ゼロデイ攻撃 と Nデイ攻撃

ゼロデイ攻撃（Zero-Day Attack）
ソフトウェアやシステムの**脆弱性が発見**もしくは**発見される前**
その修正プログラム（パッチ）が公開前に、その**脆弱性を悪用して行われるサイバー攻撃**

攻撃者側は、高度な知識と技術を要するが、攻撃の成功率と効果（被害者側の被害）が大きい
被害者側は、脆弱性が公に知られる前に攻撃を受けるために、**対策を講じる時間がなく**
非常に高いリスクを伴うことになります。

Nデイ脆弱性
脆弱性が発見された何らかのシステムに対して、**提供された修正プログラムのリリース**と、
その**修正プログラムが適用されるまでの時間に存在する脆弱性**に行われるサイバー攻撃
（皆さん、**パッチ適用の遅れるとリスク**になります）

攻撃者側は、脆弱性が公開されてからになるので、**ゼロデイ攻撃ほど高度な知識と技術は要しない**
被害者側は、システムやソフトウエアのバージョン管理やパッチ適用管理体制が出来ていないと
対策を自ら放棄することににになり、**高いリスクを背負う**事になります。**（タイムリーな適用は難しい）**

この様に**自社の努力だけでは防衛できないサイバー攻撃**に対して
1．最低限、**バックアップは小まめに取って置く**事
2．攻撃リスク回避として、**サイバーセキュリティ保険**もある