<특집> 프로세스형 제조업의 DX추진과 시스템 혁신

제조업 DX 추진을 저해하는 보틀넥과 해결 어프로치

제조 현장의 IT 인프라 개혁으로 움직이기 시작한 제조업 DX

사쿠라이 노조무(櫻井 望)
시스템 테크노 기반 시스템 사업본부 총괄

CONTENTS

요약

1 현재 대기업의 대부분의 공장들은 제어계(OT) 네트워크를 정보계(IT) 네트워크로부터 분리한 '폐쇄형 공장'이 되어 있다. 이것은 고가용성을 가장 중시하는 OT계를 외부로부터 지키기 위한 표준적인 네트워크 구조라고 할 수 있지만, 제조 현장에서의 DX(Digital Transformation) 추진에 있어 이 분리 구조가 보틀넥이 되고 있다.

2 OT 네트워크의 분리 구조는 정보 보안 기준 등의 규정을 바탕으로 운용되고 있으며 장기간에 걸쳐 재검토되지 않아 폐쇄형 공장 구조를 경직화시키는 원인이 되었다.

3 향후, 제조업은 부가 가치와 경쟁 환경이라는 면에서 하드웨어를 기점으로 소프트웨어를 활용하여 고객을 위한 계속적 부가 가치 비즈니스로의 전환이 중요하다. 제품(하드웨어), 서비스, 솔루션이라는 3가지 관점에서 고객과의 관계성을 강화할 필요가 있다.

4 '고가용성을 위한 OT 분리'와 'DX 추진을 위한 접속'이라는 상반된 요건에 대응하려면 'IT 인프라의 구조 개혁'과 '공격적인 정보 보안 기준 책정'이 필요하다.

5 앞으로 DX 활동을 추진하기 위해 가장 먼저 움직여야 할 조직은 기존의 정보 시스템 부서가 아닌, 새롭게 DX 활동을 추진하고 선도하기 위해 조직화된 DX 추진 핵심 부서여야만 한다.

6 마지막으로 DX 추진 핵심 부서가 수행해야 할 역할이나 IT 인프라 구조 개혁을 위한 활동을 시작했을 때 필요한 '공격적인 정보 보안 기준 책정' 및 'IT 인프라 디자인'이라는 두 부문에서 구체적인 구현 포인트를 제시한다.

Ⅰ. 제조업 DX 추진을 저해하는 보틀넥

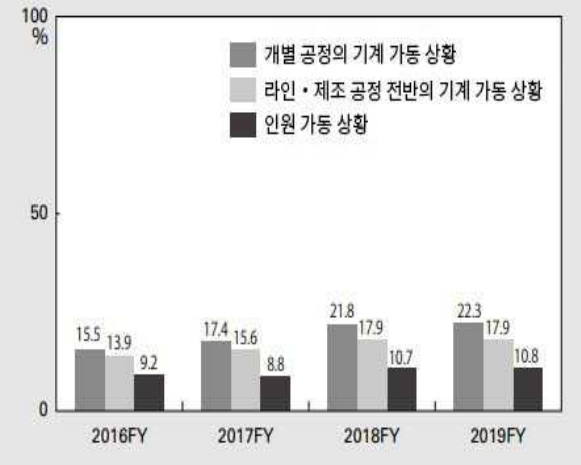
1. 폐쇄형 공장 네트워크

제조업에서 IT 인프라 환경은 크게 두 가지로 구별하여 나눈다. 첫 번째는 기간 시스템 · 전자 메일 · 파일 서버 등을 이용하기 위한 정보 IT계 네트워크(Information Technology)이며, 두 번째는 공장 내에 구축된 생산 설비의 제어 · 감시, 또는 생산 관리 시스템이 배치된 제어 OT계 네트워크(Operational Technology)이다.

IT계 네트워크는 업무 효율화나 정보 공유 · 데이터 분석 등 다양한 목적을 위해 이용되고 있다. 근무 방식 개혁의 흐름 속에서 사외 액세스도 필요로 하고, 클라우드의 이용과 활용도 추진되는 등 '광범위한 연결의 네트워크'가 요구되고 있다.

한편 OT계 네트워크는 해당 거점 생산 설비를 정상으로 가동하는 것이 목적이기 때문에 고가용성이 가장 중시된다. 따라서 OT계 IT 인프라는 최대한 변화를 주지 않고 손대지 않는 것이 기본이다. 그 결과 OS나 각종 소프트웨어의 버전 업, 단말의 바이러스 스캔조차 리스크라고 여겨져 지금도 서포트가 끊긴 OS가 바이러스 대책도 충분히 세워지지 않은 상태로 운용되고 있다.

그림1 일본 제조업의 '가시화' 실시 상황



IT계 관점에서는 보안 대책이 불충분한 OT 네트워크 접속이 리스크가 되며, OT계 관점에서는 IT 통신으로 인해 생산 설비에 미치게 되는 영향이 리스크가 되고 있다. 그리하여, 필연적으로 OT와 IT 사이에 방화벽이 설치되거나 물리적으로 격리된 '폐쇄형 공장 네트워크'가 상식이 되었다. 하드웨어형 방화벽이 생긴지 20여 년이 지났지만, 자사에서 규정한 정보 보안 기준 등을 기반으로 여전히 많은 기업이 폐쇄형 네트워크를 고수하고 있으며, 이것이 정답이라고 여기고 있다.

미국, 독일, 신흥국 등에서는 디지털 기술 혁신을 배경으로 환경 변화에 대응하는 전략을 추진 중이다. 일본에서도 Society 5.0 실현을 위한 'Connected Industries' 콘셉트가 세계로 발신되고 있지만 일본 제조업은 성장이 저조해 애를 태우고 있다. 일본 제조업이 다른 나라와 비교하여 크게 성장하지 못한 이유는 '폐쇄형 공장 네트워크'로 인하여 생산 기술 향상을 제한적으로 밖에 이용하지 못했다는 측면도 있을 것이다.

한편 신흥국은 최신 생산 기술을 탑재한 제조 장치를 도입하여 경쟁력을 높이고 미국과 유럽은 실시간 OT 활용을 통한 비즈니스 모델의 변경으로 경쟁력 자체에 변화를 주어 일본 기업에 적극적인 공세를 펼치고 있다. 그 결과 DX가 추진되지 않은 일본 제조업은 상대적으로 국제 경쟁력이 저하되었다고 볼 수 있다.

실제로 일본 제조업의 DX가 제자리걸음 상황임을 그림1 데이터를 통해 알 수가 있다. 경제산업성의 '2019년도 제조 기반 기술 진흥 시책'에 따르면 2019년도 국내 제조업에서 센서와 IT를 활용하여 '가시화'를 실시한 기업 수의 비율은 ① 개별 공정 기계: 22.3%, ② 제조 공정 전반: 17.9%, ③ 인원 가동 상태: 10.8%로 모두 낮은 추이를 보였다.

2. 바뀌지 않는 정보 보안 기준

폐쇄형 공장 네트워크의 구조는 어디에 기반하여 만들어졌을까. 대부분 기업은 각사의 정보 보안 기준과 네트워크 구축 규정이 정해져 있으며, 경우에 따라서는 불문율처럼 '연결하지 않는다'를 계승한 사례도 있을 것이다. 기존의 '폐쇄형 공장 네트워크'는 조직에 깊숙이 침투되어 있으며 리모트 액세스나 인터넷 접속 같은 이야기를 꺼내는 것조차 꺼리지는 분위기이다. 현장 레벨에서 나오는 여러 가지 대책도 '어차피 보안상 허가하지 않을 것이다.'라며 단념하는 케이스가 적지 않다고 한다.

최근 DX가 기업 경쟁력을 높이는 요소로 데이터 이용과 활용이 필수가 되고 있는데, 기존에 답이라 여겼던 '폐쇄형 공장 네트워크' 그리고 '전통적 정보 보안 기준'이 얼마나 DX를 추진하는 데에 있어 보틀넥이 되는지 우리는 명확히 이해할 필요가 있다.

요즘 공장에서 요청이 매우 많은 'Web 카메라를 이용한 리모트 감시'의 도입을 예로 들어보겠다. 필자가 알기로는 정보 보안 기준을 적절히 정비한 대기업일수록 IT 네트워크에서는 '회사 지정 단말기 이외는 원칙적으로 접속 불가'라는 규정이 많고, 소거법적으로 'OT계 혹은 전용 네트워크 세그먼트라면 Web 카메라를 사용할 수 있지 않을까'라는 발상에 이른다.

만약 OT 네트워크에 Web 카메라를 접속할 수 있게 되면 다음 장벽으로 등장하는 것이 '텔레워크 환경에서도 열람하고 싶다.'라는 요청일 것이다. 신종 코로나바이러스의 영향으로 인해 생산 관리 부문의 텔레워크 요건이 확대됨에 따라서 Web 카메라의 열람 장소가 공장 내부만이 아닌 텔레워크 환경으로도 볼 수 있기를 요청되고 있다. 즉, 공장과 텔레워크 환경 사이를 회사의 VPN 또는 인터넷을 통해 통신으로 연결하는 것이 요구되고 있는 것이다.

서두에서 언급한 제조업 DX의 원천 데이터 전송이든 Web 카메라의 접속이든 이미 '폐쇄형 공장 네트워크' 및 '종래의 정보 보안 기준'인 상태에서는 어느 요건도 만족시키지는 못하고 있다. 본래, 기업의 IT 인프라라는 것은 사업을 원활하고 효율적으로 추진하기 위한 기반이 아니었던가. 이를 방치하면 IT 인프라가 그 역할에 반하여 제조업 DX와 근무 방식의 개혁을 저해하는 장벽이 된다는 것은 두말할 필요도 없을 것이다.

3. 분리된 IT 인프라 관리 부문

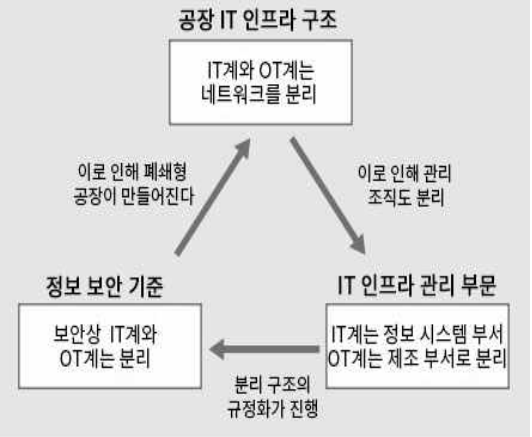
IT 네트워크와 OT 네트워크가 분리된 것처럼 각각의 IT 인프라 관리 부서 또한 분리된 경우가 많다. IT 네트워크는 회사의 정보 시스템 부서, OT 네트워크는 각 공장의 공장 관리 부서에 소속된 형태이다. 그리고 각각의 관리 부서가 정보 시스템 예산과 관리 권한을 가지는데 적절히 거리감을 유지하며 각자 서로의 영역이나 권한에 개입하지 않도록 운용해왔다.

그렇다면 제조업 DX의 저해 요인인 '종래의 정보 보안 기준'은 어디에서 관할하고 있을까. 이것은 회사의 공통 규정이기 때문에 본사의 정보 시스템 부서나 보안 부서가 담당인 경우가 많다. 그 결과 공장의 새로운 대처나 접속 요건은 본사 부서에 '정보 시큐리티 어세스먼트 신청'이라는 형식으로 전달하는데, 본사 부서에서 '종래의 정보 보안 기준'에 따라 요건을 충족하지 못한 케이스는 바로 기각해 버린다. 분리된 정보 시스템 부서와 공장 관리 부서의 온도 차나 '종래의 정보 보안 기준'에 얽매이는 조직 또한 제조업 DX를 저해하는 요인 중 하나라고 할 수 있겠다.

4. 제조업 DX 추진 저해 요인의 삼자 견제 구조

지금까지 언급한 '폐쇄형 공장 네트워크', '종래의 정보 보안 기준' 그리고 '분리된 IT

그림2 공장 IT 인프라의 경직화를 낳은 삼자 견제 구조



인프라 관리부서' 이 세 가지 요소는 한쪽을 움직이려 하면 다른 한쪽에 부딪히는 이른바 '삼자 견제 구조'에 빠져 어느 쪽도 손대기 어려운 상황이다(그림 2).

그렇다면 삼자 견제 구조의 어디서부터 손을 대야 좋을까. 먼저 착수해야 할 것은 '폐쇄'를 '연결'로 변혁하기 위한 '정보 보안 기준의 재검토'이다.

본사 정보 시스템 부서 · 시큐리티 부서가 오랫동안 견지해온 기준을 재검토하기 위해서는 그들이 행동을 바꾸기 위한 계기와 이유가 필요하다. 그 계기가 될 만한 것이 '공장의 DX 추진을 방해하는 IT 인프라 문제'의 올바른 인지와 그 영향 및 일의 중대성에 대한 이해이다.

그런데 본사 측 정보 시스템 부서는 공장 관리 부서 영역에는 관여하지 않기 때문에 공장 측의 실정을 파악하는 것이 어렵다. 따라서 양측의 조직을 서로 이어주는 '제3의 조직'이 필요하다.

Ⅱ. IT 인프라 개혁을 불러올 제3의 조직

1. DX 추진 핵심부서

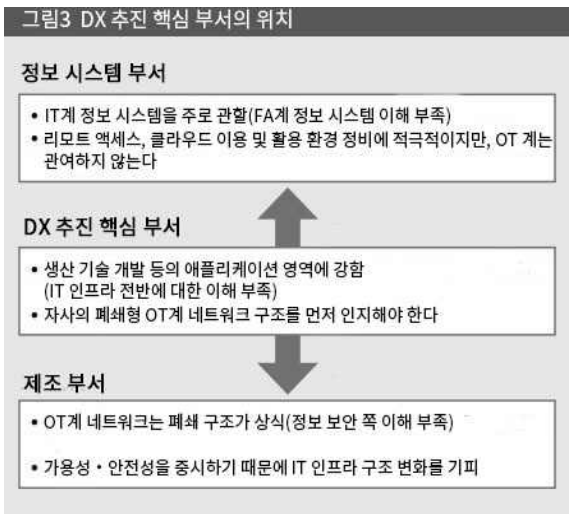
제조업의 DX 추진에는 앞서 언급한 본사 측의 정보 시스템 부서와 공장 측의 공장 관리 부서와 더불어 제3의 조직이라 말할 수 있는 'DX 추진 핵심부서'가 가장 중요한 열쇠를 쥐고 있다. 여기서 그 역할에 대해 논하겠다.

경영 전략으로 DX 추진을 내건 기업은 DX 추진을 선도하기 위해 전문 조직을 결성하는 케이스가 적지 않다. 제조업에서는 생산 기술이나 생산 전략 부서, 또는 제조 현장에 가까운 조직에서 DX 추진 인재를 모으는 경우가 많을 것이다. DX 추진 핵심부서는 제조업 DX를 추진하기 위해 제조 부서와 정보 시스템 부서 사이의 중간에 위치하여 각각을 연계 · 서로 이어주는 역할을 맡는다(그림 3).

DX 추진 핵심부서는 경향적으로 애플리케이션 영역에 강한 인재에 치우치는 경우가 많고 IT 인프라 영역을 잘 아는 전문가의 비율은 낮다. 오랫동안 공장의 폐쇄형 네트워크가 답이라고 여겨 IT 인프라 구조를 최대한 변경하지 않고 유지해온 결과, 자사의 IT 인프라 구조를 이해하기 위한 다양한 기회를 놓쳐버린 측면을 반영하고 있다고 말할 수 있다.

IT 인프라 영역의 전문가가 포함되지 않은 팀이 PoC(Proof of Concept: 개념 검증)를 시작해도 '개별 환경'에서의 트라이얼까지는 진행할 수 있지만, 폐쇄된 공장 네트워크 안에 있는 실질적 데이터를 분석 기

그림3 DX 추진 핵심 부서의 위치



반으로 보내려고 하면 도중에 IT 인프라 구조 · 보안 기준에 막힌다. 자사의 IT 인프라 환경의 실정을 알지 못한 채 추진했기 때문이다.

한편 자사의 IT 인프라 환경을 이해하는 담당자가 프로젝트 체제에 투입되는 케이스에서는 미리 자사의 IT 인프라 사정도 반영하는 것이 가능하다. 이 경우 PoC 추진과 동시에 IT 인프라 정비도 검토가 진행되기 때문에 본격적인 전개 단계에서 IT 인프라 정비의 필요성을 깨닫는 시간적 손실을 줄일 수 있다.

2. IT 인프라 개혁의 도화선

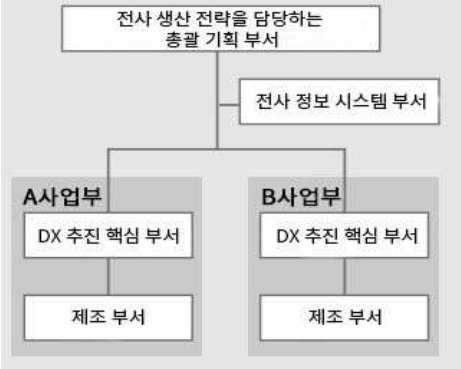
정보 시스템 부서는 OT계를 관할하지 않는 경우가 많아서 공장 측 DX 추진의 답보 상황이나 IT 인프라 구조의 문제를 파악하는 것이 어렵다. 따라서 DX 추진 핵심부서가 정보 시스템부서에 '폐쇄형 공장 네트워크'의 경종을 울리는 역할을 담당한다.

이 조직은 각 사업의 DX 추진에서 발생하는 각종 문제를 반영하는 역할로 사업부 단위로 필요로 하고 있다.

어떤 사업부의 DX 추진 핵심 부서이든 IT 인프라에 관한 문제를 발굴해도 '폐쇄형 공장 네트워크'라는 공통적인 문제에 부딪치고 만다. 이로 인해 선행한 DX 추진 핵심부서의 IT 인프라에 관한 문제 분석 결과는 타 사업부서에도 수평 전개할 수 있게 된다. 사업 부서별로 개별 검토 · 개별 최적화되지 않도록 IT 인프라 개혁 프로젝트 체제에는 '전사 생산 전략을 담당하는 총괄 기획 부서'를 체제의 가장 위에 두는 것이 바람직하다고 볼 수 있다(그림 4).

하지만 DX 추진 핵심부서는 IT 인프라의 이해도가 부족하다. 그래서 등장한 것이 평소 IT 인프라 전반을 구축하고 운용하여 그 실태를 장악하고 있는 IT 인프라 벤더이다. 유저계 IT 자회사는 가장 이에 근접한 입장이다. 상시 현장의 목소리에 귀를

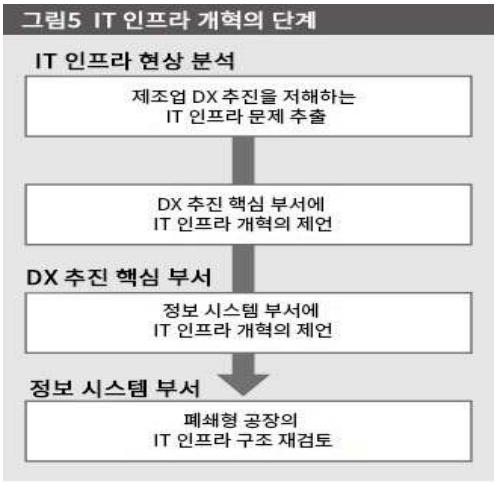
그림4 IT 인프라 개혁 추진 체제 모델



기울이고 DX 추진에서 IT 인프라에 관련된 문제를 수집하고 정리하여 현장이 얼마나 새로운 대처에 고심하고 있는지 DX 추진 핵심 부서에 있는 그대로를 전달해야만 한다. DX 추진 핵심부서가 'IT 인프라 개혁이 필요하다'라고 인지할 수 있다면 거기서부터 IT 인프라 개혁은 크게 움직이기 시작하는 것이다.

본사 측 정보 시스템 부서, 정보 보안 부서, 제조 현장을 둘러싼 IT 인프라 개혁을 위한 문제 분석과 액션 플랜 책정을 시작으로, '연결'을 전제로 한 정보 보안 기준의 재검토, 거기에 기반한 IT 인프라 구조의 재구축이라는 대략적인 흐름으로 진행되어 진다. 실제 필자가 DX 추진 핵심 부서에 제언하기 위해 수행한 사전 정보 수집에서는 어느 그룹 기업의 현장 레벨에서 횡단적으로 공청회를 실시하였다. 그때 DX 추진의 보틀넥으로 IT 인프라 구조 · 정보 보안 기준의 제약, 관리 조직 분리에 동반한 개별 최적화라는 공통적인 문제가 있다는 것을 정리하여 이것을 스테이크홀더의 공통 인식으로 끌어올리기까지 1년 이상이 걸렸다. 그 후 DX 추진 핵심 부서에서 프레젠테이션을 선보여 DX 추진을 위해 IT 인프라 개혁이 반드시 수반되어야 한다는 사실에 대해 깊은 공감을 얻었다.

당시의 고객은 민첩한 행동력으로 즉시 관계 부서를 소집해 '폐쇄형 공장 구조'의 재검토에 필요한 프로젝트 체제를 논의하였



다. 더욱이 그룹 각 사에서 공청회를 진행하여 '폐쇄형 공장 구조'가 DX 추진에서 공통적인 보틀넥이라는 사실도 재확인하였다. 얼마 뒤 전사 생산 전략을 담당하는 총괄 기획부서를 필두로 DX 추진 핵심부서, 정보 시스템부서, 보안 담당, 그리고 문제를 제기한 NRI 시스템 테크노가 IT 인프라 혁신을 위한 프로젝트 체제로서 조직되었다.

<그림 5>는 제조업 DX를 저해하는 요인의 삼자 견제 구조에 변화를 주어 IT 인프라 개혁에 도달하기 위한 단계이다. 기점이 되는 활동은 자사의 현상을 가장 잘 이해하는 IT 인프라 운용을 담당하는 IT 인프라 벤더와 유저계 IT 자회사가 적합하지만, 컨설팅 등을 통한 DX 추진 저해 요인 분석 어프로치 또한 고려 대상이라 할 수 있다.

Ⅲ. 공격적인 정보 보안 기준·IT 인프라 구현을 위한 실천 포인트

1. 연결 리스크를 최소화하기 위해서

2017년 3월에 경제산업성이 제창한 'Connected Industries'를 공장의 OT 네트워크에 적용할 경우 무엇이 요구될까. 이것은 OT 네트워크가 외부와 자유로이 쌍방향으로 통신할 수 있는 환경을 목표로 한다는 이야기가 아니다.

OT 네트워크를 디자인하려면 가장 중요한 것은 가용성의 담보이다. 21년 5월 미국 최대 송유관 업체인 콜로니얼 파이프라인이 사이버 공격을 받아 전미로의 석유 이송이 일시 중단되었다는 보도가 있었다. 이는 OT 네트워크의 '고가용성을 위한 분리'와 'DX 추진을 위한 접속'이라는 상반된 요건을 충족하는 것이 얼마나 어려운지를 다시 한번 느낄 수 있는 사건이라 할 수 있겠다. 제조업 DX에 적합한 IT 인프라 구조를 생각한다면 사이버 공격이 어디에서 올지를 가정한 다음에 제조업 DX 추진에 필요한 통신의 방향성 · 통신처 · 프로토콜 등을 밝혀내 현실적인 답을 도출할 필요가 있다.

OT 네트워크의 특징으로, 고가용성을 보장하기 위해서 단말의 바이러스 스캔이나 각종 패치의 적용 등도 수용하지 못한다는 상황을 앞서 언급하였다. 게다가 현장 담당자는 심리적으로 '외부와 접속되어 있지 않으니 OT는 공격받지 않을 것이다.'라고 착각하고 있는 경우도 매우 많다. 메인터넌스 단말이나 USB 메모리 등을 통해 OT 네트워크 내부로 들어오는 바이러스에는 무방비 상태에 있다는 것을 알고 있어야 한다.

OT 네트워크 특유의 문제라고 할 수 있는 'OS · 애플리케이션 등의 취약성 존재'를 반영한 다음에 제조업 DX로 데이터의 이용 및 활용을 실현하기 위해서는 어떻게 해야 할지에 대한 구현 포인트에 대해 설명하도록 하겠다.

2. 가장 먼저 분석 기반으로 '데이터 업로드' 실현을 목표로 한다

제조업 DX에서 우선 클라우드에 있는 분석 기반으로 '데이터 업로드'를 실현하는 것이 필요하다.

만약 '종래의 정보 보안 기준'에 저촉될 것 같으면 그곳부터 재검토가 필요하다. 기존에 없던 업무 요건인 '공장 내의 각종 데이터를 분석 기반으로 송신'을 대전제로 두

고 이에 대응한 정보 보안 기준 책정이 필요하다.

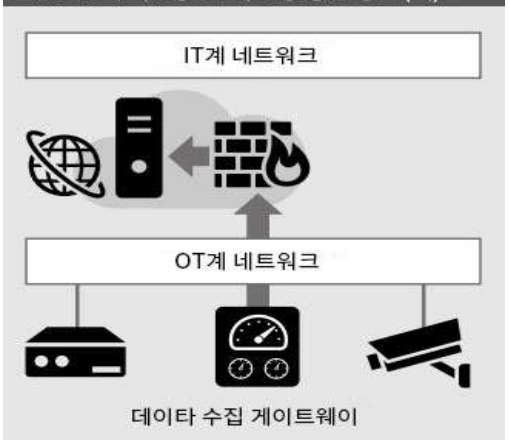
IT 인프라 구조의 관점에서는 고가용성을 중시하는 OT 네트워크에 인터넷 접속점이 존재하지 않는 것이 일반적이다. 만약 클라우드로 데이터 업로드를 고려했을 경우 그 경로로서 'IT계의 LAN · WAN · Web 프록시 등의 유용'을 떠올릴 수 있다. 그러나 아래의 두 가지 이유에서 IT계의 IT 인프라 관리자와 타협이 어려울 것으로 예상된다.

첫 번째는 OT 트래픽 업로드로 인한 IT계 WAN의 트래픽 압박에 대한 우려이다. 미래의 OT 트래픽 유량은 예측이 어렵고 IT 인프라 관리자로서는 '기간 시스템 · IT계 서비스' 보호의 관점에서 OT의 트래픽은 받아들이기 힘든 요소이다.

두 번째는 OT가 요구하는 가용성을 IT 네트워크 환경에서 담보하는 것이 어렵다는 점이다. IT계에서는 계획적으로 네트워크 기기의 노후화에 대응하고 있다. 여기서는 '네트워크 정지'도 수반하는 기기 교환이나 증강 작업이 실시되며, 일반적으로 IT계 이용자를 배려하여 휴일이나 야간에 작업 계획을 세운다. 그런데 OT의 통신 요건이 휴일이나 야간에 정지할 수 없는 요건이라면 IT 네트워크 메인터넌스 조정이 어려워지고 IT계의 IT 인프라 관리자는 OT계의 통신을 받아들이는 것이 어려워진다. 앞서 말했듯이 IT계와 OT계에서 IT 인프라의 관리 조직 · 관리 구분 · 예산 · 책임 등이 분리되어 있으며 두 가지 이유에서도 드러났듯이 'IT계의 LAN · WAN · WEB 프록시 등의 유용'은 어렵다.

그렇기 때문에 OT계 데이터를 분석 기반으로 업로드하기 위해서는 'OT계 전용의 분석 기반용 네트워크 정비'를 생각할 수 있다. <그림 6>에 나타나 있는 것처럼 먼저 IT계 네트워크에 의존하지 않는 OT계 전용의 단독 인터넷 접속점(광회선이나 모바일 회선)을 만든다.

그림6 분석 기반용 OT계 전용 통신 경로 (예)



회사에서 허용한 클라우드상의 분석 기반에 데이터를 업로드할 경우, VPN이나 인증기관 등 적절한 정보 보안 대책을 세우고 OT계 전용 게이트웨이에서 오는 데이터 송신은 허가한다. 공장의 데이터를 클라우드 분석 기반으로 보내기 위한 요건을 정보 보안 기준의 중요한 업무 요건으로 추가가 가능하다면 IT 인프라 설계나 정보 보안 대책의 구체적인 검토가 추진될 수 있다.

3. 사이버 공격을 막기 위해

과거의 IoT 디바이스 등 정보 보안 인시던트 경향을 보면, 해당 기재가 인터넷에서 직접 액세스 가능한 환경에 배치되어 초기 패스워드, 또는 쉽게 추정 가능한 패스워드로 인해 침입한 케이스가 많다. <그림 6>에서 나타낸 구성 예에서는 데이터 수집 게이트웨이가 인터넷에서 직접 액세스되지 않도록 방화벽의 내측에 배치되었다. 기존의 '폐쇄형 공장 네트워크'의 상식을 뒤엎고 OT계에 배치한 데이터 수집 게이트웨이에서 분석 기반으로의 업로드를 제한적으로 허가하는 이런 디자인은 어려운 이야기가 아니다. 한편 인터넷을 포함한 외부 네트워크에서의 접속 요구는 차단한다는 것이 대원칙이다.

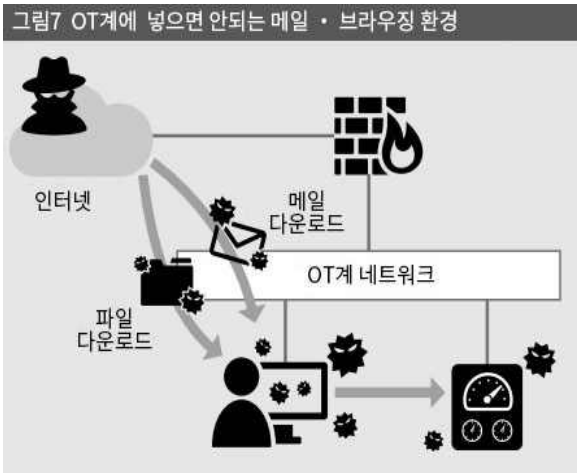
여기서부터는 OT 네트워크의 내부 구조에 대해서 설명하겠다. OT계 LAN은 단일 세그먼트로 구성된 기업도 많을 것이다. 원래 OT 네트워크는 외부 네트워크와 분리되어 있기 때문에 정보 보안 관점에서 OT 네트워크 내부를 추가로 분할할 필요성은 없었다. 그런데 최근의 OT에서는 단일 세그먼트 구조로 인한 리스크가 커지고 있다. OT계에서도 Windows 등의 범용 OS의 이용이 확대되고 있어 바이러스 대책을 세워두지 않으면 OT계 특유의 문제도 확대될 위기에 놓여 있다. 이것이 단일 세그먼트 환경하에 수용될 경우에는 쉽게 OT 네트워크 내부로 바이러스를 확산시키는 것이 가능하다. 'OT는 폐쇄형 공장 네트워크이기 때문에 안전하다.'라는 인식은 과거의 공장 시큐리티 인시던트 사례가 보여주듯이 착각이다. 제조업 DX 추진에 앞서 IT 인프라 혁신을 검토할 때, OT계 내부에서 상호 통신하는 요건의 단말에 대한 네트워크 분할(Zoning) 등을 아울러 검토해야 한다.

4. 오동작에 의한 멀웨어를 침투시키지 않기 위해서

독립 행정법인 정보처리 추진기구(IPA)의 '정보 보안 10대 위협 2021'에 따르면 '조직'에 위협이 되는 1위가 '랜섬웨어로 인한 피해', 2위가 '표적형 공격으로 인한 기밀 정보 착취'였다. 이들의 공격 수법은 사내 관계자에게 바이러스를 심은 메일을 열게 만들어 해당 단말을 감염시키거나 또는 표적 조직이 자주 이용하는 사이트를 조사한 다음 조작하여 부정한 사이트로 유도함으로써 해당 PC를 멀웨어에 감염시키는 것이다. 모두 사람을 방심시킨 뒤 멀웨어가 '침입'하도록 준비해둔 것이다. 지금도 인터넷 액세스 가능한 환경과 의도하지 않은 사람의 오퍼레이션 조합으로 인해 랜섬웨어의 피해는 그칠 줄을 모른다.

앞서 제조업 DX 추진을 위해 인터넷 접

그림7 OT계에 넣으면 안되는 메일・브라우징 환경



속점을 전용으로 마련하는 것에 대해서 언급했지만, 범용 OS 단말에 따라 브라우징이나 전자 메일을 수신하는 환경을 OT 네트워크 내에 구축해서는 안 된다(그림 7).

업무 메일인 것처럼 교묘하게 수신된 첨부 파일에 멀웨어가 들어있을 가능성을 생각하면, 취약성을 없앨 수 없는 OT 네트워크에 멀웨어가 침입할 가능성이 있는 단말 환경을 준비해서는 안 된다. '편리하니까'와 같은 감정에 휩쓸리지 않기 위해서도 정보 보안 기준에 이러한 사항도 명시해 두어야 한다.

5. 제조업 DX 추진을 위한 IT 인프라 개혁을 위해서

앞에서 고가용성을 요구하는 OT계 네트워크 고유의 사정으로 인해 OT계 네트워크・관리부서가 분리되고 정보 보안 기준을 포함한 삼자 견제 구조가 제조업 DX의 큰 저해 요인임을 밝혔다. 만약 당신이 자사 공장의 DX가 도무지 진척을 보이지 않는다는 생각이 든다면 DX 추진 핵심 부서에 이 질문을 던져보길 바란다.

"공장의 각종 데이터를 클라우드로 송신 가능한가요?"

만약, "NO." 혹은 "모르겠다."라는 답이 돌아왔다면 기존의 '폐쇄형 공장 네트워크

상식'에 사로잡혀 있을 가능성이 크다. 경영 전략상 DX 추진이 필요하다고 느낀다면 먼저 눈앞의 IT 인프라 구조 재검토의 신호탄을 쏘아 올리기 바란다. IT 인프라 개혁을 단행하여 분석에 필요한 데이터가 클라우드의 분석 기반에 도달할 수 있다면, 생산 기술 · 생산 전략 담당이 본래 원했던 클라우드 환경에서의 데이터 해석도 시작될 것이다. 제조업에서 DX의 추진으로 인해 선진적인 제조 프로세스가 생성된다면, 사람에게 의존하지 않고도 효율적이며 고품질인 생산을 실현할 수 있을 것이다.

－참고문헌－

1 경제산업성 '2019년도 제조 기반 기술 진흥 시책 제201회 국회(상회) 제출'

https://www.meti.go.jp/reprot/whitepaper/mono/2020/honbun_pdf/pdf/all.pdf

2 독립 행정법인 정보처리 추진기구 시큐리티 센터

'정보 시큐리티 10대 위협 2021'

https://www.ipa.go.jp/files/000088835.pdf

필자소개

사쿠라이 노조무(櫻井 望)
NRI 시스템 테크노 기반시스템 사업부 총괄
전문 분야는 제조업 DX 추진 지원, IT 인프라 보안 진단 등

본 기사는 知的資産創造 2021年 8月号에서 발췌하여 한국어로 번역하였습니다.

문의사항은 노무라종합연구소 서울로 연락 바랍니다.

문의처: inquiry@nri-seoul.com

홈페이지 www.nri-seoul.com의 insight메뉴에서 더 많은 기사를 볼 수 있습니다.

또한, 知的資産創造 2021年 8月号에 대한 전문 및 기사(일본어)는 www.nri.com에서 열람 가능합니다.