

# HOME-Network Sensor デモレポートにおける見るべきポイント

HOME-Network Sensor のデモ実施後に発行されるレポートに関して、見方と訴求すべきポイントを解説します。  
各チェックポイントをご確認の上、対応する原因およびセキュリティリスクをお客様にご提示ください。

## デモレポート例（接続端末数ページ）

HOME type-NS デバイスリストレポート

XX株式会社 様

平素は格別のお引き立てを賜り、厚く御礼申し上げます。HOME-Network Sensor

◆設置期間

設置期間2018年03月01日 ~ 2018年04月27日

◆接続端末数

検知総数41件

◆OS内訳 ※正確でないことがあります

Windows	7
MAC OS	4
Apple	8
Android	4
Linux	2
その他	16
Windows XP	1

◆接続端末内訳(端末名が記載されていないもの)

機器総数	41
端末名あり	11
端末名なし	30

◆接続端末内訳(メーカー別)

Apple	12
SONY	3
CANON	3
Hon	2
SAXA	2
NEC	2
BUFFALO.INC	2
ASKEY	1
Atmark	1
BIOSTAR	1
DELL	1
FUJITSU	1
Hewlett	1
Intel	1
YAMAHA	1
Iomega	1
Liteon	1
Micro-Star	1
Murata	1
RICOH	1
unknown	1
IBM	1

Check1 : ネットワークに想定以上の端末が接続されいませんか？

Check2 : サポート終了済の OS はありませんか？

Check3 : 許可していないスマートフォン、タブレットはありますか？

Check4 : 端末名が記載されていないものはありますか？

Check5 : 購入していない端末、把握していないメーカー端末はありますか？

ワンポイント : PC

ワンポイント : 購入していないメーカーの製品がないかご確認ください。

Windows

MAC OS

その他

端末名

Apple

SONY

CANON

Hon

SAXA

NEC

BUFFALO.INC

ASKEY

Atmark

BIOSTAR

DELL

FUJITSU

Hewlett

YAMAHA

Iomega

Liteon

Micro-Star

Murata

RICOH

unknown

IBM

Copyright © 2017 Canon Marketing Japan Inc. ALL RIGHT RESERVED

■デモレポート例（デバイスリストページ）

HOME type-NS デバイスリストレポート

XX株式会社 様

Check4: 端末名が記載されていないものはありますか？

Check2: サポート終了済の OS はありますか？

日時	ステータス	端末名	ベンダー情報	OS
2018/04/27 14:58	未登録	WORKGROUP¥PC1	Hon	Windows 7
2018/04/27 14:58	未登録	WORKGROUP¥PC2	Liteon	Windows 7
2018/04/27 15:45	未登録	WORKGROUP¥PC3	Intel	Windows 7
2018/04/27 16:04	未登録	WORKGROUP¥PC4	FUJITSU	Windows 10
2018/04/27 16:04	未登録	WORKGROUP¥PC5	ASKEY	Windows 10
2018/04/27 17:07	未登録	WORKGROUP¥2F	Micro-Star	Windows 10
2018/04/27 17:55	未登録	WORKGROUP¥3F	unknown	Windows 10
2018/04/27 14:58	未登録	SONY		Sony Ericsson Android
2018/04/27 14:58	未登録	SONY		Sony Ericsson Android
2018/04/27 16:03	未登録	SONY		Sony Ericsson Android
2018/04/27 17:55	未登録	DELL		RHEL 6.4 or Centos6.4
2018/04/27 14:53	未登録	NEC		Microsoft Windows XP
2018/04/27 14:58	未登録	Apple		Mac OS X 10.x
2018/04/27 14:59	未登録	Apple		Mac OS X 10.x
2018/04/27 16:03	未登録	Apple		Mac OS X 10.x
2018/04/27 14:53	未登録	Apple		Mac OS X
2018/04/27 17:55	未登録	IBM		Linux 2.4-2.6
2018/04/27 14:53	未登録	Apple		Apple iPod
2018/04/27 14:53	未登録	Apple		Apple iPod
2018/04/27 17:55	未登録	NEC		Android Tablet
2018/04/27 14:53	未登録	CANON		
2018/04/27 14:53	未登録	BUFFALO.INC		
2018/04/27 14:53	未登録	WORKGROUP¥RNPE	RICOH	
2018/04/27 14:53	未登録	CANON		
2018/04/27 14:53	未登録	CANON		
2018/04/27 14:59	未登録	SAXA		
2018/04/27 14:59	未登録	YAMAHA		

**Check4** : 端末名が記載されていないものはありますか？

**Check2** : サポート終了済の OS はありますか？

**Check5** : 購入していない端末、把握していないメーカー端末はありますか？

**Check3** : 許可していないスマートフォン、タブレットはありますか？

■各チェックポイントに対する解説

No.	項目	状態	推測される原因	セキュリティリスク
Check1	接続端末数	端末数を事前にヒアリングしておき、当該項目がその数を大幅に上回っている	<ul style="list-style-type: none"><li>・私有端末の持ち込み</li><li>・第三者の不正アクセス</li></ul>	<ul style="list-style-type: none"><li>・私有端末への重要情報のコピー、それに伴う情報流出</li><li>・私有端末からのウイルス蔓延</li><li>・端末数超過によるスループット遅延、業務効率低下</li></ul>
Check2	OS 内訳	WindowsXP など、サポート切れの OS がリストアップされている	<ul style="list-style-type: none"><li>・古いシステムを使い続けている</li></ul>	<ul style="list-style-type: none"><li>・脆弱性をついた攻撃被害</li></ul>
Check3	OS 内訳	iOS や Andoroid 等、スマートフォンやタブレット OS がリストアップされている ※会社携帯等が存在しない場合	<ul style="list-style-type: none"><li>・私有端末の持ち込み</li></ul>	<ul style="list-style-type: none"><li>・私有端末への重要情報のコピー、それに伴う情報流出</li><li>・私有端末からのウイルス蔓延</li><li>・端末数超過によるスループット遅延、業務効率低下</li></ul>
Check4	接続端末内訳 (端末名が記載していないもの)	端末名が記載されていない端末がある ※会社にて端末名を用いて管理をしている場合	<ul style="list-style-type: none"><li>・私有端末持ち込み</li><li>・第三者の不正アクセス</li></ul>	<ul style="list-style-type: none"><li>・私有端末への重要情報のコピー、それに伴う情報流出</li><li>・私有端末からのウイルス蔓延</li><li>・端末数超過によるスループット遅延、業務効率低下</li><li>・不正アクセスによる重要情報のコピー、それに伴う情報流出</li><li>・不正アクセスによる攻撃の踏み台化</li></ul>
Check5	接続端末内訳 (メーカー別)	購入した記録のないメーカーの端末がリストアップされている	<ul style="list-style-type: none"><li>・私有端末持ち込み</li><li>・第三者の不正アクセス</li></ul>	<ul style="list-style-type: none"><li>・私有端末への重要情報のコピー、それに伴う情報流出</li><li>・私有端末からのウイルス蔓延</li><li>・端末数超過によるスループット遅延、業務効率低下</li><li>・不正アクセスによる重要情報のコピー、それに伴う情報流出</li><li>・不正アクセスによる攻撃の踏み台化</li></ul>

■セキュリティリスクに対するトーク

セキュリティリスク	トーク
私有端末への重要情報のコピー、それに伴う情報流出	すでに私有端末が持ち込まれているかもしれません、また、ウイルスが社内に蔓延しているかもしれません。 <a href="#">→NS 提案へ</a>
私有端末からのウイルス蔓延	
不正アクセスによる重要情報のコピー、それに伴う情報流出	意図せずセキュリティ脅威の加害者になっているかもしれません。 <a href="#">→NS+UTM 提案へ</a>
不正アクセスによる攻撃の踏み台化	
端末数超過によるスループット遅延、業務効率低下	業務効率が悪化により無駄なコストが発生しているかもしれません。 <a href="#">→NS 提案へ</a>
古いシステムを使い続けている	古いシステムを使っていてセキュリティ脅威の被害を受けても誰も助けてくれません。 <a href="#">→UTM 提案へ</a>

以上