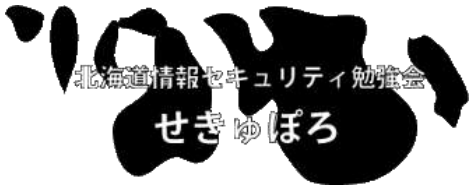
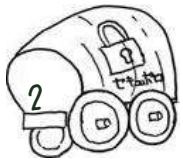
技術者100%脳

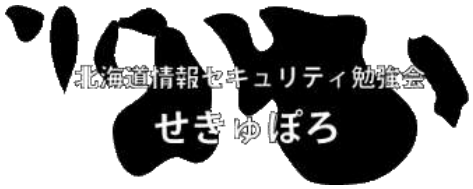
北海道情報セキュリティ勉強会
スタッフ まっちゃだいふく



自己紹介

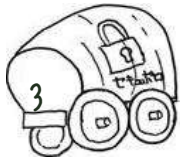
- ハンドル名：まっちゃだいふく
- やってること
  - 情報セキュリティ勉強会
    - まっちゃ139代表
    - まっちゃ445代表
    - 神戸情報セキュリティ勉強会スタッフ
    - 四国情報セキュリティ勉強会スタッフ
    - 北海道情報セキュリティ勉強会スタッフ
  - その他
    - Admintech.jpスタッフ
    - 静岡ITProo勉強会 スタッフ
- Microsoft MVP Consumer Security (2005/10-2009/09)
- ネットエージェント株式会社 エバンジェリスト♪
  - Internet Week 2008にてパネルディスカッション登壇





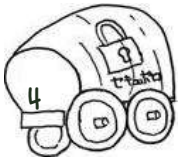
本日のアジェンダ

- 本日はセキュリティな技術ネタはまったく含まれません。
- セキュリティバリバリで聴きに来られた方ごめんなさい。



初めに、そして終わりに

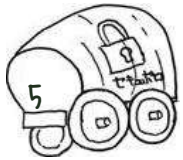
- 多層防御って知っていますか？
- 100%な製品や技術を求めず、技術を積み重ねて多層防御しましょう
- 理想論より現実論

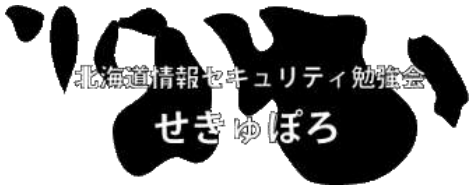


北海道情報セキュリティ勉強会
せきゅぽろ

だいいっしょう
第１章　ぼくらをとりまくじょうきょう

2008/11/01

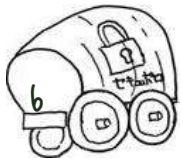


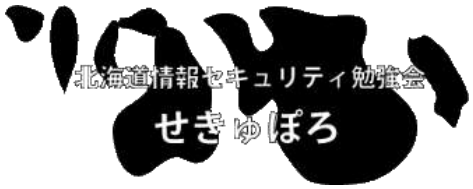


みんなをとりまくセキュリティ対策とか

- クロスサイトスクリプティング対策
- SQLインジェクション対策
- ブラウザのバグ対策
- OSの脆弱性パッチ
- DoS対策
- アプリケーションの脆弱性対策
- 未知の〇〇対策
- 未知の××対策

もう！！
どこまでやらな、あかんの！！

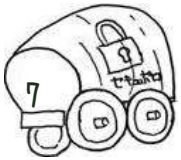




SDL（セキュア デベロップメントライフサイクル）

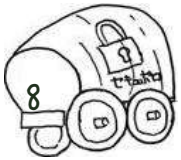
- デフォルトをセキュアにするための開発手法
- コンパイラでセキュリティをチェック
- ただ、未知の脅威・パターンは学習、再度確認（ここ重要！）
- セキュアな開発環境でエラー（脆弱性予備軍）が治らないと納品にならず
  - みんなエラー（脆弱性）について勉強するらしい

この実装！大変！



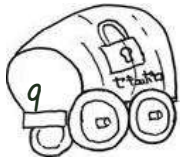
じゃ現実解は？

多層防御じゃね？



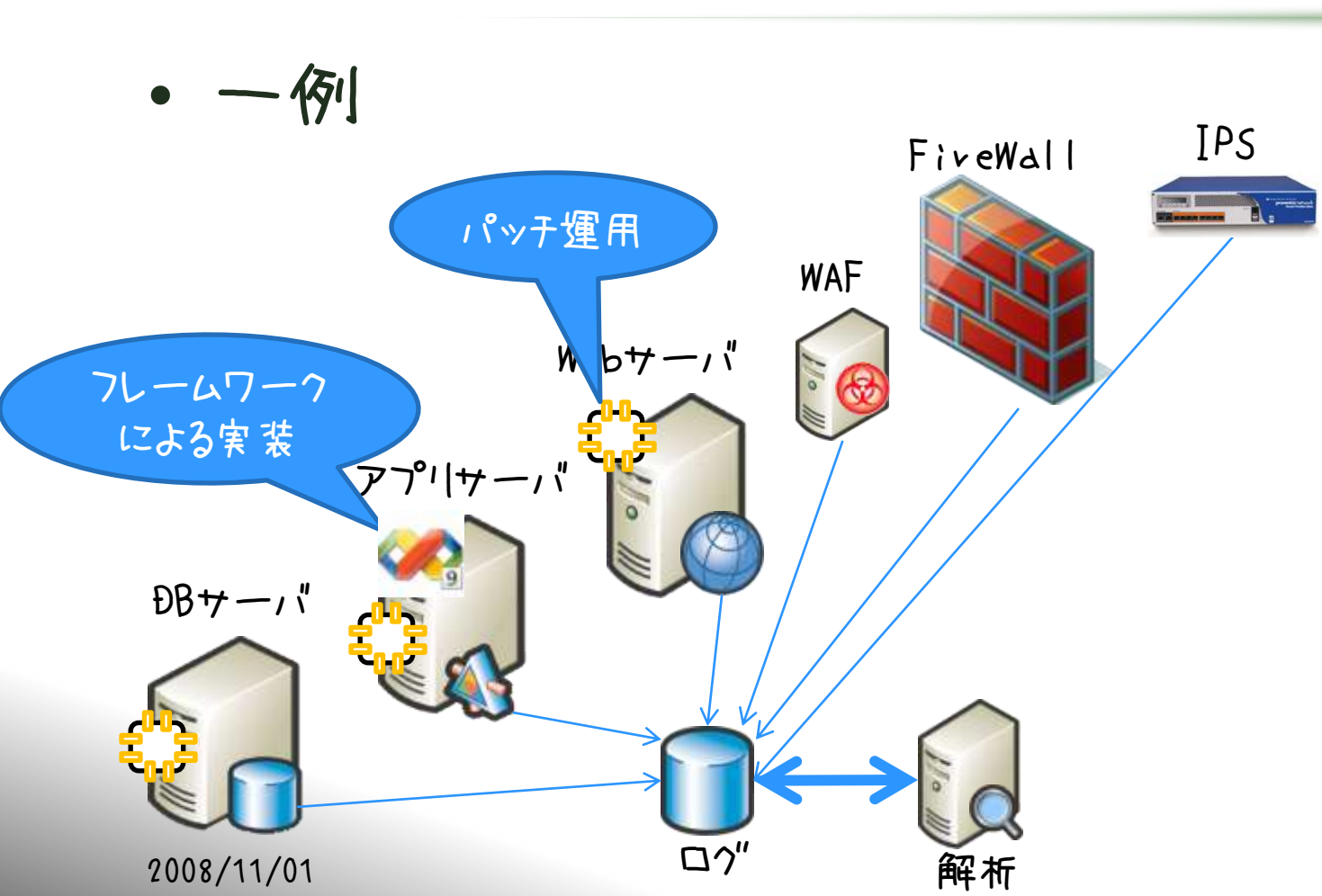
多層防御ってなに？

- 多層防御（Defense In Depth）とは、**何枚もの防衛壁を設置するように複数のセキュリティ保護対策を組み合わせて実施**することです。
  - 多層防御（Defense In Depth）とは：ScanNetSecurity - 情報セキュリティ用語辞典・用語集
    → https://www.netsecurity.ne.jp/dictionary/defenseindepth.html



ぐたいてきに～？！

- 一例


パッチ運用
フレームワーク
による実装
Webサーバ
アプリサーバ
DBサーバ
2008/11/01
WAF
FiveWall
IPS
ログ
解析

第1章終了

経験値10ポイント獲得
ゆうしゃのレベルがあがった
HPが10あがった
MPが3あがった
ポイミーのじゅもんをおぼえた

だい2しょう

第2章　ゆうしゃたちのぼうけん

あなたの周りに、こんな人いない？

- セキュリティを語りすぎて、具体的対策の実装に乏しい人
- 議論好きで、議論を展開するのが大好きで、具体的対策の実装に乏しい人
- セキュリティ対策を検討するが、なかなか進まない人

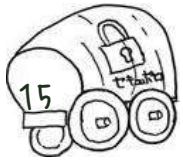
最近の技術者に多いパターン

- 未知の○○対策ができていないから、その製品ダメ（？）
  - その結果、結局A対策も、B対策も、C対策もしない
  - 結果0%
- Aを実装するには、ホワイトリストしかないよ！
  - 実際ホワイトで実装できるの？
  - 結果0%
- 机上で検討で終わり
  - 結果0%
- お金かかる
  - 結果0%

！なんかちがう！（怒

研究者のパターン

- A対策も、B対策も、C対策も、D対策も対処できる技術を考える
  - 究極と至高
  - でも究極の対策がでると、至高の攻撃が出る
  - 切磋琢磨して高めあう？
  - あっちは攻撃手法を情報共有
    （守る側の方が弱い立場・・・）



なので・・・

- 研究者は100％を求めてくださいw
- 100％の議論をどんどんしてください！！！
- よりよい研究結果が、利用者を幸せにします。

営業に多いパターン

- これだけやっていれば大丈夫
  - 100%の製品なんてありえない
- あとから・・・
  - これは、仕様です。できません…
  - サポートできません…

100%、銀の弾丸は無い！

- 銀の弾丸なんてない！
  - ソフトウェア工学の分野においては、フレデリック・ブルックスが1986年に発表した論文において、No Silver Bullet（銀の弾丸など無い）というフレーズを用いて、全ての問題に通用する万能な解決策などは存在しないと論じたことから、理想論的なソフトウェア設計について否定的な意味で用いることが多い。
    （出典：銀の弾丸　Wikipedia http://ja.wikipedia.org/wiki/%E9%8A%80%E3%81%AE%E5%BC%BE%E4%B8%B8）

技術者のあるべきパターン

- A対策も、B対策も、C対策も、D対策も対策したいが…すべては費用対効果

リスク回避（Good） A対策と、B対策は根本解決する **いわゆる根本対策**	（soso）リスク制御 C対策は、例えば管理画面のIP制限とか **間接的対策**
リスク移転（rich） 情報漏洩保険かけとこっか… **他人のせいw**	（not so good）リスク許容 もう対策とリスクを理解して、許容する大きな器wwww 対応策を事前に作っておく必要があり **ノーガード戦法**

北海道情報セキュリティ勉強会
せきゆぽろ

小さなことからコツコツと

©西川きよし

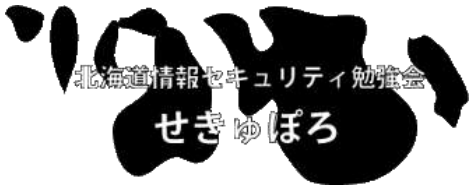
- すべてはISO的な考え方
  - できる範囲で初めて、小さくカイゼン
  - 少しずつスパイラルアップ
  - よりよくするために！！！
- だから開発運用も大切
  - 作って終わりなんてありえないw
  - SEは作るまでじゃなくって、運用まで考慮する必要あり

第2章終了

経験値100%ポイント獲得
ゆうしゃのレベルがあがった
MPが100あがった
メガテンのじゅもんをおぼえた

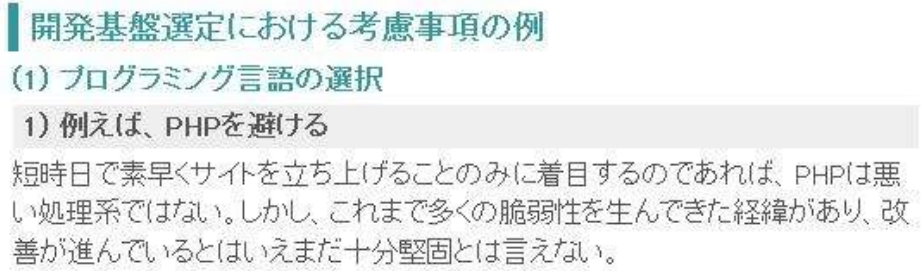
だいさんしょう

第3章　みちびいていくひとたち



現場の技術者はなにをすべき？

- 何をすればいいの？
  こういうのを、できる範囲で実装、運用開発でカイゼンしていく
  - 例えばセキュアと言われているプラットフォーム（Windows？Linux？）
  - 例えばセキュアといわれている開発規約（ライブラリ？共通モジュール？コーディングルール？）
  - 例えばセキュアといわれているフレームワーク（Hibernateとか？）
  - 保険？
  - 例えばPHPを避けるw



開発基盤選定における考慮事項の例

(1) プログラミング言語の選択

1) 例えば、PHPを避ける

短時日で素早くサイトを立ち上げることのみに着目するのであれば、PHPは悪い処理系ではない。しかし、これまで多くの脆弱性を生んできた経緯があり、改善が進んでいるとはいえまだ十分堅固とは言えない。

脆弱性検査？

- リリース前の脆弱性検査はやっておくべき
- 定期的な脆弱性検査もやった方がよいね～
  - 攻撃側はどんどん進化する！
    新しい攻撃手法の影響を確認できる
  - 開発規約があれば、同様のページを作ってない？（応用可能じゃね？）

最近の攻撃者のうごき

- OSSアプリとか（検索→ Go!）
  - 新しいぜい弱性
  - まずググるw
  - 使ってる、GO!!!!
- カスタムアプリ（単純な脆弱性→掘り下げ）
  - かるーく単純なXSSがあるぞ！
  - 怪しいなセキュアコーディングしてねーぞ
  - 次、”’”入れてみようとか思うわけで…
  - SQLエラー ktkr！

じゃ、、、すげー攻撃者は？

ゴルゴメソッド©kawa

- kawa氏の「ゴルゴメソッド」は面白かった。これは、セキュリティ系のサービスを提供する際に、クライアントに「どこまでなら守れるのか」という意味で限界があることを伝える際に使う。
  「だって、いくら優秀なボディガードを雇ったって、ゴルゴに狙われたらおしまいですよね？つまりそういうことです。この○×侵入防止システムは通常のレベルの攻撃は防ぎますが、ゴルゴ級のハッカーを防ぐことはできないです。Gは無理です。」
  こう言えばクライアントも心の底から納得するという。
- 主典：Wizard Bible vol.29 (2006.11.7)
  → http://wizardbible.org/29/29.txt

対ゴルゴ？それとも？？？

- ゴルゴ側の情報収集って常にするの？
  - 難しい問題、でも大変、てか無理
  - でも、知っておけば事前に早めに、自分たちで対応できるかも。
- で、結局攻撃って？どうよ。
  - ゴルゴじゃない人がほとんど。
- ゴルゴじゃない人の動きは？
  - 結構ニュース(ITProとかITMedia) で報道される(ITProは結構いい感じ)

ゴルゴ以外対策

- ゴルゴじゃない人の対策？
  - はるか昔、スクリプトキディと呼ばれる、ツールを使ってやっちゃう人たち（SQL注入工具とか）
  - 例えば、クロスサイトやSQLインジェクションはHibanateでほとんど落としてる？
  - 例えば、ブラックリスト（シグニチャ）で落とす？

正直、僕の拙い検査では脆弱性を発見できず…orz

なので、結局

- 結局ゴルゴ対策なんて、無理・無駄じゃない？
  - スクリプトキディを落とせばいいんじゃね？
  - そこで90%？（想定）倒せてる？
- じゃ、非ゴルゴが興味を持たなかったら？
  - ご遠慮してもらえる？
  - 結局お客さんは来ないでいいんじゃね？

だから

色々な対策で多層防御！

第3章終了

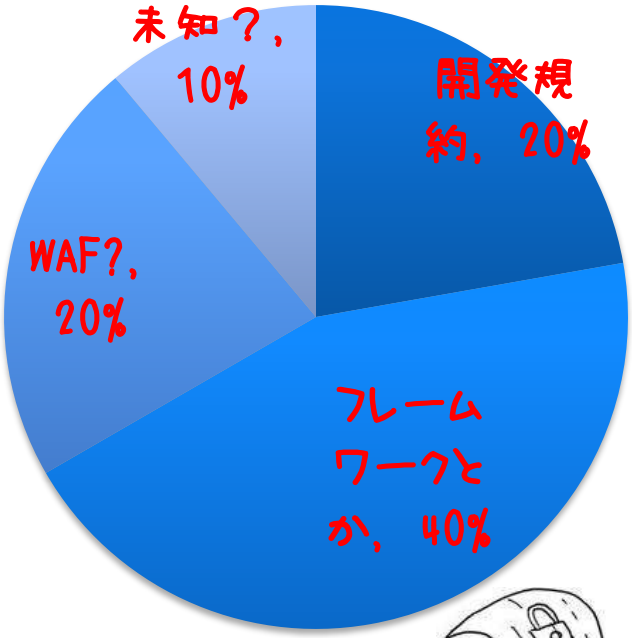
経験値46ポイント獲得
ゆうしゃのレベルがあがった
MPが1 あがった
ドラゴルゴのじゅもんをおぼえた

だいよんしょう

第4章　エンディング

結論

- 100％な製品や技術を求めず、技術を積み重ねて多層防御しましょう
- 理想論より現実論
- ぜい弱性検査は定期的に
- 究極の対策なんてありえない
- 実際の対策　→
  数値は適当wwwww



だから

- 100%なんてないんだ、究極対至高の対決が終わらないように…
- 多層防御の重要性
- まず小さなプロジェクトでカイゼン・カイゼン
- そして、適用
- 技術者よ研究者たるな！
- 研究者よ技術者たるな！

北海道情報セキュリティ勉強会
せきゅぽろ

The End

2008/11/01

北海道情報セキュリティ勉強会
せきゅぽろ

ご清聴ありがとうございました

2008/11/01