e-Gov 電子申請システム
外部連携 API
情報セキュリティ要求仕様書

1.1 版

2015 年 2 月 18 日

変更履歴

No	版数	更新日	変更箇所	変更内容
1	1.1 版	2015/2/18	2.2.電子申請システムの正当性確認と通信の暗号化	TLS のバージョンを記載。 SSL3.0 のアクセスが無効である旨を記載。

目次

1. はじめに

この仕様書は、外部連携 API を利用したソフトウェア(以下、「API 利用ソフトウェア」という)を開発するにあたり、開発するソフトウェアに対して求める情報セキュリティ対策に関する事項を記載したものです。

API 利用ソフトウェアの開発者は、この仕様書に記載する情報セキュリティ要求事項を満たすソフトウェアの開発を行ってください。

2. 情報セキュリティ要求事項

2.1. ソフトウェア ID、利用者 ID 及びアクセスキーの厳重な管理

ソフトウェア ID、利用者 ID 及びアクセスキーは、API 利用ソフトウェアが API 経由で e-Gov 電子申請システムに電子申請を行うための認証・認可を行うために必要な情報となります。ソフトウェア ID、利用者 ID 又はアクセスキーが漏えいした場合、e-Gov 電子申請システムが不正アクセスされ、なりすましによる電子申請の被害を受ける可能性が生じてしまいます。

API 利用ソフトウェアの開発者は、開発するソフトウェアに対して、ソフトウェア ID、利用者 ID、アクセスキーを外部に漏えいさせないため、以下の措置を講じてください。

(1) API 利用ソフトウェアは、ソースコードコンパイル後の実行モジュールを、暗号化・難読化する

(2) API 利用ソフトウェアは、外部（e-Gov 電子申請システムと API 利用ソフトウェア間の通信路は除く）に、ソフトウェア ID と利用者 ID を出力する際は、出力情報を暗号化・難読化を行う仕様とする

(3) API 利用ソフトウェアは、外部（e-Gov 電子申請システムと外部連携 API を使うソフトウェア間の通信路は除く）にアクセスキーを漏えいさせない仕様とする

(4) API 利用ソフトウェアは、国民等一般利用者が API 利用ソフトウェアをログアウトするタイミングで、メモリ上に保持している当該利用者が使用していたアクセスキーの値を初期化又は破棄する仕様とする

2.2. 電子申請システムの正当性確認と通信の暗号化

API 利用ソフトウェアが、e-Gov 電子申請システムと通信を行うにあたり、接続先のなりすましに気付かずに通信した場合、送信した情報がなりすましの相手に漏えい、悪用される危険を生じます。また、通信途中でデータを傍受されると、情報が第三者に漏えいする危険を生じます。

API 利用ソフトウェアの開発者は、開発するソフトウェアに対して、接続先のなりすましを回避し、通信データを暗号化するため、以下の措置を講じてください。

(1) API 利用ソフトウェアは、e-Gov 電子申請システムとの接続毎に、必ずサーバ証明書の検証を行う

(2) API 利用ソフトウェアは、サーバ証明書の検証において、以下の 2 点の有効性確認を実施する

・SSL/TLS ライブラリによるサーバ証明書の有効性確認
(TLS のバージョンは 1.0、1.1、または 1.2)
※SSL2.0 および 3.0 を利用したアクセスは無効

・サーバ証明書のコモンネームが、e-Gov 電子申請システムの FQDN 名
(api.e-gov.go.jp) と一致していることの確認

(3) API 利用ソフトウェアは、上記 2.(2)のすべての有効性が確認できた場合のみ、e-Gov 電子申請システムと暗号化通信を行う

(4) API 利用ソフトウェアは、サーバ証明書の検証において有効性が確認できない場合は、接続を中断する

2.3. 主体認証

API 利用ソフトウェアが、API 利用ソフトウェア自体の主体認証機能を持たない場合、API 利用ソフトウェアに対するアクセス権のない者が、API 利用ソフトウェアが保持する情報の参照、改ざんまたは消去を行うおそれがあります。また、API 利用ソフトウェアが、API 利用ソフトウェアからのログアウト機能を持たない場合、離席中のなりすましや共用端末でのなりすましにより、e-Gov 電子申請システムが不正にアクセスされる可能性があります。

API 利用ソフトウェアの開発者は、開発するソフトウェアについて、以下の措置を講じてください。

(1) API 利用ソフトウェアに利用者の識別及び主体認証を行う機能を設ける

(2) 主体認証情報を保存する必要がある場合には、その内容を暗号化する

(3) 主体認証情報を保存する場合に暗号化できない場合には、利用者に対して自らの主体認証情報を設定、変更又は入力させる場合に暗号化が行われないことを通知する

(4) 利用者が自ら使用するパスワードを設定、変更する機能を設ける

(5) 利用者が設定するパスワードを他者が容易に知ることができないように保持する仕様を設ける

(6) API 利用ソフトウェアにログアウト機能を設け、利用者が API 利用ソフトウェア自体から明示的なログアウトを行うことが可能とする

2.4. 利用者 ID と公開鍵証明書のバックアップ／リカバリ

e-Gov 電子申請システムは、外部連携 API 経由で電子申請を行った際に付番する送信番号及び到達番号を、利用者 ID に対応づけて管理しています。また、利用者認証時に使用する公開鍵証明書の証明書識別情報を利用者 ID と対応づけて管理しています。利用者 ID または公開鍵証明書を消失してしまった場合、API 利用ソフトウェアを使用する利用者は、e-Gov 電子申請システムを使用できなくなります。

API 利用ソフトウェアの開発者は、利用者 ID 及び電子署名用証明書を、API 利用ソフトウェアで保持または管理する仕様とする場合、API 利用ソフトウェアを導入するパソコンの故障等にともなう利用者 ID 及び電子署名用証明書の消失に備えるため、以下の措置を講じてください。

(1) API 利用ソフトウェアは、利用者 ID 及び電子署名用証明書を、バックアップ・リカバリできる手段を設けておくこと
(2) API 利用ソフトウェアが、バックアップ・リカバリを行う際は、利用者 ID 等が漏えいしない対策を行うこと

API 利用ソフトウェアが利用者 ID と利用者認証で使用する公開鍵証明書を保持・管理しない仕様である場合、利用者 ID と公開鍵証明書の忘却・紛失等に対する責任は、当該ソフトウェア利用者の責任となります。

API ソフトウェア開発者は、API 利用ソフトウェアを使用する国民等一般利用者に対して、利用者 ID と公開鍵証明書の忘却・紛失等についての注意喚起を行ってください。

2.5. 電子納付金融機関サイト表示のリターン Web ページの表示

電子納付金融機関サイト表示の API は、ブラウザ上で実行することとしており、e-Gov 電子申請システムからの HTTP レスポンスもブラウザに表示する前提としています。API 利用ソフトウェアが、HTTP レスポンスをブラウザに表示するのではなく、API 利用ソフトウェア内部で表示する場合は、API 利用ソフトウェアの利用者が、偽サイトに騙される被害を回避する対策が必要です。

API 利用ソフトウェアの開発者は、電子納付金融機関サイト表示の API を利用し、かつその HTTP レスポンスを API 利用ソフトウェア内部に表示する仕様とする場合は、適切なフィッシング対策（アドレスバーを表示する、SSL のアイコンを表示するなど）を講じてください。