# クレジット／電子マネー決済における暗号化の潮流とHSMを活用した暗号鍵管理の事例

2016年11月22日

株式会社フライトシステムコンサルティング
FLIGHT SYSTEM CONSULTING Inc.

# 1. 店舗決済スタイルの変化

- バックヤードに持って行かずに、
  顧客の目の前で決済することが時代の潮流。
- そのためには、出先での決済に用いられてきたモバイル決済を店舗でも導入することが効果的。
- タブレットやスマートフォンなどのスマートデバイスを活用したモバイル決済を店舗内で活用するケースが増えてきている。

# 2. 決済手段の多様化

## クレジットカード

磁気カード　　接触EMV　　コンタクトレスEMV



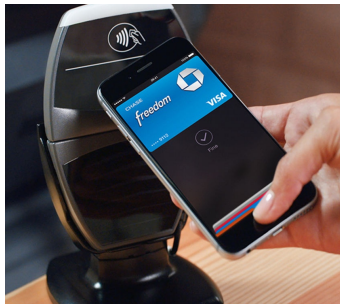

## 日本独自の電子マネー

Suica　QUICPay

nanaco　iD　楽天Edy　WAON

## 決済の多様化

## Apple Pay



## Alipay / WeChatPay

# 3. 複数決済センター接続のニーズ

- 多様化する決済の全てを1ヶ所の決済センターで担うのは困難。
- よって決済端末／決済アプリは、複数の決済センターに接続することが必須。

**<当社での複数決済センター事例>**

# 4. 複数の決済センターへ接続するための暗号鍵管理

- 決済センター毎に暗号鍵は異なる。
- 決済するカードによっては暗号鍵が必要になる。
  例：電子マネー「iD」では上限金額を超えると暗証番号が必要

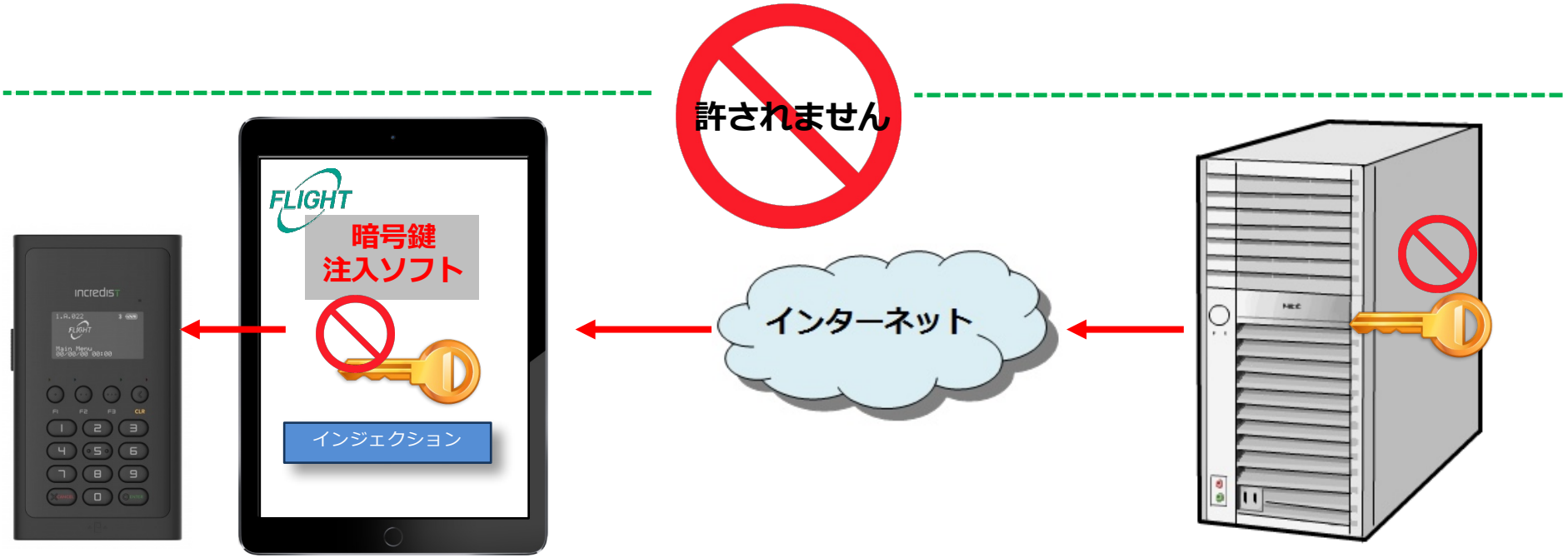
- 1台の決済装置で複数の暗号鍵を保有。
- 複数の暗号鍵を切替える機能。

- 「Incredist」及び「Incredist Premium」では、**最大15種類の暗号鍵**をセットして切り替えて使うことができる。

特許取得

# 5. 暗号鍵のリモート配信

- 決済手段の多様化に伴い、使い始めた決済装置に対して後から新しい決済手段の契約が追加されるケースが増え、そのために暗号鍵を配信したいというニーズが高くなって来ている。
- しかし暗号鍵はクレジットカードにおける業界団体PCIにて管理手法が厳格に定義されており、安易に配信することはできない。
- 例えば、単純にサーバのストレージに暗号鍵を置いておき、それを決済端末に配信するとか、ローカルのPCやiPadに暗号鍵を置いておき注入するなどはNG。



# 5. 暗号鍵のリモート配信

- 悪意のあるホストから偽の暗号鍵を注入されないため、暗号鍵の配信・注入に関して以下の国際的な規定が存在する。

  ・ANSI X9.24-1:2009 Retail Financial Services Symmetric Key Management
  ・ANSI X9 TR-31 2010 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

- 上記規定のフローに従って暗号鍵は配信し注入しないとならない。
- これらの規定により、鍵を配信する側（センター）、受け取る側（決済端末）相互に、相手を認証することなどが必須となっている。

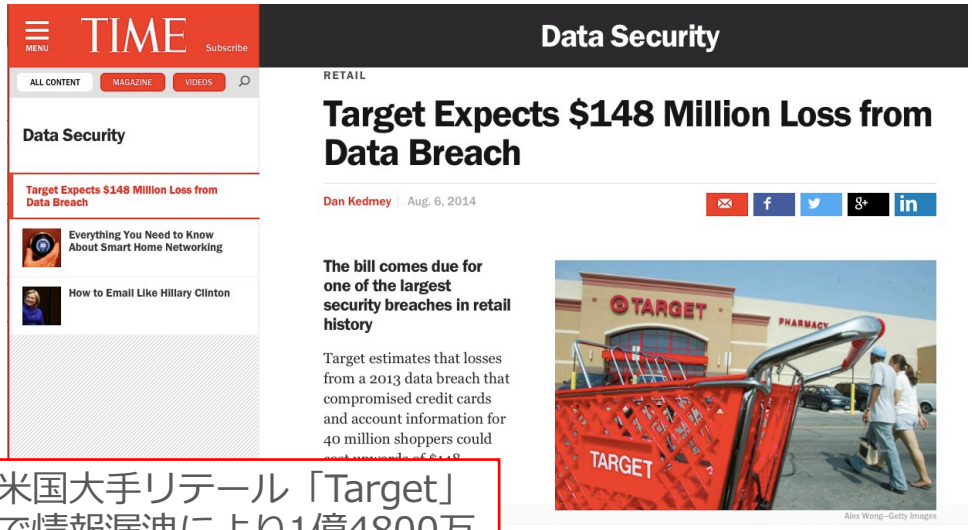
# 6. なぜそこまでナーバスになるのか？

- 全世界で毎年1兆円以上ものクレジットカードの不正利用があるから。

ペイメントカード不正のグローバルコストの推移（2009年～2013年）

| | アメリカ | その他 | 合計 |
|---|---|---|---|
| 2009年 | 32億ドル | 37億ドル | 69億ドル |
| 2010年 | 36億ドル | 40億ドル | 76億ドル |
| 2011年 | 48億ドル | 54億ドル | 102億ドル |
| 2012年 | 55億ドル | 62億ドル | 117億ドル |
| 2013年 | 71億ドル | 68億ドル | 139億ドル |

出典 ： ニルソンレポート、BI Intelligence



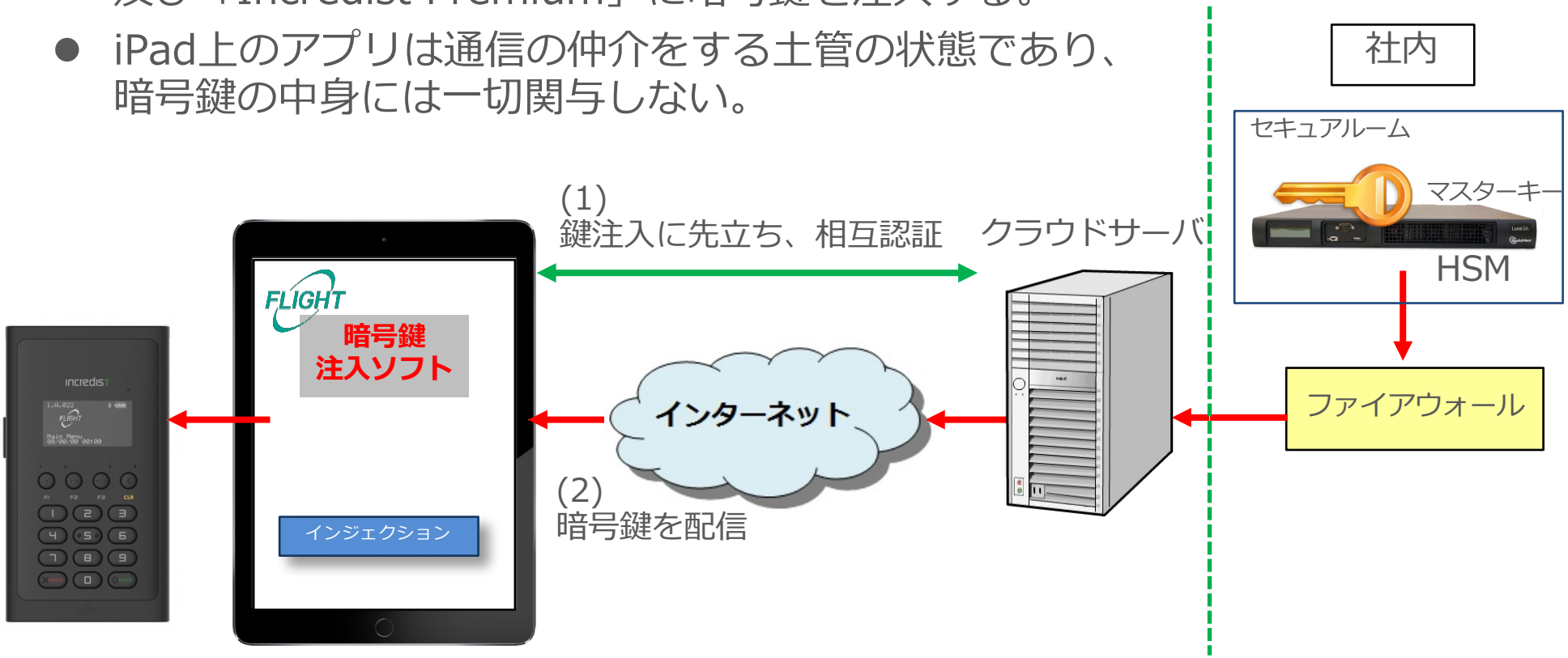

米国大手リテール「Target」で情報漏洩により1億4800万ドル（約180億円）のコスト負担予想

# 7. HSMの活用

- 欧米では暗号鍵の保管にHSMと呼ばれる耐タンパー機能の付いた暗号鍵保管システムを活用することが一般的になっている。
- ANSI X9.24並びにANSI X9 TR-31に規定された暗号鍵のマスターキーはHSMに保存すべきものである。
- 当社では、セーフネットのLunaシリーズを活用している。

# 8. HSMを活用した暗号鍵管理

- 当社の決済装置「Incredist II」、及び「Incredist Premium」に対して後から暗号鍵を変更したり追加するために、当社ではASPサービスを提供している。
- 構成は以下の通り、iPad上にキーインジェクションのアプリケーションを用意し、HSMからクラウド上のサーバを経由し、iPadを通じて「Incredist II」、及び「Incredist Premium」に暗号鍵を注入する。
- iPad上のアプリは通信の仲介をする土管の状態であり、暗号鍵の中身には一切関与しない。



# 9. 最後に

- 金融ハッカーが世界的に蔓延っており、HSM及びANSIの規定を基本とした暗号鍵の管理、運営、配信が必須な時代となりました。
- ぜひ正しい運用で事故のない決済市場を皆さんと一緒に創って行けたらと考えております。