医療分野における
IT セキュリティの実態や課題について

（JNSA OT セキュリティ WG イベント (2026/4/24)）

京都大学 医学部附属病院 医療情報企画部 講師
京都大学 大学院情報学研究科 社会情報学コース (兼任)
奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 客員准教授

油谷 曉 (ゆたに あきら)
yutani@kuhp.kyoto-u.ac.jp

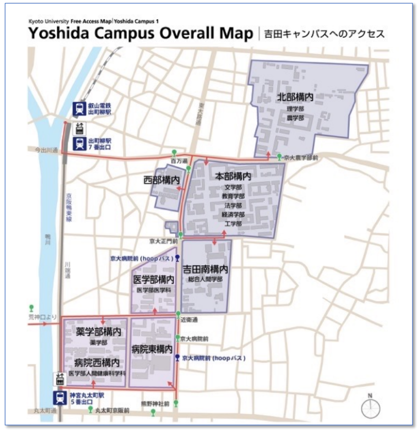
もくじ

2

京都大学 医学部附属病院

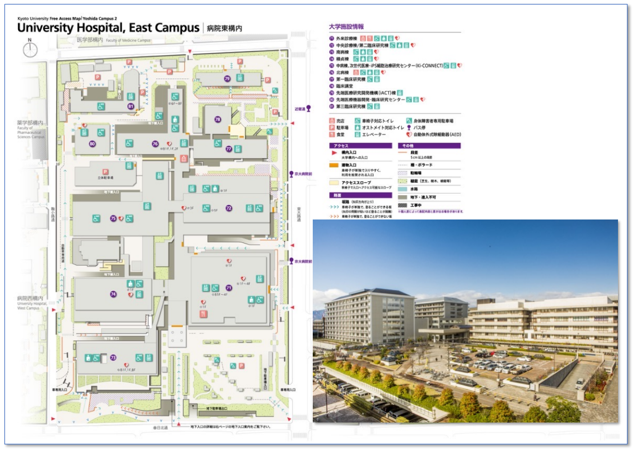
Google Map より

4


Yoshida Campus Overall Map
吉田キャンパスへのアクセス
北部構内
西部構内
本部構内
吉田南構内
医学部構内
薬学部構内
病院東構内
病院西構内

5

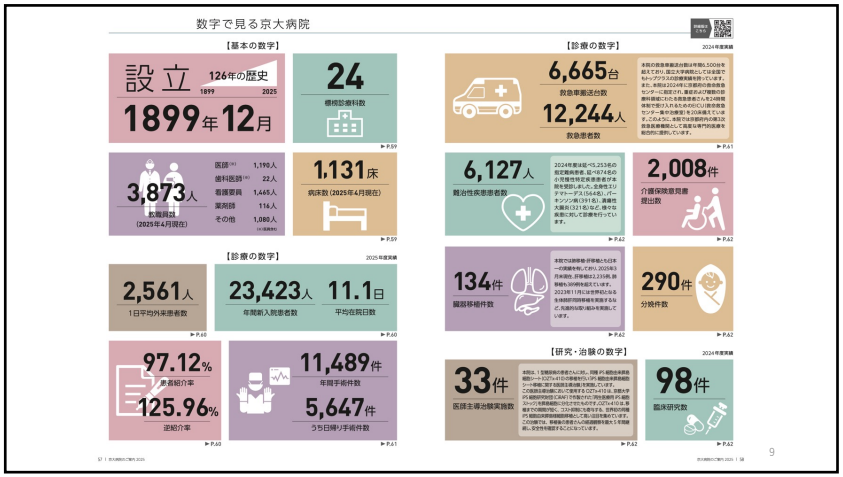
6


University Hospital, East Campus
病院東構内

7


建物・フロアご案内板
Information
病院東構内 建物案内図
病院東構内 フロア案内

8



病院情報ネットワーク

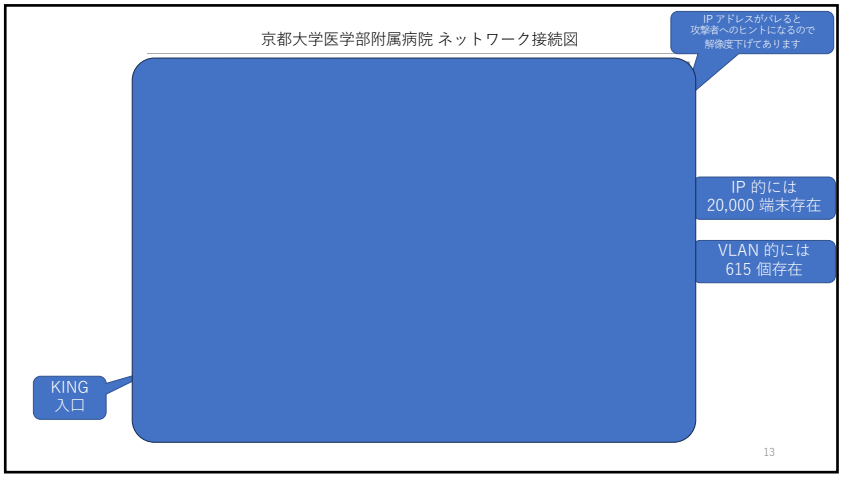
病院の外部ネットワーク

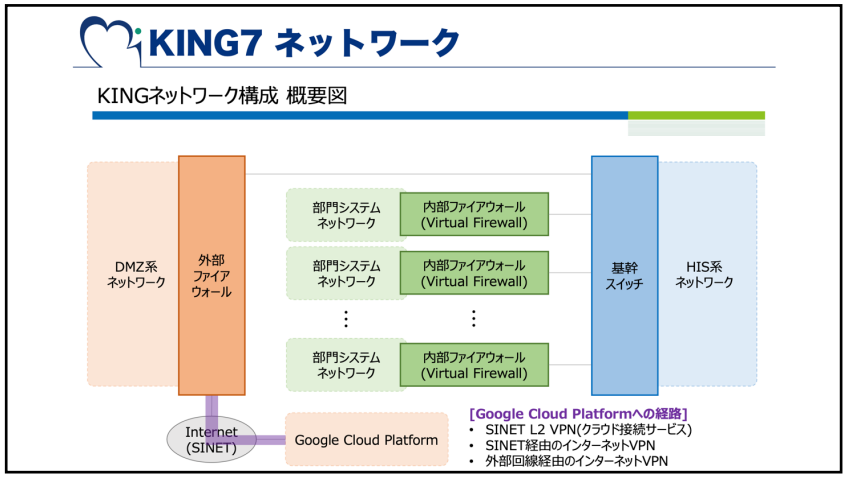
- 理想
  - 完全独立
    - 外部ネットワークを一切繋がない
    - メール等は別途事務用ネットワークを構築
- 現実
  - DMZ (DeMilitarized Zone : 非武装地帯) 構築
    - 病院外にファイアウォールの一部として出島を構築し，そこで情報交換
  - VPN (Virtual Private Network) 環境
    - 外部からのシステムメンテナンス時に利用

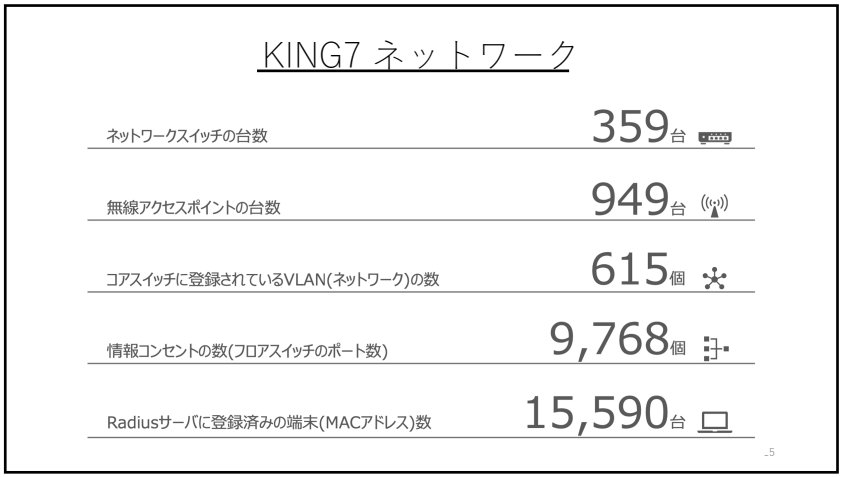
Wikipedia より

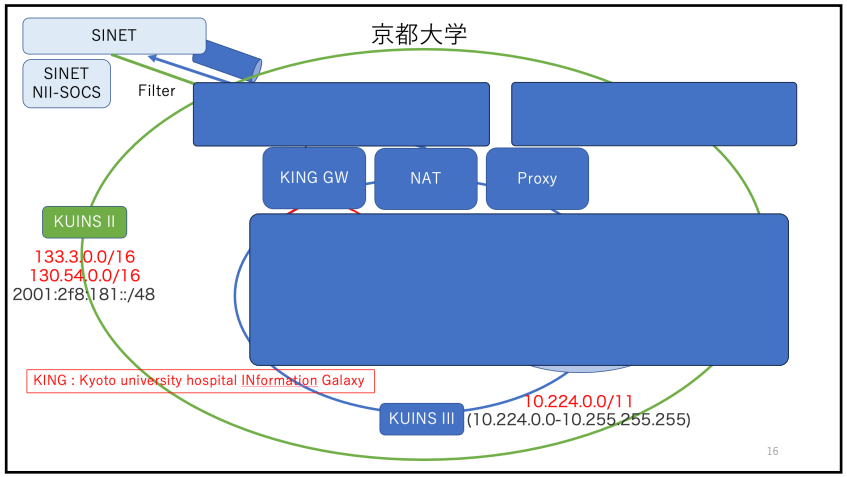
病院の内部ネットワーク

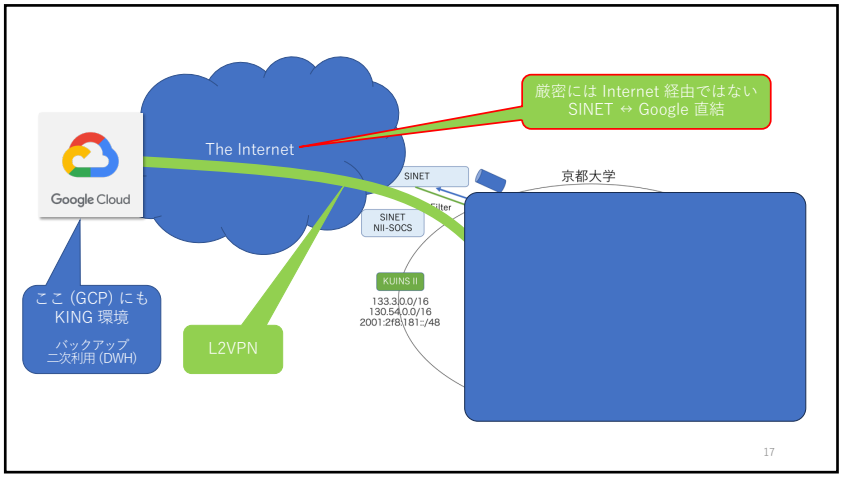
- 電子カルテ
  - 患者情報用 DB を守る (病院内からでもアクセスを限定)
  - ユーザは電子カルテを構築した仮想化サーバから使用
    - SBC (Server Based Computing) 方式を使用 (Citrix)
- 各部門システム
  - 部門システム間の通信，基本は不可 (アクセス制限)
  - 利用診療科，電子カルテ等，システムに必要な部分のみ開放 (IP, ポート)
- VPN (IPsec)
  - 接続企業と担当システム間のみ通信可能 (アクセス制限)
  - 接続時に毎回申請，接続ログ確認

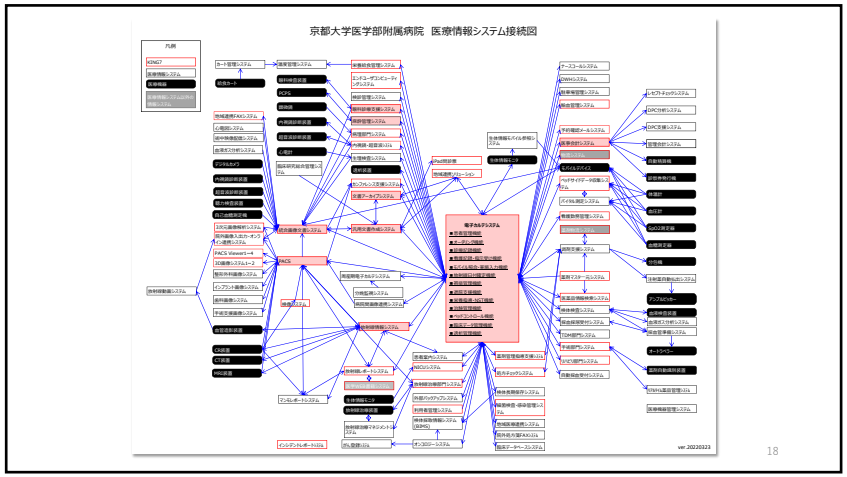

京都大学医学部附属病院 ネットワーク接続図
IP アドレスがバレると
攻撃者へのヒントになるので
解像度下げてあります
IP 的には
20,000 端末存在
VLAN 的には
615 個存在
KING
入口
13

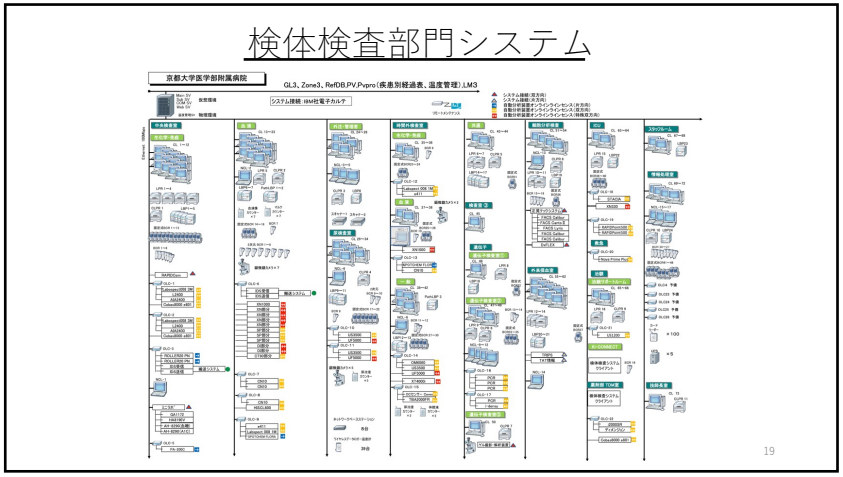

KING7 ネットワーク
KINGネットワーク構成 概要図
DMZ系
ネットワーク
外部
ファイア
ウォール
部門システム
ネットワーク
内部ファイアウォール
(Virtual Firewall)
部門システム
ネットワーク
内部ファイアウォール
(Virtual Firewall)
部門システム
ネットワーク
内部ファイアウォール
(Virtual Firewall)
基幹
スイッチ
HIS系
ネットワーク
Internet
(SINET)
Google Cloud Platform
[Google Cloud Platformへの経路]
• SINET L2 VPN(クラウド接続サービス)
• SINET経由のインターネットVPN
• 外部回線経由のインターネットVPN


KING7 ネットワーク
ネットワークスイッチの台数
359台
無線アクセスポイントの台数
949台
コアスイッチに登録されているVLAN(ネットワーク)の数
615個
情報コンセントの数(フロアスイッチのポート数)
9,768個
Radiusサーバに登録済みの端末(MACアドレス)数
15,590台
5


SINET
SINET
NII-SOCS
Filter
京都大学
KING GW
NAT
Proxy
KUINS II
133.3.0.0/16
130.54.0.0/16
2001:2f8:181::/48
KING : Kyoto university hospital INformation Galaxy
10.224.0.0/11
KUINS III
(10.224.0.0-10.255.255.255)
16


厳密には Internet 経由ではない
SINET ↔ Google 直結
The Internet
Google Cloud
SINET
京都大学
Filter
SINET
NII-SOCS
KUINS II
133.3.0.0/16
130.54.0.0/16
2001:2f8:\181::/48
ここ (GCP) にも
KING 環境
バックアップ
二次利用 (DWH)
L2VPN
17


京都大学医学部附属病院 医療情報システム接続図
18


検体検査部門システム
京都大学医学部附属病院
19

セキュリティについて

KING7 ネットワーク（再掲）

ネットワークスイッチの台数	359台
無線アクセスポイントの台数	949台
コアスイッチに登録されているVLAN(ネットワーク)の数	615個
情報コンセントの数(フロアスイッチのポート数)	9,768個
Radiusサーバに登録済みの端末(MACアドレス)数	15,590台

21

セキュリティ #1

- VLAN
  - フラット（VLAN 無し）は危ない
    - 診療部門と事務部門だけの 2 つに分離のみでの運用 !!
  - 部門システム，診療科，診察室など，全て VLAN で分離すべき
    - 院内の何処にでも VLAN を出す（dynamic VLAN）
    - 必要な部分のみ VLAN 間接続 ⇒ しかし，管理がとても大変
  - インシデント時の要塞化
    - 各システムのミニマムセットを定義（人命第一）
      - 実際の通信内容を把握

VLAN (Virtual LAN)

22

セキュリティ #2

- VPN
  - Fortigate は ヨドバシ で !?（早い，安い）
    - 脆弱性やバージョン管理など，永続的なメンテナンスは？
  - メンテナンスの裏口
    - サプライチェーン問題に直結
  - 接続ログの管理も重要

23

セキュリティ #3

- EDR と NDR
  - 侵入前提で防御
  - IDS と IPS は過去
- インシデント監視
  - 院内での対応には人的リソースに無理がある
  - 外部 SOC に 24/365 監視を依頼
    - 攻撃を検知したのでネット切断 !! ⇐ 病院で大丈夫 ??
    - ランサム感染等，その後（フォレンジックとレジリエンス）は ??
- ランサム保険（仮称）無いの？
  - 全病院が加入 !?

EDR (Endpoint Detection and Response)
NDR (Network Detection and Response)

IDS (Intrusion Detection System) 不正侵入検知
IPS (Intrusion Prevention System) 不正侵入防止

SOC (Security Oparation Center)

24

責任分界点

病院ネットワークの一般論です

責任分界点の実情

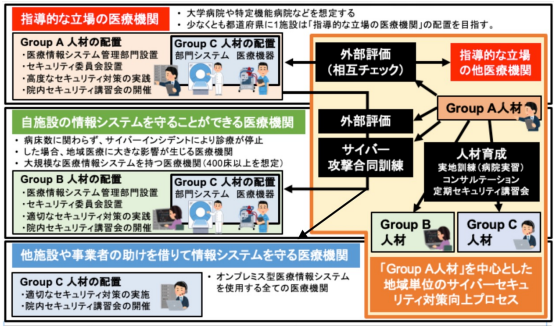
- グレー !!　⇒ 誰が対応し責任を取るの ??
  - 病院から業者に 設計/構築 を丸投げ (体質？できる担当者が居ない ??) ①②③
    - 病院設立時，追加システム導入時，インシデント発生時
    - その結果，関係する業者数が膨大に，そして疎結合，全体把握が困難 ④
  - 継続性 (運用/保守/セキュリティ対応) が軽視されている ⑤
    - 機器保守，バージョンアップ，脆弱性対応，設定変更
    - 業者から継続案を提示，病院側が却下，立場上くつがえせない
  - 業者の問題点 ⑥
    - 製品や環境構築において，セキュリティの概念がない ⑦
    - そもそも，レベルが低い ⑧

⑨ セキュリティ機器
- ヨドバシで買ってこい !?
- パスワードはそのまま
- 脆弱性対応せず

26

人材育成

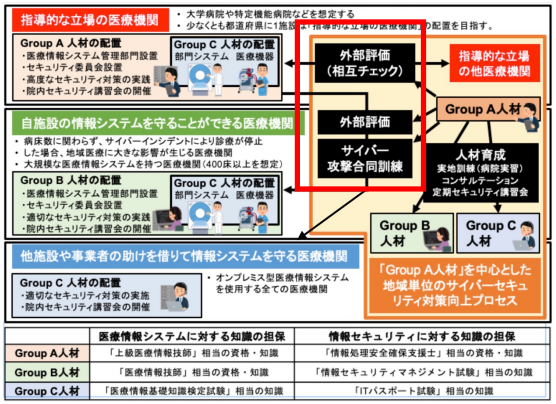
厚労科研 武田班 (2023 - 2024)
安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究



	医療情報システムに対する知識の担保	情報セキュリティに対する知識の担保
Group A人材	「上級医療情報技師」相当の資格・知識	「情報処理安全確保支援士」相当の資格・知識
Group B人材	「医療情報技師」相当の資格・知識	「情報セキュリティマネジメント試験」相当の知識
Group C人材	「医療情報基礎知識検定試験」相当の知識	「ITパスポート試験」相当の知識

28

厚労科研 黒田班 (2025 - 2026)
地域における共通基盤・集中管理体制によるサイバーセキュリティの実証のための研究



	医療情報システムに対する知識の担保	情報セキュリティに対する知識の担保
Group A人材	「上級医療情報技師」相当の資格・知識	「情報処理安全確保支援士」相当の資格・知識
Group B人材	「医療情報技師」相当の資格・知識	「情報セキュリティマネジメント試験」相当の知識
Group C人材	「医療情報基礎知識検定試験」相当の知識	「ITパスポート試験」相当の知識

29

ネットワーク情報収集

ネットワーク情報収集

- SNMP (Simple Network Management Protocol)
  - ネットワーク機器に状況を問い合わせるための規約
  - 各機器の静的な情報を入手

各機器からの静的な情報

- NetFlow
  - 流れているパケットのトラフィック情報 (ヘッダ部分) を各機器より入手
  - Cisco 社オリジナル，対応ベンダー少々，別途 sFlow (サンプリング) 等あり

各機器からのトラフィック情報

- ポート・ミラー
  - 機器から通信そのものを複製 (ミラー) して入手
  - 機器内を通過する全てのデータを入手可能 (容量問題あり)

機器から通信データの全てを入手

31

病院ネット状況の把握

- Cisco 社
  - Secure Network Analytics (PoC 中)
    - NetFlow にて全スイッチからトラフィック情報収集，異変を監視 (NDR)
- Claroty 社
  - xDome for Healthcare (PoC (2025/6/5 → 10/23) 完了)
    - 院内コアスイッチをミラーしてトラフィック収集
    - 医療機器の判別，リスク判別
- Alaxala 社
  - AX-NM (Network Manager)
    - SNMP にて全スイッチから資源情報収集 (IP 接続状況 (20,000 IP 強で安定))
  - AX-NV (Network Visualization) (PoC 中)
    - 院内コアスイッチをミラーしてトラフィック情報収集 (VLAN 間の通信は見える → 600 OK !!)
    - NetFlow 併設可能なので，未端情報はこちらから収集予定 ← 未遂

32

Secure Network Analytics

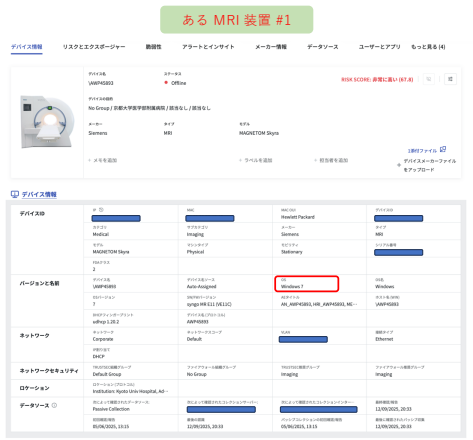
Secure Network Analytics

xDome for Healthcare

xDome for Healthcare
CLAROTY

37

xDome for Healthcare
CLAROTY



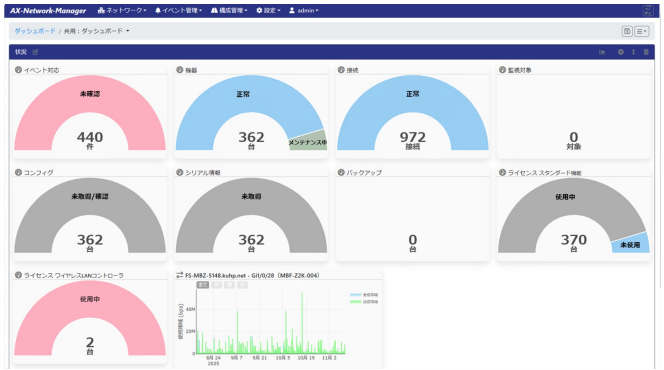
38

AX-NM

AlaxalA
A FORTINET Company

AX-NM
AlaxalA
A FORTINET Company

ダッシュボード画面



AX-NM
AlaxalA
A FORTINET Company

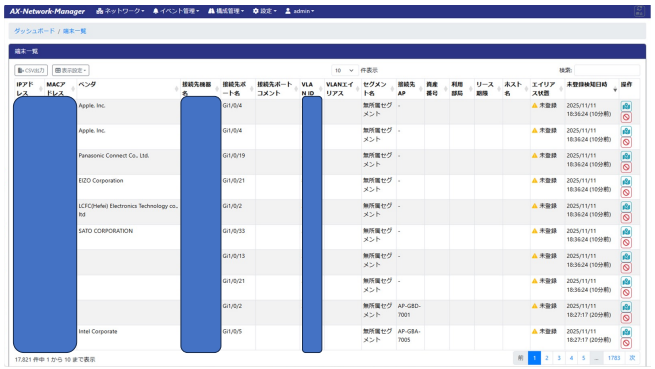
メニュー

AX-NM
AlaxalA
A FORTINET Company

機器一覧画面

端末一覧画面

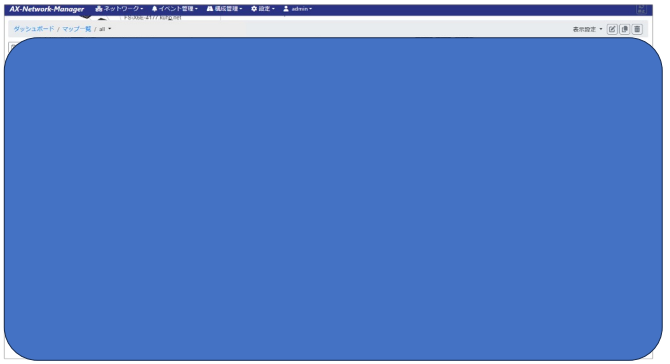
AX-NM



45

マップ画面

AX-NM



46

AX-NV

メニュー画面

AX-NV

48

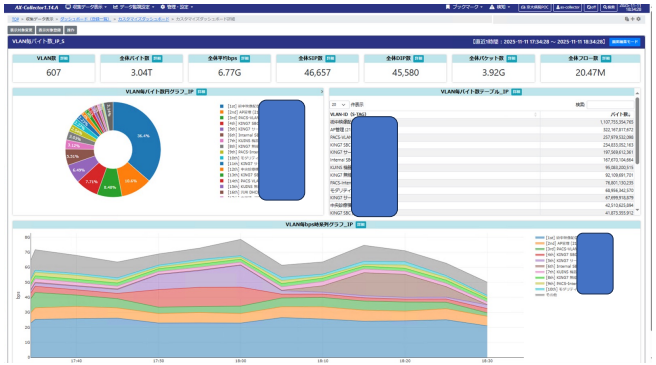
全体トラフィック

AX-NV

49

VLAN 毎トラフィック

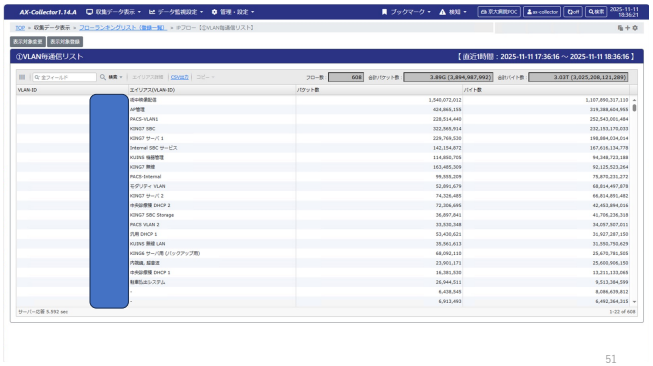
AX-NV



50

VLAN 毎トラフィック

AX-NV



51

トラフィック詳細

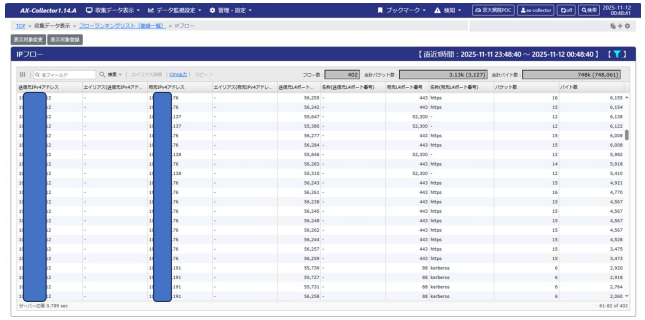
AX-NV

52

特定 IP からの通信

AX-NV

AlaxalA
A FORTINET Company

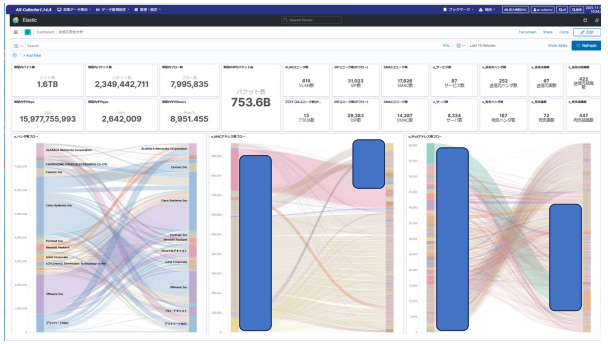


53

トラフィック詳細 #1

AX-NV

AlaxalA
A FORTINET Company

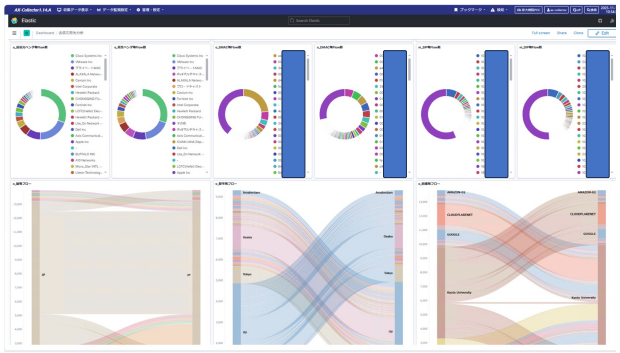


54

トラフィック詳細 #2

AX-NV

AlaxalA
A FORTINET Company

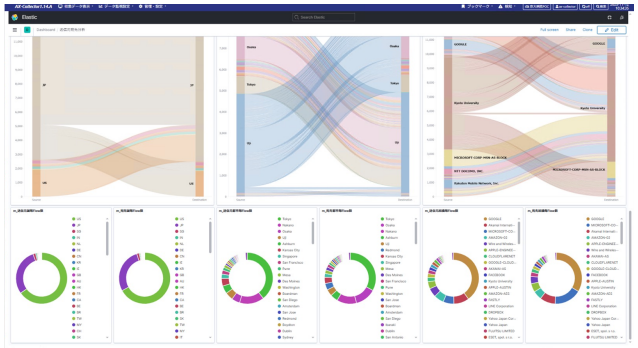


55

トラフィック詳細 #3

AX-NV

AlaxalA
A FORTINET Company



56

ネット監視ツール群 (まとめ)

- Cisco 社
  - Secure Network Analytics (PoC 中)
    - NetFlow にて全スイッチからトラフィック情報収集，異変を監視 (NDR)

通信監視・検知
SOC 向け

- Claroty 社
  - xDome for Healthcare (PoC (2025/6/5 → 10/23) 完了)
    - 院内コアスイッチをミラーしてトラフィック収集
    - 医療機器の判別，リスク判別

機器のリスク管理
強力な可視化

- Alaxala 社
  - AX-NM (Network Manager)
    - SNMP にて全スイッチから資源情報収集 (IP 接続状況)
  - AX-NV (Network Visualization) (PoC 中)
    - 院内コアスイッチをミラーしてトラフィック情報収集 (VLAN 間の通信は見える → 600 OK !!)
    - NetFlow 併設可能なので，未端情報はこちらから収集予定 ← 未遂

ネット状況の詳細把握
少々，専門家向け

SOC : Security Operation Center

57

少々悩ましいこと

駆逐すべきか？

- こんなアプリを知ってますか？
  - Chrome Remote Desktop (Google)
  - Team Viewer
  - Soft Ether
  - Tail Scale

院内の PC に仕込まれると
院外の何処からでも勝手に VPN される

情報の持ち出し や ウイルス感染 を危惧

↓

これまでの苦労は何だったんでしょう
… な，アプリ達です !!

- 通信のモニタは出来ます → 実際に使用されています …
- 使用不可になる設定を入れても，最終的にはイタチごっこ
  → なので「啓蒙して皆の正義感に訴えてみます !!」
  こっそり通信モニタは続けます

59

おわり

60