(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-346702
(P2005-346702A)
(43)公開日　平成17年12月15日(2005.12.15)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330B	5B285
G06F 17/60	G06F	17/60	138	

審査請求 未請求　請求項の数 12　OL　（全 9 頁）

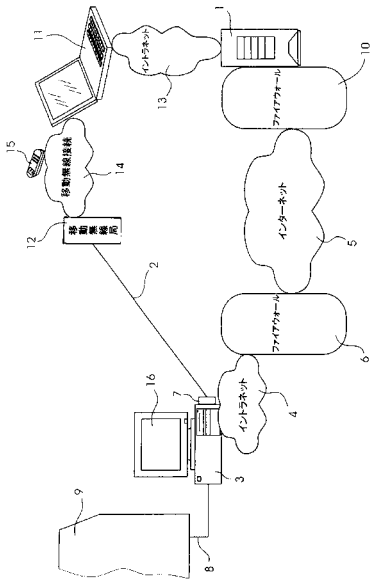
(21)出願番号　特願2005-133875 (P2005-133875)
(22)出願日　平成17年5月2日 (2005.5.2)
(31)優先権主張番号　102004022215.0
(32)優先日　平成16年5月4日 (2004.5.4)
(33)優先権主張国　ドイツ(DE)

(71)出願人　390009232
ハイデルベルガー　ドルツクマシーネン　アクチエンゲゼルシヤフト
Ｈｅｉｄｅｌｂｅｒｇｅｒ　Ｄｒｕｃｋｍａｓｃｈｉｎｅｎ　ＡＧ
ドイツ連邦共和国　ハイデルベルク　クアフユルステン－アンラーゲ　５２－６０
Ｋｕｒｆｕｅｒｓｔｅｎ－Ａｎｌａｇｅ　５２－６０，Ｈｅｉｄｅｌｂｅｒｇ，Ｆｅｄｅｒａｌ　Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｇｅｒｍａｎｙ
(74)代理人　100123788
弁理士　宮崎　昭夫
(74)代理人　100106138
弁理士　石橋　政幸

最終頁に続く

(54)【発明の名称】識別表示装置を備える診断システム

(57)【要約】
【課題】サービス作業員が処理機械のコンピュータのデータまたは操作インターフェイスへ匿名でアクセスするのを回避する。
【解決手段】印刷機９を作動させるための第１のコンピュータ３へのアクセスは製造業者または保守会社の第２のコンピュータ１からのみ可能となっている。第２のコンピュータ１は、アクセスする資格を与えられた作業員についてのアクセスデータが保存された認証装置を有しており、認証装置によって識別確認された作業員が第１のコンピュータ３にアクセスする前に、当該作業員のアクセスデータが第２のコンピュータから第１のコンピュータへ送信され、当該作業員を認識可能にする表示が、第１のコンピュータ３と接続された表示装置１６に行われる。
【選択図】図１



【特許請求の範囲】
【請求項１】
機械を作動させるための少なくとも１つの第１のコンピュータ（３）のデータまたは操作インターフェイスへ少なくとも１つの第２のコンピュータ（１，１１）から、保護され認証されたアクセスをする電子システムにおいて、
前記第２のコンピュータ（１，１１）からのみ前記第１のコンピュータ（３）の前記データまたは前記操作インターフェイスへアクセスすることができ、前記第２のコンピュータ（１，１１）は、アクセスする資格を与えられた前記作業員についてのアクセスデータが保存された認証装置を有しており、前記第２のコンピュータ（１，１１）の、アクセスする資格を与えられ識別確認された前記作業員を認識可能にする表示が、前記第１のコンピュータ（３）の前記データまたは前記操作インターフェイスへのアクセスの前に、前記第１のコンピュータ（３）と接続された表示装置（１６）に行われることを特徴とするシステム。
【請求項２】
前記第２のコンピュータ（１，１１）と前記第１のコンピュータ（３）はインターネット（５）を介して相互に接続される、請求項１に記載のシステム。
【請求項３】
前記第１のコンピュータ（３）と前記第２のコンピュータ（１，１１）はイントラネット（４，１３）を介して相互に接続されている、請求項１または２に記載のシステム。
【請求項４】
識別確認された前記各作業員に一対一に割り当てられた身分証明写真が、識別確認の時に、前記第１のコンピュータ（３）の前記表示装置（１６）に表示される、請求項１から３のいずれか１項に記載のシステム。
【請求項５】
前記作業員の、保存されている個人データを当該作業員自身が変更することができない、請求項１から４のいずれか１項に記載のシステム。
【請求項６】
管理者アクセス権によってのみ前記作業員のデータを変更することができる、請求項５に記載のシステム。
【請求項７】
前記コンピュータ（３，１，１１）間のデータ交換の間に、実行されているデータ交換を記録する記憶能力が前記コンピュータ（３，１，１１）の少なくとも１つに与えられている、請求項１から６のいずれか１項に記載のシステム。
【請求項８】
印刷機とデータ通信をするために設けられている、請求項１から７のいずれか１項に記載のシステム。
【請求項９】
機械を作動させるための少なくとも１つの第１のコンピュータ（３）のデータまたは操作インターフェイスへ少なくとも１つの第２のコンピュータ（１，１１）から、保護され認証されたアクセスをする方法において、
前記第２のコンピュータ（１，１１）からのみ前記第１のコンピュータ（３）の前記データまたは前記操作インターフェイスへアクセスすることができ、前記第２のコンピュータ（１，１１）は、前記作業員の識別確認をする装置を有しており、前記第２のコンピュータ（１，１１）の、アクセスする資格を与えられ識別確認された前記作業員を認識可能にする表示が、前記第１のコンピュータ（３）の前記データまたは前記操作インターフェイスへのアクセスの前に、前記第１のコンピュータ（３）と接続された表示装置（１６）に行われることを特徴とする方法。
【請求項１０】
前記第２のコンピュータ（１，１１）は、前記第１のコンピュータ（３）がアクセスを許可した場合にのみ、前記第１のコンピュータ（３）の前記データまたは前記操作インタ

ーフェイスへアクセスすることができる、請求項９に記載の方法。
【請求項１１】
前記データが前記第２のコンピュータ（１，１１）と前記第１のコンピュータ（３）の間で暗号化されて送信される、請求項９または１０に記載の方法。
【請求項１２】
前記第１のコンピュータ（３）の前記データまたは前記操作インターフェイスへの前記第２のコンピュータ（１，１１）からのアクセスを拒否する操作部材が前記第１のコンピュータ（３）に設けられている、請求項１０に記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、機械を作動させるための少なくとも１つの第１のコンピュータのデータまたは操作インターフェイスへ、少なくとも１つの第２のコンピュータから、保護され認証されたアクセスをする電子システムおよび方法に関する。
【背景技術】
【０００２】
産業界における処理機械は、磨耗や他の不具合による停止時間をできるだけ短く抑えるために、絶えず保守整備され、検査されなくてはならない。さらに、近年の処理機械では、産業用機械のデータを継続的に検査し、場合によってはインターネットとイントラネットを介して処理機械に保守作業を行うために、機械の制御コンピュータを、インターネットとイントラネットを介して、その機械の製造業者のサービスコンピュータと接続することが可能である。この場合、サービス作業員は産業用機械の運用者の会社の現場を訪れなくてもよく、機械の、いわゆる遠隔保守と遠隔診断を行うことができる。
【０００３】
数値制御される産業用処理機械の、コンピュータを用いた取り扱いと管理を利用したこのようなシステムが特許文献１から知られている。この場合、処理機械は、インターネットのようなデータ通信接続を介して製造業者またはサービス会社のメインコンピュータと接続された、機械側の作業コンピュータを備えている。メインコンピュータは、機械の状態のデータを処理機械の作業コンピュータからリアルタイムで呼び出してメインコンピュータに送信させ、その後、メインコンピュータ上で分析と評価を行うことができる。その後、場合によっては起こり得る問題を取り除くために、データを機械側の作業コンピュータに送り返すことができ、すなわち、照会した機械状態データから、例えば数値制御式の産業用処理機械に発生している問題を早期に発見し、それに対応する対応策を早めに開始することができる。さらに、処理機械が、改善された機械データをメインコンピュータから得られるように、機械状態データを評価することもできる。
【０００４】
このようなシステムでは、処理機械の運用者は、自分の処理機械のコンピュータに無資格者がアクセスするのを容認することはできないので、サービス作業員の識別と認証が重大な役割を果たす。すなわち、処理機械を担当する製造業者または保守会社だけが、その処理機械のコンピュータへ実際にアクセスできることが絶対に保証されなくてはならない。処理機械のコンピュータと製造業者のメインコンピュータは、多くの場合、インターネット接続を介して相互に通信しているので、この通信は、インターネットに関して知られているあらゆる危険と結び付いている。こうした危険を最低限に抑えるために、従来技術では、処理機械のコンピュータとメインコンピュータの接続を暗号化したり、あるいは、所定のコンピュータによってのみ処理機械のコンピュータへアクセスできるようにしたりされている。
【特許文献１】独国特許出願公開第１０１５２７６５号明細書
【発明の開示】
【発明が解決しようとする課題】

【０００５】
さらに、処理機械の多くの運用者は、念のため、自分が信頼する特定の者によってのみ自分の機械が保守整備されるようにしたいので、機械の製造業者または保守会社に、決まった担当者がいてほしいと望んでいる。
【０００６】
そこで、本発明の目的は、遠隔保守や遠隔診断の、顧客の受諾を増やすために、サービス作業員が処理機械のコンピュータのデータまたは操作インターフェイスへ匿名でアクセスするのを回避することにある。
【課題を解決するための手段】
【０００７】
本発明によれば、この目的は請求項１および９によって達成される。本発明の有利な実施態様が、従属請求項および図面から得られる。本発明のシステムでは、運用者の機械は、当該機械に付属し、ネットワーク接続を介して製造業者またはサービス・保守会社の少なくとも１つの第２のコンピュータと通信することができる少なくとも１つの第１のコンピュータを有している。このような通信接続は例えばインターネットを介して行うことができ、この際、このような接続は、第１のコンピュータから第２のコンピュータへ、およびこれと逆方向へ、実際にデータを送信すべき時にだけ行われなければならない。第１のコンピュータは、インターネットからのデータトラフィックを監視し、特に、第１のコンピュータへの外部からの無資格のアクセスを防止する安全対策ソフトウェアである、いわゆるファイアウォールによってインターネットに対して保護されているので、原則として、第１のコンピュータと第２のコンピュータの間の、インターネットを介した接続は、第１のコンピュータからしか確立することができない。しかし、本明細書の他の個所で特に説明する方法によって、第２のコンピュータから接続を確立することも可能である。そして、機械の第１のコンピュータのデータへの匿名のアクセスを防ぐために、本発明によれば、第１のコンピュータのデータまたは操作インターフェイスへのアクセスが第２のコンピュータからのみ可能であり、認証されていない第３のコンピュータからは可能ではなく、第２のコンピュータは、アクセスする資格を与えられた作業員についてのアクセスデータが保存された認証装置を有しており、第２のコンピュータの、アクセスする資格を与えられ識別確認された作業員を認識可能にする表示が、第１のコンピュータのデータまたは操作インターフェイスへのアクセスの前に、第１のコンピュータと接続された表示装置に行われることが意図されている。
【０００８】
それによって、実際に第２のコンピュータからのみ、すなわち製造業者またはサービス会社のコンピュータからのみ、特に、第１のコンピュータのデータにアクセスすることができ、特に、この選択された第２のコンピュータにのみデータが送信されることが保証される。したがって、第三者のコンピュータが無資格で第１のコンピュータへアクセスすることはできないので、第三者のコンピュータにはデータが送信されない。このように、第２のコンピュータが第１のコンピュータへのアクセスのフィルタとして働き、したがって、第２のコンピュータによってアクセスを認証された者しか、第１のコンピュータのデータへアクセスすることができない。そのため、サービス作業員は、第２のコンピュータと接続されている他のコンピュータにログオンしなくてはならない。このような認証装置は、例えば、対応する作業員のユーザ名とこれに付属するパスワードの入力を要求する。これらのデータによって、アクセスしている作業員を一対一に識別確認し、それによって、匿名のアクセスを回避することができる。こうして識別確認されたサービス作業員のデータは、例えば第１のコンピュータの画像スクリーンのような表示装置上に表示することができ、それによって、機械の運用者は、今実際に誰が自分の機械のデータにアクセスしようとしているのかを、画像スクリーン上ではっきりと認識することができる。
【０００９】
本発明の１つの実施態様では、識別確認される各作業員に一対一に割り当てられるべき身分証明写真が、識別確認の時に第１のコンピュータの表示装置に表示されることが意図

されている。このようにして、機械の運用者は、アクセスする者の氏名のような個人データに加えて、またはその代わりに、アクセスする作業員の、視覚的な他の表示を得ることができる。このような表示は、例えば身分証明写真を、アクセスデータの構成要素として第２のコンピュータに保存しておくことによって実現することができる。そして、この写真は、第１のコンピュータのデータへのアクセスの前に、他の識別データと共に第１のコンピュータへ送信される。対応するサービス作業員の名前と写真が第１のコンピュータの画像スクリーンに表示される。このように写真を送信することによって、作業員についての、機械の運用者への訴えかけが強められ、望ましくない匿名性がいっそう低減される。

【００１０】

さらに、保存されている作業員の個人データを作業員自身が変更できないことが意図されている。安全性に関する機械運用者の要求は高いので、運用者に送信された個人情報、例えばアクセスしているサービス作業員の名前や身分証明写真が、実際にアクセスしている者に一対一に割り当てられているのを、運用者が確信できることが重要である。このため、アクセスするサービス作業員は、自分のデータを自分自身でも変更できない。そうしないと、不正操作の恐れがあるからである。作業員は自分のユーザ名とパスワードによって、または他の識別確認によって、第２のコンピュータにログオンし、その後、データにアクセスすることしかできない。しかし、サービス作業員は、第１のコンピュータの画像スクリーンへの自分の個人データの表示に影響を与えることはなく、したがって、作業員による不正操作は不可能である。

【００１１】

本発明の特に有利な実施態様では、作業員のデータは管理者アクセス権によってのみ変更可能であることが意図されている。作業員のデータは、例えば新しいサービス作業員が採用され各機械の保守を任された時や、他の理由で保守作業員のデータが変わった時に、状況に応じて所定の間隔で更新しなくてはならない。しかし、データの、このような変更は所定の者、すなわち、第２のコンピュータのシステム管理者にしか行うことができない。それによっても、作業員のデータを変更する者が作業員自身と同一人物ではないことが保証される。保存されているサービス作業員のデータのあらゆる変更について単独で責任を負う者しか管理者として認められないので、この安全対策によっても、作業員によるデータの不正操作が困難になる。

【００１２】

さらに、コンピュータ間でデータ交換が行われる間に、実行されているデータ交換を記録する記憶能力をコンピュータの少なくとも１つに与えることが意図されるのが好ましい。場合によっては発生する問題や、機械の運用者による苦情のあった場合に、データ交換を追跡できるようにするために、第１のコンピュータ、第２のコンピュータ、または他のコンピュータにデータ交換を記録することができる。さらに、本発明のシステムによって、データ交換を引き起こした者を一対一に識別することができるので、記録されているデータをその者に一対一に結び付けることができる。それによって、誰がどのデータをいつの時点でどの機械と交換したか、その交換時にどのような問題が発生したか、および、場合によっては誰によってその問題が引き起こされたかを追跡することができる。これによって、データ交換の状況を容易に追跡することができるので、機械の運用者における安全性も、製造業者や保守会社における安全性も高められる。

【００１３】

さらに、第１のコンピュータのデータへの第２のコンピュータからのアクセスを拒否する操作部材が第１のコンピュータに設けられていることが意図されるのが好ましい。運用者の第１のコンピュータの画像スクリーンに個人データが表示された後、運用者自身が、自分のコンピュータへのアクセスを操作部材によって意のままに拒否することができる。例えば自分の知らない人物、または自分の機械の保守をする資格を与えられていない人物が、自分の機械の第１のコンピュータにアクセスしようとしているのを運用者が確認する場合、運用者は、その人物の、一対一に割り当てられた名前と身分証明写真に基づいてこのような事態を容易に知ることができ、操作部材によって保守アクセスを拒否することが

できる。それによって、自分のコンピュータのデータへのその人物のアクセスが一度妨げられる。あるいは、この実施態様は、機械の運用者が、自分が拒否した人物が自分のコンピュータへさらにアクセスするのを禁止し、拒否した人物が将来的にも自分のコンピュータへのアクセスをいっさい行えないように拡張することもできる。本発明のシステム、および本発明の方法によって、自分のコンピュータへのアクセスについて自分自身で決定するこができ、誰が自分のコンピュータにアクセスしようとしているのかいつでも認識できるようにしたいという、運用者の希望が大幅に考慮される。それにもかかわらず、サービス作業員は保守アクセスをいつでも開始することができ、定まった保守インターバルに拘束されろことはない。

【発明を実施するための最良の形態】

【００１４】

次に、本発明の実施の形態について図面を参照して説明する。

【００１５】

図１によれば、本発明のシステムは、印刷機９の保守や診断をする時にデータを照会する、または操作インターフェイスへアクセスするのに用いられている。印刷機９は、接続回線８を介して、印刷機９の運用者の所にある第１のコンピュータ３と接続されている。第１のコンピュータ３は同時に印刷機９の制御コンピュータであってもよく、画像スクリーン１６を有しているのが目的に適っている。図１によれば、第１のコンピュータ３は、印刷機９の運用者の室内に設置された第１のイントラネット４、およびインターネット５を介して、印刷機の製造業者の室内にある第２のコンピュータ１にデータを送信するための接続を確立することができる。第１のコンピュータ３と第２のコンピュータ１は、第１のコンピュータ３のデータを第２のコンピュータ１によってのみ受信することができるようにプログラミングされている。このことは、無資格者が第１のコンピュータ３のデータへアクセスするのを防ぐ助けになる。サービス作業者が印刷機９の遠隔保守を行うことができる他のコンピュータ１１が、印刷機の製造業者の所にある第２のイントラネット１３を介して第２のコンピュータ１と接続されている。このようにして、保守をする資格を与えられた各人は、識別確認に成功した後、自身のラップトップのコンピュータ１１、第２のイントラネット１３の接続、および第２のコンピュータ１を介して第１のコンピュータ３のデータにアクセスすることができる。

【００１６】

さらに、図１によれば、印刷機９の運用者の第１のイントラネット４への無資格者の侵入を防ぐために、第１のイントラネット４はインターネット５に対してファイアウォール６によって保護されている。ファイアウォール６は、原則として、第２のコンピュータ１がインターネット５を介して第１のコンピュータ３へアクセスするのも妨げるので、第１のコンピュータ３のデータへのアクセスは、常に、第１のコンピュータ３から開始される。この場合、通常、運用者が、保守ボタンを押すことによるローカルな入力を行うことによって、接続が第１のコンピュータ３から確立させられる。他の実施形態では、第１のコンピュータ３がモデム７を備え電話網２に接続されている場合、第１のコンピュータ３の、第２のコンピュータ１への接続をいつでもリーモートでも確立することができる。このモデム７は、所定の呼出信号を着信した時に、第１のコンピュータ３の、第２のコンピュータ２への接続を確立するが、呼出信号の受信後に電話の接続が再び切られるので、データが電話網２を介して送信されないように構成されている。この呼出信号によって、アクセスしているサービス作業員が保守会社に所属していることがまず識別される。この際、この呼出信号の発信は、サービス作業者のコンピュータ１１から、コンピュータ１１に内蔵されているモデムを介して行うか、あるいは、電話番号が、第２のコンピュータ１への第１のコンピュータ３の接続を確立するために認証された呼出信号として承認されている、他の各電話を介して行うことができる。図１によれば、許可を受けている移動電話１５から、移動無線接続１４と移動無線局１２を介して、呼出信号を電話網２へ転送することもできる。あるいは、ラップトップのコンピュータ１１が移動無線モデムとしてＧＳＭ（Global system for mobile communication）移動無線カードを備えていてもよく、その結

果、呼出信号は移動無線接続１４を介してコンピュータ３のモデム７へ送信される。したがって、第１のコンピュータ３から第２のコンピュータ１へデータを送信するための接続は、保守会社の電話接続からしか確立することができず、無資格の第三者が確立することはできない。第２のコンピュータ１は他のファイアウォール１０によってインターネット５に対して保護されている。

【００１７】

ただし、保守作業員は、自分のコンピュータ１１からデータを呼び出せるようになる前に、コンピュータ１１上で、サービスポータルのソフトウェアによってまず識別確認をしなければならない。そのために、作業員は、少なくとも自分のユーザ名とこれに付属するパスワードを入力しなくてはならない。本発明によれば、たとえばトークンカードによって生成されるワンタイム・パスワードを利用することを特徴とする厳しい認証が要求される。さらに、サービス作業員の、虚偽の識別確認を防止するために、指紋読み取り装置や虹彩認識用のカメラをラップトップのコンピュータ１１に設けてもよい。この際、サービス作業員のデータが第２のコンピュータ１に保存されているので、原則として、第２のコンピュータ１と接続され、サービスポータルのソフトウェアを利用できるどのコンピュータ１１からでも、識別確認とそれに続くデータ照会、または操作インターフェイスへのアクセスを行うことができる。

【００１８】

作業員の識別確認が成功し、電話網２を介してのデータ呼出の開始に成功すると、本来のデータ呼出が行われる前に、まず、アクセスしているサービス作業員の個人データが第２のコンピュータ１からインターネット５を介して第１のコンピュータ３へ送信される。すると、第１のコンピュータ３の画像スクリーン１６に、少なくともサービス作業員の名前が表示され、サービス作業員の身分証明写真も表示されるのが好ましい。このようにして、印刷機９の運用者は、どの作業員が自分のコンピュータ３に今アクセスしようとしているのかを明瞭に知ることができる。例えば、所定の人物だけが印刷機９の保守作業をしてよいことを印刷機９の製造業者と運用者の間の保守契約の中で取り決めることができる。運用者が画像スクリーン１６上に自分の知らない人物、または望んでいない人物を確認した時は、自分のコンピュータ３のキーボードを介してデータおよび操作インターフェイスへのアクセスを防ぎ、望んでいない人物を拒否することができる。さらに、本発明のシステムは、望んでいない人物が一度拒否された後は、その人物が、第１のコンピュータ３に対して、限られた回数しかアクセスを試みることができないようにプログラミングされていてもよい。あるいは、サービスポータルは、一度拒否された人物が第１のコンピュータ３へのそれ以後のアクセスを禁じられるようにプログラミングされていてもよい。このように、印刷機９の運用者は、どの人物が自分のコンピュータ３に今アクセスしようとしているかを常に知らされ、望んでいない人物を拒否することができる。

【図面の簡単な説明】

【００１９】

【図１】印刷機の運用者の所にある第１のコンピュータと、印刷機の製造業者の所にある保守用の２つのコンピュータを備える保守・診断システムを示す図である。

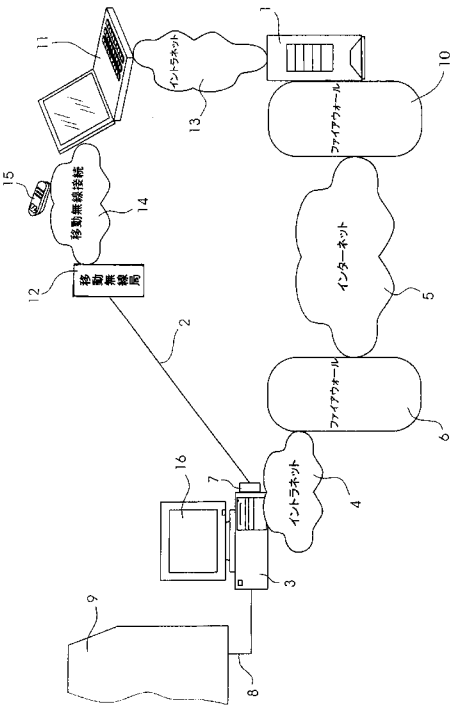
【符号の説明】

【００２０】

１，３，１１　コンピュータ
２　電話網
４，１３　イントラネット
５　インターネット
６，１０　ファイアウォール
７　モデム
８　接続回線
９　印刷機
１２　移動無線局

１４　移動無線接続
１５　移動電話
１６　画像スクリーン

【図１】



フロントページの続き

(74)代理人 100120628
弁理士 岩田 慎一
(74)代理人 100127454
弁理士 緒方 雅昭
(72)発明者 トム オエルスナー
ドイツ連邦共和国 ６０４３９ フランクフルト／マイン ゲルハルトーハウプトマンーリンク１９２

Ｆターム(参考) 5B285 AA04 CB01