フィッシング対策協議会
Council of Anti-Phishing Japan

インターネットサービス提供事業者に対する「認証方法」に関するアンケート調査結果

2019 年 6 月

フィッシング対策協議会

認証方法調査・推進ワーキンググループ

https://www.antiphishing.jp/

目次

1. はじめに

フィッシング対策協議会 認証方法調査・推進ワーキンググループ （以下 WG と略す）は、フィッシング対策と関連の高いインターネットサービスの利用者認証についての実態調査を行い、より安全なサービス提供と利用に向け、認証方法関連の情報を提供する目的で 2018 年 10 月より活動しております。このたび利用者認証の現状について把握するために、インターネットサービス事業者が採用している認証方法についてアンケート調査を実施しましたので、その結果を報告します。

2.「インターネットサービス事業者が採用している認証方法について」 アンケート調査概要

2.1 調査目的

インターネットサービス事業者が、どのような方法で利用者の認証を行っているかを調査し、現状を把握することを目的としました。具体的な目的としては、結果を業種ごとに集計し、比較することで業種ごとの現状、特徴を考察することや、認証方式と複数要素による認証利用の有無のほか、その認証の運用内容、強化のきっかけなど、詳細についても調査し、認証全般に関わる情報を得ることを目指しました。

また、アカウントの不正利用の状況についても調査することで、認証方法との関連についても考察できるよう調査しました。

2.2 調査概要

調査にあたっては、調査項目、選択肢のほか、対象とする業種を WG にて検討し、事前調査にて一定数の回答を得られることが判明した 10 業種に対して調査を実施しました。業種ごと 29 名～31 名の回答者で総数 308 名へ同一の調査項目（30 問）にて Web によるアンケートを実施しました。

インターネットサービス事業者が、どのような方法で利用者の認証を行っているか調査し、現状を把握することを目的としました。また、結果を業種ごとに集計し、比較することで各業種の現状、特徴を考察しました。調査は、認証方式と複数要素による認証利用の有無のほか、その認証の運用内容、強化のきっかけなど、詳細についても調査し、把握しました。

また、不正利用の状況についても調査し、認証方法との関連についても考察しました。

2.3 実施期間

・事前調査

2019 年 2 月 14 日～18 日

・本調査

2019 年 2 月 19 日～28 日

2.4 調査方法

外部調査システムを利用し、Web システムでアンケート調査を実施

2.5 調査対象

インターネットにてサービスを提供しており、何らかの個人認証を実施している事業者に属し、認証に関連している者

2.6 回答数

回答者数 308 名

対象業種 10 業種

対象業種詳細

業種	回答数
銀行・地銀	31
クレジットカード	31
保険	31
証券	31
インターネット販売（EC サイト）	31
ゲーム	29
不動産	31
旅行	31
交通機関	31
通信	31
合計	308

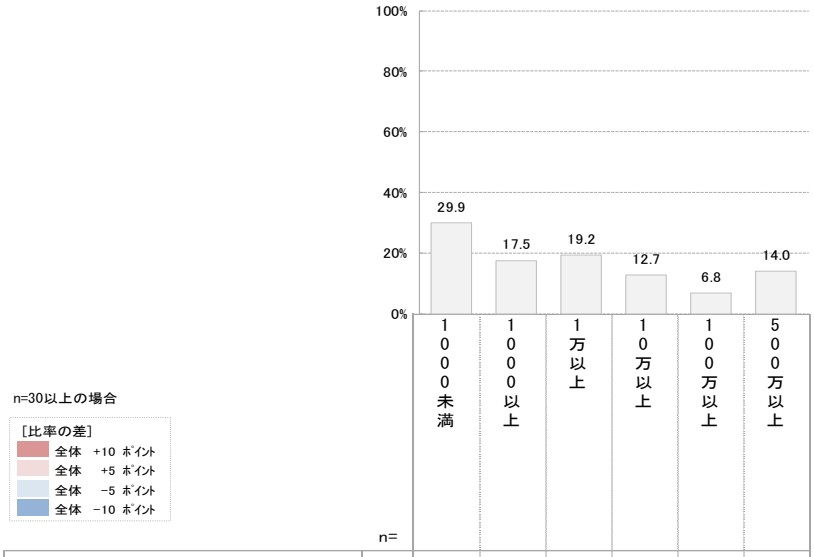
2.7 設問一覧（全 30 問）

Q1 提供しているサービスの利用者数（ID 数）は、どれくらいですか。※複数のサービスを提供している方は、メインで提供しているものについてお答えください。（以降も全て同様）
Q2 提供しているサービスの開始年月はいつですか。 ※わからない方はおおよそにてお答えください。
Q3 個人認証を主にどのような方法で実施していますか。
Q4 どのような認証方式を採用していますか。採用しているすべての方式を選択してください。
Q5 その方式を採用した理由を教えてください。（複数回答可）
Q6 ID、パスワード方式以外の認証方法を用意している場合その認証方式の利用を必須としていますか。
Q7 任意で利用できる他の方式の認証は用意していますか。（複数回答可）
Q8 パスワードに使用できる文字は、何を設定していますか。（複数回答可）
Q9 パスワード設定ルールで必須としているものを教えてください。（複数回答可）
Q10 パスワードの文字で、設定不可としているパターンはありますか。（複数回答可）
Q11 パスワードの定期的な変更を要求していますか。
Q12 パスワードの定期的な変更の実施は必須ですか。
Q13 一定回数パスワード入力を間違えた場合の対応を教えてください。
Q14 ID は、どのように決定していますか。
Q15 ログイン履歴を確認できますか。（複数回答可）
Q16 どの様なことをきっかけに認証の強化を検討しますか。（複数回答可）
Q17 ポイントの利用やクレジットカードの利用など、ユーザにとって資産価値のあるものを使用する際には追加の認証を必要としていますか。
Q18 運営しているサービスがアカウントの不正利用の被害にあったことはありますか。
Q19 それはどのような被害でしたか。（複数回答可）
Q20 不正利用が発生、発覚した時にどのような対応を行っていますか。（複数回答可）
Q21 不正利用の被害にあった利用者にどのような対応をしていますか。（複数回答可）
Q22 不正な攻撃などの被害にあったことはありますか。
Q23 それはどのような攻撃でしたか。（複数回答可）
Q24 不正な攻撃にあった場合、どのような対応を行っていますか。（複数回答可）
Q25 Web サイト側のパスワード管理は、何らかの方法で盗まれても問題ない状態で管理（ハッシュ、暗号化など）読めない状態で管理されていますか。
Q26 安全だが利用者にとって手間のかかる認証を採用している場合、どのような利用啓発や対応を行っていますか。（複数回答可）
Q27 認証についての問い合わせ数は、提供サービスに関する問い合せ数全体に対してどれくらいの割合ですか。
Q28 認証についての問い合わせはどのような質問が多いですか。
Q29 導入してみたい認証方式は、どれですか。（複数回答可）
Q30 セキュリティとユーザビリティ、主にどちらを認証技術に求めますか。

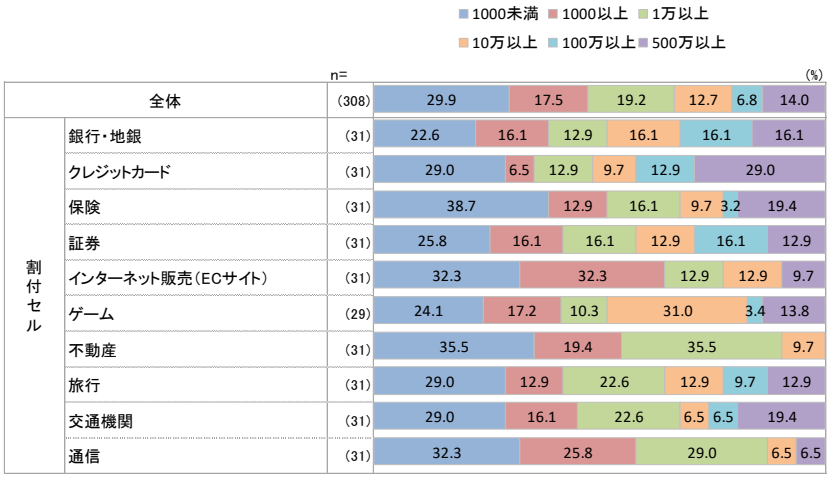
3. 調査結果

Q1

提供しているサービスの利用者数（ID 数）は、どれくらいですか。
※複数のサービスを提供している方は、メインで提供しているものについてお答えください。
（以降も全て同様）



		n=	1000未満	1000以上	1万以上	10万以上	100万以上	500万以上
全体		(308)	29.9	17.5	19.2	12.7	6.8	14.0
割付セル	銀行・地銀	(31)	22.6	16.1	12.9	16.1	16.1	16.1
	クレジットカード	(31)	29.0	6.5	12.9	9.7	12.9	29.0
	保険	(31)	38.7	12.9	16.1	9.7	3.2	19.4
	証券	(31)	25.8	16.1	16.1	12.9	16.1	12.9
	インターネット販売（ECサイト）	(31)	32.3	32.3	12.9	12.9	0.0	9.7
	ゲーム	(29)	24.1	17.2	10.3	31.0	3.4	13.8
	不動産	(31)	35.5	19.4	35.5	9.7	0.0	0.0
	旅行	(31)	29.0	12.9	22.6	12.9	9.7	12.9
	交通機関	(31)	29.0	16.1	22.6	6.5	6.5	19.4
	通信	(31)	32.3	25.8	29.0	6.5	0.0	6.5



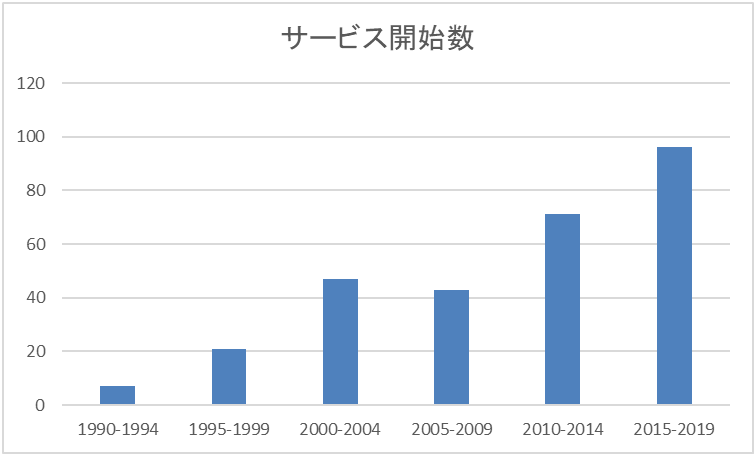
		n=	(%)						
全体		(308)	29.9	17.5	19.2	12.7	6.8	14.0	
割付セル	銀行・地銀	(31)	22.6	16.1	12.9	16.1	16.1	16.1	
	クレジットカード	(31)	29.0	6.5	12.9	9.7	12.9	29.0	
	保険	(31)	38.7	12.9	16.1	9.7	3.2	19.4	
	証券	(31)	25.8	16.1	16.1	12.9	16.1	12.9	
	インターネット販売（ECサイト）	(31)	32.3	32.3	12.9	12.9	9.7		
	ゲーム	(29)	24.1	17.2	10.3	31.0	3.4	13.8	
	不動産	(31)	35.5	19.4	35.5	9.7			
	旅行	(31)	29.0	12.9	22.6	12.9	9.7	12.9	
	交通機関	(31)	29.0	16.1	22.6	6.5	6.5	19.4	
	通信	(31)	32.3	25.8	29.0	6.5	6.5		

Q1：回答結果概要

ユーザ規模が 1000 未満のサービスが一番多いが、セキュリティ的には心配な規模である。不動産以外は 500 万以上の規模のサービスもあり、規模的には、小から大までカバーされている。

Q2

提供しているサービスの開始年月はいつですか。
※わからない方はおおよそにてお答えください。



5年レンジ	サービス開始数
1990-1994	7
1995-1999	21
2000-2004	47
2005-2009	43
2010-2014	71
2015-2019	96

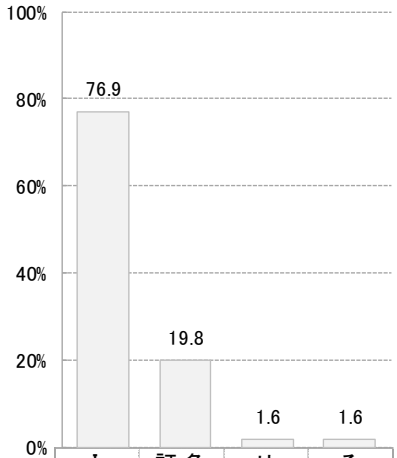
Q2：回答結果概要

全体として、回答者の約半数（５４％）が2010年以降のサービス開始となっている。回答は、年次で頂いているが、集計・分析にあたっては、５年レンジでの数値をグラフ化し傾向を把握した。

2005 年～2009 年のレンジで小さな落ち込みがある。回答者の偏りの可能性もあるが、その後の伸び率は同じなので、本レンジで落ち込む理由を調査する必要がある。

Q3

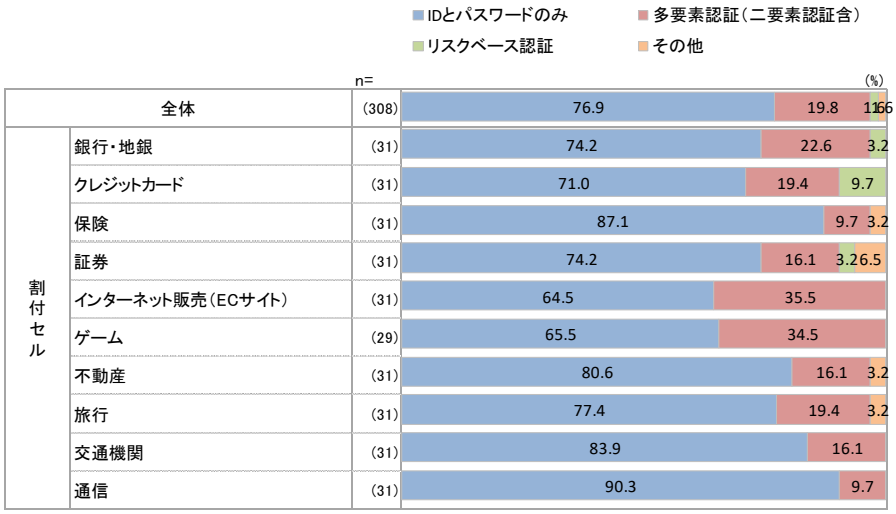
個人認証を主にどのような方法で実施していますか。



n=30以上の場合

［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	IDとパスワードのみ	多要素認証（二要素認証含）	リスクベース認証	その他
全体		(308)	76.9	19.8	1.6	1.6
割付セル	銀行・地銀	(31)	74.2	22.6	3.2	0.0
	クレジットカード	(31)	71.0	19.4	9.7	0.0
	保険	(31)	87.1	9.7	0.0	3.2
	証券	(31)	74.2	16.1	3.2	6.5
	インターネット販売（ECサイト）	(31)	64.5	35.5	0.0	0.0
	ゲーム	(29)	65.5	34.5	0.0	0.0
	不動産	(31)	80.6	16.1	0.0	3.2
	旅行	(31)	77.4	19.4	0.0	3.2
	交通機関	(31)	83.9	16.1	0.0	0.0
	通信	(31)	90.3	9.7	0.0	0.0



		n=	IDとパスワードのみ	多要素認証（二要素認証含）	リスクベース認証	その他
全体		(308)	76.9	19.8	1	1.6
割付セル	銀行・地銀	(31)	74.2	22.6		3.2
	クレジットカード	(31)	71.0	19.4	9.7	
	保険	(31)	87.1	9.7		3.2
	証券	(31)	74.2	16.1	3.2	6.5
	インターネット販売（ECサイト）	(31)	64.5	35.5		
	ゲーム	(29)	65.5	34.5		
	不動産	(31)	80.6	16.1		3.2
	旅行	(31)	77.4	19.4		3.2
	交通機関	(31)	83.9	16.1		
	通信	(31)	90.3	9.7		

Q3：回答結果概要

全体を通して 75%以上の組織が ID、パスワードのみの認証しか行っていなかった。業種は、通信、保険、交通機関で比率が高かった。インターネット販売、ゲーム業界では、30%以上が多要素認証を取り入れており、特に対応が進んでいるといえる。

Q3：WG による考察

銀行・地銀業界、クレジットカード業界では ID とパスワードのみの認証が中心であるが、これはログイン時のみで、資産の移動など重要な操作の際に追加で多要素認証等を必須にしているケースも考えられるため、一概に対応が遅れているとはいえない。

銀行・地銀業界では、 ID とパスワードのみ実施と答えた 23 サンプル中 6 サンプルが ID 数 1000 未満、クレジットカード業界では、ID とパスワードのみ実施と答えた 22 サンプル中 9 サンプルが ID 数 1000 未満だったため、これが原因で対応が遅れているように見えた。

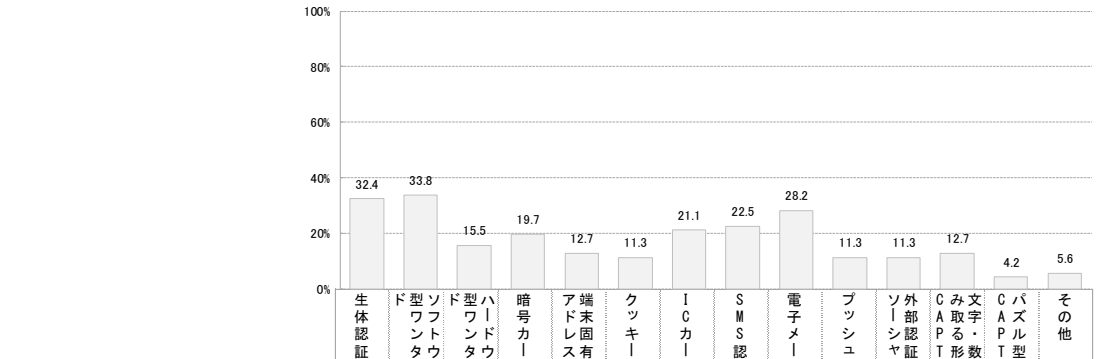
※ID 数 1000 以上のサンプルに絞った場合は、ID とパスワードのみを採用している組織は、クレジットカード業界では 59%、銀行・地銀では 70%となり、数値が下がった。

銀行・地銀では、 ID 数 1000 未満の 7 サンプル中 6 サンプルで ID とパスワードのみが採用されていた。FISC の安全対策基準にて多要素認証が推奨されているため、対応を進めていく必要がある。

クレジットカード業界では、 ID 数 1000 未満の 9 サンプル中 9 サンプルで ID とパスワードのみが採用されていた。 これらが、ID とパスワードのみの比率を上げたと思われる。ID 数が少ない企業ほど対応が遅れていると考える。

Q4

どのような認証方式を採用していますか。採用しているすべての方式を選択してください。
（Q3 にて「ID とパスワードのみ」と回答した者以外 71 名に質問）



n=30以上の場合

［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	生体認証	ソフトウェアトークン型ワンタイムパスワード	ハードウェアトークン型ワンタイムパスワード	暗号カード	端末固有番号（MACアドレス）	クッキー	ICカード	SMS認証	電子メール認証	プッシュ認証	外部認証サービス・ソーシャルログイン	文字・数字の画像を読み取る形のCAPTCHA認証	パズル型のCAPTCHA認証	その他
全体		(71)	32.4	33.8	15.5	19.7	12.7	11.3	21.1	22.5	28.2	11.3	11.3	12.7	4.2	5.6
割付セル	銀行・地銀	(8)	25.0	62.5	12.5	12.5	12.5	0.0	0.0	12.5	12.5	0.0	0.0	25.0	0.0	0.0
	クレジットカード	(9)	11.1	33.3	0.0	33.3	22.2	22.2	55.6	33.3	22.2	33.3	0.0	11.1	0.0	11.1
	保険	(4)	75.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	25.0	0.0	0.0
	証券	(8)	37.5	12.5	0.0	25.0	12.5	12.5	50.0	12.5	12.5	12.5	12.5	12.5	12.5	25.0
	インターネット販売（ECサイト）	(11)	54.5	36.4	27.3	18.2	0.0	0.0	9.1	27.3	36.4	0.0	18.2	9.1	0.0	0.0
	ゲーム	(10)	10.0	30.0	30.0	20.0	10.0	10.0	20.0	20.0	30.0	0.0	20.0	10.0	0.0	0.0
	不動産	(6)	33.3	33.3	16.7	0.0	0.0	0.0	0.0	16.7	50.0	16.7	16.7	0.0	0.0	16.7
	旅行	(7)	42.9	0.0	14.3	14.3	0.0	28.6	14.3	42.9	28.6	14.3	0.0	0.0	0.0	0.0
	交通機関	(5)	20.0	60.0	20.0	40.0	40.0	0.0	20.0	20.0	60.0	20.0	20.0	40.0	40.0	0.0
	通信	(3)	33.3	66.7	0.0	0.0	33.3	33.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Q4：回答結果概要

銀行・地銀業界では、60%以上がソフトウェアトークン型ワンタイムパスワードを採用しており、ハードウェアトークン型ワンタイムパスワードや端末固有番号、SMS 認証、ソーシャルログインなども併用していた。

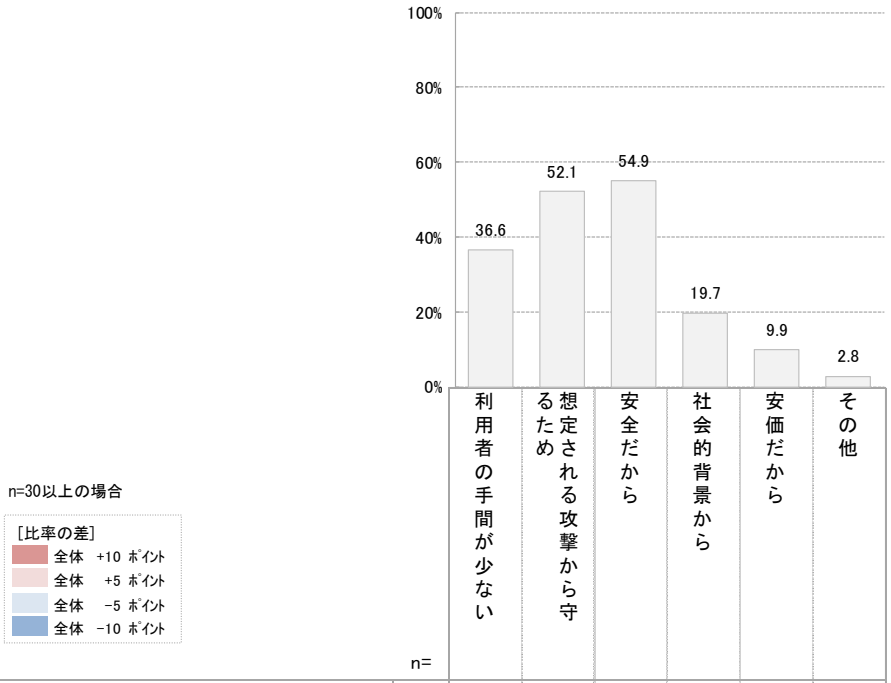
クレジットカード業界では、半数以上が IC カードを採用しており、暗号カードやソフトウェアトークン型ワンタイムパスワード、端末固有番号、クッキー、SMS 認証、電子メール認証、プッシュ認証なども併用していた。

Q4：WG による考察

併用している方式に関しては、組み合わせの種類が多いことに対して、サンプル数が少ないため（銀行・地銀：5 サンプル、クレジットカード：5 サンプル）、結果の信用性を高めるために他の調査などの確認ほか対応が必要と思われる。

Q5

その方式を採用した理由を教えてください。（複数回答可）
（Q3 にて「ID とパスワードのみ」と回答した者以外 71 名に質問）



		n=	利用者の手間が少ない	想定される攻撃から守るため	安全だから	社会的背景から	安価だから	その他
全体		(71)	36.6	52.1	54.9	19.7	9.9	2.8
割付セル	銀行・地銀	(8)	25.0	62.5	62.5	12.5	12.5	0.0
	クレジットカード	(9)	55.6	55.6	44.4	22.2	11.1	0.0
	保険	(4)	50.0	50.0	50.0	50.0	25.0	0.0
	証券	(8)	25.0	50.0	50.0	37.5	12.5	12.5
	インターネット販売（ECサイト）	(11)	45.5	36.4	63.6	0.0	0.0	0.0
	ゲーム	(10)	60.0	50.0	50.0	10.0	0.0	0.0
	不動産	(6)	16.7	83.3	33.3	33.3	16.7	16.7
	旅行	(7)	0.0	42.9	85.7	14.3	0.0	0.0
	交通機関	(5)	60.0	40.0	60.0	20.0	20.0	0.0
	通信	(3)	0.0	66.7	33.3	33.3	33.3	0.0

Q5：回答結果概要

銀行・地銀は、手間の少なさより、攻撃から守ること、安全重視となる結果だった。クレジットカードは、安全全般よりも手間の少なさが若干だがポイントが高い。インターネット販売、旅行は、安全であることが一番となっている。利便性を意識した手間の少なさが高い業種は、ゲーム、交通機関であった。

Q5：WG による考察

銀行・地銀業界、インターネット販売業界では特に、セキュリティ面を重視して認証方式を採用して

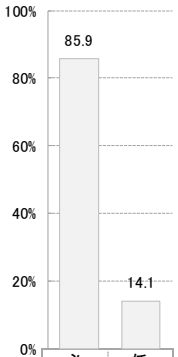
いることがわかった。これは、攻撃者によって認証が突破された際の被害が特に大きいことが理由と考えられる。

交通機関業界、ゲーム業界では、利便性も重要視した認証方式を採用する傾向にあることがわかった。

通信において、想定される攻撃から守るためが突出しているのは、セキュリティの専門性の高さを感じるところである。

Q6

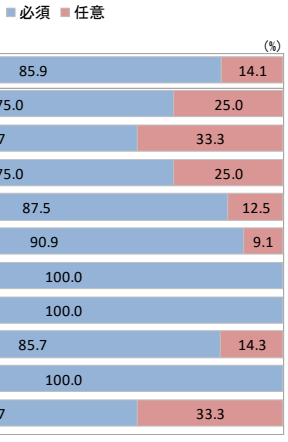
ID、パスワード方式以外の認証方法を用意している場合その認証方式の利用を必須としていますか。　（Q3 にて「ID とパスワードのみ」と回答した者以外 71 名に質問）



n=30以上の場合

［比率の差］
全体　+10 ポイント
全体　+5 ポイント
全体　−5 ポイント
全体　−10 ポイント

		n=	必須	任意
全体		(71)	85.9	14.1
割付セル	銀行・地銀	(8)	75.0	25.0
	クレジットカード	(9)	66.7	33.3
	保険	(4)	75.0	25.0
	証券	(8)	87.5	12.5
	インターネット販売（ECサイト）	(11)	90.9	9.1
	ゲーム	(10)	100.0	0.0
	不動産	(6)	100.0	0.0
	旅行	(7)	85.7	14.3
	交通機関	(5)	100.0	0.0
	通信	(3)	66.7	33.3



Q6：回答結果概要

ゲーム、不動産、交通機関が 100%、次いでインターネット販売、証券、旅行がほぼ平均以上となっている。

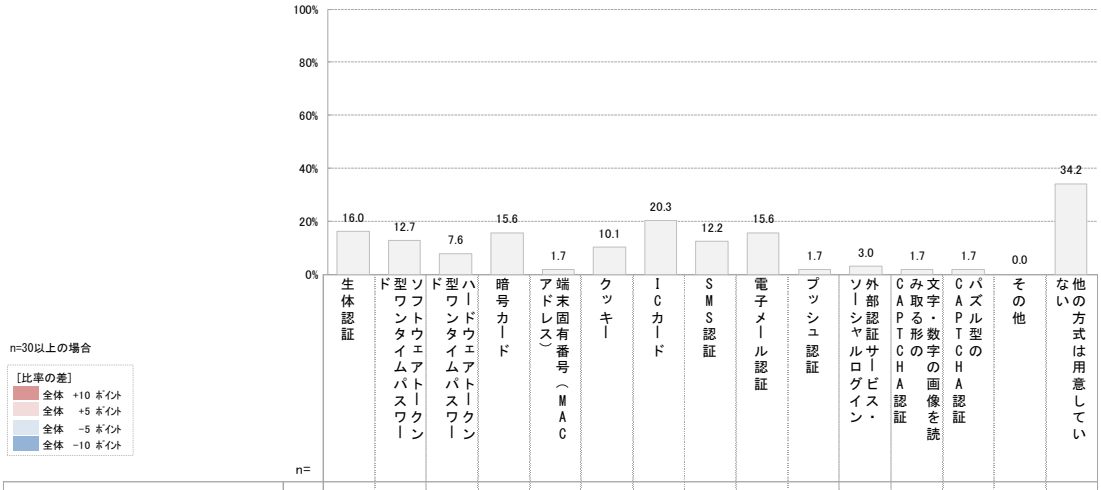
Q6：WG による考察

ID、パスワード方式以外の認証方法を用意している組織のうち 9 割近くがその認証方法を必須にしており、セキュリティ対策としては効果的に運用されているといえる。

銀行・地銀、クレジットカードが平均より低いのは、多要素認証の 2 段階目以降を求められるかは、提供サービスの内容、利用者の目的次第で変わるため、低い数値になっていると推測される。

Q7

任意で利用できる他の方式の認証は用意していますか。（複数回答可）
（Q3 にて「ID とパスワードのみ」と回答した者 237 名に質問）



n=30以上の場合
［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	生体認証	ソフトウェアトークン型ワンタイムパスワード	ハードウェアトークン型ワンタイムパスワード	暗号カード	端末固有番号（MACアドレス）	クッキー	ICカード	SMS認証	電子メール認証	プッシュ認証	外部認証サービス・ソーシャルログイン	文字・数字の画像を読み取る形のCAPTCHA認証	パズル型のCAPTCHA認証	その他	他の方式は用意していない
全体		(237)	16.0	12.7	7.6	15.6	1.7	10.1	20.3	12.2	15.6	1.7	3.0	1.7	1.7	0.0	34.2
割付セル	銀行・地銀	(23)	26.1	34.8	21.7	21.7	0.0	13.0	30.4	13.0	21.7	0.0	4.3	4.3	0.0	0.0	8.7
	クレジットカード	(22)	18.2	13.6	4.5	9.1	0.0	4.5	27.3	9.1	13.6	4.5	0.0	0.0	0.0	0.0	54.5
	保険	(27)	29.6	7.4	7.4	14.8	0.0	7.4	11.1	11.1	18.5	0.0	3.7	0.0	0.0	0.0	29.6
	証券	(23)	0.0	4.3	0.0	4.3	0.0	4.3	13.0	8.7	13.0	0.0	0.0	0.0	0.0	0.0	65.2
	インターネット販売（ECサイト）	(20)	10.0	10.0	5.0	10.0	0.0	25.0	5.0	15.0	20.0	10.0	10.0	5.0	10.0	0.0	40.0
	ゲーム	(19)	5.3	26.3	15.8	10.5	0.0	21.1	15.8	31.6	21.1	0.0	0.0	0.0	0.0	0.0	26.3
	不動産	(25)	16.0	4.0	20.0	32.0	12.0	16.0	28.0	4.0	16.0	0.0	0.0	8.0	0.0	0.0	20.0
	旅行	(24)	16.7	4.2	0.0	8.3	0.0	4.2	20.8	16.7	12.5	0.0	0.0	0.0	0.0	0.0	50.0
	交通機関	(26)	19.2	11.5	0.0	26.9	0.0	0.0	34.6	7.7	7.7	0.0	3.8	0.0	0.0	0.0	19.2
	通信	(28)	14.3	14.3	3.6	14.3	3.6	10.7	14.3	10.7	14.3	3.6	7.1	0.0	7.1	0.0	32.1

Q7：回答結果概要

以下考察にて数値の解説も合わせて説明。

Q7：WG による考察

・IC カードが 20.3%で最大。

銀行ではインターネットバンキングの法人利用の際に、システムへのログインに IC カードを利用する場合がある。

クレジットカードはクレジットカード自体、不動産は IC カードキー、交通機関は電子マネー用 IC カードの利用などが考えられる。他の用途で IC カード利用がない業界だと利用数が少ない。
現状でこの利用率であれば、マイナンバーカードの普及が進めば、個人利用で促進される可能性がある。

・生体認証

平均で 16%と予想より高めであった。スマホアプリへの認証に、スマホ端末（OS）が提供する生体認証の機能（Touch ID、Face ID など）を利用するケースで回答されていると思われる。

・SMS 認証・電子メール認証
SMS 認証が 12.2%、電子メール認証 15.6%で、合計すると 27.8%となり、IC カード認証を超えて最大の割合となる。携帯電話・スマホが普及し、SMS および電子メールという携帯電話・スマホが標準で備えている機能を利用するため利用者側の導入障壁が低いと判断されていることがうかがえる。
ただし、認証時ではなく、アカウント登録時の到達確認メッセージも含んでいる可能性がある。
各業界でまんべんなく利用されている。
経路外認証としてとらえると、プッシュ認証も合わせて 29.5%。

・ワンタイムパスワード（OTP）
ハードウェアトークンよりソフトウェアトークンの利用が進んでいる。
ハードウェアトークンについては銀行と不動産が多い。スマホを持っていない利用者の割合が高いことを考慮していると思われる。
ゲームにおいても、スマホの普及以前にゲーム内資産の移動が可能なゲームではハードウェアトークンの利用が推奨されていた。現在ではスマホの普及により、ソフトウェアトークンへの移行が進んでいる。

・暗号カード
過去にはインターネットバンキングでよく利用されていたが、現在はタイムベース・ワンタイムパスワード（TOTP）への移行が進んでいる。しかし、地銀では根強く利用されており、一部のネット銀行でも利用が続けられている。
（不動産、交通機関での利用数が多い理由は推測できなかった）

・外部認証サービス・ソーシャルログイン
Google や Yahoo！Japan のアカウントや SNS アカウントを利用する外部認証サービス（ソーシャルログイン）は 3.0%に留まった。
「外部認証サービス」および「ソーシャルログイン」が、何を差しているのか理解されていない可能性がある。
今回対象となった業界の大半である金融・インフラ関連サービスでは、認証を外部委託しづらいのは理解できる。

・少数派について
MAC アドレス、プッシュ認証、CAPTCHA（文字入力型・パズル型共に）が少数派。
それぞれが何を指すのか理解されていない可能性がある。特に CAPTCHA は、もっと利用されている印象。
「その他」は 0%。今回用意した選択肢で現状は網羅していたと考えられる。

・「他の方式は用意していない」

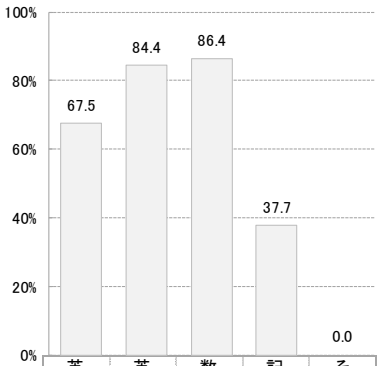
実のところ、この 34.2%の割合が最も大きい。クレジットカード、証券、旅行では半数以上。アンケート対象者全体からすると 26.3%。73.7%のサービスが利用者にパスワード以外の認証方法を提供している。
銀行は最も少なく、8.7%のみ。顧客の資産と、その移動を扱うサービスなので納得の結果と言える。
追加の認証要素は、利用者の選択肢を増やす意味でも用意されるべきだが、扱う情報・資産の内容によっては必ずしも必須とも言えない。
今後の FIDO や他の認証方式の普及により、要素追加だけでなく、要素の置き換えも含めてどう変化していくか観測していきたい。

・ID 数との相関
ID 数が少ないサービスは「他の方式を用意していない」の選択率が高い。

・複数採用しているかどうか
業界による偏りは見当たらず、単一採用の場合、複数の場合が存在した。
ID 数についても同様。

Q8

パスワードに使用できる文字は、何を設定していますか。（複数回答可）



n=30以上の場合

［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	英文字（大文字）	英文字（小文字）	数字	記号	その他
全体		(308)	67.5	84.4	86.4	37.7	0.0
割付セル	銀行・地銀	(31)	58.1	83.9	87.1	25.8	0.0
	クレジットカード	(31)	67.7	96.8	87.1	54.8	0.0
	保険	(31)	58.1	87.1	93.5	25.8	0.0
	証券	(31)	64.5	90.3	90.3	51.6	0.0
	インターネット販売（ECサイト）	(31)	71.0	87.1	96.8	45.2	0.0
	ゲーム	(29)	82.8	89.7	86.2	44.8	0.0
	不動産	(31)	67.7	77.4	74.2	32.3	0.0
	旅行	(31)	61.3	80.6	80.6	25.8	0.0
	交通機関	(31)	64.5	64.5	77.4	19.4	0.0
	通信	(31)	80.6	87.1	90.3	51.6	0.0

Q8：回答結果概要

数字、英小文字を使用できるサービスが大半。続いて英大文字。大きく減らして記号の順。その他は 0%。この割合に業界による差異は、記号の使用率がやや大きい業界がある程度。

Q8：WG による考察

組み合わせごとの回答数は以下の通り

-大文字だけ：14

-小文字だけ：23

-数字だけ：16

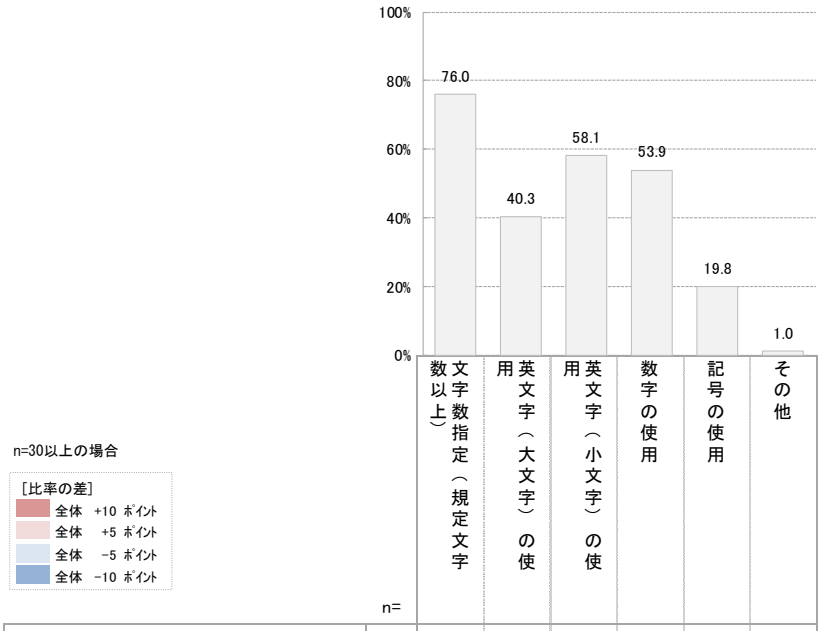
-記号だけ：0
-大文字+小文字：5
-大文字+数字：15
-大文字+記号：0
-小文字+数字：47
-小文字+記号：0
-数字+記号：1
-大文字+小文字+数字：72
-大文字+数字+記号：2
-大文字+小文字+記号：0
-小文字+数字+記号：13
-すべて使用可：100

「すべて使用可」が最大派。次点が「大文字+小文字+数字」。
大文字よりも小文字の使用可率が高い。
記号を使用可の場合は、数字も使用可。

利用者がどの文字種を使用するかは利用者の選択としても、サービス事業者側では、すべての文字種を使えるようにしておいた方が望ましいと思われる。

Q9

パスワード設定ルールで必須としているものを教えてください。（複数回答可）



		n=	文字数指定（規定文字数以上）	英文字（大文字）の使用	英文字（小文字）の使用	数字の使用	記号の使用	その他
全体		(308)	76.0	40.3	58.1	53.9	19.8	1.0
割付セル	銀行・地銀	(31)	71.0	25.8	45.2	48.4	12.9	0.0
	クレジットカード	(31)	80.6	45.2	64.5	64.5	22.6	0.0
	保険	(31)	71.0	35.5	64.5	64.5	19.4	3.2
	証券	(31)	77.4	29.0	54.8	45.2	22.6	0.0
	インターネット販売（ECサイト）	(31)	80.6	51.6	67.7	67.7	25.8	0.0
	ゲーム	(29)	82.8	34.5	55.2	51.7	17.2	0.0
	不動産	(31)	77.4	45.2	54.8	48.4	22.6	0.0
	旅行	(31)	67.7	32.3	48.4	29.0	12.9	6.5
	交通機関	(31)	74.2	41.9	54.8	58.1	9.7	0.0
	通信	(31)	77.4	61.3	71.0	61.3	32.3	0.0

Q9：回答結果概要

「文字数指定（規定文字数以上）」を 24%は指定していない。

文字数だけ必須化しており、文字種の必須化をしていないサービスは 87 件。

各文字種を指定している中の 52～69%が、その文字種に使用を必須化。

各文字種を使用可能にしているサービスで、その文字種を必須化している割合は以下の通り

-大文字使用可で必須：59.6%

-小文字使用可で必須：68.8%

-数字使用可で必須：62.4%

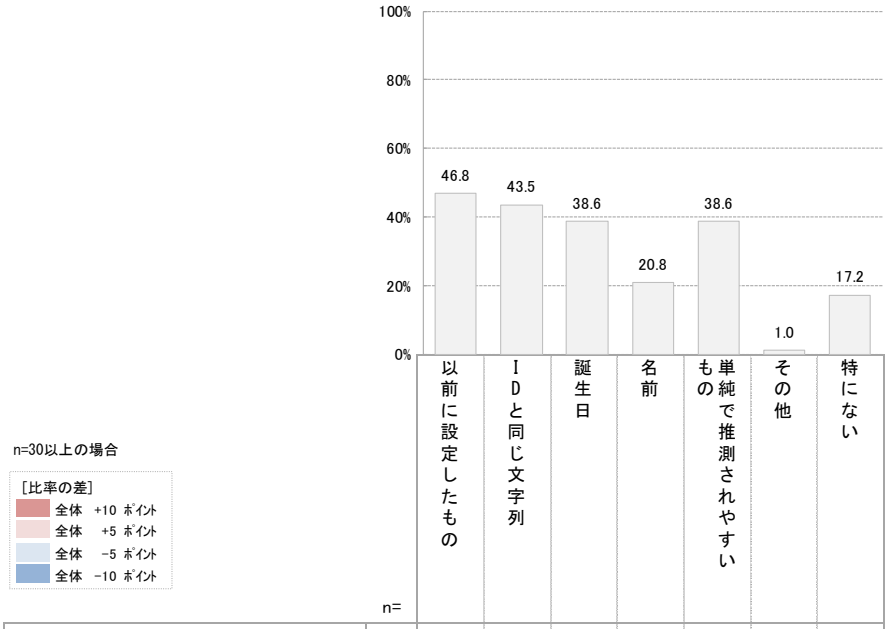
-記号使用可で必須：52.6%

Q9：WG による考察

各文字種を指定している中の 52～69%が、その文字種に使用を必須化しており、半数以上が安全性の高い状況といえる。文字種の選択の自由度を広げる反面、より安全が確保されるルールの運用が望ましい。

Q10

パスワードの文字で、設定不可としているパターンはありますか。（複数回答可）



n=30以上の場合

［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	以前に設定したもの	IDと同じ文字列	誕生日	名前	単純で推測されやすいもの	その他	特にない
全体		(308)	46.8	43.5	38.6	20.8	38.6	1.0	17.2
割付セル	銀行・地銀	(31)	41.9	35.5	58.1	19.4	48.4	0.0	12.9
	クレジットカード	(31)	51.6	54.8	54.8	29.0	45.2	0.0	9.7
	保険	(31)	58.1	41.9	35.5	12.9	41.9	6.5	12.9
	証券	(31)	41.9	22.6	32.3	19.4	41.9	0.0	29.0
	インターネット販売（ECサイト）	(31)	51.6	48.4	29.0	19.4	32.3	0.0	19.4
	ゲーム	(29)	34.5	65.5	37.9	13.8	37.9	0.0	13.8
	不動産	(31)	41.9	45.2	41.9	29.0	32.3	3.2	12.9
	旅行	(31)	41.9	41.9	19.4	12.9	38.7	0.0	19.4
	交通機関	(31)	48.4	45.2	48.4	25.8	38.7	0.0	9.7
	通信	(31)	54.8	35.5	29.0	25.8	29.0	0.0	32.3

Q10：回答結果概要

「以前に設定したもの」の設定不可が 46.8%で、逆に許容しているのが 53.2%と半数を超える。

ゲーム業界において、「ID と同じ文字列」を設定不可とする割合が大きい。

旅行業界において、「誕生日」を設定不可とする割合が小さい。

Q10：WG による考察

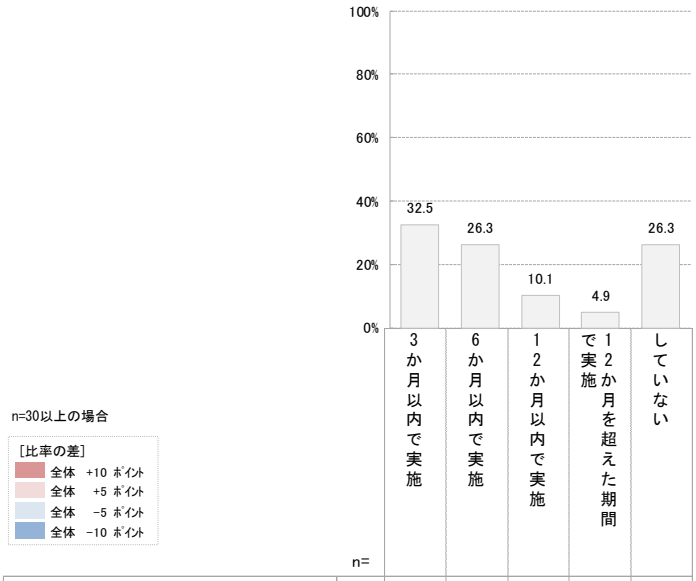
「パスワードの定期的な変更を要求している」状況とのクロスで本回答を分析すると、定期的な変更を要求していると回答した 227 件の中で、「以前に設定したもの」を設定不可としているのは 119 件で、52%。「パスワードの定期的な変更の実施を必須としている」と回答した 168 件の中で、「以前に設定したもの」を設定不可としているのは 95 件で、56.5%。パスワードの定期的変更を要求または必須としておきながらも、変更しないことを容認する場合が半数近くある状況。このようなサービスは定期的変更を実施させながらも、本質的なパスワード変更の必要性を満たしているとはいいがたい。

ゲーム業界において、「ID と同じ文字列」を設定不可とする割合が大きい。ID を利用者自身で設定できるサービスが多いことが理由と思われる。

旅行業界において、「誕生日」を設定不可とする割合が小さいが、理由の推測はできなかった。

「単純で推測されやすいもの」を設定不可とする割合が 38.6%だが、パスワード辞書攻撃で使用されやすいパスワードを不可とする対策がなされることが望ましく、今後はこの割合の増加を期待したい。

Q11
パスワードの定期的な変更を要求していますか。



		n=	3か月以内で実施	6か月以内で実施	12か月以内で実施	12か月を超えた期間で実施	していない
全体		(308)	32.5	26.3	10.1	4.9	26.3
割付セル	銀行・地銀	(31)	45.2	29.0	6.5	3.2	16.1
	クレジットカード	(31)	54.8	19.4	6.5	0.0	19.4
	保険	(31)	48.4	19.4	3.2	9.7	19.4
	証券	(31)	22.6	22.6	12.9	3.2	38.7
	インターネット販売（ECサイト）	(31)	25.8	22.6	9.7	3.2	38.7
	ゲーム	(29)	31.0	13.8	10.3	6.9	37.9
	不動産	(31)	25.8	38.7	9.7	6.5	19.4
	旅行	(31)	32.3	29.0	9.7	6.5	22.6
	交通機関	(31)	22.6	29.0	19.4	9.7	19.4
	通信	(31)	16.1	38.7	12.9	0.0	32.3

Q11：回答結果概要

3 か月以内、6 か月以内合わせての定期変更要求が 58.8%と半数となった。また、定期的な変更を行っていないサービスが 26.3%を占めた。

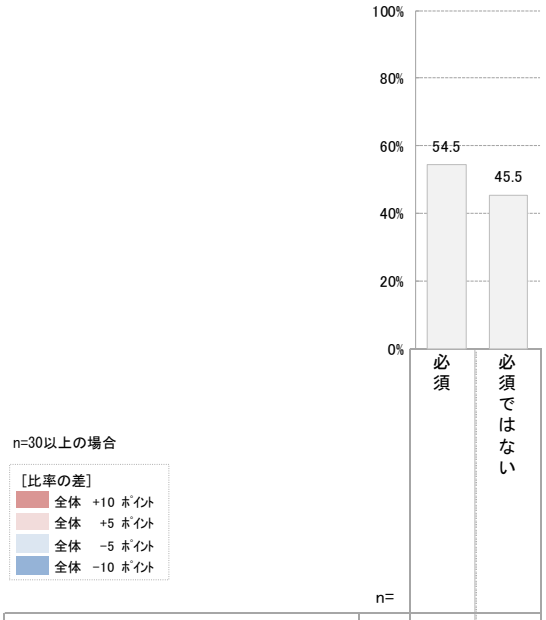
Q11：WG による考察

銀行やクレジットカード会社に関しては金銭的な被害がリスクとして想定されるためか 3 か月以内、6 か月以内の定期的な変更をユーザに呼びかけている傾向がわかった。

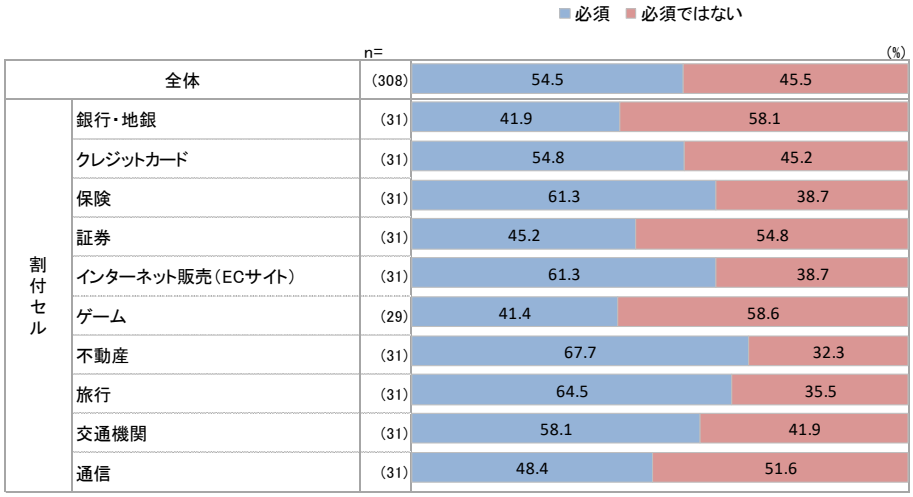
保険会社に関しても、個人情報やセンシティブな情報をやりとりするためか、3 か月以内の定期的な変更をユーザに呼びかけている傾向がわかった。

変更を要求する期間としては 3 ヶ月以内で実施することが多くみられ、12 ヶ月などの長期的な期間では要求していないことがわかった。

Q12
パスワードの定期的な変更の実施は必須ですか。



		n=	必須	必須ではない
全体		(308)	54.5	45.5
割付セル	銀行・地銀	(31)	41.9	58.1
	クレジットカード	(31)	54.8	45.2
	保険	(31)	61.3	38.7
	証券	(31)	45.2	54.8
	インターネット販売(ECサイト)	(31)	61.3	38.7
	ゲーム	(29)	41.4	58.6
	不動産	(31)	67.7	32.3
	旅行	(31)	64.5	35.5
	交通機関	(31)	58.1	41.9
	通信	(31)	48.4	51.6



Q12：回答結果概要

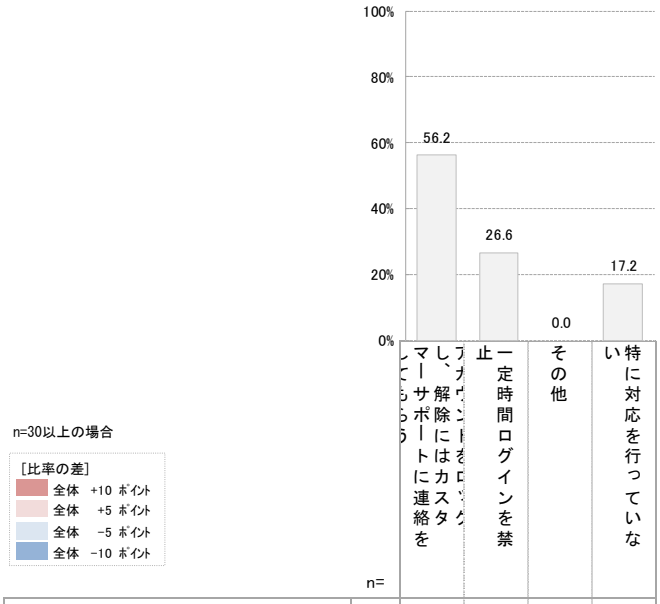
全体としては、必須 54.5%。必須、必須でないは、半々となった。銀行・地銀、ゲームが 40%そこそこで低い傾向がある。保険会社に関しては 61%が必須と答えており、必須としているシステムがやや多かった。

Q12：WG による考察

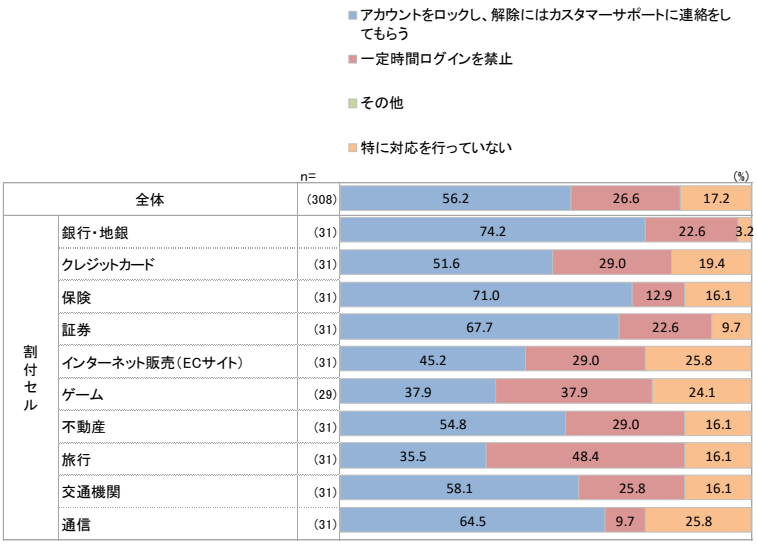
銀行やクレジットカード業者では、Q11 で定期的な変更を呼びかける傾向があったが、呼びかけるのみで変更を強制していないことがわかった。

不動産会社からも定期変更を必須としていることがわかった。また、不動産会社に関しては本質問で必須との答えと、必須ではないと答えで Q11 の回答傾向は大きく変わらなかった。（定期変更の呼びかける期間に関しては偏りがなかった）

Q13
一定回数パスワード入力を間違えた場合の対応を教えてください。



		n=	マーサポートに連絡を	一定時間ログインを禁止	その他	特に対応を行っていない
全体		(308)	56.2	26.6	0.0	17.2
割付セル	銀行・地銀	(31)	74.2	22.6	0.0	3.2
	クレジットカード	(31)	51.6	29.0	0.0	19.4
	保険	(31)	71.0	12.9	0.0	16.1
	証券	(31)	67.7	22.6	0.0	9.7
	インターネット販売（ECサイト）	(31)	45.2	29.0	0.0	25.8
	ゲーム	(29)	37.9	37.9	0.0	24.1
	不動産	(31)	54.8	29.0	0.0	16.1
	旅行	(31)	35.5	48.4	0.0	16.1
	交通機関	(31)	58.1	25.8	0.0	16.1
	通信	(31)	64.5	9.7	0.0	25.8



Q13：回答結果概要

銀行や保険証券ではカスタマーサポートの連絡をしてもらい、EC サイトは特に何も対応を行っていないと回答が多かった。

「特に対応を行っていない」と回答した方は 53 名(17.2%)

Q13：WG による考察

「特に対応を行っていない」と回答した方は 53 名(17.2%)で、多要素認証を行っている可能性もあるので確認した。

53 名中で Q3 個人認証の方法で「ID とパスワードのみ」と回答した方は 45 名(84.91%)

53 名中で Q4 認証方式の回答者は 8 名おり、

ぞれぞれの回答は

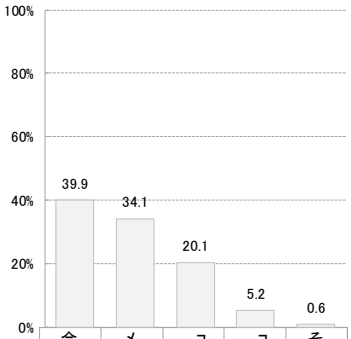
生体認証	4 件 57.14%
ソフトトークン	1 件 14.29%
ハードトークン	1 件 14.29%
SMS	2 件 28.57%
メール	1 件 14.29%
プッシュ	2 件 28.57%
外部認証	2 件 28.57%
CAPTCHA	1 件 14.29%
その他	1　14.29%

その他 1 件は「指紋」と記載されており、その方は生体認証を選択していたため、重複とみなし 0 件と考えてもよい。

このことから、対応を行っていないサービスは、ID とパスワードのみの認証であることがわかる。

対応していない理由には、ボット対応やカスタマーサポートのコストとの兼ね合いもありえる。
今後は、パスワード管理ツールの利用などで「アカウントのロック」は減っていく傾向にあると思われる。

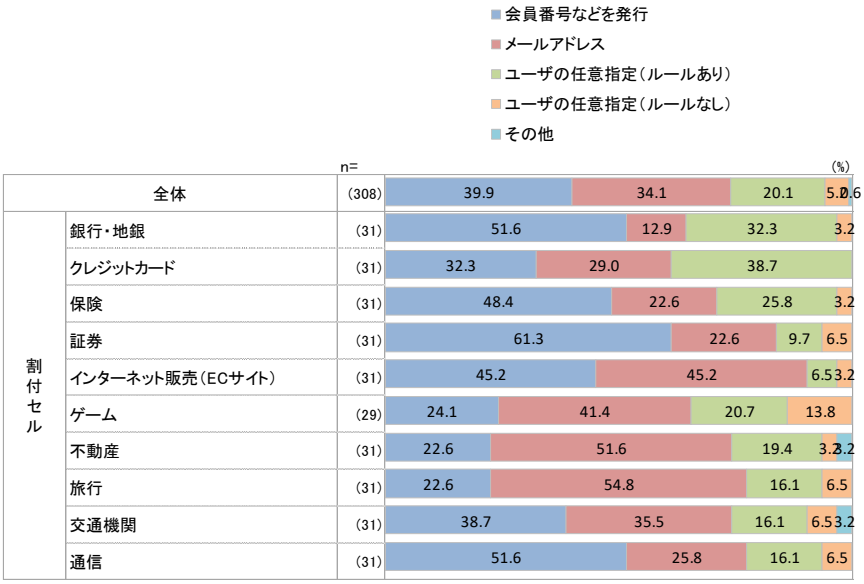
Q14
ID は、どのように決定していますか。



n=30以上の場合

[比率の差]
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	会員番号などを発行	メールアドレス	ユーザの任意指定（ルールあり）	ユーザの任意指定（ルールなし）	その他
全体		(308)	39.9	34.1	20.1	5.2	0.6
割付セル	銀行・地銀	(31)	51.6	12.9	32.3	3.2	0.0
	クレジットカード	(31)	32.3	29.0	38.7	0.0	0.0
	保険	(31)	48.4	22.6	25.8	3.2	0.0
	証券	(31)	61.3	22.6	9.7	6.5	0.0
	インターネット販売（ECサイト）	(31)	45.2	45.2	6.5	3.2	0.0
	ゲーム	(29)	24.1	41.4	20.7	13.8	0.0
	不動産	(31)	22.6	51.6	19.4	3.2	3.2
	旅行	(31)	22.6	54.8	16.1	6.5	0.0
	交通機関	(31)	38.7	35.5	16.1	6.5	3.2
	通信	(31)	51.6	25.8	16.1	6.5	0.0



		n=	会員番号などを発行	メールアドレス	ユーザの任意指定（ルールあり）	ユーザの任意指定（ルールなし）	その他
全体		(308)	39.9	34.1	20.1	5.2	0.6
割付セル	銀行・地銀	(31)	51.6	12.9	32.3	3.2	
	クレジットカード	(31)	32.3	29.0	38.7		
	保険	(31)	48.4	22.6	25.8	3.2	
	証券	(31)	61.3	22.6	9.7	6.5	
	インターネット販売（ECサイト）	(31)	45.2	45.2	6.5	3.2	
	ゲーム	(29)	24.1	41.4	20.7	13.8	
	不動産	(31)	22.6	51.6	19.4	3.2	3.2
	旅行	(31)	22.6	54.8	16.1	6.5	
	交通機関	(31)	38.7	35.5	16.1	6.5	3.2
	通信	(31)	51.6	25.8	16.1	6.5	

Q14：回答結果概要

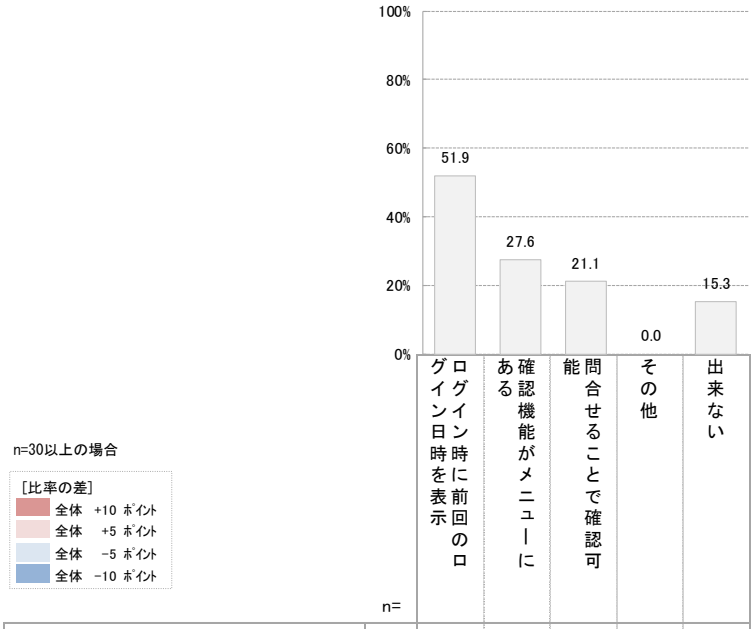
会員番号の発行のようにサービス提供者側からの指定や、メールアドレスなど既存の ID を利用させる回答が 74%と多い。特に証券、銀行・地銀、通信などは、独自の会員番号など発行してのログイン実施の傾向がみられる。

Q14：WG による考察

EC サイトはユーザの離脱を怖れ、簡単な ID 設定となっていると想定され、ユーザビリティとしてはメールアドレスの方が覚えやすいため離脱は減ると考えられ、クレジットカード会社や EC サイトに関してはメールアドレスを使う場合が多いと思われる。また会員番号による ID 設定もみられる。

EC サイトなどジャンルによっては、開発会社が専用のパッケージや ASP サービスを作っている場合も多く、この場合はそれぞれの製品に依存すると考えられるため、今後この観点での調査も必要と思われる。

Q15
ログイン履歴を確認できますか。（複数回答可）



		n=	ログイン時に前回のログイン日時を表示	確認機能がメニューにある	問合せることで確認可能	その他	出来ない
全体		(308)	51.9	27.6	21.1	0.0	15.3
割付セル	銀行・地銀	(31)	54.8	22.6	19.4	0.0	9.7
	クレジットカード	(31)	51.6	25.8	19.4	0.0	12.9
	保険	(31)	71.0	12.9	16.1	0.0	12.9
	証券	(31)	58.1	29.0	9.7	0.0	19.4
	インターネット販売（ECサイト）	(31)	41.9	32.3	19.4	0.0	22.6
	ゲーム	(29)	48.3	34.5	24.1	0.0	10.3
	不動産	(31)	58.1	38.7	25.8	0.0	19.4
	旅行	(31)	38.7	25.8	22.6	0.0	19.4
	交通機関	(31)	54.8	32.3	25.8	0.0	6.5
	通信	(31)	41.9	22.6	29.0	0.0	19.4

Q15：回答結果概要

全体としては、前回のログイン日時が表示できるサービスは約半数。特に保険の 71%が突出している。

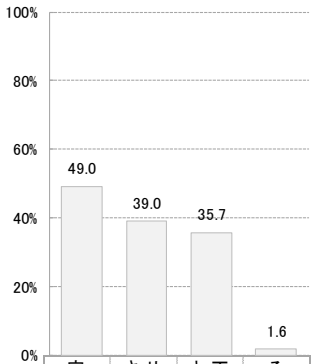
Q15：WG による考察

日常的にログイン履歴を確認することは、不正アクセスの状況をいち早く確認することにつながる。しかしながら、前回のログイン日時が表示できるサービスは約半数にとどまっていることが判明した。

問い合わせることで確認できるという回答も 20%程度あるが、簡単に確認できるようにしなければ不正対策としては効果が薄いと言える。

ログイン時に前回のログイン日時を表示し、かつ、確認機能がメニューに有る形が理想ではあるが、その割合は 11.4%にとどまっている。

Q16
どの様なことをきっかけに認証の強化を検討しますか。（複数回答可）



n=30以上の場合

［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	定期的に見直している	サービスの内容が追加されたとき	不正利用などがあったとき	その他
全体		(308)	49.0	39.0	35.7	1.6
割付セル	銀行・地銀	(31)	64.5	38.7	35.5	0.0
	クレジットカード	(31)	61.3	22.6	32.3	0.0
	保険	(31)	45.2	41.9	41.9	0.0
	証券	(31)	35.5	32.3	41.9	3.2
	インターネット販売（ECサイト）	(31)	38.7	35.5	41.9	3.2
	ゲーム	(29)	62.1	27.6	34.5	3.4
	不動産	(31)	54.8	54.8	22.6	3.2
	旅行	(31)	54.8	22.6	35.5	3.2
	交通機関	(31)	45.2	48.4	29.0	0.0
	通信	(31)	29.0	64.5	41.9	0.0

Q16：回答結果概要

定期的に認証の見直しを行っている企業が約半数ある。特に銀行、クレジットカード、ゲーム業界はその割合が平均値よりも更に高くなっている。

一方、証券やインターネット販売、通信業界はその割合が低くなっている。

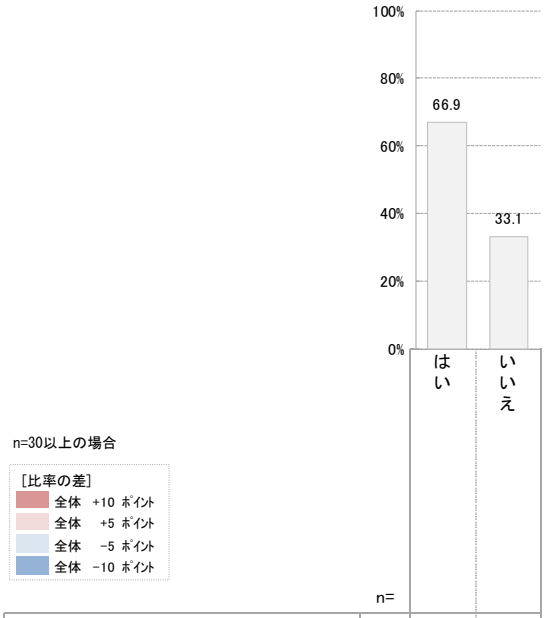
Q16：WG による考察

不正利用などがあった際の見直しは 3～4 割前後にとどまり、定期的な見直しよりも少ないのが現状である。

不正利用があった際、それが認証に起因するものかどうかを確認し、新たな対抗手段を検討することも有効と言える。

Q17

ポイントの利用やクレジットカードの利用など、ユーザにとって資産価値のあるものを使用する際には追加の認証を必要としていますか。



		n=	はい	いいえ
全体		(308)	66.9	33.1
割付セル	銀行・地銀	(31)	54.8	45.2
	クレジットカード	(31)	71.0	29.0
	保険	(31)	61.3	38.7
	証券	(31)	51.6	48.4
	インターネット販売（ECサイト）	(31)	77.4	22.6
	ゲーム	(29)	89.7	10.3
	不動産	(31)	74.2	25.8
	旅行	(31)	64.5	35.5
	交通機関	(31)	71.0	29.0
	通信	(31)	54.8	45.2

Q17：回答結果概要

資産価値のある情報を取り扱うにあたり、以前のサービスでの情報との格差が業種ごとに顕著にみられる。ゲームは、89.7%と突出している。

ゲーム、インターネット販売、不動産、クレジットカード、交通機関が、平均値を超えている。

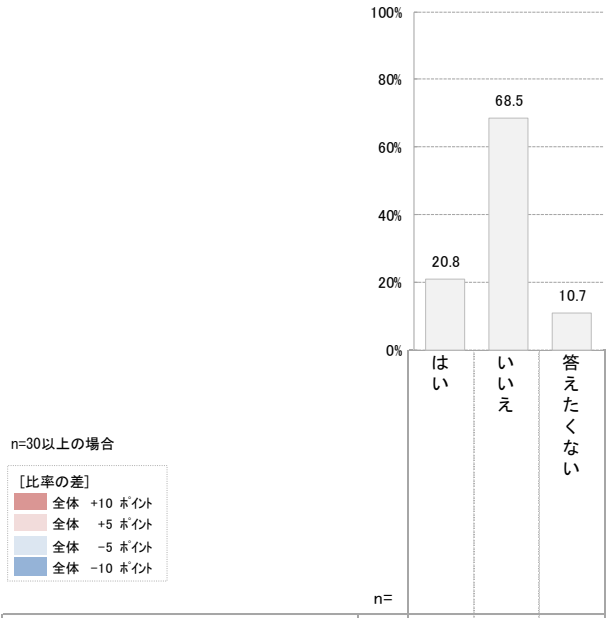
Q17：WG による考察

平均値を超えているサービスは、いずれも一般的な情報と、資産価値のある情報と併せ持っており、その価値もユーザにとって重要な内容である。それら遺産価値のある情報の利用について追加での認証の導入を積極的に検討していることは安心できるが、銀行、クレジットカードでは、実際 45%もの銀行業界の回答者が「追加認証を必要としていない」と回答していることについて、さらなる確認が必要と思われる。

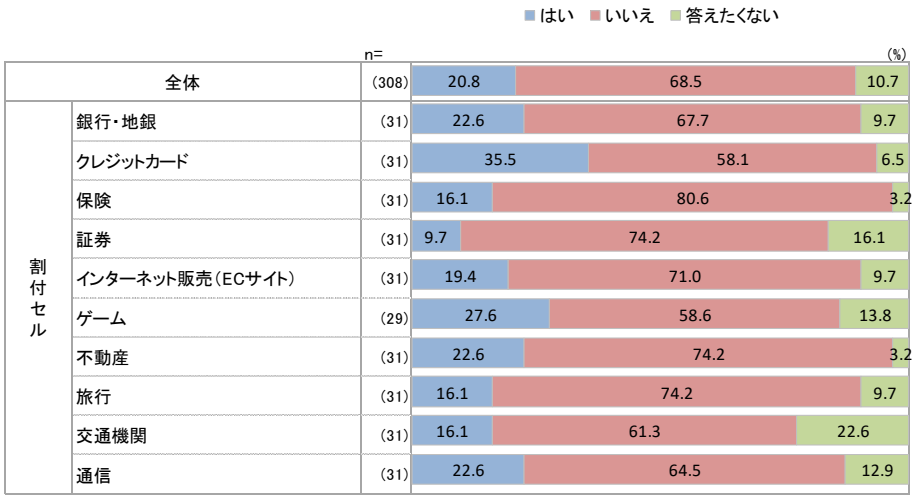
自身のサービスで追加認証を実施している場合もあるが、利用しているプラットフォーム上で追加認証を提供しているケースもあり得る。例えばゲームの場合、決済時の Google Play や App Store の認証を指しているケースも考えられる。

Q18

運営しているサービスがアカウントの不正利用の被害にあったことはありますか。



		n=	はい	いいえ	答えたくない
全体		(308)	20.8	68.5	10.7
割付セル	銀行・地銀	(31)	22.6	67.7	9.7
	クレジットカード	(31)	35.5	58.1	6.5
	保険	(31)	16.1	80.6	3.2
	証券	(31)	9.7	74.2	16.1
	インターネット販売（ECサイト）	(31)	19.4	71.0	9.7
	ゲーム	(29)	27.6	58.6	13.8
	不動産	(31)	22.6	74.2	3.2
	旅行	(31)	16.1	74.2	9.7
	交通機関	(31)	16.1	61.3	22.6
	通信	(31)	22.6	64.5	12.9



Q18：回答結果概要

不正利用の被害にあったことがあると回答したサービスは、20.8%に上った。クレジットカードやゲームが他よりも不正利用が多い状況。

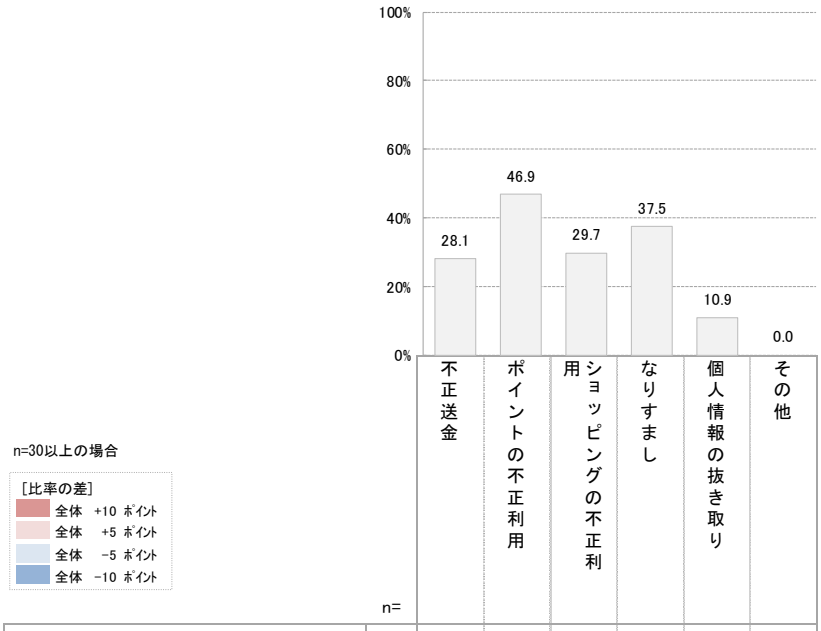
Q18：WG による考察

クレジットカードやゲームとも、一方はカードの不正利用、一方は RMT などで不正利用によって金銭的メリットを得ることができるためと推測できる。

金銭面でのメリットを享受しやすいサービスを扱っている業界がターゲットになりやすいことの裏付けにもなりえる。

Q19

それはどのような被害でしたか。（複数回答可）（Q18 で「はい」と回答した方のみ回答）



		n=	不正送金	ポイントの不正利用	ショッピングの不正利用	なりすまし	個人情報の抜き取り	その他
全体		(64)	28.1	46.9	29.7	37.5	10.9	0.0
割付セル	銀行・地銀	(7)	57.1	42.9	28.6	28.6	14.3	0.0
	クレジットカード	(11)	9.1	54.5	45.5	54.5	18.2	0.0
	保険	(5)	40.0	40.0	20.0	40.0	20.0	0.0
	証券	(3)	33.3	0.0	33.3	33.3	0.0	0.0
	インターネット販売（ECサイト）	(6)	0.0	16.7	33.3	83.3	0.0	0.0
	ゲーム	(8)	25.0	62.5	37.5	50.0	12.5	0.0
	不動産	(7)	42.9	57.1	14.3	42.9	0.0	0.0
	旅行	(5)	0.0	60.0	0.0	20.0	20.0	0.0
	交通機関	(5)	60.0	60.0	20.0	0.0	0.0	0.0
	通信	(7)	28.6	42.9	42.9	0.0	14.3	0.0

Q19：回答結果概要

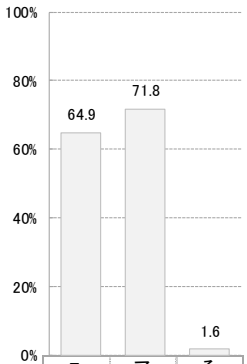
インターネット販売では、「なりすまし」被害が 83.3%と圧倒的に多い。次いで、ゲーム、交通機関、旅行のポイント不正利用が多い。

Q19：WG による考察

交通機関については、「高価値のものには追加認証」をする率が高く、「被害に遭った経験」も少ないなか、「ポイントの不正利用」「不正送金」の率が高いのは、対策の傾向をこれらに絞ることでさらに被害が減少できると思われる。

Q20

不正利用が発生、発覚した時にどのような対応を行っていますか。（複数回答可）



n=30以上の場合

［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	ユーザに知らせる	アカウントロック	その他
全体		(308)	64.9	71.8	1.6
割付セル	銀行・地銀	(31)	64.5	64.5	0.0
	クレジットカード	(31)	67.7	67.7	3.2
	保険	(31)	54.8	77.4	3.2
	証券	(31)	67.7	67.7	0.0
	インターネット販売（ECサイト）	(31)	67.7	77.4	0.0
	ゲーム	(29)	79.3	65.5	0.0
	不動産	(31)	64.5	80.6	3.2
	旅行	(31)	61.3	67.7	0.0
	交通機関	(31)	61.3	71.0	3.2
	通信	(31)	61.3	77.4	3.2

Q20：回答結果概要

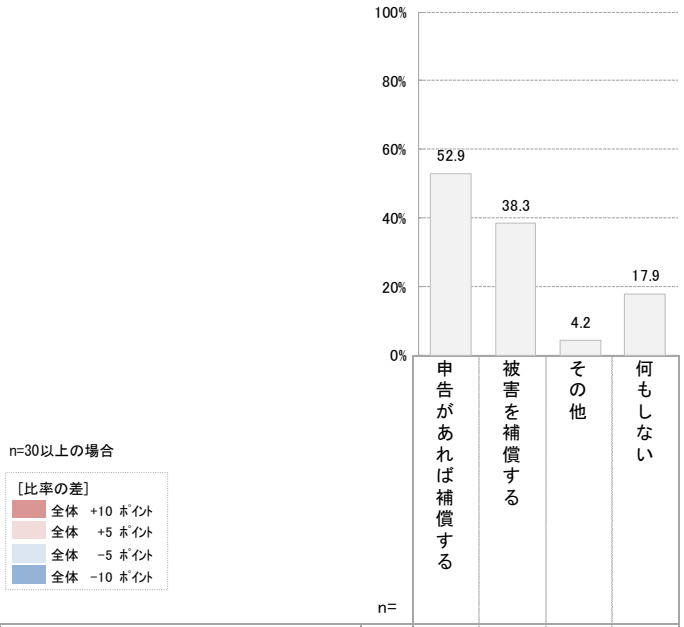
「ユーザに知らせる」64.9%、「アカウントロック」71.8%、ともに高い回答となった。

Q20：WG による考察

保険、旅行、交通機関について、不正利用が発生・発覚した際に「ユーザに知らせる」率が、他と比べて若干低くみられる。何か業界の特性がある可能性がある。

Q21

不正利用の被害にあった利用者にどのような対応をしていますか。（複数回答可）



		n=	申告があれば補償する	被害を補償する	その他	何もしない
全体		(308)	52.9	38.3	4.2	17.9
割付セル	銀行・地銀	(31)	45.2	54.8	9.7	6.5
	クレジットカード	(31)	58.1	41.9	6.5	16.1
	保険	(31)	35.5	35.5	3.2	35.5
	証券	(31)	51.6	41.9	3.2	19.4
	インターネット販売（ECサイト）	(31)	51.6	38.7	3.2	16.1
	ゲーム	(29)	58.6	44.8	0.0	10.3
	不動産	(31)	61.3	35.5	6.5	9.7
	旅行	(31)	61.3	16.1	3.2	25.8
	交通機関	(31)	64.5	48.4	0.0	3.2
	通信	(31)	41.9	25.8	6.5	35.5

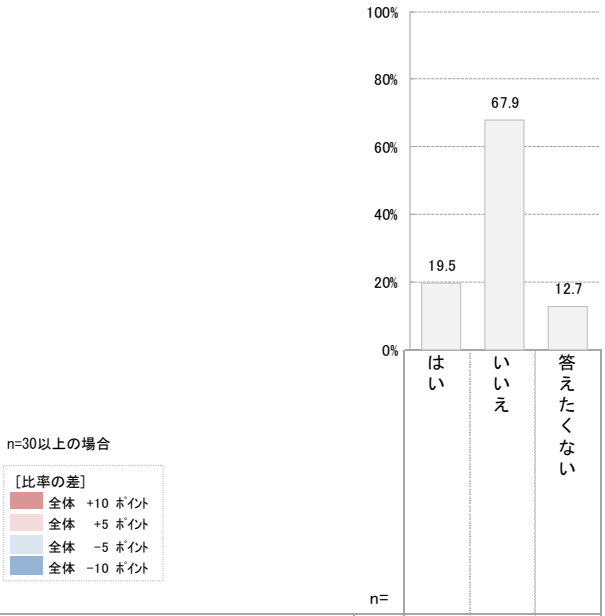
Q21：回答結果概要

「申告があれば補償する」が、必ず「被害を補償する」を超えている。保険、通信の「何もしない」が他に比べて高め。

Q21：WG による考察

被害の全部か一部かに関わらず補償するというのが大半と想定していたが、「何もしない」の率が全般的に高いと感じられる。

Q22
不正な攻撃などの被害にあったことはありますか。



		n=	はい	いいえ	答えたくない
全体		(308)	19.5	67.9	12.7
割付セル	銀行・地銀	(31)	16.1	74.2	9.7
	クレジットカード	(31)	38.7	48.4	12.9
	保険	(31)	16.1	80.6	3.2
	証券	(31)	16.1	74.2	9.7
	インターネット販売（ECサイト）	(31)	25.8	58.1	16.1
	ゲーム	(29)	31.0	51.7	17.2
	不動産	(31)	19.4	71.0	9.7
	旅行	(31)	3.2	87.1	9.7
	交通機関	(31)	12.9	61.3	25.8
	通信	(31)	16.1	71.0	12.9

Q22：回答結果概要

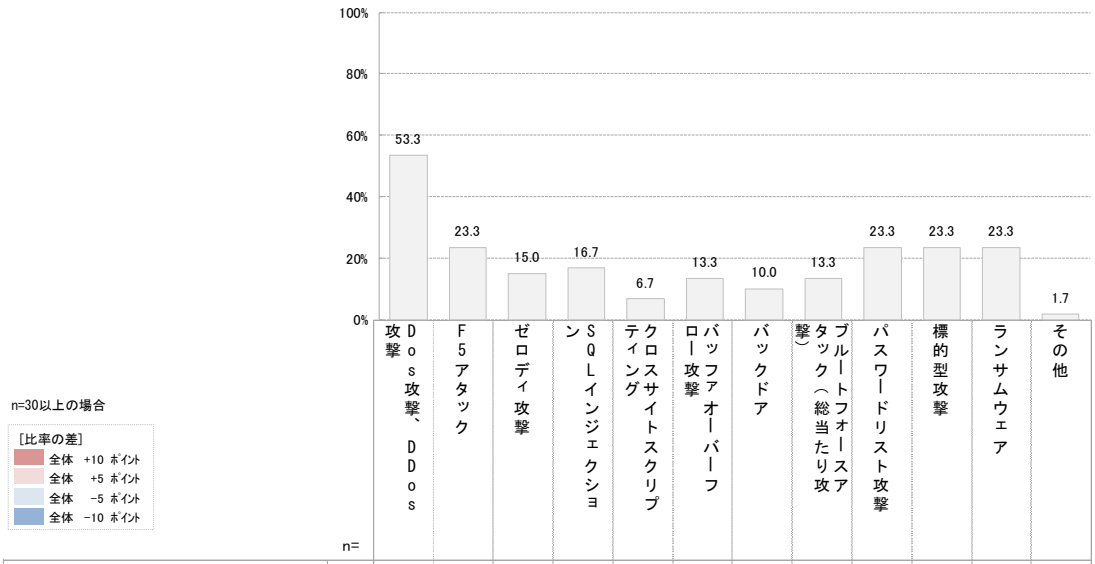
不正攻撃にあったサービスは、19.5%であった。クレジットカード 38.7%、ゲーム 31%が突出している。

Q22：WG による考察

クレジットカード、ゲーム、インターネット販売(EC)について「被害にあった」率が高いが、それだけ利活用が進んでおり、ターゲットが見つけやすい状況になっていると思われる。

一方、銀行・地銀、保険、証券については被害を受けにくくする対策が効いており、「被害にあった」という回答が低いと思われる。

Q23
それはどのような攻撃でしたか。（複数回答可）



		n=	DoS攻撃、DDoS攻撃	F5アタック	ゼロディ攻撃	SQLインジェクション	クロスサイトスクリプティング	バッファオーバーフロー攻撃	バックドア	ブルートフォースアタック（総当たり攻撃）	パスワードリスト攻撃	標的型攻撃	ランサムウェア	その他
全体		(60)	53.3	23.3	15.0	16.7	6.7	13.3	10.0	13.3	23.3	23.3	23.3	1.7
割付セル	銀行・地銀	(5)	20.0	20.0	0.0	20.0	0.0	40.0	0.0	40.0	40.0	20.0	20.0	0.0
	クレジットカード	(12)	58.3	25.0	25.0	16.7	8.3	16.7	41.7	8.3	33.3	58.3	50.0	0.0
	保険	(5)	20.0	0.0	0.0	20.0	0.0	0.0	0.0	20.0	0.0	20.0	60.0	0.0
	証券	(5)	60.0	40.0	40.0	20.0	20.0	20.0	0.0	20.0	20.0	40.0	40.0	20.0
	インターネット販売（ECサイト）	(8)	37.5	0.0	25.0	25.0	12.5	0.0	0.0	25.0	25.0	12.5	12.5	0.0
	ゲーム	(9)	77.8	22.2	22.2	22.2	11.1	0.0	0.0	0.0	22.2	0.0	0.0	0.0
	不動産	(6)	66.7	16.7	0.0	0.0	0.0	33.3	0.0	0.0	16.7	16.7	16.7	0.0
	旅行	(1)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0
	交通機関	(4)	50.0	50.0	0.0	0.0	0.0	0.0	25.0	0.0	25.0	0.0	0.0	0.0
	通信	(5)	80.0	60.0	0.0	20.0	0.0	20.0	0.0	20.0	20.0	0.0	0.0	0.0

Q23：回答結果概要

DoS 攻撃、 DDoS 攻撃が 53.3%と半数を超えている。そのほかの攻撃に大きな差はないが、業種でみた場合、偏りがみられる。

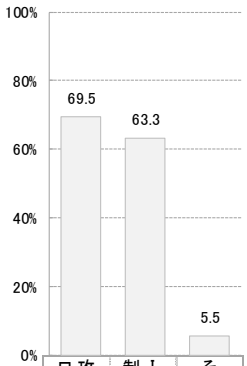
Q23：WG による考察

F５アタックも含めた DoS 攻撃、 DDoS 攻撃の割合が多くなっているが、検索エンジンからの探索や攻撃者による事前調査アクセスも回答数に含まれている可能性があり、データの読み取りに注意が必要。

Web サイトへの攻撃の内、パスワードリスト攻撃の割合が多いのはフィッシングサイト等によって詐取した ID/ パスワード が利用されている裏付けの一つになると想定される。

Q24

不正な攻撃にあった場合、どのような対応を行っていますか。（複数回答可）



n=30以上の場合

［比率の差］
全体 +10 ポイント
全体 +5 ポイント
全体 −5 ポイント
全体 −10 ポイント

		n=	攻撃者からの攻撃をブロック	IPアドレスアクセス制限	その他
全体		(308)	69.5	63.3	5.5
割付セル	銀行・地銀	(31)	71.0	61.3	9.7
	クレジットカード	(31)	61.3	61.3	12.9
	保険	(31)	77.4	54.8	3.2
	証券	(31)	74.2	54.8	6.5
	インターネット販売（ECサイト）	(31)	67.7	77.4	0.0
	ゲーム	(29)	79.3	55.2	6.9
	不動産	(31)	67.7	71.0	6.5
	旅行	(31)	64.5	64.5	6.5
	交通機関	(31)	74.2	61.3	3.2
	通信	(31)	58.1	71.0	0.0

Q24：回答結果概要

対策について組み合わせで実施しているなど、詳細な件数は、以下の通り。

2 つの対応を実施しているのは、117 件 38%

攻撃をブロック だけ 97 件 31.5%

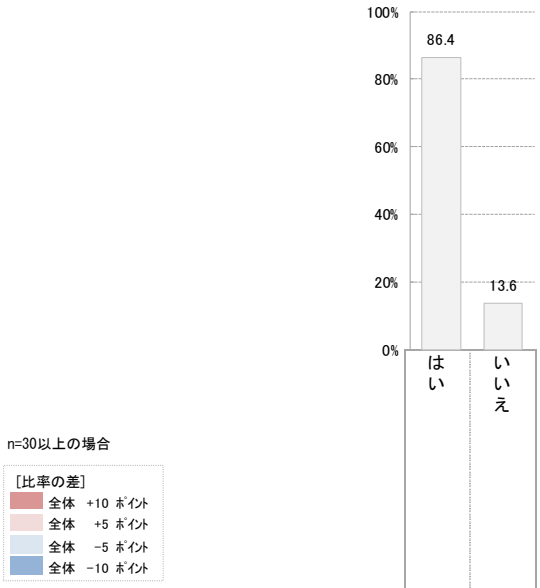
IP 制限 だけ 78 件 25.3%

Q24：WG による考察

何らかのセキュリティ機器（IPS、IDS、WAF 等）を導入し攻撃をブロックしている組織が約 70%。IP 制限による対策割合が若干少ないのは、攻撃元 IP アドレスが Bot ネット等により分散しているため制限が難しいためと考えられる。

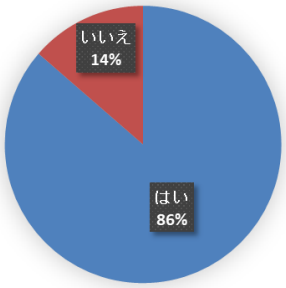
Q25

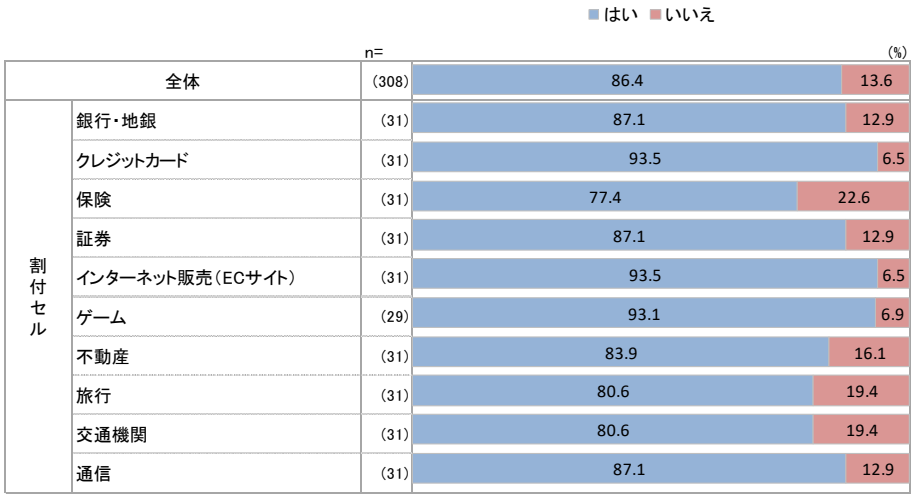
Web サイト側のパスワード管理は、何らかの方法で盗まれても問題ない状態で管理（ハッシュ、暗号化など）読めない状態で管理されていますか。



		n=	はい	いいえ
全体		(308)	86.4	13.6
割付セル	銀行・地銀	(31)	87.1	12.9
	クレジットカード	(31)	93.5	6.5
	保険	(31)	77.4	22.6
	証券	(31)	87.1	12.9
	インターネット販売（ECサイト）	(31)	93.5	6.5
	ゲーム	(29)	93.1	6.9
	不動産	(31)	83.9	16.1
	旅行	(31)	80.6	19.4
	交通機関	(31)	80.6	19.4
	通信	(31)	87.1	12.9

パスワード管理は、盗まれても問題ない状態（ハッシュ、暗号化など）読めない状態で管理されているか（n=308）





Q25：回答結果概要

86.4%の回答者が「はい（パスワードを読めない状態で管理している）」と答える一方、13.6%の回答者が「いいえ」と回答、パスワードを「平文」、つまりそのままの状態で管理していると思われる。

Q25：WG による考察

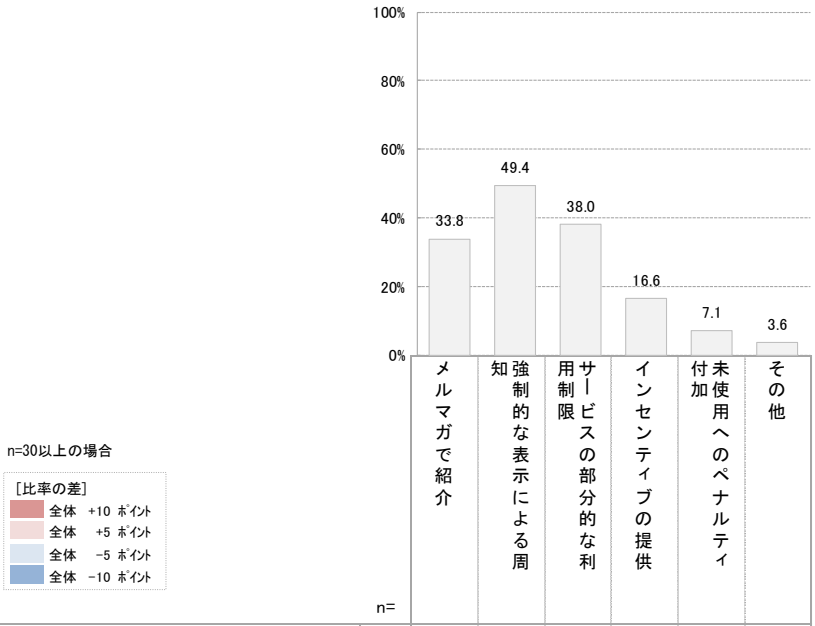
サービス事業者からの情報漏洩が頻発する中、2019 年に入ってから、利用者のパスワードデータが、パスワードそのままの「平文」で保存されていたという報道が相次いだ。

パスワードを平文のまま保存することは、万が一、パスワードデータが漏洩してしまった場合に、パスワードそのものが第三者に知られてしまい、不正アクセスにつながる恐れがある。そのため、パスワードデータを「ハッシュ化」、「暗号化」といった難読化処理を行い、元のパスワードが分からない状態で保存することで対策するが、今回「いいえ」と回答した 13.6%には、この対策が知られる前から継続している場合や、本人確認のうえ登録パスワードを知らせるサポート対応をしている場合などが含まれていると考えられる。

難読化処理は、外部からの侵入のリスクだけでなく、サービス事業者の内部スタッフが、標的型攻撃に遭い漏洩した場合や、悪意による漏洩のリスクを想定すると、標準とすべき対策だと捉えており、対応していない理由としては、サイトの稼働開始時期であったり、多層的なセキュリティ対策によりリスクを低減していたりして、改修の優先順位が低い可能性もある。アンケート結果からは承知して行っていないのか、知らずに行っていないかは判断できないため留意する必要あり。

Q26

安全だが利用者にとって手間のかかる認証を採用している場合、どのような利用啓発や対応を行っていますか。（複数回答可）



		n=	メルマガで紹介	強制的な表示による周知	サービスの部分的な利用制限	インセンティブの提供	未使用へのペナルティ付加	その他
全体		(308)	33.8	49.4	38.0	16.6	7.1	3.6
割付セル	銀行・地銀	(31)	35.5	58.1	38.7	9.7	3.2	9.7
	クレジットカード	(31)	41.9	51.6	22.6	22.6	9.7	0.0
	保険	(31)	41.9	32.3	51.6	16.1	12.9	3.2
	証券	(31)	22.6	58.1	25.8	12.9	0.0	3.2
	インターネット販売（ECサイト）	(31)	16.1	45.2	41.9	19.4	9.7	6.5
	ゲーム	(29)	34.5	48.3	37.9	17.2	3.4	0.0
	不動産	(31)	38.7	41.9	51.6	12.9	9.7	3.2
	旅行	(31)	35.5	54.8	25.8	19.4	3.2	3.2
	交通機関	(31)	38.7	51.6	38.7	22.6	12.9	3.2
	通信	(31)	32.3	51.6	45.2	12.9	6.5	3.2

Q26：回答結果概要

「表示による対応」が一番多く 49.4%とほぼ半数で実施。次いで「サービスの部分的な利用制限」「メルマガで紹介」と 30%で並ぶ。業種それぞれに 50%を超える対応があり特色がでている。

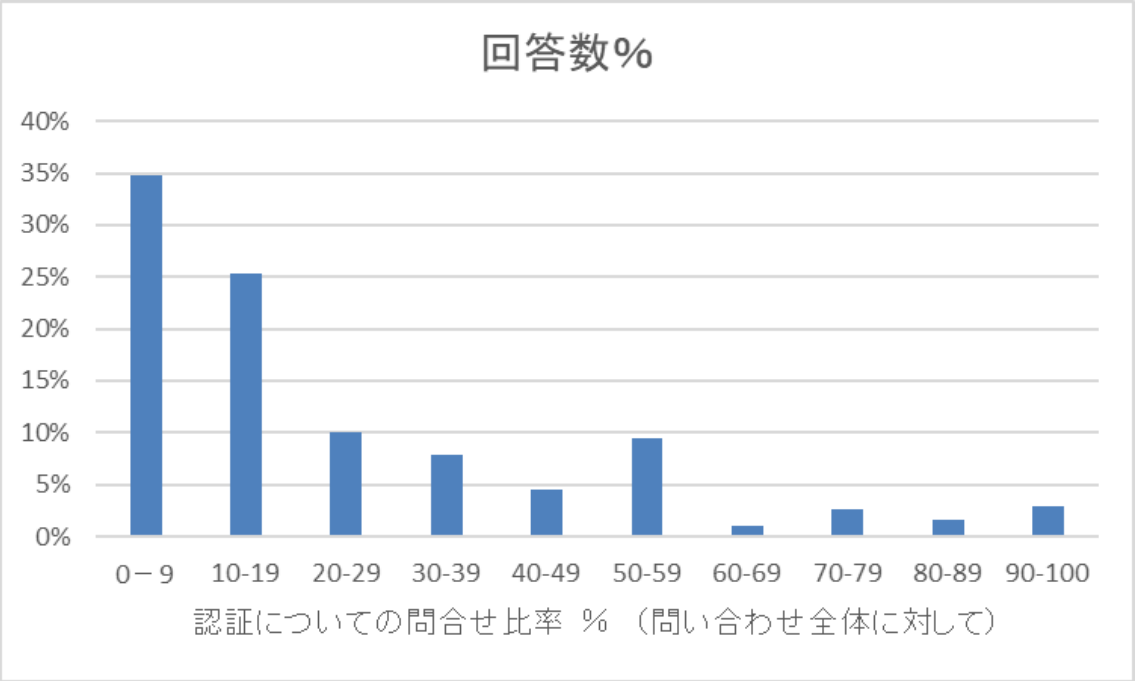
クレジットカードと交通機関が「インセンティブの提供」で 20%越えをしている。

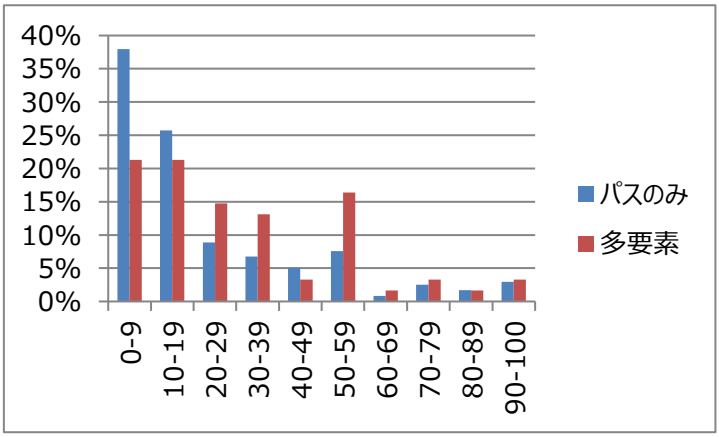
Q26：WG による考察

「サービスの部分的な利用制限」は、利用目的によって、また安全性の確保度合いによってセキュリティレベルの範囲を変えての対応で、提供者、利用者にとっても効果的な対応であると思われる。しかし、利便性を追求するサービスでは、手間のかかる認証を無理強いしにくい背景もあり、告知が主流と思われる。しかし、Web サイト上の告知であるため、対応は限定的となるのではないだろうか。

Q27

認証についての問い合わせ数は、提供サービスに関する問い合せ数全体に対してどれくらいの割合ですか





Q27：回答結果概要

認証についての問い合わせは、問合せ全体の 20%未満とする回答が 60%を占めた。逆に 50%以上とした回答も 18%ある。

認証方法によるサポートの傾向を見るため、ID パスワードだけ、多要素それぞれと比較した。多要素のほうが、認証に関するサポート対応が多いことがわかった。

Q27：WG による考察

サービス提供会社に寄せられる問い合わせの中で、認証に関連する問い合わせが占める割合は

10%未満が最も多く 35%となった。次いで 10%～20%を占める場合が 25%となり、認証に関する問い合わせ比率は 2 割以下のサービスが 60%と半数を超える。しかし、多要素認証導入と回答されたデータに絞ると、問い合わせ比率 2 割以下の回答は 43%と減少し、半数以上が認証関係と回答した比率は全体対象の 15.6%から 26.2%に増加している。

Q28

認証についての問い合わせはどのような質問が多いですか。

問い合わせ内容	カウント
ID、パスワード忘れ	77
アカウントのロック	33
ログインができない	19
認証手順	18
セキュリティについて	6
個人情報漏洩の心配	5
操作方法について	4
パスワード変更方法がわからない	3
文字数	3
パスワード設定方法	2
設定が難しい	2

問い合わせ内容	カウント
ない	54
不明	48
回答不可	9

問い合わせ内容	カウント
セキュリティの安全性の確認	1
トークンを使用しないでログインをする方法はないか	1
ハードウェアトークンの紛失	1
パスワード管理状況	1
パスワード管理方法	1
以前に使用したものに変えたい	1
英数字大文字小文字	1
顔認証の利用方法	1
高齢者からの設定のための用語についての質問。	1
生体認証がうまくできない。	1
端末の不具合など	1
定期的なID、PWの変更が不便	1
定期的な更新が必要か否か	1
認証が面倒	1
認証で貰えるはずのインセンティブが入ってこないので補填してほしい	1
認証の手間について	1
認証情報の再確認	1
認証制度全般	1
不正アカウント	1
不正アクセス	1
不正された場合の補償	1
不正利用防御対策	1
本人確認方法	1
有効期限の問い合わせ	1

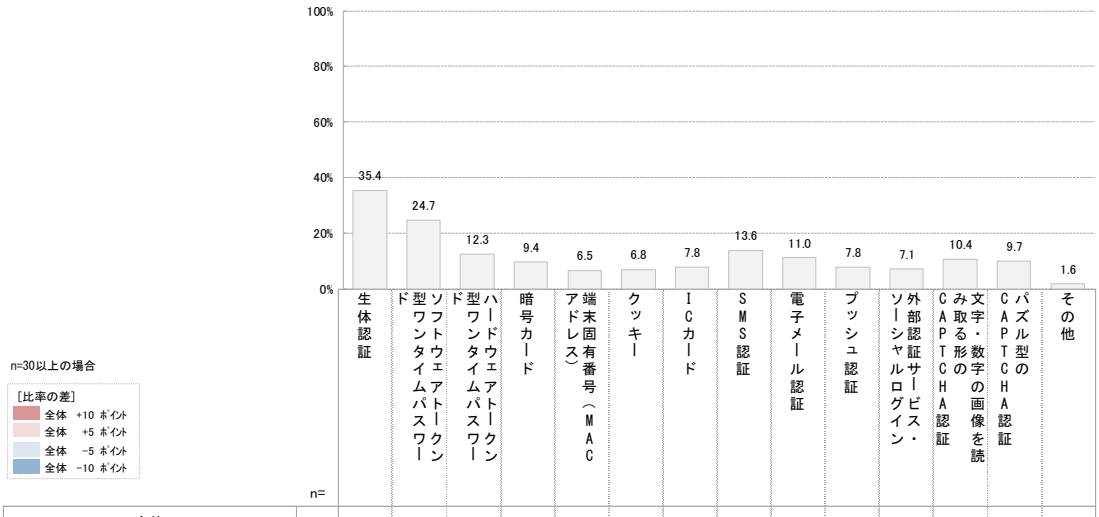
Q28：回答結果概要

認証についての問い合わせ内容は「ID、パスワード忘れ」が 77 件（25%）と最も多く、認証失敗に関する問い合わせが上位 3 つで 129 件（42%）となっている。セキュリティに関係した安全性の問い合わせも多く「セキュリティについて」、「個人情報漏洩の心配」、「操作方法について」、「パスワード変更方法がわからない」が続いており 36 件（11.7%）となっている。

Q28：WG による考察

認証ができず、サービスが利用できないことに関する問い合わせが多いのは、想定通りといえる。それに次いで情報漏洩についての質問やセキュリティに関する問い合わせなどがあることで、利用者がセキュリティに関して不安に感じている状況がわかった。

Q29
導入してみたい認証方式は、どれですか。（複数回答可）



		n=	生体認証	ソフトウェアトークン型ワンタイムパスワード	ハードウェアトークン型ワンタイムパスワード	暗号カード	端末固有番号（MACアドレス）	クッキー	ICカード	SMS認証	電子メール認証	プッシュ認証	外部認証サービス・ソーシャルログイン	文字・数字の画像を読み取る形のCAPTCHA認証	パズル型のCAPTCHA認証	その他
全体		(308)	35.4	24.7	12.3	9.4	6.5	6.8	7.8	13.6	11.0	7.8	7.1	10.4	9.7	1.6
割付セル	銀行・地銀	(31)	41.9	22.6	19.4	12.9	6.5	6.5	12.9	12.9	9.7	3.2	9.7	6.5	9.7	3.2
	クレジットカード	(31)	48.4	16.1	6.5	9.7	3.2	0.0	0.0	16.1	9.7	9.7	9.7	19.4	12.9	0.0
	保険	(31)	29.0	32.3	6.5	6.5	6.5	6.5	9.7	19.4	25.8	3.2	6.5	0.0	3.2	3.2
	証券	(31)	35.5	35.5	16.1	6.5	6.5	3.2	0.0	16.1	12.9	12.9	6.5	6.5	16.1	3.2
	インターネット販売（ECサイト）	(31)	25.8	29.0	3.2	9.7	9.7	3.2	16.1	16.1	3.2	0.0	3.2	25.8	16.1	3.2
	ゲーム	(29)	34.5	17.2	13.8	6.9	6.9	3.4	10.3	13.8	10.3	20.7	6.9	0.0	6.9	0.0
	不動産	(31)	38.7	25.8	12.9	6.5	6.5	6.5	6.5	9.7	9.7	3.2	3.2	12.9	9.7	0.0
	旅行	(31)	22.6	25.8	6.5	16.1	12.9	9.7	0.0	12.9	6.5	12.9	9.7	19.4	9.7	0.0
	交通機関	(31)	35.5	9.7	3.2	12.9	3.2	19.4	12.9	12.9	16.1	6.5	9.7	6.5	6.5	3.2
	通信	(31)	41.9	32.3	35.5	6.5	3.2	9.7	9.7	6.5	6.5	6.5	6.5	6.5	6.5	0.0

Q29：回答結果概要

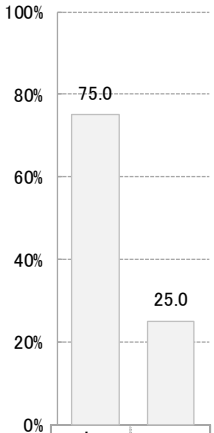
今後導入してみたい認証方式については「生体認証」となっており、クレジットカード、銀行・地銀、通信で要望が高い。次いで「ソフトウェアトークン型ワンタイムパスワード」が 24.7%となり、証券、保険、通信で要望が高い。3 番目に多いのがＳＭＳ認証となっており保険業からの要望が多い。生体認証は多要素認証をすでに導入している業界からの拡張要望、ワンタイムパスワード、ＳＭＳ認証は多要素認証導入に向けた要望となっている。生体認証は iPhone の Touch ID など、スマートフォンの生体認証利用の要望も含まれる。

Q29：WG による考察

今後導入してみたい認証方式として質問したが、現在導入が進んでいる認証方式が高い状況であり認証方式の傾向を表している。

インターネット販売業者において、CAPTCHA 認証（文字数字型）の導入要望が 25.8%あり、安全への意識が高まっていると思われる。

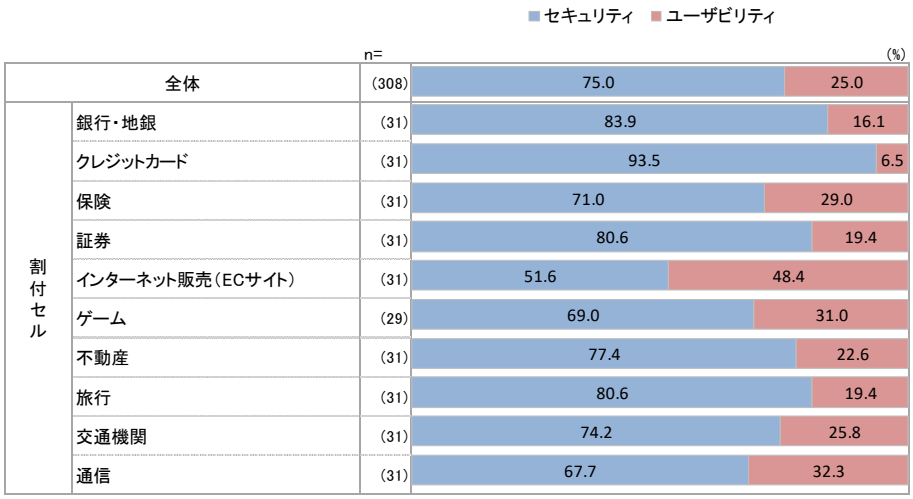
Q30
セキュリティとユーザビリティ、主にどちらを認証技術に求めますか。



n=30以上の場合

［比率の差］
全体 +10 ﾎﾟｲﾝﾄ
全体 +5 ﾎﾟｲﾝﾄ
全体 −5 ﾎﾟｲﾝﾄ
全体 −10 ﾎﾟｲﾝﾄ

		n=	セキュリティ	ユーザビリティ
全体		(308)	75.0	25.0
割付セル	銀行・地銀	(31)	83.9	16.1
	クレジットカード	(31)	93.5	6.5
	保険	(31)	71.0	29.0
	証券	(31)	80.6	19.4
	インターネット販売（ECサイト）	(31)	51.6	48.4
	ゲーム	(29)	69.0	31.0
	不動産	(31)	77.4	22.6
	旅行	(31)	80.6	19.4
	交通機関	(31)	74.2	25.8
	通信	(31)	67.7	32.3



		n=	(%)	
全体		(308)	75.0	25.0
割付セル	銀行・地銀	(31)	83.9	16.1
	クレジットカード	(31)	93.5	6.5
	保険	(31)	71.0	29.0
	証券	(31)	80.6	19.4
	インターネット販売（ECサイト）	(31)	51.6	48.4
	ゲーム	(29)	69.0	31.0
	不動産	(31)	77.4	22.6
	旅行	(31)	80.6	19.4
	交通機関	(31)	74.2	25.8
	通信	(31)	67.7	32.3

Q30：回答結果概要

認証において「セキュリティ」と「ユーザビリティ」のどちらを求めるかの質問では、「セキュリティを求める」が 75%と、ユーザビリティ要求を大きく上回った。クレジットカード、銀行・地銀、証券で 8 割以上が認証にセキュリティを求めている。

Q30：WG による考察

すべての業種において「ユーザビリティ」よりも、「セキュリティ」を求めるとなったことは、セキュリティ対策を進める本協議会、WG にとって嬉しい結果である。

クレジットカードでは 93.5%と高く、クレジットカードの不正利用に対応するためのセキュリティ強化と連動している。インターネット販売（ＥＣサイト）では要求が二分している。これは、ＥＣサイトでは認証失敗によるユーザへの影響や問い合わせ対応の増加などから、ユーザビリティ要求の比率が高くなっていると思われる。

4. まとめ

・調査対象は、１０業種、ID 規模も 1000 未満のサービスから 500 万以上のサービスまで幅広く調査できた。
・全体を通して 75%以上のサービスが ID、パスワードのみの認証しか行っていなかった。特に通信、保険、交通機関のサービス、また、ID 数が少ないサービスほど比率が高く、多要素認証への対応が遅れていると考えられる。インターネット販売、ゲーム業界では、30%以上が多要素認証を取り入れており、対応が進んでいる。
・多要素認証の種類は、金融業界が一番多くの種類を使っていた。手間を減らすよりも、安全を重視し、攻撃から守ることを重視していることがわかった。
・パスワードについては、文字の種類、ルール、定期的な変更への対応など、業種ごとの特徴が把握できた。
・認証を強化するきっかけについて、定期的に見直しているのが一番多いことで、計画的な対策がされていると推測できた。また、利用者のサービスへの接続環境が様々ある中、統一的な認証方法を強制しづらい面もあるため、定期的に見直すタイミングを作り、時世に応じた採用しやすい方法を取り入れる（流行りに乗る）ということも考えられる。
・不正利用について不正利用の被害にあったことがあると回答したサービスは、20.8%に上った。クレジットカードやゲームが他よりも不正利用が多く、金銭面でのメリットを享受しやすいサービスを扱っている業界がターゲットになりやすいことの裏付けにもなりえる。ただし、不正利用の被害がないとの回答の一部には「気づいていない」可能性があることにも留意が必要である。
・不正攻撃にあったサービスは、全体では 19.5%であったが、クレジットカード 38.7%、ゲーム 31%が突出しているのが特徴的。
・パスワードの管理にて、86.4%がパスワードデータを「ハッシュ化」、「暗号化」といった、何らかの難読化処理を行い、盗まれても問題ない状態、読めない状態で管理していると答える一方、13.6%の回答者が「いいえ」と回答、パスワードを「平文」、つまりそのままの状態で管理していると思われる。非常にショッキングな数値であった。
・認証についての問い合わせは、ID パスワードだけ、多要素それぞれと比較した結果、多要素のほうが、認証に関するサポート対応が多いことがわかった。
・認証についての問い合わせ内容は、認証関連の内容に次いで、情報漏洩についての質問やセキュリティに関する問い合わせなどがあることで、利用者がセキュリティに関して不安に感じている状況がわかった
・認証において「セキュリティ」と「ユーザビリティ」のどちらを求めるかの質問では、すべての業種において「ユーザビリティ」よりも、「セキュリティ」を求める結果となり、フィッシング被害を減らす対策を進める本協議会、WG にとって嬉しい結果である。FIDO などユーザビリティも同時に向上させるような認証方法の普及に努めていきたい。
・今後は、利用者側の意識調査も行い、サービス提供者と利用者の意識の相違や業種による適正な認証についてまとめていきたい。

5. 認証方法調査・推進ワーキンググループ メンバー

【主査】

長谷部 一泰	アルプス システム インテグレーション株式会社

【構成員】

伊藤 彰浩	株式会社アクリート
八束 啓文	ＥＭＣジャパン株式会社
山田 晃義	株式会社 ISAO
前澤 俊樹	株式会社 ISAO
田辺 英昭	NTT コミュニケーションズ株式会社
和田 亜紀夫	キヤノン IT ソリューションズ株式会社
松本 悦宜	Capy 株式会社
宿谷 昌弘	サイバートラスト株式会社
田上 利博	サイバートラスト株式会社
稲葉 厚志	GMO グローバルサイン株式会社
吉岡 道明	JPCERT コーディネーションセンター
園田 哲也	株式会社セブン・カードサービス
向井 克彦	株式会社セブン・カードサービス
井上 大輔	株式会社セブン・カードサービス
加藤 孝浩	トッパン・フォームズ株式会社
木埜 由紀子	日本ユニシス株式会社
黛 慎一	パスロジ株式会社

【事務局】

一般社団法人 JPCERT コーディネーションセンター

以上