Learn from the big mistakes of cashless payment service in Japan

HITCON2021

AIDO & Manaka(VR)

HITCON 2021
HITCON 2021
WORK FROM HOME, HACK INTO HOME

Speaker Brief (AIDO)

- ✓ Current job : CSIRT Team member of Large Bank
- ✓ General Leader of Penetration Testing Team at National center of Incident readiness and Strategy for Cybersecurity (2017,2018)
- ✓ Formulate guidelines for Developing Security Policy for Financial Institutions (2005 - 2019)
- ✓ ISLA (Information Security Leadership Awards) Senior Security Professional, Community Service Star(2019)
- ✓ HITCON Speaker (2012, 2013, 2015)

Speaker Brief (Manaka VR)

- ✓ She's from the two-dimensional world
- ✓ I'm always with her when I speak
- ✓ It's a shame we can't share our love online
- ✓ Next year, we will definitely come to Taiwan together!

Agenda

1. Common points of payment services in Japan and Taiwan
2. Status of cashless payments in Japan
3. What Japan's cashless payments are aiming for
4. Serious incidents that occurred in cashless payment in Japan
5. 7Pay overview and problems
6. docomo account overview and problems
7. Japan Post Bank and mijica overview and problems
8. Significant similarities between the three incidents
9. What we can learn from these incidents

1.Common points of payment services in Japan and Taiwan

Common points of payment services in Japan and Taiwan

- ✓ Similar cultures where cash dominates over credit cards
- ✓ Transportation cards are widespread

Suica

Easy Card

- ✓ Convenience stores are everywhere and ATMs are available

2. Status of cashless payments in Japan

Status of cashless payments in Japan

✓ be crowded with every sort of services

2018 → 2019

✓ There’re a huge number of cashless payments that can be used only in specific stores or regions

Status of cashless payments in Japan

- ✓ 6 companies (PayPay, Rakuten, DoCoMo, LINE, mercari and au) occupy most of the market share
- ✓ Four of the six companies are cell phone carriers
- ✓ To gain an edge over your competitors, you need three points:
  - Many stores and areas can be used
  - Attractive discounts and point return campaigns
  - Fulfilling Shopping site that can be used only own members
- ✓ It's just a means of payment. From the user's point of view, there is no big difference between any services
- ✓ The types of products sold on the shopping site are become similar
- ✓ Financial services are competitive in regulation, so they cannot be differentiated in the first place

Status of cashless payments in Japan

- ✓ J-COIN Pay, which was a concerted effort by many Japanese banks, sank like the Titanic because its parent company, Mizuho Bank, had a lot of major system failures
- ✓ LINE was going to be integrated into PayPay, which became the same group. However, the issue of Chinese monitoring of LINE messages was discovered, and the integration was lost for fear of being disliked by shareholders

3. What Japan's cashless payments are aiming for

What Japan's cashless payments are aiming for

- ✓ Aiming for loosely regulated "bank-like financial services"
- ✓ They want to invest assets with the collected charge balance
- ✓ They look like banks, but if they fails, they can go bankrupt (banks cannot easily go bankrupt due to deposit or protection)
- ✓ They look like banks, but they’re easy for Mergers and Acquisitions (whether they succeeds or fails)

What Japan's cashless payments are aiming for

- ✓ If they get a name value and many customers, they want to become real banks
- ✓ They want to lock in the economic zone in their corporate group
- ✓ Telephone carriers + online distribution (advertising) + shopping site+ financial services include insurance, securities
- ✓ They want to have all the services they can offer online

Why messed up Cashless payment in Japan?

- ✓ Applications and charging functions at convenience stores'ATM are easy for businesses because they only purchase external services
- ✓ It is easy to explain to shareholders the plan to open a cashless payment service so that they will not lose to their rivals
- ✓ Launching a new cashless payment service is a big credit for the **individual officers**
- ✓ Officers of the parent company, subsidiaries, and investees will start cashless payment services from the same brand group **for their own credit**

4. Serious incidents that occurred in cashless payment in Japan

Serious incidents that occurred in cashless payment in Japan

✓ I will explain three of them whose details are known

	Accrual date	Number of victims	Damage amount	Main cause
PayPay	Dec2018	Undisclosed	Undisclosed Possibility of hundreds of millions JPY	Credit card security code can be retried any times Can use Credit master key
7Pay	July2019	807	39millionJPY	Password list Attack
docomo account	Sep2020	125	28millionJPY	Vulnerabilities in Account transfer
Japan Post Bank mijica	Oct2020	380	60millionJPY	Vulnerabilities in Account transfer

✓ All are famous companies that represent Japan

Positions of PayPay

- ✓35 million users and 3 million merchants(Feb2021)
- ✓Largest share in Japan, 66% of smartphone contractors use this
- ✓Service provided by Softbank mobile group
- ✓10 billion JPY return campaign 1st (Dec2018)
- ✓10 billion JPY return campaign 2nd (Jan2019)
- ✓Scheduled to be integrated with LINE

Positions of 7Pay

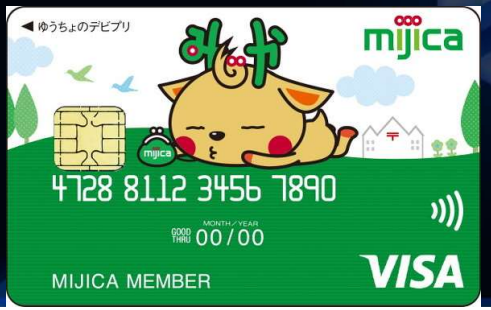
- ✓Japan’s most famous and largest convenience store
- ✓Expanded shopping site “omni7(7net shopping)” to 7Pay as Cashless payment service

Positions of docomo Account

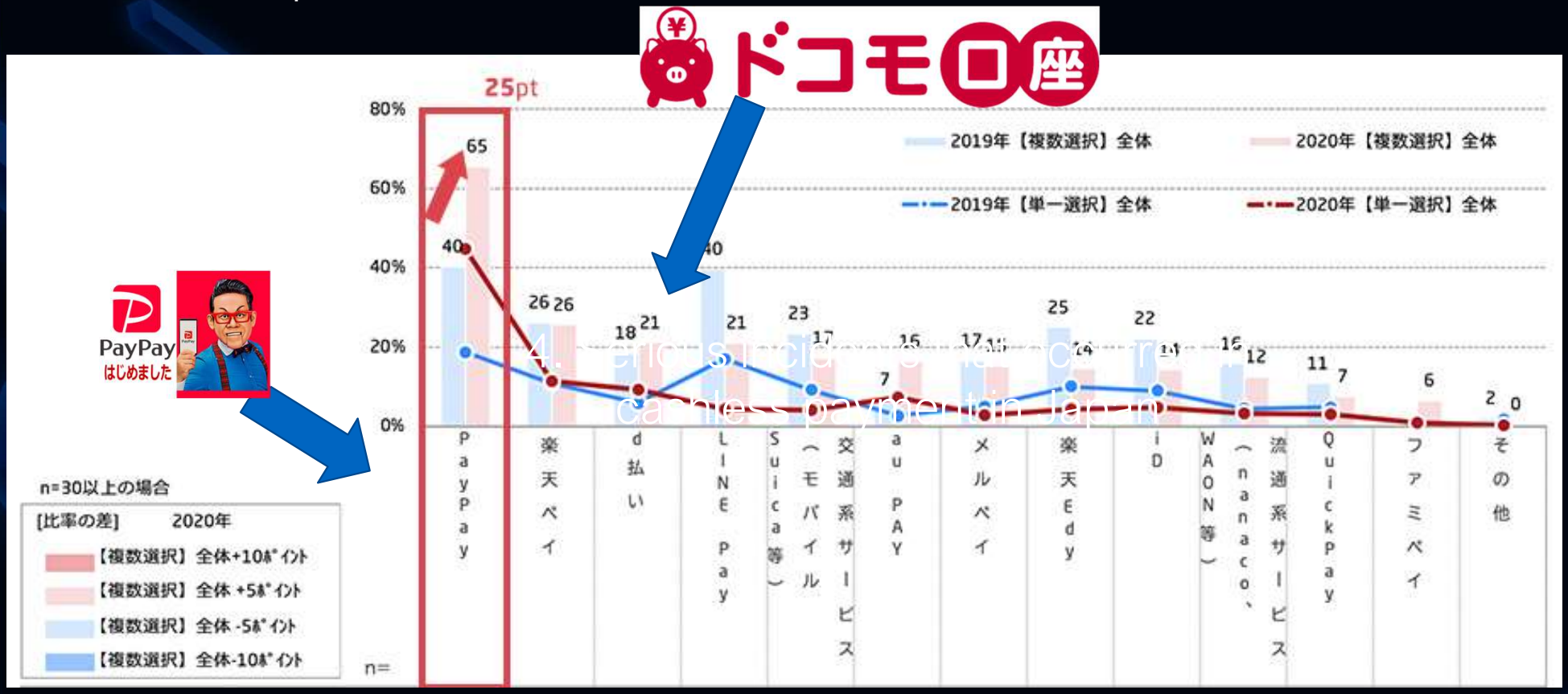
- ✓Japan's largest mobile phone career
- ✓A state-owned enterprise that originally monopolized telephone communications
- ✓Started as a service for mobile phone contractos (May2011)
- ✓Smartphone payment service ”d-payment” started (Apr2018)
- ✓Shared 21% of smartphone QR payments market
- ✓Mobile phone carriers have the largest share

Positions of Japan Post Bank ,mijica

- ✓ Japan Post Bank was originally a state-owned postal business
- ✓ Total assets
  1. Mitsubishi UFJ FG 337 trillion JPY
  2. Sumitomo Mitsui FG 220 trillion JPY
  3. Mizuho FG 215 trillion JPY
  4. Japan Post Bank 211 trillion JPY ← 4th place
- ✓ Post offices in all areas of Japan also serve as branches, Overwhelming number of branches
- ✓ mijica and Japan Post Pay are different service companies
- ✓ mijica is prepaid debit card



Share in Japan



https://www.nec-solutioninnovators.co.jp/ss/retail/whitepaper/09/?utm_source=google&utm_medium=cpc&utm_campaign=adw_retail05&utm_term=%E3%82%AD%E3%83%A3%E3%83%83%E3%82%B7%E3%83%A5%20%E3%83%AC%E3%82%B9&gclid=Cj0KCQjwsqmEBhDiARIsANV8H3Y10NLlk9dzwRaifxv1vZ_z9Mw9XiZ2dDAH_1N7bdmsk6N35bGYMW8aAu3pEALw_wcB

5.7Pay overview and problems

Overview of illegal money transfer at 7Pay

- ✓The service will start on 1st July 2019.
- ✓If you register as member,you'll get one ONIGIRI
- ✓illegal money transfer occurs the day after the service starts

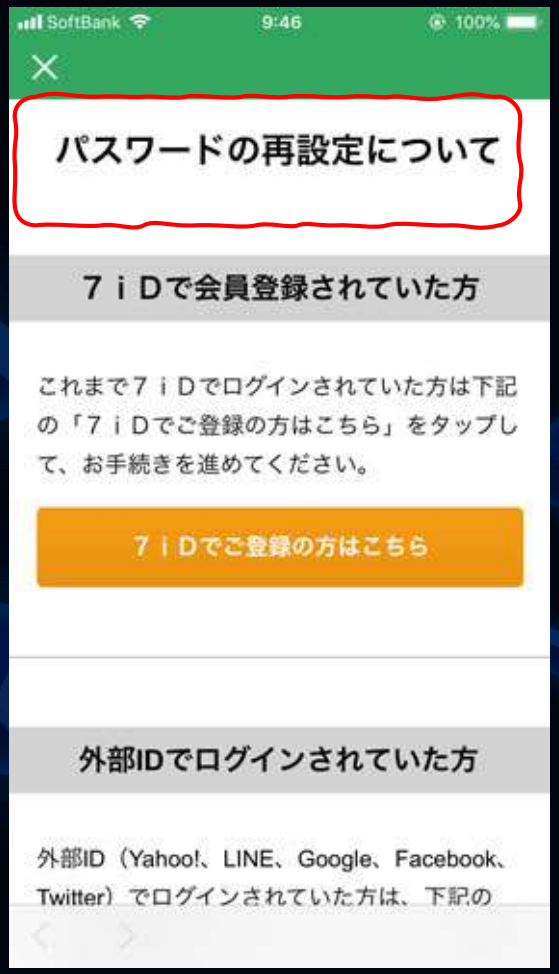
- ✓Damage 807 people / 38.6 million JPY (29th July 2019)
- ✓President's apology press conference on 4th July
- ✓The president was clearly unprepared for the press conference, and when asked by a reporter about two-factor authentication, he revealed that he did not know about it
- ✓7Pay lost a lot of trust and terminated the service

What's wrong with this case?

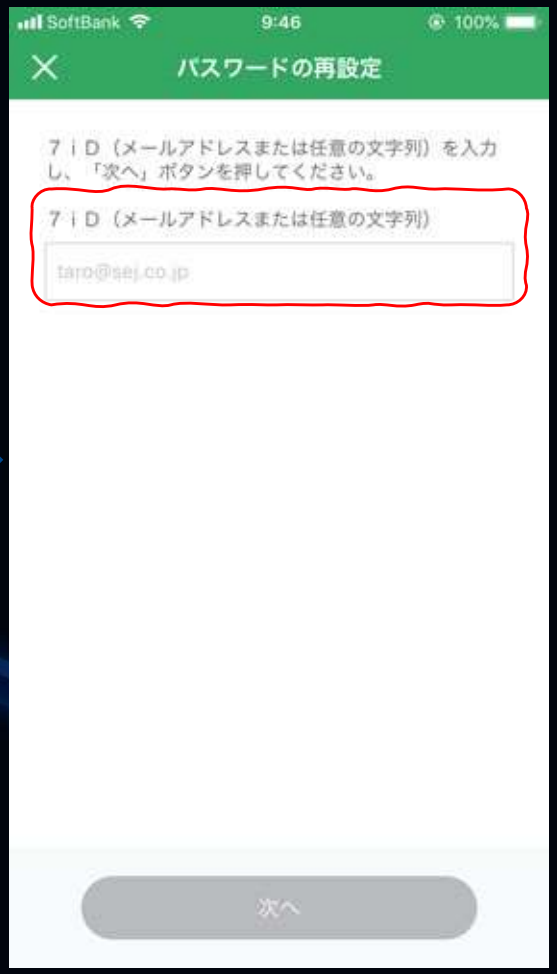
- ✓ Online shopping site for only inexpensive household goods, was not targeted with just an ID and password.
- ✓ 7Pay launched cashless payment system using the same authentication method as its site, and the next day a list-type attack occurred.
- ✓ They charged balance to their smartphone application from victim's credit card
- ✓ Withdrawer will make purchases at convenience with the charged balance
- ✓ They bought Cartons of cigarettes or e-cigarettes kits because that can easily exchange for cash
- ✓ They knew victim's ID (almost email address) and birthday. They could change the email address for reset (accounts without birthday were set default same birthday!! "1st Jan 2019")

What's wrong with this case?

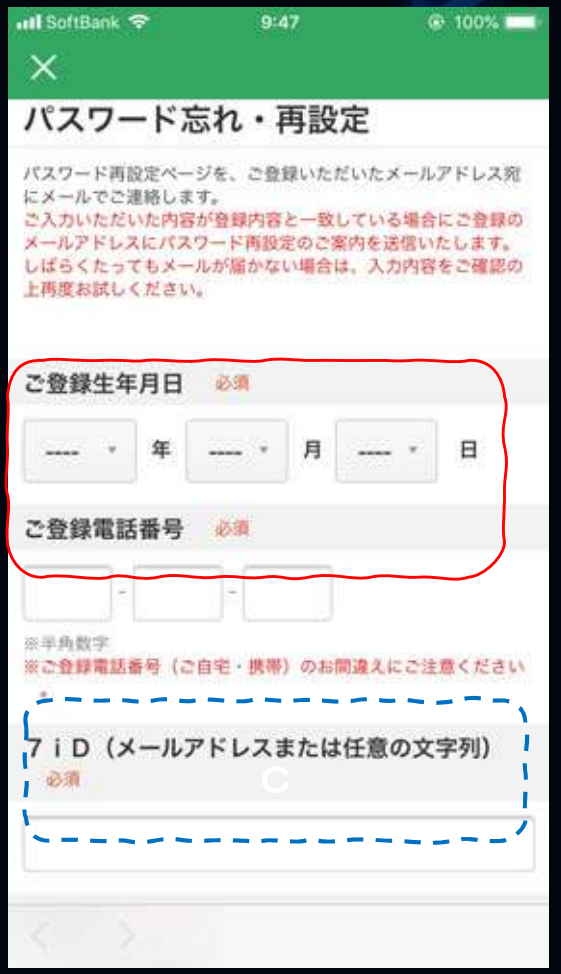
- ✓ The decisive factor was that the president held a press conference without understanding the cause of the problem
- ✓ After this incident, press conferences for major corporate scandals have been held with the president packing all the necessary knowledge in advance



Reset password



Enter the victim's email address



Enter birthday and phone number assed on the leaked list

Can enter the attacker's email address

The essential problem

Two major points

Headquarters failed to assess the risks of their services

- ✓ Only ID and password authentication was too weak for charging cashless payments
- ✓ The vulnerability Scan was done at the time of service launch. But hey could not determine if it was sufficient

Attackers were ready to go

- ✓ It is assumed that they had confirmed that the list-type attack was effective on 7-Eleven's shopping site even before the payment service was launched.
- ✓ Two days after the launch, even the role of buying cigarettes had been arranged, organized, and prepared by Attackers

6.docomo Account overview and problems

Overview of illegal money transfer at docomo Account

- ✓ Attackers took the account number, name, cash card PIN number, etc. (15th Sep 2020 Details not disclosed or unknown)
- ✓ He opened a fake docomo account in the same name as the target
- ✓ They use the target's bank account number and cash card PIN to charge the deposit to their fake docomo account
- ✓ In the 7Pay case, credit cards were used, but here, direct deposit is used
- ✓ They purchased large quantities of highly cashable electronic cigarettes and tablet devices at electronics stores

Overview of illegal money transfer at docomo Account

- ✓ Victims: 125 cases in 11 banks 28.42 million yen (27th Sep 2020)
- ✓ docomo stopped linking to bank accounts
- ✓ docomo continued the service only for accounts that subscribe to their smartphones.
- ✓ For members who have already registered their bank account but do not have a docomo's smartphone, service will be resumed by verifying their identity through eKYC or docomo Shop in face to face.(23rd Oct 2020)

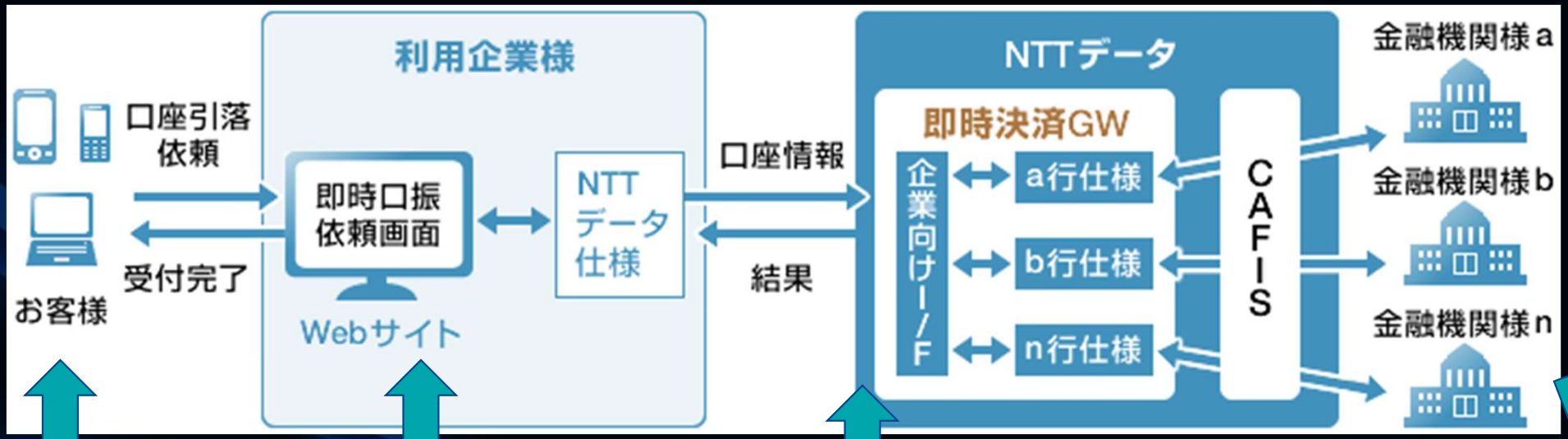
(eKYC : In Japan, the law requires a combination of facial recognition and IC reading of ID cards for online identity verification)

What's wrong with this case?

- ✓ docomo did not verify the identity sufficiently, so the Attackers were able to create fake accounts with just only email addresses
- ✓ As with Seven Pay, docomo focused on increasing the number of customers.
- ✓ If the service was only for smartphone subscribers, it was enough to verify their identity. But this failure made it easy for Attackers to create fake accounts only free e-mail address
- ✓ The direct debit system, which was designed to debit utility bills, was diverted to charge cashless payments for a different purpose.
- ✓ Direct deposit could be made using only the account number and PIN (or add date of birth)
  Few Banks adopted two-factor authentication
- ✓ In May, some attacks had already occurred at a major bank, and it had already terminated its partnership with docomo

What's wrong with this case?

- ✓ Even if the deposit balance was zero, it could be withdrawn as a loan
- ✓ Affected customers complained to banks, but banks did not listen to them
- ✓ docomo and banks couldn't figure out why, so they started blaming each other
- ✓ Even if the victim does not have docomo Account or docomo’s smartphone, the deposit was illegally withdrawn
- ✓ docomo has created a Covert Channel for withdrawing bank deposits



PC, smartphone

Site of docomo Account

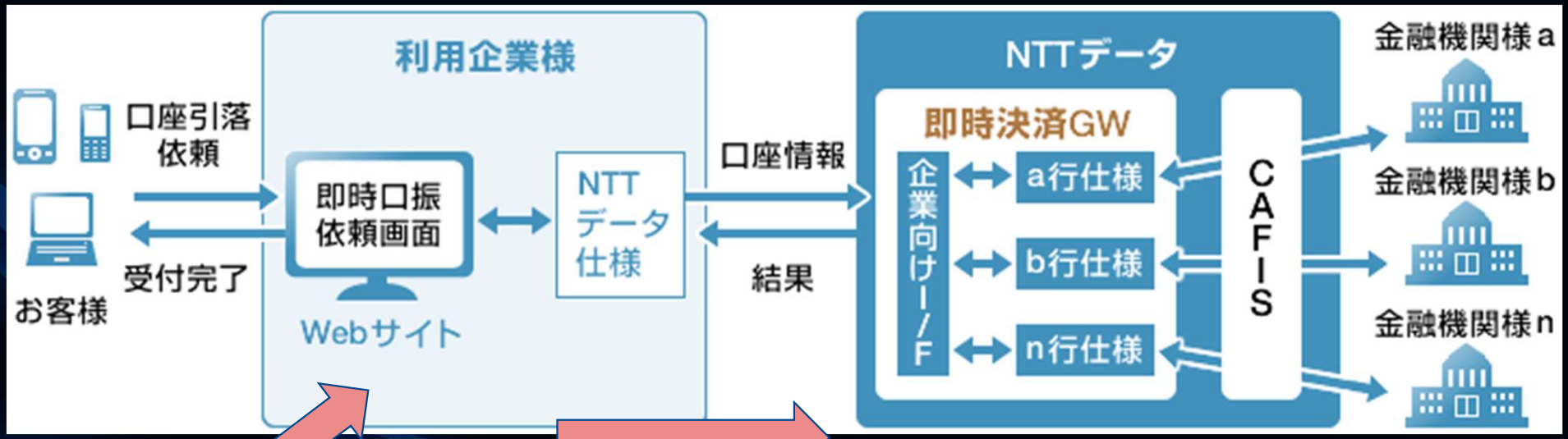
Service provider about Direct Deposit

Bank Account

authentication (Only ID and password)

Charge from Bank Account immediately

https://www.nttdata.com/jp/ja/lineup/gateway_service/



Link fake account to the Victim's account

Create fake Account at docomo account

authentication (Only ID and password)

Charge from Victim’s Bank Account immediately

https://www.nttdata.com/jp/ja/lineup/gateway_service/

NTT docomo

The essential problem

Two major points.

- ✓ Anyone could create an account with just an anonymous email address (docomo side)
- ✓ Direct deposit uses Insufficient authentication. Almost Banks thought it was safe if other banks adopted it (Bank side)

7.Japan Post Bank ,mijica overview and problems

JP BANK
ゆうちょ銀行

Overview of Japan Post Bank

- ✓ 380 peaple, 60 million JPY (22nd Sep 2020)
- ✓ Authentication is based on account number and PIN
- ✓ The handwriting on all five accounts in the identification documents is the same.
- ✓ two-thirds of them were treated as under investigation and not compensated

JP BANK ゆうちょ銀行

What's wrong with this case?

- ✓ The remittance function between members was abused
- ✓ The attacker was able to authenticate with an email address and password using list-type attack
- ✓ They could transfer money to a fictitious account with an account number and a four-digit PIN, four digits being easy to predict
- ✓ There’re countermeasures with account locks, but reverse dictionary attacks with fixed PINs are easily possible

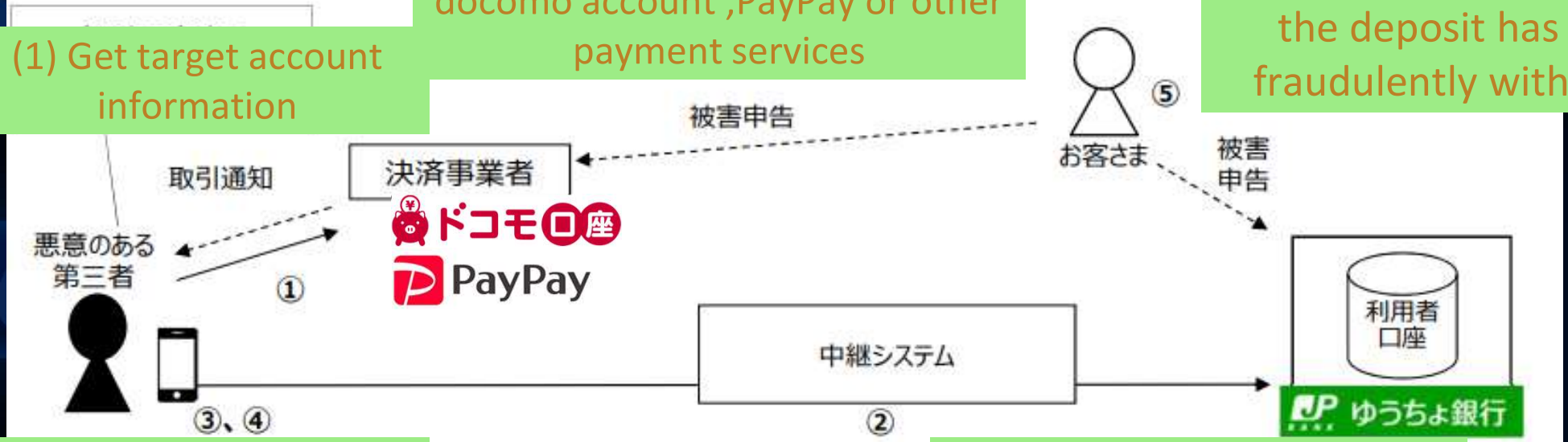
JP BANK ゆうちょ銀行

(Case 1) How to make unauthorized Direct deposit

(1) Pretending to be the target and registering as a member with docomo account ,PayPay or other payment services

(5)The victim realizes that the deposit has been fraudulently withdrawn

(1) Get target account information



(3) Guess PIN and charge target's deposit to docomo account, PayPay,etc

(4) They made purchases with QR codes and redeemed them

(2) Target's account number and docomo account, etc. will be linked

Overview of mijica

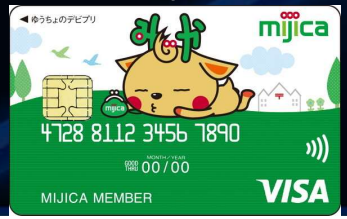
Case 2 : illegal money transfer

- ✓ The attackers were able to exploit the member-to-member transfer feature to transfer money to a fictitious account (54 peaple, 3.32 million yen)
- ✓ The five-digit PIN had no limit to the number of retries.

Case 3 : They obtained someone else's account information illegally, applied for mijica, and used it fraudulently on shopping sites before the card arrived at the account's registered address.

Case 4 : A lot of personal information was stolen due to illegal access

- ✓ 1,422 unauthorized logins (3rd Oct 2020)
- ✓ Japan Post Bank announces that it will end the service for 200,000 members （9th Nov 2020）



Case 2 : illegal money transfer

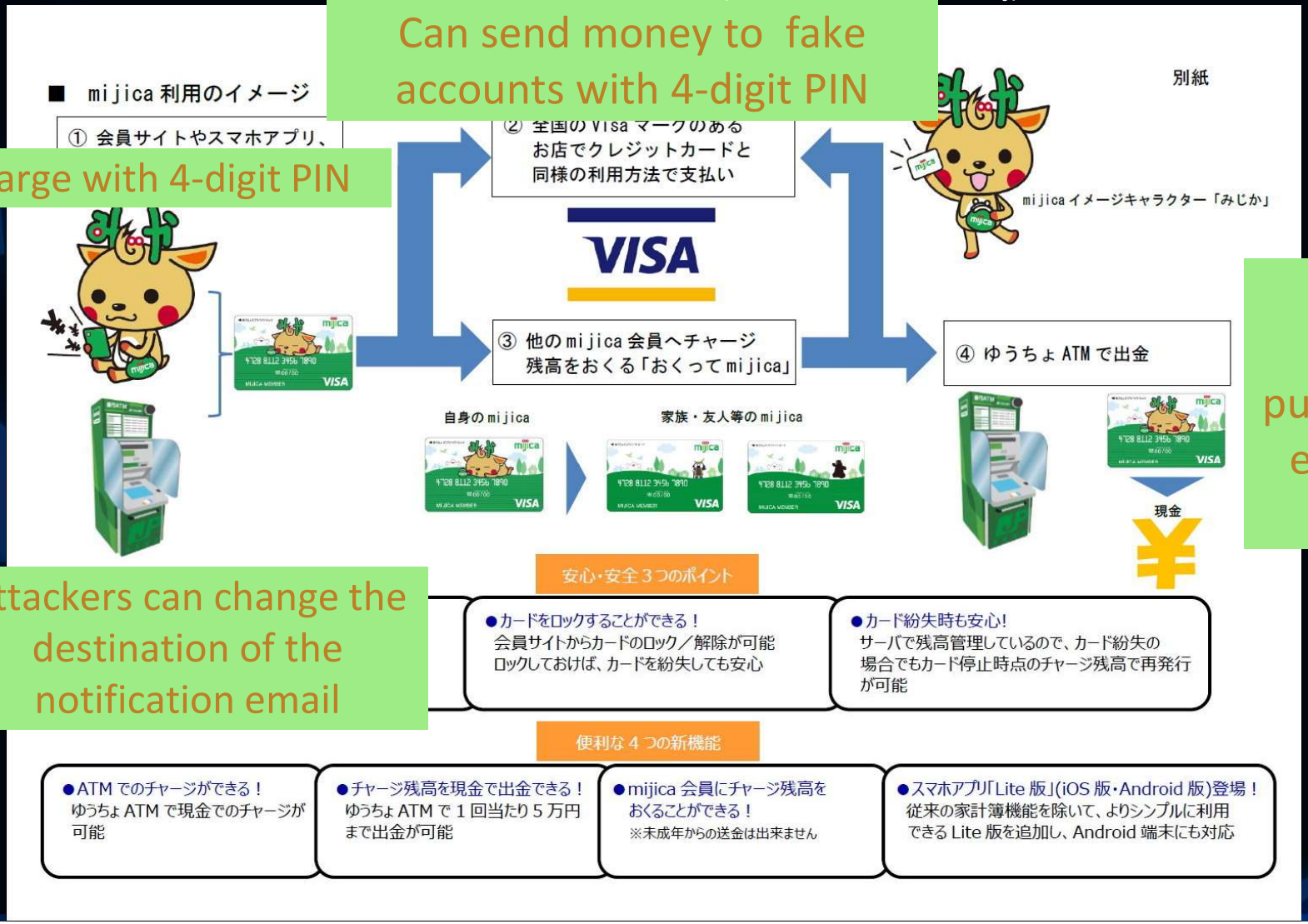
https://www.itmedia.co.jp/mobile/articles/2009/23/news109.html

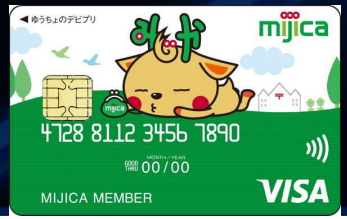
Can send money to fake accounts with 4-digit PIN

Charge with 4-digit PIN

Withdrawal at ATM
Attackers can make purchases with debit card even if they don't have Bank account

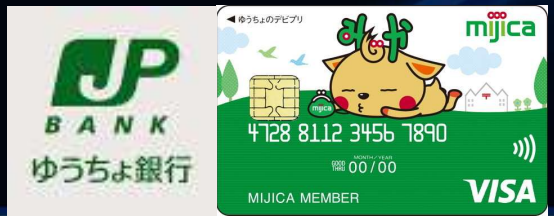
Attackers can change the destination of the notification email





The essential problem

- ✓ The illegal money transfer were detected in the system and reported to the executives, but they didn't read them.
- ✓ They knew about the illegal money transfer from the customer's complaint, but didn't say anything about it until the docomo account problem was made public



8. Significant similarities between the three incidents

Significant similarities between the three incidents

- ✓ All three have made two serious mistakes

	1st miss	2nd miss
7Pay	Password List Attack	Press Conference Reveals Lack of Management Awareness
docomo account	fake accounts Insufficient authentication	Recognizing the first incident but not acting on it
Japan Posta Bank,mijica	Insufficient authentication	The officer hadn't read the incidents report

- ✓ All of them had conducted penetration tests and other security assessments prior to the launch of the service
- ✓ Shopping site (7Pay) and services for mobile phone users (docomo) have different risks and different requirements from cashless payments
- ✓ Penetration testing should have been done again in a comprehensive way
- ✓ They should have recovered as fast as they could after the 1st miss

Significant similarities between the three incidents

- ✓ Allowing risk at cutover is not a wrong business decision
- ✓ Gaining market share = making money
- ✓ They figured that the risks found at cutover would not need to be addressed if there were no incidents for a while
- ✓ If yesterday was safe, today will be safe, and there will be going no incidents tomorrow
- ✓ They need to put people on the board who can judge the magnitude of the risk
- ✓ When asked if they are concerned about security or not, all of officers say yes. That's just a prelude
- ✓ Simply put, it's a natural response.The world-famous Japanese giant has failed to do so

The end of the three incidents

Once serious vulnerabilities were found, there's no time to take action

All three have been withdrawn

	Launch service	incident	service interruption	**end of service**
7Pay	1st July 2019	2nd July 2019	04th July 2019	**30th Sep 2019**
docomo account	April 2016 (Direct deposit)	May 2019 Aug 2020	04th Sep 2020 Stop bank account registration	**25th Oct 2021 Give up comprehensive services.**
Japan Posta Bank, Mijica	23rd Jan 2017	28th July 2020	16th Sep 2020	**03rd Oct 2020**

Comparison of the scale of damage caused by financial crime in Japan

- ✓ Fraudulent use of credit cards : 11.94 billion JPY (First half of 2020)
- ✓ Phishing at internet banking : 3,073 million JPY (Yearly maximum at 2015)
- ✓ 7Pay : 38.6 million JPY
- ✓ docomo accounts : 28.42 million JPY
- ✓ Japan Post Bank : 60 million JPY , mijica : 3.3 million JPY
- ✓ Because the problem became apparent early on, the amount of damage caused by financial crime was small
- ✓ It was inefficient as a crime because it required buying and reselling tablet devices and cigarettes
- ✓ The real risk of running a business is to lose credibility and stop service

9. What we can learn from these incidents

(1) Identity authentication on the Internet

- ✓ Never use only the information you enter on the keyboard to verify your identity
- ✓ Verify the authentication process all the way through to the point of collaboration

(2) Limit and monitor the use of the charged balance

- ✓ The types of cashable goods are limited (e.g. e-cigarettes, Tablet)
- ✓ We have already been able to detect fraudulent use of credit cards. Cashless payment can be detected in the same way

(3) Officers need to listen to their subordinates who say home truth

- ✓ The first time, there may be many circumstances, and risks may be tolerated in order to speed up the cutover
- ✓ The second failure is entirely the responsibility of officers
- ✓ Officers tend to see only the risks that hinder their career advancement
- ✓ They’re not management risk
  They’re risk that could hurt career to become officer

Finally

- ✓ Japan's giant companies had made several major mistakes in cashless payment.
- ✓ In all cases, the second miss are fatal
- ✓ I want to let people know about this Japanese mistakes, and cashless payment services in any other country in the world must not make the same 2nd misses

Thanks so much for taking the time to join today

Now I'll try to answer any questions you may have