経営者を含めた
サイバーセキュリティ強化の取組み

2023年3月17日
トヨタ自動車株式会社
古田 朋司

本日のご説明内容

1.会社概要

2.トヨタのセキュリティ取り組み体制

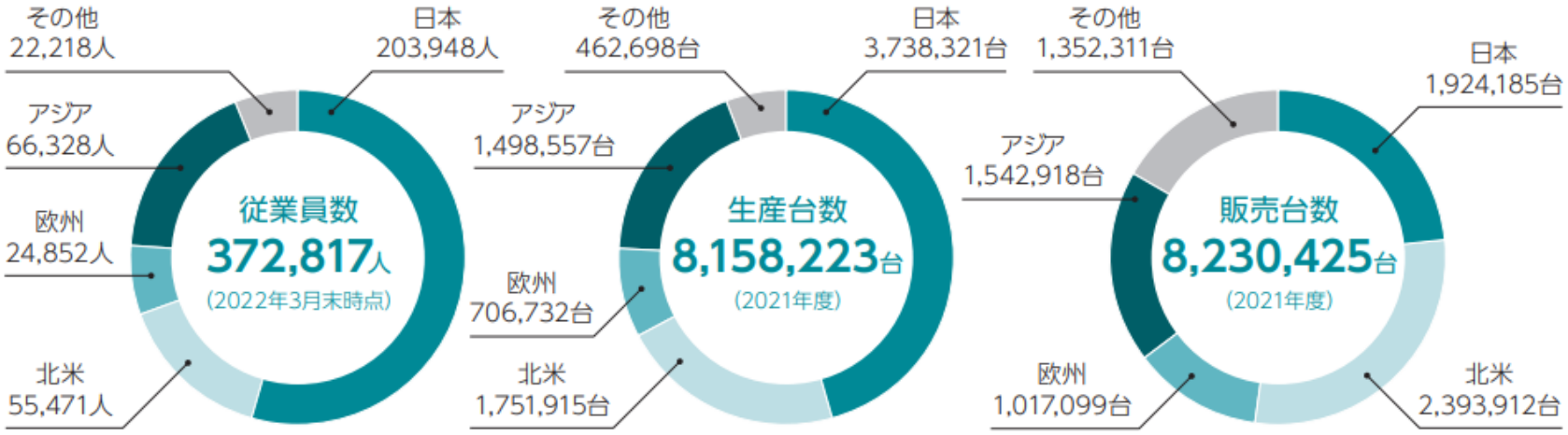
3.トヨタへのサイバー攻撃の状況、事例と対策

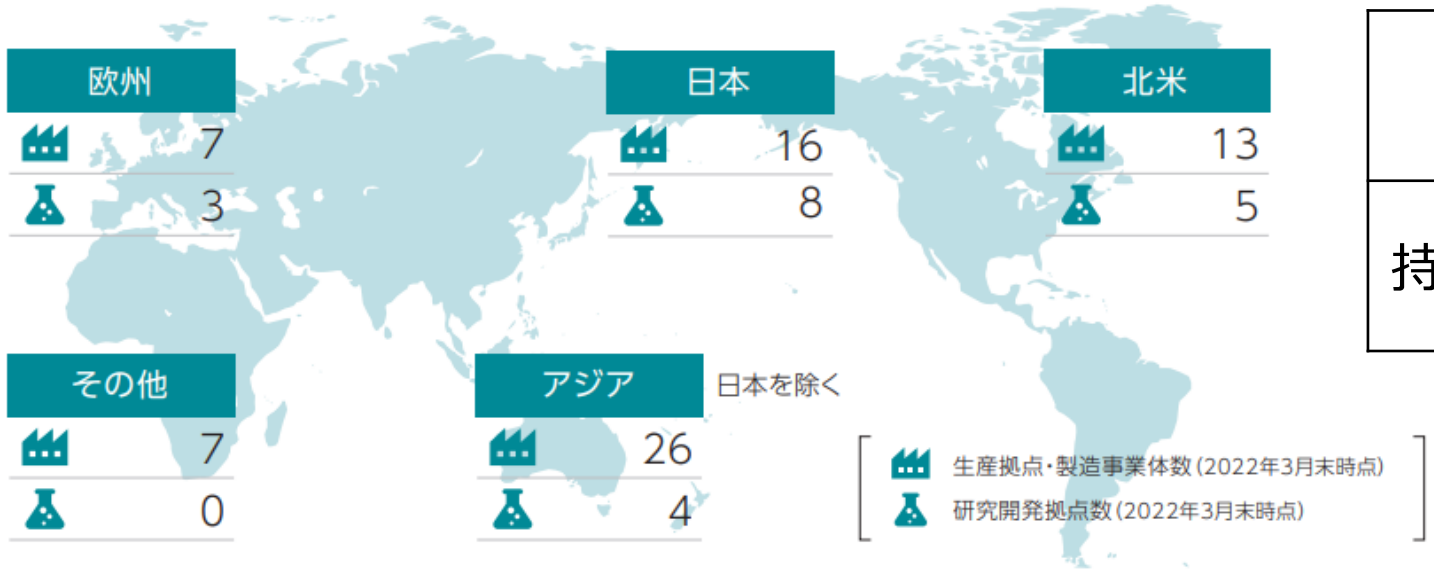
4.サプライチェーンのセキュリティ対策

トヨタに関連するインシデントを通じた学びと、苦労点をお伝えします
経営者の方々のお取り組みのご参考になれば幸いです

1．会社概要（事業展開）

グローバル展開・地域別データ

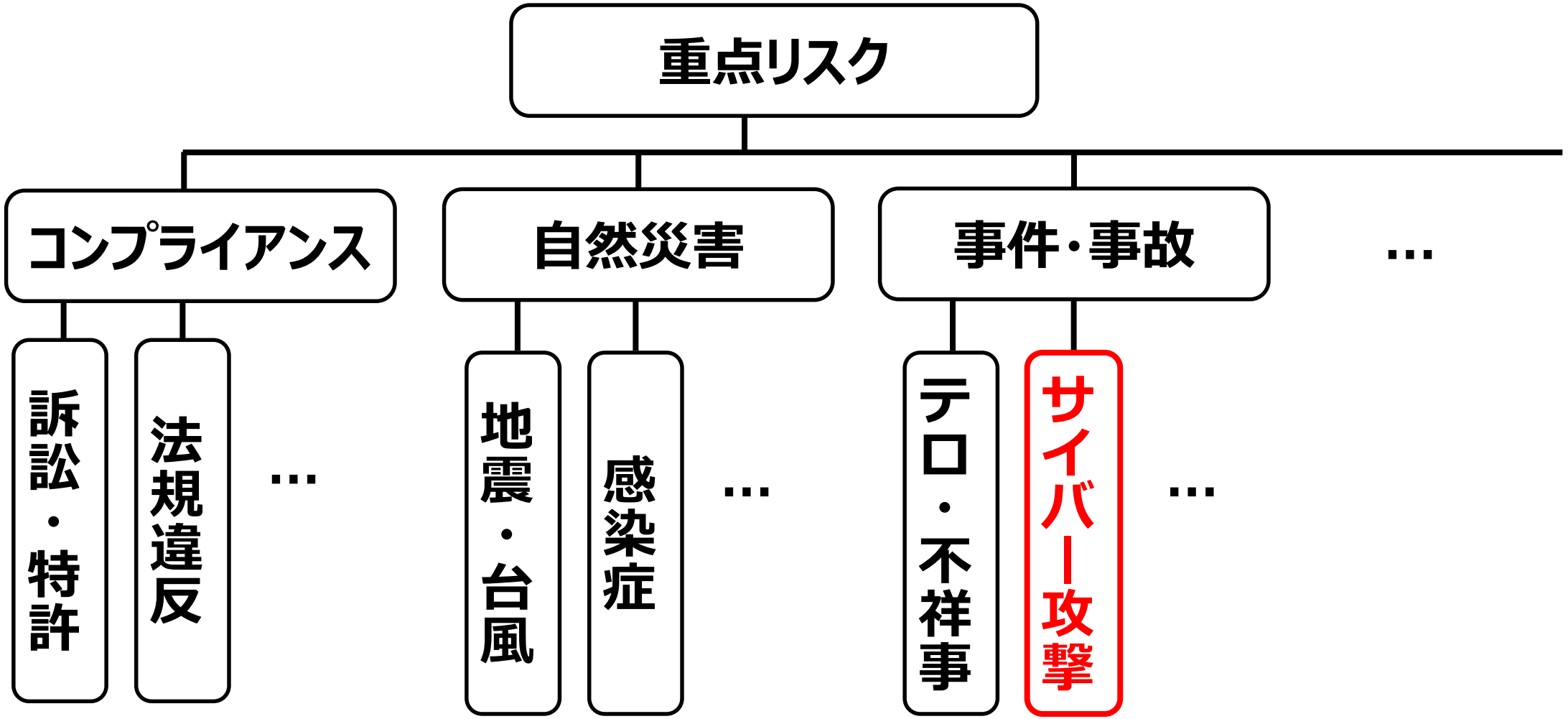




連結子会社数	**559** 社
持ち分法適用会社	**169** 社

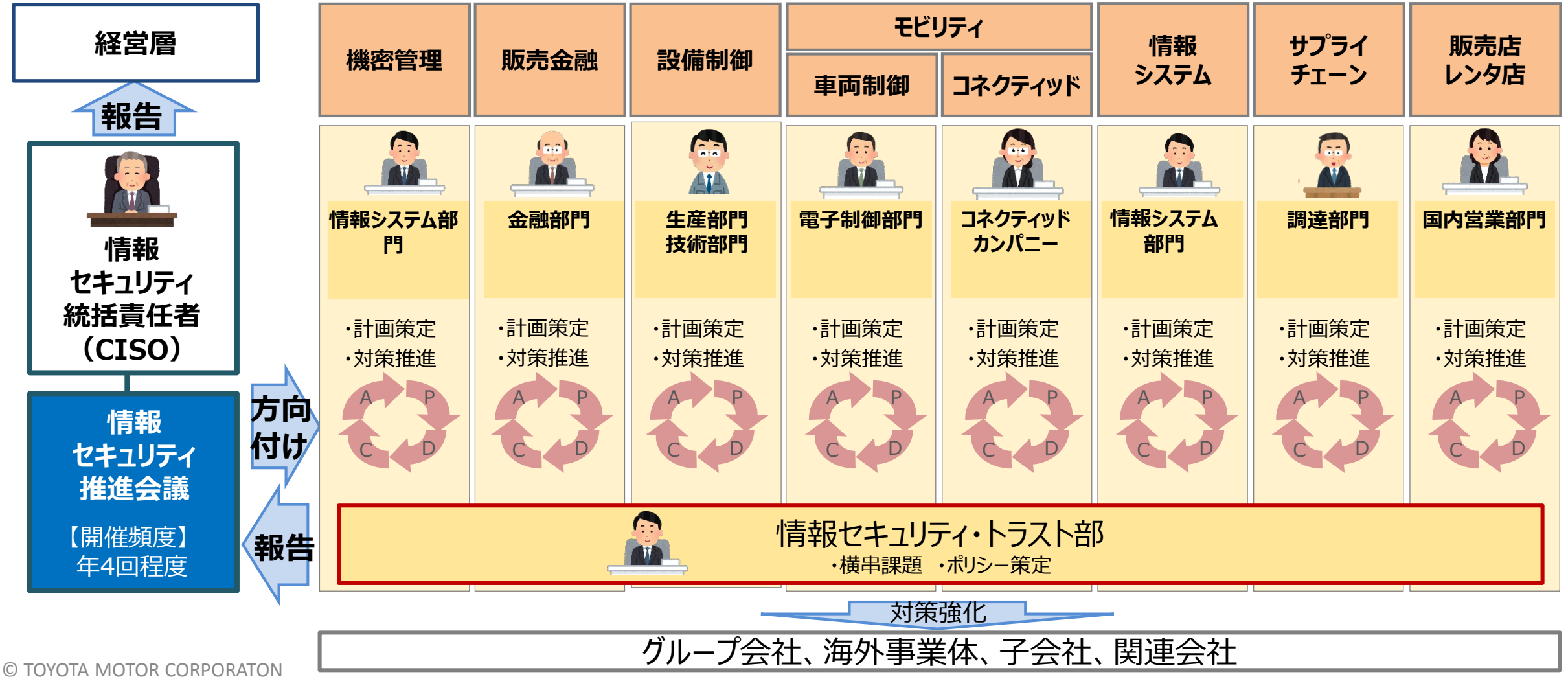
2．トヨタのセキュリティ取り組み体制

● サイバー攻撃は、全社の重点管理リスクのひとつ



2．トヨタのセキュリティ取り組み体制

- 分野別に役員クラスの責任者を設置、各分野でPDCAを回して対策を推進
- **CISOへ定期的に報告し、CISOが全体の方向付けや経営者との情報共有を実施**



3．トヨタへのサイバー攻撃の状況

- 攻撃検知件数だけでなく、グループ各社を含めた緊急対応件数が増加
- **サイバーセキュリティは対岸の火事でなく、差し迫った危機（リスク）**

＜ 緊急対応件数 ＞

※セキュリティ事故対応・予防・横展

主なサイバー攻撃	時期
販売店でお客様の個人情報漏洩の可能性	2019年3月
海外仕入先がランサム被害	2021年7月
国内仕入先がランサム被害	2022年多数
トヨタコネクティッドでメールアドレス漏洩の可能性	2022年10月

3．トヨタに関係するサイバー攻撃の事例（2022年）

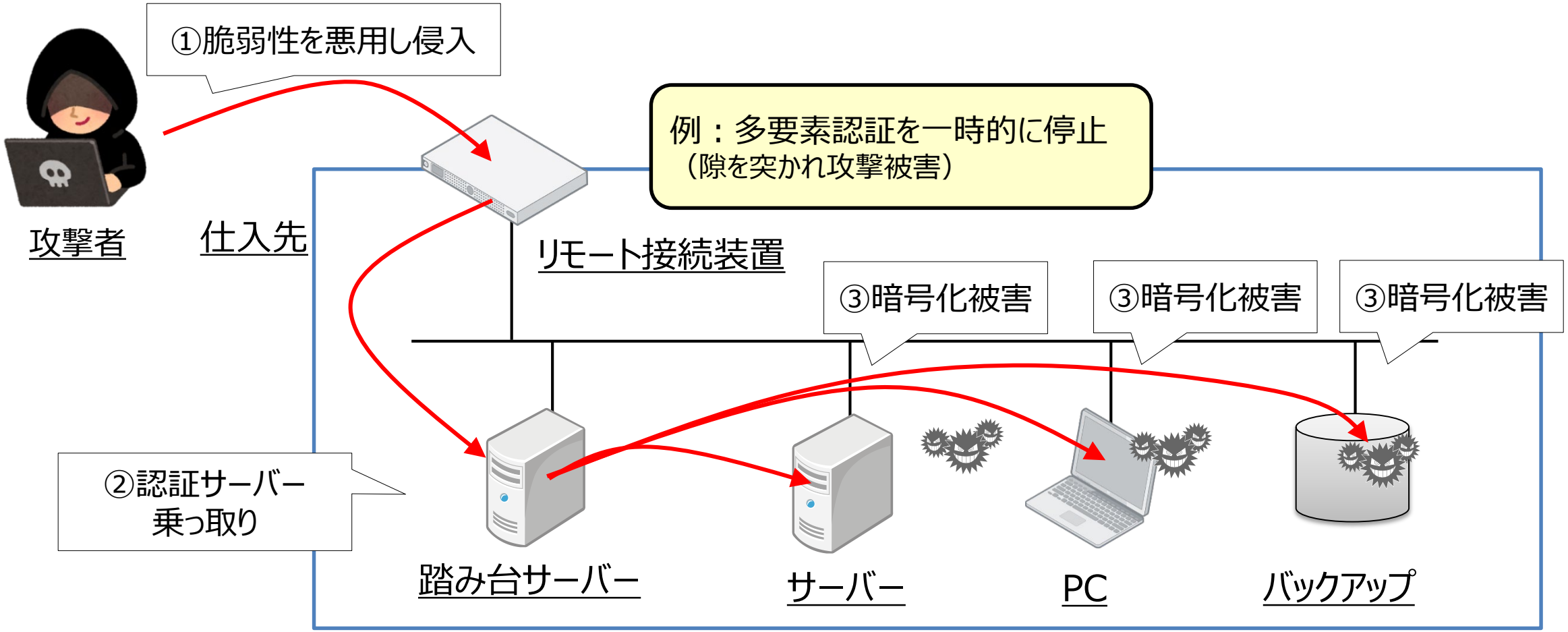
● 2022年以降、**仕入先へのランサム攻撃が多発**、業務に影響のあるケースも多い

時期	被災会社	地域	影響
2月	仕入先A	日本	**社内複数システム、N/W停止**
	仕入先B	北米	業務への影響なし
3月	仕入先C	北米	**社内複数システム、N/W停止**
	仕入先D	欧州	**社内複数システム、N/W停止**
	仕入先E	北米	業務への影響なし
4月	仕入先F	アジア	業務への影響なし
8月	仕入先G	日本	**社内複数システム、N/W停止**
9月	仕入先H	日本	**社内複数システム、N/W停止**

公開情報より自工会にて調査

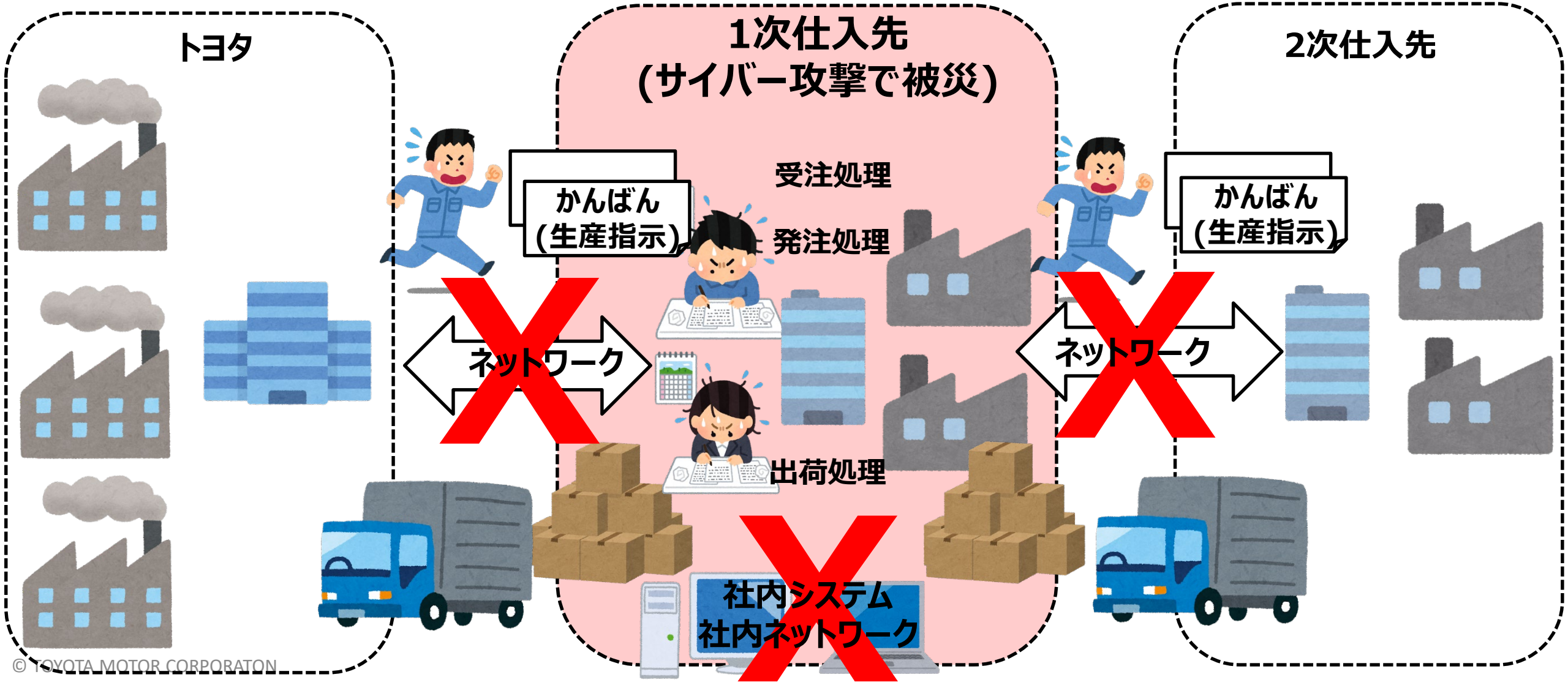
3．トヨタに関係するサイバー攻撃の事例（2022年）

- 仕入先へのランサム攻撃のほとんどが、リモート接続装置の脆弱性を起点とした攻撃



ご参考（仕入先での業務影響）

● ネットワークや社内システムを遮断する為、**マニュアルで受発注・出荷等を行い生産を継続**



ご参考（仕入先での業務影響）

- 停止システムは、受発注・出荷システムだけに限らず、**全ITシステムが停止**
  →全てをマニュアルで処理しなくてはならない
- **現場の社員の負荷・心理的重圧は非常に高い**
- **経営者は現場に寄り添った対応が大切**

こちらも
ご覧ください

トヨタイムズ サイバー

電子メール

研究・開発

生産管理

物流・在庫管理

ファイル共有

社内システム
ネットワーク

品質管理

リモート会議

販売管理

人事・給与

財務・会計

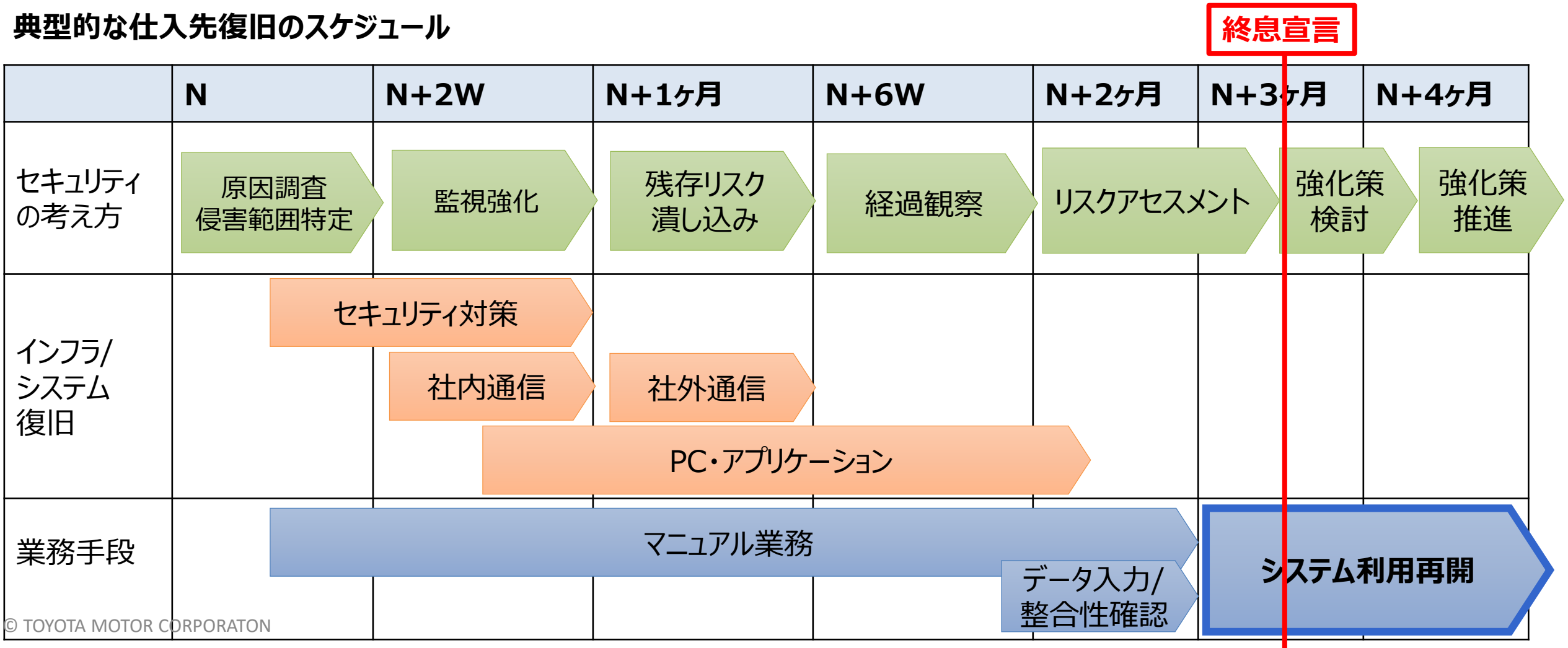
経理・原価管理

調達・購買

ご参考（仕入先での業務影響）

- 業務は継続できても、システムや業務オペレーションが**元通りになるには数か月かかることが多い**
- 仕入先への経営インパクト大 ⇒ **セキュリティは全社の経営課題**

典型的な仕入先復旧のスケジュール



4．経営者を含めた仕入先の理解活動

- 現地現物での実態調査（困りごと）で、仕入先に寄り添って対策
- **経営者**の方を含めて必要性をご説明するが、**意識醸成に苦労**
  ⇒愚直な理解活動を予定（説明会や啓蒙ビデオ）

＜トヨタの仕入先とのレベルアップ活動＞

	’22年			’23年		
	4～6月	7～9月	10～12月	1月～3月	4～6月	7～9月
セミナー― ワークショップ 問合せ窓口	セミナー	セミナー	セミナー	セミナー	セミナー	セミナー
	問合せ窓口			相談室		
現地現物での 実態調査	訪問調査トライ	訪問調査トライアルの拡大				
	【実績】延べ〇〇回			経営者を含めた 仕入先の理解活動		

ご参考 セミナーでの取り組み概要

- 緊急度／仕入先未達成項目（自己評価結果）から説明優先順位を決定

＜自動車産業ガイド 解説テーマ＞

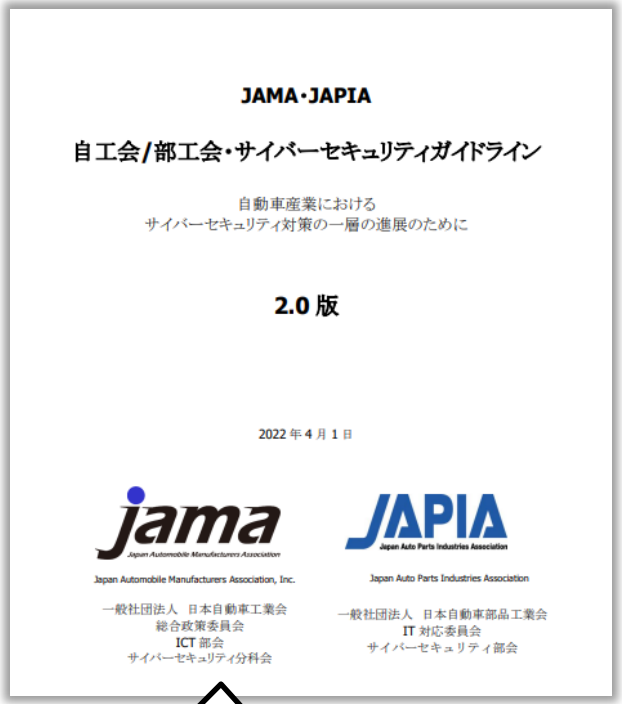
#	時期	項目分類、テーマ
第1回	2022/4	サイバー攻撃対策 -すぐ実行を検討頂きたい強化ポイント 済
第2回	2022/6	リスクアセスメント 済
第3回	2022/8	方針・体制の確立、規定の策定 済
第4回	2022/10	教育、アクセス管理 済
第5回	2022/12	セキュリティ事件事故に即効性のある設問 済
第6回	2023/2	外部との接続に関する対策 済

＜すぐ実行を検討頂きたい強化ポイント＞

No.	優先度	項目
1	高	緊急時の対応/連絡方法の確認
2	高	標的型メールに対する社内への注意喚起
3	高	OS/ソフトの最新版への更新
4	**高+**	**リモートアクセスの脆弱性対策**
5	**高**	**多要素認証の導入**
6	中	別ネットワークでのデータバックアップ
7	高	サーバーダウン時の生産継続

4．サプライチェーンのセキュリティ強化の取り組み

- ’19年～（経産省CPSFを基に）**自工会＆部工会の合同**で**業界標準ガイドライン**を策定
- ’21年3月～業界全体に対して、セキュリティレベルのセルフチェックを依頼
- 業界平均と自社セルフチェック結果との差異から**重点課題の認識**


JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

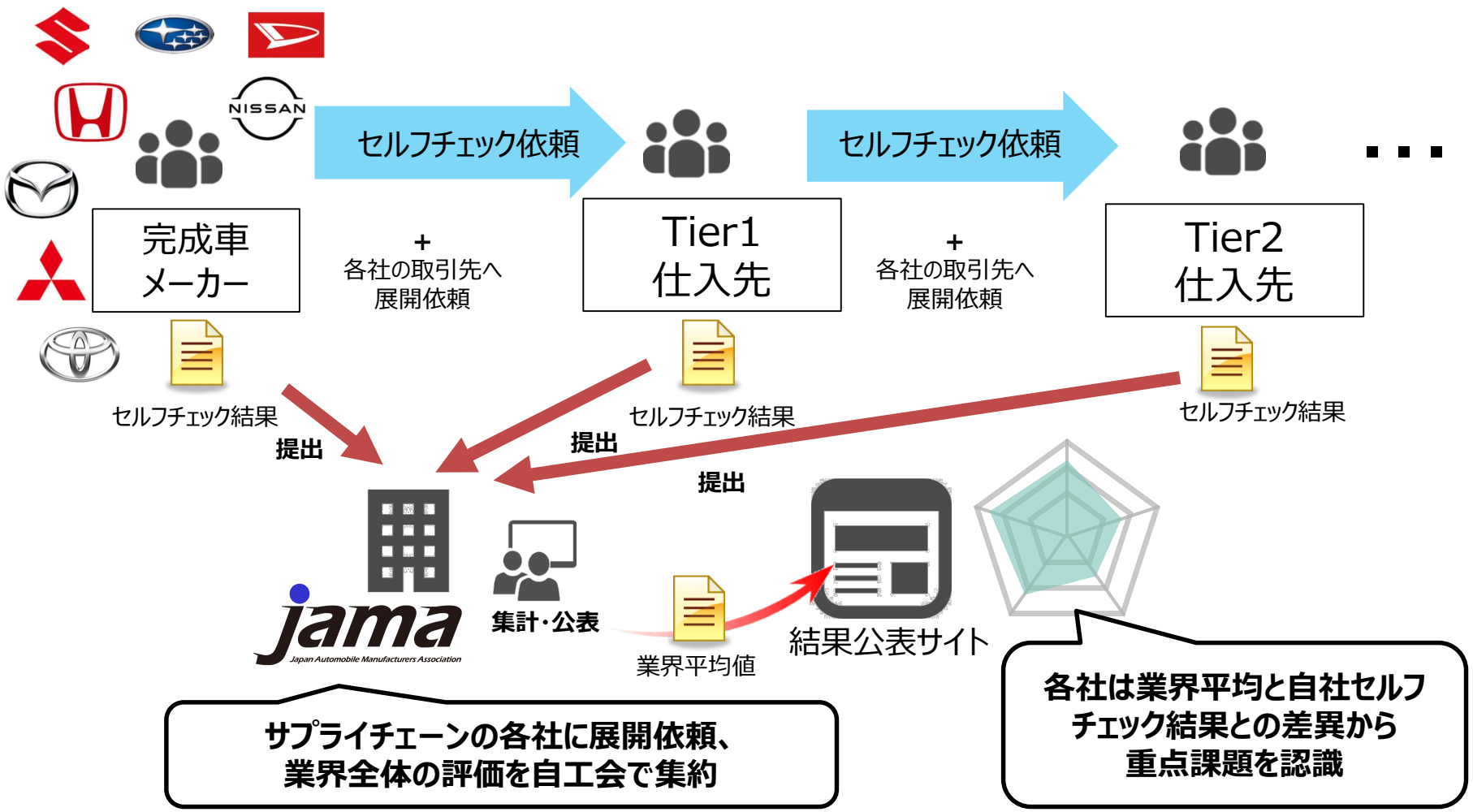
2.0 版

2022 年 4 月 1 日

jama
Japan Automobile Manufacturers Association, Inc.
一般社団法人 日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

JAPIA
Japan Auto Parts Industries Association
一般社団法人 日本自動車部品工業会
IT 対応委員会
サイバーセキュリティ部会

**自工会と部工会合同で
自動車業界標準の
セキュリティガイドラインを策定**



**サプライチェーンの各社に展開依頼、
業界全体の評価を自工会で集約**

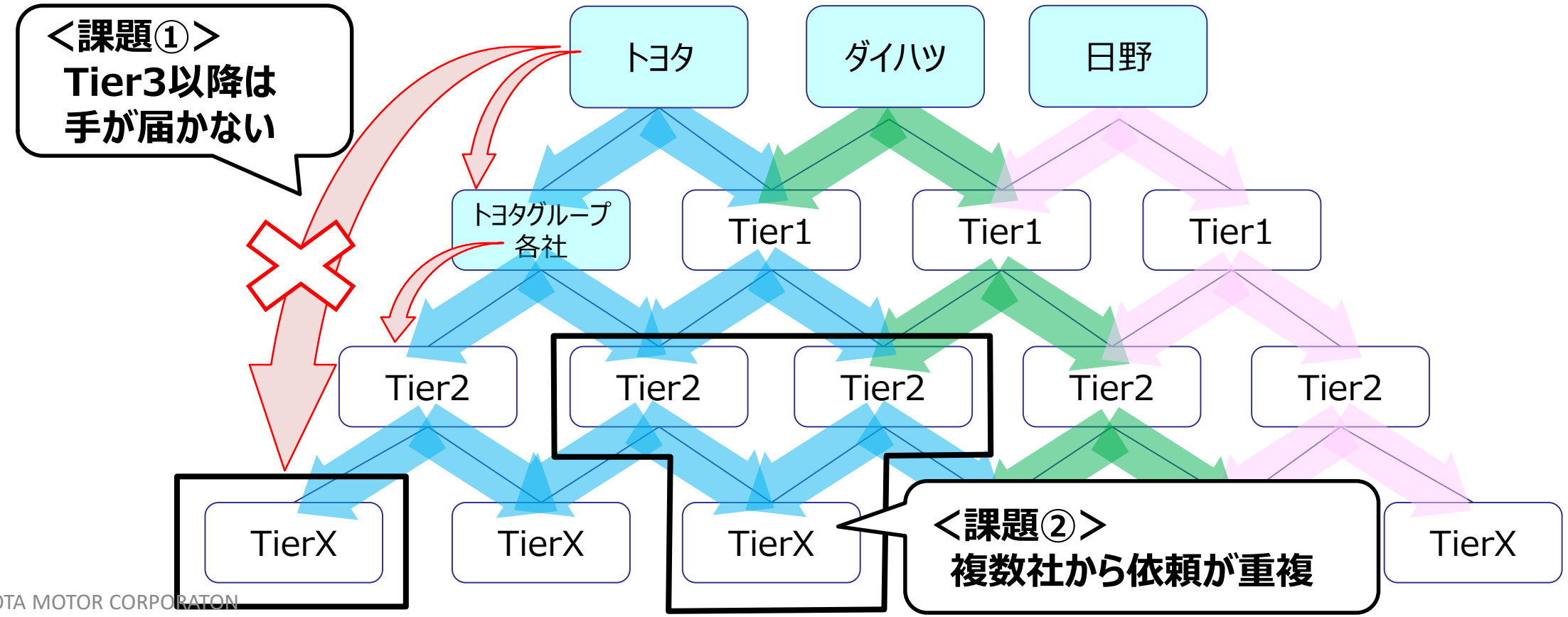
**各社は業界平均と自社セルフ
チェック結果との差異から
重点課題を認識**

※自工会資料

4．サプライチェーンセキュリティ強化での課題

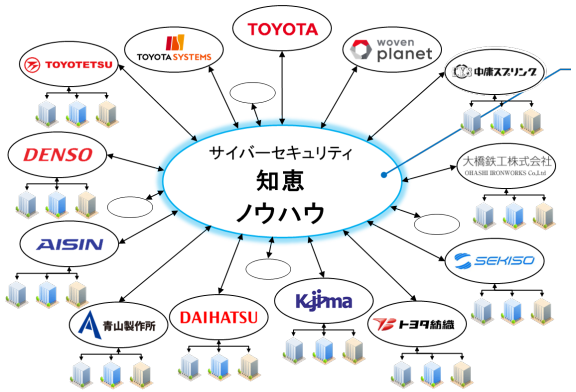
課題

① 取引契約の無い会社への対応が困難（Tier３以降）
② 仕入先が重複する場合は、複数社から依頼が重複
⇒ 特にTier３以降の仕入先のセキュリティ対策が課題



4．業界を超えたサプライチェーンセキュリティ強化に向けて

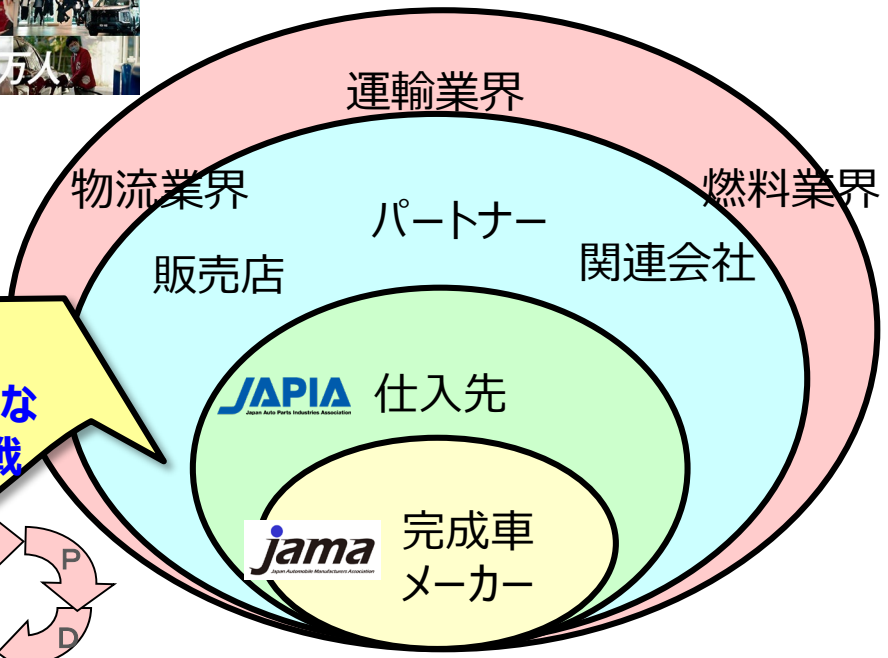
- 現在：完成車メーカーと仕入先の活動
- 今後：他業界の皆さまとも連携し、経営者を含めた意識醸成を行いたい

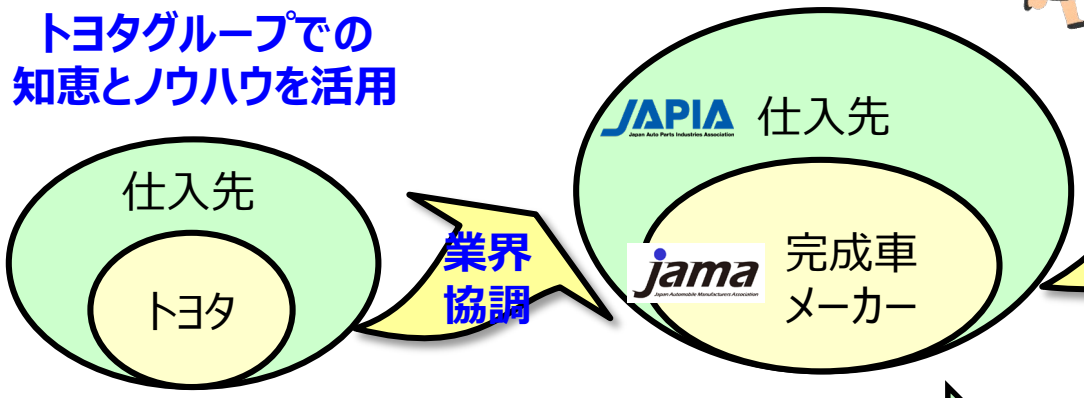


トヨタグループでの
知恵とノウハウを活用

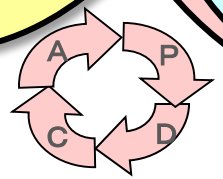
クルマを走らせる550万人
全員でレベルアップ

業界で協調して
行動





新たな
挑戦



これまでの活動

SC3 サプライチェーン・サイバーセキュリティ・コンソーシアム

※画像：自工会HPより

ご清聴ありがとうございました

TOYOTA