Highly Secure, User-Friendly Physical Security for Tatebayashi System Center

Высокая защищенность, дружественная физическая безопасность для Tatebayashi System Center

Hijiri Kawakita

FUJITSU Sci. Tech. J., Vol. 46, No. 4 (October2010). Перевод ООО «Модуль-Проекты» (Декабрь2013).

Системные подразделения в компаниях и государственных учреждениях, где быстро развиваются информационные технологии (ИТ) сталкиваются с различными вопросами, по мере того, как они становятся владельцами все большего количества серверов. В частности, они должны закупать соответствующее оборудование и осуществлять мероприятия по профилактике стихийных бедствий и принятию мер безопасности для обеспечения стабильного выполнения работы. Однако, организация надежно обеспеченных электричеством и отводом тепла помещений, которые, к тому же, могут выдерживать землетрясения, пожары и другие бедствия и реализация строгих меры безопасности на собственные средствах может быть чрезвычайно дорогостоящей. Следовательно, в различных отраслях промышленности растет спрос на центры обработки данных и этот рынок расширяется в последние годы. Чтобы оставаться конкурентоспособными на этом рынке, компания Fujitsu уделяет большую важность физической безопасности в своих системных центрах, так что клиенты могут быть уверены, что их ИТ-ресурсы являются надежными и безопасными. Эта статья описывает дополнительный функционал физической безопасности нового крыла Tatebayashi System Center компании Fujitsu, расположенного в префектуре Gumma в Японии, который открылся в ноябре 2009 года.

1. Введение

Растущий спрос на аутсорсинг ресурсов информационных технологий (ИТ) определяется различными задачами, связанными с операциями управления, например, трудностями в обеспечении надежным пространством для все большего количества серверов и необходимости закупки разнообразного оборудования для осуществления стабильной работы. В то же время, существует растущая потребность в корпоративных информационных системах хранения с целью укрепления внутреннего контроля и обеспечения непрерывности бизнеса. Центр обработки данных может предоставить пользователю следующие преимущества:

1) Экономия по сравнению с обеспечением своего собственного надежного серверного центра, стабильных источников питания и системы кондиционирования воздуха, исключения сейсмических проблем, и системы для строго контроля входа и выхода из помещения в собственной компании.
2) Снижение риска путем передачи своих ИТ-ресурсов и эксплуатации объектов специалистам.
3) Использование современного оборудования для облачных вычислений (Cloud computing) и программного обеспечения как прикладной услуги (SaaS, software-as-a-service), избавляющей от необходимости владения собственным соответствующим оборудованием.

Таким образом, использование центра обработки данных может быть очень выгодным для компании, которая стремится к гибкому развитию бизнеса. Системные центры Fujitsu предоставляют высококачественные услуги управления объектами включающими устойчивые

системы кондиционирования и электроснабжения , а также надежные меры безопасности гарантируя клиентам, что их ИТ-ресурсы являются надежными и безопасными. Эти меры безопасности включают в себя физическую безопасность, которая означает, что доступ к ИТ-ресурсам клиентов будет точно и строго контролироваться и что несанкционированное проникновение будет предотвращено даже в окружении, в котором контроль за доступом через двери, сами серверные помещения, и даже сеть являются общими для нескольких клиентов.

Данная статья описывает самые современные компоненты физической безопасности новом крыле Tatebayashi System Center, расположенном в префектуре Gumma в Японии, открытом в 2009г.

2. Планирование обеспечения безопасности.

При рассмотрении физической безопасности для всего комплекса, включающего здания, необходимо планировать на установку ворот безопасности, камер контроля и датчиков для предотвращения преступных и несанкционированных действий. В плане для нового крыла Tatebayashi System Center, первый шаг заключался в создании уровней безопасности в здании и определения потока людей, так что места установки таких устройств не будут ничего упускать из виду, при том, что меры безопасности не будут дублироваться.

2.1 Установление уровней безопасности и определение потока персонала.

План разделяет объект, а также приемные помещения, коридоры, лестницы, серверные помещения, машинные отделения и т.д. внутри здания на различные области на основе естественных границ и дверных проемов здания и устанавливает уровни безопасности для этих областей восходящим пошаговым образом. Кроме того, план определяет маршруты, ведущие к серверным комнатам и другим помещеням размещения критически важного оборудования в здании с точки зрения потока персонала в соответствии с классами пользователей, так как, в дополнение к клиентам и техникам компании, пользователи могут также включать обслуживающий персонал, сотрудников сервисной компании центра, а также сотрудников центра данных, а они используют различные маршруты.

2.2 Планирование мер безопасности

Для планирования автоматически или обычные двери использовать в тех местах, где происходит изменение уровня безопасности и где происходит объединение или разделение маршрутов сотрудников используются потоки персонала. Биометрическая аутентификация на основе венозного строения ладони (palm-based) была выбрана для управления открыванием и закрыванием дверей с использованием точной индивидуальной аутентификации. Было сделано допущение, что установка автоматических или обычных дверей в местах, где уровень безопасности или поток персонала не меняется, не предоставляет никакого эффекта для предупреждения преступности, и в то же время создает неудобства пользователям, поэтому такие места были разработаны таким образом, чтобы позволить свободный проход если иные условия, такие как правовые обязательства или требования систем кондиционирования не создают своих требований. Планы размещения камер мониторинга и датчиков были основаны на аналогичной логике.

В описанном выше подходе, необходимая степень безопасности может быть запланирована на установке в первую очередь уровней безопасности и потока персонала с последующим проектированием фактических мер безопасности. Действительно, управление потоком персонала,

выполняемое на основе подхода клиент-за-клиентом, является одной из основных особенностей Tatebayashi System Center, а 18 февраля 2010 г., общие мероприятия по обеспечению безопасности в этом центре обработки данных получили максимально возможный рейтинг информационной безопасности (AAA) от I. S. Rating Co., Ltd.

3 . Меры безопасности на практике

Меры безопасности коммерческого предприятия, как правило, состоят из осуществляемого вручную мониторинга на стойке администратора и защита центров от несчастных случаев, а также проверок права доступа на воротах безопасности путем аутентификации по смарт-картам. В случае центра обработки данных , однако, серверное помещение разделяется рядом клиентов, чьи критические информационные ресурсы работают и управляются в модулях серверных стоек. Более того, поскольку клиенты с различными подходами к безопасности и деятельности разделяют одно серверное помещение, наблюдается растущая потребность применения еще более строгих мер безопасности для персонала, который работают в таких комнатах. В последние годы мы видели появление дверей, препятствующих нежелательному проходу, таких, как автоматически закрывающиеся двери и вращающиеся двери, а также лифты, в которых этаж для остановки может быть установлен для каждого работника, чтобы персонал не имел доступа на этажи, не связанные с их работой. Также увеличилось использование биометрической аутентификации, основанной на распознавании вен, радужных оболочек и других физических характеристик на подступах к требующему большей бдительности оборудованию или помещениям для обеспечения более жесткой проверки входа и выхода. Tatebayashi System Center уделяет особое внимание приему заявок на посещение и управлению встречей посетителей в качестве исходных контрольных точек для посетителей, в то время как безопасность серверных стоек является конечной линией обороны для информационных ресурсов. В этом разделе описываются интегрированная физическая безопасность в Tatebayashi System Center, начинающаяся с этих систем и продолжающаяся системами контроля доступа и управления местонахождением, мерами по предотвращению прохода через «задние двери» (несанкционированный доступ) и маскировки, а также мониторинг сетевыми камерами и управление видео - перемещениями.

3.1. Прием заявок на проход и прием посетителей.

3.1.1. Система приема заявок на проход.

Система приема заявок на проход является важным контрольно-пропускным пунктом для заблаговременного скрининга посетителя и разрешения ему или ей на проход в здание. Система приема заявок в Tatebayashi System Center уделяет особое внимание функции точной регистрации заявителя / посетителя и функции для обмена информацией о рабочем дне посетителя и типе выполняемых им работ с сотрудниками центра.

Система приема заявок включает в себя две важные функции: одна позволяет заявителю делать запрос на посещение серверного помещения путем описания что кем должно быть сделано, а также когда и где такая работа будет сделана, в то время, как другая позволяет назначенному специалисту проверить заявление, получить одобрение руководителя, и уведомить посетителю, что разрешение на вход в здание было предоставлено. В рамках этого процесса, информация о серверном помещении, в котором посетитель планирует работать, а также о типе выполняемых работ может быть предоставлена заблаговременно заинтересованным сотрудникам центра.

Система приема заявок также использует схему аутентификации собственную инфраструктуру шифрования открытыми ключами (PKI, public key infrastructure) связанную с персональной информацией как частью логина и регистрации посетителей. Эта схема позволяет гарантировать, что заявитель / посетитель является сотрудником компании или связанной компании. Она также позволяет информации о заявителе / посетителе быть автоматически обновляемой даже в случае изменений лица служащего или организационных изменений, тем самым решая проблему сопровождения информации. В настоящее время доступ к приложению приема заявок и системе приема посетителей ограничивается персоналом Fujitsu, что означает, что регистрация клиентов и внешних посетителей осуществляется через сотрудников компании или менеджеров эксплуатации. Есть планы, однако, добавить функцию, которая позволит системе приема заявок выполняться непосредственно через Интернет.

Однако, использование такой общей системы управления циклического типа означает, что не могут быть поддержаны доступ обслуживающего персонала в случае возникновения чрезвычайной ситуации или случайного, незапланированного прохода сотрудниками. По этой причине была выполнена функция аварийного приема заявок, что ограничивает период входа и требует последующего одобрения от супервизора отдельно от обычного процесса приема посетителей. Эта функция позволяет отдельным людям подать заявление для прохода на место в периоды чрезвычайных ситуаций, в ночное время или при отпуске, и войти в здание быстро, пока уместно данное приложение.

3.1.2 Система управления приемом посетителей.

Прием посетителей в Tatebayashi System Center играет важную роль в качестве управляемой вручную контрольной точки для входа в помещение. Это контрольно-пропускной пункт регистрирует данные вен ладони для индивидуальноq аутентификации, проверяет цель работы посетителя и подтверждает его или ее индивидуальность, а также выдает карту безопасности или радиочастотный (RF) тег для посетителя.

В связи с этим, существует необходимость выделенного терминала посетителей, чтобы дать посетителям возможность регистрироваться даже без поддержки приема. Этот терминал должен был бы иметь простой, удобный интерфейс для выполнения процедуры регистрации. С этой целью была выбрана интуитивно простая в эксплуатации сенсорная панель, на базе которой было подготовлено устройство регистрации, ориентированное на посетителя, для точной и быстрой регистрации биометрических данных вен ладони. Были приняты также различные меры, чтобы сделать процесс приема как можно короче, такие как механизм регистрации данные для вен только одного ладони, а также использование данных венозного строения, зарегистрированных ранее в период, когда было разрешено построение записи.

Кроме того, администратор должен иметь возможность подтвердить идентичность посетителей и выдать карточки безопасности даже в оживленных условиях, когда пытаются зарегистрироваться многие посетители. По этой причине для терминала регистратора был выбран формат сенсорной панели и была подготовлена функциональность для ввода персональных данных (ID) карт безопасности и радиочастотных меток с помощью считывателя штрих-кодов. Эти меры позволяют быстро и точно выполнять прием посетителей.

3.2. Безопасность стойки серверов.

Здесь мы описываем безопасности стоечных серверов в Tatebayashi System Center. В прошлом серверные стойки были заперты на ключи или кодовые замки, к которым были допущены и

которые обслуживались сотрудниками, регистрируемыми с помощью бумажной бухгалтерской книги, или же доступ к ключам и кодам безопасности был управляем клиентами самостоятельно. Однако, в то время как такая система может эффективно заблокировать двери серверной стойки, управление ключами по-прежнему зависит от человеческих навыков, поэтому всегда присутствовал риск потери ключей или несанкционированного использования.

Tatebayashi System Center оборудован специальными серверными стойками с использованием электронно блокируемыми ручками на передних и задних дверях. Безопасность для этих серверных стоек, содержащих сервера клиента и сетевого оборудования, достигается за счет блокировки и разблокировки дверей стойке посредством операций, выполняемых на ключевой станции (рис. 1). Эта схема не только ограничивает операция исключительно предварительно оговоренными серверными стойками, но и значительно упрощает операции, устраняя осложнения управления физическими ключами, а также позволяет автоматическую запись использования ключа. Чтобы разблокировать стойку, пользователь переходит к ключевой станции и выполняет аутентификацию на устройстве чтения вен ладоней и клавиатуре терминала для выбора стойки для работы и получения разрешение на ее разблокирование. Затем пользователь переходит к необходимой стойке до истечения разрешения и открывает переключатель ручки, чтобы разблокировать электронный ключ и открыть дверь для начала разрешенной работы. Чтобы заблокировать стойку , пользователь снова выполняет операции на ключевой станции, но в этом случае, функция обеспечена автоматической блокировкой двери серверной стойки после определенного времени после закрытия двери. Это предотвращает несанкционированное использование стойки в случае, если пользователь забывает выполнить ее блокирование.

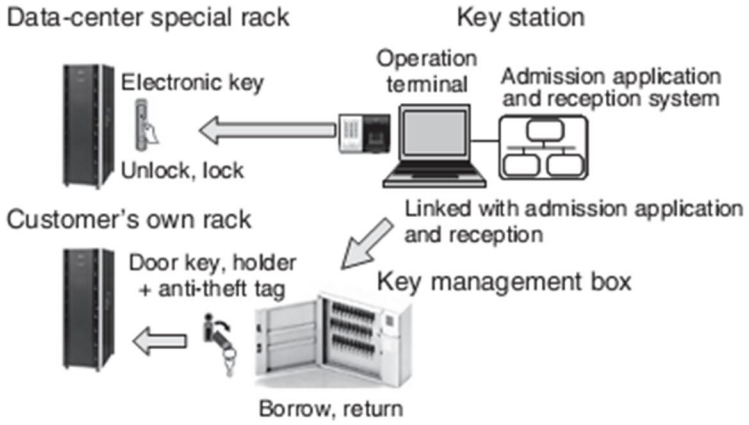

Figure 1
Server rack security scheme.

Шкаф управление ключами (key management box) также установлен вблизи станции ключей (key station) для выдачи и управления внесенными клиентами ключами для запирания и отпирания серверных стоек. В этом случае пользователь использует ключевую станцию, чтобы отпереть дверь в соседнем шкафе управления ключами и освобождает замок держателя ключа, так что может быть одолжен запрашиваемый ключ. Затем, по завершению необходимой работы пользователь снова открывает шкаф управления ключами по той же методике, как указано выше, и возвращает ключ его держателю. Если ключ не возвращается в шкаф управления ключами, противоугонная табличка (anti-theft tag), прикрепленная к ключу, вызовет подачу сигнала, если ключ выносится через ворота безопасности (рис. 1).

Серверные стойки и шкафы управления ключами, которыми можно управлять со станций ключей, связаны с системами приема заявок на посещение и приема посетителей. Серверная стойка или ключ, для которых не было предусмотрено заранее разрешение, не могут быть выбраны, что предотвращает получение этого ключ. Кроме того, путем непрерывного управления историей операций станции ключей и видео, полученного с помощью камер мониторинга записи действий по получению и возвращению ключей, а также путем предотвращения несанкционированных операций со стойками путем мониторинга камер и увязки записанного видео с историей эксплуатации стойки, стало возможным точно определить, кто работал на какой стойке и в какое время.

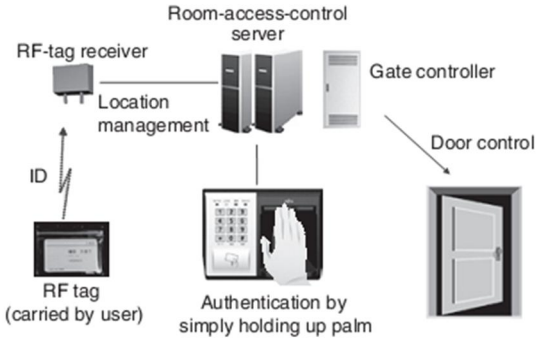

Figure 2
Smart biometric security gate system.

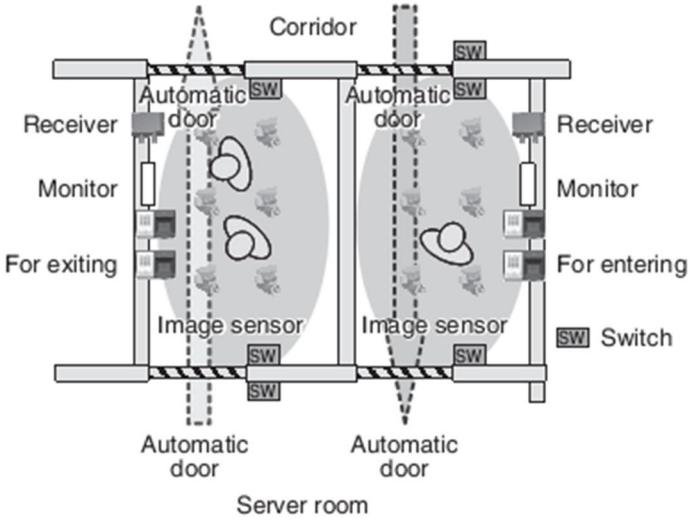

Figure 3
Checking for tailgating and impersonators (separated type).

3.3. Управление доступом и метоположением.

3.3.1. Управление доступом в помещения.

Для предоставления дружественной биометрической аутентификации, ворота безопасности в Tatebayashi System Center, которые размещены в различных местах по всему зданию, объединяют радиочастотные метки и оборудование биометрической аутентификации таким образом, чтобы пользователю достаточно поднести ладонь одной руки, чтобы проверить подлинность и получить доступ. Механизм, встроенный в этот процесс, состоит в следующем. Когда пользователь приближается к воротам безопасности, хранимый на радиочастотной метке ID, имеющейся у пользователя, автоматически считывается приемником RF-тега с указанием системе, что кто-то находится рядом с воротами. Далее, данные вен ладони, полученные, когда пользователь помещает свою ладонь поверх считывающего устройства, сравниваются с ранее сохраненными данными с использованием RF-тега ID в качестве ключа поиска. В случае успешной аутентификации, ворота разблокируются и пользователь получает проход (рис. 2).

3.3.2. Управление месторасположением.

В дополнение к воротам безопасности, описанным выше, приемники RF-тегов размещены в местах, где концентрируется поток людей, таких как коридоры и лифтовых холлах таким образом, что месторасположение персонала может быть обнаружено в реальном времени. Эта функция

управления местоположением позволяет действительное моделирование присутствия, для распознания такого факта, как присутствие пользователя в области не касающейся его или ее, или неспособности войти в комнату, несмотря на проверку подлинности биометрического оборудования аутентификации. Заглядывая вперед, есть планы по использованию такой технологии обнаружения местоположения человека на основе RF -тегов не только в целях защиты центра, но и ради безопасности пользователя и удобства.

3.4 Проверка несанкционированного доступа и имитаций.

Tatebayashi System Center включает в себя функцию для предотвращения тыловых ходов и имитаций в шлюзах, ведущих к серверному помещению (рис. 3) .

После того, как все люди из одной группы, намеревающейся войти в серверное помещение, вошли в шлюзовую комнату и автоматическая дверь закрылась, используется датчик изображения для подсчета количества людей, а также применяются радиочастотные метки для того, чтобы точно определить, сколько людей находится в шлюзовой комнате. Если число людей, подсчитанное с использованием датчика изображения, и количество радиочастотных меток не совпадает, то система определяет, что могло произойти несанкционированное проникновение, и она отклоняет вход группы в серверное помещение. Аналогичным образом, если прихожая включает в себя человека, который определяется через обнаруженный у него RF- тег как не имеющего права входить в серверное помещение, то во входе будет отказано. Однако, если результаты этих проверок оказываются нормальными и все пользователи в шлюзе прошли тест аутентификации вен ладони, то автоматическая дверь на стороне серверного помещения откроется, позволяя проход в комнату.

В Tatebayashi System Center этот механизм для предотвращения несанкционированного доступа и имитаций обеспечивается в прихожей не только для входа, но и при выходе из серверного помещения, что приводит к точному и тщательному контролю доступа в обоих направлениях.

3.5 Контроль сетевыми камерами и управлением видео-записи.

В мире наблюдения сетевые камеры становятся все более господствующими благодаря простоте их установки, низкой цены и хорошего качество. Tatebayashi System Center был первым, кто построил систему видеонаблюдения на основе широкополосного сетевого Интернет - протокола (IP), состоящую из более чем 300 камер. Эта IP- сеть используется для сбора видео-информации, мониторинга в режиме реального времени, хранения видеоинформации и целей видео - воспроизведения, а также применение соответствующего контроля пакетов предотвращает образование блока шума или потери кадров, что приводит к видеонаблюдению и хранению записей высокого качества. Система осуществляет мониторинг видео без мертвых зон в воротах безопасности или внутри серверных помещений, фокусирует мониторинг на сценах, состоящих из человеческих фигур, и записывает с качеством основных исходных данных в формате высокого разрешения со скоростью нескольких кадров в секунду. Кроме того, записанное видео повторно сжимают в соответствии с протоколом H.264/AVC , что позволяет длительное хранение свыше одного года. Данные видео архивируется на жестких дисках, так что они могут быть найдены и быстро получены в любое время для воспроизведения конкретных сцен. Кроме того, поддерживается функция управления видео - записью, которая связывает записанное видео с историей доступа в помещения и воспроизводит это видео в случае непредвиденного инцидента (рис. 4).

Для более подробной информации о проверке несанкционированного доступа и имитаций, а также мониторинга сетевыми камерами и управления видео-записями, пожалуйста, обратитесь к

“Advanced Physical Security Using Imaging Technology,” в специальном выпуске 2 Video Processing and Solutions в январском 2009 журнале FUJITSU.

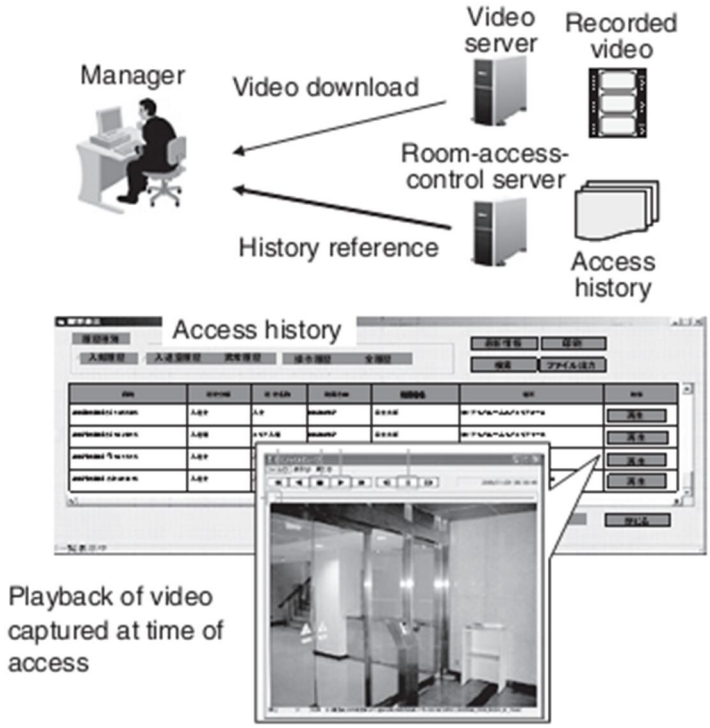

Figure 4
Scheme for access history linkage between security gate and monitoring system.

4. Перспективы для центров обработки данных следующего поколения.

В будущих центрах обработки данных распространение облачных вычислений и SaaS позволит выполнять дистанционно конфигурацию системного окружения, распределение ресурсов сервера и другие задачи управления. В результате, будет меньше поводов для входа в серверные помещения для настройки серверов, добавки оборудования и выполнения другой работу необходимой прошлом.

Таким образом, по мере того, как операции центров обработки данных достигнут прогресса в достижении формата трудосбережения с помощью дистанционного управления и, в конечном счете, к среде, не требующей присутствия оператора, также потребуются изменения к требованиям физической безопасности. В будущем больше внимания будет уделяться надежности и конфиденциальности, проверки на носители информации будут усиливаться, снятое видео будет подвергаться обработке изображений, а мониторинг будет более эффективным, чтобы минимизировать риск. Короче говоря, эта тенденция будет вести к более широкому использованию визуальных контрмер. Кроме того, так как число служащих и рабочих в центре обработки данных будет уменьшаться, все больше мер, которые принимают во внимание эффективность и безопасность станет необходимым.

Например, центры обработки данных могут прийти к тому, чтобы применить методы, аналогичные тем, которые используются в воротах безопасности аэропорта, такие как использование металлоискателей или оборудования рентгеновского изображения для усиления поиска носителей информации или механизма использования сканера всего тела для повышения

обнаружения носителей, скрытых в карманах, либо скрываемых в документах. Все эти методы содержат изображение, и в будущем мы можем ожидать, что применение обработки изображений приведет к большему количеству новшеств, такому, как автоматическое обнаружение несанкционированных предметов для предотвращения оставления незамеченными таких предметов.

Более того, поскольку бизнес аутсорсинга становится глобальным, требования физической безопасности потребуют от клиентов прихода к необходимости включения для внутреннего аутсорсинга тех, кто ранее не рассматривался необходимым в нем. При тех же условиях, что существуют за рубежом, также будет необходимо принять меры безопасности местоположения для защиты зданий и инфраструктуры от незаконного въезда и террористической деятельности.

Здесь, однако, следует заметить: в то время как сотрудники центров обработки данных и пользователи могут понять необходимость и роль таких мер безопасности, ощущение чрезмерного контроля может укорениться, что может привести в некоторых случаях, к неприятным чувствам и падению эффективности работы. Однако, если такие меры безопасности гарантировали сохранность и безопасность и в то же время удобство в их реализации, то пользователи придут к полному пониманию их необходимости. Например, мы можем рассмотреть функцию по профилактике стихийных бедствий, которая в случае инцидента, такого, как землетрясение или пожар, проверит состояние пользователей и безопасно эвакуирует их из помещений, или функцию для замедления скорости открытия / закрытия автоматических дверей, когда пользователь в инвалидной коляске входит в комнату и направления пользователя к соответствующей целевой области. Реализация функций, подобных этим, должно решить описанную выше проблему.

Таким образом, поле центров обработки данных следующего поколения, которые будут иметь дело с передовыми ИТ потребует физической безопасности , которая выделяется в высоком уровне защиты, удобстве и безопасность. За этой тенденцией будет необходимо внимательно следить.

5. Вывод.

Мы описали передовые и надежные функции физической безопасности Tatebayashi System Center демонстрирующие реальные примеры их реализации. При выборе центра обработки данных, клиенты часто цитируют удобство, надежность, доступность, разумные тарифы и безопасные & защищенные операции, как первичные условия. Чтобы убедиться, что системные центры Fujitsu станут их первым выбором, мы будем продолжать укреплять физическую безопасность системных центров в Tokyo, Akashi и Tatebayashi и работать по реализации расширенных функций безопасности в системных центрах соответствующих компаний группы.

Мы можем также ожидать, что рынок для продукции с высоким уровнем безопасности в будущем включит центры обработки данных других компаний, которые ищут укрепления внутреннего контроля, а также банки, компании по работе с ценными бумагами, центры обработки вызовов, которые обрабатывают личную и конфиденциальную информацию, научно-исследовательские лаборатории и фармацевтические компании. Меры безопасности, которые следует принимать такими учреждениями очень похожи с точки зрения целей и решений и есть много «компонентов», которые могут использоваться совместно на уровне исполнения. Имея это в виду, мы планируем организовать и разбить на модули технологии и ноу-хау используемые в

Tatebayashi System Center в форме, способствующей горизонтальной экспансии, а также изучить возможности для расширения бизнеса.