Nomura Research Institute Group

NEWS RELEASE

2020 年 7 月 15 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、暗号鍵の設計・運用レベルを評価するサービスを提供開始

～ DX で利用が拡大する暗号鍵のセキュリティ強化を支援 ～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、社長：小田島 潤、以下「NRI セキュア」）は、企業が自社の情報資産などの保護に不可欠な暗号鍵を対象として、設計・運用段階のセキュリティレベルを評価し、必要な対策の立案・実行を支援する「暗号鍵の設計・運用に関する評価支援サービス（以下「本サービス」）」を、本日から提供します。

さまざまな情報がネットワークを介してやりとりされる現在、第三者に盗まれたり改ざんされたりしないよう、機密情報をはじめとしたあらゆるデータを暗号化して受け渡すことが推奨されています。暗号化する際や暗号化されたデータを元に戻す（復号する）際に、必要となるのが「暗号鍵」です。

例えば、PCI P2PE[1]準拠の決済端末の中には暗号鍵が格納されていて、決済センターとの間で、クレジットカード情報や取引情報を暗号化する際に使われています。また、IT を活用してビジネス革新を図るデジタルトランスフォーメーション（DX）が進展するに伴って、暗号鍵は情報を秘匿する目的以外にも、電子署名や本人認証などで幅広く利用されるようになってきました。このため、暗号鍵の取り扱いにおいては、これまで以上にセキュリティの強化が求められています。

■ 本サービスの概要と特長

本サービスでは、企業が暗号鍵を設計し運用する際の安全性を高めるために、暗号鍵の生成から輸送、導入、廃棄に至るまでのライフサイクル全体を対象として、NRI セキュアの専門家が評価を行います。

本サービスは、おもに以下の 4 つの内容から構成されます。

1. 現状調査・評価対象の決定

NRI セキュアが作成した評価シートをベースに、対象となるシステム全体に関するヒアリングを行い、評価の対象範囲と項目を決定します。対象システムの特性等を加味しながら、必要に応じて評価項目のカスタマイズも可能です。

2. 机上分析

評価対象とするシステムに関する、サービス仕様書、要件定義書、設計・開発資料、運用ルール・手順書などを参照し、現状どのようなセキュリティ対策が実施されているかについて、机上分析を行います。

3. ヒアリング・現地調査

机上分析の結果を踏まえ、詳細についてシステムの担当者などにヒアリングを実施します。物理的な施設など、目視による確認が必要な場合については、現地調査を行います。

4. 評価・報告

机上分析、ヒアリング、現地調査などの結果を踏まえ、対策状況とリスクを評価します。本サービスでは、暗号鍵のライフサイクル全体を評価するために、「システム全体設計」「鍵生成」「鍵配送・輸送」「鍵導入」「鍵利用」「鍵保管・廃棄」「機器運用管理」「物理セキュリティ」の 8 つに分かれた、計約 230 の評価項目を設けています。評価の結果は、実施すべきセキュリティ対策案とともに、次の 2 つの文書にまとめて報告します。

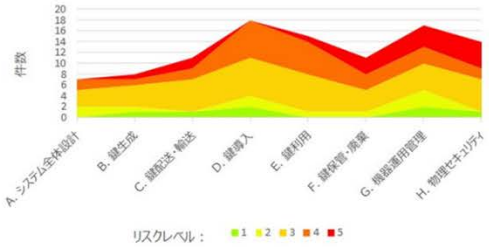
鍵管理設計・運用評価結果シート

評価項目ごとに、現在の対策状況と内在するリスクを 5 段階で判定したシートです。評価結果の詳細のほか、追加の対策が必要な項目については対策案も提示します。

評価結果サマリ

評価項目の中から判明したリスクを集計し、一覧表にまとめたものです。暗号鍵のライフサイクルを踏まえて、セキュリティレベルを一目で確認することができます（表 1、2）。

表 1：「評価結果サマリ（カテゴリごとのリスク評価）」の例

評価カテゴリ		リスクレベル毎の件数 ※高リスク(５)～低リスク(1) 5	4	3	2	1	リスク平均値	リスク分布・総評
A	システム全体設計	0	2	3	2	0	2.9	
B	鍵生成	1	1	4	1	1	3.2	
C	鍵配送・輸送	2	2	6	0	1	3.8	
D	鍵導入	0	7	7	2	2	4.1	
E	鍵利用	1	6	7	1	0	4.6	
F	鍵保管・廃棄	3	3	4	1	0	4.4	
G	機器運用管理	4	3	5	3	2	3.5	
H	物理セキュリティ	5	2	6	0	1	4.5	

【総評】
鍵管理における作業記録が適切に取得されていないケースが、どのカテゴリでも多く見受けられました。運用ルールやプロセスの事前設計と関係者への周知徹底が十分に行われていなかったことが原因と推定されます。これらを見直した上、関係者への教育実施と周知の徹底を推奨いたします。
また、一部の用途に限定はされるものの、すでに利用されている暗号鍵の一部で、暗号強度の低いものが存在しているため、鍵生成時の強度設計の見直しを推奨いたします。

表 2：「評価結果サマリ（カテゴリごとの推奨対策）」の例

評価カテゴリ		傾向の考察と有効な追加対策例
A	システム全体設計	データ暗号化鍵の強度がNISTで求められる標準レベルよりも低いものが一部あるため、鍵の強度を高めることを推奨。その際にシステムで使用する全ての鍵について見直しを行い、リストで一覧化して管理を行うこと。
B	鍵生成	鍵生成時に使用する平文鍵コンポーネントを使用する際の履歴管理がされておらず、不正を検知できる仕組みが十分ではない。デュアルコントロールで管理者承認のもと履歴管理を行うように運用を変更すること。
C	鍵配送・輸送	自社→A社（他社）間のワンタイムで使用される輸送鍵（鍵暗号化鍵）がデータ暗号化鍵よりも鍵強度が劣る。AES-128を暗号化するケースで2048bit RSAを使用しているが、3072bit RSA以上で暗号化すること。
D	鍵導入	HSMに鍵をロードする際、使用した鍵コンポーネントについてすみやかな削除が行われていない。定められた手順に従って削除をするとともに、作業記録として残すこと。
E	鍵利用	鍵利用における台帳の最新化が行われていない。鍵利用時のプロセスとして台帳管理が明記されていないため、手順書を改版する。あわせて、手順書の内容について関係者への周知徹底を行う。
F	鍵保管・廃棄	マスター鍵を管理するためのスマートカード保管場所がオフィスの机の引き出しの中で、責任者一人で複数を管理している。保管場所を鍵付きのキャビネットにし、デュアルコントロールのもとで管理すること。
G	機器運用管理	HSMへのアクセスについて記録されていない。またデュアルコントロールの実装において複数名で共通のPWを使用している。HSMへのアクセス記録を有効化するとともに、PWの共用を禁止すること。
H	物理セキュリティ	鍵生成に使用されるHSMの置かれた部屋への入退室について、監視カメラによる24時間監視が行われていない。22時から翌7時の間についても監視カメラでモニタリングを行うようにすること。

本サービスの詳細については、次の Web サイトをご参照ください。

https://www.nri-secure.co.jp/service/consulting/cryptographic-key

NRI セキュアは、2016 年に国内で初めて、カード業界において要求される高度なセキュリティレベル基準「PCI P2PE」への適合性を審査する資格「P2PE QSA」[2]を取得しました。また、暗号鍵の設計・運用に関するコンサルティングや監査で豊富な実績を有しています。さらに、ブロックチェーン技術を活用し

たシステムのアーキテクチャを評価するサービスの一環として、ウォレット [3]の鍵管理のセキュリティ評価なども支援してきました。

今後、自動車や工場をはじめとして、さまざまなモノとモノがネットワークでつながり、その通信内容の改ざん防止や認証のために、暗号化技術が一層活用されていくと考えられます。NRI セキュアは、本サービスを通じて、さまざまな業界に対して暗号鍵の設計や運用面における安全性の向上を支援し、安全・安心な DX の推進に貢献していきます。

---

[1] PCI P2PE（Payment Card Industry Point-to-Point Encryption）：対面加盟店の決済端末から決済ネットワークの手前までを対象に、クレジットカード情報を暗号化した状態で安全に処理するための、国際的な情報セキュリティ基準。国際クレジットカードブランド 5 社（VISA、Mastercard、JCB、American Express、Discover）が設立した有限責任会社 PCI SSC により制定、運用、管理されている。

[2] P2PE QSA（Point-to-Point Encryption Qualified Security Assessor）：世の中の決済ソリューションが、PCI P2PE を満たしているかどうかについて審査を行う、PCI SSC 認定の評価機関のこと。

[3] ウォレット：ブロックチェーン技術を利用して取引される暗号資産を、管理するために使用されるシステムのこと。

【ニュースリリースに関するお問い合わせ先】

NRI セキュアテクノロジーズ株式会社　広報担当

TEL：03-6706-0622　E-mail：info@nri-secure.co.jp