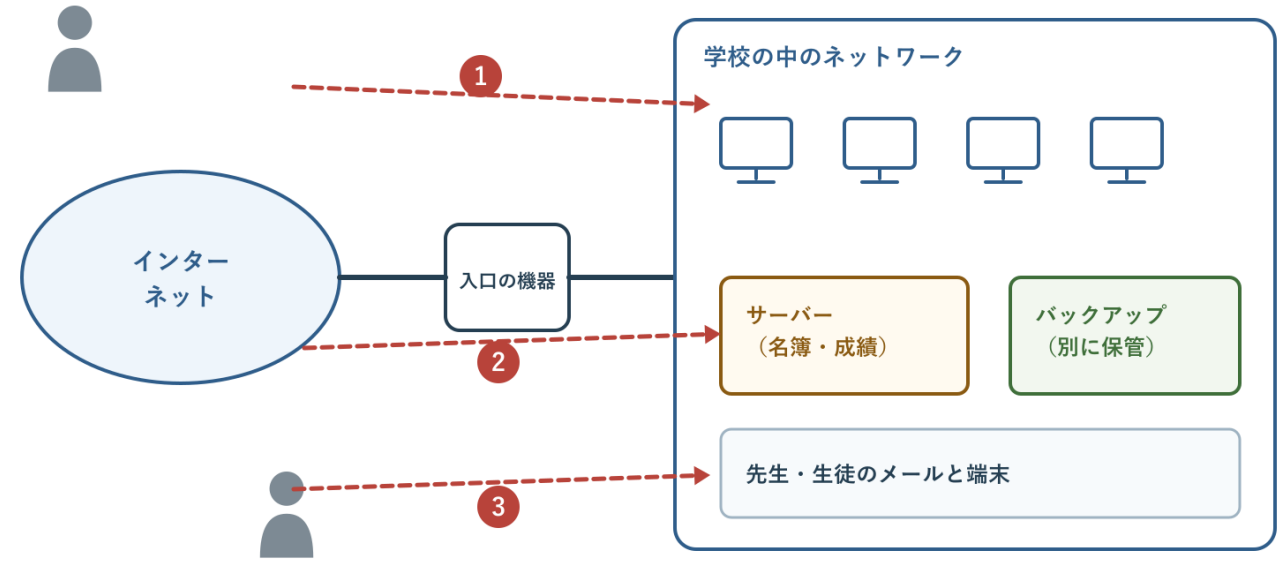
サイバー攻撃のしくみと守り方（AIの悪用を含む）

学校のネットワークは、どのような入口から攻撃され、どう守ればよいのだろう

架空の学校のネットワークと、攻撃の入口



1 不正アクセス

パスワードを当てたり盗んだりして入りこむ

守り方 長く当てにくいパスワード・多要素認証・ログインの記録を見る

2 マルウェア（ウイルスなど）

添付ファイルやにせのサイトから入る。データを暗号化して身代金を求めるものもある

守り方 ソフトを最新にする・ウイルス対策・バックアップ

3 にせのメール（フィッシング）

AIで、本物らしい文章を大量につくることもある

守り方 送り主を確かめる・リンクを開かない・すぐ相談する

守りの考え方

技術の対策（更新・暗号化・バックアップ・権限を分ける）と、人の行動（ルールを守る・あやしいと思ったら報告）の両方が必要。

AIで、本物らしいにせのメールや声、攻撃のプログラムがつくられる例もある。見た目だけで判断しない。

被害にあったら：すぐに報告する。ネットワークから切りはなす。かくさない。

※ 模式図。学校とネットワークの構成は架空。攻撃の手口は代表的なものに限った。