Edgecross

安全指导方针 概要版

Ver. 1.0.0

Edgecross consortium inquiry form Edgecross 协会 技术部会 安全指导方针制定工作组

ECD-TE4-0004-01-ZH

技术部会 安全指导方针制定工作组
参加企业(敬称略、排名不分先后)

TACHIBANA ELETECH CO., LTD

DMG MORI CO., LTD

NEC Corporation

Hitachi, Ltd

FUJITSU LIMITED

Mitsubishi Electric Corporation

修订履历

版	修订内容	发行年月
1.0.0	初版	2019 年 9 月

目次

1. 前言

1.1 概要

现代制造业正在加快 IoT（Internet of Things）的应用，以增强企业竞争力和创造新的价值。『Edgecross 基金会』正是基于这一潮流，超越企业和产业界限，由基金会成员共同构筑，提供一个日本发布的、在 FA（Factory Automation）和 IT（Information Technology）之间，实现协调、开放的边缘计算领域的软件框架『Edgecross』。

通过协调 FA 和 IT 之间的关系，可以提高工厂或者生产设备等的生产性。同时， FA 系统受到来之内外攻击的威胁也增加了。为了减少威胁，能够通过针对人工的、物理的、还有连接的网络等各种各样的对策、进行多层次的实施是最理想的。

本文展示了使用 Edgecross 构筑 FA 系统时需要考虑的信息安全的要点，是保证可以安全、安心使用的指南。作为顾客导入时推荐的信息安全对策，从硬件/操作系统，信息安全软件，Edgecross 基本软件，网络等观点进行了相关要点的描述。

1.2 本指南的对象范围

本指南的想定读者包括构筑 Edgecross 系统的技术人员、Edgecross 系统的管理员以及 Edgecross 系统的用户。

本指南根据 IoT 推进协会/总务省/经济产业省刊行的《IoT 安全指南》,对 Edgecross 系统的安全对策方针进行了细化。

表 1-1 显示了安全对策方针的要点与本文档中描述的位置之间的对应关系。

表 1-1 安全对策方针的要点和记载位置

"IoT 安全指南"ver 1.0(IoT 推进协会/总务省/经济产业省) 安全对策指针一览			本指南中的位置
大项目	方针	要点	
方针	指针 1 制定考虑 IoT 性质的基本方针	要点 1. 经营者参与 IoT 安全	1.3
		要点 2. 防备内部不正当或错误	1.3
分析	指针 2 认识 IoT 的风险	要点 3. 特定应该要守护的东西	2.2
		要点 4. 想定连接引起的风险	2.3
		要点 5. 想定连接波及的风险	2.3
		要点 6. 认识物理风险	2.3
		要点 7. 学习过去的事例	2.4
设计	指针 3 考虑应该守护的东西能被守护的设计	要点 8. 设计出个体和全体都能被守护的方案	3.1
		要点 9. 设计成不给对方带来麻烦的方案	3.1
		要点 10. 做到安全放心的设计的整合性	3.1
		要点 11. 设计成即使与不特定的对方连接,也能确保安全放心的方案	3.1
		要点 12. 对实现安全放心的设计进行验证和评价	3.1
构筑・连接	指针 4 考虑网络上的对策	要点 13. 设计能掌握机器的状态并进行记录的功能	3.2, 3.3, 3.4
		要点 14. 根据功能和用途进行适当的网络连接	3.2, 3.3, 3.4, 3.5
		要点 15. 注意默认设置	3.2, 3.3, 3.4, 3.5
		要点 16. 引入认证功能	3.2, 3.3
运用・维护	指针 5 维持安全放心的状态,进行信息发送、共享	要点 17. 发货・发行后也维持安全放心的状态	4.1
		要点 18. 发货・发行后也要掌握 IoT 风险,向有关人员传达守护需要的内容	4.2
		要点 19. 让一般使用者知道由于连接而产生的风险	4.2
		要点 20. 认识到 IoT 系统或服务的相关方的作用	4.2
		要点 21. 掌握脆弱的机器,适当地提醒注意	4.2

1.3 基本方针

1.3.1 网络安全经营

在灵活运用 IoT 系统的网络安全对策中,制定考虑到 IoT 系统性质的基本方针是非常重要的。安全对策可能会增加成本,另外,还需要想定会面临需要超出运用现场可以酌情处理范围的事态。因此,经营者层级别必须率先明示安全对策的方针。

安全对策还需要构筑各地协作对应的体制,培养能够灵活运用安全技术的人才等。而且,还需要应对威胁安全的内部不正当的可能、意外发生的错误等人为威胁。

请参考经济产业省 独立行政法人信息处理推进机构刊行的《电子安全经营指南》,配合组织来制定安全对策。

另外,Edgecross 协会发布有关 Edgecross 系统的安全信息,请一并灵活运用。

1.3.2 Edgecross 协会

Edgecross 协会作为普及促进产业界发展的平台的团体,为了能在帮助客户维持和提高利用环境的安全和放心方面做出贡献,我们将以以下 3 项为主干持续进行配合。

・构筑确保安全・放心的组织・体制

本协会为迅速应对安全问题整备了体制,在发生安全事故时与公共机构合作,迅速应对并向客户提供信息。另外,调查威胁动向・技术・制度等,应该对本协会会员企业及客户全体保持对安全的正确知识和高的意识,进行努力周知。

・实现安全・放心的产品开发

本协会与会员企业一起,分析应该守护的资产和想定的威胁,进行坚固的产品设计,为了在发货・发行后也能够维持安全・放心的状态,制定面向开发者的安全指导方针,进行实施适当的安全对策的产品开发。

・提供面向客户的安全指导方针

本协会认为,为了降低威胁,应该多层次实施人的、物理的、网络等的各种对策。因此,本协会提供了面向导入了 Edgecross 对应产品的 FA 系统进行适当运用的安全指导方针,对《Edgecross》的利用环境中安全对策导入・维持提高方面进行支援。

1.4 简称

BIOS	Basic Input Output System
CPU	Central Processing Unit
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DMZ	DeMilitalized Zone
DoS	Denial of Service
ERP	Enterprise Resources Planning
EWS	Engineering WorkStation
FA	Factory Automation
FW	FireWall
GW	GateWay
HDD	Hard Disk Drive
HMI	Human Machine Interface
ID	Identification
I/F	Interface
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MES	Manufacturing Execution System
MQTT	Message Queuing Telemetry Transport
NC	Numerical Control
OPC	OLE (Object Linking and Embedding) for Process Control
OPC UA	OPC Unified Architecture
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
WWW	World Wide Web

1.5 用语

表 1-2 中列出了本指南中使用的术语。

表 1-2 用语

用语	说明
IT 系统	使用 IT 灵活运用来自生产现场数据的系统。在本文中,特别是指经由 LAN 或因特网与生产现场连接的外部系统了。
Edgecross 系统	使用 Edgecross 的系统。
Edgecross 软件	Edgecross 基本软件、边缘应用程序、数据收集器的总称。
Edgecross 基本软件	实装 Edgecross 功能的软件。与边缘应用程序协作,能够对生产现场的数据进行分析・诊断等,以及预防错误或和云端的 IT 系统之间进行数据的交换。
边缘应用程序	在边缘计算领域中,利用由 Edgecross 提供的功能,为了灵活运用生产现场的数据进行各种各样处理的软件。
数据收集器	通过各种网络,对生产现场的数据进行收集的软件组件,由各供应商面向各种网络及连接对象机器进行提供。

1.6 相关资料

表 1-3 中列出了本指南中的相关文档。

表 1-3 相关文档

No.	资料名称	资料 No	获得方法
1	IoT 安全指南 ver 1.0 2016 年 7 月 IoT 推进协会、总务省、经济产业省	-	http://www.soumu.go.jp/main_content/000428393.pdf
2	电力安全经营指南 Ver 1.0 2015 年 12 月 经济产业省 独立行政法人 信息处理推进机构	-	http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
3	Edgecross 规格书 概要说明篇	ECD-TE1-0002	Edgecross 协会会员专用页面
4	Edgecross 基本软件 Windows 版用户手册	ECD-MA1-0001	电子市场(Edgecross 基本软件 Windows 版商品文档)

2. Edgecross 系统

本章包含系统特征、要保护的资产、想定的威胁和安全事件事例。

2. 1 系统特征

Edgecross 是实现 FA 和 IT 协作的开放的边缘计算领域的软件平台。在边缘计算领域,通过组合多供应商的组件使生态系统的构筑变为可能。

边缘计算是在生产现场侧对从生产现场收集到的数据进行的数据处理。通过在物理上接近生产场所的工业 PC 上运行的应用程序,实现了被要求实时响应的系统。

此外,因为 IT 系统灵活运用多个据点或长期数据,通过边缘计算,也实现了生产现场和 IT 系统的无缝协作。

2. 2 要保护的资产

图 2-1 显示了 Edgecross 中要保护的资产整体。作为应该不受各种安全威胁的被保护资产,这里大致分为数据、硬件/OS、Edgecross 软件及关联软件、网络等 4 种分类。

数据中包含运行信息、传感器信息等、也包括机床、工业用机器人生成的数据和 NC 程序等为了操作所必须的数据，但 Edgecross 不对 NC 程序等进行操作。

硬件/OS 包括工业 PC、Windows OS 等。

Edgecross 软件包括进行实时数据处理和数据模型管理的 Edgecross 基本软件、灵活运用生产现场数据进行各种处理的运行监视等边缘应用程序、以及通过后述的 FA 网络收集生产现场数据的数据收集器。另外,还有作为相关软件的开发套件等。

网络包括有传输生产现场数据的控制网络和现场网络等 FA 网络,以及与 MES 和 ERP 等 IT 系统协作的信息网络。

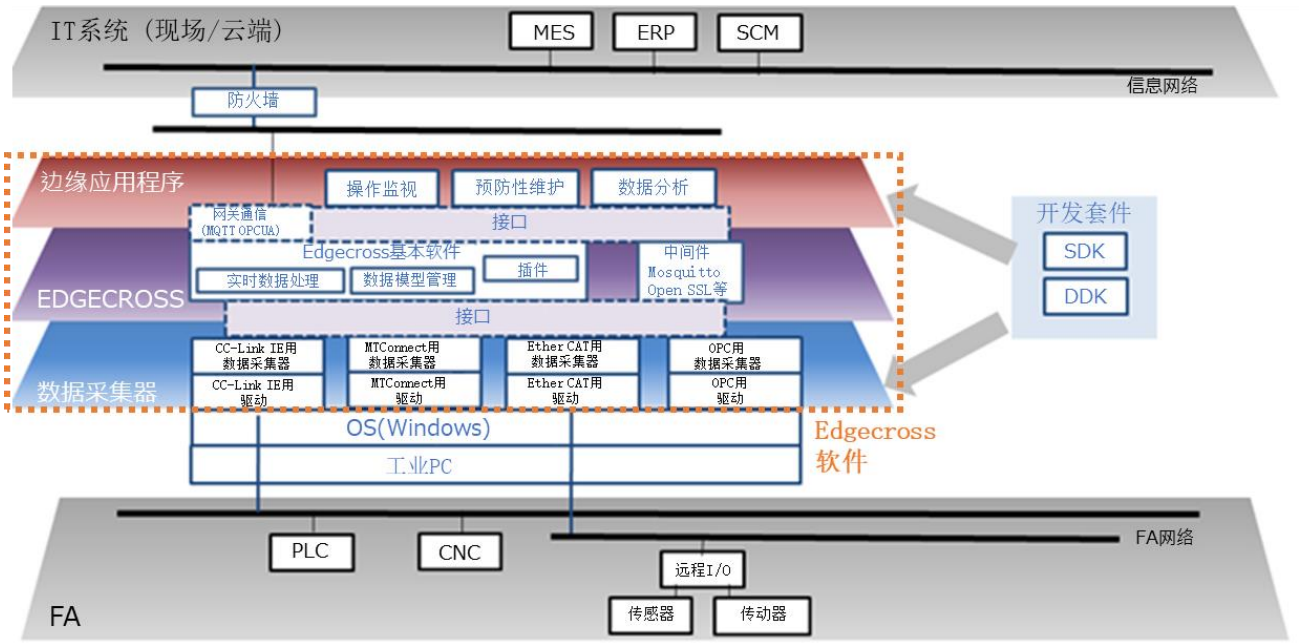

图 2-1 Edgecross 中要保护的资产

2.3 想定的威胁

列出了在前述的系统中想定的安全威胁。这些威胁的影响包括产品的供给停止、火灾等事故、不良品的生产等也被想定。

(1) 欺骗

通过对其他用户的 Windows 账户(ID 和密码)的类推或非法获取,假冒成本人非法登录到工业 PC 的威胁被想定。

(2) 信息泄漏

Edgecross 基本软件中收集的生产现场的数据等,可能会受到非法读取的威胁被想定。另外,边缘应用程序等软件从工业 PC 进行非法读取的威胁也被想定。

(3) 恶意软件

工业 PC 上安装恶意软件等非法软件的威胁被想定。

(4) 非法通信

工业 PC 中潜伏的恶意软件与外部机器进行非法通信的威胁被想定。

(5) 篡改

在工业 PC 中潜伏的恶意软件会非法地改写边缘应用程序等软件,从而导致该软件的功能受到阻碍的威胁被想定。另外,恶意软件通过对 Edgecross 基本软件中收集到的生产现场数据等进行非法改写,可能会产生不适当的统计结果,或生成出能够启动下一处理的不适当的触发器的威胁被想定。

(6)DoS/DDoS 攻击的踏板

恶意软件感染的工业 PC 被用作对服务器的 DoS/DDoS 攻击的踏板的威胁被想定。

(7) 滥用脆弱性

由于操作系统或安装的软件的脆弱性被恶意利用，恶意软件被安装在工业 PC 上的威胁被想定。

(8) 物理攻击

可疑人员物理侵入,工业 PC 被盗等物理性攻击的威胁被想定。

2.4 安全事件事例

图 2-2 显示了一个发生在乌克兰的发电厂事件的示例。 一家供电公司发生了网络攻击，造成 140 万个家庭的大规模停电，包括公共基础设施。 攻击始于外部有针对性的攻击电子邮件，感染了员工终端，试图在内部传播，最终导致发电设施通过 SCADA 系统发生故障。

这个事例表明,即使在没有直接连接到 Internet 的控制系统环境中,也可能受到网络攻击。

部署 Edgecross 系统的工厂环境也是同样的不与因特网连接的环境,但必须认识到有安全风险,必须采取安全措施。

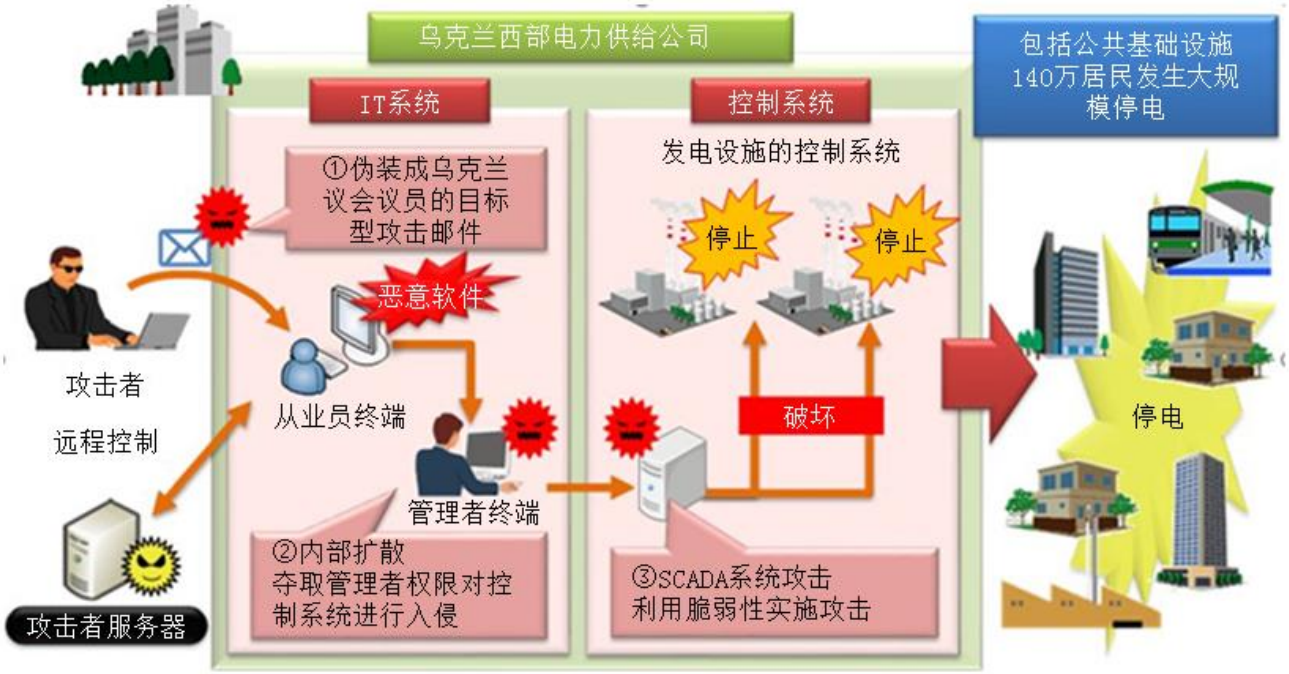

图 2-2 发电设施的事故事例

3. 构筑

3.1 构筑要点

在构筑 Edgecross 系统时,明确应该守护的对象,为了守护那些对象请按照以下(1)～(5)的观点进行系统设计。

《IoT 安全指南》中记载了以下要点。在 Edgecross 系统上,也请参照《IoT 安全指南》进行构筑。

(1) 个体、全体都能守护的设计

对于通过外部接口/内包/物理接触引起的风险,请在各个机器・系统中检讨对策。另外,在各个机器・系统无法完全对应的情况下,请在包含这些机器系统的上位的 IoT 机器・系统中研究对策。

(2)不给对方带来麻烦的设计

进行能够检测机器・系统异常的设计,请检讨检测到异常时的适当行动。

(3) 确保实现安全放心的设计的整合性

为了实现安全放心,请设计成可视化的。另外,请确认用于实现安全放心的设计的相互影响。

(4) 即使与不特定的对方连接,也能确保安全放心的设计

请检讨能够根据机器・系统相连的对方或连接的状况来判断连接方的设计。

(5) 实现安全放心的设计的验证・评价

对于连接的机器和系统,也请考虑是 IoT 的风险,对实现安全放心的设计进行验证和评价。

为了降低威胁,最理想的是考虑采取人的、物理的、以及连接的网络等多种多样的对策进行多层次的实施。推荐客户导入以下安全措施。

3.2 硬件/OS

3.2.1 硬件

(1) 采购

Edgecross 可以搭载于各种制造商的工业 PC 上。为了构筑安全・放心的机器,请从充分可靠的供应商那里采购工业 PC。

请确认供应商有接受机器支持的窗口,且容易访问,机器的各项规格和固件的更新等技术信息是否已公开等。

另外,请注意即使是可信赖的制造商的产品,流通路径也有可能存在问题。例如,可以考虑销售怀有恶意的混入恶意软件的二手销售品等情况。

(2) 设置

设置工业 PC 时,请注意防护物理性攻击。

・笔记本锁、可上锁的 PC 机架的物理盗窃的对策
・通过 USB/LAN 物理锁定来进行物理连接的对策
・操作员的进出限制

这些对策因使用环境而异,所以请根据环境进行实施。

(3) 默认设置

工业 PC 有若干关于安全性的设定。请配合使用环境和运行的软件进行适当的设定。以下列出了代表性的设置项目。详情请参照工业 PC 的手册等。

・BIOS 密码、HDD 密码等密码设定
・引导驱动器设定
・USB 设定

・Wake on Lan 等可进行外部控制功能的设定
・TPM 等安全芯片的设定

(4) 更新

请适当更新 CPU 或芯片组的固件 . BIOS、存储器或网卡的固件或驱动程序等。更新软件的取得应通过利用可信赖的 Web 站点等，可以保障更新软件没有被篡改的手段来进行。

此外,从各硬件发货到实际使用的期间,请留意固件等有可能被更新的情况,即使是最新的硬件,在构筑时也一定要确认固件等的更新信息。

(5) 运用

请确认硬件(也包括附带的软件)的技术支持期间。推荐在技术支持期内运用。

如果不得不在超过技术支持期限的情况下继续运用,请在认识到现用机器的技术支持期限已过这个风险的基础上进行适当的管理。

如果机器处于未使用状态,从而作为管理对象外的场合,非管理机器正在运转这件事可能会成为安全风险,所以请关闭该机器的电源。

3.2.2 OS

Edgecross 基本软件在 Microsoft® Windows® 10 Operating System(以下称为 Windows)上运行。在本章中,关于 Windows 的运用记载了基本的指导方针,关于实际的实施内容,请根据 Edgecross 机器的运用环境适当进行选择。

另外,Windows 的功能和用语等在今后的更新中也有可能发生变更。详细信息请参阅 Microsoft 公司主页等的信息。

(1) 帐户・密码

Windows 具有为每个用户管理帐户和密码的功能。请根据用户的作用设定帐户,并设定其他人难以推定的密码等,实施适当的管理。

用户认证的时候,除了 Windows 帐户密码之外,PIN 认证、生物认证或对以上认证方式组合的两级认证/多要素认证的使用也成为可能。

对 Windows 系统进行重要变更时，设有向管理员权限用户请求许可的安全功能(用户帐户控制功能)。建议启用本功能。

Windows 具有存储各种用户名和密码的功能。在系统中存储诸如网络访问授权信息和 Web 页面用户名・密码之类的信息可能会导致安全风险,所以推荐没有必要时不存储上述信息。

(2) 设定

Windows 包含各种各样的应用程序和服务。建议在运行 Edgecross 时禁用不必要的功能。特别是,对照相机机能和麦克风机能等 Edgecross 中不需要的个人使用机能请进行无效化设置。另外,请尽可能限制或禁用 USB 或 Bluetooth 等外部物理访问。

作为恶意软件对策,请利用 Windows 中搭载的安全功能,或者导入第三方安全软件。推荐您在个人防火墙上切断不需要的网络访问。

(3) 更新

Windows 具备在 Windows Update 中适用更新程序的功能。建议您根据环境更新为最新状态。但是,作为现实问题,伴随更新程序有再启动的情况、更新需要花费很长时间的情况、与动作环境不相容的情况、存在有故障的情况,因为上述情况有可能对 Edgecross 的运用造成障碍，所以请留意上述情况。

运用机暂时延迟更新程序的适用,为更新程序的动作验证准备试验用机器等对策是有效的。

Microsoft 公司提供了 Windows Server Update Services(WSUS)作为控制更新程序的适用过程的解决方案。

推荐将 Windows Update 定位为设备维护的一环,并有计划地运用。

3.3 安全软件

安全软件是用于计算机安全对策的应用程序软件的总称。

这些软件的一般功能是防止系统的侵入和恶意软件的感染。

作为 Edgecross 基本软件以及认定产品、推荐工业 PC 等非法软件的启动对策(检测・防止恶意软件等的启动和动作),推荐客户引进安全软件。

在导入时,请联系安全软件的产品销售商进行导入。

恶意软件等感染时,与一般的 Windows 机器感染时一样,例如有以下影响。

・安装不正当的软件
・各种数据的篡改、消失、泄露
・成为对其他系统进行攻击的跳板

安装安全软件后,推荐考虑以下 3 点。

(1) 更新合同

根据许可协议的不同,安全软件可能有一年或多年使用期限的限制的情况。

需要更新许可证协议以便在系统运行期间能够继续使用。

(2) 更新

更新安全软件的功能以增强对安全威胁的检测能力。

恶意软件检测模式通常每天更新,因此需要定期更新。

另外,当安全软件被进行大规模功能强化时,会需要版本升级,请检讨是否进行版本升级。

(3) 系统扫描

定期扫描整个系统。由于在实行扫描过程中 CPU 负荷变大,所以推荐根据系统的运行状况来进行扫描。

3.4 Edgecross 基本软件

Edgecross 基本软件在 Windows 上运行,并由以下软件组成。通过与边缘应用程序协作,可以实行生产现场的数据分析、诊断等,或者与本地或云的 IT 系统之间进行数据交换。

表 3-1 Edgecross 基本软件的构成

软件	内容
实时流程管理器	实时流程管理器是安装了实现生产现场数据的实时诊断・反馈功能的软件。 通过数据收集器(通过网络收集生产现场数据的软件)可以收集所连接的机器、装置或线路的数据,能够进行数据的处理以及加工。还可以使用插件进行机能扩展。
实时流程设计器	安装了实时流程管理器操作所需的各种设置的创建、保存、查看、实时流程管理器操作的启动/停止，以及诊断功能的软件。
Management Shell	用于对生产现场的机器、装置或线的数据建模,并将其作为分层结构来管理的软件，作为Windows服务在Windows的后台运行。 通过使用数据收集器从连接的机器、装置或线路可以读取数据或写入数据。
Management Shell Explorer	用于设置和参照Management Shell程序管理的数据模型的软件。

由于最新的 Edgecross 基本软件包含了对已知脆弱性的易受攻击性的处置,所以请确保使用 Edgecross 基本软件的最新版本。对于版本升级,推荐在动作验证的基础上进行升级。另外，Edgecross 基本软件的主要安全相关功能和注意事项如下。详细情况,请参阅 Edgecross 基本软件 Windows 版用户手册。

(1)OPC UA 连接器

Management Shell 程序作为 OPC UA 服务器运行,具有对作为 OPC UA 客户端的边缘应用程序提供模型访问 I/F、数据访问 I/F 的功能(OPC UA 连接功能)。此时,可以使用边缘应用程序的客户端证书进行认证。

(2)使用 MQTT 的边缘应用协作机能

从实时流程管理器向边缘应用程序传送数据(收集数据、加工数据),在从边缘应用程序接收应答数据时,可以用 TLS 进行加密。

(3) 事件历史记录

获取实时流程管理器和实时流程管理器使用的数据收集器中发生的事件信息,并将事件历史记录和事件的详细信息、原因、处理方法作为诊断信息进行显示。即使关闭正在运行的实时流程管理器的工业 PC 的电源,事件履历也会被保存,所以可以在重新启动工业 PC 后进行确认,或者在根据前后操作信息的确认来追究问题的发生原因时被使用。另外,在发生错误时无法确认错误代码的情况下也可以被使用。

(4) 文件保存功能

在实时流程管理器收集/加工的数据或诊断结果的数据的文件保存功能中,指定远程共享文件夹作为保存目的地时,推荐适当配置 Windows 防火墙的访问限制等。

3. 5 网络

作为保护资产的安全对策,灵活运用网络的方法如下所示。

[对网络的安全对策示例]

图 3-1 显示了网络安全措施的示例

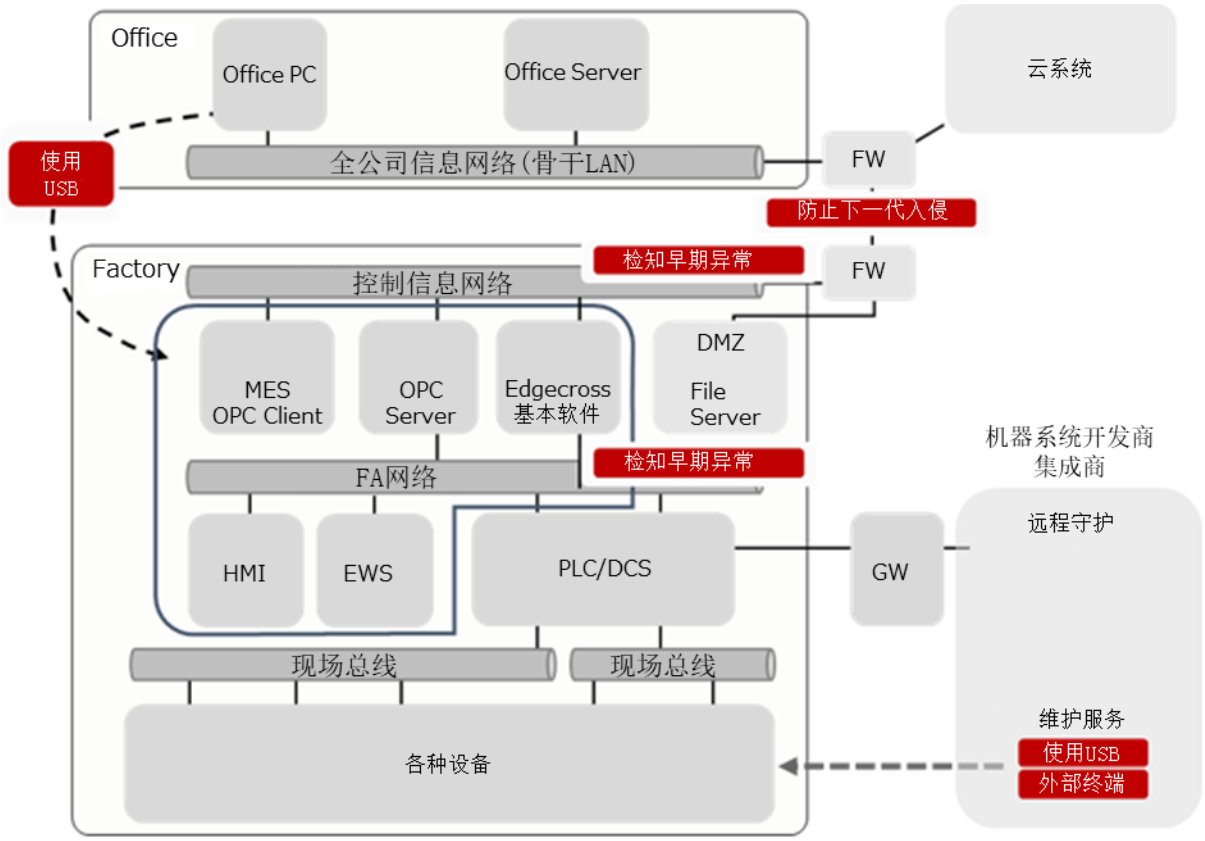

图 3-1 面向网络的安全对策的使用场所示例

[网络上的对策]

将工厂内存在的网络根据使用场所分为"控制信息网络"、"FA 网络""现场总线"层次进行说明。

(1) 对策方针

通过在网络上进行感染防止、感染后的检测,在终端侧采取感染状态的确认・检测・驱除的对策,必须最大限度地消除与网络连接时发生的风险。

(2) 网络边界对策

对作为工厂入口的控制信息网络和通常的全公司信息系统网络(以下称为 IT 系统网络)进行连接时,为了防止恶意软件从 IT 系统网络进入,要设置防火墙装置(以下称为 FW 装置)。但是,不推荐单纯的 FW 装置,而是推荐具备考虑了脆弱性对策的下一代型进入防止系统的 FW 装置。

(3) 早期异常检知对策

在控制信息网络中,考虑到网络上的机器万一受到恶意软件感染的时候,能够在网络上检测恶意软件感染的、可视化最新威胁的、能够检测到异常的标准型网络攻击检测传感器装置也被推荐使用。

(4)USB 使用对策

即使用 FW 装置切断了成为恶意软件进入路径的 IT 系统网络,也需要采取早期异常检测对策,因为通过 Edgecross 的设置，机器间被网络连接的场合下,现场运用中来自使用 USB 设备的进入路径没有消失。

即使开始通过网络收集信息,也难以从所有的点去除 USB 的运用,另外,即使去除,直到去处完成也需要一定程度的时间,所以在现场内存在 USB 设备的情况下,在使用 USB 设备进行数据收集的要点是,必须使用不需要安装的恶意软件检索・驱除工具,来确保终端的健全性。

使用不需要安装的工具的背景是，抑制通过安装恶意软件对策软件给终端带来负荷影响的作用,另外,在制造商提供的嵌入式终端等中,有时会有不允许安装恶意软件对策软件的情况。

(5) 铺设网络的导入设计的重要性

到此为止所记载的对策,是在向已有环境铺设网络时,在已知网络状态的情况下的对策。

・不清楚现状的网络环境

・每个设备都构筑了各自的最佳网络环境,不能将它们相互连接

・今后重新铺设网络

以导入 Edgecross 为契机,推进工厂的网络化时,为了有效且安全地利用网络,需要采用从设备之间的 IP 地址重复状态开始,不变更地址,有效率地连接设备之间的手法,以及采用以防止恶意软件扩散为目的的使用微分区的专用的网络设计手法。

因此,推荐向 IP 网络构筑专业的集成商，传达引进网络的目的和将来的利用方法,以便能够设计・构筑出想实现的网络。

4. 运用

4.1 脆弱性对策

近年来,工厂现场也出现恶意软件侵入,通过扩散活动,经常发生工厂停工的事件。恶意软件从 USB 设备或携带设备侵入,利用网络上机器的脆弱性,谋求对其他机器的感染扩大。

为了抑制恶意软件的感染和扩散活动,必须适当地实施各机器的 OS 和应用程序等的资产管理,并要求及时地应用 OS 和应用程序的安全补丁。

通过实施导入 Edgecross 基本软件的工业 PC 的软件版本管理,根据需要实施 Edgecross 基本软件、OS、其他应用程序的更新等,使脆弱性的对应变为可能。以下是对各部位进行更新的想法。

(1)Edgecross 基本软件

为了消除脆弱性,请确保使用 Edgecross 基本软件最新版本。在版本升级过程中,建议您在动作验证之后实行它。

因为安全信息在 Edgecross 的主页上公开,所以在确认内容后,请根据需要对应。

(2) 边缘应用和数据收集器

由于边缘应用程序和数据收集器是由 Edgecross 会员企业进行开发的,所以请从开发商那里获取信息来对应脆弱性问题。

请在动作验证后,实行版本升级。

(3)OS

Edgecross 基本软件支持的操作系统为 Windows。定期的脆弱性被发表的基础上,Microsoft 公司定期发行 OS 的修订程序。建议定期进行更新。

在更新时,请从工业 PC 制造商或 Microsoft 公司获取有关 OS 更新的信息,在动作验证之后实行更新。

(4) 硬件、BIOS、驱动程序

对于工业 PC 或与其连接的装置的 BIOS 或驱动程序,只要具有脆弱性,就必须采取措施。推荐从开发商处获取信息,并在动作验证的基础上, 进行适用。

4.2 安全管理・应对

在 Edgecross 系统内,存在各种各样的机器,也想定存在 10 年以上的长期利用的机器和系统。向系统内追加机器或设定的更新、网络环境的变更等多种环境变化伴随的脆弱性的发生也令人担心。并且,即使不对机器进行变更,也可能发现新的脆弱性。

在开始运用 Edgecross 系统后,继续进行安全管理・对应也很重要。在整个系统中,各种机器的管理者和网络管理者、系统的运用者、软件和机器的供应商等,有很多相关人员。请事先整理相关人员的作用,建立体制,以便能够有组织地进行安全管理・对应。

・请检讨和适用在必要的时间适当地实施机器的安全性上重要的更新等方法。
・Edgecross 系统的构筑者・运用者请收集・分析系统的脆弱性信息,并向相关人员发送信息。
・请向相关人员通知随意与系统连接的风险,以及希望遵守的约定。
・请对 Edgecross 系统的各种机器制造商、提供者、系统管理员、使用者等相关人员的作用进行整理。
・请建立对有脆弱性的机器可以把握的机制,并有组织地定期进行监视。
・在特定了具有脆弱性的机器时,请提醒相应机器的管理者,尽快实施脆弱性对应。

引用方:"IoT 安全指南 ver 1.0"
2.5 运用・维护 方针 5 维持安全放心的状态,进行信息发送・共享

5. 总结

为了确保使用 Edgecross 的 FA 系统的安全・放心,请灵活运用本指南。
另外，关于本指南记载的相关问题，请填写 Edgecross 联盟网站上的咨询表格进行咨询。
Edgecross 协会联系表　　https://www.edgecross.org/ja/contact/form/