BluStellar

Interop Tokyo 2026

病院運営を支えるセキュリティ基盤とICT環境の提供

2026年7月

NEC
BluStellarシナリオ統括部

NEC \Orchestrating a brighter world

本資料でお伝えしたいこと

医療DX推進に伴うセキュリティ強化の必要性と、効率的な対策の進め方

背景

- 医療DX推進が病院の業務効率化、医療の質向上に不可欠
- 医療従事者の不足や病院経営環境の悪化

課題

- 境界防御の限界
- 攻撃高度化による経営リスクの増大
- 予算の制約

対応方針

✓ 現行環境の可視化
リスク分析

✓ NW構成見直し

✓ セキュリティ対策の
段階導入とコスト適正化

Agenda

1. 医療DXの必要性
2. 医療DX推進に向けたセキュリティ対策強化の必要性
3. NECが推奨する病院のセキュリティ対策
4. セキュリティ対策をより十全に行うためのNW運用負担の抑制

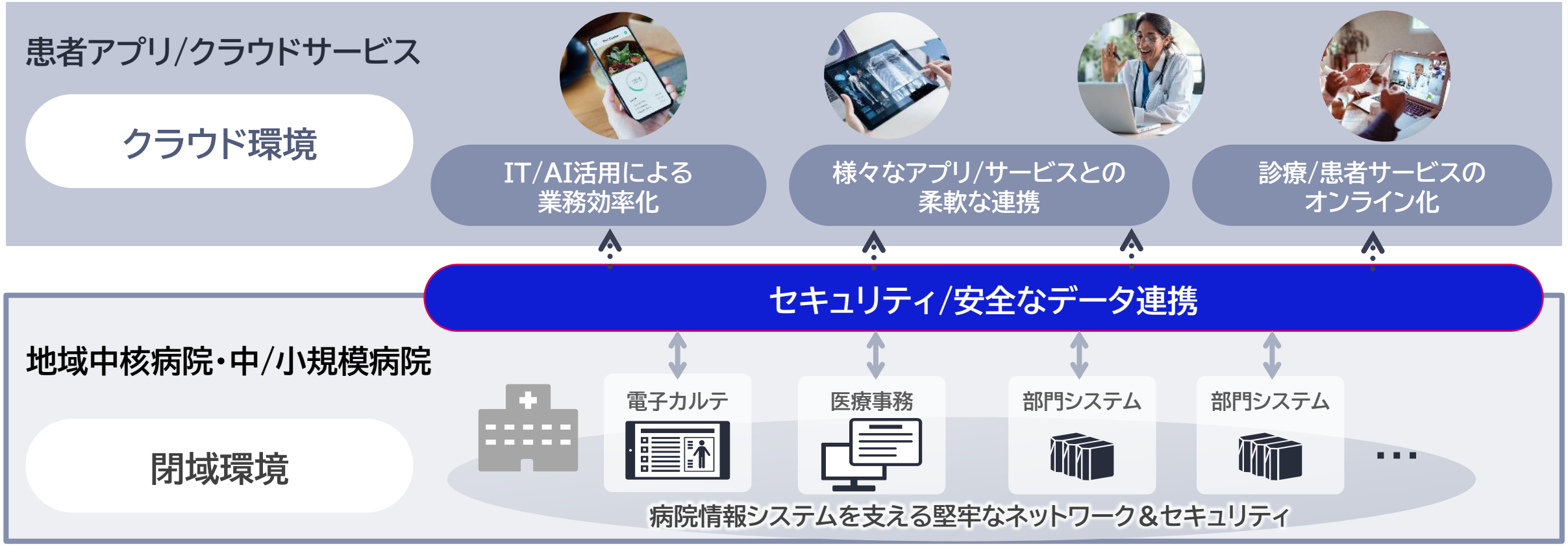
1. 医療DXの必要性

医療DX

BluStellar

医療従事者の不足を補い、質の向上を目指す医療DX※の取組みが増加

医療DXによる業務改革の推進により、医療データの連携やシステムのクラウド化が進むと、現状のセキュリティ対策では対応しきれない可能性があります。



医療DX推進のためには、新たな脅威へ対しセキュリティ対策の見直しが必要

2. 医療DX推進に向けたセキュリティ対策強化の必要性

医療DX推進にともなうセキュリティ対策強化の必要性

BluStellar

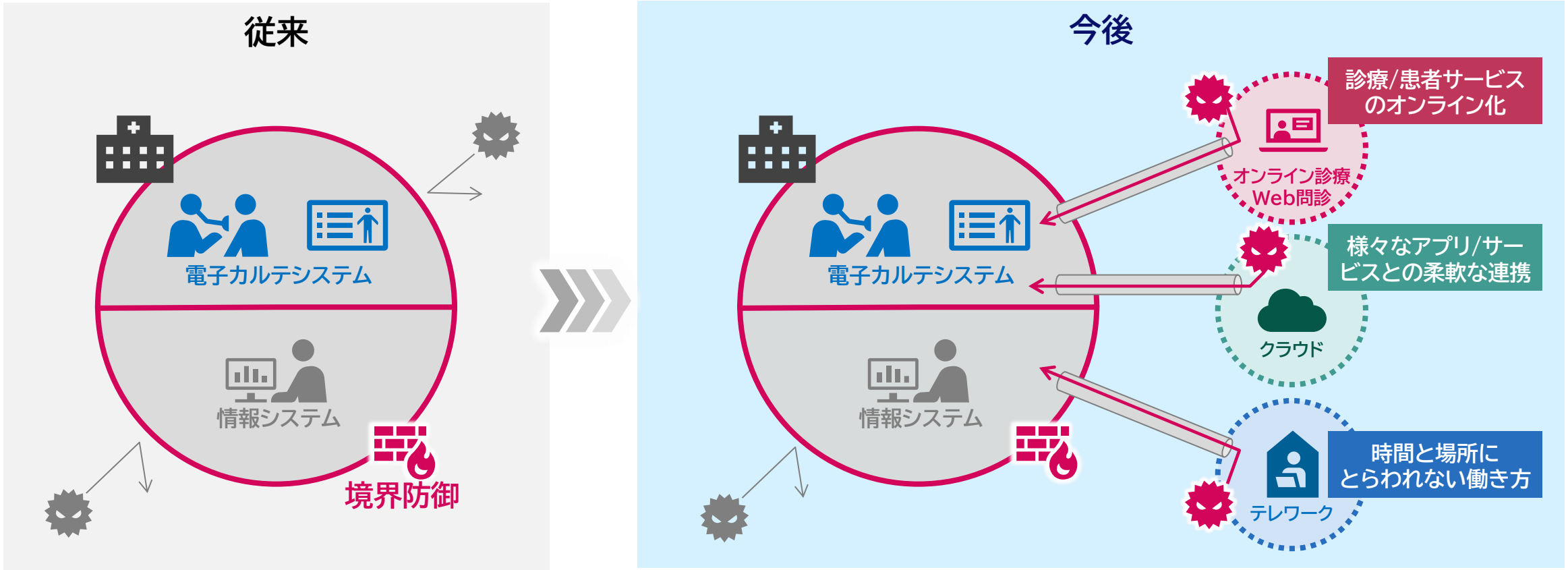
医療DX推進に伴い、医療情報システムへの攻撃ポイントの増加とセキュリティ被害の病院経営への影響が拡大するため、医療DX推進のために限られた予算内でセキュリティを見直し、強化する必要があります。

課題１	医療DX推進にともなう境界型防御の見直し
課題２	医療情報システム被害の病院経営への影響拡大
課題３	セキュリティ対策予算が限られる

課題1　医療DX推進にともなう境界型防御の見直し

BluStellar

医療DXの推進にともない、クラウドサービスなど外部との接続が増え、今後は従来の境界型防御での対策では不十分となることが想定されます。

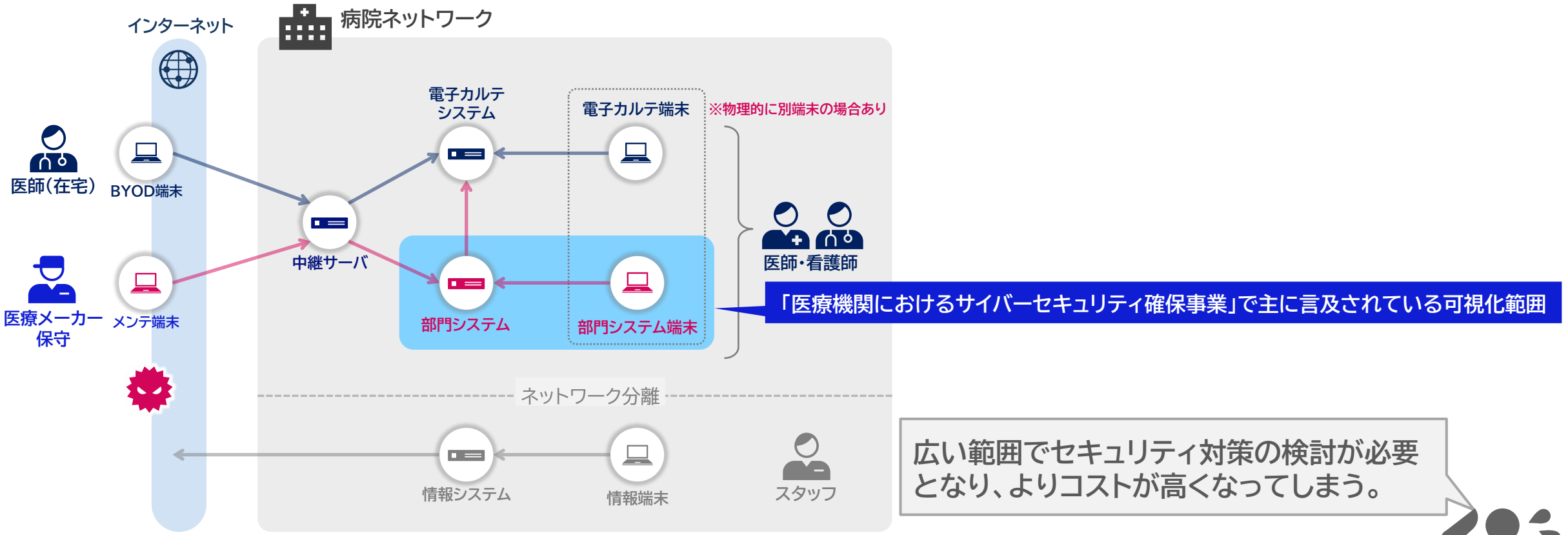


これまでの境界防御では防げない、
新しいセキュリティ脅威に対応しなければ

課題1　医療DX推進にともなう境界型防御の見直し

BluStellar

医療DX推進により、従来の境界内外に存在する複数部門のシステム・端末の連携が増加するため、セキュリティ被害を抑制するための対策箇所が増加し、インフラ全体を見渡した部門横断でのセキュリティ対策見直しが必要になります。



通信範囲の例

課題２ 医療情報システム被害の病院経営への影響拡大

BluStellar

医療機関におけるサイバー攻撃被害も発生している中、病院としての持続可能性の確保にはセキュリティ対策に対する継続的な見直しと投資が不可欠です。

①法令・規制の遵守

・個人情報保護法や3省2ガイドラインへの対応と準拠
・IT-BCP策定指針に沿った計画

Political

②経済的損失の防止と被害の最小化

・経済的損失や資産の損害を未然に防ぐ予防策
・有事の際の対応コストを削減するためのリスク管理

Economic

③患者情報の保護・社会的信用の確保

・患者情報を守ることによる患者からの信頼性構築
・医療機関としての社会的責任の確保

Social

④技術革新への適応と高度化するサイバー攻撃対策

・技術の進歩に合わせたセキュリティ対策
・日々高度化するサイバー攻撃に対する防御策

Technological

セキュリティ対策に対する継続的な見直しと投資の方針策定が重要

①法令・規制の遵守　医療機関向けガイドラインの経緯

BluStellar

2005年にe-文書法対応、個人情報保護対応を行うため、情報セキュリティ管理のガイドラインとして策定

以降、各種制度の動向や情報システム技術の進展等に対応して改定されているので、院内環境の継続的な見直しが必要です。

策定・改定	版	策定・改定概要
2005年	1	医療情報システムのセキュリティ管理を目的として策定
2007年	2	重要インフラとしての医療情報システムという観点からの対応
2008年	3	個人情報施策の議論およびモバイル端末普及への対応
2009年	4	個人情報施策の議論およびモバイル端末普及への対応
2010年	4.1	民間事業者のデータセンターにおける外部保存に関する対応
2013年	4.2	調剤済み処方せん及び調剤録等の外部保存への対応
2016年	4.3	「電子処方せんの運用ガイドライン」への対応
2017年	5	医療機関等の範囲の明確化、改正個人情報保護法対応、サイバー攻撃の動向への対応
2021年	5.1	クラウドサービスへの対応、認証・パスワードに関する対応、サイバー攻撃等による対応、外部保存受託事業者の選定基準対応
2022年	5.2	外部アプリケーションとの連携における利用者の認証・認可、ランサムウェアによる攻撃への対応、電子署名に関する記載の改定
2023年	**6**	**全体構成見直し（概説編・経営管理編・企画管理編・システム運用編の4編構成） 技術的な動向（外部委託・外部サービス利用、情報セキュリティに関する考え方、新技術・制度・規格の変更への対応）の整理**

厚生労働省「医療情報システムの安全管理に関するガイドライン第6.0版の概要及び主な改定内容」を参考にNECにて加筆修正
https://www.mhlw.go.jp/content/10808000/001102596.pdf

②経済的損失の防止と被害の最小化

BluStellar

医療機関のセキュリティインシデントは経営に深刻な打撃を与えるため、継続的なセキュリティ対策の更新と投資が不可欠です。

①患者情報漏えいによる金銭被害

▲ 6.0億

JNSAのJOモデルより1,000名の
電子カルテ情報が週出した場合の推定損害賠償額

JNSA「情報セキュリティインシデントに関する調査報告書 別紙」
https://www.jnsa.org/result/incident/2018.html

②病院業務停止による機会損失

▲ 8.6億

平均病床数（335床）の一般病院が1か月診療停止と
なった場合の医業収益の機会損失額

日本病院会「2024年度　病院経営定期調査 結果報告（概要）」
https://www.hospital.or.jp/shk/index.html

③事故対応費用

▲ 0.6億

過去事例や業者ヒアリングを基にした対応費用
（調査費用、データ復旧費用、応急処置費用等）

JCIC「サイバーリスクの数値化モデル」に記載の日本の過去事例からの費用
https://www.j-cic.com/reports.html

JCIC「サイバーリスクの数値化モデル」より被害指標を抜粋
https://www.j-cic.com/reports.html

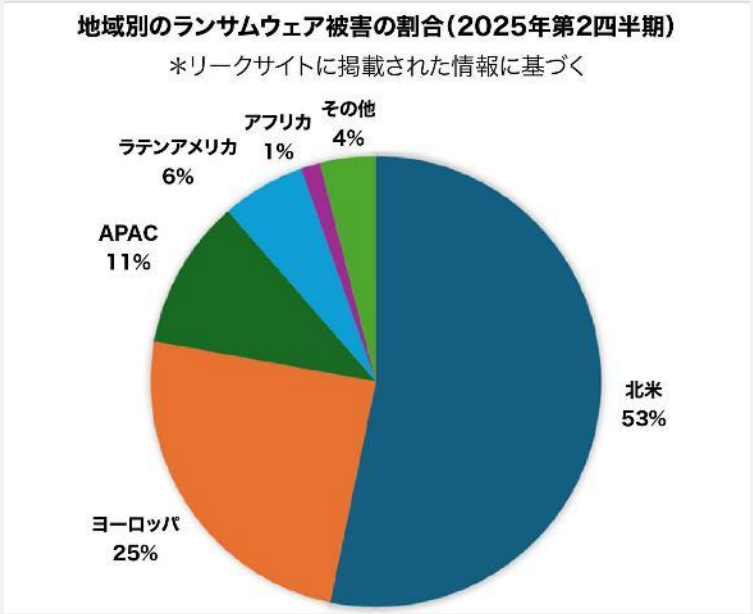
③患者情報の保護・社会的信用の確保

BluStellar

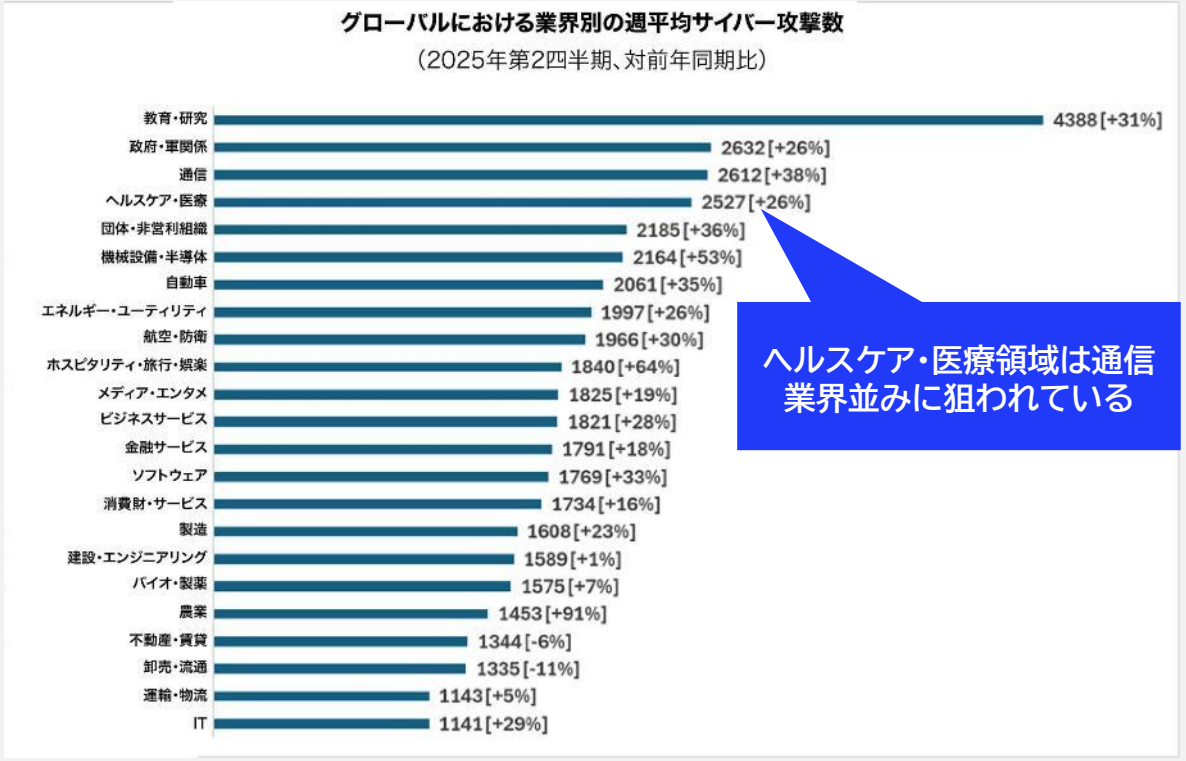
2025年2Q、全世界で約1,600件のランサムウェアインシデントが発生しています。

グローバルベースで業界別に観測された週平均のサイバー攻撃件数では、医療・ヘルスケア分野が突出して多いことが判明されているため、適切なセキュリティ対策を実施しなければなりません。特に患者情報を扱う立場として、その保護を徹底するとともに、社会的信頼を損なわない対策が必要です。

2025年2Q、全世界で約1,600件のランサムウェアインシデントが発生



グローバルにおける業界別の週平均サイバー攻撃数（2025年2Q、前年同期比）



教育・研究業界は資金不足による防御策の不備や、学生・職員の資格情報の豊富さが悪用に拍車をかけている

通信業界は攻撃数が最も増加しており、国家インフラとしての役割と機密度の高い顧客情報が狙われた可能性が示唆される

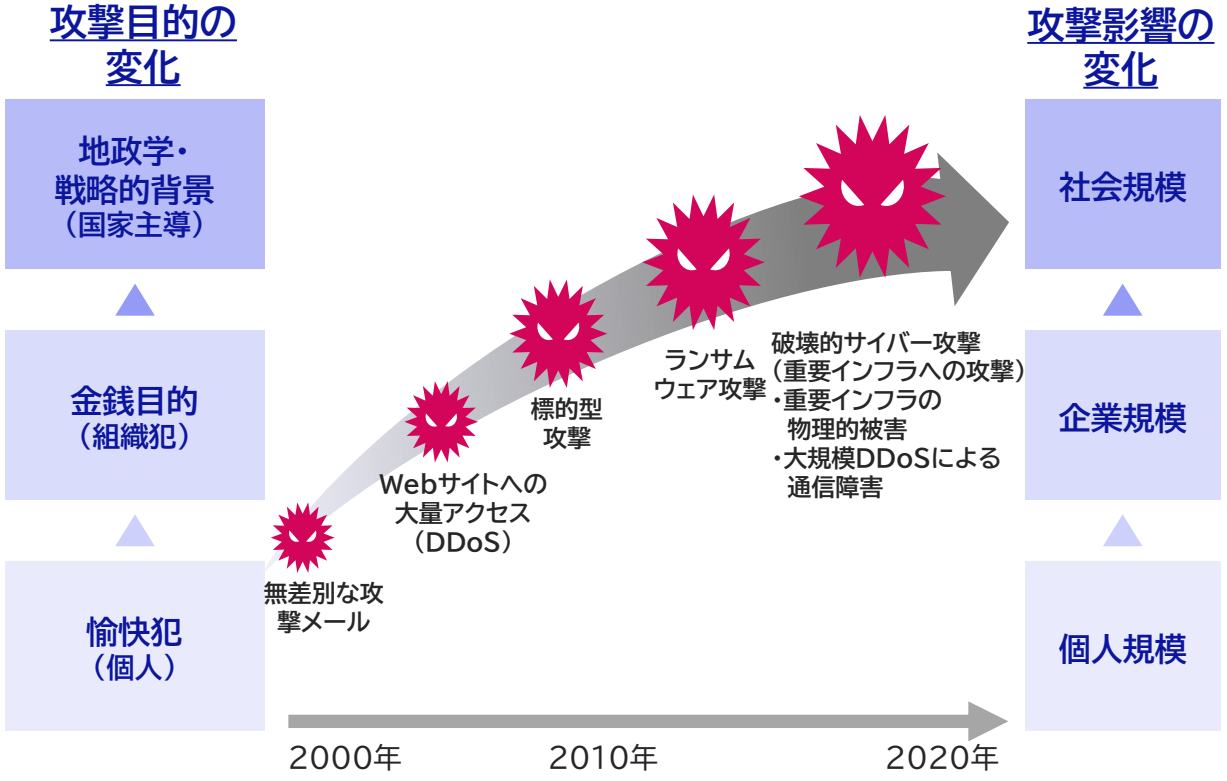
④技術革新への適応と高度化するサイバー攻撃対策

BluStellar

セキュリティ脅威が技術革新とともに急速に巧妙化している現状において、セキュリティ対策も同様に不断の進化が必要です。効果的な防御を維持するためには、脅威の最新動向を注視し、既存の対策を継続的に見直すプロセスが不可欠です。

サイバー攻撃の変遷

サイバー犯罪の組織化による攻撃の巧妙化に加え
国家による関与が疑われる攻撃も増加



サイバーセキュリティ対策の変遷

攻撃の高度化、攻撃から守る対象（情報システム・人々の働き方など）の変化に沿ってセキュリティ対策も日々変化

セキュリティの考え方

境界型防御 → ゼロトラスト

セキュリティ対策

EPP＜従来型＞（シグネチャ） → EPP＜次世代型＞（振る舞い・サンドボックス・機械学習） → EDR

FW → 次世代型FW・UTM → NDR

EDR / NDR → XDR

ID/PW認証

ICカード・証明書認証

生体認証

多要素認証

新たな領域に対してのセキュリティ対策（例：クラウド）

CASB

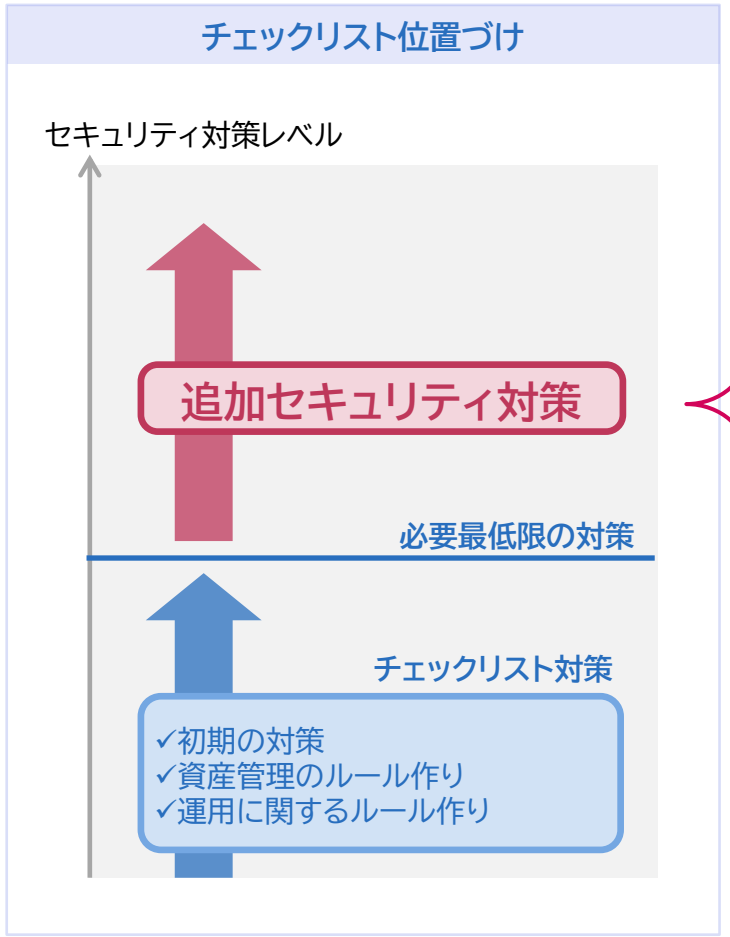
CSPM・SSPM

※ サイバーセキュリティタスクフォース（第35回）（総務省 2022/1/14） https://www.soumu.go.jp/main_content/000788349.pdf を参考にNECにて作成

課題３　セキュリティ対策予算が限られている

BluStellar

限られたセキュリティ対策予算内で課題1，2の解決を実施するための、打ち手の優先度と導入スケジュールの検討が重要です。



チェックリスト外の追加セキュリティ対策例

ネットワーク分離	感染端末の隔離
ログの統合管理	二次感染の防止
不正接続の防止	専門家の監視・分析

・
・
・

一気にすべてをやる予算も時間もない。
どれをいつやれば良いのか。

厚労省のサイバーセキュリティ対策チェックリストは必要最低限の対策としての内容の記載であり、セキュリティ被害の病院経営への影響拡大を抑えるには他にも様々な対策が必要になります。

医療DX推進にともなうセキュリティ対策見直しの必要性（深堀り）

BluStellar

課題１	医療DX推進にともなう境界型防御の見直し →病院内外のICTインフラ全体を見渡した部門横断での対策が必要
課題２	医療情報システム被害の病院経営への影響拡大 →高度化する攻撃と医療DX推進による影響範囲拡大に対処する 継続的なセキュリティ見直しが必要
課題３	セキュリティ対策費用が限られている →経営観点でのシステム重要度を踏まえた対策の優先順位付けと 段階的な導入プランの策定が必要

対策は次章でご説明

3. NECが推奨する病院のセキュリティ対策

NECが推奨するセキュリティ対策の導入Step

BluStellar

前章でご説明しました医療DX推進に必要なセキュリティ対策強化に向けて、現状環境の把握とネットワーク構成見直しの上で、システムの優先度に応じたセキュリティ対策のロードマップのご検討をおすすめします。

・病院ネットワーク内の部門システム端末の把握
・情報資産への到達性の把握
・セキュリティリスク分析

Step1
現状環境の把握

Step2
ネットワーク構成見直し

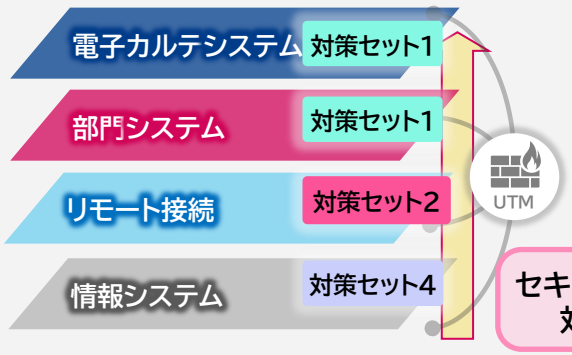
・NWの外部接続構成や内部構成の見直し

Step3
セキュリティ対策検討

		セキュリティ対策							
システム分類	端末種類	A	B	C	D	E	F	G	H
医療情報系	医療情報サーバ	×	×	×	×	○	×	○	○
	医療情報端末	×	×	○	○	○	×	○	○
	受付・会計端末	×	○	○	○	○	×	○	○
	医師BYOD	○	×	×	○	○	×	○	○
部門系	部門端末	×	×	○	○	○	×	○	○
	部門サーバー	×	×	×	×	○	×	○	○
情報系	情報端末	○	○	×	○	○	×	○	○
リモート系	中継サーバ	○	○	×	×	○	○	○	○
	メンテナンス	○	×	○	○	○	○	○	○

・サイバーセキュリティ対策・チェックリスト対応
・端末分類ごとに追加対策を検討

Step4
ロードマップ検討



セキュリティリスクに応じた対策を段階的に検討

・中長期での段階導入ロードマップを検討

Step1：現状環境の把握

BluStellar

システム重要度と病院の内部や外部とのシステム間の通信状況からリスクを分析

【お客様検討事項】

①各システムの重要度

実施事項：人命への影響や業務継続の観点から優先して保護・復旧すべきシステムを明確にする

目的　　：重要度に応じてセグメンテーションやアクセス制御のポリシー設計を実施する

②病院内システム間の通信状況

実施事項：各システム間の通信可否やシステム間の通信状況を把握する

目的　　：想定外の通信を洗い出し、不要・過剰な接続を排除し、ネットワークの構成見直しを行う

③各システムの外部通信状況

実施事項：インターネットやクラウドとの通信経路を可視化する

目的　　：外部との通信内容の管理を徹底し、不正アクセスと情報漏洩のリスクを特定する

Step1の検討事項

BluStellar

①各病院によって定めるシステムの重要度

お客様にて各システムの重要度を決めて頂く必要があります。

参考:厚労省での検討情報

基幹インフラ制度への医療分野の追加について（案）

医療機関における特定重要設備について（案）

○ **特定重要設備については、当該設備が停止した場合の社会的混乱の規模**や、**患者の生命に直結するか否か**等の観点から検討を進めており、**電子カルテ、手術部門、集中治療部門に関連する設備**から指定する方向で引き続き精査する。

特定重要設備の候補	概要
電子カルテに関連する設備	診療録を中心とした患者情報の記録・参照などに利用するもの。
手術部門に関連する設備	主として外科的処置が必要な患者に対して全身麻酔等を行いながら手術を実施するとき等に利用するもの。
集中治療部門に関連する設備	手術後の患者や全身状態が悪化した重症患者等に対して、診療密度が特に高い医療を提供するとき等に利用するもの。

令和7年11月25日
厚生労働省「基幹インフラ制度への医療機関の追加について」より抜粋
https://www.mhlw.go.jp/content/10801000/001599190.pdf

システム重要度の例（ランサムウェアなどの被害によるシステム停止が発生した場合の人命への影響度で順位付け）

重要度		システム
高 ↓ 低	参照環境を利用した最低限の病院業務継続に不可欠なもの	電子カルテ参照システム 電子カルテ・医事会計
	患者への看護対応や病状の画像情報など病院業務継続に不可欠なシステム	看護系・画像系
	外来などの診療再開に向け検査に必要なシステムや輸血関係のシステム	輸血・生理・検査など
	障害発生時に復旧まで他病院への転院などで対処可能なもの	手術・重症系など
	診療情報を含まず、運用等の代替で対処可能なもの	その他

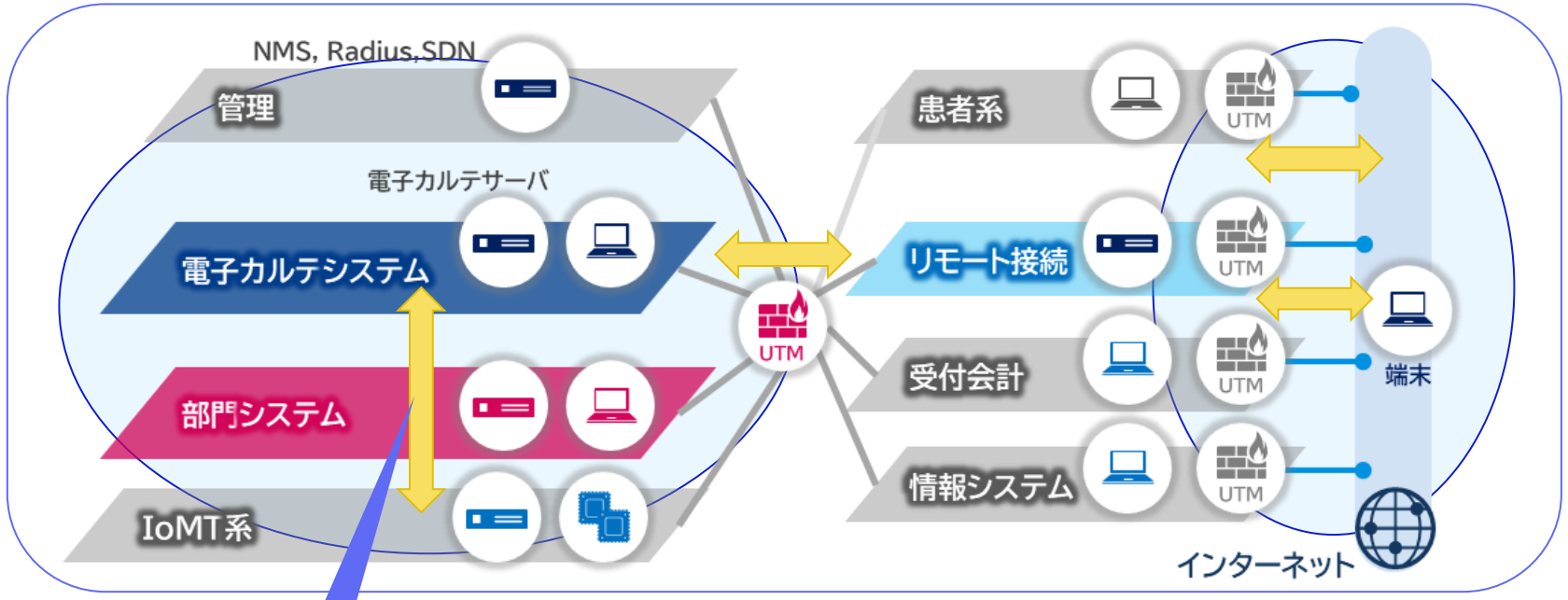
Step1の検討事項

BluStellar

②病院内システム間の通信状況

お客様側での基本設計思想と可視化結果の比較による現状把握を実施します。
特に「①各システムの重要度」で洗い出した重要システムを中心に、システム間通信可否と通信実態を把握します。

【電子カルテの場合】



電子カルテシステムと部門システムの間で
現状通信できるのか、通信が必要なのかを確認する

通信可否の把握(UNIVERGE Network Operation Engine)

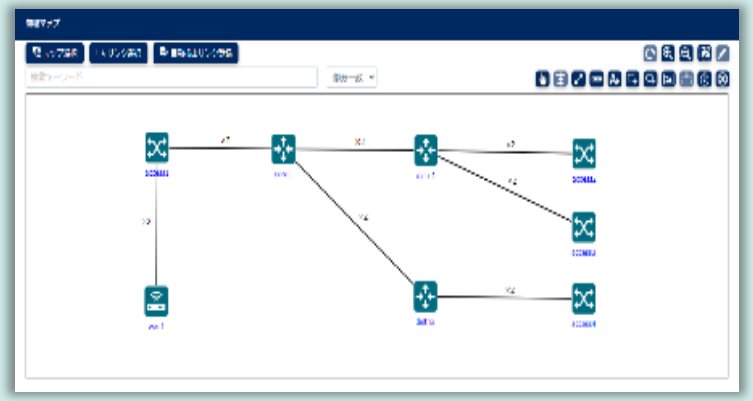
BluStellar

病院内のネットワーク接続状況を可視化し、各システム間の通信可否を把握

【NOE-STを使ったネットワーク可視化　事例】

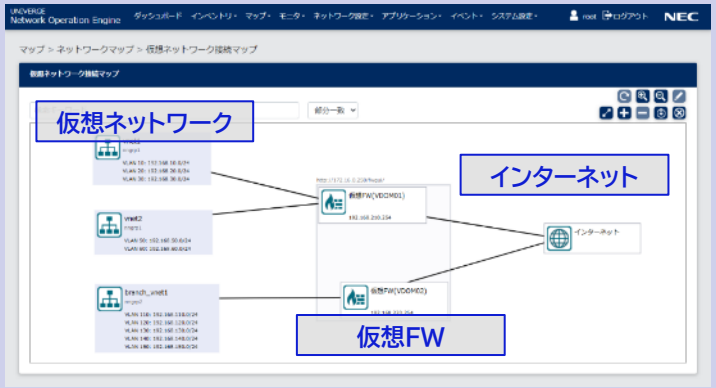
物理マップ

物理ネットワークの隣接関係をマップで確認



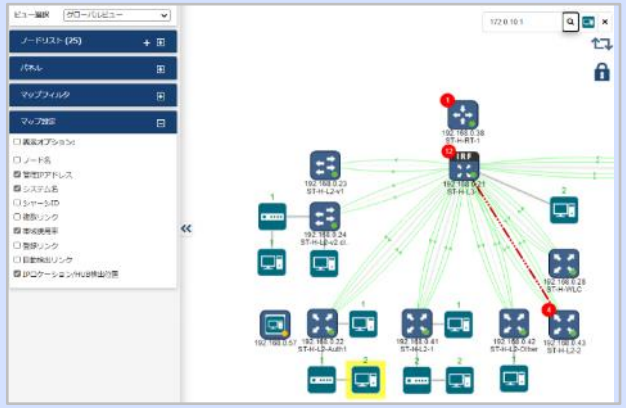
仮想マップ

仮想ネットワーク構成をシンプルなマップで確認



端末マップ

端末視点でのネットワークの関係をマップで確認



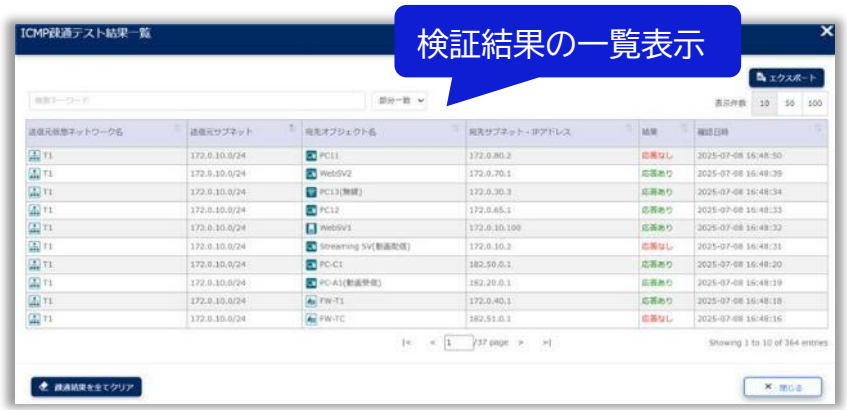
・物理ネットワーク・仮想ネットワークの接続構成をマップ表示で可視化（仮想ネットワークとFirewall/インターネットも確認可能）
・端末視点でのネットワークの接続状況を可視化

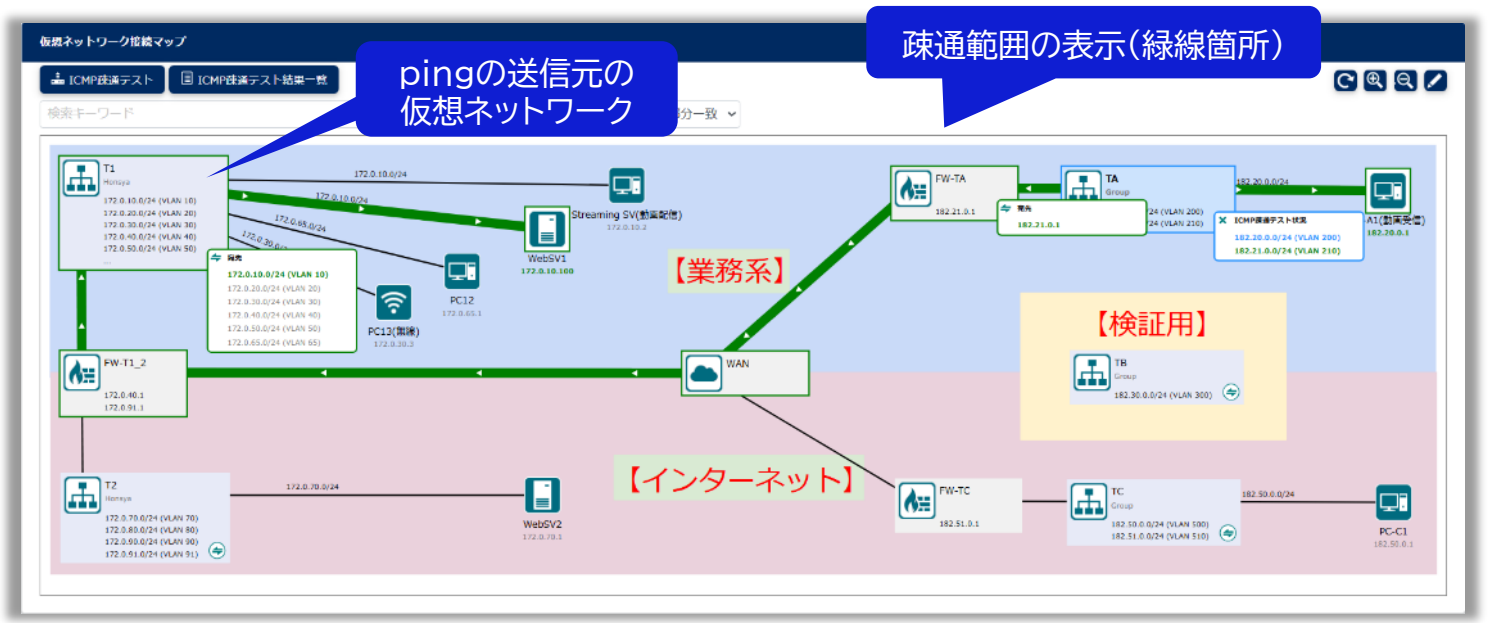
通信可否の把握(UNIVERGE Network Operation Engine)

BluStellar

疎通テストにより、病院内のネットワーク間の疎通、遮断関係を検証します。
ネットワーク設定やFirewallポリシー等の変更後の動作検証やネットワーク動作の監査に利用できます。

- **検証方法（以下の2通りが可能）**
  - ■ 全仮想ネットワーク間の疎通テスト
  - ■ 指定仮想ネットワークから、選択した指定ネットワーク/端末への疎通テスト
- **ICMP Echo(ping)によりテストを実施。仮想ネットワーク接続マップ上での表示やExcel出力も可能。**



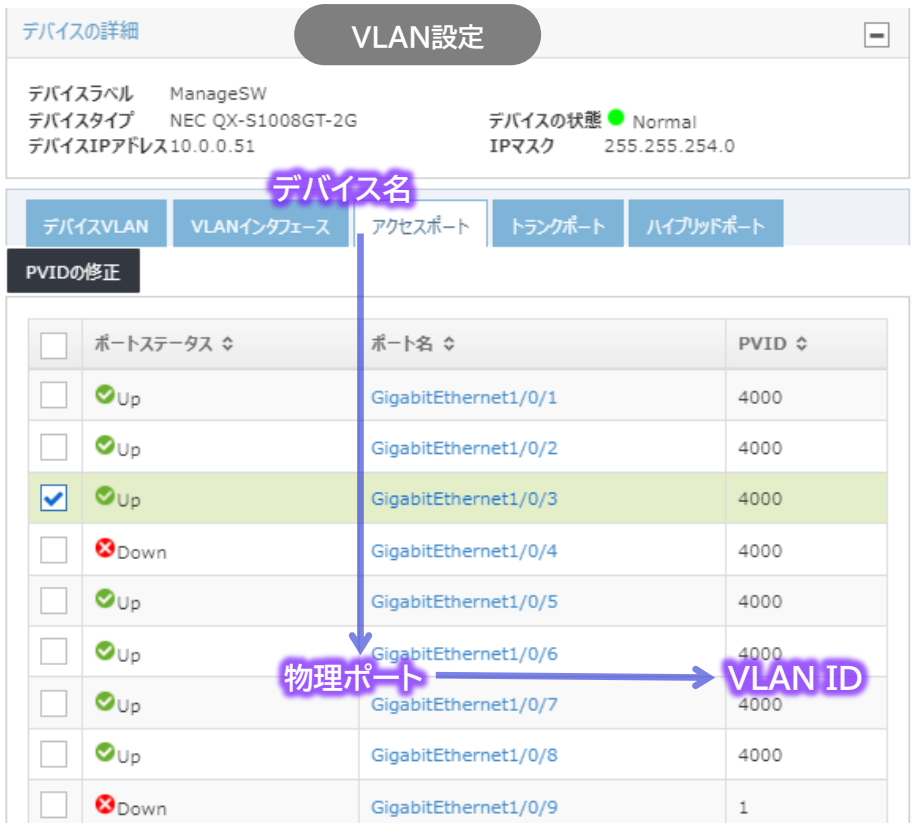


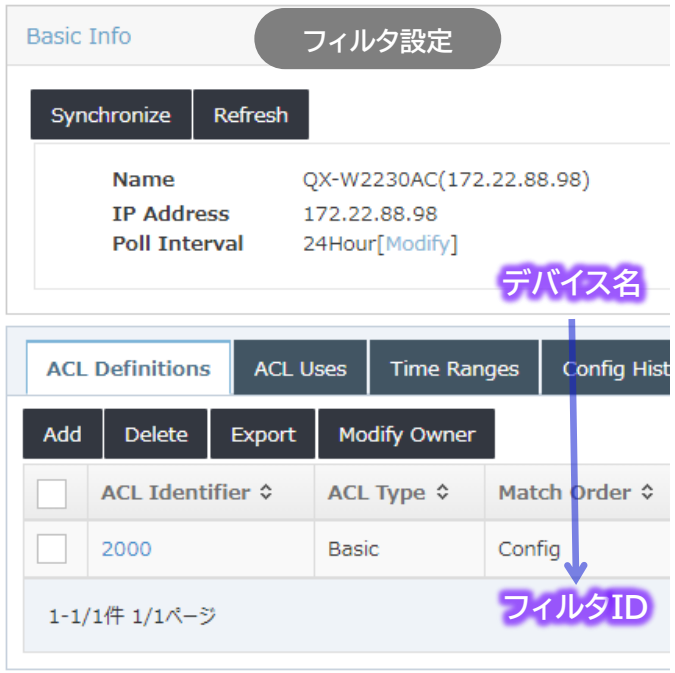
通信可否の把握(QX Management Center)

BluStellar

NOE-STより可視化の程度は劣りますが、NEC製のQXスイッチ・無線機器向け統合管理型ネットワーク監視装置「QX Management Center」でもVLAN・フィルタ設定が確認でき、ネットワーク接続状況確認に活用可能です。

【QX Management Center 画面イメージ】





通信実態の把握(WebSAM Network Flow Analyzer)

BluStellar

ネットワークを流れる アプリケーション通信 の「見える化」を実現

NFAの特長

1.ネットワークの通信状況を即座に把握・分析

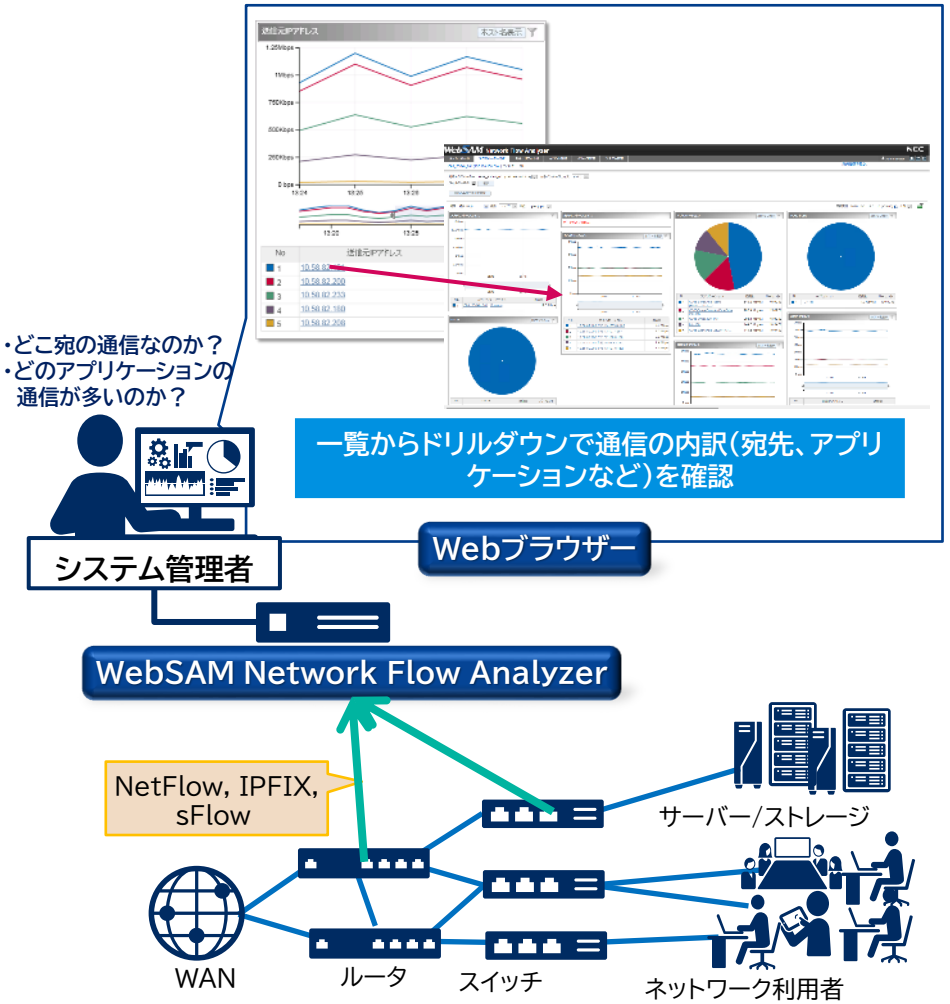
- 通信量の多い端末やアプリケーションをランキング表示し、ネットワークの負荷原因を即座に確認可能
- 表示されたアプリケーション名やIPアドレス(ホスト名)のクリック操作で容易にドリルダウン分析が可能
- アノマリー分析で普段と異なるフローデータの挙動を検知することで障害予兆を把握し未然にトラブルを防止可能

2.目的に合わせた情報表示で分析作業を効率化

- 分析対象を自由に設定できるダッシュボードで、素早い現状把握・分析をサポート
- ポート番号、IPプロトコルの情報に送信元／宛先のIPアドレス、ドメイン名を組み合わせて、固有の業務アプリケーションやサービスの通信を識別表示
- Microsoft365、BOX、Zoomなどのクラウドサービス通信負荷を可視化し、通信負荷の高いクラウドサービスのオフロード検討や新規クラウドサービス採用時の負荷調査に利用可能

3.様々なネットワーク環境を統合管理

- NetFlow, IPFIX, sFlow をサポートし、様々な環境に適用可能
- WebSAM NetvisorPro Vと連携し、ネットワークの状態をきめ細かに統合管理



通信実態の把握（PaloAltoセキュリティリスク診断）

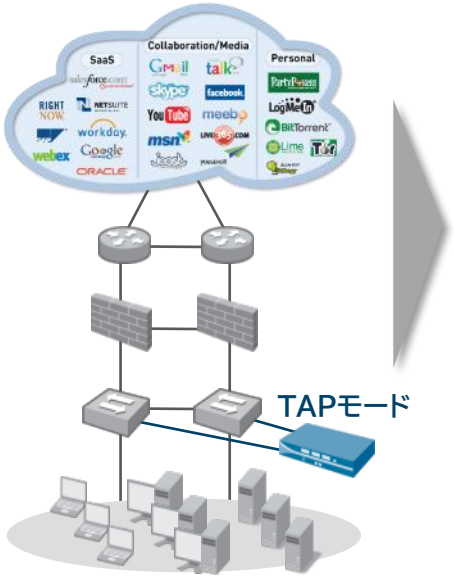
BluStellar

Palo Alto 次世代ファイアウォール によるセキュリティリスク診断（SLR）

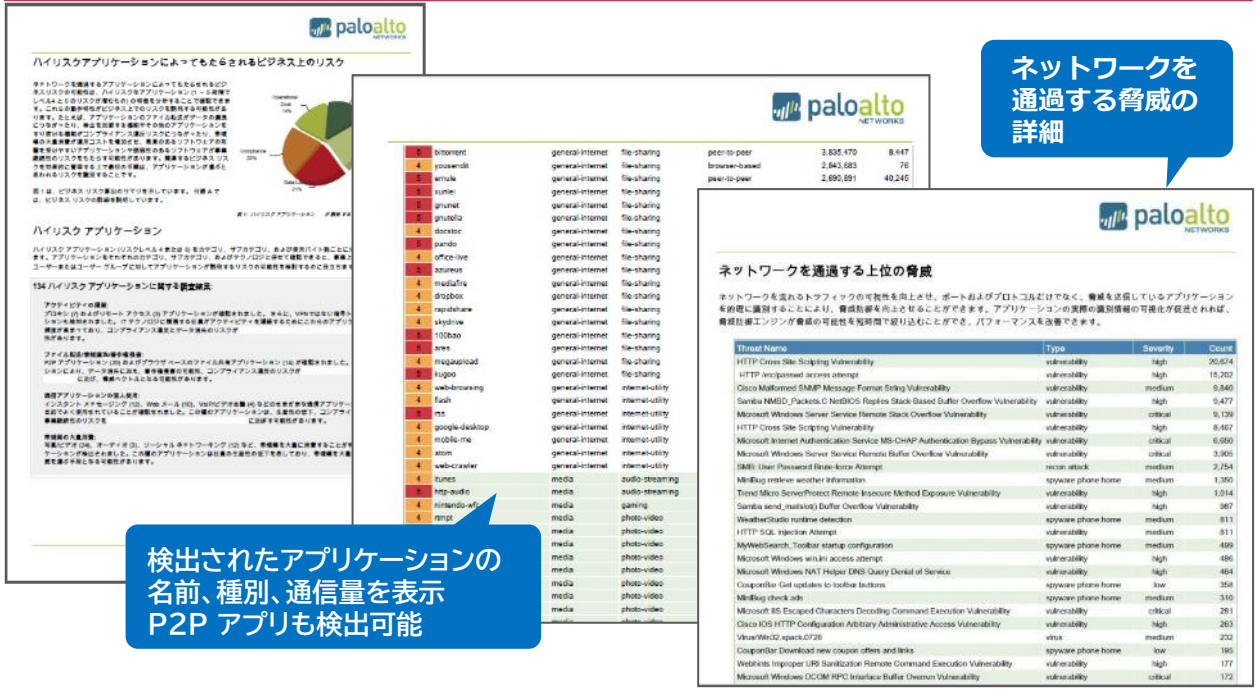
サイバー攻撃対策に定評のある「Palo Alto 次世代ファイアウォール」は、既存のネットワーク構成をほとんど変更せずにアドオンでき、通信にも影響を与えずに、手軽に セキュリティリスク診断（SLR：Security Lifecycle Review）を行うことができます。
ただし、Step1の病院の内部での各システム間の通信状況については、Palo Altoで取得したNetflowの生ログやパケットを解析する必要があります。

■診断手順

1. スイッチにミラーポートを設定
(ミラーポート設定及び設置場所確保は お客様にてご準備をお願いいたします)
2. Palo AltoをTAPモードで接続いただき、１週間ほどログを取得
(Palo Alto を無償で貸出いたします)
3. 取得したログを基に、日本語のレポート
(標的型攻撃の有無、社内のマルウェア 感染端末一覧、重症度等) を作成



■アウトプットイメージ



Step1の検討事項

BluStellar

③各システムの外部通信状況

・病院の外部との通信状況

- お客様にて各システムと外部との通信状況を把握を行います
  例えば、厚生労働省の「医療機関におけるサイバーセキュリティ確保事業」のヒアリングシートを参照し、
  外部通信状況を整理する
- 病院ネットワークのインターネット入口でFortiGateを利用している場合、FortiAnalyzerで各FortiGateを統合管理することで病院の外部との通信を把握可能

「医療機関におけるサイバーセキュリティ確保事業」のヒアリングシート（サンプル）

2. 回線情報

	回線情報				脆弱性診断									
申告回線No.	回線サービス名	回線サービスのID（CAF番号等）	回線終端装置設置場所	用途、システム名	脆弱性診断希望	通信形態	固定IP/動的IP	グローバルIPアドレス	プレフィックス長	入力チェック（記入不要）	グローバルIPアドレス設定機器	申告機器No.（ルータ/ファイアウォール/UTM）	機器種別	メーカー
例	フレッツ光ネクスト ギガファミリー・スマートタイプ	CAF1111111111	本部棟 3F サーバー室 1番ラック 3U	電子カルテ	診断希望あり	インターネット	固定IP	121.119.249.222	/32	記載に間違いございません。	機器A	例A	ルータ	シスコシステムズ
01												01A		
02												02A		
03												03A		
04												04A		
05												05A		
06												06A		
07												07A		
08												08A		
09												09A		
10												10A		
11												11A		

出典：医療機関におけるサイバーセキュリティ確保事業｜厚生労働省

参考：ログ管理、分析、レポートアプライアンスFortiAnalyzer

BluStellar

病院ネットワークのインターネット入口でFortiGateを利用している場合、FortiAnalyzerで各FortiGateを統合管理することで病院の外部との通信を把握可能

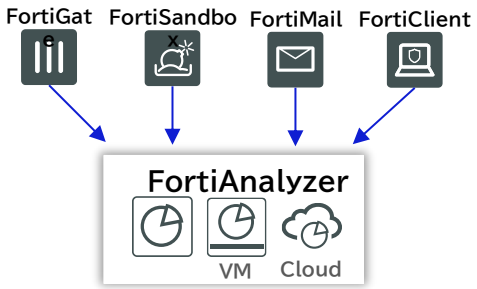
FortiAnalyzerの活用例

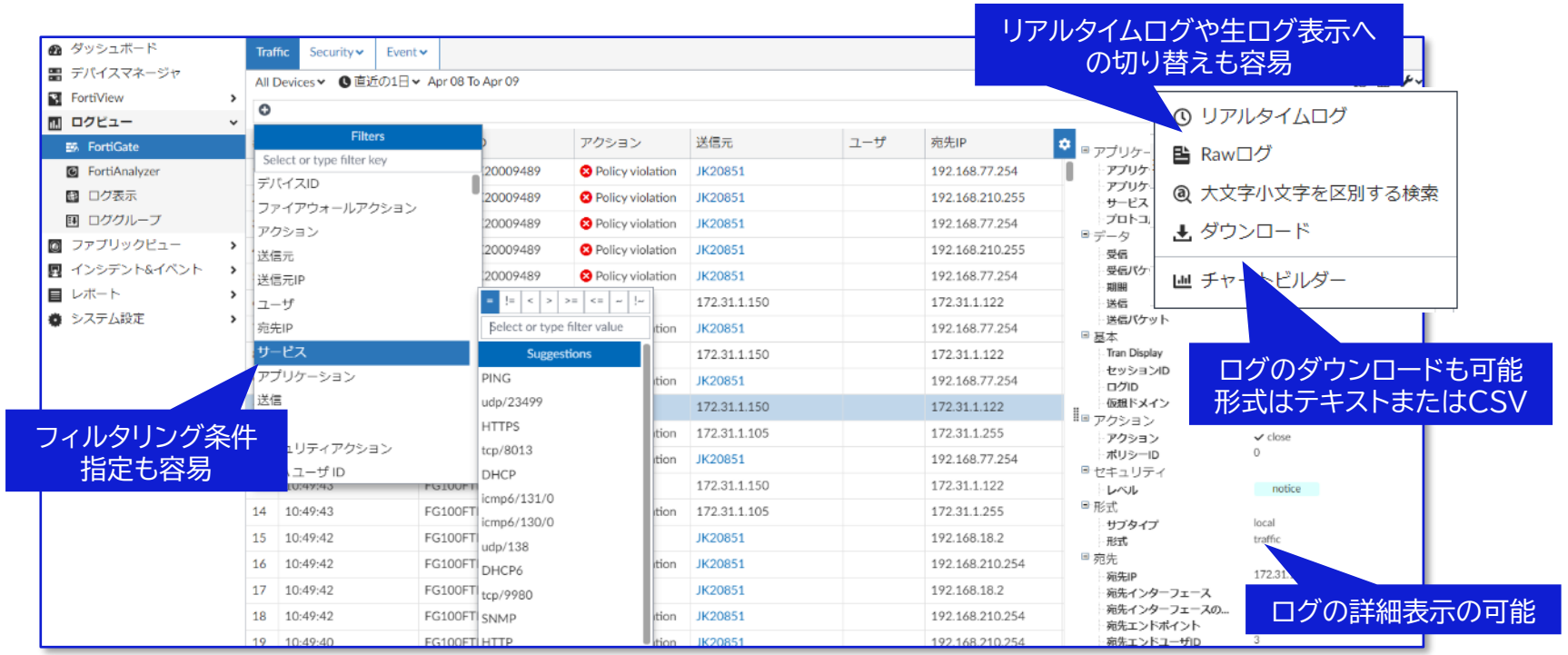
セキュリティ脅威やネットワーク状況などをリアルタイムと履歴データで包括的に可視化

- 各機器から収集したログ情報を分析しカテゴリ毎にまとめ、視覚的に分かりやすいウィジェット形式で一覧表示
- 「脅威」、「トラフィック」、「シャドウIT」、「アプリケーション&Webサイト」、「VPN」、「システム」にカテゴリ化
- 各項目はドリルダウン型の表示で、クリックするとより詳細な情報確認が可能

■ **FortiAnalyzerの幅広い集中ロギング**

・Fortinet 各製品からのログ転送が可能





トラフィックログの画面操作イメージ

Step2：ネットワーク構成見直し

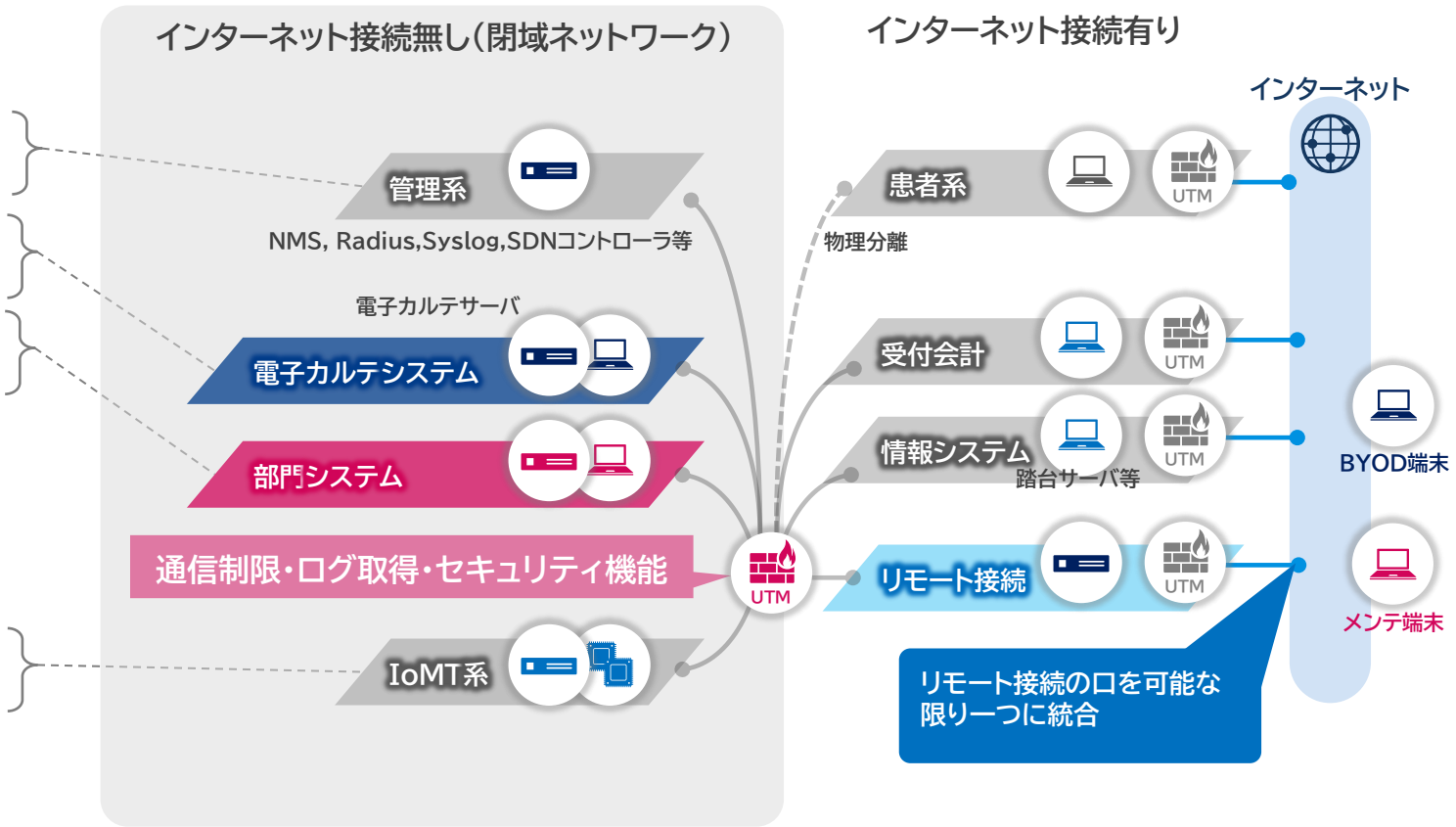
BluStellar

Step1で実施したリスク判定からネットワーク構成見直しを実施。アタックサーフェスを減らすため、リモート接続の口を可能な限り一つに統合することを推奨します。

内部ネットワークは重要システムと他システムの接続を極力内部ファイアウォールで制限することで、不正通信の遮断、ログ取得、セキュリティ対策が可能になります。

現行環境を整理した例

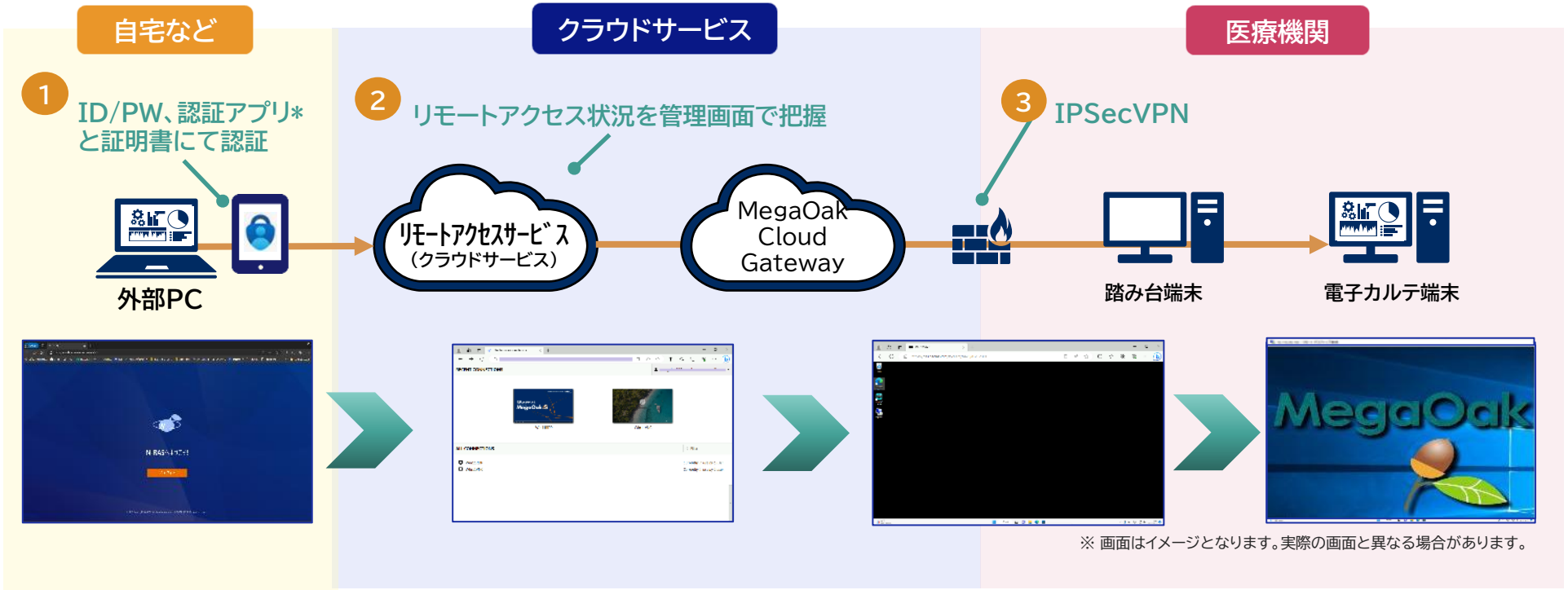
システム区分	システム	端末種類	インターネット
管理系	管理系	管理サーバ	接続 無
		管理者用端末	接続 無
医療情報システム系	電子カルテ系	電子カルテサーバ	接続 無
		HIS端末	接続 無
	部門系	部門サーバー	接続 無
		部門端末	接続 無
	受付・会計系	受付・会計システム端末	接続 有
	リモート接続系	中継サーバ	接続 有
		医師BYOD端末	接続 有
		メンテナンス用端末	接続 有
	IoMT系	医療機器管理サーバ	接続 無
		医療機器	接続 無
インターネット接続系	情報系	情報端末	接続 有
	患者系	患者持込み端末	接続 有



参考:クラウドセキュア接続サービス(MegaOak Cloud Gateway)

BluStellar

リモート接続の見直し際に、クラウドセキュア接続サービス(MegaOak Cloud Gateway)+
リモートアクセスサービスを活用し、インターネットの出入口をまとめて安心安全なリモート接続環境の構築を推奨



1. ID/PW、認証アプリ(*Microsoft Authenticator)の認証 と 証明書による端末制御を行う
2. リモートアクセス状況を可視化、利用アカウント単位で接続先を設定管理
3. ガイドラインに準拠した通信(IPSec-VPN／高セキュリティ型暗号スイートを採用)、ファイル送受信の禁止

Step3：セキュリティ対策検討

BluStellar

セキュリティリスクと重要度から必要となるセキュリティ対策※を端末単位で検討
複数の個別対策を組合わせて、対策案を整理します。

■セキュリティ対策の検討例

				チェックリストに基づいたセキュリティ対策				ガイドラインに基づいた優先度の高いセキュリティ対策				
システム区分	システム	端末種類	インターネット	マルウェア感染防止	不正接続防止	ログ統合管理	多要素認証	SOC監視・分析	感染端末の隔離	マルウェア感染防止・分析	内部ネットワーク監視	バックアップ強化
管理系	管理系	管理サーバ	接続 無	○	対象外	○	対象外	○	-	-	○	○
		管理者用端末（PC・スマホ）	接続 無	○	○	○	○	○	-	-	○	–
医療情報システム系	電子カルテ系	電子カルテサーバ	接続 無	○	対象外	○	対象外	○	-	-	○	○
		HIS端末（PC・スマホ）	接続 無	○	○	○	○	○	-	-	○	–
	部門系	部門サーバー	接続 無	○	対象外	○	対象外	○	-	-	○	○
		部門端末（PC・スマホ）	接続 無	○	○	○	○	○	-	-	○	–
	受付・会計系	受付・会計システム端末（PC・スマホ）	接続 有	○	○	○	○	○	-	○	○	–
	リモート接続系	中継サーバ	接続 有	○	対象外	○	対象外	○	○	○	○	–
		医師BYOD端末（PC・スマホ）	接続 有	-	○	○	対象外	○	○	-	○	対象外
		メンテナンス用端末（PC・スマホ）	接続 有	-	○	○	○	○	○	-	○	対象外
	IoMT系	医療機器管理サーバ	接続 無	○	対象外	○	対象外	○	-	-	○	○
		医療機器	接続 無	-	-	○	対象外	○	-	-	○	対象外
インターネット接続系	情報系	情報端末（PC・スマホ）	接続 有	○	○	○	-	○	○	○	○	対象外
	患者系	患者持込み端末	接続 有	対象外	対象外	○	対象外	○	-	対象外	○	対象外

凡例　○：対策優先度高　ー：対策優先度低
対象外：対策不要

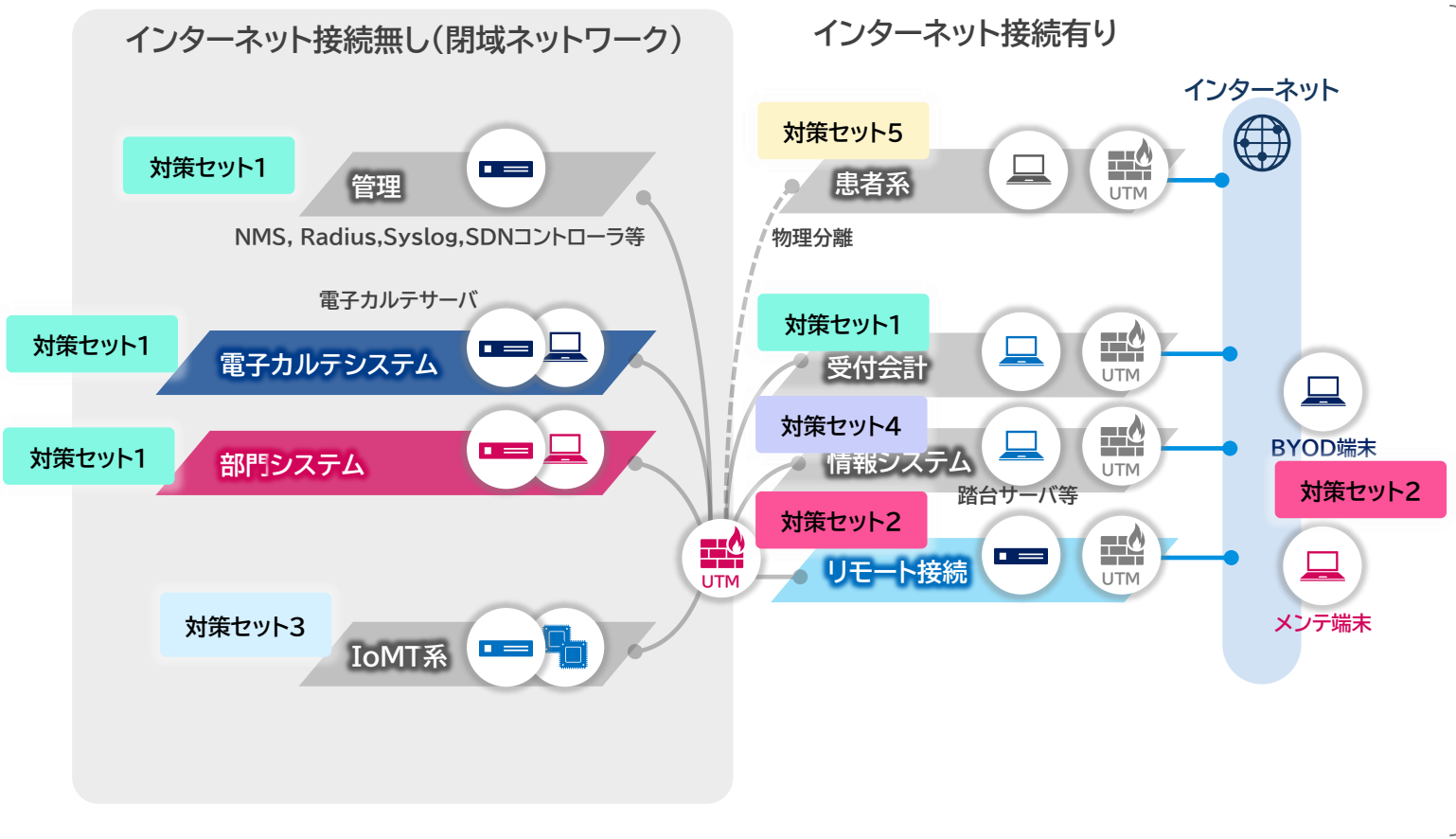
対策セット1　対策セット2　対策セット3　対策セット4　対策セット5

※各セキュリティ対策の詳細はAppendix参照

Step4：ロードマップ検討

BluStellar

Step2で実施した分離されたネットワーク単位でセキュリティ対策の導入ロードマップを検討
重要度が高い領域から順次対策を計画します。（NECが伴走型で検討ご支援も可能）



セキュリティコンサルティングサービス

✓ セキュリティ対策の優先度の検討支援

＋

ペネトレーションテスト

脆弱性診断

サイバーセキュリティ教育

ネットワーク可視化ツールの本格導入

✓ 定着化へ向けた支援

対策のまとめ

BluStellar

背景

- 医療DX推進が病院の業務効率化、医療の質向上に不可欠
- 医療従事者の不足や病院経営環境の悪化

課題

- 境界防御の限界
- 攻撃高度化による経営リスクの増大
- 予算の制約

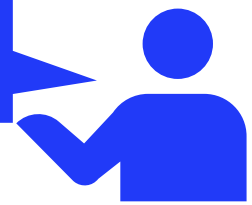
対応方針

- ✓ 現行環境の可視化 リスク分析

- ✓ NW構成見直し（外部接続とシステム間通信制限）

- ✓ セキュリティ対策の段階導入とコスト適正化

初手はネットワーク対策（可視化・構成見直し）からの実施が効率的です



セキュリティリスク分析とネットワーク対策（可視化・構成見直し）をしっかりとリンクして検討する事が適正なセキュリティ投資に繋がる

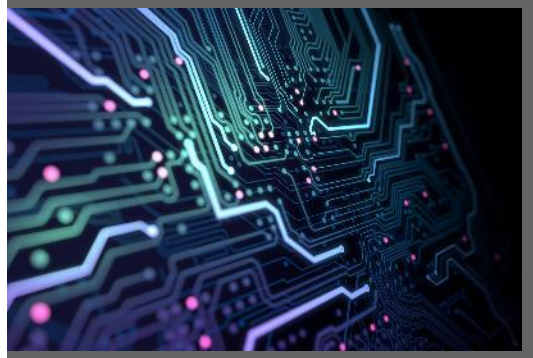
BluStellar

4. セキュリティ対策をより十全に行うためのNW運用負担の抑制

NECのSDNソリューション

BluStellar

UNIVERGE Network Operation Engine（NOE-ST）



ネットワーク可視化

- ネットワークの物理構成、分離後の論理構成をWeb GUI表示
- Web GUI上で、端末のロケーション情報を確認可能（Excel出力）

ネットワーク分離

- 装置毎の設定→Web GUIからの一括設定が可能
- 設定漏れ・装置間の設定矛盾を防ぐ仕組みを提供

ネットワーク管理

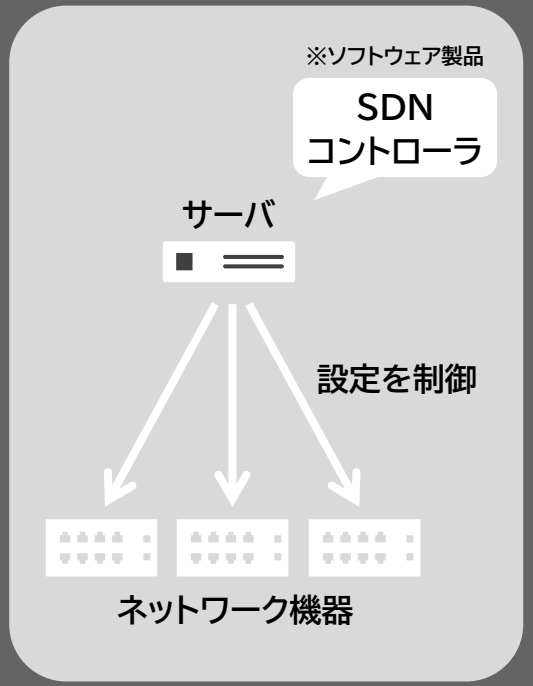
- 最新のネットワーク設定状況を一覧取得（Excel出力）
- セキュリティ機器と連携し、インシデント発生時の初動対応を自動化

マルチサイト管理

- 最大50拠点まで管理可能

安定稼働

- ネットワーク全体の稼働状況を確認可能
- ネットワーク機器の設定を制御するため、SDNコントローラ障害による通信への影響無し



ネットワーク管理(インシデント対応)

BluStellar

業務上止めて良い機器と止めてはいけない機器を区別し、止めて良い機器についてウイルス感染などのインシデント発生時に自動で隔離し初動対応を迅速化

医療情報システム安全ガイドライン 6.0版 -18章 遵守事項①システム運用編[抜粋]

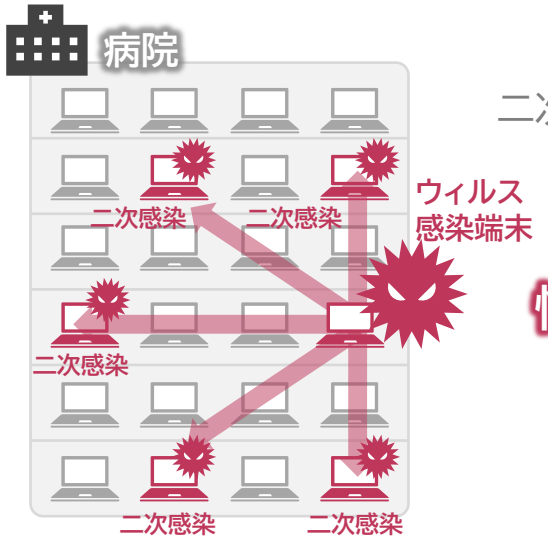
医療情報システムに対する不正ソフトウェア混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。
他の情報機器への混入拡大の防止や**情報漏洩の抑止のための当該混入機器の隔離**

医療情報システム安全ガイドライン 6.0版 -12章 サイバーセキュリティ遵守事項③企画運用編[抜粋]

サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。

従来の運用

初動対応が遅れると、、、

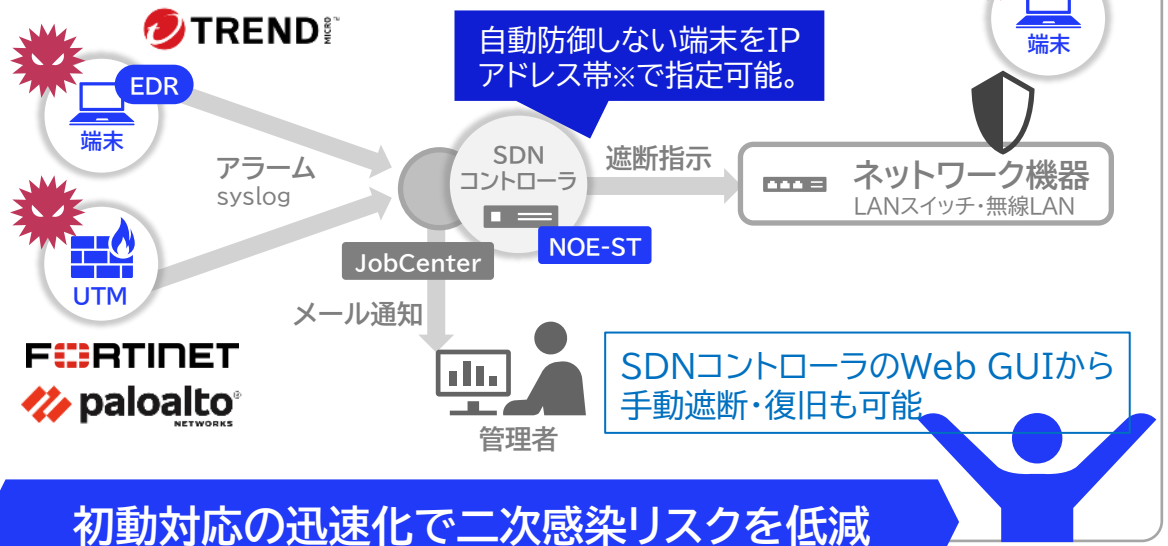


二次感染による感染拡大リスク

情報漏洩・業務停止

導入後

EDRやファイアウォールで
ウィルス感染を検知



初動対応の迅速化で二次感染リスクを低減

※自動防御しない端末のIPアドレス帯を11個以上設定する場合はサポート対象外

アノマリー分析(WebSAM Network Flow Analyzer)

BluStellar

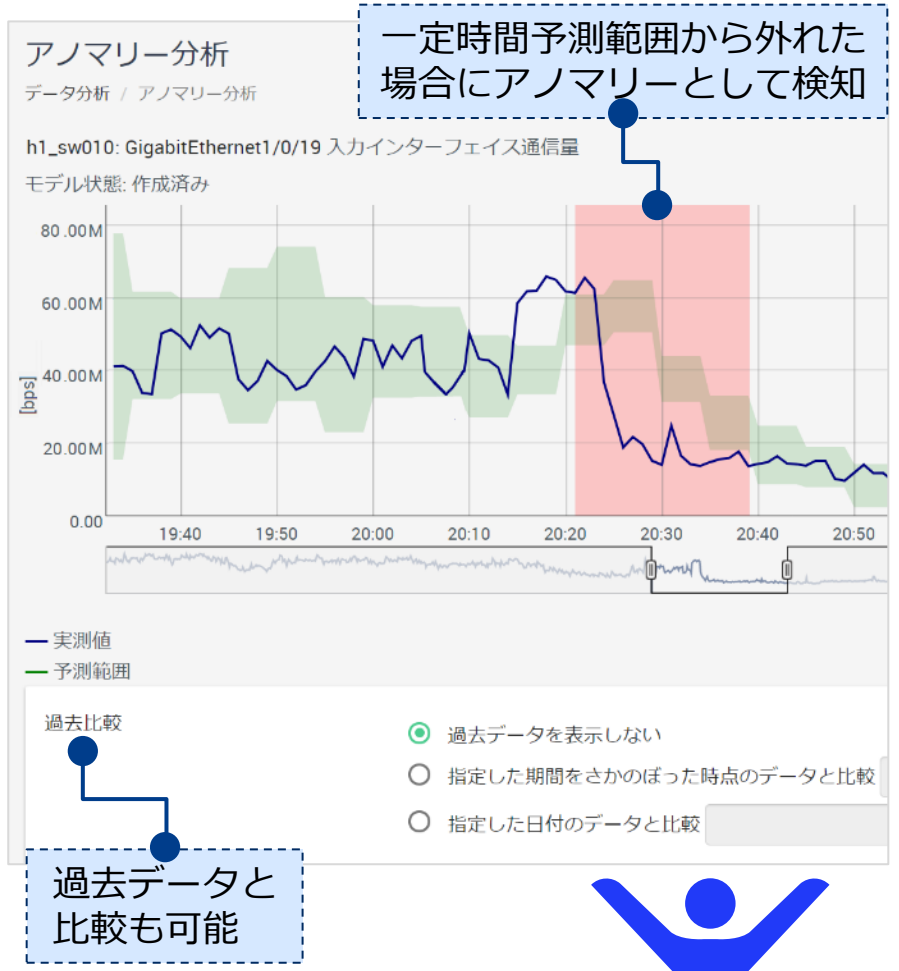
通常時の性能値の時系列データから予測モデルを作成し、普段と異なる振る舞い(アノマリー)をリアルタイムに検知可能。

通常時とは異なる振る舞いをリアルタイムに検知

- 蓄積した過去のデータから通常時のトラフィック状態を予測し、外れた場合にアノマリーとして通知することで、**障害予兆などを早期に検出可能**です。
- 通常時の振る舞いを基にした動的なしきい値監視により従来発生していた**誤検知や検知漏れを軽減することが可能**です。

フロー単位での分析も可能

- 特定の通信に絞って分析することができ、仮想環境などで**システム単位での分析が可能**です。
- 定期的に発生する通信に絞って分析を行うことで、タイミングや通信量から通常時と異なる挙動をしていることを検知し、**サイレント障害等を検知可能**です。



ネットワークの異常を検知することが可能

無線LANのトラブルシュート（QX Management Center）

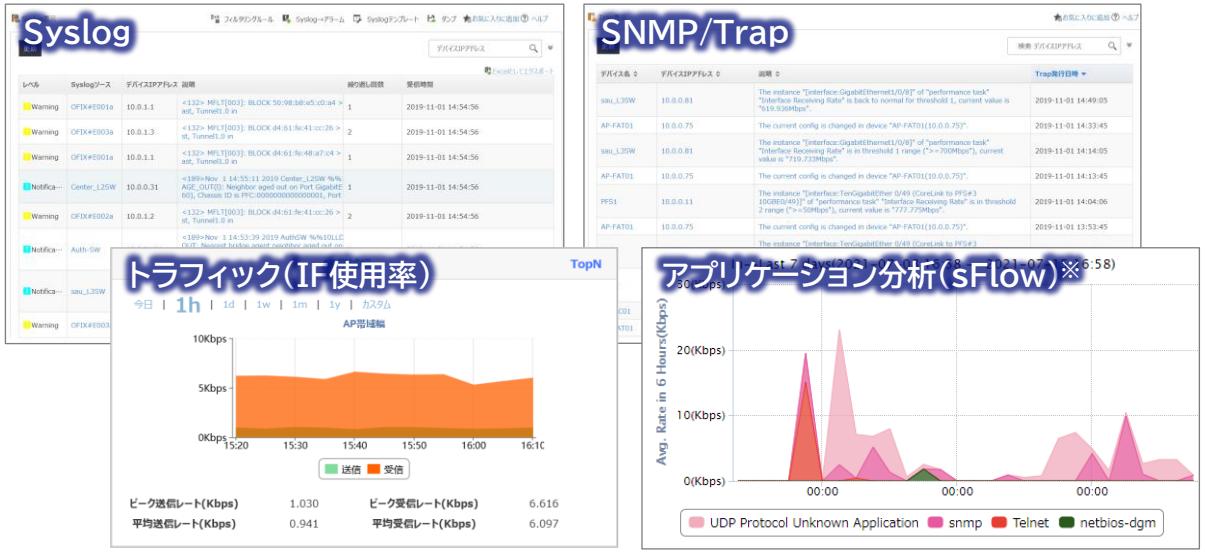
BluStellar

有線＆無線のネットワーク状況を監視し、管理画面で分かりやすく表示し、迅速な障害発生原因の特定を支援します。
過去に遡ってのネットワーク状態もレポートで確認可能であり、障害分析・改善を通じた日々の安定稼働をサポートします。

◎可視化＋トラブルシューティングに対応

電波シュミレーションがフロアレイアウト図上で実施可能→最適なAP配置を検討できます。
無線クライアントのトラブルシューティング機能を実装

◎ログ管理・ネットワーク統計情報を確認可能



※別途、NTAオプションライセンスが必要

一定期間でのログの蓄積や、有線/無線の通信（送信/受信）の利用帯域の推移を可視化
無線クライアントとの電波状況、AP負荷状況を可視化し、無線LANの接続不具合の分析を支援

【参考】NOE-ST/QMC機能比較

BluStellar

QMC：標準的なNMS機能を搭載，無線LANコントローラと連携し電波状態の可視化，無線LANのトラブルシュート機能を提供
NOE-ST：安全な設定変更（設定矛盾の回避），論理構成の可視化により、安全な運用を実現

運用項目	運用作業	QMC Advance	NOE-ST
①設定変更	a.ネットワークを設定変更（仮想NW/VLAN/フィルタ等）	△VLAN/フィルタ	◎VRF/VLAN/フィルタ
	b.一括で複数台のエッジSWを設定変更（VLAN/フィルタ設定変更等）	×未対応	◎一括設定に対応
②構成管理	a.全体ネットワーク構成の一元把握（物理/論理トポロジ/機器情報の把握）	△物理/VLAN	◎物理/VRF/VLAN
	b.ネットワーク設定情報の一元把握（仮想NW/VLAN/フィルタ等）	△VLAN	◎VRF/VLAN/フィルタ
	c.ネットワーク接続端末の可視化（接続箇所/一覧表示/検索機能）	×未対応	◎対応
	d.無線LAN管理（ヒートマップ/クライアント管理/トラブルシュート）	◎対応	×未対応
③障害管理	a.障害を迅速に通報（障害のメール/パトランプ通報等）	◎対応	○メール通報対応
	b.障害箇所の特定（マップ上での障害箇所表示）	◎対応	◎対応
	c.障害時の切り分け（ログ管理、トラフィックの可視化）	◎対応	△閲覧時点の情報のみ
	d.障害復旧の迅速化（ゼロタッチでの保守交換）	×未対応	◎対応
④性能管理	a.ネットワーク機器の性能把握（トラフィック/CPU等）	◎対応	△閲覧時点の情報のみ
⑤運用管理	a.コンフィグファイルの効率的バックアップ（コンフィグ収集/世代管理）	◎対応	△最新情報のみ
	b.ファームウェアの効率的更新（一括での各スイッチのVersion up）	◎対応	△L2スイッチのみ
⑥その他	a.日本語対応	◎対応	◎対応

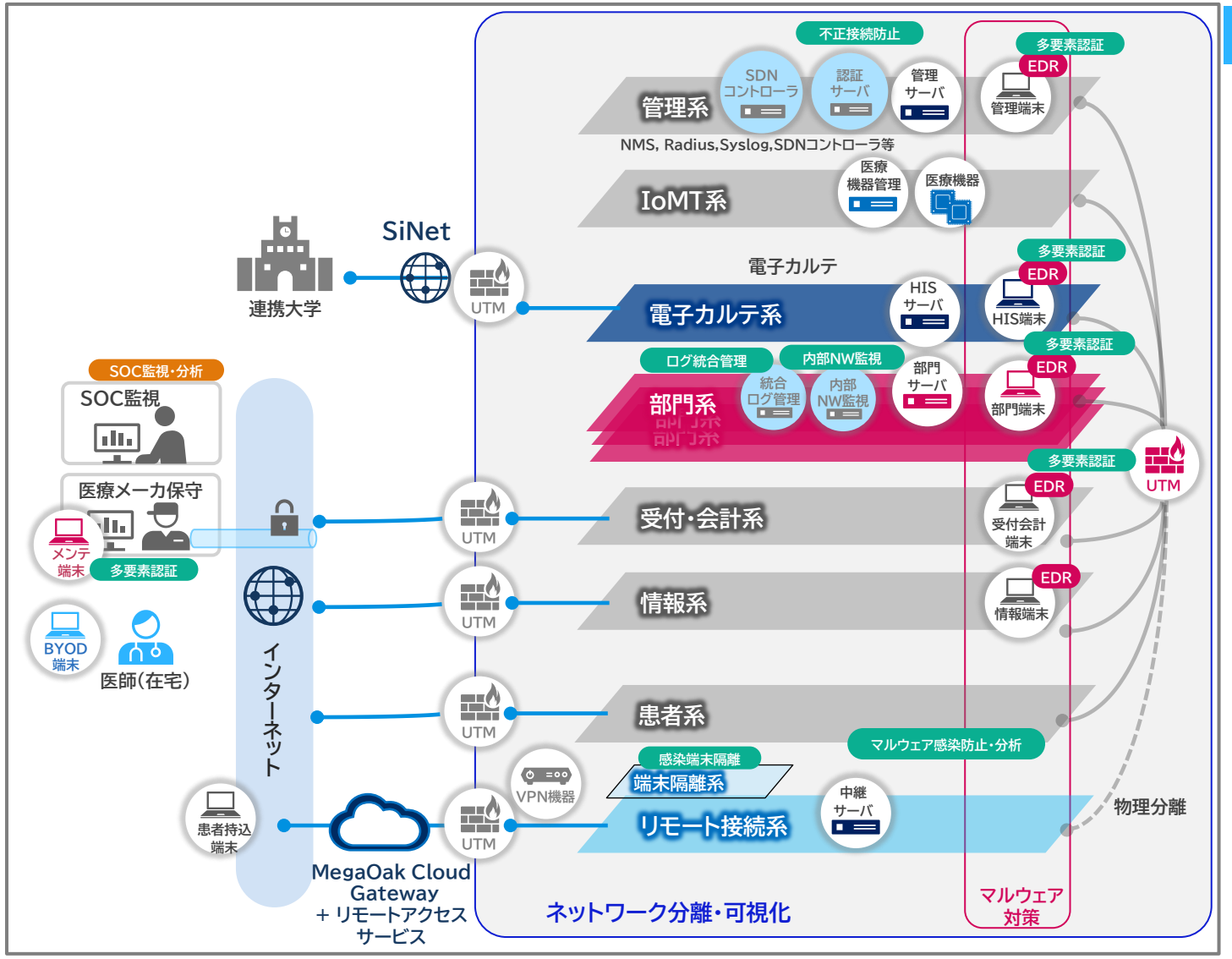
Appendix

医療ネットワーク＆セキュリティモデル

BluStellar

セキュリティを損なわず電子カルテシステムの信頼性、職員の働き方改革、医療DXを推進するモデル例

セキュリティ対策
ネットワーク分離・可視化
クラウドセキュア接続サービス（MegaOak Cloud Gateway）＋リモートアクセスサービス
マルウェア感染防止・分析（EPP）（FW）（IPS）
多要素認証
不正接続防止（認証サーバ）
ログ統合管理
SOC監視・分析
感染端末の隔離（EDR）
内部ネットワーク監視
バックアップ強化



ポイント

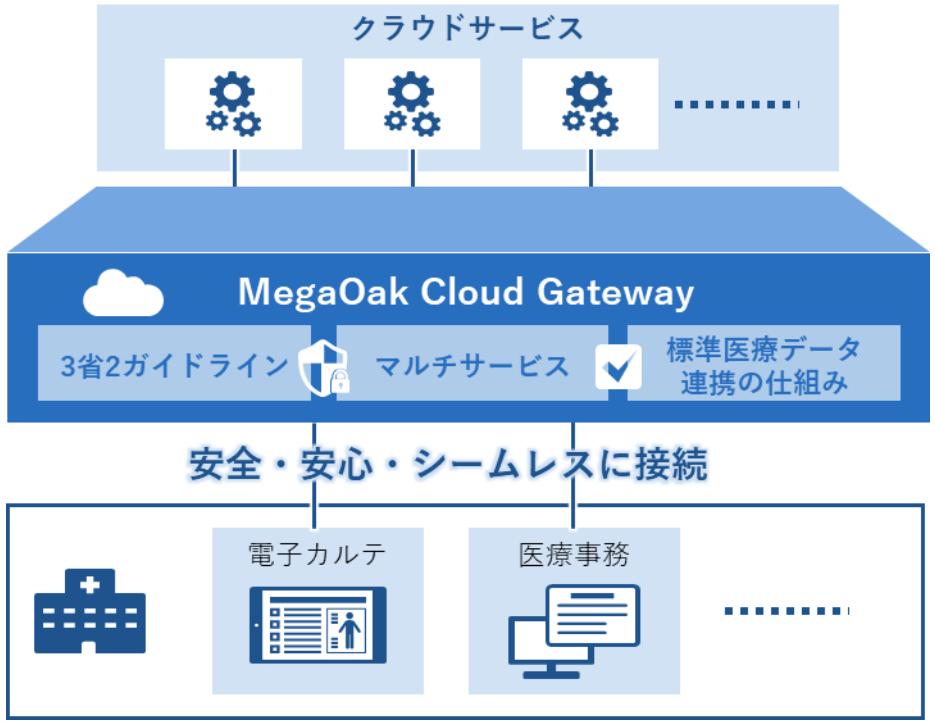
①セキュリティ対策のため、外部接続を一元管理するゲートウェイを設置する
②セキュリティ被害時の事業影響度が最も高いサーバ・端末から優先的に対策を実施する
③インシデント発生時における病院経営への影響を最小化すべく、ネットワーク分離し、必要十分な通信制御をする
④医療DXの推進状況と世の中の技術動向を踏まえて継続的にセキュリティ見直しを行う

クラウドセキュア接続サービス「MegaOak Cloud Gateway」

BluStellar

電子カルテシステムとクラウド環境にある医療現場を支援するサービスを安全・安心かつシームレスに接続
各種ガイドラインに準拠したクラウド環境と、接続における認証などの高度なセキュリティを提供

サービス提供イメージ



お客様の課題

・様々なサービスを利用するために必要な接続環境やセキュリティの確保
・上記環境を構築するためのコストや運用の負荷

期待効果

・サービスごとの接続環境やセキュリティ確保が不要
・上記により、運用負荷やコストを削減

NECの特徴

・各種ガイドラインへの対応、HIS※とのデータや認証連携、他クラウドとの連携など、医療情報システムとクラウドサービス接続において、利用者の利便性や負荷軽減、コスト削減を実現する各種機能をトータルで提供

※ Hospital Information System

実績/参考URL

クラウドセキュア接続サービス　MegaOak Cloud Gateway
https://jpn.nec.com/medical healthcare/cloudgateway/index.html

【ユースケース】マルウェア感染拡大防止（EPP）

BluStellar

マルウェアをシグネチャベースで検知
ウイルス対策、ファイアウォール、侵入防止システム（IPS）などの基本的なセキュリティ機能を提供

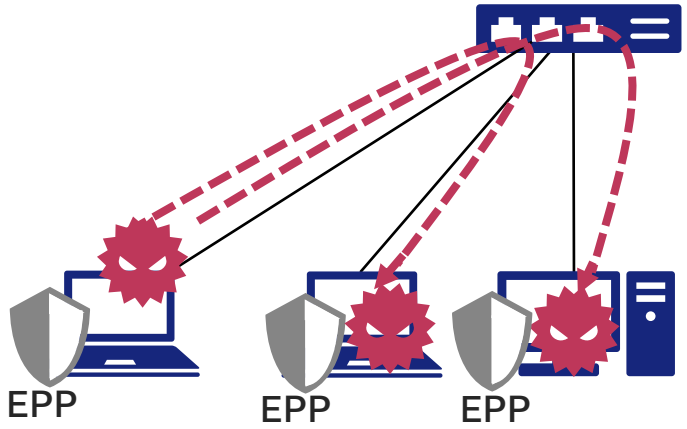
Before

マルウェアの巧妙化

インシデント対応の遅れ

エンドポイントを狙った攻撃

After



既知のマルウェアから防御

既知のマルウェアを検知

リアルタイムの防御機能

概算価格

TrendMicro ApexOne
[SV50台、PC500台]（1年間）¥ 1.8百万～
[SV100台、PC2000台]（1年間）¥ 4.4百万～

【ユースケース】マルウェア感染拡大防止（EDR）

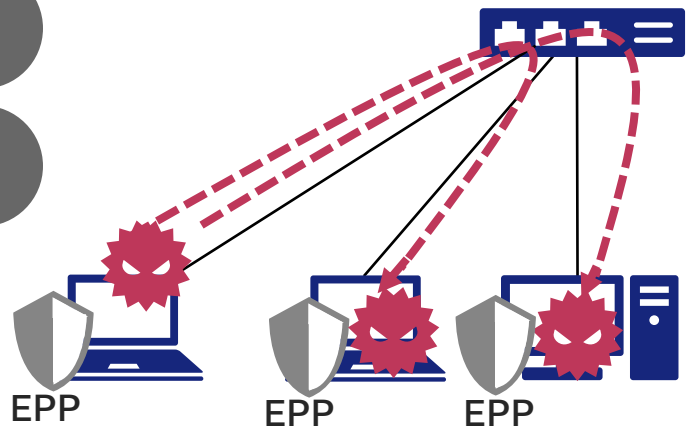
BluStellar

事前対策のアンチウイルス機能（EPP）をすり抜けたマルウェアをEDRで検知
感染端末を隔離し封じ込めることでマルウェアの横展開による被害拡大を防止

Before

マルウェアの巧妙化

横展開による被害拡大

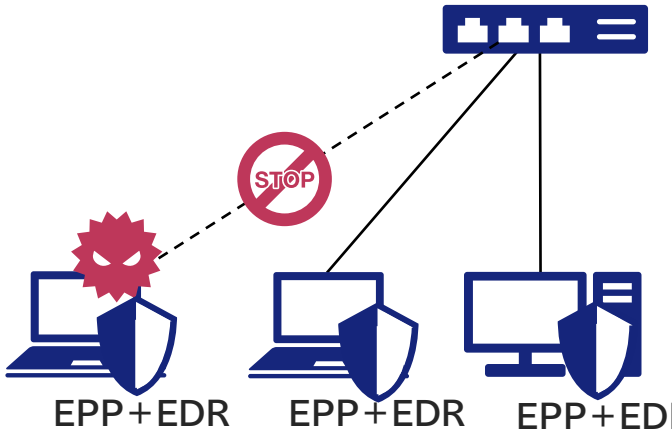


EPPだけでは対処不可能

After

未知マルウェアのふるまいを検知

マルウェア感染端末を隔離



端末のログを常時監視、未知のマルウェアも検知

概算価格

TrendMicro Apex One
[SV50台、PC500台]（1年間）¥ 13.8百万～
[SV100台、PC2000台]（1年間）¥ 25.4百万～

【ユースケース】不正接続の防止

BluStellar

医師や職員の持ち込み端末の接続をクライアント証明書認証やMACアドレス認証で制限
情報漏えいやウイルス感染リスクを軽減

Before

持ち込み端末問題

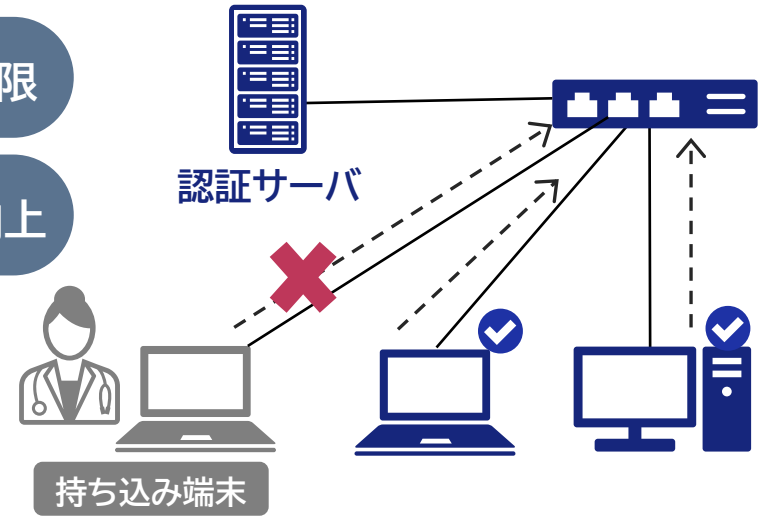
情報漏洩

不正アクセスやウイルス感染のリスク

After

不正接続を制限

セキュリティ向上



適切な認証を用いて不正接続を防止

概算価格

Netattest EPS
［SV50台、CL2000台］（初年度）￥1.8百万～ （次年度以降）￥0.9百万～

【ユースケース】ログの統合管理

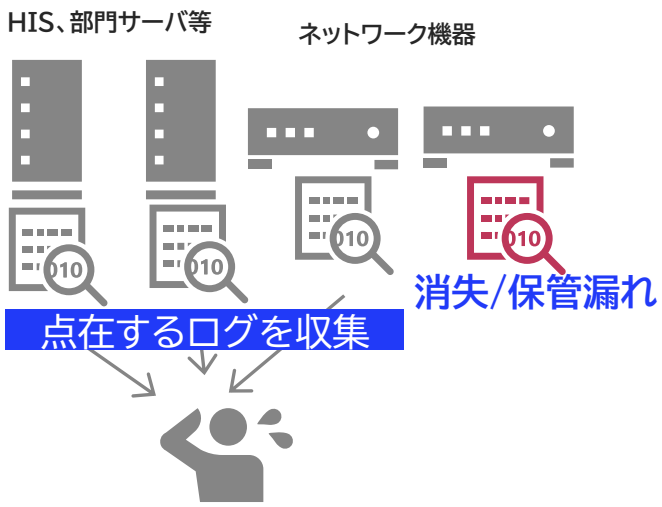
BluStellar

院内IT機器・サーバ等のログを自動収集することで、ログの消失を防ぎ、
セキュリティ事故調査に必要なログを漏れなく管理・分析を行うことが可能

Before

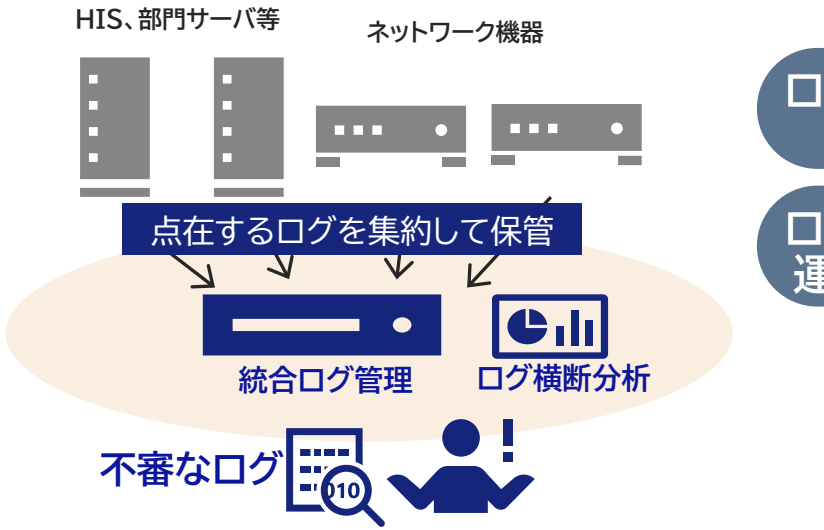
必要なログの消失/保管漏れ

ログ収集・管理の運用負担が大



ログの消失/保管漏れがあると
セキュリティ事故の原因調査が困難

After



集約したログを横断分析することで
効率的な原因調査が可能

ログの消失/保管漏れを防止

ログ収集・管理の運用負担を軽減

概算価格

Logstorage
[SV50台、PC500台]（初年度）￥ 6.6百万～（次年度以降）￥ 1.1百万～
[SV100台、PC2000台]（初年度）￥ 7.2百万～（次年度以降）￥ 1.2百万～

【ユースケース】多要素認証

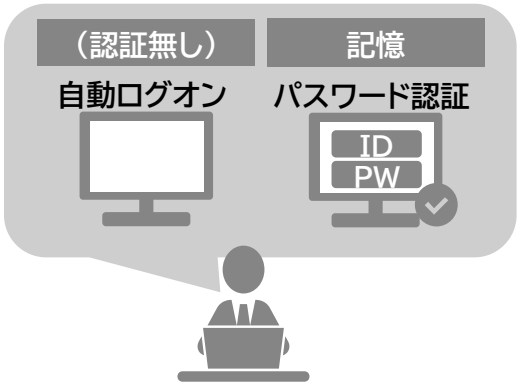
BluStellar

お客様環境に適した認証方式を選択し、利用者負荷を抑えながらセキュリティを向上
厚生労働省ガイドラインにおいても多要素認証への対応が求められている

Before

認証無しでの運用

ID/PWメモ等
モラルに依存



なりすまし等のセキュリティリスク

After

端末ログイン時に
多要素認証

認証方式の
選択・組合せ可能

内部不正や外部者の不正利用を抑止

概算価格

SmartOn ID
［ユーザー数1000人、PC500台、ICカード1000枚、ICカードリーダ500台］
（初年度）ライセンス＋デバイス　￥10百万

【ユースケース】SOCによる監視・分析

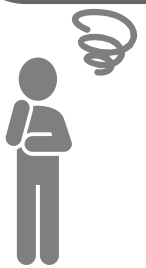
BluStellar

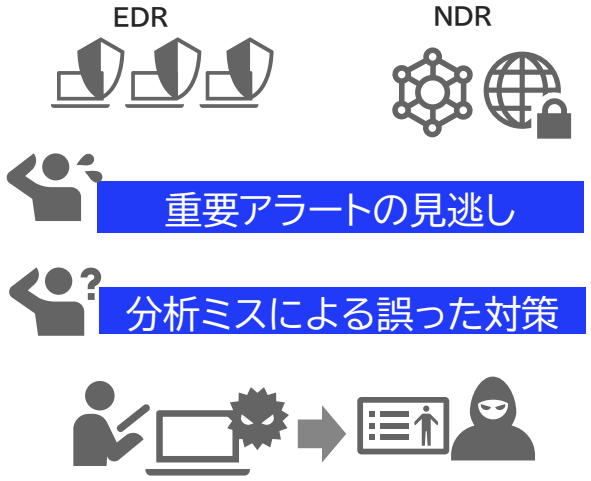
EDRなどのセキュリティ製品を纏めて監視する(SOC)サービスを利用することで
専門家の適切な判断により、迅速な対応と運用負担の軽減を実現

Before

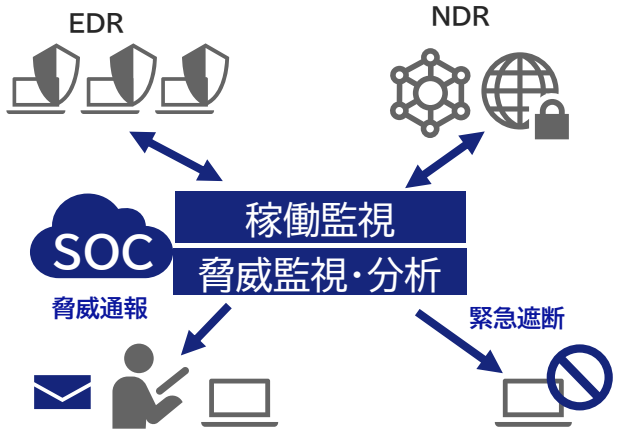
常時監視の運用負担が大きい

脅威分析をする人材不足





After



セキュリティ運用の万全な体制を実現

監視・分析の人材不足解消

適切かつ迅速に対応

概算価格

ActSecure χ
[NW機器監視(PaloAlto　PA-440 ×1台)](初年度)￥　6.9百万～　(次年度以降)￥　6.4百万～
[NW機器監視(PaloAlto PA-3410 ×1台)](初年度)￥20.0百万～　(次年度以降)￥18.5百万～

【ユースケース】内部ネットワークの監視

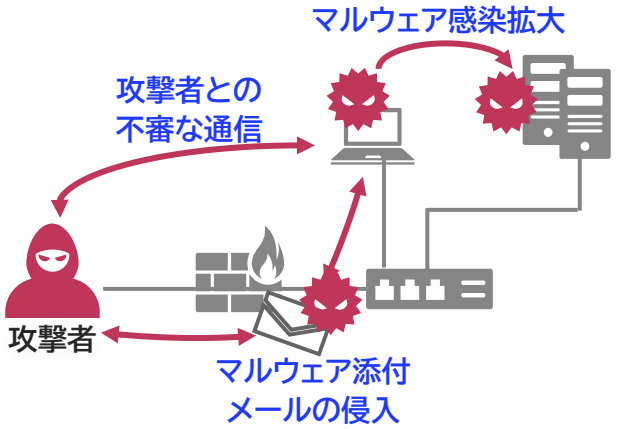
BluStellar

院内ネットワークにおけるマルウェアの不審な挙動を監視・可視化
感染後の横展開やC&Cサーバとの通信、ファイル転送など攻撃と思われる通信を検知

Before

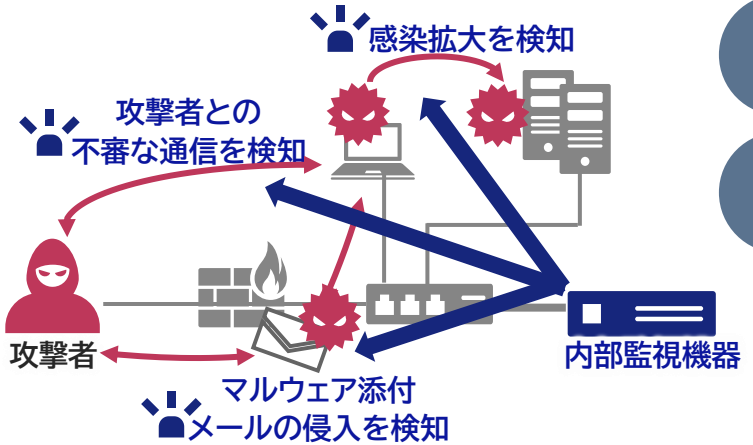
業務環境への影響

マルウェアによる感染被害拡大



マルウェアの感染拡大に気づけない

After



既存環境に影響せずに監視可能

感染時動作を検知・可視化

検知結果を元に初動対応することで、被害拡大を防止

概算価格

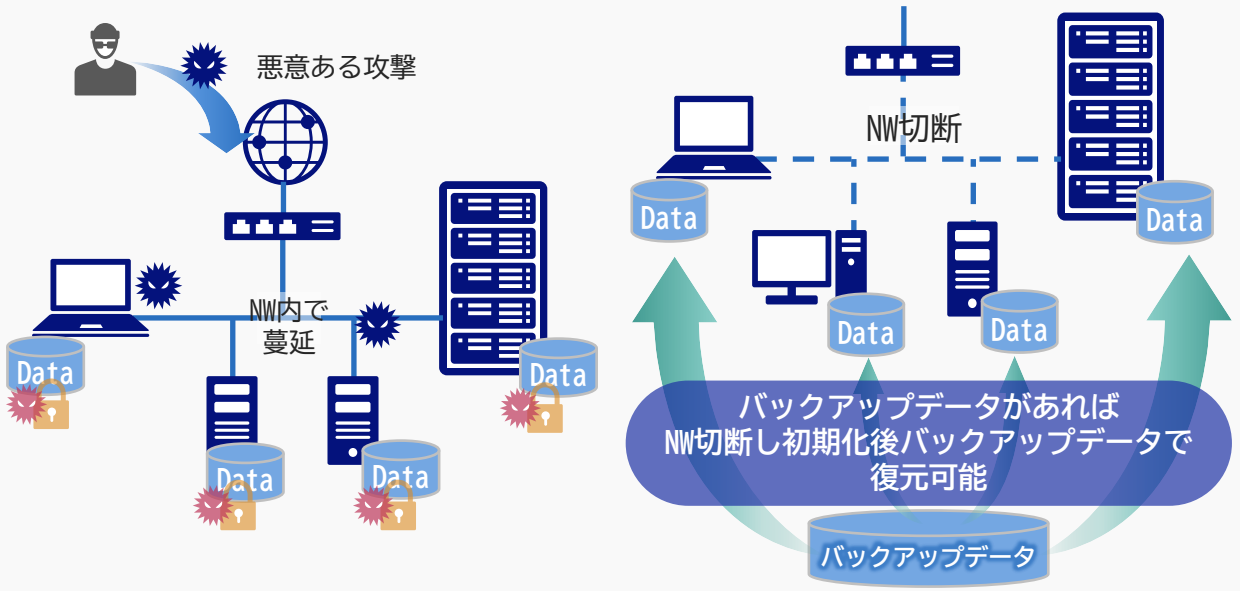
TrendMicro Deep Discovery Inspector
[最小構成]（初年度）￥ 4.0百万～（次年度以降）￥ 0.8百万～
[SV100台、PC2000台]（初年度）￥ 10.3百万～（次年度以降）￥ 2.7百万～

【ユースケース】ランサムウェア対策のバックアップ強化

BluStellar

ランサムウェア対策には、データのバックアップとして、なるべくの多くの世代を保存、ネットワークから切り離された場所に保存、現環境に大きく変更を加えないといったバックアップ強化対策が必要です。

■ランサムウェアはネットワークに接続されているデータをすべて暗号化

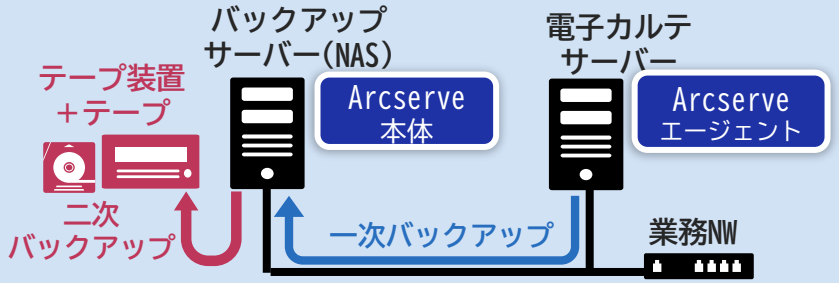


万一感染してしまった場合の復旧方法

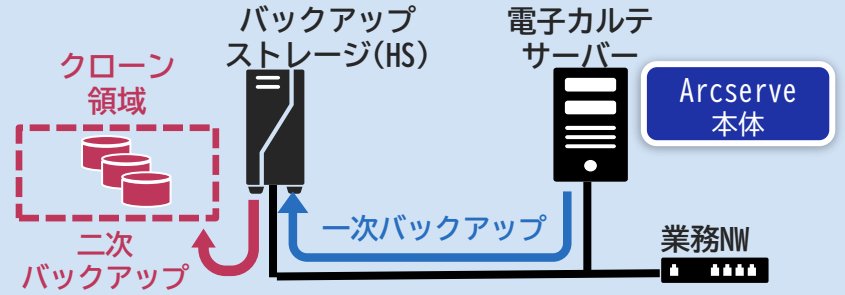
■バックアップ強化

1. なるべく多くの世代を保存
2. ネットワークから切り離された場所に保存
3. 現在の環境に大きく変更を加えない

①テープ装置追加(LTO集合型/iStorage T)



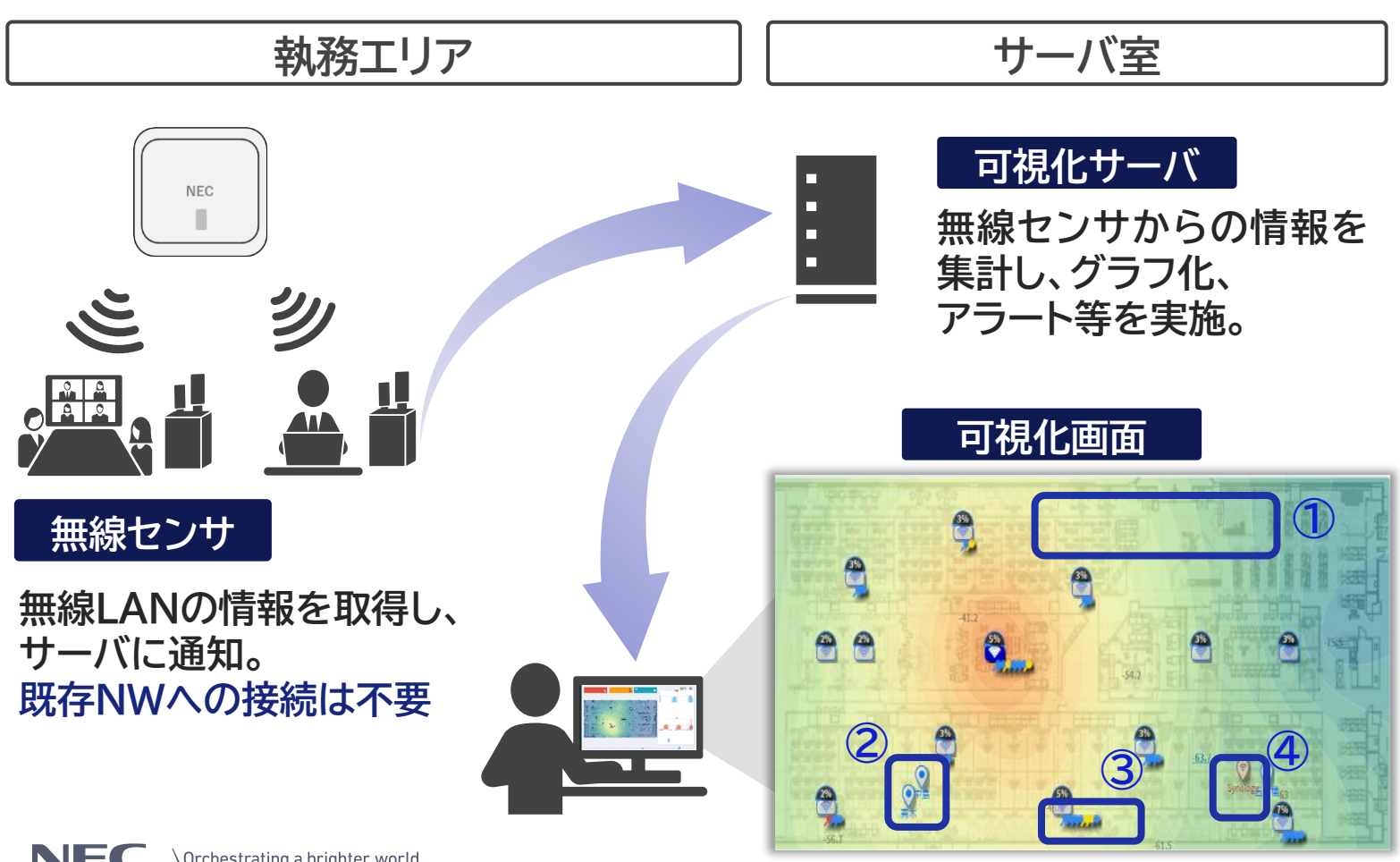
②HS利用時クローン領域追加(iStorage HSシリーズ)



NEC無線可視化ソリューション

BluStellar

アクセスポイントからの電波の強度を可視化します。電波の出力調整や庁舎外への漏洩リスクの参考として、無線LANの高いセキュリティ対策に貢献します。



可視化画面から得られる情報

①APからの電波の強度
赤に近いほど電波が強く、
青に近いほど電波が弱い。
随所に電波強度を数値化したものも表示。

②端末の(推定)位置

③APに接続している端末の数
ピンの数が各地点からAPに接続している端末の数を示す。
ピンの色は端末の品質を示す
(青:良い、黄:注意、赤:悪い)

④不正アクセスポイントの推定位置

サイバーセキュリティ教育

BluStellar

組織のセキュリティカルチャーを醸成し「人」を対象としたサイバー攻撃の対応力を強化

1 アセスメントと教育

グローバル全体のガバナンス強化、サプライチェーンリスク低減

- 教育やテストの結果から意識・知識・セキュリティカルチャーの評価
- 日本語、多言語対応した1300種類以上※のコンテンツを随時提供
- 学習管理システムで自社の教育コンテンツの登録・集中管理

※ 2023.1時点、日本語430種類以上

楽しみながら学べる

3 分析と可視化

個人、組織に適切な教育コンテンツを自動でアサインし、運用負荷の低減

- 訓練結果から個人、部署、組織レベルのリスクスコアを可視化・分析
- 推移とともに教育・訓練の効果を把握

2 サイバー攻撃の疑似体験

本番さながらのメール訓練で
サイバー攻撃に対する意識を向上

- 実践的で豊富なテンプレート提供

ランサムウェア | ビジネスメール詐欺(BEC) | 標的型攻撃

などに対応

KnowBe4
Human error. Conquered.

セキュリティ意識向上トレーニングとフィッシングシミュレーション/分析を組み合わせた世界最大の統合型プラットフォームであるKnowBe4を採用

ポイント

① 従業員のセキュリティ意識に合わせて、セキュリティカルチャーを醸成する学習メニューの作成、進捗管理が可能
② 実践的な疑似メール攻撃により、標的型攻撃への対応力を強化
③ 毎年のセキュリティ教育コンテンツの作成やメール訓練、それらの分析で必要となる工数や費用を削減

ペネトレーションテストと脆弱性診断

BluStellar

重要インフラ業務など社会的に重要な組織からリピートされる高い品質
弊社SOC及びDFIRサービス※1と連携し、日々進化する攻撃手法を取り入れた診断

シナリオとターゲットを決めて
サイバー攻撃の可能性を確認

ペネトレーションテスト

お客様と設定した前提条件や目的へ、脆弱性や設定不備などを悪用することで、
目的が達成できるか検証し、お客様環境のサイバー攻撃耐性を確認

攻撃対象領域を特定　機密情報の窃取　管理者権限奪取　…

導入・構築している(又は予定)の情報システムに関する脆弱性の有無を確認

ウェブアプリケーション診断

システム上で動くWebアプリや、
パッケージアプリ、APIへ診断

スマートフォンアプリケーション診断

Android/iOSアプリ、アプリから
呼び出されるAPIへ診断

ネットワーク診断

サーバ、ネットワーク機器を
はじめITインフラを構成する
製品システムへ診断

ホワイトハッカーチーム

専門トレーニング修了・専門資格※2を保有者が在籍

エンジニアが攻撃者視点で、システムの特徴を踏まえて深く掘り下げる診断
検出された問題をリスクベースアプローチで根本だけではなく緩和策も提示

※1デジタル・フォレンジックとインシデント対応(DFIR) ※2 CISSP, GIAC, 情報処理安全確保支援士等

\Orchestrating a brighter world