S/MIME：なりすまし、PPAP問題を解決したメール送受信を実現

Japan Security Summit 2023

2023年10月

S/MIME推進協議会　事務局
諸角昌宏

アジェンダ

1. S/MIME概要
2. S/MIME導入に向けての5つのアプローチ
3. S/MIME推進協議会　3つの提言
4. S/MIME推進協議会　活動内容

1. S/MIME概要

- S/MIMEとは？
  - MIMEでカプセル化した電子メールの公開鍵方式による暗号化とデジタル署名に関する標準規格
  - 要は、電子メールソフト（OutlookやThunderbirdなど）に、電子証明書と呼ばれる暗号化技術を使って、なりすまし防止（真正性）およびメールの機密性の保護を行えるようにしたもの

  - メールが抱えている問題とは？
    - 送信者を偽ることができる（いわゆる、なりすましが可能）
    - 送信者から受信者まで（いわゆるエンドツーエンド）の経路全体にわたって機密性を保証することは困難

S/MIME概要

- S/MIMEでできること
  1. メール送信者のなりすまし防止
     送信者が、送信するメールに電子証明書を付与。受信者は、その電子証明書に含まれる公開鍵を使用して電子署名を確認することで、そのメールが本当に送信者が送ったメールであることを確認可能。
  2. メールの改ざん検知
     電子証明書が付与されたメールが通信経路上で改ざんされた場合に、その改ざんを検知。
  3. メールの暗号化（メール本文および添付）
     送信者と受信者が、あらかじめ双方の電子証明書を交換。
     送信者は、受信者の電子証明書に含まれる公開鍵を使用して暗号化。受信者に対して安全にメールを送ることが可能。

2. S/MIME導入に向けての5つのアプローチ

1. メール配信サービスのS/MIME化
2. 会社でS/MIMEをスモールスタートする方法
3. 会社全体でS/MIME化を行う方法
4. 外資系企業でS/MIME化を行う方法
5. 個人でS/MIME化を行う方法

S/MIME導入に向けてのアプローチ(1)
メール配信サービスのS/MIME化

企業・組織がマーケティングやセールスのために配信するメールにS/MIMEの電子証明書を付与

- 2つのケース
  1. メール配信サービスを利用しているケース
     - 利用しているサービス提供ベンダーに、S/MIME対応を依頼
     - あるいは、別のS/MIME対応サービスに切り替える
       https://www.s-mime.jp/%e3%83%a1%e3%83%bc%e3%83%ab%e9%85%8d%e4%bf%a1%e3%82%b5%e3%83%bc%e3%83%93%e3%82%b9%e3%82%92s-mime%e5%8c%96%e3%81%99%e3%82%8b/
  2. 自組織でメーリングリストを管理しているケース
     - IT部門と協調してS/MIME対応を進める
     - 基本的には、配信メールアドレスに電子証明書を付与することで可能
     - 注意点
       - 送信時に送信元(From)を別のメルアドに変更していないかどうかの確認
       - 送信時にメール本体に変更を加えたりしていないかどうかの確認

S/MIME導入に向けてのアプローチ(2)
会社でS/MIMEをスモールスタートする方法

全社でS/MIME対応を行うことが難しい場合、一部の人からS/MIME対応を始める

- S/MIMEを始める際に検討するメールアカウント
  1. 外部からの問い合わせに対してやり取りを行うメールアカウント（例：info@xxx.co.jp）
  2. 頻繁に外部とやり取りを行う人のメールアカウント（例：役員）
  3. 有志がまずS/MIME対応を始める
- 方法
  - 個人のメールアカウントベースになるので、S/MIME対応の知識がある人が行う、あるいは、知識のある人のサポートが受けられる人から行う
  - 参考： https://www.s-mime.jp/s-mime%e5%af%be%e5%bf%9c%e3%83%a1%e3%83%bc%e3%83%ab%e3%82%bd%e3%83%95%e3%83%88/
- 注意点
  - 事前にIT部門に連絡し承認を得る。
  - 個人ではなく会社としての電子証明書を入手する

S/MIME導入に向けてのアプローチ(3)
会社全体でS/MIME化を行う方法

会社全体でS/MIME対応を行う（理想型）

- 課題
  - 社員一人一人が自分のメールアカウントに電子証明書を付与・管理することは困難。一括して管理者が設定できるようにする。
- 方法
  - 管理ソフトを使ってメールアカウントおよび電子証明書を一括管理する
  - 提供されているソリューションを利用（以下参照）
    https://www.s-mime.jp/%e7%b5%84%e7%b9%94%e3%81%a7%e3%81%ae%e5%88%a9%e7%94%a8%e6%96%b9%e6%b3%95/

S/MIME導入に向けてのアプローチ(4)
外資系企業でS/MIME化を行う方法

外資系企業で、海外にある本社がIT管理を行っているためS/MIME化が難しいのではないか？

- 方法
  - 日本の社員のメールアカウントごとにS/MIME設定することが可能。
  - S/MIME用の電子証明書は、日本独自に日本支社として取得する。
  - やり方としては、(2)スモールスタートの方法が取れる。
- 注意点
  - 海外本社のIT部門に事前に連絡して確認しておく必要がある

S/MIME導入に向けてのアプローチ(5)
個人でS/MIME化を行う方法

組織ではなく個人のメールアカウントに独自にS/MIME設定を行う。

- 方法
  - 個人のメールアカウントごとにS/MIME設定を行う。
  - S/MIME用の電子証明書は、個人で取得する。
- 注意点
  - ウエブメール系、Gmail（無料版）等ではS/MIMEがサポートされていない。
    OutlookやThunderbirdなどS/MIMEをサポートしているメールソフトを使用することが必要。
    以下、S/MIMEをサポートしているメールソフトの情報
    https://www.s-mime.jp/s-mime%e5%af%be%e5%bf%9c%e3%83%a1%e3%83%bc%e3%83%ab%e3%82%bd%e3%83%95%e3%83%88/
  - 以下の作業は利用者自身で行う必要がある
    - メールソフトの設定（POP/IMAP,SMTP等）
    - S/MIME用電子証明書のメールソフトへの登録
    - 複数のPCあるいはスマホにそれぞれ電子証明書の登録・設定が必要となる

S/MIME導入に向けてのアプローチ(補足)

- 設定・管理に不安がある場合には、まず無料の電子証明書を取得して、設定・テストを行い、うまくいってから有料の電子証明書に切り替える方法がある
  - 無料の電子証明書はActalisから入手可能
  - 無料の証明書と有料の証明書の違いは、本人確認ができているか。
    以下のウエブページを参照
    https://www.s-mime.jp/s-mime%e8%a7%a3%e8%aa%ac/%e7%84%a1%e6%96%99%e3%81%ae%e9%9b%bb%e5%ad%90%e8%a8%bc%e6%98%8e%e6%9b%b8%e3%81%a8%e6%9c%89%e6%96%99%e3%81%ae%e9%9b%bb%e5%ad%90%e8%a8%bc%e6%98%8e%e6%9b%b8%e3%81%ae%e9%81%95%e3%81%84/

- S/MIME対応がうまくいかない、問題を起こしてしまう場合
  - メールソフトにてS/MIME用電子証明書の付与を止めることで通常のメールとして配信可能

3. S/MIME推進協議会　3つの提言

1. セキュリティ3要素　→　セキュリティ7要素

2. メールチェックは電子証明書から

3. 真正性の文化＝全員参加型セキュリティ

提言1:セキュリティ3要素　→　セキュリティ7要素

情報セキュリティは、7要素で語っていこう！

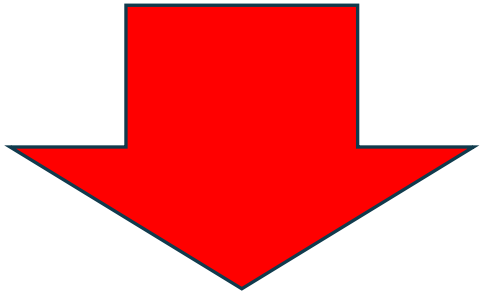
CIA　⇒　CIA　＋　4要素

JIS Q 27000　3.28　情報セキュリティ（information security）
情報の機密性（3.10），完全性（3.36）及び可用性（3.7）を維持すること。
注記 さらに，真正性（3.6），責任追跡性，否認防止（3.48），信頼性（3.55）などの特性を維持することを含めることもある。

- **真正性(authenticity)** :
  - エンティティは，それが主張するとおりのものであるという特性。
- 責任追跡性(accountability)　:
  - あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できる事を確実にする特性。
- 否認防止(non-repudiation) :
  - ある活動又は事象が起きたことを、後になって否認されないように証明する能力
- 信頼性(reliability):
  - 情報システムによる処理に欠陥や不具合がなく、期待した処理が確実に行われている特性

提言2：**メールチェックは電子証明書から**

- 「XXXをかたるフィッシングメールに注意してください」



- **「** XXXをかたるフィッシングメールに注意してください。**メールをチェックする際はまず電子証明書が付与されているかどうかを確認して下さい。電子証明書が付与されていないメールは不正なメールです」** と言える世界を作っていこう！

提言3：**真正性の文化＝全員参加型セキュリティ**

- *文化（ぶんか、ラテン語: cultura）には、いくつかの定義が存在するが、総じていうと人間が社会の構成員として獲得する多数の振る舞いの全体のことである。社会組織（年齢別グループ、地域社会、血縁組織などを含む）ごとに固有の文化があるとされ、組織の成員になるということは、その文化を身につける（身体化）ということでもある。* (WikiPediaから引用)

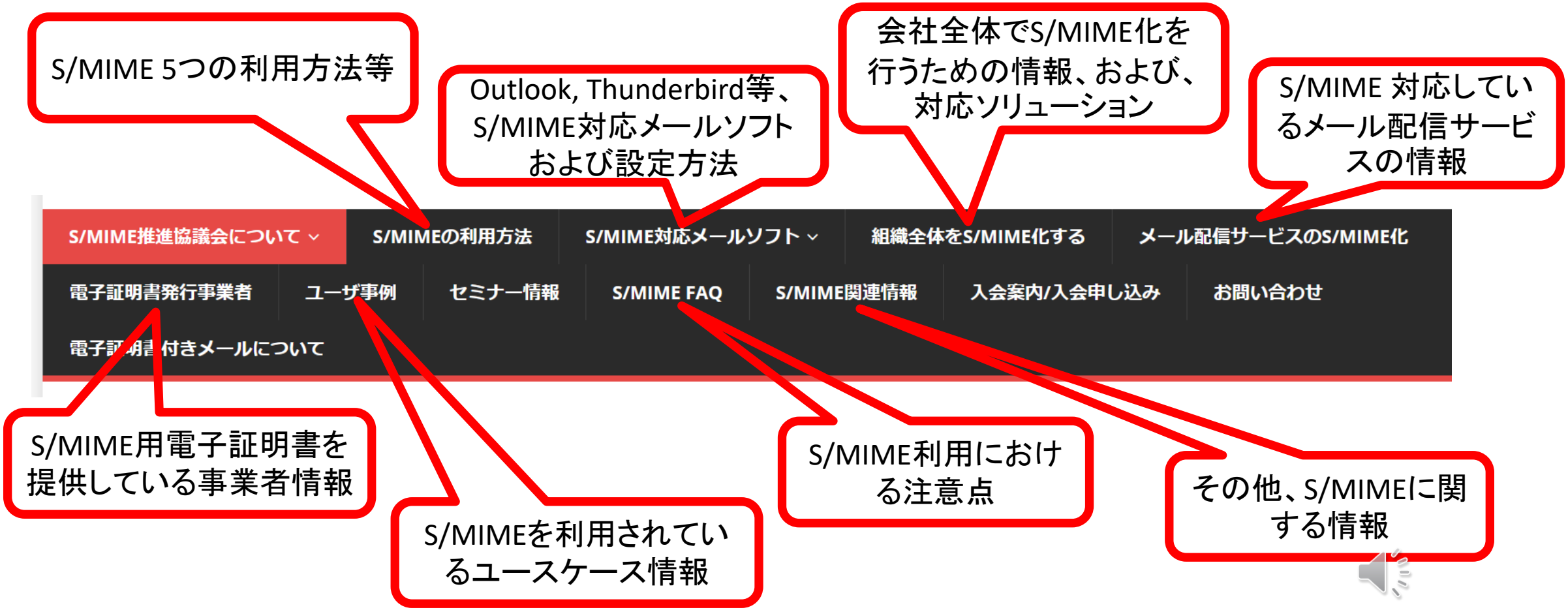
- **「真正性の文化」を築く**のは、一人一人の意識です。すべての人が電子的に情報発信する際には、**証明できる形で自分であることを表明する**ことが重要です。

4. S/MIME推進協議会 活動内容

S/MIME推進協議会では、以下の活動を通してS/MIME普及のための情報発信、啓発活動を行う。

1. **情報発信（ウエブサイト）**
   - S/MIMEの導入・利用方法に関する管理的な情報
   - S/MIME、メールサーバーレベルのソリューション情報
   - S/MIME、メールクライアントの情報
   - S/MIME、電子証明書発行事業者の情報
   - S/MIME、ユースケース
   - ブログ、その他の情報
2. **啓発活動**
   - セミナー開催（会員、非会員すべてを対象： 非定期）
   - S/MIME勉強会開催（会員、非会員すべてを対象： 2～3か月に1回）
   - S/MIME研究会開催（会員向け。S/MIME関連情報の共有等を実施： 毎月の月例会）
   - ニュース配信（会員向け。S/MIME関連情報のメール配信： 非定期）
3. **S/MIME普及の阻害要因に対するアプローチ**
   - メールソリューションのS/MIME対応の促進
   - その他、S/MIME対応の促進を妨げる要因へのアプローチ

S/MIMEの主な情報（ホームページ）



よろしくお願いします！