玉川大学
量子情報科学研究所

研究開発プロジェクト

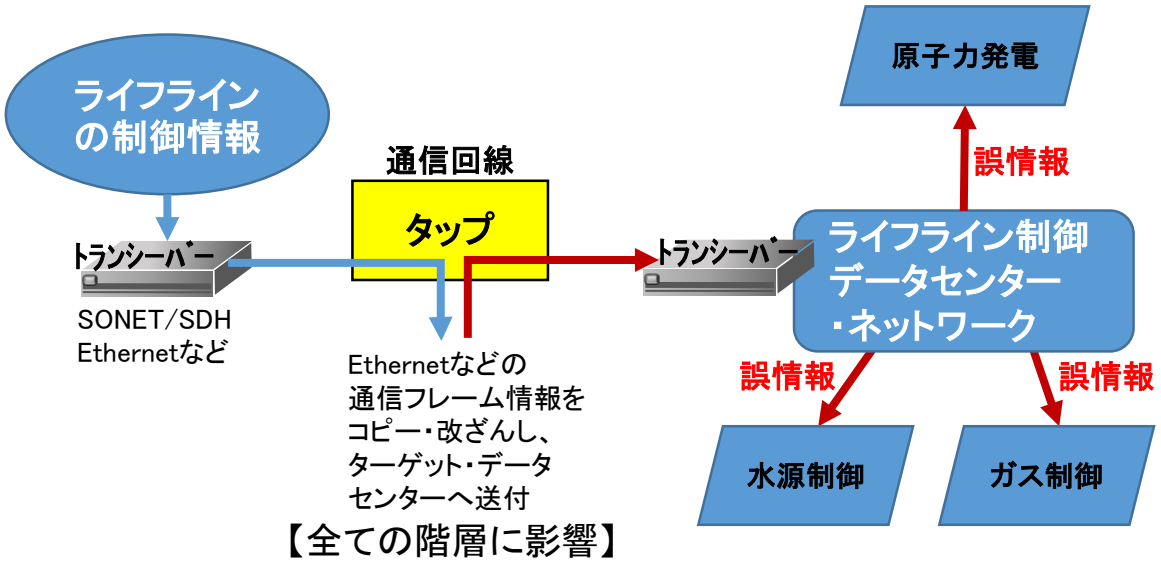
量子エニグマ暗号

[2015年3月23日]

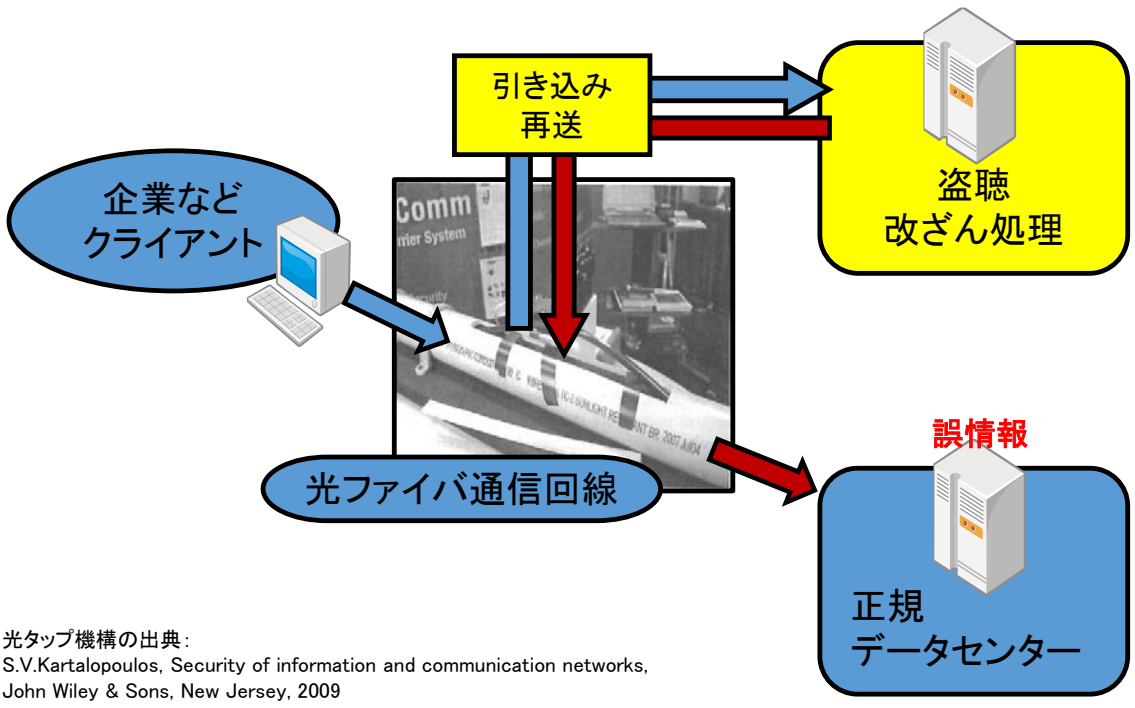
〒194-8610 東京都町田市玉川学園6-1-1 TEL 042-739-8674

物理階層へのサイバー攻撃による インフラ破壊

攻撃法（1箇所からネットワーク全体を破壊）



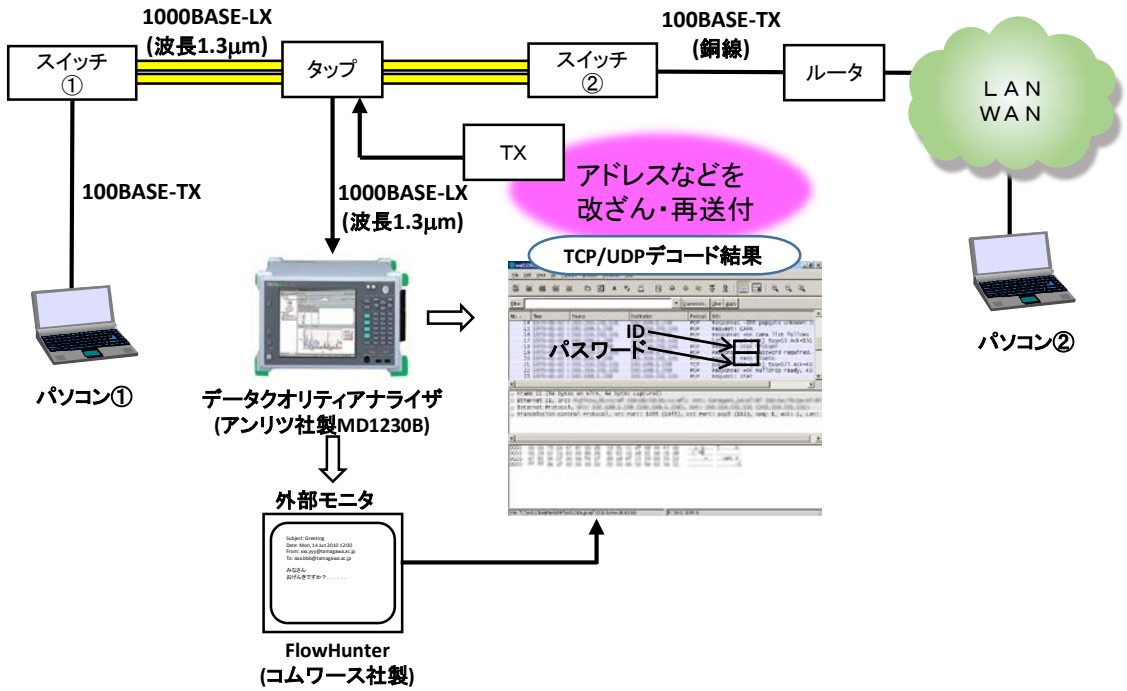
現実の海底光ケーブル攻撃事例（2013年）



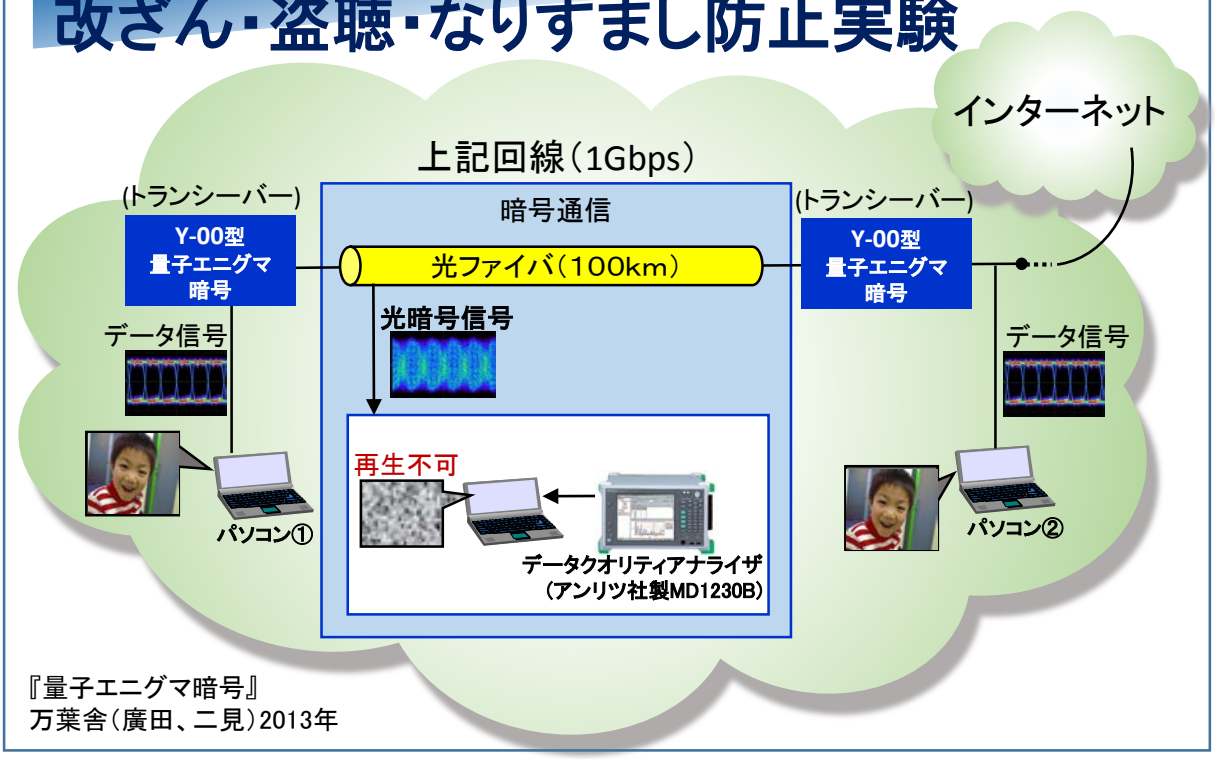
光タップ機構の出典：
S.V.Kartalopoulos, Security of information and communication networks, John Wiley & Sons, New Jersey, 2009

玉川大学量子情報科学研究所

光回線からのタッピングによる電子メール改ざん実験



改ざん・盗聴・なりすまし防止実験



『量子エニグマ暗号』
万葉舎（廣田、二見）2013年

2015/3/23

玉川大学量子情報科学研究所
＝ 量子エニグマ暗号 ＝

量子エニグマ暗号の安全性

数理暗号で光信号をスクランブル

↓

光信号を量子効果によって正しく測定させない機構

↓

数理暗号が量子効果によって情報理論的安全になる

基本Y-00プロトコル

光信号を測定する際に発生する非エルゴード的
量子雑音によって信号をマスクする機構

（加法性雑音はエルゴード性があるため、
補助的な役割で利用可）

量子エニグマ暗号

基本Y-00では暗号関数となる擬似乱数の数学的構造
を十分マスクすることができない。
量子ゆらぎ拡散機構を付与し、完全マスキングを持つ
プロトコルを量子エニグマ暗号という。

『量子エニグマ暗号』
万葉舎（廣田、二見）2013年

2015/3/23