SCS — SUPPLY CHAIN SECURITY

サプライチェーン強化に向けたセキュリティ対策評価制度を理解し、自社の次の一歩を決める —
制度の全体像から★3・★4 の違い、費用の考え方、今すぐ始められる準備までを1冊にまとめました。

SCS評価制度 完全ガイド



★3 専門家確認付き自己評価 ★4 第三者評価・技術検証 を正しく理解し、事前準備で制度対応のスピードを高める

- 制度の全体像
- 対象企業・対象業種
- 義務・強制力・罰則
- 最新スケジュール
- 費用の考え方
- 準備チェックリスト

発行 サイバーセキュリティ.com（株式会社セキュアオンライン） ／ 情報基準日 2026年11月2日

※本資料は2026年11月2日時点の公表情報に基づき作成しています。制度の詳細は今後更新される可能性があります。本資料は経済産業省・IPAの公式資料ではなく、民間事業者が作成した情報資料です。

CONTENTS

目次（数字はページ番号）

03 制度概要・公式ガイドの使い方

06 制度の背景

07 対象企業・確認ポイント

09 取得の任意性・取引条件

10 最新スケジュール

11 登録・更新のルール

13 ★3の仕組み・対象資格・取得手順

15 確認責任者の研修・料金

16 ★4 の仕組み・評価機関・取得手順

18 ★3・★4の比較

19 メリット・注意点

20 取得費用・準備チェックリスト

22 よくある質問

23 運営者情報・出典一覧

本資料の使い方

本資料は、経営者・情報システム担当者がSCS評価制度の全体像を理解し、自社の準備を具体化するためのガイドです。制度概要と公式資料の使い方を確認し、必要な★と対応体制、費用・日程を整理してください。

情報基準日：2026年11月2日。IPA・経済産業省の公表情報をもとに作成しています。制度の詳細は今後更新される可能性があるため、申請時は公式サイトをご確認ください。本資料は民間事業者が作成した情報資料です。

CHAPTER 01

SCS評価制度とは

SCS評価制度は、企業のサイバーセキュリティ対策の状況を、共通の基準にもとづいて評価する制度です。取引先から個別の質問票で対策状況を確認されるといった、企業ごとにばらばらだった確認作業を、共通の「ものさし」で可視化できるようにすることを目的としています。

制度の運営主体と評価対象

経済産業省と内閣官房国家サイバー統括室の監督のもと、IPAが運営します。★3 は企業の自己評価を専門家が確認し、★4 は指定評価機関が第三者評価を行います。

評価対象は組織のセキュリティ対策状況です。取得単位・適用範囲は公式ガイドに従って設定し、特定製品だけの評価と混同しないようにします。

★3・★4 の評価水準（ ★5は検討中 ）

項目	★3：専門家確認付き自己評価 ★★★	★4：第三者評価・技術検証 ★★★★
評価の主体	企業自身（自己評価）	評価機関
確認・評価の方法	★3 確認責任者による確認・署名	文書・実地審査と技術検証
有効期間	1年間（毎年更新）	3年間（毎年自己評価提出、3年ごとに再評価）
対策水準	一般的なサイバー攻撃への対策	被害拡大防止・供給上の役割も重視

POINT：★3 は26項目、★4 は43項目（★3相当を含む）。★3の先行取得は必須ではありません。取引先の要請と自社の役割から段階を選びます。

企業が今からできること

制度の運用開始を待つことなく、**自社の現状把握**から始められるアクションがあります。制度対応のスピードを左右する4つの取り組みです。

1 社内の担当者・推進体制を決める

制度対応は部署単独では進みません。 経営層の関与も含め、推進の責任者と担当者を明確にします。

2 評価対象とする範囲（適用範囲）を整理する

組織・拠点・システム・委託先の関係を整理し、自己評価等ガイドに従って取得単位と適用範囲を決めます。

3 自社が保有する情報資産を洗い出す

PC・サーバ・ソフトウェア・クラウドサービスなど、評価対象となり得る情報資産を棚卸しします。

4 現状のセキュリティ対策状況を自己評価してみる

最新の要求事項・評価基準と公式アセスメントシートで自己評価し、不足対策と根拠資料を整理します。

POINT 早めに現状を把握しておくことで、運用開始後の対応スピードが大きく変わります。

要求事項と公式ガイドの使い方

2026年10月末に基準と評価用ガイドが更新されました。
★3 は26項目、★4 は43項目。要求事項の見出しだけでなく、個々の評価基準と根拠資料を確認します。

要求事項・評価基準（Ver.1.1）	自社が満たすべき対策と、適合を判断する基準を確認する
自己評価等ガイド・アセスメントシート	取得単位と適用範囲を整理し、実施状況・証跡を記録する
第三者評価ガイド・技術検証ガイド	★4 の審査・技術検証について、対象・日程・対応体制を準備する
要求事項・評価基準解説書	基準の考え方や留意点を理解し、自社の運用と照合する

POINT 10月28日の公開・改訂後、29日に一部資料を軽微修正。準備には公式掲載ページの最新版を使用します。

CHAPTER 02

なぜこの制度が作られたのか

サプライチェーン攻撃の増加

取引先・委託先・子会社を経由する攻撃により、自社の情報や業務にも被害が及ぶ可能性があります。自社の対策に加え、取引先との接続や情報の共有、委託業務を踏まえた備えが必要です。

企業ごとに異なる確認負担の共通化

企業ごとに異なる質問票への回答は、発注側・受注側の双方に負担となります。SCS評価制度は、共通基準で対策状況を確認し、その負担を軽減することを目指します。個別取引で必要な追加確認は別途行います。

制度の目的

共通基準による「見える化」

対策状況を客観的に把握できるようにする

中小企業の対策底上げ

専門家の確認・第三者評価により、自己流の対策で終わらせない

発注企業側の確認負担の軽減

共通の評価結果を判断材料として活用できる

サプライチェーン全体のレジリエンス向上

一社の対策不備が全体に波及するリスクを構造的に減らす

つまりSCS評価制度は、**「個社の対策強化」**と**「社会全体の負荷軽減」**の両立を目指す制度設計となっています。

CHAPTER 03

対象企業・対象業種

取得の必要性を検討する着眼点

- 大企業・官公庁と直接取引がある
- 二次請け・三次請けとしてサプライチェーンに組み込まれている
- 取引先のシステム・ネットワークに接続している
- IT・システム開発、業務委託（BPO）関連の事業者である
- 個人情報・技術情報など重要な情報を取り扱っている
- 製造業のサプライチェーンに組み込まれている

業種・規模を問わず幅広い事業者が対象

中小企業・大企業とも対象となり得ます。取引先の要請がなくても自主的に取得を検討できます。必要な★と対応時期は、扱う情報や供給上の役割、契約条件を踏まえて判断します。

業種・業務ごとの確認ポイント

業種・業務の例	主な確認対象	検討するポイント
製造業・部品供給	供給・納品への影響	業務停止が取引先へ及ぼす影響
システム開発・運用保守	取引先への接続	アクセス権限と委託業務の範囲
BPO・業務委託	預かる情報	顧客情報・機密情報の管理
建設・インフラ関連	契約・調達条件	個別の入札・契約で求める水準
卸売・物流	情報連携と継続性	受発注・配送等の停止時の影響
小売・サービス	取引・委託関係	顧客情報、決済、外部サービス

※以下は検討する際の着眼点です。業種ごとの取得義務や公式の優先順位を示すものではありません。

取引とリスクの確認チェックリスト

取得の必要性や準備の優先順位を検討するためのチェックリストです。
該当する内容を整理し、取引先への確認や社内計画に活用してください。

- [ ] 大企業・官公庁と直接取引がある
- [ ] 個人情報や取引先の機密情報を預かっている
- [ ] 二次請け・三次請けとしてサプライチェーンに組み込まれている
- [ ] 取引先からすでにセキュリティ対策状況を確認されたことがある
- [ ] 取引先のシステム・ネットワークに接続している
- [ ] 同業他社でSCS評価取得の話を聞いたことがある

POINT

該当数で取得の要否は決まりません。取引先の要請、扱う情報、業務停止の影響を確認しましょう。

CHAPTER 04

義務・強制力・罰則

SCS評価制度は、法律によって全ての企業に一律に取得を義務づけるものではありません。未取得であること自体に対して、行政による罰則が科される制度でもありません。
義務かどうかは「法律」と「取引上の実態」の2つの軸で考える必要があります。



法律上の義務ではない

現時点で公表されている情報を踏まえる限り、 特定の業種・企業規模の事業者に対して一律に評価取得を義務づける法律は存在しません。 「SCS評価を取得していないこと」自体を理由に、行政から是正命令や罰金が科されるという制度設計にはなっていません。



罰則はあるのか

未取得自体に一律の罰則を科す制度ではありません。取引条件は当事者間で確認します。
一方、自己評価の虚偽や不正な申請が判明した場合は、登録取消し等の措置を受ける場合があります。



取引上の強制力（実質的に効いてくるところ）



発注企業の調達条件になるケース
入札や商談の土俵に立てない、選定で不利になる可能性



サプライチェーン全体への波及
直接の取引先だけでなく、二次請け・三次請けにも波及する可能性



業界・団体単位での自主的な推奨
業界内での信頼性の基準として機能していく可能性



注意：個人情報保護法や取引基本契約に定められたセキュリティ条項など、SCS評価制度とは別に存在する法令・契約上の義務は、SCS評価の有無にかかわらず引き続き適用されます。本章は一般的な情報提供を目的としており、法的助言ではありません。
個別の契約・取引における判断は、必要に応じて弁護士等の専門家にご確認ください。

CHAPTER 05

最新スケジュール（2026年11月2日時点）

基準・料金・評価用ガイドは公開済みです。企業の ★ 登録申請、専門家の登録、研修提供はそれぞれ開始時期が異なります。
公開済みの内容と今後の予定を分けて準備しましょう。



★3・★4の登録申請は2027年3月受付開始予定。最新基準による自己評価と不足対策の整理は、今から進められます。

出典：IPA「要求事項・評価基準」（10月29日更新）、「よくある質問」（10月30日更新）、「料金設定のお知らせ」（9月18日）

CHAPTER 05 | 最新スケジュール

★3・★4 の登録・更新ルール

基本規程に基づき、取得後も対策の維持と定期的な更新が必要です。登録料は2026年9月18日に公表されています。

★★★ 3 専門家確認付き自己評価



有効期間 1年間

更新方法 更新時は毎年、「★3 確認責任者」の確認・助言を受け、自己評価の更新版をIPAへ提出する。

★★★★ 4 第三者評価・技術検証



有効期間 3年間

更新方法 登録期間中は毎年、自己評価を行って評価機関へ提出する。
3年ごとに第三者評価を再実施する。

★ 共通ルール（★3 /★4 共通）



再評価 適用範囲などに**重大な変更**がある場合は、有効期間を待たずに再評価が必要。

登録料 ★3：1万円／年 ※
★4：6万円／3年

報酬 外部の★3 確認責任者・★4 評価機関への報酬は、当事者間の契約で決定される。

★3 は毎年更新、★4 は毎年の自己評価＋3年ごとの第三者評価。※★3 登録料は,2028年4月以降2万円／年。

評価機関の指定と研修の公開済みルール

確定しているルール

日本法に基づいて設立された法人が申請可能

IPAによる書類審査と指定委員会の決定が必要

申請料・指定料は公表済み（事業者向け）

指定の有効期間は**3年間**

指定機関名はIPAが公開

不正・基準違反があれば調査・改善指示・指定取消しの対象

研修実施基準で定められた内容

研修実施基準は公開済みです。具体的な講座日程・受講料は、指定研修事業者の案内で確認します。

1. 修了試験は正答率70%以上で合格
2. 受講証明書は試験合格日から3年間有効
3. 有効期間満了前の半年間等にフォローアップ研修
4. 修了試験問題はIPAが作成し、研修事業者が実施

出典：IPA「研修実施基準」（2026年9月11日）、「料金設定のお知らせ」（9月18日）、指定申請FAQ（10月21日版）

CHAPTER 06

★3（専門家確認付き自己評価）の詳細

★3は、企業自身が行う自己評価に、「**★3確認責任者**」による確認・署名が加わる仕組みです。 第三者評価・技術検証まで含む★4に比べて取り組みやすく、一般的なサイバー脅威への対応を想定した水準です。

★★★ ★3 確認責任者の役割

★3 確認責任者は、企業が実施した自己評価の内容の**妥当性を確認し、署名**する役割を担います。 企業からの求めに応じて、取得準備（自己評価の実施等）の支援を行うこともできます。

1

自己評価の実施
企業が評価を行う

2

内容の確認
確認責任者が妥当性を確認

3

署名
確認責任者が署名

取得支援は中立性・公平性の要件を満たす場合に可能です。専門家の公平性要件は2026年12月下旬に公表予定。支援と確認の役割分担は、その内容を確認して決定します。

★★★ ★3 の特徴

- **社内・社外どちらの人材でも担当可能**
- **自己評価を専門家が確認・助言し署名**
- **有効期間は1年間（毎年更新）**
- **一般的なサイバー攻撃への対策を確認**

※担当には対象資格・所定の研修・SCSセキュリティ専門家登録が必要です。

確認責任者の対象資格と★3 取得の流れ

SCSセキュリティ専門家の対象資格

資格名	資格・登録の関係機関	位置づけの目安
情報処理安全確保支援士（登録セキスペ）	IPA	登録を維持した支援士が対象
公認情報セキュリティ監査人（CAIS）	日本セキュリティ監査協会（JASA）	公認情報セキュリティ主任監査人を含む
CISSP	ISC2	国際的に認知度の高いセキュリティ全般の資格
CISM	ISACA	セキュリティマネジメントに強い国際資格
CISA	ISACA	情報システム監査に特化した国際資格
ISO27001主任審査員	JRCA等の審査員登録機関	ISMS審査の実務資格

※対象資格に加え、所定の研修と専門家登録が必要です。CAISは公認情報セキュリティ主任監査人を含みます。

★3 取得までの流れ（7ステップ）

1. **推進体制の構築**：担当者・責任者を決める
2. **適用範囲の決定**：評価対象とする組織・拠点・業務・システムの範囲を決める
3. **情報資産の洗い出し**：自社が保有する情報資産を整理する
4. **自己評価の実施**：評価基準に沿って自社の対策状況を評価する
5. **★3 確認責任者による確認**：自己評価の内容について確認・署名を受ける
6. **経営層の自己適合宣言・登録申請**：確認済みの自己評価をもとにIPAへ申請する
7. **毎年の更新**：有効期間1年のため、毎年確認・更新を行う

CHAPTER 06 | ★3の詳細

確認責任者の研修・料金と登録予定

対象資格の保有に加え、所定の研修とSCSセキュリティ専門家への登録が必要です。
一般的な制度説明会や、他制度の講習への参加だけで要件を満たしたとは判断できません。



研修と修了試験

講義3時間・演習2時間は例示。一律の必須時間ではありません。
修了試験は正答率70%以上。受講証明書は合格日から3年間有効。



フォローアップ

証明書の有効期間満了前の半年間に受講。
要求事項・評価基準の見直しに伴う研修も規定されています。



受講料と登録料

研修受講料は研修事業者が設定。具体額は募集案内で確認します。
専門家登録料はIPA料金資料の「料金案」欄に無料と掲載。受講料とは別です。



申込み・登録予定

2026年12月下旬：指定研修事業者・専門家登録手続き等を公表予定。
2027年1月以降：指定研修の提供・専門家登録の受付開始予定。



POINT

研修事業者の申請料・指定料は、研修を提供する法人向けの費用です。個人の受講料と混同しないでください。

CHAPTER 07

★4（第三者評価・技術検証）の詳細

★4は43項目（★3 相当を含む）に基づき、指定評価機関による第三者評価を受ける段階です。文書・実地審査と技術検証を通じて、管理面と技術面の対策を確認します。

★★★★ 評価機関の役割

評価機関は、自己評価と根拠資料を確認し、実地審査・技術検証を含む第三者評価を行います。技術検証を指定事業者へ委託する場合もあります。



※ 評価機関向けの申請料は2028年4月以降30万円。指定料は同額です。企業が★4を取得する際の評価費用とは異なります。

★★★★ 評価機関の指定要件（確定事項）

- 日本法に基づいて設立された法人であること
- IPAによる書類審査と指定委員会の決定を経て指定されること
- 申請料15万円・指定料30万円／3年（税込）※
- 指定の有効期間は3年間、指定機関名はIPAが公開
- 不正・基準違反があった場合、調査・改善指示・指定取消しの対象

中立性・公平性の要件

評価担当者と、評価対象システムの運用に携わる者が同一の場合は評価できません。取得支援を行う場合も、指定基準の公平性要件に従い役割を分けます。

※★4評価責任者はSCSセキュリティ専門家。評価機関の指定基準に沿った体制が必要です。

★4 取得までの流れ

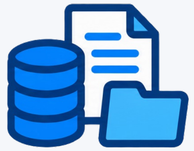
★4では、技術面と管理面の両方を確認します。自己評価と根拠資料を整え、評価機関の審査・技術検証に対応したうえで、IPAへの登録申請へ進みます。

1 

推進体制の構築
技術担当を含めた体制を決める

2 

適用範囲の決定
組織・拠点・システム・委託先を整理する

3 

情報資産・システム構成の整理
構成図・資産管理台帳等を整理する

4 

不足対策の整備・自己評価
43項目への適合と根拠資料を確認する

5 

第三者評価への対応
文書・実地審査と技術検証を受ける

6 

経営層の宣言・IPAへの登録申請
評価報告書を受領し、登録手続きを進める



いつ決まる？

指定評価機関は2026年12月下旬に公表予定。登録申請の手引は11月末頃、
企業の登録申請受付は2027年3月開始予定です。

CHAPTER 08

★3 と ★4、どちらを選ぶべきか

比較表

観点	★★★ ★3（専門家確認付き自己評価）	★★★★ ★4（第三者評価・技術検証）
制度登録料（税込）	1万円／年※（通常2万円）	6万円／3年
要求項目数	26項目	43項目（★3相当を含む）
重視する対策	一般的なサイバー攻撃への対策	被害拡大防止と取引先への影響低減
社内負担	自己評価が中心のため中程度	実地審査・技術検証への対応が加わり増加
有効期間	1年間（毎年更新）	3年間（毎年自己評価、3年ごと再評価）

判断の3つの観点

1



取引先からの要請内容

すでに特定の水準を求められているか、今後の調達条件強化が見込まれるか

2



取引先への影響

情報漏えいや供給停止が与える影響と、必要な対策水準を確認する

3



社内で対応できるリソース

★4は費用・工数ともに★3より負荷が高くなる見込み



POINT

★3の先行取得は必須ではありません。必要な★が明確な場合は、その段階に向けた準備を進めます。取得後の運用・更新まで含めて費用と社内体制を検討しましょう。

※★3の1万円は2028年3月31日までの申請に適用。専門家確認・評価費用は別途。

CHAPTER 09

メリット・デメリット

メリット

取引先への説明を効率化

共通の基準で対策状況を示せる。取引固有の追加確認はあり得る

セキュリティ対策の「棚卸し」になる

評価を受けるプロセス自体が対策の抜け漏れを可視化する機会になる

確認負担の軽減

共通の評価結果を活用し、重複する確認の負担を減らすことが期待される

取り組みを対外的に示せる

取得段階と適用範囲を正確に表示する。受注や取引継続を保証するものではない

デメリット・注意点

取得・維持のコスト

自己評価であっても確認責任者への確認依頼や書類整備の工数がかかり、★4 はさらに費用と時間がかかる。 加えて、★3 は毎年、★4 は毎年の自己評価＋3年ごとの再評価という継続コストが発生する

社内リソースの負担

専任担当者がいない中小企業ほど負荷が相対的に重くなる

未取得のまま先送りすることの相対的な不利

取引上の必須化が進むほど選定から外れるリスクが高まる

最新情報への対応

基準や手続きの更新を確認し、必要に応じて対策・記録・社内計画を見直す

CHAPTER 10

取得費用と継続費用

制度への登録料と、専門家確認・評価、研修・対策にかかる費用を分けて予算化します。公表登録料だけで取得の総額を判断しないことが重要です。



IPAへの登録料（税込）

★3：10,000円／1年
2028年3月31日までの申請に適用。
以降は20,000円／1年。
★4：60,000円／3年
専門家確認・第三者評価の費用は含みません。



専門家確認・第三者評価の費用

★3の外部確認責任者への依頼料、★4の審査・技術検証費用は個別契約で決まります。対象拠点・システム、再確認、旅費、更新対応を含むか、見積もりで確認します。



研修・対策実装にかかる費用

指定研修の受講料は事業者が設定します。社内人材の育成費、不足対策の実装費、担当者の作業時間も予算に含めます。専門家登録料の無料表記と受講料は別です。



継続費用と見積もりの確認

★3は毎年更新。 ★4は毎年の自己評価と3年ごとの第三者評価が必要です。初回だけでなく、再確認・更新・追加拠点・日程変更の費用も確認しましょう。

CHAPTER 11

今すぐ始められる準備チェックリスト

スケジュールに沿って、3つのフェーズで準備を進めましょう。 まずは今すぐ着手できるフェーズ1から。

フェーズ 1 今すぐ

今すぐ着手できること

- [ ] 社内の推進体制（担当者・責任者）を決める
- [ ] 評価対象とする組織・拠点・業務・システムの範囲（適用範囲）を検討する
- [ ] 自社が保有する情報資産を洗い出す
- [ ] 現状のセキュリティ対策を棚卸しする
- [ ] ★4 を視野に入れる場合は、システム構成図・ネットワーク構成を整理する

フェーズ 2 今すぐ

自己評価・改善

- [ ] 最新アセスメントシートで自己評価を実施する
- [ ] 不足対策と根拠資料を整理し、担当・期限を決める

フェーズ 3 2026年末以降

指定・登録情報の公表後

- [ ] 専門家・評価機関の登録・指定状況を確認する
- [ ] 費用・スケジュールを具体的に調整する
- [ ] 公開された手引に沿って申請準備を進める

該当数で優先度を決めず、取引先の期限と不足対策から計画します。
資産整理や運用記録の蓄積には時間がかかるため、早めに着手しましょう。

CHAPTER 12

よくある質問

Q SCS評価制度は義務ですか？

法律による一律の義務ではありません。 ただし、取引先の調達条件によっては事実上必要になる場合があります。

Q 取得後も費用はかかり続けますか？

はい。 ★3は毎年の更新、★4は毎年の自己評価提出と3年ごとの再評価が必要です。 継続的な費用発生を前提に検討してください。

Q 中小企業も対象になりますか？

企業規模だけで対象外になるわけではありません。 取引関係や取り扱う情報によって必要性が判断されます。

Q SCS評価制度はいつから始まりますか？

★3・★4の登録申請は2027年3月受付開始予定です。登録申請の手引は2026年11月末頃に公表予定です。

Q ★3と★4 、どちらを取得すればいいですか？

取引先からの要請内容、扱う情報の重要度、社内リソースの3点を踏まえて判断します。 迷う場合はまず★3から着手する方法もあります。

Q ★3を取得してから★4を目指す必要がありますか？

取得の順序は定められていません。 自社の状況に応じて、どちらから着手するかを判断できます。

Q 確認責任者には研修が必要ですか？

必要です。対象資格に加え、所定の研修とSCSセキュリティ専門家登録が必要です。受講料は研修事業者が設定します。

Q 取得していないと罰則がありますか？

制度自体に行政罰・罰金の規定はありません。 ただし、取引先との契約・商取引上の不利益が生じる可能性はあります。

CLOSING

運営者情報・相談窓口・出典一覧

運営者情報

本資料は、サイバーセキュリティ情報サイト「**サイバーセキュリティ.com**」（**運営：株式会社セキュアオンライン**）が作成しました。
同サイトは10年以上にわたりサイバーセキュリティに関する情報発信を続けています。

専門家への相談

SCS評価制度への対応について、自社だけで判断が難しい場合は、**専門家への相談**も選択肢の一つです。
弊社が運営する「セキュリティエージェント」ではセキュリティ専門家（情報処理安全確保支援士）が300名以上が登録しており対応可能です。

出典一覧

IPA	基本規程・制度の詳細情報 登録・更新、制度運営体制、評価の流れ
IPA	研修実施基準（2026年9月11日） 指定申請FAQ（2026年10月21日版）
IPA	料金設定のお知らせ（2026年9月18日） 企業の登録料と事業者の指定料金
IPA	要求事項・評価基準Ver.1.1と各ガイド https://www.ipa.go.jp/security/scs/requirements-criteria.html
IPA	公式FAQ（2026年10月30日更新） 開始時期、専門家の要件、今後の予定

情報基準日：2026年11月2日

本資料は公開時点でIPA・経済産業省が公表している情報をもとに作成しています。制度の詳細は今後更新される可能性があるため、最新情報は公式サイトでご確認ください。本資料は経済産業省・IPAの公式資料ではなく、株式会社セキュアオンラインが作成した情報資料です。

発行：サイバーセキュリティ.com（株式会社セキュアオンライン）