

ユビキタスセキュリティ —監視映像情報セキュリティ—

山口晃由*
山田敬喜**
松井 充***

Ubiquitous Security—Information Security for Surveillance Camera System—

Teruyoshi Yamaguchi, Keiki Yamada, Mitsuru Matsui

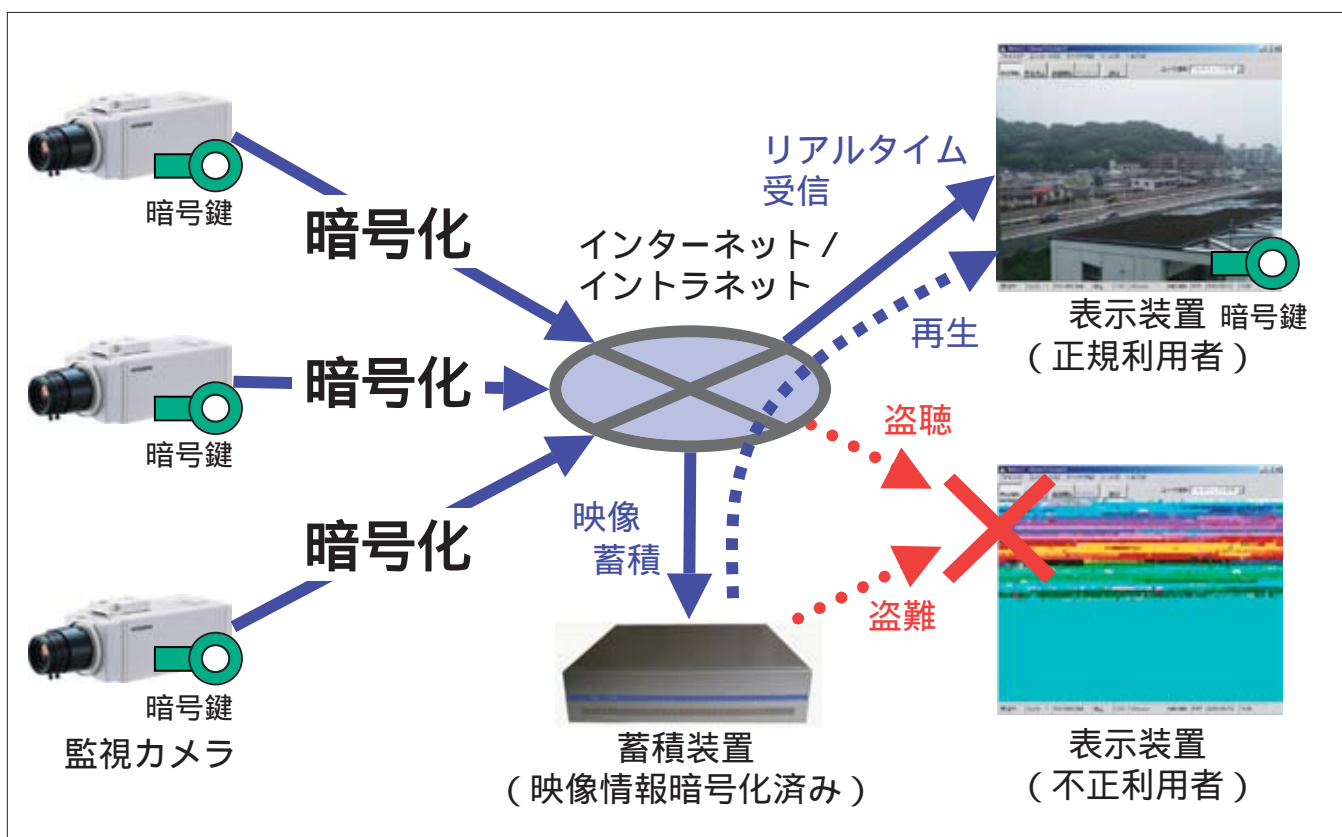
要 旨

近年の犯罪率増加と犯罪検挙率減少を背景として、ビル・マンション・商店街等を中心に、監視カメラを用いた映像監視システムを導入する動きが広がっている。一方で、無制限な監視カメラの設置はプライバシーを侵害するという声も少なからずある。映像情報を適切に扱うことで、映像監視への理解を得ることができる。特に通信路の盗聴や映像を蓄積したストレージの盗難といった不正な漏洩(ろうえい)から、映像情報を保護する必要がある。

このような漏洩から映像情報を保護する方法として、映像を暗号化し、閲覧可能者を限定する方法がある。しかしながら、映像監視システムでは、CPU(Central Process-

ing Unit)速度やメモリ容量などのハードウェア的な制約、画像サイズ・フレームレート(1秒間に何枚の映像を流せるか)などの性能的な制約の下で、映像を暗号化することが要求される。特に、監視カメラや表示装置では、演算に組み込みマイコンを用いるため、暗号処理は非常に重い処理となる点が問題である。この解決のために暗号処理ハードウェアを追加することは、大幅なコスト増につながり、好ましくない。

本稿では、映像監視システムにおいても要求される性能を満たしつつ暗号処理を実現する技術について述べる。具体的には、組み込みマイコンでも高速に処理が行える暗号アルゴリズム、及び高効率画像暗号化法について論じる。



映像監視システムにおける映像情報の暗号化

映像監視システムは、多数の監視カメラで撮影した映像を蓄積し、必要に応じて表示を行う。近年、映像監視システムもデジタル化が進み、インターネットや共用LAN(Local Area Network)を使って映像を配信している。そこで、通信・蓄積の過程での映像の盗聴や盗難に対して映像情報を保護するために、カメラで撮影した映像をリアルタイムで暗号化し、表示装置においてリアルタイムに復号する。監視カメラと同じ暗号鍵(かぎ)を持つ正規利用者は映像を正しく表示できるが、暗号鍵を持たない不正利用者は映像を正しく表示できない。