Edgecross

面向用户的安全指南　详细版

Ver. 1.0.0

Edgecross 协会　技术部会　安全指南制定 WG

ECD-TE4-0006-01-JA

技术部会　安全指南制定ＷＧ
参加企业(敬称略、不分先后)

TACHIBANA ELETECH CO., LTD.

DMG MORI CO., LTD.

NEC Corporation

Hitachi, Ltd.

FUJITSU LIMITED.

Mitsubishi Electric Corporation

McAfee Co., Ltd

Microsoft Japan K.K.

DELTA ELECTRONICS (JAPAN), INC.

Trend Micro Co., Ltd.

修订历史

Ver.	修订内容	发行年月
1.0.0	初版发行	2020 年 6 月

目录

1. 前言 …… 1

1.1 概要 …… 1

1.2 本书的对象范围 …… 1

1.3 基本方针 …… 1

1.4 简称 …… 3

1.5 术语 …… 4

1.6 相关资料 …… 4

2. Edgecross 系统 …… 5

2.1 系统的特征 …… 5

2.2 应保护的资产 …… 5

2.3 设想的威胁 …… 6

2.4 控制系统的安全意外事例 …… 7

2.5 实例 …… 9

3. 构筑的安全对策 …… 21

3.1 要点 …… 21

3.2 硬件/OS …… 22

3.3 安全软件 …… 24

3.4 Edgecross 基本软件 …… 26

3.5 网络 …… 32

4. 运用中的安全对策 …… 36

4.1 脆弱性对策 …… 36

4.2 安全管理、意外事件应对 …… 38

5. 总结 …… 39

附录　全体工厂的安全威胁详情

1. 前言

1.1 概要

现在制造业正在加速利用 IoT（Internet of Things）来强化竞争力和创造新的价值。“Edgecross 协会”是基于这个时代，超越企业和产业的界限，由协会会员共同构筑，从而提供实现与 FA（Factory Automation）和 IT（Information Technology）协调的开放的日本边缘计算领域的软件平台“Edgecross”。通过 FA 和 IT 的协调，令人期待的是工厂的生产性提高，但另一方面，受到 FA 系统内外攻击的威胁也会增加。为了减少威胁，最好考虑在多层网络上实施对人、物理、甚至连接的网络等各种各样的策略。

本书例举了在 Edgecross 典型用例中设想的具体威胁的基础上，展示了在使用 Edgecross 构建 FA 系统时应考虑的安全要点，是确保安全、安心的指导方针。作为推荐客户导入的安全对策，从硬件/OS、安全软件、Edgecross 基本软件、网络观点等归纳的重点，将会比概要版描述的更详细。

1.2 本书的对象范围

作为本书的对象读者，我们预想应为构筑 Edgecross 系统的技术人员、Edgecross 系统的管理人员以及 Edgecross 系统的运营人员。

本书以 IoT 推进协会/总务省/经济产业省发行的《IoT 安全指南》为基础，具体化了 Edgecross 系统的安全对策方针。

表 1-1 中显示了安全对策方针的要点和与本书记载部分的对应。

表 1-1 安全对策方针的要点和记载位置

“IoT 安全方针”ver1.0（IoT 推进协会/总务省/经济产业省） 安全对策方针一览			本书的记载位置
大项目	方针	要点	
方针	方针 1 制定考虑 IoT 性质的基本方针	要点 1. 经营者致力于 IoT 安全	1.3
		要点 2. 防备内部不合规或错误	1.3
分析	方针 2 认识 IoT 的风险	要点 3. 指定要保护的东西	2.2
		要点 4. 设想因连接而产生的风险	2.3, 2.5
		要点 5. 设想因联接而波及的风险	2.3, 2.5
		要点 6. 认识物理风险	2.3, 2.5
		要点 7. 学习过去的事例	2.4
设计	方针 3 考虑保护应该被保护的东西的设计	要点 8. 使用无论是各自还是整体都能保护的设计	3.1
		要点 9. 使用不会给对方造成困扰的设计	3.1
		要点 10. 采取实现安全安心设计的整合性	3.1
		要点 11. 使用即使和不特定的对象连接也能确保安全放心的设计	3.1
		要点 12. 对实现安全安心的设计进行验证和评价	3.1
构筑、连接	方针 4 思考网络上的对策	要点 13. 设置掌握机器等的状态并记录的功能	3.2, 3.3, 3.4
		要点 14. 根据功能及用途适当地进行网络连接	3.2, 3.3, 3.4, 3.5
		要点 15. 注意初始设置	3.2, 3.3, 3.4, 3.5
		要点 16. 导入认证功能	3.2, 3.3
运用、维护	方针 5 维持安全安心的状态，进行信息发送和共享	要点 17. 发货、发布后也维持安全安心的状态	4.1
		要点 18. 发货、发布后也要掌握 IoT 风险，传达希望相关人员遵守的事项	4.2
		要点 19. 通过连接让一般使用者知晓风险	4.2
		要点 20. 认识到在 IoT 系统服务中相关人员的作用	4.2
		要点 21. 掌握脆弱的机器，适当地提醒注意	4.2

另外，作为 FA 相关的安全文献，也有控制系统的安全标准 IEC62443 等，请根据需要进行参考。

1.3 基本方针

1.3.1 网络安全运营

在利用 IoT 的系统的网络安全对策中，制定考虑 IoT 系统性质的基本方针是很重要的。安全对策可能会花费成本，可能面临需要临时判断，酌情处理运用现场超出成本的情况。因此，经营人员层的水平需要率先提出安全对策的方针。

对于安全对策，各个地方协作应对的体制的构筑，能活用安全技术的人才的培养等也变得必要。并且，还要求应对威胁安全的内部不合规的可能性、无意中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发行的《网络安全经营指南》，作为组织致力于安全对策。

另外，Edgecross 协会还发布了有关 Edgecross 系统的安全信息，请一并使用。

1.3.2 Edgecross 协会

Edgecross 协会作为促进产业界发展的平台普及的团体，将以以下 3 点为支柱，持续致力于为客户在使用环境中维持、提高安全、安心做出贡献。

・为确保安全、安心而构筑的组织和体制

本协会为了迅速应对安全问题而整备体制，在安全事件发生时与 JPCERT/CC 联合迅速应对并向客户提供信息。同时，调查威胁动向、技术、制度等，为了对本协会会员企业及全体客户保持正确的安全知识和高度的意识，我们将努力做到使大家周知。

・实现安全、放心的产品开发

本协会与会员企业一起，分析必须保护的资产和设想的威胁，进行坚固的产品设计，为了在发货、发布后也能保持安全、安心的状态，制定了面向开发者的安全方针，进而实施适当的安全对策进行产品开发。

・面向顾客的安全方针的提供

本协会认为，为了降低威胁，在理想的情况下考虑，对人、物理、网络等各种各样的对策进行多层实施。因此，本协会为在引进了 Edgecross 对应产品的 FA 系统中，提供能适当运用的安全指导方针，并在“Edgecross”的使用环境中，支持安全对策导入/维持提高。

1.4 简称

BIOS	Basic Input Output System
C&C	Command and Control
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Data Base
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
IPS	Intrusion Prevention System
I/F	Interface
IoT	Internet of Things
IP	Internet Protocol
IPA	Information-technology Promotion Agency
IT	Information Technology
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
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
OSS	Open Source Software
PC	Personal Computer
PIN	Personal Identification Number
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WWW	World Wide Web

1.5 术语

本书中使用的术语如表 1-2 所示。

表 1-2 术语

术语	说明
IT 系统	使用 IT，活用来自生产现场的数据的系统。本书特指用于表示生产现场通过与 LAN 和互联网连接的外部系统。
Edgecross 系统	利用 Edgecross 的系统。
Edgecross 软件	Edgecross 基本软件、边缘应用程序、数据采集器、IT 网关的总称。
Edgecross 基本软件	安装了 Edgecross 功能的软件。与边缘应用程序相结合，可以实现对生产现场的数据进行分析、诊断等，以及与本地部署和云的 IT 系统之间进行数据交换。
搭载 Edgecross 的 PC	搭载了 Edgecross 基本软件的工业 PC。
边缘应用程序	在边缘计算区域，利用 Edgecross 提供的功能，执行用于生产现场的数据活用的各种处理的软件。 本文中特指通过 Edgecross 协会的认证试验并获得认证的软件。
数据采集器	通过各网络，收集生产现场数据的软件组件，面向各种网络及连接对象设备的各供应商提供。
IT 网关	为了活用生产现场的数据，各供应商提供与 IT 系统通信的软件组件。

1.6 相关资料

本文相关资料如表 1-3 所示。

表 1-3 相关资料

No.	资料名称	资料 No	获取方法
1	IoT 安全指南 ver 1.0 平成 28 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	网络安全经营指南 Ver 1.0 平成 27 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 式样书概要说明篇	ECD-TE1-0002	Edgecross 协会会员用主页
4	Edgecross 基本软件 Windows 版用户手册	ECD-MA1-0001	网上市场（Edgecross 基本软件 Windows 版 商品文档）
5	控制系统的安全风险分析指南 第 2 版	-	https://www.ipa.go.jp/files/000069436.pdf
6	网络・物理・安全对策架构 Version 1.0 平成 31 年 4 月 经济产业省	-	https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

2. Edgecross 系统

本章介绍了系统的特征、应保护的资产、设想的威胁、安全意外事件。

2. 1 系统的特征

Edgecross 是实现 FA 和 IT 协调的开放的边缘计算领域的软件平台。可在边缘计算领域通过多供应商的组件相结合构建生态系统。

边缘计算是将从生产现场收集的数据在生产现场进行数据处理。通过在与生产现场物理接近的工业用 PC 上执行应用程序，实现要求实时应答的系统。

另外，为了活用 IT 系统处理多个据点和长期的数据，通过边缘计算也将实现生产现场和 IT 系统的无缝合作。

2. 2 应保护的资产

图 2-1 所示为 Edgecross 中应保护的全部资产。作为应被保护各种安全威胁的资产，这里大致分为数据、硬件/OS、Edgecross 软件以及相关软件、网络 4 种。

数据中包含工作信息、传感器信息等工作机械、工业机器人生成的数据和 NC 程序等操作所需的数据，但 Edgecross 不处理 NC 程序等。

硬件/OS 有工业用 PC、Windows OS 等。

Edgecross 软件包括执行实时数据处理和数据模型管理的 Edgecross 基本软件，活用生产现场的数据执行各种处理的运行监视等边缘应用，有通过后述的 FA 网络收集生产现场数据的数据采集器，实现与 IT 系统无缝数据协作的 IT 网关，Mosquitto、OpenSSL 等中间件。另外，相关软件还有开发套件等。

网络上有传送生产现场数据的控制网络、现场网络等 FA 网络、与 MES、ERP 等与 IT 系统相结合的信息网络。

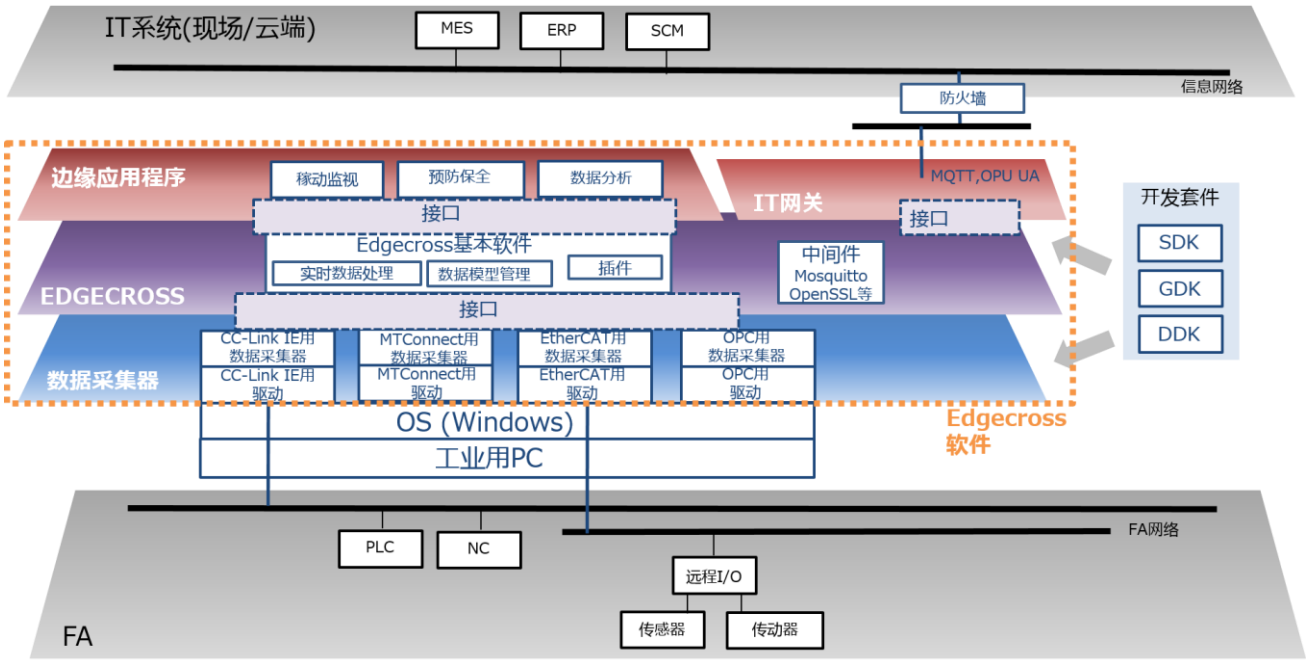


图 2-1 在 Edgecross 中应保护的资产

2.3 设想的威胁

列举出上述系统中设想的安全威胁。受这些威胁的影响，可以设想到产品停止供应、火灾等事故、不良品的产生等。

(1) 冒充

设想其他用户的 Windows 账号（ID 和密码）被推算或非法获取，如果伪装成本人的话，有可能会受到来自非法登录到搭载 Edgecross 的 PC 上的威胁。

(2) 窃取信息

设想 Edgecross 基本软件收集的生产现场数据等被非法读取的威胁。另外，也设想 Edgecross 软件可能会受到来自搭载 Edgecross 的 PC 非法读取的威胁。

(3) 恶意软件

设想恶意软件将被安装在搭载 Edgecross 的 PC 上。

(4) 非法通信

设想搭载 Edgecross 的 PC 上潜在的恶意软件可能会与外部设备非法通信的威胁。

(5) 篡改

设想搭载 Edgecross 的 PC 上潜藏的恶意软件非法改写 Edgecross 软件，可能会对该软件的功能造成威胁。另外，设想恶意软件将 Edgecross 基本软件收集的生产现场的数据等非法篡改，可能会产生不恰当的统计结果，以及产生不适当触发启动下一个处理的威胁。

(6) 高负荷攻击的踏板

设想被恶意软件感染了的搭载 Edgecross 的 PC，被当成对服务器 DoS/DDoS 攻击的踏板所产生的威胁。

(7) 脆弱性的滥用

设想被恶意使用 OS 和安装的软件的脆弱性，恶意软件被安装在搭载 Edgecross 的 PC 上，类似这种威胁。

(8) 物理攻击

假设有可疑人员物理侵入，盗窃搭载 Edgecross 的 PC 等物理攻击的威胁。

2. 4 控制系统的安全意外事例

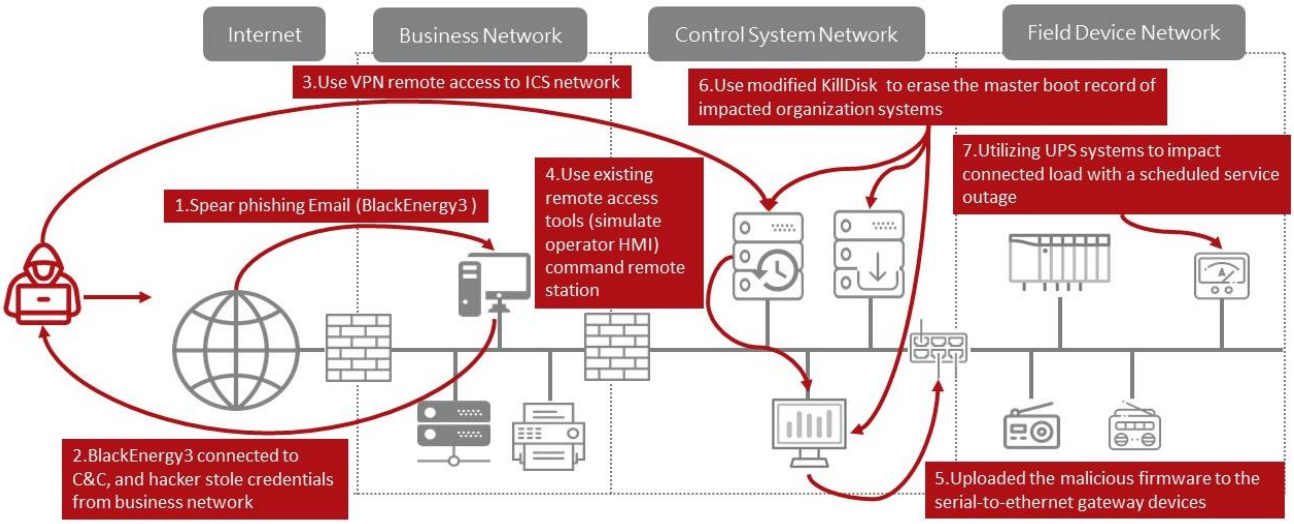
首先，提及一下在乌克兰发生的发电设施的意外事件。

2015 年 12 月，乌克兰各地区的 3 家电力公司，因大量网络攻击而被迫发生意外停电。据报道，停电长达 3 小时，约有 25 万名顾客受到影响。

攻击者利用“虚拟专网（Virtual private Network、VPN）”接入 SCADA 网络，控制了发电设施。因此，不仅使顾客停电，设施的操作也陷入了无法操作的状态。

这个事例表明，即使在没有直接连接到互联网的控制系统环境下，也有可能受到网络攻击的伤害。

即使是配置了 Edgecross 系统的工厂环境，有可能与之同样没有连接到互联网。即使在离线环境下，也要认识到还残留着安全风险，必须采取防止受害的安全对策。



（出处：趋势 威胁数据库・安全性 Blog https://blog.trendmicro.co.jp/archives/14203）

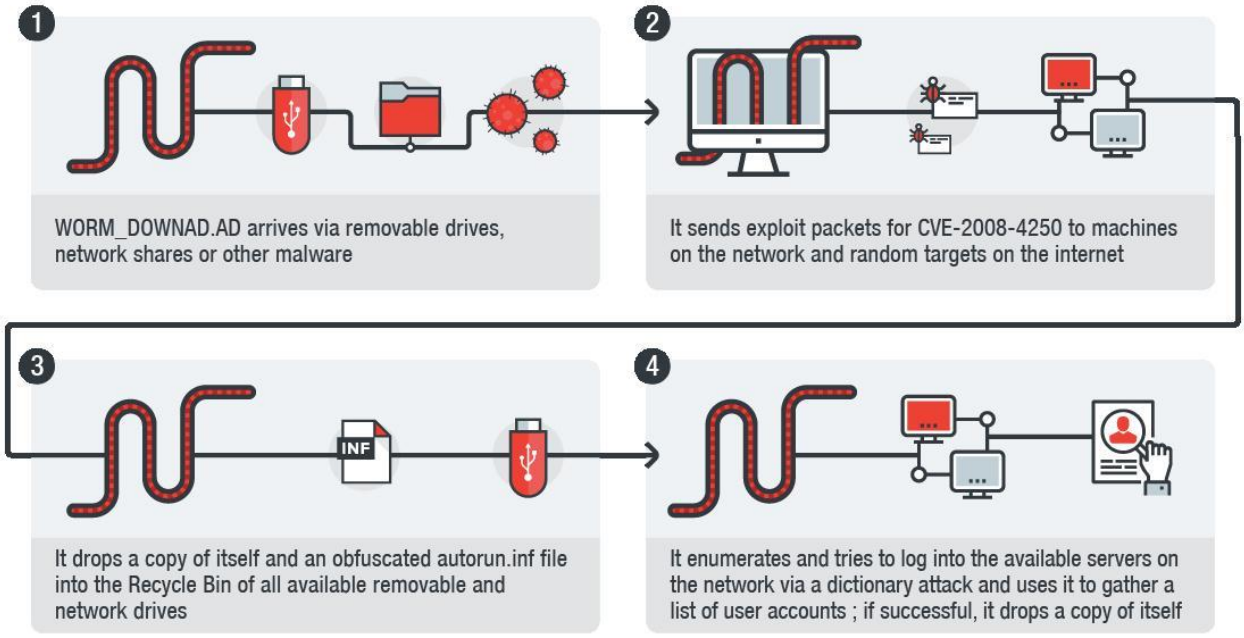
下一个例子是仍在工厂继续扩散的 DOWNAD(别名：Conflicker)事件。

DOWNAD 首次作为威胁兴起是在 2008 年 11 月。报告称，初次确认威胁后，世界上几十万台电脑瞬间感染了 DOWNAD。在这里着重强调的是，即使在全盛期已过去了 12 年的现在，DOWNAD 还是“对旧系统持续发挥威力的恶意软件”。

像“WannaCry”和“PETYA”这样，作为更现代的恶意软件，虽不是让一般人都能引起兴趣的恶意软件，但只要网络中存在不支持更新脆弱性的旧系统，依然是存在威胁，今后这种情况也不会发生变化。

这一事例表明，恶意软件可能会被外部带入的可移动介质侵入，并扩散到 LAN 的终端和网络驱动器上，有可能导致二次被害。

即使在配备 Edgecross 系统的工厂环境中，由于保养、维护等原因，也会有可能使用 USB 存储器、CD-ROM 等可移动介质的情况。在使用带入终端和可移动介质的情况下，必须要认识到还残留着由于维护人员的疏忽造成的安全风险，为了不遭受损失，必须采取事先确认等安全对策。



（出处：趋势 威胁数据库・安全性 Blog　https://blog.trendmicro.co.jp/archives/16614）

2.5 实例

2.5.1 系统构成

作为 Edgecross 使用时典型的系统构成，表现为大型工厂和小型工厂这两种情况。

【模式 1 】大型工厂的场合（图 2-2）

在大型工厂中，管理楼使用的进度管理用电脑等连接的信息网络和工厂内使用的网络分开，信息网络和工厂内的网络的通信和向互联网的通信是通过防火墙进行的。

工厂内的网络分为，工程管理工具和 MES Client 连接的信息控制网络[1]、机床连接的控制网络[2]、PLC 控制设备和 HMI 连接的本地网络[3]。

搭载了 Edgecross 的 PC（搭载 EdgecrossPC）连接到控制网络或信息控制网络上进行使用。

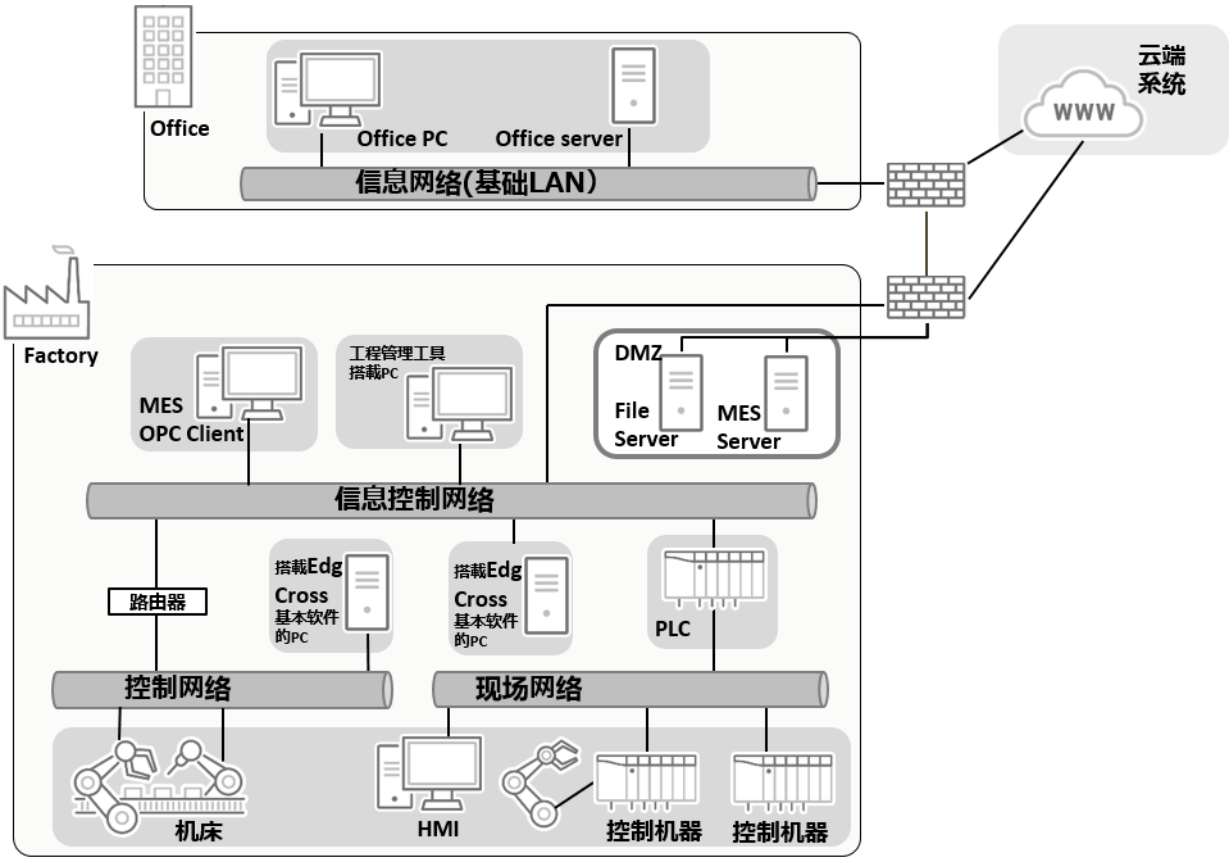


图 2-2 【模式 1 】系统构成的例子（大型工厂）

【模式 2 】小型工厂的场合（图 2-3）

在小型工厂，事务所内的办公用电脑、工程 PC、FileServer 等与机床连接在一个网络上。

搭载 Edgecross 的 PC 也连接在同一个网络上使用。

[1] 在工厂内的网络中，连接电脑和服务器等的信息系统网络

[2] 根据基于以太网的协议进行控制用通信的网络

[3] 以控制器间和本地设备间的控制通信为主要目的的网络

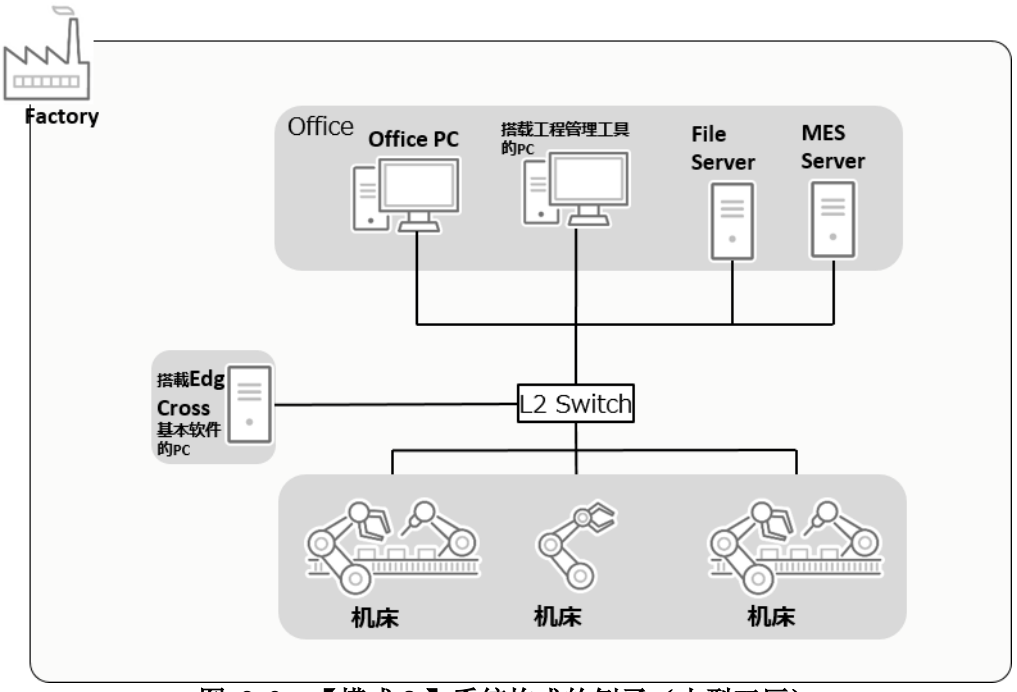


图 2-3 【模式 2 】系统构成的例子（小型工厂）

2.5.2 方案示例

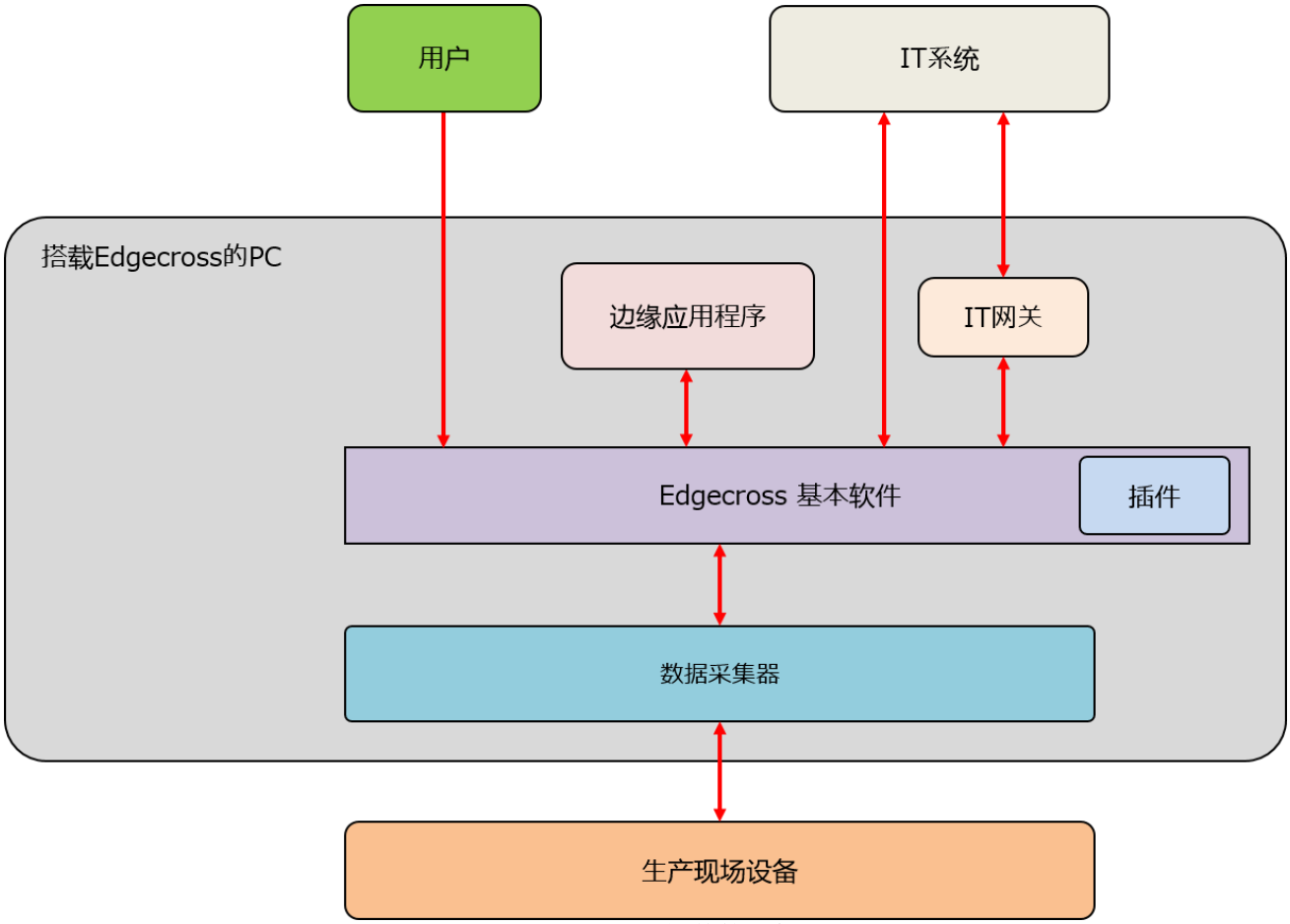


图 2-4 Edgecross 软件构成概要图

首先，Edgecross 软件的构成如上图所示。Edgecross 基本软件通过数据采集器进行生产现场设备的数据收集和反馈。边缘应用程序对数据进行分析、诊断。另外，与外部 IT 系统之间进行数据交换。

Edgecross 基本软件还包括实时流程管理器、实时流程设计器、Management Shell、Management Shell 资源管理器。

实时流程管理器是安装了实现生产现场数据实时诊断、反馈功能的软件。使用数据采集器（通过网络，收集生产现场数据的软件），可以收集连接的设备、装置或生产线的数据，进行数据的加工和分析。还可以使用插件来进行功能扩展。实时流程设计器将作为 Windows 服务被启动/停止。

实时流程设计器是一种安装了，可实现实时流管理器的动作所需的各种设定的制作、保存、显示、实时流程管理器的动作开始/停止、以及进行诊断功能的软件。

Management Shell 是对生产现场的设备、装置或生产线相关数据进行建模，并作为层次结构进行管理的软件。可以使用数据采集器读取连接的设备、装置或生产线的数据，并写入数据。Management Shell 资源管理器将作为 Windows 服务被启动/停止。

Management Shell 资源管理器对 Management Shell 管理的数据模型进行设定和参照，负责 Management Shell 的动作开始/停止。

在表 2-1 中、使用 Edgecross 的脚本示例，如表 2-1 所示。

表 2-1 使用 Edgecross 的脚本示例

	类别	脚本名	备注
(a)	设定	系统启动（实时流程设计）	通过实时流程管理访问机器
(b)		系统启动（Management Shell 资源管理器）	通过 Management Shell 访问机器
(c)	数据收集	基于 OPC UA 的边缘应用程序（MES Server 等）的数据访问	
(d)		利用边缘应用程序中的历史数据	
(e)		在 FileServer 中的数据积累	
(f)		云服务数据分析	不在模式 2 中进行。
(g)	反馈	来自边缘应用程序的反馈	边缘应用程序的诊断+反馈

(a) 系统启动（使用实时流程设计的事例）

启动实时流程设计器，进行实时流程管理相关的设定等。

① 用户启动实时流程设计器，选择要使用的数据采集器，设置访问目标设备。

② 接下来，进行“数据 Logging 流程设定”或“数据诊断流程设定”。

③ 最后应用设置。

④ 在数据诊断等中使用边缘应用程序时，进行该设置。

(b) 系统启动（使用 Management Shell 资源管理器的事例）

启动 Management Shell 资源管理器，进行 Management Shell 相关的设定等。

① 用户使用 Management Shell 资源管理器选择要使用的数据采集器，设置访问目标设备。

② 进行组件树编辑，制作工厂内系统的模型。

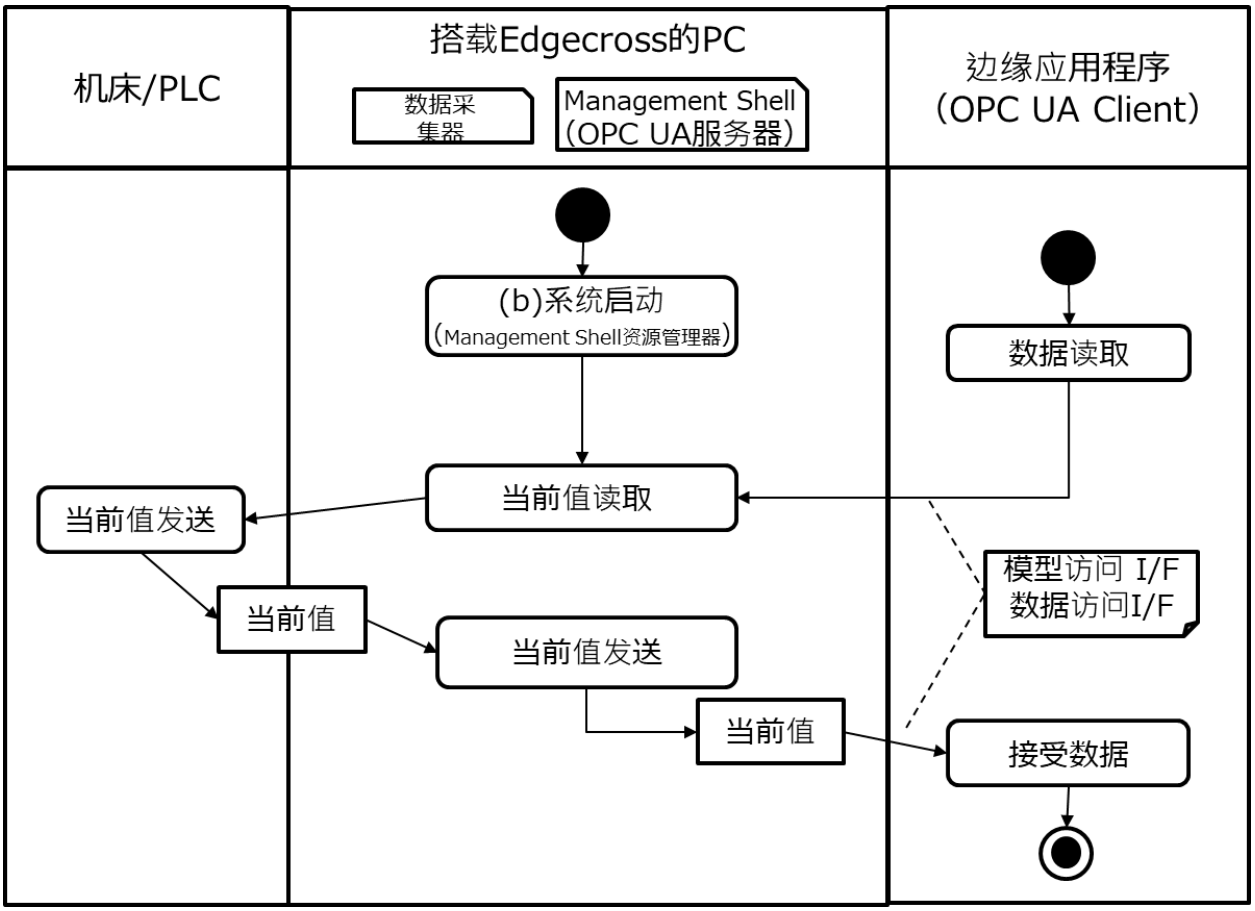
③ 使用 IT 网关的场合，进行网关设置。

④ 使用 OPC UA 的场合、进行 OPC UA 设置。

⑤ 根据使用的边缘应用程序，进行 OPC UA 通信的设置和数据模型的参照目标等必要的设置。

(c) 基于 OPC UA 的边缘应用程序（MES 服务器等）的数据访问

使用 Edgecross 的模型访问 I/F（OPC UA）、数据访问 I/F（OPC UA），边缘应用程序（MES 服务器等）参照机床/PLC 的当前值的事例。



※在这个事例中，为了使用 Management Shell，要事先启动（b）系统（使用 Management Shell 资源管理器的事例）。

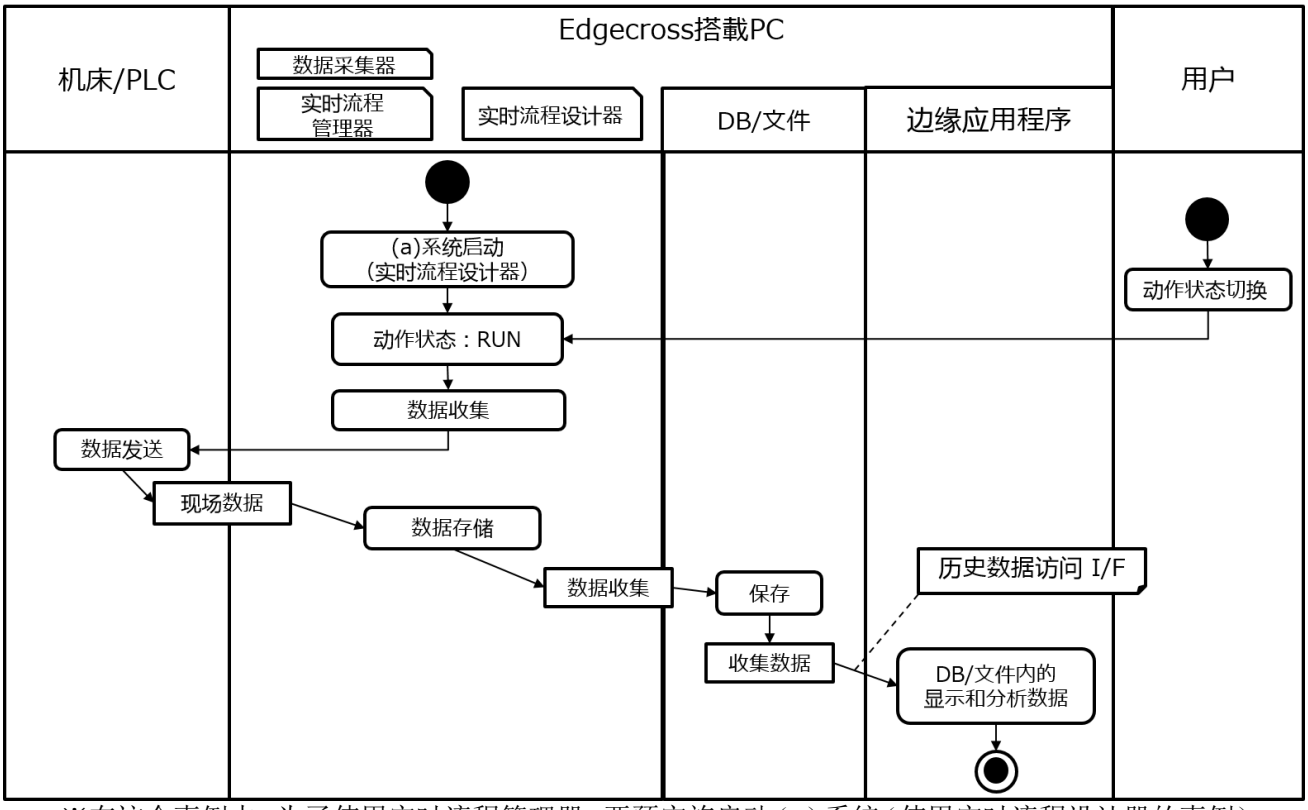
① 边缘应用程序通过模型访问 I/F 或数据访问 I/F，执行在 Management Shell 中读取数据。

② Management Shell 通过数据采集器，从机床/PLC 中读取当前值。

③ 将读出的当前值，发送给提出请求的边缘应用程序。

(d) 利用边缘应用程序中的历史数据

使用 Edgecross 历史数据访问 I/F，利用边缘应用程序对历史数据分析等事例。



※在这个事例中，为了使用实时流程管理器，要预实施启动（a）系统（使用实时流程设计器的事例）。

① 用户从实时流程设计器，把实时流程管理器的动作状态切换到 RUN。

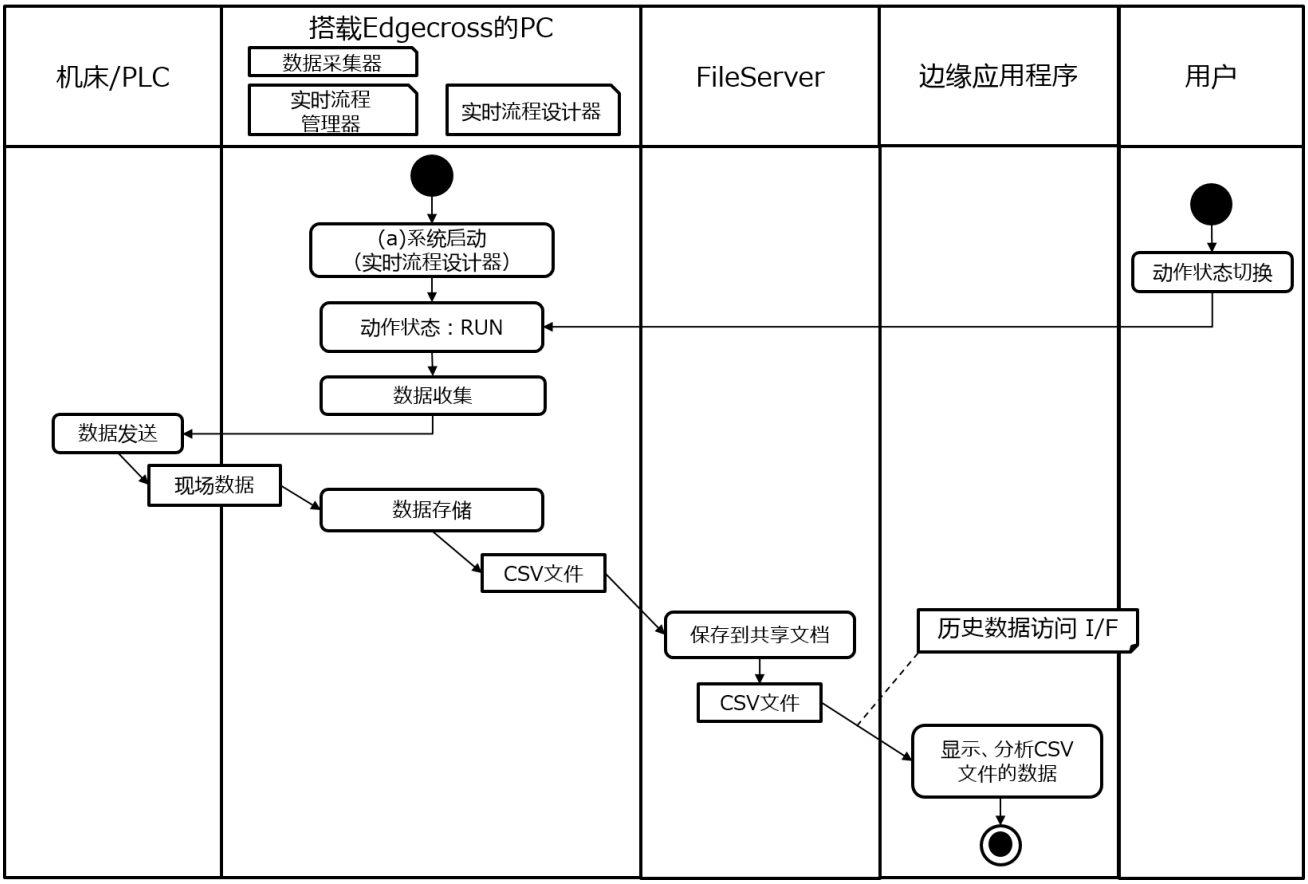
② 实时流程管理器通过数据采集器，从机床/PLC 进行数据收集。

③ 收集到的现场数据通过实时流程管理器的数据存储功能被保存到 DB/文件中。（※也有通过数据存储功能保存到文件中的事例。）

④ 边缘应用程序通过历史数据访问 I/F，从 DB/文件中获取收集数据，进行显示、分析等。

(e) FileServer 中的数据积累

实时流程管理器的数据存储功能将 CSV 文件保存在 FileServer 中的收集数据，用于边缘应用程序的分析等事例。



※在这个事例中，为了使用实时流程管理器，要预实施启动（a）系统（使用实时流程设计器的事例）。

① 用户从实时流程设计器，把实时流程管理器的动作状态切换到 RUN。

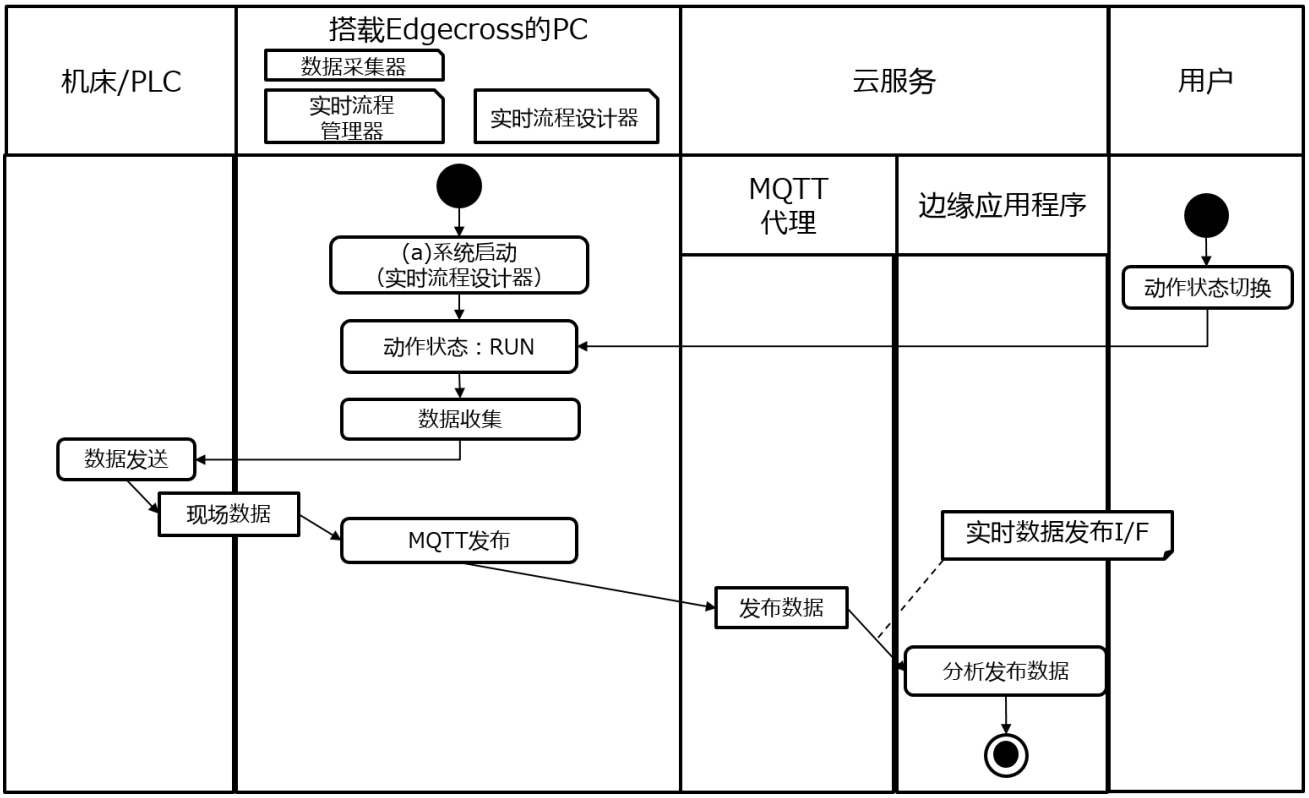
② 实时流程管理器通过数据采集器，从机床/PLC 进行数据收集。

③ 收集到的现场数据，通过数据存储功能，生成为 FileServer 共享文件夹上的 CSV 文件。

④ 边缘应用程序通过历史数据访问 I/F，从 FileServer 上的 CSV 文件取得收集数据，进行显示、分析等。

(f) 云服务中的数据分析

利用实时流程管理器的数据发送功能（MQTT 发送功能），在 MQTT 将数据集积到云服务中，用于实时数据发送 I/F 对应的边缘应用程序的分析等事例。



※在这个事例中，为了使用实时流程管理器，要预实施启动（a）系统（使用实时流程设计器的事例）。

① 用户从实时流程设计器，把实时流程管理器的动作状态切换到 RUN。

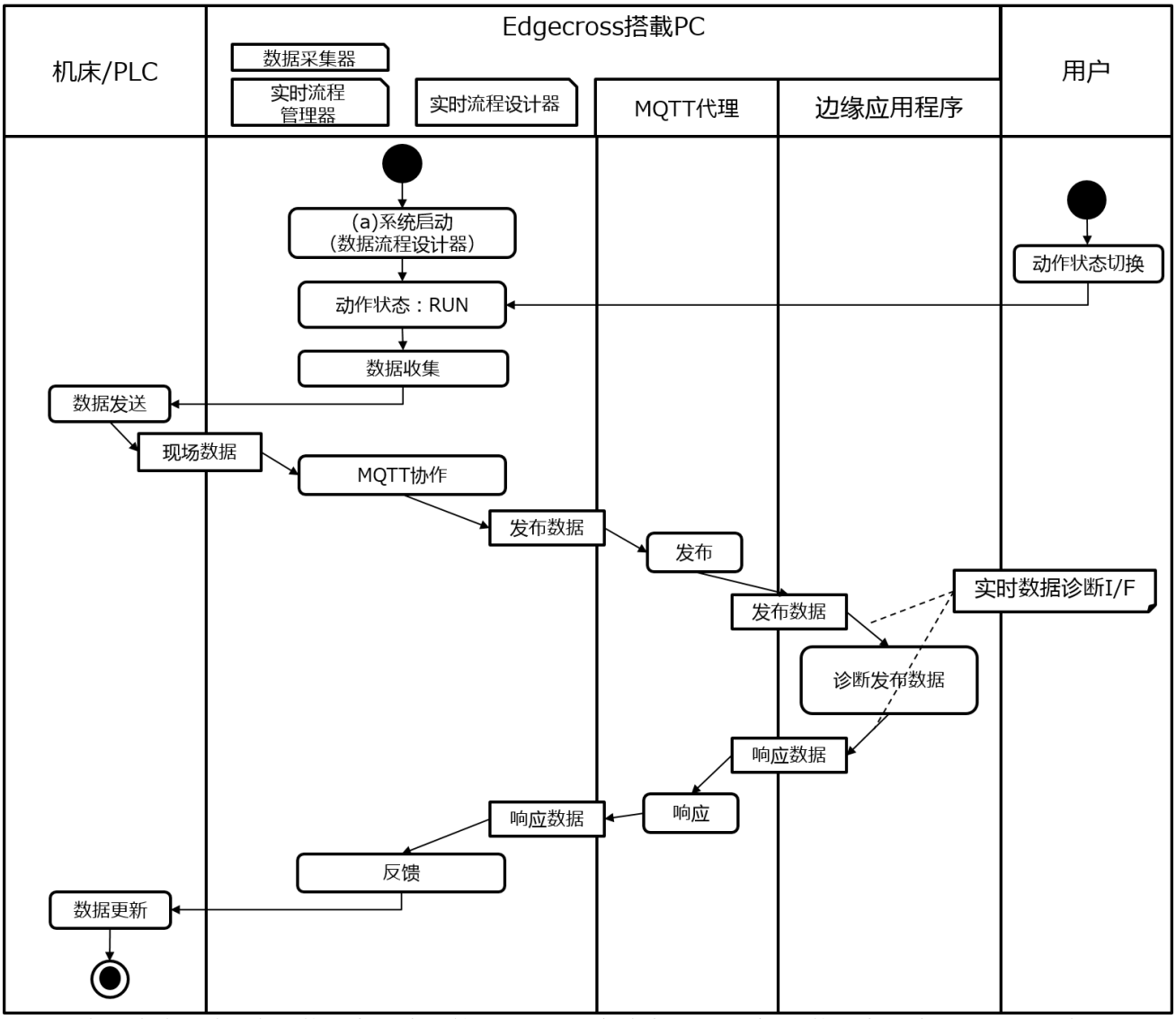
② 实时流程管理器通过数据采集器，从机床/PLC 进行数据收集。

③ 收集的现场数据，通过实时流程管理器的 MQTT 发送功能，被发送到云服务上的 MQTT 代理。

④ 云服务上的边缘应用程序，通过实时数据发送 I/F，从 MQTT 代理取得发送数据，进行显示、分析等。

(g) 来自边缘应用程序的反馈

执行实时流程管理器的数据诊断功能（MQTT 协作），向实时数据诊断 I/F（MQTT）对应的边缘应用程序发送数据，进行诊断和反馈的事例。



※在这个事例中，为了使用实时流程管理器，要预实施启动（a）系统（使用实时流程设计器的事例）。

① 用户从实时流程设计器，把实时流程管理器的动作状态切换到 RUN。

② 实时流程管理器通过数据采集器，从机床/PLC 进行数据收集。

③ 收集的现场数据，通过实时流程管理器的 MQTT 发送功能，被发送到 MQTT 代理。

④ 边缘应用程序，通过实时数据诊断 I/F，从 MQTT 代理接收分发数据，进行诊断。

⑤ 诊断完成时的响应数据，通过实时数据诊断 I/F，从边缘应用程序发送到 MQTT 代理。

⑥ 实时流程管理器，通过 MQTT 协作功能接收响应数据，通过反馈执行功能，通过数据采集器更新机床/PLC 的设备数据。

2.5.3 设想的威胁

2.5.1 在系统构成所示的用例中设想的威胁如表 2-2 所示。

该表中的威胁类别遵循 IPA 发行的《控制系统的安全风险分析指南第 2 版》中的威胁分类，图 2-5 所示为该指南中记载的威胁类别的因果关系。另外，模式 1、模式 2 分别表示 2.5.1 中记载的“大型工厂”、“小型工厂”， 在符合设想的威胁的模式上标记为 “〇”并记录为攻击表面。另外，为了指出针对各威胁的安全对策，记载了后述 3. 构筑的安全对策和 4. 运用的安全对策的相应章节编号。

以下，对表 2-2 的每个威胁类别都记载了概要和意外事件。另外，以搭载 Edgecross 的 PC 为中心的整体工厂的安全威胁，记载在附录里了。

(1) 非法访问

有恶意第三方通过网络侵入搭载 Edgecross 的 PC，执行对存储的信息进行窜改等攻击。

(2) 物理侵入

有恶意的第三方或蓄意的内部相关人员（员工或协力人员中，拥有访问搭载 EdgecrossPC 权限的人）非法侵入了被限制进出的配置了搭载 Edgecross 的 PC 场所。或者解除了设置有机架和箱子物理访问限制的，搭载 EdgecrossPC 的限制。

(3) 非法操作

(2) 之后，直接操作搭载 Edgecross 的 PC 的控制台等，执行从 Web 站点下载并安装非法软件等的攻击。

(4) 过失操作

诱发内部相关人员的过失操作，执行对搭载 Edgecross 的 PC 的 OS 进行非法设定等攻击。对于搭载 Edgecross 的 PC，连接了正规的 USB 存储器和 SD 卡等外部存储装置，结果无意中进行恶意软件的传播等攻击。

(5) 非法介质、机器连接

将有恶意的第三方或蓄意的内部相关人员非法带入的外部存储装置连接到搭载 Edgecross 的 PC 上，执行对生产信息和日志进行盗窃等攻击。

(6) 进程非法执行

(1), (3), (4) 非法执行位于攻击对象的搭载 Edgecross 的 PC 上的正规程序、命令、服务等过程。

(7) 恶意软件感染

(1), (3), (4), (5) 使恶意软件感染、运行在攻击对象的搭载 Edgecross 的 PC 上。

(8) 窃取信息

(6) 或(7) 盗窃搭载 Edgecross 的 PC 中存储的信息（生产信息、日志、软件、认证信息、构成设定信息、密码密钥等机密信息）。

(9) 信息篡改

(6)或(7) 篡改搭载 Edgecross 的 PC 中存储的信息。

(10) 破坏信息

(6)或(7) 破坏搭载 Edgecross 的 PC 中存储的信息。

(11) 非法发送

(6)或(7) 使得搭载 Edgecross 的 PC 向机床或 PLC 等装置发送不正确的控制命令（设定值变更、电源断开等）或非法数据（不正确的值、不正确的形式等）。

(12) 停止机器

(6)，(7)，(13) 使搭载 Edgecross 的 PC 的功能停止。

(13) 高负荷攻击

(7) 感染了恶意软件的搭载 Edgecross 的 PC，被胁迫参与 DDoS 攻击等，向 File Server 等其他设备发送大量数据，妨碍该设备的正常动作。另外，感染的恶意软件，会要求搭载 Edgecross 的 PC 运行超出处理能力的处理，妨碍该 PC 的正常运行。

(14) 盗窃

(2) 之后，盗窃搭载 Edgecross 的 PC。

(15) 通过盗窃、报废时分解窃取信息

(14) 之后，通过被盗的搭载 Edgecross 的 PC 和被分解报废的 PC，窃取保存在 PC 内部的信息。

(16) 窃听、通信数据篡改

有恶意的第三方，窃听或篡改搭载 Edgecross 的 PC-File Server 之间，网络上的通信信息。

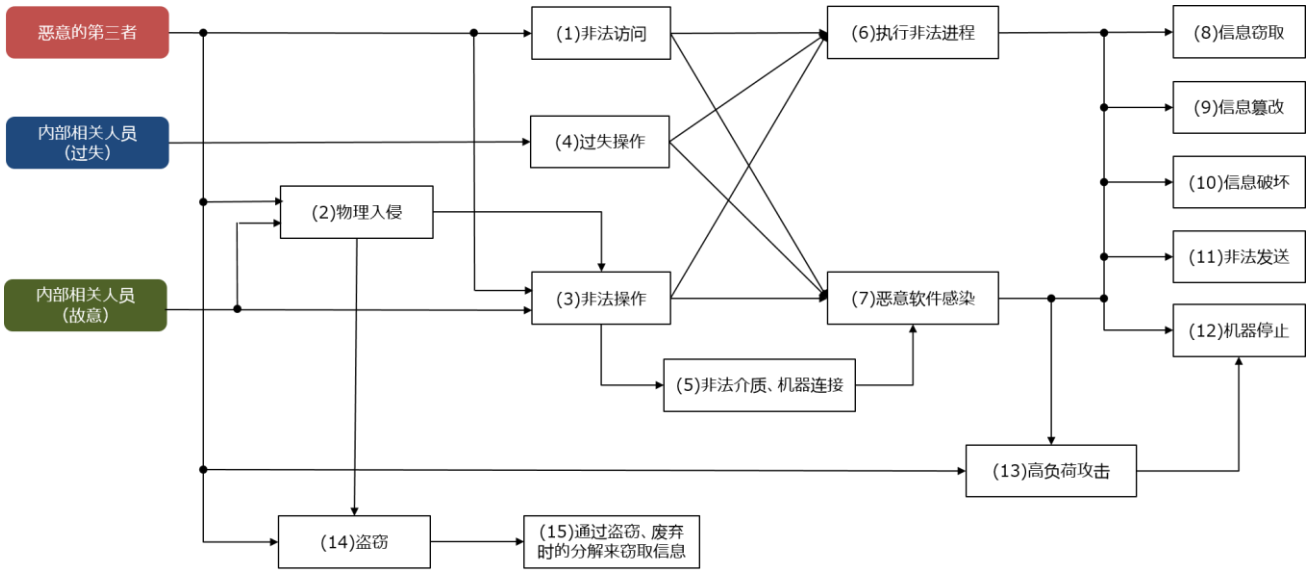


图 2-5 威胁类别的因果关系

表 2-2　Edgecross 用例中的设想威胁一览

No.	威胁类别	设想的威胁	STRIDE 分类 ※	模式1 (Attack Surface)	模式2 (Attack Surface)	对策
1	01. 非法访问	通过窃取密码或利用脆弱性等手段，从工厂外线路（互联网）非法访问搭载Edgecross的PC内部。	冒充	○ (互联网-Edgecross)+GG5:H40		3.2.2 (1)(3) 3.4.2 (1) 3.4.3 (1) 3.4.4 (1) 3.5 (4)(6)(12) 4.1
2		被从外部非法人员盗取的正规服务器、PC，非法访问搭载Edgecross的PC内部。	冒充	○ (服务器-Edgecross)		3.5 (5)
3		通过客户端PC等工厂内设备、非法连接的机器、工厂内感染的恶意软件等，从信息控制网络内非法访问搭载Edgecross的PC内部。	-	○ (机器-Edgecross)	○ (机器-Edgecross)	3.5 (5)(9)
4		即使对搭载Edgecross的PC有非法的访问和操作，也会因为发现的晚或遗漏而造成损失扩大。	-	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.5 (5)(6)
5		在能够远程操作搭载Edgecross的PC的终端上没有认证通信对象的机制，执行了非法的命令，搭载Edgecross的PC被非法操作。	冒充	○ (远程终端-Edgecross)	○ (远程终端-Edgecross)	3.5 (5)(12)
6		从冒充MES的攻击者那里，收到了对搭载Edgecross的PC的非法的指示。	冒充	○ (MES-Edgecross)	○ (MES-Edgecross)	3.5 (6)
7	02. 物理入侵	安装有能够远程操作搭载Edgecross的PC的终端的区域的出入规则，没有被恰当管理，由规定的作业员以外的人员非法操作搭载Edgecross的PC。	-	○ (远程终端-Edgecross)	○ (远程终端-Edgecross)	3.2.1 (2)
8	03. 非法操作	正规利用者离席过程中，操作中的搭载Edgecross的PC被没有操作权限的作业员访问。	冒充	○ (人-Edgecross)	○ (人-Edgecross)	3.2.2 (1)
9		能够远程操作搭载Edgecross的PC的终端被设置在没有专用的管理区域中，搭载Edgecross的PC被规定以外的工作人员非法操作。	冒充	○ (远程终端-Edgecross)	○ (远程终端-Edgecross)	3.2.1 (2) 3.4.2 (1) 3.4.3 (1)
10		让被允许作业的工作人员以外，偷窥了搭载Edgecross的PC画面。	-	○ (人-Edgecross)	○ (人-Edgecross)	3.2.1 (2)
11		由于冒充作业者的攻击者直接操作，非法的软件被安装在搭载Edgecross的PC上。	冒充	○ (人-Edgecross)	○ (人-Edgecross)	3.2.2 (1) 3.3.1
12		由于突破脆弱性的权限升级攻击，非法的软件被安装在了搭载Edgecross的PC上。	权限升级	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.3.1 3.4.4 (1) 4.1
13		工作人员将从互联网获取的非法软件安装到搭载Edgecross的PC上。	-	○ (人-Edgecross)		3.3.1 3.3.2
14	04. 错误操作	由于正规访问权限者的操作错误，导致搭载Edgecross的PC的异常设定、信息丢失、软件非当执行等的发生。	-	○ (人-Edgecross)	○ (人-Edgecross)	3.3.1
15	05. 非法介质、设备连接	将非法设备（USB设备、以太网设备、无线设备等）连接到搭载Edgecross的PC或搭载Edgecross的PC的外部通信路径，进行非法操作。	-	○ (机器-Edgecross)	○ (机器-Edgecross)	3.2.2 (2) 3.5 (3)(8)(11)(13)
16	06. 进程非法执行	由于非法访问、非法操作、恶意软件感染等，导致在搭载Edgecross的PC内并非本意的进程被执行。	-	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.4.3 (4)
17	07. 恶意软件感染	连接未进行安全检查的外部带入终端（维护终端），经由外部带入终端（维护终端），使搭载Edgecross的PC感染恶意软件。	-	○ (外部终端-Edgecross)	○ (外部终端-Edgecross)	3.3.1 3.5 (9)(12)
18		网络设备的空闲端口在可连接的状态下被放置，被连接非法终端，将恶意软件发送到搭载Edgecross的PC。	-	○ (机器-Edgecross)	○ (机器-Edgecross)	3.3.1 3.5 (5)
19		服务器上连接了未进行安全检查的外部介质（USB等）和外部带入终端（维护终端），通过这些使搭载Edgecross的PC感染了恶意软件。	-	○ (外部终端-Edgecross)	○ (外部终端-Edgecross)	3.3.1 3.5 (8)(9)(12)
20		通过从FileServer取得的文件，使搭载Edgecross的PC感染了恶意软件。	-	○ (FileServer-Edgecross)	○ (FileServer-Edgecross)	3.3.1 3.5 (4)(5)
21		通过从互联网获取的文件，使搭载Edgecross的PC感染了恶意软件。	-	○ (互联网-Edgecross)		3.3.1 3.5 (4)
22		搭载Edgecross的PC感染了恶意软件，感染范围扩大到其他机器，对生产产生了影响。	-	○ (Edgecross-机器)	○ (Edgecross-机器)	3.3.1 3.5 (5)
23		由于感染了恶意软件，非法的软件被安装在搭载Edgecross的PC上。	-	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.3.1
24	08. 窃取信息	非法访问、非法操作、恶意软件感染等，导致搭载Edgecross的PC内的信息被窃取/篡改/破坏。	信息泄漏	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.3.2
25	09. 信息篡改	由于冒充作业者的攻击者的直接操作，搭载Edgecross的PC的设置被非法变更。	篡改	○ (人-Edgecross)	○ (人-Edgecross)	3.3.2
26	10. 信息破坏	由于非法访问，删除了搭载Edgecross的PC内的必要的日志数据。	否认	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.3.1
27		通过删除搭载Edgecross的PC内的认证信息来妨碍服务。	-	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.3.1
28	11. 非法发送	通过搭载Edgecross的PC，向PLC输入了不合规的目标值，设备会执行非法动作从而被破坏。	-	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.4.2 (1)(2)(3) 3.4.3 (1)(2)(3)(5)(6) 3.5 (5)
29		搭载Edgecross的PC感染了恶意软件，执行了非法的指令，对生产产生了不良影响。	-	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.3.1 3.5 (5)
30		搭载Edgecross的PC感染了恶意软件向PLC发送了非法的指示。	-	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.3.1 3.5 (5)
31		由于感染了恶意软件，非法文件将从搭载Edgecross的PC上传到FileServer。	-	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.3.1 3.5 (4)(5)
32		通过伪装成作业员的攻击者的直接操作，非法文件将从搭载Edgecross的PC上传到FileServer。	冒充	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.2.2 (1) 3.5 (4)(5)
33		通过感染的恶意软件，搭载Edgecross的PC内的信息被发送到互联网外。	-	○ (Edgecross-互联网)		3.3.1 3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)(6)
34		通过伪装成工作人员的攻击者的直接操作，搭载Edgecross的PC内的信息被发送至互联网外。	冒充	○ (Edgecross-互联网)		3.2.2 (1) 3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)(6)(12)
35		将伪装成正规服务器、PC的服务器与PC连接起来，使搭载Edgecross的PC发送数据。	冒充	○ (Edgecross-服务器)	○ (Edgecross-服务器)	3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)
36	12. 功能停止	由于伪装成工作人员的攻击者的直接操作，使得搭载Edgecross的PC处于停止状态。	冒充	○ (人-Edgecross)	○ (人-Edgecross)	3.2.2 (1)
37		由于感染了恶意软件，搭载Edgecross的PC处于过载、停止状态。	-	○ (人/机器-Edgecross)	○ (人/机器-Edgecross)	3.3.1
38	13. 高负荷攻击	对IT网关和数据模型管理功能进行高负荷的通信，进行服务干扰。	DoS攻击	○ (互联网-Edgecross)	○ (互联网-Edgecross)	3.5 (4)(5)
39	14. 盗窃	被人为侵入工厂内，对搭载Edgecross的PC进行物理攻击、盗窃等。	-	○ (人-Edgecross)	○ (人-Edgecross)	3.2.1 (2)
40	15. 通过被盗、废弃时的分解来窃取信息	通过被废弃、盗窃的搭载Edgecross的PC的反向工程进行信息窃取。	信息泄漏	○ (人-Edgecross)	○ (人-Edgecross)	3.3.2
41	16. 窃听、通信数据篡改	从搭载Edgecross的PC向FileServer发送和接收的数据中发生泄漏和篡改。	信息泄漏 篡改	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.3.2
42	17. Windows相关	在未进行兼容性验证的情况下，执行未预期的WindowsUpdate，发生意外的Shutdown、Reboot，或在系统中发生故障。	-	○	○	3.2.2 (3) 4.1 (3)
43		执行WindowsUpdate，导致搭载Edgecross的PC的资源枯竭，不能执行必要的处理。	-	○	○	3.2.2 (3) 4.1 (3)
44		Windows测评进程的负荷过高，不能执行必要的处理。	-	○	○	3.2.2 (3) 4.1 (3)
45		不实施WindowsUpdate的话，已知的脆弱性会累积起来。	-		○	3.2.2 (3) 3.5 (7) 4.1 (3)
46		由于在Windows的支持服务结束后仍继续使用，已知的脆弱性会累积起来。	-	○	○	3.2.2 (3) 3.5 (7) 4.1 (3)

※STRIDE 是指，Spoofing(冒充)、Tampering(篡改)、Repudiation(否认)、Information disclosure(信息

泄漏)、Denial of service(DoS 攻击)、Elevation of privilege(权限升级) 的首字母构成了威胁分析手法之一。

3. 构筑的安全对策

3.1 要点

Edgecross 系统位于连接 FA 领域和 IT 领域的边界。因此，从安全的角度来看，必须考虑到生产现场设备和 IT 系统两方面的访问。

此外，用户可以在 Edgecross 基本软件中规定动作，再加上，通过组合数据采集器、边缘应用程序、插件等各种软件，可以构筑自由度高的系统。为了确保安全，构筑什么样的系统、如何保护，需要用户来主导。

在构建 Edgecross 系统时，请明确需保护的对象，并从以下(1)～(5) 的观点进行系统设计，予以保护该对象。

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

(1) 无论是个自还是整体都能保护的设计

对于通过外部接口/包含/物理接触产生的风险，请在各个机器、系统中探讨对策。另外，如果各个机器和系统无法对应，请在包含这些的上层 IoT 设备和系统中探讨对策。

(2) 不会给涉及对象造成困扰的设计

请进行可检测设备、系统异常的设计，探讨检测到异常时的适当处理。

(3) 确保实现安全安心的设计的一致性

为了实现安全安心，请进行可视化的设计。另外，请确认为实现安全安心的设计的相互影响。

(4) 即使和不特定的对象连接也能确保安全安心的设计

请探讨能根据机器和系统连接的对象和连接的状况来判断连接方法的设计。

(5) 实现安全安心的设计的验证和评价

连接的机器和系统，也要考虑到 IoT 特有的风险，请实现安全放心的设计的验证和评价。

为了减少威胁，最理想的考虑多层实施，在人的、物理的、甚至连接的网络等各种各样的对策。推荐客户导入以下安全对策。

3.2 硬件/OS

3.2.1 硬件

(1) 采购

Edgecross 可以安装在各种制造商的工业 PC 上。为了构建安全、安心的机器，请从十分可靠的供应商那里采购工业用 PC。

请确认供应商有设备支持的售后窗口，并且可以很容易地访问，机器的规格和固件的更新等技术信息已经公开。

另外，即使是值得信赖的制造商的产品，也请注意流通路径上发生问题的可能性。例如，考虑到有故意销售混入恶意软件的二手商品的情况。

Edgecross 协会，介绍了经 Windows 版 Edgecross 基本软件动作认证过的，推荐的工业用 PC。详情请参阅 Edgecross 协会主页 (https://www.edgecross.org/)。

(2) 设置

设置工业用 PC 时，请注意对物理攻击的防护。

・安全线的锁，或 PC 机架上锁而引发的物理盗窃的对策

・通过 USB/LAN 物理锁而产生的物理连接对策

・操作员的进出限制

这些对策会根据使用环境而变化，因此请根据环境来实施。

(3) 初期设定

与工业用 PC 安全有关的几个设定。请根据使用环境及要运行的软件进行适当的设定。下面列出代表性的设定项目。详情请参照工业用 PC 的手册等。

・BIOS 密码、HDD 密码等密码的设定

・启动驱动的设定

・USB 设定

・使 Wake on Lan 等外部控制成为可能的功能的设定

・TPM 等安全芯片的设定

※推荐使用 TPM。

(4) 更新

请适当升级 CPU 和芯片组的固件、BIOS、存储和网卡的固件和驱动程序等。获取升级软件时，请使用可靠的网站等，采取可确保不被篡改的手段。

另外，注意在各硬件出厂后到实际使用为止的期间内，固件等有可能被更新，

即使是最新的硬件，在构建时也请务必确认固件等的更新信息。

(5) 运用

请确认硬件（以及附带软件）的支持周期。推荐在支持期间内运用。

过了支持期不得不继续运用时，请在认识到当前设备的支持期已过的风险后进行适当的管理。

如果设备处于未使用状态，且被排除在管理对象之外的情况，非管理设备的运行可能会出现安全风险，请关闭该设备的电源。

3.2.2 OS

Edgecross 基本软件 Windows 版，在 Microsoft® Windows® 10 Operating System（以下称 Windows）上运行。本章，虽记载了关于 Windows 的运用的基本指导方针，但关于实际的实施内容请根据 Edgecross 机器的运用环境适当选择。

另外，Windows 的功能和用语等可能会在今后的升级中有所变更。详情请参照 Microsoft 的主页等信息。

(1) 账户和密码

Windows 具有对每个用户账户以及密码的管理功能。请根据用户的角色设定账户，同时设定他人难以推测的密码等，并实施适当的管理。

用户认证时，除了 Windows 账号和密码外，也可以使用 PIN 认证、生物识别认证、和结合这些的二级认证/多要素认证。

Windows 系统发生重要变更时，具备向管理者权限用户请求许可的安全功能（用户账户控制功能）。推荐将本功能设为有效。

Windows 具有记录各种用户名和密码的功能。如果将网络访问的资格信息、网页的用户名、密码等信息记录在系统内，可能会导致安全风险，所以不建议在非必要的情况下进行保存。

(2) 设定

Windows 包含着各种各样的应用程序和服务。在运用 Edgecross 时，建议把不需要的功能设置成无效。特别是请将相机功能和麦克风功能等 Edgecross 不需要的个性化功能无效化。另外，请尽量限制或禁用 USB 或蓝牙等外部的物理访问。

作为恶意软件对策，请使用安装在 Windows 上的安全功能，或者导入第三方的安全软件。另外，推荐使用个人防火墙来阻断不需要的网络访问。

(3) 更新

Windows 具有通过 Windows Update 应用更新程序，始终保持最新状态的功能。推荐在通用的使用环境中不断更新到最新的状态。

但是，更新程序中有需要重新启动的，也有更新时需要耗费时间的。因为有与运行环境相适应的或不合适的问题存在，所以建议在确认 Edgecross 实际运行没有问题后再更新。

在特定用途中使用的工业用 PC 等，将更新程序的应用暂时延期，先准备更新程序的运行验证用测试用机器等更为有效的对策。 Microsoft 公司提供 Windows Server Update Services (WSUS)，作为控制组织内的 Windows 更新程序的有效利用的解决方案。

选择 WSUS 作为 Windows 更新程序的来源时，使用组织策略将 Windows PC 设置为面向 WSUS 服务器。更新程序会定期从 Windows Update 下载到 WSUS 服务器，通过 WSUS 管理控制台或组织策略进行管理、承认、展开，企业更新程序的管理也会合理化。

如果不能及时的进行 Windows Update，可以通过利用下一代 IPS，通过虚拟补丁采取暂时的缓和对策。

3.3 安全软件

安全软件是用于计算机安全对策的应用软件的总称，防止恶意软件的入侵和由此而引起的感染，防止非法访问、信息窃取/篡改、以及成为对其他系统的攻击垫脚石的目的。向客户推荐在 Edgecross 基本软件及认证产品、推荐工业用 PC 等之中，导入适当的安全软件。

3.3.1 恶意软件对策软件

在具体的讨论时，有必要根据系统的用途和运用选择安全软件。作为恶意软件的对策软件，有以下方式，当作参考记述下来。详情请咨询产品销售方和销售代理店后，再进行导入。

黑名单方式

优势： 丰富的多层防御技术的安装。

弱点： 应对最新威胁的及时更新。以 OS 的支持生命周期为基准的产品支持。

白名单方式（根据特定用途化的锁定）

优势： 支持生命周期的长度。以系统更新周期为基准的更新。资源的平均化。

弱点： 与系统特性的匹配（频繁的执行文件的变更处理或有开头的情况等）

万一遇到感染了恶意软件等情况，和一般的 Windows 机器感染的情况一样，会产生例如下记的影响。在怀疑有这样的症状的情况下，有那种不需要安装应用程序就能确认有无恶意软件的 USB 型恶意软件检查和驱除工具，推荐可根据需要加以利用。

- 被安装了非法的软件
- 各种数据的篡改、消失、泄露
- 被当作攻击其他系统的垫脚石

在导入恶意软件对策软件后，推荐考虑以下 3 点。

(1) 协议的更新

对于恶意软件对策软件，根据许可协议，有 1 年或数年的使用期限限制的情况。为了在系统运转中能够继续使用，需要更新许可证协议。

(2) 更新

对于恶意软件对策软件，为了应对外部威胁的变化，有必要进行以提高功能为目的的更新。因为恶意软件的检测模式每天被更新的地方有很多，所以如果使用黑名单方式的恶意软件的对策软件的话需要定期更新。如果要使用白名单型的恶意软件的对策软件的时候，需要在系统修改的时点更新名单。当恶意软件对策软件的脆弱性被公开时，可能会另外提供产品版本升级和安全补丁。请考虑在注意脆弱性信息的基础上的适当应用。

(3) 系统扫描

定期扫描整个系统。扫描执行中 CPU 负荷变大，因此建议根据系统的运行状况来执行。有安装恶意软件对策软件的常驻型和不需要安装软件的非常驻型（USB 型恶意软件检查、恢复工具）等。

3.3.2 其它安全软件

推荐导入内置 OS 的个人防火墙和第三方通信接入控制软件作为非法访问和垫脚石的对策。

在信息窃取/篡改对策中，搭载 Edgecross 的 PC 与外部通信的对策，请参照 3．4 Edgecross 基本软件的通信加密。 对于搭载 Edgecross 的 PC 内部数据的情报窃取/篡改对策，推荐导入第三方的加密软件和防篡改软件。因此，Edgecross 系统的规模越大，加密密钥、证书的分发、管理、废弃越复杂，推荐可根据需要使用第三方密钥管理软件。

3.4 Edgecross 基本软件

3.4.1 构成

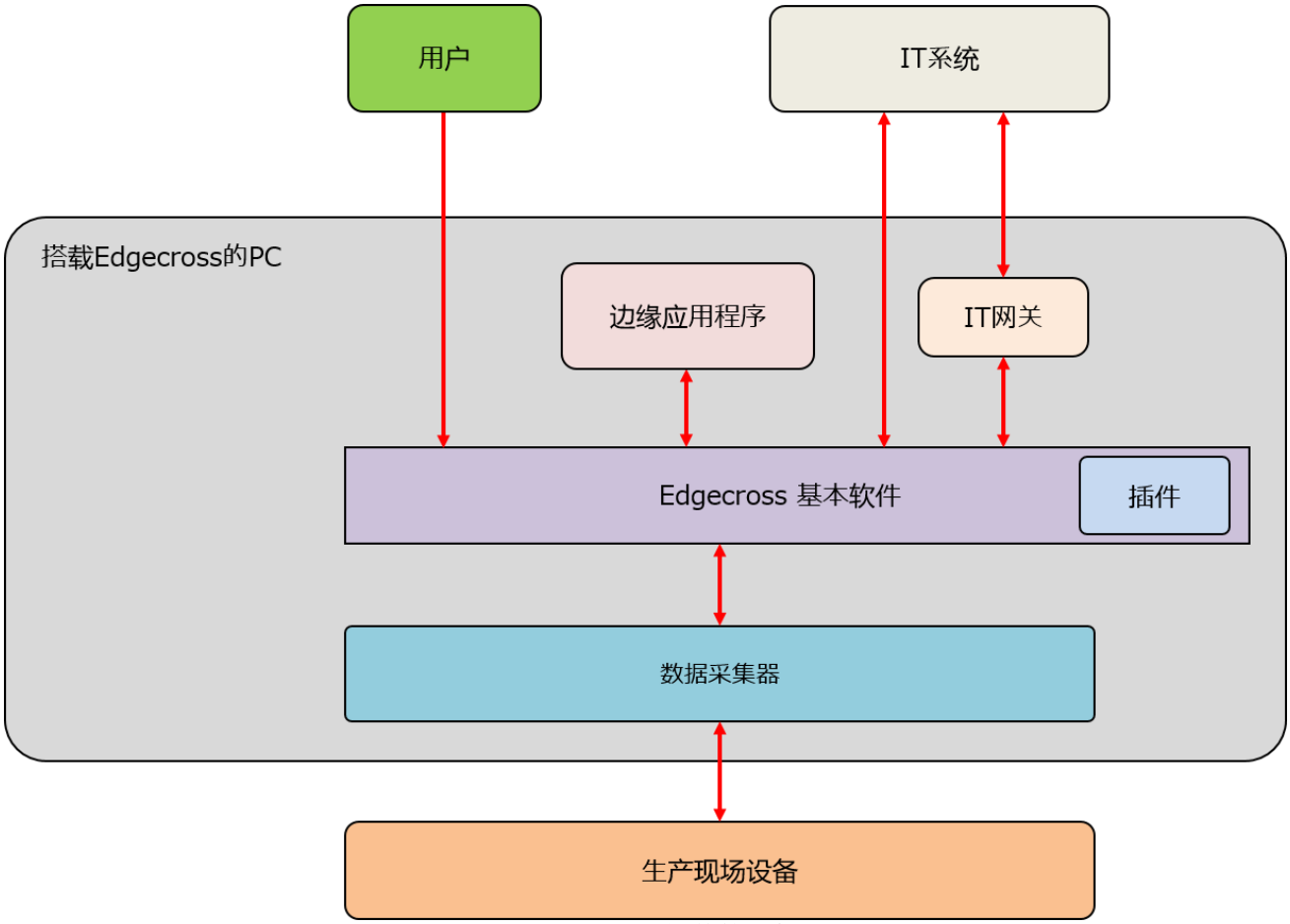


图 3-1 Edgecross 软件构成概要图

上图是 Edgecross 软件构成的概要图。

Edgecross 基本软件通过数据采集器，进行生产现场设备的数据收集和反馈。边缘应用程序对数据进行分析、诊断。另外，与外部 IT 系统之间进行数据交换。

数据采集器是可以直接控制生产现场设备的软件。数据采集器以及可访问数据采集器（通过 Edgecross 基本软件）的软件的边缘应用程序和 IT 网关，是足够可靠的软件，请使用。

从外部 IT 系统到 Edgecross 的访问有 2 种形式。

一种是直接访问 Edgecross 基本软件的形式。在这种形式下，通过向外部 IT 系统公开 Edgecross 基本软件和边缘应用的接口来实现。请留意向外部公开接口的安全风险。关于接口的详情，请参阅 3.4.2 数据模型管理及 3.4.3 实时数据处理。

另一种形式是，通过 IT 网关访问 Edgecross 基本软件。在这种形式下，通过 IT 网关访问 Edgecross 是被限制的。另外，如果 IT 网关具备安全功能，也可以利用该功能。

用户登录 OS 进行 Edgecross 基本软件的各种操作。

通过 Edgecross 基本软件的操作，不仅可以浏览信息，还可以通过数据采集器访问生产现场设备。 请留意，可访问 Edgecross 基本软件的用户，有可能访问生产现场设备（即，有非法操作生产现场设备的可能）。 Edgecross 基本软件没有控制每个用户账户的功能，因此请使用 OS 的账户控制。

表 3-1 Edgecross 基本软件的构成

机能	软件	内容
实时 数据处理	实时流程管理器	实现生产现场数据实时诊断、反馈功能的软件。 使用数据采集器（通过网络，收集生产现场数据的软件），可以收集连接的设备、装置或产线的数据，进行数据的加工和分析。另外，也可以使用插件来扩展功能。 将实时流程设计器作为Windows服务来启动/停止。
	实时流程设计器	安装了，实现了实时流程管理器的动作所需的各种设定的创建、保存、显示、实时流程管理器的运行开始/停止以及诊断功能的软件。
数据模型 管理	Management Shell	是对生产现场的设备、装置或生产线相关数据进行建模，并作为层次结构进行管理的软件。 可以进行利用数据采集器读取连接的设备、装置或生产线的数据，并写入数据。 将Management Shell资源管理器作为Windows服务来启动/停止。
	Management Shell资源管理器	进行Management Shell管理的数据模型的设置以及参考，负责Management Shell的运行开始/停止。

Edgecross 基本软件由上表的软件构成。详细内容，请通过 Edgecross 基本软件 Windows 版用户手册进行确认。

Edgecross 基本软件大致分为，实时数据处理和数据模型管理 2 种功能。下记对各个功能的详细内容和安全注意事项进行记述。

3.4.2 数据模型管理

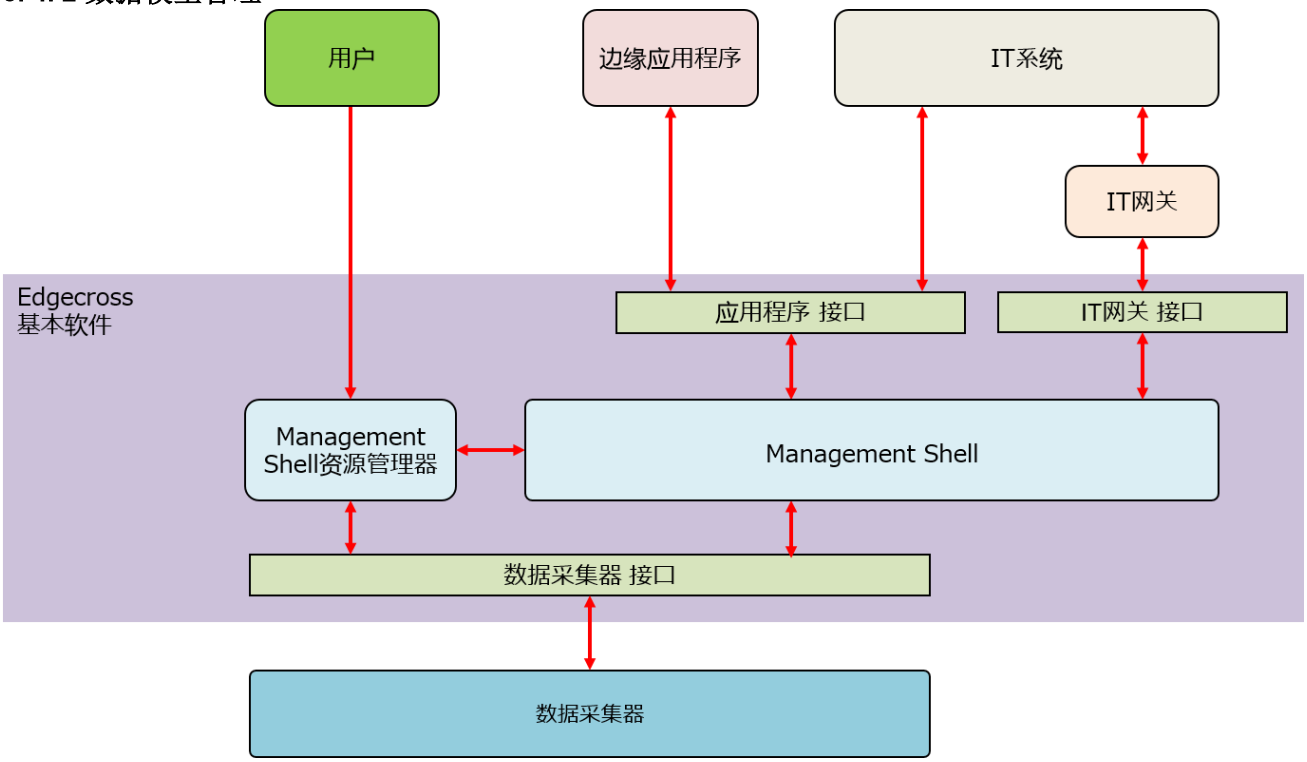


图 3-2 数据模型管理概要图

数据模型管理是将生产现场的设备、装置或生产线相关的数据建模，并作为层次结构进行管理的功能，可以使用数据采集器进行读取连接的设备、装置或生产线的数据，并写入数据。在安全方面，请留意具有能够通过数据采集器操作生产现场设备的能力。

执行数据模型管理的有用户、边缘应用程序、外部 IT 系统 3 个主体。

用户将 Management Shell 资源管理器作为用户界面进行操作。

边缘应用程序将 OPC UA 服务器作为应用程序接口进行操作。

外部 IT 系统将 OPC UA 服务器及 IT 网关作为接口进行操作。

(1) Management Shell 资源管理器

通过操作 Management Shell 资源管理器，可以设置以及参考 Management Shell 管理的数据模型。也就是说，可以从生产现场的装置、机器中，读取、写入数据。如果一旦 Management Shell 资源管理器被非法用户操作，可能会导致生产现场的停止和数据的泄漏、篡改等。作为对策，请设定为只有可信赖的用户，才能登录搭载 Edgecross 的 PC（登录 Windows）。

此外，Management Shell 的启动、停止，OPC UA 服务器的设定等，只有拥有 Windows 管理权限的用户（或者，知道管理者权限账户密码的用户）可以执行。

(2) OPC UA

Management Shell 作为 OPC UA 服务器运行，对于有 OPC UA 客户端的边缘应用程序，具有提供模型访问 I/F、数据访问 I/F 的功能（OPC UA 连接功能）。此时，可以进行边缘应用程序的客户端证书进行认证。另外，可以在通信中进行加密。

请留意 OPC UA 接口，也可通过数据采集器操作生产现场的设备。OPC UA 的客户端证书的所有者，也同样可以操作生产现场设备。

(3) 边缘应用程序

边缘应用程序，可以通过 OPC UA 进行数据模型管理的操作。另外，因为作为 Windows 上的应用程序运行，所以也可以进行数据模型管理以外的动作。如果导入了恶意的边缘应用程序，有可能会导致生产现场的停止和数据的泄漏、篡改等。

推荐从 Edgecross 销售网站等可靠供的应商处，获取边缘应用程序，。

(4) IT 网关

IT 网关是提供外部 IT 系统和 Edgecross 基本软件之间通信的软件组件。

如果可以利用 IT 网关，推荐上述 OPC UA 禁止外部对搭载 Edgecross 的 PC 的访问，并且在搭载 Edgecross 的 PC 内配置边缘应用程序。通过采用这样的结构，可以将外部 IT 系统对 Edgecross 的访问限定为通过 IT 网关，由此可以构建牢固的应对对外部访问的系统。IT 网关的使用方法，请从 IT 网关提供方处获取 IT 网关的手册。

3.4.3 实时数据处理

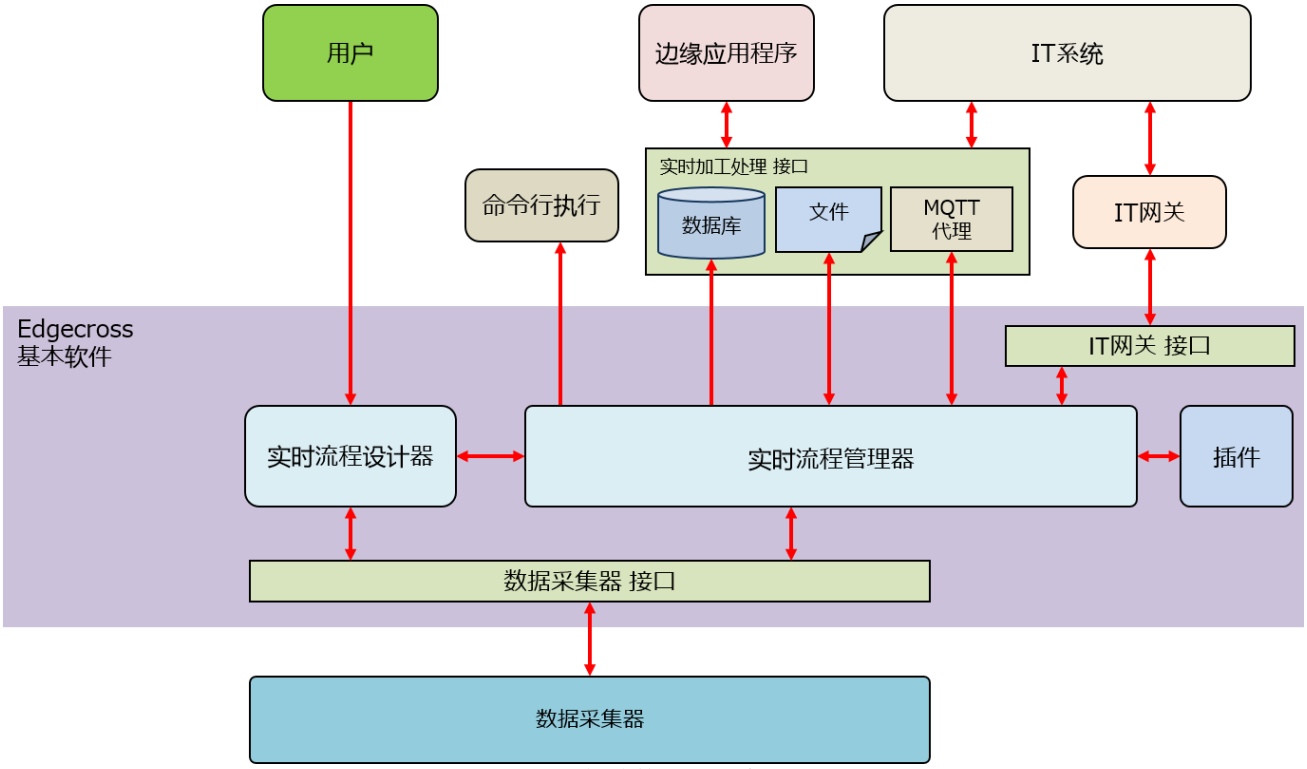


图 3-3 实时数据处理概要图

实时数据处理是从数据采集器收集生产现场的数据，进行数据的加工、分析。也可以将数据的加工、分析结果（通过数据采集器）反馈给生产现场设备。还可以和 IT 系统进行数据收发。此外，还具备在 OS 上执行命令行程序的功能。

实时流程管理器是负责数据流程的服务，用户通过实时流程设计制作动作流程。

通过导入边缘应用程序和插件，可以扩展数据加工和分析功能。

边缘应用程序通过 MQTT 和文件、数据库与实时流程管理器进行通信。

直接从实时流程管理器中调用插件。

外部 IT 系统和 Edgecross 基本软件通过与边缘应用程序相同的接口（MQTT、文件、数据库）以及 IT 网关进行通信。

实时数据处理也和数据模型管理一样，需要防备非法用户操作。此外，请留意实时数据处理是处理生产现场的数据以及加工过的数据，并进行动作。也就是说，除非法用户的操作外，还需要防备非法数据的非法访问。

例如，如果创建了通过数据采集器将发送给 MQTT 的数据传送给现场设备的流程，则可能会存在因向 MQTT 发送非法数据而导致现场设备的非法操作的危险性。在这种情况下，向现场设备发送的数据，需要采取防止非法数据访问的措施，就像为了限制在可靠的边缘应用程序内生成的正常数据而构建流程等。

(1) 实时流程设计器

用户可以通过操作实时流程设计器来创建实时流程管理器操作所需的各种设置。和数据模型管理一样，实时流程设计器被非法用户操作，如果实时流程管理器的设定被改写的话，有可能导致生产现场的停止、数据的泄漏、篡改等。作为对策，请设定为只有可信赖的用户才能登录搭载 Edgecross 的 PC（登录 Windows）。

(2) MQTT

MQTT 用于从实时流程管理器向边缘应用程序发送数据（收集数据、加工数据），以及从边缘应用程序接收响应数据。另外，也可用于与外部 IT 系统的通信。

虽然 MQTT 是广泛使用的通信标准，但是由于不恰当的设定等原因，经常会产生安全风险。有报告称，2018 年在互联网上发现了数万台处于脆弱状态的 MQTT 服务器（代理）。在 Edgecross 系统中，不仅有信息泄露，也有可能因非法数据注入导致现场设备的非法操作，因此请注意不要在脆弱的状态下公开 MQTT。

以下是 Edgecross 系统中 MQTT 的典型设置示例。

① 实时流程管理器和边缘应用程序之间的数据收发

将边缘应用程序和 MQTT 代理配置在搭载 Edgecross 的 PC 内，设定为不向 PC 外公开 MQTT（在个人防火墙中，禁止 MQTT 的 PC 内部方向的通信）。

② 向外部 IT 系统发送数据

在外部 IT 系统端配备 MQTT 代理，仅限于从 Edgecross 系统向外部 IT 系统的数据传输，并通过 TLS 对 Edgecross 和 MQTT 代理之间进行加密。

上述①②均构建为，不对外公开 Edgecross 系统端的 MQTT，避免向 Edgecross 系统注入数据。

(3) 文件/数据库

以文件和数据库为接口的通信与 MQTT 的通信具有相同的性质。也就是说，文件的公开有可能导致信息泄露，文件的写入有可能导致非法数据注入。文件/数据库的公开，请像 MQTT 一样慎重。

作为 Edgecross 基本软件的功能，可以将文件配置在远程共享文件夹中。请在共享文件夹中设置适当的用户账户/密码。

虽然也可以使用不使用用户账户的共享文件夹，但请注意远程共享文件夹的访问权为“ANONYMOUS LOGON”。 这意味着所有可访问远程 PC 的用户都可以在无认证的情况下访问文件。

建议不使用用户账户的远程共享文件夹只在十分可靠的网络内使用，或者不使用这样的远程共享文件夹。

(4) 命令行执行

实时流程管理器具有从命令行执行指定程序的功能。此外，可将诊断数据指定为程序参数。指定的程序以系统权限运行，因此搭载 Edgecross 的 PC 几乎都可以操作。

将诊断数据指定为参数并执行命令线程序的功能，从安全性角度来看，意味着攻击者有可能通过注入恶意数据来获得操作系统的机会。使用本功能时，请进行充分的讨论，请考虑恶意数据在程序中执行的可能性。

无法消除对数据注入攻击的担忧时，建议不要使用将诊断数据指定为程序参数的功能。

(5) 边缘应用程序

边缘应用程序通过 MQTT、文件、数据库，承担数据的加工、分析，因作为 Windows 上的应用程序运行，所以也可以进行数据加工、分析以外的动作。如果导入有恶意的边缘应用程序，有可能导致生产现场的停止、数据的泄露、篡改等。

边缘应用程序推荐从 Edgecross 销售市场等可靠供应商处获取。

(6) 插件

插件是在实时数据处理的执行控制下设置的、从实时数据处理中调用的软件。插件在系统权限下运行，大部分搭载 Edgecross 的 PC 都可以操作。如果混入了恶意插件，可能会导致生产现场停止、数据泄漏、篡改等。

建议从可靠供应商处获得插件，例如 Edgecross 销售市场等。

(7) IT 网关

IT 网关是提供外部 IT 系统和 Edgecross 基本软件之间通信的软件组件。

3.4.2(3) 与“IT 网关”中记载的内容相同，可通过 IT 网关构建通过外部 IT 系统访问 Edgecross 的牢固系统。IT 网关的使用方法，请从 IT 网关提供方获取 IT 网关的手册。

3.4.4 维护、运用

(1) 软件更新

因为最新的 Edgecross 基本软件包含了对已知的脆弱性的处理，所以请使用 Edgecross 基本软件的最新版。在版本升级过程中，建议在动作验证后再执行。另外，相关联的 OSS 也请进行脆弱性的对应。

详情请参照 4.1“脆弱性对策”。

(2) 历史保存

不仅在安全事件发生时，在故障和软件故障等发生时，事件信息也会带来很多有用的信息。Edgecross 系统的管理员，请检查事件信息的历史。

Edgecross 基本软件取得实时流程管理器、Management Shell 以及在这些使用的数据采集器中产生的事件信息，并将事件的履历和事件的详细信息、原因、处理方法显示为诊断信息。事件历史记录是，即使关闭了运行实时流程管理器的工业 PC 的电源也会被保存，因此可以在重新启动工业 PC 后进行确认，或者通过确认前后的操作信息来追究问题发生的原因的时候进行使用。另外，发生错误时无法确认错误代码时也可以使用。

3. 5 网络

作为应保护资产的安全对策，有关高效利用网络的技巧如下所示。

[网络安全对策位置的示例]

图 3-4 是展示网络安全对策位置的事例。

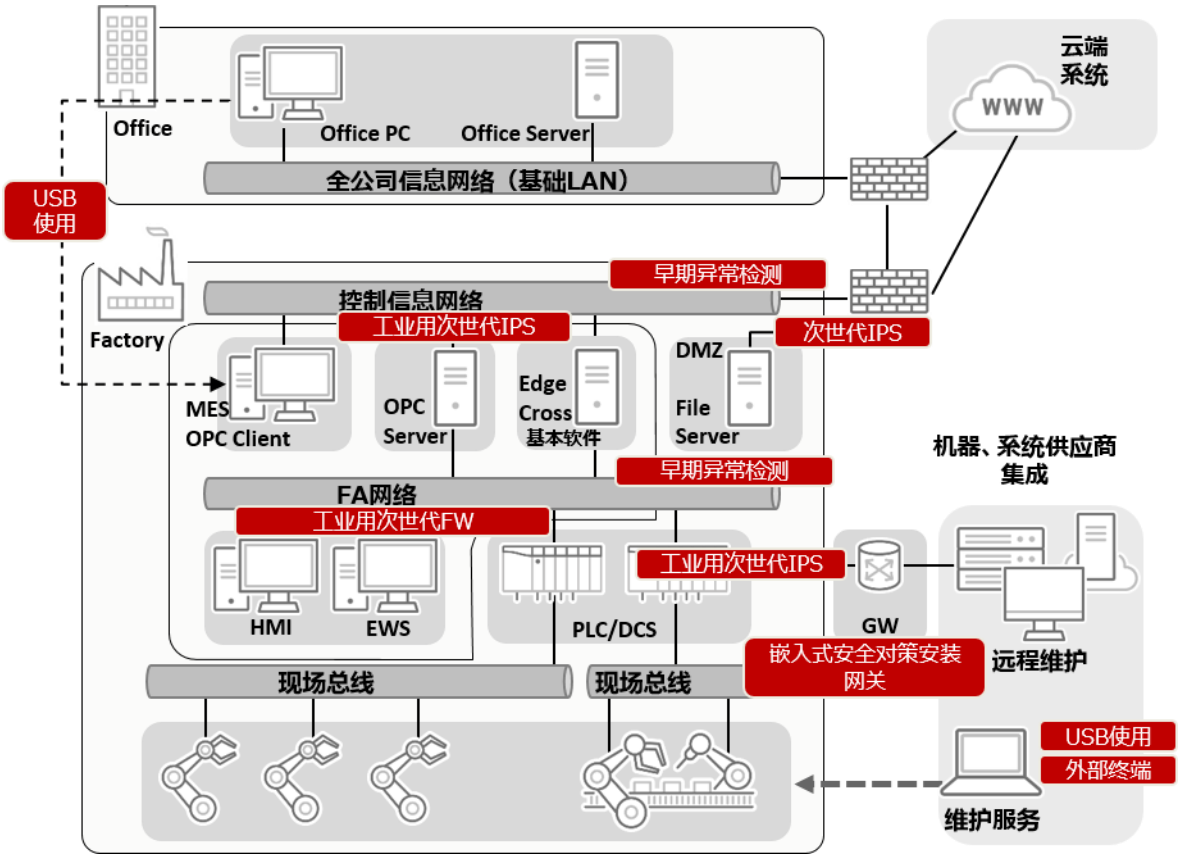


图 3-4　网络安全对策位置示例

[网络上的对策]

将工厂内存在的网络按照利用位置分为“控制信息网络”“FA 网络”“现场总线”来进行分层说明。

(1) 方针对策

在网络上，通过采取防止感染、感染后的检测，在终端一侧执行对感染状况的确认、检测、消除的对策，最大限度地消除与网络连接时产生的风险是有必要的。

(2) 资产管理

如果把握不住应该保护的资产，产生安全对策遗漏，会出现发生意外时不能迅速确认状况的可能性。因此，需要列出控制信息网络、FA 网络上的设备或该设备所使用的应用程序（通信协议）等信息，制作资产管理一览表。推荐在不影响现有系统和现有网络的情况下，从通信分组的监视器等设备中检测出网络上的设备，并设置可进行资产管理的网络可视化装置。

(3)　网络构成管理

如果不能掌握网络的构成，发生突发事件时，有可能无法迅速确认影响范围。因此，需要制作能够了解控制信息网络、FA 网络的物理构成、逻辑构成、数据流等的网络构成图。推荐设置网络监视装置和网络可视化装置，可以通过通信数据包的监视器和 SNMP 等数据收集来绘制网络构成图。

(4) 网络边界对策

连接工厂出入口的控制信息网络和普通的全公司信息系统网络（以下称为 IT 系网络）时，为了防止恶意软件从 IT 系网络进入，要设置防火墙装置（以下称为 FW 装置）。另外，不仅仅是单纯的 FW 装置的设置，鉴于控制信息网络下属的产业控制系统的脆弱性对策等，推荐追加防止侵入系统（下一代 IPS），或者安装搭载了与此相同功能的下一代 FW。

(5) 早期异常检测对策

在控制信息网络中，考虑到网络上的设备万一感染了恶意软件时，建议设置内部对策装置（网络攻击检测传感器），通过网络通信检测非法行为和异常，使风险威胁和对应优先度可视化。

(6) 非法通信检测对策

在工厂网络的运用中，除了人为的失误之外，也可以预想到由于带有恶意的相关人员而导致陷入严重事态的情况。另外，在导入对策方面，必须要考虑不给现有的系统和网络增加负担，并可后续简单导入，避免涉及过高的网络知识、消耗设定工时等。通过防止错误操作和可疑通信，具备自动生成设置功能的白名单（访问许可列表）的开关策略，是有效的。外部攻击自不必说，还可以防止未被允许的内部访问。

(7)追求长期可用性的通用 OS 所使用的 SCADA 和 HMI（平板电脑等），对 IPC 的对策

根据设备的不同，也有使用系统资源有限的平板电脑等来运行 SCADA 和 HMI 的情况。对于视情况而难以追加安全对策软件的控制终端，作为替代方案，推荐在装置的 LAN 端口上进行产业用次世代 IPS 的连接。由此，不仅实施了脆弱性对策的缓解措施，还通过活用与产业控制协议和控制命令对应的协议白名单功能，可以采取将安装了 Edgecross 基本软件的 IPC 的上位通信，只可限制为 MQTT 和 OPC-UA 的对策。

(8) USB 使用对策

即使将作为恶意软件进入路径的 IT 系网络用 FW 装置阻断，也需要早期异常检测对策，是因为在通过 Edgecross 的设置而使机器之间网络连接的情况下，现场运行所使用的 USB 设备的进入路径并不会消失。

即使开始了经由网络的信息收集，从所有的点也很难去除对 USB 的运用，而且，即使去除，在那个完成之前也需要一定程度的时间，所以在现场环境存在 USB 设备的情况下，执行使用 USB 设备的数据收集的重点是，需要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。

在使用不需要安装的工具的背景下，通过安装恶意对策软件来抑制对终端造成负荷影响的作用，也因此会有，在制造商提供的嵌入式终端等，不允许安装恶意软件的情况。

(9) 便携 PC 对策

有报告称，工厂工作人员将感染了恶意软件的私人电脑连接到工厂内的网络，导致公司内部感染扩大的事件。不仅要限制文档的安全操作规则，还要限制与工厂网络的连接。为了保护工厂网络，不影响现有网络结构，防止未注册的终端和注册 NG 的终端的连接的网络型的对策是有效的。通过将未注册的个人电脑和私人智能手机等从工厂网络中阻断，保护工厂网络免受非法访问、恶意软件感染而引起的信息泄露。

(10)铺设网络的引进设计的重要性

到目前，所记述的对策是在向现有环境铺设网络时，在了解网络状态的情况下采取的对策。

・不太清楚网络环境现状

・以设备为单位构建了最适合各自的网络环境，但那些不能相互连接

・现在开始新铺设网络

以引进 Edgecross 为契机，在推进工厂的网络化的情况下，为了有效且安全地利用网络，需要考虑从设备之间的 IP 地址重复状态到不变更地址而有效地连接设备之间的方法，以及防止恶意软件扩散目的的微处理器需要专用的网络设计方法。

因此，推荐向 IP 网络构筑专业的集成，传达网络导入的目的和未来的利用方式，并使依托实现的网络的设计、构筑成为可能。

(11) 无线网络

由于 AGV 等无线通信威胁无线信号的扩散，因此建议在工厂网络环境内设置无线信号。

(12) 机器、系统集成供应商的维护服务

为了确保在大规模网络环境中提供维护服务时的安全性，建议将远程 GW 的连接作为最低限度，采取以下防御措施。

1. Dynamic virtual private network (D-VPN)的利用
2. 连接设备的白名单访问控制
3. 通过产业用次世代 FW 和 GW 的互联网连接

另外，系统集成供应商进行维修服务时，最好与工厂负责人协商，限制时间。

图 3-5 所示为最小构成的面向网络的安全对策位置示例。

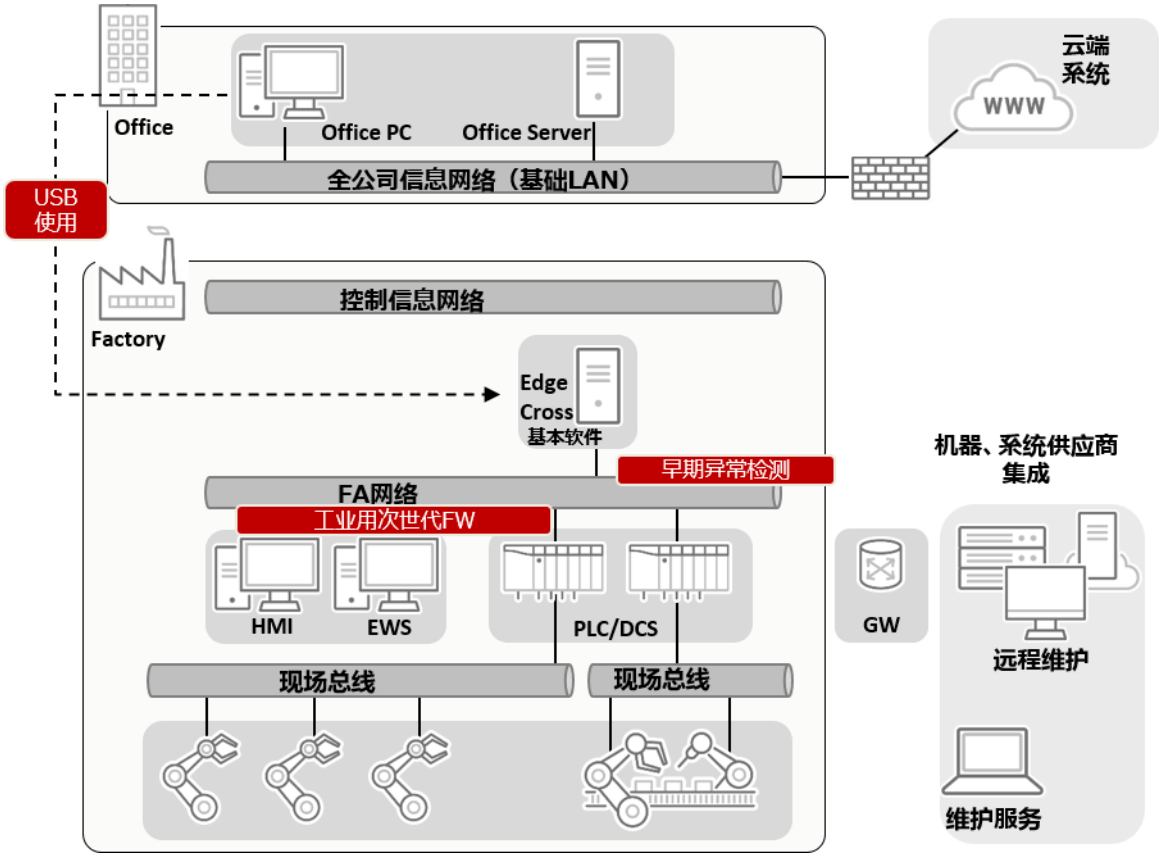


图 3-5　最小构成的面向网络的安全对策位置示例

[网络上的对策]

将工厂内存在的网络按照利用场所分为“控制信息网络”“FA 网络”“现场总线”进行分层说明。

(1) 方针对策

在导入初期，在构成单独的网络而没有网络连接的阶段，对在 office-Factor y 之间为了取得数据而使用的 USB 的对策，以及在使用 USB 等时假想感染的情况下早期异常检测为目的的产业用下一代 FW 对策。

关于具体的对策，请确认前述所示的 USB 对策及早期异常检测对策。

4. 运用中的安全对策

在运用之前，在整理上述的构成管理、利用者/运用者/管理者、访问管理、日志管理等的同时，在运用开始后除了这些管理之外，还要继续实施脆弱性/威胁信息收集、脆弱性管理等安全管理是非常重要的。另外，为了迅速应对突发事件，需要完善监视、异常检测、问题应对（应急、永久）、恢复体制。

以下将详细说明脆弱性对策及安全管理、事件应对。

4.1 脆弱性对策

近年来，由于恶意软件入侵工厂现场，并进行扩散活动而导致工厂停产的案例屡屡发生。恶意软件从USB 设备和带入的机器侵入，利用网络上的机器的脆弱性，意图对其他的机器扩大感染。

为了抑制恶意软件的感染和扩散活动，需要适当执行各设备的 OS 和应用程序等资产管理，并及时应用安全补丁。

进行对导入 Edgecross 基本软件的工业 PC 软件的版本管理，并根据需要实施 Edgecross 基本软件、OS、其他应用程序的更新等，可以应对脆弱性。以下是关于各部位更新的考量。

(1) Edgecross 基本软件

为了消除脆弱性，请使用 Edgecross 基本软件的最新版。建议在动作验证后，进行安全补丁的适配和版本升级。

Edgecross 基本软件的最新版在 Edgecross 的销售市场上进行公开，请参考。

Edgecross 基本软件 Windows 版相关的 OSS 如下表所示。

从安全的角度来看，最好做了动作确认，并且使用新的版本。

另外，在所使用的 OSS 被公开了脆弱性的情况时，Edgecross 协会将尽快实施动作确认，尽量迅速公开信息。

OSS 的使用形式有 2 种。

一种是将 OSS 源代码和程序库导入 Edgecross 基本软件中所使用的形式。在这种形式的 OSS 上脆弱性被公开，如果需要处理时，则需要升级 Edgecross 基本软件。请参照 Edgecross 基本软件更新时的 Edgecross 协会对应。

另一个是在 Edgecross 基本软件以外独立运行的 OSS。这个形式的 OSS 的脆弱性的处理被委托给用户。 请获取 OSS 的信息，执行动作验证后，进行更新工作。

还有最新的信息请在下面确认。

https://www.edgecross.org/ja/data-download/

表 4-1 Edgecross 基本软件的相关 OSS 一览表

	OSS 名称	使用形式
1	Eclipse Mosquitto	在 Edgecross 基本软件内使用
2	OpenSSL	在 Edgecross 基本软件内使用
3	PostgreSQL	Edgecross 基本软件以外
4	PSQLODBC.DLL	Edgecross 基本软件以外
5	pthread	在 Edgecross 基本软件内使用

(2) 边缘应用程序以及数据采集器

边缘应用程序以及数据采集器，由 Edgecross 的会员企业开发，请从开发方和销售市场获取相关，采取脆弱性对策。

推荐在动作验证的基础上，进行安全补丁的适配和版本升级。

Edgecross 销售市场：

https://www.marketplace.edgecross.org/

(3) OS

Windows 具备通过 Windows Update 进行应用程序的更新，始终保持最新状态的功能。推荐在通用的使用的环境中，总保持更新到最新的状态。

但是，更新程序中有需要重新启动的，也有需要耗费更新时间的。因为存在与动作环境相适应的问题，也有不适合的问题，所以建议在确认 Edgecross 实际运用没有问题后再更新。

在特定用途中使用的工业用 PC 等，将更新程序的应用暂时延期，为更新程序的动作验证准备测试用机器等对策是行之有效的。 Microsoft 公司提供 Windows Server Update Services (WSUS) 作为控制组织内 Windows 更新程序应用的解决方案。

选择 WSUS 作为 Windows 更新程序的来源时，使用组织策略将 Windows PC 设置为面向 WSUS 服务器。更新程序会定期从 Windows Updat 下载到 WSUS 服务器，通过 WSUS 管理控制台或组织策略进行管理、承认、展开，企业更新程序的管理也会合理化。

(4) 硬件、BIOS、驱动

工业用 PC 和与其连接的装置的 BIOS 和驱动，有脆弱性的话也必须对应。推荐从开发方获取信息，在动作验证后，进行适配。

4.2 安全管理、意外事件应对

设想在 Edgecross 系统内，存在多种类型的机器，还有 10 年以上的长期使用的机器和系统。系统内的机器的追加和设置的更新，网络环境的变更等，伴随着很多环境变化的脆弱性的发生而感到担忧。并且，即使不进行机器的变更，也会发现新的脆弱性。

在开始运用 Edgecross 系统后，继续进行安全管理和对应也很重要。在整个系统中，存在着各种机器的管理者、网络管理者、系统的运用者、软件和机器的供应厂商等很多相关人员。请事先整理相关人员的职责，组织好安全管理和应对措施。

・请考虑并应用，在必要的时间，机器安全上的重要的更新等的恰当的执行方法。

・请 Edgecross 系统的构筑人员和运用人员，收集、分析系统的脆弱性信息，并向相关人员发送信息。

・请向相关人员告知，因不小心连接到系统而产生的风险和希望其遵守的事项。

・请整理 Edgecross 系统的各种机器制造商、提供者、系统管理者和操作者等相关人员的职责。

・请构建把握有脆弱性机器的机制，并有组织地进行定期监视。

・如果查明了具有脆弱性的设备，请向相应机器的管理者提起注意，尽量实施脆弱性应对。

参考:「IoT 安全指南　ver 1.0」
2.5 【运用、维护】 指针 5 维持安全安心的状态，进行信息发送和共享

请事先配备迅速应对突发事件的体制。

・请建立确认 3．4 Edgecross 基本软件历史记录和**エラー！ 参照元が見つかりません。** 网络日志等的机制，定期监视，尽早检测事件发生。另外，由于要求高度专业性的监视，所以在人员难以确保的情况下，也可以活用外部的 SOC 服务。

・检测意外事件时，请根据事先准备好的应对步骤，将损害控制在最小限度。

・请通过与相关人员的联络、协作，迅速查明意外事件的原因并进行修复作业。

5. 总结

为了确保使用 Edgecross 的 FA 系统的安全、安心，请活用本指南。

此外，如有关于本书记述的疑问，请在 Edgecross 协会主页的咨询表格中填写并咨询。

Edgecross 协会咨询表格　https://www.edgecross.org/ja/contact/form/

附页(资产一览表)
式样1

No.		1	2	3	4	5	6	7	8	9
资产名		进度管理用电脑	笔记本电脑(无线连接)	防火墙(因特网)	防火墙(管理楼)	防火墙(工厂)	File Server	MES Server	MES Client	工程用PC
资产类别	信息类资产	○	○				○	○	○	○
	控制类资产									
	网络资产			○	○	○				
资产所具有的功能	输入/输出	○	○				○	○	○	○
	数据存储						○			
	命令发布							○	○	○
	门			○	○	○				
线路类别		LAN(有线)	LAN(有线／无线)	LAN／WAN(有线)	LAN／WAN(有线)	LAN／WAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)
安装位置		管理楼	管理楼		管理楼	工厂(DMZ)	工厂(DMZ)	工厂(DMZ)	工厂	工厂
连接到NW	信息网络	○	○	○	○					
	DMZ			○		○	○	○		
	控制信息网络			○		○			○	○
	控制网络									
	控制器间网络									
	因特网		○	○	○	○				
管理端口的连接目标		×	×	信息网络	信息网络	DMZ	×	×	×	×
是否有操作I/F		○	○	×	×	×	○	○	○	○
USB端口/送信I/F的利用		○(USB)	○(USB)	○(LAN)	○(LAN)	○(LAN)	○(USB)	○(USB)	○(USB)	○(USB)
是否稳定运用介质、设备连接		×	×	×	×	×	×	×	×	×
是否有无线功能		×	○	×	×	×	×	×	×	×
稳定运转、非稳定运转		稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转
数据类型和路径		另行记载								
构建供应商/设备制造商		A公司／X公司	A公司／X公司	A公司／Y公司	A公司／Y公司	A公司／Y公司	A公司／X公司	A公司／X公司	A公司／X公司	A公司／X公司
OS类型/版本		Windows 10	Windows 10	独立OS	独立OS	独立OS	Windows Server 2016	Windows Server 2016	Windows 10	Windows 10
要使用的协议		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP
安全策略(※)		设备连接和使用限制[19],权限管理[23]	设备连接和使用限制[19],权限管理[23]	FW(数据包过滤型)[1]	FW(数据包过滤型)[1]	FW(数据包过滤型)[1]	设备连接和使用限制[19],权限管理[23]	设备连接和使用限制[19],权限管理[23]	设备连接和使用限制[19],权限管理[23]	设备连接和使用限制[19],权限管理[23]

※IPA记载“控制系统的安全风险分析指南第2版”的“表4-29安全对策项目一览表”的安全对策

附页(资产一览表)
式样1

No.		10	11	12	13	14	15	16	17	18
资产名		路由器	Edgecross 搭载PC 1	Edgecross 搭载PC 2	HMI	PLC	控制机器 1	控制机器 2	工作机械 1	工作机械 2
资产类别	信息类资产		○	○						
	控制类资产				○	○	○	○	○	○
	网络资产	○								
资产所具有的功能	输入/输出		○	○	○					
	数据存储									
	命令发布		○	○	○	○				
	门	○								
线路类别		LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)
安装位置		工厂	工厂	工厂	工厂	工厂	工厂	工厂	工厂	工厂
连接到NW	信息网络									
	DMZ									
	控制信息网络	○		○		○				
	控制网络	○	○						○	○
	控制器间网络				○	○	○	○		
	因特网		○	○						
管理端口的连接目标		控制信息网络	×	×	×	×	×	×	×	×
是否有操作I/F		×	○	○	○	×	×	×	○	○
USB端口/送信I/F的利用		○(LAN)	○(USB)	○(USB)	×	×	×	×	×	×
是否稳定运用介质、设备连接		×	○	○	×	×	×	×	×	×
是否有无线功能		×	×	×	×	×	×	×	×	×
稳定运转、非稳定运转		稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	定常稼働	稳定运转
数据类型和路径		另行记载								
构建供应商/设备制造商		A公司／Y公司	A公司／X公司	A公司／X公司	A公司／Z公司	A公司／Z公司	A公司／Z公司	A公司／Z公司	A公司／Z公司	A公司／Z公司
OS类型/版本		独立OS	Windows 10	Windows 10	独立OS	独立OS	独立OS	独立OS	独立OS	独立OS
要使用的协议		TCP,UDP	TCP,UDP	TCP,UDP	CC-LinkIE	TCP,UDP,CC-LnkIE	CC-LinkIE	CC-LinkIE	TCP,UDP	TCP,UDP
安全策略(※)			设备连接和使用限制[19], 权限管理[23]	设备连接和使用限制[19], 权限管理[23]						

附页(资产一览表)
式样2

No.		1	2	3	4	6	7	8	9	10
资产名		办公用PC	工程用PC	File Server	生产管理应用程序	L2 Switch	Edgecross搭载PC	工作机械1	工作机械2	工作机械3
资产类别	信息类资产	○	○	○	○		○			
	控制类资产							○	○	○
	网络资产					○				
資産の持つ機能	输入/输出	○	○	○	○		○			
	数据存储			○						
	命令发布		○		○		○			
	门					○				
线路类别		LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)	LAN(有线)
安装位置		办事处	办事处	办事处	办事处	工厂	工厂	工厂	工厂	工厂
连接到NW	信息网络									
	DMZ									
	控制信息网络	○	○	○	○	○	○	○	○	○
	控制网络									
	控制器间网络									
	因特网									
管理端口的连接目标		×	×	×	×	×	×	×	×	×
是否有操作I/F		○	○	○	○	×	○	×	×	×
USB端口/送信I/F的利用		○(USB)	○(USB)	○(USB)	○(USB)	×	○(USB)	×	×	×
是否稳定运用介质、设备连接		×	×	×	×	×	○	×	×	×
是否有无线功能		×	×	×	×	×	×	×	×	×
稳定运转、非稳定运转		稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转	稳定运转
数据类型和路径		別途記載								
构建供应商/设备制造商		A公司／X公司	A公司／X公司	A公司／X公司	A公司／X公司	A公司／Y公司	A公司／X公司	A公司／Z公司	A公司／Z公司	A公司／Z公司
OS类型/版本		Windows 10	Windows 10	Windows 10	Windows 10	独立OS	Windows 10	独立OS	独立OS	独立OS
要使用的协议		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP
安全策略		设备连接和使用限制[19],权限管理[23]	设备连接和使用限制[19],权限管理[23]	设备连接和使用限制[19],权限管理[23]	设备连接和使用限制[19],权限管理[23]		设备连接和使用限制[19],权限管理[23]			

※IPA记载“控制系统的安全风险分析指南第2版”的“表4-29安全对策项目一览表”的安全对策

附页（攻击脚本）式样1

※1：攻击据点是指，可以对攻击对象进行最终攻击的机器和场所
※2：攻击对象是指，假定为最终攻击对象的机器

No.	事业损失	事业损失级别	事业损失的概要和攻击脚本							
1	停止广域的产品供应	3	事业损失的概要	由于对制造设备等的网络攻击，在广域内发生产品停止供应，给社会带来巨大影响， 产生赔偿费用等高额损失，同时本公司的信赖也大幅下降。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点（※1）	攻击对象（※2）	最后攻击	可用性	完整性	机密性
			1-1	由于MES Server与各装置之间的通信干扰，使生产管理数据消失，无法进行制造工序的管理、对作业者的指示，导致生产停止。	信息网络 DMZ 控制信息网络	MES Server	由于MES Server和各装置之间的通信干扰， 使生产管理数据消失	○	○	－
			1-2	MES Server感染了恶意软件，导致生产管理数据消失，无法对制造工序的管理、作业人员进行指示，导致生产停止。	因特网 信息网络 DMZ 控制信息网络	MES Server	MES Server感染了恶意软件，生产管理数据消失	○	○	－
			1-3	搭载Edgecross的PC感染了恶意软件，实行了停产操作，导致生产停止。	因特网 DMZ 控制信息网络 控制网络	Edgecross搭載PC	搭载Edgecross的PC感染了恶意软件，执行生产停止操作	○	－	－
2	停止在限定地区的产品供应	2	事业损失的概要	由于对制造设备等的网络攻击，在限定地区发生供应停止，对社会产生影响， 产生赔偿费用等损失，同时本公司的信赖度降低。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点（※1）	攻击对象（※2）	最后攻击	可用性	完整性	机密性
			2-1	搭载Edgecross的PC上安装了未许可的应用程序， 导致处理性能发生故障，访问发生延迟。	控制信息网络 控制网络	搭载Edgecross的PC	搭载Edgecross的PC上安装了未许可的应用程序。	○	○	－
			2-2	由于HMI感染了恶意软件，导致无法进行监视操作等作业，因此一部分生产停止。	控制器间网络	HMI	HMI感染了恶意软件，使监视操作等作业无法进行	○	－	－
			2-3	对系统的脆弱性的认识不够充分，处于还残留着脆弱性的状态， 系统脆弱性受到攻击。	因特网	搭载Edgecross的PC	由于服务器和控制机器的不合规操作，工厂停止	○	－	－
			2-4	工作人员等的身份确认和行动监视不够充分，受到内部工作人员等的攻击。	控制信息网络 控制网络	搭载Edgecross的PC	由于服务器和控制机器的不合规操作，工厂停止	○	－	－
			2-5	由于内部线路的管理不够充分，被擅自接入不合规的外部线路，受到通过监管外的外部网络进行的不合规的连接和攻击。	因特网	搭载Edgecross的PC	由于服务器和控制机器的不合规操作，工厂停止	○	－	－
			2-6	由于连接到外部网络的信息系统终端的安全策略不够充分，因此通过信息系统终端，导致对设施内的攻击。	因特网	搭载Edgecross的PC	由于服务器和控制机器的不合规操作，工厂停止	○	－	－
			2-7	外部连接用网络设备的安全对策不够充分，受到通过外部网络连接的攻击。	因特网	搭载Edgecross的PC	由于服务器和控制机器的不合规操作，工厂停止	○	－	－
			2-8	搭载Edgecross的PC未设置专用的管理区划，导致规定的作业员以外的人员进行不合规操作。	控制信息网络 控制网络	搭载Edgecross的PC	由于不合规操作导致工厂停止、设定值被窜改、信息泄露等的发生	○	○	○
			2-9	未妥善管理搭载有Edgecross的PC所设置区划的进出，被规定的作业者以外的人员进行不合规操作。	控制信息网络 控制网络	搭载Edgecross的PC	由于不合规操作导致工厂停止、设定值被窜改、信息泄露等的发生	○	○	○
			2-10	搭载Edgecross的PC没有认证通讯对象，执行了不合规的命令，被进行了不合规的操作。	因特网 DMZ 控制信息网络 控制网络	搭载Edgecross的PC	由于不合规操作导致工厂停止、设定值被窜改、信息泄露等的发生	○	○	○

附页（攻击脚本）式样1

※1：攻击据点是指，可以对攻击对象进行最终攻击的机器和场所
※2：攻击对象是指，假定为最终攻击对象的机器

No.	事业损失	事业损失级别	事业损失的概要和攻击脚本							
3	规格不良产品的供应	2	事业损失的概要	由于对制造设备等的网络攻击，给顾客提供了不符合规定规格的产品，对社会造成影响， 产生赔偿费用等损失的同时，降低了对本公司的信赖。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点（※1）	攻击对象（※2）	最后攻击	可用性	完整性	机密性
			3-1	由于MES Server感染了恶意软件，所以生产管理数据被窜改，制造工序的管理、对作业者的指示变为无意义的指示，导致供应规格不良的产品。	因特网 信息网络 DMZ 控制信息网络	MES Server	MES Server感染了恶意软件，篡改了生产管理数据	○	○	－
			3-2	MES Client通过感染恶意软件，生产管理数据被篡改，对制造工序的管理、对作业者的指示变为无意义的指示，导致供应规格不良的产品。	DMZ 控制信息网络 控制网络	MES Client	MES Client感染了恶意软件，篡改了生产管理数据	○	○	－
4	设备的破坏	3	事业损失的概要	由于对制造设备等的网络攻击，设备被破坏，供应停止发生的同时，出现了员工和附近居民的死伤， 给社会带来很大的影响，产生赔偿费用等高额损失的同时，也大大降低了对本公司的信赖。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点（※1）	攻击对象（※2）	最后攻击	可用性	完整性	机密性
			4-1	通过向PLC输入不合适的目标值， 设备的控制发生异常，设备被破坏。	控制信息网络 控制器间网络	PLC	向PLC输入不正确的目标值	○	○	－
			4-2	由于工程PC感染了恶意软件，所以被设定为不合适的工程， 设备控制异常，各设备被破坏。	DMZ 控制信息网络 控制网络	工程PC	工程PC感染了恶意软件， 工程设定被窜改	○	○	－
			4-3	对于HMI的脆弱性的认识不够充分，处于还残留着脆弱性的状态， 系统脆弱性受到攻击。	控制器间网络	HMI	HIM的停止导致了无监视状态的发生	○	－	－
			4-4	对于终端设置场所，未对被许可的进出者进行限制管理， 被规定的作业者以外的人偷看画面、进行不合规操作。	工厂	工程PC	由于不合规操作导致设备停止、设定值被窜改、信息泄露等的发生	○	○	○
			4-5	系统的权限管理和作业监视不充分，规定的作业员越权， 对系统和终端/控制盘进行不正当操作。	工厂	工程PC	由于不合规操作导致设备停止、设定值被窜改、信息泄露等的发生	○	○	○
			4-6	HMI的登录管理和登录信息的管理不充分， 被正规的作业员以外的人进行不合规登录和操作。	工厂	HMI	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
			4-7	HMI的权限管理和作业监视不充分，规定的作业员越权， 对系统和终端进行不合规操作。	工厂	HMI	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
			4-8	在未进行安全确认的USB等外部介质连接时， 被恶意软件通过外部介侵入。	外部介质	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-9	在连接未进行安全确认的外部带入终端时， 被恶意软件通过外部带入终端侵入。	外部带入终端	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-10	网络设备的空闲端口在可连接的状态下被放置， 被不合规终端连接，并导入恶意软件。	FW的空白端口	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-11	由于对服务器的脆弱性的认识不够充分，处于还残留着脆弱性的状态， 系统脆弱性受到攻击。	因特网 信息网络 DMZ 控制信息网络	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-12	PLC没有认证通信对象的机制，执行了不合规的命令， 被迫执行不合规的动作。	控制信息网络 控制器间网络	PLC	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
			4-13	PLC的ID和密码未被适当设置，容易被侵入者访问，进行不合规操作。	工厂	PLC	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
			4-14	对机床和控制机器的脆弱性的认识不够充分，处于脆弱性残留的状态， 系统脆弱性受到攻击。	控制网络 控制器间网络	机床、 控制机器	因攻击导致机床、控制机器的停止	○	－	－
			4-15	网关设备没有限制通信目标的机制，执行了不合规的命令， 被迫进行不合规的动作。	控制信息网络 控制网络	路由器	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
			4-16	各种控制盘、配电盘上有在业界广泛通用的钥匙，容易被开锁，被规定的作业者以外的人员进行不合规操作。	工厂	各装置	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
			4-17	开关等网络设备的设置场所处于未被安全管理、任何人都可以接触的状态， 被规定的作业者以外的人员进行不合规操作。	工厂	FW,路由器	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－

附页(攻击脚本)式样1

※1:攻击据点是指，可以对攻击对象进行最终攻击的机器和场所
※2:攻击对象是指，假定为最终攻击对象的机器

No.	事业损失	事业损失级别	事业损失的概要和攻击脚本							
5	大规模对策费用的产生	1	事业损失的概要	受到网络攻击，虽然没有发生产品停止供应的灾害，但是现行对策的脆弱性变得明显，为了解决这个问题而产生了庞大的对策费用。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
			5-1	由于维护等原因在不知道与外部连接的情况下连接，通过管理外的外部网络连接，受到恶意软件感染和非法侵入。	因特网	MES Server	由于恶意软件感染和非法侵入而发生数据被篡改和信息泄露	-	○	○
			5-2	防火墙的安全措施不充分，受到通过外部网络连的入侵。	因特网	MES Server	由于非法侵入而发生数据被篡改和信息泄露	-	○	○
			5-3	由于云服务器的信用信息管理不充分而流出，被非法访问。	因特网	云上的服务器	由于非法侵入而发生数据被篡改和信息泄露	-	○	○
6	机密信息的泄露	1	事业损失的概要	_				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
			6-1	通过物理侵入工厂内或通过互联网窃取MES Server的生产数据，使机密信息泄漏到外部。	因特网 工厂	MES Server	提取MES Server的生产数据	-	-	○
			6-2	物理侵入工厂内，或者通过互联网从FileServer中窃取机密信息，泄露到外部。	因特网 工厂	FileServer	从FileServer中窃取机密信息	-	-	○
			6-3	物理侵入工厂内，或者通过互联网从搭载Edgecross的PC中窃取机密信息，泄露到外部。	因特网 工厂	搭载Edgecross的PC	从搭载Edgecross的PC上窃取机密信息	-	-	○

附页（攻击脚本）式样2

※1:攻击据点是指，可以对攻击对象进行最终攻击的机器和场所
※2:攻击对象是指，假定为最终攻击对象的机器

No.	事业损失	事业损失级别	事业损失的概要和攻击脚本							
1	停止广域的产品供应	3	事业损失的概要	由于对制造设备等的网络攻击，在广域内发生产品停止供应，给社会带来巨大影响， 产生赔偿费用等高额损失，同时本公司的信赖也大幅下降。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
			1-1	由于生产管理应用程序和各装置之间的通信干扰，使生产管理数据消失，无法进行制造工序的管理、对作业者的指示，生产停止。	控制信息网络	生产管理 应用程序	由于生产管理应用程序和各装置之间的通信干扰，使生产管理数据消失	○	○	－
			1-2	由于生产管理应用程序感染了恶意软件，生产管理数据消失，制造工序的管理、对作业者的指示变得不能进行，制造停止。	控制信息网络	生产管理 应用程序	生产管理应用程序感染了恶意软件，生产管理数据消失	○	○	－
			1-3	搭载Edgecross的PC感染了恶意软件，实行了停产操作，导致生产停止。	控制信息网络	搭载Edgecross的PC	搭载Edgecross的PC感染了恶意软件，执行生产停止操作	○	－	－
2	停止在限定地区的产品供应	2	事业损失的概要	由于对制造设备等的网络攻击，在限定地区发生供应停止，对社会产生影响， 产生赔偿费用等损失，同时本公司的信赖度降低。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
			2-1	搭载Edgecross的PC上安装了未许可的应用程序， 处理性能发生故障，访问发生延迟。	控制信息网络	搭载Edgecross的PC	搭载Edgecross的PC上安装了未许可的应用程序	○	○	－
			2-2	工作人员等的身份确认和行动监视不够充分，受到内部工作人员等的攻击。	控制信息网络	搭载Edgecross的PC	由于服务器和控制器的非法操作，工厂停止	○	－	－
			2-3	搭载Edgecross的PC未设置专用的管理区划，导致规定的作业员以外的人员进行不合规操作。	控制信息网络	搭载Edgecross的PC	由于不合规操作导致工厂停止、设定值被窜改、信息泄露等的发生	○	○	○
			2-4	未妥善管理搭载有Edgecross的PC所设置区划的进出，被规定的作业者以外的人员进行不合规操作。	控制信息网络	搭载Edgecross的PC	由于不合规操作导致工厂停止、设定值被窜改、信息泄露等的发生	○	○	○
			2-5	搭载Edgecross的PC没有认证通讯对象，执行了不合规的命令，被进行了不合规的操作。	控制信息网络	搭载Edgecross的PC	由于不合规操作导致工厂停止、设定值被窜改、信息泄露等的发生	○	○	○
3	规格不良产品的供应	2	事业损失的概要	由于对制造设备等的网络攻击，给顾客提供了不符合规定规格的产品，对社会造成影响， 产生赔偿费用等损失的同时，本公司的信赖度降低。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
			3-1	由于生产管理应用程序感染了恶意软件，生产管理数据被窜改，制造工序的管理，对作业者的指示成为无意的指示，导致供应规格不良的产品。	控制信息网络	生产管理 应用程序	生产管理应用程序感染了恶意软件，篡改了生产管理数据	○	○	－

附页（攻击脚本）式样2

※1:攻击据点是指，可以对攻击对象进行最终攻击的机器和场所
※2:攻击对象是指，假定为最终攻击对象的机器

No.	事业损失	事业损失级别	事业损失的概要和攻击脚本							
4	设备的破坏	3	事业损失的概要	由于对制造设备等的网络攻击，设备被破坏，供应停止发生的同时，出现了员工和附近居民的死伤， 给社会带来很大的影响，产生赔偿费用等高额损失的同时，也大大降低了对本公司的信赖。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
			4-2	由于工程PC感染了恶意软件，所以被设定为不合适的工程， 设备控制异常，各设备被破坏。	控制信息网络	工程PC	工程PC感染了恶意软件， 工程设定被窜改。	○	○	－
			4-4	对于终端设置场所，未对被许可的进出者进行限制管理， 被规定的作业者以外的人偷看画面、进行不合规操作。	工厂	工程PC	由于不合规操作导致设备停止、设定值被窜改、信息泄露等的发生	○	○	○
			4-5	系统的权限管理和作业监视不充分，规定的作业员越权， 对系统和终端/控制盘进行不正当操作。	工厂	工程PC	由于不合规操作导致设备停止、设定值被窜改、信息泄露等的发生	○	○	○
			4-8	在未进行安全确认的USB等外部介质连接时， 被恶意软件通过外部介侵入。	外部介质	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-9	在连接未进行安全确认的外部带入终端时， 被恶意软件通过外部带入终端侵入。	外部带入终端	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-10	网络设备的空闲端口在可连接的状态下被放置， 被不合规终端连接，并导入恶意软件。	L2 Switch的空白端口	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-11	由于对服务器的脆弱性的认识不够充分，处于还残留着脆弱性的状态， 系统脆弱性受到攻击。	因特网 信息网络 DMZ 控制信息网络	搭载Edgecross的PC	搭载Edgecross的PC的停止、设定被篡改、信息泄露等的发生	○	○	○
			4-14	对机床和控制机器的脆弱性的认识不够充分，处于脆弱性残留的状态， 系统脆弱性受到攻击。	控制信息网络	机床	因攻击导致机床的停止	○	－	－
			4-16	各种控制盘、配电盘上有在业界广泛通用的钥匙，容易被开锁，被规定的作业者以外的人员进行不合规操作。	工厂	各装置	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
			4-17	开关等网络设备的设置场所处于未被安全管理、任何人都可以接触的状态， 被规定的作业者以外的人员进行不合规操作。	工厂	L2 Switch	由于非法操作导致设备停止或设定值被窜改的发生	○	○	－
5	大规模对策费用的产生	1	事业损失的概要	受到网络攻击，虽然没有发生产品停止供应的灾害，但是现行对策的脆弱性变得明显， 为了解决这个问题而产生了庞大的对策费用。				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
6	机密信息的泄露	1	事业损失的概要	_				受影响 A、I、C		
			脚本#	攻击脚本	攻击据点(※1)	攻击对象(※2)	最后攻击	可用性	完整性	机密性
			6-1	由于物理侵入工厂内，从File Server中获取机密信息，并泄漏到外部。	工厂	File Server	从File Server中窃取机密信息	－	－	○
			6-2	由于物理侵入工厂内，从搭载Edgecross的PC中获取机密信息，并泄漏到外部。	工厂	Edgecross搭载PC	从搭载Edgecross的PC上窃取机密信息	－	－	○