サイバー・セキュリティ
未知の脅威を阻止

Sophos Authorized Partner

株式会社リナ・システム

LYNA

2020年

Ver.4.1

サイバー攻撃

- 誰もが攻撃対象となる脅威
  - 鉄砲や槍は飛んでこない（目に見えない脅威）
- パソコン、スマホ、タブレット、AIスピーカー、IoT電子機器、電子マネー、クレジットカードへ
- ウィルスや脅迫メール、大量の迷惑メールだけではない
- 日常生活の奥深く潜んで、お金を盗み、盗撮、ばらまき
- 情報がデータとして蓄積され、悪用や別の目的に利用されている

- それに気がついていないだけかもしれません

サイバー攻撃の種類

サイバー攻撃は主にサーバーやパソコン等ネットワークを対象に行われるテロリズムです。

- 攻撃の種類は大別して、
  - データの破壊
  - データの窃取
  - データの改ざん
  - コンピューターウィルスの感染

攻撃を細分化すると（1）

①ブルートフォースアタック

暗号解読方法の一つ。パスワード等を可能な組合わせをすべて試す方法です。例えば4桁の暗証番号があった場合は、0000～9999までの1万通りを試すという原始的な方法。ツールも普及していて試行回数などの制約がない限りは、確実に割り出すことが可能。全ての暗証番号を入力していく方法、人間だと時間と労力が掛かり大変ですが、これをコンピュータで自動的に処理させることで暗証番号を見つけ出します。

②Dos攻撃/DDos攻撃

ウェブサービスに対して、サーバやネットワークなどのリソースに意図的に過剰な負荷をかけたり脆弱性を突いたりすることで、一時閲覧できなくなったりサービスが停止するような攻撃です。「利用中のサイトがいきなり閲覧できなくなった」、レンタルサーバを借りている人は、障害報告によく報告されています。閲覧者側は、利用できないだけで、あまり被害は受けませんが、サイトを運営している側はサービスが停止することになり大きな被害になります。

③SQLインジェクション

アプリケーションのセキュリティ上の不備を意図的に利用し、データベースシステムを不正に操作する攻撃方法のこと。サイト改ざんや個人情報漏洩につながる脅威となる。日本では2005年3月にクラブツーリズムでクレジットカード情報を含む個人情報漏洩が起こり、その後数年にわたり多数の企業がこのSQLインジェクションにより個人情報漏洩の被害にあっています。顧客などのデータは、データベースというところに格納管理されています。一般の人がサービスを利用する際は会員番号などを利用しますが、その番号が正しいかどうかデータベースと照合する必要があります。その際にカード番号が含まれているSQLという命令が発行されます。それを逆手に取った手法です。考えられる会員番号をSQLに含ませてインターネットからデータベースに照合して、顧客情報を盗むという手口です。現在は暗号化などの技術的な対策でSQLインジェクションで漏洩が起こらないような対策をどの企業も必ず行っています。

攻撃を細分化すると（2）

④クロスサイトスクリプティング

他人のウェブサイトへ悪意のあるスクリプトを埋め込む事。掲示板があることが前提条件となります。その掲示板のフォームに悪意のあるスクリプトが埋め込まれ、そのサイトを閲覧したPCがスクリプトを実行してしまうのが一連の流れです。そのスクリプトが実行されてしまうと、例えばクッキー情報の漏洩等が出てきます。クッキー情報は主にログインしたIDやパスワード等が保存されている情報なので漏洩してしまった結果、他人に乗っ取られる可能性があります。ホームページを見た時に、自分のPCに悪意のあるプログラムを忍ばせ情報を盗む手口です。この被害にあわないようにするには、怪しいサイトの閲覧をしないこと、わけのわからないボタンを押さないことです。特に日本語以外の表記サイトでは気をつけて下さい。

⑤ルートキット攻撃（マルウェア）

複数の不正プログラムを合わせたパッケージのようなツール群でPCに侵入すること。侵入してしまったら見つけ出すことが困難で、PCへの侵入口をふさいだとしても再侵入の手助けをする等様々な被害が想定されます。「トロイの木馬」が特に有名です。標的となる管理者権限を奪うことが最大の目的で、その先にはパスワード情報の窃取等が実行されてしまいます。これもホームページを見た時に、自分のPCに浸入してきます。怪しいサイトの閲覧はしないことが被害に合わないになります。

ルートキット攻撃（マルウェア）

◆ ランサムウェア

重要なファイルへのアクセスを出来なくし、金銭の支払いを要求する。悪質なメールの添付ファイルや改ざんされたWebサイトへのアクセスが要因です。

◆ Exploits

エクスプロイトとは、アプリケーション、ネットワークやハードウェアの脆弱性を悪用する攻撃です。攻撃は、コンピュータ システムを意のままにコントロールすることまたはネットワーク上に保存されているデータを盗むことを目的とし、ソフトウェアまたはコードの形態を取ります。SQLインジェクションの進化系。

◆ フィッシング

金融機関などからの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などを詐取する詐欺。

◆ Cryotojacking

Webページに仮想通貨マイニング用のソフトウェアを仕込んでおき、ページを閲覧しにきたユーザが知らないうちに仮想通貨マイニングを行うようにする行為を指す。

サイバー戦争（核兵器はいらない）

- ロシアによるサイバー攻撃
  - 2007年エストニアの政府機関、銀行システムがダウン
  - 2014年ウクライナの国営通信センターが攻撃される
  - 2018年平昌オリンピックでドローンでのハイライトが中止
- 中国によるサイバー攻撃
  - 2015年米国連邦人事管理局から個人情報が大量流出
  - 2015年日本年金機構から152万人の年金個人情報流出
  - 2017年米海軍第7艦隊のイージス艦の相次ぐ事故
- アメリカによるサイバー攻撃
  - 2009年イランの核燃料施設の攻撃
  - 2017年北朝鮮のミサイル打上げ失敗
- 北朝鮮によるサイバー攻撃
  - 2014年米国ソニーピクチューから従業員・家族の個人情報流出
  - 2017年バングラディシュ中央銀行から8100万米ドルを奪う

2020年1月20日朝日新聞1面に掲載
三菱電機にサイバー攻撃
防衛・電力・鉄道情報流出か
中国系組織関与の可能性
管理職の端末標的、開始時期は不明

証拠を示すと、自らの調査能力を知られるので、確固たる証拠は明らかにされていない
よってすべて推測です

日本での大規模サイバー攻撃事件

- 大手旅行会社顧客情報流出事件（2016年）
  - 特定オペレータを狙ったなりすましメール（pdfファイル内のマルウェア）
  - 約4300人分の有効期限中の旅券番号流出
- 日本年金機構情報流出事件（2015年）
  - 学術機関の職員を装った偽メール（添付ファイルにマルウェア）
  - 個人PCへ禁止されていたファイルをコピーして作業
- ベネッセ顧客情報漏洩事件（2014年）
  - 委託会社のシステムエンジニアの情報持出し（名簿売却目的）
  - スマートフォンへコピー
  - 賠償と対策で260億円
- 日本航空ビジネスメール詐欺事件(2017年）
  - 金融機関の担当者を装った偽メールでの振込詐欺（トロイの木馬）
  - 3億6千万円＋2400万円
- コインチェック仮想通貨流出事件（2018年）
  - オフライン（施錠状態）の金庫をオンラインにしていた
  - 約5800億円の仮想通貨が流出（銀行強盗）

NHKで報道された中小企業の事例

- https://www.nhk.or.jp/ohayou/digest/2019/11/1127.html?fbclid=IwAR0OiTsNBtuGVdq78cWSd9qb7Dti9mvs27ELa6VUzBTQIS0a08KL8Gsmz4U

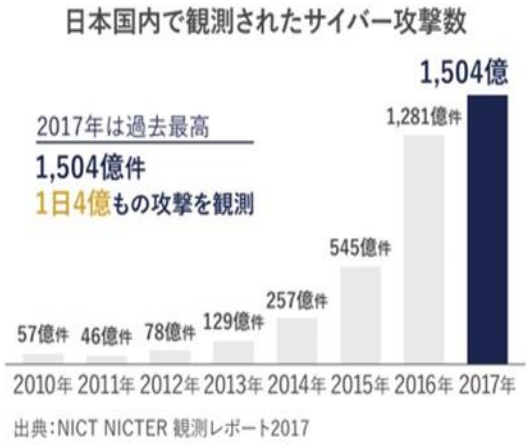
- 従業員14人の中小企業。2018年に会社の根幹を担う販売管理システムが、突如使えなくなる
- 感染したのは「ランサムウェア」
  - システムの復旧と引き換えに、金銭を要求する身代金型。
    中小企業を入り口に、取引先のネットワークを悪用し、大企業までも狙う「サプライチェーン攻撃」
- 中小企業の弱点を突き、盗んだ情報から、取引先になりすますなどして、その中小企業と取り引きのある他の企業のシステムに侵入。
- 被害総額は、約500万円

サイバー攻撃の分類

	無差別型	標的型
対象	個人が多い	企業、金融機関、政府機関、病院、交通機関など
経路	メール、ウェブサイト、外部メディア（USB、CD-ROM等）	
方法	・マルウェアを添付したメールをばらまく ・汚染されたウェブサイトを閲覧させる ・フィッシング（メール送付⇒汚染サイトへ	・偽メール⇒遠隔操作

2017年で

日本国内で観測されたサイバー攻撃数1,504億件



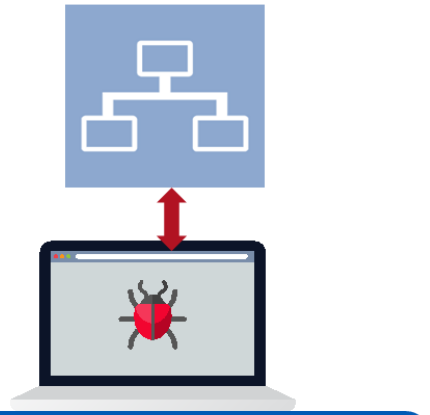
これは2017年のNICT NICTER 観測レポートによるデータで、１日あたり4億件もの攻撃が行われていたことになります。さらに、平成29年度の警察庁発表による「上半期におけるサイバー空間をめぐる脅威の情勢等について」のデータでは、サイバー犯罪の相談件数だけで7万件。同年の不正アクセス行為の認知件数は1,202件で、内訳を見ると一般企業が1,177件と最多。企業にとっては、機密情報の改ざんや漏えい、不正送金など、死活問題に発展してるのが現状です。

経営者がやらなければならない重要10項目

リーダシップの表明と体制の構築	1	**サイバーセキュリティリスクの認識 組織全体での対応の策定**
	2	サイバーセキュリティ管理体制の構築
リスク管理の枠組み決定	3	リスクの把握と対応計画の策定
	4	PDCAサイクルの実施と対策状況の開示
	5	系列企業・ビジネスパートナーの対策実施及び状況把握
攻撃を防ぐための事前対策	6	予算確保・人材配置及び育成
	7	ITシステム管理の外部委託
	8	情報収集と情報共有
攻撃を受けた場合に備えた準備	9	緊急時対応体制の整備とトレーニングの実施
	10	被害発覚後の必要な情報の把握、開示体制の整備

東京都産業労働局商工部調整課発行「サイバーセキュリティ対策の極意」より抜粋

侵入ポイント



ネットワーク

システムの脆弱性を狙って、ネットワークを通じて感染

ネットワーキングの仕組みの脆弱性を狙って、悪質プログラムを実行

Wanna、Petya の手口

メール

スパムやフィッシングメールによって感染

Office の文書ファイル、PDF、実行ファイルなどの添付ファイルを開くように仕向け、エクスプロイトキットや悪質プログラムをダウンロード

Locky、TorrentLocker の手口

Web

不正サイトへのアクセスや、悪質広告、ダウンロードを通じて感染

メールの例と同じような手口で悪質ファイルがダウンロードされたり、不正サイトに誘導され、エクスプロイトキットがドライブバイダウンロードされる

CryptoWall、TeslaCrypt の手口

攻撃手順

【有効な対策 】
・Web
プロテクション
・メールプロテクション

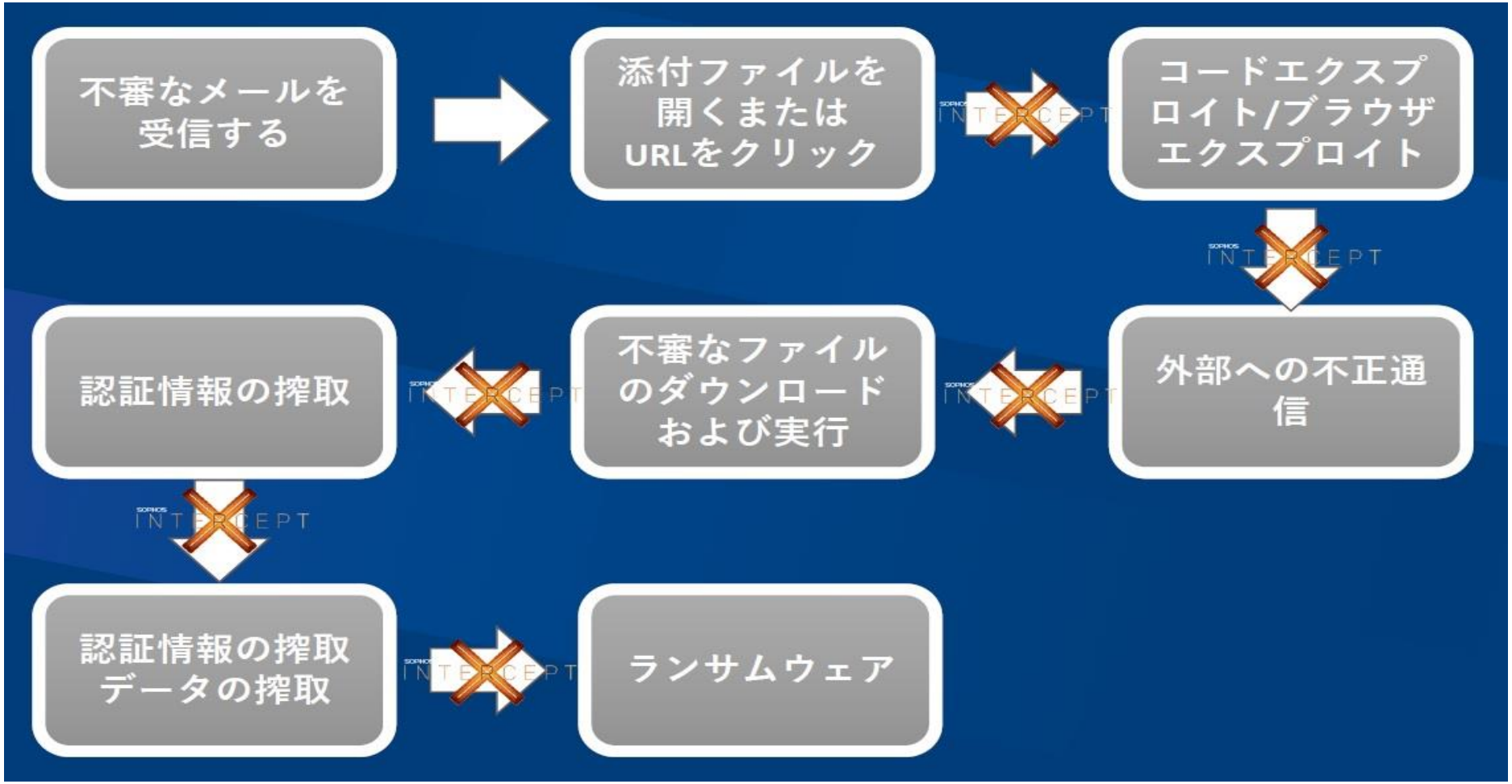
【有効な対策 】
・エクスプロイト対策
(コード メモリ 他)
・アプリケーション
ロックダウン
・アプリケーション
コントロール

【有効な対策 】
・人工知能
(DEEPLEARNING 型 AI)
・HIPS
(振る舞い検知
解析)

【有効な対策 】
・MALICIOUS
TRAFFIC
DETECTION
(不正な通信を検知)

【有効な対策 】
・アンチランサムウェア
・認証情報搾取対策
・動的解析型振る舞い
検知
・根本原因解析

負の連鎖を断ち切ることが超重要



ポイント製品では不十分
既存のルータ、ウイルスソフトでは防ぎきれない

- 1つのシステムとして機能するサイバー脅威
- サイバー犯罪者は、1つの手法やテクノロジーを用いるのではなく、複数の手法を組み合わせた組織的システムで攻撃を行います。
- たとえば、攻撃者は悪意のある URL を含むフィッシングメールで攻撃を開始するかもしれません。メールを受信したユーザーがリンクをクリックすると、C＆C (コマンド＆コントロール) センターに接続されてしまいます。そこで攻撃者は、認証情報の窃取、権限昇格、悪意のある実行ファイルといった手法を組み合わせて、ユーザーの情報を盗み出したり、情報を引き換えに「身代金」を要求したりして、最終目標を遂行するといった具合です。

ウィルスソフトだけでは不十分

	一般的なウィルスソフト	Sophos社製FirewallXG
ネットワークの侵入・保護	×	◎
なりすましメール	×	○
脆弱（ぜいじゃく）性への攻撃	△	○
DDos攻撃（集中砲火）	×	○
アカウント乗っ取り	×	○
フィッシング詐欺	△	○
ワンクリック詐欺	×	○
未知のウィルス	×	◎
外部媒体の管理（USBメモリなど）	×	管理
迷惑メール	ブロック	ブロックと送信

サイバーセキュリティ対策

入出管理

マルウェアの侵入を防ぐ
①メール対策
②ウェブ・ブラウザ対策
③外部メディア対策

事後対策

①運用監視
⇒情報通信記録(ログ)の蓄積
②事後対応
⇒原因・犯人の追跡
⇒被害後の対応支援

マルウェアを検出

- 「パターンマッチング方式」　・・・指名手配犯を捜す
  - シグニチャー（署名）を照合
- 「レピュテーション方式」　　・・・前科者を疑え
  - グレーゾーンのファイルの安全性を見極める
- 「サンドボックス方式」　　・・・不審者を泳がせ監視する
  - 隔離エリアに格納し、一定時間監視する
- 「振舞検知方式」　　・・・不審者を尾行する
  - 異常な行動パターンをするファイルを排除する

未知の脅威を阻止するために

◆ 英国Sophos社の次世代型ファイアウォール製品の導入を推奨

- Sophos社

  1985年に英国アビンドンに設立（従業員約3,000名）、1997年から日本での販売開始（従業員約80名）。

  主な日本での顧客：岩波書店、講談社、芝浦工業大学、東京大学、早稲田大学、朝日新聞社、伊那市、豊川市など官公庁、地方自治体、銀行、大学、自動車メーカー、電機メーカーなど。

- 製品名：XG Firewall

  UTM：Unified Threat Management 】統合脅威管理

  アプライアンス：特化したコンピュータ

XG Firewall を推奨する理由

- 最新の保護機能の数々が備わっていて、設定・管理が簡単
- 不正システムを一目で把握し、自動隔離できる
- アプリケーションやユーザのリスクをこれまでにないレベルで詳しく把握できるレポート機能を搭載

- ファイアウォールのルールやポリシーのオプションがすべて一箇所にまとめられ、わかりやすい
- 評価機関（NSS Labs、Gartner など）や業界の専門家から、保護機能、パフォーマンス、価格のすべてにおいて高い評価

状況をわかりやすく視覚化、簡単にセキュリティ対応

- 隠れたリスクを顕在化
  - 危険なアクティビティ、疑わしいトラフィック、高度な脅威を分かりやすく表示し、ネトワークを適切に制御
- 未知の脅威を阻止
  - ディープラーニング（AI)や侵入防止システムである次世代型の強力な保護テクノロジーによって組織を保護
- 感染したシステムを隔離
  - 脅威への自動対応機能によって、ネットワーク上の感染したシステムを即座に隔離し、脅威の拡散を阻止

未知の脅威を阻止

- 基本的な保護機能を確実に導入する
- 攻撃の侵入口を減らす
- 開かれたポートを適切に保護する
- Web やメールトラフィックにサンドボックスを適用する
- ネットワークを通じた感染拡大のリスクを最小化する
- 感染システムを自動的に隔離する

高性能のハードウェアアプライアンス

- 業界トップレベルの価格、柔軟性、接続性、信頼性を兼ね備える

- 専用設計で高性能
  - 全機種に、最新のIntelマルチプロセッサ、十分な容量のRAM，SSD（ディスク）を装備
- 柔軟な接続オプションでネットワークの接続要件に一致
  - Wi-Fi、3G/4G、DSL、最高40GEまでのcopper/fiberオションなど、あらゆる業種や規模の組織に対応、総合型/モジュール型と接続オプションを提供
- ビジネス継続性
  - 導入オプション及び電源とディスクの2重化で、万が一の障害でも継続使用可能

包括的な次世代セキュリティ対策

- セキュリティ対策とコンプライアンス遵守に不可欠
  - 高度なネットワーク機能、保護機能、ユーザ、アプリケーションの制御

管理	ファイアウォール管理機能	集中管理機能	ステータスと警告	レポートとログ
ユーザとアプリの制御	ユーザ識別	アプリケーションコントロール	Webコントロール	コンテンツ制御
保護機能	ファイアウォールとIPS	クラウド型サンドボックス	マルウェア対策 業務アプリケーション	Webプロテクション メールとデータ
ネットワーク	ルーティングとブリッジ パフォーマンス	ゾーンのセグメント化 VPN	トラフィックシェービング RED VPN	ワイヤレスコントローラ 暗号化されたトラフック

セキュリティ、使いやすさ、解析力のすべてに優れた製品

隠れたリスクを顕在化

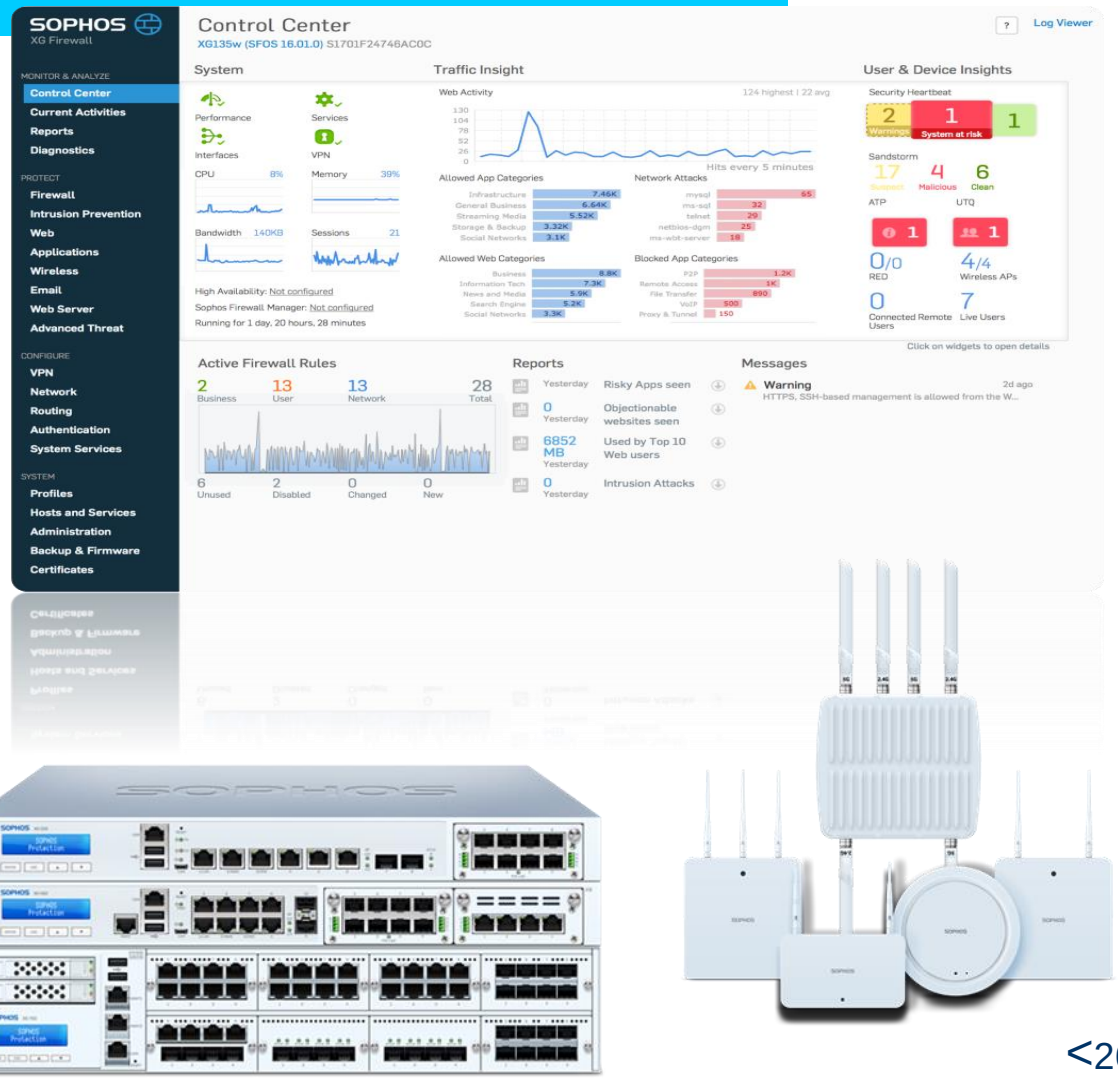
- ✓アプリ、ユーザー、悪質プログラム、脅威
- ✓見やすく色分けされたダッシュボード
- ✓豊富なレポート機能を搭載
- ✓問題を先回りして阻止

ネットワーク脅威をブロック

- ✓多様な保護機能
- ✓IPS、APT、サンドボックス
- ✓Web コントロールとアプリケーションコントロール
- ✓単一画面から簡単に管理

インシデントへの自動対応

- ✓独自技術の Security Heartbeat™
- ✓エンドポイントのセキュリティ状態をルールに反映
- ✓感染システムをすばやく特定
- ✓感染システムを自動的に隔離



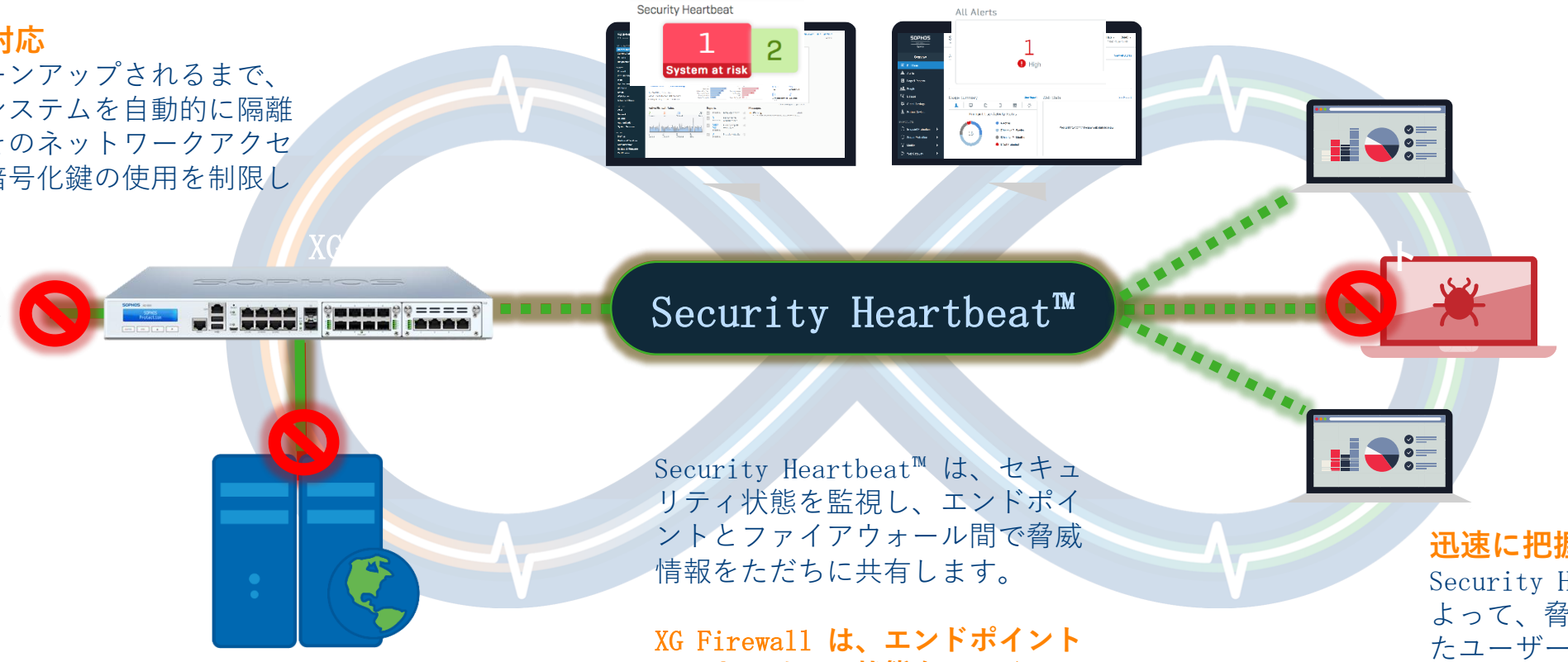
設置方法

ファイアウォール/ルータの置換え

インライン
（逆も可）

Synchronized Security – 自動対応

自動対応
クリーンアップされるまで、感染システムを自動的に隔離し、そのネットワークアクセスや暗号化鍵の使用を制限します



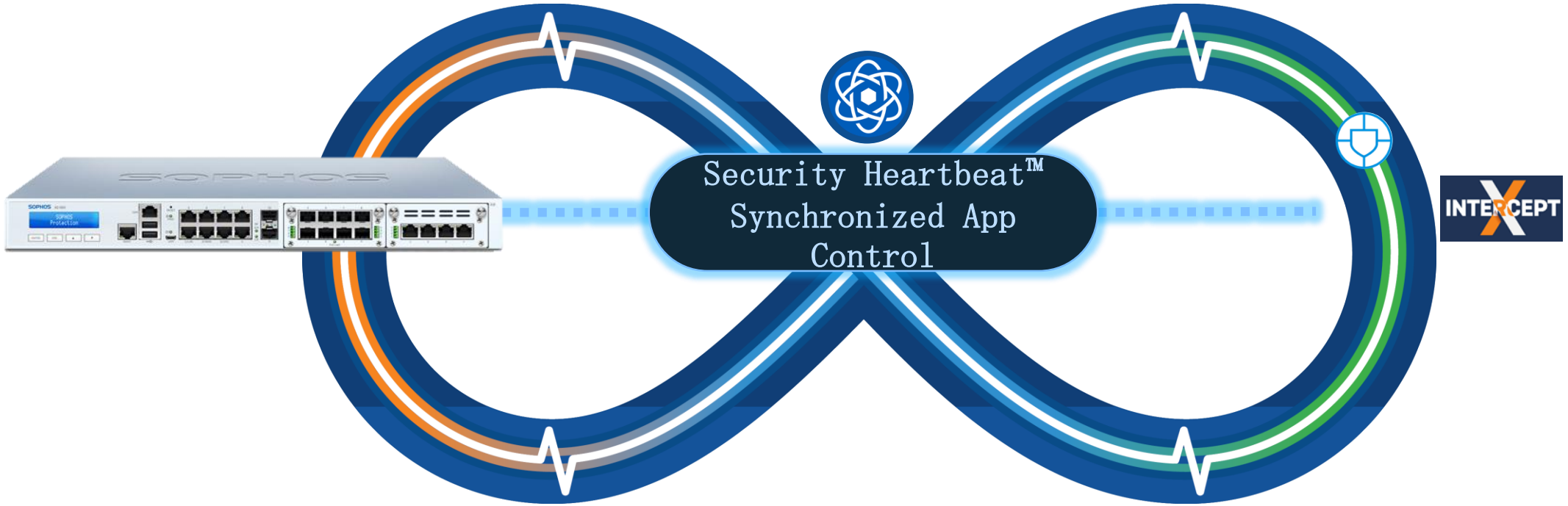
Security Heartbeat™ は、セキュリティ状態を監視し、エンドポイントとファイアウォール間で脅威情報をただちに共有します。

XG Firewall は、エンドポイントのセキュリティ状態をファイアウォールルールに含めることができる唯一のファイアウォール製品です。

迅速に把握
Security Heartbeat によって、脅威の影響を受けたユーザー、システム、プロセスなどの情報を即時に収集・共有します

究極のコンビネーション

◆ 最新のランサムウェアや高度な脅威から保護



比較

XEROX社製品と比較：従業員20名

XEROX		SOPHOS	
Beatbox Firewall、リモート接続、 報告書		XG115	119.000
リモートアクセス・VPN	1,101,600	ライセンス＋保守	107,000
Virusソフト（トレンド）	300,000	Virusソフト InterceptX	316,800
3年間概算	1,401,600		542,800
1年間概算	467,200 （513,920）		181,000

（当社調べ）

中小企業向けモデル

概算価格、使用状況と実際のPC数によってお見積いたします

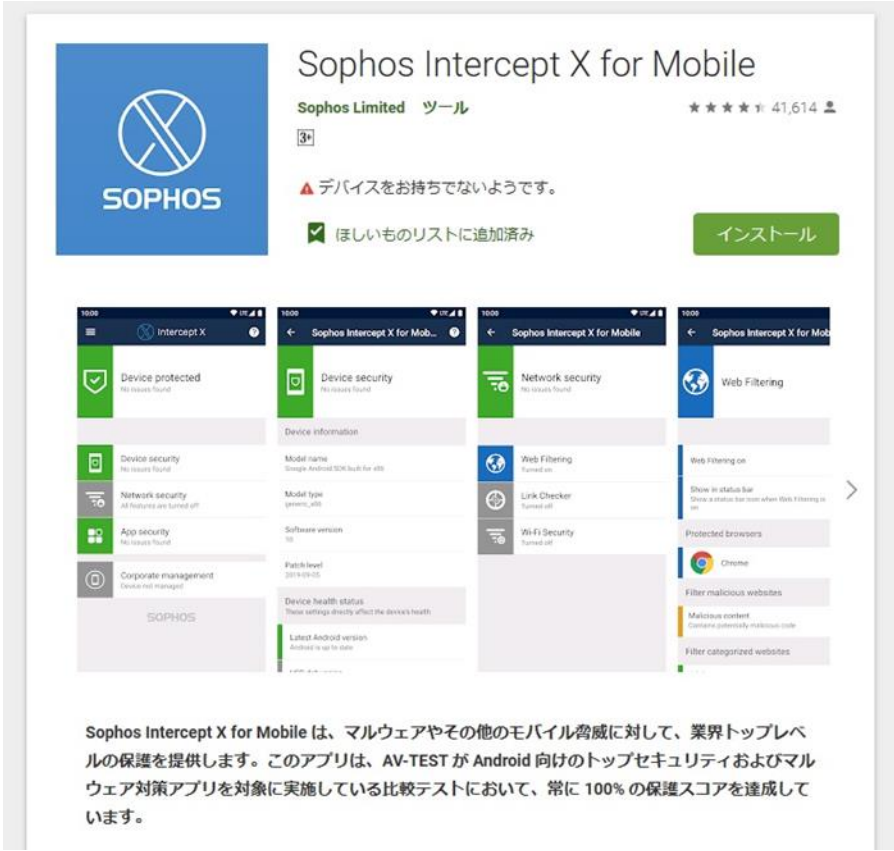
ユーザ数	モデル	アプライアンス価格	ライセンス＋保守	Virusソフト	3年間合計	2年延長
5名程度	XG86	70,000	48,800	16,780x5	202,700	32,400
10名程度	XG106	94,000	66,000	15,840x10	318,400	43,900
20名程度	XG115	119,000	107,000	15,840x20	542,800	71,200
30名程度	XG135	209,000	250,800	14,370x30	890,900	166,700
50名程度	XG210	289,000	498,500	13,180x50	1,446,500	331,600

（円）

*最長5年間のみ使用できる仕様です
*営業所用等他オプションあります
*Wi-Fiモデルもあります
*2年延長は、（ライセンス＋保守）の2年分の価格です

付録（個人のスマホユーザへ）

無償で使えるスマホセキュリティソフト
・App StoreまたはGoogle Playから「sophos」で検索
・ダウンロードして安全のためお使いください



付録（情報管理が不適切な場合の処罰など）

情報の種類	根拠法による規定		処罰など
個人情報 （マイナンバーを含む）	個人情報保護法	1)虚偽申告命令違反	6か月以下の懲役または30万円以下の罰金、業務停止命令
		2)データベース提供材	1年以下の懲役または50万円以下の罰金
	民法（不法行為による損害賠償709条）		損害賠償
	建設業法		役員または使用人が懲役刑に処せられた場合は営業停止命令
	マイナンバー法 （個人及び法人に対して）		秘密を漏らし、または盗用した者は、3年以下の懲役もしくは150万円以下の罰金。行為者を雇用する法人にも罰金
会社から預かった秘密情報 （外部非公開データなど）	不正競争防止法の営業秘密不正取得・利用行為など		損害賠償、信頼回復措置
自社の秘密情報 （非公開ノウハウなど）	不正競争防止法の営業秘密不正取得・利用行為など		善管注意義務違反に対する関係者からの損害賠償請求（経営者に対する民事訴訟）
上場会社の株価に影響の可能性がある未公開の内部情報	金融商品取引法		内部情報をもとに取引が行われた場合、罰金または課徴金の可能性

連絡先

お薦めしたいSophos製品

- FirewallXG　:UTM
- InterceptX　:End Point
- Phish　Treat:社員教育用
- Cloud Optix:Cloud環境向け

株式会社リナ・システム
http://www.lyna.co.jp
〒102-0074
千代田区九段南4-4-5 さかきばらビル2F
電話 03-3262-6641
Mail: isao-Odakura@lyna.co.jp

◆都営地下鉄新宿線 市ヶ谷駅A3出口より徒歩3分
◆JR市ヶ谷駅より徒歩6分