SQUIRE PATTON BOGGS

システムベンダのセキュリティ対策義務

～東京地裁平成26年1月23日判決
（平23（ワ)32060号）を素材として～

「愚者は自分の経験から学ぶという。私はむしろ、最初から自分の誤りを避けるため、他人の経験から学ぶのを好む。」（オットー・フォン・ビスマルク）

スクワイヤ外国法共同事業法律事務所
弁護士　武田勝弘
Katsuhiro.takeda@squirepb.com

0. 目次

1．問題の背景

SQUIRE PATTON BOGGS

従来のセキュリティ・脆弱性対策は，Webアプリのベンダに責任ないことが明確だった

例：ファイアウォール，セキュリティパッチ，ウイルス対策

→Webアプリシステムのセキュリティ・脆弱性に対する責任の所在が曖昧のまま放置

ユーザー側の思惑

- セキュリティのことはよく分からない
- 必要なセキュリティ対策は「当然に」ベンダが行っているはずだ

ベンダ側の思惑

- 対策しても操作性が悪くなりコストアップしたのではコンペに負ける
- RFPにセキュリティー要求仕様がない→「当然に」受注の範囲外のはずだ

→2014年1月，双方の思惑の違いが争点となった事件に判決が下される…

2. 事案の概要

SQUIRE PATTON BOGGS

原告（ユーザー）：インテリア商材の販売等を事業とする会社
被告（ベンダ）：　情報処理システムの企画・開発・保守等を事業とする会社

2009年2月：　ウェブにおける商品受注システムの設計・製作を発注（890万円）
2009年4月：　原告がシステムの使用を開始
2010年1月：　顧客のクレジットカード種別を把握できるよう仕様変更を要求(31万円)
2010年5月：　Webサイトメンテナンス契約を締結（月額5.5万円）
2011年4月：　サーバへの不正アクセス，顧客クレジットカードの不正利用が発覚
2011年?月：　民事調停が不調に終わる
2011年10月：委任契約の債務不履行があったとして，顧客への謝罪や売上減少等
約1億900万円の損害賠償請求訴訟を提起
2014年1月：東京地方裁判所が被告に2262万円等の支払を命じる判決
→控訴されず確定

3. 本判決のポイント（1）

SQUIRE PATTON BOGGS

1） クレジットカード情報を含む個人情報流出の原因を，直接裏付ける証拠がないにもかかわらずSQLインジェクションが原因であると認定

2） 契約書に明示されていなくても，契約当時の技術水準に従ったセキュリティ対策を施したプログラムを提供することが，当事者間で黙示的に合意されていたと認定

3） 契約書に明示されていないことから，目的とする情報処理に不要なクレジットカード情報を削除もしくは暗号化する義務を当然に被告（ベンダ）が負うことにはならない

4） 契約書に明示されていないことから，被告（ベンダ）はセキュリティ対策に問題があることを説明すべき義務を負わない

→本稿では2） 3） 4)を検討

3. 本判決のポイント（2）

SQUIRE PATTON BOGGS

5) クレジットカード情報を扱うように仕様変更したにもかかわらず，被告（ベンダ）にセキュリティ対策を指示しなかった原告（ユーザー）に3割の過失相殺を認定

6) 秘密保持義務違反の場合は賠償額を契約金額の範囲とする契約書の規定は適用されない

7) 故意または重過失がある場合は賠償額を契約金額の範囲とする契約書の規定は適用されない

8) SQLインジェクション対策を施さなかった被告（ベンダ）に重大な過失があったと認定

→本稿では8)を検討

4. 黙示的な脆弱性対策の合意（1）

SQUIRE PATTON BOGGS

判決の理由に記された裁判所の考え方

- 事実：2006年2月，経産省が，独立行政法人情報処理推進機構(IPA)の紹介するSQLインジェクション対策を行うよう注意喚起し，2007年4月，IPAが，同対策として，バインド機構の使用またはエスケープ処理を施すべきであると注意喚起

- 事実：本件システムが発注された2009年2月当初から，顧客の個人情報がデータベースに保存される設定になっていた

- 結論：当事者間では，SQLインジェクション対策としてバインド機構の使用またはエスケープ処理の施されたプログラムを提供することが**黙示的に合意**されていた

→経産省・IPAが注意喚起すれば当事者の意思に関わらず義務になる！？

4. 黙示的な脆弱性対策の合意（2）

判決の理由に記されてない裁判所の考え方

- 裁判官の経験則：一般的に日本の契約書は概括的な事項しか記載されておらず，重要な合意事項であっても記載されていない場合が少なからずある。

- 書かれざる前提1：本件契約書にシステムの脆弱性対策に関する事項が記載されていなかったとしても，当事者が合意していた事項が存在するはずである。

参考判例（東京地判平16.6.23）

「もともとソフトウェアの仕様書は複雑なものであり，専門家でなければ容易にわかり得ないものであるから，仕様書に記載がないからといって，契約の内容になっていないということはできない。」

4. 黙示的な脆弱性対策の合意（3）

SQUIRE PATTON BOGGS

判決の理由に記されてない裁判所の考え方（続き）

- 書かれざる前提2：

  個人情報取扱事業者として個人データの安全管理措置を講ずる義務のあるユーザーとしては，

  システム開発の専門家であるベンダにシステム開発を発注するに際して，

  特別な指示をしなくても，既知の脆弱性に対し，当時の技術水準に応じた対策がなされたプログラムが提供されることを通常期待するはずで，

  かつベンダもそのことを知っていたはずだ。

「ユーザーの期待」＋「ベンダの認容」→「黙示の合意」

- 後述する重過失の認定では同様の内容について言及

4. 黙示的な脆弱性対策の合意（4）

SQUIRE PATTON BOGGS

若干の検討と小活

- 裁判所の考える「常識」と，業界の「常識」は，しばしば異なる
  →裁判所の「常識」に基づく判断は，業界にとって「非常識」な判断になることも

- 裁判所も個々の事案の特殊性を無視するものではない
  →個別の事案で裁判所の考える「常識」を覆すだけの事実・証拠があるかが勝負

- 業界の人間であれば当然知っておくべき「常識」であるが故に記録に残りにくい
  →いざ裁判になって業界の「常識」を立証することは極めて困難

- 裁判官の考える「常識」が，本件では通用しないことを裏付ける事実を，紛争になる前から積み重ねておくことが大切

4. 黙示的な脆弱性対策の合意（5）

SQUIRE PATTON BOGGS

- 望まれる事前対応策案：
  i. RFP（提案依頼書）にセキュリティ要求仕様を入れてもらう
     参考資料：JNSAセキュアシステム開発ガイドライン「Webシステム　セキュリティ要求仕様(RFP)」編 β 版
  ii. 見積書にオプションとして脆弱性（セキュリティ）対策費目を入れる
  iii. 同対策が契約内容に含まれないことを契約書に明記する
  iv. 同対策が契約内容に含まれないことを説明して記録を残す
  v. 契約書に完全合意条項を入れる

- 経産省・IPAの注意喚起する脆弱性対策が，契約書に記載されていない本件と同様な事例であっても，対策が契約内容になっていないことを裏付ける事実を積み重ねることで，黙示的な対策の合意があったと認定される可能性を大幅に低減できる

- ただし，今後は，契約書に記載がない場合，何も手を打っていないと一般的な脆弱性（セキュリティ）対策がシステムの標準装備として義務化されてしまうおそれがある

5. 不要情報削除・暗号化義務（1）

SQUIRE PATTON BOGGS

- 厚労省・経産省の個人情報保護法ガイドライン（2007年）

  クレジットカード情報等について，利用目的達成に必要最小限の保存期間を設定し，保存期間経過後は適切かつ速やかに破棄すること等を，特に講じることが望ましい安全管理措置として例示

  →不要情報削除はあくまで「望ましい」措置に過ぎない

- IPAの公表文書(2007年)

  個人情報について暗号化することが望ましいと指摘

  →暗号化はあくまで「望ましい」措置に過ぎない

- 同じIPA文書内

  サーバに負荷をかけぬよう特定のカラムだけ暗号化する考慮も必要と指摘

  →暗号化の設定内容は程度により異なり，これによりベンダの作業量や代金も増減

5. 不要情報削除・暗号化義務（2）

SQUIRE PATTON BOGGS

- 判示「契約で特別に合意していなくても，当然に，被告がクレジットカード情報を本件サーバ及びログに保存せず，若しくは保存しても削除する設定とし，又はクレジットカード情報を暗号化して保存して保存すべき債務を負っていたとは認められない。」

- 疑問点：不正侵入されないように脆弱性を除去すること，仮に不正侵入されても被害が拡大しないように不要な情報は保存しない，または情報を暗号化することは，いずれもセキュリティー対策の基本では？

→脆弱性対策は当然義務化されたのに，不要情報削除・暗号化等が当然には義務化されなかったのは，理屈よりもガイドライン等の証拠の問題

→本判決の結論は絶対ではない，今後の事実・証拠次第では不要情報削除・暗号化等も当然に義務化される余地がある

→脆弱性と同様の事前対応策を検討すべき

6. 説明義務（1）

SQUIRE PATTON BOGGS

- 判決理由では，被告（ベンダ）は原告（ユーザー）に対し，セキュリティ対策について選択できるように説明すべき義務を負わないとした。

- 理由１：被告がSQLインジェクション対策をしないことが債務不履行なのだから，被告が債務不履行に陥っている旨の説明を，原告にしなかったことをもって，独立した債務不履行だとする意味がない。

- 理由２：原告は，被告から「クレジット情報は保持しないのがセキュリティ上より良く，一般的である」との説明を受けており，クレジットカード情報の保存による情報流出の危険性を認識していた。

→ベンダに説明義務がないという本判決の判断は，すでにベンダが別の債務不履行に陥っていたこと，及びすでに説明していたことが要因

→本判決の結論が，システム開発契約全般にあてはまると考えるべきではない

6. 説明義務(2)

SQUIRE PATTON BOGGS

- 取引価額が高額で，かつ当事者間の情報・専門的知識に大きな格差がある場合，情報・専門的知識のある当事者から他方当事者に対し，**信義則上の情報提供義務**が課されることがある。

  例：不動産売買，投資・投機的取引，フランチャイズ契約

- 参考判例：ユーザーからの仕様変更の申し入れがシステムの不具合・障害の発生の可能性を増大させる場合，ベンダはソフトウェア開発契約の**付随的義務**として，その専門的知見・経験に照らし，ユーザーにこれを**告知して説明する義務**を負うと判示した事例（東京高判平26.1.15）

- 事案によっては，ベンダーもユーザーに対して，システムのセキュリティ対策の必要性等について，情報提供・説明義務が課される可能性がある

  →RFPにセキュリティ要求仕様がない場合でも，当該システムにどのようなセキュリティ上の問題があり，どのような脅威にさらされているか最低限の指摘をして記録に残したい

7. 重過失(1)

SQUIRE PATTON BOGGS

- 裁判所は，契約書に記載されていない脆弱性対策を施さなかった被告(ベンダ)に重過失を認めた。

- 参考判例(東京高判平25.7.24)

「著しい注意義務違反(重過失)というためには，結果の予見が可能であり，かつ，容易であること，結果の回避が可能であり，かつ，容易であることが要件となる」

→結果予見容易性＋結果回避容易性＝重過失

- 前提1：ベンダーはシステム開発の専門業者であり，ユーザーもその専門的知見を信頼してシステムを発注した

→ ベンダーに求められる注意義務の程度は比較的高度と判断

Cf. 注意能力の程度：[一般人]＜[詳しい一般人]＜[専門家]＜[詳しい専門家]

7. 重過失(2)

SQUIRE PATTON BOGGS

- 前提2：経産省及びIPAのSQLインジェクション攻撃に対する注意喚起
  →対策を行わなければ個人情報が流出することを，ベンダは容易に予見できた
- 前提3：IPAが対策として紹介しているバインド機構の使用またはエスケープ処理を行うことで個人情報流出は回避できた
- 前提4：同対策を行うことに多大な労力や費用がかかることをうかがわせる証拠はない
  →ベンダは容易に結果を回避することができた

結論：ベンダーに重過失が認められる

- そもそも義務違反かが争われる事案では，義務違反を基礎付ける証拠が見つかると，過失も認定されることが多い

7. 重過失(3)

SQUIRE PATTON BOGGS

未知の脆弱性？ Yes→ 重過失なし

No ↓

その脆弱性は業界の間で十分に認知されている？ No→重過失なし

Yes ↓

対応策が見つかっている？ No→重過失なし

Yes ↓

対応策が業界の間で十分に認知されている？ No→重過失なし

Yes ↓

当該事案で対応策に効果がある？ No→重過失なし

Yes ↓

対応策の実施に多大な労力・時間・費用がかかる？ Yes→重過失なし

No ↓

重過失あり

8. 判決の射程とまとめ

既知の脆弱性で対策が確立しているものについては，契約書やRFPに明示されていなくても，原則として，ベンダは対策を施したシステムを納入するべきとの枠組みは，今後の裁判でも維持される可能性が高く，対策が急務

本件事案では，不要な情報の削除義務・情報の暗号化義務は認められなかったが，今後の政府等の注意喚起などの事実関係が変化すれば，当然義務化される余地があることに注意

本件事案では，ベンダの説明義務違反は問われなかったが，情報の非対称性がある場合に説明（情報提供・告知）義務を問うことは一般的であり，今後の裁判では説明義務違反が問われる可能性も十分あることに注意

脆弱性対策を当然義務づけるような証拠が見つかった段階で重過失認定を避けるのは難しく，そもそも義務違反を問われない事前対応策が必要

9．控訴されなかった理由（想像）

SQUIRE PATTON BOGGS

- 原告（ユーザー）側の事情

  勝訴判決→情報漏えいの責任はベンダにあったことを顧客・株主にアピールできる
  →訴訟の目的達成

- 被告（ベンダ）側の　事情

  原告の過失相殺3割認定　→被告の言い分が取り入れられた＆賠償額が受注金額程度で落ち着いた　→訴訟の目的達成

- 双方の事情

  控訴審での予測が困難（地裁の法律構成に基づく新証拠の収集，担当裁判官の心証，過失相殺の相場がない）

  紛争の長期化によるデメリット（人員，費用，イメージ）

<<ご静聴いただきありがとうございました。>>