HITACHI

未許可PCの通信遮断「ネット助っ人交番」

株式会社日立システムズ
公共プラットフォーム事業部
アドバンスドサービス本部
第一サービス部
第一グループ

Contents

1. 最近のセキュリティトピックス

HITACHI

1-1. 情報セキュリティ10大脅威 2025

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

「ランサムウェアによる被害(1位)」が年々増加しています！

アラートを検知してから、解析/特定/判断/処置など、人手対応では時間がかかります。

不正持ち込み端末がランサムウェアの起点になり、「内部不正による情報漏えいなどの被害(4位)」になることもあります。

不正接続端末は即時自動切り離しが必要です！

2024年もランサムウェアによる被害が 1 位でした。

情報セキュリティ10大脅威 2025 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

HITACHI

1-2. ランサムウェアとは

ランサムウェア

ランサム(身代金)を奪う目的のマルウェア。
交渉に応じない場合は暗号化データの非復旧やネットへのデータ公開等の手法で脅迫し身代金を要求する。

攻撃者の狙い

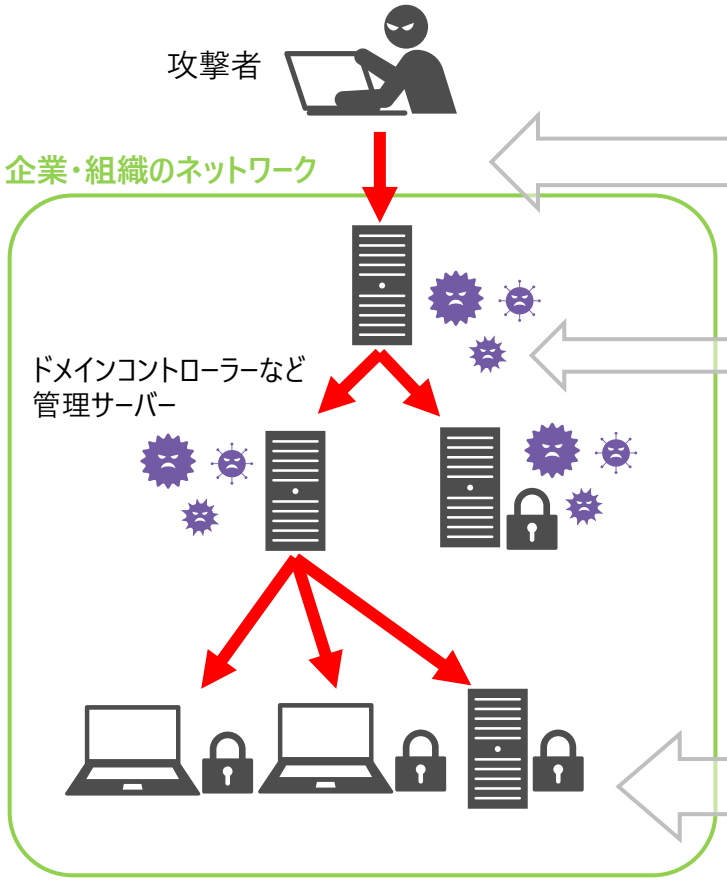
(1)被害企業、組織が自力でデータやシステムを復旧するのにかかる平均的な費用よりも、身代金を支払った方が低価格
(2)業務が止まると損失が大きい業種を狙い、早急な支払いを促す

実際に

(1)受発注システムが感染し工場の操業を一時停止した組織
(2)莫大な身代金を支払って復旧させた組織

HITACHI

1-3. ランサムウェアの活動 5 ステップ



1. ネットワークへの侵入
リモートデスクトップサービスを経由した侵入、VPN装置のぜい弱性を悪用した侵入、メール記載のURLリンクからウイルス感染させて端末を乗っ取ることによる侵入。

2. ネットワーク内の侵害範囲拡大
ネットワーク構成の把握や管理者権限の奪取を行い移動する。

3. データの窃取 (二重の脅迫の場合)
企業、組織の機微情報等のデータの探索、収集、
攻撃者のサーバーやクラウドストレージへのアップロード等が行われる。

4. データの暗号化、システム停止
企業、組織のデータを暗号化する。
暗号化によって、システムの停止にもつながる。

5. 窃取したデータの公開 (二重の脅迫の場合)
窃取したデータの公開方法として、リークサイトでの公開や、オークションサイトでの販売が挙げられる。

(出典)【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について | アーカイブ | IPA 独立行政法人 情報処理推進機構

HITACHI

1-4. ランサムウェア対策

1. 対策全般
システム設計、装置セキュリティ、運用管理、人的体制等で多層の対策を講じる

2. 企業・組織のネットワークへの侵入対策
攻撃対象領域の最小化、アクセス制御と認証、ぜい弱性対策、攻撃メール対策

➡ **ネット助っ人交番で対策**

脅威の局所化

(1)内部脅威対策:許可された端末のみ通信許可
(2)外部脅威対策:「UTM/EPP連携」で侵害範囲の拡大防御をアシスト

3. データ、システムのバックアップ
適切なデータバックアップと復旧計画の整備

4. 情報窃取とリークへの対策
IRM(Information Rights Management)等の情報漏えい対策、重要データ・システムのセグメント化

5. 事業継続計画(BCP)、対応方針
事業継続計画(BCP)の策定、厳しい状況でのインシデント対応の説明責任

6. インシデント対応
影響範囲の特定、計画、封じ込め、根絶と復旧

2. ネット助っ人交番(NSK)の主要機能のご紹介

HITACHI

2-1. ネット助っ人交番(NSK)について

◆概要

ネットワーク接続が許可されていない端末を、自動的に検知、遮断し、組織内ネットワークのセキュリティ脅威を排除します。

1 接続端末の可視化

組織内ネットワークの端末接続状況を
自動で見える化が可能。

2 不正接続検知、遮断を自動実行

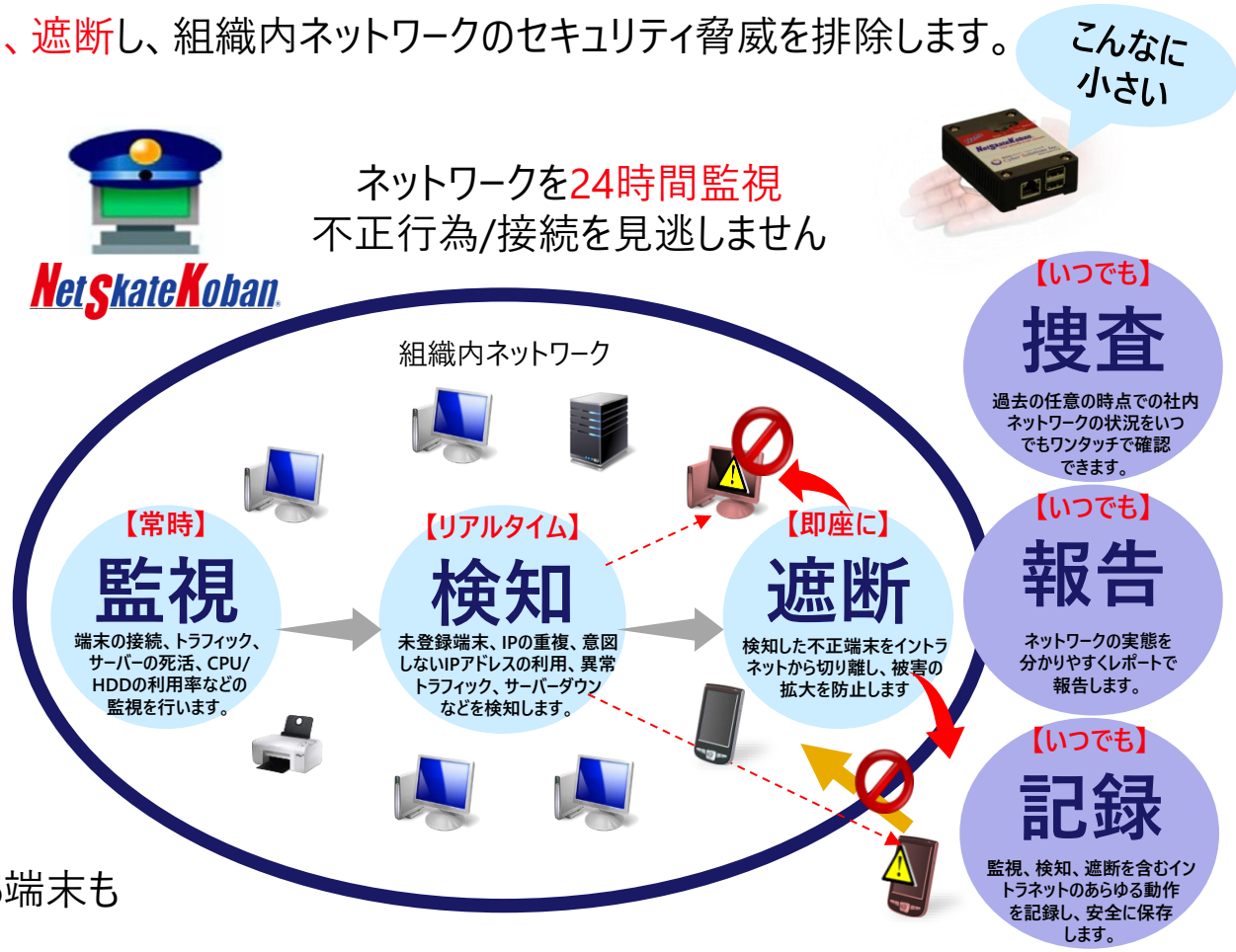
人手を介すことなく自動検知、遮断するので、
対応工数とリスク低減が可能。

3 UTM/EPP連携

FortigateなどのUTMやEPP(アンチウィルスソフトウェア)との連携により、脅威を検知した端末を遮断するとともに、物理的な位置も把握できるので、速やかな対処が可能。

4 ネットワーク構成図を自動作成

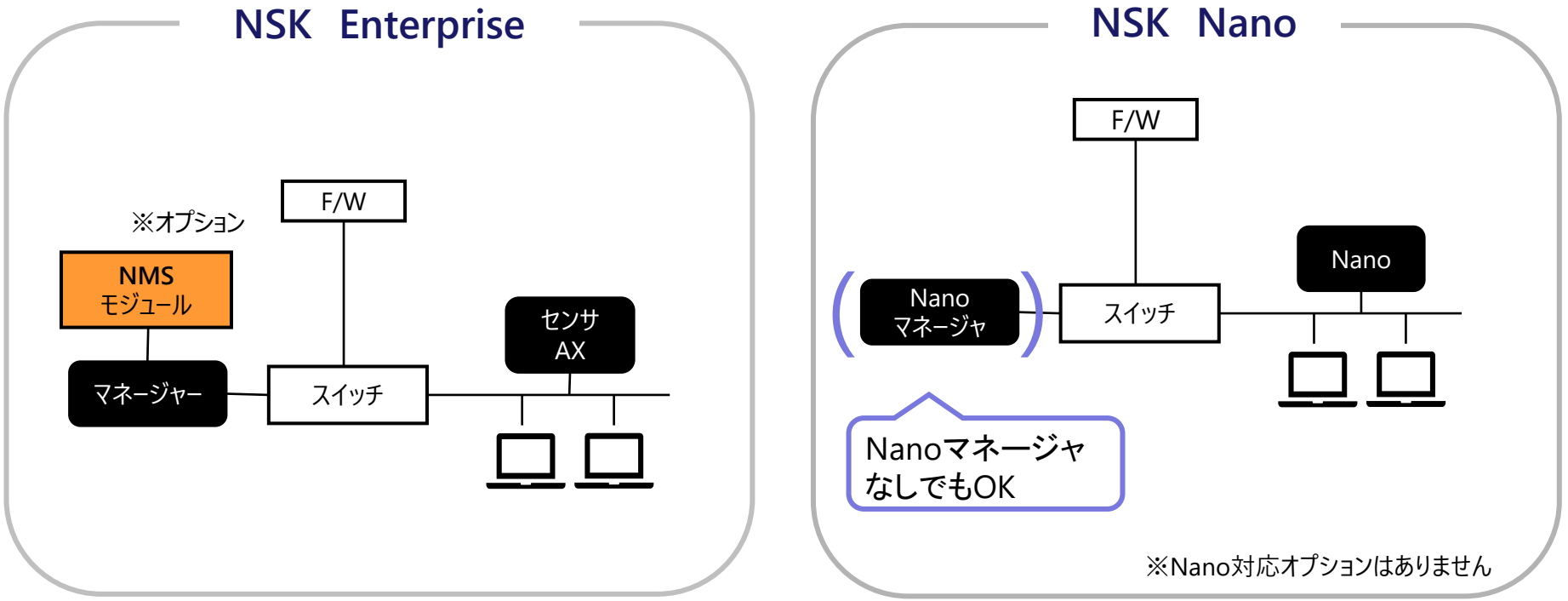
ネットワーク構成図は、有線LAN以外にも、Wi-FiやIPv6端末も
自動で検知、作図するので、対応工数の低減が可能。



HITACHI

2-2. 製品構成概要

シンプルな端末接続監視から、さまざまなオプションに対応しています。



項番	製品名	備考
1	マネージャー	システムの中心となるサーバー機能
2	センサAX	対象セグメントの情報収集・遮断を実施
3	NMSモジュール	ネットワーク地図の自動作成(オプション)
4	Nano	マネージャー・センサーを１製品に集約

HITACHI

2-3. 主要機能１:接続端末の可視化

– 現在のネットワーク環境 –

組織内ネットワークに接続されている機器の全数把握ができていない。

– よくある課題 –

資産管理ソフトウェアを導入しており管理台帳に一致する機器の把握はできるが、未登録機器の接続把握ができない。

HITACHI

2-3. 主要機能 1 :接続端末の可視化

ワンクリックで「ホワイトリスト」への登録が可能。

– 課題解決 –

NSK Nanoを導入。

接続するだけで、ネットワークに接続されている端末情報を自動的に収集し、検知端末一覧で表示します。

– お届けする価値 –

1 自動で接続機器の管理ができる。

2 アクティブ検知で非通信機器(プリンターやスキャナーなど)も検知し、端末一覧を作成できる。

HITACHI

2-4. 主要機能2:不正接続検知、遮断の自動実行

– 現在のネットワーク環境 –

未許可端末をネットワーク接続させない仕組みがない。

– よくある課題 –

Wi-Fi利用などの未許可端末の把握、制御ができておらず、不正接続による情報漏えいリスクを抱えている。

HITACHI

2-4. 主要機能2:不正接続検知、遮断の自動実行

－ 課題解決 －

NSK Nanoを導入。

1 接続機器の管理。

2 不正接続端末の自動検知・遮断。

－ お届けする価値 －

1 接続されている機器が把握できるようになることで
管理、監視が可能になる。

2 検知、遮断を自動で実施することで
情報漏えいリスクを抑えられる。

3 ホワイトリストに登録済端末は通信可能。
ホワイトリストに未登録端末は通信遮断。

(参考)
社内の無線LAN利用状況について、60.5%の従業員が社内ネットワークに私用端末を接続している。
→従業員がスマートフォンやノートパソコンを無線LANに接続することで、知らないうちにぜい弱性が生じ、情報漏えいや不正アクセスのリスクが高まる。
(出典)
社内ネットワークの危機！私用端末の接続実態とセキュリティリスクを再認識しよう | 法人向けサポートサイト【ビジ助channel】

HITACHI

2-5. 主要機能3:UTM/EPP (アンチウイルスソフトウェアなど)連携

– 現在のネットワーク環境 –

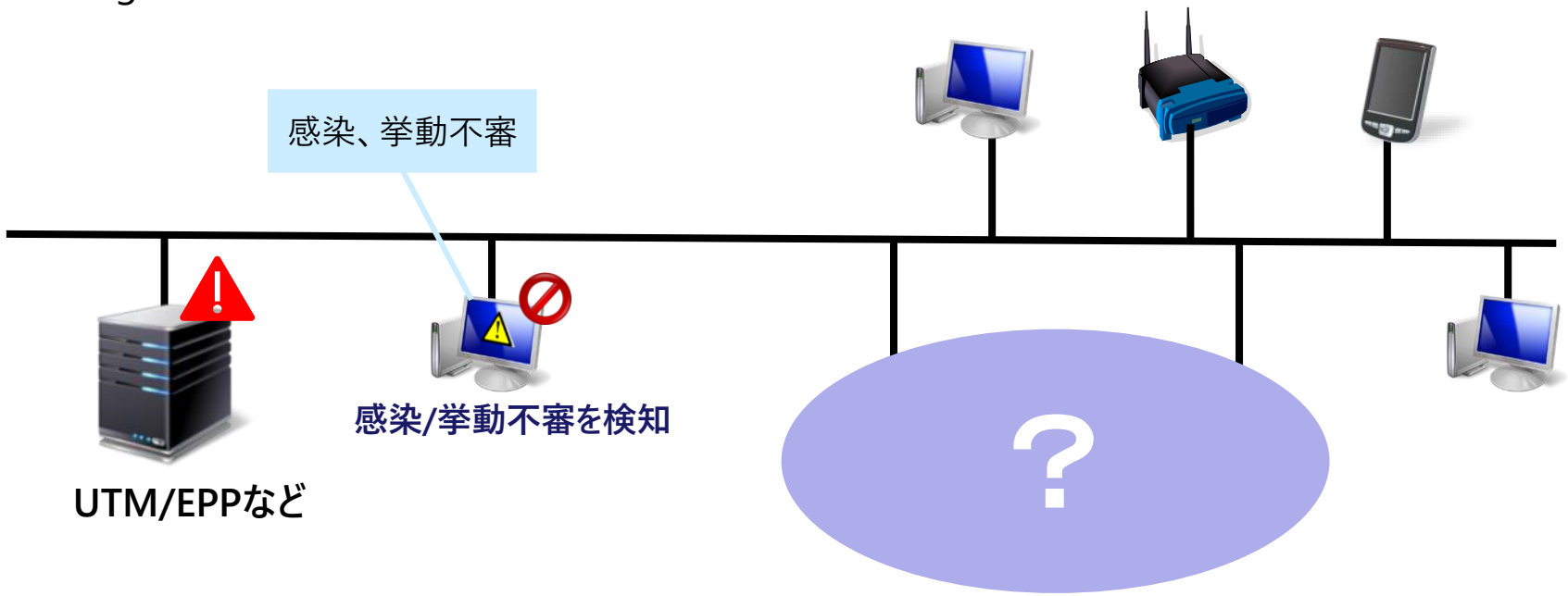
マルウェア感染の疑いのある機器を手動で切り離ししている。

脅威

IPA 情報セキュリティ10大脅威 2025
1位 ランサムウェアによる被害
4位 内部不正(不正接続)による 情報漏えい(対策)

– よくある課題 –

不正接続から接続遮断までにタイムラグが発生してしまう。
※Fortigateで境界は守っているが内部のセキュリティも向上させたい。



HITACHI

2-5. 主要機能3:UTM/EPP (アンチウイルスソフトウェアなど)連携

※詳しくは、「付録４」をご覧ください。

－ 課題解決 －

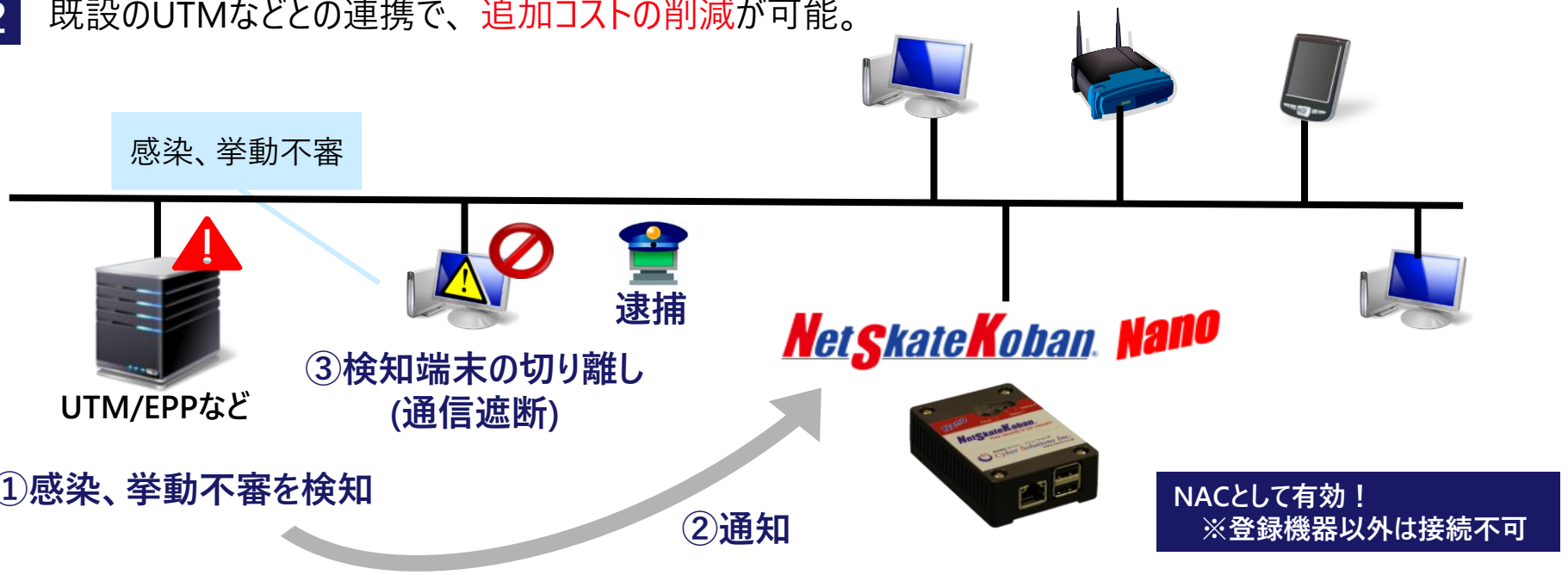
NSK Nanoを導入。 ▶ UTM/EPP(アンチウイルスソフトウェア)などの連携により即時切り離しが可能。

－ お届けする価値 －

◎ピンポイントで外部、内部の両通信を遮断し感染防止

1 機器の即時自動切り離しで、脅威の局所化が可能。※内部セキュリティ向上

2 既設のUTMなどとの連携で、追加コストの削減が可能。



HITACHI

2-6. 主要機能4:ネットワーク地図の自動作成

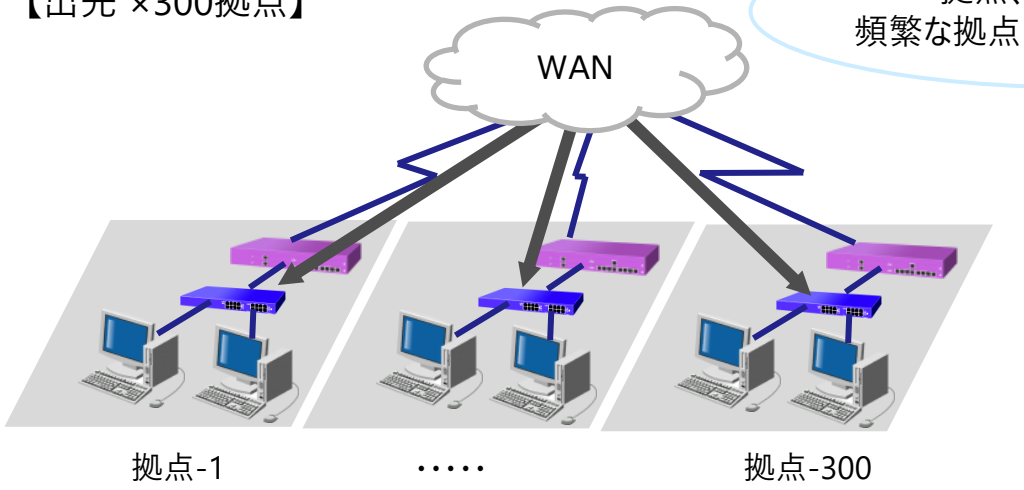
– 現在のネットワーク環境 –

多拠点におけるレイアウト変更、接続機器の管理を手動で実施している。

– よくある課題 –

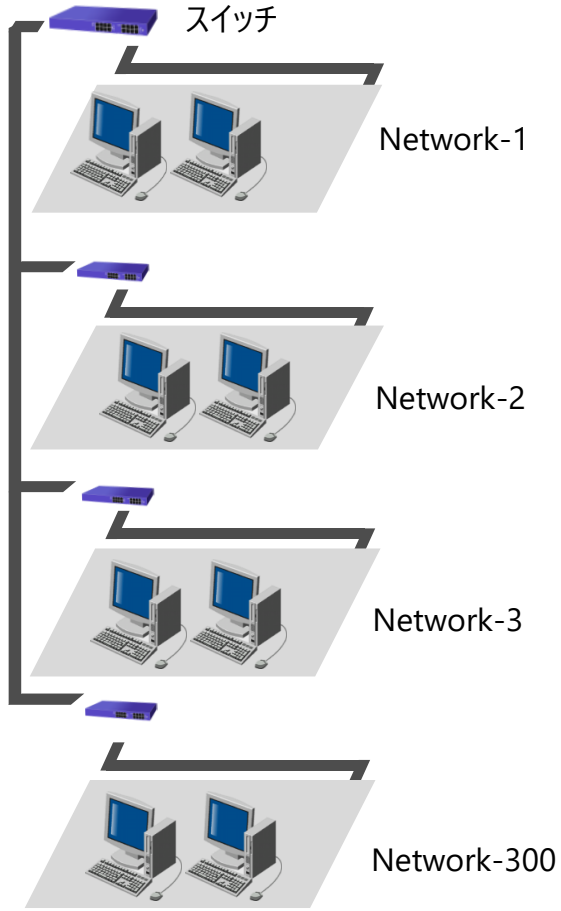
1. 頻繁なレイアウト変更は、人による対応工数がかかる。
2. 障害発生時の機器特定には、ネットワーク接続図と
フロアレイアウト図の両方を参照する必要があり煩雑。

【出先 ×300拠点】



拠点、装置多すぎ。。。
頻繁な拠点内変更の反映は無理

【本庁】



HITACHI

2-6. 主要機能4:ネットワーク地図の自動作成(L2MAP)

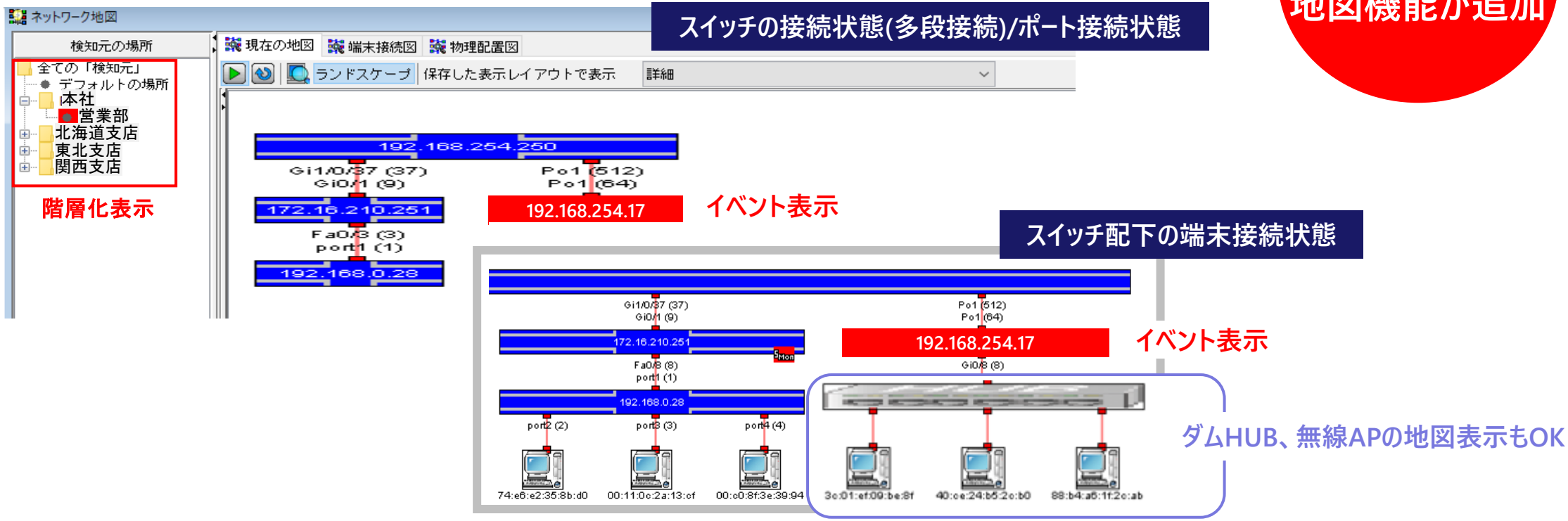
– 課題解決 –

NSK Enterprise、NMSモジュール、センサAXを導入。 ▶ ネットワーク地図の自動作成(L2MAP)

– お届けする価値 –

自動でネットワーク接続図を作成し、管理者の負担軽減ができる。

25年6月より
Nanoへ
地図機能が追加



HITACHI

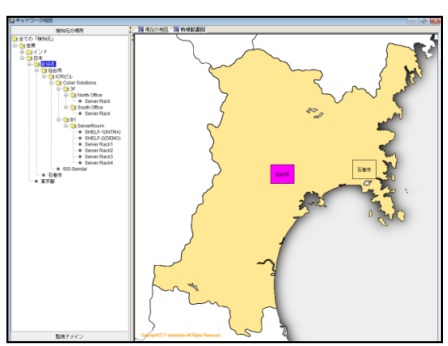
2-6. 主要機能4:ネットワーク地図の自動作成(物理配置) ※Enterprise版のみ

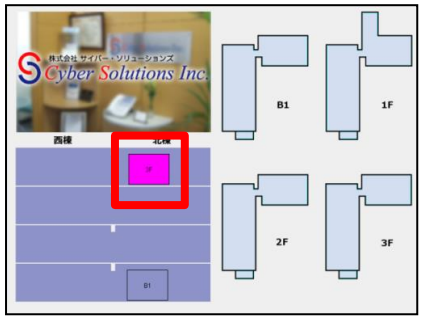
－ 課題解決 －

NSK Enterprise、NMSモジュール、センサAXを導入。 ▶ フロアレイアウト図のマッピングが可能

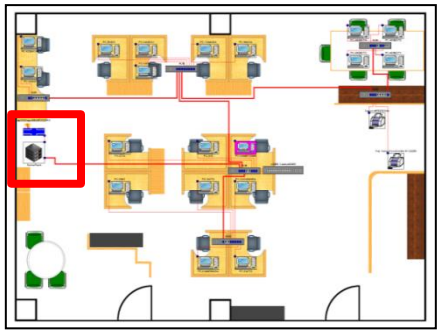
－ お届けする価値 －

ネットワーク接続図とフロアレイアウト図が1画面で表示され、接続機器の見える化を実現。





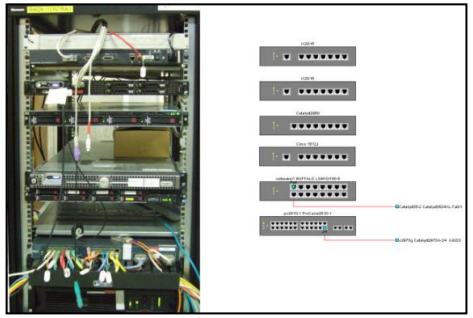
12F



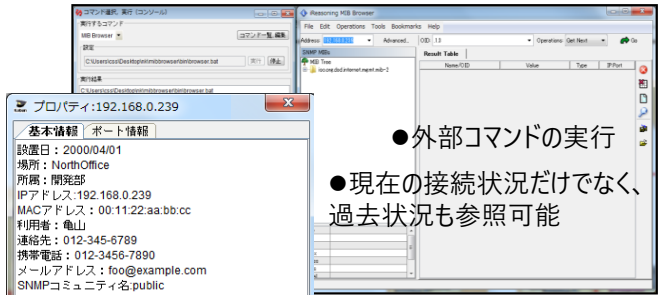
●階層ごとの物理配置図で直観的に監視対象機器を管理

●イベントが発生した場合、ハイライトを追跡することで原因を特定

12F Server Rack

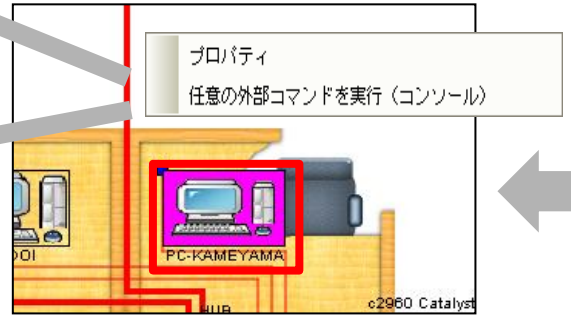


●機器やLANケーブルのプロパティ情報の管理



●外部コマンドの実行

●現在の接続状況だけでなく、過去状況も参照可能



HITACHI

2-7. ネット助っ人交番(+Fortigateなど)による内外脅威対策

※1　NSKにより、外部脅威だけでなく、内部脅威の対策が可能となる。

※2　C＆Cサーバーへの通信を検知した際、NWの出口（境界）だけでなく、端末単位で遮断可能　【ダメージ局所化できる】

※4　NGAVを導入することにより、AI/ふるまい検知が可能となる。NSK+FGは費用対効果が高い。

（凡例）
◎：優良（機能あり）
〇：良（機能あるが一部制限あり）
△：可（機能あるが制限あり）
×：不可（機能なし）

	内部脅威対策（内部統制、セキュリティポリシー）		外部脅威対策				評価
脅威	故意による内部不正		不正アクセス		マルウェア(ランサムウェアなど)		
内容	不正端末接続		標的型攻撃 C＆Cサーバー通信		標的型攻撃 マルウェア感染		
対策	構成の可視化による最新情報把握	シャドウIT排除	C＆Cサーバー通信遮断（NW境界での遮断）	C＆Cサーバー通信遮断（対象端末遮断）	マルウェアブロック（シグネチャベース）	マルウェアブロック（ふるまい検知）	
ネット助っ人交番(NSK)	◎	◎	–	–	–	–	内部対策に有効
Fortigate(FG)	–	–	◎	×	△ URL/IPﾏｯﾁすれば通信遮断(NW遮断)	△ URL/IPﾏｯﾁすれば通信遮断(NW遮断)	**外部対策に有効**
NSK+Fortigate(FG)	◎ ※1	◎ ※1	◎ ※2	◎ ※2 LAN内の感染拡大抑止	〇 URL/IPﾏｯﾁすれば通信遮断(端末遮断可能)	〇 URL/IPﾏｯﾁすれば通信遮断(NW遮断)	**費用対効果高（内部＋外部）**

3． 製品ラインアップ

HITACHI

3-1. 製品と規模間比較

オプションを追加し、高度な監視を実現できます

HITACHI

3-2. 代表的な製品一覧

項番	製品名 Nano	備考
1	NetSkateKoban Nano	ネットワークへ不正接続した端末の自動検知・遮断が可能、接続リストの自動作成も実施
2	NetSkateKoban Nano(V)	Nanoの複数ネットワーク対応装置（10VLAN対応モデル 、40VLAN対応モデルあり）
3	NetSkateKoban Nanoマネージャ	Nanoを持つ複数の組織を容易に管理(接続端末状況を一覧で確認)するためのツール

項番	製品名 Enterprise	備考
1	マネージャアプライアンス	Nanoの機能に加えネットワークの可視化が可能 （1万台対応モデル、2万台対応モデル、冗長化対応モデル、仮想基板用モデルあり）
2	マネージャ	サーバーインストールモデル（Windows版、Linux版あり）
3	センサAX（選択*1）	監視対象ネットワークに設置する装置（1セグメント対応）
4	マルチVLANセンサAX/EX （選択*1）	センサAXの複数のネットワーク(VLAN)対応装置 （AX：16VLANまで対応、EX：200VLANまで対応）

項番	製品名 オプション	備考
1	NMSモジュール	ネットワーク地図の自動作成やフロアレイアウトのマッピングが可能
2	エンタープライズ SwiMonモジュール（選択*1）	既存のインテリジェントスイッチと連携し社内ネットワーク内への不正接続防止と接続状況の把握できるスイッチ連携モジュール
3	RtrMonセンサEX (RtrMonモジュール)（選択*1）	端末のMACアドレスとIPアドレス情報を収集し、不正接続端末を検知 （ルーター200台まで対応、仮想基盤用モデルあり）
4	DHCPサーバ連携モジュール	DHCPサーバーのMACアドレスフィルタと連携し、未登録端末へのIPアドレス振出しを阻止
5	DBシンクロナイザー	資産管理システムと連携し、製品単体では実現できなかった高度な管理が可能
6	Webコンソール	NetSkateKobanの主要な機能を、Webブラウザーから操作、利用することが可能

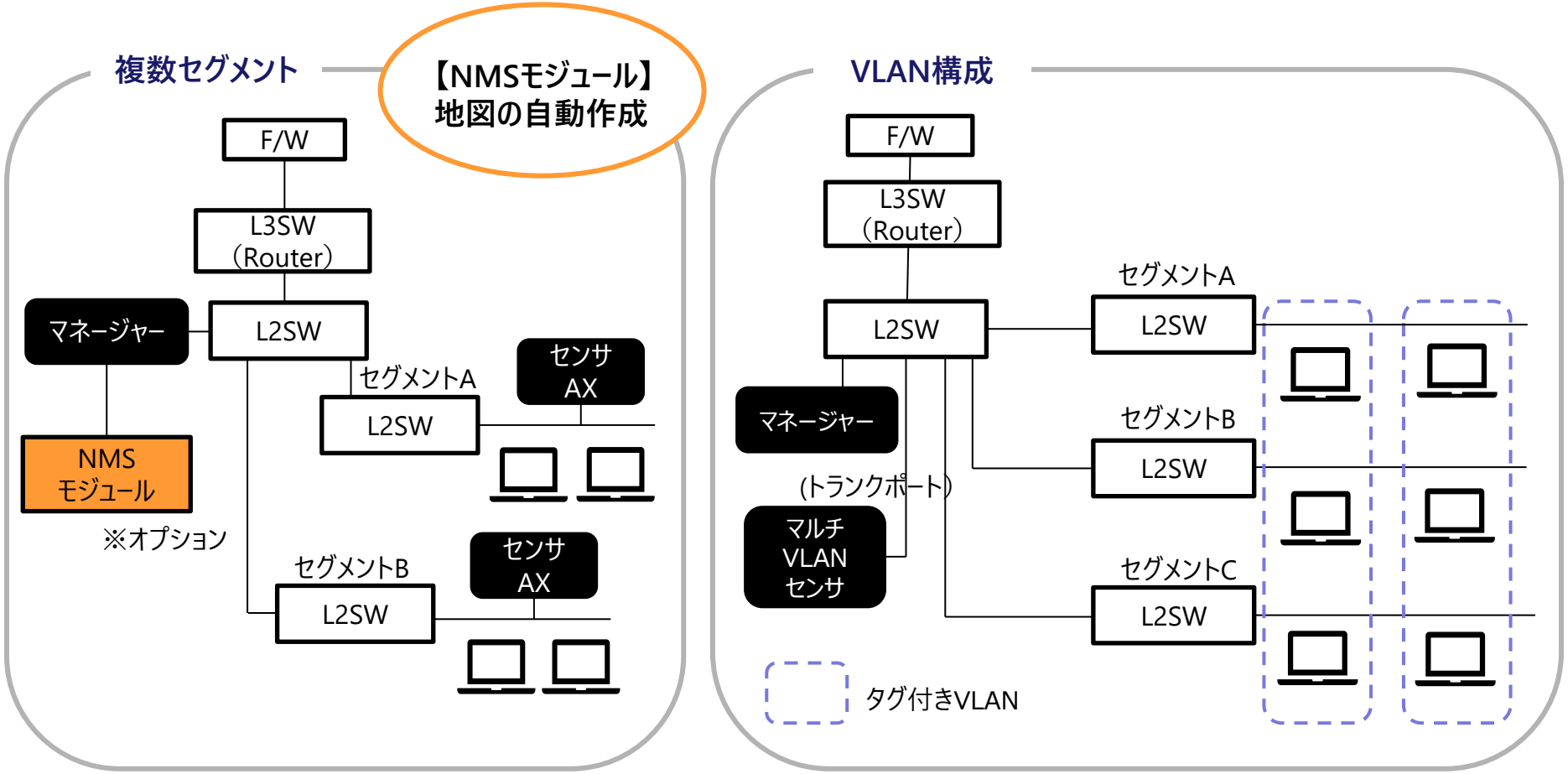
*1 センサーはEnterprise利用時に構成により選択となります。

HITACHI

3-3. 構成例(NSK Enterprise その1)

主要機能 4

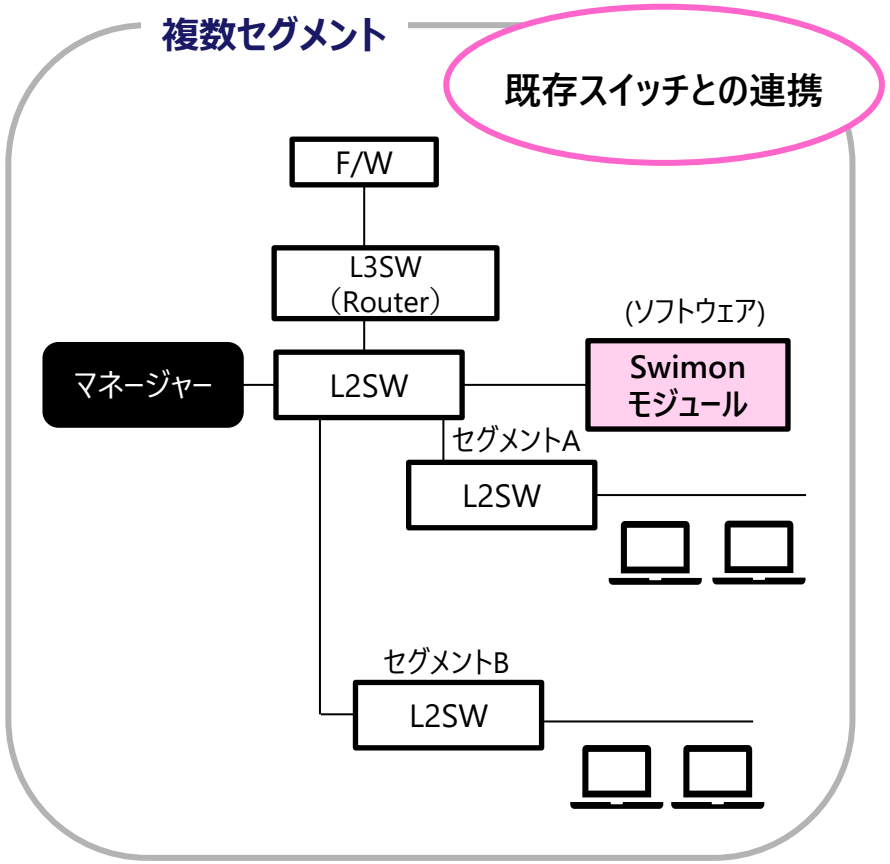
シンプルな端末接続監視から、さまざまなオプションに対応しています。

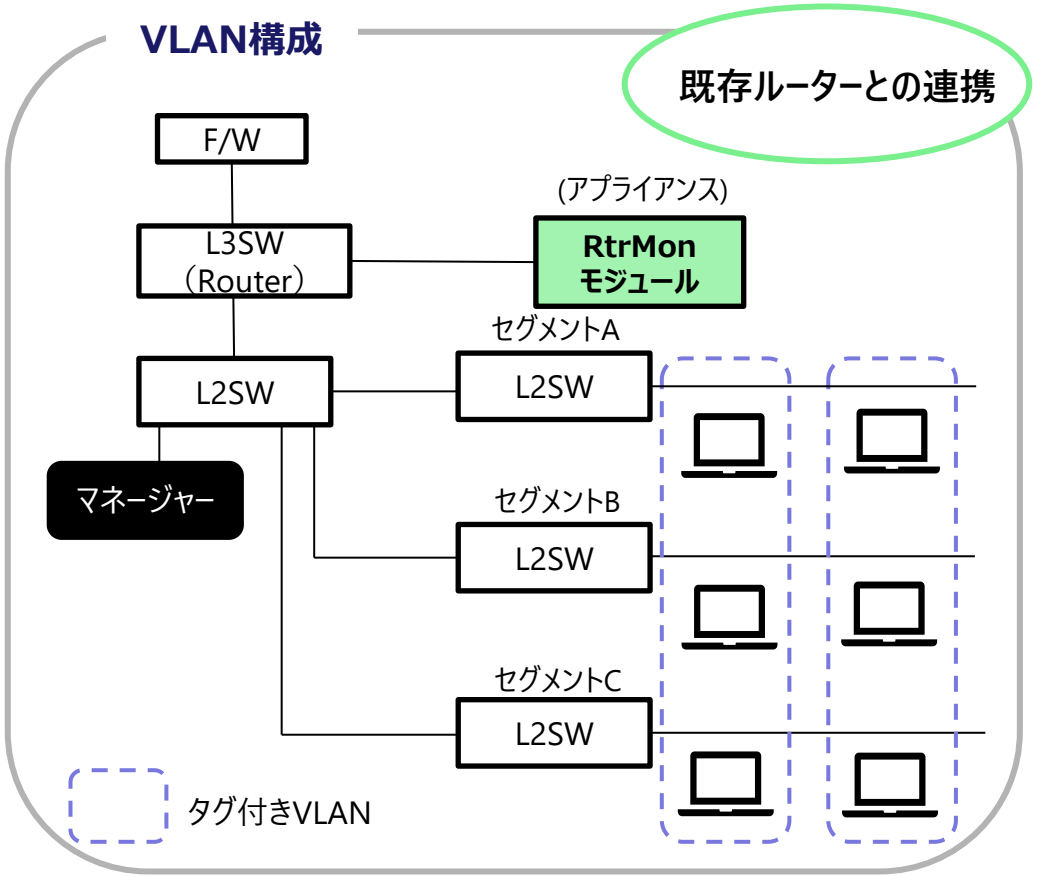


HITACHI

3-4. 構成例(NSK Enterprise その2)

既存スイッチやルーターと連携が可能で、お客さまシステム構成変更なしに導入ができます。
センサーに代わって監視装置としてスイッチ又はルーターが利用でき、現地にセンサーを置く必要がありません。



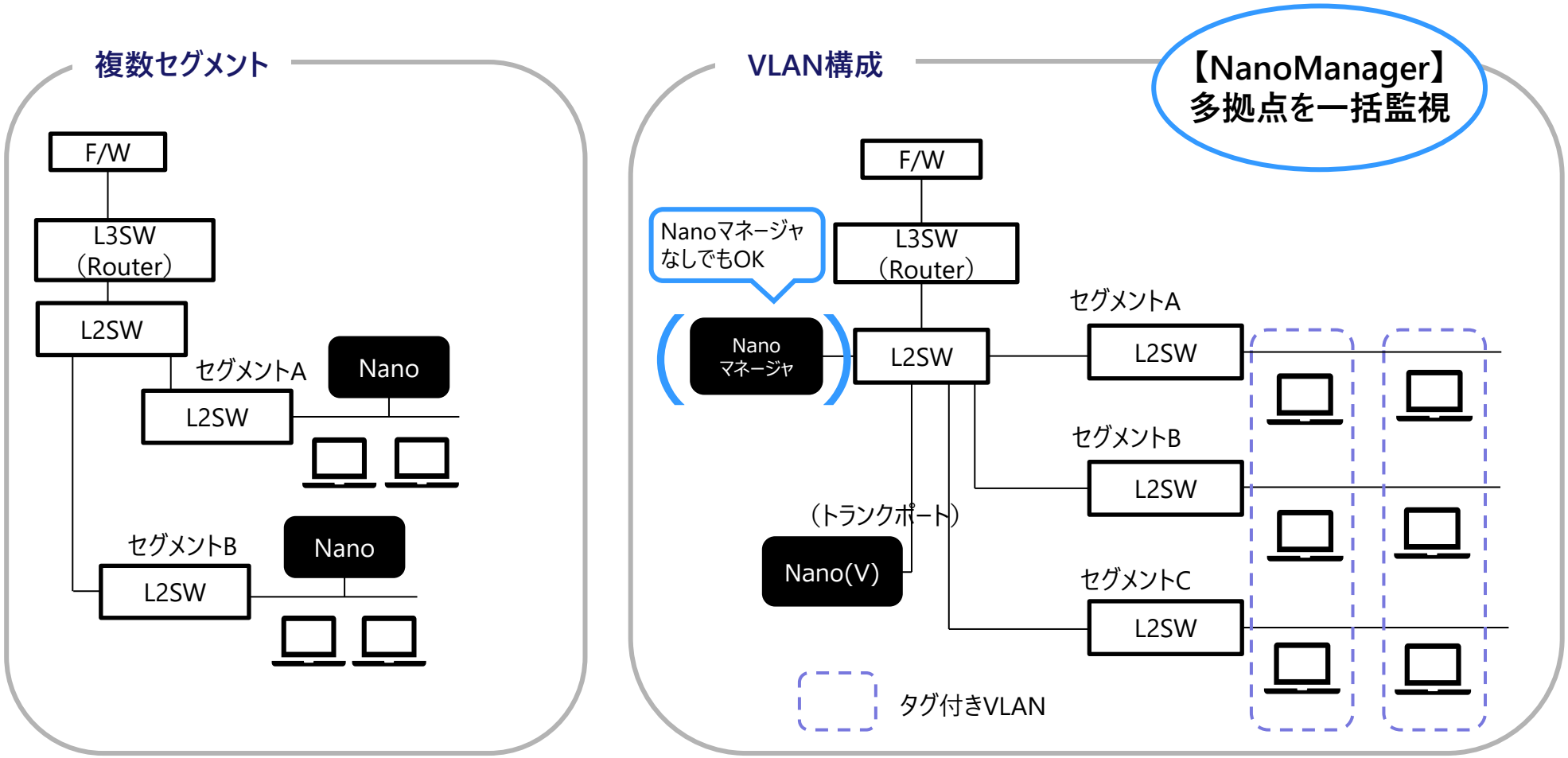


HITACHI

3-5. 構成例(NSK Nano/Nano(V))

主要機能1,2,3

小規模から多拠点の監視など幅広く対応できます。



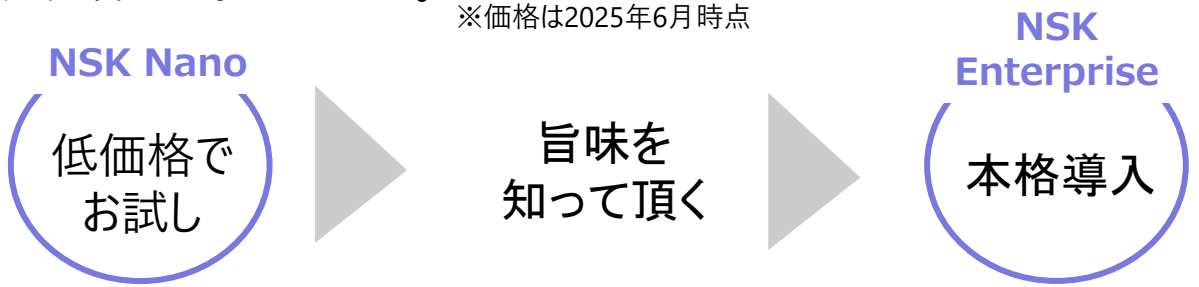
4. お客さまへのおすすめポイントまとめ

HITACHI

消耗品枠として低価格に購入できる

スモールスタート可能

NSK Nanoは9万円台から導入できます。 ※価格は税抜き表示です。別途消費税がかかります。
※価格は2025年6月時点



	NSKで実現できること	おすすめポイント	備考
1	低価格	9万円台で導入できる、消耗品枠で購入可能。 ※価格は税抜き表示です。別途消費税がかかります。 *他社製品は10万円を超えるため固定資産となる。	
2	小スペース対応	マグネット設置可能。*1 *他社は筐体が大きく重い。	
3	接続端末の可視化	接続するだけで、組織内ネットワークに接続されている機器一覧を表示できる	主要機能1
4	不正端末検知・遮断	・未許可端末の遮断が可能。 ・ネットワークのアドオンで実現可能。※既存ネットワークの変更不要。 ・端末へのエージェントインストール不要。	主要機能2
5	既存のUTM/EPPなどとの連携	・不審なふるまいをFortigateで検知 → NSKで遮断が可能。 ・マルウェアの拡散範囲拡大を防ぐ → ランサムウェア対策に有効	主要機能3
6	ネットワーク地図の作成	・自動で構成図が作成可能。 ※1回/日で更新機能あり ・接続されている機器の洗い出しに便利。	主要機能4

*1 オプションです。

5. さいごに

HITACHI

製品についてもう少し詳しい説明をご用意しております。
ご興味がございましたら補足資料をご案内しますので、お声がけをお願いします。

補足資料		概要
1	NSK監視・遮断開始までのフロー編	NSK監視までの流れと手順
2	ネットワーク地図の自動作成編	ネットワーク地図の作成例
3	モジュール編	5つのモジュールの機能
4	オプション編	スイッチ構成図 閾値、到達性監視
5	ポリシー管理編	ポリシーの詳細(簡易、高度)
6	オプション無しで他にできること編	基本の「収集・検知・遮断」以外にオプション無しでできる機能
7	製品リスト編	NSKの製品ラインアップ NSKのスケール比較 他社製品との比較表
8	Nano編	Nanoの機能 スタートガイド
9	構成例編	10の事例と構成例の紹介

HITACHI

END

未許可PCの通信遮断「ネット助っ人交番」

株式会社日立システムズ
公共プラットフォーム事業部
アドバンスドサービス本部
第一サービス部
第一グループ

HITACHI