\Orchestrating a brighter world NEC

InfoCage 不正接続防止(通常版) 紹介資料

NEC InfoCage不正接続防止窓口　2025年1月

はじめに

セキュリティ対策は、企業の規模を問わず、今やあらゆる企業に欠かせません。

多くの企業が、社内のPCに対して、ウイルス対策ソフトの導入や、外部記録メディアの禁止といった対策を実施しています。

しかし、社外から持ち込まれたPCに対する対策はできていますか？

持ち込みPC対策における課題

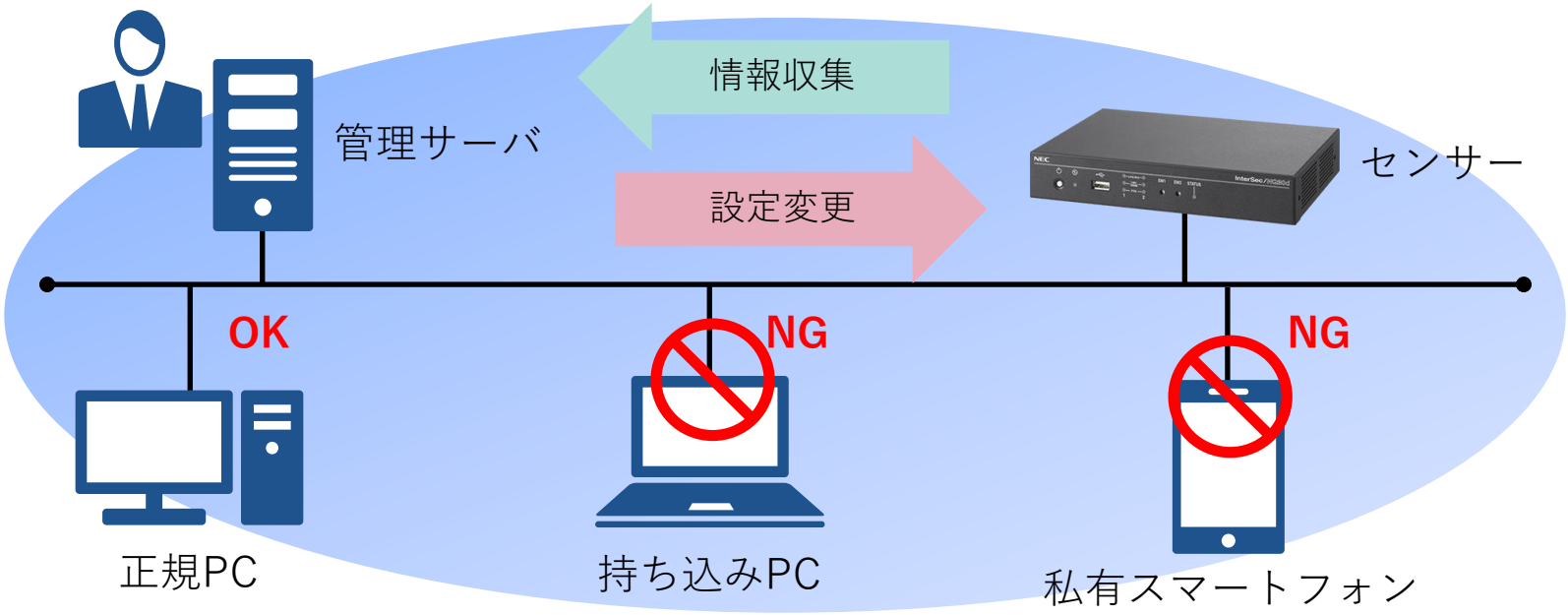
- 不十分な持ち込みPC対策によって発生する問題
  - 内部犯行による不正アクセス
  - ウイルスに感染したPCのネットワーク接続によるウイルスの蔓延

- 持ち込みPC対策に対するネットワーク管理者の声
  - 高価なシステムは簡単には導入できない。
  - ネットワークの設定変更はできるかぎり避けたい。

不正アクセスやウイルスによる被害は**情報漏えい事故**を引き起こし、
損害賠償や**社会的信用の失墜**に繋がります。

InfoCage 不正接続防止とは

- ネットワークに接続された端末をセンサーが自動的に検知し、不正に接続された端末の通信を遮断します。
- 検知した端末情報は管理サーバ上で集中的に管理できます。

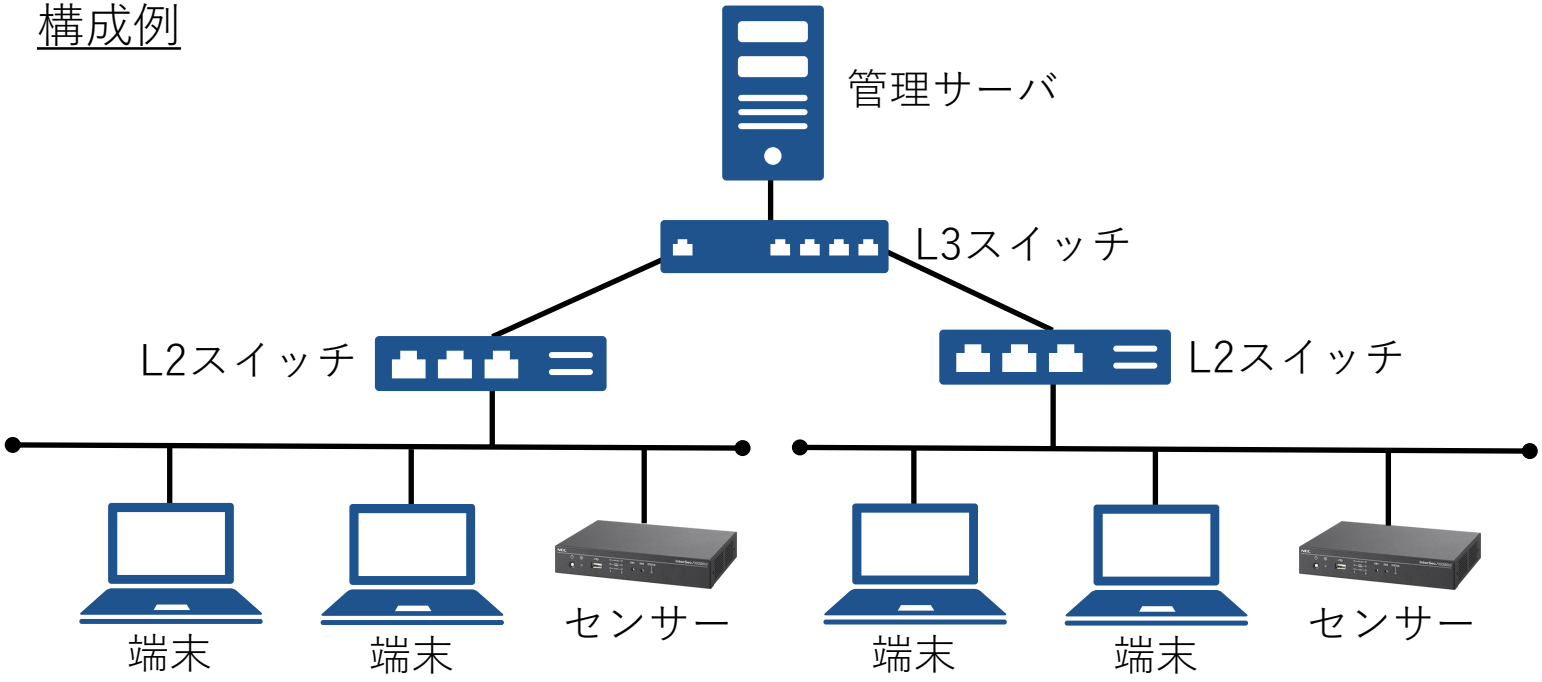


不正な端末のネットワークへの接続を防止し、
不正アクセスやウイルスからネットワークを守ります。

簡単導入

- エージェントレス
  - セグメントごとに設置したセンサーが通信を監視するため、端末へのソフトウェアのインストールが不要です。
- ネットワーク機器非依存
  - スイッチの機能を使用しないので、既存のネットワーク機器の入れ替えや設定変更が不要です。

構成例



OT環境への導入

- OT環境への本製品の導入の有効性を第三者機関(※)の検証によって確認しました。
  - IPベースのプロトコルを使用する制御システムにおいて、InfoCage 不正接続防止による遮断はセキュリティ対策として有効。
  - 模擬プラントで使用されている各種の制御プロトコルの動作に干渉せず、ネットワーク負荷にもほとんど影響を及ぼさない。

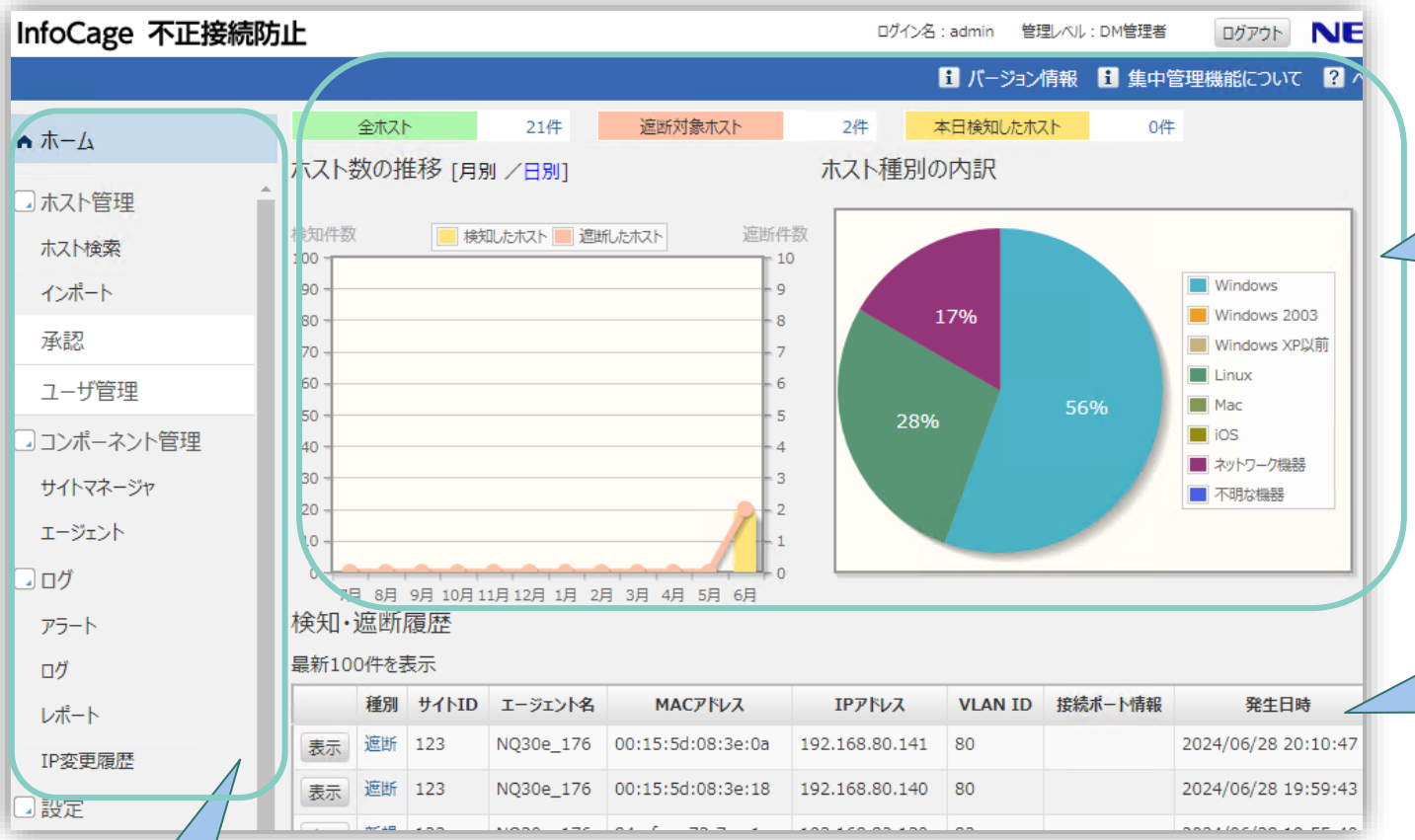
ミッションクリティカルなOT環境にも、
安心して、アドオンで導入いただけるセキュリティ製品です。

※技術研究組合 制御システムセキュリティセンター (CSSC) http://www.css-center.or.jp/
実際の制御システムを模した9種のプラントが設置されており、サイバーセキュリティの演習や検証などに活用されています。

機能紹介

グラフィカルな管理画面

- ブラウザでアクセスし、操作を直感的に行うことができます。



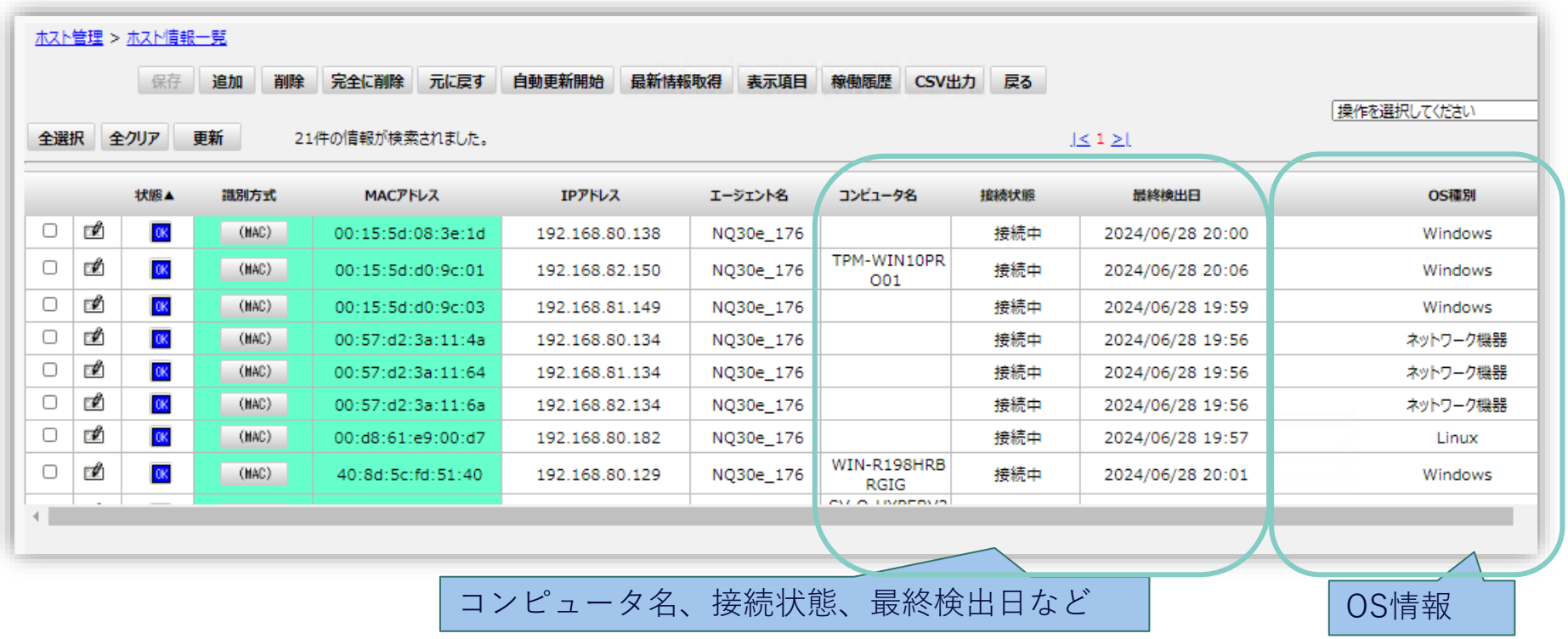
ホストのOS種別の内訳、検知数などを可視化。

遮断、検知のアラート情報の表示

操作メニュー

端末情報の自動収集

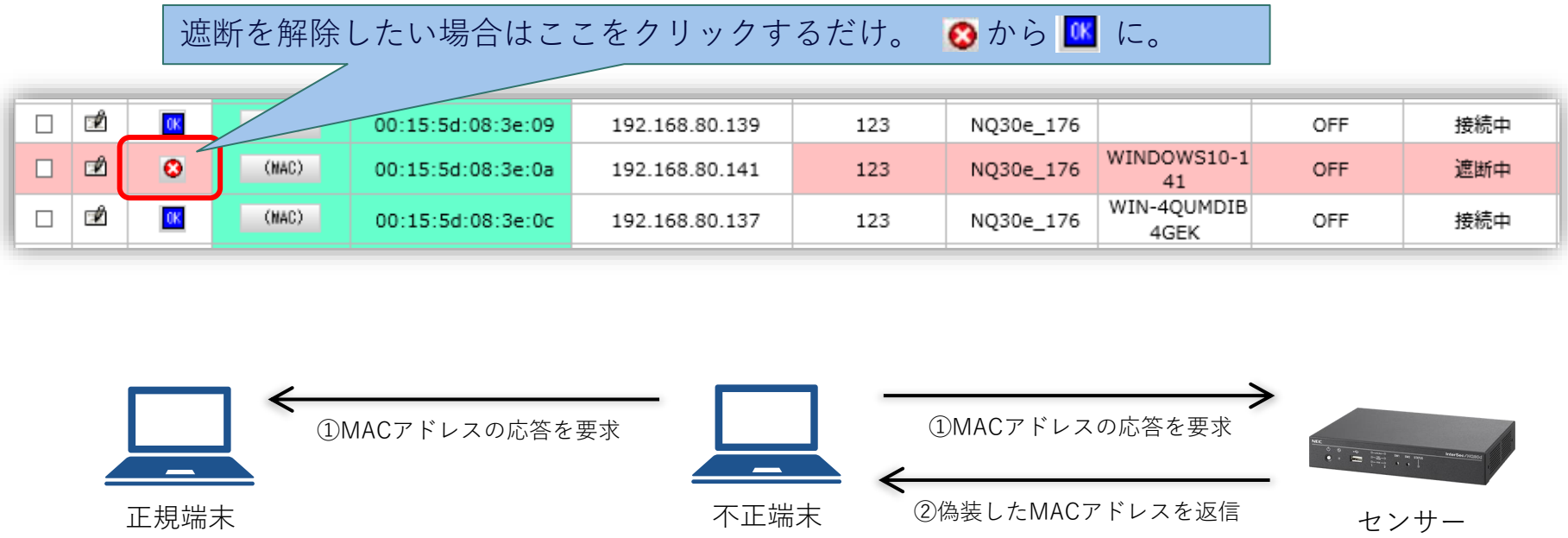
- 端末情報を自動収集し管理コンソールで、一覧表示。ホストの管理が容易にできます。



※ホスト名はWindows OSのコンピュータ名とDNS名の両方を取得できます。
※OS種別は送受信パケットに基づく推測のため、環境や状態によっては正しく判別できない場合があります。

不正端末の遮断

- NG登録された不正端末や未登録端末の接続を遮断します。
  - 未登録端末に対しては接続を許可する設定もできます。
  - IPv6アドレスを使用した通信も遮断できます。



ARPスプーフィングによる遮断イメージ

※MACアドレスの応答要求はブロードキャストによって行われるため、ネットワーク上の全端末に届きます。
※偽装するMACアドレスはセンサー自身のMACアドレスです。

接続先スイッチのポート情報の表示

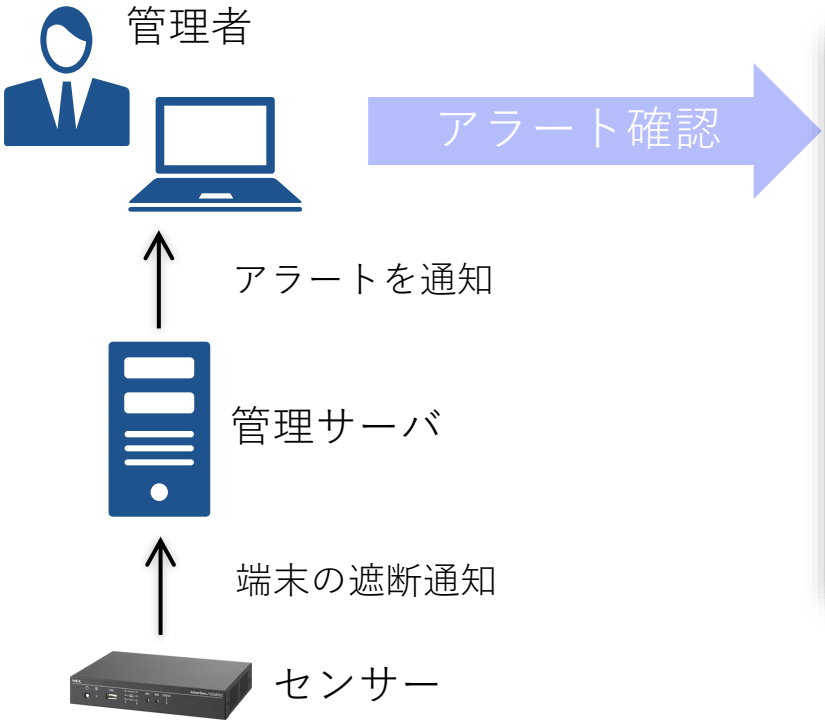
- 端末接続先のスイッチングハブのIPアドレスとポート情報を管理コンソールに表示できます。
  - 不正端末が接続されている物理的な場所を迅速に特定できます。

		状態	識別方式	MACアドレス	IPアドレス	接続状態	接続ポート情報▲	スイッチアドレス	ポート検出日時
☐		OK	(MAC)	b0:c7:45:5f:82:df	192.168.12.212	接続中	Fa0/12	192.168.11.254	2024/03/07 12:14:05
☐		OK	(MAC)	00:15:5d:0b:d4:03	192.168.12.216	接続中	Fa0/12	192.168.11.254	2024/03/07 12:14:05
☐		✖	(MAC)	1c:1b:0d:8f:a6:f2	192.168.11.161	遮断中	Fa0/16	192.168.11.254	2024/03/07 12:14:05
☐		OK	(MAC)	8c:df:9d:0a:df:06	192.168.11.98	接続中	Fa0/24	192.168.11.254	2024/03/07 12:14:05
☐		OK	(MAC)	8c:df:9d:0a:d3:9c	192.168.11.244	接続中	Fa0/24	192.168.11.254	2024/03/07 12:14:05
☐		OK	(MAC)	7c:66:9d:19:e2:10	192.168.11.246	接続中	Fa0/24	192.168.11.254	2024/03/07 12:14:05
☐		OK	(MAC)	f8:ca:85:54:83:60	192.168.11.209	接続中	Fa0/24	192.168.11.254	2024/03/07 12:14:05
☐		OK	(MAC)	f8:ca:85:54:81:83	192.168.11.208	接続中	Fa0/24	192.168.11.254	2024/03/07 12:14:05
☐		OK	(MAC)	f8:ca:85:54:82:53	*		Fa0/5	192.168.11.254	2024/03/07 12:14:05

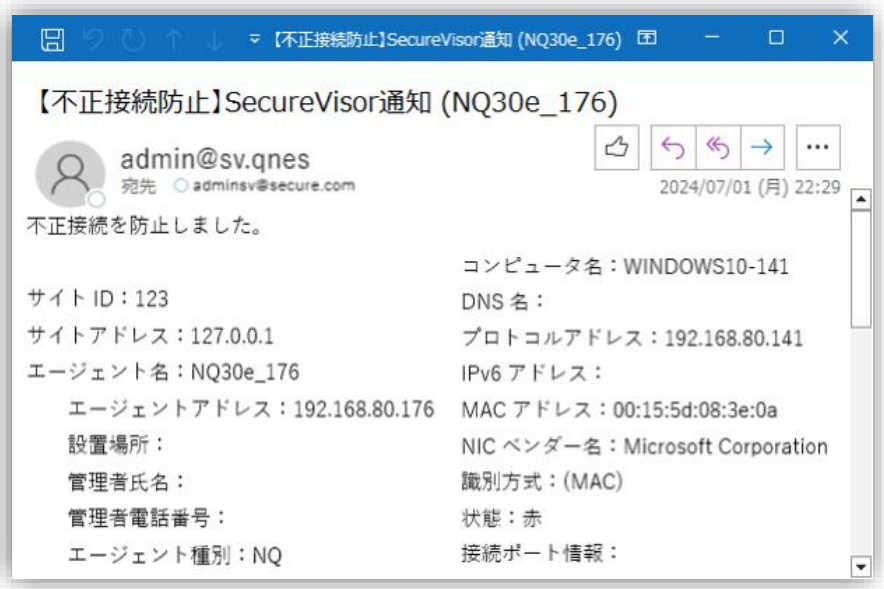
接続ポート情報は、スイッチで設定したポート名称が表示されます。

アラートの通知

- 未登録端末の検知と不正端末の遮断の実行時に管理者へアラートを通知します。
  - 端末の接続状況をリアルタイムに監視できます。



アラートメールの例



※ 紙面の関係上、上記は加工しています。

※アラートは電子メール送信、ポップアップダイアログ表示、SNMP Trap送信、任意コマンド実行がご利用になれます。

防止メッセージの表示

- 遮断された端末のWebブラウザ上に防止メッセージを表示できます。
  - メッセージは自由にカスタマイズできるため、解除申請など、利用者への説明や案内を記載することもできます。

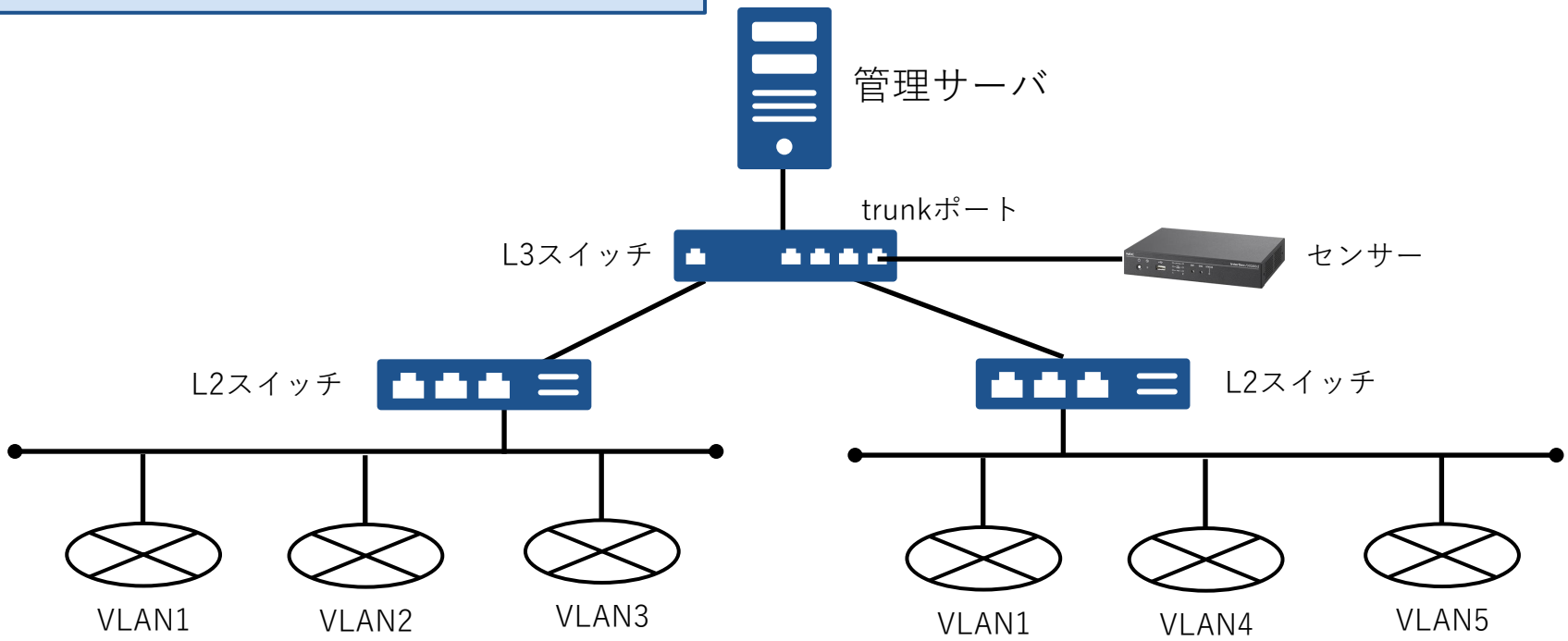
※HTTPでアクセス時のみ表示されます。

複数NWの管理①　タグVLAN環境の管理

- タグVLAN環境では1台のセンサーで最大32VLANを管理できます。
  - センサーの集約により導入コストを削減できます。

構成例

1台のセンサーでVLAN1～VLAN5を管理

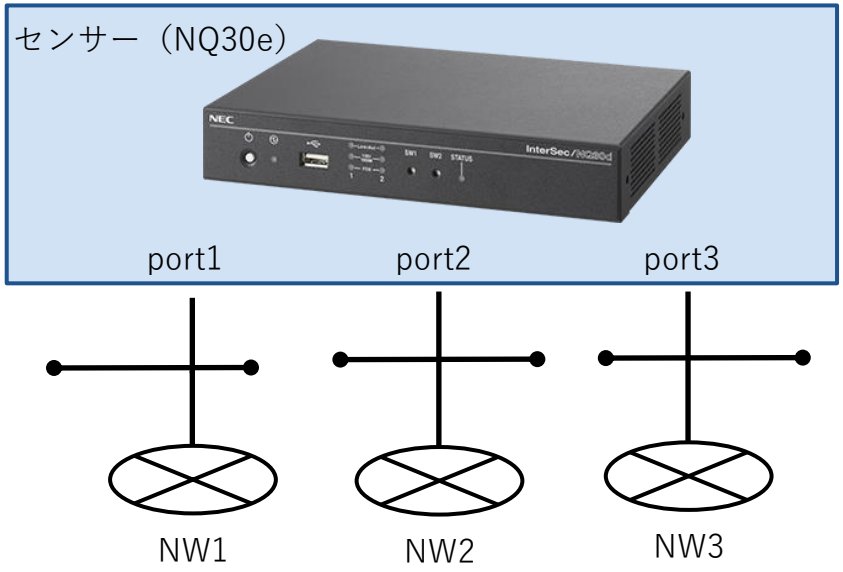


※本機能のご利用にはVLAN追加ライセンスが必要です。

複数NWの管理②　3ポート管理

- NQ30eは3ポートありますので、3セグメントまでは1台で管理可能です。
  - センサーの集約により導入コストを削減できます。
  - タグVLANでもご利用になれます。 物理的配線が可能であることが前提。

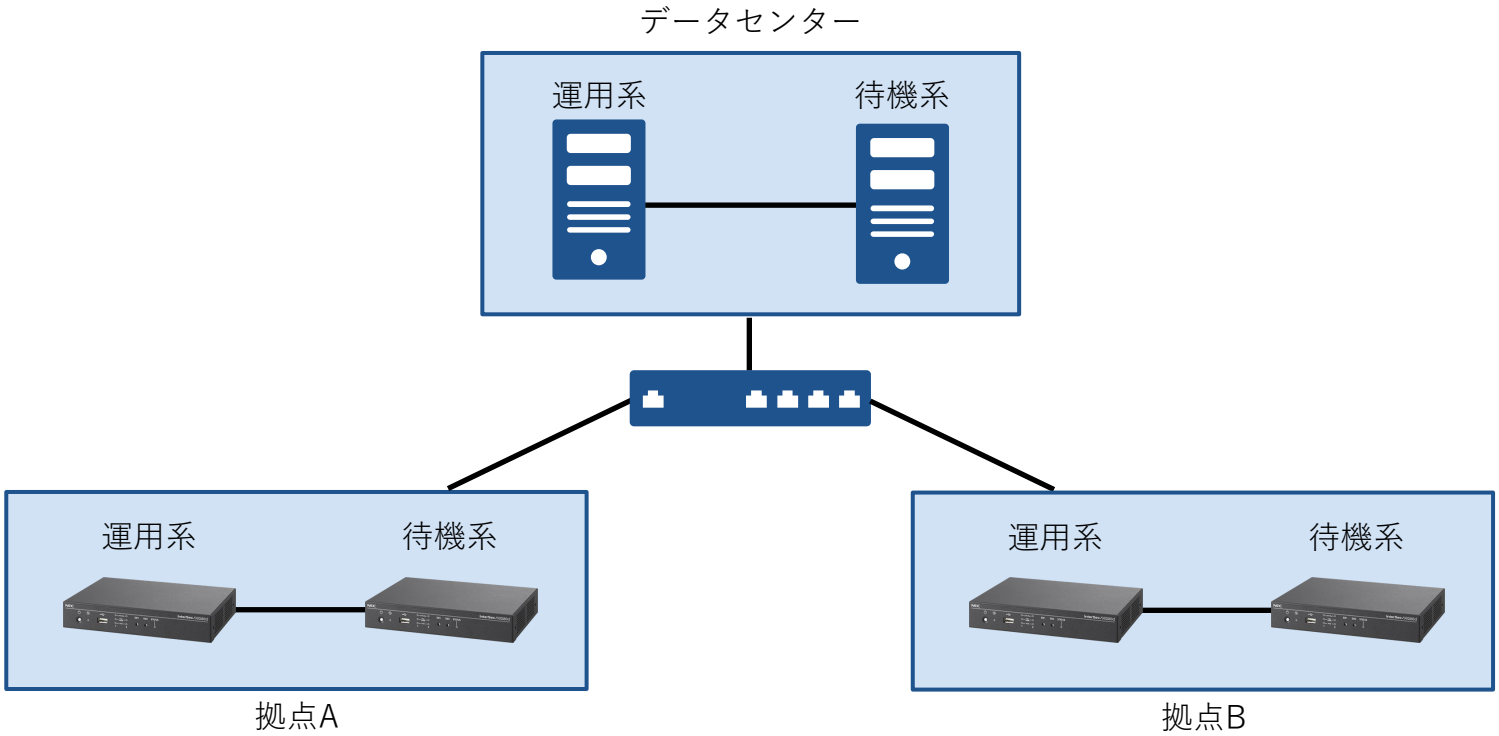
構成例



※本機能のご利用に際して、追加オプションは不要です。

管理サーバ・センサーの冗長化

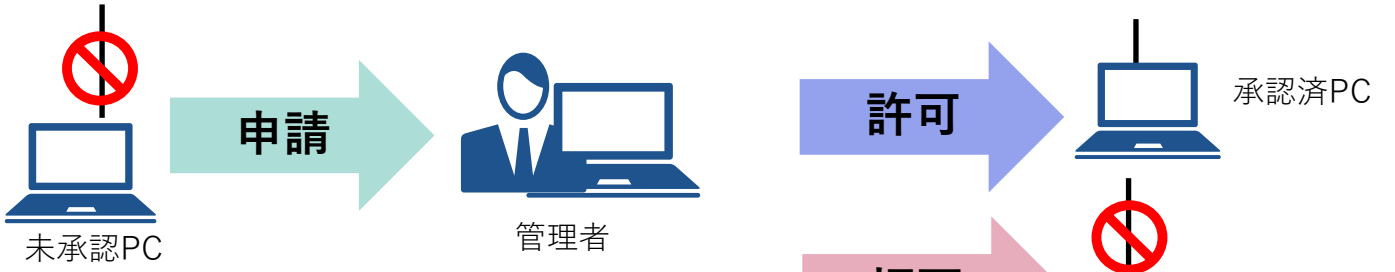
- 管理サーバやセンサーを冗長化し、運用系がダウンした際に待機系が動作を引き継ぎます。
  - 管理サーバやセンサーで障害が発生した際も、システムを継続して稼働させることができます。

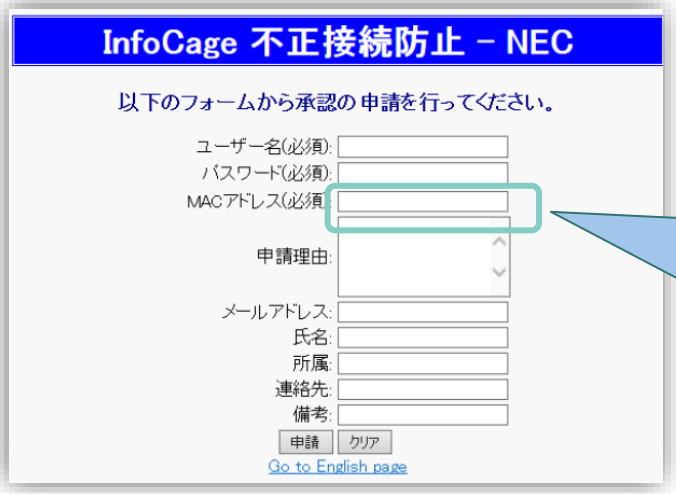


※管理サーバはCLUSTERPRO製品により冗長化されるため、別途CLUSTERPROのライセンス費用が必要です。
※センサーはInfoCage 不正接続防止製品の機能により冗長化されます。

承認申請ワークフロー

- 未承認PCをネットワーク接続する際、そのPCからWebブラウザを利用して管理者に申請ができます。
- 承認済みの端末から、未承認端末の接続申請もできます。
- 管理者による承認、 LDAPの認証による自動承認、ユーザID/PWによる承認が選択可





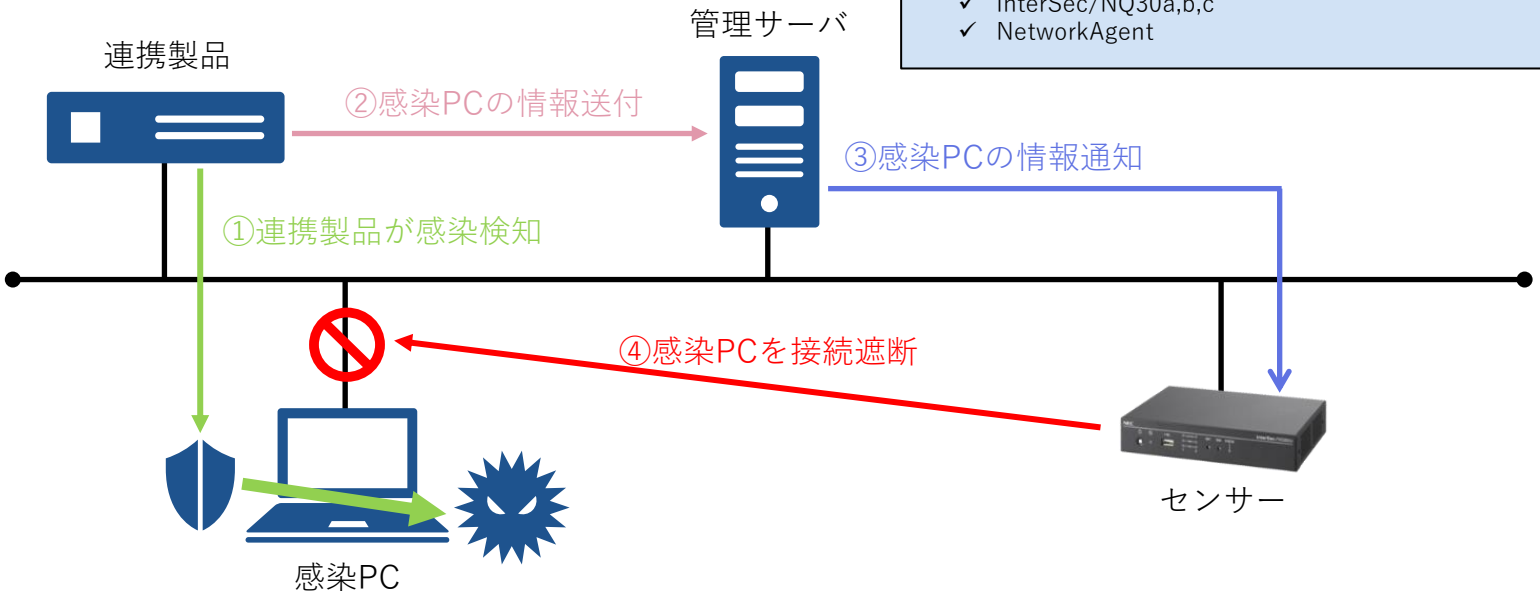
承認済み端末から未承認端末の申請をする場合は、未承認端末のMACアドレスを指定。

他システム連携

- マルウェア対策製品と連携し、マルウェア感染を検知した端末を自動的にネットワークから遮断できます。

※ 本連携機能の対象製品は以下の通りです。
- ✓ 「FireEye NXシリーズ V7.8～V7.9」
- ✓ 「DDI Ver.3.8 SP1、SP3」
- ✓ 「ウイルスバスター コーポレートエディション XG」
- ✓ 「Palo Alto V8.1」
- ✓ 「FortiOS V5.6系」

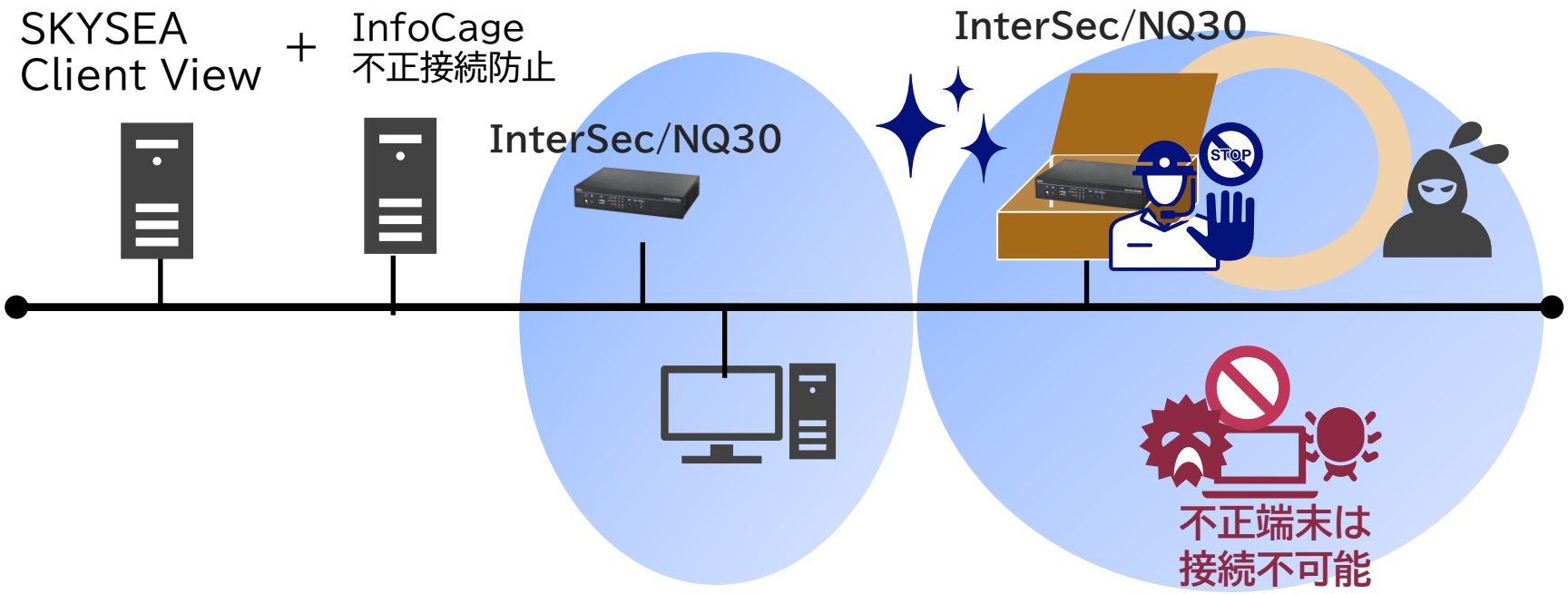
※ 以下のエージェントはサポート対象外です(InterSec/NQ30d以降でサポート)。
- ✓ InterSec/NQ30a,b,c
- ✓ NetworkAgent



※ FireEyeはFireEye, Inc.の商標または登録商標です。
※ Deep Discovery Inspectorならびにウイルスバスターはトレンドマイクロ株式会社の登録商標です。
※ Palo AltoはPalo Alto Networks社の登録商標です。
※ FortiGateはFortinet社の登録商標です。

SKYSEA Client View連携

- SKYSEA Client Viewと連携しご利用することが可能です。
- SKYSEA Client Viewの画面でホストを一元管理、InterSec/NQ30で遮断することが可能です。
- 他にも連携してご利用いただくことによりメリットが多数ございます。

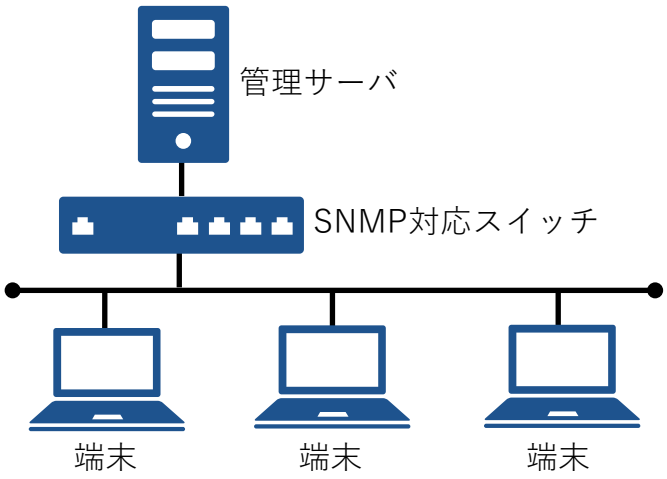


※ 詳細は下記をご参照ください。
https://jpn.nec.com/infocage/prevention/skyseaclientview.html
Sky社のIT資産管理製品「SKYSEA Client View」との連携: 不正PC接続防止ソフトウェア InfoCage 不正接続防止 | NEC

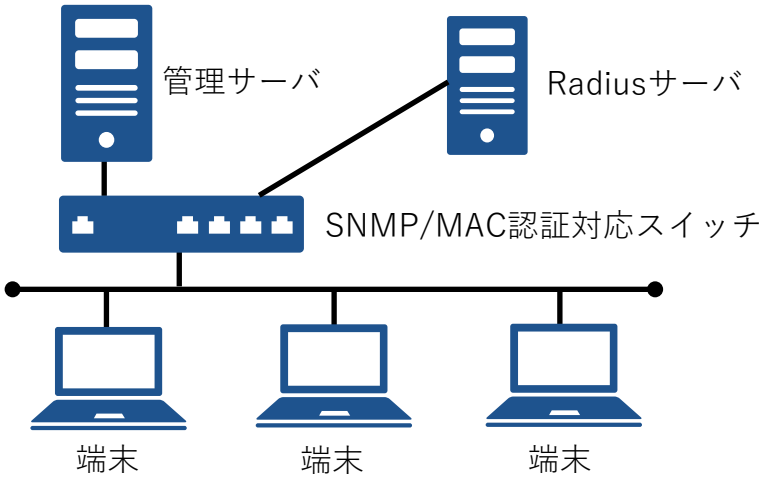
スイッチ連携

- スイッチの機能を利用して端末の検知と遮断を行います。
  - 管理する端末数が少ない場合、センサーより低コストで導入できます。
- システム要件
  - 検知のみ： SNMP通信に対応したスイッチ
  - 検知＋遮断：SNMP通信/MACアドレス認証に対応したスイッチ、
    Radiusサーバ(Network Policy Server + Active Directory)

構成例：検知のみ



構成例：検知＋遮断

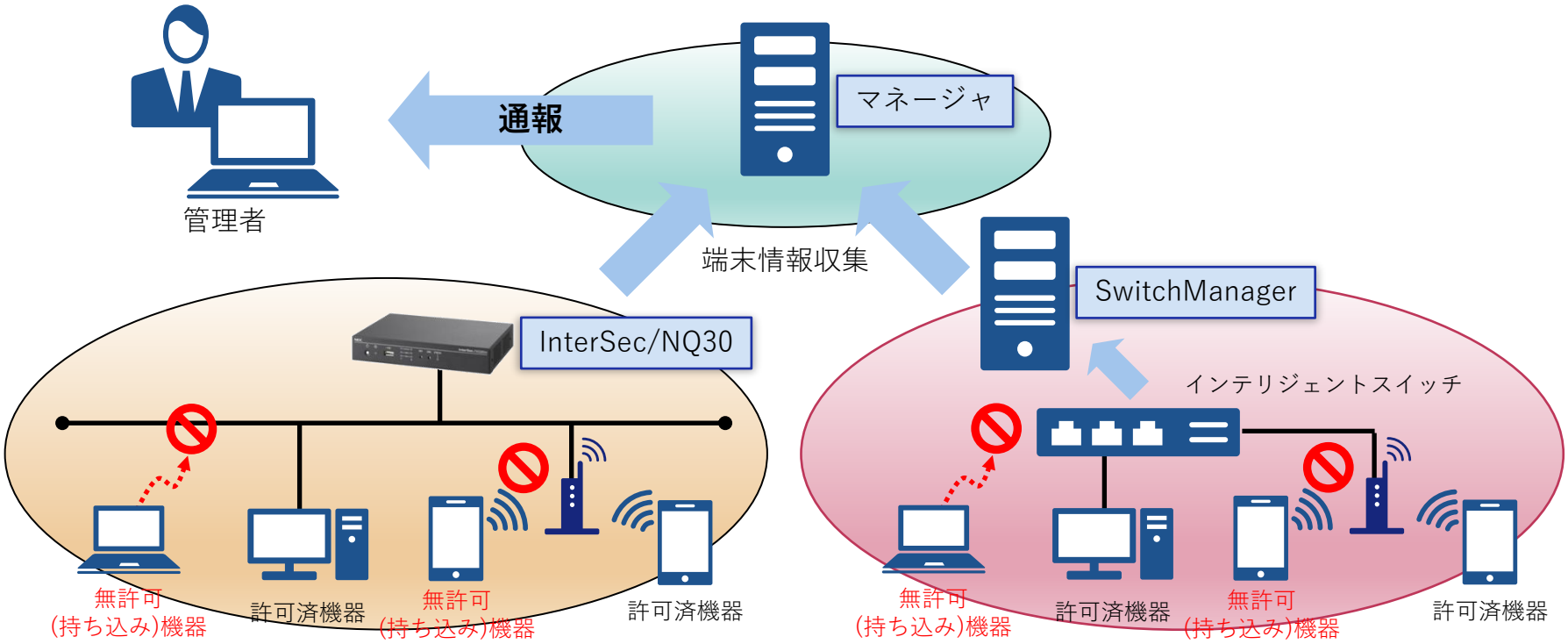


※本機能のご利用にはスイッチ連携オプションライセンスが必要です。
※センサーを設置しない管理方式のためセンサーの機能はご利用になれません。
※スイッチがSNMP通信/MACアドレス認証に対応しているか事前の検証を推奨いたします。

システム構成

システム構成イメージ

- ネットワーク接続機器の固有情報の収集機能と、その情報の管理機能で構成されます。
  - 管理機能：InfoCage 不正接続防止 マネージャ
  - 収集機能：InterSec/NQ30、SwitchManager



センサーによる管理セグメント

スイッチ連携による管理セグメント

導入実績・導入事例

導入実績

- 2002年12月の発売以来、官公庁、製造、流通業など業種を問わず、数多くのお客様に導入いただいています。
- NECグループのネットワークにて、10万台規模での運用実績があります。

業種	企業名
製造・プロセス業	P社、K社、O社、S社、M社、D社、・・・
流通サービス業	K社、B社、I社、F社、・・・
情報サービス産業	O社、C社、S社、・・・
電力・通信・放送業	T社、N社、M社、Oテレビ、B新聞社、P印刷、I電力、電話会社、・・・
建設業	O社、A社、・・・
金融・証券業	U証券、S証券、N証券、A信金、M信金、・・・
学校	O大学、Z高校、A研究所、独立行政法人、・・・
省庁・公共	○省、T市役所、Y市水道局、○農政局、I町役場、○県警、・・・
その他	鉄道会社、製薬会社、病院、旅行会社、運送会社、消防所、・・・

- 大規模環境での実績
  - ✓ A社(サービス業) ・・・ 435セグメント、49,000端末
  - ✓ B社(サービス業) ・・・ 270セグメント、40,000端末
  - ✓ C社(通信業) ・・・ 600セグメント、45,000端末
  - ✓ D省(官公庁) ・・・ 1100セグメント

製品構成例・製品体系/価格・動作環境

製品構成例(1)

◆ 最小構成(1拠点・1セグメント)

製品名	個数	製品単価	PP保守単価	HW保守単価	製品小計	PP保守小計	HW保守小計
InfoCage 不正接続防止 メディアキット	1	¥20,000	ー	ー	¥20,000	ー	ー
InfoCage 不正接続防止 マネージャ	1	¥290,000	¥4,260	ー	¥290,000	¥4,260	ー
InterSec/NQ30e	1	¥215,000	¥1,960	¥1,120	¥215,000	¥1,960	¥1,120
				合計	¥525,000	¥6,220	¥1,120

製品構成例(2)

◆ 拠点分散ネットワーク(10セグメント／非タグVLAN)

製品名	個数	製品単価	PP保守単価	HW保守単価	製品小計	PP保守小計	HW保守小計
InfoCage 不正接続防止 メディアキット	1	¥20,000	ー	ー	¥20,000	ー	ー
InfoCage 不正接続防止 マネージャ	1	¥290,000	¥4,260	ー	¥290,000	¥4,260	ー
InterSec/NQ30e	10	¥215,000	¥1,960	¥1,120	¥2,150,000	¥19,600	¥11,200
				合計	¥2,460, 000	¥23,860	¥11,200

◆ 拠点集中ネットワーク(10セグメント／タグVLAN)

製品名	個数	製品単価	PP保守単価	HW保守単価	製品小計	PP保守小計	HW保守小計
InfoCage 不正接続防止 メディアキット	1	¥20,000	ー	ー	¥20,000	ー	ー
InfoCage 不正接続防止 マネージャ	1	¥290,000	¥4,260	ー	¥290,000	¥4,260	ー
InfoCage 不正接続防止 VLAN追加ライセンス	9	¥35,000	￥810	ー	¥315,000	¥7,290	ー
InterSec/NQ30e	1	¥215,000	¥1,960	¥1,120	¥215,000	¥1,960	¥1,120
				合計	¥840,000	¥13,510	¥1,120

製品体系/価格・動作環境

- 製品体系/価格については以下の製品サイトをご参照ください。
  製品体系/価格: 不正PC接続防止ソフトウェア InfoCage 不正接続防止 | NEC

- 動作環境については以下の製品サイトをご参照ください。
  動作環境: 不正PC接続防止ソフトウェア InfoCage 不正接続防止 | NEC

付録

通常版とLite版の比較

	通常版	Lite版
管理サーバの有無	必須	不要
管理コンソール	Webコンソール	Windowsアプリケーション
接続許可条件	IP・MACアドレスの組み合わせ	MACアドレス
1台のNQで管理可能なMACアドレス数	8,000	1,000
最小構成価格	¥525,000 ＋ 管理サーバ費用	¥360,000
端末情報の自動収集	○	○
不正端末の遮断	○	○
IPv6通信の検知と遮断	○	○
接続先スイッチのポート情報の表示	○	×
アラートの通知	○	○
防止メッセージの表示	○	○
タグVLAN環境の管理	○	○
管理サーバ・センサーの冗長化	○	ー
承認申請ワークフロー	○	×
他システム連携	○	×
スイッチ連携	○	×

センサーとスイッチ連携の比較

	InterSec/NQ30e	スイッチ連携
遮断方式	偽装ARPによる通信妨害	IEEE802.1xによるMACアドレス認証
接続許可条件	IP・MACアドレスの組み合わせ	MACアドレスのみ
遮断解除の反映タイミング	即時	再認証時
1台のセンサーで 管理可能なMACアドレス数	8000	ー
端末情報の自動収集	○	×
不正端末の遮断	○	○
アラートの通知	○	○
防止メッセージの表示	○	×
接続ポートの検知	○	×
IPv6通信の検知と遮断	○	×
タグVLAN環境の管理	○	×
管理サーバ・センサーの冗長化	○	ー
承認申請ワークフロー	○	×
他システム連携	○	×

注意事項

- NEC製ソフトウェアのサポートポリシーでは、サポート適用範囲の一貫性の保証ならびに全てのお客様への平等なサービス提供のため、以下の制約を設けております。
  - システム単位(案件毎)でご契約いただくこと。
  - 原則、ご使用中のすべてのソフトウェア製品(待機系での利用含む)についてご契約いただくこと。
  - ソフトウェア製品引渡時から継続してサポートを契約していること。
- 本製品では購入している以下すべてのライセンスのサポート契約が必要です。
  - InterSec/NQ30ソフトウェア
  - マネージャ
  - リモートコンソール
  - VLAN追加ライセンス
  - スイッチ連携オプション
  - NetworkAgent
- サポート契約が正しく行われていない場合、以下のサポートサービスを提供することができません。
  - レスポンスサービス、インフォメーションサービス
  - ライセンスサービス(バージョンアップ)
  - ライセンスサービス(リビジョンアップ)

※サポートが受けられないケース
- マネージャのサポートは契約しているが、InterSec/NQ30ソフトウェアのサポートを契約していない。
- マネージャとInterSec/NQ30ソフトウェアのサポートは契約しているが、VLAN追加ライセンスのサポートを契約していない。
- ソフトウェア製品引渡時から現在までにサポート未契約の期間がある。

製品ご紹介サイト/お問い合わせ先

- 製品ご紹介サイト／お問い合わせ先
  https://jpn.nec.com/infocage/prevention

資料請求・お問い合わせはこちらから受け付けております。

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC