別紙１

ウェブサービスに関するID・パスワードの管理・運用実態調査結果のポイント

平成27年7月30日
総務省　情報セキュリティ対策室

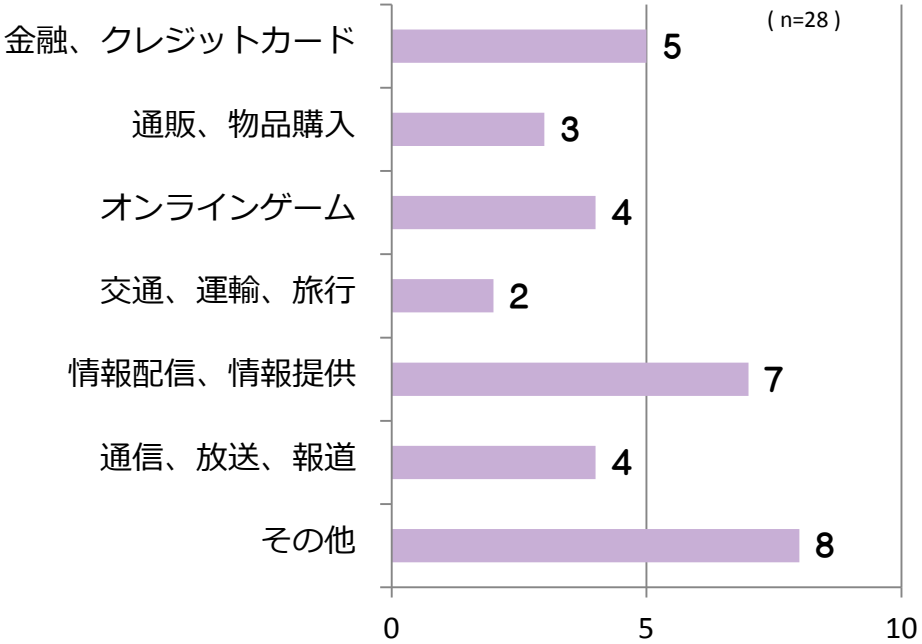
調査の概要

項目	概要
調査背景	インターネットショッピングやインターネットバンキング、ソーシャルネットワーキングサービス等、インターネットを通じて様々な社会経済活動が営まれており、ネットワークを通じた社会経済活動の安全は、利用者が本人であることの真正性の証明に立脚している。現在ウェブサービスにおいて利用者の真正性を確認する主な手段としてID・パスワードが利用されていることを踏まえ、企業におけるウェブサービスに関するID・パスワードの運用管理実態について調査を実施した。
調査方法	ウェブアンケート
調査期間	平成27年2月～3月
調査対象	下記業種に該当する企業200弱に調査への協力を依頼。 最終的に協力を得られた28社からの回答を集計。 [対象業種] 〇金融・クレジットカード　〇通販、物品購入　〇オンラインゲーム 〇交通、運輸、旅行　　〇情報配信、提供　〇通信、放送、報道 〇その他
備考	各個社に対し、本調査は匿名で集計・公表する旨告知した上で調査を依頼したが、不正アクセスの被害有無やパスワードの内部管理方法といった機微な情報に関する調査であることから、回答を控える企業が多かった。 次ページ以降に記載する調査結果において、 パーセントで示したグラフ中の括弧で記載した数字は回答社数を示している。また、丸め誤差により合計が100%にならない場合がある。

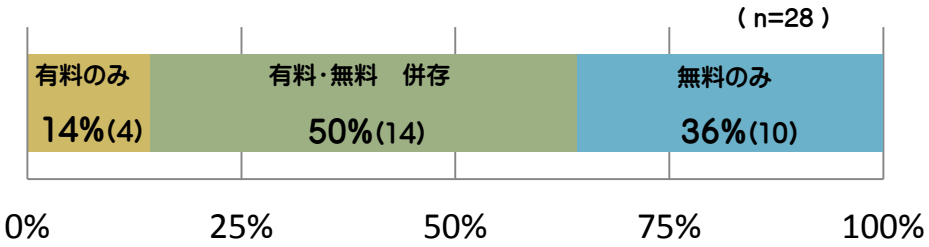
調査対象企業概略

- 想定したすべての業種から回答を得ることができた。
- 回答を得られた企業の6割強が有料を含むサービスモデルであり、有料のサービスが一般的になっていることがわかる。
- 回答を得られた企業のうち、3割が不正ログイン被害の経験があると回答している。発見できていない場合も考慮すると、より高い割合で被害にあっていることが推測される。

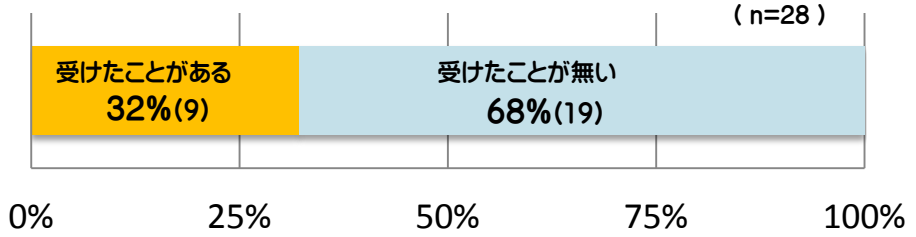
■アンケートの回答があった業種（複数選択可）



■提供するサービスの料金モデル



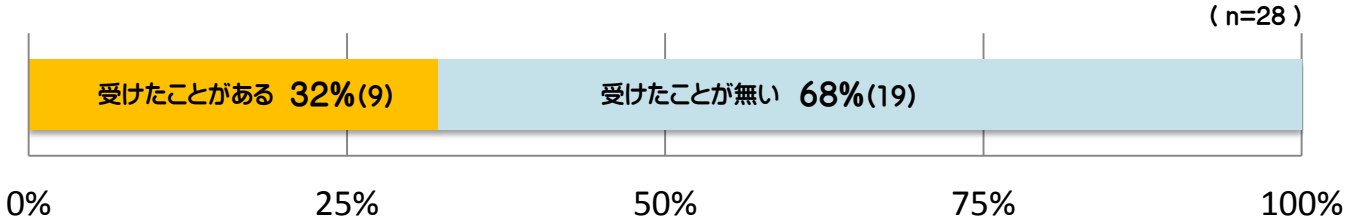
■不正ログイン被害 経験有無



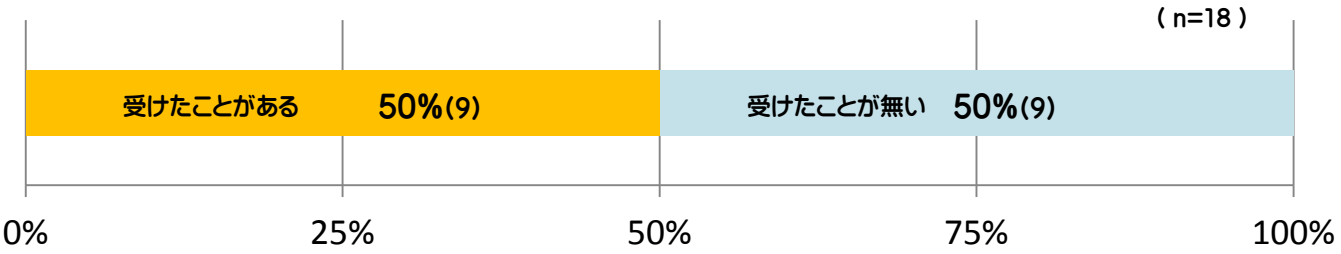
不正アクセスの被害有無と料金モデル

- 回答を得られた企業の約3割が不正アクセスの被害を受けていた。
- 有料を含むサービスを提供している企業のみに限定すると、被害率が上がり、5割の企業が不正アクセス被害を受けている。
- 攻撃者がより重要な情報があると思われる企業を狙って攻撃している可能性が考えられる。

■不正ログイン被害 経験有無（全回答者）（再掲）



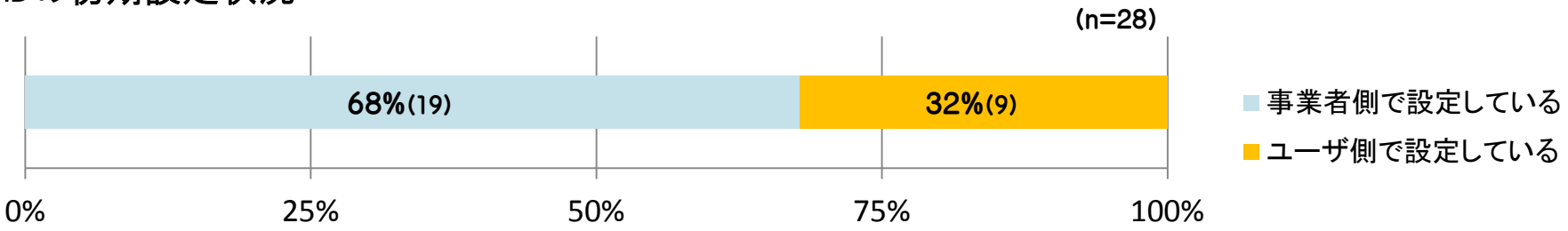
■不正ログイン被害 経験有無（内有料を含むサービス提供者）



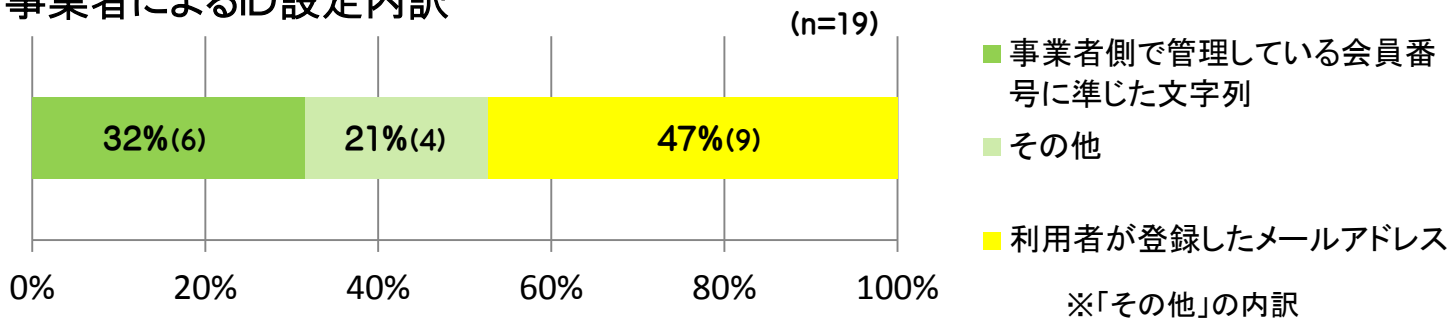
IDの初期設定値

- Webサービスを利用する際のIDについて初期値を誰が決定しているのか調査を行った。
- 約7割が事業者側で設定していると回答している。
- 事業者が設定しているIDが何に基づいて設定されているのかを見ると、半数近くがユーザが登録したメールアドレスを利用していた。

■IDの初期設定状況



■事業者によるID設定内訳



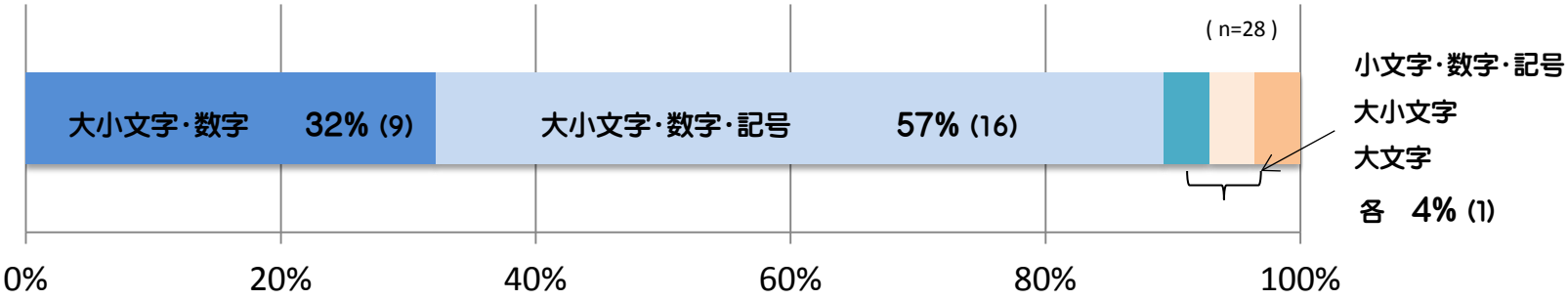
※「その他」の内訳

- ランダムな文字列
- 氏名と数字を組み合わせた文字列
- メールアドレスのエイリアス
- メールアドレスと会員番号に準じた文字列の併用

ユーザが設定可能なパスワード

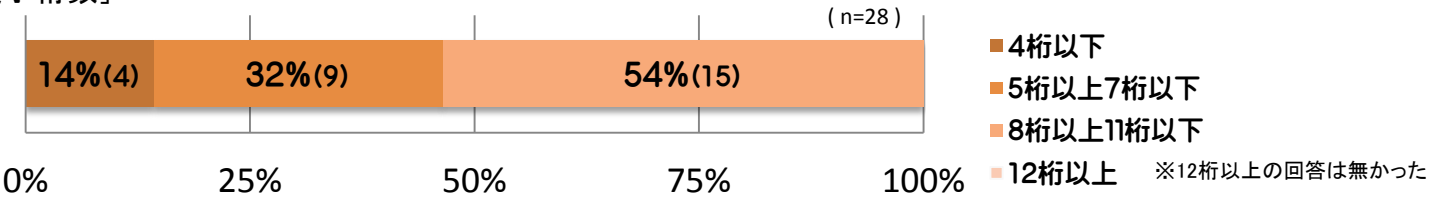
- ユーザがパスワードを設定する際に利用可能な文字種や文字列長について調査を行った。
- ユーザが設定可能なパスワード文字種については大文字・小文字・数字の3種は約9割で利用可能であり、多くの企業で複数文字種への対応がなされていることが確認できた。
- 設定可能な最小文字列長は5割以上が8桁以上の設定を必要としているが、1割強の企業では未だ4桁以下であった。また、最大文字列長については、未だ4分の1の企業において12桁に満たず、利用者が強いパスワードを設定したくとも設定できない状況になっている。

■利用可能な文字種

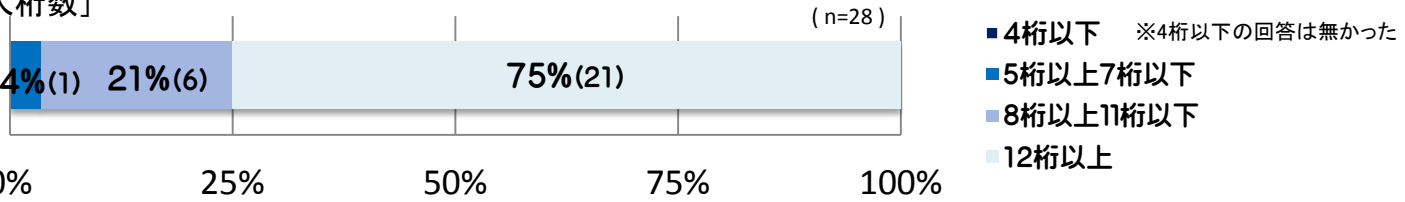


■設定可能な文字列長

［最小桁数］



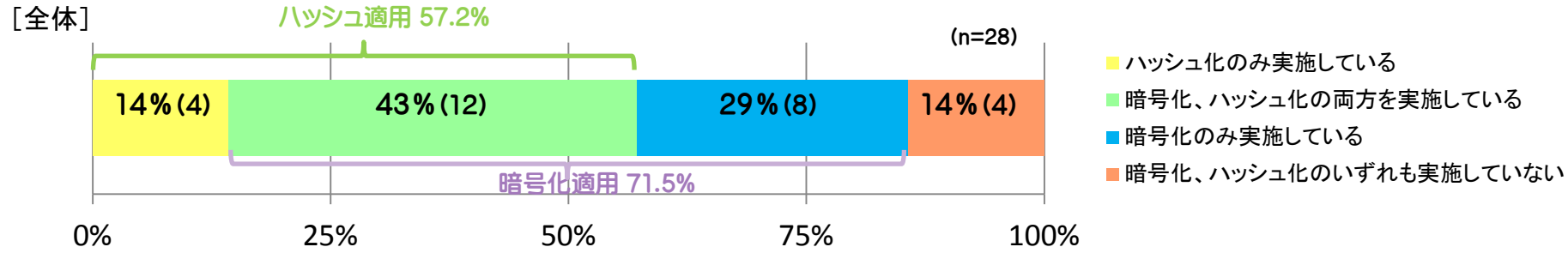
［最大桁数］



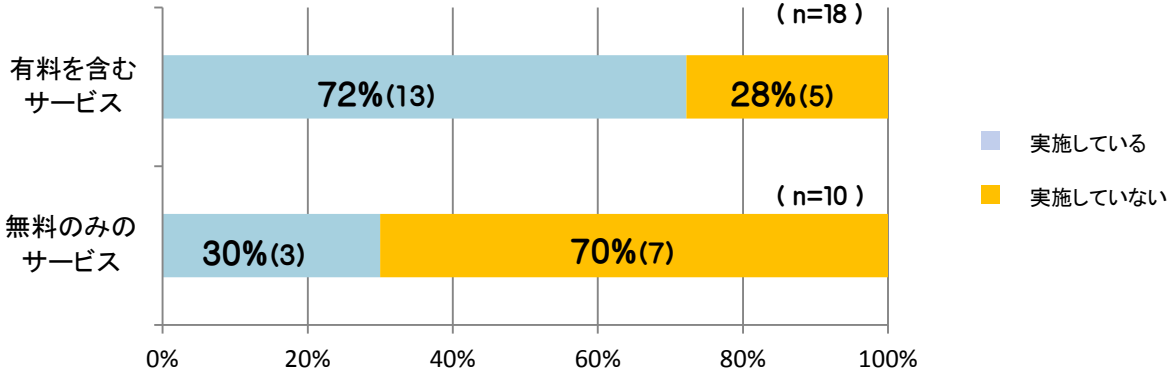
企業のパスワード管理状況　1

- パスワードの管理においては不正なログインへの対策だけでなく、管理サーバが不正アクセスを受け、パスワードが格納されたデータを奪われる等の被害も想定した対策が望まれる。代表的な対策であるパスワードの暗号化及びハッシュ化について企業における実施状況を調査した。
- パスワード保管時の対策については、暗号化の適用が約7割、ハッシュ化の適用については6割弱の企業が実施していた。
- ハッシュ化の対策は有料を含むサービスでは約7割実施しているのに対し、無料のみのサービスでは3割の実施に留まり、無料のみのサービスを提供する企業ではハッシュ化が普及していないことが分かった。

■パスワード保管時の暗号化・ハッシュ化の実施状況



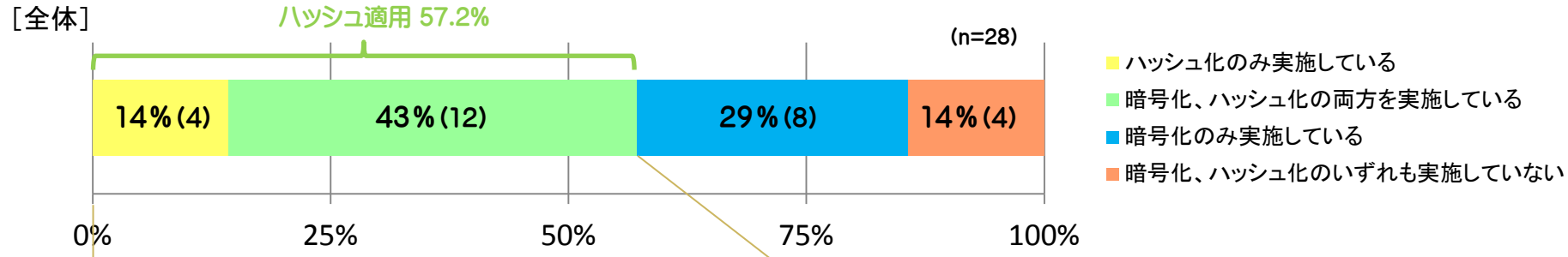
■ハッシュ化の実施率 （有料無料の別）



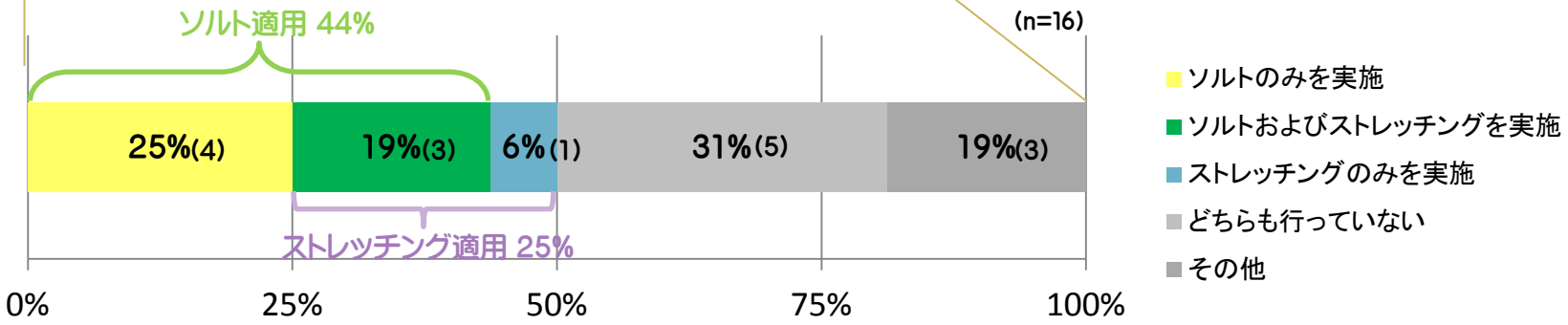
企業のパスワード管理状況　2

- パスワードのハッシュ化を行っている企業において、ハッシュ化時の保護強化の取組であるハッシュ化前のパスワードに文字列を追加するソルト及びハッシュ化を繰り返すストレッチングを行っているか調査を行った。
- パスワードのハッシュ化を行っている企業の内、5割の企業がソルト、ストレッチングいずれかの保護強化の取組を実施しており、ソルトの実施は約4割、ストレッチングの実施は2割強であった。

■パスワード保管時の暗号化・ハッシュ化（再掲）



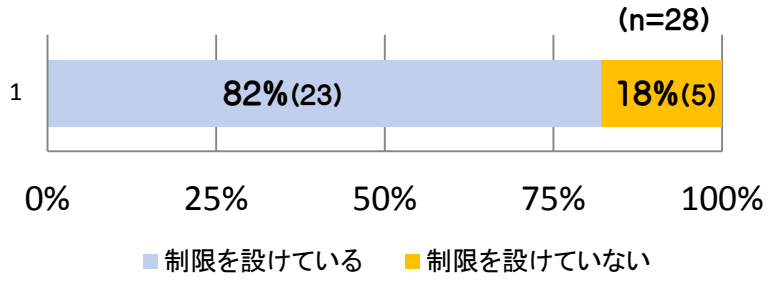
■ハッシュ化時の保護強化の取組



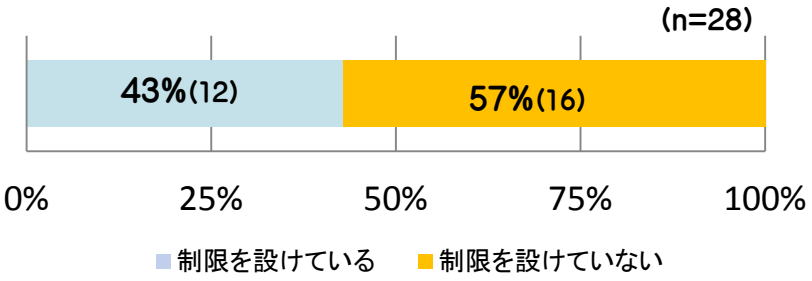
同一ID・IPに対する不正ログイン対策状況

- 同一IDに対してパスワードを変更しながらログインを試行するブルートフォース攻撃への対策の1つとして考えられる同一IDに対するログイン試行回数の制限は約8割の企業が行っており、積極的な対策が行われていることが明らかとなった。
- 一方、リバースブルートフォース等のIDを変えながらログインを行う攻撃への対策の1つとして考えられる同一IPからのログイン試行回数の制限について調査したところ、実施しているのは約4割に留まり、同一IDに対するログイン試行制限に比べ、導入が進んでいない。

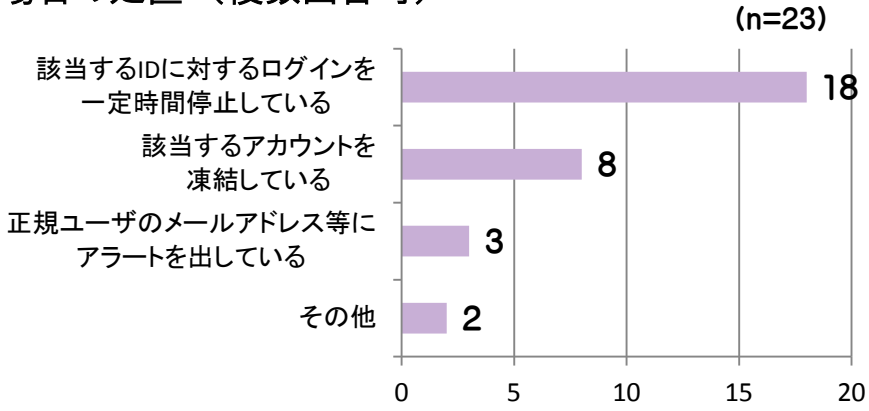
■ 同一IDに対するログイン失敗回数制限を設けているか



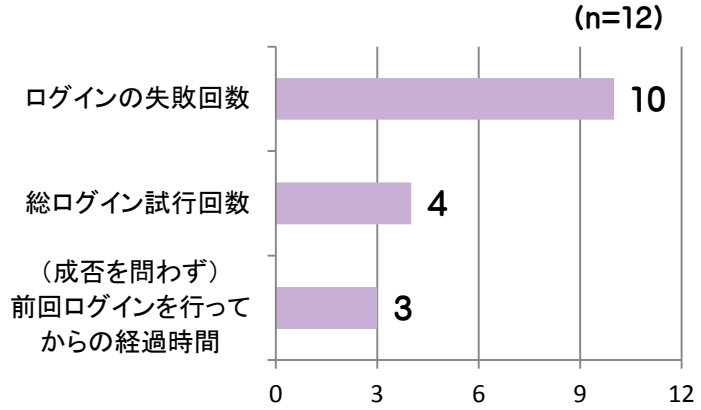
■ 同一IPアドレスからのログイン試行回数制限を設けているか



■ 同一IDに対するログイン失敗回数が制限に達した場合の処置（複数回答可）



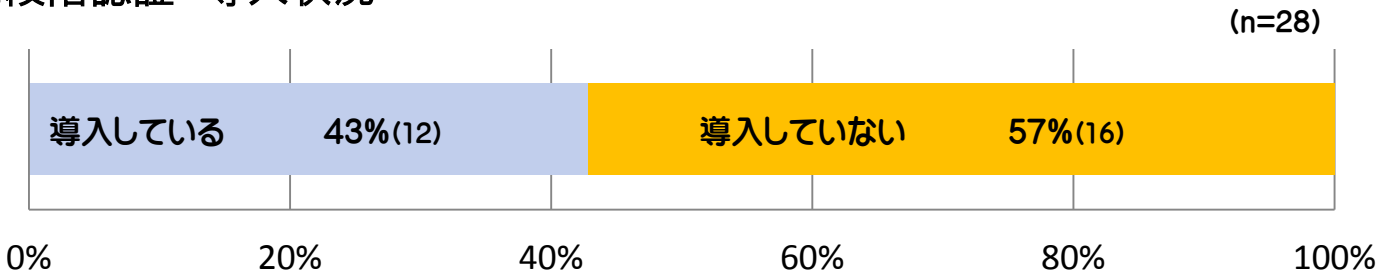
■ 同一IPアドレスからのログイン制限について何を基準に行っているか（複数回答可）



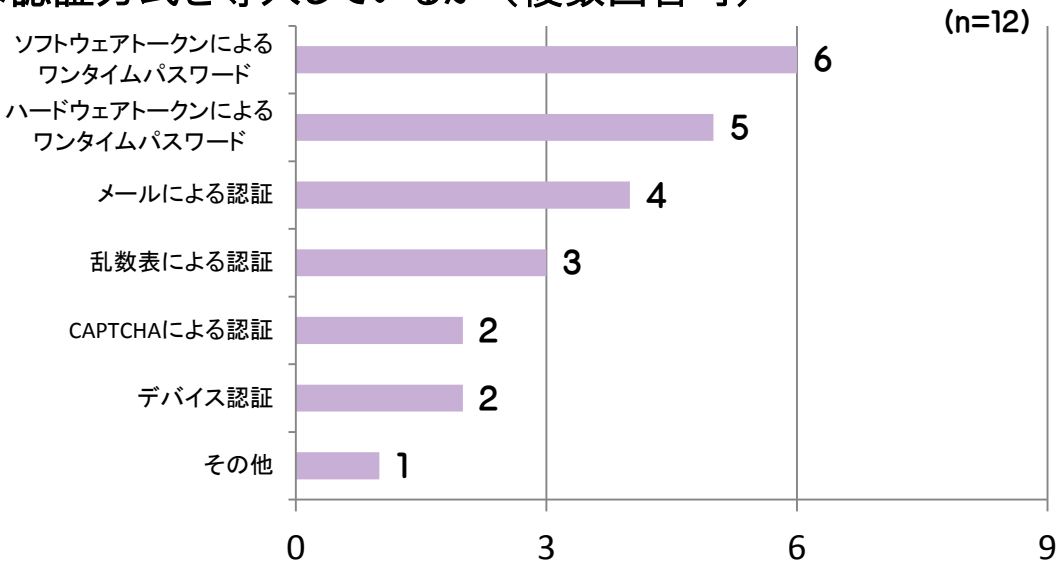
高度な不正ログイン対策導入状況～2段階認証～

- リスト型攻撃等への対策に有効と思われる2段階認証について調査を行った。
- 2段階認証については約4割の導入となっている。ID・パスワード以外の何らかの手段を用意する必要があるため、同一IDからのログイン試行対策に比べ導入が進んでいないと思われる。

■2段階認証　導入状況



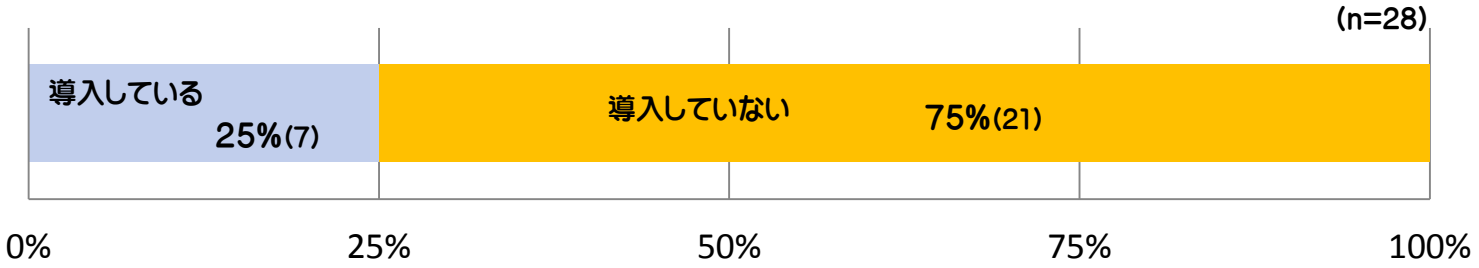
■どのような認証方式を導入しているか（複数回答可）



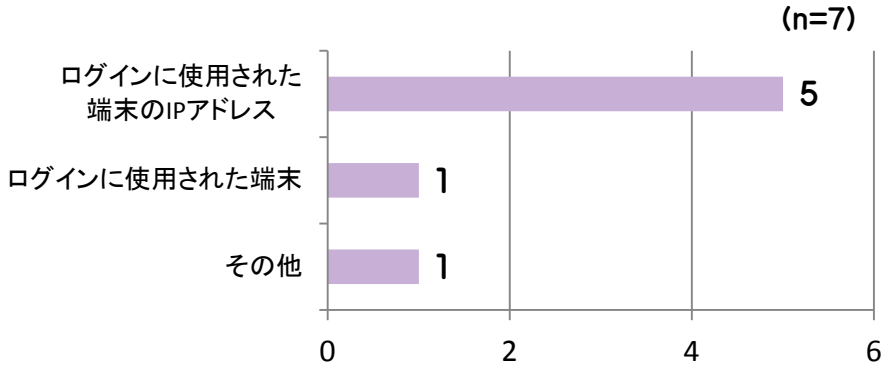
高度な不正ログイン対策導入状況～リスクベース認証～

- 通常と異なるIPアドレスやタイムゾーンからのログインといった通常の状況との差を検知するリスクベース認証はユーザのなりすましといった攻撃への対策として考えられ、導入状況を調査したところ、リスクベース認証は3割以下の導入となっている。
- リスクベース認証を導入している企業7社の内、5社が2段階認証も導入しており、リスクベース認証で疑わしいと思われるログインに対して、2段階認証を求めるといった利用方法で導入されている。

■リスクベース認証を導入しているか



■何に基づいて行っているか（複数回答可）



リスクベース認証と2段階認証の利用事例

- 本調査において確認されたリスクベース認証と2段階認証を組み合わせた利用事例を以下に示す。