Orchestrating a brighter world

NEC

# InfoCage 不正接続防止 紹介資料

2017年10月 NEC

# 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

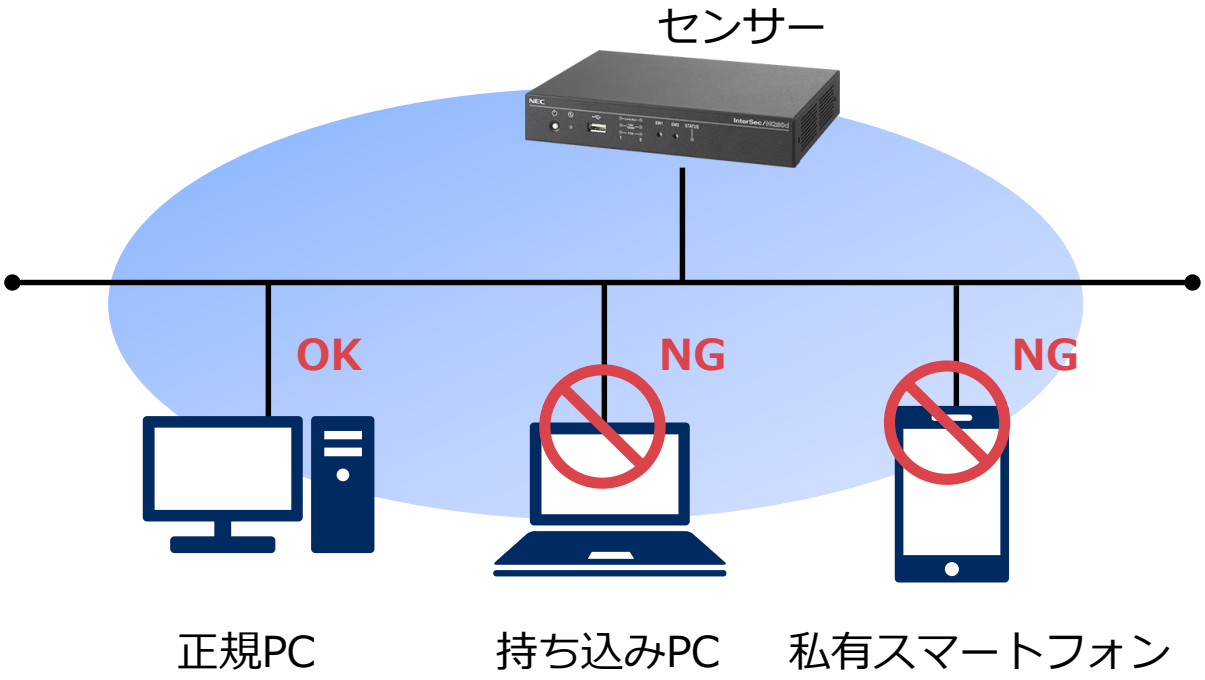
## 持ち込みPC対策に対するネットワーク管理者の声

- 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

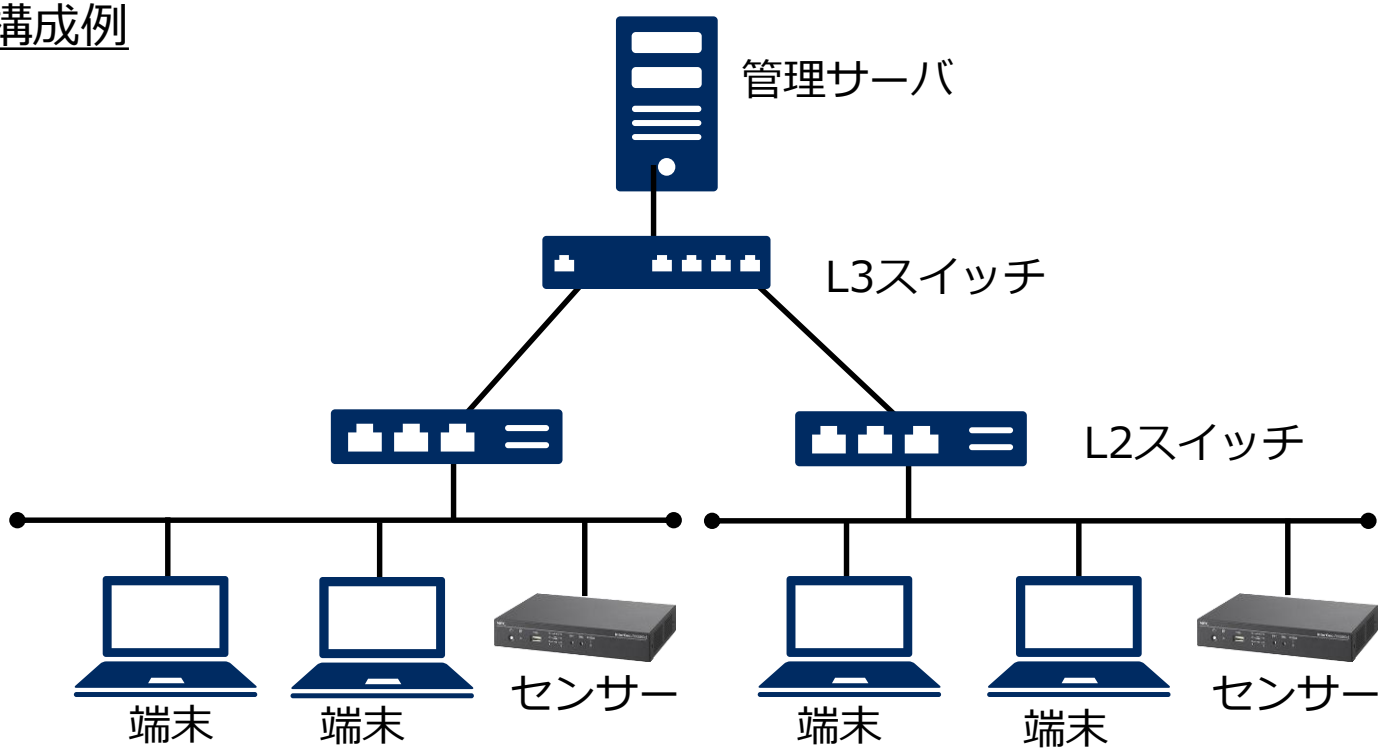
## エージェントレス

- 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 |

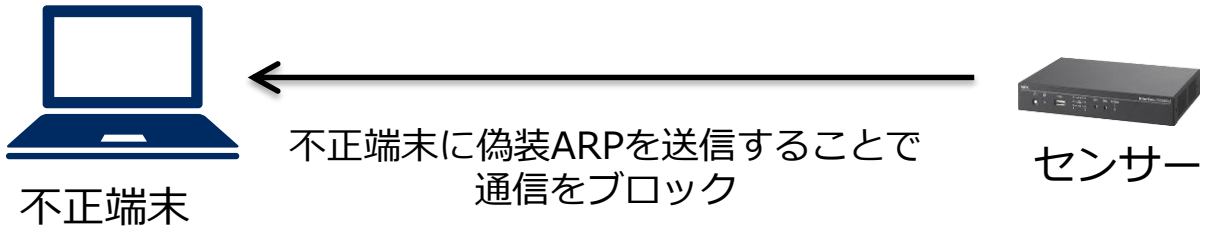
※機器種別はパケットからの推測であるため、環境によって正しく判別できない場合があります。
※接続ポートとスイッチアドレスは通常版でのみ表示できます。

# 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

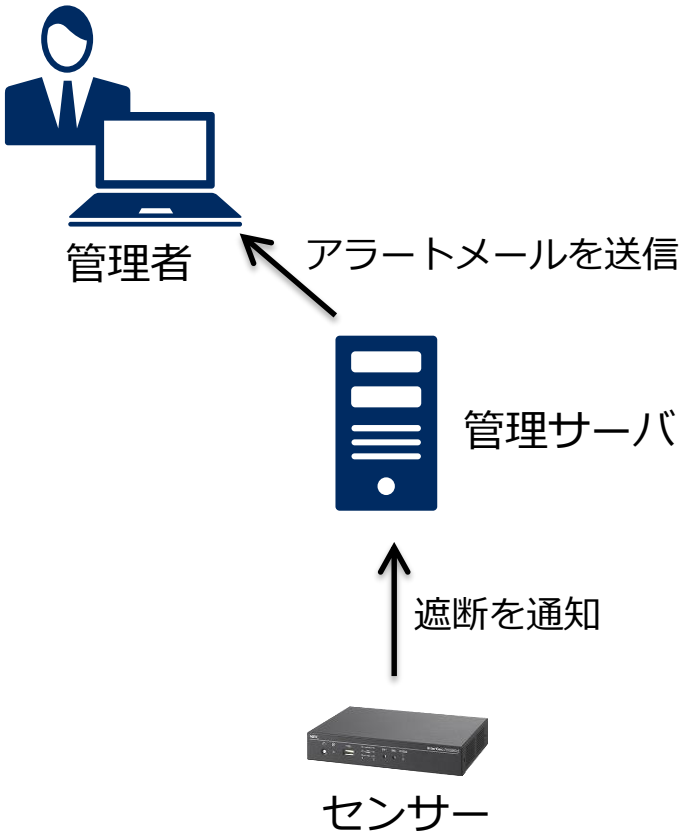
## 不正端末を遮断した際に、管理者にアラートを通知できます。

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

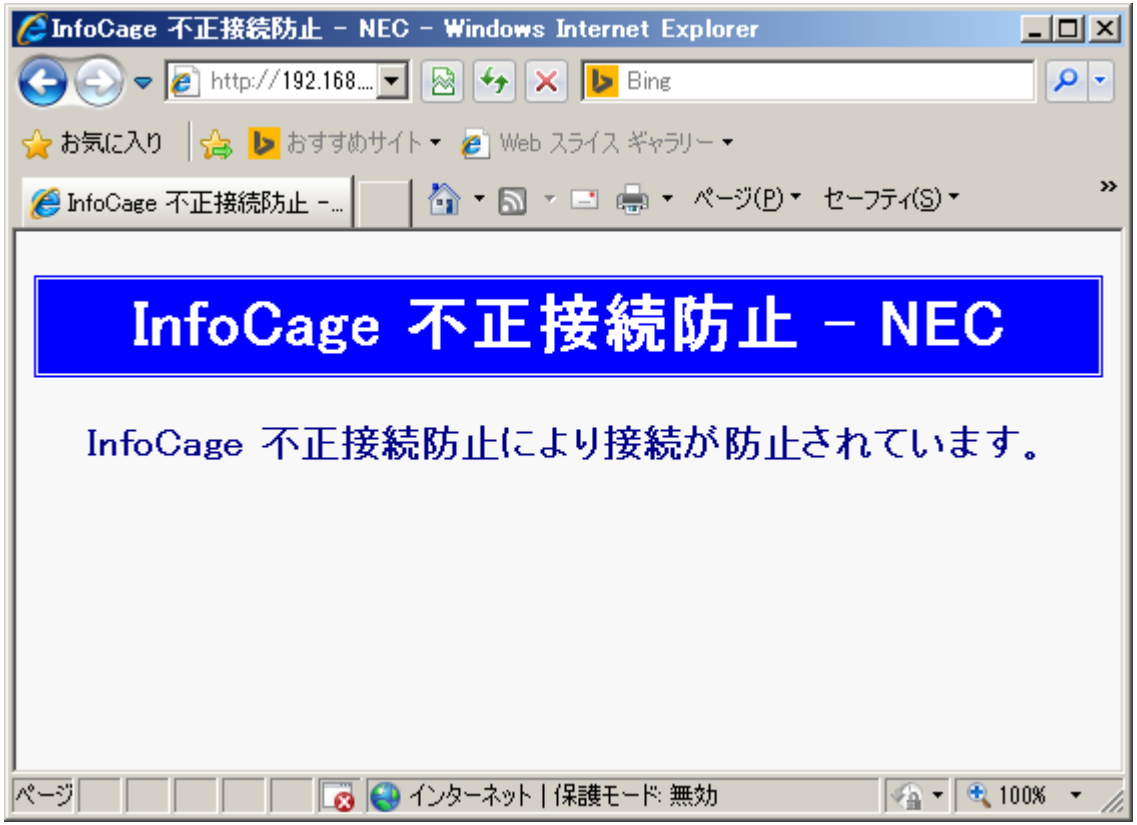
・
・
・



# 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。



# 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 |

# 構成例

# 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。

# 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 2015年度実績：シェアNo.1**

※出典：㈱富士キメラ総研 2016 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

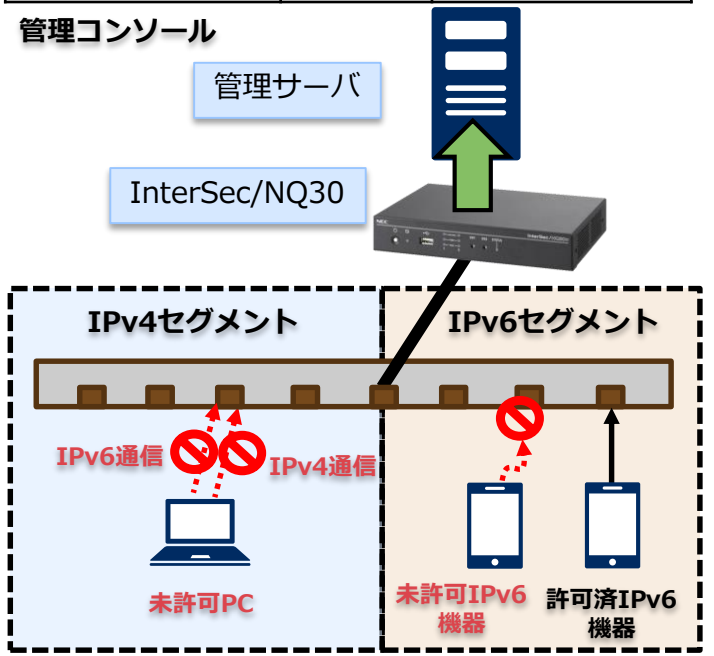
・セキュリティ対策として、
登録外の端末の接続を制限したい。
・IPv6対応製品を開発しているため、
部分的にIPv6セグメントが存在している。
・IPv4通信については接続制限を実施しているが、IPv6通信についても同様の対策が急務。

## 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。

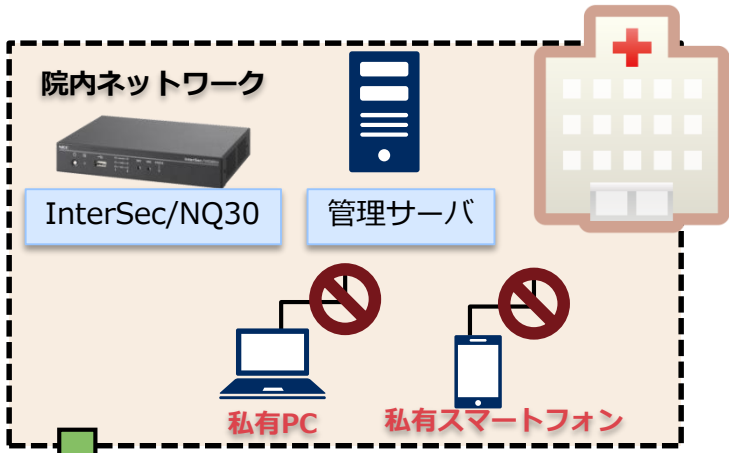
## 導入の背景

・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 |


Orchestrating a brighter world
NEC