(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102202296 B
(45)授权公告日 2014.02.26

(21)申请号 201110080966.7
(22)申请日 2011.03.25
(30)优先权数据
2010-069511 2010.03.25 JP
(73)专利权人 巴法络股份有限公司
地址 日本爱知县
(72)发明人 沙武寿·沙哈里尔
(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
代理人 刘新宇
(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/04(2009.01)
H04L 29/06(2006.01)

(56)对比文件
US 2009205025 A1,2009.08.13, 全文.
US 2005160287 A1,2005.07.21, 说明书第20、21、35、38段,图2.
CN 1378405 A,2002.11.06, 全文.
US 2009199300 A1,2009.08.06, 全文.

审查员 张莹

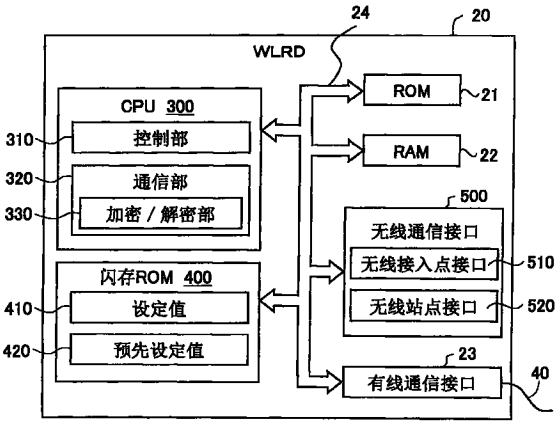
权利要求书3页 说明书14页 附图13页

(54)发明名称

无线局域网中继装置、无线通信系统、无线局域网中继装置的控制方法

(57)摘要

本发明涉及一种用于将外部装置连接到网络的无线局域网中继装置,该无线局域网中继装置包括通信部,该通信部控制与外部装置之间的有线通信及使用无线包的无线通信,且该通信部在初始状态中,在未对进行无线通信时使用的无线包进行加密的状态下进行无线通信;而在从外部装置接收到设定指示的情况下,用无线局域网中继装置中预先规定的密码键和加密方法,来对进行无线通信时使用的无线包进行加密。



CN 102202296 B

1. 一种无线局域网中继装置，用于将外部装置连接到网络，具备：

通信部，控制与所述外部装置之间的有线通信及使用无线包的无线通信，所述通信部在初始状态中，未对进行所述无线通信时的所述无线包进行加密，在从所述外部装置接收到设定指示的情况下，使用在所述无线局域网中继装置中预先规定的密码键和加密方法，来对进行所述无线通信时的所述无线包进行加密；

设定值存储部，存储现行密码键和现行加密方法，其中，所述现行密码键是所述通信部对所述无线包进行加密时应使用的密码键，所述现行加密方法是所述通信部对所述无线包进行加密时应使用的加密方法；

预设值存储部，存储既定密码键和既定加密方法，其中，所述既定密码键是所述预先规定的密码键，所述既定加密方法是所述预先规定的加密方法；以及

控制部，在获取了来自所述外部装置的请求时，将所述现行密码键、所述现行加密方法、所述既定密码键以及所述既定加密方法发送给所述外部装置，在获取了来自所述外部装置的设定指示时，使用由所述外部装置更新的更新后的密码键和更新后的加密方法来改写所述设定值存储部中存储的所述现行密码键和所述现行加密方法，该更新后的密码键和更新后的加密方法分别表示所述无线局域网中继装置中预先规定的密码键和加密方法。

2. 一种无线局域网中继装置，用于将外部装置连接到网络，具备：

通信部，控制与所述外部装置之间的有线通信及使用无线包的无线通信，所述通信部在初始状态中，未对进行所述无线通信时的所述无线包进行加密，在从所述外部装置接收到设定指示的情况下，使用在所述无线局域网中继装置中预先规定的密码键和加密方法，来对进行所述无线通信时的所述无线包进行加密；

设定值存储部，存储现行密码键和现行加密方法，其中，所述现行密码键是所述通信部对所述无线包进行加密时应使用的密码键，所述现行加密方法是所述通信部对所述无线包进行加密时应使用的加密方法；

预设值存储部，存储既定密码键和既定加密方法，其中，所述既定密码键是所述预先规定的密码键，所述既定加密方法是所述预先规定的加密方法；以及

控制部，在获取了来自所述外部装置的请求时，将所述现行密码键和所述现行加密方法发送给所述外部装置，在获取了来自所述外部装置的设定指示时，用所述预设值存储部中存储的所述既定密码键和所述既定加密方法来改写所述设定值存储部中存储的所述现行密码键和所述现行加密方法。

3. 如权利要求 1 或 2 所述的无线局域网中继装置，其特征在于，该无线局域网中继装置还包括：

状态存储部，存储所述通信部进行所述无线通信时是否对所述无线包进行了加密这一状态信息，

所述控制部在获取了来自所述外部装置的请求时，取代发送所述现行密码键和所述现行加密方法，而发送存储在所述状态存储部中的状态信息。

4. 如权利要求 1 或 2 所述的无线局域网中继装置，其特征在于，

所述通信部能够构筑多个逻辑无线网络，

所述现行密码键和所述现行加密方法以与用来相互识别所述多个逻辑无线网络的识别符建立了对应关系的形式，被存储在所述设定值存储部中，

所述既定密码键和所述既定加密方法以与所述识别符建立了对应关系的形式，被存储在所述预设值存储部中，

所述控制部在获取了来自所述外部装置的设定指示时，改写与所述设定指示中包含的至少一个所述识别符相对应的所述现行密码键和所述现行加密方法。

5. 如权利要求 3 所述的无线局域网中继装置，其特征在于，

所述通信部能够构筑多个逻辑无线网络，

所述现行密码键和所述现行加密方法以与用来相互识别所述多个逻辑无线网络的识别符建立了对应关系的形式，被存储在所述设定值存储部中，

所述既定密码键和所述既定加密方法以与所述识别符建立了对应关系的形式，被存储在所述预设值存储部中，

所述控制部在获取了来自所述外部装置的设定指示时，改写与所述设定指示中包含的至少一个所述识别符相对应的所述现行密码键和所述现行加密方法。

6. 一种无线通信系统，包括权利要求 1 至 5 中的任一项所述的无线局域网中继装置和所述外部装置，

所述外部装置包括 ：

请求获取部，向所述无线局域网中继装置发送请求，并根据作为对所述请求的应答而接收到的所述设定值存储部中存储的信息或所述状态存储部中存储的信息，来判断所述通信部是否对所述无线包进行了加密，并且，在判断为未对所述无线包进行加密的情况下，受理使用者所作的对所述无线包进行加密的选择 ；以及

指示部，在受理了对所述无线包进行加密的选择的情况下，向所述无线局域网中继装置发送所述设定指示。

7. 如权利要求 6 所述的无线通信系统，其特征在于，

包括多个无线局域网中继装置，

所述请求获取部向所述多个无线局域网中继装置发送请求，并根据作为对所述请求的应答而从各所述无线局域网中继装置接收到的所述设定值存储部中存储的信息或所述状态存储部中存储的信息，来判断各所述无线局域网中继装置的所述通信部是否对所述无线包进行了加密，并且，在判断出存在未对所述无线包进行加密的所述无线局域网中继装置的情况下，受理使用者所作的在所有所述无线局域网中继装置中对所述无线包进行加密的选择，

所述指示部在受理了对所述无线包进行加密的选择的情况下，至少向所有未对所述无线包进行加密的所述无线局域网中继装置发送所述设定指示。

8. 一种无线通信系统，包括权利要求 4 或 5 所述的无线局域网中继装置和所述外部装置，

所述外部装置包括 ：

请求获取部，向所述无线局域网中继装置发送请求，并根据作为对所述请求的应答而接收到的所述设定值存储部中存储的信息或所述状态存储部中存储的信息，来针对所述多个逻辑无线网络分别判断是否对所述无线包进行了加密，并且，在判断为存在未对所述无线包进行加密的无线网络的情况下，对于未对所述无线包进行加密的无线网络中的至少一个，受理使用者所作的对所述无线包进行加密的选择 ；以及

指示部，在受理了对所述无线包进行加密的选择的情况下，向所述无线局域网中继装置发送包含选择出的所述无线网络的所述识别符的所述设定指示。

9. 一种用于将外部装置连接到网络的无线局域网中继装置的控制方法，具备以下工序：

(a) 控制与外部装置之间的有线通信及使用无线包的无线通信，在初始状态中，未对进行所述无线通信时的所述无线包进行加密，在从所述外部装置接收到设定指示的情况下，用所述无线局域网中继装置中预先规定的密码键和加密方法，来对进行所述无线通信时使用的所述无线包进行加密；

(b) 存储现行密码键和现行加密方法，其中，所述现行密码键是在所述工序 (a) 中对所述无线包进行加密时应使用的密码键，所述现行加密方法是所述通信部对所述无线包进行加密时应使用的加密方法；

(c) 存储既定密码键和既定加密方法，其中，所述既定密码键是所述预先规定的密码键，所述既定加密方法是所述预先规定的加密方法；

(d) 在获取了来自所述外部装置的请求时，将所述现行密码键、所述现行加密方法、所述既定密码键以及所述既定加密方法发送给所述外部装置；以及

(e) 在获取了来自所述外部装置的设定指示时，使用由所述外部装置更新的更新后的密码键和更新后的加密方法来改写通过所述工序 (b) 存储的所述现行密码键和所述现行加密方法，该更新后的密码键和更新后的加密方法分别表示所述无线局域网中继装置中预先规定的密码键和加密方法。

10. 一种用于将外部装置连接到网络的无线局域网中继装置的控制方法，具备以下工序：

(A) 控制与外部装置之间的有线通信及使用无线包的无线通信，在初始状态中，未对进行所述无线通信时的所述无线包进行加密，在从所述外部装置接收到设定指示的情况下，用所述无线局域网中继装置中预先规定的密码键和加密方法，来对进行所述无线通信时使用的所述无线包进行加密；

(B) 存储现行密码键和现行加密方法，其中，所述现行密码键是在所述工序 (A) 中对所述无线包进行加密时应使用的密码键，所述现行加密方法是所述通信部对所述无线包进行加密时应使用的加密方法；

(C) 存储既定密码键和既定加密方法，其中，所述既定密码键是所述预先规定的密码键，所述既定加密方法是所述预先规定的加密方法；

(D) 在获取了来自所述外部装置的请求时，将所述现行密码键、所述现行加密方法发送给所述外部装置；以及

(E) 在获取了来自所述外部装置的设定指示时，使用由所述工序 (C) 所存储的所述既定密码键和所述既定加密方法来改写由所述工序 (B) 所存储的所述现行密码键和所述现行加密方法。

无线局域网中继装置、无线通信系统、无线局域网中继装置的控制方法

技术领域

[0001] 本发明涉及一种无线局域网中继装置。

背景技术

[0002] 近年来，无线局域网 (Local Area Network，LAN) 在不断普及。无线局域网是指，在无线局域网接入点（无线局域网中继装置）和具有无线局域网连接用器件的终端（例如，个人电脑等）之间利用电波进行双方向通信的网络环境。在无线局域网中，只要在电波到达的范围内，任何人都能够不使用特殊工具而监听通信内容。对此，现有技术中提出了对无线局域网接入点和终端之间的无线包进行加密的技术（例如，专利文献 1)，以作为针对这种窃听风险而采取的一种对策。

[0003] 然而，使用上述现有技术会遇到以下问题：为了对无线包进行加密，需要对无线局域网接入点进行有关安全性的种种设定，因而，使用者需要具备有关安全性的知识。

[0004] 本发明是为解决上述技术问题中的至少一部分而提出的，目的在于，提供一种能够简便地对无线局域网中继装置进行涉及安全性的设定的技术。

[0005] 【专利文献 1】：日本特开 2001-111544 号公报。

发明内容

[0006] 为了达到上述目的，本发明具有以下特徵。即，本发明适用于用来将外部装置连接到网络的无线局域网中继装置。

[0007] 并且，上述目的是通过采用以下构成而达到的，即，无线局域网中继装置包括通信部，该通信部控制与外部装置之间的有线通信及使用无线包的无线通信，该通信部在初始状态中，在未对进行无线通信时使用的无线包进行加密的状态下进行通信，而在无线包的通信中，若接收到来自外部装置的设定指示，则用无线局域网中继装置中预先规定的密码键和加密方法，来对进行无线通信时使用的无线包进行加密。

[0008] 基于该构成，无线局域网中继装置在接收到来自外部装置的设定指示的情况下，用无线局域网中继装置中预先规定的密码键和加密方法来对无线包进行加密，因而，能够简便地对无线局域网中继装置进行涉及安全性的设定。

[0009] 在此，无线局域网中继装置也可以构成为：无线局域网中继装置还包括：设定值存储部，存储现行密码键和现行加密方法，其中，现行密码键是通信部对无线包进行加密时应使用的密码键，现行加密方法是通信部对无线包进行加密时应使用的加密方法；预设值存储部，存储既定密码键和既定加密方法，其中，既定密码键是预先规定的密码键，既定加密方法是预先规定的加密方法；以及控制部，在获取了来自外部装置的请求时，将现行密码键和现行加密方法发送给外部装置，在获取了来自外部装置的设定指示时，用预设值存储部中存储的既定加密鍵和既定加密方法来改写设定值存储部中存储的现行密码键和现行加密方法。

[0010] 基于该构成，无线局域网中继装置的控制部在获取了来自外部装置的设定指示时，用预设值存储部中存储的预先规定的既定密码键和既定加密方法来改写设定值存储部中存储的对无线包进行加密时应使用的现行密码键和现行加密方法，因而，能够简便地对无线局域网中继装置进行涉及安全性的设定。

[0011] 另外，无线局域网中继装置也可以被构成为：无线局域网中继装置还包括：设定值存储部，存储现行密码键和现行加密方法，其中，现行密码键是通信部对无线包进行加密时应使用的密码键，现行加密方法是通信部对无线包进行加密时应使用的加密方法；预设值存储部，存储既定密码键和既定加密方法，其中，既定密码键是预先规定的密码键，既定加密方法是预先规定的加密方法；以及控制部，在获取了来自外部装置的请求时，将现行密码键和现行加密方法以及既定密码键和既定加密方法发送给外部装置，在获取了来自外部装置的设定指示时，用经外部装置更新的更新后的密码键和更新后的加密方法来改写设定值存储部中存储的现行密码键和现行加密方法。

[0012] 基于该构成，无线局域网中继装置的控制部在获取了来自外部装置的设定指示时，用经外部装置更新的更新后的密码键和更新后的加密方法来改写设定值存储部中存储的对无线包进行加密时应使用的现行密码键和现行加密方法，因而，能够简便地对无线局域网中继装置进行涉及安全性的设定。

[0013] 进一步，无线局域网中继装置可以被构成为：无线局域网中继装置还包括设定值存储部，存储现行密码键和现行加密方法，其中，现行密码键是通信部对无线包进行加密时应使用的密码键，现行加密方法是通信部对无线包进行加密时应使用的加密方法；预设值存储部，存储既定密码键和既定加密方法，其中，既定密码键是预先规定的密码键，既定加密方法是预先规定的加密方法；状态存储部，存储通信部进行无线通信时是否对无线包进行了加密这一状态信息；以及控制部，在获取了来自外部装置的请求时，将存储在状态存储部中的状态信息发送给外部装置，在获取了来自外部装置的设定指示时，用预设值存储部中存储的既定加密鍵和既定加密方法来改写设定值存储部中存储的现行密码键和现行加密方法。

[0014] 或者，无线局域网中继装置可以被构成为：无线局域网中继装置还包括：设定值存储部，存储现行密码键和现行加密方法，其中，现行密码键是通信部对无线包进行加密时应使用的密码键，现行加密方法是通信部对无线包进行加密时应使用的加密方法；预设值存储部，存储既定密码键和既定加密方法，其中，既定密码键是预先规定的密码键，既定加密方法是预先规定的加密方法；状态存储部，存储通信部进行无线通信时是否对无线包进行了加密这一状态信息；以及控制部，在获取了来自外部装置的请求时，将现行密码键和现行加密方法以及既定密码键和既定加密方法发送给外部装置，在获取了来自外部装置的设定指示时，用经外部装置更新的更新后的密码键和更新后的加密方法来改写设定值存储部中存储的现行密码键和现行加密方法。

[0015] 基于该构成，无线局域网中继装置的控制部在获取了来自外部装置的请求时，可以发送状态存储部中存储的信息，以取代发送现行密码键和现行加密方法。

[0016] 进一步，无线局域网中继装置还可以被构成为：无线局域网中继装置中，通信部能够构筑多个逻辑无线网络，现行密码键和现行加密方法以与用来相互识别多个逻辑无线网络的识别符建立了对应关系的形式，被存储在设定存储部中，既定密码键和既定加密方法

以与识别符建立了对应关系的形式，被存储在预设值存储部中，控制部在获取了来自外部装置的设定指示时，改写与设定指示中包含的至少一个识别符相对应的现行密码键和现行加密方法。

[0017] 基于该构成，无线局域网中继装置的通信部在获取了来自外部装置的设定指示时，改写与设定指示中包含的至少一个用于相互识别逻辑无线网络的识别符相对应的现行密码键和现行加密方法，因而，在能够构筑多个逻辑无线网络的无线局域网中继装置中，能够简便地对各个逻辑无线网络进行涉及安全性的设定。

[0018] 另外，本发明适用于具备用于将外部装置连接到网络的无线局域网中继装置和外部装置的无线通信系统。

[0019] 并且，上述目的可以通过采用以下构成来达到。即，无线局域网中继装置包括：通信部，控制与外部装置之间的有线通信及使用无线包的无线通信，并且，在初始状态中，在未对进行无线通信时使用的无线包进行加密的状态下进行通信；在所述无线包的通信中，若接收到来自外部装置的设定指示，则用无线局域网中继装置中预先规定的密码键和加密方法，来对进行无线通信时使用的无线包进行加密；设定值存储部，存储现行密码键和现行加密方法，其中，现行密码键是通信部对无线包进行加密时应使用的密码键，现行加密方法是通信部对无线包进行加密时应使用的加密方法；预设值存储部，存储既定密码键和既定加密方法，其中，既定密码键是预先规定的密码键，既定加密方法是预先规定的加密方法；状态存储部，存储通信部进行无线通信时是否对无线包进行了加密这一状态信息；以及控制部，在获取了来自外部装置的请求时，将现行密码键和现行加密方法发送给外部装置，在获取了来自外部装置的设定指示时，用预设值存储部中存储的既定加密鍵和既定加密方法来改写设定值存储部中存储的现行密码键和现行加密方法，外部装置包括：请求获取部，向无线局域网中继装置发送请求，并根据作为对请求的应答而接收到的设定值存储部中存储的信息或状态存储部中存储的信息，来判断通信部是否对无线包进行了加密，并且，在判断为未对无线包进行加密的情况下，受理使用者所作的对无线包进行加密的选择；以及指示部，在受理了对无线包进行加密的选择的情况下，向无线局域网中继装置发送设定指示。

[0020] 基于该构成，无线通信系统的外部装置在受理了使用者所作的对无线包进行加密的选择时，向无线局域网中继装置发送设定指示，因而能够简便地对无线局域网中继装置进行涉及安全性的设定。

[0021] 在此，也可以采用以下构成：通信部能够构筑多个逻辑无线网络，现行密码键和现行加密方法以与用来相互识别多个逻辑无线网络的识别符建立了对应关系的形式，被存储在设定存储部中，既定密码键和既定加密方法以与识别符建立了对应关系的形式，被存储在预设值存储部中，另外，外部装置包括：请求获取部，向无线局域网中继装置发送请求，并根据作为对请求的应答而接收到的设定值存储部中存储的信息或状态存储部中存储的信息，来判断多个逻辑无线网络的每一个是否都对无线包进行了加密，并且，在判断出存在未对无线包进行加密的无线网络的情况下，对于未对无线包进行加密的无线网络中的至少一个，受理使用者所作的对无线包进行加密的选择；以及指示部，在受理了对无线包进行加密的选择的情况下，向无线局域网中继装置发送包含有被选择的无线网络的识别符的设定指示。

[0022] 基于该构成，无线通信系统的外部装置在受理了使用者所作的对无线包进行加密

的选择时，向无线局域网中继装置发送包含有用于相互识别被选择的逻辑无线网络的识别符的设定指示，因而，在能够构筑多个逻辑无线网络的无线局域网中继装置中，可以简便地对各个逻辑无线网络进行涉及安全性的设定。

[0023] 进一步还可以采用以下构成：无线通信系统包括多个无线局域网中继装置，请求获取部向多个无线局域网中继装置发送请求，并根据作为对请求的应答而从各无线局域网中继装置接收到的设定值存储部中存储的信息或状态存储部中存储的信息，来判断各无线局域网中继装置的通信部是否对无线包进行了加密，并且，在判断出存在未对无线包进行加密的无线局域网中继装置的情况下，受理使用者所作的在所有无线局域网中继装置中对无线包进行加密的选择，指示部在受理了对无线包进行加密的选择的情况下，至少向所有未对无线包进行加密的无线局域网中继装置发送设定指示。

[0024] 基于该构成，无线通信系统的外部装置在受理了使用者所作的对无线包进行加密的选择时，至少向所有未对无线包进行加密的无线局域网中继装置发送设定指示，因而，能够简便地进行具备多个无线局域网中继装置的无线通信系统的涉及安全性的设定。

附图说明

[0025] 图 1 是表示本发明的第一实施方式的无线通信系统的概要构成的图。

[0026] 图 2 是表示第一实施方式中采用的个人电脑的概要构成的图。

[0027] 图 3 是表示第一实施方式中采用的接入点 WLRD 的概要构成的图。

[0028] 图 4 是表示第一实施方式中的设定值的一例的图。

[0029] 图 5 是表示第一实施方式中的预先设定值的一例的图。

[0030] 图 6 是表示第一实施方式中的安全性设定处理顺序的序列图。

[0031] 图 7 是表示图 6 所示的安全性设定处理中所显示的确认画面的一例的图

[0032] 图 8 是表示图 6 所示的安全性设定处理中预先设定值的值作为设定值的值而被复制的情形的图。

[0033] 图 9A 是表示图 6 所示的安全性设定处理中的设定值的一例的图。

[0034] 图 9B 是表示图 6 所示的安全性设定处理中所显示的确认画面的另一例的图。

[0035] 图 10 是表示图 6 所示的安全性设定处理中预先设定值的值作为设定值的值被复制的情形的图。

[0036] 图 11A 是表示图 6 所示的安全性设定处理中的设定值的另一例的图。

[0037] 图 11B 是表示图 6 所示的安全性设定处理中所显示的确认画面的另一例的图。

[0038] 图 12 是表示本发明的第二实施方式中采用的接入点 WLRD 的概要构成的图。

[0039] 图 13 是表示第二实施方式中的安全性状态值的一例的图。

[0040] 图 14 是表示第二实施方式中的安全性设定处理顺序的序列图。

[0041] 图 15 是表示本发明的第三实施方式的无线通信系统的概要构成的图。

[0042] 图 16 是表示第三实施方式中的安全性设定处理顺序的序列图。

[0043] 图 17 是表示第三实施方式中的接入点 WLRD 选择画面的一例的图，该画面用于受理对要实施安全性设定的接入点 WLRD 所进行的选择。

[0044] 图 18 是表示本发明的第四实施方式中的安全性设定处理顺序的序列图。

具体实施方式

[0045] 下面说明本发明的实施方式。

[0046] <第一实施方式>

[0047] 图 1 是表示本发明的第一实施方式的无线通信系统的概要构成的图。第一实施方式的无线通信系统 10 包括 :作为无线局域网中继装置的无线局域网接入点 (以下,也称为“WLRD”)20,和作为具备无线局域网连接用器件的外部装置的个人电脑 (以下,也称为“PC”)30。在后述的安全性设定处理中,WLRD20 和 PC30 如图 1 所示那样由局域网电缆 40 连接 (即,有线连接)。另外,为了形成后述的安全性设定处理中使用的处理部,在 PC30 中装入了预先存储在 CD(Compact Disc,光盘)50 中的计算机程序。

[0048] 图 2 是表示第一实施方式中的 PC30 的概要构成的图。PC30 包括 :RAM(Random Access Memory,随机存取存储器)31、ROM(Read Only Memory,只读存储器)32、显示部 33、操作部 34、有线通信接口 35、能够用来读取上述 CD50 的 CD 驱动器 37、能够利用无线局域网来进行无线通信的无线通信接口 38、CPU(中央处理器)100、硬盘 200,上述各构成要素分别通过总线 36 而相互连接。

[0049] CPU100 通过将硬盘 200 中存储的计算机程序展开到 RAM31 中执行,来控制 PC30 的各个部。另外,CPU100 也通过将由 CD50 装入并存储在硬盘 200 中的计算机程序展开到 RAM31 中执行,来发挥请求获取部 110、指示部 120 的作用。请求获取部 110 和指示部 120 的详细功能将在后文中说明。

[0050] 显示部 33 包括未图示的显示器和显示器驱动器,具有向使用者进行视觉性画面显示的功能。操作部 34 包括未图示的鼠标、键盘及它们的驱动器,具有受理使用者所进行的输入的功能。有线通信接口 35 上连接着用来连接局域网的局域网电缆 40。

[0051] 硬盘 200 中存储着安全性设定值 210。安全性设定值 210 是以表格状态存储的 PC30 通过无线通信与 WLRD20 连接时所采用的涉及安全性设定的设定值。安全性设定值 210 中存储着与后述的 WLRD20 的设定值 410 相同的内容。

[0052] 图 3 是表示第一实施方式中的 WLRD20 的概要构成的图。WLRD20 包括 :ROM21、RAM22、有线通信接口 23、CPU300、闪存 ROM400、无线通信接口 500,这些构成要素分别通过总线 24 而相互连接。

[0053] CPU300 通过将 ROM21 中存储的计算机程序展开到 RAM22 中执行,来控制 WLRD20 的各个部。另外,CPU300 也通过将闪存 ROM400 中存储的固件 (firmware) 展开到 RAM22 中执行,来实现控制部 310、通信部 320、加密 / 解密部 330 的功能。控制部 310 的详细功能将在下文中说明。通信部 320 具有控制与通过有线通信接口 23 与 WLRD20 连接的 PC30 之间所进行的有线通信的功能。并且,通信部 320 具有根据对后述的设定值 410 定义的内容,来控制与通过无线与 WLRD20 连接的 PC30 之间所进行的无线通信 (使用无线包的通信) 的功能。通信部 320 至少能够进行基于 IEEE(The Institute of Electrica and Electronics Engineers :美国电气电子学会)802.11 规格的无线局域网通信。加密 / 解密部 330 包括在通信部 320 中作为在通信部 320 对无线包进行加密时以及通信部 320 对被加密的无线包进行解密时,被通信部 320 叫出而被使用的模块。作为设定值存储部及预设值存储部的闪存 ROM400 中存储着设定值 410 和预先设定值 420。

[0054] 无线通信接口 500 是用于进行无线通信的接口,包括无线接入点接口 510 和无线

站点（非接入点的终端）接口 520。无线接入点接口 510 发挥接入点的作用，与作为站点的其它无线通信装置之间以无线的方式发送接收包。无线站点接口 520 发挥站点的作用，与作为接入点的其它无线通信装置之间以无线的方式发送接收包。无线接入点接口 510 和无线站点接口 520 以能够向外部发送电波、并从外部接收电波的状态被内置于 WLRD20 中。CPU300 的各功能部通过它们来与其它无线通信装置之间进行通信。无线接入点接口 510 和无线站点接口 520 可以由一个无线模块构成，也可以分别由不同模块构成。有线通信接口 23 上连接着用来与局域网连接的局域网电缆 40。

[0055] 图 4 是表示设定值 410 的一例的图。设定值 410 是存储有 WLRD20 的现行的涉及安全性的设定值的表格。设定值 410 包含项目 EIM、识别符 EID、密码键 EEK、加密方式 EEM、认证方法 EAT。其中，“涉及安全性的设定值”是指用于对无线包进行加密的密码键、加密方法（加密中使用的方法、认证中使用的方法）等的设定值。以下，对于图示的密码键和加密方法，基本上使用 IEEE802.11 规格中所规定的，缩写也使用基于本规格的缩写。也就是说，有关密码键和加密方法的详细内容，可以参照上述规格，因而在本说明书中省略其说明。

[0056] 在项目 EIM 栏中，标有用于识别设定值 410 中存储的各个对象 (entry) 的唯一的序号。在识别符 EID 栏中，存储着用于相互识别 WLRD20 所能构筑的多个逻辑无线网络（以下，也称为“逻辑无线网络”）的识别符 (SSID :Service Set Identifier，服务集标识）。在密码键 EEK 栏中，存储着通信部 320 对无线包进行加密时应使用的密码键（以下，也称为“现行密码键”）。在加密方式 EEM 栏中，存储着通信部 320 对无线包进行加密时应使用的加密方式。在认证方法 EAT 栏中，存储着通信部 320 对无线包进行加密时应使用的认证方法。另外，加密方式与认证方法的组合也称为“加密方法”。另外，也将通信部 320 对无线包进行加密时应使用的加密方法称为“现行加密方法”。

[0057] 本实施方式中的 WLRD20 是具备能用一台来构筑多个逻辑无线网络的多 SSID 功能的无线局域网中继装置。现行密码键和现行加密方法以与用于相互识别各逻辑无线网络的识别符（识别符 EID 栏的值）建立了对应关系的形式，被存储在设定值 410 中。另外，将设定值 410 的表格构成为可被读取 / 写入。并且，设定值 410 的内容不光被用于通信部 320 所进行的加密，还可被用于解密。

[0058] 如图 4 所示，在 WLRD20 的初始状态中，对于项目 EIM 的 1 ～ 4 中被识别的各对象，密码键 EEK 栏中存储着“No Key”这一值，加密方式 EEM 栏中存储着“No Encryption”这一值，认证方法 EAT 栏中存储着“No Authentication”这一值。也就是意味着，在 WLRD20 的初始状态中，所有的逻辑无线网络都不对无线包进行加密。

[0059] 图 5 是表示预先设定值 420 的一例的图。预先设定值 420 是预先存储有对 WLRD20 适用安全性设定时的初始 (default) 设定值的表格。预先设定值 420 包含项目 PIM、识别符 PID、密码键 PEK、加密方式 PEM、认证方法 PAT。

[0060] 在项目 PIM 栏中，存储着用于识别预先设定值 420 中存储的各对象的唯一的序号。在识别符 PID 栏中，存储着用于相互识别 WLRD20 所能构筑的多个逻辑无线网络的识别符 (SSID)。在密码键 PEK 栏中，存储着预先规定的密码键（以下，也称为“既定密码键”）。在加密方式 PEM 栏中，存储着预先规定的加密方式。在认证方法 PAT 栏中，存储着预先规定的认证方法。另外，预先被规定的加密方法（加密方式和认证方法的组合）也被称为“既定加密方法”。

[0061] 如此，既定密码键和既定加密方法以与用于相互识别各逻辑无线网络的识别符（识别符 PID 栏的值）建立了对应关系的形式，被存储在预先设定值 420 中。另外，较佳的是，将预先设定值 420 的表格构成为只能进行读取。

[0062] 接下来，参照图 6 ～ 8，来说明本发明的第一实施方式中的安全性设定处理。图 6 是表示第一实施方式中的安全性设定处理的顺序的序列图。在安全性设定处理中，如上所述那样，PC30 和 WLRD20 通过局域网电缆 40 而被连接为有线连接状态。PC30 的请求获取部 110 向 WLRD20 发送希望获取安全性状态信息的请求（步骤 S100）。接收到该请求的 WLRD20 的控制部 310 将设定值 410 中存储的内容（项目 EIM、识别符 EID、密码键 EEK、加密方式 EEM、认证方法 EAT 的各栏的值）以及预先设定值 420 中存储的内容（项目 PIM、识别符 PID、密码键 PEK、加密方式 PEM、认证方法 PAT 的各栏的值）发送给 PC30（步骤 S102）。

[0063] 接收到来自 WLRD20 的应答的 PC30 的请求获取部 110 基于设定值 410 中存储的内容，来判断各逻辑无线网络的每一个是否都对无线包进行了加密。具体而言，例如，识别符 EID 的值为“SSID1”、密码键 EEK 的值为“NoKey”，则可判断为用 SSID1 识别的逻辑无线网络未对无线包进行加密。另外，也可以用密码键 EEK 以外的其它项目（加密方式 EEM、认证方法 EAT）的值来进行该判断。请求获取部 110 如上所述那样来对所有的逻辑无线网络进行是否加密的判断，只要判断出有一个未对无线包进行加密的逻辑无线网络存在，便在显示部 33（图 2）上显示确认画面（步骤 S104）。

[0064] 图 7 是表示图 6 所示的安全性设定处理的步骤 S104 中所显示的确认画面的一例的图。确认画面 WD1 中包括复选框 CK、OK 按钮 AB1 及取消按钮 CB1。若无线通信系统 10 的使用者希望取消安全性设定处理，则可按下取消按钮 CB1。若取消按钮 CB1 被押下，则图 6 的处理结束。

[0065] 相反，若无线通信系统 10 的使用者希望继续进行安全性设定处理，则可在复选框 CK 中输入选择符号并按下 OK 按钮 AB1。在复选框 CK 中被输入了选择符号的状态下 OK 按钮 AB1 被按下，则请求获取部 110 当作使用者作出了希望对 WLRD20 中的无线包进行加密的选择，从而继续处理。

[0066] PC30 的指示部 120 将预先设定值 420 的值复制为设定值 410 的值（步骤 S106）。具体而言，指示部 120 将在步骤 S102 接收到的预先设定值 420 的识别符 PID 与在步骤 S102 接收到的设定值 410 的识别符 EID 相一致的数据提取出，并将预先设定值 420 的各项目（密码键 PEK、加密方式 PEM、认证方法 PAT）的值复制为设定值 410 的各项目（密码键 EEK、加密方式 EEM、认证方法 EAT）的值。其中，将复制预先设定值 420 的密码键 PEK 而得到的密码键 EEK 也称为“更新后的密码键”。另外，将复制预先设定值 420 的加密方式 PEM 而得到的加密方式 EEM、复制认证方法 PAT 而得到的认证方法 EAT 的组也称为“更新后的加密方法”。另外，较佳的是，该数据的复制只对在步骤 S104 被判断为未对无线包进行加密的逻辑无线网络进行。

[0067] PC30 的指示部 120 将设定指示发送给 WLRD20（步骤 S108）。设定指示中包含：通过步骤 S106 而被更新的项目 EIM、识别符 EID、更新后的密码键以及更新后的加密方法。接收到设定指示的 WLRD20 的控制部 310 用在步骤 S108 接收到的设定指示中包含的各值来更新闪存 ROM400 中存储的设定值 410（步骤 S110）。具体而言，提取设定指示中包含的识别符 EID 与设定值 410 的识别符 EID 一致的对象，并将设定指示中包含的数据复制给设定值 410

的对象。

[0068] 其后，控制部 310 将更新的结果（成功 / 失败）发送给 PC30（步骤 S112）。若更新的结果为“成功”，则 PC30 的指示部 120 用更新后的密码键和更新后的加密方法，来更新硬盘 200 中存储的安全性设定值 210（步骤 S114）。

[0069] 图 8 是表示在图 6 的步骤 S106 中预先设定值 420 的值被复制为设定值 410 的值的情形的图。PC30 的请求获取部 110 判断为，识别符 SSID1 ～ SSID4 的所有的逻辑无线网络未对无线包进行加密（图 4、图 6 ：步骤 S104）。PC30 的指示部 120 将有关识别符 SSID1 ～ SSID4 的所有的逻辑无线网络的预先设定值 420 的值复制为设定值 410 的值。具体而言，例如，将与预先设定值 420 的识别符 PID 为 SSID1 的数据相对应的密码键 PEK、加密方式 PEM、认证方法 PAT 的各值复制为与设定值 410 的识别符 EID 为 SSID1 的数据相对应的密码键 EEK、加密方式 EEM、认证方法 EAT 的各值。

[0070] 如以上说明过那样，在第一实施方式中，WLRD20 的控制部 310 获取了来自 PC30 的设定指示时，用经外部装置更新的更新后的密码键（复制预先设定值 420 的密码键 PEK 而得到的密码键 EEK）、更新后的加密方法（复制预先设定值 420 的加密方式 PEM 而得到的加密方式 EEM、复制认证方法 PAT 而得到的认证方法 EAT），来改写设定值存储部（设定值 410）中存储的对无线包进行加密时应使用的现行密码键（密码键 EEK）、现行加密方法（加密方式 EEM、认证方法 EAT）。即，由于 WLRD20 通过接收来自 PC30 的设定指示，来用 WLRD20 内部预先规定的密码键和加密方法对无线包进行加密，所以能够简便地对 WLRD20 进行涉及安全性的设定。

[0071] 图 9B 是表示在图 6 所示的安全性设定处理的步骤 S104 中所显示的确认画面的另一例的图，图 9A 是表示此时的设定值 410 的一例的图。图 9A 中，通过项目 EIM2、4 而识别的对象的密码键 EEK、加密方式 EEM、认证方法 EAT 的各栏中存储着用于使安全性有效的设定值。即意味着，在具有这样的设定值 410 的 WLRD20 中，由识别符 SSID2、4 识别的逻辑无线网络对无线包进行加密，而由识别符 SSID1、3 识别的逻辑无线网络不对无线包进行加密。

[0072] 图 9B 中的确认画面 WD2 中包含着识别符清单 ERN、选择按钮 EBT（EBT1 ～ EBT4）、取消按钮 CB2。识别符清单 ERN 列出了多个逻辑网络的识别符（SSID1 ～ SSID4）。选择按钮 EBT 是对各逻辑网络的识别符所分配的按钮。较佳的是，将该选择按钮 EBT 以相应于设定值 410 中所设定的内容而切换选择有效 / 无效的状态来显示。具体而言，例如，请求获取部 110 可以对基于设定值 410 中存储的内容而判断为已对无线包进行了加密的逻辑无线网络，进行将选择按钮 EBT 变暗（图中是用影线表示）等的控制。即，当设定值 410 的内容为图 9A 所示的内容时，用项目 EIM2、4 识别的对象被判断为已对无线包进行了加密，所以将选择按钮 EBT2、EBT4 变暗显示。这样，便能避免已存储在设定值 410 中的用于使安全性有效的设定值被错误地更新的情况。

[0073] 无线通信系统 10 的使用者不是在图 7 所示的确认画面 WD1 中的复选框 CK 中输入选择符号并按下 OK 按钮 AB1，而是在图 9B 所示的确认画面 WD2 中按下希望进行安全性设定处理的逻辑网络的识别符旁设置的选择按钮 EBT。若选择按钮 EBT 被按下，则请求获取部 110 当作使用者作出了对有关 WLRD20 的被选择的逻辑网络的无线包进行加密的选择，从而继续图 6 的安全性设定处理。

[0074] 在图 6 的安全性设定处理的步骤 S106 中，PC30 的指示部 120 将预先设定值 420

的值复制为设定值 410 的值时，只复制有关通过图 9B 的画面而选择的逻辑无线网络的数据。进一步，在步骤 S108 中，PC30 的指示部 120 向 WLRD20 发送在步骤 S106 中被更新的项目 EIM、识别符 EID、更新后的密码键、更新后的加密方法，即，发送只包含了有关通过图 9B 的画面而选择的逻辑无线网络的数据的设定指示。这样一来，接收到设定指示的 WLRD20 的控制部 310 便改写与设定指示中包含的识别符（识别符 EID）相对应的现行密码键和现行加密方法（步骤 S110）。

[0075] 图 10 是表示在图 6 的步骤 S106 中，预先设定值 420 的值被复制为设定值 410 的值的情形的图。在图 9B 的确认画面 WD2 中，选择按钮 EBT1 被按下时，PC30 的指示部 120 将识别符 SSID1 的逻辑无线网络的预先设定值 420 的值复制为设定值 410 的值。

[0076] 另外，图 9B 所示的画面只不过是一例而已，也可以采用各种其它方式。具体而言，例如，也可以采用以下构成，即，在选择画面 WD2 中，取代选择按钮 EBT，而具备针对识别符清单 ERN 的各个项目的每一个而显示的多个复选框、及一个 OK 按钮，通过按下 OK 按钮，能够一次执行使用者通过复选框而选择了的至少一个逻辑无线网络的安全性设定处理。

[0077] 如上所述，只要使用确认画面 WD2，WLRD20 的通信部 320 便可在获取了来自 PC30 的设定指示时，改写与设定指示中包含的至少一个用于相互识别逻辑无线网络的识别符 (SSID) 相对应的现行密码键（密码键 EEK）和现行加密方法（加密方式 EEM、认证方法 EAT），所以，在能够构筑多个逻辑无线网络（具备多 SSID 功能）的 WLRD20 中，可以对各个逻辑无线网络简便地进行涉及安全性的设定。

[0078] 图 11B 是表示图 6 所示的安全性设定处理的步骤 S104 中所显示的确认画面的另一例的图，图 11A 是表示此时的设定值 410 的一例的图。图 11A 的详细内容与图 9A 中说明过的内容一样，所以省略其说明。

[0079] 在图 11B 中，确认画面 WD3 包含识别符清单 ERN、安全性设定状态显示栏 SST、选择按钮 EBT(EBT1 ～ EBT4)、取消按钮 CB3。识别符清单 ERN 列出了多个逻辑网络的识别符 (SSID1 ～ SSID4)。安全性设定状态显示栏 SST 显示出各逻辑网络中的涉及安全性的设定的状态。作为涉及安全性设定的状态，例如，也可以如图 11B 所示那样，直接显示设定值 410 的加密方式 EEM 栏的值，也可以进行“安全性有效”、“安全性无效”等显示。

[0080] 选择按钮 EBT 是对每一个逻辑网络的识别符分配的按钮。较佳的是，将该选择按钮 EBT 构成为，不同功能相应于设定值 410 中所设定的内容而动作。具体而言，例如，请求获取部 110 对于根据设定值 410 中存储的内容而判断为未对无线包进行加密的逻辑无线网络，使选择按钮 EBT 上所显示的名称为“Enable”。相反，对于判断为已经对无线包进行了加密的逻辑无线网络，使选择按钮 EBT 上显示的名称为“Back to Preset”。

[0081] 当无线通信系统 10 的使用者按下了显示着“Enable”的选择按钮 EBT 时，请求获取部 110 当作使用者作出了对 WLRD20 的被选择的逻辑网络的无线包进行加密的选择，从而继续图 6 的安全性设定处理。详细内容与在图 9B 中说明过的相同。

[0082] 当无线通信系统 10 的使用者按下了显示着“Back to Preset”的选择按钮 EBT 时，请求获取部 110 使指示部 120 执行为了使 WLRD20 的被选择的逻辑网络的无线包加密设定返回初始状态而需进行的处理。

[0083] 以下说明为了使对无线包进行加密的设定返回初始状态而需进行的处理。首先，PC30 的指示部 120 对于设定值 410 中的有关通过图 11B 所示的画面而选择了的逻辑无线网

络的数据，用“No Key”这个值来更新密码键 EEK ；用“No Encryption”这个值来更新加密方式 EEM ；用“No Authentication”这个值来更新认证方法 EAT。进一步，指示部 120 向 WLRD20 发送进行了数据更新的项目 EIM、识别符 EID、更新后的密码键和更新后的加密方法，即，发送只包含了有关通过图 11B 所示的画面而选择的逻辑无线网络的数据的设定指示。这样一来，接收到设定指示的 WLRD20 的控制部 310 便用初始设定值来改写与设定指示中包含的识别符（识别符 EID）相对应的现行密码键和现行加密方法。

[0084] 如上所述，只要使用确认画面 WD3，WLRD20 的通信部 320 便可在获取了来自 PC30 的设定指示时，改写与设定指示中包含的至少一个用于相互识别逻辑无线网络的识别符 (SSID) 相对应的现行密码键（密码键 EEK）和现行加密方法（加密方式 EEM、认证方法 EAT），因而，在能够构筑多个逻辑无线网络（具备多 SSID 功能）的 WLRD20 中，可以简便地进行对于各个逻辑无线网络的涉及安全性的设定。并且，这样一来，还可以通过简单的操作，使已经进行了涉及安全性的设定的逻辑网络恢复到初始设定的状态（安全性无效的状态）。

[0085] ＜第二实施方式＞

[0086] 图 12 是表示本发明的第二实施方式中的 WLRD20a 的概要构成的图。与图 3 所示的第一实施方式相比，不同之处仅在于，闪存 ROM400a 中还具备安全性状态值 430，其它构成与第一实施方式相同。因而，下面只对构成和动作与第一实施方式不同的部分进行说明。图中，对于与第一实施方式相同的构成部分，使用与在前面说明过的第一实施方式相同的符号，并省略其详细说明。

[0087] 图 13 是表示第二实施方式中的安全性状态值 430 的一例的图。安全性状态值 430 是存储了 WLRD20 的通信部 320 所构筑的各逻辑无线网络是否对无线包进行了加密这一状态信息的表格。安全性状态值 430 包含有识别符 SID 和安全性状态 SST。

[0088] 在识别符 SID 栏中，存储着用于相互识别 WLRD20 所能构筑的多个逻辑无线网络的识别符 (SSID1 ～ SSID4)。在安全性状态 SST 栏中，存储着各逻辑无线网络是否对无线包进行了加密这一状态信息。在安全性状态 SST 栏中，例如，在未对无线包进行加密的情况下可存储“No Security”这个值；而在对无线包进行了加密的情况下可存储“Secure”这个值。

[0089] 图 14 是表示有关第二实施方式中的安全性设定处理的顺序的序列图。PC30 的请求获取部 110 向 WLRD20 发送希望获取安全性状态值的请求（步骤 S200）。接收到该请求的 WLRD20 的控制部 310 向 PC30 发送安全性状态值 430 中存储的内容（识别符 SID、安全性状态 SST 的各栏的值）（步骤 S202）。

[0090] 接收到来自 WLRD20 的应答的 PC30 的请求获取部 110 根据安全性状态值 430 中存储的内容，来判断各逻辑无线网络的每一个是否都对无线包进行了加密。具体而言，例如，若识别符 SID 的值为“SSID1”，安全性状态 SST 的值为“No Security”，则可判断为用 SSID1 识别的逻辑无线网络未对无线包进行加密。如此，请求获取部 110 对所有的逻辑无线网络是否加密进行判断，只要判断出有一个未对无线包进行加密的逻辑无线网络存在，便将确认画面显示于显示部 33（步骤 S204）。步骤 S204 中所显示的确认画面可以是图 7、图 9B、图 11B 中说明过的各种形式的画面。

[0091] 在确认画面中进行前述的规定操作，请求获取部 110 判断为使用者作出了对 WLRD20 中的无线包进行加密的选择的情况下，PC30 的指示部 120 向 WLRD20 发送作为设定指示的更新指令（步骤 S206）。该更新指令可以采用例如“Copy Preset”这样的文字列。

并且，在采用了图 9B、图 11B 中说明过的确认画面的情况下，可以将在画面上选择的逻辑网络的识别符附加为更新指令的参数。

[0092] 接收了设定指示的 WLRD20 的控制部 310 用闪存 ROM400a 的内部所存储的预先设定值 420 来更新闪存 ROM400a 的内部所存储的设定值 410（步骤 S208）。具体而言，控制部 310 提取预先设定值 420 的识别符 PID 与设定值 410 的识别符 EID 相一致的对象，并将预先设定值 420 的各项目（密码键 PEK、加密方式 PEM、认证方法 PAT）的值复制为设定值 410 的各项目（密码键 EEK、加密方式 EEM、认证方法 EAT）的值。此时，若在所接收的更新指令中附加有逻辑网络的识别符，则只更新具有与该逻辑网络的识别符相一致的识别符 EID 的对象。并且，较佳的是，在所接收的更新指令中未附加有逻辑网络的识别符的情况下，若已对设定值 410 存储了涉及安全性的设定值（即，密码键 EEK 栏等中存储着有效的值的情况下），则不对对象进行更新。

[0093] 其后，控制部 310 将更新的结果（成功 / 失败）发送给 PC30（步骤 S210）。在更新的结果为成功的情况下，控制部 310 将更新的结果与被更新的设定值 410 中存储的内容（项目 EIM、识别符 EID、密码键 EEK、加密方式 EEM、认证方法 EAT 的各栏的值）一起发送给 PC30。若更新的结果为“成功”，则 PC30 的指示部 120 根据接收到的设定值 410 中存储的内容，来更新硬盘 200 中存储的安全性设定值 210（步骤 S212）。

[0094] 如上所述那样，在第二实施方式中，WLRD20 的控制部 310 在获取了来自 PC30 的设定指示时，用预设值存储部（预先设定值 420）中存储的预先规定的既定密码键（密码键 PEK）和既定加密方法（加密方式 PEM、认证方法 PAT）来改写设定值存储部（设定值 410）中存储的对无线包进行加密时应使用的现行密码键（密码键 EEK）和现行加密方法（加密方式 EEM、认证方法 EAT）。即，WLRD20 通过接收来自 PC30 的设定指示，用 WLRD20 内部预先规定的密码键和加密方法来对无线包进行加密，因而，能够简便地对 WLRD20 进行涉及安全性的设定。

[0095] 进一步，在第二实施方式中，对于来自 PC30 的希望获取安全性状态的请求，发送安全性状态值 430 中存储的内容，并用设定指令作为来自 PC30 的设定指示。因此，能够减少设定值 410、预先设定值 420 中存储的内容在 WLRD20 与 PC30 之间发送接收的次数。其结果，能够提高安全性设定处理中的保密性。

[0096] < 第三实施方式 >

[0097] 图 15 是表示本发明的第三实施方式的无线通信系统的概要构成的图。与图 1 所示的第一实施方式相比，不同之处在于，具备多个 WLRD(WLRD20v ～ WLRD20z)，其它构成与第一实施方式相同。因而，在以下的说明中，只说明构成及动作与第一实施方式不同的部分，而对于相同的构成，省略其说明。另外，在图中，对于与第一实施方式相同的构成，使用与在前说明过的第一实施方式相同的符号。

[0098] 图 16 是表示第三实施方式中的安全性设定处理的顺序的序列图。与图 6 所示的第一实施方式相比，不同之处在于，增加了步骤 S300，其它处理的概要与第一实施方式相同。以下，主要对与第一实施方式不同的部分进行说明。

[0099] PC30 的请求获取部 110 对所有的 WLRD(WLRD20v ～ WLRD20z) 发送希望获取安全性状态信息的请求（步骤 S100）。接收到该请求的各 WLRD 的控制部 310 向 PC30 发送各自的设定值 410 中存储的内容和预先设定值 420 中存储的内容（步骤 S102）。接收到来自各

WLRD 的应答的 PC30 的请求获取部 110 将为了受理进行安全性设定的 WLRD 的选择而使用的画面显示于显示部 33（步骤 S300）。

[0100] 图 17 是表示为了受理进行安全性设定的 WLRD 的选择而使用的 WLRD 选择画面的一例的图。WLRD 选择画面 WD4 中包含有 WLRD 清单 WLRDL、WLRD 选择按钮 SLB(SLB1 ～ SLB5) 及取消按钮 CB4。WLRD 清单 WLRDL 列出了多个 WLRD 的识别符 (WLRD1 ～ WLRD5)。WLRD 选择按钮 SLB 是对各 WLRD 分配的按钮。无线通信系统 10b 的使用者在 WLRD 选择画面 WD4 中按下为希望进行安全性设定的 WLRD 分配的 WLRD 选择按钮 SLB。若 WLRD 选择按钮 SLB 被按下，则 PC30 的请求获取部 110 显示有关所选择的 WLRD 的确认画面（例如图 7、图 9B、图 11B 中说明过的画面）（步骤 S104）。另外，若取消按钮 CB4 被按下，则图 16 的处理结束。另外，步骤 S106 之后的处理的详细内容与图 6 中说明过的相同。

[0101] 如上所述，基于第三实施方式，也可以得到与第一实施方式相同的效果。并且，在第三实施方式中，还可以在具备多个 WLRD 的无线通信系统中，简便地进行涉及安全性的设定。

[0102] ＜第四实施方式＞

[0103] 图 18 是表示本发明的第四实施方式中的安全性设定处理的顺序的序列图。第四实施方式中的无线通信系统的构成与图 15 中说明过的第三实施方式的相同。

[0104] 第四实施方式与图 16 所示的第三实施方式相比不同之处在于，没有步骤 S300，其它处理的概要与第三实施方式的相同。以下，主要对不同于第三实施方式的部分进行说明。

[0105] 在步骤 S102 中，接收到来自各 WLRD 的应答的 PC30 的请求获取部 110 根据从各 WLRD 接收到的设定值 410 中存储的内容，来判断每一个 WLRD 是否都对无线包进行了加密。请求获取部 110 对所有的 WLRD 进行是否加密的判断，只要判断出有一个未对无线包进行加密的 WLRD 存在，则将图 7 中说明过的确认画面 WD1 显示于显示部 33（步骤 S104）。

[0106] 在图 7 所示的确认画面 WD1 中，若在复选框 CK 中输入了选择符号的状态下按下 OK 按钮 AB1，则请求获取部 110 当作使用者作出了对所有的 WLRD 中的无线包进行加密的选择，从而继续进行处理。

[0107] PC30 的指示部 120 将从各 WLRD 接收到的预先设定值 420 的值复制为设定值 410（步骤 S106）。另外，较佳的是，该数据的复制只对在步骤 S104 中判断为未对无线包进行加密的 WLRD 进行。

[0108] 其后，PC30 的指示部 120 至少向在步骤 S104 中被判断为未对无线包进行加密的所有 WLRD 发送设定指示（步骤 S108）。另外，也可以对所有的 WLRD 广播该设定指示。接收了设定指示的各 WLRD 的控制部 310 用在步骤 S108 接收到的设定指示中包含的各值来分别更新闪存 ROM400 中存储的设定值 410（步骤 S110）。

[0109] 其后，各 WLRD 的控制部 310 将更新的结果（成功 / 失败）发送给 PC30（步骤 S112）。对于更新的结果为“成功”的 WLRD，PC30 的指示部 120 用更新后的密码键、更新后的加密方法来更新硬盘 200 中存储的安全性设定值 210（步骤 S114）。

[0110] 如上所述那样，基于第四实施方式，也能够得到与第一实施方式相同的效果。并且，第四实施方式的 PC30 在受理了使用者所作的对无线包进行加密的选择时，至少向所有未对无线包进行加密的 WLRD 发送设定指示，所以，能够在具有多个 WLRD 的无线通信系统中，较为简便地进行涉及安全性的设定。

[0111] 另外，本发明不受上述实施方式的限定，在不超越其要旨的范围内可以用各种方式来实施，例如，可以进行如下变形。

[0112] 上述实施方式中的无线通信系统的构成只不过是一例而已，也可以采用任何其它方式。例如，可以省略无线通信系统的构成要素中的一部分，也可以对无线通信系统进一步增加构成要素，还可以对无线通信系统的构成要素的一部分进行变更。

[0113] 例如，在上述各实施方式中，是当作 WLRD 和个人电脑在有线连接的状态下进行安全性设定处理的，然而，WLRD 和个人电脑也可以在无线连接的状态下进行上述安全性设定处理。

[0114] 另外，在上文中说明过，上述实施方式中的请求获取部和指示部的功能是通过执行由 CD 装入的用户程序而实现的，然而，请求获取部和指示部的各功能也可以通过将 WLRD 作为服务器的 WEB 系统来提供。即，也可以通过 Web 浏览器从个人电脑接入 WLRD 侧准备好的设定画面显示用地址，并使个人电脑的浏览器显示出设定画面，从而通过利用该浏览器而进行的设定来实现请求获取部和指示部的各项功能。在此情况下，为了提高 WLRD20 和 PC30 之间的保密性，最好利用 HTTPS(Hypertext Transfer Protocol over Secure Socket Layer，安全套接字层上的超文本传输协议）协议。另外，不局限于上述实施方式中记载的 CD，也可以通过 DVD 等合适的非暂时性 (non-transitory) 记录媒介或载波 (propagation signal) 等暂时性的记录媒介来提供用户程序。

[0115] 另外，上述实施方式中的 WLRD 的构成只不过是一例而已，也可以采用任何其它形式的构成。例如，可以对 WLRD 的构成进行如下变形 :省略 WLRD 的构成要素的一部分、或对 WLRD 进一步增加构成要素、或对 WLRD 的构成要素的一部分进行变更。

[0116] 例如，在此是将 WLRD 作为具有用一台可构筑多个逻辑无线网络的多 SSID 功能的无线局域网中继装置，然而，WLRD 也可以是用一台只能构筑一个逻辑无线网络的无线局域网中继装置。在此情况下，设定值、预先设定值、安全性状态的表格中只存储一个对象。

[0117] 另外，在此将设定值、预先设定值及安全性状态值作为 WLRD 的闪存 ROM 中存储的内容来进行了说明。然而，这些表格也可以被存储于闪存 ROM 以外的存储媒介中。例如，也可以当作 WLRD 具备 USB(Universal Serial Bus，通用串行总线）接口，而将上述各表格存储于 USB 存储器等装拆自如的存储媒介中。

[0118] 并且，设定值、预先设定值及安全性状态值的各表格中也可以具备上述说明过的栏之外的其它栏。另外，作为表格中应存储的值，上述实施方式中说明过的值只不过是举例而已，也可以采用任何其它的值。

[0119] 另外，也可以将加密 / 解密部构成为，独立于通信部而存在的进行加密 / 解密的处理部，而不是包含在通信部中的由通信部呼出使用的模块。在此情况下，可通过使加密 / 解密部与通信部协同工作，来发挥上述实施方式中的“通信部”的作用。进一步，在上述的各实施方式中，将无线局域网中继装置当作是在作为外部装置的个人电脑之间能够进行无线通信的构成而进行了说明，但也可以将其构成为，接入点具有无线路由器的功能，个人电脑能够通过具有该无线路由器的功能的无线局域网中继装置与外部局域网或 WAN(Wide Area Network，宽域网）进行通信。

[0120] 并且，对于上述实施方式中说明过的安全性设定处理，可以在不超越本发明的要旨的范围内进行任意变更。例如，可以进行如下变形 :省略安全性设定处理的一部分、或对

安全性设定处理进一步增加处理内容、或对安全性设定处理的一部分进行变更。

[0121] 例如，在上文中说明过，第三、四实施方式中执行的安全性设定处理（图16、18）是第一实施方式的安全性设定处理（图6）的变形。然而，也可以是对第二实施方式的安全性设定处理（图14）的变形。

[0122] 另外，对上述实施方式中示出的确认画面，可以在不超越本发明的要旨的范围内进行任意变更。例如，可以进行如下变形：省略画面显示项目的一部分、或对画面显示项目进一步增加构成要素、或者对画面显示项目的一部分进行变更。

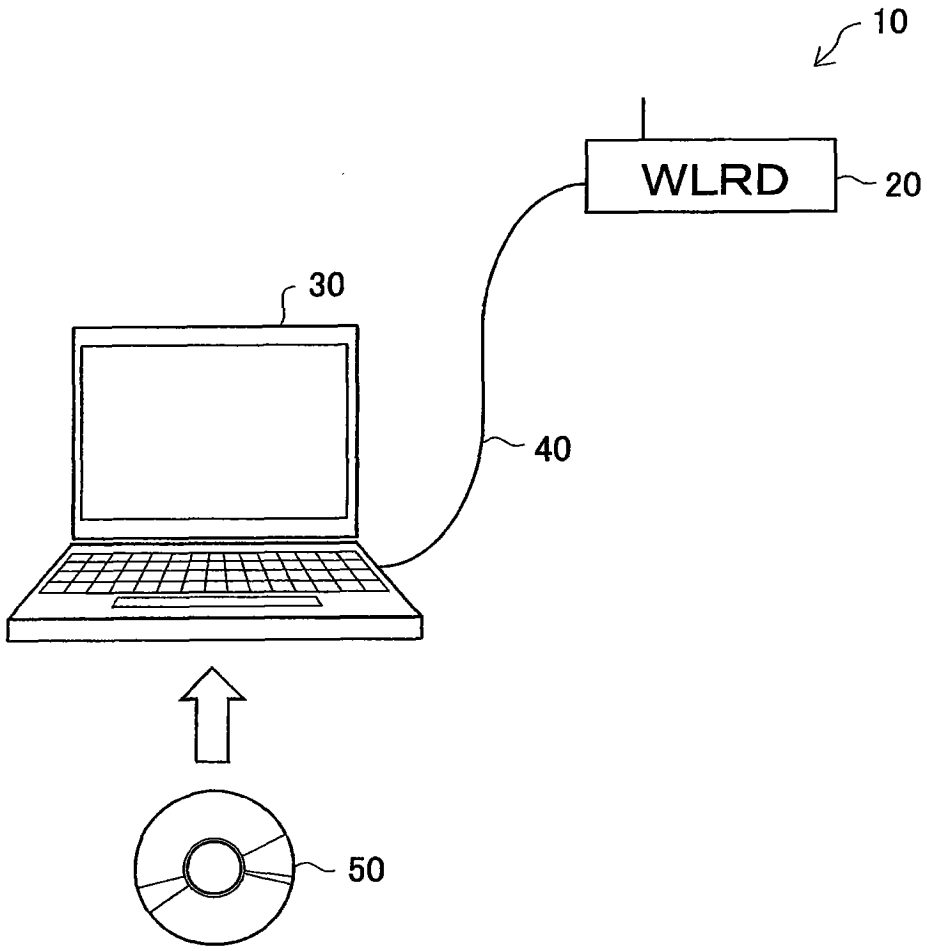


图 1

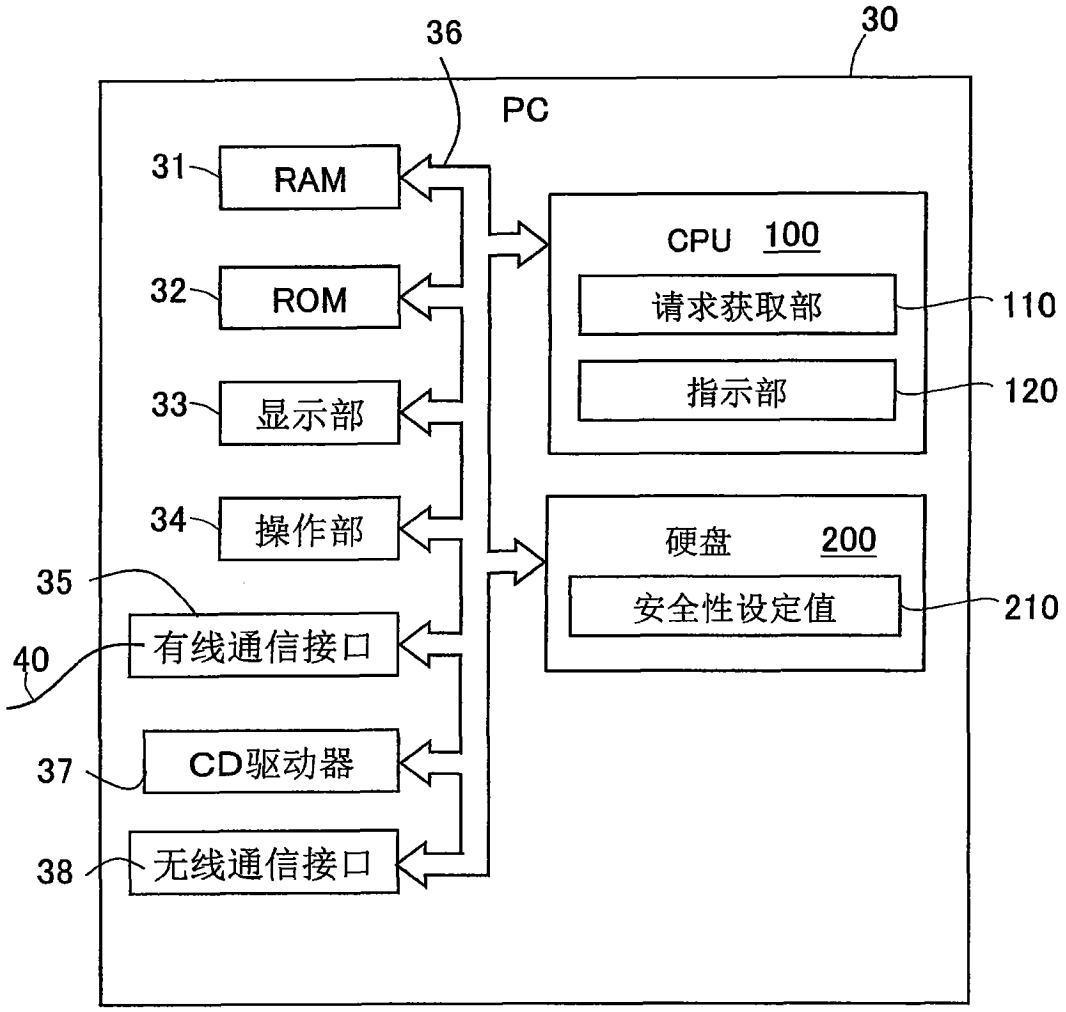

36
30
PC
31
RAM
32
ROM
33
显示部
34
操作部
35
有线通信接口
40
37
CD驱动器
38
无线通信接口
CPU 100
请求获取部
110
指示部
120
硬盘 200
安全性设定值
210

图 2

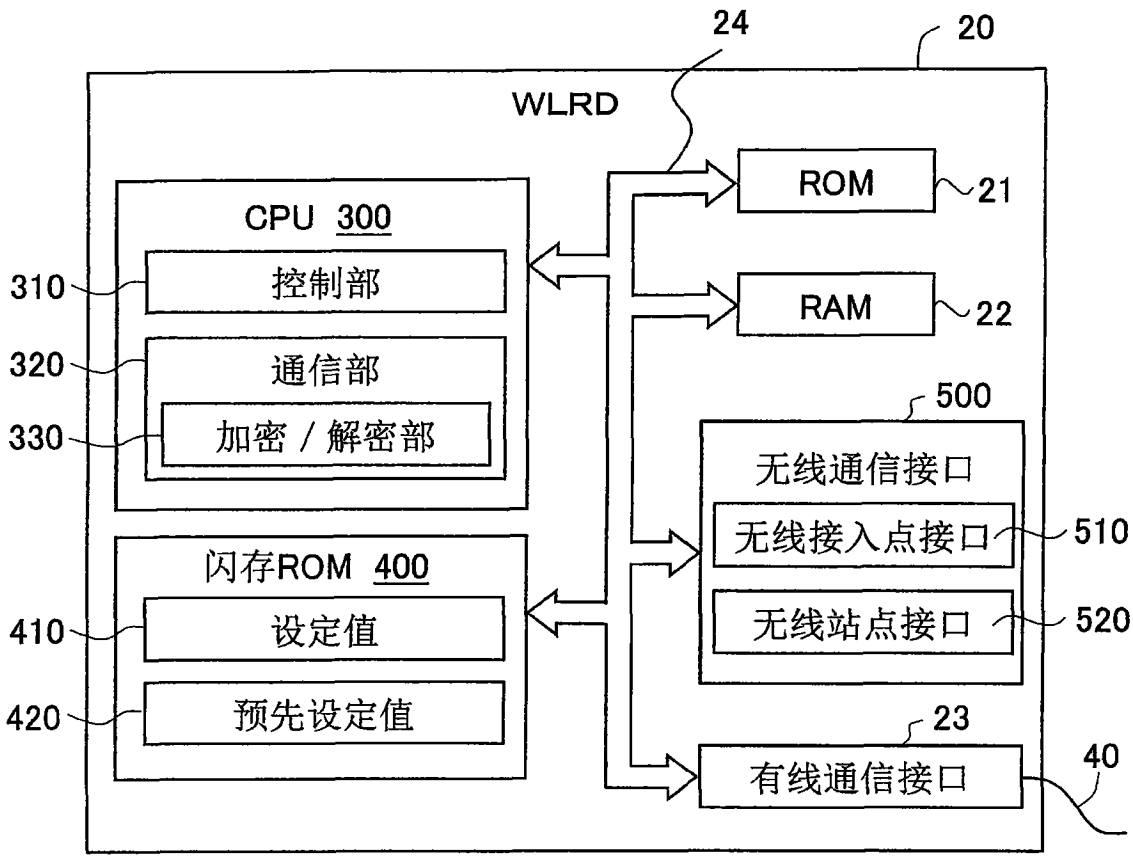


图 3

410

项目:EIM	识别符：EID	密码键：EEK	加密方式：EEM	认证方法：EAT
1	SSID1	No Key	No Encryption	No Authentication
2	SSID2	No Key	No Encryption	No Authentication
3	SSID3	No Key	No Encryption	No Authentication
4	SSID4	No Key	No Encryption	No Authentication

图 4

420

项目:PIM	识别符:PID	密码键:PEK	加密方式:PEM	认证方法:PAT
1	SSID1	11111111…	MIX(TKIP/AES)	WPA2
2	SSID2	22222222…	TKIP	WPA2
3	SSID3	33333333…	AES	WPA2
4	SSID4	44444444…	MIX(TKIP/AES)	WPA2

图 5

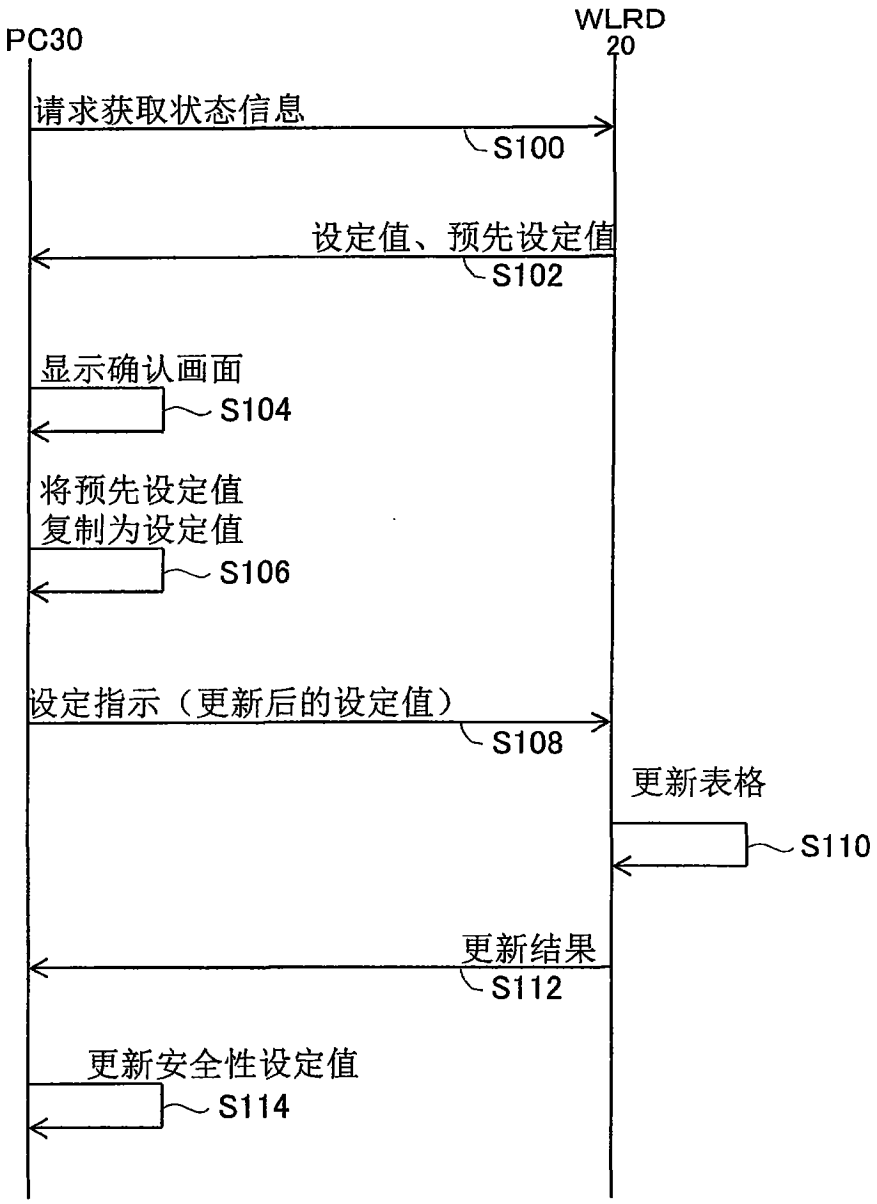


图 6

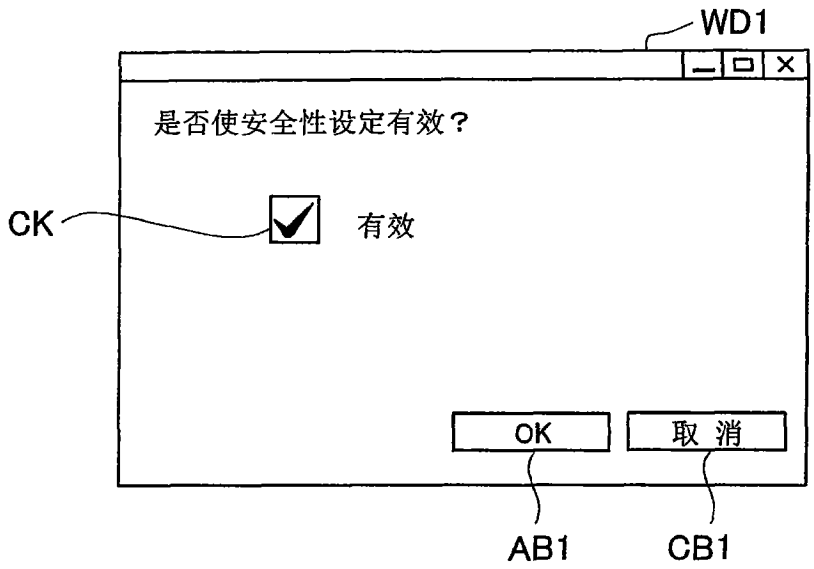


图 7

410

项目:EIM	识别符:EID	密码键:EEK	加密方式:EEM	认证方法:EAT
1	SSID1	11111111…	MIX(TKIP/AES)	WPA2
2	SSID2	22222222…	TKIP	WPA2
3	SSID3	33333333…	AES	WPA2
4	SSID4	44444444…	MIX(TKIP/AES)	WPA2

420

项目:PIM	识别符:PID	密码键:PEK	加密方式:PEM	认证方法:PAT
1	SSID1	11111111…	MIX(TKIP/AES)	WPA2
2	SSID2	22222222…	TKIP	WPA2
3	SSID3	33333333…	AES	WPA2
4	SSID4	44444444…	MIX(TKIP/AES)	WPA2

图 8

410

项目:EIM	识别符:EID	密码键:EEK	加密方式:EEM	认证方法:EAT
1	SSID1	No Key	No Encryption	No Authentication
2	SSID2	12345678…	MIX(TKIP/AES)	WPA2
3	SSID3	No Key	No Encryption	No Authentication
4	SSID4	12345678…	AES	WPA2

图 9A

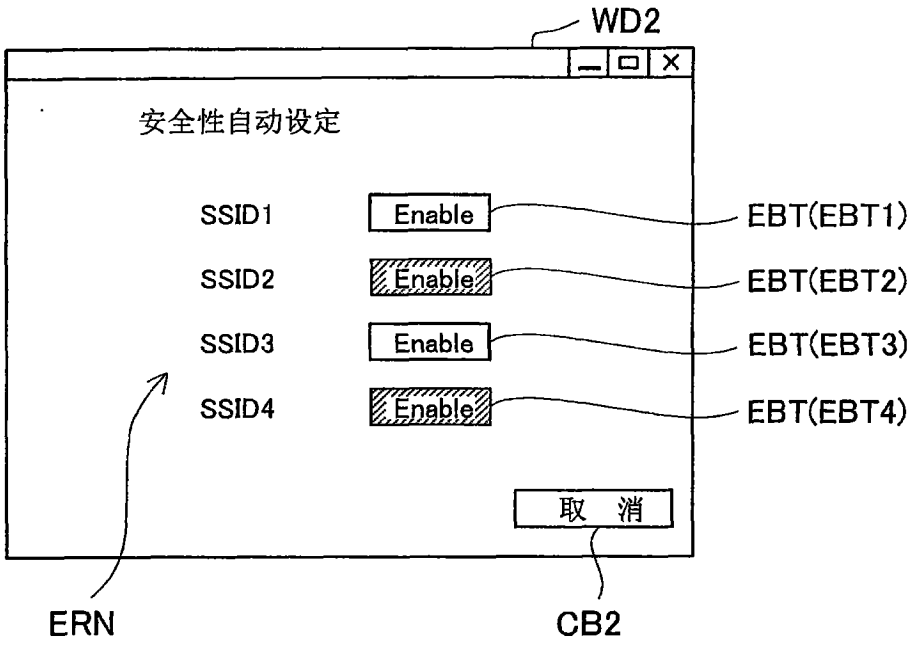


图 9B

410

项目:EIM	识别符:EID	密码键:EEK	加密方式:EEM	认证方法:EAT
1	SSID1	11111111…	MIX(TKIP/AES)	WPA2
2	SSID2	12345678…	MIX(TKIP/AES)	WPA2
3	SSID3	No Key	No Encryption	No Authentication
4	SSID4	12345678…	AES	WPA2

420

项目:PIM	识别符:PID	密码键:PEK	加密方式:PEM	认证方法:PAT
1	SSID1	11111111…	MIX(TKIP/AES)	WPA2
2	SSID2	22222222…	TKIP	WPA2
3	SSID3	33333333…	AES	WPA2
4	SSID4	44444444…	MIX(TKIP/AES)	WPA2

图 10

410

项目:EIM	识别符:EID	密码键:EEK	加密方式:EEM	认证方法:EAT
1	SSID1	No Key	No Encryption	No Authentication
2	SSID2	12345678…	MIX(TKIP/AES)	WPA2
3	SSID3	No Key	No Encryption	No Authentication
4	SSID4	12345678…	AES	WPA2

图 11A

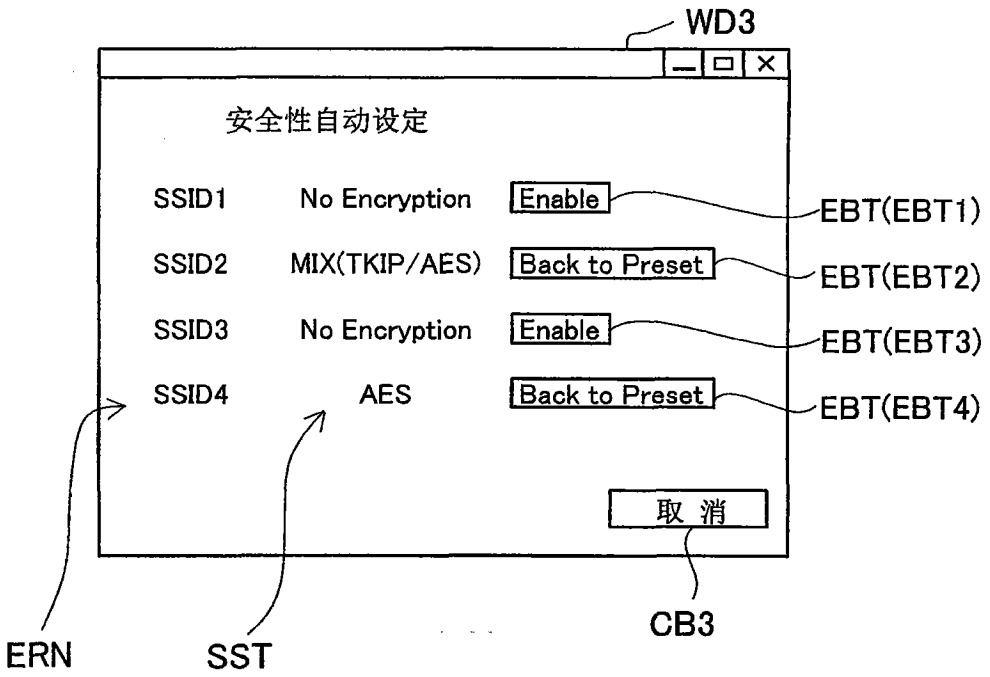

WD3
安全性自动设定
SSID1
No Encryption
Enable
EBT(EBT1)
SSID2
MIX(TKIP/AES)
Back to Preset
EBT(EBT2)
SSID3
No Encryption
Enable
EBT(EBT3)
SSID4
AES
Back to Preset
EBT(EBT4)
取 消
ERN
SST
CB3

图 11B

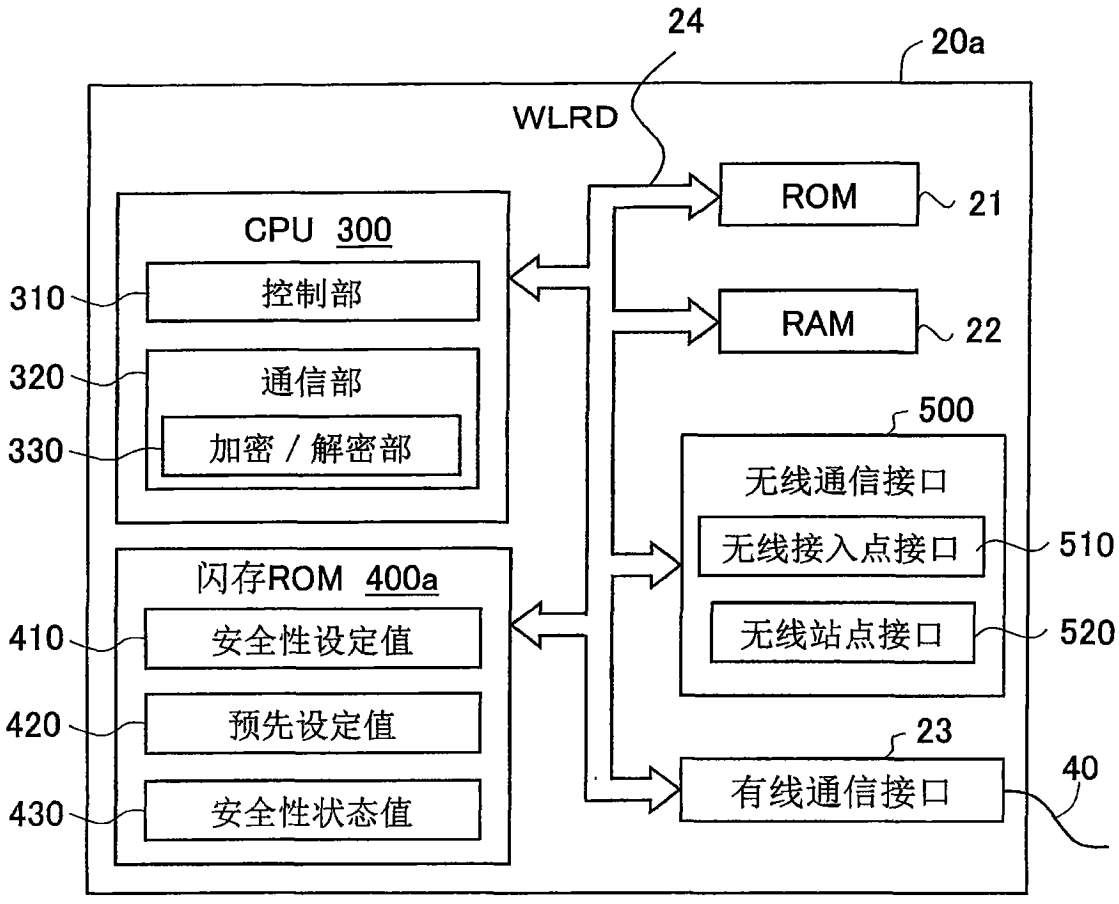

24
20a
WLRD
ROM
21
CPU 300
310
控制部
RAM
22
320
通信部
330
加密 / 解密部
500
无线通信接口
无线接入点接口
510
闪存ROM 400a
410
安全性设定值
无线站点接口
520
420
预先设定值
23
有线通信接口
40
430
安全性状态值

图 12

430

识别符:SID	安全性状态:SST
SSID1	No Security
SSID2	Secure
SSID3	No Security
SSID4	Secure

图 13

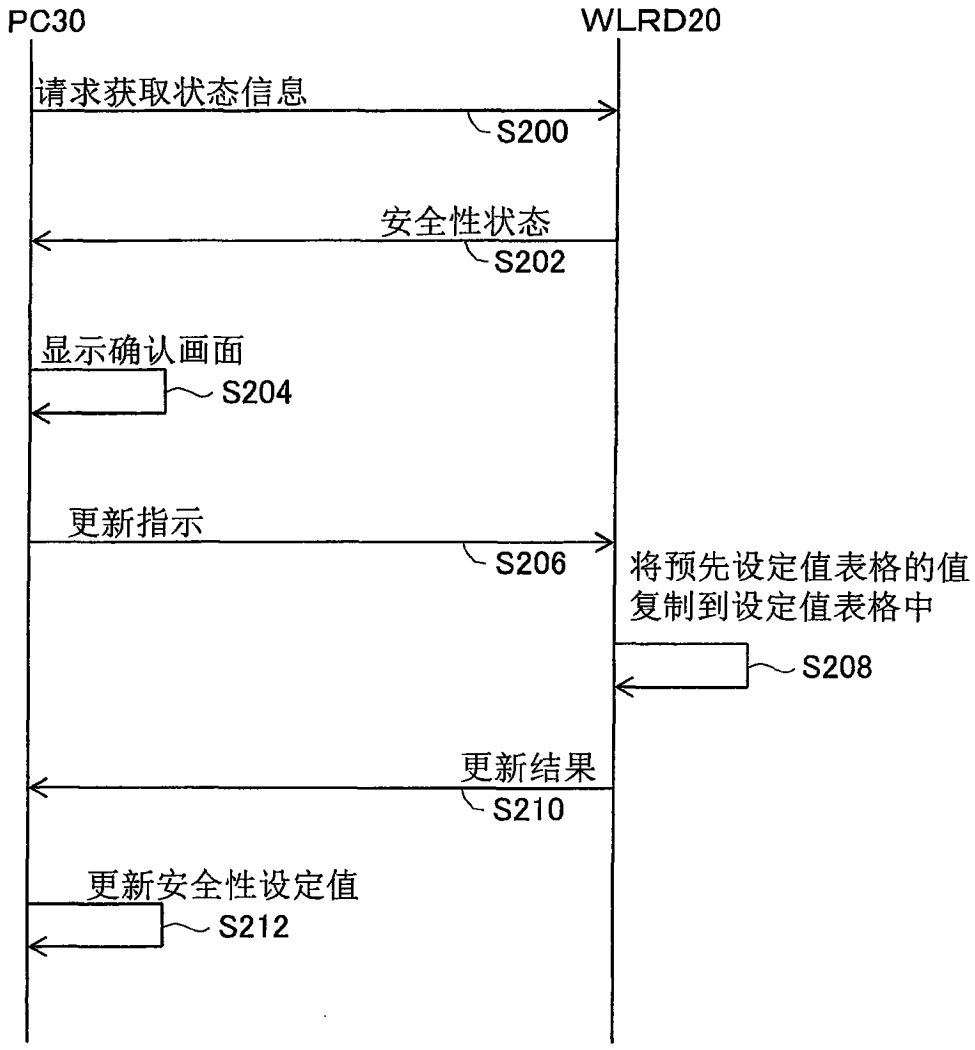


图 14

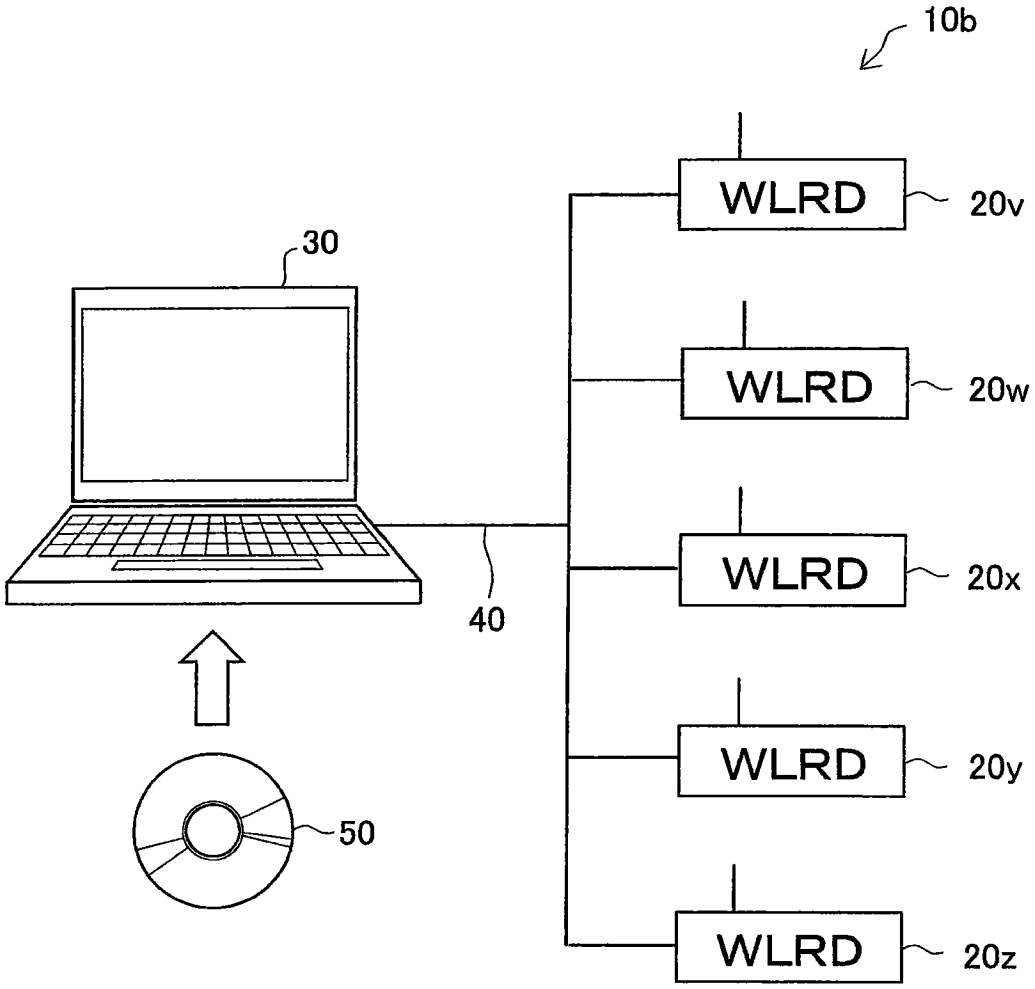


图 15

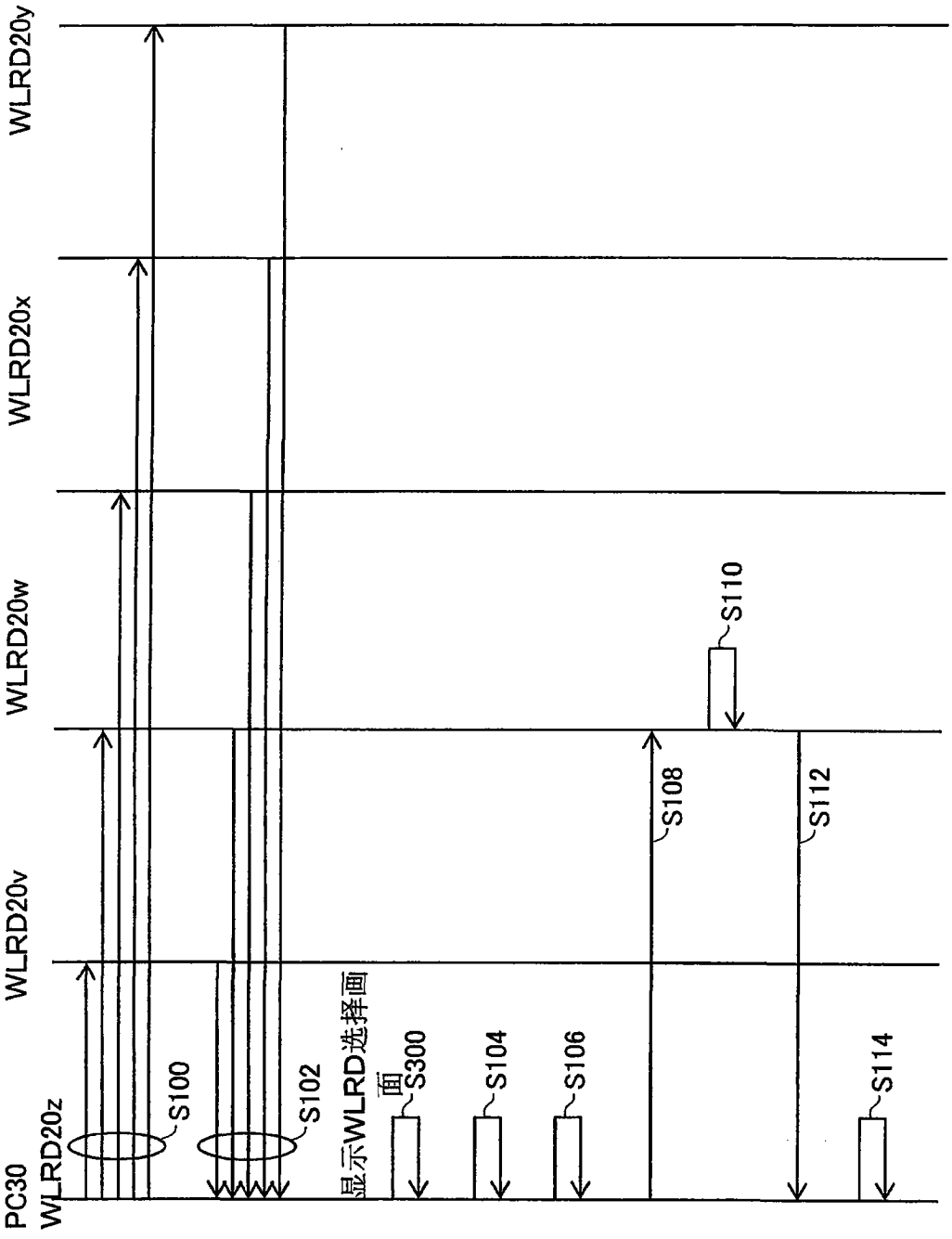

WLRD20y
WLRD20x
WLRD20w
WLRD20v
WLRD20z
PC30
S100
S102
显示WLRD选择画面
S300
S104
S106
S108
S110
S112
S114

图 16

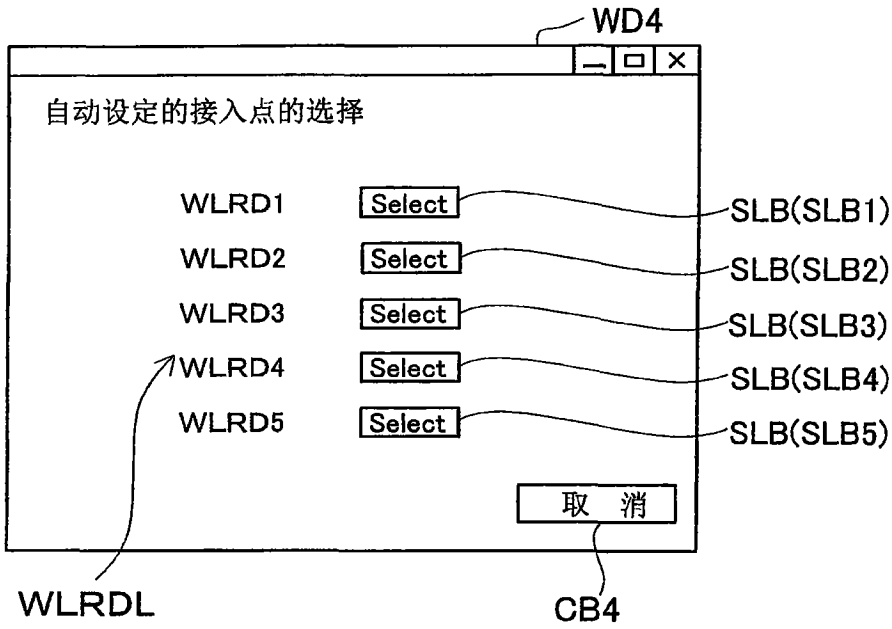

WD4
自动设定的接入点的选择
WLRD1
Select
SLB(SLB1)
WLRD2
Select
SLB(SLB2)
WLRD3
Select
SLB(SLB3)
WLRD4
Select
SLB(SLB4)
WLRD5
Select
SLB(SLB5)
取 消
WLRDL
CB4

图 17

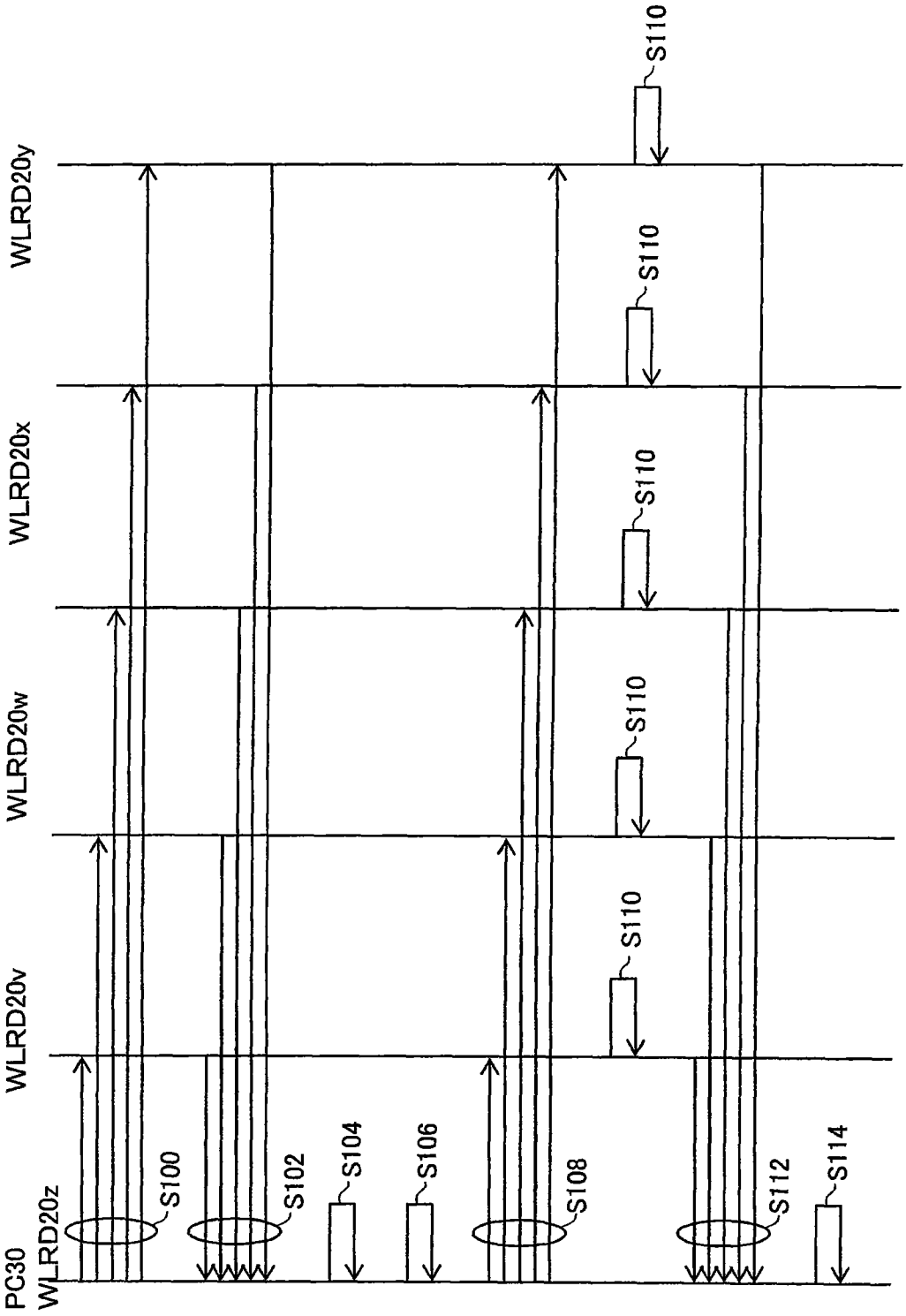

S110
WLRD20y
S110
WLRD20x
S110
WLRD20w
S110
WLRD20v
S110
PC30
WLRD20z
S100
S102
S104
S106
S108
S112
S114

图 18