

PKI アクションプラン

OASIS
PKI (Public Key Infrastructure)
TC (Technical Committee)
によって準備・発行された

日付：2004年2月22日

バージョン：1.0

PKI アクションプラン

目次

1. はじめに.....	3
2. 調査結果.....	4
3. PKI アクションプラン.....	6
3.1. アクションアイテム.....	6
3.2. 次のステップ.....	7
4. 「PKI アクションプラン」のサポーター.....	8
4.1 支持する組織体と個人.....	8
4.2 OASIS PKI TC メンバー.....	9

Copyright (C) OASIS Open 2004. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This translated document is provided by Information-technology Promotion Agency, Japan as an informational service to the global community. This is an unofficial, non-normative translation of the official document, PKI Action Plan, located at <http://www.oasis-open.org/committees/pki/pkiactionplan.pdf>, © copyright OASIS February 22, 2004. This translation is published with acknowledgement of and in agreement with terms specified in the OASIS Translation Policy. Neither OASIS nor Information-technology Promotion Agency, Japan assume responsibility for any errors contained herein.

本翻訳は、独立行政法人 情報処理推進機構によって、世界規模のコミュニティに対する情報サービスとして提供されている。<http://www.oasis-open.org/committees/pki/pkiactionplan.pdf>にあるPKI Action Plan (© copyright OASIS 2004年2月22日)が公式なものであり、この翻訳は公式なものではないとともに基準となるものでもない。この翻訳は、OASIS 翻訳ポリシーによって承認されたものであり、その中に定められた条件によって発行されている。OASIS および独立行政法人 情報処理推進機構は、本書中の誤記に対して何ら責任を負うものではない。

PKI アクションプラン

1. はじめに

公開鍵インフラストラクチャ (PKI) は 20 年以上も前に考案され、現在、多くの重要な標準やプロトコル (例えば、SSL/TLS、IPSEC 等) に使われている。毎日、数百万というユーザがショッピングやバンキングの目的でセキュアな Web サイトを訪れ、PKI はその接続をセキュアにするために使われている。

しかし、PKI が持つすべての潜在能力に到達しているとはいえない。PKI はユーザ認証に使用でき、大量の PIN とパスワードを記憶する必要性を取り除く。また、PKI は、商用トランザクションをセキュアにしたり、電子メールや電話での会話のプライバシーを保護するために使用できる。しかし、アプリケーションの不足、高いコスト、PKI の理解不足、および相互運用可能性の問題等、数々の障害により、PKI の使用が制限されているのが現状である。

「OASIS 公開鍵インフラストラクチャ技術委員会 (PKI TC)」は、デジタル証明書の導入に関する問題を克服するという共通の任務を持つ PKI ユーザ、ベンダー、および専門家で構成されるグループである。PKI TC の最初のミーティングにおいて、TC の重要な役割は、PKI の導入と利用に対する障害を認識し、これらの障害を克服することであると、メンバー間で意見が一致した。この論点について、2 つの調査が実施された。調査の結果 (セクション 2 で概説) により、PKI の導入と利用に対する 5 つの大きな障害が明らかになり、これらの障害を克服するためのいくつかの推奨事項も提案された。

調査結果に基づいて、PKI TC は、障害を克服するために一致した取り組みを呼びかける「PKI アクションプラン」を構築した。これらの取り組みによってコストの削減とセキュリティの強化がもたらされ、PKI ユーザ、将来のユーザ、ソフトウェアベンダー等、すべての団体にとって有益なものになるであろう。ただし、すべての団体による一致した取り組みが不可欠である。PKI TC は連携を保つためだけの、つまり調整役としての役割を果たすのみである。

このため、OASIS PKI TC は、すべての PKI 関係者 (ユーザ、ベンダー、標準化グループ、および専門家) に「PKI アクションプラン」のレビュー、コメント、およびサポートを依頼している。そして、2004 年 2 月に、多くのサポーターとともにアクションプランを発表し、発表と同時にプランの実行を開始する予定である。PKI TC は、すべての団体による真剣な取り組みによってプランが遂行され、大幅な改善がもたらされるものと確信している。

PKI アクションプラン

2. 調査結果

最初の調査は 2003 年 6 月に実施され、回答者に PKI の導入と利用の妨げになっている主な要因を明確にするよう求めた。この調査は、高いレベルの多くの回答者を得られたという点において成功し、いくつかの特定の障害が明らかになった。これに続いて 2003 年 8 月に第 2 回目の調査が実施され、PKI TC は障害の認識をよりいっそう深めた。これらの調査結果は、以下の URL で参照できる。

<http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf>

<http://www.oasis-open.org/committees/pki/pkiobstaclesaugust2003surveyreport.pdf>

これらのレポートを読み、調査の回答者によって明らかにされた障害を完全に理解することが必要である。しかし、「PKI アクションプラン」の段階を設定するために、ここではその概要を示すことにする。

PKI TC 調査には、200 名以上の回答者が参加した。これらの回答者は様々な経歴を持ち、IT 管理者とスタッフも数多く含まれている。注目すべき点として、回答者の 90% が PKI の導入または PKI 関連ソフトウェアの開発を経験している。

調査の結果、PKI の導入と利用をはばむ障害のトップ 5 が次のように明らかになった。

1. ソフトウェアアプリケーションが PKI をサポートしていない
2. コストがかかり過ぎる
3. PKI の理解不足
4. あまりに技術に注目し過ぎており、十分にニーズに応えていない
5. 相互運用可能性が貧弱である

他の障害も指摘されているが、この 5 つが他よりも上位に位置付けられる。

調査の回答者は、最も重要なアプリケーションは、ドキュメント署名、セキュア電子メール、電子商取引、およびシングルサインオンであると指摘した。ドキュメント署名は、フォームへの署名、契約への署名、配布前の文書への署名に細分化されるが、これらの 3 つのサブカテゴリは、ほぼ等分の関心がもたれている。

調査の回答者は、これらの障害の原因と、PKI TC または他の人々がこれらの障害を克服するためにできることを、各自の言葉で書くよう求められた。多くの回答者によって繰り返されたテーマは次のとおりである。

- ・ PKI のサポートが不統一である。アプリケーションやオペレーティングシステムにこれが欠落しているケースもある。存在する場合でも、サポートされる内容が大幅に異なる。これによって、コストと複雑さが大幅に高められ、相互運用可能性を確保することは至難である。
- ・ 現在の PKI 標準は不十分である。場合によっては（証明書管理のように）標準が多すぎる。また（スマートカードのように）標準が少なすぎることもある。存在する場合でも、標準が柔軟かつ複雑すぎる。つまり、あまりにも柔軟で複雑なので、異なるベンダーによる実装間ではほとんど相互運用可能性がない。

PKI アクションプラン

- ・ 標準をどのように使用すべきかを示す特定のプロファイルまたはガイドラインを作成する。ガイドラインは、ベンダーと顧客が正しく実装し、PKI の相互運用可能性を確保できるよう、簡潔で明快なものにすること。場合によっては、標準を作成、統合、または改善することも必要。
- ・ 相互運用可能性のテストおよび相互運用可能性を改善するテストイベントを実施する。
- ・ シンプルな PKI を構築するための、クックブック方式の簡単な手順を提供する。もちろん、より高度な PKI にはカスタマイズが必要である。
- ・ 低コストまたは無料でテスト用の PKI を構築できるようなフリーソフトウェアと CA を提供する。このフリーソフトウェアは低い保証しか提供しないが、テスト用として、また PKI を開始するきっかけを人々に与えるものとして役に立つ。

PKI TC は、これらの提案を慎重に検討し、PKI TC のメンバーの経験と本書の書記のドラフトに対する数多くのコメントを加味して「PKI アクションプラン」を準備した。

これらのアイテムの中には、すでに他の人によって進行中のものもある。調査の回答は、これらの優れた取り組みを奨励する必要がある。PKI TC はこれらの人々に単に指針を与えるだけであろう。

PKI アクションプラン

3. PKI アクションプラン

PKI TCは、「本アクションプランの策定と実施において、独自路線を歩むことはできない」と認識している。PKIには、多くの主体が参画する。：顧客およびユーザ、CA運用者、ソフトウェア開発者（アプリケーション、PKIコンポーネント、プラットフォームおよびライブラリを含む）、産業界および標準化団体、法律家、監査人、セキュリティエキスパート等。これらの主体の支持なしに、この「PKIアクションプラン」を実施することはできない。PKI TCは、主に、変化のきっかけを与える者（Catalyst）もしくは調整者としての役割を果たすことを意図している。この見地から、本書は、産業界に対してアクションを求めるものである。本TCがこのような求めを行うことは厚かましいことであるかもしれませんが、本TCは、数百ものPKIユーザおよび顧客によるサーベイの結論と、このプランのオープンなレビューに参画した多くの関係者による結論をパスしているに過ぎない。

3.1. アクションアイテム

- 名称: PKI の利用についてのアプリケーションガイドラインを策定する
内容: 最も一般的な 3 つのアプリケーション（文書署名、セキュア電子メール、および電子商取引）において、このアプリケーションに対して標準をどのように使用するかを示す適切なガイドラインを策定する。これらのガイドラインは、ベンダーと顧客が正しく実装し、PKI の相互運用可能性を確保できるよう、簡潔で明快なものにする必要がある。
PKI TC のメンバーは、アプリケーションベンダ、業界グループ、および標準化グループと連絡を取り、このようなガイドラインがすでに存在するかどうか、存在しない場合は、誰がガイドラインを作成できるまたは作成すべきなのかを決定する。場合によっては、標準を作成、統合、または改善することも必要である。アプリケーションのガイドラインがすでに存在する場合は、PKI TC は単にそれを示すだけである。
担当: PKI TC Guidelines 小委員会、アプリケーションベンダ、業界グループ、標準化団体
時期: 最初の作業について 2004 年春
- 名称: 相互運用可能性を向上させるための実験を増やす
内容: 相互運用可能性を改善するために、最も一般的な 3 つのアプリケーション（文書署名、セキュア電子メール、および電子商取引）に対し、適合テストのセット、相互運用可能性テスト、およびテストイベントを提供する。証明書管理プロトコルについても考慮する。ブランド付けおよび認定が望ましい。このような取り組みが既に行われている場合は、PKI TC は単にそれを示すだけである。行われていない場合は、作成を督促する。
相互運用可能性には、多くの観点がある。詳細については、<http://www.pkiforum.org/whitepapers.html>にある PKI 相互運用可能性フレームワークについてのホワイトペーパーを参照。
担当: PKI TC Testing小委員会（業界グループ、標準化グループと協働）
時期: 最初の作業について 2004 年春

PKI アクションプラン

- 名称: アプリケーション ベンダーに何が必要であるかを問う
内容: OASIS PKI TC のメンバーは、最も一般的な3つのアプリケーション(文書署名、セキュア電子メール、および電子商取引)のアプリケーションベンダに対し、よりよいPKIサポートを提供するためには、何が必要なかを問う。次に、これらの要件をどのような方法で満たすことができるのかを考慮する(たとえば、顧客の要望の定量化や良いサポートライブラリ等)。
担当: PKI TC Ask Vendors小委員会(アプリケーションベンダと協働)
時期: 最初の作業について2004年春
- 名称: PKI についての教材を集めて提供する
内容: PKI の利点、価値、ROI、およびリスクマネジメント効果を、技術用語を使用せずに説明する。特定の PKI アプリケーションの例を実際の利点と ROI をまじえて紹介する。また、PKI が最も適している(または適さない)状況を説明する。教材は、偏向せず、誰でも利用できるようにする。これらの教材が既に存在する場合は、PKI TC は単にそれを示すだけである。存在しない場合は、作成する。
担当: PKI TC Educational 小委員会(他者と協働)
時期: 最初の作業について2004年春
- 名称: コストを削減するための方策を追求する
内容: ソフトウェア開発コミュニティ(オープンソースコミュニティも含む)を督励し、組織がリーズナブルなコストでPKIを試用およびテストできるオプションを提供してもらう(実際に、コストがPKIの利用を阻む障害となっている)。もちろん、PKI 製品の運用には、ソフトウェアの購入以外にも多くのコストがかかるため、全世界でのPKI導入におけるコスト削減のベストプラクティスを収集し、配布することから取り組みを実行するとよい。
担当: PKI TC Lower Costs小委員会、開発コミュニティ、顧客等
時期: 最初の作業について2004年春

3.2. 次のステップ

2004年の2月に、このアクションプランは、正式に発表される。そして、これを実施する作業が開始される。上述のように、この作業には、多くのPKI関係者(顧客、ベンダー、標準化団体、エキスパート等)が参画することになる。あなたが「PKIアクションプラン」を支持することを望む場合、PKI TCに参加するか、あるいは、この努力を助けていただきたい。pki-tc-comment@lists.oasis-open.org 宛に連絡していただきたい。

PKI TCは、将来、PKI 配備および利用についての障害を解消することについての進捗を評価するために、追加的なサーベイを行う予定である。我々は、「PKIアクションプラン」開始後2年間以内に測定可能な成果が存在することを期待する。

「PKIアクションプラン」が成功した場合、(他のアプリケーションについての利用ガイドラインのような)他の要素項目も含むように拡大される可能性がある。

PKI アクションプラン

4. 「PKI アクションプラン」のサポーター

4.1 支持する組織体と個人

下記の組織体と個人が、「PKI アクションプラン」を支持しています。

組織体

Ascertia Limited
AssuredBytes Inc
Authora Inc.
Izecom BV
Paperless Chile
RSA Security Inc.
SETECS Corporation
Sun Microsystems, Inc.

個人（名字のアルファベット順）

Sharon Boeyen, Entrust Inc.
Kefeng Chen, Ph.D. CISSP
Dr. Whitfield Diffie, Sun Fellow, Chief Security Officer, Sun Microsystems, Inc.
Joseph A. Doekbrijder, SwissSign AG
James Falkner, Enterprise Software Deployment Architect, Sun Microsystems, Inc.
Philip Fulchino, Director of Product Management, RSA Security, Inc.
Per Hagero, CISA, Principal Product Manager, PortWise AB
Stephen Hanna, Senior Staff Engineer, Sun Microsystems, Inc.
Jeremy Hilton CEng
Russ Housley, IETF Security Area Director, Founder of Vigil Security, LLC
Liaquat Khan, CTO, Ascertia Limited
June Leung
Lance Michalson, Michalsons Attorneys
Mr. Yasuo Miyakawa, Information-technology Promotion Agency, Japan
Dr. Sead Muftic, President/CEO, SETECS Corporation
Bakul Patel, VP Engineering, AssuredBytes Inc.
Dr. Radia Perlman, Distinguished Engineer, Sun Microsystems, Inc.
Jari Pirhonen, Information Security Manager & Security Consultant (CISSP, CISA),
AtBusiness Communications Corp.
David Skyberg, Director of Engineering, RSA Security, Inc.
Ross Smith
Donald Teo
Pablo Vicuña Tupper, Paperless Chile, CDO Founder
Tia Walker, CEO, Authora Inc.
David L. Wasley, IT Infrastructure Planner, Univ. of Calif, Office of the President

PKI アクションプラン

4.2 OASIS PKI TC メンバー

「PKIアクションプラン」の策定に参画しているOASIS PKI Technical Committeeのメンバーは下記のとおり。：

Hemant Adarkar, Infosys
Paola Bassanese, U.K. Office of the e-Envoy
Sharon Boeyen, Entrust
Derek Brink, RSA Security, Inc.
Kefeng Chen, GeoTrust Inc.
Alex Deacon, VeriSign
Peter Doyle, Baltimore (now BeTrusted)
Paul Evans, Booz Allen Hamilton
Phil Fulchino, RSA Security
Andrew S. Gottfried, Lockheed Martin
Phil Griffin, Individual Member
Steve Hanna, Sun Microsystems, Inc.
Jeremy Hilton, Individual Member
Dr. Stephen Kent
Terry Leahy, Wells Fargo
June Leung, FundSERV
Mark Lundin, KPMG
John Messing, Individual Member
Tony Nadalin, IBM
Steve Orrin, Sanctum, Inc.
Jean Pawluk, Visa International
Virginia Roth, Novell
John Sabo, Computer Associates
David Skyberg, RSA Security, Inc.
Ross Smith, Government of Canada, Treasury Secretariat
Jeff Stapleton, KPMG
Ann Terwilliger, Visa International
Clifford Thompson, Individual Member
Krishna Yellepeddy, IBM