

PR : TechTargetジャパン特集



☐ ホワイトペーパー/カタログのみ

登録内容の更新のお願い
登録された内容がしばらく更新されていません。お手数をお掛けしますが、右のボタンから登録内容の確認と更新をお願いいたします。 ※ 登録内容の更新が反映されるまで、しばらく時間がかかることがあります。

セキュリティ

» 2013年05月31日 00時00分 UPDATE

Webアプリケーション開発に関する法律問題に詳しい弁護士に聞く

セキュリティ法律相談 脆弱性の責任を取るのは誰？

Webアプリケーションに脆弱性が発見された場合、その責任は実際に開発した企業にある——発注元はそう考えがちだ。果たして本当だろうか。システム開発に詳しい弁護士に聞いた。

外部の企業に開発を依頼したWebアプリケーションに脆弱性があり、個人情報漏えいなどのセキュリティインシデントが発生した場合、発注元企業の利用者に対する責任は、契約責任と不法行為責任が考えられる。

契約責任について、利用者は発注元企業との間で、利用規約等に基づく契約を締結している場合が通常であるから、発注元企業が契約責任を否定して開発企業にだけ責任があるとするのは難しい。

また、発注元企業の開発企業に対する指揮・監督関係が認められると、使用者責任が発生し、不法行為責任を否定することも困難である。

利用者に対する責任

その理由の1つは発注元企業に開発企業を監督する責任があるからだ。例えば個人情報を扱うWebアプリケーションに関連して言えば、「個人情報の保護に関する法律」（個人情報保護法）の第20条で、次のように明記されている。

第20条：個人情報取り扱い事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない

ここでいう「個人情報取り扱い事業者」とはWebアプリケーションを提供、保有する発注元企業であり、個人情報の安全管理について「必要かつ適切な措置」を取ることが求められる。加えて、個人情報保護法の第22条では、個人情報取り扱い事業者は委託先の「必要かつ適切な監督を行わなければならない」と定めている。Webアプリケーションを自社で管理せずに開発業者などに預けている場合も同様だ。

「発注元企業が、開発企業に個人情報の管理を委託する場合、開発企業などに対し、必要かつ適切な措置を行わなければならない。『必要かつ適切な措置』として要求される具体的な内容は、分野ごとに異なるが、安全管理措置の内容を指示していない場合などは、個人情報保護法第22条に違反することになる可能性が高い」（松島氏）

1年で切れる瑕疵担保責任と故意・過失の立証まで必要な不法行為責任

発注元企業が開発企業に対し、瑕疵担保責任や不法行為責任を追及する場面でも注意が必要である。

松島氏は「請負契約で開発されたWebアプリケーションの納品を受け、本稼働に入った後に脆弱性が発見された場合、瑕疵担保責任は無過失責任であるため、脆弱性が『瑕疵』と判断されれば、開発企業の過失の有無を問わず、法律上は、引渡しから1年間（民法637条）、瑕疵担保責任を根拠に発注元企業は開発企業に対して損害賠償等を請求することが

バラクーダネットワークス

できる」と説明する。

ここで、発注元企業が注意をしたいのは、契約で特約がなければ、「引渡しから1年経過した後に瑕疵の存在が判明しても、瑕疵担保責任を追及することはできないし、逆に特約により瑕疵担保責任の期間が短縮されている場合もある」ということだ。

加えて松島氏は引渡しの時点では既知となっていなかった脆弱性について、「瑕疵と評価できるか否かは、意見が割れそうであるし、発注元企業と開発企業との間で脆弱性対策に関する契約上の合意が全くなく、それゆえ対価が安価に設定されている場合、開発企業は、脆弱性対策は作業の対象外であるから瑕疵に該当しないと反論してくることも考えられる」と指摘する。また、「瑕疵担保責任の期間が満了している場合、不法行為責任を検討することになるが、この場合には、故意・過失の立証まで必要となり、事件発生時に既知となっていなかった脆弱性については、故意・過失が否定される場合もあるのではないかと考えられる」と述べる。



松島淳也弁護士

脆弱性の見過ごしも発注元企業に責任

さらに発注元企業が脆弱性を見過ごした場合は、より大きな非難を受ける可能性が高い。例えば納入したWebアプリケーション開発に脆弱性が潜むことを開発企業が発見し、発注元企業に報告していたにもかかわらず、発注元企業がそれを見過ごしてセキュリティインシデントが発生した場合、「知っていて脆弱性を放置したのであれば、発注元企業はなおさら非難されるだろう」と松島氏は話す。この場合、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と規定する個人情報保護法第20条に違反しているものと考えられる。

予算の都合などでセキュリティ対策に腰が重い企業は多い。そのような企業の常套句は「一度セキュリティインシデントが発覚すると予算が付くのだが……」だ。しかし、松島氏は、「1回失敗しないと対策ができないというのはおかしい」と企業に警鐘を鳴らす。

発注元企業は、脆弱性について、開発企業に任せておけば、開発企業がすべて問題なく対応できるはずと考えているかもしれないが、それでは抜本的な解決にならない。脆弱性に基づく個人情報等の漏えい事故を防止するためには、発注元企業側も発注段階からセキュリティ要件として脆弱性対策を盛り込むべきであるし、開発が終了した後も、開発企業との運用・保守に関する契約の中で、脆弱性対策に関する取り決めをすべきである。

求められるWAFによる安全性の底上げ

松島氏は「個人情報が漏えいした場合、会員に対して500円～1000円程度の商品券などを配布する企業があるが、個人情報の数を掛け合わせると多額の出費になる。セキュリティ対策によって、情報漏えい事故が予防できるのであれば、セキュリティ対策に費用を投じた方が効果的。また、セキュリティ対策をどの程度講じていたのかという点は、その企業の信用にも関わる。十分な対策を講じていた場合と、全く対策を講じていなかった場合では、世間の受け止め方も異なってくるだろう。個人情報を大量に保有している企業であれば、セキュリティ対策は当然すべき」と強調する。

松島氏の話から分かるのは、発注元企業が脆弱性を放置したことによる信頼の失墜や、多額のコスト発生というリスクと、それに対するセキュリティ対策の重要性だ。Webアプリケーションの開発元企業は自らが主導し、セキュリティ対策を行う必要があるといえるだろう。セキュリティ対策はさまざまな方法があるが、特にWebアプリケーションの保護に欠かせないのはWebアプリケーションファイアウォールだ。

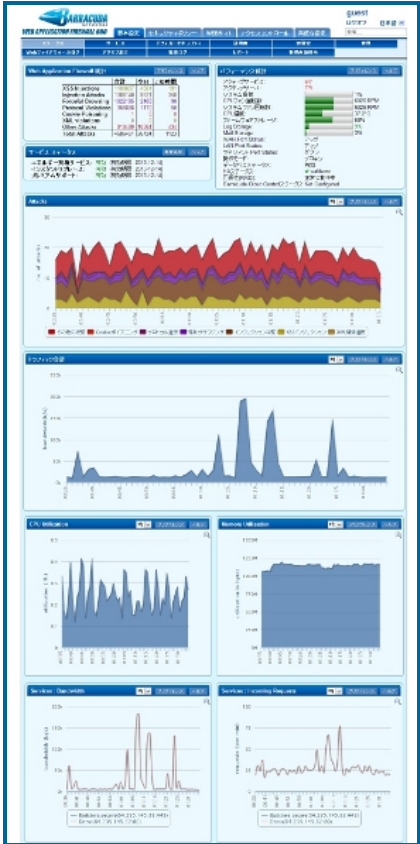
WAFとはその名の通りWebアプリケーションの保護を目的に導入するセキュリティソリューション。Webサーバで発生する通信を監視し、外部からの攻撃など不正な通信をブロックする。WAFは多くの製品が市場に出ているが、その中で注目されているのが

「Barracuda Web Application Firewall（以下、Barracuda WAF）」だ。



Barracuda Web Application Firewall

Barracuda WAFは、アプリケーションレイヤーへの攻撃はもちろんのこと、IPレピュテーションによるDDoS攻撃防止、ユーザーアクセス制御、データ盗難防止機能などを備えた総合的なWAFアプライアンスだ。自動アップデートで新種の脅威に常時対応するので、最新の防御が期待できる。



Barracuda WAFの管理GUI画面。公開されているWebサイトには、日々SQLインジェクションなどの攻撃が押し寄せていることが分かる。多くの企業にとって脆弱性攻撃はもはや対岸の火事ではない《クリックで拡大》

SSLオフロードや負荷分散などで高速処理をバックアップするので、ネットワークのパフォーマンス低下を心配する必要はない。また、設定はテンプレートや直感的なWebインタフェースを活用して簡単に行える。

Webアプリケーション開発の発注元企業にとって法的なリスクは決して無視できない。WAFによる脆弱性対策の強化で、セキュリティの底上げが必要だ。

提供：バラクーダネットワークスジャパン株式会社
アイティメディア営業企画／制作：TechTarget編集部

- ログイン
- 会員登録
- パスワード再設定
- よくあるご質問
- TechTargetジャパンとは
- お問い合わせ
- 広告掲載について
- サイトマップ
- 初めての方

ITインフラ

- クラウド
- 仮想化
- サーバ&ストレージ
- スマートモバイル
- ネットワーク
- システム運用管理

業務アプリ

- ERP
- データ分析

経営

- 経営とIT
- 中堅・中小企業とIT

開発

- システム開発

セキュリティ

- セキュリティ

医療

- 医療IT

☐ ホワイトペーパー／カタログのみ

TechTargetサービス

- ホワイトペーパー
- ホワイトペーパーキーワード

<div>IT総合</div> <div>ITmedia 総合TOP ITmedia ニュース ITmedia News スマート ITmedia Keywords ONETOPI 質問！ITmedia zenbackキーワードズ</div>	<div>デジタル・ガジェット</div> <div>ITmedia Mobile ITmedia PC USER ITmedia LifeStyle デジカメプラス eBook USER ガジェット ITmedia Shopping ITmedia Store ITmedia Store × 楽天市場 ITmedia Store × Yahoo!ショッピング</div>	<div>ビジネス</div> <div>Business Media 誠 誠 Biz.ID 誠 Style 誠ブログ ITmedia プロモバ ITmedia エグゼクティブ ITmedia PC USER SOHO IFRS フォーラム</div>	<div>カルチャー</div> <div>ねとらぼ ライブガイド</div>	<div>アプリ</div> <div>ITmedia for iPhone/iPad ITmedia for Android ONETOPI ライブガイド (β) Biz誠 for iPhone Biz誠 for Android ITmedia エンタープライズ ねこらぼ ついとピ！</div>
<div>企業IT</div> <div>ITmedia エンタープライズ 情報システム用語事典 オルタナティブ・ブログ TechTargetジャパン ホワイトペーパー スマートジャパン ITmedia マーケティング マーケター通信 調査のチカラ</div>	<div>テクノロジー</div> <div>@IT総合TOP QA@IT イベントカレンダー+ログ</div>	<div>エンジニアリング</div> <div>MONOist EE Times Japan EDN Japan モノづくりライブラリ</div>	<div>キャリア</div> <div>@IT自分戦略研究所 エンジニアライフ</div>	