

報道関係各位

株式会社 USEN ICT Solutions

## 「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」スタートに向け 全国1,932名の情シス担当者に聞いた、セキュリティ対策の実態調査レポートを公開

USEN&U-NEXT GROUPの株式会社 USEN ICT Solutions（本社：東京都品川区、代表取締役社長：高橋 領一、以下、当社）は、企業におけるセキュリティ対策の実態を明らかにするため、全国1,932名の情報システム担当者を対象にヒアリング調査を実施し、本日2月3日（火）に調査レポートを公開したことをお知らせします。



### ■調査実施の背景

近年、大企業のみならず中堅・中小企業を起点としたサプライチェーン攻撃が増加しており、取引先を含めた包括的なセキュリティ対策の重要性が一層高まっています。こうした状況を背景に、経済産業省では、企業に求められるセキュリティ対策の成熟度を共通の基準で可視化する「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（以下、SCS評価制度）※1」の運用開始を、2026年度末頃に向けて進めています。

※1 企業に求められるセキュリティ対策の成熟度を複数段階で評価し、共通の基準で可視化することで、サプライチェーン全体でのセキュリティ水準の向上を図る制度です。

参考：経済産業省ウェブサイト (<https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html>)

制度開始を見据え、多くの企業が自社のセキュリティ体制の棚卸しや課題整理に着手し始めている一方で、現場では「どこまで対策すべきか分からぬ」「他社と比べて自社の水準が適切なのか判断できない」といった声も少なくありません。制度やガイドラインの存在は認識していても、実際の運用や対応の優先順位付けに悩むケースが多いのが実情です。

そこで当社では、単なる導入有無や意識調査にとどまらず、実際の運用状況や担当者が直面している課題を明らかにすることを目的に、日々のお客様との対話を通じて収集してきた延べ1,932名分の回答・相談内容を対象に、項目ごとに整理・分析しました。その結果をホワイトペーパーとしてまとめたものが、「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スタート直前！情シス1,932名に聞いたセキュリティ対策の実態調査レポート」です。

Webアンケートでは把握しにくい、運用負荷や人材不足、対応の優先順位付けといった現場視点の実情を可視化することで、企業が自社のセキュリティ対策を客観的に見直し、次の一手を検討するための材料を提供することを目的としています。

## ■本調査データから見えてきたこと

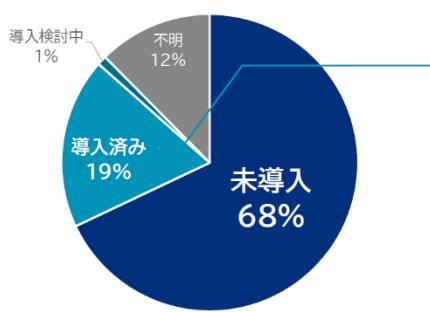
本調査では、サプライチェーン攻撃の脅威が高まる中、約7割の企業がEDR（事後対策）を導入していないことが明らかになりました。さらに、導入を検討している企業もわずか1%にとどまっており、政策として求められる水準と、現場の実態との間に大きなギャップが存在することが浮き彫りとなりました。

### EDRの導入状況

EDR(Endpoint Detection and Response)未導入企業は約70%に上り、高度なセキュリティ対策への理解は未だ不十分な状況が分かります。さらに、導入を検討している企業もわずか1%にとどまっており、政策として求められる水準と、現場の実態との間に大きなギャップが存在することが浮き彫りとなりました。しかし、「導入済」と回答した19%の企業に利用しているEDRサービスを伺ったところ、**「従来のアンチウイルスソフトにEDRオプションを追加するのではなく、新興のEDRサービスに切り替えていく」**ことが見受けられました。つまり、EDRを導入した企業においては、既存のエンドポイントセキュリティの在り方から見直しを行った背景が予想されます。今後はサイバー攻撃の増加に伴い、再発防止策の一手としてEDRの導入率は上昇していくと予想されます。

Q EDRの導入状況を教えてください。

有効回答数:587



#### 利用しているEDRサービスTOP5

1位	CrowdStrike
2位	Cybereason
3位	らくらくEDR
4位	Microsoft Defender
4位	SentinelOne

© 2026 USEN ICT Solutions CORPORATION

5

また、既存のセキュリティ機器の運用状況についても、約半数の企業がファームウェアの更新状況を「把握していない」または「更新していない」と回答しました。対策を導入していても、その後の運用・管理が十分に行われていないケースが少なくないことがうかがえます。

### ゲートウェイセキュリティ機器のファームウェアについて

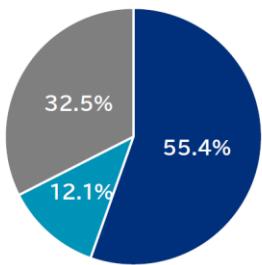
ゲートウェイセキュリティ機器のファームウェアのアップデートは、セキュリティを維持し、機器を安全に使い続けるために欠かせない作業です。本番環境に適用する前にパッチテストを要する場合はなかなか難しいですが、ファームウェアを常に最新の状態に保つため、自動更新機能を有効にするのが好ましいでしょう。しかし、Q1の設問に対しては、半数近くの企業が「いいえ(最新にアップデートしていない)・わからない」と回答しており、対策を導入していても、その後の運用・管理が十分に行われていないケースが少なくないことがうかがえます。こうした状況では、自社が被害を受けるリスクにとどまらず、攻撃の踏み台となり、結果的に取引先を含むサプライチェーン全体に影響を及ぼす可能性も否定できません。セキュリティ対策は「導入して終わり」ではなく、継続的な運用が不可欠であることが、改めて示された形です。また、Q2の方では「どのようにアップデートしているかわからない」の回答が最も多いことから、もしかするとQ1で「はい(最新にアップデートしている)」と回答している企業のなかにも、**ベンダーにまかせっきりで契約内容が確認できていない企業などが多い可能性**もある結果となっています。

Q1 ゲートウェイセキュリティ機器のファームウェアは最新にアップデートされていますか。

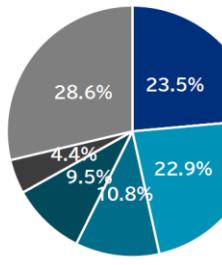
有効回答数:157

Q2 ゲートウェイセキュリティ機器のファームウェアのアップデートはどのように対応されていますか。

有効回答数:157



- はい
- いいえ
- わからない



- 自社でアップデート情報を把握して自社で作業を行っている
- 専門業者が自動的にアップデートしてくれている
- 専門業者からアップデートの連絡が来て、都度、設定変更費用を支払って依頼している
- 専門業者からアップデートの連絡があり、都度、無料で対応してくれている
- 導入してから変更していない
- わからない

© 2026 USEN ICT Solutions CORPORATION

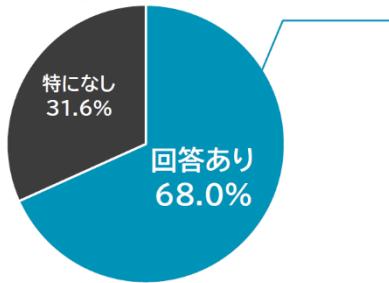
7

こうした状況では、自社が被害を受けるリスクにとどまらず、攻撃の踏み台となり、結果的に取引先を含むサプライチェーン全体に影響を及ぼす可能性も否定できません。セキュリティ対策は「導入して終わり」ではなく、継続的な運用が不可欠であることが、改めて示された形です。

一方で、SCS 評価制度という国の取り組みに対して、現場の担当者の関心自体は高いことも本調査から確認されました。その反面、具体的に何から着手すべきか分からず、優先順位を付けられないといった声も多く、制度対応に向けた実務面でのハーフドルが存在していることが推察されます。

「今後気になる・対策が必要だと感じていること

1位の「特定の脅威や攻撃・最新技術への対策」からは、回答者がどのような攻撃手法がトレンドになっているのかへの興味が高いことがうかがえます。2位については**61件中54件が2026年度末スタート予定のSCS評価制度に関する回答**であり、経済産業省が掲げる同施策についてはとても関心が高いことが分かります。また、6位の「全般的な懸念」には、「具体的に聞きたい」「何を聞けばよいのか分からない」「何から始めたらよいのか分からない」など漠然とした不安の声があり、そういった層でさえ「回答あり」約7割に含まれているということは、「特になし」と回答があった約3割の企業は、セキュリティ対策関連において現状全く気にかけていない層になるのではないかでしょうか。



Q セキュリティ関連で今後気になる・対策が必要だと感じていることは何ですか。

回答数:n=605(全体)／回答あり:n=414／特になし:n=191(複数回答)

1 特定の脅威や攻撃・最新技術への対策	67
2 セキュリティ対策評価制度・ガイドライン対応・コンプライアンス	61
3 ネットワーク・境界防御について	58
4 エンドポイントセキュリティについて	52
5 人的ミスへの対応・リソース不足・研修・従業員教育について	41
6 全般的な懸念	39
7 コスト・費用対効果・予算	23
8 現状把握・今後の方針について	17
9 クラウドセキュリティ・データ保護	16
10 デバイス管理・モバイル端末のセキュリティ	12
11 脆弱性管理・診断・ログ監視	11
12 インシデント事例について	9
- その他	21

© 2026 USEN ICT Solutions CORPORATION

8

SCS 評価制度の本格運用まで一定の準備期間が残されている今、まずは自社の対策状況を正しく把握し、どこに課題があるのかを可視化することが、次の一手を検討する上で重要であると言えます。

## ■調査概要

対象期間：2024年11月1日～2025年10月31日

対象者：全国1,932名の情報システム担当者

方法：当社インサイドセールス統括部による電話でのヒアリング・郵送ダイレクトメールによるアンケート回答

調査レポートは、以下のダウンロードフォームよりお申し込みいただくとご確認いただけます。

「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スタート直前！情シス1,932名に聞いたセキュリティ対策の実態調査レポート」

URL：<https://www.gate02.ne.jp/document/fact-finding-survey-of-security-measures>

## ■ 主なヒアリング項目

- ・利用しているマルウェア対策ソフト
- ・EDR の導入状況
- ・利用しているUTM
- ・ゲートウェイセキュリティ機器のファームウェアについて
- ・セキュリティ関連で気になる・対策が必要だと感じていること
- ・今後導入したいセキュリティ対策
- ・セキュリティの専門家に無料で相談できるとしたら聞きたいこと
- ・情報セキュリティ調査票の提出を求められたことがあるか

\* 本調査は、当社が実施した延べ1,932社へのヒアリング・アンケート内容をもとに、設問・テーマごとに回答を整理・分析したものです。  
そのため、設問ごとに回答数は異なります。

## ■サイバーセキュリティラボ 運営責任者コメント

株式会社 USEN ICT Solutions 取締役執行役員 長幡 開介

サプライチェーン攻撃の脅威が高まるなか、多くの企業が対策の必要性を感じつつも、コストや人材不足により『最適な解』を見つけられずにいます。弊社では 2025 年 1 月に「サイバーセキュリティラボ」という情報発信機関を立ち上げ、日本の中小企業に向けて、サイバーセキュリティに関するさまざまな情報を届けてしましました。

今回は、1,900 名を超える担当者の生の声を集めたことで、日本のセキュリティ対策の“平均値”と“課題”が明確になりました。本レポートが、自社のセキュリティレベルを客観視し、次なる一手をご検討いただく際の一助となれば幸いです。

## ■参考資料

本調査レポートの背景となる SCS 評価制度については、以下のホワイトペーパーでも解説しています。

「SCS 評価制度（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） 解説します - 2026 年更新版 -」

URL : <https://www.gate02.ne.jp/document/cybersecurity-measures-evaluation-overview>

## ■「サイバーセキュリティラボ」とは

インシデントニュース発信や有益なセキュリティ記事、セミナー、無料相談窓口や無料でできるアカウント流出チェックなど、中小企業のセキュリティをアップデートするためのコンテンツが豊富です。

国・外郭団体・民間・専門家などのサイバーセキュリティに関する情報をまとめて発信する機関です。身近な情報セキュリティ事故に関する被害事例の掲載や専門家によるセミナー・座談会の開催などを通して、被害の減少に役立つ情報を中堅・中小企業向けに分かりやすく発信してまいります。

「サイバーセキュリティラボ」 : <https://gate02.ne.jp/lab>

## ■会社概要

会社名 : 株式会社 USEN ICT Solutions

所在地 : 東京都品川区上大崎三丁目 1 番 1 号 目黒セントラルスクエア

代表者 : 代表取締役社長 高橋 領一

設立 : 2017 年 6 月 16 日

事業内容 : 電気通信事業法に基づく電気通信事業（届出番号/A-29-16072）、ICT サービス等に関わる事業

URL : <https://usen-ict.co.jp>

法人向け ICT ソリューション「USEN GATE 02」 : <https://www.gate02.ne.jp>

サイバーセキュリティラボ : <https://www.gate02.ne.jp/lab>

### 【報道関係者からのお問い合わせ先】

株式会社 U-NEXT HOLDINGS 広報部

TEL : 03-6823-2010 E-MAIL : [unhdpr@unext-hd.jp](mailto:unhdpr@unext-hd.jp)

お問い合わせフォーム : [こちら](#)

### 【本調査レポートに関するお問い合わせ先】

株式会社 USEN ICT Solutions

お問い合わせフォーム : [こちら](#)