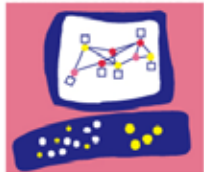


Check Point
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

Webセキュリティ FAQ

2004年5月

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社



Intelligent Security



We Secure the Internet.

Web セキュリティ FAQ



一般的なFAQ

1. 今回、チェック・ポイントは何を発表したのですか。

チェック・ポイントは、既に発表済みのWebセキュリティ戦略を実行するためのいくつかの新製品および技術について発表を行いました。

- **Connectra™** は、安全なリモート・アクセスを実現する為のWebセキュリティ・ゲートウェイです。Connectraはチェック・ポイントのアプライアンスです。
- **Web Intelligence™** は、Connectraに統合されるウェブ・アプリケーション・ファイアウォール技術で、VPN-1™ Pro及びVPN-1 Expressへの追加オプションとしても利用可能です。
- **SSL Network Extender** は、ソフトウェアをインストールすることなく、SSL による最大限のネットワーク・レベル・アクセスを提供する WEB ブラウザのためのプラグ・インです。SSL Network Extender は Connectra に組み込み済みで、VPN-1 Pro 及び VPN-1 Express に追加可能なオプションです。

2. 製品はいつから利用可能でしょうか。

チェック・ポイントのWebセキュリティ製品は既に発注可能です。

- VPN-1 用の Web Intelligence は 2004 年 5 月出荷開始予定です。また、Web Intelligence は、VPN-1 Pro および VPN-1 Express リリース・バージョン R55W と共に出荷されます。
- Connectra は 2004 年 6 月出荷開始予定です。Web Intelligence は Connectra に含まれ出荷されます。
- SSL Network Extender は 2004 年 7 月に出荷開始予定です。

3. 既にファイアウォールを導入していますが、なぜ更にWebセキュリティが必要なのですか？

チェック・ポイントのWeb Intelligenceは、ウェブ・アプリケーションおよびウェブ・インフラ活用する組織のために設計されています。Web Intelligenceは、ウェブ・アプリケーションに対する確実且つ効果的な保護を実現することを特に目的としています。チェック・ポイントConnectraおよびSSL Network Extenderは、ウェブ上でのセキュアな連携を必要とする組織のために設計されています。一般に、WEBやWEBアプリケーションを活用する企業やネットワークは、より高度なWebセキュリティが必要です。

4. 統合Webセキュリティソリューション対応製品がOPSECパートナーよりリリースされる予定はありますか。

いくつかのOPSECパートナーは既にチェック・ポイントのWebセキュリティ製品をサポートしています：RSA、Citrix、VeriSign、Computer Associates、Layer N、およびKey Computingよりリリースされています。



We Secure the Internet.

Web セキュリティ FAQ



Web Intelligence 製品に関する FAQ

1. Web Intelligenceとは何ですか。

Web Intelligenceはチェック・ポイント製品用のウェブ・アプリケーション・ファイアウォール技術です。主に以下の機能を提供します。

Malicious Code Protector

チェック・ポイントが特許出願中のバッファ・オーバーフローによる攻撃およびトラフィック中の悪意のあるコードを効果的に検出する技術。

Advanced Streaming Inspection

INSPECT™アーキテクチャによる検査およびパケットを再構成し検査する能力を拡張し、生のトラフィック・ストリームに対するトラフィック・コントロール機能を追加。

簡単な導入と管理

複雑なチューニングおよび難しい設定を行うことなくウェブサーバを確実に保護。

既存チェック・ポイント製品とシームレスな統合

チェック・ポイント製品とのシームレスな統合により、ウェブ環境全体に保護を実現します。

2. Web IntelligenceとApplication Intelligenceの違いは何ですか。

チェック・ポイントのFireWall-1およびSmartDefenseへ緊密に統合されたApplication Intelligenceはアプリケーション・レベルに対する攻撃を検知し防御します。Web Intelligenceは、ウェブ環境に特化した更なる防御手段を提供します。

- Malicious Code Protector
- SQL Injection
- Command Injection
- 段階的に設定可能なHTTPフォーマット・サイズ
- 段階的に許可できるHTTPメソッド
- HTTPヘッダ・スプーフィング

3. 現在SmartDefenseをあるウェブの保護に使用していますが、それらの機能はR55Wへのアップグレードにより無くなってしまおうのですか。

いいえ。SmartDefenseに含まれる既存のWebセキュリティ機能は、ソフトウェア・サブスクリプションが有効な顧客であれば、追加コストなしにR55Wにおいて引き続き利用可能です。Web Intelligence機能は、GUIに新たに追加された「Web Intelligence」タブより利用可能です。

4. 既にWEBサーバを防御する為にIDS/IPSソリューションを導入していますが、Web Intelligenceは必要ですか。

Web Intelligenceは、特にウェブ・アプリケーションおよびウェブ環境に特化して設計されています。IDS/IPSソリューションは、ウェブの防御はできますが、あくまでも一般的な防御しかできないので、チェック・ポイントのWeb Intelligenceが提供できる様々なウェブ・アプリケーションに特化した多くの防御は行えません。



5. Malicious Code Protectorとは何ですか。

チェック・ポイントのMalicious Code Protectorは、バッファ・オーバーフロー攻撃および悪意のあるコードを検出する為の特許出願中の技術です。 Malicious Code Protectorは、他の製品とは異なりパターン・ファイルやシグネチャを必要とせずに防御を提供する革新的な機能を提供します。

Malicious Code Protectorは、ウェブ通信内に含まれる悪意のある実行可能なコードを識別し、検知するだけでなく、悪意のある振る舞いを実行する可能性のあるコードをデータ・ストリームより識別及び検出します。 Malicious Code Protectorはカーネルベースでの防御を行っているため、ワイヤ・スピードの性能を実現できます。

6. Malicious Code ProtectorはWeb Intelligenceにおいてのみ利用可能なのですか、SmartDefenseのような他の製品はどうですか。

現在、Malicious Code Protectorはウェブ・アプリケーションにのみ利用可能ですが、同技術は、他製品でも同様にアプリケーション防御を行う為に利用可能です。

7. Web Intelligenceは、VPN-1ゲートウェイの性能に影響を与えますか。

Web Intelligenceは、VPN-1 ProおよびVPN-1 Expressゲートウェイに若干の性能影響を与えます。 Malicious Code Protectorを使用した場合5～10パーセントの影響、Active Streamingを使用した場合、10～20パーセントの影響。 Malicious Code ProtectorおよびActive Streamingを併用した場合、20～30%の影響を与えます。

8. Web Intelligenceはどのプラットフォームをサポートしますか。

VPN-1 ProおよびVPN-1 ExpressでWeb Intelligenceを使用する場合、Application Intelligence R55Wが必要です。 R55Wは、SecurePlatform、Linux、SolarisおよびWindowsを含むVPN-1ゲートウェイがサポートするプラットフォームをすべてサポートします。 ノキアIPSOは5月末日までにサポートされる予定です。

Web IntelligenceはConnectraにも含まれており、2004年Q4を目処にInterSpectへ統合される予定です。

9. Web Intelligenceは、いつからノキア・プラットフォームで利用可能でしょうか。

Web Intelligenceは、2004年5月末頃にはIPSO 3.7および3.71で利用可能になります。 現在、IPSO 3.8でWeb Intelligenceをサポートする予定はありません。

10. どのような場合R55WまたはR55を使用すべきですか。

R55Wは、Web Intelligenceを必要とするか、DNSセキュリティ機能あるいはピア・ツー・ピアセキュリティ機能などSmartDefenseが新たにサポートした保護機能を使用する必要があります。

R55は、Web Intelligenceあるいは特定のSmartDefense保護を必要としない顧客が使用します。



We Secure the Internet.

Web セキュリティ FAQ



11. Web Intelligenceはどのように管理できますか。

Web Intelligenceは、現在SmartCenterから管理が可能で、将来的にはProvider-1による管理にも対応予定です。管理者は、単一の管理コンソールよりファイアウォール・ポリシー、SmartDefenseおよびWeb Intelligenceに関する設定を行えます。Web Intelligenceに関するログは、単一の管理サーバへ集約し他のチェック・ポイント製品のログと結合し、分析を行うことが可能です。

12. Web Intelligenceはハイ・アベイラビリティをサポートしますか。

はい。Web Intelligenceはチェック・ポイントClusterXLと統合が可能です。また、VRRPおよび他の外部クラスタリング技術と連携することも可能です。



We Secure the Internet.

Web セキュリティ FAQ



Connectra 製品に関する FAQ

1. Connectraとは何ですか。

Connectraは安全なリモート・アクセスを実現するためのWebセキュリティ・ゲートウェイです。Connectraは主に以下の機能を提供します。

安全なウェブ・ベースのコネクティビティ

ウェブ環境全体のセキュリティを向上するための、SSL VPNウェブおよびネットワーク・レベルのアクセス方法を提供します。

統合サーバ・セキュリティ

チェック・ポイントのステートフル・インスペクション、Application IntelligenceおよびWeb Intelligenceによる、強力なサーバ保護を実現します。

適応性のあるエンド・ポイントセキュリティ

スパイウェア、完全性および柔軟性のあるアクセス保護を様々なアクセス・ニーズに適応します。

ワン・クリックのSSLリモート・アクセス

ユーザ・ポータルおよびSSL Network Extenderにより内部のサーバやネットワーク・インフラストラクチャを変更せずに、内部サーバをSSL対応にします。

2. IPSecによるリモート・アクセスとSSL VPNは何が異なるのですか。

IPSec VPN および SSL VPN はそれぞれ異なるプロトコルを使用します。また、各ソリューションはそれぞれ利点、欠点があります。一般的に、IPSec VPN は、エンド・ポイントのデバイス上にリモートアクセス・クライアントが必要ですが、SSL VPN はリモートアクセス・クライアントとしてSSLに対応したWEB ブラウザを使用します。詳細については、技術白書「リモート・アクセスに関するIPSecとクライアント・レスVPNの比較」をご覧ください。

3. なぜSSL VPNが必要なのですか。

SSL VPNが必要かどうかは導入する環境に依存します。一般的に、SSL VPNは、クライアント・レスによるリモート・アクセスを必要とする企業が導入します。詳細については、技術白書「リモート・アクセスに関するIPSecとクライアント・レスVPNの比較」をご覧ください。

4. SSL VPNはIPSec VPNと同レベルのセキュリティですか。

SSLやIPSecなどのVPNは本質的な意味でのセキュリティではありませんので、SSLおよびIPSec VPNは、より安全にするために統合エンド・ポイントおよびゲートウェイが統合されたセキュリティの能力が必要です。チェック・ポイントは、エンド・ポイントおよびゲートウェイ・セキュリティを兼ね備えたIP Sec VPNを創出したです。また、SSL VPNは、チェック・ポイントが企業に求められる高度なセキュリティ要件を満たす製品をはじめ提供するベンダーです。

5. サイト間VPN用のゲートウェイとしてConnectraを使用することができますか。

Connectraは、ウェブ・ベースのリモート・アクセス専用設計されたので、サイト間VPNを行うためのゲートウェイとしては利用できません。 サイト間VPNが必要な場合には、チェック・ポイントVPN-1を使用してください。

6. Connectraはファイアウォール機能が付属しますか。 SmartDefenseとWeb Intelligenceは付属しますか。

Connectraは、ウェブ・ベースのテクノロジーを利用しリモート・ユーザと安全な接続を行うことに特化したWebセキュリティ・ゲートウェイで、汎用のファイアウォールとは異なる機能を提供します。優れた接続性に加えConnectraは、ユーザやアプリケーションに対するアクセス・コントロール、またWEBトラフィックのためのWeb Intelligenceを含む複数のレベルの保護を提供します。このような統合可能なセキュリティにより、境界セキュリティに影響を与えることなく、既存ファイアウォールと統合することが可能です。

7. Connectraはどのプラットフォームで利用可能ですか。

Connectraはチェック・ポイント・アプライアンスとしてのみ利用可能です。 Connectraアプライアンスは、DELL社と共同開発されました。

8. Connectraにはどのような機種がありますか。

Connectra モデル	ターゲット顧客	ユーザ・ライセンス・ オプション	追加オプション
Connectra 1000	中規模環境	50、100、250	エンド・ポイント・セキュリティ
Connectra 2000	中～エンタープライズ 環境	100、250、無制限	エンド・ポイント・セキュリティおよび電源 二重化
Connectra 6000	エンタープライズ～ハ イエンド環境	250、500、無制限	エンド・ポイント・セキュリティ(6000は SSLアクセラレーション及び二重化電源 を含む)

9. ConnectraがサポートしているOSプラットフォームは何ですか。

Connectraはチェック・ポイントがセキュリティ・チューニングを施したセキュアなオペレーティング・システムであるSecurePlatform™に対応しています。

10. Connectraはどのように管理を行えますか。

Connectraは、チェック・ポイントのSMARTアーキテクチャに基づいたWebベースのGUIによるローカル管理に対応しています。 Connectraを管理するための独立した管理システムは必要ありません。また、ConnectraのログはSmartView™ Trackerで確認することが可能です。



Web セキュリティ FAQ



11. Connectraは、ネットワークに対しどのような導入が行えますか。

一般的な環境であれば、ConnectraはDMZに配置します。先進のアクセス・コントロールおよび攻撃に対する確実な防御を可能にするセキュアなプラットフォームであるConnectraは、境界ファイアウォールの前、又は後ろにも設置することができます。

12. Connectraはハイ・アベイラビリティをサポートしますか。

Connectra 1.0でハイ・アベイラビリティを構成する場合には、個別に設定を行った2台以上の機器構成によりHAをサポートします。今後、より高度なHA構成に対応予定です。

13. ユーザがアクセスできるネットワーク・リソースを制御することは可能ですか。

Connectraの管理インターフェースは、管理者が個々のアプリケーション、ウェブ・リンクおよびファイル共有などに関する定義を行えます。ネットワーク・ユーザは、管理者によりアクセス権限を明示的に与えられているネットワーク・リソースのみアクセスすることが可能です。また、各ネットワーク・リソースは管理者があらかじめ設定したセキュリティ感度のレベルが定義されます。ユーザは、エンド・ポイントに対し定義されたセキュリティ・レベルや状況に応じ、明示的に許可されたリソースへのアクセス権限が与えられます。

14. ConnectraはRSA SecureIDと連携できますか。

はい、ConnectraはSecureIDを使用するためのACEサーバと通信することができます。さらに、管理者はSecureIDを使用しユーザ認証が行われた場合にのみアクセスできるリソースを定義することができます。

15. チェック・ポイントは、どのようにエンド・ポイントに対するセキュリティに取り組みますか。

Connectraは、エンド・ポイント・セキュリティにおけるマーケット・リーダーであるZone Labsにより開発されたエンド・ポイント・セキュリティとのインテグレーションを提供する予定です。Connectraは、エンド・ポイントでのスパイウェア、キー・ストローク・ロガー、およびハッキング・ツール等を検査することができるようになります。さらに、Connectraは、エンド・ポイントのセキュリティ・レベルに応じた、ダイナミックなリソースへのアクセス・コントロールが行えます。例えば、セキュリティ・ポリシーとして、エンド・ポイント検査に適合し、トークンによる認証を行ったユーザのみあるリソースに対しアクセス権を与えるよう設定することが可能です。

16. Connectraはどのようなブラウザをサポートしますか。

Connectraは、Internet Explorer バージョン5.5又はそれ以降のバージョン、Mozilla、SafariおよびNetScapeに対応しています。Connectraの管理は、Internet Explorer バージョン5.5又はそれ以降のバージョンをサポートします。

17. Connectra はPDAや携帯電話による接続をサポートしますか。

ConnectraはSSL対応のブラウザによってのみ接続することができます。PDAや携帯電話による接続は、エンド・ポイントの機器が対応するウェブ・ブラウザに依存します。



We Secure the Internet.

Web セキュリティ FAQ



SSL Network Extenderに関するFAQ

1. SSL Network Extenderとは何ですか。

SSL Network Extenderは、WEBブラウザ向けのプラグ・インで、ソフトウェアをインストールする必要なしに、SSLによる最大限のネットワーク・レベル・アクセスを提供します。SSL Network ExtenderはConnectraに組み込み済みです。またVPN-1 ProおよびVPN-1 Expressに追加することも可能です。

2. SSLによる接続を行う場合には、SSL Network Extenderが必要なのですか。

いいえ、SSL Network Extenderは、クライアント/サーバ型のアプリケーションにSSL VPNによる接続性を提供します。ウェブ、電子メールおよびファイル共有については、SSL対応ウェブ・ブラウザで、Connectraに付属するウェブ・ポータル経由でアクセスが可能です。

3. SSL Network Extenderはどのチェック・ポイント製品と統合することができますか。

SSL Network ExtenderはConnectraに統合されます。また、VPN-1ゲートウェイへの追加オプションとして統合が可能です。

4. SSL Network Extenderはどのようなアプリケーションをサポートしますか。

SSL Network Extenderは、FTPやVoIPに代表される動的なポートを使用するアプリケーション、を含むTCP、UDPアプリケーションをサポートします。SSL Network Extenderを使用するためには、リモートのエンド・ポイント上で、ウェブ・プラグ・インおよび管理者権限が必要です。

5. SSL Network Extenderを使用するためのエンド・ポイントでの要件は何ですか。

SSL Network ExtenderはWindows 2000又はそれ以降のバージョンのOS、及びIE 5.5およびそれ以降のバージョンのWEBブラウザが必要です。



We Secure the Internet.

Web セキュリティ FAQ



Intelligent Security

サポートに関するFAQ

1. Connectraを使用するにあたりUserCenter上でライセンスを生成する必要はありますか。

いいえ。Connectraは、自動的にUserCenterに表示されます。また、すべてのConnectra システムにあらかじめライセンスが与えられており、ライセンスをアクティベートする必要なしに、購入後すぐに使用できます。ただし、Connectra各デバイスに同梱されているSmartDefense 購読サービスを利用するには、User Center でConnectraを登録する必要があります。

2. Connectraに保証期間はありますか。

Connectraは1年のハードウェア保障が付属します。ハードウェア保障は、EBS購入により拡張が可能です。

3. ConnectraのRMAについて教えてください。

InterSpect、VPN-1 EdgeおよびSafe@Officeと同様のRMA処理です。サービスのリクエストおよびRMAプロセスはチェック・ポイントのテクニカル・サービスが行います。RMAに関する詳細は以下のURLをご覧ください。
(<http://www.checkpoint.com/support>)



We Secure the Internet.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail : info@checkpoint.co.jp Tel 03 (5367) 2500

© 2004 Check Point Software Technologies Ltd. All rights reserved.