ストレージデバイスを複数用いた機密情報の分散通信手法*

東京電機大学 理工学部 情報システム工学科†
小野 真和 高橋 広幸 桧垣 博章‡ §

1 背景と目的

近年、インターネットやLANなどのコンピュータネットワークの発達により、様々なデジタルデータがネットワークを介して伝送されている。同時に機密性が必要となるデータもネットワークを介して伝送されるようになり、伝送の際の安全性が求められている。ネットワークを介したデータ伝送の際には、第三者によるデータの傍受や改ざんが不正に行なわれる危険性がある。この問題の解決方法として暗号化技術が挙げられる。暗号化技術を用いたデータ伝送は、送信元で暗号化処理を行ない、暗号化データをネットワークを用いて伝送し、受信先で復号化処理を行なって機密データの平文を得る技術である。ネットワーク上で暗号化データが傍受された場合でも平文データではないため、そのままでは機密情報の内容を読みとることはできない。各暗号化手法は解読に要する時間が十分に長いことを安全性の根拠としているが、第三者は暗号化データをネットワークから得ることができるため、強度の高い暗号化を施したとしても複数の高性能なコンピュータを用いることで解読される可能性がある。以上により、機密データの伝送に暗号化技術は有用であると考えられる。しかし、ネットワークを介さずにオフラインでデータを移動する方法は、暗号化データを傍受される危険性の低い、より安全な伝送手法であると考えられる。

一方、近年の半導体メモリの大容量化、小型化、低価格化により、パーソナルコンピュータのUSB(Universal Serial Bus) インタフェースに接続するフラッシュメモリを用いたストレージデバイス (以下、USBフラッシュメモリとよぶ) が開発されている。USBフラッシュメモリの筐体は10cm程度のスティック形状で、5ー20グラム程度と小型、軽量であり、2GBの記録容量をもつ製品も存在する。また、USBポートをもつコンピュータの多くでソフトウェアを追加することなく使用できる。以上の特徴を持つUSBフラッシュメモリは、文書や画像などのデジタルデータを持ち運ぶ手軽な記録メディアである。全世界における出荷数は2002年の500万台から、2003年の3000万台へ増加し、一般に広く普及している。

USBフラッシュメモリを用いてデータをオフラインで持ち歩くことができる。このとき、ネットワーク上の第三者によるデータの傍受は不可能である。すなわち、セキュアな通信路が実現されているといえる。しかし、盗難や紛失によってUSBフラッシュメモリが第三者の手に渡ると、USBフラッシュメモリに書き込まれているデータは容易に第三者がアクセスすることが可能であるという問題点がある。ここで、第三者がアクセスしてもデータの読み取りを防ぐために、USBフラッシュメモリ内のデータを暗号化しておくことが考えられる。この場合、暗号鍵の配送を適切に実現しなければならない。USBフラッシュメモリ内のデータにアクセスする可能性のあるすべてのコンピュータに暗号鍵を格納する方法では、鍵を変更するごとに鍵交換プロトコルを実行することが必要となる。また、限られたコンピュータでしかアクセスすることができなくなる。一方、暗号鍵をもUSBフラッシュメモリに格納する方法では、盗難、紛失した場合には、ネットワークにおける傍受と同様、すべてのデータが第三者の手に渡ることとなり、暗号化データがすべて解読されることとなる。

本論文では、USBフラッシュメモリを用い、各USBフラッシュメモリにデータの一部を暗号化したデータを格納するとともに、暗号鍵を異なるUSBフラッシュメモリに格納することで機密データのためのセキュアな通信路を実現する手法を提案する。

2 従来手法

暗号通信に用いられる秘密暗号鍵は送信元と送信先で共有することが必要である。秘密鍵の共有のために、公開鍵暗号方式に基づいた、公開鍵基盤PKI(Public Key Infrastructure) などのプロトコルを用いる必要がある。公開鍵暗号方式を用いても、共有する秘密鍵はネットワーク上で交換されるため、傍受される可能性がある。

また、TCP/IPインターネットなどのネットワークを介してデータを通信する際、暗号化データを含むパケット群は単一経路で配送される。そのため、盗聴者は一箇所の経路を特定することで、すべてのデータを傍受することが可能である。この問題に対し、IP通信拡散手法 [2] が提案されている。IP通信拡散手法ではパケットの配送に単一経路を用いず、オンデマンドに決定された複数経路を用いてパケットを配送する。したがって、盗聴者がすべてのデータを傍受することは困難である。しかし、一部の経路が特定され、データの一部を傍受される可能性がある。

データ通信の際にオフラインのメディアを用いる、Webコンテンツの可搬性が検討されている [3]。ここでは、大容量のコンテンツをあらかじめディスク装置に格納し、これを輸送することで、広帯域なネットワークを用いて通信するよりも低いダウンロードコストで通信できる可能性を示している。

本論文の手法においては、オフラインで通信することにより、配送中のデータや暗号鍵が傍受されることを防止している。また、USBフラッシュメモリそのものが第三者に入手された場合でも、USBフラッシュメモリ単体では暗号データの一部のみしか獲得することができず、さらに、秘密鍵は他のUSBフラッシュメモリに格納されることから、第三者が平文データを得ることは

*Secure Communication with Multiple Storage Devices
†Tokyo Denki University
‡Masakazu Ono, Hiroyuki Takahashi and Hiroaki Higaki
§{masa, hiro, hig}@higlab.k.dendai.ac.jp

できない。

3 提案手法

オフラインの通信路として USB フラッシュメモリを複数個用い、機密データを安全に通信できる手法を提案する。USB フラッシュメモリへのデータ格納を送信、他のコンピュータでのデータ復元を受信とする。本手法では機密データはすべて USB フラッシュメモリに保存されるため、第三者がネットワークを介して機密データを得ることはできない。複数の USB フラッシュメモリは利用者が別々の場所に厳重に保管、移動することが必要である。USB フラッシュメモリのいずれかを紛失あるいは盗難されたとしても、機密データのすべてを第三者が得ることはできず、正規の利用者は機密データが紛失または盗難されたことを発見することが可能である。

以下に提案手法における送信手順と受信手順を示す。なお、ここでは図 1 に示すように通信路として n 個の USB フラッシュメモリを使用する場合を考える。

[送信手順]

1. 機密データ D を $D_1, \cdots, D_n$ に分割する。
2. 暗号化に用いる鍵 $Key_1, \cdots, Key_n$ をそれぞれ独立に生成する。
3. 各分割データ D_i を鍵 Key_i で暗号化し、暗号文 $encript(D_i, Key_i)$ を得る。
4. USB フラッシュメモリ M_i には、暗号文 $encript(D_i, Key_i)$ と鍵 $Key_{(i+1) \bmod n}$ を格納する。

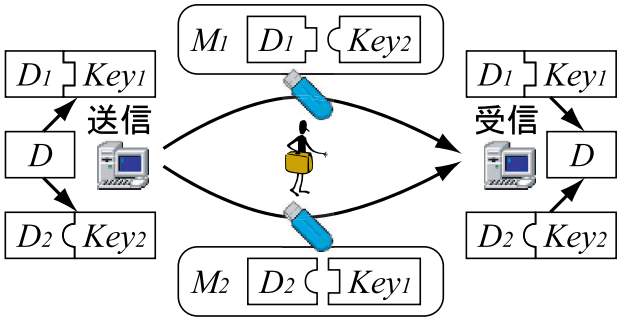

図 1: データの送信・受信

このとき、それぞれの USB フラッシュメモリ M_i に格納されている暗号文 $encript(D_i, Key_i)$ は、同じ USB フラッシュメモリ M_i に格納されている暗号鍵 $Key_{(i+1) \bmod n}$ を用いて復号することはできない。すなわち $decript(encript(D_i, Key_i), Key_{(i+1) \bmod n}) \neq D_i$ である。盗聴者が D_i を入手するためには、$encript(D_i, Key_i)$ を格納した USB フラッシュメモリ M_i と Key_i を格納した $M_{(i-1) \bmod n}$ の 2 つの USB フラッシュメモリを入手しなければならない。

次に受信の手順を示す。

[受信手順]

1. 各 USB フラッシュメモリ M_i に格納された暗号文 $encript(D_i, Key_i)$ と暗号鍵 $Key_{(i+1) \bmod n}$ を取り出す。
2. $encript(D_i, Key_i)$ と Key_i から $D_i = decript(encript(D_i, Key_i), Key_i)$ を入手する。
3. すべての D_i を結合し、機密データ D を得る。

4 評価

提案手法を UNIX 上のアプリケーションとして実装し、動作速度の測定を行った。USB フラッシュメモリには USB1.1 規格と USB2.0 規格の製品があり、読み書きの速度性能が異なることから、複数種類の USB フラッシュメモリを用いて測定を行った。なお、同時に読み書きを行う 2 つの USB フラッシュメモリは同一製品を用いた。測定を行った環境は Pentium4(2.0GHz)、メモリ 512MB、USB2.0 ポートを持つパーソナルコンピュータを用い、OS は RedHat Linux8.0(Kernel 2.4.18-14) を用いた。また、暗号方式として DES [1] を用いた。データを暗号化した場合と暗号化しない場合のアクセス速度を測定した。1MByte から 10MByte までの 1MByte 毎のデータに対してそれぞれ 10 回処理を行い、平均値を求めた。アクセス速度の平均値を表 1 に、暗号化処理による速度低下の割合を表 2 に示す。

表 1: アクセス速度の性能評価結果 [Kbyte/sec]

処理	送信		受信	
暗号化の有無	有	無	有	無
製品 A(USB1.1)	688.2	729.0	1352.9	1729.2
製品 B(USB1.1)	660.9	714.0	1363.9	1748.0
製品 C(USB2.0)	1069.0	1286.6	1360.8	1754.8
製品 D(USB2.0)	1586.6	2115.2	1362.0	1746.7

表 2: 暗号化処理による速度低下の評価結果 [%]

	送信	受信
製品 A(USB1.1)	5.6	21.8
製品 B(USB1.1)	7.4	22.0
製品 C(USB2.0)	16.9	22.5
製品 D(USB2.0)	25.0	22.0

表 2 より、転送速度の遅い USB フラッシュメモリでは速度低下は少ないといえるが、転送速度の速い USB フラッシュメモリでは速度低下の割合が大きい。これは USB フラッシュメモリの読み書き速度よりも暗号処理に時間がかかっているためと考えられる。

5 まとめ

オフラインの通信手段である USB フラッシュメモリを複数用いて、機密情報を安全に通信する手法を提案した。本手法は暗号化に用いる秘密鍵をデータとは異なる USB フラッシュメモリに格納するため、分割、暗号化されたデータの一部が第三者に漏洩した場合でも、暗号解読は困難である。また、暗号化のためのアクセス速度は 20%程度の低下であり、実用的であるといえる。今後は処理速度の向上、他の暗号化方式の使用について検討する。

参考文献

[1] ANSI X3.92, “American National Standard for Data Encryption Algorithm (DEA),” American National Standards Institute (1981).

[2] 有泉, 寺西, 横山, 桧垣, “IP 通信拡散手法を用いた VPN 装置の実装と性能評価,” 情報処理学会マルチメディア通信と分散処理ワークショップ論文集, Vol. 2003, No. 19, pp. 55–60 (2003).

[3] 中川, 杉浦, 井上, 木村, 土池, “コンテンツ容量から見た情報モビリティに関する検討,” 情処研報, Vol. 2003, No. 93, pp. 39–44 (2003).