

CSIJ 共通評価フレームワーク（クラウド版） アンケート調査結果レポート 「2024 年度 一般公開版」



**※本レポートは一般公開用として
調査のポイントのみを公開しています。**

サイバーセキュリティイニシアティブジャパン（CSIJ）
2024 年 9 月 2 日

目次

1. 本調査の概要.....	- 3 -
1.1. 調査目的	- 3 -
2. 総評	- 4 -
3. 前回調査結果との比較	- 5 -
3.1. 全体の傾向.....	- 5 -
3.2. 分野別の傾向（実施率が高いカテゴリ、低いカテゴリ）	- 6 -
3.3. 組織属性による傾向	- 7 -
3.4. 対応が進んでいない項目	- 8 -
4. 調査分析結果	- 8 -
4.1. 全体の実施率分布.....	- 8 -
4.2. 外部セキュリティベンダの利用状況による分析	- 9 -
4.3. クラウド環境におけるリスク/インシデント事例に関する実施率	- 13 -
4.4. 業種・業界別の利用状況について	- 19 -
5. 集計結果より提言.....	- 21 -
6. CSIJ の活動.....	- 23 -
6.1. CSIJ は評価フレームワークを通して、企業の対策のサポートを実現します。.....	- 23 -
6.2. 本アンケート調査方法の詳細	- 24 -

1. 本調査の概要

1.1. 調査目的

CSIJ 共通評価フレームワーク(クラウド版)を活用し、企業のクラウドセキュリティ対策の現状を把握・分析することにより、企業の課題を明らかにし、クラウド技術の安全な利用を促進するとともに、クラウドセキュリティに関する啓発活動を展開することを目的としている。

1.2. 調査対象

クラウドサービス(IaaS, PaaS, SaaS)[※]を利用している企業

※ IaaS, PaaS, SaaS はそれぞれ責任分界点が異なるため企業が意識するセキュリティ対策も異なると判断し、クラウドサービス形態毎に調査を実施している。

1.3. 調査方法

クラウドサービスを利用している企業のセキュリティ、システム、ネットワーク等を管理している担当者や意思決定者に対し、CSIJ 共通フレームワーク(クラウド版)を活用したアンケート調査を実施して調査した。

なお、調査方法の詳細については本レポートの末尾に記載している。

2. 総評

本調査では、クラウドサービスを利用する上での基本的な事項について、遵守できているかをアンケート形式で確認し、回答結果から実施率を算出している。

本調査においてはクラウドサービスの形態別（IaaS,PaaS,SaaS）に調査を行っているが、いずれの形態においても実施率が 60%台であった。本調査の設問は「クラウドサービスを利用する上での基本的な事項」の実施率を問うものであるため、100%に近い実施率を期待するものであったが、実施率全体の実施率が 60%台という結果であり、我々の期待や想定を下回るものであった。特にインシデントが発生した際の対応手順の整備状況に関する設問（インシデントレスポンスカテゴリ）や、設定状況・脆弱性情報の管理に関する設問（設定・脆弱性管理カテゴリ）においては実施率が低く、対策が不足している状況が見られた。

本調査の結果を企業の従業員規模別にみた場合、従業員規模が大きくなるほど実施率も高くなる傾向が見られた。企業規模が大きいほど、効果的に外部ベンダを活用しつつセキュリティ投資や教育を継続的に実施しているものと考えられる。中小規模の企業においても外部ベンダを活用している企業ではそうでない企業と比較して明確に実施率が高い結果となっており、外部ベンダの支援によって限られた社内リソースをより効果的に活用できているものと思われる。

業種・業界別にみた場合でも概ね全ての業界において、外部ベンダの利用に積極的であり、また外部ベンダを活用している企業の方が実施率においても良い結果が見られた。一方で、一部の業界においては外部ベンダの利用率が低いながらも実施率が高いものがあり、業種・業界特有の方針やノウハウがあるものと考えられる。

先述の通り本調査では 100%に近い実施率を期待するものであるため、60%台の実施率ではクラウドサービス利用にあたってのセキュリティ上の取り組みが不足しており、中小規模の企業を含めて社会全体のセキュリティ意識の向上・取り組みの促進が必要であると考え。CSIJ としては今後もセキュリティ啓発活動や会員各社の業務を通じて、セキュリティ状況改善を実施していきたい。

3. 前回調査結果との比較

CSIJ では、2022 年 12 月にも本フレームワークを使用した調査を実施し、その結果を公開している。その際の結果と本調査の結果との比較を以下に示す。

(参考：2022 年度調査結果「クラウド時代の セキュリティマネジメント」

https://www.csi-japan.org/_files/ugd/e66227_ef6f7303401643bc8d7762e4f5de6d3d.pdf)

3.1. 全体の傾向

全体の実施率(IaaS, PaaS, SaaS の合計)を以下に示す。

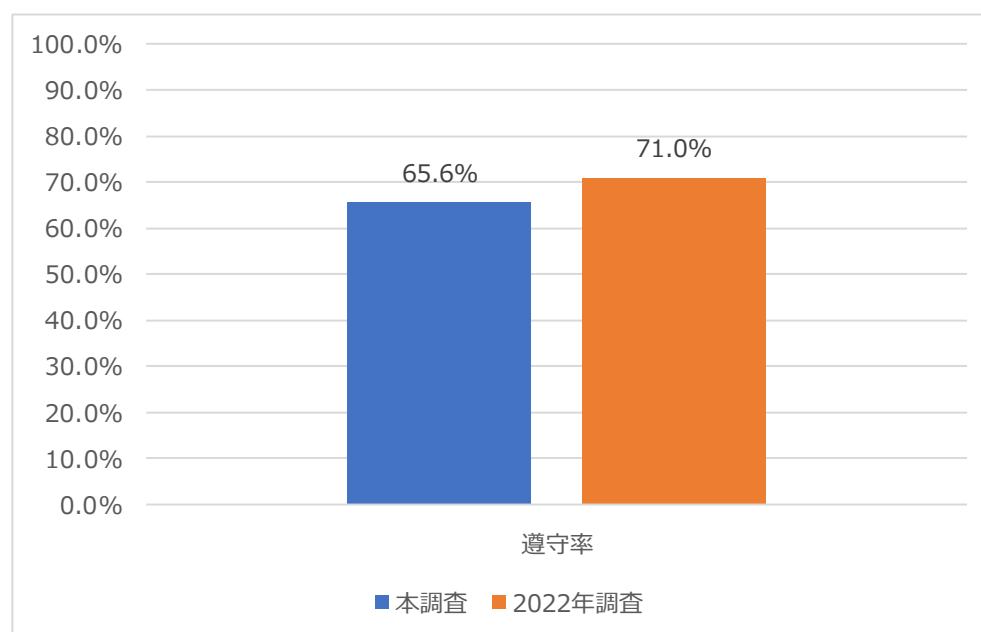


図 3-1：前回調査との実施率の比較

全体の実施率は 2022 年度調査の結果から約 3.4% 下がる結果となった。

2022 年の調査では、CSIJ 会員企業の顧客を中心に調査を行った。サイバーセキュリティの対策に興味・関心を持っている企業を対象としているため、今回調査よりも実施率が高かったと考えられる。

一方で、今回の調査は無作為に抽出した企業を対象としているため、より社会一般の実態を表した結果と考えられる。

3.2. 分野別の傾向（実施率が高いカテゴリ、低いカテゴリ）

カテゴリ毎の実施率を以下に記す。

表 3-1：前回調査とのカテゴリごとの実施率

	本調査結果		2022 年調査結果	
実施率が高かった カテゴリ	認証・アカウント管理	67.59%	データ保護・通信保護	84%
実施率が低かった カテゴリ	インシデントレスポンス	64.74%	設定・脆弱性管理	59%
	設定・脆弱性管理	64.86%	ガバナンス	52%

2022 年の結果と比較して、今回の調査では各カテゴリの実施率は認証アカウント管理の項目で高い実施率が出ていた。一方で、実施率の低い項目としてインシデントレスポンスが新たに抽出された。また 2022 年度調査から引き続き設定・脆弱性管理の項目も低い結果となっている。

クラウドサービスに対するセキュリティ対策における変動には以下のような要因が考えられる。

【会員限定公開部分】

要因分析の記述

3.3. 組織属性による傾向

企業規模毎の各カテゴリ平均実施率を以下に記す。

なお、本調査においては、従業員数 1-299 人を「小規模企業」、300-999 人を「中規模企業」、1000 人以上を「大規模企業」と定義している。

本調査結果

表 3-2：従業員規模別割合

従業員数	ガバナンス	インシデントレスポンス	コンプライアンス	設定・脆弱性管理	認証・アカウント管理	データ保護・通信保護
1-299	57.5%	55.8%	57.2%	56.0%	60.3%	56.0%
300-999	69.9%	66.8%	68.5%	70.2%	70.0%	68.5%
1000-	77.0%	76.2%	77.4%	73.2%	77.3%	75.3%
全規模	68.3%	66.4%	67.8%	66.8%	69.3%	66.8%

2022 年結果

表 3-3：従業員規模別割合

従業員数	ガバナンス	インシデントレスポンス	コンプライアンス	設定・脆弱性管理	認証・アカウント管理	データ保護・通信保護
1-299	57.8%	51.8%	54.4%	63.8%	79.6%	73.1%
300-999	—	75.0%	100.0%	50.0%	92.9%	50.0%
1000-	54.7%	77.3%	84.0%	56.2%	68.9%	86.0%
全規模	51.2%	73.8%	79.9%	59.4%	77.2%	83.0%

従業員規模別のセキュリティ実施率の変動は、企業の規模やリソースに依存する部分大きい。小規模企業はリソース不足により実施率が低下しやすく、中規模企業は管理の複雑さが課題であり、なおかつ大規模企業ほどのセキュリティが難しく、実施率を引き下げる要因となっているものと思われる。一方、大規模企業は全体的に高い実施率を維持しており、セキュリティ対策が進んでいる。全体のセキュリティ実施率を向上させるためには、各企業規模に応じた対策と支援が必要である。

前回調査ではセキュリティに力を入れている企業を対象にアンケートを実施したため、小規模・中規模企業においても大規模企業よりも実施率が高い項目が存在したが、本調査では無作為に選出した企業を対象に調査を行ったため、企業規模と実施率がおおよそ比例する結果となった。

3.4. 対応が進んでいない項目

対応が進んでいない項目(実施率が低い項目)を以下に記す。

【会員限定公開部分】

実施率が低い項目(今回及び 2022 年)の記述

4. 調査分析結果

本章では各設問の回答結果や、複数の設問の相関分析を実施、考察を示す。

4.1. 全体の実施率分布

本調査における全体の実施率の傾向について分析を行った。

実施率 91%~100%および実施率 0%~10%の両極端の回答が特に件数が多かったが、その中間については特段大きな差はみられず、特別な傾向は無いものと思われる。後述する「外部セキュリティベンダの利用経験有無」別においては、ベンダ利用経験なしの企業の方が実施率も低くなる傾向が見られた。

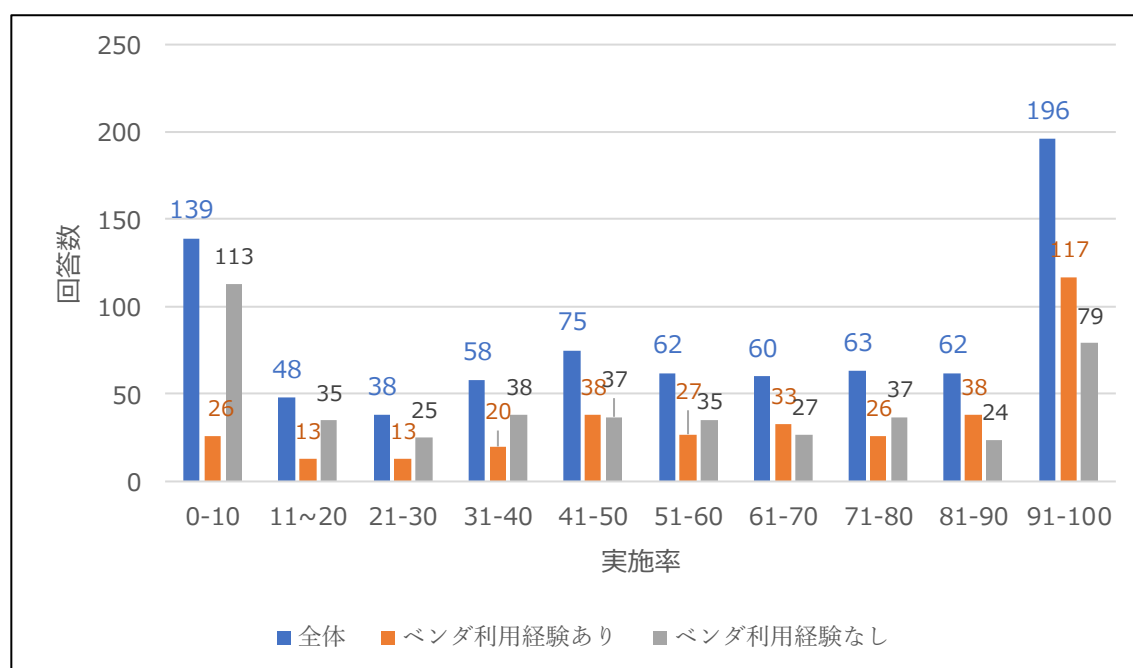


図 4-1：実施率ごとの回答件数の分布

4.2. 外部セキュリティベンダの利用状況による分析

本調査では、「クラウドサービスの構成や設定に関して、外部の専門家によるレビューや評価のサービス（例えば監査や診断など）を利用した経験はありますか。」という設問を設けた。

外部セキュリティベンダの利用有無により、セキュリティ対策にどのような傾向が表れるのか、以下に記す。

4.2.1. 外部セキュリティベンダの利用状況について

外部セキュリティベンダの利用について、“ある”と回答した企業は 351 社、“ない”と回答した企業は 450 社だった。

また、企業規模別に利用状況を確認すると、従業員数が 1-299 人以下の企業では外部ベンダの利用が 25%に留まっているのに対し、300-999 人の企業では 51.4%、1000 人以上の企業では 49.6%とそれぞれ 2 倍近い割合になっていることがわかった。

中規模企業よりも大規模企業の方がベンダ利用率が高くなる理由として、実施率従業員数の少ない企業では、セキュリティ対策にリソースを割くことが難しい一方で、1000 人以上の大企業では、自社内でセキュリティ対策の推進を行う環境を整えていることが、今回の調査結果となった一因と考えられる。

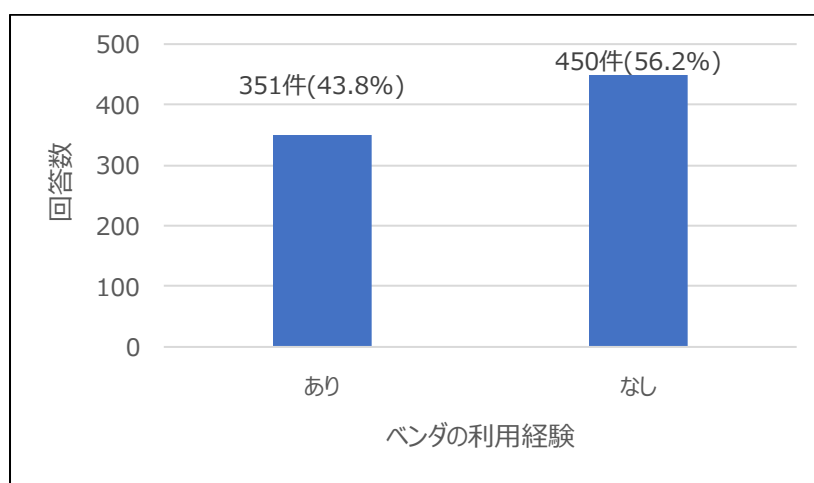


図 4-2：外部セキュリティベンダの利用状況

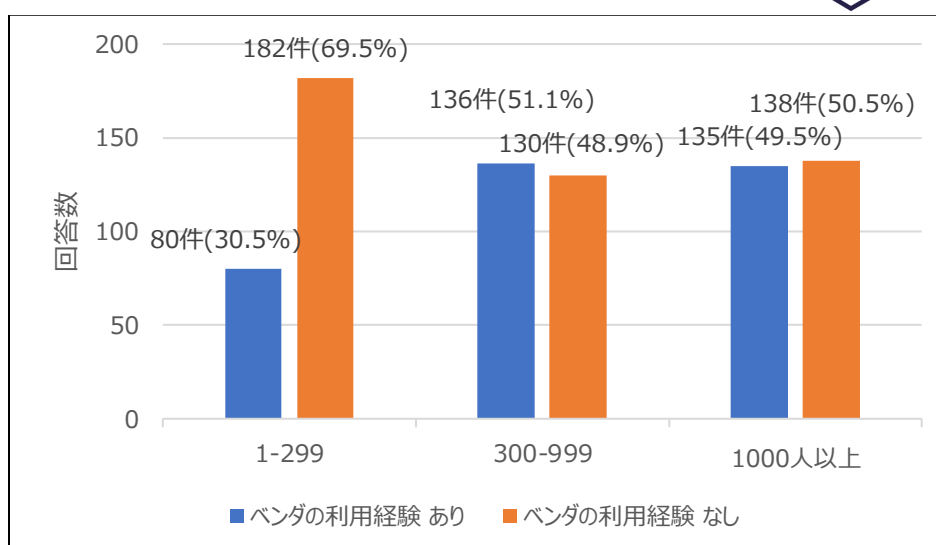


図 4-3：企業規模別外部セキュリティベンダの利用状況

4.2.2. 外部セキュリティベンダの利用状況と実施率の関連性について

外部セキュリティベンダの利用経験がある、と回答した企業の平均実施率は 75.9%、利用経験が無いと回答した企業の平均実施率は 60.7%となり、実施率において大きな差が生じていることがわかった。

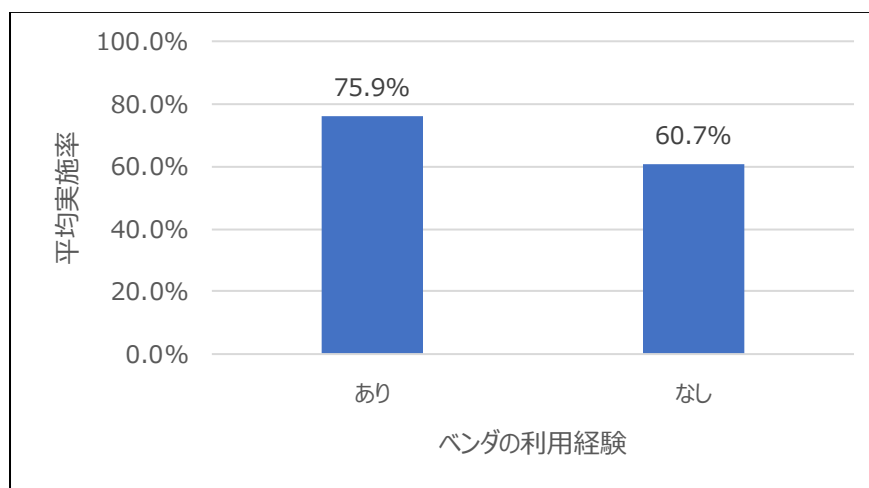


図 4-4：外部セキュリティベンダの利用経験別平均実施率

また、企業規模別の外部セキュリティベンダの利用有無と平均実施率は、下表の通りである。

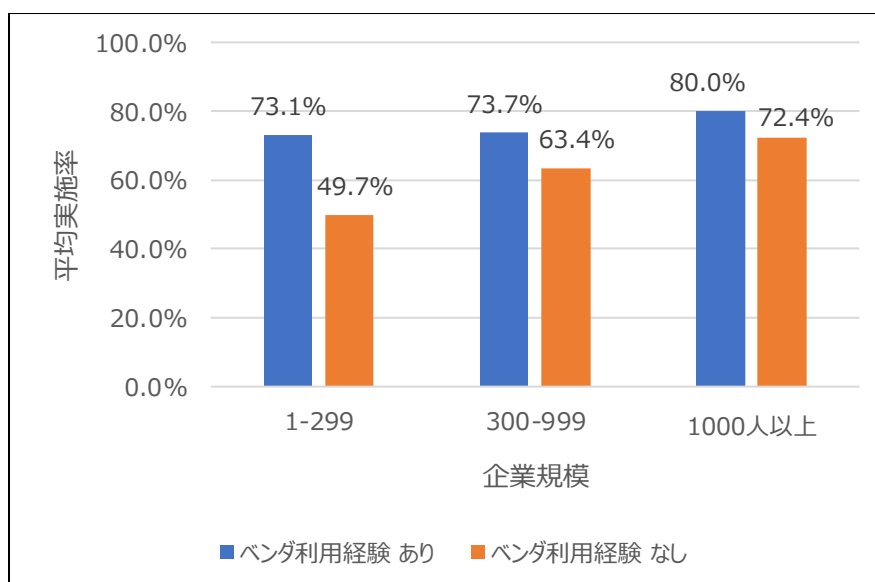


図 4-5：企業規模別外部セキュリティベンダの利用有無と平均実施率

外部セキュリティベンダを利用する企業の実施率が、いずれの規模においても利用しない企業を大きく上回っており、70%を超える高い遵守率となっていることが確認された。これは、セキュリティベンダが提供する専門的な知識やリソースが、企業のセキュリティ対策の実施に大きく貢献していること

を示している。特に、小規模企業では 30.3 ポイントの差異が見られ、内部リソースが限られている企業ほど、ベンダの支援が効果的であることがわかる。

企業規模に着目すると、企業規模が大きくなるにつれて、セキュリティ対策の実施率が向上する傾向が見られる。特に、1000 人以上規模の企業では、ベンダ利用企業の実施率が 80.0%に達しており、非利用企業でも 72.4%と比較的高い水準を保っている。これは、大規模企業が内部にセキュリティ推進組織を有しており、セキュリティ対策に割く予算やリソースも多いことが一因と考えられる。

一方で、小規模企業ではベンダを利用しない場合の実施率が 49.7%と非常に低く、セキュリティ対策が十分に実施されていないことが浮き彫りになった。これらの企業に対しては、外部セキュリティベンダの利用を推奨するとともに、無料で利用できるセキュリティリソースの提供などが必要と考えられる。

4.2.3. セキュリティベンダの利用有無の違いにより実施率の差が大きい設問

外部セキュリティベンダの利用有無による、実施率の差異が大きかった設問は下記の通りであった。

表 4-1：ベンダ利用の有無による実施率の差異

【会員限定公開部分】

ベンダ利用の有無による実施率の差異表(企業規模別)の記述

小・中規模企業において、セキュリティベンダの利用有無による大きな実施率の差異が見られる項目は、クラウドサービスの運用管理に関する基本的な体制の整備に集中していることがわかった。これは、小・中規模企業が内部リソースや専門知識の不足により、セキュリティ対策の基本的な運用管理体制を独自に整備することが難しいことが一因と考えられる。規模が小さいほど、規定類や手順書等の作成が困難であり、また属人的な対応で業務をこなす傾向が強いため、承認フロー等の業務プロセスが整備されづらく、形骸化しやすい状況にある。

一方で、大規模企業におけるセキュリティベンダの利用は、クラウドサービスの高度な運用管理と評価において重要な役割を果たしていると考えられる。特に、ソフトウェアの管理、診断の実施、提供事業者の評価といったプロセスにおいて、ベンダの専門知識やリソースが大きな効果を発揮している。ベンダの支援を受けることで、これらのプロセスが標準化され、セキュリティリスクの低減と企業全体のセキュリティレベルの向上が実現される。

本結果から、企業規模に応じたセキュリティベンダの支援の重要性が改めて確認された。特に、小規模および中規模企業においては、内部リソースや専門知識の不足を補完するために、ベンダの支援が不可欠であると考えられる。一方で、大規模企業は複雑なシステム管理と高度な評価が求められ、ベンダの専門的なサービスがそのニーズを満たしているように見受けられる。

4.3. クラウド環境におけるリスク/インシデント事例に関する実施率

クラウドサービスが利用される中で、多くのインシデントが発生している。これらのインシデントには、人為的な設定ミスによる情報漏えいもあれば、マルウェアなど悪意ある攻撃によるものも含まれている。

このようなインシデントが発生する背景には、クラウドサービスの複雑さとそれに伴う管理の難しさがある。

そこで本章では、今回の調査結果を基に、インシデントに関連する設問に焦点を当て、その実施率を比較・分析を行う。

4.3.1. アカウント窃取

アカウント窃取・乗っ取りに関連する調査項目は以下 6 つであった。

表 4-2：アカウント窃取・乗っ取りに関連する調査項目

項目番号	調査項目
30	特権アカウント、運用者・開発者用アカウント、利用者用アカウントについて、認証機能を用いて認証を実施していますか。
31	クラウドサービス環境へアクセスする特権アカウント、運用者・開発者用アカウントについて、多要素認証を利用していますか。
32	特権アカウント、運用者・開発者用アカウントについて、新規登録、更新及び削除を行う場合の申請・承認フローは存在しますか。
34	特権アカウント、運用者・開発者用アカウント、利用者用アカウントについて、複数回ログインを失敗した場合にアカウントをロックする仕組みはありますか。併せて、管理者に通知する仕組みはありますか。
35	特権アカウント、運用者・開発者用アカウント、利用者用アカウントについて、適切なパスワードポリシーを設けて定義していますか。
36	特権アカウント、運用者・開発者用アカウント、利用者用アカウントについて、アカウントの利用者やアクセス権限は必要最小限に絞って割り当てられていますか。

表 4-3：企業規模とベンダ利用経験別実施率

項目番号	1-299 人		300-900 人		1000 人以上	
	ある	ない	ある	ない	ある	ない
30	76.7%	62.4%	72.8%	72.3%	81.9%	75.0%
31	71.9%	45.1%	76.1%	61.9%	80.7%	72.1%
32	70.6%	50.0%	74.3%	63.5%	79.6%	69.6%
34	78.8%	53.3%	73.2%	65.8%	80.4%	78.3%
35	72.5%	58.0%	75.0%	64.6%	80.4%	77.5%
36	71.9%	60.7%	73.2%	71.5%	80.8%	74.6%

【会員限定公開部分】
調査項目間の相関係数分析の記述

小規模組織では、全ての項目で実施率が低く、特に多要素認証（MFA）の導入率が 36.1% と低迷している。小規模企業のセキュリティ対策の不備は、サプライチェーンリスクを引き起こす可能性が高く、全体のセキュリティレベルに影響を与えるため、対策の強化が必要である。

また、大規模企業においても未だ 30% 台の企業が対策を実施していない状況がうかがえる。100%の実施率を期待する本調査においては物足りない結果となった。

調査項目間での実施率の相関について、IaaS・SaaS カテゴリにおいては各設問間での回答状況に全体的に相関が見られた。設問 30 と設問 36 においては強い相関関係があり、各種アカウントの認証を実施している企業は、それぞれ最小限の権限を付与する運用に留意している現状がうかがえる。

4.3.2. 設定ミスによる情報漏えい

設定ミスによる情報漏えいに関する設問は以下 6 つであった。

表 4-4：情報漏洩に関する調査項目

項目番号	調査項目
2	クラウドサービス利用に関して、利用申請・承認フローを整備していますか。
15	クラウドサービス環境のサーバやネットワーク機器などのセキュリティに関するシステムの監視をしていますか。
22	クラウドサービス環境に関するシステムの構成情報を管理していますか。
23	システム（クラウドサービス上のネットワーク機器および仮想コンテナ）の変更管理を行う場合、適切な変更プロセスに基づいてリリース前レビューを実施していますか。
25	利用しているクラウドサービス（仮想コンテナ）において、不要なサービス（ポート、プロトコルなど）は、停止していますか。
36	特権アカウント、運用者・開発者用アカウント、利用者用アカウントについて、アカウントの利用者やアクセス権限は必要最小限に絞って割り当てられていますか。

表 4-5：企業規模とベンダ利用経験別実施率

項目番号	1-299 人		300-900 人		1000 人以上	
	ある	ない	ある	ない	ある	ない
2	81.9%	46.7%	79.0%	60.4%	83.3%	70.7%
15	69.6%	56.4%	76.7%	65.6%	77.1%	77.0%
22	79.5%	47.7%	80.7%	68.9%	80.9%	72.4%
23	68.8%	44.8%	69.9%	59.0%	73.5%	69.7%
25	66.1%	51.2%	70.5%	63.1%	71.0%	68.4%
36	71.9%	60.7%	73.2%	71.5%	80.7%	74.6%

【会員限定公開部分】

調査項目間の相関係数分析の記述

設定ミスによる情報漏えいは頻繁に発生しており、比較的高い実施率の大企業においても多数報告されているのが現状である。人的ミスを 0 にすることは困難であるため、申請・承認フローの整備やセキュリティ監視、システム構成情報の管理アクセス権限の最小化といった運用面/技術面の両面から対策を推進することが重要と考えられる。

調査項目間での実施率の相関について、IaaS カテゴリにおいては各設問間での回答状況に一定程度の相関が見られた。特に設問 22 と設問 15 および設問 23 には強い相関がみられ、昨今のランサムウェア等のセキュリティ脅威の高まりから、構成情報の管理と共にシステム監視・変更管理を実施し、自社環境情報のリアルタイムな把握に注力している状況が伺える。

4.3.3. 脆弱性管理、対策

脆弱性を悪用した攻撃は引き続き多く確認されている。最近では、ベンダがパッチをリリースする前に攻撃者が脆弱性を発見し、攻撃を仕掛けるゼロデイ攻撃も確認されている。このような観点から、クラウド環境においても脆弱性の管理・対応は昨今のセキュリティ対策において切っ掛けを離せない対策となっている。

以下に、本調査より脆弱性管理に関する調査項目を列挙した。

【会員限定公開部分】

脆弱性管理に関する調査項目別実施率表の記述

4.3.4. 不正アクセス

クラウドサービスに対する不正アクセス事例が多く確認されている。主に、アカウント管理の不備によって、クラウドサービスのアカウント情報が攻撃者の手に渡り、不正アクセスおよび情報の窃取に繋がる事例が多くみられる。このような観点からアカウント管理や多要素認証の設定、およびインシデント発生時の対策手順の策定が重要となっている。

以下に、本調査より不正アクセスに関する調査項目を列挙した。

【会員限定公開部分】

不正アクセスに関する調査項目別実施率表の記述

4.3.5. 情報漏えい

先述したクラウドサービスに対する不正アクセスが発生することで、クラウドサービス上に保管されたデータが漏えいする事例が確認されている。また、悪意の有無に関わらずクラウドサービスの設定ミスによる情報漏えい事例も存在するため、攻撃への対策と併せて、設定ミスを防止するための教育やレビュー体制の整備が重要である。

以下に、本調査より情報漏えいに関する調査項目を列挙した。

【会員限定公開部分】

情報漏えいに関する調査項目別実施率表の記述

4.3.6. シャドーIT

組織の規程・ルールでは利用が認められていないクラウドサービスを無断で利用する事例(シャドーIT)が多く確認されている。シャドーIT の問題点として、組織内におけるクラウドサービス利用実態の全容把握が困難になり、機密情報等が漏えいした際などに対応が遅れることが挙げられる。

このため、組織内におけるクラウドサービス利用規定・ルールの整備や周知が重要である。

以下に、本調査よりシャドーIT に関する調査項目を列挙した。

【会員限定公開部分】

シャドーIT に関する調査項目別実施率表の記述

4.3.7. データ消失

攻撃やクラウドサービス提供事業者の都合等によりクラウドサービス上のデータが消失・利用不可となった場合、業務の停滞や顧客・取引先への損害に発展する恐れがある。そのため、これらの事象への備えとして、バックアップの実施や対応手順の策定が重要である。

以下に、本調査よりデータ消失に関する調査項目を列挙した。

【会員限定公開部分】

データ消失に関する調査項目別実施率表の記述

4.4. 業種・業界別の利用状況について

業種・業界別の実施率を以下に記す。

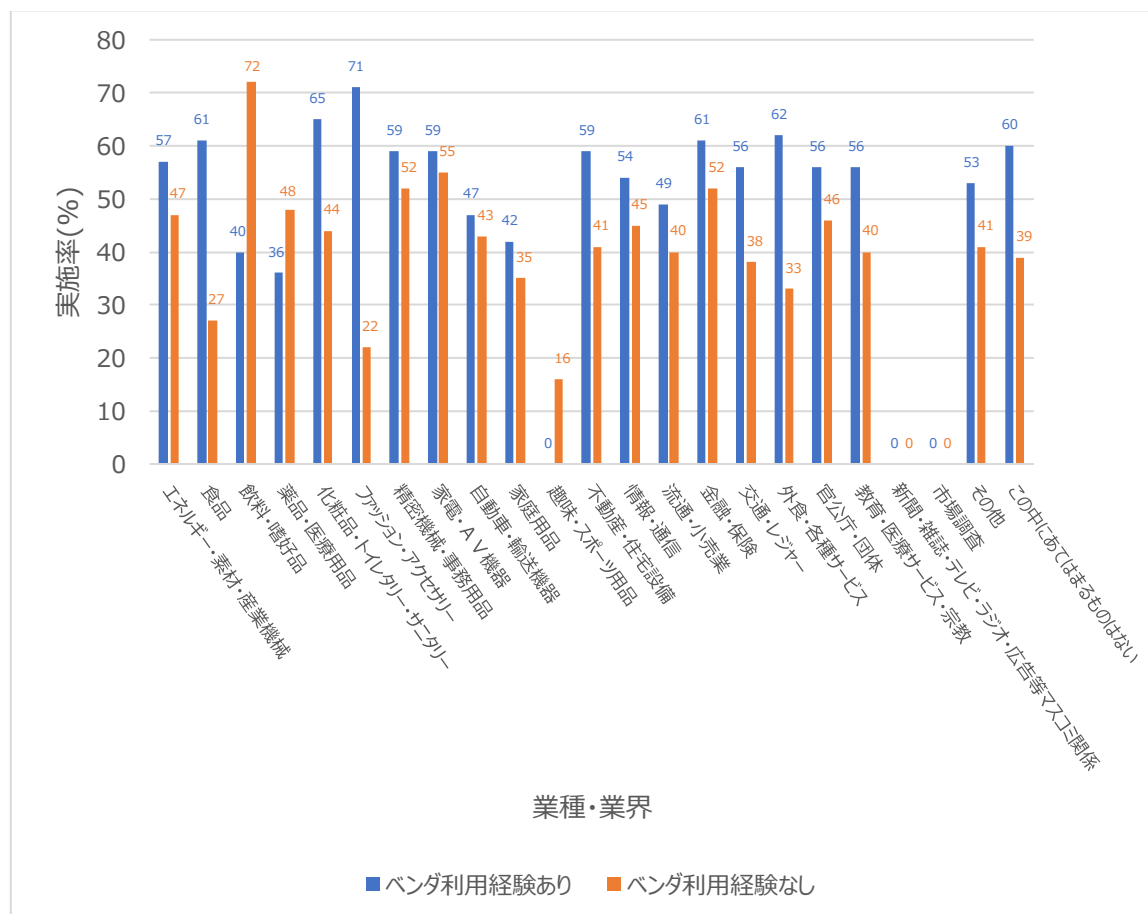


図 4-6：業種・業界別の実施率の分布

概ねすべての業種・業界において、外部ベンダを利用した経験のある企業の実施率がそうでない企業を上回る結果となった。

また、回答数においても多くの業種・業界で外部ベンダを利用した経験のある企業が多数であるが、一部業界ではベンダを利用していない企業の数が多くなっている。

「金融・保険」業界や、「家電・AV 機器」「エネルギー・素材・産業機械」業界等においては実施率が高く、また外部ベンダも積極的に活用している状況が見られた。一方で、「飲料・嗜好品」「薬品・医療用品」業界においては外部ベンダを利用していない回答が多く、特に「飲料・嗜好品」業界は外部ベンダを利用せずに内製で対策し、実施率が高い対策状況となっている。

4.4.1. 平均実施率の高い業界における、実施率の低い設問について

表 4-6：平均実施率の高い業界(上位 3 業界)

順位（上位）	業界・業種	実施率
1	金融・保険	78.6%
2	家電・A V 機器	78.0%
3	エネルギー・素材・産業機械	76.6%

※20 件以上の回答があった業界・業種を対象に集計

※「その他」および「この中にあてはまるものはない」回答は除外

【会員限定公開部分】

実施率上位 3 業界における実施率の低い調査項目の記述

4.4.2. 平均実施率の低い業界における、実施率の低い設問について

表 4-7：平均実施率の低い業界(下位 3 業界)

順位（下位）	業界・業種	実施率
1	交通・レジャー	57.6%
2	外食・各種サービス	59.4%
3	流通・小売業	61.9%

※20 件以上の回答があった業界・業種を対象に集計

※「その他」および「この中にあてはまるものはない」回答は除外

【会員限定公開部分】

実施率下位 3 業界における実施率の低い調査項目の記述

5. 集計結果より提言

本調査においては全体的に中小規模の企業は、大規模企業と比較して対策ができていない傾向が見られた。そのため、中小企業のセキュリティ対策を促進させることで、全体的なクラウドセキュリティ施策のレベルを底上げする必要がある。

本調査において特に実施率が低かった項目として、設問 20 や設問 18 等のインシデントレスポンスに関連する課題が挙げられる。また、設問 33 設問 32 等の設定・脆弱性管理にまつわる課題も多く確認されたため、クラウドの設定状況の見直しや、インシデント発生に備えて対応体制の強化が必要である。これらの課題は CSIJ 会員各社のサービスにおいて改善の支援が可能であるため、自社内での対策が困難な場合は外部ベンダの活用も検討いただきたい。

以下に本調査にて実施率が低かった設問と、それに対応する CSIJ 会員企業の提供製品・サービス例を記載する。

表 5-1：実施率が低かった設問と対応する製品・サービス例

ワースト	実施率	設問 No.	設問	対応製品・サービス例
1	63.2%	設問 33	開発環境において、テストフェーズなどで本番環境のデータを利用する際に、データの無害化などを実施していますか。	グローバルセキュリティエキスパート株式会社 -文書作成支援
		設問 20	サービスの計画停止に際し、自社業務および、顧客提供サービスへの影響範囲・内容の確認を実施していますか。また、その対応を事前に用意していますか。	株式会社ラック -定期コンサルティング -セキュリティドキュメンテーション支援 等 グローバルセキュリティエキスパート株式会社 -文書作成支援 -CSIRT 構築支援 等 エムオーテックス株式会社 -個別方針策定支援
3	63.8%	設問 22	N T P 機能を利用し、時刻同期を行っていますか。	株式会社ラック -定期コンサルティング -セキュリティ監査 等 グローバルセキュリティエキスパート株式会社 -アセスメント
4	64.1%	設問 32	システム（クラウドサービス上のネットワーク機器及び仮想コンテナ）の変更管理を行う場合、適切な変更プロセスに基づいて、リリース前レビューを実施していますか。	株式会社ラック -プラットフォーム診断 -Web アプリケーション診断 等 グローバルセキュリティエキスパート株式会社 -文書作成支援 -アセスメント 等

ワースト	実施率	設問 No.	設問	対応製品・サービス例
5	64.2%	設問 18	クラウドサービス環境で発生したインシデント対応に関して、役割や担当を定義していますか。	株式会社ラック -定期コンサルティング -セキュリティドキュメンテーション支援 等 グローバルセキュリティエキスパート株式会社 -インシデント対応規程 -CSIRT 構築支援 等 エムオーテックス株式会社 -マニュアル策定支援 -インシデント訓練
		設問 51	特権アカウント、運用者・開発者用アカウント、利用者用アカウントについて、パスワードを保存する時に暗号化またはハッシュ化していますか。	株式会社ラック -HashiCorp Vault グローバルセキュリティエキスパート株式会社 -文書作成支援 -クラウド診断 等
7	64.6%	設問 19	クラウドサービス環境で発生したインシデントに関して、自社内で優先度を定めるための基準が存在しますか。	株式会社ラック -定期コンサルティング -セキュリティドキュメンテーション支援 等 グローバルセキュリティエキスパート株式会社 -アセスメント -文書作成支援 等 エムオーテックス株式会社 -マニュアル策定支援
8	65.0%	設問 34	利用しているクラウドサービス（仮想コンテナ）において、不要なサービス（ポート、プロトコルなど）は、停止していますか。	株式会社ラック -プラットフォーム診断 -Web アプリケーション診断 等 グローバルセキュリティエキスパート株式会社 -アセスメント -プラットフォーム診断 等
9	65.3%	設問 49	仮想コンテナ（インスタンス）に作成したサーバに関して、マルウェア対策ソフトを導入していますか。	グローバルセキュリティエキスパート株式会社 -プラットフォーム診断 -CrowdStrike Falcon 等 エムオーテックス株式会社 -LANSCOPE Cyber Protection ・CylancePROTECT ・DeepInstinct
10	65.4%	設問 26	取得したバックアップを用いたリストア手順は作成していますか。	株式会社ラック -定期コンサルティング -セキュリティドキュメンテーション支援 等 グローバルセキュリティエキスパート株式会社 -アセスメント -文書作成支援 等 エムオーテックス株式会社 -マニュアル策定支援

6. CSIJ の活動

昨今のサイバーセキュリティにおいては、予防的観点からも考慮された適切かつ継続的な対応を行い、安全・安心な事業継続を図ることが重要であるとともに、これらの対策を行いうる人材の確保も大きな課題となっている。

このような状況における課題解決に向けて、CSIJ では環境変化を常にキャッチアップし、これからの将来を見据えて企業が行うべき必要かつ現実的で、さらには日本の市場特性も考慮した「サイバーセキュリティ対応」の提言と、実効性のある実装にむけた支援を行い、この「サイバーセキュリティ対応・実装」に必要な人材輩出に向けた活動も実施している。

6.1. CSIJ は評価フレームワークを通して、企業の対策のサポートを実現します。

CSIJ では環境変化を常にキャッチアップし、これからの将来を見据えて企業が行うべき必要かつ現実的、さらに、日本の市場特性も考慮した「サイバーセキュリティ対応」を提言するだけでなく、実装にむけての支援を行います。加えて、この「サイバーセキュリティ対応・実装」に必要な人材輩出に向けた活動も実施します。

現在、CSIJ では「共通対策評価フレームワーク分科会」および「サイバーセキュリティプロフェッショナル人材フレームワーク分科会」の二つの分科会が活動しております。

共通対策評価フレームワーク分科会では下記の観点で共通対策評価フレームワークを作成しております。

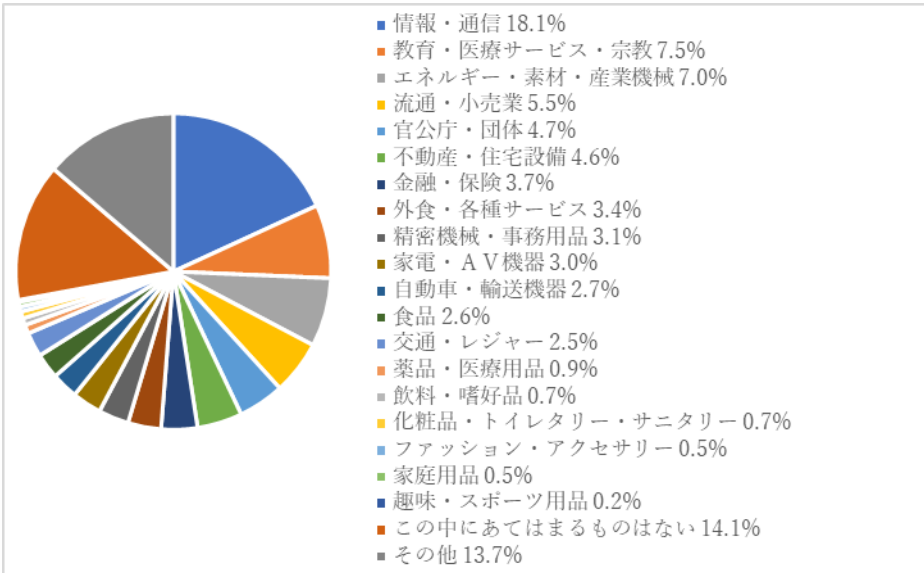
- 新領域（クラウド、ゼロトラスト等）利用にフォーカスし、日本特有環境を踏まえ広範に企業が活用できる内容とする。
- 既存の各種国際・国内基準、ガイドラインの内容をベースとしつつ、具体的・網羅的かつシンプルに重要ポイントを押さえた内容とする。
- この「セキュリティ対策評価フレーム」評価結果を踏まえた具体的な対策支援が、会員企業から顧客企業に提供できるよう連携を図る。
- 評価データを蓄積し、企業（業種別、規模別など）セキュリティレベルの実状概況を把握可能とする（予定）。

CSIJ の活動詳細は下記リンク（CSIJ 公式ウェブサイト）の活動内容をご覧ください。

- CSIJ 活動内容
<https://www.csi-japan.org/active>

6.2. 本アンケート調査方法の詳細

調査目的	企業のクラウドセキュリティ対策の現状を把握・分析することで課題を明らかにし、クラウド技術の安全な利用を促進し、クラウドセキュリティに関する啓発普及活動に展開することを目的としている。
調査手法	インターネット調査
調査対象	クラウドサービス(IaaS, PaaS, SaaS)(※1)を利用している企業のセキュリティ、システム、ネットワーク等を管理している担当者や意思決定者 ※1…IaaS, PaaS, SaaS はそれぞれ責任分界点が異なるため企業が意識するセキュリティ対策も異なると判断し、クラウドサービス形態毎に調査を実施している。
調査内容	回答者の属性を調査する設問(10 問)と、クラウドのセキュリティ対策の状況を問う 6 カテゴリー(※2)の設問(最大 42 問)に回答。 6 カテゴリーの設問数は、「最も使用しているクラウドサービス形態」の項目で回答したクラウドサービスによって変動する。 IaaS…42 問 PaaS…41 問 SaaS…28 問 (※2)＜評価カテゴリー＞ ① ガバナンス…クラウドの利用に関するルールの整備や教育の実施など、クラウド利用の前提となるガバナンス整備状況を確認するカテゴリー ② インシデントレスポンス…ログの取得やインシデントレスポンスの整備など、インシデント発生時の対応準備状況を確認するカテゴリー ③ コンプライアンス…レギュレーションに沿ったデータ保存国やその他契約などのコンプライアンス面の状況を確認するカテゴリー ④ 設定・脆弱性管理…クラウドサービスに関する設定や脆弱性の管理状況を確認するカテゴリー ⑤ 認証・アカウント管理…クラウドサービスに関する認証やアカウントの管理に関する整備状況を確認するカテゴリー ⑥ データ保護・通信保護…クラウドサービスに関するデータ保護や通信保護に関する対応状況を確認するカテゴリー

分析方法	○×△の 3 段階で設問に回答してもらい、得点を算出。得点を利用し、実施すべき対策がどれくらいできているかをセキュリティ対策実施率として表す。(以下、実施率と表記) ○…設問内容を実施している。(2 点換算) ×…設問内容を実施していない。(0 点換算) △…○とも×とも断定できない実施状況である。(1 点換算) 実施率…獲得点数/総得点数(単位: %)																									
サンプル数	総計 801 サンプル ＜クラウドサービス提供形態・従業員規模ごとの回収数詳細＞ <table><tr><th></th><th>従業員 1-299 人の企業</th><th>従業員 300-999 人の企業</th><th>従業員 1000 人-の企業</th><th>TOTAL</th></tr><tr><td>IaaS</td><td>101</td><td>99</td><td>105</td><td>305</td></tr><tr><td>PaaS</td><td>120</td><td>117</td><td>116</td><td>353</td></tr><tr><td>SaaS</td><td>41</td><td>50</td><td>52</td><td>143</td></tr><tr><td>TORAL</td><td>262</td><td>266</td><td>273</td><td>801</td></tr></table> ＜回答者業界割合＞  - 情報・通信 18.1% - 教育・医療サービス・宗教 7.5% - エネルギー・素材・産業機械 7.0% - 流通・小売業 5.5% - 官公庁・団体 4.7% - 不動産・住宅設備 4.6% - 金融・保険 3.7% - 外食・各種サービス 3.4% - 精密機械・事務用品 3.1% - 家電・A V機器 3.0% - 自動車・輸送機器 2.7% - 食品 2.6% - 交通・レジャー 2.5% - 薬品・医療用品 0.9% - 飲料・嗜好品 0.7% - 化粧品・トイレタリー・サニタリー 0.7% - ファッション・アクセサリー 0.5% - 家庭用品 0.5% - 趣味・スポーツ用品 0.2% - この中にあてはまるものはない 14.1% - その他 13.7%		従業員 1-299 人の企業	従業員 300-999 人の企業	従業員 1000 人-の企業	TOTAL	IaaS	101	99	105	305	PaaS	120	117	116	353	SaaS	41	50	52	143	TORAL	262	266	273	801
	従業員 1-299 人の企業	従業員 300-999 人の企業	従業員 1000 人-の企業	TOTAL																						
IaaS	101	99	105	305																						
PaaS	120	117	116	353																						
SaaS	41	50	52	143																						
TORAL	262	266	273	801																						
調査時期	2024 年 1 月～2 月																									
調査主体	サイバーセキュリティニシアティブジャパン																									

■ 本調査結果レポート作成者（敬称略、五十音順）

作成者	所属企業
足立 道拡 上田 直哉 広瀬 真一 山口 雅史	NRI セキュアテクノロジーズ株式会社
小関 直樹 刀川 郁也	エムオーテックス株式会社
西野 哲生	グローバルセキュリティエキスパート株式会社
仲上 竜太 安田 良明	ニューリジェンセキュリティ株式会社
奥野 康城（評価分科会リーダー） 岡本 大輝 櫻井 祐輔 谷口 諒之介 藤原 青空 持田 啓司（CSIJ 事務局代表）	株式会社ラック

■ CSIJ 入会案内

本調査結果レポートの会員限定公開部分については、CSIJ 入会により閲覧可能となります。

入会のご検討をいただけますと幸いです。

<https://www.csi-japan.org/join>

■ 本調査結果レポートに関するお問合せ先（制作・著作）

サイバーセキュリティイニシアティブジャパン（CSIJ）

東京都千代田区平河町 2 丁目 16 番 1 号 平河町森タワー

E-Mail : sec@csi-japan.org

URL : <https://www.csi-japan.org/>

