Internet Initiative Japan

セキュリティホワイトペーパー

IIJ IDサービスのISO/IEC 27017に基づくセキュリティ要求事項への取り組み

改訂履歴

版数	制定/改定日	改定箇所、改訂理由	備考
1.0	2021.11.19		初版

目次

はじめに

組織におけるクラウドサービスの利用において、セキュリティへの懸念は必ず取り上げられる問題の一つです。

そのような状況の中、2015年12月に、クラウドセキュリティの国際標準規格であるISO/IEC 27017:2015が発行され、クラウドサービスの利用者と事業者が行うべきセキュリティ管理策が定義されました。

本書では、IIJ IDサービス（以下、IIJ ID）におけるISO/IEC 27017:2015への取り組みを解説いたします。

IIJは、ISMS認証やプライバシーマークなど多くの第三者認証を取得しており、クラウドセキュリティ推進協議会の発足メンバーです。

また、セキュリティインシデントに対応する国際組織（FIRST）へ国内企業で初めての加入や、情報セキュリティレベルの向上に寄与するNPO日本ネットワークセキュリティ協会（JNSA）の役員を務めるなど、安全安心なネットワーク社会の実現に向けて積極的な活動を行ってきました。

これらの活動や十数年前からクラウドを運用している豊富な経験、お客様に安心してご利用いただける環境を提供しております。

本書でIIJ IDにおけるクラウドセキュリティの取り組みを知っていただき、IIJ IDをご活用いただくことで、今後ますますお客様の事業発展のお役に立ちたいと考えております。

なお、本書の内容は作成時点での取組みに基づいて記述しております。内容は変更される場合がございますので、最新の情報は担当営業へご確認くださいますようお願い致します。

IIJ IDのサービス概要

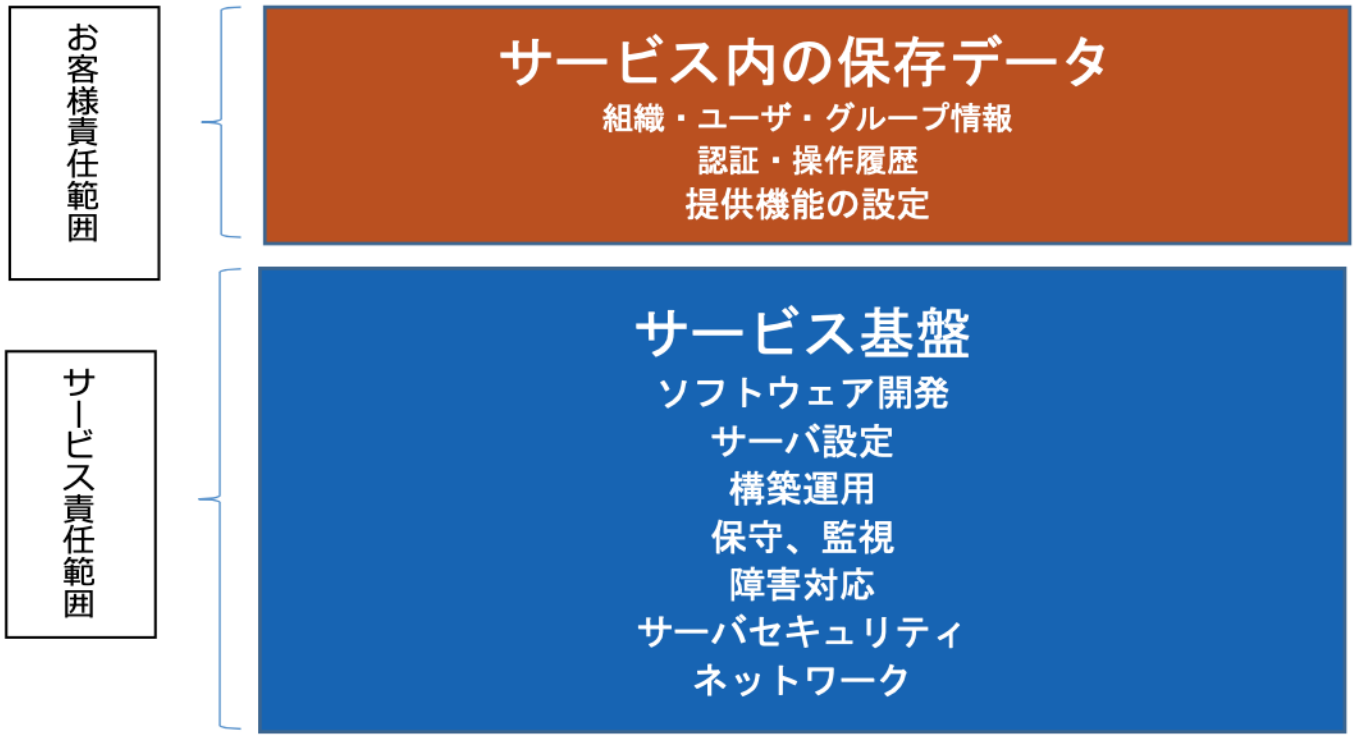
IIJ IDは、様々なサービスのIDを連携させ、SSO（シングルサインオン）を可能にするクラウド型のID管理サービス（IDaaS）です。

不正ログインの検知・防止ができる強力な多要素認証機能も提供します。

責任分界点

IIJ IDにおける責任分界点は、下記の通りとなります。

弊社の責任範囲はサービス基盤部分となり、お客様責任範囲は、より上層のサービス内の保存データ（以下、保存データ）となります。



保存データとは、サービス設備に保存された組織・ユーザ・グループ情報、認証・操作履歴、および、IIJ ID で提供する機能の設定を指します。

本サービスに関するドキュメント類

IIJ IDは、IIJインターネットサービス契約約款に基づき役務提供しております。サービス仕様、サービスのご利用にあたっての操作方法等につきましては、サービス詳細資料、オンラインマニュアル及び、ご利用の手引きをご用意しております(本書ではこれらの文書をサービスドキュメントと表記しています)。

これらのドキュメントの掲載、お客様へのお知らせ、問合せ窓口や運用管理担当者、管理者ID、利用者IDを管理するためにIIJサービスオンラインおよびIIJ IDコンソールをご用意しております(本書では、これらのサイトをお客様専用のポータルサイトと表記しています)。

ISO/IEC27017の概要

国際標準化機構 (ISO) と国際電気標準会議 (IEC)が定める情報セキュリティマネジメントの国際規格にISO/IEC27000シリーズがあります。

ISO/IEC27017は、このシリーズの1つで、2015年12月に発行されたクラウドサービスにおける情報セキュリティマネジメントの指針を記したものになります。

ISO/IEC27017の特徴

「ISO/IEC 27002の管理策に対する追加の実施の手引き」と「クラウドサービスに対する追加の管理策及び実施の手引き」ISO/IEC27002は情報セキュリティマネジメントの汎用的な指針であるのに対し、ISO/IEC27017はクラウドサービス向けの指針です。

ISO/IEC 27002を前提としたISO/IEC 27017 には、ISO/IEC 27002に対して、クラウドサービスに固有の事項を追加されています。

具体的に、ISO/IEC27017には、以下の内容が記載されています。

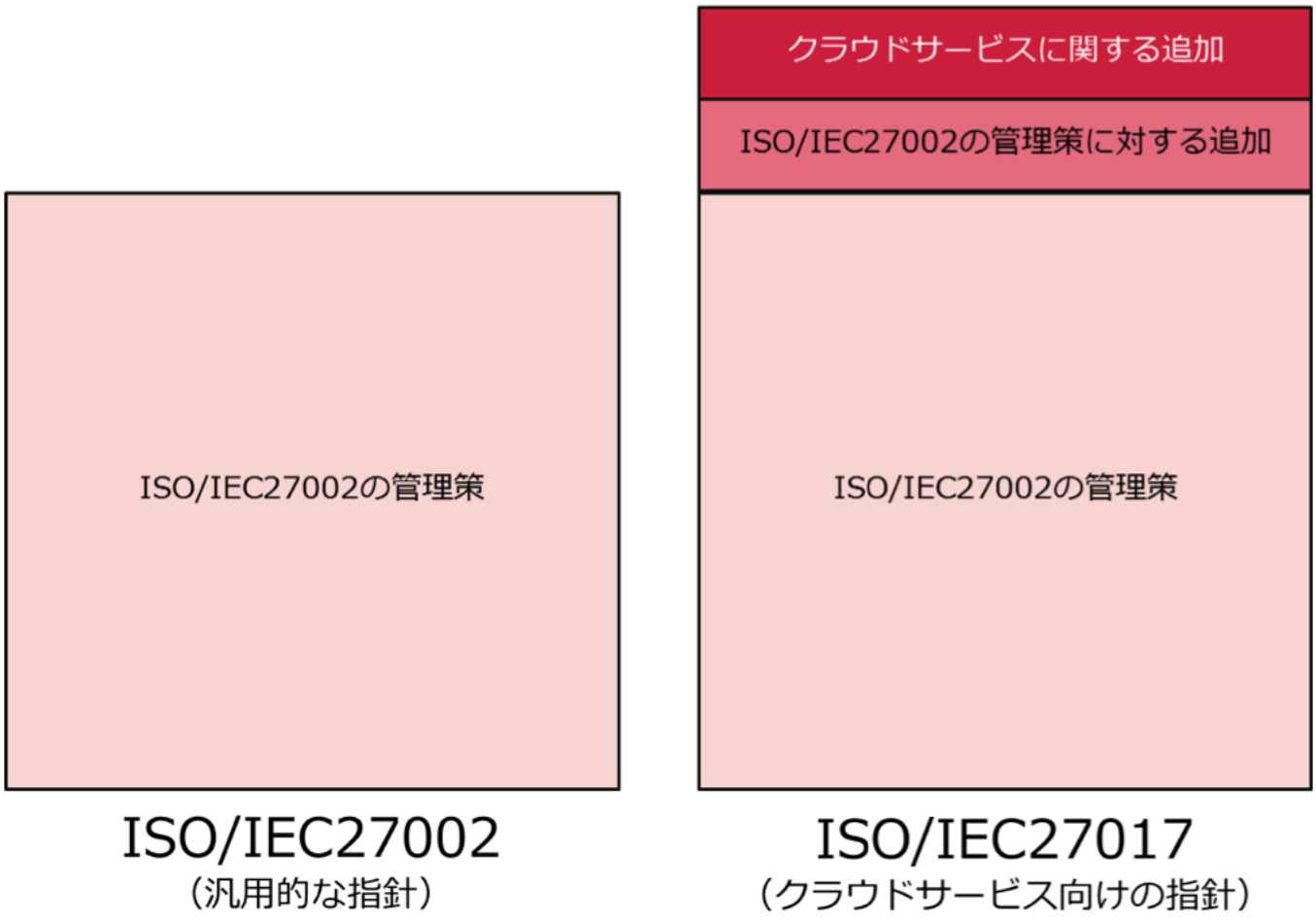


図2. ISO/IEC27002 とISO/IEC27017の体系イメージ

ISO/IEC27017にて、新たに追加されたクラウドサービス事業者向けの管理策について、IIJ IDでの取り組みを次頁以降に記載しています。

ISO/IEC27017に対する取り組み

１．情報セキュリティのための方針群

1.1 情報セキュリティのための方針群

ISO/IEC27017項番：5.1.1

IIJ ID では、弊社の情報セキュリティ基本方針に従い、セキュリティに関しまして極めて重要な事項として取り扱い、サービス運営を行います。 詳細は、IIJ 情報セキュリティ方針(https://www.iij.ad.jp/securitypolicy/)をご覧ください。

また、クラウドサービスの提供にあたり、お客様の情報セキュリティ要求を満たすため、次の事項を考慮します。

1. クラウドサービスの設計・実装に適用する情報セキュリティ要求事項
2. クラウドサービスカスタマの隔離について
3. クラウドサービスカスタマデータへのアクセスや保護
4. 変更管理におけるクラウドサービスカスタマへの通知
5. 仮想化に関するセキュリティ
6. 違反の通知、調査ならびにフォレンジックを支援するための情報共有

２．情報セキュリティのための組織

2.1 情報セキュリティの役割及び責任

ISO/IEC27017項番：6.1.1

IIJインターネットサービス契約約款やサービスドキュメントにて契約やサービス内容を定義し、サービス提供を実施しております。 アプリケーション、設備などサービス基盤の運用は弊社の責任範囲としてサービスの提供範囲に含まれております。 保存データはお客様責任範囲となります。

2.2 関係当局との連絡

ISO/IEC27017項番：6.1.3

弊社の本社所在地は、東京都千代田区富士見2-10-2 飯田橋グラン・ブルームとなります。 お問い合わせ窓口はサービスドキュメントに記載しております。 なお、IIJ IDに保存された情報の所在は日本国内となります。

2.3 クラウドコンピューティング環境における役割及び責任の共有及び分担

ISO/IEC27017項番： CLD.6.3.1

IIJインターネットサービス契約約款やサービスドキュメントにてサービス内容を定義し、サービス提供を実施しております。 また、責任分界点の詳細は、“2.1 情報セキュリティの役割及び責任”を参照ください。

３．人的資源のセキュリティ

3.1 情報セキュリティの意識向上、教育及び訓練

ISO/IEC27017項番：7.2.2

弊社では情報セキュリティ基本方針(https://www.iij.ad.jp/securitypolicy/index.html)を定め、方針に従いサービスを運営しております。 なお、上記規程に、全ての社員に対する教育活動を実施する旨を定めております。

４．資産の管理

4.1 資産目録

ISO/IEC27017項番：8.1.1

お客様の情報資産(お客様にて保存されるデータ)と弊社がサービスを運営する為の情報は、明確に分離しております。

4.2 情報のラベル付け

ISO/IEC27017項番：8.2.2

ご契約頂きましたサービスやオプションの一覧やサービス機能を定めたサービスドキュメントが、お客様専用のポータルサイトにて閲覧可能です。 また、ご契約頂きましたサービスは、サービスコードにて、お客様毎の識別及び利用サービスを分類しております。

4.3 クラウドサービスカスタマの資産の除去

ISO/IEC27017項番：CLD8.1.5

IIJ IDのサービス解約の際、弊社サービス設備に残存したお客様の情報資産に関しては、解約日の翌日を起算日（1日目）として、起算日から8日目の任意の時間に、すべての情報が物理削除されます。

５．アクセス制御

5.1 利用者登録及びネットワークサービスへのアクセス

ISO/IEC27017項番：9.2.1

お客様専用のポータルサイトにて、ご契約頂きましたサービスに対する運用管理担当者、利用者 ID の登録及び削除機能を提供しております。

登録、削除に必要な手順、情報はサービスドキュメントに記載しております。

5.2 利用者アクセスの提供

ISO/IEC27017項番：9.2.2

お客様専用のポータルサイトにて、ご契約頂きましたサービスに対する運用管理担当者、管理者ID、利用者IDの権限管理機能を提供しております。

権限ごとのアクセス可能な範囲、及び権限の変更手順はサービスドキュメントに記載しております。

5.3 特権的アクセス権の管理

ISO/IEC27017項番：9.2.3

お客様専用のポータルサイトの管理者認証に関しましては、IDとパスワードの認証に加え、アクセス元IPアドレスによる制限を設定する機能を提供しております。

また、多要素認証オプションをご契約頂くことで、FIDO2を利用した生体認証や、クライアント証明書によるデバイス認証などをご利用頂くことができます。

5.4 利用者の秘密認証情報の管理

ISO/IEC27017項番：9.2.4

お客様専用のポータルサイトを利用される際の運用管理担当者、管理者ID、利用者IDの登録やパスワード変更、再発行方法につきましては、サービスドキュメントに記載しております。

5.5 情報へのアクセス制限

ISO/IEC27017項番：9.4.1

お客様専用のポータルサイトの管理者権限、ユーザ権限等、権限ごとのアクセス可能な範囲につきましては、サービスドキュメントに記載しております。

5.6 特権的なユーティリティプログラムの使用

ISO/IEC27017項番：9.4.4

お客様専用のポータルサイトにて発行したアクセストークン・リフレッシュトークンを利用することで、IIJが提供する Directory Sync や Password Sync といったユーティリティを利用したり、お客様のプログラムから IIJ ID の API にアクセスすることができます。

アクセス可能なAPIの機能の範囲は、お客様がアクセストークン・リフレッシュトークン発行時に設定した権限に準じます。

5.7 仮想コンピューティング環境における分離

ISO/IEC27017項番：CLD.9.5.1

お客様がアクセスするネットワークと弊社運用担当者が利用する管理ネットワークは分離しています。 また、お客様間のデータ分離は、ソフトウェアにて適切に制御しております。

5.8 仮想マシンの要塞化

ISO/IEC27017 項番：CLD 9.5.2

設備に対するIPアドレスによるアクセス制限の実施、及び不要なポート、常駐プログラムは停止しております。

6．暗号

6.1 暗号による管理策の利用方針

ISO/IEC27017項番：10.1.1

お客様にご登録頂いた主要な情報については暗号化して保存しております。 またパスワード情報はハッシュ化して保存しております。

暗号化アルゴリズムの採用にあたっては、OWASP、NIST、電子政府推奨暗号リストなどの複数の指針を参考に弊社にて決定し、定期的に見直しを行っております。

本サービスとの通信につきましてはTLSによる暗号化通信が利用できます。

７．物理的及び環境的セキュリティ

7.1 装置のセキュリティを保った処分又は再利用

ISO/IEC27017項番：11.2.7

設備を再利用、廃棄する際には適切なプロセスで、保存データの物理削除や設備の破壊を実施しております。

８．運用のセキュリティ

8.1 変更管理

ISO/IEC27017項番：12.1.2

サービス内容を変更する場合、影響のあるお客様に対し変更内容をお客様専用のポータルサイトへのアナウンス掲載、及び運用管理担当者宛にメールにてご連絡しております。

8.2 容量・能力の管理

ISO/IEC27017項番：12.1.3

安定的にサービスを提供できる仕組みを構築しています。具体的には、リソースの量及び稼働状況を管理しております。

8.3 情報のバックアップ

ISO/IEC27017項番：12.3.1

サービスの復旧を目的としたバックアップを実施し、遠隔地にて保存しておりますが、お客様にて保存データを直接的にバックアップする機能は付帯していません。

バックアップを管理する必要がある場合は、お客様にてご取得ください。

サービスの復旧を目的としたバックアップについては、一日に複数回、複数世代で取得しております。 またデータ復旧手順の作成と復旧試験の実施を行っております。

8.4 イベントログの取得

ISO/IEC27017項番：12.4.1

お客様専用のポータルサイトにおいて、ログイン履歴、ジョブ履歴など最大過去90日分の記録を提供しています。

8.5 実務管理者の運用担当者の作業ログ

ISO/IEC27017項番：12.4.3

弊社の責任範囲において、サービスの維持管理に必要となる作業ログを取得しております。

8.6 クロックの同期

ISO/IEC27017項番：12.4.4

弊社では、NTPによる時刻同期の仕組みを有しており、日本時間(JST)で管理しています。IIJ IDで記録される時刻は、すべて時刻同期に基づいて記録されています。

8.7 技術的ぜい弱性の管理

ISO/IEC27017項番：12.6.1

弊社では非公開情報を含め、脆弱性情報を常時収集しております。 収集した情報を元に、サービス設備への影響を評価し、弊社の責任範囲において影響がある場合は、速やかに対応しております。

また、第三者機関による脆弱性診断を定期的に実施しております。

8.8 実務管理者の運用のセキュリティ

ISO/IEC27017項番：CLD 12.1.5

IIJ IDをご利用頂くにあたり、必要な操作手順につきましては、サービスドキュメントにて提供しております。

8.9 クラウドサービスの監視

ISO/IEC27017項番：CLD 12.4.5

お客様専用のポータルサイトにおきまして、ジョブ履歴を提供しております。

9.通信のセキュリティ

9.1 ネットワークの分離

ISO/IEC27017項番：13.1.3

お客様がアクセスするネットワークと弊社運用担当者が利用する管理ネットワークは分離しています。 また、お客様間のデータ分離は、ソフトウェアにて適切に制御しております。

9.2 仮想及び物理ネットワークのセキュリティ管理の整合

ISO/IEC27017項番：CLD 13.1.4

帯域の監視と予兆検知を実施し、仮想および物理ネットワークの整合性を確保しております。

10. システムの取得、開発及び保守

10.1 情報セキュリティ要求事項の分析及び仕様化

ISO/IEC27017項番：14.1.1

情報セキュリティ基本方針、ホワイトペーパー及びサービスドキュメントに定めております。

10.2 情報セキュリティに配慮した開発のための方針

ISO/IEC27017項番：14.2.1

IIJ IDでは「セキュリティ実装チェックリスト(IPA)」を満たすことの他、「安全なWebサイトの作り方(IPA)」などの複数の指針を含めた、セキュアコーディングルールに準拠することを開発ルールとして定めて開発しております。

また、変更管理に関するプロセスを定めてサービス開発・運営を実施しております。 変更管理プロセスでは、リスクアセスメントを実施した後、サービスのリリースをしております。

加えて、第三者機関による脆弱性診断を定期的に実施しております。

11. 供給者関係

11.1 供給者関係のための情報セキュリティの方針

ISO/IEC27017項番：15.1.1

IIJ IDでは、お客様から事前に了承をいただいている場合を除き、弊社運用担当者がお客様の情報にアクセスすることはありません。（障害対応で必要となる場合は、この限りではありませんが、その場合でも情報へのアクセスは最低限とするように努めます） また、物理的にセキュアな環境で開発・運用し、お客様の契約を超えて保存データのアクセスが発生しない仕組みを整えています。

11.2 供給者との合意におけるセキュリティの取扱い

ISO/IEC27017項番：15.1.2

IIJ IDはクラウドサービスとなり、責任分界点の詳細は、“2.1 情報セキュリティの役割及び責任”を参照ください。 また情報セキュリティ対策も“2.1 情報セキュリティの役割及び責任”の範囲において必要なセキュリティ対策を実施しております。

11.3 ICTサプライチェーン

ISO/IEC27017項番：15.1.3

IIJ IDの提供のために必要となる構成要素（PaaS・データセンター・機器等）の供給については、弊社のセキュリティ方針に沿うようリスク管理しております。

またIIJ IDと同等の情報セキュリティ水準を有していることを確認し採用しております。

12. 情報セキュリティインシデント管理

12.1 責任及び手順

ISO/IEC27017項番：16.1.1

IIJの責任範囲である、契約者情報やお客様に影響のあるサービス運営上の派生データ等に関する情報セキュリティインシデントが発生した場合には、お客様専用のポータルサイトやメールにて速やかに報告いたします。

12.2 情報セキュリティ事象の報告

ISO/IEC27017項番：16.1.2

情報セキュリティ事故が発生した場合には、お客様専用のポータルサイトやメール等にて速やかに報告いたします。また、お客様からの事象報告はお問い合わせ窓口にて受け付けております。

12.3 証拠の収集

ISO/IEC27017項番：16.1.7

お客様責任範囲における情報セキュリティインシデントに関するログ等の証拠の収集はお客様にてご実施頂く範囲となります。 弊社責任範囲でのログ等の証拠が必要な場合は、お客様の要望に応じて個別に対応しております。 都度、ご相談ください。

13. 順守

13.1 適用法令及び契約上の要求事項の特定

ISO/IEC27017項番：18.1.1

IIJ IDのサービス設備は日本国内に設置しております。 本サービスをご利用にあたり、当社と契約者の間で訴訟の必要が生じた場合、東京地方裁判所を当社と契約社の第一審の専属的合意管轄裁判所と定めております。 詳細はIIJ インターネットサービス契約約款(https://www.iij.ad.jp/svcsol/agreement/)に記載しておりますので、ご確認ください。

13.2 知的財産権

ISO/IEC27017項番：18.1.2

サービス提供機能で設定された内容やアカウント情報はお客様管理下にあります。 IIJ IDお問い合わせ窓口はサービスドキュメントに記載しております。

13.3 記録の保護

ISO/IEC27017項番：18.1.3

ログイン履歴、ジョブ履歴などの記録を収集し、お客様専用のポータルサイトにおいて、最大過去90日分の記録を提供しております。 お客様の契約を超えてこれら記録へのアクセスが発生しない仕組みを整えております。

13.4 暗号化機能に対する規制

ISO/IEC27017項番：18.1.5

お客様専用のポータルサイトではSSL/TLSの暗号化を使用しております。 なお、輸出規制の対象となる暗号化の利用はありません。

13.5 情報セキュリティの独立したレビュー

ISO/IEC27017項番：18.2.1

組織的な取り組みとして弊社ではISMS認証やプライバシーマークを取得しております。

Copyright

IIJ IDサービスのISO/IEC 27017に基づくセキュリティ要求事項への取り組み 株式会社インターネットイニシアティブ

IIJ-IID008-0001