コラボレーション
プラットフォーム資料

「令和２年度中小企業向けサイバーセキュリティ対策支援構築事業」から

自動車サプライチェーンにおけるセキュリティ実態と課題の考察

2021年1月29日

To Be a Good Company

東京海上日動

TOKIO MARINE
NICHIDO

教学　大介　Daisuke Kyogaku

【所属】
東京海上日動火災保険株式会社　企業商品業務部Ｒ＆Ｄチーム
東京海上日動リスクコンサルティング株式会社　チーフコンサルタント

【業務内容】
企業向けのニューリスクに対する新商品開発業務に従事
サイバーセキュリティに関するコンサルティング業務に従事

【プロフィール】
１９９７年　東京海上火災保険株式会社　入社
２００５年　賠償責任保険の商品開発およびアンダーライティング業務に従事

２０１５年　国内損保初「サイバーリスク保険」を開発
２０１９年　サイバーセキュリティ事業を開始
２０２０年　「Tokio Cyber Port」の立上げ

令和2年度「サイバーセキュリティお助け隊事業」について
（東京海上日動リスクコンサルティング株式会社）

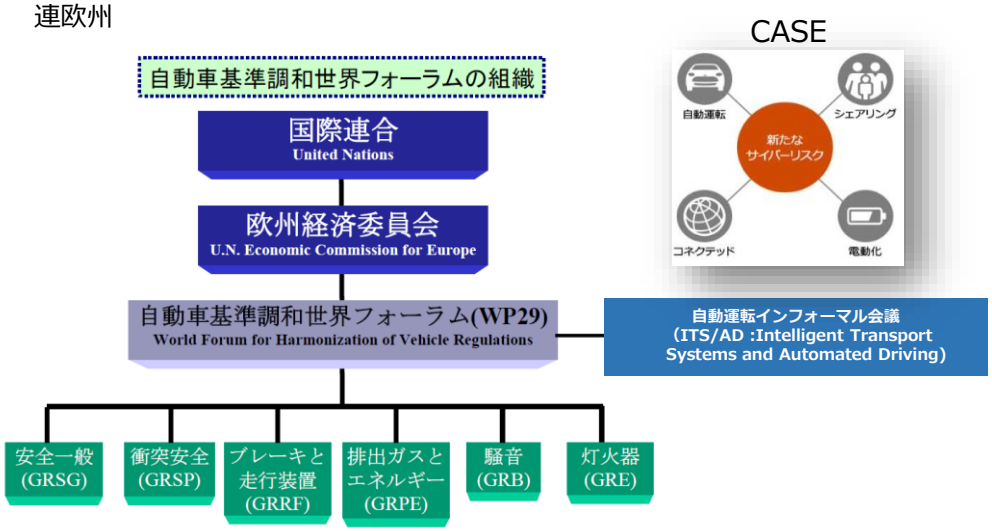
自動車産業を対象としたお助け隊実証事業への参画

国連の自動車基準調和世界フォーラム（WP29）に関連し、今後、日本においても車両の型式認可を受ける際に、国際基準を満たす体制であることを示す必要があり、自動車メーカーだけでなく、サプライヤーも含めたセキュリティ体制構築が急務。

（参考）WP29について　＊自動車業界における外的要因

自動車産業ではサプライヤーの「プロセス認証」がOEMの「型式認証」の条件になる

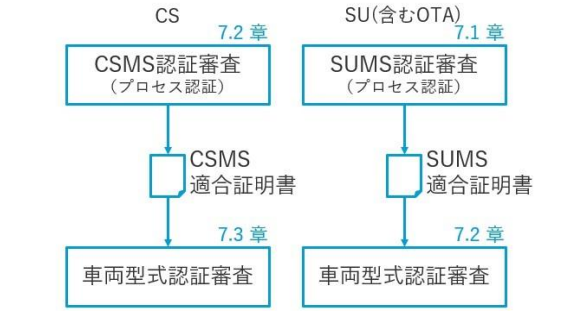
WP29：Working Party 29
「自動車基準調和世界フォーラム
（World Forum for Harmonization of Vehicle Regulations）」の略称
自動車の安全・環境基準の国際調和や相互承認について多国間で審議する、国連欧州

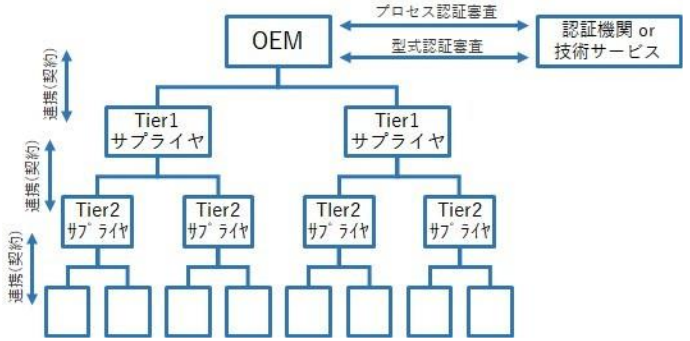


CASE

自動運転インフォーマル会議
(ITS/AD :Intelligent Transport Systems and Automated Driving)

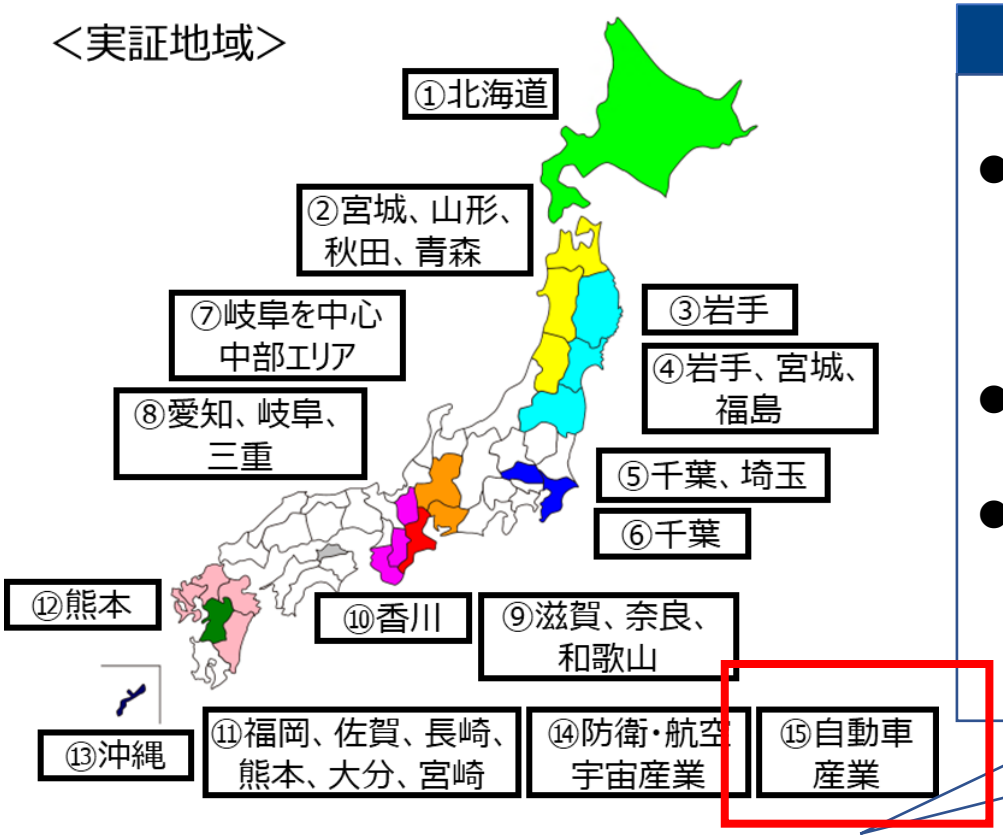
Cyber Security Management System　**Software Update Management System**





自動車産業を対象としたお助け隊実証事業への参画

経済産業省 「令和2年度　サイバーセキュリティお助け隊」実証事業について



お助け隊実証事業の概要

- 経済産業省とIPAが、中小企業のサイバーセキュリティ対策の強化を目的として、昨年度、全国8地域で8事業者が実証実験を実施。
- 今年度は、更に規模を拡大し15事業者が採択済。
- 本座組では、自動車産業におけるサプライチェーンに焦点を当て、事業を推進する見込み（詳細は次頁）

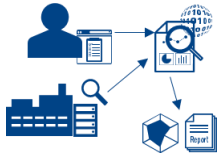
中小企業サプライヤーの実態について
（サイバーセキュリティお助け隊事業の結果）

実証内容

本実証では、セキュリティ対策実行サイクルの6項目中4項目を検証(※一部実施の場合有)

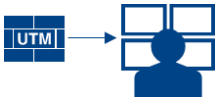
①問診＋診断：

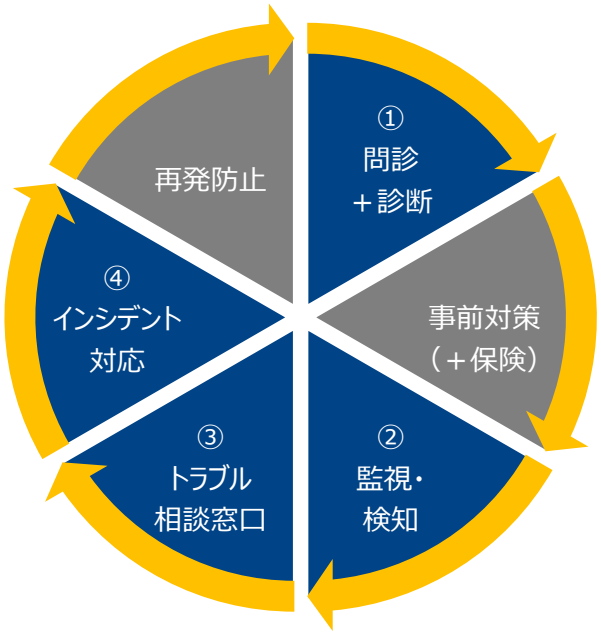
・Web問診により担当者のセキュリティ意識を調査
・外部/内部（端末）診断でシステム環境のセキュリティ対策状況を可視化
・マルウェア対策診断による対策の実施有無の把握



②監視・検知：

・不正通信監視機器の設置によるサイバー攻撃の実態を把握





セキュリティ対策実行サイクル

③トラブル相談窓口：

・何かおかしいと違和感を感じたら、電話もしくはメールで
気軽に相談できる窓口を設置

④インシデント対応：

・トラブル相談や不正通信監視中に重篤な問題を
検出した場合にリモートサポートで解決を実施
※リモートによる解決が困難と判断した場合は駆け付け対応

【実証スコープ外】事前対策(＋保険)：

・問診＋診断の結果、到達すべき最低限のセキュリティ対策レベルを
満たしていない企業に対して、モデル化された事前対策の実施及び
リスク回避手段としての保険を含めた事前対策サービスを今後検討

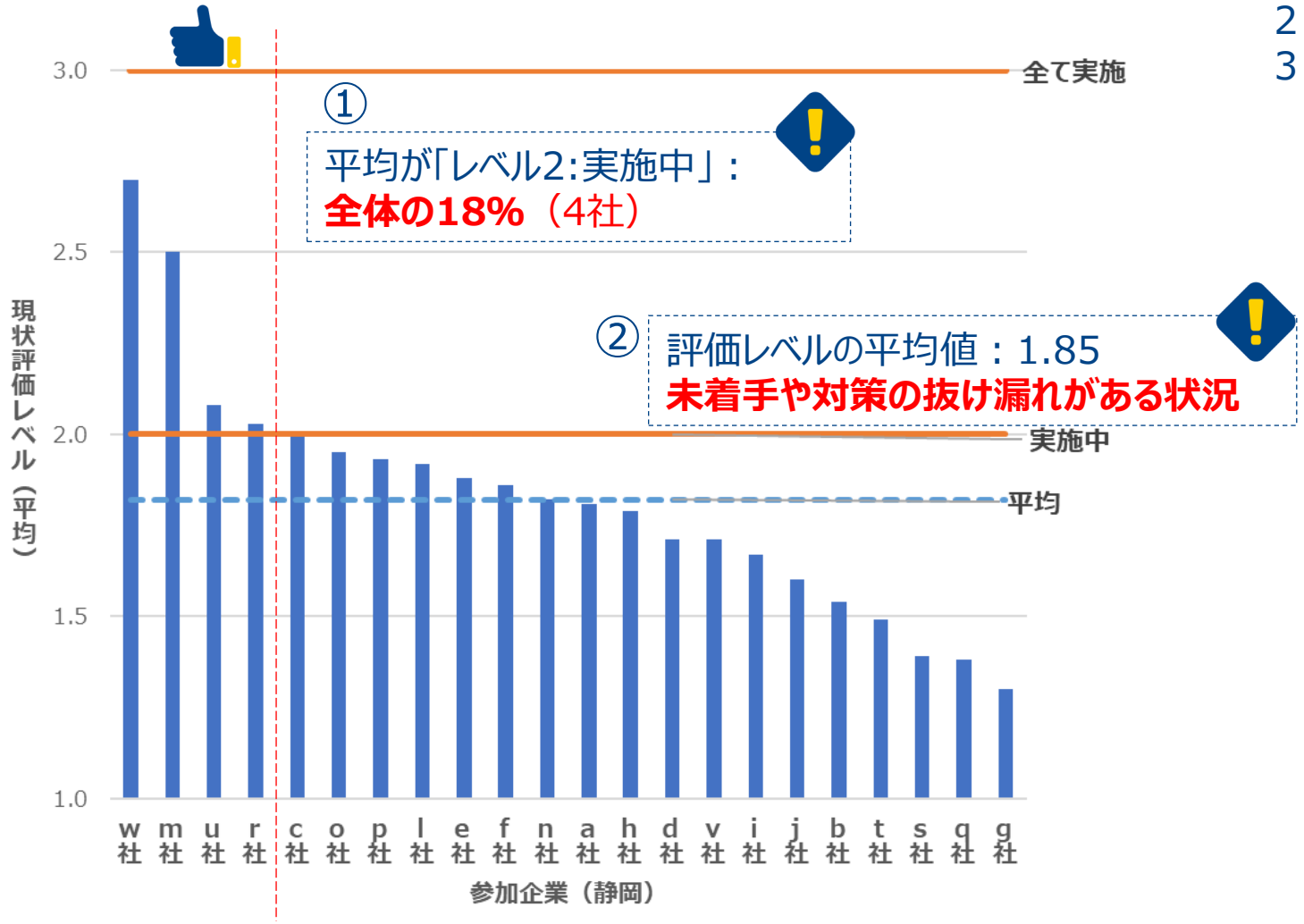
【実証スコープ外】再発防止：

・インシデント対応後に対策相談や専門家派遣等の再発防止に必要な
サービスを今後検討

Web問診の回答結果（企業別）

企業別の評価レベル（全項目平均）

【評価レベル】
1 ：未実施
2 ：実施中
3 ：実施済

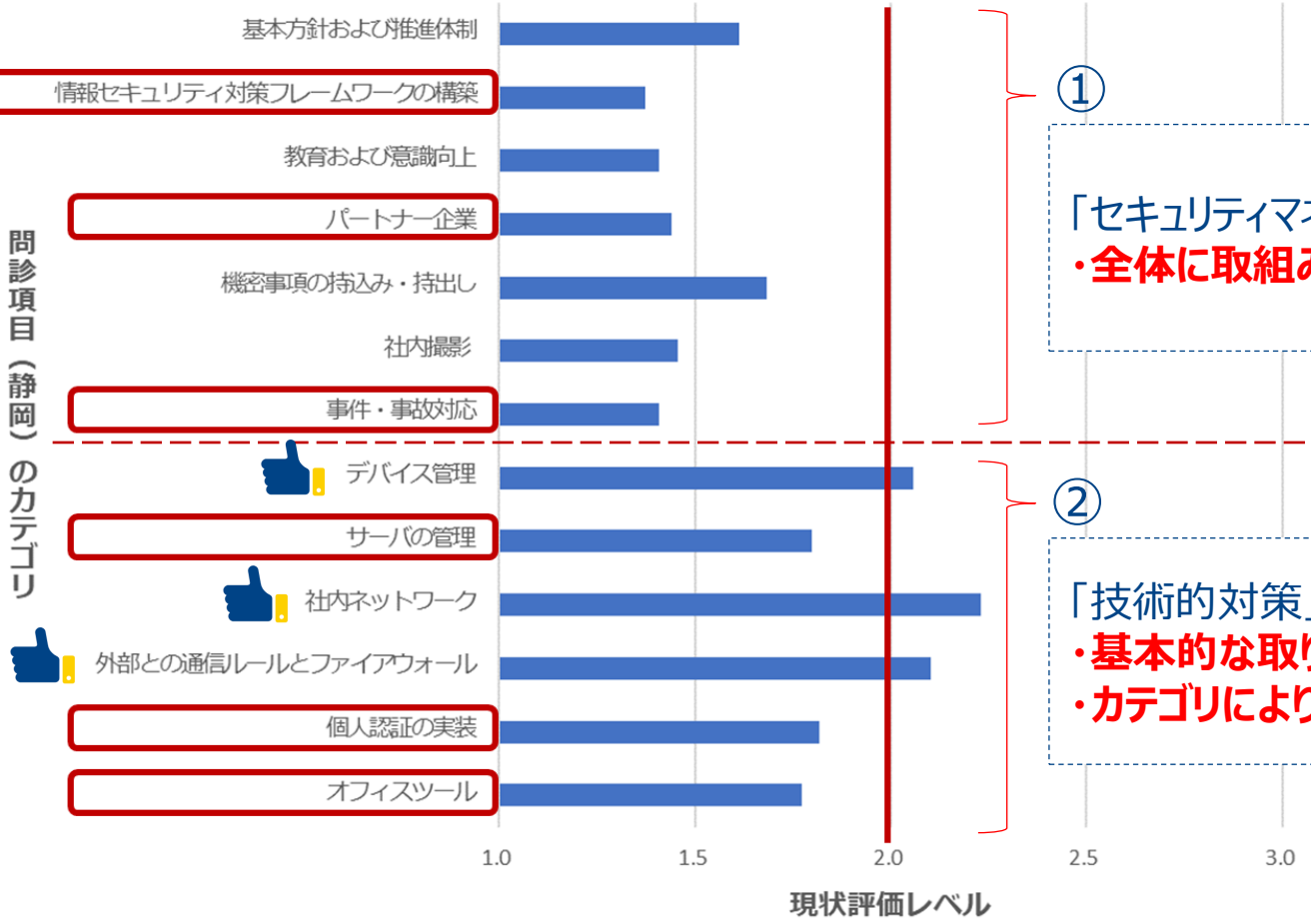


Web問診の回答結果（カテゴリ別）

カテゴリ別の評価レベル（平均）

「レベル2:実施中」に達しているのは**3カテゴリ**

【評価レベル】
1 ：未実施
2 ：実施中
3 ：実施済



①

「セキュリティマネジメント」の観点：
・全体に取組みに遅れがある

②

「技術的対策」の観点：
・基本的な取り組みが進みつつある。
・カテゴリにより差がある。

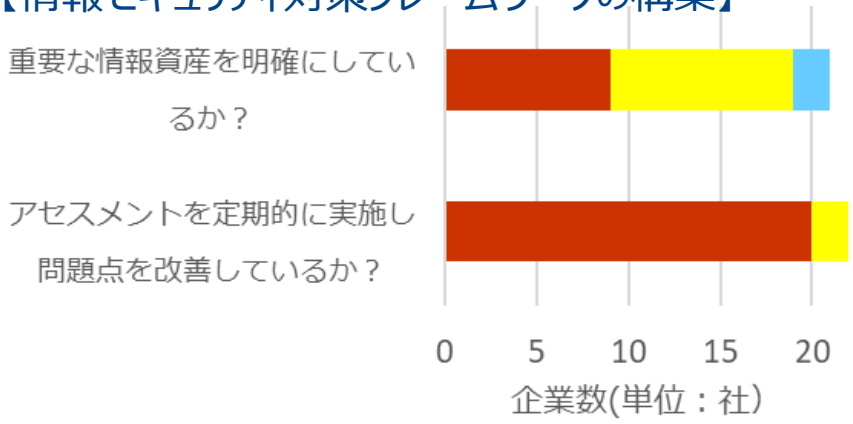
Web問診の回答結果（項目別） 1/4

「セキュリティマネジメント」の観点で
評価レベルが低い診断項目（抜粋）

傾向・想定される問題点

■ 1.未実施 ■ 2.実施中 ■ 3.実施済

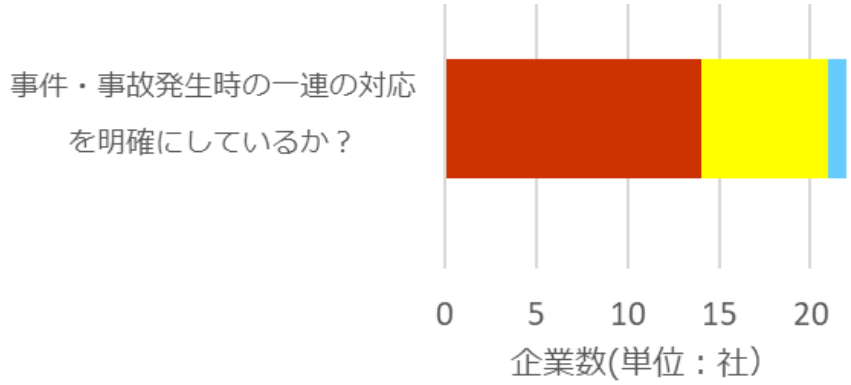
【情報セキュリティ対策フレームワークの構築】



情報資産の定義等の初期の取り組みは
一定程度進んでいる

継続的な改善まではできていない

【事件・事故対応】

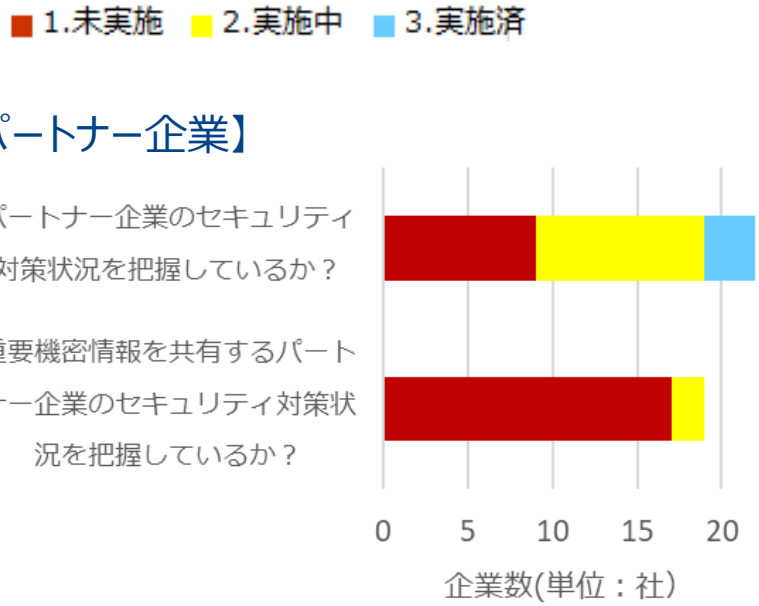


インシデント発生時の一次連絡先が
なんとなく決まっている状況
明確なルールや対応手順が決まっていない

Web問診の回答結果（項目別） 2/4

「セキュリティマネジメント」の観点で
評価レベルが低い診断項目（抜粋）

傾向・想定される問題点



【パートナー企業】

取引先（自社にとってのサプライヤー）
のセキュリティ対応は手が回っていない

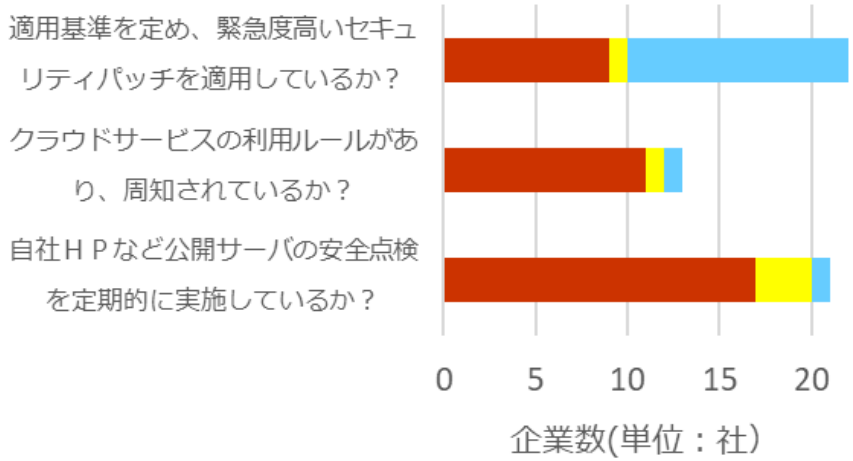
Web問診の回答結果（項目別） 3/4

「技術的対策」の観点で
評価レベルが低い診断項目（抜粋）

傾向・想定される問題点

■ 1.未実施 ■ 2.実施中 ■ 3.実施済

【サーバの管理】

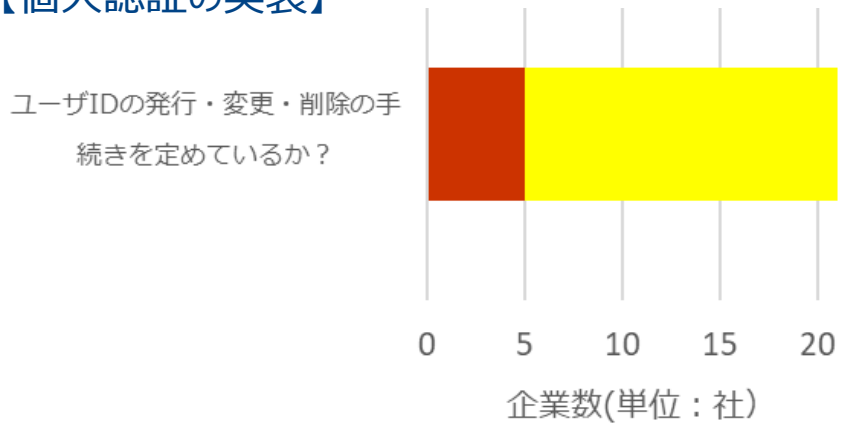


セキュリティパッチの適用を実施は一定割合存在。

適用時の動作保証ができない等の理由で**パッチ適用していない**場合も存在。

HP等の公開サーバに関する**セキュリティチェックが不十分**

【個人認証の実装】



退職者のアカウントの削除等、
「登録→アクセス権変更→削除、棚卸」
といった**一連の手続きが未整備**

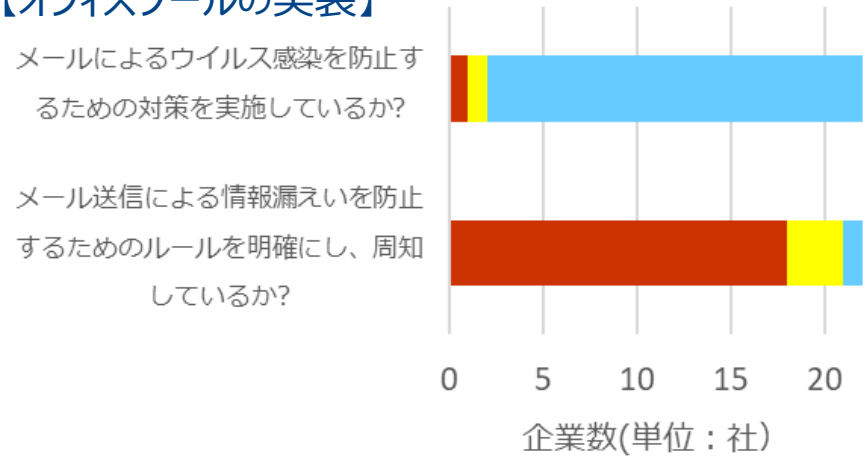
Web問診の回答結果（項目別） 4/4

「技術的対策」の観点で
評価レベルが低い診断項目（抜粋）

傾向・想定される問題点

■ 1.未実施 ■ 2.実施中 ■ 3.実施済

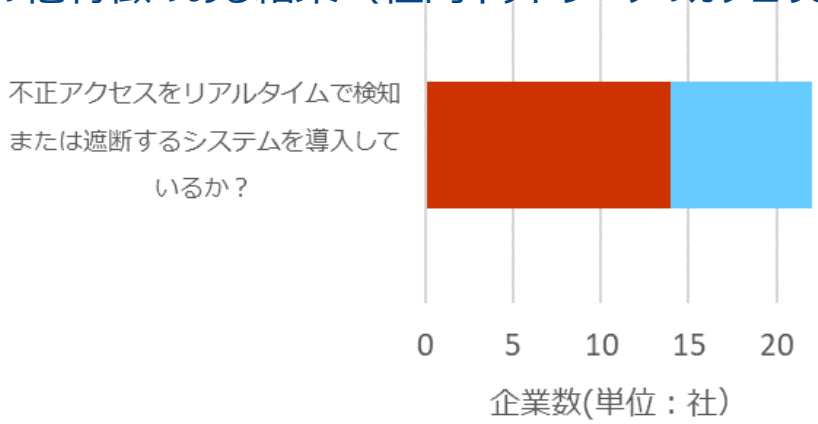
【オフィスツールの実装】



ウイルス対策ソフト導入等の基本的な対策は実施済。
標的型攻撃等の**高度な攻撃への対応が課題**となる企業も一部存在。

メール誤送信による情報漏洩を防止するための**ルールがなく**、社員に徹底が不十分。

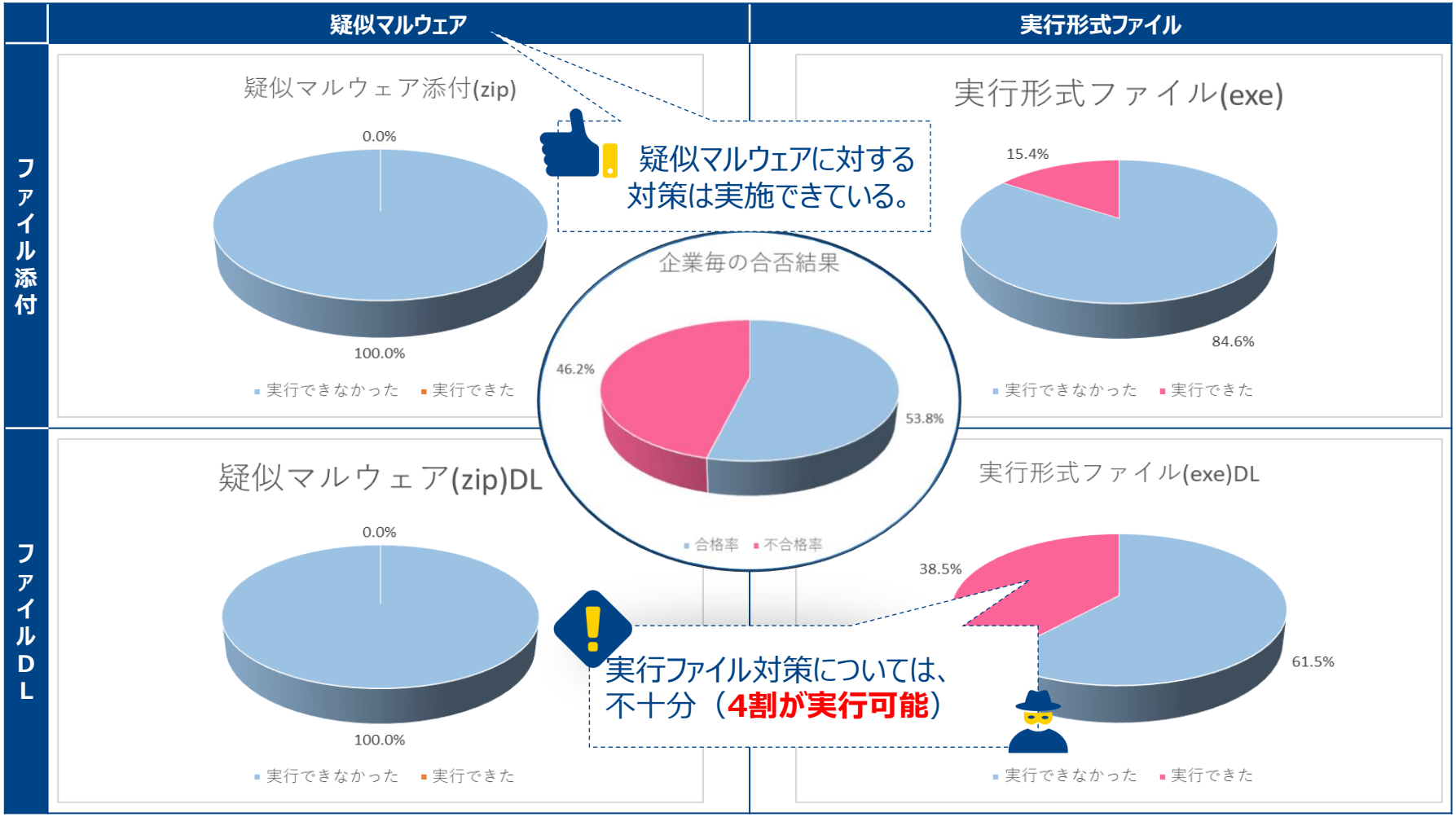
その他特徴のある結果（社内ネットワークのカテゴリより）



・対策が2極化
・サイバー攻撃等で社内ネットワークへ侵入された場合に検知/遮断する仕組みがない。**攻撃に気づけない恐れがある。**

メール・ファイルDL診断結果

実施結果と傾向

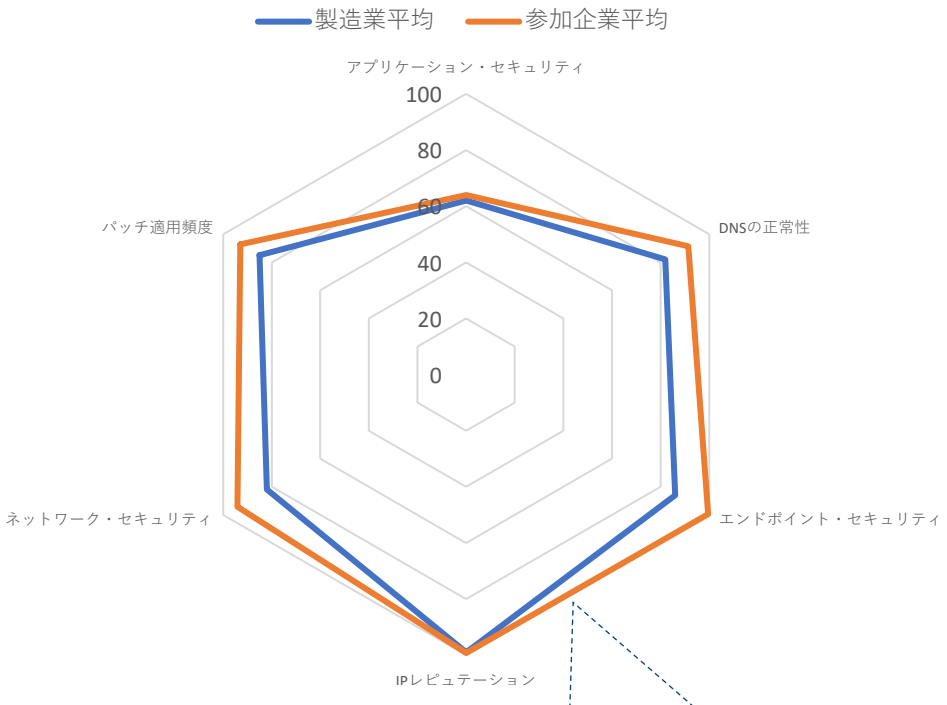


外部診断結果

実施結果

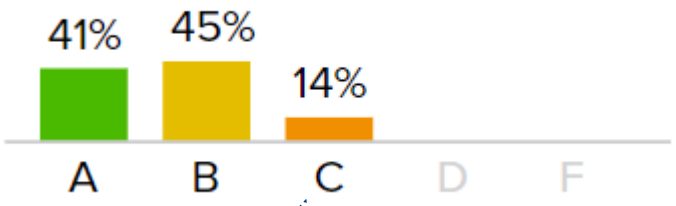
①サプライチェーン(SC)内のセキュリティ管理レベルの状況

1）製造業と参加企業全体のセキュリティ管理レベルの各分類と平均値



製造業全体の平均と比べ、参加企業平均の**セキュリティ管理レベルは高い**

2）参加企業総合判定ランクの分布



参加企業の14%(3社)がCランク
サプライチェーン内のリスク要素となる可能性がある

外部診断結果

実施結果

3）参加企業各社のセキュリティ管理レベル傾向

参加企業	a社	b社	c社	d社	e社	f社	g社	h社	i社	j社	k社	l社	m社	o社	p社	q社	r社	s社	t社	u社	v社	w社
トータルランク	A	C	A	B	B	B	B	C	B	B	B	B	A	A	A	B	A	A	A	B	C	B
セキュリティスコア	95	75	93	85	82	87	84	74	89	89	82	89	96	91	94	85	92	93	92	89	72	86
アプリケーション・セキュリティ	B	F	A	D	F	D	F	F	D	D	B	D	B	C	C	F	C	C	C	C	F	F
キュービット・スコア	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
DNSの正常性	A	A	A	A	A	A	A	A	A	A	B	A	A	A	A	A	A	A	A	A	A	A
エンドポイント・セキュリティ	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
ハッカーチャッター	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
IPレピュテーション	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
ネットワーク・セキュリティ	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
漏洩された情報	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
パッチ適用頻度	A	A	A	B	A	A	A	A	A	A	F	B	A	A	A	A	A	A	A	A	F	A
ソーシャル・エンジニアリング	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A

・全体として**アプリケーション・セキュリティが7社で”Fランク”**
→Webサーバのセキュリティ設定見直しと対策の検討が急務。

・2社で脆弱性パッチの適用レベルが”Fランク”
→サーバの運用状況の見直しが必要。

1. 実証結果報告
1.3 外部診断

実施結果

②インターネット上で悪用される可能性の高いアプリケーションポートの公開

c社、d社、h社の3社

データベースの標準ポートがインターネットからアクセス可能な状態

③インターネット上にシャドーITの可能性のあるシステムがあるか。

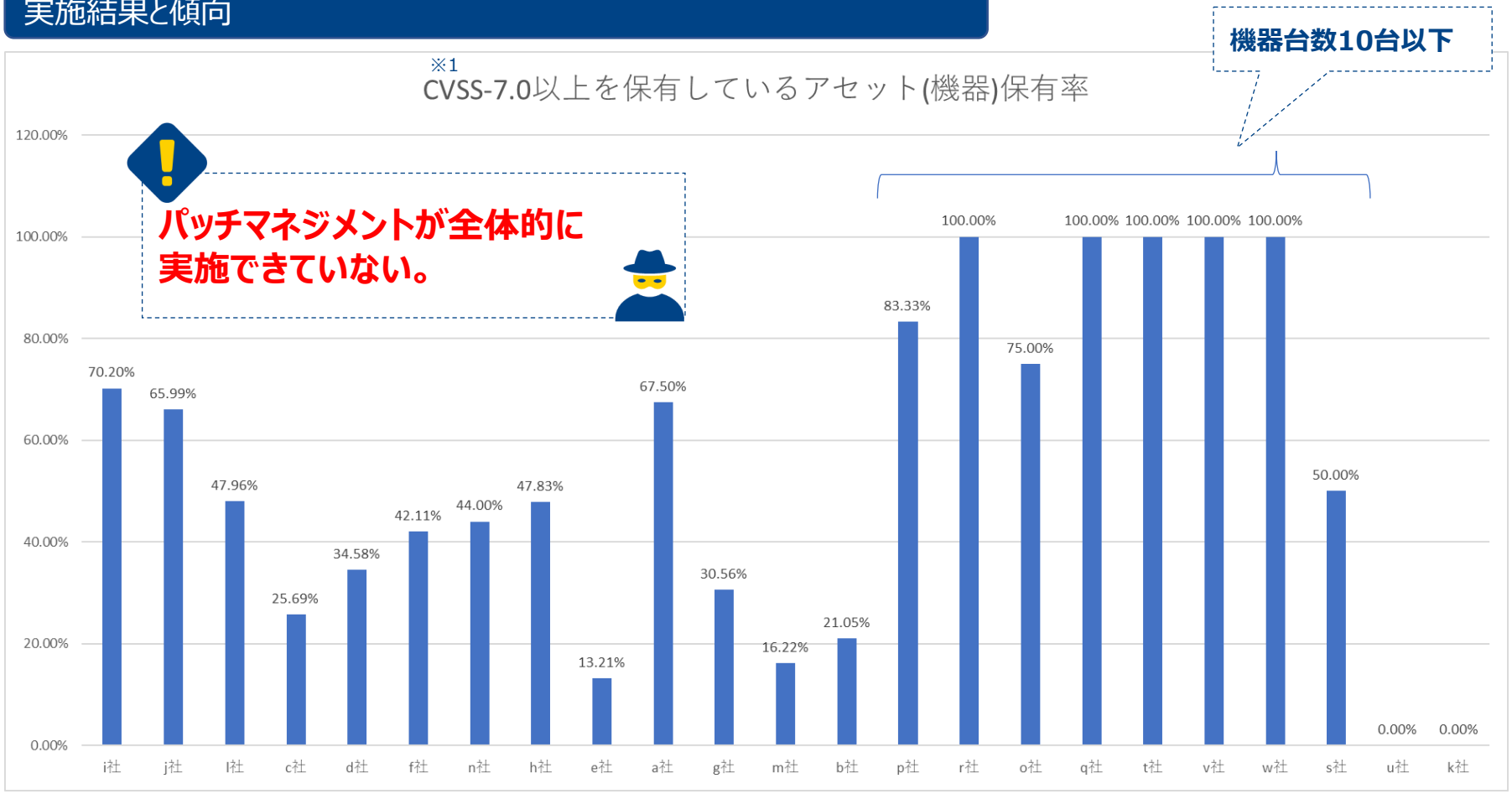
SSL証明書の期限が切れたまま放置されているサーバは無し

④マルウェア通信の可能性の高いトラフィックが生じているか。

対象企業の中で、マルウェア通信とみられるトラフィックの形跡は無し

内部診断／端末診断結果

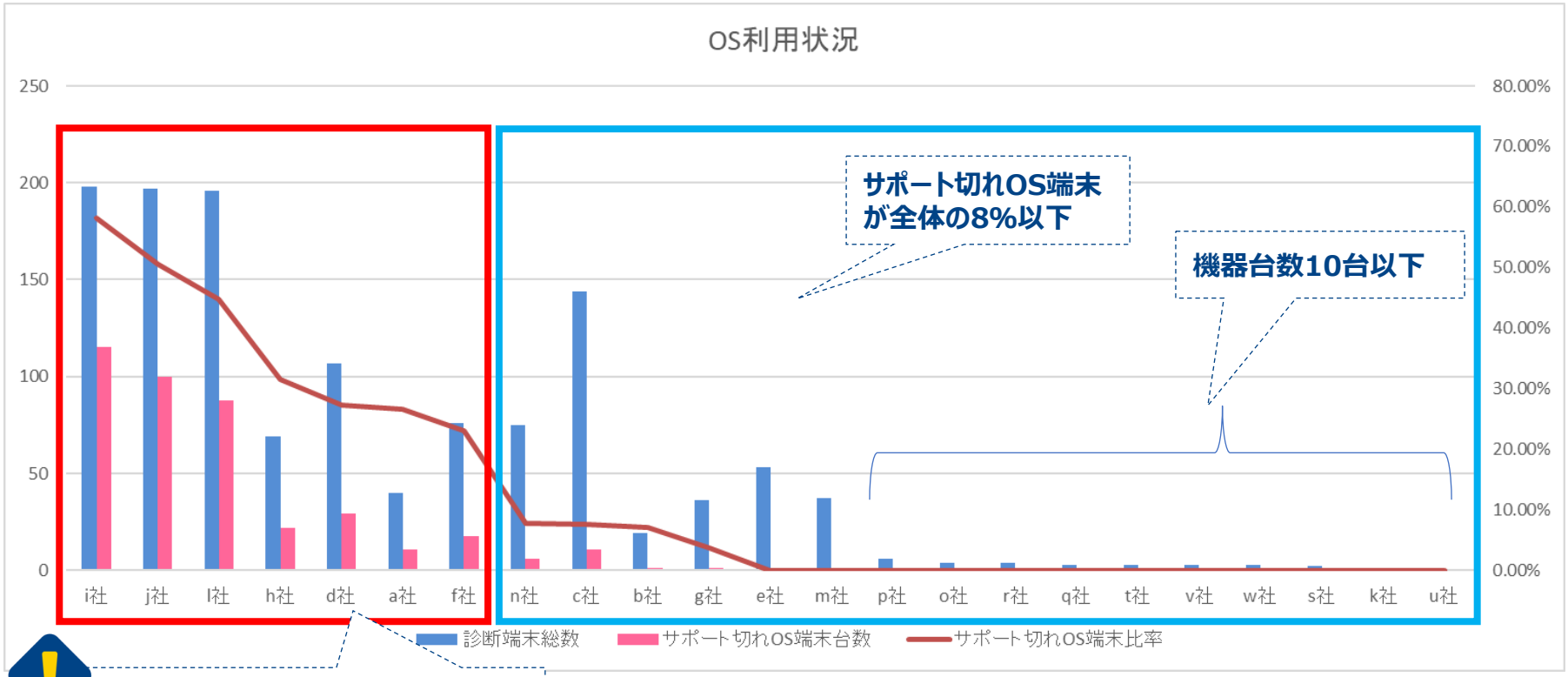
実施結果と傾向



※1　CVSS(Common Vulnerability Scoring System：共通脆弱性評価システム)とは、IT機器の脆弱性(攻撃されやすさ)を示す指標で、脆弱性の危険度を点数(0.0～10.0)で表します。10.0は最も危険度が高い脆弱性を示し、一般に7.0以上の危険度を持つ脆弱性は優先度が高く、対応することが推奨されています。

内部診断／端末診断結果

実施結果と傾向

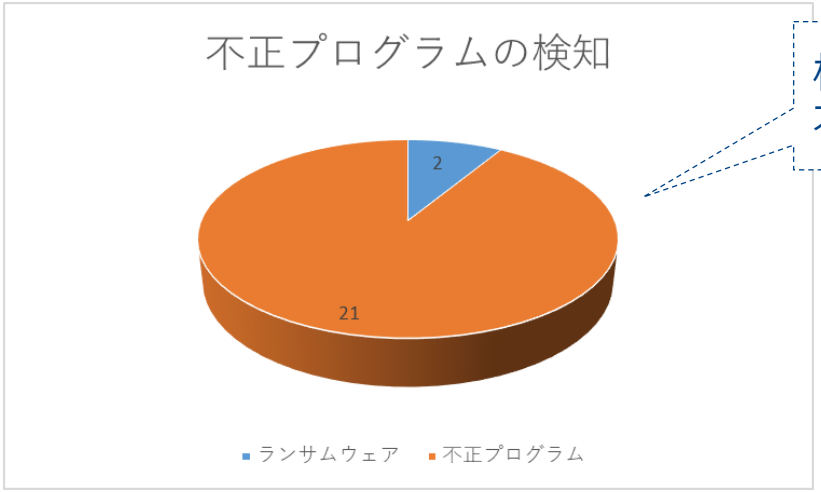


サポート切れOSの端末が
約60～20%を占めている

サポート切れ端末が「存在する企業」と
「存在しない企業」に**2極化**

不正通信モニタリング結果

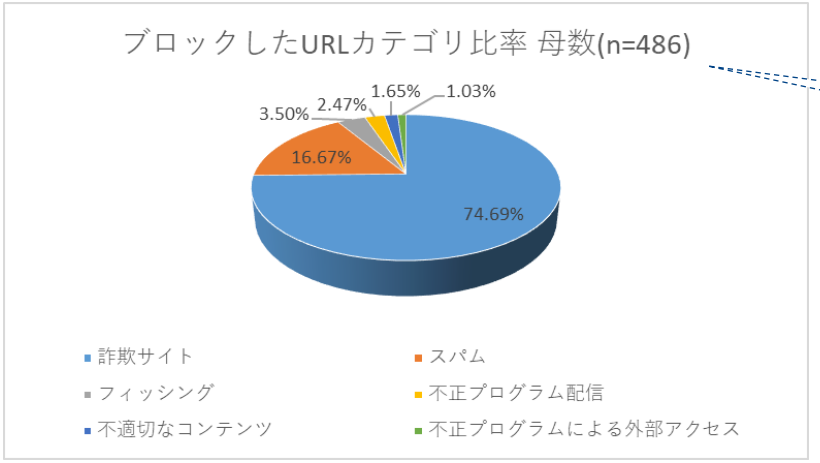
実施結果



検知/ブロックした
不正プログラム等は**23件**

特定企業において
検知が多かった

Web広告等の業務に関係ない
アクセスのブロック数　11,097,615 件



特に不審なサイトへの
アクセスブロック数は**486件**

※1
詐欺サイトへ誘導される
ケースが多かった

※1　詐欺サイト：個人または団体から信用を得た上で金銭などをだまし取ろうとするWebサイト

不正通信モニタリング結果

モニタリング結果からわかること

即座に緊急対応を伴うインシデント発生はゼロ件

だが、この短期間にも関わらず

「不正プログラム」や「詐欺サイト/スパムサイトへの誘導」等

ウイルス感染に繋がる可能性のある

サイバー攻撃が検出されている。（UTMが防御した。）

つまり、

自動車産業を支える**サプライヤーは、サイバー攻撃の標的となっている**

ことが、言える。

中小企業サプライヤーの課題について

中小企業企業ご担当者の悩み

中小企業サプライヤーの課題について

サイバーセキュリティ対策への取り組みに対する取引先からの要求は始まりつつあるものの、十分な対策が実施できていない傾向が見受けられた。

主な課題

【セキュリティ・マネジメントの側面】

- セキュリティに対する全社的な**課題認識の不足**
- セキュリティ対策における**人的リソースの不足**
- セキュリティ対策への**投資コストの不足**
- セキュリティ標準として**何をどこまで実施すべきか不明確**（今回のアセスメントは有益だったという声が多数あり）
- 自社及び取引先に対する**セキュリティ対策状況の把握**

【技術的対策の側面】

- サイバー攻撃への**一歩踏み込んだ対策**が不十分
  - 安全なWebサイト運用
  - 標的型メールや不正サイトへの誘導に対する対策
  - 脆弱な端末へのパッチ適用等
  - 工場ネットワークの分離
  - 不正アクセスの検知/遮断や見守り

解決の方向性

- 経営者向け**啓発活動**
- セキュリティ担当者の**相談窓口の整備**（気軽に利用できること）
- サプライチェーンのOEM（または、団体や組合）主導による**セキュリティ標準の提示**、ガイドラインや各種ドキュメント標準**ひな形の公開**及び各企業への**適用支援**
- 社員に対するセキュリティ**教育**コンテンツの提供及びIT運用者に対する必要スキルの**研修**メニューの提供
- 自社及び取引先含む**同業の対策状況の可視化**（マネジメントの観点でもわかること）
- **経済的**に利用可能な**対策サービス**の提供
- サイバーリスク保険の活用による、**想定外のセキュリティリスク**に対する**移転**

今後必要なサービス検討について（案）

今後に向けた取り組みについて

前頁の総評にも記載しました今回の実証を通じて把握できた課題に対する解決の方向性をとして、以下の取り組みが効果的ではないかと**対策案**を検討した。

対策案１：規定や資産管理関連の策定支援ツールおよび社員教育コンテンツの提供

対策案２：セキュリティ対策レベルの把握および対策に向けたセキュリティ診断の定期的な実施

対策案３：セキュリティ対策に向けた事業者ニーズに合った対策サービスメニューの提供

対策案４：セキュリティに関して気軽に相談できる窓口の提供(地場のSier等との連携含む)

対策案５：見守り監視ソリューションに紐付くサイバーリスク保険の提供

※提供形態も**1社1社の個別対応ではなく、団体・組合等と連携**しながら進めることで、全体の底上げならびに、経済的なサービスとして実現可能なアイデアを検討したい。

「Tokio Cyber Port」のご活用のおすすめ

「Tokio Cyber Port」
アクセスはこちらから

東京海上日動 Tokio Cyber Port 検索

https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/

TOKIO MARINE NICHIDO

さいごに

ご清聴ありがとうございました。