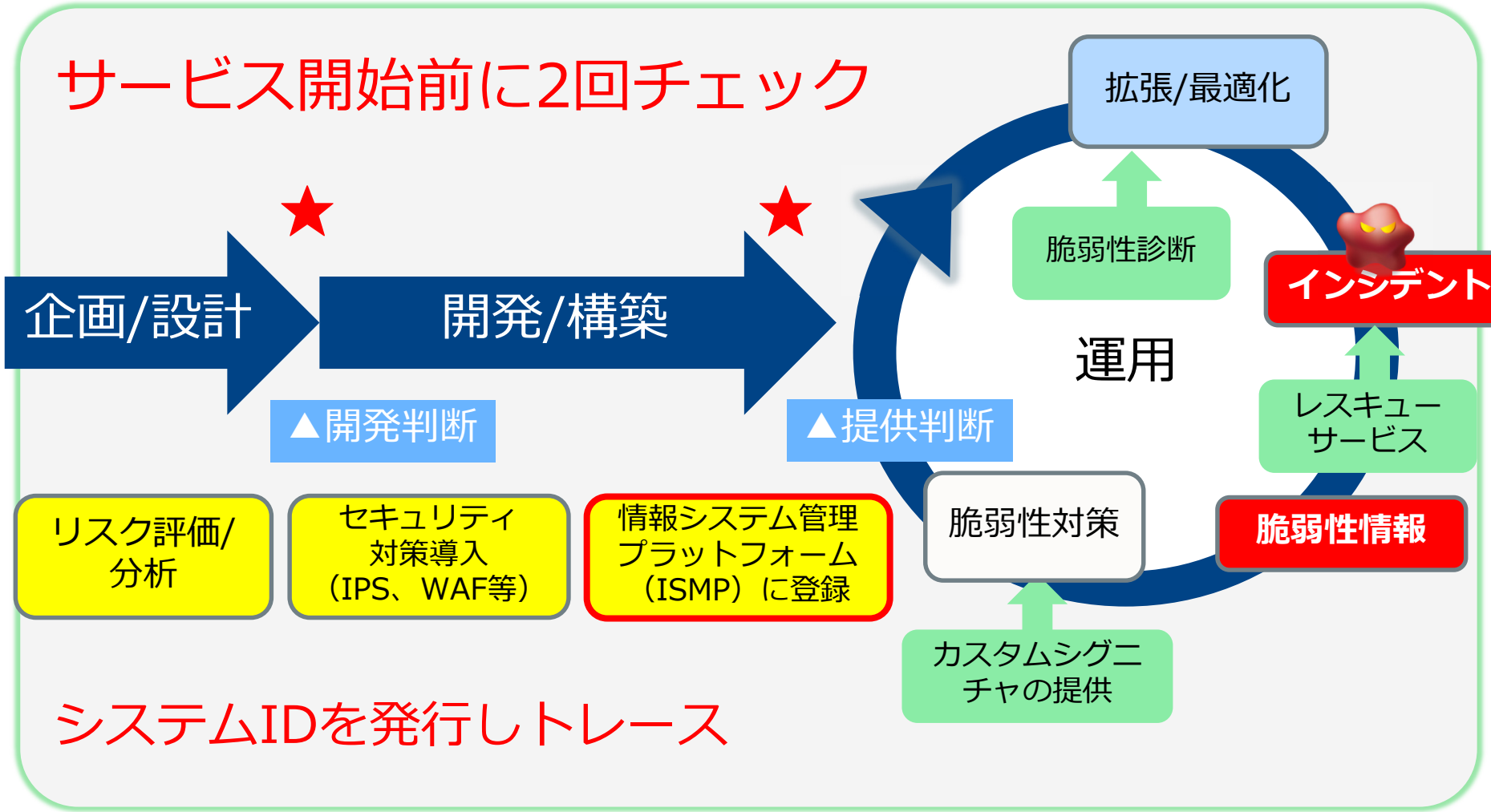
NTT Communications
Transform. Transcend.

Webサイトの脆弱性対策
～サービスを止めるという判断～

2017年11月28日
NTTコミュニケーションズ株式会社
情報セキュリティ部

Transform your business, transcend expectations with our technologically advanced solutions.

NTTコムのリスクマネジメントフレームワーク

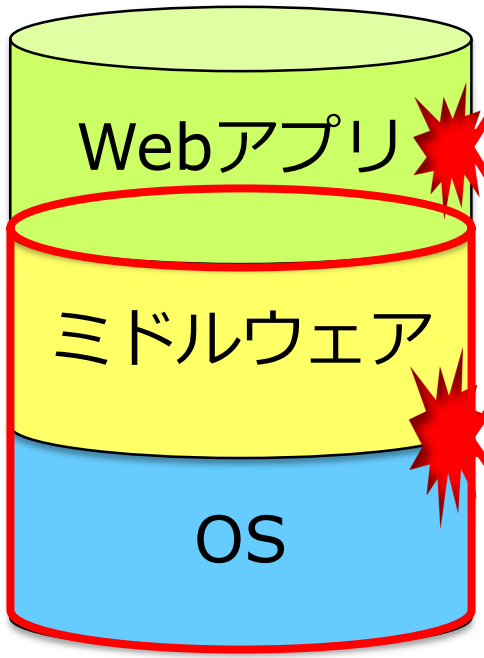


OS・ミドルウェア等とWebアプリの脆弱性

脆弱性対応には、製品ソフト等を利用したOS・ミドルウェア等と自社で開発したWebアプリケーションの両面の対応を実施

Webアプリの脆弱性
例）自社開発したソフト

OS・ミドルウェア等の脆弱性
例）Linux、Apache
Tomcat、OpneSSL



SQLインジェクション、ディレクトリトラバーサル等

ベンダ、コミュニティから脆弱性公表に伴い攻撃 等

脆弱性を突かれた過去の大事件

ソフトウェアの脆弱性を突かれた過去の大事件

２０１３年７月、OCN IDサービスのフロントサーバで利用するソフトウェアの脆弱性を突かれて、システムに不正侵入をされる。

１６日にソフトウェア提供元より脆弱性情報及び、パッチが発表され、
１７日より不正アクセスが開始される。

１８日にバックドアが設置され、１９日の早朝に情報が搾取される。

２３日の定期作業中に、不審なプロセスに気づき、続いて不審なファイルが発見される。

そして、事件発覚・・・

当時のニュースリリース

NTT Communications
Transform. Transcend.

News Release

NTT Communications

2013 年 7 月 24 日

OCN IDのサーバーへの不正アクセスについて

NTT コミュニケーションズ(略称：NTT Com)が提供する、メールアドレスを利用して各種 Web サービスにログインできる OCN IDのサーバーにおいて、外部からの不正アクセスが発生していたことが判明しました。現時点では、お客さまの情報などの流出被害は確認されておりませんが、OCN ID 用のメールアドレスと暗号化されたパスワードが外部へ流出した可能性があります。

このような事態が発生し、お客さまに多大なご迷惑をおかけすることになりましたことを、深くお詫び申し上げます。

NTT Com では、今回の事象の発生を厳粛に受け止め再発防止に努めますので、何卒ご理解を賜りますようお願い申し上げます。

1.発生事象

メールアドレスを利用して、OCN メール・OCN マイページ・マイポケットなどにログインできる OCN ID サービスを管理するサーバーにおいて、2013 年 7 月 23 日に 5 つの不審なプログラムファイルを発見しました。当該ファイルや通信ログなどを調査した結果、OCN ID のサーバーが外部から

不正アクセスの概要

公演の画面スライドにてご説明いたします

不正アクセスで行った対策

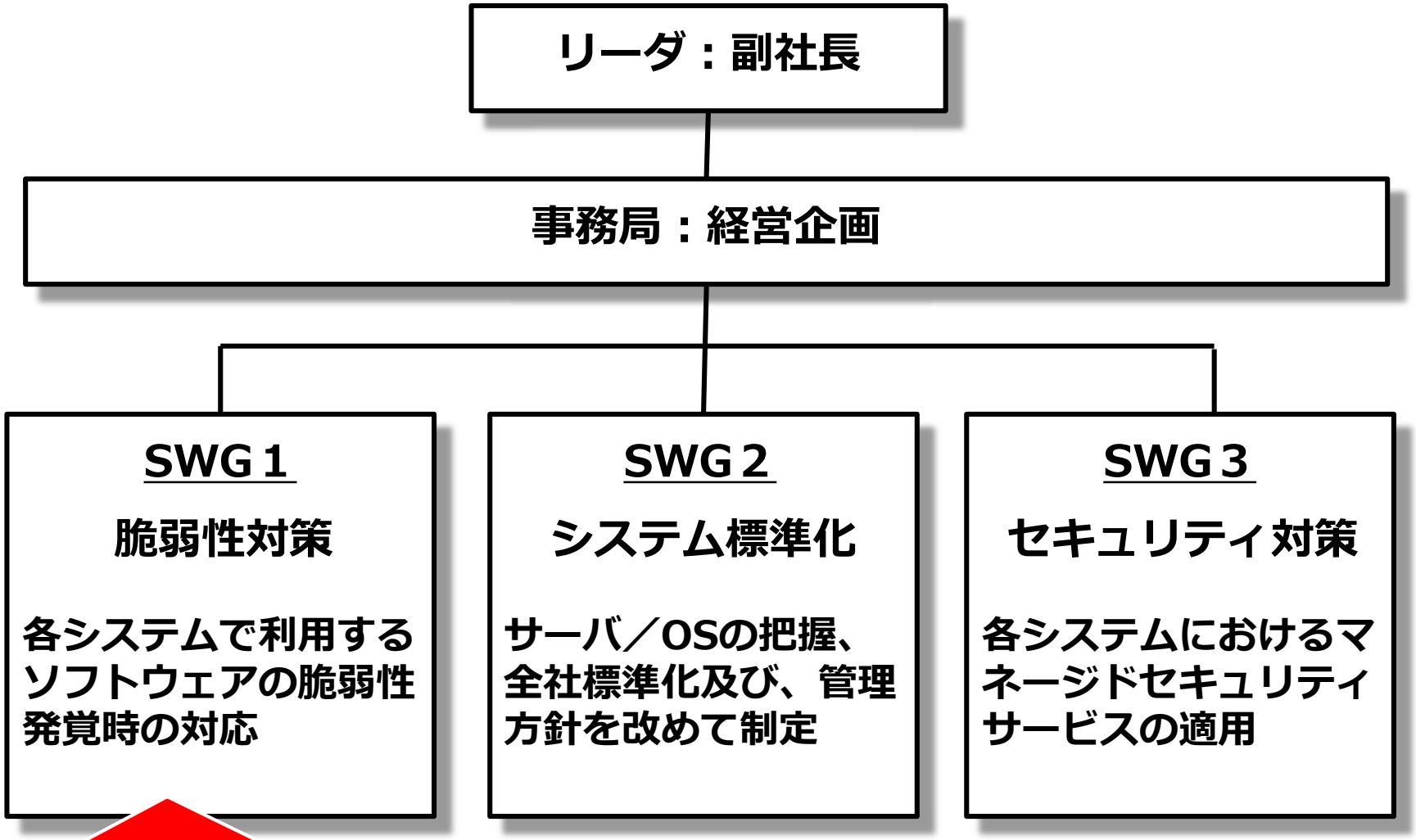
公演の画面スライドにてご説明いたします

OS・ミドルウェアソフト等の脆弱性対策強化

セキュリティリスクマネジメントの見直し

- セキュリティリスクマネジメントの欠如が露呈
- **全社ITシステム**等を徹底調査し、**セキュリティリスク低減策**を講じるとともに、
- お客様に提供する全サービス・全システムにおける統一したルールや体制を整備
- ITシステムの全社管理と**セキュリティリスクマネジメントの新たな業務運営プロセス**を確立

セキュリティ対策強化のための全社WG発足



7項目の見直しを実施

★全社ITシステムのセキュリティリスク低減策

1. 全社ITシステム等の調査
2. ITシステムのソフトウェア脆弱性解消の対応策
3. セキュリティ強化策

★セキュリティリスクマネジメントの新たな業務運営プロセス

4. 全社ITシステムの管理方針を改めて策定
5. ソフトウェア脆弱性発覚時の対応
6. ソフトウェア脆弱性発覚時の対応訓練
7. 規程/約款の改定

情報システム管理プラットフォーム（ISMP）

従来のシステム管理台帳を廃止し、情報システム管理プラットフォーム（ISMP）に一本化。より簡易に抜け漏れなく、ガバナンス強化を実現

フェーズ1	フェーズ2	フェーズ3
システム情報の登録・管理	脆弱性検知・収集管理	対策ステイタス・リスク管理

■システム情報管理
- –システム責任者、担当者管理
- –ソフトウェア（SW）構成管理

■脆弱性情報提供
- –SW構成に基づく脆弱性情報配信
- –脆弱性情報の対策履歴管理

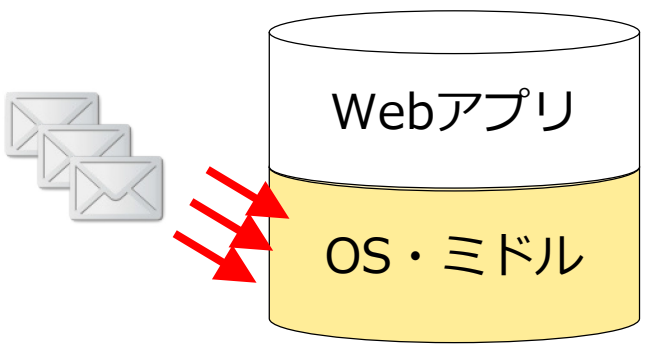
■脆弱性診断／検出
- –診断実施
- –診断結果の対策履歴管理

＜トップ画面＞

OS・ミドルウェア等の脆弱性対策

OS・ミドル脆弱性情報収集

配信される脆弱性情報を確認

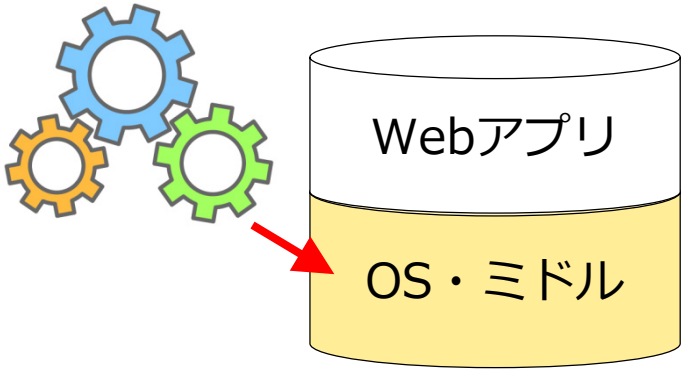


<日々実施>

OS・ミドル等の脆弱性情報収集・検知

OS・ミドル脆弱性診断

ツールを利用した診断

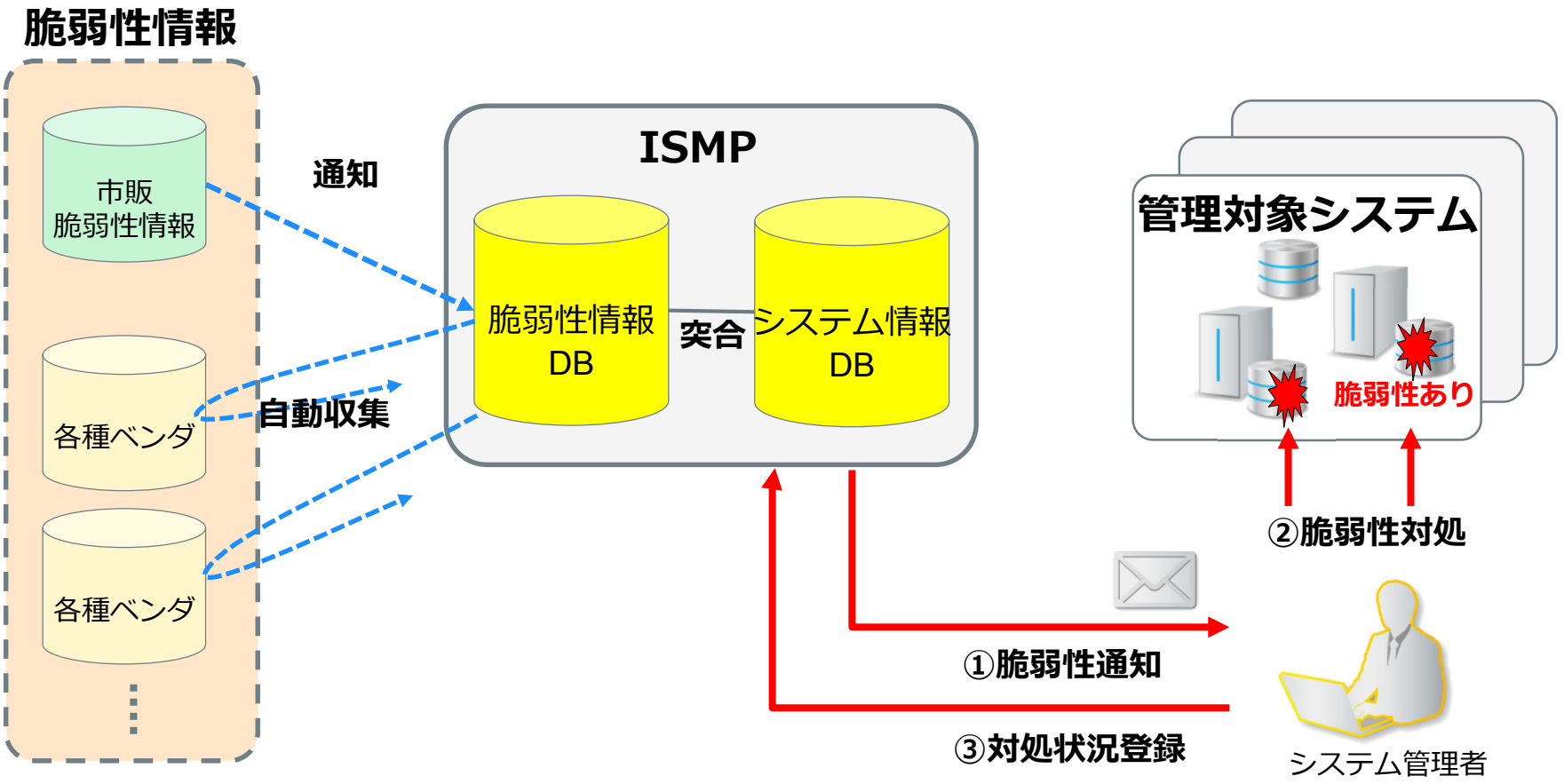


<毎年実施>

OS・ミドル等に診断

脆弱性検知・収集管理（OS・ミドルウェア等）

脆弱性情報をISMPで一元的に収集、事前に登録した管理対象のシステム情報と突合（脆弱性検知）を行い、システム管理者に脆弱性通知を実施。
システム管理者は脆弱性を対処し、ISMPに対処状況を登録（収集管理）。



OS・ミドルウェア等の脆弱性発覚時の対応

公演の画面スライドにてご説明いたします

脆弱性のランク判定基準（リスクレベル５）

公演の画面スライドにてご説明いたします

ISMPから送信されるメール

公演の画面スライドにてご説明いたします

脆弱性対策強化のための運用

■ ISMPへシステム登録漏れの防止

⇒ ISMPにシステム登録をしないと物品調達が出来ない仕組み

■ サポート体制の強化

⇒ 脆弱性に対するサポート窓口を設置

■ 迅速なサービス停止の判断、実施

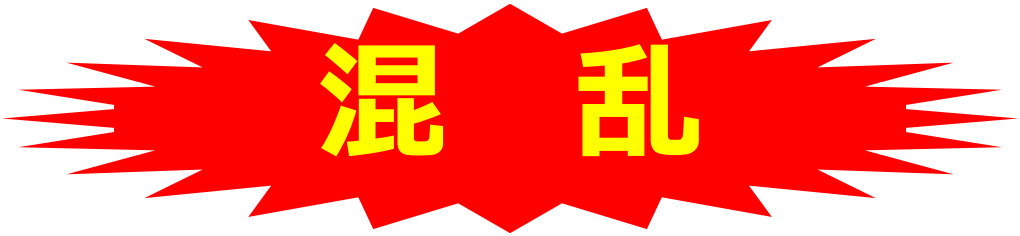
⇒ サービス責任者の判断でサービス停止を許可
⇒ 約款上に脆弱性によりサービス停止する可能性を記載
⇒ サービス停止手順、お客様対応手順を事前に準備
⇒ １時間以内停止判断、３時間以内サービス停止をルール化

■ 脆弱性対応の見える化

⇒ 社長の出席する会議で脆弱性対応状況を報告

運用が始まった当時は、、、

- 対応ルールが守られずに脆弱性が放置される
- 責任者がサービス停止を判断出来ない
- 本当に危険なのかとサポート窓口が責められる



脆弱性対策が浸透した理由

- 副社長から各組織長（幹部）への大号令
  ⇒お客様情報を守るためにはサービス停止も辞さない
- 危険な脆弱性発覚時、担当者からの地道な連絡
  ⇒嫌われても、怒られても、無視されても重要性を説く
- 結果的に過剰対応でも、サービス停止を責めない
  ⇒ルールに基づく対応は評価する
- 脆弱性対応状況について定期的に幹部全員へ報告
  ⇒幹部は上手く利用する

トップクラスの関与
地道にルールを徹底

脆弱性対策強化を行ってから4年．．．

2017年3月

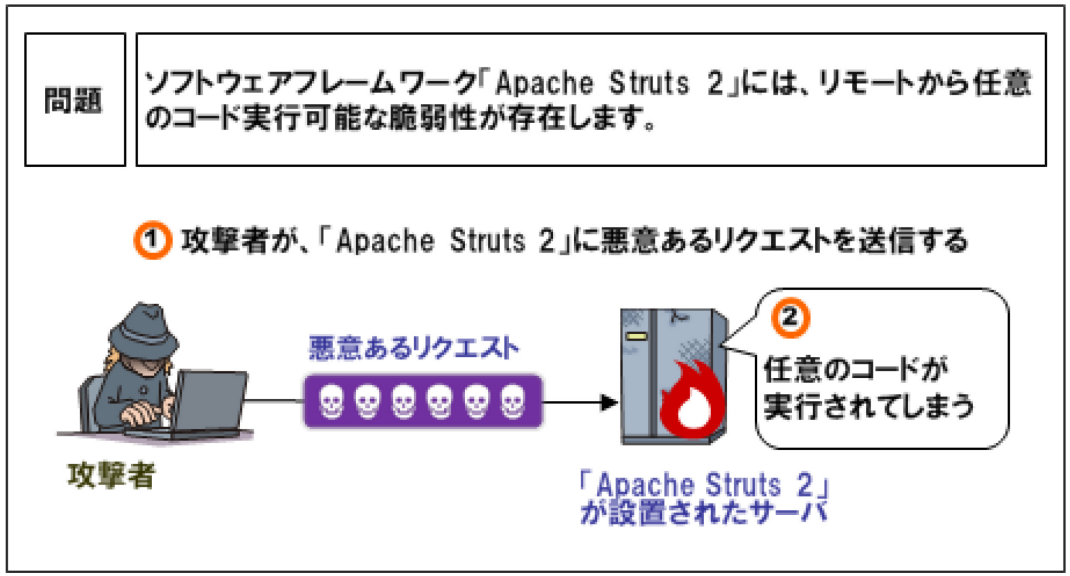
Webサーバの脆弱性を悪用された主な事例

発生	事例等	原因（想定）
2014年3月	リモートから任意コマンド実行	Apache Struts脆弱性
2014年4月	SSL秘密鍵、暗号通信漏えい	OpenSSL脆弱性（Heartbleed）
2014年9月	リモートから任意コマンド実行	Bash脆弱性（ShellShock）
2015年7月	細工されたリスクエスによりサービス停止	BIND脆弱性
2015年10月	リモートから管理者権限奪取等	Joomla!脆弱性
2015年12月	リモートから任意コマンド実行	Joomla!脆弱性
2016年4月	リモートから任意コマンド実行	ケータイキット脆弱性
2016年4月	リモートから任意コマンド実行	Apache Struts脆弱性
2016年10月	細工されたリスクエスによりサービス停止	BIND脆弱性
2017年2月	リモートからサイト改ざん	WordPress脆弱性
2017年3月	リモートから任意コマンド実行	Apache Struts脆弱性
2017年5月	リモートから任意コマンド実行	Windows SMB脆弱性

Apache Struts脆弱性(CVE-2017-5638)概要

■Apache Struts 2 のファイルアップロードの処理に任意のコードを実行される問題
■脆弱性概要と影響
リモートから細工したHTTPリクエストを送信することで、任意のコードが実行可能（不正プログラムの埋め込み・情報漏えい等）
■影響を受けるバージョン
Apache Struts 2.3.5 ～ 2.3.31　／　2.5 ～ 2.5.10
■対策方法
最新版（2.3.32, 2.5.10.1）にアップデート
暫定策：WAFやサーブレットフィルタにて不正リクエストを遮断

時間	事象
3/6 21時	脆弱性情報公開（ゼロディ）
3/7 12時	中国セキュリティベンダーサイトに注意喚起と攻撃コード掲載
3/8 3時	公式サイトにてパッチ公開
3/8 14時	IPAより脆弱性情報が公開



イラスト出典：Apache Struts2 の脆弱性対策について(CVE-2017-5638)(S2-045)(S2-046)（出典：IPA）

Apache Struts脆弱性(CVE-2017-5638)主な被害

公演の画面スライドにてご説明いたします

NTTコムにおける脆弱性対応の時系列

公演の画面スライドにてご説明いたします

脆弱性発覚時の標準プロセスと今回の対応状況

公演の画面スライドにてご説明いたします

何故、早期にサービス開始が出来たのか？

■ 復旧手順を事前に作成するためのルール化

⇒ サービス停止も考慮した事前の復旧手順を作成

■ 暫定対応のための仕組みの導入

⇒ ＷＡＦを導入すると共に、社内でカスタムシグニチャ作成・提供

■ 緊急パッチ適用時の検証項目の事前精査

⇒ 緊急でパッチを適用することを前提に必須検証項目を絞り込み実施

■ 四年間の実践経験

⇒ 危険性の高い脆弱性の発生するソフトウェアを利用するシステムはある程度限定されており、実践経験から得られた対応力

最後に、最近緊急度「高」として対応した事例

■**9月6日：Apache Struts脆弱性**
CVE-2017-9805（S2-052）
- RESTプラグイン使用環境におけるリモートコード実行の脆弱性
⇒ **RESTプラグインを使用していなかった**

■**9月7日：Apache Struts脆弱性**
CVE-2017-12611（S2-053）
- FreeMarker使用環境におけるリモートコード実行の脆弱性
⇒ **ユーザからの入力文字列をFreeMarkerタグ内で使用していなかった**

■**9月20日：Apache Tomcat脆弱性**
CVE-2017-12615
- HTTP PUTリクエスト受付環境におけるリモートコード実行の脆弱性
⇒ **readonlyパラメータをfalseにしていなかった**

結局、脆弱性の成立条件に合致しているケースがなく事なきを得る

「オオカミ少年」VS「万一のリスク回避」の鬩ぎ合い

脆弱性対策強化の取組みを振り返って

NTT Communications
Transform. Transcend.

- **幹部の巻き込み、幹部への定期報告は非常に有効**
  ⇒社内に緊張感、モチベーションが生まれる

- **対策を推進、実行する実働部隊が重要**
  ⇒ルールを整理するだけでは駄目、実務者が必要である

- **社内システムの数により取組みレベルを判断**
  ⇒本日紹介した取組みはシステム数が多い時には有効だが
  ルール、基準を決めすぎると現場が思考停止になる

- **ルールを厳しくするだけでは実効性を失う**
  ⇒重要情報の有無等を考慮し、許容ルールの検討も必要で
  ある

ご清聴ありがとうございました