

# InfoCage 不正接続防止 V5.3 強化内容説明資料

2017年10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。

## 強化項目一覧

- ① ウイルスバスター連携
- ② 承認申請ワークフロー
- ③ 冗長化機能の強化
- ④ アラート検索の強化
- ⑤ Deep Discovery Inspector(DDI)連携の条件指定
- ⑥ syslog/SNMPトラップ アラート追加
- ⑦ DomainManager無償化
- ⑧ 最新プラットフォーム対応

# ①ウイルスバスター連携

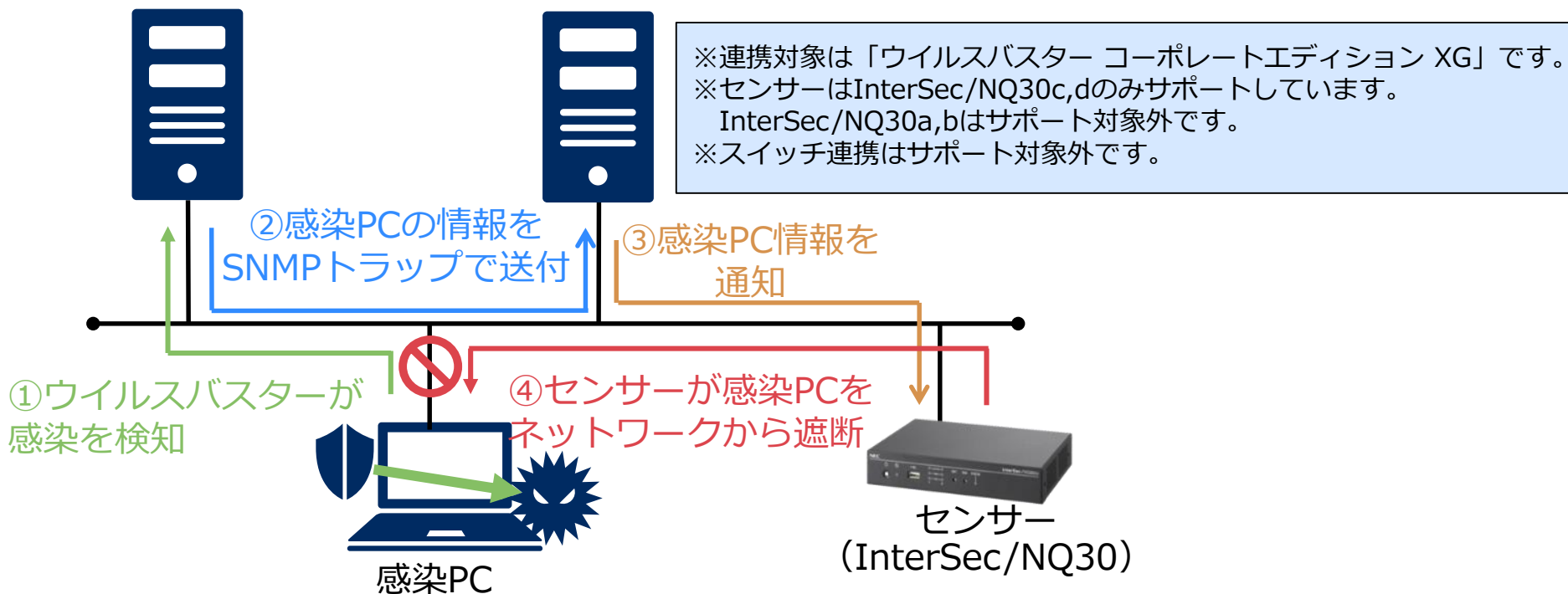
マルウェア対策製品「ウイルスバスター」が検知したマルウェア感染端末を自動的にネットワークから遮断できるようになりました。

管理画面の表示イメージ

状態	IP アドレス	検知 製品名	イベント名
×	192.168.0.1	VirusBuster	ウイルス/不正プログラム

ウイルスバスター  
Corp.サーバ

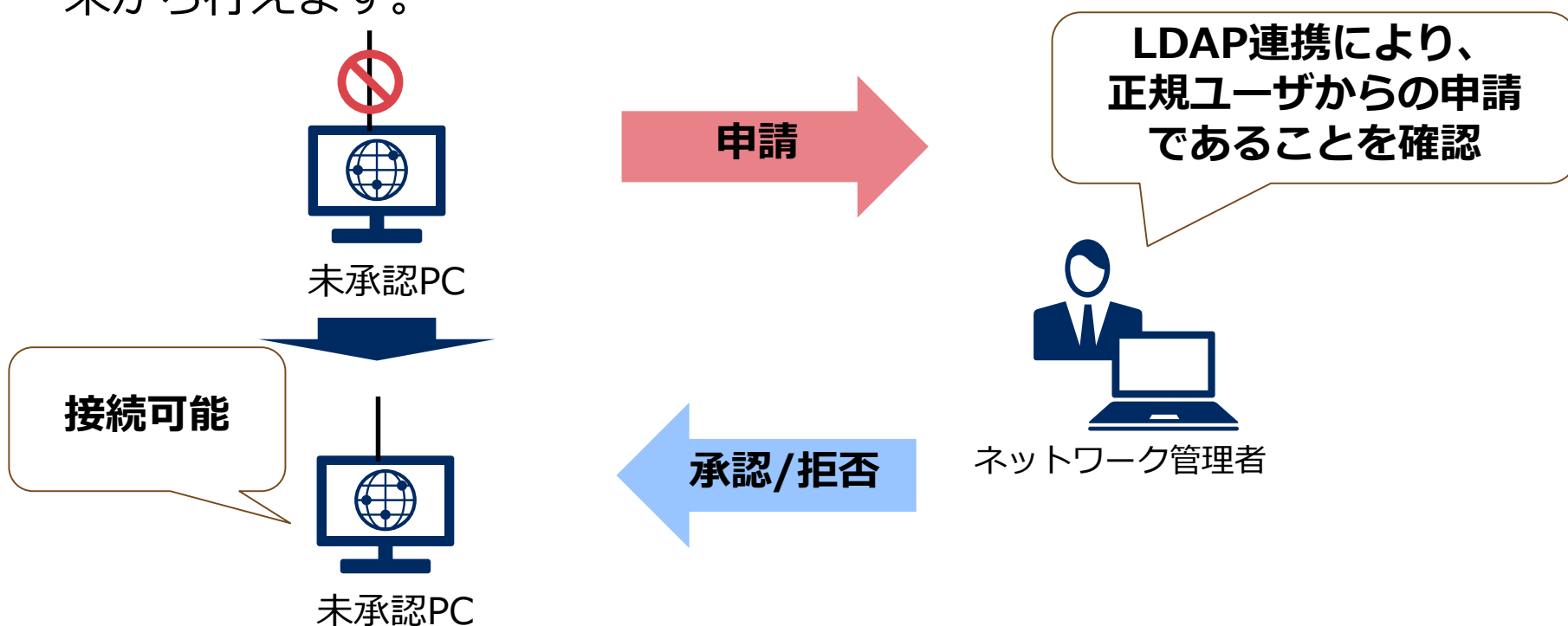
InfoCage 不正接続防止  
管理サーバ



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。

## ②承認申請ワークフロー

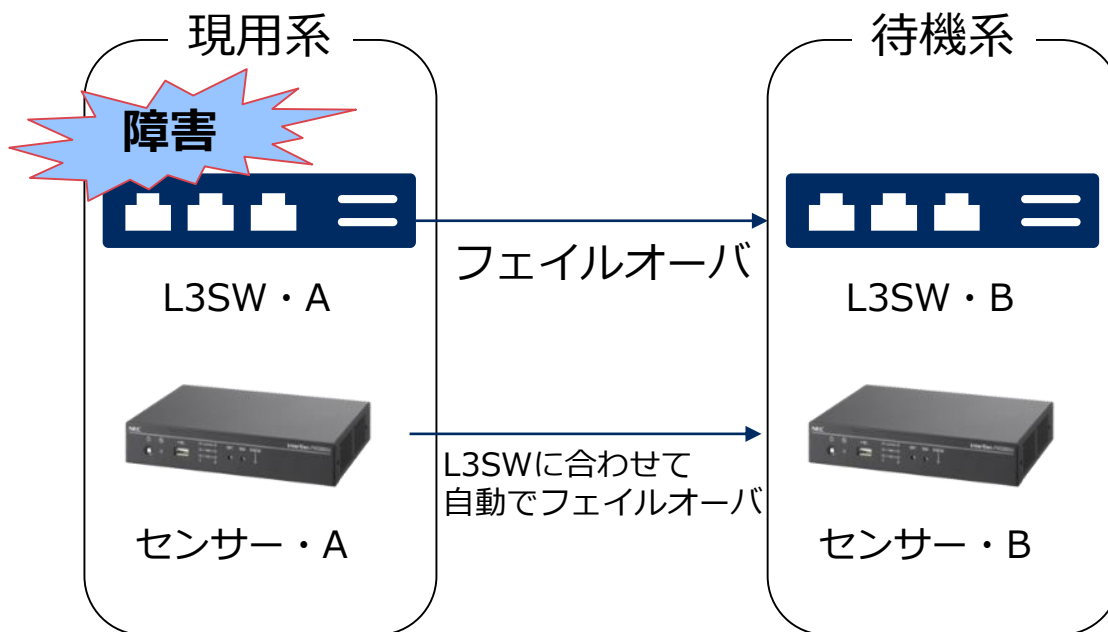
- 承認申請ワークフローにより、正規ユーザが未承認PCを使う際、そのPCから管理者に申請できます。
- LDAP連携により、正規ユーザによる申請であることを確認した上で承認することが可能です。正規ユーザになりすました不正ユーザによる申請の排除に役立ちます。
- Webブラウザを持たない機器の申請を、Webブラウザを持つ承認済み端末から行えます。



### ③冗長化機能の強化

L3スイッチの冗長化をサポートしました。現用系/待機系両方のL3スイッチにセンサーを接続しておくことで、L3スイッチのフェイルオーバーが発生した際、センサーの現用系/待機系も自動で切り替わり、ネットワークの監視を継続できます。

センサーのフェイルバック機能を追加しました。



## ④アラート検索の強化

- MACアドレスやIPアドレスを指定してアラートを検索できるようになりました。
- インシデント発生時など、特定のアドレスに絞ってアラートを確認したい際に役立ちます。

サイトID	<input type="text"/>	エージェント名	<input type="text"/>	VLAN ID	<input type="text"/>
MACアドレス	<input type="text"/>	IPアドレス	<input type="text"/>		
開始時期 (yyyy/mm/dd)		終了時期 (yyyy/mm/dd)			
<input checked="" type="checkbox"/> 新規ホストの検出	<input type="checkbox"/> エージェント通信不可	<input type="checkbox"/> SM通信不可			
<input type="checkbox"/> ホストの接続防止	<input type="checkbox"/> エージェント通信回復	<input type="checkbox"/> SM通信回復			
<input type="checkbox"/> ホストの申請許可	<input type="checkbox"/> フェイルオーバー	<input type="checkbox"/> 防止対象検知			
<input type="checkbox"/> ホストの申請拒否	<input type="checkbox"/> 冗長化不可	<input type="checkbox"/> syslog/SNMPトラップ受信			
<input type="button" value="戻る"/>		<input type="button" value="アラート通知設定"/>			
<input type="button" value="検索"/>					

## ⑤DDI連携の条件指定、⑥syslog/SNMPトラップ アラート追加

### ⑤Deep Discovery Inspector(DDI)連携の条件指定

- DDI連携機能において、イベント名と重要度の組み合わせで条件を指定できるようになりました。
- 従来通り、推奨設定をそのまま使用することもできます。

### ⑥syslog/SNMPトラップ アラート追加

- 外部連携システムからsyslogまたはSNMPトラップを受信したことを示すアラートを追加しました。
- 通知の受信に対してアラートを出すため、実際に遮断を行わない場合でも通報できます。
- 自動遮断に該当しない場合でも、管理者の判断で遮断を実施できます。



# ⑦DomainManager無償化、⑧最新プラットフォーム対応

## ⑦DomainManager無償化

- DomainManagerを無償化しました。

## ⑧最新プラットフォーム対応

- 管理サーバがWindows Server 2016に対応しました。
- Linux版NetworkAgentがCentOS 7.3に対応しました。
- Microsoft Edgeでの承認申請画面および防止メッセージの表示、UserAgentによるOS判別に対応しました。

 **Orchestrating** a brighter world

**NEC**