デジタル複合機のセキュリティ

2009/3/12

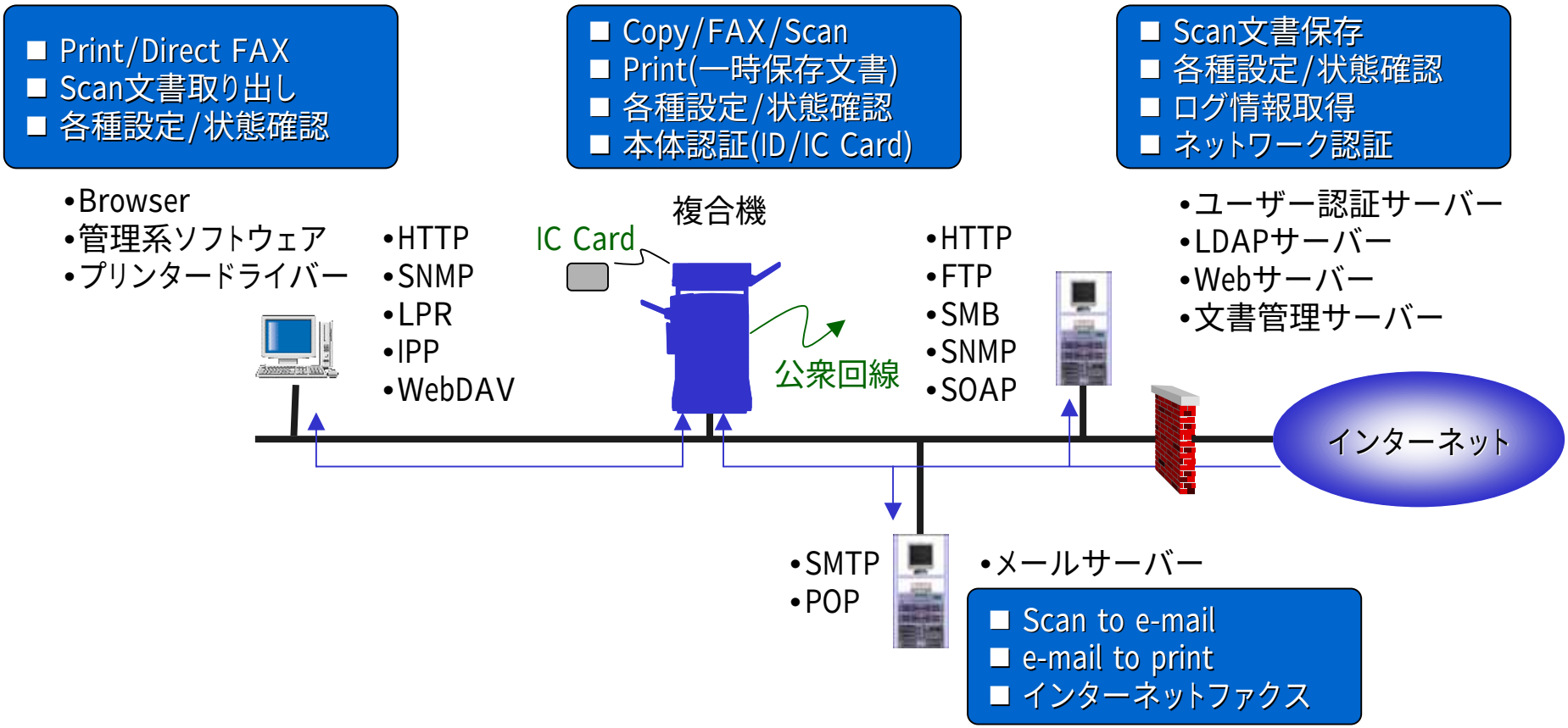
(社) 電子情報技術産業協会　TCG専門委員会
委員 斎藤 宏之 (富士ゼロックス株式会社)

内容

1. デジタル複合機の特徴
2. 保護資産と脅威
3. SSL/TLS
4. S/MIME
5. 電子文書セキュリティ
6. IPsec、SNMP、HDD暗号化
7. IEEE P2600

デジタル複合機の特徴

- 基本機能　：Copy、Print、FAX、Scan機能
- 高機能化　：PCやServerが備える機能・・・Web Server、Browser、Server access、etc



保護資産と脅威

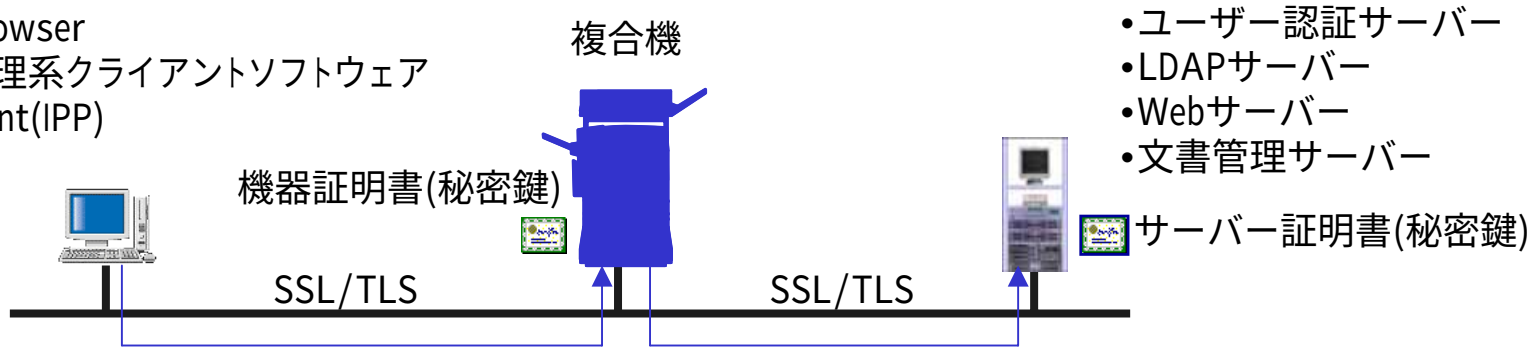
JEITA

- IT機器として　：不正アクセスによる参照･消去･改ざん･盗聴、可用性への攻撃
- 複合機特有　　：紙文書、課金情報

種 別	保 護 資 産	脅 威 例
文書	紙文書、電子文書(HDD内･通信路)	不正コピー、不正アクセス(参照･消去･改ざん･盗聴)
利用者データ	アドレス帳、認証情報	不正アクセス(参照･消去･変更･盗聴)
設定データ	複合機設定、機器証明書(秘密鍵)、権限情報	不正アクセス(参照･消去･変更･盗聴)
ログ	各種ログ	不正アクセス(参照･消去･改ざん･盗聴)
プログラム	複合機の制御･処理を行うソフトウェア	不正更新
課金情報	使用量、部門付け替え情報	不正アクセス(消去･改ざん･盗聴)
物理的資産	HDD	解析
提供機能	可用性	不正利用、過負荷攻撃
IT環境	他のIT機器･サービス	複合機を踏み台として攻撃

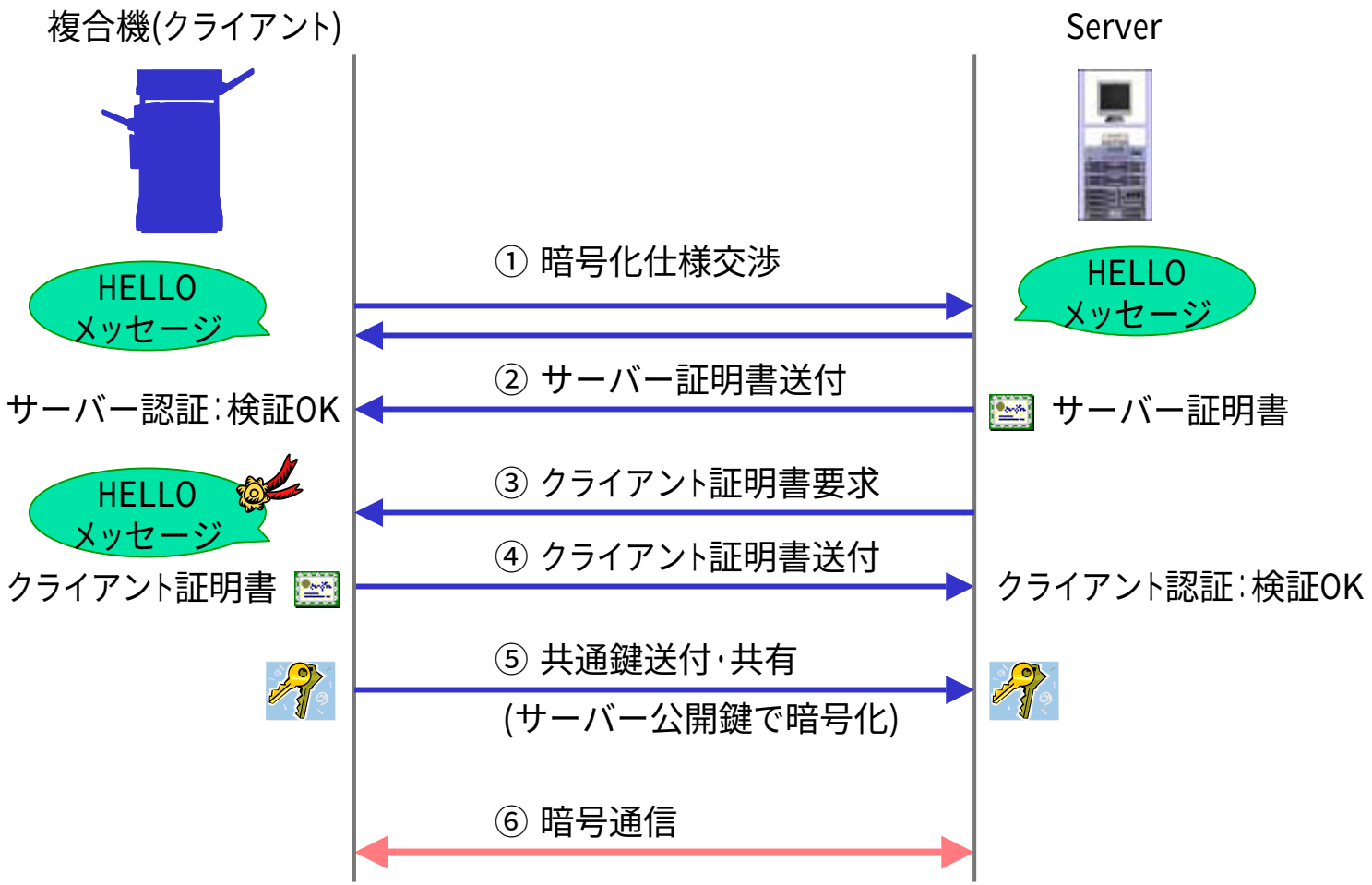
ネットワークセキュリティ SSL/TLS (1)

- SSLサーバー機能
  - クライアントから複合機のリモート管理機能/プリント機能/複合機内部蓄積文書へのアクセスを行う場合の通信を暗号化。複合機の機器証明書利用。
- SSLクライアント機能
  - 複合機からのWebアクセス/プッシュスキャン/ネットワーク認証を行う場合の通信を暗号化。
  - サーバー認証/クライアント認証に対応。



ネットワークセキュリティ SSL/TLS (2)

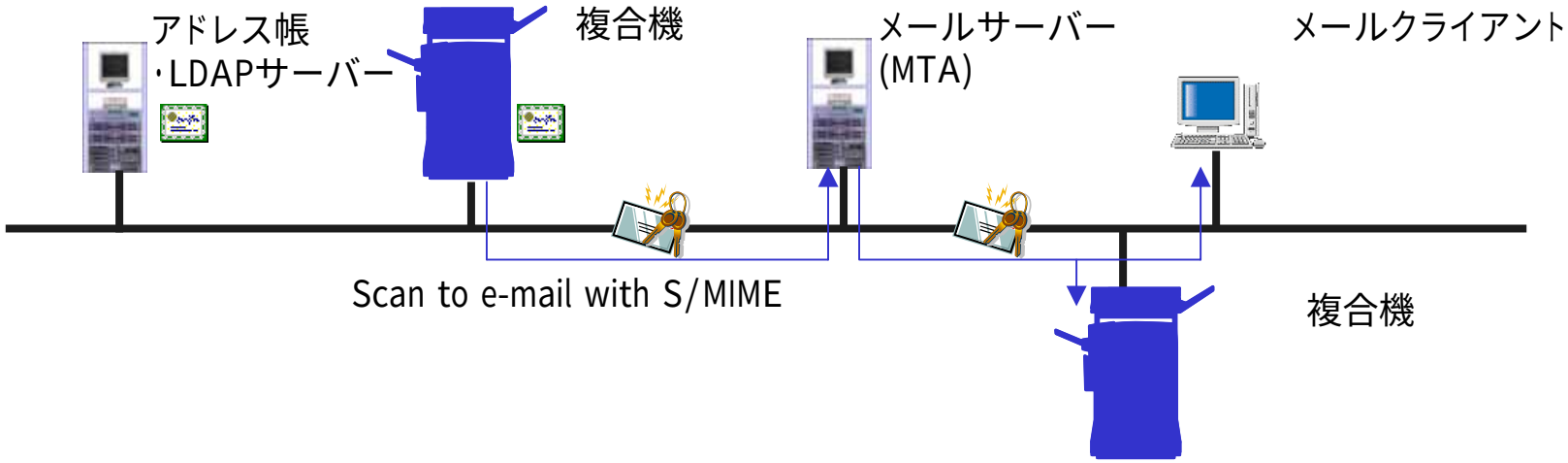
■ PCとサーバのSSL通信同様のネゴシエーションを行う。



ネットワークセキュリティ S/MIME (1)

■ 複合機が送受信するメールの暗号/署名に対応

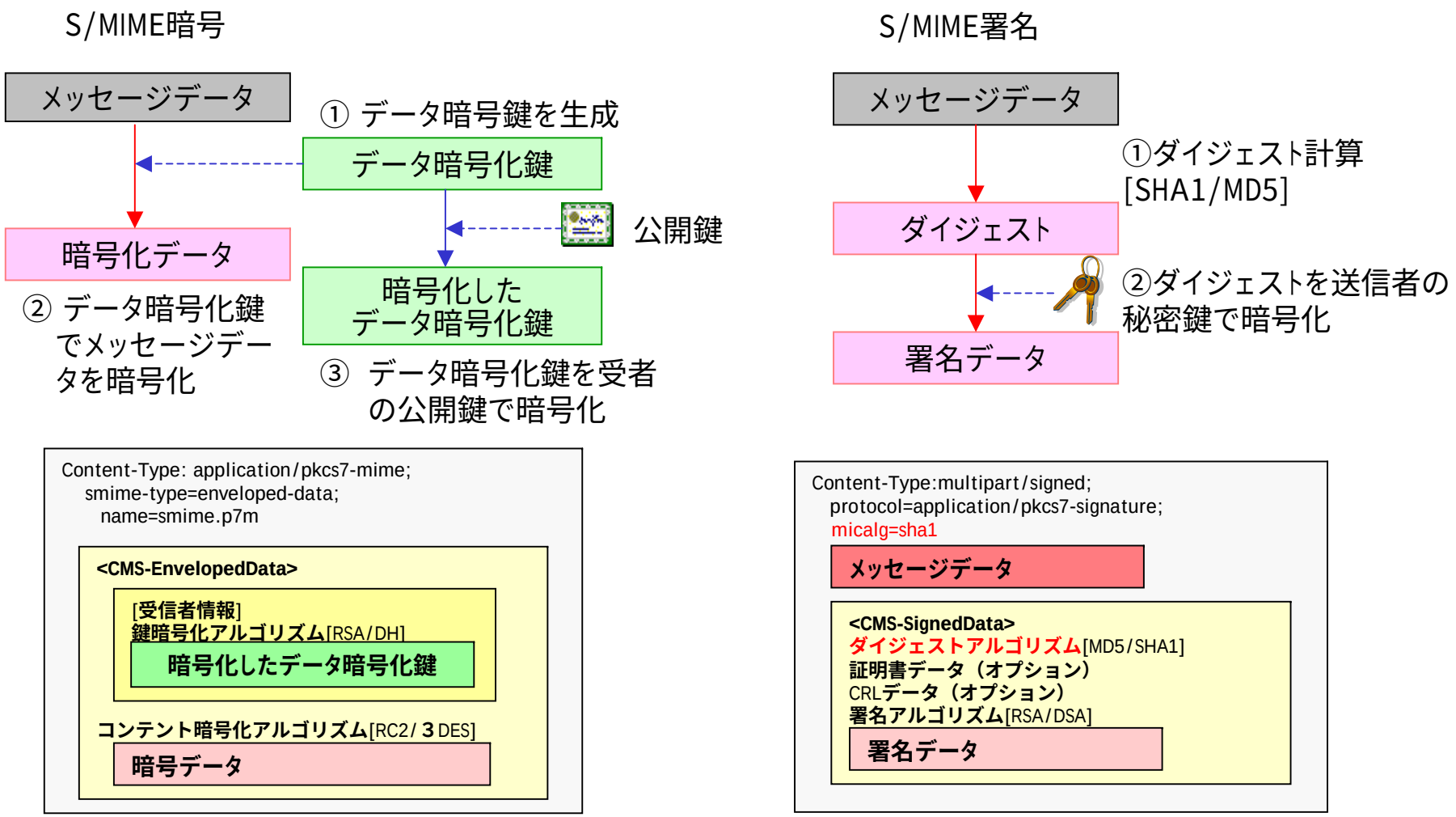
- メール送信時
  宛先の公開鍵で暗号化、複合機の秘密鍵で電子署名
- メール受信時
  複合機の秘密鍵で復号、送信者の公開鍵で署名検証/なりすまし検知
- Internet FAXも同様



MTA ：Mail Transfer Agent メール転送エージェント

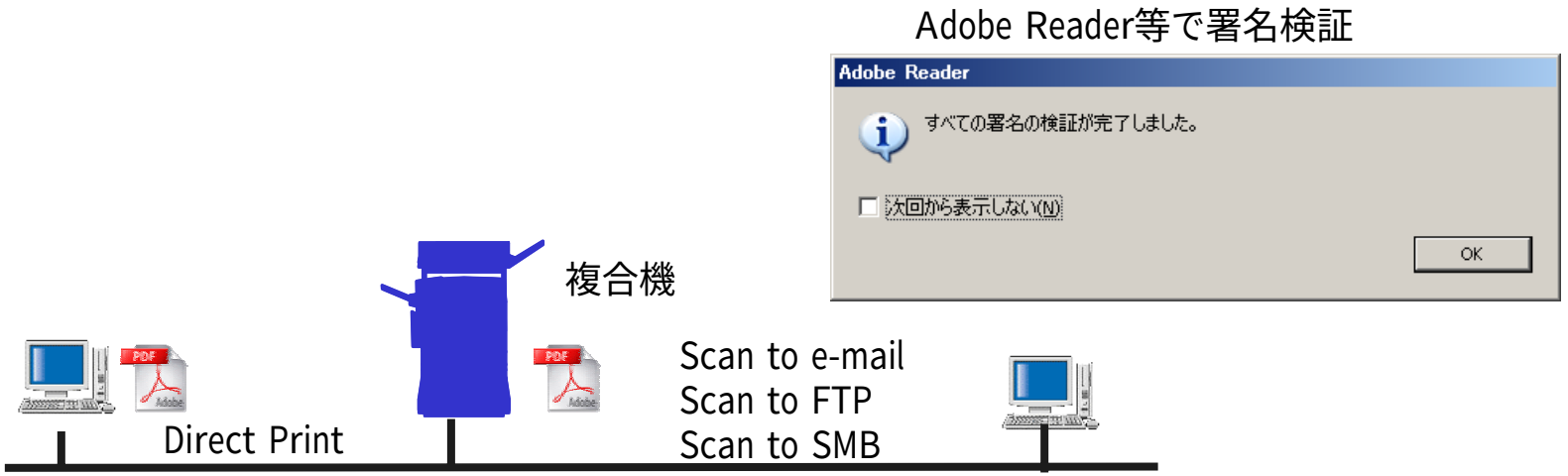
ネットワークセキュリティ S/MIME (2)

■ 電子メールのMIME規格の拡張版 Secure Multipurpose Internet Mail Extensions



電子文書セキュリティ

- Scan(PDF)
  - パスワード暗号　　：パスワードを使って暗号化
  - PKI署名　　：デバイス証明書を使って電子署名
  - 操作制限　　：操作（文書編集/印刷/コピー）を制御
- Print(PDF)
  - パスワード暗号　　：パスワード暗号化されたPDF文書を複合機に設定された
    パスワードで復号して、PDFダイレクトプリント



IPsec、SNMP、HDD暗号化

■ IPSec

- ➢ IPパケット単位で暗号化を行うプロトコル。
- ➢ IKE認証がデジタル署名方式の場合、IPsec用証明書として、複合機の機器証明書を利用。
- ➢ IPv6 Ready Logo Program Phase-2 ：IPsecを含めた認定。

■ SNMP v3

- ➢ IPネットワーク上のネットワーク機器を監視･制御する通信プロトコル。
- ➢ Version 3で、セキュリティ機能が強化
  1. メッセージの完全性　：パケットの完全性チェックによる改竄検出。
  2. 認証　：メッセージが正当なソースから発信されたかどうかを判別。
  3. 暗号化　：パケットの暗号化。

■ ハードディスクの暗号化

- ➢ HDDに一時保存される電子文書やデータの暗号化と復号を行う。
- ➢ AESの利用が多い。
  - ● Advanced Encryption Standard：米国政府の次世代標準暗号化方式
  - ● 日本の電子政府推奨暗号リストの1つ

IEEE P2600 概要

- IEEEのPWGの下部組織として発足。
- HardCopyデバイス(MFP/複写機/Printer/Scanner)とそのシステムに関するセキュリティ要件を定義する。
  - Main-Body : IEEE標準
  - Annexes : PP(Protection Profile)のISO/IEC15408評価、PPの認証取得を目指している。2009年1月末評価終了、2月末 NIAP VOR の計画。
- 参加企業
  - Chair : Lexmark
  - Vice Chair : Canon
  - Secretary&Editor : Ricoh
  - Editor : Lexmark

  Brooktrout、Equitrack、HP、IBM、NetSilicon、Print4Sight、Oce、Xerox、O2 Micro Epson、Kyocera-Mita 、FujiXerox、Sharp、Toshiba、Okidata、Konica Minolta
- '04.3～'09.2まで、41回開催。 過去2回は、東京。
- TCG Hard Copy WGと同一場所で連続した日程の開催もあり。

IEEE P2600 PP

JEITA

- P2600.1 Protection Profile for Operational Environment A

  高度な文書セキュリティ、操作アカウンタビリティ、情報の保証などが必要な、制限された情報を扱う環境を想定したもの。商取引、基幹業務、法規制の対象で扱われる情報。

- P2600.2 Protection Profile for Operational Environment B

  日常的な文書・ネットワークセキュリティが必要な一般企業を想定したもの。

- P2600.3 Protection Profile for Operational Environment C

  文書セキュリティの保証は必要としないが、アクセス制御や利用量などを重要視する、コピーセンター、図書館、インターネットカフェなどの公共の場を想定したもの。

- P2600.4 Protection Profile for Operational Environment D

  SOHOなどの小規模な環境を想定したもの。

※ 認証完了の見込みは、‘09.3.15。 (http://www.niap-ccevs.org/cc-scheme/in_evaluation/)

※ PP-Aは、NIAPのドラフトレポートで、テクニカルな問題はないことが確認された模様。(‘09.2.25)
(http://grouper.ieee.org/groups/2600/)

ご清聴ありがとうございました。