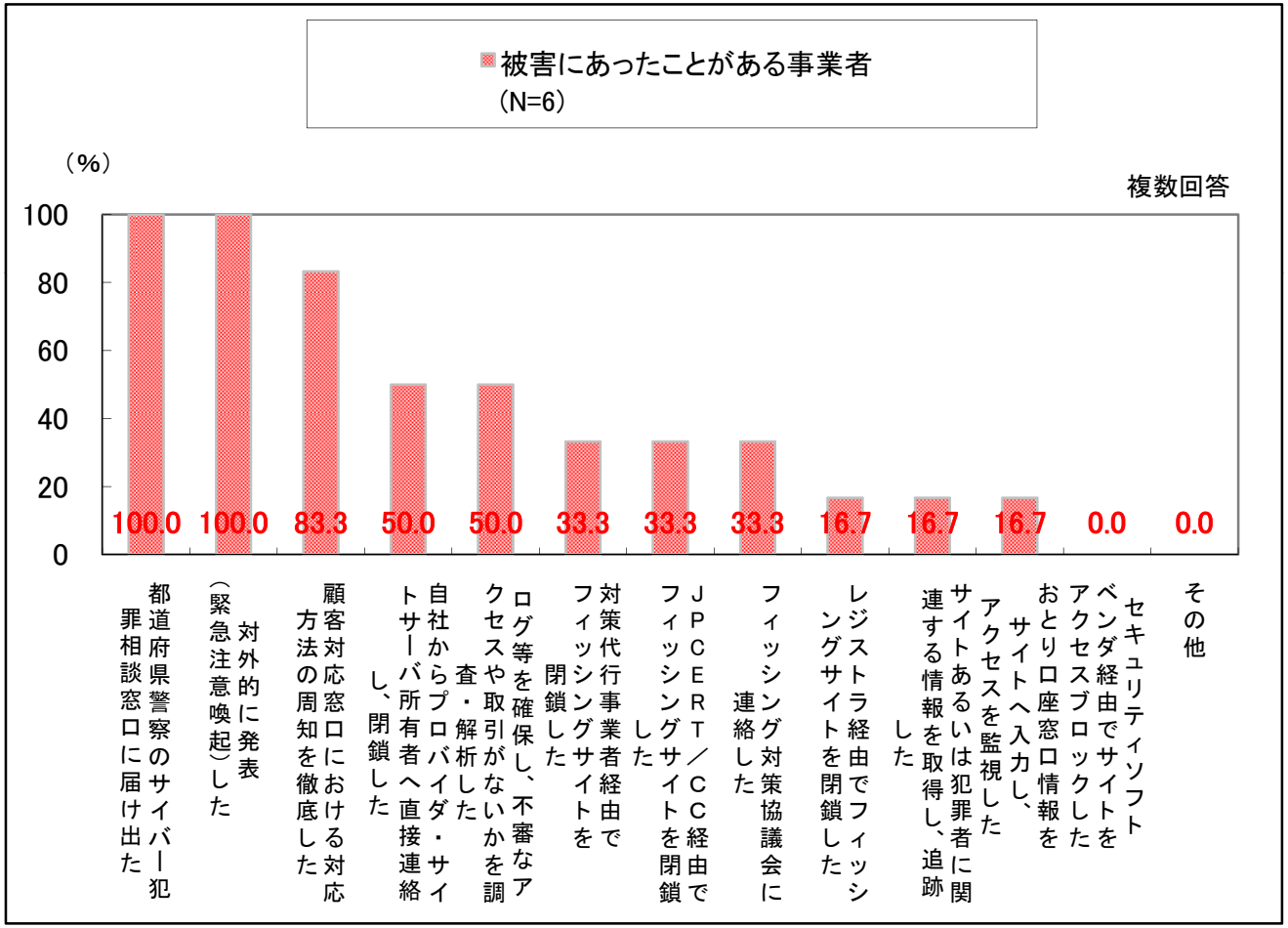



※サンプル数が少数のため注意する必要がある。

# 3.被害にあった際の対応（Q1-4）及び発表方法（Q1-4-1）

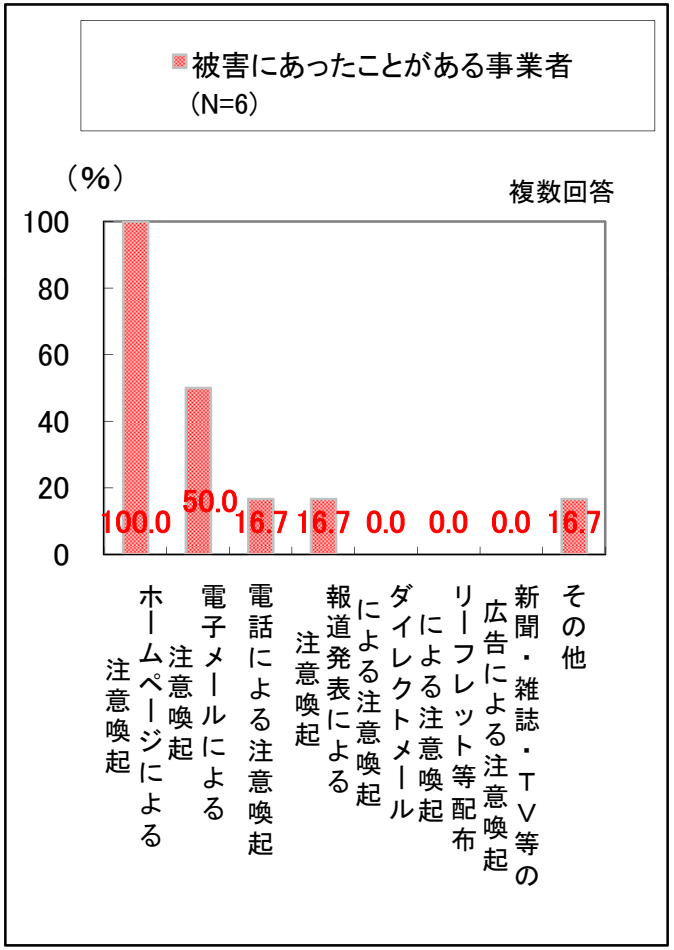
◆被害にあった際の対応
「都道府県警察のサイバー犯罪相談窓口に届け出た」「対外的に発表した」が100%と、どの事業者でも警察に届出をし、対外的に発表を行っている。また、「顧客対応窓口における対応方法の周知を徹底した」（83.3%）も8割を占め、発表後の対策を行っている様子がうかがえる。
◆発表方法
どの事業者においても「ホームページによる注意喚起」（100%）をしており、「電子メールによる注意喚起」が半数。

■被害にあった際の対応(Q1-4)




※サンプル数が少数のため注意する必要がある。

■発表方法(Q1-4-1)

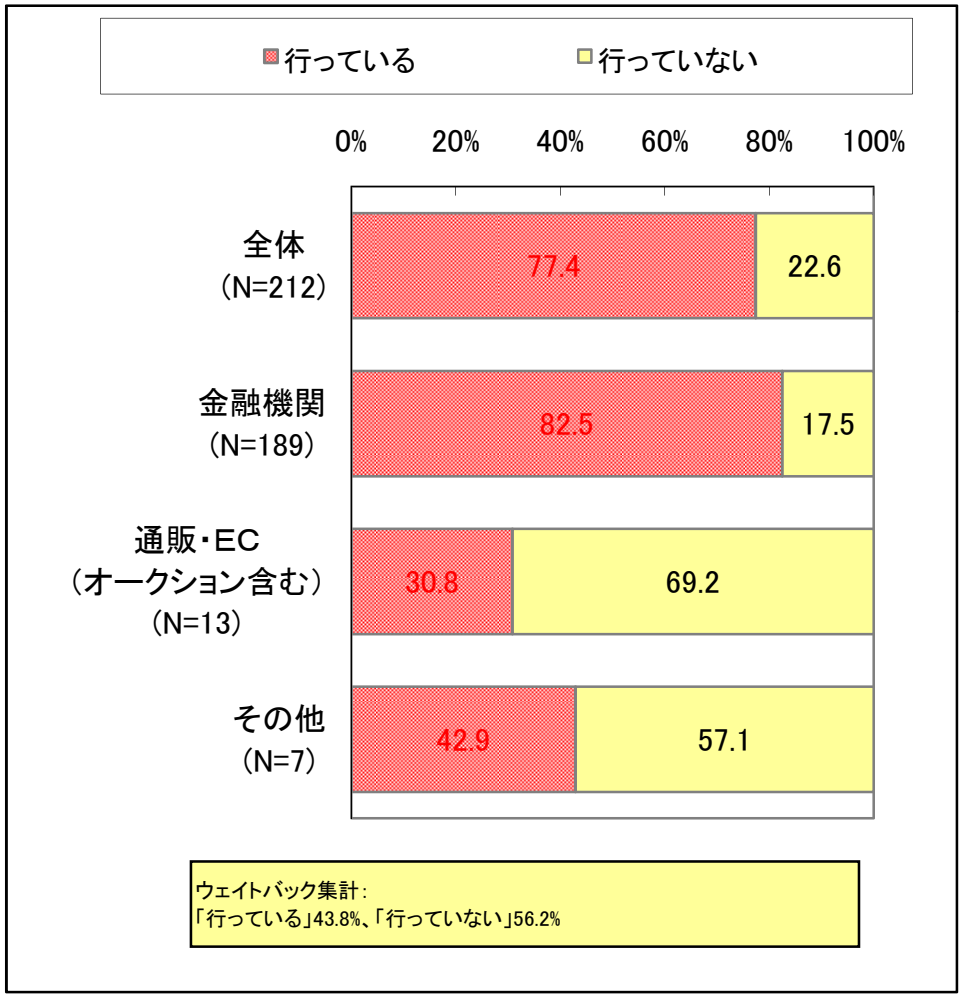



※サンプル数が少数のため注意する必要がある。

# 4.被害を未然に防ぐための注意喚起（Q2）

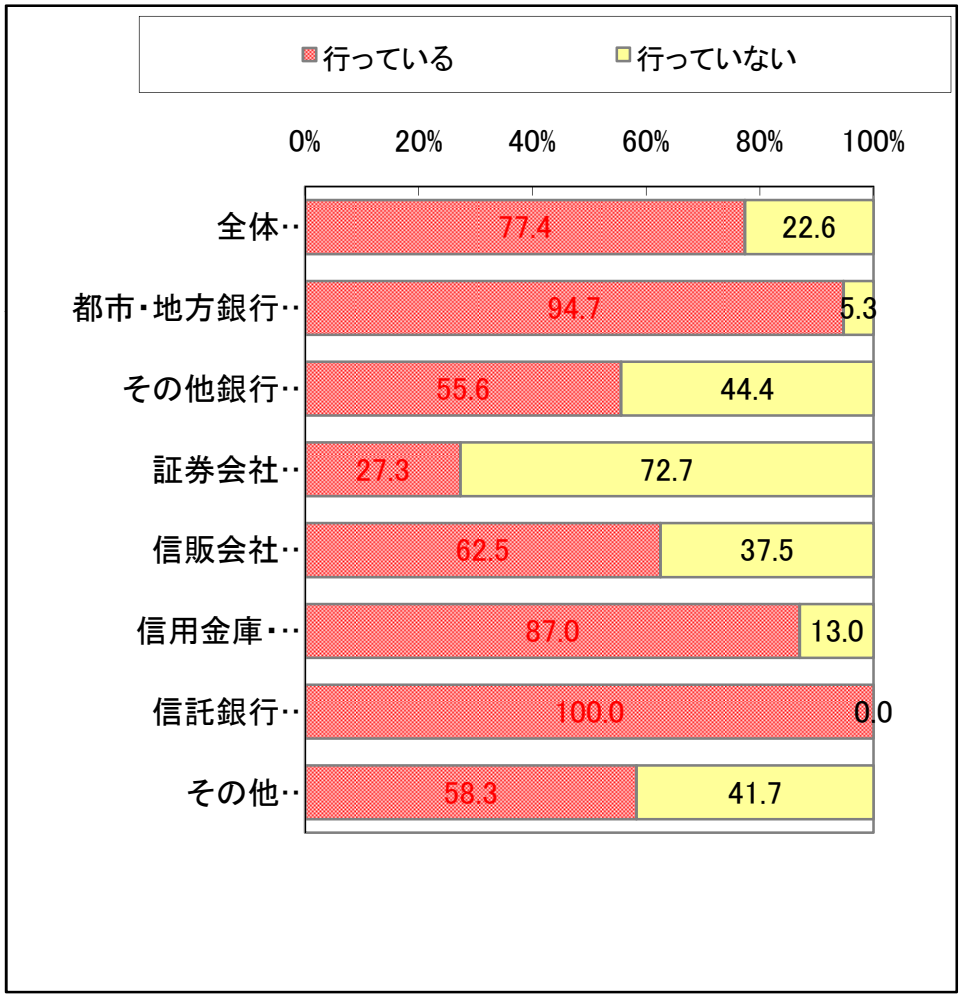
◆全体では、被害を未然に防ぐための注意喚起を「行っている」は77.4%と8割近い。
業種形態別にみると、【金融機関】では「行っている」（82.5%）が8割を占めて高い。サンプル数が少数（n<30）のため注意が必要ではあるが、【通販・EC】では「行っていない」（69.2%）がほぼ7割。
カテゴリ金融機関別にみると、サンプル数が少数（n<30）のため、注意が必要ではあるが、【都市・地方銀行】（94.7%）では9割以上、「信用金庫・信用組合」（87.0%）では9割近くが被害を未然に防ぐための注意喚起を「行っている」。

■被害を未然に防ぐための注意喚起（Q2） ①業種形態別構成比




ウェイトバック集計：
「行っている」43.8%、「行っていない」56.2%

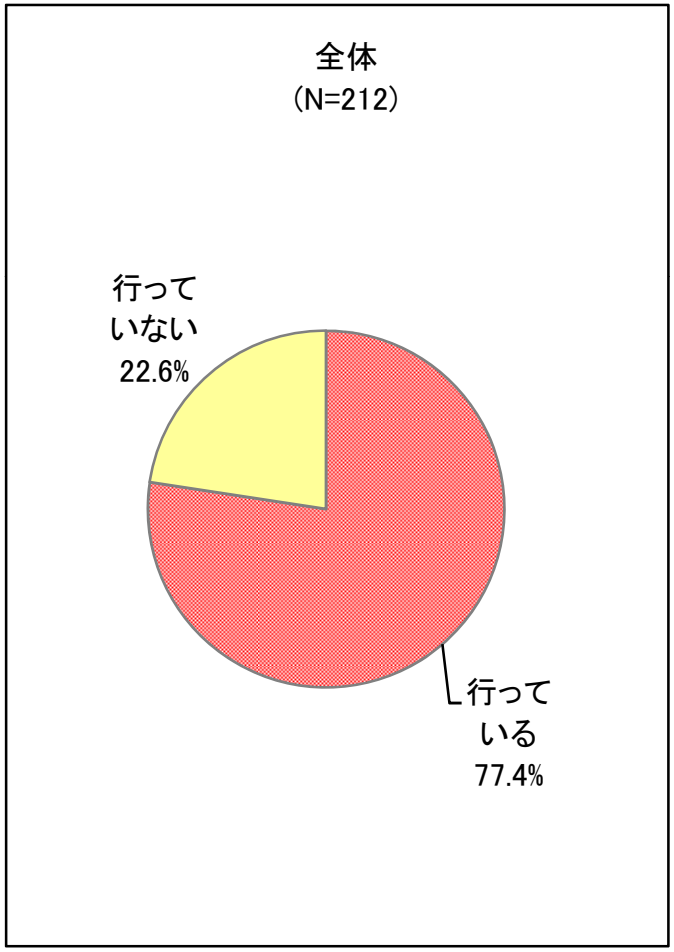
■被害を未然に防ぐための注意喚起（Q2） ②カテゴリ金融機関区分別構成比



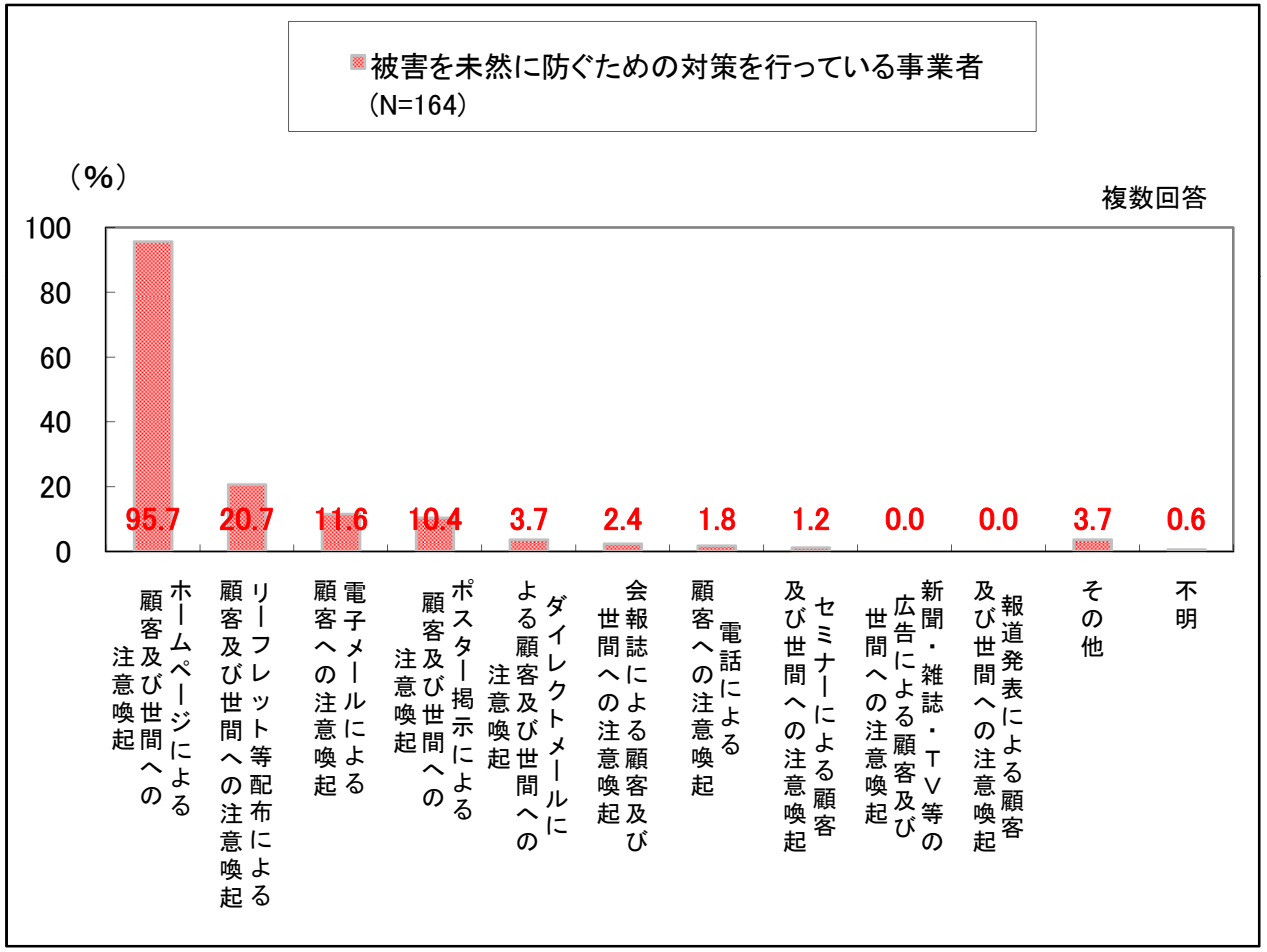
# 5.被害を未然に防ぐための注意喚起(Q2)及び顧客啓発の方法(Q2-1)

◆被害を未然に防ぐための注意喚起
「行っている」が77.4%と8割近くを占める。
◆顧客啓発の方法
「ホームページによる顧客及び世間への注意喚起」(95.7%)が最も高く9割以上と、大多数の事業者で実施しており、他の方法を大きく引き離している。2位の「リーフレット等配布による顧客及び世間への注意喚起」(20.7%)は2割程度にとどまる。

■被害を未然に防ぐための注意喚起(Q2)



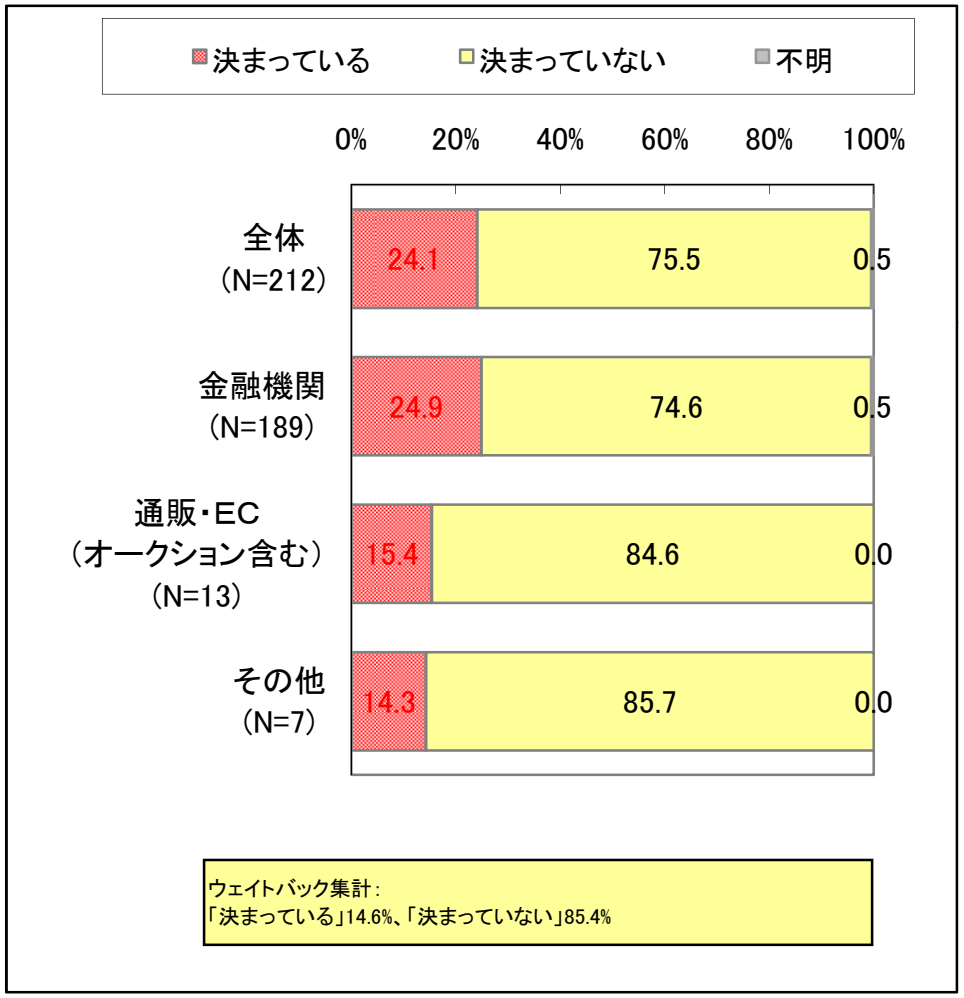

■顧客啓発の方法(Q2-1)



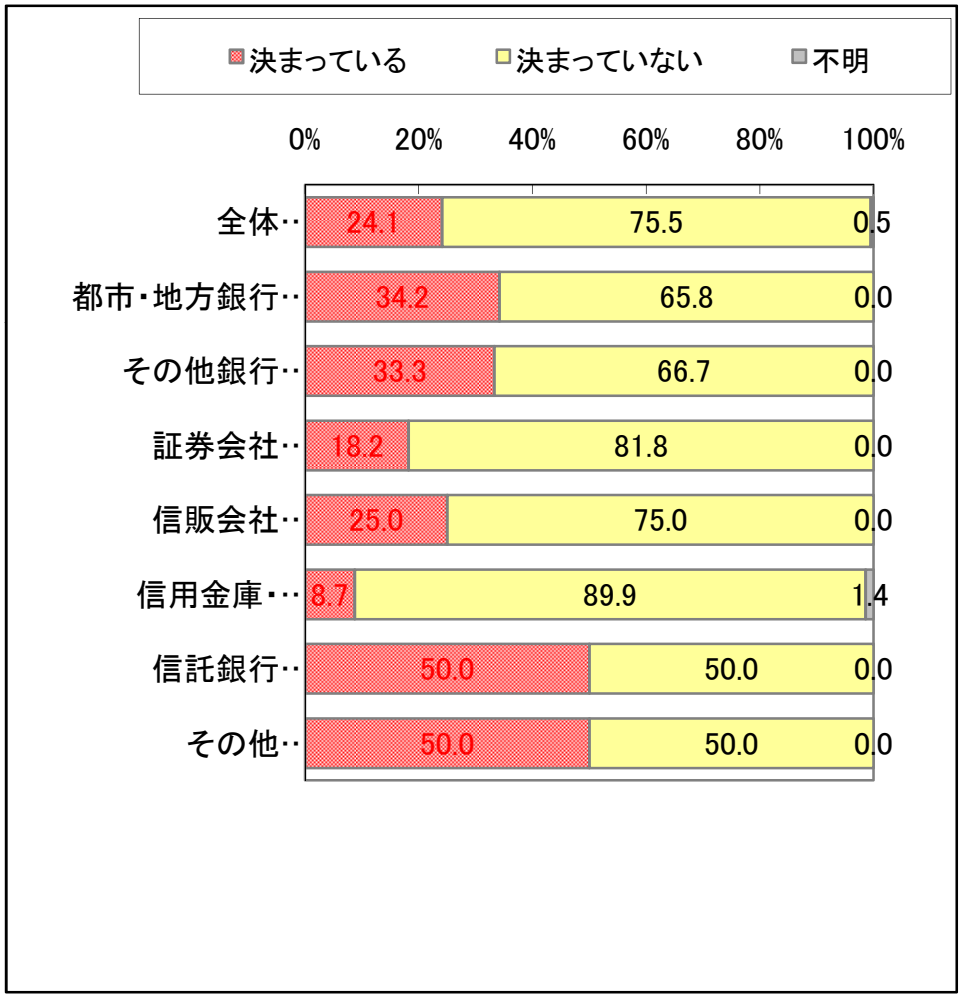
# 6.ブランド不正使用の対象となった場合の対策手順（Q3）

◆全体では、ブランド不正使用の対象となった場合の対策手順が「決まっている」（24.1%）は2割強にすぎず、7割以上が「決まっていない」（75.5%）としている。
業種形態別にみると、サンプル数が少数（n<30）のため注意する必要があるが、【金融機関】では「決まっている」（24.9%）が2割半と、【通販・EC】より高い。

■ブランド不正使用の対象となった場合の対策手順（Q3） ①業種形態別構成比



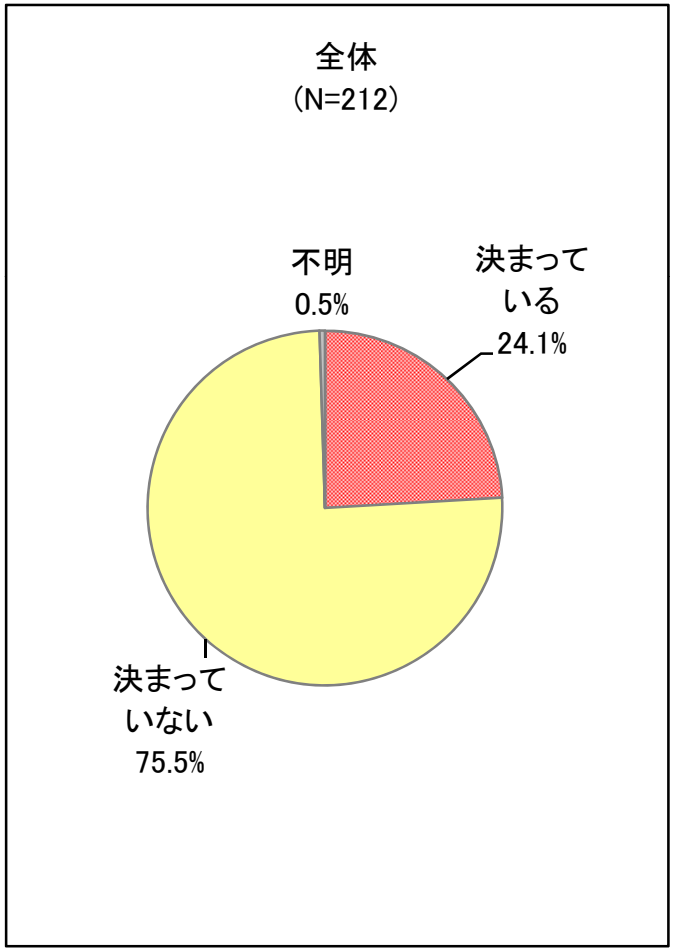

■ブランド不正使用の対象となった場合の対策手順（Q3） ②カテゴリ金融機関区分別構成比



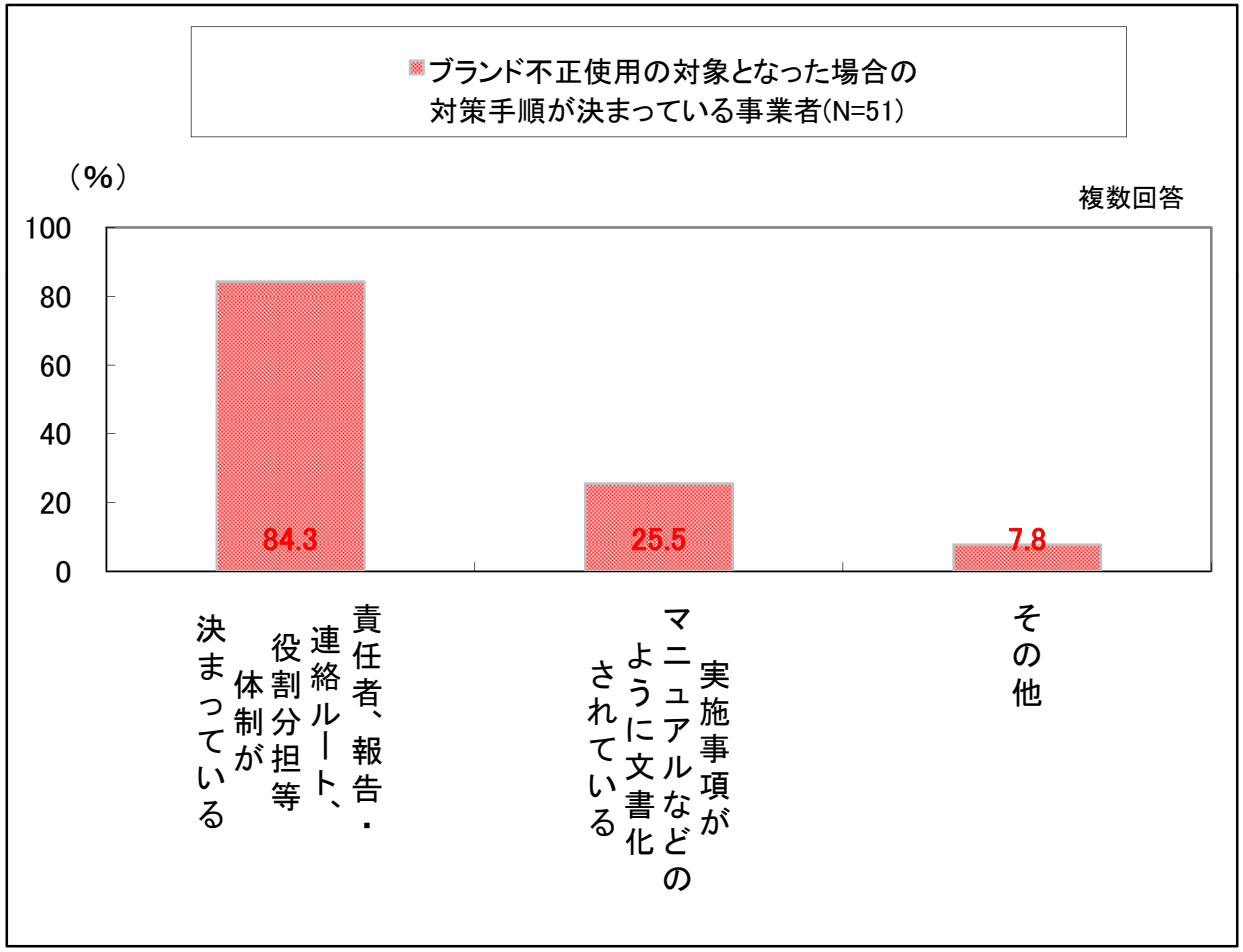
# 7.ブランド不正使用の対象となった場合の対策手順(Q3)及び決まっている対策手順(Q3-1)

◆ブランド不正使用対象となった場合の対策手順
「責任者、報告・連絡ルート、役割分担等体制が決まっている」(84.3%)が最も高く8割強と、次点の「実施事項がマニュアルなどのように文書化されている」(25.5%)を大きく引き離している。

■ブランド不正使用の対象となった場合の対策手順(Q3)



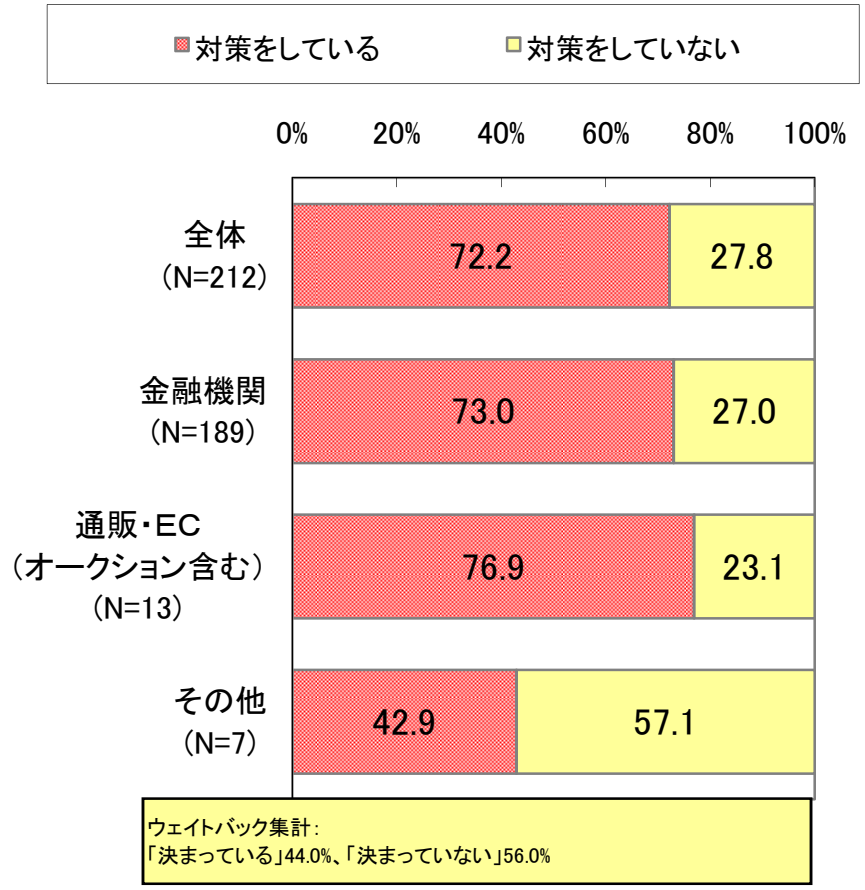

■決まっている対策手順(Q3-1)



# 8.被害防止の対策状況（Q4）

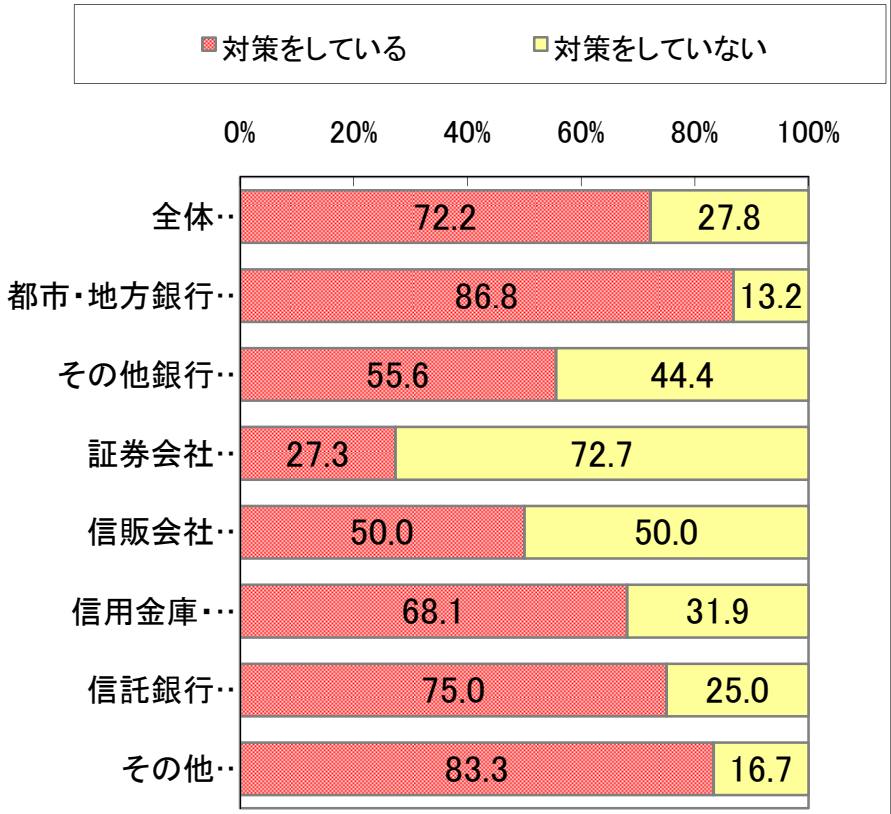
◆全体では、被害防止の「対策をしている」（72.2%）が7割を占める。
業種形態別にみると、【金融機関】は「対策をしている」が73.0%、【通販・EC】のそれ（76.9%）とあまり変わらない。
カテゴリ金融機関別にみると、【都市・地方銀行】は「対策をしている」（86.8%）が8割後半と他の金融機関より高い。【証券会社】は銀行や信用組合などに比べて、被害防止対策にあまり積極的ではない様子。※サンプル数が少数（n<30）の層は注意が必要。

■被害防止の対策状況（Q4） ①業種形態別構成比




※回答者にはネット利用者顧客を持たない（ネットサービスをしていない）事業者（8.5%）も含まれる。

■被害防止の対策状況（Q4） ②カテゴリ金融機関区分別構成比

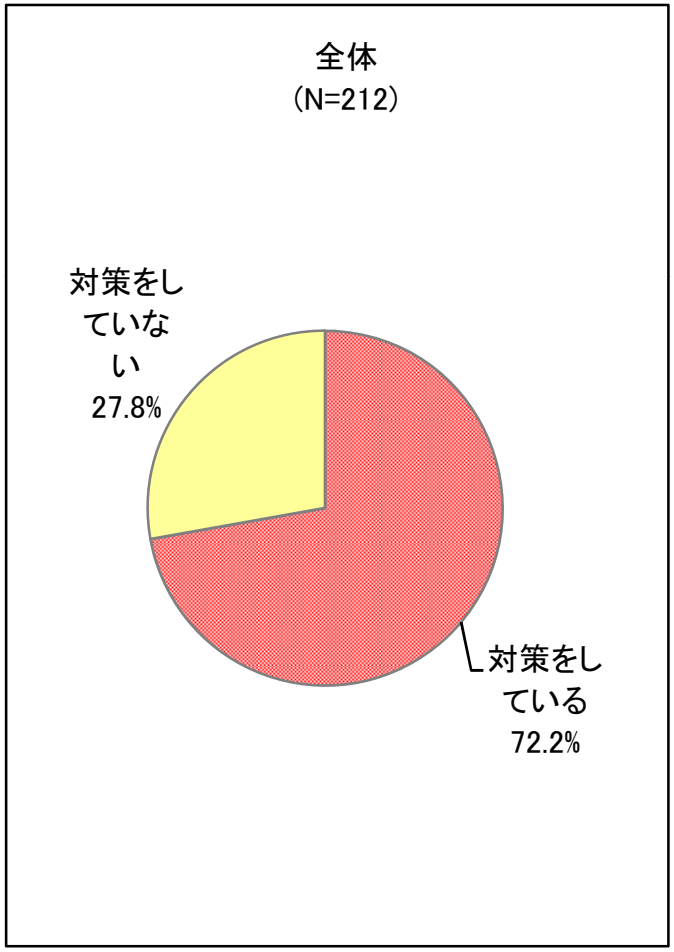



※回答者にはネット利用者顧客を持たない（ネットサービスをしていない）事業者（8.5%）も含まれる。

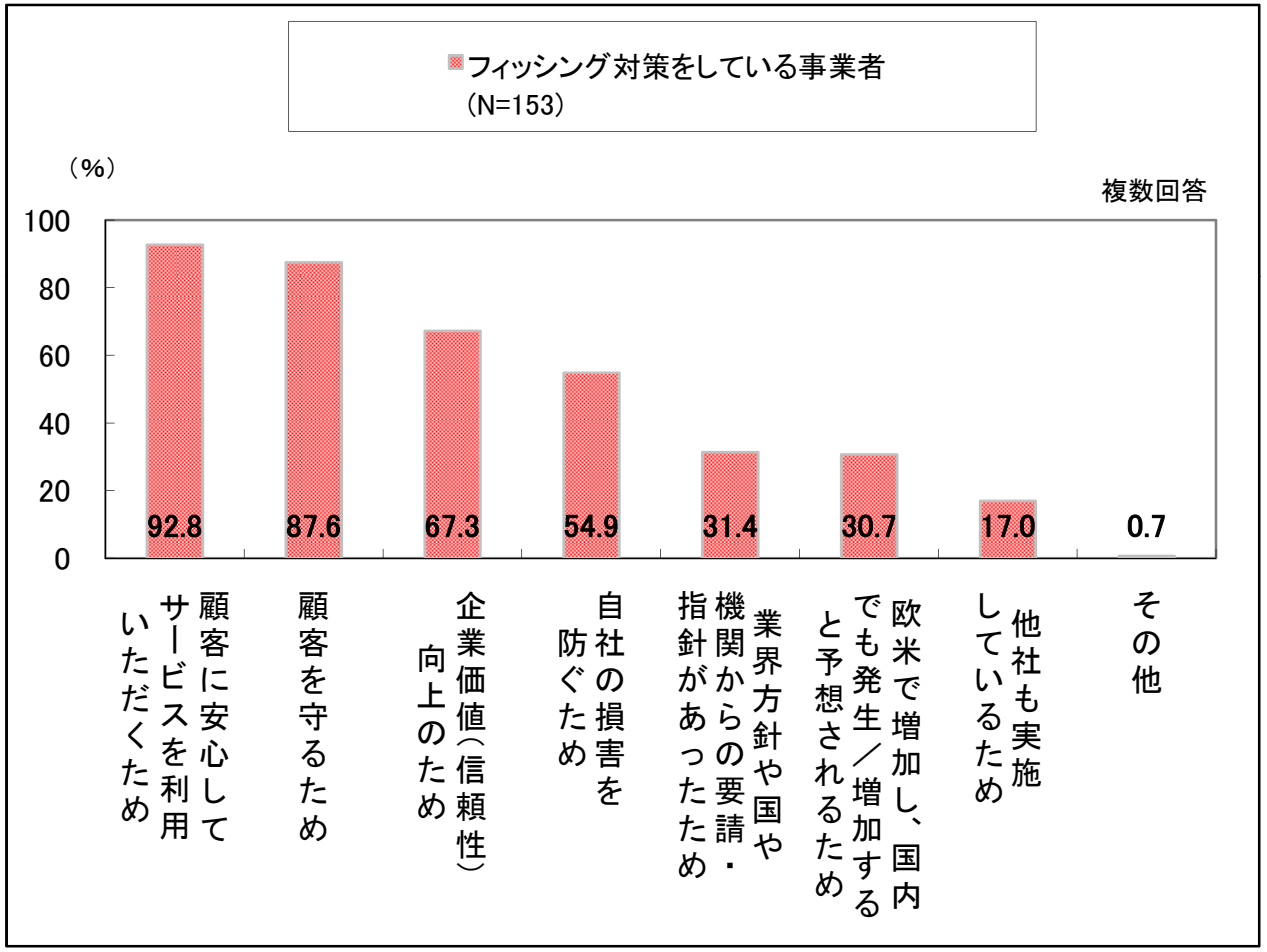
# 9.被害防止の対策状況（Q4）及び防止対策を行う理由（Q4-1）

◆防止対策を行う理由
「顧客に安心してサービスを利用いただくため」（92.8%）が9割以上と最も高く、「顧客を守るため」（87.6%）が9割近くで続く。「企業価値向上のため」「自社の損害を防ぐため」といった自己防衛策より、顧客を重視した企業活動としての意識が高いようである。

■被害防止の対策状況（Q4）



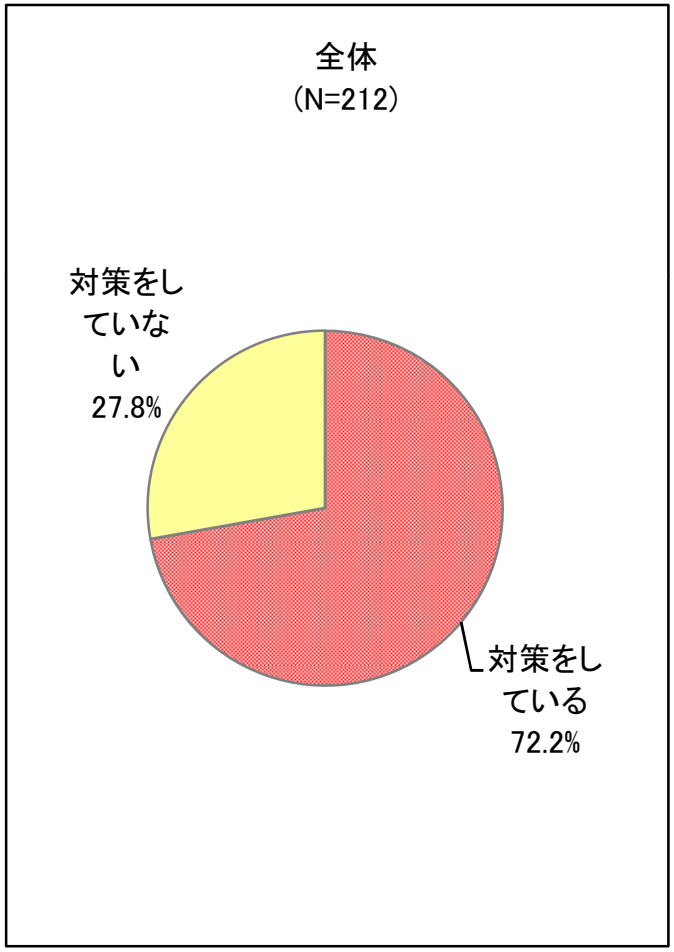

■防止対策を行う理由(Q4-1)



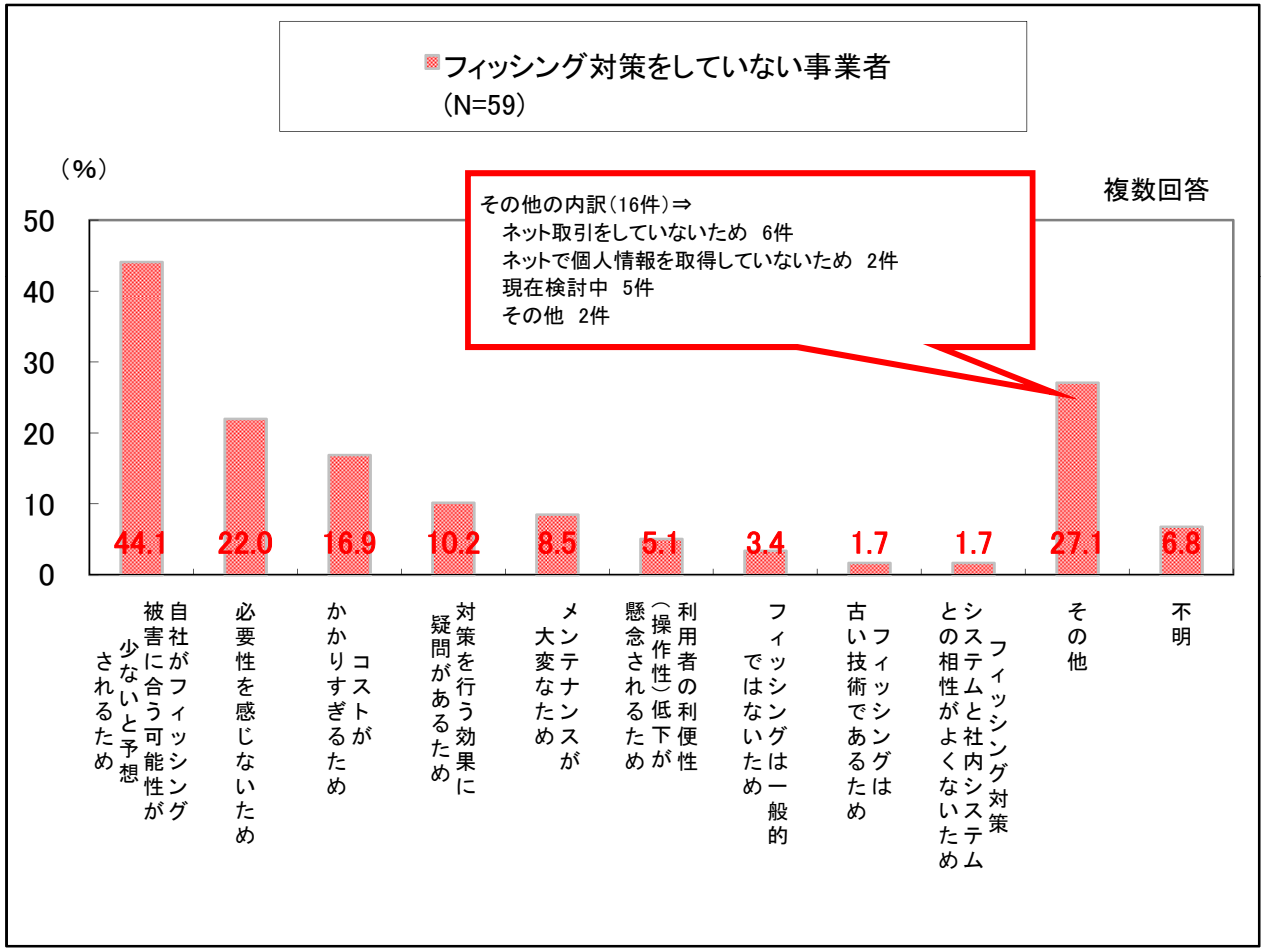
# 10.被害防止の対策状況（Q4）及び防止対策を行わない理由（Q4-2）

◆防止対策を行わない理由
「自社がフィッシング被害に逢う可能性が少ないと予想されるため」（44.1%）が4割強と最も高く、2位以下より20ポイント以上高い。被害に合う可能性がない、必要性を感じない、コストがかかりすぎるなど、費用対効果の面から対策を手控えているようである。

■被害防止の対策状況（Q4）



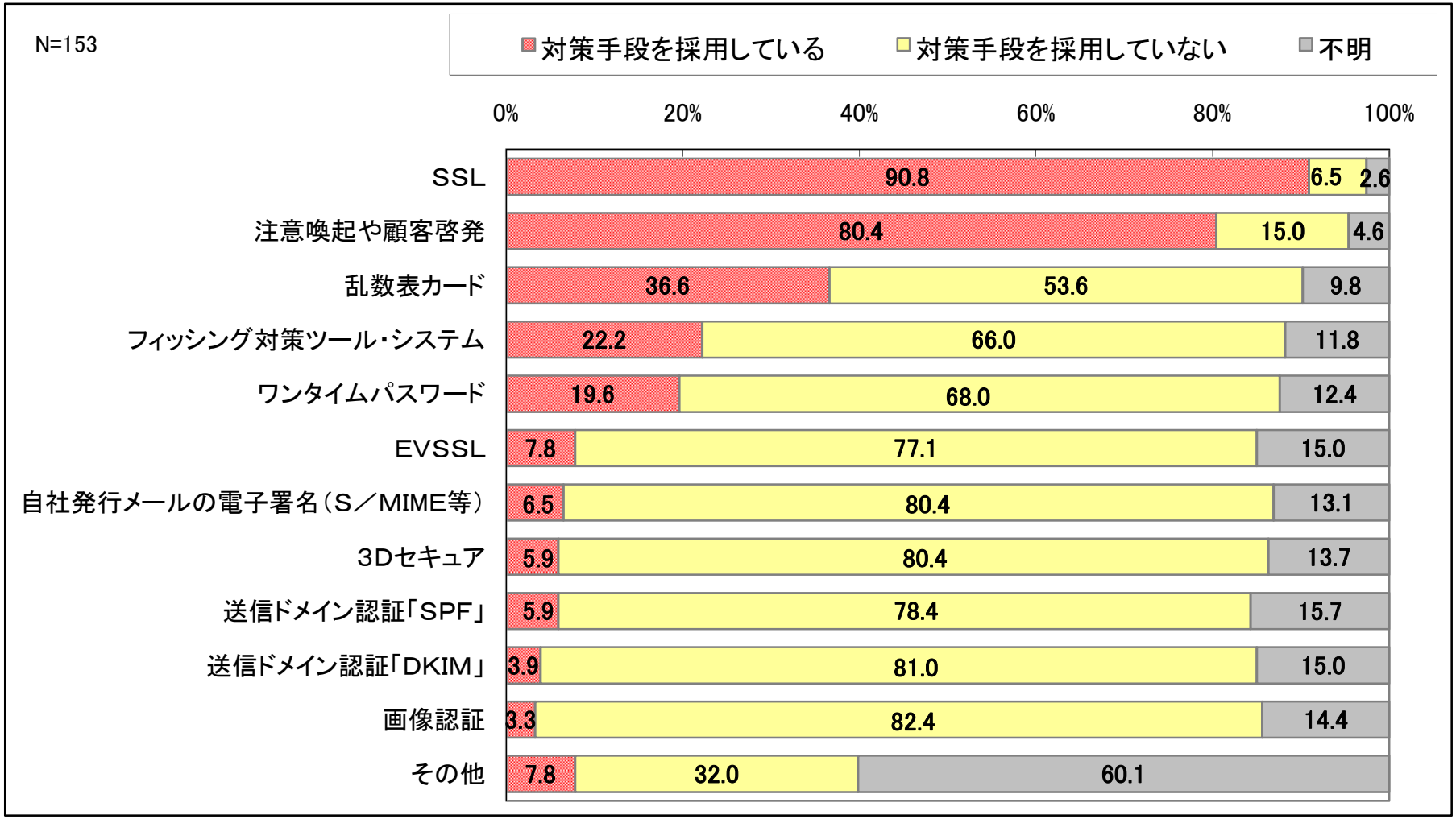

■防止対策を行わない理由(Q4-2)



# 11.採用している対策（Q4-3）

◆採用している対策
【SSL】（90.8%）が最も高く、9割と大多数の事業者が採用している。【注意喚起や顧客啓発】（80.4%）が8割で続き、それ以下を大きく引き離している。
【乱数表カード】（36.6%）は3割半ば、【フィッシング対策ツール・システム】（22.2%）、【ワンタイムパスワード】（19.6%）は2割程度で続く。

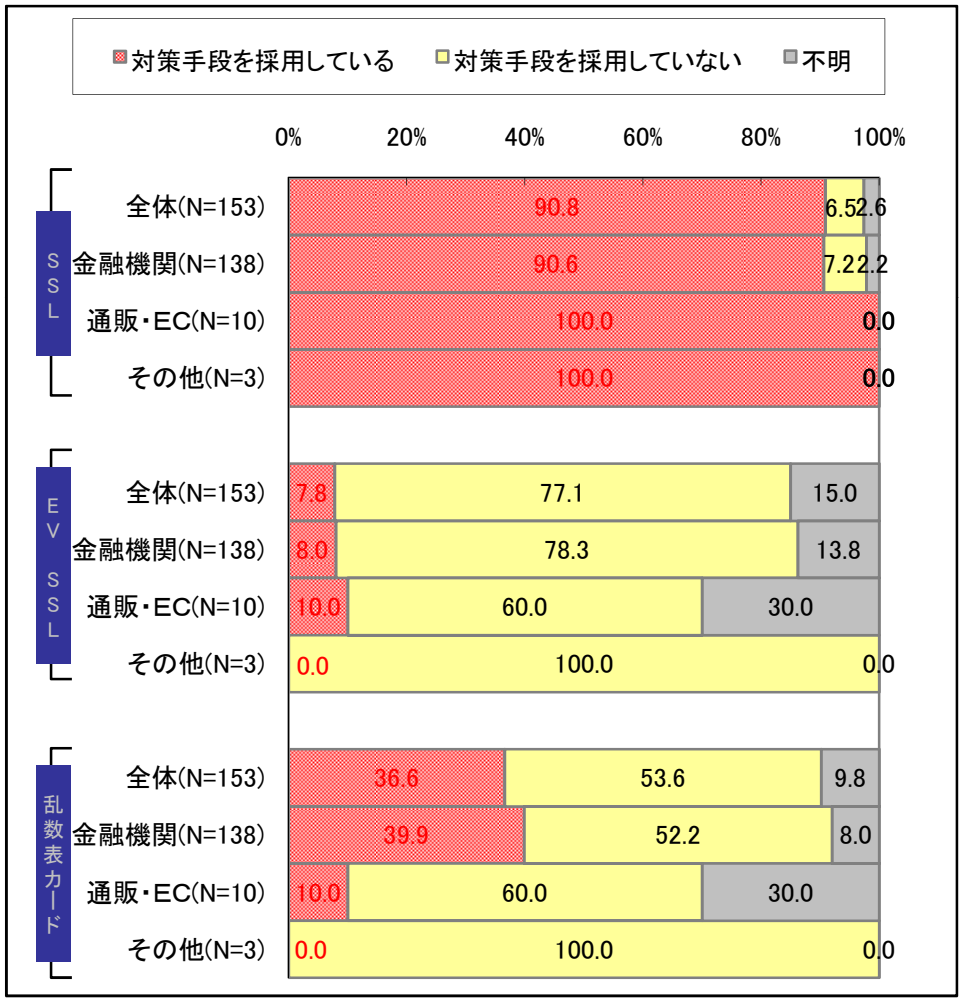
■採用している対策(Q4-3)



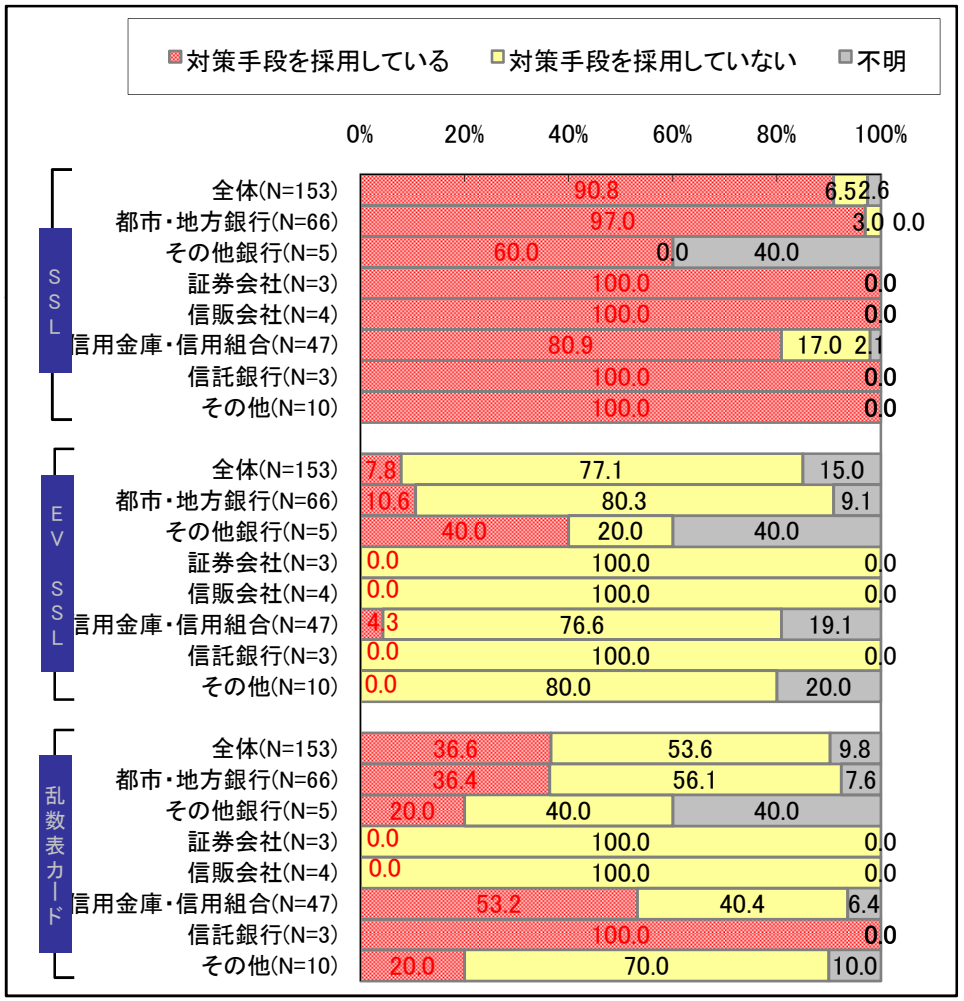
# 11.採用している対策（Q4-3）

業種形態別にみると、SSLを採用している事業者は9割を超え、非常に高い。また、乱数表カードでは、【金融機関】は「対策手段を採用している」（39.9%）が、【通販・EC】（10.0%）より高い。（サンプル数が少数（n<30）のため、注意が必要）
カテゴリ金融機関別にみると、SSLを採用している金融機関は、（n<30の層は、注意が必要）【その他銀行】【信用金庫・信用組合】を除き、ほぼ全事業者で採用している。乱数表カードでは、【信用金庫・信用組合】の「対策手段を採用している」（53.2%）は【都市・地方銀行】（36.4%）より高い。

■採用している対策(Q4-3) ①業種形態別構成比



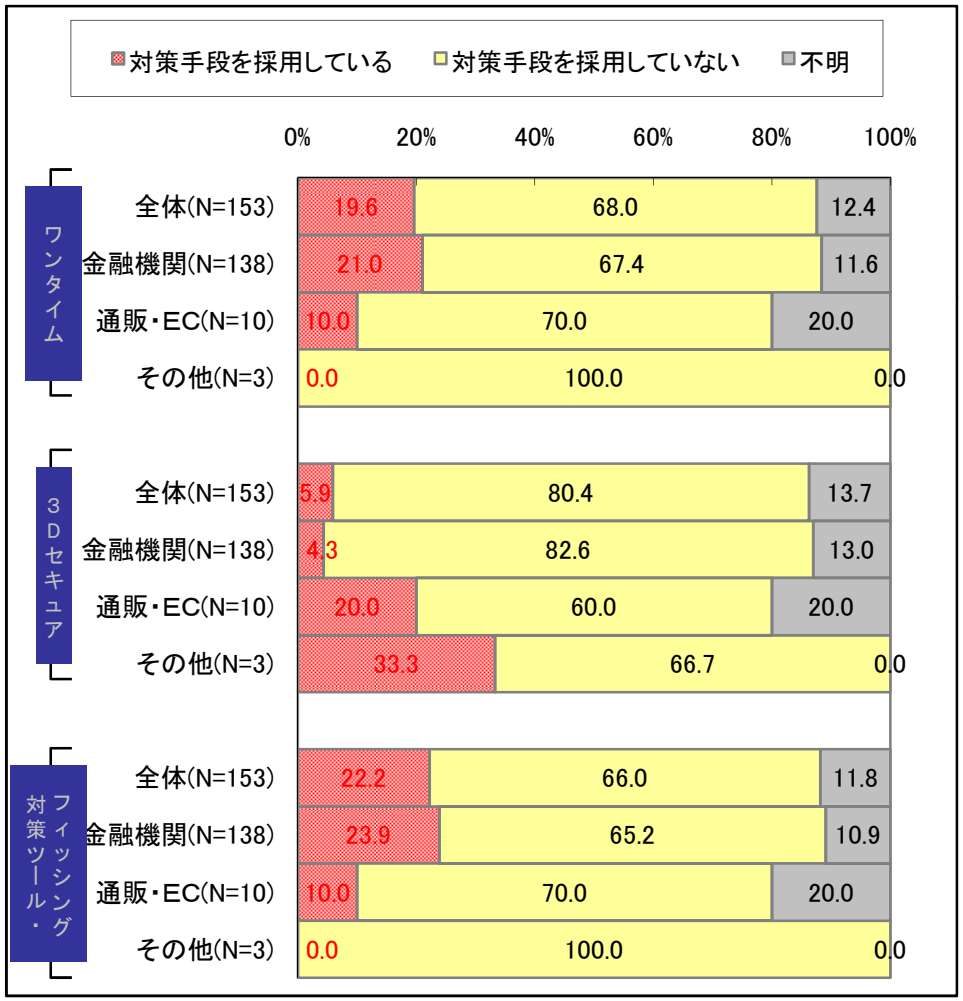

■採用している対策(Q4-3) ②カテゴリ金融機関区分別構成比



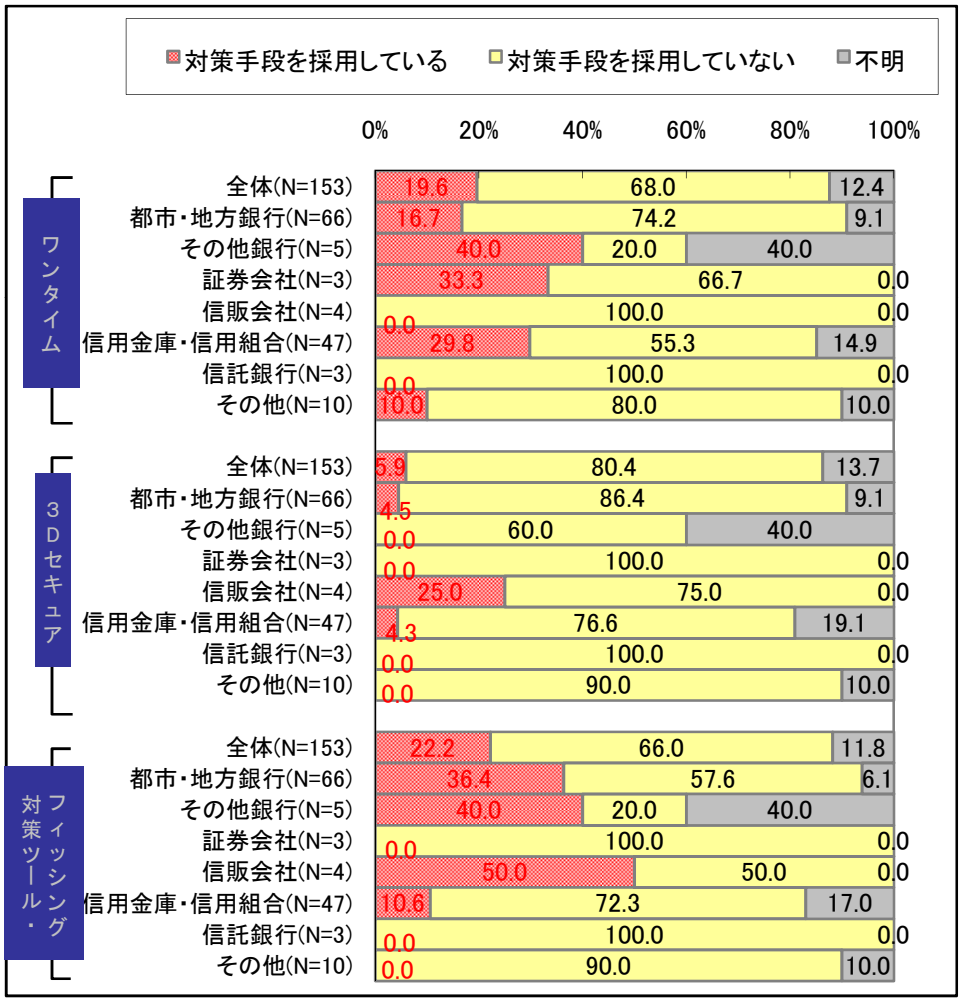
# 11.採用している対策（Q4-3）

業種形態別に「対策手段を採用している」をみると、ワンタイムパスワードでは【金融機関】（21.0%）が、3Dセキュアでは【通販・EC】「20.0%」が、フィッシング対策ツール・システムでは【金融機関】（23.9%）が他の業種より高い。しかし、サンプル数が少数（n<30）の層は注意が必要。
カテゴリ金融機関別に「対策手段を採用している」をみると、ワンタイムパスワードでは【信用金庫・信用組合】（29.8%）が【都市・地方銀行】（16.7%）より高い。逆に、フィッシング対策ツール・システムでは【都市・地方銀行】（36.4%）は【信用金庫・信用組合】（10.6）より高い。

■採用している対策(Q4-3) ①業種形態別構成比



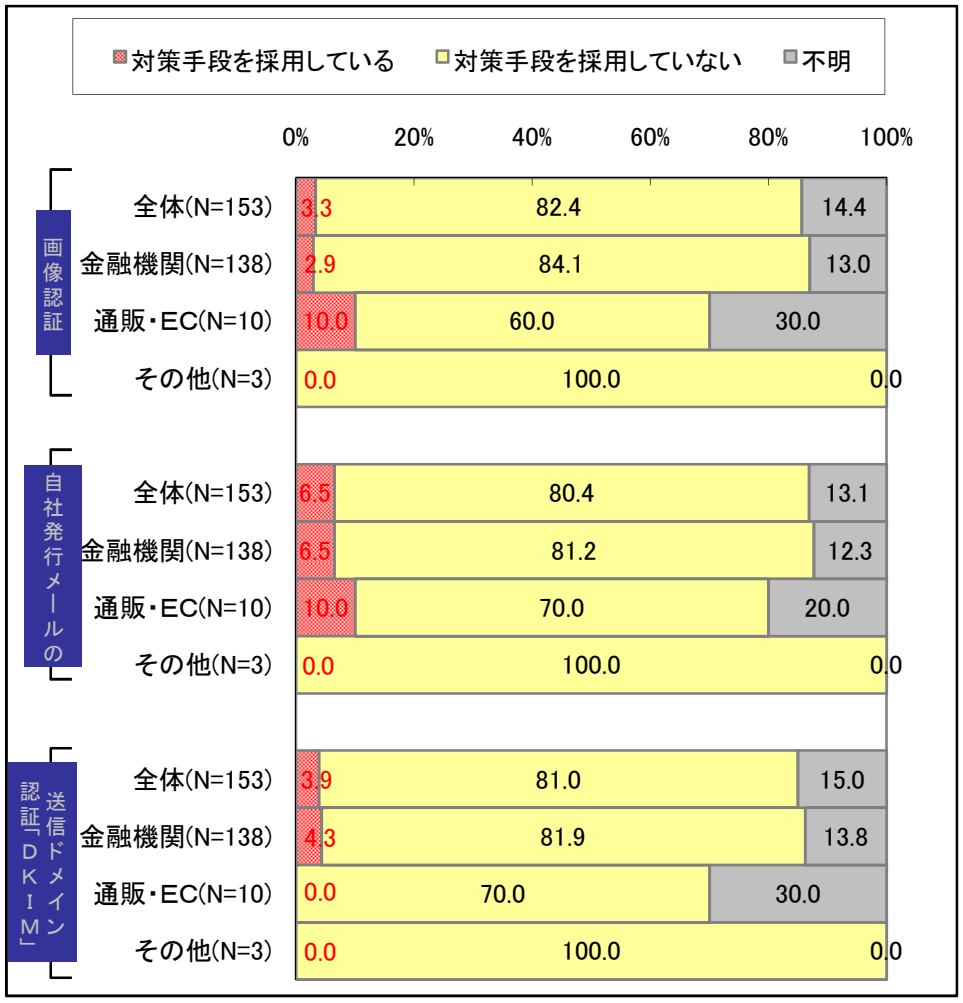

■採用している対策(Q4-3) ②カテゴリ金融機関区分別構成比



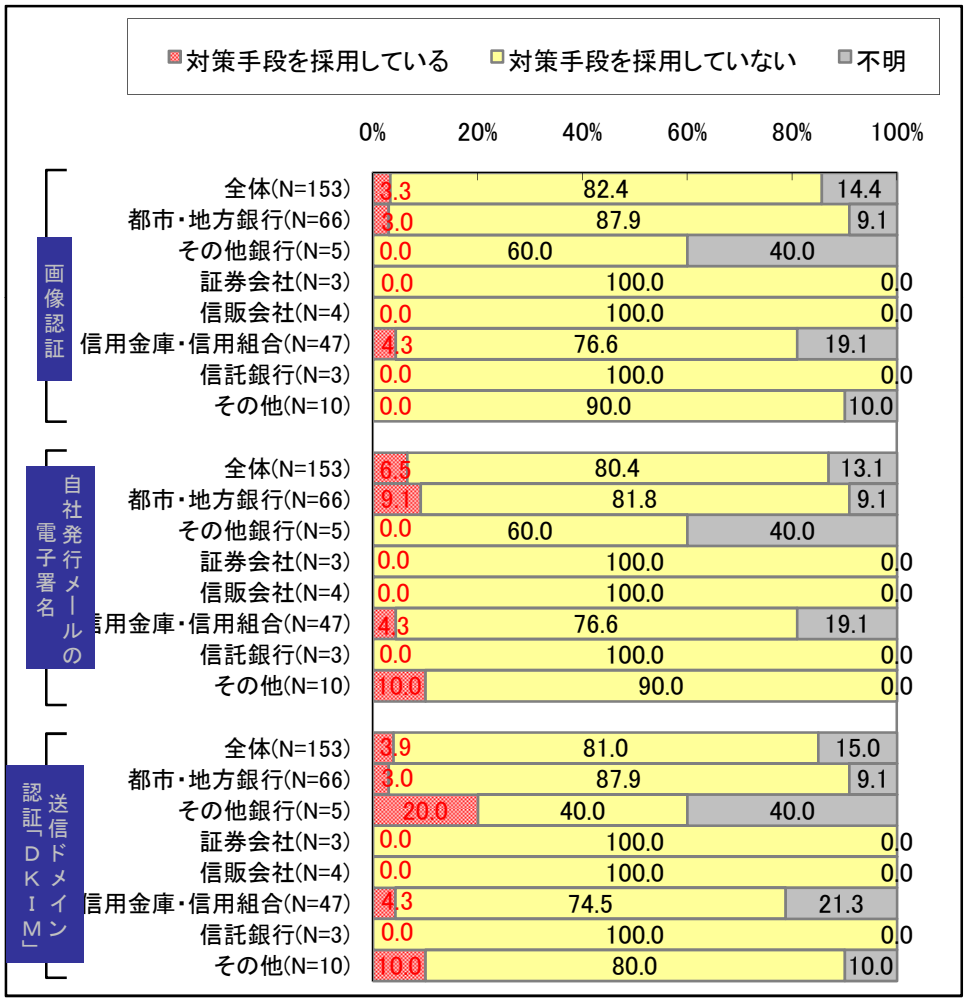
# 11.採用している対策（Q4-3）

業種形態別にみると、画像認証では、【通販・EC】は「対策手段を採用している」が他の業種よりも高い。送信ドメイン認証「KDIM」では、【金融機関】のみで「対策手段を採用している」。
カテゴリ金融機関別にみると、画像認証や自社発行メールの電子署名では、ほぼ、【都市・地方銀行】【信用金庫・信用組合】のみで「対策手段を採用している」。送信ドメイン認証「KDIM」でも同様の傾向にあり、【証券会社】【信販会社】【信託銀行】では、いずれの対策も採用していない。

■採用している対策(Q4-3) ①業種形態別構成比



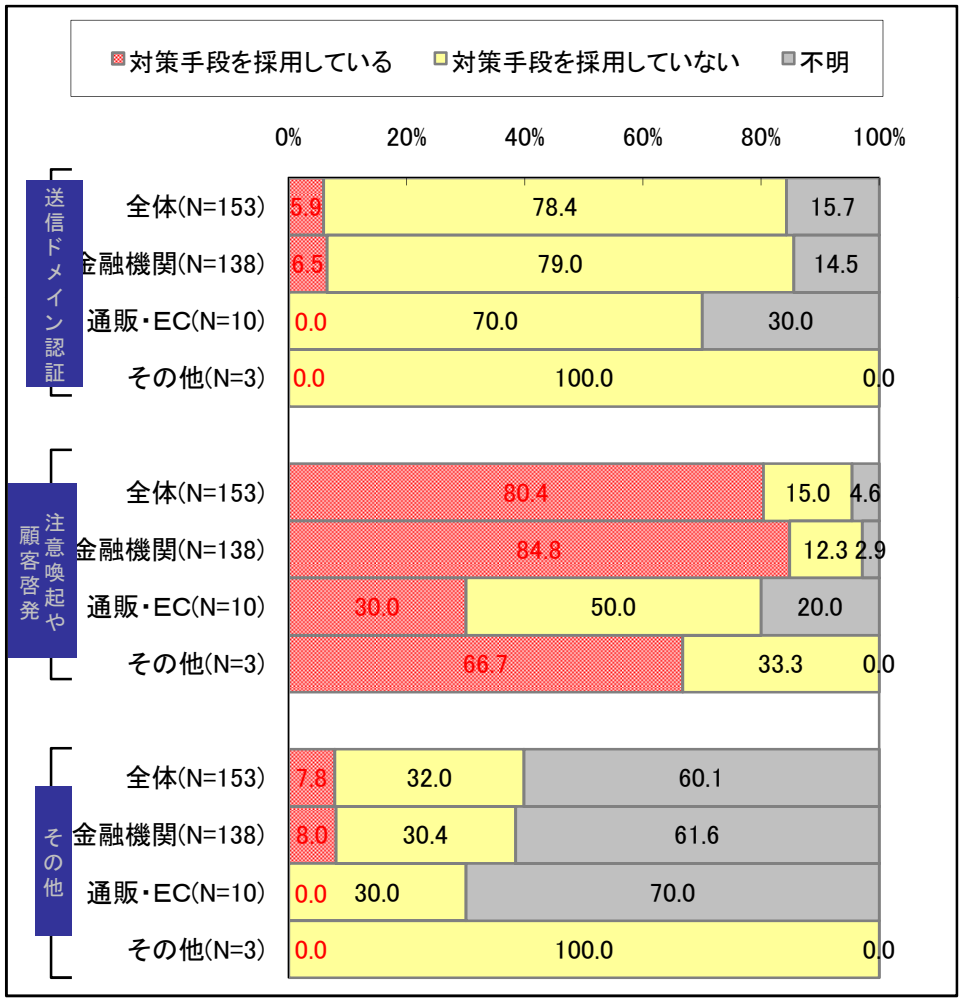

■採用している対策(Q4-3) ②カテゴリ金融機関区分別構成比



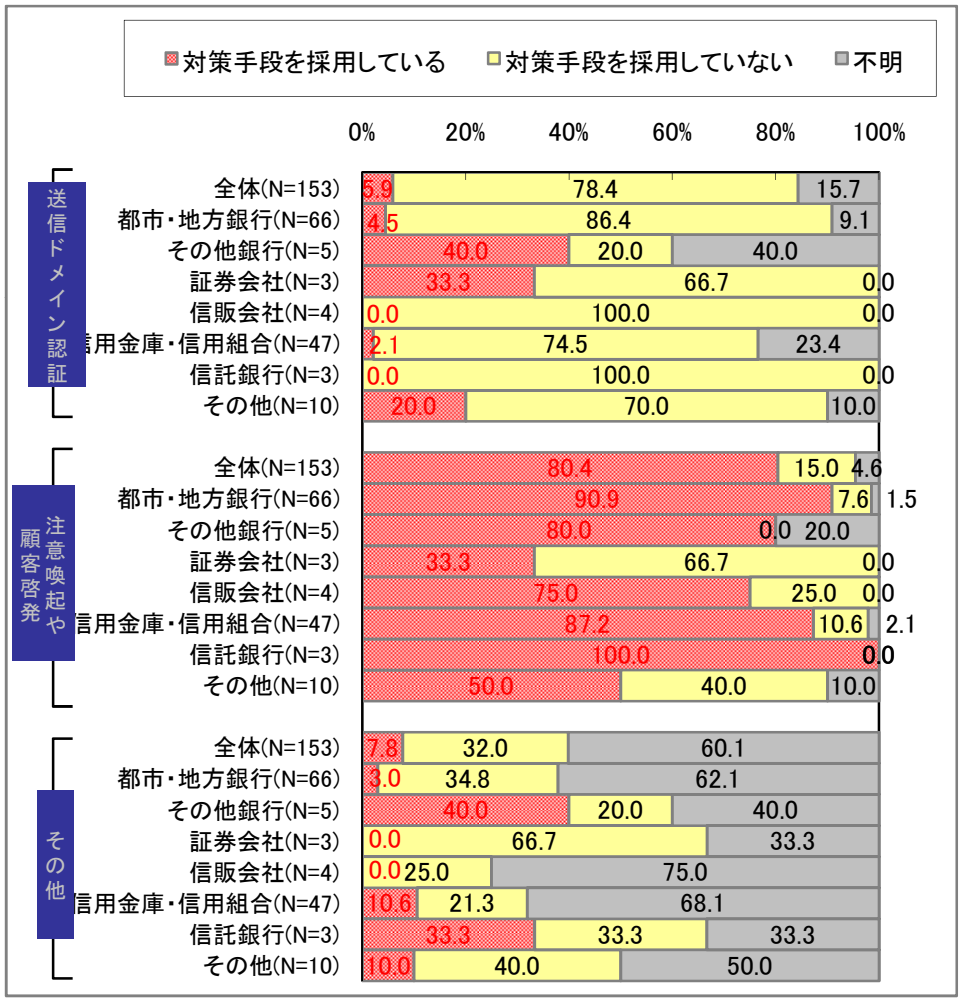
# 11.採用している対策（Q4-3）

業種形態別にみると、送信ドメイン認証「SPF」は、【金融機関】のみで「対策手段を採用している」。また、注意喚起や顧客啓発では、【金融機関】は「対策手段を採用している」（84.8%）と8割半ばなのに対し、【通販・EC】（30.0%）では3割程度にとどまる。
カテゴリ金融機関別にみると、注意喚起や顧客啓発では、【都市・地方銀行】（90.9%）、【信用金庫・信用組合】（87.2%）は「対策手段を採用している」が9割前後と他の金融機関より高い。※サンプル数がn<30の層は少数のため注意が必要。

■採用している対策(Q4-3) ①業種形態別構成比




■採用している対策(Q4-3) ②カテゴリ金融機関区分別構成比



# 12.対策を採用した理由（Q4-3）

◆対策を採用した理由は、「信頼性が高いため」が最も多く、「効果実績があるため」が続く。コストパフォーマンスより、信頼性、効果実績を重視している様子。SSLは、「信頼性が高いため」（67.6%）が約7割と最も高く、それ以下を大きく引き離す。乱数表カードは、「信頼性が高いため」（44.6%）が4割半と最も高く、「関係者の推奨のため」「他社も採用しているため」が3割強で続く。ワンタイムパスワードは、「信頼性が高いから」（60.0%）が6割と最も高く、それ以下を大きく引き離す。注意喚起や顧客啓発は、「コストが安いため」（52.0%）が半数と最も高く、以下、「他社も採用しているため」（31.7%）、「関係者の推奨のため」（26.0%）が続く。EV SSLは、「信頼性が高いため」（41.7%）が最も高く、「最新技術であるため」（33.3%）が続き、新しい技術として有望視されている様子がうかがえる。

■対策を採用した理由（Q4-3）

※複数回答

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| SSL | 全体 | 信頼性が高いため | 効果実績があるため | 他社も採用しているため | 関係者の推奨のため | コストが安いため | 最新技術であるため | その他 | 不明 |
| | （n=139） | 67.6 | 39.6 | 37.4 | 25.9 | 24.5 | 14.4 | 3.6 | 2.2 |
| EVSSL | 全体 | 信頼性が高いため | 最新技術であるため | コストが安いため | 効果実績があるため | 関係者の推奨のため | 他社も採用しているため | その他 | 不明 |
| | （n=12） | 41.7 | 33.3 | 16.7 | 16.7 | 8.3 | 8.3 | － | 41.7 |
| 乱数表カード | 全体 | 信頼性が高いため | 関係者の推奨のため | 他社も採用しているため | コストが安いため | 効果実績があるため | 最新技術であるため | その他 | 不明 |
| | （n=56） | 44.6 | 32.1 | 32.1 | 30.4 | 28.6 | 5.4 | 3.6 | 16.1 |
| ワンタイムパスワード | 全体 | 信頼性が高いため | 効果実績があるため | 関係者の推奨のため | 他社も採用しているため | コストが安いため | 最新技術であるため | その他 | 不明 |
| | （n=30） | 60.0 | 20.0 | 13.3 | 13.3 | 10.0 | 10.0 | 6.7 | 23.3 |
| 3Dセキュア | 全体 | 信頼性が高いため | 効果実績があるため | 他社も採用しているため | コストが安いため | 関係者の推奨のため | 最新技術であるため | その他 | 不明 |
| | （n=9） | 44.4 | 22.2 | 22.2 | 11.1 | 11.1 | － | － | 44.4 |
| フィッシング対策ツール・システム | 全体 | 信頼性が高いため | 効果実績があるため | 他社も採用しているため | コストが安いため | 最新技術であるため | 関係者の推奨のため | その他 | 不明 |
| | （n=34） | 38.2 | 32.4 | 32.4 | 23.5 | 23.5 | 11.8 | － | 17.6 |
| 画像認証 | 全体 | 信頼性が高いため | 効果実績があるため | 他社も採用しているため | コストが安いため | 関係者の推奨のため | 最新技術であるため | その他 | 不明 |
| | （n=5） | 20.0 | 20.0 | 20.0 | － | － | － | － | 80.0 |
| 自社発行メールの電子署名 | 全体 | 信頼性が高いため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | コストが安いため | 関係者の推奨のため | その他 | 不明 |
| | （n=10） | 60.0 | 20.0 | 20.0 | 20.0 | 10.0 | － | 10.0 | 40.0 |
| 送信ドメイン認証「DKIM」 | 全体 | 信頼性が高いため | 最新技術であるため | コストが安いため | 関係者の推奨のため | 効果実績があるため | 他社も採用しているため | その他 | 不明 |
| | （n=6） | 50.0 | 16.7 | － | － | － | － | － | 50.0 |
| 送信ドメイン認証「SPF」 | 全体 | 信頼性が高いため | 効果実績があるため | 関係者の推奨のため | 他社も採用しているため | コストが安いため | 最新技術であるため | その他 | 不明 |
| | （n=9） | 44.4 | 33.3 | 22.2 | 11.1 | － | － | － | 33.3 |
| 注意喚起や顧客啓発 | 全体 | コストが安いため | 他社も採用しているため | 関係者の推奨のため | 効果実績があるため | 信頼性が高いため | 最新技術であるため | その他 | 不明 |
| | （n=123） | 52.0 | 31.7 | 26.0 | 20.3 | 9.8 | 2.4 | 8.9 | 11.4 |
| その他 | 全体 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 効果実績があるため | 最新技術であるため | 他社も採用しているため | その他 | 不明 |
| | （n=12） | 41.7 | 41.7 | 25.0 | 25.0 | 16.7 | 16.7 | 25.0 | 16.7 |

# 12.対策を採用した理由（Q4-3）

◆SSLでは、サンプル数が少数（n<30）のため、注意する必要があるが、【通販・EC】は「信頼性が高いため」（80.0%）が8割と最も高く、以下を大きく引き離している。EV SSLでは、全体は「信頼性が高いため」（41.7%）が最も高く、「最新技術であるため」（33.3%）が続き、新しい技術として有望視されている様子がうかがえる。乱数表カードでは、全体は「信頼性が高いため」（44.6%）が4割半と最も高く、「関係者の推奨のため」「他社も採用しているため」が3割で続く。ワンタイムパスワードでは、全体は「信頼性が高いため」（60.0%）が6割と最も高い。

## ■対策を採用した理由（Q4-3） ①業種形態別構成比

| | | SSL ※複数回答 | | | | | | | | | EV SSL ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 139 | 94 | 34 | 36 | 20 | 55 | 52 | 5 | 3 | 12 | 5 | 2 | 1 | 4 | 2 | 1 | – | 5 |
| | % | 100.0 | 67.6 | 24.5 | 25.9 | 14.4 | 39.6 | 37.4 | 3.6 | 2.2 | 100.0 | 41.7 | 16.7 | 8.3 | 33.3 | 16.7 | 8.3 | - | 41.7 |
| 金融機関 | N | 125 | 84 | 31 | 35 | 19 | 52 | 49 | 5 | 3 | 11 | 4 | 2 | 1 | 4 | 2 | 1 | – | 5 |
| | % | 100.0 | 67.2 | 24.8 | 28.0 | 15.2 | 41.6 | 39.2 | 4.0 | 2.4 | 100.0 | 36.4 | 18.2 | 9.1 | 36.4 | 18.2 | 9.1 | - | 45.5 |
| 通販・EC | N | 10 | 8 | 2 | 1 | 1 | 1 | 2 | – | – | 1 | 1 | – | – | – | – | – | – | – |
| | % | 100.0 | 80.0 | 20.0 | 10.0 | 10.0 | 10.0 | 20.0 | - | - | 100.0 | 100.0 | - | - | - | - | - | - | - |
| その他 | N | 3 | 1 | 1 | – | – | 2 | 1 | – | – | – | – | – | – | – | – | – | – | – |
| | % | 100.0 | 33.3 | 33.3 | - | - | 66.7 | 33.3 | - | - | - | - | - | - | - | - | - | - | - |

| | | 乱数表カード ※複数回答 | | | | | | | | | ワンタイムパスワード ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 56 | 25 | 17 | 18 | 3 | 16 | 18 | 2 | 9 | 30 | 18 | 3 | 4 | 3 | 6 | 4 | 2 | 7 |
| | % | 100.0 | 44.6 | 30.4 | 32.1 | 5.4 | 28.6 | 32.1 | 3.6 | 16.1 | 100.0 | 60.0 | 10.0 | 13.3 | 10.0 | 20.0 | 13.3 | 6.7 | 23.3 |
| 金融機関 | N | 55 | 24 | 17 | 18 | 3 | 16 | 18 | 2 | 9 | 29 | 17 | 3 | 4 | 3 | 6 | 4 | 2 | 7 |
| | % | 100.0 | 43.6 | 30.9 | 32.7 | 5.5 | 29.1 | 32.7 | 3.6 | 16.4 | 100.0 | 58.6 | 10.3 | 13.8 | 10.3 | 20.7 | 13.8 | 6.9 | 24.1 |
| 通販・EC | N | 1 | 1 | – | – | – | – | – | – | – | 1 | 1 | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | - | - | - | - | 100.0 | 100.0 | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |

| | | 3Dセキュア ※複数回答 | | | | | | | | | フィッシング対策ツール・システム ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 9 | 4 | 1 | 1 | – | 2 | 2 | – | 4 | 34 | 13 | 8 | 4 | 8 | 11 | 11 | – | 6 |
| | % | 100.0 | 44.4 | 11.1 | 11.1 | - | 22.2 | 22.2 | - | 44.4 | 100.0 | 38.2 | 23.5 | 11.8 | 23.5 | 32.4 | 32.4 | - | 17.6 |
| 金融機関 | N | 6 | 1 | 1 | 1 | – | 1 | 1 | – | 4 | 33 | 12 | 8 | 4 | 8 | 11 | 11 | – | 6 |
| | % | 100.0 | 16.7 | 16.7 | 16.7 | - | 16.7 | 16.7 | - | 66.7 | 100.0 | 36.4 | 24.2 | 12.1 | 24.2 | 33.3 | 33.3 | - | 18.2 |
| 通販・EC | N | 2 | 2 | – | – | – | – | – | – | – | 1 | 1 | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | - | - | - | - | 100.0 | 100.0 | - | - | - | - | - | - | - |
| その他 | N | 1 | 1 | – | – | – | 1 | 1 | – | – | – | – | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | 100.0 | 100.0 | - | - | - | - | - | - | - | - | - | - | - |

# 12.対策を採用した理由（Q4-3）

◆注意喚起や顧客啓発では、全体は「コストが安いため」(52.0%)が半数と最も高く、以下、「他社も採用しているため」(31.7%)、「関係者の推奨のため」(26.0%)が続く。

## ■対策を採用した理由(Q4-3) ①業種形態別構成比

| | | 画像認証 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 5 | 1 | – | – | – | 1 | 1 | – | 4 |
| | % | 100.0 | 20.0 | - | - | - | 20.0 | 20.0 | - | 80.0 |
| 金融機関 | N | 4 | – | – | – | – | – | – | – | 4 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| 通販・EC | N | 1 | 1 | – | – | – | 1 | 1 | – | – |
| | % | 100.0 | 100.0 | - | - | - | 100.0 | 100.0 | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

| | | 自社発行メールの電子署名 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 10 | 6 | 1 | – | 2 | 2 | 2 | 1 | 4 |
| | % | 100.0 | 60.0 | 10.0 | - | 20.0 | 20.0 | 20.0 | 10.0 | 40.0 |
| 金融機関 | N | 9 | 5 | 1 | – | 2 | 2 | 2 | 1 | 4 |
| | % | 100.0 | 55.6 | 11.1 | - | 22.2 | 22.2 | 22.2 | 11.1 | 44.4 |
| 通販・EC | N | 1 | 1 | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

| | | 送信ドメイン認証「DKIM」 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 6 | 3 | – | – | 1 | – | – | – | 3 |
| | % | 100.0 | 50.0 | - | - | 16.7 | - | - | - | 50.0 |
| 金融機関 | N | 6 | 3 | – | – | 1 | – | – | – | 3 |
| | % | 100.0 | 50.0 | - | - | 16.7 | - | - | - | 50.0 |
| 通販・EC | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

| | | 送信ドメイン認証「SPF」 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 9 | 4 | – | 2 | – | 3 | 1 | – | 3 |
| | % | 100.0 | 44.4 | - | 22.2 | - | 33.3 | 11.1 | - | 33.3 |
| 金融機関 | N | 9 | 4 | – | 2 | – | 3 | 1 | – | 3 |
| | % | 100.0 | 44.4 | - | 22.2 | - | 33.3 | 11.1 | - | 33.3 |
| 通販・EC | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

| | | 注意喚起や顧客啓発 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 123 | 12 | 64 | 32 | 3 | 25 | 39 | 11 | 14 |
| | % | 100.0 | 9.8 | 52.0 | 26.0 | 2.4 | 20.3 | 31.7 | 8.9 | 11.4 |
| 金融機関 | N | 117 | 11 | 61 | 31 | 3 | 23 | 38 | 11 | 14 |
| | % | 100.0 | 9.4 | 52.1 | 26.5 | 2.6 | 19.7 | 32.5 | 9.4 | 12.0 |
| 通販・EC | N | 3 | 1 | 1 | 1 | – | 1 | 1 | – | – |
| | % | 100.0 | 33.3 | 33.3 | 33.3 | - | 33.3 | 33.3 | - | - |
| その他 | N | 2 | – | 1 | – | – | 1 | – | – | – |
| | % | 100.0 | - | 50.0 | - | - | 50.0 | - | - | - |

| | | その他 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 12 | 5 | 5 | 3 | 2 | 3 | 2 | 3 | 2 |
| | % | 100.0 | 41.7 | 41.7 | 25.0 | 16.7 | 25.0 | 16.7 | 25.0 | 16.7 |
| 金融機関 | N | 11 | 5 | 5 | 3 | 2 | 3 | 2 | 3 | 1 |
| | % | 100.0 | 45.5 | 45.5 | 27.3 | 18.2 | 27.3 | 18.2 | 27.3 | 9.1 |
| 通販・EC | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

# 12.対策を採用した理由（Q4-3）

◆SSLでは、【都市・地方銀行】は「信頼性が高いため」（70.3%）が7割と最も高く、以下を引き離している。続いて、「効果実績があるため」「他社も採用しているため」が4割半ばで並ぶ。一方、【信用金庫・信用組合】では、「信頼性が高いため」に続き、「関係者の推奨のため」（36.8%）が3割半ばと他の金融機関より高くなっている。乱数表カードでは、【都市・地方銀行】は「信頼性が高いため」（45.8%）が4割半ばと最も高く、「コストが安いため」「他社も採用しているため」が4割で続く。ワンタイムパスワードでは、全体は「信頼性が高いため」（60.0%）が6割と最も高く、以下を大きく引き離す。

■対策を採用した理由（Q4-3） ②カテゴリ金融機関区分別構成比

| | | SSL ※複数回答 | | | | | | | | | EV SSL ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 139 | 94 | 34 | 36 | 20 | 55 | 52 | 5 | 3 | 12 | 5 | 2 | 1 | 4 | 2 | 1 | – | 5 |
| | % | 100.0 | 67.6 | 24.5 | 25.9 | 14.4 | 39.6 | 37.4 | 3.6 | 2.2 | 100.0 | 41.7 | 16.7 | 8.3 | 33.3 | 16.7 | 8.3 | - | 41.7 |
| 都市・地方銀行 | N | 64 | 45 | 15 | 17 | 13 | 30 | 30 | 2 | 1 | 7 | 3 | 2 | 1 | 3 | 2 | 1 | – | 3 |
| | % | 100.0 | 70.3 | 23.4 | 26.6 | 20.3 | 46.9 | 46.9 | 3.1 | 1.6 | 100.0 | 42.9 | 28.6 | 14.3 | 42.9 | 28.6 | 14.3 | - | 42.9 |
| その他銀行 | N | 3 | 2 | 3 | 1 | 1 | 3 | 1 | – | – | 2 | – | – | – | 1 | – | – | – | 1 |
| | % | 100.0 | 66.7 | 100.0 | 33.3 | 33.3 | 100.0 | 33.3 | - | - | 100.0 | - | - | - | 50.0 | - | - | - | 50.0 |
| 証券会社 | N | 3 | 3 | – | – | – | 1 | 2 | – | – | – | – | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | 33.3 | 66.7 | - | - | - | - | - | - | - | - | - | - | - |
| 信販会社 | N | 4 | 3 | 1 | 1 | – | 2 | 3 | – | – | – | – | – | – | – | – | – | – | – |
| | % | 100.0 | 75.0 | 25.0 | 25.0 | - | 50.0 | 75.0 | - | - | - | - | - | - | - | - | - | - | - |
| 信用金庫信用組合 | N | 38 | 21 | 8 | 14 | 4 | 8 | 8 | 3 | 2 | 2 | 1 | – | – | – | – | – | – | 1 |
| | % | 100.0 | 55.3 | 21.1 | 36.8 | 10.5 | 21.1 | 21.1 | 7.9 | 5.3 | 100.0 | 50.0 | - | - | - | - | - | - | 50.0 |
| 信託銀行 | N | 3 | 2 | 1 | 1 | – | 2 | 1 | – | – | – | – | – | – | – | – | – | – | – |
| | % | 100.0 | 66.7 | 33.3 | 33.3 | - | 66.7 | 33.3 | - | - | - | - | - | - | - | - | - | - | - |
| その他 | N | 10 | 8 | 3 | 1 | 1 | 6 | 4 | – | – | – | – | – | – | – | – | – | – | – |
| | % | 100.0 | 80.0 | 30.0 | 10.0 | 10.0 | 60.0 | 40.0 | - | - | - | - | - | - | - | - | - | - | - |

| | | 乱数表カード ※複数回答 | | | | | | | | | ワンタイムパスワード ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 56 | 25 | 17 | 18 | 3 | 16 | 18 | 2 | 9 | 30 | 18 | 3 | 4 | 3 | 6 | 4 | 2 | 7 |
| | % | 100.0 | 44.6 | 30.4 | 32.1 | 5.4 | 28.6 | 32.1 | 3.6 | 16.1 | 100.0 | 60.0 | 10.0 | 13.3 | 10.0 | 20.0 | 13.3 | 6.7 | 23.3 |
| 都市・地方銀行 | N | 24 | 11 | 10 | 9 | 1 | 7 | 10 | 1 | 2 | 11 | 8 | – | 1 | 3 | 2 | 3 | – | 3 |
| | % | 100.0 | 45.8 | 41.7 | 37.5 | 4.2 | 29.2 | 41.7 | 4.2 | 8.3 | 100.0 | 72.7 | - | 9.1 | 27.3 | 18.2 | 27.3 | - | 27.3 |
| その他銀行 | N | 1 | – | – | – | – | – | 1 | – | – | 2 | 2 | 1 | – | – | 2 | – | – | – |
| | % | 100.0 | - | - | - | - | - | 100.0 | - | - | 100.0 | 100.0 | 50.0 | - | - | 100.0 | - | - | - |
| 証券会社 | N | – | – | – | – | – | – | – | – | – | 1 | 1 | – | – | – | 1 | 1 | – | – |
| | % | - | - | - | - | - | - | - | - | - | 100.0 | 100.0 | - | - | - | 100.0 | 100.0 | - | - |
| 信販会社 | N | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| 信用金庫信用組合 | N | 25 | 9 | 5 | 8 | 2 | 6 | 5 | 1 | 7 | 14 | 5 | 2 | 3 | – | 1 | – | 2 | 4 |
| | % | 100.0 | 36.0 | 20.0 | 32.0 | 8.0 | 24.0 | 20.0 | 4.0 | 28.0 | 100.0 | 35.7 | 14.3 | 21.4 | - | 7.1 | - | 14.3 | 28.6 |
| 信託銀行 | N | 3 | 2 | 1 | – | – | 2 | 1 | – | – | – | – | – | – | – | – | – | – | – |
| | % | 100.0 | 66.7 | 33.3 | - | - | 66.7 | 33.3 | - | - | - | - | - | - | - | - | - | - | - |
| その他 | N | 2 | 2 | 1 | 1 | – | 1 | 1 | – | – | 1 | 1 | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | 50.0 | 50.0 | - | 50.0 | 50.0 | - | - | 100.0 | 100.0 | - | - | - | - | - | - | - |

# 12.対策を採用した理由（Q4-3）

◆フィッシング対策ツール・システムでは、全体は「信頼性が高いため」（38.2%）が4割近くと最も高く、「効果実績があるため」「他社も採用しているため」が3割で続く。サンプル数が少数（n<30）のため、注意が必要ではあるが、【都市・地方銀行】は「信頼性が高いため」「他社も採用しているため」が4割以上と高い。

## ■対策を採用した理由（Q4-3） ②カテゴリ金融機関区分別構成比

| | | 3Dセキュア ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 9 | 4 | 1 | 1 | – | 2 | 2 | – | 4 |
| | % | 100.0 | 44.4 | 11.1 | 11.1 | - | 22.2 | 22.2 | - | 44.4 |
| 都市・地方銀行 | N | 3 | – | 1 | 1 | – | – | 1 | – | 2 |
| | % | 100.0 | - | 33.3 | 33.3 | - | - | 33.3 | - | 66.7 |
| その他銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 証券会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信販会社 | N | 1 | 1 | – | – | – | 1 | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | 100.0 | - | - | - |
| 信用金庫信用組合 | N | 2 | – | – | – | – | – | – | – | 2 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| 信託銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

| | | フィッシング対策ツール・システム ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 34 | 13 | 8 | 4 | 8 | 11 | 11 | – | 6 |
| | % | 100.0 | 38.2 | 23.5 | 11.8 | 23.5 | 32.4 | 32.4 | - | 17.6 |
| 都市・地方銀行 | N | 24 | 10 | 7 | 3 | 8 | 8 | 10 | – | 3 |
| | % | 100.0 | 41.7 | 29.2 | 12.5 | 33.3 | 33.3 | 41.7 | - | 12.5 |
| その他銀行 | N | 2 | 1 | – | – | – | 1 | 1 | – | – |
| | % | 100.0 | 50.0 | - | - | - | 50.0 | 50.0 | - | - |
| 証券会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信販会社 | N | 2 | – | 1 | 1 | – | 1 | – | – | – |
| | % | 100.0 | - | 50.0 | 50.0 | - | 50.0 | - | - | - |
| 信用金庫信用組合 | N | 5 | 1 | – | – | – | 1 | – | – | 3 |
| | % | 100.0 | 20.0 | - | - | - | 20.0 | - | - | 60.0 |
| 信託銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

| | | 画像認証 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 5 | 1 | – | – | – | 1 | 1 | – | 4 |
| | % | 100.0 | 20.0 | - | - | - | 20.0 | 20.0 | - | 80.0 |
| 都市・地方銀行 | N | 2 | – | – | – | – | – | – | – | 2 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| その他銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 証券会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信販会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信用金庫信用組合 | N | 2 | – | – | – | – | – | – | – | 2 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| 信託銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |

| | | 自社発行メールの電子署名 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 10 | 6 | 1 | – | 2 | 2 | 2 | 1 | 4 |
| | % | 100.0 | 60.0 | 10.0 | - | 20.0 | 20.0 | 20.0 | 10.0 | 40.0 |
| 都市・地方銀行 | N | 6 | 4 | – | – | 2 | 1 | 2 | 1 | 2 |
| | % | 100.0 | 66.7 | - | - | 33.3 | 16.7 | 33.3 | 16.7 | 33.3 |
| その他銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 証券会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信販会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信用金庫信用組合 | N | 2 | – | – | – | – | – | – | – | 2 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| 信託銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | 1 | 1 | 1 | – | – | 1 | – | – | – |
| | % | 100.0 | 100.0 | 100.0 | - | - | 100.0 | - | - | - |

# 12.対策を採用した理由（Q4-3）

◆注意喚起や顧客啓発では、全体は「コストが安いため」(52.0%)が半数と最も高く、以下、「他社も採用しているため」(31.7%)、「関係者の推奨のため」(26.0%)が続く。【都市・地方銀行】は、全体と同様の傾向にあるが、【信用金庫・信用組合】は「関係者の推奨のため」(22.0%)が「コストが安いため」(34.1%)に続いて高い。

## ■対策を採用した理由(Q4-3) ②カテゴリ金融機関区分別構成比

| | | 送信ドメイン認証「DKIM」 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 6 | 3 | – | – | 1 | – | – | – | 3 |
| | % | 100.0 | 50.0 | - | - | 16.7 | - | - | - | 50.0 |
| 都市・地方銀行 | N | 2 | – | – | – | – | – | – | – | 2 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| その他銀行 | N | 1 | 1 | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | - | - | - | - |
| 証券会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信販会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信用金庫信用組合 | N | 2 | 1 | – | – | 1 | – | – | – | 1 |
| | % | 100.0 | 50.0 | - | - | 50.0 | - | - | - | 50.0 |
| 信託銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | 1 | 1 | – | – | – | – | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | - | - | - | - |

| | | 送信ドメイン認証「SPF」 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 9 | 4 | – | 2 | – | 3 | 1 | – | 3 |
| | % | 100.0 | 44.4 | - | 22.2 | - | 33.3 | 11.1 | - | 33.3 |
| 都市・地方銀行 | N | 3 | – | – | 1 | – | – | – | – | 2 |
| | % | 100.0 | - | - | 33.3 | - | - | - | - | 66.7 |
| その他銀行 | N | 2 | 1 | – | 1 | – | 1 | – | – | – |
| | % | 100.0 | 50.0 | - | 50.0 | - | 50.0 | - | - | - |
| 証券会社 | N | 1 | 1 | – | – | – | 1 | 1 | – | – |
| | % | 100.0 | 100.0 | - | - | - | 100.0 | 100.0 | - | - |
| 信販会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信用金庫信用組合 | N | 1 | – | – | – | – | – | – | – | 1 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| 信託銀行 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| その他 | N | 2 | 2 | – | – | – | 1 | – | – | – |
| | % | 100.0 | 100.0 | - | - | - | 50.0 | - | - | - |

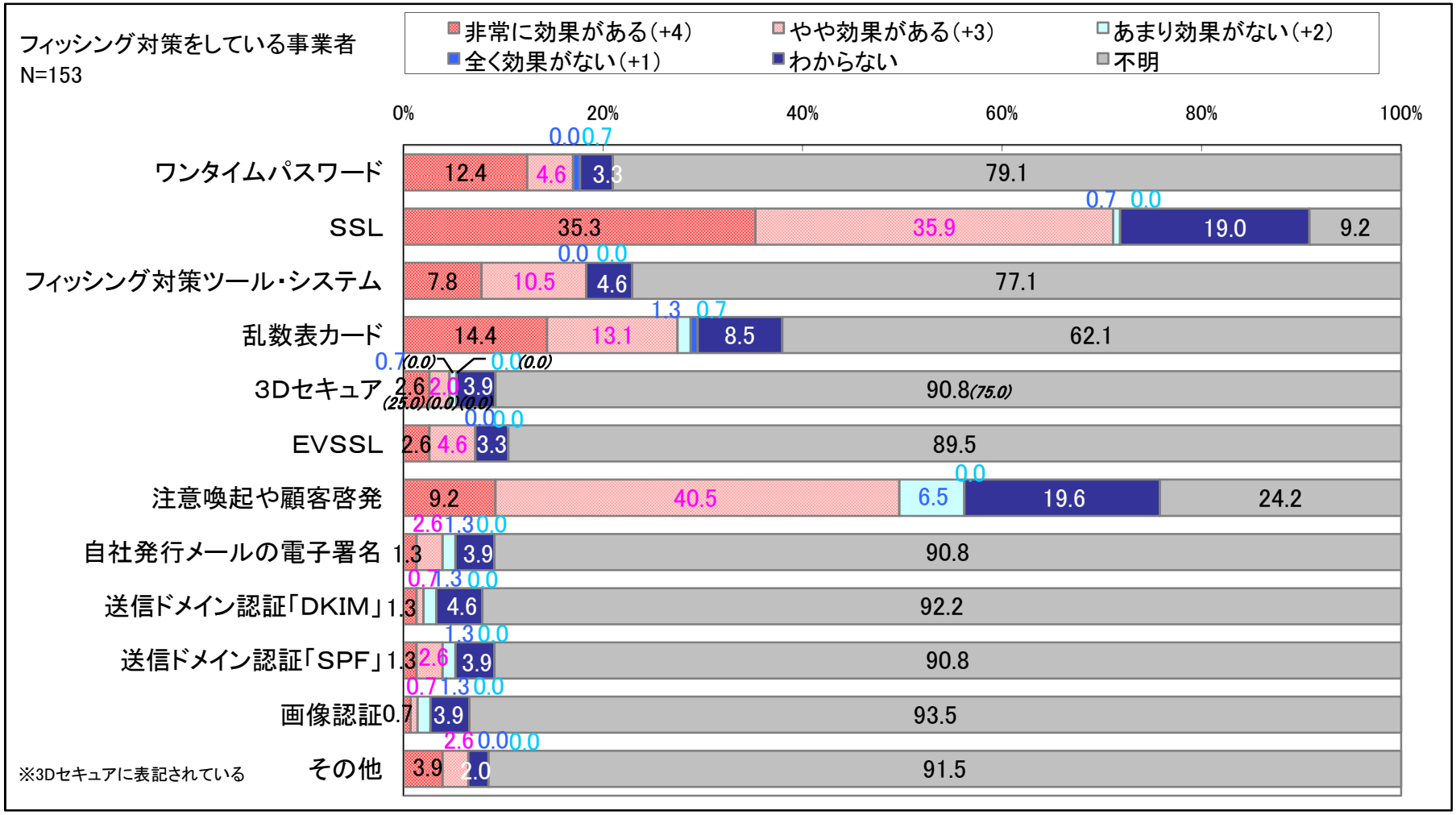
| | | 注意喚起や顧客啓発 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 123 | 12 | 64 | 32 | 3 | 25 | 39 | 11 | 14 |
| | % | 100.0 | 9.8 | 52.0 | 26.0 | 2.4 | 20.3 | 31.7 | 8.9 | 11.4 |
| 都市・地方銀行 | N | 60 | 4 | 39 | 18 | 2 | 15 | 27 | 6 | 1 |
| | % | 100.0 | 6.7 | 65.0 | 30.0 | 3.3 | 25.0 | 45.0 | 10.0 | 1.7 |
| その他銀行 | N | 4 | 1 | 3 | 2 | – | 2 | 1 | 1 | – |
| | % | 100.0 | 25.0 | 75.0 | 50.0 | - | 50.0 | 25.0 | 25.0 | - |
| 証券会社 | N | 1 | – | – | – | – | – | – | – | 1 |
| | % | 100.0 | - | - | - | - | - | - | - | 100.0 |
| 信販会社 | N | 3 | – | – | – | – | – | 1 | 1 | 1 |
| | % | 100.0 | - | - | - | - | - | 33.3 | 33.3 | 33.3 |
| 信用金庫信用組合 | N | 41 | 4 | 14 | 9 | 1 | 4 | 7 | 3 | 10 |
| | % | 100.0 | 9.8 | 34.1 | 22.0 | 2.4 | 9.8 | 17.1 | 7.3 | 24.4 |
| 信託銀行 | N | 3 | – | 2 | 1 | – | 1 | – | – | – |
| | % | 100.0 | - | 66.7 | 33.3 | - | 33.3 | - | - | - |
| その他 | N | 5 | 2 | 3 | 1 | – | 1 | 2 | – | 1 |
| | % | 100.0 | 40.0 | 60.0 | 20.0 | - | 20.0 | 40.0 | - | 20.0 |

| | | その他 ※複数回答 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 計 | 信頼性が高いため | コストが安いため | 関係者の推奨のため | 最新技術であるため | 効果実績があるため | 他社も採用しているため | その他 | 無回答 |
| 全体 | N | 12 | 5 | 5 | 3 | 2 | 3 | 2 | 3 | 2 |
| | % | 100.0 | 41.7 | 41.7 | 25.0 | 16.7 | 25.0 | 16.7 | 25.0 | 16.7 |
| 都市・地方銀行 | N | 2 | 2 | 1 | – | – | – | 1 | – | – |
| | % | 100.0 | 100.0 | 50.0 | - | - | - | 50.0 | - | - |
| その他銀行 | N | 2 | – | 1 | – | – | 1 | – | 1 | – |
| | % | 100.0 | - | 50.0 | - | - | 50.0 | - | 50.0 | - |
| 証券会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信販会社 | N | – | – | – | – | – | – | – | – | – |
| | % | - | - | - | - | - | - | - | - | - |
| 信用金庫信用組合 | N | 5 | 3 | 2 | 3 | 2 | 2 | 1 | 1 | 1 |
| | % | 100.0 | 60.0 | 40.0 | 60.0 | 40.0 | 40.0 | 20.0 | 20.0 | 20.0 |
| 信託銀行 | N | 1 | – | 1 | – | – | – | – | – | – |
| | % | 100.0 | - | 100.0 | - | - | - | - | - | - |
| その他 | N | 1 | – | – | – | – | – | – | 1 | – |
| | % | 100.0 | - | - | - | - | - | - | 100.0 | - |

# 13.採用した対策の効果（Q4-4）

◆採用した対策の効果では、【SSL】は「非常に効果がある」（35.3%）が他の対策より高く3割半ば。【ワンタイムパスワード】【乱数表カード】も「非常に効果がある」が比較的高い。
◆採用した対策の効果度を加重平均で比較した場合、【ワンタイムパスワード】が最も高く、3.6。【SSL】（3.5）、【フィッシング対策ツール・システム】（3.4）、【乱数表カード】（3.4）、【EV SSL】(3.4)、【3Dセキュア】(3.4)が続き、他の対策より高い。

■採用した対策の効果（Q4-4）



# 13.採用した対策の効果（続き/Q4-4）

◆Q4-4のデータを表形式で以下に示す。

■採用した対策の効果（Q4-4）

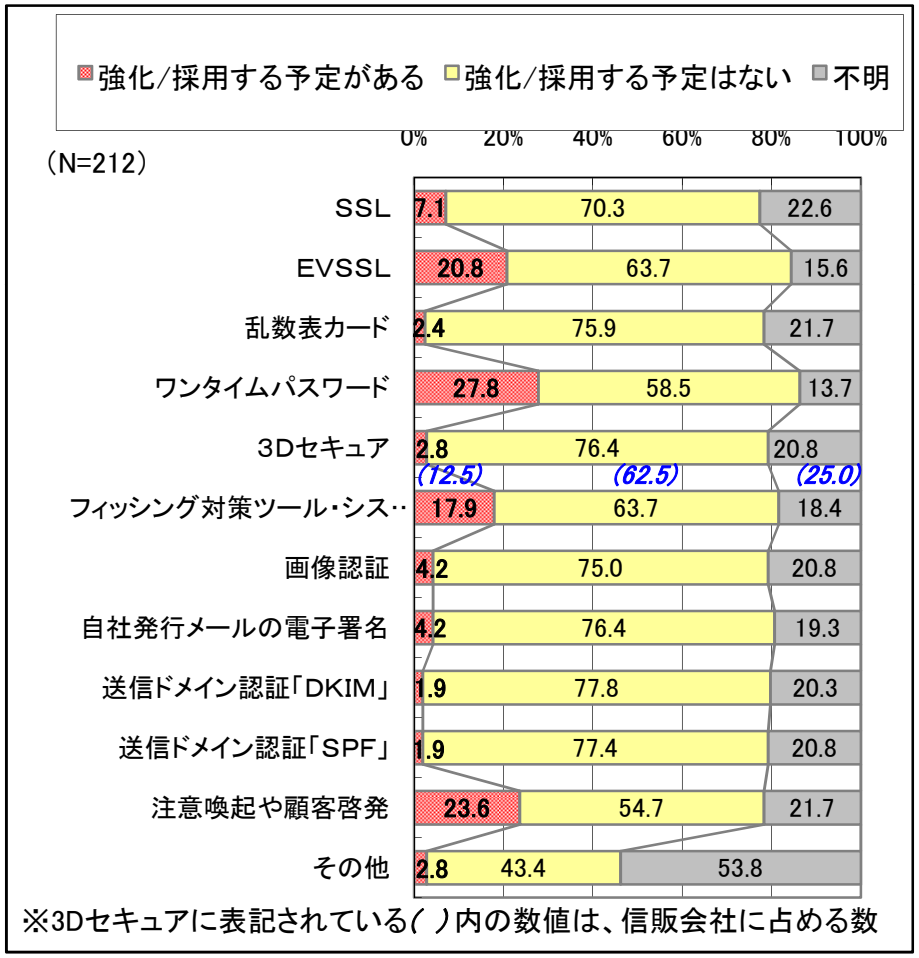
フィッシング対策をしている事業者　　単位（加重平均除く）：％

| | 非常に効果がある（+4） | やや効果がある（+3） | あまり効果がない（+2） | 全く効果がない（+1） | わからない | 不明 | 加重平均 |
|---|---|---|---|---|---|---|---|
| ワンタイムパスワード | 12.4 | 4.6 | － | 0.7 | 3.3 | 79.1 | 3.6 |
| SSL | 35.3 | 35.9 | 0.7 | － | 19.0 | 9.2 | 3.5 |
| フィッシング対策ツール・システム | 7.8 | 10.5 | － | － | 4.6 | 77.1 | 3.4 |
| 乱数表カード | 14.4 | 13.1 | 1.3 | 0.7 | 8.5 | 62.1 | 3.4 |
| 3Dセキュア | 2.6 | 2.0 | 0.7 | － | 3.9 | 90.8 | 3.4 |
| EVSSL | 2.6 | 4.6 | － | － | 3.3 | 89.5 | 3.4 |
| 注意喚起や顧客啓発 | 9.2 | 40.5 | 6.5 | － | 19.6 | 24.2 | 3.1 |
| 自社発行メールの電子署名 | 1.3 | 2.6 | 1.3 | － | 3.9 | 90.8 | 3.0 |
| 送信ドメイン認証「DKIM」 | 1.3 | 0.7 | 1.3 | － | 4.6 | 92.2 | 3.0 |
| 送信ドメイン認証「SPF」 | 1.3 | 2.6 | 1.3 | － | 3.9 | 90.8 | 3.0 |
| 画像認証 | 0.7 | 0.7 | 1.3 | － | 3.9 | 93.5 | 2.8 |
| その他 | 3.9 | 2.6 | － | － | 2 | 91.5 | 3.6 |

# 14.各対策の強化予定状況(Q5)及び対策の採用予定時期(Q5)

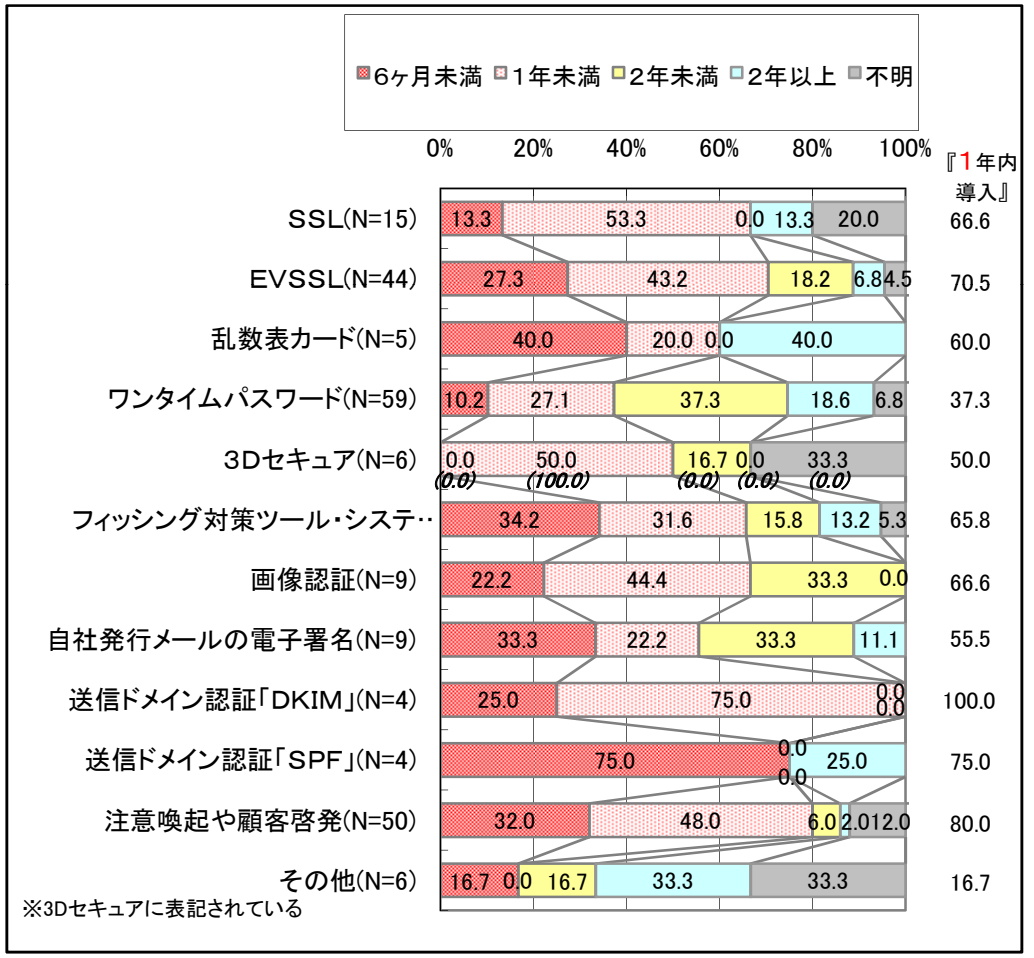
◆各対策の強化予定状況では、【ワンタイムパスワード】は「強化する予定がある」(27.8%)が3割近くと他のカテゴリより高く、【注意喚起や顧客啓発】(23.6%)、【EV SSL】(20.8%)が2割以上、【フィッシング対策ツール・システム】(17.9%)も、他のカテゴリより比較的高かった。
◆対策の採用予定時期では、【注意喚起や顧客啓発】は『年内導入』(80.0%)が8割、新技術として有望視されている【EV SSL】は『1年内導入』(70.5%)が7割、【フィッシング対策ツール・システム】(65.8%)のそれも6割半ばと、他の対策より早期に採用されそう。また、強化対策予定状況で高かった「ワンタイムパスワード」は、「2年未満」(37.3%)が高く、他の対策より採用が遅くなりそうである。

■各対策の強化予定状況(Q5)




※3Dセキュアに表記されている( )内の数値は、信販会社に占める数

■対策の採用予定時期(Q5)

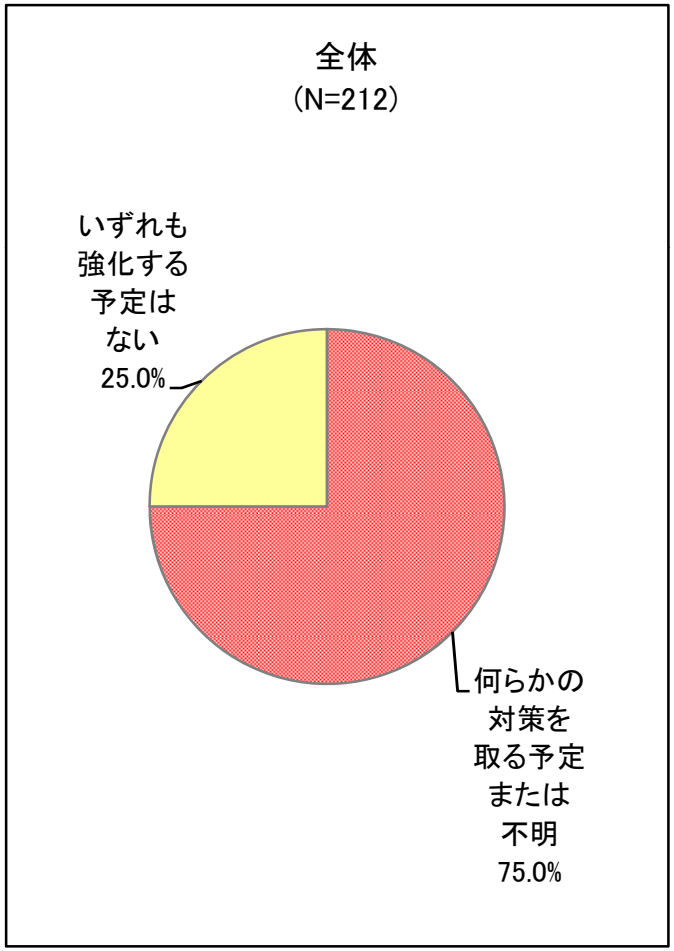



※3Dセキュアに表記されている

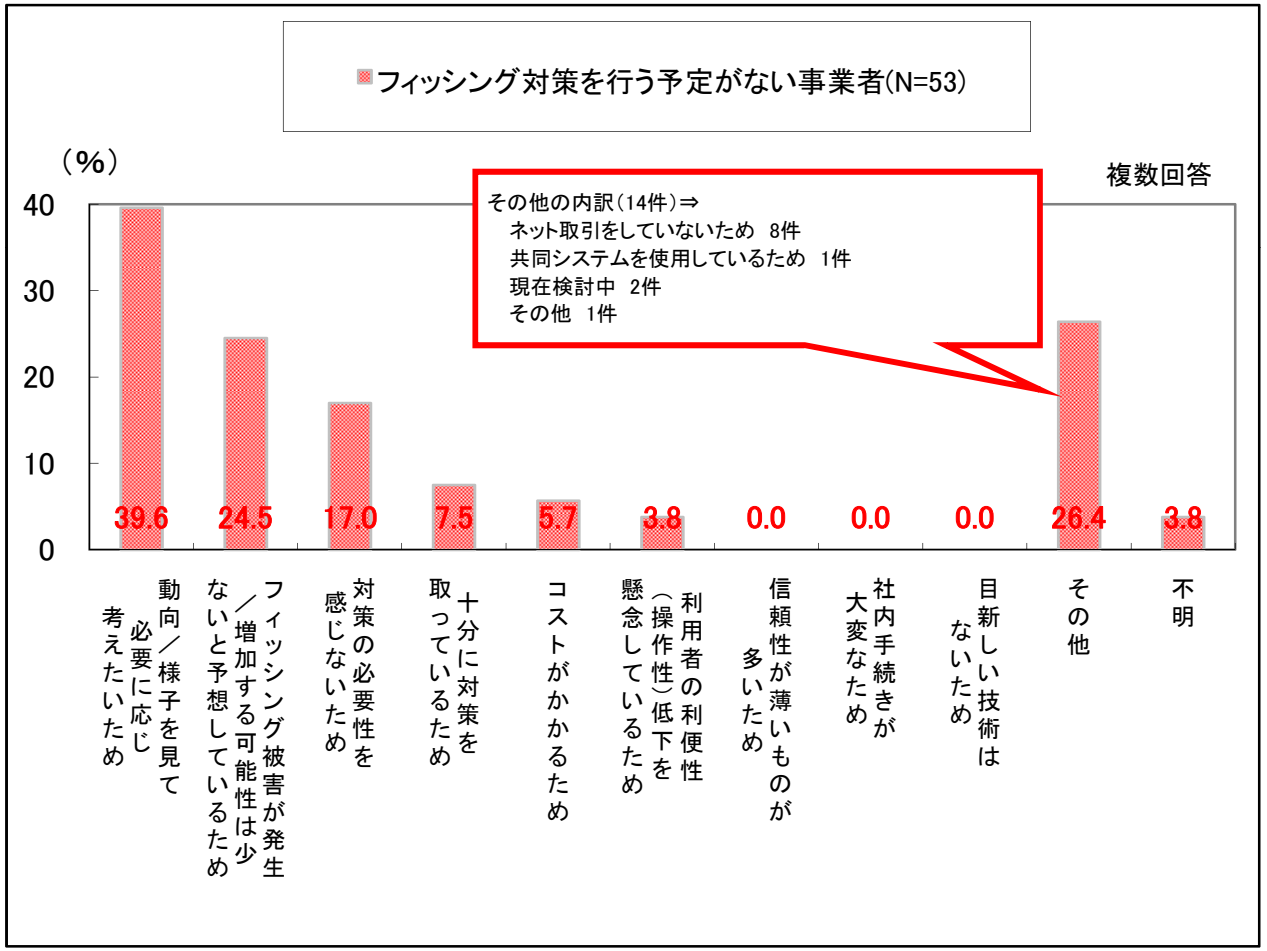
# 15.各対策の強化予定状況(Q5)及び対策強化を行わない理由(Q5-1)

◆各対策の強化予定状況
「いずれも強化する予定はない」事業者が25.0%存在する。
◆対策強化を行わない理由
「動向/様子を見て、必要に応じ考えたいため」(39.6%)が最も高く、約4割。「フィッシング被害が発生/増加する可能性は少ないと予想しているため」(24.5%)が2割強で続き、「対策の必要性を感じないため」(17.0%)が2割近く。フィッシング詐欺の被害に遭っている事業者が少ない為、対策を講じるほどではないと考えているようである。

■各対策の強化予定状況(Q5)



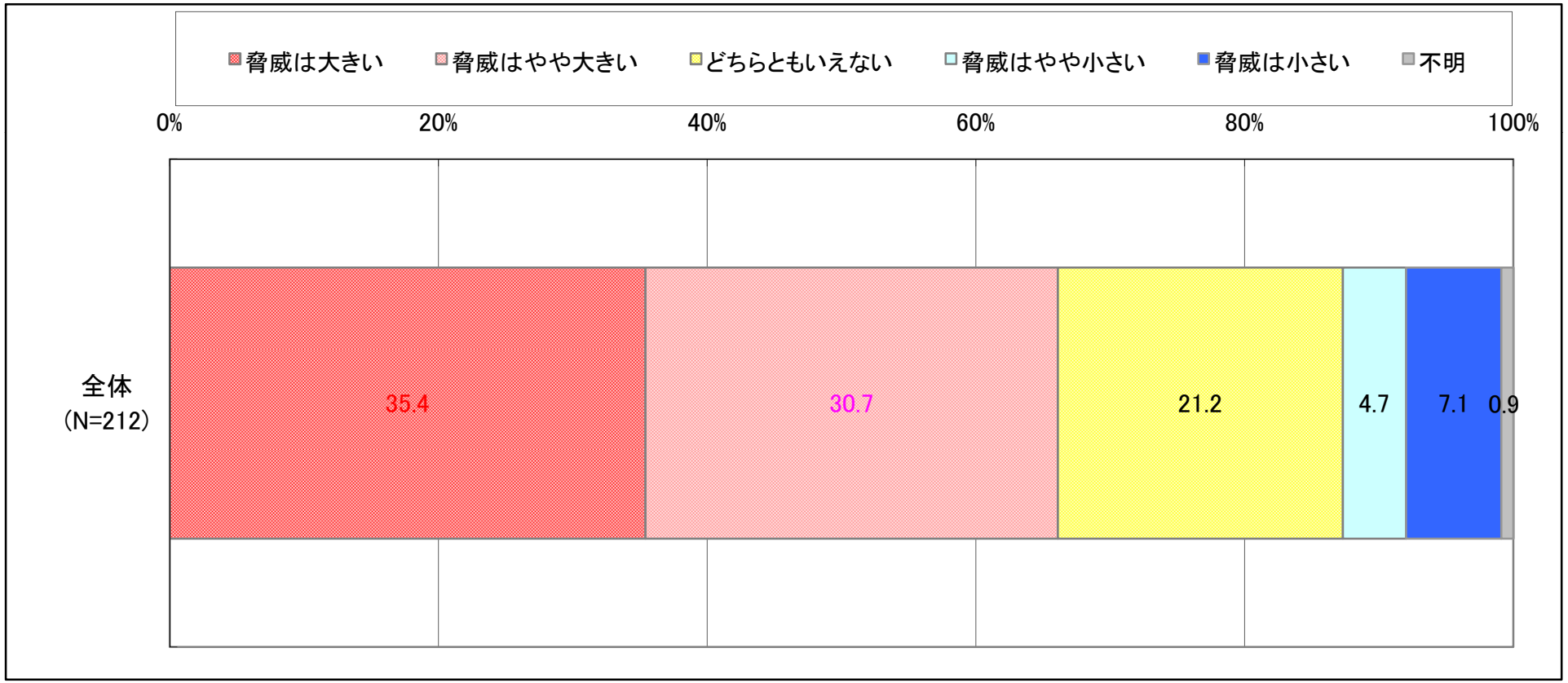

■対策強化を行わない理由(Q5-1)



# 16.フィッシング詐欺に対する脅威(Q6)

◆フィッシング詐欺に対する脅威
「脅威は大きい」(35.4%)、「脅威はやや大きい」(30.7%)を合わせると、6割半ばが『脅威』を感じている。

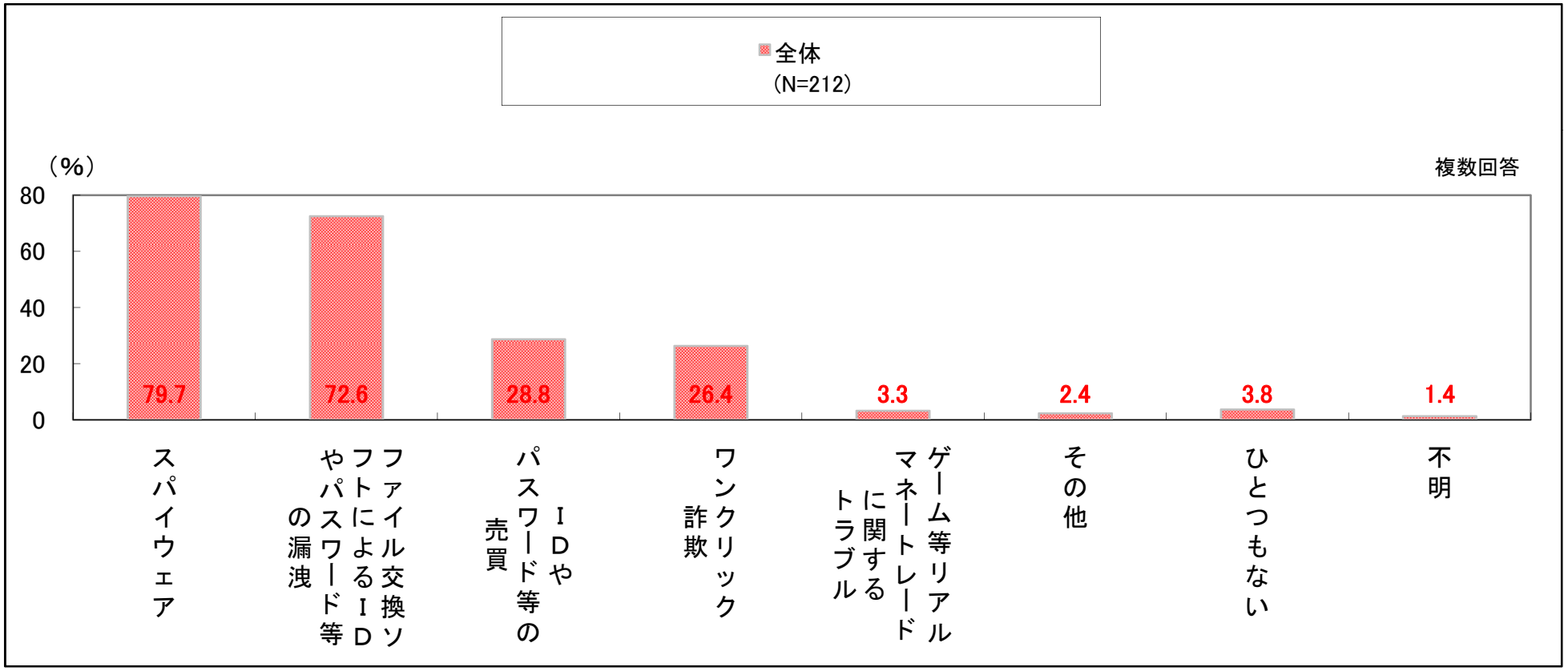
■フィッシング詐欺に対する脅威(Q6)



# 17.フィッシング詐欺以外の脅威（Q7）

◆フィッシング詐欺以外の脅威
「スパイウエア」が最も高く、79.7%と、約8割。「ファイル交換ソフトによるIDやパスワードなどの漏洩」（72.6%）が7割以上で続き、他の項目を大きく引き離している。昨年、金融機関、特に銀行系が対策を強化したため、「スパイウエア」に対する意識が高いものと推察される。

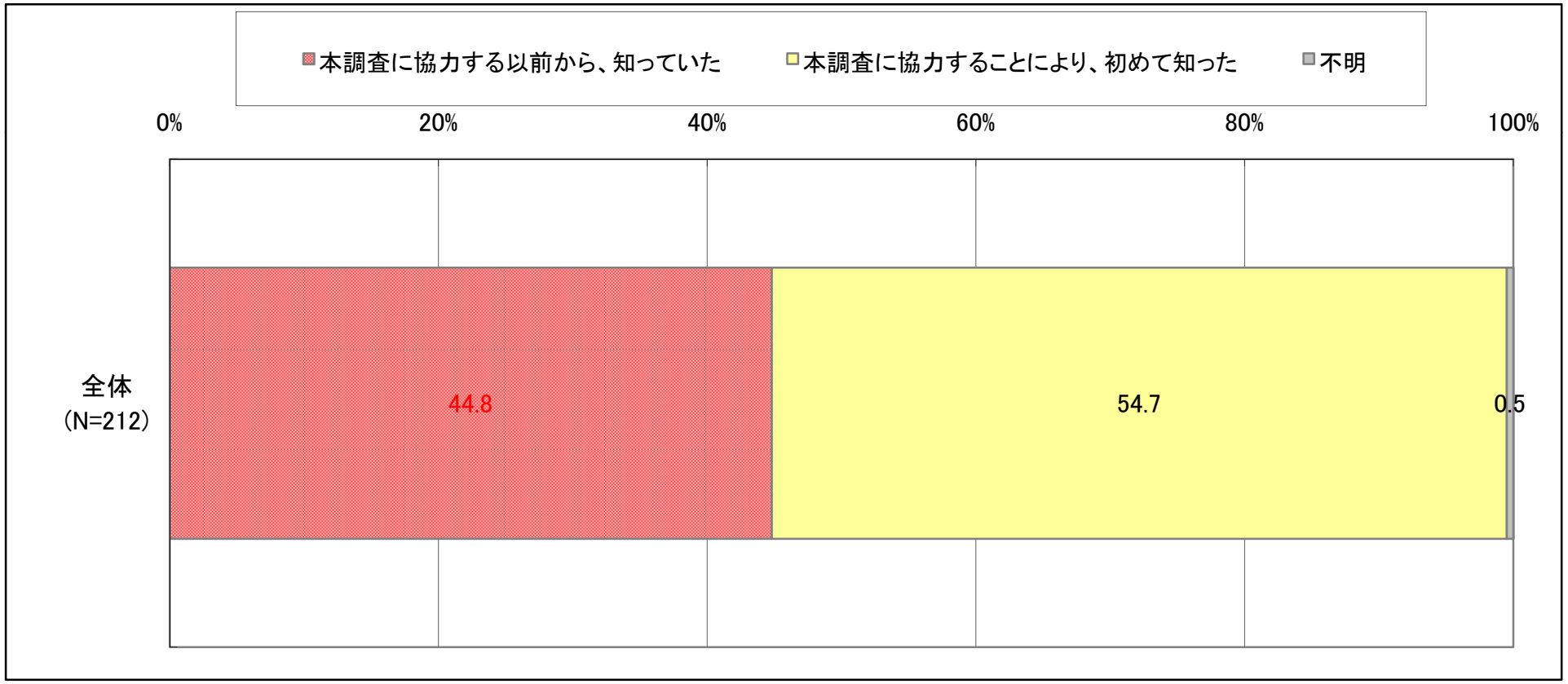
■フィッシング詐欺以外の脅威(Q7)



# 18.フィッシング対策協議会の認知度（Q8）

◆フィッシング対策協議会の認知度
「本調査に協力する以前から、知っていた」（44.8%）は4割半ば、「本調査に協力することにより、初めて知った」（54.7%）と、半数を越える。半数以上の事業者がフィッシング対策協議会を知らなかったと回答している。

■フィッシング対策協議会の認知度(Q8)



# 結果総括

# 結果総括

Points

日本では、フィッシング被害の対策について様子見の状況ではあるが、将来より高度な対策を計画している傾向が見受けられる。

（％）

| 仮説 | 調査結果 |
| --- | --- |
| ■ 対策で採用される手段の傾向は何か？ | ■よく採用されている手段<br>⇒SSL、注意喚起（P16参照）。注意喚起で多く採用される手段は、HPによるもので、次いでリーフレットや電子メール。<br>TVなどメディアによる手段を採用しているとの回答はなかった（P10）。<br>■あまり採用されていない手段<br>⇒EVSSL、自社発行メールの電子署名、3Dセキュア、送信ドメイン認証、画像認証（P16参照）。<br>■対策の手順が決まっている会社は少ない。（P11参照） |
| ■日本ではフィッシングが欧米ほど多くは発生してないので、様子見なのか？ | ■様子見の状態。今後の対策をしない会社が約25.0％（P15、P29参照）。但し、近々対策強化しようとして |
| ■業種により利便性vs厳格性の重さが異なるのか？ | その可能性はある。地方・都市銀行の対策実施比率は高い。（P13、P24参照） |
| ■将来より高度な対策を計画しているのか？ | 今後強化する予定の対策で、最も高いものは「ワンタイムパスワード」。次いで「EVSSL」となっている（P28参照）。 |

# 調査票

# 調査票

**以下、フィッシング詐欺※に対する対策状況ついてお聞きします。**

※以下「フィッシング詐欺」とは、金融機関（銀行やクレジットカード会社）などからの正規のメールやウェブサイトを装い、住所、氏名、銀行口座番号、クレジットカード番号、暗証番号などの個人情報を入力させ詐取する行為です。電子メールのリンクから金融機関等の正規のサイトを装った偽サイトに誘導し、そこで個人情報を入力させる手口が一般的です。
本アンケートでは、**被害の定義を貴社名やサービス名等ブランドやログイン画面等が不正使用されたフィッシング詐欺行為が行われた場合とし、顧客の金銭的実害発生の有無には依らないもの**とします。

**（全員の方にお聞きします）**

**問1.**貴社はフィッシング被害（フィッシングでの貴社ブランド不正使用）にあったことがありますか。
当てはまるものに○を1つ付けてください。

1.被害にあったことはない → **問2.へ(P.2)**
2.被害にあったが、金銭的顧客被害は未遂に終わった
3.被害にあい、金銭的被害にあった顧客がいる

**（問1.で「2.被害にあったが、金銭的被害は未遂に終わった」、「3.被害にあい、金銭的被害にあった顧客がいる」と回答した方にお聞きします）**

**問1－1.**貴社が最初に被害を認知したきっかけは何でしたか。当てはまるものに○を1つ付けてください。
なお、「5.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.顧客からの通報　2.匿名からの通報　3.警察からの確認
4.社内チェック　5.その他(　　)

**問1－2.**被害にあったフィッシングの手法はどのようなものでしたか。当てはまるものに○をいくつでも付けてください。
なお、「3.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.電子メールのリンクから偽サイトに誘導し、そこで個人情報を入力させる手法
2.スパイウェア・クライムウェアを用いた手法
3.その他(　　)
4.わからない

**問1－3.**被害にあったフィッシング行為で詐取対象になったものはどのようなものでしたか。
当てはまるものに○をいくつでも付けてください。
なお、「9.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.氏名　2.住所　3.ID(口座番号/ｸﾚｼﾞｯﾄｶｰﾄﾞ番号含む)
4.暗証番号/パスワード　5.生年月日　6.年齢
7.メールアドレス(携帯電話メールアドレス含む)　8.電話番号(携帯電話番号含む)
9.その他(　　)

**（問1.で「2.被害にあったが、金銭的被害は未遂に終わった」、「3.被害にあい、金銭的被害にあった顧客がいる」と回答した方にお聞きします）**

**問1－4.**フィッシング被害にあった際、貴社はどのような対応を取りましたか。当てはまるものに○をいくつでも付けてください。
なお、「13.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.自社からプロバイダ・サイトサーバ所有者へ直接連絡し、フィッシングサイトを閉鎖した
2.対策代行事業者経由でフィッシングサイトを閉鎖した
3.JPCERT/CC経由でフィッシングサイトを閉鎖した
4.レジストラ(インターネット上の住所にあたるドメイン名の登録申請を受け付ける組織)経由でフィッシングサイトを閉鎖した
5.セキュリティソフトベンダ経由でフィッシングサイトをアクセスブロックした
6.都道府県警察のサイバー犯罪相談窓口に届け出た
7.フィッシング対策協議会に連絡した
8.フィッシングサイトあるいは犯罪者に関連する情報を取得し、追跡した
9.おとり口座情報をフィッシングサイトへ入力し、アクセスを監視した
10.ログ等を確保し、不審なアクセスや取引がないかを調査・解析した
11.顧客対応窓口における対応方法の周知を徹底した
12.対外的に発表(緊急注意喚起)した
13.その他(　　)

**「12.対外的に発表した」を回答していない → 問2.へ**

**（問1-4で「12.対外的に発表(緊急注意喚起)した」と回答した方にお聞きします）**

**問1－4－1.**どのような方法で対外的に発表しましたか。当てはまるものに○をいくつでも付けてください。
なお、「8.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.ホームページによる顧客及び世間への注意喚起
2.電子メールによる顧客への注意喚起
3.電話による顧客への注意喚起
4.ダイレクトメールによる顧客及び世間への注意喚起
5.リーフレット等配布による顧客及び世間への注意喚起
6.新聞・雑誌・TV等の広告による顧客及び世間への注意喚起
7.報道発表による顧客及び世間への注意喚起
8.その他(　　)

**（全員の方にお聞きします）**

**問2.**フィッシング詐欺被害を未然に防ぐために注意喚起や顧客啓発を行っていますか。
当てはまるものに○を1つ付けてください。

1.行っている　2.行っていない → **問3.へ(P.3)**

**（問2.で「1.行っている」と回答した方にお聞きします）**

**問2－1.**どのような方法で実施していますか。当てはまるものに○をいくつでも付けてください。
なお、「11.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.ホームページによる顧客及び世間への注意喚起/顧客啓発
2.電子メールによる顧客への注意喚起/顧客啓発
3.電話による顧客への注意喚起/顧客啓発
4.会報誌による顧客への注意喚起/顧客啓発
5.ダイレクトメールによる顧客及び世間への注意喚起/顧客啓発
6.ポスター掲示による顧客及び世間への注意喚起/顧客啓発
7.新聞・雑誌・TV等の広告による顧客及び世間への注意喚起/顧客啓発
8.リーフレット等配布による顧客及び世間への注意喚起/顧客啓発
9.セミナーによる顧客及び世間への注意喚起/顧客啓発
10.報道発表による顧客及び世間への注意喚起/顧客啓発
11.その他(　　)

→ **問3.へ(P.3)**

# 調査票

**（全員の方にお聞きします）**

**問3.**フィッシングで貴社ブランドが不正使用の対象となった場合の対策手順(実施事項、体制)は決まっていますか。当てはまるものに○を1つ付けてください。

1.決まっている　　2.決まっていない → **問4.へ**

**（問3.で「1.決まっている」と回答した方にお聞きします）**

**問3－1.**それはどのような内容ですか。当てはまるものに○をいくつでも付けてください。
なお、「3.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.実施事項がアクションアイテムリストやマニュアルなどのように文書化されている
2.責任者、報告・連絡ルート、役割分担等体制が決まっている
3.その他(　　)

**（全員の方にお聞きします）**

**問4.**貴社がフィッシング被害にあわないような対策をしていますか。当てはまるものに○を1つ付けてください。

1.対策をしている　　2.対策をしていない → **問4-2.へ**

**（問4.で「1.対策をしている」と回答した方にお聞きします）**

**問4－1.**フィッシング対策をしている理由は何ですか。当てはまるものに○をいくつでも付けてください。
なお、「8.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.顧客を守るため
2.顧客に安心してサービスを利用いただくため
3.企業価値(信頼性)向上のため
4.自社の損害を防ぐため
5.業界方針や国や機関からの要請・指針があったため
6.欧米でフィッシングが増加しており、国内でもフィッシングが発生/増加すると予想されるため
7.他社も実施しているため
8.その他(　　)

→ **問4-3.へ(P.4)**

**（問4.で「2.対策をしていない」と回答した方にお聞きします）**

**問4－2.**貴社が、フィッシング被害対策をしていない理由は何ですか。当てはまるものに○をいくつでも付けてください。
なお、「10.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.対策を行う効果に疑問があるため
2.コストがかかりすぎるため
3.メンテナンスが大変なため
4.フィッシングは古い技術であるため
5.フィッシングは一般的ではないため
6.フィッシング対策システムと社内システムとの相性がよくないため
7.必要性を感じないため
8.自社がフィッシング被害に合う可能性が少ないと予想されるため
9.利用者の利便性(操作性)低下が懸念されるため
10.その他(　　)

→ **問5.へ(P.6)**

**（問4.で「1.対策をしている」と回答した方にお聞きします）**

**問4－3.**フィッシング詐欺に対して、下記の各対策を採用していますか。採用している場合には「2.対策手段を採用している」をA)～L)の内採用している対策全てに、採用していない場合は、「1.対策手段を採用していない」に○をお付けください。また、採用している場合、その理由は何ですか。A)～L)のそれぞれについて、1.～7.の当てはまるものに○をいくつでも付け、「L)その他」や「7.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。
**なお、次ページに記載しております各選択肢の説明文をご参考の上、ご回答ください。**

| | 1.対策手段を採用していない | 2.対策手段を採用している | 対策を採用した理由 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | 1.信頼性が高いため | 2.コストが安いため | 3.関係者の推奨のため | 4.最新技術であるため | 5.効果実績があるため | 6.他社も採用しているため | 7.その他 |
| A) SSL | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| B) EV SSL | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| C) 乱数表カード | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| D) ワンタイムパスワード | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| E) 3Dセキュア | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| F) フィッシング対策ツール・システム | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| G) 画像認証 | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| H) 自社発行メールの電子署名(S/MINE 等) | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| I) (メールサーバに)送信ドメイン認証『DKIM』 | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| J) (メールサーバに)送信ドメイン認証『SPF』 | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| K) 注意喚起や顧客啓発 | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |
| L) その他 (　　) | 1 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 (　　) |

**（問4.で「1.対策をしている」と回答した方にお聞きします）**

**問4－4.**フィッシング詐欺に対する下記の対策について、実施後の効果をどのように思われますか。
A)～L)の問4－3で対策手段を採用しているを選択したものそれぞれについて、1.～5.の当てはまるものについて○を1つずつ付け、「L)その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。
**なお、次ページに記載しております各選択肢の説明文をご参考の上、ご回答ください。**

| | 1.非常に効果がある | 2.やや効果がある | 3.あまり効果がない | 4.全く効果がない | 5.わからない |
|---|---|---|---|---|---|
| A) SSL | 1 | 2 | 3 | 4 | 5 |
| B) EV SSL | 1 | 2 | 3 | 4 | 5 |
| C) 乱数表カード | 1 | 2 | 3 | 4 | 5 |
| D) ワンタイムパスワード | 1 | 2 | 3 | 4 | 5 |
| E) 3Dセキュア | 1 | 2 | 3 | 4 | 5 |
| F) フィッシング対策ツール・システム | 1 | 2 | 3 | 4 | 5 |
| G) 画像認証 | 1 | 2 | 3 | 4 | 5 |
| H) 自社発行メールの電子署名(S/MINE 等) | 1 | 2 | 3 | 4 | 5 |
| I) (メールサーバに)送信ドメイン認証『DKIM』 | 1 | 2 | 3 | 4 | 5 |
| J) (メールサーバに)送信ドメイン認証『SPF』 | 1 | 2 | 3 | 4 | 5 |
| K) 注意喚起や顧客啓発 | 1 | 2 | 3 | 4 | 5 |
| L) その他 | 1 | 2 | 3 | 4 | 5 |

→ **問5.へ(P.6)**

**【選択肢説明文】**

A)「SSL」
電子証明書を使ってサーバの正当性を認証し、暗号技術により送受信データを保護するプロトコル。URLが「https://」から始まり、ブラウザウィンドウ右下等に錠前のマークが表示される。

B)「EV SSL」
電子証明書の一種類で、通常のSSLよりもサーバ真正性について高い信頼性を提供するため、サーバ証明書発行時にSSL発行時よりも厳格な申請者、当該サイトの実在証明審査が行われる。Microsoft Internet Explorer7等では、「EV SSL」証明書を提供しているサーバにアクセスした際にアドレスバーが緑色で強調表示され、サイトを訪れたユーザーにウェブサイトの信頼性が高いことを示す。

C)「乱数表カード」
インターネットバンキング等を利用する際に、必要な「契約者番号」「第二暗証番号」等を記載したカード。カード上に数字がマトリックス状に記載されており、利用者はログイン時にカード上の指定された位置に記載されている数字を入力する。

D)「ワンタイムパスワード」
一度きりしか使うことのできないパスワードのことで、一分単位で変化するパスワードを表示する機械(トークン)を顧客に配布し、ログイン時に(固定の)暗証番号と表示されたパスワードを組み合わせて入力する。

E)「3Dセキュア」
クレジットカード決済の際、ショッピングを行おうとしているサイトの登録パスワードとは別に、クレジットカード会社に事前に登録したパスワードを入力することで、本人確認を多重に行うシステム。

F)「フィッシング対策ツール・システム」
フィッシングサイトから送信された疑いのあるメッセージを開こうとする際、あるいは、ブラウザがフィッシングサイトの疑いのあるサイトを開こうとする際に警告を発するソフトウェアやシステム。または、安全なサイトであることを表示したりするソフトウェアまたはシステム。

G)「画像認証」
ログイン時に顧客が事前登録した画像を提示することでサイトの真正性を確認するか、あるいは、多数の画像を提示して、顧客が事前に登録した画像を選択させることにより本人確認を行うような認証方式。

H)「自社発行メールの電子署名(S/MIME 等)」
第三者による「送信者なりすまし」を検出するための手法であり、公開鍵暗号を組み合わせることでメッセージの暗号化による機密性の確保を行うこともできる。

I)「(メールサーバに)送信ドメイン認証『DKIM』」
DNSサーバを活用して、電子メール送信サーバのFQDNあるいはドメインごとに電子証明書を登録、配布する電子署名の方式。主に、不正な電子メール送信、なりすましといった迷惑メール対策として使われている。電子署名はユーザー、メーラーではなく送信サーバで行われ、署名の検証は受信サーバで行われる。

J)「(メールサーバに)送信ドメイン認証『SPF』」
DNSサーバを活用して、電子メール送信サーバが所属するドメインにて電子メールの送信を許可されたものかどうかを検証することができるような方式。迷惑メールの排除ではなく、なりすましなどに効果があるとされる。

**(全員の方にお聞きします)**

**問5.** 今後、顧客がフィッシング詐欺の被害を受けないように対策を強化しようとしていますか。強化する予定がある場合は「2.強化する予定がある」に、予定がない場合は「1.強化する予定はない」に○をお付けください。また、強化しようとしている場合、その強化予定の対策を採用するまでの時期はどれですか。A)～L)のそれぞれについて、1.～4.の当てはまるものに○を1つずつ付け、「L)その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。**なお、次ページに記載しております各選択肢の説明文をご参考の上、ご回答ください。**

| | 1.強化する予定はない | 2.強化する予定がある | 対策の採用予定時期 | | | |
|---|---|---|---|---|---|---|
| | | | 1. 6ヶ月未満 | 2. 1年未満 | 3. 2年未満 | 4. 2年以上 |
| A) SSL | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| B) EV SSL | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| C) 乱数表カード | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| D) ワンタイムパスワード | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| E) 3Dセキュア | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| F) フィッシング対策ツール・システム | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| G) 画像認証 | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| H) 自社発行メールの電子署名(S/MINE 等) | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| I) (メールサーバに)送信ドメイン認証『DKIM』 | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| J) (メールサーバに)送信ドメイン認証『SPF』 | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| K) 注意喚起や顧客啓発 | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |
| L) その他 ( ) | 1 | 2 ⇒ | 1 | 2 | 3 | 4 |

**A)～L)のいずれも「1.強化する予定はない」と回答した⟶ 問5-1.へ(P.8)**
**A)～L)のいずかを「2.強化する予定がある」と回答した⟶ 問6.へ(P.8)**

# 調査票

**【選択肢説明文】**

A)「SSL」
電子証明書を使ってサーバの正当性を認証し、暗号技術により送受信データを保護するプロトコル。URLが「https://」から始まり、ブラウザウィンドウ右下等に錠前のマークが表示される。

B)「EV SSL」
電子証明書の一種類で、通常のSSLよりもサーバ真正性について高い信頼性を提供するため、サーバ証明書発行時にSSL発行時よりも厳格な申請者、当該サイトの実在証明審査が行われる。Microsoft Internet Explorer7等では、「EV SSL」証明書を提供しているサーバにアクセスした際にアドレスバーが緑色で強調表示され、サイトを訪れたユーザーにウェブサイトの信頼性が高いことを示す。

C)「乱数表カード」
インターネットバンキング等を利用する際に、必要な「契約者番号」「第二暗証番号」等を記載したカード。カード上に数字がマトリックス状に記載されており、利用者はログイン時にカード上の指定された位置に記載されている数字を入力する。

D)「ワンタイムパスワード」
一度きりしか使うことのできないパスワードのことで、一分単位で変化するパスワードを表示する機械(トークン)を顧客に配布し、ログイン時に(固定の)暗証番号と表示されたパスワードを組み合わせて入力する。

E)「3Dセキュア」
クレジットカード決済の際、ショッピングを行おうとしているサイトの登録パスワードとは別に、クレジットカード会社に事前に登録したパスワードを入力することで、本人確認を多重に行うシステム。

F)「フィッシング対策ツール・システム」
フィッシングサイトから送信された疑いのあるメッセージを開こうとする際、あるいは、ブラウザがフィッシングサイトの疑いのあるサイトを開こうとする際に警告を発するソフトウェアやシステム。または、安全なサイトであることを表示したりするソフトウェアまたはシステム。

G)「画像認証」
ログイン時に顧客が事前登録した画像を提示することでサイトの真正性を確認するか、あるいは、多数の画像を提示して、顧客が事前に登録した画像を選択させることにより本人確認を行うような認証方式。

H)「自社発行メールの電子署名(S/MIME 等)」
第三者による「送信者なりすまし」を検出するための手法であり、公開鍵暗号を組み合わせることでメッセージの暗号化による機密性の確保を行うこともできる。

I)「(メールサーバに)送信ドメイン認証『DKIM』」
DNSサーバを活用して、電子メール送信サーバのFQDNあるいはドメインごとに電子証明書を登録、配布する電子署名の方式。主に、不正な電子メール送信、なりすましといった迷惑メール対策として使われている。電子署名はユーザー、メーラーではなく送信サーバで行われ、署名の検証は受信サーバで行われる。

J)「(メールサーバに)送信ドメイン認証『SPF』」
DNSサーバを活用して、電子メール送信サーバが所属するドメインにて電子メールの送信を許可されたものかどうかを検証することができるような方式。迷惑メールの排除ではなく、なりすましなどに効果があるとされる。

**(問5.でA)～L)のいずれも、「1.強化する予定はない」と回答した方にお聞きします)**

**問5-1.**今後、顧客がフィッシング詐欺の被害を受けないような対策強化を行わない理由は何ですか。
当てはまるものに○をいくつでも付けてください。
なお、「10.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.対策の必要性を感じないため
2.十分に対策を取っているため
3.コストがかかるため
4.信頼性が薄いものが多いため
5.社内手続きが大変なため
6.目新しい技術はないため
7.フィッシング被害が発生/増加する可能性は少ないと予想しているため
8.動向/様子を見て必要に応じ考えたいため
9.利用者の利便性(操作性)低下を懸念しているため
10.その他(　　)

**(全員の方にお聞きします)**

**問6.**フィッシング詐欺に対する脅威はどの程度感じていますか。当てはまるものに○を1つ付けてください。

1.脅威は大きい　2.脅威はやや大きい　3.どちらともいえない　4.脅威はやや小さい　5.脅威は小さい

**(全員の方にお聞きします)**

**問7.**フィッシング詐欺以外に脅威を感じているものはありますか。当てはまるものに○をいくつでも付けてください。
なお、「6.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.スパイウェア
2.ワンクリック詐欺
3.ファイル交換ソフトによるIDやパスワード等の漏洩
4.IDやパスワード等の売買
5.ゲーム等リアルマネートレードに関するトラブル
6.その他(　　)
7.ひとつもない

**(全員の方にお聞きします)**

**問8.**以前からフィッシング対策協議会をご存知でしたか。当てはまるものに○を1つ付けてください。

1.本調査に協力する以前から、知っていた
2.本調査に協力することにより、初めて知った

**(全員の方にお聞きします)**

**問9.**フィッシング詐欺やその対策等に関して、ご意見やご要望がございましたら、ご自由にご記入下さい。

## 貴社についてお聞きします

**（全員の方にお聞きします）**

**問10.**貴社の会社形態はどれですか。当てはまるものに○を1つ付けてください。

1.外資系企業　　2.国内系企業

**問11.**貴社の従業員数はどれですか。当てはまるものに○を1つ付けてください。

1. 50人未満　　2. 50人以上～300人未満　　3. 300人以上～1000人未満
4. 1000人以上～10000人未満　　5. 10000人以上

**問12.**貴社の業種形態はどれですか。当てはまるものに○を1つ付けてください。
なお、「3.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1.金融機関　　2.通販・EC（オークション含む）　　3.その他（　　）→ **問13.へ**

**（問12.で「1.金融機関」と回答した方にお聞きします）**

**問12-1.**貴社の会社区分はどれですか。当てはまるものに○を1つ付けてください。
なお、「7.その他」に○を付けた場合、具体的な内容を括弧内にご記入ください。

1. 都市銀行　　2. 地方銀行　　3. 外資系銀行　　4. ネット系銀行
5. 証券会社　　6. 信販会社　　7. その他（　　）

**問13.**貴社の顧客との取引形態はどれですか。当てはまるものに○を1つ付けてください。

1.ネット取引が主　　2.ネット取引とそれ以外が半々　　3.ネット取引以外が主

**問14.**貴社の顧客規模とそのうち、ネットを利用する顧客規模を下記の例を参考にご記入ください。

例：「5,000人」の場合は0.5万人、「1,000,000人」の場合は100万人。

万人　　のうち、ネット利用者は、　　万人

**～　以上、ご協力ありがとうございました　～**

フィッシング被害にあった場合（未遂含む）またはフィッシングに関する情報がありましたら、
フィッシング対策協議会への情報提供にご協力をお願いします。
【フィッシング対策協議会への連絡先】 info@antiphishing.jp