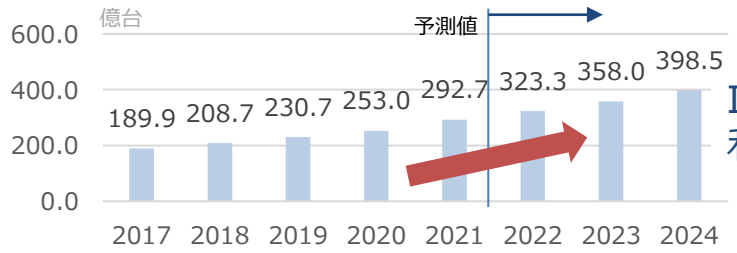
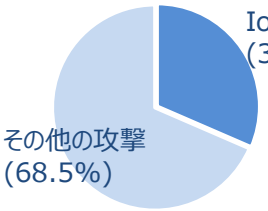
IoT機器の利用拡大に伴い増加するリスクと、その経営への影響

ネットワークに接続される機器(IoT機器)は増加傾向、IoT機器を狙った攻撃は多い



IoT機器の
利用数は増加

世界のIoT機器数の推移及び予測(※1)



ダークネットにおける年間観測パケット数の割合(※2)

不審な通信のうち
約1/3はIoT機器を狙った攻撃

[※1] 出所:総務省「情報通信白書令和4年版 データ集」(3章関連データ)
[※2] 出所:NICT「NICTER観測レポート2022」調査を除く攻撃パケットのうち、23/TCP、22/TCP、5555/TCP、81/TCPへのパケットを集計。

IoTにおけるセキュリティインシデントが経営に大きな影響を及ぼす可能性が高まっている

操業停止や逸失利益の発生を含む事業への直接的な影響

半導体製造工場の制御装置に対する攻撃によって、**3日間の操業停止、営業機会損失が発生(売上高(四半期)の3%損失)**[台湾:2018]

石油化学工場の安全計装システムを対象とした攻撃による**操業停止。プラント爆発のおそれ**[サウジアラビア:2017]

脆弱性対応や損害賠償を含む追加費用の発生

脆弱性発見による自動車140万台のリコールの発生。脆弱性等の対応で、**2億9900万ユーロ(約394億円)の赤字を計上**(四半期の最終損益) [米国:2015]

評判の低下等より生じる競合優位性の低下

高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下** [オーストリア: 2017]

[参考] 各公開情報を基に作成

IoT-SSF(※3)活用によるリスクマネジメントのメリット

[※3] IoT-SSF:IoTセキュリティ・セーフティ・フレームワーク

セキュリティリスクへの対処には、
組織全体や関係者の現状を把握した上でリスクの抽出とそれらを考慮した対策が必要

IoT-SSFを活用することで、包括的にIoTにおけるリスクの抽出とそのリスクへの対策が可能

特徴1

関係者と協力することで
抜け漏れなく対策が可能

特徴2

けがや事業への被害を
考慮しつつ包括的に
IoTのリスクを特定可能

特徴3

既存の
製品安全分野の検討結果と
調整しつつ対策が可能

- IoTに関係するシステム・関係者の全体を把握できていない
- 攻撃を受けたときに想定している影響範囲に不安がある
- 効果的な対策や投資範囲がわからない

セキュリティリスクへの対処に
あたって想定される悩み(例)

【適用実証に参加された事業者からお寄せいただいたお声】

- ◆ 組織外部の関係者におけるリスクを確認できた点にメリットを感じた。(家庭用機器製造事業者)
- ◆ 関係者間で共通の認識を持った上で、事業リスクを考慮しつつ脅威を整理することができた。(住宅メーカ/住宅設備製造販売事業者)
- ◆ 製品安全分野の技術者とセキュリティ分野の技術者間で認識をすり合わせつつ、IoT-SSFを適用できた。(制御機器メーカ)