NCWG会合 2015/9

ビルトイン・セキュリティ

アプリケーション・セキュリティを実現するベストプラクティスとは

OWASP Japan Lead
株式会社アスタリスク・リサーチ
岡田 良太郎

riotaro.okada@owasp.org

About 岡田良太郎

1. 情報セキュリティ・ベーシック/アドバンスドトレーニング（一般、技術関係職）
2. システム環境、設計のリスクアナリシス（調達、構築、運用管理、更新）
3. 開発・設計会社のためのビルドイン・セキュリティソリューション（開発会社）
4. データセキュリティ・サービス（例：PHR x EHR）

コミュニティ・コラボレーション：

- セキュリティ/災害対策/医療
- カレー大學 教授

Asterisk Research, Inc.

OWASP JAPAN

その他公共関連の貢献活動

- マレーシア政府セキュリティイニシアチブ教育インストラクタ（外務省）
- 政府調達担当向けサイバー演習評価委員（総務省）
- セキュリティキャンプ インストラクタ（経済産業省）
- 自治体IT調達調査（IPA）

Hardening Project 2015

オワスプナイト

Asterisk Research, Inc.

5th

“開発者によるセキュリティの実現”

「アスタリスク・リサーチがソフトウェアセキュリティにおけるソリューションを提供するパートナーとしてCigitalを選択してくれたことをうれしく思います。優れたソフトウェアセキュリティを実現する市場を開発することは実社会においてまさに望まれていることであり、私たち両社がともに長い期間目指してきたものです」

Cigital

Chief Technology Officer
Gary McGraw（ゲイリー・マグロー）

「この提携により、当社がこれまでお客様に提供してきたコンサルティングならびにトレーニングのサービス・ラインアップに、Cigital社のソリューションを加わることとなり、さらにより多くの開発チームに貢献できるようになります。これにより、当社のセキュリティ事業分野のミッションである“enabling security for developers”を実現し、ひいては安全かつ安定的に持続可能なインターネット社会の実現に貢献できればと考えています」

Asterisk Research, Inc.

代表取締役
岡田 良太郎

Cyber Attacks and damage

- 5,080,000 attack to Japanese Government
- 9,312,543 personal data breached
- 2,020,657,500 US$ for legal reparations
- 1,602,400 US$ average legal reparations cost for each cracked orgs

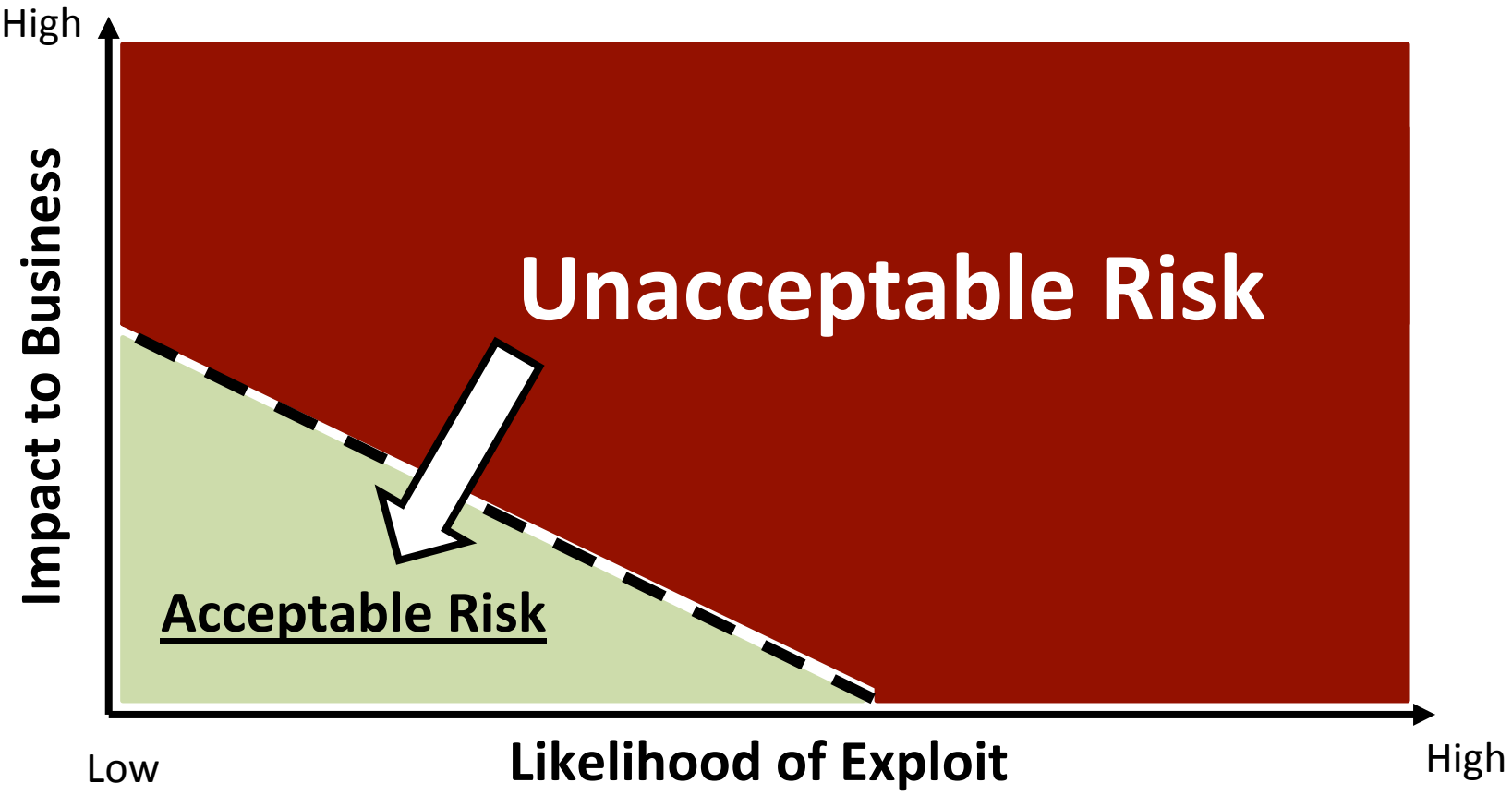
damaged industry <- attack

- ICT
- SNS
- Retail trade･Wholesale
- Government and public service
- Financial industry
- Insurance industry
- Education industry

- Intrusion
- Denial of Service
- Software Vulnerability
- Listed credential attack
- APT: Advanced Persistent Threat
- Phishing
- Malware
- Ransom-ware

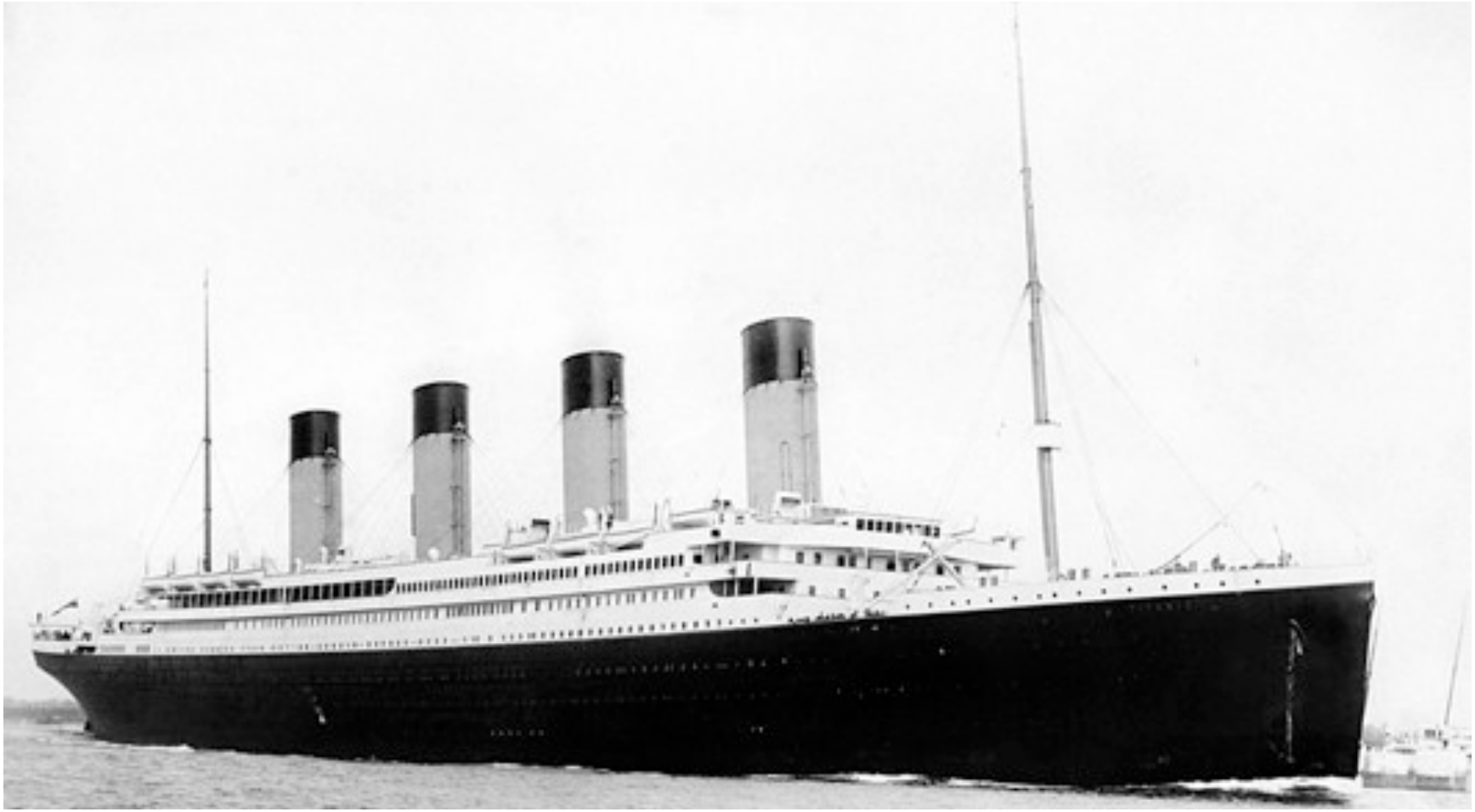
Security Goal: Reduce Risk

Reduce cyber security risk to an acceptable level



キーワード “Attack Surface”

最大の脆弱性は？



RMS Titanic departing Southampton on April 10, 1912. (Photo: Creative Commons)

“思い込み”脆弱性は最強

- 一般に「メリットは大きめ、
  リスクは小さめ」
  - 好みや欲求
  - 立場や役職に基づく利害
  - Peer pressure：モラルハザード
- プロでも
  - 注目しているリスクを大きめに見る傾向

Attack surfaceに関する“思い込み”例

- コンプライアンスこそが情報セキュリティ確保の第一歩だ
- 「内部向け」のシステムは攻撃領域としては影響は低い
- ネットワーク通信が暗号化されていれば、通信路の攻撃リスクは取るに足らない
- システムは、最終的にFirewall, WAFや、運用をがんばればアプリケーションはそれほど重要ではない
- 自分の知らない間に自分のIDや認証を悪用されることは、まず、ない

WHERE IS THE ATTACK SURFACE?

https://www.reddit.com/r/funny/comments/1m628n/the_new_iphone_5s_provides_unmatched_security/

“Internet of Things”

Consumer & Home

Smart Infrastructure

Security & Surveillance

Healthcare

Network

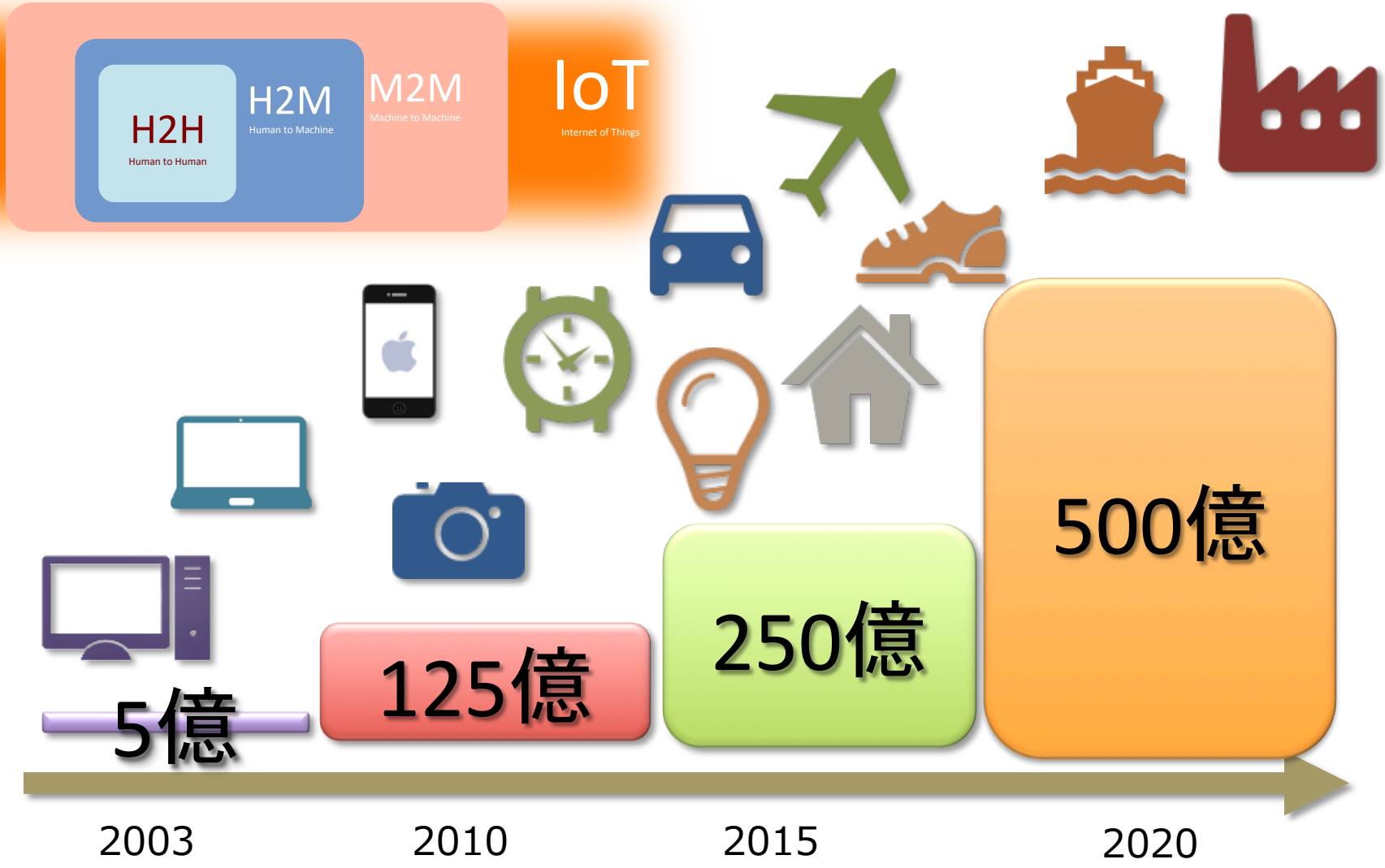
Transportation

Retail

Industrial

Others

「2020年には500億超のIoT“モノ”がつながる」attack surfaceはどうなる…？



2015/9/4
サイバーセキュリティ戦略 閣議決定

このため、2020 年までに、市場ニーズに応える安全な IoT システムを実現し、我が国の IoT システムの国際的評価を高めることを目指し、以下の取組を実施する。

(1) 安全な IoT システムを活用した新規事業の振興

IoT システムに係る新たな事業を成功させるためには、競争力の源泉となる高いレベルでのセキュリティ品質の実現が不可欠である。しかし、セキュリティを後付けで導入しても、IoT システムが本質的に安全になるものではない。むしろ単にコストの大幅な増加の要因となる。このため、連携される既存システムを含めて、IoT システム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。具体的には、IoT システムに係る事業について、セキュリティ・バイ・デザインの考え方に基づき所要のセキュリティ対策を業態横断的に推進し、メリハリをもって、積極的に新規事業の振興を図る

インタビュー&トーク

ITpro

「日本はオイシイ」からサイバー攻撃で狙われる

セキュリティ技術は既に、IT技術者にとって必ず身に付ける必要がある一般教養になりつつあると思う。ITシステムを作り、運用する一人一人の技術者がセキュリティを理解し、意識していないと、現在の脅威にはとても対応しきれない。

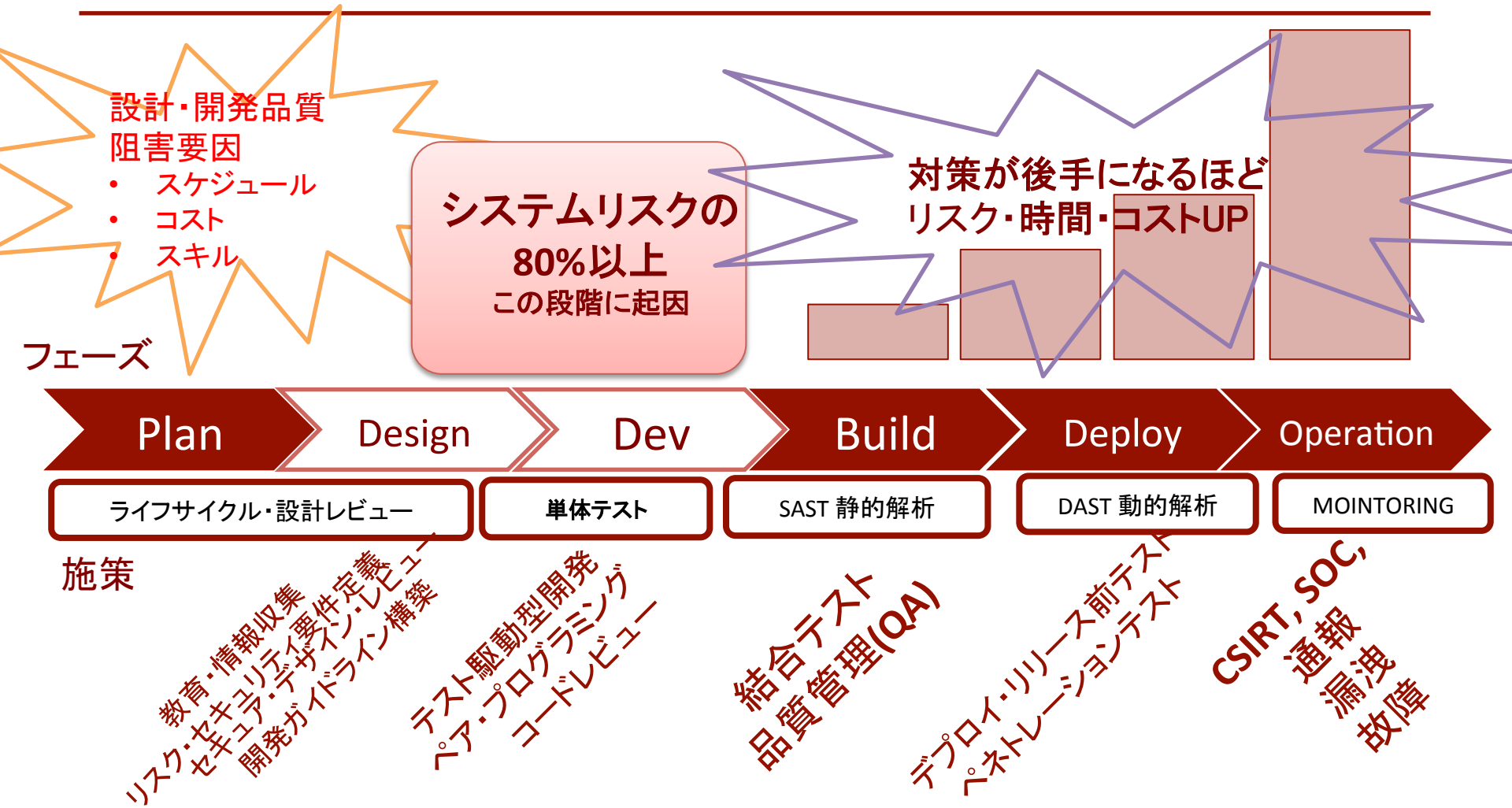
― 一般教養としてのセキュリティで今、いちばん情報が足りない分野はなんでしょうか？

設計・開発段階からセキュリティの機能を組み込む「セキュアプログラミング」だろう。ITの担い手であるプログラマーたちのセキュリティ意識が低すぎる。すべてのプログラマーがセキュアプログラミングを常識として知っているべきだと思うが、残念ながらセキュアプログラミングを学ぶための情報は限られている。

「日本はオイシイ」からサイバー攻撃で狙われる
奈良先端科学技術大学院大学 山口英教授

http://itpro.nikkeibp.co.jp/atcl/interview/14/262522/090700192/

“ビルドイン・セキュリティ”
設計・開発段階におけるセキュリティ。



開発成果物の価値が効率良く向上するサイクルのコツ
見つけるだけではなく、修正し、改善プロセスをみる

1. Find risky coding and vulnerabilities **earlier**

セキュリティ問題を潜在を早期発見

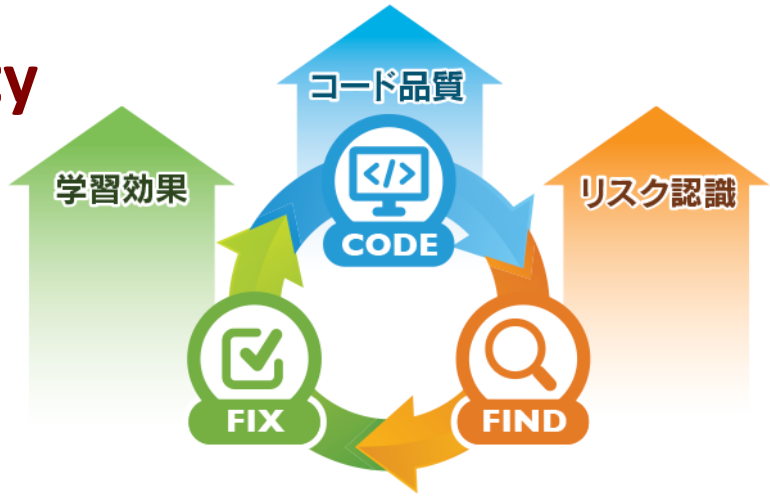
2. Fix & **Prevent** them

リスクのあるコーディングを修正・未然に防ぐ

3. Improved education and quality

throughout SDLC

開発ライフサイクルを通してソフトウェア品質向上



他業界のビルド・イン・セキュリティ例：

PCI DSS準拠条件

	PCI DSS 3.0要件(引用)
要件6 安全性の高いシステムとアプリケーションを開発し、保守する	要件6は、現在および変化し続ける脆弱性、および安全なコード化ガイドラインを反映させるため要件が追加・更新されています。開発環境、開発者トレーニングに関する要件が更新されています。また、コーディング実践に関する要件が追加されています。
要件 11: セキュリティシステムおよびプロセスを定期的にテストする。	要件11では、発展型要件、追加のガイダンス、明確化と多角的に要件が発展しています。特に、脆弱性テストには期間（四半期ごと）のみならず、訂正内容を検証するための繰り返しテストの要件についても明確化されました。
要件12 すべての担当者の情報セキュリティに対応するポリシーを維持する。	要件12では、2.0に引き続き、担当者教育の重要性が強調されています。入社時、また年ごとに行うよう規定されています。

OWASP Internet of Things Top 10

I1 安全でないウェブインターフェース
I2 欠陥のある認証・認可機構
I3 安全でないネットワークサービス
I4 通信路の暗号化の欠如
I5 プライバシー
I6 安全でないクラウドインターフェース
I7 弱いモバイルインターフェース
I8 設定の不備
I9 ソフトウェア・ファームウェアの問題
I10 物理的な問題

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

コードのテストケースは、脆弱性検査より詳細：
OWASP ASVS, OWASP Top 10, CWE Top 25, PCI DSS

Asterisk Research, Inc.

入力値バリデーションならびに出力値のエンコードを徹底

Cross-Site Scripting *
> Output Sent to Browser
> Output Data in Web Page
> DOM Object
> HTTP Header Manipulation
> GET Requests
> HTML Comments in JSP or PHP File
> Hidden Field
> Data Usage from HTTP Request
> Output Encoding Set to False

SQL Injection *
> Dangerous Method Calls
> Database Query Manipulation
> Untrusted Data Source for Query
> Dynamic Database Query

Path Manipulation *
> Unsanitized Data Usage
> Directory Call with Dynamic Inputs

Denial of Service Attack
> Hanging JRE
> Dynamic Web Page Content
> Processing Sensitive Data
> Race Condition
> Struts Config
> XML Attacks

File Input/Output
> Exposed Buffers
> Temporary Files in Shared Directories

Other Unvalidated User Input *
> LDAP Injection *
> Xpath Injection *
> Command Injection *
> Remote Code Execution
> Javax Persistence Security

* 2013 OWASP Top 10の関連項目

セキュアでないデータの取り扱いによる問題を回避

Insecure Data Storage
> Insecure File Modes
> No Access Control *
> User Credentials Stored *
> Hardcoded Password *
> Access to Cache
> HTTP Auth Credentials Stored *

Sensitive Information Leakage
> Dynamic Web Page Content
> System Information Leak
> Exposure of Authentication Objects
> Use of printStack Trace
> Exception Handling
> Autocomplete Setting
> External Storage Used
> Screen View Captured
> Web Page Saved to Device
> HTML Form Data
> Insecure Configuration in Manifest

Weak Cryptography *
> Security Features
> Weak Cryptographic Hash
> Weak Encryption
> Outdated Cipher
> Weak Algorithm
> Secure Number Randomization
> Insufficient Key Size
> Inadequate RSA Padding

Trust Boundary Violations
> User Supplied Data to Beans
> Calls Affecting CURL Requests
> Untrusted Data Source
> Unsanitized String
> Injection in Email
> Points of Interest
> Entry Point Violation
> Socket Connection Timeout
> Socket Stream Timeout

Unvalidated Redirects & Forwards
> URL Redirection *
> User Redirection *

正しいコーディング手法の導入・徹底

Thread APIs
> Call to Notify()
> Invocation of Thread.stop()
> Invocation of Thread.run()

Struts Misconfiguration
> XML Injection
> XML DTD Attack
> Missing/Duplicate Form Bean *
> Missing Forward Name Attribute *
> Missing Path/Type Attribute *
> Unnecessary Attribute
> Required Input Attribute
> Invalid Exception Scope
> Missing Form-Property Type
> Dangerous Relative Path
> Action Not Validated

Configuration
> ASP.NET Configuration *
> PHP Configuration *
> Environment Variable Value
> Session Timeout Configuration *
> Session Inactive Interval *
> Implementation Time Logic Flaws
> Call to ReadLine
> Race Condition
> Hidden Field

Improper Error Handling
> Unspecified Error Page
> JSP Defines Error Page
> JSONRPC Security

Log Handling
> Unsanitized Data Written to Logs
> Private User Data Logged

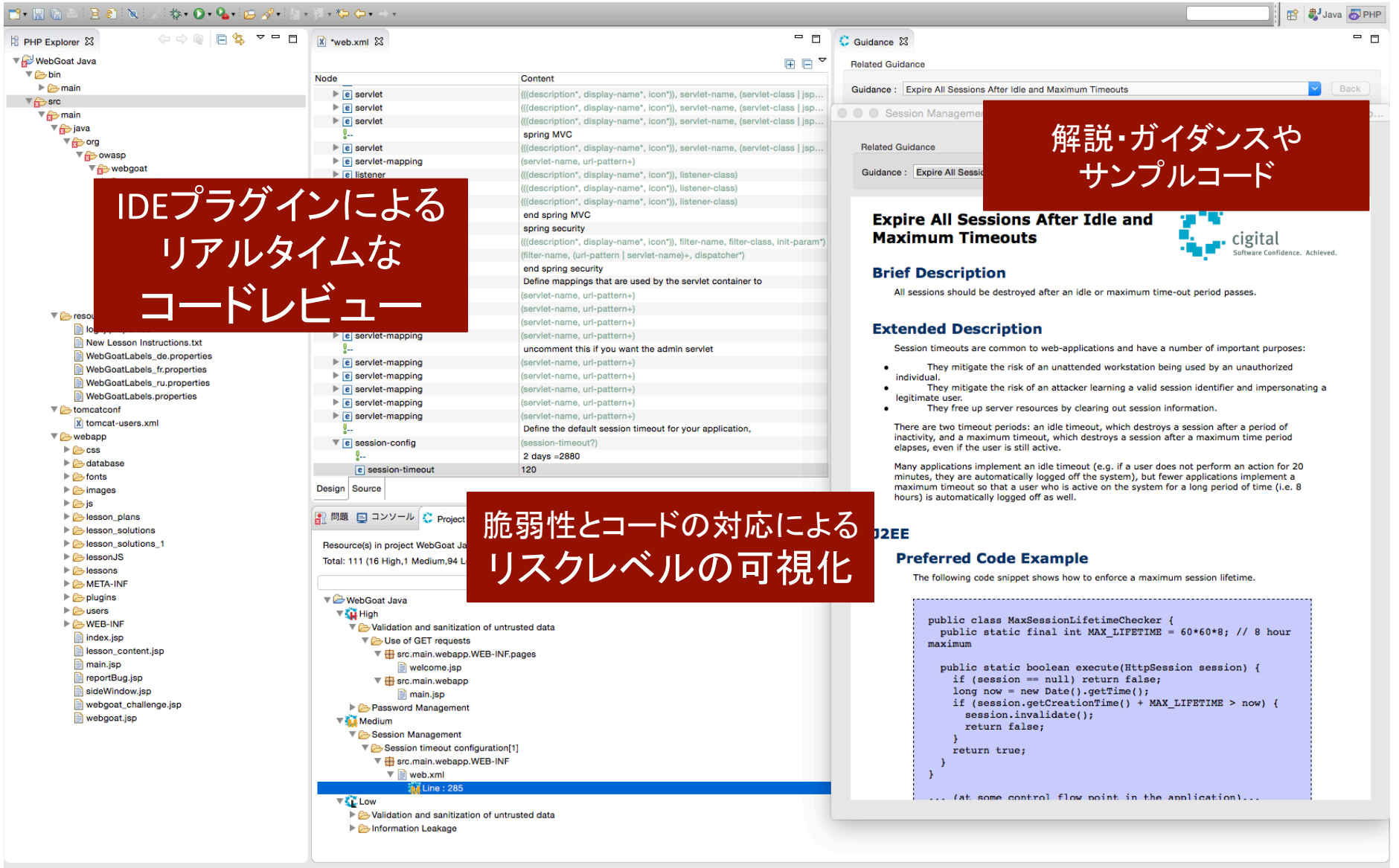
Cookie Security *
>Overly Broad Paths
> Insufficient Transport Layer Protection
> Session Management

Resource Handling
> File Input Output
> Hibernate Security
> Resource Not Closed in Finally Block

SecureAssist リアルタイムコードレビュー・リスク指摘・修正ガイダンス

Asterisk Research, Inc.

https://www.asteriskresearch.com/



まとめ

- 最大のリスクは「思い込み」。
  - リファレンス（ファクト・データ・メソドロジ）など事実に基づいて本質的に考えること。コラボレーション、コミュニケーションはこれを打破する鍵になる。
- システムは、人為的なものではないトラフィックに埋め尽くされていく。
  - アタックサーフィスは多様化し、後付け対応、事後対策的アプローチは破綻する。
- セキュリティ・バイ・デザイン、ビルトインセキュリティで対策するほうが有効で、低コスト。

IBM Security Services
Ahead of the Threat.®

IBM

2015年　上半期
Tokyo SOC
情報分析レポート

- ドライブ・バイ・ダウンロード型感染推移
- Flashプラグインのリスクと対処法
- 標的型攻撃のパターンと国内事情

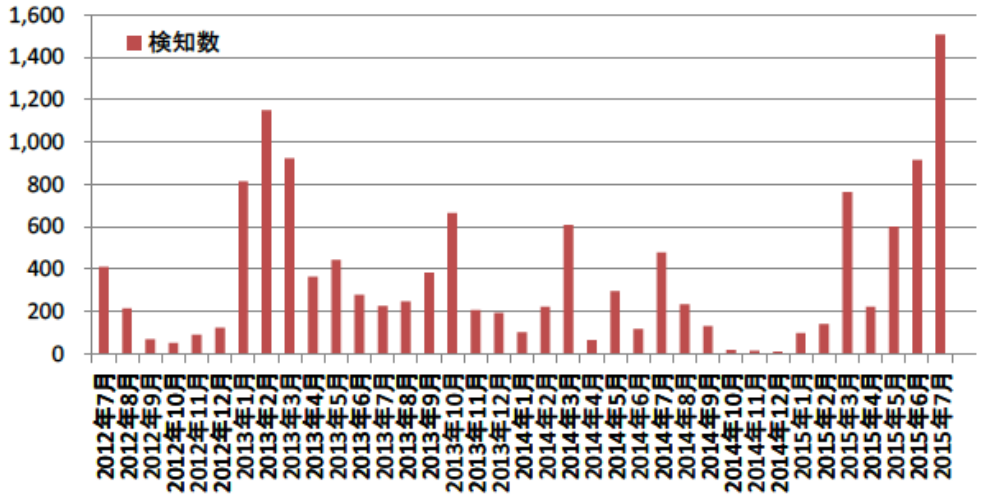
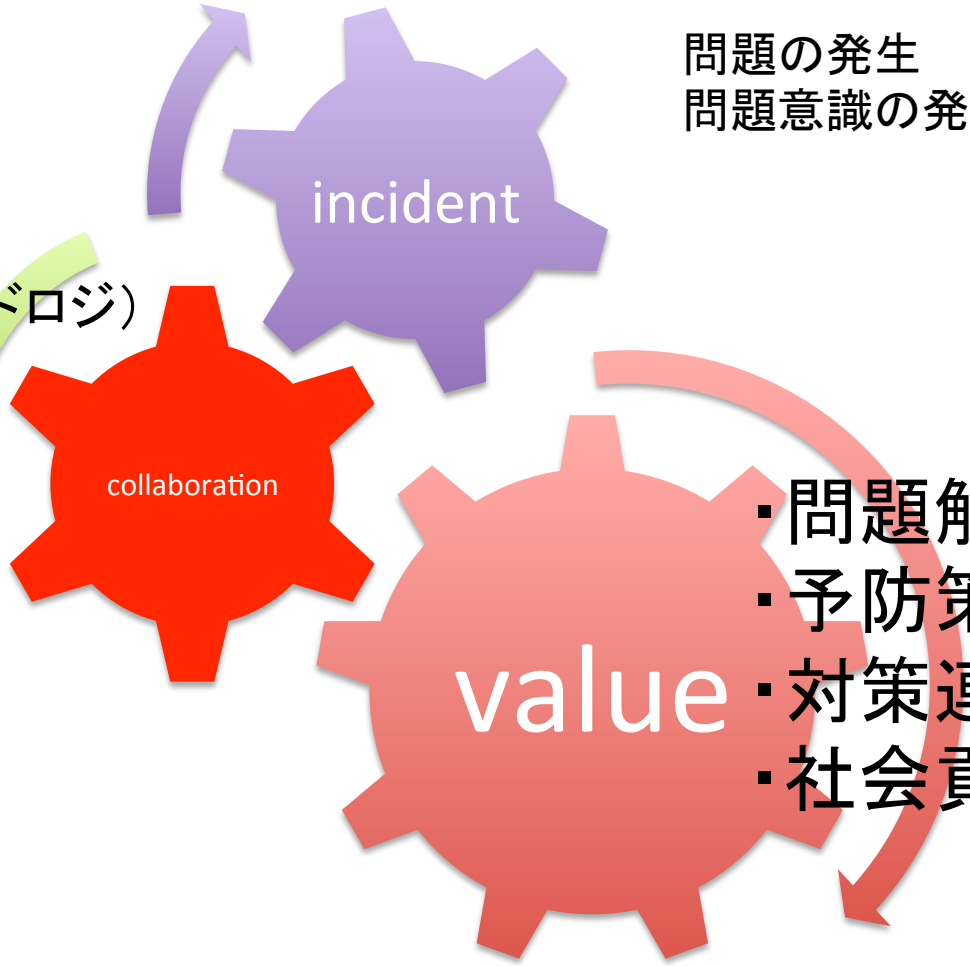


図 6.ドライブ・バイ・ダウンロード攻撃の月別検知数推移(日本国内)
(Tokyo SOC 調べ：2012 年 7 月 1 日～2015 年 7 月 31 日)

コミュニケーション・コラボレーションが効く。

1. リファレンス
   （データ・ファクト・メソドロジ）
2. コミュニケーション
3. コラボレーション



問題の発生
問題意識の発生

- 問題解決
- 予防策共有
- 対策連携強化
- 社会貢献

NCWGの皆さんからのご依頼は優先します。ぜひどうぞ。

タイミング	トピック	URL
10/1 14:30 – 16:30 ベルサール神保町 主催：SONY DNA & Asterisk Research	アプリケーションセキュリティスーパーブリーフィング（神保町） ～ 年末リリースに間に合う！ 最新情報と打ち手 ※ Android アプリの品質統計 OWASP カンファレンス報告 事例とツール紹介	http://twitter.com/okdt/status/641073158317998080 https://www.sonydna.com/sdna/topics/sec_seminar_20151001.html お急ぎください
10/1 18:30 EDITORY 神保町 ¥2000	Usable x Security Meetup 「めんどくさくないセキュリティ？あるのかまじでミートアップ」 ※ プレゼンが聞ける楽しい会	https://usablesecurity.doorkeeper.jp/events/31208 残席わずか
いつでも！ 無料！	ビルトインセキュリティのご相談 ・研修/教育コンテンツのご相談 ・自動化ツールのトライアル ・協力会社・開発会社の選定評価	https://www.asteriskresearch.com riotaro@rsrch.jp 岡田まで

Usable x Security Meetup

https://usablesecurity.doorkeeper.jp/events/31208

Application Security Super Briefing 2015 Fall

https://www.sonydna.com/sdna/topics/sec_seminar_20151001.html

Application Security Super Briefing 2015 Fall ～年末リリースに間に合う！アプリケーションセキュリティの最新事情と次の一手～

株式会社アスタリスク・リサーチ
エグゼクティブ・ディレクタ 岡田良太郎

セキュリティイニシアチブ・インストラクター。セキュア開発支援ツールSecureAssistや、E-Learningベースのセキュリティ・トレーニングを通し、開発チームを支援する事業等に従事。また、技術コミュニティの活動として、国内の「WASForum Hardening Project(ワスフォーラム・ハーデニングプロジェクト)」、またグローバルコミュニティでは「OWASP(オワスプ) Japan」チャプターリーダーを務める。2014年にはOWASPよりBest Chapter Leader賞を受賞。CISA、MBA。
Twitterアカウント: @okdt

ソニーデジタルネットワークアプリケーションズ株式会社
Chief Security Technology Officer 松並 勝

日本におけるSDL(Security Development Lifecycle)の第一人者であり、ソニーグループのセキュリティ活動を牽引。一般社団法人日本スマートフォンセキュリティ協会(JSSEC)の技術部会 セキュアコーディンググループリーダー。2015年には情報セキュリティプロフェッショナルの育成と発展に寄与した、アジア・パシフィック地域のリーダーとその功績を表彰している「(ISC)2 Asia-Pacific ISLA プログラム」を受賞。

セミナー概要

対象: 自社プロダクト開発会社、受託開発会社の皆様
開発部門、品質管理部門、セキュリティ部門の皆様

内容: アプリケーション開発は、ウェブサイトはもちろんのこと、スマートフォン、ウェアラブル、社内のイントラシステムなど適用範囲が急激に拡がっています。これに伴い、攻撃は多様化しており、被害の影響も多様化しています。事後対応的な手段は追いつかなくなっており、ソフトウェア開発者に対する対外的な責任も期待も大きくなっています。では、どうすれば良いのか。セキュアなものづくりを実現する現実的な手立ては何か。最新レポートと次の一手をブリーフィングします。

開催日時: 2015年10月1日 (木) 14:30～16:30
(14:00受付開始)

会場: ベルサール神保町 Room1
〒101-0065 東京都千代田区西神田3-2-1　住友不動産千代田ファーストビル南館2・3F
(近隣の「ベルサール神保町アネックス」とお間違えのない様お気をつけください。)

www.asteriskresearch.com