2007 年 8 月 14 日

国立情報学研究所　情報処理軽井沢セミナー　研修報告
平成 19 年度テーマ：認証技術を知る　～PKI を中心として～

関西医科大学　大学情報センター学術部
新貝　欣久

1．セミナー課題：自施設における PKI の利用を考える
- 発表タイトル：認証技術の利用　～セキュアメールインフラへの利用～

2．セミナー課題発表内容の概要（スライド資料は本編に追記）
- PKI によって診療情報のような高度に秘匿性ある情報を電子メールで行う学内メール基盤の提案
- 電子証明書を個々人で取得するのではなく組織としての電子証明書を利用し秘匿性と内容を担保するシステム構成を策定する
- Public と Private 認証局を相互に利用することで学外ステークホルダ（メール受信側）への経費的課題の解決を図る
- 学外ステークホルダを TrustedRecipient として、本人確証を情報送信側でおこなう運用手順を策定する。

3．セミナーで学んだ技術及び知識

(ア) PKI の基礎知識
① 暗号・電子署名・認証の必要性
② 暗号技術
③ 認証と電子署名
④ 公開鍵証明書と認証局
⑤ 公開鍵証明書を利用した通信

(イ) UPKI 概要
① UPKI の計画概要
② 3 層アーキテクチャの実装についての詳細
③ これからの課題、認証連携
④ 導入事例

(ウ) 認証連携としての shibboleth
① shibboleth 及び認証連携の概要
② shibboleth の実装手順
③ 認証連携の現状、shibboleth の動向

(エ) グリッドにおける認証技術の利用
① グリッド利用のための認証
② グリッド認証局の運用

４．セミナーの成果（所属機関でどのように利用するかの展望）

- NAREGI－CA スタートアップキットによるキャンパス PKI 実装。学内認証局としての導入評価とスタッフのスキルアップを目的として行う。
- 課題発表の電子メール基盤への利用を次期構築計画として検討する。
- 学外ステークホルダとの VPN 接続認証に PKI 利用も対象に入れる。
- 学内 LAN 機器認証へ 802.1x 認証を導入するに当たり、よりセキュアな TLS 導入および学内認証局の構築を考える。学内 PKI 基盤には UPKI でのキャンパス PKI モデルおよびガイドラインをシステム要件として採用する。
- 電子文書法における電子署名について関連部署と連携し積極的導入を推進するため、技術的側面から援助、助言を行う。

５．セミナーの事前、事後において、参考になった URL と内容

- http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html
- http://www.atmarkit.co.jp/fsecurity/special/04smime/smime01.html
  - ✧ 電子メールで電子証明書を利用するための実装手順
- http://www.atmarkit.co.jp/fsecurity/rensai/elesign01/elesign01-1.html
  - ✧ PKI 導入から CA 運用について管理者への指南詳細

６．事前準備として知っておいた方が良かったと思われること

- PKI の基本となる鍵作成方法から証明書取得からサーバ（WEB など）への証明書登録へ至るまでの PKI 利用の最も基礎的な手順を事前に実施体験しておけば、疑問点を研修中に解決でき、より効果的にこのような機会を生かせたのでは。さらにセミナー実習の理解と自職場への応用発想が広がったのではと思われる。

７．セミナーの感想

- PKI 基礎の講義は実装例を交えて講義していただいたため技術職にとっては非常に理解しやすいものであった。
- UPKI については UPKI イニシアティブ報告の総論的な内容を講義していただき現時点での全体像を把握できた。所属組織でどのようにまたどの部分で関わっていくかという方針を考える良い機会であった。
- 感覚的に捉えにくい認証連携を、shibboleth の実装を実習することでかなり具体的に理解できた。ただ実際に自施設に認証基盤を導入しようとする立場からいえば、業務上で即必要とするものと少々乖離があるのではという印象がのこる。
- 研修目的にあるように最新情報に触れる機会をいただき感謝いたします。今後、研修応募要綱にあるように「到達目標が達成できる」ことを重視していただいて、即戦力的な研修内容を加味、策定していただければより充実した研修になると考えます。
- できるならば、PKI のような深い内容は基礎編、実装編、運用管理編など STEP 形式でそれぞれのテーマをしっかりとご教授願いたい。

８．その他

- 集中して研修するには最適な環境であったと考えます。
- 研修期間を通して、国立情報学研究所スタッフのご配慮に感謝いたします。

セミナー課題資料

認証基盤の利用

～セキュアメールインフラへの利用～

国立情報学研究所　情報処理軽井沢セミナー
～認証技術を知る～
研修課題
於軽井沢国際高等セミナーハウス
2007年8月3日
関西医科大学　大学情報センター学術部　新貝欣久

PKIのメリットとは何か？

- ユーザID＆パスワードで足りるのならばPKIは必要ない。
- PKIの十分条件を考察する（認証、秘匿性の観点から）
  - 認証作業の利便性、簡便化（SSO、接続機器認証）
  - ユーザID＆パスワードを利用できないケース（電子署名）
  - 不特定の相手との通信に秘匿性が要求されるケース
  - 相互信頼性の担保
- 情報交換相手が互いの管理下になく、しかし交換される情報に高い秘匿性が求められるというケースに最大の効果を発揮する

セキュアメールインフラ

- 概要
  - 診療現場を抱える医科大学として、秘匿性の高い診療情報の学外との伝達インフラを、診療系メール基盤とPKIを利用して構築する
  - 学内、学外を問わず情報漏えい措置を担保するアーキテクチャを実装
  - 上記アーキテクチャに基づくセキュリティを保障する運用手順
  - 学内セキュリティポリシーに沿った方策であり大学としてオーソライズできるインフラサービスを提供

システム導入の必要性

- 近年、診療情報の電子化が進行しているが情報漏えい対策の立場から電子的手段による情報授受インフラ整備は遅れている。
- 強度な秘匿性を追及した学内外の通信システムでは、学外ステークホルダにも高コストを強要し現実的でない場合がある。
- 現在運用されている大学メールシステムは研究、業務での使用を前提としているため、セキュリティポリシーでも診療情報掲載は禁じている。
- ユーザがメールの非秘匿性を理解していない場合、診療情報授受に使用する危惧がある。
- にもかかわらず、大学として対外的にセキュリティを担保した電子的な情報伝達インフラや手段が提供されていない。
- 結果、セキュリティインシデント回避はユーザのモラルとリテラシに一任されている。

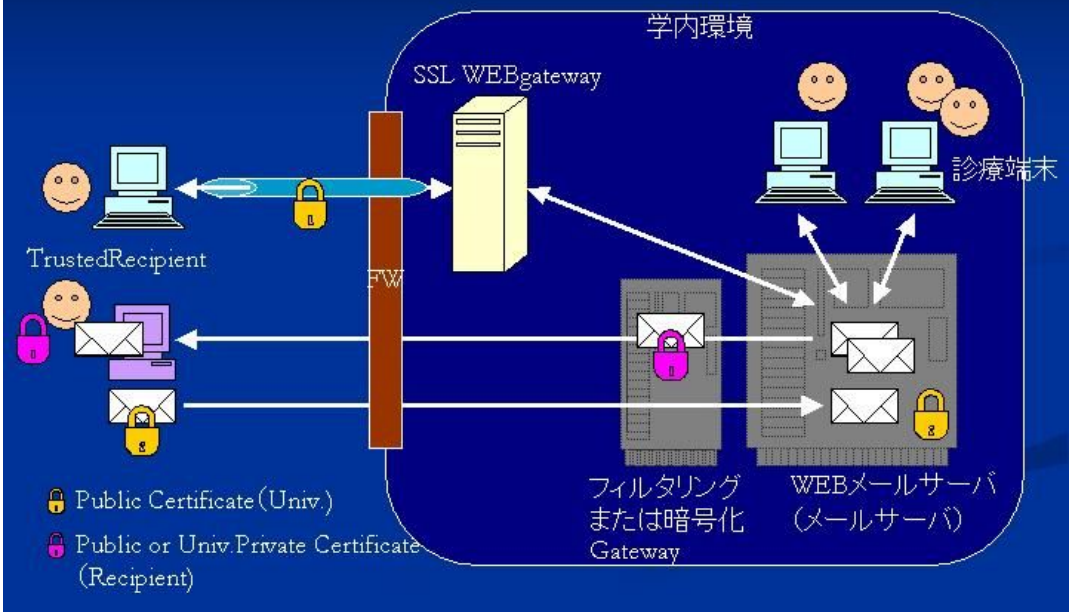
システム要件

- 学内のネットワークセキュリティポリシーに沿う
- システム的に秘匿性が保障され、インシデント対策としてオペレーション時のフールプルーフ要素を考慮
- 既存システムや学内アカウント取得時の本人認証手順を利用することで、導入が容易であり利便性をあまりそこなわない運用手順
- 学外ステークホルダにとって高コストを課さない方法

構造

- 診療業務専用のドメインを持つメールインフラを利用（診療業務に携わる職員にメールアカウントを発行）。
- メールシステムへのアクセスは、PCに情報を残さないWEBメールを唯一のインターフェースとし、WEBメールエントリのユーザ認証は病院内グループウェアと連携
- 学外への送信メールは原則暗号化（受信者のパブリックまたは大学認証局のプライベート証明書、S/MIMEなど）を行う
- 一括して大学の電子証明書（TrustedThirdPartyによるパブリック証明書、S/MIME）を添付
- 暗号化を行うあるいは暗号化されていないメールは通さないgatewayを設置
- メール受信相手をTrustedRecipientとして認証済み受信先の電子証明書とアドレスを登録する運用プロセスを策定
- 学内プライベートPKIのCAを開設。パブリックPKIと大学プライベートPKIの混在利用。

概念図



TrustedRecipientへ提供する アクセス手段

- SSL-gatewayによるWEBメールシステムへのアクセス(学内アカウント取得者対象)
  - ユーザ認証は学内アカウントと連携。。
  - SSL-gatewayにはTTP等によるパブリックの大学サイト証明書
  - SSLによるHTTP経路の秘匿性確保
- PGPまたはS/MIMEによる暗号化メールを送信(学外ステークホルダ)
  - 学外へは暗号化されていないものは出せない構造
    - WEBメールで暗号化+フィルタリング用gateway または 暗号化専用gateway
  - TrustedRecipientの登録手順
    - パブリック証明書を取得する。あるいは大学プライベートPKIによる証明書を発行。
      - パブリック証明書を取得する。
      - プライベートPKIによる証明書を発行。TrustedRecipient認証部署へ申請メール。CallBackで実在確認ののち、証明書発行サイトへ誘導。
    - TrustedRecipient認証部署へ署名つきメールの送信。大学電子署名のメール返信。送信先メーラーに証明書の登録
    - WEBメールシステムアドレス帳にTrustedアドレスとして登録。WEBメールシステムへ証明書の登録
    - 学内ユーザから診療情報をTrustedRecipientに送信。暗号化され大学の電子署名入りで届く。

成果

- 診療情報が透過的にステークホルダ（検査等の依頼元）へ届くセキュアインフラの提供。
- 大学が取得するパブリック電子証明書は少数でよい。
- 診療メールシステムを明確に分けることによるユーザのセキュリティ意識向上
- アドレスミスによる誤送信の抑止

課題

- システム面
  - 暗号化、電子署名に対応したWEBメールアプリケーションが少ないため、選定や作りこみが必要
  - フィルタリングgatewayの暗号化アルゴリズムへの対応状況
  - 暗号化によって中間経路でのウイルス検知が難しくなる
- 運用面
  - 職員のリテラシ教育。情報保護姿勢の公示。
  - TrustedRecipientの登録プロセス。
    - 登録手順の周知方法。
    - なりすまし対策。本人確認プロセスの最適化。
    - 認可するTTPの選定。あるいはプライベート認証局の整備。
  - 情報主体への同意プロセスのマニュアル化とポリシー改訂。
  - TrustedRecipient側への対策
    - PC盗難によるなりすましやPtoPウイルスによる情報漏えいへの注意喚起。

認証基盤の利用
～セキュアメールインフラへの利用～

国立情報学研究所　情報処理軽井沢セミナー
～認証技術を知る～
研修課題
於軽井沢国際高等セミナーハウス
2007年8月3日
関西医科大学　大学情報センター学術部　新貝欣久

PKIのメリットとは何か？

- ユーザID＆パスワードで足りるのならばPKIは必要ない。
- PKIの十分条件を考察する（認証、秘匿性の観点から）
  - 認証作業の利便性、簡便化（SSO、接続機器認証）
  - ユーザID＆パスワードを利用できないケース（電子署名）
  - 不特定の相手との通信に秘匿性が要求されるケース
  - 相互信頼性の担保
- 情報交換相手が互いの管理下になく、しかし交換される情報に高い秘匿性が求められるというケースに最大の効果を発揮する

セキュアメールインフラ

- 概要
  - 診療現場を抱える医科大学として、秘匿性の高い診療情報の学外との伝達インフラを、診療系メール基盤とPKIを利用して構築する
  - 学内、学外を問わず情報漏えい措置を担保するアーキテクチャを実装
  - 上記アーキテクチャに基づくセキュリティを保障する運用手順
  - 学内セキュリティポリシーに沿った方策であり大学としてオーソライズできるインフラサービスを提供

システム導入の必要性

- 近年、診療情報の電子化が進行しているが情報漏えい対策の立場から電子的手段による情報授受インフラ整備は遅れている。
- 強度な秘匿性を追及した学内外の通信システムでは、学外ステークホルダにも高コストを強要し現実的でない場合がある。
- 現在運用されている大学メールシステムは研究、業務での使用を前提としているため、セキュリティポリシーでも診療情報掲載は禁じている。
- ユーザがメールの非秘匿性を理解していない場合、診療情報授受に使用する危惧がある。
- にもかかわらず、大学として対外的にセキュリティを担保した電子的な情報伝達インフラや手段が提供されていない。
- 結果、セキュリティインシデント回避はユーザのモラルとリテラシに一任されている。

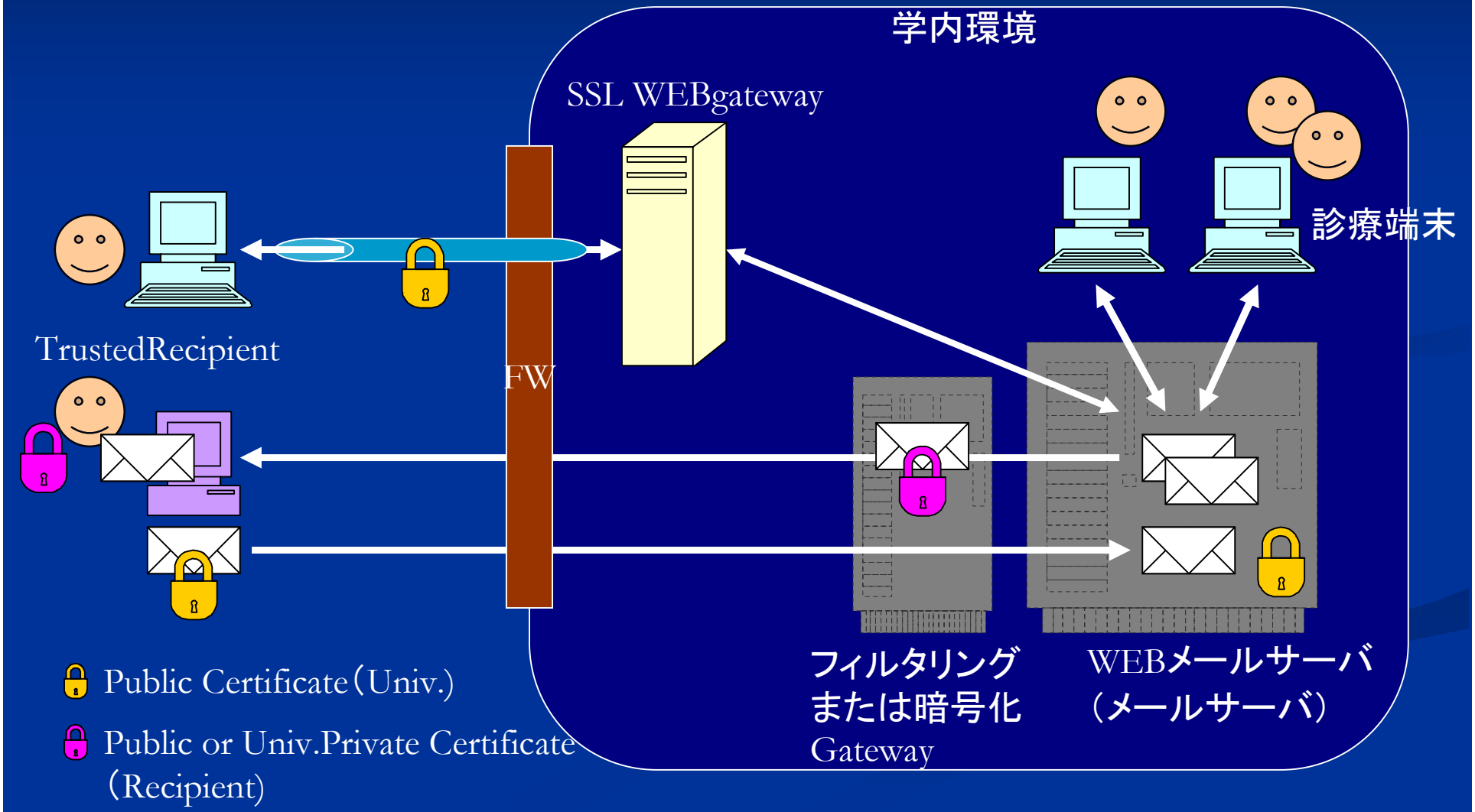
システム要件

- 学内のネットワークセキュリティポリシーに沿う
- システム的に秘匿性が保障され、インシデント対策としてオペレーション時のフールプルーフ要素を考慮
- 既存システムや学内アカウント取得時の本人認証手順を利用することで、導入が容易であり利便性をあまりそこなわない運用手順
- 学外ステークホルダにとって高コストを課さない方法

構造

- 診療業務専用のドメインを持つメールインフラを利用（診療業務に携わる職員にメールアカウントを発行）。
- メールシステムへのアクセスは、PCに情報を残さないWEBメールを唯一のインターフェースとし、WEBメールエントリのユーザ認証は病院内グループウェアと連携
- 学外への送信メールは原則暗号化（受信者のパブリックまたは大学認証局のプライベート証明書、S/MIMEなど)を行う
- 一括して大学の電子証明書（TrustedThirdPartyによるパブリック証明書、S/MIME)を添付
- 暗号化を行うあるいは暗号化されていないメールは通さないgatewayを設置
- メール受信相手をTrustedRecipientとして認証済み受信先の電子証明書とアドレスを登録する運用プロセスを策定
- 学内プライベートPKIのCAを開設。パブリックPKIと大学プライベートPKIの混在利用。

概念図


学内環境
SSL WEBgateway
診療端末
TrustedRecipient
FW
フィルタリング
または暗号化
Gateway
WEBメールサーバ
（メールサーバ）
Public Certificate（Univ.）
Public or Univ.Private Certificate
（Recipient）

TrustedRecipientへ提供するアクセス手段

- SSL-gatewayによるWEBメールシステムへのアクセス（学内アカウント取得者対象）
  - ユーザ認証は学内アカウントと連携。。
  - SSL-gatewayにはTTP等によるパブリックの大学サイト証明書
  - SSLによるHTTP経路の秘匿性確保
- PGPまたはS/MIMEによる暗号化メールを送信（学外ステークホルダ）
  - 学外へは暗号化されていないものは出せない構造
    - WEBメールで暗号化＋フィルタリング用gateway　または　暗号化専用gateway
  - TrustedRecipientの登録手順
    - パブリック証明書を取得する。あるいは大学プライベートPKIによる証明書を発行。
      - パブリック証明書を取得する。
      - プライベートPKIによる証明書を発行。TrustedRecipient認証部署へ申請メール。CallBackで実在確認ののち、証明書発行サイトへ誘導。
    - TrustedRecipient認証部署へ署名つきメールの送信。大学電子署名のメール返信。送信先メーラーに証明書の登録
    - WEBメールシステムアドレス帳にTrustedアドレスとして登録。WEBメールシステムへ証明書の登録
    - 学内ユーザから診療情報をTrustedRecipientに送信。暗号化され大学の電子署名入りで届く。

成果

- 診療情報が透過的にステークホルダ（検査等の依頼元）へ届くセキュアインフラの提供。
- 大学が取得するパブリック電子証明書は少数でよい。
- 診療メールシステムを明確に分けることによるユーザのセキュリティ意識向上
- アドレスミスによる誤送信の抑止

課題

- システム面
  - 暗号化、電子署名に対応したWEBメールアプリケーションが少ないため、選定や作りこみが必要
  - フィルタリングgatewayの暗号化アルゴリズムへの対応状況
  - 暗号化によって中間経路でのウイルス検知が難しくなる
- 運用面
  - 職員のリテラシ教育。情報保護姿勢の公示。
  - TrustedRecipientの登録プロセス。
    - 登録手順の周知方法。
    - なりすまし対策。本人確認プロセスの最適化。
    - 認可するTTPの選定。あるいはプライベート認証局の整備。
  - 情報主体への同意プロセスのマニュアル化とポリシー改訂。
  - TrustedRecipient側への対策
    - PC盗難によるなりすましやPtoPウイルスによる情報漏えいへの注意喚起。