본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

2013년 3월 8일 9시 갱신

중소 공급자를 위한 실천적 ISO26262 도입 (2)

추진 조직 설립의 착실한 "준비"가 ISO26262 대응 활동의 형해화*를 막는다

형해화*: 형태만 남기고 실질적인 권한은 없게 하는 것. 앙상한 모습처럼 부실해 짐.

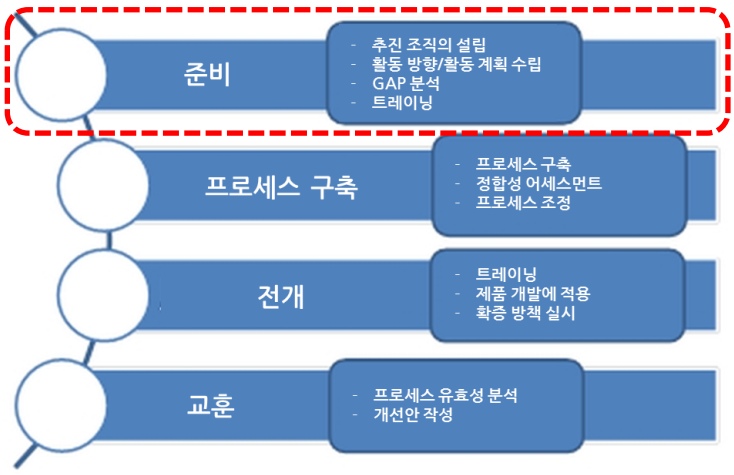
중소 공급자를 대상으로, ISO 26262를 실시하는 데 있어서 실천적인 시책에 대해서 소개하는 본 연재, 제 2회는, 기능안전 대응의 추진 역할이 정해진 후의 "준비"에 대해서 해설한다.

글: DNV 비즈니스 • 어슈어런스 • 재팬기능안전부팀 | 출처: MONOist

번역: 이채원 • 카이젠컨설팅

저번 회에서는, 자동차 전용 기능안전 규격인 ISO 26262 대응을 위한 활동을 시작하기 전에 이해해 두어야 할 "리스크"나, 규격의 대상 범위, 추진 역할의 결정 등에 대해서 설명했습니다.

이번 회는, 기능안전 대응의 추진 역할이 정해진 후의 "준비" 작업에 대해서 해설하고자 합니다.



ISO 26262 대응에 맞춘 일반적인 흐름

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

2013년 3월 8일 9시 갱신

추진 조직의 설립

추진 역할이 정해지면, 그 담당자는 드디어 본격적으로 사내의 기능안전 대응 활동을 개시합니다. 이 때, 주로 관리층에게 주의 바라는 점이 몇 가지 있습니다.

추진자에게 권한 부여

먼저, 추진 역할 수행을 위한 직급 선정, 권한을 명확하게 하고, 사내에 알리는 것입니다. ISO 26262의 Part2 (기능안전의 관리)에는 “5.4.2 안전 문화” 라는 항목이 있고, 그 중에서 “5.4.2.8 조직은 안전 활동을 실행 또는 지원하는 사람이 그 책임과 역할을 다하기에 충분한 권한이 있는 것을 보증해야 한다” 라는 요구가 있습니다.

ISO 26262가 제품 개발 라이프사이클 전체를 망라한 대규모 규격인 것은 저번 회에서도 말했습니다. 이 때문에, 기능안전의 추진 역할은, 많은 조직이나 부서, 담당자와의 협상, 조정이 필요하게 됩니다. 이 때, 추진 담당자의 사내의 위상과 권한이 애매한 상태에서는 각 부서와의 조정이 난항을 겪을 것이며, 효과적인 대응책을 마련할 수 없게 될 우려가 있습니다. 최악의 상황으로, 개발 현장과의 충돌, 의식의 괴리가 일어나, 결과적으로 현재 상황을 감안하지 않는 형해화한 활동이 되어버릴 수 있습니다.

일반적으로 추진 역할은, 규격을 이해하고 요구 내용을 사내 프로세스로 파고드는, 다시 말해, 기술적인 활동이 중심인 것처럼 여겨지기 마련입니다. 하지만 현실은, 사내 각 부서와의 조정, 부서간의 이해 득실의 정리 같은 조정 업무에 많은 시간이나 노력을 소비하게 됩니다.

이러한 부담을 조금이라도 줄이기 위해서, 추진 역할의 “권한”을 명확하게 하고, 그 후에 경영진의 지원이 있는 것을 명확하게 내세워 줄[*1)] 필요가 있습니다.

*1) 기능안전 활동의 킥오프 회의 등에서 전사적으로 공지하는 것이 일반적입니다.

동시에, 각 관련 부서의 역할이나 의사 결정자가 누구인가 라는 인터페이스를 명확히 할 필요도 있습니다. 이것이 추진 역할의 고립화를 막고, 기능안전 활동을 효과적 및 원활하게 진행시키기 위해 도움이 될 것입니다. 추진 역할자가 열정적으로 움직이는가 여부가, 이 활동의 성패에 달려 있음을 알아주시기 바랍니다.

추진을 위한 리소스 확보

다음으로, 필요한 리소스, 특히 인적 리소스를 추진 조직에 할당하는 것입니다. 추진에 필요한 권한이 부여되었다고 하더라도, 그것을 수행하기 위한 리소스가 없으면 의미가 없습니다. 이에 대해서도, ISO 26262의 Part2 (기능안전의 관리), “5.4.2 안전 문화” 중에서 “5.4.2.6 조직은 기능안전 달성에 필요한

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

리소스를 제공해야 한다" 라는 요구가 있습니다.

여기서 말하는 리소스에는, 인적 리소스뿐만 아니라, 개발 지원 툴 등도 포함되어 있습니다. 하지만, 실제로 가장 어려운 것이 인적 리소스의 확보이지 않을까요. 국내 기업에서는, 기능안전 활동은 외압(유럽에서)에 의해서 체결된 "쓸데없는 작업"이며, "본업은 아니다" 라고 인식되어 버리는 일이 있습니다. 하지만, 기능안전 활동은 안전에 관련한 제품에 대해서는, 분명히 쓸데없는 작업이 아니라 제품 개발 프로세스 그 자체입니다. "확증 방안 (Confirmation Measure)"*2) 등의 생소한 작업 요구가 추가되고 있긴 합니다만, 이들은 선행한 타 분야에서 얻은 지식과 의견이 반영된 결과이며, 안전한 제품을 만들기 위한 노하우 (방법)로 여기고 긍정적으로 추진해야 하죠. 먼저, "쓸데없는 작업" 이라는 인식을 완전히 제거하는 것이 시작의 대 전제가 됩니다.

*2) 안전 확보에 대한 비용이나 납기에서 압력을 받지 않는, 객관적인 시점에서 확인한다 (안전을 확인한다)라는 사고 방식이나, 단면을 다양한 측면 (성과물 관점, 프로세스 관점)에서 확인한다 라는 사고 방식은, 안전이 필수 시스템인 세계에서는 정착한 사고 방식입니다.

하지만, 만일 "쓸데없는 작업" 이라는 인식을 없앴다고 하더라도, 기능안전 활동에 필요 및 충분한 인적 리소스를 확보하는 것은 매우 어려운 것이 현실이죠. 그래서 활동의 정리, 의사 결정 등의 중요한 업무는 추진 조직에서 행하고, 경우에 따라서, 그것 이외의 업무에 외부 리소스를 활용하게 되는 것입니다.

추진 조직의 출범에서부터, 기능안전을 적용한 제품 개발을 개시하기까지의 작업에서, 양적으로도 질적으로도 큰 부담이 되는 것은, 기능안전에 대응한 프로세스의 구축입니다. 이 작업에 외부 리소스를 활용하는 예는 비교적 많은 것 같습니다. 프로세스를 만든다 라는 작업은, 규격을 이해한 전문가가 대응하는 쪽이 효율 면에서 유리한 것은 분명합니다. 하지만, 완전히 떠맡겨 버리면, 구축된 프로세스가 개발 현장의 현실과 동떨어져 버리는, 설령 규격에 적합한 훌륭한 것이라고 하더라도, 좀처럼 현장에는 어울리지 않습니다. "부처 만들고 혼을 안 넣다(중요한 것을 빼먹다)"라는 것 이겠죠?

이러한 사태를 피하기 위해서는, 외부 리소스를 활용할 때에는, 이상과 현실 (사내 사정)을 이해하는 사내 경험자의 깊은 관여가 전제되는 것에 주의해야 합니다.

활동 방침・활동 계획의 수립

추진 조직이 설립되면, 가장 먼저 해야 하는 일은 활동 방침 및 전략, 활동 계획의 수립입니다. 활동 계획이라고 하더라도 큰 것은 아니고, 예를 들어 현재의 목표를 향해 큰 틀의 절차나 전략을 정해 놓는 것입니다. 다음은, 이 계획을 수립할 때, 최소한으로 필요한 것을 3 가지의 항목으로 나누어 둡니다.

(1) 바탕이 되는 프로세스의 결정

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

바탕이 되는 프로세스란, 기능안전 활동을 추가 정의할 경우의 근거가 되는 프로세스로, 이미 많은 기업에서 도입되고 있는 품질 경영 프로세스*3) 를 기초로 하는 예가 많습니다. 품질・신뢰성 관련한 업무에 종사해 온 사람이라면 매우 친숙한 프로세스일 것이며, 만일 추진 회사에 "품질관리 시스템"이 존재하고 있다면, 기능안전 규격의 전제인 근거가 되는 프로세스로써 적합합니다. 단지, 이들의 규격은 조직적 측면에서의 관리 규격이기 때문에, ISO 26262의 Part2 (기능안전의 관리)나 Part8 (지원 프로세스) 등의 관리 프로세스와의 궁합은 좋습니다만, Part4 (시스템), Part5 (하드웨어), Part6 (소프트웨어) 등의 엔지니어링 프로세스에 대해서는, 상응하는 연구가 필요하게 되겠죠.

*3) ISO9001이나 TS16949 등의 규격에 대응한 관리 매니지먼트 프로세스.

한편, 소프트웨어 개발을 중시해 온 기업에서는, CMU/SEI*4) 의 CMMI (Capability Maturity Model Integration)나, 유럽의 자동차 산업이 추진하고 있는 Automotive SPICE 등에 대응한 프로세스를 운용하고 있는 경우도 많고, 이들의 프로세스 자산을 바탕으로 한 예도 많습니다. 유럽의 경우, 이전부터 소프트웨어에의 대처에 적극적이었던 Robert Bosch는 CMMI 기초 프로세스에서, Automotive SPICE의 추진・보급에 열심인 Continental은 Automotive SPICE 기초 프로세스에서 기능안전 프로세스를 구축한 것과 같이, 지금까지의 자사의 활동 자산이나 경험을 어떻게 살리는가 라는 관점에서 프로세스 구축 전략이 정해져 있는 것 같습니다.

*4) Carnegie Mellon University | Software Engineering Institute

특히, Automotive SPICE는 유럽에서는 넓게 보급되고 있어, ISO 26262와 중복되는 요구 (표1)도 많고, 기능안전에 임할 때 기초 프로세스로써는 가장 적합할지도 모릅니다. 이 점에 주목해, Automotive SPICE에 대응해서 기능안전 확장한 통합 SPICE를 책정하는 움직임도 활발화*5) 하고 있습니다.

*5) 대표적인 것이 SS7740 이라는 스웨덴 규격입니다. Automotive SPICE에 ISO26262의 요구를 추가한 통합판 SPICE가 나왔습니다. 국내에서도, 일본 SPICE 네트워크 유지 멤버들을 통해, 기능안전 확장의 검토가 진행되고 있습니다.

ISO26262의 요구		Automotive SPICE	
Part2	기능안전의 관리	SUP.9	문제 해결 관리
		MAN.3	프로젝트 관리
		SUP.1	품질 관리
Part4	시스템 레벨에 있어서 제품개발	ENG.1	요건 추출
		ENG.2	시스템 요건분석
		ENG.3	시스템 아키텍처 설계
		ENG.9	시스템 통합테스트
Part6	소프트웨어 레벨에 있어서 제품개발	MAN.3	프로젝트 관리
		ENG.4	소프트웨어 요건분석
		ENG.5	소프트웨어 설계

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

		ENG.6	소프트웨어 구축
		ENG.7	소프트웨어 통합테스트
		ENG.8	소프트웨어 테스트
Part8	지원 프로세스	ACQ	조달관련 프로세스
		SUP.8	구성관리
		SUP.10	변경관리
		SUP.2	검증
		SUP.7	문서화

표1 ISO 26262와 Automotive SPICE의 관계

(2) 기능안전 활동의 역할 분담

ISO 26262에는, “안전관리자” 라고 불리는 제품 개발에서 기능안전 활동에 대한 책임을 갖는 역할이 있습니다. 업무 내용으로는 프로젝트 매니지먼트에 가깝기 때문에, 프로젝트 관리자가 안전관리자를 겸임할 수 있습니다. 하지만, 직접적으로 비용 절감이나 납기 준수의 압력을 받는 프로젝트 관리자가, 안전을 최우선 하는 책임을 져야 하는 안전 관리자의 업무를 겸임하는 것에 의한 폐해는 충분히 고려되어야 하겠죠.

안전관리자의 법적 책임

매년 유럽에서는 VDA QMC가 주최하고 있는 VDA Automotive SYS Conference라는 국제 회의가 있습니다. 작년에(2012년)도 독일의 베를린에서 개최되어, 기능안전의 화제도 많이 다루어졌었습니다. 이 회의에서, 법률가와 함께한 워크숍이 행해져, 법적인 측면에서 본 “안전관리자”의 책임에 대해서 활발한 논의가 행해졌었습니다. 과거의 판례를 근거로 한 논의였기 때문에 일률적으로 안전관리자의 책임이 어디까지 미치는가를 정의하는 것은 어렵습니다만, 어쨌든 만약 개발한 제품에 안전상의 결함이 발견되어, 그 문제가 법정에 반입되는 사태가 벌어지면, 어떠한 형태로 안전관리자가 휘말리는 것은 피할 수 없을 것 같습니다.

기능안전 활동은, 안전관리자 이외에도 “확증 review”를 실시하는 “reviewer”, “기능안전 감사”를 실시하는 “감사인”, “기능안전 평가”를 실시하는 “평가자” 라는, 확증 방책이라고 불리는 제품 개발의 각 단계에서 중요한 업무를 담당하는 전문가가 필요하게 됩니다.

안전관리자의 책임은, 안전상의 책임을 진다는 점을 제외하면 지금까지의 프로젝트 관리 업무에 가까운 역할인 것은 앞에서 말했습니다.

한편, 확증 review나 기능안전 감사, 기능안전 평가 (표2)라는 새로운 역할에 대해서는, 어느 경험을 쌓은 사람이 적합한지, 어느 능력이 필요한지, 향후 어느 기술을 몸에 익혀야 하는지 등등, 많은 조직이 고민하고 있는 과제입니다. 이 점은, 다음에 말하는 조직 구조의 과제와 함께 규격 요구의 의도를 충분

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

히 이해한 다음에 신중히 검토해야 하겠죠.

토픽	확증 리뷰	기능 안전 감사	기능 안전 평가
대상	성과물	프로세스	아이템(제품)
평가의 관점	대상 성과물의 ISO 26262 준거	대상 프로세스의 준수	아이템 (제품)의 기능 안전의 달성

표2 확증 방책의 개요 (ISO 26262 Part2 에서 일부 발췌하여 인용)

(3) 기능안전 활동의 조직 구조 (독립성의 확보)

이러한 확증 방안은, 개발하는 제품의 안전도 수준 (ASIL: Automotive Safety Integrity Level)이나 확증 방안의 대상이 되는 것에 따라, 요구되는 독립성이 바뀝니다. 가장 엄격한 안전 레벨을 요구하는 ASIL D의 제품에서는, 많은 확증 방안이 개발을 담당한 조직과는 다른 계통의 조직에서 실시되는 것을 요구하고 있습니다. 즉, 기능안전의 새로운 책임 및 역할에 대해서는 어떠한 능력을 가진 사람이 실행하는가를 검토할 뿐만 아니라, 이러한 활동이 높은 독립성을 유지하는 데는 어떠한 조직이 필요한가, 어떠한 지시에 따라야 하는가 라는 조직적 측면의 검토도 필요하게 됩니다.

확증 방안의 목표는, 아래에 나타낸 2가지라고 볼 수 있습니다.

- 객관적인 관점 및 다양한 측면 (성과물 측면 및 프로세스 측면)에서 확인하는 것으로, 개발 당사자가 간과해버리는 것을 발견한다.
- 발견된 안전상의 누락이, 비즈니스상의 압력 (비용이나 납입 기한)을 받지 않고 확실히 받아들여져 해결된다.

어떤 사람을 기능안전 활동에 할당하는가, 어떤 조직을 만드는가, 그 조직이 어떤 기능을 갖게 하는가 라는 과제는, 각각의 회사 사정에 맞춰 연구하는 수 밖에 없습니다. 하지만, 어느 대응책이건 이 규격이 요구하는 활동의 목적을 이해한 대응책이 아니면 안됩니다. 그렇지 않으면, 형식상으로는 규격 요구를 만족시키고 있지만, 활동 자체에서는 아무런 효과도 없이 규격 준거를 위한 단순한 알리바이 조작이라는 사태가 될 수 있습니다.

예를 들어, 확증 방안이 형식적인 검사밖에 이루어지지 않아, 안전상의 누락을 발견하는 것은 거의 있을 수 없는 일 이라는 사태(상황)가 발생하면, 검증을 실행하는 조직에서도, 검증을 받는 조직에서도 불행한 일입니다.

중요한 것은, 제품 개발 중에서 행해지는 수많은 검증 활동을 누락하지 않고 안전상의 결함을 어떻게 발견하는가 라는 점입니다. 그 때문에 대응책을, 조직의 특징과 강점을 살려 활동하는 것이야 말로, 실질적인 성과를 내는 지름길 입니다.

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

확증 방안의 보충

우주 개발 분야에서는, 자본적으로 독립한 조직이 실시하는 IV&V (Independent Verification & Validation)이라는 활동이 있습니다. 국제 우주 정거장의 개발 시에 NASA의 제안으로 JAXA (당시는 NASDA)가 도입되어, 적용되고 있습니다. 이 활동은, 바로 독립한 조직이 객관적인 입장에서 제품 (성과물)에 대한 평가를 필요에 의해 고도의 기술 (위험 분석이나 형식 검증 등)을 구사하여 실시합니다. 현재, IV&V 활동은, 유인 우주 시스템 사가 담당하고 있어, 많은 우주기 개발 속에서 적용되고 있습니다. 이 예는, 평가 전문가로 독자적인 기술을 갖고 있는 예 입니다. 확증 방안을 생각하며 제품 성향의 지식과 경험을 중시하는 회사도 있습니다만, 이 우주 분야의 예와 같이 객관적인 관점에서 평가 노하우를 중시하는 사고 방식도 있습니다. 물론, 어느 쪽이 옳고 어느 쪽이 그르다고 할 수는 없어서 회사의 사정, 방침 등을 고려하여 정한다면 좋을 것이라고 생각합니다.

GAP 분석

GAP (갭) 분석은, 현재의 프로세스가 ISO 26262의 요구를 어느 정도 만족시키고 있는가, 무엇을 만족하지 못하였나 라는 프로세스 간의 gap을 명백히 하는 작업입니다. 본 기사에서는, 계획 수립 후에 실시하는 흐름입니다만, 현재 상태가, 많은 경우 기능안전 요구에 대응하는 프로세스가 거의 없는 것을 이미 알고 있다 라는 이유로 gap분석을 실시하지 않는 경우도 많습니다. 오히려, 프로세스 정의를 진행시키면서, 그 때마다 규격과의 적합성을 판별하여 방향성을 확인해 가는, 말하자면 달리면서 돌아보는 듯한 접근 방식이 늘고 있습니다.

또, 최근에는 이미 기능안전 대응을 의무화한 제품 개발도 시작되고, 거기서 개발된 작업 성과물 (예를 들어 기술안전 요구나 시스템 설계서 등)이 규격에 적합해 있는가를 확인하는 “확증 리뷰”에 가까운 작업 의뢰도 늘고 있습니다.

프로세스를 구축하는 작업에 실제 제품 개발 프로젝트를 어떻게 관련 지을 지는, 기업마다의 전략・계획에 의존하므로 거기에 맞춰 GAP 분석이나 적합성 평가를 계획하는 것이 좋겠죠. 적합성 평가에 대해서는 “프로세스 구축” 연재 시 이야기하고자 합니다.

트레이닝

기능안전의 트레이닝은, 기능안전 활동에 종사하는 사람을 대상으로 대응의 지식을 심어주기 위해 실시하는 케이스로, ISO 26262의 Part2 (기능안전의 관리), “5.4.3 능력 관리” 속에 있는 “5.4.3.1 조직은 안전 라이프사이클에 관련한 사람들이, 그 책임과 역할에 대응할 충분한 레벨의 기능, 능력 및 자격을 갖춘 것을 보증해야 한다”라는 요구, 즉 자격 부여를 위해 실시하여야 합니다. 표 3은, 자격 부여를 전제로 한 트레이닝 코스의 예입니다. (DNV 비즈니스 어슈어런스 재팬의 경우).

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

코스	기간
기능안전 엔지니어 코스	2~3일간
안전관리자 코스	5일간
기능안전 어세서 코스	5일간
HW엔지니어 코스	1일간
SW엔지니어 코스	1일간

표3 트레이닝 코스의 예

안전관리자(전)용이나 기능안전 어세서(전)용의 트레이닝은, 대개 5일간 정도로 실시하는 것이 일반적입니다. 참가자의 다수는, 본업인 “제품 개발”에 종사하고 있기 때문에 5일간에 걸쳐 진행하는 것은 개발 현장에 큰 영향을 줄 가능성이 있습니다. 이른 단계부터 충분한 사전 교섭이 필요하겠죠.

이러한 “능력 관리”나 “교육 프로그램”에 의한 자격 부여라는 접근은, 엔지니어를 희망하는 사람이 많은 유럽과 미국의 사회 환경이 배경인 사고 방식으로, 일상 업무 속에서의 육성을 중시하는 일본적인 사고 방식으로 보면 위화감을 갖는 사람도 많을 것입니다. 이러한 사고 방식이 과연 일본 기업에도 큰 혜택이 있는가 생각해보면, 필자 자신도 의문을 품습니다. 하지만, 국제적인 대책이라고 생각하면 받아들이지 않을 수 없는 것이 현실입니다.

이에 대해서는, 일본적인 좋은 프로세스 (육성)를 버리지 않고, 현재의 좋은 방식을 살리면서, 유럽과 미국적인 방식을 도입하여 “일본 고유의 정신과 서양의 학문을 갖춤 (화혼양재)”적인 입장에 서서 임할 필요가 있을지도 모르겠습니다.

원문 | http://monoist.atmarkit.co.jp/mn/articles/1303/08/news012.html

http://monoist.atmarkit.co.jp/mn/articles/1303/08/news012_2.html

http://monoist.atmarkit.co.jp/mn/articles/1303/08/news012_3.html