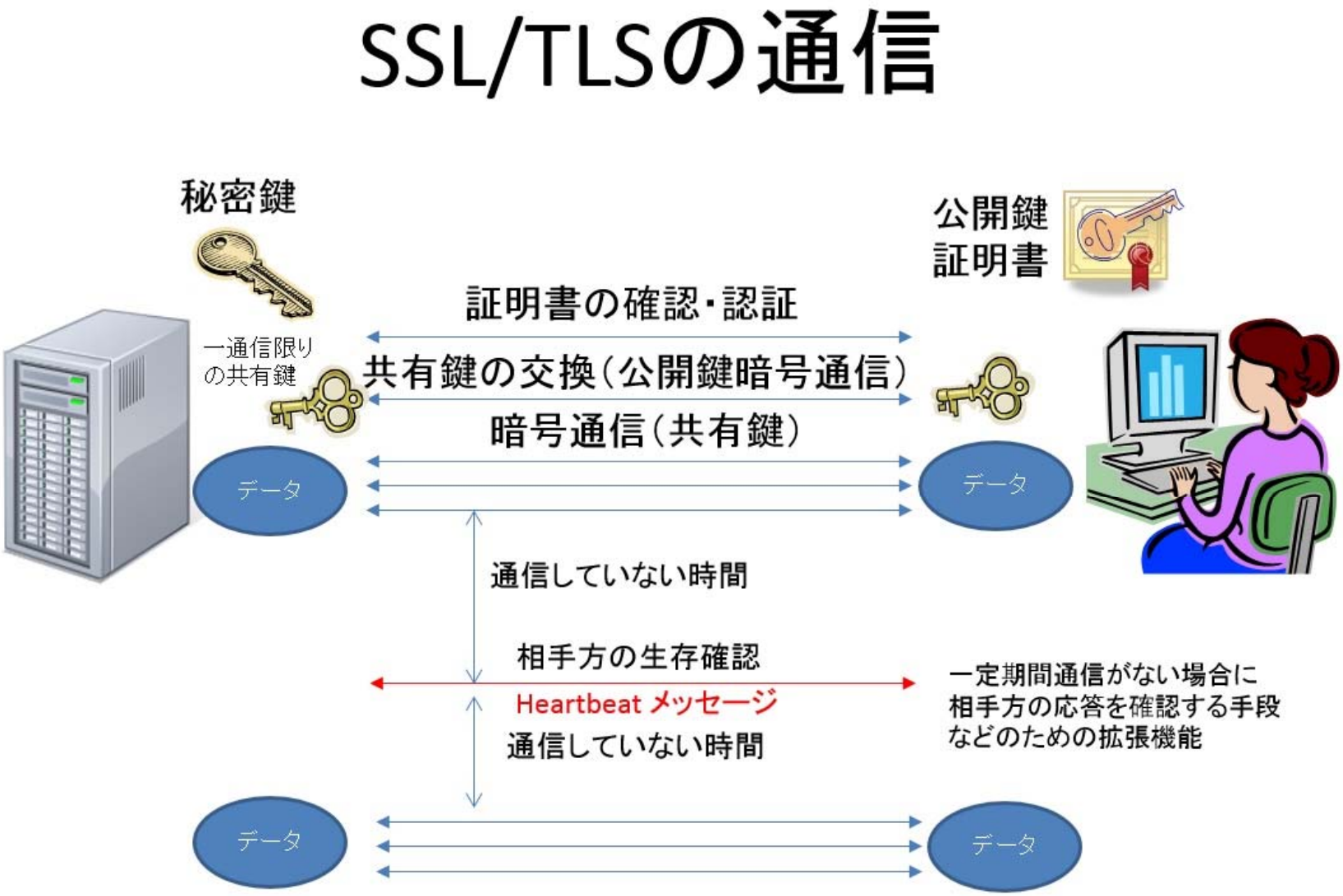
昨今のセキュリティ問題を考える

HeartBleed～Strutsまで、いくつかの問題提起

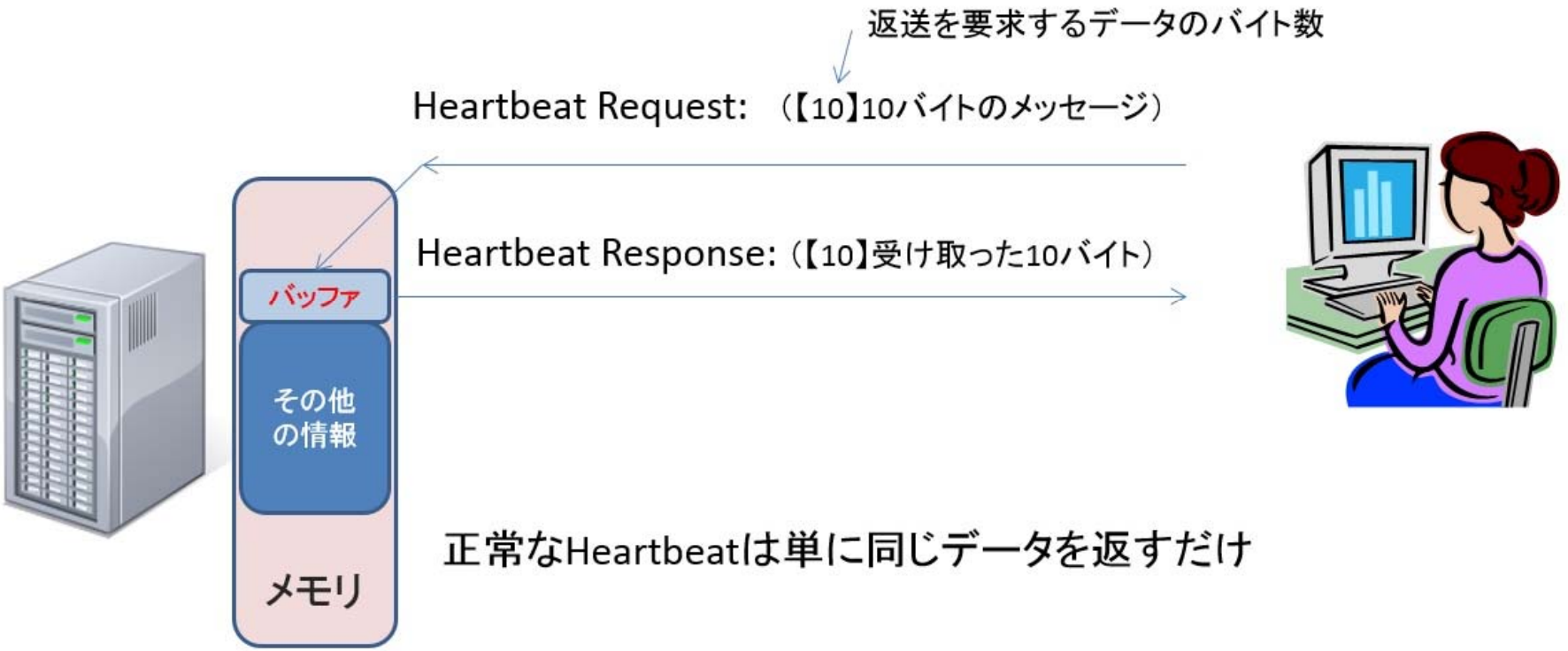
JNSA社会活動部会

HeartBleed脆弱性

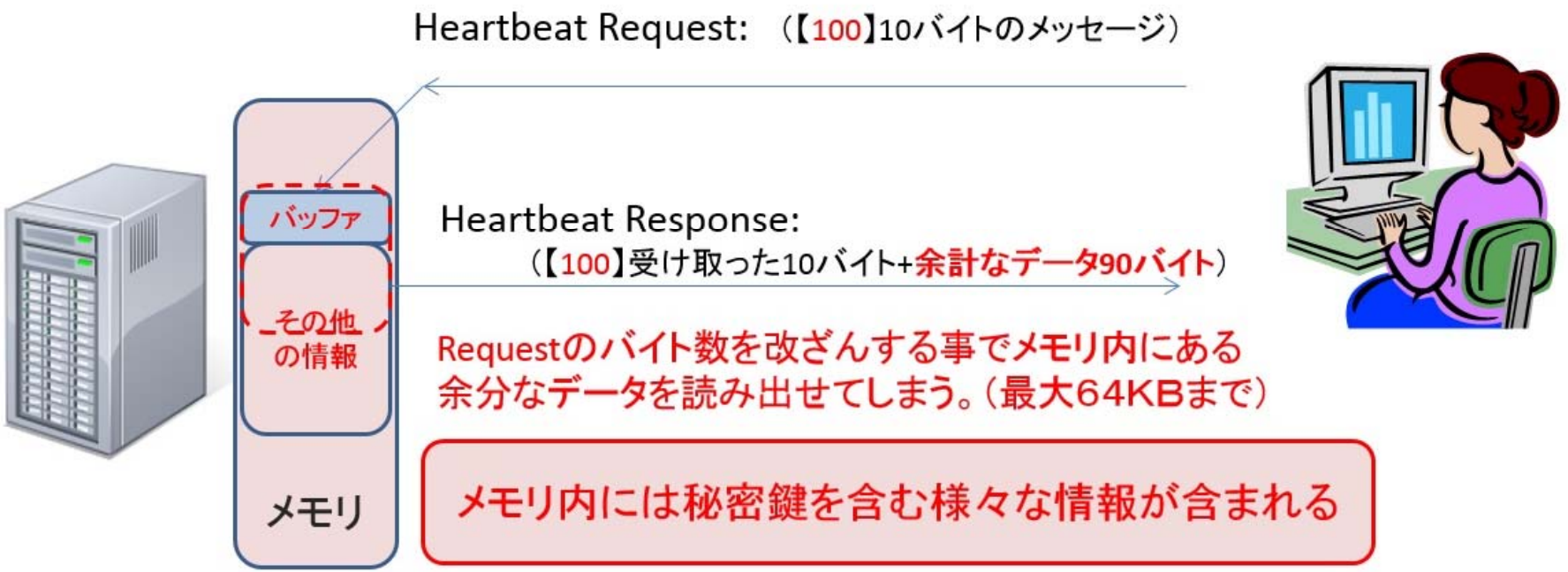


HeartBleed脆弱性

Heartbeatの通信



Heartbleed脆弱性



色々騒がれましたが・・・

秘密鍵が盗まれます・・・・

何百回、何千回繰り返せば、可能性はある・・・

たまたま、そこに秘密鍵があった場合で、それに気づくことができれば・・・・

通信を盗聴されます

理論的には秘密鍵を使った通信解読は可能。でも、Man in The Middleが前提なので、その仕掛けがまず必要

パスワードが盗まれます

これは疑問。そもそも、ヒープメモリに他人のパスワードが展開されるのだろうか・・・（通常のヒープはプロセスごとのメモリ領域なのでは？） 一方、通信が盗聴された場合は可能性がある

個人情報が盗まれます（ました？）

これも盗聴の場合。しかし、盗まれた事実はサーバ側では決してわからない（ログなんか残らない）。また相当の期間、公共の場所でMiTMをやらないと、大量の情報は収集できない。（攻撃者にとっては、SQLインジェクションでも仕掛けた方が、ぜんぜん効率がいい！？）

サーバ証明書を悪用されます

サーバの公開鍵は利用できるが、証明書はCAの鍵がないと改竄は不可能。唯一の方法は、同一のサーバ名を持つサーバで使用すること。

結構、「都市伝説」化していたかもしれない・・・・

そもそも、どうしてここまでの「大騒ぎ」になったのだろうか・・・・

DNSキャッシュ汚染（Poisoning）

DNSキャッシュサーバに対して、特定の名前に不正なIPアドレスを強制的に記憶させる攻撃

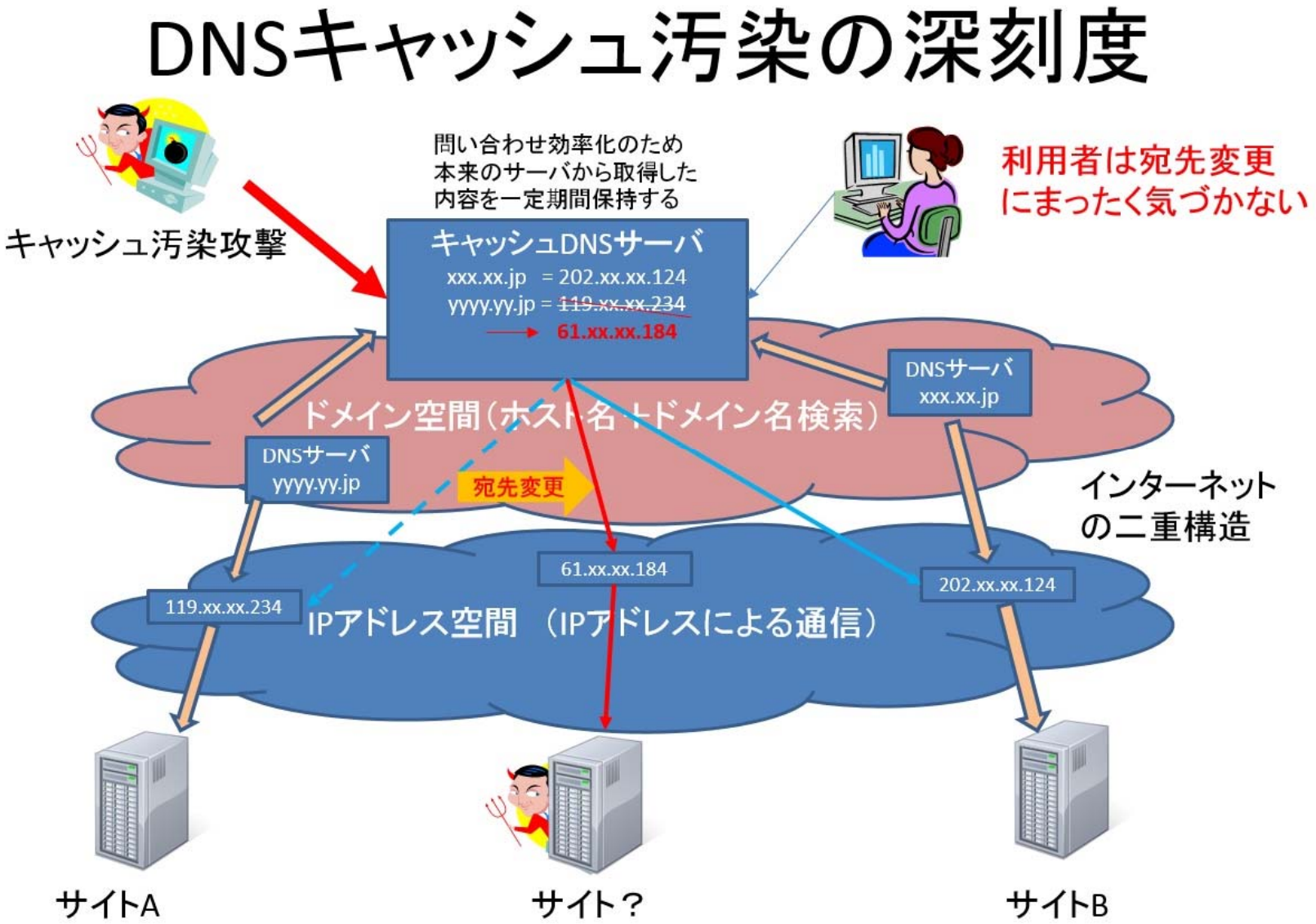
そのDNSサーバを使っているユーザは、特定のサイトにアクセスしようとした時に、不正サイトに接続してしまう。

大きな組織のDNSサーバが狙われると非常に危険

標的型攻撃に使われる可能性も

フィッシングサイトにアクセスさせられたことに気づけない

DNSキャッシュ汚染（Poisoning）



DNSキャッシュ汚染の対策

根本的対策

DNS情報の信頼性（真正性）を担保すること
（たとえば、DNSSecの利用とか・・・・）

結構、ハードルが高い・・・・・

緩和策　（かなり有効）

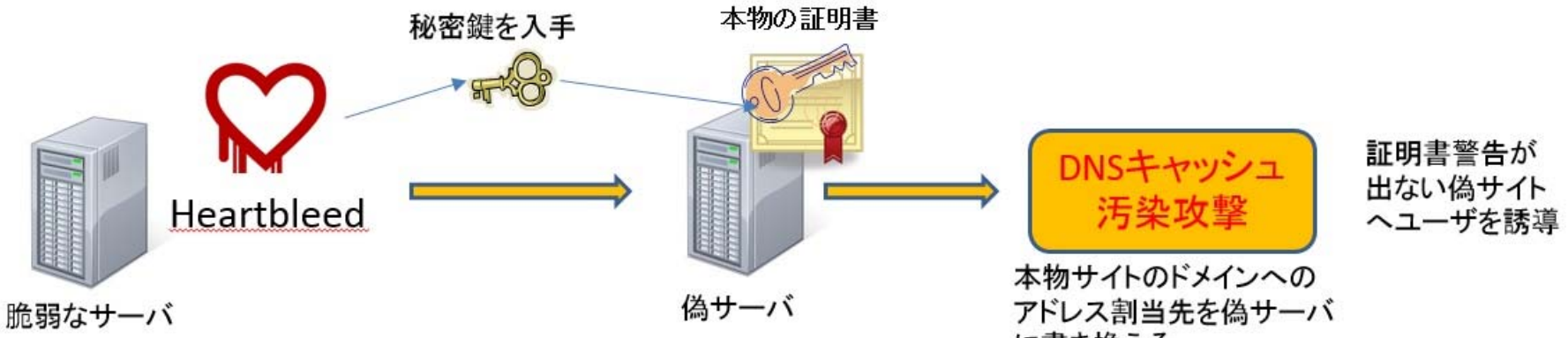
ソースポートやIDのランダム化（推測困難化）など

サーバソフトウエアの最新化で対応できるが・・・
未対応のサーバも多い。
機器組み込みのDNSキャッシュは？・・・

いまひとつ危機感が薄い・・・・・でも、インターネットにとっては*死活問題*かも

もっと怖い「合わせ技」

【完璧なフィッシング】



【標的型攻撃】

配布サーバが狙われる

GOM Player によるマルウエア感染

更新プログラムの配布サーバが攻撃を受け、更新プログラムにマルウエアが混入された。

（株）バッファローダウンロードサイトへのマルウエア混入

サイト上に掲載された機器ファームウエア更新プログラム（PC用の実行プログラム）等が改竄され、マルウエアが混入された

こうした、多くの利用者がアクセスするサービス、さらには利用者が操作しなくても自動的にソフトウエアが配布されるようなサービスを乗っ取られた場合、深刻な被害につながりかねない。（IoT、スマート家電なども標的にされるかも・・・）

サポート切れ問題

Windows Xp そして、Windows Server 2003

何年も前からアナウンスされてきた話なのに、なぜ今頃大騒ぎに？

Apache Struts 1

はたしてサポート切れは意識されていたのか？

オープンソースにおける脆弱性対応の課題は？

入れ替えが難しい「開発用フレームワーク」のライフサイクルをどう考えるべきなのだろう

脆弱性対応は間に合うのか？

密かに使われる「ゼロデイ」の増加？

発覚した時点で、攻撃が行われている。攻撃コードも流通している・・・・

攻撃対象の拡大

メジャーなOSとかソフトウエアから一般のアプリへ・・・

PCからスマホ、家電、IoTへ

体制が整っていないベンダ、ボランタリーなコーディネーション・・・・→　手が回らない？

まだまだ低い利用者の意識、さらなる利用者層の拡大

そろそろ利用者の努力に頼るのは無理なのでは？