Janog43
サイバーセキュリティBOF #4

2019年1月23日

発表者紹介

森崎 樹弥 氏

一般社団法人JPCERT コーディネーションセンター早期警戒グループ

- JPCERT/CCの足軽…つまり、何でも屋です。マルウェアを追っていたら、スパム・踏み台・オープンポートなどabuseの世界へ。。。
- 食べ物は肉、肉、肉が好き！

森川 慶彦 氏

株式会社KDDI ウェブコミュニケーションズ
クラウドホスティング事業本部 サービス運用部

- ネットワークインフラをメインに、 AS9597の運用に従事
  abuse宛メールを受け取ることが多く、逃げられなくなる
- 菓子パンが好きです。

藤ノ原 真雄 氏

株式会社 NTTPCコミュニケーションズ
テクノロジー＆オペレーション開発本部 CSOスタッフ（CSIRT担当）

- 運用から開発までなんでもござれのセキュリティ担当者
- 関東では食べられない…資さんうどん

山下 健一 氏

さくらインターネット株式会社 技術本部

- 仮想化サービスの運用 …がいつの間にabuse 担当に
  もうダメだ …おしまいだぁ …
- もりそばが好き、 ざるよりもりがいいかなぁ

久保田 雄 氏

NTTコミュニケーションズ株式会社 クラウドサービス部

- Cloud^{n}なんでも担当。事業計画からAbuseまで
- カライ。スキ。デモ。ホッキョク。ダメ。ゼッタイ！

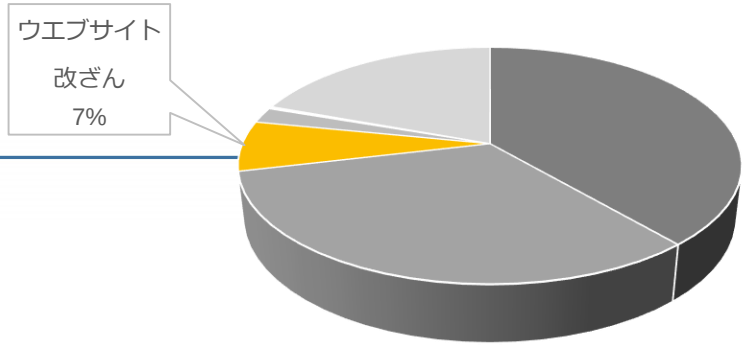
本日の流れ

1．サイバーセキュリティの現状
(JPCERT)

2．各事業者の取り組み
(さくら/KWC/NTTPC/NTTCom)

3．フリートーク
～事前アンケートの結果とともに～

改ざんについて

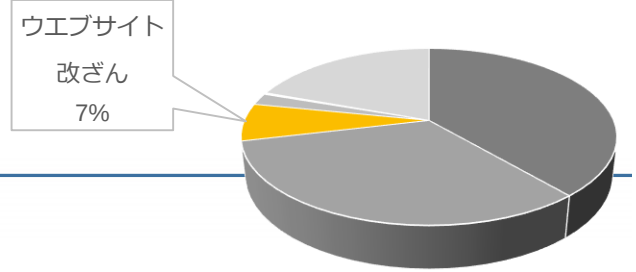


- **代表的な手法**
  - アカウント窃取による不正ログオン
  - ソフトウエア (CMS やフレームワークなど)の脆弱性を利用
  - アプリケーション開発時に含んでしまった脆弱性を利用

過去には、脆弱性の影響による急増も

JPCERT/CC インシデント報告対応レポート https://www.jpcert.or.jp/ir/report.html
JPCERT/CC Webサイトへのサイバー攻撃に備えて 2018年7月 https://www.jpcert.or.jp/newsflash/2018071801.html

改ざんについて

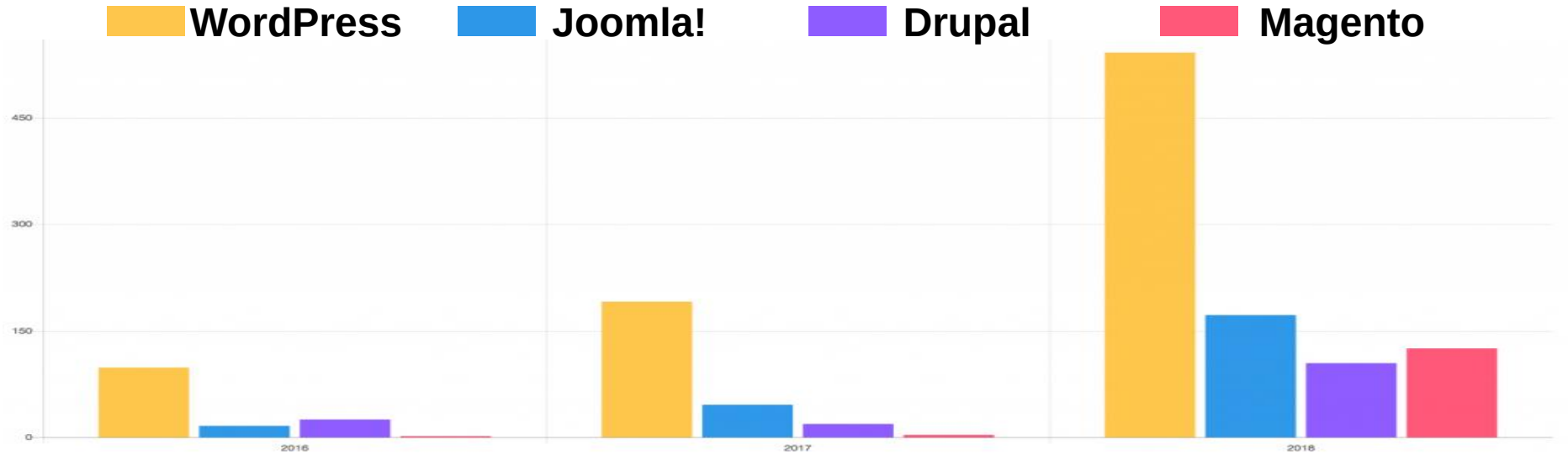


年々増加傾向にある CMS の利用率

―うち WordPress は 全体の 32.7%（2019/1時点）

2011/1	2012/1	2013/1	2014/1	2015/1	2016/1	2017/1	2018/1	2019/11
23.6%	29.0%	31.8%	35.2%	38.3%	43.4%	46.7%	48.7%	54.7%

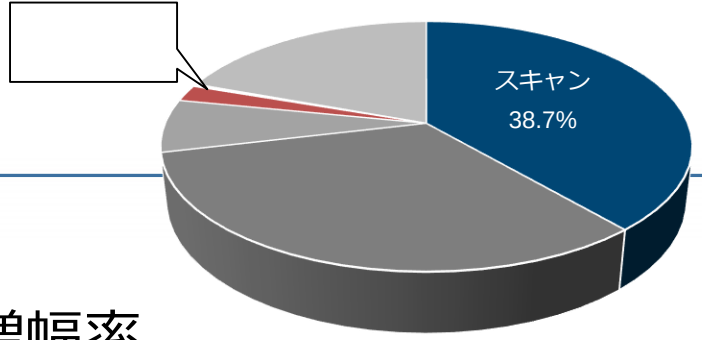
図 CMS を利用しているサイトの割合 (Q-Successより)



各 CMS 共に脆弱性の観測数が急増

The State of Web Application Vulnerabilities in 2018（Imperva）
https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/

DoS、DDoS について

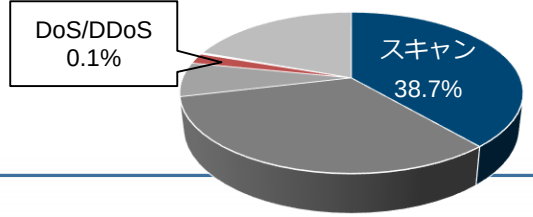


- **オープンポートの問題**
  - DDoS でよく使われるポートと増幅率
  - これらは Udp の仕組みを悪用し増幅したレスポンスを送ることで攻撃を仕掛ける

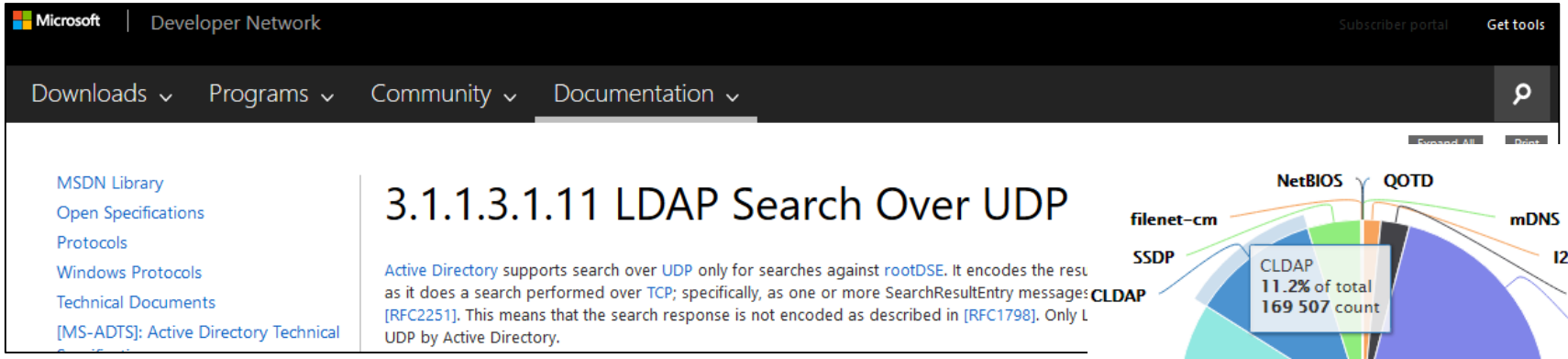
ポート番号	プロトコル	増幅率
53 / Udp	DNS	28 ～ 54
123 / Udp	NTP	556.9
161 / Udp	SNMP	6.3
389 / Udp	CLDAP	56 ～ 70
1900 / Udp	SSDP	30.8
11211 / Udp	Memcached	10,000 ～ 51,000

【出典】リフレクション攻撃(アンプ攻撃）を防御する方法（A10 ネットワークス）
https://www.a10networks.co.jp/news/blog/how-defend-against-amplified-reflection-ddos-attacks.html

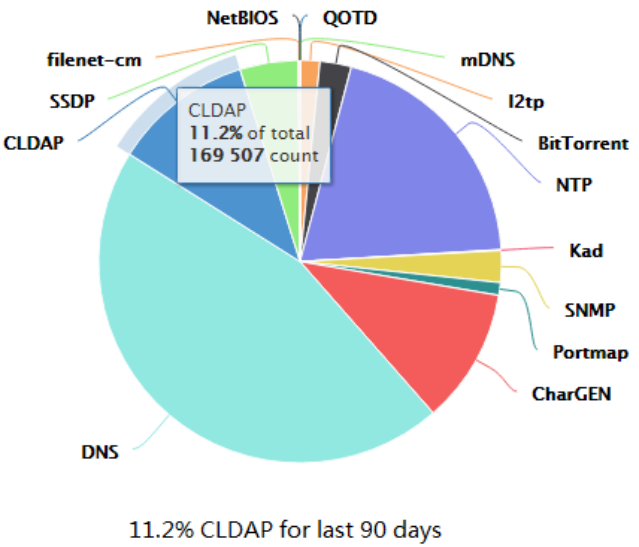
CLDAP の観測



- **Connection-less** Lightweight Directory Access Protocol（CLDAP）
  - LDAPUDP による接続 (389/udp)
  - Microsoft Active Directory が 389/udp を利用



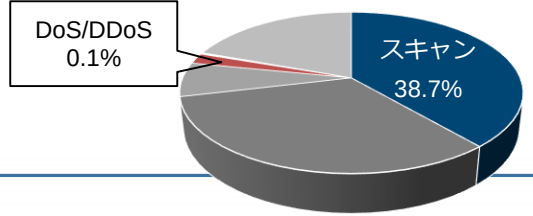
- DDoSMon の観測結果によると、DDoS全体で3番目に観測が多い（図は2017年11月時点）



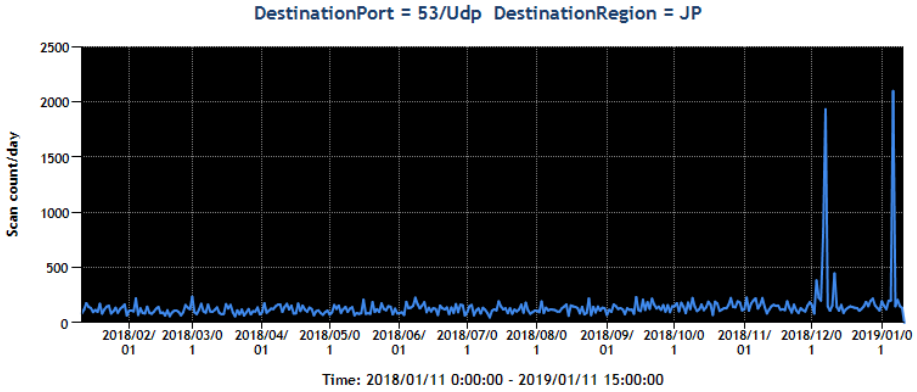
11.2% CLDAP for last 90 days

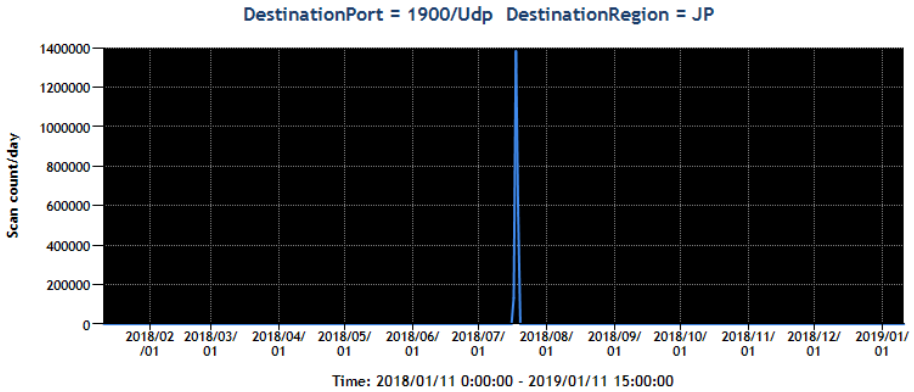
【出典】CLDAP is Now the No.3 Reflection Amplified DDoS Attack Vector, Surpassing SSDP and CharGen（Qihoo 360）
https://blog.netlab.360.com/cldap-is-now-the-3rd-reflection-amplified-ddos-attack-vector-surpassing-ssdp-and-chargen-en/

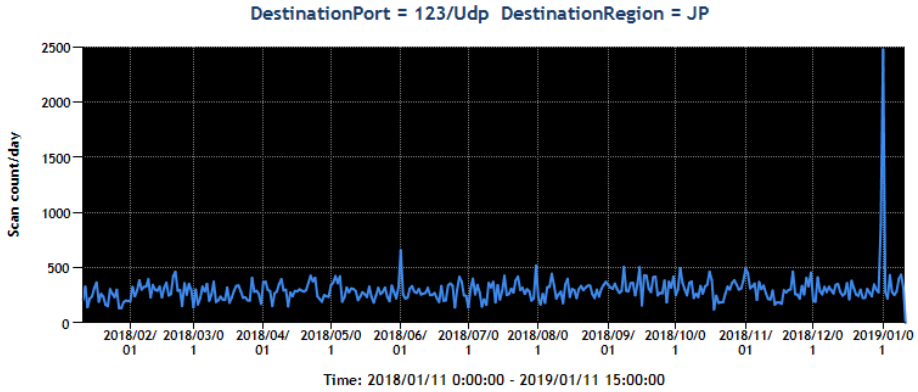
TSUBAMEでの観測

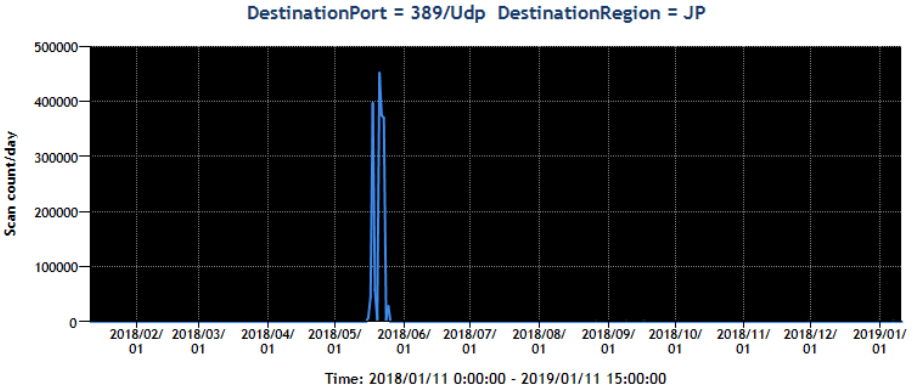


DDoS常連ポートのスキャン状況（直近１年）



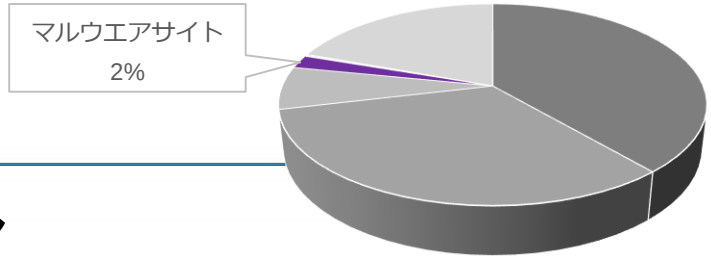






直近でもスキャンの急増は確認されている

スパムメール送信について



マルウエア感染を目的としたばらまきメール

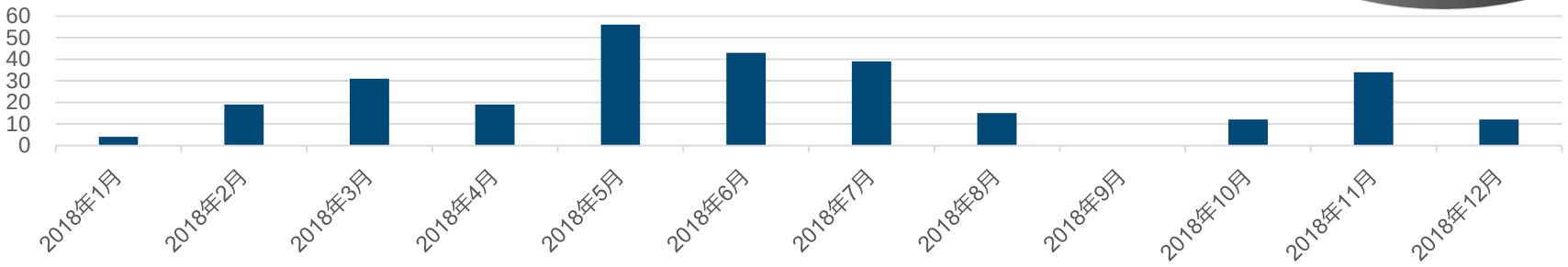


図 ばらまきメール観測数（種類数）

【参考】catnap707（Twitter）
https://twitter.com/catnap707

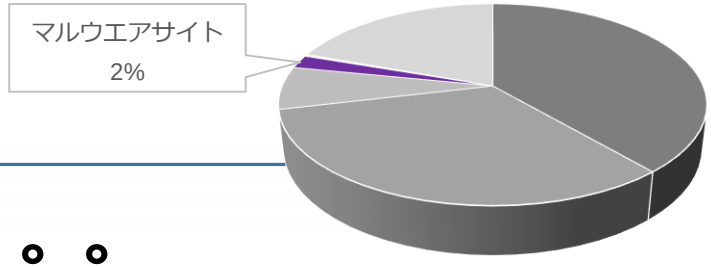
ばらまきメール件名の例

- 12月、原価請求書です。
- Re: ヴィスト修正
- 注文書の件
- 申請書類の提出
- 立替金報告書の件です。
- 納品書フォーマットの送付
- 請求データ送付します

ボットネット CUTWAIL の利用

- 2018年に国内で確認されたマルウエア拡散メール攻撃では、CUTWAILと呼ばれるボットネットが多く利用されていた。

スパムメールの踏み台について



ばらまきメールの送信元を見ると。。。

2018年12月16日07時
【件名】Amazonアカウントが閉鎖しようとしています！
【送信元】
amazo000019@m19.coreserver.jp

2018年12月18日17時
【件名】_申請書類の提出
【送信元】texthh15@ab.auone-net.jp

2018年11月26日18時
【件名】あなたの*受信メールアドレス* メールアカウントは一時停止されます！
【送信元】honjo-zddan@mui.biglobe.ne.jp

2018年11月01日17時
～2018年11月05日09時
【件名】オークリー(oakley)正規商品販売店限り活動特価2499円【85%OFF】三つを買うなら、配達無料
【送信元】e-glasses@shop.rakuten.co.jp

Webメールが踏み台になっているケースが散見される

２．各事業者の取り組み

①不正に気付くための取り組み
②不正がわかった後の取り組み
③不正を起こさないための取り組み

①不正利用に気付くための取り組み

	A社	B社	C社	D社
改ざん	-	-	-	-
DoS、DDoS	○	○	○	○
スパム送信	○	○	○	-
不正プロキシ	○	-	△	-
自動検出 (AIとか)	-	-	-	-

○:対応実施　△:チェックのみ　-:実施なし

②不正がわかった後の取り組み

	A社	B社	C社	D社
サービスやアカウント停止のタイミング	検知即、連絡後、停止時期はサービスに依る	検知次第 即時停止 (以前は連絡後)	原則連絡後 (緊急性の高い場合即時もある)	原則連絡後 (緊急性の高い場合即時もある)
サービスやアカウント再開の判断基準	顧客からの対応完了連絡後	顧客からの対応完了連絡後	顧客からの対応完了連絡後	顧客からの対応完了連絡後
顧客への連絡時の反応 (対応速度や感度など)	半年近く経過後に連絡来る場合が！	改竄などは概ね対応してもらえるがなかなか話が通じないことも	Webサイト系は反応があるメール/プロキシ系は反応が薄い	基本レスなし (悪意があるためか？)
面白ネタ (あれば、フリーテキストで)			サービス停止の可能性がある度だと無視される。サービス停止予告ぐらいでないと対応されない	顧客の顧客(=エンドユーザ)が不正をしたときの対処が悩ましい (顧客に悪意はないが…)

②不正がわかった後の取り組み

サービス停止のタイミング

・不正確認後即アカウント停止。

・ユーザーへの警告後に停止。
(ただし法執行機関からの通報に関しては即停止)

サービス再開の判断基準

・顧客からの対応完了連絡。
ただし判断基準はそれぞれ、さっと見るだけ　コンテンツの初期化まで

顧客の反応

・通知だけだとやはり対応速度は遅め。アカウントの停止を行うと
迅速に対応していただける。

・エンドユーザーの温度感。

③不正を起こさないための取り組み

	A社	B社	C社	D社
申込サイトアクセス制限	△	-	-	○
本人性確認 (メール/電話認証)	○	-	-	○
メール制限 (ドメイン等)	○	-	-	-
発番制限(海外発番ブロック等)	○	-	-	○
本人性確認 (身分証提出)	-	-	-	-
住所確認 (開案の郵送など)	△	-	△	△
クレカ制限 (独自ブラックリスト等)	-	○	-	△
人の目による確認	○	○	○	○
自動検出(AIとかで)		-	-	やりたい！

○:対応実施　△:チェックのみ　-:実施なし

③不正を起こさないための取り組み

効果があると思うもの

・人の目による怪しいと思われる契約内容の粗探し
・郵送物の送付(宛先不明になったらBAN)

効果が薄いと思うもの

・海外からの申込(IP)制限＆発番制限
(すり抜け方法がいくらでもある…)

効果があると思うができてない/できないもの

・メールドメイン制限(海外系のドメインをブロックしたい…)
・身分証(効果が高いと思うが確認稼働＆個人情報取り扱い…)

３．フリートーク
～事前アンケート結果とともに～