ユニシス研究会
JAPAN UNISYS USERS ASSOCIATION

どこまでやるのセキュリティ

～”守るべき情報“に応じた、情報漏えい対策の検討

2014年度　研究活動　関西３グループ

株式会社ノエビアホールディングス
松原竜太
けいしんシステムリサーチ株式会社
永田　喜洋

BITS 2015
NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

ユニシス研究会関西3Gについて

メンバー構成

氏　名	所　属　会　社	役割
松原　竜太	株式会社ノエビアホールディングス	リーダー
永田　喜洋	けいしんシステムリサーチ株式会社	サブリーダー
室井　昭広	因幡電機産業株式会社	
長谷川　智治	Ｇ＆Ｕシステムサービス株式会社	
粟野　恵介		
松本　靖	日本ユニシス株式会社	アドバイザー
中田　和宏	日本ユニシス株式会社	アドバイザー

アジェンダ

1.研究テーマ選定
2.目指すべきゴールと
　　ゴールへのアプローチ
3.セキュリティ基準の作成
4.セキュリティ基準の検証
5.まとめ

研究テーマ

どこまでやるの　セキュリティ

■選定背景

関西支部はユニシス研究会史上初「分野別エントリー方式」
メンバー募集時は「情報セキュリティに関する研究」

■ステップ1　ブレインストーミング

自身の会社へWAF（WebApllicationFirewall）
導入の提案をしたが、上司から却下された。
どうすれば良いのか

却下理由
・費用
・WAF or IPS/IDS

研究テーマ

■テーマ候補

IEの脆弱性

業務効率・利便性

自社のセキュリティ対策の有効性

情報漏えい

クレジットカードのセキュリティ

費用対効果

組み込み機器セキュリティ

スマートデバイス

災害時の備え

研究テー

もし、しなければならない
セキュリティ対策が
決まっていたら？

■テーマ候補

自社のセキュリティ対策の有効性

十分？不十分？

業務効率・利便性

セキュリティとどちらを優先？

費用対効果

どこまで費用をかけるべき？

研究テーマ

採るべき
セキュリティ対策の基準
が明確に存在すれば、
解決！！

■テーマ候補

自社のセキュリティ対策の有効性

基準と比較して過不足確認！

業務効率・利便性

不便でも基準通りに！

費用対効果

費用に見合わないと思っても基準通りに！

研究テーマ

採るべきセキュリティ対策の基準を作成したい！！

セキュリティ。
しなきゃいけないのはわかってる。
でも、時間もない。お金もない。
いったい、どこまでしたらいいの？

研究テーマ

採るべきセキュリティ対策の基準を作成したい！！

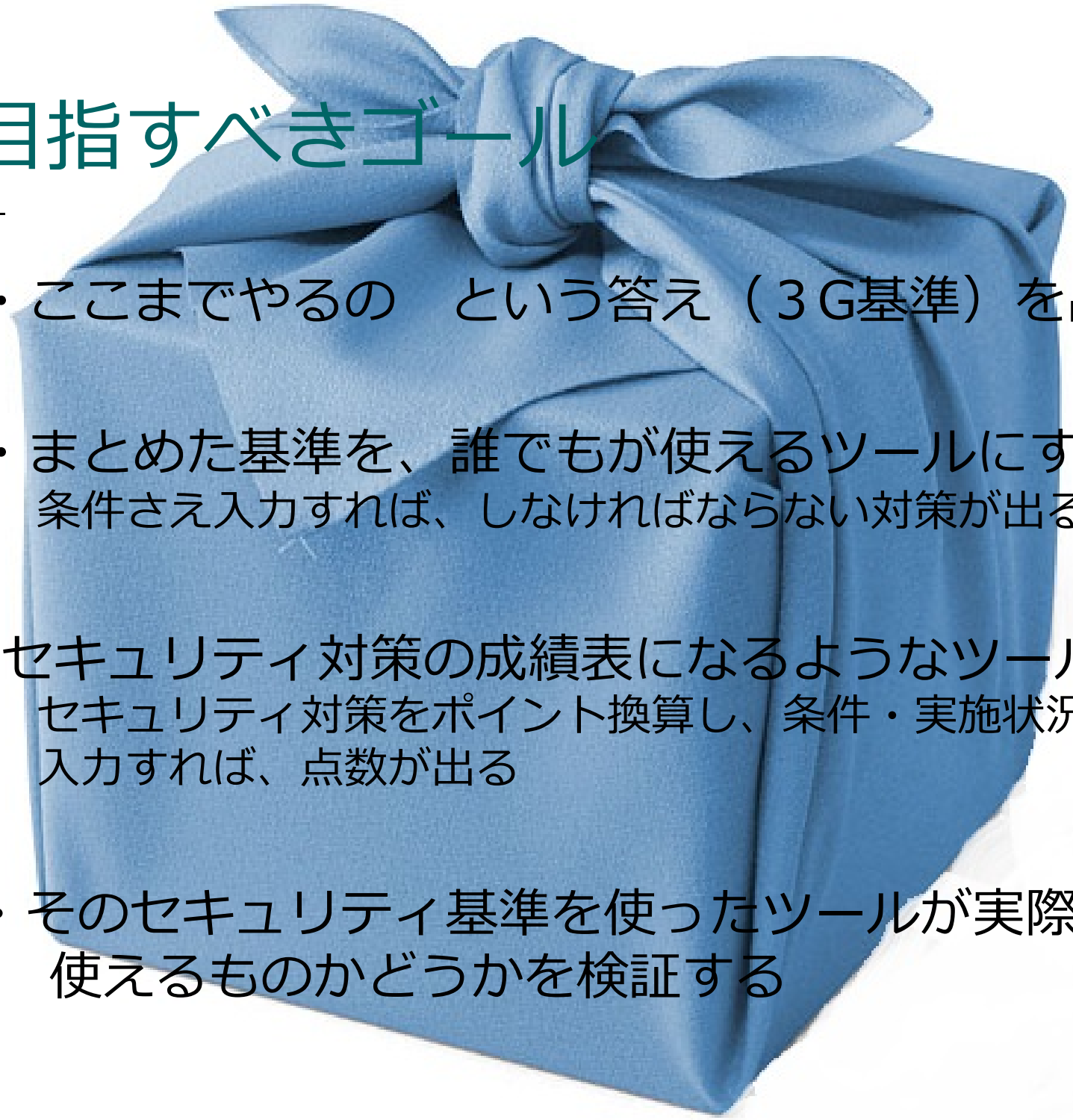
セキュ
しなき

テーマ決定！！
どこまでやるの　セキュリティ

サブテーマ

”守るべき情報”に応じた、情報漏えい対策の検討

目指すべきゴール



・ここまでやるの　という答え（３G基準）を出す

・まとめた基準を、誰でもが使えるツールにする
条件さえ入力すれば、しなければならない対策が出る

・セキュリティ対策の成績表になるようなツールにする
セキュリティ対策をポイント換算し、条件・実施状況を
入力すれば、点数が出る

・そのセキュリティ基準を使ったツールが実際に
使えるものかどうかを検証する

ゴールへのアプローチ

■**ステップ1**

守るべきもの/リスク/対策のピックアップから始めた。

- 個人情報
- 新製品情報
- Webサイト
- PC、サーバ
- 企業イメージ
- ブランドイメージ
- 社員の安全

サブテーマ

”守るべき情報”に応じた、情報漏えい対策の検討

某通信教育企業の大事件のニュース

守るべきもの　→”個人情報”

リスク　→”情報漏えい”

情報内容・利用方法・保管場所　等の条件毎に、
採るべき情報漏えい対策は異なるはず

ゴールへのアプローチ

■ステップ2

個人情報にもいろいろ

最も価値が高いものは？

漏えいした際に、最も被害額が高いものは？

クレジットカード情報

国際カードブランド5社が共同で作ったセキュリティ基準

PCIDSS(Payment Card Industry Data Security　Standards)

PCIDSS

要件1

カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること

～

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、保守すること

～

要件12

情報セキュリティに関するポリシーを整備すること

300個以上のセキュリティ項目からなるセキュリティ基準

セキュリティ基準の作成

関西3Ｇが作成するセキュリティ基準(３Ｇ基準)のイメージ

	条件A	条件B	条件C
セキュリティ対策項目①	○	×	○
セキュリティ対策項目②	○	○	○
セキュリティ対策項目③	×	○	×

セキュリティ基準の作成

■縦軸（セキュリティ対策項目）

PCIDSS

・具体的・定量的で理解し易い。が、一部…

→我々なりに咀嚼し、分かり易い表現に変更

・300以上のセキュリティ対策項目

→類似性の強いものを集約した結果、230項目

セキュリティ基準の作成

■横軸（条件）

個人情報の種類
①基本情報　：氏名、住所、生年月日、性別、電話番号
②機微情報　：病歴、犯歴、思想・宗教など
③カード情報：カード番号、有効期限、セキュリティコード

情報の入出力経路（Web、イントラ）

保存方法（データベース、紙）

セキュリティ基準の作成

■ **横軸（条件）** 15条件

個人情報なし	個人情報あり														
	ｸﾚｼﾞｯﾄｶｰﾄﾞ				機微情報					基本情報					
	Web入力		ｲﾝﾄﾗ入力		Web入力		ｲﾝﾄﾗ入力			Web入力		ｲﾝﾄﾗ入力			
	DB格納あり	DB格納なし	DB格納あり	DB格納なし	DB格納あり	DB格納なし	DB格納あり	DB格納なし	紙で保存	DB格納あり	DB格納なし	DB格納あり	DB格納なし	紙で保存	

セキュリティ基準の作成

230項目のセキュリティ対策 × 15条件＝3,450

15　条件

230項目

	個人情報あり										
	クレジットカードあり				機微情報						
	Webサイトからの入力あり		イントラからの入力あり		Webサイトからの入力あり		イントラからの入力あり			Webサイトからの入力あり	
備考	DB格納あり	DB格納なし	DB格納あり	DB格納なし	DB格納あり	DB格納なし	DB格納あり	DB格納なし	紙で保存	DB格納あり	DB格納なし
少なくとも90日ごとに非アクティブなユーザアカウントを削除／無効化する。	全員同じ：○	多数決　：○ ×は、松原	全員同じ：○	多数決　：○ ×は、松原	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	多数決　：× ○は、長谷川	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分 松原 永田 長谷 室井
ベンダーがリモートアクセス経由でシステムへのアクセス、サポート、メンテナンスが必要な場合、必要な期間内だけ有効にする。	全員同じ：○	全員同じ：○	全員同じ：○	全員同じ：○	全員同じ：○	全員同じ：○	全員同じ：○	全員同じ：○	多数決　：○ ×は、室井	全員同じ：○	全員同
ベンダーがリモートアクセス経由でシステムへのアクセス、サポート、メンテナンスが必要な場合、使用時にログ等で監視する。	全員同じ：○	多数決　：○ ×は、松原	全員同じ：○	多数決　：○ ×は、松原	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	多数決　：× ○は、長谷川	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見 松原 永田 長谷 室井
6回以下の試行で、ユーザIDをロックアウトする。 （遅延管理もしくは、管理者による再有効化）	全員同じ：○	多数決　：○ ×は、松原	全員同じ：○	多数決　：○ ×は、松原	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	多数決　：× ○は、長谷川	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	意見 松原 永田 長谷 室井
セッションのアイドル状態が15分を超えた場合、セッション再アクティブ化にユーザの再認証を必要とする。	全員同じ：○	全員同じ：○	全員同じ：○	全員同じ：○	多数決　：○ ×は、永田	多数決　：○ ×は、永田	多数決　：○ ×は、永田	多数決　：○ ×は、永田	意見分裂 松原　：○ 永田　：× 長谷川：○ 室井　：×	多数決　：○ ×は、永田	多数 ×は、
パスワードの暗号化を行う。	全員同じ：○	全員同じ：○	多数決　：○ ×は、松原	多数決　：○ ×は、松原	多数決　：○ ×は、永田	意見分裂 松原　：○ 永田　：× 長谷川：○ 室井　：×	意見分裂 松原　：× 永田　：× 長谷川：○ 室井　：○	多数決　：× ○は、長谷川	多数決　：× ○は、長谷川	多数決　：○ ×は、永田	意見 松原 永田 長谷 室井
パスワードのリセット、新しいトークンの準備、新しいキー生成依頼の再、ユー					意見分裂 松原　：○	意見分裂 松原　：○	意見分裂 松原　：○	意見分裂 松原　：○	意見分裂 松原　：○	意見分裂 松原　：○	意見 松原

セキュリティ基準の作成

セキュリティ基準の作成

■**メンバー間の意見の分かれ**

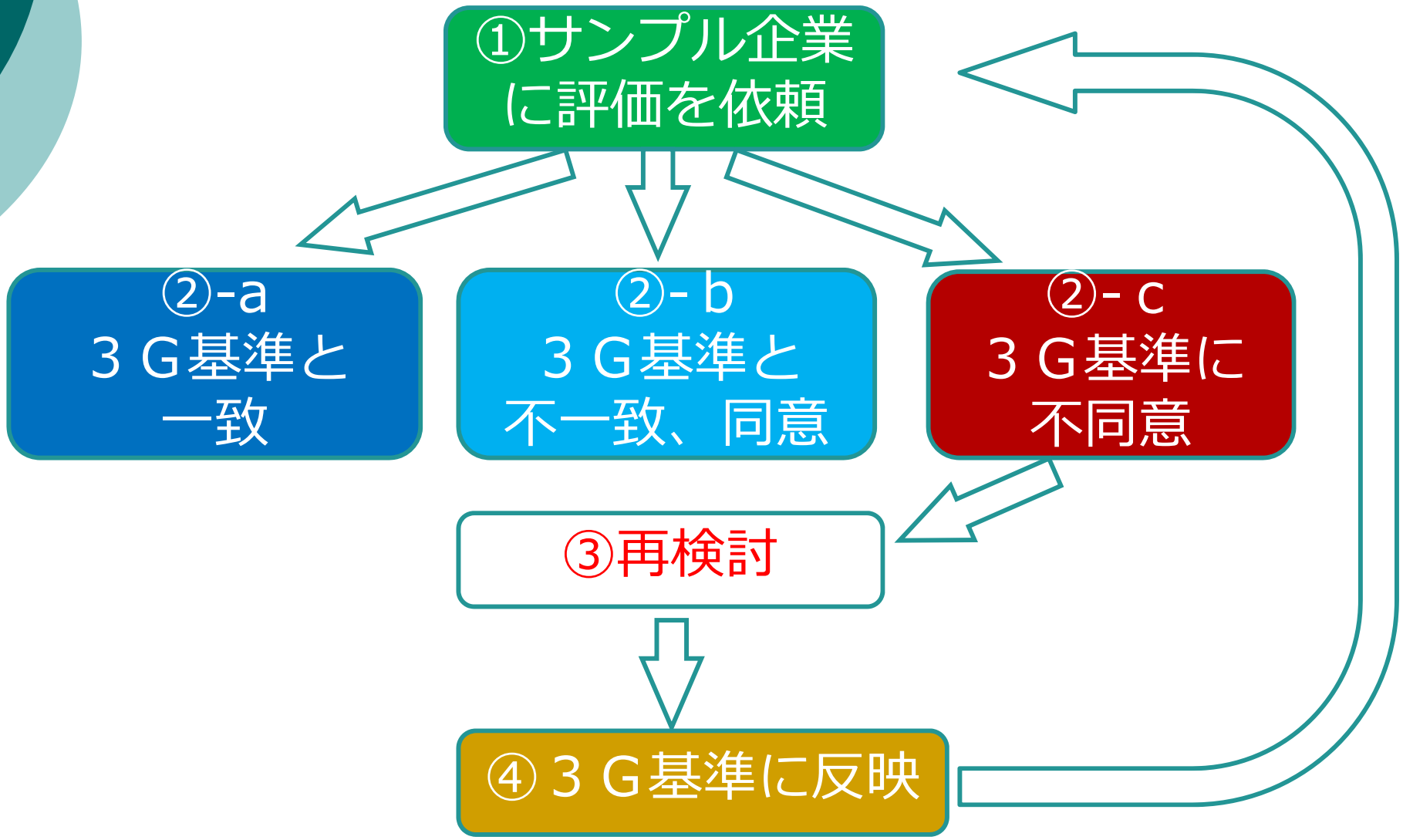
4：0	一致	40%	
3：1	多数決	42%	
2：2	不一致	18%	617件

グループ内で討議し、３Ｇとして意見を一致させた

3G基準（β版）の完成

セキュリティ基準の検証

■ **３Ｇ基準の妥当性の検証方法 & ブラッシュアップ**



セキュリティ基準の検証

■ ３Ｇ基準の妥当性の検証

・サンプル企業３社

企業	基本情報	入力	DB格納
サンプルA社	あり	Webサイト	あり
サンプルB社	あり	イントラのみ	あり
サンプルC社	あり	イントラのみ	あり

・要件6（２５項目）

「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」

・妥当性の判断基準

判断条件	妥当性
○・×が３Ｇ基準と一致している	妥当である
○・×が３Ｇ基準と不一致だが、３Ｇ基準に同意する	妥当である
○・×が３Ｇ基準と不一致で、３Ｇ基準に同意しない	妥当でない

セキュリティ基準の検証

■３Ｇ基準の評価結果

判断条件／企業	A社	B社	C社	合計
○・×が３Ｇ基準と一致している	16	17	15	48
○・×が３Ｇ基準と不一致だが、３Ｇ基準に同意する	6	1	1	8
○・×が３Ｇ基準と不一致で、３Ｇ基準に同意しない	3	7	9	19
妥当性	88%	72%	64%	75%

→不一致・不同意の項目について、再討議

セキュリティ基準の検証

■不一致・不同意項目の再討議

「イントラ入力」・・・メンバー間の認識相違

前提

・イントラ入力のみのシステムに対して、外部からのアクセスはない

・セキュリティホールをついてまで攻撃を行う攻撃者は、内部には存在しない

要件6.2

「OSおよびソフトウェアの重要なセキュリティパッチをリリース後1カ月以内に適用する」

要件6.5.1

「アプリケーション開発において、SQLインジェクションに対応したセキュアコーディングを行う」

セキュリティ基準の検証

■３Ｇ基準の評価結果

判断条件／企業	A社	B社	C社	合計
○・×が3G基準と一致している	16	17	15	48
○・×が3G基準と不一致だが、3G基準に同意する	6	1	1	8
○・×が3G基準と不一致で、3G基準に同意しない	3	7	9	19
妥当性	88%	72%	64%	75%

■３Ｇ基準の再評価結果

判断条件／企業	A社	B社	C社	合計
○・×が3G基準と一致している	16	21	20	57
○・×が3G基準と不一致だが、3G基準に同意する	6	1	1	8
○・×が3G基準と不一致で、3G基準に同意しない	3	3	4	10
妥当性	88%	88%	85%	86%

セキュリティ基準の検証

■不同意の項目

要件6.2

「OSおよびソフトウェアの重要なセキュリティパッチをリリース後1カ月以内に適用する」

３Ｇ基準・Ｃ社	×
Ｂ社	○

要件6.5.5

「アプリケーション開発において、適切なエラー処理を行う(具体的なエラー表示をせず、汎用エラーメッセージを表示する)」

３Ｇ基準・Ｂ社	×
Ｃ社	○

セキュリティ基準の検証

■不同意の項目

企業	基本情報	入力	DB格納
サンプルA社	あり	Webサイト	あり
サンプルB社	あり	イント三のみ	あり
サンプルC社			

妥当性100%、存在する？

判断条件／企業	A社	B社	C社	合計
○・×が3G基準と一致している	16	21	20	57
○・×が3G基準と不一致だが、3G基準に同意する	6	1	1	8
○・×が3G基準と不一致で、3G基準に同意しない	3	3	4	10
妥当性	88%	88%	85%	86%

まとめ

■**成果**

どこまでやるの

個人情報に絞り、PCIDSSを基に

230項目のセキュリティ対策項目　×　15条件

→**3,450**の項目からなるセキュリティ基準の作成

基準の検証

同意 ＝ 妥当　という考え方

要件6(25項目)　×　2条件　の50項目

妥当性**86%**の信頼できるセキュリティ基準

基準のツール化

残念ながら…

まとめ

■成果

ご来場の皆さま

・全項目検証済みの信頼できるセキュリティ基準

・セキュリティ対策状況を評価できるツール

関西３Gメンバー

・セキュリティに関する知識

・セキュリティに関する意識

ご清聴ありがとうございました。