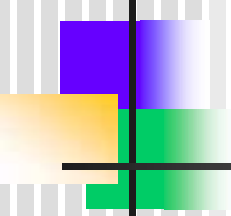


MOF2008合同デモシステム向け セキュリティ報告

XMLコンソーシアムDay 2009年01月09日
セキュリティ部会
大沼啓希(日本アイ・ピー・エム株式会社)
松永 豊 (TELデバイス)



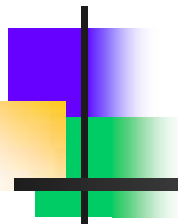


ご説明内容

- 生産工場のセキュリティに対する取り組み – 経緯と概要
- MOF2008合同デモシステム向けセキュリティ報告書
- MOF2008概要
- MOF2008合同デモシステム向けセキュリティ報告書 目次
- オープンソースのツールによる暗号化実践
- 今後の計画



生産工場のセキュリティに対する 取り組み – 経緯と概要



生産工場のセキュリティに対する取り組み

- アライアンス・パートナーとの協調活動として、生産工場のセキュリティに関する取り組みを行ってきました



製造業XML推進協議会



PSLXフォーラム

- 2007年 システム コントロール フェア (SCF) 2007

- [セキュリティ検討報告書](#)
- 合同デモシステムについてセキュリティ上のリスクを分析し対策を検討

- 2008年 Manufacturing Open Forum (MOF) 2008

- [合同デモシステム向けセキュリティ報告書](#)
- 暗号化と電子署名について具体的な手段を検討して報告



SCF2007製造情報連携デモシステム セキュリティ検討報告



製造情報連携フォーラム SCF2007 デモシステム向け
セキュリティ検討報告書

2007 年 11 月
XML コンソーシアム
セキュリティ部会

1. はじめに.....	2
1.1. 概要.....	2
1.2. 対象.....	2
1.3. XMLに関するセキュリティ.....	2
1.4. 検討メンバー.....	3
2. 現状分析 = リスク分析.....	3
2.1. リスク分析の手順.....	3
2.2. 3つの重点課題.....	3
2.3. リスクの種類.....	3
2.4. シナリオ分析.....	4
2.5. モジュールごとのリスク.....	7
3. 対策.....	8
3.1. 方針.....	8
3.2. リスクごとのセキュリティ対策技術.....	9
3.3. 全体のセキュリティ対策.....	10
3.4. XMLデータの保護.....	11
3.5. モジュールごとのセキュリティ対策.....	12
4. セキュリティ対策の評価.....	14

■システム コントロール フェア 2007

– 2007/11/13(火) ~ 16(金) 東京ビッグサイト

– 主催：社団法人 日本電機工業会 (JEMA)、社団法人 日本電気制御機器工業会 (NECA)

■XMLコンソーシアムのセキュリティ部会が製造情報連携フォーラムの合同デモシステムに対してセキュリティ面の対策を検討 → 報告

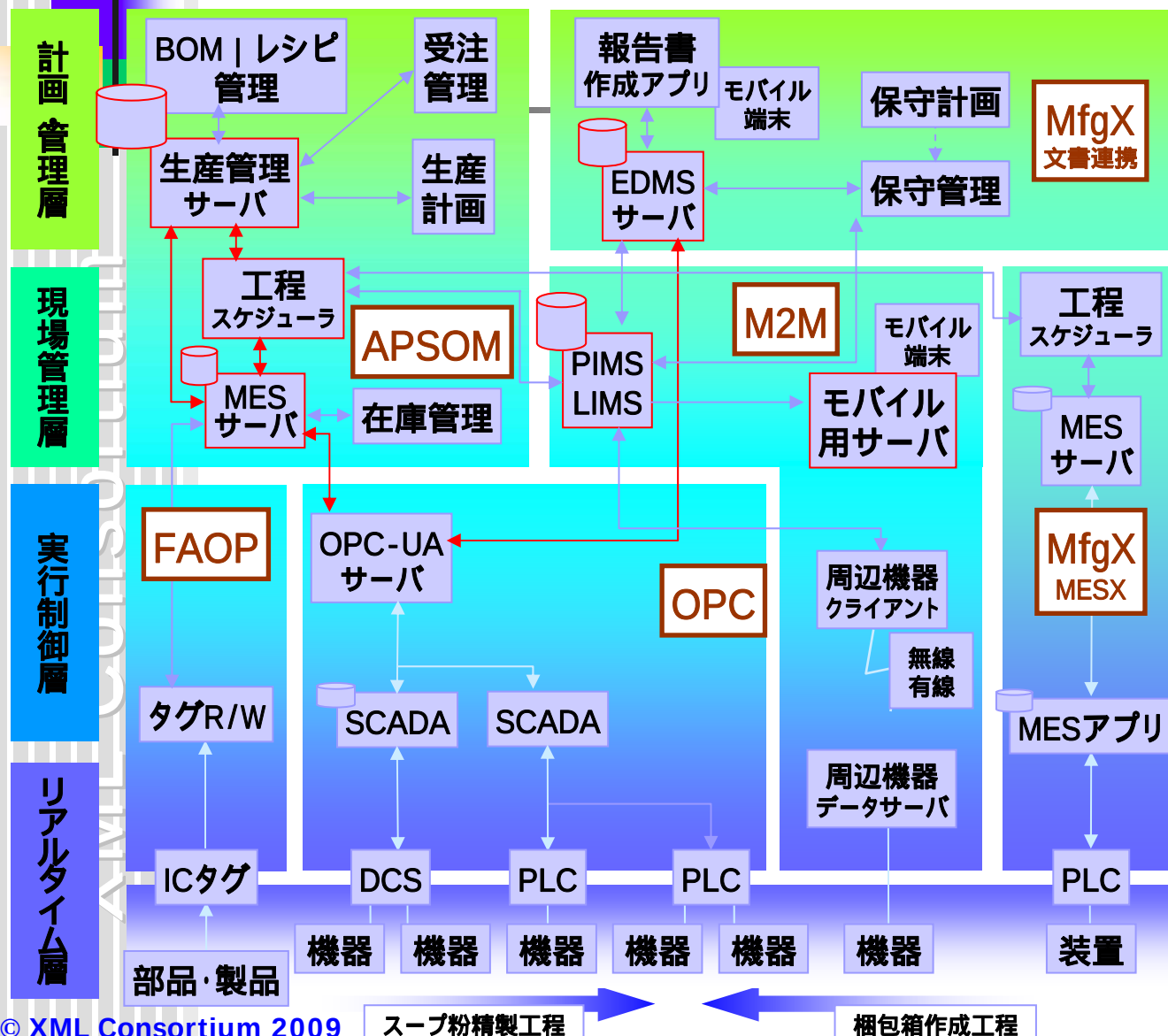
報告書：

<http://www.xmlconsortium.org>



Security Sig
09-JAN-2009

モジュールごとの セキュリティ対策 - 全体像



●アクセス制御

●DB監査ログ
●重要なデータの暗号化

●メッセージ保護



MOF2008概要

- <http://www.mstc.or.jp/iaf/mof2008/>
- 名称: マニュファクチャリング オープン フォーラム2008 (MOF2008)
- 会期: 2008年9月10日(水) ~ 9月12日(金) 10:00 ~ 17:00
- 場所: 東京ビックサイト(東京国際展示場)
会議棟6F (サミット、セミナー、パネルディスカッション)、
東1ホール (展示)
- 主催: I A懇談会 (I A: Industrial Automation)
- 共催: (社) 日本能率協会
(社) 計測自動制御学会 産業応用部門
計測・制御ネットワーク部会
(財) 製造科学技術センター
- 協賛: XMLコンソーシアム
バーチャル・エンジニアリング・カンパニー (VEC)



MOF2008合同デモシステム向けセキュリティ報告書

<http://www.xmlconsortium.org/>



XML Consortium Top - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り

アドレス(D) <http://www.xmlconsortium.org/> 移動

XML コンソーシアム

HOME 会員の窓 セミナー情報 プレスリリース XML 関連情報 ご紹介 Introduce

現在の会員数...154会員

- ・会員一覧
- ・アライアンスパートナー一覧
- ・会員製品一覧

入会のご案内

- ・ノックアウト(PDF 25KB)

部会活動

- ・セキュリティ部会
 - 活動要綱
 - 開催案内: 第5回 11/19(水) 公開ブログ
- ・Webサービス実証部会
 - 活動要綱
 - 開催案内: 第6回 11/19(水) 公開ブログ
- ・Web2.0部会
 - 活動要綱
 - 開催案内: 第6回 12/10(水) 公開ブログ
- ・SOA部会
 - 活動要綱
 - 開催案内: 第5回 11/20(木) 公開ブログ
- ・ビジネス・イノベーション研究部会
 - 活動要綱
 - 開催案内: 第5回 11/20(木) 公開ブログ
- ・クロスメディア・パブリッシング部会

トピックス、主催イベント、関連イベント

■トピックス、主催イベント

- ・1月9日(金) 第10回XMLコンソーシアムDay
- ・12月18日(木) XMLコンソーシアムセミナー 「エンタープライズマッシュアップ、次世代クライアント製品徹底検証」(Part2)
- ・12月17日(水) XML設計技術勉強会(第七回) <会員限定>
- ・12月2日(火) 「XMLコンソーシアム エバンジェリストブログ」を開始
- ・11月28日(金) XMLコンソーシアムセミナー 「エンタープライズマッシュアップ、次世代クライアント製品徹底検証」(Part1)
- ・11月20日(木) XML設計技術勉強会(第六回) <会員限定>
- ・11月10日(月) メルマガ発行 → <会員専用>、<一般公開版> ◆メルマガ購読方法:<会員会社の方>、<会員会社以外の方>
- ・10月31日(金) XMLコンソーシアムセミナー ～XMLマスタープロフェッショナル (アプリケーション開発)直前対策セミナー～

Webサービス関連

- ・技術解説書
- ・開発ガイド
- ・観光情報Webサービス実証プロジェクト資料
- ・TravelXML利用Webサービス実証実験プロジェクト成果資料
- ・道路交通情報Webサービスを使った複合Webサービス実証実験成果資料

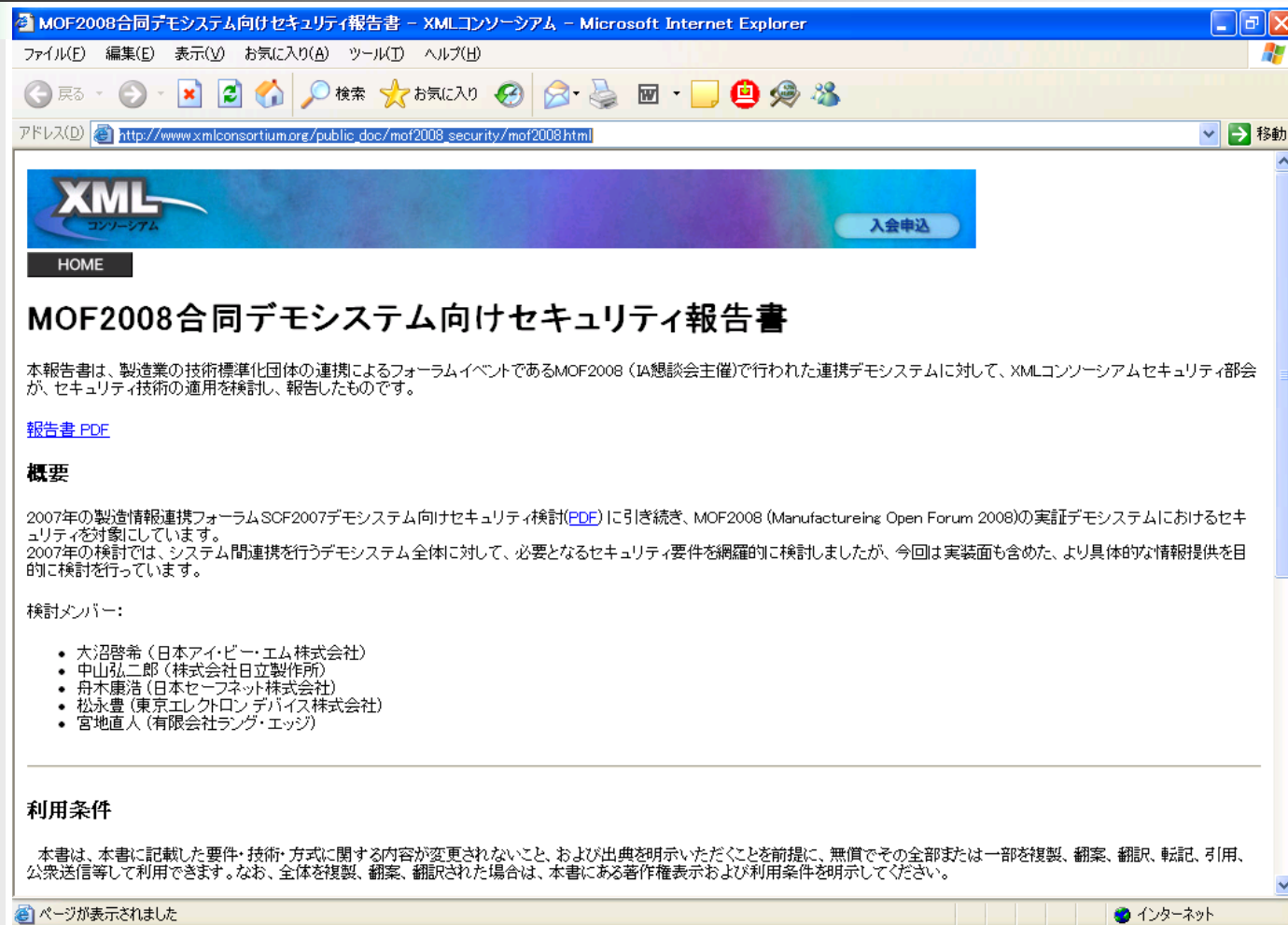
公開資料

- ・XMLDBIに関する質問回答集 New
- ・MOF2008合同デモシステム向けセキュリティ報告書 New
- ・XML利用実態俯瞰図
- ・製造情報連携フォーラム
- ・SCF2007 デモシステム向けセキュリティ検討報告書
- ・「エンタープライズ・システムのためのWeb 2.0」提言書
- ・Web Services Security 日本語訳
- ・TravelXML 仕様勧告案
- ・ContentsBusinessXML 仕様勧告案
- ・XMLQuery UseCases(W3Cワーキングドラフト日本語訳版)
- ・XML PathLanguage (XPath) 2.0 (W3Cワーキングドラフト日本語訳版)
- ・ContactXML version 1.1a



MOF2008合同デモシステム向けセキュリティ報告書

http://www.xmlconsortium.org/public_doc/mof2008_security/mof2008.html



MOF2008合同デモシステム向けセキュリティ報告書 - XMLコンソーシアム - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 進む 印刷 検索 お気に入り 移動

アドレス(D) http://www.xmlconsortium.org/public_doc/mof2008_security/mof2008.html

XML Consortium 入会申込

HOME

MOF2008合同デモシステム向けセキュリティ報告書

本報告書は、製造業の技術標準化団体の連携によるフォーラムイベントであるMOF2008（IA懇談会主催）で行われた連携デモシステムに対して、XMLコンソーシアムセキュリティ部会が、セキュリティ技術の適用を検討し、報告したものです。

[報告書 PDF](#)

概要

2007年の製造情報連携フォーラム SCF2007デモシステム向けセキュリティ検討(PDF)に引き続き、MOF2008 (Manufacturing Open Forum 2008)の実証デモシステムにおけるセキュリティを対象としています。

2007年の検討では、システム間連携を行うデモシステム全体に対して、必要となるセキュリティ要件を網羅的に検討しましたが、今回は実装面も含めた、より具体的な情報提供を目的に検討を行っています。

検討メンバー:

- 大沼啓希 (日本アイ・ピー・エム株式会社)
- 中山弘二郎 (株式会社日立製作所)
- 舟木康浩 (日本セーフネット株式会社)
- 松永豊 (東京エレクトロニクス株式会社)
- 宮地直人 (有限会社ラング・エッジ)

利用条件

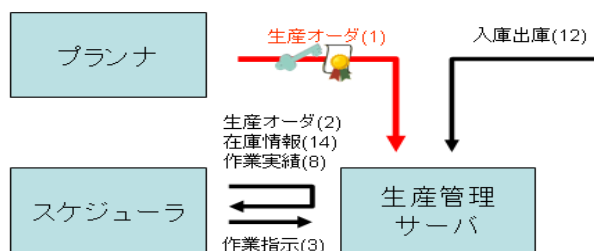
本書は、本書に記載した要件・技術・方式に関する内容が変更されないこと、および出典を明示いただくことを前提に、無償でその全部または一部を複製、翻案、翻訳、転記、引用、公衆送信等して利用できます。なお、全体を複製、翻案、翻訳された場合は、本書にある著作権表示および利用条件を明示してください。

ページが表示されました インターネット



XMLコンソーシアム MOF2008合同デモシステム セキュリティ報告書のご案内

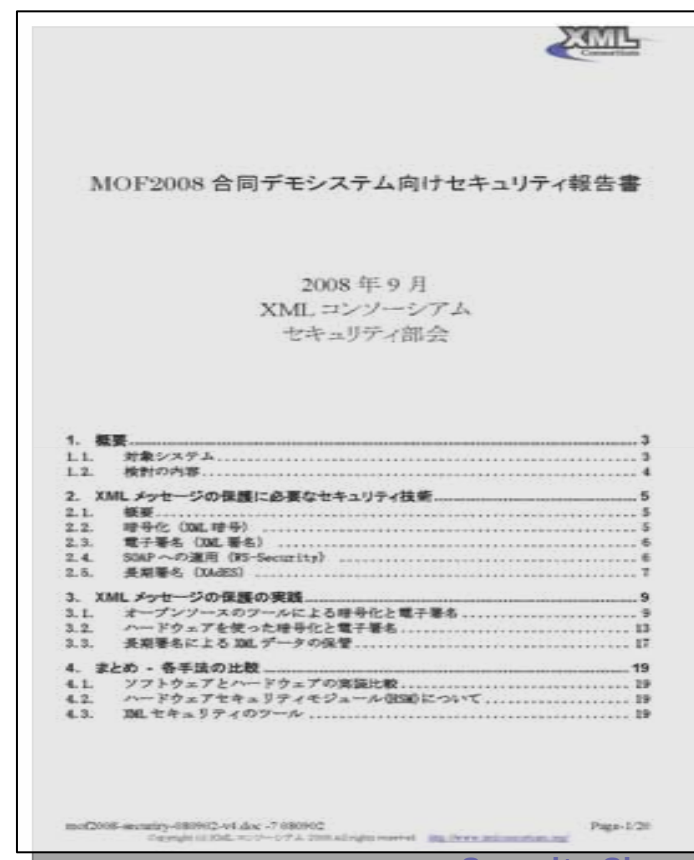
効率化と利便性を求めて、工場設備の情報の統合・連携が指向されるなかで、セキュリティ面の危険性も指摘されています。XMLコンソーシアムでは、実証システム中のAPSOMが担当する生産管理サーバからスケジューラに送信される生産オーダー情報を対象としたセキュリティシステムの実装例を検討し、報告書を公開しました。



XMLで通信される生産オーダー情報に対して2種類のセキュリティ要件を想定し、その実現情報を検討しました。

- 機密性を暗号化で確保する
 - 情報漏洩を防止する
- 完全性を電子署名で確保する
 - 不正な改ざんを検知する
 - 成りすましを防止する

報告書では、必要なセキュリティ技術や標準規格の解説に加え、各種セキュリティツール(オープンソース、商用ソフトウェア、アプライアンス)を使ったセキュリティ適用の検証結果を紹介しています。報告書はXMLコンソーシアムWebサイトより自由にダウンロードできます。<http://www.xmlconsortium.org>
お問い合わせ:XMLコンソーシアム事務局 03-5600-6205
xmlcons_staff@fsi.co.jp



MOF2008合同デモシステム向けセキュリティ報告書 目次

1. 概要

1.1. 対象システム

1.2. 検討の内容

2. XMLメッセージの保護に必要なセキュリティ技術

2.1. 概要

2.2. 暗号化(XML暗号)

2.3. 電子署名(XML署名)

2.4. SOAPへの適用(WS-Security)

2.5. 長期署名(XAdES)

3. XMLメッセージの保護の実践

3.1. オープンソースのツールによる暗号化と電子署名

3.2. ハードウェアを使った暗号化と電子署名

3.3. 長期署名によるXMLデータの保管

4. まとめ - 各手法の比較

4.1. ソフトウェアとハードウェアの実装比較

4.2. ハードウェアセキュリティモジュール(HSM)について

4.3. XMLセキュリティのツール

私の担当分



オープンソースのツールによる暗号 実践

- XML暗号、XML署名は、商用製品やオープンソースなど様々なソフトウェアにおいて実装されている。代表的なオープンソース実装であるApache XML Securityを用いてXML暗号を実践する。
- Apache XML Securityは、Apache Software FoundationのApache XMLプロジェクトによって開発されているXML暗号・XML署名の実装である。Apache XML Securityは、当プロジェクトのWebサイト(<http://xml.apache.org/security/>)によりJavaおよびC++の実装が公開されているが、Java版の実装について実践する。

中山弘二郎（株式会社日立製作所）さんがまとめ役



オープンソースのツールによる暗号実践

- XML暗号・XML署名を実践するためのJavaの標準APIは、それぞれJSR 106 (XML Digital Encryption APIs)とJSR 105 (XML Digital Signature APIs)で規定されている。JSR105についてはすでに最終版の仕様が公開されておりJava SE 6にもその実装が取り込まれているが、JSR106はまだ仕様策定途中である。そのため、これらのJavaの標準APIではなく、Apache XML Securityの独自APIを用いたコード例について説明する。



オープンソースのツールによる暗号実践

```
// AESによる私有鍵の生成
KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
keyGenerator.init(128);
Key symmetricKey = keyGenerator.generateKey();
// 私有鍵を暗号化するDESによる共通鍵の生成
keyGenerator = KeyGenerator.getInstance("DESede");
SecretKey kek = keyGenerator.generateKey();
String algorithmURI = XMLCipher.TRIPLEDES_KeyWrap;
XMLCipher keyCipher = XMLCipher.getInstance(algorithmURI);
keyCipher.init(XMLCipher.WRAP_MODE, kek);
// 共通鍵の暗号化
EncryptedKey encryptedKey = keyCipher.encryptKey(document, symmetricKey);
// 暗号化方法の設定
XMLCipher xmlCipher = XMLCipher.getInstance(algorithmURI);
xmlCipher.init(XMLCipher.ENCRYPT_MODE, symmetricKey);
// 暗号化データに組み込む<KeyInfo>要素の設定
EncryptedData encryptedData = xmlCipher.getEncryptedData();
KeyInfo keyInfo = new KeyInfo(document);
keyInfo.add(encryptedKey);
encryptedData.setKeyInfo(keyInfo);
// 暗号化する要素名
Element enElement = (Element) document.getElementsByTagName("要素名").item(int 要素位置);
// 暗号化すべきデータをEncryptedData要素により置換
xmlCipher.doFinal(document, enElement, true);
```



今後の計画(1)

■ JPCERTよりイベント招待、講演依頼

Subject: 制御システムセキュリティに関する啓発イベント開催と、ご講演のお願い

MOF2008 (Manufactureing Open Forum 2008) において貴コンソーシアムセキュリティ部会の検討メンバーの皆様が検討された

「**MOF2008 合同デモシステム向けセキュリティ報告書**」(下記のURLにて公開されたもの)について知り、制御系セキュリティに関する技術者向けイベントにて御講演をお願いできないかと考え、メールをお送りした次第です。

- 制御システムのセキュリティに関する取組みの中で
2009年2月に普及啓発イベント→ 招待、講演(調整中)



今後の計画(2)

■ Security ツール調査、ツール検証

– ツール調査

- アプリケーションサーバー、ライブラリ、ゲートウェイ/ESB、テストツール
- この分野は2005年5月のXMLコンソーシアムWeekにおける発表内容の更新
- 以下の機能を持つツールの調査

XML暗号・復号機能

XML電子署名付与機能

XML電子署名検証機能

WS-Security(Web Services Security)機能

.....

– ツール検証

- MOF2008合同デモシステム向けセキュリティ報告書での「[XMLメッセージの保護の実践](#)」の継続検証
- プラットフォーム (Windows, Linux, ..)
- Java6対応状況
- Webサービス実証部会との協業

