HITACHI
Inspire the Next

IoTデバイス向けセキュリティソリューション ご説明資料

株式会社 日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

<昨今の背景>

総務省、経済産業省「IoTセキュリティガイドラインの概要」

インターネットに接続される機器の数は年々増加しており、**家電、防犯機器、自動車、医療機器、事務機器、産業機器**など、200億を超えるさまざまな「モノ」がつながる**「モノのインターネット（IoT）」**が形成されています。

IoTデバイスにおいては、**システムとしてのリーソス資源が少ないこと**や、市場での販売拡大を優先に価格を抑えるあまり、**十分なセキュリティ対策を実装せずに販売**されています。

「IoTセキュリティガイドライン」は、対象者を、**供給側の経営者、機器の生産者、サービス提供者、**利用側の企業利用者、一般利用者として、**適切なサイバーセキュリティ対策の重要性**を提言しています。

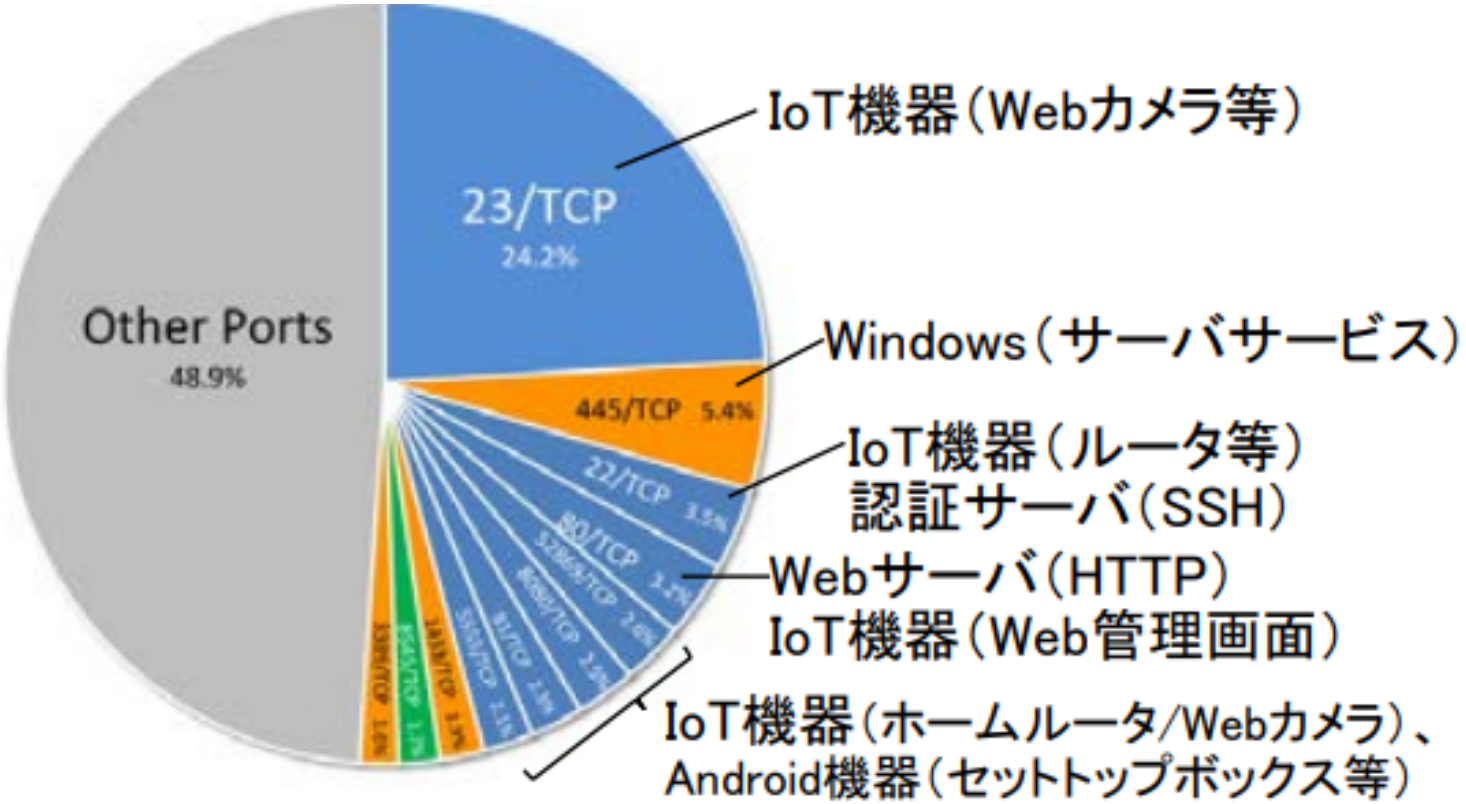
DXにおけるIoTデバイスの活用においても、これまでセキュリティ脅威とされていなかったさまざまな「モノ」や「システム」がサイバー攻撃などのセキュリティ脅威にさらされるため、**IoTセキュリティへの対応とその対策の必要性はこれまで以上に高まっている現状です。**

1 .IoTデバイスのセキュリティ現状

1-１．IoTデバイスの市場拡大とサイバー攻撃の現状

HITACHI
Inspire the Next

2019年時点、
IoTデバイスを狙ったサイバー攻撃の割合は半数弱



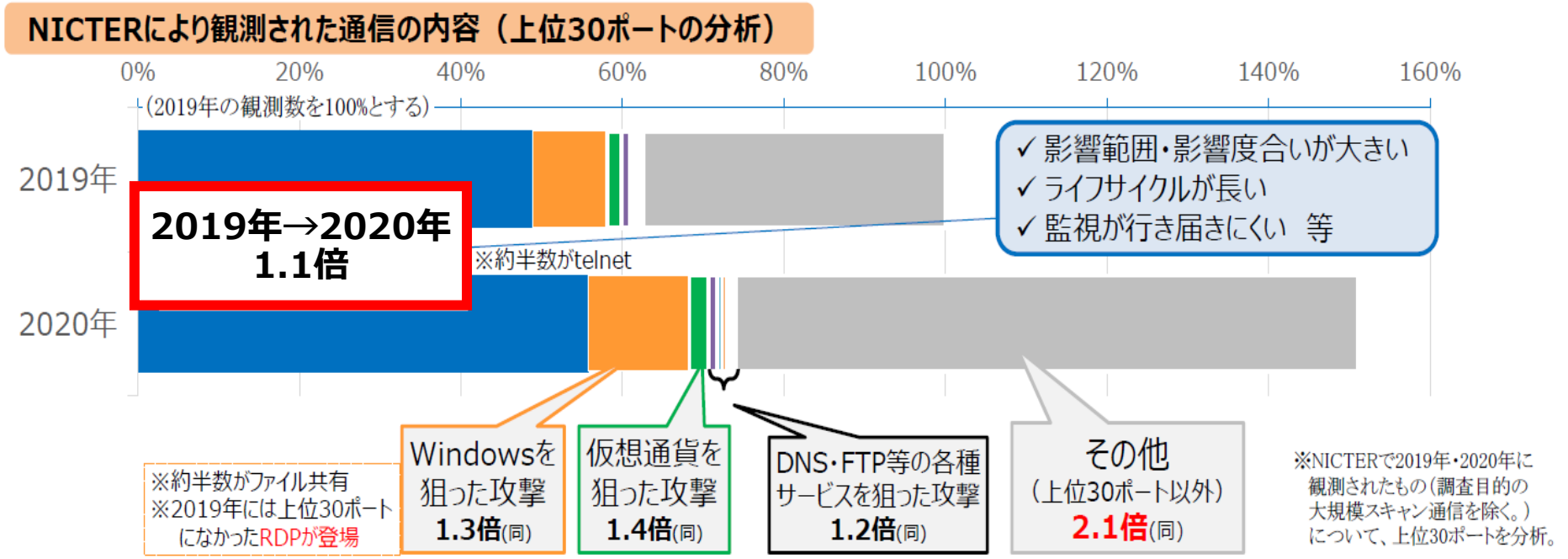
2019年　主なサイバー攻撃対象（宛先ポート番号）

出典：NICTER観測レポート2019(情報通信研究機構)

1-１．IoTデバイスの市場拡大とサイバー攻撃の現状

HITACHI
Inspire the Next

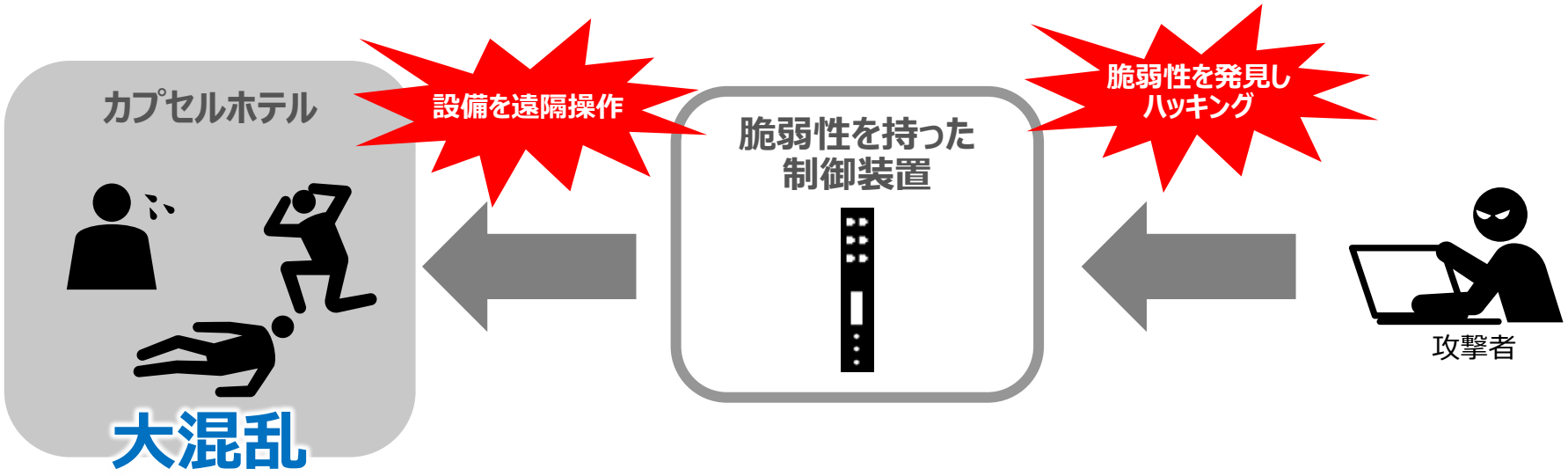
2020年にかけ、
IoTデバイスを狙ったサイバー攻撃が増加



出典：総務省におけるこれまでの取り組み及び最近のサイバーセキュリティ動向より(2022年1月)

1-2. IoTデバイスへのサイバー攻撃事例１（国内）

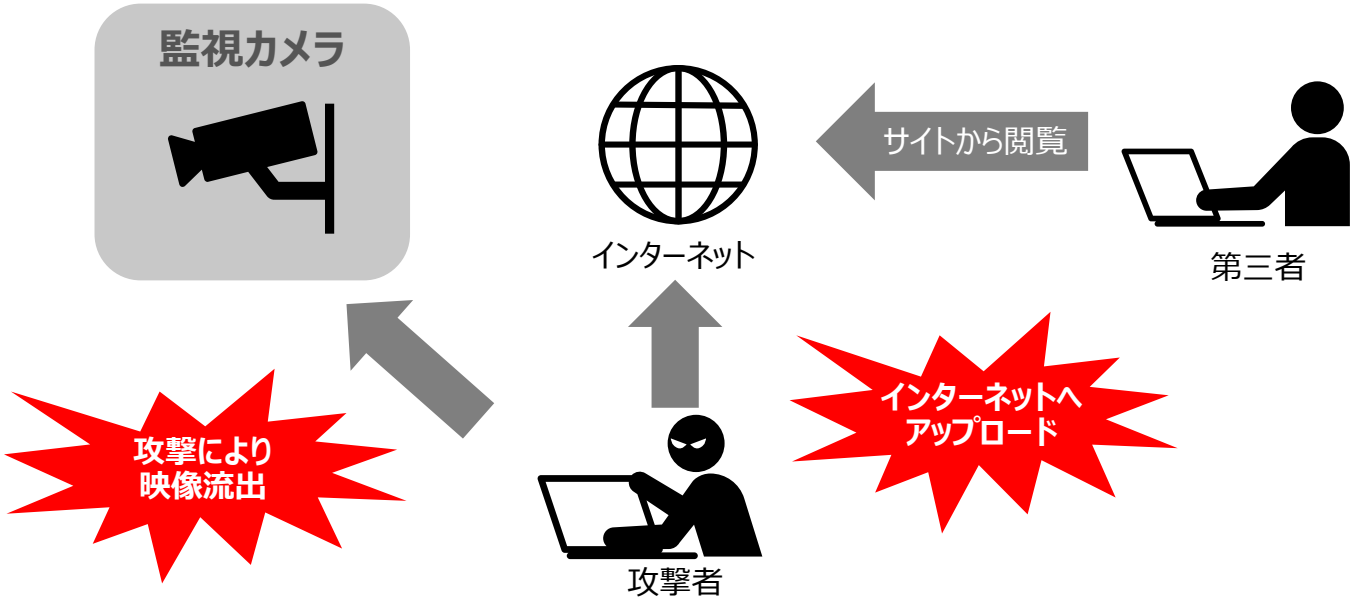
攻撃者がカプセルホテルの制御装置の脆弱性を発見。
他の客室の照明や空調機、ベッドを遠隔操作し、宿泊客のクレームに繋がった。



サービスのイメージダウンから企業経営へ影響する恐れが・・・

1-3. IoTデバイスへのサイバー攻撃事例２（国内・各国）

セキュリティ対策が不十分な世界中の監視カメラの映像がインターネットで公開。
日本でも*5,000*台以上のカメラの映像がだれでも確認できてしまう事態に。



盗聴・覗き見から個人のプライバシーの侵害に繋がってしまう・・・

HITACHI
Inspire the Next

2．IoTデバイスが抱える課題と対策

2-１．IoTデバイスが抱える課題

HITACHI
Inspire the Next

≪被害の特徴≫
・調達部品に脆弱性が混入している

・大規模なサイバー攻撃の入り口として狙われやすい

・サイバー攻撃に初期段階で気付くことが難しい

特徴からみえる課題は・・・

課題１：外部調達部品及びIoTデバイスそのもののセキュリティ基準、評価項目が整っていない

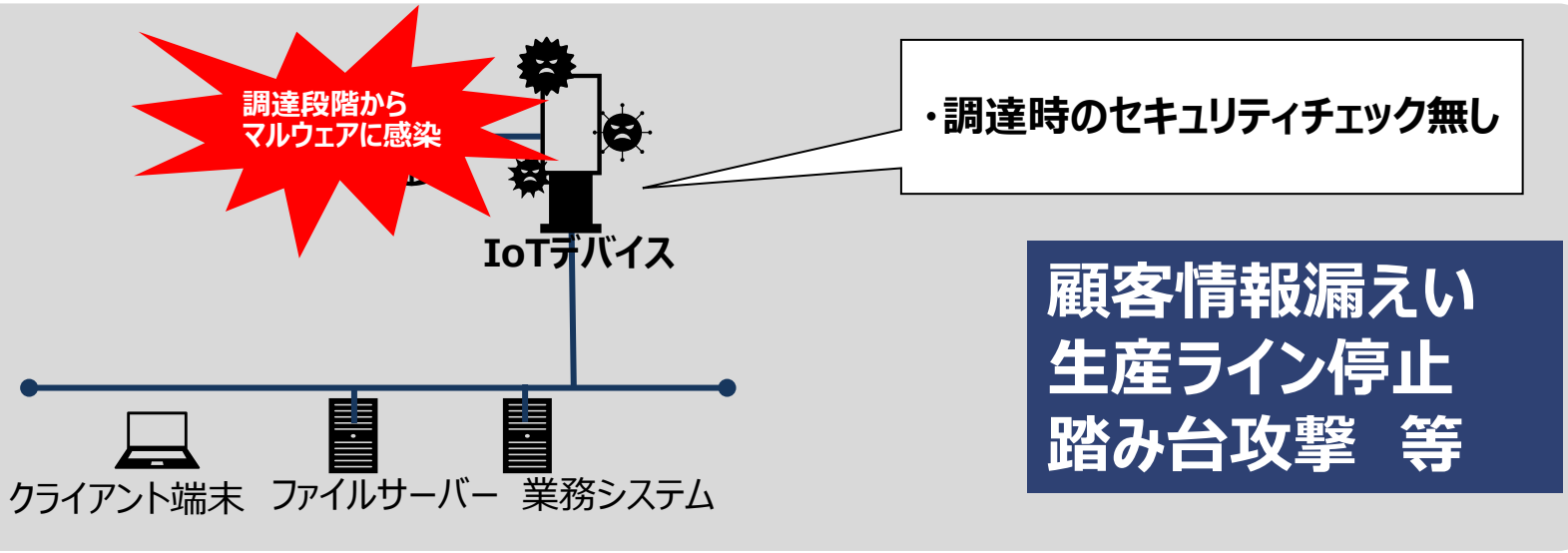
課題２：セキュリティ対策が難しく、セキュリティホールができやすい

課題３：IoTデバイスを常時モニタリングする仕掛けがない

HITACHI
Inspire the Next

課題１：外部調達部品及びIoTデバイスそのものの セキュリティ基準、評価項目が整っていない

社内にセキュリティに関する基準が無いと、
調達もしくは製造の段階から、セキュリティリスクが生まれてしまう。

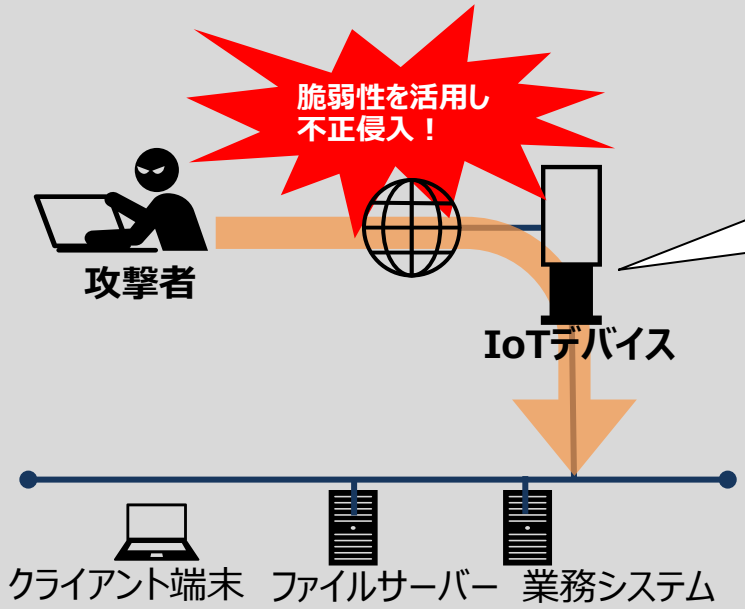


顧客情報漏えい
生産ライン停止
踏み台攻撃　等

HITACHI
Inspire the Next

課題2：セキュリティ対策が難しく、セキュリティホールができやすい

長期に渡って使用され続けること、使えるリソースが限られていることから、
PCのように常に十分なセキュリティ対策を実装することが難しい。



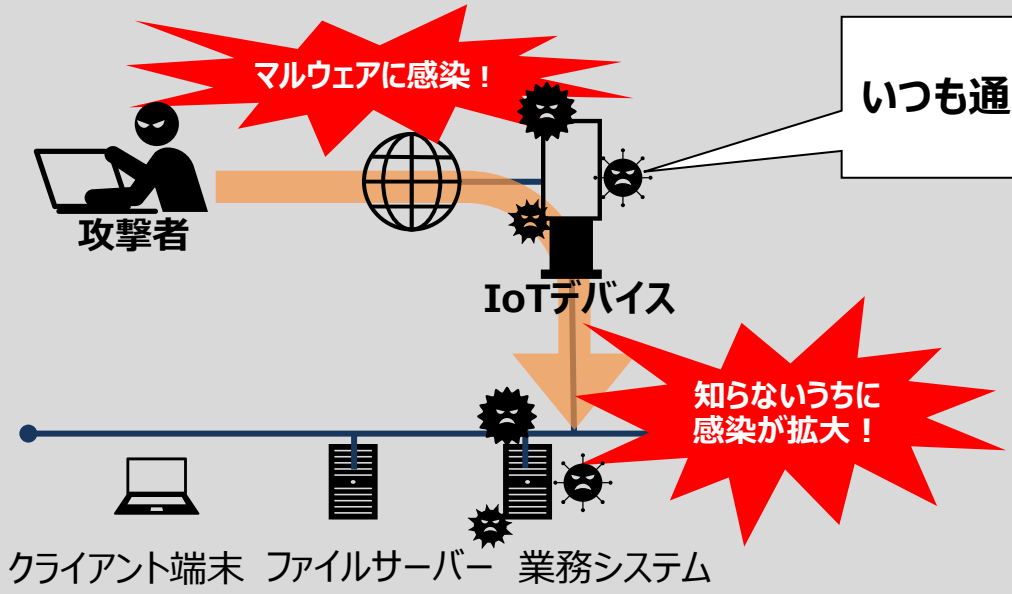
・導入後5年経過
・セキュリティ対策無し
・脆弱性有り

顧客情報漏えい
生産ライン停止
踏み台攻撃　等

HITACHI
Inspire the Next

課題3：IoTデバイスを常時モニタリングする仕掛けがない

稼働状況をモニタリングする運用になっておらず、
サイバー攻撃にリアルタイムに気づきにくい



顧客情報漏えい
生産ライン停止
踏み台攻撃　等

2-２.課題に対する効果的な対策

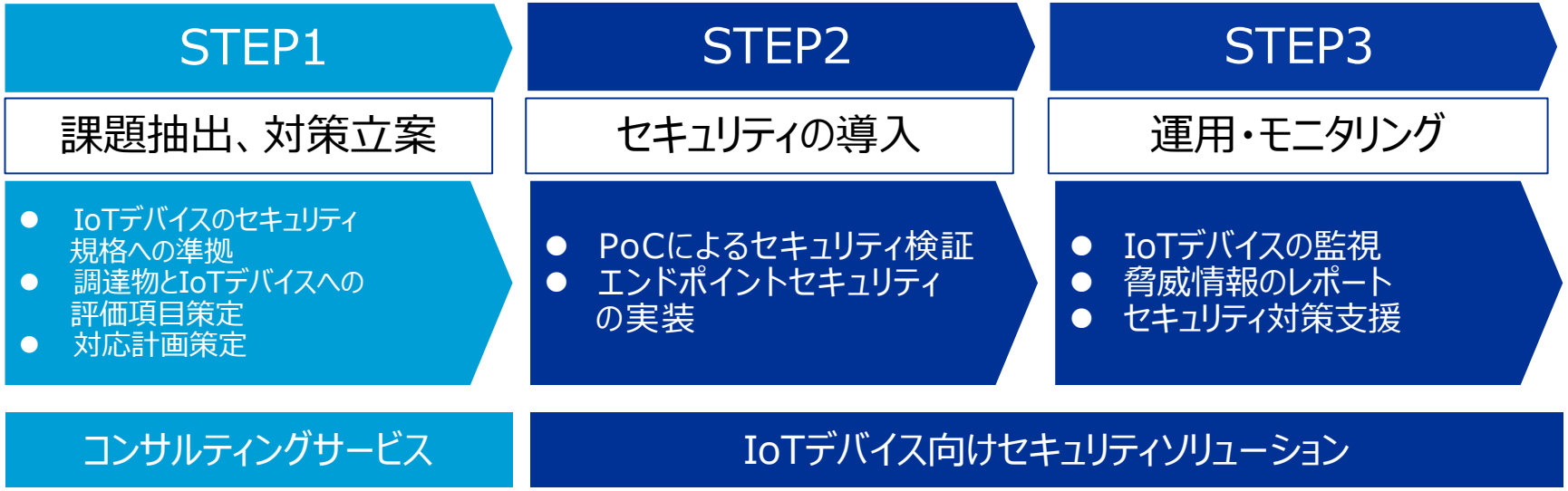
HITACHI
Inspire the Next

課題	解決策
外部調達部品及びIoTデバイスそのもののセキュリティ基準、評価項目が整っていない	セキュリティ規格や調達要件に応じたセキュリティの確保
セキュリティ対策が難しく、セキュリティホールができやすい	IoTデバイスに適した、負荷の少ないセキュリティ対策の導入 ・入口・出口対策 ・不審なふるまい検知　等
デバイスを常時モニタリングする仕掛けがない	IoTデバイスを常時モニタリングし、管理運用 ・稼働状況のモニタリング ・検知した脅威情報の通知 ・インシデント発生時の調査　等

2-3.当社がお手伝いできること

コンサルティングからセキュリティソリューションの導入・運用までをワンストップで提供することで、IoTデバイスのセキュリティ強化を支援します。

■具体的なSTEP



2-3.当社がお手伝いできること

HITACHI
Inspire the Next

【STEP 1】

IoTデバイスの開発環境における
セキュリティ規格への対応を支援します。

企画 → **設計** → **生産**

当社支援により、開発プロセスを確立し、製品のセキュリティを強化

支援内容	日立ソリューションズ・クリエイトの強み
① IoTデバイスの特性に応じた外部規格、法規制への準拠	① 外部規格(NIST SP800 171等)、法規制にも精通した**「各種BP・規格の知見」**
② 製品に対する評価項目の策定と開発プロセスとの連動	② 多様なビジネス領域での製品セキュリティによる**「セキュリティソリューションの実績」**
③ 外部調達品に対する評価項目の策定ならびに 外部サプライヤーとの連動	③ サプライヤ/発注者の双方の立場でセキュリティを確保してきた**「豊富な顧客対応実績」**

2-3.当社がお手伝いできること

HITACHI
Inspire the Next

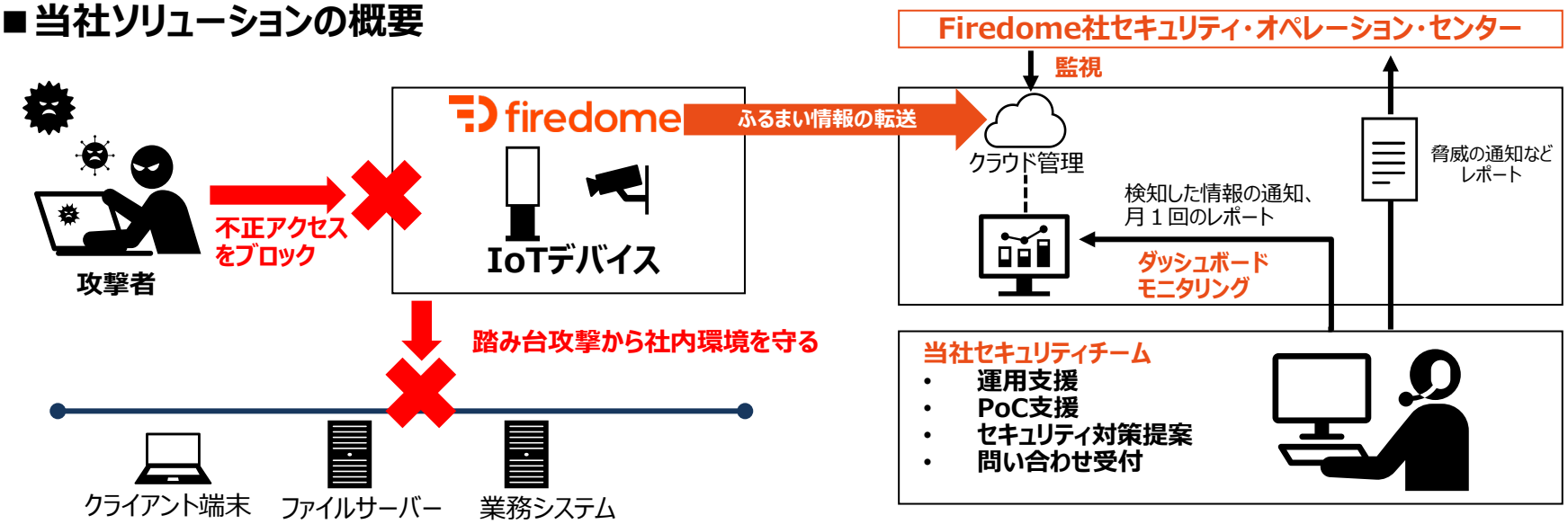
【STEP 2】
【STEP 3】

IoTデバイスに向けた **セキュリティの強化と運用を支援**します。

エージェント導入による強固なセキュリティ

モニタリングによるデバイスの管理

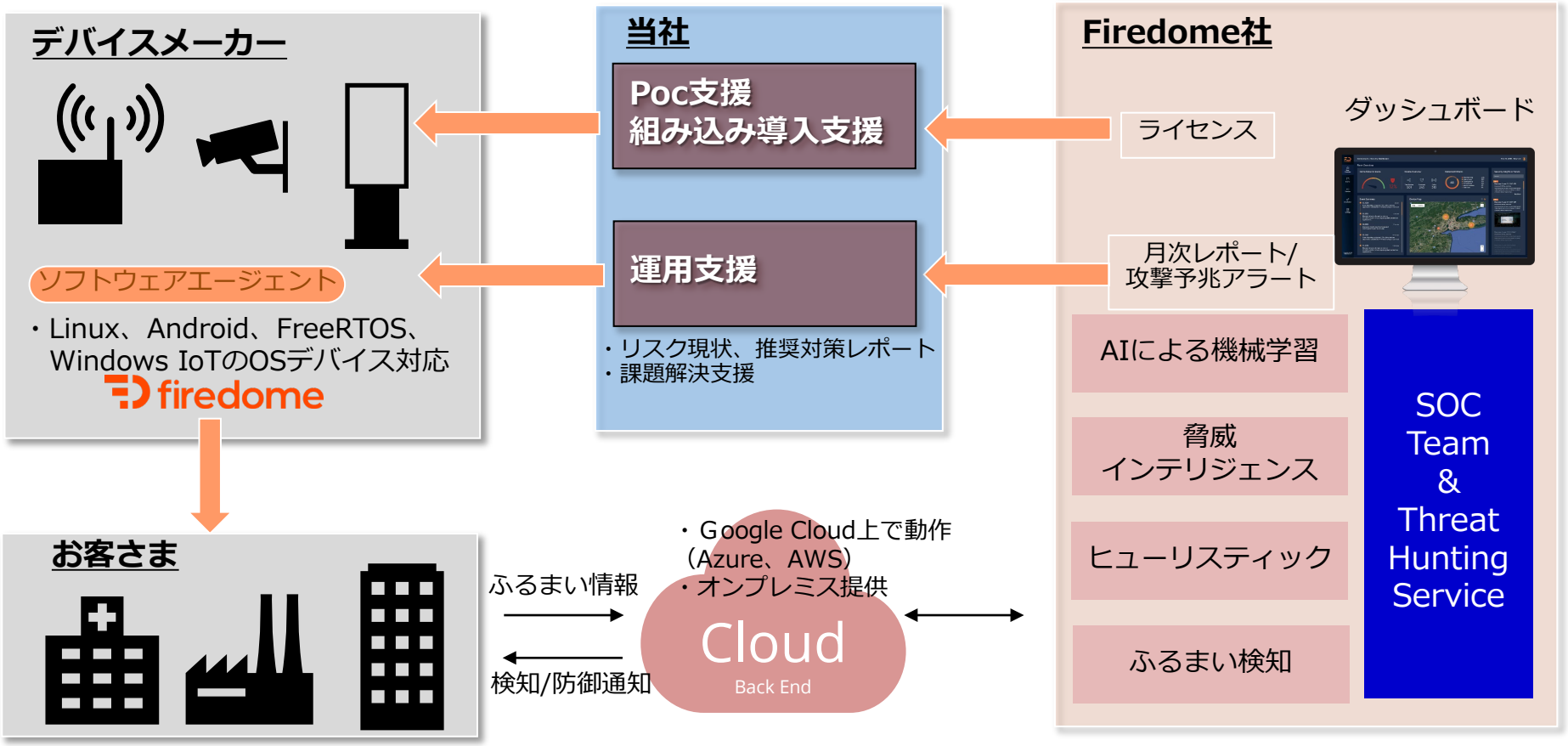
■当社ソリューションの概要



HITACHI
Inspire the Next

Firedomeを活用したソリューション

- **Firedome社と当社の強力な連携により、IoTデバイスセキュリティ強化と運用負荷軽減に貢献します。**

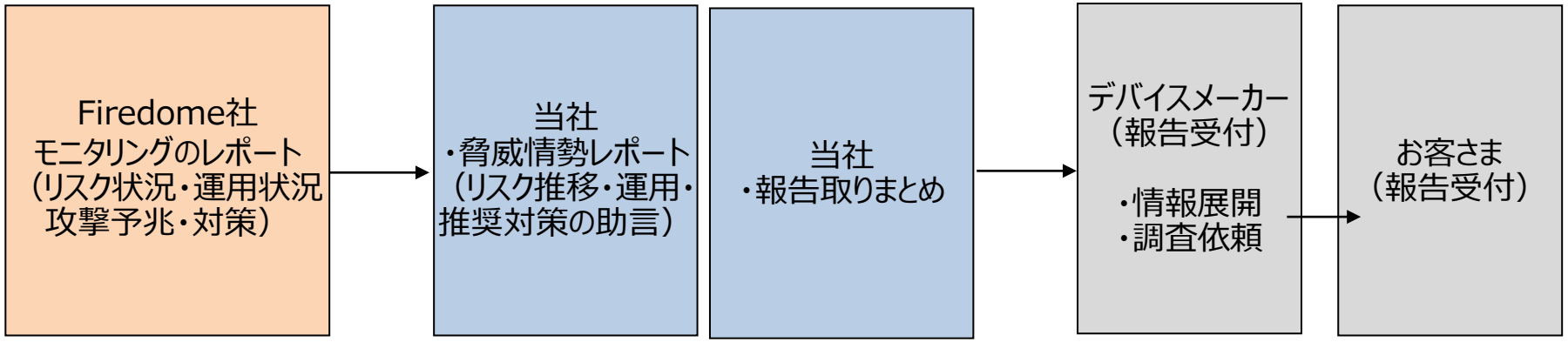


17

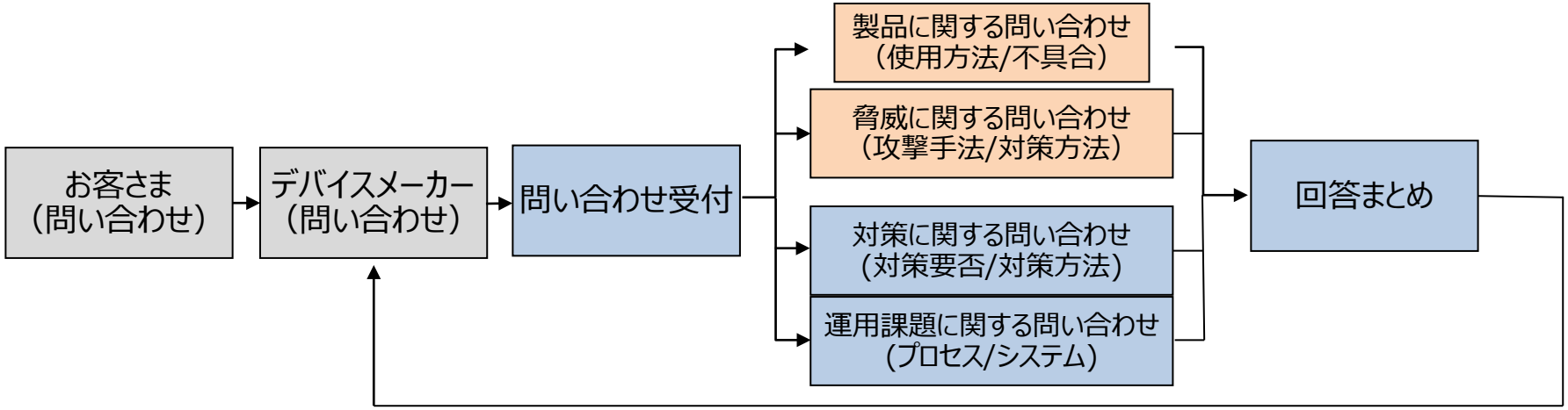
HITACHI
Inspire the Next

＜運用支援提供サービスにおけるFiredome社、当社の役割＞

（1）定期報告会（月次）



（2）レポート及び製品Q&A



HITACHI
Inspire the Next

３．デジタルサイネージにおけるFiredomeの技術検証

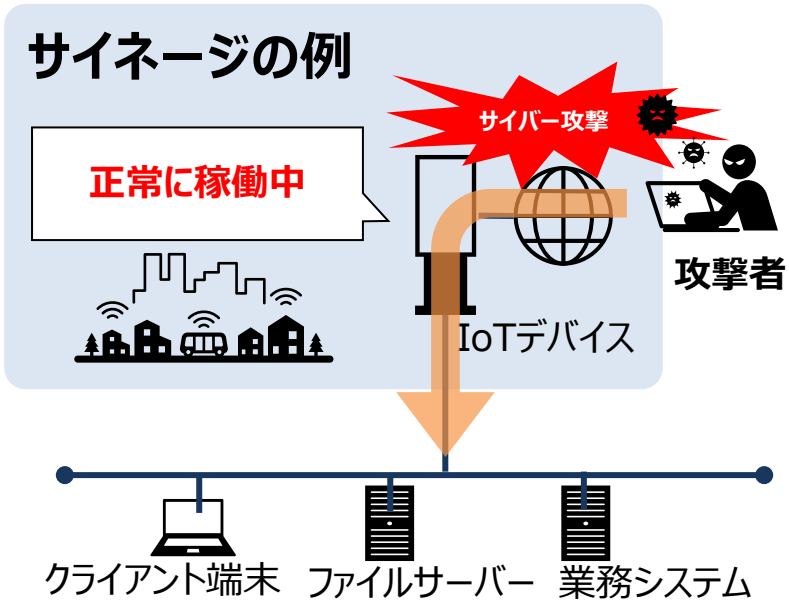
HITACHI
Inspire the Next

今回は、サイネージ画面の乗っ取りをシミュレーション

サイバーキルチェーン

偵察	ポートスキャンによる攻撃対象の調査
武器化	攻撃のためのマルウェアの作成
配達	総当たり攻撃による不正アクセス
攻撃	攻撃コード実行によるマルウェアダウンロード
インストール	既知・未知のマルウェア実行
遠隔制御	マルウェア感染したデバイスによるC&Cサーバー接続

サイネージの例



HITACHI
Inspire the Next

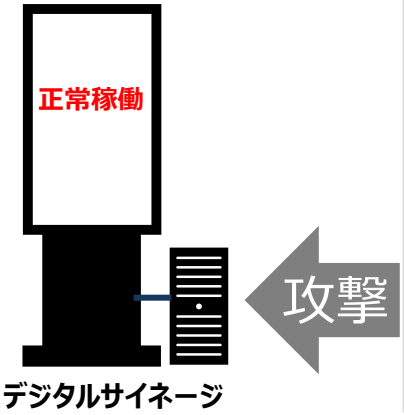
Firedome無しの場合・・・

3-2.サイバー攻撃のシミュレーション

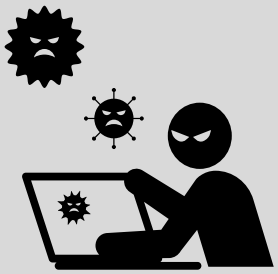
HITACHI
Inspire the Next

偵察 **ポートスキャンによる攻撃対象の調査**

不正アクセス可能な
ポート番号として以下を検知
- **sshリモートログイン**
- **WebページHTTPサービス**
- **Remote Procedure サービス**
- **NetBIOSセッションサービス**
- **SMBサービス**
  （ファイル/プリンタの共有）
- **Remote Desktop**



デジタルサイネージ



```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 05:15 UTC
Nmap scan report for 10.100.1.57
Host is up (0.0012s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:04:5F:74:DA:79 (Avalue Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds


Finished Port Scanning.
```

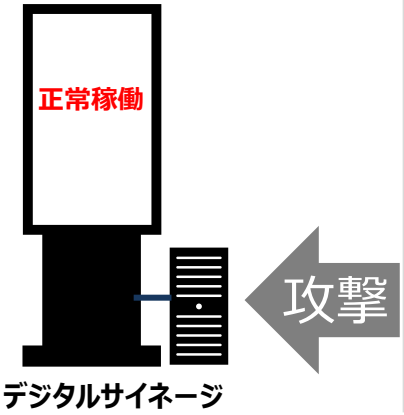
攻撃者の画面

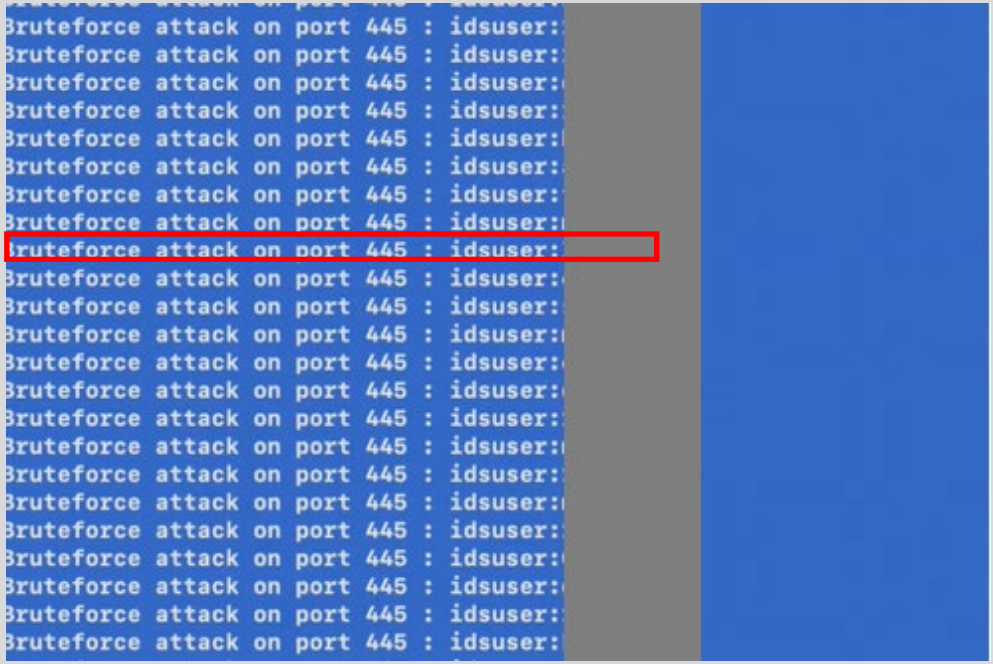
3-2.サイバー攻撃のシミュレーション

HITACHI
Inspire the Next

配達 **総当たり攻撃による不正アクセス**

ポートスキャンで開放を
確認したSMBサービスに対し
総当たり攻撃を実施





攻撃者の画面

3-2.サイバー攻撃のシミュレーション

HITACHI
Inspire the Next

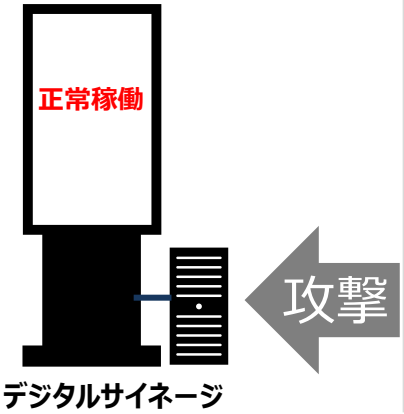
総当たり攻撃による
不正アクセス成功後
遠隔操作が可能になる
ツールをインストール

攻撃

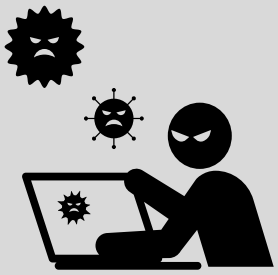
攻撃コード実行によるマルウェアインストール

```
C:\>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 0EFB-373F

 Directory of C:\

06/14/2021  02:41 PM        23,493,145 20210614_1.zip
09/20/2021  02:27 AM                 4 aa.txt
09/19/2021  06:31 PM                 4 aab.txt
06/05/2018  04:52 PM    <DIR>          Drivers
06/14/2021  02:47 PM    <DIR>          hitachi
06/14/2021  03:41 PM    <DIR>          IDS
11/15/2019  03:28 PM    <DIR>          inetpub
10/01/2019  02:00 PM    <DIR>          Intel
09/13/2021  09:05 PM    <DIR>          MediaSpace
06/11/2021  05:40 PM               105 netTime.bat
08/24/2021  06:03 PM    <DIR>          OpenSSH-Win32
08/24/2021  06:03 PM         3,198,737 OpenSSH-Win32.zip
08/24/2021  06:37 PM    <DIR>          OpenSSH-Win64
06/06/2018  09:59 AM    <DIR>          PerfLogs
10/07/2021  01:38 AM    <DIR>          Program Files
10/07/2021  01:38 AM    <DIR>          Program Files (x86)
06/14/2021  02:21 PM    <DIR>          RIDS
10/06/2021  07:03 PM    <DIR>          temp
06/14/2021  03:43 PM    <DIR>          Users
10/08/2020  11:19 AM    <DIR>          W3SVC1
08/30/2021  05:56 PM    <DIR>          Windows
07/04/2018  09:47 AM    <DIR>          ?␣?c?[??
               5 File(s)     26,691,995 bytes
              17 Dir(s)  42,748,157,952 bytes free
```

攻撃者の画面

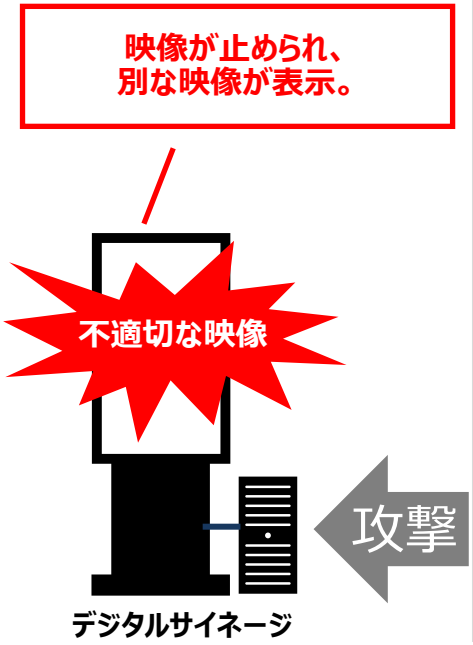


デジタルサイネージ



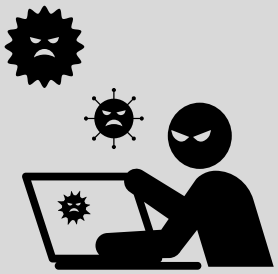
3-2.サイバー攻撃のシミュレーション

HITACHI
Inspire the Next



インストール **既知・未知のマルウェア実行**

遠隔制御 **マルウェア感染したデバイスによるC&Cサーバー接続**



- マルウェア実行
- C&Cサーバーと通信
- 悪意のあるソフトウェアをダウンロードし実行
- **不適切な映像が表示**
- **IoTデバイスを踏み台に、社内システムへの攻撃も可能**

HITACHI
Inspire the Next

Firedome有りの場合・・・

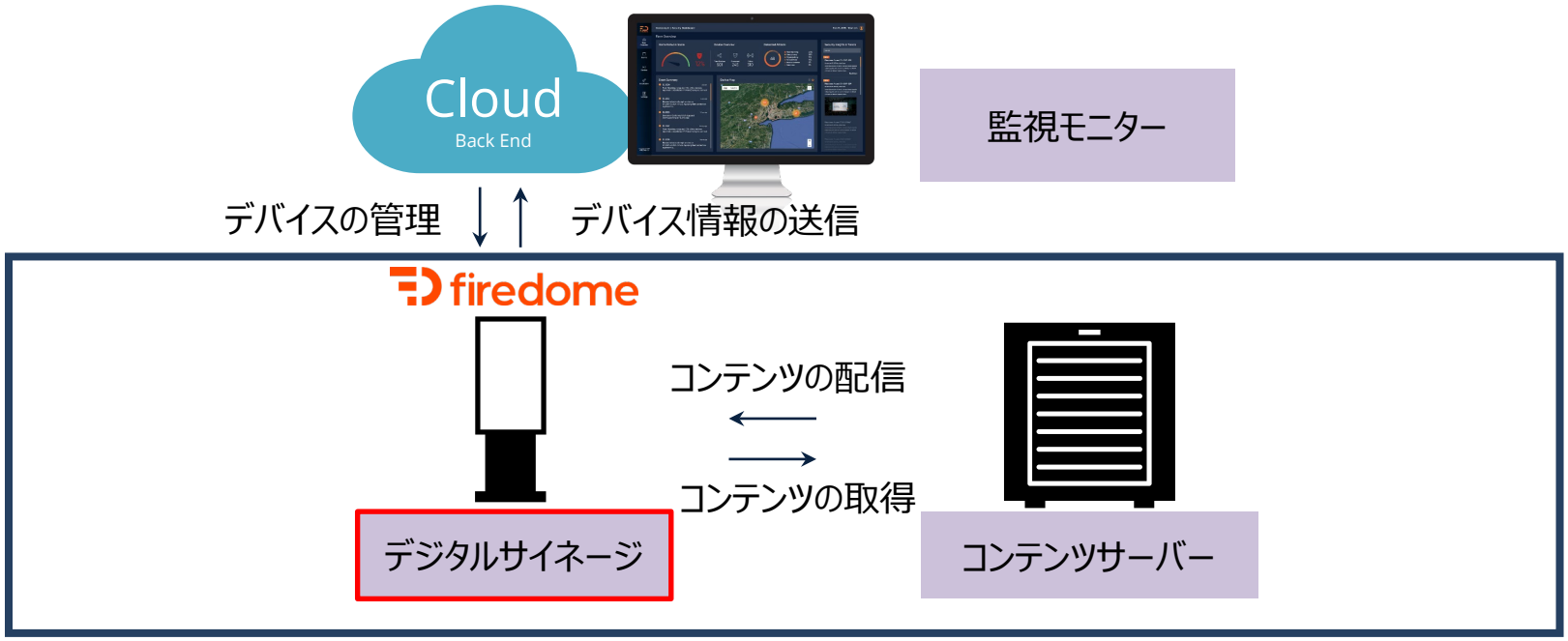
3-2.サイバー攻撃のシミュレーション

HITACHI
Inspire the Next

Firedomeでは、
下記のように<u>サイバーキルチェーンに即した対策</u>が取られています。

3-2.サイバー攻撃のシミュレーション

＜デモンストレーション環境＞
①デジタルサイネージにFiredomeエージェントをインストール
②監視モニターから、デバイスの情報・受けたサイバー攻撃の情報を管理



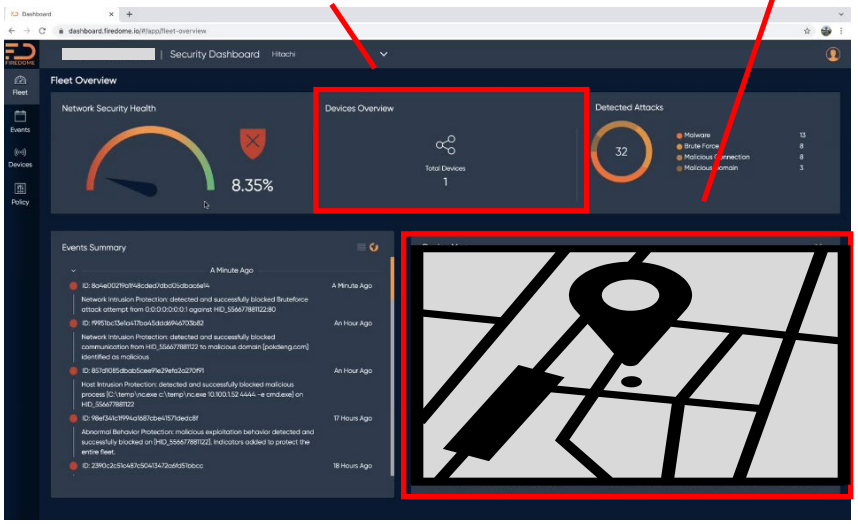
3-2.サイバー攻撃のシミュレーション

監視モニターから、IoTデバイスの状態をモニタリング

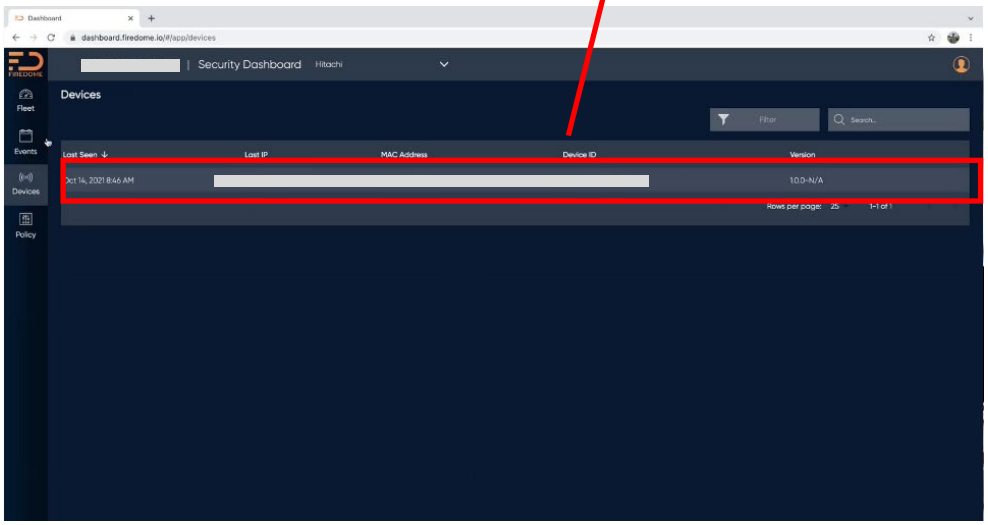
管理している
デバイス数

MAPによるデバイス
位置情報

デバイス情報



監視モニター

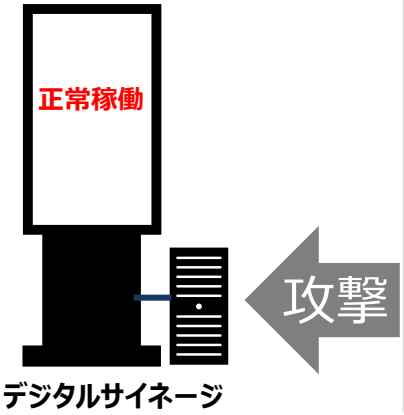


監視モニター

3-2.サイバー攻撃のシミュレーション

HITACHI
Inspire the Next

不正アクセス可能な
ポート番号として以下を検知
- **sshリモートログイン**
- **WebページHTTPサービス**
- **Remote Procedure サービス**
- **NetBIOSセッションサービス**
- **SMBサービス**
  （ファイル/プリンタの共有）
- **Remote Desktop**

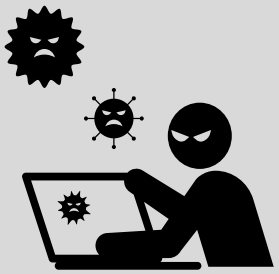


デジタルサイネージ

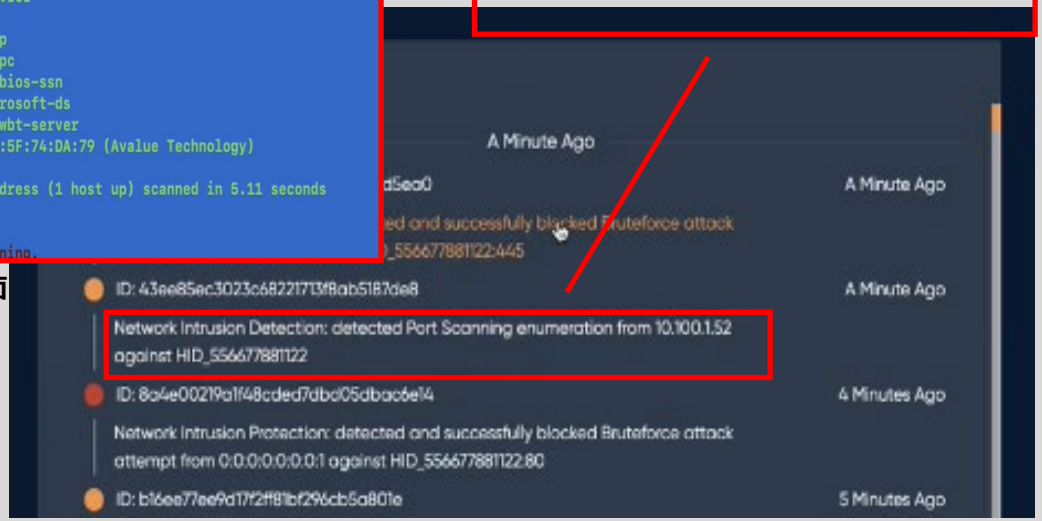
偵察 ポートスキャンによる攻撃対象の調査

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 05:15 UTC
Nmap scan report for 10.100.1.57
Host is up (0.0012s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:04:5F:74:DA:79 (Avalue Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds

Finished Port Scanning.
```

攻撃者の画面



監視モニターより、ポートスキャンの検知情報を確認



監視モニター

3-2.サイバー攻撃のシミュレーション

HITACHI
Inspire the Next

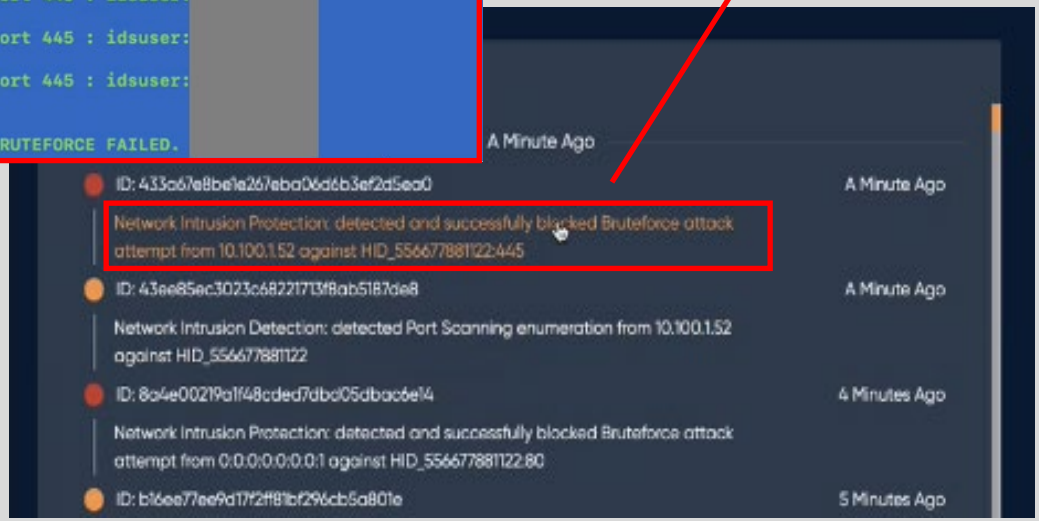
配達 **総当たり攻撃による不正アクセス**

総当たり攻撃の失敗

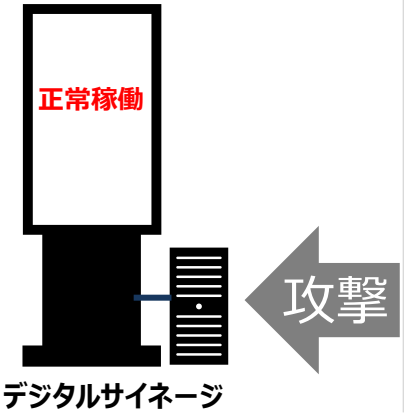
```
Bruteforce attack on port 445 : idsuser:
Bruteforce attack on port 445 : idsuser:
Bruteforce attack on port 445 : idsuser:
 Connection failed
Bruteforce attack on port 445 : idsuser:
 Connection failed
Bruteforce attack on port 445 : idsuser:
 Connection failed
Bruteforce attack on port 445 : idsuser:
 Connection failed
Bruteforce attack on port 445 : idsuser:
 Connection failed

CANNOT REACH TARGET, BRUTEFORCE FAILED.
```

攻撃者の画面

監視モニターより、総当たり攻撃の検知情報を確認



監視モニター



デジタルサイネージ

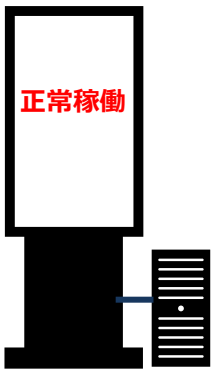
3-2.サイバー攻撃のシミュレーション

HITACHI
Inspire the Next

偵察 **ポートスキャンによる攻撃対象の調査**

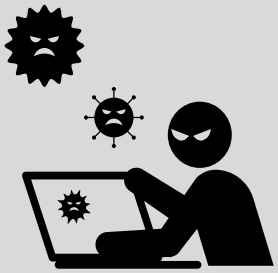
インストール **既知・未知のマルウェア実行**

サイネージの映像が変わらず正常稼働

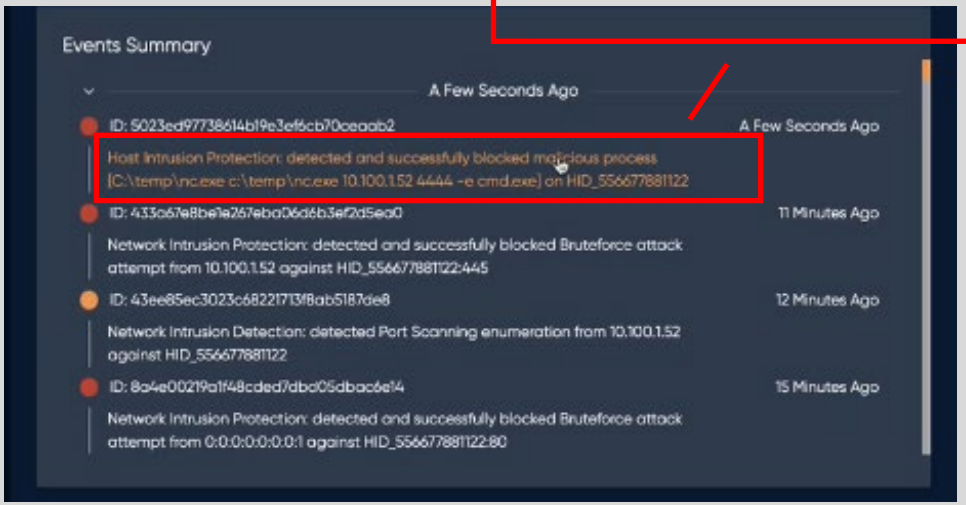


デジタルサイネージ

攻撃



監視モニターより、マルウェアの防御通知を確認



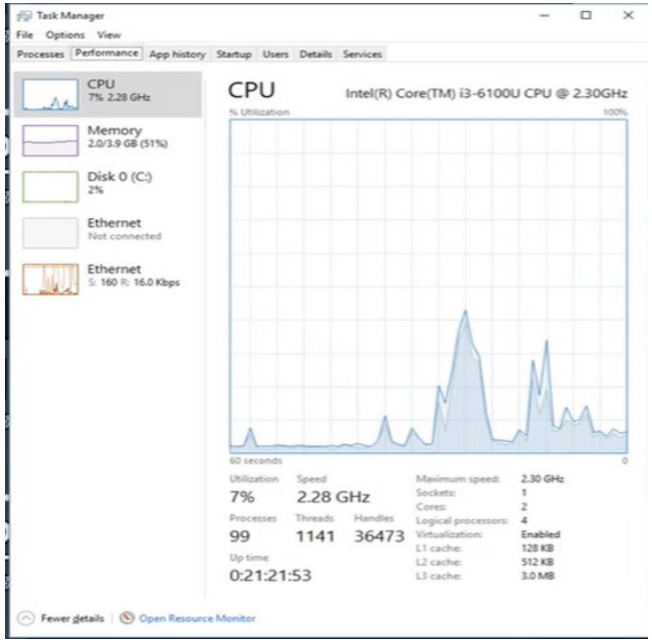
監視モニター

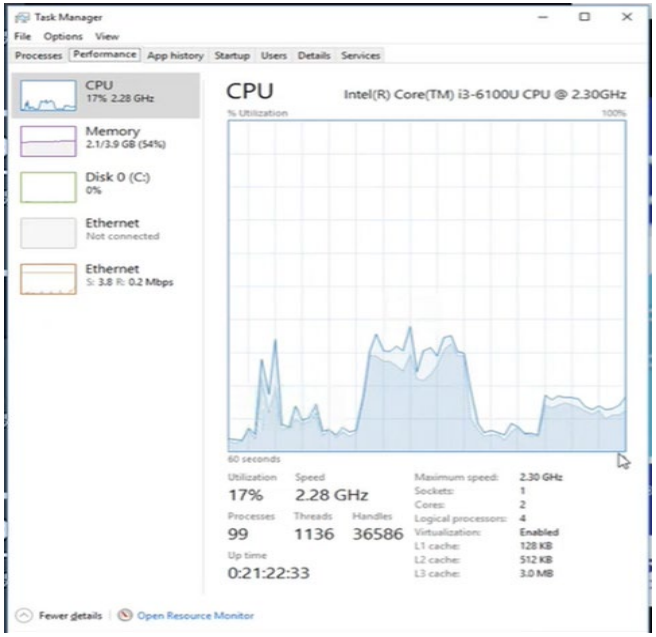
3-3.シミュレーション時のデバイスリソース情報

HITACHI
Inspire the Next

- **リソース情報（Firedome有り・無し）**

	Firedome　有り	Firedome　無し
CPU	7%	17%
Memory	51%	54%
Ethernet	16.0Kbps	200.0Kbps





3-４.サイバー攻撃のシミュレーション結果

HITACHI
Inspire the Next

Firedomeでは、
下記のようにサイバーキルチェーンに即した対策が取られています。

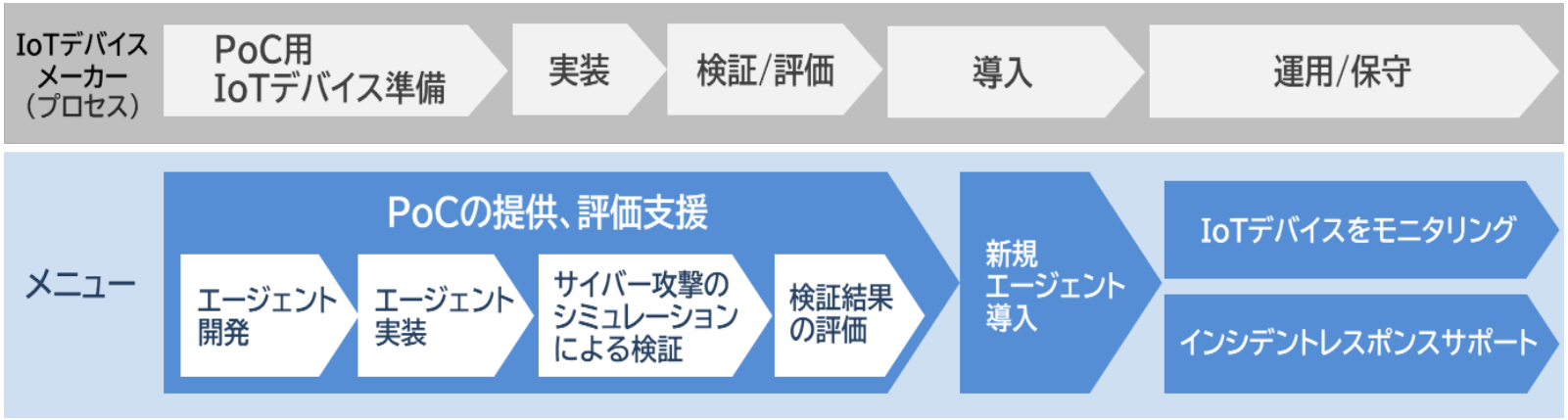
3- 5 .スケジュール（フィジビリティスタディ）

項目	担当	N月	N月＋1	N月＋2	N月＋3
イベント		▲ デバイス準備	▲ エージェント作成	▲ エージェントインストール 実機検証	▲ 検証まとめ/評価
デバイス選定&準備	デバイスメーカー				
デバイス評価環境構築	当社				
デバイスに対応した エージェント作成	Firedome社				
エージェントインストール	当社				
ビジネス検証 ・拡販シナリオ（ユースケース、ユーザーヒアリング）	当社 デバイスメーカー				
技術検証 ・スペック（負荷）検証 ・セキュリティ検証 ・運用検証	当社 Firedome社 デバイスメーカー				
POC検証結果まとめ	当社				
結果評価	当社 デバイスメーカー Firedome社				

HITACHI
Inspire the Next

IoTデバイス向けセキュリティソリューション

導入からその後の運用／保守までトータルでサポートします。
まずはPoC（有償）で効果を体験してください。
本ソリューションの導入前／導入後でサイバー攻撃をシミュレーションすることで、
有効性を確認いただきます。



HITACHI
Inspire the Next

ソリューションメニュー

ソリューション	提供形態	価格（税別）	備考
Firedomeソフトウェア エージェント作成費	売切り	￥4,000,000	・1製品（OS、ハード仕様が同じ）
Firedome エージェント 年間サブスクリプション	サブスクリプション／年間利用料	￥4,000,000	・1製品（OS、ハード仕様が同じ）無制限ライセンス
監視モニタリング利用料／検知・防御モニタリングサービス	年間利用料	￥6,000,000	・IoTベンダーへの定期的な分析レーポート
PoC検証支援サービス	売切り	個別見積	・技術検証、ビジネス検証支援
導入支援サービス	売切り	個別見積	・技術検証、ビジネス検証支援

補足資料　IoTデバイスセキュリティ対策ソフトの比較

HITACHI
Inspire the Next

セキュリティ対策	仕組み	運用
ブラックリスト型セキュリティ	動かしてはいけないプログラム、スクリプトをリスト化しデバイスに配布	**セキュリティの抜け穴が大きい** ・定期的にウイルス定義ファイルの更新が必要 ・フルスキャンが必要 ・デバイスに負荷を与える
ホワイトリスト型セキュリティ	動かしても良いプログラム、スクリプトをリスト化しデバイスに配布	**維持するための運用負担が大きい** ・ウイルス定義ファイルの更新は不要 ・フルスキャンは不要 ・デバイスに負荷を与えない ・新しいアプリケーションを追加、アプリケーションのアップデートによる更新時にリストの見直しが必要
Firedome	Firedomeのエージェントをインストール ・ふるまい、AI機械学習、ヒューリスティック、脅威インテリジェンスエンジンによる検知 ・プロセス監視、ネットワークの不正アクセス監視を行い悪意のあるアクティビティをブロック	**デバイスセキュリティ監視の運用負荷低減** ・ウイルス定義ファイルの更新は不要 ・フルスキャンは不要 ・デバイスに負荷を与えない ・デバイス監視サービス(24時間365日 監視)

お問い合わせ

HITACHI
Inspire the Next

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

ご相談、ご依頼いただいた内容は、回答等のため、当社親会社（株式会社日立ソリューションズ）、親会社の関連会社及び株式会社日立製作所に提供（共同利用も含む）することがあります。取り扱いには十分注意し、お客様の許可なく他の目的に使用することはありません。

表示に関する注意事項

■他社商品名、商標などの引用に関する表示

- Firedomeのロゴ及び製品名は米国法人Firedome, Inc.の米国における登録商標、または商標です。
- Windows、AzureはMicrosoft Corporation の米国及びその他の国における商標または登録商標です。
- Androidは、Google Inc.の商標または登録商標です。
- FreeRTOSは、Amazon Web Services, Inc.の米国及びその他の国における登録商標もしくは商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2022年4月現在のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。