# OpreX Managed Service의 플랫폼 아키텍처

***마츠후지 카츠히코 (Katsuhiko Matsufuji)****1*

*Yokogawa는 고객의 가치 사슬을 강화하기 위해 2020년에 OpreX Managed Service를 출시했습니다. 이 서비스 솔루션 프로그램은 고객의 인력, 프로세스 및 기술을 결합하여 문제를 해결할 수 있도록 지원합니다. Managed Service Suite는 OpreX Managed Service의 디지털화 플랫폼입니다.*

*오늘날 운영 기술(OT)은 점점 더 복잡해지고 있으며, 격리된 기존의 시스템은 광범위한 자산 전반에 걸쳐서 다양한 문제를 야기하는 경향이 있습니다. 따라서 운영 지원 플랫폼에는 유지 보수 작업의 효율성을 개선하고 운영 위험을 방지하기 위해 확장 가능하고 유연하며 고도로 안전한 아키텍처가 있어야 합니다. 본 글에서는 Managed Service Suite의 주요 기능과 이 플랫폼이 이러한 요구 사항을 어떻게 충족시키는지 간략히 살펴봅니다.*

## 도입

최근 수년 동안 제조업에서는 생산성과 품질을 개선하고, 안전하고 안정적인 운영을 보장하기 위해 다양한 혁신 활동이 이루어져 왔습니다. 그 결과 플랜트의 운영 기술(operational technology, OT) 영역은 다양한 기계, 장비, 시스템, 컴퓨터 및 센서와 함께 점점 더 정교해지게 되었습니다. 그러나 이러한 정교함으로 인해 애플리케이션이 격리되고 여러 레거시 시스템이 공존하게 되어 기업은 정보와 데이터를 관리하고 통합적인 방식으로 적절한 운영 및 유지보수를 수행하는 것이 어려워졌습니다. 노후화된 애플리케이션 및 시스템을 적절히 운영하고 유지 관리할 수 있는 인력의 수가 감소하고 있으며, 고도로 전문화된 애플리케이션과 시스템을 유지 관리할 수 있는 인력은 찾아보기 어렵습니다.

또한 유지 보수 및 운영에 필요한 정보 및 관리 프로세스는 각 애플리케이션과 시스템별로 다르며, 유지 보수 활동의 효율성을 높이기 위해서는 시각화 및 표준화가 필요합니다[(1)(2)]. OT 도메인에서 유지 보수 활동에 대한 이러한 과제를 극복하기 위해 Yokogawa는 플랜트 전반에 걸쳐 유지 보수 정보를 통합하고 부서와 위치상의 차이를 넘어 일관된 운영 및 유지 보수를 가능하게 하는 실행 지원 플랫폼 Managed Service Suite를 개발했습니다. 이는 유연하고 확장 가능하며 보안성이 높은 아키텍처를 갖추고 지속해서 성장하는 플랫폼으로, 이미 Yokogawa OpreX Managed Service 솔루션의 일부로 이용할 수 있습니다.

본 글에서는 Managed Service Suite의 구조, 기능 및 요구 사항을 소개하고, 이 플랫폼이 고객의 운영 및 유지 보수 활동에 어떻게 기여하는지에 대해 설명합니다.

*1 디지털 솔루션 본부 산하 라이프사이클 서비스 사업부
솔루션 개발부

## 개발 콘셉트(Development Concept)

플랜트 OT의 운영 및 유지 보수는 점점 더 복잡해지고 있으며, 더 이상 자산 소유자의 유지 관리 인력만으로는 처리할 수 없고, 각 자산 및 애플리케이션에 대한 폭넓은 지식을 갖춘 전문 엔지니어를 확보하여 이들이 함께 작업하도록 해야 합니다. 그러나 이러한 전문 엔지니어는 일반적으로 플랜트와 떨어진 곳에서 작업하며, 내부 제어 및 사이버 보안을 위해 원격지에서 OT 자산에 접근하는 것은 엄격히 제한됩니다. 따라서 OT 자산의 운영 및 유지 보수는 현지 서비스 엔지니어의 기술에 크게 좌우됩니다.

한편 Yokogawa는 그동안 유지 보수 및 운영 지원 시스템을 구축하고 대규모 플랜트를 위한 서비스 솔루션을 제공할 수 있는 많은 기회가 있었습니다. 하지만 극복해야 할 하나의 기술적 과제가 있었습니다. 대규모 플랜트에서는 정보를 통합하고 액세스를 제어하며 OT 도메인의 광범위한 개체를 종합적으로 유지 관리하기 위해 정보 플랫폼이 필요합니다. 이러한 요구 사항을 충족하는 상용 패키지가 없기 때문에 일반적으로 여러 IT 운영 관리 제품을 사용자 정의하여 사용합니다. 그러나 이러한 접근 방식은 확장 가능성, 비용 및 대응 속도 측면에서 문제가 있습니다. 그래서 우리는 "단일 창(single pane of glass)" 접근 방식과 OSS-지향 모듈형 설계를 채택하고, OT 도메인에서 유지 보수를 위한 새로운 서비스 지원 플랫폼을 개발했습니다.

(1) 단일 창(Single pane of glass)

"단일 창"은 다양한 요소들이 한 장소에 모여 있는 것을 가리킵니다. 우리는 모든 사용자 역할 및 사용 시나리오에 대해 일관된 플랫폼 사용자 인터페이스(UI) 를 개발하여, 사용자가 자산 및 애플리케이션과 관련된 필요 정보를 한 눈에 볼 수 있도록 했습니다.

운영 상태에 대한 데이터는 단일 디지털 플랫폼에서 수집된 다음, 상시 분석 및 모니터링 됩니다. 이를 통해 OT 도메인의 다양한 자산 및 애플리케이션의 상태를 중앙집중 방식으로 파악하고 필요한 조치를 취할 수 있습니다. 이러한 자산 및 애플리케이션에는 컴퓨터, PLC/DCS, 네트워크, DCS 애플리케이션, 안전 애플리케이션, 보안 애플리케이션 등이 있습니다. 이 정보는 아래 설명된 티켓팅 시스템에도 연결되며, 다양한 기관 및 담당 인력과 자동으로 통지 및 공유됩니다. 게다가 원격 운영 및 컨텐츠 배포와 같은 유지 보수 업무 흐름 제어와 정보를 통합할 경우, 종합적이고 효율적인 유지 보수 활동이 이루어질 수 있습니다.

(2) OSS- oriented modular design

기존의 오픈 소스 소프트웨어(OSS) 솔루션은 Managed Service Suite를 구성하는 주 소프트웨어 프로그램을 구축하는 데 사용됩니다. 이 원칙은 OpreX Managed Service 및 그 실행 지원 플랫폼인 Managed Service Suite가 라이프사이클 지원을 제공하면서 플랜트 내 OT 도메인에서 적용 범위와 솔루션을 확장할 수 있도록 보장합니다. 개발자와 사용자 커뮤니티의 도움으로 OSS는 품질과 가치를 향상시켰고, 시스템 간 통합 및 플러그인을 위한 여러 가지 고급 소프트웨어 제품이 있습니다. OSS를 사용하면, 상용 소프트웨어를 사용자 정의하거나 사내에서 만드는 것에 비해 유연하고, 안정적이며, 우수한 솔루션을 더 빨리 개발할 수 있습니다.

## 아키텍처(ARCHITECTURE)

### 전반적 구조

OpreX Managed Service에 대한 실행 지원 플랫폼은 Managed Service Suite, 티켓팅 시스템, 네트워크 운영 센터로 구성됩니다. Managed Service Suite는 중앙 구성 요소와 현장 구성 요소로 구성됩니다(그림 1).

Managed Service Suite는 정보를 시각화 하여, 필요할 경우 이를 서비스 운영 지원 팀에 통지합니다.

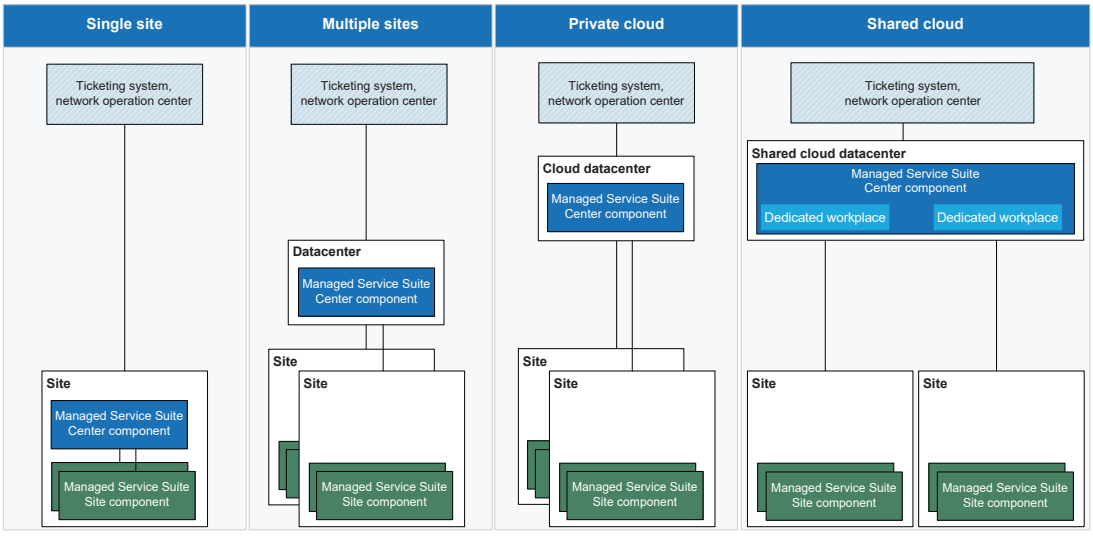


**그림1** Managed Service Suite의 전개 패턴

티켓팅 시스템에서도 알림을 받으며, 팀은 티켓을 지속해서 업데이트 하고, 이를 전문 엔지니어에게 지속해서 확대하며, 진행 상황을 관리합니다. 네트워크 운영 센터는 Managed Service Suite의 운영 상태를 모니터링 하고, 계획된 유지 보수 및 긴급 유지 보수를 수행하며, 제공되는 콘텐츠를 관리합니다.

**현장 구성 요소(Site Component)**

OT 자산 및 애플리케이션에서 정보를 수집하기 위해 Managed Service Suite의 현장 구성 요소는 OT 자산 및 애플리케이션에 가까운 개방형 시스템간 상호 접속(open systems interconnection, OSI) 참조 모델의 네트워크 계층에 배치됩니다.

현장의 OT 도메인을 담당하는 사람이 관리하는 현장 구성 요소는 어떤 사용자에게 자산 및 애플리케이션에 대한 어떤 정보가 이용 가능한지 상세히 명시합니다. 이 기능은 각 기관 또는 담당 인력이 서비스 계약의 범위 내에서만 서비스를 이용할 수 있도록 합니다.

**중앙 구성 요소(Center Component)**

OpreX Managed Service의 예상 사용자는 두 가지 그룹으로 분류됩니다. 즉, OT 자산 및 애플리케이션 담당자와 장비 담당 인력 등 현장에서 근무하는 사용자 그룹, 그리고 지원 데스크 인력 및 전문 엔지니어와 같이 외부에서 유지 보수 활동을 지원하는 사용자 그룹입니다. 외부에서 현장 구성 요소에 직접 접근하는 것은 보안 위험이 있기 때문에 허용되지 않습니다. 현장 구성 요소와 물리적으로 분리된 중앙 구성 요소는 필요한 정보에 접근할 수 있도록 하위 그룹에 속합니다.

현장 구성 요소가 OT 자산 및 애플리케이션에 대한 정보를 수집한 다음, 중앙 구성 요소는 이를 시각화하고, 접근 제어를 적용하며, 지원 데스크 및 전문 엔지니어에게 해당 정보를 제공합니다. 현장 구성 요소의 인증을 받은 사용자는 자산 및 애플리케이션과의 상호 작용, 예를 들면 원격 접속 및 파일 전송을 할 수 있습니다. 이 경우, 중앙 구성 요소가 런처(launcher) 역할을 합니다. 또한 중앙 구성 요소는 확인된 보안 업데이트 파일을 현장 구성 요소로 전달하는 등 콘텐츠 전달 서비스를 위한 상위 저장소 역할을 하도록 설계되었습니다.

**전개 패턴(Deployment Patterns)**

위에서 설명한 대로, Managed Service Suite는 중앙 구성 요소와 현장 구성 요소로 구성되어 있습니다. 이 물리적 구성을 이용하여 Managed Service Suite는 네트워크 정책 및 기타 요구 사항에 따라 다양한 방식으로 배치될 수 있습니다(그림 1).

- 단일 현장(Single site, 단일 기업용)
  사무실 또는 현장에 중앙 구성 요소 및 현장 구성 요소를 모두 배치합니다
- 복수 현장(Multi-site, 단일 기업용)
  데이터 센터에 중앙 구성 요소를 배치하고, 복수의 사무실 및 현장에 현장 구성 요소를 배치합니다.
- 개인 클라우드(Private cloud, 단일 기업용)
  개인 클라우드 데이터 센터에 중앙 구성 요소를, 복수의 사무실 및 현장에 현장 구성 요소를 배치합니다.
- 공유 클라우드(Shared cloud, 복수 기업용)
  공유 클라우드 데이터 센터에 중앙 구성 요소를 배치하고, 복수의 사무실 및 현장에 현장 구성 요소를 배치합니다. 중앙 구성 요소는 각 기업, 사무실, 현장에 대해 준비된 전용 작업 장소를 통해 접근을 제어합니다.

## 기본 기능(BASIC FUNCTIONS)

본 섹션에서는 Managed Service Suite의 기능에 대해 설명합니다. 그림 2는 그 기본 기능을 개략적으로 보여줍니다.

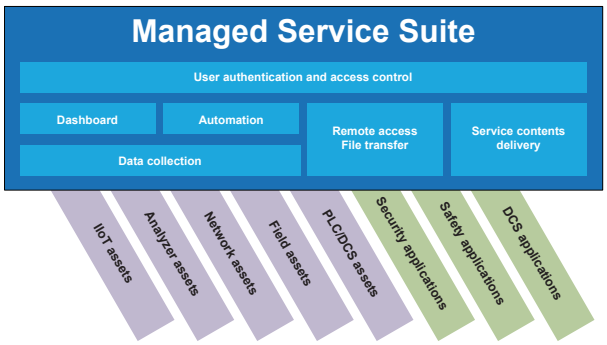


**그림2** Managed Service Suite의 기능

**데이터 수집(Data Collection)**

현장 구성 요소는 다양한 자산 및 애플리케이션의 유지 보수와 관련된 데이터를 수집합니다. 이 기능은 플러그인으로 사용자 정의가 가능합니다. 수집된 데이터는 중앙 구성 요소로 전송되며, 대시보드 및 자동화 기능을 통해 각 자산 및 애플리케이션에 대한 지원 헬프 데스크 및 전문 엔지니어에게 제공됩니다.

**사용자 인증(User Authentication) 및 액세스 제어**

Managed Service Suite는 OT 자산/애플리케이션 관리자 및 현장에서 근무하는 그 밖의 장비 책임자는 물론, 지원 데스크의 인력 및 외부에서 유지 보수 활동을 지원하는 전문 엔지니어 등 폭넓은 범위의 사용자가 있습니다. 따라서 사용자 및 데이터 자원 액세스를 지속해서 관리해야 합니다. 중앙 및 현장 구성 요소에 대한 접근 권한은 Active Directory에서 관리합니다. 사용자 인증에 대해서는 Cisco Duo 및 Google AuthenticatorTM과 같은 다양한 다중 요소 인증 방법을 플러그인으로 사용할 수 있습니다.

**대시보드(Dashboard)**

중앙 구성 요소의 대시보드는 현장 구성 요소에 의해 수집된 정보를 표시하며, 그 디스플레이 구성은 자산과 애플리케이션에 대해 쉽게 전환될 수 있습니다. 대시보드 상단에는 핵심 성과 지표(KPI), 추세 그래프, 파이 차트 및 다양한 그래픽의 상위 10위까지의 목록이 표시됩니다. 자산 관리 및 애플리케이션 관리를 위한 대시보드 디스플레이가 기본으로 제공됩니다. 그러나 각 조직 또는 담당자가 서로 다른 정보 세트를 필요로 하는 경우가 많기 때문에 사용자는 표시할 창과 정보의 배열을 맞춤으로 구성할 수 있습니다.

다음은 대시보드 디스플레이의 두 가지 예입니다. 그림 3은 보안 애플리케이션 관리자가 보안 업데이트 및 바이러스 백신 소프트웨어 업데이트의 진행 상황을 한 눈에 확인할 수 있도록 한 대시보드를 보여줍니다. 그림 4는 컴퓨터 자산 유지 관리를 지원하여 운영 상태 및 리소스 활용을 한 눈에 확인할 수 있도록 하는 전문 엔지니어용 디스플레이입니다.

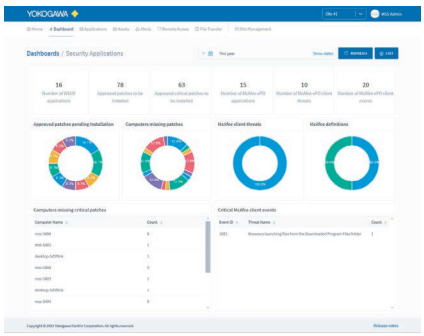

**그림3** 보안 애플리케이션용 대시보드

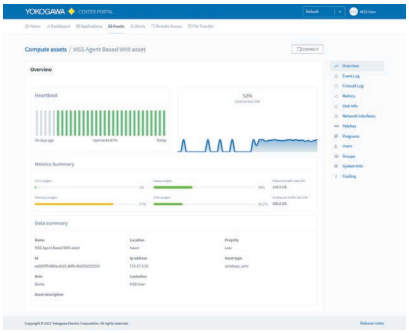

**그림4** 컴퓨터 자산용 대시보드

### 자동화(Automation)

대시보드에 유용한 정보가 표시되긴 하지만, 사용자가 항상 디스플레이를 주시하고 있는 것은 아닙니다. Managed Service Suite는 OT 자산 및 애플리케이션을 모니터링하고 그 다양한 상태 변화를 분석합니다. 이러한 변화 내용이 주의가 필요한 것이라면 Managed Service Suite는 사용자에게 이러한 변화 내용을 알리기 위해 이메일 알림을 전송하고 외부 티켓팅 시스템을 활성화하는 등의 필요한 조치를 자동적으로 수행합니다. 이러한 조치를 수행하기 위해 자산의 중요도, 현재 작업 상태, 값의 임계치, 수신자 등 다양한 조건 및 규칙을 지정하고 결합할 수 있습니다.

### 원격 액세스(Remote Access) 및 파일 전송

중앙 및 현장 구성 요소에 대해 인증을 받은 사용자는 사이트에 있는 OT 자산 및 응용 프로그램에서 원격으로 액세스하고 파일을 송수신(send/receive)할 수 있습니다. 현장에서 OT 도메인을 담당하는 사용자를 위해 Managed Service Suite는 단순한 역할 기반 액세스 제어 설정뿐만 아니라 요청, 승인, 감사 등에 사용할 수 있는 세 가지 옵션 설정도 제공합니다. 이를 통해 Managed Service Suite는 OT 도메인에 액세스가 필요한 다양한 시나리오에서 모든 운영 정책을 준수할 수 있습니다.

- 세션 제어(Session control)
  각 세션에 대한 승인 요청 및 지정된 시간 또는 애플리케이션에 대해서만 설정되는 세션 허용과 같은 설정을 구성할 수 있습니다.
- 실시간 뷰(Live view)
  원격 액세스의 활성 세션을 현장 관리자 및 그 밖의 사용자와 공유할 수 있습니다.
- 원격 액세스 세션 기록(Remote access session recording)
  원격 액세스 세션 동안 영상 및 키보드 동작을 기록할 수 있습니다.

### 서비스 콘텐츠 전달(엔드포인트 서비스)

보안상의 이유로, OT 자산 및 애플리케이션은 일반적으로 인터넷상의 리소스에 액세스할 수 없거나 엄격하게 제한됩니다. Managed Service Suite는 고객, 네트워크 및 시스템 구성의 유지 보수 및 운영 정책에 따라 현장 외부에서 OT 도메인의 자산으로(또는 그 반대로) 서비스 콘텐츠 전달(엔드포인트 서비스)을 위해 사용할 수 있습니다(그림 5). 보안 업데이트 배포 서비스 및 메일 릴레이 서비스는 이 엔드포인트 서비스의 예로 아래에 설명되어 있습니다.

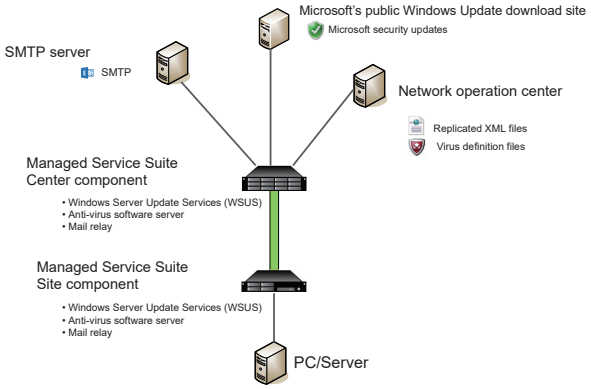


**그림5** 서비스 콘텐츠 전달의 구성 예

- 보안 업데이트 배포 서비스
  중앙 구성 요소 및 현장 구성 요소는 모두 윈도우즈 서버 업데이트 서비스(Windows Server Update Services, WSUS) 및 바이러스 백신 소프트웨어 서버와 함께 기본으로 제공됩니다. 이들은 OT 도메인의 컴퓨터에 대한 보안 업데이트를 관리할 수 있습니다. 이 서버들은 네트워크 운영 센터에서 전달된 검증된 최신 Microsoft 보안 업데이트 및 바이러스 정의 파일을 수신합니다. 이 서비스는 이러한 파일을 결합하여 현장의 엔드컴퓨터에 전달합니다.
- 메일 릴레이 서비스(Mail relay service)
  OT 자산이나 애플리케이션이 이메일을 통해 그 운영 상태를 출력하는 기능을 가지고 있는 경우, 이 서비스는 중앙 및 현장 구성 요소와 SMTP 서버에 있는 메일 릴레이 기능을 통해 외부 당사자에게 해당 이메일을 배포할 수 있도록 지원합니다.

## MANAGED SERVICE SUITE의 보안성

사이버 보안 위협이 지속적으로 증가함에 따라, Yokogawa는 IEC 62443 시리즈 등의 국제 표준을 기반으로 OpreX Managed Service 및 Managed Service Suite에 대한 사이버 보안 정책을 수립하고, 개발, 운영 및 유지 보수의 모든 측면에서 해당 정책에 따라 평가를 수행하고 조치를 취해 왔습니다. 긴급한 취약성이 발견될 경우, 일반적인 OT 애플리케이션의 경우와 마찬가지로 Managed Service Suite에 패치가 적용됩니다. 또한 약 4개월마다 최신 버전을 출시하여 보안을 평가하고 이 주기에서 예방 목적으로 설계를 수정합니다. 이를 통해 보안 플랫폼이 지속적이고, 안정적이며, 신속하게 제공될 수 있게 됩니다.

중앙 및 현장 구성 요소의 네트워크 구성은 물론, 그 물리적 및 데이터 액세스 제어는 Yokogawa 와 OT 도메인 관리자가(고객을 대신하여) 상호 보안 정책을 기반으로 철저히 논의하고 합의한 것으로, 이는 OpreX Managed Service 구현 계획에 명확하게 정의되어 있습니다.

## 비상 유지 보수의 예

다음은 제어 시스템에 심각한 문제가 발생한 경우 비상 유지 보수를 위해 Managed Service Suite를 어떻게 사용할 수 있는지에 대한 하나의 예입니다 (그림 6).

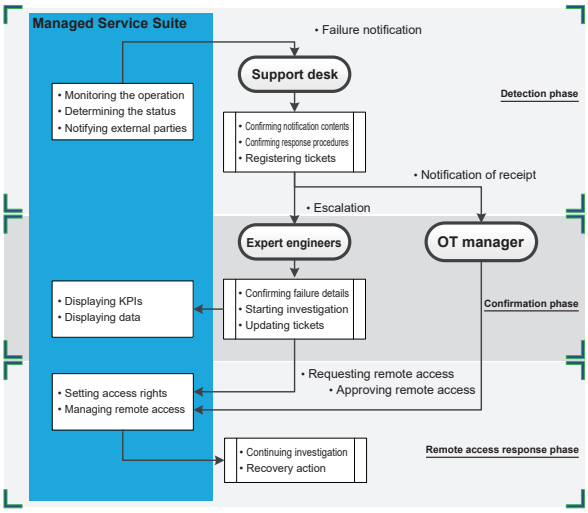


**그림6** 비상 유지 보수의 예

■ 감지 단계(Detection phase)
현장 구성 요소에 의한 지속적인 모니터링을 통해 자산 또는 애플리케이션의 문제나 고장이 발생할 경우 자동적으로 지원 데스크에 통지됩니다. 지원 데스크는 중앙 구성 요소에 표시된 현장 지도와 티켓팅 시스템에 활성화된 티켓을 참조하여 사고 발생을 신속하게 인식하고 초기 대응을 촉구합니다.

■ 확인 단계(Confirmation phase)
지원 데스크는 상황의 심각도에 따라 전문 엔지니어에게 상황에 대해 알려줍니다. 그런 다음 전문 엔지니어는 중앙 구성 요소의 대시보드에서 정보를 확인하고, 원격 액세스 서비스가 필요한지 여부를 결정합니다.

■ 원격 액세스 대응 단계(Remote access response phase)
원격 액세스 서비스가 필요한 경우, 전문 엔지니어는 중앙 구성 요소에 대한 세션을 요청합니다. OT 도메인 관리자가 현장 구성 요소에 대한 세션을 허가하면 전문 엔지니어는 조사를 시작하고 원격 액세스 및 파일 전송 기능을 이용하여 조치를 취합니다.

이 예에서는 지원 데스크, OT 도메인 관리자, 전문 엔지니어가 어떻게 협력하고 고도의 효율성, 투명성, 확실성 및 보안을 갖춘 비상 유지 보수를 수행하기 위해 Managed Service Suite를 어떻게 최대한 활용하는지를 보여줍니다.

## 결론

Managed Service Suite는 OpreX Managed Service의 디지털화 플랫폼입니다. 본 글에서는 OT 도메인에서의 다양한 문제를 해결하기 위해 필요한 요건들을 이 플랫폼이 어떻게 충족시키는지 설명했습니다. OpreX Managed Service의 지속적이고 안정적인 제공 외에도 Yokogawa는 고객의 새로운 요구 사항 및 문제를 파악하고 이를 극복하기 위해 필요한 프로세스와 플랫폼을 개선하며, 고객의 가치를 높이기 위해 노력할 것입니다[3].

## 참고문헌

(1) Japan Institute of Plant Maintenance, “Summary of 2020 Maintenance Survey Report,” 2021, pp. 26-36 (in Japanese)
(2) Ministry of Economy, Trade and Industry, “Measures to Promote Manufacturing Technology (Part 1-1-3, White Paper on Monozukuri 2020),” 2021, pp. 65-103 (in Japanese)
(3) Joseph Ting, “Digital Transformation in Process Industries,” Yokogawa Technical Report English Edition, Vol. 64, No. 1, 2021, pp. 1-8