電子メール最新技術動向

オレンジソフト 渡部 直明
kitarou@orangesoft.co.jp

Orangesoft

今年のキーワード

- 通信傍受法の成立
  - 電子メールも傍受の対象に
- 電子メール感染型ウィルスの流行
- 携帯電話の登場
  - 手軽に電子メールが見られる/書ける(?)
  - 電子メール利用者の急増
  - 今まで利用しなかった人まで利用し始めた
- 電子メール転送の問題
  - 携帯電話、PDA等デバイスによって転送先を切り替える必要があった。
  - これらを統合するサービスの出現
    - でも、セキュリティは大丈夫?

Orangesoft

従来の技術

- SMTP(Simple Mail Tranfser Protocol)
- POP3(Post Office Protocol) & APOP
- MIME (RFC2045-RFC2049)
- POP before SMTP
- S/MIME,PGP(PGP/MIME)
- IMAP4rev1(RFC2060)
  - Internet Message Access Protocol
- LDAPv3(RFC2251-2256)
  - Lightweight Directory Access Protocol

Orangesoft

今年も継続している技術

- IMAP4rev1
- S/MIME,PGP(PGP/MIME)
- LDAPv[2|3]

Orangesoft

今年のトピックス

- SMTP AUTH(RFC2554)
  - SMTP Service Extention for Authentication
- MDNs(RFC2298)
  - Message Disposition Notifications
- DSNs(RFC1894)
  - An Extensible Message Format for Delivery Status Notifications)

Orangesoft

携帯電話がやってきた

Orangesoft

電子メールにひとつの切り分け

- ビジネスの電子メール
  - 電子メールを全て転送されていたら大変
  - 電子署名、暗号化などへの対応
  - より、セキュアな運用・管理
- 遊びとしての電子メール
  - 携帯電話等手軽なデバイスを使用
  - 長いメッセージ、添付ファイル等は使用できない
    - MIME位理解してね

Orangesoft

電子メール転送の恐怖

- 社内メールをキャリアのメールボックスへ転送
- キャリアのメールシステムで配送の遅延が発生
- キャリアのメールボックスに頼っていると社内メールに気が付かない
  - 社内メールなので本来ならすぐに読めるはず
  - 知らなかったは許される？
- 外出中もメールが読めて便利なはずが

Orangesoft

次なるサービス大胆予想

- キャリアによる電子メールサービスはそろった
- 競っているのは受信可能文字数だけ
  - これってちょっと本質とは違うのでは?
- 今や電子メールは文字だけではない
  - MIMEも処理できないで電子メールと言えるか
- サービスとしては完全に横並び
- さて、次なるサービスは?

Orangesoft

電子メールの危険性

- 盗聴
  - 経路上での盗聴
  - ファイルの盗聴
- メール爆弾
  - 大量のメールの送付
- 不正中継
- なりますし

Orangesoft

盗聴(経路上での盗聴)

- 技術的には十分可能
- 実際は大量のデータの中から必要なデータはどう取出すか
- 通信傍受法も１つの盗聴
  - どうデータを切り分けるか

Orangesoft

盗聴(ファイルの盗聴)

- メールサーバのスプール
  - 暗号化等で対応可能
- 中継途中でのファイル
  - 全ての中継するサーバが安全とは限らない
  - DNS(MX)等を不正に書換え
- PCに保存されているデータ

Orangesoft

メール爆弾

- 大量なメールで相手のメールサーバを使用不能にする
  - サイズが大きなメールを送りつける
  - 沢山のメールを一斉に送りつけ大量のセッションをはる
- 受信するPCも使用不能になる
- しかし、最近は減ったかな?

Orangesoft

不正中継

- メールサーバを不正中継に利用されてしまう
  - サーバの負荷が高くなり本来の業務に支障がでる
  - 苦情が来て、企業の信用を落とす
  - 最近では不正中継対策が行われているので少なくなった
    - 商用製品では不正中継対策機能は必須

Orangesoft

なりすまし

- 特定個人になります
- 企業などの代表アドレスになりすます
  - webmaster@会社名.co.jp
  - 今後EC等に向けてどう対処して行くか
- 商用メールになりすます
  - メール新聞、メールマガジンになりすます
- なりすましでスパムメールの送信
  - どう対処する?

Orangesoft

なりすましスパムメール

- いつ被害にあうかわからない
- 送信されていても自分達は気づかない
  - 急にエラーメールが沢山送られてくる
  - 何がおきたたのか最初はわからない
- 対処の方法はない
  - 現在のInternetメールシステムの脆弱さ

Orangesoft

メール管理
IMAP4rev1

Orangesoft

IMAP4

- Internet Mail Access Protocol Ver.4
- 商用製品ではサポートは当たり前
- メールの管理はサーバ側
  - 未読/既読の管理
  - フォルダの管理
  - メールの保存は基本的にサーバ側
- 各自のメールのバックアップはサーバで

Orangesoft

MailConnect 5

- IMAP4以外にDSN,MDNのテストも行われた
  - でも、これには参加しなかった
- やはり日本語の検索についてはみんな興味があった。
- IMAP4 Language Extensionのテスト
  - draft-gahrns-imap-language-00.txt
  - Netscape,Orangesoft
- 等など

Orangesoft

Language Extension

- サーバからの応答メッセージの言語を指定する事ができる
- SMTPみたいにコードの方がいいのでは?
  - サーバ内での事象はサーバしかわからない
  - コードだけでは情報不足
- 何がうれしいか?
  - “パスワードが違います”と日本語で出せる
  - “○○なので管理者に連絡してください”

Orangesoft

Messaging Interoperability Japan

- USだと大変なんで日本でもやりたかった
- JANOGのMLやる言ったら後に引けなかった
- 4/7-8にIRIで開催(10社が参加)
- さて、どんな問題があったか?
- 何がわかったか

Orangesoft

参加社

- 日本電気株式会社(ExpressMail)
- 日本電気テレコムシステム株式会社(WeMail32)
- カスタム・テクノロジー株式会社(N-PLEX)
- 日本ネットスケープ・コミュニケーションズ株式会社(Netscape Messaging
- Server,Netscape Communicator)
- アライドテレシス株式会社(AT-Mail Server,AT-承認メール)
- ロータス株式会社(Domino,Notes)
- 株式会社オレンジソフト(Winbiff)
- 株式会社クニリサーチインターナショナル(Eudora)
- 株式会社ケイ・ジー・ティー(IMail Server for Windows NT)
- コンパックコンピュータ株式会社(Software.com社製 InterMail)

Orangesoft

Messaging Interoperability Japan 2nd

- 1999年11月8日,9日
- さて結果は…..

Orangesoft

IMAP4だけなぜいじめられるの?

- IMAPにはセキュリティホールが….ある?
- サーバにHDDが無限に必要?
  - サーバにためなくてもユーザは自分のPCにためる
- IMAPはスケールしない?
  - IMAPはプロトコル
  - スケールするか、しないかは実装しだい
- 基本的に情報不足……...

Orangesoft

IMAP4は重い

- メールが一杯あると大きなファイルを開くので重い
  - メールボックスはUnixのmbox形式だけじゃない
- プロトコルと、データの操作は分けて考えよう
  - ファイル(メール)へのアクセスは実装に依存
  - 検索などの速度も実装依存
- 製品(ソフト)をしっかり吟味しよう

Orangesoft

例えばcyrus imapd

```
-rw-------  1 cyrus  mail  6662756 May 21 21:09 cyrus.cache
-rw-------  1 cyrus  mail      136 Feb  8 20:27 cyrus.header
-rw-------  1 cyrus  mail   426444 May 21 21:09 cyrus.index
-rw-------  1 cyrus  mail       53 Feb  8 20:36 cyrus.seen

-rw-------  1 cyrus  mail      402 May 21 21:09 8200.
-rw-------  1 cyrus  mail   438674 Mar 30 08:28 8199.
-rw-------  1 cyrus  mail   179410 Mar 30 08:28 8198.
-rw-------  1 cyrus  mail    66076 Mar 30 08:28 8197.
-rw-------  1 cyrus  mail    66319 Mar 30 08:28 8196.
-rw-------  1 cyrus  mail   152660 Mar 30 08:28 8195.
-rw-------  1 cyrus  mail    43279 Mar 30 08:27 8194.
-
```

Orangesoft

製品にはターゲットがある

- 数百万メールボックスを扱う何千万円もの製品
- 数十ユーザをターゲットにした数万円の製
- 同じに比較できるの?

Orangesoft

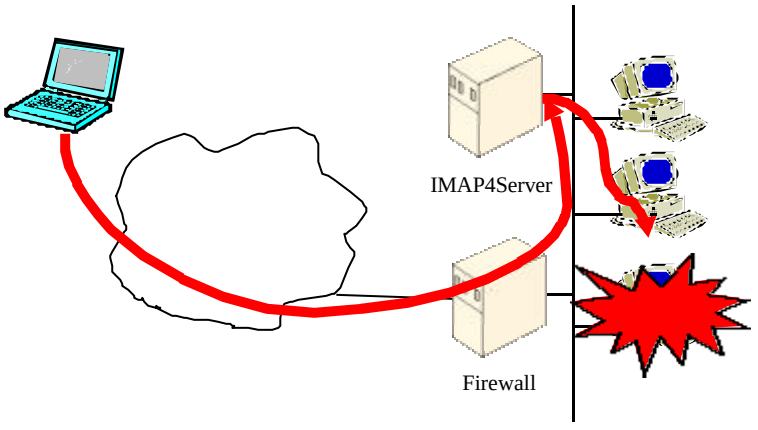
S/MIME PGP

Orangesoft

暗号メールの基本

- なぜ、電子メールに暗号が必要か
  - 理由は明確
  - 暗号で解決できるのか？
- Firewallでは守れないのか?
  - 電子メールはFirewallを通過してやってくる
  - SMTP、POP、IMAP4はFirewallを通過して通信する
- 暗号化すれば安全か
  - 暗号は破られないのか？
- 自分が出したメールでないことを証明する
  - 他人が自分のアドレスを勝手に使用

Orangesoft



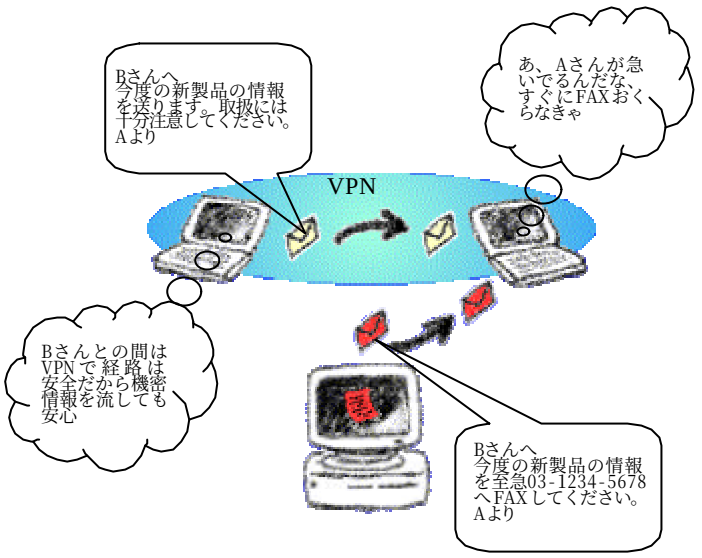
Orangesoft

改竄はどこで行われるか?

- 送信時のメールサーバ
- 相手先のメールサーバ
  - 中継中のサーバー
- 受信後の自分のPC
  - ローカルファイルの改竄

Orangesoft

Orangesoft



Orangesoft

暗号に必要な技術

- 暗号技術
  - 共通鍵暗号
    - DES,3DES,RC2,RC4,IDEA,MISTY,FEAL
  - 公開鍵暗号
    - RSA,Diffie-Hellman,ElGamal
- ハッシュ関数
  - SHA-1 ,MD5

Orangesoft

共通鍵暗号と公開鍵暗号

- 共通鍵暗号
  - お互いが同じ鍵を使用する
    - 相手が多いと鍵交換が面倒
    - 処理速度は速い
- 公開鍵暗号
  - 秘密鍵と公開鍵の2つを使用する
    - 公開鍵は誰にでも公開できる
    - 秘密鍵の管理が重要
    - 処理速度は遅い

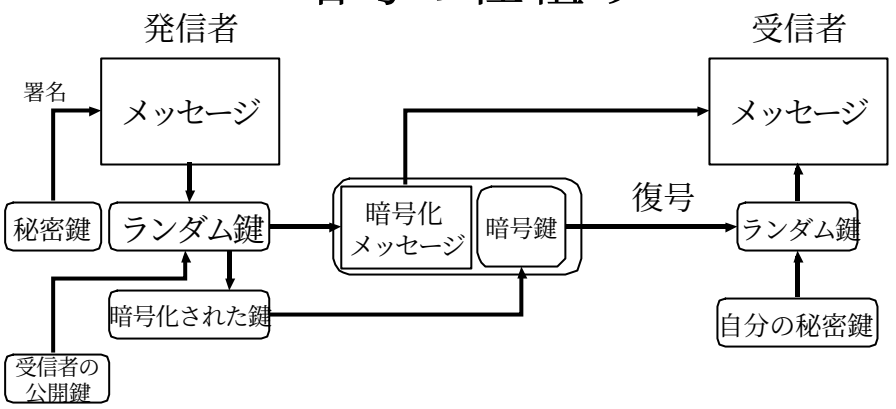
Orangesoft

暗号化

- 公開鍵暗号と、共有鍵暗号の組合わせ
- ランダム鍵でメッセージを暗号化
- 公開鍵でランダム鍵を暗号化
  - 人数分の公開鍵で暗号化する

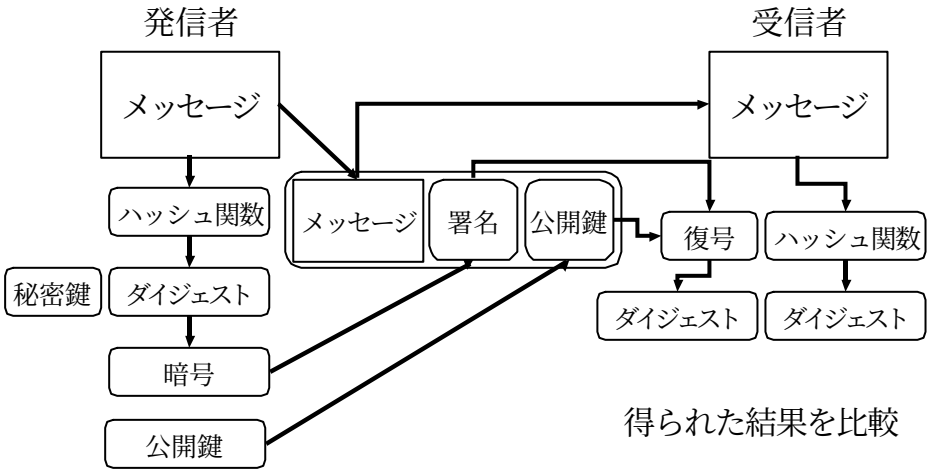
Orangesoft

暗号の仕組み



Orangesoft

電子署名の仕組み



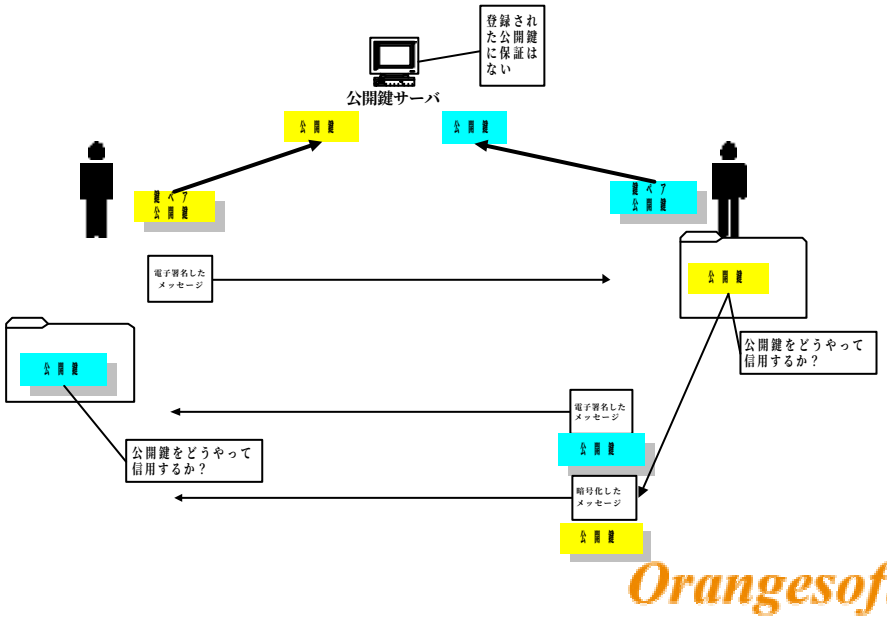
Orangesoft

S/MIME,PGPの認証の違い

- PGP
  - 公開鍵に対する認証はお互いが信用に基づく
  - 信頼の輪
    - 信用できる証明者
  - PGP5.5
- S/MIME
  - 公開鍵に信頼できる機関による認証が行われる
    - 認証局による証明書の発行
  - Netscape Communicator,OutlookExpress,Winbiff等々

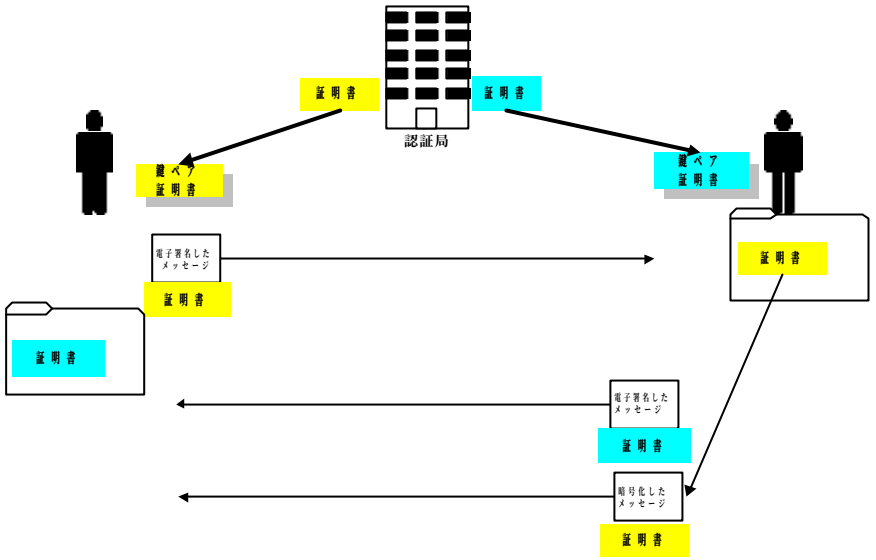
Orangesoft

PGPでの鍵交換



Orangesoft

S/MIMEでの鍵交換



Orangesoft

安全な公開鍵の交換

- S/MIME
  - 認証局による証明書を信用する
  - 認証局をどうやって信用するか?
- PGP(S/MIME)
  - Finger Printを使用する
    - 公開鍵を送った後に電話などでお互いに確認する

Orangesoft

公開鍵はいつ無効になるか

- 秘密鍵の紛失
- 証明書の期限切れ
  - 認証局の証明書の期限切れ
- 退職等
- 秘密鍵を盗まれる

Orangesoft

秘密鍵の管理

- 各クライアントで生成するか?
- 管理者がまとめて生成するか?
- 秘密鍵の管理はユーザまかせか?
  - 鍵を紛失したときにどうするか?
- システム管理者が全員の鍵を管理するか?
  - 誰の権限で管理するか?

Orangesoft

CRLの運用
Certification Revocation List

- どうやって配布するか?
  - LDAP
- いつ配布(取得)するか?
  - オフラインの時はどうするか?
- すべてのCRLを公開してもいいのか?

Orangesoft

日本語での問題

- 電子署名時の漢字コードの問題
  - 電子署名時のコードと配送時のコード
- 標準はISO-2022-JPに電子署名
  - 配送中のMTAは**絶対**にコードを変換しない
- MTAによるcharset等の書換えも行わない
  - 他の弊害が発生する可能性もある

Orangesoft

今後の普及に期待

- MDNs(RFC2298)
  - Message Disposition Notifications
- DSNs(RFC1894)
  - An Extensible Message Format for Delivery Status Notifications)

Orangesoft

配達通知,開封確認は必要か?

- グループウェアではできる
  - Internetメールは開封確認がないから使えない
- 見たことを知られたくない時もある
  - プライバシ問題?
  - 仕事では必要か
- クライアントの実装では開封確認を出すかどか選択できるようにしよう

Orangesoft

```
Received: from orangesoft.co.jp (dhcp75.orangesoft.co.jp [202.223.0.75])
        by orangegw.orangesoft.co.jp (8.9.3/3.7W) with ESMTP id PAA09658
        for <kitarou@orangesoft.co.jp>; Sat, 13 Nov 1999 15:22:20 +0900 (JST)
Message-ID: <382D0395.689C5DD3@orangesoft.co.jp>
Disposition-Notification-To: nonki <nonki@orangesoft.co.jp>
Date: Sat, 13 Nov 1999 15:22:13 +0900
From: nonki <nonki@orangesoft.co.jp>
X-Mailer: Mozilla 4.6 [ja] (WinNT; I)
X-Accept-Language: ja
MIME-Version: 1.0
To: kitarou@orangesoft.co.jp
Subject: MDNs
Content-Type: text/plain; charset=iso-2022-jp
Content-Transfer-Encoding: 7bit
```

Orangesoft

SMTPでの認証の必要性

- 本来はMTA,MTA間の転送が目的
- なぜかMUAも使いはじめた
  - 認証がないので誰でも利用できてしまう
- POP before SMTPの登場
  - でも、これって本当に解決?
- AUTH SMTPを実装しよう

Orangesoft

電子メールは相互接続が重要

- サーバ、クライアント間の接続
  - SMTP,IMAP,LDAP
- End To Endの接続
  - MIME,S/MIME
- 利用者は増える一方
  - ほとんどが一般ユーザ
- 今後も様々な接続テスト等を実施し行きたい

Orangesoft