国立研究開発法人
情報通信研究機構

プレスリリース
平成 27 年 10 月 20 日

暗号プロトコルのセキュリティ評価結果をリスト化・公開

～標準化された 50 個以上の暗号プロトコルの適切な利用促進に期待～

【ポイント】

- 58 個もの大規模な暗号プロトコルについてセキュリティ評価結果を整備し、リストで提供
- NICT のポータルサイトで公開、評価の追試が可能
- システム設計者の目的に応じた暗号プロトコルの適切な利用に期待

国立研究開発法人情報通信研究機構（NICT、理事長: 坂内 正夫）は、標準化された 51 個の暗号プロトコル[*1]とその他 7 個の主要プロトコルについて、学術論文数十本の成果に相当するセキュリティ評価結果をリストとしてまとめ上げ、NICT のポータルサイトで公開し、誰もが入手できるようにしました。ネットワークシステムでは、目的に応じて暗号プロトコルを適切に利用することが重要となりますが、システム設計者が本リストを判断基準として用いることで、暗号プロトコルの適切な利用促進が期待されます。

暗号プロトコル評価ポータルサイト: http://crypto-protocol.nict.go.jp/

【背景】

情報社会の安全性を支える基幹技術として、暗号を組み合わせて用いた通信手順（暗号プロトコル）が、世界中の研究者・技術者により設計され、ITU-T、IETF、ISO/IEC などの標準化団体で規格が策定（標準化）され、様々なネットワーク機器や PC、携帯電話、スマートフォンに実装されています。

これまでに、個々の暗号のセキュリティ評価結果をまとめたリストが CRYPTREC 暗号リスト（http://www.cryptrec.go.jp/list.html）や The SHA-3 Zoo（http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo）で公開されていますが、暗号プロトコルのセキュリティ評価結果をまとめたリストはありませんでした。個々の暗号が安全であっても、その組合せ方によって情報漏えいや、なりすましなどの問題が生じることがしばしば指摘されており、ネットワークシステムで暗号を安心して利用するためには、組み合わせた結果である暗号プロトコルのセキュリティを確認することが不可欠です。しかし、暗号プロトコルのセキュリティ評価結果は数も少なく世界中に散らばっており、システム設計者は評価結果の収集・分析に膨大な労力を費やしている状況で、その労力を削減する暗号プロトコル評価リストが切望されていました。

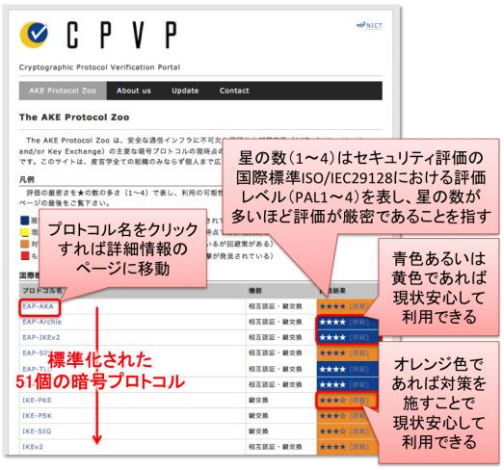

図 1 暗号プロトコル評価リスト

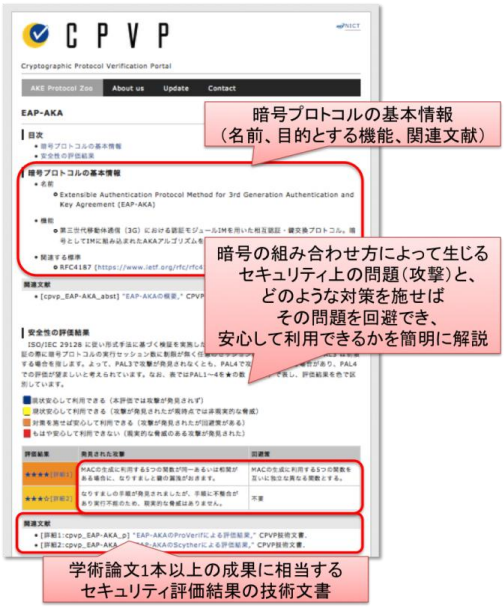

図 2 暗号プロトコルの個別ページ

【今回の成果】

今回 NICT は、標準化された 51 個の暗号プロトコルとその他 7 個の主要プロトコルについて、セキュリティ評価結果を集約する作業を行い、暗号プロトコル評価リスト（図 1 参照）を NICT のポータルサイトで公開しました（http://crypto-protocol.nict.go.jp/）。

リストの整備に当たっては、自動検証ツールを用いてプロトコルを評価しました。そして、評価対象のプロトコルすべてに関して評価結果を精査し、問題点を洗い出しました。さらに、国際標準 ISO/IEC29128[*2] における評価レベルのいずれに相当するかを明らかにしました。

一般に、自動検証ツールによる評価結果の解釈は専門家以外では不可能であり、1 つの暗号プロトコルの評価は学術論文として公表されるほど膨大な労力を必要とします。そのため、単一の機関が 58 個ものプロトコル対して、複数の自動検証ツールを用いて、本リストを取りまとめたことは、世界でも類がなく、初めての試みです。

本ポータルサイトはオープンであり、誰でもリストを入手できます。

システム設計者は、本リストを一覧することで、目的とする機能を実現する暗号プロトコルについて、「現状安心して使える」、「対策を施せば安心して使える」、「もはや安心して使えない」を容易に判断できます。

また、暗号プロトコルの個別ページ（図 2 参照）では、これまでに発見されたセキュリティ上の問題や、その回避方法、自分でセキュリティを評価するための手順などの有用な知見が得られます。

さらに、学術論文でもまれにしか公開されない、オープンソースの自動検証ツールへの入力ソースも提供しており、誰もが評価を追試できます。

【今後の展望】

現在の暗号プロトコル評価リストは、標準化された暗号プロトコルを中心としていますが、今後は標準化候補の暗号プロトコルの評価結果も充実させ、システム設計者が、目的に適した暗号プロトコルを設計する際に役立つ情報を提供していく予定です。それにより、ネットワークシステムの効率的な構築やネットワーク全体の安心・安全の向上に貢献します。

＜ 本件に関する問い合わせ先 ＞
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室
吉田 真紀、平 和昌
Tel: 042-327-7634
E-mail: crypto-protocol@ml.nict.go.jp

＜ 広報 ＞
広報部 報道担当
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

＜用語解説＞

*1 暗号プロトコル

暗号プロトコルとは、暗号を組み合わせて用いた通信手順（プロトコル）であり、代表例として、インターネットにおける通信相手の認証や、通信内容の秘匿と改ざん検知を目的とした SSL/TLS（Secure Sockets Layer/Transport Layer Security）が挙げられます。

SSL/TLS は、様々なネットワーク機器や PC、携帯電話、スマートフォンに実装され、広く普及しています。そのような広く普及した暗号プロトコルに、設計の問題が発見されることが少なくありません。

例えば、2014 年 10 月、約 15 年使われていた SSL3.0（Secure Sockets Layer version 3.0）に POODLE と呼ばれる致命的な脆弱性が発見され、2015 年 6 月に RFC 7568 によって使用が禁止されました。発見時、SSL3.0 しかサポートしていないインターネット機器やフィーチャーフォンが数多くあったため、本脆弱性の影響は無視できないものでした。この脆弱性は、暗号の組合せ方によって生じたセキュリティ上の問題の一例であり、ほかにも数多くの問題が発見されています。

図 3 暗号を組み合わせて用いた通信手順例

*2 ISO/IEC29128

国際標準 ISO/IEC29128 では、暗号プロトコルのセキュリティ評価を、人手による証明あるいは形式手法に基づく検証で厳密化することを目指して、評価基準を定めています。具体的には、セキュリティ評価を、「プロトコル仕様、攻撃者モデル、セキュリティ要件」の記述と「プロトコル仕様が攻撃者モデルに対してセキュリティ要件を満たしていること」の評価に分け、記述と評価の厳密さによってレベルを 4 つに分けています（PAL1～4）。

PAL1 は厳密性が一番低く、記述と評価のいずれも形式化されていない場合を指します。PAL2～4 は記述が形式化されている点では共通ですが、PAL2 は人手による証明、PAL3、4 は形式手法に基づく検証ツールの適用を想定しており、評価の厳密性については必ずしも比較できません。PAL3 では暗号プロトコルの実行セッション数を制限していますが、PAL4 では実行セッション数の制限なしで脆弱性を探索するため、同じ形式化の下であれば、PAL3 より PAL4 の方が厳密な評価といえます。よって、PAL2 と PAL4 の両方のレベルで評価することが望ましいと考えられます。

評価レベルPAL4（暗号プロトコルリストにおける星4つ）では、セキュリティ評価が検証ツールで自動化され、暗号プロトコルの実行セッション数に制約が無いため、厳密に評価されている

	PAL1	PAL2	PAL3	PAL4
プロトコル仕様	PPS_SEMIFORMAL 準形式的	PPS_FORMAL 形式的	PPS_MECHANIZED 形式的（検証ツールの数学的な文法に従う）	
攻撃者モデル	PAM_SEMIFORMAL 準形式的	PAM_FORMAL 形式的	PAM_MECHANIZED 形式的（検証ツールの数学的な文法に従う）	
セキュリティ要件	PSP_SEMIFORMAL 準形式的	PSP_FORMAL 形式的	PSP_MECHANIZED 形式的（検証ツールの数学的な文法に従う）	
評価	PEV_ARGUMENT 非形式的な議論	PEV_HANDPROVEN 人手による証明	PEV_BOUNDED 検証ツールによる解析 実行セッション数有限	PEV_BOUNDED 検証ツールによる解析 実行セッション数無限

図 4　ISO/IEC29128 における 4 つの評価レベル

補足資料

今回公開した暗号プロトコル評価リスト

暗号プロトコル評価リストでは、標準化された 51 個の暗号プロトコル及びその他の代表的な 7 個の暗号プロトコルについて、目的とする機能（通信相手の認証や暗号化通信のための鍵交換）、ISO/IEC29128 における評価レベル（PAL1～4、星の数で表現）、セキュリティ評価結果を提供しています。特に、セキュリティ評価結果を 4 つに分類し色分けをすることで、一見して容易に結果を区別できるようにしています。

- 青■：現状安心して利用できる（現時点において攻撃が発見されていない）
- 黄■：現状安心して利用できる（攻撃が発見されているが現時点では非現実的な脅威）
- 橙■：対策を施せば安心して利用できる（攻撃が発見されているが回避策がある）
- 赤■：もはや安心して利用できない（現実的な脅威のある攻撃が発見されている）

すなわち、赤色以外で星が多いことが安心して利用できる目印となります。

さらに、個別の暗号プロトコルについてセキュリティ評価結果の詳細な情報を知りたい場合は、プロトコル名のリンクをクリックすることで、個別のページにアクセスできます。個別のページは、「暗号プロトコルの基本情報」と「安全性の評価結果」から成ります。「暗号プロトコルの基本情報」には、暗号プロトコルの名前、目的とする機能の概要、関連する標準へのリンクがあり、さらには暗号プロトコルで利用されている暗号とその組合せ方である通信手順を解説した技術文書も提供しています。「安全性の評価結果」には、国際標準 ISO/IEC29128 において高い評価レベルである PAL3 あるいは PAL4 に相当する評価結果を提供しています。具体的には、セキュリティ上の問題（攻撃）の有無、暗号の組合せ方をどのように工夫すればその攻撃を回避できるかの簡明な解説と、個別の評価結果について、評価手順と内容、評価結果の詳細を技術文書として提供しています。技術文書には、学術論文でもまれにしか提供されない貴重な情報である検証ツールへの入力ソースも公開しています。評価に使用されている検証ツールはオープンソースであり、本技術文書があれば、誰でも評価を追試することができます。

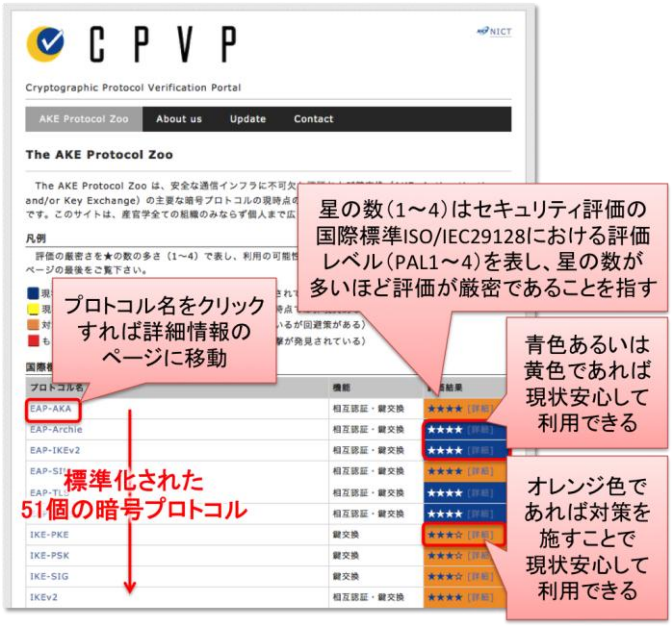

図 1 暗号プロトコル評価リスト（再掲）

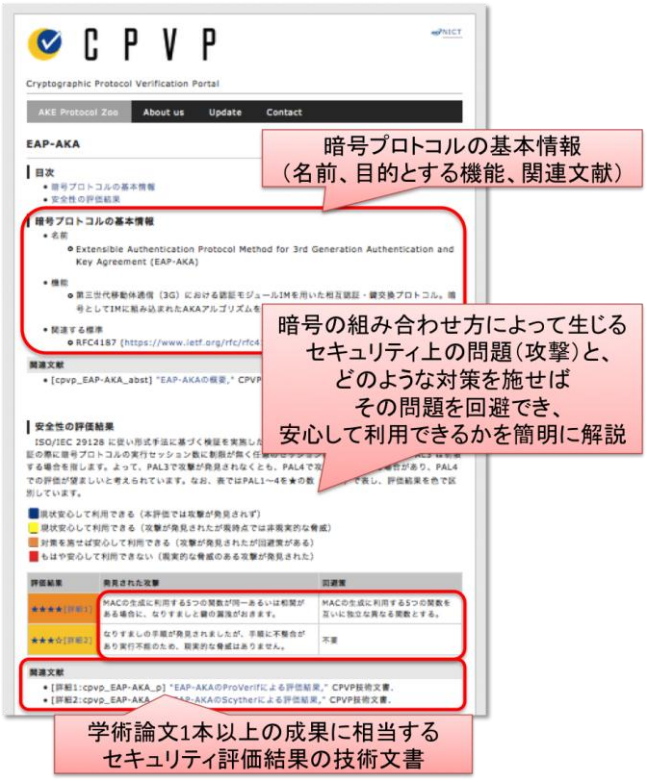

図 2 暗号プロトコルの個別ページ（再掲）