

1. システム概要

本ドキュメントは、私が住居侵入対策を目的として開発した、玄関ドアに設置する電子鍵のシステムについての、開発動機から反省点までを記載した概要書です。1～2日ぐらいでドラクエしながら猛ダッシュで書いたので、かなりアバウトな内容ある事をご容赦ください。

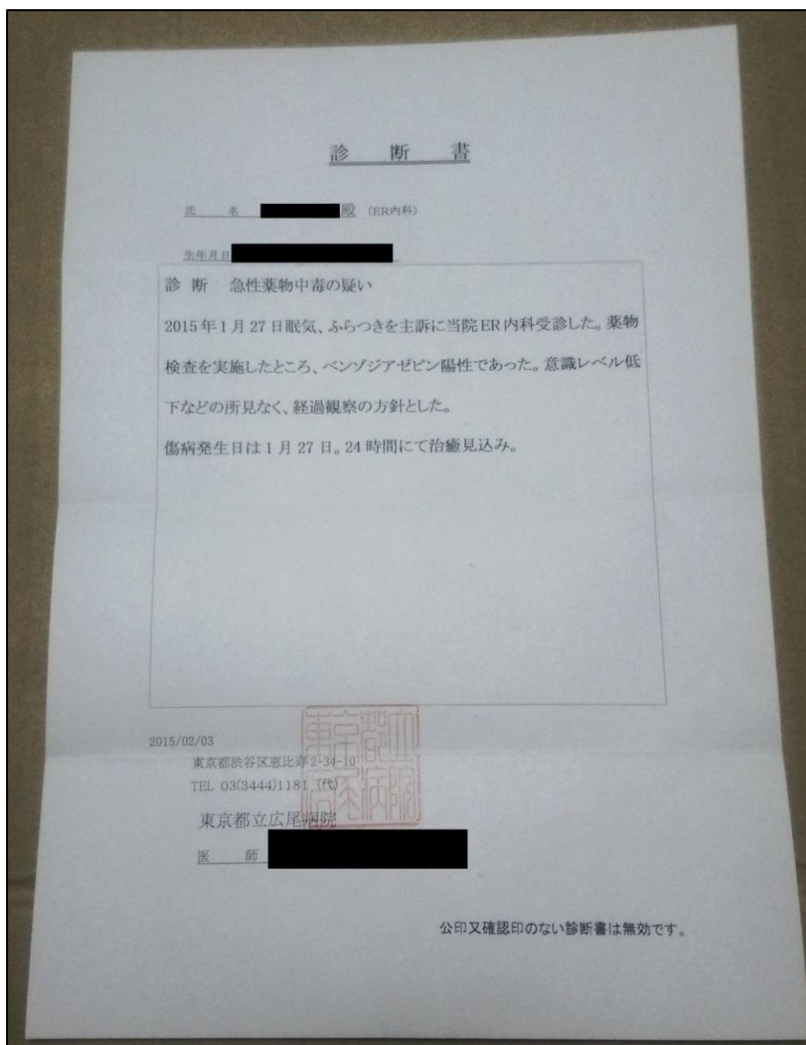
2. 開発理由

開発の理由はシンプルで、私や家族は長年のわたり住居侵入等やつきまとい等の被害に悩まされてきており近年その被害がエスカレートしたからです。

少し長文になりますが、この被害は世間の一部では「集団ストーカー」と呼ばれている悪質な犯罪でありまったくのデマ話と共に都市伝説の様に流布されている犯罪です。

そもそも犯行自体を隠蔽する目的で、オカルトの話の類として印象付ける為にデマと共に語られていますが個々の犯行は現実的で、実在している悪質な犯罪被害になります。

「証拠を見せろ」と言う話になると思いますが、例えば次の写真は証拠の一つです。



写真解説

職場において体調不良になり
定時後に病院に直行して
検査した結果の診断書

薬物の検出と共に
「急性薬物中毒」と書かれており
犯人共にとっては不都合である様子

これは東京都の広尾にある都立広尾病院において作成して頂いた診断書になります。検出された「ベンゾジアゼピン」と言うのは、睡眠薬や精神安定剤や濫用薬物として扱われている薬でありつまりこの写真は、私を検査した結果としてその薬物が検出された際の診断書を撮影した物になります。

当然、私にこれが処方されていた事実はなく、また私が入手して飲んだ事実ありません。これは状況から言うと、私の当時の職場において、私の離席中にデスクに置いておいたコーヒーにこの薬物が混入されたと言う、周囲に居た人々によるものと思われる組織的な犯罪被害の証拠と言う事になります。

問題はこの薬物が混入された状況にあります。

当時私はメガバンクの大規模なシステム開発の現場に出入りしており、世界的に有名なIT企業の名を借りて仕事をしていたのですが、ここに入出入りする様になって間も無くから被害が始まり

私物のブリーフケースを物色されたり、自宅等へ住居侵入して知りえたと思われる噂話をする不審者達を見掛けるようになる等、気持ちの悪い目に遭わされていた訳です。

当時私は、それまで職場において被害に遭う事は少なかった事から突然被害が頻発する様になった状況に驚き、警察等に相談していた訳です。

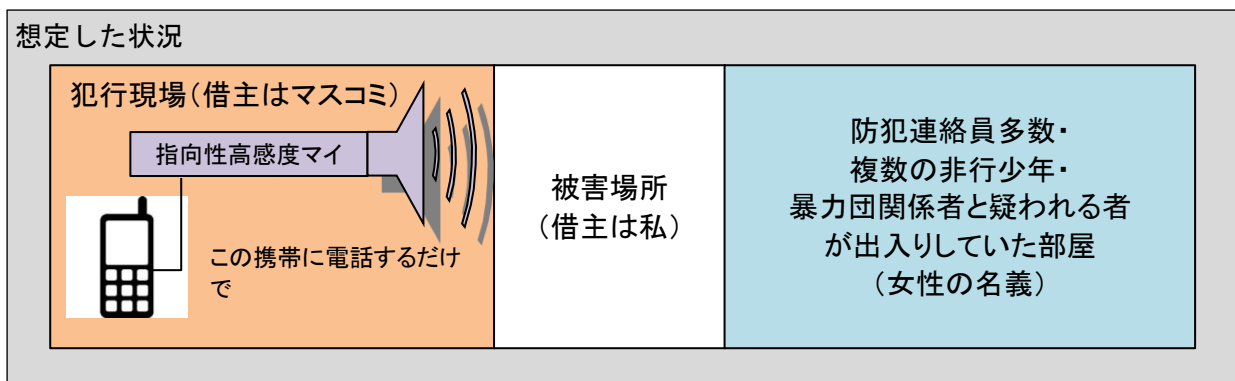
警察も含めた政府関係も、ある種の共謀関係があると知っていたけれど・・・

何故私がそんな事を知っていたのか？

それは・・・長年私や家族に付きまどってきた連中にはマスコミが含まれており自宅などが盗聴されてきており、彼らがそれによって得た情報を、番組の出演者である政財界の連中等と共有してきた事実があるからです。

例えば、2009年頃、私は自宅がマスコミから長年盗聴され続けておりそれによって得た情報を、テレビ番組のネタ等に利用されている状況が確実に存在していました。状況から想定していた盗聴の手口は、被害場所の隣室を借り上げて盗聴器を設置し携帯電話に接続し、遠隔から盗聴するという手法です。

つまりこんな感じ



通常この手の想像をする人は精神病だとされるので、私は探偵さんに調べて貰い事実の裏付けを取得しました。

結果は驚く程にハッキリと得られ、隣室の借主は想像通り私や家族の私生活を覗き見て番組のネタにしてきた番組制作会社の社員名義だったわけです。

私が何度となく社会問題の背景があり、マスコミとして誠実な対応を求めて来たのにそれを拒否して来ながら犯行をエスカレートさせてきたので、制作会社については明記させていただくと次の企業になります。

企業名:株式会社 ビー・ブ레인
URL: <http://beebrain.co.jp/>

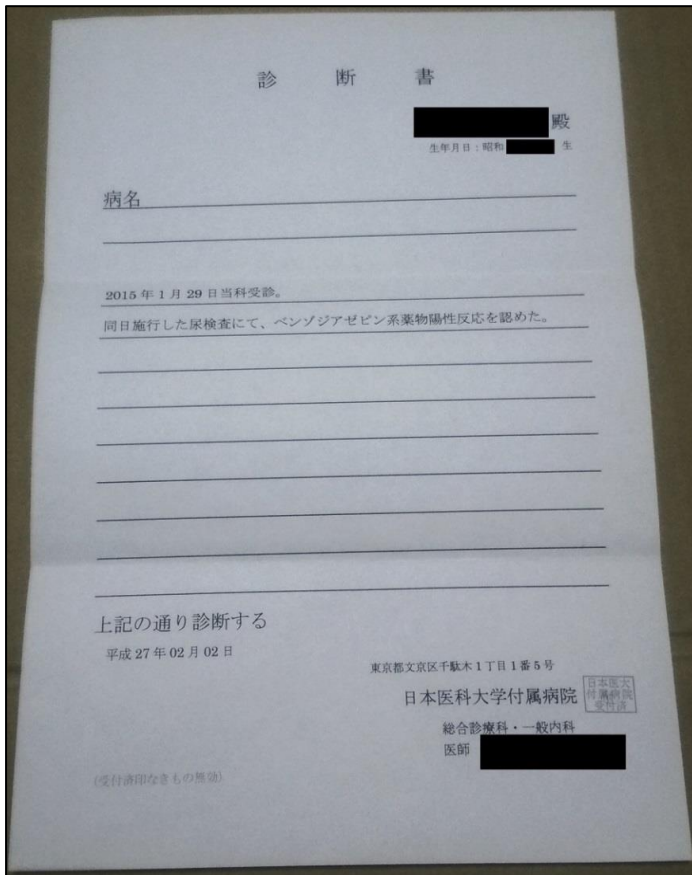
如何言う企業なのかは自分で確認してください。

しかも即座に逃走する必要性から、携帯電話を使用しているものと思い機器にて計測してみると、ドコモのFOMA携帯の通話状態の電波が18時間連続で発信されていました。

その他にも長年色々と被害に遭ってきており、その都度やれ宇宙人が如何のとか、超能力が如何のとか色々な物事に揶揄されて番組のネタにされてきており

まだ冷戦だった頃から、「米ソの活発なスパイ活動、これだから漏えいしないんだ」と思っていました。

ですので、その後も調査や検査を繰り返してきた結果として



ここ数年の薬物被害が疑われた場所はシステム関係、特にIT企業の職場ばかり・・・

※企業活動との関係は不明です！

- ・自宅
- ・実家
- ・ソフトバンクモバイルの開発拠点
- ・ワークスアプリケーションズの開発拠点
- ・日本IBMの開発拠点
- ・富士通システムズ・ウエストの開発拠点
- ・SCSKの開発拠点

疑われる被害の手口

- ・飲食物への薬物の混入(診断書の通りです。)
- ・住居侵入(三日連続不正開錠されました。)
- ・盗聴・盗撮(嫌がらせ電話で誇示されたりします。)
- ・自宅無線LAN等の監視
- ・私物のブリーフケース等の物色
- ・自宅PCのスパイウェアによる監視

※いずれも不審者達が噂話している内容と

と言う具合に、その他にも色々と判明したりしてきたので、方々に相談してきました。当然、警察にも相談してきたのですが、警察に盗聴器を納入していた業者さんから話を聞くと警察も盗聴しているので、取り締まりには乗り気では無い様ですし前述の通り、実際に隣室に出入りしている不審者には、地域の防犯連絡員も多数おり直接どんな関係なのかと警察署にて質問しても、まったく話をはぐらかされる

一部の防犯連絡員については個人名等を特定しているので、それが所属している防犯協会の連絡先を問いただしたのですが、防犯協会の連絡先すら教えない警察署に電話し、拒否する法的根拠は何かと尋ねると

「法的根拠わぁ！、法的根拠はありませ～ん ガチャ」

私も

「秘密法わぁ！、秘密法は守る義務はありませ～ん」

と言いたい気分をぐっと我慢し、対応策を考えた結果が今回のシステム開発です。

3. 対応の方針

痕跡はあるものの、何だか分からない得体の知れない人々への対抗策なのでその方法は推測の域を出ず、その上での要求仕様の策定となります。危機管理とはその様なものであり、確実な危機管理等を言うものは信じてはならない訳です。

仕様を検討していた当時、大凡判断材料になりそうだった出来事は

- (1)住居侵入等の犯行の意図は強く、遭遇する不審者共は良く噂話をして見せて誇示してみせる
- (2)ディンプル鍵等のピッキング対策されている鍵でも、器用に二つ一度に開錠したりしてくる
- (3)赤外線方式の電子鍵であっても、物理的に壊そうとする一方で、暫くするときちんと開錠してくる
- (4)室内にICレコーダーを置いて録音してみても、侵入者は器用にそれを見つけた上で録音データを削除してから逃走していったりする
- (5)ストーカー調査等で探偵に依頼していた内容や、私が撮影した不審者の写真等に興味がある様でPCの中身を覗き見している様子があり、不審者に遭遇すると噂話をしている様子がある
同様にVeraCryptでPCのドライブ自体を暗号化しても覗き見して来ている様子があり遠隔でPCをウイルス感染させてきている可能性を感じる
- (6)役所や医療機関にも話が通じる様で、法に抵触する様な嘘を吐かれたりする
検査の直前に、病院の最寄り駅にて尿検査した結果、かなりクッキリと薬物の陽性反応が出た場合でも病院で検査すると陰性反応と言われ、その上で診断書の作成が出来ない旨を主張される
直前に私服警官二名と思われる者達が来て医師と話をしていた事から、かなり怪しい
少なくとも診断書は医師法において作成を拒否は出来ない物とされており
単に虚偽だと言うだけでは無く、法に抵触する様な嘘を吐かれる事がある
- (7)私書箱等を使ってやりとりしても、届いたものを取り出した時だけ尾行者がついてきたりとハッキリと警察の関与が疑われる一方で、嫌がらせの電話をしてきてそれを録音される等犯行を誇示する割には、注意していると痕跡を残したりする 結構アホな連中だ
- (8)想像以上に沢山居る、一度に数名に遭遇は日常的、外国人等も混じっていて
同じ日に同じ不審者を複数回見掛けたりする事もあり、距離を取って囲い込んで尾行してくる等手法が玄人な感じ
- (9)当然の事ながら卑劣だ、不審者達は噂話が大好きで、遭遇すると仄めかすのを我慢できない
時にエロイ話等で盛り上がり、ニヤニヤしていて分かり易い
テレビの出演者がよく分からない理由でニヤニヤしている時が有るのも、そんな理由だと思う
また犯行を揶揄して会話して見せる事を止める事が出来ない
「株式会社グルー」と言う番組制作会社の社員を名乗る不審者に遭遇した事があるが
一部の犯人たちは、特に20代の連中は本当にミニオンズみたいな軽いノリで犯行を繰り返している。
- (10)メガバンクのネットバンキングシステムの開発現場にすら現れたりする
アカウント管理機能を開発している様な場所にも出現し、技術水準としては正に玄人であり想像以上にハイスペック

つまり想定される相手は、そこそこハイスペック変態集団と言う事であり、超変態集団なのにハイスペックです。
~~さすがメーカーも共謀していそうな変態集団と言う事になります。~~元マイクロソフト社員の戸崎さんの言う通りだから
よって、ここまで来てもエキセントリック変態集団すぎて何が有効か不明なので、基本に忠実に対応を考え
最初の対応方針として自宅への侵入対策を決めました。

特に鍵を開錠される事が頻発する様になったので、玄関ドアへの対策をする事にしました訳です。

つまり鍵の開発をしようと思った訳です。

4. 開発の目標、要求仕様

ここまで色々と記載してきたとおり、相手はハイスペック変態集団なので、技術に詳しいのは明白であり当然、少なくともピッキング対策された鍵程度は余裕で開錠してきます。

更に三日連続で開錠されていて、警察に通報しても誤魔化され、事件性が無いとか言う

「ちょっとこの人には精神医療が必要なんじゃないの？」

と言う様な話をされる事から、マスコミ以外にも公安警察や公安調査庁等の関与がかなり疑われ相応なセキュリティレベルの実現が必要となります。

高いセキュリティレベルが必要とされる一方で、個人的に可能な範囲で対処しないといけない事からハイスペックでありながらシンプルな対応が必要となり、結果として電子鍵を開発する際の仕様として次の要件を満たす事を目標としました。

(1)定型の鍵や固定されたパスワードではない方式の実現

ディンプル鍵や赤外線リモコン鍵は帰宅すると開錠されていたので、特定の形状やシグナルの鍵は開錠される前提で開発する必要がある。

よって、開錠の都度違うパスワードになる等の方法を実現は必須となります。

(2)壊されにくい形状の実現

被害について法務局に相談に行った事があり、帰ってくると数ヵ月前に設置した電子鍵を壊そうとした痕跡がこのっていた事があります。

警察は勝手に壊れただのと寝言と言っていたので、永久にお休みなさいして貰いたいのを期待しません。

この為、ドアの外部に露出している箇所等有ると、破壊してくるのは明白なので

その様な事を考慮した物を開発する必要があります。

(3)不正開錠の検知機能の実現

相手が相手なので、努力して鍵を設置しても破壊や不正開錠される可能性が十分にあります。

この為、その様に不正開錠の痕跡が残る事が望ましい訳です。

(4)高い復旧性の実現

不正開錠されたりした場合でも、元のセキュリティ水準に復旧出来る事を考慮した仕組みを実現する必要があります。

電子鍵のパスワードが盗まれる等しても、再度別のパスワードを振りなおす事でセキュリティ水準を復旧する必要があります。

長期戦も覚悟する必要があり、当然一度や二度の不正開錠でセキュリティ水準が破綻する様では、殆ど役に立ちません。

(5)調達容易性の実現

健全な市民生活は、自分個人の安全だけでは実現する事はありません。

また自分個人だけ幸せな生活をし、他の人々は苦痛に満ちた生活をしていると言う状況の実現可能性は低く、現実感の無い期待だと思われます。

多くの人々にとっても、私と同様にやれば多少なりとも状況が改善出来る様な

そんなシステムの実現は、社会的にも個人的にも有益な事だと私は思っています。

よって今回は、一般的に流通している物でシステムの開発を行う方針に決めました。

ソフト・ハード共に比較的普及している技術を使い、多少知識がある人であれば

努力して真似すれば同様の物が出来る、そんなシステムの開発を目指しました。

スパイ活動全般に言える事ですが、犯行を繰り返す努力が嫌いな卑劣な人々でさえ

真似すれば有益だからこそスパイ活動をする訳です。

超難解で一部の人にはしか有益できない情報なんて、盗んでもしょうがないのです。

日頃のテストにパスする為に、ハーバードや東大の学長をカンニングする必要は無いのですから

(6)汎用性の実現

ドア等の特定の場所だけ狙ってくれるテロ組織は無いものです。
当然、今後も我々が生活していく上で、同様の被害が各所で発生するのは明白です。
よって今回は、鍵自体のみならずその構成要素や技術も含めて、今後に応用が利くシステム開発を目標設定に取り入れました。

5. 実現方法

必要となる要件を踏まえて、その実現の可否や方式を検討し、とりあえず個別の要件について次の様に開発目標を設定し、順次更新しながら開発を進めました。

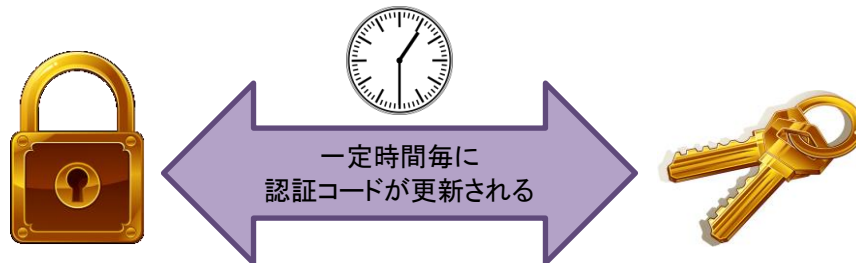
(1)定型の鍵や固定されたパスワードではない方式の実現

通信の規約を検討し、無線通信について次の方式の実現を目指しました。

※実際の方法は少し複雑なので、別紙にまとめました。

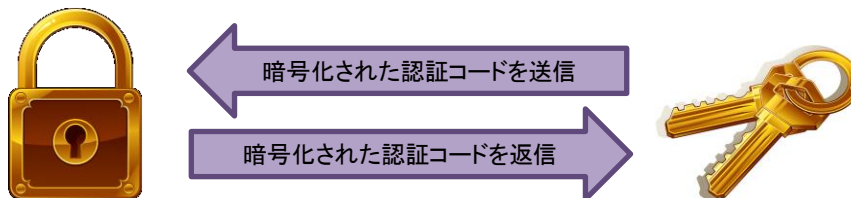
a)ワンタイムパスワードの実現

同一の認証情報を送信する場合でも、一定時間毎に送信データの暗号化キーが更新される方式を実現
無線通信を傍受した上で、認証情報を再送する方法による不正開錠が行えない様にする。



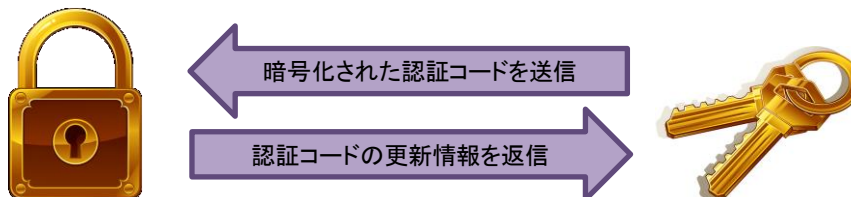
b)相互認証方式の実現

鍵と錠前の中で、相互に検証可能な認証情報を送りあう事によって、相互に認証が出来る様にする。



c)フローティングキー方式の実現

無線データ通信による認証が成功した際に、認証キーの更新データを返信する事で
認証成功の度に、認証情報が更新される様にする。
同様に、通信データの暗号化キーについても認証成功時に更新する事で
通信データを傍受されても、容易に解読されない様にする。



(2)壊されにくい形状の実現

破損に強い事が必要なので、ドアの外側に露出部分が無い、無線リモコン式の鍵として開発する事で、要件を満たす事に決めました。

(3)不正開錠の検知機能の実現

破壊や不正開錠等が予期されるので、その様な攻撃に対する検知機能を実現する事で目標を達成する事にしました。
具体的には不正な開錠や開放の検知、人の接近の検知を、センサー機能の導入となります。

(4)高い復旧性の実現

物理的な破壊や認証情報の窃取等により、鍵が機能不全にされる事が予期されるのでその様な事態を想定して、その様な事態に陥っても鍵機能の復旧が可能な仕組みを実現する事にしました。
具体的には次の機能を実現し、認証情報が窃取された場合にもセキュリティ水準が復旧出来る様にしました。

- a)複数の認証(鍵)情報の管理機能
- b)認証情報の付け替え機能(外部メモリ化)
- c)認証情報の更新機能

また、物理的な破壊については一般に流通している部品を使用して開発しドア外に露出部分の無い仕組みにする事によって、破壊される箇所を限定しそれが破損しても、代替可能にすることを実現しました。

(5)調達容易性の実現

これは一般に流通している電子部品等を使用する事で実現しました。
更に電子鍵なので、ある程度構造が複雑になってしまう事が予期されたので出来る限りシンプルな構造を実現する事で、調達容易性を向上を目指しました。

(6)汎用性の実現

ハードウェア・ソフトウェアに分けて検討し、次の様に汎用性の確保をする事にしました。

a)ハードウェア

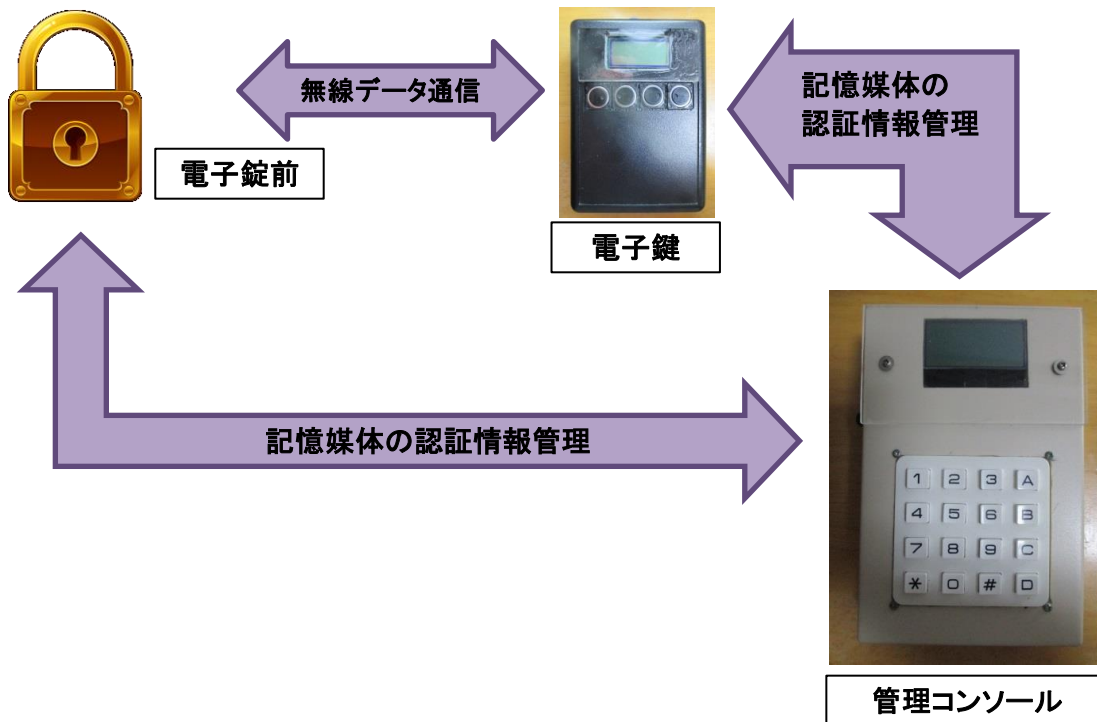
- ・デジタル電子工作で使われる基本的な手法の習得を通じたノウハウの確保
- ・一般的に流通しているモジュールを採用する事による、モジュール単位での流用性を確保

b)ソフトウェア

- ・認証方式等の通信プロトコルの策定による、他デバイスへの応用性を確保
- ・ソフトウェアのライブラリ化によって、他デバイス開発への応用性を確保
- ・ソフトウェアのオープンソース化により、技術面に詳しい他の被害者の参考資料化

6. システム構成

以上を踏まえてシステム構成を考え、次の様なシステム構成にする事にしました。
ハードウェアは鍵・錠前・管理コンソールの三点です。



情報処理をする為のマイコンと無線通信モジュールについては、最近のIOTの話題に付随して話題になっていた、東京コスモスが販売している「TWE-LITE」と言う製品を使用して開発をする事に決めました。インターネットへの直接接続は無いものの、物同士の無線通信についてはこれで実現可能です。

詳細はメーカーさんのサイトをご覧ください。

<https://mono-wireless.com/jp/index.html>

このマイコン、入出力インターフェースとしては、I2Cと言う規格が使えると表記されていたのでこれを採用して外部のRTC(時計の電子部品です)や記憶媒体と接続

LCD: ST7032Iを使用した16×2のLCDを使用

RTC: DS3231

EEPROM: 24LC256

暗号化については、製品が共通鍵暗号として128bitのAES暗号をサポートしているとの事ですが今回、通信方式を検討した結果として、AESよりもハッシュ関数が必要である事からこれは自作のライブラリで実現

メモリが32KBと少なく、メーカーに問い合わせしたところメーカー提供のソフトウェア等もメモリを使用するので、実際に使用できるのは18KBとの話だったのですがまあ、「初めてのデジタル電子工作」(初めてなんです。)なので、読み切れない事は多いのですが着手しないと何も始まらないので、開発に着手しました。

7. 開発の実行

多少知識はあるものの、デジタルデバイスのハードウェア開発に関しては初めてだったので何の見通しも立てられない事から、要素ごとにプロトタイピングを繰り返す事だけを決め開発に着手しました。

実際、ここまで記載した方針は当初から決めていたものばかりではなく、様々な要素を様々なマイコン等で検証した結果です。

例えば次の様な感じで

- ・FlashAir→簡単だが出来る事が限られており、処理能力も貧弱
- ・Arduino→簡単だが、大きい割にメインメモリ少なく(2KB程度)、処理能力不足
- ・Attiny→開発環境の構築に躓き、メインメモリ少なく、I2C使用のサンプルを実装してみると不安定
- ・MSP430→開発環境構築に躓き、参考情報も少なく、ライトプロテクト等の機能の使用方法不明

実際にトライアル的に色々と試しました。

その結果として「TWE-LITE」で開発する事にした訳ですが、この「TWE-LITE」についても実際に開発に着手してみると、様々な問題が発生しました。

結果として何とか誤魔化しながら開発はした訳ですが、色々と問題もあり率直に書くと

(1)主メモリが足りない

メーカー提供のデフォルト設定では、本システムの実現は不能
メーカーに問い合わせをし、使用可能なメモリサイズ(ヒープ領域)の設定方法を聞いて解決

(2)I2Cインターフェースがとても不安定

メーカーサイトを参照しても、数バイト程度のデータのやり取りを想定している旨が記載されており
今回のシステムで必要となる、時に数百バイトを超えるデータのやり取りには耐えられない
やむなく試行錯誤した上で、基本的なI2Cインターフェースの機能をラッピング化し
誤魔化しながらシステム開発を進める
この問題により、結果として開発工数が3倍近くになっており、大変に問題を感じる

CPUの部分はオランダのNXP社の製品の様なので、マニュアル等を見た限り
ここのハードか、同社のイギリス辺りの人が実装して提供しているファームウェアから使う
ライブラリの問題だと思いますが、いずれにしろ予測不能の不安定さで
もの凄く大変な思いをしました。
同じ処理をコピーして関数化し、ネストして実装すると動いたりして意味が分からない・・・

(3)デバッグ機能が無い

例えば、パソコンやサーバーで稼働するJava等のコンピュータ言語で開発した
アプリケーションであれば、デバッグ実行等の環境が整っていますし
PC用のシステムであれば、C言語などでも同様の事が出来ます。
マイコンでも一部の製品では、ICE等と呼ばれる同様の開発環境がありますが
この「TWE-LITE」の開発環境には無い・・・
そこで今回は、マイコンとパソコンをシリアル接続し、開発段階のデバッグメッセージを表示しながら
順次開発を進めました。

8. 開発結果

私は被害について訴訟をしようとしているので、忙しいのであまり詳細を記載している暇が無い為此のドキュメントも2日ぐらいでドラクエの片手間に猛ダッシュで書いている事から結論から記載しますと、一応機能する物は出来ました。

ソフトウェアはオープンソース化して、回路やソフト面の個別の機能等は別紙にメモ書きしてみたので興味のある人はそちらをご覧ください。

当初期待していた程度の物は、それらしく出来た

この結果を踏まえての反省点ですが

(1)目標設定プロセスから失敗だ

初めてのデジタルデバイスの開発であった事から、全面的に不明点ばかりで何もかもが不明瞭の中で目標設定した為、当然失敗しています。
マイコンの選択一つとっても、スイッチのオンオフの世界であるデジタルの世界の事ですからI2Cのインターフェースが使用可能と書いてある事で、普通に使える物と思いましたが実際には、各マイコンや通信相手となるLCDのチップ等も他国のメーカー製でマニュアルも全部英文だったりして、どうやって動かして良いのかよく分からず開発を始めた頃にはネット上にも情報があまり無く、大変な思いをしました。

つまりリスクだらけである事を理解した上で、今後何十年も続くであろう犯罪被害を考慮し開発に着手した訳ですが、想像以上に様々な問題が発生し、非常に色々と経験しました。独学で月に2〜3度は、帰宅すると玄関の鍵が開錠されていたりしていた状況でしたので様々な制約や本人のやる気やドラクエやらもあり、非常に非効率な学習期間でしたが犯罪被害からもシステム開発からも沢山の事を学んだ訳です。

一方で世界的なスパイ活動の社会的な背景を垣間見る様な事もありながら、それに付随して多数の失敗をした訳です。
その最大の失敗は最初の目標設定です。

元々犯罪被害が原因でしたので、選択肢が無かった事が後押しをしその当初から、漠然と電子鍵を実現する事にし、漠然と必要となる機能を検討し漠然と開発してしまいました。
その結果として、目標設定の段階から次の様な問題が発生しました。

a)開発対象の選定

そもそも鍵である必要が有ったのか？ 相手には国家権力がサポートしているかの様な連中も居てそこまで来ると、どんな破壊行為をしても必要に応じて住居侵入はしてくる事が想定される訳です。

「鍵作っても無駄じゃねーの？
最近は帰宅すると月に数回は玄関の鍵が開錠されているし」

と言う事は、直ぐに思ったのですが、まあ他の代替手段も見つからず・・・

b)実現方式の選定

開発対象の設定に付随して、技術的な実現性の見通しも無く開発対象を選んだ結果

「出来ると書かれていたが、実際には限定的にしか出来ない」

とか

「やりかた分からな〜い、調べ方から分からな〜い
広告に出来ると書かれている事だけしか知らな〜い」

つまり、長期の視点に基づいて始めた割に、事前の実現性の検証が甘かったと言う事です。

(2)新領域の開発には余裕が必要だ

これは、使用するマイコンから工数やコストまで含めての事です。
世の中のIT関係等の専門書には、もっともらしい事が沢山書いてありますが
現実には工数の定量的な見積もりや、リスクの回避は出来ていないのが現実です。
大企業でもコストや工数の超過が良く報道されている様に、新しい事はやった人が居ないから
新しい訳であり

やっても無い事をキチンと見積もれるとか言う偉い人達は死んでくれ！！！！

と、今回のプロジェクトでは強く思われました。

特にデバッグの機能が制約されている状況下における、I2Cインターフェースを経由した通信の不具合にはずいぶんと悩まされました。

結果として部品・工具類の調達から、簡易オシロスコープ、ロジックアナライザ等の計測機器等の購入から、問題発生都度、自作のデバックユーティリティの作成まで

初めてのデジタルデバイス開発としては、大変に様々な事に手を出す事になり

正直に言って、こんなポンコツな所が有る二度とごめんです。

教訓としては、特にマイコンなどの複雑で重要な部品については、十二分に開発に必要な情報や性能に余裕のある製品を使用する必要性を感じました。

「Raspberry Pi Zero」等で開発していたら、こんな苦労は無かったでしょう。

(3)イレギュラーである事を良く考えよう

これは、今回の様なセキュリティ対策であり、一般的では無い背景に起因していますが
被害に遭っていると一々対応が必要であり、例えばパソコンを起動するにしても
ドライブの暗号化をしているので、パスワード認証したり、起動に時間が掛かったり

そもそも自宅への住居侵入が頻発しているので、開発リソースを自宅に置いておくリスクもあり

一方で工業製品は、他の人も同様の手法で実行する事や、同様の製品を使用する等
様々な点で共通化を前提とした物です。
つまり、イレギュラーな生活をしていると、そのライフスタイルが標準化や共通化等とぶつかり
問題が生じる事は必須だと言う事です。

例えば、戦時下の無線封鎖の様にネット封鎖していると、ネット上の情報が参照出来ない
あまりしっかり通信封鎖していると、犯人達は本格的に犯行をエスカレートしてきて
情報窃盗の被害以外にも含めて、深刻な被害が出てしまう。

この問題の単純な解決策は無く、諸々のシステムをよく理解して、戦場を無闇に広げず
リスクを局所化をしながら一方で合理的すぎず、時に不明瞭さ等でリスクを相手に理解して貰う

制約下だからこそ戦力を集中し、限られた選択肢の中からリスクの最小化をしていくしか
大きな観点では、対応策は無いと思われると言う事です。

(4)それでも必要な事はしなければならない

特にここ数年、自分でも驚く程に調べてみると不審な事が分かったり、被害に遭ったりしてきました。調べてみると被害が実現する様な形で、社会制度に意図的な欠陥が埋め込まれているかの様な制度や役所の対応が判明し、様々な社会システムに対して、まったく信用出来なくなりました。

しかし北朝鮮の問題などから、テレビに出てくる偉い人達による危機管理の話は良く報道されその専門家と称する人々は、もっともらしく様々な話をし企業の偉い人達も、政治家も、学者も、もっともらしく様々な話をしながら問題解決の方針を主張しています。

しかしそんな彼らが、我々と同様の被害に遭っている様子は無く当然、その問題を解決している気配は1ミリもありません。

つまりあれは現実世界とは違う虚構世界の話だと思われれます。

こんな社会に従順ならば、我々の様な目に遭わないのでしょうか？

また、こう言う社会の在り方に反抗して、結果を出した人が居るのでしょうか？

そもそも、そんな人たちが居れば、こんな目には遭わないのでは無いのでしょうか？

診断書の様な客観的な事実すら警察が認めない社会においてなんでも透明性が云々と言う連中は、リスクを押し付けてくるだけの害獣に過ぎません。

そんな連中には、試しに「お前のメールアカウント情報を開示しろよ」と言ってみればどれだけ虚構に満ちたふざけた連中なのかが分かるでしょう。

人々にとって様々なセキュリティの必要性は明白であり、一方で開示すべき情報もある

多くの人はテレビの中の人と、同じ状況を共有している事実はありませんし状況が違えば対応が違うのは当然です。

きちんと状況を判断して、諦めずに取捨選択をし、成すべき事はなさねばならないのです。

以上が今回のプロジェクトの反省点・・・の抜粋 多すぎて書ききれない

日々細かく後悔する事で学習し、次のシステムに活かして行きたいと思います。

往相にして不可避である事が多いので、解決策が無いからまたやっちゃうのしょうけれど

そう言う事実を直視しないで、「ソリューション」だの言って、この世の中の問題は自分達の問題解決能力に応じて用意されているかの様に思い込み

その上で解決策があるとして仕事するから

みんなそうやって、偉い人達の妄想に付き合わされて失敗するんだあれ

現実逃避と状況認識の甘さですね

「お前等の能力に合わせて世界は作られていない」と言いたいです。