txOne networks *The Leader of OT Zero Trust*

2022年 ICS/OTサイバーセキュリティ実態調査に関する報告
Insights Into ICS/OT Cybersecurity 2022

2023年3月30日

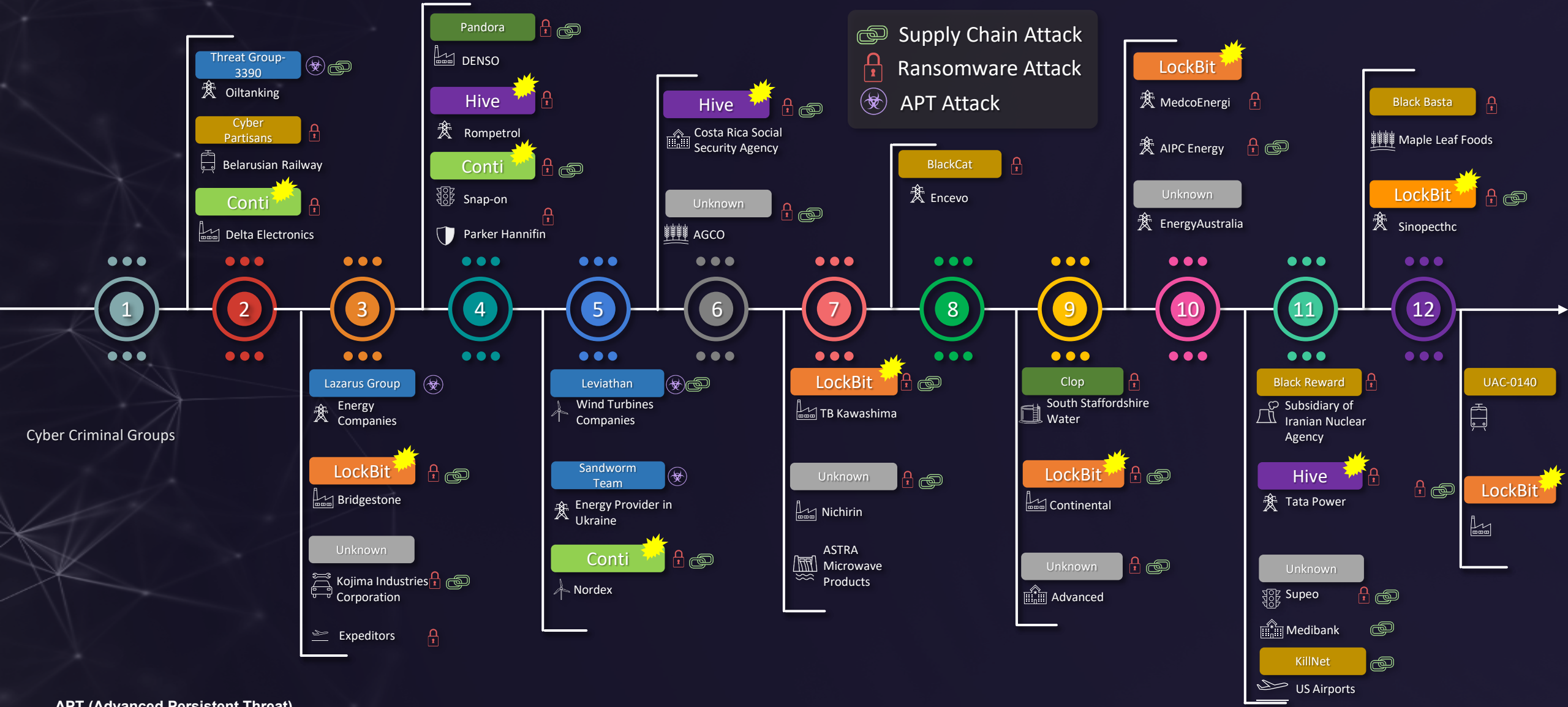
TXOne Networks Japan合同会社

本報告の内容

1. 2022年 サイバーセキュリティインシデント状況
2. OTセキュリティを取り巻く環境
3. OTセキュリティ エンドユーザ調査結果
4. TXOne Networksの取り組み

第1部
2022年 ICS/OTサイバーインンシデント状況

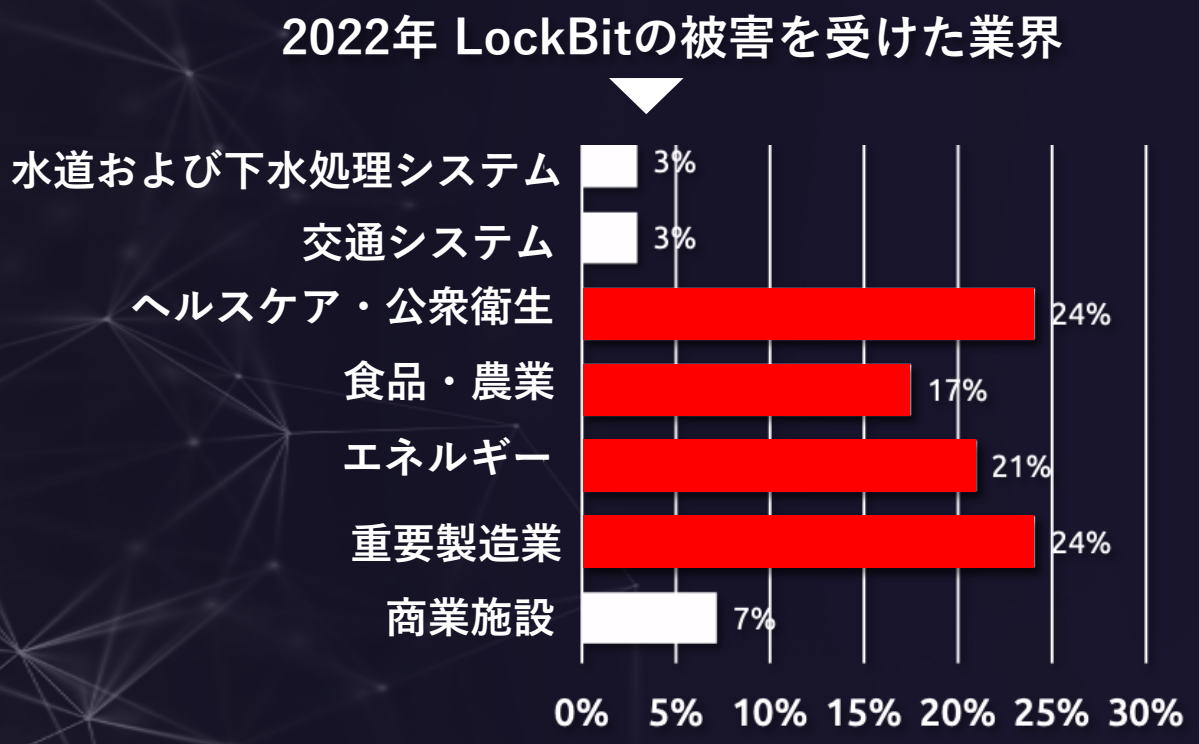
2022年の 主なOTセキュリティインシデント



APT (Advanced Persistent Threat)
特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続するサイバー攻撃

Source: ANNUAL REPORT Insights Into ICS/OT Cybersecurity 2022

多重脅迫型ランサムウェアが急増



Source: TXOne Networks Annual Report Insight Into ICS/OT Cybersecurity 2022

1. ランサムウェアの活発化・多重脅迫・高度化

- LockBit 3.0をはじめとする多種多様なRaaS (Ransomware-as-a-Service) の活動増加
- 脅迫手段の多様化(多重脅迫)
  - (1) データ破壊・暗号化
  - (2) 窃取した情報の暴露
  - (3) DDoS(Distributed Denial of Service)攻撃
  - (4) 被害者の顧客・利害関係者への連絡
- 解析を妨げる様々な手法の登場
  - パスパラメータ
  - 高度な暗号化

2. 重要インフラへのランサムウェアによる被害拡大

- 電力・石油・ガス・水処理施設に加え、医療・公衆衛生機関をもターゲットに

ランサムウェアとRaaS

従来のランサムウェア攻撃

攻撃者に高い技術が必要

RaaSの利用

進化

技術がなくとも容易に攻撃可能

代表的なRaaS

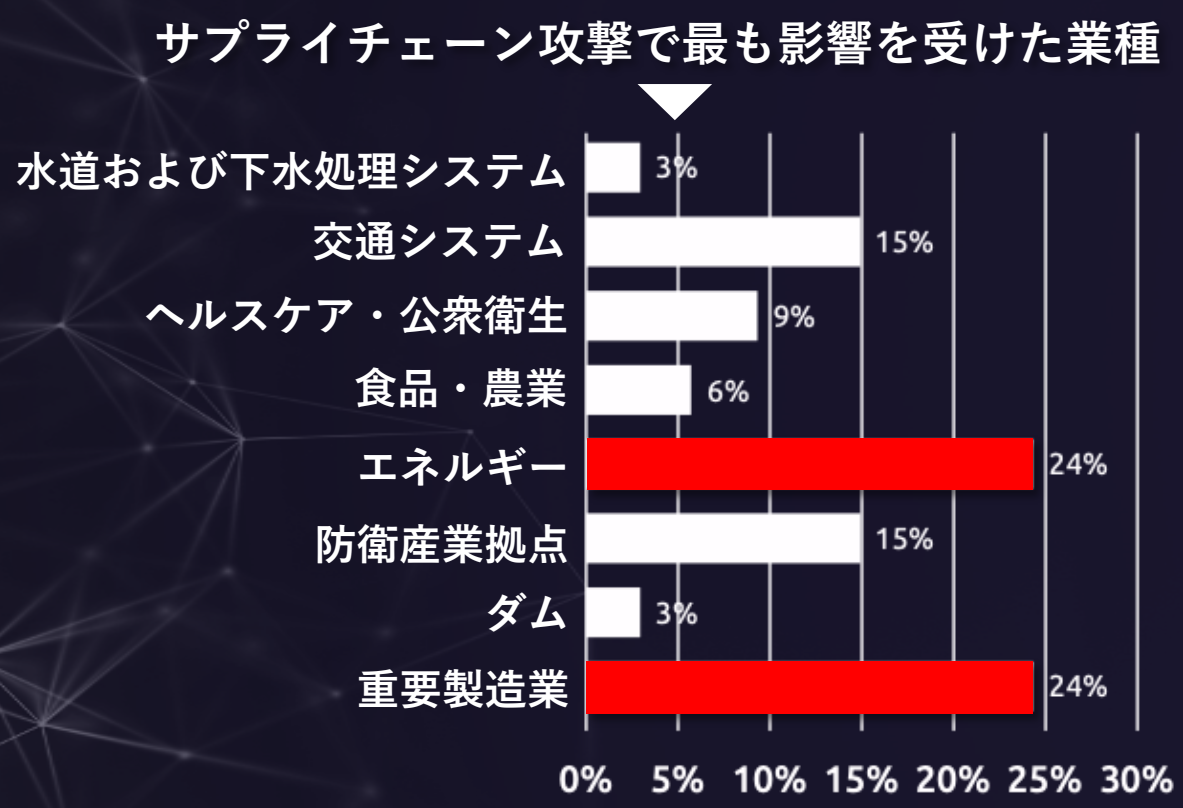
Conti
- きわめて悪質、医療機関を標的に
- 身代金支払い後もデータ復旧不可、情報漏洩の事例が多数

LockBit 3.0
- 解析を困難にするためのさまざまな技術
- 内通者に報奨金、バグ報奨金プログラム
- ロシアおよび旧ソ連諸国の資産は攻撃対象外
- 2022年7月、被害者データが自由に閲覧できる状態に

Hive
- 多種多様な攻撃手段を備える
- 米国では医療機関への脅威として注意喚起
- 2023年1月に米FBIがいくつかのサイトの差し押さえに成功

txOne networks

サプライチェーン攻撃が増加



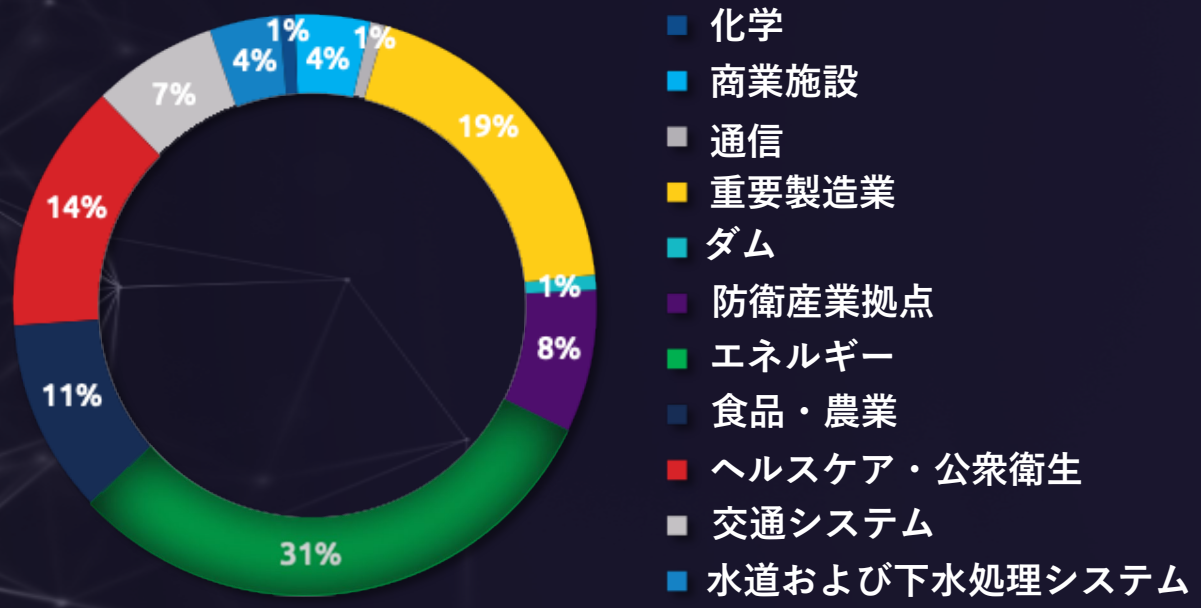
Source: ANNUAL REPORT Insights Into ICS/OT Cybersecurity 2022

- 2022年は99のサプライチェーンインシデントを観測
  (Q1:13, Q2:23, Q3:29 and Q4:33)
  - 最もサプライチェーン攻撃を受けた業種は、エネルギーおよび重要製造業

- サプライチェーン攻撃により重要な企業活動が中断
  - 各企業では、サプライチェーンリスクアセスメントの優先度を上げて取り組むべき

重要インフラがターゲットに

重要インフラで発生したサイバーインシデント
業種内訳



Source: ANNUAL REPORT Insights Into ICS/OT Cybersecurity 2022

- 重要インフラで合計85件のインシデント
  - エネルギーが主要ターゲット
- エネルギーや公共事業で、Raas (Conti, LockBit, Hiveなど) が猛威を振るう
- 地政学的な対立により重要インフラのセキュリティリスクが増加
- 重要インフラ産業の相互依存性の高さを狙い、サプライヤーに対して持続的標的型（APT：Advanced Persistent Threat）やランサムウェア攻撃の脅威が増大

第2部
OTセキュリティを取り巻く環境

2.1 ITとOTシステムの統合

- IT/OT統合によるイノベーション推進
  - ITインテリジェンスがOT資産に適用され、効率改善・運用合理化・新サービス導入が促進
- IT/OT組織的統合
  - 共通ガバナンスモデル
  - プロセス整合
  - データ・セキュリティ一元管理

- インダストリアルIOTアーキテクチャ浸透による脆弱性の拡大
  - クラウド接続による攻撃対象領域の拡大
- OT特有の課題
  - エアギャップ環境(ネットワークに接続せずに隔離)への対策
  - 多様なOTプロトコル
  - レガシOSの存在
  - 規制や保証対応のためのエンドポイント制約

2.2 各国政府による政策と規制強化

日本

- Society 5.0により、サイバー空間と物理空間を高度に統合することを国家戦略として推進
- 2022年11月の経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」で、参照すべき考え方やステップを提示
- 2022年12月16日の国家安全保障戦略で「積極的サイバー防御」 の方針

米国

- 2021年5月の大統領令14028号「国家サイバーセキュリティの強化」で、重要インフラの保護のためのOTサイバーセキュリティの重要性を強調。
- 2022年3月、「重要インフラに関するサイバーインシデント報告法令(CIRCIA)」が法制化。IT/OTセキュリティの規制(インシデント発生から72時間以内、身代金支払いから24時間以内の報告義務)

EU

- 2020年12月の「EU NIS (Security of Network and Information Systems) 2.0指令」により、重要インフラにフォーカス
- 欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe）を設立、大規模サイバーセキュリティ事故発生時の対応を強化
- 2022年9月のサイバーレジリエンス法案では、設計段階からのセキュリティの作り込み(セキュリティ・バイ・デザイン)を推進

2.2 グローバリゼーションから ローカリゼーションへの回帰

- 「グローバリゼーション」から「ローカリゼーション」や「リージョナライゼーション（地域化）」、リショアリングへ
  - 安い労働力・土地を第一条件とした立地戦略から、生産ラインを母国に戻す回帰戦略へ
  - 米国・ドイツ・日本・韓国・英国等でも、製造業のリショアリング（自国回帰）を推進
- 新工場の建設時からのICS/OTサイバーセキュリティ対策

第3部
OTセキュリティに関する
エンドユーザ調査と考察

企業調査の背景

- 製造業・重要インフラを標的とした攻撃の増加により、OTに対するセキュリティの重要性が再認識されつつある
  - 生産ラインの操業中断、生産性低下による経済的損失
  - 情報漏洩による経済的損失、顧客からの信頼失墜、ブランド価値低下

- OTネットワークの保護を情報セキュリティ戦略に大きな責任を持つ企業経営者・情報セキュリティ責任者にインタビュー実施
- 今後のOTサイバーセキュリティを提供するための基盤

OTセキュリティに関するエンドユーザ調査

対象国

ドイツ
33%

米国
33%

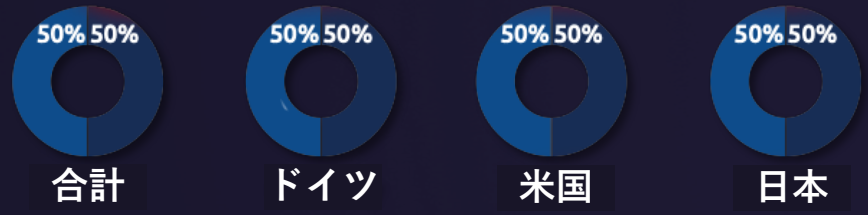
日本
33%

業種

役職

	合計	ドイツ	米国	日本
経営幹部・取締役（COO, CSO, CISO, CIO, VP/工場オペレーション/製造担当ディレクター）	40%	40%	40%	40%
その他管理職（工場/製造オペレーションマネージャー，製造責任者/工場オペレーション，セキュリティ・チーム・リーダ）	60%	60%	60%	60%

半導体製造業者の割合



OTに対する責任

	合計	ドイツ	米国	日本
OTサイバーセキュリティ管理の責任者	67%	65%	71%	65%
OT業務に関して職務範囲で報告する立場	33%	35%	29%	35%

FROST & SULLIVAN

txOne networks

OTセキュリティの現状

Insight 1:

サイバーセキュリティの複雑さにどう対処するか

Insight 2:

OTサイバーセキュリティ特有の課題

Insight 3:

新規アセットをOT現場に持ち込むための注意事項

Insight 4:

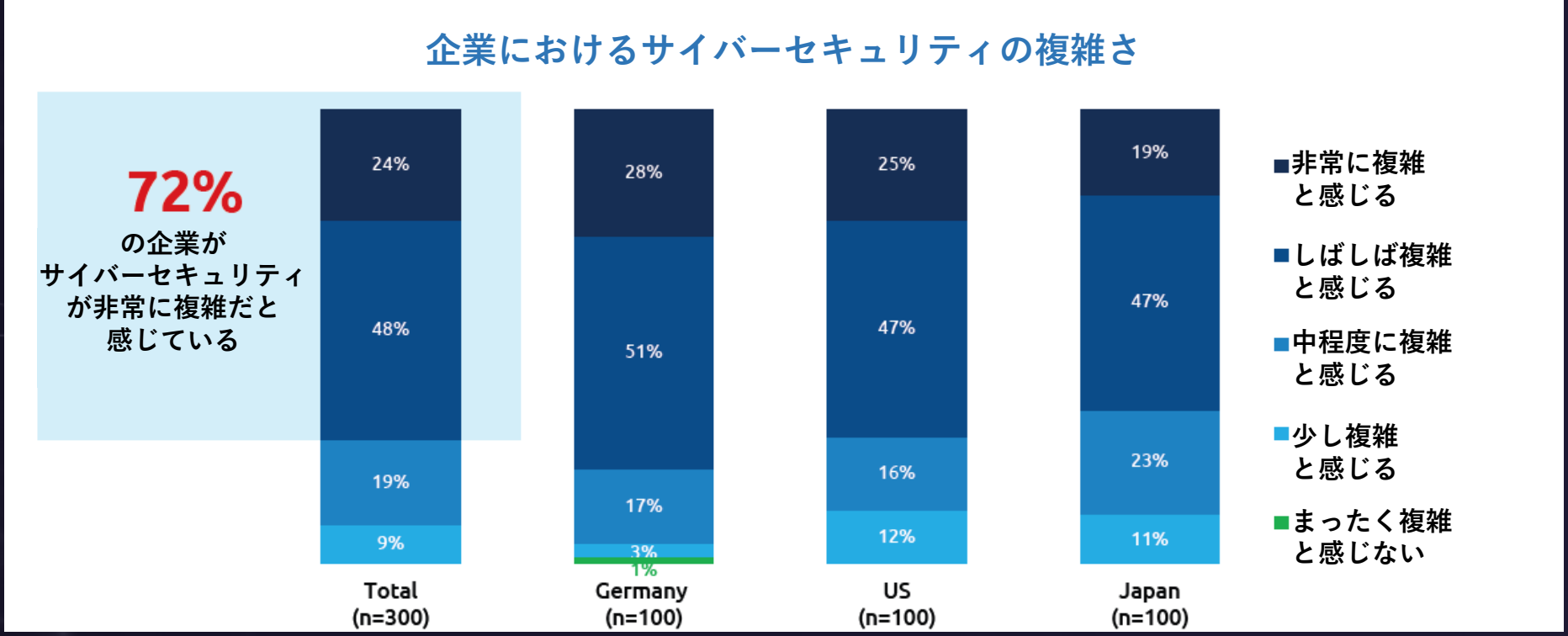
OT特化のサイバーセキュリティの必要性

Insight 5:

OTセキュリティ関連予算の増加

Insight 1:
サイバーセキュリティの複雑さにどう対処するか

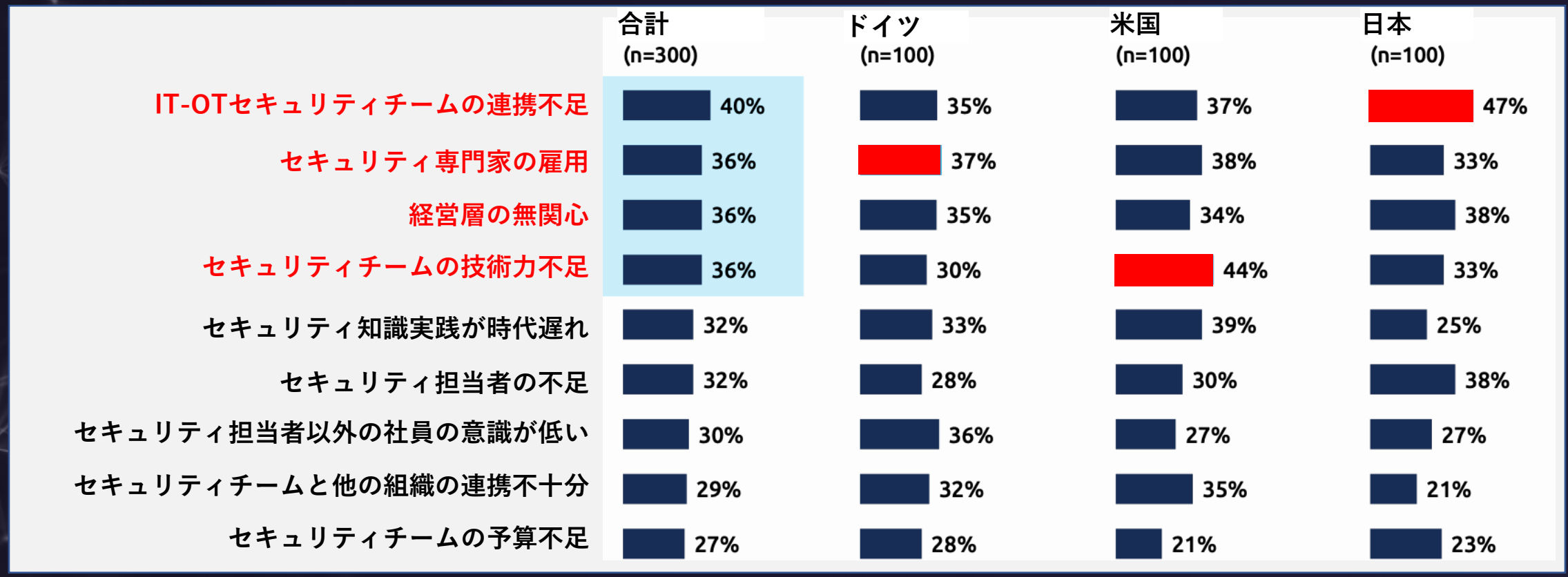
72%の企業がサイバーセキュリティが著しく複雑であると回答



Q - あなたの企業ではどの程度サイバーセキュリティが複雑だと感じていますか？
（評価 1-まったく複雑だと感じない　～　5 - 非常に複雑だと感じる）

Source: Frost & Sullivan

OTセキュリティの人材問題



Q - 過去12カ月間に直面してきたセキュリティ人材の主な課題は何ですか？

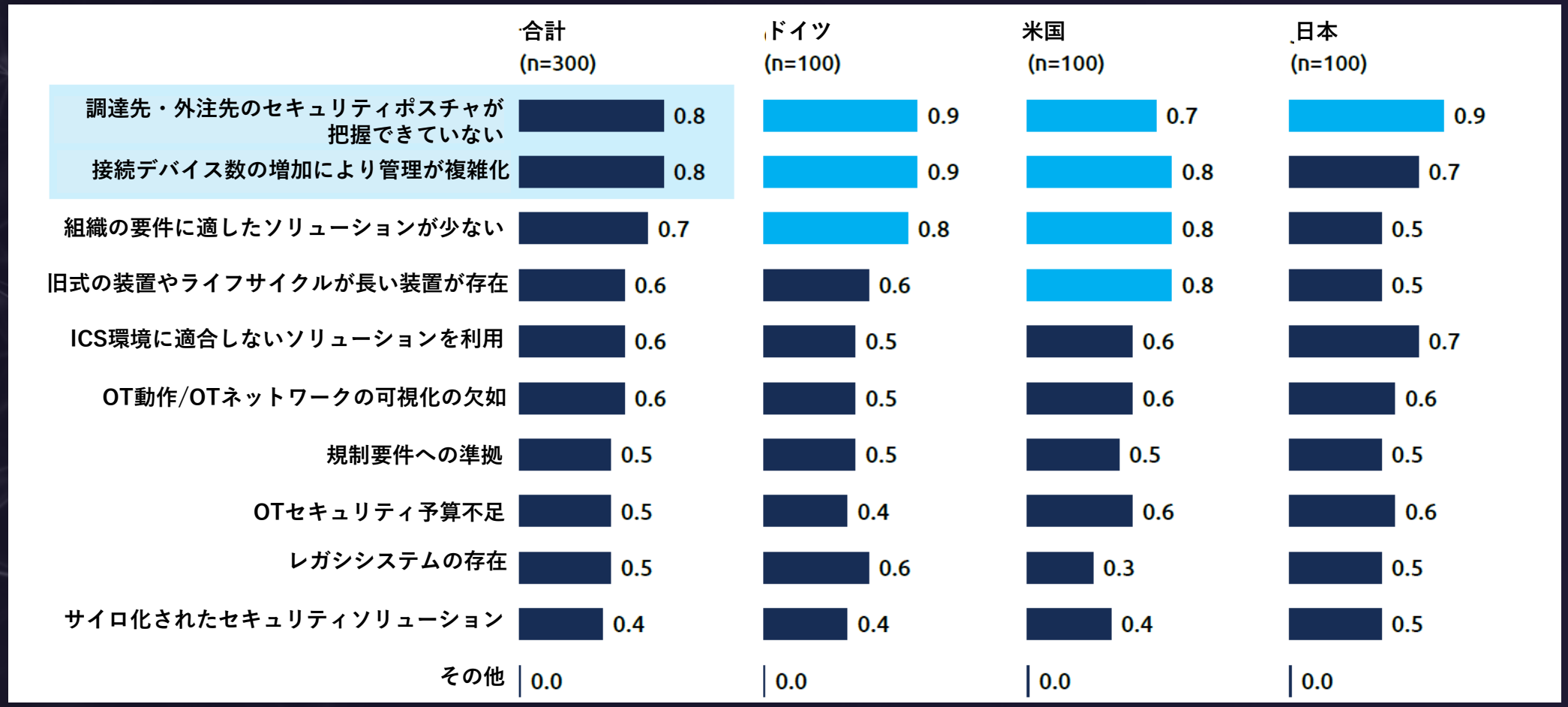
Source: Frost & Sullivan

セキュリティの複雑さへの取り組み

- ITとOTの両方のセキュリティ部門の連携
- セキュリティ人材の確保
- 経営層のコミットメント
- 技術的手段導入による複雑さの回避

Insight 2:
OTセキュリティ環境における新たな課題

OTサイバーセキュリティの主な課題



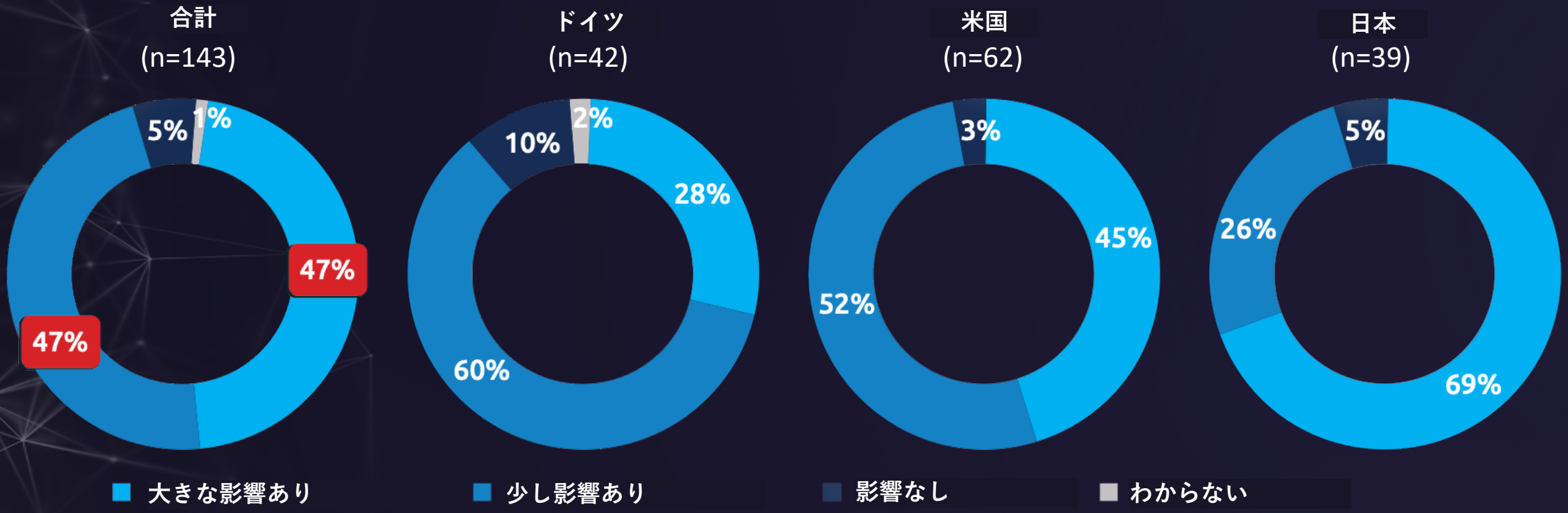
Q.直面しているOTサイバーセキュリティ上の主な課題は何ですか？上位3つを選択してください。（平均スコアでランク付け）

Source: Frost & Sullivan

txOne networks

ITセキュリティインシデントのOT環境への影響度

94%のITセキュリティインシデントがOT環境にも影響が波及

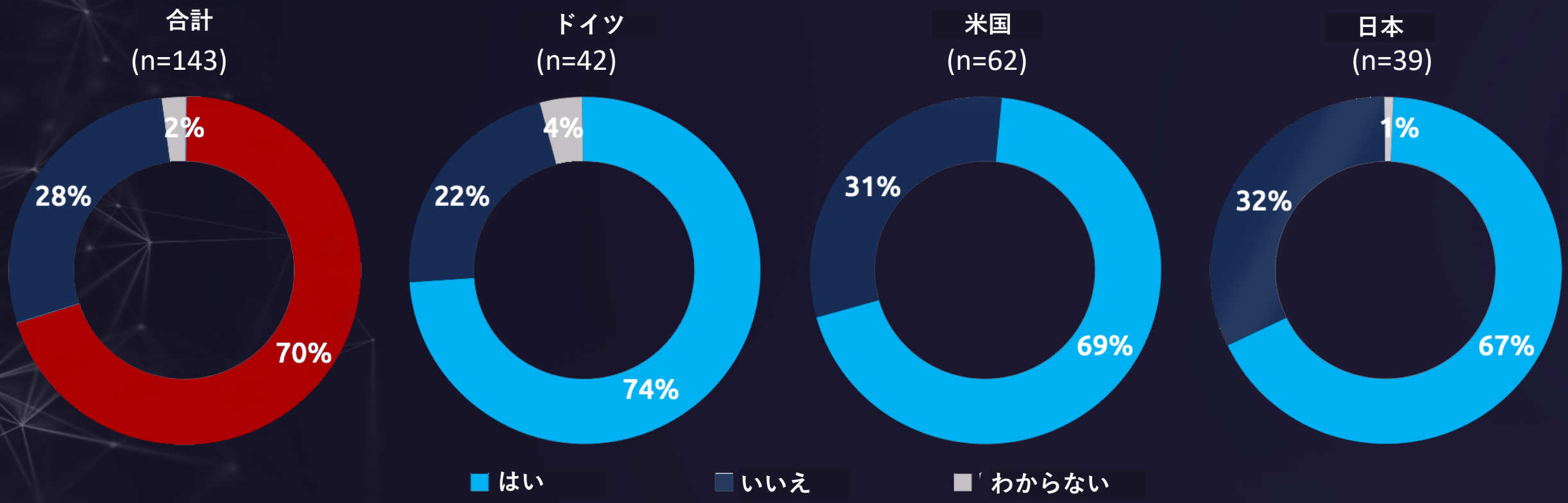


Q - ITセキュリティインシデントは、OT環境にも影響がおよびましたか？

Source: Frost & Sullivan

70%の企業がデータや事業活動を人質に取られた経験

ランサムウェア攻撃で甚大な損失・経済的損害
最も一般的な手口は、データや事業活動を人質に取ること



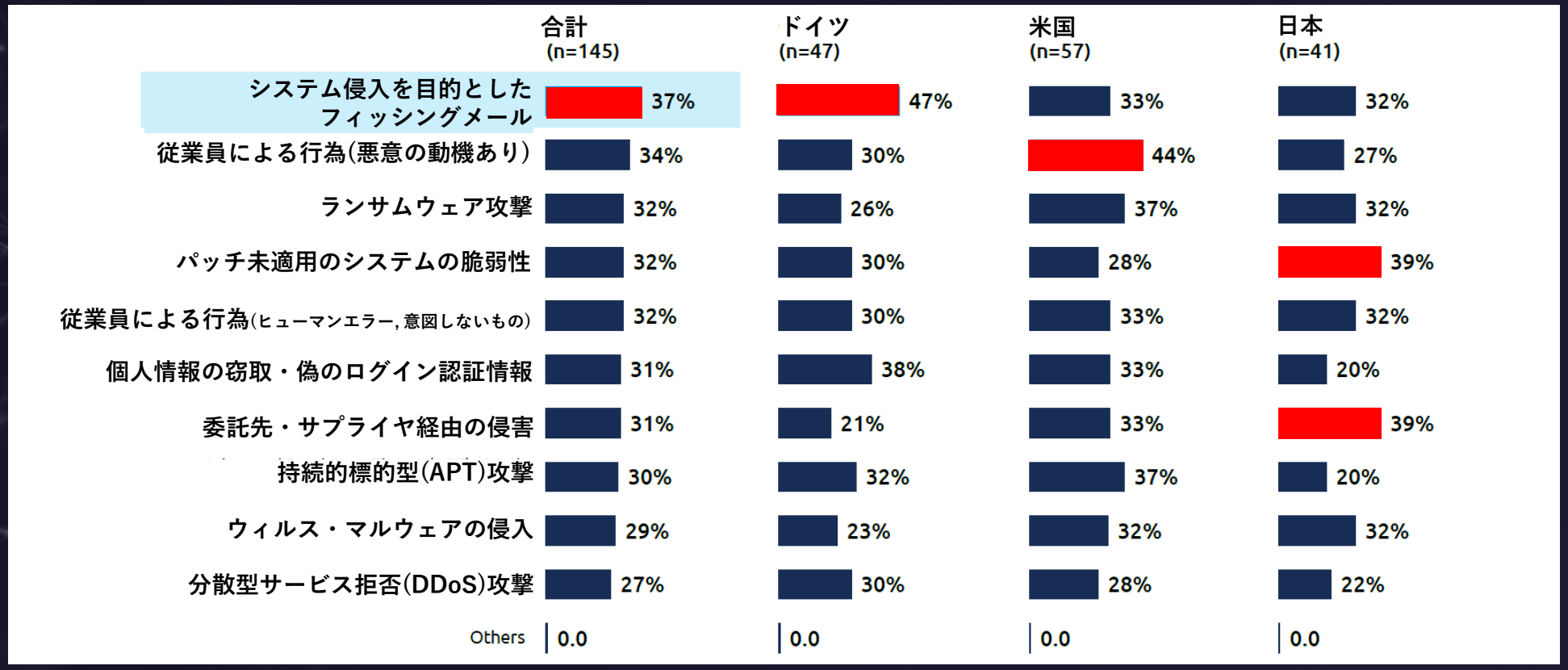
Q - データや事業活動を人質に取られたことがありますか？

Source: Frost & Sullivan

Insight 3:
新規アセットをOT現場に持ち込むための注意事項

OTセキュリティインシデントの種類

- IT由来のフィッシングメール、内部関係者によるもの、ランサムウェア攻撃がトップ３
- 外部/内部からの攻撃や横移動の防止が必要

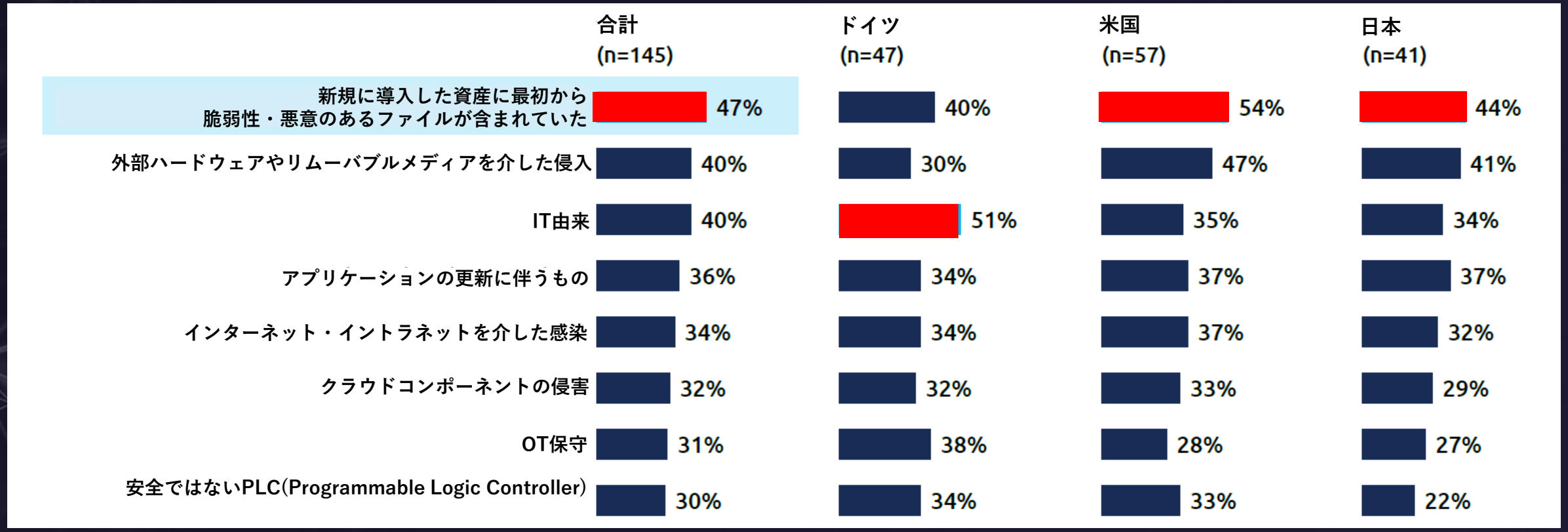


Q - 過去12カ月に経験したOTセキュリティインシデントは次のうちどれですか？

Source: Frost & Sullivan

OTセキュリティインシデントの原因

- 最も多いのは、新規に導入した資産に脆弱性や悪意のあるファイルが含まれていたこと
- 外部ハードウェア、リムーバムルメディア(USBメモリスティックなど)が続く
- 個々の新規アセットのスキャニングが有効な保護手段

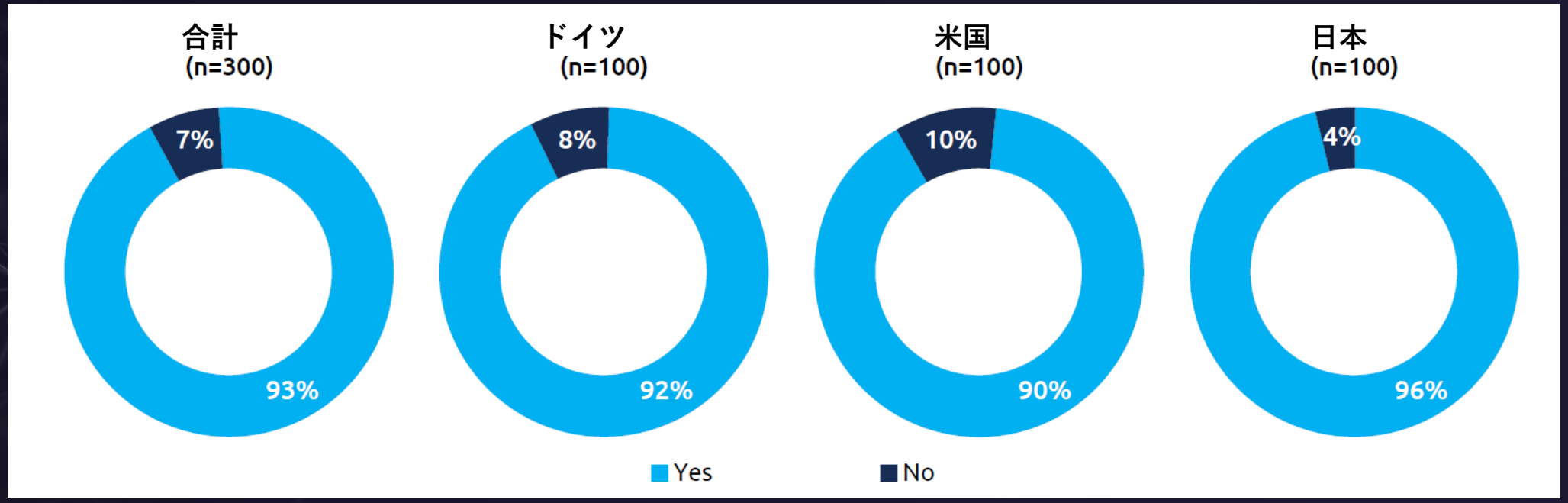


Q - 過去12カ月に発生したOTセキュリティインシデントの原因は何ですか？

Source: Frost & Sullivan

Insight 4:
OT特化のサイバーセキュリティの必要性

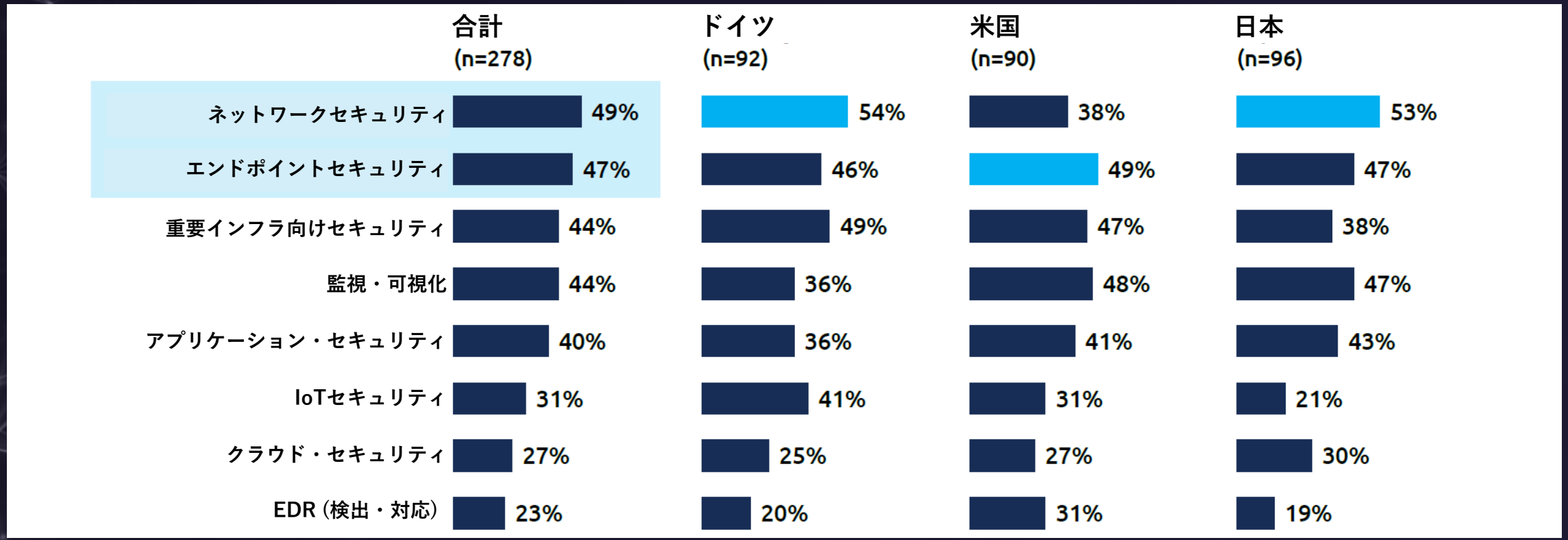
現在のサイバーセキュリティソリューションの使用状況
すでにOTセキュリティの導入は進んでいるが・・・



Q - 現在、OTセキュリティ用にサイバーセキュリティソリューションを使用していますか？

Source: Frost & Sullivan

OTセキュリティに提供しているサイバーセキュリティソリューション



Q - 現在、OTセキュリティ用に使用しているサイバーセキュリティソリューションは次のうちどれですか（カテゴリー別）？

Source: Frost & Sullivan

OT環境に適したセキュリティ対策の必要性

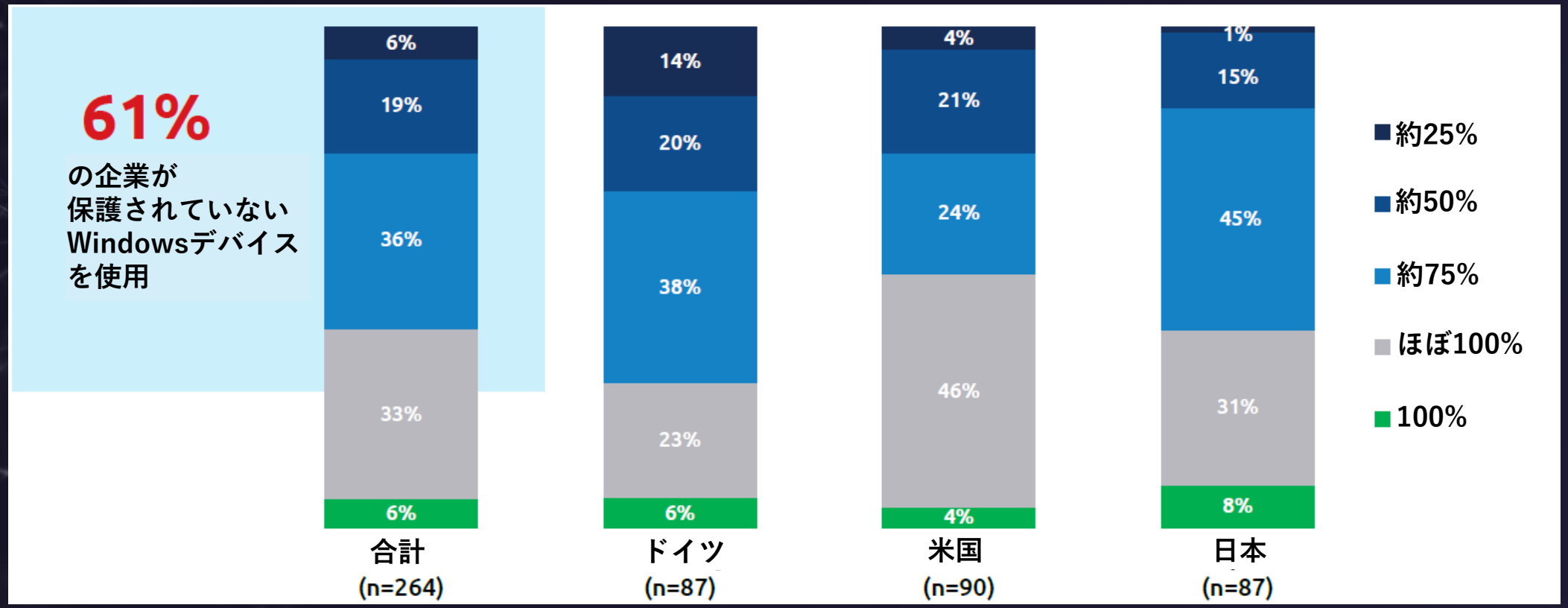
93%の企業がセキュリティを導入し、OT環境にも対策適用済みにもかかわらず、
なぜ重大なインシデントが頻発するのか？

考えられる理由：

1. **不適切なソリューションの適用**
   - OT環境にITソリューションを適用
   - 約70%の企業が、ITソリューションをOT環境への転用を検討
2. **人手不足**
   - 特に日本ではセキュリティに携わる人員が極めて少ない。
     - 平均、１担当者あたり101～200台のデバイス
     - 最悪の場合、１担当者あたり301～400台のデバイス
3. **セキュリティ対策が不徹底**
   - 61%の企業で、保護されていないWindowsデバイスを使用している。
4. **サポート対象外の旧式デバイスに適用**
5. **人的ミス（オペレーションミス）**

すべてのWindowsデバイスへのエンドポイントセキュリティ対策を行っている企業はわずかに6%

- OT環境での保護されていないWindowsデバイスの存在は攻撃されるリスク大
- 多様なOT環境に対応できる適切なエンドポイントソリューションが望まれる



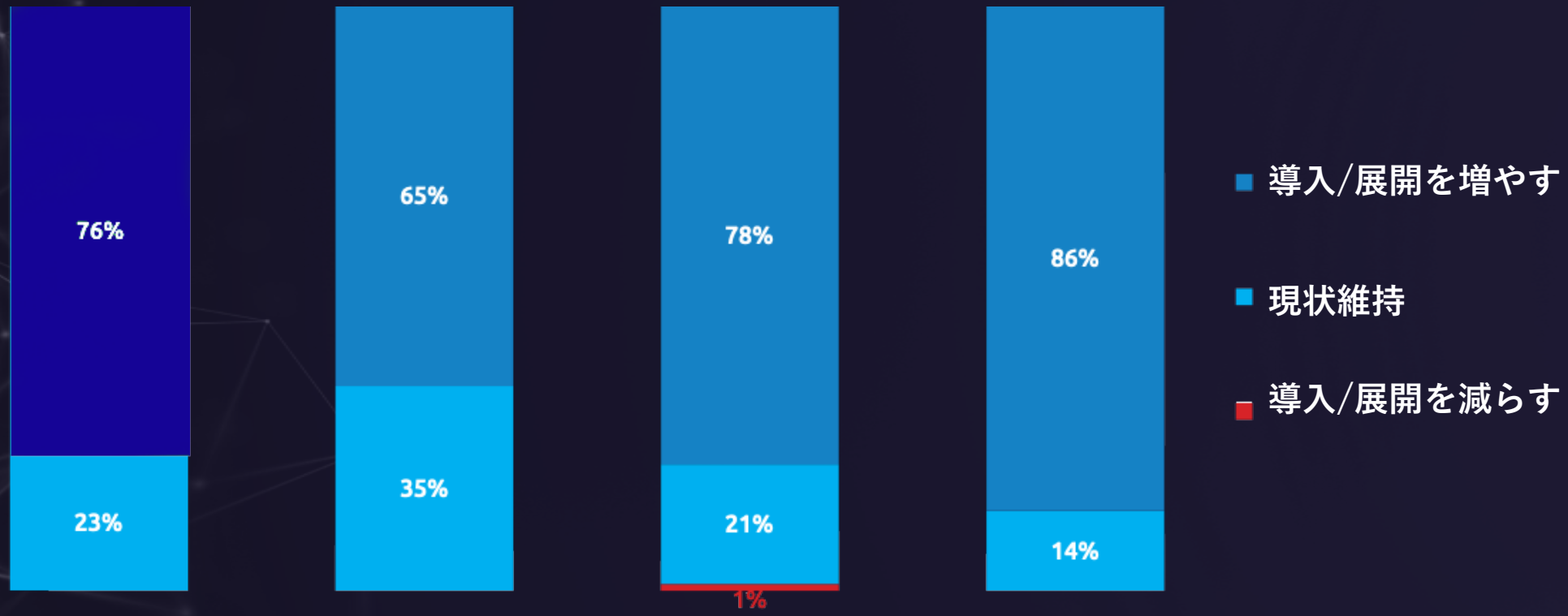
*Q - エンドポイント・セキュリティ・ソリューションで保護されている**Windows**ベースの**PC**およびデバイスの割合はどの程度ですか？*

Source: Frost & Sullivan

Insight 5:
OTセキュリティ関連予算の増加

OTセキュリティの予算は増加傾向

- 76%の企業がOTセキュリティの導入・展開を進めようとしている



Q - OTセキュリティ用サイバーセキュリティソリューションの導入/展開を増やす/減らす予定はありますか？

Source: Frost & Sullivan

まとめ

課題	今後の取り組み
Insight 1: セキュリティの複雑さ ITセキュリティ・インシデントがOT環境に影響	IT/OT両方のセキュリティ部門の連携 技術手段の導入
Insight 2: OT特有の課題 供給業者・委託先のセキュリティポスチャ把握	供給業者・委託先のセキュリティ管理手法の確立
Insight 3: 新規アセット導入 新規導入のアセットに脆弱性	資産導入前の対策強化
Insight 4: OT特化 ITソリューションの適用には問題あり	旧式から新型まで、包括的に導入可能なソリューションの採用

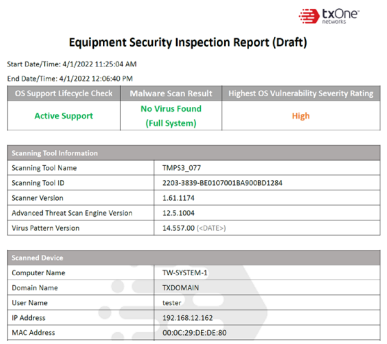
第4部
TXOne Networksの取り組み

OT環境の特性にフィットした"OT-Native"な製品

セキュリティ検査

Portable Security

導入装置や作業用PC経由の感染を防ぐ


txOne networks

Equipment Security Inspection Report (Draft)

Start Date/Time: 4/1/2022 11:25:04 AM
End Date/Time: 4/1/2022 12:06:40 PM

OS Support Lifecycle Check	Malware Scan Result	Highest OS Vulnerability Severity Rating
Active Support	No Virus Found (Full System)	High

Scanning Tool Information	
Scanning Tool Name	TMPS3_077
Scanning Tool ID	2203-3839-BE0107001BA900BD1284
Scanner Version	1.61.1174
Advanced Threat Scan Engine Version	12.5.1004
Virus Pattern Version	14.557.00 (<DATE>)

Scanned Device	
Computer Name	TW-SYSTEM-1
Domain Name	TXDOMAIN
User Name	tester
IP Address	192.168.12.162
MAC Address	00:0C:29:DE:DE:80

- インストール不要
- 端末に挿入するだけの簡単操作
- 検索結果をLEDで通知

＜レポート取得情報＞

- マルウェア検索結果
- システム情報
  (ホスト名、IPアドレス、OS、MACアドレス等)
- インストール済アプリケーション
- 適応済みパッチ
- 未適応パッチと関連する脆弱性情報
  (次期Verで実装予定)

OTエンドポイント保護

TXOne Stellarシリーズ

マシンリソースが不十分、パッチ適用が
困難なWindows端末の保護

OT向け
次世代アンチウイルス

Windows 7
Windows Server 2008
以降に対応

ロックダウン型
セキュリティ対策

Windows XP
Windows 7
Windows 2000
以降に対応

ネットワーク保護

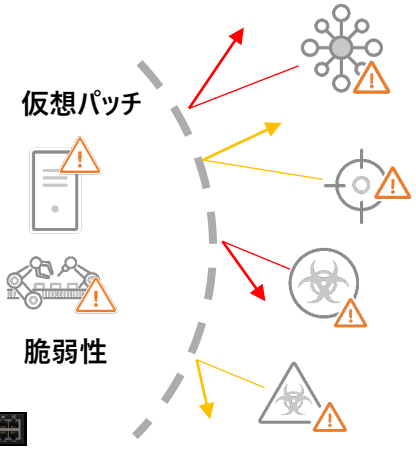
TXOne Edgeシリーズ

ネットワークセグメンテーションによる感染拡大防止
ソフトウェアをインストールできない環境の保護

EdgeFire

EdgeIPS

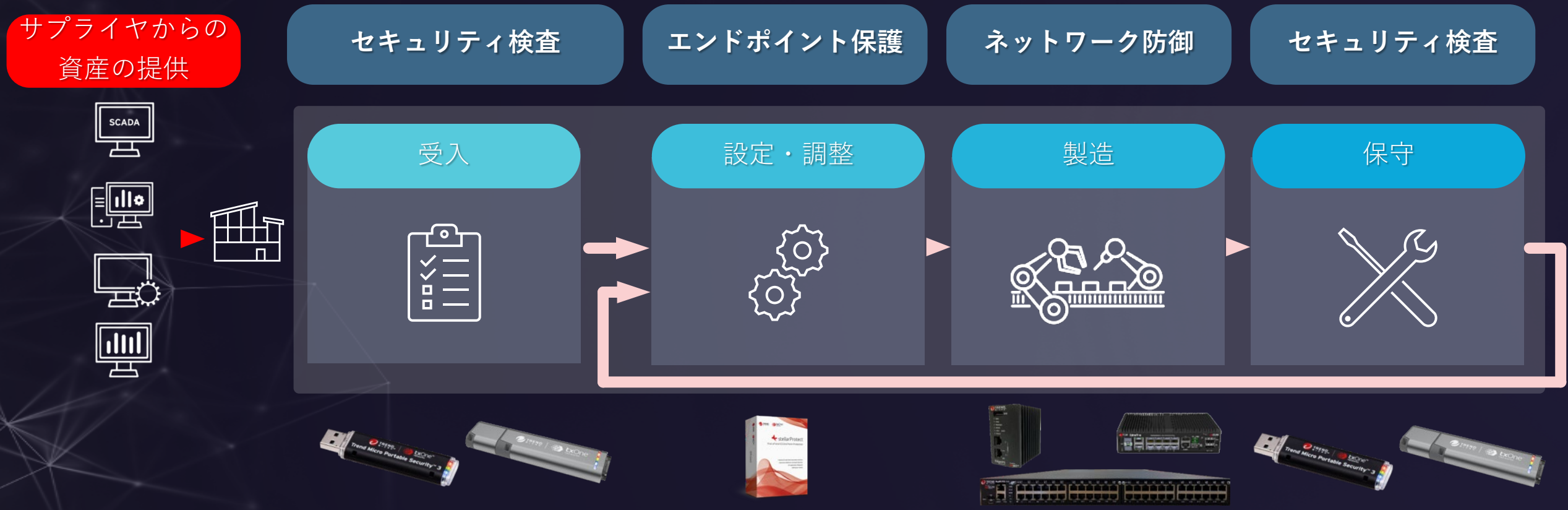
EdgeIPS Pro



仮想パッチ技術

txOne networks

OTの資産ライフサイクル保護 – OT Zero Trust Approach



Never trust, and always verify assets at every stages

資産のすべてのステージで「常に疑い、常に検証」

txOne networks

Thank You

Keep the operation running!