【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成19年1月18日(2007.1.18)

【公開番号】特開2005-295038(P2005-295038A)
【公開日】平成17年10月20日(2005.10.20)
【年通号数】公開・登録公報2005-041
【出願番号】特願2004-104635(P2004-104635)
【国際特許分類】
　Ｈ０４Ｌ　12/28　　(2006.01)
【ＦＩ】
　Ｈ０４Ｌ　12/28　　２００Ｚ

【手続補正書】
【提出日】平成18年11月22日(2006.11.22)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　セキュリティ通信を行うために必要な情報を第１の装置と第２の装置に提供する提供装置であって、
　セキュリティ通信を行うためのパラメータの候補を、第１の装置及び第２の装置から受信する受信手段と、
　第１の装置及び第２の装置から受信したパラメータの候補に基づいて、セキュリティ通信を行うために必要な情報を生成する生成手段と、
　前記生成手段により生成されたセキュリティ通信を行うために必要な情報を、前記第１の装置及び第２の装置に送信する送信手段とを有することを特徴とする提供装置。
【請求項２】
　第１の装置と第２の装置がセキュリティの確保された通信を行うために必要な情報を第１の装置と第２の装置に提供する提供装置であって、
　第１の装置と第２の装置間の通信を識別する識別情報、及び、セキュリティを確保するためのパラメータの候補を、第１の装置及び第２の装置から受信する受信手段と、
　第１の装置及び第２の装置から受信したパラメータの候補に基づいて、通信のセキュリティを確保するために必要な情報を生成する生成手段と、
　識別情報により識別される通信のセキュリティを確保するために前記生成手段により生成された前記通信のセキュリティを確保するために必要な情報を、前記第１の装置及び第２の装置に送信する送信手段とを有することを特徴とする提供装置。
【請求項３】
　セキュリティ通信を行うために必要な情報を第１の装置と第２の装置に提供する提供方法であって、
　セキュリティ通信を行うためのパラメータの候補を、第１の装置及び第２の装置から受信し、
　第１の装置及び第２の装置から受信したパラメータの候補に基づいて、セキュリティ通信を行うために必要な情報を生成し、
　前記生成されたセキュリティ通信を行うために必要な情報を、前記第１の装置及び第２の装置に送信することを特徴とする提供方法。
【請求項４】

第１の装置と第２の装置がセキュリティの確保された通信を行うために必要な情報を第１の装置と第２の装置に提供する提供方法であって、
第１の装置と第２の装置間の通信を識別する識別情報、及び、セキュリティを確保するためのパラメータの候補を、第１の装置及び第２の装置から受信し、
第１の装置及び第２の装置から受信したパラメータの候補に基づいて、通信のセキュリティを確保するために必要な情報を生成し、
識別情報により識別される通信のセキュリティを確保するために前記生成された前記通信のセキュリティを確保するために必要な情報を、前記第１の装置及び第２の装置に送信することを特徴とする提供方法。
【請求項５】
請求項３の提供方法を実現するためのプログラム。
【請求項６】
請求項４の提供方法を実現するためのプログラム。
【請求項７】
通信相手との間で行う通信のセキュリティを確保するために必要な情報を提供装置から受け取る通信装置であって、
セキュリティを確保するためのパラメータの候補を、提供装置に送信する送信手段と、
セキュリティを確保するために必要な情報を、提供装置から受信する受信手段と、
前記受信手段により提供装置から受信した情報を元に、通信相手との通信にセキュリティを確保するセキュリティ確保手段とを有することを特徴とする通信装置。
【請求項８】
通信相手との間で行う通信のセキュリティを確保するために必要な情報を提供装置から受け取る通信装置であって、
通信相手との間で確立された通信を識別する識別子、及び、セキュリティを確保するためのパラメータの候補を、提供装置に送信する送信手段と、
セキュリティを確保するために必要な情報を、提供装置から受信する受信手段と、
前記受信手段により提供装置から受信した情報を元に、通信相手との間で確立された通信にセキュリティを確保するセキュリティ確保手段とを有することを特徴とする通信装置。
【請求項９】
通信相手との間で行う通信のセキュリティを確保するために必要な情報を提供装置から受け取る通信方法であって、
セキュリティを確保するためのパラメータの候補を、提供装置に送信し、
セキュリティを確保するために必要な情報を、提供装置から受信し、
前記提供装置から受信した情報を元に、通信相手との通信にセキュリティを確保することを特徴とする通信方法。
【請求項１０】
通信相手との間で行う通信のセキュリティを確保するために必要な情報を提供装置から受け取る通信方法であって、
通信相手との間で確立された通信を識別する識別情報、及び、セキュリティを確保するためのパラメータの候補を、提供装置に送信し、
セキュリティを確保するために必要な情報を、提供装置から受信し、
前記提供装置から受信した情報を元に、通信相手との間で確立された通信にセキュリティを確保することを特徴とする通信方法。
【請求項１１】
請求項９の提供方法を実現するためのプログラム。
【請求項１２】
請求項１０の提供方法を実現するためのプログラム。
【請求項１３】
前記パラメータの候補は、認証アルゴリズム又は暗号化アルゴリズムの候補であること

を特徴とする請求項１又は２の提供装置、請求項５又は６のプログラム、請求項７又は８の通信装置、もしくは、請求項１１又は１２のプログラム。
【請求項１４】
前記必要な情報は、認証アルゴリズム又は暗号化アルゴリズムであることを特徴とする請求項１又は２の提供装置、請求項５又は６のプログラム、請求項７又は８の通信装置、もしくは、請求項１１又は１２のプログラム。
【請求項１５】
前記必要な情報は、セキュリティを確保するための鍵であることを特徴とする請求項１又は２の提供装置、請求項５又は６のプログラム、請求項７又は８の通信装置、もしくは、請求項１１又は１２のプログラム。