保坂さん卒論まとめ

わからないこと書き出す→調べて書き出す
〇具体的に理解できたか(100%)、△文章だけは理解できたか(50%)、？？理解できない(0%)
アンダーラインは自分の考え

タイトル － IP アドレスをコモンネームとして持つ Web サーバー証明書の正当性確認

わからないこと － コモンネーム、Web サーバー証明書の正当性について

・コモンネーム － SSL サーバ証明書の設定項目の一つで、SSL 暗号化通信を行うサイトの URL のうち、サブドメインまでを含んだドメイン部分のこと　〇
・Web サーバー証明書の正当性とは － 信頼性があるかどうか　△
①ルート証明書が発行されている Web サーバー証明書は信頼性がある？？orWeb サーバー証明書の信頼性を検証するためにルート証明書がある？？
自分では両方正しいと考えている
②この研究は証明書チェーンを調べること？(何の証明書を調べる？)
証明書チェーンの中で自分で何か基準を決めて、その基準によって Web サーバー証明書に信頼性があるかどうか調べていくと考えている

証明書チェーン － クライアント、サーバなどの証明書から、ルート証認局の証認局証明書までの連なりのこと

Web サーバー証明書と SSL サーバー証明書と WebIP 証明書は同義？？
WebIP 証明書は違う気がする
ルート証明書が発行される対象は Web サーバー証明書 orWeb サーバー？？

第一段落　はじめに

書かれていること
研究の背景、研究の目的や内容、調査結果、考察

まず、現在の情報社会においての Web、Web サーバーについて書かれていて
10 行目の「しかし」から 13 行目が理解できなかった

12,13 行目　Web サーバー証明書の所有者が Web サーバー証明書に記載されている IP アドレスの利用権を有しているかの確認はできない。有しているか否かでなにが変わるのか？？
14 行目　利用権を有していない IP アドレスが記載された証明書を取得できてしまう可能性が存在する。→取得出来たらどうなるか？？
その後、研究内容、どのような調査をするのか
調査①Windows のマシンを用いてリソース証明書の使用状況や内容に関しての調査
調査②リソース証明書の収集や処理
調査③WebIP 証明書に使用されている IP アドレスが該当の WebIP 証明書の被発行者が利用権を持っている IP アドレスであるのかの調査
そして、具体的な調査内容が書かれていて
結果として出るものが
Web サーバー証明書の抽出、抽出された Web サーバー証明書のうちにどれだけ WebIP 証明書が含まれるのか、WebIP 証明書の CN や SAN にどれだけ IP アドレスが含まれるのか、WebIP 証明書に含まれる回数が多かった Subject 属性上位 10 種の調査、
プライベート IP アドレスを含む WebIP 証明書が全体の約 7 割（プライベート IP アドレスは良くない）WebIP 証明書に含まれている個数の多かった Subject 属性上位 10 個を含む WebIP 証明書だけで WebIP 証明書の総数のおおよそ半分を占めていることが判明（だから何？？）

信頼性がないとどういう不具合が起こるのか説明がない
調べた結果 － とりあえず危険
ブラウザがサイトの危険性を察知すると警告してくれる
警告→有効期間切れ、認証機関の信頼性、名前不一致
自己署名証明書 － 公開鍵をそれに対応する私有鍵で著名した公開鍵証明書（自己署名証明書の SSL 証明書の信頼性は低い）
リソース証明書 － アドレス資源の割り振りや割り当て
IP アドレスと AS 番号の利用権利を示す電子証明書番号
インターネットレジストリの IP アドレスの割り振り構造と同じツリー構造で PKI の認証局を構築することで、利用されている IP アドレスと AS の正当性を保証するための仕組み

WebIP 証明書 － 調べても出てこなかった

どんな調査をしているか（調査内容)、具体的には理解できなかった
頑張って 1 つずつ調べていけば理解できそう
なんとなくわかれば良いのであれば飛ばす、完璧に理解する必要があるのであればしっかり調べて理解する

第二段落　前提知識

IP ○　通信するためのプロトコル(約束事)
IP アドレス　△　ネットワークに接続された機器を識識するための識別データ(何の基準で識別する？？)
DNS　○　ホスト名を IP アドレスに変換し通信を行うため(ホスト名のままでは通信できないから)
PKI　○　公開鍵を利用するための技術
認証局　○　鍵と証明書の保持者の関係(間柄)についての信憑性について
登録局　○　鍵と証明書の保持者の信憑性について
公開鍵証明書　△　証明書に記載された公開鍵と秘密鍵のペアの所持者であることの証明書、認証局から発行された証明書とその保持者の関係性(信憑性を上げるためのもの？？)
証明書失効リスト　△　証明書の有効期間よりも早く失効した証明書の識別リスト(なぜ有効期間より早く失効されるの？？→認証局の信頼性の欠如、名前不一致のため？？)
証明書利用者　○　認証局から発行された証明書の秘密鍵を持っていて、その証明書を利用するための存在(利用する理由は安全性の確認？？)
ディレクトリ　△　各種情報の集合体、公開鍵証明書の情報をまとめたもの？？
証明書有効性検証局　○　認証局や証明書の信憑性を確かめる組織
Web サーバー証明書　○　インターネット上での SSL/TLS 通信の際に暗号化された情報の安全性を確かにするもの、また通信するものを暗号化する
リソース証明書　○　IP アドレスと AS 番号の利用権利があることを示すもの
AS 番号　○　統一されたルールのもと運用、管理されているネットワークのこと
ZMap　○　インターネット上で広範囲のネットワーク調査を行うもの

第三段落　調査内容・手法

リソース証明書の関する調査
リソース証明書に関する調査では、WebIP アドレスが該当の WebIP 証明書の被発行者が本当に使用していい IP アドレスであるのかを調査することを目的とした。具体的に採った手法としてはリソース証明書の使用状況や内容に関しての調査と、リソース証明書の収集及び処理を行った。ここではその調査と作業に用いた環境とその手法について示す。○
この調査の内容は理解したが、具体的な操作はわからない(同じことをしろと言われたら助けてもらいながらでないとできない)

Web サーバー証明書に関する調査

Web サーバー証明書に関する調査では、まずは WebIP 証明書がどれだけ社会で使われているのかを確認することを目的とした。その為にインターネット上に存在している全サーバーの 443 番のポートを対象にポートスキャンを行い、ポートスキャンの結果応答のあったサーバーから Web サーバー証明書を収集した。そして収集した Web サーバー証明書から WebIP 証明書の抽出を行い、WebIP 証明書の割合調査と WebIP 証明書の内容に関する調査を行った。△

この調査の内容は理解したが、具体的な操作はわからない(同じことをしろと言われたら助けてもらいながらでないとできない)

→調査時に使用した環境？？

割とわからないかも、、

第四段落　調査結果

リソース証明書に関する調査の結果　〇　(こんな結果が出たよと分かっただけ)

Web サーバー証明書に関する調査の結果　〇　(こんな結果が出たよと分かっただけ)

第五段落　考察

WebIP 証明書が使用される状況

Subject 属性の内容(表 14)、どういうものかわからない？？

Subject 属性を含んでいる WebIP 証明書は、クラウドやゲートウェイなどネットワークに関する機器と思われるホストやクラウドのサービスを提供するための仮想マシンらしきホスト向けに発行されやていると考察したこと

Subject 属性を含んでいる WebIP 証明書が全 WebIP 証明書の半数を占めるので WebIP 証明書のほとんどはネットワーク機器や仮想マシン向けに発行されたものであると予想した

だからネットワークに関する機器や技術に関わる場面は WebIP 証明書が使用される主要な状況の一つと考えた　△

ホスト － コンピュータネットワークに接続されたコンピュータやデバイス

クラウド － インターネットなどを経由してコンピュータ資源をサービスの詳細(手段)はわからないが利用できるサービスとしてでできる仕組み

仮想マシン － コンピュータの動作をエミュレート(ものまね)するソフトウェアやフレームワークのこと

ゲートウェイ － コンピュータネットワークをプロトコルの異なるネットワークと接続するためのネットワークノード

ルータ ー コンピュータネットワーク上で２つ以上の異なるネットワーク間にデータを中継する機器
オープンソース ー 公開されたソースコード

不適切な WebIP 証明書
不適切な WebIP 証明書の１つはネットワーク機器にデフォルトで設定された証明書だと考え、WebIP 証明書の約７割がデフォルト設定のもの
デフォルトで設定された証明書とはコモンネームやネットワークストレージ(SAN)にプライベート IP アドレスのみが記載された WebIP 証明書
このような証明書が使われている理由は不特定の第三者による外部からの https アクセスを想定していなかったから
WebIP 証明書に含まれている Subject 属性を見ていくと、その内容から SonicWALL 社により用意された自己署名証明書であることがわかった、これは不適切と思われる WebIP 証明書の 25%である
SonicWALL 社は企業などの団体のネットワークセキュリティに関わる機器の製造販売を行っているため、上記の証明書は外部ネットワークよりの https アクセスが想定されていない SonicWALL 製品に設定された証明書だと考えた
そしてほかにも同じものがあり不特定の第三者による外部からの https アクセスを想定していなかったということを予想した

中にはグローバル IP アドレスも同時に含んだ WebIP 証明書もあり、それは外部への公開を意図していると考えられるので問題が少ないように思える
しかし、デフォルト設定の証明書が設定された機器が外部からの https アクセスを受け付ける状態になっているている、これが危険
その機器が外部からの https アクセスを想定していないのにも関わらず実際はアクセスできてしまう状態なので、セキュリティに大きなリスクを抱えているといえる、そういった機器が数多くある
そのことを踏まえて、デフォルト設定ではなく新たに発行された Web サーバー証明書を使用することが望まれる(新たに発行された Web サーバー証明書は安全なのか)

デフォルト ー 初期値、基準値

第六段落　まとめ

この研究の目的と何の調査をしたか
リソース証明書の調査について
調査の中身

調査の結果とその結果に対しての考察
今後の課題
IP アドレスの利用権の割り当ての確認手法の考案
それについて、リソース証明書は AS 番号や IP アドレスといった情報資源の管理のための電子証明書であるために、最適の情報源となると予想
→リソース証明書とは、IP アドレスと AS 番号の利用権利があることを示すもの
なので最適かどうかわからないが、情報源になるのは当たり前なのでは？？
リソース証明書の内容は難しいので、それがわからないままでも IP アドレスと AS 番号の利用権利を確認できる方法を考える必要があるらしい
リソース証明書とは、必ずしも IP アドレスと AS 番号の利用権利があることを示すものではない？？