



サプライチェーンセキュリティ 2026年度版 セキュリティ対策と課題

2026年10月16日
インフォテック株式会社

本資料は、2026年7月時点での情報をもとに作成しております。

Copyright © 2026 Infotec Inc.

目次

• はじめに(背景)		3
• サイバー攻撃の標的は？		4
• なぜ今、サプライチェーンセキュリティなのか		5
• セキュリティ対策が不十分な場合の可能性について		8
• 委託先企業が直面する“5つの困りごと”		10
• 対策を進めるための取り組むべき 3ステップ		11
• まとめ		12
• 参考文献		13

はじめに(背景)

近年、取引先に影響を与えるようなサイバー攻撃事案が頻発しており、サプライチェーン全体でのサイバーセキュリティ対策の強化が求められています。

※1

No.	発生時期	事例	内容
1	2026年 7月	【食品・流通】ニチレイ (不正アクセスによるシステム障害)	ニチレイグループはサイバー攻撃を受け、出荷業務に関わるシステムで障害が発生しました。今回の事例は、大規模物流企業のシステム障害がサプライチェーン全体に影響を及ぼすリスクを示しています。取引先を含めたリスク管理やBCP(事業継続計画)の重要性が改めて浮き彫りとなりました。
2	2025年 10月	【EC・流通】アスクル (物流停止に波及した大規模被害)	業務委託先のPCから管理者アカウント情報が漏えいし、不正利用された事例です。多要素認証が未設定だったため容易に侵入を許し、ネットワーク内を移動して権限を拡大し被害が出ました。
3	2025年 9月	【製造(飲料)】アサヒグループHD (工場稼働停止と物流寸断)	製造と物流が密接に連携するサプライチェーン(供給網)の弱点が突かれた事例です。製造ラインだけでなく、受発注や物流システムが停止することで事業全体が麻痺するリスクが浮き彫りになりました。

※1 ニチレイ 不正アクセスによるシステム障害 <https://www.nichirei.co.jp/news/2026/512.html>
アスクル株式会社 ランサムウェア攻撃の影響調査結果および 安全性強化に向けた取り組みのご報告 <https://pdf.irpocket.com/C0032/PDLX/O3bg/N4O3.pdf>
アサヒグループホールディングス サイバー攻撃によるシステム障害発生について <https://www.asahigroup-holdings.com/newsroom/detail/20250929-0102.html>

サイバー攻撃の標的は？

攻撃者の標的は、“発注元”から“委託先”へ変化しています。

下の表にある**サプライチェーンや委託先を狙った攻撃**とは、大手企業を直接狙うのではなく、委託先企業を踏み台にして取引先へ侵入する攻撃を指し、近年被害が急増しています。

情報セキュリティ10大脅威(2026) 10大脅威のうち上位5項目を抜粋

※1

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い (2016年以降)
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目

※1 IPA 情報セキュリティ10大脅威 2026より抜粋 <https://www.ipa.go.jp/security/10threats/10threats2026.html>

なぜ今、サプライチェーンセキュリティなのか

なぜ攻撃者は、直接大手企業にサイバー攻撃を実施せず、委託先企業などグループ企業へ攻撃をするようになったのでしょうか。それは、「**本命の大手企業は守りが固いため、比較的守りが弱い委託先やグループ企業を踏み台にして侵入する方が成功しやすい**」(※1)からです。

以下のようにまとめることができます。

- 攻撃者はサプライチェーンでいう「最も侵入しやすい場所」を狙います。

大手企業は多額の予算をかけて、EDR、SOC、ゼロトラスト、MFA(多要素認証)などの対策を導入しています。一方で、中小規模の委託先企業は人員や予算が限られ、同レベルの対策を実施できない場合があります。

- 被害は侵入された企業だけではなく、サプライチェーン全体に及ぶ可能性があります。

被害は侵入された企業だけにとどまらず、接続先への侵入、情報漏えい、サービス停止などを通じて、委託元、取引先、サービス利用企業へ波及する可能性があります。

- 委託元は、サプライチェーン全体のセキュリティ水準を把握し、委託先を選定しようとしています。

委託元では、委託先の選定および契約期間中に、セキュリティ体制、アクセス管理、インシデント対応、再委託先管理などの確認・評価を行うことを重要視しています。

※1 IPA指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策1, <https://www.ipa.go.jp/security/economics/practices/navi/practice236.html>

なぜ今、サプライチェーンセキュリティなのか

攻撃手法の変化により取引先企業が、サプライチェーン全体のリスクを管理するようになった結果、現在はこのような要求が増加しています。

- **ISMS/Pマーク認証の取得**

情報漏えいや不正アクセスなどのリスク低減に向けた管理体制が整備されているか確認するため、ISMS(情報セキュリティマネジメントシステム)認証やプライバシーマーク(Pマーク)が活用されています。

- **SBOM(ソフトウェア部品表)の提出・共有**

昨今、ソフトウェアの脆弱性やライセンス上のリスクを管理するため、SBOM(Software Bill of Materials)の提出・共有を取引先や委託先に求める動きが広がっています。特に、海外の政府調達や医療機器分野などで先行しており、国内でも官公庁、重要インフラ、自動車・組込み機器など、セキュリティ要求の高い分野を中心に導入・検討が進んでいます。

- **開発環境/委託先管理状況の開示**

開発工程やサプライチェーンにおける情報漏えい、不正アクセスなどのリスクを把握し、適切なセキュリティ管理が実施されているかを確認するため、開発環境のセキュリティ対策や管理体制の開示を求められます。



なぜ今、サプライチェーンセキュリティなのか

前述したようにセキュリティに対し、あらゆる要求が増えたことで、実際に委託先企業では以下のような対応が求められます。

- 取引先からセキュリティチェックシートへの回答を定期的に求められる
- 委託先管理の一環として、体制や対策状況の説明を年度ごとに求められる
- 事故発生時に、取引先への説明責任や再発防止策の策定、初動対応マニュアル整備が発生する



セキュリティ対策が不十分な場合の可能性について

サプライチェーンセキュリティ対策が不十分な場合、以下のよう
な影響が考えられます。

① 取引機会への影響(可能性)

- ・セキュリティ要件に十分応えられない場合、是正対応が求められる。

また、取引先からの評価に影響を与え、今後の案件への参画機会や新規案件の選定に影響する可能性もある。

② インシデント発生時の負担

- ・万一の漏えい・侵害時には、調査費用・通知対応・賠償の話し合いなどが発生しうる。

- ・顧客対応や原因究明に、想定以上の時間とコストがかかる傾向にある。



セキュリティ対策が不十分な場合の可能性について

③ 公的制度での評価

・国や業界では、企業のセキュリティ対策状況を評価・見える化する取り組みが進んでいるため、将来的には、その評価結果が取引先選定や委託先評価の参考情報として活用される可能性がある。

④ 社内の負荷

・取引先からの問い合わせ・監査対応が、都度の手作業になりがち。
・IT担当者の負担増(チェックシート対応等が負担になる)となるため、本業への影響が出る。
・専任担当がないことで、インシデント発生時の初動対応に不安が残る。
・マルウェア対策(EDRなど)やネットワーク対策(UTMなど)を導入しても、自力では運用しきれない。

これらによって「すぐに何かが起きる」わけではありませんが、取引先からの要求が厳しくなりつつある昨今において、準備の有無で差が出てくる可能性があります。



委託先企業が直面する”5つの困りごと”

サプライチェーンセキュリティの重要性は理解できて、実際には何から始めればよいかわからない企業も少なくありません。

【経営層の声】

- ①「何から手を付ければいいのか、正直わからない」
- ②「コストとリスク、どこまでかければ十分なのか判断軸がない」

【IT担当者の声】

- ③「本業の開発・運用で手一杯。セキュリティに割く時間がない」
- ④「設定変更やトラブル対応、自分の判断で進めて大丈夫か不安」

【共通の声】

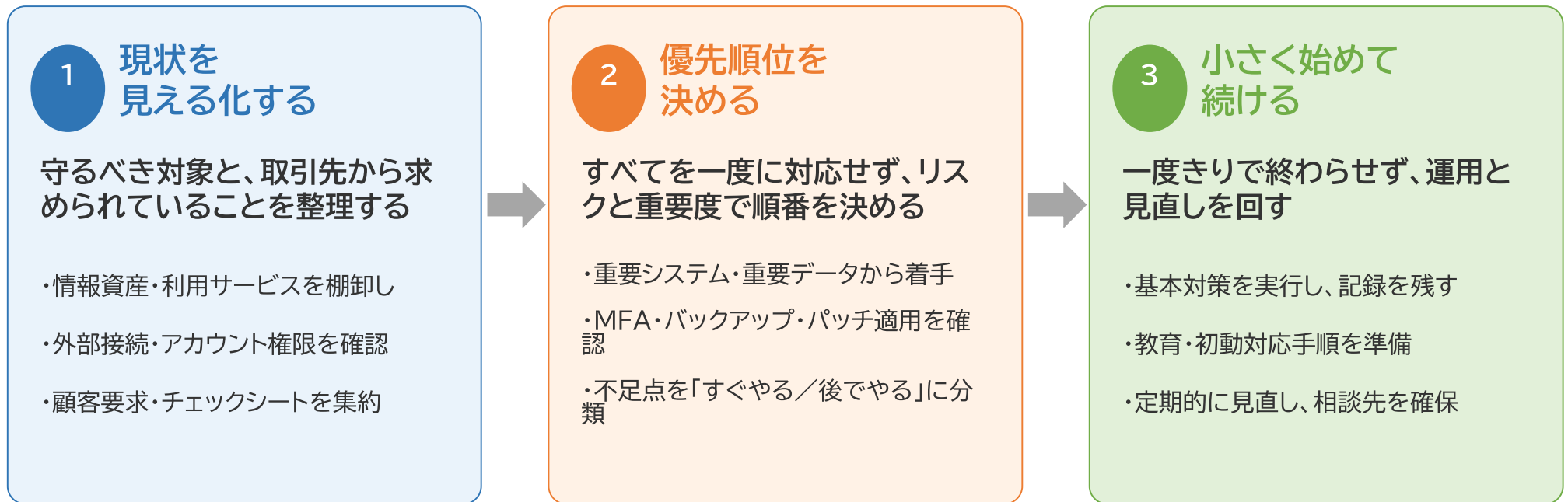
- ⑤「顧客からセキュリティチェックシートが届いても、どう答えればよいかわからない」



対策を進めるための取り組むべき 3ステップ

これまでの課題について、まずは「現状を知る」ことから始めるのが重要です。

まずは「自社の状況を説明できる資料」と「最低限の基本対策」を整えることから始めましょう。



まとめ

本資料のポイントは以下のとおりです。

攻撃トレンドの変化

攻撃は巧妙化し継続的となり、企業単独対策の限界が明確になっています。

サプライチェーンの経営課題化

サプライチェーンセキュリティは全ての企業にとって重要な経営課題となっています。

連携と可視化の重要性

サプライチェーン全体での連携と可視化が不可欠で、効果的な対策が望めます。

リスク認識と行動促進

自社のリスクを再確認し、現実的なセキュリティ対策の一步を踏み出しましょう。



セキュリティは後付けでは守れない

セキュリティ対策は、システム開発の設計段階から対策することが重要です。
 インフォテックが提供するセキュリティソリューションは
Security By Design x DevSecOpsをベースに構築、確かな安心をお届けします。

Security By Design

システム設計段階からセキュリティを組み込んで開発を行います

CIS Benchmarks® (*1)やCIS Controls® (*2)を活用し、設計・開発・保守におけるセキュリティの標準化と継続的な評価改善を可能とします

DevSecOps

保守フェーズではDevSecOpsに基づき、PDCAサイクルにWebアプリケーション脆弱性診断(*3)やクラウド／SaaSのセキュリティ態勢管理(CSPM(*4)・SSPM(*5))を組み込むことで、運用の継続的な改善をご支援します

お問い合わせ・資料請求はこちらから

インフォテック株式会社HP お問い合わせ窓口

<https://www.iftc.co.jp/contact/form/?kind=2>

お電話でのお問い合わせ

03-3348-0360 ※【受付時間】土日祝日を除く平日の9:00～17:30

- (*1) OSやクラウドなどのITシステムに対する安全な設定方法をまとめたガイドラインで、セキュリティ強化や監査対応に活用
- (*2) サイバー攻撃から組織を守るための18の優先度付きセキュリティ対策で、実践的かつ段階的な導入が可能なベストプラクティス集
- (*3) スリーシェイク社の「Securify」を用いた自動診断
- (*4) クラウド環境の設定ミスや脆弱性を検出・修正し、セキュリティとコンプライアンスを維持する管理ツール
- (*5) SaaSアプリのセキュリティ設定を監視・管理し、データ漏洩や権限の過剰付与などのリスクを防ぐための管理ツール

「CIS®」、「CIS Benchmarks®」、「CIS Controls®」、「CIS SecureSuite®」、「CIS-CAT®」は、Center for Internet Security, Inc.(CIS)の米国およびその他の国における登録商標です。本記事は、CISの商標またはサービスに関する公式な提携、認定、スポンサーシップを示すものではありません。