ALways Security OK
ALSOK

制御システムセキュリティカンファレンス2017

制御システムのサイバー＆物理セキュリティ

2017年2月21日

綜合警備保障株式会社
佐藤　将史

アジェンダ

1 会社紹介

2 物理空間の脅威になったサイバー攻撃

3 情報セキュリティと物理セキュリティの現状

4 融合空間のセキュリティにおける「真の多層防御」とは？

5 まとめ

1 会社紹介

2 物理空間の脅威になったサイバー攻撃

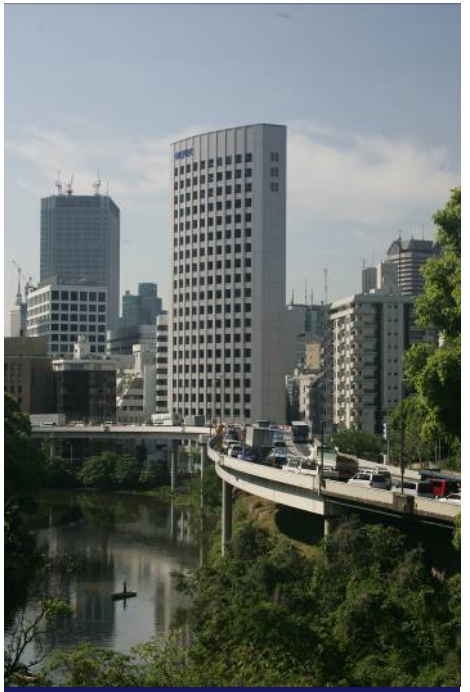
3 情報セキュリティと物理セキュリティの現状

4 融合空間のセキュリティ「真の多層防御」とは?

5 まとめ

会社紹介

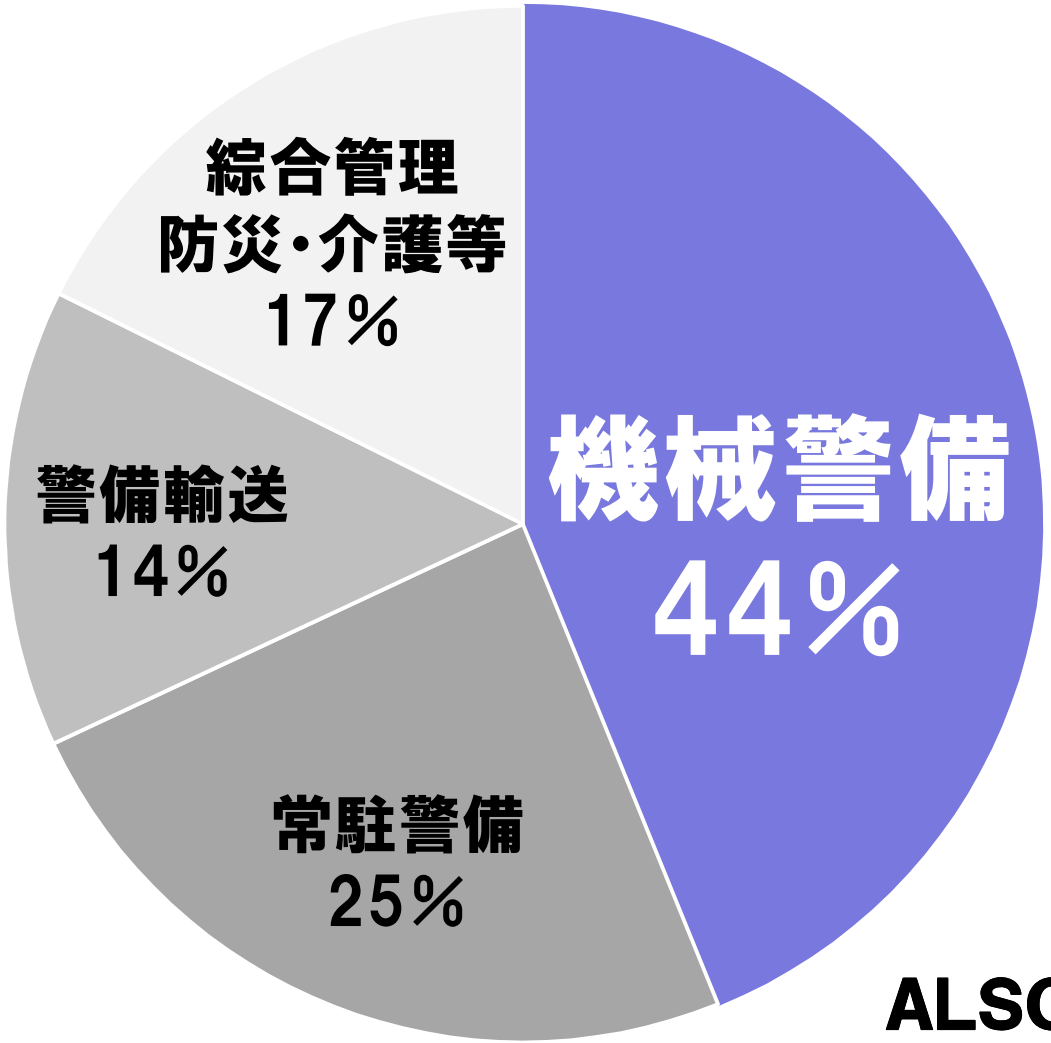
設　立	1965年7月16日
資本金	186億7,501万1,600円
売上高	3,818億円(連結)
経常利益	306億円(連結)
社員数	31,446名(連結)
事業拠点	10地域本部／64支社／39支店／247営業所
グループ会社	79社
海外拠点	タイ、ミャンマー、ベトナム、上海、マレーシア、 インドネシア、インド



本社ビル(赤坂)

2016年3月31日現在

ALSOKの業務内容



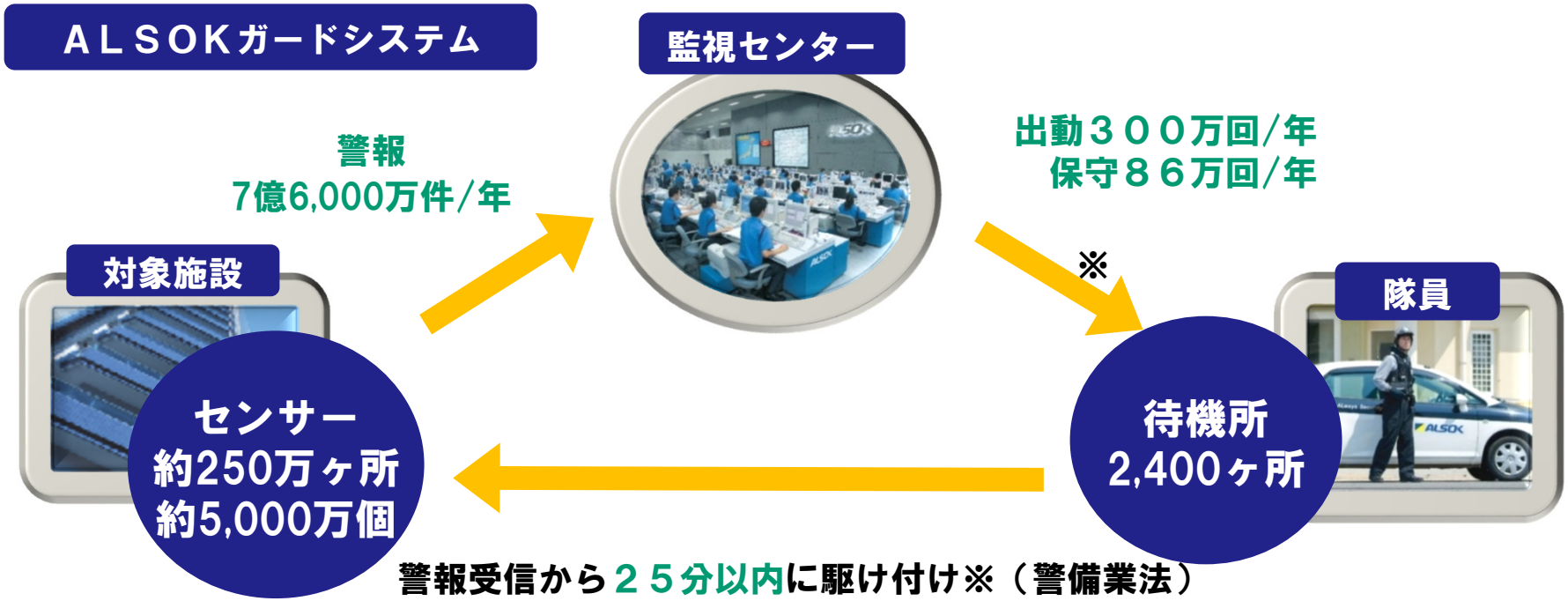
ALSOKの売上構成

機械警備

- 法人向けセキュリティシステム
- ホームセキュリティ
- 遠隔画像監視

機械警備とは

■ 機械警備は警備員を常駐配置せず異常時に駆け付ける仕組み。
■ 「モノ」と「情報」と「人」の高度な連携により成立。
■ ＩＣＴ利用の高度化がサービス品質の向上に直結。

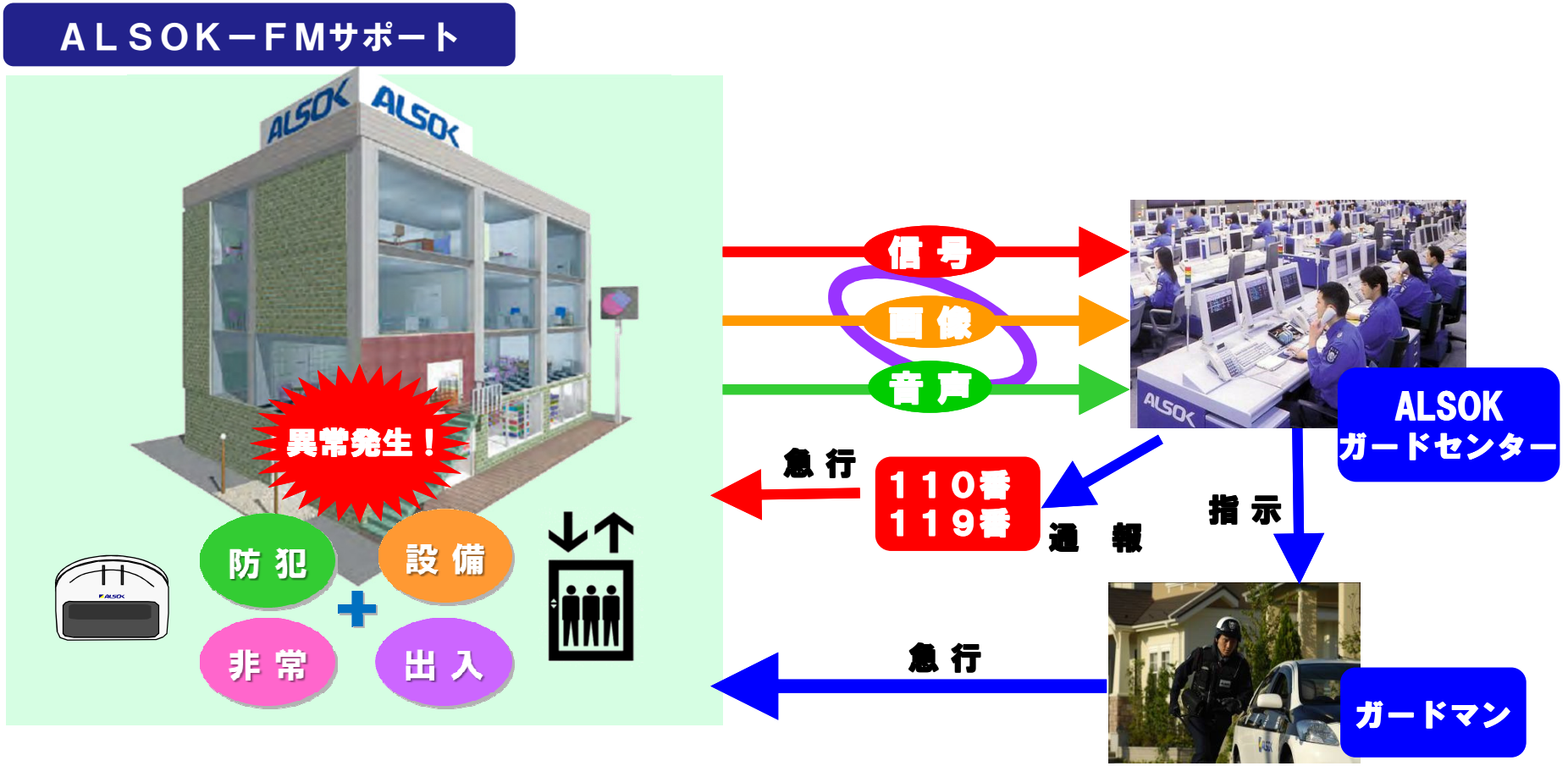


警報受信から２５分以内に駆け付け※（警備業法）

※お客様の施設に最も近い隊員をGPS情報により特定しタフスマホに直行指示

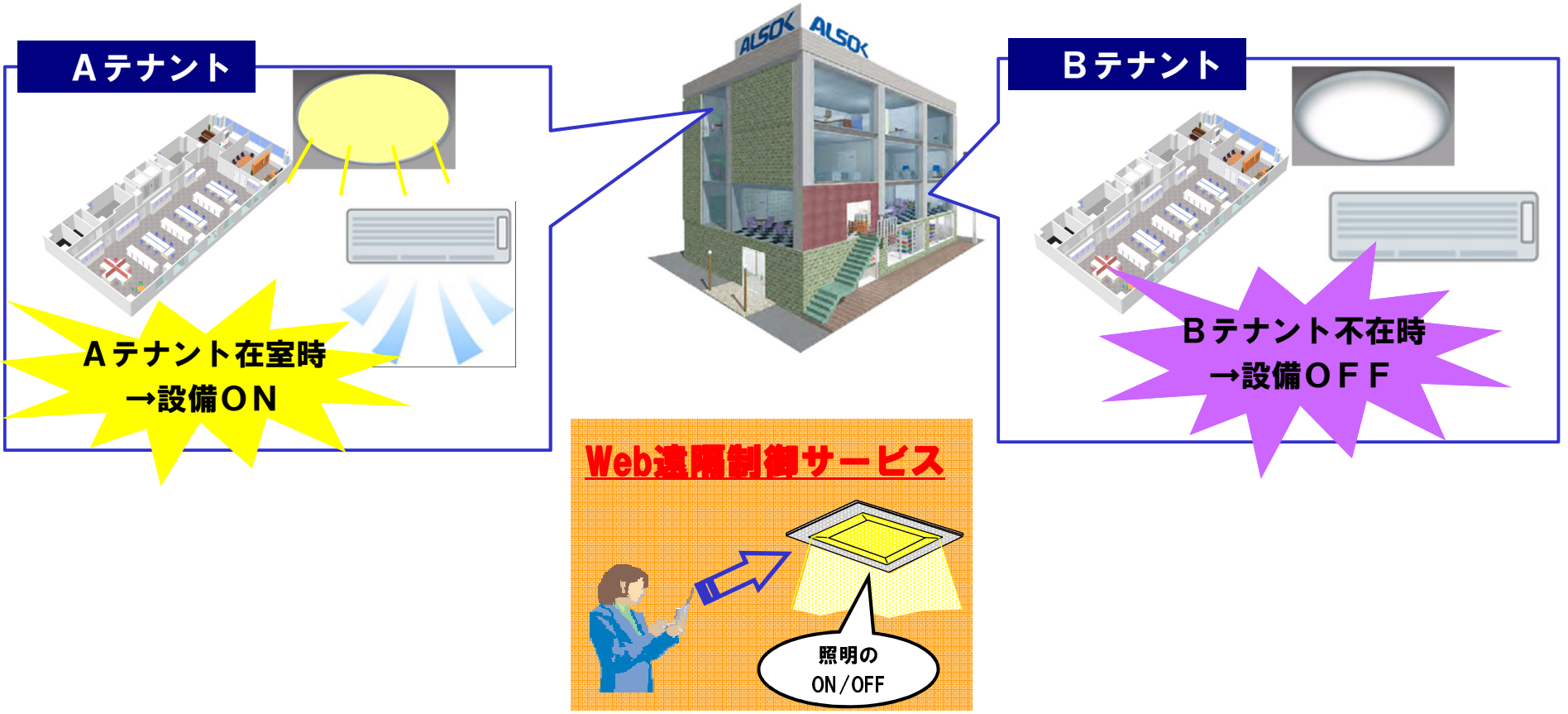
ＡＬＳＯＫにおける設備監視への取組み

- 従来、防災センターに常駐する警備員が施設の防犯、出入管理、設備制御を集中管理するサービスを提供してきた。
- 現在は警備と設備の統合オンライン監視サービスに発展。



施設の設備制御

■ テナント毎に設備を制御。
（スケジュール・警備連動による自動制御も可能）
■ 制御対象は、照明・空調・シャッター・電気錠等。
■ 管理者がＷｅｂ経由で設備の状態確認や遠隔操作も可能。



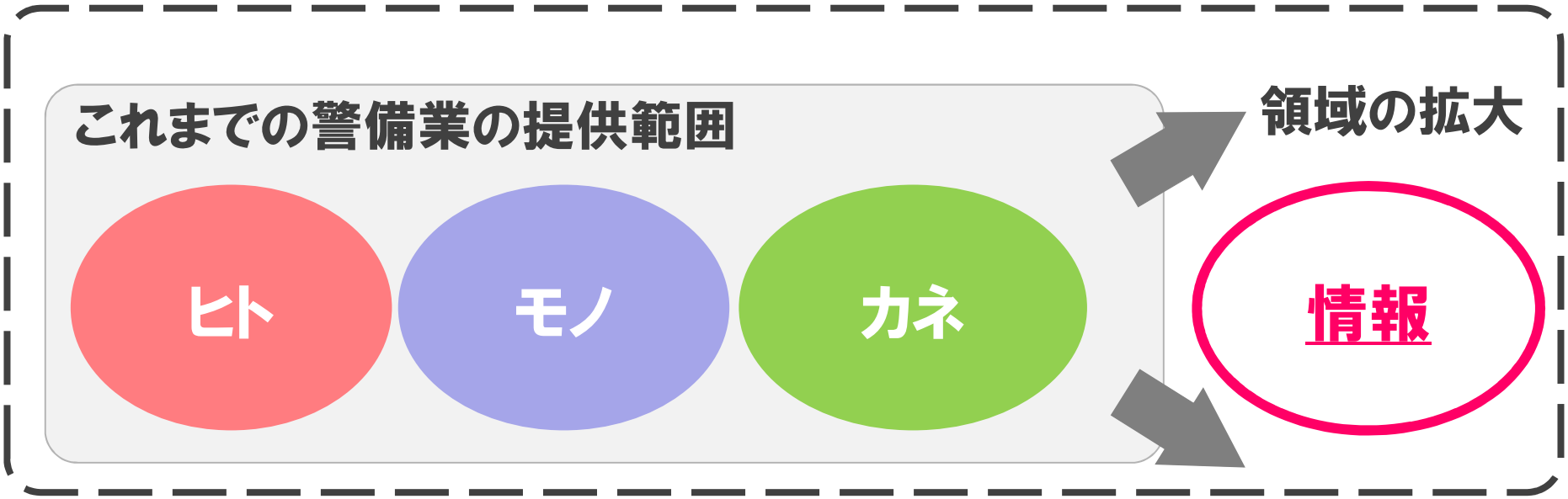
ATMコーナーの制御

■ 防犯に加えて資金管理も含めたＡＴＭ運用を一括で提供。

■ 日々の開閉店は警備会社の装置が自動制御している。

拡大する警備対象

■ インターネットの普及に伴い、警備対象は「ヒト・モノ・カネ」に加えて「情報」にも拡大。



警備業の守るべき対象は“情報”にも拡大

1 会社紹介

2 物理空間の脅威になったサイバー攻撃

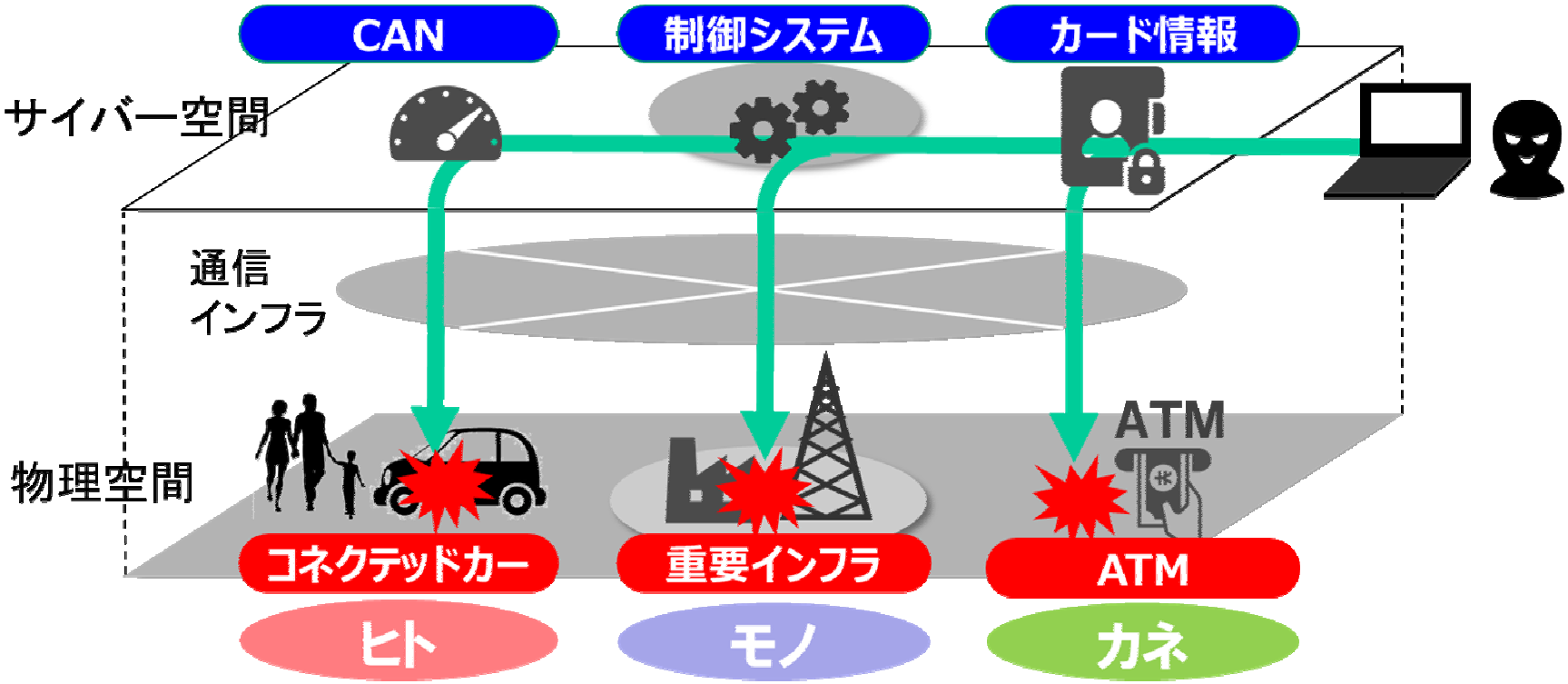
3 情報セキュリティと物理セキュリティの現状

4 融合空間のセキュリティ「真の多層防御」とは？

5 まとめ

物理空間の脅威と一体化するサイバー攻撃

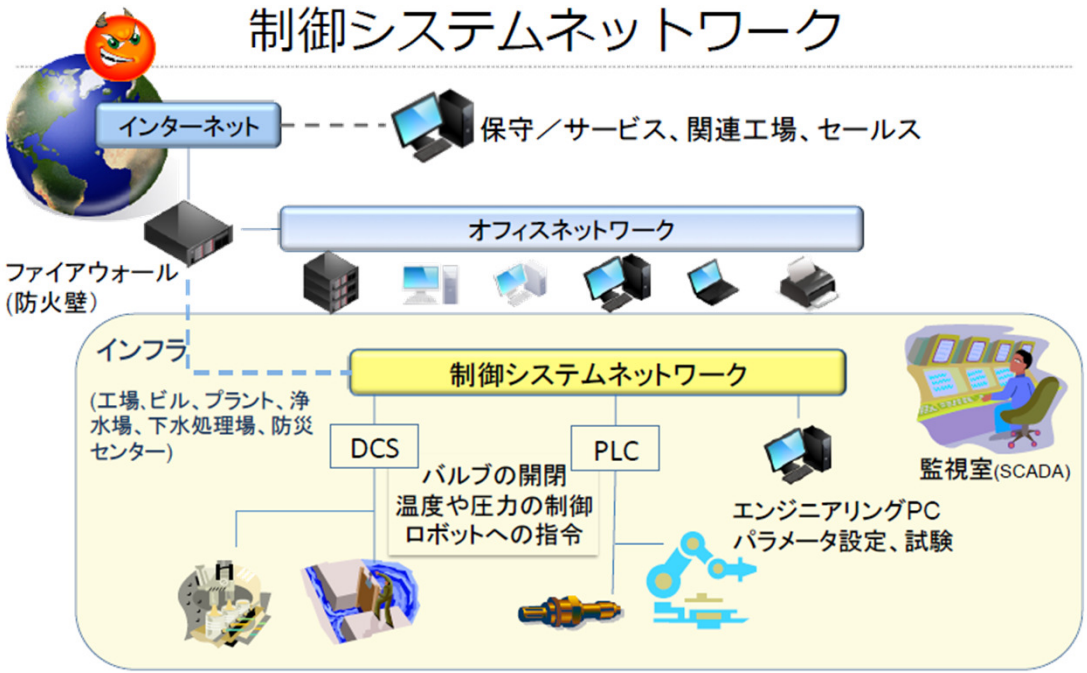
■ インターネットの普及と活用範囲の拡大により、サイバー空間からの攻撃対象は、情報のみならず、ヒト・モノ・カネに拡大。



ALSOKにて作成

制御システムセキュリティの現状

- 制御システムとは、エネルギーや石油・化学分野等のプラントにおける、生産ラインの監視・制御等に利用されているシステム
- 従来、**閉じたネットワーク**で運用されることが多く、**セキュリティ対策が遅れがち**であった。
- 近年、**生産性向上のためネットワーク化が急進**。海外を中心に**サイバー攻撃のリスクが増加**している。



出展：技術研究組合制御システムセキュリティセンター紹介資料

制御システムのサイバー攻撃事例(１)

- 2008年トルコで、石油パイプランが爆発。パイプラインに設置されている監視カメラの通信ソフトの脆弱性を利用して攻撃者が内部ネットワークに侵入。プラントの動作制御を不正に操作し、石油の流量を増加させ、パイプ内の圧力を異常に高めて爆発を引き起こした。
- 攻撃者は警報装置(監視カメラやセンサー)の動作停止操作も実施。

Oil pipeline

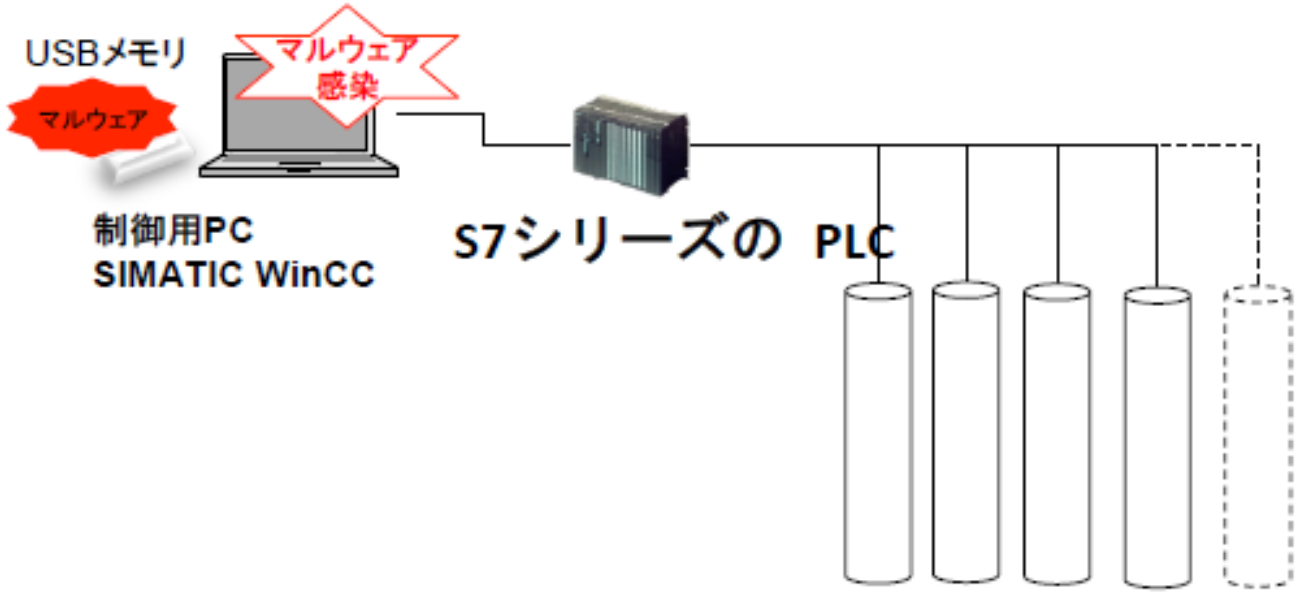
Will Russell/CC BY 2.0　写真は参考画像です

Oil pipeline(全体図)

出展:技術研究組合制御システムセキュリティセンター紹介資料

制御システムのサイバー攻撃事例(２)

- 2010年にイランの核燃料施設のウラン濃縮用遠心分離機を標的にサイバー攻撃が行なわれた。USBメモリにより制御用PCをマルウェアに感染させ、遠心分離機に異常な動作をさせた。結果、遠心分離機には過剰な負荷がかかり、20%が破壊されたと言われている。
- これによりイランの核開発計画は3年程度遅れたとする見方もある。



遠心分離機

出展:技術研究組合制御システムセキュリティセンター紹介資料

制御システムのサイバー攻撃事例(３)

- ドイツの製鉄所の溶鉱炉を制御するPCがマルウェアに感染。外部から遠隔操作できる状態になり制御を乗っ取られた。攻撃者の不正な操作により溶鉱炉が制御不能となり甚大な損傷が発生。
- 高度なフィッシングやソーシャル・エンジニアリングで職員をだましマルウェアを侵入させた。

出展:Ina Fassbender-REUTERS

制御システムにおける物理的侵入の例

■ 制御システムに対する物理層からの攻撃例として、以下のようなケースが想定される。

①不正なコントロール端末の接続による中間者攻撃。

（情報搾取や、通信のループ発生によるトラフィック増大）

②USBメモリ経由による監視端末の設定書換え攻撃。

USBポート

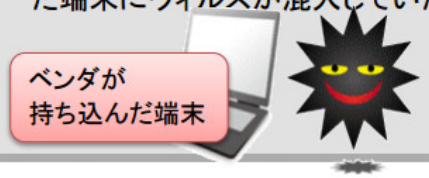
- USBメモリからのウィルス感染事例は頻繁に発生している

リモートメンテナンス回線

- 某社は米国の中央監視室からリモートメンテナンス回線によりタービンをリアルタイム監視
- リモートメンテナンス回線の先の端末からの不正アクセス・マルウェア混入

操作端末の入れ替え

- 日本の自動車会社では、ベンダが入れ替えた端末にウィルスが混入していた事例あり



物理的侵入

- 監視端末のパスワードが無い
- IDやパスワードは共通化、壁に張出し

出展：技術研究組合制御システムセキュリティセンター紹介資料

1 会社紹介

2 物理空間の脅威になったサイバー攻撃

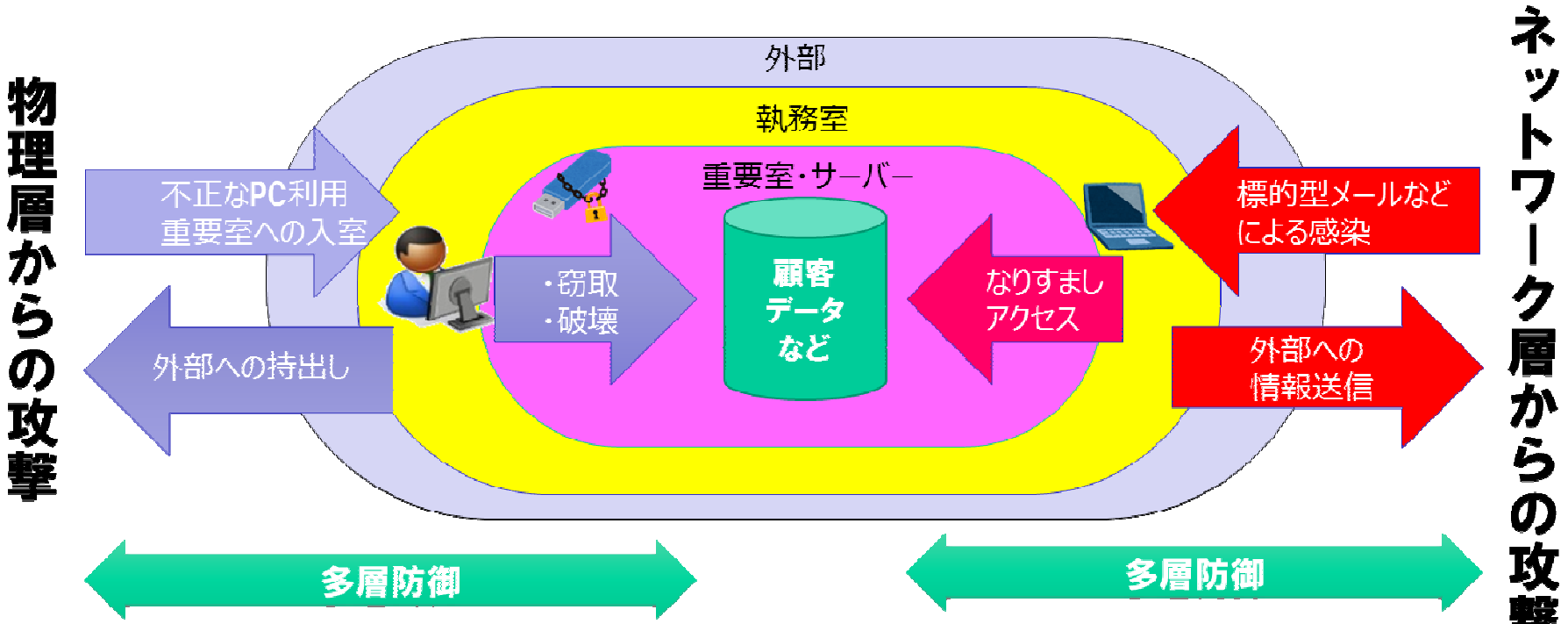
3 これまでの情報セキュリティと物理セキュリティ

4 融合空間のセキュリティ「真の多層防御」とは？

5 まとめ

情報セキュリティと物理セキュリティの現状

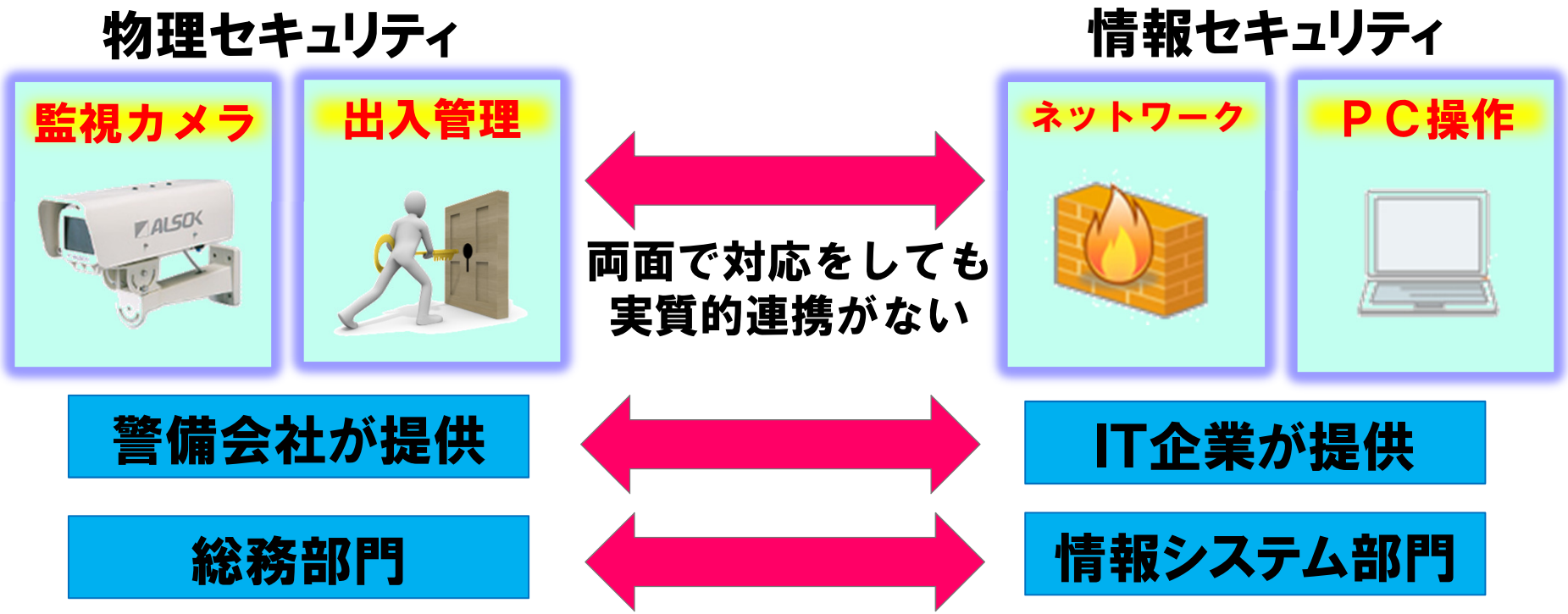
■ 従来からも、サイバー攻撃に対しては「情報」と「物理」の両面からセキュリティを構築する必要性が説かれてきた。



ALSOKにて作成

これまでの問題点1

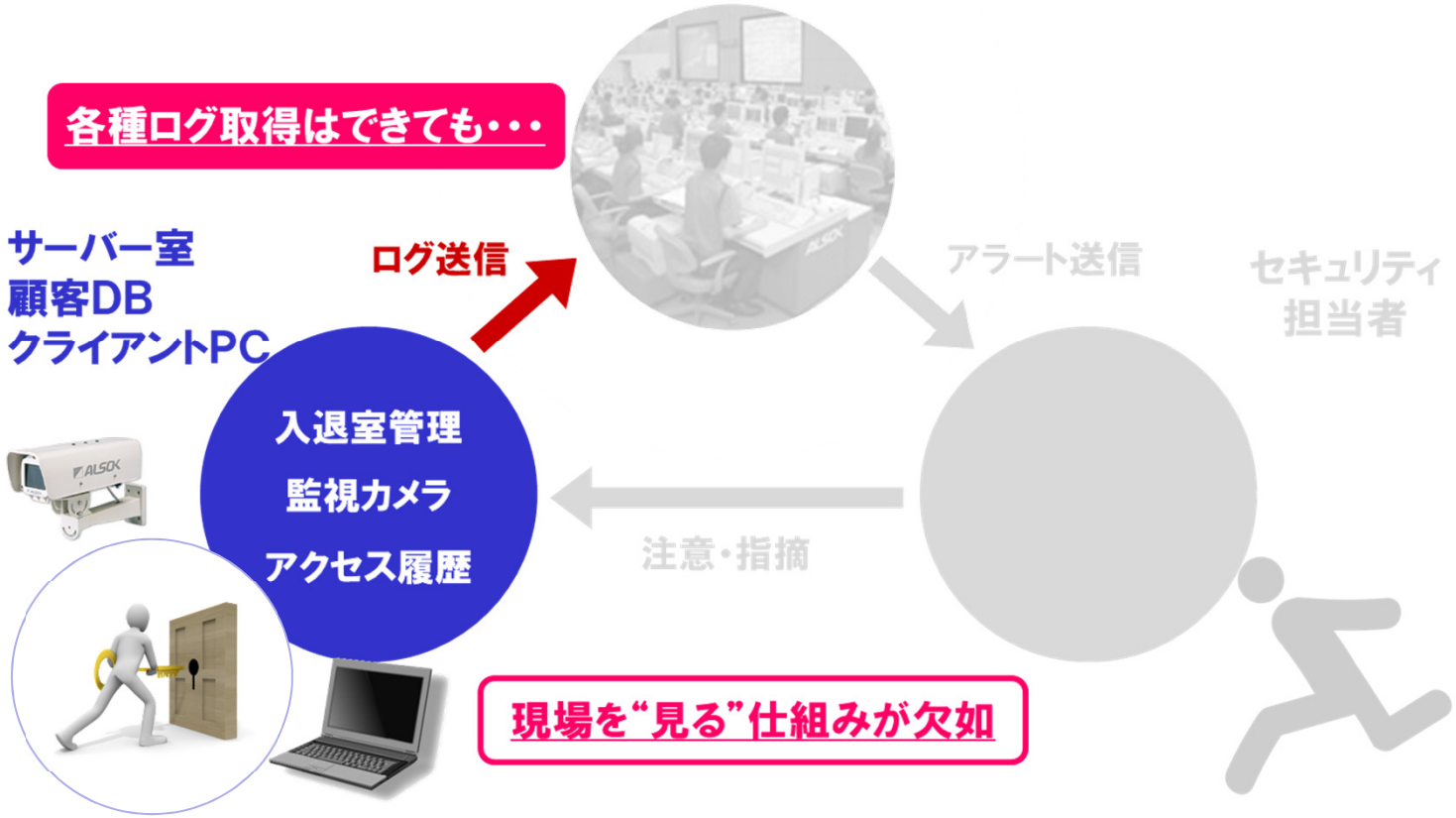
- しかし、物理セキュリティと情報セキュリティの対策は、個々の対応にとどまり、連携まで行われているケースは稀。
- メインサプライヤーの違いや利用者の管轄部署の違い（物理セキュリティ：総務部門、情報セキュリティ：情報システム部門）も要因の一つ。



ALSOKにて作成

これまでの問題点2

■ 結果、必要なログを取得していても、その後の監視・分析（アラート送信とその後の対応の枠組み）において、情報セキュリティと物理セキュリティのログ活用に関する検討がされていない場合が多い。

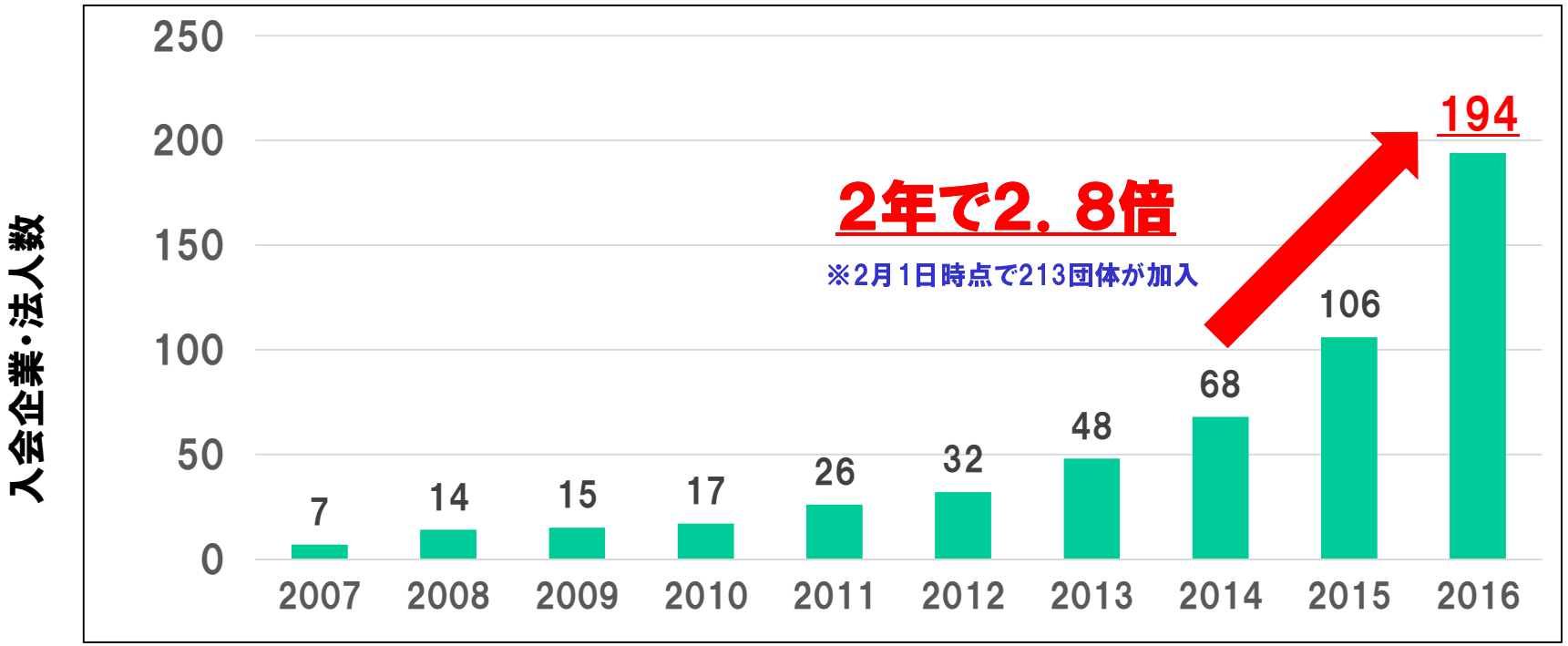


ALSOKにて作成

CSIRT設置企業・法人の急増

■ 一方、近年自社内にCSIRTを設置する企業・法人が急増。
■ こうした企業・法人では、事態の早期把握に向けた総務部門と情報システム部門の情報一元管理体制構築の動きが見られはじめた。

日本CSIRT協議会への入会数推移



出展：日本CSIRT協議会のホームページより当社にて集計

1 会社紹介

2 物理空間の脅威になったサイバー攻撃

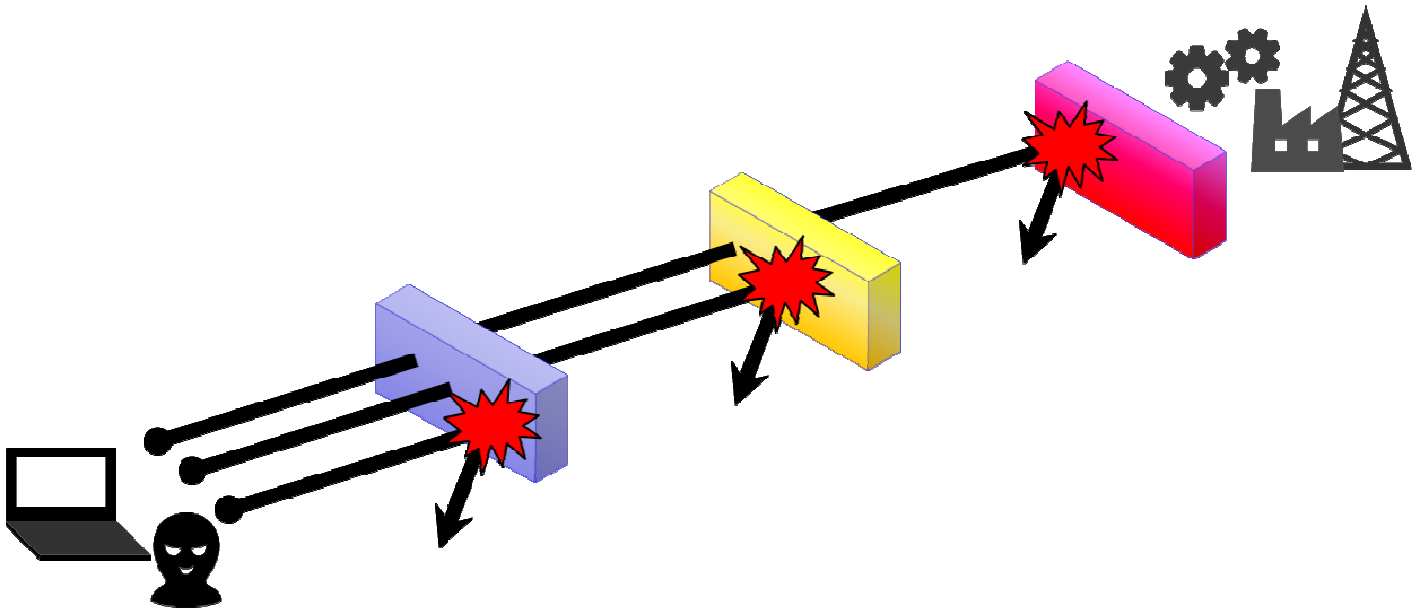
3 情報セキュリティと物理セキュリティの現状

4 融合空間のセキュリティ「真の多層防御」とは?

5 まとめ

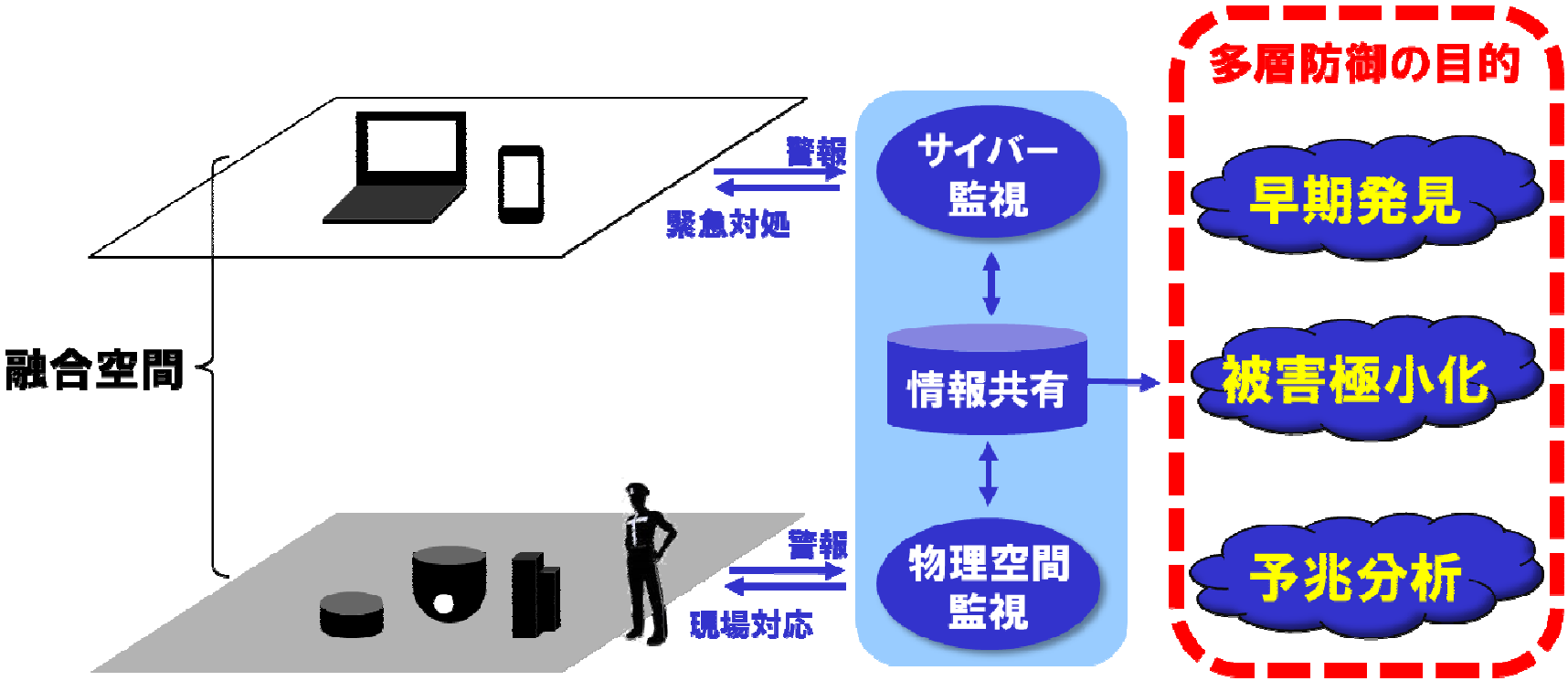
「多層防御」の考え方

- サイバー攻撃の高度化により、ウィルス対策ソフト等、従来のセキュリティ対策のみではもはや被害を防ぎきれない。
- 大切なのは「事業継続のために例え**侵入を許しても拡大を防ぐ手段を講じる等**、最低限守るべきなのは何か」を明らかにした上で、様々なセキュリティ対策を組み合わせた多層防御を行い、重要資産の要塞化を図ること。



融合空間における「真の多層防御」とは？

- サイバー空間と物理空間における脅威の一体化が進む中、重要資産を守るには両空間での監視連携と物理的対処が有効。
- 特に制御システムは、人命をはじめとした甚大な被害につながることが多く、常に両空間を意識した「真の多層防御」が必要。



ALSOKにて作成

早期発見につなげる

■ 出入管理との連携例（後述する図1と関連）

- 制御端末がある部屋への時間外入室を検知。
- 一般権限社員入室後に管理者権限でのシステムログイン検知。
- 清掃業者による清掃時間中の端末起動やUSBメモリ挿入検知。

■ 機械警備との連携例（後述する図1と関連）

- 警備セット中（無人状態）での不審な通信を検知。
  - ※　巧妙なマルウェアはひっそりと動き、感染拡大期は通信量も少なく検知が難しい。

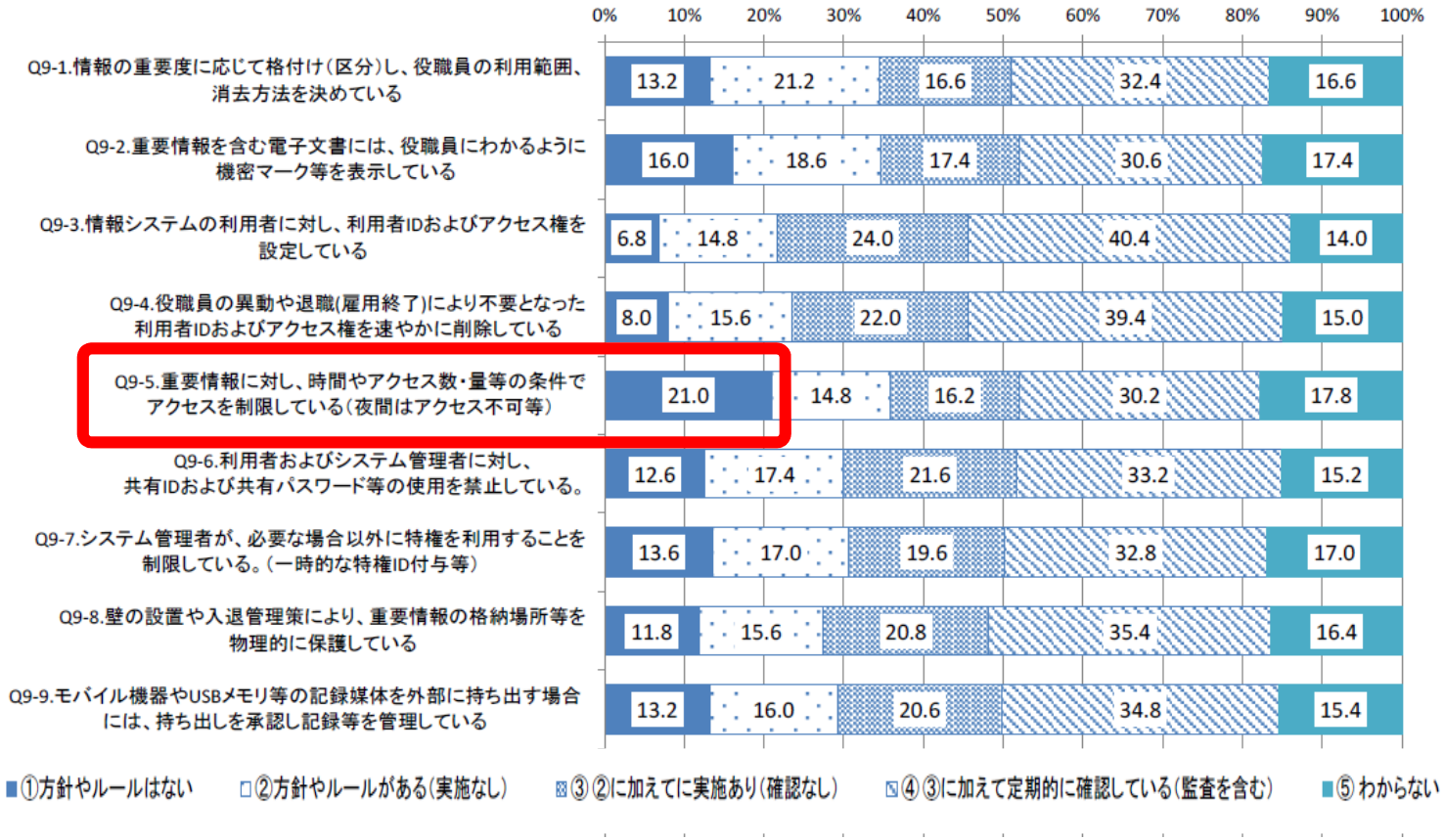
■ 監視カメラとの連携例（後述する図2と関連）

- 共連れ作業の検知。
- カメラへの細工（方向を変える/目隠しをする）を検知。

⇒物理セキュリティのログ活用で人の動きがより明確化するはずだが・・・

早期発見に向けた課題　図1（資料）

■ 従業員300人以上の企業500社が実施している内部不正対策項目のうち、最も「方針やルールがない」のが「時間やアクセス数、量等の条件でアクセス制限をしていない」（21％）



出展：IPA「内部不正による情報セキュリティインシデント実態調査」
https://www.ipa.go.jp/security/fy27/reports/insider/

早期発見に向けた課題　図2（資料）

■ 同調査で「方針やルールがない、あっても実施なし」の合計で最も多いのは「**単独での作業を制限し、やむをえず単独で作業する場合は事前承認及び事後確認をしている**」（39.8％）

⇒ **実質的なチェックが難しく、共連れ等を発見しづらい。**

出展：IPA「内部不正による情報セキュリティインシデント実態調査」
https://www.ipa.go.jp/security/fy27/reports/insider/

被害の極小化につなげる

■ システムの手動停止

- ➢ サイバー攻撃により、システムの遠隔制御ができなくなった場合、現地で手動停止を行う。

■ 非難誘導

- ➢ ビル制御システム等への攻撃時は非難誘導の発生を考慮する。

■ フォレンジックの為の現場保全と一次対処

- ➢ LAN配線の物理的切り離し。
- ➢ マルウェア感染判定や解析情報を収集する為のツール実行。
- ➢ 現場写真等、対処状況の記録。

ALSOKにおける現場対応力向上の為の取組み

- しかし、制御システムに不慣れな者（例えば警備員）が手動停止等の現場対処を行う為には仕組みが必要。
- ALSOKでは、ICT機器を装備した警備員と、監視センターでの情報解析を組み合わせた高度対処を実現。提供する警備サービスの品質向上と平準化を図っている。

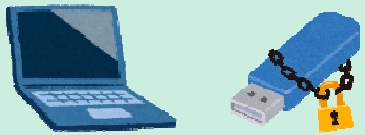
ＡＬＳＯＫゾーンセキュリティマネジメント®

ALSOKにて作成

予兆分析につなげる

■ これまでサイバー監視とは連携されてこなかった物理側の情報から、情報セキュリティインシデントの予兆分析につなげることも可能に。

拾得物
（PC、USBメモリ）



停電

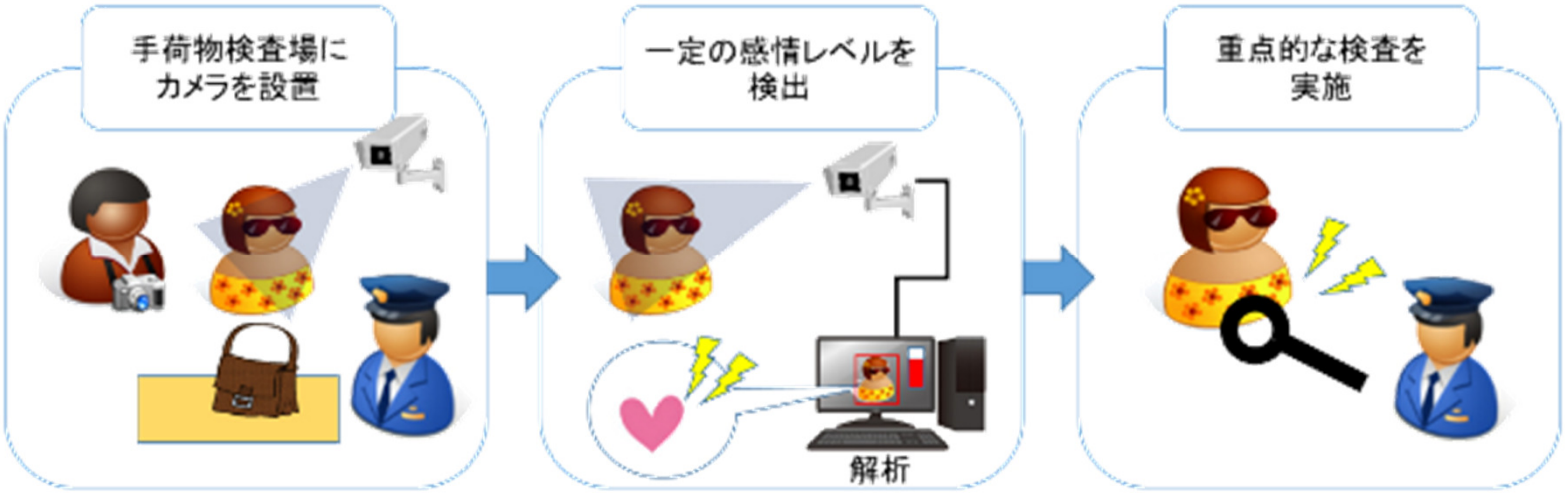
設備停止
（エレベータ、電話）

異音・異臭

ALSOKにて作成

ALSOKにおける予兆分析への取組み

■ 人の感情を可視化する画像解析技術を取り入れ、犯罪を起こす可能性がある人物を検知することで、未然防止に役立てる技術は既に実用段階に入っている。



感情の高ぶりによる無意識の体の揺れ、震えから犯罪の予兆を検知

ALSOKにて作成

1 会社紹介

2 物理空間の脅威になったサイバー攻撃

3 情報セキュリティと物理セキュリティの現状

4 融合空間のセキュリティ「真の多層防御」とは?

5 まとめ

まとめ

■ インターネットの普及と拡大により、サイバー空間からの攻撃対象は、情報のみならず、ヒト・モノ・カネに拡大。

■ 制御システムは、人命等の甚大な被害につながることが想定される為、日頃から「最低限守るべきなのは何か」を明らかにした上で、多層防御の上で重要資産の要塞化を図ることが重要。

■ この多層防御には物理層からの攻撃も想定し、カメラや出入管理等のログについても解析することでインシデントの①**早期発見**、②**被害の極小化**、③**予兆分析**が可能になる。

ALSOK

ALways Security OK