Orchestrating a brighter world

NEC

InfoCage 不正接続防止 紹介資料

2018年3月 NEC

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

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

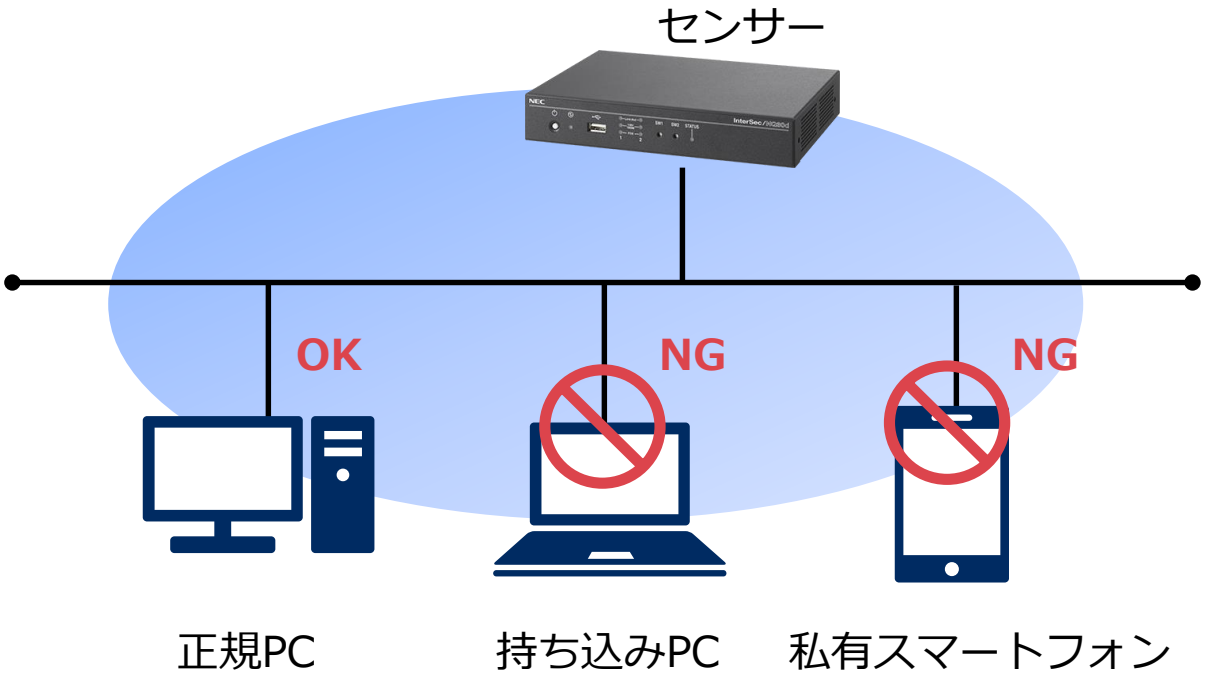
持ち込みPC対策に対するネットワーク管理者の声

- 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などはできる限り避けたい。

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(InterSec/NQ30)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。



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

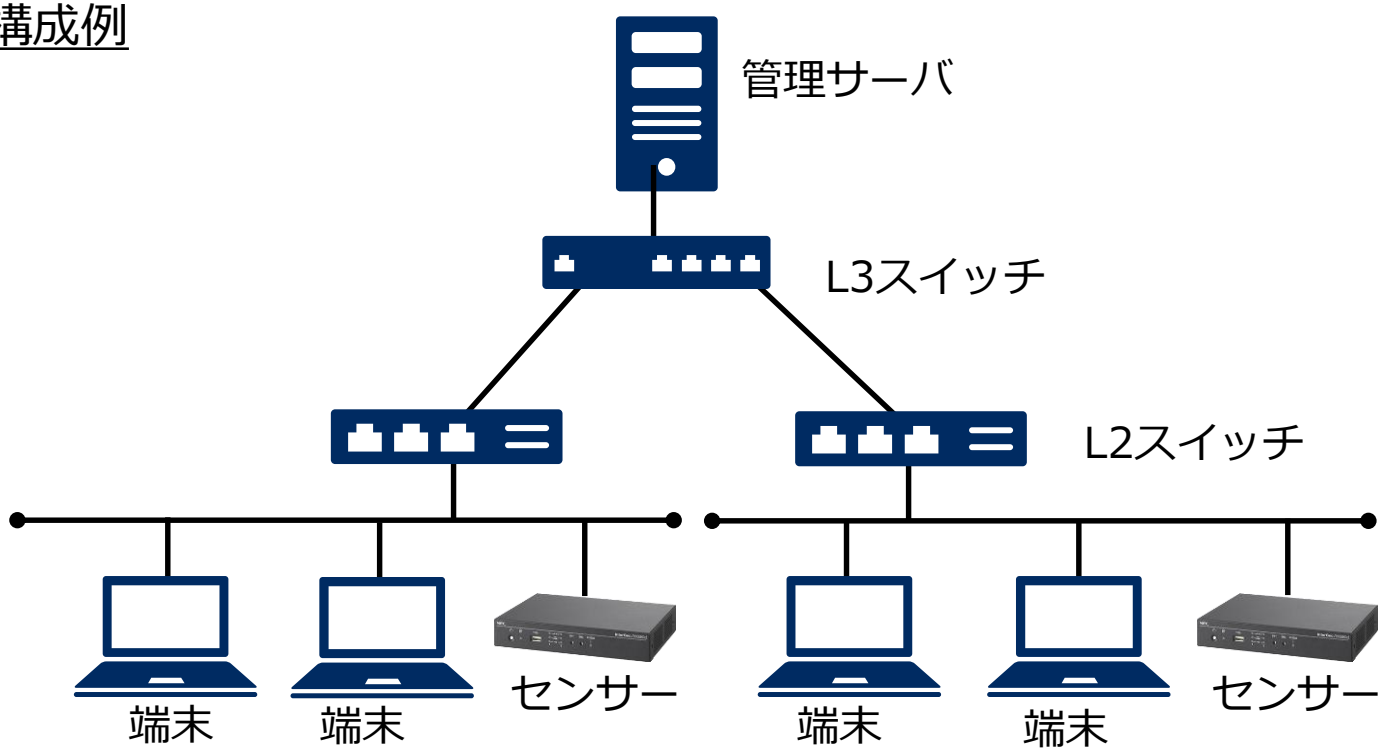
エージェントレス

- 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ため、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



機能紹介

端末情報の自動収集

ネットワークに接続されている端末の情報を自動収集し、管理コンソールに一覧表示します。

- ネットワークにどのような端末が何台接続されているのかを把握できます。
- ネットワークに管理外の端末が接続されていないか確認できます。
- ネットワークにサポートの切れた古いOSが接続されていないか確認できます。

状態	MACアドレス	IPアドレス	機器種別	接続ポート	スイッチアドレス
OK	0A:00:01:0A:00:01	192.168.0.1	Windows XP	Fa/01	192.168.0.254
OK	0B:00:02:0B:00:02	192.168.0.2	Windows 7 SP1	Fa/02	192.168.0.254
OK	0C:00:03:0C:00:03	192.168.0.3	Windows 8	Fa/03	192.168.0.254
NG	0D:00:04:0D:00:04	192.168.1.1	Linux	Fa/01	192.168.1.254
NG	0E:00:05:0E:00:05	192.168.1.2	ネットワーク機器	Fa/02	192.168.1.254
NG	0F:00:06:0F:00:06	192.168.2.1	iOS	Fa/01	192.168.2.254

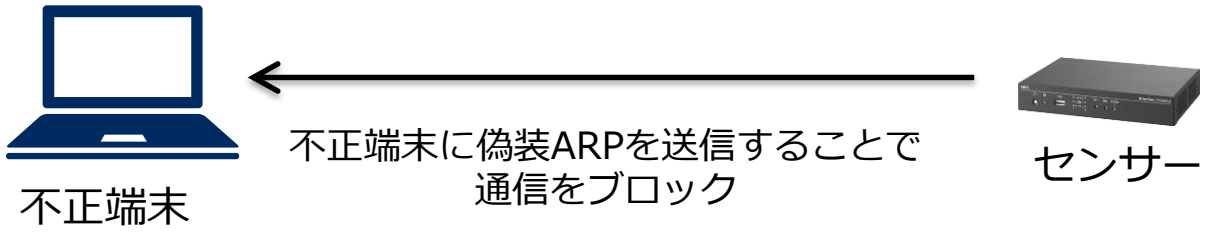
※機器種別はパケットからの推測であるため、環境によって正しく判別できない場合があります。
※接続ポートとスイッチアドレスは通常版でのみ表示できます。

不正端末の遮断

状態がNGで登録された端末や未登録の端末の接続を防止します。

- 不正端末による不正アクセスやウイルス感染からネットワークを守ることができます。

状態	MACアドレス	IPアドレス
OK	0A:00:01:0A:00:01	192.168.0.1
OK	0B:00:02:0B:00:02	192.168.0.2
OK	0C:00:03:0C:00:03	192.168.0.3
NG	0D:00:04:0D:00:04	192.168.0.4
NG	0D:00:04:0D:00:05	192.168.0.5
NG	0D:00:04:0D:00:06	192.168.0.6



※不正端末の遮断は、偽装ARPによるARPスプーフィングによって実現しています。

アラート通知

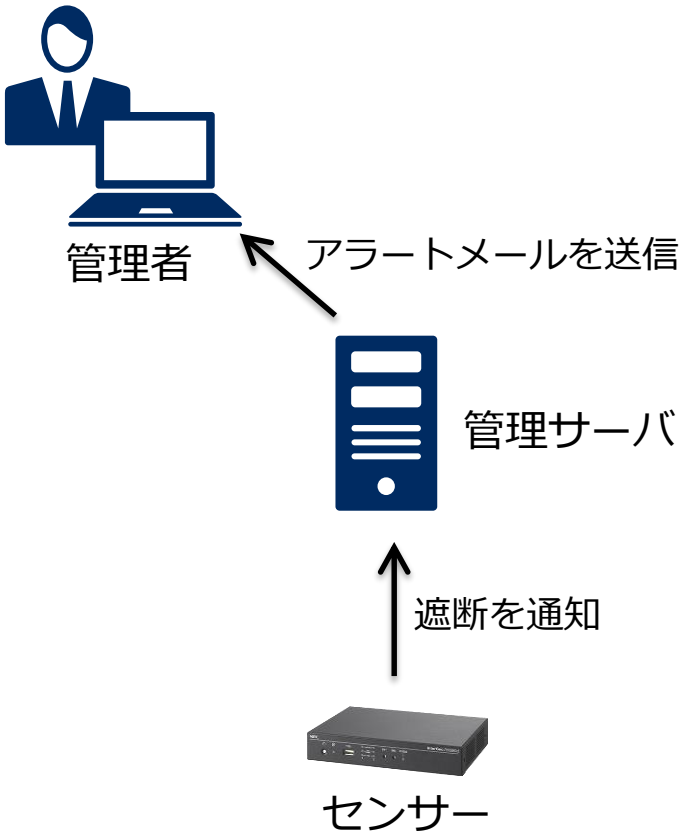
- 不正端末を遮断した際や連携製品からの通知を受け取った際に、管理者にアラートを通知できます。

アラートメールの例

不正接続を防止しました。

サイトID：1
サイトアドレス：192.168.0.1
エージェント名：NQ01
　エージェントアドレス：192.168.0.100
　設置場所：本社
　管理者氏名：日電太郎
　管理者電話番号：1-23-45678
　エージェント種別：NQ

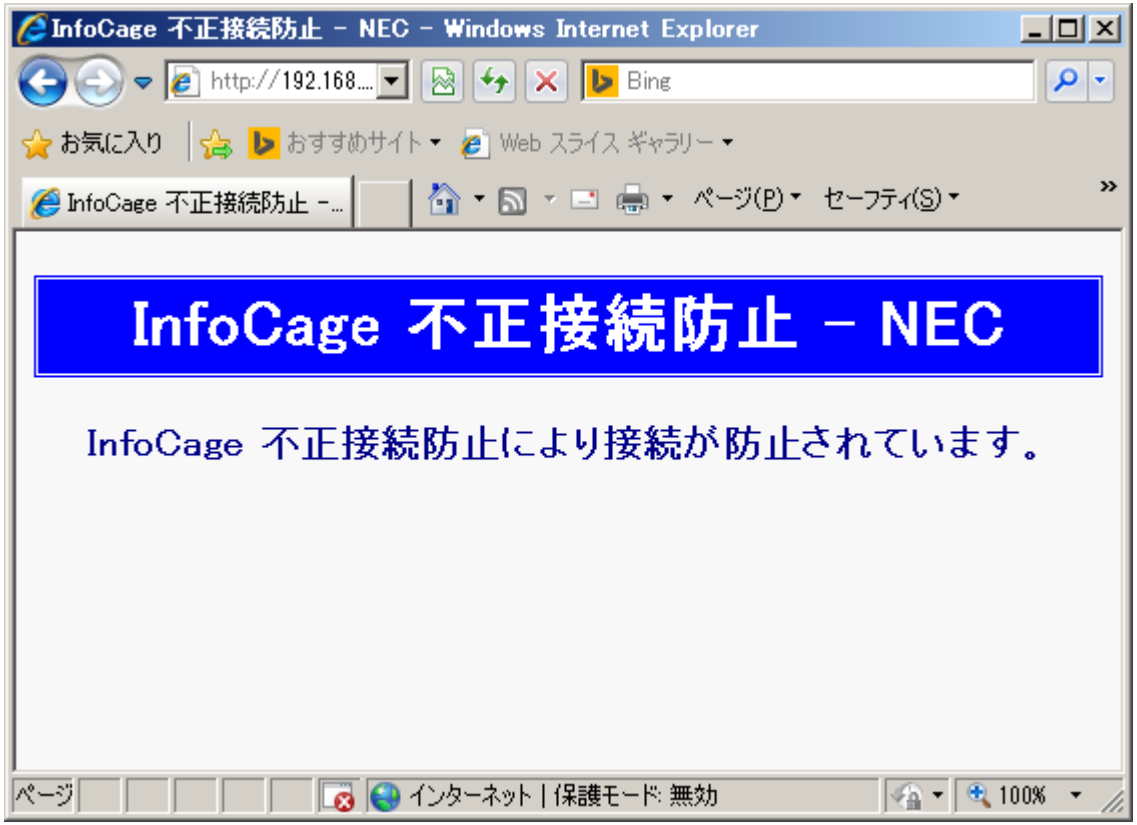
・
・
・



防止メッセージ表示

遮断された端末のWebブラウザに防止メッセージを表示できます。

- 画面は自由にカスタマイズできるため、連絡先などを表示することもできます。



接続ポート検知

端末が接続されているスイッチのIPアドレスとポート情報を管理コンソールに表示します。

- 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。

システム要件

- スイッチがSNMPv1またはSNMPv2cに対応している必要があります。
- 管理サーバ1台あたり最大600件のスイッチ情報を登録できます。

状態	MACアドレス	IPアドレス	接続ポート	スイッチアドレス
OK	0A:00:01:0A:00:01	192.168.0.1	Fa/01	192.168.0.254
OK	0B:00:02:0B:00:02	192.168.0.2	Fa/02	192.168.0.254
OK	0C:00:03:0C:00:03	192.168.0.3	Fa/03	192.168.0.254
NG	0D:00:04:0D:00:04	192.168.1.1	Fa/01	192.168.1.254
NG	0E:00:05:0E:00:05	192.168.1.2	Fa/02	192.168.1.254
NG	0F:00:06:0F:00:06	192.168.2.1	Fa/01	192.168.2.254

※通常版でのみ使用できます。
※Cisco社のCatalystはVLANごとにスイッチ情報を登録する必要があるため、1VLANにつき1件のスイッチ情報として数えます。

IPv6対応

IPv4と同様に、IPv6の通信も検知・遮断できます。

- WindowsはVista以降でIPv6が標準で有効なため、IPv4通信を防止していても、IPv6による通信が自動的に行われます。このため、現在のネットワーク環境で持ち込みPCの通信を防止するためには、**IPv6対応が必須**です。

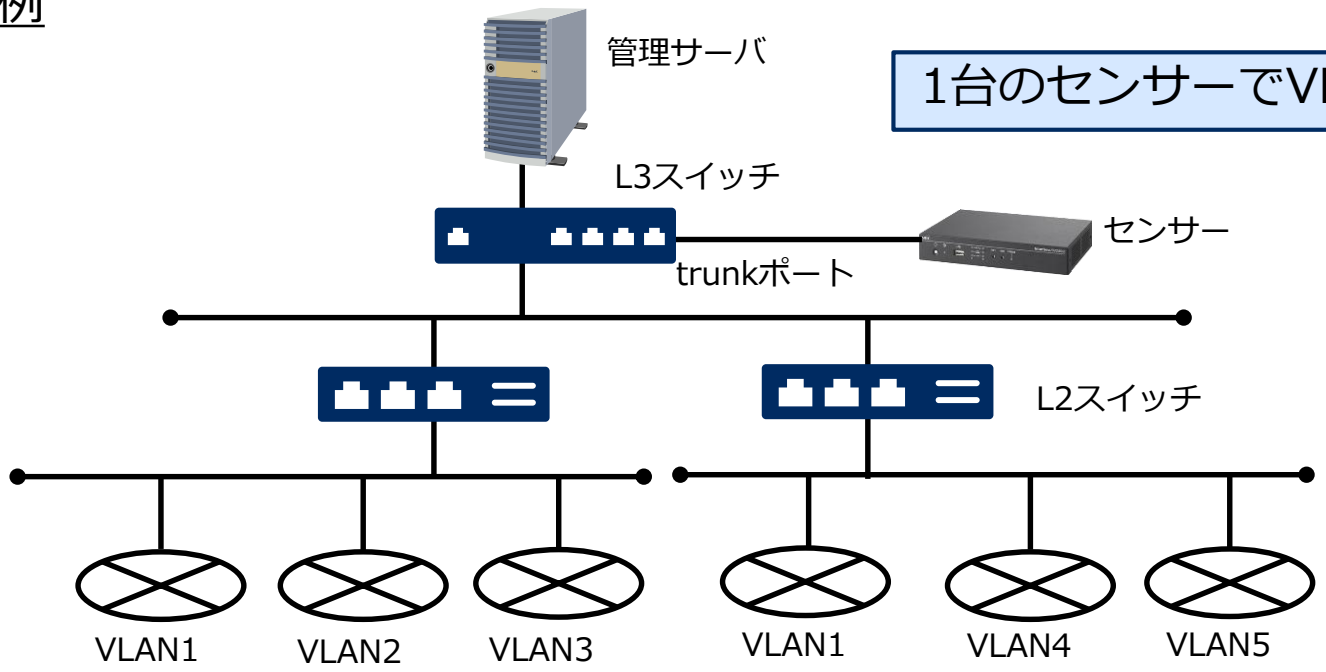
状態	MACアドレス	IPアドレス	IPv6アドレス
OK	0A:00:01:0A:00:01	192.168.0.1	2001:1234::1
OK	0B:00:02:0B:00:02	192.168.0.2	2001:1234::2
OK	0C:00:03:0C:00:03	192.168.0.3	2001:1234::3
NG	0D:00:04:0D:00:04	192.168.0.4	2001:1234::4
NG	0D:00:04:0D:00:05	192.168.0.5	2001:1234::5
NG	0D:00:04:0D:00:06	192.168.0.6	2001:1234::6

タグVLAN対応

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。

- センサーの台数を削減できます。

構成例

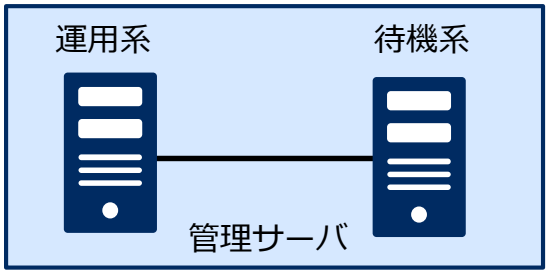


※別途VLAN追加ライセンスが必要です。
※管理可能VLAN数はセンサーのバージョンによって異なります。

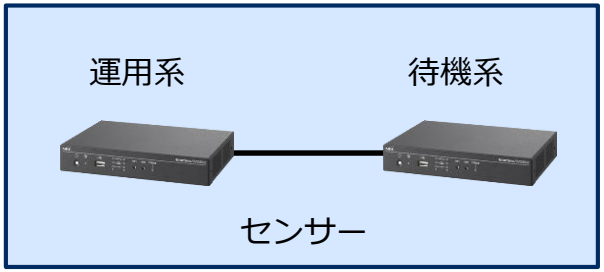
冗長化

- 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。

CLUSTERPROで冗長化



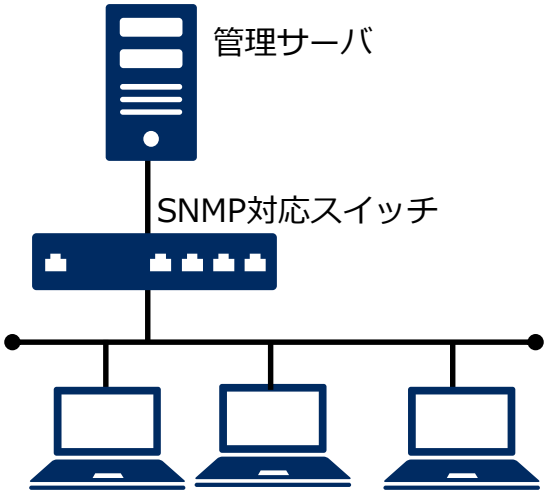
製品機能で冗長化



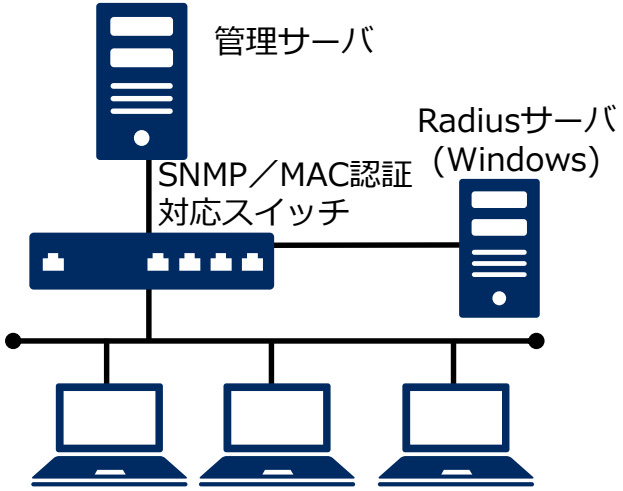
スイッチ連携

- センサーを使用せず、スイッチの機能を使用して端末の検知と遮断を行います。
  - セグメントあたりの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に対応したスイッチ
  - 検知＋遮断：SNMPとMAC認証に対応したスイッチ

構成例：検知のみ



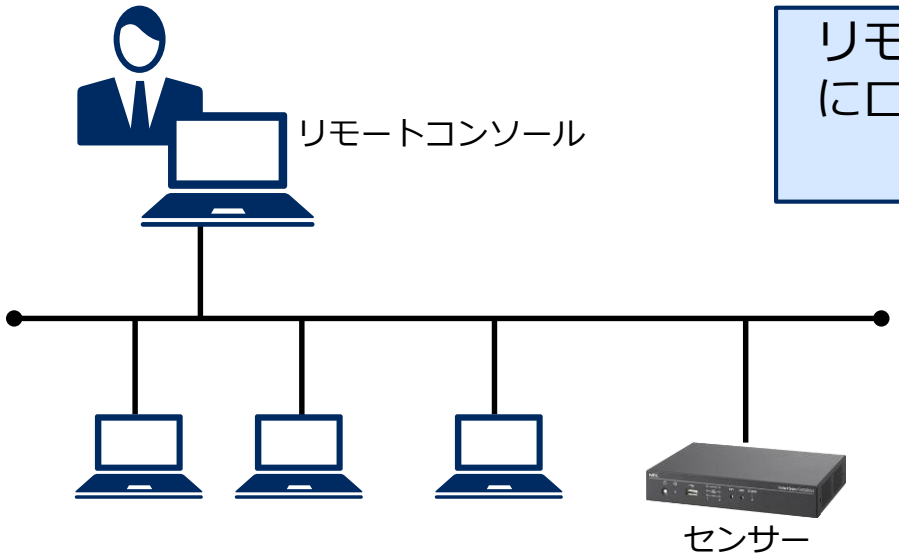
構成例：検知＋遮断



InfoCage 不正接続防止 Lite

管理サーバを設置せず、センサー単独で使用できます。

- 管理サーバが不要であるため、導入コストを削減できます。



リモートコンソールからセンサーにログインして端末一覧の確認や設定変更を行います。

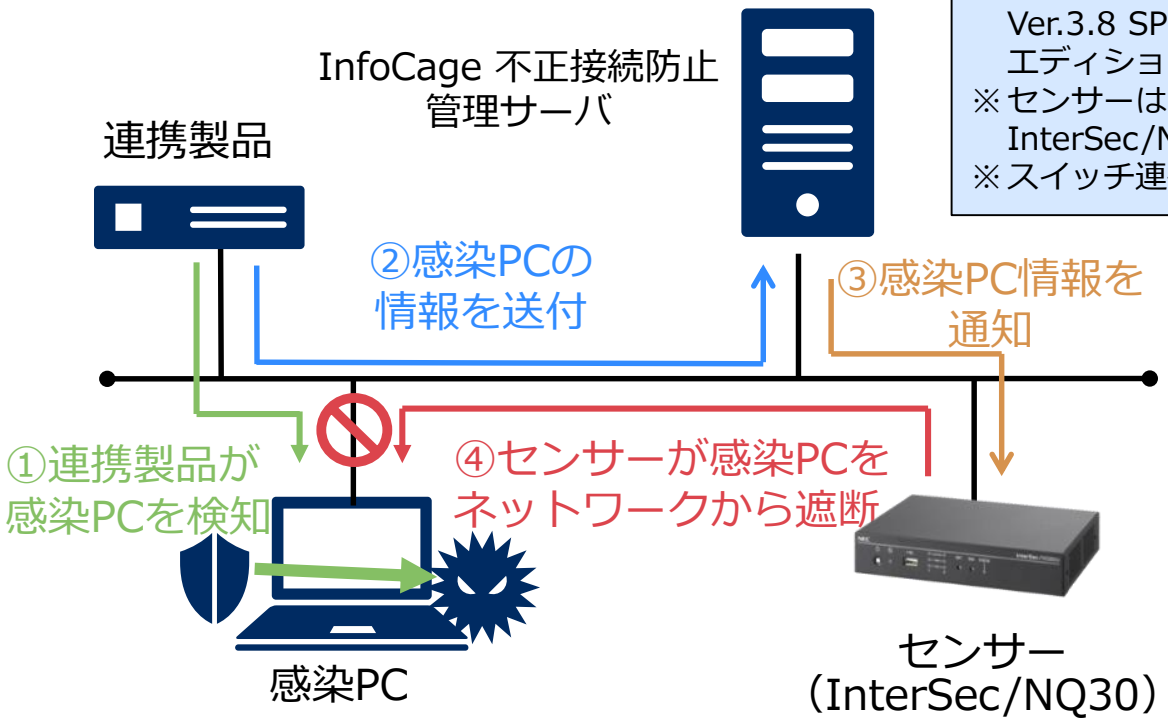
マルウェア対策製品連携

「FireEye」「Deep Discovery Inspector(DDI)」「ウイルスバスター」が検知したマルウェア感染端末を即座にネットワークから遮断できます。

状態	MAC アドレス	IP アドレス	検知 製品名	検知 日時	検知 機器名	検知機器 IPアドレス	イベント名	危険度
✕	00:00:4c:b7:a1:8d	192.168.0.1	FireEye	May 25 2016 17:04:32 JST	MPS	192.168.0.63	Ips-event	8

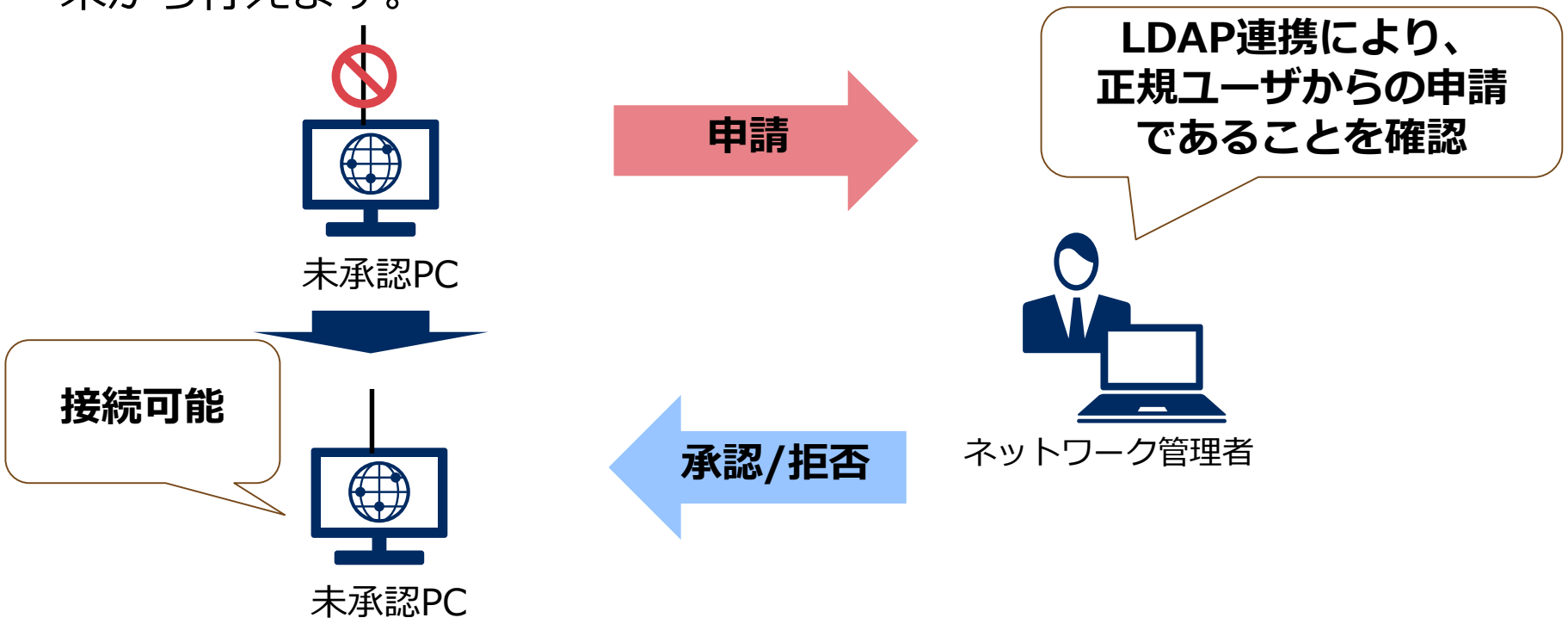
管理画面の表示イメージ

※連携対象は「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」です。
※センサーはInterSec/NQ30c,dのみサポートしています。InterSec/NQ30a,bはサポート対象外です。
※スイッチ連携はサポート対象外です。



承認申請ワークフロー

- 承認申請ワークフローにより、正規ユーザが未承認PCを使う際、そのPCから管理者に申請できます。
- LDAP連携により、正規ユーザによる申請であることを確認した上で承認することが可能です。正規ユーザになりすました不正ユーザによる申請の排除に役立ちます。
- Webブラウザを持たない機器の申請を、Webブラウザを持つ承認済み端末から行えます。

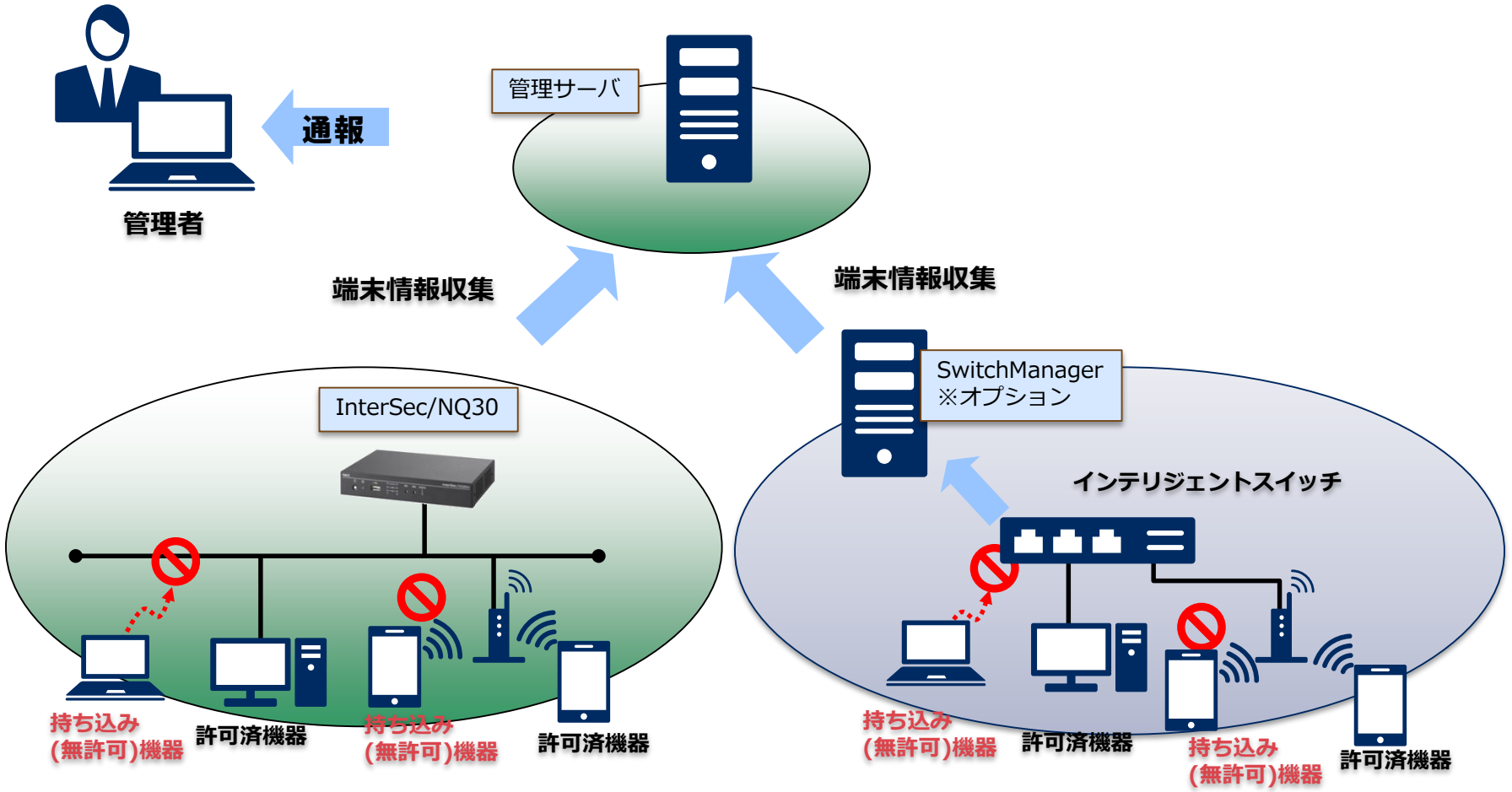


構成例

システム構成

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 管理サーバ
- 収集機能：InterSec/NQ30、SwitchManager



構成例（通常版、10セグメント）

製品名	個数	単価	価格(税別)
InfoCage 不正接続防止 V5.3 メディアキット	1	¥20,000	¥20,000
InfoCage 不正接続防止 V5.3 マネージャ 1ライセンス	1	¥290,000	¥290,000
InterSec/NQ30d	5	¥178,000	¥890,000
		合計	¥1,200,000

※InterSec/NQ30dは1台で2セグメントの管理が可能です。

構成例（Lite版、2セグメント）

製品名	個数	単価	価格(税別)
InfoCage 不正接続防止 V5.3 Lite リモートコンソール	1	¥145,000	¥145,000
InterSec/NQ30d	1	¥178,000	¥178,000
		合計	¥323,000

※メディアキットはリモートコンソールに同梱
※InterSec/NQ30dは1台で2セグメントの管理が可能です。

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、約1,300社への導入実績があります。
- NECグループの全セグメントにて、10万台規模で現在運用中です。

不正接続防止領域 2016年度実績：シェアNo.1

※出典：㈱富士キメラ総研 2017 ネットワークセキュリティビジネス調査総覧 <検疫ツール【不正接続防止ツール】>

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**

導入事例：製造業A社様

IPv4セグメントだけでなく、部分的に導入していたIPv6セグメントについても同様に接続機器の管理と不正接続防止を実現

導入の背景

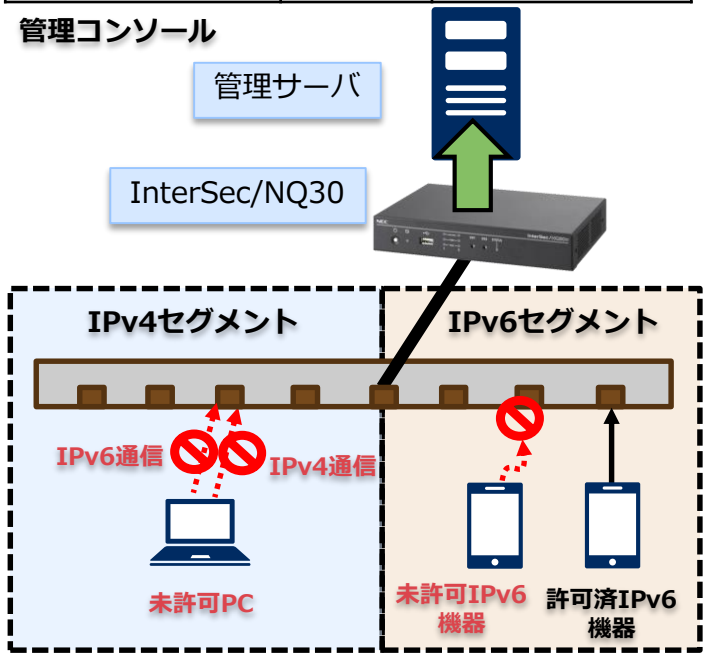
・セキュリティ対策として、
登録外の端末の接続を制限したい。
・IPv6対応製品を開発しているため、
部分的にIPv6セグメントが存在している。
・IPv4通信については接続制限を実施しているが、IPv6通信についても同様の対策が急務。

選定理由と効果

・類似製品は多くあるが、IPv4に加えてIPv6に対応していたことが最大のポイント。
・Windows 7は標準でIPv6が有効になっていることを知り、
従来の対策では不十分だと気づいたが、
本製品の導入により解決できた。
・IPv6機器が予想以上に存在することが分かった。

導入イメージ

MACアドレス	IPアドレス	IPv6　アドレス
0A:00:01:0A:00:01	1.1.1.1	2001:1234::1
0A:00:01:0A:00:02	1.1.1.2	2001:1234::2



10拠点、100セグメントを統合管理

導入事例：医療法人B病院様

ネットワーク内の端末をInterSec/NQ30で見える化、
医師や職員の勝手な機器の持ち込みを制限。

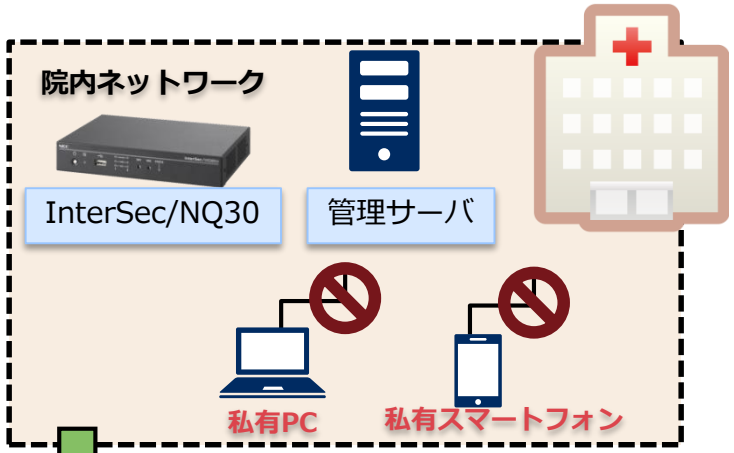
導入の背景

・医師や職員が勝手に私有のPCやタブレットを接続している状況のため、情報漏洩事故の不安を感じていた。
・ネットワークの使用ルールを徹底したいが、医師の権限が強いため運用での対策が困難であり、システムでの対策の必要性を感じていた。

効果

・許可された端末以外は接続ができなくなることで、自然と私有機器の持ち込みはなくなった。
結果、情報漏えい事故のリスクもなくなり、安心してネットワーク管理ができている。

導入イメージ



接続端末一覧

MACアドレス	IPアドレス	OS種別	コンピュータ名
0A:00:01:0A:00:01	1.1.1.1	Windows	HOST001
0B:00:02:0B:00:02	1.1.1.2	Windows	HOST002
0C:00:03:0C:00:03	1.1.1.3	iPhone	iPhone001

導入事例：金融業C社様

InterSec/NQ30とスイッチ連携を併用することで、
小規模の店舗についても本社と同様のセキュリティレベルを安価に実現。

導入の背景

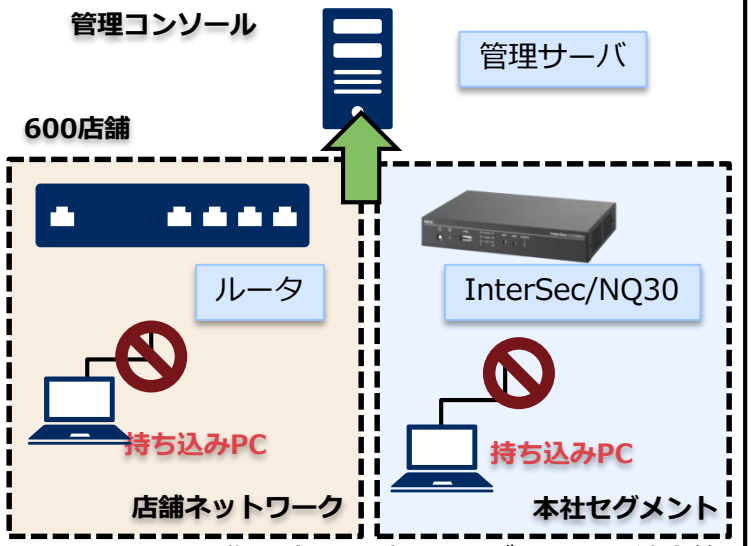
・数十セグメントある本社に加えて、600以上の店舗からなるネットワーク構成となっているが、各店舗に勝手にPCが接続されている痕跡あった。
・本社に加えて、不正に接続しているPCを検出できる仕組みを全ての店舗に導入したい。
ただし、PCが3台のみの小さな店舗もあり、全ての店舗にセンサーを置く構成は費用が高額になるため避けたい。

選定理由と効果

・複数社の製品を選定して見積もりを依頼したが、小さい店舗にはセンサーを置かずに安価に導入できたのはNECのみ。
・センサーでの管理とスイッチを利用しての管理を併用することで、全ての店舗にシステムを導入できた。管理も画面一つで統合管理でき、想定より簡単に運用ができている。

導入イメージ

MACアドレス	IPアドレス	エージェント名
0A:00:01:0A:00:01	1.1.1.1	InterSecNQ30
0B:00:02:0B:00:02	1.1.1.2	InterSecNQ30
0E:00:05:0E:00:05	1.1.1.5	SwitchManager



600拠点含む、計700セグメントを統合管理

動作環境・価格

動作環境 (マネージャ)

	DomainManager/SiteManager同居 DomainManagerのみ	SiteManagerのみ
OS	・Windows Server 2008 Standard（SP2） ・Windows Server 2008 Enterprise（SP2） ・Windows Server 2008 Standard x64（SP2） ・Windows Server 2008 Enterprise x64（SP2） ・Windows Server 2008 R2 Standard（SP1） ・Windows Server 2008 R2 Enterprise（SP1） ・Windows Server 2012 Standard ・Windows Server 2012 Datacenter ・Windows Server 2012 R2 Standard ・Windows Server 2012 R2 Datacenter ・Windows Server 2016 Standard ・Windows Server 2016 Datacenter	・Windows Server 2008 Standard（SP2） ・Windows Server 2008 Enterprise（SP2） ・Windows Server 2008 Standard x64（SP2） ・Windows Server 2008 Enterprise x64（SP2） ・Windows Server 2008 R2 Standard（SP1） ・Windows Server 2008 R2 Enterprise（SP1） ・Windows Server 2012 Standard ・Windows Server 2012 Datacenter ・Windows Server 2012 R2 Standard ・Windows Server 2012 R2 Datacenter ・Windows Server 2016 Standard ・Windows Server 2016 Datacenter ・Windows 7 Professional（SP1）/ x64（SP1） ・Windows 7 Ultimate（SP1） / x64（SP1） ・Windows 7 Enterprise （SP1） / x64（SP1）
CPU	Intel® Xeon® CPU E5502 @ 1.87GHz相当以上	Intel® Xeon® CPU E5502 @ 1.87GHz相当以上
メモリ	2GB以上	2GB以上
ディスク	40GB以上の空き容量	150MB以上の空き容量
備考	・.NET Framework 3.5 SP1 必須 ・Web コンソールの対応ブラウザはInternet Explorer 9～11 (ただし、OSがサポートしていないバージョンの利用は対象外) ・SQL Server 2008 R2 Express または SQL Server 2014 Express (SQL Server 2014 Expressは製品バンドル)	

動作環境 (RemoteConsole)

		RemoteConsole
OS	32bit	Windows 7 Professional（SP1） Windows 7 Ultimate（SP1） Windows 7 Enterprise（SP1） Windows 8.1 Pro Windows 8.1 Enterprise Windows 10 Pro Windows 10 Enterprise
	64bit	Windows 7 Professional（SP1） Windows 7 Ultimate（SP1） Windows 7 Enterprise（SP1） Windows 8.1 Pro Windows 8.1 Enterprise Windows 10 Pro Windows 10 Enterprise
CPU		1.87GHz以上
メモリ		1GB以上
ディスク		150MB以上の空き容量

動作環境 (スイッチ連携オプション)

	SwitchManager
OS	Windows Server 2008 Standard (SP2) Windows Server 2008 Enterprise (SP2) Windows Server 2008 Standard x64 (SP2) Windows Server 2008 Enterprise x64 (SP2) Windows Server 2008 R2 Standard (SP1) Windows Server 2008 R2 Enterprise (SP1) Windows Server 2012 Standard Windows Server 2012 Datacenter Windows Server 2012 R2 Standard Windows Server 2012 R2 Datacenter ※Windows Server 2016には対応していません
CPU	Intel® Xeon® CPU E5502 @ 1.87GHz相当以上
メモリ	2GB 以上
ディスク	1.1GB以上の空き容量
備考	・下記のいずれかがインストールされていること Java Runtime Environment Version 6 Java Runtime Environment Version 7 Java Runtime Environment Version 8

価格 (本体)

【センサー】

製品名	希望小売価格(税別)	月額保守料（税別）
InterSec/NQ30d	¥ 178,000	ハードウェア： ¥800 ソフトウェア： ¥1,700

【メディアキット・ライセンス(通常版)】

製品名	希望小売価格(税別)	月間保守料（税別）
InfoCage 不正接続防止 V5.3 メディアキット	¥20,000	ー
InfoCage 不正接続防止 V5.3 マネージャ 1ライセンス	¥290,000	¥3,700

【メディアキット・ライセンス(Lite版)】

製品名	希望小売価格（税別）	月間保守料（税別）
InfoCage 不正接続防止 V5.3 Lite リモートコンソール	¥145,000	¥1,900

【補足説明】

- メディアキットには、マネージャ、SwitchManagerの媒体を含みます。
- 1台の管理サーバで、InterSec/NQ30を400台まで管理可能です。

価格 (VLAN追加ライセンス)

【VLAN追加ライセンス】

製品	希望小売価格（税別）	月間保守料（税別）
InfoCage 不正接続防止 V5.3 1VLAN追加ライセンス	オープン価格	
InfoCage 不正接続防止 V5.3 3VLAN追加ライセンス		
InfoCage 不正接続防止 V5.3 10VLAN追加ライセンス		
InfoCage 不正接続防止 V5.3 30VLAN追加ライセンス		
InfoCage 不正接続防止 V5.3 100VLAN追加ライセンス		

【補足説明】

- **タグVLAN環境では1台のInterSec/NQ30で複数のVLANを監視できます。**
  その場合、”監視するVLAN数－１”の 「VLAN追加ライセンス」 が必要です。
- **InterSec/NQ30dは1台で32VLANまで管理可能です。**

(例)1台のNQで7つのタグVLAN環境を監視する場合、以下の製品が必要です。
- InterSec/NQ30 ：1台
- InterSec/NQ30 3VLAN追加ライセンス ： 2つ

価格 (スイッチ連携オプション)

【スイッチ連携オプションライセンス】

製品	希望小売価格（税別）	月間保守料（税別）
InfoCage 不正接続防止 V5.3 スイッチ連携オプション 100クライアントライセンス	¥500,000	¥6,300
InfoCage 不正接続防止 V5.3 スイッチ連携オプション 300クライアントライセンス	¥1,500,000	¥18,800
InfoCage 不正接続防止 V5.3 スイッチ連携オプション 1000クライアントライセンス	¥5,000,000	¥62,500
InfoCage 不正接続防止 V5.3 スイッチ連携オプション 3000クライアントライセンス	¥15,000,000	¥187,500

【補足説明】

- スイッチ連携機能で監視するクライアント数分のスイッチ連携オプションライセンスが必要です。
  監視するセグメント数分の購入が必要なセグメントライセンスもございます。
- スイッチ連携を利用する際のSwitchManagerの構成については、
  ご利用になる環境の情報を添えてご相談ください。
  - 1台のSwitchManagerに、100台までのスイッチを登録できます。
  - 目安として、1台のSwitchManagerで10,000件程度のホストを管理可能です。

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
端末情報の自動収集	○	○
未登録機器の遮断	○	○
アラート通知	○	○
IPv6対応	○	○
接続されているスイッチのポート検知	○	×
接続履歴の可視化	○	×
承認申請ワークフロー	○	×
機種別許可設定	○	×
資産管理製品との連携	○	○
InterSec/NQ30の冗長化	○	×
スイッチ連携	○	×
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
1台のNQで管理可能なVLAN数	32	32
最小構成価格	¥488,000 + 管理サーバ費用	¥323,000

InterSec/NQ30とスイッチ連携の比較

		スイッチ連携	InterSec/NQ30
構成		インテリジェントスイッチが必要 スイッチに認証設定が必要	セグメント毎の配置が必要
収集できる主な情報		MACアドレス、IPアドレス	MACアドレス、IPアドレス ホスト名、ＯＳ情報
接続許可条件		MACアドレスのみ	IP・MACアドレスの組み合わせ
不正端末の遮断方式		端末ごと(送信元MACアドレスで識別)に認証	偽装ARPで通信妨害
管理者権限の設定		SwitchManager単位	InterSec/NQ30単位 LANグループ単位
状態変更時の動作	設定の反映（青→赤） （赤→青）	再認証時	即時
	遮断解除時、端末側の復旧操作	ネットワーク再接続	操作不要で即時復旧

- **スイッチ連携機能で利用できない主な機能**
  IPv6対応、接続履歴の可視化、承認申請ワークフロー、
  機種別許可設定、資産管理製品との連携、マルウェア対策製品連携

InterSec/NQ30cとNQ30dの比較

	InterSec/NQ30c	InterSec/NQ30d
型番	N8100-1400Q	N8100-1500Q
希望小売価格（税別）	￥178,000	￥178,000
1台のInterSec/NQ30で管理可能なホスト数（※１）（※2）	4,000件（V3.8～） 2,000件（V3.6～V3.7） 1,000件（～V3.4）	8,000件（V5.2～） 4,000件（V3.8～V5.1） 2,000件（V3.6～V3.7） 1,000件（～V3.4）
1台のInterSec/NQ30に登録可能な承認ポリシーの数	100,000件	100,000件
監視セグメント数 (非タグVLAN環境/タグVLAN環境)	1セグメント/16VLAN	2セグメント/32VLAN
「NQ冗長化機能」で待機系NQに設定できるVLANインターフェースの数	32個	64個
電源スイッチ	有り (電源スイッチ押下でシャットダウンが可能) 電源ケーブルを挿したときは自動起動 (ボタン押下は不要)	有り (電源スイッチ押下でシャットダウンが可能) 電源ケーブルを挿したときは自動起動 (ボタン押下は不要)
LANポート	10Base-T/100Base-TX/ ×1ポート	10Base-T/100Base-TX/ 1000Base-T　×2ポート
工場出荷時のバージョン	2.2～3.8（※3）	2.2～5.2（※3）

（※1）一日に検出したMACアドレス数（目安としてホスト一覧の最終検出日がその日になっているものの件数）が該当します。
（※2）サーバレスのLite版を利用する場合は1台のInterSec/NQ30で管理可能なホスト数が1,000件となります。
（※3）バージョン2.2から3.8および5.2に対応するモジュールがプリインストールされています。
　　ダウングレードする初期化を実施するとバージョンはV2.2となります。

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

http://jpn.nec.com/infocage/prevention

お問い合わせ・資料請求は
こちらから受け付けております。


Orchestrating a brighter world
NEC