

DX 컨트롤러 보안 가이드라인

△ 안내 (For Reference Only)

본 문서는 AI 번역으로 작성된 참고용 국문자료입니다.
일부 표현은 원문과 다소 다를 수 있으며,
중요한 내용은 원문과 함께 참고해 주시기 바랍니다.

양해 말씀

- 본 자료에는 안전에 관한 주의 사항을 포함하여, 사용 시의 상세 내용에 대해서는 기재하고 있지 않습니다. 반드시 본 자료에서 사용하는 각 기기의 매뉴얼이나 취급설명서를 입수하여, 「안전상의 주의」, 「안전상의 요점」, 「사용상의 주의」 등 안전에 관한 주의 사항을 포함해 내용을 확인한 후 사용하십시오.
- 본 자료 내용의 일부 또는 전부를 오무론 주식회사의 허가 없이 복사, 복제, 전재하는 것을 금지합니다.
- 본 자료의 내용에 관해서는 개량을 위해 예고 없이 사양 등을 변경하는 경우가 있습니다. 미리 양해해 주시기 바랍니다.
- 본 자료의 내용에 관해서는 만전을 기하고 있습니다만, 만일 의심스러운 점이나 오류 등 발견하신 사항이 있으시면 번거로우시겠지만 담당자에게 연락해 주십시오.

상표

- Microsoft, Windows, Excel, Visual Basic, Microsoft Edge는 미국 Microsoft Corporation의 미국 및 그 밖의 국가에서의 등록상표 또는 상표입니다.
- ODVA, CIP, CompoNet, DeviceNet, EtherNet/IP는 ODVA의 상표입니다.
- SpeedBee Synapse는 주식회사 솔티스터의 상표입니다.
- Grafana는 Grafana Labs의 상표입니다.

그 밖에 본문 중에 게재하고 있는 회사명 및 제품명은 각 사의 상표 또는 등록상표입니다.

저작권

- 스크린샷은 마이크로소프트의 허락을 받아 사용하고 있습니다.
- 본 제품에는 서드파티 소프트웨어가 내장되어 있습니다. 이 소프트웨어에 관련된 라이선스와 저작권에 대해서는 <https://www.fa.omron.co.jp/product/tool/dx-info/index.html> 을 참조하십시오.

머리말

본서의 목적

본서는 고객께서 당사 FA 제품의 보안 대응을 이해하시도록 하는 것과, 당사 FA 제품을 이용하시는 고객께서 실시해 주셨으면 하는 보안 대책을 제시하는 것을 목적으로 하며, DX 시리즈 데이터 플로우 컨트롤러를 사용하여 실시할 수 있는 보안 대책을 제시합니다.

FA 시스템 보안 가이드라인 및 관련 매뉴얼과 함께 읽어 주십시오.

대상이 되는 독자 여러분

본서는 보안 대책을 계획, 검토, 실시하시는 다음 분들을 대상으로 기술하고 있습니다.

- 생산 현장의 데이터 활용 시스템을 설계, 운용하시는 분
- 생산 현장의 보안 시스템을 설계, 운용하시는 분

대상이 되는 제품

본서는 다음 제품을 대상으로 하고 있습니다.

- DX 시리즈 데이터 플로우 컨트롤러(이하, 「DX 컨트롤러」라고 기재합니다.)

제품의 사양에 대해서는 제품의 매뉴얼을 참조하십시오.

면책 사항

본서에서의 고객에 대한 권장 사항은 당사가 실시한 분석 및 검토 결과에 근거하고 있습니다. 적절한 보안 대책은 고객의 환경에 따라 다르므로, 해당 권장 사항으로 고객의 환경에
서의 모든 보안 피해의 방지를 보증하는 것은 아닙니다. 본서를 참고하여 고객 자신이 고객의 환경에 맞는 분석
및 적절한 대책을 검토하고 실시해 주십시오.

AI 번역본
-For Reference Only-

AI 번역본
-For Reference Only-

목차 구성

		1
1	DX 컨트롤러의 보안 대책	2
2	DX 컨트롤러의 보안 기능	3
3	보안 패치 적용	4
4	기기의 안전한 폐기	A
A	부록	

AI 번역본
-For Reference Only-

목차

머리말	1
본서의 목적	1
대상이 되는 독자 여러분	1
대상이 되는 제품	1
면책 사항	1
목차 구성	3
관련 가이드라인 · 매뉴얼	6
개정 이력	7

제1 장 DX 컨트롤러의 보안 대책

1-1 DX 컨트롤러의 사용 환경	1-2
1-2 DX 컨트롤러의 기술 계층의 보안 대책	1-3

제2 장 DX 컨트롤러의 보안 기능

2-1 통신 회선상의 데이터 보호	2-2
2-1-1 보안 통신 기능	2-2
2-2 DX 컨트롤러에 대한 부정 접속 방지	2-4
2-2-1 계정 관리(사용자 인증) 기능(DX 컨트롤러)	2-4
2-2-2 USB 포트 관리 기능	2-4
2-3 DX 컨트롤러의 부정 조작 방지	2-6
2-3-1 계정 관리(조작 권한 인증) 기능(DX 컨트롤러)	2-6
2-4 애플리케이션에 대한 부정 접속 방지	2-7
2-4-1 계정 관리(사용자 인증) 기능(애플리케이션)	2-7
2-5 애플리케이션의 부정 조작 방지	2-8
2-5-1 조작 권한 인증 기능(애플리케이션)	2-8
2-6 부인 방지	2-9
2-6-1 로그 기능	2-9

제3 장 보안 패치 적용

3-1 DX 컨트롤러 업데이트	3-2
3-1-1 펌웨어 업데이트 이력	3-2
3-2 PC의 OS 업데이트	3-3
3-3 브라우저 업데이트	3-4

제4 장 기기의 안전한 폐기

4-1 DX 컨트롤러 내의 데이터 소거	4-2
4-1-1 초기화(공장 초기화) 기능	4-2

부록

A-1 본서 및 당사 FA 제품에 관한 문의 A-2

AI 번역본
-For Reference Only-

관련 가이드라인 · 매뉴얼

본서와 관련된 가이드라인 · 매뉴얼은 아래 표와 같습니다. 함께 읽어 주십시오.

문서 명칭	No.	용도
FA 시스템 보안 가이드라인	SBCA-140	FA 시스템 전반에 관련된 보안의 사고방식에 대해 알고 싶을 때.
DX 시리즈 데이터 플로우 컨트롤러 사용자 매뉴얼	SBSB-538	DX 시리즈 데이터 플로우 컨트롤러에 탑재하고 있는 보안 기능과 사용법을 알고 싶을 때.
DX 시리즈 Web UI 조작 매뉴얼	SBSB-539	DX 시리즈 데이터 플로우 컨트롤러에 탑재하고 있는 보안 기능의 설정 방법을 알고 싶을 때.

AI 번역본
-For Reference Only-

개정 이력

개정 기호는 앞표지 · 뒤표지에 기재되어 있는 카탈로그 번호의 끝에 부기됩니다.

카탈로그 번호

SBSB-030A

↑ 개정 기호

개정 기호	개정 연월	개정 이유 · 개정 페이지
A	2025 년9 월	초판

AI 번역본
-For Reference Only-

AI 번역본
-For Reference Only-

DX 컨트롤러의 보안 대책

DX 컨트롤러는 여러 보안 기능에 의해 다층 방어를 실현합니다.
본 장에서는 DX 컨트롤러를 사용하는 환경과 DX 컨트롤러의 보안에 대해
설명합니다.

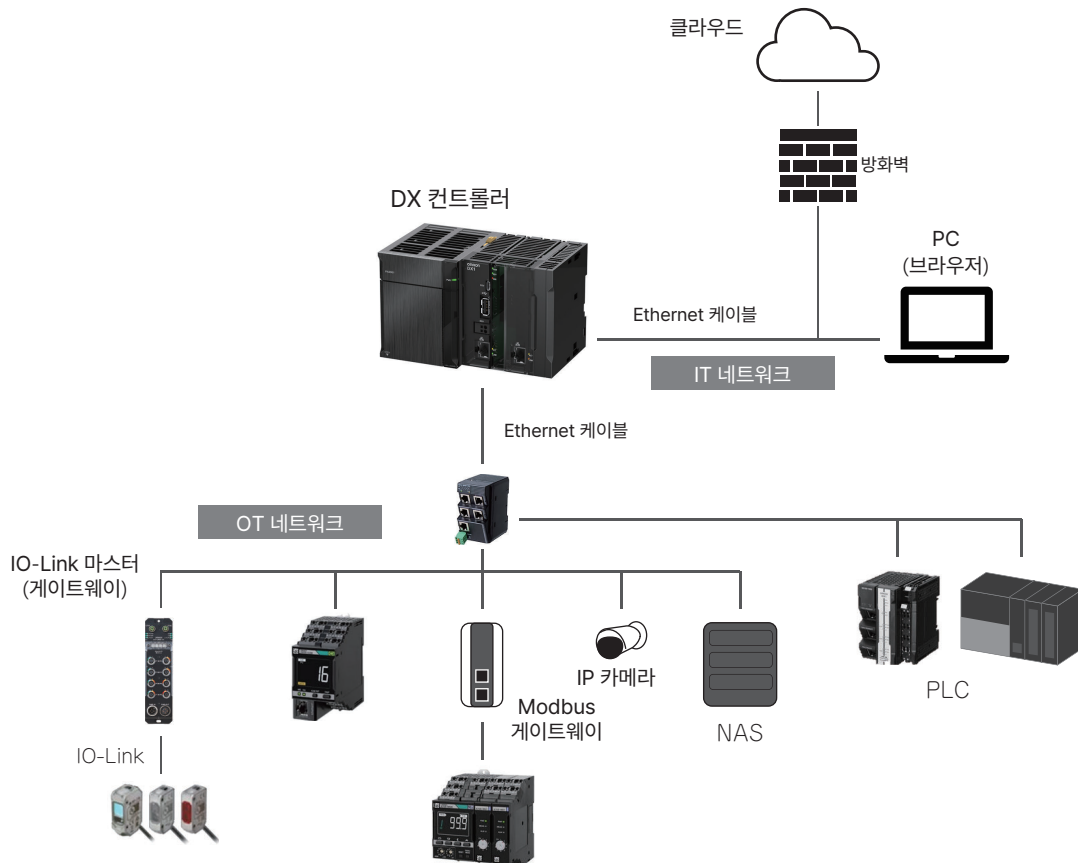
1-1	DX 컨트롤러의 사용 환경.....	1-2
1-2	DX 컨트롤러의 기술 계층의 보안 대책.....	1-3

AI 번역본
-For Reference Only-

1-1 DX 컨트롤러의 사용 환경

DX 컨트롤러는 그 보안 기능을 활용함으로써, 시스템이나 장치의 보안을유지한 채로 데이터의 수집이나 가시화 기능을 추가할 수 있습니다. DX 컨트롤러에서는 장치나 디바이스에서 수집한 데이터를 지키기 위해 부정 접속이나 부정 조작을 방지합니다.

DX 컨트롤러를 사용하는 환경에서는 목적, 위협에 따라 『FA 시스템 보안 가이드라인(SBCA-140)』에 제시된 대책을 조합하여 다층 방어를 강구해 주십시오.



고객께서 실시해 주셨으면 하는 사항

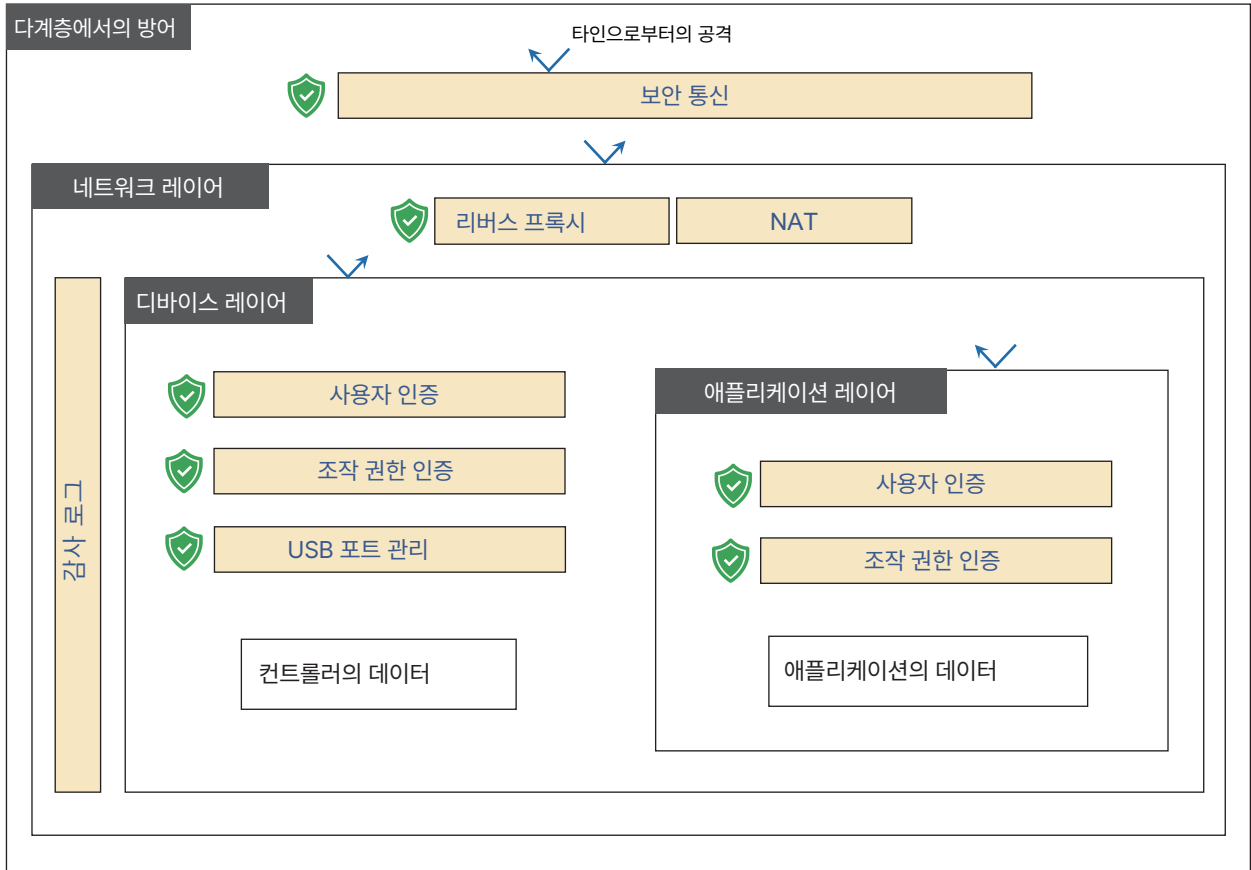
- 장치나 디바이스의 네트워크는 방화벽이나 패킷 필터링을 도입해 주십시오.
- IT 네트워크(PC, 서버, MES 등의 네트워크)와 OT 네트워크(장치, 디바이스의 네트워크)는 분리해 주십시오.
- 다음을 사용하는 경우는 그것들을 안전하게 사용할 수 있는 네트워크 환경에서 운용해 주십시오.
NTP, DNS, mDNS, DHCP
- 장치나 디바이스 자체의 보안 기능을 유효하게 활용해 주십시오.
- 안전한 운용을 하기 위해 시스템이나 장치 / 디바이스, 그리고 DX 컨트롤러의 설치 구역에 대한 출입 관리나 물리적 잠금을 실시해 주십시오.

1-2 DX 컨트롤러의 기술 계층의 보안 대책

DX 컨트롤러는 지켜야 할 데이터에 대해 다층 방어로 보호할 수 있도록 보안 기능을 탑재하고 있습니다.

공격자로부터의 부정 접속이나 부정 조작을 방지함으로써 데이터를 지킬 수 있습니다.

또한 본서에서는 고객께서 특히 대응해 주셨으면 하는 사항을 각 보안 기능의 설명에 제시하고 있습니다. 함께 읽어 보시고 대책을 실시해 주십시오.



AI 번역본
-For Reference Only-

각 계층에서 제공하고 있는 기능을 아래에 제시합니다.

고객께서 설정이나 작업을 해 주셨으면 하는 기능에 대해서는 2 장에서 설명하고 있으므로 참조해 주십시오.

데이터를 지키는 레이어	목적	당사 제품이 탑재하고 있는 기능	본서 참조처
네트워크 레이어	통신 회선상의 데이터 보호	보안 통신 기능	P.2-2
	DX 컨트롤러에 대한 외부로부터의 공격 차단	리버스 프록시 · 애플리케이션의 Web 서버의 IP 주소를 외부로부터 은닉하여, 외부에서 직접 애플리케이션에 액세스하는 것을 방지합니다.	—
		NAT · 데이터 플로우 컨트롤러 내의 IP 주소를 외부로부터 은닉하여, 외부로부터의 공격을 방지합니다.	—
디바이스 레이어	DX 컨트롤러에 대한 부정 접속 방지	계정 관리(사용자 인증) 기능(DX 컨트롤러)	P.2-4
		USB 포트 관리 기능	P.2-4
	DX 컨트롤러의 부정 조작 방지	계정 관리(조작 권한 인증) 기능(DX 컨트롤러)	P.2-6
애플리케이션 레이어	애플리케이션에 대한 부정 접속 방지	계정 관리(사용자 인증) 기능(애플리케이션)	P.2-7
	애플리케이션의 부정 조작 방지	계정 관리(조작 권한 인증) 기능(애플리케이션)	P.2-8
레이어 공통	부인 방지	감사 로그 기능	P.2-9

AI 번역본
-For Reference Only-

DX 컨트롤러의 보안 기능

본 장에서는 DX 컨트롤러가 탑재하고 있는 보안 기능에 대해 설명합니다.

2-1	통신 회선상의 데이터 보호.....	2-2
2-1-1	보안 통신 기능.....	2-2
2-2	DX 컨트롤러에 대한 부정 접속 방지.....	2-4
2-2-1	계정 관리(사용자 인증) 기능(DX 컨트롤러).....	2-4
2-2-2	USB 포트 관리 기능.....	2-4
2-3	DX 컨트롤러의 부정 조작 방지.....	2-6
2-3-1	계정 관리(조작 권한 인증) 기능(DX 컨트롤러).....	2-6
2-4	애플리케이션에 대한 부정 접속 방지.....	2-7
2-4-1	계정 관리(사용자 인증) 기능(애플리케이션).....	2-7
2-5	애플리케이션의 부정 조작 방지.....	2-8
2-5-1	조작 권한 인증 기능(애플리케이션).....	2-8
2-6	부인 방지.....	2-9
2-6-1	로그 기능.....	2-9

AI 번역본
-For Reference Only-

2-1 통신 회선상의 데이터 보호

인터넷에 접속하는 장치에서는 네트워크를 통해 사이버 공격을 받을 리스크가 있습니다. 통신 회선을 흐르는 데이터로부터의 정보 누설이나 변조, 서비스 방해를 방지합니다.

2-1-1 보안 통신 기능

보안 통신은 DX 컨트롤러와 그 밖의 기기나 시스템 사이의 통신 보안 향상을 목적으로 한 기능입니다. 통신

데이터를 암호화하고 또한 해시값을 붙여 송수신을 실시하므로, 제3자에 의한 통신 데이터의 도청이나 변조를 방지하는 데 도움이 됩니다.

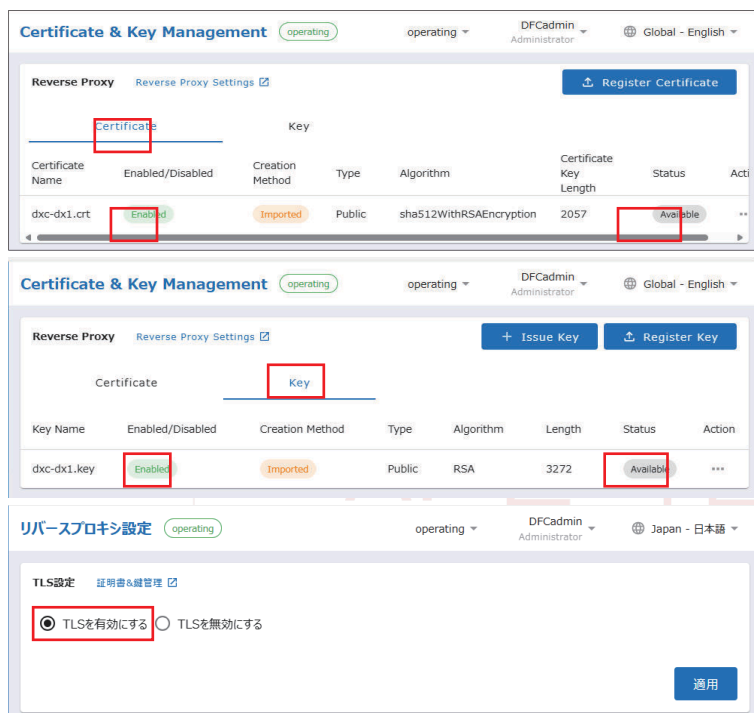
DX 컨트롤러는 다음 기기와의 사이에서 보안 통신을 이용할 수 있습니다.

- 브라우저(PC)
- 다른 DX 컨트롤러

브라우저(PC)와의 사이의 보안 통신을 설정하는 순서에 대해서는 『 DX 시리즈 CPU 유닛 사용자 매뉴얼(SBSB-538) 』을 참조해 주십시오.

또한 설정이 다음과 같이 되어 있으면 브라우저(PC)와의 사이의 보안 통신이 가능합니다.

- 인증서와 키가 등록되어 있고, 각각에서 [유효/무효] 가 [유효] , [스테이터스] 가 [Available] 로 되어 있다.
- [TLS 설정] 에서 [TLS를 유효로 한다] 에 체크가 들어가 있다.



DX 컨트롤러끼리의 사이에서 보안 통신을 설정하는 순서에 대해서는 『 DX 시리즈 사용자 매뉴얼(공장 감시 패키지판)(SGTE-731) 』을 참조해 주십시오.

대책할 수 있는 위협

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
○	○		○	○	

고객께서 실시해 주셨으면 하는 사항

- 보안성 향상을 위해 지원 기한 내의 OS를 사용하는 PC나 디바이스를 사용해 주십시오.
- 제어 시스템이나 장치의 네트워크는 방화벽(미사용 통신 포트의 차단, 통신 호스트의 제한)을 도입하고, IT 네트워크로부터의 분리를 실시하며, PC의 DX 컨트롤러에 대한 접속은 방화벽 내에서 이루어지도록 해 주십시오.
- NTP, DHCP, DNS 서버는 신용할 수 있는 내부 네트워크 내에 배치하고, 서버의 보안 대책을 강구해 주십시오.
- 애플리케이션의 기능을 사용하여 다른 기기와 통신을 실시할 때, 암호화 통신의 설정이 있는 경우는 암호화 통신을 사용할 것을 권장합니다.
예를 들어 SpeedBee Synapse의 컴포넌트 중에는 암호화 통신을 설정할 수 있는 것이 있습니다. 컴포넌트에 대해서는 『DX 시리즈 SpeedBee Synapse 사용자 매뉴얼 (SBSB-540)』을 참조해 주십시오. 암호화 통신이 가능한 컴포넌트에 대해서는 암호화 기능이 설명되어 있습니다.
암호화 통신이 불가능한 경우는 안전한 운용을 하기 위해 시스템이나 장치 / 디바이스, 그리고 DX 컨트롤러의 설치 구역에 대한 출입 관리나 물리적 잠금을 실시해 주십시오.
- 보안 통신에 관한 서버 인증서 / 비밀키의 제3자에 의한 도난, 정보 누설, 변조에 의해 데이터의 부정 취득, 데이터의 변조, 통신 불가 등 보안상의 문제가 될 가능성이 있습니다. 고객 자신이 인증서, 비밀키의 관리와 도난, 정보 누설, 변조 방지 대책의 충분한 조치를 강구해 주십시오. 특히 비밀키를 취득하는 경우에는 암호화된 안전한 통신 경로를 사용하는 등 정보 누설이 되지 않도록 해 주십시오. 또한 비밀키의 관리에서는 유출될 가능성을 극력 배제한 장소에 보관하는 등의 조치를 해 주십시오.

AI 번역본
-For Reference Only-

2-2 DX 컨트롤러에 대한 부정 접속 방지

고객의 소중한 생산 정보 데이터를 도용이나 부정 이용으로부터 지키기 위해, 쉽게 DX 컨트롤러에 액세스할 수 없도록 DX 컨트롤러 접속 시에 인증하는 기능을 사용합니다.

2-2-1 계정 관리(사용자 인증) 기능(DX 컨트롤러)

온라인 접속 시에 사용자명과 패스워드에 의한 사용자 인증을 실시하여, 온라인 조작하는 사용자를 특정합니다.

사용자 인증 기능은 DX 컨트롤러를 조작하는 사용자를 미리 DX 컨트롤러에 등록해 두고, DX 컨트롤러를 온라인 조작하는 사용자를 특정하는 기능입니다. DX 컨트롤러에 온라인 접속할 때 사용자명과 패스워드의 입력이 요구됩니다. 사용자명 및 패스워드가 미리 설정된 것과 일치하지 않으면 온라인 접속할 수 없습니다.

또한 각 사용자에게는 관리자, 설계자, 또는 보전자 중 하나의 롤을 할당합니다. 이에 따라 각 사용자가 자신에게 할당된 롤의 권한 범위에서만 DX 컨트롤러에 대한 온라인 조작을 할 수 있도록 합니다.

사용자명, 패스워드, 그리고 해당 사용자의 롤 정보 등의 사용자 인증 설정은 DX 컨트롤러에 저장됩니다. 따라서 다른 PC에서 DX 컨트롤러에 접속해도 사용자 인증 기능을 사용할 수 있습니다.

대책할 수 있는 위험

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
○	○	○	○	○	○

사용자 인증 기능에서는 PC에서 DX 컨트롤러의 Web UI에 온라인 접속할 때 사용자명과 패스워드를 입력하면, 할당되어 있는 롤의 권한 범위에서 DX 컨트롤러를 조작할 수 있게됩니다. 조작 방법의 자세한 내용은 『DX 시리즈 Web UI 조작 매뉴얼(SBSB-539)』을 참조해 주십시오.

고객께서 실시해 주셨으면 하는 사항

- 초기 등록되어 있는 사용자 계정은 무효화해 주십시오.
- 패스워드는 고객 자신이 정기적으로 변경해 주십시오.
- 브루트포스 공격 등에 의한 패스워드 해석이 상정되므로, 복잡한 패스워드(8 문자 이상, 복수의 문자 종별)를 설정해 주십시오.
- DX 컨트롤러에서는 외부 시스템에서 DX 컨트롤러에 액세스하기 위한 사용자별 액세스 토큰(인증 키)을 생성할 수 있습니다. 액세스 토큰은 제3자에게 알려지지 않도록 엄중히 관리해 주십시오.

2-2-2 USB 포트 관리 기능

DX 컨트롤러의 USB 포트를 사용하지 않는 경우에, USB 포트를 사용할 수 있는 상태로 두면 USB 포트에서 DX 컨트롤러에 액세스될 위험성이 있습니다. USB 포트를 사용하지 않는 경우는 USB 포트를 무효화해 둬으로써, 제3자가 USB 포트에서 DX 컨트롤러에 액세스할 수 없도록 합니다.

USB 포트의 무효화 방법에 대해서는 『 DX 시리즈 Web UI 조작 매뉴얼(SBSB-539) 』의 USB 포트 관리 설명을 참조해 주십시오.

대책할 수 있는 위협

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
	○		○	○	

AI 번역본
-For Reference Only-

2-3 DX 컨트롤러의 부정 조작 방지

DX 컨트롤러의 부정 조작을 방지하여, 고객의 소중한 생산 정보 데이터의 도용이나 부정 이용, 그리고 시스템의 이상을 방지합니다.

고객께서 실시해 주셨으면 하는 사항

- 안전한 운용을 하기 위해 시스템이나 장치 / 디바이스, 그리고 DX 컨트롤러의 설치 구역에 대한 출입 관리나 물리적 잠금을 실시해 주십시오.

2-3-1 계정 관리(조작 권한 인증) 기능(DX 컨트롤러)

DX 컨트롤러의 데이터를 변경하는 경우, 조작 실수에 의해 데이터의 수집이나 활용이 올바르게 이루어지지 않는 등의 피해를 줄 위험성이 있습니다. 조작자에게 부여하는 룰에 의해 조작할 수 있는 기능을 제한하여, 조작 실수를 방지합니다.

조작 권한 인증 기능을 사용하여, 관리자가 조작자마다 역할에 따른 룰을 설정함으로써 운용합니다.

대책할 수 있는 위협

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
	○		○	○	○

조작 권한 인증 기능의 설정은 『DX 시리즈 Web UI 조작 매뉴얼(SBSB-539)』을 참조해 주십시오.

고객께서 실시해 주셨으면 하는 사항

- 브루트포스 공격 등에 의한 패스워드 해석이 상정되므로, 복잡한 패스워드(8 문자 이상, 복수의 문자 종별)를 설정해 주십시오.
- 패스워드는 고객 자신이 정기적으로 변경해 주십시오.

AI 번역본
-For Reference Only-

2-4 애플리케이션에 대한 부정 접속 방지

고객의 소중한 생산 정보 데이터를 도용이나 부정 이용으로부터 지키기 위해, 쉽게 DX 컨트롤러 내의 데이터 수집이나 가시화 애플리케이션에 액세스할 수 없도록 각 애플리케이션에 접속할 때 인증하는 기능을 사용합니다.

2-4-1 계정 관리(사용자 인증) 기능(애플리케이션)

DX 컨트롤러 내의 애플리케이션에 접속할 때 사용자명과 패스워드에 의한 사용자 인증을 실시하여, 온라인 조작하는 사용자를 특정합니다. DX 컨트롤러에 접속하기 위한 사용자 인증에 더하여, 다시 애플리케이션마다 개별적으로 계정 관리를 실시해 사용자 인증을 함으로써, 보안을향상시킵니다.

애플리케이션의 사용자 인증 기능은 애플리케이션을 조작하는 사용자를 미리 애플리케이션에 등록해 두고, 애플리케이션을 온라인 조작하는 사용자를 특정하는 기능입니다. DX 컨트롤러 내의 애플리케이션에 접속할 때 사용자명과 패스워드의 입력이 요구됩니다. 사용자명 및 패스워드가 미리 설정된 것과 일치하지 않으면 애플리케이션에 접속할 수 없습니다.

또한 각 사용자에게는 권한을 할당합니다. 이에 따라 각 사용자가 자신에게 할당된 권한 범위에서만 애플리케이션의 조작을 할 수 있도록 합니다.

사용자명, 패스워드, 그리고 그 권한의 정보 등의 사용자 인증 설정은 DX 컨트롤러에 저장됩니다. 따라서 다른 PC에서 DX 컨트롤러에 접속해도, 애플리케이션의 사용자 인증 기능을 사용할 수 있습니다.

대책할 수 있는 위험

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
○	○	○	○	○	○

애플리케이션의 사용자 인증 기능에서는 DX 컨트롤러 내의 애플리케이션에 접속할 때 사용자명과 패스워드를 입력하면, 할당되어 있는 권한의 권한 범위에서 조작할 수 있게 됩니다.

조작 방법의 자세한 내용은 SpeedBee Synapse에 대해서는 『DX 시리즈 SpeedBee Synapse 사용자 매뉴얼(SBSB-540)』을, Grafana에 대해서는 Grafana의 매뉴얼을 참조해 주십시오. 또한 패키지에 대해서는 『DX 시리즈 대시보드 제너레이터 사용자 매뉴얼(SGTE-729)』을 참조해 주십시오.

고객께서 실시해 주셨으면 하는 사항

- 초기 등록되어 있는 사용자 계정은 무효화 또는 삭제해 주십시오.
- 패스워드는 고객 자신이 정기적으로 변경해 주십시오.
- 브루트포스 공격 등에 의한 패스워드 해석이 상정되므로, 복잡한 패스워드(8 문자 이상, 복수의 문자 종별)를 설정해 주십시오.
- 액세스 토큰은 제3자에게 알려지지 않도록 엄중히 관리해 주십시오.

2-5 애플리케이션의 부정 조작 방지

DX 컨트롤러 내의 애플리케이션의 부정 조작을 방지하여, 고객의 소중한 생산 정보 데이터의 도용이나 부정 이용, 그리고 시스템의 이상을 방지합니다.

고객께서 실시해 주셨으면 하는 사항

- 익스포트한 파일에 기밀 정보가 포함되는 경우는, 제3자에게 누설되거나 변조되지 않도록, 이용자가 암호화하여 엄중히 관리해 주십시오. 또한 임포트할 데이터를 입수했을 때에는 해시값이 기대한 값과 일치하는지를 확인하여, 변조되지 않았음을 확인해 주십시오.

2-5-1 조작 권한 인증 기능(애플리케이션)

애플리케이션의 데이터를 변경하는 경우, 조작 실수에 의해 데이터의 수집이나 활용이 올바르게 이루어지지 않는 등의 피해를 줄 위험성이 있습니다. 조작자에게 부여하는 권한에 의해 조작할 수 있는 기능을 제한하여, 조작 실수를 방지합니다.

조작 권한 인증 기능을 사용하여, 관리자가 조작자마다 역할에 따른 권한을 설정함으로써 운용합니다.

대책할 수 있는 위험

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
	○		○	○	○

조작 권한 인증 기능의 설정은 SpeedBee Synapse에 대해서는 『DX 시리즈 SpeedBee Synapse 사용자 매뉴얼(SBSB-540)』을, Grafana에 대해서는 Grafana의 매뉴얼을 참조해 주십시오.

고객께서 실시해 주셨으면 하는 사항

- 브루트포스 공격 등에 의한 패스워드 해석이 상정되므로, 복잡한 패스워드(8 문자 이상, 복수의 문자 종별)를 설정해 주십시오.
- 패스워드는 고객 자신이 정기적으로 변경해 주십시오.

사본역본
-For Reference Only-

2-6 부인 방지

데이터를 지키기 위해서는 부정한 조작이 이루어진 것을 파악하는 것도 중요합니다. 또한 보안 인시던트 발생 시에는 그 원인이나 경위를 밝힐 필요가 있습니다. 보안 위반이나 사이버 공격을 기록함으로써, 누가 언제 무슨 조작을 했는지를 확인할 수 있어, 문제 발생 시의 부인 방지로서 사용할 수 있습니다.

2-6-1 로그 기능

DX 컨트롤러에서는 DX 컨트롤러에 대해 사용자가 Web UI를 사용하여 실시한 온라인 조작 중 보안에 관련된 중요 조작을 조작 로그에 등록합니다. 조작 내용, 시각, 사용자명, 실행 결과(성공 / 실패)를 기록합니다. 또한 DX 컨트롤러상의 애플리케이션도 각각 독자적으로 로그를 등록하며, 그중 보안에 관련된 로그를 감사 로그로서 이용할 수 있습니다. 또한 애플리케이션의 로그는 데이터 플로우 컨트롤러에 등록하는 로그와 애플리케이션 내부에 등록하는 로그 2 가지가 있습니다.

DX 컨트롤러의 로그에 대해서는 『DX 시리즈 CPU 유닛 사용자 매뉴얼 (SBSB-538)』을 참조해 주십시오.

애플리케이션의 로그에 관해서는 SpeedBee Synapse에 대해서는 『DX 시리즈 SpeedBee Synapse 사용자 매뉴얼(SBSB-540)』을, Grafana에 대해서는 Grafana의 매뉴얼을 참조해 주십시오. 또한 패키지에 대해서는 『DX 시리즈 대시보드 제너레이터 사용자 매뉴얼(SGTE-729)』을 참조해 주십시오.

대책할 수 있는 위협

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
		○			

고객께서 실시해 주셨으면 하는 사항

- 기록된 로그의 일시가 정확하지 않으면 부인 방지를 할 수 없을 가능성이 있습니다. DX 컨트롤러와 PC의 시각은 올바르게 설정해 주십시오. 올바른 일시를 유지하기 위해 NTP에서의 일시 설정을 권장합니다.
- 로그가 소거되면 부인 방지를 할 수 없습니다. 로그는 기록 가능 건수를 초과하여 이벤트가 발생한 경우, 오래된 정보부터 덮어쓰기됩니다. 또한 애플리케이션의 로그는 초기화(공장 초기화)에 의해 소거됩니다. 이용하시는 환경, 운용에서 로그가 남는 기간을 바탕으로 정기적으로 로그를 다운로드하여, 일정 기간 보존할 것을 권장합니다.

AI 번역본
-For Reference Only-

3

보안 패치 적용

3

나날이 진보하는 사이버 공격으로부터 데이터를 지키기 위해서는, 사용하고 있는 기기를 최신 상태로 하여 보안 강도를 높이는 것이 유효합니다.

본 장에서는 업데이트에 관해, DX 컨트롤러가 탑재하고 있는 기능에 대해 설명합니다.

3-1	DX 컨트롤러 업데이트.....	3-2
3-1-1	펌웨어 업데이트 이력.....	3-2
3-2	PC의 OS 업데이트.....	3-3
3-3	브라우저 업데이트.....	3-4

AI 번역본
-For Reference Only-

3-1 DX 컨트롤러 업데이트

기능의 추가나 조작성의 개선, 보안의 강화를 위해, DX 컨트롤러는 항상 최신 버전으로 업데이트하여 사용해 주십시오.

펌웨어 업데이트에 대한 자세한 내용은 『DX 시리즈 CPU 유닛 사용자 매뉴얼(SBSB-538)』을 참조해 주십시오.

고객께서 실시해 주셨으면 하는 사항

- 업데이트에는 USB 메모리를 사용합니다. 정당한 작업자에 의해서만 업데이트 작업이 이루어 지도록, 적절한 조작 권한의 설정, 그리고 출입 관리나 물리적 잠금 등을 실시해 주십시오.
- 업데이트에서 USB 메모리를 사용할 때에는 USB 포트를 유효하게 할 필요가 있습니다. 업데이트 전에 USB 포트를 무효로 해 두었던 경우는, 업데이트 후에 USB 포트를 무효로 되돌려 주십시오.

3-1-1 펌웨어 업데이트 이력

DX 컨트롤러의 로그에서 펌웨어의 업데이트 이력을 확인합니다.

DX 컨트롤러의 로그 확인 방법에 대해서는, 『DX 시리즈 Web UI 조작 매뉴얼(SBSB-539)』을 참조해 주십시오.

대책할 수 있는 위협

S: 위장	T: 변조	R: 부인	I: 정보 누설	D: 서비스 방해	E: 권한 상승
		○			

AI 번역본
-For Reference Only-

3-2 PC의 OS 업데이트

OS의 취약성에 기인하는 보안 리스크를 회피하기 위해, Web UI를 사용하는 PC의 OS를 항상 최신 상태로 해주십시오.

AI 번역본
-For Reference Only-

3-3 브라우저 업데이트

브라우저의 취약성에 기인하는 보안 리스크를 회피하기 위해, Web UI에 접속하는 브라우저를 항상 최신 상태로 해주십시오.

AI 번역본
-For Reference Only-

4

기기의 안전한 폐기

본 장에서는 폐기에 관해, DX 컨트롤러가 탑재하고 있는 기능에 대해 설명합니다.

4

4-1	DX 컨트롤러 내의 데이터 소거.....	4-2
4-1-1	초기화(공장 초기화) 기능.....	4-2

AI 번역본
-For Reference Only-

4-1 DX 컨트롤러 내의 데이터 소거

당사 제품을 폐기 또는 양도하는 경우, 기기에 저장하고 있는 사용자 데이터 등의 정보를 제3자가 보게 되어, 정보가 누설될 우려가 있습니다.

폐기 또는 양도하기 전에, 고객께서 책임을 지고 사용자 데이터를 소거해 주십시오.

4-1-1 초기화(공장 초기화) 기능

초기화(공장 초기화) 기능은 DX 컨트롤러 내의 설정을 공장 출하 시의 상태로 되돌리는 기능입니다. 사용자가 설정한 데이터도 소거됩니다.

공장 초기화 기능의 자세한 내용은 『DX 시리즈 CPU 유닛 사용자 매뉴얼 (SBSB-538)』을 참조해 주십시오.

고객께서 실시해 주셨으면 하는 사항

- DX 컨트롤러에는 설정의 초기화(공장 초기화) 등을 실시하기 위한 DIP 스위치가 있습니다. 안전한 운용을 하기 위해, DIP 스위치의 부정 조작을 방지하기 위한 대책을 실시해 주십시오. 예를 들어 출입 관리나 물리적 잠금 등을 실시해 주십시오.

AI 번역본
-For Reference Only-



부록

A-1 본서 및 당사 FA 제품에 관한 문의.....A-2



AI 번역본
-For Reference Only-

A-1 본서 및 당사 FA 제품에 관한 문의

본서나 당사 FA 제품에 관한 문의는, 아래 링크의 가까운 당사 지점 · 영업소로 연락해 주십시오. **일본 국내 문의처**

<https://www.fa.omron.co.jp/sales/local/ocShoplist/>

해외 문의처

<https://www.fa.omron.co.jp/sales/global/>

AI 번역본
-For Reference Only-

⚠ 안내 (For Reference Only)

본 문서는 AI 번역으로 작성된 참고용 국문자료입니다.
일부 표현은 원문과 다소 다를 수 있으며,
중요한 내용은 원문과 함께 참고해 주시기 바랍니다.

 Industrial Web ▶ <http://www.ia.omron.co.kr>

한국 오므론 제어기기 주식회사

서울특별시 서초구 강남대로 465, B동 18층(서초동, 교보타워)

TEL: 1522-8994 FAX: 02-3483-7788