サプライチェーン セキュリティ教育資料

情報処理推進機構
産業サイバーセキュリティセンター5期
「初めてのセキュリティ塾」プロジェクト

本書の目的と対象読者

サプライチェーンリスクについて理解する

目的：　委託元としてサプライチェーンリスクを
考慮した契約の重要性を学ぶ

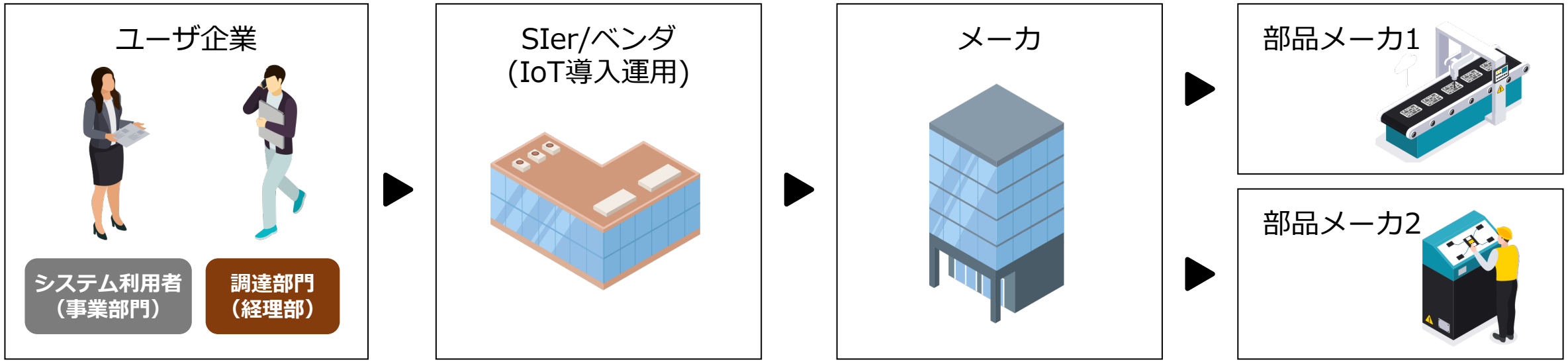
対象読者　：委託元として契約業務に関わる方

第1章　サプライチェーンとは

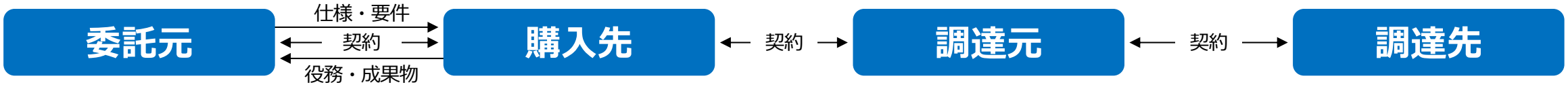
1.1 サプライチェーンとは

業務の外部委託や物品の調達等におけるライフサイクル全般のこと

多くの企業では、ビジネスパートナーや委託先も含めたサプライチェーンを持っており、さまざまな企業と連携して業務を行っています。
企業で行われている業務の全てが自社内で完結する訳ではありません。



契約におけるサプライチェーン

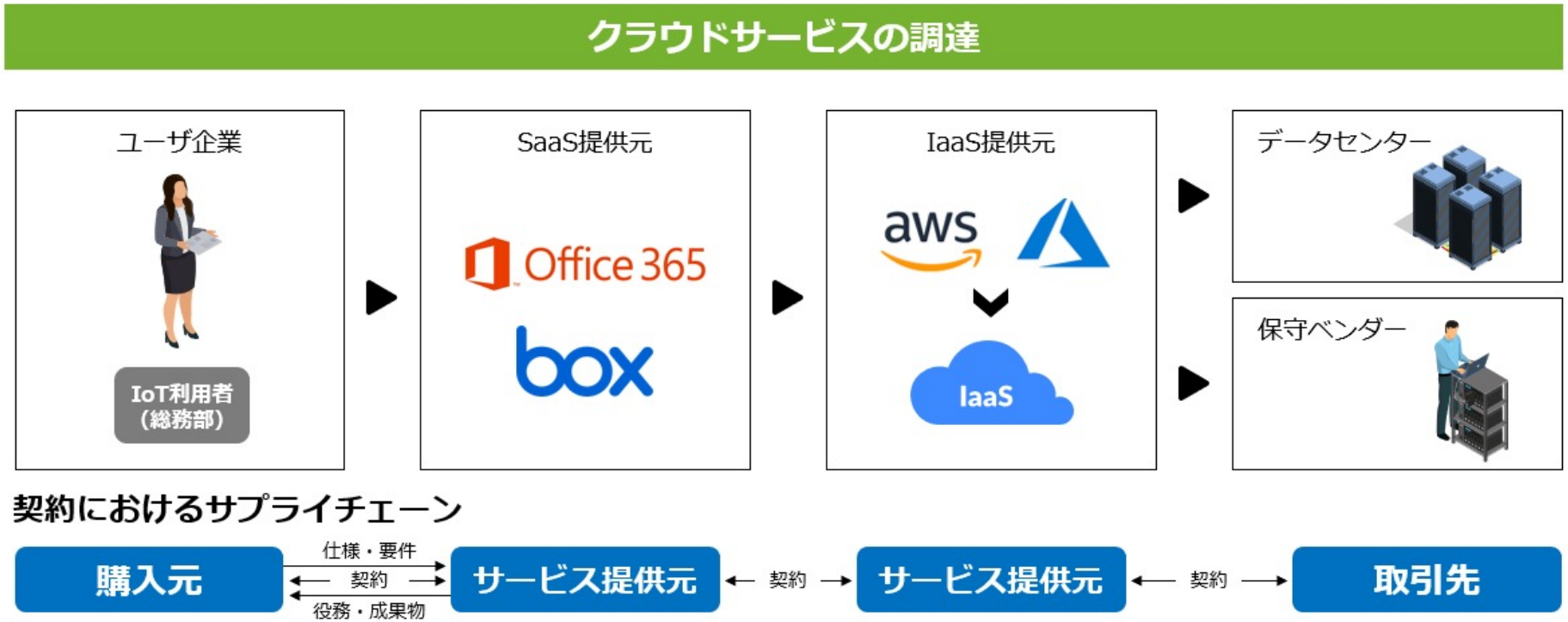


【参考jURL】https://www.ipa.go.jp/files/000066773.pdf

1.2 様々なサプライチェーン

物の調達以外にもサービスの利用や人の調達など様々なサプライチェーンがある

近年、クラウドサービスの利用事例も多くみられますが、その裏側では様々なビジネスパートナーとの連携や外部委託が行われており、サプライチェーンを構成していると言えます。事業を取り巻く環境には様々なサプライチェーンが存在することを理解する必要があります。



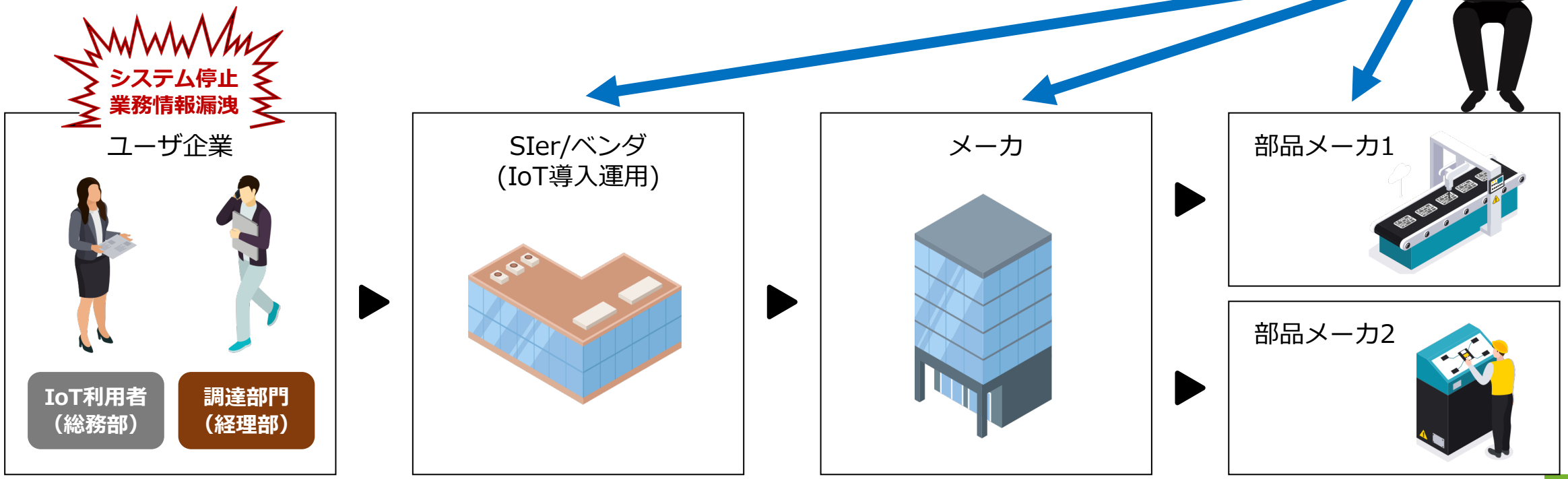
第2章　サプライチェーンリスク

2.1 サプライチェーンにおけるサイバーセキュリティリスクとは

調達ベンダーや、委託先などを狙ったサイバー攻撃によって引き起こされる業務停止や情報漏洩のリスク

委託先がサイバー攻撃を受けると、調達/システム構築プロセスの遅延や委託元の業務情報を漏洩が発生し得ます。こうしたリスクを**サプライチェーンにおけるサイバーセキュリティリスク**と言います

IoT機器を活用したシステム導入運用の場合



2.2 サプライチェーンリスクにおける国内・海外動向

国内外でサプライチェーンリスクについてガイドラインなどに記載されており、重要視されている。

① 国内動向

- 経済産業省：サイバーセキュリティ経営ガイドラインで重要項目になっています
- IPA (情報処理推進機構) ：情報セキュリティ10大脅威第３位になっています

② 世界動向

- 米国：「重要製品のサプライチェーン」に関する大統領令が発行されており、また事業者は国防総省と取引する際には、サプライチェーンに関するガイドラインであるNIST SP 800-171(*)に準拠することが求められます。
- 欧州：サイバーセキュリティ認証フレームワーク(Cybersecurity Certification Framework)等でサプライチェーンにおけるセキュリティ対策が述べられています。

順位	組織
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報の窃取
3位	サプライチェーンの弱点を悪用した攻撃
4位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	ビジネスメール詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

【参考URL】https://www.ipa.go.jp/security/vuln/10threats2022.html

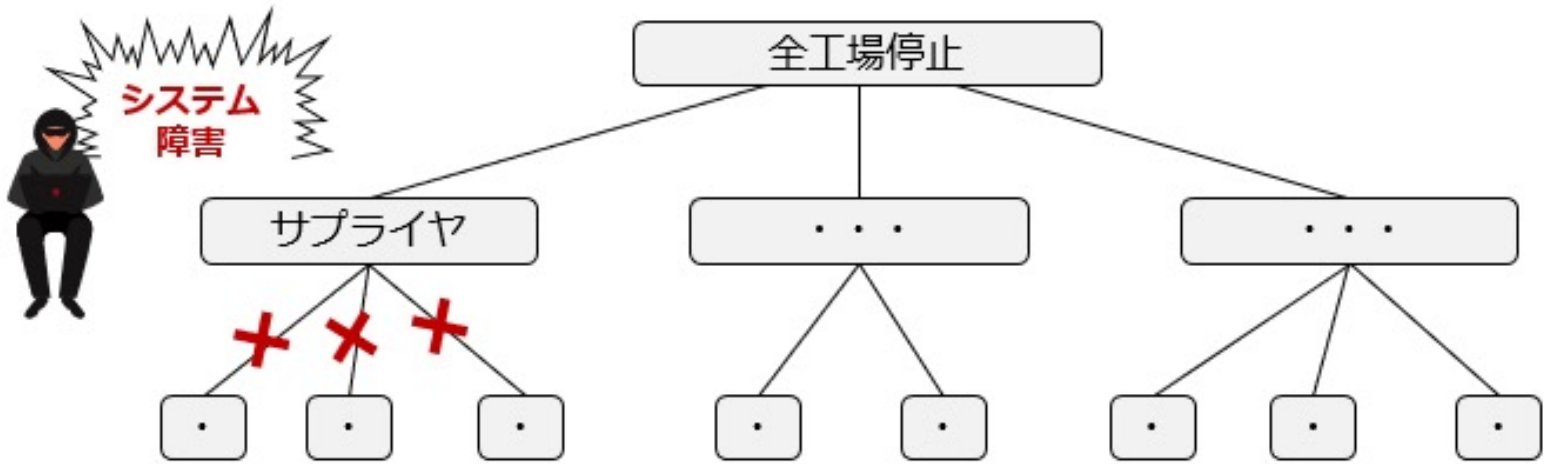
＊米国国立標準技術研究所（NIST）によるセキュリティ基準を示すガイドライン

2.3 事例①

サプライヤがサイバー攻撃を受け、メーカの工場が全停止した

2022年3月、大手自動車工場の取引先部品メーカであるサプライヤがサイバー攻撃を受けました。その結果、部品の供給が止まり、大手自動車工場では、国内すべての工場が停止せざるを得なくなりました。

さらに、グループ子会社の自動車メーカも複数の工場において製造を停止しなければならなくなりました。工場の停止により自動車メーカは甚大な損害を被ったと言われています。



2.4 事例②

ソフトウェア開発会社がサイバー攻撃を受け、不正なプログラムをアップデートファイルに混入され感染被害が拡大した

2020年に米国大手ITベンダが提供するネットワーク監視ソフトウェアに不正なプログラムが含まれていることが判明しました。不正なプログラムはソフトウェアアップデートを通じて拡散され、米政府機関含め約18,000組織が影響を受けたと報道されています。

感染被害拡大の要因

正規の供給元によるアップデートファイル配布のため

ユーザ側での対策は非常に困難であった

➡ **攻撃者はサプライチェーンを利用することで、広範囲に影響を与える効果的な攻撃ができる**
このリスクを認識することが重要

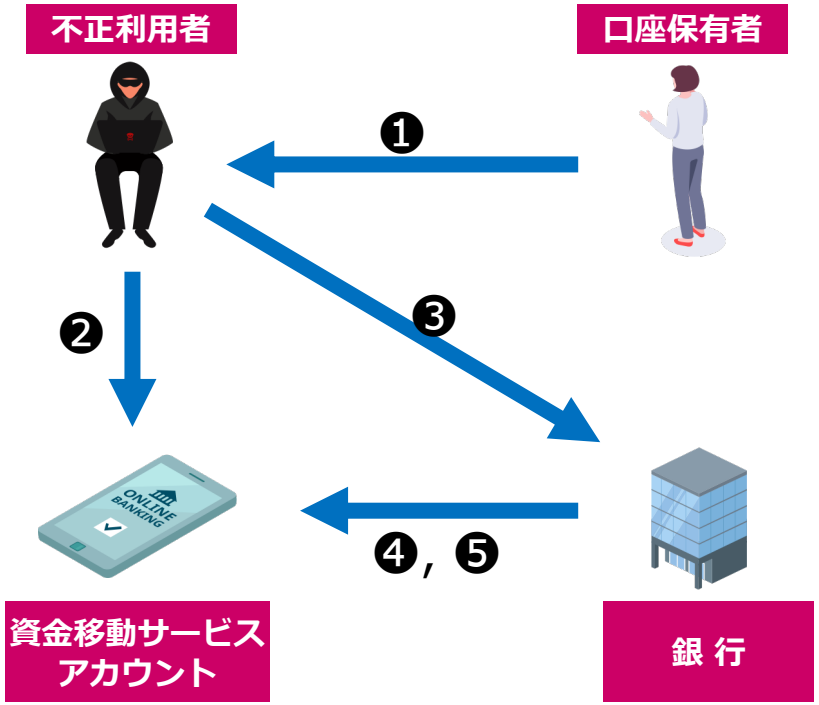
2.5 事例③

資金移動業者の提供する決済サービスを悪用した不正出金

2020年に資金移動事業を営んでいる大手携帯会社において、
不正な資金の引き出しが行われる被害がありました。これは、

1. 悪意のある第三者が預金口座情報を不正に入手
2. 当該預金者の名義で資金移動サービスのアカウントを開設
3. 銀行口座と資金移動サービスのAPIを連携
4. 銀行口座から資金移動サービスのアカウントへ残高をチャージ
5. 不正な引き出しを行う

という流れで被害が発生しました。

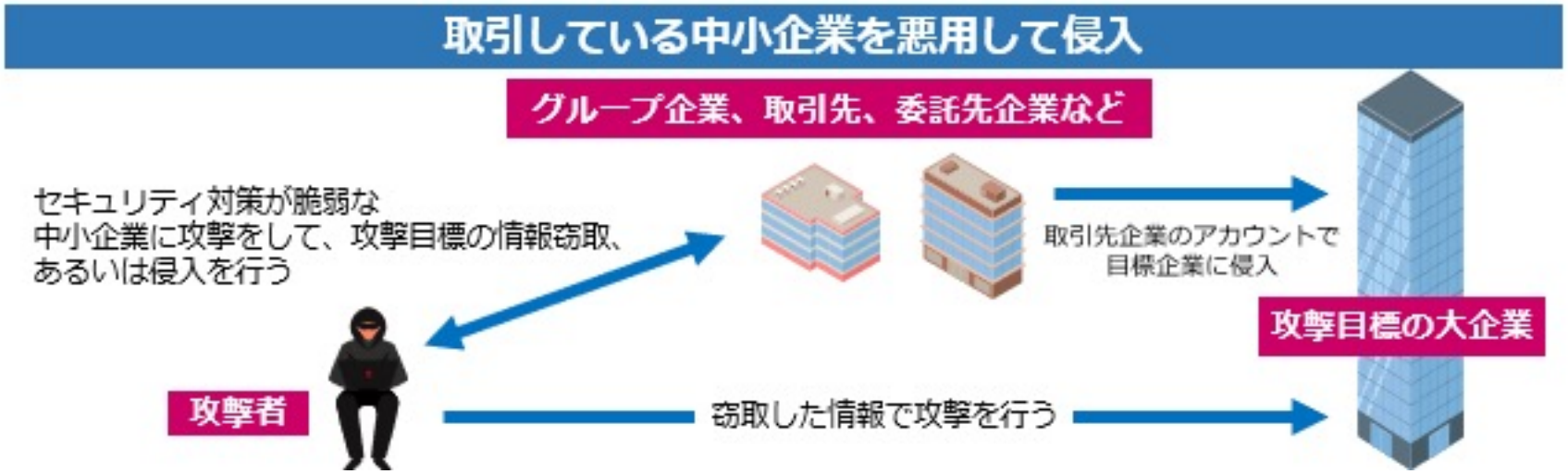


複数の企業にまたがるセキュリティインシデントであったため、
金融機関と資金移動事業者（携帯会社）で調査が難航して事態の収束に時間を要しました。
また、両者の責任範囲が不明確であったとも言われています。

攻撃者視点で考えると

攻撃目標の大企業を直接狙った攻撃だけでなく、
グループ会社を含むサプライチェーンを攻撃の起点として狙う

- 比較的セキュリティ対策が強固な企業に対してサイバー攻撃を行い、その企業に侵入することは困難です
- 大企業のサプライチェーンを構成するグループ企業や委託先企業は国内外問わず存在し、対策や管理の徹底は難しく、それら中小企業はセキュリティ対策にかけられる予算が大企業ほど潤沢ではありません
- そこで、その標的企業のサプライチェーンに関わる他の企業を踏み台として攻撃し、そこを起点として標的企業への連鎖的な影響を狙います



第3章　気を付けるべきポイントと対策

事例から学ぶ組織課題①

求めるセキュリティ対策が曖昧な場合、委託元が期待するセキュリティ対策の水準を委託先が実質的に満たせていない

契約時に委託元が提示するセルフチェックの実施を要件としていても、
求めるセキュリティ対策が曖昧な場合、委託元側において期待される**セキュリティ対策の内容を理解し、その対策の水準を満たせていないこともあります**

委託元

**セキュリティ対策してますか？
セルフチェックお願いします～**

- インシデント発生時に対応するための体制を整備すること
- システムの可用性を高めるため冗長化構成を取ること
- 保存されているデータが暗号化し、定期的にバックアップを取得すること

委託先

セキュリティ担当者はいるし、
暗号化機能があるHDD２台
にバックアップを１年に一回
取っているし、たぶんよし！

対策してます！

お互いのセキュリティ対策の認識に差がある

事例から学ぶ組織課題②

契約時に責任範囲を明確にしていない

- 委託元と委託先でサイバー攻撃などのインシデントが発生した際の情報共有や体制を契約時に取り決めていない企業が多数存在します

- 責任範囲が曖昧な場合、インシデントが発生した際に迅速な対応がとれず、調査が難航し、さらなるトラブルに発展する場合があります

1.「新たな脅威が顕在化した際の対応」について責任範囲の明記がない割合は 8 割。　委託元

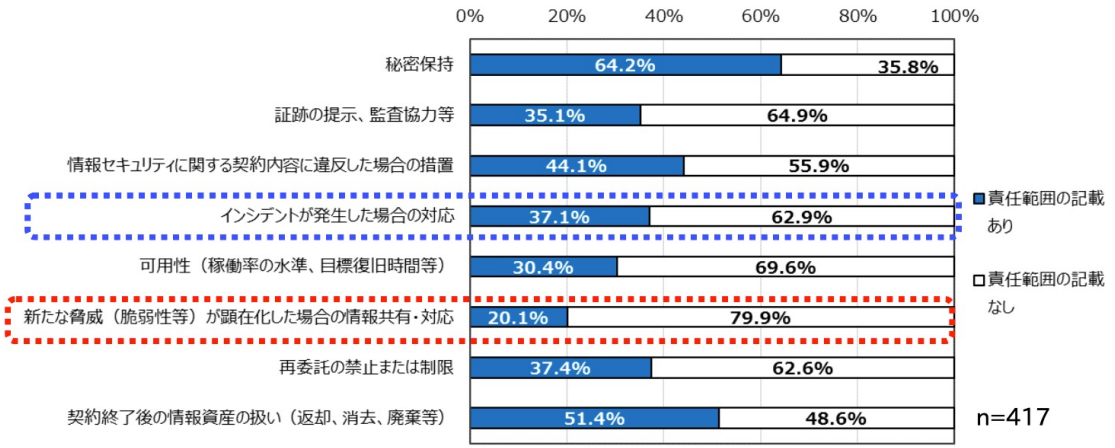


図 1：委託元が文書で明確にしているセキュリティに係る要求事項

引用：https://www.ipa.go.jp/files/000073416.pdf

対策

委託先に求めるセキュリティ対策と責任範囲を明確にする契約書雛形の見直しが有効

- 責任範囲を明確にするためには、まず組織の契約関連の文書の見直しが有効です
- 障害やサイバーインシデント被害を受けた際の責任範囲をあらかじめ契約書に明記しましょう
- 他にもガイドラインの整備や委託先とのリスクアセスメントの実施も有効です

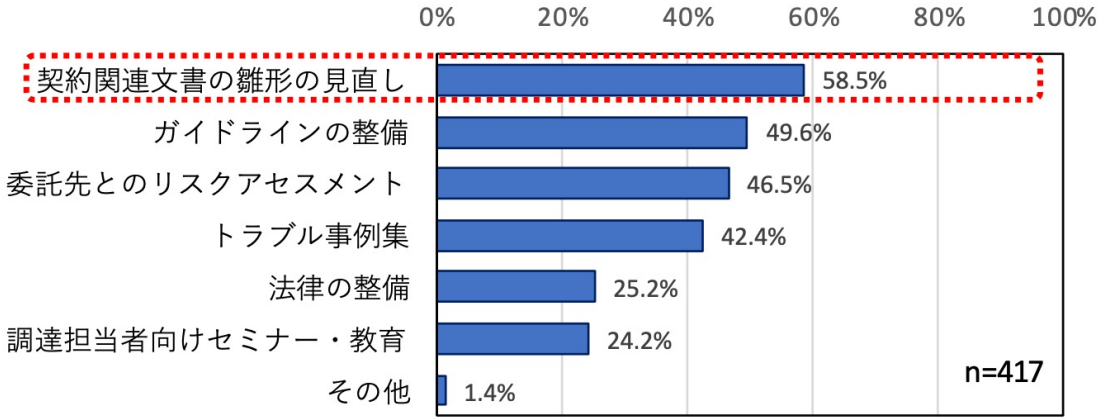


図５：責任範囲を明確にするために有効な施策（複数回答）

引用：https://www.ipa.go.jp/files/000073416.pdf

参考：情報システムに係る政府調達におけるセキュリティ要件策定マニュアル

内閣サイバーセキュリティセンターの指標を参考にする

内閣サイバーセキュリティセンターが公表している「情報システムに係る政府調達におけるセキュリティ要件策定マニュアルの対策要件集」には対策方針や仕様記載例、対策の提案例について記載されています。自社のセキュリティ担当や調達部門と相談のうえ契約書雛型を見直す際の参考にしてください。

対策方針	仕様記載例	対策の提案例
可用性確保	サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として【 】を超えることのない運 用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。	・装置及びネットワークの冗長化（ホットスタンバイ、コールドスタンバイ等） ・信頼性の高いハードウェア及びソフトウェアの採用等の基盤サービスの信頼性確保 ・オンライン又はオフラインバックアップ
機器等の調達における対策	機器等の製造工程において、府省庁が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。	・製造過程における情報セキュリティ管理体制や管理手順等が記載された書類の提出
主体認証	情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスす る主体のうち【 】の認証を行う機能として、【 】の方式を採用し、主体認証情報の推測や盗難 等のリスクの軽減を行う機能として、【 】の条件を満たすこと。	・ 耐タンパ性を備えたICカード認証生体認証（指紋、顔、静脈、虹彩等）２つ以上の主体認証方式を用いて認証を行う ・多要素主体認証方式情報システムの認証履歴の記録と通知 ・指定回数以上の認証失敗時のアクセス拒否

【参考URL】 https://www.nisc.go.jp/pdf/policy/general/SBD_manual_annex_a.pdf

記載例中の【 】は、仕様書記載時に具体化すべき箇所

まとめ

委託元・委託先の双方がサプライチェーンリスクを

正しく把握した上で責任と対策を明確化し、合意をすることが重要

- **委託元と委託先の双方で定める具体的なセキュリティ対策について合意し、契約する**

- **セキュリティ対策に関しての責任範囲を明確化したうえで、その内容について委託先と合意する**