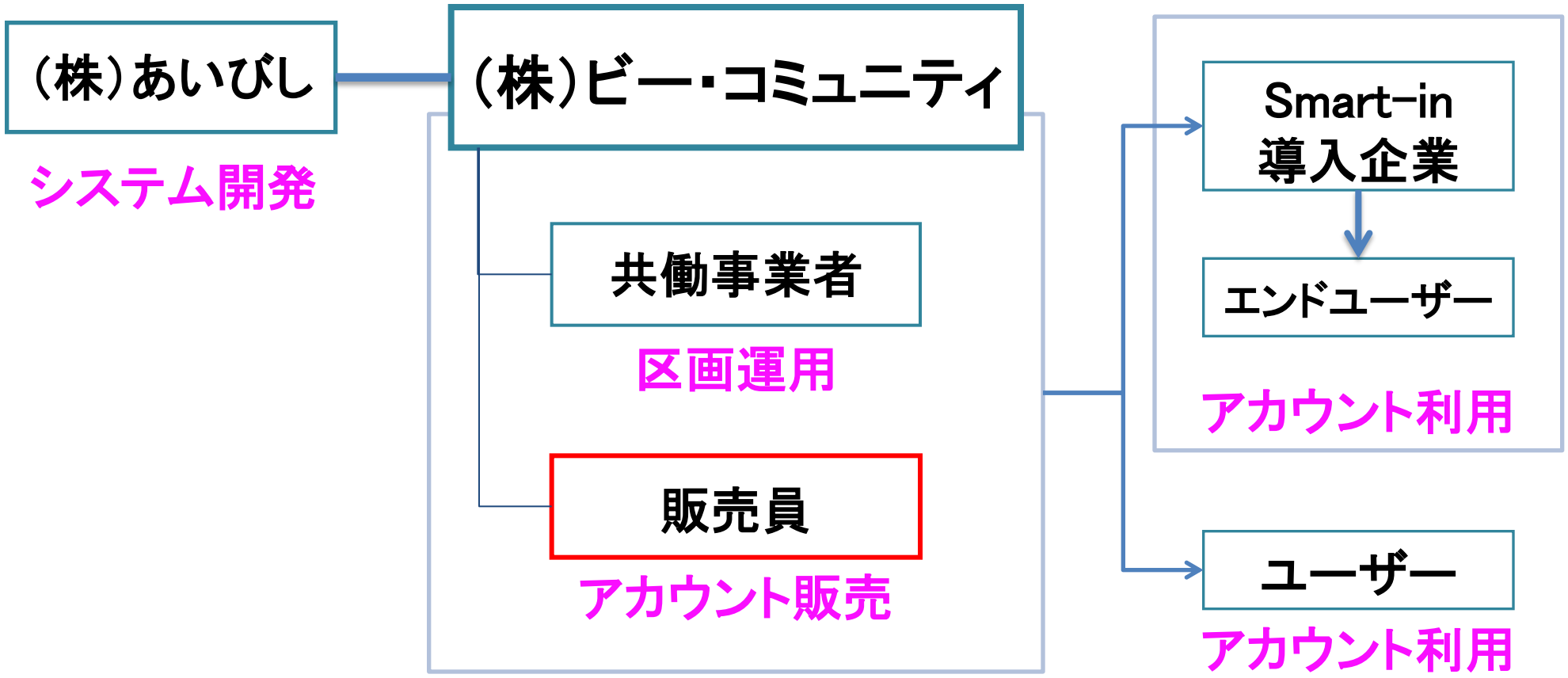
Smart-in拡販プロジェクト 事業説明（販売員募集）

201503181706NH

株式会社ビー・コミュニティ

目次

相関図



会社紹介

社名	株式会社ビー・コミュニティ （Bee-Community Co.,Ltd.）
本社所在地	〒105-0004 東京都港区新橋5-20-3 新橋STビル 7F
設立	2014年2月
事業内容	情報セキュリティ商品等の販売及び仲介 セキュリティ情報及び各種データの収集・処理・提供等のサービス 出版物の企画、製作、発行及び販売 広告代理業 損害保険代理業及び生命保険の募集に関する業務 不動産の売買・交換・貸借及びその仲介並びに所有・管理及び利用 コンサルタント業務

会社紹介

私達を取り巻く環境は、人類の発展と叡智により目まぐるしく変化し、日々これらの新しい技術に触れ、その恩恵に預かっています。

そして、たった今も地球のどこかで、革新的な技術や仕組みが開発され、進歩を遂げています。私たちは、これら多くの技術のうち、社会性の高いソリューションを探求し、その前進と定着に貢献する事を目指しています。

そのため、情報化社会によって複雑化してしまった様々なサービス・技術の中において、サービスの提供者と受益者の間に立ち、受益者又は社会ニーズの本質を見極め、共働して新たなスタンダードを生み出すこと。それが、私たち株式会社ビー・コミュニティの目的と考えております。

それは社名の由来にもなっています。花には雌しべと雄しべがありますが、ほとんどの場合、それぞれ単体では受粉せず、実を結びません。

受粉には様々な媒介がありますが、、私たちは、提供者と受益者を結びつけ、蜜をもらいながら飛び回る「蜂」の様に、また古来より存在する共同生産方式、言い換えますとコミュニティーを活用し、自然の形に乗っ取った存在又は会社でありたいと思い、社名を株式会社ビー・コミュニティ（Bee-Community、略称「ビーコミ」または「ビー社」）と命名し活動を開始致しました。

株式会社ビー・コミュニティ　商品選択基準

1. 商品自体に公益性があり、社会的需要がそこに存在し得ているか？

公益性、つまり「不特定かつ多数の者の利益の増進に寄与するものとなっているか」という点と「社会性があり、広く必要とされている商品であるか」ということです。

2. 自らの評価だけではなく、第3者の正しい評価を受けているか？

一般的に、その商品、サービスの開発者は時間と労力、資金を費やしており、自身が作った商品を自身の子供のように「これが世界一だ」と自負しています。しかし、それが本当に世間に必要とされる商品なのかは周囲の意見がなくては判断することができません。その為、自身の評価だけではなく公正で専門的かつ客観的な評価、すなわち第三者の評価を受けている必要があります。

3. サービスを提供する側、サービスを利用する側、事業者等が、
その事業に参画するにあたり公正な事業活動を行えるか？

ここで大切なことは、参画する者が持つ資金・能力を問わず、大切なものを互いに認め、互いの信頼をもとに助け合うことができること、また、そこにある商品を活用・提供しあい、相互の利益の向上を目標として安心・安全に共栄できる事業活動を行えるかということです。

私たちは、『売れそうなものだから売る』『儲かりそうだから売る』わけではなく、これら3つの選定基準により、皆が共栄できる新たなスタンダードとなる商品を選定します。

ビー・コミュニティ　第一弾サービス

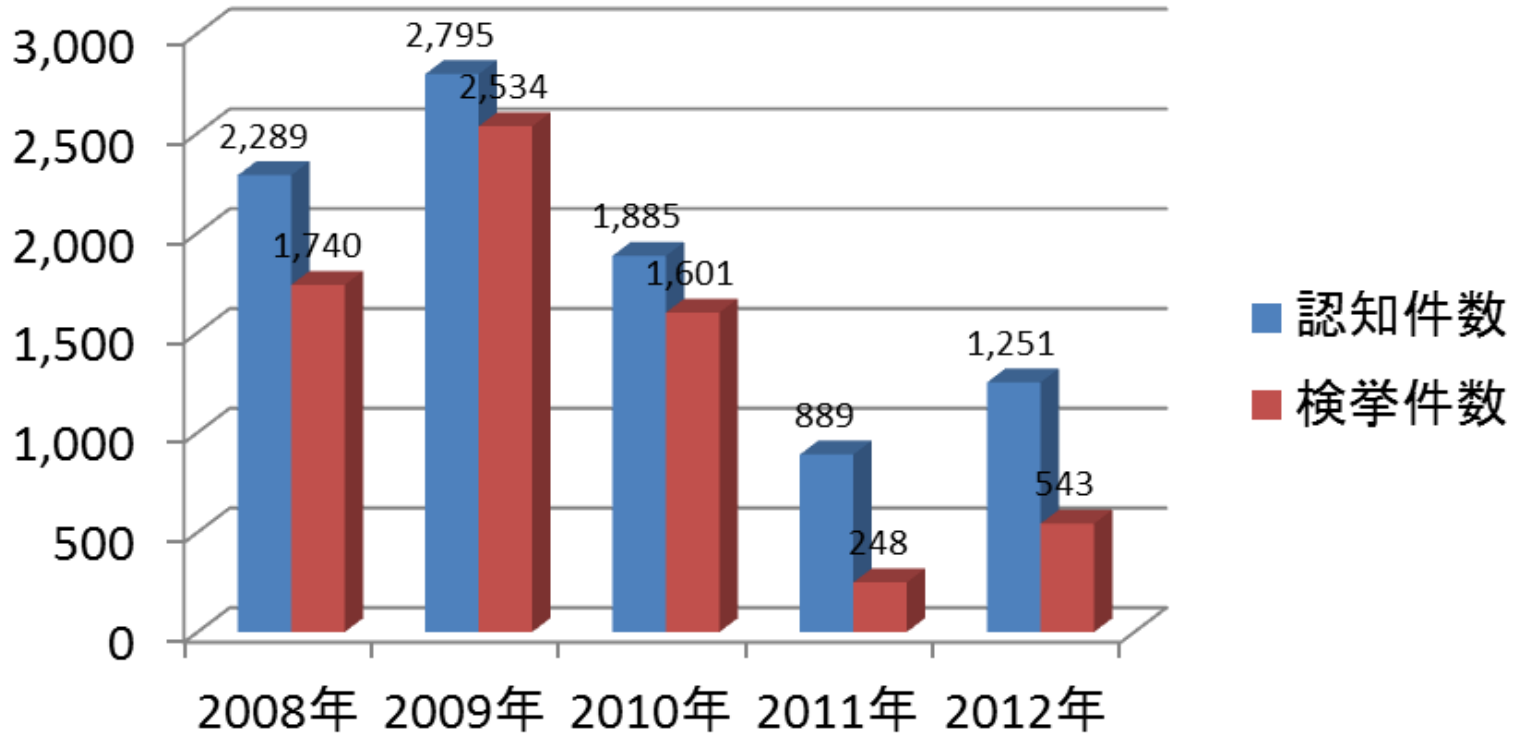
ID・パスワードが漏洩しても安全なシステム

Smart-inは、フィッシング詐欺・ハッキング・なりすまし等の情報を盗む行為に対し、
シンプルなアプローチで問題を解決する新セキュリティーシステムです。

情報セキュリティ対策の必要性

現代は、インターネットの普及に伴いネットショッピングやインターネットバンキングの利用者が増加しておりますが、コンピューターやスマートフォン等に対する不正侵入、つまり**不正アクセスによる個人情報の盗み出し、なりすまし、**などが多く見受けられ、ホームセキュリティと同じように、情報を守る事、つまり**情報セキュリティ**の問題は社会問題といえる状況になっています。

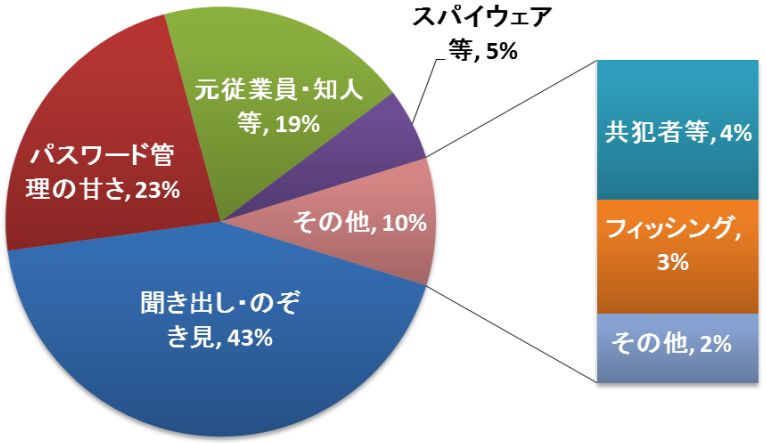
警察庁 不正アクセス 認知件数・検挙件数



『平成25年3月28日　国家公安委員会・総務大臣・経済産業大臣
不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 P2およびP4』より作成

実際はより多くの不正アクセスが発生していると想定されます。

ID・パスワードの使いまわし



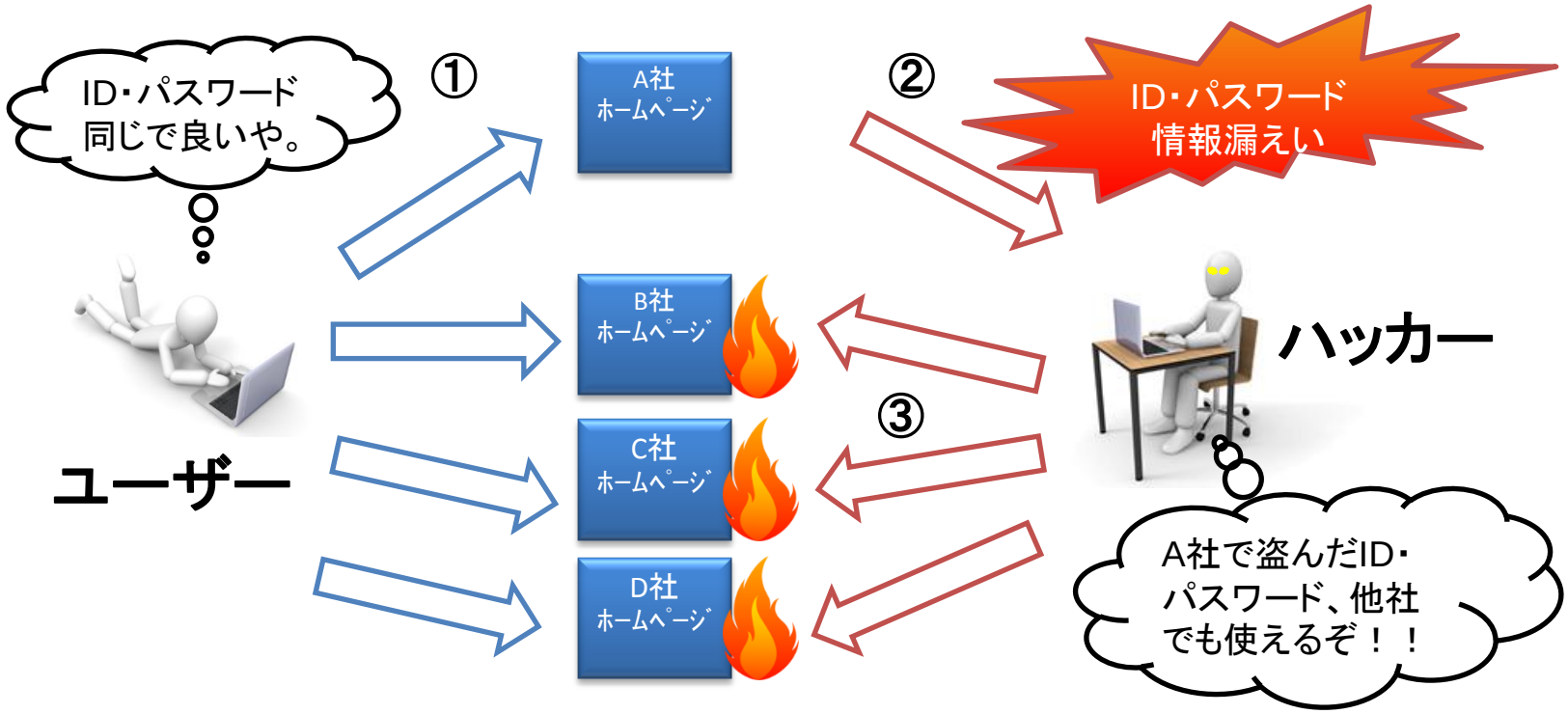
『平成25年3月28日　国家公安委員会・総務大臣・経済産業大臣
不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 P6』より作成

インターネットでの本人確認の基本的な方法として個人を識別する「ID」と本人しか知らない合言葉である「パスワード」を使う方法がありあます。

検挙された不正アクセス行為の手口の件数割合は、**「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」**が23%と多くなっています。

これは、インターネット上のサービスごとにID・パスワードを管理するのは手間が掛かる為、ID・パスワードを簡単で類推しやすいものにしていたり、**複数のサービスで同じID・パスワードを使いまわしているケース**が多くなっているためと考えられます。

不正アクセス①　パスワードリスト攻撃の脅威



そのパスワードの設定・管理の甘さを狙っているのが、「パスワードリスト攻撃」と言う不正アクセスの手口です。

事前に入手したIDとパスワードを自動的に連続入力するプログラムなどを用いて、ログインを試みる手口であり、ここでログインが成立したIDとパスワードは、その後、他のサイトへの不正アクセスに利用され、**最終的には直接的・金銭的被害に結びつく**ものと考えられます。

2012年2月　パスワードリスト攻撃状況

協力企業数	のべログイン試行回数(*2)	のべ不正アクセス回数(*2)	侵入率
13社	260,896回	17,514回	6.7%

『平成24年3月15日 警察庁広報資料
平成23年中の不正アクセス行為の発生状況等の公表について 別紙』より引用

　警察庁がインターネットで各種サービスを提供する企業13社の協力を得て、2012年2月を対象に不正ログインの状況について調査した結果では、平均侵入率が6.7%と、とても高確率でした。高い侵入率の原因は、パスワードの使いまわしなどであるとみられています。
　また、2013年4月～8月の期間でパスワードリスト攻撃を受けたことをWEB上で公表した企業が20社前後確認でき、企業によっては不正ログイン成功件数が数万件となっています。
不正アクセスは極めて稀な事ではありません。

不正アクセスの被害例

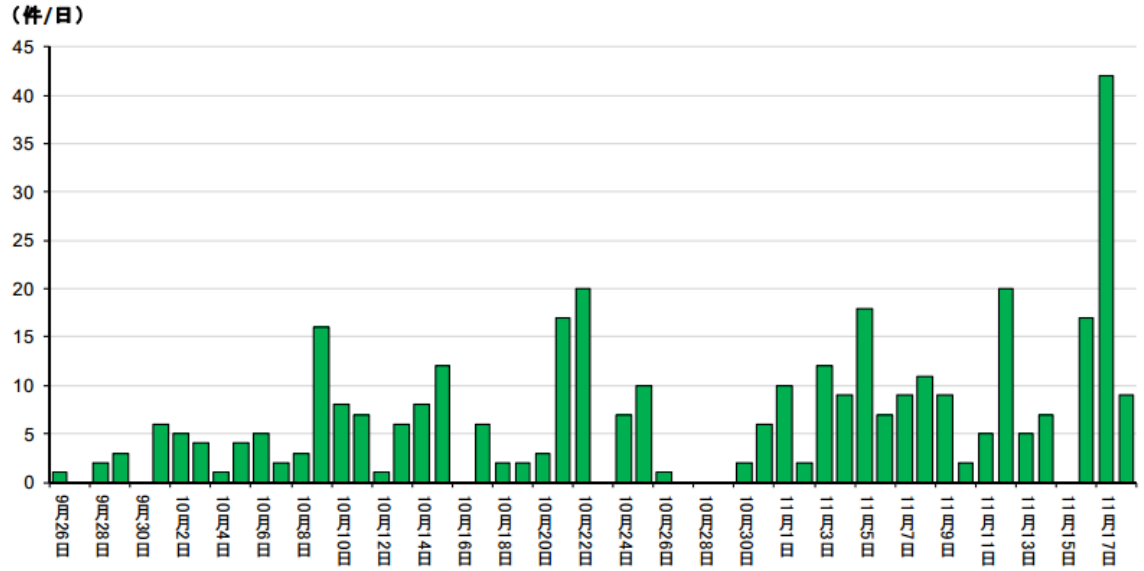
区分 ＼ 年次	平成23年	平成24年
オンラインゲーム、コミュニティサイトの不正操作	358	662
インターネットショッピングの不正購入	172	223
情報の不正入手	74	99
インターネットバンキングの不正送金	188	95
ホームページの改ざん・消去	28	42
インターネット・オークションの不正操作	22	29
不正ファイルの蔵置	4	1
その他	43	100

『平成25年3月28日　国家公安委員会・総務大臣・経済産業大臣
不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 P3』より引用

不正アクセスの被害例
- ブログやSNSにログインされ、悪意のある記事が掲載されたり、電話帳やメール、写メ像が流出してしまった。
- お金を掛けて手に入れたネットゲームの大切なアイテムを勝手に売られた、お金を不正引き出された。
- インターネットショッピングで知らないうちに商品が購入されており商品は届かず請求だけ届いた。
- 勝手にクレジットカードが使われていた。
- 頑張って貯めたマイレージポイントが景品と交換しようとしたら、盗み出されていた。

フィッシングサイトの急増と警察庁による注意喚起

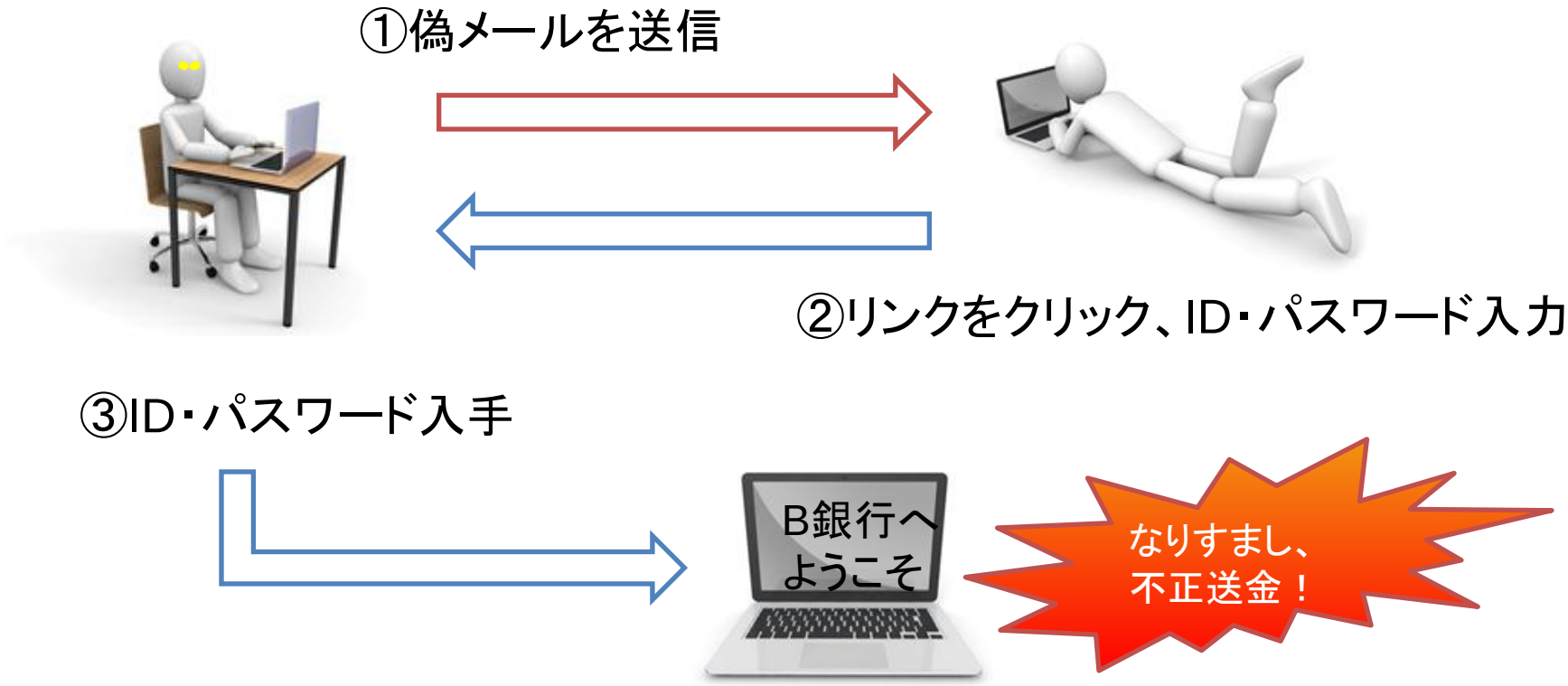
「.cn.com」ドメインのフィッシングサイトの警察庁認知状況（H25. 9.26～H25.11.18）



『平成25年11月21日 警察庁 「.cn.com」ドメインを利用したフィッシングサイトの増加について』より引用

フィッシング（金融機関などからの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などを詐取する詐欺）を行うサイトが、2013年夏ごろから増加し、2013年11月に急増したことを受け、
警察庁は2013年11月21日にフィッシングサイトの増加について、注意喚起を行っています。
なお、上記グラフは2日おきの数値をまとめたものです。ほぼ毎日フィッシングサイトが発見されている事がわかります。

不正アクセス②　フィッシング



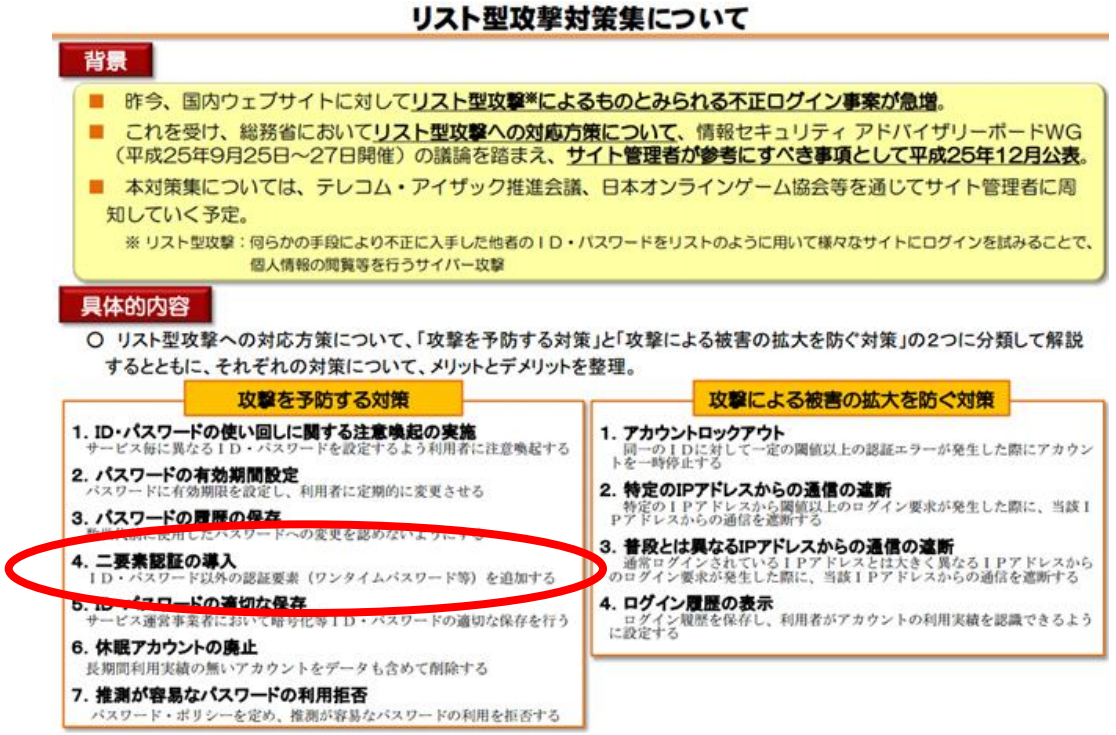
情報を盗む手口として、ID、パスワードを偽の画面に入力させる「フィッシング」と言う手口が横行しています。
銀行等の企業を装ってメールを送り、メールの受信者に、実在する企業の偽ホームページにアクセスさせて、そのページでクレジットカード番号やID・パスワード等を入力させるなどして不正に個人情報等を入手する行為です。**手口はどんどん巧妙になっており、被害は増え続けています。**

インターネットバンキング　不正送金

平成26年1月30日 警察庁 広報資料 『平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について』より引用

インターネットバンキングでは大きな被害が出ており、警察庁発表によると、
2013年の不正送金被害額は14億円と過去最悪となっています。
さらに2014年1月～2月のわずか2カ月間で不正送金被害額は6億円となっており、
被害はますます拡大すると推測されています。

総務省からの注意喚起　2013年12月18日



リスト型攻撃対策集について

背景

- 昨今、国内ウェブサイトに対して**リスト型攻撃※によるものとみられる不正ログイン事案が急増**。
- これを受け、総務省において**リスト型攻撃への対応方策について**、情報セキュリティ アドバイザリーボードWG（平成25年9月25日～27日開催）の議論を踏まえ、**サイト管理者が参考にすべき事項として平成25年12月公表**。
- 本対策集については、テレコム・アイザック推進会議、日本オンラインゲーム協会等を通じてサイト管理者に周知していく予定。

※ リスト型攻撃：何らかの手段により不正に入手した他者のＩＤ・パスワードをリストのように用いて様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃

具体的内容

○ リスト型攻撃への対応方策について、「攻撃を予防する対策」と「攻撃による被害の拡大を防ぐ対策」の2つに分類して解説するとともに、それぞれの対策について、メリットとデメリットを整理。

攻撃を予防する対策

1. **ID・パスワードの使い回しに関する注意喚起の実施**
   サービス毎に異なるＩＤ・パスワードを設定するよう利用者に注意喚起する
2. **パスワードの有効期間設定**
   パスワードに有効期限を設定し、利用者に定期的に変更させる
3. **パスワードの履歴の保存**
   [illegible]に使用したパスワードへの変更を認めないようにする
4. **二要素認証の導入**
   ＩＤ・パスワード以外の認証要素（ワンタイムパスワード等）を追加する
5. **ID・パスワードの適切な保存**
   サービス運営事業者において暗号化等ＩＤ・パスワードの適切な保存を行う
6. **休眠アカウントの廃止**
   長期間利用実績の無いアカウントをデータも含めて削除する
7. **推測が容易なパスワードの利用拒否**
   パスワード・ポリシーを定め、推測が容易なパスワードの利用を拒否する

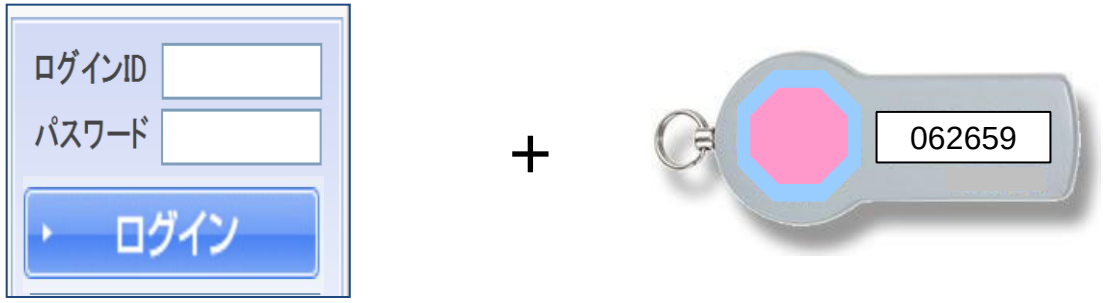
攻撃による被害の拡大を防ぐ対策

1. **アカウントロックアウト**
   同一のＩＤに対して一定の閾値以上の認証エラーが発生した際にアカウントを一時停止する
2. **特定のIPアドレスからの通信の遮断**
   特定のＩＰアドレスから閾値以上のログイン要求が発生した際に、当該ＩＰアドレスからの通信を遮断する
3. **普段とは異なるIPアドレスからの通信の遮断**
   通常ログインされているＩＰアドレスとは大きく異なるＩＰアドレスからのログイン要求が発生した際に、当該ＩＰアドレスからの通信を遮断する
4. **ログイン履歴の表示**
   ログイン履歴を保存し、利用者がアカウントの利用実績を認識できるように設定する

平成25年12月18日 総務省「リスト型アカウントハッキングによる不正ログインへの対応方策について（サイト管理者などインターネットサービス提供事業者向け対策集）」から引用

これらの問題に対して監督省庁としても様々な対応をしておりますが、
その一つとして2013年12月18日に総務省から事業者に向けて注意喚起がなされています。
この中で、**不正ログインに対する防衛策として「二要素認証の導入」が推奨**されています。

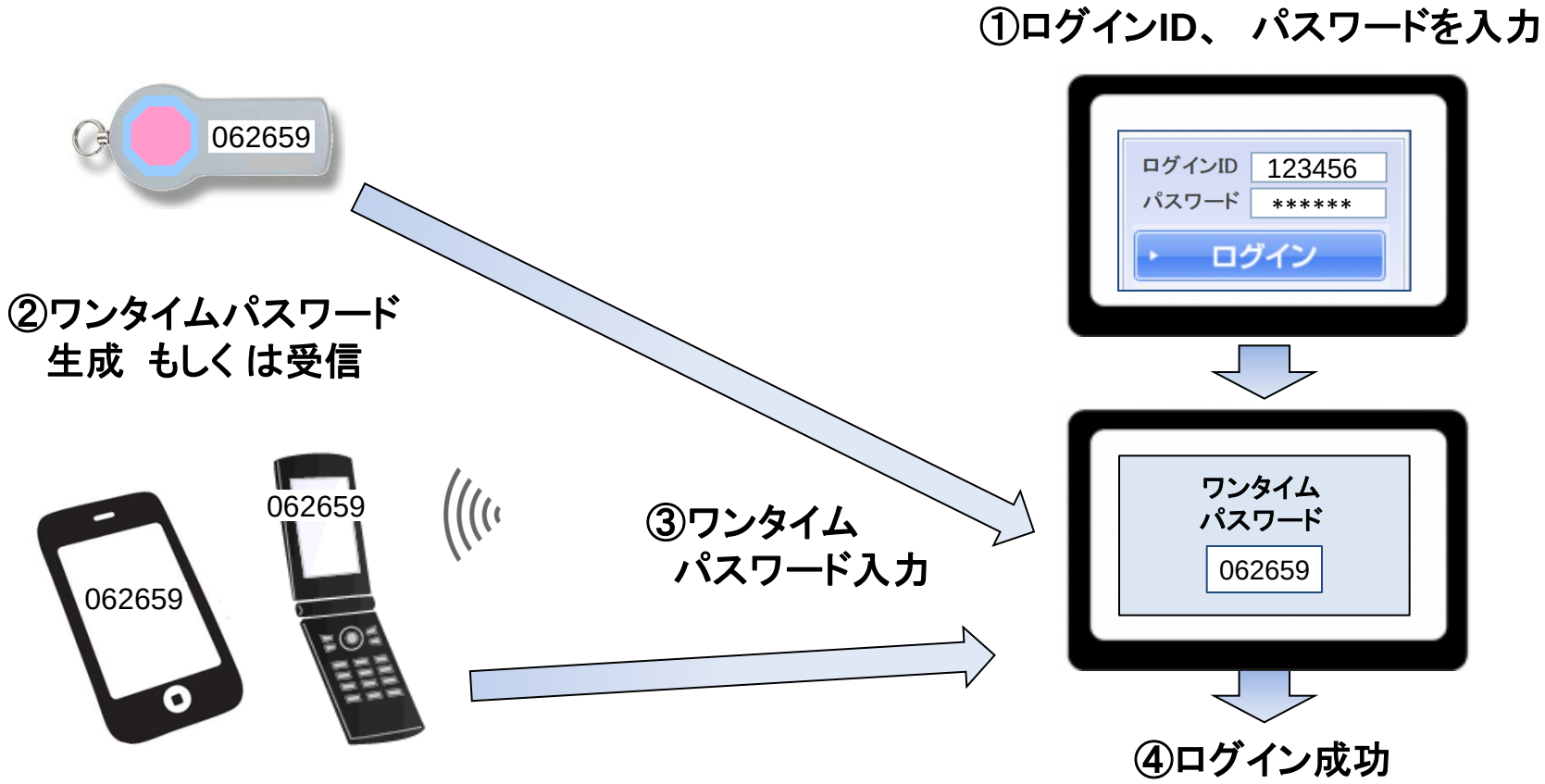
二要素認証の導入



知っているもの　　持っているもの

一般的に、二要素とはID,PASSの一要素（知っているもの）と、
ワンタイムパスワードや乱数表などの一要素（持っているもの）を合わせたものです。

ワンタイムパスワードとは



①ログインID、パスワードを入力すると、②ユーザー側に配布された機器（もしくはスマホのアプリ）で期間限定のパスワードが作成表示され※、③それを入力する事により本人確認となり、④ログインできます。パスワードの盗み見などによる不正アクセスを防ぐ方法です。 ※携帯電話のSMSにパスワードが送信される場合もあります。

現状の対策と問題点

セキュリティレベルを高くすると、利用者側では手間・面倒が増え、提供側では対策費用が増加すると言う傾向があります。

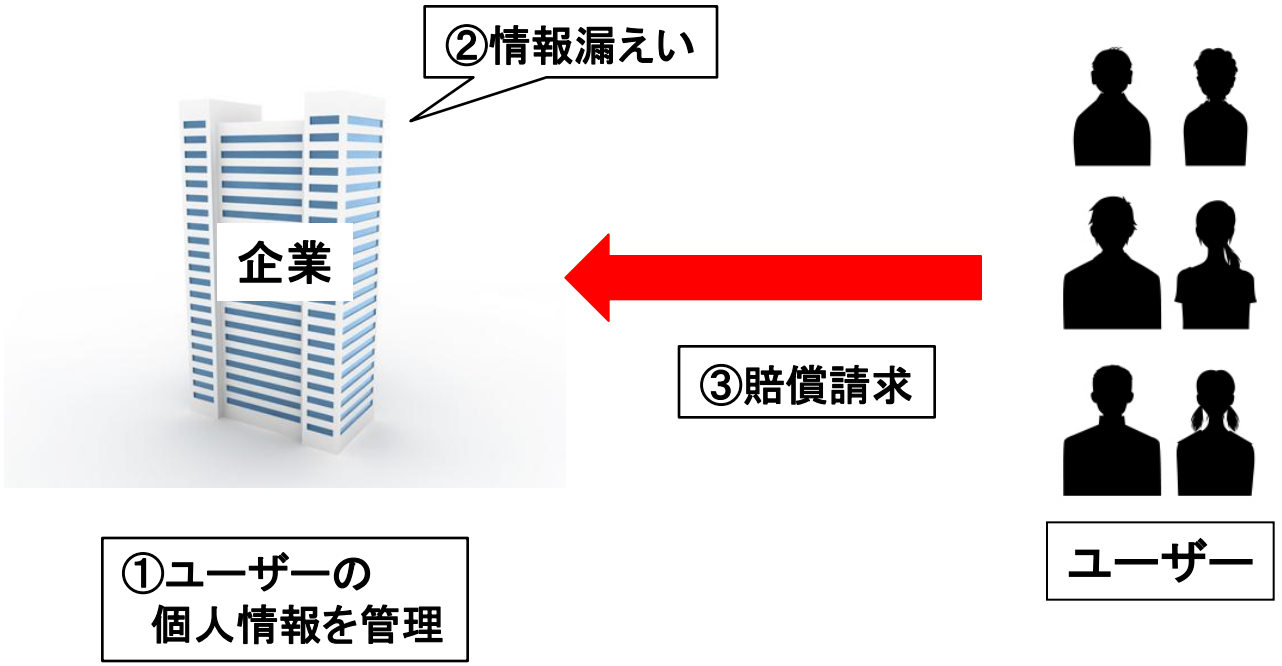
例：セキュリティレベルが高いと言われているワンタイムパスワード

■利用者側 → 手間・面倒の増加
機器複数所持、パスワード入力の手間

■企業側 → コスト増加、責任や損害賠償リスクの存在
・コスト例（金額は例）
機器タイプ：機器1個あたり 初期費用1,980円（1年間無償交換）、
ソフトウェア初期費用70万円、年間保守費用14万円（100アカウントまで）
SMSタイプ及び通話タイプ：10円前後のSMS送信費用、通話費用など
スマートフォンアプリタイプ：インターネット網利用による盗み取りのリスク

・不正ログインの原因特定困難→企業の責任や損害賠償のリスク

企業の情報漏えいリスク



訴えられた場合、情報漏えいの原因を特定し、明確な責任の所在を証明できないと、
個人情報取扱事業者として責任を負わなければなりません。
多額の損害賠償、信用失墜、資産喪失、機会損失、対策費用発生など、
大変なことになります。

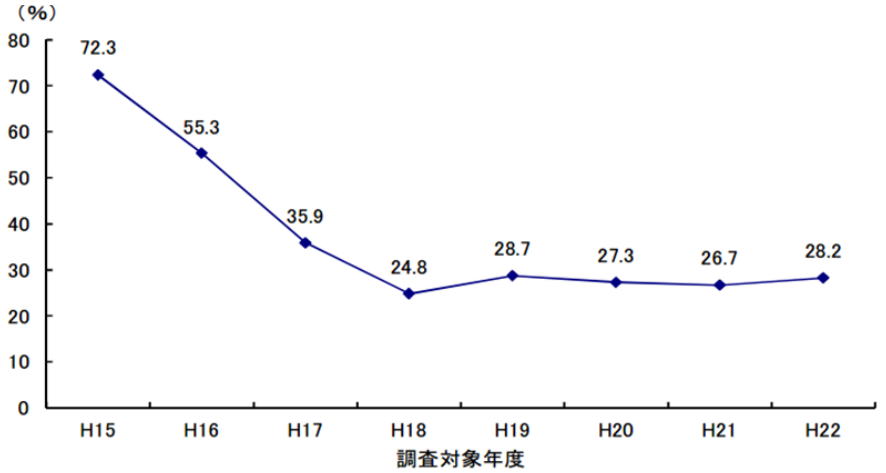
情報セキュリティ対策費用とトラブル発生率

■情報セキュリティの情報処理関係支出総額比（事業収入規模別）

年間事業収入規模	1%未満	1～3%未満	3～5%未満	5～7%未満	7～10%未満	10%以上
～1億円以下	20%	―	―	―	―	80%
1億円超～5億円以下	3%	14%	17%	7%	14%	45%
5億円超～10億円以下	4%	13%	7%	8%	16%	53%
10億円超～20億円以下	7%	15%	8%	8%	13%	49%
20億円超～100億円以下	10%	24%	12%	10%	9%	35%
100億円超～1,000億円以下	24%	32%	14%	8%	5%	17%
1,000億円超～	37%	35%	14%	6%	4%	4%
不　明	14%	22%	8%	―	11%	44%
合　計	17%	26%	12%	8%	8%	28%

参考 「経済産業省 情報処理実態調査・調査関係資料 平成24年調査関係資料(平成25年11月1日公表)
表5-2-3-2-2 情報セキュリティの対策費用の情報処理関係支出総額比（業種/年間事業収入規模別）」

■情報セキュリティトラブルの発生率



「経済産業省　平成23年情報処理実態調査結果報告書 P27」より引用

企業（サービス提供者）はセキュリティに多額の資金を掛け続けていますが、
トラブルは起こり続けています！
様々なセキュリティ対策を講じている金融機関でさえ、被害を免れていません！

情報セキュリティに関するまとめ

1. 多くの人が会員サービスを利用していますが、ほとんどの人がID・パスワードを
   使いまわしており、不正アクセスの危険にさらされています！

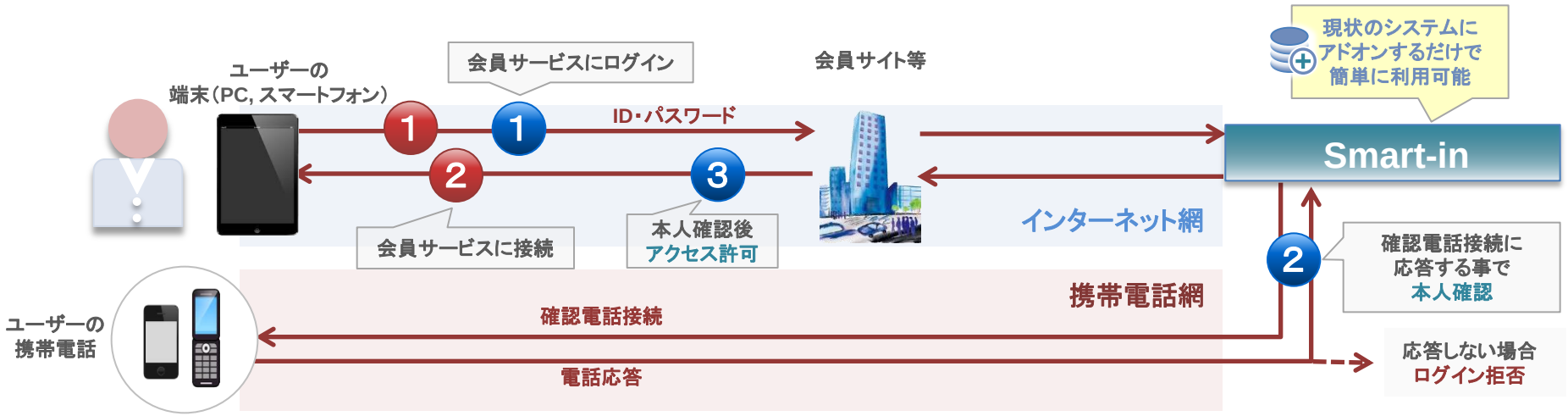
2. 個人情報が漏えいすると、多額の損害賠償、信用失墜、資産喪失、機会損失、
   対策費用発生など、大変なことになります。

3. 企業はセキュリティに相当のコストをかけ続けていますが、トラブルは起こり続けています！
   様々なセキュリティ対策を講じている金融機関でさえ、被害を免れていません！

4. セキュリティを高めようとすると、コスト増加と利便性の低下と言う問題があります。

Smart-in
サービスとは

Smart-inの仕組み



導入前

1 会員サイトにアクセス

ユーザーが端末から会員サイトにアクセス。
ID・パスワードを入力する。

2 ID・パスワードで認証して、アクセス

ID・パスワード情報が漏えいすれば、
誰でもアクセス可能

導入後

1 会員サイトにアクセス

ユーザーの端末から会員サイトにアクセス。
ID・パスワードを入力する。
Smart-inシステムがユーザー自身の携帯電話に
接続される。

2 本人が電話に応答することで本人確認

○ 接続されたユーザーが「応答」することで本人確認

× システムからの自動電話に一定時間応答がない場合は、
不正アクセスとみなしログイン拒否

3 ID・パスワード・電話で認証して、アクセス許可

本人確認が確定した場合のみ、
アクセス許可

Smart-in の特徴

1. Smart-in は、「安全性」を確保します。

一要素認証	解決	二要素認証
セキュリティ脆弱性		二経路認証

2. Smart-in は、責任の所在を明確にする「リスク回避商品」です。

情報漏えいの追跡困難	解決	認証による責任を明確化
管理担当者への責任		管理責任者の責任を回避

3. Smart-in は、パスワードを簡素化・一元化できる「利便性」があります。

記憶困難な複雑なパスワード	解決	パスワードの簡素化・一元化

Smart-in導入側とユーザーのメリット

1 既存のWEB上の会員サービスが安全に利用しやすくなります。（ユーザー）

・ID・パスワードが漏れても、電話が繋がらないとログインできないので、**簡単なID・パスワードでも大丈夫！**
・様々な会員サービスに**同じID・パスワードを使っても大丈夫！**
・自分に着信が入ることにより、**不正アクセスをリアルタイムに把握し、未然に防ぐことができます！**

2 個人情報の保護や管理にかかるコストとリスクを低減します。（導入側）

・ログインはユーザーの「電話」で行うため、**個人情報保護における責任が軽減します！**
・有料サービスにおける、**ID・パスワードの不正共用利用を防止できます！**
・複数の個人情報管理者がいる場合、複数の管理者アカウントを設定でき、操作ログが残るため、
操作責任者や操作内容を特定でき、個人情報漏えいの抑止力となります！

3 ログイン以外にも、様々な場面での「承認」に利用できます。（導入側）

・「伝えた」「聞いてない」などの**コミュニケーション上のトラブルは様々な場面で見られます！**
・Smart-inでは、**承認を得るまでのプロセスと情報管理が便利で安全です！**

携帯電話の自己管理

携帯電話不正利用防止法（2006年4月施行、2010年12月最終改正）　「総務省　携帯電話不正利用防止法　関係資料」より引用

■携帯電話事業者・レンタル業者への規則

1. 携帯電話事業者（事業者）と貸与業者（レンタル業者）は、ユーザーに携帯電話などの契約締結時および譲渡時（貸与時）に、運転免許証などで本人確認を行い、その記録を3年間保持しなければならない。
2. レンタル業者が事業者に無断で、“業として”有償で通話可能な携帯電話などを譲渡する場合、処罰の対象となる。
3. ユーザー（申込者）の氏名などを確認せずに、業として有償で携帯電話の貸し出しなどを行なうと処罰の対象となる。
4. 携帯電話が犯罪に利用された場合などは、警察署長からの求めで、事業者は契約者の本人確認することができる。
5. 事業者は、ユーザーが本人確認に応じない場合、サービス提供を拒否することができる。
6. SIMカードも携帯電話端末と同等の扱いとし、本人確認などを要するものとする。
7. 国家公安委員会は、事業者に対して情報の提供や振り込め詐欺対策に対する国民の理解を得るために、必要な措置を講ずることができる。

■契約者・利用者（ユーザー）に対する規則

1. レンタル携帯電話、携帯電話等の契約時に、虚偽の氏名、住居又は生年月日を申告すると処罰の対象となる。
2. 自己名義のSIMカード、携帯電話等を携帯電話事業者に無断で譲渡すると処罰の対象となる。
3. **他人名義のSIMカード、携帯電話等を譲渡する又は譲り受けると処罰の対象となる。**

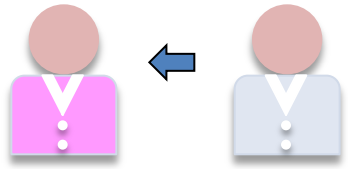
※“譲渡”ではなく無償での“貸与”のつもりでも、ユーザーは携帯電話事業者の承諾を得なければ法律違反となります。

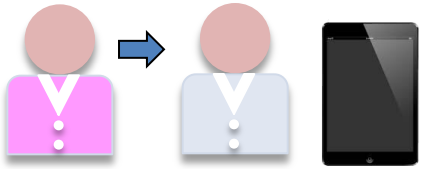
情報漏えいをした者が、「携帯電話を貸していた相手に勝手にSmart-inの操作をされた」と言う言い逃れができないように、契約者（または使用者）による携帯電話・スマートフォンの管理義務が法律で定められています。

Smart-inを電子承認として活用

サービス側
（A社）

ユーザー（B）





1 口頭「承認」

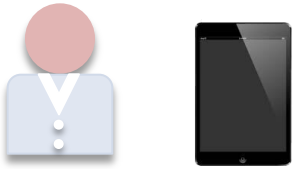
2 「承認依頼メール」送付

B様

この度はありがとうございます。
「説明内容」
この内容に同意いただけますなら、下記URLよりログインをお願いします。
ID・パスワードは下記のものを記載してください。
ログイン後、B様に着信がございます。
折返していただけることで、「同意」されたものとみなします。

ID　〇〇〇〇
PW　△△△△
URL：https://www.a-corporation.com/login

A社担当者



3 メールURLログイン

4 着信応答＝「承認」

5 担当者確認、A社全体共有

開発　㈱あいびし

主要取引先	・株式会社野村総合研究所 ・システムセンス株式会社 ・ケイティーシステム株式会社 ・株式会社ビー・コミュニティ ・合同会社PAYCREW

代表者プロフィール	
略歴	昭和41年4月　日本電信電話公社（現NTT）　入社 平成元年5月　NTTデータ社設立に伴いNTTから転籍 平成23年4月　株式会社あいびし設立、取締役会長就任 平成25年8月　株式会社あいびし　代表取締役就任
実績	○銀行業界初のFAX利用による振込みシステムの構築 ※特許によりほぼ市場を独占 ○定期券初の自動機によるキャシュレス購入の仕組みを考案 ※地下鉄定期券のキャシュレス購入実証実験を実施 ○平成12年 5月　日本初、電子決済インフラ"ペイジー"の仕組みを考案 ※日本マルチペイメント協議会を設立し事務局長に就任 ※各種仕様等を取りまとめ、ペイジーのシステムを構築 ※国庫金、地方公金、公共料金等がネットやATMから支払い可能となる

㈱あいびし 代表 菱沼 昇　氏
NTTデータ在籍時に、数々の画期的な仕組みを考案。
2000年には日本初、**電子決済インフラ「ペイジー」の仕組みを考案**し、
税金や公共料金等がネットやATMから支払い可能となりました。
これらの実績の中からSmart-inが生まれました。

販売展開方法

・オンプレミス
・Saas（ASP）

オンプレミスとは企業の業務システムなどで、自社で用意した設備でソフトウェアなどを導入・利用すること（自社運用）を言います。Smart-inで言うと、Smart-inサービスを提供するサーバを自社で購入・運用し、Smart-inを利用する形態です。

今回、Smart-inの大きな可能性を受けて、日本のシステム業界において多数の顧客を抱える某上場企業（社内でSmart-inサービスを導入済み）が、Smart-inサービスをオンプレミスで販売することになっています。

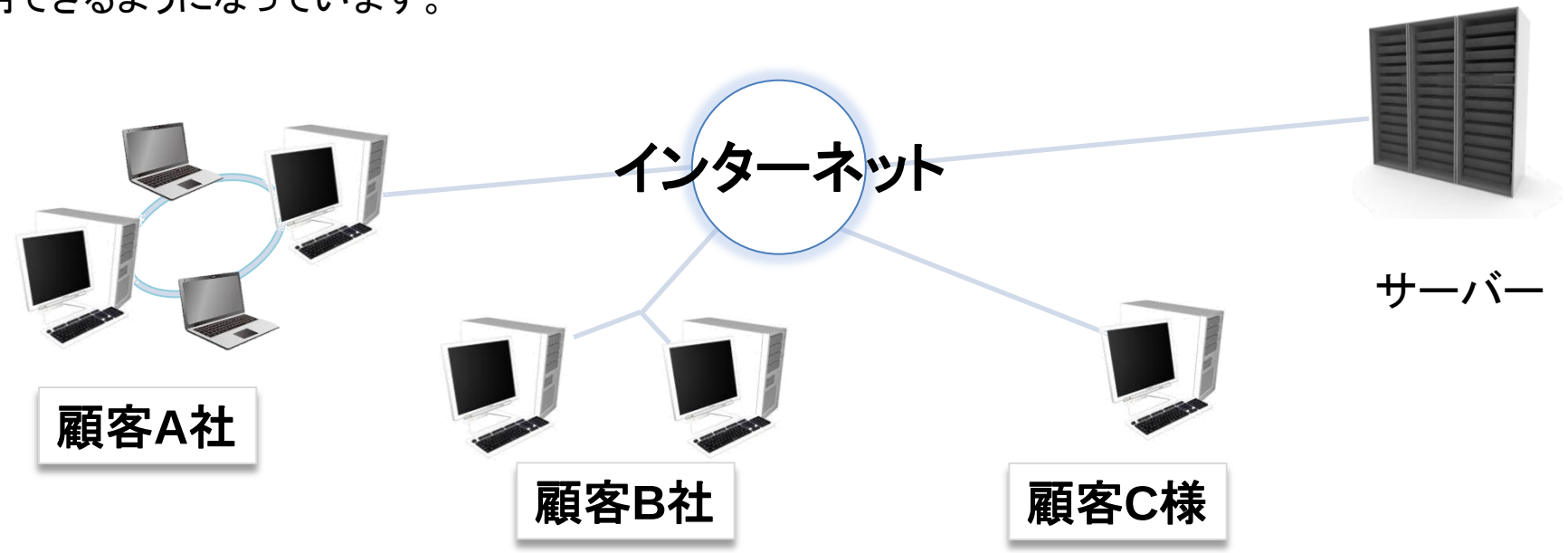
一方、ビー・コミュニティはコストやメンテナンスの面で、中小企業でも導入しやすいSaas（ASP）と言う提供形態で、Smart-inサービスの販売を担っていきます。Saas（ASP）での一般大企業向け販売には、セキュリティ業界において特に大きな影響力を持つ某大手上場企業も参画することになっています。

Saas（ASP）とは

Saas（Software as a Service）もしくはASP（Application Service Provider）とは、一般にインターネットなどのネットワークを経由し、遠隔地からASPのサーバにアクセスすることで、そのサーバ内に格納された各種アプリケーションソフトの機能をサービスの形で利用することをいいます。

これにより、自社での専用のシステム開発を行う場合と比較して、**導入の手間や時間とコストを大幅に削減し、保守・メンテナンスの責任を負うこともなくなるため、小規模での運用などにも優れています。**

大手ポータルサイトのメールサービス（ Gmail、ヤフーメールなど）、データのストレージサービス（google drive、sky driveなど）など、多くのサービスがASPによって提供されており、便利なサービスを安価で多くのユーザーが利用できるようになっています。



Smart-in ASPサーバー

企業用サーバー

100万アカウント

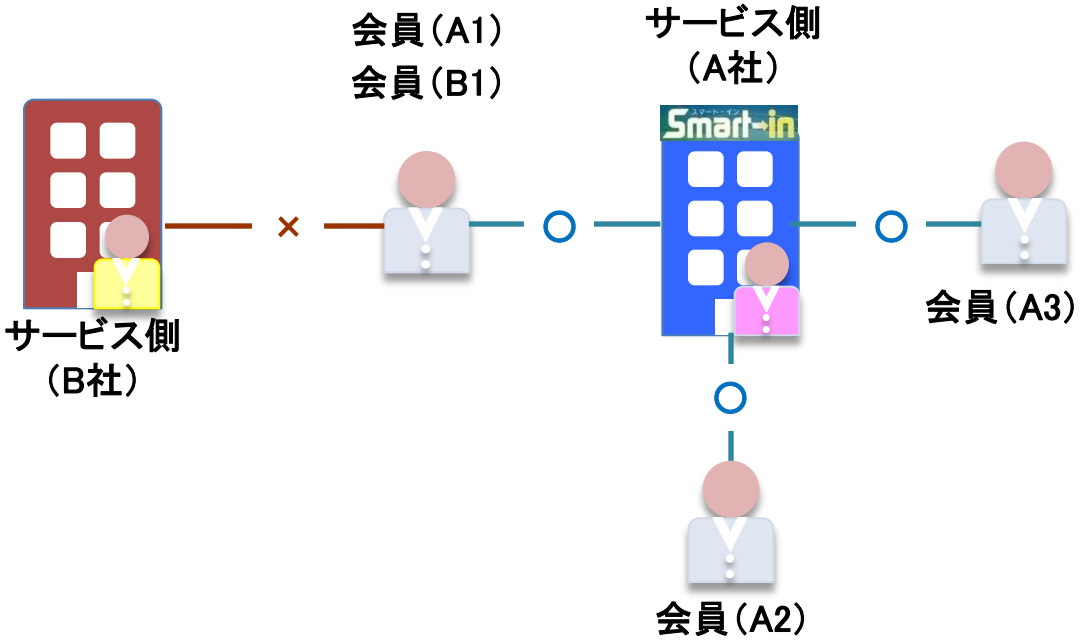
個別用サーバー

100万アカウント

Smart-inのASPサービスは、「企業用サーバー」、「個別用サーバー」という2つのサーバーで提供していきます。1サーバー当たりのSmart-inの募集アカウント数はそれぞれ100万アカウントです。なお、アカウントとは「（Smart-inを）使用する権利」の事を言います。

企業用サーバー アカウント

1 企業用サーバー



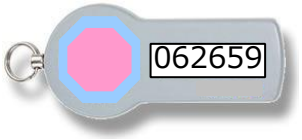
企業用サーバーは、「自社が展開するサービス」もしくは「社内システム」にsmart-inを導入する場合に使うサーバーです。例えば、会員制サイトの運営会社が会員に対してSmart-inのセキュリティを導入できます。

この図では、A社が企業用Smart-inアカウントを購入し、会員A1～A3に付与すると、A1～A3の会員はA社でSmart-inが利用できます。しかし、B社の会員でもあるB1は、B社がSmart-inを導入していないため、B社では利用できません。

企業用サーバー 販売パッケージ

サーバー	パッケージ	アカウント売価	
		パッケージあたり	アカウント単価
企業用（100万アカウント）	スタンダード	100 アカウントまで 15,000/月	150円/月
	スモール	1,000 アカウントまで50,000/月	50円/月
	ミドル	5,000 アカウントまで150,000/月	30円/月
	ラージ	10,000 アカウントまで 200,000/月	20円/月

他の認証方法との比較

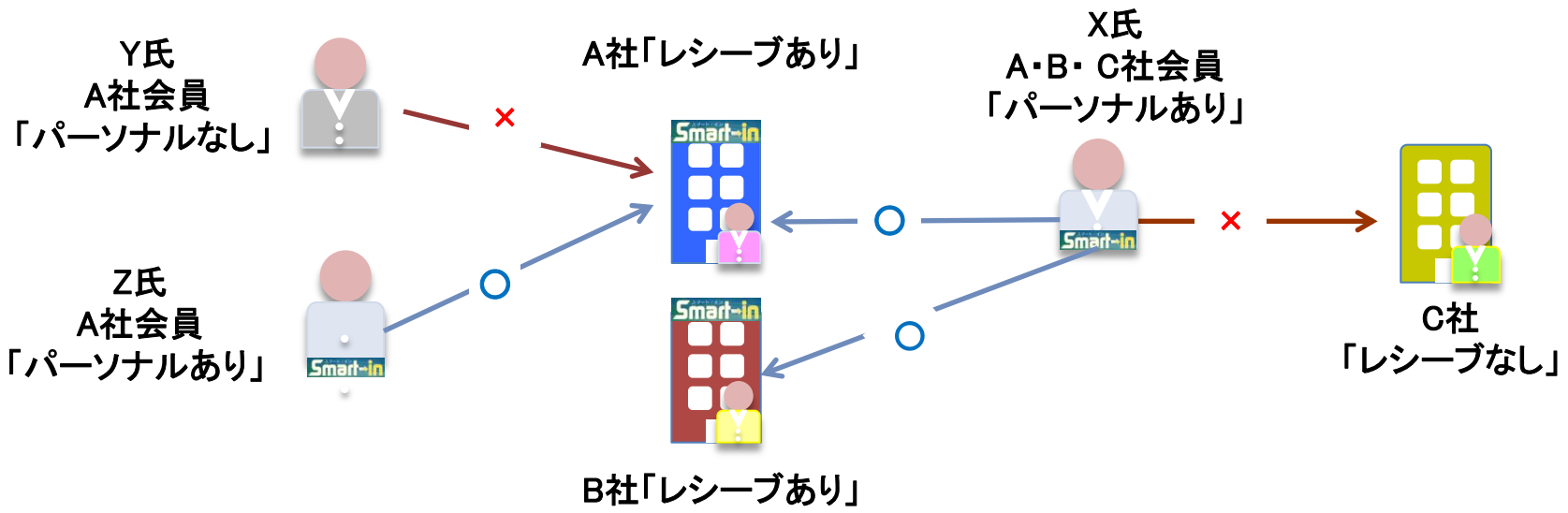


	ワンタイムパスワード トークン型		ワンタイムパスワード SMS型		Smart-in Saas(ASP)型	
セキュリティ	○	一経路二要素	◎	二経路二要素	◎	二経路二要素
初期費用※1	△	90万円	○	0円	◎	0円
月額費用※1		12,000円		50,000円+α ※2		15,000円
利便性	△	複数の専用機器数字の入力	○	数字の入力	◎	着信に折り返し
信頼性・安定性	○	しばらく使わないと時刻ずれで認証エラーになる場合がある	○	SMSの受信の遅れや未達がある	◎	圏外やバッテリー切れなど以外は繋がる

※1　100アカウントあたり費用、税別。ワンタイムパスワードの費用は一般的な価格を例示
※2　1ユーザー月100回以上の認証は1回6.6円を追加課金

個別用サーバー アカウント

② 個別用サーバー（パーソナルアカウント ／ レシーブアカウント）

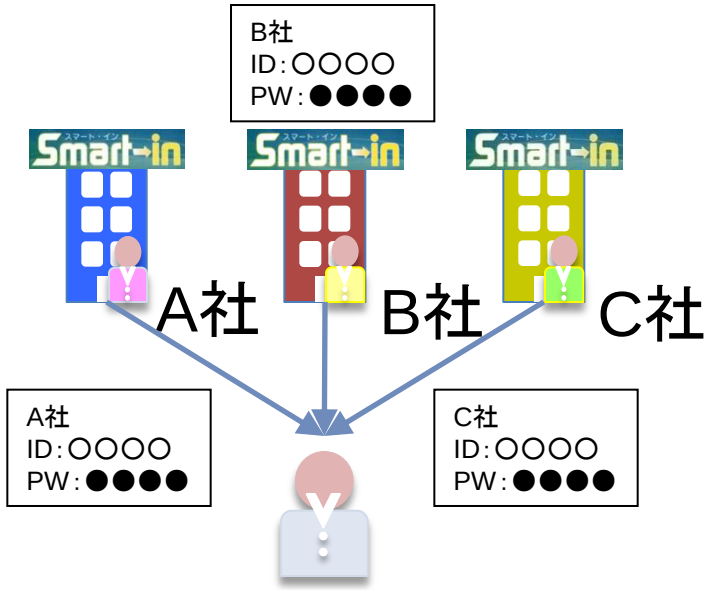


個別用サーバーは、個人がSmart-inを様々な会員サービスで利用したい場合のアカウントを提供します。個人で個別用サーバーの「パーソナルアカウント」（パーソナルと略す）を一つ持つだけで、Smart-inを使うことができます。この際、サービスを提供する企業は個別用サーバーの受信用アカウントである「レシーブアカウント」（レシーブと略す）を所持している必要があります。

例えば、この図では、Xさんはパーソナルを所有しており、レシーブを所有するA社、B社では、Smart-inが利用できますが、レシーブを所有していないC社ではSmart-inを利用できません。Yさんは A社の会員ですが、パーソナルを所有してない為、Smart-inを利用できません。なお、レシーブは1つのアカウントで、全てのパーソナル契約者に対応可能です。例えば、A社はXさんとは別のZさんに対応する為に、レシーブアカウントを追加で購入する必要はありません。

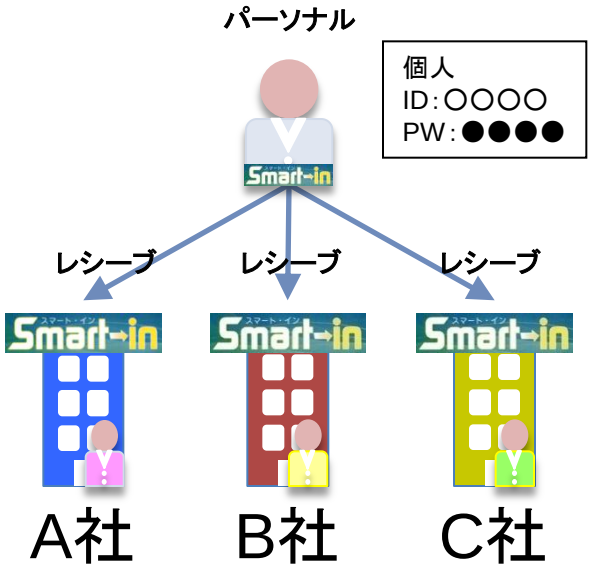
企業用アカウントと個別用アカウント

① 企業用アカウント利用



ID・PW　複数管理

② 個別用アカウント利用



1つのID・PW でOK

企業用サーバーのアカウントを利用した場合、上記のように各社から一人のユーザーにID,パスワードがそれぞれ付与され、複数のID・パスワードを管理する必要があります。一方、個人がパーソナルアカウントを利用した場合は、レシーブアカウントを持っている各社のサービスを1つの共通ID、パスワードで使えるようになり非常に便利です。企業のうち「アカウントの管理を簡単にしたい」企業や、「全会員にはアカウントを配布する必要はないがパーソナルアカウントを持つ個人には使えるようしたい」企業は、個別サーバーのレシーブアカウントを購入するようになると考えられます。

個別用サーバー 販売パッケージ

サーバー	種別	アカウント売価
個別用（100万アカウント）	パーソナル	1アカウント　500円/月
	レシーブ	1アカウント 10,000円/月

Smart-inの想定顧客

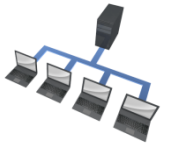
①インターネットバンキング・ネット証券
　2013年のオンラインバンキング不正送金被害額は約14億円で過去最悪
②クレジットカード
　高額決済時の本人確認で不正利用を未然に防止。2012年の不正使用被害額68.1億円

③EC サイト
　不正購入やポイントの盗難。S社サイトで最大15万件のカード情報漏洩の可能性

④ポイントプログラムサービス
　2014年2月N社不正ログイン発覚43人数十万円分マイル搾取、3月Z社9名112万マイル詐取
⑤会員制サービス
　複数アカウントの利用防止によるコンプライアンス向上。なりすましによる不正利用防止
　2014年2月 大手SNSにて約1万7000件の不正ログイン--身に覚えのないつぶやき投稿

⑥オンラインゲーム
⑦不動産賃貸管理システム
⑧電子カルテ・電子薬歴（院内システム、在宅医療）
　院内システムおよび訪問看護、訪問介護時の医療情報利用における本人確認

⑨社内システム（グループウェア、勤怠管理、経費精算、研究開発、顧客管理）
⑩在宅勤務
⑪社外での営業支援（保険設計等）
⑫BCPを含む災害時の本人確認



Smart-inの想定販売企業

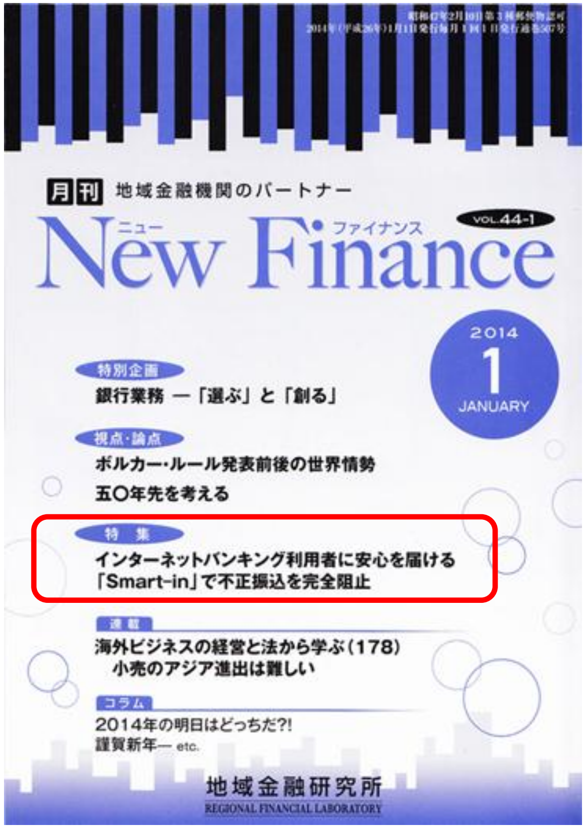
①システム販売会社
既存顧客への販売、
セキュリティ関連商品とのセット販売による商品力・ブランド力強化

②携帯電話・タブレット販売会社・代理店
既存顧客への販売、新規顧客にセット販売

③保険代理店
個人情報漏洩保険を取り扱う損害代理店、
および法人向け生命保険代理店が既存顧客への販売、既存顧客にセット販売

④PマークおよびJAPHICマーク、ISO27001取得コンサル会社
既存顧客への販売、新規コンサル時にセット販売

金融機関向け専門誌　特集掲載（2014年1月）



New Finance　2014年1月号
（通巻507号）

インターネットバンキング利用者に安心を届ける

「Ｓｍａｒｔ－ｉｎ®」で不正振込を完全阻止

㈱あいびし　www.aibc.co.jp/
代表取締役　要沼　異

一．歯止めがかからない不正送金被害

インターネットバンキングで利用者のＩＤやパスワードが盗み取られ預貯金を不正に送金される被害が昨年夏頃から急増し歯止めがかからない状況となっています。その手口は様々ですが、ほとんどのケースは利用者のパソコンをウイルスに感染させ、気付かないうちにＩＤ、パスワード、暗証番号、乱数表、合言葉を盗み取るというもので、銀行が被害を防ぐため取引のたびに変える「ワンタイムパスワード」まで盗まれています。

この多発するインターネットバンキングの不正送金被害に遭わないようにするためには、「パソコンのブラウザーやアプリケーションソフトの脆弱性を解消する」「ウイルス対策ソフトを導入する」「メール添付ファイルは絶対に開かない」「ＩＤやパスワードは流用せず、可能ならワンタイムパスワードを利用する」「口座やカード利用明細を定期的に確認、アクセス利用履歴もチェックする」等の対策を講じる必要があります。しかし、このような対策を講じれば講じるほど、操作・手順は煩雑となり実用性は低下するため、セキュリティ対策という課題に対してバランスをとる必要が出てきます。

二．全く新しい発想で不正振込を阻止する「Ｓｍａｒｔ－ｉｎ®」

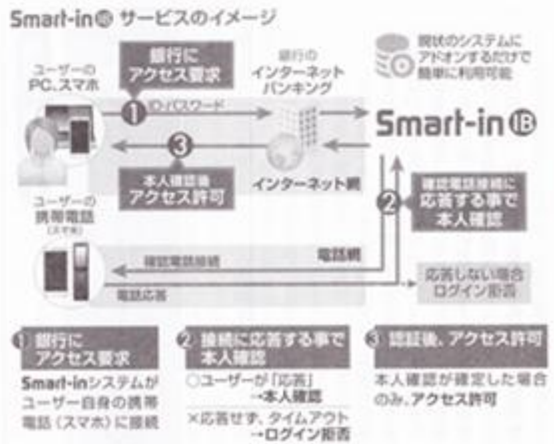
そもそも、インターネットは規制のないオープンネットワーク構造を有しており、インターネット上を流れる情報は「誰かに見られるかもしれないし、書き換えられるかもしれない」という意味で安全ではありませんし、これらの情報を完璧に防衛することは困難といえます。

そこで、その課題を解決するために、今まで全く発想がなかった「電話網（注）」という閉域網とインターネットの融合による本人認証の仕組み（特許出願中）」を活用したサービスが「Ｓｍａｒｔ－ｉｎ®」なのです。

「Ｓｍａｒｔ－ｉｎ®」は、情報（ＩＤ・パスワード）と物（携帯電話）の「二要素認証」および、インターネットと電話網の「二経路認証」で不正ログインを防ぐ仕組みであり、上図❷の通り、「Ｓｍａｒｔ－ｉｎ®」を利用していないのに携帯電話（スマホ）に接続があった場合は第三者の不正ログイン操作中（なりすまし）と判断・検知し排除します。

従って、不正利用者が不正に入手したＩＤやパスワード、第二暗証（口座暗証）でログインを試みても、なりすましを検知しログイン自体ができませんので、不正振込を完全に阻止できるということになります。

このように、「Ｓｍａｒｔ－ｉｎ®」は、既存の電話接続を利用することで、「低コストで高セキュリティを実現」しているサービスであり、「安全にインターネットバンキングを利用してもらいたい」、「インターネットバンキングをもっと普及促進させたい」と考えている金融機関にとっては注目に値するサービスと言えます。



❶ 銀行に アクセス要求
Smart-inシステムがユーザー自身の携帯電話（スマホ）に接続

❷ 接続に応答する事で本人確認
○ユーザーが「応答」→本人確認
×応答せず、タイムアウト→ログイン拒否

❸ 認証後、アクセス許可
本人確認が確定した場合のみ、アクセス許可

（注）「電話網」は「インターネット網」と異なり、「規制の多いプライベートネットワークである」「通信事業者が管理・保全を行っている」「接続端末は通信事業者が提供する認定品である」「電話番号自体が交換機から割り当てられた番号のため"なりすまし"ができない」といった特性があります。

ビー・コミュニティの商品選択基準での評価

1. 公益性・社会的需要
   - ・不正アクセス対抗

2. 自らの評価・第3者評価
   - ・技術力、ノウハウ、特許申請
   - ・業界大手採用、販売

3. サービス提供者・サービス利用者・事業者が公正な事業活動を行えるか
   - ・企業　　コスト軽減、社会的信用保護
     情報管理責任者の責任軽減
   - ・利用者　利便性
   - ・大企業、中小企業、個人共に導入可能

Smart-in拡販プロジェクト
事業参画のご案内

Smart-in販売員の募集

販売員の収入

業務委託費の支払い

販売したSmart-inアカウントの売上の5%を受取り（毎月）

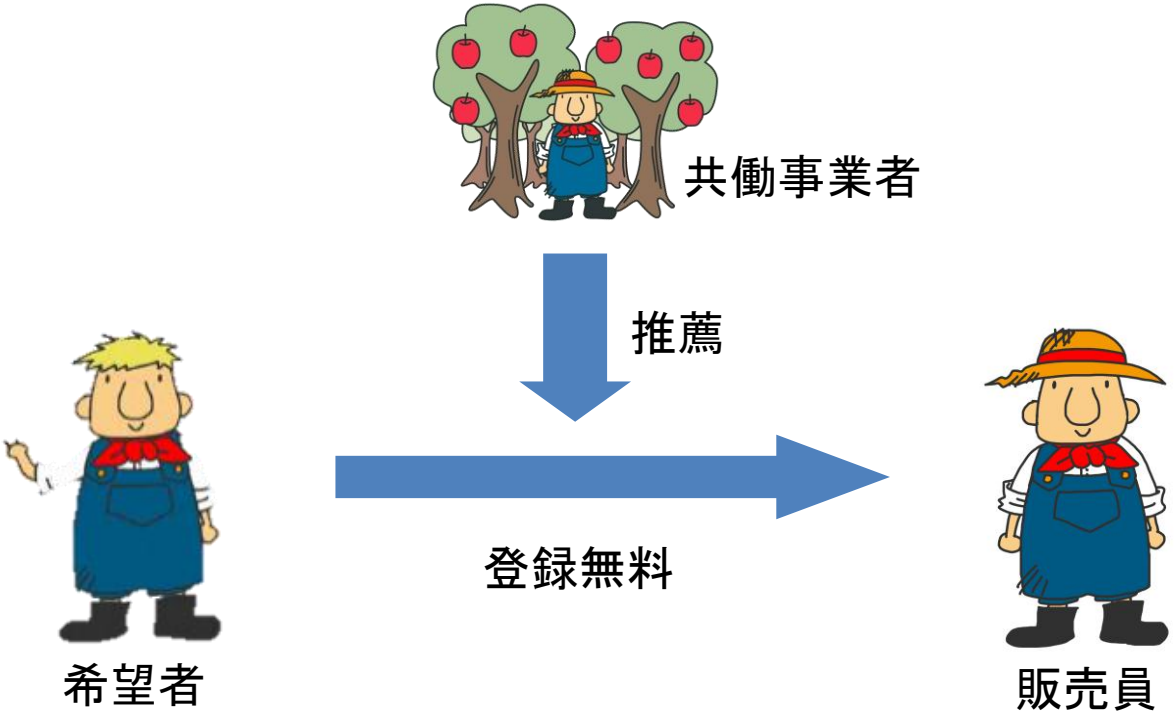
収入例

企業用サーバーのアカウントを3パッケージ販売

パッケージ	アカウント売価			業務委託料		収入例
	アカウント数	単価	総額	月額	年額	
スタンダード	100	150円/月	15,000/月	750/月	9,000/年	27,000/年
スモール	1,000	50円/月	50,000/月	2,500/月	30,000/年	90,000/年
ミドル	5,000	30円/月	150,000/月	7,500/月	90,000/年	270,000/年
ラージ	10,000	20円/月	200,000/月	10,000/月	120,000/年	360,000/年

販売員登録の流れ

共働事業者の推薦により、無料で登録



販売員希望者は(株)ビー・コミュニティの共働事業者から推薦を受け、所定の手続きを行うことで、販売員として登録することが出来ます。

販売員登録方法

https://www.bee-community.org/

https://www.bee-community.net/

登録するためには、共働事業者が共働事業者専用HPから販売員の推薦を行い、その後、
販売員希望者が販売員専用HP※から販売員登録を行います。

※一般用HP下部にリンク、ID,PASSは共働事業者専用HPに記載

販売員　募集要項

応募資格
反社会的勢力と一切関係を有していない満18歳以上の個人または法人となります。
ただし、満18歳以上の未成年者の登録には、弊社所定の面談が必要となります。面談の詳細については、弊社からご連絡いたします。また、本事業における誓約書や、親権者の同意書を提出していただきます。

業務委託料
月末締め、翌月20日払いです。20日が金融機関の休業日の場合、翌営業日になります。

振込手数料
キャンペーン期間を除き、報酬の振込手数料は原則、販売者の負担となります。

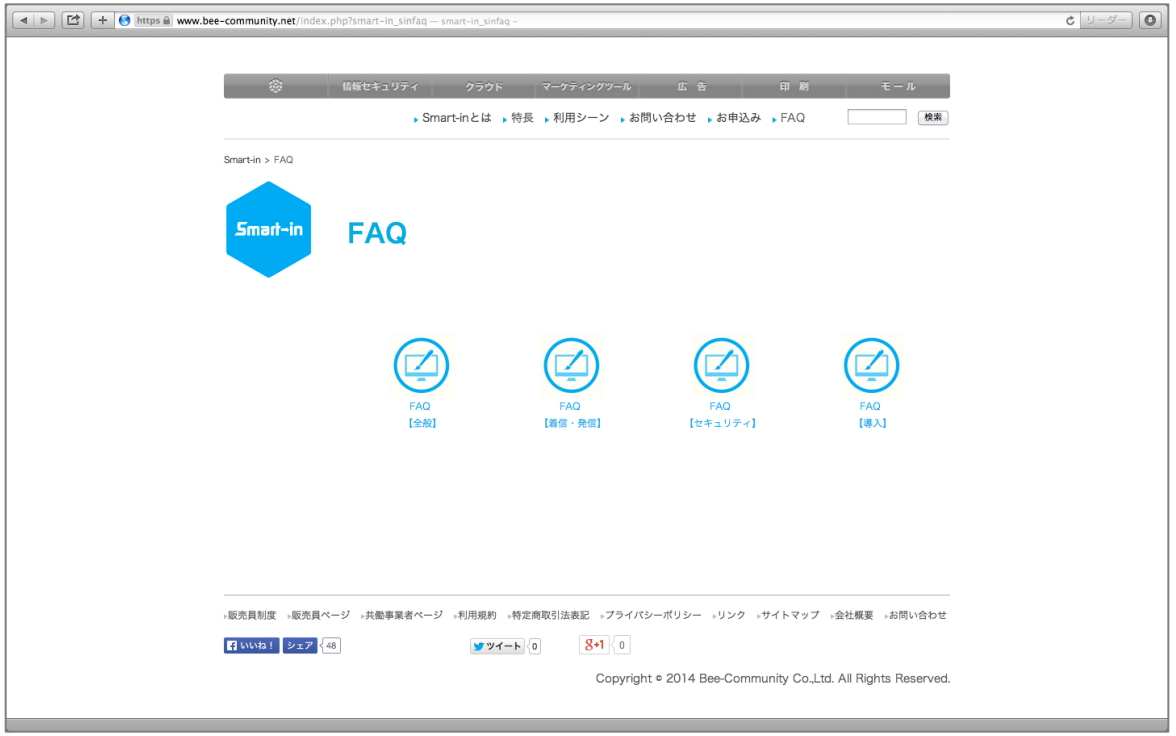
譲渡
販売員の資格に関しては、弊社が認める場合を除き、弊社の許可なく第三者に譲渡、売買、名義変更、質権その他担保に供する等の行為をすることはできません。

契約期間
契約の有効期間は当該販売員に対して販売員IDを発行してから1年間です。但し、期間満了の30日前までに弊社若しくは販売員が本規約に基づく販売員契約を更新しない旨の意思を表示しない限り、本規約に基づく販売員契約は更に1年間更新されるものとし、その後も同様とします。

良くある質問とその答え

ご不明な点、ご質問等ございましたら、まずは公式サイトのFAQ（良くある質問とその答え）をご覧ください。

https://www.bee-community.net/index.php?smart-in_sinfaq



注意事項

1. 本資料の記載事項以外の不確かな内容を説明されて生じた損害に関しては、説明者の責任となります。予めご了承ください。

2. 許可なく本資料の複製、転写、改変等を禁じます。

3. 自己の印刷物・画像・画面等に、本事業に関連する商標等を使用することを希望する場合には、事前に弊社に書面による承諾を得なければなりません。