



侵入されても発症しない新世代セキュリティ

APPGUARD

■ AppGuard ® 正規販売パートナー

株式会社 ITガード （英名：IT Guard Corporation）
（株式会社BluePlanet-works 100%子会社）

2015年設立 資本金（資本準備金含む） 6,100万

代表取締役 前田 悟
執行役員 吉川 剛史（プロダクト技術マネージャー）

社員数：10名（役員、嘱託含む）
取引銀行：みずほ銀行

東京都渋谷区神宮前2-4-11
Daiwa 神宮前ビル 3F

03-6804-2750
<https://www.itgc.co.jp>

アンチウイルスソフトとの違い



APPGUARD



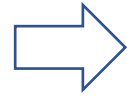
不正な挙動を
制御するため、



既知・未知、
ともに阻止

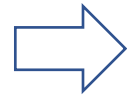
新種のウイルスが次々に企業を攻撃

新しいマルウェアが
作られる数



100万個/日

一つの企業に対して同じ
ウイルスが使われる割合



約0.5%

同じマルウェアが使われないことを示しており、定義ファイル型の製品ではすぐに検知することが難しいと言えます。

直近で起きたサイバー攻撃



2020年11月16日

大阪府中央区平野町三丁目1番3号
株式会社カプコン
代表取締役社長 辻本 春弘
(コード番号:9697 東証第1部)

不正アクセスによる情報流出に関するお知らせとお詫び

株式会社カプコンは、第三者からのオーダーメイド型ランサムウェアによる不正アクセス攻撃を受け、当社グループが保有する個人情報流出の発生を確認いたしました。

また、この攻撃により、当社が保有している個人情報・企業情報が流出した可能性があることを確認しましたので、「2. 流出の可能性がある情報」にて併せてお知らせいたします。

なお、現時点ではコンテンツ開発や事業遂行において支障はございません。

お客様はじめ多くのご関係先にご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。

【被害内容】

- ・顧客情報など
最大35万件が流出
- ・**11億円**ほどの身代金要求
- ・財務状況や社員の給与などが**WEB上に公開**される
- ・システム障害が発生したことによる**業務停止**

ラグナロッカー（犯行グループ）
による攻撃
同種の犯行集団が他にも18集団、
確認されている

2020年にサイバー攻撃を受けた主な企業



ほぼ**ネットワーク全体**が影響を受け、社内でシステム障害が起こるだけでなく、結果的に**海外を含めて**、生産ラインが**2日間**、停止するという事態に追い込まれる。



自社ネットワークが不正アクセスを受け、社内の機密情報等が外部へ漏えいした可能性あり。
(**個人情報**・**企業機密情報**・**防衛省の機微情報**・**他**)

これらの企業以外にもサイバー攻撃を受けながら**公表していない**著名な大企業は**数十社以上**存在します。

大企業ともなれば、セキュリティの**多層防御策**を講じておりますが、**それでも被害を受けている**ことが実情となっています。



最近では中小企業も標的になっており、
大手の取引企業への攻撃の踏み台となるケースが増加している。

Emotetに対抗できていないアンチウイルス

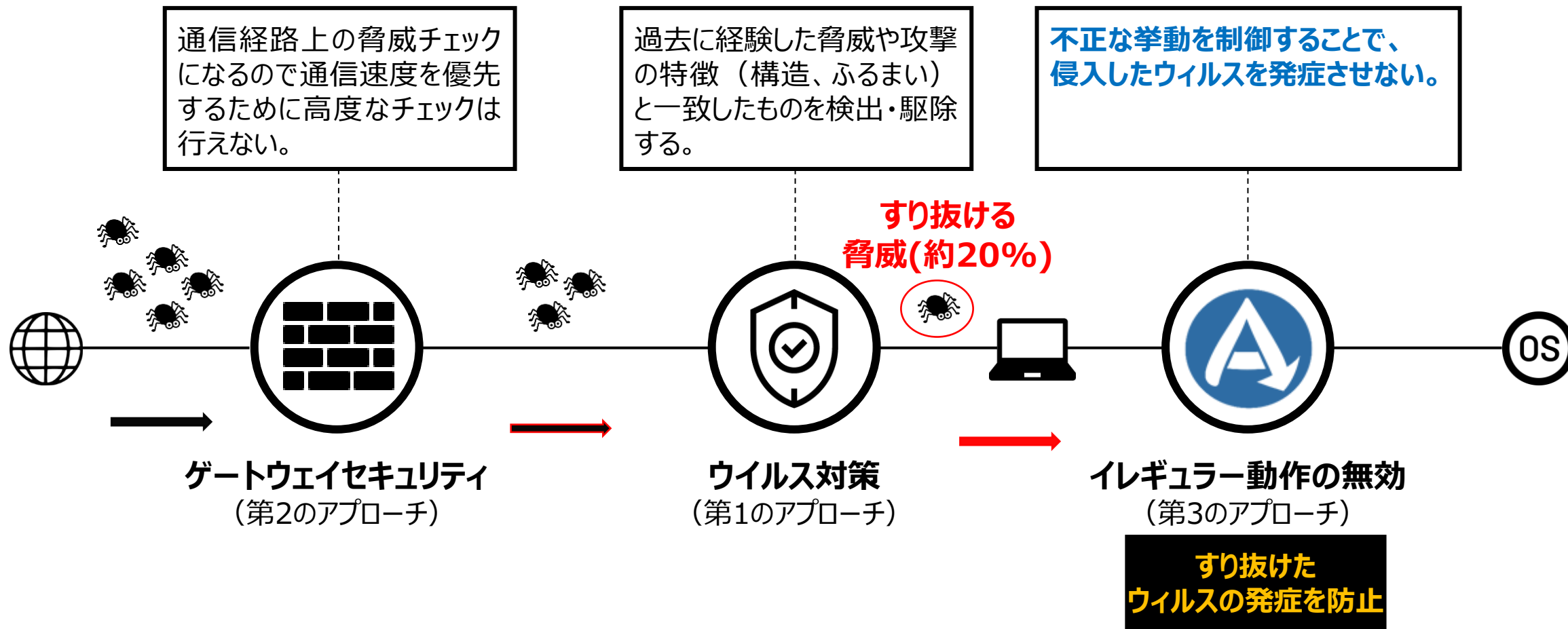
Emotetの検体をランダムで採取してVirus Totalにて検出可能か検査（2020.10.27 AM04:00時点）

	Symantec	TrendMicro	McAfee	F-Secure	ESET	Kaspersky	Microsoft	Cylance
Emotet検体#1	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
Emotet検体#2	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
Emotet検体#3	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知	検知できず
Emotet検体#4	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
Emotet検体#5	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知	検知できず
Emotet検体#6	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知	検知できず
Emotet検体#7	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知	検知できず
Emotet検体#8	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
Emotet検体#9	検知できず	検知できず	検知	検知できず	検知	検知できず	検知	検知できず
Emotet検体#10	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず

Emotet検体#1:d9b79ac09c1bfb45e09d5d9a10303ef99eb66572df7e48e1695a7cdc661904ae
Emotet検体#2:49073674853bc96f1b5d76117cc31b2e48f0c5bd7cf6acc575719ec2e101a997
Emotet検体#3:d09ff7972acdc57a90d3a820d60bcacb3fe23695380388c82ae39dfd9c7d9e1
Emotet検体#4:9122e95b67345a679500db2d8686519d700fc0209878065f774b69b1d1b94995
Emotet検体#5:8f33f8964ac7ae087988eec8f692539de1cd11e6bd47480fee2797aaf2336bc3
Emotet検体#6:a904b40bf78d71b91006ea203a7263cd11782c27f7de18635514a38a45e67eeb
Emotet検体#7:72f3867ffdfb88733bb3f134b0a2a53f39f70475dbb3e45be29499ada36727eb
Emotet検体#8:11e7539b54001557afd9dd62b4cb9d0bd56815d51bcc8e2027ede590a3b87f2
Emotet検体#9:8a7fd67f95a3619931f66425060437758cdd4c69812c2e8e520219dba5ce6db
Emotet検体#10:3674df9b29f7c99f3ec320f0e4af600844f2438dba4a2d948770e44a9e6c83d0

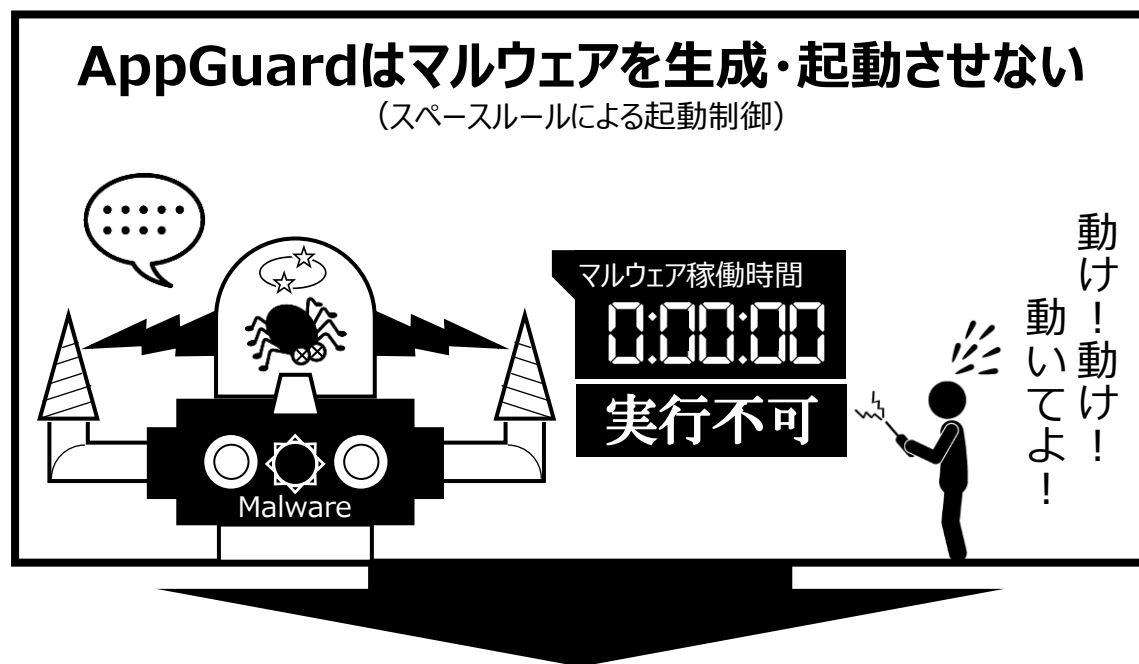
異なる視点で端末を保護する「AppGuard」

侵入した脅威は端末内で発症することができず無害化され ユーザーの業務継続性を担保



AppGuardが提供する攻撃を阻止する2つの制御

AppGuardは2つの制御で 「マルウェア/マルウェア生成ファイルの起動」と「端末の乗っ取り」を阻止



スペースルール



改竄処理の防止

他社製品比較

		マルウェア動作ステージ							防御率	
ソリューション	製品例	初期侵入	マルウェア感染	基盤構築	内部侵入	目的達成	再拡散		既知	未知
		・ 標的型メール ・ Webサイト ・ USBメディア	・ レジストリ変更 ・ ファイル書換え ・ メモリの書換え	・ 侵入経路作成 ・ 端末環境情報の入手 ・ 常駐化	・ 他端末侵入 ・ サーバ侵入 ・ 管理者情報搾取	・ 情報搾取 ・ システム破壊	・ 侵入経路を使用して再侵入	利用する脅威情報		
アンチウイルス								過去	90%	70%
アンチエクスプロイト								過去	90%	70%
ふるまい検知								過去	90%	70%
ホワイトリストリング								利用せず	90%	70%
サンドボックス								過去	90%	70%
EDR								過去	90%	70%
IT資産管理								防御はしない		
AppGuard								利用せず	100%	100%

以降のステージに移行できない

いたちごっこから解放される！

他のセキュリティ対策機能との比較

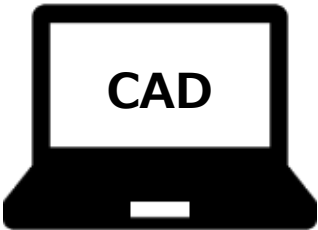
	 APPGUARD	アンチウイルス	振る舞い検知	AI機械学習	EDR	ホワイトリスト
防御の目的	不正プログラムを動作させない	不正プログラムを見つけ出して、駆除する				
防御の手法	プロセスコントロール	定義ファイルによる静的解析	動的解析	機械学習による静的解析	動きを記録・解析	決めたものだけ起動
未知・ランサムウェア・最新の脅威からの防御	○	×	△	△	△	×
ファイルレスマルウェアからの防御	○	×	△	△	△	×
メモリ攻撃からの防御	○	×	△	△	△	×
定期的なディスクスキャンの実施	○ 不要	×	×	△	×	○ 不要
CPU負荷（軽量・軽快）	○ 軽量	×	×	△	×	×
アップデート（定義ファイル・AIエンジン）	○ 不要	×	×	△ 年に数回	×	○ 不要
マルウェアの駆除	×	△	△	△	△	×
常時ネットワーク接続	○ 不要	×	×	△	×	○ 不要
運用コストの削減	○ 可能	×	×	×	×	×

AppGuardはパフォーマンスへの影響を最小化

名前	CPU	メモリ	ディスク	ネットワーク	電力消費	電源使用率
AppGuard Agent Service	0%	12.5MB	0MB/秒	0Mbps	非常に低い	非常に低い
Windows Defender Antivirus Service 通常時	0%	115.8MB	0MB/秒	0Mbps	非常に低い	非常に低い
Windows Defender Antivirus Service クイックスキャン時	16.3%	146.9MB	1.5MB/秒	0Mbps	非常に高い	非常に低い
Symantec Endpoint Protection 通常時（Auto-Protect起動）	0%	133.0MB	0MB/秒	0Mbps	非常に低い	非常に低い
Symantec Endpoint Protection クイックスキャン時	16.3%	173.2MB	10MB/秒	0Mbps	非常に高い	非常に低い

出展：筆者本人の端末にてタスクマネージャーを利用して調査（2020.3.25）

高負荷なアプリケーションの
妨げにならない



低スペックなマシンの動作
にも影響しない



アプリケーション複数同時
起動状態でも影響しない



AppGuard 採用実績



導入企業4,220社、200,000ライセンスを提供

AppGuardファミリー製品比較表

品目	Solo	SBE	Enterprise
対象規模	1～	1～299	1～
管理方式	統合管理不可	AGMSによる統合管理	AGMSによる統合管理
管理機能	—	作成可能な ポリシーテンプレートは無制限	Enterpriseの全ての機能が ご利用可能 作成可能なポリシーテンプレートは 無制限
管理コンソール アカウント数	—	制限なし	制限なし
管理タイプ	オンプレミス	クラウド	クラウド/オンプレミス
適応ポリシー	メーカー推奨ポリシー適用済み (LINE,Zoom,Slackなど)	推奨オリジナルポリシー適用済但し カスタマイズ可能	フルオーダーポリシー
インフラ	スタンドアローン	マルチテナント型 共有データベース	マルチテナント型 お客様専用データベース
インターネット接続要否	必要	不要（閉域環境でも可）	不要（閉域環境でも可）

ITガードが選ばれる 3つの理由!!

1. 圧倒的No.1の導入実績

- AppGuard日本上陸時から販売開始
- 導入ライセンス&導入社数 ともにダントツNo.1
- (株)HIS様はじめ、様々な業種への豊富な導入実績

2. プロ集団の技術力

- 開発メーカー出身の技術者をはじめ、AppGuardを熟知したチームがフルサポート
- AppGuardに関することはもちろん、セキュリティに関するご要望にも柔軟に対応

3. 迅速かつ正確な対応力

- 導入前のご案内から導入後のフォローまで専属チームが担当
- 顧客目線で正確に対応
- 独自の導入マニュアルやサポートツールを駆使して対応

さらに・・・

ITガードだけの専用サイバー保険付！

大規模なDDos攻撃、ゼロディ攻撃を起因したサイバー攻撃被害を補償する当社専用のサイバー保険がAppGuardに自動付帯



世間一般でも
2020年は前年対比1.6倍
の申し込みあり

ITガード専用サイバーセキュリティ保険

エンドポイント製品として業界初のサイバー保険を自動付帯

注：サイバーセキュリティ保険付帯ライセンスはMDであるITガード社/アイセル社を通じて調達したライセンスに限ります。



損保ジャパン日本興亜

補償内容

導入企業に対してAppGuard1ライセンスあたり

①賠償責任

②事故対応特別費用

合計 **500万円** の補償

＜補償額の例＞

10ライセンス 保険金額：500万円×10=5,000万円

50ライセンス 保険金額：500万円×50=2億5,000万円

101ライセンス以上 保険金額：支払い上限5億円

補償項目	内容
賠償責任に関する補償	AppGuard製品を購入した事業者に提起された損害賠償請求について、事業者が負担する損害賠償金等を補償します。
事故時または事故後の対策等に必要な費用の補償	損害賠償請求が発生するおそれがある場合に、その事故に対応するためAppGuard製品を購入した事業者が支出した情報漏えい対応費用や再発防止実施費用等を補償します。

支払いの対象となる損害

「10Gbps以上のDDoS攻撃」または「ゼロデイ攻撃」を受けたことにより生じた、①または②の事由

①ネットワークの所有、使用もしくは管理または情報メディアの提供にあたり生じた偶然な事由

②情報漏洩またはその恐れ

サービス料金

年間サブスクリプションサービスとしてご提供

■ITガードクラウドセキュリティサービス for AppGuard Enterprise/SBE

<AppGuard Enterprise/SBE>

- Agentライセンス
- AppGuard 管理 コンソール
- クラウド利用料※1
- コンソール接続用VPNアカウント※2

<ITガード独自サービス>

- サイバーセキュリティ保険
- AGユーティリティアプリ（20年7月正式リリース）※3
 - ①AppGuard プロテクション簡易コントロール機能
 - ②ソフトウェアセキュアインストール機能
- イベントログ用ダッシュボード（20年7月正式リリース）※3

※1）クラウドサーバーはマルチテナント型の共有インスタンスでのご提供です。

※2）VPNアカウントは標準で最大3カウントまで発行可能。追加1アカウントにつき 年間 ¥ 500 （SBEは1アカウントのみ）

※3）申し込み必要。

・ Enterprise(クラウド型)

台数ボリューム	1～499	500～999	1000～2499	2500～4999	5000～9999	10000～
ITGクラウドセキュリティサービス	¥ 7,500	¥ 7,200	¥ 6,900	¥ 6,600	¥ 6,300	¥ 6,000

・ SBE(クラウド型)

台数ボリューム	1～299
ITGクラウドセキュリティサービス	¥7,500

初期導入費用 別途発生します。個別でお問い合わせください。

■AppGuard Solo

< AppGuard Solo>

- Agentライセンス

<ITガード独自サービス>

- サイバーセキュリティ保険

・ Solo(スタンドアローン型)

台数ボリューム	1～
AppGuard Solo	¥6,000

(税抜価格)

ITガードクラウドセキュリティサービス AppGuard Server for Windows

<AppGuard Server>

- Serverライセンス
- AppGuard 管理 コンソール
- クラウド利用料※1
- コンソール接続用VPNアカウント※2

※1) クラウドサーバーはマルチテナント型の共有インスタンスでのご提供です。

※2) VPNアカウントは標準で最大3カウントまで発行可能。追加1アカウントにつき 年間 ¥ 500 (SBEは1アカウントのみ)

※3) 申し込み必要。

Server (クラウド型)

台数ボリューム	1～9	10～49	50～99	100～
ITGクラウド セキュリティ サービス	¥60,000	¥57,000	¥54,000	要相談

初期導入費用

(税抜価格)

別途発生します。個別でお問い合わせください。

AppGuard 紹介動画



- 長州力出演！「AppGuard（アップガード）」CMメイキング映像公開！

https://youtu.be/yGDR_Es16mk

- TV-CM「飛ぶぞデータ」篇

<https://www.youtube.com/watch?v=JwShKvNjH0Y>

- TV-CM「感染を告げる妖精」編

https://www.youtube.com/watch?v=_6DH_-XxADY

- AppGuard紹介動画「もう、セキュリティで悩まない。」

<https://www.youtube.com/watch?v=tCH8nrLxT8s&t=70s>

- 【おしえて！！AppGuardマン】AppGuard機能紹介

<https://www.youtube.com/watch?v=npvQicT4-Lw>



お問い合わせ先

株式会社ITガード

清水 智也

080-7950-5551

t.shimizu@itgc.co.jp

機能：スペースルールによるマルウェアの起動阻止

